National Security Agency
Cybersecurity Technical Report

Zero Trust Implementation Guideline

Phase Two

January 2026

U/OO/107298-26
PP-25-4758
Version 1.0

Notices and History

Document Change History

Date	Version	Description
January 2026	1.0	Initial publication

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations for National Security Systems, Department of War information systems, and the Defense Industrial Base. This information may be shared broadly to reach all appropriate stakeholders.

Acknowledgements

The National Security Agency (NSA) acknowledges the valuable contribution and support of the Department of War (DoW) Chief Information Officer's Zero Trust (ZT) Portfolio Management Office (PfMO) on this endeavor.

Author(s)

National Security Agency (NSA)
Cybersecurity Directorate

Contact Information

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov

Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov

Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov

Department of War (DoW) Chief Information Office (CIO) Zero Trust (ZT) Portfolio Management Office (PfMO): osd.zt-pfmo@mail.mil

Executive Summary

Zero Trust (ZT) represents a fundamental enhancement in cybersecurity. Rather than relying on perimeter defenses, ZT emphasizes continuous authentication and authorization of every User/Person Entity (PE), device/Non-Person Entity (NPE), and application, operating under the principles of “never trust, always verify” and “assume breach.” This approach is critical for safeguarding sensitive data, systems, and services against increasingly sophisticated cyber threats.

As mandated by Executive Order (EO) 14028, the United States Government (USG) developed several ZT strategies to achieve ZT. These strategies include frameworks, guidelines, and maturity models designed to assist organizations in implementing ZT. Key foundational documents outlining architecture, maturity models, and guidance supporting this effort include:

- National Institute of Standards and Technology (NIST), Zero Trust Architecture Special Publication (SP) 800-207, August 2020
- The Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model, Version 2.0, January 2022
- The Department of War[1] (DoW) Zero Trust Reference Architecture (ZT RA), Version 2.0, July 2022
- The DoW Zero Trust Strategy, Version 1.0, October 2022

The National Security Agency (NSA), using its Cybersecurity authorities and role as National Manager (NM) for U.S. National Security Systems (NSS), developed the Zero Trust Implementation Guidelines (ZIGs), leveraging NIST and DoW published guidance. The ZIGs are intended to assist the DoW, Defense Industrial Base (DIB), NSS, and affiliated organizations with incorporating ZT principles into their processes, enabling them to achieve Target-level ZT, as described in the DoW ZT Framework from the DoW ZT Strategy.

In close partnership with the DoW CIO, and in an effort to organize the 152 ZT Activities contained within the DoW ZT Strategy, five phases were developed (Discovery, Phase One, and Phase Two which are Target-level, and Phase Three and Phase Four, which are Advanced-level). These phases are not doctrinal but are a structured approach to organize the ZT Activities. ZT is a framework; therefore in keeping with that model, the

[1] Per EO 14347, the Department of War (DoW) is an authorized secondary title for the Department of Defense (DoD).

phases outlined in the ZIGs are modular and can be aligned to an organization's specific environment.

The current set of ZIGs consist of a Primer and three ZT Implementation Guidelines (Discovery, Phase One, and Phase Two) designed to assist skilled practitioners in adopting and integrating ZT Target-level Capabilities (42) and Target-level Activities (91). ZIGs for Phase Three and Phase Four may be developed at a later time. These guidelines provide a modular structure adhering to the DoW ZT Framework's Pillars, Capabilities, and Activities, as well as NIST SP 800-207 as guidance for implementation.

The ZIGs align with the DoW Target-level phased implementation approach, with this ZIG (Phase Two) covering the 41 Activities that support the 34 Capabilities in Phase Two. The Activities within the Phase Two ZIG mark the beginning of integrating distinct ZT fundamental solutions within the Component environment. The remaining Target-level Activities and Capabilities are addressed in other ZIGs (Discovery and Phase One), as applicable.

The ZIGs are intended to assist DoW and the NSS communities in implementing ZT concepts to achieve Target-level, as described in the DoW ZT Framework.

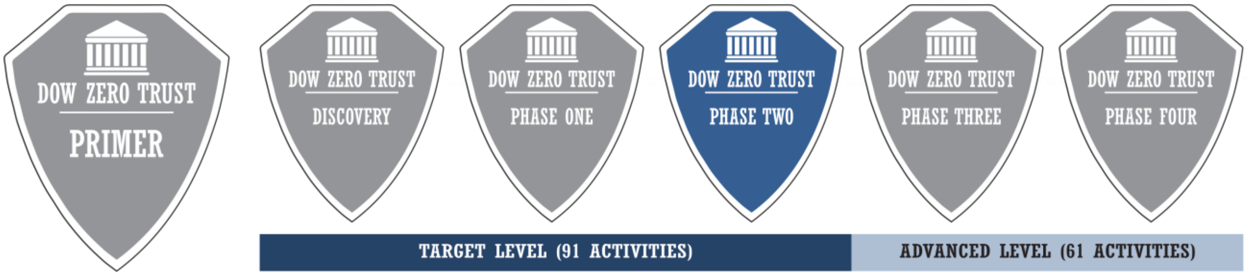


Figure 1: Zero Trust Implementation Guidelines (ZIGs)

Contents

Background

EO 14028, *Improving the Nation's Cybersecurity,* mandates USG agencies to adopt a Zero Trust Architecture (ZTA). Specifically, for NSS networks, National Security Memorandum 8 (NSM-8), *Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems,* implements those cybersecurity requirements mandated by EO 14028. NSM-8 focuses on requirements for NSS as they are defined in 44 U.S.C. § 3552(b)(6), as well as all other DoW and Intelligence Community systems, as described in 44 U.S.C. § 3553(e)(2) and 3553(e)(3). These directives aim to modernize the nation's cybersecurity posture in response to evolving threats by strengthening digital infrastructure, addressing critical vulnerabilities, bolstering cybersecurity practices, and fostering collaboration between the public and private sectors.

A ZT mindset assumes that all environment traffic, users, devices, and infrastructure may be compromised, necessitating a rigorous authentication and authorization process for all access requests. Implementing these measures enhances the security posture of federal networks by rigorously validating every access request, which prevents unauthorized changes, reduces risk of malicious code insertion, and ensures the integrity of software and supply chains, ultimately strengthening the overall cybersecurity of the United States.

Adopt a Zero Trust Mindset

Adopting a ZT mindset involves fundamentally reassessing and rethinking how cybersecurity is approached within an organization. It augments traditional perimeter-based security models, creating a more dynamic approach that assumes no entity can be trusted by default, regardless of its location, inside or outside the environment.

To effectively address the modern dynamic threat environment, organizations should:

- Implement coordinated and comprehensive system monitoring, management, and defensive operations for continuous protection.
- Continuously verify and validate all resource requests and environment traffic.
- Continuously verify and validate the security posture of all devices and infrastructure.
- Prepare for rapid response and recovery, acknowledging the inherent risk incurred in all access approvals to critical resources.

The guiding principles of ZT, outlined in NIST SP 800-207, are the core of a ZTA:

- **Never trust, always verify** – Treat every User/PE/NPE, device, application/workload, and data flow as untrusted. Dynamically authenticate and explicitly approve all activity, adhering to the principle of Least Privilege.
- **Assume breach** – Operate and defend resources under the assumption that an adversary already has presence within the environment. Plan for deny-by-default and heavily scrutinize all users, devices, data flows, and requests. Continuously log, inspect, and monitor all configuration changes, resource accesses, and environment traffic for suspicious activity.
- **Verify explicitly** – Securely and consistently verify access to all resources, using multiple attributes (dynamic and static), to derive confidence levels for contextual access decisions.

Zero Trust Design Concepts

The following are key concepts to address when designing a ZTA:

- **Define mission outcomes** – Derive the ZTA from organization-specific mission requirements that identify the critical DAAS.
- **Architect from the inside out** – First, focus on protecting critical DAAS. Second, secure all paths to access DAAS.
- **Determine who/what needs access to the DAAS to create Access Control policies** – Create security policies and apply them consistently across all environments (e.g., Local Area Network (LAN), Wide Area Network (WAN), endpoint, perimeter, mobile, etc.).
- **Inspect and log all traffic before acting** – Establish comprehensive, complete visibility of all activities across all layers, from endpoints to the environment, to enable analytics that can detect, trace, and make sense of suspicious activity.

ZT is more than an Information Technology (IT) solution; it is a holistic cybersecurity approach. While ZT may leverage technologies or specific products, it is not a singular capability or device. Adopting ZT is a journey that requires integrating capabilities, technologies, solutions, processes, and enablers. This journey necessitates the involvement of stakeholders to ensure alignment and buy-in, a prioritization scheme to focus resources effectively, and a continuous feedback loop for ongoing improvement and adaptation. In support of this holistic cybersecurity approach, the DoW ZT Strategy outlines four (4) high-level strategic goals for achieving ZT applicable to any Component or Enterprise [1]. The goals are:

- ZT cultural adoption
- Secured and defended Information systems
- Technology acceleration
- ZT enablement

These goals encompass supporting functions that drive the successful implementation of ZT and address the enablers and governance to support a successful ZTA. The supporting functions included in the DoW ZT Strategy are discussed throughout the ZIGs, with the exception of policy and training, which are outside the scope of the ZIGs and only discussed briefly here.

- **Policy**: Policies are necessary to ensure the DoW ZT Framework is uniformly applied and fully interoperable across the Enterprise. Enterprise-level processes, policies, and resources may need to be developed, redefined, and synchronized across the applicable Components with ZT principles and approaches.
- **Training**: An Enterprise-wide ZT mindset is essential. It guides the design, development, integration, and deployment of IT across the Enterprise and requires a culture where all personnel are aware of, understand, commit to, and are trained to embrace ZT. A training model should be developed that analyzes the skills needed by the Enterprise to accomplish the mission and/or business needs. Adequate training is fundamental to the ZT process and should address various training needs, including:
    - Awareness Training – Incorporate ZT concepts into ongoing security and privacy literacy training. This training should cover core ZT principles, benefits, and practical implications for daily work.
    - Role-Based Training – Identify the specific roles requiring ZT role-based training. This training, tailored for the assigned duties, may be technical or managerial.
    - Developer Provided Training – Require any system developers, system components, or system services within the environment to provide training on the proper use and operation of the implemented security functions or mechanisms to ensure ZT principles are maintained during operational use.

Purpose

The purpose of this Phase Two ZIG document is to provide an overview and linkage to the overarching guidance provided by the DoW, CISA, and NIST for achieving a ZTA at the Target-level, exclusively for the defined Phase Two Phase Activities and Capabilities. The Phase Two ZIG provides direction and guidance, and outlines the steps to implement the technologies and processes that will enable the Target-level ZT Capabilities, Activities, and Expected Outcomes defined by the DoW ZT Framework.

The prior two ZIGs, Discovery and Phase One, prepare the skilled practitioner to implement and integrate the activities contained in this ZIG, Phase Two. The purpose of the Activities within the Discovery Phase ZIG is to collect information about the organization's environment(s), such as DAAS, Users/PEs/NPEs, etc. The Phase One ZIG Activities build upon or further refine the Component environment(s) to establish a secure foundation that supports ZT Capabilities. Finally, in this ZIG, Phase Two, the Activities mark the beginning of integrating distinct ZT fundamental solutions within the Component environment. Figure 2 depicts the DoW ZT Framework alignment to the ZIGs by ZT Phase (Discovery, Phase One, Phase Two, Phase Three, Phase Four), Level (Target, Advanced), and the associated Capabilities and Activities included in each document. While the DoW ZT Framework used for the ZIGs may not perfectly align with previous NSA Zero Trust Cybersecurity Information Sheet (CSI) publications, the general principles are consistent. NSA is aware of this and plans to update the CSIs in 2026 to better align with the Zero Trust Implementation Guidelines (ZIGs).

ZIGs addressing the Advanced Levels, Phase Three and Phase Four, may be developed at a later date.

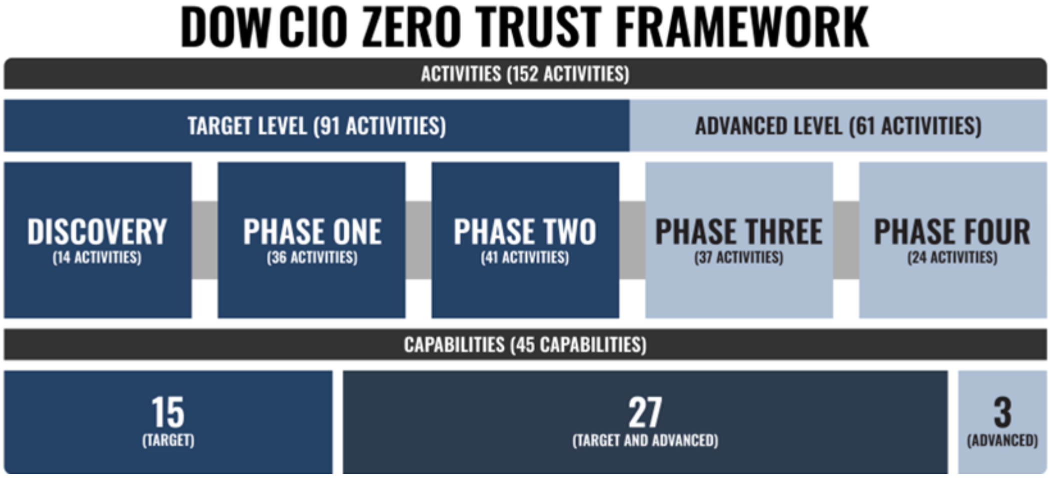

DOW CIO ZERO TRUST FRAMEWORK
ACTIVITIES (152 ACTIVITIES)
TARGET LEVEL (91 ACTIVITIES)
ADVANCED LEVEL (61 ACTIVITIES)
DISCOVERY (14 ACTIVITIES)
PHASE ONE (36 ACTIVITIES)
PHASE TWO (41 ACTIVITIES)
PHASE THREE (37 ACTIVITIES)
PHASE FOUR (24 ACTIVITIES)
CAPABILITIES (45 CAPABILITIES)
15 (TARGET)
27 (TARGET AND ADVANCED)
3 (ADVANCED)

Figure 2: ZIG Alignment to the DoW ZT Framework

Target Audience

This document is designed to be used by skilled practitioners, individuals, stakeholders, and teams responsible for implementing ZT technical and strategic aspects. It may be used within the DoW, DIB, NSS, industry, academia, and affiliated organizations. The target audience includes the following:

- **Technical Implementers/Skilled Practitioners** – Practitioners managing the technical implementation of ZT enabling technologies and configurations.
- **Enterprise Environment Owners** – Stakeholders responsible for maintaining and securing large-scale IT infrastructures.
- **Cybersecurity Leaders** – Professionals tasked with designing, overseeing, and optimizing cybersecurity measures.
- **External Partners and Vendors** – Collaborators providing technologies, services, and/or expertise to support ZT efforts.

Scope

The Phase Two ZIG is designed to guide and support organizations within various environments by providing practical, actionable recommendations to facilitate ZT implementation.

In alignment with the current DoW ZT Framework, the ZIGs are most applicable in an IT Enterprise. Future updates may address other contextual environments, including Operational Technology (OT), Defense Critical Infrastructure (DCI), and/or Tactical/Weapons Systems. The ZIGs will continue to be modified as capabilities and technologies advance.

The Primer and associated ZIGs are **not**:

- Prescriptive or mandatory. Organizations should identify their starting points and tailor the Capabilities and Activities to their specific needs.
- A one-size-fits-all or step-by-step sequential guide to implementing ZT.
- Vendor-specific. Technologies listed in the Capabilities sections are included for consideration, may not contain all possible technologies, and are vendor agnostic.
- Designed to supersede, impact, or alter any existing authority, law, or policy.

Assumptions

The following assumptions drive the Primer and associated ZIGs:

- The ZIGs are not designed or intended to have a fixed implementation start or end point. Organizations have the flexibility to choose their starting point and tailor the guidance to their specific environment.
- Activities can be implemented concurrently.
- Readers have a foundational understanding of cybersecurity architectures, principles, and their organization's Critical Infrastructure and Key Resources (CIKR).
- Readers possess technical expertise in areas, such as Identity and Access Management (IAM), endpoint security, network security, and security analytics.
- Implementing organizations are familiar with ZT, their architecture, and the DoW ZT Framework.

- Personnel have the necessary skills and training to implement Software-Defined Networking (SDN), Development, Security, and Operations (DevSecOps) practices, Artificial Intelligence (AI)/Machine Learning (ML) solutions, data protection capabilities, and security orchestration, including Automation and Orchestration (A&O) and Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines. This includes the ability to leverage cloud-based solutions (e.g., Platform as a Service (PaaS)/Software as a Service (SaaS)/Infrastructure as a Service (IaaS)/Anything as a Service (XaaS), etc.) for ZT implementations.
- Future ZIGs will address the ZT Advanced-level and subsequent Phases (Phases Three and Four).

ZIG Design Methodology

The Phase Two ZIG refines the guidance that the DoW ZT Framework provides for ZTA implementation. It closely follows the DoW ZT Framework’s structure beginning at the Pillar level. The DoW ZT Framework defined Capabilities and associated Activities are further broken down into the implementation process for each Activity.

The ZIG methodology focuses on the framework's Activity Level as the lowest-level element, guiding skilled practitioners in building and tailoring their implementation approach. Each Activity is structured into discrete tasks that are further decomposed into recommended processes and actions to meet the Activity's intent.

The DoW ZT Framework uses Pillars and Capabilities to define the “What” and “Why” of implementing a ZTA. The Activities describe the “Why” and the “How” to achieve these goals.

The ZIGs are intentionally designed with some duplication to ensure that each Capability and Activity can function as a standalone reference. Acronyms are consistently spelled out across sections to promote clarity and modularity. Activity names are italicized throughout the document to enhance visibility and ease of identification.

ZIG Structure

The ZIGs are structured as follows:

Pillars

This section introduces each Pillar pertaining to Phase Two of the DoW ZT Framework. The ZT Pillars provide a framework for securing modern IT systems by emphasizing continuous verification, validation, strict access controls, and data protection. Figure 3 shows a graphical description of the DoW ZT Pillars.

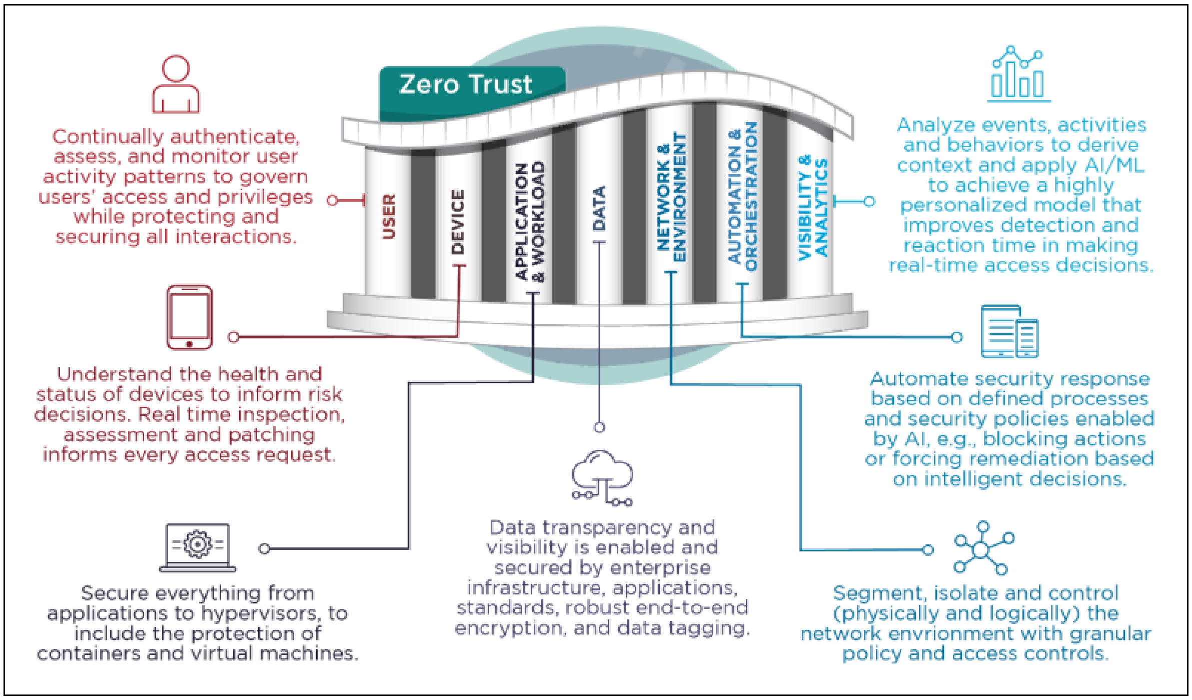
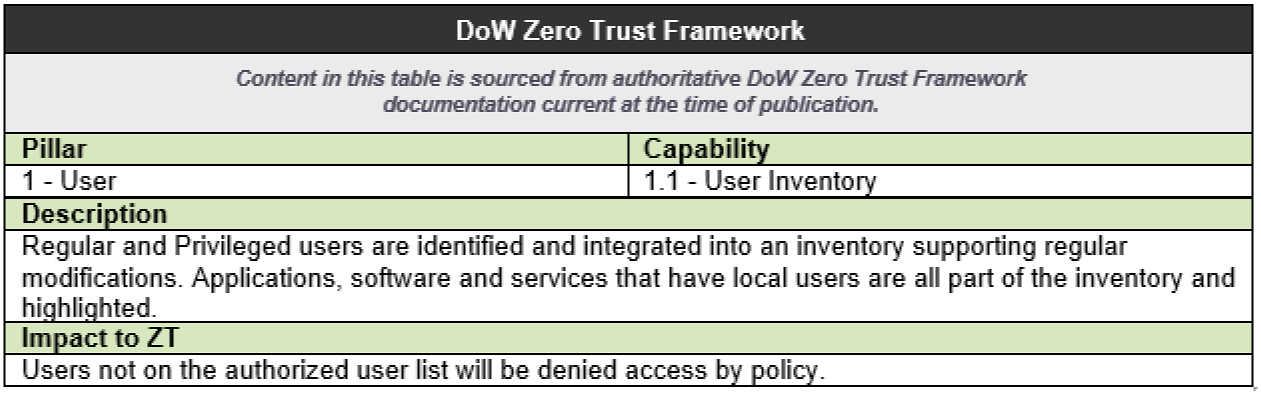

Zero Trust
USER
DEVICE
APPLICATION & WORKLOAD
DATA
NETWORK & ENVIRONMENT
AUTOMATION & ORCHESTRATION
VISIBILITY & ANALYTICS
Continually authenticate, assess, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.
Understand the health and status of devices to inform risk decisions. Real time inspection, assessment and patching informs every access request.
Secure everything from applications to hypervisors, to include the protection of containers and virtual machines.
Data transparency and visibility is enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.
Segment, isolate and control (physically and logically) the network envrionment with granular policy and access controls.
Automate security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.
Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Figure 3: Description of the DoW Zero Trust Pillars

For additional information, see the DoW ZT Framework documents published on the DoW CIO Library, including the Zero Trust Capabilities and Activities, the DoW Zero Trust Strategy, NSA Zero Trust Cybersecurity Information Sheets (CSIs), and the ZT RA [1-11].

Capabilities

This section introduces each Phase Two Capability associated with the DoW ZT Framework. The Capability section precedes the associated Activities and describes each ZT Capability defined by the DoW. It begins with a table similar to Figure 4, which maps to the applicable Pillar and the Capability description. The Pillar and the Capability descriptions shown in Figure 4 are taken from DoW CIO guidance, specifically, the DoW Zero Trust Execution Road Map v 1.1 Data Tables [17]. They are included verbatim, without any changes.



DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
1 - User	1.1 - User Inventory
Description	
Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted.	
Impact to ZT	
Users not on the authorized user list will be denied access by policy.	

Figure 4: Sample Capability Table

Following the Capability table are the Scenario, Positive Impacts, and Technology subsections, which relate to the Capability. The Scenario subsection illustrates practical applications, highlighting how the technologies underpinning each Capability can address specific challenges or opportunities. These scenarios are not comprehensive, nor do they serve to assess a system's ZT implementation. They provide examples of practical applications and considerations, helping stakeholders understand the value and impact of adopting a Capability. This approach supports informed decision-making and aligns the Capability with organizational objectives.

The Positive Impacts subsection provides examples of potential benefits an organization may derive from implementing the Capability.

The Technology subsection includes a representative list of technologies that enable the Capability and is not an all-inclusive list of technologies that an organization could consider.

For additional information, see the DoW ZT Framework documents published on the DoW CIO Library, including the Zero Trust Capabilities and Activities, the DoW Zero Trust Strategy, and the ZT RA [1-3].

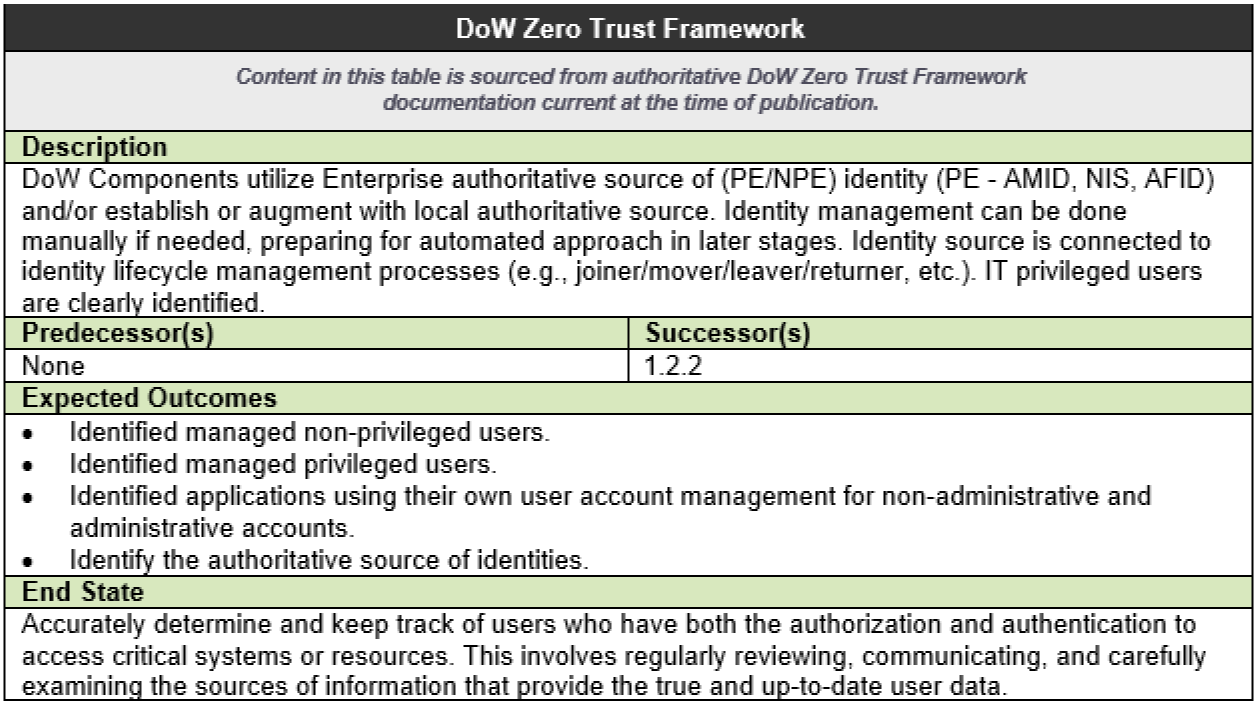
Activities

This section introduces the Activities associated with Phase Two of the DoW ZT Framework. The Activity section begins with the Activity Table, which contains information sourced from the DoW CIO Library’s published updates on ZT Capabilities and Activities, current as of this document’s publication date. Figure 5 depicts a sample Activity Table, and Table 1 details the source of information for each of the sections of the table.

The terms “Enterprise” and “Component” are used throughout the Activities.

- Enterprise refers to an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements, etc.). The Enterprise is responsible for providing policies and guidance to those Components that fall under its purview [12].
- Component refers to the organization implementing ZT.

For additional information, see the DoW ZT Framework documents published on the DoW CIO Library, including the Zero Trust Capabilities and Activities, the DoW Zero Trust Strategy, and the ZT RA [1-3].



DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components utilize Enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity lifecycle management processes (e.g., joiner/mover/leaver/returner, etc.). IT privileged users are clearly identified.	
Predecessor(s)	**Successor(s)**
None	1.2.2
Expected Outcomes	
• Identified managed non-privileged users. • Identified managed privileged users. • Identified applications using their own user account management for non-administrative and administrative accounts. • Identify the authoritative source of identities.	
End State	
Accurately determine and keep track of users who have both the authorization and authentication to access critical systems or resources. This involves regularly reviewing, communicating, and carefully examining the sources of information that provide the true and up-to-date user data.	

Figure 5: Sample Activity Table

Table 1: Activity Table Source of Information

Element	Source	Comment
ID	DoW CIO Library > Defend Against Cyber Attacks > Zero Trust Capabilities and Activities as of 18 Mar 25	
Description		Includes recommended corrections (grammar, capitalization, hyphens, etc.)
Predecessor(s)		
Successor(s)		
Expected Outcomes	DoW CIO Library > Defend Against Cyber Attacks > Zero Trust Capabilities and Activities as of 18 Mar 25	Includes recommended corrections (grammar, capitalization, hyphens, etc.)
End State		Includes recommended corrections (grammar, capitalization, hyphens, etc.)

Considerations

The Considerations subsection clearly explains the prerequisites, challenges, and lessons learned that may influence the successful implementation of each Activity. It highlights processes and applicable documentation and outlines any limitations or dependencies that may affect the execution of specific Activities. By addressing these considerations, the section aims to equip practitioners and decision-makers with the insights needed to effectively plan and adapt the provided guidance to their unique organizational environments.

Implementation

The Implementation subsection provides an actionable roadmap that guides practitioners through the practical execution of each task, ensuring alignment with the overall ZT objectives and facilitating measurable progress toward implementation.

The Implementation section defines high-level Tasks and process steps derived from the Activity Description, Expected Outcomes, and End State outlined in the DoW ZT Framework.

Summary

The Summary subsection provides a high-level overview of key considerations and Expected Outcomes for successfully implementing each Activity, which are presented in a workflow diagram.

- **Readiness Assessment** – Highlights critical ZT readiness questions to consider before implementing the ZT activity, focusing on organizational readiness.
- **Strategic Insights** – A high-level overview that outlines the intended results and benefits expected after implementing the Activity.
- **Expected Outcomes** – The Expected Outcomes are defined in the DoW ZT Framework. To achieve the Expected Outcomes, organizations should align their execution plans with the DoW ZT Strategy.

Appendices

The following Appendices can be found at the end of the document:

- Appendix A – Terms and Definitions
    - A compiled list of terms and definitions specific to the Phase Two ZIG.
- Appendix B – Abbreviations and Acronyms
    - A compiled list of abbreviations and acronyms specific to the Phase Two ZIG.
- Appendix C – References
    - A compiled list of references specific to the Phase Two ZIG.
- Appendix D – Activity Task Diagrams
    - A compilation of activity task implementation diagrams specific to the Phase Two ZIG.

The ZIG Primer Appendices contain all terms and definitions, abbreviations and acronyms, references, and activity diagrams related to the Primer, Discovery, Phase One and Phase Two ZIGs.

User Pillar

Capability 1.2 Conditional User Access

Table 2: Capability 1.2 — Conditional User Access

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
1 - User	1.2 - Conditional User Access
Description	
Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role-based access controls across a federate ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.	
Impact to ZT	
Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component implements a Conditional Access system integrated with its Identity, Credential, and Access Management (ICAM) framework, initially using Role-Based Access Controls (RBACs) for all Users/Person Entities (PEs).
- Over time, the Component enhances its Conditional Access capabilities by mapping application-focused roles to Enterprise attributes, ensuring User/PE access is specific to job functions and required resources.
- The system incorporates dynamic access rules, automatically adjusting access based on User/PE risk profiles, which consider factors like location, login behavior, and device security posture, in alignment with Zero Trust (ZT) principles of continuous verification and Least Privilege.
- A system administrator logs in from an unrecognized device in an unusual location, triggering the Conditional Access system to assign a MEDIUM risk level to the User/PE.
- The administrator's access is restricted to read-only permissions for critical systems and an alert is sent to the Security Operations Center (SOC) for review.
- SOC analysts investigate the activity, confirming that the login was unauthorized and initiated from a compromised account.

- The Component's dynamic access rules escalate the User/PE's risk profile to HIGH, immediately revoking all access and isolating the compromised account from the network, demonstrating the ZT principles of assuming breach and minimizing impact.
- Additional forensic analysis identifies the source of the breach and ensures that no sensitive data was accessed during the incident.
- Regular reviews of Conditional Access policies and Enterprise attributes allow the Component to continuously refine risk assessments and ensure access rules adapt to emerging threats.
- By dynamically managing User/PE risk profiles and fine-grained access controls, the Component successfully prevents unauthorized access while minimizing disruption to legitimate User/PEs, fully embodying ZT principles.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Risk-Adaptive Security: By evolving from static RBAC to dynamic attribute-based access, the Component can automatically adjust security controls based on real-time risk factors, strengthening the protection of sensitive resources without hampering legitimate work.
- Operational Flexibility: The maturity progression allows the Component to implement access controls that adapt to changing business needs, supporting new workflows and organizational structures without requiring complete security redesigns.
- Reduced Administrative Burden: As the Component advances through maturity levels toward attribute-based access, it significantly decreases manual access management tasks, as permissions adjust automatically based on Enterprise attributes rather than requiring explicit assignment.
- Enhanced User Experience: Dynamic access rules enable seamless authentication experiences tailored to risk levels, eliminating unnecessary friction for low-risk scenarios while applying appropriate verification steps when needed.
- Improved Compliance Posture: The Component can demonstrate more sophisticated governance by showing how access is continuously evaluated against Enterprise attributes and policies, providing better alignment with regulatory requirements for Least Privilege access.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Attribute-Based Access Control (ABAC)
- Identity as a Service (IDaaS)
- Identity, Credential, and Access Management (ICAM)
- Platform as a Service (PaaS)
- Role-Based Access Control (RBAC)

Activity 1.2.1 Implement Application-Based Permissions per Enterprise

Table 3: Activity 1.2.1 — Implement Application-Based Permissions per Enterprise

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW ICAM governance establishes a set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Lifecycle Management Part 1" activity process for a complete Enterprise standard. The Enterprise Identity, Credential, and Access Management (ICAM) solution are enabled for adding/updating attributes within the solution to better support identity federation. Remaining Privileged Access Management (PAM) activities are approved and tailored as specified by roles.	
Predecessor(s)	**Successor(s)**
None	None
Expected Outcomes	
• Enterprise roles/attributes needed for user authorization to application functions and/or data have been vetted and approved through the ICAM governance processes. • Approved Component ICAM implementations will maintain and make available authoritative information about their personnel (i.e., attributes and entitlements), while maximizing the usage of self-service attributes and entitlements. • Components identify attributes associated with PAM activities within their environment. • Component ICAM implementation obtains authoritative information about personnel (i.e., attributes, and entitlements) from a central attribute source once available, or from other Components using standard profiles.	
End State	
Authoritative attributes required to implement conditional user access into applications are available to support privileged access management.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Consider completing Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)* prior to this activity, to enforce authentication and authorization.
- Consider completing Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1* prior to this activity, to obtain existing Privileged Access Management (PAM) attributes.
- Enterprise has defined Identity, Credential, and Access Management (ICAM) governance and made the service(s) available.

- A mitigation plan has been defined for legacy systems.
- ICAM governance is enabling asset management.
- For completeness, this activity should integrate with Activity 1.5.2 (Phase Two) – *Enterprise Identity Lifecycle Management (ILM) Part 1*.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 4: Implementation Tasks for Activity 1.2.1 — Implement Application-Based Permissions per Enterprise

Leverage the Enterprise ICAM requirements.
Obtain the Enterprise ICAM authoritative policy/guidance: ☐ Review the approved Enterprise authoritative policy/guidance for ICAM governance on User's/Person Entity's (PE's) roles and attributes. ☐ Review the latest Enterprise ICAM strategy related to the creation of digital entities, maintenance of associated attributes, and issuance of credentials for User/PE. **Review, verify, and validate requirements:** ☐ Determine specific application functions and data that require access control. ☐ Verify and validate the roles and attributes needed for authorization. ☐ Verify and validate the accuracy of data, including data received from other data sources [13]. **Review roles and attributes:** ☐ Review roles based on job functions, responsibilities, and access needs. ☐ Verify and validate that the assigned Users/PEs to roles have appropriate access. ☐ Identify attributes such as User identity, role, department, location, device type, time of access, and other relevant factors to make dynamic access decisions.
Identify Enterprise-defined PAM attributes to associate with privileged Users/PEs.
Leverage Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1,* to verify and validate previously established PAM attributes: ☐ User Attributes: Username, role, department, and contact info. ☐ Access Attributes: Access levels, permissions, and entitlements.

☐ Session Attributes: Start and end times, session duration, and session logs.

☐ Authentication Attributes: Multi-Factor Authentication (MFA) status and authentication methods used.

☐ Audit Attributes: Access logs, change logs, and compliance reports.

Assess current PAM activities:

☐ Create an inventory of remaining associated activities.

☐ Identify the tools and methods currently used for PAM activities.

☐ Identify any gaps in the implementation of the current PAM.

Verify and validate the migration plan:

☐ Map the identified PAM attributes to the corresponding features in the chosen or existing PAM solution.

☐ Plan to migrate the remaining User/PE data, access permissions, and session logs to the PAM solution.

☐ Test the migration process in a controlled environment to ensure data integrity and functionality.

☐ Integrate the PAM solution with remaining systems (e.g., Identity and Access Management (IAM), directories, logging systems, etc.).

Integrate PAM into the Enterprise ICAM solution.

Review, verify, and validate the centralized identity store:

☐ Verify, validate, and establish that an approved single or cluster of authoritative centralized source(s) is leveraged by both PAM and ICAM solutions for consistent access control across the Component.

☐ Review, verify, and validate the permission-based access request workflow for seamless integration.

Maintain secure credential management:

☐ Verify and validate capability to associate digital identity with an authoritative source of truth.

Leverage the MFA capability building block from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP),* to enforce authentication and authorization:

☐ Implement authentication and authorization mechanisms to ensure that only approved systems and Users/PEs can access the attribute data.

Establish and maintain secure access management:

☐ Leverage trusted identities and authoritative credentials to develop and map permission-based access control policy to resources.

Enable built-in capability for federation integration:

☐ Develop and enable cross-boundaries trust and policy-based access control across multiple Components and approved partners.

Monitor and update:

☐ Continuously monitor the connection and data synchronization process to ensure data accuracy and consistency.

☐ Implement mechanisms to manage updates and changes in the centralized repository.

Verify and validate implementation activity for expected outcomes.
Enable continuous monitoring and logging capabilities to support verification and validation of the activity: ☐ Run routine and periodic testing to ensure compliance and application access control. ☐ Identify and remediate potential excessive access privileges. ☐ Monitor and audit any security violations caused by privilege misalignment.

Summary

This diagram outlines the Activity 1.2.1 (Phase Two) – *Implement Application-Based Permissions per Enterprise* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on approved Identity, Credential, and Access Management (ICAM) implementations and application-based User/Person Entity (PE) roles and permissions. It highlights key questions for managing Component roles/attributes necessary for User/PE approval, strategic insights driving implementation, and expected outcomes surrounding approved ICAM and Privileged Access Management (PAM) implementations.

Table 5: Activity 1.2.1 — Implement Application-Based Permissions per Enterprise - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the Enterprise role and attribute schema used for User/ PE authorization to application functions and data? 2. How is self-service functionality for adding/updating attributes managed in the Enterprise ICAM solution? 3. What processes are in place to ensure that privileged activities are fully migrated to the PAM solution?

STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for obtaining ICAM governance-approved Enterprise roles and attributes, ensuring alignment with Enterprise guidance and regulatory standards to control user approval for application functions and data. • The Component demonstrates compliance by implementing a vetted process to confirm that Enterprise roles and attributes used for approval have undergone ICAM governance review, maintaining authoritative information about User/ PE attributes and entitlements. • The Component provides evidence that these Enterprise roles and attributes are integrated into Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) models, dynamically adjusting access based on real-time conditions, ensuring that all attribute data is accurate, tamper-proof, and consistently managed. • The Component ensures that PE activities related to privileged access are aligned with the PAM solution, migrating any remaining PAM attributes and activities to the centralized PAM platform and maintaining continuous monitoring and auditing. • The Component securely obtains authoritative personnel attributes and entitlements from a central or federated Enterprise source using standard profiles, maintaining connectivity, synchronizing data, and monitoring updates, thereby ensuring that the Identity Lifecycle Management (ILM) processes remain consistent, compliant, and aligned with Enterprise standards.

EXPECTED OUTCOMES

1. Enterprise roles/attributes needed for user authorization to application functions and/or data have been vetted and approved through the ICAM governance processes.

2. Approved Component ICAM implementations will maintain and make available authoritative information about their personnel (i.e., attributes and entitlements), while maximizing the usage of self-service attributes and entitlements.

3. Components identify attributes associated with PAM activities within their environment.

4. Component ICAM implementation obtains authoritative information about personnel (i.e., attributes, and entitlements) from a central attribute source once available, or from other Components using standard profiles.

Activity 1.2.2 Rule-Based Dynamic Access Part 1

Table 6: Activity 1.2.2 — Rule-Based Dynamic Access Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components utilize the rules from the "Periodic Authentication" activity to build rules enabling and disabling privileges dynamically. IT Privileged user accounts utilize the PAM solution to move to dynamic privileged access using Just-in-Time (JIT) access and Just Enough Administration (JEA) methods.	
Predecessor(s)	**Successor(s)**
1.1.1, 1.8.1	1.2.3, 7.6.1
Expected Outcomes	
• Access to applications/services functions and/or data is limited to users with appropriate Attribute-Based Access Control (users, devices, environment, etc.), allowing for granular and flexible control. • All possible applications use JIT/JEA permissions for administrative users.	
End State	
Periodic challenges occur where access is affected if challenge is failed within accepted response parameters. Access is always predicated on authentication and authorization with activity happening (decisions made) in real-time.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 1.1.1 (Discovery) – *Inventory User* and Activity 1.8.1 (Phase One) – *Single Authentication* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Consider completing Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1* prior to this activity, to leverage the Privileged Access Management (PAM) solution.
- Consider completing Activity 1.8.2 (Phase Two) – *Periodic Authentication* prior to this activity, to leverage established rules that determine how User/Person Entity (PE) privileges are adjusted.
- Recommend strongly assured methods for all personnel with access to critical resources [5].
- Verification and validation of a PAM solution assumes that the Component has implemented a Security, Incident, and Event Management (SIEM) solution.

- Effectively leveraging Just-in-Time (JIT) and Just Enough Administration (JEA) will involve reassigning Users/Person Entities (PEs) to appropriate roles and defining rules that grant temporary privileged access based on those roles and contextual factors.
- Activity 1.2.3 (Phase Three) – *Rule-Based Dynamic Access Part 2* and Activity 7.6.1 (Phase Three) – *AI-Enabled Network Access* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 7: Implementation Tasks for Activity 1.2.2 — Rule-Based Dynamic Access Part 1

Implement a process to adjust User/PE privileges dynamically based on rules established in Activity 1.8.2 (Phase Two) – *Periodic Authentication*.
Review authentication rules: ☐ Leverage previously established rules that determine how User/PE privileges should be adjusted based on authentication events. Rules could be based on the frequency of authentication, the method of authentication (e.g., Multi-Factor Authentication (MFA), etc.), or the authentication context (e.g., location, device, etc.). **Set up an authentication mechanism:** ☐ Implement an authentication method that can trigger events based on authentication outcomes. • This could involve integrating with an existing Identity and Access Management (IAM)/Identity, Credential, and Access Management (ICAM) solution, from Activity 1.2.1 (Phase Two) – *Implement Application-Based Permissions per Enterprise*. **Implement event handling:** ☐ Configure event handling to listen for authentication events and apply the corresponding rules to adjust User/PE privileges. • This could include using message queues, webhooks, or direct Application Programming Interface (API) calls. **Monitor and audit:** ☐ Continuously monitor the system to ensure that privileges are being adjusted correctly. Implement auditing to track changes in User/PE privileges and ensure compliance with security policies.

Implement Attribute-Based Access Control (ABAC) to limit access to applications/services and/or data.

Expand User/PE attributes in support of ABAC:

☐ User/PE attributes (e.g., role, department, clearance level, location, etc.).

☐ Resource attributes (e.g., resource type, classification, owner, etc.).

☐ Environment attributes (e.g., time, Internet Protocol (IP) address, device type, etc.).

Define policies:

☐ Create policies that specify which attributes are required to access specific resources or actions.

Configure an ABAC/logic engine:

☐ Utilize an ABAC**/**logic engine to evaluate policies and make access control decisions.

Integrate with applications:

☐ Integrate the ABAC engine with all the applications, to the greatest extent possible, to enforce access control decisions. Configure the application to query the ABAC**/**logic engine before granting access to resources or actions.

Monitor and audit:

☐ Continuously monitor access control decisions and audit logs to verify and validate policy compliance and detect any anomalies.

Leverage the PAM solution, selected in Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1*, to move accounts to dynamic privileged access using JIT and JEA access control methods.

Integrate JIT and JEA into existing PAM solution:

☐ Assess the existing PAM solution, from Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1*, to determine if it supports JIT and JEA.

- If the PAM solution does not support JIT and JEA, select and implement a PAM solution that does support JIT and JEA.

Refine privileged roles and tasks in support of JEA:

☐ Leverage previously defined roles and tasks that require privileged access and reassess the minimum permissions required to perform these tasks.

Configure JIT access:

☐ Configure access to grant privileged access only when needed and for a limited time, as defined by the Component.

☐ Configure approval workflows for JIT access requests.

Implement JEA configurations:

☐ Create JEA configurations to limit the scope of administrative tasks.

Integrate with existing systems:

☐ Integrate the PAM solution with your existing IAM systems, directories, and applications.

☐ Ensure the PAM solution can manage and monitor privileged access across all systems.

Monitor and audit:

☐ Continuously monitor privileged access sessions and audit logs to ensure compliance with security policies.

☐ Implement alerting for any suspicious, unapproved activities.

Verify and validate the integration of the PAM solution with SIEM.

Identity integration points:

☐ Determine the specific integration points between PAM and SIEM solutions.

☐ Configure the PAM solution to send log and event data to the SIEM solution.

SIEM integration:

☐ Ensure the PAM solution can push event information to the established SIEM solution.

☐ Ensure the SIEM correctly assimilates the event information to provide actionable intelligence.

Verify and validate integration functionality.

☐ Regular audits should be performed to verify and validate that the PAM solution is functioning as expected.

- Demonstrate that User/PE access is managed correctly in accordance with the JIT/JEA provisioning.
- Strongly recommend, at a minimum, an annual audit.

☐ Continuously monitor SIEM integration to ensure the PAM logs and events are correctly forwarded.

Summary

This diagram outlines the Activity 1.2.2 (Phase Two) – *Rule-Based Dynamic Access Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on enabling and disabling basic rules for privileges. It also highlights key questions for managing high-risk User/Person Entity (PE) accounts, strategic insights driving implementation, and expected outcomes including implementation of Attribute-Based Access Controls (ABACs) and Just-in-Time (JIT)/ Just Enough Administration (JEA) methods.

Table 8: Activity 1.2.2 — Rule-Based Dynamic Access Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are basic rules for enabling and disabling privileges dynamically implemented? 2. How are high-risk User/ PE accounts managed using JIT and JEA methods?

STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for dynamically adjusting User/ PE privileges based on periodic authentication events, ensuring all privileged access methods (e.g., strong Multi-Factor Authentication (MFA), JIT, JEA, etc.) align with established rules and security standards. • The Component demonstrates compliance by implementing ABACs for application and service functions or data, enforcing continuous monitoring and auditing to maintain adherence to defined attribute-based policies. • The Component integrates a Privileged Access Management (PAM) solution that supports JIT and JEA controls, confirming that privileged roles are clearly defined, scoped, and managed through PAM workflows. • The Component provides evidence that PAM solutions are fully integrated with Security Information and Event Management (SIEM) solutions, ensuring logs and events are forwarded, parsed, and correlated to detect and respond to anomalous privileged activities in real-time. • The Component regularly monitors, audits, and refines its Identity and Access Management (IAM), ABAC, PAM, and SIEM integrations, providing compelling evidence of compliance and the effectiveness of these controls in dynamically managing User/PE privileges and mitigating identity-related risks.

EXPECTED OUTCOMES
1. Access to applications/services functions and/or data is limited to users with appropriate ABAC (users, devices, environment, etc.), allowing for granular and flexible control. 2. All possible applications use JIT/JEA permissions for administrative users.

Capability 1.4 Privileged Access Management (PAM)

Table 9: Capability 1.4 — Privileged Access Management (PAM)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
1 - User	1.4 - Privileged Access Management (PAM)
Description	
The capability focuses on removal of permanent administrator/elevated privileges by first creating a Privileged Account Management (PAM) system and migrating privileged users to it. The capability is then expanded upon by using automation with privilege escalation approvals and feeding analytics into the system for anomaly detection.	
Impact to ZT	
Critical assets and applications secured, controlled, monitored, and managed through limits on admin access.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component implements a Privileged Access Management (PAM) solution, requiring all Users/Person Entities (PEs) with administrator privileges to be migrated to the centralized PAM solution.
- Permanent elevated privileges are removed, and User/PEs are required to request Just-In-Time (JIT) access for administrative tasks, aligning with Zero Trust (ZT) principles by ensuring privileges are granted only when needed and for a limited time.
- Privileged accounts are secured in a password vault, accessible only through the PAM solution with strict authentication requirements.
- To enhance monitoring, the Component integrates the PAM solution with its security analytics platform, enabling real-time detection and response to unusual privilege usage patterns.
- A privileged User/PE requests access to a critical database for routine maintenance, triggering an automated privilege escalation approval workflow.
- The PAM solution uses analytics to evaluate the request against historical patterns, identifying it as legitimate and granting temporary access.
- Later, an anomaly is detected when another privileged User/PE requests access to sensitive resources at an unusual time, from an unapproved device.

- The PAM solution flags the request, denies access, and alerts the Security Operations Center (SOC) for investigation.
- SOC analysts confirm that the flagged request was an attempt by a compromised privileged account, which was stopped before any damage occurred.
- By controlling, monitoring, and auditing privileged accounts, the Component reduces the risk of insider threats and unauthorized access to critical assets, reinforcing the ZT focus on minimizing trust assumptions and ensuring compliance with Enterprise requirements.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security for Critical Systems: PAM ensures that only approved individuals can access sensitive systems, reducing the risk of insider threats and external attacks.
- Stronger Access Controls: By enforcing the principle of Least Privilege, PAM limits access to only what is necessary, preventing excessive permissions that could lead to security breaches.
- Improved Auditability and Compliance: PAM provides detailed logs and session recordings, helping the Component meet regulatory requirements and monitor privileged account activity.
- Reduced Risk of Credential Compromise: By centralizing and securing privileged credentials, PAM minimizes the chances of password theft, misuse, or exposure.
- Greater Operational Efficiency: Automating access requests and approvals streamlines workflows, reducing administrative overhead while maintaining strong security controls.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Data Loss Prevention (DLP)
- Encryption and Key Management
- Identity, Credential, and Access Management (ICAM)
- Just Enough Access (JEA)
- Just-in-Time (JIT) Access
- Privileged Access Management (PAM)
- Role-Based Access Control (RBAC)

Activity 1.4.2 Implement System and Migrate Privileged Users Part 2

Table 10: Activity 1.4.2 — Implement System and Migrate Privileged Users Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components utilize the inventory of supported and unsupported Applications/Services for integration with the Privileged Access Management (PAM) solution to extend integrations. PAM is integrated with the more challenging Applications/Services to maximize PAM solution coverage. Exceptions are managed in a risk-based methodical approach with the goal of migration off and/or decommissioning Applications/Services that do not support the PAM solution.	
Predecessor(s)	**Successor(s)**
1.4.1	1.4.3
Expected Outcomes	
• Privileged activities are migrated to PAM and access is fully managed.	
End State	
Ensure secure and controlled access to privileged accounts and resources through fully implemented PAM solution, mitigating the risk of unauthorized access and potential cyber threats.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Utilize a risk-based methodology to determine decommission or exception.
- Activity 1.4.3 (Phase Three) – *Real-Time Approvals and Just-in-Time (JIT) and Just Enough Administration (JEA) Analytics Part 1* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 11: Implementation Tasks for Activity 1.4.2 — Implement System and Migrate Privileged Users Part 2

Leverage inventory, from Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1,* and migrate supported applications/services to Privileged Access Management (PAM).
Review inventory: ☐ Obtain and review the inventory of applications and services that require privileged access. ☐ Ensure the inventory includes application names, types, privileged accounts, and current access methods. **Leverage the Component PAM solution:** ☐ Leverage the Component PAM solution, from Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1*. **Plan the migration:** ☐ Develop a migration plan that includes timelines, resources, and steps for migrating each application/service to PAM. ☐ Prioritize applications based on criticality and risk. **Integrate applications/services:** ☐ Integrate each application/service with the PAM solution. ☐ Configure the application to use the PAM solution for authentication and access control. **Test, verify, and validate:** ☐ Test the integration to ensure that privileged access is managed correctly. ☐ Verify and validate that the PAM solution is functioning as expected and that access controls are enforced. **Monitor and audit:** ☐ Continuously monitor the PAM solution to ensure privileged access is managed securely. ☐ Perform regular audits to verify and validate compliance with security policies.
Obtain approval for unsupported applications/services.
Identify unsupported applications/services: ☐ Review the inventory of applications and services to identify those not currently supported by the PAM solution. **Assess risks:** ☐ Conduct a risk assessment to understand the potential security risks of managing these applications and services outside the PAM solution. **Develop a proposal:** ☐ Develop a proposal outlining the need to manage unsupported applications and services. ☐ Identify what risks are involved. ☐ Identify compensating controls to be implemented.

Seek approval: ☐ Present the proposal to relevant stakeholders to obtain approval. **Implement compensating controls:** ☐ Implement identified compensating controls to mitigate the risks associated with managing unsupported applications and services. ☐ Implement monitoring, logging, and access controls. **Document and monitor:** ☐ Document the approval process. ☐ Document compensating control implemented. ☐ Verify and validate continuous monitoring of applications and services to ensure the implemented controls are effective.
Decommission applications/services not approved.
Request for exception or decommission: ☐ System owners request exceptions for the applications/services that cannot be integrated into the PAM solution. ☐ Manage exceptions based on established risk methodologies. ☐ Migrate applications/services that cannot be integrated into the PAM solution or are not eligible to be decommissioned.
Ensure all privileged accesses are migrated and managed with the PAM solution.
Identify privileged accounts: ☐ Consolidate privileged accounts and secure access rights safely for centralized management. **Audit the PAM system:** ☐ Enforce the separation of duties principle to restrict admin access privileges from PAM system monitoring and audit capabilities, requiring a set of separate credentials for each mission task [14]. ☐ Deploy PAM in conjunction with Multi-Factor Authentication (MFA) to add an extra layer of protection, requiring Users/Person Entities (PEs) to provide additional verification and validation [14]. **Continuous authentication:** ☐ Apply risk-based authentication decisions and mechanisms to assess login attempts and access requests based on user behavior and device posture [6]. **Implement Least Privilege:** ☐ Audit all privileged access processes and solutions to set a Least Privilege baseline [6]. ☐ Restrict privileged accounts to specific personnel or roles to prevent day-to-day Users/PEs from accessing privileged functions or information.

Implement Just-in-Time (**JIT):** ☐ Employ JIT access control methods to grant privileges to controlled resources only for predetermined periods of time on an as-needed basis.
Ensure all privileged accesses are fully integrated with the PAM solution.
Test, verify, and validate: ☐ Test the integration to ensure that privileged access is managed according to policy. ☐ Verify and validate that the PAM solution is functioning as expected and that access controls are enforced. **Monitor and audit:** ☐ Continuously monitor the PAM solution to ensure privileged access is managed securely. ☐ Perform regular audits to verify and validate compliance with security policies.

Summary

This diagram outlines the Activity 1.4.2 (Phase Two) – *Implement System and Migrate Privileged Users Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on built-in account management tools. It presents strategic insights that drive implementation and expected outcomes, including the incorporation of applications that support Privileged Access Management (PAM) solutions.

Table 12: Activity 1.4.2 — Implement System and Migrate Privileged Users Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are privileged activities migrated to the PAM solution? 2. How are unsupported applications/services managed in a risk-based approach?

STRATEGIC INSIGHTS
• The Component defines a systematic approach for migrating privileged users, applications, and services to the PAM solution selected in Activity 1.4.1 (Phase One) – Implement System and Migrate Privileged Users Part 1, leveraging existing inventories and prioritizing based on risk and criticality. • The Component demonstrates security and compliance by enforcing PAM integration, implementing Least Privilege and Just-in-Time (JIT) access controls, and applying risk-based authentication to manage privileged accounts securely across the remaining applications/services. • The Component provides verifiable enforcement through integration testing, verification, validation, and continuous monitoring, ensuring all privileged access is managed, logged, and audited within the PAM framework. • The Component leverages compensating controls for unsupported applications, enforcing Multi-Factor Authentication (MFA) and security monitoring to mitigate risks when full PAM integration is not feasible. • The Component ensures ongoing security by enforcing the separation of duties, continuously auditing privileged access, and adapting access policies to evolving threats and organizational requirements.

EXPECTED OUTCOMES
1. Privileged activities are migrated to PAM and access is fully managed.

Capability 1.5 Identity Federation and User Credentialing

Table 13: Capability 1.5 — Identity Federation and User Credentialing

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
1 - User	1.5 - Identity Federation and User Credentialing
Description	
The initial scope of this capability focuses on standardizing the Identity Lifecycle Management (ILM) processes and integrating with the standard Component IdP/IdM solution. Once completed the capability shifts to establishing an Enterprise ILM process/solution either through a single solution or identity federation.	
Impact to ZT	
Visibility and accuracy of user authentication information is increased, to include DoW users and users managed by other agencies. Users lacking sufficient credentials are denied access according to established policies.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component standardizes its Identity Lifecycle Management (ILM) processes by integrating its existing Identity Provider (IdP) and Identity and Access Management (IAM) solutions, ensuring consistent management of User/Person Entity (PE) credentials.
- As part of the integration, a single process is established for issuing, updating, and revoking User/PE and device credentials across all systems.
- The Component expands its ILM processes into an Enterprise solution, enabling identity federation to share authentication and authorization data securely across trusted domains, reinforcing Zero Trust (ZT) by verifying and validating every access request regardless of origin.
- A Single Sign-On (SSO) capability is implemented, allowing authenticated Users/PEs to access multiple systems and applications without requiring repeated logins.
- A contractor attempts to access a restricted resource using an expired credential. The federation system detects the invalid credential, denies access, and automatically notifies the contractor's agency to issue updated credentials.
- A routine audit identifies gaps in credential issuance timelines, prompting the Component to automate the process of deactivating credentials when User/PEs leave or their roles change.

- The Component establishes trust domains with other agencies, sharing real-time identity data to provide seamless access for inter-agency collaborations while maintaining strict authentication policies.
- An unauthorized login attempt from a non-federated domain is blocked and an alert is sent to the Security Operations Center (SOC) for review.
- Analysts confirm the attempt was part of a phishing attack targeting federated credentials and strengthen cross-domain authentication policies based on the findings.
- By standardizing and federating ILM processes, the Component improves visibility and accuracy of User/PE authentication information, reducing manual errors, enhancing User/PE convenience, and ensuring adherence to ZT principles.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Seamless Access Across Systems: Identity federation enables users to access multiple applications and services with a single set of credentials, reducing the need for multiple logins and improving user experience.
- Stronger Security and Access Control: Centralized User/PE credentialing ensures consistent authentication policies across the Component, reducing the risk of unapproved access.
- Improved Compliance and Auditing: By consolidating Identity Management (IdM), the Component gains better visibility into User/PE access and activity, supporting regulatory compliance and security audits.
- Reduced Password Fatigue and Information Technology (IT) Overhead: Users/PEs no longer need to manage multiple passwords, decreasing password-related support requests and administrative burden.
- Enhanced Collaboration and Scalability: Federated identity allows seamless integration with external partners, cloud services, and third-party applications, making it easier for the Component to scale securely.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Automated Provisioning/Deprovisioning
- Attribute-Based Access Control (ABAC)
- Role-Based Access Control (RBAC)
- Identity Governance and Administration (IGA)
- Single Sign-On (SSO) and Federation

Activity 1.5.2 Enterprise Identity Lifecycle Management (ILM) Part 1

Table 14: Activity 1.5.2 — Enterprise Identity Lifecycle Management (ILM) Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Specified policies and supporting process are followed by DoW Components. Components implement the Enterprise Identity Lifecycle Management process for the maximum number of identities, attributes, groups, credentials, and permissions. Exceptions to the policy are managed in a risk-based methodical approach.	
Predecessor(s)	**Successor(s)**
1.5.1	1.5.3
Expected Outcomes	
• Automated identity lifecycle processes. • Integrated with Enterprise ICAM process and tools.	
End State	
Implementation of consistent and well-defined processes and controls for managing the maximum number of identities in the lifecycle.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM)* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Identify if the Component will need to support federation.
- Multi-Factor Authentication (MFA) has been implemented per Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*.
- Activity 1.5.3 (Phase Three) – *Enterprise Identity Lifecycle Management (ILM) Part 2* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 15: Implementation Tasks for Activity 1.5.2 — Enterprise Identity Lifecycle Management (ILM) Part 1

Leverage Identity Lifecycle Management (ILM) process, from Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM)*.
Define requirements and policies: ☐ Leverage previously established requirements and policies to further develop policies supporting automation. **Expand ILM process scope and goals:** ☐ Incorporate new automation requirements into the existing ILM. Include processes that support Just-in-Time (JIT) to automatically revoke access to Data, Applications, Assets, and Services (DAAS) as needed [6, 15].
Integrate with the Enterprise ICAM solution.
Conduct a current state analysis of the existing ILM: ☐ Develop an assessment plan to evaluate compliance requirements for existing data sources, Identity Management (IdM) systems, access control policies, and credential management in accordance with the Enterprise ICAM established policy. ☐ Review data flow security requirements between different elements and the Enterprise ICAM system, including identity repositories, User/Person Entity (PE) interfaces, and third-party access portals. **Facilitate system deployment and data migration to the Enterprise ICAM platform:** ☐ Integrate, configure, and update the approved ILM solution to functionally integrate with the Enterprise ICAM platform. ☐ Review, verify, and validate the functional, performance, and system integration acceptance requirements to ensure the deployment of all functionalities against defined requirements and expected outcomes. **Enforce access control and a secure integration design architecture:** ☐ Leverage data encryption and existing protection mechanisms to safeguard the integrity of DAAS during data exchange across all platforms. ☐ Adopt Application Programming Interface (API) integration and adhere to all relevant and applicable security standards (e.g., National Institute of Standards and Technology (NIST), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), etc.) and protocols while connecting to existing credential repositories, identity storages, applications, and databases.

Automate identity lifecycle processes.

Select ICAM solutions:

☐ Select ICAM solutions that support automation and integration.

☐ Ensure the ICAM solutions integrate seamlessly with existing systems and applications within the Component.

☐ Ensure integration with MFA, from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*.

Provisioning:

☐ Automate the creation of identities, attributes, groups, credentials, and permissions.

Management:

☐ Implement automated processes for managing changes to these elements (e.g., role change, attribute updates, group memberships, etc.).

De-provisioning:

☐ Automate the removal of identities, attributes, groups, credentials, and permissions when no longer needed.

Identify and approve exceptions to JIT/Just Enough Administration (JEA) automation.

Manage Exceptions:

☐ Users/PEs outside the standard ILM process are:

- Identified
- Documented
- Approved or rejected

☐ Risks are determined by the Enterprise and/or Component.

☐ Approval is granted when justification for the exception outweighs the risks to the Enterprise/Component.

☐ Approvals are periodically reassessed.

Verify and validate implementation activity for expected outcomes.

Enable continuous system performance testing capability to support activity verification and validation:

☐ Conduct routine and regular performance testing to ensure seamless integration, security, and functionality compliance.

☐ Enable reporting and monitoring built-in capabilities to audit repositories, data access, and centralized identity database activities.

Summary

This diagram outlines the Activity 1.5.2 (Phase Two) – *Enterprise Identity Lifecycle Management (ILM) Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of Enterprise Identity Lifecycle Management (ILM) processes, policies, and standards across the Component environment. It presents strategic insights that drive implementation and expected outcomes, including an automated identity lifecycle process and the integration of Enterprise Identity, Credential, and Access Management (ICAM) processes and solutions.

Table 16: Activity 1.5.2 — Enterprise Identity Lifecycle Management (ILM) Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are the ILM processes, policies, and standards aligned across DoW Components? 2. How is the Enterprise ILM process implemented using centralized or federated Identity Provider (IdP) and ICAM solutions?

STRATEGIC INSIGHTS
• The Component defines policies and automation strategies for ILM, integrating Just-in-Time (JIT) and Just Enough Administration (JEA) principles to enforce dynamic access revocation for Data, Applications, Assets, and Services (DAAS). • The Component demonstrates security and compliance by expanding ILM scope, integrating with Enterprise ICAM solutions, and enforcing secure data exchange through encryption and Application Programming Interface (API)-based identity integration. • The Component provides verifiable enforcement through automated identity provisioning, management, and de-provisioning, ensuring strict access controls while continuously verifying and validating system performance and compliance. • The Component leverages ICAM solutions to streamline authentication, integrate with Multi-Factor Authentication (MFA), and automate role-based access changes while adhering to industry security standards such as National Institute of Standards and Technology (NIST), General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA). • The Component ensures continuous security by maintaining exception management protocols, enforcing periodic risk assessments, and enabling automated monitoring and auditing to verify and validate ILM functionality and policy adherence.

EXPECTED OUTCOMES
1. Automated identity lifecycle processes. 2. Integrated with Enterprise ICAM process and tools.

Capability 1.6 Behavioral, Contextual ID, and Biometrics

Table 17: Capability 1.6 — Behavioral, Contextual ID, and Biometrics

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
1 - User	1.6 - Behavioral, Contextual ID, and Biometrics
Description	
Utilizing the Enterprise IdP, User and Entity Behavior Analytics (UEBA) are enabled with basic user attributes. Once completed this is expanded into Component specific attributes using Component IdPs as available. Finally, UEBA are integrated with the PAM and JIT/JEA systems to better detect anomalous and malicious activities.	
Impact to ZT	
Behavioral, contextual, and biometric telemetry enhances MFA.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component integrates its Enterprise Identity Provider (IdP) with a User and Entity Behavior Analytics (UEBA) solution, utilizing basic user attributes such as login frequency, location, and device type to establish baseline behaviors.
- User Activity Monitoring (UAM) solution is deployed to track activity patterns across applications and systems, providing real-time insights into normal and anomalous User/Person Entity (PE) behaviors.
- The Component expands the UEBA solution to include contextual attributes, such as time of access, geolocation, and network type, improving its ability to detect unusual activity.
- Biometric telemetry, including facial recognition and fingerprint scans, is added to the authentication process to strengthen Multi-Factor Authentication (MFA) for high-risk roles.
- A privileged User/PE attempts to access sensitive data from an unrecognized device outside normal working hours, triggering an alert in the UEBA solution.
- The UEBA solution flags the access attempt as anomalous and temporarily denies access, requiring additional biometric authentication for verification.
- The User/PE fails biometric verification and validation, prompting the Security Operations Center (SOC) to investigate further, discovering that the access attempt originated from a compromised account.

- The Component integrates the UEBA solution with its Privileged Access Management (PAM) and Just-in-Time (JIT) access controls, ensuring privilege escalation requests are dynamically evaluated for risk.
- Regular tuning of the UEBA solution and feedback loops from security analysts allow the Component to continuously refine detection thresholds and reduce false positives.
- By leveraging behavioral, contextual, and biometric telemetry, the Component enhances its risk-based authentication and access controls, successfully mitigating insider threats and external attacks while adhering to Zero Trust (ZT) principles.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Authentication Security: Behavioral and contextual identification, combined with biometrics, adds an extra layer of security by analyzing unique User/PE patterns, making unapproved access significantly harder.
- Reduced Reliance on Passwords: By leveraging biometric authentication and contextual data, the Component can minimize password-related risks, such as phishing and credential theft.
- Adaptive Access Control: Real-time behavioral analysis allows the Component to adjust authentication requirements based on risk factors, ensuring a balance between security and User/PE convenience.
- Improved User/PE Experience: Biometric authentication and contextual identity reduce friction by allowing seamless logins without the need for repetitive password entry.
- Stronger Fraud Prevention: By continuously monitoring User/PE behavior and contextual signals, the Component can detect and respond to anomalies, preventing account takeovers and fraudulent activity.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Audit and Logging
- Endpoint Detection and Response (EDR)
- Endpoint Security solutions
- User and Entity Behavior Analytics (UEBA)
- User Activity Monitoring (UAM)

Activity 1.6.1 Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling

Table 18: Activity 1.6.1 — Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components procure and implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions. Initial integration point with Enterprise IdP is completed, enabling future usage in decision-making.	
Predecessor(s)	**Successor(s)**
None	1.3.3, 2.3.1, 7.2.5, 7.3.2, 7.4.1
Expected Outcomes	
• UEBA and UAM functionality is correlated with the Master User Record and integrated with Enterprise IdP.	
End State	
Establish a comprehensive and continuously adaptive security solution that leverages behavior analytics, detects anomalies, and protects against unauthorized access.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Identity Provider (IdP) has been implemented per Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*.
- The Component has an existing Security Information and Event Management (SIEM) solution.
- The User and Entity Behavior Analytics (UEBA)/User Activity Monitoring (UAM) solution(s) should be integrated with the existing systems/services, such as:
  - SIEM
  - Endpoint Detection and Response (EDR)
  - Identity and Access Management (IAM)
- Activity 1.3.3 (Phase Four) – *Alternative Flexible Multi-Factor Authentication (MFA) Part 2,* Activity 2.3.1 (Phase Three) – *Entity Activity Monitoring Part 1,* Activity 7.2.5 (Phase Two) – *User and Device Baselines*, Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior*, and Activity 7.4.1 (Phase Two) –

Baseline and Profiling Part 1 are defined by the Department of War (DoW) Zero Trust (ZT) Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 19: Implementation Tasks for Activity 1.6.1 — Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling

Implement UEBA and UAM solutions by integrating them with the Enterprise IdP.
Define baseline User/Person Entity (PE)/Non-Person Entity (NPE) behavior: ☐ Leverage Activity 7.2.5 (Phase Two) – *User and Device Baselines*. ☐ Leverage Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior*. ☐ Define behavior deviation thresholds. ☐ Configure behavioral analytic rules to detect anomalies and potential security threats, such as: • Unusual login locations • Impossible travel activity • Excessive access requests **Requirements, objectives, and risks:** ☐ Determine the specific requirements for UEBA and UAM solutions. ☐ Define the objectives for implementing UEBA and UAM, such as detecting insider threats, monitoring User/PE activities and accounts, and ensuring compliance [11]. **Select UEBA and UAM solutions:** ☐ Select UEBA and UAM solutions that support integration with the Enterprise IdP, from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*, and existing systems (e.g., SIEM, IAM, Data Loss Prevention (DLP) systems, etc.). **Evaluate UEBA/UAM solutions:** ☐ Assess various UEBA solutions based on features, integration capabilities, and compatibility with the existing infrastructure. ☐ Assess UAM solutions based on the ability to provide comprehensive monitoring and reporting capabilities, and integration with UEBA solutions. ☐ Verify and validate that the UEBA/UAM solutions integrate with existing systems.

Deploy and configure UEBA solutions:

☐ Deploy the selected UEBA solution into the Component environment(s).

☐ Configure the UEBA solution to collect data from necessary elements such as endpoints, network devices, servers, applications, and cloud services.

☐ Implement anomaly detection algorithms to identify deviations from baseline behavior.

☐ Integrate the UEBA solution with existing systems.

Deploy and configure the UAM solution:

☐ Deploy the selected UAM solution into the Component environment(s).

☐ Configure the UAM solution to monitor User/PE activities, including keystrokes, screen captures, and application usage.

☐ Determine which User/PE and resource attributes are required for the Enterprise by conducting a comprehensive inventory and characterizing Users/PEs, resources, and the User's/PE's ability to protect the data [6].

☐ Create detailed monitoring policies based on User/PE roles, attributes, and application requirements.

☐ Define and implement access control policies based on roles and attributes.

☐ Define policies for acceptable and unacceptable behavior based on the Enterprise guidelines.

☐ Ensure the UAM solution integrates seamlessly with the UEBA solution to provide comprehensive monitoring and analytics.

Verify and validate UEBA/UAM solutions.

Verify and validate:

☐ Ensure that the UEBA and UAM solutions integrate as expected with existing services/systems by verifying and validating the UEBA and UAM solutions:

- Receive the necessary information in the supported formats from other devices.
- Provide the necessary information to other systems/services in a supported format.

☐ Demonstrate the UEBA and UAM solutions function as expected by performing simulations of anomalous behavior with the intent of triggering UEBA and UAM-defined actions.

Analyze the attributes over time to indicate unusual deviations or values.

Continuous monitoring and analytics:

☐ Utilize the UEBA and UAM solutions to monitor User/PE and entity activities continuously.

☐ Collect logs and telemetry data from endpoints, network devices, and applications.

☐ Implement real-time analytics to detect anomalies and potential security threats.

☐ Configure automated response actions to isolate or remediate threats in real-time.

Monitor and audit:

☐ Monitor the UEBA and UAM solutions continuously to ensure they function as expected.

☐ Periodically verify and validate the solutions to ensure that the UEBA and UAM solutions continue to behave as expected and continue to comply with security policies as the environments change over time.

☐ The frequency with which the UEBA and UAM solutions should be reevaluated will depend on the nature of the Component's mission and operational requirements. It is strongly recommended that the reassessment be done at an interval no longer than annually [4].

Summary

This diagram outlines the Activity 1.6.1 (Phase Two) – *Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) tools across the Enterprise Identity Provider (IdP). It presents strategic insights that drive implementation and expected outcomes, including UEBA and UAM functionality integrated across the Enterprise IdP.

Table 20: Activity 1.6.1 — Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is UEBA and UAM tooling implemented for the Enterprise IdP? 2. What attributes are utilized in the initial implementation of UEBA?

STRATEGIC INSIGHTS
• The Component defines objectives and security requirements for UEBA and UAM solutions, integrating them with the Enterprise IdP to detect insider threats, monitor activities, and ensure compliance. • The Component demonstrates security and operational effectiveness by selecting and deploying UEBA and UAM solutions, figuring behavioral analytics to detect anomalies, and implementing access control policies based on User/Person Entity (PE) roles, attributes, and activity patterns. • The Component provides verifiable enforcement through integration verification and validation, security simulations, and anomaly detection, ensuring continuous monitoring, logging, and automated response actions to mitigate potential threats in real-time. • The Component leverages existing security infrastructure, including Security Information and Event Management (SIEM), Identity and Access Management (IAM), and Data Loss Prevention (DLP) solutions, to enhance data collection, analysis, and threat detection. • The Component ensures ongoing security by continuously monitoring UEBA and UAM effectiveness, conducting periodic audits, and reassessing solutions at least annually to adapt to evolving security threats and operational requirements.

EXPECTED OUTCOMES
1. UEBA and UAM functionality is correlated with the Master User Record and integrated with Enterprise IdP.

Capability 1.8 Continuous Authentication

Table 21: Capability 1.8 — Continuous Authentication

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
1 – User	1.8 - Continuous Authentication
Description	
DoW Components and overall Enterprise will methodically move towards continuous attribute-based authentication. Initially the capability focuses on standardizing legacy single authentication to a organizationally approved IdP with users and groups. The second stage adds in based rule-based (time) authentication and ultimately matures to Continuous Authentication based on the application/software activities and privileges requested.	
Impact to ZT	
Users not continuously presenting multiple forms of authentication will be denied access to DAAS system and resources.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component begins by standardizing legacy single authentication processes, transitioning all systems to use the Enterprise/Component-approved Identity Provider (IdP) for managing Users/Person Entities (PEs) and groups.
- The IdP is configured to enforce periodic re-authentication at fixed intervals based on time and session duration, ensuring Users/PEs remain verified and validated during extended access periods.
- Over time, the Component integrates rule-based authentication policies that consider factors such as time of access, location, and device security posture to dynamically adjust re-authentication requirements.
- A privileged User/PE accesses the Data, Applications, Assets, and Services (DAAS) solution for maintenance tasks, triggering continuous authentication policies that monitor the session for real-time anomalies.
- Mid-session, the system detects an unusual change in User/PE behavior, such as accessing resources not typically associated with the User's/PE’s role or activity patterns.
- The continuous authentication system prompts the User/PE to re-authenticate using multiple factors, including a biometric scan, to confirm their identity.
- The User/PE fails the biometric re-authentication, and the session is immediately terminated, preventing potential misuse of the compromised session.

- Security analysts review the incident and determine that an attacker attempted to hijack the active session using stolen credentials.
- The Component further refines its continuous authentication policies by incorporating real-time application and software activity data to evaluate privileges requested during sessions.
- By enforcing continuous authentication approval, the Component ensures that Users/PEs are consistently verified and validated, minimizing the risk of unapproved access and maintaining alignment with Zero Trust (ZT) principles.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Real-Time Threat Detection: Continuous authentication monitors User/PE behavior and context throughout a session, allowing the Component to detect and respond to anomalies in real-time.
- Reduced Risk of Session Hijacking: By continuously verifying and validating User/PE identity, the Component can prevent unapproved access even if credentials are compromised during an active session.
- Enhanced User Experience: Seamless, ongoing authentication reduces the need for frequent reauthentication, allowing Users/PEs to work securely without unnecessary disruptions.
- Adaptive Security Controls: Risk-based authentication dynamically adjusts security measures based on User/PE behavior, device trust, and location, ensuring the right level of protection at all times.
- Improved Compliance and Accountability: Continuous monitoring provides detailed activity logs, helping the Component meet regulatory requirements and strengthen auditability.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Audit and Logging
- Endpoint Detection and Response (EDR)
- Multi-Factor Authentication (MFA)
- User and Entity Behavior Analytics (UEBA)
- Just-in-Time (JIT) Access

Activity 1.8.2 Periodic Authentication

Table 22: Activity 1.8.2 — Periodic Authentication

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components enable periodic authentication for applications and services. Traditionally, these are based on duration and/or duration timeout, however, other period-based analytics can be used to enforce reauthentication of user sessions.	
Predecessor(s)	**Successor(s)**
1.8.1	1.8.3, 7.6.1
Expected Outcomes	
• Authentication implemented multiple times per session based on security attributes and criticality of the data, user, application, system, and source user location.	
End State	
Authentication occurs per the requirement and standard.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 1.8.1 (Phase One) – *Single Authentication* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Identity Provider (IdP) has been implemented per Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*.
- The Component has existing Security Information and Event Management (SIEM) and Multi-Factor Authentication (MFA) solutions.
- Periodic Authentication is traditionally based on duration and/or time-out.
- Activity 1.8.3 (Phase Three) – *Continuous Authentication Part 1* and Activity 7.6.1 (Phase Three) – *AI-Enabled Network Access* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 23: Implementation Tasks for Activity 1.8.2 — Periodic Authentication

Identify periodic authentication requirements.

Security attributes and criticality levels:

☐ Identify relevant attributes, such as:

- User/Person Entity (PE) role
- Data sensitivity
- Application/system criticality
- Source location
- Device/network context

☐ Collaborate with the Enterprise to obtain current directives and updated policies on vulnerability management.

☐ Define and categorize criticality levels (e.g., low, medium, high) for data, Users/PEs, systems, and access scenarios.

Establish/update authentication policies:

☐ Develop authentication policies based on criticality and context, specifying frequency and conditions for periodic reauthentication.

☐ Integrate MFA using the approved Identity Provider (IdP), from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*.

☐ Establish dynamic authentication policies that adjust based on the context of the access request.

☐ Establish policies that leverage time-based reauthentication intervals, to include periodicity attributes, in accordance with the criticality of access. For example:

- The period of time allowed between User/PE reauthentication is shorter for critical resources.

Establish access control policies:

☐ Define access control policies based on roles and attributes. Access control mechanisms should consider granularity, reliability, availability, and the potential risks to the resource [6].

☐ Ensure alignment with reauthentication policies and support for adaptive enforcement.

Identify/select solutions:

☐ Select Identity and Access Management (IAM) / Identity, Credential, and Access Management (ICAM) solutions that:

- Are compliant with the Enterprise standards and integrate with existing systems.
- Support context-aware and adaptive authentication.
- Support continuous authentication.
- Verify and validate User/PE identities throughout the sessions based on behavior, device posture, and other contextual factors.

Implement periodic authentication requirements for applications and services, including multiple authentication periods based on security attributes and the criticality of data, Users/PEs, applications, systems, and source User/PE locations.

Implement periodic authentication:

☐ Define reauthentication intervals based on criticality and session risk.

☐ Configure authentication to recur based on time, User/PE behavior, location changes, or sensitivity of accessed data.

☐ Apply dynamic reauthentication logic where appropriate.

Configure IAM/ICAM and MFA:

☐ Ensure all Users/PEs are enrolled in MFA and subject to periodic reauthentication.

☐ Configure IAM/ICAM to enforce authentication policies and manage User/PE sessions.

☐ Configure the MFA solution to prompt Users/PEs for reauthentication at defined intervals or when certain conditions are met (e.g., accessing sensitive data, changing network locations, etc.).

Implement and integrate with existing systems.

Implement and integrate:

☐ Integrate IAM/ICAM and MFA solutions with all relevant applications and services.

☐ Ensure consistent enforcement of authentication policies across all systems.

☐ Verify and validate system compatibility with dynamic and periodic reauthentication workflows.

Verify and validate periodic authentication and integration.

Verification and validation actions:

☐ Demonstrate that Users/PEs are periodically authenticated in accordance with the defined frequency/conditions.

☐ Ensure MFA authentication is applied across defined resources.

☐ Verify and validate the authentication solution(s) successfully integrate with the IdP.

☐ Review and adjust policy and configurations based on testing, monitoring, and evolving risk conditions.

Summary

This diagram outlines the Activity 1.8.2 (Phase Two) – *Periodic Authentication* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of authentication across applications per session. It presents strategic insights that drive implementation and expected outcomes, including authentication multiple times per session, based on security attributes and the criticality of data.

Table 24: Activity 1.8.2 — Periodic Authentication - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is periodic authentication implemented multiple times per session based on security attributes?

STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for administering User/Person Entity (PE) authentication via the Component Identity Provider (IdP) solution, incorporating Multi-Factor Authentication (MFA) in accordance with the established MFA/IdP framework from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*. • The Component demonstrates compliance by authenticating privileged and non-privileged Users/PEs at least once per session using MFA, ensuring that all sessions comply with defined security practices. • The Component provides evidence that these periodic authentication measures leverage strong, multi-factor methods to reduce unapproved access risks and maintain adherence to documented policies. • The Component verifies and validates that its IdP and MFA controls are regularly monitored, audited, and updated to align with evolving requirements, ensuring continuous identity assurance and robust cybersecurity protection.

EXPECTED OUTCOMES
1. Authentication implemented multiple times per session based on security attributes and criticality of the data, user, application, system, and source user location.

Capability 1.9 Integrated Identity, Credential, and Access Management (ICAM) Platform

Table 25: Capability 1.9 — Integrated Identity, Credential, and Access Management (ICAM) Platform

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
1 - User	1.9 - Integrated Identity, Credential, and Access Management (ICAM) Platform
Description	
DoW Components and overall Enterprise employ enterprise-level identity management and Public Key Infrastructure (PKI) systems to track user, administrator and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Components can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool. PKI systems can be federated but must either trust a central root Certificate Authority (CA) and/or cross-sign standardized organizational CA's.	
Impact to ZT	
Identities of users and NPE are centrally managed to ensure authorized and authenticated access to DAAS resources across platforms.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component implements an Enterprise-level Identity, Credential, and Access Management (ICAM) platform, centralizing the management of User/Person Entity (PE), administrator, and Non-Person Entity (NPE) identities.
- A Public Key Infrastructure (PKI) solution is deployed, with all certificates issued by a central root Certificate Authority (CA), ensuring trust across the network.
- The ICAM platform integrates with identity governance and administration tools to establish role-based access policies, limiting access to resources based on the principle of "need and right to know."
- Credential management systems are implemented to track the issuance, renewal, and revocation of digital certificates for all identities, ensuring only valid credentials are in use.
- During an inter-agency collaboration, the Component federates its PKI solution with a trusted partner, leveraging cross-signed certificates to enable seamless, secure access.

- An unauthorized User/PE attempts to access a sensitive Data, Applications, Assets, and Services (DAAS) resource using a spoofed digital certificate, but the ICAM platform detects the invalid certificate and denies access.
- Regular audits of the ICAM platform identify several inactive User/PE accounts with valid certificates. These accounts are flagged and their certificates revoked to reduce the risk of misuse.
- The Component integrates the ICAM platform with an access management tool, enabling real-time enforcement of Zero Trust (ZT) access policies based on identity attributes and authentication status.
- Continuous monitoring of User/PE/NPE activities allows the Component to detect and respond to anomalies, such as unexpected access patterns, improving overall security.
- By centralizing Identity Management (IdM) through the ICAM platform, the Component ensures only authorized and authenticated User/PEs and NPEs can access DAAS resources and enhancing network security.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Centralized Identity Governance: A structured ICAM solution ensures the Component maintains a unified approach to User/PE Identity Management (IdM), reducing inconsistencies and security gaps.
- Stronger Access Control: By enforcing role-based and attribute-based access policies, ICAM ensures that Users/PEs only have access to the resources necessary for their roles, enhancing security.
- Improved Credential Security: Secure credential management, including encryption and Multi-Factor Authentication (MFA), protects against credential theft and unapproved access.
- Enhanced Compliance and Auditing: ICAM provides detailed access logs and identity tracking, helping the Component meet regulatory requirements and improve security auditing capabilities.
- Streamlined User Lifecycle Management: Automating account provisioning and deprovisioning ensures access is granted and revoked efficiently, reducing administrative overhead and security risks.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Identity, Credential, and Access Management (ICAM)
- Identity Provider (IdP)
- Identity as a Service (IDaaS)
- Multi-Factor Authentication (MFA)
- Public Key Infrastructure (PKI)

Activity 1.9.1 Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1

Table 26: Activity 1.9.1 — Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Enterprise works with Components to implement Enterprise Public Key Infrastructure (PKI) solutions in a centralized and/or federated fashion. The Enterprise PKI solution utilizes a single or set of Enterprise level Root Certificate Authorities (CAs) that can then be trusted by Components to build Intermediate CAs. Component PKI Certificate Authorities are integrated with the Enterprise PKI. An Enterprise Identity Provider (IdP) platform is implemented. The IdP solution may either be a single solution or federated set of Component IdPs with standard level of access across Components and standardized set of attributes. Component IdPs are integrated with the Enterprise IdP.	
Predecessor(s)	**Successor(s)**
None	1.9.2
Expected Outcomes	
• Enterprise PE & NPE CONOPS, taxonomy, and naming standards are developed. • Components Certificate Authorities (CAs) are integrated with the DoW PKI Hierarchy. • Enterprise level requirements are implemented, including mandated user attributes for a validated and verified Enterprise Identity Provider (IdP) Platform. • Enterprise wide IdP platform is implemented through a single solution or integration of multiple solutions.	
End State	
All PEs and NPEs are issued a validated and verified digital identity that can be tracked at the Enterprise level using the strongest authentication available.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Centralized and/or federated Enterprise Public Key Infrastructure (PKI) solutions/requirements have already been established.
- Enterprise User/Person Entity (PE)/Non-Person Entity (NPE) Concept of Operations (CONOPS), taxonomy, and naming standards have already been developed.
- Centralized and/or federated Enterprise Identity Provider (IdP) solutions/requirements have already been established.
- Mandated User/PE attributes are included in implementation requirements to ensure a verified and validated Enterprise IdP solution has been established.

- Hardware Security Module (HSM) implementation requires strong cryptographic integrity, such as Federal Information Processing Standard (FIPS) 140-3 Level 3 compliant modules for secure key protection, selection between network-attached or Payment Card Industry (PCI) card form factors based on environment, and M of N authentication to prevent insider threats during critical Certificate Authority (CA) operations.
- Certificate lifecycle management involves automated notifications at 60/30/15 days to prevent unexpected expirations, self-service renewal portals integrated with Enterprise IdP solutions, and 24/7 emergency revocation procedures to quickly invalidate compromised certificates.
- Integration touchpoints include directory services connections for accurate certificate subject information, automated Human Resources (HR) system workflows for certificate lifecycle management, and Enterprise Online Certificate Status Protocol (OCSP) responders for real-time validation without frequent Certificate Revocation List (CRL) downloads.
- Activity 1.9.2 (Phase Three) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part* 2 is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a successor to this activity.

Implementation

The below implementation table provides practical, actionable recommendations to help organizations achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 27: Implementation Tasks for Activity 1.9.1 — Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1

Requirements gathering and Enterprise alignment.
Establish Component policy and governance: ☐ Review Enterprise User/PE/NPE PKI CONOPS, taxonomy, and naming standards. ☐ Align Component policies with Enterprise standards. ☐ Document certificate use cases, volume projections, and types needed. ☐ Establish operational procedures for certificate lifecycle management.

Technical requirements analysis:

☐ Document integration requirements with Enterprise Root CA and IdP.

☐ Define hardware/software requirements and security standards.

- Example: Cryptographic specifications (Secure Hash Algorithm (SHA)-256 minimum, 2048-bit Rivest-Shamir-Adleman (RSA) keys).

Transition assessment:

☐ Perform gap analysis between Component IdP/Multi-Factor Authentication (MFA) and Enterprise offerings.

☐ Identify if the Component IdP solution can integrate with the Enterprise IdP solution.

☐ Identify technologies that cannot transition to the Enterprise solution(s).

☐ Develop a migration plan with a timeline and resource requirements.

☐ Create remediation strategy for non-compatible systems (decommission, exception).

Component-level PKI architecture.

Architecture and policy development:

☐ Align to Enterprise PKI hierarchy.

☐ Design subordinate CA hierarchy and IdP federation architecture.

☐ Review and adopt Certificate Policies (CP) and Certification Practice Statement (CPS).

☐ Review and align to Enterprise certificate profile.

☐ Establish key management and certificate verification and validation policies.

- Example: Validity periods by certificate type (for example: User/PE: 1 year, NPE: 2 years).

Security framework:

☐ Design physical/logical security controls and access management.

☐ Determine key storage mechanisms (HSM implementation).

☐ Establish audit logging, monitoring, and Incident Response (IR) procedures.

Review and establish Component-level key management strategy:

☐ Review and define key generation.

☐ Review and define key storage, retrieval, and recovery.

☐ Review and define key lifecycle management.

Adopt a phased PKI deployment:

☐ Review Enterprise certificate enrollment guidelines (e.g., renewal, revocation, etc.).

☐ Review and establish PKI-based security controls (e.g., CA servers, HSM, etc.).

☐ Verify and validate PKI Interoperability across systems.

Solution capability testing.

Environment setup and functional testing:

☐ Create a test PKI infrastructure with Enterprise Root CA connectivity.

☐ Configure certificate templates and enrollment processes.

☐ Test certificate issuance, revocation, and IdP integration.

Integration testing:

☐ Verify and validate interoperability with applications and services.

☐ Test certificate deployment to end entities.

☐ Verify and validate IdP federation and attribute validation.

- Example: Federation protocol verification (Security Assertion Markup Language (SAML), Open Authorization (OAuth), OpenID Connect (OIDC)).

☐ Test integration with Automation and Orchestration and Visibility and Analytics pillar solutions.

Phased deployment.

Infrastructure and CA installation:

☐ Deploy and secure subordinate CA hardware/software.

☐ Request and install subordinate CA certificate from Enterprise root CA.

☐ Configure CRL/Online Certificate Status Protocol (OCSP) infrastructure and certificate templates.

☐ Implement IdP federation with standardized attributes.

Pilot deployment:

☐ Issue certificates to limited User/PE group.

☐ Test IdP federation with pilot Users/PEs.

☐ Gather feedback and adjust configurations.

- Example: User/PE experience testing with certificate enrollment workflow.

☐ Integrate with Automation and Orchestration and Visibility and Analytics pillar solutions.

Solution validation.

Performance and security testing:

☐ Verify and validate certificate processes and IdP federation in production.

☐ Monitor system metrics and verify and validate security controls.

☐ Test disaster recovery and business continuity procedures.

- Example: Recovery Time Objective (RTO) verification for CA restoration.

System and application integration:

☐ Verify and validate certificate chain and path discovery.

☐ Test trust relationships across organizational boundaries.

☐ Verify and validate application functionality with issued certificates. ☐ Ensure compliance with Enterprise PKI and IdP requirements.
Periodic review and maintenance.
Establish continuous PKI testing, verification, and validation: ☐ Conduct regular security assessments and penetration testing. ☐ Ensure logging and monitoring of PKI activities are captured and ingested by Automation and Orchestration and Visibility and Analytics pillar solutions. ☐ Verify and validate adherence to Enterprise policies and standards. ☐ Review certificate profiles and template configurations. ☐ Maintain IdP federation and attribute standardization. • Example: Quarterly certificate policy compliance verification and validation checklist.

Summary

This diagram outlines the Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of Public Key Infrastructure (PKI)/Identity Provider (IdP) solutions across a Component. It presents strategic insights that drive implementation and expected outcomes, including Enterprise-level requirements that mandate User/Person Entity (PE) attributes for a verified and validated Enterprise IdP.

Table 28: Activity 1.9.1 — Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the Enterprise PKI/ IdP solution implemented across organizations? 2. How are components utilizing IdP with Multi-Factor Authentication (MFA) for all applications and services? 3. How are organizational PKI Certificate Authorities (CAs) integrated with the Enterprise PKI solution?

STRATEGIC INSIGHTS
• The Component defines comprehensive PKI governance by aligning Component policies with Enterprise standards, documenting certificate use cases, establishing operational procedures for certificate lifecycle management, and reviewing Enterprise User/Person Entity (PE)/Non-Person Entity (NPE) PKI Concept of Operations (CONOPS), taxonomy, and naming standards. • The Component demonstrates technical readiness through rigorous gap analysis between Component Identity Provider (IdP) / Multi-Factor Authentication (MFA) and Enterprise offerings, identifying technologies that cannot transition to Enterprise solutions, and developing migration plans with specific timelines and resource requirements. • The Component provides robust security frameworks by designing physical/logical security controls, determining key storage mechanisms, establishing audit logging, monitoring and Incident Response (IR) procedures, and validating interoperability across systems. • The Component leverages phased implementation approaches including test environments, pilot deployments with limited user groups, and iterative feedback cycles to ensure smooth integration with Enterprise Root Certificate Authority (CA) and IdP systems while validating certificate processes and IdP federation in production. • The Component ensures ongoing compliance and optimization through continuous PKI testing, regular security assessments, verification of adherence to Enterprise policies, and maintenance of IdP federation with standardized attributes, while integrating with Automation and Orchestration and Visibility and Analytics pillar solutions.

✓ EXPECTED OUTCOMES

1. Enterprise PE & NPE CONOPS, taxonomy, and naming standards are developed.
2. Components Certificate Authorities (CAs) are integrated with the DoW PKI Hierarchy.
3. Enterprise level requirements are implemented, including mandated user attributes for a validated and verified Enterprise Identity Provider (IdP) Platform.
4. Enterprise wide IdP platform is implemented through a single solution or integration of multiple solutions.

Device Pillar

Capability 2.1 Device Inventory

Table 29: Capability 2.1 — Device Inventory

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
2 - Device	2.1 - Device Inventory
Description	
DoW Components establish and maintain an approved inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI (802.1x) machine certificate, device object, patch/vulnerability status and others to enable successor activities.	
Impact to ZT	
By default policy, devices will be denied network access; the only devices permitted access to the network shall be known, authorized, and listed in the device inventory.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component conducts a device health tool gap analysis to identify missing capabilities required for tracking and managing devices on the network.
- A centralized device inventory system is implemented, enrolling all devices with their attributes such as Public Key Infrastructure (PKI) machine certificates, device objects, and patch/vulnerability status.
- The Component establishes a policy that denies network access to any device not listed in the inventory, ensuring only known and authorized devices can connect.
- During the initial enrollment Phase, several legacy devices with outdated firmware are flagged as non-compliant and either updated or removed from the network.
- A contractor attempts to connect a personal device to the network without prior enrollment, triggering an automatic block and generating an alert for the Security Operations Center (SOC).
- The Component's security team uses the inventory system to verify and validate that all connected devices are patched and meet baseline security standards before allowing continued network access.

- During a routine vulnerability scan, a device on the network is identified as non-compliant due to an expired PKI certificate. The inventory system flags the device and quarantines it until the certificate is renewed.
- Non-Person Entities (NPEs) such as Internet of Things (IoT) devices are also enrolled in the inventory with detailed attributes, enabling the Component to manage and monitor these devices alongside User/Person Entity (PE)-operated systems.
- The Component integrates its device inventory with the Enterprise Identity Provider (IdP) to ensure device trust is continuously verified in conjunction with User/PE authentication.
- By maintaining a trusted device inventory, the Component ensures only authorized, compliant devices can access the network, thereby reducing the attack surface and reinforcing Zero Trust (ZT) principles.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security: Establishing a trusted inventory reduces the risk of unapproved device access, reinforcing security protocols.
- Improved Compliance: Regular checks and updates ensure that all devices meet security standards, aiding in compliance with regulations.
- Streamlined Device Management: Centralized inventory allows for efficient tracking and management of devices, reducing administrative overhead.
- Reduced Attack Surface: The Component minimizes potential entry points for cyber threats by denying access to unapproved devices.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Asset/Device/Endpoint Management solutions
- Configuration Management Database (CMDB)
- IT Asset Management (ITAM) Software
- Internet of Things (IoT) Discovery
- Inventory and Asset Management solutions

Activity 2.1.3 Enterprise Identity Provider (IdP) Part 1

Table 30: Activity 2.1.3 — Enterprise Identity Provider (IdP) Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Enterprise Identity Provider (IdP), either using a centralized technology or federated organizational technologies, integrates Non-Person Entities (NPEs), such as devices and service accounts. Integration is tracked in the Enterprise Device Management solution when applicable as to whether it is integrated or not. NPEs not able to be integrated with the IdP are either marked for retirement or excepted using a risk-based methodical approach.	
Predecessor(s)	**Successor(s)**
None	2.1.4
Expected Outcomes	
• Component NPEs are integrated with Enterprise IdP. • Where applicable, ensure tracking in the UEM solution.	
End State	
All NPEs are assigned static attributes in an identity provider, provided an exception based on risk analysis, or marked for retirement, as part of the Enterprise Life Cycle Management plan.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Presumption: The Component has completed Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM)* prior to this activity. Non-Person Entities (NPEs) will be integrated with the Component Identify Lifecycle Management (ILM).
- Consider completing Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1* prior to this activity, as it is necessary to establish an Enterprise Identity Provider (IdP) prior to the enrollment of NPEs.
    - If an Enterprise IdP is not available, then the Component should have established its own IdP, per Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*.
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, to leverage device inventory.
- Consider completing Activity 2.6.1 (Phase One) – *Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools* prior to this activity, to

leverage the Unified Endpoint and Device Management (UEDM) solution to track NPEs.

- Consider completing Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) Part 1* prior to this activity, to leverage the Enterprise Device Management (EDM) solution to track NPEs.
- Use a risk-based methodology to determine NPE decommission or exceptions.
- Activity 2.1.4 (Phase Three) – *Enterprise Identity Provider (IdP) Part 2* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 31: Implementation Tasks for Activity 2.1.3 — Enterprise Identity Provider (IdP) Part 1

Define NPE ILM requirements.
Lifecycle management of NPEs: ☐ Leverage the Component ILM plan, from Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM)*. ☐ Define how NPEs will be managed by the existing Component ILM plan. ☐ Identify NPE information that will be tracked in accordance with the ILM. Information should include at a minimum: • NPE attributes • Integration status with the IdP • Support for automated reporting and alerting
Manage NPEs outside the standard ILM process through risk-based exceptions.
Manage exceptions: ☐ NPEs outside the standard ILM process are: • Identified • Documented • Approved/Rejected

☐ The Enterprise and/or Component determines risk.

- This methodology should consider factors such as the NPE's function, criticality, security posture, and the potential impact of not integrating it with the IdP.
- Document the rationale for any exceptions granted.

☐ Approval is granted when the exception justification outweighs the risk(s) to the Enterprise/Component.

☐ Approval is periodically reassessed.

Integrate NPEs, such as devices and service accounts, with the Enterprise IdP.

Integrate NPE device inventory from established inventory lists in prior activities:

☐ Leverage approved Hardware/Software List for environment authentication, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis.*

- Ensure consistent device identification and attributes across systems and avoid onboarding unapproved devices.

☐ Ensure the minimum attestation (verification and validity period) is defined and documented.

☐ Verify and validate that proper processes are in place and enforced.

Document applications and services that the NPEs will access:

☐ Document all applications, operating systems, and cloud services the NPEs will access, as applicable, to inform appropriate access control policies.

Configure and integrate the EDM solution:

☐ Collaborate with the Enterprise to obtain and review the established requirements for NPE integration with the Enterprise IdP.

☐ Designated System Administrators (SAs) install and configure the EDM, ensuring it supports NPEs, meets Component needs, and maintains a healthy cybersecurity posture.

Integrate Enterprise IdP with Component applications:

☐ Integrate the IdP with each identified application using appropriate integration methods (e.g., Security Assertion Markup Language (SAML), Open Authorization (OAuth), etc.).

☐ Document all configuration choices and deviations from standard configurations as necessary.

☐ A review should be conducted by appropriate personnel, as needed, for the integration to ensure compliance with Enterprise regulatory policies and guidance.

☐ Establish connections between the Enterprise IdP and all Component applications, ensuring seamless authentication and approval processes.

Ensure alignment with Enterprise security and privacy regulations:

☐ Verify and validate that the integration complies with relevant Enterprise security and privacy regulations (e.g., General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), etc.).

Assign all NPEs’ static attributes in the IdP and provide an exception based on risk analysis, or mark the NPEs for retirement as part of the Enterprise Lifecycle Management plan.

Define and manage NPE roles and access controls:

☐ Leverage Enterprise defined and established guidance, from Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) Part 1*, for assigning NPE attributes in the IdP.

☐ Establish clear authentication protocols, ports, services, approval rules, and NPE management policies [16].

☐ Identify each of the following for all NPEs:

- Role(s)
- Access(es)
- Privilege(s)

☐ System Administrators define, assign, and manage roles/access controls for NPEs, specifying what each NPE can/cannot access, adhering to the principle of Least Privilege.

Utilize EDM solution(s) to track NPEs.

Leverage the EDM solution:

☐ Leverage the Component Unified Endpoint and Device Management (UEDM) solution, from Activity 2.6.1 (Phase One) – *Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools.*

☐ Leverage the Component EDM solution, from Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) Part 1.*

☐ Verify and validate the EDM solution to automate, where possible, device management related to critical data and services.

☐ Document any EDM ILM integration deficiencies in accordance with Component policies and implement an alternate solution as required.

Summary

This diagram outlines the Activity 2.1.3 (Phase Two) – *Enterprise Identity Provider (IdP) Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of Non-Person Entity (NPE) integration into the Enterprise Identity Provider (IdP). It presents strategic insights that drive implementation and expected outcomes, including the integration of NPE into the Enterprise IdP and tracking within the Unified Endpoint and Device Management (UEDM) solution.

Table 32: Activity 2.1.3 — Enterprise Identity Provider (IdP) Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are NPEs including devices integrated with the Enterprise IdP? 2. How are devices tracked in the Enterprise Device Management (EDM) solution?

STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for integrating NPEs, such as devices and service accounts, with the Enterprise IdP, ensuring alignment with the Enterprise guidelines, security standards, and ZT principles. • The Component demonstrates compliance by identifying NPEs, establishing secure authentication methods (e.g., certificates, tokens, etc.), and configuring trust relationships with the Enterprise IdP, assigning static attributes, roles, and appropriate access controls based on defined policies and a risk-based approach. • The Component provides evidence that NPE integration with the IdP is tested, monitored, and continuously assessed for security and functionality, including the use of Security Information and Event Management (SIEM) and automated response actions to detect and remediate anomalies in real-time. • The Component leverages UEDM solutions to track and manage NPEs, maintaining a complete lifecycle management plan that includes regularly reviewing device attributes, enforcing Least Privilege, and decommissioning or granting exceptions for NPEs as necessary. • The Component ensures ongoing compliance through continuous auditing, policy reviews, and personnel training, updating integration processes and IdP configurations, as needed, to address emerging threats, maintain interoperability, and uphold the Enterprise security mandates.

EXPECTED OUTCOMES
1. Component NPEs are integrated with Enterprise IdP. 2. Where applicable, ensure tracking in the UEM solution.

Capability 2.2 Device Detection and Compliance

Table 33: Capability 2.2 — Device Detection and Compliance

<table>
<tr><th colspan="2">DoW Zero Trust Framework</th></tr>
<tr><td colspan="2"><em><strong>Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.</strong></em></td></tr>
<tr><td><strong>Pillar</strong></td><td><strong>Capability</strong></td></tr>
<tr><td>2 - Device</td><td>2.2 - Device Detection and Compliance</td></tr>
<tr><td colspan="2"><strong>Description</strong></td></tr>
<tr><td colspan="2">DoW Components employ asset management systems for user devices to maintain and report on IT and Cybersecurity compliance. Managed devices (enterprise and mobile) attempting to connect to a network or access a DAAS resource is detected and has its compliance status confirmed (via C2C)</td></tr>
<tr><td colspan="2"><strong>Impact to ZT</strong></td></tr>
<tr><td colspan="2">Any device attempting to connect to the network will be detected; only those devices that are compliant (e.g., anti-virus is up to date, approved configuration) will receive access to requested DAAS.</td></tr>
</table>

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component deploys an asset management solution that continuously monitors all devices attempting to connect to the network, including Enterprise, mobile, Internet of Things (IoT), and unmanaged devices.
- A compliance-based network authorization process is implemented to ensure only secure devices can access Data, Applications, Assets, and Services (DAAS) or connect to the network. This process is enforced by Comply-to-Connect (C2C), which supports Zero Trust (ZT) by requiring all devices to continuously meet security baselines before being granted access to any resources.
- Devices are evaluated against a compliance baseline that includes requirements such as up-to-date antivirus software, approved configurations, and recent patch status.
- A managed laptop connects to the network but fails the compliance check due to an outdated antivirus definition. The system denies access and notifies the User/Person Entity (PE) to update their device.
- During a regular compliance audit, the Component identifies several unmanaged personal devices attempting to access the network, which are automatically detected and blocked.
- A mobile device with a jailbroken configuration is flagged by the system as non-compliant, triggering an alert for the Security Operations Center (SOC) and isolating the device from sensitive resources.

- IoT devices, such as printers and cameras, are enrolled in the asset management system, and their compliance status is regularly monitored to prevent vulnerabilities from being exploited.
- The compliance-based network authorization process is extended to include detection of rogue devices, allowing the Component to identify and investigate unauthorized devices attempting to breach the network.
- To enhance security, the Component integrates its asset management system with the Enterprise Identity Provider (IdP), ensuring that only devices linked to authenticated User/PEs are evaluated for compliance.
- By employing device detection and compliance systems, the Component ensures that only secure and authorized devices gain access, preventing potential breaches.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security: The Component reduces the risk of breaches and vulnerabilities by ensuring that only compliant devices can access the network.
- Improved Compliance Management: The continuous monitoring of devices helps maintain compliance with internal policies and external regulations.
- Streamlined Device Management: Automated detection and compliance checks simplify managing a diverse range of devices, including IoT and personal devices.
- Increased Operational Efficiency: By automating compliance checks, Information Technology (IT) teams can focus on more strategic tasks rather than manual monitoring and remediation.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Cloud Access Security Broker (CASB)
- Cloud Security Posture Management (CSPM)
- Comply-to-Connect (C2C)
- Device Health Monitoring
- Network Access Control (NAC)
- Security Content Automation Protocol (SCAP)

Activity 2.2.1 Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1

Table 34: Activity 2.2.1 — Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Enterprise refines policy, standards, and requirements for Comply-to-Connect (C2C). Components implement and enforce compliance-based network authorization to meet ZT Target-level functionalities.	
Predecessor(s)	**Successor(s)**
2.1.2, 2.3.4, 2.4.2, 2.5.1	2.2.2
Expected Outcomes	
• C2C is enforced at the Component level for all environments. • All mandated devices checks are implemented using C2C at the Component level.	
End State	
A policy exists or is developed that dictates the need for all devices to be authorized, authenticated, and C2C compliant before connecting to the network.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 2.1.2 (Phase One) – *Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management*, Activity 2.3.4 (Discovery) – *Integrate Next-Generation Antivirus (NextGen AV) Tools with Comply-to-Connect (C2C)*, Activity 2.4.2 (Phase Two) – *Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support*, and Activity 2.5.1 (Phase One) – *Implement Asset, Vulnerability, and Patch Management Tools*, are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, to leverage device inventory.
- Presumption: The Enterprise has refined and established device policies, standards, and requirements before allowing environment access, as enforced by Comply-to-Connect (C2C).

- The primary scope and objectives of implementing C2C, such as improvements in security, enforcing compliance, or eliminating unapproved access, have been clearly outlined.
- Environments have been determined to be included in the initial rollout and subsequent Phases (e.g., low-risk, testing, production, etc.). Factors to consider include:
    - Integration with existing infrastructure
    - Automation capabilities
    - Scalability
    - Performance
    - Vendor support
    - Cost
- Solutions are chosen to meet the Component’s evolving scalability, performance, and cybersecurity needs.
- Activity 2.2.2 (Phase Three) – *Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 2* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 35: Implementation Tasks for Activity 2.2.1 — Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1

Leverage the prioritized Hardware/Software List for integration with C2C.
Review and prioritize asset inventory: ☐ Leverage approved Hardware/Software List for environment authentication, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis.* ☐ Ensure the list is up-to-date and accurately reflects the current device landscape. ☐ Review and prioritize the Hardware/Software List based on Enterprise cybersecurity policies. **Perform C2C integration readiness testing:** ☐ Conduct a readiness assessment of all environments to identify dependencies and integration points.

☐ Establish a baseline for environment performance, User/Person Entity (PE) activity, and device connections in all environments, as it is essential for measuring the impact of C2C implementation.

☐ Consider scaling requirements for implementing C2C in higher-risk and mission-critical environments.

☐ Engage stakeholders to verify and validate operational impacts and obtain approval for broader C2C implementation, as applicable.

Obtain Enterprise policies, standards, and requirements for C2C compliance and integration.

Obtain and review Enterprise policy guidance:

☐ Engage with the Enterprise to acquire the latest C2C policies, standards, and requirements.

☐ Review and analyze Enterprise C2C guidance to identify mandatory controls and compliance obligations.

Ensure C2C requirements align with existing Enterprise policy guidance:

☐ Map C2C requirements to existing Component-level security policies and frameworks.

☐ Identify policy gaps and areas where updates or new policies are required to align with Enterprise C2C mandates.

Consider stakeholder collaboration:

☐ Collaborate with legal, compliance, and cybersecurity teams to ensure applied Component-level policies align with Enterprise guidance.

☐ Document compliance matrices to track adherence to all Enterprise C2C requirements.

☐ Provide guidance and training sessions for relevant stakeholders on updated Enterprise C2C policies and standards.

Integrate C2C with the Environment infrastructure.

Establish C2C integration success criteria:

☐ Define clear and measurable success criteria for C2C integration.

☐ Develop a phased rollout plan for C2C deployment in all environments, including rollback procedures.

☐ Coordinate with stakeholders to minimize operational disruptions during integration.

☐ Document lessons learned from the integration to inform broader C2C deployment efforts.

Verify and validate C2C integration and connection establishment:

☐ Conduct a comprehensive assessment of the current environment infrastructure to identify integration touchpoints for C2C.

☐ Ensure environment segmentation is in place to support staged C2C enforcement across all environments.

☐ Deploy C2C Policy Enforcement Points (PEP) at critical environment interfaces (e.g., switches, routers, firewalls, control planes, etc.).

☐ Configure C2C systems to interface with existing environment approval solutions (e.g., Identity Credential Access Management (ICAM) solutions, etc.), as applicable. **Verify and validate the environment performance:** ☐ Perform integration testing to verify and validate the environment performance, availability, and cybersecurity post-integration. ☐ Implement logging and monitoring capabilities to track C2C activities and environment approval decisions. ☐ Maintain documentation of integration architecture, including data flow diagrams and operational workflows.
Implement all C2C device checks to maintain compliance.
Confirm C2C device compliance checks: ☐ Identify all device compliance checks specified by the Enterprise C2C policies (e.g., patch levels, configuration baselines, antivirus status, encryption settings, etc.). ☐ Configure C2C solutions to perform automated compliance checks before environment access authorization. **Ensure comprehensive device checks:** ☐ Verify and validate that C2C device checks cover all endpoint types (e.g., Bring Your Own Device (BYOD), Internet of Things (IoT), cloud-based assets, etc.). ☐ Ensure the C2C performs real-time, scheduled, and unscheduled compliance assessments. ☐ Test the accuracy and completeness of compliance checks in many operational scenarios. ☐ Implement access controls based on real-time compliance status (e.g., privileged access, restricted access, quarantine, etc.). ☐ Establish procedures for non-compliant device remediation, including automated patching and configuration correction. ☐ Provide end user guidance and technical support for resolving compliance failures.
Maintain C2C enforcement, monitoring, and reporting.
Verify and validate C2C enforcement: ☐ Enable C2C enforcement policies to maintain compliance with Enterprise standards and policies across all environments. ☐ Periodically conduct penetration tests and/or security assessments to verify and validate the efficacy of C2C enforcement. **Implement C2C compliance monitoring and reporting:** ☐ Review compliance failure reports and refine C2C policies and enforcement logic. ☐ Iterate C2C enforcement policies based on feedback and operational data collected. ☐ Prepare detailed reporting on C2C enforcement outcomes, highlighting lessons learned and best practices.

Summary

This diagram outlines the Activity 2.2.1 (Phase Two) – *Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on incorporating the implementation of a Comply-to-Connect (C2C) solution for low-risk and testing environments. It presents strategic insights that drive implementation and expected outcomes, including the enforcement of C2C at the Component level across all environments and mandated device checks.

Table 36: Activity 2.2.1 — Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the C2C solution implemented for low-risk and testing environments? 2. What basic device checks are implemented using C2C?

STRATEGIC INSIGHTS
• The Component defines and documents policies, standards, and requirements for implementing C2C in low-risk and testing environments, aligning with Enterprise guidance and ensuring that established compliance criteria (e.g., device posture, up-to-date patches, antivirus, etc.) are clearly understood and enforced. • The Component demonstrates compliance by integrating C2C with its network infrastructure through a planned approach, which involves inventorying assets, segmenting networks, configuring micro-segmentation, and implementing security controls, including Multi-Factor Authentication (MFA), Least Privilege, and continuous monitoring, among others. This approach establishes clear timelines, tests scenarios, and defines user acceptance criteria. • The Component provides evidence that mandated device checks are automated and continuously enforced by C2C solutions (e.g., Network Access Control (NAC), Security Information and Event Management (SIEM), Identity and Access Management (IAM), etc.), performing ongoing compliance-based approval, detecting anomalies through behavioral analytics, and ensuring comprehensive logging and auditing capabilities to identify and remediate non-compliant devices. • The Component ensures that the C2C implementation includes periodic reviews and improvements to policies and procedures, guided by feedback, lessons learned, and emerging threats, thus continuously refining the compliance posture and maintaining relevance to evolving security and regulatory standards. • The Component maintains continuous monitoring and reporting of C2C enforcement at the device level, integrating health checks, Incident Response (IR) plans, and centralized logging to ensure ongoing visibility, accountability, and adherence to established compliance requirements throughout the Enterprise.

✓ EXPECTED OUTCOMES

1. C2C is enforced at the Component level for all environments.
2. All mandated devices checks are implemented using C2C at the Component level.

Capability 2.3 Device Authorization with Real-Time Inspection

Table 37: Capability 2.3 — Device Authorization with Real-Time Inspection

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
2 - Device	2.3 - Device Authorization with Real-Time Inspection
Description	
DoW Components conduct foundational and extended device tooling (Next-Generation AV, AppControl, File Integrity Monitoring (FIM), etc.) integration to better understand the risk posture. Organizational PKI systems are integrated to expand the existing Enterprise PKI to devices as well. Lastly Entity Activity Monitoring is also integrated to identify anomalous activities.	
Impact to ZT	
Components can use policies to deny devices by default and explicitly allow access to DAAS resources only by devices that meet mandated configuration standards. Security threats identified are remediated faster through continuous activity inspection enables faster remediation of security threats.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component integrates foundational device security solutions, including Next-Generation Antivirus (NextGen AV), Application Control, and File Integrity Monitoring (FIM), to assess the risk posture of all devices attempting network access.
- The Enterprise Public Key Infrastructure (PKI) solution is expanded to include device certificates, ensuring that all devices, including unmanaged and infrastructure devices, are uniquely identifiable and verifiable.
- A deny-by-default policy is implemented, allowing network access only to devices that meet strict configuration and security standards.
- A device attempting to connect is flagged as non-compliant due to missing a valid PKI certificate, and access is denied automatically.
- Real-time Entity Activity Monitoring (EAM) solutions are deployed, tracking device behavior across endpoints and information Technology (IT) infrastructure to identify anomalous or malicious activities.
- During routine operations, EAM detects a device exhibiting unusual activity, such as frequent failed access attempts to restricted resources, and raises an alert for the security team.

- The alert triggers an automated response that quarantines the device, isolates it from the network, and initiates further inspection.
- Investigation reveals that the anomalous activity originated from malware attempting to exploit a misconfigured application on the device, which is quickly remediated using integrated NextGen AV and FIM solutions.
- The Component integrates the device security stack with the Comply-to-Connect (C2C) solution, ensuring that devices are continuously monitored and inspected throughout their session in alignment with Zero Trust (ZT) principles, not just at the point of entry.
- By combining real-time inspection with robust device authorization policies, the Component enhances its ability to prevent unauthorized access and mitigate threats quickly.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Comprehensive Risk Assessment: Integrating advanced security tools like NextGen AV, Application Control, and FIM, provides a more accurate understanding of the overall security landscape.
- Enhanced Authentication and Trust: The Component expands PKI integration to devices, establishing stronger identity verification and validation and securing communications across the infrastructure.
- Early Threat Detection: The EAM identifies anomalous behaviors before they escalate into significant security incidents.
- Reduced Security Blind Spots: The Component combines multiple security technologies into a cohesive system, enabling more thorough protection against sophisticated threats.
- Data-Driven Security: Decision-making is supported by integrated tooling that provides actionable intelligence about potential vulnerabilities and attack vectors.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- File Integrity Monitoring (FIM)
- Multi-Factor Authentication (MFA)
- Public Key Infrastructure (PKI)
- Network Access Control (NAC)
- Next-Generation Antivirus (NextGen AV)
- Real-Time Monitoring

Activity 2.3.3 Implement Application Control and File Integrity Monitoring (FIM) Tools

Table 38: Activity 2.3.3 — Implement Application Control and File Integrity Monitoring (FIM) Tools

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components procure and implement File Integrity Monitoring (FIM) and application control (e.g., execution deny/allow listing, containment, isolation) solutions. FIM ensures any data altered is authorized, and unauthorized changes are detected by FIM. Application containment is used to isolate any suspicious behavior or permissions to prevent any malicious lateral movement, expanding the capabilities and response of traditional executable containment. Both FIMs and application containment continues the development of the Device, Data, and Application & Workload pillars.	
Predecessor(s)	**Successor(s)**
None	None
Expected Outcomes	
• Application control and FIM tooling is implemented on all service applications and endpoint devices with C2C orchestration. • EDR tooling covers maximum amount of services applications and endpoint devices.	
End State	
Components deploy FIM and application control tooling in alignment with EDR, SOAR, and UEM. C2C orchestration and regular control audits and alerts are in place.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Where applicable, Endpoint Detection and Response (EDR), Security Orchestration, Automation, and Response (SOAR), Unified Endpoint Management (UEM), and Comply-to-Connect (C2C) solutions should already be integrated into the environment before starting this activity.
- Integrate appropriate Application Control (e.g., execution deny/allow listing, containment, isolation, etc.) and File Integrity Monitoring (FIM) solution(s) based on Enterprise policies and procedures.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 39: Implementation Tasks for Activity 2.3.3 — Implement Application Control and File Integrity Monitoring (FIM) Tools

Plan and prepare for Application Control and FIM implementation.
Initial environment assessment: ☐ Conduct a comprehensive assessment of the current Application Control landscape, identifying critical applications and file systems. ☐ Identify directories and files containing data critical to the Component's operation, security, and compliance and require continuous monitoring. ☐ Define the scope of Application Control and FIM deployment, including endpoints, servers, and cloud environments. ☐ Prioritize Application Control and FIM deployment based on Enterprise and/or Component-defined risk level/criticality. **Select Application Control and FIM solutions that align with Enterprise policies and procedures:** ☐ Define the overall security and compliance objectives for both Application Control and FIM, including preventing unapproved application execution, detecting malicious activity, and ensuring data integrity. ☐ Identify stakeholders (e.g., Information Technology (IT) operations, security teams, application owners, etc.) and formal Enterprise structure. ☐ Select Application Control and FIM tools compatible with the existing infrastructure and cybersecurity tools. ☐ Develop a phased implementation plan with timelines, resource requirements, risk mitigation strategies, and rollback procedures.
Deploy Application Control tools.
Prepare the environment for solution integration: ☐ Establish baseline application inventories by scanning systems for installed and running applications. ☐ Define, monitor, and implement application whitelist, greylist, and blacklist policies. ☐ Configure the Application Control solution to enforce the defined whitelist, greylist, and blacklists policies. **Based on environment needs, apply Indicators of Compromise (IoC) solutions and maintain application whitelist, greylist, and blacklist:** ☐ Integrate Application Control solutions with IoC solutions (e.g., Endpoint Protection Platform (EPP), EDR, etc.). ☐ During Application Control solution integration, follow Enterprise Application Control policies in a staged manner (e.g., audit mode before enforcement, etc.) to minimize operational disruption.

☐ Conduct pilot testing in non-production environments to analyze impacts on environmental performance, User/Person Entity (PE) experience, and overall Component cybersecurity posture.

☐ Regularly review and update the application whitelist, greylist, and blacklist based on operational needs and emerging threats.

Deploy FIM tools.

Prepare the environment for FIM solution integration:

☐ Verify and validate critical files, directories, system configurations, and application binaries that require integrity monitoring.

☐ Organize files based on their criticality, importance, and sensitivity to ensure the most critical files are prioritized for monitoring during FIM solution integration.

☐ Deploy FIM solutions on targeted systems, ensuring coverage across on-premises, cloud, and hybrid environments.

Integrate FIM solutions to monitor data integrity:

☐ Configure FIM solutions to monitor for altered data and unapproved changes (e.g., file modifications, additions, deletions, permission changes, etc.).

☐ Establish real-time alerting and automated response mechanisms for critical file integrity violations.

☐ Ensure integration of FIM solutions with Security Information and Event Management (SIEM) platforms for centralized log management and correlation.

☐ Conduct baseline scans to establish a known, good state for monitored files and configurations.

Verify and validate Application Control and FIM efficacy.

Assess, review, and improve Application Control and FIM deployment:

☐ Perform verification and validation testing by simulating unapproved application executions and file modifications.

☐ Conduct security assessments and penetration testing to ensure the strength of implemented controls, as applicable.

☐ Review Application Control and FIM alerts and adjust policies to reduce noise without compromising cybersecurity posture.

☐ Analyze historical data from FIM to detect patterns of anomalous activity, potential insider threats, and/or Advanced Persistent Threats (APTs).

☐ Implement continuous feedback loops with stakeholders to refine and optimize FIM configurations.

Integrate Application Control and FIM solutions with the broader security environment.

Supplement existing Enterprise cybersecurity strategies with the integration of Application Control and FIM solutions:

☐ Ensure integration of Application Control and FIM solutions with existing EDR, SIEM, C2C, and network security solutions.

☐ Configure automated workflows for Incident Response (IR) based on alerts from Application Control and FIM solutions. ☐ Enable Role-Based Access Controls (RBACs) within Application Control and FIM solutions to control, monitor, and maintain privileged access. ☐ Utilize Application Control and FIM solution data to enable continuous verification and validation for User/PE/Non-Person Entity (NPE) authentication.
Maintain Application Control and FIM solution management.
Manage Application Control and FIM solutions: ☐ Define operational processes for managing Application Control and FIM solutions, including reviews and updates. ☐ Schedule regular audits, integrity scans, and regulatory compliance checks to ensure continuous alignment with evolving Enterprise cybersecurity policies. ☐ Perform root cause analysis for Application Control breaches and FIM alerts to continuously inform Enterprise cybersecurity policy refinement. **Monitor, optimize, and improve Application Control and FIM solutions:** ☐ Continuously develop and enact reporting mechanisms to track Application Control and FIM solution performance metrics (e.g., false positive rates, response times, etc.), incident trends, and Enterprise compliance status. ☐ Adjust Application Control and FIM solution policies based on threat intelligence, operational feedback, and evolving Enterprise and regulatory compliance requirements.

Summary

This diagram outlines the Activity 2.3.3 (Phase Two) – *Implement Application Control and File Integrity Monitoring (FIM) Tools* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of File Integrity Monitoring (FIM) and application control solutions. It presents strategic insights that drive implementation and expected outcomes, including application control and FIM tooling implementation across all service applications and endpoint devices, with Comply-to-Connect (C2C) orchestration.

Table 40: Activity 2.3.3 — Implement Application Control and File Integrity Monitoring (FIM) Tools - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are FIM and Application Control solutions procured and implemented? 2. How is the integration with Enterprise and organizational Public Key Infrastructure (PKI) environments achieved for application allowances? 3. How is Next-Generation Antivirus (NextGenAV) tooling expanded to cover all possible services and applications?

STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for implementing FIM and application control measures, ensuring alignment with Enterprise security standards and requirements for Endpoint Detection and Response (EDR), Security Orchestration, Automation, and Response (SOAR), Unified Endpoint and Device Management (UEDM) solution, and C2C orchestration. • The Component demonstrates compliance by deploying FIM tools to detect unapproved file changes, establishing baselines, and integrating with Security Information and Event Management (SIEM) and Identity and Access Management (IAM) systems, as well as by implementing application control solutions that employ whitelisting, greylisting, blacklisting, and certificate-based allowances to isolate suspicious behavior and prevent lateral movement. • The Component provides evidence that these measures (FIM and application control) undergo continuous monitoring, regular audits, and policy updates, with training and tabletop exercises ensuring that Information Technology (IT) and security personnel can effectively respond to alerts, adapt to new threats, and maintain compliance with regulatory guidance. • The Component ensures that EDR solution is selected, deployed, and integrated to cover a broad range of services, applications, and endpoints, and that it aligns with Enterprise standards, supports scalability, and works seamlessly with existing security tools (e.g., SIEM, threat intelligence, etc.). • The Component continuously improves its overall security posture by conducting pilot deployments, verifying and validating configurations, reviewing logs and reports, performing after-action reviews, and incorporating lessons learned into refined policies and procedures, thereby maintaining compliance and adapting to evolving cyber threats.

✓ EXPECTED OUTCOMES

1. Application control and FIM tooling is implemented on all service applications and endpoint devices with C2C orchestration.
2. EDR tooling covers maximum amount of services applications and endpoint devices.

Capability 2.4 Remote Access

Table 41: Capability 2.4 — Remote Access

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
2 - Device	2.4 - Remote Access
Description	
DoW Components audit existing device access processes and tooling to set a Least Privilege baseline. In Phase Two this access is expanded to cover basic BYOD and IoT support using the Enterprise IdP for approved applications. The final Phases expand coverage to include all BYOD and IT devices for services using the approved set of device attributes.	
Impact to ZT	
Enables properly authorized and authenticated users and NPEs to access DAAS from remote locations.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component conducts an audit of existing remote access processes and tooling, identifying gaps in security and setting a Least Privilege baseline for all remote connections.
- A deny-by-default policy is implemented, ensuring only authorized User/Person Entities (PEs)/Non-Person Entities (NPEs) are allowed to establish remote connections.
- The Component integrates its Enterprise Identity Provider (IdP) with remote access systems, enabling secure access to approved applications for managed devices while enforcing strong authentication requirements.
- Bring Your Own Device (BYOD) and Internet of Things (IoT) remote access policies are developed, and the necessary capabilities are deployed to provide secure, managed, and limited access to specific services following compliance verification.
- A contractor requests remote access using a personal device. The system verifies the device’s compliance with required security attributes, such as updated antivirus and encryption, before granting limited access to approved and necessary resources.
- The Component verifies and validates the success of the BYOD access controls by securely enabling multiple Users/PEs to work remotely without expanding the

threat surface, ensuring Zero Trust (ZT) principles are upheld through identity-driven access and continuous device posture enforcement.

- Later real-time monitoring of remote access sessions detect unusual activity from a User/PE's personal device accessing an unusually high amount of Data, Applications, Assets, and Services (DAAS) resources. The session is automatically terminated, and the User/PE is required to re-authenticate.
- The User/PE fails to re-authenticate and the suspicious activity comes to an end.
- Post-incident analysis reveals that the unusual activity came from an unexpected geographic location and was an attempted session hijack. After review, the Component updates its remote access policies to include additional checks for location-based anomalies.
- By establishing secure remote access policies which meet the operational needs of their environment, and by managing BYOD and IoT connections through the Enterprise IdP, the Component adheres to ZT principles, ensuring only authorized and compliant User/PEs and devices can access DAAS from remote locations.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Strengthened Security Foundation: By establishing Least Privilege baseline, minimizing potential attack surface, and reducing unapproved access risks.
- Controlled Expansion of Device Ecosystem: The Component safely incorporates BYOD and IoT devices while maintaining security standards via Component IdP integration.
- Consistent Security Enforcement: Standardized Attribute-Based Access Controls (ABACs) across all device types ensures uniform protection regardless of device ownership.
- Improved User/PE Experience: Enabling secure access to approved applications from personal devices increases productivity while maintaining security boundaries.
- Scalable Security Architecture: The Component accommodates future growth in device diversity and quantity without compromising protection levels or requiring a complete redesign.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Cloud Access Security Broker (CASB)
- Endpoint Detection and Response (EDR)
- Enterprise Mobility Management
- Mobile Device Management (MDM)
- Network Access Control (NAC)

Activity 2.4.2 Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support

Table 42: Activity 2.4.2 — Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components utilize Enterprise Device Management Solution to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP. Enabling user and device-based authorization is supported. Device access requires dynamic access policies and the practice of Least Privilege.	
Predecessor(s)	**Successor(s)**
None	2.2.1, 2.4.3
Expected Outcomes	
• All Component access must be governed by dynamic access permissions for BYOD and IoT devices. • Component BYOD and IoT device permissions are baselined and integrated with Enterprise IdP.	
End State	
Components establish a foundation for risk-based access control for BYOD and IoT with dynamic permissions.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* and Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) Part 1* can inform the implementation of an Enterprise Device Management (EDM) solution capable of managing Bring Your Own Device (BYOD) and Internet of Things (IoT) devices.
- Presumption: Dynamic access policies for device access to the Component environment should already be established.
  - Policies include consideration of device posture, user context, and resource sensitivity.
  - Define specific criteria for granting or denying access based on these factors.

- Presumption: The Component has completed Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1*, as this activity requires Enterprise Identity Provider (IdP) integration.
- Ensure Enterprise IdP is already configured, implemented, and fully operational before starting this activity.
- Verify and validate the compatibility of EDM solutions with existing Information Technology (IT) infrastructure, including IdP, environment components, and other security solutions.
- Ensure the EDM solution can scale to accommodate future growth, an evolving Component environment, and increased BYOD and IoT devices.
- Regularly review and update Enterprise cybersecurity policies to address emerging threats and vulnerabilities specific to BYOD and IoT devices, such as mobile device management policies, IoT security guidelines, and data encryption requirements as they relate to mobile and IoT threats.
- Integrate EDM solutions with threat intelligence feeds to stay informed about emerging threats, where applicable.
- Implement alerts for suspicious activities, policy violations, or Indicators of Compromise (IoC), ensuring that dynamic access controls are working as intended, where applicable.
    - Examples include: Unapproved access attempts from BYOD or IoT devices, compromised device indicators, attempts to access restricted resources, and non-compliance with security policies.
- Activity 2.2.1 (Phase Two) – *Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1* and Activity 2.4.3 (Phase Three) – *Managed and Full BYOD and IoT Support Part 1* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 43: Implementation Tasks for Activity 2.4.2 — Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support

Develop Component EDM integration plan.
Develop an EDM integration plan: ☐ Leverage approved Hardware/Software List for environment authentication, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis.* ☐ Leverage the Component EDM solution, from Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) Part 1*. ☐ Leverage existing Enterprise policies and procedures to develop requirements for managing the EDM. ☐ Verify and validate the EDM solution supports BYOD and IoT and provides device management automation related to critical data and services. ☐ Document any EDM deficiencies in accordance with the Enterprise's policies and implement an alternate solution as required for BYOD and IoT devices.
Manage BYOD and IoT devices that cannot be managed by the EDM solution through risk-based exceptions.
Manage exceptions: ☐ BYOD and IoT devices incompatible with the EDM solution are: • Identified • Documented • Approved/Rejected ☐ The Enterprise and/or Component determines risks. ☐ Approval is granted when justification for the exception outweighs the risks to the Enterprise/Component. ☐ Approval is periodically reassessed.
Integrate BYOD and IoT devices with the Enterprise IdP.
☐ Configure EDM solution for BYOD and IoT device enrollment and integration with the Enterprise IdP for seamless authentication and approval. ☐ Test the authentication process by logging in to a managed device (e.g., BYOD, IoT, etc.) to ensure proper integration and access control.
Establish BYOD and IoT device permission baselines and integrate them with the Enterprise IdP.
Define BYOD and IoT device access permissions based on the device baseline: ☐ Identify and document the baseline access permissions for all BYOD and IoT devices that exist within the Component environment. ☐ Establish role-based or device-specific permissions based on Enterprise and Component security policies.

Integrate BYOD and IoT device permissions with the Enterprise IdP:

☐ Ensure device-specific access permissions are linked to User/PE/NPE profiles within the Enterprise IdP.

☐ Configure and integrate the IdP to automatically synchronize User/PE/NPE identity data with device profiles, ensuring consistent and accurate adherence to access control policies.

Verify and validate permissions and perform cybersecurity audits:

☐ Conduct testing to ensure the baseline permissions are applied correctly for each BYOD and IoT device and the Enterprise IdP is enforcing the correct access rights.

☐ Audit device access logs and permissions regularly to ensure any deviations from the baselines are promptly addressed, maintaining Enterprise and Component security and compliance.

Establish risk-based access control for BYOD and IoT devices with dynamic permissions.

Define risk-based access control criteria:

☐ Establish risk-based access controls that consider factors like device health, compliance status, User/PE/NPE behavior, and environmental context (e.g., location, network conditions, etc.).

☐ To maintain a healthy cybersecurity posture, document risk levels and map them to specific access permissions or restrictions for BYOD and IoT devices.

Adjust permissions dynamically based on risk assessment results:

☐ Configure Access Control List(s) (ACL(s)) to dynamically adjust device access permissions based on real-time risk assessments (e.g., deny access for non-compliant or unmanaged devices, etc.).

Test and monitor risk-based Access Controls:

☐ Test the implementation of risk-based access controls to verify and validate dynamic permission changes.

☐ Set up monitoring and alerting systems to track deviations from expected access patterns, ensuring the Access Control system adapts effectively to emerging threats and vulnerabilities.

Implement dynamic Access Control for all BYOD and IoT devices within the Component environment.

Implement dynamic Access Control policies:

☐ Implement dynamic access control policies based on device type, User/Person Entity (PE)/Non-Person Entity (NPE) role, and security posture (e.g., device health, compliance status, etc.).

☐ Ensure the policies are adaptable, allowing real-time adjustments based on location, time of access, and/or device status.

Integrate device status into Access Control policies:

☐ Configure the system to collect and use real-time device status (e.g., device type, operating system, security compliance, etc.) to determine and control access levels.

☐ Ensure that the access permissions are automatically adjusted based on the status (e.g., denying access for non-compliant and/or unmanaged devices, etc.).

Enable real-time monitoring and auditing:

☐ Configure and apply the established EDM solution to track and audit access requests made by BYOD and IoT devices to critical services, applications, and devices within the environment.

Test, verify, and validate dynamic Access Controls:

☐ Perform testing with BYOD and IoT devices to ensure dynamic access control policies are correctly enforced in various scenarios.

Verify and validate access is granted or denied according to the dynamic rules, based on the current status of the device and compliance with Enterprise policies.

Summary

This diagram outlines the Activity 2.4.2 (Phase Two) – *Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of policies to closely manage devices introduced into the Enterprise Identity Provider (IdP) environment. It presents strategic insights that drive implementation and expected outcomes, including Component Bring Your Own Device (BYOD) and Internet of Things (IoT) device permissions governed by dynamic access permissions.

Table 44: Activity 2.4.2 — Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are managed BYOD and IoT devices integrated with the Enterprise IdP to support User/Person Entity (PE) and device-based authorization? 2. How are dynamic access policies enforced for all applications requiring device access?

STRATEGIC INSIGHTS
• The Component defines a Unified Endpoint and Device Management (UEDM) solution strategy by aligning with Enterprise policies, conducting gap analysis, and developing a structured approach for managing BYOD and IoT integration. • The Component demonstrates security and compliance by implementing dynamic access control policies, integrating device health assessments, and enforcing real-time authentication approval through the Enterprise IdP. • The Component provides verifiable enforcement through continuous monitoring, access audits, and dynamic risk-based controls, ensuring that device permissions are consistently applied and automatically adjusted based on compliance status and security posture. • The Component leverages real-time device status data, automated synchronization with IdP profiles, and security baselines to enforce adaptive access control mechanisms and mitigate risks associated with unmanaged or non-compliant devices. • The Component ensures ongoing security by establishing cybersecurity audits, testing risk-based access controls, and continuously refining UEDM policies to align with evolving Enterprise security frameworks and threat landscapes.

EXPECTED OUTCOMES
1. All Component access must be governed by dynamic access permissions for BYOD and IoT devices. 2. Component BYOD and IoT device permissions are baselined and integrated with Enterprise IdP.

Capability 2.6 Unified Endpoint Management (UEM) and Mobile Device Management (MDM)

Table 45: Capability 2.6 — Unified Endpoint Management (UEM) and Mobile Device Management (MDM)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
2 - Device	2.6 - Unified Endpoint Management (UEM) and Mobile Device Management (MDM)
Description	
DoW Components establish a centralized UEM solution that provides the choices of agent and/or agentless management of computer and mobile devices to a single console regardless of device location. DoW-issued devices can be remotely managed and security policies are enforced.	
Impact to ZT	
DAAS resources are protected through agent and agentless management, IT is able to manage, secure, and deploy resources and applications on any device from a single console to provide redress of cybersecurity threats. Security vulnerabilities are mitigated and policy enforcement measures are received through IT remote management of DoW-issued mobile devices.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component implements a centralized Unified Endpoint Management (UEM) solution, enabling agent and agentless management of all computer and mobile devices through a single console.
- Security policies are configured in the UEM solution to enforce device compliance, such as requiring encryption, up-to-date antivirus software, and secure configurations.
- Information Technology (IT) administrators use the UEM solution to remotely manage Enterprise/Component issued devices, applying patches, deploying applications, and monitoring compliance status regardless of device location.
- An Enterprise/Component issued mobile device is reported lost by a User/Person Entity (PE), and the IT team uses the UEM solution to remotely lock the device, wiping sensitive data to prevent unauthorized access.
- During a routine compliance scan, the UEM solution detects a non-compliant device with outdated security patches and restricts its access to Data, Applications, Assets, and Services (DAAS) resources until the issue is resolved.

- A malicious actor attempts to connect a rogue mobile device to the network, but the UEM solution, operating under Zero Trust (ZT), automatically blocks unregistered and unverified devices from gaining access.
- The Component leverages the UEM solution to deploy a critical security update to all managed devices within hours of a vendor vulnerability announcement, reducing exposure to potential exploits.
- IT administrators monitor real-time analytics in the UEM console, detecting unusual device behavior, such as unauthorized application installations, and taking corrective action.
- Regular audits of the UEM solution ensure that all security policies remain effective and that emerging vulnerabilities are quickly addressed.
- By centralizing device management through the UEM solution, the Component ensures DAAS resources are protected, security vulnerabilities are mitigated, and policies are enforced remotely.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Streamlined Device Management: The Component implements a unified console that handles both agent-based and agentless approaches, significantly reducing administrative complexity and overhead.
- Location-Independent Security Control: Consistent policy enforcement regardless of where devices are physically located protects organizational assets everywhere.
- Enhanced Operational Visibility: Centralized monitoring capabilities provide a comprehensive view of all managed devices from a single management platform.
- Improved Security Posture: Consistent application and enforcement of security policies across the entire device fleet reduces configuration drift and security gaps.
- Increased Administrative Efficiency: Remote management capabilities that eliminate the need for physical access to devices enables faster response times and reduces support costs.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Asset/Device/Endpoint Management solutions
- Device Health Monitoring
- Enterprise Mobility Management
- Mobile Device Management (MDM)
- Next-Generation Antivirus (NextGen AV)

Activity 2.6.3 Enterprise Device Management (EDM) Part 2

Table 46: Activity 2.6.3 — Enterprise Device Management (EDM) Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components migrate the remaining devices to Enterprise Device Management (EDM) solution. EDM solution is integrated with risk and compliance solutions as appropriate.	
Predecessor(s)	**Successor(s)**
2.6.2	None
Expected Outcomes	
• Manual inventory of devices, software, and security posture of each device is integrated with an automated management solution for all services.	
End State	
All devices are managed and automation is utilized where applicable for rapid threat mitigation.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, to leverage device inventory.
- Consider completing Activity 2.5.1 (Phase One) – *Implement Asset, Vulnerability, and Patch Management Tools* prior to this activity, to leverage asset vulnerability and patch management solutions.
- Ensure Enterprise data privacy regulations are met, protecting sensitive information.
- Verify and validate compatibility with the existing infrastructure, including legacy systems, environment Components, and other security solutions.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 47: Implementation Tasks for Activity 2.6.3 — Enterprise Device Management (EDM) Part 2

Migrate the remaining devices to the Unified Endpoint and Device Management (UEDM) solution and integrate the devices with risk and compliance solutions, as appropriate.
Review the Enterprise UEDM Integration and Device Migration Plan: ☐ Leverage existing Enterprise standards and policies for managing the UEDM solution, from Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) Part 1*. ☐ Leverage approved Hardware/Software List for environment authentication, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis.* ☐ Verify and validate that the Component Master Device Inventory accurately reflects the current environment(s). **Verify and validate the migration plan:** ☐ Develop a strategy for migrating the manual device inventory to an automated process using the UEDM solution. ☐ Leverage existing Enterprise strategies and guidance to migrate all remaining approved devices to the Enterprise UEDM solution. ☐ Confirm the accuracy and completeness of the manual inventory data. **Verify and validate UEDM functionality:** ☐ Confirm the configuration of the UEDM solution. ☐ Confirm import of manual inventory data. ☐ Confirm UEDM output to the manual inventory list. ☐ Confirm automated management of the devices running critical services. ☐ Confirm interoperability with existing compliance tools that support risk assessment and compliance monitoring.
Enforce patch management and configuration baselines.
Establish patch management and configuration baseline plans: ☐ Leverage Enterprise policies for patch management, including patch management (e.g., identify, test, deploy, verify and validate, etc.) and configuration baseline management (e.g., create, enforce, monitor, etc.). ☐ Leverage the Component selected Asset Vulnerability and Patch Management solutions, from Activity 2.5.1 (Phase One) – *Implement Asset, Vulnerability, and Patch Management Tools*.

☐ Review vulnerability management activities in the other pillars, if completed, to ensure consistent implementation across Component Devices, Applications, Assets, and Services (DAAS).

Confirm implementation of patch management and configuration baseline plans:

☐ Verify and validate the implementation and configuration of patch management solutions to automate patch deployment, verification, and validation.

☐ Verify and validate the creation, enforcement, and monitoring of configuration baselines.

Confirm interoperability with the existing compliance monitoring solution:

☐ Verify and validate solution interoperability across multiple systems within the Component's environment.

☐ Verify and validate interoperability between compliance solutions to ensure a hardened security posture.

Integrate device information with UEDM.

UEDM device integration:

☐ Leverage the Component UEDM solution, from Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) Part 1*.

☐ Integrate devices into the UEDM solution.

☐ Verify and validate the output of UEDM for the accuracy of the manual inventory of devices, software, and security posture.

☐ Verify and validate UEDM's interoperability, integration, and configuration with the Security Information and Event Management (SIEM) and Configuration Management (CM) solutions to ensure continuous security and monitoring.

☐ Verify and validate Enterprise policy compliance and identify any potential issues.

Implement device quarantine for non-compliant devices.

Enforce Enterprise cybersecurity guidance:

☐ Verify and validate device compliance criteria, including security posture, software updates, and configuration baselines.

☐ Verify and validate Enterprise policies that define the response for non-compliant devices, such as environment isolation, restricted access, and remediation steps.

Verify and validate the integration of compliance tools:

☐ Verify and validate security tools that support device isolation, remote quarantine, continuous monitoring and alerting, and interoperability with existing tools.

Verify and validate the integration of the UEDM solution:

☐ Verify and validate that the UEDM solution will be configured to monitor devices continuously and automatically quarantine non-compliant devices.

☐ Verify and validate the integration of the UEDM solution with SIEM tools to ensure continuous monitoring and alerting.

Continuously test and monitor solutions and devices to maintain compliance.

Test, verify, and validate solution functionality:

☐ Conduct functional testing to ensure that the quarantine capability works as expected. Testing should include at a minimum:

- Isolating compromised devices.
- Network restrictions during quarantine.
- The process for releasing devices from quarantine.
- Specific frequency of these tests (e.g., after every major update, quarterly, etc.).

☐ Perform security testing to identify and mitigate any vulnerabilities. Such as penetration testing, vulnerability scanning, etc.

- The Component should assign security testing to groups as appropriate. Examples include internal or external vulnerability management teams, Cybersecurity Service Providers (CSSPs), etc.

☐ Resolve/remediate vulnerabilities in accordance with the Component vulnerability management plan.

Monitor and audit devices to maintain security compliance:

☐ Monitor all implementation and integration to ensure security and performance.

- Monitoring should be conducted to facilitate the effectiveness of the vulnerability management plan as well as operational impacts and performance metrics, such as resource usage (e.g., storage space, Central Processing Unit (CPU)/Random-Access Memory (RAM) usages, etc.).

☐ Perform regular audits to verify and validate security policy compliance and identify potential issues.

☐ Monitor all devices in real-time/near real-time to enable the Enterprise to detect and respond to potential security threats promptly, ensuring the protection of sensitive data and resources [17].

Summary

This diagram outlines the Activity 2.6.3 (Phase Two) – *Enterprise Device Management (EDM) Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the integration of device migration into the Enterprise Device Management (EDM) solution and the integration of that solution with risk and compliance solutions. It presents strategic insights that drive implementation and expected outcomes, including the integration of manual inventory with an automated management solution.

Table 48: Activity 2.6.3 — Enterprise Device Management (EDM) Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are remaining devices migrated to the EDM solution? 2. How is the EDM solution integrated with risk and compliance solutions?

STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for migrating remaining devices into an EDM solution, integrating with risk and compliance tools, patch management systems, and configuration baseline frameworks in alignment with Enterprise security requirements. • The Component demonstrates compliance by selecting Unified Endpoint and Device Management (UEDM) solutions that provide comprehensive device coverage and implementing automated processes for asset discovery, enrollment, continuous monitoring, patch deployment, and baseline Configuration Management (CM), ensuring that all devices adhere to established Enterprise requirements. • The Component provides evidence that the UEDM solution is integrated with risk assessment and compliance monitoring platforms, Security Information and Event Management (SIEM) solutions, and Network Access Control (NAC) mechanisms, enabling real-time security posture assessments, threat detection, and automated remediation (e.g., quarantining non-compliant devices, etc.) across all endpoints. • The Component ensures that manual inventories are replaced with a fully automated, policy-driven management approach, consolidating device, software, and security posture data into a single approved source, thereby simplifying reporting, improving operational efficiency, and enhancing the Component's overall cybersecurity posture. • The Component continuously audits, tests, verifies, and validates the integrated solutions, employing User Acceptance Testing (UAT), functional and security assessments, and compliance reviews, and makes necessary adjustments to policies, tool configurations, and procedures to maintain ongoing compliance, effectiveness, and alignment with ZT principles.

✓ EXPECTED OUTCOMES

1. Manual inventory of devices, software, and security posture of each device is integrated with an automated management solution for all services.

Capability 2.7 Endpoint and Extended Detection and Response (EDR and XDR)

Table 49: Capability 2.7 — Endpoint and Extended Detection and Response (EDR and XDR)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
2 - Device	2.7 - Endpoint and Extended Detection and Response (EDR and XDR)
Description	
DoW Components use Endpoint Detection and Response (EDR) tooling to monitor, detect, and remediate malicious activity on endpoints. Expanding the capability to include XDR tooling allows organizations to account for activity beyond the endpoints such as cloud and network as well.	
Impact to ZT	
Threats originating from network-connected endpoints are initially reduced through active investigation and response. Maturation focuses on forensics and faster threat detection and remediation are enabled by correlating data across multiple security layers (e.g., email, cloud, endpoint).	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component deploys Endpoint Detection and Response (EDR) solutions to monitor all endpoints on the network, detecting and mitigating malicious activity in real-time.
- Security policies are configured in the EDR solution to automatically isolate compromised endpoints from the network, embodying the Zero Trust (ZT) principle of assuming breach and limiting the spread of potential threats.
- The Component’s Security Operations Center (SOC) receives an alert from the EDR solution noting unusual activity on a workstation, including unauthorized attempts to escalate privileges.
- SOC analysts investigate the alert, leveraging the EDR solution to retrieve detailed forensic data, confirming that malware was installed on the endpoint.
- The compromised endpoint is quarantined remotely, and remediation steps such as removing malware and applying patches, are executed through the EDR solution.
- To expand visibility beyond endpoints, the Component integrates Extended Detection and Response (XDR) solutions, correlating data from email, cloud, and network activity with endpoint telemetry.

- XDR detects a coordinated attack where malicious actors attempt to exfiltrate data by exploiting both endpoint and cloud-based vulnerabilities.
- The integrated XDR solution automatically triggers a containment response, blocking suspicious activity across multiple security layers and notifies the SOC.
- Post-incident analysis reveals gaps in the Component’s detection policies, prompting updates to strengthen EDR and XDR rules and improve threat-hunting capabilities.
- By leveraging EDR for endpoint security and expanding to XDR for multi-layered threat detection and response, the Component minimizes risks from network-connected endpoints and advanced threats.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Threat Detection: Continuous monitoring of endpoints enables rapid identification of suspicious activities before they can cause significant damage.
- Accelerated Incident Response (IR): Employing automated remediation options that can contain threats in real-time minimizes potential impacts on critical systems and data.
- Expanded Visibility: Integrating cloud and network data with endpoint information across multiple security domains creates a more comprehensive security picture.
- Improved Threat-Hunting Effectiveness: The correlation of activities across different environments helps security teams identify complex attack patterns that might otherwise go undetected.
- Strengthened Security Analytics: Leveraging richer contextual data from multiple sources enables more accurate risk assessments and better-informed security decisions.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
- Managed Detection and Response (MDR)
- Next-Generation Antivirus (NextGen AV)

Activity 2.7.2 Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1

Table 50: Activity 2.7.2 — Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components procure and implement Extended Detection and Response (XDR) solution(s). Integration points with cross-pillar capabilities (network, cloud services, applications) are identified and prioritized based on risk. XDR is aligned with C2C program. XDR capabilities either supplement or replace EDR implementations. Analysis and correlation capabilities are sent from the XDR solution stack to the SIEM.	
Predecessor(s)	**Successor(s)**
2.7.1, 7.2.1	2.7.3
Expected Outcomes	
• XDR solution is implemented and replaces EDR where possible. • Integration points have been identified and prioritized per capability. • XDR and SIEM have integrations to gain a comprehensive view of data integration, correlation, analytics, incident response, and automation.	
End State	
Expanding from an EDR to an XDR solution provides a holistic view of the threat landscape, allowing for coordinated response, automation, and orchestration when responding to threats.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 2.7.1 (Phase One) – *Implement Endpoint Detection and Response (EDR) Tools and Integrate with Comply-to-Connect (C2C)* and Activity 7.2.1 (Phase One) – *Threat Alerting Part 1* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Expanding an Enterprise Endpoint Detection Response (EDR) to an Enterprise Extended Detection and Response (XDR) solution provides a holistic view of the threat landscape that allows for more effective Incident Response(s) (IR(s)).
- Activity 2.7.3 (Phase Three) – *Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 2* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 51: Implementation Tasks for Activity 2.7.2 — Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1

Identify XDR requirements.
Assess the environment in preparation for a transition from an EDR to an XDR solution: ☐ Select an XDR solution aligned with Component requirements to ensure compatibility with existing solutions. ☐ Identify EDR deployments that can be replaced or extended by the XDR solution based on enhanced capabilities (e.g., cross-pillar correlation, advanced analytics, etc.). ☐ Develop a phased approach to deployment, prioritizing assets that present the most risk to the Component/Enterprise. ☐ Develop a phased approach to decommission any redundant EDR solutions, ensuring no coverage gaps occur during the transition.
Implement an XDR solution and replace EDR, where applicable.
☐ Deploy XDR solutions across endpoints, environment devices, cloud services, and applications, where applicable. **Configure XDR policies within the environment:** ☐ Unify threat detection across multiple domains to simplify security management and improve visibility of devices across environments. ☐ Automate response and remediation workflows to accelerate IR and reduce manual effort. ☐ Conduct testing in isolated environments to ensure minimal disruption during production deployment. ☐ Verify and validate that the XDR solution effectively replaces and/or supplements the existing EDR and is functionally compatible with the C2C and Security Information and Event Management (SIEM) solutions. ☐ Update operational documentation to reflect new XDR processes and configurations.

Identify integration points between cross-pillar capabilities and the XDR and conduct a risk assessment of the identified integration points, where applicable.

Conduct a cross-pillar assessment to identify integration points between the XDR and existing solutions:

☐ Review previously implemented activities to ensure successful integration and interoperability of the XDR and the existing EDR, C2C, and SIEM solutions.

Perform a risk assessment for each integration point and use the results to prioritize the integration points accordingly:

☐ During the risk assessment, consider the data sensitivity, threat likelihood, potential impacts, and exposure to external networks for each integration point.

☐ Prioritize integration points based on criticality to Enterprise cybersecurity posture.

☐ Based on risk assessment findings, ensure XDR integration prioritizes the high-risk areas of the threat landscape within the environment (e.g., privileged access, external-facing applications, etc.).

☐ Document dependencies, constraints, and challenges to inform further integration across the environment.

Ensure integration of XDR and SIEM solutions, which enable comprehensive data sharing and effective IR, where applicable.

Integrate the XDR and the SIEM solutions:

☐ Identify critical data points from the XDR stack (e.g., alerts, behavioral anomalies, threat indicators, etc.) and configure the XDR to continuously normalize and forward the data to the SIEM for advanced correlation.

☐ Establish data normalization and parsing rules within the SIEM to ensure data integrity.

Conduct integration checks to ensure data integrity and sharing enables effective IR:

☐ Verify and validate data integrity before, during, and after data sharing between the XDR and SIEM solutions.

☐ Verify and validate that SIEM dashboards and reports reflect XDR-generated analytics accurately.

☐ Adjust SIEM correlation rules to incorporate XDR-specific telemetry for enhanced threat detection and response.

Integrate, test, verify, and validate the XDR with C2C, where applicable.

Integrate XDR with C2C:

☐ Identify critical telemetry and compliance data from the XDR that should be shared with the C2C solution (e.g., endpoint compliance status, User/Person Entity (PE)/Non-Person Entity (NPE) behavior anomalies, etc.).

☐ Establish secure integration between the XDR and C2C platforms using appropriate authentication and encryption mechanisms.

☐ Configure automated workflows within C2C to leverage XDR insights for dynamic access decisions.

Verify and validate the XDR and C2C integration:

☐ Verify and validate that C2C uses XDR data effectively for device authentication and approval decisions, and IR.

☐ Ensure continuous monitoring and logging of XDR and C2C integration points.

Summary

This diagram outlines the Activity 2.7.2 (Phase Two) – *Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the implementation of an Extended Detection and Response (XDR) solution to extend monitoring functionality. It presents strategic insights that drive implementation and expected outcomes, including the integration of XDR and Security Information and Event Management (SIEM) solutions to replace Endpoint Detection and Response (EDR) solutions where possible and appropriate.

Table 52: Activity 2.7.2 — Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How are XDR tools procured and implemented to extend monitoring functionality?
2. How are integration points with cross-pillar capabilities identified and prioritized?

STRATEGIC INSIGHTS

- The Component defines and documents policies and procedures for identifying cross-pillar integration points (e.g., endpoint security, network security, Identity Management (IdM), threat intelligence, etc.) and prioritizing them based on risk, ensuring alignment with Enterprise requirements.

- The Component demonstrates compliance by deploying and configuring XDR solutions to replace or extend existing EDR capabilities, integrating with Comply-to-Connect (C2C) systems, Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and other security solutions, and enforcing policy-driven automated responses to threats.

- The Component provides evidence that it has incorporated a strategy for continuous monitoring, data sharing, and enforcement across all pillars, integrating Endpoint Protection Platforms (EPPs), EDR, and XDR to maximize coverage of services, applications, endpoints, and cloud environments, thereby enhancing threat detection, Incident Response (IR), and compliance enforcement.

- The Component verifies and validates that critical data from XDR is transmitted to the SIEM solution, ensuring that basic analytics, events, and alerts are accurately correlated and enriched and that suspicious activities are detected, escalated, and addressed in real-time through integrated SOAR solutions.

- The Component continuously tests, verifies, validates, and audits these integrations (e.g., XDR with C2C, EDR with XDR, XDR with SIEM, etc.), performing functional, security, and User Acceptance Testing (UAT) to confirm that all components align with ZT principles, maintain compliance, and effectively mitigate evolving threats.

EXPECTED OUTCOMES

1. XDR solution is implemented and replaces EDR where possible.
2. Integration points have been identified and prioritized per capability.
3. XDR and SIEM have integrations to gain a comprehensive view of data integration, correlation, analytics, IR, and automation.

Application and Workload Pillar

Capability 3.2 Secure Software Development and Integration

Table 53: Capability 3.2 — Secure Software Development and Integration

<table>
<tr><th colspan="2">DoW Zero Trust Framework</th></tr>
<tr><td colspan="2"><b><i>Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.</i></b></td></tr>
<tr><td><b>Pillar</b></td><td><b>Capability</b></td></tr>
<tr><td>3 - Application and Workload</td><td>3.2 - Secure Software Development and Integration</td></tr>
<tr><td colspan="2"><b>Description</b></td></tr>
<tr><td colspan="2">Foundational software and application security processes and infrastructure are established following Zero Trust principles and best practices. Controls such as code review, runtime protection, secure API gateways, container and serverless security are integrated and automated.</td></tr>
<tr><td colspan="2"><b>Impact to ZT</b></td></tr>
<tr><td colspan="2">Zero Trust security concepts, processes, and capabilities are accepted and integrated across the DevOps toolchain, to include static and dynamic application security testing necessary for the discovery of weaknesses and vulnerabilities during application development.</td></tr>
</table>

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component establishes foundational software security processes, integrating Zero Trust (ZT) principles such as Attribute-Based Access Controls (ABACs), runtime protection, and secure Application Programming Interface (API) gateways into its development infrastructure.
- A Development, Security, and Operations (DevSecOps) toolchain is implemented, enabling development teams to incorporate security controls at every stage of the Software Development Lifecycle (SDLC).
- Static Application Security Testing (SAST) solutions are integrated into the code review process, automatically scanning for vulnerabilities in source code before it is merged into the main branch.
- Dynamic Application Security Testing (DAST) solutions are configured to simulate real-world attack scenarios during pre-production testing, ensuring runtime protection is verified and validated.
- During a security scan, the SAST solutions identifies a critical vulnerability in a new feature being developed for a custom application. The build process is halted automatically, and developers receive detailed remediation guidance.

- Developers fix the vulnerability and resubmit the code, which passes the automated security checks before being approved for deployment.
- The Component integrates container and serverless security solutions into its Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines, ensuring that vulnerabilities in application environments are detected and mitigated before deployment.
- A Runtime Application Self-Protection (RASP) solution is deployed, providing real-time monitoring and protection for applications in production against unanticipated threats.
- The Component conducts regular training for development teams on secure coding practices and updates its security policies to align with emerging threats and technologies.
- By adopting DevSecOps practices and automating security testing and remediation, the Component minimizes vulnerabilities in custom software, ensuring secure integration of third-party components.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Reduced Attack Surface: Layered controls minimize vulnerability to breaches, containing threats before they can spread throughout the component.
- Accelerated Development: Automated security checks catch issues early, reducing costly delays and accelerating delivery timelines.
- Lower Breach Costs: Runtime protections and API controls limit incident scope, minimizing both financial impact and operational downtime.
- Streamlined Compliance: Integrated security controls simplify audit processes and documentation, making regulatory requirements easier to meet.
- Enhanced Reputation: Demonstrable security practices build trust with customers and partners, creating market differentiation.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Application Security Testing Orchestration (ASTO)
- Code Signing
- Containerization and Orchestration Tools
- Dynamic Application Security Testing (DAST)
- Infrastructure as Code (IaC) Configuration Management/Security Monitoring and Auditing
- Static Application Security Testing (SAST)

Activity 3.2.3 Automate Application Security and Code Remediation Part 1

Table 54: Activity 3.2.3 — Automate Application Security and Code Remediation Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
A standardized approach to application security including code remediation is implemented across the DoW Enterprise. Part one (1) of this activity includes the integration of securing API gateways (e.g., API management, WAF, continuous API testing, distributed enforcement—not just perimeter) with applications utilizing API or similar calls. Code reviews are conducted in a methodical approach, and standardized protections for containers and their infrastructure are in place. Additionally, any serverless functions where the third-party manages the infrastructure, such as Platform as a Service (PaaS), utilize adequate serverless security monitoring and response functions. Code reviews, container and serverless security functions are integrated into the CI/CD and/or DevSecOps process, as appropriate.	
Predecessor(s)	**Successor(s)**
2.5.1, 3.2.1, 3.3.3	3.2.4, 3.4.7
Expected Outcomes	
• Enterprise sets standardized approach to application security, including code remediation. • Secure API Gateway is operational, and the majority of API calls are passing through the gateway. • Application Security functions (e.g., code review, container and serverless security) are implemented as part of CI/CD and DevSecOps.	
End State	
Standardize and modernize security infrastructure tools and security integration into application development processes.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 2.5.1 (Phase One) – *Implement Asset, Vulnerability, and Patch Management Tools*, Activity 3.2.1 (Phase One) – *Build Development, Security, and Operations (DevSecOps) Software Factory Part 1*, and Activity 3.3.3 (Phase Two) – *Vulnerability Management Program Part 2* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Resource Authorization Gateways were established in Activity 3.4.1 (Phase One) – *Resource Authorization Part 1*. Consider how these will integrate with this activity's secure Application Programming Interface (API) deployment.
- The Component Vulnerability Management plan was established in Activity 3.3.2 (Phase One) – *Vulnerability Management Program Part 1* and Activity 3.3.3

(Phase Two) – *Vulnerability Management Program Part 2*. Consider how code remediation actions support and potentially leverage the plan.

- The Enterprise has implemented a standardized approach to Application Security (AppSec), including a code remediation policy.
- Development, Security, and Operations (DevSecOps) and/or Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) processes include serverless security functions as appropriate.
    - Additionally, serverless functions where the infrastructure is managed by a third-party, such as Platform as a Service (PaaS), should utilize adequate serverless security monitoring and response functions.
    - Code reviews are conducted methodically, and standardized protections for containers and their infrastructure are in place.
    - Ensure static/dynamic manual or automated code reviews occur during development efforts.
- Activity 3.2.4 (Phase Three) – *Automate Application Security and Code Remediation Part 2* and Activity 3.4.7 (Phase Four) – *REST API Micro-Segments* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 55: Implementation Tasks for Activity 3.2.3 — Automate Application Security and Code Remediation Part 1

Establish governance.
Identify stakeholders that will be responsible for the governance of AppSec: ☐ Create and implement a governance structure that will identify and establish Component application security in accordance with Enterprise requirements. ☐ Consider existing governing bodies within the Component and determine if expanding their roles and responsibilities to cover application security or establishing a new body is optimal.

Obtain and implement the Enterprise standardized approach to AppSec, including code remediation policy.

Obtain and implement a standardized AppSec approach:

☐ Implement a code remediation policy aligned with Enterprise requirements, best business practices, and industry standards that support the Component's operational needs.

☐ Establish and implement a unified security posture to ensure a secure and consistent AppSec development lifecycle process.

☐ Integrate automated security tools to develop a pipeline for early detection and mitigation of vulnerabilities including:

- Static Application Security Testing/Dynamic Application Security Testing (SAST/DAST)
- Software Composition Analysis (SCA)

☐ Develop a formal code remediation policy requiring developers to promptly address identified security flaws and apply security patches in accordance with Enterprise compliance standards.

☐ Implement CI/CD practices integrated with security automation to streamline secure development and deployment processes.

☐ Implement real-time vulnerability remediation and Incident Response (IR) to enhance AppSec compliance maturity across the Enterprise.

☐ Implement policies to foster close collaboration among development, security, and operations teams, supported by ongoing education, training, and awareness initiatives to ensure adherence to Enterprise cybersecurity directives.

☐ Establish the time frame for periodic review/assessment of AppSec requirements.

Utilize adequate serverless security monitoring and response functions for any serverless functions where the third-party manages the infrastructure, such as PaaS.

Ensure adequate security for serverless functions in PaaS environments:

☐ Select and configure security solutions that monitor serverless workloads for vulnerabilities and compliance (e.g., event-driven security monitoring, anomaly detection based on behavioral analysis, serverless runtime protection, etc.).

☐ Enable structured logging and automated monitoring to detect, analyze, and respond to security events in real-time.

☐ Implement Least Privilege access controls (e.g., Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), etc.) to enforce security boundaries and prevent unapproved actions, such as:

- Function-specific identity policies
- Attribute-based approval
- Just-in-Time (JIT) access

☐ Secure API interactions with proper authentication, encryption, and gateway protections (e.g., token-based authentication, request verification, validation, filtering, end-to-end Transport Layer Security (TLS) encryption, etc.).

☐ Deploy real-time security alerts with automated responses to mitigate risks quickly, including:

- Automated rollback on detection of malicious activity
- Dynamic threat scoring
- Security event escalation workflows

☐ Integrate security monitoring into DevSecOps workflows to continuously assess and improve serverless security posture, including:

- Automated security scanning in CI/CD pipelines
- Infrastructure as Code (IaC) security checks
- Real-time compliance verification and validation

Ensure secure API gateways (e.g., API management, Web Application Firewall (WAF), continuous API testing, distributed enforcement, not just perimeter, etc.) are used with applications utilizing API or similar calls.

Ensure API gateways serve as central points of control to manage and secure API traffic effectively:

☐ Implement API gateways with layered security measures, ensuring protection beyond the environment perimeter, such as:

- Namespace isolation
- Endpoint security
- Proxy enforcement

☐ Manage API authentication, approval, and access controls to detect and prevent unapproved access (e.g., token-based authentication, Open Authorization (OAuth), rate limiting, etc.).

☐ Integrate WAF protections and continuous API testing within CI/CD pipelines to detect and mitigate threats.

☐ Apply continuous security testing for API vulnerabilities throughout the development lifecycle.

☐ Enforce distributed API security policies across cloud environments to ensure consistent protection.

☐ Enhance API security with automated threat detection and response mechanisms (e.g., Artificial Intelligence (AI)-driven anomaly detection, automated remediation workflows, cryptographic integrity checks, etc.).

☐ Secure application environments with isolation techniques to prevent unapproved code execution, for example:

- Kernel integrity monitoring
- Secure boot enforcement
- Hypervisor registry protections

☐ Integrate automated security remediation into API workflows to address known vulnerabilities, including:

- Automated Common Vulnerabilities and Exposures (CVE) patching
- Runtime security monitoring
- Integrity verification and validation

Incorporate standardized protections and integrate containers (with associated architecture) and serverless security functions within the CI/CD and/or DevSecOps process as appropriate.

Standardize, protect, and integrate container and serverless security functions:

☐ Secure modern cloud-native applications by implementing protections for computing, storing, and managing containers and serverless functions. This includes digital security hash checksums or equivalent live challenges to detect container image vulnerabilities and serverless function misconfigurations.

☐ Integrate security into the CI/CD pipeline to automate and enforce security checks throughout the development lifecycle, for example:

- Scanning container images for vulnerabilities.
- Ensuring compliance with security policies.
- Monitoring serverless functions for misconfigurations and runtime issues.

☐ Apply industry-standard kernel hardening practices, as a baseline, for evolving security functions within a DevSecOps approach. This ensures security is embedded in the code committed for deployment.

☐ Secure container orchestration platforms by customizing default configurations, adapting open-source security scripts, and enforcing access controls based on Least Privilege and Separation of Duties.

☐ Ensure seamless interaction between Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems while maintaining traceability for API Hypertext Transport Protocol (HTTP) client/server and web-tier operations, including:

- Create, Read, Update, and Delete (CRUD) transaction tracking
- Real-time security event correlation
- Automated threat response workflows

☐ Protect compute, storage, and managed Hyperconverged Infrastructure (HCI) pod container buckets to secure resources during runtime activities, including but not limited to:

- Identity and Access Management (IAM) for containerized workloads
- Encryption of sensitive data at rest and in transit
- Policy-driven resource allocation

☐ Define and enhance serverless architecture with real-time monitoring, Identity and Access Management (IAM), and event-driven security controls.

☐ Customize and re-standardize security configurations by integrating them into automated pipelines. This allows for early detection and remediation of security issues, reducing breach risks through an agile development process.

☐ Enforce authentication of User/Person Entity (PE)/Non-Person Entity (NPE) accounts to prevent file image breach techniques.

Ensure DevSecOps and/or CI/CD processes include serverless security functions as appropriate.

Integrate serverless security into DevSecOps and CI/CD Processes:

☐ Safeguard serverless applications by applying granular security measures across cloud-native and HCI environments, including protections for compute and storage resources.

☐ Implement Information Technology Operations Management (ITOM)-informed security controls to manage software binary configurations, script changes, patch management, and IR. For example:

- Version-controlled Configuration Management (CM)
- Automated integrity checks for software binaries
- Centralized patch and change control

☐ Embed serverless security into DevSecOps and CI/CD pipelines to automate security checks throughout the AppSec development lifecycle.

☐ Automate runtime protection and event logging to capture AI/Machine Learning (ML)-driven threat indicators in the pipeline.

☐ Ensure API integrity in CI/CD workflows by verifying and validating request consistency through challenge-response mechanisms. This serves as an AI-driven early warning system for anomalous behavior.

☐ Apply automated testing at multiple levels to verify and validate serverless security across services and environments. Examples include:

- Unit and integration tests for API endpoints
- Security verification and validation for microservices interactions
- Automated error recovery in containerized deployments

☐ Deploy dynamic CI/CD dashboards to provide real-time visualizations supporting security monitoring and decision-making.

☐ Integrate DevSecOps into CI/CD pipelines to enforce serverless security functions as a core automation step. This ensures effective governance for Information Assurance Vulnerability Management (IAVM), patch management, and IR, such as:

- Dashboard-driven security control verification and validation
- Managed security metrics to measure compliance
- Secure configuration baselines for serverless workloads

Verify and validate AppSec.
Verify and validate code remediation: ☐ Periodically reassess code remediation actions to ensure they comply with Enterprise/Component AppSec requirements. Conduct assessments at the frequency determined by the Component AppSec governing body. **Verify and validate secure API gateways:** ☐ Periodically reassess the efficacy of the secure API gateways to ensure they comply with Enterprise/Component AppSec requirements. Conduct assessments at the frequency determined by the Component AppSec governing body. **Verify and validate serverless assets:** ☐ Periodically reassess serverless assets/resources to ensure they are being managed to align with Enterprise/Component AppSec requirements. Conduct assessments at the frequency determined by the Component AppSec governing body.

Summary

This diagram outlines the Activity 3.2.3 (Phase Two) – *Automate Application Security and Code Remediation Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of a secure Application Programming Interface (API) gateway for applications using API calls and code reviews for container/serverless security functions integrated into the Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipeline. It presents strategic insights that drive implementation and expected outcomes, including the integration of application security functions and a secure API gateway for all API calls.

Table 56: Activity 3.2.3 — Automate Application Security and Code Remediation Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How is a secure API gateway integrated with applications using API calls?
2. How are code reviews and container/serverless security functions integrated into the CI/CD pipeline?

STRATEGIC INSIGHTS

- The Component defines an Application Security (AppSec) governance structure by identifying responsible stakeholders, aligning policies with Enterprise requirements, and implementing standardized code remediation and security policies across the development lifecycle.
- The Component demonstrates security and compliance by integrating automated security tools into the Development, Security, and Operations (DevSecOps) process, securing serverless functions and APIs, and enforcing Role-Based Access Controls (RBACs) and Attribute-Based Access Controls (ABACs) to protect applications from unapproved access.
- The Component provides verifiable enforcement through structured logging, continuous security verification and validation, automated monitoring of serverless functions, API gateways, and containerized workloads, enabling the detection and mitigation of threats in real-time.
- The Component leverages industry standards such as Open Worldwide Application Security Project (OWASP)Top 10, National Institute of Standards and Technology (NIST), and Information Technology Operations Management (ITOM) to secure modern cloud-native applications, automate vulnerability remediation in CI/CD pipelines, and ensure consistent security enforcement across all application environments.
- The Component ensures continuous security by embedding security verification and validation in CI/CD workflows, performing periodic reassessments of AppSec controls, and dynamically updating security policies to address evolving threats and compliance requirements.

✓ EXPECTED OUTCOMES

1. Enterprise sets standardized approach to application security, including code remediation.

2. Secure API Gateway is operational, and the majority of API calls are passing through the gateway.

3. Application Security functions (e.g., code review, container and serverless security) are implemented as part of CI/CD and DevSecOps.

Capability 3.3 Software Risk Management

Table 57: Capability 3.3 — Software Risk Management

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
3 - Application and Workload	3.3 - Software Risk Management
Description	
DoW Components establish software/application risk management program. Foundational controls include Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. Additional controls include Continual validation within the CI/CD pipelines and vulnerability maturation with external sources.	
Impact to ZT	
Code used in DAAS and associated components of the supply chain is secure, vulnerabilities are reduced, and DoW is aware of potential risks.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component deploys a comprehensive software and application risk management program designed to support Zero Trust (ZT) principles by eliminating implicit trust in third-party code, suppliers, and update mechanisms.
- Foundational controls include enforcement of Software Bill of Materials (SBOM) reporting, supplier reputation checks, use of approved repositories, and tightly managed update channels, ensuring all software components are verified before integration.
- As implementation begins, analysts identify multiple applications relying on outdated or untracked third-party libraries acquired outside approved repositories, many with unknown maintainers and no formal risk assessment.
- The Component also discovers gaps in vulnerability tracking, where previously identified issues lack follow-up actions or remain unpatched due to unclear ownership or missing validation within the development pipeline.
- During a scheduled update cycle, a compromised open-source library is introduced into a staging environment through a developer’s manual inclusion of a seemingly minor dependency update.

- Though the update initially bypasses traditional controls, the Component's continuous validation pipeline detects abnormal changes in the dependency's metadata and flags the instance for review, triggering an automated quarantine response.
- The security team uses SBOM and supplier history logs to trace the origin of the suspicious update, cross-referencing threat intelligence feeds to confirm it as part of an ongoing supply chain attack targeting widely used developer tools.
- The Component immediately blocks the element from production environments, initiates remediation across all impacted staging systems, and distributes a verified alternative via its approved update channels, demonstrating containment and rapid response.
- Following the incident, the Component expands supplier risk scoring, mandates validation for all repository interactions, and integrates external vulnerability intelligence feeds directly into its Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines for real-time risk assessment.
- By applying ZT principles of explicit verification, continuous monitoring, and assuming breach, the Component prevented exploitation from a sophisticated supply chain threat and strengthened its ability to detect, respond to, and recover from future software-based attacks.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security: Components can significantly reduce vulnerabilities in their software supply chain by implementing a robust software risk management program.
- Improved Compliance: Adopting these practices ensures alignment with industry standards and regulatory requirements, enhancing overall compliance posture.
- Increased Transparency: The generation of SBOMs provides transparency regarding software components' origin and risk posture, fostering accountability.
- Proactive Risk Management: Continuous verification, validation, and integration of external intelligence sources allow Components to manage and respond to emerging threats proactively.

- Streamlined Development Processes: By defining approved repositories and secure update channels, development teams can work more efficiently while adhering to security best practices.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Container Security Scanning
- Dynamic Application Security Testing (DAST)
- Git Security and Governance
- Software Composition Analysis (SCA)
- Static Application Security Testing (SAST)

Activity 3.3.3 Vulnerability Management Program Part 2

Table 58: Activity 3.3.3 — Vulnerability Management Program Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Processes are established at the DoW Enterprise level for managing the disclosure of vulnerabilities in DoW maintained and operated services, both publicly and privately accessible. Components expand the vulnerability management program to track and manage closed vulnerability repositories such as DIB-VDP, CERT, and others.	
Predecessor(s)	**Successor(s)**
3.3.2	3.2.3
Expected Outcomes	
• Components utilize controlled (e.g., DIB-VDP, CERT) sources for tracking vulnerabilities. • Enterprise sets minimum standards for vulnerability management program accepting external/public disclosures for managed services. • Vulnerability remediation plans are developed and implemented at the Component level.	
End State	
Enterprise-established processes for automated threat sharing from controlled sources are integrated into Component vulnerability management programs.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 3.3.2 (Phase One) – *Vulnerability Management Program Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- The Enterprise has already established a Vulnerability Disclosure Program (VDP) for managing the disclosure of vulnerabilities in maintained/operated services, both publicly and privately accessible.
- The Enterprise has already established processes for automated threat sharing from controlled sources, which are viable for integration into Component Vulnerability Management Programs (VMPs).
- The Enterprise has already established a VMP to unify the process of tracking and managing vulnerabilities. The Enterprise VMP should:
    - Improve the tracking and management of vulnerabilities from closed repositories.

  - Identify closed vulnerability repositories to be integrated (e.g., Common Vulnerabilities and Exposures (CVE), Computer Emergency Response Team (CERT) repositories, etc.).
  - Improve the tracking and management of vulnerabilities from Enterprise-approved repositories.
- Activity 3.2.3 (Phase Two) – *Automate Application Security and Code Remediation Part 1* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 59: Implementation Tasks for Activity 3.3.3 — Vulnerability Management Program Part 2

Adopt the Enterprise VMP.
Review Enterprise policies and standards: ☐ Collaborate with the Enterprise and other Components to obtain relevant directives and updated policy guidance on vulnerability management. ☐ Adopt and participate in the VDP to discover and disseminate the most relevant and updated security bulletins on Indicators of Compromise (IoC) and potential threats. **Perform a VMP gap analysis:** ☐ Identify areas within the Component VMP, from Activity 3.3.2 (Phase One) – *Vulnerability Management Program Part 1*, that should change to align with the Enterprise VMP. ☐ Establish clear objectives for expanding and implementing Enterprise-directed changes. ☐ Clearly define the scope of the program expansion. • Include and highlight the specific repositories to be integrated. • Include the types of vulnerabilities to be managed [18]. **Update the Component VMP to align with the Enterprise VMP:** ☐ Leverage the vulnerability management team, from Activity 3.3.2 (Phase One) – *Vulnerability Management Program Part 1,* to incorporate these changes into the existing vulnerability management solution(s).

Implement automated threat sharing from controlled sources that are viable for integration into vulnerability management programs.

Define objectives and scope:

☐ Establish clear objectives within the VMP for automated threat sharing.

- Include improving threat detection.

☐ Enhance vulnerability management.

☐ Support proactive defense.

- Identify, mitigate, and monitor emerging threats.

☐ Define the scope of the threat-sharing process.

- Include specific sources of threat intel.
- Include types of threats to be shared.
- Include components of the VMP to be integrated.

Identify controlled threat intelligence sources:

☐ Identify controlled sources of threat intel.

- Include Information Sharing and Analysis Centers (ISAC).
- Include approved agencies.
- Include commercial threat intel. providers.

☐ Determine types of threat intelligence data to be integrated.

- Include IoC.
- Include threat actor profiles.
- Include Tactics, Techniques, and Procedures (TTP).
- Include vulnerability information.

Select threat-sharing and integration solutions:

☐ Select solutions for aggregating and sharing threat intelligence.

☐ Utilize solutions to track and manage vulnerabilities throughout their lifecycles.

☐ Utilize solutions to integrate threat intelligence data into the VMP.

☐ Integrate granular access controls and threat protections to enhance situational awareness and mitigate application-specific threats [7].

Develop integration workflows:

☐ Design detailed workflows for integrating threat intelligence data into the VMP.

- Include steps for data collection.
- Include steps for normalization.
- Include steps for ingestion.
- Include steps for correlation.

☐ Identify and categorize applications needed for critical workflows [7]. ☐ Define roles and responsibilities for each step in the integration workflow [7]. ☐ Leverage a high-level federal vulnerability disclosure framework and information flow to ensure clear accountability and coordination [18]. **Implement continuous monitoring and reporting:** ☐ Configure continuous monitoring to track threat intelligence data and its integration into the VMP in real-time. ☐ Implement an automated continuous monitoring solution with integrated threat intelligence and testing to isolate and mitigate any software identified as having a supply chain compromise [7]. ☐ Implement reporting mechanisms to provide real-time visibility into threat intelligence data and its integration into the vulnerability management program.
Obtain an Enterprise-level policy for processes utilized when managing the disclosure of vulnerabilities in maintained/operated services that are both publicly and privately accessible.
Adopt and align policies to manage the disclosure of vulnerabilities: ☐ Review and leverage Enterprise-level policies designed to streamline processes that manage the disclosure of vulnerabilities in public and private-maintained/operated services. ☐ Ensure senior leadership verifies and validates that the VMP's objectives are compatible with the Component's strategic direction and are seamlessly transitioned into the existing processes [18]. ☐ Emphasize leadership support for continuous improvement and include a monitoring and auditing mechanism to report progress to upper management [18]. ☐ Ensure the VDP publishes system-level advisories [18]. ☐ Exploit available vulnerability reports and approved partner's security bulletins to tailor and develop a robust mitigation strategy specific to the Enterprise mission. ☐ Leverage and participate in open channels and legal safe harbors for discovering vulnerabilities to report to appropriate stakeholders [18].

Summary

This diagram outlines the Activity 3.3.3 (Phase Two) – *Vulnerability Management Program Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of vulnerability tracking and a process for accepting external disclosures. It presents strategic insights that drive implementation and expected outcomes, including the controlled tracking of vulnerabilities and the development and implementation of vulnerability management plans.

Table 60: Activity 3.3.3 — Vulnerability Management Program Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How are controlled sources of vulnerabilities, such as Defense Industrial Base (DIB) and Computer Emergency Response Team (CERT), utilized for tracking?

2. How is the Vulnerability Management Program (VMP) process for accepting external/public disclosures established?

STRATEGIC INSIGHTS

• The Component defines a structured approach to adopting the Enterprise VMP, aligning policies, integrating automated threat intelligence sharing, and ensuring comprehensive vulnerability lifecycle management.

• The Component demonstrates security and compliance by conducting a gap analysis against Enterprise VMP standards, incorporating controlled threat intelligence sources, and leveraging automation to detect, mitigate, and monitor emerging threats.

• The Component provides verifiable enforcement through real-time monitoring, reporting, and integration of threat intelligence into vulnerability workflows, ensuring proactive defense and continuous situational awareness.

• The Component leverages Enterprise-supported Threat Intelligence Platforms (TIPs), government and commercial sources, and structured Vulnerability Disclosure Programs (VDPs) to enhance security coordination and rapid response.

• The Component ensures ongoing security by integrating leadership oversight, continuous monitoring, and policy-driven vulnerability disclosure processes, reinforcing strategic alignment with Enterprise directives and mission priorities.

EXPECTED OUTCOMES

1. Components utilize controlled (e.g., DIB, VDP, CERT) sources for tracking vulnerabilities.

2. Enterprise sets minimum standards for VMP accepting external/public disclosures for managed services.

3. Vulnerability remediation plans are developed and implemented at the Component level.

Activity 3.3.4 Continual Validation

Table 61: Activity 3.3.4 — Continual Validation

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components implement a continuous validation approach for application development, where security is constantly assessed throughout the development, integration, and deployment. Validation includes security principles when planning and designing, security testing (to include code reviews), incident response, and SIEM alerting/logging. These principles are integrated and continuously executed with the CI/CD pipeline. Applications developed outside of CI/CD process should still adhere to continuous validation in an ad hoc/manual manner.	
Predecessor(s)	**Successor(s)**
None	None
Expected Outcomes	
• Continual validation tools are implemented and applied to code in the CI/CD pipeline. • Updated applications are only deployed in a live and/or production environment with a continuous validation approach. • Applications developed outside of the CI/CD pipeline are still validated in an ad hoc/manual manner, as established in the continuous validation approach.	
End State	
Establish a continuous validation process and tooling that are seamlessly integrated with application planning and design, security testing, incident response, and SIEM alerting/logging.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Consider completing Activity 3.2.1 (Phase One) – *Build Development, Security, and Operations (DevSecOps) Software Factory Part 1* and Activity 3.2.2 (Phase One) – *Build Development, Security, and Operations (DevSecOps) Software Factory Part 2,* prior to this activity, as this activity relies on the Component Development, Security, and Operations (DevSecOps) policy.
- Consider completing Activity 3.3.2 (Phase One) – *Vulnerability Management Program Part 1* and Activity 3.3.3 (Phase Two) – *Vulnerability Management Program Part 2* prior to this activity, as this activity relies on the Component Vulnerability Management Program (VMP).

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 62: Implementation Tasks for Activity 3.3.4 — Continual Validation

Review Enterprise guidance on DevSecOps adoption.
Review and align to Enterprise best practices: ☐ Review Enterprise DevSecOps requirements. ☐ Leverage the Component DevSecOps Policy, from Activity 3.2.1 (Phase One) – *Build Development, Security, and Operations (DevSecOps) Software Factory Part 1.* **Review objectives and scope:** ☐ Leverage existing Enterprise/Component policies and procedures to establish clear objectives for continuous verification and validation within the Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipeline. ☐ Verify and validate that the scope spans the entire lifecycle, including the design, development, distribution, deployment, acquisition, maintenance, and destruction of the system [19]. ☐ Define the scope of the verification and validation processes, including the types of verification and validation to be performed. ☐ Extend the existing Component DevSecOps policy to include the new continuous verification and validation requirements. **Leverage existing Component VMP, from Activity 3.3.2 (Phase One) – *Vulnerability Management Program Part 1* and Activity 3.3.3 (Phase Two) – *Vulnerability Management Program Part 2:*** ☐ Identify the environments/systems that are the most vulnerable and will cause the most significant environmental impact if compromised [19]. ☐ Leverage industry standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Supply Chain Risk Management (C-SCRM) publication, to guide the Component on how to identify, assess, select, and implement risk management processes and mitigating controls [20].
Integrate security into the CI/CD pipeline.
Deploy and enforce security requirements into the CI/CD pipeline: ☐ Leverage automation processes, from Activity 3.2.1 (Phase One) – *Build Development, Security, and Operations (DevSecOps) Software Factory Part 1* and Activity 3.2.2 (Phase One) – *Build Development, Security, and Operations (DevSecOps) Software Factory Part 2*, to enforce security verification and validation throughout the various Phases of the CI/CD pipeline [7]. • Include code commit.

- Include build.
- Include testing.
- Include staging.
- Include deployment.

Integrate the planning phase:

☐ Conduct threat modeling to identify potential security threats and vulnerabilities [19].

☐ Establish security policies and guidelines that should be considered throughout the development cycle.

Integrate coding phase:

☐ Use static code analysis solutions to identify security vulnerabilities and code quality issues early in the development process.

☐ Conduct regular code reviews with a focus on security by vetting developed source code and common libraries through DevSecOps development practices [7].

☐ Use peer reviews and automated solutions to ensure that security best practices are followed.

Integrate the build phase:

☐ Use dependency management solutions to identify and address vulnerabilities in third-party libraries and dependencies.

☐ Automate the build process to ensure consistency and repeatability.

☐ Integrate security testing into the build process.

Integrate the testing phase:

☐ Implement automated testing for security, functionality, and performance.

☐ Perform regular vulnerability scans to identify security weaknesses.

☐ Conduct penetration testing to identify, exploit, and remediate vulnerabilities and weaknesses proactively [7].

Integrate the deployment phase:

☐ Use Infrastructure as Code (IaC) solutions to automate the provisioning and configuration of the infrastructure.

☐ Implement Configuration Management (CM) to ensure that systems are securely configured.

☐ Configure security monitoring to detect and respond to security incidents.

Leverage Cyber Threat Intelligence (CTI) and vulnerability management for verification and validation compliance.

Review existing vulnerability management programs:

☐ Leverage technical capabilities, from Activity 3.3.2 (Phase One) – *Vulnerability Management Program Part 1* and Activity 3.3.3 (Phase Two) – *Vulnerability Management Program Part 2,* to maintain software Supply Chain Risk Management (SCRM) compliance with existing VMPs.

☐ Augment software for C-SCRM solutions with threat intelligence to flag any software identified as having a supply chain compromise or an increased risk profile, facilitating additional testing, verification, and validation [7].

☐ Monitor for the most common risks identified through best practices [19].

- Include insertion of counterfeits.
- Include unapproved production.
- Include tampering and theft.
- Include insertion of malicious software and hardware.

☐ Monitor factors from outside vendors that allow for low-cost, interoperability, rapid innovation, and multiple product features, among others, which increase the risk of a supply chain compromise, leading to risks to the User/Person Entity (PE) [19].

Review the existing acquisition and supply chain risk assessment lifecycle:

☐ Ensure effective C-SCRM procedures are implemented, enforced, and routinely audited Enterprise-wide to evaluate third-parties' software vulnerabilities, risk exposure, and involve each tier [7].

- Include Component.
- Include mission/business processes.
- Include information systems.

☐ Manage cybersecurity risks in the supply chain by ensuring the integrity, security, quality/resilience of the supply chain [19].

Document and approve, exceptions.

Manage exceptions:

☐ Applications/services that do not support CI/CD continuous verification and validation:

- Identified
- Documented
- Approved/Rejected

☐ The Enterprise and/or Component determines risks.

- Consider how risks can be mitigated, such as through upgrades, replacements, or decommissioning of applications/services that cannot be migrated.

☐ Approval is granted when justification for the exception outweighs the risks to the Enterprise/Component.

☐ Approval is periodically reassessed.

Automate continuous verification, validation, and Incident Response (IR).

Enforce verification and validation reviews:

☐ Develop and mandate an application security checklist as part of the broader code review process.

☐ Develop and implement an IR plan to quickly address security incidents.

☐ Leverage application feedback loops to feed and automate security testing and vulnerability patching.

Implement continuous monitoring and reporting:

☐ Implement reporting mechanisms to provide visibility into verification, validation results, and compliance status.

☐ Leverage both manual code reviews and automated static analysis to create opportunities for continuous review of application security vulnerabilities.

Enable continuous monitoring and testing.

Monitor and audit:

☐ Leverage existing CTI feeds, Common Vulnerability Exposures (CVE), and other Indicators of Compromise (IoC) to monitor the threat landscape and update the vulnerability management processes to effectively account for emerging threats and unknown vulnerabilities.

☐ Perform regular security audits to ensure compliance with security policies and regulatory requirements.

Test, verify, and validate:

☐ Conduct functional testing to ensure that the verification and validation workflows work as expected and effectively identify issues.

☐ Perform security testing to identify and mitigate any vulnerabilities in the verification and validation workflows [19].

☐ Monitor the verification and validation workflows to ensure their effectiveness and performance.

☐ Verify and validate that activity/events are ingested and actioned by Component Visibility and Analytics and/or Automation and Orchestration solutions.

Summary

This diagram outlines the Activity 3.3.4 (Phase Two) – *Continual Validation* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of validation tools to continuously verify and validate applications and codes. It presents strategic insights that drive implementation and expected outcomes, including the implementation and application of continual validation tools.

Table 63: Activity 3.3.4 — Continual Validation - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How are updated applications deployed in a live and/or production environment?
2. How are applications marked for retirement and transition decommissioned?
3. How are continual validation tools implemented and applied to code in the Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipeline?
4. How is code requiring continuous validation identified and validation criteria established?

STRATEGIC INSIGHTS

- The Component defines and aligns its Development, Security, and Operations (DevSecOps) adoption strategy with Enterprise guidance by extending existing policies to incorporate continual validation across the full system lifecycle, integrating security into each CI/CD Pipeline Phase from design and development through deployment and decommissioning.
- The Component demonstrates security-by-design practices by embedding threat modeling, code analysis, and vulnerability scanning throughout the Software Development Lifecycle (SDLC), verifying and validating that automated processes enforce security requirements at every CI/CD Phase, including build, test, and deployment.
- The Component ensures operational and supply chain integrity by integrating threat intelligence, Cybersecurity Supply Chain Risk Management (C-SCRM) standards, and vulnerability management practices into verification and validation workflows, thereby continuously monitoring, testing, and mitigating known risks, such as counterfeit insertion or tampering.
- The Component leverages existing vulnerability management programs and DevSecOps automation infrastructure to drive compliance, streamline Incident Response (IR), and create feedback loops that enhance vulnerability patching and threat detection in real-time.
- The Component ensures sustained and auditable security verification and validation through continuous monitoring, exception management, and routine assessments, enabling visibility into compliance status, enforcing policy, and verifying and validating the ingestion and response of security telemetry via analytics and orchestration platforms.

EXPECTED OUTCOMES

1. Continual validation tools are implemented and applied to code in the CI/CD pipeline.
2. Updated applications are only deployed in a live and/or production environment with a continuous validation approach.
3. Applications developed outside of the CI/CD pipeline are still validated in an ad hoc/manual manner, as established in the continuous validation approach.

Capability 3.4 Resource Authorization and Integration

Table 64: Capability 3.4 — Resource Authorization and Integration

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
3 - Application and Workload	3.4 - Resource Authorization and Integration
Description	
DoW establishes a standardized resource authorization gateway for authorizations via the CI/CD pipelines in a risk approach that reviews the User, Device and Data security posture. Authorizations utilize a programmatic (e.g., Software-Defined) approach in a live/production environment. Attributes are enriched utilizing other pillar activities and the API and Authorization gateway. Approved enterprise APIs are micro-segmented using authorizations.	
Impact to ZT	
Resource authorization enables the ability for limited access to those resources and in a programmatic way in later stages. This improves the ability to remove access when it is not needed.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component establishes a standardized resource authorization gateway, integrated with its Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines, to assess and approve resource access based on a risk-based review of User/Person Entity (PE)/Non-Person Entity (NPE) and data security postures.
- A programmatic approach to resource authorization is implemented, leveraging Software-Defined Controls (SDCs) to automate access management in both staging and live production environments.
- Attributes from other Zero Trust (ZT) pillars, such as device compliance and user authentication data, are enriched and incorporated into the authorization process, providing a more comprehensive risk assessment.
- The Component micro-segments its enterprise Application Programming Interfaces (APIs) using the authorization gateway, ensuring access to each API is limited to approved users and devices based on their roles and attributes.
- During deployment, an automated authorization check detects a CI/CD pipeline attempting to access a sensitive resource with insufficient privileges, blocking the request and generating an alert.

- Developers are notified of the issue, review the gateway logs, and update the pipeline's authorization attributes to align with the approved resource access policy.
- Real-time monitoring identifies an inactive User/PE account still associated with resource permissions. The gateway automatically revokes access, reducing the risk of insider threats.
- A micro-segmented API is flagged for anomalous behavior due to an unusual access pattern, triggering an investigation that reveals an attempted attack on the API.
- The Component conducts regular audits to verify and validate that resource authorization rules align with evolving security policies and adjust micro-segmentation boundaries as needed.
- By standardizing resource authorization, integrating it with CI/CD pipelines, and enriching attributes for risk-based decisions, the Component ensures secure, granular access control while maintaining flexibility.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security: Components can significantly reduce the risk of unapproved access and potential data breaches by implementing a standardized resource authorization gateway.
- Automated Access Management: The integration with CI/CD pipelines allows for automated decision-making, reducing the manual overhead associated with access management and improving operational efficiency.
- Improved Compliance: Regular audits and real-time monitoring ensure that access controls remain aligned with evolving security policies, aiding in compliance with regulatory requirements.
- Risk Mitigation: The capability enables Components to identify and respond to potential threats quickly, such as revoking access for inactive accounts or detecting anomalous behavior.
- Flexibility and Scalability: The programmatic approach to resource approval allows Components to adapt to changing business needs while maintaining secure access controls across various environments.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Attribute-Based Access Control (ABAC)
- Identity, Credential, and Access Management (ICAM)
- Policy Enforcement Points (PEPs)
- Role-Based Access Control (RBAC)
- Security Orchestration, Automation, and Response (SOAR)

Activity 3.4.2 Resource Authorization Part 2

Table 65: Activity 3.4.2 — Resource Authorization Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Policy enforcements and decisions are used for all possible applications and services. Applications unable to utilize gateways are either decommissioned or accepted using a risk-based methodical approach. Authorizations are further integrated with the CI/CD pipeline for automated decision making.	
Predecessor(s)	**Successor(s)**
3.4.1	None
Expected Outcomes	
• Policy enforcement is utilized for all applications and services. • Applications and services are identified that are accepted or decommissioned.	
End State	
Resource authorization gateways leveraging PDP and PEP integrated with identity and access management systems are implemented for all applications. Authorization policies are embedded within DevSecOps and the CI/CD pipeline to ensure automated, continuous, and secure access control decisions.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 3.4.1 (Phase One) – *Resource Authorization Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Applications that cannot be migrated or mitigated to a level acceptable by the Enterprise/Component are decommissioned.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 66: Implementation Tasks for Activity 3.4.2 — Resource Authorization Part 2

Implement approved resource authorization gateways for all potential application and service resources.
Implement authorization gateways on all applications and services: ☐ Leverage the application/service migration roadmap/implementation plans, from Activity 3.4.1 (Phase One) – *Resource Authorization Part 1*. ☐ Adopt, adapt, test, and integrate: • Conduct testing, verification, and validation of proposed changes in the Development, Security, and Operations (DevSecOps) virtualized landscape environment, focusing on applicable areas. • Continuously refine proposed changes based on Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) testing results to ensure they meet performance, security, and functional requirements [21]. ☐ Migrate all applications and services: • Following Component stakeholder approval, deploy applications and services with approved resources (e.g., disk, memory, Central Processing Unit (CPU), Graphics Processing Unit (GPU) generic , Tensor Processing Unit (TPU), media, bandwidth, ports, protocols, Process Identifiers (PIDs), etc.) that have successfully passed testing to the appropriate CI/CD environment (e.g., prototype, live, or production).
Manage applications and services that cannot leverage the resource authorization gateways.
Manage exceptions: ☐ Applications/services that cannot be migrated are: • Identified • Documented • Approved/Rejected ☐ The Enterprise and/or Component determines risks. • Consider how risks can be mitigated, such as upgrades, replacements, or decommissioning applications/services that cannot be migrated. ☐ Approval is granted where the justification for the exception outweighs the risks to the Enterprise/Component. ☐ Approval is periodically reassessed. ☐ Applications that cannot be migrated or mitigated to a level acceptable by the Enterprise/Component should be decommissioned.

Complete verification and validation.
Verify and validate migrated applications/services: ☐ Ensure applications/services continue to function as expected/required. ☐ Ensure that applications/services cannot be accessed through methods not leveraging authorization gateways. **Verify and validate authorization gateways:** ☐ Ensure authorization gateways are configured in accordance with the Enterprise requirements. ☐ Ensure configured authorization gateways provide the necessary functionality to support the Component’s operational requirements.
Conduct periodic assessments.
☐ Periodically verify and validate the applications/services and authorization gateways to ensure they meet Enterprise/Component requirements.

Summary

This diagram outlines the Activity 3.4.2 (Phase Two) – *Resource Authorization Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of resource approval integration for Development, Security, and Operations (DevSecOps), and Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) automated functions. It presents strategic insights that drive implementation and expected outcomes, including policy enforcement for all applications.

Table 67: Activity 3.4.2 — Resource Authorization Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the resource authorization gateway utilized for all applications? 2. How is resource authorization integrated with DevSecOps and CI/CD for automated functions?

STRATEGIC INSIGHTS
• The Component defines and documents a structured process for implementing approved resource authorization gateways across all applications and services, aligning with established migration roadmaps and Enterprise security standards to control access to computing resources, such as memory, Central Processing Unit (CPU), disk, and network protocols. • The Component demonstrates compliance by conducting rigorous testing and integration of resource authorization gateways within a virtualized DevSecOps landscape, verifying and validating performance, security, and functionality through CI/CD pipelines before migrating services to prototype, live, or production environments. • The Component provides verified and validated evidence of operational integrity by ensuring that migrated applications and services utilize approved resources exclusively and are inaccessible via unapproved methods, maintaining strict adherence to Enterprise-defined configuration and functionality requirements. • The Component leverages exception management procedures to identify, document, and assess applications or services that cannot integrate with authorization gateways, supporting decisions to approve, mitigate, or decommission based on periodic risk assessments and operational impact. • The Component ensures ongoing alignment with Enterprise mandates by performing periodic assessments of both applications/services, as well as their associated authorization gateways, verifying and validating continued compliance, secure operation, and readiness to adapt to evolving performance or policy requirements.

✓ EXPECTED OUTCOMES

1. Policy enforcement is utilized for all applications and services.
2. Applications and services are identified that are accepted or decommissioned.

Activity 3.4.4 Software-Defined Compute (SDC) Resource Authorization Part 2

Table 68: Activity 3.4.4 — Software-Defined Compute (SDC) Resource Authorization Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Components use approved and validated code/binaries via the Software Bill of Materials (SBOM) process to ensure that applications that can and cannot support the approach are identified. Applications which can support modern Software-Based Configuration and Management (SBCM) approaches are identified and transitioned. Applications that support SBCM have been transitioned to a production/live environment and are in normal operations. Applications which cannot support SBCM are identified and allowed through exception using a risk-based approach.	
Predecessor(s)	**Successor(s)**
1.8.1, 3.4.3, 5.3.1	None
Expected Outcomes	
• Updated applications are deployed in a live and/or production environment. • Applications that were marked for retirement and transition have a decommissioned indicator. • Applications unable to be updated to an approved binaries/code are marked for retirement and transition plans are created. • Identified applications are updated to use approved binaries/code.	
End State	
Components operationalize validated code and binaries through use in the production environment.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 1.8.1 (Phase One) – *Single Authentication*, Activity 3.4.3 (Phase One) – *Software-Defined Compute* (*SDC) Resource Authorization Part 1,* and Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Consider completing Activity 3.1.1 (Discovery) – *Application and Code Identification* prior to this activity, to access the Master Application Inventory.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 69: Implementation Tasks for Activity 3.4.4 — Software-Defined Compute (SDC) Resource Authorization Part 2

Develop Component Software Bill of Materials (SBOMs).
Develop SBOM: ☐ Extend the Component Master Application Inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification*, to include at least the following data points in accordance with SBOM documentation: • Name • Version • Supplier/Vendor • Type (e.g., open-source, third-party, proprietary, etc.) • Unique Identifiers/Hash
Test the application Software-Defined Computing (SDC) migration.
Test migration: ☐ Leverage the list of compatible software, from Activity 3.4.3 (Phase One) – *Software-Defined Compute* (*SDC) Resource Authorization Part 1*. ☐ Migrate compatible software within a controlled/test environment. ☐ Verify and validate post-migration application functionality.
Migrate application functionality to platforms that support SDC.
Application migration: ☐ Enable SDC on SDC-supported platforms. ☐ Transition application functionality to applications that support SDC.
Manage SDC exceptions.
Manage exceptions: ☐ Applications/services that cannot be migrated are: • Identified • Documented • Approved/Rejected

☐ Risks are determined by the Enterprise and/or Component. • Consider how risks can be mitigated, such as upgrades, replacements, or decommissioning of applications/services that cannot be migrated. ☐ Approval is granted when justification for the exception outweighs the risks to the Enterprise/Component. ☐ Approval is periodically reassessed.
Conduct periodic assessments.
☐ Periodically reassess Component SDC policy/procedures to ensure they align with Enterprise requirements.

Summary

This diagram outlines the Activity 3.4.4 (Phase Two) – *Software-Defined Compute (SDC) Resource Authorization Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the enforcement of Software-Defined Compute (SDC) standards. It presents strategic insights that drive implementation and expected outcomes, including updating applications to adhere to SDC standards and retiring applications that cannot be updated to the new standards.

Table 70: Activity 3.4.4 — Software-Defined Compute (SDC) Resource Authorization Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How do authorization policies incorporate confidence levels in making authorization decisions? 2. How are confidence levels for attributes defined?

STRATEGIC INSIGHTS
• The Component defines and maintains a comprehensive Software Bill of Materials (SBOM) by extending the Master Application Inventory to include critical metadata—such as name, version, supplier, type, and unique identifiers—in alignment with Enterprise SBOM documentation standards. • The Component demonstrates the secure and functional migration of compatible software by leveraging pre-approved software lists, conducting controlled testing in designated environments, and verifying and validating application behavior post-migration to ensure SDC compatibility. • The Component provides evidence of successful migration and operational readiness by transitioning application functionality to platforms that support SDC, ensuring continuity, security, and alignment with Enterprise performance expectations. • The Component leverages an exception management framework to document, assess, and justify applications or services that cannot be migrated, enabling risk-informed decisions such as upgrades, replacements, or decommissioning, with periodic reassessments to uphold security and functionality. • The Component ensures sustained compliance through regular reassessment of SDC-related policies and procedures, maintaining alignment with evolving Enterprise standards, platform capabilities, and risk management strategies.

EXPECTED OUTCOMES

1. Updated applications are deployed in a live and/or production environment.
2. Applications that were marked for retirement and transition have a decommissioned indicator.
3. Applications unable to be updated to an approved binaries/code are marked for retirement and transition plans are created.
4. Identified applications are updated to use approved binaries/code.

Data Pillar

Capability 4.2 DoW Enterprise Data Governance

Table 71: Capability 4.2 — DoW Enterprise Data Governance

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
4 - Data	4.2 - DoW Enterprise Data Governance
Description	
DoW establishes enterprise data labeling/tagging and DAAS access control/sharing policies (e.g., SDS policy) that are enforceable. Developed enterprise standards ensure an appropriate level of interoperability between DoW Organizations.	
Impact to ZT	
Decision rights and accountability framework ensure appropriate behavior in the valuation, creation, consumption, and control of data and analytics.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component defines data tagging and labeling standards in accordance with Enterprise requirements, ensuring all data assets are classified by sensitivity, purpose, and access requirements.
- Data access control policies are established, including Software-Defined Storage (SDS) policies, to enforce granular access permissions at the field level across all Data, Applications, Assets, and Services (DAAS) systems.
- Interoperability standards are developed to enable seamless data sharing between components while maintaining consistent enforcement of tagging and access control policies.
- Automated solutions are deployed to tag and label data assets upon creation, ensuring compliance with Enterprise standards without manual intervention.
- A sensitive dataset is improperly labeled as public, triggering an automated alert during a routine validation process.
- The tagging is corrected, and access controls are updated to restrict the dataset to authorized Users/Person Entities (PEs)/Non-Person Entities (NPEs) only, preventing potential unauthorized exposure.

- During an inter-agency data-sharing initiative, the interoperability standards are used to securely share tagged data, ensuring consistent enforcement of access controls across participating Components.
- The Component conducts periodic audits of tagged datasets to identify discrepancies and ensure tagging and access control policies remain effective.
- Anomalous access patterns to sensitive datasets are detected, prompting the security team to investigate and confirm adherence to access control policies.
- By establishing Enterprise data governance policies and interoperability standards grounded in Zero Trust (ZT), the Component ensures decision rights, accountability, and proper data management and safeguarding data assets.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Data Security: Components can significantly reduce the risk of unapproved access to sensitive data by implementing robust tagging and access control policies.
- Seamless Collaboration: Standardized data-sharing policies enable secure information exchange between different teams without compromising security or creating unnecessary friction.
- Reduced Complexity: Unified Enterprise standards eliminate the need for multiple custom solutions, lowering maintenance costs and simplifying the overall security architecture.
- Enhanced Compliance Verification: Automated enforcement of data access controls provides clear audit trails and evidence of regulatory adherence across the entire data lifecycle.
- Cross-Functional Interoperability: Components operating under consistent standards can efficiently integrate systems and processes, accelerating mission capabilities while maintaining appropriate security boundaries.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Data Lifecycle Management
- Data Standardization
- Governance, Risk, and Compliance (GRC)
- Interoperability and Data Exchange Frameworks
- Policy Decision Points (PDPs)
- Policy Enforcement Points (PEPs)

Activity 4.2.3 Develop Software-Defined Storage (SDS) Policy

Table 72: Activity 4.2.3 — Develop Software-Defined Storage (SDS) Policy

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Enterprise will work with Components to determine if Software-Defined Storage (SDS) is in use. Components develop policy and standards based on industry best practices, and evaluate current data storage strategy and technology for implementation of SDS. Components assess their existing data storage strategies and technologies to determine the suitability for implementing SDS. If deemed appropriate, the identified storage technologies are considered for SDS implementation.	
Predecessor(s)	**Successor(s)**
None	4.7.1, 4.7.4, 4.7.6
Expected Outcomes	
• Enterprise defines and refines minimum attribution requirements for SDS to support Zero Trust enablement. • Components assess their existing data storage for SDS implementation considerations.	
End State	
Ensure holistic approach for SDS security alignment within Components to strengthen access and availability, data protection, and adherence to best practices.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- The Enterprise does not have an established Software-Defined Storage (SDS) policy or standards.
- Consider completing Activity 3.1.1 (Discovery) – *Application and Code Identification* and Activity 4.1.1 (Discovery) – *Data Analysis* prior to this activity, as the Component Data Catalog and Component Master Application Inventory will provide insights into existing data storage solutions within the environment.
- Activity 4.7.1 (Phase Two) – *Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1*, Activity 4.7.4 (Phase Two) – *Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1*, and Activity 4.7.6 (Phase Three) – *Implement Software-Defined Storage (SDS) Tool and/or Integrate with Data Rights Management (DRM) Tool Part 1* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 73: Implementation Tasks for Activity 4.2.3 — Develop Software-Defined Storage (SDS) Policy

Coordinate with the Enterprise to develop SDS policies and standards based on technology, industry best practices, and Component-evaluated current data storage strategies.
Establish SDS standards and policy: ☐ Identify stakeholders to establish a unified SDS framework. ☐ Identify existing SDS and/or the potential need for SDS based on Component operational demands. ☐ Review industry best practices, technology trends, third-party recommendations, and vendor accreditations to tailor a Component SDS strategy. ☐ Collaborate with the Enterprise to define the overarching SDS standards and policy.
Develop Component policies and standards for implementing SDS, leveraging an integrated approach for SDS security alignment to strengthen access and availability, data protection, and best practice standards.
Define and establish SDS standards: ☐ Define clear goals, objectives, and scope for the Component SDS policy based on mission-operational objectives and requirements. ☐ Align the developed SDS strategy and policy with existing Enterprise SDS policy, mandates, and standards for compliance. ☐ Define multiple storage tiers based on performance, cost, data sensitivity, and compliance requirements. Establish storage criteria that are aligned with the overall Enterprise data governance. ☐ Establish data residency rules as applicable and mandated by federal, Enterprise, and local laws and regulations. Determine relevant factors such as application requirements, data categorization, geographic location, and operational constraints. **Develop applicable use cases for SDS:** ☐ Engage with various stakeholders across all Components to develop the Component SDS solution. Prioritize and characterize sensitive applications and workloads to gain security insights. ☐ Analyze all relevant workloads and applications to better understand performance requirements, capacity demands, and data access traffic patterns. ☐ Establish SDS policy for data replication, snapshots, and backups to ensure data high availability and disaster recovery compliance. Review and enforce recovery point and time objectives as a baseline to meet business continuity requirements.

☐ Integrate Access Control security policies with the SDS strategy to restrict access to storage resources based on data categorization, User/Person Entity (PE)/Non-Person Entity (NPE) roles and attributes, and environment conditions. Key features to consider:

- Data encryption
- Scalability and performance
- Capacity management
- Quality of Service
- Hard Disk Drive (HDD) and Solid State Drive (SSD) storage types

Assess existing data storage strategies and technologies to determine the suitability for implementing SDS.

Review data storage strategies:

☐ Leverage the Component SDS policy and standards.

☐ Identify all data storage solutions within the Component environment. Leverage the:

- Component Master Data Inventory, from Activity 4.1.1 (Discovery) – *Data Analysis*
- Component Master Application Inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification*

☐ Review benchmarks and key performance metrics to verify and validate the expected outcomes associated with the data storage policy.

☐ Review, verify, and validate the effectiveness of data backup strategy, data availability and reliability, disaster recovery capabilities, data retention requirements, privacy compliance, and overall data access-control security.

Execute SDS strategy, policies, technologies, and practices.

Publish a comprehensive SDS strategy:

☐ Engage stakeholders for SDS policy adoption. Monitor and enable feedback for business leaders on operational impact.

☐ Incorporate the developed SDS policy with a broader data governance strategy and data security. Key features to consider:

- Service Level Agreements (SLAs)
- Data growth forecast
- Key performance indicators
- Data Access Control Lists (ACLs)

Summary

This diagram outlines the Activity 4.2.3 (Phase Two) – *Develop Software-Defined Storage (SDS) Policy* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development and implementation of Software-Defined Storage (SDS) policy and standards. It presents strategic insights that drive implementation and expected outcomes, including the minimum attribution required for SDS.

Table 74: Activity 4.2.3 — Develop Software-Defined Storage (SDS) Policy - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. The Component defines SDS policies and standards by identifying stakeholders, evaluating existing storage strategies, and aligning with industry best practices and Enterprise mandates. 2. The Component demonstrates compliance by developing SDS policies that enhance data security, access control, and governance, incorporating encryption, scalability, and disaster recovery requirements. 3. The Component provides evidence by assessing current storage solutions, verifying and validating performance metrics, and ensuring SDS policies meet data availability, retention, and compliance requirements. 4. The Component leverages SDS integration with access control policies, workload analysis, and data categorization to optimize performance, cost efficiency, and security. 5. The Component ensures ongoing SDS effectiveness through continuous monitoring, stakeholder engagement, and strategic alignment with broader data governance and security frameworks.

STRATEGIC INSIGHTS
• How is the SDS policy and standards developed and implemented?

EXPECTED OUTCOMES
1. Enterprise defines and refines minimum attribution requirements for SDS to support ZT enablement. 2. Components assess their existing data storage for SDS implementation considerations.

Capability 4.3 Data Labeling and Tagging

Table 75: Capability 4.3 — Data Labeling and Tagging

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
4 - Data	4.3 - Data Labeling and Tagging
Description	
Data owners label and tag data in compliance with DoW Enterprise governance on labeling/tagging policy. As Phases advance automation is used to meet scaling demands and provide better accuracy.	
Impact to ZT	
Establishing machine enforceable data access controls, risk assessment, and situational awareness require consistently and correctly labeled and tagged data.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component implements data tagging and classification solutions to help data owners label and tag datasets in compliance with Enterprise governance policies.
- Initial efforts focus on manual tagging, with data owners applying labels for sensitivity, classification, and access requirements to small-scale datasets.
- During a data audit, a mislabeled dataset is discovered, leading to improperly configured access controls. The dataset is re-tagged to ensure compliance and proper enforcement of security policies.
- The Component establishes workflows to verify and validate manually tagged data, ensuring consistency and accuracy across departments.
- As data volume grows, automation solutions are deployed to scale tagging efforts and reduce human error, leveraging Artificial Intelligence (AI) and pattern recognition to classify data accurately.
- Automated solutions detect an untagged dataset uploaded to a cloud repository, apply the appropriate tags based on content, and configure access controls automatically.
- A periodic review of tagging practices highlights discrepancies between manual and automated tags, prompting updates to improve automation accuracy and minimize conflicts.
- Automated tagging solutions integrate with risk assessment systems, enabling real-time situational awareness by identifying and prioritizing high-risk datasets.

- Consistently labeled and tagged data facilitates machine-enforceable access controls, preventing unauthorized Users/Person Entities (PEs) from accessing sensitive datasets and ensuring compliance with Enterprise policies, aligning with the Zero Trust (ZT) focus on strict access controls and verification.
- By transitioning from manual to automated data tagging, the Component achieves scalability, accuracy, and consistent enforcement of data governance policies.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Precision Protection: Components apply exactly the right security controls to each data asset based on accurate classification, eliminating both over-protection and under-protection scenarios.
- Improved Data Security: Consistent and accurate tagging facilitates machine-enforceable access controls, protecting sensitive datasets from unapproved access.
- Scalability: Automating tagging processes allows Components to manage larger volumes of data efficiently without compromising accuracy.
- Reduced Human Error: Automated solutions minimize the risk of mislabeling and ensure consistent tag application across datasets.
- Increased Situational Awareness: Integration with risk assessment systems enables real-time identification and prioritization of high-risk datasets, improving Component responsiveness.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Content Inspection solutions
- Data Classification, Discovery, Labeling solutions
- Data Standardization
- Data Tagging and Protection
- Metadata Management Systems

Activity 4.3.2 Manual Data Tagging Part 1

Table 76: Activity 4.3.2 — Manual Data Tagging Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Components map DoW Enterprise ZT tags to local labeling to meet minimum essential metadata criteria for compliance.	
Predecessor(s)	**Successor(s)**
4.1.1, 4.2.1	4.3.3, 4.5.3, 4.6.2
Expected Outcomes	
• Data tagging is conducted at the Component-level with basic attributes.	
End State	
A standardized data tagging and labeling solution is in place, ensuring all Components comply with ZT principles. Metadata criteria are consistently applied, enhancing data security and access control across the Enterprise.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 4.1.1 (Discovery) – *Data Analysis* and Activity 4.2.1 (Phase One) – *Define Data Tagging Standards* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Consider completing Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools* prior to this activity, to leverage data tagging solutions and conventions.
- While the title of this Activity is “Manual Data Tagging”, the Component should make all attempts at performing this activity in an automated manner. The implementation table below is written in support of automation.
- Activity 4.3.3 (Phase Three) – *Manual Data Tagging Part 2,* Activity 4.5.3 (Phase Two) – *Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1,* and Activity 4.6.2 (Phase Two) – *Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 77: Implementation Tasks for Activity 4.3.2 — Manual Data Tagging Part 1

Leverage Component data tagging solution(s).
Create comprehensive mapping relationships: ☐ Leverage the Component-defined data tagging solution(s), from Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools*. ☐ Develop a formal tag mapping document that explicitly correlates each Enterprise ZT tag to corresponding Component-level tags, documenting rationale for each mapping decision. ☐ Identify and document gap areas where Enterprise tags have no Component equivalent, with clear remediation plans, including timeframes, for developing missing tags. ☐ Establish a tiered prioritization schema for implementing tag mappings, focusing first on data that directly supports security decisions in the ZT environment. ☐ Create visual mapping matrices for different data categories showing Enterprise-to-Component tag relationships that can be referenced by both technical teams and data owners. ☐ Develop tag coverage metrics that measure both the breadth (percentage of data tagged) and depth (completeness of applied tags) across Component data assets. **Develop a tagging implementation plan:** ☐ Develop a Component-level tagging implementation roadmap with clear phases tied to data sensitivity and criticality, ensuring the most sensitive data receives tags first. ☐ Create tag application templates for common data types that streamline consistent tag application and reduce manual decision-making. ☐ Implement tag inheritance rules for derivative data to maintain proper classification as data is transformed within the workflows. ☐ Document tag override procedures for exceptional cases where standard tag mappings may not apply, with appropriate approval chains.
Implement data tagging.
Streamline the data tagging process: ☐ Leverage tagging conventions, defined in the key access store, from Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools*. ☐ Apply data tagging to data objects through a phased approach, prioritizing data in accordance with data tagging standards, from Activity 4.2.1 (Phase One) – *Define Data Tagging Standards.*

Enable practical tag integration across boundaries:

☐ Develop automated tag translation services that can convert between Enterprise and Component tag schemas when data crosses organizational boundaries.

☐ Implement tag persistence policies, ensuring that original Enterprise tags remain associated with data even when Component-specific tags are applied.

☐ Create tag validation checkpoints at key data exchange points to verify that mapped tags maintain semantic equivalence and security properties.

☐ Establish data lineage tracking to maintain the history of tag translations as data moves between Enterprise and Component environments.

Integrate tagging with the environment:

☐ Configure Data Loss Prevention (DLP) and Data Rights Management (DRM) solutions to recognize and enforce both Enterprise and Component-level tag schemas.

☐ Develop security policy mapping documents showing precisely how different tags trigger specific security controls and restrictions.

☐ Implement real-time tag verification capabilities at security enforcement points to prevent tag manipulation or removal.

☐ Create integration reference architectures demonstrating how tags flow between tagging systems, Security Information and Event Management (SIEM) solutions, and security control mechanisms.

☐ Develop operational use cases that demonstrate how mapped tags enhance access decisions in alignment with ZT principles. Ensure data tags can be ingested by SIEM, Security Orchestration, Automation, and Response (SOAR), and other tools/solutions supporting the Visibility and Analytics and/or Automation and Orchestration pillars.

Verify and validate data tagging implementation.

Review, verify, and validate expected outcomes:

☐ Verify and validate data tags/metadata criteria are consistently applied to data objects in accordance with Component policy and standards.

☐ Routinely conduct audits to ensure data tagging remains effective and compliant with applicable laws and regulations. Enable exception handling to drive future lessons learned sharing.

☐ Review and report all the data tagging inconsistencies to help improve processes and procedures. Enable feedback loop mechanisms to verify and validate tag accuracy and consistency over time.

Summary

This diagram outlines the Activity 4.3.2 (Phase Two) – *Manual Data Tagging Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of manual data tagging for basic attributes at the Enterprise level. It presents strategic insights that drive implementation and expected outcomes, including manual data tagging at the Enterprise level with basic attributes.

Table 78: Activity 4.3.2 — Manual Data Tagging Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How has manual data tagging been initiated at the Enterprise level with basic attributes?

STRATEGIC INSIGHTS
• The Component defines a data tagging solution that leverages the Key Access Store and established tagging standards to classify and manage data effectively. • The Component demonstrates compliance by implementing tagging conventions, applying tags through a phased approach, and ensuring alignment with security and regulatory requirements. • The Component provides evidence through verification and validation testing, routine audits, and exception handling to maintain consistency, accuracy, and compliance. • The Component leverages data tagging to enhance security by integrating with Data Loss Prevention (DLP), Data Rights Management (DRM), Security Information and Event Management (SIEM), and Security Orchestration, Automation, and Response (SOAR) solutions, improving access control and metadata management. • The Component ensures ongoing effectiveness through continuous monitoring, training, and phased testing to refine tagging accuracy and minimize operational disruptions.

EXPECTED OUTCOMES
1. Data tagging is conducted at the Component-level with basic attributes.

Capability 4.4 Data Monitoring and Sensing

Table 79: Capability 4.4 — Data Monitoring and Sensing

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
4 - Data	4.4 - Data Monitoring and Sensing
Description	
Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets. Data Loss Prevention (DLP) and Data Rights Management (DRM) enforcement point analysis is conducted to determine where tooling will be deployed. Data outside of DLP and DRM scope such as File Shares and Databases is actively monitored for anomalous and malicious activity using alternative tooling.	
Impact to ZT	
Data in all states are detectable and observable.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component deploys solutions to capture active metadata, including information on access, sharing, transformation, and usage of all data assets, ensuring data observability in all states.
- Data Loss Prevention (DLP) solutions are implemented at key enforcement points, supporting Zero Trust (ZT) by continuously validating User/Person Entity (PE) actions and flagging potentially unauthorized behaviors.
- Data Rights Management (DRM) solutions are configured to track how data is accessed, shared, and transformed within approved applications and workflows.
- An analysis of enforcement point logs reveals gaps in coverage, prompting the deployment of additional DLP and DRM solutions at critical locations, such as file servers and endpoints.
- Alternative monitoring solutions are implemented to observe activity on data sources outside DLP and DRM scope, such as file shares and databases, to detect anomalous or malicious behavior.
- Anomalous activity is detected on a shared drive, where a User/PE unexpectedly downloads large volumes of sensitive files during non-working hours.
- Alerts generated by the file activity monitoring tool prompt the Security Operations Center (SOC) to investigate the User/PE's behavior, confirming the action as unauthorized.

- The User/PE’s access is revoked, and the anomalous activity logs are forwarded for further analysis, leading to policy updates to prevent similar incidents.
- Database activity monitoring solutions identify unusual query patterns that attempt to access restricted tables, prompting an automated response to block the queries and notify the database administrator.
- By capturing active metadata and monitoring data activities comprehensively across all systems, the Component ensures that data is detectable and observable, preventing unauthorized access.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Data Security: By implementing DLP and DRM solutions, Components can significantly reduce the risk of data breaches and unapproved access to sensitive information.
- Improved Compliance: The ability to monitor and manage data usage helps Components comply with regulatory requirements related to data protection and privacy.
- Increased Visibility: Active metadata capture provides Components with comprehensive visibility into how data is accessed and used, enabling better decision-making.
- Evidence-Based Governance: Comprehensive monitoring creates a complete audit trail of data access and transformation, helping components demonstrate compliance and exercise greater control over their information assets.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Anomaly Detection
- Behavioral Analytics solutions
- Data Loss Prevention (DLP)
- Digital Rights Management (DRM)
- File Integrity Monitoring (FIM)
- Monitoring and Analytics solutions

Activity 4.4.4 File Activity Monitoring Part 2

Table 80: Activity 4.4.4 — File Activity Monitoring Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components utilize File Monitoring tools to monitor all regulatory protected data (e.g., CUI, PII, PHI, etc.) in applications, services, and repositories. Extended integration is used to send data to appropriate inter/intra-pillar solutions such as Data Loss Prevention, Data Rights Management/Protection and User & Entity Behavior Analytics.	
Predecessor(s)	**Successor(s)**
4.4.3	1.2.3, 4.4.5, 4.4.6
Expected Outcomes	
• Data and files of all regulated designations are identified and actively monitored. • Establish and manage business rules to consume regulated designations and manage outcomes.	
End State	
Components extend regulation to data files and integrations to strengthen data loss prevention, and prevent malicious attacks from spreading.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 4.4.3 (Phase One) – *File Activity Monitoring Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Activity 1.2.3 (Phase Three) – *Rule-Based Dynamic Access Part 2*, Activity 4.4.5 (Phase Three) – *Database Activity Monitoring*, and Activity 4.4.6 (Phase Four) – *Comprehensive Data Activity Monitoring* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 81: Implementation Tasks for Activity 4.4.4 — File Activity Monitoring Part 2

Extend the File Activity Monitoring (FAM) solution.
Leverage the existing Component FAM solution: ☐ Extend the existing Component FAM solution, from Activity 4.4.3 (Phase One) – *File Activity Monitoring Part 1*, to include regulatory protected data (e.g., Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), Protected Health Information (PHI), etc.). ☐ Create a prioritized implementation schedule for adding monitoring coverage to different categories of regulated data, considering factors such as: • Data volume and distribution across repositories. • Regulatory compliance deadlines. • Technical complexity of detection requirements. • Integration dependencies with other security systems. ☐ Develop specialized detection patterns for each regulatory data type (CUI, PII, PHI) that weren't covered in the critical data monitoring implemented in Activity 4.4.3 (Phase One) – *File Activity Monitoring Part 1*, such as: • Content-based patterns specific to regulatory frameworks. • Contextual access patterns unique to regulated data. • Organizational usage patterns requiring special monitoring attention. ☐ Create configuration templates for extending existing FAM deployments to include regulated data types, documenting: • Detection rule modifications needed for regulatory compliance. • Monitoring depth adjustments required for different data types. • Alert thresholds specific to regulatory requirements. • Reporting parameters necessary for compliance documentation. ☐ Establish supplemental monitoring policies, specifically addressing regulatory requirements not covered in critical data monitoring, with detailed specifications for: • Minimum monitoring coverage requirements by regulation. • Evidence collection standards for regulatory audits. • Integration points with compliance management systems. • Regulatory-specific retention policies for monitoring data.

Implement the Component-defined FAM solution on regulatory data.

Extend FAM solution:

☐ Implement the extended FAM coverage/capabilities in a phased approach, prioritizing data based on:

- Risk-based implementation tiers: Create a multi-tier implementation framework categorizing regulated data by risk level, with highest-risk data categories (e.g., classified CUI, PHI with large volume, etc.) implemented first.
- Regulatory deadline alignment: Synchronize the implementation schedule with compliance deadlines and audit cycles to ensure timely coverage of regulated information subject to upcoming reviews.
- Data exposure surface: Prioritize monitoring for regulated data with the broadest access patterns or largest user base to maximize initial security impact.
- Technical complexity considerations: Develop a complexity assessment matrix to identify which regulatory data types require specialized detection mechanisms beyond standard pattern matching.

Verify and validate FAM solution integration.

Verify and validate:

☐ Ensure the FAM solution continues to meet the needs of the Component.

☐ Confirm that the operational impact of the FAM solution is acceptable to the Component.

☐ Continuously reassess the functionality of the FAM tool to ensure comprehensive coverage and compliance with Enterprise/Component requirements.

- The Enterprise/Component must define frequency, but the application of digital policy requires consistent oversight.

☐ Conduct regular gap analysis against regulatory requirements, integration effectiveness, and coverage.

Summary

This diagram outlines the Activity 4.4.4 (Phase Two) – *File Activity Monitoring Part 2* of the Department of War Zero Trust (ZT) Framework, focusing on monitoring of regulatory-protected data types using File Activity Monitoring (FAM) solutions. It presents strategic insights that drive implementation and expected outcomes, including the establishment and management of business rules to consume critical data designations and manage outcomes.

Table 82: Activity 4.4.4 — File Activity Monitoring Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are regulatory protected data types monitored using FAM tools?

STRATEGIC INSIGHTS
• The Component defines an extended FAM solution to include regulatory-protected data, such as Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), and Protected Health Information (PHI). • The Component demonstrates compliance by ensuring the extended FAM solution aligns with Enterprise security and regulatory requirements. • The Component provides evidence through verification and validation testing, confirming functionality, security, and operational impact. • The Component leverages periodic reassessments to maintain comprehensive coverage and ensure continued compliance. • The Component ensures ongoing alignment with evolving Enterprise mandates through continuous monitoring and policy updates.

EXPECTED OUTCOMES
1. Data and files of all regulated designations are identified and actively monitored. 2. Establish and manage business rules to consume regulated designations and manage outcomes.

Capability 4.5 Data Encryption and Rights Management

Table 83: Capability 4.5 — Data Encryption and Rights Management

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
4 - Data	4.5 - Data Encryption and Rights Management
Description	
DoW Components establish and implement a strategy for encrypting data at rest and in transit using Data Rights Management (DRM) tooling. The DRM solution utilizes data tags to determine protection and lastly integrates with ML and AI to automate protection.	
Impact to ZT	
Encrypting data in all states reduces the risk of unauthorized data access and improves data security.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component develops a comprehensive strategy for encrypting data at rest and in transit, using encryption standards that meet Enterprise compliance requirements.
- Data Rights Management (DRM) solutions are deployed to enforce encryption policies and manage access rights based on data tags and classifications.
- During deployment, data owners tag sensitive datasets, such as those containing Personally Identifiable Information (PII), ensuring prioritization for encryption and access control.
- The DRM solutions are configured to dynamically apply encryption to tagged datasets, enforcing Zero Trust (ZT) by ensuring only authorized entities can access sensitive data in storage or transit.
- A policy mandates that all sensitive data transmitted across the network must use secure protocols, such as Transport Layer Security (TLS), and be encrypted in transit to protect against interception.
- A data transfer request from an unencrypted channel is flagged by the DRM solution and automatically blocked, triggering an alert for the data owner.
- The Component integrates DRM solutions with Machine Learning (ML) and Artificial Intelligence (AI) systems to automate the identification and tagging of sensitive data, further enhancing protection.
- ML algorithms detect an untagged sensitive dataset stored in a shared location, apply the appropriate tags, and enforce encryption automatically.

- Analytics generated by the DRM solution highlight access patterns and potential risks, enabling data owners to adjust tagging and encryption policies to address emerging threats.
- By encrypting data in all states and leveraging DRM solutions integrated with data tags, ML, and AI, the Component reduces the risk of unauthorized access and enhances data security.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Persistent Protection: Components maintain security controls that follow sensitive data throughout its lifecycle, ensuring it remains protected regardless of location or transmission state.
- Intelligent Safeguarding: Using tag-based protection decisions, Components automatically apply appropriate encryption levels, eliminating manual classification burdens while preventing over- and under-protection.
- Adaptive Security Posture: AI-powered DRM solutions learn from data usage patterns, allowing components to continuously refine their protection strategies without constant human intervention.
- Breach Impact Reduction: Even if perimeter defenses fail, components with comprehensive encryption experience significantly reduced damage, as encrypted data remains unusable to unapproved parties.
- Simplified Compliance: Components demonstrate regulatory adherence more easily when sensitive data is systematically encrypted based on classification tags, streamlining audit processes and reducing compliance costs.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Data Encryption
- Digital Rights Management (DRM)
- Encryption and Key Management solutions
- Runtime Application Self-Protection (RASP)
- Trusted Execution Environment (TEE)

Activity 4.5.2 Implement Data Rights Management (DRM) and Protection Tools Part 2

Table 84: Activity 4.5.2 — Implement Data Rights Management (DRM) and Protection Tools Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DRM and protection coverage is expanded to cover all required data objects. Protection mechanisms are automatically managed to meet best practices (e.g., FIPS). Extended data protection attributes are implemented based on the environment classification.	
Predecessor(s)	**Successor(s)**
4.5.1	None
Expected Outcomes	
• DRM and protection tools are enabled for all required repositories.	
End State	
No data object bypasses the compliance requirement.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 4.5.1 (Phase One) – *Implement Data Rights Management (DRM) and Protection Tools Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Presumption: A data lifecycle management process exists that includes data cleansing and data quality management.
- Implement contextual access policies for repositories: Assess device health and enable an Attribute-Based Access Control (ABAC) policy.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 85: Implementation Tasks for Activity 4.5.2 — Implement Data Rights Management (DRM) and Protection Tools Part 2

Review the Enterprise/Component Data Rights Management (DRM) policy guidelines.
Leverage existing DRM policies: ☐ Review Enterprise and Component guidelines on DRM policies and data taxonomy and ensure compliance adherence. **Review data protection mechanisms:** ☐ Develop and enforce data asset protection to help safeguard sensitive data across the entire Component environment. Leverage Policy Decision Points (PDPs), Policy Enforcement Points (PEPs), and Access Control policies to perform critical asset mapping.
Extend the DRM and data protection solution.
Extend the Component DRM solution: ☐ Leverage the Component implemented DRM solution, from Activity 4.5.1 (Phase One) – *Implement Data Rights Management (DRM) and Protection Tools Part 1*. **Asset alignment and license management:** ☐ Maintain audit trails of all data assets activities based on predefined rules and actions. Implement and secure system logs to enable forensic analysis. Deploy a centralized licensing server to manage, verify, and validate licenses. ☐ DRM Policy Enforcement: Implement mechanisms to enforce DRM policies, restricting access, usage, and distribution based on license terms. ☐ Secure Key Management: Implement a robust system for generating, storing, and distributing decryption keys, ensuring only authorized users and devices can access protected content. ☐ License Validation: Deploy a centralized licensing server to manage, verify, and validate licenses, preventing unauthorized access and usage. ☐ Audit Trails (DRM-Specific): Maintain audit trails of all DRM-related activities, including license requests, key access, and policy violations. ☐ Real-time Monitoring (DRM-Specific): Monitor DRM system activity for suspicious behavior and potential policy breaches. • License Expiration & Revocation: Implement automated license expiration and revocation mechanisms. **Implement the DRM solution:** ☐ Deploy the DRM solution on all data and test extensively to verify and validate that the expected outcomes were achieved. • Adhere to Enterprise/Component DRM policies. • Leverage to vendor recommendations. • Test system integration and compatibility. ☐ Develop automation playbooks for policy enforcement.

Encrypt data:

☐ Implement and deploy a strong and vetted Key Management System (KMS) to restrict access to encryption keys only to approved identities.

☐ Enable encryption on all data located on servers, databases, cloud storage, data repositories, and endpoint devices; leverage updated security protocols (e.g., Hypertext Transfer Protocol Secure (HTTPS), Transport Layer Security (TLS), etc.) to protect data either at rest or in transit.

- Key management
- Encryption keys
- End-to-end encryption
- Watermarking

Implement protection mechanisms:

☐ Apply fine-grained permissions on all data assets and enable DRM protection-based Access Control to only allow approved Users/Person Entities (PEs)/Non-Person Entities (NPEs). Ensure the following solutions are implemented:

- Multi-Factor Authentication (MFA)
- ABAC
- Data Loss Prevention (DLP)

Verify and validate DRM protection compliance on all data objects.

Ensure data is encrypted:

☐ Verify and validate all data objects are encrypted in a manner that meets Enterprise/Component data steward requirements.

Test operational impacts of DRM implementation:

☐ Test to ensure Component operations are acceptable/sustainable under DRM implementation on high-risk data objects.

☐ Establish a performance baseline after the DRM solution is implemented.

☐ Verify and validate activity/events are ingested and actioned by Component Visibility and Analytics and/or Automation and Orchestration solutions.

Integrate and automate DRM solutions into existing data security protection solutions.

Enforce User and Entity Behavior Analytics (UEBA) and continuous monitoring:

☐ Implement DRM solutions compatible with continuous monitoring, leveraging UEBA to automatically enforce DRM policies, trigger alerts, and DLP for suspicious activity.

Automate content encryption:

☐ Leverage Application Programming Interfaces (APIs) and plugins for seamless application integration between DRM solutions and Content Management Systems (CMSs) to enable automatic encryption and packaging of content at creation and upon collection.

Automate audit logging and alerting: ☐ Build and implement workflows and playbooks to automatically alert and trigger data security, mitigating countermeasures such as DLP, license monitoring, and API-driven data rights access management.
Verify and validate that continuous DRM policy testing and data activity monitoring are in place.
Track and monitor data usage: ☐ Continuously verify and validate access log monitoring to track content and approved device management. ☐ Verify and validate activity/events are ingested and actioned by Component Visibility and Analytics and/or Automation and Orchestration solutions.

Summary

This diagram outlines the Activity 4.5.2 (Phase Two) – *Implement Data Rights Management (DRM) and Protection Tools Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of Data Rights Management (DRM) and Protection solution expansion to all data repositories deemed within scope. It presents strategic insights that drive implementation and expected outcomes, including enabling DRM and protection solutions for all required repositories.

Table 86: Activity 4.5.2 — Implement Data Rights Management (DRM) and Protection Tools Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the DRM and Protection solution coverage expanded to all in-scope data repositories?

STRATEGIC INSIGHTS
• The Component leverages Enterprise and Component DRM policies to ensure alignment with compliance requirements, data taxonomy standards, and protection mechanisms. • The Component demonstrates compliance improving upon existing DRM solutions, enforcing access controls, and maintaining audit trails for license management and forensic analysis across all data objects. • The Component provides evidence through encryption implementation, testing operational impacts, and verifying and validating DRM enforcement across all data objects. • The Component leverages automation by integrating DRM with continuous monitoring, User and Entity Behavior Analytics (UEBA), and security solutions to detect and mitigate unapproved access. • The Component ensures ongoing compliance through automated audit logging, real-time tracking of data usage, and continuous policy verification and validation, safeguarding sensitive assets.

EXPECTED OUTCOMES
1. DRM and protection tools are enabled for all required repositories.

Activity 4.5.3 Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1

Table 87: Activity 4.5.3 — Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Enterprise provides a standard for data access control and protections. Components establish data rights management (DRM) and protection solutions that are used with data tags defined by the data producer. High-risk data objects are identified and monitored with protection, detection, and response actions enabled. Data at rest is encrypted and protected (e.g., hardware/object/disk encryption, access control) in repositories.	
Predecessor(s)	**Successor(s)**
4.3.2	4.5.4
Expected Outcomes	
• Components DRM utilizes Attribute-Based Access Control standards set by Enterprise. • Based on data tags, data is encrypted at rest.	
End State	
Protections are applied and appropriate access is enforced for each data object.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 4.3.2 (Phase Two) – *Manual Data Tagging Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Consider completing Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools* prior to this activity, as the Global Key Access Store solution will be needed in this activity.
- Consider completing Activity 4.4.2 (Discovery) – *Data Rights Management (DRM) Enforcement Point Logging and Analysis* prior to this activity, to leverage the Component data access policy.
- Consider completing Activity 4.2.1 (Phase One) – *Define Data Tagging Standards* and Activity 4.3.2 (Phase Two) – *Manual Data Tagging Part 1* prior to this activity, to leverage existing data tagging standards.

- Consider completing Activity 4.5.2 (Phase Two) – *Implement Data Rights Management (DRM) and Protection Tools Part 2* prior to this activity, in order to encrypt the data at rest.
- The Enterprise standards for data access control and protection have been established and provided.
- High-risk data objects refer to sensitive data (e.g., Personally Identifiable Information (PII), financial data, intellectual property, etc.) that require heightened security measures to prevent breaches.
- To achieve interoperability, each participating Component should standardize a Data Rights Management (DRM) schema, such as Intelligence Community-Trusted Data Format (IC-TDF) or Zero Trust Data Format (ZTDF), to ensure the end products for all Components can decrypt shared files.
- DRM solutions should use an unencrypted wrapper so data cataloging services can scan and categorize files appropriately.
- Activity 4.5.4 (Phase Three) – *Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 2* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 88: Implementation Tasks for Activity 4.5.3 — Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1

Review Enterprise-approved standards on data access controls.
Review Enterprise standards for data Access Control and protection: ☐ Leverage the Global Key Access Store as the centralized tag repository/single source of truth for all tags, from Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools*. ☐ Leverage the Component data access policy, from Activity 4.4.2 (Discovery) – *Data Rights Management (DRM) Enforcement Point Logging and Analysis*. ☐ Review and update the Component data access policy to align with existing Enterprise data Access Control standards and industry best practices, as applicable.

☐ Review, verify, and validate legal and regulatory compliance requirements as well as mission-specific security data protection mechanisms.

☐ Review, verify, and validate broader alignment with Enterprise data governance, Attribute-Based Access Control (ABAC) policies, and digital modernization strategy.

☐ Ensure that the existing DRM solution complies with relevant data protection regulations (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), etc.).

Review and enforce Enterprise data tagging standards and taxonomy.

Leverage existing data tagging standards, from Activity 4.2.1 (Phase One) – *Define Data Tagging Standards* and Activity 4.3.2 (Phase Two) – *Manual Data Tagging Part 1,* to enhance DRM policy enforcement:

☐ Configure DRM solutions to automatically enforce policies based on data tags.

☐ Ensure DRM protects the data at rest, in transit, and during usage based on the data tag's restrictions and ABAC policies.

☐ Collaborate with data owners to enforce standardized data tagging schemes (e.g., classification, license rights, metadata, etc.).

Review and refine ABAC's existing policies:

☐ Enforce granular Access Control and time-based access restrictions tied to data asset tags (e.g., view, edit, copy, save, print, etc.).

☐ Leverage existing ABAC policies to effectively tailor DRM enforcement and compliance while improving the User/Person Entity (PE) experience.

Optimize contextual DRM policy enforcement through metadata:

☐ Configure DRM solutions and tools to align with contextual enforcement based on User/PE attributes and data asset characteristics.

☐ Enforce data tagging integration into data protection mechanisms for DRM compliance and loss prevention.

Integrate Incident Response (IR) and analytics for data access violations into DRM policies.

Develop playbooks to automate tag-based DRM policies:

☐ Leverage the existing digital asset tags with relevant metadata information to create a policy engine with a predefined set of rules capable of translating data tag information into DRM actions.

☐ Review and enforce compliance requirements and acceptance criteria for the protection of copyrighted data and sensitive material.

Enforce data encryption at rest, from Activity 4.5.2 (Phase Two) – *Implement Data Rights Management (DRM) and Protection Tools Part 2:*

☐ Leverage existing Enterprise standards to enforce encryption across entire repositories or specific files, as appropriate.

☐ Use hardware-based encryption for physical assets (e.g., disk encryption, secure storage hardware, etc.).

Enforce secure key management:

☐ Use a centralized Key Management System (KMS) to generate, store, and rotate encryption keys.

☐ Enforce policies for key lifecycle management (e.g., expiration, revocation, etc.).

☐ Protect keys with Hardware Security Modules (HSMs) or secure cloud KMS solutions.

Leverage analytics to detect DRM policy violations through data usage tracking:

☐ Combine User and Entity Behavior Analytics (UEBA) and Security Information and Event Management (SIEM) solutions to monitor digital assets, User/PE behavior, and access patterns to identify potential violations of copyrighted data usage.

☐ Enforce IR orchestration into the data security protection scheme to proactively act on anomaly detection, such as sudden spikes in downloads, restricted geolocation, or compromised identities.

☐ Enforce Representational State Transfer Application Programming Interface (REST API) integration for DRM enforcement of cloud-based data assets and repositories.

Enable data-driven DRM testing, verification, and validation.

Enforce continuous monitoring and auditing:

☐ Enforce real-time alerting for critical DRM violations on sensitive data assets.

☐ Enforce regular monitoring and auditing of adherence to DRM-approved policies.

Enforce data-driven DRM compliance:

☐ Enforce a comprehensive log collection of the DRM system, including access requests, license usage, and policy enforcement points.

☐ Centralize and aggregate all tags and metadata information relevant to digital data assets to develop a system baseline for an approved and acceptable use policy.

Enforce logging and real-time alerting:

☐ Enable logging for repository access and data operations.

☐ Use real-time monitoring tools to detect unapproved or suspicious activity.

☐ Regularly review access logs and audit reports for anomalies.

Summary

This diagram outlines the Activity 4.5.3 (Phase Two) – *Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1* component of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on basic data tag integration and monitoring with Data Rights Management (DRM). It presents strategic insights that drive implementation and expected outcomes, including the utilization of Attribute-Based Access Control (ABAC) standards set by the Enterprise for DRM and data encryption at rest.

Table 89: Activity 4.5.3 — Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are basic data tags integrated with DRM and monitored repositories expanded?

STRATEGIC INSIGHTS
• The Component defines and aligns its data access control strategy with Enterprise-approved standards by updating its data access policies to incorporate legal, regulatory, and mission-specific requirements while leveraging centralized tagging from the Global Key Access Store and existing DRM enforcement policies. • The Component demonstrates adequate data protection by configuring DRM solutions to enforce ABAC policies using standardized data tags, ensuring that data is safeguarded at rest, in transit, and during use based on classification, metadata, and user context. • The Component provides robust evidence of compliance and governance by integrating real-time monitoring, logging, and auditing into its DRM enforcement framework, including continuous tracking of access requests, license usage, and policy violations to detect anomalies and unapproved activity. • The Component leverages centralized key management systems and hardware-based encryption to enforce secure data protection, automating key lifecycle processes and ensuring alignment with Enterprise encryption policies and compliance requirements for sensitive or classified data assets. • The Component ensures resilient and adaptive data access controls through ongoing verification, validation, and analytics, employing Security Information and Event Management (SIEM) and User and Entity Behavior Analytics (UEBA) solutions to detect threats, automate Incident Response (IR) playbooks, and maintain a dynamic baseline of acceptable data usage across cloud and on-premise environments.

EXPECTED OUTCOMES
1. Components DRM utilizes ABAC standards set by Enterprise. 2. Based on data tags, data is encrypted at rest.

Capability 4.6 Data Loss Prevention (DLP)

Table 90: Capability 4.6 — Data Loss Prevention (DLP)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
4 - Data	4.6 - Data Loss Prevention (DLP)
Description	
DoW Components utilize the identified enforcement points to deploy approved DLP tools and integrate tagged data attributes with DLP. Initially, the DLP solution is put into a "monitor-only" mode to limit business impact, and later, using analytics, is put into a "prevent" mode. Extended data tag attributes are used to feed the DLP solution and lastly integrate with ML and AI.	
Impact to ZT	
Data breaches and data exfiltration transmissions are detected and mitigated.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component identifies key enforcement points for Data Loss Prevention (DLP) such as endpoints, email servers, and cloud storage systems, based on the flow of sensitive data.
- Approved DLP solutions are deployed at the identified enforcement points, configured to monitor all data transmissions, and detect potential breaches or exfiltration attempts.
- Initially, the DLP solution is put into a "monitor-only" mode to observe data flows, collect analytics, and minimize disruptions to business operations.
- Tagged data attributes, such as sensitivity level and access restrictions, are integrated with the DLP solutions to enhance detection accuracy and align with Enterprise/Component-defined policies.
- Analytics from the monitor-only phase highlight frequent attempts to share sensitive data over unauthorized channels, prompting the Component to refine DLP rules and policies.
- The DLP solution is transitioned to a "prevent" mode, aligning with Zero Trust (ZT) principles by actively blocking unauthorized data transfers and requiring verification before allowing access.
- An attempt to email an unencrypted sensitive document to an external recipient is detected and blocked by the DLP solution, triggering an alert and notifying the sender of policy violations.

- Machine Learning (ML) and Artificial Intelligence (AI) capabilities are integrated with the DLP solution, enabling it to detect patterns indicative of insider threats or sophisticated data exfiltration techniques.
- The ML-enhanced DLP solution identifies anomalous behavior, such as a User/Person Entity (PE) attempting to upload large amounts of tagged data to a personal cloud account and prevents the action automatically.
- By deploying DLP solutions at enforcement points, integrating tagged data attributes, and leveraging ML and AI, the Component successfully detects and mitigates data breaches and exfiltration attempts.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Data-Driven Protection: By using analytics to transition from monitoring to prevention, Components implement controls based on actual usage patterns rather than theoretical risks, minimizing false positives.
- Enhanced Detection Precision: Extended data tag attributes provide the DLP solution with richer contextual information, allowing components to distinguish between legitimate and suspicious data access with greater accuracy.
- Continuous Improvement: AI-powered systems learn from ongoing data interactions, enabling components to automatically refine policies as usage patterns and threat landscapes evolve.
- Data Visibility: Analytics provide insights into data flows, helping Components understand where sensitive data resides and how it is used.
- Proactive Threat Detection: Integration of AI and ML allows for identifying anomalous behavior, enabling quicker responses to potential insider threats or data exfiltration attempts.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Data Loss Prevention (DLP)
- Data Tagging and Protection
- File Integrity Monitoring (FIM)
- Incident Response (IR)
- Policy Enforcement Points (PEPs)

Activity 4.6.2 Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1

Table 91: Activity 4.6.2 — Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Data Loss Prevention (DLP) solution is updated from monitor only mode to prevention mode. Zero Trust tagging incorporates indicators to facilitate DLP through cooperative cyber enforcement.	
Predecessor(s)	**Successor(s)**
4.3.2	4.6.3
Expected Outcomes	
• Enterprise sets the minimum standards for indicators that support cyber enforcement. • Components technology is enabled for enforcement.	
End State	
Support prevention of data loss through development of data attributes that support cyber enforcement of data loss.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 4.3.2 (Phase Two) – *Manual Data Tagging Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis*, Activity 3.1.1 (Discovery) – *Application and Code Identification*, and Activity 4.1.1 (Discovery) – *Data Analysis* prior to this activity, to assist with the verification and validation of DLP enforcement.
- Consider completing Activity 4.6.1 (Phase One) – *Implement Enforcement Points* prior to this activity, as this activity transitions the previously established Data Loss Prevention (DLP) solution from monitor mode to enforcement mode.
- Consider completing Activity 7.1.2 (Phase One) – *Log Parsing* prior to this activity, to ensure adherence to established logging standards.
- Presumption: The Enterprise has set minimum standards for indicators that support cyber enforcement.

- Transition the DLP solution from a passive monitoring role to an active prevention mode to proactively block unapproved data access and/or exfiltration.
- Activity 4.6.3 (Phase Three) – *Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 2* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 92: Implementation Tasks for Activity 4.6.2 — Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1

Identify Enterprise cyber enforcement indicators.
Enterprise cyber enforcement indicators: ☐ Coordinate with the Enterprise to identify the minimum indicator standards supporting DLP. • Review Enterprise security directives and privacy requirements. • Map indicator standards to Component's data environment. • Identify any gaps between Component capabilities and Enterprise standards. • Develop indicator implementation roadmap aligned with Enterprise requirements. ☐ Extend the Component DLP policy to include the Enterprise requirements that: • Incorporate Enterprise-defined indicator standards. • Define specific enforcement triggers based on indicators. • Establish thresholds for different enforcement actions. • Create data tag-to-enforcement action mappings. ☐ Develop testing criteria to verify and validate the enforcement functionality within the Component environment. • Develop test scenarios for each enforcement action and data type. • Create validation criteria for successful enforcement. • Establish performance impact assessment methodologies. • Define acceptable operational thresholds for enforcement actions.

Test DLP enforcement in a controlled environment.

Test DLP enforcement:

☐ Where possible, test DLP enforcement policies in a controlled/development environment to limit potential negative operational impacts. If a testing environment cannot be utilized, consider a limited rollout of the capability to a small subset of test Users/Person Entities (PEs) and Data, Applications, Assets, and Services (DAAS).

☐ Implement a phased testing approach that evaluates:

- Tag recognition accuracy across enforcement points.
- Enforcement action is appropriate for different scenarios.
- System performance under various enforcement loads.
- User/PE experience impact across different enforcement types.

☐ Verify and validate that the DLP enforcement actions align with the Enterprise standards and Component DLP policy.

☐ Ensure activity/events are captured in logging in accordance with the logging standards, from Activity 7.1.2 (Phase One) – *Log Parsing*.

☐ Verify and validate that activity/events are ingested and actioned by Component Visibility and Analytics and/or Automation and Orchestration solutions.

Update the DLP solution from monitor-only mode to enforcement mode.

Implement DLP enforcement:

☐ Leveraging a phased approach, develop a strategic enforcement transition plan that:

- Prioritizes data categories based on criticality and sensitivity.
- Establishes a phased implementation schedule.
- Defines success criteria for each implementation phase.
- Creates rollback procedures for enforcement issues.
- Includes communication plans for affected stakeholders.

☐ Prioritize data with a higher level of criticality/sensitivity, as defined in the Data Catalog from Activity 4.1.1 (Discovery) – *Data Analysis.*

- Begin with highest-risk data categories.
- Apply enforcement to clearly defined, high-value assets first.
- Expand to broader data categories in measured phases.
- Add complexity to enforcement rules incrementally.

Manage systems/data that cannot integrate/leverage DLP enforcement through risk-based exceptions.

Manage exceptions:

☐ Systems/data incompatible with DLP enforcement are:

- Identified
- Documented
- Approved/Rejected

☐ The Enterprise and/or Component determines risks.

☐ Approval is granted when justification for the exception outweighs the risks to the Enterprise/Component.

☐ Approval is periodically reassessed.

Verify and validate DLP enforcement across the Component environment.

Verify and validate DLP enforcement:

☐ Expand the verification and validation approach, from Activity 4.6.1 (Phase One) – *Implement Enforcement Points*, to ensure compliance with Enterprise standards:

- Conduct comprehensive enforcement coverage assessments.
- Verify and validate alignment with Enterprise indicator requirements.
- Verify and validate enforcement consistency across all DAAS components.
- Test edge cases and boundary conditions.

☐ Verify and validate DLP enforcement is established across all DAAS. Leverage:

- Component Master Device Inventory, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis*
- Component Master Application Inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification*
- Component Data Catalog, from Activity 4.1.1 (Discovery) – *Data Analysis*

☐ Verify and validate DLP enforcement meets the requirements established by the Component.

☐ Verify and validate that the DLP enforcement actions align with the Enterprise standards and Component DLP policy.

☐ Ensure activity/events are captured in accordance with the logging standards, from Activity 7.1.2 (Phase One) – *Log Parsing*.

☐ Verify and validate activity/events are ingested and actioned by Component Visibility and Analytics and/or Automation and Orchestration solutions.

Summary

This diagram outlines the Activity 4.6.2 (Phase Two) – *Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the prevention of mode integration by utilizing the logging schema and manual tags through enforcement points. It presents strategic insights that drive implementation and expected outcomes, including setting enforcement points to prevent mode integration in the logging schema and manual tagging.

Table 93: Activity 4.6.2 — Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are enforcement points set to prevent mode integrating the logging schema and manual tags?

STRATEGIC INSIGHTS
• The Component defines cyber enforcement indicators by coordinating with the Enterprise to align Data Loss Prevention (DLP) policies with minimum indicator standards and compliance requirements. • The Component demonstrates compliance by extending the Component DLP policy to integrate Enterprise requirements and ensuring enforcement actions align with established standards. • The Component provides evidence by implementing DLP enforcement policies using a phased approach, prioritizing high-criticality data as defined in the Component Data Catalog. • The Component leverages logging, analytics, and automation solutions to capture and analyze DLP events, ensuring enforcement actions are consistently applied across all Data, Applications, Assets, and Services (DAAS). • The Component ensures continuous verification and validation of DLP enforcement through monitoring, logging, and integration with visibility and orchestration solutions, maintaining compliance and security effectiveness.

EXPECTED OUTCOMES
1. Enterprise sets the minimum standards for indicators that support cyber enforcement. 2. Components technology is enabled for enforcement.

Capability 4.7 Data Access Control

Table 94: Capability 4.7 — Data Access Control

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
4 - Data	4.7 - Data Access Control
Description	
DoW Components ensure appropriate access to and use of data based on the data and user/NPE/device properties. Software-Defined Storage (SDS) is utilized to scale manage permissions to DAAS. Lastly, the SDS solution(s) is integrated with DRM tooling improving protections.	
Impact to ZT	
Unauthorized entities, or any entity on an unauthorized device cannot access data; Zero Trust cybersecurity will be sufficiently strong to separate community of interest data access for data in the same classification.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component establishes policies to ensure data access is granted only to authorized Users/Person Entities (PEs)/Non-Person Entities (NPEs) based on defined properties such as role, classification, and compliance status.
- A Software-Defined Storage (SDS) solution is implemented to scale and manage data access permissions across Data, Applications, Assets, and Services (DAAS) resources dynamically and efficiently.
- The SDS solution integrates with the Component's Identity Provider (IdP) to ensure that User/PE and device authentication is enforced consistently across all data access requests.
- Data owners configure access controls in the SDS solution to restrict sensitive datasets to specific roles and approved devices, ensuring separation of Communities of Interest (COI) data within the same classification.
- During a routine audit, the SDS solution identifies a misconfiguration that allows broader access than intended. The policy is corrected to limit access to the intended entities.
- An unauthorized User/PE attempts to access a restricted dataset from an unapproved device. The SDS system denies the request and generates an alert for the security team.

- The SDS solution integrates with Data Rights Management (DRM) solutions, ensuring that data is protected during access and use, such as enforcing encryption and limiting sharing permissions dynamically.
- Machine Learning (ML) analytics, integrated with the SDS solution, detect anomalous access patterns such as repeated failed attempts from a valid account, triggering further investigation.
- Access logs are regularly reviewed by data owners and security analysts, ensuring policies remain aligned with Enterprise/Component requirements.
- By leveraging SDS and integrating it with DRM and IdP solutions, the Component enforces Zero Trust (ZT) by ensuring only continuously verified and authorized entities can access and use data.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Targeted Security Enforcement: Components implement nuanced controls based on multiple attributes (e.g., User/PE, device, data sensitivity, etc.), eliminating the overly broad permissions that frequently lead to data exposure incidents.
- Adaptive Protection: When integrated with the DRM solution, Components can automatically adjust security controls as data or User/PE contexts change, maintaining appropriate protection without manual intervention.
- Scalable Governance: Software-defined approaches allow Components to expand data access management across growing environments without proportional increases in administrative overhead.
- Comprehensive Security Integration: By connecting SDS and DRM solutions, Components create a cohesive protection ecosystem where access controls and usage rights work together, eliminating protection silos that attackers typically exploit.
- Operational Efficiency: Automating access controls through SDS streamlines the process of managing permissions, reducing administrative overhead.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Attribute-Based Access Control (ABAC)
- Context-Aware Access Control
- Digital Rights Management (DRM)
- Just-in-Time (JIT) Access
- Policy Decision Points (PDPs)

Activity 4.7.1 Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1

Table 95: Activity 4.7.1 — Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Governance mechanisms ensure that Component DAAS policy is sufficient for Zero Trust outcomes as established by the SDS policy, if deemed appropriate as established in "4.2.3 Develop Software-Defined Storage (SDS) Policy".	
Predecessor(s)	**Successor(s)**
4.2.3	4.7.2
Expected Outcomes	
• DAAS access policy is developed with Enterprise and Component support.	
End State	
A centralized DAAS security approach is implemented across the Enterprise exercising best practices, reducing risk and attack surface area.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 4.2.3 (Phase Two) – *Develop Software-Defined Storage (SDS) Policy* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Consider completing Activity 1.1.1 (Discovery) – *Inventory User* prior to completing this activity, as a comprehensive list of Users/Person Entities (PEs) is necessary to understand access requirements.
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to completing this activity, as a comprehensive list of devices is necessary to understand access requirements.
- Consider completing Activity 3.1.1 (Discovery) – *Application and Code Identification* prior to completing this activity, as a comprehensive list of applications/services is necessary to understand access requirements.

- Consider completing Activity 4.1.1 (Discovery) – *Data Analysis* should be considered prior to completing this activity, as a comprehensive list of data/data types is necessary to understand access requirements.
- Consider completing Activity 3.4.1 (Phase One) – *Resource Authorization Part 1* and Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure* prior to completing this activity, as the Component established Access Control solutions could be leveraged to meet Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs) requirements.
- Activity 4.7.2 (Phase Three) – *Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 2* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 96: Implementation Tasks for Activity 4.7.1 — Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1

Develop Component Data, Applications, Assets, and Services (DAAS) policy in coordination with Enterprise support.
Conduct stakeholder engagement: ☐ Establish a governance structure of clear roles and responsibilities for ensuring DAAS compliance with Software-Defined Storage (SDS) requirements. ☐ Identify stakeholders and assign accountability for policy implementation, compliance monitoring, and enforcement. **Define objectives and scope:** ☐ Identify Enterprise-defined Access Control requirements for DAAS management. ☐ Identify any existing Component policies to align with or build upon. ☐ Define the scope of the Component DAAS policy. **Develop a policy framework and governance model:** ☐ Define governance structures, roles, and responsibilities for managing DAAS policy. ☐ Establish policy controls for data security, asset management, Access Control, and compliance monitoring.

Identify Component DAAS to collect requirements:

☐ Component Master User Inventory, from Activity 1.1.1 (Discovery) – *Inventory User*.

☐ Component Master Device Inventory, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis*.

☐ Component Master Application Inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification*.

☐ Component Data Catalog, from Activity 4.1.1 (Discovery) – D*ata Analysis*.

Draft policy document:

☐ Create a formal Component DAAS policy document detailing objectives, scope, roles, standards, and processes.

☐ Ensure the policy addresses all relevant aspects:

- Data management
- Asset protection
- Application security
- Service continuity

☐ Ensure the policy aligns with the Component SDS policy from Activity 4.2.3 (Phase Two) – *Develop Software-Defined Storage (SDS) Policy,* particularly regarding storage management, data security, and compliance standards.

Conduct risk assessment and impact analysis:

☐ Perform a risk assessment to identify potential vulnerabilities and impacts of DAAS components.

☐ Update the policy based on identified risks to mitigate key security and operational concerns.

Select Component DAAS policy enforcement solution(s).

Identify existing access control mechanisms:

☐ Leverage the approval gateways, from Activity 3.4.1 (Phase One) – *Resource Authorization Part 1.*

☐ Leverage the SDN Application Programming Interfaces (APIs), from Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure*.

☐ Leverage authentication decision points and implement segmentation gateways, from Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure*.

☐ Determine if the existing access control mechanisms meet the PEP/PDP needs of the Enterprise/Component DAAS policy.

☐ Define specific control mechanisms to enforce compliance, such as Access Controls, encryption, and data monitoring within both DAAS and SDS frameworks.

☐ Ensure these mechanisms address SDS requirements for data security, privacy, and storage management.

Verify and validate the functionality of the Component DAAS policy solution.
Pilot and test the policy enforcement: ☐ Deploy PEPs/PDPs. ☐ Conduct a pilot implementation to evaluate the effectiveness of the DAAS policy. ☐ Gather feedback from stakeholders and adjust policy details as needed.
Implement DAAS Access Control.
Implement DAAS Access Control: ☐ Officially publish the DAAS policy across relevant entities and ensure consistent enforcement. **Implement PEPs:** ☐ Enable PEPs to monitor and enforce DAAS policies in line with SDS requirements. ☐ Enable PDPs to interpret and apply rules specified in DAAS policies. ☐ Configure PEPs and PDPs to automatically detect, log, and respond to non-compliance with DAAS and SDS policies.
Verify and validate Component DAAS policy enforcement through PEPs/PDPs.
Verify and validate DAAS policy enforcement: ☐ Test, verify, and validate that DAAS is accessible and operational requirements have been maintained. ☐ Test, verify, and validate that DAAS has the minimum necessary access in accordance with Component DAAS policy.
Periodically reassess DAAS policy/enforcement.
Monitor, review, and update policy: ☐ Continuously monitor the policy's effectiveness and alignment with Enterprise goals. ☐ Review and update the DAAS policy periodically based on emerging threats, technology advancements, and Enterprise requirements. **Develop compliance monitoring and reporting processes:** ☐ Define continuous monitoring processes for tracking compliance with DAAS and SDS requirements. ☐ Establish reporting mechanisms to provide visibility into compliance statuses, such as Security Information and Event Management (SIEM) with dashboards, alerts, and periodic reports. **Automate compliance checks and audits:** ☐ Implement automated compliance tools to assess DAAS policy adherence to SDS requirements regularly. ☐ Schedule periodic audits to verify and validate compliance and identify gaps requiring remediation.

Implement incident management and remediation processes:

☐ Establish Incident Response (IR) and remediation processes for non-compliance instances with DAAS and SDS policies.

☐ Define escalation paths and corrective actions to address policy violations, ensuring swift alignment with SDS standards.

Review, update, and refine governance mechanisms:

☐ Periodically review governance mechanisms to ensure ongoing compliance with evolving DAAS and SDS policy requirements.

☐ Update governance practices as needed to address new storage technologies, threats, or regulatory changes.

Report and review compliance status with key stakeholders:

☐ Regularly report compliance status to governance bodies and stakeholders, providing insights into DAAS alignment with SDS.

☐ Use stakeholder feedback to enhance and strengthen compliance mechanisms over time.

Summary

This diagram outlines the Activity 4.7.1 (Phase Two) – *Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1* component of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on Data, Applications, Assets, and Services (DAAS) policy development, and integration. It presents strategic insights that drive implementation and expected outcomes, including the development of a DAAS policy with Enterprise and component-level support.

Table 97: Activity 4.7.1 — Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the DAAS policy developed with Enterprise and Component-level support? 2. What is the plan for integrating Software-Defined Storage (SDS) with the DAAS policy?

STRATEGIC INSIGHTS
• The Component defines a DAAS policy by establishing governance structures, identifying stakeholders, and aligning with Enterprise SDS requirements. • The Component demonstrates compliance by developing policy controls for data security, access management, and enforcement, integrating access control mechanisms such as Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs). • The Component provides evidence through verification and validation testing, pilot deployments, and continuous monitoring to ensure policy effectiveness and alignment with SDS mandates. • The Component leverages automated compliance checks, audits, and reporting mechanisms to track DAAS policy adherence, ensuring visibility and enforcement. • The Component ensures ongoing compliance through periodic policy reviews, governance updates, and Incident Response (IR) processes to mitigate risks and adapt to evolving security requirements.

EXPECTED OUTCOMES
1. DAAS access policy is developed with Enterprise and Component support.

Activity 4.7.4 Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1

Table 98: Activity 4.7.4 — Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components integrate attributes associated with access control and data location, and establish a means for interoperability across DLP, DRM, and storage infrastructure solutions with Enterprise IdP.	
Predecessor(s)	**Successor(s)**
2.1.3, 4.2.3	4.7.5, 4.7.6
Expected Outcomes	
• Component data security solutions are integrated with IdP (e.g., API, LDAP, SAML).	
End State	
Integrating DLP, DRM, and SDS with the IdP solution to ensure data protection and access is granted to only authenticated and authorized users.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 2.1.3 (Phase Two) – *Enterprise Identity Provider (IdP) Part 1* and Activity 4.2.3 (Phase Two) – *Develop Software-Defined Storage (SDS) Policy* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Ensure Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1* has been completed and that the Component has integrated with the Enterprise Identity Provider (IdP) solution.
- Consider completing Activity 4.2.2 (Phase One) – *Interoperability Standards* prior to completing this activity, as the communication standards will be necessary to integrate with the IdP as well as the Component solutions from the Visibility and Analytics and/or Automation and Orchestration Pillars.
- Consider completing Activity 4.7.1 (Phase Two) – *Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1* prior to this activity, to leverage Data, Application, Assets, and Services (DAAS) policy governance stakeholders.

- Consider completing Activity 7.1.2 (Phase One) – *Log Parsing* prior to this activity, to ensure audit logs comply with Enterprise/Component logging standards.
- Activity 4.7.5 (Phase Three) – *Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 2* and Activity 4.7.6 (Phase Three) – *Implement Software-Defined Storage (SDS) Tool and/or Integrate with Data Rights Management (DRM) Tool Part 1* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 99: Implementation Tasks for Activity 4.7.4 — Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1

Integrate with attributes associated with access control and data location in the IdP.
Conduct stakeholder engagement: ☐ Leverage Component DAAS policy governance stakeholders, from Activity 4.7.1 (Phase Two) – *Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1*. **Understand Enterprise requirements:** ☐ Reassess Enterprise-defined control requirements. ☐ Reassess Component DAAS policy requirements. ☐ Leverage Component IdP, integrated with the Enterprise, from Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1*, which manages Users/Person Entities (PEs)/Non-Person Entities (NPEs), after Activity 2.1.3 (Phase Two) – *Enterprise Identity Provider (IdP) Part 1*. ☐ Leverage Component-defined interoperability standards, from Activity 4.2.2 (Phase One) – *Interoperability Standards*. **Develop DAAS and User/PE/NPE attribute integration plan:** ☐ Ensure the IdP can access an attribute repository where User/PE/NPE data and access attributes are stored.

☐ Map the required attributes (e.g., User/PE/NPE role, location, access level, etc.) from the attribute repository to the IdP. This allows the IdP to leverage these attributes during authentication and approval.

☐ Define the metadata configuration for each attribute, specifying how attributes are structured and the values allowed.

Enable logging and monitoring for governance:

☐ Enable logging in the IdP to track when and how Access Control and location-based attributes are used. This can include:

- Monitoring User/PE/NPE access logs to identify who is accessing specific data, from where, and using which attributes.
- Tracking policy enforcement logs of access control policies, including access denials or Multi-Factor Authentication (MFA) triggers based on User/PE/NPE attributes. Location-based access control will be implemented as a component of the overall access control policy, leveraging Attribute-Based Access Control (ABAC) principles.

☐ Monitor and document anomalies. Incorporate identified anomalies when implementing Security Information and Event Management (SIEM) solutions, to detect unusual access patterns such as attempts to access sensitive data from unapproved locations.

Implement continuous monitoring and updates:

☐ Review and update Access Control and data location policies regularly based on changes in regulatory requirements, business needs, and threat landscapes.

☐ Ensure the attributes in the IdP are continuously synchronized with the authoritative data source to reflect any changes in roles, clearance levels, or locations.

☐ Perform periodic compliance audits to ensure Access Control mechanisms align with regulatory requirements for data location.

Test IdP-integrated Attribute-Based Access Control (ABAC) functionality/interoperability.

Pilot and test interoperability and policy enforcement:

☐ Test integration and interoperability between Data Loss Prevention (DLP), Data Rights Management (DRM), storage infrastructure, and the IdP, simulating different scenarios to ensure smooth communication, identity verification and validation, and policy enforcement.

- Test different roles, locations, and access levels to consistently verify and validate that appropriate Access Control and data protection measures are applied.

☐ Simulate data leakage and/or data exfiltration scenarios to ensure that the DLP system is effectively preventing unapproved data sharing or transfer based on User/PE/NPE attributes.

☐ Simulate and test various access scenarios to ensure Access Control policies function as intended.

☐ Verify and validate access logs and monitoring to ensure audit trails capture all relevant access details, including which attributes were used in policy decisions.

Establish interoperability with cloud and on-premise solutions:

☐ Ensure interoperability between on-premises storage solutions and cloud-based DLP and DRM systems.

- Implement Application Programming Interface (API) Integration between cloud services and on-premise DLP/DRM solutions to synchronize data protection and access policies across both environments.
- Use Cloud Access Security Brokers (CASBs) to enforce consistent DLP and DRM policies across cloud environments, leveraging the IdP for authentication and Access Control.

☐ Cloud storage integration: If the Component uses cloud storage solutions, ensure that DLP and DRM solutions are integrated with cloud-based storage to maintain secure data transfers, encryption, and compliance with Enterprise security policies.

Enforce IdP-integrated ABAC.

Implement IdP-integrated ABAC:

☐ Using a phased approach, deploy/enforce the IdP-integrated ABAC solution.

Verify and validate the IdP-integrated ABAC.

Verify and validate auditing and monitoring across systems:

☐ Ensure audit logs comply with Enterprise/Component logging standards, from Activity 7.1.2 (Phase One) – *Log Parsing*.

☐ Verify and validate integration with Component solutions from the Visibility and Analytics and/or Automation and Orchestration Pillars.

Continuous monitoring.

Provide continuous monitoring and updates:

☐ Conduct regular audits to verify and validate that the interoperability between systems is functioning effectively and that policies are being enforced consistently across the Component environment in accordance with Enterprise requirements.

Summary

This diagram outlines the Activity 4.7.4 (Phase Two) – *Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development of an integration plan between Software-Defined Storage (SDS) and the Enterprise Identity Provider (IdP). It presents strategic insights that drive implementation and expected outcomes, including the integration of component data security solutions with the IdP.

Table 100: Activity 4.7.4 — Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the integration plan between SDS and the Enterprise IdP developed?

STRATEGIC INSIGHTS
• The Component defines an integration plan for access control and data location attributes within the Enterprise IdP, aligning with Data, Applications, Assets, and Services (DAAS) policy governance and interoperability standards. • The Component demonstrates compliance by mapping User/Person Entity (PE)/Non-Person Entity (NPE) attributes to the IdP, enforcing location-based access controls, and ensuring secure authentication and approval processes. • The Component provides evidence through logging, monitoring, and anomaly detection, integrating with Security Information and Event Management (SIEM) solutions to track access patterns, enforce policies, and detect unapproved access to sensitive data. • The Component leverages automated policy enforcement through IdP-integrated Attribute-Based Access Control (ABAC), ensuring consistent access management across storage systems, security solutions, and Enterprise applications. • The Component ensures ongoing compliance through continuous monitoring, periodic audits, and updates to access control mechanisms, maintaining alignment with regulatory and security requirements.

EXPECTED OUTCOMES
1. Component data security solutions are integrated with IdP (e.g., Application Programming Interface (API), Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), etc.).

Network and Environment Pillar

Capability 5.2 Software-Defined Networking (SDN)

Table 101: Capability 5.2 — Software-Defined Networking (SDN)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
5 - Network and Environment	5.2 - Software-Defined Networking (SDN)
Description	
DoW Components define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane. Integrations are conducted with decision points and segmentation gateway to accomplish the plane separation. Analytics are then integrated to real-time decision making for access to resources.	
Impact to ZT	
Enables the control of packets to a centralized server, provides additional visibility into the network, and enables integration requirements.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component begins by defining Application Programming Interface (API) decision points that will enable programmable control of network traffic, ensuring consistent application of access policies across the network.
- A Software-Defined Networking (SDN) infrastructure is implemented to separate the control and data planes, centralizing the management of network elements and improving visibility into traffic flows.
- Network flows are segmented into three (3) distinct planes: control, management, and data, providing better isolation and security for sensitive operations.
- A network asset discovery process is conducted to identify and document all connected devices, optimizing traffic management and ensuring all assets comply with SDN policies.
- Integration of decision points with the segmentation gateway ensures that API-driven policies are enforced at every point of interaction within the network.
- The SDN infrastructure is integrated with analytics solutions to enable real-time visibility into traffic patterns and decision-making for resource access requests.

- A suspicious packet attempting to bypass a segmentation gateway is detected by the SDN analytics solution. The centralized controller blocks the packet, preventing unauthorized access to sensitive resources.
- During a routine review, SDN analytics reveal suboptimal routing in the data plane. The controller automatically adjusts the routing configuration to optimize performance without compromising security.
- Real-time access decisions are further enhanced by integrating User/Person Entity (PE)/Non-Person Entity (NPE) and application attributes from other Zero Trust (ZT) pillars, ensuring traffic is only allowed when fully authorized.
- By leveraging SDN programmable infrastructure and real-time analytics, the Component gains granular control over network traffic and enhances security through segmentation for managing and protecting network resources.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security: By implementing SDN and segmentation, Components can isolate sensitive operations and reduce the risk of lateral movement by attackers.
- Improved Traffic Management: Centralized control over network traffic enables better optimization and routing, resulting in enhanced performance.
- Real-Time Analytics: Integration with analytics tools provides visibility into traffic patterns, enabling proactive decision-making and rapid response to threats.
- Alignment with Zero Trust Principles: The capability supports a ZT architecture by ensuring that access decisions are based on comprehensive User/PE, device, and application attributes.
- Operational Efficiency: Automating network management tasks reduces the burden on Information Technology (IT) staff, enabling them to focus on strategic initiatives rather than routine maintenance.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Network Function Virtualization (NFV)
- Network Virtualization
- Macro-Segmentation
- Micro-Segmentation
- Internet Protocol Security (IPsec)
- Traffic Filtering and Inspection

Activity 5.2.3 Segment Flows into Control, Management, and Data Planes

Table 102: Activity 5.2.3 — Segment Flows into Control, Management, and Data Planes

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Network infrastructure and flows are segmented either physically or logically into separate and distinct control, management, and data planes. Segmentation using IPv6/VLAN approaches is implemented to better organize traffic across data planes. Analytics and NetFlow from the updated infrastructure are automatically fed into operations centers and analytics tools.	
Predecessor(s)	**Successor(s)**
None	5.3.2, 5.4.2
Expected Outcomes	
• Enterprise provides guidance/policy on segmentation. • IPv6/VLAN segmentation is implemented. • Enable automated NetOps information reporting. • Ensure configuration control across Enterprise. • Integrated with SIEM/SOAR.	
End State	
Enterprise provides policy and/or guidance on segmentation. Components further segment network traffic limiting the scope of attack, isolating incidents, and preventing malicious attempts from lateral movement across the network.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Presumption: Enterprise has provided guidance/policy on segmentation.
- Presumption: Component has selected a Software-Defined Networking (SDN) solution.
- Presumption: Component has implemented Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) solutions.
- Consider completing Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure* prior to this activity, to leverage the SDN infrastructure.
- Consider completing Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation* prior to this activity, to leverage access control points.

- Isolate the control plane responsible for routing, signaling, and network management to protect network configuration and control traffic from User/Person Entity (PE)/Non-Person Entity (NPE) data traffic and potential attacks.
- Segregate environment traffic to prevent unapproved access and reduce the attack surface.
    - Management functions are separated logically, or physically isolated within a management plane.
    - Environmental access control functions are separated and logically, or physically isolated within a control plane.
    - Operational functions remain in the newly declared data plane.
- Establish strong monitoring and logging mechanisms for all three (3) planes (control, management, and data).
- Review technical requirements and limitations for legacy systems.
- Activity 5.3.2 (Phase Two) – *Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation* and Activity 5.4.2 (Phase Two) – *Application and Device Micro-Segmentation* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 103: Implementation Tasks for Activity 5.2.3 — Segment Flows into Control, Management, and Data Planes

Review and align with the Enterprise policies and standards on programmatic network segmentation and control.
Review devices and network security hardening guidelines: ☐ Review existing and revised best practices and industry standards for network segmentation, security, and protection. Always rely on multiple layers of defense for a more secure network design [22]. ☐ Ensure redundant devices in critical core areas are implemented across all network segments to provide availability, fault tolerance, load balance, and maximum network throughput [22].

☐ Adopt and enforce Enterprise recommended cryptographic algorithms for end-to-end network traffic encryption with built-in capability for Deep Packet Inspection (DPI) and monitoring [23].

Review and manage risks from SDN controllers:

☐ Adopt a cluster of load-balanced SDN controllers to avoid a single point of compromise. Maintain the secure integrity of the cluster and all the elements of the controller through strict authentication and authorization policies [24].

☐ Stay aware and vigilant of all known vulnerabilities associated with different SDN elements. Implement a repeatable process for rapidly applying vetted software updates to all elements of the SDN architecture(s) [24].

Review and manage risk from communication protocols, including Transport Layer Security (TLS) inspection:

☐ Routinely review all TLS security settings, including version, cipher suites, and certificate authorities, for strict access controls and to verify and validate continuous compliance with the Enterprise and industry-vetted security best practices, policies, and standards [25].

☐ The adoption of encrypted communication channels is recommended for all SDN implementations. Enforce OpenFlow communications over the strongest version of TLS with systematic authentication and authorization controls for each session.

Design a secure controller-based SDN architecture.

Leverage the SDN infrastructure, from Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure,* to further review controller and software-defined architecture:

☐ Adopt a secure design for the SDN architecture to satisfy essential functions, such as:

- Secure automated resources provisioning
- Control plane abstraction
- Segmentation and dynamic security policy enforcement

☐ Adopt a distributed application-aware firewall deployed at each segment boundary to restrict access control and properly segregate traffic between different SDN elements and planes.

☐ Align SDN design objectives for network automation, centralized management, security enforcement, improved agility, and scalability with the broader Enterprise network security strategy and modernization.

Leverage the SDN implementation, from Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure,* to verify and validate the deployment of a controller and centralized control:

☐ Leverage previous applications and network flow mappings to better understand the network infrastructure's normal operational profile and establish a functional baseline. Identify and approve only vetted traffic patterns by implementing a deny-by-default approach to all network traffic.

☐ Select a cluster of controllers that are logically centralized, scalable, and load-balanced to manage network devices across the entire SDN architecture. Design a fault-tolerant SDN cluster of controllers for high availability in support of network scalability.

☐ Ensure the SDN elements' decoupling and segregating different planes through a layered design architecture to centralize and restrict control plane access.

Implement the Southbound interface (data plane):

☐ Select a compatible open standard protocol to facilitate the control and data plane interface. Avoid vendor lock-in with non-interoperable and proprietary protocols.

☐ Configure the SDN controller to authenticate southbound Application Programming Interface (API) control-plane messages received from SDN-enabled network elements using a Federal Information Processing Standards (FIPS)-approved message authentication code algorithm [26].

☐ Enable secure configuration to protect the data plane and the various forwarding traffic functions initiated by the control plane across the integrated network domains.

Implement the Northbound interface (management plane):

☐ Configure the SDN controller to authenticate northbound API messages received from business applications and management systems using a FIPS-approved message authentication code algorithm [26].

☐ Select a compatible northbound API to seamlessly integrate and connect with the SDN controllers seamlessly. Representational State Transfer Application Programming Interface (REST API) should be considered for its standardization, flexibility, and significant acceptance.

☐ Define and design API endpoints that provide secure access to relevant network segment information and allow applications to perform necessary management actions, such as network topology, Virtual Local Area Network (VLAN) configuration, and Access Control List (ACL) tables.

☐ Implement caching mechanisms to improve API performance, reduce network latency, enhance scalability, and help load balance the SDN controllers.

Deploy an integrated and unified security solution for the entire network infrastructure, focusing on the SDN elements.

Enforce access control:

☐ Leverage ACLs on network devices and gateway endpoints to filter traffic based on network parameters. Deploy distributed Next-Generation Firewalls (NGFWs) to restrict unapproved traffic and enforce access control-based policies between approved network segments.

☐ Leverage the concept of the security group to implement Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) types of identity profiles and enforce granular security policies at each session request and every gateway endpoint.

☐ Leverage the Access Control points, from Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation,* to enforce access control policies and restrict access to approved entities only. Enforce authentication and approval policies based on application and service identities, the underlying network parameters, and User/PE/NPE identities [27].

☐ Leverage IDS/ IPS solutions for network monitoring, tracking, and restricting inbound and outbound traffic to include, whenever applicable, full-packet capture capability.

☐ Implement systematic identity verification, device posture validation, and strong authentication and authorization before granting access to the approved network segment using the principle of Least Privilege.

Identify, group, and segregate similar network traffic:

☐ Leverage traffic monitoring solutions and DPI techniques to capture and analyze network traffic. Examine network packets to identify applications, protocols, ports, and data types.

☐ Analyze traffic flows to understand approved communication patterns between different network elements. Apply appropriate tags for each plane of the SDN architecture and group network traffic based on criteria such as:

- Application
- Protocol
- Port
- Sensitivity Tag
- Network Segment
- VLAN ID

☐ Leverage traffic monitoring solutions and DPI techniques to capture and analyze network traffic. Examine network packets to identify applications, protocols, ports, and data types.

☐ Configure separate logical, trusted subnets using planning to isolate distinct types of network traffic. Leverage Artificial Intelligence (AI) and Machine Learning (ML) algorithms to automate the network traffic pattern analysis process over time.

Enable Internet Protocol Version 6 (IPv6) addressing compatibility:

☐ Whenever applicable, comply with Enterprise directives and industry best practices to select and deploy network technologies that are IPv6-enabled and ready for a seamless Enterprise-wide integration [28].

☐ Leverage vendor Subject Matter Expert (SME) support and approved solution integrators to build a seamless migration strategy plan.

☐ Adopt a phased approach for legacy systems, requiring an IPv4-IPv6 migration.

Leverage API integration and automated deployment for configuration control and advanced network telemetry.

Maintain complete network visibility:

☐ Leverage the various API integrations to provide and maintain real-time network visibility into the entire infrastructure landscape, enabling data flow control between different network elements, planes, and security solutions on the SDN architecture.

☐ Implement centralized logging by using APIs to collect, aggregate, and analyze log data from various security appliances, network segments, and system events into a secure, centralized log management platform.

Enable triggered workflows:

☐ Design workflow logic and automate security policy enforcement and monitoring. Integrate network configuration changes into the Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines to orchestrate testing and deployment of configurations.

Enable API gateway integration:

☐ Leverage a broader API adoption, developed using open standards to minimize proprietary data interfaces, to avoid vendor lock-in integrations throughout the acquisition program lifecycle [29].

☐ Integrate security solutions via API to programmatically update network policies based on real-time events, security threats, Indicators of Compromise (IoC) containers, and system performance.

☐ Adopt industry best practice standards such as Open Authorization 2.0 (OAuth2) and JavaScript Object Notation (JSON) Web Tokens (JWT) for systematic authentication and authorization of all API consumers. Leverage API gateway and service mesh to centralize policy enforcement points for monitoring, management, and auditing.

Enable performance monitoring, advanced analytics, and reporting:

☐ Deploy network device APIs to collect advanced telemetry performance data and security events. Leverage streaming telemetry protocols to create real-time dashboards, visualize network performance, identify IoC, and help troubleshoot issues.

Enable API integration for configuration control:

☐ Leverage emerging technologies and tools, such as Configuration as Code (CaC) and Infrastructure as Code (IaC) to design and build immutable network deployments through vetted templating, Zero-Touch Provisioning (ZTP), and automated rollbacks built-in capabilities.

Enable testing, verification, and validation of the flow segmentation into control, management, and data planes.

Review testing, verification, and validation strategies:

☐ Create a testing environment for the simulation of traffic generation and capture. Tailor each flow for the specific plane, and leverage packet capture capability at gateway entry points to analyze network traffic.

☐ Leverage flow monitoring solutions to ensure that network traffic is accurately segmented, and each traffic pattern is correctly associated with each segment and the specific plane.

☐ Confirm that segmentation enforcement defaults to a deny-all posture, only allowing explicitly defined flows based on identity- and policy-driven authorization decisions.

☐ Integrate with Automation and Orchestration and Visibility and Analytics pillar solutions.

Adopt verification and validation of isolation.

☐ Perform isolation testing to verify and validate that traffic is segregated and restricted in accordance with network segment policies.

☐ Leverage Virtual Local Area Network (VLAN) and Virtual Routing and Forwarding (VRF) technologies to test network ACLs between network segments. Capture and analyze all flow logs to identify any violations or weaknesses in traffic filtering.

Summary

This diagram outlines the Activity 5.2.3 (Phase Two) – *Segment Flows into Control, Management, and Data Planes* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on network infrastructure and the segmentation of flows into control, management, and data planes. It presents strategic insights that drive implementation and expected outcomes, including enabling automated Network Operations (NetOps) information reporting, Internet Protocol version 6 (IPv6) segmentation, and configuration control across the Enterprise.

Table 104: Activity 5.2.3 — Segment Flows into Control, Management, and Data Planes - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are network infrastructure and flows segmented into control, management, and data planes?

STRATEGIC INSIGHTS
• The Component defines and documents network segmentation policies and security hardening procedures in alignment with Enterprise standards, ensuring a multi-layered defense strategy that enhances resilience against cyber threats. • The Component demonstrates adherence to Enterprise security guidelines by reviewing and managing risks associated with Software-Defined Networking (SDN) controllers, communication protocols, and cryptographic standards to prevent unapproved access and ensure network integrity. • The Component provides evidence that SDN controllers, encryption protocols, and communication mechanisms are evaluated for security compliance, including the implementation of Transport Layer Security (TLS) and OpenFlow encryption for secure communication. • The Component leverages redundancy and fault-tolerant design to ensure that critical network segments remain available and resilient, reducing the risk of single points of failure while maintaining performance across all infrastructure components. • The Component ensures continuous monitoring, auditing, and updating of segmentation policies to mitigate risks, improve enforcement of Least Privilege access, and align with evolving Enterprise security directives.

✓ EXPECTED OUTCOMES

1. Enterprise provides guidance/policy on segmentation.
2. IPv6/VLAN segmentation is implemented.
3. Enable automated NetOps information reporting.
4. Ensure configuration control across Enterprise.
5. Integrated with Security Information and Event Management (SIEM)/ Security Orchestration, Automation, and Response (SOAR).

Capability 5.3 Macro-Segmentation

Table 105: Capability 5.3 — Macro-Segmentation

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
5 - Network and Environment	5.3 - Macro-Segmentation
Description	
DoW Components establish network boundaries and provide security against networked assets located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection.	
Impact to ZT	
Network segmentation is defined by a large perimeter to enable resource segmentation by function and user type.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component establishes macro-segmentation policies, defining large network perimeters based on resource functions and User/Person Entity (PE) types, such as datacenters and business-critical environments.
- A centralized system is deployed to verify and validate the identity of devices, Users/PEs/Non-Person Entities (NPEs) before they are allowed to access resources within segmented perimeters, enforcing Zero Trust (ZT) through continuous identity verification.
- Datacenter resources are grouped into macro-segments, such as compute, storage, and processing environments, each with distinct access rules and boundaries.
- Security policies are tailored for each macro-segment, ensuring that sensitive resources, such as production databases, are only accessible to Users/PEs/NPEs explicitly authorized for that segment.
- Monitoring solutions provide real-time insights into traffic flows across macro-segments, allowing the Component to detect and respond to unusual activity patterns quickly.
- An anomalous device is flagged for review following attempts to communicate across network segments.

- Once flagged, the device is blocked at the network level until validated by the security team, ensuring only authenticated and authorized devices can access resources.
- By halting access attempts in real-time, the Component minimizes lateral movement for potential attackers and strengthens Incident Response (IR) effectiveness.
- Periodic reviews of macro-segmentation boundaries ensure that access controls remain aligned with Component functions, reducing the risk of segmentation drift.
- By establishing macro-segmentation with robust validation processes, the Component enhances its ability to secure networked assets, limiting unauthorized access.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security: The Component improves security posture by limiting access to sensitive resources to approved personnel only.
- Enhanced Compliance: Implementing tailored security policies for each segment based on regulatory requirements improves compliance.
- Enhanced Visibility: Employing monitoring capabilities enables rapid detection and response to potential threats.
- Reduced Lateral Movement Risk: The Component limits the ability of threats to spread within the network, minimizing the impact of potential breaches.
- Streamlined Access Management Processes: The Component improves overall operational efficiency and User/PE experience.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Macro-Segmentation
- Micro-Segmentation
- Policy Decision Points (PDPs)
- Policy Enforcement Points (PEPs)
- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
- Next-Generation Firewall (NGFW)

Activity 5.3.2 Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation

Table 106: Activity 5.3.2 — Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation

<table>
<tr><th colspan="2">DoW Zero Trust Framework</th></tr>
<tr><td colspan="2"><b><i>Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.</i></b></td></tr>
<tr><td colspan="2"><b>Description</b></td></tr>
<tr><td colspan="2">DoW Components implement mission/organization-based macro-segmentation using logical network zones that limit lateral movement. Proxy and/or enforcement checks are integrated with the SDN or alternative networking approach solution(s) based on device attributes and behavior.</td></tr>
<tr><td><b>Predecessor(s)</b></td><td><b>Successor(s)</b></td></tr>
<tr><td>5.2.3</td><td>None</td></tr>
<tr><td colspan="2"><b>Expected Outcomes</b></td></tr>
<tr><td colspan="2">• Establish proxy/enforcement checks of attributes (device, location, data), access and flow (client, tenant, traffic patterns), and Component principles (asset life cycle, compliance, policy).
• Analyze activities of application-specific security stacks for firewall configuration and access policies.</td></tr>
<tr><td colspan="2"><b>End State</b></td></tr>
<tr><td colspan="2">SDN or alternative networking approach solutions incorporate proxy and enforcement checks based on device attributes and behavior, ensuring robust security. Application delivery control proxies, SIEM logging, UAM, and authentication decision points are integrated and operational. Segmentation gateways are deployed to enhance network security and efficiency.</td></tr>
</table>

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 5.2.3 (Phase Two) – *Segment Flows into Control, Management, and Data Planes* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, as a complete device inventory will be necessary.
- Consider completing Activity 3.1.1 (Discovery) – *Application and Code Identification* prior to this activity, as a complete application inventory will be necessary.
- Consider completing activity 3.4.1 (Phase One) – *Resource Authorization Part 1* prior to this activity, to leverage Resource Authorization Gateways across multiple regions.

- Consider completing Activity 3.4.2 (Phase Two) – *Resource Authorization Part 2* prior to this activity, to leverage Policy Enforcement Points (PEPs) across multiple regions.
- Consider completing Activity 3.4.3 (Phase One) – *Software-Defined Compute (SDC) Resource Authorization Part 1* prior to this activity, to leverage Software-Defined Compute (SDC) Authorization Gateways across multiple regions.
- Consider completing Activity 5.1.2 (Phase One) – *Define Granular Control Access Rules and Policies Part 2* prior to this activity, to leverage the established access control policies across multiple regions.
- Consider completing Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure* prior to this activity, to leverage Authentication Decision Points and implement Segmentation Gateways across multiple regions.
- Consider completing Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation* prior to this activity, to leverage the established guidance in support of implementing virtual environments across multiple regions.
- Consider completing Activity 5.4.1 (Phase One) – *Implement Micro-Segmentation* prior to this activity, to leverage micro-segmentation across multiple regions.
- Presumption: The Enterprise has established guidance/requirements on network modernization.
- Consider how strict policies for controlling traffic flow, ensuring only approved users or services can navigate between zones will be established. This may involve using Virtual Local Area Networks (VLANs), firewalls, or Virtual Private Networks (VPNs) to enforce policy.
- Consider that critical systems or applications that require communication between zones will need to do so securely, using secure tunneling or encrypted communication channels as necessary.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 107: Implementation Tasks for Activity 5.3.2 — Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation

Establish a mission/Component-based network macro-segmentation strategy.
Review and define mission objectives: ☐ Review and leverage the existing Enterprise network modernization guidance and standards. ☐ Review and leverage existing: • Component Master Device Inventory, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* • Component Master Application Inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification* • Component micro-segmentation architecture, from Activity 5.4.1 (Phase One) – *Implement Micro-Segmentation* • Application Programming Interface (API) Gateways, from Activity 5.1.2 (Phase One) – *Define Granular Control Access Rules and Policies Part 2* • Resource Authorization Gateways, from Activity 3.4.1 (Phase One) – *Resource Authorization Part 1* • Software-Defined Compute Authorization Gateways, from Activity 3.4.3 (Phase One) – *Software-Defined Compute (SDC) Resource Authorization Part 1* ☐ Review or develop accurate environment topology artifacts to understand the existing Component multi-region/location environment structure and security posture [9]. ☐ Review and ensure that greater environment visibility is enabled to maintain global cyber situational awareness.
Design and implement Base/Camp/Post/Station (B/C/P/S)-based network macro-segmentation.
Establish regional Installation Service Nodes (ISNs): ☐ Design and configure network devices to create and enforce regional policy-driven segmentation boundaries, such as [9]: • Switches • Routers • Firewalls • Installation Gateways (IGs) **Implement multi-region environment segmentation:** ☐ Choose tools for implementing environment segmentation. ☐ Use internal security controls, such as [9]: • VLANs to enforce security controls [9] • Defined access policies written into firewall rules [9] • Software-Defined Networking (SDN) [9]

☐ Choose solutions for managing access control within and between segments.

- Include Network Access Control (NAC) solutions.
- Include Identity, Credential, and Access Management (ICAM) solutions.

☐ Utilize access policies to restrict lateral movement between segments [9].

Enforce B/P/C/S security overlays:

☐ Leverage network security overlays, from Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation,* to create B/P/C/S-based secure virtual network segments.

Select security tools and technologies:

☐ Select or leverage firewall solutions for implementing application-specific security stacks [30].

☐ Select or leverage access control solutions for managing access policies.

☐ Select or leverage tools for monitoring and logging application activities.

☐ Select or leverage UAM solutions to monitor User/Person Entity (PE) activity [31].

☐ Select or leverage existing Endpoint Detection and Response (EDR) solutions to monitor device activity.

☐ Select or leverage existing authentication decision solutions.

Integrate proxy and/or enforcement checks with SDN or alternative networking approach solution(s) based on device attributes and behavior.

Segregate segment traffic:

☐ Leverage the data flow segmentation and mapping, from Activity 5.2.3 (Phase Two) – *Segment Flows into Control, Management, and Data Planes.*

☐ Leverage Authentication Decision Points and Implement Segmentation Gateways, from Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure.*

☐ Leverage PEPs, from Activity 3.4.2 (Phase Two) – *Resource Authorization Part 2.*

Review and enforce B/P/C/S applicable Attribute-Based Access Control (ABAC) policies:

☐ Establish clear objectives for rule-based dynamic policy and enforcement checks across B/C/P/S. Determine if existing solutions meet the multi-location requirements [23].

- Include improved network security.
- Include enhancing visibility.
- Include supporting dynamic access control.

☐ Map and integrate Identity and Access Management (IAM) roles and permissions into B/P/C/S segments access control for dynamic identity and attribute-based policy restriction.

Identify device attributes and behavior:

☐ Identify key attributes to be monitored. Determine if existing defined attributes meet the multi-location requirements.

- Include device type.

- Include operating system.
- Include security posture.

☐ Identify behavioral patterns to be monitored.

- Include network traffic patterns.

Select proxy and enforcement:

☐ Choose proxy tools for monitoring [23].

☐ Choose proxy tools for controlling network traffic [23].

☐ Select a service mesh to help monitor and map traffic flows [23].

☐ Select enforcement tools for implementing access control.

☐ Select enforcement tools for policy enforcement.

Establish network monitoring, testing, and IG.

Implement continuous monitoring and reporting:

☐ Configure environment continuous monitoring to track application activities and alert on potential segment access violations [31].

- Include proxy/enforcement, decision logs, and network flows.

☐ Generate log records and make them available for continuous monitoring [31].

- Include detection of anomalies [31].

☐ Implement reporting mechanisms to provide visibility into network access and application activities, such as:

- Policy enforcement and allow adjustments and revisions as needed [31].
- Cross-domain compliance and ensure cybersecurity risk management performance is evaluated and updated as required [31].

☐ Prevent unnecessary protocols across the network boundary [30].

☐ Configure UAM solution to monitor User/PE activity and generate alerts for suspicious behavior.

☐ Configure Security Information and Event Management (SIEM) solution to collect, monitor, and analyze security events from all components [30].

Conduct periodic network penetration testing:

☐ Collaborate with key stakeholders to develop rules of engagement and scope.

- Review the environment components.
- Review the system dependencies.
- Analyze traffic patterns and data flows.

☐ Assess the current security posture of each environment segment and identify security requirements [31].

- Include existing firewall rules [30].
- Include environment segment access policies.

Verify and validate macro-segmentation security configuration:

☐ Conduct functional environment testing to ensure the macro-segmentation configuration works as intended.

☐ Ensure security configuration can identify, verify, validate, and record environment access requests, attempts, and violations [31].

Develop testing of a multi-tenancy capability to ensure environment isolation and continuous compliance among different network environments.

Summary

This diagram outlines the Activity 5.3.2 (Phase Two) – *Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the implementation of Base/Camp/Post/Station (B/C/P/S) macro-segmentation policies to limit lateral movement. It presents strategic insights that drive the implementation and expected outcomes, including the establishment of a proxy and enforcement checks of device Attributes, Access and Flow, and Component Principles.

Table 108: Activity 5.3.2 — Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are B/C/P/S macro-segmentation policies being implemented to limit lateral movement?

STRATEGIC INSIGHTS
• The Component defines a mission-based macro-segmentation strategy by aligning with Enterprise network modernization standards and leveraging existing inventories, segmentation architectures, and topology artifacts to inform secure B/C/P/S segmentation. • The Component demonstrates segmentation enforcement by configuring regional boundaries with Software-Defined Networking (SDN), firewalls, Network Access Control (NAC), and Identity, Credential, and Access Management (ICAM) tools to control access and restrict lateral movement across multi-region environments. • The Component provides verification and validation through continuous monitoring, penetration testing, and logging to ensure segmentation functions as intended and supports multitenancy and secure isolation. • The Component leverages Attribute-Based Access Control (ABAC) policies, device attributes, and behavioral indicators to enforce dynamic, policy-based access control within and between network segments. • The Component ensures compliance and visibility through Security Information and Event Management (SIEM), User Activity Monitoring (UAM), and automated reporting, supporting real-time detection, response, and ongoing policy refinement.

EXPECTED OUTCOMES
1. Establish proxy/enforcement checks of attributes (device, location, data), access and flow (client, tenant, traffic patterns), and Component principles (asset life cycle, compliance, policy). 2. Analyze activities of application-specific security stacks for firewall configuration and access policies.

Capability 5.4 Micro-Segmentation

Table 109: Capability 5.4 — Micro-Segmentation

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
5 - Network and Environment	5.4 - Micro-Segmentation
Description	
DoW Components define and document network segmentation based on identity and/or application access in their virtualized and/or cloud environments. Automation is used to apply policy changes through programmatic (e.g., API) approaches. Lastly, where possible, Components will utilize host-level process micro-segmentation.	
Impact to ZT	
Network segmentation enabled by narrower and specific segmentation in a virtualized environment via identity and/or application access, allowing for improved protection of data in transit as it crosses system boundaries (e.g., in a coalition environment, system high boundaries) and supported dynamic, real-time access decisions and policy changes.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- A university-affiliated Component is collaborating with international partners on a sensitive cloud-hosted research project involving proprietary data and restricted access.
- The Component uses identity-based network segmentation to ensure that each partner organization only accesses resources necessary for their role, with policies scoped to individual Users/Person Entities (PEs) and specific applications.
- During a scheduled system upgrade, an employee at a partner organization unknowingly downloads a compromised software package containing ransomware.
- The ransomware attempts lateral movement within the shared virtual environment to access other virtual machines and encrypted data repositories.
- Micro-segmentation at the host level enforces Zero Trust (ZT) by preventing unauthorized processes from communicating beyond their designated scope.
- Simultaneously, application-based segmentation prevents the malicious process from accessing the research data storage, which only allows approved applications to connect.

- Security logs detect abnormal process behavior and automatically trigger an Application Programming Interface (API)-based policy update that temporarily revokes access for the affected identity.
- The automation platform immediately propagates updated segmentation rules across the environment, isolating the compromised system within seconds.
- Security analysts investigate the incident in a contained environment, confirming the breach was neutralized before data exfiltration or service disruption occurred.
- The Component conducts a post-incident review and further tightens segmentation rules, reinforcing adaptive, real-time access control for future collaborations.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security: Micro-segmentation significantly reduces the attack surface by limiting access to only those resources necessary for each application or User/PE.
- Improved Compliance: Organizations can better align with regulatory requirements by implementing strict access controls and monitoring.
- Dynamic Policy Management: Automation enables real-time adjustments to security policies, thereby enhancing responsiveness to threats.
- Reduced Risk of Lateral Movement: Isolating processes and applications minimizes the potential for unapproved lateral movement within the network.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Firewall as a Service (FWaaS)
- Micro-Segmentation
- Network Access Control (NAC)
- Software-Defined Networking (SDN)
- Virtual Extensible Local Area Network (VXLAN)

Activity 5.4.2 Application and Device Micro-Segmentation

Table 110: Activity 5.4.2 — Application and Device Micro-Segmentation

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components utilize Software-Defined Networking (SDN) or alternative networking approach solution(s) to establish infrastructure meeting the ZT Target-level functionalities—i.e., logical network zones; Role-, Attribute-, and Condition-Based Access Control for users and devices; Privileged Access Management Services for network resources; and policy-based control on API access.	
Predecessor(s)	**Successor(s)**
5.2.3, 5.4.1	3.4.5
Expected Outcomes	
• Assign Role-, Attribute-, and Condition-Based Access Control to users and devices. • Provide PAM services. • Limit access a Per-Identity basis for users and devices. • Create logical network zones. • Support policy control via REST API.	
End State	
SDN or alternative networking approach infrastructure is established across DoW Components, providing robust Role-, Attribute-, and Condition-Based Access Control for PEs and NPEs. PAM services are in place for network resources. Logical network zones are created, and policy-based controls are enforced on API access via REST APIs. This ensures secure and controlled access management, enhancing the overall security posture.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 5.2.3 (Phase Two) – *Segment Flows into Control, Management, and Data Planes* and Activity 5.4.1 (Phase One) – *Implement Micro-Segmentation* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Consider completing 1.2.2 (Phase Two) – *Rule-Based Dynamic Access Part 1* prior to this activity, to leverage User/Person Entity (PE)/Non-Person Entity (NPE) identities for access control.
- Consider completing Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1* or Activity 1.4.2 (Phase Two) – *Implement System and Migrate Privileged Users Part 2* prior to this activity, to leverage the previously established Privileged Access Management (PAM) solution(s).

- Consider completing Activity 1.5.2 (Phase Two) – *Enterprise Identity Lifecycle Management (ILM) Part 1* prior to this activity, to leverage the Enterprise Lifecycle Management Plan.
- Consider completing Activity 3.4.1 (Phase One) – *Resource Authorization Part 1* prior to this activity, to leverage the established authorization gateways.
- Consider completing Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure* prior to this activity, to leverage the Software-Defined Network (SDN) and SDN Application Programming Interfaces (APIs).
- Consider completing Activity 5.3.1 (Phase One) – *Datacenter Micro-Segmentation* prior to this activity, to integrate workload labels defined for access enforcement.
- Continuously monitor and log network traffic across zones for signs of malicious activity, misconfigurations, or unapproved access attempts, ensuring comprehensive visibility and accountability.
- Ensure the segmentation framework can scale as the network grows and adapts to new organizational or mission requirements without compromising security or performance.
- Significant environmental changes can negatively impact Continuity of Operations (COOP)/Disaster Recovery efforts. Ensure the micro-segmented environment still meets the Components recovery objectives.
- Activity 3.4.5 (Phase Three) – *Enrich Attributes for Resource Authorization Part 1* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 111: Implementation Tasks for Activity 5.4.2 — Application and Device Micro-Segmentation

Define environment application and device micro-segmentation objectives and scope.

Collaborate with key stakeholders to further refine environment compartmentalization.

☐ Leverage the Component micro-segmentation architecture, from Activity 5.4.1 (Phase One) – *Implement Micro-Segmentation*, as a starting point.

☐ Define requirements, including:

- Ensure Role-Based Access Controls (RBACs)/Attribute-Based Access Controls (ABACs) are assigned.
  - Leverage the Enterprise Lifecycle Management Plan, from Activity 1.5.2 (Phase Two) – *Enterprise Identity Lifecycle Management (ILM) Part 1*
- Provide PAM services.
  - Leverage the PAM solution, from Activity 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1* or Activity 1.4.2 (Phase Two) – *Implement System and Migrate Privileged Users Part 2*
- Limit access on a per-identity basis for Users/PEs and devices.
  - Leverage Activity 1.2.2 (Phase Two) – *Rule-Based Dynamic Access Part 1*
- Create logical network zones.
  - Leverage Activity 5.2.3 (Phase Two) – *Segment Flows into Control, Management, and Data Planes*
- Support policy control via Representational State Transfer Application Programming Interface (REST API). Leverage the access control points:
  - Authorization gateways, from Activity 3.4.1 (Phase One) – *Resource Authorization Part 1*
  - SDN API, from Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure*
  - Authentication Decision Points and Implement Segmentation Gateways, from Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure*

☐ Identify Component workloads, the units of computation or processing, that run on an environment, which include:

- Applications
- Services
- Processes
- Hosts (virtual or physical)
- Containers

☐ Identify micro-segmentation types that best support the Component's operational requirements and identified workloads. Micro-segmentation types include:

- Application segmentation
- Tier segmentation
- Container segmentation [21]

☐ Create Component Service Offering Matrix:

- Identify interconnections, communication flows, and dependencies between workloads, including required ports and protocols.
- Catalog all running processes and associate them with applications.
- Map processes to specific Users/Person Entities (PEs) and Non-Person Entities (NPEs).
- Document north-south (client-to-server) and east-west (server-to-server) traffic patterns.
- Classify workloads based on sensitivity.
- Identify and document workload labels. Labels will need to be defined by the Component, but would typically include the application name, stage in the development cycle, location, and the workload's role.

Design environment micro-segmentation architecture:

☐ Extend the Component reference architecture to include the micro-segmentation requirements. Leverage the Component Service Offering Matrix to develop a functional inter-workload dependence connectivity map.

☐ Identify micro-segmentation and workload labeling automation solutions that meet the Enterprise/Component requirements. Examples include:

- Hypervisor-based firewalls for virtualized environments.
- Cloud-native security groups for cloud deployments.

Verify and validate micro-segmentation and workload labeling solutions.

Verify and validate functionality/interoperability of micro-segmentation/workload labeling solutions.

☐ Test and confirm that the solution(s) functionality performs as expected within the Component development environment.

☐ Ensure implementation challenges are documented and accounted for in the solution implementation plan.

Deploy micro-segmentation workload labeling and automation.

Workload labeling:

☐ Leverage the workload labeling solution(s) to apply the previously determined labels across all workloads within the Component environment.

☐ Integrate workload labels into the micro-segmentation automation solution(s), and access enforcement solutions, from Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation*.

Implement application/service micro-segmentation.

Application-level policy creation:

☐ Define granular rules for web servers (e.g., allow only Hypertext Transfer Protocol (HTTP)/Hypertext Transfer Protocol Secure (HTTPS) on ports 80/443 to application servers, etc.).

☐ Restrict database access to only application servers using specific ports (e.g., 5432 for PostgreSQL, 3306 for MySQL, etc.).

☐ Implement time-bound access policies for maintenance windows.

☐ Create separate rules for administrative access (e.g., Secure Shell (SSH), Remote Desktop Protocol (RDP), etc.) with stronger authentication requirements.

Application Component isolation:

☐ Separate web, application, and database tiers with different security groups or zones.

☐ Ensure applications traverse API gateways between components and dependencies.

☐ Create separate segments for different microservices within the same application.

Application identity-based controls:

☐ Implement service mesh technology for microservice applications.

☐ Use workload identity/labels rather than Internet Protocol (IP) addresses for policy enforcement.

☐ Configure mutual authentication services (e.g., mutual Transport Layer Security (mTLS), etc.) between application components, where applicable.

Implement host/process-based micro-segmentation.

Host-based segmentation:

☐ Deploy specialized micro-segmentation agents on hosts, where possible.

☐ Use centralized policy management tools for consistency.

☐ Implement Host-Based Intrusion Prevention Systems (HIPS).

☐ Consider Endpoint Detection and Response (EDR) integration, from Activity 2.3.3 (Phase Two) – *Implement Application Control and File Integrity Monitoring (FIM) Tools.*

Emergency access procedures:

☐ Define break-glass procedures for emergency access.

☐ Create fallback policies for disaster recovery scenarios.

☐ Establish a process for temporary policy exceptions.

Process-level access controls:

☐ Configure host systems to control which processes can be executed.

☐ Apply mandatory access control mechanisms to restrict process capabilities.

File system and registry isolation:

☐ Implement process-specific access controls to sensitive file system areas.

Memory protection mechanisms:

☐ Implement Data Execution Prevention (DEP) to prevent code execution in data areas.

☐ Use Control Flow Integrity (CFI) or similar technologies to prevent malicious code from changing the flow of programs.

☐ Restrict Inter-Process Communication (IPC) mechanisms (pipes, sockets, shared memory) between processes.

☐ Implement message queue access controls for processes, where applicable.

Resource usage limitations:

☐ Set process-specific Central Processing Unit (CPU) and memory quotas, where applicable.

☐ Configure Input/Output (I/O) controls to prevent resource monopolization, where applicable.

☐ Apply disk quota limits for process-specific users, where applicable.

☐ Implement resource control technologies where applicable.

Enable container orchestration.

Define and select a container orchestration platform:

☐ Identify mission-specific use cases for container orchestration, such as microservices deployment, batch processing, or application dynamic scaling.

☐ Evaluate the existing Software Development Lifecycle (SDLC) infrastructure, applications, and capability to justify and review the adoption of containerization technologies.

Application deployment:

☐ Define a preferred application deployment model using manifests and charts.

☐ Develop Yet Another Markup Language (YAML) file for K8s to define application resources (e.g., deployment, services, ConfigMaps, etc.) or Helm charts for templating.

☐ Build automation into deployment by developing and implementing Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines. Key principles to consider:

- Horizontal scaling
- Scaling policies
- Cluster configuration

Implement sidecar proxies for microservice telemetry.

Select and deploy sidecar proxies:

☐ Select and implement a sidecar proxy based on operational requirements.

☐ Deploy sidecar proxies as part of container orchestration to simplify deployment.

☐ Enable telemetric collection to capture different metric types (e.g., error rate, latency, logging, etc.). Implement distributed tracing. Key elements to consider:

- Metrics aggregation
- Sidecar containers

Verify and validate Application and Device micro-segmentation.

Validation:

☐ Verify and validate all Component workloads function/work post-segmentation.

☐ Verify and validate that the micro-segmentation solutions have expected granular control.

☐ Ensure unapproved communication to the micro-segmented workload is blocked.

☐ Confirm network visibility allows detection of anomalies and violations.

☐ Test operational performance to identify any latency introduced by segmentation.

Periodically reassess implementation.

Periodic reassessment:

☐ Conduct security assessments using automated scanning tools to verify and validate micro-segmentation controls function properly and identify potential policy drift or vulnerabilities. Conduct at a frequency in accordance with Enterprise/Component requirements. It is strongly recommended to be quarterly.

☐ Schedule traffic pattern analysis to identify changes in application communication flows and update the Component Service Offering Matrix and segmentation policies accordingly; no more than biannually. It is strongly recommended to conduct at a frequency in accordance with Enterprise/Component requirements.

☐ Perform tabletop exercises simulating breach scenarios to test lateral movement restrictions and emergency access procedures. Conduct at a frequency in accordance with Enterprise/Component requirements. It is strongly recommended to be at least annually.

☐ Review logs and monitoring dashboards to identify denied connections that may indicate legitimate business needs requiring policy adjustments. Conduct at a frequency in accordance with Enterprise/Component requirements. It is strongly recommended to be monthly.

☐ Establish a policy review process with stakeholders to align micro-segmentation controls with evolving business requirements and new workloads. Conduct it at a frequency in accordance with Enterprise/Component requirements. It is strongly recommended that it be semi-annual.

☐ Conduct technology assessment to evaluate new micro-segmentation capabilities against current implementation and identify potential improvements. Conduct at a frequency in accordance with Enterprise/Component requirements. It is strongly recommended to be annual.

Summary

This diagram outlines the Activity 5.4.2 (Phase Two) – *Application and Device Micro-Segmentation* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the application and device micro-segmentation policies enforced using Software-Defined Networking (SDN) solutions. It presents strategic insights that drive implementation and expected outcomes, including assigning role, attribute, and condition-based access control to Users/Person Entities (PEs) and devices, providing privileged access management services, and creating logical network zones.

Table 112: Activity 5.4.2 — Application and Device Micro-Segmentation - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are application and device micro-segmentation policies enforced using SDN solutions?

STRATEGIC INSIGHTS
• The Component defines and documents micro-segmentation policies by leveraging the Component micro-segmentation architecture, refining environment compartmentalization, and ensuring proper segmentation of Data, Applications, Assets, and Services (DAAS) across distinct security zones. • The Component demonstrates compliance by identifying Component workloads (e.g., applications, services, hosts, containers, etc.), applying Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), and integrating Privileged Access Management (PAM) solutions to limit per-identity access for users and devices based on Enterprise-defined security requirements. • The Component provides a structured framework for mapping interconnections, communication flows, and dependencies between workloads, enabling logical network zoning and implementing policy control via Representational State Transfer Application Programming Interface (REST API) using authorization gateways, SDN APIs, and authentication decision points for access enforcement. • The Component leverages Component Service Offering Matrix to establish workload labels and segment traffic patterns and deploy hypervisor-based firewalls, cloud-native security groups, and other automation tools to enforce workload boundaries and minimum access requirements in alignment with Enterprise security policies. • The Component ensures continuous verification and validation by monitoring micro-segmentation effectiveness, conducting negative testing to confirm unapproved access is blocked, and executing performance testing to verify and validate that segmentation does not introduce excessive latency, while maintaining compliance with Enterprise-defined periodic assessment intervals.

✓ EXPECTED OUTCOMES

1. Assign Role-, Attribute-, and Condition-Based Access Control to users and devices.
2. Provide PAM services.
3. Limit access on a Per-Identity basis for users and devices.
4. Create logical network zones.
5. Support policy control via REST API.

Activity 5.4.4 Protect Data in Transit

Table 113: Activity 5.4.4 — Protect Data in Transit

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Based on the data flow mappings and monitoring standards provided by DoW Enterprise, policies are enabled by Components to mandate protection of data in transit. Common use cases, such as Coalition Information Sharing, sharing across system boundaries, and protection across architectural components, are included in protection policies.	
Predecessor(s)	**Successor(s)**
None	None
Expected Outcomes	
• Enterprise guidance is provided on protecting Data in Transit. • Protect data in transit during Coalition Information Sharing. • Protect data in transit across system high boundaries. • Integrate data in transit protection across architecture components.	
End State	
Policies are effectively implemented to protect data in transit during coalition information sharing across system high boundaries, and within various architectural components. Data in transit is securely encrypted and monitored ensuring ZT.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Presumption: Enterprise provides data flow mappings and monitoring standards.
- Review existing data flow mapping.
- Monitor standards compliance.
- Implement end-to-end secure communication and sensitive content encryption.
- Adopt strong encryption standards. Consider leveraging industry standards such as Federal Information Processing Standard (FIPS) 140-3 Security Requirements for Cryptographic Modules, as well as emerging National Institute of Standards and Technology (NIST) guidance on Post-Quantum Encryption (PQE) [32].
- Enforce access control policies.
- Enable routine audit and Incident Response (IR).
- Verify and validate interoperability requirements with legacy systems.
- Review alignment with legal and regulatory requirements.
- Assess third-party risk management for approved data sharing.

- Consider completing Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP) Enforcement Point Logging and Analysis*, Activity 4.5.1 (Phase One) – *Implement Data Rights Management (DRM) and Protection Tools Part 1* and Activity 4.5.3 (Phase Two) – *Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1* prior to this activity, to leverage data encryption and rights management capability, criticality, and control markings.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 114: Implementation Tasks for Activity 5.4.4 — Protect Data in Transit

Leverage Enterprise policy guidance to implement data protection in transit.
Acquire and review the Enterprise policies, regulations, and frameworks that ensure the protection of Data in Transit (DiT): ☐ Analyze the guidance or recommendations provided by the Enterprise on data protection while at rest, in transit, and in use to ensure secure information exchange. ☐ Leverage data criticality and control markings (e.g. to include transmission requirements for cross-domain and coalition info sharing use cases), from Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP) Enforcement Point Logging and Analysis* and Activity 4.5.1 (Phase One) – *Implement Data Rights Management (DRM) and Protection Tools Part 1,* to restrict data access, protect DiT, and safeguard data assets. **Identify security standards and technical controls required to ensure the Confidentiality, Integrity, and Availability (CIA) of DiT:** ☐ Apply encryption, cryptographic key management, secure communication protocols, and access control mechanisms. Enforce authentication and authorization requirements previously implemented to restrict data access to only approved Users/Person Entities (PEs)/Non-Person entities (NPEs).
Develop policies to enforce data protection in transit.
Develop encryption requirements: ☐ Leverage the Enterprise Public Key Infrastructure (PKI) and digital certificates to safeguard data assets while in transit. ☐ Review cryptographic algorithms to establish strong encryption specifications. ☐ Develop policies mandating encryption, secure protocols (e.g., Transport Layer Security (TLS), Internet Protocol Security (IPsec), etc.), and authentication mechanisms for secure data transmission.

Enforce authentication and authorization:

☐ Leverage existing Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) implementations to restrict data access to approved users.

☐ Enforce Multi-Factor Authentication (MFA), or alternative, appropriate solution, to require strong authentication mechanisms for accessing sensitive data assets.

Enforce secure communication channels:

☐ Establish Enterprise guidelines for secure information sharing through secure communication channels.

☐ Align with Enterprise-approved communication platforms.

☐ Periodically validate that channels remain secure.

Establish data integrity:

☐ Enforce hashing algorithms to safeguard sensitive data assets and ensure data integrity.

☐ Enable self-detection and automated response (e.g. policy revocation, session teardown, etc.) to data tampering attempts.

Leverage previously developed Data Loss Prevention (DLP) and Data Rights Management (DRM) to enforce data protection mechanisms for information sharing.

Understand approved information sharing requirements:

☐ Identify the types of data to be shared and their sensitivity levels.

☐ Define the scope of the Information Sharing Agreement (ISA) and partnering objectives.

☐ Identify interoperability requirements.

- Comply with Enterprise and regulatory mandates for information sharing compliance.
- Identify existing and future Component-level interoperability operational needs.

Review and refine mechanisms:

☐ Periodically review the protection mechanisms to ensure alignment with evolving requirements.

☐ Incorporate lessons learned from operations and audits to improve system effectiveness.

☐ Leverage data encryption and rights management capability, criticality, and control markings, from Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP) Enforcement Point Logging and Analysis*, Activity 4.5.1 (Phase One) – *Implement Data Rights Management (DRM) and Protection Tools Part 1*, and Activity 4.5.3 (Phase Two) – *Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1*, to restrict data access, protect DiT and safeguard data assets.

Enable data integrity testing, verification, and validation.

Configure monitoring and logging:

☐ Enable monitoring tools to oversee data transfers across system-high boundaries.

☐ Maintain audit logs for compliance and incident investigation.

Integrate monitoring and auditing tools:

☐ Deploy monitoring systems to detect anomalies or unapproved access during data transmission.

☐ Enable alerting on anomalies or policy violations.

☐ Enable logging and auditing for compliance and IR purposes.

Test, verify, and validate integration:

☐ Conduct end-to-end testing to ensure mechanisms function seamlessly across components.

☐ Verify and validate data security under operational conditions and simulated environments.

Test, verify, and validate Implementation:

☐ Verify and validate data transfer security against established security requirements.

Summary

This diagram outlines the Activity 5.4.4 (Phase Two) – *Protect Data in Transit* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on how the data in transit is protected across system boundaries using segmentation policies. It presents strategic insights that drive implementation and expected outcomes, including the segmentation of host-level processes for security policies, as well as supporting real-time access decisions and policy changes.

Table 115: Activity 5.4.4 — Protect Data in Transit - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is data in transit protected across system boundaries using segmentation policies?

STRATEGIC INSIGHTS
• The Component defines and documents policies ensuring the Confidentiality, Integrity, and Availability (CIA) of Data in Transit (DiT) by aligning with Enterprise policy guidance, regulations, and frameworks, leveraging encryption, secure communication protocols, and authentication mechanisms. • The Component demonstrates compliance by applying cryptographic key management, enforcing Multi-Factor Authentication (MFA), and utilizing Enterprise-approved Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) to restrict data access to approved Users/Person Entities (PEs)/Non-Person Entities (NPEs). • The Component provides an Enterprise-approved framework for enforcing encryption requirements, ensuring data integrity through the use of hashing algorithms, and leveraging Data Loss Prevention (DLP) and Data Rights Management (DRM) to prevent unapproved access and safeguard sensitive data assets. • The Component leverages DLP Enforcement Point Logging and Analytics, as well as DRM protection tools developed in prior activities, to enforce data protection mechanisms for secure information sharing, ensuring compliance with approved Information Sharing Agreements (ISAs). Additionally, it utilizes DRM protection tools developed in prior activities to enforce data protection mechanisms for secure information sharing. This ensures compliance with approved ISAs and regulatory mandates. • The Component ensures ongoing security by configuring monitoring and logging tools, integrating audit mechanisms, and conducting end-to-end security verification and validation to continuously assess DiT security posture, detect anomalies, approved access, and verify and validate compliance under operational and simulated conditions.

EXPECTED OUTCOMES

1. Enterprise guidance is provided on protecting DiT.
2. Protect data in transit during Coalition Information Sharing.
3. Protect data in transit across system high boundaries.
4. Integrate data in transit protection across architecture components.

Automation and Orchestration Pillar

Capability 6.1 Policy Decision Point (PDP) and Policy Orchestration

Table 116: Capability 6.1 — Policy Decision Point (PDP) and Policy Orchestration

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
6 - Automation and Orchestration	6.1 - Policy Decision Point (PDP) and Policy Orchestration
Description	
DoW Components initially collect and document all rule-based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. DoW Components mature this capability by establishing PDPs and PEPs (including the Next-Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy.	
Impact to ZT	
PDPs and PEPs ensure proper implementation of DAAS access policies to users or endpoints that are properly connected (or denied access) to requested resources.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component initiates a comprehensive review of its existing Data, Applications, Assets, and Services (DAAS) access procedures, collecting and documenting all rule-based policies to create a centralized policy inventory.
- Policies are updated to align with Zero Trust (ZT) principles, ensuring granular access control rules based on User/Person Entity (PE) identity, Non-Person Entity (NPE) compliance, and data sensitivity.
- A Policy Decision Point (PDP) is established to serve as the central authority for evaluating and enforcing DAAS access policies dynamically, embodying the ZT approach by continuously assessing trust levels before granting access.
- Policy Enforcement Points (PEPs), including a Next-Generation Firewall (NGFW), are deployed to enforce access decisions made by the PDP, monitoring and controlling traffic to DAAS resources.
- A User/PE attempts to access a DAAS resource from an unmanaged NPE. The PEP consults the PDP, which evaluates the request against predefined policies and denies access due to the NPE’s non-compliance.

- The Component develops an Enterprise Security Profile that defines the attributes, risk tolerances, and access controls required for various User/PE roles, NPEs, and data types.
- Real-time monitoring and automation are integrated into the PDP and PEP framework, enabling the system to dynamically adapt policies in response to emerging threats or changes in User/PE or NPE status.
- During a simulated attack, the PDP detects an anomaly in a User/PE's access pattern and instructs the PEP to terminate the connection, preventing unauthorized access to critical DAAS resources.
- Policy orchestration solutions provide detailed logs and analytics on access decisions, enabling security teams to refine policies and ensure they remain effective over time.
- By leveraging PDPs and PEPs in conjunction with updated policies and automation, the Component ensures secure, monitored, and dynamic access to DAAS resources.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security: By implementing PDPs and PEPs, Components can enforce strict access controls, reducing the risk of unapproved access to sensitive resources.
- Dynamic Policy Adaptation: Real-time monitoring allows for policies to adapt swiftly to emerging threats, ensuring ongoing protection.
- Centralized Policy Management: A centralized policy inventory simplifies the management and updating of access rules, promoting consistency and compliance.
- Improved Compliance: Aligning with ZT principles enables Components to meet regulatory requirements and standards, thereby enhancing their overall compliance posture.
- Operational Efficiency: Automating access decisions reduces the burden on security teams, allowing them to focus on strategic initiatives rather than manual policy enforcement.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Attribute-Based Access Control (ABAC)
- Identity and Access Management (IAM)
- Identity-Based Access Control (IBAC)
- Policy Decision Points (PDPs)
- Policy Enforcement Points (PEPs)
- Role-Based Access Control (RBAC)
- Structured Threat Information eXpression (STIX) protocols
- Trusted Automated Exchange of Intelligence Information (TAXII)

Activity 6.1.3 Enterprise Security Profile Part 1

Table 117: Activity 6.1.3 — Enterprise Security Profile Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Enterprise security profile rules initially cover the User, Data, Network & Environment, and Device pillars. Existing Component security profile rules are integrated for non-mission/task DAAS access following an iterative approach to tuning access.	
Predecessor(s)	**Successor(s)**
6.1.2	6.1.4
Expected Outcomes	
• Enterprise profile rules are created to access DAAS using capabilities from User, Data, Network & Environment, and Device pillars. • Component profile rules are integrated with the Enterprise profile rules using a standardized approach. • Service catalog and/or CMDB exists with ZT components; at a minimum PDP(s), PEP(s), and PIP(s) details are inventoried.	
End State	
The patterns of behavior are established for necessary outcomes of access control at the Enterprise level.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 6.1.2 (Phase One) – *Organization Access Profile* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Leverage Application Programming Interfaces (APIs), discovery solutions, and integrations with existing security solutions to automatically populate and update the Service Catalog/Configuration Management Database (CMDB), reducing manual effort and minimizing data inconsistencies, where applicable.
- Define a consistent strategy for cataloging ZT solutions (e.g., Policy Decision Points (PDPs), Policy Enforcement Points (PEPs), Policy Information Points (PIPs), etc.) with attributes like ownership, policy enforcement role, and integration dependencies, to ensure clarity and interoperability.
- Implement processes including version control, periodic audits, and automated alerts to maintain accuracy as security requirements and infrastructure evolve.

- When establishing access profiles, it is important that the Component is aligned with the Enterprise; however, only the Component will be able to address the granularity of their particular environment(s).
- Activity 6.1.4 (Phase Three) – *Enterprise Security Profile Part 2* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 118: Implementation Tasks for Activity 6.1.3 — Enterprise Security Profile Part 1

Develop Enterprise and Component security profile rules to refine policies utilizing the User, Data, Network and Environment, and Device Pillar Capabilities to access Data, Applications, Assets, and Services (DAAS).
Complete Activity 6.1.2 (Phase One) – *Organization Access Profile,* to obtain Enterprise and Component security profile rules: ☐ Leverage established Enterprise profile rules for DAAS access using the established User/Person Entity (PE)/Non-Person Entity (NPE) lists, from Activity 6.1.2 (Phase One) – *Organization Access Profile.* ☐ Utilize the established Enterprise profile rules to develop security profiles at the Component level. ☐ Test, verify, and validate security profile rule efficacy in a controlled environment, where applicable. ☐ Document security profile rules and ensure consistency with ZT principles. Identify any potential conflicts or gaps between the security profile and ZT goals, like Least Privilege access, continuous verification, and micro-segmentation. Describe how any identified discrepancies will be addressed.
Integrate Enterprise profile rules with Component profile rules for DAAS access.
Manage DAAS access through Enterprise and Component profile rules: ☐ Inventory existing Component security profile rules and assess alignment with Enterprise policies. ☐ Standardize integration processes for merging Component rules into the Enterprise environment. ☐ Implement an iterative tuning approach to refine rule enforcement without disrupting access. ☐ Monitor and document rule efficacy, adjusting configurations as needed.
Establish a standardized approach for profile rule management.
Standardize profile rule management across the Component environment: ☐ Define Component processes for managing Component profile rules.

☐ Define rules based on operational processes.

☐ Develop version control and change management procedures for rule updates, while maintaining rollback capability in case of rule failure.

☐ Automate rule application and enforcement using security orchestration tools, where possible.

☐ Document and refine rule management processes, to include dependency mapping.

Maintain a Service Catalog and/or CMDB with ZT devices for PDPs, PEPs, and PIPs.

Select and integrate a Service Catalog/CMDB with existing security solutions:

☐ Identify and leverage key ZT components, including PDP, PEP, and PIP details, where applicable.

☐ Develop, populate, and continuously maintain a Service Catalog/CMDB to provide comprehensive visibility into all ZT elements (e.g., attributes, relationships, dependencies, etc.).

☐ Establish an automated process for updating the Service Catalog/CMDB as the Component environment evolves.

☐ Ensure Service Catalog/CMDB integration with security monitoring and Incident Response (IR) solutions (e.g., PDPs, PEPs, PIPs, etc.), that allows for querying during IR to trace policy pathway.

Summary

This diagram outlines the Activity 6.1.3 (Phase Two) – *Enterprise Security Profile Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development and integration of Enterprise security profile(s) into existing organizational security profiles for non-mission/task Data, Applications, Assets, and Services (DAAS) access. It presents strategic insights, driving implementation and expected outcomes that include the creation of Enterprise profile rules to access DAAS using capabilities from User, Data, Network, and Device pillars.

Table 119: Activity 6.1.3 — Enterprise Security Profile Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the Enterprise security profile developed to integrate existing organizational security profiles for non-mission/task DAAS access?

STRATEGIC INSIGHTS
• The Component defines security profile rules for DAAS by leveraging User, Data, Network & Environment, and Device Pillar capabilities, ensuring alignment with Enterprise policies. • The Component demonstrates compliance by integrating Enterprise and Component profile rules, refining enforcement through iterative tuning, and validating rule efficacy in controlled environments. • The Component provides evidence through standardized profile rule management, version control, and automated enforcement using security orchestration solutions. • The Component leverages a Service Catalog/Configuration Management Database (CMDB) to maintain visibility into ZT components, including Policy Decision Points (PDPs), Policy Enforcement Points (PEPs), and Policy Information Points (PIPs). • The Component ensures ongoing compliance by continuously updating the Service Catalog/CMDB, integrating with security monitoring and Incident Response (IR) solutions, and adapting to evolving security requirements.

EXPECTED OUTCOMES
1. Enterprise profile rules are created to access DAAS using capabilities from User, Data, Network & Environment, and Device pillars. 2. Component profile rules are integrated with the Enterprise profile rules using a standardized approach. 3. Service catalog and/or CMDB exists with ZT components; at a minimum PDP(s), PEP(s), and PIP(s) details are inventoried.

Capability 6.2 Critical Process Automation

Table 120: Capability 6.2 — Critical Process Automation

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
6 - Automation and Orchestration	6.2 - Critical Process Automation
Description	
DoW Components employ automation methods, such as RPA, to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles.	
Impact to ZT	
Response time and capability is increased with orchestrated workflows and risk management processes.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component conducts a task automation analysis to identify repetitive and predictable tasks across critical functions such as data enrichment, security controls, and Incident Response (IR) workflows.
- Robotic Process Automation (RPA) is implemented to handle routine tasks like log analysis, vulnerability scanning, and incident ticket creation, freeing up analysts to focus on higher-value activities.
- An automated workflow is established to enrich security alerts with contextual data, such as Non-Person Entity (NPE) compliance, User/Person Entity (PE) identity, and threat intelligence, improving incident prioritization.
- During a phishing attack simulation, the automation system detects a suspicious email, isolates it, and extracts Indicators of Compromise (IoC) for further analysis without manual intervention.
- The IoC are automatically cross-referenced with external threat intelligence feeds and flagged for inclusion in the Component’s threat database.
- Security controls, such as firewall rules and endpoint protection configurations, are dynamically updated in response to the detected threat, reducing exposure time.
- An IR workflow is triggered, orchestrating automated tasks like quarantining affected endpoints, notifying stakeholders, and generating a detailed incident report.

- The automation framework integrates with Enterprise workflow solutions to ensure that all critical steps, including manual approvals and escalation protocols, are completed seamlessly.
- Continuous monitoring and analysis of automated processes provide insights into their effectiveness, enabling the Component to optimize workflows and reduce response times further.
- By employing automation methods like RPA and orchestrating critical workflows, the Component improves response times, enhances risk management and system security engineering practices.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Increased Efficiency: Automating repetitive tasks enables analysts to focus on higher-value activities, thereby improving overall productivity.
- Improved IR: Automated workflows enhance the speed and effectiveness of IR, reducing potential damage from threats.
- Enhanced Accuracy: Automation minimizes human error in critical processes, leading to more reliable outcomes in security operations.
- Better Resource Allocation: By automating routine tasks, Components can allocate resources more effectively, ensuring that skilled personnel are engaged in strategic initiatives.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Automation Frameworks and Libraries
- Automation Orchestration solutions
- Continuous Integration and Continuous Delivery (or Deployment) (CI/CD) Pipelines
- Disaster Recovery and Business Continuity solutions
- Managed Detection and Response (MDR)

Activity 6.2.2 Enterprise Integration and Workflow Provisioning Part 1

Table 121: Activity 6.2.2 — Enterprise Integration and Workflow Provisioning Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Enterprise establishes baseline integration and interoperability within the Security Orchestration, Automation, and Response (SOAR) solution, required to enable ZTA Target-level functionality, where actionable and relevant information resides. Components identify instrument, integration, and interoperability points and prioritization per the Enterprise baseline. The necessary integrations in User, Device, Application & Workload, and Network & Environment pillars to automate IR functions are completed.	
Predecessor(s)	**Successor(s)**
None	6.2.3
Expected Outcomes	
• DoW Enterprise establishes baseline integration and interoperability with SOAR to enable ZT Target-level functionality. • Components identify key integrations. • Components implement Enterprise integration and interoperability for critical services. • Components identify recovery and protection requirements.	
End State	
Critical integrations occur to meet key services and enable recovery and protection capabilities.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Consider completing Activity 6.5.2 (Phase One) – *Implement Security Orchestration, Automation, and Response (SOAR) Tools* prior to this activity, to select and effectively implement Security Orchestration, Automation, and Response (SOAR) solutions.
- A comprehensive Disaster Recovery Plan (DRP) must be in place with automated verification and validation, and regular testing to ensure business continuity and minimize operational risks. A failure to implement or maintain a DRP compromises security, data integrity, and recovery capabilities.
- Ensure alignment with the Enterprise security architecture by verifying and validating that SOAR integrations support Zero Trust (ZT) Target-level requirements and adhere to established Enterprise policies and procedures.

- Verify and validate system interoperability and Application Programming Interface (API) compatibility across security solutions (e.g., Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Identity and Access Management (IAM), Network Access Control (NAC), etc.) to prevent integration failures and ensure seamless data exchange for automated Incident Response (IR).
- Assess operational impact and resource availability by confirming that network bandwidth, scalability, compute capacity, and personnel expertise are sufficient to support SOAR deployment, orchestration, and ongoing maintenance.
- Activity 6.2.3 (Phase Three) – *Enterprise Integration and Workflow Provisioning Part 2* is defined by the Department of War (DoW) ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 122: Implementation Tasks for Activity 6.2.2 — Enterprise Integration and Workflow Provisioning Part 1

Establish baseline SOAR integration and interoperability at the ZT Target-level.
Define baseline and integration requirements for SOAR: ☐ Define baseline integration requirements based on ZT Target-level functionality, and Enterprise/Component security policies. ☐ Identify key data sources and security solutions (e.g., SIEM, EDR, NAC, etc.) that require integration with SOAR. ☐ Develop standardized data formats in alignment with existing schema, logging mechanisms, and API communication protocols for interoperability. ☐ Conduct initial functional testing to verify and validate baseline integrations and ensure SOAR can ingest actionable security data. ☐ Document and refine integration for IR automation and security operations.

Identify key integration points for enabling ZT for critical services.

Determine key integration points across ZT Pillars:

☐ Map critical integration points, to include Policy Decision Point (PDP)/Policy Enforcement Point (PEP)/ Policy Information Point (PIP) relationships, across the User, Device, Application and Workload, and Network and Environment pillars.

☐ Prioritize integrations based on their potential to enhance ZT's security posture. Consider the following factors when determining integration priority:

- Risk Reduction: Minimizing the attack surface. Focus on integrating services with high-risk exposure first.
- Operational Needs and ZT Enablement: Prioritize integrations that support core operational needs while simultaneously advancing ZT principles.
- Alignment with Enterprise SOAR Baseline: Leverage the Enterprise SOAR baseline to streamline integration efforts and ensure interoperability. This promotes consistent security policy enforcement and automated responses to threats, further strengthening the ZT framework.

☐ Perform a gap analysis to identify process deficiencies, required data, response capability gaps (e.g. data fidelity, timestamp integrity), and automation opportunities for implementing ZT principles.

☐ Collaborate with the Enterprise to define security event triggers, response actions, and policy enforcement criteria.

☐ Verify and validate integration performance through controlled testing and iterative refinements.

Leverage Enterprise integration in User, Device, Application and Workload, and Network pillars to automate IR functions.

Integrate security solution(s) for IR automation:

☐ Deploy SOAR integration for bidirectional exchange with EDR, SIEM, Identity and Access Management (IAM) (e.g., Identity, Credential, and Access Management (ICAM), etc.), and network segmentation solutions.

☐ Configure automated strategies for threat detection, IR, and recovery based on ZT policies.

☐ Establish secure communication channels (e.g., API authentication, secure tunnels, etc.) for real-time data sharing between SOAR and security solutions, where applicable.

- Authentication should occur via tokens or certificates, which must be actively managed to ensure they are valid, approved, and not revoked.

☐ Monitor integration performance, fine-tune automation workflows, and conduct testing to ensure system resilience.

☐ Monitor and optimize solutions for continuous improvement, ensuring integrations evolve with new security threats and Enterprise needs.

Create and prepare to implement DRP, as needed.
Define DRP that leverages SOAR for IR and recovery: ☐ Enterprise and Component collaborate to develop DRP that leverages SOAR for IR and recovery requirements in accordance with Enterprise policies and procedures. ☐ Implement SOAR-driven recovery mechanisms, including containment, rollback, and system restoration procedures. ☐ Verify and validate data integrity across integration points before and after data sharing. ☐ Establish continuous monitoring, verification, and validation processes to ensure compliance with recovery and protection objectives. ☐ Conduct testing to refine recovery strategies and assess IR and recovery efficacy.

Summary

This diagram outlines the Activity 6.2.2 – *Enterprise Integration and Workflow Provisioning Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the integration of Security Orchestration, Automation, and Response (SOAR) solutions across the Enterprise. It presents strategic insights driving implementation and expected outcomes that include establishment of baseline integration and interoperability with SOAR to enable Target-level Zero Trust Architecture (ZTA) and identification of key integrations.

Table 123: Activity 6.2.2 — Enterprise Integration and Workflow Provisioning Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the full Enterprise integration of SOAR solutions implemented and key integrations identified?

STRATEGIC INSIGHTS
• The Component integrates the Enterprise baseline requirements for SOAR and automating Incident Response (IR) workflows using cybersecurity solutions such as Security Information and Event Management (SIEM), Threat Intelligence Platforms (TIPs), and Endpoint Detection and Response (EDR). • The Component establishes automated workflows and security policies to enhance threat detection, response, and recovery by leveraging cryptographic techniques, dynamic SOAR integrations, and interoperability across Policy Information Points (PIPs), Policy Decision Points (PDPs), and Policy Enforcement Points (PEPs). • The Component ensures secure and automated communication by implementing encryption for data in transit and at rest, and optimizing SIEM telemetry for real-time operational insights and root cause analysis. • The Component develops critical service interoperability plans, incorporating Application Programming Interfaces (APIs), automation solutions, and modular architectures to enable seamless interaction between identity, endpoint, and network solutions, while implementing phased testing, stress validation, and continuous monitoring to ensure compliance with Enterprise requirements. • The Component automates IR and disaster recovery processes through iterative testing and tabletop exercises supported by SOAR workflows, threat analytics, and Disaster Recovery Plans (DRPs), ensuring operational resilience, continuous improvement, and alignment with evolving regulatory and cybersecurity requirements.

✓ EXPECTED OUTCOMES

1. DoW Enterprise establishes baseline integration and interoperability with SOAR to enable ZT Target-level functionality.
2. Components identify key integrations.
3. Components implement Enterprise integration and interoperability for critical services.
4. Components identify recovery and protection requirements.

Capability 6.3 Machine Learning (ML)

Table 124: Capability 6.3 — Machine Learning (ML)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
6 - Automation and Orchestration	6.3 - Machine Learning (ML)
Description	
DoW Components employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.	
Impact to ZT	
Response time and capability is increased with orchestrated workflows and risk management processes.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component implements Machine Learning (ML) solutions to support critical functions, including Incident Response (IR), anomaly detection, User/Person Entity (PE)/Non-Person Entity (NPE) baselining, and data tagging.
- ML algorithms are trained on historical incident data, enabling them to identify patterns and suggest automated responses for future incidents.
- User/PE behavior baselining is then introduced, with ML analyzing access patterns and activity logs to establish normal behaviors and detect deviations in real time.
- ML-based data tagging solutions are integrated to classify new datasets dynamically, applying appropriate sensitivity and access labels without manual intervention.
- The Component then integrates ML outputs into the Security Orchestration, Automation, and Response (SOAR) framework, enabling real-time adjustments to security policies and workflows based on evolving threats.
- Insights generated by the ML solution are continuously analyzed to refine models, improving detection accuracy and reducing false positives.
- Later, a sophisticated insider threat emerges when a contractor with legitimate system access begins exfiltrating sensitive data using methods that mimic normal user behavior patterns

- The threat actor leverages knowledge of business processes to schedule data transfers during peak usage times and utilizes legitimate tools, initially evading traditional signature-based detection systems
- The ML-enhanced detection solution successfully identifies and contains the insider threat within hours of detecting the anomalous behavior pattern, automatically implementing additional access controls and alerting security teams before sensitive data could be exfiltrated.
- By employing ML to enhance anomaly detection, User/PE/NPE baselining, and automated responses, the Component strengthens its overall Zero Trust (ZT) posture by providing continuous verification of User/PE/NPE activities and automated policy enforcement across all Data, Assets, Applications, and Services (DAAS).

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Improved Incident Response Times: Faster detection and automated responses lead to quicker resolution of security incidents.
- Enhanced Risk Management: Continuous analysis and adjustment of security policies based on real-time data improve overall risk management strategies.
- Reduction in False Positives: Ongoing refinement of ML models increases detection accuracy, minimizing unnecessary alerts and resource allocation.
- Dynamic Data Classification: Automated data tagging ensures that sensitive information is appropriately classified without manual intervention, streamlining compliance and access control.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Artificial Intelligence/Machine Learning (AI/ML)-Based Tagging and User Behavior Analysis
- Behavioral Analytics solutions
- Cyber Threat Modeling
- Data Standardization
- User and Entity Behavior Analytics (UEBA)

Activity 6.3.1 Implement Data Tagging and Classification Machine Learning (ML) Tools

Table 125: Activity 6.3.1 — Implement Data Tagging and Classification Machine Learning (ML) Tools

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components utilize existing Data Tagging and Classification standards and requirements to integrate Machine Learning (ML) solution(s)/capability as needed. ML solution(s) is implemented by Components, and existing tagged and classified data repositories are used to establish baselines. ML solution(s) applies data tags in a supervised approach to continually improve analysis.	
Predecessor(s)	**Successor(s)**
4.2.1	4.3.4, 4.3.5
Expected Outcomes	
• Components implement ML capabilities with data tagging and classification.	
End State	
Machine learning solution is acquired, trained, and implemented in accordance with DoW established Data Tagging and Classification tools. Machines are trained on a high-quality subset of data developed under activity 4.3.1 with human oversight and assessment.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 4.2.1 (Phase One) – *Define Data Tagging Standards* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Consider completing Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools* prior to this activity, to create the Global Key Access Store before completing this activity.
- Consider completing Activity 5.4.4 (Phase Two) – *Protect Data in Transit* prior to this activity, to access Component data handling protocols.
- Components should closely control access to data and models to improve the overall Enterprise/Component cybersecurity posture.
- Activity 4.3.4 (Phase Three) – *Automated Data Tagging and Support Part 1* and Activity 4.3.5 (Phase Four) – *Automated Data Tagging and Support Part 2* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 126: Implementation Tasks for Activity 6.3.1 — Implement Data Tagging and Classification Machine Learning (ML) Tools

Utilize existing data tagging, classification standards, and requirements to select Machine Learning (ML) solutions.
Review existing standards and requirements: ☐ Leverage documentation and review existing data tagging, classification standards, and requirements to select appropriate ML solutions. ☐ Identify existing tagging schemas (e.g., metadata, labels, security levels, etc.) to determine their suitability for informing ZT Access Control policies and driving automated tagging with the chosen ML solution. ☐ Ensure the ML solution complies with Component security objectives and requirements [10]. **Identify relevant data sets:** ☐ Leverage the Component-federated tag library, from Activity 4.2.1 (Phase One) – *Define Data Tagging Standards,* which contains tagged and classified data used within the Component environment, ensuring tagging is standardized. ☐ Utilize the Global Key Access Store, a centralized data tag repository and single source of truth for all tags, from Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools.* ☐ Determine data formats (e.g., structured, unstructured, images, text, etc.) and assess their compatibility with ML solutions. ☐ Ensure data is validated, accurately tagged, and classified according to standards, from Activity 4.2.1 (Phase One) – *Define Data Tagging Standards.* **Determine an appropriate ML solution based on compatibility and requirements:** ☐ Select the appropriate ML solution (e.g., supervised learning, reinforcement learning, etc.) based on data availability and classification needs. ☐ Evaluate whether the ML solution supports classification constraints (e.g., need for role-based access to specific data types). ☐ Verify and validate that the ML solution can accommodate Component-determined labeling and classification. ☐ Confirm ML systems comply with Component data handling protocols, from Activity 5.4.4 (Phase Two) – *Protect Data in Transit.*

Implement ML solution(s) and use existing tagged and classified data repositories to establish baselines.

Deploy ML solution:

☐ Run the ML model in a test environment before deploying it in operational workflows to ensure performance and compatibility.

☐ Integrate ML solution with existing Component data management systems, where applicable.

Ingest and process data for ML solutions:

☐ Ingest and process data in the ML solution from the Component-federated tag library and the Global Key Access Store (e.g., data normalization, data transformation, feature engineering, etc.).

☐ Verify and validate that the ML solution maintains existing data tags and classifications [33].

Establish performance baselines:

☐ Define Key Performance Indicators (KPIs) for tagging accuracy, precision, false negative rate, recall, and overall model efficiency.

☐ Compare ML outputs to existing labels and classifications to determine deviations.

☐ Identify categorize, and document misclassifications (e.g., annotation error, system bias, model drift, etc.) in comprehensive error reports in preparation for model refinement.

- If errors are detected, restore to a known good state.

Refine ML models using ingested data:

☐ Adjust parameters and data preprocessing techniques to improve performance.

☐ Retrain the model using a subset of verified and validated data to improve generalization, where applicable.

Verify and validate implemented data management/ML solutions:

☐ Conduct manual verification of ML-generated classifications against ground-truth labels.

☐ Confirm that the data management/ML solutions are operational and performing as expected.

- If errors are detected, restore to a known good state.

Use ML solution(s) to apply data tags in a supervised approach to continually improve analysis.

Train ML solution with supervised learning to improve analysis results:

☐ Select an approved, validated representative training dataset containing tagged and classified examples from existing data repositories.

☐ Use Enterprise and Component-approved supervised learning techniques to map input data to correct tags and classification labels.

☐ Implement cross-validation techniques to avoid errors (e.g., overfitting, bias-variance, data leakage, etc.).

Apply automated data tagging:

☐ Configure ML models to apply classification tags to new data.

☐ Integrate real-time tagging within Component data processing pipelines.

☐ Implement confidence scoring mechanisms to flag uncertain classifications for review.

Monitor performance through Subject Matter Experts (**SMEs) and automated reviews:**

☐ Track and document tag and classification accuracy metrics over time.

☐ Create a workflow where SMEs review and approve ML-generated tags and classifications.

☐ Establish automated alerting for tagging and classification anomalies.

☐ Implement a feedback loop where incorrect classifications are fed back into training datasets.

Iterate and improve the ML solution:

☐ Retrain models in an iterative approach using corrected datasets from human reviews.

☐ Regularly update training datasets to reflect evolving tagging and classification patterns.

- If errors are detected, restore to a known good state.

Ensure compliance and security:

☐ Conduct periodic compliance reviews to ensure the ML solution follows Enterprise and Component tagging and classification standards and requirements.

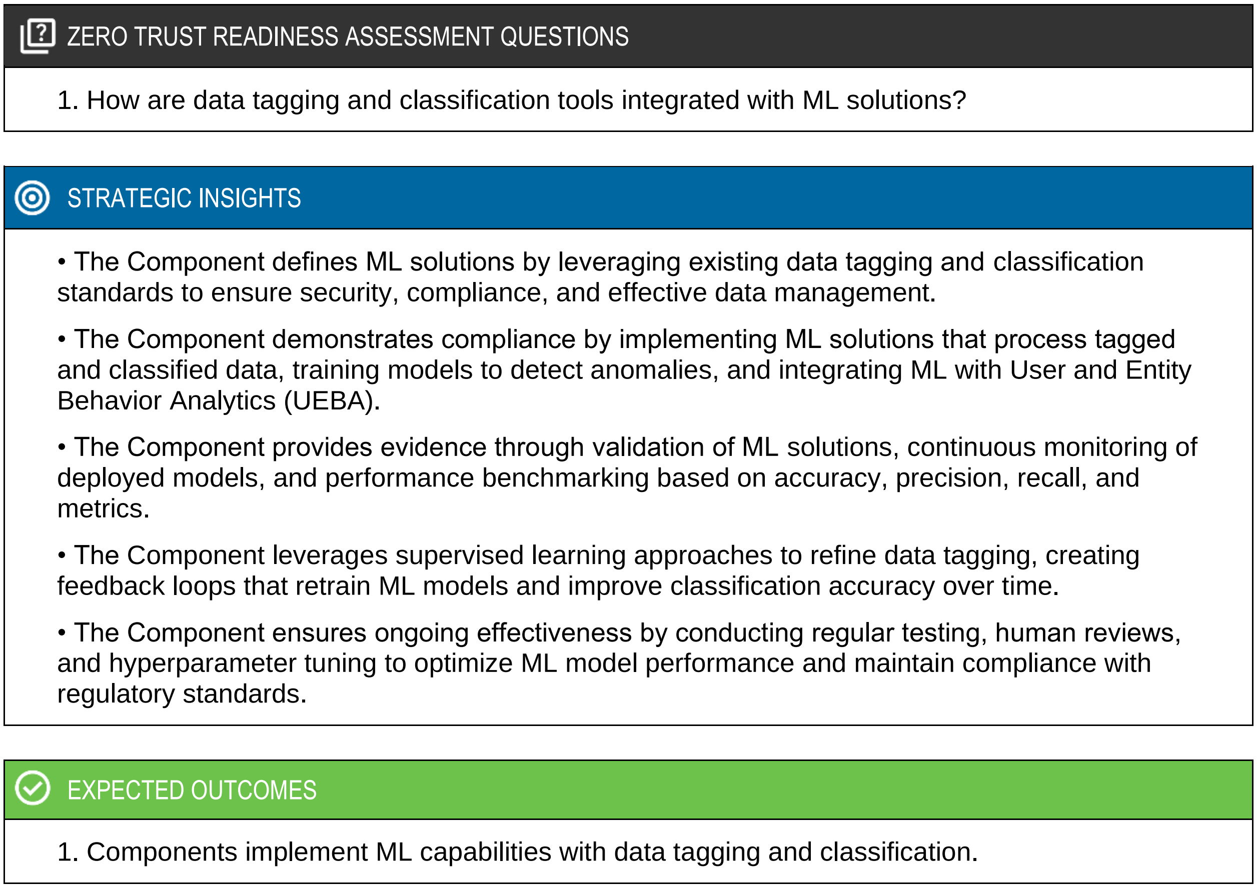
☐ Implement Role-Based Access Controls (RBACs) to prevent unapproved classification modifications.

☐ Maintain audit logs of ML tagging (e.g., who/what applied the tag) and classification activity for review and accountability.

Summary

This diagram outlines the Activity 6.3.1 (Phase Two) – *Implement Data Tagging and Classification Machine Learning (ML) Tools* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on data tagging and classification tool integration with Machine Learning (ML) solutions. It presents strategic insights driving implementation and expected outcomes that include implementation of ML capabilities with data tagging and classification.

Table 127: Activity 6.3.1 — Implement Data Tagging and Classification Machine Learning (ML) Tools - Workflow



ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How are data tagging and classification tools integrated with ML solutions?

STRATEGIC INSIGHTS

• The Component defines ML solutions by leveraging existing data tagging and classification standards to ensure security, compliance, and effective data management.

• The Component demonstrates compliance by implementing ML solutions that process tagged and classified data, training models to detect anomalies, and integrating ML with User and Entity Behavior Analytics (UEBA).

• The Component provides evidence through validation of ML solutions, continuous monitoring of deployed models, and performance benchmarking based on accuracy, precision, recall, and metrics.

• The Component leverages supervised learning approaches to refine data tagging, creating feedback loops that retrain ML models and improve classification accuracy over time.

• The Component ensures ongoing effectiveness by conducting regular testing, human reviews, and hyperparameter tuning to optimize ML model performance and maintain compliance with regulatory standards.

EXPECTED OUTCOMES

1. Components implement ML capabilities with data tagging and classification.

Capability 6.6 Application Programming Interface (API) Standardization

Table 128: Capability 6.6 — Application Programming Interface (API) Standardization

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
6 - Automation and Orchestration	6.6 – Application Programming Interface (API) Standardization
Description	
DoW establishes and enforces enterprise-wide programmatic interface (e.g., API) standards; all non-compliant APIs are identified and replaced.	
Impact to ZT	
Standardizing APIs across the department improves application interfaces, enabling orchestration, and enhancing interoperability.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component conducts a tool compliance analysis to identify all existing Application Programming Interfaces (APIs) and evaluate their adherence to Enterprise-wide programmatic interface standards.
- A catalog of non-compliant APIs is created, prioritizing those that pose the highest security or operational risks for replacement or remediation.
- Standardized API schemas and calls are defined, ensuring all new and existing APIs meet the Component’s interoperability, security, and orchestration requirements.
- Developers are trained on the standardized API framework, ensuring they understand the required specifications and best practices for building compliant interfaces.
- An automated solution is deployed to monitor API traffic, flagging non-compliant API calls for review and notifying developers of policy violations.
- A legacy API used for a critical application is flagged as non-compliant. The Component replaces it with a standardized API, ensuring seamless integration and improved security controls.
- During a simulated attack, the standardized API framework detects and blocks a malformed API request, preventing the attacker from exploiting a vulnerability in the interface.

- Standardized APIs enable streamlined orchestration across applications, improving workflow automation and reducing development complexity for integrating systems.
- Regular audits of API compliance ensure that new APIs are built according to standardized schemas and that existing APIs are updated as needed to maintain compliance.
- By enforcing enterprise-wide API standards, the Component enhances application interfaces, strengthens security, and ensures consistent interoperability across the department.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security: By enforcing standardized API protocols, Components can significantly reduce vulnerabilities and improve their security posture.
- Improved Interoperability: Standardized APIs facilitate seamless integration between different systems and applications, enhancing overall operational efficiency.
- Reduced Development Complexity: Developers benefit from clear guidelines and standards, which simplify the process of creating and maintaining APIs.
- Streamlined Workflow Automation: With standardized APIs, Components can automate workflows more effectively, leading to faster and more reliable processes.
- Consistent Compliance Monitoring: Regular audits and compliance checks ensure that all APIs adhere to established standards, reducing the risk of non-compliance and associated penalties.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- API Management solutions
- Cyber Threat Intelligence (CTI) ingestion from multiple approved sources
- Data Integration and Extract, Transform, Load (ETL)
- Interoperability Standards and Protocols
- Microservices APIs

Activity 6.6.3 Standardized Application Programming Interface (API) Calls and Schemas Part 2

Table 129: Activity 6.6.3 — Standardized Application Programming Interface (API) Calls and Schemas Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components will ensure that all ZT applications/services (i.e., PEP, PDP, PIP) adopt the API standard. Information Systems required to follow ZT Target or Advanced-levels prioritize integration with the API standard to simplify automation.	
Predecessor(s)	**Successor(s)**
6.6.2	None
Expected Outcomes	
• Components implement API Standard for all ZT Applications/Services (i.e., PEP, PDP, PIP).	
End State	
For each ZT service edge, Components will have an automated pattern and protocol service.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 6.6.2 (Phase One) – *Standardized Application Programming Interface (API) Calls and Schemas Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Each ZT service edge element will have an automated pattern and protocol service.
- ZT applications/services have been identified and defined as providing the Policy Enforcement Point (PEP), Policy Decision Point (PDP), and/or Policy Information Point (PIP) functionality.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 130: Implementation Tasks for Activity 6.6.3 — Standardized Application Programming Interface (API) Calls and Schemas Part 2

Assess all Component ZT applications/services for Application Programming Interface (API) standard adoption.
Determine ZT applications/services readiness for adoption of API standard, from Activity 6.6.2 (Phase One) – *Standardized Application Programming Interface (API) Calls and Schemas Part 1*: ☐ Evaluate governance readiness and technical interoperability for all Component ZT applications/services (e.g., PEP, PDP, PIP, etc.) for API standard adoption. ☐ Determine which Component ZT applications/services are prepared to adopt the API standard based on readiness and interoperability evaluation. **Manage Exceptions:** ☐ Applications/services that cannot adopt API standards are: • Identified • Documented • Approved or rejected ☐ Approval is granted when justification for the exception outweighs the risks to the Enterprise/Component. ☐ Risks are determined by the Enterprise and/or Component. ☐ Approvals are periodically reassessed.
Develop and implement a plan for API standard integration across the Component environment.
Develop and execute an integration plan: ☐ Develop a strategy to integrate the API standard across the Component environment, prioritizing high-impact (e.g., enforcement points) systems first. ☐ Create a roadmap for API standard adoption across all prepared ZT applications/services, to include required schema alignment (e.g., mandatory attributes for PDP/PEP), focusing on those requiring Target-level or Advanced integration. ☐ Develop a transition plan to replace ZT applications/services that are determined unprepared for API standard adoption. ☐ Collaborate with relevant teams to outline technical and security requirements for API standard adoption in each ZT application/service. ☐ Implement necessary updates to the environment of ZT applications/services to facilitate API standard integration.
Monitor, verify, and validate API standard adoption for ZT applications/services.
Implement continuous monitoring and automation to ensure compliance: ☐ Configure continuous monitoring to track API usage, performance, drift detection, and security events in real-time.

☐ Verify and validate API standard compliance through regular testing for all ZT applications/services.

☐ Provide feedback and continuous improvement recommendations to further optimize API standard compliance and automation.

Test, verify, and validate API standard adoption and automation:

☐ Conduct functional testing to ensure the APIs function as expected and adhere to the prior defined standards.

Audit and document API standard integration and automation:

☐ Conduct regular audits to verify and validate compliance with API standards and confirm that integration and automation are functioning as expected.

☐ Document audit results to identify gaps and areas for improvement in the API integration across the Component environment.

Summary

This diagram outlines the Activity 6.6.3 (Phase Two) – *Standardized Application Programming Interface (API) Calls and Schemas Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the migration to the new programmatic interface standard. It presents strategic insights driving implementation and expected outcomes that include implementation of Components Application Programming Interface (API) standard for all ZT applications/services.

Table 131: Activity 6.6.3 — Standardized Application Programming Interface (API) Calls and Schemas Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the migration to the new programmatic interface standard completed for all tools?

STRATEGIC INSIGHTS
• The Component defines objectives and establishes a verification plan to ensure all applications and services adopt API standards, focusing on compliance, security, and interoperability across the Enterprise architecture. • The Component demonstrates adherence to API security standards by implementing measures such as authentication, authorization, encryption, logging, and continuous monitoring to align with Enterprise requirements. • The Component provides evidence that API management solutions, including API gateways, are configured to manage and monitor API traffic, integrate with edge stacks, and enforce access controls to secure communication and data sharing. • The Component ensures the prioritization and integration of high-impact information systems with API standards, streamlining automation processes for provisioning, monitoring, and remediating devices and virtual assets. • The Component maintains continuous monitoring, functional and security testing, and regular audits to validate API performance, compliance, and security while automating enforcement mechanisms to address vulnerabilities.

EXPECTED OUTCOMES
1. Components implement API Standard for all ZT Applications/Services (i.e., Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Information Point (PIP)).

Capability 6.7 Security Operations Center (SOC) and Incident Response (IR)

Table 132: Capability 6.7 — Security Operations Center (SOC) and Incident Response (IR)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
6 - Automation and Orchestration	6.7 - Security Operations Center (SOC) and Incident Response (IR)
Description	
In the event a Computer Network Defense Service Provider (CNDSP) does not exist, DoW Components define and stand up Security Operations Centers (SOC) to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.	
Impact to ZT	
Standardized, coordinated, and accelerated incident response and investigative efforts.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- In the absence of a Computer Network Defense Service Provider (CNDSP)/Cybersecurity Service Provider (CSSP), the Component defines the requirements for a Security Operations Center (SOC) to monitor, protect, and respond to security incidents across Data, Applications, Assets, and Services (DAAS) resources.
- The SOC is established with dedicated teams and tools to provide 24/7 monitoring, centralized threat detection, and Incident Response (IR) capabilities.
- Upward visibility workflows are designed to provide real-time security status updates to leadership, while downward visibility workflows enable tactical implementation of security protections.
- Automation tooling is implemented to enrich SOC workflows by integrating data from multiple service providers and technologies, enhancing situational awareness and decision-making.
- During a simulated ransomware attack, the SOC's automated workflows detect abnormal activity on multiple endpoints and trigger an IR workflow.

- Enrichment tools collect and correlate contextual information, such as the attack vector, affected systems, and potential vulnerabilities, providing a comprehensive view of the incident.
- The automated workflow quarantines affected endpoints, notifies stakeholders, and generates a detailed incident report for further analysis by SOC analysts.
- Continuous workflow enrichment is applied, integrating advanced threat intelligence feeds and vulnerability databases to improve detection and response accuracy.
- Periodic reviews of SOC processes and workflows ensure that automation tooling and enrichment strategies evolve to address emerging threats and Component requirements.
- By standing up a SOC and automating workflows, the Component achieves standardized, coordinated, and accelerated IR and investigative efforts, ensuring robust security monitoring.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Security Posture: Establishing a SOC enables Components to proactively monitor and respond to threats, thereby significantly improving their overall security posture.
- Rapid IR: Automated workflows enable quicker detection and response to security incidents, minimizing potential damage and recovery time.
- Improved Situational Awareness: The integration of various threat intelligence feeds enhances situational awareness, enabling informed decision-making during incidents.
- Standardization of Processes: The establishment of a SOC leads to standardized IR procedures, ensuring consistency and effectiveness across the Component.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Endpoint Protection Platform (EPP)
- Indicators of Compromise (IoC)
- Multi-Factor Authentication (MFA)
- Privileged Access Management (PAM)
- Threat Intelligence Platform (TIP)

Activity 6.7.2 Workflow Enrichment Part 2

Table 133: Activity 6.7.2 — Workflow Enrichment Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components identify and establish extended workflows for additional incident response types in alignment with the activity "Threat Alerting Pt2". Initial enrichment data sources are used for existing workflows. Additional enrichment sources (e.g., UAM, UEBA, profiles, and baselines) are identified for future integrations.	
Predecessor(s)	**Successor(s)**
6.7.1	6.7.3
Expected Outcomes	
• Workflows for advanced threat events are developed by Components. • Advanced threat events are identified.	
End State	
Component workflows provide security teams with the intelligence needed to better detect, investigate, and respond to incidents more effectively.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Consider completing Activity 7.2.2 (Phase Two) – *Threat Alerting Part 2* prior to this activity, to identify additional Incident Response (IR) types.
- Activity 6.7.3 (Phase Three) – *Workflow Enrichment Part 3* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 134: Implementation Tasks for Activity 6.7.2 — Workflow Enrichment Part 2

Identify and establish extended workflows for additional IR types in alignment with Activity 7.2.2 (Phase Two) – *Threat Alerting Part 2*.
Leverage the established Cyber Threat Intelligence (CTI) policy, from Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1*: ☐ Utilize the Enterprise and Component cybersecurity IR procedures, from Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1.* **Identify additional advanced incident categories, scenarios, and response types for integration into existing workflows:** ☐ Leverage IR types as determined in Activity 7.2.2 (Phase Two) – *Threat Alerting Part 2.* ☐ Identify advanced incident categories and scenarios (e.g., phishing, ransomware, insider threats, Advanced Persistent Threats (APTs), etc.). **Extend existing workflows to integrate the additional advanced incident categories, scenarios, and response types:** ☐ Map current IR processes, to include decision-point sources (e.g., policy Decision Point (PDP) decision logs, Policy Enforcement Point (PEP) denial logs), and identify opportunities to leverage data analytics and threat intelligence to inform and automate ZT responses. ☐ Identify gaps and bottlenecks that prevent effective implementation of ZT principles during IR. Focus on areas where automation and data enrichment can improve security and reduce risk. ☐ Extend workflows to incorporate advanced incident categories and scenarios, gradually increasing automation and sophistication as the Component's ZT implementation matures.
Use initial enrichment data sources for existing extended workflows, where applicable.
Identify enrichment data sources, from Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1*: ☐ Verify and validate internal and external enrichment data sources meet fidelity thresholds (e.g., approved sources, timestamp accuracy, confidence scoring, etc.), from Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1*. **Integrate enrichment data sources into the existing extended workflow developed in the previous task:** ☐ Map the existing extended workflow to the enrichment data sources (e.g., steps, decision points, data flows, etc.). ☐ Identify gaps, bottlenecks, and areas where automation and/or additional enrichment data should improve the extended workflow. ☐ Use the mapping to extend existing workflows to include enrichment data, which will provide security teams with the intelligence necessary to respond more effectively to incidents.

Identify advanced threat events and develop appropriate workflows for IR.

Utilize the CTI policy, from Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1,* to identify CTI data feeds for advanced threat discovery:

☐ Leverage CTI data to enhance ZT data quality and integration.

- Evaluate, verify, and validate CTI data feeds for their accuracy, timeliness, and relevance to ZT security. Prioritize feeds that provide high-fidelity threat intelligence and integrate seamlessly with existing ZT security solutions.
- Conduct periodic reviews and purge intelligence/feeds as necessary.
- Expand IR workflows to incorporate automated data analysis and correlation, combining internal security data with external threat intelligence to improve threat detection and response within a ZT framework.

Test, verify, validate, and optimize extended IR workflows and enrichment sources.

Verify and validate IR workflows:

☐ Confirm existing IR workflows, from Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1*, continue to function as expected.

☐ Verify and validate IR workflows:

- Successfully integrate and associate the advanced threat intelligence data with events as appropriate.
- Equip security teams with the intelligence required to detect, investigate, and respond to incidents more efficiently and effectively.

Monitor and optimize IR workflows and enrichment sources:

☐ Implement continuous monitoring to track the performance of the IR workflows and to identify issues and/or areas of improvement.

☐ Continuously optimize the IR workflows based on feedback and performance data to ensure they remain efficient and effective.

Identify additional enrichment sources (e.g., User Activity Monitoring (UAM), User and Entity Behavior Analytics (UEBA), User/Person Entity (PE)/Non-Person Entity (NPE) profiles, baselines, etc.) for future integrations, where applicable.

Collaborate with the Enterprise to select approved enrichment sources based on Enterprise policies and procedures for future integration:

☐ Leverage Enterprise policies and procedures to select additional enrichment sources (e.g., UAM, UEBA, User/PE/NPE profiles, baselines, etc.).

Evaluate Component environment integration points during enrichment source adoption:

☐ Identify integration requirements for data flow between the Component environment and enrichment source(s).

☐ Determine the expected outputs and the impact on the existing security workflows before adoption.

☐ Before adoption, consider component environment scalability and interoperability (e.g., Application Programming Interface (API) availability, data formats, protocols, etc.).

☐ Ensure the Component environment can effectively ingest, process, and correlate enrichment data.

Summary

This diagram outlines the Activity 6.7.2 (Phase Two) – *Workflow Enrichment Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on identification and workflow development for advanced threat events. It presents strategic insights driving implementation and expected outcomes that include identification of Advanced Threat events and development of workflows for Advanced Threat events by Component.

Table 135: Activity 6.7.2 — Workflow Enrichment Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are advanced threat events identified and workflows developed for these events?

STRATEGIC INSIGHTS
• The Component defines objectives and scope for extended Incident Response (IR) workflows, aligning with industry and Enterprise standards to address critical incident types such as malware, data breaches, insider threats, phishing, and Distributed Denial-of-Service (DDoS) attacks. • The Component demonstrates the development and implementation of detailed IR workflows for each incident type, capturing essential phases including detection, analysis, containment, eradication, recovery, and post-incident review, with roles and responsibilities clearly defined. • The Component provides evidence of integrating enrichment data sources—such as asset inventories, Threat Intelligence Platforms (TIPs), User and Entity Behavior Analytics (UEBA), and Endpoint Detection and Response (EDR) solutions—into existing workflows, automating data normalization, correlation, and contextual analysis for enhanced detection and response. • The Component ensures advanced threat detection through continuous monitoring, anomaly detection, and the development of workflows leveraging baselines, behavioral analysis, and Machine Learning (ML) techniques, with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions configured to alert and respond to deviations in real-time. • The Component maintains effective security operations by automating incident workflows, enabling enrichment of security solutions, conducting regular audits, and refining processes to improve response efficiency, ensuring compliance with Enterprise standards and evolving threat landscapes.

EXPECTED OUTCOMES
1. Workflows for advanced threat events are developed by Components. 2. Advanced threat events are identified.

Visibility and Analytics Pillar

Capability 7.1 Log All Traffic (Network, Data, Apps, Users)

Table 136: Capability 7.1 — Log All Traffic (Network, Data, Apps, Users)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
7 - Visibility and Analytics	7.1 - Log All Traffic (Network, Data, Apps, Users)
Description	
DoW Components collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or Security Operations Center (SOC). Logs and events follow a standardized format and rules/analytics are developed as needed.	
Impact to ZT	
Foundational to the development of automated hunt and incident response playbooks.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component implements a logging framework to collect and process logs from all critical sources, including network, data, applications, and Users/Person Entities (PEs)/Non-Person Entities (NPEs).
- A standardized format for logs is established to ensure consistency across sources and enable efficient analysis by the Security Operations Center (SOC) and Computer Network Defense Service Provider (CNDSP)/Cybersecurity Service Provider (CSSP).
- Logging infrastructure is designed with scalability in mind, accounting for increased data volumes from expanding network, cloud, and application environments.
- Logs are parsed and normalized into a centralized system, enabling real-time correlation and analysis of events across multiple domains.
- The SOC configures automated analytics rules to detect anomalies, such as unusual login attempts, unexpected data transfers, or unauthorized access to sensitive applications.
- During routine monitoring, the analytics solution identifies anomalous traffic from a compromised User/PE account attempting to access restricted resources,

emphasizing the Zero Trust (ZT) focus on strict access controls and Least Privilege.

- An alert is generated and the SOC triggers a playbook to investigate, isolate the account, and prevent further unauthorized activity.
- Historical logs are reviewed to trace the origin of the compromise, revealing a phishing attempt that successfully stole the User/PE’s credentials.
- The insights gained from log analysis are used to refine automated hunting playbooks and improve the detection of similar threats in the future.
- By collecting and processing logs from all traffic sources, the Component establishes a robust foundation for threat detection, proactive hunting, Incident Response (IR) and enhanced security visibility.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Threat Detection: By collecting and analyzing logs from all critical sources, Components can quickly identify and respond to potential security threats.
- Improved IR: This capability enables effective IR through automated alerts and playbooks, thereby minimizing the impact of security incidents.
- Standardized Logging Practices: Establishing a standardized log format promotes consistency and efficiency in log analysis across different systems and devices.
- Informed Decision-Making: Insights gained from log analysis can inform security strategies and improve overall Component security posture.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
- Log Management solutions
- Monitoring and Auditing solutions
- Network Flow Data
- Network Traffic Analysis (NTA)

Activity 7.1.3 Log Analysis

Table 137: Activity 7.1.3 — Log Analysis

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Enterprise develops common user and device activities. Components identify and prioritize activities based on risk. Events/flows deemed the most simplistic and risky have analytics created using different data sources, such as logs. Trends and patterns are developed over longer periods of time.	
Predecessor(s)	**Successor(s)**
None	7.2.5, 7.3.2
Expected Outcomes	
• Identify activities to analyze. • Determine risk level per events/flows.	
End State	
Components utilize logs to develop risk level for each user and device.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Component has procured appropriate Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions to meet the needs of the environment.
- Consider completing Activity 7.1.2 (Phase One) – *Log Parsing* prior to this activity, to enforce appropriate logging policies and procedures.
- Activity 7.2.5 (Phase Two) – *User and Device Baselines* and Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 138: Implementation Tasks for Activity 7.1.3 — Log Analysis

The Enterprise defines key activities and events for analysis.
Establish baseline User/Person Entity (PE)/Non-Person Entity (NPE) behavior profiles: ☐ Define process, rules, and attributes to establish normal activity baselines per each User/PE/NPE: • Expected login locations • Working hours • Typical access patterns **Identify security-relevant activities and events that should be assigned a risk level:** ☐ Map security-relevant activities (e.g., authentication, access, escalation, data movement, etc.) to policy-driven access control decisions, ensuring alignment with policies that enforce ZT through dynamic, role- and attribute-based rules. ☐ Leverage Activity 7.1.2 (Phase One) – *Log Parsing,* to implement a reliable and appropriate event logging and retention policy with the capability to process, sort, search, and purge logs [34, 35]. ☐ Audit logs for common User/PE/NPE activity details. • Leverage the Component Log Source Codex, developed in Activity 7.1.2 (Phase One) – *Log Parsing*, to compare against the existing logs in order to identify any missing sources/prevent blind spots within the environment. **Prioritize activities and events based on risk level and associated threat potential:** ☐ Activities and events are classified based on risk to the ZT Architecture (ZTA), prioritizing those that indicate potential policy violations, unauthorized access attempts, or anomalous behavior. ☐ High-risk examples may include: • Multiple failed logins from unusual locations and/or devices. • Attempts to access sensitive data without proper authorization or from unmanaged devices. • Anomalous network traffic patterns indicative of data exfiltration or suspicious activity. • Unexpected disabling of logging or telemetry.
Assign risk scores to identified activities and events in alignment with Enterprise and Component security policies.
Develop Cyber Risk Scoring (CRS) and define thresholds for security action: ☐ In collaboration with the Enterprise, the Component defines CRS methodology and assigns initial weights based on security criticality (e.g., weighted scoring, statistical anomaly detection, etc.) [22]. ☐ Example thresholds: • 0-30: Normal (no action) • 31-70: Medium risk (log for review, minor alert) • 71-100: High risk (trigger immediate security response)

Leverage contextual enrichment to strengthen ZT policy enforcement and automation:

☐ Enrich raw event data with context, such as application behavior, time-sync validation, data access patterns, and network traffic analysis, to inform policy decisions and enable automated responses to security events within the ZT framework.

Implement dynamic risk adjustments:

☐ Leverage behavioral analytics to inform policy decisions by detecting deviations from historical activity patterns, triggering binary outcomes such as access grant/deny or triggering supplemental protections based on predefined ZT procedures.

Continuously refine CRS to support ZT policy enforcement:

☐ Analyze false positives/negatives to enhance the accuracy of risk signals that inform binary policy outcomes (e.g., access grant/deny).

☐ Automatically update risk scores based on new Indicators of Compromise (IoC) and Tactics, Techniques, and Procedures (TTPs) to ensure dynamic, context-aware adjustments that drive real-time policy decisions.

Integrate CRS into security solutions and dashboards.

Ensure security solutions can process and act on risk scores for all User/PE/NPEs based on ZT principles:

☐ Feed risk scores into SIEM and SOAR solutions and configure solutions to trigger automated responses, as needed.

Correlate behavioral and contextual signals across User/PE/NPEs to inform consistent policy-based access decisions in accordance with ZT principles:

☐ Track cumulative risk based on various signals across multiple activities (i.e., one high-risk event may not trigger action, but multiple events over time should be investigated).

☐ Implement entity risk scoring to assess collective risk and support identity stitching across multiple accounts or identities for the same User/PE/NPE.

Summary

This diagram outlines the Activity 7.1.3 (Phase Two) – *Log Analysis* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development of analytics for common User/Person Entity (PE)/Non-Person Entity (NPE) activities to identify trends. It presents strategic insights that drive implementation and expected outcomes, including the identification of activities for analysis and the determination of risk levels per Events/Flows.

Table 139: Activity 7.1.3 — Log Analysis - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are analytics developed for common User/PE and device activities to identify trends and patterns?

STRATEGIC INSIGHTS
• The Component establishes a robust logging framework to capture, normalize, and enrich User/PE and device activity details, ensuring consistent analysis across diverse data sources while adhering to event retention policies. • The Component performs risk assessments on event logs and flows to determine risk levels, ranging from low to high, enabling a thorough understanding of security posture and prioritization of anomalous activities. • The Component leverages historical log data and analytics to establish baseline behaviors for User/PE roles and device activities, using these baselines to identify and highlight deviations or anomalous behaviors. • The Component develops long-term analytics to identify trends and patterns in User/PE and device activity over extended periods, ensuring alignment with data retention policies for ongoing monitoring and analysis. • The Component determines and assigns risk levels to individual Users/PEs and devices based on log analysis, baseline behaviors, and risk assessments, enabling actionable insights for access control revisions and improved security posture.

EXPECTED OUTCOMES
1. Identify activities to analyze. 2. Determine risk level per events/flows.

Capability 7.2 Security Information and Event Management (SIEM)

Table 140: Capability 7.2 — Security Information and Event Management (SIEM)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
7 - Visibility and Analytics	7.2 - Security Information and Event Management (SIEM)
Description	
Computer Network Defense Service Provider (CNDSP) or Security Operations Centers (SOCs) monitor, detect, and analyze data logged into a Security Information and Event Management (SIEM) tool. User and device baselines are created using security controls and integrated with the SIEM. Alerting within the SIEM is matured over the phases to support more advanced data points (e.g., cyber threat intel, baselines, etc.)	
Impact to ZT	
Processing and exploiting data in the SIEM enables effective security analysis of anomalous user behavior, alerting, and automation of relevant incident response to common threat events.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component deploys a Security Information and Event Management (SIEM) solution in order to centralize the collection, monitoring, and analysis of logs from network, application, data, and Non-Person Entity (NPE) sources.
- Baselines for normal User/Person Entity (PE)/NPE behavior are created using historical data and security controls, serving as a foundation for detecting anomalies.
- Initial SIEM threat alerting is configured to identify common security events, such as failed login attempts, unauthorized data access, and suspicious network activity.
- During routine monitoring, the SIEM solution detects anomalous behavior; a User/PE account attempting to access sensitive data outside normal working hours.
- The alert is correlated with other logged events, such as a recent failed login attempt from an unrecognized Internet Protocol (IP) address, elevating the threat severity.

- Security Operations Center (SOC) analysts investigate the alert using enriched data from the SIEM, determining that the anomalous activity is part of an attempted account compromise.
- Automated Incident Response (IR) is triggered, isolating the User/PE account, blocking access to sensitive resources, and notifying relevant stakeholders.
- Advanced threat intelligence feeds are integrated into the SIEM, enabling the solution to correlate known Indicators of Compromise (IoC) with detected activity, further refining alerting accuracy.
- Regular tuning of the SIEM improves its ability to process and exploit data effectively, reducing false positives and ensuring alerts are actionable.
- By leveraging the SIEM for centralized logging, baseline development, and threat detection, the Component enhances its ability to monitor, analyze, and respond to threats.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Threat Detection: SIEM solutions provide real-time monitoring and analysis, enabling Components to detect and respond to threats more swiftly.
- Centralized Logging: By centralizing log data, Components can streamline investigations and improve compliance with regulatory requirements.
- Automated IR: The ability to automate responses to common threats reduces the time to mitigate incidents and minimizes potential damage.
- Improved Anomaly Detection: Establishing baselines for User/PE and device behavior enables more accurate identification of anomalies, resulting in quicker threat detection.
- Integration with Threat Intelligence: Incorporating advanced threat intelligence feeds enhances the SIEM's ability to correlate and analyze data, improving overall security effectiveness.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Governance, Risk, and Compliance (GRC)
- Managed Detection and Response (MDR)
- Security Information and Event Management (SIEM)
- Threat Intelligence Platform (TIP)
- Vulnerability Management solutions

Activity 7.2.2 Threat Alerting Part 2

Table 141: Activity 7.2.2 — Threat Alerting Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components expand threat alerting in the Security Information and Event Management (SIEM) solution to include Cyber Threat Intelligence (CTI) data feeds. Deviation and anomaly rules are developed in the SIEM to detect advanced threats.	
Predecessor(s)	**Successor(s)**
7.2.1, 7.5.1	7.2.3
Expected Outcomes	
• Rules developed for advanced threat correlation (e.g., behavioral, baseline deviation).	
End State	
Components augment SIEM with threat data from CTI feeds.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 7.2.1 (Phase One) – *Threat Alerting Part 1* and Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Cyber Threat Intelligence (CTI) teams are established in Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1*.
- Component has procured an appropriate Security Information and Event Management (SIEM) solution to meet the environment's needs.
- Proactive planning for false positive management is crucial. A well-defined process for triage, investigation, and rule refinement is essential.
- Share relevant CTI with trusted partners and collaborate on mitigation efforts using threat intelligence.
- Federal guidance suggests collaboration and sharing of cyber threat data between private sector and government entities to enhance national cybersecurity defense [36, 37].
- Activity 7.2.3 (Phase Three) – *Threat Alerting Part 3* is defined by the DoW ZT Framework as a successor to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 142: Implementation Tasks for Activity 7.2.2 — Threat Alerting Part 2

Expand existing SIEM solution to include CTI data feeds.
Integrate CTI data feeds to enhance ZT threat detection and response: ☐ Leverage CTI data feeds, from Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1*, focusing on those that deliver relevant, actionable insights into threats targeting ZT vulnerabilities, or attempting to bypass ZT controls. **Implement a standardized data normalization process and ingest data into SIEM:** ☐ Utilize Structured Threat Information eXpression (STIX)/Trusted Automated Exchange of Intelligence Information (TAXII) or similar standards to map CTI data to a common format within the SIEM. This may require custom parsers or data transformation scripts. ☐ Ingest normalized CTI data into the SIEM, mapping it to relevant event categories to enable correlation with internal security logs and improve threat detection capabilities within the ZT framework. ☐ Ensure seamless integration into SIEM to avoid performance issues or data inconsistencies. **Document CTI feed integration details:** ☐ Maintain CTI feed and SIEM integration data (e.g., source, format, update frequency and expiration).
Develop automated deviation and anomaly rules within the SIEM to detect and alert advanced threats.
Conduct threat modeling: ☐ Perform threat modeling exercises to identify potential vulnerabilities within the Zero Trust Architecture (ZTA). Focus on scenarios that attempt to bypass ZT controls. ☐ Leverage the threat model to guide SIEM rule development. **Create automated rules to detect and prevent ZT policy violations and data exfiltration:** ☐ Correlate CTI data with internal logs to detect malicious activity. ☐ Develop and prioritize SIEM rules leveraging behavioral analytics that trigger alerts on anomalous activities indicative of: • Deviations from network and/or behavioral baselines • ZT policy violations • Unapproved access attempts

- Correlations between CTI-identified threat actor Tactics, Techniques, and Procedures (TTPs) with internal events
- Data exfiltration attempts, such as increased traffic volume or time-based anomalies [31]

Refine and optimize rules:

☐ Implement a rigorous testing and tuning process of SIEM rules to minimize false positives/negatives and ensure accurate detection.

☐ Analyze alert data through a rigorous testing process to refine rules to:

- Minimize false positives.
- Improve the accuracy of threat detection and prevention.
- Improve the efficiency of threat detection and prevention.

☐ Regularly update CTI data feeds and review integration processes to adapt to emerging threats and maintain a strong ZT security posture.

☐ Establish a feedback loop to continuously refine rules based on real-world incidents and threat intelligence updates.

Create Incident Response (IR) Playbooks.

Develop IR Playbooks:

☐ Create IR playbooks for responding to alerts generated by SIEM rules that outline specific steps for investigation, containment, and remediation in alignment with ZT response actions.

☐ Integrate the SIEM with a Security Orchestration, Automation and Response (SOAR) solution to automate IR tasks, where possible.

Define alert escalation procedures:

☐ Establish clear, risk-based escalation paths for different alert types, to include:

- How and when alerts should be triaged
- Who is responsible for each escalation tier
- How incidents are transferred across teams (e.g., Security Operations Center (SOC), IR, leadership)

Review established rules, CTI feeds, and access controls.

Establish a rule review process:

☐ Conduct regular reviews of all SIEM rules to ensure their continued effectiveness and relevance.

☐ Update SIEM rules as needed based on changes to the threat landscape and the Component environment.

Maintenance of CTI feed by authorized User/Person Entities (PEs):

☐ Authorized User/PEs:

- Monitor the health and performance of CTI feeds (e.g., feed stops updating, latency increases, source becomes unreachable).

- Evaluate and ingest new CTI feeds.

Monitor and report performance.

Monitor SIEM performance and rule efficacy:

☐ Track key performance metrics, for example:

- Alert volume
- False positive rate
- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)

☐ Generate regular reports on threat detection and response activities.

Document SIEM rules and parameters:

☐ Maintain comprehensive documentation of all developed rules, including purpose, logic, and tuning parameters.

Summary

This diagram outlines the Activity 7.2.2 (Phase Two) – *Threat Alerting Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the expansion of the Security Information and Event Management (SIEM) solution to include alerts for Cyber Threat Intelligence (CTI) data feeds. It presents strategic insights that drive implementation and expected outcomes, including the development of rules for advanced threat correlation.

Table 143: Activity 7.2.2 — Threat Alerting Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is threat alerting expanded in the SIEM solution to include CTI data feeds?

STRATEGIC INSIGHTS
• The Component expands the SIEM solution by integrating CTI data feeds from trusted sources such as Cybersecurity and Infrastructure Security Agency (CISA), Information Sharing and Analysis Centers (ISACs), and commercial providers to enrich event data and enhance the detection of emerging threats. • The Component develops and configures automated SIEM correlation rules to identify Indicators of Compromise (IoC), detect advanced threats, and trigger alerts based on known Tactics, Techniques, and Procedures (TTPs) derived from CTI. • The Component correlates event, vulnerability, identity, device, and network flow data within the SIEM to detect deviations, anomalous behavior, and suspected adversarial activities across environments. • The Component collaborates with trusted partners by sharing relevant CTI data to enhance collective awareness, improve incident mitigation, and strengthen national cybersecurity defenses. • The Component ensures a Component-wide perspective on incident awareness and response by analyzing aggregated incident data and correlating individual responses with threat intelligence inputs.

EXPECTED OUTCOMES
1. Rules developed for advanced threat correlation (e.g., behavioral, baseline deviation).

Activity 7.2.5 User and Device Baselines

Table 144: Activity 7.2.5 — User and Device Baselines

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components develop a subject/attribute baseline approach based on typical pattern and behavior in activity "Establish User Baseline Behavior". This approach will serve as a benchmark for security when identifying and responding to abnormal or malicious activity.	
Predecessor(s)	**Successor(s)**
1.6.1, 7.1.3, 7.3.2	1.6.2, 2.3.1
Expected Outcomes	
• Components identify a subject/attribute baseline approach.	
End State	
Components can utilize a baseline approach to build profiles in activity "Baseline and Profiling Pt1".	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 1.6.1 (Phase Two) – *Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling*, Activity 7.1.3 (Phase Two) – *Log Analysis*, and Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Use scalable architectures to handle dynamic profiling efficiently.
- Continuously refine baselines to prevent outdated profiles from causing unnecessary alerts.
- Enrich baseline profiles with contextual data to reduce false positives, where possible.
- Consider completing Activity 7.4.1 (Phase Two) – *Baseline and Profiling Part 1* prior to this activity*,* to leverage established baselines to build profiles.
- Activity 1.6.2 (Phase Three) – *User Activity Monitoring Part 1* and Activity 2.3.1 (Phase Three) – *Entity Activity Monitoring Part One* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 145: Implementation Tasks for Activity 7.2.5 — User and Device Baselines

Define the baseline approach for subjects and attributes.
Identify key subjects and attributes for profiling: ☐ Ensure all Users/Person Entities (PEs)/Non-Person Entities (NPEs) are uniquely and non-reputably identified via strong identity binding (e.g., Public Key Infrastructure (PKI) certificates, etc.), then explicitly assigned to roles based on approved functions. Group entities by role and required access to resources and assets as defined by Enterprise and Component-level policies. ☐ Define, and continually refresh, attributes that support Attribute-Based Access Control (ABAC) by providing contextual input to policy decisions based on assigned roles and approved access. Attribute categories include: • User/PE attributes: Login behavior, geographic location, typical working hours, access patterns to resources and systems • NPE attributes: Network communication patterns, installed software, expected workloads, and service interaction behaviors **Establish subject and attribute baseline behavior:** ☐ Leverage tools procured in Activity 1.6.1 (Phase Two) – *Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling,* to measure and document baseline behaviors. ☐ Leverage Activity 7.1.3 (Phase Two) – *Log Analysis* and Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior,* to establish subject and attribute baseline behaviors. ☐ Adjust baselines to account for changes in User/PE/NPE roles, responsibilities, and/or expected behavior patterns.
Utilize the established baselines to build profiles, where applicable.
Leverage established baselines to build profiles in Activity 7.4.1 (Phase Two) – *Baseline and Profiling Part 1*: ☐ Define policy-driven criteria that determine whether User/PE/NPE activity satisfies conditions for access, based on identity, assigned role, and contextual attributes, in real-time, to enforce decisions (e.g., grant, deny, or apply safeguards) consistent with ZT principles. ☐ Use a non-repudiation service for User/PE/NPE attribution for all actions performed.

Build adaptive profiling:

☐ Implement dynamic profiling that updates as new behavior trends emerge.

☐ Create role-based baselines to compare User/PE/NPEs to peer groups and/or standard behavior as established in the baseline behavior data.

Integrate baseline profiles to enhance ZT anomaly detection and response:

☐ Feed profiles into Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and User and Entity Behavior Analytics (UEBA) solutions to establish baselines of normal activity within the environment and enable detection of anomalous behavior that could indicate policy violations, unapproved access attempts, and/or malicious activity. Prioritize anomalies that pose the greatest risk to ZT security.

☐ Implement dynamic monitoring to compare live activity against baseline behaviors.

☐ Implement analysis rules to detect deviations from typical behavior patterns.

Summary

This diagram outlines the Activity 7.2.5 (Phase Two) – *User and Device Baselines* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development of User/Person Entity (PE)/Non-Person Entity (NPE) baselines according to Enterprise standards. It presents strategic insights that drive implementation and expected outcomes, including the identification of a subject/attribute baseline approach.

Table 146: Activity 7.2.5 — User and Device Baselines - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are User/PE and device baselines developed based on DoW Enterprise standards?

STRATEGIC INSIGHTS
• The Component develops and documents a subject/attribute baseline approach by identifying primary Users/PEs, their roles, and typical behavior patterns (e.g., logon times, accessed resources, etc.) while leveraging User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) to evaluate access conditions and establish dynamic risk baselines. • The Component leverages historical User/PE activity data to establish initial behavioral baselines for User/PE roles and individuals, using the subject/attribute baseline approach as a benchmark to identify and respond to atypical or malicious activity via system event logging and Security Information and Event Management (SIEM) solutions. • The Component ensures ongoing monitoring and detection by defining Machine Learning (ML)-driven anomaly detection rules, logging critical events, and monitoring for deviations that indicate inappropriate activity while enabling timely incident reporting and resolution processes. • The Component builds risk-based User/PE profiles by determining criteria for typical, atypical, unapproved activities, adjusting baselines dynamically to account for changes in User/PE roles, responsibilities, and behavior patterns, while utilizing non-repudiation services to ensure user attribution. • The Component implements periodic assessments and baseline analysis rules to verify and validate accuracy and effectiveness over time, refining behavioral thresholds and ensuring alignment with evolving Component requirements, security policies, and activity risk profiling processes.

EXPECTED OUTCOMES
1. Components identify a subject/attribute baseline approach.

Capability 7.3 Common Security and Risk Analytics

Table 147: Capability 7.3 — Common Security and Risk Analytics

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
7 - Visibility and Analytics	7.3 - Common Security and Risk Analytics
Description	
Computer Network Defense Service Provider (CNDSP) or Security Operations Centers (SOC) employ data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors.	
Impact to ZT	
Analysis integrated across multiple data types to examine event, activities, and behaviors.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component deploys big data analytics tools to unify the collection of multiple data types, including network, Non-Person Entity (NPE), User/Person Entity (PE), application, and log data.
- A centralized data repository is established, enabling the Security Operations Center (SOC) and Computer Network Defense Service Provider (CNDSP) teams to examine events, activities, and behaviors across the Enterprise.
- User/PE baseline behavior is established by analyzing historical activity data, such as login patterns, file access, and network usage, providing a reference for detecting anomalies.
- An analytics solution detects a deviation from the baseline when a User/PE accesses an unusually large number of sensitive files in a short time period.
- The solution correlates this activity with additional data, such as the NPE location and associated application usage, identifying a potential insider threat.
- SOC analysts are alerted to the anomaly and use the analytics dashboard to investigate, confirming that the behavior poses a significant security risk.
- Automated risk scoring assigns a high threat level to the incident, triggering an immediate response to isolate the User/PE account and secure the affected systems, embodying Zero Trust (ZT) by enforcing strict access controls and minimizing potential damage.

- The analytics system integrates external threat intelligence feeds to enhance its detection capabilities, identifying Indicators of Compromise (IoC) associated with known attack vectors.
- Regular analysis of collected data is used to refine User/PE baselines and improve detection algorithms, reducing false positives and enhancing accuracy.
- By employing common security and risk analytics tools, the Component achieves a unified view of Enterprise activity, enabling comprehensive threat detection, behavioral analysis, and Incident Response (IR).

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Threat Detection: Improved ability to identify and respond to potential threats through unified data analysis and anomaly detection.
- Reduced False Positives: Continuous refinement of User/PE baselines and detection algorithms leads to fewer false alarms, allowing security teams to focus on genuine threats.
- Accelerated IR: Automated risk scoring and alerts enable quicker responses to security incidents, minimizing potential damage.
- Comprehensive Visibility: A unified view of enterprise activity enables better monitoring and understanding of User/PE behavior, as well as potential risks.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Data Analytics and Visualization solutions
- Governance, Risk, and Compliance (GRC)
- Managed Detection and Response (MDR)
- Threat Intelligence Platform (TIP)
- User Entity and Behavior Analytics (UEBA)
- Vulnerability Management solutions

Activity 7.3.2 Establish User Baseline Behavior

Table 148: Activity 7.3.2 — Establish User Baseline Behavior

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Utilizing the analytics tools implemented, subject behavior patterns are analyzed to identify patterns and deviations from normality. Techniques in analytics involve machine learning and UEBA.	
Predecessor(s)	**Successor(s)**
1.6.1, 7.1.3	7.2.5, 7.4.1
Expected Outcomes	
• Establish subject behavior patterns in order to differentiate normality/abnormality. • Identify opportunities for ML usage in analytics.	
End State	
Patterns established will provide Components with decision making for user/device baselines.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 1.6.1 (Phase Two) – *Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling* and Activity 7.1.3 (Phase Two) – *Log Analysis* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Component has procured appropriate Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions to meet the needs of the environment.
- Component has procured appropriate analytics solutions to meet the needs of the environment.
- Activity 7.2.5 (Phase Two) – *User and Device Baselines* and Activity 7.4.1 (Phase Two) – *Baseline and Profiling Part 1* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 149: Implementation Tasks for Activity 7.3.2 — Establish User Baseline Behavior

Obtain and analyze subject behavior patterns using existing analytics solutions.
Utilize existing analytics solutions and logs to establish baseline behaviors: ☐ Leverage Activity 1.6.1 (Phase Two) – *Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling*, to obtain existing analytics solutions. ☐ Leverage predecessor Activity 7.1.3 (Phase Two) – *Log Analysis,* to obtain assign risk scores for security-relevant activities and events. **Analyze behavior and determine baseline behaviors/patterns:** ☐ Analyze identity-centric log data to establish behavioral baselines for Users/Person Entities (PEs) and Non-Person Entities (NPEs) (e.g., typical logon times, resource access patterns, etc.). • Ensure consistent PEs behavior analysis across multiple accounts/devices by applying the principle of identity stitching. ☐ Use these baselines to inform ZT rule modeling and adaptive policy enforcement, enabling detection of anomalous behavior and context-aware access decisions. ☐ Determine the frequency in which baselines will be reevaluated to account for shifting responsibilities, mission, and operating requirements. ☐ Periodically reassess and reestablish baselines in accordance with the Enterprise or Component defined frequency.
Analyze behavior patterns and identify anomalies.
Analyze behavior patterns to detect and respond to ZT policy violations and unauthorized access attempts: ☐ Leverage SIEM and SOAR solutions to continuously monitor User/PE/NPE behavior within the environment, detecting deviations from established baselines that may indicate unauthorized attempts to: • Bypass access controls • Escalate privileges • Access sensitive data ☐ Investigate anomalous behaviors to determine the root cause in correlation with User/PE/NPE posture and/or network context before taking appropriate action to enforce ZT policies and mitigate potential threats.

Identify opportunities for Machine Learning (ML) usage in analytics.

Leverage ML to enhance ZT threat detection and response:

☐ Assess the effectiveness of current SIEM and SOAR analytics in detecting threats to the Zero Trust Architecture (ZTA) and identify opportunities where ML can:

- Improve accuracy
- Reduce false positives/negatives
- Automate response actions

☐ Evaluate and select ML models suitable for detecting anomalous behavior and policy violations within the environment, prioritizing those that align with ZT principles and address specific ZT security challenges.

☐ Train and validate ML models using historical data representative of a healthy environment, ensuring that they effectively identify and prioritize threats.

☐ Integrate ML-driven insights into security monitoring and Incident Response (IR) workflows, enabling more proactive and automated threat detection and response within the ZT framework.

Summary

This diagram outlines the Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the identification of Users/Person Entities (PEs) for baseline behavior analysis. It presents strategic insights that drive implementation and expected outcomes, including the establishment of subject behavior patterns to differentiate between normality and abnormalities.

Table 150: Activity 7.3.2 — Establish User Baseline Behavior - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are Users/PEs identified for baseline behavior analysis?

STRATEGIC INSIGHTS
• The Component identifies Users/PEs and establishes baseline behavior patterns by leveraging User and Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), and historical data to define typical User/PE roles, access patterns, and activities while ensuring data quality through normalization and noise reduction. • The Component implements behavior analytics models by defining normal baselines, selecting appropriate Machine Learning (ML) algorithms (e.g., clustering, anomaly detection, etc.), and training verified and validated models with labeled datasets to effectively monitor deviations. • The Component performs real-time monitoring by integrating ML models with monitoring systems, correlating behavior data with contextual information, and prioritizing detected anomalies based on severity to streamline Incident Response (IR). • The Component continuously evaluates and refines behavior analytics by assessing model performance metrics (precision, recall, false positives), identifying gaps in data or modeling, and retraining models to adapt to evolving behavioral trends. • The Component ensures the ongoing optimization and enhancement of behavior analytics by exploring new ML opportunities, updating datasets, and improving anomaly detection accuracy to maintain a proactive and adaptive monitoring framework.

EXPECTED OUTCOMES
1. Establish subject behavior patterns in order to differentiate normality/abnormality. 2. Identify opportunities for ML usage in analytics.

Capability 7.4 User and Entity Behavior Analytics (UEBA)

Table 151: Capability 7.4 — User and Entity Behavior Analytics (UEBA)

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
7 - Visibility and Analytics	7.4 - User and Entity Behavior Analytics (UEBA)
Description	
DoW Components initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. Computer Network Defense Service Provider (CNDSP) or Security Operations Centers (SOC) mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies.	
Impact to ZT	
Advanced analytics support detection of anomalous users, devices, and NPE actions and advanced threats.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component implements a User and Entity Behavior Analytics (UEBA) solution to create profiles and activity baselines for Users/Person Entities (PEs) and Non-Person Entities (NPEs).
- Historical activity data, such as login patterns, resource access, and data usage, is analyzed to establish normal behavior for each entity.
- The UEBA solution begins monitoring real-time activities, correlating them with baselines to detect anomalies indicative of potential threats.
- A User/PE account triggers an alert after accessing resources outside of typical working hours and from an unusual geographic location.
- The UEBA solution correlates the anomaly with additional suspicious behavior, such as multiple failed login attempts and unusual file transfer activity.
- The Security Operations Center (SOC) is alerted to the anomaly and uses the UEBA dashboard to investigate, identifying the behavior as an account compromise attempt.
- Advanced analytics refine the risk profile of the incident, escalating it for immediate remediation. Automated actions, such as isolating the account and requiring multi-factor re-authentication, are initiated to enforce Zero Trust (ZT) by verifying and validating every access attempt.

- The Component matures its UEBA capabilities by integrating Machine Learning (ML) models to continuously adapt baselines and improve anomaly detection accuracy.
- Regular audits of the UEBA solution ensure profiles remain up-to-date, incorporating changes in User/PE roles, NPE usage, and Component workflows.
- By employing and maturing UEBA capabilities, the Component detects anomalous activities and advanced threats more effectively, enabling proactive response.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Threat Detection: Components can identify anomalous behavior and potential threats more effectively, reducing the risk of security breaches.
- Proactive Incident Response (IR): Automated responses to detected anomalies enable quicker remediation, thereby minimizing potential damage.
- Improved Security Posture: Continuous adaptation of baselines through ML leads to a more resilient security framework aligned with ZT principles.
- Reduced False Positives: Advanced analytics enhance the accuracy of threat detection, resulting in fewer false alarms and more targeted security efforts.
- Comprehensive Auditing and Compliance: Regular audits ensure that User/PE profiles and behavior patterns are up-to-date, aiding in compliance with security regulations and standards.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Artificial Intelligence (AI)/Machine Learning (ML)-based Tagging and User Behavior Analysis
- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)
- User Access Management (UAM)
- User and Entity Behavior Analytics (UEBA)

Activity 7.4.1 Baseline and Profiling Part 1

Table 152: Activity 7.4.1 — Baseline and Profiling Part 1

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Utilizing the baselines developed in the "User/Device Baselines" activity, threat profiles are created to assess the level of risk for individual subjects associated with the overall Component security. Profiles should be integrated into the "Organization Access Profile" activity for decision making.	
Predecessor(s)	**Successor(s)**
1.6.1, 7.1.3, 7.3.2	7.4.2, 7.4.3
Expected Outcomes	
• Identify subject/attribute threat profiles. • Develop analytics to detect changing threat conditions.	
End State	
Components are able create risk profiles to mitigate compromised accounts, suspicious activity, and insider threats.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 1.6.1 (Phase Two) – *Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling*, Activity 7.1.3 (Phase Two) – *Log Analysis*, and Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Consider completing Activity 6.1.2 (Phase One) – *Organization Access Profile* prior to this activity, to leverage threat profiles.
- Consider completing Activity 7.2.5 (Phase Two) – *User and Device Baselines* prior to this activity, as it is necessary to establishing baseline behavior data.
- Component has procured appropriate Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions to meet the needs of the environment.
- Activity 7.4.2 (Phase Three) – *Baseline and Profiling Part 2* and Activity 7.4.3 (Phase Three) – *User and Entity Behavior Analytics (UEBA) Baseline Support Part 1* are defined by the DoW ZT Framework as successors to this activity.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 153: Implementation Tasks for Activity 7.4.1 — Baseline and Profiling Part 1

Develop subject and attribute-based threat profiles using data collected and analyzed in predecessor activities.
Utilize existing analytics tools, logs, and baseline behaviors: ☐ Leverage Activity 1.6.1 (Phase Two) – *Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling*, to obtain existing analytics tools. ☐ Leverage Activity 7.1.3 (Phase Two) – *Log Analysis,* to gather User/Person Entity (PE)/Non-Person Entity (NPE) logs and associated risk scores. ☐ Leverage Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior,* to determine baseline behaviors/patterns for Users/PEs/NPEs. **Develop adaptive ZT threat profiles using data-driven insights:** ☐ Create and continuously refine threat profiles based on historical data, real-time activity, and threat intelligence feeds, enabling a dynamic and adaptive approach to ZT security. ☐ Threat profiles should expire and be recalculated regularly to ensure they remain accurate and up to date as Users/PEs/NPEs evolve over time. **Enhance threat profiling with dynamic risk scoring:** ☐ Leverage the Cyber Risk Scoring (CRS) methods, from Activity 7.1.3 (Phase Two) – *Log Analysis,* to assign weights based on security criticality of subjects and events (e.g., weighted scoring, statistical anomaly detection, etc.) [38]. ☐ Secure and integrate threat profiles and risk scores into automated security workflows and decision-making processes, enabling a data-driven and responsive ZT security posture.
Develop and implement analytics for threat detection.
Develop analytics to detect and respond to ZT policy violations and anomalies: ☐ Develop analytics that continuously monitor User/PE/NPE behavior within the environment, detecting deviations from established baselines that may indicate both overt (e.g., brute-force, privilege misuse, etc.) and covert (e.g., lateral movement, data staging, etc.) activities. ☐ Conduct rigorous testing to verify and validate the accuracy of analytics in identifying and prioritizing threats to ZT security.

☐ Leverage SIEM and SOAR solutions to correlate threat profile deviations with security events, enabling automated responses and streamlined incident investigation within the ZT framework. ☐ Establish alert thresholds based on dynamic risk scoring assessments and ZT policy requirements, ensuring that security teams are notified of critical events that could compromise ZT security.
Integrate threat profiles into dynamic access policies to guide decision-making.
Leverage threat profiles to define and enforce access rules, from Activity 6.1.2 (Phase One) – *Organization Access Profile*: ☐ Create dynamic access rules based on established threat profiles, such as restricting access for high-risk Users/PEs/NPEs [38]. ☐ Integrate SIEM and SOAR solutions into the ZT framework to dynamically adjust access policies based on real-time threat intelligence and anomalous behavior detection, reinforcing continuous verification and adaptive access control with auditable and reversible actions. ☐ Enforce Component dynamic access policies to guide a decision-making framework, such as a Policy Decision Point (PDP) capable of consuming threat profiles [38, 39]. **Continuously monitor and update analytics:** ☐ Implement continuous monitoring and automated policy enforcement to ensure access decisions reflect the latest risk, as determined by the Enterprise and Component. ☐ Continuously review and refine threat profiles and SIEM/SOAR rules within the ZT framework to incorporate insights from behavioral analytics and shifts in baseline activity, ensuring access decisions remain context-aware and responsive to emerging threats.

Summary

This diagram outlines the Activity 7.4.1 (Phase Two) – *Baseline and Profiling Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development of common profiles for typical User/Person Entity (PE)/Non-Person Entity (NPE) types using analytics. It presents strategic insights that drive implementation and expected outcomes, including the identification of subject/attribute threat profiles and the development of analytics to detect changing threat conditions.

Table 154: Activity 7.4.1 — Baseline and Profiling Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are common profiles for typical User/PE and device types created using developed analytics?

STRATEGIC INSIGHTS
• The Component defines subject/attribute-based Threat Profiles by analyzing baseline data collected from predecessor activities, mapping User/PE behaviors, attributes, and known vulnerabilities to specific threat categories. • The Component classifies Users/PEs and roles into threat levels based on observed behaviors, attributes, and risk indicators, documenting standardized Threat Profiles that outline characteristics, risks, and mitigation strategies. • The Component develops analytics to detect threat conditions by implementing statistical or Machine Learning (ML) models capable of identifying behavioral anomalies, verifying and validating detection accuracy through simulations, and enabling real-time data monitoring. • The Component integrates Threat Profiles into Dynamic Access Policies to create rules that guide decision-making frameworks, such as Policy Decision Points (PDP), dynamically restricting or adjusting access based on User/PE threat levels. • The Component automates and continuously updates Threat Profiles and policies using Identity and Access Management (IAM) solutions to enforce rules in real-time, regularly reviewing and refining access policies based on evolving analytics and updated baseline data.

EXPECTED OUTCOMES
1. Identify subject/attribute threat profiles. 2. Develop analytics to detect changing threat conditions.

Capability 7.5 Threat Intelligence Integration

Table 155: Capability 7.5 — Threat Intelligence Integration

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Pillar	**Capability**
7 - Visibility and Analytics	7.5 - Threat Intelligence Integration
Description	
Computer Network Defense Service Provider (CNDSP) or Security Operations Centers (SOCs) integrate threat intelligence information and streams about identities, motivations, characteristics, and Tactics, Techniques, and Procedures (TTP) with data collected in the SIEM.	
Impact to ZT	
Integrating threat intelligence into other SIEM data enhances monitoring efforts and incident response.	

Scenario

The following scenario illustrates the practical applications and considerations for this capability:

- The Component establishes a Cyber Threat Intelligence (CTI) program to aggregate threat intelligence information, including details about identities, motivations, characteristics, and Tactics, Techniques, and Procedures (TTP) of known adversaries.
- The CTI program integrates multiple external and internal threat intelligence streams into the Component’s Security Information and Event Management (SIEM) solution.
- The SIEM solution is configured to correlate threat intelligence data with existing logs from network traffic, application activity, and User/Person Entity (PE) behavior to enhance anomaly detection.
- During routine monitoring, the SIEM solution identifies a network activity pattern that matches a known TTP from an active cyber threat group.
- The Security Operations Center (SOC) receives an alert enriched with contextual threat intelligence, including the adversary’s methods, tools, and likely objectives, enabling rapid decision-making.
- Automated response workflows are triggered, isolating affected systems and blocking the identified Indicators of Compromise (IoC) from further network activity.
- SOC analysts use threat intelligence data to conduct a deeper investigation, uncovering additional vulnerabilities exploited by the adversary and prioritizing their remediation.

- The Component matures its CTI program by integrating Machine Learning (ML) algorithms, enabling real-time updates to threat models and improving the accuracy of SIEM correlation rules.
- Periodic reviews of the CTI integration ensure that the intelligence feeds remain relevant and up-to-date, focusing on emerging threats and adversary behaviors.
- By integrating threat intelligence with the SIEM solution and automated workflows, the Component supports a Zero Trust (ZT) approach by enabling proactive threat mitigation and enforcing dynamic access control based on real-time risk.

Positive Impacts

The below is not a comprehensive list of benefits, but rather a selection of the advantages fundamental to this capability:

- Enhanced Threat Detection: Improved ability to identify and respond to threats through enriched data from threat intelligence.
- Accelerated IR: Automated workflows enable quicker isolation of affected systems, reducing potential damage.
- Proactive Vulnerability Management: Continuous monitoring and analysis enable the identification and remediation of vulnerabilities before they can be exploited.
- Improved Decision-Making: SOC analysts have access to contextual threat intelligence, aiding in informed and rapid decision-making during incidents.

Technology

The below is not a comprehensive list of technologies, but rather a selection fundamental to this capability:

- Governance, Risk, and Compliance (GRC)
- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
- Managed Detection and Response (MDR)
- Security Orchestration, Automation, and Response (SOAR)
- Threat Intelligence Platform (TIP)

Activity 7.5.2 Cyber Threat Intelligence (CTI) Program Part 2

Table 156: Activity 7.5.2 — Cyber Threat Intelligence (CTI) Program Part 2

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
DoW Components expand their Cyber Threat Intelligence (CTI) teams to include new stakeholders as appropriate. Existing and authenticated, private and controlled threat intelligence is analyzed, and appropriate actions and controls are enforced across ZT Pillars. CTI Program adapts strategy over time with expansion of threat intelligence developed in solutions and program maturity.	
Predecessor(s)	**Successor(s)**
7.5.1	None
Expected Outcomes	
• Component Cyber Threat Intelligence team is in place with extended stakeholders as appropriate. • Integration is in place for extended enforcement points across ZT Pillars (e.g., UEBA, UAM).	
End State	
Component CTI teams utilize threat intelligence data to support control enforcement to a greater extent throughout the organization via tooling.	

Considerations

Below is a list of key prerequisites, potential challenges, and lessons learned that may influence the successful implementation of this activity. While informative, this list is not exhaustive, and its relevance may vary based on the specific environment and architecture.

- Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Establish a Cyber Threat Intelligence (CTI) program that adapts strategy and works to improve over time across leveraging solutions (e.g., Open-Source Intelligence (OSINT), etc.) and program maturity.
- Consider completing Activity 7.1.3 (Phase Two) – *Log Analysis* prior to this activity, to access Cyber Risk Scoring (CRS) methodology.

Implementation

The implementation table below provides practical, actionable recommendations to help Components achieve the expected outcomes of this activity. These recommendations are not prescriptive or mandatory, and their applicability may vary depending on the specific environment and architecture. For a visual representation of the activity tasks covered in this section, refer to Appendix D.

Table 157: Implementation Tasks for Activity 7.5.2 — Cyber Threat Intelligence (CTI) Program Part 2

Expand CTI teams to include new stakeholders, as appropriate.

Review CTI program maturity and perform gap analysis:

☐ Leverage CTI policy and team(s), from Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1,* to identify gaps in processes, teams, and tools.

☐ Integrate CTI program improvements by mapping threat intelligence to potential attack paths within the Zero Trust Architecture (ZTA). Use this intelligence to meet Component mission priorities by:

- Informing policy tuning.
- Refining risk-based access controls.
- Prioritizing monitoring of high-risk assets and identities.

Expand stakeholder engagement:

☐ Identify and onboard new Enterprise approved Communities of Interest (COI), to include mission-critical stakeholders.

Enhance threat intelligence for data-driven ZT security:

☐ Continuously update CTI feeds with validated, diverse, and high-quality data sources that enrich security context within the environment.

☐ Prioritize data that can be integrated into security analytics platforms and used to inform automated responses, enabling a more data-driven and adaptive ZT security posture.

Strengthen ZT enforcement integration across pillars:

☐ Extend enforcement points across ZT Pillars, incorporating User and Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), and other advanced analytics tools.

☐ Automate enforcement of CTI-informed policies by integrating threat intelligence into ZT decision points (e.g., identity, device, and application access) to dynamically adjust security controls in accordance with ZT policy and continuous risk evaluation.

Document and update the CTI program to support ZT security:

☐ Maintain a CTI strategy document that aligns with the Component's ZT strategy and Enterprise cybersecurity guidance. Clearly articulate the CTI program:

- Supports ZT principles.
- Informs ZT policy enforcement.
- Enhances threat detection and response.

☐ Ensure strategy documents are accessible to all relevant teams and integrated into operational workflows.

Analyze the reviewed and approved threat intelligence for enforcement across ZT Pillars.

Analyze threat intelligence to enhance ZT security:

☐ Verify and validate CTI data feeds for accuracy, relevance, and alignment with ZT security objectives, prioritizing data that:

- Informs access control decisions.
- Enables automated responses.
- Supports proactive threat hunting.

☐ Categorize intelligence data based on its applicability to ZT pillars and enforcement points (e.g., UEBA, UAM, etc.) to ensure that relevant threat information is readily available to the appropriate security solutions and teams.

Correlate threat intelligence to enhance ZT visibility and proactive defense:

☐ Leverage Threat Intelligence Platforms (TIPs) and Security Information and Event Management (SIEM) to correlate CTI data with security events and logs within the environment.

☐ Identify trends and patterns in threat activity that could bypass or exploit weaknesses in ZT controls, enabling proactive security measures and enhancing visibility into the threat landscape.

Prioritize and assess threats:

☐ Consider using the Component defined CRS methodology from Activity 7.1.3 (Phase Two) – *Log Analysis*, to assign risk scores

☐ Alternatively, evaluate threats based on impact, likelihood, and relevance to mission-critical assets.

Enforce and continuously improve security controls across ZT Pillars:

☐ Apply Identity and Access Management (IAM) policies to protect sensitive assets and dynamically adjust access based on threat intelligence.

☐ Regularly refine and validate CTI data ingestion, analysis, and enforcement mechanisms to ensure threat intelligence informs dynamic, risk-based access decisions and policy updates across ZT enforcement points, to include Policy Decision Points (PDPs), Policy Enforcement Points (PEPs), UEBA, etc.

☐ Conduct regular assessments to verify and validate the efficacy of ZT policy enforcement, ensuring access controls, segmentation, and detection mechanisms function as intended under adversarial conditions.

Refine the CTI program to meet demands of evolving threat environment, as needed.

Maintain stakeholder engagement and collaboration:

☐ Regularly update stakeholder roles and responsibilities to reflect emerging threat landscapes and shifts in organizational priorities.

☐ Foster ongoing collaboration among stakeholders to ensure continuous alignment of CTI initiatives with ZT principles, enabling informed decision-making, dynamic policy enforcement, and continuous verification across the Component environment.

Continuously optimize the CTI program for data-driven ZT security:

☐ Regularly evaluate the quality, relevance, and timeliness of threat intelligence data used within the ZTA.

☐ Refine the CTI program to improve data collection, analysis, and integration processes, ensuring that the program effectively supports data-driven security decisions and automated responses within the ZT framework.

☐ Validate CTI program security decisions and automated response pathways, for example: intel -> decision -> enforcement, with consistent logging and visibility of events.

Summary

This diagram outlines the Activity 7.5.2 (Phase Two) – *Cyber Threat Intelligence (CTI) Program Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the integration of authenticated, private, and controlled Cyber Threat Intelligence (CTI) data feeds into the Security Information and Event Management (SIEM) and enforcement points. It presents strategic insights that drive implementation and expected outcomes, including the creation of a CTI team that incorporates extended stakeholders as appropriate.

Table 158: Activity 7.5.2 — Cyber Threat Intelligence (CTI) Program Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are authenticated, private, and controlled CTI data feeds integrated into the SIEM and enforcement points?

STRATEGIC INSIGHTS
• The Component defines an expanded CTI program by reviewing maturity, performing gap analyses, and aligning program improvements with evolving cyber threats, Component priorities, and ZT requirements. • The Component demonstrates enhanced stakeholder engagement by onboarding new, Enterprise-approved communities of interest, strengthening intelligence sources, and integrating advanced analytics solutions, such as User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM), to improve CTI enforcement across ZT Pillars. • The Component provides a structured approach to threat intelligence verification and validation, correlation, and enforcement by leveraging Threat Intelligence Platforms (TIPs), SIEM, and security controls to prioritize threats and dynamically adjust defense measures based on intelligence-driven insights. • The Component leverages Identity and Access Management (IAM) policies and automated enforcement mechanisms to refine CTI ingestion, analysis, and response, continuously adapting security controls through regular cybersecurity assessments and verification and validation efforts. • The Component ensures ongoing CTI program refinement by maintaining stakeholder collaboration, evaluating the effectiveness of strategies, and adapting policies, tools, solutions, and methodologies to address emerging threats, thereby ensuring proactive threat detection and response across all ZT Pillars.

EXPECTED OUTCOMES
1. Component CTI team is in place with extended stakeholders as appropriate. 2. Integration is in place for extended enforcement points across ZT Pillars (e.g., UEBA, UAM).

Appendix A – Terms and Definitions

Terms and definitions used within this Zero Trust Implementation Guideline.

Access Control
The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).
Source: NIST Computer Security Resource Center (CSRC) Glossary

Access Control List
A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Access Management
Access Management is how an agency authenticates enterprise identities and authorizes appropriate access to protected services.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Advanced Persistent Threat
An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Alerts
Data that indicates some trigger or threshold passing event has occurred and which is transmitted from the managed device/service to the managing service. A notification that a specific attack has been detected or directed at an organization's information systems.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Analytics
Information resulting from the systematic analysis of data or statistics. This analysis includes discovering, interpreting, and communicating significant patterns in data.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Application Programming Interface

A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Artificial Intelligence

The capability of computer processes to perform functions that are normally associated with human intelligence such as reasoning, learning and self-improvement.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Attribute-Based Access Control

An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Automation

Ability to create and apply application technology to monitor and control the production and delivery of otherwise manual services.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Availability

Ensuring timely and reliable access to and use of information.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Behavior

Aggregate data from logs and reports that provides packet, flow, file, and other types of information, as well as certain kinds of threat data to figure out whether certain kinds of activity and behavior are likely to constitute a cyberattack.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Big Data

The ability to enable enhanced insight, decision making, and process automation by consuming high-volume, high-velocity and/or high-variety information assets.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Biometrics

A biometric is a measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. (FIPS 201)

Source: DoD Zero Trust Reference Architecture, Version 2.0

Bring Your Own Device

A non-organization-controlled telework client device.

Source: NIST SP.1800-22 Mobile Device Security: Bring Your Own Device (BYOD)

CI/CD Pipeline

A CI/CD pipeline is a component of a broader toolchain that entails continuous integration, version control, automated testing, delivery, and deployment. It automates the integration and delivery of applications and enables organizations to deploy applications quickly and efficiently

Source: NSA/CISA CSI, Defending Continuous Integration/Continuous Delivery (CI/CD) Environments

Capability

A combination of mutually reinforcing security and privacy controls implemented by technical, physical, and procedural means. Such controls are typically selected to achieve a common information security- or privacy-related purpose.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Certificate Authority

A trusted entity that issues and revokes public key certificates.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Certificate Revocation List

A list of revoked public key certificates created and digitally signed by a certification authority. *Source: NIST Computer Security Resource Center (CSRC) Glossary*

Certificate

A set of data that uniquely identifies a public key (which has a corresponding private key) and an owner that is authorized to use the key pair. The certificate contains the owner’s public key and possibly other information and is digitally signed by a Certification Authority (i.e., a trusted party), thereby binding the public key to the owner.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Challenge

Additional or secondary question and response from a user to confirm identity or further authenticate.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Chief Information Officer

The senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Cloud Access Security Brokers

A software tool that manages access to secure data with record keeping capabilities that use updated encryption keys and log records to regulate access.
Source: Cybersecurity and Infrastructure Security Agency, United States Digital Service, and Federal Risk and Authorization Management Program, Cloud Security Technical Reference Architecture, Version 2.0

Cloud Security Posture Management

A continuous process of monitoring a cloud environment; identifying, alerting on, and mitigating cloud vulnerabilities; and improving cloud security.
Source: Cybersecurity and Infrastructure Security Agency, United States Digital Service, and Federal Risk and Authorization Management Program, Cloud Security Technical Reference Architecture, Version 2.0

Code

Computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler, or other translator.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Common Vulnerabilities and Exposures

A list of entries-each containing an identification number, a description, and at least one public reference-for publicly known CS vulnerabilities.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Communities of Interest

A collaborative group of users (working at the appropriate security level or levels) who exchange information in pursuit of their shared goals, interests, missions, or business processes, and must have a shared vocabulary for the information exchanged. The group exchanges information within and between systems.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Comply-to-Connect

Comply-to-Connect (C2C) is the identification, protection, and detection of DoDIN connected devices to ensure a continuous secure configuration. C2C enables the conduct of Defensive Cyber Operations in response to detected and prevailing threats by providing critical enabling information for the development of a Common Operating Picture. C2C standards are based on a framework of managing access to the network and its information resources by restricting or limiting access to those devices that do not comply with the standards.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Component

The organization implementing ZT.

Source: ZIG Primer

Concept of Operations

Verbal and graphic statement, in broad outline, of an organization's assumptions or intent in regard to an operation or series of operations of new, modified, or existing organizational systems.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Confidentiality

Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Configuration

The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Configuration Management

A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Container

A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Continuous

Occur periodically without interruption during the ordinary performance of services.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Continuous Authentication

The ability validate network users are the ones who they claim to be throughout an entire session at every step.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Continuous Integration/Continuous Delivery

Continuous Integration/Continuous Delivery (CI/CD) is a development process for quickly building and testing code changes that helps organizations maintain a consistent code base for their applications while dynamically integrating code changes. CI/CD is a key part of the Development, Security, and Operations (DevSecOps) approach that integrates security and automation throughout the development lifecycle.

Source: NSA/CISA CSI, Defending Continuous Integration/Continuous Delivery (CI/CD) Environments

Continuous Monitoring

The ability to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Control Plane

In a Zero Trust environment, there should be a separation (logical or possibly physical) of the communication flows used to control and configure the network and application/service communication flows used to perform the actual work of the organization. This is often broken down to a control plane for network control communication and a data plane for application/service communication flows. The control plane is used by various infrastructure components (both enterprise-owned and from service providers) to maintain and configure assets; judge, grant, or deny access to resources; and perform any necessary operations to set up communication paths between resources. The data plane is used for actual communication between software components.

Source: NIST SP 800-207 Zero Trust Architecture

Controlled Unclassified Information

Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Countermeasures

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system. Synonymous with security controls and safeguards.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Credential

An object or data structure that authoritatively binds an identity, via an identifier or identifiers, and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Credential Management

To manage the life cycle of entity credentials used for authentication.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Cyber Threat Intelligence

Cyber threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Cybersecurity Service Provider

A CSSP is an organization that provides one or more cybersecurity services to implement and protect the Department of Defense Information Network (DODIN).

Source: United States Cybersecurity Magazine

Data Catalog

Data Catalog contains descriptions and meta data about the data without itself holding that data.

Source: DoD Zero Reference Architecture, Version 2.0

Data Governance

Set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority, management and decision-making parameters related to the data produced or managed by the enterprise.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Data Loss Prevention

A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Data Plane

The data plane is used for communication between software components. This communication channel may not be possible before the path has been established via the control plane. For example, the control plane could be used by the PA and PEP to set up the communication path between the subject and the enterprise resource. The application/service workload would then use the data plane path that was established.

Source: NIST SP 800-207 Zero Trust Architecture

Data Rights Management

DRM is a set of access control technologies and policies that proactively detect and protect access to data and proprietary hardware and prevent unauthorized modification or redistribution of protected data.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Data Tagging
The ability to associate a data object with characterizing metadata for a defined purpose.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Defense Industrial Base
The U.S. Defense Industrial Base (DIB) is the network of organizations, facilities, and resources that provides the U.S. government—particularly the Department of Defense (DOD)—with defense-related materials, products, and services.

The DIB encompasses a wide variety of entities, including commercial firms operated on a for-profit basis, not-for-profit research centers and university laboratories, and government-owned industrial facilities. It provides everything from large, technologically sophisticated weapon systems and highly specialized operational support to general commercial products and routine services. By supplying and equipping the armed services, the DIB enables the United States to execute national strategy and develop, maintain, and project military power.
Source: Congress.Gov

Development, Security, and Operations
A combination of software engineering methodologies, practices, and tools that unifies software development (Dev), security (Sec), and operations (Ops). It emphasizes collaboration across these disciplines, along with automation and continuous monitoring to support the delivery of secure, high-quality software. DevSecOps integrates security tools and practices into the development pipeline, emphasizes the automation of processes, and fosters a culture of shared responsibility for performance, security, and operational integrity throughout the entire software lifecycle, from development to deployment and beyond.
Source: DoD Enterprise DevSecOps Fundamentals, Version 2.5

Device
A combination of components that function together to serve a specific purpose.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Disaster Recovery Plan
A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Dynamic
Occurring in near-real-time under conditions then present.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Dynamic Policy Enforcement
The ability to adapt policy and configurations, and enforce that change, in near real time based on environmental circumstances and indications of user and network behavior.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Enclave

A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Encryption

Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Encryption at Rest

The ability to protect data from a system compromise or data exfiltration by encrypting data while stored.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Endpoint

Endpoint is role given to any devices capable of initiating or terminating a session on a network. Often described as end-user devices, such as mobile devices, laptops, and desktop machine. Hardware servers in data centers. Devices such as zero clients, virtualized systems, and infrastructure equipment (i.e. routers, switches, virtual desktop machine) are considered endpoints.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Enterprise

The governing body that an organization falls under or reports to. The Enterprise is responsible for providing policies and guidance to those Components that fall under its purview.

Source: ZIG Primer

Enterprise Identity Provider

A service which provides state/status determination and access to Identity and Credential information. It may also provide baseline user/NPE access roles.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Executive Order

Legally binding orders given by the President, acting as the head of the Executive Branch, to Federal Administrative Agencies. Executive Orders are generally used to direct federal agencies and officials in their execution of congressionally established laws or policies.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Federal Information Processing Standards

A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.

Source: NIST Computer Security Resource Center (CSRC) Glossary

File Integrity Monitoring
Detecting any suspicious changes to files in a computer system.
Source: MITRE D3FEND

Geolocation
Determining the approximate physical location of an object, such as a cloud computing server.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Health Insurance Portability and Accountability Act
A federal statute that called on the federal Department of Health and Human Services to establish regulatory standards to protect the privacy and security of individually identifiable health information.
Source: NIST Computer Security Resource Center (CSRC) Glossary

High Availability
A failover feature to ensure availability during device or component interruptions.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identification and Authentication
The process of establishing the identity of an entity interacting with a system.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity
The set of physical and behavioral characteristics by which an individual is uniquely recognizable.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity Federation
A group of organizations that agree to follow the rules of a trust framework.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity Governance and Administration
Identity governance and administration system supports automated service provisioning of access certifications, access requests, password & token management following pre-established governance polies.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Identity Lifecycle Management
The evolution of an identity from creation to deactivation.
Source: GSA Identity Lifecycle Management Playbook, Version 1.3

Identity Management
Identity Management is how an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for employees and contractors.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Identity Provider

The party in a federation transaction that creates an assertion for the subscriber and transmits the assertion to the RP.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity and Access Management

Broadly refers to the administration of individual identities within a system, such as a company, a network or even a country. In enterprise IT, identity management is about establishing and managing the roles and access privileges of individual network users.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Identity as a Service

Identity as a service (IDaaS) is when a company offers identity, credential, and access management (ICAM) services to customers through a Software as a Service (SaaS) cloud-service model.

Source: NIST IR 8335 (Initial Public Draft) Announcement

Identity, Credential, and Access Management

Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency‘s resources. See also attribute-based access control (ABAC).

Source: NIST Computer Security Resource Center (CSRC) Glossary

Incident Response

The remediation or mitigation of violations of security policies and recommended practices.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Indicators of Compromise

Technical artifacts or observables that suggest that an attack is imminent or is currently underway or that a compromise may have already occurred.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Infrastructure as Code

The process of managing and provisioning an organization’s IT infrastructure using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Infrastructure as a Service

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Source: NIST Computer Security Resource Center (CSRC) Glossary

Integrity

Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Internet Protocol

Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Internet Protocol Security

A protocol that adds security features to the standard IP protocol to provide confidentiality and integrity services.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Internet of Things

The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Intrusion Prevention Systems

A system that can detect an intrusive activity and also attempt to stop the activity, ideally before it reaches its targets.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Inventory

A listing of items including identification and location information.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Just-in-Time

Using the current values of all indicators and analytics as input to a policy decision or enforcement.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Key

A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Key Performance Indicators

A metric of progress toward intended results.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Least Privilege

A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Logs

Digital information that provided a history of events and states of a specific system or device.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Machine Learning

The development and use of computer systems that adapt and learn from data with the goal of improving accuracy.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Macro-Segmentation

Similar in concept to physical network segmentation, macro-segmentation can be achieved through the application of additional hardware or VLANs.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Maintenance

Any act that either prevents the failure or malfunction of equipment or restores its operating capability.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Mandatory Access Control

An access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: (i) passing the information to unauthorized subjects or objects; (ii) granting its privileges to other subjects; (iii) changing one or more security attributes on subjects, objects, the information system, or system components; (iv) choosing the security attributes to be associated with newly-created or modified objects; or (v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Master User Record

A unique representation of a user’s accounts, personas, attributes, entitlements, and credentials within an organization.

Source: GSA Identity Lifecycle Management Playbook, Version 1.3

Metadata

Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).

Source: NIST Computer Security Resource Center (CSRC) Glossary

Micro-Segmentation
Micro-segmentation is the practice of dividing (isolating) the network into small logical segments by enabling granular access control, whereby users, applications, workloads and devices are segmented based on logical, not physical, attributes. This also provides an advantage over traditional perimeter security, as the smaller segments present a reduced attack surface (for malicious actors). In a ZT Architecture, security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Microservices
Small, decoupled components that ideally work independently of the other software components.
Source: GAO Agile Assessment Guide

Mobile Device Management
The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers. MDM is usually implemented through a third-party product that has management features for particular vendors of mobile devices.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Multi-Factor Authentication
Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/Personal Identification Number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Source: NIST Computer Security Resource Center (CSRC) Glossary

National Security Systems
Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Network Access Control
A feature provided by some firewalls that allows access based on a user’s credentials and the results of health checks performed on the telework client device.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Next-Generation Firewall

Allows integration of other tools to defend the network against malicious activity.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Non-Person Entity

An entity with a digital identity that acts in cyberspace but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts.

Source: NIST Computer Security Resource Center (CSRC) Glossary

OpenID Connect

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. This specification allows developers to authenticate users across websites and applications without having to own and manage password files. This specification can obtain basic profile information about the end-user in an interoperable and Representational State Transfer (REST)-like manner. OpenID Connect allows clients of all types, including web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users.

Source: US Department of Veterans Affairs, VA Technical Reference Model v 25.7

Operating System

The software “master control application” that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Permission

Authorization to perform some action on a system.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Person Entity

The role a human actor (i.e., User) performs when accessing IT assets with a specific identify.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Personally Identifiable Information

Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Pillars

A Pillar is a key focus area for implementation of Zero Trust controls.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Platform as a Service

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Policy

Statements, rules, or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Policy Decision Point

Mechanism that examines requests to access resources and compares them to the policy that applies to all requests for accessing that resource to determine whether specific access should be granted to the particular requester who issued the request under consideration.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Policy Enforcement Point

This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA. This is a single logical component in ZTA but may be broken into two different components: the client (e.g., agent on a laptop) and resource side (e.g., gateway component in front of resource that controls access) or a single portal component that acts as a gatekeeper for communication paths.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Policy Engine

This component is responsible for the ultimate decision to grant access to a resource for a given subject. The PE uses enterprise policy as well as input from external sources (e.g., CDM systems, threat intelligence services described below) as input to a trust algorithm (see Section 3.3 for more details) to grant, deny, or revoke access to the resource. The PE is paired with the policy administrator component. The policy engine makes and logs the decision (as approved, or denied), and the policy administrator executes the decision.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Policy Information Point

Serves as the retrieval source of attributes, or the data required for policy evaluation to provide the information needed by the policy decision point to make the decisions.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Privileged Access Management

A class of solutions that help secure, control, manage and monitor privileged access to critical assets.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Privileged User

A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Public Key Infrastructure

A framework that is established to issue, maintain and revoke public key certificates.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Reference Architecture

An authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.

Source: DoD Reference Architecture Description, Version 1.0

Remote Desktop Protocol

A proprietary network protocol that allows an individual to control the resources and data of a computer over the Internet.

Source: Federal Bureau of Investigation (FBI) Public Service Announcement

Resource

Resources are data, information, performers, materiel, or personnel types that are produced or consumed.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Risk Assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Role-Based Access Control

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Secure Hash Algorithm

A hash algorithm with the property that it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Secure Shell

A protocol for securely logging into a remote host and executing commands on that host (e.g., administrative commands).

Source: NIST IR7966 Security of Interactive and Automated Access Management Using Secure Shell (SSH)

Security Assertion Markup Language

A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Security Content Automation Protocol

A suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Security Information and Event Manager

Control log management system that helps filter the types of events and reduce alert fatigue.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Security Orchestration, Automation, and Response

A security strategy that has evolved in recent years to automate the IR process. Some of the state of practice applications of SOAR include threat detection and response, vulnerability prioritization, compliance checks, and security audits with potential applications in many emerging areas, such as IoT management.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Separation of Duty

Refers to the principle that no user should be given enough privileges to misuse the system on their own. For example, the person authorizing a paycheck should not also be the one who can prepare them. Separation of duties can be enforced either statically (by defining conflicting roles, i.e., roles which cannot be executed by the same user) or dynamically (by enforcing the control at access time). An example of dynamic separation of duty is the two-person rule. The first user to execute a two-person operation can be any authorized user, whereas the second user can be any authorized user different from the first [R.S. Sandhu., and P Samarati, "Access Control: Principles and Practice," IEEE Communications Magazine 32(9), September 1994, pp. 40-48.]. There are various types of SOD, an important one is history-based SOD that regulate for example, the same subject (role) cannot access the same object for variable number of times.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Service Provider

A provider of basic services or value-added services for operation of a network; generally refers to public carriers and other commercial enterprises.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Single Sign-On
An authentication process by which one account and its authenticators are used to access multiple applications in a seamless manner, generally implemented with a federation protocol.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Software Factory
In the DoD, a software factory is defined as a collection of people, tools, and processes that enables teams to continuously deliver value by deploying software to meet the needs of a specific community of end users. It leverages automation to replace manual processes.
Source: DoD Enterprise DevSecOps Fundamentals, Version 2.5

Software as a Service
The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Software-Defined Networking
The ability to separate the control and data planes and centrally manage and control the elements in the data plane.
Source: DoD Zero Trust Reference Architecture, Version 2.0

Supply Chain Risk Management
A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).
Source: NIST Computer Security Resource Center (CSRC) Glossary

System
A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Source: NIST Computer Security Resource Center (CSRC) Glossary

System Owner
Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.
Source: NIST Computer Security Resource Center (CSRC) Glossary

Tactics, Techniques and Procedures

The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Tailoring

The process by which security control baselines are modified by: identifying and designating common controls, applying scoping considerations on the applicability and implementation of baseline controls, selecting compensating security controls, assigning specific values to organization-defined security control parameters, supplementing baselines with additional security controls or control enhancements, and providing additional specification information for control implementation.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Telemetry

Telemetry is the automated collection of measurements or other data at remote points and their automatic transmission to receiving equipment for monitoring.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Token

Something that the Claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant’s identity. A portable, user-controlled, physical device (e.g., smart card or memory stick) used to store cryptographic information and possibly also perform cryptographic functions.

Source: DoD Zero Trust Reference Architecture, Version 2.0

Transport Layer Security

An authentication and encryption protocol widely implemented in browsers and Web servers. HTTP traffic transmitted using TLS is known as HTTPS.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Trusted Automated Exchange of Intelligence Information

An application layer protocol for exchanging Cyber Threat Intelligence over HTTPS.

Source: OASIS Cyber Threat Intelligence (CTI) Technical Committee

User Activity Monitoring

The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threat and to support authorized investigations.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Virtual Machine

A software-defined complete execution stack consisting of virtualized hardware, operating system (guest OS), and applications.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Virtual Private Network

A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Zero Trust

A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Zero Trust Architecture

An enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

Source: NIST Computer Security Resource Center (CSRC) Glossary

Appendix B – Abbreviations and Acronyms

The following provides a complete list of abbreviated terms and acronyms used within this Zero Trust Implementation Guideline.

A&O	Automation and Orchestration
ABAC	Attribute-Based Access Control
ACL	Access Control List
AI	Artificial Intelligence
API	Application Programming Interface
AppSec	Application Security
APT	Advanced Persistent Threat
ASTO	Application Security Testing Orchestration
B/C/P/S	Base/Camp/Post/Station
BYOD	Bring Your Own Device
C2C	Comply-to-Connect
CA	Certificate Authority
CaC	Configuration as Code
CASB	Cloud Access Security Broker
CCPA	California Consumer Privacy Act
CERT	Computer Emergency Response Team
CFI	Control Flow Integrity
CI/CD	Continuous Integration/Continuous Delivery (or Deployment)
CIA	Confidentiality, Integrity, and Availability
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Office
CISA	Cybersecurity and Infrastructure Security Agency
CMDB	Configuration Management Database
CMS	Content Management System
CNDSP	Computer Network Defense Service Provider
COI	Communities of Interest
CONOPS	Concept of Operations
COOP	Continuity of Operations
CP	Certificate Policies
CPS	Certification Practice Statement
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRS	Cyber Risk Scoring
CRUD	Create, Read, Update, and Delete
C-SCRM	Cybersecurity Supply Chain Risk Management
C-SCRM	Cybersecurity Supply Chain Risk Management

CSI	Cybersecurity Information Sheet
CSPM	Cloud Security Posture Management
CSSP	Cybersecurity Service Provider
CTI	Cyber Threat Intelligence
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposure
DAAS	Data, Applications, Assets, and Services
DAST	Dynamic Application Security Testing
DCI	Defense Critical Infrastructure
DDoS	Distributed Denial-of-Service
DEP	Data Execution Prevention
DevSecOps	Development, Security, and Operations
DIB	Defense Industrial Base
DiT	Data in Transit
DLP	Data Loss Prevention
DoD	Department of Defense (now Department of War (DOW))
DoW	Department of War
DoW CIO	Department of War Chief Information Office (formerly DoD CIO)
DPI	Deep Packet Inspection
DRM	Data Rights Management
DRP	Disaster Recovery Plan
EAM	Entity Activity Monitoring
EDR	Endpoint Detection and Response
EO	Executive Order
EPP	Endpoint Protection Platform
ETL	Extract, Transform, Load
FIM	File Integrity Monitoring
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
GRC	Governance, Risk, and Compliance
HCI	Hyperconverged Infrastructure
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host-Based Intrusion Prevention Systems
HR	Human Resources
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service

IaC	Infrastructure as Code
IAM	Identity and Access Management
IAVM	Information Assurance Vulnerability Management
ICAM	Identity, Credential, and Access Management
IC-TDF	Intelligence Community-Trusted Data Format
IDaaS	Identity as a Service
IdM	Identity Management
IdP	Identity Provider
IDS	Intrusion Detection System
IG	Installation Gateway
IGA	Identity Governance and Administration
ILM	Identity Lifecycle Management
IoC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPC	Inter-Process Communication
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv6	Internet Protocol Version 6
IR	Incident Response
ISA	Information Sharing Agreement
ISAC	Information Sharing and Analysis Center
ISN	Installation Service Node
IT	Information Technology
ITAM	Information Technology Asset Management
ITOM	Information Technology Operations Management
JEA	Just Enough Administration
JIT	Just-In-Time
JSON	JavaScript Object Notation
JWT	JavaScript Object Notation (JSON) Web Tokens
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
MDR	Managed Detection and Response
MFA	Multi-Factor Authentication
ML	Machine Learning
mTLS	mutual Transport Layer Security
NAC	Network Access Control
NetOps	Network Operations

NextGen AV	Next-Generation Antivirus
NFV	Network Function Virtualization
NGFW	Next-Generation Firewall
NIST	National Institute of Standards and Technology
NM	National Manager
NPE	Non-Person Entity
NSA	National Security Agency
NSM	National Security Memorandum
NSS	National Security Systems
NTA	Network Traffic Analysis
OAuth	Open Authorization
OCSP	Online Certificate Status Protocol
OIDC	OpenID Connect
OSINT	Open-Source Intelligence
OT	Operational Technology
OWASP	Open Worldwide Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PCI	Payment Card Industry
PDP	Policy Decision Point
PE	Person Entity
PEP	Policy Enforcement Point
PfMO	Portfolio Management Office
PHI	Protected Health Information
PID	Process Identifier
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIP	Policy Information Point
PKI	Public Key Infrastructure
PQE	Post-Quantum Encryption
RA	Reference Architecture
RAM	Random-Access Memory
RASP	Runtime Application Self-Protection
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
REST API	Representational State Transfer Application Programming Interface
RPA	Robotic Process Automation
RSA	Rivest-Shamir-Adleman
RTO	Recovery Time Objective
SaaS	Software as a Service

SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SCAP	Security Content Automation Protocol
SCRM	Supply Chain Risk Management
SDC	Software-Defined Compute
SDLC	Software Development Lifecycle
SDN	Software-Defined Networking
SDS	Software-Defined Storage
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Manager
SLA	Service Level Agreement
SME	Subject Matter Expert
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SSH	Secure Shell
SSO	Single Sign-On
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated Exchange of Intelligence Information
TEE	Trusted Execution Environment
TIP	Threat Intelligence Platform
TLS	Transport Layer Security
TPU	Tensor Processing Unit
TTP	Tactics, Techniques, and Procedures
UAM	User Activity Monitoring
UAT	User Acceptance Testing
UEBA	User and Entity Behavior Analytics
UEDM	Unified Endpoint and Device Management
UEM	Unified Endpoint Management
USG	United States Government
VDP	Vulnerability Disclosure Program
VLAN	Virtual Local Area Network
VMP	Vulnerability Management Program
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VXLAN	Virtual Extensible Local Area Network
WAF	Web Application Firewall
WAN	Wide Area Network
XAAS	Anything as a Service

XDR	Extended Detection and Response
YAML	Yet Another Markup Language
ZIG	Zero Trust Implementation Guideline
ZT	Zero Trust
ZTA	Zero Trust Architecture
ZTDF	Zero Trust Data Format
ZTP	Zero-Touch Provisioning

Appendix C – References

[1] Department of War Office of the Chief Information Officer. "Department of Defense Zero Trust Strategy, Version 1.0." 2022. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[2] Department of War Office of the Chief Information Officer. "Department of Defense Zero Trust Capabilities and Activities, Dated 22 January 2025." 2024. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-CapabilitiesActivities.pdf?ver=-o9HgcID4LQHccIGjNQtiw%3d%3d

[3] Department of War Office of the Chief Information Officer. "Zero Trust Reference Architecture, Version 2.0." 2022. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[4] National Security Agency. "CSI: Embracing a Zero Trust Security Model." 2021. Available: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[5] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the User Pillar." 2023. Available: https://media.defense.gov/2024/May/30/2003475230/-1/-1/0/CSI-VISIBILITY-AND-ANALYTICS-PILLAR.PDF

[6] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Device Pillar." 2023. Available: https://media.defense.gov/2023/Oct/19/2003323562/-1/-1/0/CSI-DEVICE-PILLAR-ZERO-TRUST.PDF

[7] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Application and Workload Pillar." 2024. Available: https://media.defense.gov/2024/May/22/2003470825/-1/-1/0/CSI-APPLICATION-AND-WORKLOAD-PILLAR.PDF

[8] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Data Pillar." 2024. Available: https://media.defense.gov/2024/Apr/09/2003434442/-1/-1/0/CSI_DATA_PILLAR_ZT.PDF

[9] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Network and Environment Pillar." 2024. Available: https://media.defense.gov/2024/Mar/05/2003405462/-1/-1/0/CSI-ZERO-TRUST-NETWORK-ENVIRONMENT-PILLAR.PDF

[10] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Automation and Orchestration Pillar." 2024. Available: https://media.defense.gov/2024/Jul/10/2003500250/-1/-1/0/CSI-ZT-AUTOMATION-ORCHESTRATION-PILLAR.PDF

[11] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Visibility and Analytics Pillar." 2024. Available: https://media.defense.gov/2024/May/30/2003475230/-1/-1/0/CSI-VISIBILITY-AND-ANALYTICS-PILLAR.PDF

[12] National Institute of Standards and Technology. "Computer Security Resource Center Glossary." 2021. Available: https://csrc.nist.gov/glossary/

[13] Department of War Office of the Chief Information Officer. "Identity, Credential, and Access Management (ICAM) Strategy." 2020. Available: https://dodcio.defense.gov/Portals/0/Documents/Cyber/ICAM_Strategy.pdf

[14] National Security Agency and Cybersecurity and Infrastructure Security Agency. "Identity and Access Management: Recommended Best Practices for Administrators." 2023. Available: https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF

[15] General Services Administration. "Identity Lifecycle Management Playbook." 2024. Available: https://www.idmanagement.gov/playbooks/ilm/

[16] Jason Garbis and Jerry W. Chapman. "Zero Trust Security: An Enterprise Guide." 2021. Available: https://www.oreilly.com/library/view/zero-trust-security/9781484267028

[17] Department of War Office of the Chief Information Officer. "Zero Trust Execution Roadmap, Version 1.1." 2024. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-ExecutionRoadmap-v1.1.pdf

[18] National Institute of Standards and Technology. "Recommendations for Federal Vulnerability Disclosure Guidelines, NIST Special Publication 800-216." 2023. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216.pdf

[19] National Institute of Standards and Technology. "Cybersecurity Supply Chain Risk Management (C-SCRM)." 2025. Available: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

[20] National Institute of Standards and Technology. "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST Special Publication 800-161, Rev.1, Update 1." 2024. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

[21] Department of War Office of the Chief Information Officer. "DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes, Version 2.1." 2021. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20-%20CNCF%20Kubernetes%20w-DD1910_cleared_20211022.pdf

[22] National Security Agency. "CTR: Network Infrastructure Security Guide." 2023. Available: https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

[23] National Security Agency and Cybersecurity & Infrastructure Security Agency. "CSI: Implement Network Segmentation and Encryption in Cloud Environments, Version 1.0." 2024. Available: https://media.defense.gov/2024/Mar/07/2003407861/-1/-1/0/CSI-CloudTop10-Network-Segmentation.PDF

[24] National Security Agency. "Overview of Software Defined Networking Risks." 2017. Available: https://hpc.mil/images/hpcdocs/ipv6/Overview-of-Software-Defined-Networking-SDN-Risks.pdf

[25] National Security Agency. "CSI: Managing Risk From Transport Layer Security Inspection." 2019. Available: https://media.defense.gov/2019/Dec/16/2002225460/-1/-1/0/INFO%20SHEET%20%20MANAGING%20RISK%20FROM%20TRANSPORT%20LAYER%20SECURITY%20INSPECTION.PDF

[26] Defense Information Security Agency. "SDN Controller Security Requirements Guide, Finding ID V-206728." 2024. Available: https://stigviewer.com/stigs/sdn_controller_security_requirements_guide/2024-05-28/finding/V-206728

[27] National Institute of Standards and Technology. "A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments, NIST Special Publication 800-207A." 2023. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.pdf

[28] Department of War Office of the Chief Information Officer. "DoD Instruction 8440.02: DoD Implementation of Internet Protocol, Version 6." 2024. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/844002p.PDF

[29] Office of Systems Engineering and Architecture and Office of the Under Secretary of War for Research and Engineering. "Application Programming Interface (API) Technical Guidance." 2024.

Available: https://www.cto.mil/wp-content/uploads/2024/08/API-Tech-Guidance-MVCR1-July2024-Cleared.pdf

[30] MITRE. "MITRE ATT&CK: Filter Network Traffic, Version 1.1." 2024. Available: https://attack.mitre.org/mitigations/M1037/

[31] National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." 2024. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[32] National Institute of Standards and Technology. "Security Requirements for Cryptographic Modules, NIST Federal Information Processing Standards Publication 140-3." 2019. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

[33] National Institute of Standards and Technology. "Data Classification Concepts and Considerations for Improving Data Protection, NIST Internal Report 8496, Initial Public Draft." 2023. Available: https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8496.ipd.pdf

[34] National Institute of Standards and Technology. "Cybersecurity Log Management Planning Guide, NIST Special Publication 800-92, Rev. 1, Initial Public Draft." 2023. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-92r1.ipd.pdf

[35] Australian Cyber Security Centre. "Best Practices for Event Logging and Threat Detection." 2024. Available: https://www.cyber.gov.au/sites/default/files/2024-08/best-practices-for-event-logging-and-threat-detection.pdf

[36] President Barack Obama. "Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing." 2015. Available: https://www.federalregister.gov/documents/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing

[37] Cybersecurity and Infrastructure Security Agency. "Automated Indicator Sharing (AIS)." 2025. Available: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais

[38] National Institute of Standards and Technology. "Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, Rev. 5." 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[39] National Institute of Standards and Technology. "Zero Trust Architecture, NIST Special Publication 800-207." 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[40] National Institute of Standards and Technology. "Mobile Device Security: Bring Your Own Device (BYOD), NIST Special Publication 1800-22." 2023. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf

[41] National Security Agency and Cybersecurity and Infrastructure Security Agency. "CSI: Defending Continuous Integration/Continuous Delivery (CI/CD) Environments, Version 1.0." 2023. Available:

[42] Cybersecurity and Infrastructure Agency. "Cloud Security Technical Reference Architecture." 2022. Available: https://www.cisa.gov/sites/default/files/2023-02/cloud_security_technical_reference_architecture_2.pdf

[43] National Security Agency. "CTR: Zero Trust Implementation Guideline Primer, Version 1.0." 2026. Available: https://media.defense.gov/2026/Jan/08/2003852320/-1/-1/0/CTR_ZERO_TRUST_IMPLEMENTATION_GUIDELINE_PRIMER.PDF

[44] United States Cybersecurity Magazine. "Department of Defense (DOD) Cybersecurity Service Providers (CSSPs): A Unique Component of DOD’s Defense–in–Depth Strategy." n.d. Available: https://www.uscybersecurity.net/dod/

[45] Congressional Research Service. "The U.S. Defense Industrial Base: Background and Issues for Congress." 2024. Available: https://www.congress.gov/crs-product/R47751

[46] Department of War Office of the Chief Information Officer. "DoD Enterprise DevSecOps Fundamentals, Version 2.5." 2024. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Enterprise%20DevSecOps%20Fundamentals%20v2.5.pdf

[47] MITRE. "MITRE D3FEND." 2025. Available: https://d3fend.mitre.org

[48] National Institute of Standards and Technology. "Identity as a Service for Public Safety Organizations, NIST IR 8335." 2021. Available: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8335-draft.pdf

[49] Government Accountability Office. "Agile Assessment Guide: Best Practices for Adoption and Implementation." 2023. Available: https://www.gao.gov/assets/d24105506.pdf

[50] Department of Veterans Affairs. "Open Identifier (OpenID) Connect, VA Technical Reference Model, Version 25.7." 2025. Available: https://www.oit.va.gov/Services/TRM/StandardPage.aspx?tid=6769#

[51] Department of War Office of the Chief Information Officer. "DoD Reference Architecture Description." 2010. Available: https://dodcio.defense.gov/Portals/0/Documents/Ref_Archi_Description_Final_v1_18Jun10.pdf

[52] Federal Bureau of Investigation. "Cyber Actors Increasingly Exploit the Remote Desktop Protocol to Conduct Malicious Activity." 2018. Available: https://www.ic3.gov/PSA/2018/PSA180927#:~:text=Definition,making%20intrusions%20difficult%20to%20detect

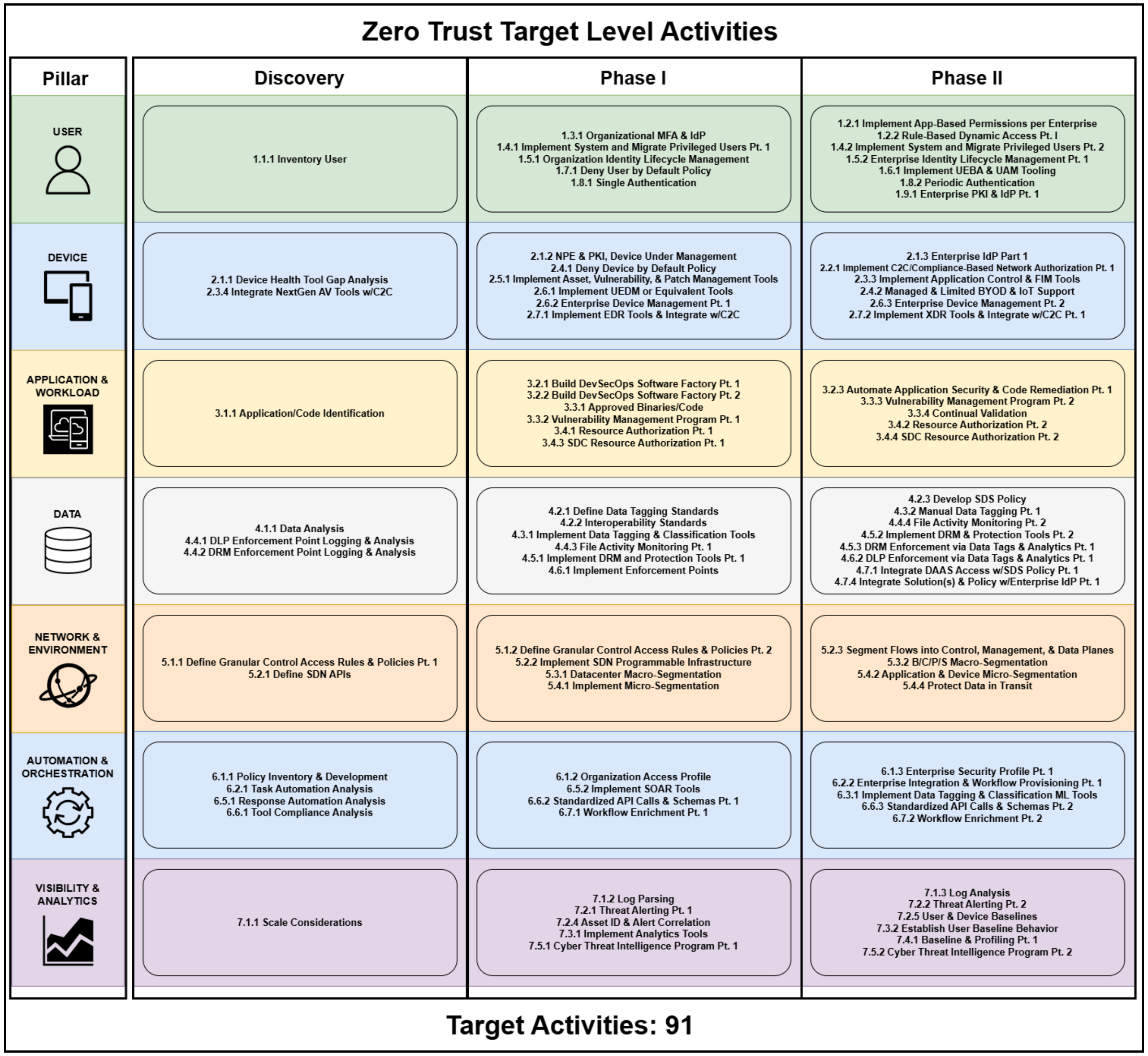
[53] National Institute of Standards and Technology. "Security of Interactive and Automated Access Management Using Secure Shell (SSH), NIST IR 7966." 2015. Available: https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.7966.pdf

[54] OASIS. "Introduction to TAXII." 2024. Available: https://oasis-open.github.io/cti-documentation/taxii/intro.html

Appendix D – Activity Task Diagrams

The Department of War (DoW) Chief Information Office (CIO) Zero Trust (ZT) Framework defines 152 Activities (91 Target-level) that describe how organizations can implement ZT. The relationship between the implementation of these Activities is identified through DoW-defined predecessors and successors for each Activity. These Zero Trust Implementation Guidelines (ZIGs) provide a set of Implementation Tasks associated with DoW-defined ZT Activities to accomplish the Expected Outcomes and Capability intents.

In the ZIGs, the activities feature multiple tasks, with several predecessors and successors, leading to a complex and intricate implementation process. Additionally, dependency and constraint relationships between tasks within a single Activity or across different activities add to this complexity. The following Activity Task Diagrams provide a non-linear, illustrative example of a one-to-one visualization of the Activity, beginning on the left with any defined predecessors, followed by the Activity tasks as outlined in the applicable Activity, and ending on the right with defined successors. A filled in circle at the beginning indicates that there is/are no DoW-defined predecessor(s) and a non-filled in circle at the end indicates there is/are no DoW-defined successor(s) for that particular Activity. The diagrams provide a standardized visual representation for navigating the implementation process. Appendix D begins with a linear graphic illustrating the Pillars and Activities, by both Pillar and Phase. This diagram serves as a reference guide to the subsequent Activity Task Diagrams.



Zero Trust Target Level Activities

Pillar	Discovery	Phase I	Phase II
USER	1.1.1 Inventory User	1.3.1 Organizational MFA & IdP 1.4.1 Implement System and Migrate Privileged Users Pt. 1 1.5.1 Organization Identity Lifecycle Management 1.7.1 Deny User by Default Policy 1.8.1 Single Authentication	1.2.1 Implement App-Based Permissions per Enterprise 1.2.2 Rule-Based Dynamic Access Pt. I 1.4.2 Implement System and Migrate Privileged Users Pt. 2 1.5.2 Enterprise Identity Lifecycle Management Pt. 1 1.6.1 Implement UEBA & UAM Tooling 1.8.2 Periodic Authentication 1.9.1 Enterprise PKI & IdP Pt. 1
DEVICE	2.1.1 Device Health Tool Gap Analysis 2.3.4 Integrate NextGen AV Tools w/C2C	2.1.2 NPE & PKI, Device Under Management 2.4.1 Deny Device by Default Policy 2.5.1 Implement Asset, Vulnerability, & Patch Management Tools 2.6.1 Implement UEDM or Equivalent Tools 2.6.2 Enterprise Device Management Pt. 1 2.7.1 Implement EDR Tools & Integrate w/C2C	2.1.3 Enterprise IdP Part 1 2.2.1 Implement C2C/Compliance-Based Network Authorization Pt. 1 2.3.3 Implement Application Control & FIM Tools 2.4.2 Managed & Limited BYOD & IoT Support 2.6.3 Enterprise Device Management Pt. 2 2.7.2 Implement XDR Tools & Integrate w/C2C Pt. 1
APPLICATION & WORKLOAD	3.1.1 Application/Code Identification	3.2.1 Build DevSecOps Software Factory Pt. 1 3.2.2 Build DevSecOps Software Factory Pt. 2 3.3.1 Approved Binaries/Code 3.3.2 Vulnerability Management Program Pt. 1 3.4.1 Resource Authorization Pt. 1 3.4.3 SDC Resource Authorization Pt. 1	3.2.3 Automate Application Security & Code Remediation Pt. 1 3.3.3 Vulnerability Management Program Pt. 2 3.3.4 Continual Validation 3.4.2 Resource Authorization Pt. 2 3.4.4 SDC Resource Authorization Pt. 2
DATA	4.1.1 Data Analysis 4.4.1 DLP Enforcement Point Logging & Analysis 4.4.2 DRM Enforcement Point Logging & Analysis	4.2.1 Define Data Tagging Standards 4.2.2 Interoperability Standards 4.3.1 Implement Data Tagging & Classification Tools 4.4.3 File Activity Monitoring Pt. 1 4.5.1 Implement DRM and Protection Tools Pt. 1 4.6.1 Implement Enforcement Points	4.2.3 Develop SDS Policy 4.3.2 Manual Data Tagging Pt. 1 4.4.4 File Activity Monitoring Pt. 2 4.5.2 Implement DRM & Protection Tools Pt. 2 4.5.3 DRM Enforcement via Data Tags & Analytics Pt. 1 4.6.2 DLP Enforcement via Data Tags & Analytics Pt. 1 4.7.1 Integrate DAAS Access w/SDS Policy Pt. 1 4.7.4 Integrate Solution(s) & Policy w/Enterprise IdP Pt. 1
NETWORK & ENVIRONMENT	5.1.1 Define Granular Control Access Rules & Policies Pt. 1 5.2.1 Define SDN APIs	5.1.2 Define Granular Control Access Rules & Policies Pt. 2 5.2.2 Implement SDN Programmable Infrastructure 5.3.1 Datacenter Macro-Segmentation 5.4.1 Implement Micro-Segmentation	5.2.3 Segment Flows into Control, Management, & Data Planes 5.3.2 B/C/P/S Macro-Segmentation 5.4.2 Application & Device Micro-Segmentation 5.4.4 Protect Data in Transit
AUTOMATION & ORCHESTRATION	6.1.1 Policy Inventory & Development 6.2.1 Task Automation Analysis 6.5.1 Response Automation Analysis 6.6.1 Tool Compliance Analysis	6.1.2 Organization Access Profile 6.5.2 Implement SOAR Tools 6.6.2 Standardized API Calls & Schemas Pt. 1 6.7.1 Workflow Enrichment Pt. 1	6.1.3 Enterprise Security Profile Pt. 1 6.2.2 Enterprise Integration & Workflow Provisioning Pt. 1 6.3.1 Implement Data Tagging & Classification ML Tools 6.6.3 Standardized API Calls & Schemas Pt. 2 6.7.2 Workflow Enrichment Pt. 2
VISIBILITY & ANALYTICS	7.1.1 Scale Considerations	7.1.2 Log Parsing 7.2.1 Threat Alerting Pt. 1 7.2.4 Asset ID & Alert Correlation 7.3.1 Implement Analytics Tools 7.5.1 Cyber Threat Intelligence Program Pt. 1	7.1.3 Log Analysis 7.2.2 Threat Alerting Pt. 2 7.2.5 User & Device Baselines 7.3.2 Establish User Baseline Behavior 7.4.1 Baseline & Profiling Pt. 1 7.5.2 Cyber Threat Intelligence Program Pt. 2

Target Activities: 91

Figure D-1: Target-level Activities by Pillar

Activity 1.2.1 Implement Application-Based Permissions per Enterprise

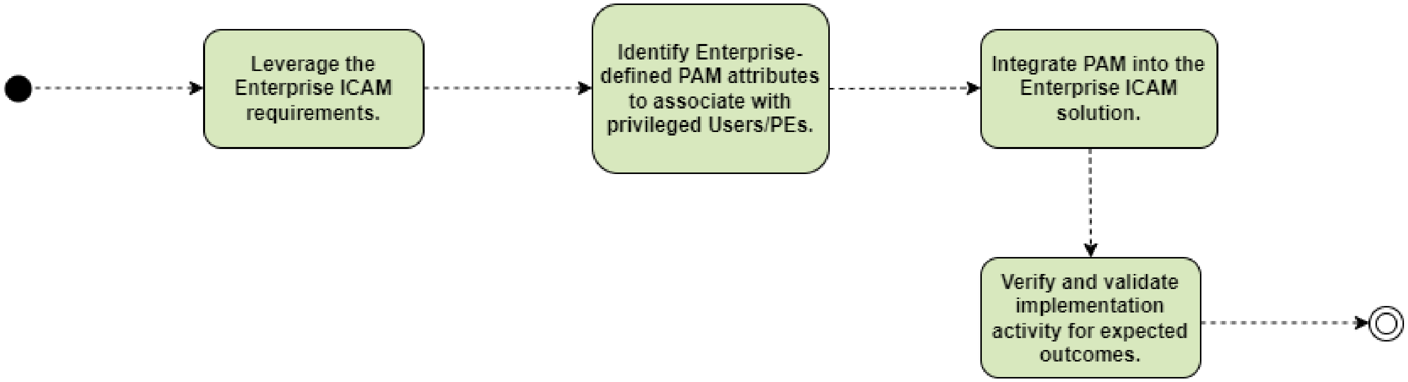

Leverage the Enterprise ICAM requirements.
Identify Enterprise-defined PAM attributes to associate with privileged Users/PEs.
Integrate PAM into the Enterprise ICAM solution.
Verify and validate implementation activity for expected outcomes.

Figure D-2: Implementation Tasks for Activity 1.2.1 — Implement Application-Based Permissions per Enterprise

Activity 1.2.2 Rule-Based Dynamic Access Part 1

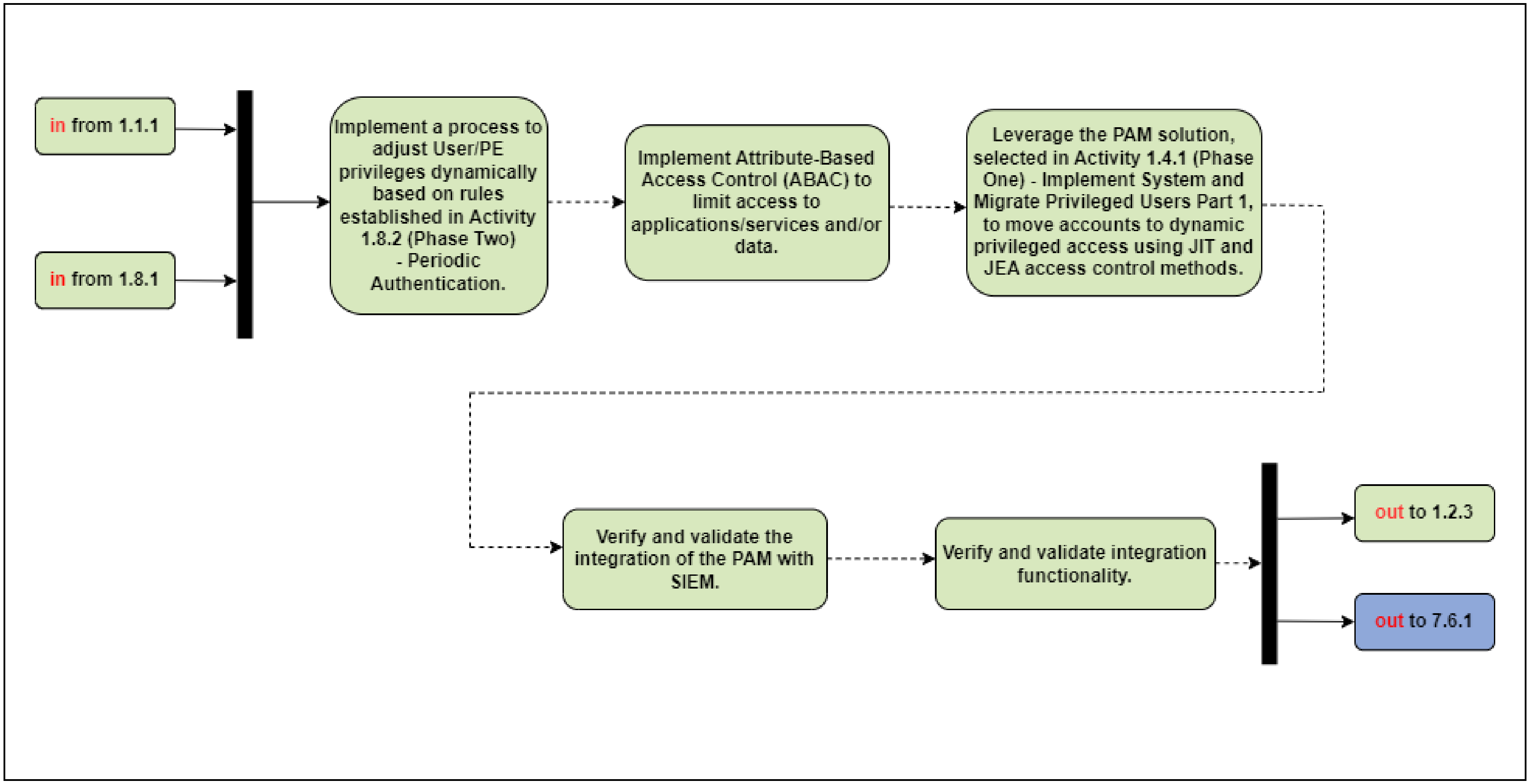

in from 1.1.1
in from 1.8.1
Implement a process to adjust User/PE privileges dynamically based on rules established in Activity 1.8.2 (Phase Two) - Periodic Authentication.
Implement Attribute-Based Access Control (ABAC) to limit access to applications/services and/or data.
Leverage the PAM solution, selected in Activity 1.4.1 (Phase One) - Implement System and Migrate Privileged Users Part 1, to move accounts to dynamic privileged access using JIT and JEA access control methods.
Verify and validate the integration of the PAM with SIEM.
Verify and validate integration functionality.
out to 1.2.3
out to 7.6.1

Figure D-3: Implementation Tasks for Activity 1.2.2 — Rule-Based Dynamic Access Part 1

Activity 1.4.2 Implement System and Migrate Privileged Users Part 2

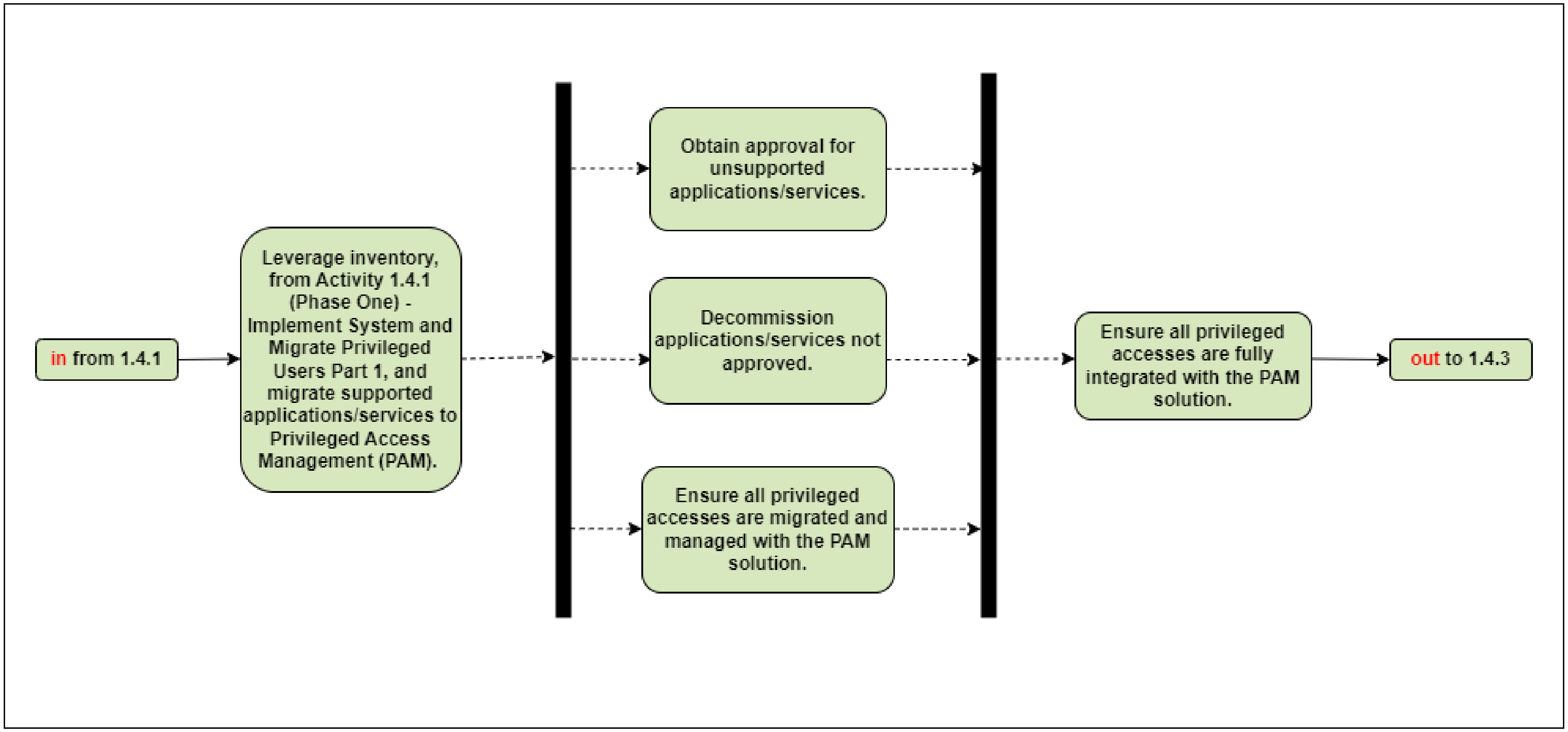

in from 1.4.1
Leverage inventory, from Activity 1.4.1 (Phase One) - Implement System and Migrate Privileged Users Part 1, and migrate supported applications/services to Privileged Access Management (PAM).
Obtain approval for unsupported applications/services.
Decommission applications/services not approved.
Ensure all privileged accesses are migrated and managed with the PAM solution.
Ensure all privileged accesses are fully integrated with the PAM solution.
out to 1.4.3

Figure D-4: Implementation Tasks for Activity 1.4.2 — Implement System and Migrate Privileged Users Part 2

Activity 1.5.2 Enterprise Identity Lifecycle Management (ILM) Part 1

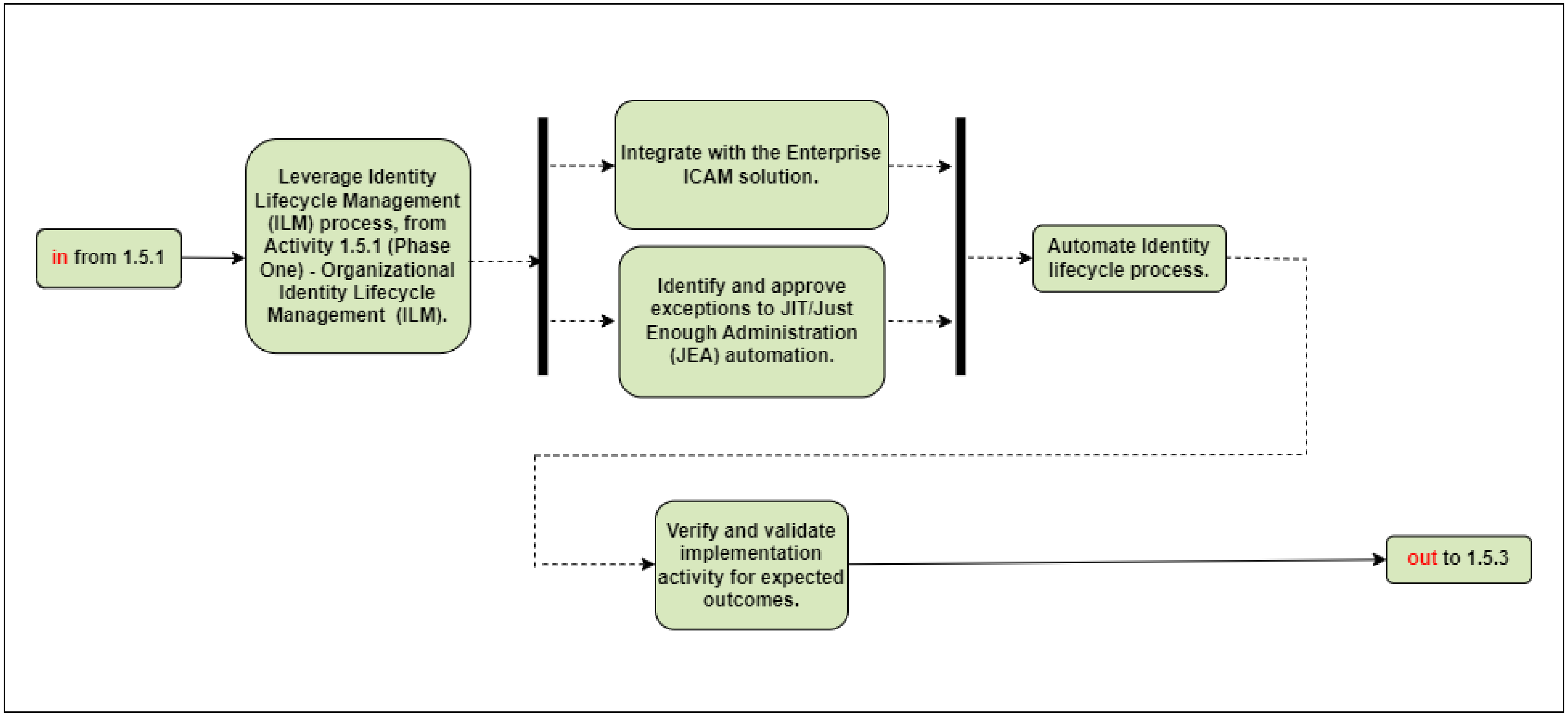

in from 1.5.1
Leverage Identity Lifecycle Management (ILM) process, from Activity 1.5.1 (Phase One) - Organizational Identity Lifecycle Management (ILM).
Integrate with the Enterprise ICAM solution.
Identify and approve exceptions to JIT/Just Enough Administration (JEA) automation.
Automate Identity lifecycle process.
Verify and validate implementation activity for expected outcomes.
out to 1.5.3

Figure D-5: Implementation Tasks for Activity 1.5.2 — Enterprise Identity Lifecycle Management (ILM) Part 1

Activity 1.6.1 Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling

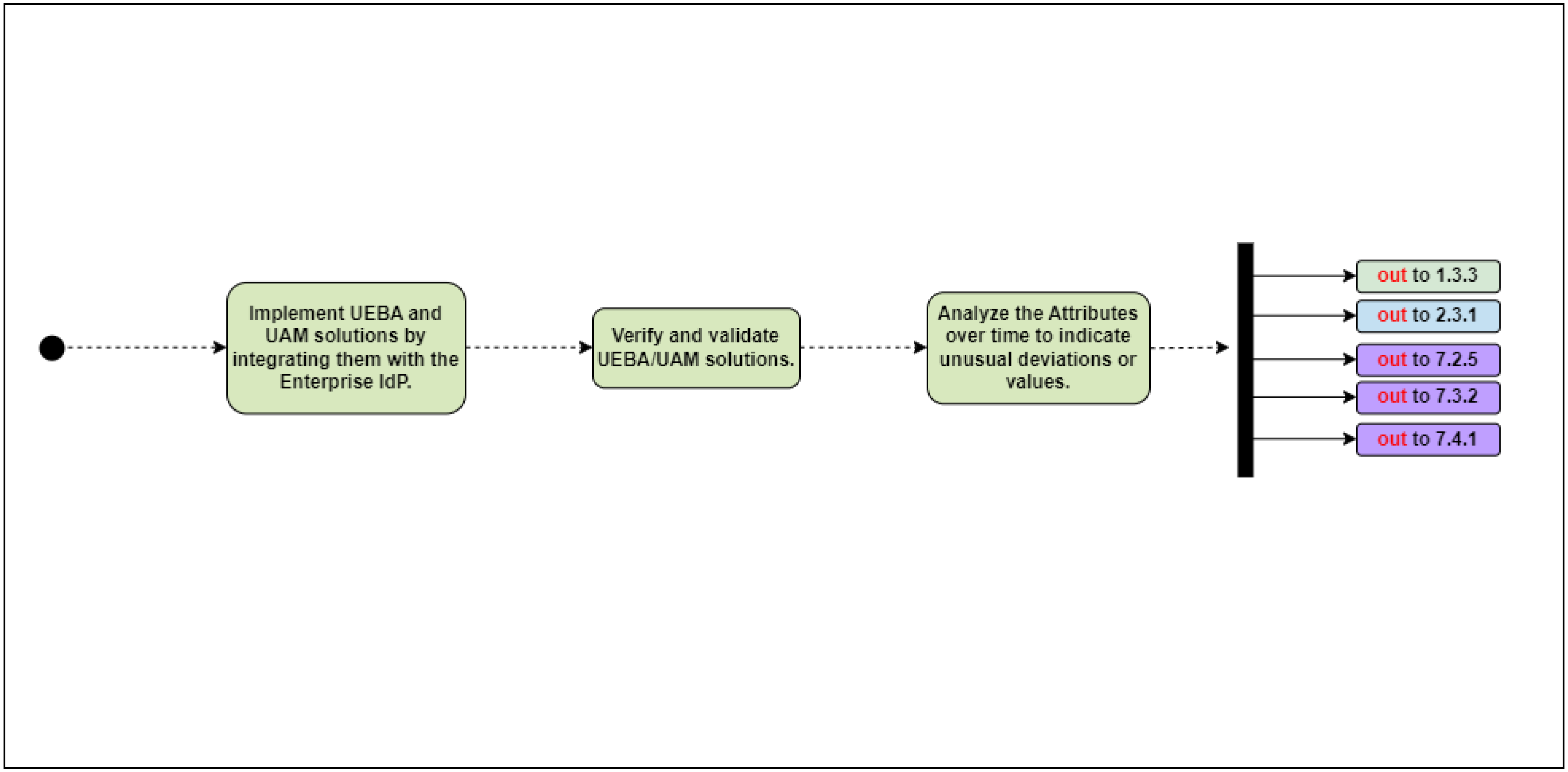

Implement UEBA and UAM solutions by integrating them with the Enterprise IdP.
Verify and validate UEBA/UAM solutions.
Analyze the Attributes over time to indicate unusual deviations or values.
out to 1.3.3
out to 2.3.1
out to 7.2.5
out to 7.3.2
out to 7.4.1

Figure D-6: Implementation Tasks for Activity 1.6.1 — Implement User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) Tooling

Activity 1.8.2 Periodic Authentication

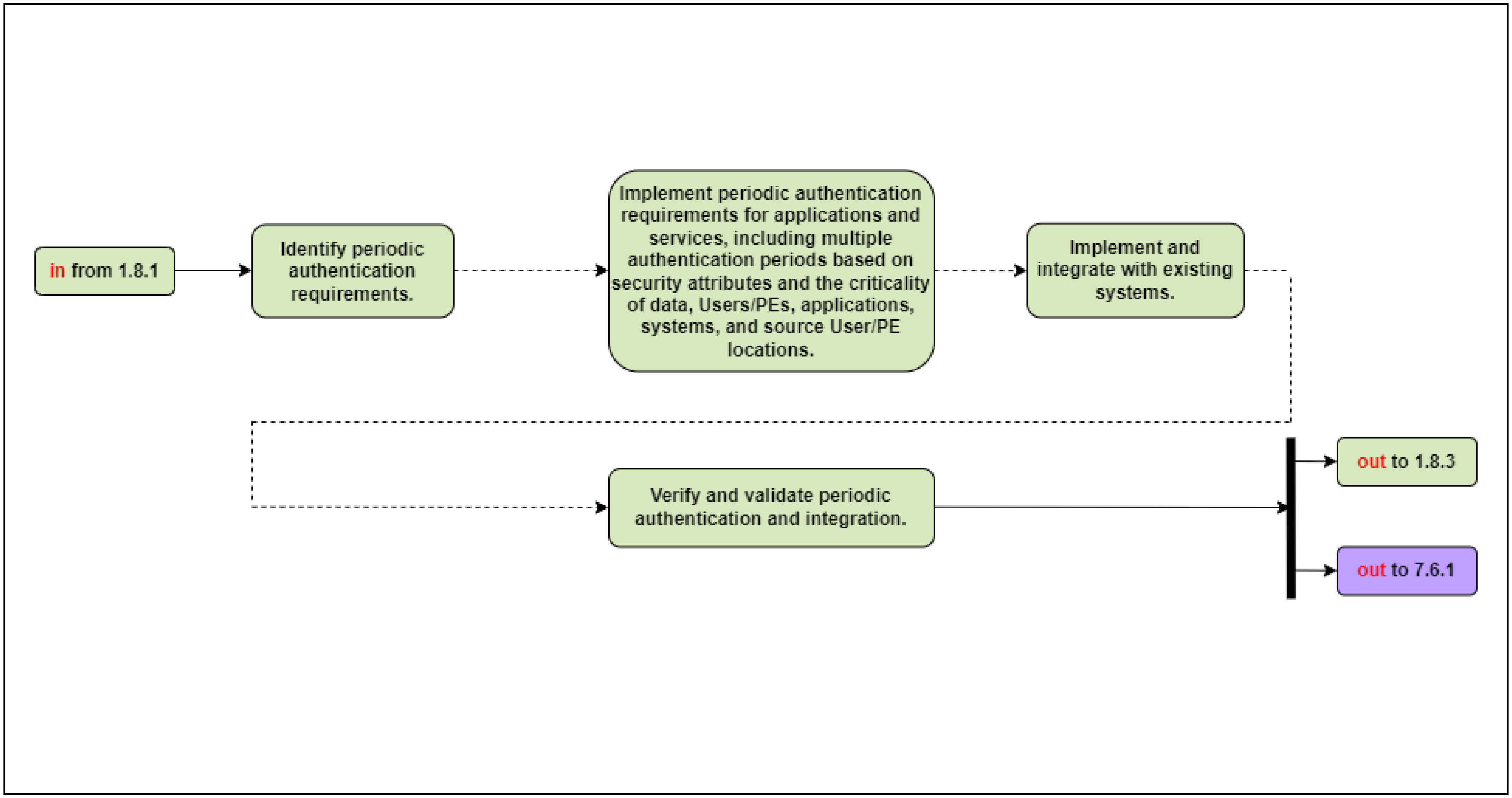

in from 1.8.1
Identify periodic authentication requirements.
Implement periodic authentication requirements for applications and services, including multiple authentication periods based on security attributes and the criticality of data, Users/PEs, applications, systems, and source User/PE locations.
Implement and integrate with existing systems.
Verify and validate periodic authentication and integration.
out to 1.8.3
out to 7.6.1

Figure D-7: Implementation Tasks for Activity 1.8.2 — Periodic Authentication

Activity 1.9.1 Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1

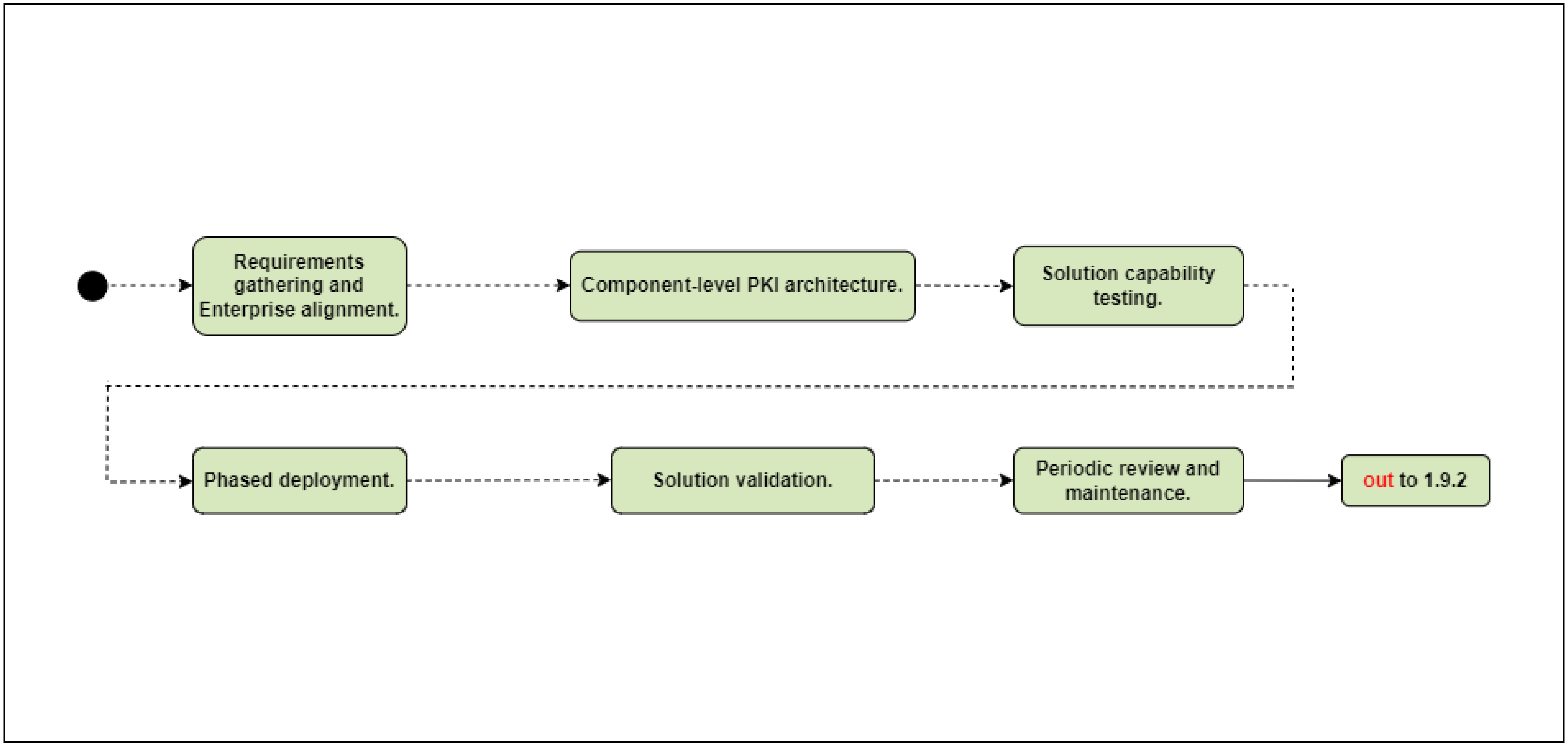

Requirements gathering and Enterprise alignment.
Component-level PKI architecture.
Solution capability testing.
Phased deployment.
Solution validation.
Periodic review and maintenance.
out to 1.9.2

Figure D-8: Implementation Tasks for Activity 1.9.1 — Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1

Activity 2.1.3 Enterprise Identity Provider (IdP) Part 1

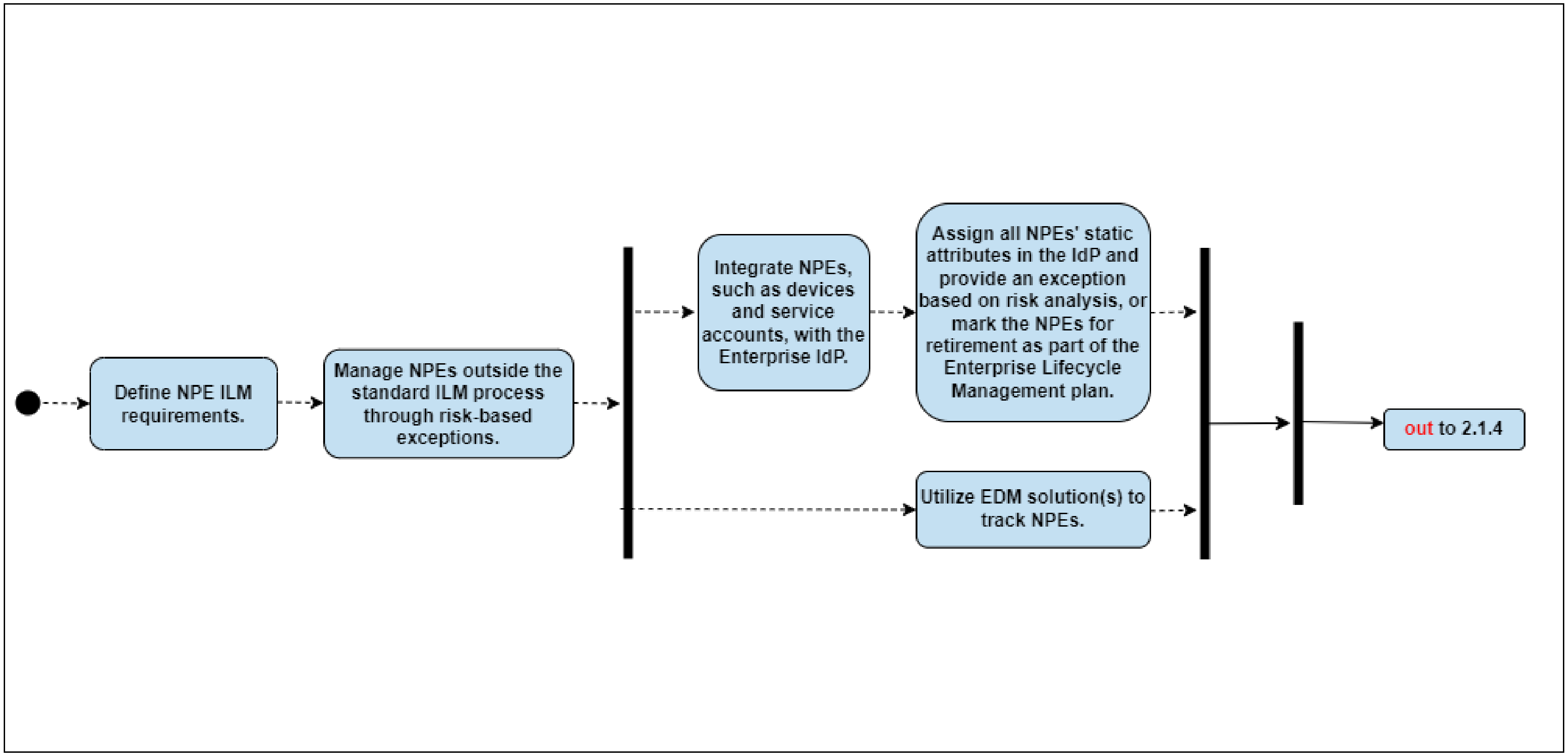

Define NPE ILM requirements.
Manage NPEs outside the standard ILM process through risk-based exceptions.
Integrate NPEs, such as devices and service accounts, with the Enterprise IdP.
Assign all NPEs' static attributes in the IdP and provide an exception based on risk analysis, or mark the NPEs for retirement as part of the Enterprise Lifecycle Management plan.
Utilize EDM solution(s) to track NPEs.
out to 2.1.4

Figure D-9: Implementation Tasks for Activity 2.1.3 — Enterprise Identity Provider (IdP) Part 1

Activity 2.2.1 Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1

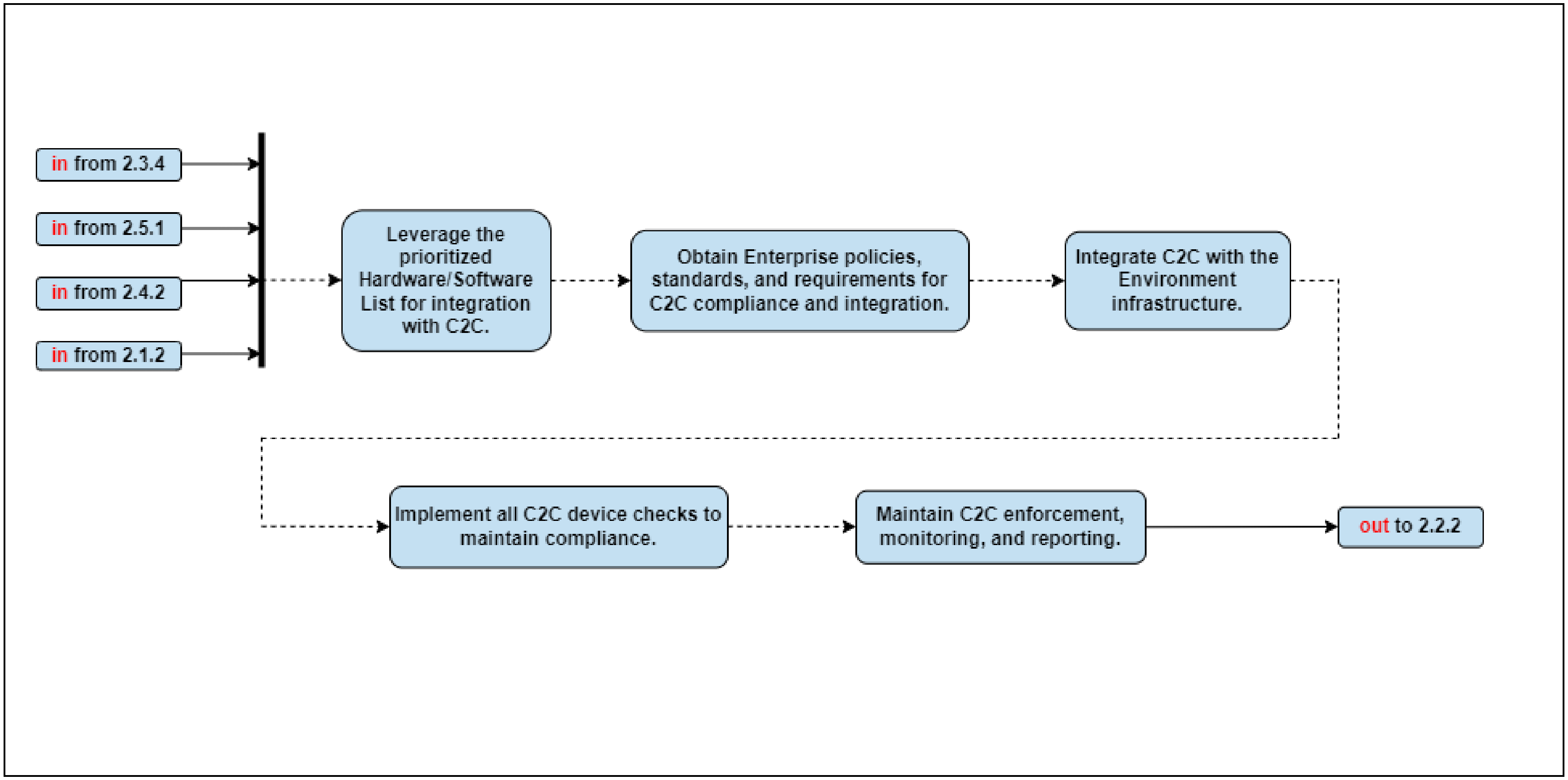

in from 2.3.4
in from 2.5.1
in from 2.4.2
in from 2.1.2
Leverage the prioritized Hardware/Software List for integration with C2C.
Obtain Enterprise policies, standards, and requirements for C2C compliance and integration.
Integrate C2C with the Environment infrastructure.
Implement all C2C device checks to maintain compliance.
Maintain C2C enforcement, monitoring, and reporting.
out to 2.2.2

Figure D-10: Implementation Tasks for Activity 2.2.1 — Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1

Activity 2.3.3 Implement Application Control and File Integrity Monitoring (FIM) Tools

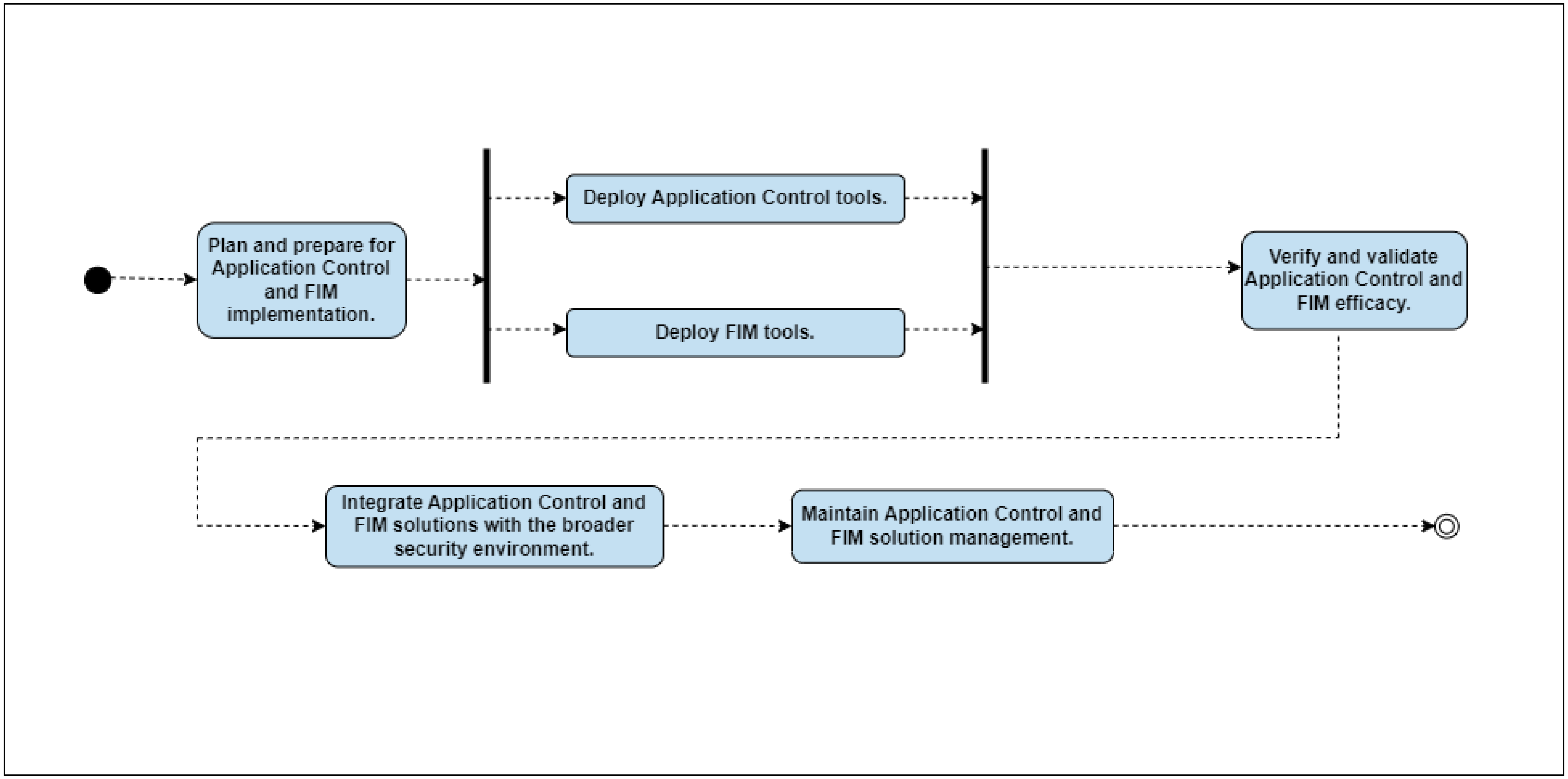

Plan and prepare for Application Control and FIM implementation.
Deploy Application Control tools.
Deploy FIM tools.
Verify and validate Application Control and FIM efficacy.
Integrate Application Control and FIM solutions with the broader security environment.
Maintain Application Control and FIM solution management.

Figure D-11: Implementation Tasks for Activity 2.3.3 — Implement Application Control and File Integrity Monitoring (FIM) Tools

Activity 2.4.2 Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support

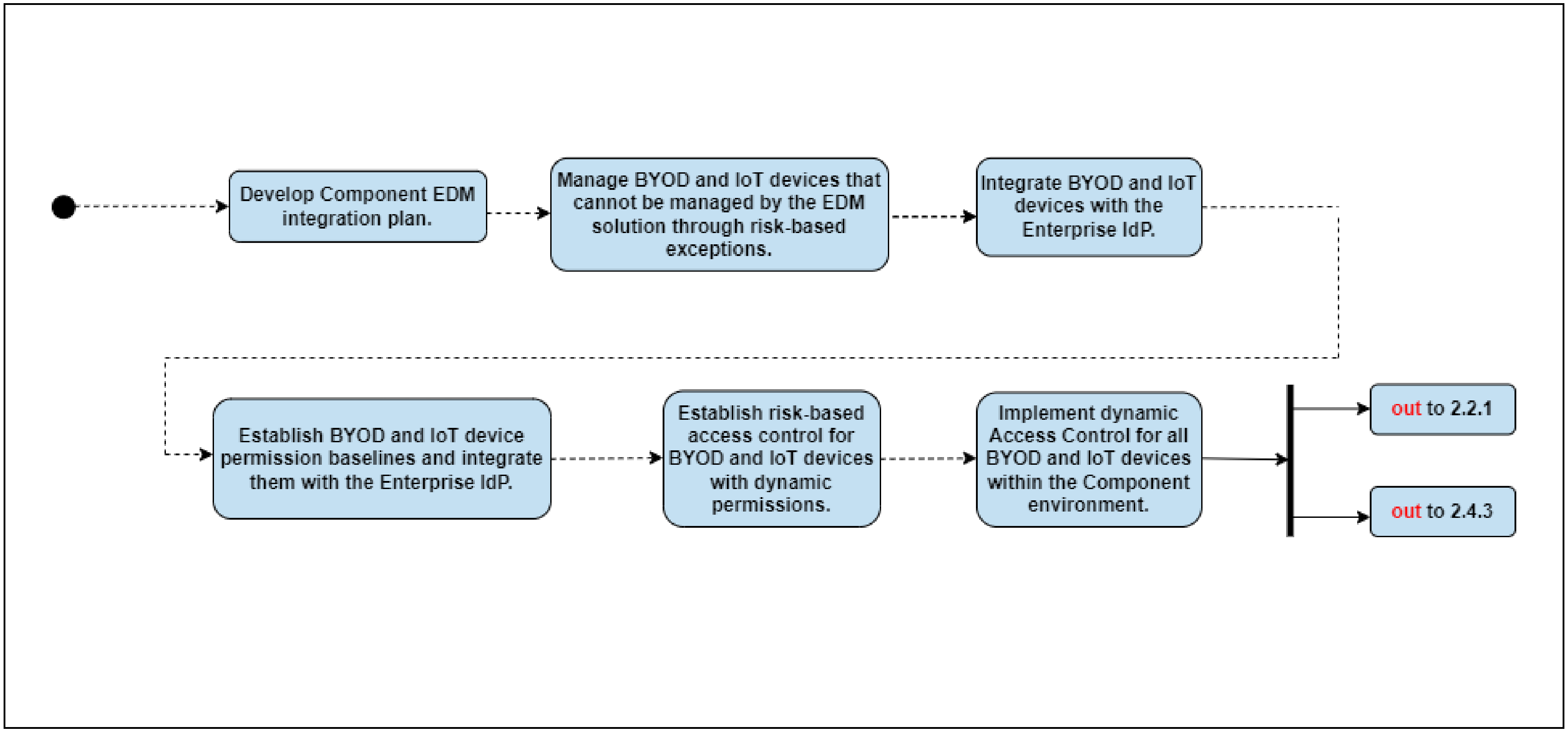

Develop Component EDM integration plan.
Manage BYOD and IoT devices that cannot be managed by the EDM solution through risk-based exceptions.
Integrate BYOD and IoT devices with the Enterprise IdP.
Establish BYOD and IoT device permission baselines and integrate them with the Enterprise IdP.
Establish risk-based access control for BYOD and IoT devices with dynamic permissions.
Implement dynamic Access Control for all BYOD and IoT devices within the Component environment.
out to 2.2.1
out to 2.4.3

Figure D-12: Implementation Tasks for Activity 2.4.2 — Managed and Limited Bring Your Own Device (BYOD) and Internet of Things (IoT) Support

Activity 2.6.3 Enterprise Device Management (EDM) Part 2

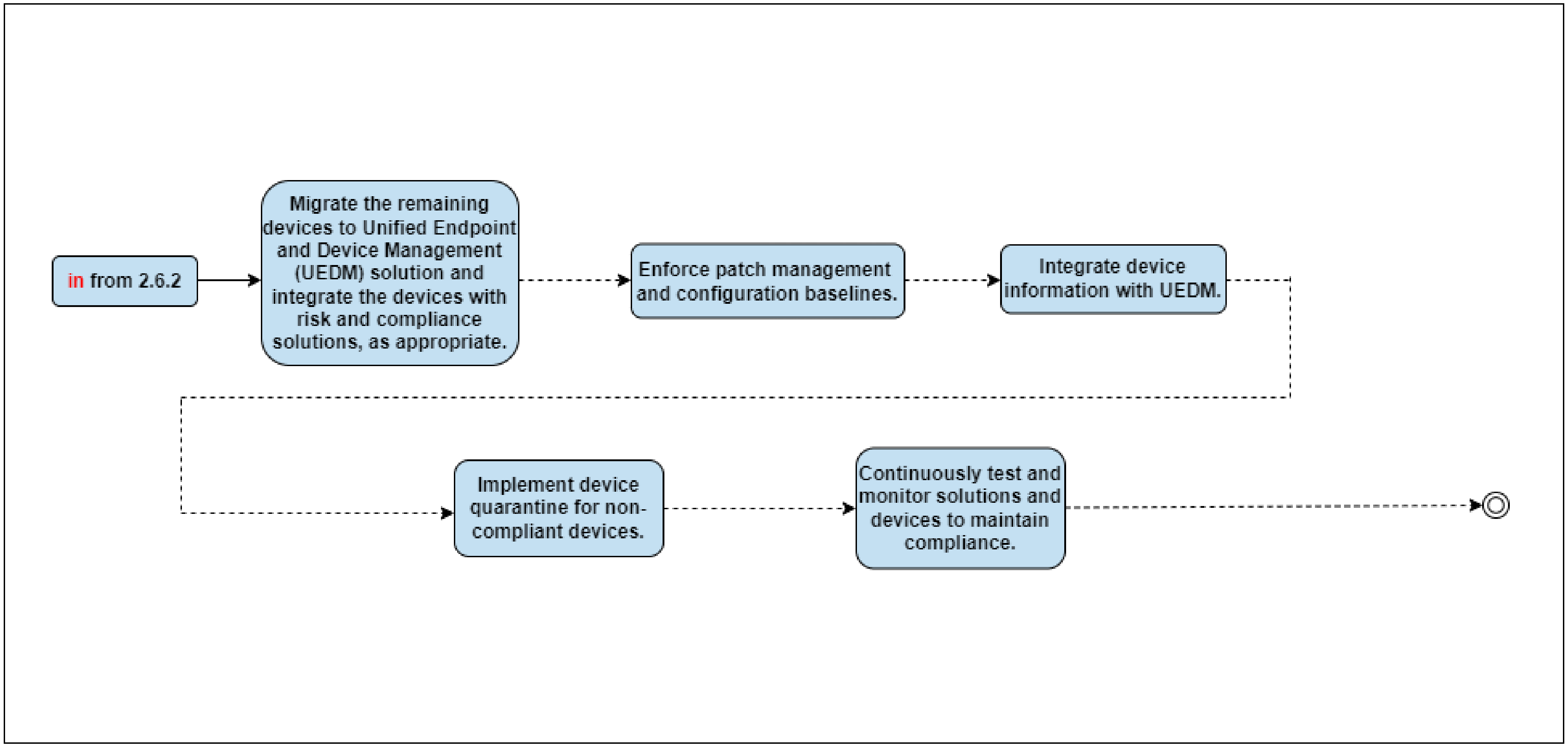

in from 2.6.2
Migrate the remaining devices to Unified Endpoint and Device Management (UEDM) solution and integrate the devices with risk and compliance solutions, as appropriate.
Enforce patch management and configuration baselines.
Integrate device information with UEDM.
Implement device quarantine for non-compliant devices.
Continuously test and monitor solutions and devices to maintain compliance.

Figure D-13: Implementation Tasks for Activity 2.6.3 — Enterprise Device Management (EDM) Part 2

Activity 2.7.2 Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1

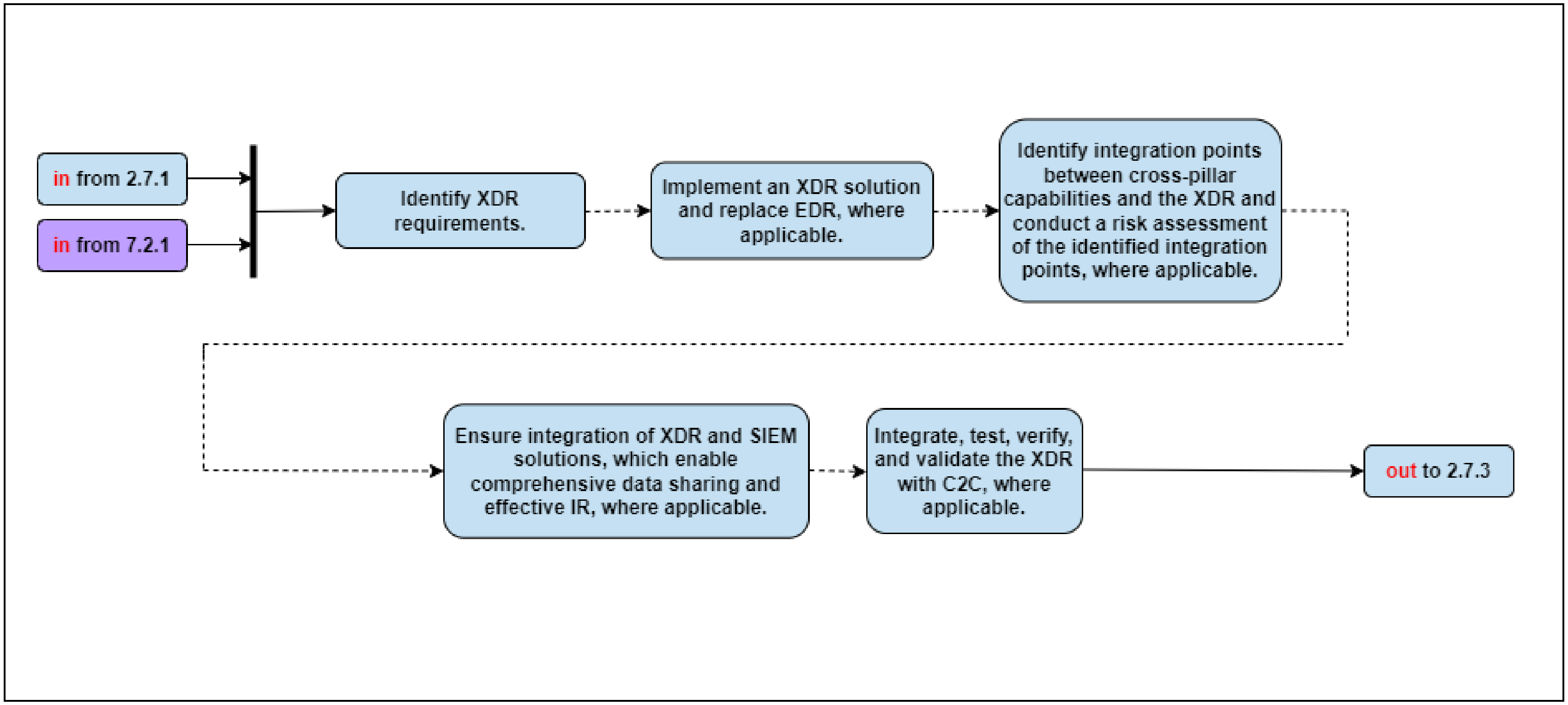

in from 2.7.1
in from 7.2.1
Identify XDR requirements.
Implement an XDR solution and replace EDR, where applicable.
Identify integration points between cross-pillar capabilities and the XDR and conduct a risk assessment of the identified integration points, where applicable.
Ensure integration of XDR and SIEM solutions, which enable comprehensive data sharing and effective IR, where applicable.
Integrate, test, verify, and validate the XDR with C2C, where applicable.
out to 2.7.3

Figure D-14: Implementation Tasks for Activity 2.7.2 — Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1

Activity 3.2.3 Automate Application Security and Code Remediation Part 1

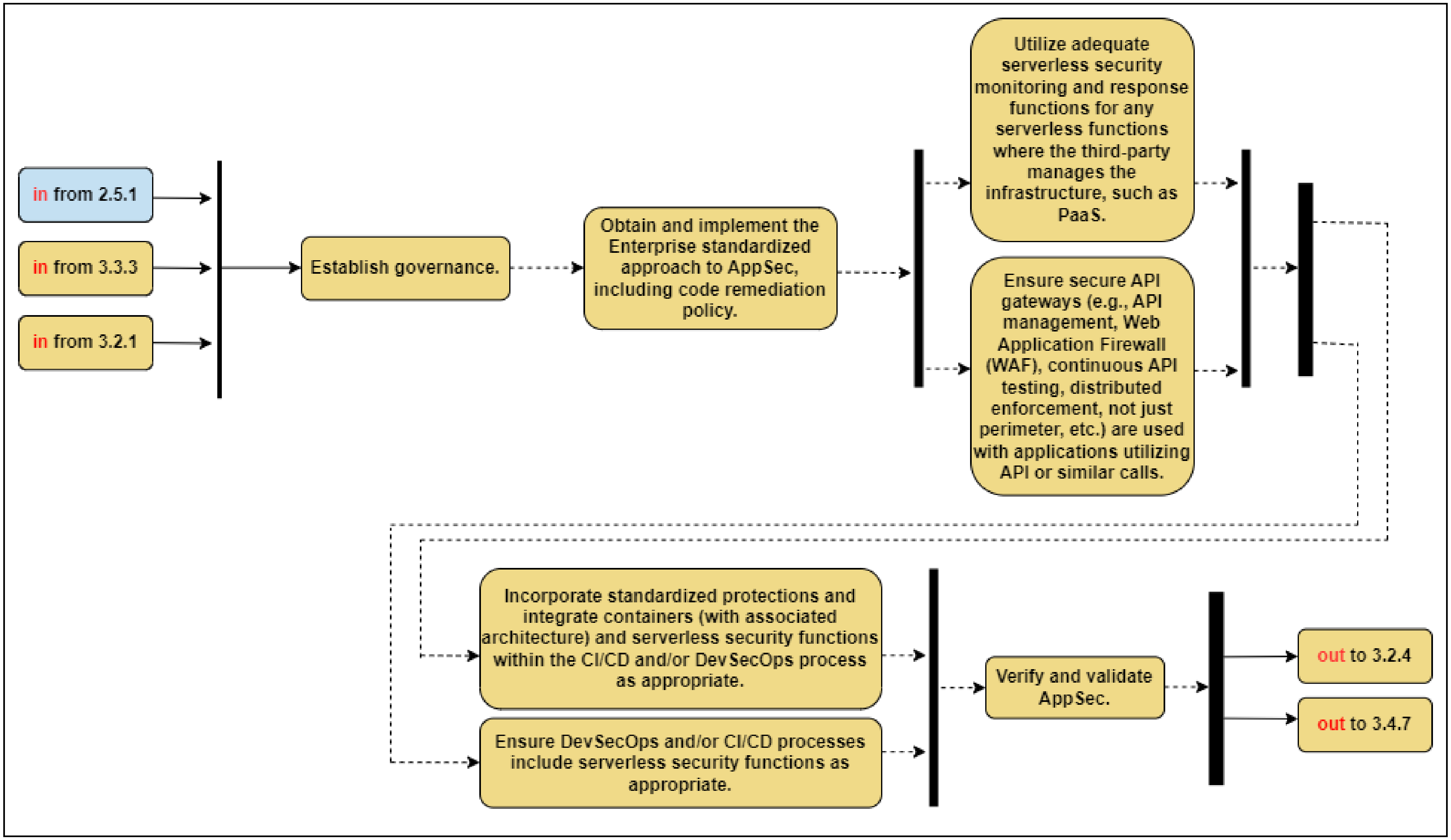

in from 2.5.1
in from 3.3.3
in from 3.2.1
Establish governance.
Obtain and implement the Enterprise standardized approach to AppSec, including code remediation policy.
Utilize adequate serverless security monitoring and response functions for any serverless functions where the third-party manages the infrastructure, such as PaaS.
Ensure secure API gateways (e.g., API management, Web Application Firewall (WAF), continuous API testing, distributed enforcement, not just perimeter, etc.) are used with applications utilizing API or similar calls.
Incorporate standardized protections and integrate containers (with associated architecture) and serverless security functions within the CI/CD and/or DevSecOps process as appropriate.
Ensure DevSecOps and/or CI/CD processes include serverless security functions as appropriate.
Verify and validate AppSec.
out to 3.2.4
out to 3.4.7

Figure D-15: Implementation Tasks for Activity 3.2.3 — Automate Application Security and Code Remediation Part 1

Activity 3.3.3 Vulnerability Management Program Part 2

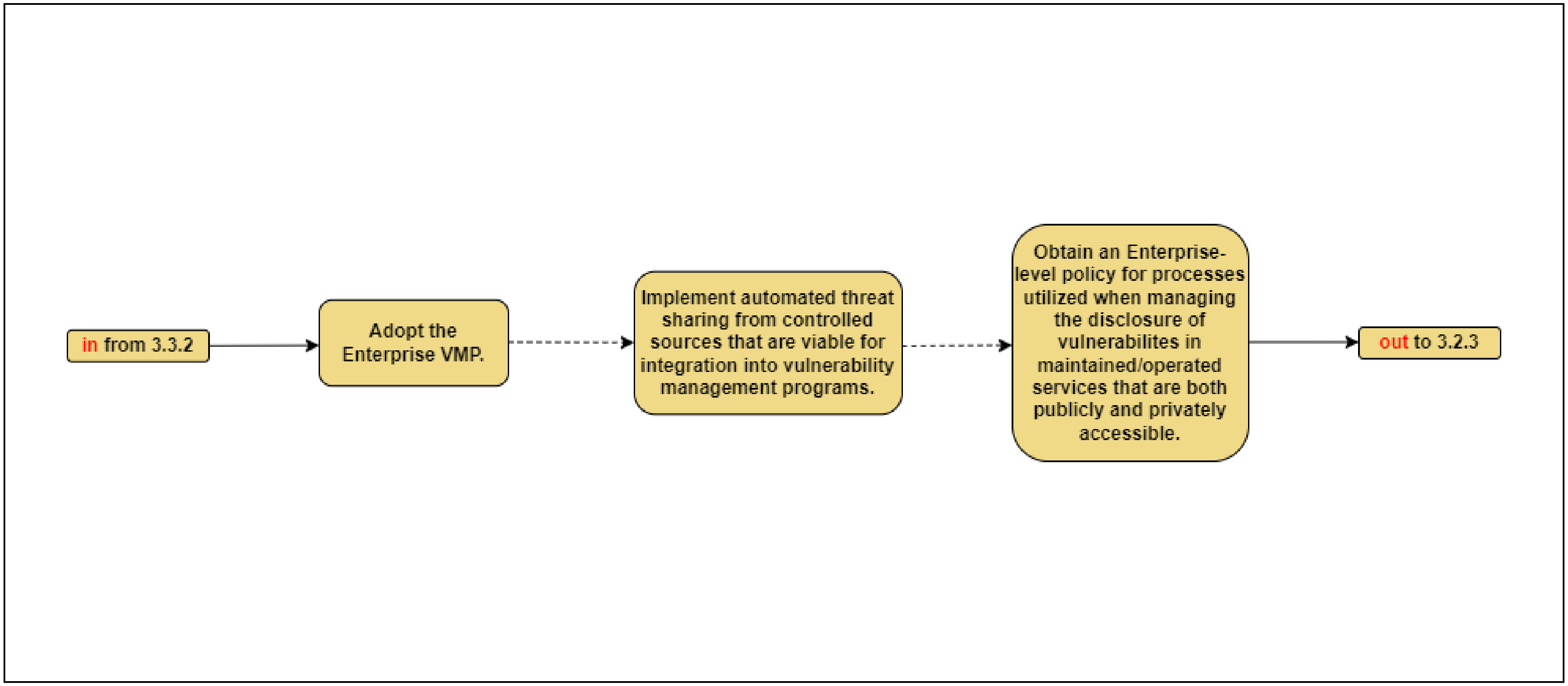

in from 3.3.2
Adopt the Enterprise VMP.
Implement automated threat sharing from controlled sources that are viable for integration into vulnerability management programs.
Obtain an Enterprise-level policy for processes utilized when managing the disclosure of vulnerabilites in maintained/operated services that are both publicly and privately accessible.
out to 3.2.3

Figure D-16: Implementation Tasks for Activity 3.3.3 — Vulnerability Management Program Part 2

Activity 3.3.4 Continual Validation

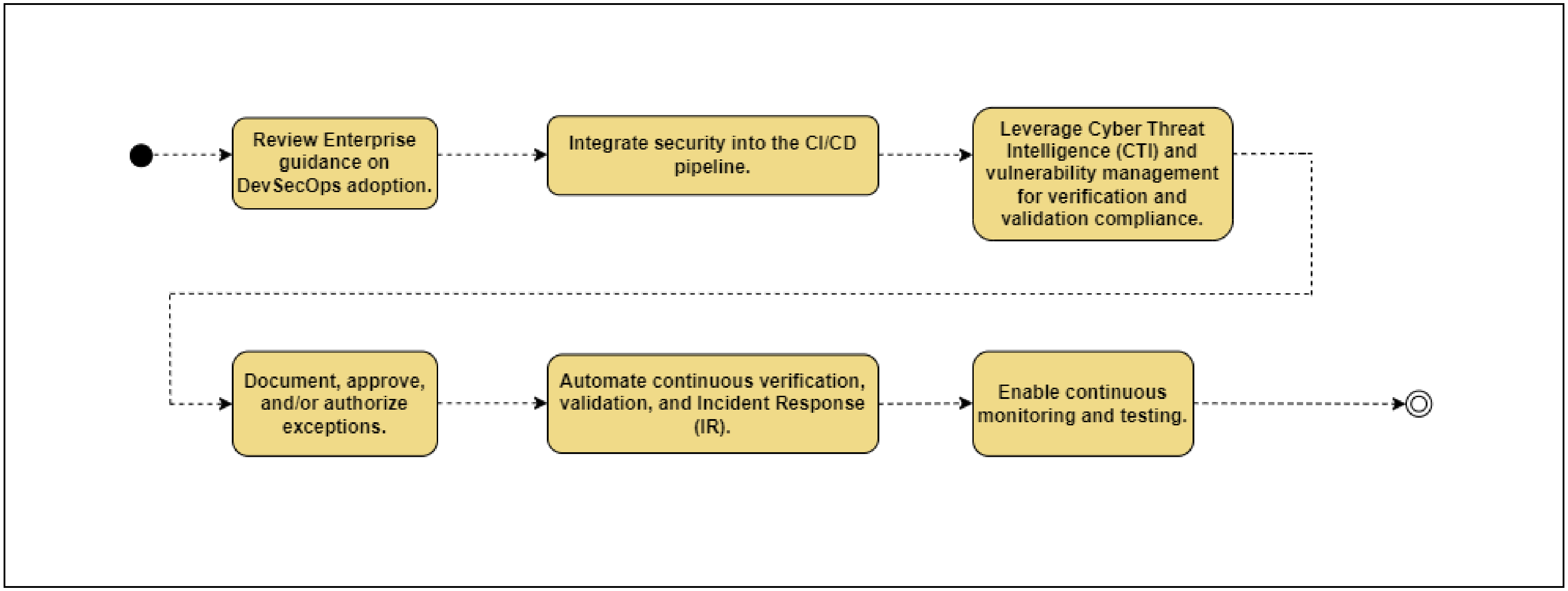

Review Enterprise guidance on DevSecOps adoption.
Integrate security into the CI/CD pipeline.
Leverage Cyber Threat Intelligence (CTI) and vulnerability management for verification and validation compliance.
Document, approve, and/or authorize exceptions.
Automate continuous verification, validation, and Incident Response (IR).
Enable continuous monitoring and testing.

Figure D-17: Implementation Tasks for Activity 3.3.4 — Continual Validation

Activity 3.4.2 Resource Authorization Part 2

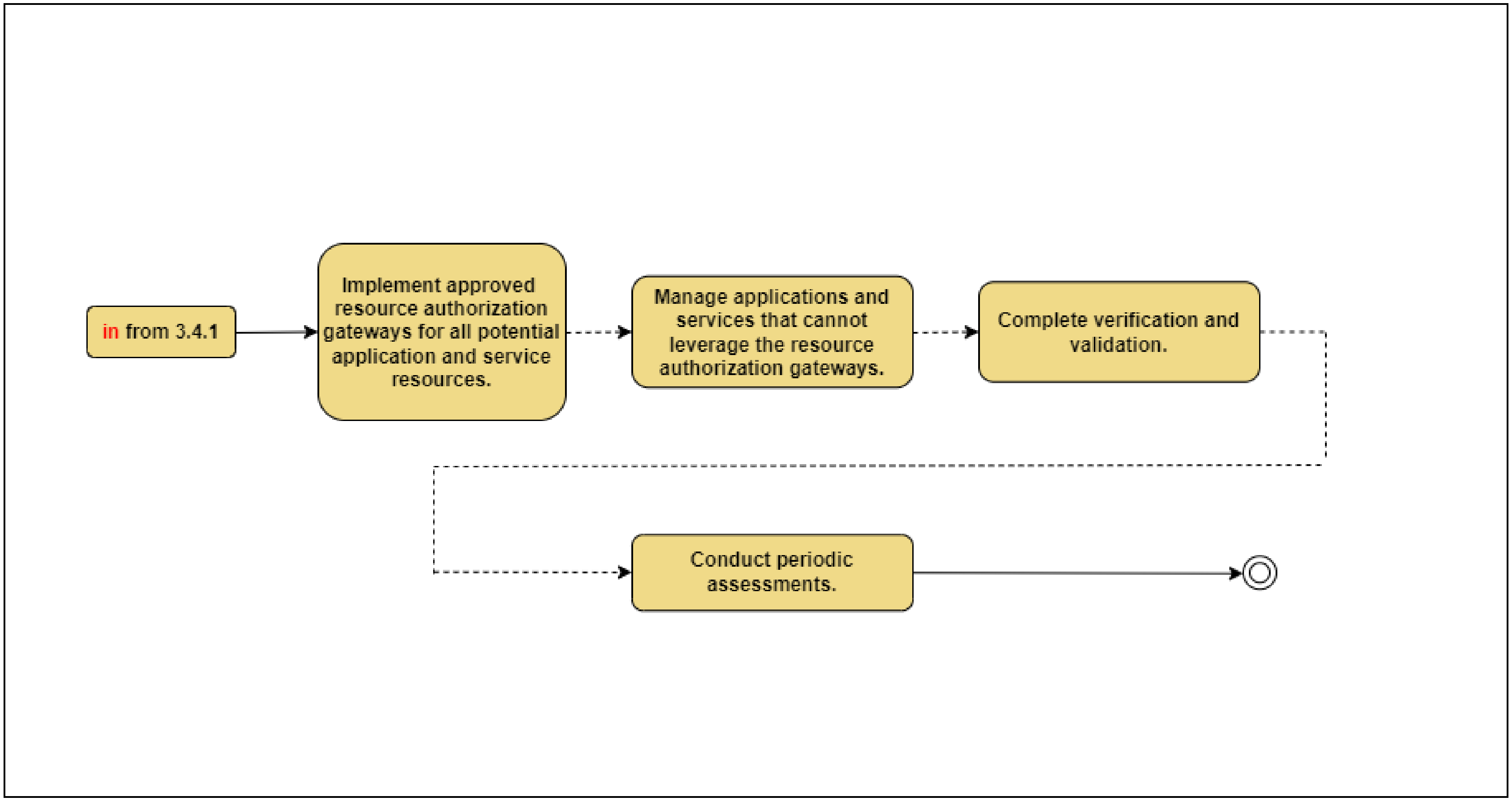

in from 3.4.1
Implement approved resource authorization gateways for all potential application and service resources.
Manage applications and services that cannot leverage the resource authorization gateways.
Complete verification and validation.
Conduct periodic assessments.

Figure D-18: Implementation Tasks for Activity 3.4.2 — Resource Authorization Part 2

Activity 3.4.4 Software-Defined Compute (SDC) Resource Authorization Part 2

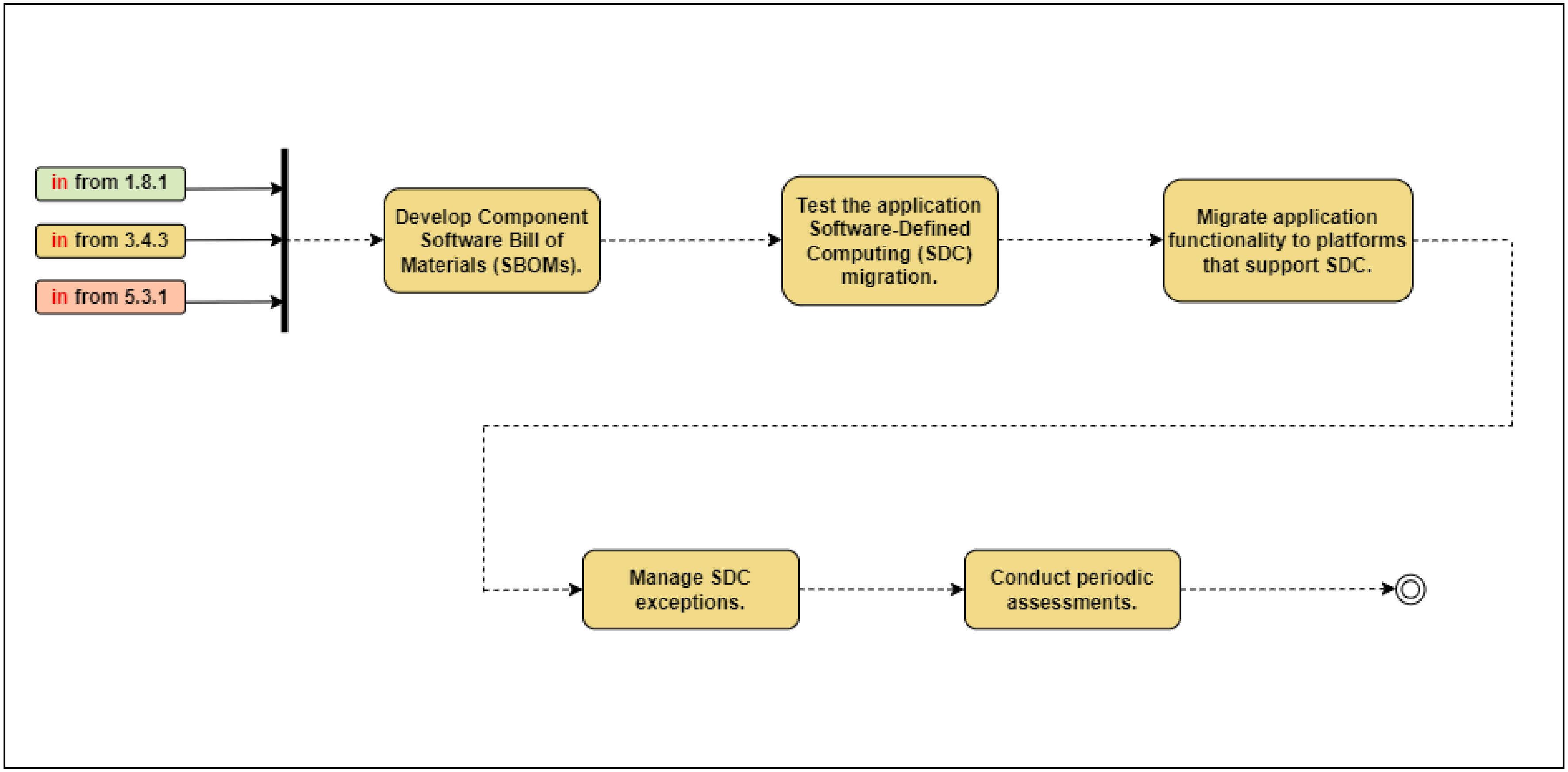

in from 1.8.1
in from 3.4.3
in from 5.3.1
Develop Component Software Bill of Materials (SBOMs).
Test the application Software-Defined Computing (SDC) migration.
Migrate application functionality to platforms that support SDC.
Manage SDC exceptions.
Conduct periodic assessments.

Figure D-19: Implementation Tasks for Activity 3.4.4 — Software-Defined Compute (SDC) Resource Authorization Part 2

Activity 4.2.3 Develop Software-Defined Storage (SDS) Policy

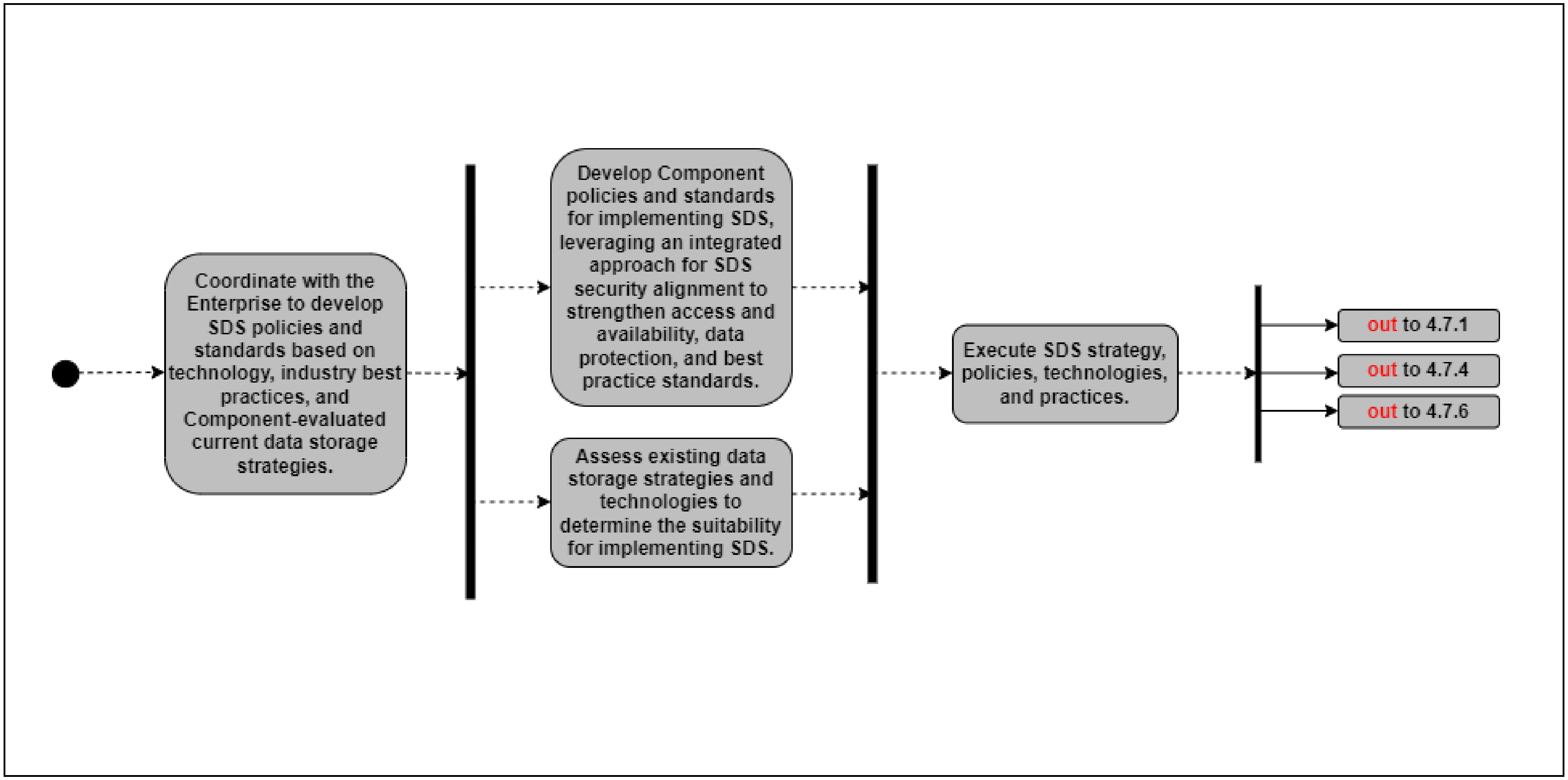

Coordinate with the Enterprise to develop SDS policies and standards based on technology, industry best practices, and Component-evaluated current data storage strategies.
Develop Component policies and standards for implementing SDS, leveraging an integrated approach for SDS security alignment to strengthen access and availability, data protection, and best practice standards.
Assess existing data storage strategies and technologies to determine the suitability for implementing SDS.
Execute SDS strategy, policies, technologies, and practices.
out to 4.7.1
out to 4.7.4
out to 4.7.6

Figure D-20: Implementation Tasks for Activity 4.2.3 — Develop Software-Defined Storage (SDS) Policy

Activity 4.3.2 Manual Data Tagging Part 1

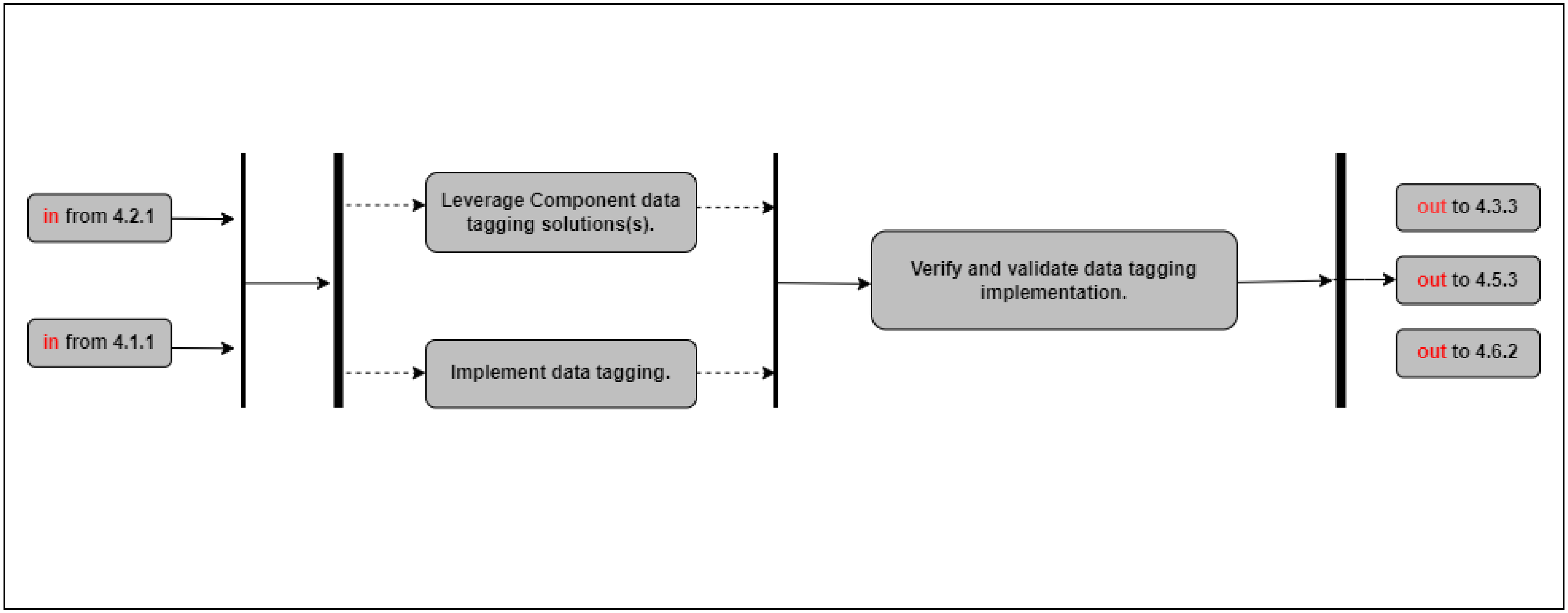

in from 4.2.1
in from 4.1.1
Leverage Component data tagging solutions(s).
Implement data tagging.
Verify and validate data tagging implementation.
out to 4.3.3
out to 4.5.3
out to 4.6.2

Figure D-21: Implementation Tasks for Activity 4.3.2 — Manual Data Tagging Part 1

Activity 4.4.4 File Activity Monitoring Part 2

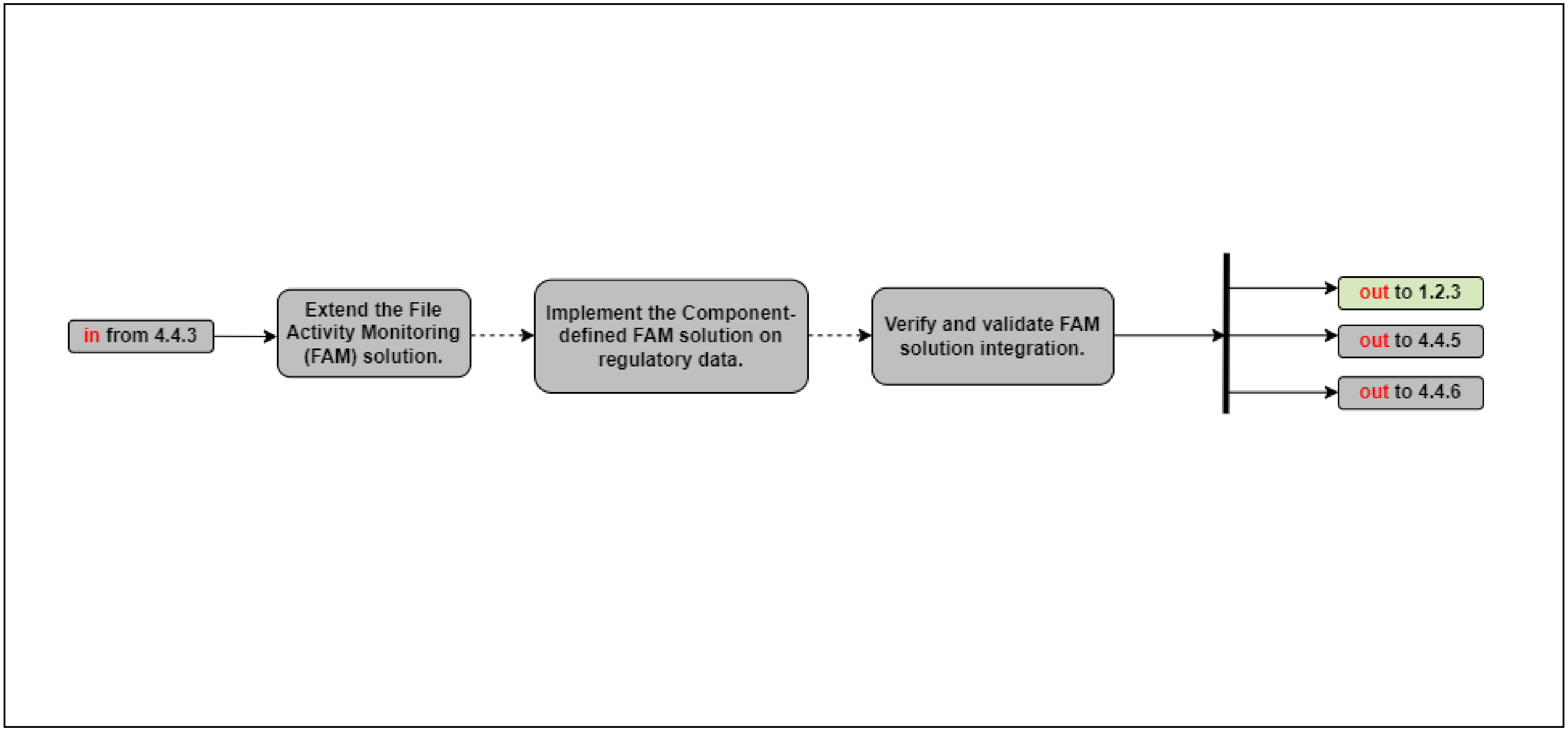

in from 4.4.3
Extend the File Activity Monitoring (FAM) solution.
Implement the Component-defined FAM solution on regulatory data.
Verify and validate FAM solution integration.
out to 1.2.3
out to 4.4.5
out to 4.4.6

Figure D-22: Implementation Tasks for Activity 4.4.4 — File Activity Monitoring Part 2

Activity 4.5.2 Implement Data Rights Management (DRM) and Protection Tools Part 2

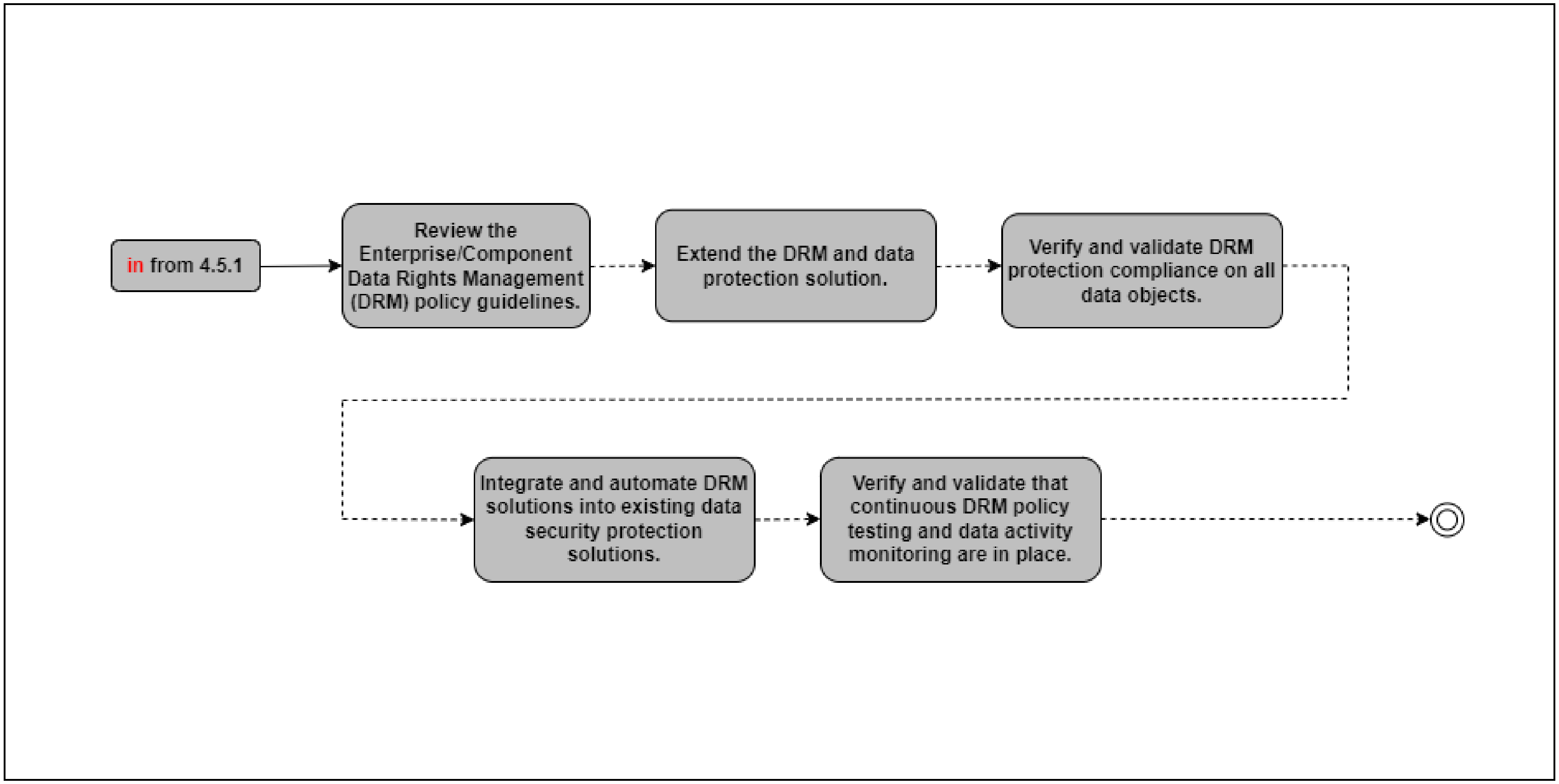

in from 4.5.1
Review the Enterprise/Component Data Rights Management (DRM) policy guidelines.
Extend the DRM and data protection solution.
Verify and validate DRM protection compliance on all data objects.
Integrate and automate DRM solutions into existing data security protection solutions.
Verify and validate that continuous DRM policy testing and data activity monitoring are in place.

Figure D-23: Implementation Tasks for Activity 4.5.2 — Implement Data Rights Management (DRM) and Protection Tools Part 2

Activity 4.5.3 Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1

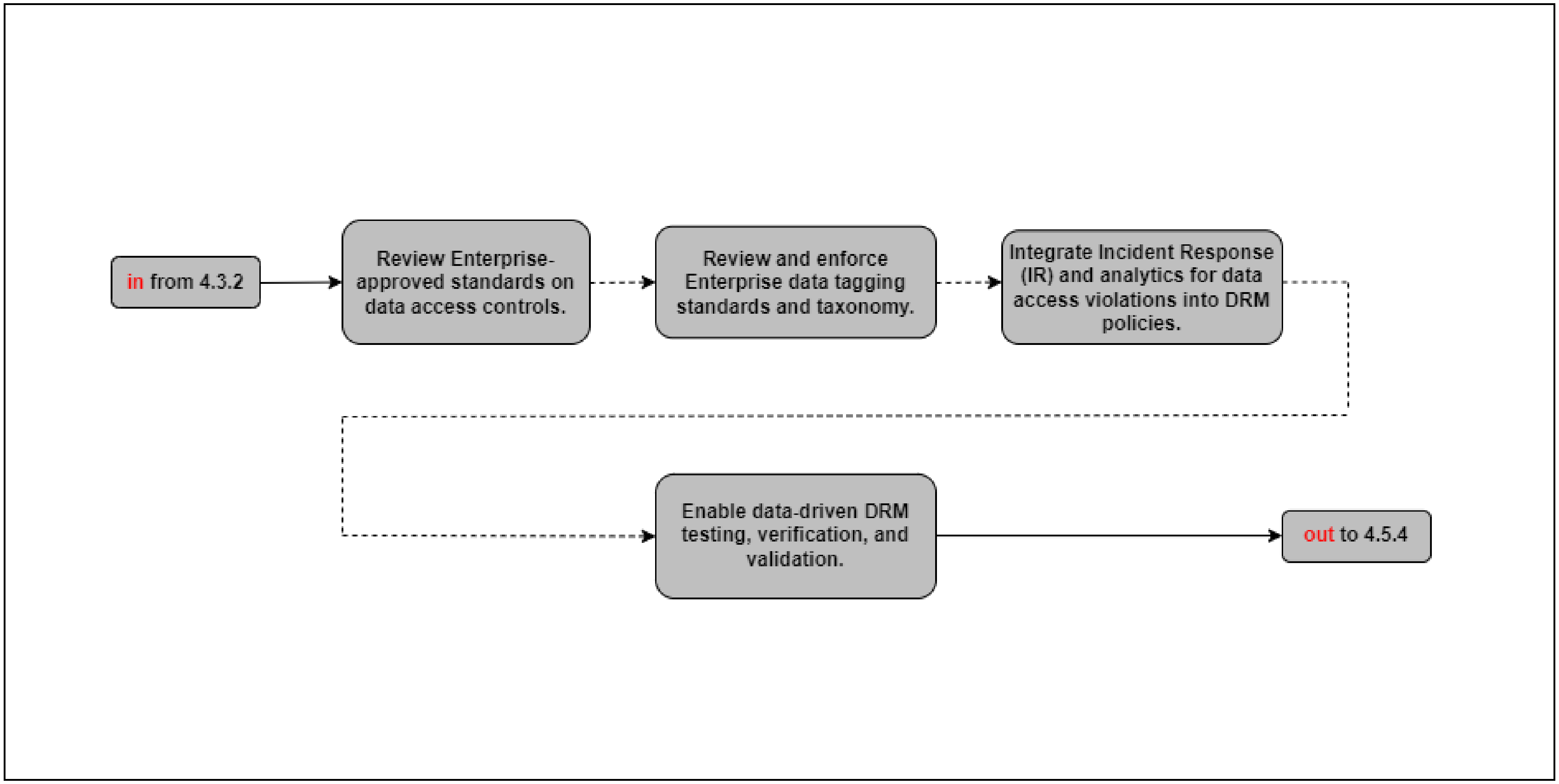

in from 4.3.2
Review Enterprise-approved standards on data access controls.
Review and enforce Enterprise data tagging standards and taxonomy.
Integrate Incident Response (IR) and analytics for data access violations into DRM policies.
Enable data-driven DRM testing, verification, and validation.
out to 4.5.4

Figure D-24: Implementation Tasks for Activity 4.5.3 — Data Rights Management (DRM) Enforcement via Data Tags and Analytics Part 1

Activity 4.6.2 Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1

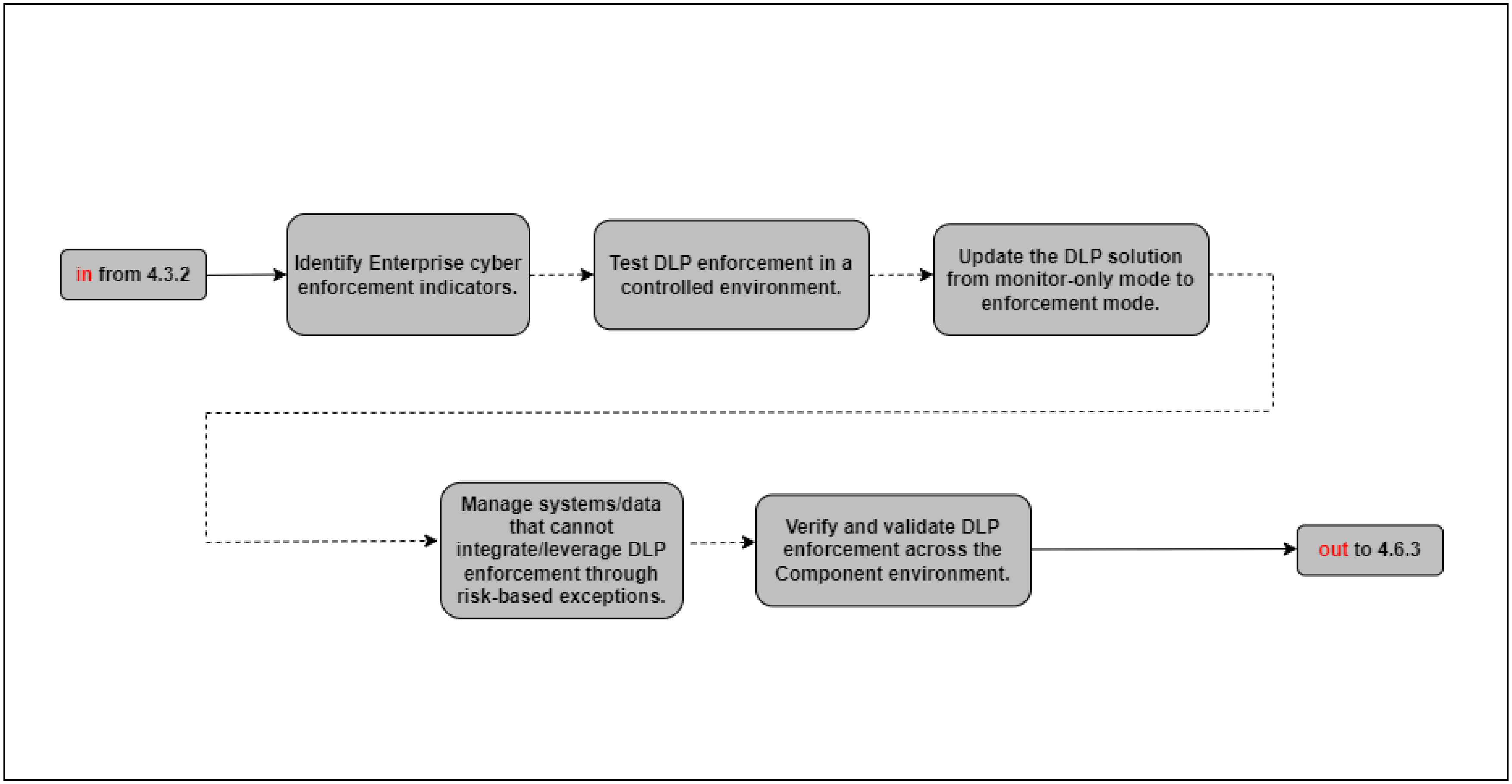

in from 4.3.2
Identify Enterprise cyber enforcement indicators.
Test DLP enforcement in a controlled environment.
Update the DLP solution from monitor-only mode to enforcement mode.
Manage systems/data that cannot integrate/leverage DLP enforcement through risk-based exceptions.
Verify and validate DLP enforcement across the Component environment.
out to 4.6.3

Figure D-25: Implementation Tasks for Activity 4.6.2 — Data Loss Prevention (DLP) Enforcement via Data Tags and Analytics Part 1

Activity 4.7.1 Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1

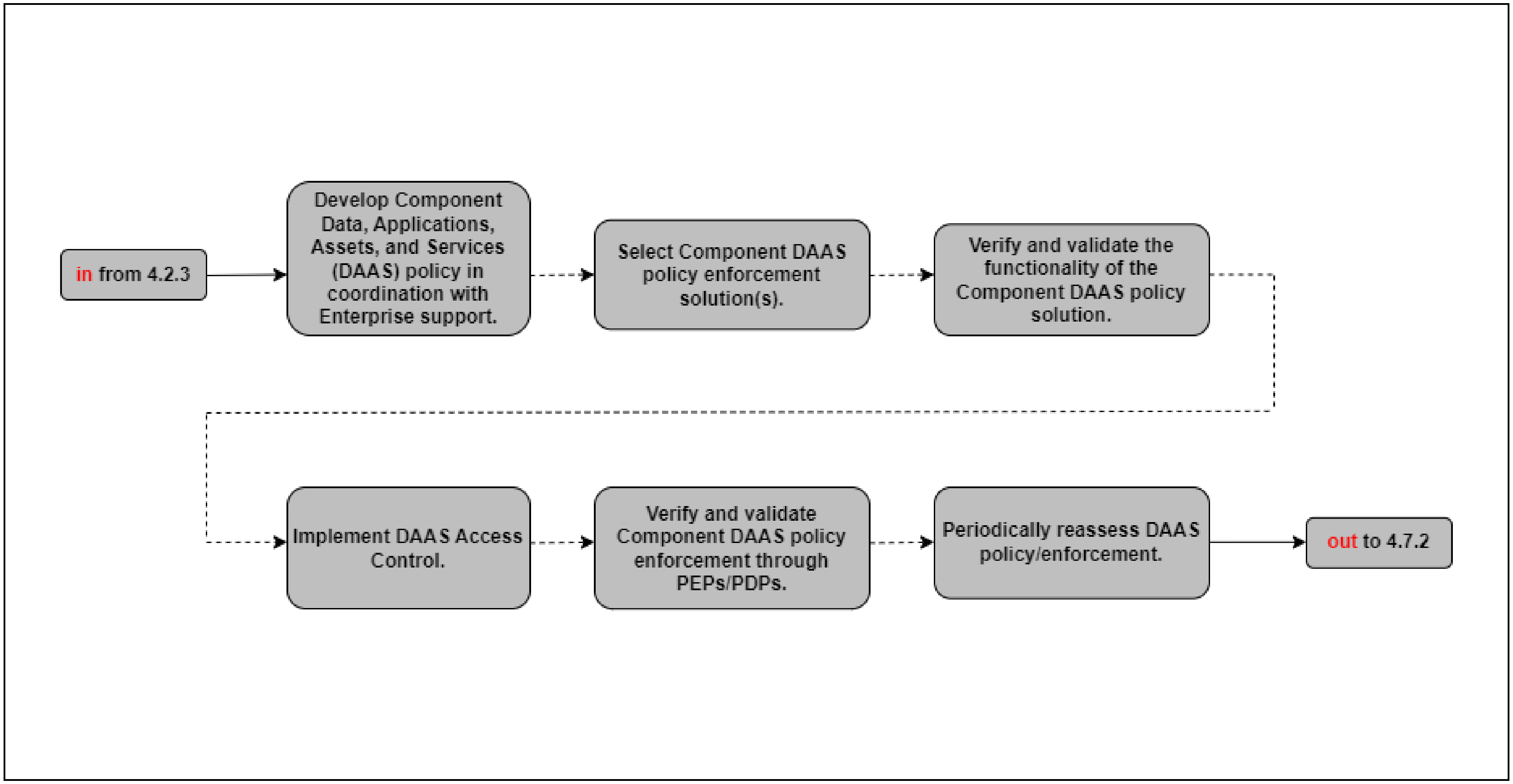

in from 4.2.3
Develop Component Data, Applications, Assets, and Services (DAAS) policy in coordination with Enterprise support.
Select Component DAAS policy enforcement solution(s).
Verify and validate the functionality of the Component DAAS policy solution.
Implement DAAS Access Control.
Verify and validate Component DAAS policy enforcement through PEPs/PDPs.
Periodically reassess DAAS policy/enforcement.
out to 4.7.2

Figure D-26: Implementation Tasks for Activity 4.7.1 — Integrate Data, Applications, Assets, and Services (DAAS) Access with Software-Defined Storage (SDS) Policy Part 1

Activity 4.7.4 Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1

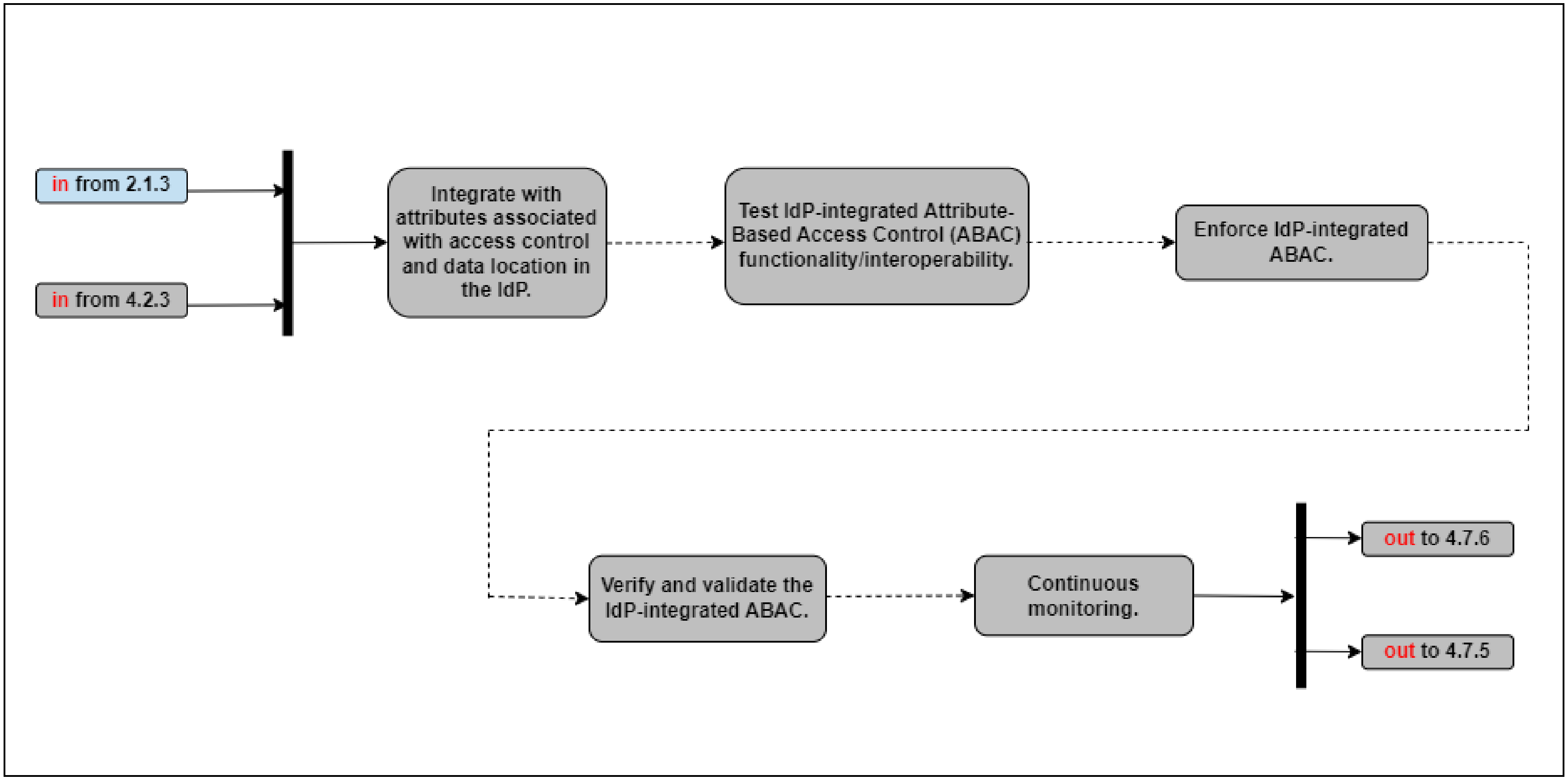

in from 2.1.3
in from 4.2.3
Integrate with attributes associated with access control and data location in the IdP.
Test IdP-integrated Attribute-Based Access Control (ABAC) functionality/interoperability.
Enforce IdP-integrated ABAC.
Verify and validate the IdP-integrated ABAC.
Continuous monitoring.
out to 4.7.6
out to 4.7.5

Figure D-27: Implementation Tasks for Activity 4.7.4 — Integrate Solution(s) and Policy with Enterprise Identity Provider (IdP) Part 1

Activity 5.2.3 Segment Flows into Control, Management, and Data Planes

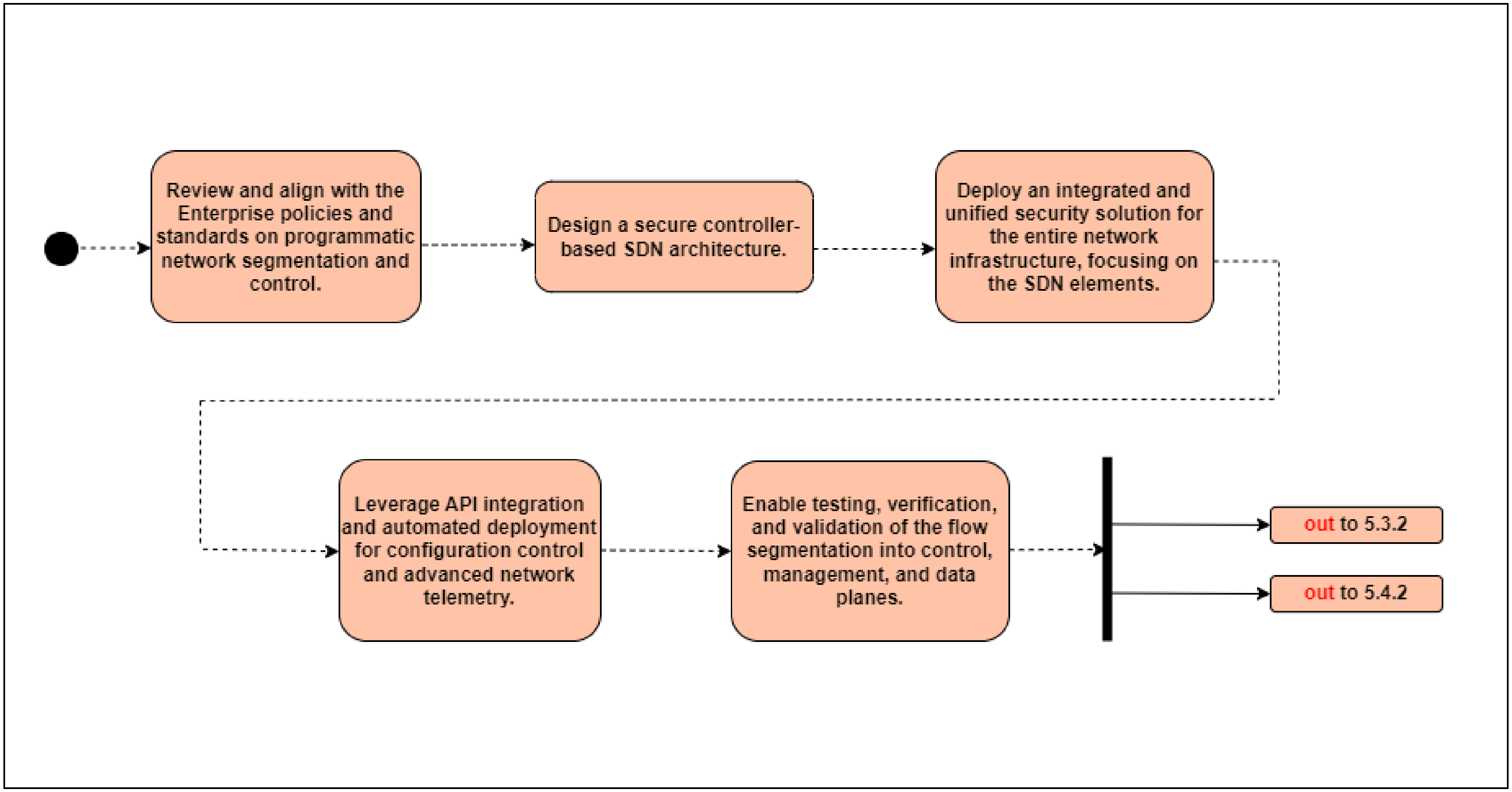

Review and align with the Enterprise policies and standards on programmatic network segmentation and control.
Design a secure controller-based SDN architecture.
Deploy an integrated and unified security solution for the entire network infrastructure, focusing on the SDN elements.
Leverage API integration and automated deployment for configuration control and advanced network telemetry.
Enable testing, verification, and validation of the flow segmentation into control, management, and data planes.
out to 5.3.2
out to 5.4.2

Figure D-28: Implementation Tasks for Activity 5.2.3 — Segment Flows into Control, Management, and Data Planes

Activity 5.3.2 Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation

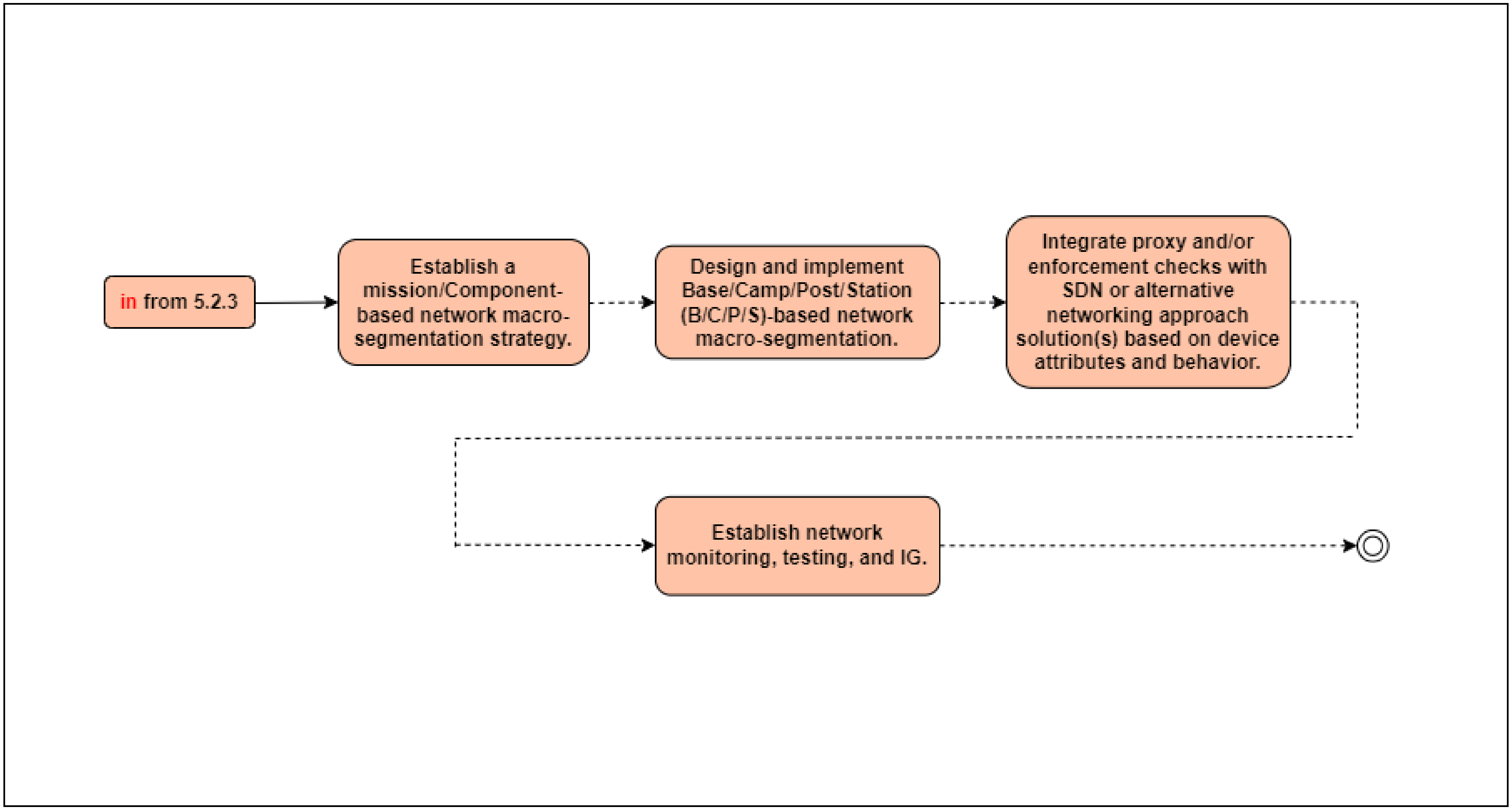

in from 5.2.3
Establish a mission/Component-based network macro-segmentation strategy.
Design and implement Base/Camp/Post/Station (B/C/P/S)-based network macro-segmentation.
Integrate proxy and/or enforcement checks with SDN or alternative networking approach solution(s) based on device attributes and behavior.
Establish network monitoring, testing, and IG.

Figure D-29: Implementation Tasks for Activity 5.3.2 — Base/Camp/Post/Station (B/C/P/S) Macro-Segmentation

Activity 5.4.2 Application and Device Micro-Segmentation

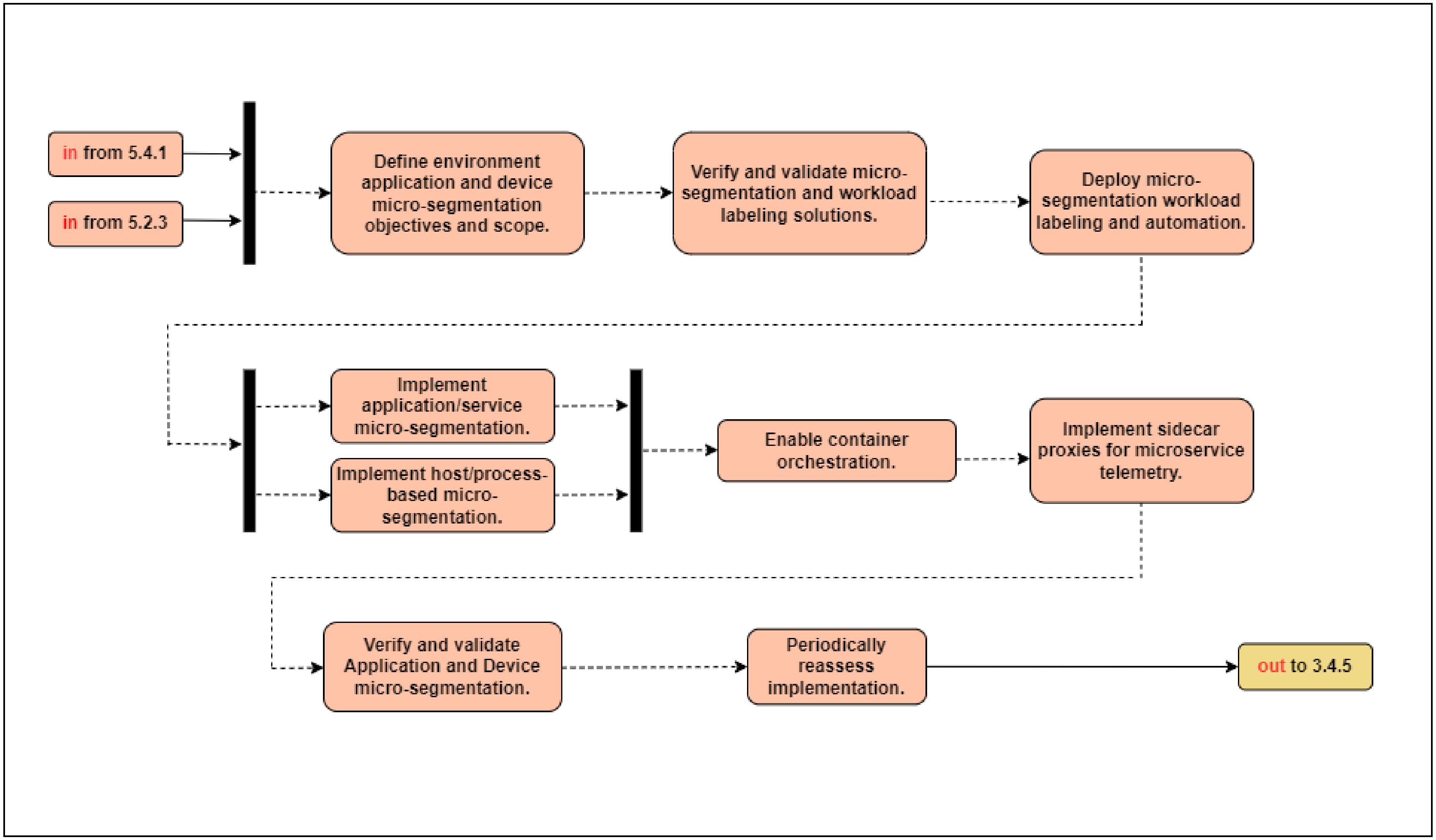

in from 5.4.1
in from 5.2.3
Define environment application and device micro-segmentation objectives and scope.
Verify and validate micro-segmentation and workload labeling solutions.
Deploy micro-segmentation workload labeling and automation.
Implement application/service micro-segmentation.
Implement host/process-based micro-segmentation.
Enable container orchestration.
Implement sidecar proxies for microservice telemetry.
Verify and validate Application and Device micro-segmentation.
Periodically reassess implementation.
out to 3.4.5

Figure D-30: Implementation Tasks for Activity 5.4.2 — Application and Device Micro-Segmentation

Activity 5.4.4 Protect Data in Transit

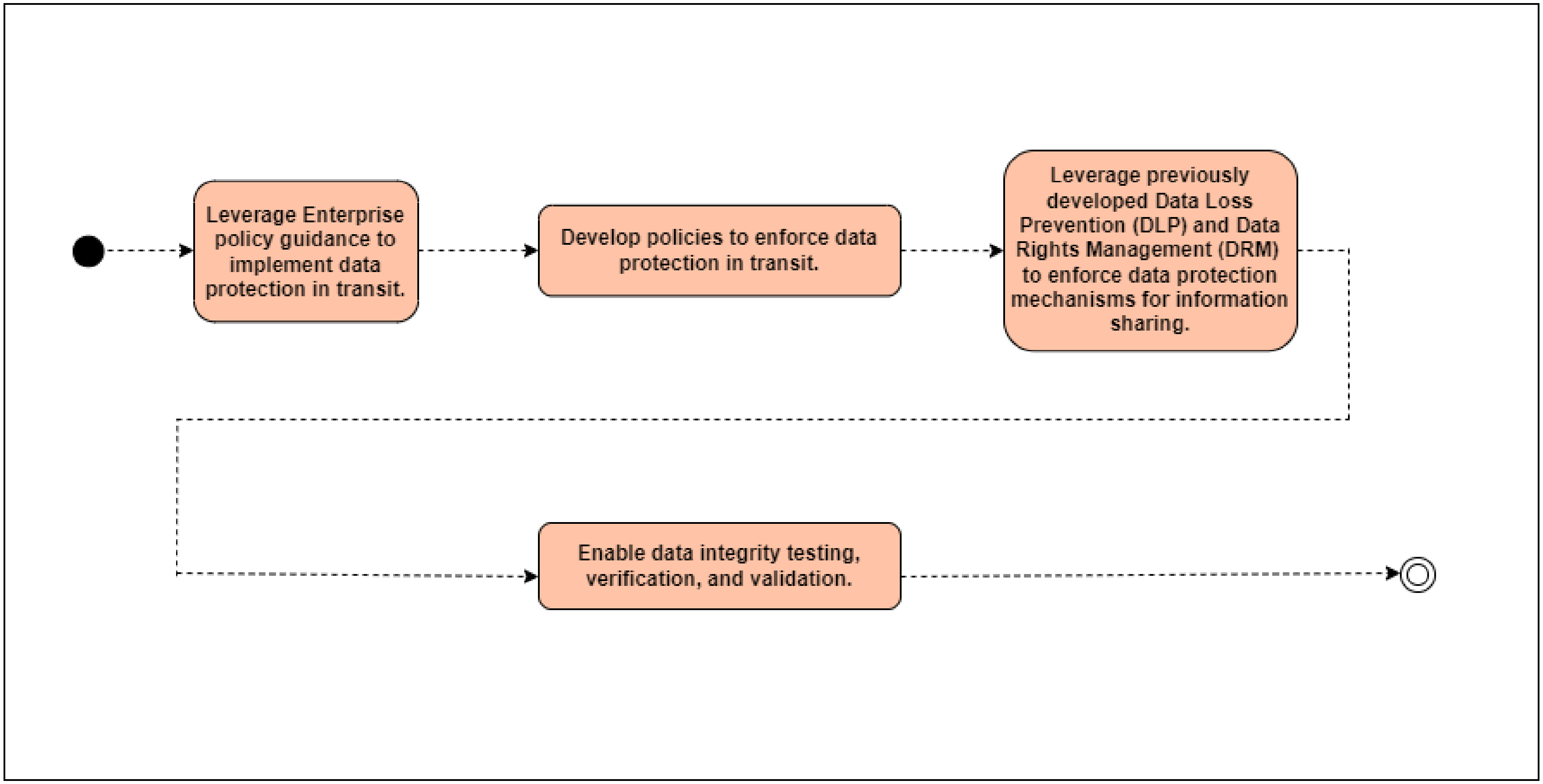

Leverage Enterprise policy guidance to implement data protection in transit.
Develop policies to enforce data protection in transit.
Leverage previously developed Data Loss Prevention (DLP) and Data Rights Management (DRM) to enforce data protection mechanisms for information sharing.
Enable data integrity testing, verification, and validation.

Figure D-31: Implementation Tasks for Activity 5.4.4 — Protect Data in Transit

Activity 6.1.3 Enterprise Security Profile Part 1

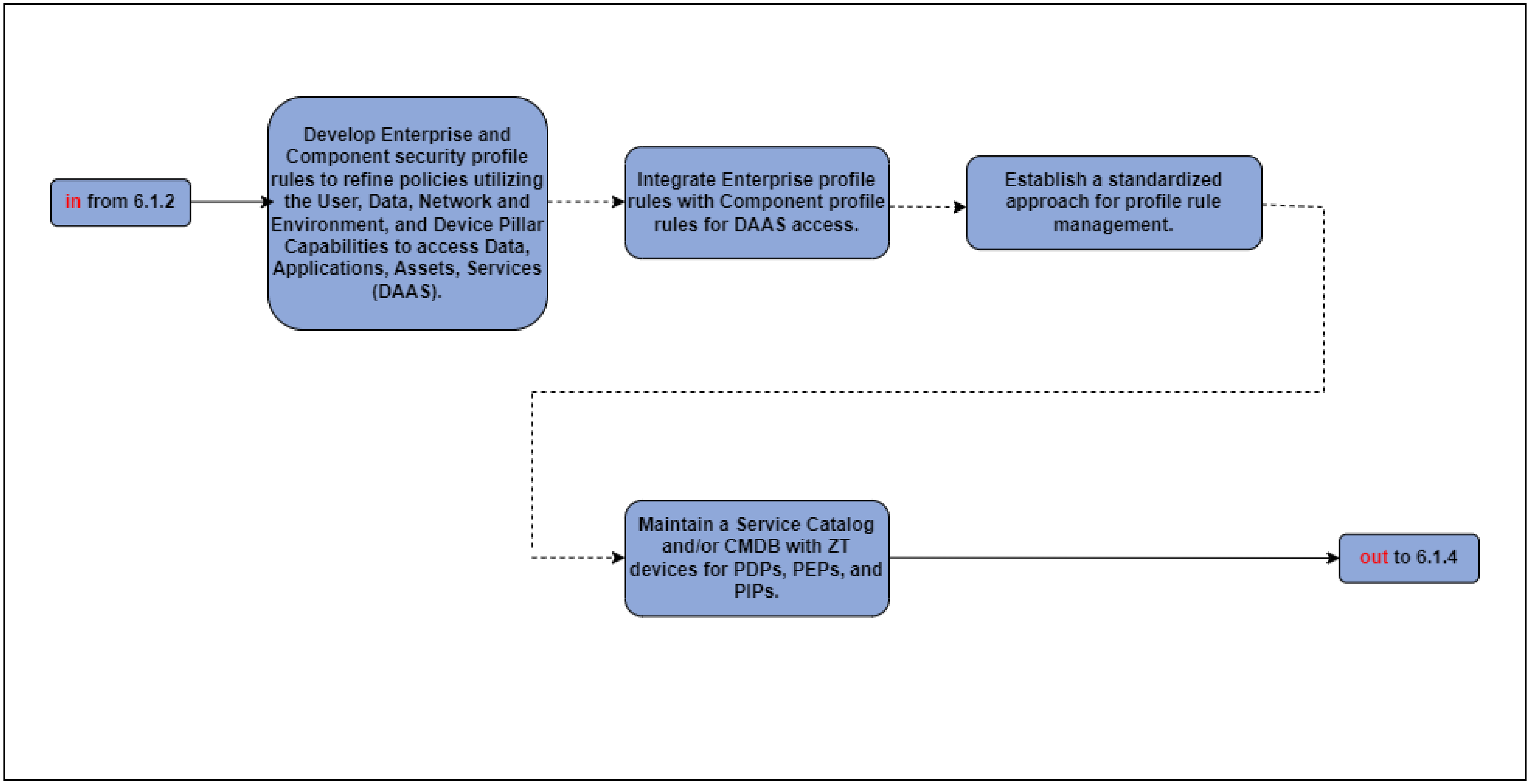

in from 6.1.2
Develop Enterprise and Component security profile rules to refine policies utilizing the User, Data, Network and Environment, and Device Pillar Capabilities to access Data, Applications, Assets, Services (DAAS).
Integrate Enterprise profile rules with Component profile rules for DAAS access.
Establish a standardized approach for profile rule management.
Maintain a Service Catalog and/or CMDB with ZT devices for PDPs, PEPs, and PIPs.
out to 6.1.4

Figure D-32: Implementation Tasks for Activity 6.1.3 — Enterprise Security Profile Part 1

Activity 6.2.2 Enterprise Integration and Workflow Provisioning Part 1

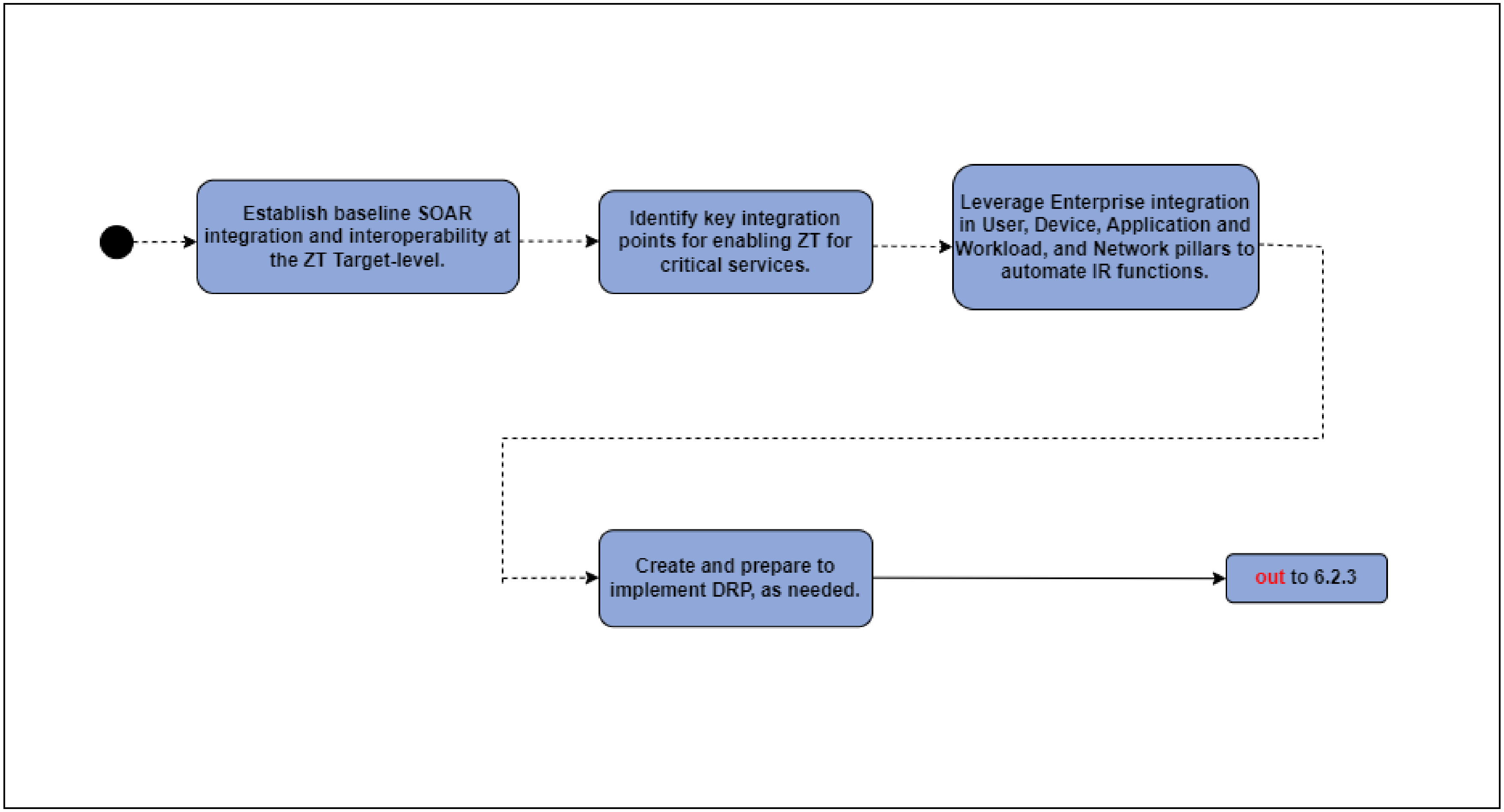

Establish baseline SOAR integration and interoperability at the ZT Target-level.
Identify key integration points for enabling ZT for critical services.
Leverage Enterprise integration in User, Device, Application and Workload, and Network pillars to automate IR functions.
Create and prepare to implement DRP, as needed.
out to 6.2.3

Figure D-33: Implementation Tasks for Activity 6.2.2 — Enterprise Integration and Workflow Provisioning Part 1

Activity 6.3.1 Implement Data Tagging and Classification Machine Learning (ML) Tools

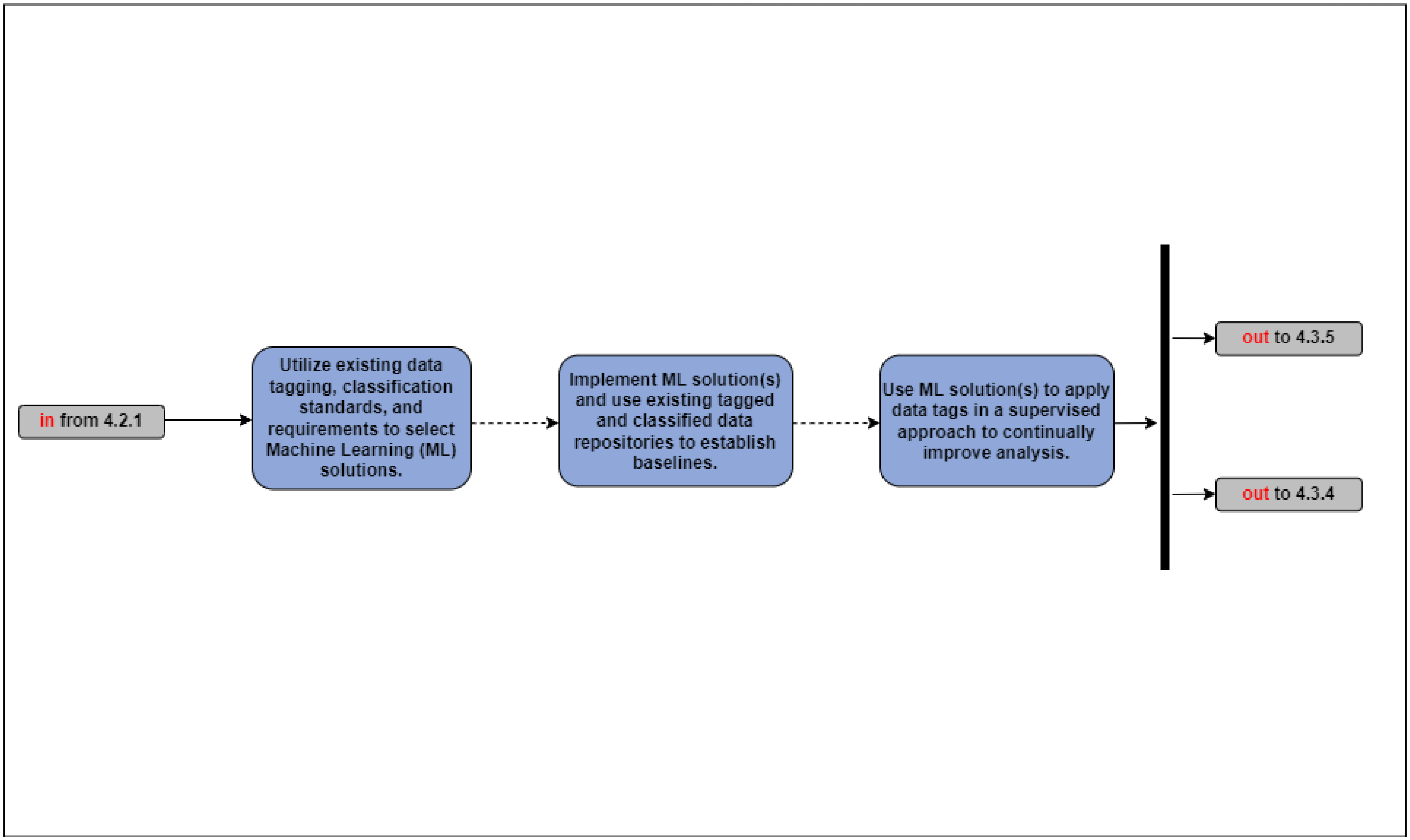

in from 4.2.1
Utilize existing data tagging, classification standards, and requirements to select Machine Learning (ML) solutions.
Implement ML solution(s) and use existing tagged and classified data repositories to establish baselines.
Use ML solution(s) to apply data tags in a supervised approach to continually improve analysis.
out to 4.3.5
out to 4.3.4

Figure D-34: Implementation Tasks for Activity 6.3.1 — Implement Data Tagging and Classification Machine Learning (ML) Tools

Activity 6.6.3 Standardized Application Programming Interface (API) Calls and Schemas Part 2

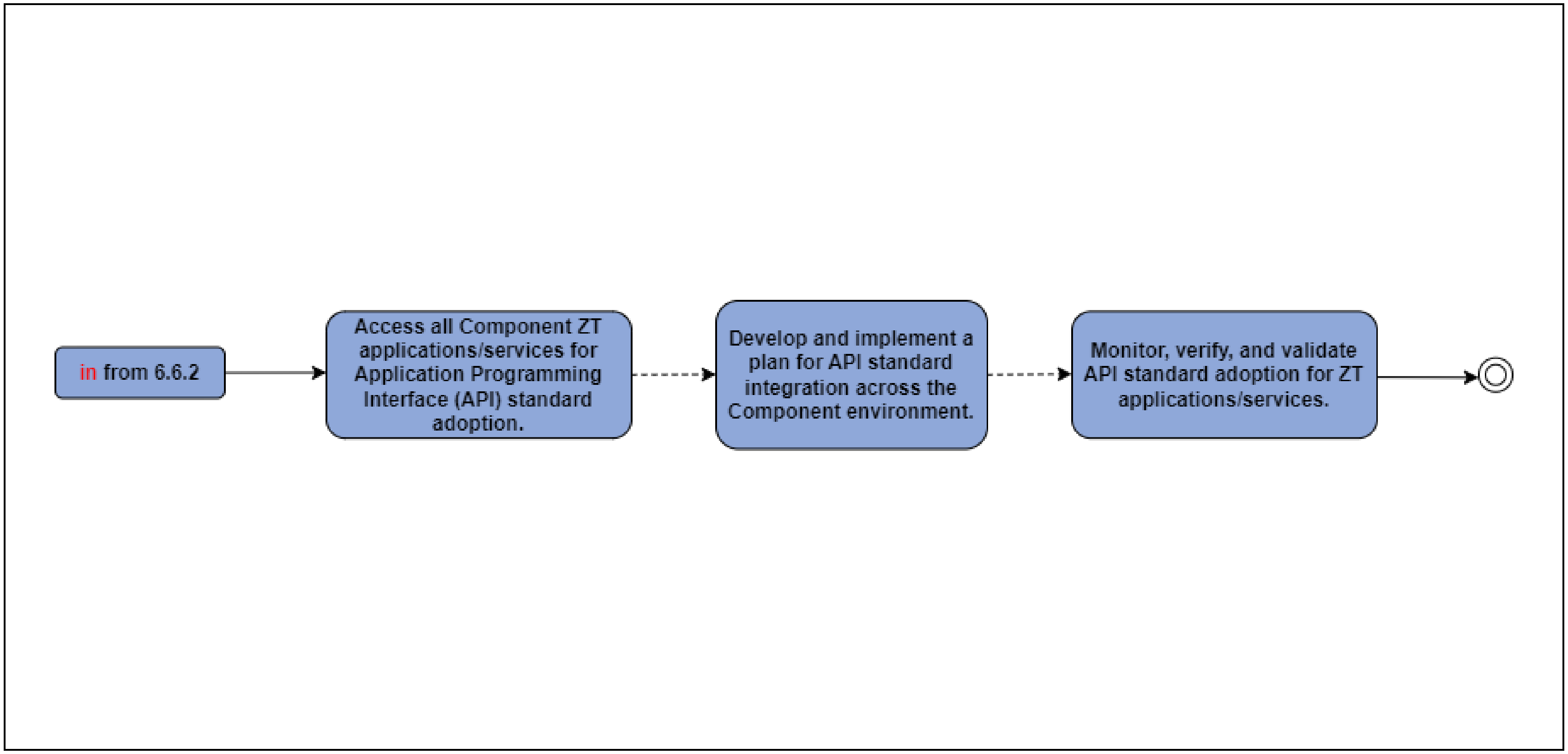

in from 6.6.2
Access all Component ZT applications/services for Application Programming Interface (API) standard adoption.
Develop and implement a plan for API standard integration across the Component environment.
Monitor, verify, and validate API standard adoption for ZT applications/services.

Figure D-35: Implementation Tasks for Activity 6.6.3 — Standardized Application Programming Interface (API) Calls and Schemas Part 2

Activity 6.7.2 Workflow Enrichment Part 2

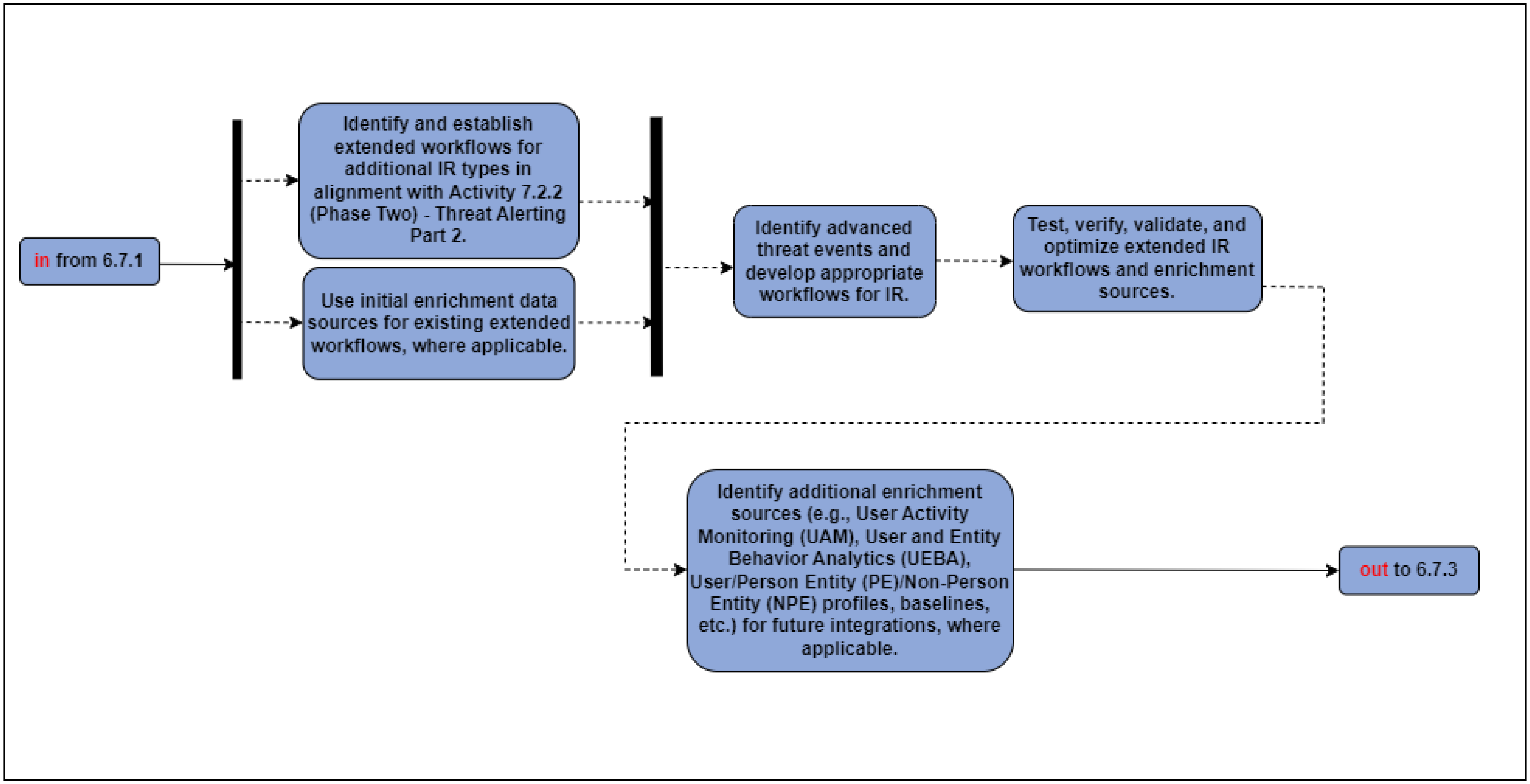

in from 6.7.1
Identify and establish extended workflows for additional IR types in alignment with Activity 7.2.2 (Phase Two) - Threat Alerting Part 2.
Use initial enrichment data sources for existing extended workflows, where applicable.
Identify advanced threat events and develop appropriate workflows for IR.
Test, verify, validate, and optimize extended IR workflows and enrichment sources.
Identify additional enrichment sources (e.g., User Activity Monitoring (UAM), User and Entity Behavior Analytics (UEBA), User/Person Entity (PE)/Non-Person Entity (NPE) profiles, baselines, etc.) for future integrations, where applicable.
out to 6.7.3

Figure D-36: Implementation Tasks for Activity 6.7.2 — Workflow Enrichment Part 2

Activity 7.1.3 Log Analysis

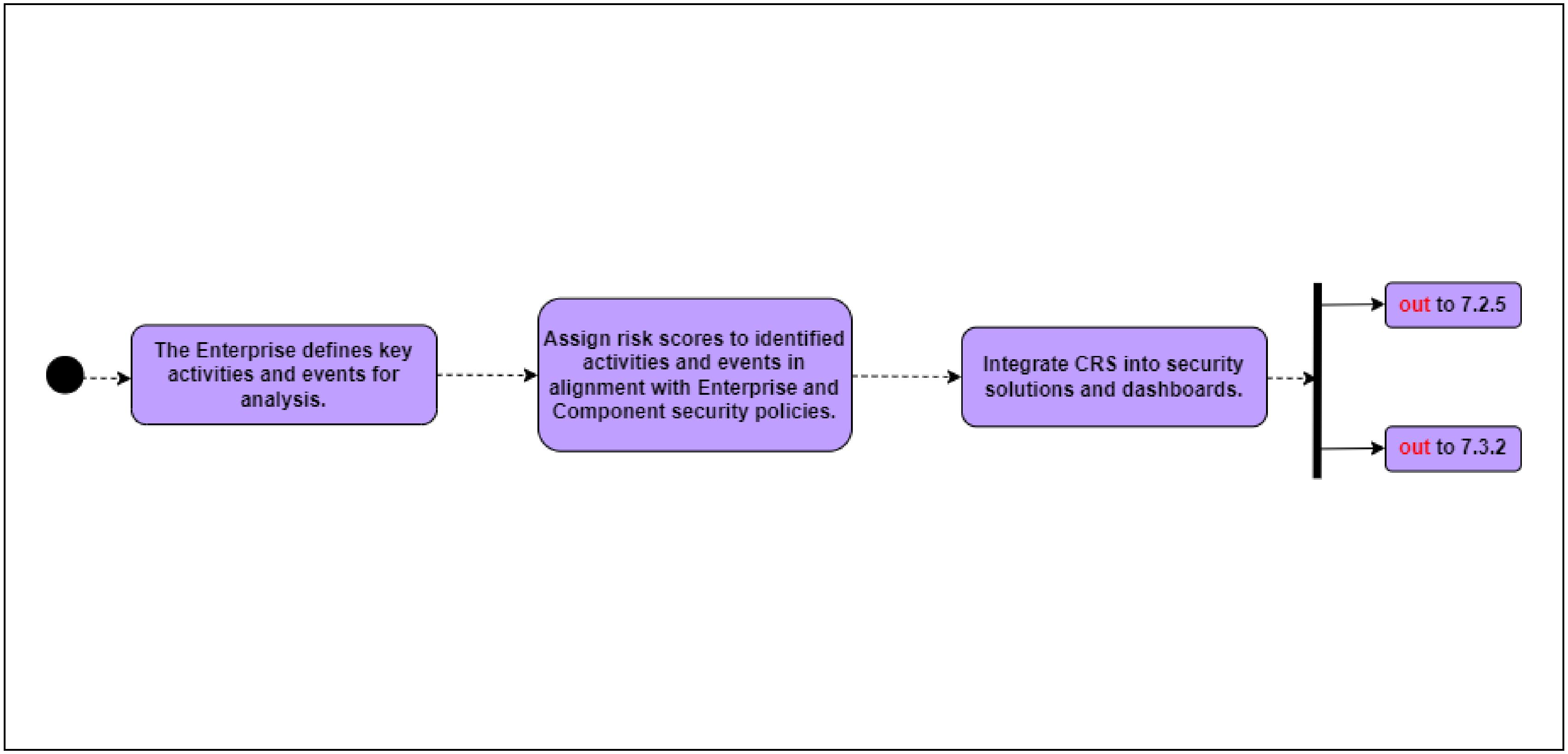

The Enterprise defines key activities and events for analysis.
Assign risk scores to identified activities and events in alignment with Enterprise and Component security policies.
Integrate CRS into security solutions and dashboards.
out to 7.2.5
out to 7.3.2

Figure D-37: Implementation Tasks for Activity 7.1.3 — Log Analysis

Activity 7.2.2 Threat Alerting Part 2

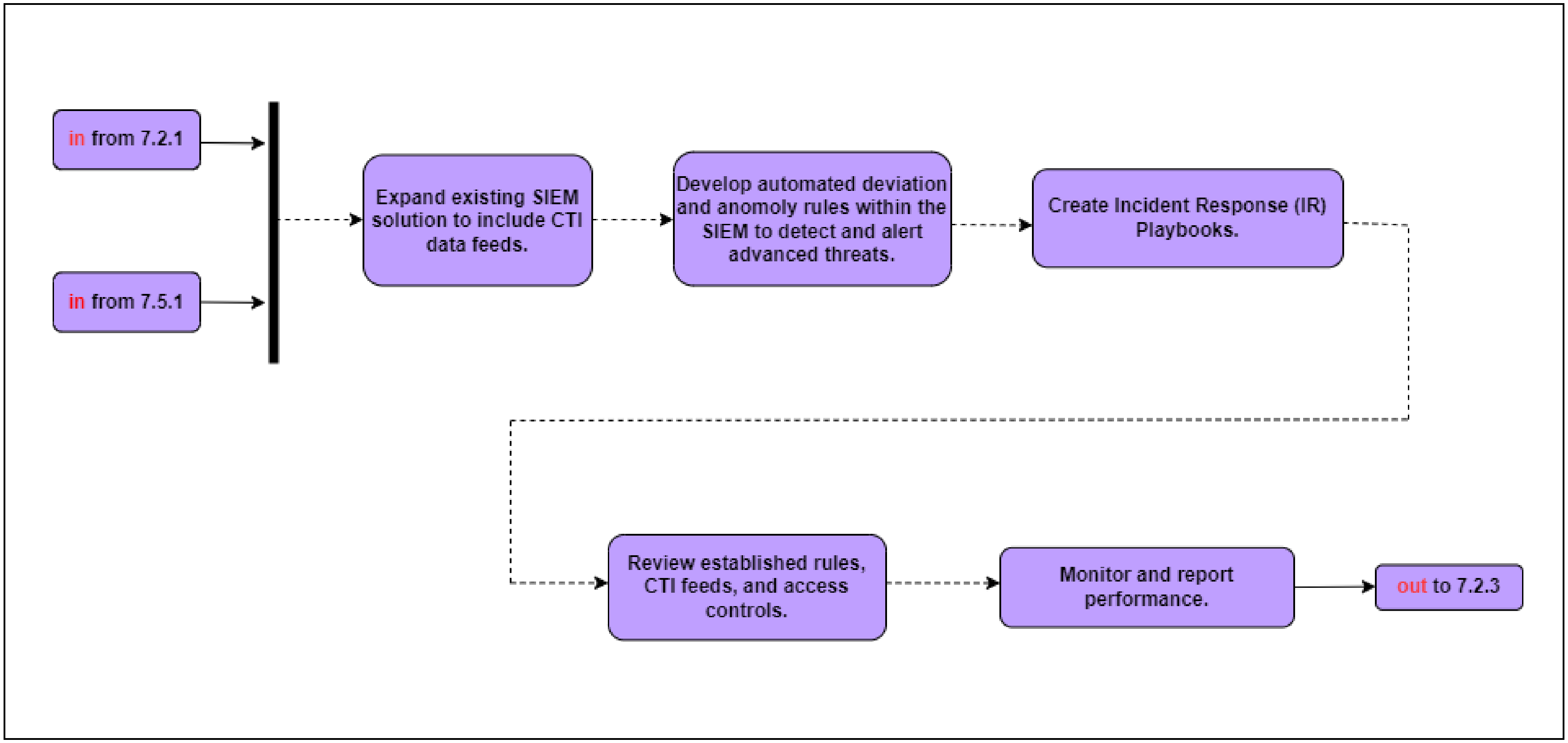

in from 7.2.1
in from 7.5.1
Expand existing SIEM solution to include CTI data feeds.
Develop automated deviation and anomoly rules within the SIEM to detect and alert advanced threats.
Create Incident Response (IR) Playbooks.
Review established rules, CTI feeds, and access controls.
Monitor and report performance.
out to 7.2.3

Figure D-38: Implementation Tasks for Activity 7.2.2 — Threat Alerting Part 2

Activity 7.2.5 User and Device Baselines

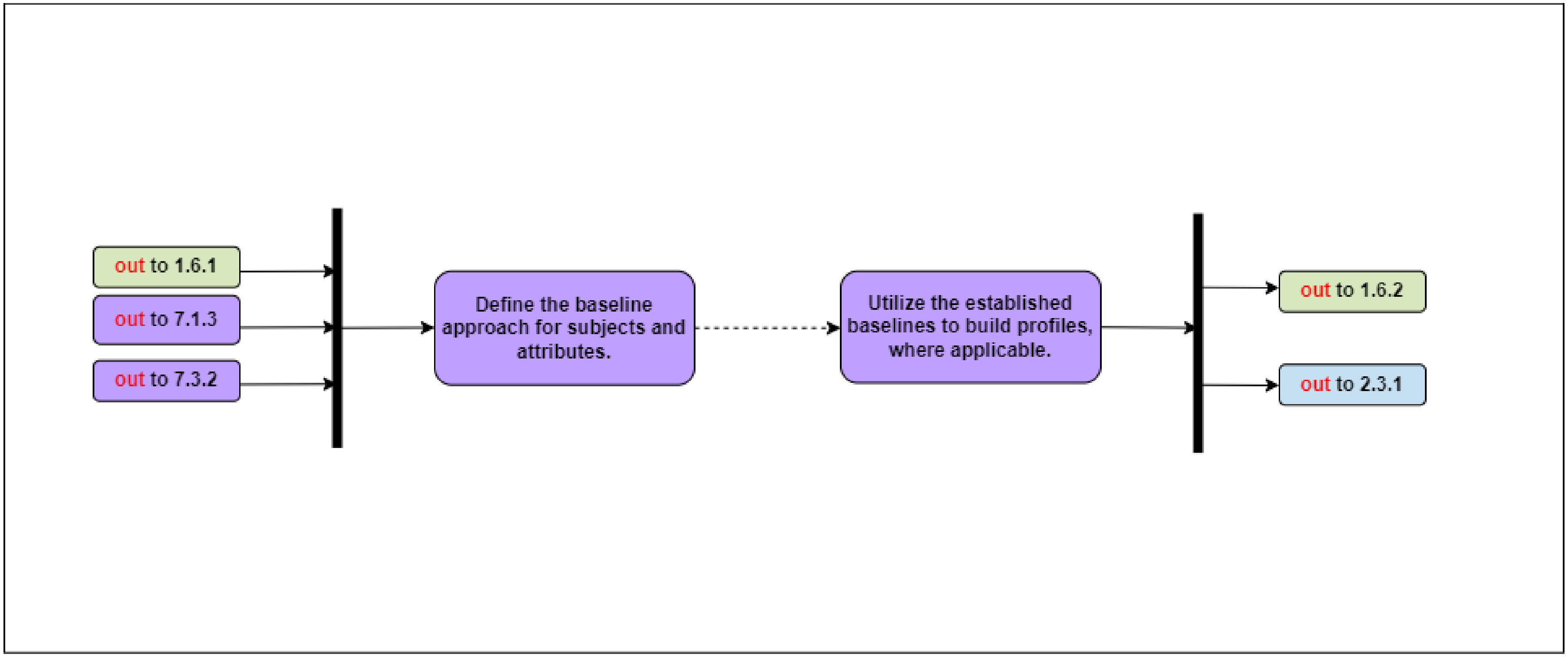

out to 1.6.1
out to 7.1.3
out to 7.3.2
Define the baseline approach for subjects and attributes.
Utilize the established baselines to build profiles, where applicable.
out to 1.6.2
out to 2.3.1

Figure D-39: Implementation Tasks for Activity 7.2.5 — User and Device Baselines

Activity 7.3.2 Establish User Baseline Behavior

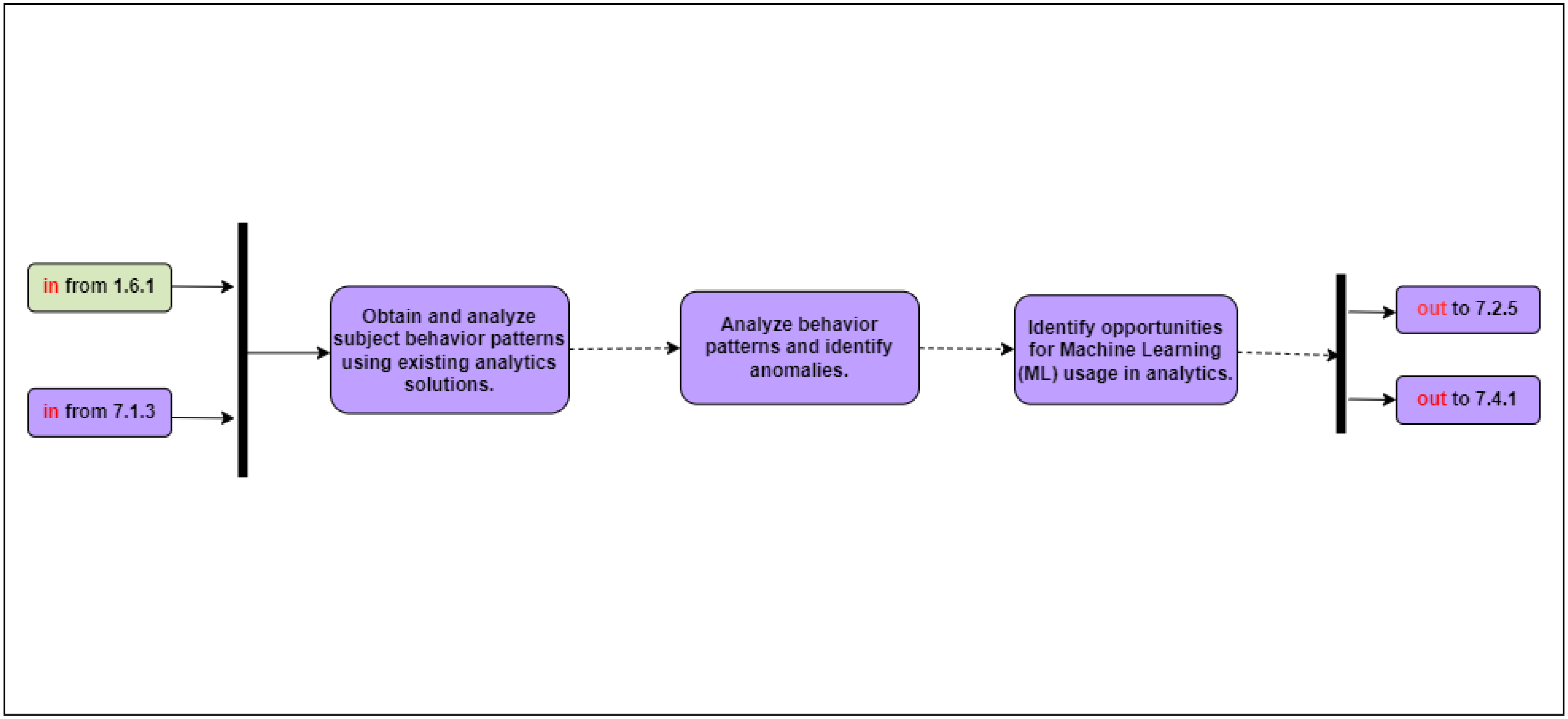

in from 1.6.1
in from 7.1.3
Obtain and analyze subject behavior patterns using existing analytics solutions.
Analyze behavior patterns and identify anomalies.
Identify opportunities for Machine Learning (ML) usage in analytics.
out to 7.2.5
out to 7.4.1

Figure D-40: Implementation Tasks for Activity 7.3.2 — Establish User Baseline Behavior

Activity 7.4.1 Baseline and Profiling Part 1

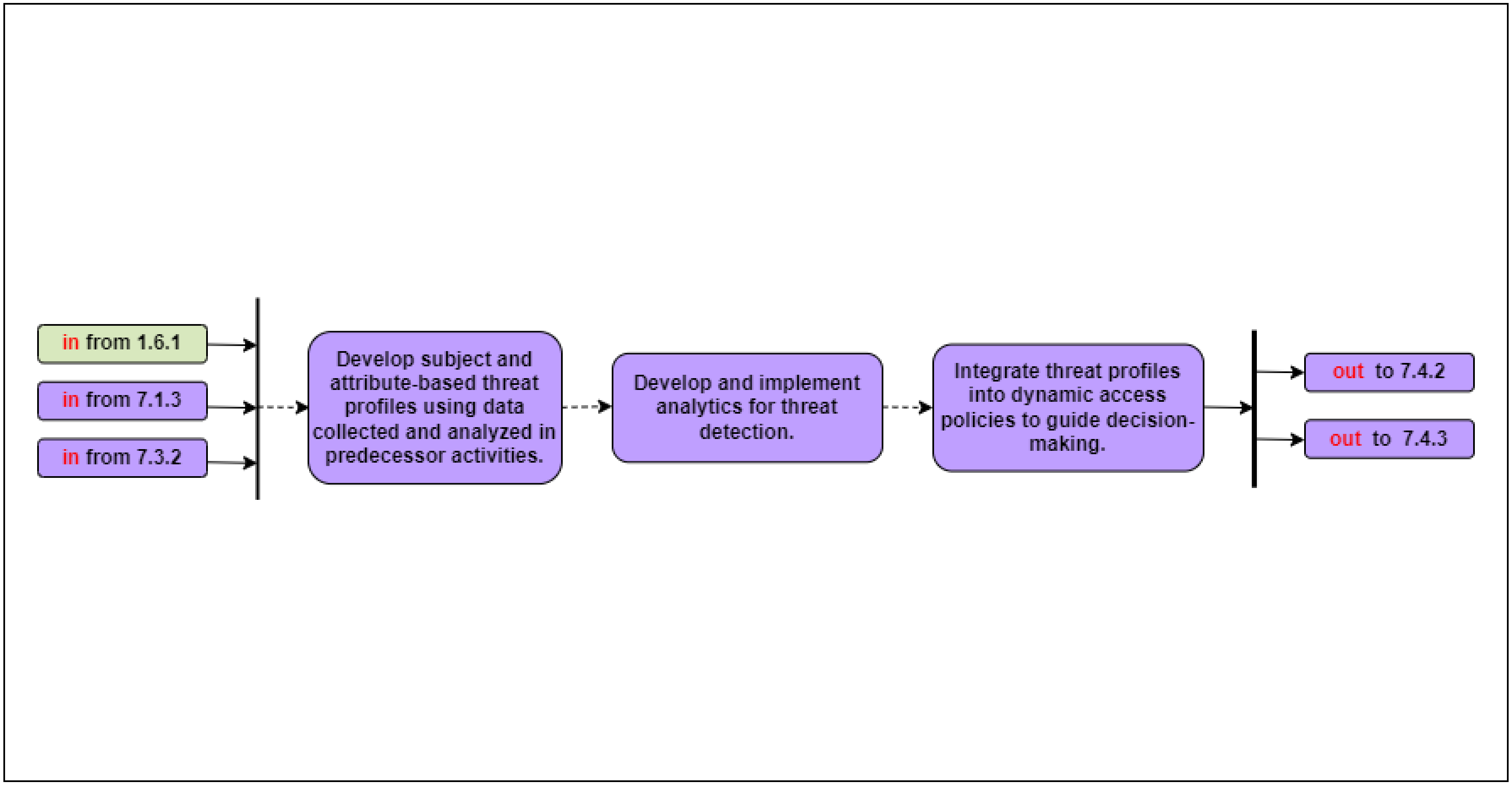

in from 1.6.1
in from 7.1.3
in from 7.3.2
Develop subject and attribute-based threat profiles using data collected and analyzed in predecessor activities.
Develop and implement analytics for threat detection.
Integrate threat profiles into dynamic access policies to guide decision-making.
out to 7.4.2
out to 7.4.3

Figure D-41: Implementation Tasks for Activity 7.4.1 — Baseline and Profiling Part 1

Activity 7.5.2 Cyber Threat Intelligence Program Part 2

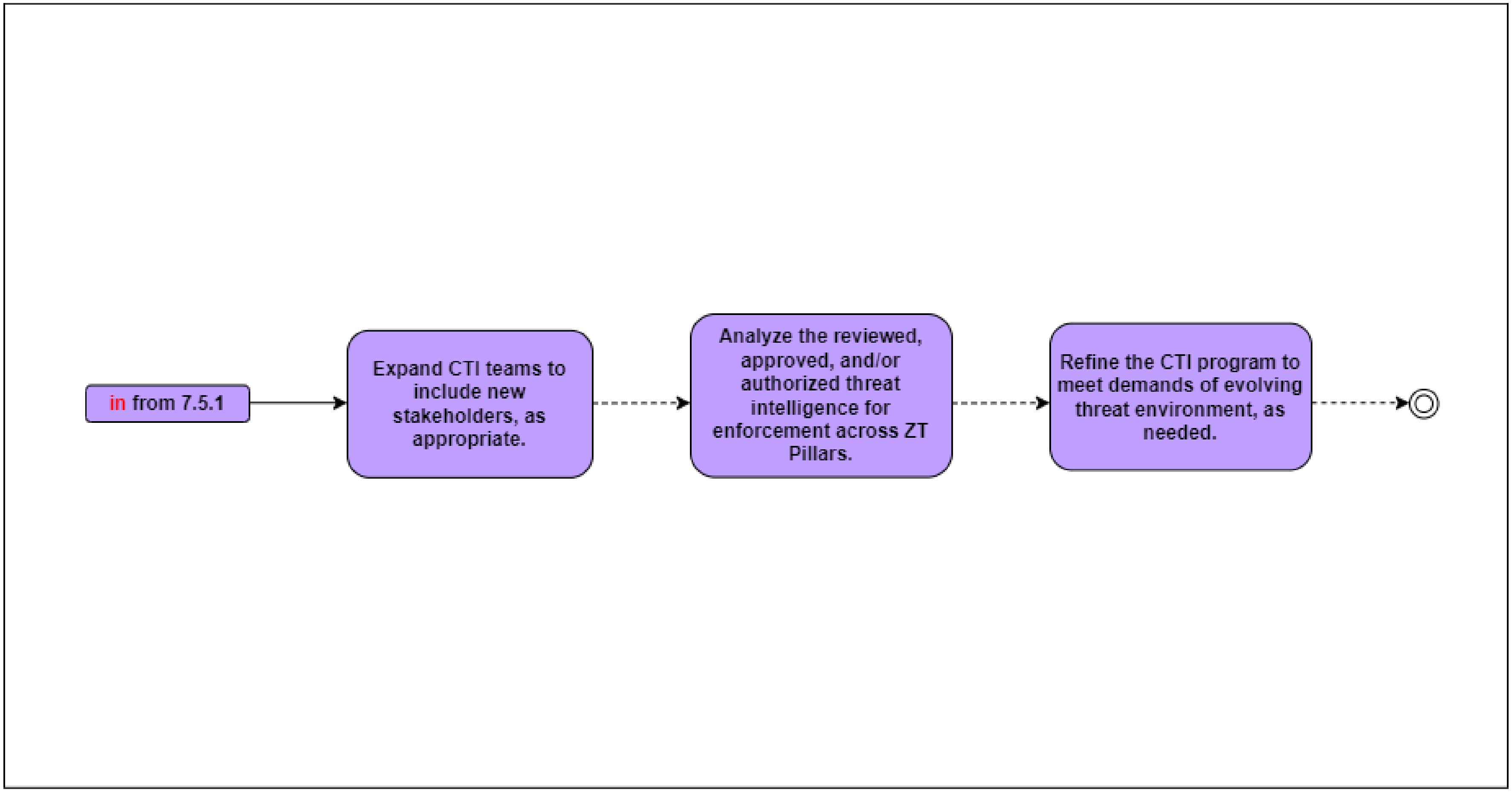

in from 7.5.1
Expand CTI teams to include new stakeholders, as appropriate.
Analyze the reviewed, approved, and/or authorized threat intelligence for enforcement across ZT Pillars.
Refine the CTI program to meet demands of evolving threat environment, as needed.

Figure D-42: Implementation Tasks for Activity 7.5.2 — Cyber Threat Intelligence Program Part 2