National Security Agency
Cybersecurity Technical Report

Zero Trust Implementation Guideline

Phase One

January 2026

U/OO/107297-26
PP-25-4750
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 One) covering the 36 Activities that support the 30 Capabilities in Phase One. Phase One Activities build upon or further refine the Component environment(s) to establish a secure foundation that supports ZT Capabilities. The remaining Target-level Activities and Capabilities are addressed in other ZIGs (Discovery and Phase Two), 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.

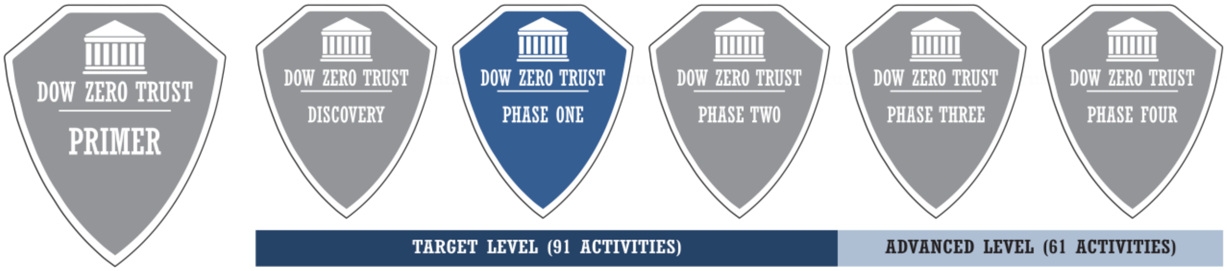


Figure 1: Zero Trust Implementation Guidelines (ZIGs)

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 Data, Assets, Applications, and Services (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 One 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 One Activities and Capabilities. The Phase One 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 purpose of the Activities within the Discovery Phase ZIG is to collect information about the Component's environment(s), such as DAAS, Users/PEs/NPEs, etc. In this Phase One ZIG, the Activities build upon or further refine the Component environment(s) to establish a secure foundation that supports ZT Capabilities. Finally, in the Phase Two ZIG, 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.

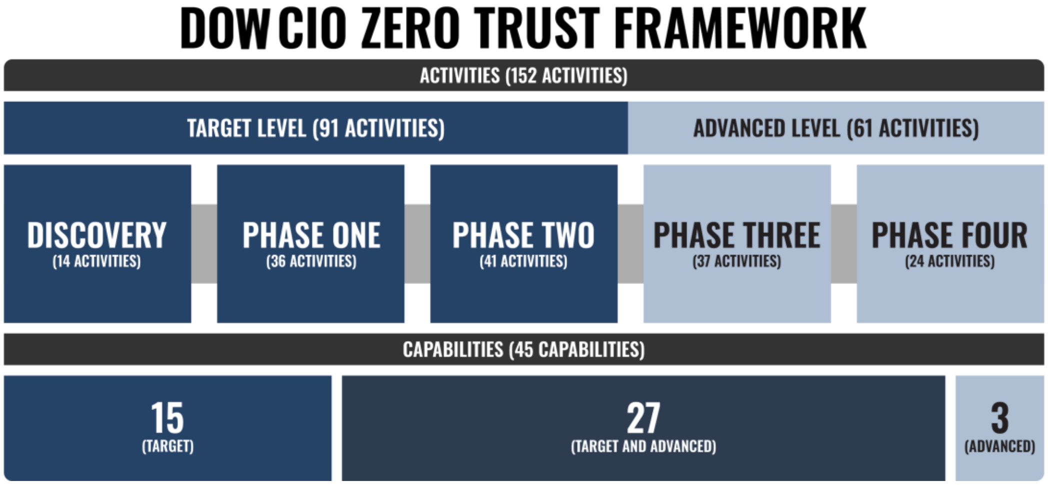

DOW CIO ZERO TRUST FRAMEWORK
ACTIVITIES (152 ACTIVITIES)
TARGET LEVEL (91 ACTIVITIES)
ADVANCED LEVEL (61 ACTIVITIES)
DISCOVERY (14 ACTIVITIES)
PHASE ONE (36 ACTIVITIES)
PHASE TWO (41 ACTIVITIES)
PHASE THREE (37 ACTIVITIES)
PHASE FOUR (24 ACTIVITIES)
CAPABILITIES (45 CAPABILITIES)
15 (TARGET)
27 (TARGET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

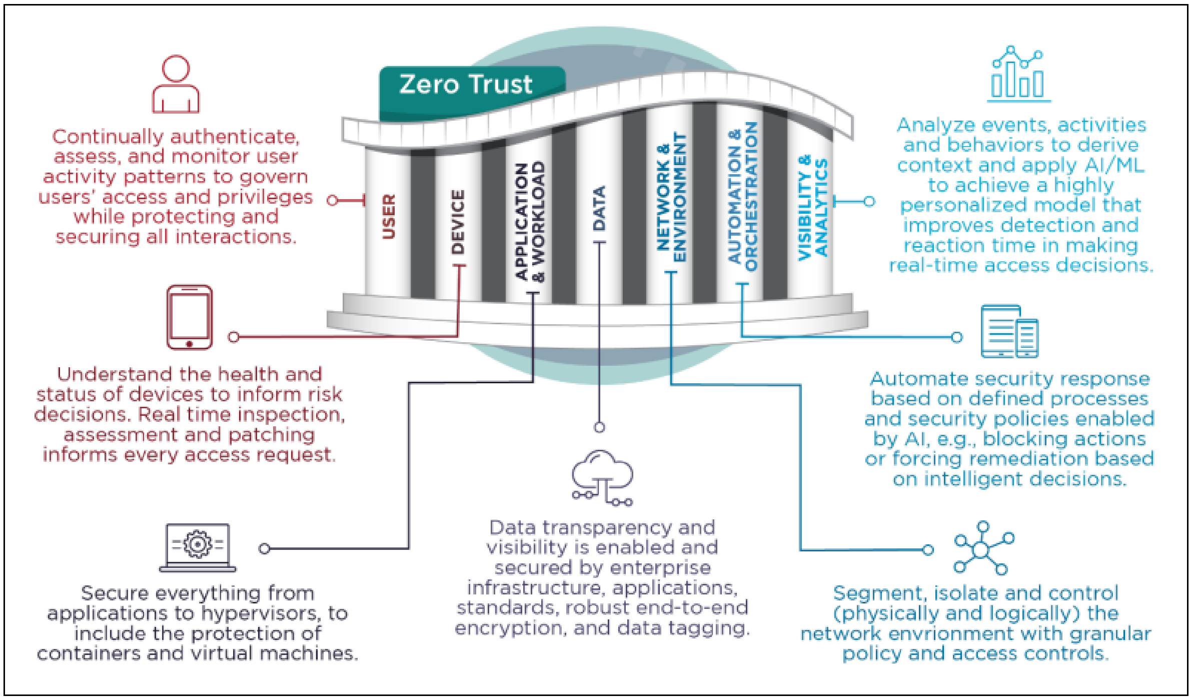
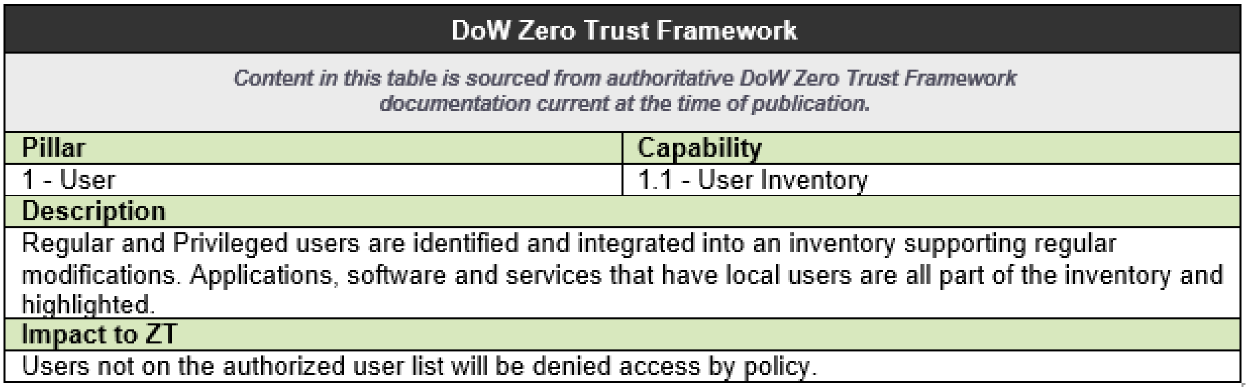

Zero Trust
USER
DEVICE
APPLICATION & WORKLOAD
DATA
NETWORK & ENVIRONMENT
AUTOMATION & ORCHESTRATION
VISIBILITY & ANALYTICS
Continually authenticate, assess, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.
Understand the health 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 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 One Capability associated with the DoW ZT Framework. The Capability section precedes the associated Activities and describes each ZT Capability as 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 [34]. 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].

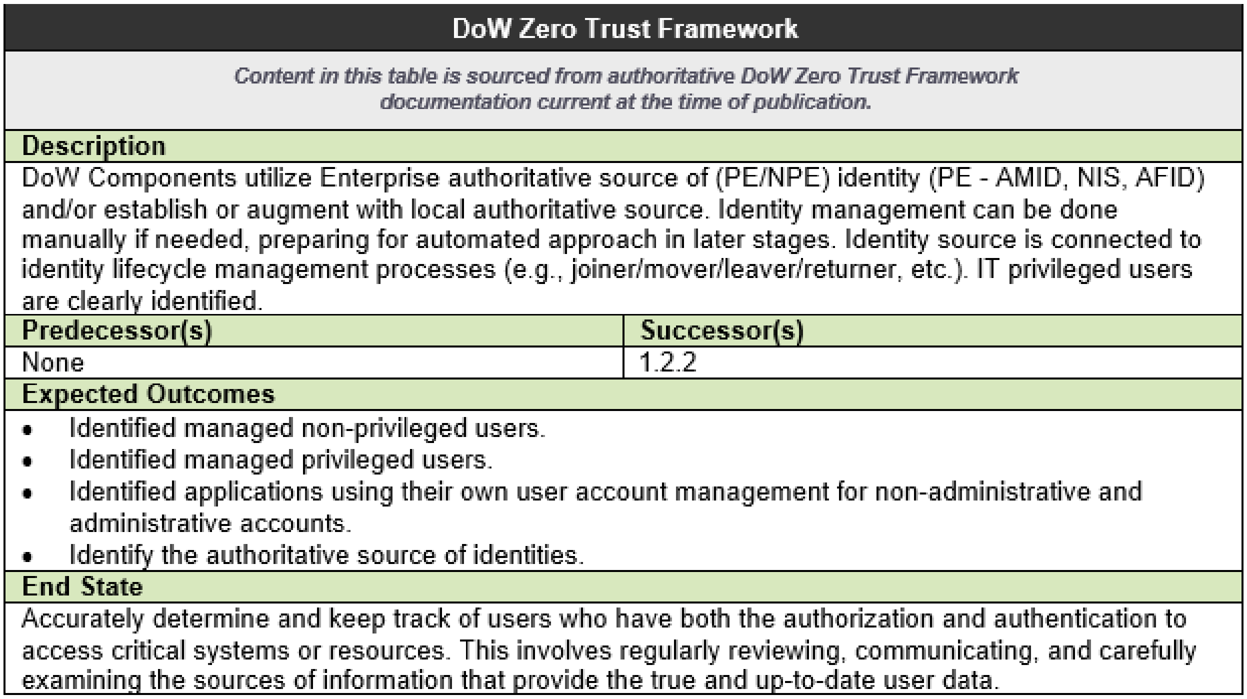
Activities

This section introduces the Activities associated with Phase One 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].



<table>
<tr><th colspan="2">DoW Zero Trust Framework</th></tr>
<tr><td colspan="2"><em>Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.</em></td></tr>
<tr><td colspan="2"><strong>Description</strong></td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td><strong>Predecessor(s)</strong></td><td><strong>Successor(s)</strong></td></tr>
<tr><td>None</td><td>1.2.2</td></tr>
<tr><td colspan="2"><strong>Expected Outcomes</strong></td></tr>
<tr><td colspan="2">• 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.</td></tr>
<tr><td colspan="2"><strong>End State</strong></td></tr>
<tr><td colspan="2">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.</td></tr>
</table>

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 subsection 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 One ZIG.
- Appendix B – Abbreviations and Acronyms
  - A compiled list of abbreviations and acronyms specific to the Phase One ZIG.
- Appendix C – References
  - A compiled list of references specific to the Phase One ZIG.
- Appendix D – Activity Task Diagrams
  - A compilation of activity task implementation diagrams specific to the Phase One 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 1.3 Multi-Factor Authentication (MFA)

Table 2: Capability 1.3 — Multi-Factor Authentication (MFA)

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	1.3 - Multi-Factor Authentication (MFA)
Description	
This capability initially focuses on developing a Component focused Multi-Factor Authentication (MFA) provider and Identity Provider (IdP) to enable the centralization of users. Retirement of local and/or built-in accounts and groups is a critical piece to this capability. At the later maturity levels alternative and flexible MFA tokens can be used to provide access for standard and external users.	
Impact to ZT	
Users not 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 deploys a centralized Multi-Factor Authentication (MFA) solution integrated with its Identity Provider (IdP), consolidating all User/Person Entity (PE) accounts and retiring local and built-in accounts.
- All Users/PEs, including external partners, are required to authenticate using at least two of three (2 of 3) attributes: knowledge (e.g., password), possession (e.g., token or Common Access Card (CAC)), or inherence (e.g., fingerprint or iris scan).
- A phased rollout begins with standard Users/PEs and then privileged Users/PEs, ensuring a seamless transition and educating Users/PEs on how to use the MFA solution.
- During a routine security audit, the Component identifies several active local accounts on legacy systems and prioritizes their migration to the centralized MFA solution.
- A cyber threat actor attempts to gain unapproved access to the Component’s resources using compromised credentials obtained from a phishing attack.

- The MFA solution detects the login attempt and prompts for the second authentication factor, which the threat actor does not possess, automatically denying access.
- Security analysts investigate the failed login attempt and flag the compromised account for remediation, preventing further exploitation.
- To improve accessibility, the Component implements alternative MFA methods, such as biometric authentication for external Users/PEs without tokens, while maintaining stringent security standards.
- Regular security reviews and User/PE feedback enable the Component to refine its MFA policies, ensuring flexible options are available for both internal and external Users/PEs while maintaining compliance with Enterprise requirements.
- By requiring multiple forms of authentication, the Component achieves robust access control, reducing the risk of unapproved access to its Data, Applications, Assets, and Services (DAAS) system and aligning fully 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:

- Stronger Security: MFA adds an extra layer of protection, making it significantly harder for unapproved Users/PEs to access systems and sensitive data.
- Regulatory Compliance: Implementing MFA helps ensure compliance with industry standards and regulations, reducing legal and financial risks.
- Reduced Credential Theft: MFA minimizes the risk of phishing attacks and password-related breaches by requiring multiple verification factors.
- Improved Trust and Accountability: Employees and customers gain confidence knowing their accounts and information are better protected.
- Lower Risk of Business Disruptions: Preventing unapproved access reduces the likelihood of costly security incidents that could disrupt operations.

Technology

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

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

Activity 1.3.1 Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)

Table 3: Activity 1.3.1 — Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)

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 or Identity Provider (IdP) solution using approved credential or approved alternative Multi-Factor Authentication (MFA). The IdP and MFA solution may be combined in a single application or separated as needed, assuming automated integration is supported by both solutions. Both IdP and MFA support integration with the Enterprise PKI capability as well as enabling key pairs to be signed by the trusted root certificate authorities. Authentication for mission/task-critical applications and services is MFA-Enabled and leverages the related authentication mechanisms to manage users and groups.	
Predecessor(s)	**Successor(s)**
None	None
Expected Outcomes	
• Component is using IdP with MFA for critical applications/services. • Components have implemented an Identity Provider (IdP) that enables DoW PKI Multi-Factor Authentication (e.g., CAC, DPIV, DoW Issued PIV-I, FIPS 201 Compliant softcerts, etc.). • DoW Enterprise is the approved organizational PKI for critical services (ECA, FPKI, Category I/II/III PKI, etc.). • Utilize approved Alternative Hardware Tokens as needed - USB Security Key and/or OTP device (e.g., YubiKey FIPS for smartcard, FIDO2, FIDO U2F, OTP, RSA SecurID for OTP, etc.). • For access to low-risk resources (e.g., PII, publicly released information), utilize alternative two-step, two-factor authentication using software authenticators (e.g., Mobile Connect, Yubico, Okta Verify, etc.).	
End State	
Critical applications are identified and use MFA in alignment with a federated IdP solution.	

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 1.1.1 (Discovery) – *Inventory User* prior to this activity, to obtain User/Person Entity (PE) inventory list.
- Consider completing Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM)* prior to this activity, to assist in the deployment of an Identity Provider (IdP) and Multi-Factor Authentication (MFA) solution.

- Consider the requirements of Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1*, as all Component MFA/IdP actions will need to integrate with Enterprise solutions in this future activity.
    - If an Enterprise IdP/MFA solution already exists, then collaborate with the Enterprise to align the Component's actions.
- Consider completing Activity 3.1.1 (Discovery) – *Application and Code Identification* prior to this activity, as a comprehensive list of applications/services is necessary to ensure Least Privilege is applied consistently and completely.
- The MFA and IdP solution may be combined into a single solution or separated as needed. This provides a stronger security solution to protect Users/PEs, devices, networks, assets, etc.
- MFA provides security on at least two (2) of three (3) distinct levels of authentication to protect unapproved access to a restricted resource. The three (3) methods for MFA protection include:
    1. Something you have: a trusted device, a hardware key, a security fob, or an identification card for entry access.
    2. Something you are: the personal attributes of a human person, including fingerprints, iris or retina scans, hand geometry, voice recognition, or face recognition.
    3. Something you know: a security token, one-time password, an access code, a personal identification code, or a rotational password code.
- Identity as a Service (IDaaS) provides centralized identity management with MFA. Centralized identity management is an instance of Identity and Access Management (IAM) occurring in one (1) location (e.g., Single Sign-On (SSO), etc.), where SSO makes it easier for Users/PEs to adhere to IAM requirements.

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 1.3.1 — Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)

Identify all critical applications requiring MFA and IdP integration.
Identify all critical applications: ☐ Leverage the application inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification,* to identify the critical applications. **Review MFA requirements:** ☐ Refer to the approved Enterprise guidelines to define and review the MFA system and application requirements. **Leverage the Master User Inventory, from Activity 1.1.1 (Discovery) – *Inventory User* for component identities:** ☐ Leverage the previously developed User/PE inventory database to help establish User/PE identities at the Component level.
Develop and plan in support of a Component MFA and IdP deployment.
Establish communication with all key stakeholders: ☐ Prioritize applications, systems, and Users/PEs based on Enterprise/Component determined risk. ☐ Define the goals and scope of MFA and IdP implementation. **Identify Component IdP requirements:** ☐ Leverage the Component Identity Lifecycle Management (ILM) process, from Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM),* to assess and validate IdP key requirements. The Component ILM process will then be used to apply and enforce these established requirements. ☐ Review the Enterprise-approved guidelines on identity management and requirements applicable to the Component (e.g., authoritative data source, attributes, vetting, etc.). ☐ Consider industry standards/best business practices such as the National Institute of Standards and Technology (NIST) - Federal Information Processing Standards (FIPS) 140-3, standards for cryptographic modules. ☐ Determine how the Component will prioritize MFA and IdP deployment and integration within the existing environment(s). **Select a compatible IdP and MFA solution:** ☐ Identify compatible IdP and MFA solution(s) that meet the Component ILM requirements, from Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM)*. ☐ Identify how the infrastructure and security products will integrate with the IdP. Also, identify if those products support the Attribute-Based Access Control (ABAC)/Role-Based Access Control (RBAC)/Identity-Based Access Control (IBAC) decisions made to support Policy Decision Point (PDP)/Policy Enforcement Point (PEP), from Activity 3.4.2 (Phase Two) – *Resource Authorization Part 2* and 6.1.2 (Phase One) – *Organization Access Profile*. Do not expect uniformity for all products.

- When selecting an MFA solution:
    - In the absence of Enterprise-defined MFA solutions, consider the following:
        - Hardware Tokens: Universal Serial Bus (USB) Security Keys and/or One-Time Password (OTP) devices, as needed.
        - Software authenticators that provide two-step/two-factor authentication.
- When selecting an IdP solution:
    - Determine if it will support more advanced access control capabilities (e.g., ABAC, IBAC, etc.).
    - Plan for enough granularity for access to the IdP to allow for granting/removing a single privilege without granting/removing extra privileges.
    - Determine if on-premises or cloud-based IdP solutions are most suitable.

Verify and validate Component IdP and MFA solution capabilities:

☐ Test the selected IdP and MFA solutions to ensure they:

- Integrate with the Component environment.
- Provide the necessary capabilities identified during selection.

Deploy Component MFA and IdP solutions.

Deploy and implement the selected MFA and IdP solutions:

☐ Provide clear policy guidelines and support for User/PE enrollment in MFA.

☐ Implement a phased approach deployment, leveraging the Component-defined priorities, to migrate Users/PEs and integrate MFA and IdP with existing Data, Applications, Assets, and Services (DAAS).

Verify and validate MFA and IdP deployment/integration.

Verify and validate Component MFA solution:

☐ Ensure all Users/PEs are required to leverage the Component selected MFA solution.

☐ Ensure access to Component-determined DAAS is restricted to Users/PEs who leverage the approved MFA solution.

Verify and validate Component IdP solution:

☐ Ensure that all Users/PEs are integrated with the Component IdP solution in accordance with the Component ILM policy established in Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM).*

Verify and validate logging:

☐ Ensure the MFA and IdP can externally send all relevant logs to the Security Information and Event Management (SIEM) or find third-party software to export appropriate logs that can run on the platform.

☐ Verify and validate the MFA and IdP can provide detailed logs for the SIEM/Security Orchestration, Automation, and Response (SOAR), and/or Artificial Intelligence/Machine Learning (AI/ML) to utilize.

- Log standardization, from Activity 7.1.2 (Phase One) – *Log Parsing.*
- SIEM log detail requirements, from Activity 7.2.4 (Phase One) – *Asset ID and Alert Correlation.*
- AI/ML integration, from Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior.*

Summary

This diagram outlines the Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of Multi-Factor Authentication (MFA) to verify and validate User/Person Entity (PE) identities. It presents strategic insights that drive implementation and expected outcomes, including the successful incorporation of MFA strategies.

Table 5: Activity 1.3.1 — Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP) - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How is the Identity Provider (IdP) with MFA used for critical applications/services?
2. How has the IdP enabled DoW Public Key Infrastructure (PKI) MFA?
3. How is the organizational standardized PKI used for critical services?

STRATEGIC INSIGHTS

- The Component defines a structured approach for identifying critical applications that require MFA and IdP integration, leveraging existing inventories and risk assessments to prioritize deployments.
- The Component demonstrates security and compliance by establishing clear IdP requirements, selecting compatible MFA/IdP solutions, and ensuring seamless integration with existing infrastructure while supporting Attribute-Based Access Control (ABAC) and Identity-Based Access Control (IBAC).
- The Component provides verifiable enforcement through testing, phased deployment, verification, and validation, ensuring all Users/PEs authenticate via approved MFA and IdP solutions.
- The Component leverages Enterprise identity lifecycle management policies, security best practices (e.g., National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-3, etc.), and external logging to Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions for continuous monitoring.
- The Component ensures ongoing security by maintaining audit-ready logging, refining access policies, and continuously evaluating MFA and IdP integrations to adapt to evolving threats and organizational needs.

✓ EXPECTED OUTCOMES

1. Component is using IdP with MFA for critical applications/services.

2. Components have implemented an IdP that enables DoW PKI Multi-Factor Authentication (e.g., CAC, DPIV, DoW Issued PIV-I, FIPS 201 Compliant softcerts).

3. DoW Enterprise is the approved organizational PKI for critical services (ECA, FPKI, Category I/II/III PKI, etc.).

4. Utilize approved Alternative Hardware Tokens as needed - USB Security Key and/or OTP device (e.g., YubiKey FIPS for smartcard, FIDO2, FIDO U2F, OTP, RSA SecurID for OTP, etc.).

5. For access to low-risk resources (e.g., PII, publicly released information), utilize alternative two-step, two-factor authentication using software authenticators (e.g., Mobile Connect, Yubico, Okta Verify, etc.).

Capability 1.4 Privileged Access Management (PAM)

Table 6: 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 Users/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 Administration (JEA)
- Just-in-Time (JIT) Access
- Privileged Access Management (PAM)
- Role-Based Access Control (RBAC)

Activity 1.4.1 Implement System and Migrate Privileged Users Part 1

Table 7: Activity 1.4.1 — Implement System and Migrate Privileged Users 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 a Privileged Access Management (PAM) solution to support all critical privileged use cases. Application/Service integration points are identified to determine status of support for the PAM solution. Applications/Services that easily integrate with the PAM solution are transitioned to using the solution, versus static and direct privileged permissions.	
Predecessor(s)	**Successor(s)**
None	1.4.2
Expected Outcomes	
• Privilege Access Management (PAM) tooling is implemented. • Applications and devices that support and do not support PAM tools are identified. • Applications that support PAM, now use PAM for controlling emergency/built-in accounts.	
End State	
Components implement a PAM tool with a clear transition plan that identifies the applications and decides what applications require a PAM tool.	

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 1.1.1 (Discovery) – *Inventory User* prior to this activity, to compile the privileged User/Person Entity (PE) account list.
- Consider completing Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)* prior to this activity, to leverage systematic Multi-Factor Authentication (MFA) enforcement.
- Consider completing Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM) Part 1* prior to this activity, as it provides relevant identity management policies.
- Consider completing Activity 3.1.1 (Discovery) – *Application and Code Identification* prior to this activity, to obtain the application inventory.
- Consider the requirements from Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1* when selecting a Privileged Access Management (PAM) solution, as it will need to integrate with Enterprise MFA/IdP solutions in this future activity.

- Adopt a scalable architecture design for future growth and diverse data authoritative sources.
- Promote a flexible and adaptable platform environment (e.g., cloud-based, microservice, etc.).
- Define and regularly review service accounts (Users/PEs) lifecycle account management.
- Focus on people, processes, and technology that require privileged access and enforce policies specific to access control requirements.
- Activity 1.4.2 (Phase Two) – *Implement System and Migrate Privileged Users 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 8: Implementation Tasks for Activity 1.4.1 — Implement System and Migrate Privileged Users Part 1

Gather Component PAM solution requirements.
Leverage existing privileged access policies: ☐ Leverage and review established identity policies, from Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM) Part 1*. ☐ Leverage the Component Identity Lifecycle Management (ILM) board/stakeholders, from Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM) Part 1.* **Define scope and objectives:** ☐ Focusing on mission and security compliances, define the scope and objectives for a successful PAM implementation. ☐ Establish the criteria for which applications will/will not require access to the Component-defined PAM solution. **Identify privileged accounts:** ☐ Refer to the Enterprise identity authoritative source and the Component local identity repository to verify, validate, and review User/PE and application-privileged accounts.

Review existing User/PE and application inventories:

☐ Leverage the application inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification,* to identify the critical applications.

☐ Leverage the Master User Inventory, from Activity 1.1.1 (Discovery) – *Inventory User,* to compile the privileged User/PE account list.

☐ 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 existing MFA capability:

☐ Refer to the approved Enterprise guidelines to define and review the MFA solution and application requirements. Leverage systematic MFA enforcement, from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*.

Select Component PAM solution.

Select PAM solution:

☐ Choose a PAM solution that meets the Component's security requirements.

☐ Ensure the solution supports the applications and services in the inventory.

☐ Consider the requirements for integration into a Public Key Infrastructure (PKI), from Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1,* when selecting a PAM solution.

Verify and validate Component PAM feasibility.

Test the PAM solution:

☐ Ensure the PAM solution meets the Enterprise and/or Component requirements.

☐ Ensure the PAM solution integrates with the Component environment.

Implement the Component PAM solution.

Configure PAM to manage a diverse range of credentials from authoritative sources:

☐ Configure PAM to control access to privileged access for the identified applications/services, leveraging a secure credential vault.

☐ Configure policies, roles, and access controls.

☐ Configure limited User/PE account permissions to those required to perform their job [13].

Plan the migration for integration into existing and legacy systems:

☐ 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 each application/service with the PAM solution:

☐ Implement a phased approach deployment, leveraging the Component-defined priorities, to integrate applications/services with the PAM solution.

☐ Leverage Identity, Credential, and Access Management (ICAM) capabilities for seamless integration and complete identity governance and access control policies.

Manage applications/services that cannot integrate with PAM through risk-based exceptions.

Manage exceptions:

☐ Applications/services that do not support PAM are:

- Identified
- Documented
- Approved or Rejected

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

☐ The Enterprise and/or Component determine risks.

☐ Approval is periodically reassessed.

Verify and validate the Component PAM solution.

Verify and validate the PAM solution:

☐ Test the integration to ensure that privileged access is managed correctly.

☐ Verify and validate that the PAM solution is functioning as expected and access controls are enforced.

Verify and validate logging:

☐ Verify and validate that the PAM solution can provide detailed logs for the Security Information and Event Management (SIEM)/Security Orchestration, Automation, and Response (SOAR), and/or Artificial Intelligence/Machine Learning (AI/ML) to utilize.

- Log standardization, from Activity 7.1.2 (Phase One) – *Log Parsing.*
- SIEM log detail requirements, from Activity 7.2.4 (Phase One) – *Asset ID and Alert Correlation.*
- AI/ML integration, from Activity 7.3.2 (Phase Two) – *Establish User Baseline Behavior.*

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 1.4.1 (Phase One) – *Implement System and Migrate Privileged Users Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of a Privileged Access Management (PAM) solution. It presents strategic insights that drive implementation and expected outcomes, including the implementation of a PAM solution and the identification of applications/devices that do not support PAM tools.

Table 9: Activity 1.4.1 — Implement System and Migrate Privileged Users Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is PAM tooling implemented for managing privileged Users/Person Entities (PEs)? 2. How are applications that support and do not support PAM tools identified? 3. How are emergency and built-in accounts managed using PAM?

STRATEGIC INSIGHTS
• The Component provides a structured approach to PAM through a migration plan that leverages existing identity lifecycle policies, sets clear security objectives, and identifies privileged accounts across applications, users/PEs, and services. • The Component demonstrates security and compliance by selecting and integrating a PAM solution that enforces Multi-Factor Authentication (MFA) and systematically governs privileged access to critical systems. • The Component defines and documents policies and procedures to identify which applications support PAM capabilities, distinguishing these from applications that do not support PAM or privileged identity management. • The Component provides verifiable enforcement through phased migration plan, integration testing, and policy-driven access controls, ensuring that privileged accounts are managed securely and restricted to necessary functions. • The Component leverages Enterprise Identity, Credential, and Access Management (ICAM) capabilities to streamline PAM integration, enforce role-based access, and maintain centralized oversight of privileged accounts. • The Component ensures ongoing security by continuously monitoring privileged access, verifying and validating PAM logs through Security Information and Event Management (SIEM), and performing regular audits to maintain compliance and mitigate emerging threats.

EXPECTED OUTCOMES
1. PAM tooling is implemented. 2. Applications and devices that support and do not support PAM tools are identified. 3. Applications that support PAM, now use PAM for controlling emergency/built-in accounts.

Capability 1.5 Identity Federation and User Credentialing

Table 10: 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 Users/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 1.5.1 Organizational Identity Lifecycle Management (ILM)

Table 11: Activity 1.5.1 — Organizational Identity Lifecycle Management (ILM)

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 establish a process for lifecycle management of users both privileged and non-privileged. Utilizing an approved Identity Provider (IdP) the process is implemented and followed by the maximum number of users. Users falling outside of the standard process are approved through risk-based exceptions to be evaluated regularly for decommission.	
Predecessor(s)	**Successor(s)**
None	1.5.2
Expected Outcomes	
• Standardized account lifecycle process.	
End State	
Establishes a comprehensive and efficient process that ensures the accurate and secure management of user identities throughout their entire lifecycle within the Component’s 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.

- The Identity Lifecycle Management (ILM) process should be developed:
  - to align with the Enterprise requirements.
  - through inclusive stakeholder engagement.
  - to meet the unique needs of the Component.
- Determine how your Component will manage guest and/or federated identities.
- Identity, Credential, and Access Management (ICAM) are elements of the Identity and Access Management (IAM) software solution for Users/Person Entities (PEs) and Component identity management.
- User/PE credentialing should be included in the security policy, along with authentication, authorization, credential management, and Identity Management (IdM). This policy should detail how to identify and verify and validate User/PE credentials and identities throughout the system's lifecycle, leveraging Attribute-Based Access Control (ABAC) to dynamically grant access based on User/PE attributes, resource attributes, and environmental conditions.

- Activity 1.5.2 (Phase Two) – *Enterprise Identity Lifecycle Management (ILM) Part 1* 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 12: Implementation Tasks for Activity 1.5.1 — Organizational Identity Lifecycle Management (ILM)

Establish an ILM process that covers both privileged and non-privileged Users/PEs.
Lifecycle management of privileged/non-privileged Users/PEs: ☐ Identify and implement an approved Identity Provider (IdP) that supports the full identity lifecycle, including provisioning, access changes, and deprovisioning. ☐ Define the criteria for where Users/PEs are added, modified, and/or removed from the IdP. At a minimum, this should include: • Onboarding: Role assignment, access provisioning, and initial IdP registration. • Role/job changes: Role-based access updates and system privilege adjustments. • Offboarding: Timely account disablement/removal and revocation of privileges and credentials. ☐ Define and document a risk-based exception process for Users/PEs who cannot be integrated into the IdP, including criteria for exception eligibility, approval process, and oversight mechanisms.
Migrate Users/PEs to the approved IdP, excluding minimal exceptions.
Migrate Users/PEs: ☐ Develop and implement a phased migration plan to onboard all eligible Users/PEs into the IdP, prioritizing privileged Users/PEs and high-risk roles. ☐ Verify and validate accurate mapping of user accounts to roles, access rights, and organizational structures.
Manage Users/PEs outside the standard ILM process through risk-based exceptions.
Manage exceptions: ☐ Users/PEs outside the standard ILM process are: • Identified • Documented • Approved or Rejected

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

☐ The Enterprise and/or Component determine and document risks associated with each exception.

☐ Approval is periodically reassessed and documented on a scheduled basis.

Periodically assess Users/PEs for deprovisioning and decommissioning.

Conduct periodic assessments:

☐ Leverage the ILM process to periodically review the status of all Users/PEs, focusing on:

- Role-based changes that require access adjustment.
- Accounts eligible for deactivation or deletion due to inactivity or separation.

☐ Reassess and reauthorize exceptions based on their current justification, risk posture, and any changes to system architecture or user roles. The frequency of verification and validation should be proportionate to the risks associated with their role, access, and any other factors deemed relevant to the Enterprise or Component.

☐ Maintain logs and audit documentation of all reviews, approvals, and changes for compliance verification.

Verify and validate ILM process / IdP.

Verify and validate:

☐ At least annually, the Component should verify and validate the ILM process:

- Aligns with current Enterprise policy and guidance.
- Supports secure and accurate identity lifecycle operations.
- Includes effective exception and deprovisioning mechanisms.

☐ Confirm that responsible teams and stakeholders understand the ILM process and are effectively implementing ILM activities. For example:

- The ILM process is understood and implemented by responsible parties within the Component.
- Users/PEs moving to a new role within the Component have their accounts modified as necessary within the IdP.
- Users/PEs with an IdP exception are reassessed to ensure the original justification for the exception is relevant and the Component is managing most of its Users/PEs within the IdP.

Summary

This diagram outlines the Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM)* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of an Identity Lifecycle Management (ILM) process. It presents strategic insights that drive the implementation and expected outcomes of a standardized account lifecycle process.

Table 13: Activity 1.5.1 — Organizational Identity Lifecycle Management (ILM) - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the Organizational ILM process for regular and privileged Users/Person Entities (PEs) established and implemented? 2. How are exceptions to the ILM process managed and regularly evaluated?
STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for managing the lifecycle of both privileged and non-privileged Users/PEs, including onboarding, offboarding, and periodic access reviews, ensuring alignment with Enterprise Identity, Credential, and Access Management (ICAM) governance within a Component ILM plan. • The Component demonstrates compliance by migrating users into the ILM process, leveraging Personal Identity Verification (PIV) credentials and continuous vetting solutions, while enforcing role-based and Just-in-Time (JIT) access principles to maintain Least Privilege. • The Component provides evidence that risk-based exceptions are used sparingly and documented for Users/PEs who fall outside the standard ILM process, supported by appropriate security policies, controls, and compliance measures. • The Component periodically assesses Users/PEs for deprovisioning and decommissioning, consolidates data sources, ensures data retention and reporting functions remain centralized and compliant, and maintains access to relevant records even after legacy systems are retired. • The Component continuously monitors, audits, and updates ILM policies, leveraging Identity and Access Management (IAM) and Privileged Access Management (PAM) solutions to document and automate critical processes, ensuring that the User/PE lifecycle management framework remains effective, secure, and adaptable to evolving requirements.
EXPECTED OUTCOMES
1. Standardized account lifecycle process.

Capability 1.7 Least Privileged Access

Table 14: Capability 1.7 — Least Privileged Access

<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>1 - User</td><td>1.7 - Least Privileged Access</td></tr>
<tr><td colspan="2"><strong>Description</strong></td></tr>
<tr><td colspan="2">DoW Components govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities. DoW Application Owners identify the necessary roles and attributes for standard and privileged user access. Privileged access for all Components DAAS is audited and removed when unneeded.</td></tr>
<tr><td colspan="2"><strong>Impact to ZT</strong></td></tr>
<tr><td colspan="2">Users on the network only have access to the DAAS for which they are authorized and authenticated over a specific timeframe.</td></tr>
</table>

Scenario

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

- The Component implements a "deny-by-default" policy, ensuring Users/Person Entities (PEs) are granted access only to the minimum resources required to perform their assigned tasks.
- Application owners within the Component define and document roles and attributes for both standard and privileged Users/PEs, specifying which Data, Applications, Assets, and Services (DAAS) resources each role requires.
- The Component reviews existing access rights comprehensively, identifying and removing excessive or unnecessary privileges.
- Privileged access is configured with strict time-based limits, requiring Users/PEs to request temporary access for specific tasks through Just-In-Time (JIT) workflows.
- During a routine audit, the Component discovers a dormant privileged account that has not been used in six (6) months. The account is immediately deactivated and flagged for further investigation.
- The Component's security solutions automatically deny any access attempts to sensitive DAAS resources that fall outside a User's/PE’s defined role scope, enforcing the "deny-by-default" policy.

- Security analysts within the Component review denied access attempts, identify suspicious behavior patterns, and escalate cases for further investigation when necessary.
- The Component implements role reassignment processes during organizational changes, ensuring Users/PEs only retain access relevant to their new responsibilities.
- Regular audits of privileged access logs allow the Component to proactively identify and remove unnecessary access, ensuring compliance with Least Privilege principles.
- By strictly enforcing Least Privileged access and denying access by default, the Component reduces its attack surface and mitigates potential threats.

Positive Impacts

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

- Minimized Security Risks: Enforcing Least Privileged access ensures Users/PEs and systems only have the permissions necessary for their roles, reducing the attack surface and limiting potential damage from compromised accounts.
- Prevention of Insider Threats: By restricting access to sensitive systems and data, the Component mitigates the risk of accidental or intentional misuse by employees or third parties.
- Enhanced Regulatory Compliance: Implementing Least Privileged access helps the Component meet compliance requirements by enforcing strict access controls and reducing unnecessary exposure of critical information.
- Improved Operational Efficiency: Automating Role-Based Access Control (RBAC) streamlines permissions management, reducing administrative overhead while ensuring employees have access to perform their tasks.
- Reduced Impact of Credential Compromise: Even if an account is compromised, limited access rights prevent attackers from moving laterally within the Component’s environment, minimizing the potential damage.

Technology

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

- Attribute-Based Access Control (ABAC)
- Audit and Logging
- Cloud Security Platforms
- Just-in-Time (JIT) Access
- Privileged Access Management (PAM)
- Role-Based Access Control (RBAC)

Activity 1.7.1 Deny User by Default Policy

Table 15: Activity 1.7.1 — Deny User by Default 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 Components audit user and group usage for permissions and revoke permissions when appropriate. This activity includes the revocation and/or decommission of excess permissions and access for application/service-based identities and groups. Where possible, static privileged users are decommissioned or permissions are reduced, preparing for future rule-/dynamic-based access. The implemented audit and governance functions are automated where possible.	
Predecessor(s)	**Successor(s)**
None	None
Expected Outcomes	
• Applications updated to deny-by-default to functions/data requiring specific roles/attributes for access. • Reduced default permission levels are implemented. • Applications/services privileged users have been reviewed and audited, and unnecessary access has been removed. • Applications identify functions and data requiring specific roles/attributes for access. • Audit functions and governance processes are implemented and automated, when possible, to update user authentication and authorization.	
End State	
Users must be authorized and authenticated to access data, applications, assets, and services. Audit and access validation occurs consistently.	

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 1.1.1 (Discovery) – *Inventory User* prior to this activity, as a comprehensive list of Users/Person Entities (PEs) is necessary to ensure Least Privilege is applied consistently and completely.
- Consider completing Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)* prior to this Activity, as it is necessary to effectively remove static permission assignments to Users/PEs*.*
- Consider completing Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM)* prior to this activity, as it is necessary to have this in place to understand and define permissions for Users/PEs, roles, and groups.

- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, as a comprehensive list of devices is necessary to ensure Least Privilege is applied consistently and completely.
- Consider completing Activity 3.1.1 (Discovery) – *Application and Code Identification* prior to this activity, as a comprehensive list of applications/services is necessary to ensure Least Privilege is applied consistently and completely.
- Consider completing Activity 4.1.1 (Discovery) – *Data Analysis* prior to this activity, as a comprehensive list of data/data types is necessary to ensure Least Privilege is applied consistently and completely.

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 16: Implementation Tasks for Activity 1.7.1 — Deny User by Default Policy

Identify Component Data, Applications, Assets, and Services (DAAS).
Identify data: ☐ Leverage the data inventory, from Activity 4.1.1 (Discovery) – *Data Analysis*. **Identify applications/services:** ☐ Leverage the application/code inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification.* **Identify assets:** ☐ Leverage the device inventory, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis*.
Assess current User/PE permissions.
Identify Users/PEs: ☐ Leverage the Master User Record, from Activity 1.1.1 (Discovery) – *Inventory User*. **Identify authorization source(s):** ☐ Leverage the authorization sources, from Activity 1.1.1 (Discovery) – *Inventory User;* **or** ☐ Leverage the organizational Identify Provider(s) (IdP(s)), from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*.

Document permissions: ☐ Document the existing permissions provisioned to Users/PEs through the Component authorization source(s). • If possible, leverage permissions and roles, from Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM).* ☐ Identify permissions that can be attributed to roles rather than directly assigned to Users/PEs. ☐ Assess current permissions to determine the least necessary access Users/PEs or roles required to perform their assigned functions, to remove unnecessary privileges. ☐ Document the new permission baselines for all Users/PEs and roles.
Remove excess permissions for Users/PEs.
Remove/delete excess permissions: ☐ Implement the new baseline permissions and assign roles as necessary to implement Least Privilege and Role-Based Access Control (RBAC) in accordance with the new Component-defined baselines.
Decommission static privilege Users/PEs and groups.
Decommission static privileges: ☐ Leverage the IdP(s), from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP),* to provide dynamic permission management for Users/PEs. ☐ Leverage the Component Identity Lifecycle Management (ILM) process, from Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM),* to minimize Users/PEs that are statically assigned permission/privileges.
Configure DAAS to deny access by default.
Configure assets and applications to deny access: ☐ Leverage the identified DAAS and implement access controls that deny-by-default. ☐ Ensure the Component approved Users/PEs continue to have appropriate access in support of their role/job functions.
Verify and validate that the deny-by-default access level has been applied to the environment(s).
Conduct access assessment: ☐ Verify and validate that unauthenticated Users/PEs cannot access Component applications/resources. ☐ Verify and validate that authenticated Users/PEs cannot access Component applications/resources that are outside the scope of their permissions.

Continuously revise and assess management rules, rulesets, and policies to align with changes in Component structure and data assets. Revoke access for Users/PEs and groups that no longer require access.

Continuously revise access controls:

☐ Organizational access rules can change for various reasons, including organizational changes, role changes, project changes, security updates, and the implementation of automated solutions.

☐ Continuously monitor User/PE permissions to align with the Organizational ILM plan.

☐ Continuously monitor Component applications/resources are effectively applying deny-by-default and access level restrictions in accordance with the permissions granted.

Summary

This diagram outlines the Activity 1.7.1 (Phase One) – *Deny User by Default Policy* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of permission level management for applications/services to ensure a policy of denying-by-default. It presents strategic insights that drive implementation and expected outcomes, including reducing default permissions across all applications/services and regular auditing of all User/Person Entity (PE) privileges.

Table 17: Activity 1.7.1 — Deny User by Default Policy - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How are applications updated to deny-by-default to functions/data requiring specific roles/attributes for access?

2. How are default permissions levels reduced and managed?

3. How are applications/services reviewed and audited to identify all privileged Users/PEs and remove those who do not need that level of access?

4. How are application functions and data requiring specific roles/attributes for access identified and managed?

STRATEGIC INSIGHTS

- The Component defines a structured approach to identifying and managing Data, Applications, Assets, and Services (DAAS), leveraging existing inventories and approval sources to establish clear access baselines and enforce the principles of Least Privilege.

- The Component demonstrates security and compliance by assessing and documenting current user and role-based permissions, removing excess privileges, and transitioning to dynamic access controls.

- The Component provides verifiable enforcement through deny-by-default access policies, periodic access assessments, and continuous monitoring, ensuring only approved Users/PEs have access to critical resources.

- The Component leverages the Identity Lifecycle Management (ILM) plan, from Activity 1.5.1 (Phase One) – *Organizational Identity Lifecycle Management (ILM)*, and organizational Identity Providers (IdPs), from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*, to automate permission management, enforce authentication, and minimize static privilege assignments.

- The Component ensures ongoing security by continuously revising access controls, adapting policies to organizational changes, and maintaining compliance through automated monitoring, role reassessments, and regular audits.

EXPECTED OUTCOMES

1. Applications updated to deny-by-default to functions/data requiring specific roles/attributes for access.
2. Reduced default permission levels are implemented.
3. Applications/services privileged users have been reviewed and audited, and unnecessary access has been removed.
4. Applications' identify functions and data requiring specific roles/attributes for access.
5. Audit functions and governance processes are implemented and automated when possible to update user authentication and authorization.

Capability 1.8 Continuous Authentication

Table 18: 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 an 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 and 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 1.8.1 Single Authentication

Table 19: Activity 1.8.1 — Single 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 authenticate users and NPEs at least once per session (e.g., logon) using CAC and other DoW-approved methods. Users being authenticated are managed by the parallel activity "Organizational MFA/IdP" with the Component Identity Provider (IdP). Components do not use application/service-based identities and groups.	
Predecessor(s)	**Successor(s)**
None	1.2.2, 3.4.1, 3.4.4
Expected Outcomes	
• Authentication implemented at least once per session.	
End State	
Component applications apply single authentication to the specified standard.	

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 20: Implementation Tasks for Activity 1.8.1 — Single Authentication

Authenticate Users/Person Entities (PEs)/Non-Person Entities (NPEs) with Multi-Factor Authentication (MFA) at least once per session.
Authentication with MFA requires the following: ☐ Leverage the approved IdP and MFA, from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*. ☐ Ensure that all Component-managed resources enforce authentication at session initiation using a Common Access Card (CAC) or other approved MFA methods. ☐ Confirm Users/PEs and NPEs are included in the authentication policy, with authentication required for each session initiated. ☐ Configure session timeout and termination settings based on inactivity thresholds, in alignment with the Enterprise policy.
Verify and validate that Users/PEs are authenticated at least once per session.
To verify and validate that authentication is met: ☐ Confirm that Enterprise and Component policies and procedures require session-based MFA for all Users/PEs, enforced through the approved IdP solution.

☐ Verify and validate the configuration of session timeout/termination policies for all access points, ensuring they are enforced across all systems and services.

☐ Demonstrate that a User/PE is required to authenticate when accessing a Component resource.

☐ Document findings and address gaps through policy, technical remediation, or exception tracking, as appropriate.

Summary

This diagram outlines the Activity 1.8.1 (Phase One) – *Single Authentication* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of single authentication across applications per session. It presents strategic insights driving implementation and the expected outcome of single authentication at least once per session.

Table 21: Activity 1.8.1 — Single Authentication - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is single authentication implemented across applications per session?

STRATEGIC INSIGHTS
• The Component defines authentication requirements by enforcing Multi-Factor Authentication (MFA) for all Users/Person Entities (PEs)/Non-Person Entities (NPEs) at least once per session, leveraging Identity Provider (IdP) solutions and implementing session timeout policies. • The Component demonstrates compliance by verifying and validating authentication enforcement, ensuring session termination due to inactivity, and verifying and validating that all Users/PEs/NPEs must authenticate before accessing resources. • The Component provides verifiable enforcement through authentication logs, policy audits, and real-time verification and validation, confirming that MFA policies are consistently applied and sessions are securely managed. • The Component leverages existing MFA and IdP solutions to streamline authentication, enhance security, and mitigate risks of unapproved access. • The Component ensures continuous security by maintaining strict session management policies, regularly reviewing authentication mechanisms, and adapting to evolving security requirements.

EXPECTED OUTCOMES
1. Authentication implemented at least once per session.

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, as single authentication is more easily implemented with an established Identity Provider (IdP).
- Activity 1.2.2 (Phase Two) – *Rule-Based Dynamic Access Part 1,* Activity 3.4.1 (Phase One) – *Resource Authorization Part 1*, and Activity 3.4.4 (Phase Two) – *Software-Defined Compute (SDC) Resource Authorization Part 2* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as successors to this activity.

Device Pillar

Capability 2.1 Device Inventory

Table 22: 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 2.1.2 Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management

Table 23: Activity 2.1.2 — Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management

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 DoW Enterprise PKI solution/service to deploy X.509 certificates to all supported and managed devices. Other Non-Person Entities (NPEs) (e.g., web servers, network devices, routers, applications, etc.) that support X.509 certificates are assigned them in the PKI and/or IdP systems.	
Predecessor(s)	**Successor(s)**
2.6.2	2.2.1, 2.3.6, 2.4.1
Expected Outcomes	
• Non-person entities are managed via Component PKI and IdP.	
End State	
Components use established PKI and IdP solutions to manage all NPEs.	

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 obtain an accurate device inventory list.
- Determine whether the system will utilize its own internal Certificate Authority (CA), Public Key Infrastructure (PKI), or a combination of both.
- Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1* establishes the integration of the Component to the Enterprise PKI. If this activity has not yet been completed, then the Component will need to establish its own internal CA.
- Determine the most secure certificate encryption type and signing algorithm for each product in the environment in accordance with Enterprise requirements and Component operational demands.
- Where possible, allow for the ability to issue multiple encryption strengths that meet the Component's security requirements.
- Leverage cryptographic industry standards, such as National Institute of Standards (NIST) Federal Information Processing Standards (FIPS) 140-3.
    - Examples include Advanced Encryption Standard (AES)-256, Rivest-Shamir-Adleman (RSA)-4096, and Elliptic Curve Digital Signature Algorithm (ECDSA) with appropriate key lengths.
    - Consider Post-Quantum Cryptography (PQC) options, to include emerging NIST PQC guidance.
- Create a plan to issue certificates for devices, Users/Person Entities (PEs), and Non-Person Entities (NPEs), and establish a policy to determine when certificate sharing is permitted.
    - Policies should clearly define the conditions under which certificate sharing is permissible, such as for specific application integrations or service accounts, and mandate robust security controls to mitigate risks.
- Determine the approved signed certificates for use across multiple functions within a product (e.g., Secure Shell (SSH), Hypertext Transfer Protocol Service (HTTPS), Lightweight Directory Access Protocols (LDAPs), etc.).

- Create a plan to renew and revoke certificates within the environment, including automated revocation through Security Orchestration, Automation, and Response (SOAR) policies for a maximum duration based on the encryption strength.
- Check accesses regularly, as revocation may be needed if an NPE is no longer necessary or if solutions change in such a way that the level of access is no longer required.
- Activity 2.2.1 (Phase Two) – *Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1*, Activity 2.3.6 (Phase Three) – *Enterprise Public Key Infrastructure (PKI) Part 1*, and Activity 2.4.1 (Phase One) – *Deny Device by Default Policy* 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 24: Implementation Tasks for Activity 2.1.2 — Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management

Implement Enterprise PKI solution/service to deploy X.509 certificates to all supported and managed devices.
The process for PKI to deploy X.509 certificates is focused on the following: ☐ Leverage approved inventory, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis,* of all supported and managed (devices) and NPEs. ☐ Ensure the minimum validity period is documented, verified, and validated to ensure that proper processes are followed to ensure complete coverage and avoid certificate issuance for unapproved devices. **Define certificate policies:** ☐ Leverage previously established regulations/guidelines to define policies that will govern the issuance and usage of the X.509 certificates (PKI certificates and Protocols) [2]. ☐ Identify specific detailed PKI requirements (e.g., CA (Root, Intermediate, or Subordinate), Validation Authority (VA), and Registration Authority, etc.) along with required devices for issuing X.509 certificates [2]. **Establish a CA:**

☐ Establish a CA using Component PKI certificates as required by policy. A CA is needed to issue required public-key certificates and provide the core authentication, integrity, and confidentiality services [14].

Generate X.509 Certificates:

☐ Generate X.509 certificates for each supported and managed device.

☐ Ensure the established CA signs certificates.

☐ Ensure certificates include the required information: device identity, expiration date, and usage constraints [14].

Establish a certificate enrollment process (enroll all devices in the environment in accordance with Comply-to-Connect (C2C) policies):

☐ Implement a secure and automated process for devices to enroll X.509 certificates.

☐ Enforce strong Multi-Factor Authentication (MFA), approval methods to ensure only approved devices can request and receive certificates.

☐ Verify and validate password security for the X.509 certificates. Malicious hackers may try to intercept messages as they are transmitted between computers and software entities [14].

☐ Enforce strong password authentication methods. When passwords are extracted, all Enterprise and/or sensitive data can be accessed without proper permission and approval [14].

Deploy a certificate management solution:

☐ Configure a certificate management infrastructure that allows for the distribution, revocation, and renewal of X.509 certificates.

☐ Include mechanisms for securely storing and distributing certificates to the supported devices.

Integrate a PKI solution:

☐ Integrate PKI solution with the environment architecture.

☐ Configure the devices to use the X.509 certificates to authenticate, approve supported and managed devices.

Continuous monitoring and maintenance:

☐ Ensure continuous monitoring of the PKI solution to verify and validate proper functionality of the certificate management process, such as certificate expirations, revocation status, and CA health.

☐ Update and renew certificates as required to maintain the security and integrity of the system.

☐ Backup X.509 certificates and maintenance.

Assign NPEs (e.g., web servers, network devices, routers, applications, etc.) that support X.509 certificates to the Enterprise PKI or the implemented PKI/Identity Provider (IdP) solution.

Implement NPEs into a Component's PKI and IdP:

☐ Generate X.509 certificates:

- NPEs can request an X.509 certificate.

- Approve X.509 certificates with PKI and Single Sign-On (SSO) and apply Least Privilege access control.

□ Continuous monitoring and revocation:

- Implement a process to continuously monitor and revoke outdated/no longer valid X.509 certificates and back up X.509 certificates with security keys (private keys). CAs should consider issuing and processing Certificate Revocation Lists (CRLs). The RA has the privilege to revoke NPE certificates after they have been issued [15].
- Develop a Component security awareness program for NPEs.
- Integrate the process with the Component Incident Response (IR) community.

Summary

This diagram outlines the Activity 2.1.2 (Phase One) – *Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of an Enterprise Public Key Infrastructure (PKI) solution to deploy X.509 certificates and Non-Person Entity (NPE) management. It presents strategic insights that drive implementation and expected outcomes, including NPE management via Component PKI and Identity Provider (IdP).

Table 25: Activity 2.1.2 — Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the DoW Enterprise PKI solution used to deploy X.509 certificates to all supported and managed devices? 2. How are NPEs managed via organizational PKI and IdP systems?

STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for implementing the Enterprise PKI solution, issuing X.509 certificates to all supported and managed devices, and aligning with established Enterprise requirements, certificate policies, and security requirements. • The Component demonstrates compliance by conducting a comprehensive inventory of supported devices, establishing a Certificate Authority (CA) and enrollment process, and ensuring that each device receives and properly uses X.509 certificates for authentication and approval. • The Component provides evidence that strong authentication methods (e.g., Multi-Factor Authentication (MFA), secure password handling, etc.) are enforced for certificate issuance, deployment, and renewal, thereby mitigating the risk of unapproved access. • The Component integrates the PKI solution into its network architecture, continuously monitors the PKI infrastructure, and maintains certificate management processes (including revocation and renewal) to ensure ongoing certificate integrity and trust. • The Component incorporates NPEs into the PKI and IdP solution, assigning X.509 certificates and implementing continuous monitoring, revocation procedures, and security awareness programs to maintain compliance and protect critical resources.

EXPECTED OUTCOMES
1. Non-Person Entities are managed via Component PKI and IdP.

Capability 2.4 Remote Access

Table 26: 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 Users/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 2.4.1 Deny Device by Default Policy

Table 27: Activity 2.4.1 — Deny Device by Default Policy

<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 Enterprise sets standards and requirements for overall policy, with Components tailoring them to their specific environments and mission requirements. Components will block access from all unmanaged remote and local devices to resources. Managed, compliant devices are provided risk-based, methodical access following ZT Target-level concepts.</td></tr>
<tr><td><b>Predecessor(s)</b></td><td><b>Successor(s)</b></td></tr>
<tr><td>2.1.2</td><td>None</td></tr>
<tr><td colspan="2"><b>Expected Outcomes</b></td></tr>
<tr><td colspan="2">• Enterprise sets standards for Deny Device by Default policy.
• Components will block unmanaged devices remotely/locally.
• Access is enabled strictly for compliant devices remotely/locally following the "Deny Device by Default" policy approach.</td></tr>
<tr><td colspan="2"><b>End State</b></td></tr>
<tr><td colspan="2">All device access is authorized, verified, and compliant and all other devices are blocked by default.</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 2.1.2 (Phase One) – *Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Presumption: The Hardware/Software List from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis*, is up to date and reflects the current environment.
- Evaluate Enterprise device compliance policies to ensure they meet requirements before granting access to the Component environment.

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 28: Implementation Tasks for Activity 2.4.1 — Deny Device by Default Policy

Establish policies that follow Enterprise Deny Device by Default access standards and requirements.
Develop a Component-level Deny Device by Default policy: ☐ Leverage existing Enterprise Deny Device by Default standards and requirements when developing Component-level Deny Device by Default policy. ☐ Collaborate with the Enterprise to define access policies for both managed and unmanaged devices, ensuring a mutual understanding of enforcement expectations. ☐ Ensure Component-level policies align with Enterprise standards and industry best practices for deny-by-default. [16]. ☐ Map and tailor Enterprise Deny Device by Default requirements to the existing Component-level cybersecurity policies. ☐ Include conditions for reclassification of devices as compliant or non-compliant based on posture validation tools (e.g., Comply-to-Connect (C2C), Enterprise Device Management (EDM), etc.). **Apply the Component-level Deny Device by Default policy:** ☐ Establish a baseline Component-level Deny Device by Default policy that denies access to all devices by default and blocks all unmanaged remote and local device access to all Component resources. ☐ Define explicit permissions for each device and ensure that access permissions are granted based on the principle of Least Privilege. ☐ Ensure policy-based access is conditional, risk-informed, and dynamically reassessed based on device posture changes. ☐ Integrate policy into access control systems (e.g., Network Access Control (NAC), firewalls, endpoint security, etc.) for automated enforcement, where possible.
Manage devices outside the deny-by-default policy through risk-based exceptions.
Manage exceptions: ☐ Devices outside the deny-by-default policy are: • Identified • Documented • Approved or Rejected ☐ Approval is granted when justification for the exception outweighs the risks to the Enterprise/Component. ☐ The Enterprise and/or Component determines risks. ☐ Approval is periodically reassessed. ☐ Maintain and regularly review a centralized exception register for audit and accountability.

☐ All exceptions should include:

- Risk justification
- Temporary duration
- Compensating controls (e.g., segmentation, limited access scope, etc.)

Verify and validate access for compliant devices.

Implement access control mechanisms:

☐ Configure Access Control Lists (ACLs) for devices in the environment to enforce the Deny Device by Default policy, ensuring only compliant devices are granted access.

☐ Implement Role-Based Access Control (RBAC) to manage access permissions based on User/Person Entity (PE)/Non-Person Entity (NPE) roles.

☐ Utilize Attribute-Based Access Control (ABAC) to enforce access decisions based on User/PE/NPE attributes (e.g., identity, role, location, device security posture, etc.).

☐ Document compliance matrices to track adherence to all Component-level Deny Device by Default requirements.

☐ Verify and validate compliance status using posture assessment solutions integrated with C2C and/or Endpoint Detection and Response (EDR) platforms.

☐ Test controls under live scenarios (e.g., simulated unmanaged device access, etc.) to verify and validate enforcement accuracy.

Verify and validate that unmanaged devices are blocked remotely and locally.

Integrate continuous device monitoring and auditing:

☐ Block access for all unmanaged remote and local devices to Component resources.

☐ Continuous monitoring should be incorporated to track all access attempts, including denied connections from unmanaged or non-compliant devices.

☐ Conduct regular audits to ensure compliance and identify gaps with Enterprise access control policies.

☐ Use logging, alerting, and ticketing to document and respond to unapproved device access attempts.

☐ Verify and validate blocking efficacy through routine risk assessments and/or threat emulation exercises, where possible.

Summary

This diagram outlines the Activity 2.4.1 (Phase One) – *Deny Device by Default Policy* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of a policy to block access to resources from unmanaged remote and local devices. It presents strategic insights that drive implementation and expected outcomes, including the strict management of access for compliant devices locally and/or remotely in accordance with the policy standards set by the Enterprise.

Table 29: Activity 2.4.1 — Deny Device by Default Policy - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the deny device by default policy implemented to block unmanaged remote and local device access to resources?

STRATEGIC INSIGHTS
• The Component defines deny device by default policies by aligning with Enterprise standards, collaborating with stakeholders, and tailoring access control requirements to enforce strict device security measures. • The Component demonstrates security and compliance by establishing a policy baseline that denies all device access by default, implementing explicit access permissions based on the principle of Least Privilege, and verifying and validating that only compliant devices can connect to Component resources. • The Component provides verifiable enforcement through access control mechanisms such as Access Control Lists (ACLs), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC), ensuring only approved and properly secured devices are permitted. • The Component leverages continuous monitoring, compliance tracking, and regular audits to detect and prevent unapproved access, integrating real-time device verification and validation with Enterprise security frameworks. • The Component ensures ongoing security by maintaining an adaptive policy framework, blocking unmanaged devices, and continuously assessing alignment with evolving Enterprise and National Institute of Standards and Technology (NIST) deny-by-default standards.

EXPECTED OUTCOMES
1. Enterprise sets standards for Deny Device by Default policy. 2. Components will block unmanaged devices remotely/locally. 3. Access is enabled strictly for compliant devices remotely/locally following the Deny Device by Default policy approach.

Capability 2.5 Partially and Fully Automated Asset, Vulnerability, and Patch Management

Table 30: Capability 2.5 — Partially and Fully Automated Asset, Vulnerability, and Patch 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**
2 - Device	2.5 - Partially and Fully Automated Asset, Vulnerability, and Patch Management
Description	
DoW Components establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed.	
Impact to ZT	
Risk is minimized by automatically deploying vendor patches to all network devices.	

Scenario

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

- The Component implements asset, vulnerability, and patch management solutions to maintain an up-to-date inventory of connected devices, including their patch and vulnerability statuses.
- A hybrid patch management process is established, combining automated and human oversight to ensure vendor patches are tested and deployed efficiently without disrupting operations.
- The Component configures automated solutions to continuously scan vendor feeds for critical patches and match them against its device inventory to identify affected devices.
- During a routine scan, the solutions detect a critical vulnerability affecting multiple network devices and prioritize these devices for immediate patching.
- Automated systems deploy the patch to non-critical devices in a sandbox environment for testing while human administrators review the results to ensure the patch does not introduce issues.
- Upon successful testing, the patch is rolled out to critical devices across the network, with the automated system monitoring deployment progress and verifying and validating successful installation.

- The Component's security solutions detect a rogue device attempting to exploit the now-patched vulnerability but fail to gain access due to the updated patch status of all compliant devices.
- Vulnerability scans confirm that the Component’s patching efforts have closed the critical security gap, reducing the network's overall risk.
- The Component schedules periodic audits to review the effectiveness of its patch management process, ensuring the hybrid approach adapts to emerging threats and technology changes.
- The Component minimizes risk by automating asset, vulnerability, and patch management processes and ensures timely deployment of vendor patches.

Positive Impacts

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

- Significantly Reduced Vulnerability Exposure: Timely application of security updates minimizes the window of opportunity for potential attackers.
- Increased Operational Efficiency: The Component automates routine patch testing and deployment processes while maintaining human oversight for critical decisions.
- More Consistent Patch Coverage: The Component eliminates protection gaps that often occur with purely manual patching approaches across the device ecosystem.
- Enhanced Resilience Against Emerging Threats: The Component’s rapid response abilities can quickly deploy critical security fixes when new vulnerabilities are discovered.
- Optimized Resource Utilization: Balancing automated processes with strategic human intervention allows technical staff to focus on complex issues while routine updates proceed automatically.

Technology

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

- Configuration Management Database (CMDB)
- IT Asset Management (ITAM) Software
- Patch Management solutions
- Security Orchestration, Automation, and Response (SOAR)
- Vulnerability Management solutions

Activity 2.5.1 Implement Asset, Vulnerability, and Patch Management Tools

Table 31: Activity 2.5.1 — Implement Asset, Vulnerability, and Patch Management 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 implement solution(s) for managing asset/device configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, C2C, UEM, etc.), teams can confirm or deny managed device compliance. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.	
Predecessor(s)	**Successor(s)**
None	2.2.1, 3.2.3
Expected Outcomes	
• Components can confirm if devices meet minimum compliance standards or not. • Component solutions enable integration across asset management, vulnerability, and patching systems while considering automation capabilities.	
End State	
Continuously identify and address vulnerabilities, manage assets effectively, and apply necessary patches to mitigate potential threats and maintain a secure 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.

- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, to obtain an accurate device inventory list.
- Prioritize asset, vulnerability, and patch management solutions that offer robust Application Programming Interfaces (APIs) or other programmatic interfaces. This will enable automation and integration with other security solutions (e.g., Security Orchestration, Automation, and Response (SOAR), Comply-to-Connect (C2C), etc.).
- Ensure that asset, vulnerability, and patch management solutions selections are interoperable with existing and evolving system solutions (e.g., Enterprise Device Management (EDM), Security Information and Event Management (SIEM), threat intelligence platforms, etc.). Consider using standardized data formats and communication protocols to facilitate integration.

- Create a configuration management plan and document all interactions between products so the secondary effects of unintended consequences of upgrades are understood.
- Determine each solution's criticality with respect to how it affects Users/Person Entities (PEs)/Non-Person Entities (NPEs) in the environment to help determine updates, as appropriate.
- When selecting asset, vulnerability, and patch management solutions, consider scalability, integration, automation, compliance, and cost.
- Activity 2.2.1 (Phase Two) – *Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1* and Activity 3.2.3 (Phase Two) – *Automate Application Security and Code Remediation 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 32: Implementation Tasks for Activity 2.5.1 — Implement Asset, Vulnerability, and Patch Management Tools

Evaluate the Component system to ensure it meets Enterprise security compliance requirements.
Review and prioritize asset inventory: ☐ Leverage the approved Hardware/Software List for Environment authentication and approval, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis.* ☐ Ensure the list is up-to-date and accurately reflects the current assets in the Environment. ☐ Review and prioritize the Hardware/Software List based on Enterprise cybersecurity policies. ☐ Perform gap analysis between existing security policies for asset, vulnerability, patch management, and Enterprise requirements. **Establish evaluation criteria for the Component system:** ☐ Develop specific evaluation criteria for the Component system based on Enterprise asset, vulnerability, and patch management solutions compliance requirements (e.g., asset inventory accuracy, vulnerability assessment frequency, patch deployment availability, etc.).

☐ Establish baseline standards for each criterion to measure compliance in accordance with the existing Enterprise policies (e.g., Security Technical Implementation Guides (STIGs), C2C, Unified Endpoint Management (UEM), etc.).

Choose evaluation solutions and methods:

☐ Select appropriate cybersecurity assessment, compliance management platforms, and auditing solutions/technologies for evaluating Component compliance with Enterprise policies.

☐ Determine preferred methods for conducting the evaluation. (e.g., manual audits, automated scans, interviews with key personnel, etc.).

Perform asset, vulnerability, and patch management solution integration readiness testing:

☐ Conduct a readiness assessment of all Component environments to identify dependencies and integration points for the asset, vulnerability, and patch tooling solutions.

Conduct asset management testing:

☐ Conduct manual audits to cross-check the inventory against physical assets and other data sources.

☐ Use automated discovery solutions to verify and validate the accuracy and completeness of the asset inventory.

Conduct vulnerability management testing:

☐ Review the vulnerability assessment schedule to ensure that testing meets Enterprise compliance requirements.

☐ Confirm vulnerability scanning solutions are properly configured to identify asset, system, and application weaknesses.

☐ Ensure identified vulnerabilities are assessed for criticality to maintain a secure environment.

Conduct patch management testing:

☐ Verify and validate the system which monitors vendor announcements, security advisories, and threat intelligence sources to identify available patches and updates, where applicable.

☐ Verify and validate that patch releases are tested in a timely manner and pushed in a controlled environment to ensure compatibility and stability prior to deployment.

☐ Verify and validate patches have been applied and known vulnerabilities are remediated.

Implement and integrate management tools.

Confirm asset, vulnerability, and patch management solutions compliance checks:

☐ Identify all asset, vulnerability, and patch management solutions compliance checks as specified by Enterprise policies (e.g., asset inventory accuracy, vulnerability scanning, patch levels, configuration baselines, antivirus status, encryption settings, etc.).

☐ Configure asset, vulnerability, and patch management tooling solutions to perform compliance checks using available APIs or integration mechanisms. Where APIs are not yet fully implemented, design configurations to support future automation and integration capabilities prior to environment access approval.

☐ Configure asset, vulnerability, and patch management solutions to interface with existing network approval solutions systems (e.g., SIEM, etc.), endpoint protection solutions, and Incident Response (IR) platforms.

Leverage asset, vulnerability, and patch management solutions to identify and address vulnerabilities, manage devices, and apply necessary patches:

☐ Implement continuous monitoring to identify and address vulnerabilities, manage assets effectively, and apply necessary patches to mitigate potential threats and maintain a secure environment.

☐ Conduct regular reviews of the asset, vulnerability, and patch management processes to identify areas for improvement, and verify and validate the efficacy of the solution's enforcement.

☐ Establish procedures for non-compliant device remediation, including automated patching and configuration correction.

☐ Provide guidance and technical support for resolving compliance failures.

Leverage or establish a vulnerability management and governance board.

Leverage existing, or build, a comprehensive vulnerability management team:

☐ Establish policy, assign responsibilities, and provide guidelines for participation in the Component Vulnerability Management Process.

Vulnerability triage and reporting:

☐ Develop technical analysis and remediation capabilities to select and prioritize vulnerabilities based on severity, exploitability, exposure, and compliance requirements [17].

☐ Empower the vulnerability management team to receive vulnerability reports from approved sources, coordinate and investigate to identify vulnerable systems, share findings reports with approved stakeholders for actions, and disseminate advisories and security bulletins on found vulnerabilities to the broader community as appropriate [17].

Summary

This diagram outlines the Activity 2.5.1 (Phase One) – *Implement Asset, Vulnerability, and Patch Management Tools* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of tools to confirm compliance across asset, vulnerability, and patch management. It presents strategic insights that drive implementation and expected outcomes, including component solutions that enable the integration of tools to test whether compliance standards are being met, and facilitate integration across systems.

Table 33: Activity 2.5.1 — Implement Asset, Vulnerability, and Patch Management Tools - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are asset, vulnerability, and patch management tools implemented to confirm if devices meet minimum compliance standards? 2. How are asset management, vulnerability, and patching systems integrated across systems using Application Programming Interfaces (APIs)?

STRATEGIC INSIGHTS
• The Component defines evaluation criteria and compliance standards for system security by aligning with Enterprise asset, vulnerability, and patch management policies, ensuring adherence to established cybersecurity requirements. • The Component demonstrates compliance by integrating approved asset management tools, conducting vulnerability assessments, and verifying and validating patch deployment processes to maintain a secure and up-to-date environment. • The Component provides verifiable enforcement through continuous monitoring, compliance checks, and integration of asset, vulnerability, and patch management solutions, ensuring security baselines are met before network access is granted. • The Component leverages Security Information and Event Management (SIEM), endpoint protection, and Incident Response (IR) platforms to automate security enforcement, track system health, and efficiently remediate vulnerabilities. • The Component ensures ongoing security by performing regular compliance audits, refining remediation processes for non-compliant devices, and continuously updating security configurations to align with evolving Enterprise cybersecurity policies.

EXPECTED OUTCOMES
1. Components can confirm if devices meet minimum compliance standards or not. 2. Component solutions enable integration across asset management, vulnerability, and patching systems while considering automation capabilities.

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

Table 34: 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 2.6.1 Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools

Table 35: Activity 2.6.1 — Implement Unified Endpoint and Device Management (UEDM) or Equivalent 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 will work closely with the "Implement Asset, Vulnerability, and Patch Management Tools" activity to procure and implement a Unified Endpoint and Device Management (UEDM) solution ensuring that requirements are integrated with the procurement process. Once a solution is procured the UEDM team(s) ensure that critical ZT Target-level functionalities such as minimum compliance, asset management, and API support are in place.	
Predecessor(s)	**Successor(s)**
None	2.3.6
Expected Outcomes	
• Components can confirm if devices meet minimum compliance standards or not. • Components have asset management system(s) for user devices (phones, desktops, laptops) that maintains IT compliance, which is reported up to DoW Enterprise. • Components asset management systems can programmatically (i.e., API) provide device compliance status and if it meets minimum standards.	
End State	
UEDM implementation enables effective patch management and configuration baselines. It also provides an ability to deny/quarantine devices remotely that are not in compliance.	

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 2.5.1 – (Phase One) *Implement Asset, Vulnerability, and Patch Management Tools* prior to this activity, to identify individual Component solution requirements and procurement processes. Careful coordination is essential to ensure successful Unified Endpoint and Device Management (UEDM) implementation:
    - Conduct a comprehensive assessment of the Component's specific environment requirements and technical constraints.
    - Thoroughly review and understand the Enterprise procurement policies, timelines, and approval workflows.

  - Establish early collaboration with procurement stakeholders to identify UEDM solutions that offer seamless integration capabilities with existing infrastructure.
  - Coordinate procurement timelines with implementation schedules to ensure the selected UEDM solution is acquired and available when needed for deployment.
- Components should consider developing a remediation plan for non-compliant devices (e.g., marking the device as non-compliant, remotely locking the device, denying network access, quarantining the device, etc.) and communicating directly with the device owner regarding non-compliance.
- Activity 2.3.6 (Phase Three) – *Enterprise Public Key Infrastructure (PKI) Part 1* 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 36: Implementation Tasks for Activity 2.6.1 — Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools

Identify and implement a UEDM solution.
Develop a UEDM integration plan: ☐ Integrate requirements, from Activity 2.5.1 – (Phase One) *Implement Asset, Vulnerability, and Patch Management Tools,* to develop a strategy for integrating asset, vulnerability, and patch management tools with the UEDM solution. **Configure UEDM solutions:** ☐ Configure the UEDM solution to discover and inventory all endpoints and devices. ☐ Establish signatures and baseline behaviors for devices within the environment [6]. ☐ Configure the vulnerability management tool to perform regular scans and assessments. ☐ Configure the patch management tool to handle patch deployment and testing [18]. ☐ Ensure interoperability between solutions to ensure a hardened security posture.

Implement an asset management system.

Develop an asset management integration plan:

□ Leverage and review the established Enterprise strategy as a blueprint, where applicable, for integrating the asset management system with other security tools and systems within the infrastructure.

□ Verify and validate security policies are in place to protect the assets and User/Person Entity (PE)/Non-Person Entity (NPE) devices throughout the integration process [18].

Configure asset management solutions:

□ Configure the asset management solution to identify and inventory all User/PE/NPE devices.

□ Implement configuration management policies to ensure all User/PE/NPE devices are securely configured and compliant with Component guidelines and standards [6].

□ Configure the asset management solution to collect the necessary data points (e.g., timestamp configurations, logs, operating systems, etc.) for compliance reporting.

□ Configure reporting templates to align with Component requirements, including the required data fields and formats.

Integrate tools where applicable:

□ Ensure tool interoperability across multiple systems within the Component.

Verify and validate the Component capability for compliance reporting in alignment with Enterprise standards.

Maintain Enterprise compliance through continuous monitoring, reporting, and asset management:

□ Ensure all devices meeting minimum compliance and integration requirements are enrolled in a Component-wide asset management system capable of tracking configuration, compliance posture, and lifecycle data.

□ Document and maintain a plan for enrolling remaining devices as they achieve required compliance and integration readiness.

□ Regularly review and apply Enterprise standards and requirements for continuous monitoring and reporting, ensuring all systems meet or exceed baseline expectations.

□ Monitor device compliance (e.g., patch levels, software inventory, security configurations, etc.) to verify and validate ongoing adherence to policy requirements.

□ Routinely confirm that all systems and devices maintain valid Authorizations to Operate (ATOs) and operate within approved security parameters.

Generate compliance reports and submit reports to the appropriate authorities:

□ Conduct functional testing to ensure operational compliance reporting meets Enterprise guidance and requirements.

□ Generate and submit required compliance reports to the Enterprise, ensuring visibility and accountability for all managed assets utilizing the asset management solution [6].

☐ Review reports for accuracy and completeness.

☐ Confirm that the Enterprise received the compliance reports and gather feedback on the reporting process.

Verify and validate ZT Target-level functionalities.

Verify and validate Enterprise compliance requirements:

☐ Leverage and review Enterprise regulatory guidance and documentation that identifies critical ZT Target functionalities and minimum requirements necessary for compliance.

☐ Conduct functional testing to ensure minimum compliance requirements are met.

☐ Conduct security testing to identify and mitigate any vulnerabilities in the compliance validation process.

☐ Verify and validate the hardware, software, and services of physical and virtual platforms are managed in compliance with the Component's risk strategy (e.g., Comply-to-Connect (C2C), etc.) [19].

☐ Verify and validate that log records are generated and made available for continuous monitoring [19].

Summary

This diagram outlines the Activity 2.6.1 (Phase One) – *Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of device compliance and asset management through a Unified Endpoint and Device Management (UEDM) solution. It presents strategic insights that drive implementation and expected outcomes, including programmatically managed asset compliance.

Table 37: Activity 2.6.1 — Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How is the Unified Endpoint Management (UEM) solution implemented to ensure critical ZT functionalities such as minimum compliance and asset management?
2. How are asset management systems for User/Person Entity (PE) devices maintained to report Information Technology (IT) compliance?
3. How does the UEM solution support Application Programming Interface (API) integration for device compliance status?

STRATEGIC INSIGHTS

- The Component defines and documents policies and procedures for selecting and implementing a UEDM solution that integrates asset, vulnerability, and patch management capabilities in accordance with Enterprise guidance and ZT requirements.
- The Component demonstrates compliance by deploying UEDM tools that discover, inventory, and continuously monitor endpoints, integrating with vulnerability scanners, patch management systems, and asset management solutions to ensure the integrity, currency, and protection of hardware and software.
- The Component provides evidence that data exchange between solutions (e.g., via APIs, etc.) is secure, with authenticated and encrypted channels protecting data at rest, in transit, and in use, maintaining Confidentiality, Integrity, and Availability (CIA) and adhering to backup, logging, and auditing mandates.
- The Component ensures that continuous monitoring and reporting are in place, leveraging real-time visibility into endpoint configurations, anomalies, and compliance checks. It also ensures that alerts and event logs are fed into Security Information and Event Management (SIEM) and other security platforms for timely detection and response.
- The Component verifies and validates that the chosen UEDM solutions meet critical ZT target functionalities (e.g., minimum compliance levels, asset management, API support, etc.) and regularly audits, refines, and updates these tools, documenting lessons learned and maintaining resilient, policy-aligned cybersecurity operations.

✓ EXPECTED OUTCOMES

1. Components can confirm if devices meet minimum compliance standards or not.

2. Components have asset management system(s) for user devices (phones, desktops, laptops) that maintains IT compliance, which is reported up to DoW Enterprise.

3. Components asset management systems can programmatically (i.e., API) provide device compliance status and if it meets minimum standards.

Activity 2.6.2 Enterprise Device Management (EDM) Part 1

Table 38: Activity 2.6.2 — Enterprise Device Management (EDM) 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 sets standards and policies for Enterprise Device Management (EDM). Components migrate the manual device inventory to an automated approach using an EDM solution. Approved devices are able to be managed regardless of location. Devices part of critical services are managed by the EDM solution supporting automation.	
Predecessor(s)	**Successor(s)**
None	2.1.2, 2.6.3, 3.4.1
Expected Outcomes	
• Enterprise sets standards and policies for EDM. • Components manual inventory is integrated with an automated management solution for critical services. • Components enable ZT device management (from any location with or without remote access). • Where applicable, ensure tracking of NPEs in the UEM solution.	
End State	
Implementing consistent and well-defined processes and controls for managing devices.	

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 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, as a complete device inventory is needed in order to select and implement an Enterprise Device Management (EDM) solution.
- If Activity 2.6.1 (Phase One) – *Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools* has been completed prior to this activity, then ensure that the Component aligns actions within this activity with previous device management actions.
- EDM policies should consider including guidelines for data collection and how the data is stored, used, shared, and/or destroyed in compliance with relevant privacy regulations and data protection policies.
- Cross-platform support should be implemented for managed devices across multiple operating systems. Consider the level of management and security features available for each platform.

- Centralized management should provide a single console for managing all devices including capabilities for policy deployment, software distribution, patch management, and security monitoring.
- Security compliance ensures all devices meet security standards and policies.
- Remote support and control provide Information Technology (IT) teams troubleshooting and remote management of devices.
- Activity 2.1.2 (Phase One) – *Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management*, Activity 2.6.3 (Phase Two) – *Enterprise Device Management (EDM) Part 2*, and Activity 3.4.1 (Phase One) – *Resource Authorization 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 39: Implementation Tasks for Activity 2.6.2 — Enterprise Device Management (EDM) Part 1

Obtain Enterprise EDM standards and policies and develop an EDM integration plan.
Develop a comprehensive EDM integration plan: ☐ Review current Enterprise-level policies and procedures related to data management, including data standards, metadata management, data quality, data sharing, and security/privacy requirements. ☐ Define technical and operational requirements needed to integrate EDM into Component systems, including: • Data exchange standards (e.g., Application Programming Interfaces (APIs), data models) • Metadata tagging and cataloging processes • Data lineage and auditability expectations • Role-Based Access Controls (RBACs) and data ownership models ☐ Identify where existing policies fall short in supporting EDM integration (e.g., lack of interoperability standards, insufficient metadata requirements, etc.) and recommend updates or new policy development. ☐ Outline phased steps for EDM integration, including key milestones, responsible stakeholders, data systems in scope, and timelines.

Obtain and review inventory:

☐ Review and utilize the current manual device inventory system and Component Master Device Inventory, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis.*

Deploy an EDM solution based on the integration plan:

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

Migrate the manual device inventory to an automated process using the EDM solution, where applicable.

Develop migration plan:

☐ Develop a strategy for migrating the manual device inventory to an automated process using the EDM solution.

Prepare manual inventory data:

☐ Consolidate manual inventory data from all sources into a standardized format and clearly document the data fields and their meaning [6].

☐ Compare the manual inventory data against other data sources (e.g., Active Directory, network scans, etc.). Manually verify a sample of devices to ensure accuracy. Address any discrepancies or missing information before proceeding with the migration [20].

Confirm configuration of the EDM solution:

☐ Configure the EDM solution to support various enrollment methods (e.g., self-service enrollment, automated enrollment, and bulk enrollment). Configure device management policies and security baselines.

☐ Configure the inventory settings to collect the required data fields and update frequency.

☐ Configure the EDM solution to log all data input and changes to the device inventory. Enable audit logging to track user actions and system events.

Import manual inventory data:

☐ Import the verified and validated manual inventory data into the EDM solution using the EDM import options.

☐ Map and document the data fields from the manual inventory to the corresponding fields in the EDM solution to ensure data integrity and consistency.

☐ Verify the imported device inventory in the EDM by comparing it to the original manual inventory, resolving any discrepancies before proceeding.

Enable ZT device management on all devices, regardless of physical or virtual location.

Establish requirements:

☐ Determine which EDM features will be used for ZT device management (e.g., device posture checks, compliance enforcement, conditional access, etc.).

☐ Define the scope of device management (e.g., devices, operating systems, locations, etc.).

☐ Outline the integration with other security tools, such as:

- Identity Provider (IdP), from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)* and Activity 1.9.1 (Phase Two) – *Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) Part 1*.
- Comply-to-Connect (C2C), from Activity 2.2.1 (Phase Two) – *Implement Comply-to-Connect (C2C) and Compliance-Based Network Authorization Part 1*.
- Proxy Enforcement Points, from Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation*.

☐ Define the requirements for supporting ZT principles managing devices with and without remote access:

- Strong device authentication
- Device health checks
- Data encryption
- Least Privilege access control

☐ Develop and document a remote access plan for accessing systems through approved managed access points.

Configure device management solution:

☐ Configure the EDM solution to enroll and manage all devices, regardless of the device procurement and/or location.

☐ Ensure all remote access to systems is routed through designated access control points that are explicitly approved by the Component, centrally managed, and configured to enforce security policies (e.g., Virtual Private Network (VPN) gateways, secure jump servers, or ZT Network Access solutions) [20].

☐ Integrate the EDM with Network Access Control (NAC) solutions to enforce device registration before granting network access.

☐ Implement security policies and Enterprise compliance requirements within the EDM solution.

☐ Leverage 3rd party device management solutions to monitor and enforce policies, regardless of the device's physical location, as needed [6].

☐ Configure the EDM to assign unique device identities and use these identities for authentication and authorization purposes.

Enable tracking of Non-Person Entities (NPEs) within the EDM solution.

Establish device management requirements:

☐ Define the requirements for identifying, inventorying, and managing devices running NPEs within the EDM solution. Requirements should include the ability to:

- Automatically discover and identify NPE devices on the network.
- Assign unique identifiers to NPEs.

- Track NPE attributes (e.g., device type, operating system, location, etc.).
- Monitor NPE activity.
- Enforce security policies and compliance checks on NPEs.

Validate EDM solution capabilities:

☐ Verify and validate the EDM solution provides comprehensive NPE management, monitoring, and compliance capabilities.

Develop an EDM implementation plan:

☐ Develop a strategy for enabling tracking of NPEs within the EDM solution:

- Define the scope of NPE tracking.
- Determine how NPEs will be identified and inventoried.
- Outline the integration with other security solutions.
- Define device enrollment policies with device tagging [20].
- Create a Least Privileged device baseline [6].
- Develop a timeline and resource plan for implementation.

☐ Use a consistent device tagging strategy and leverage tags to categorize and manage NPEs based on their function, location, or criticality.

Implement continuous monitoring and automation:

☐ Schedule continuous monitoring to track devices running NPEs (e.g., network activity, system logs, security events, etc.) [6].

☐ Continuously verify that NPEs maintain compliance with security policies and have appropriate access rights [6].

☐ Integrate the EDM solution with IT Service Management (ITSM) systems to automate change requests, incident management, and problem resolution for NPEs [6].

☐ Implement automation to streamline processes such as device enrollment, inventory updates, and compliance checks.

Test, monitor, and audit NPE solutions.

Test, verify, and validate:

☐ Verify and validate the NPEs' capability to authenticate and access resources as required.

☐ Verify and validate secure communications.

☐ Perform security testing to identify and mitigate any vulnerabilities found during the automation implementation of critical services and associated devices processes [20].

Monitor and audit:

☐ Monitor the NPE tracking solution to ensure its security and performance.

☐ Conduct regular audits to verify compliance with security requirements to identify and respond to any potential issues [20].

☐ Automate security assessments for NPEs, including vulnerability scans, compliance checks, and actions like quarantining or blocking threats [6].

☐ Enforce and document audit logs utilizing audit logging tools [20].

Summary

This diagram outlines the Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of device inventory and management integration with a Unified Endpoint and Device Management (UEDM) solution for critical services. It presents strategic insights that drive implementation and expected outcomes, including the integration of manual inventory with an automated management solution based on Enterprise standards.

Table 40: Activity 2.6.2 — Enterprise Device Management (EDM) Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the manual device inventory integrated with the Unified Endpoint Management (UEM) solution for critical services? 2. How is ZT device management enabled for devices with and without remote access?

STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for UEDM solutions that align with Enterprise standards, ensuring compliance with Enterprise requirements. • The Component demonstrates compliance by selecting and implementing UEM solutions to automate device inventory, management, and compliance, migrating from manual processes to an automated, policy-driven framework that continuously monitors health, configurations, and security status of devices for critical services. • The Component provides evidence that critical services, endpoints, and Non-Person Entities (NPEs) are enrolled and managed within the UEM solution under ZT principles, enabling device identification, granular access controls, and risk-based enforcement—regardless of physical location—and integrating with broader Enterprise security architectures and tools. • The Component ensures that the UEM solution supports continuous monitoring, automation, secure data sharing, and compliance checks for all managed devices, employing role-based and time-based access controls, Multi-Factor Authentication (MFA), and encryption to safeguard sensitive resources and maintain the confidentiality, integrity, and availability of device-related information. • The Component regularly audits and updates the Enterprise Data Management (EDM) and UEM processes, verifying and validating that inventory data is accurate, security policies remain aligned with Enterprise requirements, and the EDM solution effectively detects anomalies, enforces policy compliance, and mitigates risks to critical Component assets.

✓ EXPECTED OUTCOMES

1. Enterprise sets standards and policies for EDM.
2. Components manual inventory is integrated with an automated management solution for critical services.
3. Components enable ZT device management (from any location with or without remote access).
4. Where applicable, ensure tracking of NPEs in the UEM solution.

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

Table 41: 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 2.7.1 Implement Endpoint Detection and Response (EDR) Tools and Integrate with Comply-to-Connect (C2C)

Table 42: Activity 2.7.1 — Implement Endpoint Detection and Response (EDR) Tools and Integrate with Comply-to-Connect (C2C)

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 Endpoint Detection and Response (EDR) solution(s) within environments. EDR is protecting, monitoring, and responding to malicious and anomalous activities enabling ZT Target-level functionality and is sending data to the Comply-to-Connect (C2C) solution for expanded device and user checks.	
Predecessor(s)	**Successor(s)**
2.3.4	2.7.2
Expected Outcomes	
• EDR tooling is implemented. • Critical EDR data is being sent to C2C for checks. • Endpoint Protection Platform (EPP) tooling covers the maximum amount of services/applications.	
End State	
Detect advanced threats that are undetectable by a traditional antivirus program, optimizing the response time of incidents, discarding false positives, implement blocking, and protect against multiple threats happening simultaneously across various threat vectors.	

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 2.3.4 (Discovery) – *Integrate Next-Generation Antivirus (NextGen AV) Tools with Comply-to-Connect (C2C)* 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 obtain an accurate device inventory list.
- Endpoints are physical devices that connect to and exchange information with a computer network (e.g., mobile devices, desktop computers, virtual machines, embedded devices, Internet of Things (IoT) devices, servers, etc.).
- Endpoint Detection Response (EDR) is a fundamental element of an Endpoint Protection Platform (EPP).

- EDR gives security teams the visibility and automation needed to improve Incident Response (IR) and prevent attacks on endpoints from spreading.
- Evaluate agent-based, agentless, or hybrid EDR deployment models based on system requirements.
- Assess whether a single EDR solution or multiple EDR solutions are required to meet the Component's needs.
- Verify and validate that the EDR solution(s) can provide logs with enough data for the Security Information and Event Management (SIEM)/Security Orchestration, Automation, and Response (SOAR) and Artificial Intelligence (AI)/Machine Learning (ML) to utilize, where applicable.
- Verify and validate that the EDR solution(s) can integrate with the Privileged Access Management (PAM), Identity Provider (IdP), SIEM, and SOAR.
- Assess EDR performance limits, considering the potential volume of signatures and behavioral patterns within the environment.
- Identify EDR exceptions to allow for functionality that balances exceptions between security and usability while meeting the overall cybersecurity goals.
- Activity 2.7.2 (Phase Two) – *Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) 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 43: Implementation Tasks for Activity 2.7.1 — Implement Endpoint Detection and Response (EDR) Tools and Integrate with Comply-to-Connect (C2C)

Identify endpoints for implementing an EDR solution.
Review existing device inventory: ☐ Leverage approved asset inventory, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis*. ☐ Verify and validate against the Configuration Management Database (CMDB) and asset management systems for accuracy.

☐ Update the Configuration Item Baseline (CIB) as required. ☐ Identify unsupported legacy systems that may require compensating controls. ☐ Identify how EDR will integrate with existing Component-defined IR policies and procedures. Identify which EDR metrics will be used to identify incidents.
Implement EDR across all identified endpoints.
Leverage existing EPP integration: ☐ Leverage the Component-selected EPP solution, from Activity 2.3.4 (Discovery) – *Integrate Next-Generation Antivirus (NextGen AV) Tools with Comply-to-Connect (C2C).* ☐ Confirm the EDR is a fundamental component of the EPP solution, which, when integrated together, enables a robust, comprehensive endpoint security strategy. ☐ Verify and validate that the selected EDR solution integrates seamlessly with the existing EPP framework. ☐ Ensure endpoint configurations adhere to Enterprise security baselines. ☐ Document all verification and validation processes, including rollback and recovery procedures. ☐ Monitor the EDR solutions for incidents and IRs in accordance with the Component IR policies.
Verify and validate EDR solution(s), monitor, protect, and respond to malicious and anomalous activities (e.g., antivirus, antimalware, blocking, protection measures, etc.).
Verify and validate EDR monitoring capabilities: ☐ Confirm real-time monitoring of endpoints for malware, ransomware, unapproved access, and behavioral anomalies. ☐ Test EDR response capabilities, including automatic quarantine, process termination, and alert generation. ☐ Verify and validate the integration of antivirus and anti-malware capabilities within the EDR solution. ☐ Conduct simulation exercises (e.g., malware injection tests, etc.) to confirm effective detection and response functionality. ☐ Review logs and alerts to verify and validate accuracy and completeness.
Configure EDR to transmit critical data to the C2C solution(s) for enhanced device and User/Person Entity (PE) checks.
Confirm EDR to C2C configuration: ☐ Ensure critical telemetry data points (e.g., process creation, file access, etc.) for transmission have been identified. ☐ Verify and validate secure communication channels (e.g., encrypted Application Programming Interface (API) calls, etc.) between EDR and C2C platforms have been established. ☐ Confirm EDR is configured to forward relevant logs and alerts to the C2C solution in real-time.

☐ Verify and validate that EDR data fields have been mapped to corresponding C2C analytics requirements for consistency. ☐ Ensure the implementation of data normalization and enrichment processes for C2C correlation has transpired. ☐ Test, verify, and validate data transmission integrity and consistency across all integrated endpoints.
Verify and validate that C2C is receiving critical data from the EDR.
Confirm C2C receipt of critical data from the EDR: ☐ Conduct end-to-end verification and validation to ensure C2C systems ingest EDR telemetry without data loss and with original data integrity. ☐ Verify and validate that C2C accurately reflects endpoint health and security posture. ☐ Perform correlation tests to ensure EDR data enhances the C2C ability to detect complex threats. ☐ Simulate endpoint security incidents and verify and validate the C2C triggers appropriate security workflow and response. ☐ Monitor data transmission latency and resolve performance bottlenecks. ☐ Establish continuous monitoring and alerting on data ingestion failures.
Verify and validate that the EPP solution covers the broadest range of services and applications, where possible.
Assess and validate the EPP solution: ☐ Assess EPP coverage across all Enterprise applications and services. ☐ Verify and validate compatibility with various operating systems, virtual environments, and mobile platforms. ☐ Test EPP effectiveness against diverse threat vector exploits (e.g., phishing, web-based attacks, zero-day threats, advanced persistent threats, etc.). ☐ Verify and validate that EPP integrates seamlessly with EDR and C2C platforms. ☐ Review vendor updates and threat intelligence feeds regularly to ensure comprehensive protection. ☐ Conduct periodic assessments and penetration tests to validate EPP resilience.

Summary

This diagram outlines the Activity 2.7.1 (Phase One) – *Implement Endpoint Detection and Response (EDR) Tools and Integrate with C2C* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of an Endpoint Detection and Response (EDR) solution to monitor, detect, and remediate malicious activity within endpoints. It presents strategic insights that drive implementation and expected outcomes, including EDR tooling, where critical data is sent to Comply-to-Connect (C2C) for verification and validation.

Table 44: Activity 2.7.1 — Implement Endpoint Detection and Response (EDR) Tools and Integrate with Comply-to-Connect (C2C) - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the EDR solution implemented to monitor, detect, and remediate malicious activity on endpoints? 2. How is critical EDR data sent to C2C for checks?

STRATEGIC INSIGHTS
• The Component defines and documents policies and procedures for identifying all relevant endpoints (e.g., workstations, mobile devices, servers, Internet of Things (IoT), cloud, and edge environments, etc.) that require EDR coverage, ensuring alignment with Enterprise security guidelines and ZT principles. • The Component demonstrates compliance by deploying EDR solutions across maximum amount of identified endpoints, performing pilot tests, tuning configurations, and continuously monitoring for malicious and anomalous activities, ensuring that EDR capabilities (e.g., antivirus, anti-malware, threat hunting, etc.) meet established performance and security requirements. • The Component provides evidence that the EDR solution integrates with C2C solutions, transmitting critical endpoint data in real-time via secure Application Programming Interfaces (APIs), enabling enhanced device posture checks, automated alerts, and improved Incident Response (IR) capabilities. • The Component verifies and validates that the C2C platform receives, logs, and appropriately responds to critical EDR alerts and events, tests data flows, performs regular audits, and ensures that compliance and enforcement rules are effectively automated and maintained. • The Component confirms that Endpoint Protection Platform (EPP) tools provide comprehensive security coverage (e.g., antivirus, data encryption, data loss prevention, etc.) for all services, applications, and endpoints, supporting ZT strategies by protecting assets outside the traditional network perimeter and maintaining continuous visibility of the security posture.

EXPECTED OUTCOMES

1. EDR tooling is implemented.
2. Critical EDR data is being sent to C2C for checks.
3. EPP tooling covers the maximum amount of services/applications.

Application and Workload Pillar

Capability 3.2 Secure Software Development and Integration

Table 45: Capability 3.2 — Secure Software Development 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	3.2 - Secure Software Development and Integration
Description	
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.	
Impact to ZT	
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.	

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
- Infrastructure as Code (IaC) Configuration Management/Security Monitoring and Auditing
- Static Application Security Testing (SAST)
- Dynamic Application Security Testing

Activity 3.2.1 Build Development, Security, and Operations (DevSecOps) Software Factory Part 1

Table 46: Activity 3.2.1 — Build Development, Security, and Operations (DevSecOps) Software Factory 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 provide best practices for modern DevSecOps processes and CI/CD pipelines. The concepts are applied in a standardized technology stack across Components able to meet future Application Security requirements, including requirements gathering, design, development, testing and deployment.	
Predecessor(s)	**Successor(s)**
None	3.2.2, 3.2.3
Expected Outcomes	
• Developed security best practices for DevSecOps and CI/CD pipelines. • Vulnerability management is integrated into CI/CD pipelines.	
End State	
Implementing consistent and well-defined processes and controls for DevSecOps.	

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.

- Enterprise has provided best practices for modern Development, Security, and Operations (DevSecOps) processes and Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines.
- Activity 3.2.2 (Phase One) – *Build Development, Security, Operations (DevSecOps) Software Factory Part 2* and Activity 3.2.3 (Phase Two) – *Automate Application Security and Code Remediation Part 1* are 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 47: Implementation Tasks for Activity 3.2.1 — Build Development, Security, and Operations (DevSecOps) Software Factory Part 1

Obtain DevSecOps best practice processes and CI/CD pipelines.
Review recommended DevSecOps best practice architecture to include CI/CD pipelines: ☐ Adopt guidance on how specific collections of technologies form a secure and effective DevSecOps platform for building software [21]. ☐ Leverage Software as a Service (SaaS) deployment and Infrastructure as Code (IaC) to quickly and securely establish a DevSecOps environment where development tools are separated from testing and production deployments [21]. **Establish Component-level DevSecOps policy and processes aligned with mission specifics:** ☐ Leverage the advanced and highly scalable programmable infrastructure provided by an approved Cloud Service Provider (CSP) while considering potential vendor lock-in when selecting and deploying services. ☐ Explore existing programs, such as the Defense Information Systems Agency (DISA) Hosting and Computer Center (HaCC), for secure cloud service templating and the ability to preserve security controls when pursuing Authorization to Operate (ATO) [21]. ☐ Communicate and ensure that security requirements for software development are shared and known by all stakeholders, including third-party partners providing commercial and customized software components [22].
Implement Enterprise DevSecOps best practices and CI/CD pipelines to ensure compliance with application security requirements (e.g., requirement gathering, design/development, testing, deployment, etc.).
Assemble cross-functional teams to execute a DevSecOps strategy: ☐ Define goals and objectives in establishing a DevSecOps program, such as: • Build secure, agile applications. • Reduce mean time to production. • Improve mean time to recovery. • Automate risk and threat modeling. • Create an immutable platform, such as a logical container that prevents modification after instantiation. ☐ Promote and adopt a DevSecOps culture where self-organized teams break down silos and unify software development, deployment, security, and operations through the adoption of an automated CI/CD pipeline [23]. **Build standardized playbooks:** ☐ Assess the current security posture in accordance with the Enterprise/Component requirements. ☐ Adopt continuous knowledge sharing. ☐ Enable software built-in security.

☐ Leverage secure open source.

☐ Implement approved automated toolchains to reduce human effort and improve security practices' accuracy, reproducibility, usability, and comprehensiveness throughout the Software Development Lifecycle (SDLC) [22].

Automate approved deployments:

☐ Enforce secure, mandatory code signing.

☐ Automate all repeatable tasks.

☐ Adopt CI.

☐ Adopt CD.

☐ Enable security testing automation.

☐ Integrate security into the CI/CD pipeline.

Enable continuous Specific, Measurable, Achievable, Relevant, and Time-bound (SMART) performance metrics: [24]

☐ Continuously develop technical expertise to advance DevSecOps adoption and improvement.

☐ Adopt a capability model, **not** a maturity model, leveraging tempo metrics (e.g., deployment frequency, change lead time, etc.) and stability metrics (e.g., mean time to recovery, change failure rate, etc.) [24].

☐ Establish a software factory model through the adoption of the known four (4) key Phases: [24]

- Design
- Instantiate
- Verify and validate
- Operate and monitor

☐ Adopt containerized microservices.

☐ Persistently strive for built-in cyber resilience—the ability to anticipate, withstand, recover from, and adapt to adverse threat conditions—while ensuring the confidentiality, integrity, and availability of essential key mission requirements remain secure [24].

Implement a vulnerability management program integrated with the CI/CD pipeline.

Assess security and select vulnerability testing methodologies:

☐ Define criteria for software security checks and enable tracking throughout the SDLC [22].

☐ Adopt and implement a range of software security testing methodologies to include:

- Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST)
- Software Composition Analysis (SCA)
- Container security scanning
- IaC scanning

- Runtime Application Self-Protection (RASP)
- Cybersecurity testing and evaluation

Integrate vulnerability scanning into the CI/CD pipeline:

☐ Incorporate multiple security checks at each stage of the CI/CD pipeline (e.g., build, test, deploy, etc.).

☐ Conduct early and frequent testing and evaluation to rapidly adapt to change and ensure safe failure mechanisms for critical vulnerabilities.

Prioritize, report, and remediate:

☐ Establish a straightforward process for triaging and prioritizing critical, high-value vulnerabilities based on severity, mission impact, and exploitability.

☐ Develop built-in feedback loops to streamline the remediation process. Conduct early and frequent scanning and share reports with developers, quality assurance testers, and the teams for quick intervention.

Summary

This diagram outlines the Activity 3.2.1 (Phase One) – *Build Development, Security, and Operations (DevSecOps) Software Factory Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the creation and implementation of foundational standards for Development, Security, and Operations (DevSecOps) processes and Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines. It presents strategic insights that drive implementation and expected outcomes, including the integration of best practices for DevSecOps and CI/CD pipelines.

Table 48: Activity 3.2.1 — Build Development, Security, and Operations (DevSecOps) Software Factory Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are foundational standards for DevSecOps processes and CI/CD pipelines created and implemented? 2. How is the Enterprise-wide Vulnerability Management program integrated with the CI/CD pipeline?

STRATEGIC INSIGHTS
• The Component defines a comprehensive DevSecOps strategy by adopting industry best practices, integrating CI/CD pipelines, and aligning development, security, and operations to ensure secure and efficient software delivery. • The Component demonstrates security and operational excellence by automating deployments, enforcing secure coding practices, implementing built-in security controls, and integrating vulnerability management throughout the Software Development Lifecycle (SDLC). • The Component provides verifiable enforcement through automated security testing, containerized micro-services, and continuous monitoring, ensuring software resilience, compliance, and adaptability to evolving threats. • The Component leverages Infrastructure as Code (IaC), secure open-source frameworks, and automated toolchains to enhance security posture, improve deployment efficiency, and reduce human error across the development process. • The Component ensures continuous improvement by adopting Specific, Measurable, Achievable, Relevant, and Time-bound (SMART) performance metrics, integrating cybersecurity testing into CI/CD pipelines, and fostering a DevSecOps culture that prioritizes resilience, automation, and proactive threat mitigation.

EXPECTED OUTCOMES
1. Developed security best practices for DevSecOps and CI/CD pipelines. 2. Vulnerability management is integrated into CI/CD pipelines.

Activity 3.2.2 Build Development, Security, and Operations (DevSecOps) Software Factory Part 2

Table 49: Activity 3.2.2 — Build Development, Security, and Operations (DevSecOps) Software Factory 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 use their approved CI/CD pipelines to develop most new applications. Any exceptions will follow a standardized approval process to be allowed to develop in a legacy fashion. DevSecOps processes are also used to develop all new applications and update existing applications. Continual validation functions are integrated into the CI/CD pipelines and DevSecOps processes and integrated with existing applications.	
Predecessor(s)	**Successor(s)**
3.2.1	3.5.1
Expected Outcomes	
• Implement Component CI/CD pipeline(s) and Software Factory per the DoW CIO DevSecOps Instruction/Directive. • Application development adopts the use of CI/CD pipelines. • Continual validation process/technology is implemented and in use (see "Continual Validation" activity). • Application development adopts the use of the DevSecOps process and technology.	
End State	
Ensure code changes and updates are secure and compliant, reducing risk of an exploit.	

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 3.2.1 (Phase One) – *Build Development, Security, and Operations (DevSecOps) Software Factory Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- The Enterprise has provided a standardized approach for code-based compute management.
- Review Enterprise-defined requirements on Development, Security, and Operations (DevSecOps).
- Explore Artificial Intelligence (AI) modeling for advanced and continuous testing and evaluation.
- Activity 3.5.1 (Phase Three) – *Continuous Authorization to Operate (cATO) 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 50: Implementation Tasks for Activity 3.2.2 — Build Development, Security, and Operations (DevSecOps) Software Factory Part 2

Leverage the Enterprise requirements on DevSecOps strategy.
Review the Enterprise Directives on DevSecOps and software modernization strategy: ☐ Leverage Enterprise policy and guidance. **Develop a Component-level DevSecOps program to streamline the software modernization strategy:** ☐ Establish different process workflows essential for a secure Software Development Lifecycle (SDLC) to align with specific mission constraints, such as: • System complexity • Architecture model • Technical requirements • Risk tolerance level • Service level agreement • User/Person Entity (PE) experience ☐ Leverage the cloud Infrastructure as Code (IaC) reference design to build secure native cloud infrastructure for the DevSecOps environment [21]. ☐ Establish a version-controlled, Component-wide DevSecOps governance based on Enterprise guiding principles, evolving toward a stringent, continuous security posture improvement.
Establish a software factory.
Build and deliver a resilient software capability at the speed of relevance [25]: ☐ Leverage the Enterprise's DevSecOps Managed Service Provider (MSP) to design, build, and establish an approved DevSecOps software factory platform with multi-tenancy capabilities. ☐ Assess and upgrade the existing infrastructure and technology stack to ensure compliance with DevSecOps toolchains, Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) platforms, microservice architecture, and emerging automation toolkits. ☐ Adopt a multitude of CI/CD pipelines to build resilient, distinct, and standardized structures for source code with specific tools, workflows, scripts, environments, and a set of automated tasks to achieve CI and delivery of new applications [24].

Adopt standardized design patterns:

☐ Develop a consistent, fixed infrastructure by adopting automated and standardized design patterns using templating and IaC-type deployment.

☐ Build modular software components, loosely coupled, for enhanced agility and scalability.

☐ Leverage Application Programming Interface (API) for seamless integration and interoperability compliance.

Leverage Enterprise-approved Cloud Service Provider (CSP) programmable infrastructure:

☐ Explore and leverage the extensive resources of approved commercial CSPs to develop secure native cloud applications.

☐ Integrate Software as a Service (SaaS)-managed service capabilities with on-premises infrastructure deployment to build DevSecOps platforms, CI/CD pipelines, and automation toolchains at different information impact levels [21].

Enforce mandatory code signing and repository-privileged access control:

☐ Implement security policies throughout the software factory by enforcing secure code signing to protect the repository source code, data, and the infrastructure platform.

☐ Leverage Policy Enforcement Point (PEP) and Policy Decision Point (PDP) throughout all Phases of the SDLC to regulate and restrict resource access to only approved Users/PEs/Non-Person Entities (NPEs).

Develop CI/CD pipelines within DevSecOps environments.

Maintain and keep CI/CD tools up to date:

☐ Avoid Poisoned Pipeline Execution (PPE) by implementing two (2)-person rules for all code and tool updates.

☐ Implement Least Privilege policies for CI/CD access by enabling CI/CD Pipeline-Based Access Controls [26].

Enforce Enterprise-approved cryptography:

☐ Leverage the industry standards and/or recommendations, such as Federal Information Processing Standards (FIPS) 140-3 approved cryptographic modules, to implement and configure a robust cryptographic algorithm to protect data, protect secret keys generated across the CI/CD pipelines, and secure the API ecosystem [26].

☐ Implement granular segmentation and traffic filtering.

☐ Implement workload-based management throughout the SDLC by leveraging micro-segmentation to achieve application-level segmentation that extends beyond the traditional Transport Layer Four and reaches to Application Layer Seven.

☐ Apply the ZT principle of “deny all by default” to reduce the attack surface further and restrict privilege escalation and lateral movement.

Adopt secure accounts, Least Privilege, and separation of duties:

☐ Automate security as code and configuration as code to enforce access control policies, version control, automated testing, and integrate User and Entity Behavior Analytics (UEBA).

Enforce whitelisting for libraries and CI/CD tools:

☐ Define the most comprehensive criteria for the whitelisting policy to continuously verify and validate the integrity of CI/CD tools and components by enforcing whitelisting for CI/CD libraries and tools. Consider key features such as:

- Reputation
- Licensing
- Security bulletin
- Accreditation
- Latest Common Vulnerabilities and Exposures (CVEs)

Implement continuous Operational Test and Evaluation (OT&E).

Integrate Testing and Evaluation (T&E) goals at the program's inception to influence requirements, Request for Proposals (RFPs), and acquisitions:

☐ Enable secure and rapid software deployment without compromising T&E processes by automating the capture and analysis of relevant metrics that best reflect functional and non-functional software requirements [24].

☐ Encourage continuous upskilling to maintain a broader competency pool of technical talent capable of successfully developing and testing software, DevSecOps platforms, and CI/CD pipelines.

☐ Integrate ZT principles throughout the SDLC to support Cyber Survivability Endorsement (CSE) for specific applications, data, and infrastructure [27].

Promote zero-day vulnerability programs:

☐ Promote a culture of transparency, where collaborative teams of researchers and partners can legally, ethically, and securely test and share findings of the latest potential exploits and vulnerabilities to help strengthen the security posture of developed software applications.

Implement continuous improvement:

☐ Monitor Key Performance Indicators (KPIs) and security metrics to track the latest vulnerability releases and emerging threats.

☐ Enable dashboard alerting to monitor vulnerability count, remediation time, and scan coverage.

Summary

This diagram outlines the Activity 3.2.2 (Phase One) – *Build Development, Security, and Operations (DevSecOps) Software Factory Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of application migration and continual verification and validation technology into the Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipeline. It presents strategic insights that drive implementation and expected outcomes, including the adoption of the Development, Security, and Operations (DevSecOps) process and technologies.

Table 51: Activity 3.2.2 — Build Development, Security, and Operations (DevSecOps) Software Factory Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the development of applications migrated to the CI/CD pipeline? 2. How is continual validation technology implemented in the CI/CD pipeline?

STRATEGIC INSIGHTS
• The Component defines a DevSecOps strategy by aligning with Enterprise policies, establishing secure software development workflows, and integrating cloud-native infrastructure. • The Component demonstrates compliance by building a standardized software factory, enforcing CI/CD security controls, and adopting modular design patterns to ensure interoperability and resilience. • The Component provides evidence through mandatory code signing, repository access controls, and workload-based segmentation, applying ZT principles to reduce risks and enforce the principle of Least Privilege. • The Component leverages cryptographic security, automation, and continuous testing to enhance software integrity, detect vulnerabilities, and ensure compliance with Enterprise cybersecurity standards. • The Component ensures ongoing security through continuous operational testing, monitoring Key Performance Indicators (KPIs), tracking emerging threats, and fostering a zero-day vulnerability program to strengthen software resilience.

EXPECTED OUTCOMES
1. Implement Component CI/CD pipeline(s) and Software Factory per the DoW CIO DevSecOps Instruction/Directive. 2. Application development adopts the use of CI/CD pipelines. 3. Continual validation process/technology is implemented and in use (see "Continual Validation" activity). 4. Application development adopts the use of the DevSecOps process and technology.

Capability 3.3 Software Risk Management

Table 52: 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 3.3.1 Approved Binaries and Code

Table 53: Activity 3.3.1 — Approved Binaries and Code

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 uses best practices to manage approved binaries and code in a methodical approach, including supplier sourcing risk management, approved repository usage, Software Bill of Materials (SBOM), supply chain risk management, and industry-standard vulnerability management.	
Predecessor(s)	**Successor(s)**
3.3.2	None
Expected Outcomes	
• Supplier sourcing risk evaluated and identified for approved sources. • Repository and update channel established for use by development teams. • SBOMs are created for applications to identify source, supportability, and risk posture. • Defense Industry Base (DIB) standards and approved vulnerability databases are pulled in to be used in DevSecOps.	
End State	
Safeguard the creation, storage, and delivery of code.	

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.
- Consider completing Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)* prior to this activity, to implement strong encryption and version control.
- The Enterprise has provided a standardized approach for code-based compute management.
- Cloud Service Provider (CSP) native services offerings.
- Include Artificial Intelligence (AI) model development in the security requirements for software development infrastructure and processes [22].
- Code integrity as an authorization gate [28].
- Supply Chain Risk Management (SCRM).

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 54: Implementation Tasks for Activity 3.3.1 — Approved Binaries and Code

Leverage the Enterprise standards and requirements on software modernization and approval requirements.
Develop Component-level, secure source code policy in accordance with Enterprise requirements: ☐ Identify and document all Enterprise software development infrastructure and processes security requirements. Update and maintain the requirements over time to ensure continuous compliance [29]. ☐ Establish clear and comprehensive binary code security policies across all development teams, infrastructures, third-party software suppliers, and internal software factories. ☐ Implement environment security around the infrastructures, source code development, network access, Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines, component dependencies, and third-party libraries. **Review industry-approved best practices:** ☐ Adopt and mandate adherence to best secure coding practices and standards (e.g., Open Worldwide Application Security Project (OWASP), Computer Emergency Response Team (CERT), National Institute of Standards and Technology (NIST), etc.) to protect the integrity of approved binaries and source code. ☐ Mandate input verification and validation across the entire software development lifecycle. Adhere to the principle of Least Privilege throughout the integration of software components. ☐ Establish a component-wide versioned Development, Security, and Operations (DevSecOps) governance based on guiding principles evolving to the rigorous continuous validation process [21].
Define Component-level software source code compliance requirements.
Establish a source code approval process: ☐ Establish acceptance criteria and requirements for approved binaries and source code. Define the characteristics that binaries and source code should meet to comply with the approval process. ☐ Implement source code versioning and the integrity check of different component dependencies to track and manage approved binaries and source codes. **Secure software code development:** ☐ Ensure the development platform and CI/CD infrastructure are secure, restricted, and segmented with filtered access through Policy Enforcement Points (PEPs).

☐ Leverage the Software Bill of Materials (SBOM) as a critical security element to perform an in-depth analysis of all software components routinely and systematically. Check libraries and frameworks to include open source for known vulnerabilities.
Establish a secure code repository.
Integrate Access Control policy and secure code signing: ☐ Enforce digital code signing and binary scanning to protect against tampering, malware intrusion, poisoned pipeline execution, and insecure first-party code. ☐ Adopt and leverage the Public Key Infrastructure (PKI) to implement trusted certificates, hash value verification for integrity checks, and enforce control policies to track changes to code and binaries. ☐ Select a repository platform (e.g., cloud-based, self-hosted, fully managed, etc.) that meets Component requirements, with solid security features, collaboration tools, built-in robust access controls, and seamless DevSecOps integration. **Implement strong encryption and version control:** ☐ Enable version control to track changes made to code over time and maintain a complete history of all modifications. ☐ Leverage Multi-Factor Authentication (MFA), from Activity 1.3.1 (Phase One) – *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP),* to implement strong authentication and approval mechanisms. ☐ Implement secure Enterprise-approved cryptography and consider industry-best standards, such as NIST and Federal Information Processing Standards (FIPS), to secure sensitive source code, binaries, Application Programming Interface (API) keys, passwords, and encryption keys.
Establish SCRM for code sources.
Leverage the supply chain vetting process: ☐ Keep third-party suppliers of binary code and different CI/CD pipelines separated from each other through isolation, segmentation, containerization, and API accesses [21]. ☐ Develop AI modeling technology for risk-based secure code storage to include model weights, pipelines, reward models, and other AI model elements that protect the confidentiality, integrity, and availability of the binaries and source code [21]. **Enforce continuous threat monitoring:** ☐ Review and restrict third-party libraries upon license compliance checks, vulnerability scanning, and systematic code review. Enforce the adoption of Software Composition Analysis (SCA) solutions for in-depth software analysis.

Summary

This diagram outlines the Activity 3.3.1 (Phase One) – *Approved Binaries and Code* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of supplier-sourcing risk evaluation and the use of approved vulnerability databases in Development, Security, and Operations (DevSecOps). It presents strategic insights that drive implementation and expected outcomes, including the integration of supplier-source risk evaluations for approved sources. This integration drives implementation and expected outcomes, which, in turn, drive the integration of supplier-source risk evaluations for approved sources. These outcomes also include adherence to industry standards for approved vulnerability databases in DevSecOps.

Table 55: Activity 3.3.1 — Approved Binaries and Code - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is supplier sourcing risk evaluated and identified for approved sources? 2. How are repositories and update channels established for use by development teams? 3. How is the Software Bill of Materials (SBOM) created for applications to identify source, supportability, and risk posture? 4. How are industry-standards and approved vulnerability databases used in DevSecOps?

STRATEGIC INSIGHTS
• The Component defines a secure software development policy aligned with Enterprise requirements, establishing strict approval requirements, access controls, and security measures for source code, binaries, and third-party dependencies. • The Component demonstrates compliance by enforcing secure coding practices, implementing version control, conducting continuous verification and validation, and leveraging a SBOM to assess software components for vulnerabilities. • The Component provides verifiable enforcement through digital code signing, supply chain risk management, and encryption standards, ensuring the integrity, security, and compliance of all software assets. • The Component leverages industry best practices, such as National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and Open Worldwide Application Security Project Top 10 (OWASP), to secure the software development lifecycle, enforce strong authentication mechanisms, and mitigate risks associated with third-party libraries and dependencies. • The Component ensures continuous security by integrating Artificial Intelligence (AI)-driven threat monitoring, isolating Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines, and implementing automated scanning to detect and remediate vulnerabilities across the software supply chain.

EXPECTED OUTCOMES

1. Supplier sourcing risk evaluated and identified for approved sources.
2. Repository and update channel established for use by development teams.
3. SBOMs are created for applications to identify source, supportability, and risk posture.
4. Defense Industry Base (DIB) standards and approved vulnerability databases are pulled in to be used in DevSecOps.

Activity 3.3.2 Vulnerability Management Program Part 1

Table 56: Activity 3.3.2 — Vulnerability Management Program 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 collaborates with Components to establish and manage a comprehensive Vulnerability Management program. The program, at a minimum, encompasses the tracking and management of public vulnerabilities based on DoW applications and services. Each Component is responsible for establishing a vulnerability management team comprised of key stakeholders. This team convenes to discuss and manage vulnerabilities in accordance with established Enterprise policy and standards.	
Predecessor(s)	**Successor(s)**
None	3.3.1, 3.3.3
Expected Outcomes	
• Components establish a vulnerability management governance team with appropriate stakeholder membership. • Enterprise provides a vulnerability management policy and standard for minimum tracking and management of public vulnerabilities based on DoW applications and services.	
End State	
Provide structure and an approach to addressing vulnerabilities in accordance with Enterprise policy.	

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 1.1.1 (Discovery) – *Inventory User* prior to this activity, as a comprehensive list of Users/Person Entities (PEs) is necessary to ensure Least Privilege is completely and consistently applied.
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, as a comprehensive list of devices is necessary to ensure Least Privilege is completely and consistently applied.
- Consider completing Activity 3.1.1 (Discovery) – *Application and Code Identification* prior to this activity, as a comprehensive list of applications/services is necessary to ensure Least Privilege is completely and consistently applied.
- Consider completing Activity 4.1.1 (Discovery) – *Data Analysis* prior to this activity, as a comprehensive list of data/data types is necessary to ensure Least Privilege is completely and consistently applied.
- Coordinate with the Enterprise to share vulnerability management intelligence with other Components.

- Activity 3.3.1 (Phase One) – *Approved Binaries and Code* 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 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 57: Implementation Tasks for Activity 3.3.2 — Vulnerability Management Program Part 1

Obtain Enterprise directives, policies, and standards on vulnerability management.
Review policies and standards: ☐ Collaborate with the Enterprise to obtain relevant directives and updated policies on vulnerability management. ☐ Ensure the Enterprise-provided policies include minimum requirements for tracking, assessing, reporting, and remediating vulnerabilities for applications and services within the Component environment. ☐ Document how Component-level practices will align with Enterprise vulnerability categorization and reporting thresholds.
Develop a Component-level vulnerability management program.
Define scope and objectives: ☐ Clearly define vulnerability mission objectives aligned to broader directives and defense strategies, such as: • Reduce the attack surface. • Continuous compliance. • Leverage the threat intelligence and vulnerability sharing to build a robust and effective Incident Response (IR). ☐ Ensure that defined mission objectives integrate measurable outcomes for vulnerability response timelines, stakeholder collaboration, and remediation success. **Develop a vulnerability management strategy:** ☐ Leverage Enterprise-defined requirements. ☐ Identify vulnerability intelligence sources (e.g., vendor bulletins, Common Vulnerabilities and Exposures (CVEs), etc.).

☐ Develop vulnerability remediation workflows, for example:

- Document vulnerability and affected applications and services.
- Identify corrective actions.
- Develop implementation
- Verify and validate correction/resolution.

☐ Identify Component Data, Applications, Assets, and Services (DAAS).

☐ Leverage the device Inventory, from Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis*.

☐ Leverage the application/code inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification.*

☐ Leverage the data inventory, from Activity 4.1.1 (Discovery) – *Data Analysis*.

☐ Integrate a centralized tracking system to record and update the lifecycle status of each vulnerability (e.g., open, in review, remediated, verified, etc.).

Establish a vulnerability management and governance board.

Build a comprehensive vulnerability management team and governance board:

☐ Establish policy, assign responsibilities, and provide guidelines for participation in the Component vulnerability management process, to include:

- Cross-functional stakeholders
- System owners
- Application developers
- Mission assurance
- Compliance teams

☐ Ensure the governance board is responsible for oversight of response timelines, policy adherence, and coordination with Enterprise counterparts.

Vulnerability triage and reporting:

☐ Develop technical analysis and remediation capabilities to select and prioritize vulnerabilities based on severity, exploitability, exposure, and compliance requirements [17].

☐ Empower the vulnerability management team to:

- Receive vulnerability reports from approved sources.
- Coordinate and investigate to identify vulnerable systems.
- Share findings report(s) with approved stakeholders for actions.
- Disseminate advisories and security bulletins on found vulnerabilities to the broader community as appropriate [17].

☐ Define and document criteria for escalation, communication channels, and reporting cadence to Enterprise-level vulnerability management stakeholders.

☐ Establish periodic reviews to assess performance metrics, identify outstanding critical vulnerabilities, and ensure alignment with Enterprise Service Level Agreements (SLAs).

Summary

This diagram outlines the Activity 3.3.2 (Phase One) – *Vulnerability Management Program Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of establishing a vulnerability management policy and creating a corresponding team. It presents strategic insights that drive implementation and expected outcomes, including the establishment of a vulnerability management governance team.

Table 58: Activity 3.3.2 — Vulnerability Management Program Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is a vulnerability management team established with appropriate stakeholder membership? 2. How is the vulnerability management policy and process agreed upon with stakeholders? 3. How are public sources of vulnerabilities utilized for tracking?
STRATEGIC INSIGHTS
• The Component defines a structured vulnerability management program aligned with Enterprise directives, establishing policies, governance, and remediation workflows to enhance security resilience. • The Component demonstrates compliance by leveraging vulnerability intelligence sources, prioritizing vulnerabilities based on risk, and implementing a systematic approach to discovery, remediation, and continuous compliance. • The Component provides verifiable enforcement through vulnerability triage, reporting, and governance oversight, ensuring threats are identified, assessed, and mitigated in coordination with approved stakeholders. • The Component leverages Enterprise-defined requirements, security bulletins, and Common Vulnerabilities and Exposures (CVE) intelligence to proactively manage risks across Data, Applications, Assets, and Services (DAAS). • The Component ensures continuous security by maintaining a dedicated vulnerability management team, integrating threat intelligence, and establishing a structured process for real-time vulnerability response and reporting.
EXPECTED OUTCOMES
1. Components establish a vulnerability management governance team with appropriate stakeholder membership. 2. Enterprise provides a vulnerability management policy and standard for minimum tracking and management of public vulnerabilities based on DoW applications and services.

Capability 3.4 Resource Authorization and Integration

Table 59: 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 3.4.1 Resource Authorization Part 1

Table 60: Activity 3.4.1 — Resource 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 standardizes policy enforcement approaches (e.g., Software-Defined Perimeter) with the Components. At a minimum, the access and authorization gateways will be integrated with identities and devices once authentication is achieved. Components deploy approved resource authorization gateways and enable them for external facing applications and services. Additional applications for migration and applications unable to be migrated are identified for exception or decommission.	
Predecessor(s)	**Successor(s)**
1.8.1, 2.6.2, 5.3.1	3.4.2
Expected Outcomes	
• DoW Enterprise sets standards on policy enforcement approach. At a minimum, access and authorization is integrated with identities and devices once authentication is achieved. • Components deploy approved resource authorization gateways and enable them for external facing applications and services. • DoW Enterprise-wide interoperability guidance is communicated to stakeholders.	
End State	
Policy enforcement points are fully integrated with identity and device management systems, ensuring consistent and secure 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 1.8.1 (Phase One) – *Single Authentication*, Activity 2.6.2 (Phase One) – *Enterprise Device Management (EDM) 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 leverage the Application/Code inventory for migration planning.
- Activity 3.4.2 (Phase Two) – *Resource 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 61: Implementation Tasks for Activity 3.4.1 — Resource Authorization Part 1

Collaborate with the Enterprise to set standards for policy enforcement.
Review and apply the following Enterprise policies and standards, as applicable: □ Collaborate with the Enterprise to align Component-level policy enforcement with established Enterprise standards. This collaboration should ensure consistency, interoperability, and compliance across environments. □ Understand Enterprise standards, such as: • Interoperability requirements • Development, Security, and Operations (DevSecOps) [30] • Information Technology Operations Management (ITOM) [31] • Applicable regulations, policies, and governance requirements **Deploy and enable selected gateways in accordance with Enterprise security and configuration standards:** □ Integrate deployed gateways with Identity and Access Management (IAM) solutions to enforce authentication and access policies. □ Enforce and track access control decisions across integrated systems. □ Conduct continuous monitoring, data collection, parsing, analysis, and prioritized reporting of gateway and application activity.
Deploy approved resource authorization gateways and enable them for external-facing applications and services.
Resource authorization gateways: □ Define the gateway authorization requirements. □ Identify external-facing web applications and services. □ Choose resource gateways for the Component. □ Integrate gateways with Identity and Access Management (IAM). □ Enforce and track Access Control. □ Continuous monitoring, keen collection, parsing, analysis, and priority reporting of applications and services.

Identify additional applications for migration and determine the ones that are non-migratable for exception or decommissioning.

Application migration planning:

☐ Leverage the Application/Code inventory, from Activity 3.1.1 (Discovery) – *Application and Code Identification*, to identify applications and services that are compatible with the authorization gateways.

- Determine if applications and services are capable of migration.
- Identify/document systems for migrations and exceptions, as necessary.

☐ Verify and validate application/service compatibility with the authorization gateways.

☐ Develop application/service migration roadmap/implementation plans.

Document and approve exceptions to application/service migration.

Manage exceptions:

☐ Applications/services that cannot be migrated are:

- Identified
- Documented
- Approved/ or Rejected

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

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

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

☐ Approval is periodically reassessed.

Migrate applications/services.

Implementation:

☐ Migrate applications/services behind the authorization gateways.

- Consider prioritizing applications/services that present the most risk to the Component/Enterprise.

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 that do not leverage the authorization gateways.

Verify and validate authorization gateways: ☐ Ensure authorization gateways are configured in accordance with the Enterprise requirements. ☐ Ensure authorization gateways are configured to provide the necessary functionality to support the Component’s operational requirements.
Conduct periodic assessments.
Periodically verify and validate: ☐ Periodically verify and validate the applications/services and authorization gateways to ensure they meet Enterprise/Component requirements.

Summary

This diagram outlines the Activity 3.4.1 (Phase One) – *Resource Authorization Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of a resource approval policy, as well as gateways for external applications. It presents strategic insights that drive implementation and expected outcomes, including the deployment of approved resource authorization gateways, which enable external-facing applications and services.

Table 62: Activity 3.4.1 — Resource Authorization Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How is the resource authorization gateway implemented for external-facing applications? 2. How is the resource authorization policy integrated with identity and device management? 3. How is Enterprise-wide guidance on conversion standards communicated to stakeholders?
STRATEGIC INSIGHTS
• The Component defines a standardized policy enforcement approach by aligning governance, compliance, and security policies with Enterprise standards, including Development, Security, and Operations (DevSecOps), Information Technology Operations Management (ITOM), and interoperability requirements. • The Component demonstrates security and operational efficiency by deploying resource authorization gateways, integrating them with Identity and Access Management (IAM), and systematically migrating applications and services while ensuring continuous monitoring and compliance. • The Component provides verifiable enforcement through access control verification and validation, exception management, and periodic policy reviews, ensuring that authorization gateways enforce security policies and mitigate risks effectively. • The Component leverages Enterprise threat intelligence, vulnerability insights, and risk-sharing mechanisms to enhance security posture and support informed decision-making on application migration, exceptions, and decommissioning. • The Component ensures continuous security by maintaining an iterative assessment process, verifying and validating authorization gateways, and conducting periodic evaluations to align with evolving Enterprise requirements and operational priorities.
EXPECTED OUTCOMES
1. DoW Enterprise sets standards on policy enforcement approach. At a minimum, access and authorization is integrated with identities and devices once authentication is achieved. 2. Components deploy approved resource authorization gateways and enable them for external facing applications and services. 3. DoW Enterprise-wide interoperability guidance is communicated to stakeholders.

Activity 3.4.3 Software-Defined Compute (SDC) Resource Authorization Part 1

Table 63: Activity 3.4.3 — Software-Defined Compute (SDC) Resource 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 establishes best practices for code-based compute management (i.e., Software-Defined Compute (SDC)). Using risk-based approaches, baselines are created using the approved set of code libraries and packages. Components work with Activity 3.3.1 (Phase One) – *Approved Binaries and Code* to ensure that applications are identified which can and cannot support the approach. Applications that can support a modern software-based configuration and management approaches are identified, and transitioning begins. Applications that cannot follow software-based configuration and management approaches are identified and allowed through exception using a methodical approach.	
Predecessor(s)	**Successor(s)**
	3.4.4
Expected Outcomes	
• Enterprise-wide guidance on SDC standards are communicated to stakeholders. • Components identify applications that can support the SDC approach.	
End State	
Enterprise best practices support Component efforts in leveraging SDC 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 3.1.1 (Discovery) – *Application and Code Identification* prior to this activity, as a comprehensive list of applications/services is necessary to ensure Least Privilege is completely and consistently applied.
- Utilize Enterprise-approved Application Programming Interface (API) gateways and application calls within macro-segmented environments.
- Enforce micro-segmented application and workload access, permitting only approved and authenticated connections to specific destinations (e.g., microservices, etc.).
- Ensure regulatory guidance is established, and configurations are correctly implemented.
- Develop flexible Software-Defined Compute (SDC) resource allocation and scalability mechanisms, incorporating robust authentication techniques.

- Implement reliable Representational State Transfer (REST) APIs to establish micro-segmentation between environments and application workload pillars, ensuring secure interactions between Users/Person Entities (PEs)/Non-Person Entities (NPEs) and Data, Applications, Assets, and Services (DAAS).
- Activity 3.4.4 (Phase Two) – *Software-Defined Compute (SDC) Resource Authorization 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 64: Implementation Tasks for Activity 3.4.3 — Software-Defined Compute (SDC) Resource Authorization Part 1

Collaborate with the Enterprise to set standards for SDC.
Leverage Enterprise SDC standards: ☐ Establish SDC standards based on understanding of Enterprise standards, to include: • Interoperability requirements • Development, Security, and Operations (DevSecOps) • Regulations, policies, best business practices, etc. ☐ Collaborate with stakeholders. ☐ Align Component governance and compliance policies with Enterprise requirements. ☐ Conduct a periodic review of policies on a defined schedule. **Document and sustain SDC-tracked changes:** ☐ Document all changes, build release versions, and new features for project, program, or software builds and baselines [32]. ☐ If completed, consider patch management and Incident Response (IR) processes within a tracking system solution, established in Activity 3.3.2 (Phase One) – *Vulnerability Management Program Part 1*, to effectively track changes, update build release baselines, and apply patches using the Component Vulnerability Management processes [33]. **Identify, plan, and establish a distinct elements strategy for managing build, release, and version-controlled SDC activities:** ☐ Apply an agile risk management plan, mutually agreed upon by Component stakeholders, to categorize and define a baseline approach within the configuration management review process.

- Ensure the plan addresses both supported and non-supported assets as elements, including their interfaces and workload processes across Hyperconverged Infrastructure (HCI) or native cloud landscapes.

☐ Plan and ensure the establishment of real-time risk management and control by functional categories, criteria, or elements. Implement this as a routine and non-routine systemic process using dashboards or messaging techniques.

☐ Plan and ensure the quantification of supported binaries, build releases, and related script activities through a gap analysis systemic approach. Define “normal” SDC API routine scriptable runtime signatures and identify “anomalous” non-routine, non-signature SDC API activities to be determined or resolved.

Identify applications that support SDC.

Application migration planning:

☐ Leverage the Application and Code inventory, from Activity 3.1.1 (Discovery) – *Application and Code* Identification*,* to identify applications and services compatible with the SDC.

- Determine if applications and services are capable of migration.
- Identify/document systems for migrations and exceptions, as necessary.

☐ Verify and validate application/service compatibility with the authorization gateways.

☐ Assess the feasibility of this transition across different Phases and timelines with defined milestone deliverables.

- Consider factors such as the current and target future states of manual processes, binaries, API script calls, Continuous Integration and Continuous Delivery (or Deployment) (CI/CD) pipelines, micro-segmentation, available resources, and organizational priorities.

Document and approve exceptions to application/service migration.

Manage exceptions:

☐ Identify and document applications/services that cannot support SDC, along with their technical limitations or operational dependencies.

☐ Document the business or mission justification for each exception.

☐ Evaluate each exception request against Enterprise SDC standards and Component risk tolerance:

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

☐ Consider mitigation strategies for non-compliant applications/services, including:

- Targeted upgrades or refactoring
- Replacement with supported alternatives
- Segmentation or isolation
- Eventual decommissioning, where possible

☐ Periodically reassess all exceptions in coordination with evolving Enterprise and Component guidance and threat intelligence to ensure continued validity.

Conduct periodic assessments.

Reassess SDC policy/procedures:

☐ Periodically reassess Component SDC policy/procedures to ensure they align with Enterprise requirements.

☐ Validate ongoing alignment with updated Enterprise guidance, best practices, and threat-informed risk postures.

☐ Review the list of applications/services identified for SDC transition and update status (e.g., migrated, in-progress, exception, etc.).

☐ Analyze the effectiveness of SDC implementation using measurable indicators such as:

- Number of compliant applications/services
- Reduction in configuration drift
- Timeliness of patching and release cycles

Summary

This diagram outlines the Activity 3.4.3 (Phase One) – *Software-Defined Compute (SDC) Resource Authorization Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the establishment and implementation of Software-Defined Compute (SDC) standards. It presents strategic insights that drive implementation and expected outcomes, including the identification of applications that support the SDC approach.

Table 65: Activity 3.4.3 — Software-Defined Compute (SDC) Resource Authorization Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How does the resource authorization receive data from the analytics engine? 2. How do authorization policies incorporate identified attributes in making authorization decisions? 3. How are attributes for initial enrichment identified and assigned to resources or entities?

STRATEGIC INSIGHTS
• The Component defines SDC standards by collaborating with the Enterprise to document interoperability requirements, governance policies, and compliance frameworks that align with Development, Security, and Operations (DevSecOps) best practices, as well as regulatory requirements. • The Component demonstrates a structured approach to identifying, tracking, and documenting SDC-related changes, including build release versions, patch updates, and configuration baselines, ensuring alignment with Enterprise vulnerability management and Incident Response (IR) processes. • The Component provides verifiable documentation of application compatibility with SDC, conducting assessments to categorize supported and non-supported assets, track migration feasibility, and document risk-based justifications for exceptions. • The Component leverages application and code inventories to evaluate SDC readiness, documenting system migration pathways and exception approvals, and workload processes across all relevant compute environments (e.g., on-premises, cloud, containerized, and virtualized infrastructures). • The Component ensures continuous alignment with Enterprise SDC policies by periodically reassessing documented standards, maintaining a structured process for reviewing changes, and updating governance frameworks as technology and security requirements evolve.

EXPECTED OUTCOMES
1. Enterprise-wide guidance on SDC standards are communicated to stakeholders. 2. Components identify applications that can support the SDC approach.

Data Pillar

Capability 4.2 DoW Enterprise Data Governance

Table 66: 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 4.2.1 Define Data Tagging Standards

Table 67: Activity 4.2.1 — Define Data Tagging Standards

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 tagging standard for identifying ZT labels must be defined. DoW Enterprise works with Components to establish data tagging and classification standards based on industry best practices. Classifications are agreed upon and implemented in processes. Tags are identified as manual and automated for future activities.	
Predecessor(s)	**Successor(s)**
None	4.3.1, 4.3.2, 4.3.4, 6.3.1
Expected Outcomes	
• Enterprise establishes the standard pattern for control vocabulary and how it is managed. • Components align to Enterprise standards and begin implementation. • Components implement data tagging and labeling standards.	
End State	
The data dictionary and structure is developed at a broader DoW Enterprise level. ZT-specific data attributes are defined in alignment with the Enterprise data dictionary and structure.	

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.

- Existing data tagging and standards should be leveraged as a reference to ensure consistency and accuracy.
  - Standardizing data tags enhances uniformity and facilitates interoperability.
  - Analyzing metadata improves data organization and retrieval.
- The entire data lifecycle, including retention, should align with regulatory requirements and business strategies.
  - Adhering to regulatory compliance ensures legal and ethical data handling.
  - Aligning data retention policies with business strategies supports long-term objectives.
- Data collection, processing, classification, and analysis should support Component goals and enhance accessibility.
  - Enhancing data discoverability improves efficiency and usability.

  - Supporting data and analytic missions ensures alignment with Component priorities.
- Data structure and formatting should accommodate diverse data types and support analytical needs.
  - Effective data tagging and metadata management are critical for enhancing the usability of unstructured data types.
  - Exploring and visualizing data aids in decision-making and generating insights.
  - Establishing clear data type definitions promotes consistency and accuracy.
- Ensuring data interoperability enables the exchange and use of data across systems and platforms, facilitating integration efforts.
  - Adopting open standards facilitates seamless data exchange.
  - Maintaining data compliance and reporting ensures regulatory adherence.
  - Streamlining data flow and workflows optimizes operational efficiency.
- Compliance and reporting mechanisms should be established to meet legal, regulatory, and business requirements.
- Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools*, Activity 4.3.2 (Phase Two) – *Manual Data Tagging Part 1*, Activity 4.3.4 (Phase Three) – *Automated Data Tagging and Support Part 1*, and Activity 6.3.1 (Phase Two) – *Implement Data Tagging and Classification Machine Learning (ML) Tools* 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 68: Implementation Tasks for Activity 4.2.1 — Define Data Tagging Standards

Collaborate with the Enterprise to develop standard pattern(s) for control vocabulary.
Enterprise-Component collaboration framework: ☐ Establish cross-functional working groups with representation from Enterprise data governance teams, Component data stewards, security specialists, and end users to ensure comprehensive input. ☐ Document formal communication channels between the Enterprise and Components to facilitate ongoing alignment and updates to standards. ☐ Create a standardized feedback loop to provide insights on implementation challenges and improvement opportunities back to Enterprise governance bodies.
Establish strategic data governance standards.
Data taxonomy development: ☐ Conduct comprehensive data inventory to identify all data types, sources, and usage patterns across the Component. ☐ Map existing classification schemes to the Enterprise standard and document translation requirements. ☐ Define taxonomy hierarchy levels that align with Enterprise-defined data sensitivity classifications while supporting Component-specific needs. ☐ Create visual reference materials (e.g., decision trees, flowcharts, etc.) to help data owners determine appropriate tags. **Control vocabulary management:** ☐ Implement version control systems for tag libraries to track changes and maintain historical records. ☐ Establish authorization workflows for proposing, reviewing, and approving new tags or modifying existing tags. ☐ Define metadata schemas that include mandatory and optional fields aligned with Enterprise standards. ☐ Establish tag conflict resolution procedures when multiple classification schemes apply to the same data. ☐ Create tag validation processes to ensure consistency and compliance with standards. **Data tagging policy implementation:** ☐ Develop comprehensive documentation that clearly articulates tagging requirements, procedures, and responsibilities. ☐ Establish compliance monitoring mechanisms to track adherence to tagging standards. ☐ Implement periodic audit procedures to validate tag accuracy and completeness. ☐ Create remediation processes for addressing non-compliant or incorrectly tagged data.

Cross-Component interoperability:

☐ Implement a federated tag library architecture that supports both Enterprise-wide and Component-specific tags.

☐ Establish metadata exchange protocols between Components to maintain consistency.

☐ Define cross-boundary data handling procedures to preserve tags when data moves between Components.

☐ Create integration testing frameworks to validate tag interoperability prior to production implementation.

System integration requirements:

☐ Define Application Programming Interface (API) specifications for integrating tagging capabilities into existing systems.

☐ Establish data exchange formats that preserve tag metadata during transfers.

☐ Implement tag propagation mechanisms to maintain classification through data transformations.

☐ Create technical validation procedures to ensure systems correctly interpret and apply tag restrictions.

Security implementation requirements:

☐ Define tag-based access control mechanisms that enforce ZT principles.

☐ Where necessary, implement tag encryption requirements for sensitive classification metadata.

☐ Establish tag verification procedures to verify and validate authenticity and prevent tampering.

☐ Create security monitoring capabilities that leverage tag information for anomaly detection.

Migration planning:

☐ Develop transition strategies from legacy classification systems to new tagging standards.

☐ Establish data remediation procedures for previously untagged or improperly tagged data.

☐ Create rollback capabilities to address potential implementation issues.

☐ Define contingency operations to maintain security during transition periods.

Implementation risk assessment and mitigation:

☐ Identify critical implementation risks such as operational impacts, resource constraints, and technical limitations.

☐ Develop targeted mitigation strategies for each identified risk.

☐ Establish risk monitoring mechanisms to detect emerging implementation challenges.

☐ Create escalation procedures for addressing critical implementation blockers.

Select Component data tagging solution.

Select data tagging solution:

☐ Identify a data tagging solution that supports both Component needs and Enterprise interoperability requirements.

☐ Where possible, select a solution that can implement tag inheritance mechanisms to efficiently apply tags to data hierarchies.
Verify and validate Component selected data tagging solution.
Test data tagging solution: ☐ Within a controlled environment, ensure the selected solution(s): • Meet previously identified requirements. • Integrate with the Component environment(s). • Successfully provide the advertised functionality within the Component environment(s).
Manage data that cannot leverage the Component-selected data tagging solution.
Manage exceptions: ☐ Data/data types on systems that are incompatible with the data tagging solution are: • Identified • Documented • Approved or Rejected ☐ Approval is granted when justification for the exception outweighs the risks to the Enterprise/Component. • If approved, they are documented for manual tagging. ☐ The Enterprise and/or Component determines risks. ☐ Approval is periodically reassessed.
Define data tagging and classification processes.
Manual tagging processes: ☐ Develop role-based tagging responsibilities, clearly defining who is authorized to assign types of tags. ☐ Establish quality control checkpoints to verify and validate manually applied tags.

Summary

This diagram outlines the Activity 4.2.1 (Phase One) – *Define Data Tagging Standards* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on data tagging and classification standards. It presents strategic insights that drive implementation and expected outcomes, including the establishment and implementation of a standard pattern for control vocabulary and its management.

Table 69: Activity 4.2.1 — Define Data Tagging Standards - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are data tagging and classification standards established and communicated to stakeholders?

STRATEGIC INSIGHTS
• The Component defines and documents the establishment of control vocabulary patterns in collaboration with the Enterprise, ensuring alignment with Enterprise-wide data governance standards and supporting the ongoing development of an updated data taxonomy baseline. • The Component demonstrates compliance by assigning responsibilities for managing data requirements, leveraging the Enterprise-wide data dictionary, and categorizing the data tagging classification process as manual or automatic to enable future automation and operational efficiency. • The Component provides a structured approach to data governance, enforcing data-handling procedures, tagging requirements, and strategic policies in coordination with Enterprise data governance bodies to promote consistency and compliance. • The Component leverages a federated tag library capability, integrating Enterprise-controlled tag libraries to ensure interoperability across systems and datasets, defining critical metadata elements such as classification, policy, and rules, as well as tags and associated metadata. • The Component ensures continuous monitoring and compliance of data tagging processes, implementing built-in labeling capabilities, quarantine mechanisms for untagged files, and periodic process reviews to maintain alignment with evolving Enterprise data governance requirements.

EXPECTED OUTCOMES
1. Enterprise establishes the standard pattern for control vocabulary and how it is managed. 2. Components align to Enterprise standards and begin implementation. 3. Components implement data tagging and labeling standards.

Activity 4.2.2 Interoperability Standards

Table 70: Activity 4.2.2 — Interoperability Standards

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, collaborating with Components, develops interoperability standards and methods, including mandatory Data Rights Management (DRM) overlays and protection mechanisms, with necessary technologies to enable ZT Target-level functionality.	
Predecessor(s)	**Successor(s)**
None	4.5.1
Expected Outcomes	
• Standard patterns are in place by the Enterprise for appropriate interoperability data sharing.	
End State	
Interoperability standards for DRM and protection are established and enforced across the Enterprise. These standards are supported by a common language (terms list and scientific definitions) to ensure consistency and clarity. Equal computation outcomes are produced for any rule, and an action agent (enforcement) based on computational results is executed. This unified approach promotes secure, consistent, and compliant data 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 4.1.1 (Discovery) – *Data Analysis* prior to this activity, to leverage the Component Data Catalog.
- Consider completing Activity 4.4.2 (Discovery) – *Data Rights Management (DRM) Enforcement Point Logging and Analysis* prior to this activity, as the Data Rights Management (DRM) policies will be necessary to complete this activity.
- Data integration with third-party providers and partners.
    - Evaluate data quality requirements for business needs.
    - Define regulatory compliance requirements.
    - Review supply chain data access management.
- Enterprise has established interoperability standards, integrating mandatory DRM and protection solutions as necessary.
- Open standards.
    - Open standards are **not** the same as open source.
    - Avoid vendor lock-in.

  - Prioritize mature and vetted technologies and standards where appropriate, while also establishing a process for evaluating and piloting emerging technologies that offer significant interoperability benefits.
- 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 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 71: Implementation Tasks for Activity 4.2.2 — Interoperability Standards

Leverage the Enterprise-approved interoperability standards.
Enterprise alignment: ☐ Inventory existing Enterprise interoperability standards by cataloging all approved data exchange formats, protocols, and frameworks already in use across the DoW. ☐ Establish an interoperability assessment framework to evaluate current capabilities against ZT requirements. ☐ From cross-functional working groups with Enterprise and Component representatives to ensure a comprehensive understanding of technical and operational requirements. ☐ Identify regulatory and compliance mandates that impact data interoperability, particularly those related to classification levels and handling requirements. **Component-specific requirements:** ☐ Leverage the Component Data Catalog, from Activity 4.1.1 (Discovery) – *Data Analysis*, to identify critical data assets requiring interoperability solutions. ☐ Document existing data-sharing agreements with other Components, partners, and third parties. ☐ Map data flows across systems to identify integration points and interoperability requirements. ☐ Conduct stakeholder interviews to identify operational needs and challenges related to data sharing. **DRM integration:** ☐ Leverage the Component-level access control policies, from Activity 4.4.2 (Discovery) – *Data Rights Management (DRM) Enforcement Point Logging and Analysis*. ☐ Assess current DRM implementations to determine compatibility with Enterprise standards. ☐ Identify interoperability standards for DRM and protection to enforce comprehensively across the Component environment(s), utilizing a common language.

Develop Interoperability Framework.
Define and document data exchange patterns considering ZT principles: ☐ Authentication and authorization requirements for all data exchanges. ☐ Encryption standards for data in transit and at rest. ☐ Audit and logging requirements for accountability. ☐ Mechanisms for enforcing data exchange policies across participating systems. **Establish and document standardized data models for each identified data category, considering interoperability and enforcement needs:** ☐ Schema definitions with mandatory and optional fields. ☐ Data type specifications and validation rules. ☐ Standard identifier formats for cross-system references. **Develop and document machine-to-machine communication protocols aligned with approved interoperability and security standards:** ☐ Real-time data exchange with minimal latency. ☐ Asynchronous communication for non-critical exchanges. ☐ Error handling and resiliency mechanisms. ☐ Standard authentication, authorization, and enforcement mechanisms to ensure consistent access control.

Summary

This diagram outlines the Activity 4.2.2 (Phase One) – *Interoperability Standards* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development and integration of interoperability standards. It presents strategic insights that drive implementation and expected outcomes, including the incorporation of standard patterns for appropriate interoperable data sharing.

Table 72: Activity 4.2.2 — Interoperability Standards - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are interoperability standards developed and integrated into Data Rights Management (DRM) and protection solutions?

STRATEGIC INSIGHTS
• The Component defines and documents machine-to-machine communication requirements, ensuring alignment with Enterprise data governance and interoperability standards, including centralized, replicated, federated, collaborative, and decentralized data models. • The Component demonstrates compliance by supporting Enterprise data interoperability requirements and criteria, leveraging Enterprise-approved standards, and integrating Component-specific data communication needs within the Component Data Catalog, from Activity 4.1.1 (Discovery) – *Data Analysis*. • The Component offers a structured approach to data and communication standardization, ensuring interoperability across systems by documenting standards, models, and governance policies within its data governance framework. • The Component leverages existing Enterprise data standardization efforts and Component-specific data communication requirements to maintain compatibility, enhance efficiency, and ensure long-term sustainability of data-driven operations. • The Component ensures continuous monitoring, assessment, and updates of interoperability rules and data governance policies to align with evolving Enterprise requirements, technological advancements, and operational priorities.

EXPECTED OUTCOMES
1. Standard patterns are in place by the Enterprise for appropriate interoperability data sharing.

Capability 4.3 Data Labeling and Tagging

Table 73: 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 4.3.1 Implement Data Tagging and Classification Tools

Table 74: Activity 4.3.1 — Implement Data Tagging and Classification 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 implement a solution to create new rules, modify existing rules, delete existing rules, check for rule collision, rule deviation, or compound rule inconsistency, and testing of collective rule sets for an outcome. Tools must be adaptable to advanced analytic techniques.	
Predecessor(s)	**Successor(s)**
4.2.1	4.6.1
Expected Outcomes	
• Tooling is designed based on Component data tagging efforts that are well-formed with Enterprise-dictated patterns and standards, and are machine readable. • Data classification uses data tagging attribution to specify allowed values.	
End State	
All valid tags can be processed, and invalid tags cannot.	

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.
- Assumption: The Component has an existing Security Information and Event Management (SIEM) solution.
- Activity 4.6.1 (Phase One) – *Implement Enforcement Points* 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 75: Implementation Tasks for Activity 4.3.1 — Implement Data Tagging and Classification Tools

Establish a data collection architecture.
Identify data storage/management solutions, constraints, and data collection points, and establish a standardized data collection architecture: ☐ Identify existing data storage and management solutions, including local, cloud, and/or Hyperconverged Infrastructure (HCI). Examples include: • Data Lakes • Data Marts • Operational databases (e.g., Online Transaction Processing (OLTP) Database, Metadata repositories, etc.) ☐ Identify data storage and management constraints: • Capacity and Performance: ○ Storage limits, processing capacity, query performance, Service Level Agreements (SLAs), and concurrent User/Person Entity (PE) support boundaries that impact architecture decisions. • Security and Compliance: ○ Data protection requirements, regulatory constraints, Access Controls, and audit trails needed for sensitive information. • Integration and Compatibility: ○ Limitations in connecting with existing systems, tools, and Application Programming Interfaces (APIs), and the need to support various data formats and schemas. • Governance and Data Quality: ○ Requirements for metadata management, lineage tracking, data verification and validation, and alignment with Enterprise standards. • Operational Boundaries: ○ Maintenance windows, deployment restrictions, disaster recovery requirements, and lifecycle management constraints. ☐ Identify existing data collection points, such as: • Data Collection Node (DCN) • System Log (Syslog) data collection • Forwarders • Hypertext Transfer Protocol (HTTP) Event Collector (HEC) ☐ Establish standardized data tagging and classification models. Implement solutions to automatically tag data at the point of creation or production and provide mechanisms for data stewards to tag and classify existing data assets.

Select a data tagging solution.

Select data tagging solution(s):

☐ Leverage data tagging and criticality standards, documented in the federated tag library, from Activity 4.2.1 (Phase One) – *Define Data Tagging Standards*.

☐ Identify data tagging tools/solutions that meet Enterprise/Component-defined requirements and align with the standards in the federated tag library. At a minimum, the data tagging solution(s) should include the following functionalities:

- Data tagging at creation
- Tagging for data discovery
- Tagging for imported data
- Quarantine untagged data

☐ Identify a global key access store solution to act as a centralized tag repository/single source of truth for all tags:

- Ensure the key access store solution can align with the federated tag library standards.

☐ Design federation processes.

☐ Define data quality requirements and create a data model:

- Develop data metrics.
- Determine acceptable data duplication and collision ratio.
- Alert on inconsistent data events.

☐ Define data quality requirements and data duplication/standardization.

☐ Define rule-based tagging algorithms aligned with established classification criteria.

☐ Implement Machine Learning (ML) models for content-based classification that can be iteratively improved.

☐ Establish confidence thresholds for automated tagging with human review requirements for borderline cases.

☐ Create exception handling processes for data that cannot be automatically classified with sufficient confidence.

Hybrid tagging approaches:

☐ Define workflow integration points between manual and automated processes.

☐ Establish escalation procedures for resolving tagging discrepancies.

☐ Implement feedback mechanisms to continuously improve automation accuracy based on manual corrections.

☐ Create automated quality sampling to validate both manual and automated tagging processes.

☐ Define a data tagging process for testing, verification, and validation:

- Enable monitoring and auditing to verify and validate compliance with expected outcomes.
- Create and review audit trails from data access and tagging activities.

Test data tagging solution functionality.

Verify and validate data tagging solutions:

☐ Ensure the selected solutions provide the necessary capabilities by testing their ability to implement Enterprise/Component requirements.

Deploy the data tagging solution.

Technical Infrastructure:

☐ Implement federation processes.

☐ Implement Access Controls and security layers.

☐ Develop monitoring and reporting solutions.

Workflow Implementation:

☐ Develop data tagging workflows (e.g., creation, discovery, import, etc.).

☐ Create quarantine mechanisms for untagged data.

☐ Build search and discovery interfaces.

Deployment:

☐ Pilot implementation with limited scope.

☐ Progressive rollout across data domains or business units.

☐ Integration with existing systems.

Verify and validate the Component data tagging solution.

Metrics and monitoring:

☐ Define Key Performance Indicators (KPIs) for data tagging effectiveness (e.g., accuracy, completeness, timeliness, etc.).

☐ Implement tagging coverage monitoring to identify gaps in tagged data stores.

☐ Establish periodic compliance reviews to validate alignment with Enterprise standards.

☐ Create automated dashboards to visualize tagging implementation progress and effectiveness.

Continuous improvement process:

☐ Implement feedback collection mechanisms from data users and stakeholders.

☐ Establish regular review cycles to evaluate tagging effectiveness and identify improvement opportunities.

☐ Create pilot programs for testing enhancements before full implementation.

☐ Develop knowledge sharing platforms to exchange best practices between Components.

Summary

This diagram outlines the Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of data classification and tagging solutions utilizing Artificial Intelligence (AI)/Machine Learning (ML). It presents strategic insights that drive implementation and expected outcomes, including tooling design based on component data tagging.

Table 76: Activity 4.3.1 — Implement Data Tagging and Classification Tools - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
• How are data classification and tagging tools integrated to support ML and AI? • What steps have been taken to implement data classification and tagging tools at both Component and Enterprise levels?

STRATEGIC INSIGHTS
1. The Component defines and documents policies and procedures for establishing a standardized data collection architecture, identifying existing storage and management solutions while addressing constraints such as capacity, performance, security, compliance, and governance to ensure Enterprise-wide alignment. 2. The Component demonstrates compliance by identifying data collection and integrating data tagging solutions that adhere to federated tag library standards, ensuring tagging at creation, discovery, and import while enforcing quarantine mechanisms for untagged data. 3. The Component provides evidence that data tagging solutions are tested, verified, validated, and monitored to maintain compliance with Enterprise data governance standards. This includes ensuring audit trails for data access and tagging activities, defining data quality metrics, and enabling alerts for inconsistent data events to ensure accuracy and integrity. 4. The Component leverages a Key Access Store as a single source of truth for all tags, ensuring alignment with federation processes and enabling seamless integration with Security Information and Event Management (SIEM) solutions and advanced analytics, such as Artificial Intelligence (AI)-driven pattern recognition and automated categorization. 5. The Component ensures ongoing compliance through continuous auditing, adaptive data governance, and iterative enhancements to data collection and tagging processes, maintaining interoperability with evolving Enterprise security mandates and emerging data management technologies.

EXPECTED OUTCOMES
1. Tooling is designed based on Component data tagging efforts that are well-formed with Enterprise-dictated patterns and standards, and are machine readable. 2. Data classification uses data tagging attribution to specify allowed values.

Capability 4.4 Data Monitoring and Sensing

Table 77: 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 4.4.3 File Activity Monitoring Part 1

Table 78: Activity 4.4.3 — File Activity Monitoring 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 File Monitoring tools to monitor the most critical data classification levels in applications, services, and repositories. Analytics from monitoring is fed into the SIEM with basic data attributes to accomplish ZT Target-level functionality.	
Predecessor(s)	**Successor(s)**
None	4.4.4
Expected Outcomes	
• Data and files of critical data designations are identified and actively monitored. • Establish and manage business rules to consume critical data designations and manage outcomes. • Integration is in place with monitoring system (e.g., SIEM, XDR).	
End State	
Files are associated with data assets and objects. File integrity monitoring occurs at the data asset and object levels, allowing for greater visibility and accuracy.	

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 4.1.1 (Discovery) – *Data Analysis* prior to this activity, to leverage data tagging standards.
- This activity integrates with Activity 4.2.1 (Phase One) – *Define Data Tagging Standards*, Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools*, and Activity 4.6.1 (Phase One) – *Implement Enforcement Points*.
- This Activity is Part 1 of 2 and is scoped to critical data.
- Activity 4.4.4 (Phase Two) – *File Activity Monitoring 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 79: Implementation Tasks for Activity 4.4.3 — File Activity Monitoring Part 1

Identify File Activity Monitoring (FAM) requirements.
Collaborate with stakeholders: ☐ Identify stakeholders to establish FAM policy/processes. ☐ Collaborate with the Enterprise to gather overarching requirements. **Leverage data tagging solutions/standards:** ☐ Leverage data tagging standards, from Activity 4.1.1 (Discovery) – *Data Analysis*. ☐ Leverage the Component key access store, from Activity 4.2.1 (Phase One) – *Define Data Tagging Standards*, as the single source of truth on tagging standards. ☐ Leverage the Component Data Loss Prevention (DLP) policy, from Activity 4.6.1 (Phase One) – *Implement Enforcement Points*. ☐ Create a detailed mapping document connecting data tagging standards, from Activity 4.1.1 (Discovery) – *Data Analysis*, to specific FAM monitoring requirements, ensuring semantic alignment between tags and monitoring rules. ☐ Develop technical integration specifications for how the FAM solution will interface with the Component key access store to obtain authoritative tag information in real-time. ☐ Define specific DLP policy extensions focused on monitoring critical data with clear documentation of how DLP and FAM solutions will complement each other rather than duplicate functionality.
Select a FAM solution.
Select a FAM solution: ☐ Identify a potential FAM solution that will integrate with the existing: • Data tagging standards • Data, Applications, Assets, and Services (DAAS) • Visibility and Analytics Pillar solutions (e.g., Security Information and Event Management (SIEM), etc.) • Automation and Orchestration Pillar solutions (e.g., Security Orchestration, Automation, and Response (SOAR), Extended Detection and Response (XDR), etc.)

☐ Collaborate with Incident Response (IR) teams to ensure potential FAM solutions meet Enterprise/Component alerting and monitoring requirements, as established in the Component DLP policy.

☐ Create a FAM solution requirements matrix that evaluates capabilities across key dimensions including:

- Support for monitoring structured and unstructured data across diverse repository types.
- Ability to detect and alert on unusual access patterns to critical data.
- Capabilities to identify data misclassification based on content analysis.
- Forensic capabilities to provide detailed activity history for investigations.
- Performance impact assessment under various monitoring configurations.

☐ Develop an integration validation checklist to verify FAM solution compatibility with:

- Both Enterprise and Component-specific data tag formats.
- Existing data repositories and file systems requiring monitoring.
- Specific SIEM/SOAR/XDR solutions currently deployed in the environment.
- Legacy systems containing critical data that may require specialized monitoring approaches.

☐ Establish FAM testing scenarios that simulate critical threat patterns to validate detection capabilities, including:

- Mass file access or downloads of critical data.
- Off-hours access to sensitive repositories.
- Unusual data access patterns indicating potential exfiltration.
- Modification of critical files by unauthorized users.

Develop a FAM solution implementation plan:

☐ Develop a detailed phased deployment roadmap based on critical data prioritization, with clear milestones, dependencies, and success criteria for each Phase.

☐ Create implementation templates for common repository types to accelerate consistent deployment across similar environments.

☐ Establish a deployment verification process that confirms comprehensive monitoring coverage for each critical data repository before proceeding to the next deployment Phase.

☐ Document FAM monitoring exclusions and exceptions with appropriate justifications and compensating controls where direct monitoring isn't feasible.

☐ Develop detailed integration specifications for each security platform, including:

- Data field mappings between systems.
- Event normalization rules to ensure consistent interpretation.
- Bi-directional integration capabilities for coordinated response actions.
- Correlation rules leveraging FAM data to enhance other security detections.

☐ Create integration test scenarios that validate end-to-end workflows from detection through alerting to response across connected systems.

Enhanced Business Rules Implementation:

☐ Develop a comprehensive rule library mapping specific critical data classifications to corresponding detection rules, with clear documentation of:

- Event thresholds triggering alerts.
- Correlation requirements with other security events.
- Response workflows for different alert severities.
- Exceptions handling procedures for authorized deviations.

☐ Create custom rule templates for Component-specific critical data types that may not align with standard Enterprise classifications.

☐ Implement progressive rule deployment starting with monitoring-only mode before enabling alerting and enforcement actions.

Verify and validate FAM functionality.

Test FAM capabilities:

☐ Develop a comprehensive test plan with specific validation scenarios for each critical data designation, including:

- Tests for detection accuracy across different repository types.
- Performance impact testing under peak load conditions.
- False positive/negative analysis for alert configurations.
- Verification of proper tag interpretation and policy application.

☐ Ensure the selected FAM solution meets the Enterprise/Component-defined requirements.

Manage FAM exceptions.

Manage exceptions:

☐ Files that cannot be monitored or systems incompatible with the FAM are:

- Identified
- Documented
- Approved or Rejected

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

☐ The Enterprise and/or Component determine risks.

☐ Approval is periodically reassessed.

Deploy FAM solution(s).

Implement FAM:

☐ Deploy FAM solution(s) through a phased approach in accordance with Enterprise/Component-defined priorities, risk determination, and operational impacts.

- This Activity is scoped to critical data.

☐ Implement business rules to consume critical data designations and manage outcomes in accordance with the Component DLP policy.

☐ Integrate the FAM solution(s) with Visibility and Analytics and Automation and Orchestration Pillar solutions, to include:

- SIEM
- SOAR
- Endpoint Detection and Response (EDR)
- User and Entity Behavior Analytics (UEBA)

Verify and validate FAM solution(s) integration.

Verify and validate:

☐ Ensure the FAM solution(s) meets the needs of the Component and align with Enterprise requirements after implementation.

☐ Confirm that the operational impact of the FAM solution is acceptable to the Component.

☐ Periodically reassess the functionality of the FAM solution(s) to ensure comprehensive coverage and compliance with Enterprise/Component requirements.

☐ Create processes for periodic rule tuning based on false positive/negative analysis and evolving threat patterns.

☐ Where possible, implement continuous monitoring of FAM solution efficiency with metrics tracking:

- Alert-to-investigation ratio measuring detection quality.
- Mean time to detect critical data incidents.
- Coverage percentage across critical data repositories
- Performance impact trending on monitored systems.

Summary

This diagram outlines the Activity 4.4.3 (Phase One) – *File Activity Monitoring Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the critical data classification capabilities provided by 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, as well as the integration of a monitoring system (e.g., Security Information and Event Management (SIEM), Extended Detection and Response (XDR), etc.).

Table 80: Activity 4.4.3 — File Activity Monitoring Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are critical data classifications monitored using FAM tools?

STRATEGIC INSIGHTS
• The Component defines a FAM policy by identifying stakeholders, gathering Enterprise requirements, and aligning with data tagging and Data Loss Prevention (DLP) policies. • The Component demonstrates compliance by selecting FAM solutions that integrate with data tagging, Data, Applications, Assets, and Services (DAAS), SIEM, and Security Orchestration, Automation, and Response (SOAR) while ensuring alignment with alerting and monitoring requirements. • The Component provides evidence through verification and validation testing, confirming that the FAM solution, deployed on critical data, meets Enterprise and Component requirements for security, visibility, and enforcement. • The Component leverages a phased deployment approach, implementing business rules, integrating with SIEM, SOAR, and User and Entity Behavior Analytics (UEBA), and ensuring minimal operational impact. • The Component ensures ongoing compliance through periodic reassessments, refining FAM policies, and maintaining alignment with evolving Enterprise security mandates.

EXPECTED OUTCOMES
1. Data and files of critical data designations are identified and actively monitored. 2. Establish and manage business rules to consume critical data designations and manage outcomes. 3. Integration is in place with monitoring system (e.g., SIEM, XDR).

Capability 4.5 Data Encryption and Rights Management

Table 81: 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) solutions
- Trusted Execution Environments (TEE)

Activity 4.5.1 Implement Data Rights Management (DRM) and Protection Tools Part 1

Table 82: Activity 4.5.1 — Implement Data Rights Management (DRM) and Protection Tools 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 DRM and Protection solution(s) as needed, following the Enterprise standard and requirements. Newly implemented DRM and protection solution(s) are applied to high-risk data objects.	
Predecessor(s)	**Successor(s)**
4.2.2	4.5.2
Expected Outcomes	
• DRM and protection tools are enabled for high-risk data repositories with protections.	
End State	
No high-risk 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 4.2.2 (Phase One) – *Interoperability Standards* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Consider completing Activity 4.4.2 (Discovery) – *Data Rights Management (DRM) Enforcement Point Logging and Analysis* prior to this activity, as the Data Rights Management (DRM) policies will be necessary to complete this activity.
- Activity 4.5.2 (Phase Two) – *Implement Data Rights Management (DRM) and Protection Tools 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 83: Implementation Tasks for Activity 4.5.1 — Implement Data Rights Management (DRM) and Protection Tools Part 1

Review the Enterprise/Component guidelines on DRM policies.
Leverage existing DRM policies: ☐ Review Enterprise/Component guidelines on DRM policies and data taxonomy and ensure compliance adherence. Assess mission-critical data assets and categorize them based on predefined approved rules. • Review Enterprise data classification. • Leverage critical asset mapping. **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, such as: • PDP • PEP • Time-based restrictions **Review DRM technical requirements:** ☐ Refer to the Enterprise technical requirements and industry best practices while selecting a DRM solution. The following is a list of features to consider supporting growth, facilitate integration, enforce compliance, and enhance security. • Encryption capability • Application Programming Interface (API) calls compatibility • Seamless integration • Automated policy enforcement
Implement DRM and data protection solutions.
Leverage the Component DRM solution: ☐ Leverage the Component selected DRM solution, from Activity 4.4.2 (Discovery) – *Data Rights Management (DRM) Enforcement Point Logging and Analysis.* ☐ Ensure the DRM solution meets the requirements established in this activity. ☐ Depending on the regulatory bodies, rules, and requirements, the compliance capability should be built into all DRM solutions to help maintain adherence to legal and regulatory compliance. • Compliance support • Violation reporting

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.

- Audit logs
- Real-time monitoring
- License expiration and management
- Distribution of decryption keys

Implement DRM solution:

☐ Deploy the DRM solution on high-risk data, as defined in the Global key access store and Component Data Catalog, and test extensively to verify and validate that the expected outcomes were achieved.

- Adhere to Enterprise/Component DRM policies.
- Leverage vendor recommendations.
- Test system integration and compatibility.

☐ Develop automation playbooks for policy enforcement.

Encrypt sensitive data:

☐ Implement and deploy a strong and vetted Key Management System (KMS) to restrict access to encryption keys only to approved identities.

☐ Enable encryption of sensitive 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 to high-risk data assets and enable DRM protection-based access control to only allow approved Users and identities.

- Multi-Factor Authentication (MFA)
- Attribute-Based Access Control (ABAC)
- Data Loss Prevention (DLP)

Review data privacy protection under DRM policies:

☐ Review all applicable data privacy guidelines to maintain established Personal Identity Verification (PIV) requirements. Leverage industry best practices, such as Federal Information Processing Standards (FIPS) 201, to verify and validate compliance.

Enhance existing Identity and Access Management (IAM) policies to verify, validate, and automate DRM enforcement: ☐ Review IAM access control policies to verify and validate the capability to automatically grant or revoke license rights based on User/Person Entity (PE)/Non-Person Entity (NPE) attributes, roles, permissions, behavior, and data sensitivity levels.
Verify and validate DRM protection compliance on high-value targets and critical data.
Ensure data is encrypted: ☐ Verify and validate that high-risk 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 that activity/events are ingested and actioned by Component Visibility and Analytics and/or Automation and Orchestration solutions.
Enable continuous DRM policy testing and data activity monitoring.
Track and monitor data usage: ☐ Enable tracking of illegal, unapproved distribution of proprietary and sensitive data assets. ☐ Leverage geo-location to enforce data access restrictions to safeguard critical data assets. ☐ Enable access logs monitoring to track content and approved device management. ☐ Review device binding and offline access authorization in compliance with mission requirements. ☐ 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 4.5.1 (Phase One) – *Implement Data Rights Management (DRM) and Protection Tools Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the incorporation of Data Rights Management (DRM) and protection solutions for high-risk data repositories. It presents strategic insights that drive implementation and expected outcomes, including enabling DRM and protection solutions for high-risk data repositories with robust protections.

Table 84: Activity 4.5.1 — Implement Data Rights Management (DRM) and Protection Tools Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are DRM and protection tools enabled for high-risk data repositories?

STRATEGIC INSIGHTS
• The Component defines DRM policies by reviewing Enterprise guidelines, classifying mission-critical data, and aligning with approved data protection rules. • The Component demonstrates compliance by enforcing DRM protections, leveraging Policy Decision Points (PDP) and Policy Enforcement Points (PEPs), and implementing time-based access restrictions. • The Component provides evidence through DRM technical verification and validation, ensuring encryption, automated policy enforcement, and seamless integration with Enterprise security frameworks. • The Component leverages asset alignment and license management by maintaining audit logs, enabling real-time monitoring, and deploying centralized license verification and validation for DRM enforcement. • The Component ensures ongoing compliance through continuous DRM policy testing, data activity monitoring, and adherence to regulatory requirements, thereby safeguarding sensitive data against unapproved distribution.

EXPECTED OUTCOMES
1. DRM and protection tools are enabled for high-risk data repositories with protections.

Capability 4.6 Data Loss Prevention (DLP)

Table 85: 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) solutions
- Policy Enforcement Points (PEPs)

Activity 4.6.1 Implement Enforcement Points

Table 86: Activity 4.6.1 — Implement Enforcement Points

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) is aligned to and strengthened by Data Privacy and Protection (DPP). Then through attribution, attributes can be injected that address where data is coming from, its movement across ZT control boundaries, and the invocation of protection measures (e.g., encryption, obfuscation, etc.). Data loss prevention (DLP) solution is deployed to the in-scope enforcement points. It is recommended to start with "monitor-only" and/or "learning" mode to limit impact. Collaboration with cyber functions should occur with respect to any observed data loss activity.	
Predecessor(s)	**Successor(s)**
4.3.1	5.4.3
Expected Outcomes	
• A formal process is established with cybersecurity to share loss activity observations. • Identified enforcement points have DLP tool deployed.	
End State	
DLP solutions are effectively deployed at all identified enforcement points and operating in monitor only mode with standardized logging. Policies are continuously refined based on DLP results to ensure robust data protection and risk management. Collaborative efforts are established to share insights and strategies, enhancing overall data loss prevention activities 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 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools* 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 comprehensive device inventory is necessary to ensure DLP is deployed across all necessary devices.
- Consider completing Activity 3.1.1 (Discovery) – *Application and Code Identification* prior to this activity, as a comprehensive data flow inventory is necessary for successful DLP implementation.
- Consider completing Activity 4.1.1 (Discovery) – *Data Analysis* prior to this activity, as data sensitivity/classification is critical to Data Loss Prevention (DLP) activities.

- Consider completing Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP) Enforcement Point Logging and Analysis* prior to this activity, in order to leverage the established Component DLP policy.
- Activity 5.4.3 (Phase Three) – *Process Micro-Segmentation* 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 87: Implementation Tasks for Activity 4.6.1 — Implement Enforcement Points

Ensure the Component DLP policy supports the loss activity detection process.
Loss activity coordination: ☐ Review the Component DLP policy, established in Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP) Enforcement Point Logging* and *Analysis,* and enhance it with specific Data Privacy and Protection (DPP) alignment, ensuring coordination with Incident Response (IR)/Cybersecurity service providers. • DPP alignment includes policies, practices, and technologies implemented by Components to safeguard personal data from unauthorized access, use, or disclosure. ☐ Extend the existing policy actions for handling loss activity (e.g., detection, coordination, response) by adding privacy-specific considerations, such as: • Privacy impact assessment requirements. • Data subject notification procedures. • Privacy-enhancing technologies implementation criteria. • Cross-border data transfer restrictions. ☐ Develop attribute injection frameworks that identify, enable, and address: • Data provenance tracking across ZT control boundaries. • Privacy classification metadata preservation during data movement. • Contextual privacy requirements based on data location and use. ☐ Leverage enforcement points and analyze additional DPP-specific requirements, established in Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP) Enforcement Point Logging and Analysis*, such as: • Privacy-specific data filtering requirements.

- Encryption requirements for different data classifications.
- Obfuscation needs for sensitive personal information.
- Consent verification mechanisms at enforcement boundaries.

☐ Develop attribute-based enforcement specifications that define:

- How data origin attributes affect protection requirements.
- How movement across boundaries triggers specific protections.
- When encryption or obfuscation measures should be invoked
- What privacy metadata must be preserved during transfers.

Deploy enforcement points and decision points.

Deploy decision points:

☐ Evaluate and enforce access requests against predefined access control policies using Identity Access Management (IAM) policies, device posture, and Data, Applications, Assets, and Services (DAAS) context to authorize system resource access. Enable effective policy enforcement by:

- Automating policy orchestration.
- Leveraging a centralized policy repository.
- Continuously evaluating access policies for accuracy and effectiveness.

☐ Extend the evaluation capabilities, from Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP) Enforcement Point Logging and Analysis*, to incorporate privacy-specific decision factors by:

- Using IAM policies from existing systems.
- Incorporating device health assessments from existing monitoring.
- Adding DAAS information.

☐ Enhance policy orchestration by:

- Integrating privacy requirements into the decision framework.
- Adding attribute-based privacy controls to the decision logic.
- Implementing privacy impact assessment triggers at boundaries.
- Creating privacy-specific enforcement actions.

☐ Leverage the centralized policy repository, from Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP) Enforcement Point Logging and Analysis*, to add the following, as applicable:

- Privacy regulation compliance requirements
- Data subject rights enforcement rules
- Purpose limitation constraints
- Jurisdictional privacy requirements

Establish enforcement points:

☐ Build upon the enforcement point identification, from Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP)* Enforcement *Point Logging and Analysis*, by implementing enhanced capabilities through:

- Configuring enforcement points to recognize privacy-related attributes.
- Enabling attribute-based privacy protections at boundaries.
- Implementing encryption and obfuscation capabilities.
- Deploying advanced DLP monitoring with privacy awareness.

☐ Enhance the rule-based engine with specific privacy protection capabilities:

- Content-aware privacy rule evaluation
- Context-sensitive privacy enforcement
- Attribute-based privacy decisions
- Regulatory compliance validation

☐ Implement enhanced enforcement policies that:

- Apply appropriate protection measures based on privacy attributes.
- Enforce consistent privacy controls across similar data types.
- Adapt privacy protections based on context and use.
- Address specific regulatory requirements for different jurisdictions.

☐ Evaluate decision access policies and enforce policy-based decisions. Communicate with Policy Decision Points (PDPs) to consistently enforce policies, such as:

- Enable a rule-based engine.
- Implement enforcement policies.
- Establish real-time communication.

Implement DLP solutions to the in-scope enforcement points using "Learning Mode” and/or “Monitor Only" mode.

Implement DLP solutions:

☐ Leverage the in-scope enforcement points defined earlier and implement DLP in "Monitor Only" mode to:

- Gather baseline data on privacy impacts before enforcement.
- Document potential privacy issues without disrupting operations.
- Test privacy attribute handling across boundaries.
- Ensure alignment with organizational Componential security policies and compliance requirements.

☐ Ensure alignment with Component security and privacy policies by:

- Monitoring privacy impact indicators.

- Validating privacy protection effectiveness.
- Identifying potential privacy compliance gaps.

☐ Configure the DLP solution to specifically monitor key aspects, such as:

- Protection measure application based on data attributes.
- Privacy metadata preservation during transfers.
- Encryption and obfuscation effectiveness.
- Privacy boundary crossing events.

Implement cybersecurity collaboration for privacy incidents.

Enhanced cyber collaboration:

☐ Building on the collaboration foundations establish specific processes for privacy incidents, for example:

- Specialized privacy breach reporting workflows.
- Privacy-focused incident classification criteria.
- Privacy Subject Matter Expert (SME) engagement protocols.
- Privacy regulatory notification requirements.

☐ Create privacy-enhanced collaborative analysis procedures, such as:

- Privacy impact assessment integration
- Data subject impact analysis methods
- Regulatory compliance evaluation

Observe and define baseline activity.

Establish baselines:

☐ Conduct an assessment and develop baseline profiles for acceptable use policy, approved security posture, and vulnerability management.

☐ Leverage the assessment approaches, from Activity 4.4.1 (Discovery) – *Data Loss Prevention (DLP) Enforcement Point Logging and Analysis*, to develop privacy-specific baseline profiles, such as:

- Privacy-focused acceptable use patterns.
- Normal privacy attribute handling behaviors.
- Typical privacy boundary crossing patterns.
- Expected privacy protection measure application.

☐ Develop privacy-enhanced behavior profiles accounting for:

- Privacy-compliant access patterns.
- Proper handling of privacy-sensitive data.
- Appropriate application of privacy controls.

☐ Implement privacy-aware anomaly detection that identifies:

- Unusual privacy attribute modifications.
- Unexpected privacy boundary crossings.
- Abnormal privacy protection bypass attempts.
- Potential privacy compliance violations.

☐ Leverage historical system events and logs to define what is an approved normal system and User/Person Entity (PE)/Non-Person Entity (NPE) behavior.

- Develop approved behavior profiles.
- Implement anomaly detection.
- Develop data as a service expected baselines.

Conduct continuous verification and validation of DLP implementation.

Continuously assess DLP solutions:

☐ Implement comprehensive validation measures that focus specifically on privacy enhancements, such as:

- Privacy attribute preservation testing.
- Privacy protection effectiveness verification.
- Privacy boundary control validation.
- Privacy regulatory compliance assessment.

☐ Conduct regular assessments to fine-tune enforcement rules.

☐ Ensure minimal operational impact while maintaining data security.

☐ Establish real-time communication between enforcement points and policy management systems.

Summary

This diagram outlines the Activity 4.6.1 (Phase One) – *Implement Enforcement Points* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the identification and monitoring of enforcement points for Data Loss Prevention (DLP) solutions. It presents strategic insights that drive implementation and expected outcomes, including the establishment of a formal process for sharing loss activity observations with cybersecurity.

Table 88: Activity 4.6.1 — Implement Enforcement Points - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are identified enforcement points for DLP tools deployed and set to monitor mode?
STRATEGIC INSIGHTS
• The Component defines a DLP policy that coordinates loss activity detection, ensuring alignment with Incident Response (IR) and cybersecurity service providers. • The Component demonstrates compliance by deploying decision and enforcement points, leveraging Identity and Access Management (IAM) policies, Policy Decision Points (PDP), and automated policy orchestration to enforce access controls. • The Component provides evidence through "Learning Mode” and/or “Monitor Only" mode deployment, baseline activity assessments, and anomaly detection to refine enforcement strategies while minimizing disruptions. • The Component leverages continuous verification, validation, and monitoring to adjust DLP enforcement rules, optimize policy effectiveness, and maintain compliance. • The Component ensures real-time communication between enforcement points and policy management systems to sustain ongoing security and operational integrity.
EXPECTED OUTCOMES
1. A formal process is established with cybersecurity to share loss activity observations. 2. Identified enforcement points have DLP tool deployed.

Network and Environment Pillar

Capability 5.1 Data Flow Mapping

Table 89: Capability 5.1 — Data Flow Mapping

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	5.1 - Data Flow Mapping
Description	
DoW Components reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources specifically tagging programmatic (e.g., API) access when possible.	
Impact to ZT	
Sets the foundation for network segmentation and tighter access control by understanding data traffic on the network.	

Scenario

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

- The Component begins by gathering network traffic data to identify and document data flows across all systems, applications, and Data, Applications, Assets, and Services (DAAS) resources.
- Traffic patterns are mapped and visualized using specialized tools, highlighting connections between Users/Person Entities (PEs), devices, applications, and data repositories.
- Programmatic access, such as Application Programming Interface (API) traffic, is identified and tagged to differentiate it from User/PE or device-generated data flows, ensuring more granular insights into network activity.
- Analysis of the mapped data flows reveals several unapproved or unexpected connections between systems, prompting further investigation.
- Granular access control rules and policies are defined based on the mapped data flows, ensuring that only approved Users/PEs, devices, and services can interact with specific network segments and resources.
- During implementation, the Component applies these policies to enforce network segmentation, isolating sensitive resources and limiting exposure to unapproved traffic.

- A routine review of data flow maps reveals an anomaly: A device is attempting to access DAAS resources outside its designated scope. The connection is automatically blocked and an alert is raised.
- The Component integrates continuous monitoring tools to ensure that changes in network traffic patterns are detected and updated in the data flow maps in near real-time.
- Security analysts utilize visualized data flow maps to verify and validate compliance with Zero Trust (ZT) principles, identifying opportunities for additional network segmentation and policy refinement.
- By reconciling, mapping, and visualizing data flows, the Component gains a comprehensive understanding of its network traffic, enabling tighter access controls, enhanced segmentation, and improved protection of network and 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 mapping and visualizing data flows, Components can identify unapproved access attempts and anomalies, leading to improved security posture.
- Improved Compliance: Continuous monitoring, verification, and validation against ZT principles help Components maintain compliance with regulatory requirements.
- Granular Access Control: This capability enables the definition of precise access control policies, ensuring that only approved users, personnel, and devices can access sensitive resources.
- Informed Decision-Making: With a comprehensive understanding of network traffic, Components can make better-informed decisions regarding network segmentation and resource allocation.
- Proactive Threat Management: Continuous monitoring and real-time alerts enable Components to respond swiftly to potential threats, reducing the risk of data breaches.

Technology

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

- Anomaly Detection
- API Gateway and Management solutions
- API Integration Frameworks
- Behavioral Analytics solutions
- Monitoring and Analytics solutions
- Threat Intelligence Platform (TIP)

Activity 5.1.2 Define Granular Control Access Rules and Policies Part 2

Table 90: Activity 5.1.2 — Define Granular Control Access Rules and Policies 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 data tagging and classification standards to develop data filters for API access to the SDN or alternative networking approach. API Decision Points are formalized within the SDN or alternative network architecture and implemented with non-mission/task-critical applications and services.	
Predecessor(s)	**Successor(s)**
5.1.1	None
Expected Outcomes	
• Define data tagging filters for API infrastructure to support interoperability. • Enforce authentication for all APIs at the API layer.	
End State	
Security is enforced at an API level to strengthen authorization and authentication, promote enabling encryption protocols, and support monitoring of malicious behavior at an API level to improve incident response.	

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 5.1.1 (Discovery) – *Define Granular Control Access Rules and Policies Part 1* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Consider completing Activity 3.4.1 (Phase One) – *Resource Authorization Part 1* prior to this activity, to identify and integrate Application Programming Interface (API) decision points for non-mission or task-critical applications within the Software-Defined Networking (SDN) environment.
- Consider completing Activity 4.2.2 (Phase One) – *Interoperability Standards* prior to this activity, to ensure prerequisite API interoperability and tagging standards are in place.
- Consider completing Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools* prior to this activity, to obtain data tagging and classification standards.
- Leverage Infrastructure as Code (IaC) for future growth.

- Enforce micro-segmentation.
- Leverage SDN technologies.
- Develop or adopt policy management solutions.
- Enable Authentication Decision Point, Application Delivery Control Proxy, and segmentation gateways automation implementations.
- Ensure all deployed implementations are adequately scaled. Establish, contain, and maintain a baseline of necessary APIs and other programmatic interfaces that enable SDN-grouped microservices or alternative networking approach functionalities.
- Leverage API gateways to manage and reduce attack surface area exposed with API communications.

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 91: Implementation Tasks for Activity 5.1.2 — Define Granular Control Access Rules and Policies Part 2

Leverage data tagging and classification standards, from Activity 4.3.1 (Phase One) – *Implement Data Tagging and Classification Tools,* to develop data filters for API access within the SDN infrastructure.
Develop data filters for API access: ☐ Identify all query parameters susceptible to enhancing API technology security, efficiency, and data filtering. Develop a dataset for specific criteria to help retrieve security metrics. Develop a standardized query language syntax for API filtering based on: • Representational State Transfer (REST) API Endpoint • API query parameters • Parsing capability for query parameters **Design query parameters for API:** ☐ Establish clear and descriptive parameters for query requests. Facilitate developer and tool understanding of API functions associated with specific queries, including: • Define error handling. • Develop comprehensive documentation. ☐ Identify API functions.

Leverage Activity 4.2.2 (Phase One) – *Interoperability Standards,* to enable interoperable API tagging.

Integrate tagging policies with API management:

☐ Apply policies at the API gateway to enable API management for common scenarios such as authentication, caching, and transformation of requests or responses. Configure and standardize policies to support:

- Reference to approved API management policy templates.
- Extensible Markup Language (XML) to JavaScript Object Notation (JSON) format conversion.
- Standardized API policy configurations for consistency and interoperability.

Enable data tagging across:

☐ Ensure that API tags can communicate with different data sources. Enable interoperability between API tagging and existing security tools policy enforcement across platforms. Establish and document an API tagging schema that includes:

- Defined access control requirements for APIs to govern data exposure and interactions.

Leverage Activity 3.4.1 (Phase One) – *Resource Authorization Part,* to identify, document, and integrate API decision points to all non-mission/task-critical applications and services within the SDN architecture.

Dynamic documentation and reference for API integration:

☐ Where possible, establish or implement an API management solution that supports dynamic documentation and real-time updates to APIs. Incorporate automation capabilities such as:

- Dynamic documentation generation and synchronization.
- Pipeline automation for continuous API integration and updates.
- Documentation generators to maintain accurate, real-time API references.

API security and SDN:

☐ Leverage SDN technology and API gateways to enforce security policies at granular levels and encrypt data in traffic. SDN provides centralized visibility into network traffic. Require all API communications to be executed over secure channels and protocols (e.g., Hypertext Transfer Protocol Secure (HTTPS), mutual Transport Layer Security (mTLS), etc.). This provides:

- Traffic visibility
- Adaptive security

☐ Adopt policy-based management.

Enforce API authentication and migration throughout the SDN platform.

Identify API gateway points:

☐ Establish API gateways as entry points for API traffic throughout the SDN platform. Leverage API gateways to enforce security policies (e.g., authentication, authorization, etc.) at key locations, such as:

- Edge gateways
- Internal gateways
- Micro-segmentation points
- Service-to-service authentication points

Enforce authentication policies:

☐ Implement API gateways to act as a proxy for different third-party and client requests. Enable third-party integrations to enhance security and scalability and maintain traffic visibility. Enable the following capabilities:

- API management
- Access control
- Secure traffic control
- Data protection through encryption

API migration planning:

☐ Verify and validate API/service compatibility with the authorization gateways.

☐ Develop API/service migration roadmap/implementation plans.

Enable continuous API integration testing, verification, and validation.

Set up test environment:

☐ Whenever applicable, create a replica of the production environment dedicated to functional testing, positive testing, and non-functional testing to include different scenarios:

- Endpoint validation
- Input/Output validation
- Create, Read, Update, and Delete (CRUD) operations
- Test data preparation

Select the most appropriate testing solutions:

☐ Leverage automation to select testing solutions compatible with dependent services to ensure comprehensive testing and API response validation.

Test reporting, logging, verification, and validation:

☐ Analyze each test result to identify issues, malfunctions, and vulnerabilities.

☐ Generate comprehensive test reports with details concerning mitigation actions required, anomalies found, and a summary of the test results.

☐ As much as possible, automate the test reporting, logging, and data input verification and validation of the testing environment to improve efficiency and ensure continuous threat detection and reporting.

Summary

This diagram outlines the Activity 5.1.2 (Phase One) – *Define Granular Control Access Rules and Policies Part 2* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on defining and implementing data tagging filters for Application Programming Interface (API) access to the Software-Defined Networking (SDN) infrastructure. It presents strategic insights that drive implementation and expected outcomes, including defining data tagging filters for API infrastructure to support interoperability and enforcing authentication for all APIs at the API layer.

Table 92: Activity 5.1.2 — Define Granular Control Access Rules and Policies Part 2 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are data tagging filters being defined and implemented for API access to the SDN infrastructure?

STRATEGIC INSIGHTS
• The Component defines the requirements for developing API data filters within the SDN infrastructure by leveraging existing data tagging and classification standards to structure query parameters, security metrics, and standardized API syntax. • The Component demonstrates a structured approach to integrating tagging policies with API management by documenting interoperability requirements, establishing access controls for APIs, and ensuring alignment with Enterprise interoperability standards. • The Component provides a documented framework for identifying API gateway points, enforcing authentication policies, and mapping API decision points to non-mission/task-critical applications and services within the SDN architecture. • The Component leverages API management policies, security tagging schemas, and gateway enforcement mechanisms to support secure API communications, structured data transformation, and consistent policy enforcement across different platforms. • The Component ensures continuous verification and validation of API security and functionality by establishing test environments, selecting appropriate testing tools, and automating test reporting, logging, and threat detection for ongoing assessment and compliance monitoring.

EXPECTED OUTCOMES
1. Define data tagging filters for API infrastructure to support interoperability. 2. Enforce authentication for all APIs at the API layer.

Capability 5.2 Software-Defined Networking (SDN)

Table 93: 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 5.2.2 Implement Software-Defined Networking (SDN) Programmable Infrastructure

Table 94: Activity 5.2.2 — Implement Software-Defined Networking (SDN) Programmable Infrastructure

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
Following the API standards, requirements, and SDN API functionalities, DoW Components will implement Software-Defined Networking (SDN) or alternative networking approach infrastructure to enable automation tasks. Segmentation gateways and authentication decision points are integrated into the SDN or alternative networking approach infrastructure along with output logging into a standardized repository (e.g., SIEM, log analytics, etc.) for monitoring and alerting.	
Predecessor(s)	**Successor(s)**
5.2.1, 6.6.2	None
Expected Outcomes	
• Components implement application delivery control proxy. • Components integrate authentication decision points. • Components implement segmentation gateways.	
End State	
The SDN or alternative networking approach infrastructure is fully implemented across Components, with segmentation gateways and authentication decision points integrated and operational. Comprehensive logging and monitoring are established through SIEM and log analytics, ensuring continuous oversight and rapid response capabilities. The automation of these processes enhances network security, efficiency, and compliance with ZT principles.	

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 5.2.1 (Discovery) – *Define Software-Defined Networking (SDN) Application Programming Interfaces (APIs)* and Activity 6.6.2 (Phase One) – *Standardized Application Programming Interface (API) Calls and Schemas Part 1* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- Design the Software-Defined Networking (SDN) architecture.
- Outline technical requirements for the data-forwarding function.
- Select an SDN controller compatible with all applicable protocols.
- Develop Application Programming Interface (API) gateway integration.
- Adopt policy enforcement.
- Implement network virtualization and automation.

- Enable containerization technologies.
- Deploy software-programmable infrastructure, avoiding vendor lock-in.
- Develop network orchestration workflows.
- Promote open-source technologies.
- Develop automation and dynamic scaling workflows.
- Develop data flow mapping diagrams.

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 95: Implementation Tasks for Activity 5.2.2 — Implement Software-Defined Networking (SDN) Programmable Infrastructure

Implement SDN infrastructure to leverage a centralized log repository (e.g., Security Information and Event Management (SIEM)) for monitoring, analytics, alerting, etc.).
Define objectives and scope: ☐ Clearly define and identify use cases pertinent to the business and mission needs related to network performance, security posture enhancement, and threat detection capability. Determine specific metrics and analytics requirements for the SDN. Key elements to consider: • Validate mission use case. • Assess the current environment. • Address any existing roadblocks or challenges. • Review, verify, and validate design with vendors, Subject Matter Experts (SMEs), and stakeholders. **Design SDN architecture:** ☐ Prioritize an API-driven networking architecture. Leverage the SDN as a centralized platform to deploy Information Technology (IT) infrastructure and to manage, secure, and direct traffic and data flows across the environment. Key considerations include: • Consider simplified network design principles. • Account for cloud computing and hybrid deployment requirements. • Evaluate on-premises versus cloud-based environment configurations. • Align with interoperability requirements and open standards.

Deploy SDN controller and network endpoints:

☐ Design, procure, and build an approved SDN infrastructure compatible with a centralized deployment approach around an SDN controller. Deploy southbound and northbound APIs to facilitate communication among the three (3) layers:

- Application layer to communicate with the data plane to manage network applications and services.
- Control layer to communicate with the control plane, acting as the command center of the network management platform.
- Infrastructure layer to communicate with different physical network endpoints (e.g., routers, switches, etc.) that move data packets.

Implement logging configuration:

☐ Enable support for logging capability across all managed network resources. Standardize log format across the network infrastructure to facilitate interoperability and log analysis. Collect log events from all sources, including:

- User/Person Entity (PE) activity
- Applications and services
- Network devices
- API gateways

Select a centralized log repository:

☐ Establish requirements for the log repository and ensure they align with Enterprise specifications. Define storage requirements such as data-at-rest encryption, out-of-band management, and data retention policy. Key features to consider:

- Ensure log integrity.
- Enable access-control policy to log repository.
- Configure strong encryption on log storage.
- Enable real-time log streaming capability.

Integrate logging with the main controller:

☐ Deploy the SDN controller so logs from different network sources can be collected and centralized. Leverage syslog configurations on network devices over a secure channel to deliver logs to the log repository. Leverage API integration to secure logs from applications and services. Key features to consider:

- Syslog configuration.
- Create a virtual private network segment for log delivery.
- Implement critical event alerting.
- Develop log enrichment capability for event correlation.

Implement SDN infrastructure to automate tasks in accordance with API standards, requirements, and SDN API functionalities.

Define automation goals:

☐ Establish automation goals and objectives. Automate the provisioning of network resources using APIs to build and modify network configuration templates. Automate the deployment and enforcement of security policies. Leverage network telemetry to automate alert generation on key performance metrics. Some key features to consider:

- Network resources provisioning
- Dynamic resource scaling
- Dynamic policy enforcement
- Workflow creation and deployment

Identify API standards and requirements:

☐ Develop or adopt APIs, following industry standards and best practices. Develop specific requirements tailored to mission needs and operational constraints. Some recommended key features to consider:

- Client-server architecture
- Statelessness
- Cacheability capability
- Layered system
- Uniform interface
- Resource-based
- Standardized methods

Leverage SDN API functionalities:

☐ Leverage SDN APIs to provide a control plane abstraction to allow centralized network management. Adopt a diversity in protocol, supporting interoperable communications between network components. Key features to consider:

- Network programmability
- Zero-touch provisioning
- Network security
- Centralized management
- Application performance
- Portability across different platforms
- Scalability and flexibility

Integrate Authentication Decision Points within the SDN infrastructure, forwarding output logging into the standardized log repository (e.g., SIEM, Log Analytics, etc.) for monitoring and alerting.

Enable analytics and alerting:

☐ Develop real-time/near real-time analytics capability for the centralized log repository based on business or mission requirements. Enable logs and historical data analysis to set up alerts for critical events. Implement powerful search engines for faster query requests. Key features to consider:

- Develop dashboards for visualization.
- Implement anomaly detection.
- Review performance metrics.
- Automate Incident Responses (IRs).

Implement network decision and enforcement points:

☐ Define policy rules leveraged by Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) to grant or deny access to network resources. Enforce access control policies. Monitor and evaluate resource access by applying predefined rules, ensuring compliance with security policies. Key features to consider:

- Dynamic security
- PEP
- PDP
- Policy Information Point (PIP)
- Policy Administration Point (PAP)
- Attribute-Based Access Control (ABAC)

Implement segmentation gateways.

Enable network segmentation:

☐ Implement segmentation gateways to isolate parts of the network and reduce the attack surface. Introduce enforcement points between network segments for packet inspection and access control. Enable and deploy network security zones to further protect the SDN infrastructure. Key features to consider:

- Software-defined access policy
- Group-based policy
- Role-based policy

Implement secure communication protocols:

☐ Design and deploy a robust security framework for SDN by adopting secure network communication.

☐ Enable device authentication.

☐ Ensure data encryption in transit by leveraging secure protocols, such as the latest Transport Layer Security (TLS) or Secure Shell (SSH), etc., for remote access management. Some secure protocols to consider:

- TLS, Hypertext Transfer Protocol Secure (HTTPS), provides end-to-end encryption for network communications.
- SSH for remote access and infrastructure management.
- Internet Protocol Security (IPsec), for network layer security, provides packet encryption and authentication.
- Simple Network Management Protocol version 3 (SNMPv3) for network management security.
- Secure Network Configuration (NETCONF) protocol for secure configuration management.
- OpenFlow Protocol Security.

Deny all ports by default:

☐ Adopt the “deny all, permit by exception” strategy rule. Perform a NetFlow analysis to baseline the normal operation status of the environment to restrict the control access policy. Deny all network communications traffic by default and only allow network communications traffic by exception. Key points to consider:

- Review legacy application compatibility.
- Account for unexpected dependencies.
- Adopt a deployment-Phased approach.
- Enable rollback capabilities to avoid critical service interruption.

Implement application delivery control proxy.

Define a strategic placement:

☐ Consider internal segmentation, perimeter boundaries, and remote access requirements before deploying control proxies at the edge and throughout the SDN. Verify and validate a business use case for legacy systems and applications for easy transition. Evaluate the benefits of implementing an Application Delivery Controller (ADC) vs. the traditional Virtual Private Network (VPN). Key features to consider:

- Legacy systems and application requirements
- Remote Access Policy
- Multi-tenancy support

Establish key functions:

☐ ADCs perform multiple functions. Some key functions to consider are:

- Reverse proxy
- Load balancing
- TLS offloading
- Traffic optimization

- Health monitoring
- Distributed Denial-of-Service (DDoS) protection
- Web application firewall
- Central authentication
- Multi-tenancy support
- Caching

Summary

This diagram outlines the Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the implementation of Software-Defined Network (SDN) programmable infrastructure to support segmentation gateways and authentication decision points. It presents strategic insights that drive the implementation and expected outcomes, including the implementation of Authentication Decision Points, Segmentation Gateway(s), and an Application Delivery Control Proxy.

Table 96: Activity 5.2.2 — Implement Software-Defined Networking (SDN) Programmable Infrastructure - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How is SDN programmable infrastructure being implemented to support segmentation gateways and authentication decision points?

STRATEGIC INSIGHTS

- The Component defines the objectives and architecture for SDN infrastructure by aligning with Enterprise requirements for centralized logging, security monitoring, and automated network management.
- The Component demonstrates a structured approach to SDN implementation by identifying key components, defining Application Programming Interface (API)-driven automation goals, and ensuring network segmentation through Policy-Based Access Control (PBAC) and enforcement points.
- The Component provides a documented framework for integrating authentication decision points, deploying segmentation gateways, and implementing secure communication protocols to protect network traffic and enhance security posture.
- The Component leverages centralized log repositories such as Security Information and Event Management (SIEM) to enhance real-time monitoring, anomaly detection, and automated Incident Response (IR) across SDN environments.
- The Component ensures network resilience by enforcing a "deny all, permit by exception" strategy, securing API communications, and adopting best practices for network segmentation, policy enforcement, and application delivery control proxies.

EXPECTED OUTCOMES

1. Components implement application delivery control proxy.
2. Components integrate authentication decision points.
3. Components implement segmentation gateways.

Capability 5.3 Macro-Segmentation

Table 97: 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/Intrusion Prevention Systems (IDS/IPS)
- Next-Generation Firewall (NGFW)

Activity 5.3.1 Datacenter Macro-Segmentation

Table 98: Activity 5.3.1 — Datacenter 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.	
Description	
DoW Components implement service-based architectures to restrict lateral movement between public and private components of a solutions architecture. Proxy and/or enforcement checks are integrated with the SDN or alternative networking approach solution(s) based on device attributes and behavior.	
Predecessor(s)	**Successor(s)**
None	3.4.1, 3.4.3, 5.4.1
Expected Outcomes	
• Establish proxy/enforcement checks of attributes (device, location, data), access and flow (client, tenant, traffic patterns), and Component principles (asset life cycle, compliance, and policy).	
End State	
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.	

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 1.1.1 (Discovery) – *Inventory User* prior to 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 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 this activity, as a comprehensive list of applications/services is necessary to understand access requirements.
- Consider completing Activity 4.1.1 (Discovery) – *Data Analysis* prior to this activity, as a comprehensive list of data/data types is necessary to understand access requirements.
- Consider completing Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure* prior to this activity, to obtain the Software-Defined Networking (SDN) Application Programming Interfaces (APIs).

- Identify the full extent of the Component environment(s), to include:
  - Traditional networks
  - Hyperconverged Infrastructure (HCI)
  - Cloud offerings/instances
  - Serverless deployments and external service offerings
- The Component has an established Security Information and Event Management (SIEM) solution.
- Automate the detection and remediation of access control failures where possible. Many commercial solutions used for SDN provisioning can also be used for detection and correction.
- If the Component leverages a Cybersecurity Service Provider (CSSP), ensure logging standards are adhered to and monitored appropriately/in accordance with Service Level Agreements (SLAs).
- Activity 3.4.1 (Phase One) – *Resource Authorization Part 1*, Activity 3.4.3 (Phase One) – *Software-Defined Compute (SDC) Resource Authorization Part 1*, and Activity 5.4.1 (Phase One) – *Implement 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 99: Implementation Tasks for Activity 5.3.1 — Datacenter Macro-Segmentation

Define public/private environment segments.
Collaborate with key stakeholders to identify public-facing Data, Applications, Assets, and Services (DAAS): ☐ Identify public DAAS by establishing cross-organizational joint workgroups to collaboratively identify all services and offerings within the environment, along with their operational requirements, accessible to Users/PEs/Non-Person Entities (NPEs) external to the Component.

☐ Leverage the following artifacts/activities to define public/private DAAS:

- 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) – *Data Analysis*

Design a public/private environment architecture:

☐ Develop a public/private environment architecture that places additional safeguards on DAAS that are externally accessed, to include logical segmentation of public resources from private resources, with access enforced at the risk boundaries.

Manage public DAAS that cannot be migrated to a Demilitarized Zone (DMZ) through risk-based exceptions.

Manage exceptions:

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

- Consider how risks can be mitigated to achieve an Enterprise/Component-approved acceptable level.

☐ Public DAAS that cannot be migrated to a DMZ are:

- Identified.
- Documented.
- Approved or Rejected.

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

☐ Approval is periodically reassessed.

Leverage proxy and enforcement checks to restrict movement of entities based on defined segments established in previous section.

Implement Access Control points:

☐ Leverage the SDN APIs, authentication decision points, and implement segmentation gateways, from Activity 5.2.2 (Phase One) –*Implement Software-Defined Networking (SDN) Programmable Infrastructure*.

Enforce service communication security:

☐ Implement secure communication channels to encrypt and protect all service-to-service communications.

- Leverage modern, Enterprise/Component-approved authentication and encryption transport protocols to protect data in transit, including internal/intra-segment traversal.
- Enable secure WebSocket connections.

- Implement cryptographic capabilities to ensure data integrity.

☐ Key features to consider:

- Service mesh
- API gateways
- Mutual Transport Layer Security (TLS)
- Open Authorization 2.0 (OAuth 2.0)/OpenID Connect

Ensure log activities are captured in SIEM.

Monitoring and logging:

☐ Implement centralized logging through secure channels to protect against tampering.

☐ Capture and monitor all access logs, interaction events, and system activities.

☐ Integrate SIEM tools with log repository and SDN infrastructure. Key elements to consider:

- Centralized logging
- Real-time event monitoring
- Network traffic monitoring
- Runtime Application Self-Protection (RASP)

Log collection and aggregation:

☐ Identify all log sources and enable secure log transmission. Review legacy devices, services, and applications for log collection compatibility.

☐ Adopt a collection method, agent-based or agentless, based on system and application requirements, where possible.

☐ Select and deploy a log aggregation solution and verify and validate expected outcomes.

☐ Review and implement log encryption based on Enterprise data governance and retention policy. Key features to consider:

- Secure log transmission, from Activity 5.4.4 (Phase Two) – *Protect Data in Transit*
- Data log storage
- Log collection, processing, analysis, from Activity 7.1.2 (Phase One) – *Log Parsing*
- Leverage API calls to retrieve logs programmatically, using the interoperability standards, from Activity 4.2.2 (Phase One) – *Interoperability Standards*

Analyze activities within the analytics engine.

Activity monitoring and analysis:

☐ Establish monitoring objectives and goals.

☐ Identify monitoring points using segment boundaries and environment perimeter.

☐ Capture and monitor traffic flows between environment segments.

☐ Leverage agent-based or agentless API calls to monitor critical environment access, where possible. Select and implement monitoring tools with built-in analysis capability for anomaly and threat detection. Key elements to consider:

- Available threat intelligence ingestion
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- NetFlow/Flow collectors
- Full packet capture capability
- Real-time analysis and response
- Integration with SIEM/Security Orchestration, Automation, and Response (SOAR) resources

☐ Continuously researching emerging threats and verifying and validating Component macro-segmentation efforts continue to mitigate the risks to the Enterprise/Component level of acceptance.

Summary

This diagram outlines the Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the implementation and enforcement of data center macro-segmentation policies. It presents strategic insights that drive the implementation and expected outcomes, including the establishment of a proxy and enforcement checks for device Attributes, Access, and Flow, as well as component principles.

Table 100: Activity 5.3.1 — Datacenter Macro-Segmentation - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are datacenter macro-segmentation policies being implemented and enforced?

STRATEGIC INSIGHTS
• The Component defines and documents the classification of public and private Data, Applications, Assets, and Services (DAAS), ensuring alignment with Enterprise security policies and regulatory requirements for segmenting external and internal resources. • The Component demonstrates the identification of public-facing DAAS through collaborative workgroups, leveraging existing inventories such as the Component Data Catalog, Application Inventory, Device Inventory, and User Inventory to ensure comprehensive visibility and risk assessment. • The Component provides a structured approach for designing a public/private environment architecture, incorporating logical segmentation and risk-based access controls to safeguard externally accessible resources while enforcing security at the designated risk boundaries. • The Component leverages risk-based exception management by identifying, documenting, and evaluating public DAAS that cannot be migrated to a Demilitarized Zone (DMZ), ensuring appropriate mitigation strategies and periodic reassessments are in place. • The Component ensures continuous enforcement of secure service communication through authentication gateways, Application Programming Interface (API) security, and encryption protocols to protect DAAS interactions.

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, and policy).

Capability 5.4 Micro-Segmentation

Table 101: 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 5.4.1 Implement Micro-Segmentation

Table 102: Activity 5.4.1 — Implement 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 implement micro-segmentation infrastructure into SDN or alternative networking approach environment, enabling basic segmentation of service components (e.g., web, app, DB, etc.), ports, and protocols. Basic automation is accepted for policy changes, including API decision-making. Virtual hosting environments implement micro-segmentation at the host/container-level.	
Predecessor(s)	**Successor(s)**
5.3.1	5.4.2
Expected Outcomes	
• Accept automated policy changes. • Implement API decision points. • Implement distributed Next-Generation Firewall (NGFW)/micro-FW/endpoint agent in virtual hosting environment.	
End State	
Automated policy changes and API decision-making processes are established, enhancing the agility and security of the infrastructure. Virtual hosting environments employ micro-segmentation at the host/container-level, providing robust security controls and improving overall management efficiency. The infrastructure includes integrated application delivery control proxies, SIEM logging, UAM, authentication decision points, and segmentation gateways, ensuring comprehensive security and monitoring 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.

- Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Leverage automated discovery solutions to ensure a complete and comprehensive inventory is obtained.
    - Ensure the Component-approved discovery solutions are given the appropriate environment access to perform their intended tasks.
- Leverage available segmentation capabilities within the virtual hosting environment to isolate hosts or containers to only necessary connections.
- Assumption: Implementers have access to existing Enterprise and/or Component Incident Response (IR) policies and plans, which provide the framework for

identifying, reporting, and remediating access control or segmentation policy violations.

- Activity 5.4.2 (Phase Two) – *Application and Device Micro-Segmentation* 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 103: Implementation Tasks for Activity 5.4.1 — Implement Micro-Segmentation

Define environment micro-segmentation objectives and scope.
Collaborate with key stakeholders to further refine environment compartmentalization: ☐ Identify and collaborate with key stakeholders, including the Enterprise, to develop a micro-segmentation plan to refine the Component public/private architecture to: • Distribute Data, Applications, Assets, and Services (DAAS) across systems with explicit access controls. Examples include: ○ Separating the database from a web server on a different host. ○ Separating security functions, like vulnerability scanning, from non-security dedicated hosts. ○ Separating management functions, like network device administration, from non-management dedicated hosts. • Ensure virtual hosting environments employ micro-segmentation at the host/container level. • Confirm services are provided through application delivery control proxies. Note: These actions will directly support Activity 5.2.3 (Phase Two) – *Segment Flows into Control, Management, and Data Planes.* **Design environment micro-segmentation architecture:** ☐ Extend the Component public/private architecture, from Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation*, to develop a Component micro-segmentation architecture. **Update violation and remediation actions:** ☐ Leverage the Component IR policy/plans. • Identify how the Component will handle access violations and extend the Component IR policies/plans to incorporate these actions.

☐ Identify how the Component will remediate access control failures, such as misconfigured access points, proxies, network Access Control Lists (ACLs), etc.

- Remediation actions could include technical automation and/or manual actions in accordance with the Component's policies and procedures.
- Misconfiguration of access controls could be governed by vulnerability management.

Migrate DAAS to appropriately defined host systems.

Migrate services:

☐ Leverage the micro-segmentation plan and implement a phased approach to:

- Migrate the identified services to new appropriate hosts.
- Configure micro-segmentation on virtual systems/hosts.
- Deploy application delivery control proxies and migrate necessary services.
- Establish minimum necessary access to the services/hosts to support Enterprise/Component requirements, Least Privilege, and Role-Based Access Control (RBAC).

Implement Application Programming Interface (API) decision points.

Implement API decision points:

☐ Leverage the access control points, from Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation*, to secure Component DAAS. Additional access control points are also defined after completing:

- Activity 3.4.1 (Phase One) – *Resource Authorization Part 1* defines authorization gateways.
- Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure* defines authentication decision points and implements segmentation gateways.

Verify and validate DAAS migration.

Verify and validate DAAS migration:

☐ Test, verify, and validate DAAS are accessible, and operational requirements have been maintained.

☐ Test, verify, and validate that DAAS has the minimum necessary access in accordance with Enterprise/Component requirements.

☐ Test, verify, and validate that the final implementation is aligned with the Component micro-segmentation plan and/or update the plan as necessary.

Implement automated policy changes.

Dynamic policy engines:

☐ Implement and integrate dynamic policy engines capable of automatically evaluating and enforcing segmentation, access, and logging requirements in real-time based on predefined rules, contextual attributes, and system state.

☐ Configure automated policies to design, build, and securely deploy consistent container applications.

☐ Enforce dynamic policies through the access enforcement solutions, from Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation*. Key elements to consider:

- Real-time adaptation
- Machine learning
- Orchestration tools

Trigger-based policy updates:

☐ Enable event-based policy updates, such as security alerts, identity profile changes, and logging patterns.

☐ Implement scheduled updates for routine review to ensure compliance with established policies.

Integrate micro-segmentation with Capabilities from the Automation and Orchestration Pillar and the Visibility and Analytics Pillar:

☐ Based on the ZT Automation and Orchestration Pillar:

- Integrate segmentation policy enforcement points with Component automation and orchestration tools to support real-time policy deployment and updates.

☐ Based on the ZT Visibility and Analytics Pillar:

- Ensure all micro-segmentation activities generate and forward logs that align with Component logging and visibility standards.
- Continuously assess segmentation effectiveness, detect policy violations, and validate automated enforcement actions.

Periodic Assessment.

Periodic Assessment:

☐ Periodically reassess that functionality meets operational demands and access control is maintained in accordance with Enterprise/Component policy. The assessment interval is determined by the Enterprise/Component-defined policy, but it is strongly recommended that the interval is no longer than annually.

Summary

This diagram outlines the Activity 5.4.1 (Phase One) – *Implement Micro-Segmentation* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the implementation of micro-segmentation policies automated within Software-Defined Networking (SDN) environments. It presents strategic insights that drive implementation and expected outcomes, including the acceptance of automated policy changes and the implementation of Application Programming Interface (API) decision points.

Table 104: Activity 5.4.1 — Implement Micro-Segmentation - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS

1. How is the implementation of micro-segmentation policies automated within SDN environments?

STRATEGIC INSIGHTS

- The Component defines and documents a micro-segmentation strategy to refine environment compartmentalization, ensuring that Data, Applications, Assets, and Services (DAAS) are distributed with explicit access controls across dedicated systems, supporting Least Privilege and Role-Based Access Control (RBAC) principles.
- The Component demonstrates a structured environment micro-segmentation architecture, extending from the public/private segmentation, from Activity 5.3.1 (Phase One) – *Datacenter Macro-Segmentation*, ensuring logical separation of security functions, management tasks, and hosted services.
- The Component provides a framework for handling access violations and remediation actions, incorporating Incident Response (IR) policies and misconfiguration corrections to address access control failures, and ensuring secure and enforceable segmentation policies are maintained.
- The Component leverages established Access Control Points, including Authorization Gateways, SDN APIs, and Segmentation Gateways, to enforce API decision points for secure DAAS operations, aligning with Enterprise security requirements.
- The Component ensures continuous verification and validation of DAAS migration, enforcing dynamic policy updates based on event-driven triggers, real-time adaptation, and Machine Learning (ML) insights while integrating Automation, Orchestration, and Visibility Analytics to maintain compliance and operational effectiveness through periodic reassessments.

EXPECTED OUTCOMES

1. Accept automated policy changes.
2. Implement API decision points.
3. Implement distributed Next-Generation Firewall (NGFW)/micro-FW/endpoint agent in virtual hosting environment.

Automation and Orchestration Pillar

Capability 6.1 Policy Decision Point (PDP) and Policy Orchestration

Table 105: 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)
- Role-Based Access Control (RBAC)
- Policy Decision Points (PDPs)
- Policy Enforcement Points (PEPs)
- Structured Threat Information eXpression (STIX) protocols
- Trusted Automated Exchange of Intelligence Information (TAXII)

Activity 6.1.2 Organization Access Profile

Table 106: Activity 6.1.2 — Organization Access Profile

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 access profile rules for mission/task and non-mission/task DAAS access using the data from the User, Data, Network & Environment, and Device pillars. The Enterprise works with Components to develop Enterprise security profile rules using the existing Component security profiles to create a common access approach to DAAS. A Phased approach can be used by Components to limit risk to mission-/task-critical DAAS access once the security profile(s) are created.	
Predecessor(s)	**Successor(s)**
None	6.1.3
Expected Outcomes	
• Component scoped profile rules are created to determine access to DAAS using capabilities from User, Data, Network & Environment, and Device pillars. • Initial Enterprise profile rules for access standard is developed for access to DAAS. • When possible, Component profile(s) utilize Enterprise available services in the User, Data, Network & Environment, and Device pillars. • Component mission-/task-critical profile rules are created.	
End State	
The patterns of behavior are established for what outcomes are needed for access control at the Component 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.

- Consider completing Activity 1.1.1 (Discovery) – *Inventory User* and Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, to obtain User/Person Entity (PE)/Non-Person Entity (NPE) inventory lists to ensure Organization Access Profiles are consistently applied across all PEs/NPEs.
- Activity 6.1.3 (Phase Two) – *Enterprise Security Profile Part 1* 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 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 107: Implementation Tasks for Activity 6.1.2 — Organization Access Profile

Leverage User/PE/NPE lists in preparation for defining profile rules for Data, Applications, Assets, and Services (DAAS) access.
Consider completing Activity 1.1.1 (Discovery) – *Inventory User* and Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis,* to obtain User/PE/NPE lists: ☐ Leverage Activity 1.1.1 (Discovery) – *Inventory User,* to obtain an accurate and comprehensive User/PE list as established in the User Pillar. ☐ Leverage Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis,* to obtain an accurate and comprehensive Hardware/Software List as established in the Device Pillar.
Define profile rules for DAAS access using the established User/PE/NPE lists.
Collaborate with Enterprise to establish the DAAS access policy: ☐ Utilize the Enterprise access policy to establish Users/PEs/NPEs profile rules. **Leverage the Enterprise access policy to define Component profile rules for DAAS access:** ☐ Adopt the access policy to define profile rules managing DAAS access for all Users/PEs/NPEs. ☐ Define the levels of access required for each role (e.g., read-only, read-write, administrative, etc.). ☐ Specify conditions and/or constraints for access (e.g., time-based, location-based, frequency, etc.). ☐ Employ a deny-by-default strategy that denies access to all resources by default and only explicitly grants access based on defined roles and responsibilities for all Users/PEs/NPEs. ☐ Finalize profile rules for DAAS access that meet these requirements.
Use profile rules to define and document access profiles across the Component environment using Access Control Lists (ACLs).
Create access profiles that adhere to established profile rules: ☐ Document detailed access profiles for each role (e.g., access permissions, conditions, constraints, etc.). **Deploy ACLs that adhere to access profiles across the Component environment:** ☐ Configure ACLs for all Users/PEs/NPEs to enforce the defined access profiles. ☐ Where applicable, use existing Policy Decision Points (PDPs) solutions to verify and validate that ACLs are operational and functioning as expected.
Extend profile rules to limit mission/task-critical access to DAAS.
Supplement existing profile rules to restrict mission/task-critical access to DAAS within the Component environment for all Users/PEs/NPEs: ☐ Using the existing profile rules, create extended rules to further restrict mission/task-critical access to DAAS.

☐ Update ACL configurations based on these extended profile rules. ☐ Use existing Policy Decision Point (PDP) solutions to verify and validate that updated ACLs are operational and functioning as expected, where applicable.
Review and update profile rules, access profiles, and ACLs to ensure they are in alignment with Enterprise requirements.
Regularly review and update all profile rules, access profiles, and ACLs: ☐ Conduct regular reviews of profile rules and access profiles to ensure they remain effective, and in alignment with Enterprise and Component policies and procedures. ☐ Where applicable, update access profiles and ACLs as needed to reflect roles, responsibilities, and access requirements changes.

Summary

This diagram outlines the Activity 6.1.2 (Phase One) – *Organization Access Profile* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the creation of access profiles for mission and task-related Data, Applications, Assets, and Services (DAAS) access using data from User, Data, Network, and Device pillars. It presents strategic insights driving implementation and expected outcomes that include the creation of Component-scoped profile rules to determine access to DAAS using capabilities from User, Data, Network, and Device pillars.

Table 108: Activity 6.1.2 — Organization Access Profile - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are Component access profiles created for mission and task-related DAAS access using data from User, Data, Network, and Device pillars?
STRATEGIC INSIGHTS
• The Component defines profile rules for DAAS access by leveraging User/Person Entity (PE)/Non-Person Entity (NPE) lists and aligning with Enterprise access policies. • The Component demonstrates compliance by establishing role-based access levels, enforcing a Deny-by-Default strategy, and implementing conditions and constraints for access control. • The Component provides evidence through the deployment of Access Control Lists (ACLs), validating Policy Decision Points (PDPs), and documenting access profiles across the Component environment. • The Component leverages extended profile rules to restrict mission-critical access, updating ACL configurations to enforce stricter access controls where necessary. • The Component ensures ongoing compliance by conducting regular reviews and updates of profile rules, access profiles, and ACLs to maintain alignment with Enterprise security policies and operational requirements.
EXPECTED OUTCOMES
1. Component scoped profile rules are created to determine access to DAAS using capabilities from User, Data, Network & Environment, and Device pillars. 2. Initial Enterprise profile rules for access standard is developed for access to DAAS. 3. When possible, Component profile(s) utilize Enterprise available services in the User, Data, Network & Environment, and Device pillars. 4. Component mission-/task-critical profile rules are created.

Capability 6.5 Security Orchestration, Automation, and Response (SOAR)

Table 109: Capability 6.5 — Security Orchestration, Automation, and Response (SOAR)

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	6.5 - Security Orchestration, Automation, and Response (SOAR)
Description	
DoW Components achieve initial operational capability of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation.	
Impact to ZT	
Predefined playbooks from collection to incident response and triage enables initial process automation that accelerates a security team's decision and response speed.	

Scenario

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

- The Component conducts a response automation analysis to identify repetitive and high-priority tasks in security operations, such as threat detection, vulnerability management, and Incident Response (IR).
- Security Orchestration, Automation, and Response (SOAR) solutions are implemented to centralize and automate the ingestion of alert data from security technologies, including Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs).
- Predefined playbooks are developed for common security incidents, such as phishing attacks, malware detection, and unapproved access attempts, enabling consistent and efficient responses.
- During a routine security scan, a SOAR solution ingests an alert indicating anomalous network traffic, which is indicative of potential malware activity.
- The SOAR solution triggers a playbook that isolates the affected device, conducts a quick malware scan, and sends a notification to the Security Operations Center (SOC).
- The playbook gathers contextual data, such as recent device activity, User/Person Entity (PE) details, and threat intelligence, enriching the alert and reducing the time required for manual investigation.

- A vulnerability in a critical application is identified during threat management. The SOAR solution automates the remediation process by applying patches to affected systems and verifying and validating successful deployment.
- The SOAR solution integrates with the Component's policy orchestration framework to dynamically adjust PEP and PDP rulesets based on the threat level, blocking similar traffic patterns across the network.
- Analytics from SOAR processes are reviewed periodically to refine playbooks, ensuring they remain effective against evolving threats and vulnerabilities.
- By automating alert ingestion, triggering playbooks, and orchestrating policies, the Component accelerates response times, improves decision-making, and enhances its overall security posture.

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 reduces the burden on security teams, allowing them to focus on more complex issues.
- Accelerated IR: Predefined playbooks enable quicker reactions to security incidents, minimizing potential damage.
- Improved Decision-Making: Contextual data gathered during automated processes enhances the quality of decisions made by security teams.
- Enhanced Security Posture: Continuous monitoring and automated remediation help maintain a robust defense against evolving threats.

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)
- Policy Decision Points (PDPs)
- Policy Enforcement Points (PEPs)
- Security Orchestration, Automation, and Response (SOAR)
- Security Information and Event Management (SIEM)

Activity 6.5.2 Implement Security Orchestration, Automation, and Response (SOAR) Tools

Table 110: Activity 6.5.2 — Implement Security Orchestration, Automation, and Response (SOAR) 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 Enterprise, working with Components, develops a standard set of requirements for Security Orchestration, Automation, and Response (SOAR) tooling to enable ZT Target-level functionality. Components use approved requirements to procure and implement a SOAR solution. Infrastructure integrations for future SOAR functionality is completed.	
Predecessor(s)	**Successor(s)**
6.6.2, 6.7.1	None
Expected Outcomes	
• Enterprise develops requirements for SOAR tools. • Components procure SOAR tools. • Components develop Implementation Plan (e.g., Integration Points, Incident Response, Architecture, Interoperability, Scalability, etc.) for SOAR. • Complete full implementation of SOAR.	
End State	
Components conduct appropriate planning to ensure effective implementation of a SOAR tool with relevant connections and interoperability.	

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* and Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as predecessors to this activity.
- When selecting Security Orchestration, Automation, and Response (SOAR) solutions, the Component should consider key features, such as scalability, flexibility, and system integration.
- Assumption: The Component has an established Incident Response (IR) plan in alignment with 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 111: Implementation Tasks for Activity 6.5.2 — Implement Security Orchestration, Automation, and Response (SOAR) Tools

Component assesses and prepares the environment for selection and implementation of SOAR solution(s).
Assess current Component ZT posture and identify gaps: ☐ Perform a gap analysis to determine how existing security automation capabilities support or hinder ZT principles and identify areas of improvement that can be resolved with appropriate SOAR solution(s). ☐ Identify Component-specific security gaps hindering ZT adoption that could be addressed by SOAR solution(s), focusing on automation opportunities for Least Privilege and continuous verification. **Complete predecessor Activity 6.6.2 (Phase One) – *Standardized Application Programming Interface (API) Calls and Schemas Part 1,* in order to:** ☐ Leverage standardized Application Programming Interface (API) calls to enable seamless SOAR solution(s) integration, consistent communication, and secure data exchange across the Component's security infrastructure. **Complete predecessor Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1,* in order to:** ☐ Leverage SOAR workflows to automate key ZT actions, such as access revocation, micro-segmentation changes, verification, and validation of device posture, improving IR and threat mitigation. **Component collaborates with the Enterprise to develop SOAR solution(s) requirements, such as:** ☐ Develop baseline technical and operational requirements in alignment with ZT principles and ZT Target-level functionality. ☐ Define functional capabilities (e.g., IR automation, scalability, threat intelligence integration, etc.). ☐ Reconcile any conflicts between Enterprise cybersecurity policies and ZT principles when implementing SOAR, prioritizing ZT requirements where feasible.
Procure SOAR solution(s) that meet the requirements established above.
Develop procurement strategy: ☐ Determine appropriate procurement approach (e.g., Enterprise-wide contract, individual Component procurements, etc.). ☐ Ensure alignment with Enterprise and Component acquisition policies. **Component evaluates and procures appropriate SOAR solution(s):** ☐ Conduct technical assessments and tool demonstrations before selecting a SOAR solution capable of meeting the Component's requirements and achieving the objectives.

☐ Evaluate SOAR solution(s) based on compliance with established requirements, ZT principles, and Component needs.

☐ Component should procure the relevant SOAR solution(s) based on the evaluation results in alignment with appropriate procurement policies.

Develop initial SOAR functionalities:

☐ Implement baseline configurations and policies to automate actions, such as access requests, security event analysis, and vulnerability remediation in alignment with ZT principles.

☐ Begin initial integrations with the existing Component cybersecurity infrastructure.

Develop and integrate the Implementation Plan for a SOAR solution to enable ZT Target-level functionality.

Develop SOAR Implementation Plan:

☐ Define a phased integration approach based on the Component’s ZT maturity, beginning with automation of foundational capabilities such as Identity, Credential, and Access Management (ICAM), endpoint protection, and network segmentation.

☐ Identify integration points between the SOAR solution(s) and existing security solutions (e.g., Security Information and Event Management (SIEM), threat intelligence platforms, vulnerability management, and endpoint detection and response) to enable contextual data sharing and automated decision-making.

☐ Establish interoperability and scalability standards to ensure SOAR workflows can dynamically orchestrate IR actions, enforce access policies, and adapt to evolving threat conditions across environments.

Implement SOAR solution(s):

☐ Deploy SOAR solution(s) across Components per the Implementation Plan developed above to enable ZT Target-level functionality.

☐ Establish continuous monitoring for dynamic decision-making based on Access Control policies and performance metrics.

☐ Integrate SOAR into the Component's IR plan, automating ZT responses like access revocation and system isolation to enforce Least Privilege and minimize the impact of breaches.

Verify and validate SOAR integration and functionality:

☐ Confirm that SOAR solution(s) perform all required functions specified in the established requirements.

☐ Confirm that SOAR integrations enable automated enforcement of ZT policies, including Access Control policies, data protection policies, and IR playbooks.

☐ Establish continuous monitoring with verification and validation procedures to ensure continued functionality throughout the environment.

Summary

This diagram outlines the Activity 6.5.2 (Phase One) – *Implement Security Orchestration, Automation, and Response (SOAR) Tools* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on Security Orchestration, Automation, and Response (SOAR) tool implementation. It presents strategic insights driving implementation and expected outcomes that include development of requirements and procurement of SOAR tools.

Table 112: Activity 6.5.2 — Implement Security Orchestration, Automation, and Response (SOAR) Tools - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are SOAR tools implemented and what are the requirements for their integration?
STRATEGIC INSIGHTS
• The Component collaborates with the Enterprise to define standardized SOAR requirements, aligning with Enterprise requirements and existing Information Technology (IT) infrastructure compatibility to support mission-critical goals such as automated Incident Response (IR), threat intelligence integration, and security compliance. • The Component procures SOAR solutions that meet operational and security requirements, prioritizing key features such as orchestration, playbook automation, incident management, scalability, and integration capabilities with existing security tools and infrastructure. • The Component develops and implements a comprehensive IR strategy, including robust IR plans, team formation, and SOAR workflows integrated with security telemetry, Application Programming Interface (API) gateways, Policy Enforcement Points (PEPs), and Security Information and Event Management (SIEM) to streamline automated responses and outcome validation. • The Component builds Standard Operating Procedures (SOPs) for SOAR deployment, creating detailed workflows, automation opportunities, and specific use cases, while providing training materials, knowledge-sharing resources, and compliance guidance to operational teams. • The Component implements and validates fully vetted SOAR solutions through real-time monitoring, continuous testing, and automated enforcement to respond to security incidents, ensuring seamless integration, threat intelligence enrichment, network isolation, and Security Operation Center (SOC) reporting for improved operational efficiency and security posture.
EXPECTED OUTCOMES
1. Enterprise develops requirements for SOAR tools. 2. Components procure SOAR tools. 3. Components develop Implementation Plan (e.g., Integration Points, IR, Architecture, Interoperability, Scalability, etc.) for SOAR. 4. Complete full implementation of SOAR.

Capability 6.6 Application Programming Interface (API) Standardization

Table 113: 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 6.6.2 Standardized Application Programming Interface (API) Calls and Schemas Part 1

Table 114: Activity 6.6.2 — Standardized Application Programming Interface (API) Calls and Schemas 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 establish an Application Programming Interface (API) standard (or equivalent automated interchange mechanism), which at least outlines the approved patterns and protocols. Components identify existing APIs and update to the standard.	
Predecessor(s)	**Successor(s)**
None	5.2.2, 6.5.2, 6.6.3
Expected Outcomes	
• API Standard (or equivalent automated interchange mechanism) is established with Component commitment. • Automated pattern and protocol services are implemented.	
End State	
Existing APIs are assessed against automated pattern and protocol services.	

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 3.2.3 (Phase Two) – *Automate Application Security and Code Remediation Part 1* prior to this activity, to obtain identified Application Programming Interfaces (APIs).
- Consider completing Activity 5.2.1 (Discovery) – *Define Software-Defined Networking (SDN) Application Programming Interfaces (APIs) 1* prior to this activity, to obtain the Software-Defined Networking (SDN) API inventory.
- Implementation success may depend on the availability and maturity of API discovery and documentation capabilities. Where possible, leverage standardized approaches such as OpenAPI to ensure consistent schema definitions and improve interoperability across systems.
- Activity 5.2.2 (Phase One) – *Implement Software-Defined Networking (SDN) Programmable Infrastructure*, Activity 6.5.2 (Phase One) – *Implement Security Orchestration, Automation, and Response (SOAR) Tools*, and Activity 6.6.3 (Phase Two) – *Standardized Application Programming Interface (API) Calls and*

Schemas Part 2 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 115: Implementation Tasks for Activity 6.6.2 — Standardized Application Programming Interface (API) Calls and Schemas Part 1

Components collaborate with the Enterprise to establish an API standard that outlines approved patterns and protocols.
Define the API standard or equivalent automated interchange mechanism: ☐ Component collaborates with the Enterprise and considers best practices for existing API standards that support robust authentication/authorization mechanisms (e.g., OAuth 2.0, OpenID Connect, etc.) and data encryption for data in transit and at rest. ☐ Define a comprehensive API standard document that outlines: • Approved patterns, protocols, and security measures. • Logging, monitoring, and Incident Response (IR). • Data formats based on the Enterprise/Component collaboration and industry best practices.
Manage APIs that do not meet standards through risk-based exceptions.
Manage exceptions: ☐ Identify and document APIs that are incompatible with established standards. ☐ Evaluate and document risks associated with each noncompliant API in accordance with Enterprise and/or Component risk assessment policies. ☐ Determine disposition for each API: • Approved with a documented exception, or • Rejected and scheduled for remediation or decommissioning. ☐ Grant approval only when the mission justification outweighs the assessed security risks. ☐ Periodically reassess all approved exceptions to confirm continued necessity and acceptable risk.

Identify and update existing APIs through the adoption of the API standard developed here.

Catalog all existing APIs across the Component:

☐ Identify all APIs within the Component environment(s).

- Where possible, leverage automated discovery tools and create an API catalog with details on usage, data sensitivity, and current security posture.
- Leverage the SDN API inventory, from Activity 5.2.1 (Discovery) – *Define Software-Defined Networking (SDN) Application Programming Interfaces (APIs).*
- Leverage identified APIs, from Activity 3.2.3 (Phase Two) – *Automate Application Security and Code Remediation Part 1.*

☐ Review the API catalog to identify which APIs require updates for compliance and which must maintain backward compatibility for legacy integrations.

Develop a plan for the Component to adopt the API standard.

☐ Collaborate and coordinate on existing API standards or equivalent automated interchange mechanisms as agreed upon across the Component environment.

☐ Determine environment-specific requirements in preparation for adopting the API standard or equivalent automated interchange mechanisms.

☐ Assess environment applications and services to identify necessary updates for alignment with the API standard, where applicable, across the Component environment.

☐ Develop a phased rollout plan to minimize disruption that prioritizes APIs based on risk, criticality, and update feasibility.

Implement API standards.

Update existing APIs through adoption of the new API standard:

☐ Test implementation of the new API standard in a controlled environment, for example:

- Confirm APIs properly apply and support configurations defined by the new standard.
- Verify that deployed solutions and integrated systems remain compatible with the updated API requirements.

☐ Update existing APIs to comply with new API standard.

Verify and validate updated APIs:

☐ Perform:

- Functional testing on the updated APIs to ensure they meet the new standards.
- Integration testing to confirm interoperability with other systems across the Component environment.
- Security testing, such as penetration testing, vulnerability scanning, etc.
- Performance testing.

☐ Where possible, create automated services or workflows that will enforce the API standards.

☐ Establish continued monitoring and alerting for non-compliance or deviations from the established API standard.
Continuously verify and validate compliance with API standards.
Monitor and document solutions to ensure functionality: ☐ Establish real-time/near real-time monitoring solutions to track the status of API performance and security compliance. ☐ Leverage API gateway logs and Security Information and Event Management (SIEM) systems to detect anomalous API activity that could indicate malicious activity.

Summary

This diagram outlines the Activity 6.6.2 (Phase One) – *Standardized Application Programming Interface (API) Calls and Schemas Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on standardization and implementation of Application Programming Interface (API) calls and schemas. It presents strategic insights driving implementation and expected outcomes that include establishment of API standards with Component commitment and implementation of automated pattern and protocol services.

Table 116: Activity 6.6.2 — Standardized Application Programming Interface (API) Calls and Schemas Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are initial API calls and schemas standardized and implemented across the DoW Enterprise?

STRATEGIC INSIGHTS
• The Component collaborates with the Enterprise to establish a comprehensive API standard, aligning with Enterprise requirements and digital modernization goals to define approved patterns, protocols, security policies, and governance frameworks for mission-centric API development. • The Component adopts Enterprise API standards by implementing API modeling, developing standardized rules and best practices, and ensuring APIs are discoverable, reusable, compliant, secure, and consistently monitored using defined Key Performance Indicators (KPIs). • The Component develops an Enterprise-wide API management strategy, automating API governance, versioning, and inventory, while enforcing policies for reference patterns, protocols, and security to maintain a centralized API policy framework. • The Component automates the API lifecycle by leveraging OpenAPI specifications, Continuous Integration/Continuous Delivery (or Deployment) (CI/CD) pipelines, Infrastructure as Code (IaC), container orchestration, and serverless technologies to ensure consistent deployment, compliance, and integration across the Enterprise. • The Component ensures API quality and compliance through automated testing, validation, and deprecation processes, streamlining API development with linting tools, code validation, and infrastructure automation to align with mission requirements and Enterprise standards.

EXPECTED OUTCOMES
1. API Standard (or equivalent automated interchange mechanism) is established with Component commitment. 2. Automated pattern and protocol services are implemented.

Capability 6.7 Security Operations Center (SOC) and Incident Response (IR)

Table 117: 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 6.7.1 Workflow Enrichment Part 1

Table 118: Activity 6.7.1 — Workflow Enrichment 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 establish cybersecurity incident response guidance using industry best practices, such as NIST and a list of approved threat data sources as specified in "Cyber Threat Intelligence (CTI) Program Pt1". Components enable workflows for security events using internal context, past threat events, and other threat intelligence. Approved external sources of enrichment are identified for future integration. These workflows are used to determine incident response procedures.	
Predecessor(s)	**Successor(s)**
None	6.5.2, 6.7.2
Expected Outcomes	
• Threat events are identified utilizing DoW Enterprise guidance and best practices. • Components establish workflows for threat events and include enrichment from approved sources and business/mission context.	
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.

- Consider completing Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1* prior to this activity, to enable the development of the Cyber Threat Intelligence (CTI) policy required for this activity.
- Activity 6.5.2 (Phase One) – *Implement Security Orchestration, Automation, and Response (SOAR) Tools* and Activity 6.7.2 (Phase Two) – *Workflow Enrichment Part 2* 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 119: Implementation Tasks for Activity 6.7.1 — Workflow Enrichment Part 1

Component collaborates with the Enterprise by leveraging Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1,* to develop a CTI policy and cybersecurity Incident Response (IR) procedures based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and industry best practices.
Consider completing Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1,* to develop a CTI policy: ☐ Component collaborates with the Enterprise to develop a CTI policy that informs ZT actions, such as access revocation, network segmentation changes, and enhanced security monitoring, based on real-time threat data. • Ensure scalability and adaptability to future threats, from Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1*. **Component continues collaboration with the Enterprise to develop cybersecurity IR procedures based on the CTI policy:** ☐ Leverage the established CTI policy to develop cybersecurity IR procedures in alignment with Enterprise and Component policies and the NIST CSF functions: • Identify • Protect • Detect • Respond • Recover. ☐ Incorporate automated ZT actions into the IR procedures, such as access revocation, system isolation, and dynamic network segmentation, to support timely detection, containment, mitigation, and incident recovery.
Leverage internal context, historical threat events, and other threat intelligence to enable security response workflows based on cybersecurity IR procedures.
Implement security response workflows that incorporate contextual and threat intelligence to drive adaptive, automated responses: ☐ Prioritize detected security incidents based on their potential impact to the ZT Architecture (ZTA), considering User/Person Entity (PE)/Non-Person Entity (NPE) behavior, historical threat trends, access logs, and other relevant data. ☐ Analyze historical threat events to identify patterns, techniques, or exploit paths that could circumvent ZT controls, and use findings to enhance preventive and detective capabilities. ☐ Enhance security response workflows by integrating CTI feeds into ZT enforcement points, enabling automated incident containment actions such as access revocation, host isolation, or dynamic network segmentation in accordance with the Component IR procedures.

Identify approved sources of enrichment for future integrations.

Define enrichment requirements to support ZT-aligned IR workflows:

☐ Collaborate with the Enterprise to verify and validate external enrichment sources before ingestion, ensuring data accuracy, reliability, and relevance to ZT access control and automated responses.

☐ Identify the types of enrichment data required (e.g., entity behavior, device posture, vulnerability indicators) to enhance threat prioritization, detection fidelity, and response decisions.

Identify key enrichment data sources, from Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1*:

☐ Utilize internal data sources (e.g., Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), monitoring solutions, etc.) to gain comprehensive visibility into the security posture of ZT environments. Focus on data that provides insights into User/PE access patterns, device security, and application behavior.

☐ Reference approved external data sources, from Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1* (e.g., threat intelligence feeds, vulnerability databases, industry reporting).

Plan environmental readiness for future enrichment integrations, where applicable:

☐ Identify where enrichment data will be consumed (e.g., policy enforcement points, analytics platforms) to strengthen ZT enforcement decisions.

☐ Ensure technical and policy prerequisites are defined for future ingestion and orchestration of approved enrichment data.

Test, verify, and validate security response workflows and enrichments.

Test and validate security response workflows and IR processes prior to full implementation:

☐ Conduct controlled environment testing to ensure workflows include sufficient context (e.g., affected system, incident type, attribution metadata) for successful implementation.

☐ Verify and validate security response workflows and IR processes:

- Can be implemented across the environment in accordance with Enterprise-aligned CTI policy and IR procedures.
- Accurately and appropriately incorporate CTI and enrichment data.
- Drive Component IR procedures, commensurate with the threat event level, ensuring that the action(s) taken align with the threat category and potential risks.
- Support the intended ZT enforcement decision paths for future automation.

Summary

This diagram outlines the Activity 6.7.1 (Phase One) – *Workflow Enrichment Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the identification and workflow development for threat events using industry best practices. It presents strategic insights driving implementation and expected outcomes that include identification of threat events utilizing Enterprise guidance and best practices.

Table 120: Activity 6.7.1 — Workflow Enrichment Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are threat events identified and workflows for threat events developed using industry best practices?

STRATEGIC INSIGHTS
• The Component defines objectives and establishes a cybersecurity Incident Response (IR) standard aligned with Enterprise requirements and industry best practices, incorporating threat modeling, behavioral analysis, and continuous threat monitoring for effective Cyber Threat Intelligence (CTI) policy deployment. • The Component demonstrates the capability to ingest and standardize Indicators of Compromise (IoC) from multiple approved sources, enabling analysis across file-based, host-based, network-based, behavioral, and web-traffic IoC, prioritized by risk severity. • The Component provides evidence of robust IR workflows that leverage internal logs, historical threat events, and threat intelligence feeds, integrating frameworks such as MITRE ATT&CK, D3FEND, and User and Entity Behavior Analytics (UEBA). • The Component ensures collaboration with approved Enterprise partners, academic institutions, and commercial CTI platforms to enrich security workflows with advanced, tactical, operational, and strategic threat intelligence, supporting enhanced detection, response, and analysis capabilities. • The Component maintains enriched security response workflows by integrating contextual metadata, automating threat analysis, and orchestrating data-backed security decisions to streamline IR, detect anomalies, and defend against advanced threat actors.

EXPECTED OUTCOMES
1. Threat events are identified utilizing DoW Enterprise guidance and best practices. 2. Components establish workflows for threat events and include enrichment from approved sources and business/mission context.

Visibility and Analytics Pillar

Capability 7.1 Log All Traffic (Network, Data, Apps, Users)

Table 121: 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 7.1.2 Log Parsing

Table 122: Activity 7.1.2 — Log Parsing

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 prioritize log and flow sources (e.g., firewalls, Endpoint Detection & Response, Active Directory, switches, routers, etc.) and develop a plan for collection of high-priority logs first, then low-priority. An open industry-standard log format is agreed upon at the Enterprise level with the Components, and implemented in future procurement requirements. Existing solutions and technologies are migrated to this format on a continual basis.	
Predecessor(s)	**Successor(s)**
None	7.2.4, 7.3.1
Expected Outcomes	
• Enterprise standardized log formats. • Components implement rules developed for each log format.	
End State	
Components filter and forward all applicable log events to the SIEM.	

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 1.1.1 (Discovery) – *Inventory User* prior to this activity, to obtain an accurate inventory of Users/Person Entities (PEs).
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, to obtain an accurate inventory of Non-Person Entities (NPEs).
- Component has procured an appropriate Security Information and Event Management (SIEM) solution to meet the environment's needs.
- Manage log ingest to avoid SIEM becoming overwhelmed, which can lead to performance degradation, increased storage costs, and slow query times.
- Optimize data storage to account for log volume and operational demands.
- Ensure secure log transmission and integrity by protecting data in transit and at rest to prevent tampering, interception, and/or loss.
- Activity 7.2.4 (Phase One) – *Asset ID and Alert Correlation* and Activity 7.3.1 (Phase One) – *Implement Analytics Tools* 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 123: Implementation Tasks for Activity 7.1.2 — Log Parsing

Collaborate with the Enterprise to establish a standardized log format.
Assess existing standards and define standardized log fields: ☐ Review current industry-standard log formats (e.g., JavaScript Object Notation (JSON), Common Event Format, System Logging (Syslog) Protocol, etc.) and Enterprise compliance requirements. ☐ Define standardized log fields that support ZT visibility, analytics, and Incident Response (IR), ensuring compliance with Enterprise policies, National Institute of Standards and Technology (NIST) guidance, and ZT requirements. ☐ In collaboration with the Enterprise, the Component establishes a common log format, including mandatory standardized fields (e.g., timestamp, source, severity, etc.). **Develop documentation for environment integration:** ☐ Create documentation detailing the log format structure, mapping rules, and compliance requirements necessary for integration into the existing environment.
Identify, prioritize, and collect log and flow sources.
Develop Component Log Source Codex: ☐ Leverage Activity 1.1.1 (Discovery) – *Inventory User*, to obtain an accurate and comprehensive User/PE inventory. ☐ Leverage Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis*, to obtain an accurate and comprehensive Hardware/Software inventory. ☐ Leverage Activity 3.1.1 (Discovery) – Application and Code Identification, to obtain an accurate and comprehensive application inventory. ☐ Identify and document all log sources in the Component Log Source Codex ☐ Leverage the Component Log Source Codex to further identify critical log-producing assets (e.g., security devices, network devices, Users/PEs, etc.). ☐ Leverage automation where possible, such as network discovery solutions, SIEM, asset inventory discovery, to ensure completeness and validate logging sources. **Collaborate with Cyber Threat Intelligence (CTI) teams, from Activity 7.5.1 – *Cyber Threat Intelligence (CTI) Program Part 1,* to prioritize log sources from inventory lists:** ☐ Categorize logs based on their relevance to ZT security, prioritizing logs that support access control decisions, threat detection, and IR within the ZT Framework.

☐ Leverage Cyber Threat Intelligence (CTI) to prioritize log sources that provide insights into potential threats to the ZT Architecture (ZTA), focusing on User/PE/NPE access, device behavior, and application activity.

Develop a log collection strategy:

☐ Establish procedures for log collection, ensuring minimal impact on system performance and storage.

☐ Configure logging to retain the most critical information while filtering out redundant data.

Standardize log configuration across the Component environment:

☐ Apply logging standards across all systems to ensure adherence to Enterprise requirements.

Monitor collection efficacy:

☐ Continuously verify log collection accuracy by comparing expected vs. actual collected logs.

☐ Set up alerts for missing logs, time errors, and/or inconsistencies.

Migrate existing solutions and technologies to the newly developed Enterprise standard log format.

Evaluate current log formats:

☐ Inventory existing log sources and determine compatibility with the standardized format.

☐ Use appropriate log analysis solutions to map current formats to the new logging schema.

Develop log transformation rules:

☐ Use log parsers to normalize logs in alignment with standardized format.

Test, verify, and validate migrations:

☐ Conduct pilot tests on a subset of logs before full-scale migration to test compatibility.

☐ Verify and validate that logs maintain accuracy and completeness after transformation.

Establish continuous migration testing and update processes accordingly:

☐ Regularly update log transformation rules to accommodate new log sources.

Filter and forward applicable log events to the SIEM.

Define log filtering criteria:

☐ Establish event filtering policies to ensure only security-relevant and ZT-aligned telemetry is forwarded to the SIEM.

☐ Collaborate with the IR team to define inclusion and exclusion rule sets for threat prioritization, for example:

- Include: authentication failures, privilege escalations, firewall denials
- Exclude: routine successful logins, low-severity debug messages

Implement secure log forwarding mechanisms:

☐ Configure log sources to transmit data using secure, encrypted protocols. Approved methods are defined in Activity 5.4.4 – *Protect Data in Transit.*

☐ Validate that systems and SIEM ingestion pipelines can scale to handle log volume without degradation or data loss.

Optimize log storage and processing efficiency:

☐ Apply log aggregation and normalization techniques to reduce duplication.

☐ Configure log retention policies in alignment with Enterprise and Component compliance requirements.

Ensure adherence to Enterprise logging standards:

☐ Verify and validate that all forwarded logs conform to the standardized schemas and field requirements to support ZT visibility, analytics, and IR automation.

Continuously monitor and refine filtering rules as needed:

☐ Regularly review and adjust log filtering criteria based on evolving threat intelligence and updates to the ZTA. Prioritize logs related to User/PE/NPE access, device posture, and application activity within the environment.

☐ Implement automated tuning mechanisms to dynamically adjust log collection in response to emerging threats and security incidents. Ensure the SIEM receives the most relevant data for accurate threat detection and effective IR.

Summary

This diagram outlines the Activity 7.1.2 (Phase One) – *Log Parsing* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the identification and prioritization of log and flow sources. It presents strategic insights that drive implementation and expected outcomes, including the standardization of log formats and the implementation of rules developed for each log format.

Table 124: Activity 7.1.2 — Log Parsing - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are log and flow sources identified and prioritized for collection?

STRATEGIC INSIGHTS
• The Component identifies and prioritizes log and flow sources, including firewalls, Endpoint Detection and Response (EDR), Active Directory, switches, and routers, ensuring critical systems and high-risk areas are aligned with visibility and compliance objectives. • The Component develops and implements standardized rules, requirements, and enrichment strategies for log data, including storage retention, indexing for efficient querying, and automated enrichment processes to enhance security monitoring and Incident Response (IR) capabilities. • The Component establishes a centralized log and flow collection strategy, ensuring secure data transmission, integration with Security Information and Event Management (SIEM) solutions, and verification and validation of ingestion accuracy while eliminating redundant sources to optimize performance. • The Component collaborates with the Enterprise to adopt an open, industry-standard log format, ensuring interoperability across systems through stakeholder engagement, testing, and the implementation of a standardized schema. • The Component verifies the completeness and accuracy of log forwarding to the SIEM, conducts periodic audits, and migrates existing solutions to the agreed-upon format, ensuring continuous alignment with evolving requirements, threats, and Enterprise standards.

EXPECTED OUTCOMES
1. Enterprise standardized log formats. 2. Components implement rules developed for each log format.

Capability 7.2 Security Information and Event Management (SIEM)

Table 125: 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) solutions
- Managed Detection and Response (MDR) solutions
- Security Information and Event Management (SIEM)
- Threat Intelligence Platform (TIP)
- Vulnerability Management solutions

Activity 7.2.1 Threat Alerting Part 1

Table 126: Activity 7.2.1 — Threat Alerting 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 existing Security Information and Event Management (SIEM) solution to develop rules and alerts for common threat events (e.g., malware, phishing, etc.). Alerts and/or rule triggers are fed into the parallel "Asset ID & Alert Correlation" activity to begin automation of responses.	
Predecessor(s)	**Successor(s)**
None	2.7.2, 7.2.2
Expected Outcomes	
• Rules developed for Component-derived threat correlation. • Rules developed for asset ID-based responses.	
End State	
Components augment SIEM with threat data developed from incident response analysis.	

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 1.1.1 (Discovery) – *Inventory User* prior to this activity, to obtain an accurate inventory of Users/Person Entities (PEs).
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, to obtain an accurate inventory of Non-Person Entities (NPEs).
- Component has procured an appropriate Security Information and Event Management (SIEM) solution to meet the environment's needs.
- Component has access to reliable and accurate threat intelligence data to support the development of threat correlation rules and alerts.
- Leverage industry best practices and threat frameworks to understand malicious Tactics, Techniques, and Procedures (TTP) and develop alerting and mitigation strategies.
- Activity 2.7.2 (Phase Two) – *Implement Extended Detection and Response (XDR) Tools and Integrate with Comply-to-Connect (C2C) Part 1* and Activity 7.2.2 (Phase Two) – *Threat Alerting Part 2* are defined by the Department of War (DoW) Zero Trust (ZT) Framework as successors to this activity.

Implementation

The implementation below table 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 127: Implementation Tasks for Activity 7.2.1 — Threat Alerting Part 1

Leverage the existing Component SIEM solution to identify and develop rules/alerts for common threat events.
Deploy and configure the existing SIEM solution to support ZT threat alerting: ☐ Confirm that the SIEM solution supports the collection, normalization, and analysis of security event data from all required sources [34]. ☐ Identify and configure existing data sources to forward relevant data into the SIEM. ☐ Ensure SIEM data handling complies with Component data retention, integrity, and auditability policies [34]. **Develop SIEM rules and alerts that detect threats to the ZT Architecture (ZTA):** ☐ Integrate validated threat intelligence to identify and alert on activities that violate ZT policies or indicate anomalous behavior (e.g., unauthorized access attempts, atypical data access patterns, etc.). ☐ Develop rules to detect known attack patterns capable of bypassing or exploiting weaknesses in ZT enforcement points, leveraging frameworks such as MITRE ATT&CK and prioritizing threats based on their potential impact to protected assets [35]. ☐ Continuously update alert logic and threat signatures based on evolving threat intelligence, SIEM insights, and Incident Response (IR) feedback to maintain detection efficacy [36]. **Monitor SIEM for continuous ZT enhancement:** ☐ Review SIEM alerts and event trends to identify gaps within ZT policies, logging, segmentation decisions, and enforcement controls. Use findings to iteratively strengthen the overall ZT posture.
Develop threat correlation rules and generate threat detection alerts within the SIEM.
Leverage threat intelligence to identify and correlate threats to the ZTA: ☐ Review historical security incidents and known attack vectors that have previously bypassed or exploited weaknesses in ZT controls. ☐ Align with validated internal and external threat intelligence to identify threats that pose the highest risk to critical assets and ZT enforcement points. **Configure SIEM rules and alerts to support data-driven ZT security:** ☐ Develop correlation rules that combine enriched log data, entity behavior, and threat intelligence to identify and prioritize suspicious activity.

☐ Tune alert logic and severity thresholds based on ZT-aligned risk assessments to ensure the SIEM drives effective and timely data-driven security decisions. **Enhance alert quality, by aligning with Activity 7.2.4 (Phase One) – *Asset ID and Alert Correlation*:** ☐ Where feasible, include asset identification data in alerts to improve future correlation and response decisions when Activity 7.2.4 (Phase One) – *Asset ID and Alert Correlation* is implemented. **Test, verify, and validate rules before operational use:** ☐ Simulate representative threat scenarios to verify alerts trigger consistently and accurately. ☐ Refine correlation rule parameters based on results to optimize detection effectiveness and reduce false positives. **Monitor alert performance for continuous ZT enhancement:** ☐ Review alert trends and outcomes to identify detection gaps and refine ZT policies and SIEM detection logic to prevent future incidents.
Develop asset identification-based rules for IR.
Gather accurate User/PE/NPE lists for environment: ☐ Leverage Activity 1.1.1 (Discovery) – *Inventory User,* to obtain an accurate and comprehensive User/PE List as established in the User Pillar. ☐ Leverage Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis,* to obtain an accurate and comprehensive Hardware/Software List, as established in the Device Pillar. ☐ Where possible, monitor and maintain asset inventories using automated solutions [15]. **Align IR procedures to asset types to support ZT responses:** ☐ Define and document IR workflows tailored to different assets categories (e.g., endpoints, servers, etc.). ☐ Ensure procedures include rapid asset identification, location, and criticality assessment [37]. **Enable automation of the asset impact assessment in the IR procedures:** ☐ Quickly assess the impact on assets before, during, and after an incident (e.g., automatically retrieve asset details from inventory, etc.) [37]. ☐ Predefine IR actions for specific types of assets based on risk for future automated response capabilities. **Monitor and update IR procedures and asset rules:** ☐ Review and refine asset-based alert logic regularly to reflect changes in asset inventory and Component priorities [36].

Prepare and validate automated response actions for future ZT enforcement.

Identify threat events suitable for future automation using known and discovered threat signatures:

☐ Collaborate with IR and threat-hunting teams to identify alert types appropriate for automated response in future capability maturation.

☐ Prioritize low-risk events with appropriate mitigation actions [36].

Develop data-driven response playbooks aligned with ZT security:

☐ Create playbooks that define response actions mapped to specific alert types and risk levels based on enriched security data, threat intelligence, and contextual information.

☐ Incorporate decision points using contextual data to ensure actions remain appropriate and proportional.

Validate playbook logic in a controlled environment:

☐ Test response pathways using simulations to confirm they support ZT enforcement without operational disruption.

☐ Continuously monitor and improve responses to enhance resilience and minimize false positives to support automation readiness [36].

Summary

This diagram outlines the Activity 7.2.1 (Phase One) – *Threat Alerting Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development of basic rules and alerts for common threat events using existing Security Information and Event Management (SIEM) solutions. It presents strategic insights that drive implementation and expected outcomes, including the development of rules for component-derived threat correlations and asset ID-based responses.

Table 128: Activity 7.2.1 — Threat Alerting Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are basic rules and alerts for common threat events developed using the existing SIEM solution?

STRATEGIC INSIGHTS
• The Component establishes and configures a SIEM solution to collect, normalize, and analyze security event data, integrating known threat signatures and leveraging threat intelligence to detect and alert on attack patterns. • The Component develops asset-based correlation rules and maintains an automated, accurate asset inventory to enable targeted threat detection, triggering alerts tied to specific assets for effective incident investigation and response. • The Component creates Incident Response (IR) procedures tailored to asset types, automating asset impact assessments and predefined IR actions to streamline responses based on risk level and asset criticality. • The Component automates responses to known threat events by developing and testing response playbooks for repeatable, well-understood threats, ensuring human oversight at key decision points to avoid false positives. • The Component continuously monitors, tests, and refines SIEM automation workflows and asset-based IR rules to enhance threat detection accuracy, optimize response efficiency, and align with evolving threat intelligence and asset priorities.

EXPECTED OUTCOMES
1. Rules developed for Component-derived threat correlation. 2. Rules developed for asset ID-based responses.

Activity 7.2.4 Asset ID and Alert Correlation

Table 129: Activity 7.2.4 — Asset ID and Alert Correlation

DoW Zero Trust Framework	
Content in this table is sourced from authoritative DoW Zero Trust Framework documentation current at the time of publication.	
Description	
All assets in SIEM are identified and correlated to alerts in order to provide security teams with accurate and detailed information. This information contributes to the incident response speed. Asset IDs also allow better visibility while performing vulnerability assessments.	
Predecessor(s)	**Successor(s)**
7.1.2	None
Expected Outcomes	
• Identify and provide as much detail as needed for identification of all assets in SIEM, including correlation to alerts in support of "Threat Alerting Pt1".	
End State	
Security is able to quickly identify assets in relation to threat events in a way that betters supports incident response.	

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 7.1.2 (Phase One) – *Log Parsing* 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 this activity, to obtain an accurate inventory of Users/Person Entities (PEs).
- Consider completing Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis* prior to this activity, to obtain an accurate inventory of Non-Person Entities (NPEs).
- Consider completing Activity 7.2.1 – *Threat Alerting Part 1,* to assist with data enrichment pipeline implementation.
- 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.
- Enhance data storage and query efficiency to support fast and accurate asset correlation.
- Ensure continuous asset tracking across dynamic environments.

- Implement context-aware alert enrichment without overloading SIEM processing, where possible.

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 7.2.4 — Asset ID and Alert Correlation

Obtain a comprehensive asset inventory for identification and logging within the SIEM.
Gather accurate User/PE/NPE lists for environment: ☐ Leverage Activity 1.1.1 (Discovery) – *Inventory User,* to obtain an accurate and comprehensive User/PE List as established in the User Pillar. ☐ Leverage Activity 2.1.1 (Discovery) – *Device Health Tool Gap Analysis,* to obtain an accurate and comprehensive Hardware/Software List, as established in the Device Pillar. **Ensure all assets are identified and logged in SIEM with relevant metadata:** ☐ Integrate authoritative asset telemetry sources (e.g., Content Management Database (CMDB), Endpoint Detection and Response (EDR), vulnerability management solutions, etc.) with the SIEM to: • Provide real-time context for trust evaluation and enforcement for alert enrichment. • Support continuous validation of device state, ownership, and ZT compliance. ☐ Continuously discover and validate assets through dynamic telemetry ingestion. Flag unmanaged, orphaned, or non-compliant assets to reinforce deny-by-default principles. **Verify and validate asset visibility and accuracy:** ☐ Cross-check SIEM asset inventory against external asset repositories. ☐ Perform periodic audits to confirm asset inventory completeness and accuracy.
Correlate assets with SIEM threat alerts.
Enrich alerts with asset and identity metadata: ☐ Ensure predecessor Activity 7.1.2 (Phase One) – *Log Parsing* is completed, to provide standardized and normalized log fields (e.g., User/PE/NPE identifiers, device IDs, application identifiers), enabling accurate asset correlation within the SIEM. ☐ Map asset identifiers to alerts to enable policy enforcement based on the type and criticality of affected resources based on contextual understanding of threats.

Implement data enrichment pipelines:

☐ Use SIEM enrichment capabilities to automatically populate security alerts to enable ZT-aligned Incident Response (IR) decisions based on dynamic trust factors based on contextual asset identification data, including:

- Asset ownership
- Device posture/compliance indicators
- Asset criticality
- Recent access activity

☐ Consider completing Activity 7.2.1 – *Threat Alerting Part 1,* to align alert enrichment with Enterprise policies and procedures to maintain asset identifiers across SIEM alerts.

☐ Tag alerts that indicate potential violations of ZT policies, such as:

- Unauthorized access attempts.
- Suspicious resource access behavior.
- Deviations from established baselines.

☐ Use alert tags to categorize and track policy violations, enabling trend analysis and informing policy refinement.

Verify and validate the accuracy and completeness of ZT asset correlation:

☐ Simulate representative incidents to verify alerts consistently display accurate asset and identity information for decision-making within the ZT Framework.

☐ Collaborate with Component security team(s) to identify and address any discrepancies or gaps in enrichment data.

Optimize IR decision-making with asset-aware alert correlation.

Enable ZT-driven alert triage and asset containment:

☐ Enable Component security team(s) to quickly investigate impacted assets and associated threats using contextual identity, with visibility into assigned roles, authentication history, and current compliance posture.

☐ Support prioritization of alerts involving unmanaged or non-compliant assets.

☐ Ensure containment respects the Least Privilege model, applying narrowly scoped actions (e.g., network micro-segmentation, revoking access to specific resources, etc.) rather than broad-based shutdowns.

Enhance IR workflows with identity-based telemetry and correlation:

☐ Correlate identity provider (IdP) signals, device compliance status, and segmentation zone context to improve impact evaluation and scope definition.

☐ Provide IR teams with enriched context, such as:

- Asset criticality
- Role/privilege level

- Segmentation zone membership
- History of policy violations

☐ Tailor IR workflow based on asset criticality, User/PE/NPE role, and real-time trust level (e.g., deny, quarantine, monitor).

Continuously improve correlation quality and ZT support:

☐ Conduct post-incident reviews to determine whether enriched alerts enabled effective containment and response.

☐ Refine enrichment sources and correlation logic based on ZT posture gaps, telemetry blind spots, and IR feedback.

Summary

This diagram outlines the Activity 7.2.4 (Phase One) – *Asset ID and Alert Correlation* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development of basic correlation rules using asset and alert data in response to common threat events. It presents strategic insights that drive implementation and expected outcomes, including the identification of all assets in Security Information and Event Management (SIEM), as well as correlation to alerts in support of Activity 7.2.1 (Phase One) – *Threat Alerting Part 1.*

Table 131: Activity 7.2.4 — Asset ID and Alert Correlation - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are basic correlation rules using asset and alert data developed for automating responses to common threat events?

STRATEGIC INSIGHTS
• The Component develops a comprehensive, centralized database to manage unique Asset Identities (IDs) by compiling granular details, such as machine tags, user Security Identifiers (SIDs), Media Access Control (MAC) addresses, digital keys, tokens, labels, and role-based attributes, for both User/Person Entity (PE) and machine credentials. • The Component establishes Asset ID-based Security Information and Event Management (SIEM) rules to enable scalable and interactive data feeds, verify and validate configurations, and map security guidance frameworks. The SIEM rules incorporate Asset IDs to identify compliant, non-compliant, and unknown configurations while addressing Zero-Day Threats (ZDTs), Advanced Persistent Threats (APTs), and other vulnerabilities. • A threat correlation map linked to Asset IDs is developed to support Incident Response (IR) by leveraging hardware/software tracking systems, identifying correlated threats, and automating response actions. Specific dashboards and tools/solutions are implemented to monitor and analyze metrics, including Central Processing Unit (CPU) usage, bandwidth, processes, ports, and protocols, for both typical and atypical scenarios. • The SIEM solution associates assets with alerts and correlates security events using the unique Asset ID database, ensuring granular tracking and automated workflows. Real-time interactive integrations between SIEM and Security Orchestration, Automation, and Response (SOAR) solutions provide the security team with sufficient information to assess, respond to, and resolve incidents. • Testing, verification, and validation of Asset ID and alert correlation rules are conducted across virtualized environments to ensure the completeness, accuracy, and traceability of results. These outputs are compiled into gap analysis lists and readiness baselines, serving as critical references for Information Technology Operations Management (ITOM) and IR sustainment. • A systematic IR sustainment guide is developed to enhance the Component's security posture, incorporating automated Asset ID-based approaches, change management processes, and traceability for mission objectives.

✓ EXPECTED OUTCOMES
1. Identify and provide as much detail as needed for identification of all assets in SIEM, including correlation to alerts in support of "Threat Alerting Pt1".

Capability 7.3 Common Security and Risk Analytics

Table 132: 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 (SOCs) 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 and Entity Behavior Analytics (UEBA)
- Vulnerability Management solutions

Activity 7.3.1 Implement Analytics Tools

Table 133: Activity 7.3.1 — Implement Analytics 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 Enterprise provides minimum requirements for analytics tool capabilities to analyze data across all ZT pillars. Components procure and implement an analytics tool in order to provide actionable insights and intelligence.	
Predecessor(s)	**Successor(s)**
7.1.2	None
Expected Outcomes	
• Enterprise develops requirements for analytic environment. • Components procure and implement analytic tools.	
End State	
Analytics tools provide intelligence and guidance to security teams in order to make improvements on threat monitoring and response.	

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 7.1.2 (Phase One) – *Log Parsing* is defined by the Department of War (DoW) Zero Trust (ZT) Framework as a predecessor to this activity.
- Ensure all tooling selections adhere to Enterprise and Component procurement policies (e.g., security, system integration, scaling, etc.) and align with ZT requirements and industry best practices.
- Optimize data ingestion and normalization to prevent performance bottlenecks.

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 7.3.1 — Implement Analytics Tools

Define requirements for analytic tool capabilities.
Define requirements for analytics tools to enable data-driven ZT security and policy enforcement: ☐ Identify data sources and analytical capabilities needed to support continuous trust evaluation, threat detection, and security monitoring across all ZT pillars. ☐ Determine performance and scalability requirements to ensure that analytics tools can process the data volume needed for ZT security insights. ☐ Plan deployment to ensure data accessibility, security, and integration with existing ZT enforcement and telemetry solutions. **Define ZT-aligned integration points within the environment:** ☐ Identify how analytic tools will integrate with existing policy enforcement and telemetry platforms (e.g., Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Identity Provider (IdP), etc.) to support dynamic trust evaluation and enforcement. ☐ Prioritize integration paths that enable real-time context sharing and identity- and asset-aware alerting aligned to ZT principles. ☐ Identify automation capabilities for future maturation that will support dynamic monitoring and risk-based alert prioritization in accordance with ZT decision-making models. **Finalize and document analytic tool requirements:** ☐ Compile requirements into Enterprise-aligned procurement documentation. ☐ Verify and validate with stakeholders prior to procurement, where applicable.
Evaluate and select analytic tool(s) according to defined requirements.
Research industry solutions: ☐ Evaluate SIEM, User and Entity Behavior Analytics (UEBA), and other analytics technologies for their ability to support ZT operations, including identity-centric anomaly detection, continuous trust evaluation, and integration with enforcement mechanisms. ☐ Consider commercial, open-source, and custom-built options, where applicable. **Evaluate and select analytic tools that strengthen ZT security monitoring:** ☐ Assess the ability of tools to integrate with existing ZT visibility and decision-support solutions. ☐ Evaluate capabilities based on scalability, usability, detection efficacy, and cost. ☐ Select tools that demonstrate alignment with defined requirements and existing ZT security infrastructure. **Select and procure analytic tool(s) based on findings:** ☐ Collaborate with procurement teams to acquire licenses and associated services. ☐ Establish vendor support agreements and Service Level Agreements (SLAs), where required.

Implement and integrate analytics tool(s) into existing environment.

Deploy analytic tool(s) and integrate with existing infrastructure:

☐ Prepare the environment for deployment and configure secure data pipelines for data sharing and ingestion.

☐ Integrate analytics tools with SIEM, EDR, firewalls, and threat intelligence feeds to enable continuous trust assessment, identity-aware correlation, and real-time policy enforcement across the ZT architecture (ZTA).

Define custom detection rules, as needed:

☐ Implement analytics rules that incorporate threat indicators, historical incidents, and dynamic trust signals (e.g., identity behavior, device posture, access anomalies, etc.) to support continuous trust evaluation and adaptive ZT policy enforcement.

Verify and validate data accuracy and alerting:

☐ Run test scenarios across identity, device, and access contexts to verify that analytics support accurate threat detection and monitoring.

☐ Continuously refine detection thresholds and behavioral baselines to reduce false positives while maintaining sensitivity to anomalous activity.

Continuously improve analytics capabilities to better support security operations.

Monitor performance and threat detection quality:

☐ Monitor ZT efficacy metrics such as alert accuracy, reduction in false positives, and trust score fluctuations.

☐ Continuously adjust analytics and trust evaluation models based on evolving threat intelligence, identity behavior shifts, and post-incident ZT assessments.

Enhance threat intelligence correlation:

☐ Once validated, integrate new and/or updated threat feeds into analytics tool(s) to improve analytic accuracy.

☐ Cross-reference alerts with approved threat intelligence, ensuring that only verified and validated, context-rich intelligence is used to inform security decisions and actions, in accordance with ZT principles.

☐ Ensure correlation logic continues to elevate threats with strongest contextual risk signals.

Gather feedback and refine analytic capabilities:

☐ Conduct periodic reviews with Component security team(s) to refine analytics configurations and outputs.

☐ Update analytic techniques as needed to reflect evolving threats, ensuring that access and actions are governed by dynamic, context-driven policies that align with the Policy-Based Access Control (PBAC) model to enforce least-privilege and adaptive security principles.

Summary

This diagram outlines the Activity 7.3.1 (Phase One) – *Implement Analytics Tools* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development of requirements for the analytic environment. It presents strategic insights that drive implementation and expected outcomes, including the development of requirements for an analytic environment and the procurement and implementation of analytic tools.

Table 135: Activity 7.3.1 — Implement Analytics Tools - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are requirements for the analytic environment developed?

STRATEGIC INSIGHTS
• The Component defines and documents baseline requirements for real-time analytic environments by engaging with Enterprise stakeholders, identifying use case scenarios, data/metadata needs, and performance metrics while integrating Artificial Intelligence (AI)/Machine Learning (ML)-driven analytics to detect anomalies and emerging threats. • The Component procures vetted analytic tools/solutions aligned with Enterprise cybersecurity policies, acquisition frameworks, and technical standards. Tools/solutions are evaluated for scalability, security compliance, automation capabilities, and integration with existing Enterprise systems. • The Component implements analytic tools/solutions through a defined deployment strategy, integrating tools/solutions with existing infrastructure, configuring real-time monitoring, and establishing governance for Mission Essential Functionality (MEF). Continuous testing, training, and optimization ensure seamless deployment and scalability. • The Component generates actionable security intelligence by collecting and enriching data from diverse sources, applying behavioral analytics, threat correlation, and dynamic tuning to identify vulnerabilities, anomalies, and threats, producing prioritized alerts and reports for Information Technology Operations Management (ITOM) and Incident Response (IR) teams. • The Component establishes a continuous monitoring and reporting process with dashboards, Key Performance Indicators (KPIs), and real-time alerts, ensuring ongoing analysis, escalation of security incidents, and actionable intelligence delivery to stakeholders to maintain an optimized and risk-aware security posture.

EXPECTED OUTCOMES
1. Enterprise develops requirements for analytic environment. 2. Components procure and implement analytic tools.

Capability 7.5 Threat Intelligence Integration

Table 136: 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 7.5.1 Cyber Threat Intelligence (CTI) Program Part 1

Table 137: Activity 7.5.1 — Cyber Threat Intelligence (CTI) Program 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 develop a Cyber Threat Intelligence (CTI) program policy, standard, and process. Components utilize this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI teams gather intelligence from common data feeds across ZT Pillars and aggregate all intelligence to a centralized repository (e.g., SIEM).	
Predecessor(s)	**Successor(s)**
None	7.2.2, 7.5.2
Expected Outcomes	
• DoW Enterprise develops a Cyber Threat Intelligence (CTI) program policy. • Component CTI team is in place with critical stakeholders. • Common CTI feeds are being utilized by SIEM for monitoring. • Integration points exist with device and network PEP/PDP (e.g., NextGen AV, NGFW, NG-IPS) are built at appropriate integration points across each pillar.	
End State	
Component CTI teams are established in accordance with Enterprise policy and have integrated CTI data feeds in their SIEM(s).	

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.

- Define clear roles and responsibilities in Cyber Threat Intelligence (CTI) policy to ensure accountability and consistent threat intelligence handling.
- Engage security operations, risk management, and leadership early to align CTI objectives with Component priorities.
- Prioritize high-fidelity threat intelligence sources to reduce noise and improve actionable insights within the Security Information and Event Management (SIEM).
- Regularly test the efficacy of CTI-driven security controls.
- Activity 7.2.2 (Phase Two) – *Threat Alerting Part 2* and Activity 7.5.2 (Phase Two) – *Cyber Threat Intelligence (CTI) Program Part 2* 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 7.5.1 — Cyber Threat Intelligence (CTI) Program Part 1

Develop and implement a CTI program policy, standard, and process.
Develop a CTI program to enable data-driven ZT security and adaptation: ☐ Create a CTI program that provides rich threat context and data-driven insights to support continuous monitoring, risk assessment, and policy adaptation within the ZT Architecture (ZTA). ☐ Develop a CTI policy that emphasizes the collection and analysis of diverse threat data sources, including open-source intelligence, commercial threat feeds, and internal security logs (e.g., National Institute of Standards and Technology (NIST) Cybersecurity Framework, MITRE ATT&CK, etc.) [15]. ☐ Define processes for correlating threat intelligence with internal security data and integrating it into ZT security analytics platforms, enabling a more comprehensive and data-driven approach to ZT security. ☐ Design policies to be scalable and adaptable, ensuring they continuously integrate verified and validated threat intelligence to support context-aware enforcement decisions consistent with ZT principles. **Prepare for CTI integration to improve ZT adaptation and resilience:** ☐ Establish a process for regularly updating and integrating validated threat intelligence, enabling the architecture to adapt to evolving threats and maintain a strong security posture. ☐ Define integration points for CTI data that support improved visibility and context for policy and enforcement decisions across the ZTA.
Establish CTI teams with stakeholders, leveraging CTI program policy.
Establish CTI teams to enable ZT adaptation and informed decision-making: ☐ Identify key stakeholders responsible for making decisions regarding ZT security policies, architecture, and operations. ☐ Ensure CTI teams provide timely and actionable threat intelligence to stakeholders, enabling them to adapt the ZTA to emerging threats and make informed decisions about risk mitigation and resource allocation. **Define CTI team collaboration and information-sharing processes:** ☐ Develop structured workflows for intelligence sharing within Enterprise-approved Communities of Interest (COI).

☐ Establish protocols for ingesting, validating, and distributing threat intelligence based on operational relevance and impact.

Integrate CTI to enhance ZT adaptation and resilience:

☐ Establish processes for continuously integrating and maintaining validated threat intelligence within the environment to improve situational awareness and resilience.

☐ Define how CTI data will inform policy adjustments, support risk-based prioritization, and improve the resilience of the ZTA against evolving and emerging threats.

☐ Regularly review and refine CTI integration strategies to ensure ongoing support ZT adaptation and resilience objectives.

CTI teams gather intelligence from common and vetted threat feeds into a centralized repository (e.g., SIEM, etc.) for aggregation and analysis.

Identify, verify, and validate common threat intelligence feeds:

☐ Select and continuously verify and validate threat intelligence feeds based on Enterprise-defined validation standards to ensure only high-confidence, relevant indicators are used to inform policies and enforcement.

Ingest and normalize threat intelligence for policy-driven usage:

☐ Integrate threat intelligence feeds into the SIEM using standardized formats (e.g., Structured Threat Information eXpression (STIX), Trusted Automated Exchange of Intelligence Information (TAXII), etc.) to ensure consistency across analytics and ZT Policy Decision Points (PDPs).

Correlate threat intelligence with security events:

☐ Map verified and validated threat indicators (e.g., Internet Protocols (IPs), domains, file hashes, Tactics, Techniques, and Procedures (TTP), etc.) to real-time user, workload, and system activity to improve visibility and enable context-aware security assessments.

Establish threat intelligence sharing.

Formalize intelligence-sharing partnerships and define secure sharing protocols:

☐ Build trusted relationships with Enterprise approved COIs.

☐ Establish structured processes for securely sharing threat intelligence in compliance with Enterprise and Component security and privacy policies.

Integrate shared intelligence into Component operations:

☐ Ensure CTI teams apply proper validation processes before sharing or acting on external intelligence.

☐ Integrate validated intelligence into SIEM, SOAR, and other analytics solutions to support situational awareness and informed security decision-making.

Continuously evolve sharing strategies:

☐ Regularly assess the value and relevance of intelligence-sharing partnerships.

☐ Refine engagement and collaboration strategies as threat landscape evolves.

Build appropriate integration and enforcement points across the ZT infrastructure.

Establish CTI-driven integration and enforcement points:

☐ CTI teams coordinate with existing enforcement solutions (e.g., firewalls, endpoint security, intrusion prevention systems) to incorporate validated CTI context into access control and segmentation logic.

☐ Leverage technologies such as Identity and Access Management (IAM), Policy Enforcement Points (PEPs), Policy Decision Points (PDPs), and Endpoint Detection and Response (EDR) to apply ZT-aligned policies across the environment [38].

Ensure cross-pillar integration:

☐ Align integration points across identity, device, network, application, and data security layers to achieve consistent CTI-driven visibility and control across the ZTA.

Implement continuous monitoring, dynamic alert reporting, and automated Incident Response (IR).

Implement continuous monitoring to maintain threat awareness:

☐ Continuously assess evolving threat landscape using validated threat intelligence to inform policy decisions, alert tuning, and control prioritization across SIEM, SOAR, and related monitoring solutions.

Enable dynamic alerting and reporting:

☐ Configure SIEM and related solutions to handle alerts based on CTI-informed context (e.g., observed TTP, malicious indicators).

☐ Ensure alerts are actionable and prioritized based on validated intelligence and associated risk.

Continuously refine CTI detection and policy efficacy:

☐ Conduct routine evaluations to ensure CTI-informed detections align with ZT enforcement priorities.

☐ Regularly test and validate monitoring, alerting, and response mechanisms through threat-informed assessments (e.g., penetration tests, red teaming, on-net assessments, etc.) to enhance ZT enforcement accuracy and effectiveness.

☐ Refine detection logic, CTI data feeds, and validation workflows based on findings from post-incident reviews, assessments, and evolving threat intelligence to continuously improve the fidelity and relevance of ZT-aligned detections.

Summary

This diagram outlines the Activity 7.5.1 (Phase One) – *Cyber Threat Intelligence (CTI) Program Part 1* of the Department of War (DoW) Zero Trust (ZT) Framework, focusing on the development of Cyber Threat Intelligence (CTI) teams with key mission/task stakeholders. It presents strategic insights that drive implementation and expected outcomes, including the development of a CTI program policy and the utilization of common CTI feeds by Security Information and Event Management (SIEM) for monitoring.

Table 139: Activity 7.5.1 — Cyber Threat Intelligence (CTI) Program Part 1 - Workflow

ZERO TRUST READINESS ASSESSMENT QUESTIONS
1. How are CTI teams developed with key mission/task stakeholders?

STRATEGIC INSIGHTS
• The Component defines a CTI program policy, standard, and process that align with Enterprise security strategies, regulatory requirements, and industry frameworks (e.g., National Institute of Standards and Technology (NIST) Cybersecurity Framework, MITRE ATT&CK, etc.), ensuring clear roles, responsibilities, intelligence-sharing protocols, and data protection measures. • The Component demonstrates structured CTI policy deployment by establishing ingestion, analysis, and intelligence-sharing workflows within security teams and integrating CTI with Enterprise security architecture, including SIEM, Next-Generation Antivirus (NextGen AV), Next-Generation Firewall (NGFW), and Next-Generation-Intrusion Prevention System (NG-IPS) for effective threat detection and response. • The Component provides a robust intelligence-sharing framework by onboarding key stakeholders, defining collaboration workflows, and integrating verified and validated threat intelligence feeds into centralized security repositories, enhancing real-time threat correlation and automated Incident Response (IR) capabilities. • The Component leverages ZT infrastructure to enforce CTI-driven security policies across identity, device, network, application, and data security layers, utilizing Identity and Access Management (IAM), Policy Enforcement Points (PEPs), Endpoint Detection and Response (EDR), and automated orchestration solutions for dynamic threat containment. • The Component ensures continuous monitoring, dynamic alert reporting, and automated IR through SIEM and Security Orchestration, Automation, and Response (SOAR) integrations, refining detection rules, updating IR procedures, and enhancing cyber resilience through regular assessments, penetration testing, and incident reviews.

✓ EXPECTED OUTCOMES

1. DoW Enterprise develops a CTI program policy.
2. Component CTI team is in place with critical stakeholders.
3. Common CTI feeds are being utilized by SIEM for monitoring.
4. Integration points exist with device and network PEP/PDP (e.g., NextGen AV, NGFW, NG-IPS) are built at appropriate integration points across each pillar.

Appendix A – Terms and Definitions

Terms and definitions used within this Zero Trust Implementation Guideline.

API Standardization
The ability to reach agreement and publish locally, the application programming interface for a commonly used service. Enforcement of compliance in the use of commonly agreed API's.
Source: DoD Zero Trust Reference Architecture, Version 2.0

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

Active Directory
A Microsoft directory service for the management of identities in Windows domain networks.
Source: NIST Computer Security Resource Center (CSRC) Glossary

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

Audit and Accountability
Entails that organizations (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity; and (ii) ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable.
Source: NIST SP 800-12 Revision 1- An Introduction to Information Security

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

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 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 Service Provider
An external company that provides a platform, infrastructure, applications, and/or storage services for its clients.
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 Access Card
The standard identification for active duty uniformed Service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to DoD computer network and systems.
Source: DoD Common Access Card

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

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 (or Deployment)

Continuous Integration/Continuous Delivery (or Deployment) (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

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 Survivability Endorsement

The Joint Staff developed the Cyber Survivability Endorsement (CSE) criteria to ensure joint warfighting systems' requirements are articulated sufficiently, to prevent, mitigate and recover from cyber events by applying a risk-managed approach to countering a capable and determined adversary.

Source: Defense Acquisition University (DAU) Cyber Survivability Endorsement Implementation Guide, Version 2.0

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 Lake

A data lake is a centralized repository that allows you to store all your structured and unstructured data at any scale. You can store your data as-is, without having to first structure the data, and run different types of analytics—from dashboards and visualizations to big data processing, real-time analytics, and machine learning to guide better decisions.

Source: DoD Zero Trust Reference Architecture, Version 2.0

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 Policy Administrator (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

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 in Transit

The ability to protect data if communications are intercepted while data moves between sites or services. This protection is achieved by encrypting the data before transmission; authenticating the endpoints; and decrypting and verifying the data on arrival.

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

Endpoint Agent

Client software installed on a network endpoint that communicates or is controlled by a centralized system.

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

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

Impact Levels

The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high.

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 nonrepudiation 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

Lightweight Directory Access Protocol
The Lightweight Directory Access Protocol, or LDAP, is a directory access protocol.
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

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

Media Access Control
A unique 48-bit value that is assigned to a particular wireless network interface by the manufacturer.
Source: NIST Computer Security Resource Center (CSRC) Glossary

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

Operational Test and Evaluation

The field test, under realistic conditions, of any item (or key component) of weapons, equipment, or munitions for the purpose of determining the effectiveness and suitability of the weapons, equipment, or munitions for use in combat by typical military users, and the evaluation of the results of such tests.

Source: Defense Acquisition University (DAU) 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 applied 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 Policy Engine 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 Policy Engine 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

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

Rule Set

The capture of policy in a collection of Event/Condition/Action, or other forms of assertive statements, that can be interpreted by an algorithm.

Source: DoD Zero Trust Reference Architecture, Version 2.0

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 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

Security Technical Implementation Guide

Based on Department of Defense (DoD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.

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

Simple Network Management Protocol

A standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. To work with SNMP, network devices utilize a distributed data store called the Management Information Base (MIB). All SNMP-compliant devices contain a MIB which supplies the pertinent attributes of a device. Some attributes are fixed or “hard-coded” in the MIB, while others are dynamic values calculated by agent software running on the device.

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

VPN Gateway

Virtual Private Network (VPN) gateways provide secure connectivity between multiple sites, such as on-premises data centers, Virtual Private Cloud (VPC) networks, and VMware Engine private clouds. Traffic is encrypted because the VPN connections traverse the internet. Each VPN gateway can support multiple connections. When you create many connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.

Source: DoD Zero Trust Reference Architecture, Version 2.0

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
ADC	Application Delivery Controller
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ASTO	Application Security Testing Orchestration
ATO	Authorization to Operate
AV	Antivirus
BYOD	Bring Your Own Device
C2C	Comply-to-Connect
CA	Certificate Authority
CAC	Common Access Card
CASB	Cloud Access Security Brokers
cATO	Continuous Authorization to Operate
CERT	Computer Emergency Response Team
CI/CD	Continuous Integration and Continuous Delivery (or Deployment)
CIA	Confidentiality, Integrity, and Availability
CIB	Configuration Item Baseline
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Office
CISA	Cybersecurity and Infrastructure Security Agency
CMDB	Configuration Management Database
CNDSP	Computer Network Defense Service Provider
COI	Communities of Interest
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRUD	Create, Read, Update, and Delete
CSE	Cyber Survivability Endorsement
CSF	Cybersecurity Framework
CSI	Cybersecurity Information Sheet
CSP	Cloud Service Provider
CSSP	Cybersecurity Service Provider
CTI	Cyber Threat Intelligence

CVE	Common Vulnerabilities and Exposure
DAAS	Data, Applications, Assets, and Services
DAST	Dynamic Application Security Testing
DB	Database
DCI	Defense Critical Infrastructure
DCN	Data Collection Node
DDoS	Distributed Denial-of-Service
DevOps	Development and Operations
DevSecOps	Development, Security, and Operations
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoD	Department of Defense
DoW	Department of War (authorized secondary title for the DoD)
DoW CIO	Department of War Chief Information Office (formerly DoD CIO)
DPIV	Digital Personal Identity Verification
DPP	Data Privacy and Protection
DRM	Data Rights Management
ECA	External Certification Authority
ECDSA	Elliptic Curve Digital Signature Algorithm
EDM	Enterprise Device Management
EDR	Endpoint Detection and Response
EO	Executive Order
EPP	Endpoint Protection Platform
ETL	Extract, Transform, Load
FAM	File Activity Monitoring
FIDO	Fast Identity Online
FIM	File Integrity Monitoring
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
FW	Firewall
FWaaS	Firewall as a Service
GRC	Governance, Risk, and Compliance
HaCC	Hosting and Computer Center
HCI	Hyperconverged Infrastructure
HEC	Hypertext Transfer Protocol (HTTP) Event Collector
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/A/RBAC	Identity, Attribute, Role-Based Access Control

IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
IBAC	Identity-Based Access Control
ICAM	Identity, Credential, and Access Management
ID	Identification
IDaaS	Identity as a Service
IdM	Identity Management
IdP	Identity Provider
IDS	Intrusion Detection Systems
IGA	Identity Governance and Administration
ILM	Identity Lifecycle Management
IoC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPsec	Internet Protocol Security
IR	Incident Response
IT	Information Technology
ITAM	IT Asset Management
ITOM	Information Technology Operations Management
ITSM	IT Service Management
JEA	Just Enough Administration
JIT	Just-In-Time
JSON	JavaScript Object Notation
KMS	Key Management System
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MDM	Mobile Device Management
MDR	Managed Detection and Response
MEF	Mission Essential Functionality
MFA	Multi-Factor Authentication
ML	Machine Learning
MSP	Managed Service Provider
mTLS	mutual Transport Layer Security
NAC	Network Access Control
NETCONF	Network Configuration
NextGen AV	Next-Generation Antivirus

NFV	Network Function Virtualization
NGFW	Next-Generation Firewall
NG-IPS	Next-Generation Intrusion Prevention System
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
OAuth	Open Authorization
OLTP	Online Transaction Processing
OMB	Office of Management and Budget
OS	Operating System
OT	Operational Technology
OT&E	Operational Test and Evaluation
OTP	One-Time Password
OWASP	Open Worldwide Application Security Project
PA	Policy Administrator
PaaS	Platform as a Service
PAM	Privileged Access Management
PAP	Policy Administration Point
PBAC	Policy-Based Access Control
PDP	Policy Decision Point
PE	Person Entity
PEP	Policy Enforcement Point
PfMO	Portfolio Management Office
PfMO	Portfolio Management Office
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIP	Policy Information Point
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKI	Public Key Infrastructure
PPE	Poisoned Pipeline Execution
PQC	Post-Quantum Cryptography
RA	Reference Architecture
RASP	Runtime Application Self-Protection
RBAC	Role-Based Access Control
REST	Representational State Transfer
RFP	Request for Proposal

RPO	Recovery Point Objective
RSA	Rivest-Shamir-Adleman
SaaS	Software as a Service
SAST	Static Application Security Testing
SBOM	Software Bills of Material
SCA	Software Composition Analysis
SCRM	Supply Chain Risk Management
SDC	Software-Defined Compute
SDLC	Software Development Lifecycle
SDN	Software-Defined Networking
SDS	Software-Define Storage
SID	Security Identifier
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMART	Specific, Measurable, Achievable, Relevant, and Time-bound
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SOP	Standard Operating Procedure
SP	Special Publication
SSH	Secure Shell
SSO	Single Sign-On
STIG	Security Technical Implementation Guide
STIX	Structured Threat Information eXpression
Syslog	System Log
T&E	Testing and Evaluation
TAXII	Trusted Automated Exchange of Intelligence Information
TEE	Trusted Execution Environments
TIP	Threat Intelligence Platform
TLS	Transport Layer Security
TTP	Tactics, Techniques, and Procedures
UAM	User Activity Monitoring
UEBA	User and Entity Behavior Analytics
UEDM	Unified Endpoint and Device Management
UEM	Unified Endpoint Management
USB	Universal Serial Bus
USG	United States Government
VA	Validation Authority
VPN	Virtual Private Network

VXLAN	Virtual Extensible Local Area Network
WAN	Wide Area Network
X.509	International Public Key Certificate Standard for secure signatures and web browsers
XaaS	Anything as a Service
XDR	Extended Detection and Response
XML	Extensible Markup Language
ZDT	Zero-Day Threat
ZIG	Zero Trust Implementation Guideline
ZT	Zero Trust
ZTA	Zero Trust Architecture

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/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.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 & 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 & Environment Pillar." 2024. Available: https://media.defense.gov/2024/Jul/10/2003500250/-1/-1/0/CSI-ZT-AUTOMATION-ORCHESTRATION-PILLAR.PDF

[10] National Security Agency. "CSI: Advancing Zero Trust Maturity Throughout the Automation & 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 & 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] Microsoft. "What is Privileged Access Management (PAM)?" 2025. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam

[14] Julian Ashbourn. "PKI Implementation and Infrastructures." 2023. Available: https://www.oreilly.com/library/view/pki-implementation-and/9781000844962/

[15] 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

[16] National Institute of Standards and Technology. "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41, Rev. 1." 2025. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[17] 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

[18] Defense Acquisition University. "Transforming Cybersecurity: Unified Endpoint and Device Management." 2024. Available: https://www.dau.edu/sites/default/files/2024-05/DAU%20Zero%20Trust%20Whitmer%2020240516.pdf

[19] 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

[20] National Institute of Standards and Technology. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST Special Publication 800-171, Rev. 3." 2024. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf

[21] Department of War Office of the Chief Information Officer. "A DoD Enterprise DevSecOps Reference Design, Version 0.01, b385." 2022. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoDRefDesignCloudGithub.pdf

[22] National Institute of Standards and Technology. "Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile, NIST Special Publication 800-218A." 2024. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf

[23] Department of War Office of the Chief Information Officer. "DoD Enterprise DevSecOps Strategy Guide, Version 2.0." 2021. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsStrategyGuide.pdf

[24] Department of War Office of the Chief Information Officer. "DevSecOps Playbook, Version 2.1." 2021. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DevSecOps%20Playbook_DoD-CIO_20211019.pdf

[25] Department of War and Office of the Deputy Secretary of War. "Department of Defense Software Modernization Strategy, Version 1.0." 2021. Available: https://media.defense.gov/2022/feb/03/2002932833/-1/-1/1/department-of-defense-software-modernization-strategy.pdf

[26] National Security Agency and Cybersecurity and Infrastructure Security Agency. "Cybersecurity Information (CSI): Defending Continuous Integration/Continuous Delivery (CI/CD) Environments, Version 1.0." 2023. Available:

[27] 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

[28] Microsoft. "Platform Code Integrity." 2024. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/code-integrity

[29] National Institute of Standards and Technology. "Secure Software Development Framework (SSDF), Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST Special Publication 800-218." 2022. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

[30] 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

[31] Department of War Office of the Chief Information Officer. "DoD Enterprise DevSecOps Reference Design, Version 1.0." 2019. Available: https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf

[32] GeeksforGeeks. "Baseline Items in Software Development." 2024. Available: https://www.geeksforgeeks.org/baseline-items-in-software-development/

[33] National Institute of Standards and Technology. "Control Baselines for Information Systems and Organizations, NIST Special Publication 800-53B." 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

[34] 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

[35] MITRE. "MITRE ATT&CK." 2025. Available: https://attack.mitre.org

[36] National Institute of Standards and Technology. "Guide to Computer Security Log Management, NIST Special Publication 800-92." 2006. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

[37] Cybersecurity and Infrastructure Security Agency. "Continuous Diagnostics and Mitigation (CDM) Program." 2025. Available: https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program

[38] 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

[39] National Institute of Standards and Technology. "An Introduction to Information Security, NIST Special Publication 800-12, Rev. 1." 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.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] 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

[42] Department of War. "Common Access Card (CAC)." n.d. Available: https://www.cac.mil/Common-Access-Card/

[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] Defense Acquisition University. "Cyber Survivability Endorsement Implementation Guide." n.d. Available: https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Guide%20-%20Cyber%20Survivability%20Endorsement%20Implementation.pdf

[45] 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/

[46] Congressional Research Service. "The U.S. Defense Industrial Base: Background and Issues for Congress." 2024. Available: https://www.congress.gov/crs-product/R47751

[47] MITRE. "MITRE D3FEND." 2025. Available: https://d3fend.mitre.org

[48] General Services Administration. "Identity Lifecycle Management Playbook." 2024. Available: https://www.idmanagement.gov/playbooks/ilm/#stage-2---provisioning--identity-governance-administration-iga

[49] 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

[50] Government Accountability Office. "Agile Assessment Guide: Best Practices for Adoption and Implementation." 2023. Available: https://www.gao.gov/assets/d24105506.pdf

[51] 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#

[52] Defense Acquisition University. "Defense Acquisition University Glossary." n.d. Available: https://www.dau.edu/glossary

[53] 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

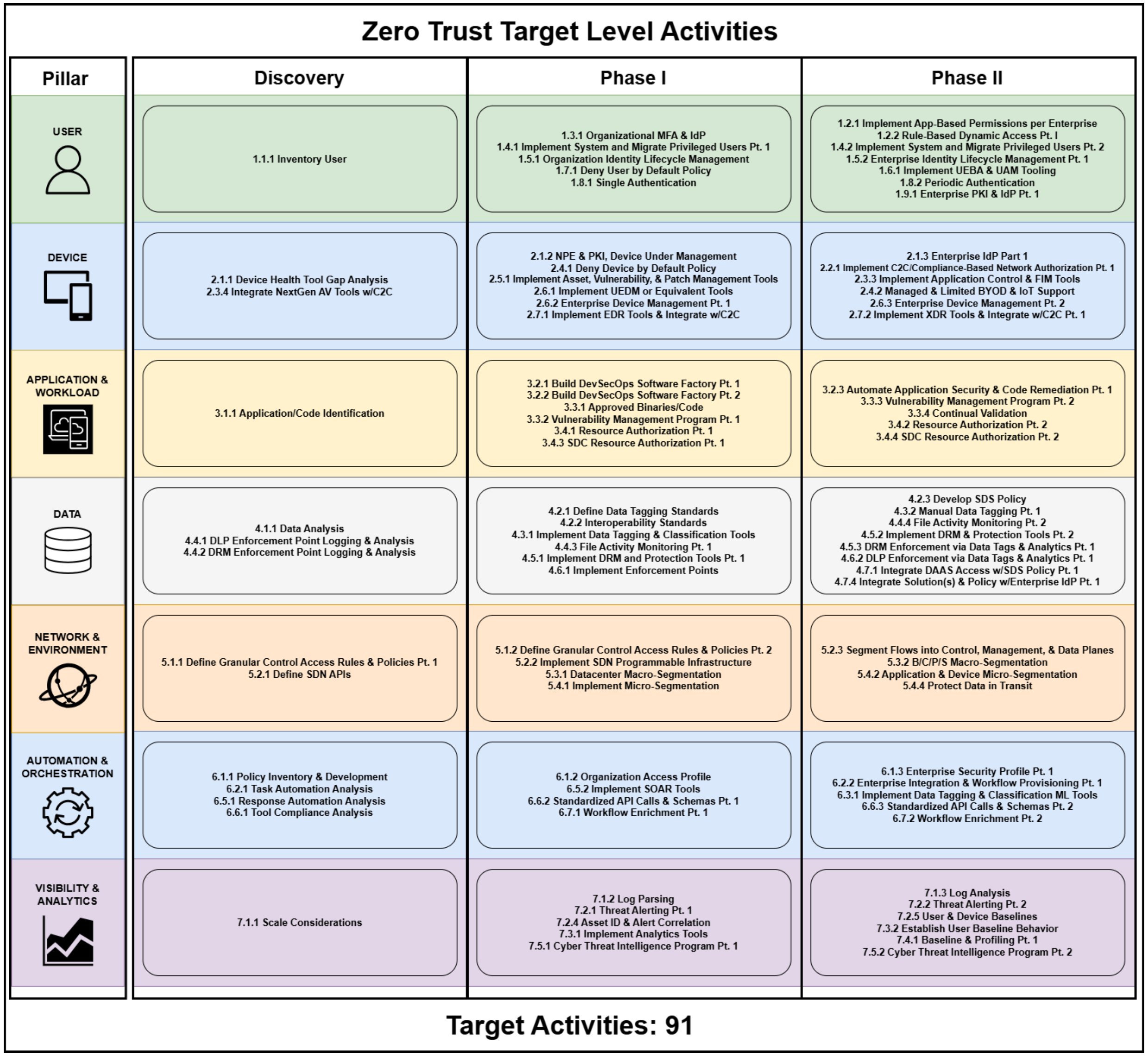
[54] National Institute of Standards and Technology. "Security of Interactive and Automated Access Management Using Secure Shell (SSH), NIST IR 7966." 2015. Available: https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.7966.pdf

[55] 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 1.3.1 Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)

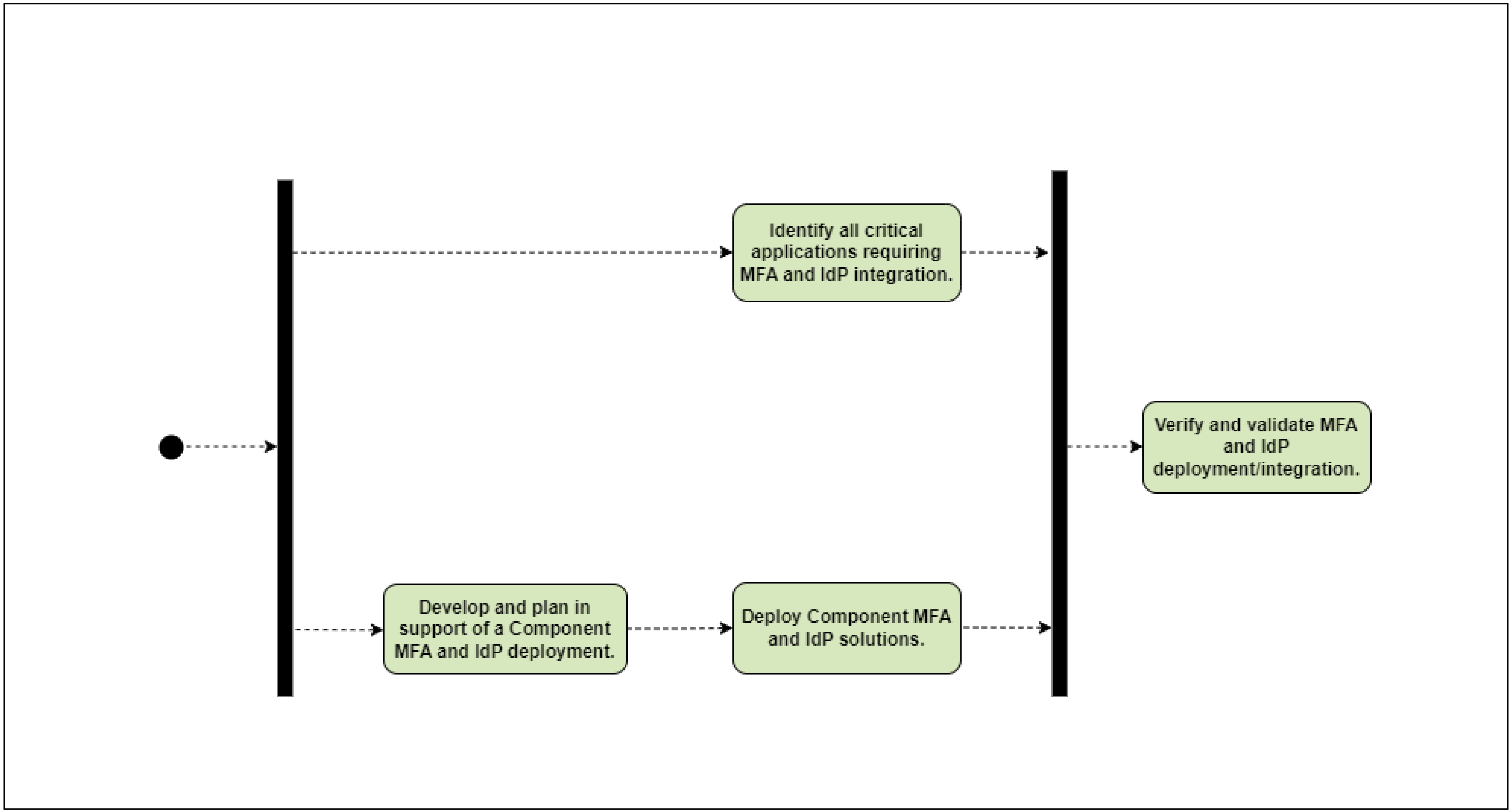

Identify all critical applications requiring MFA and IdP integration.
Develop and plan in support of a Component MFA and IdP deployment.
Deploy Component MFA and IdP solutions.
Verify and validate MFA and IdP deployment/integration.

Figure D-2: Implementation Tasks for Activity 1.3.1 — *Organizational Multi-Factor Authentication (MFA) and Identity Provider (IdP)*

Activity 1.4.1 Implement System and Migrate Privileged Users Part 1

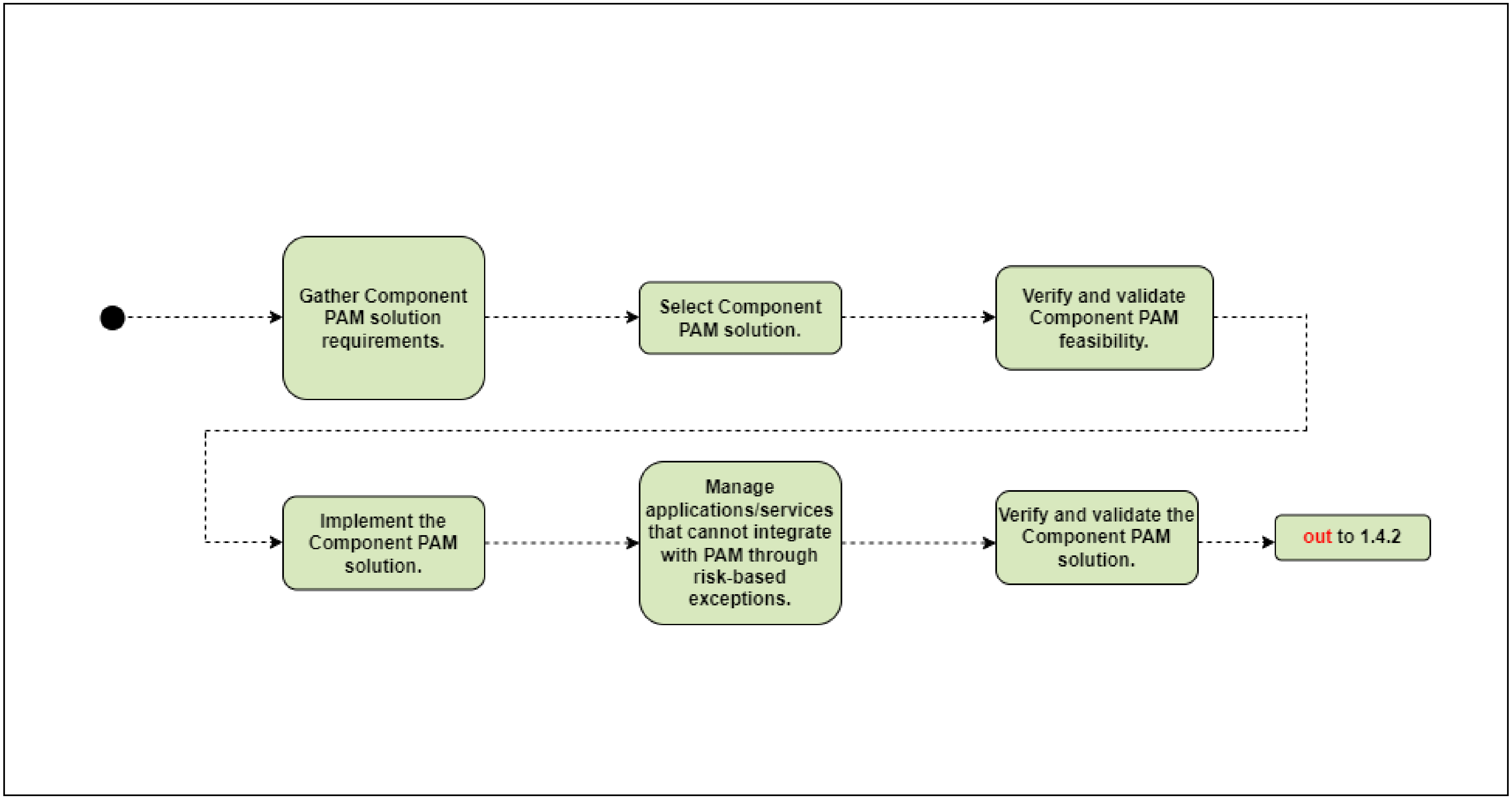

Gather Component PAM solution requirements.
Select Component PAM solution.
Verify and validate Component PAM feasibility.
Implement the Component PAM solution.
Manage applications/services that cannot integrate with PAM through risk-based exceptions.
Verify and validate the Component PAM solution.
out to 1.4.2

Figure D-3: Implementation Tasks for Activity 1.4.1 — *Implement System and Migrate Privileged Users Part 1*

Activity 1.5.1 Organizational Identity Lifecycle Management (ILM)

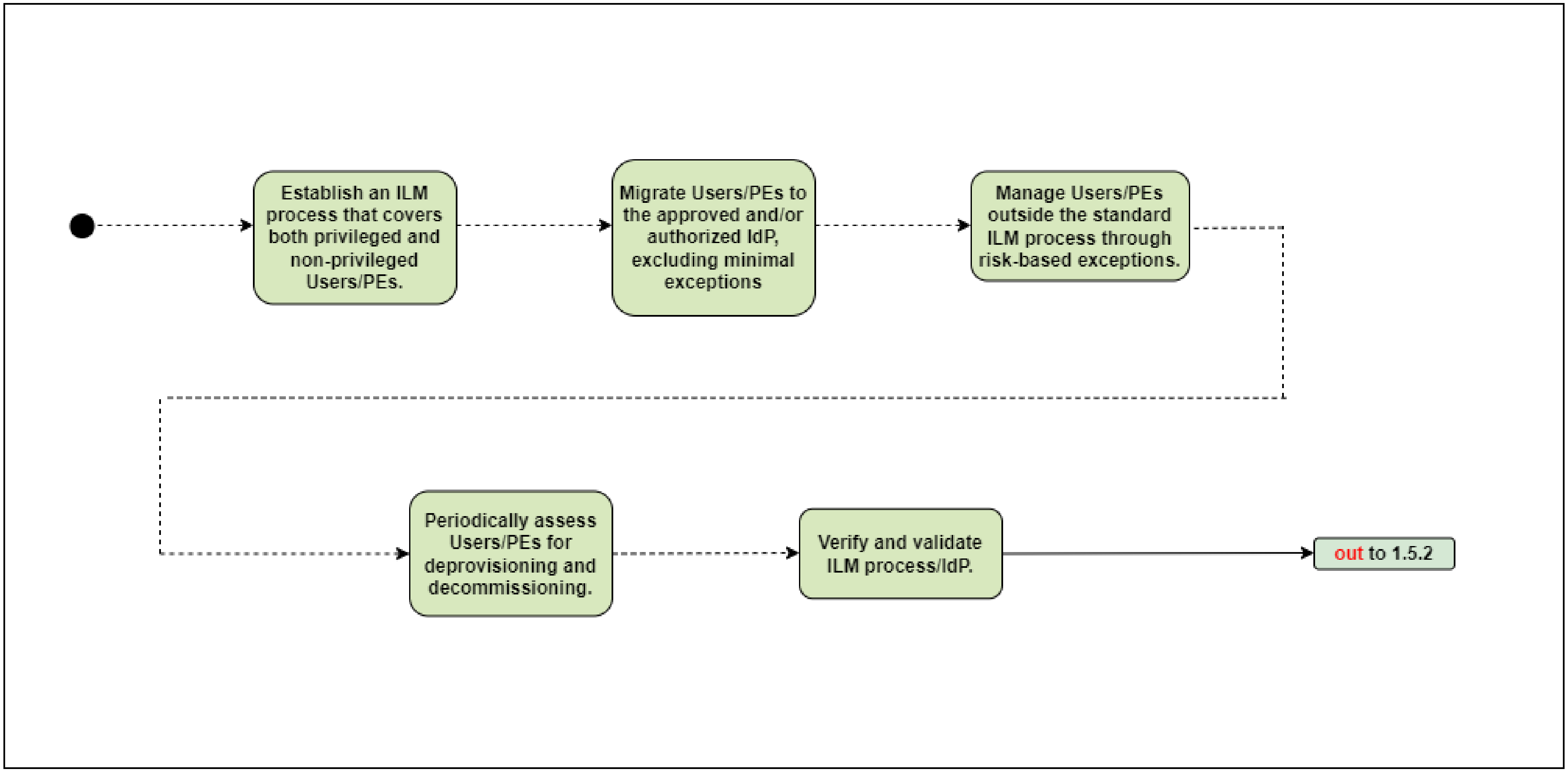

Establish an ILM process that covers both privileged and non-privileged Users/PEs.
Migrate Users/PEs to the approved and/or authorized IdP, excluding minimal exceptions
Manage Users/PEs outside the standard ILM process through risk-based exceptions.
Periodically assess Users/PEs for deprovisioning and decommissioning.
Verify and validate ILM process/IdP.
out to 1.5.2

Figure D-4: Implementation Tasks for Activity 1.5.1 — *Organizational Identity Lifecycle Management (ILM)*

Activity 1.7.1 Deny User by Default Policy

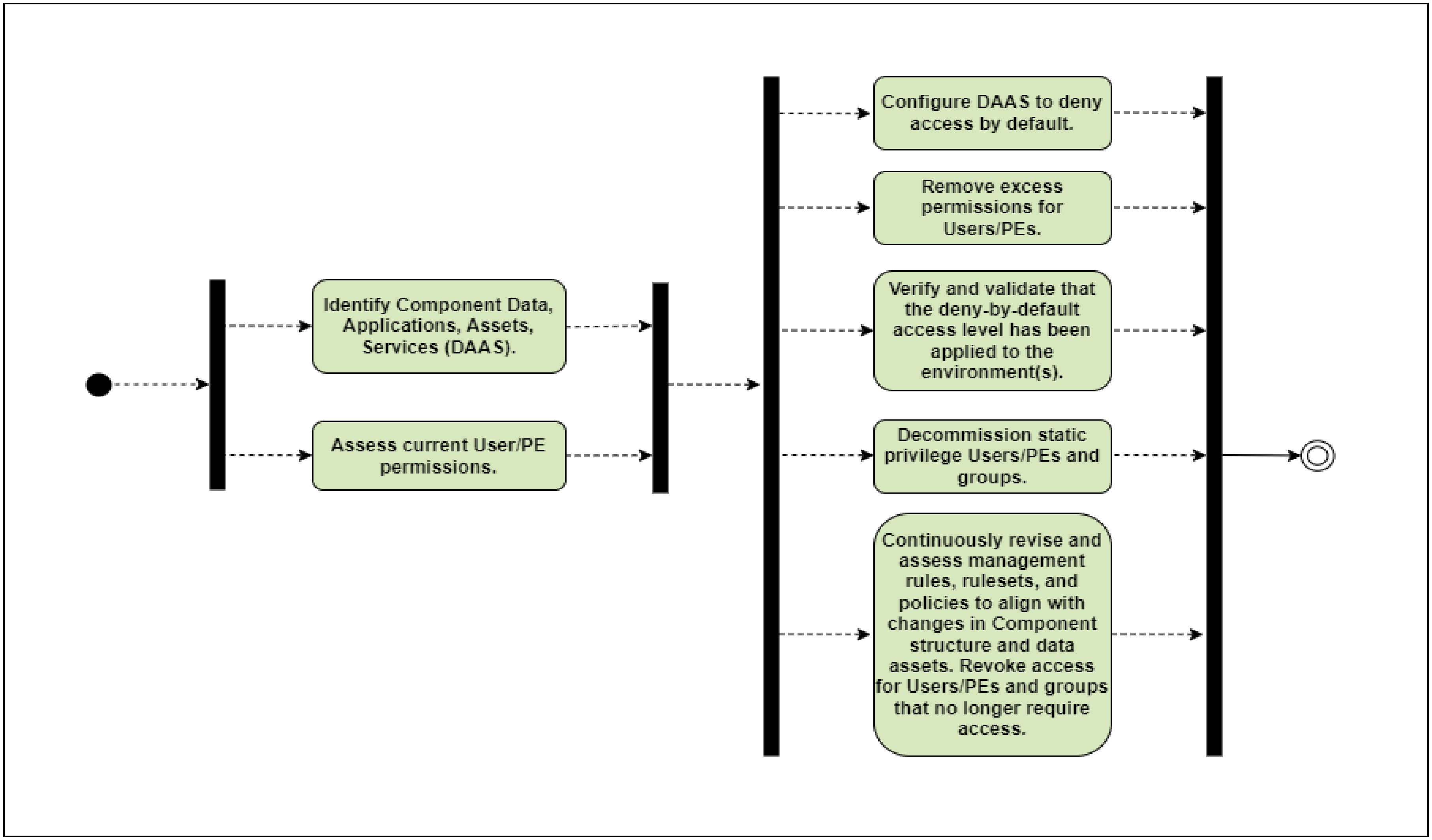

Identify Component Data, Applications, Assets, Services (DAAS).
Assess current User/PE permissions.
Configure DAAS to deny access by default.
Remove excess permissions for Users/PEs.
Verify and validate that the deny-by-default access level has been applied to the environment(s).
Decommission static privilege Users/PEs and groups.
Continuously revise and assess management rules, rulesets, and policies to align with changes in Component structure and data assets. Revoke access for Users/PEs and groups that no longer require access.

Figure D-5: Implementation Tasks for Activity 1.7.1 — *Deny User by Default Policy*

Activity 1.8.1 Single Authentication

Flow chart illustrating Activity *x.x.x – Activity Title* using the steps outlined in the Implementation Tasks for Activity 1.1.1 table.

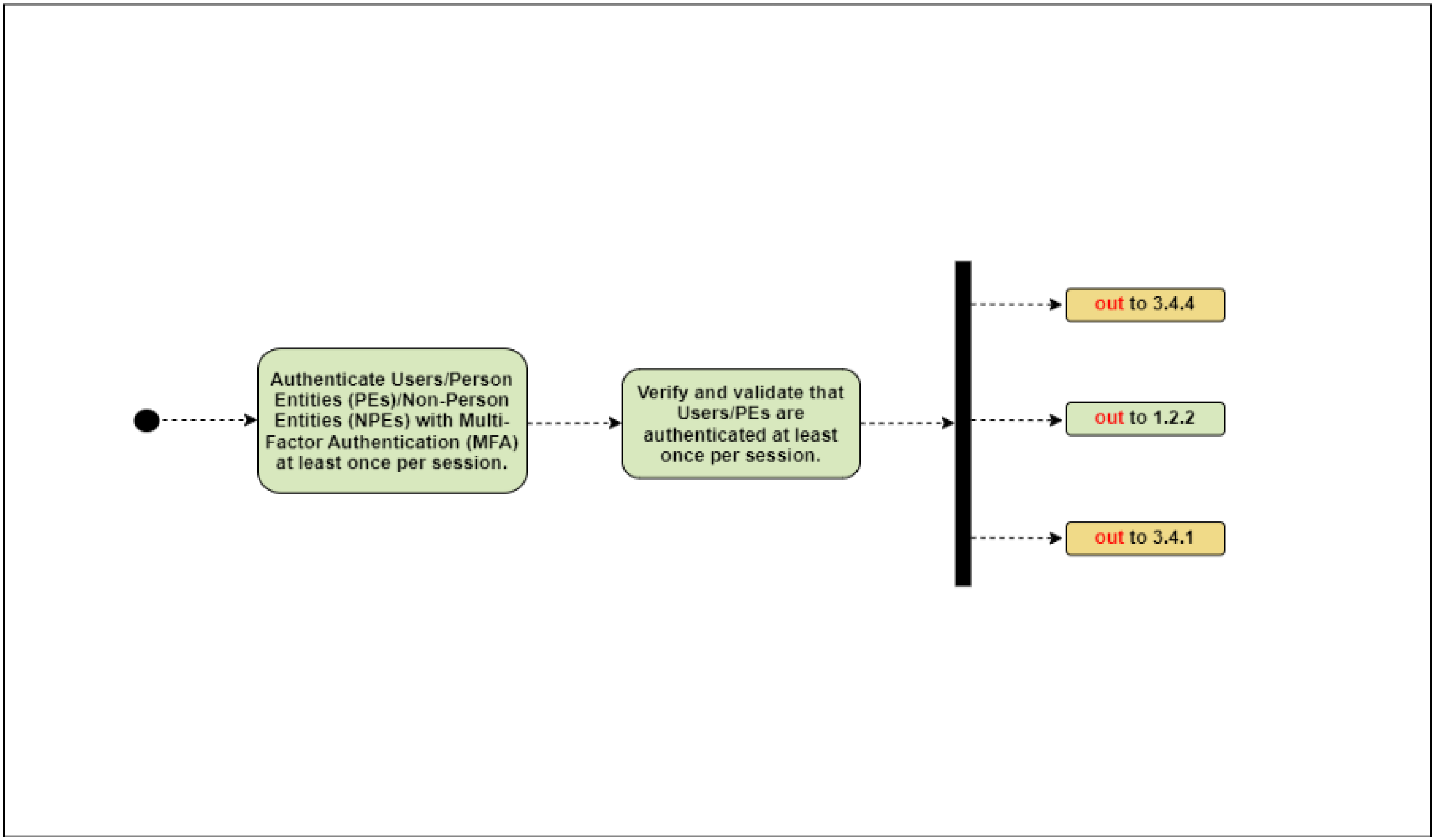

Authenticate Users/Person Entities (PEs)/Non-Person Entities (NPEs) with Multi-Factor Authentication (MFA) at least once per session.
Verify and validate that Users/PEs are authenticated at least once per session.
out to 3.4.4
out to 1.2.2
out to 3.4.1

Figure D-6: Implementation Tasks for Activity 1.8.1 — *Single Authentication*

Activity 2.1.2 Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management

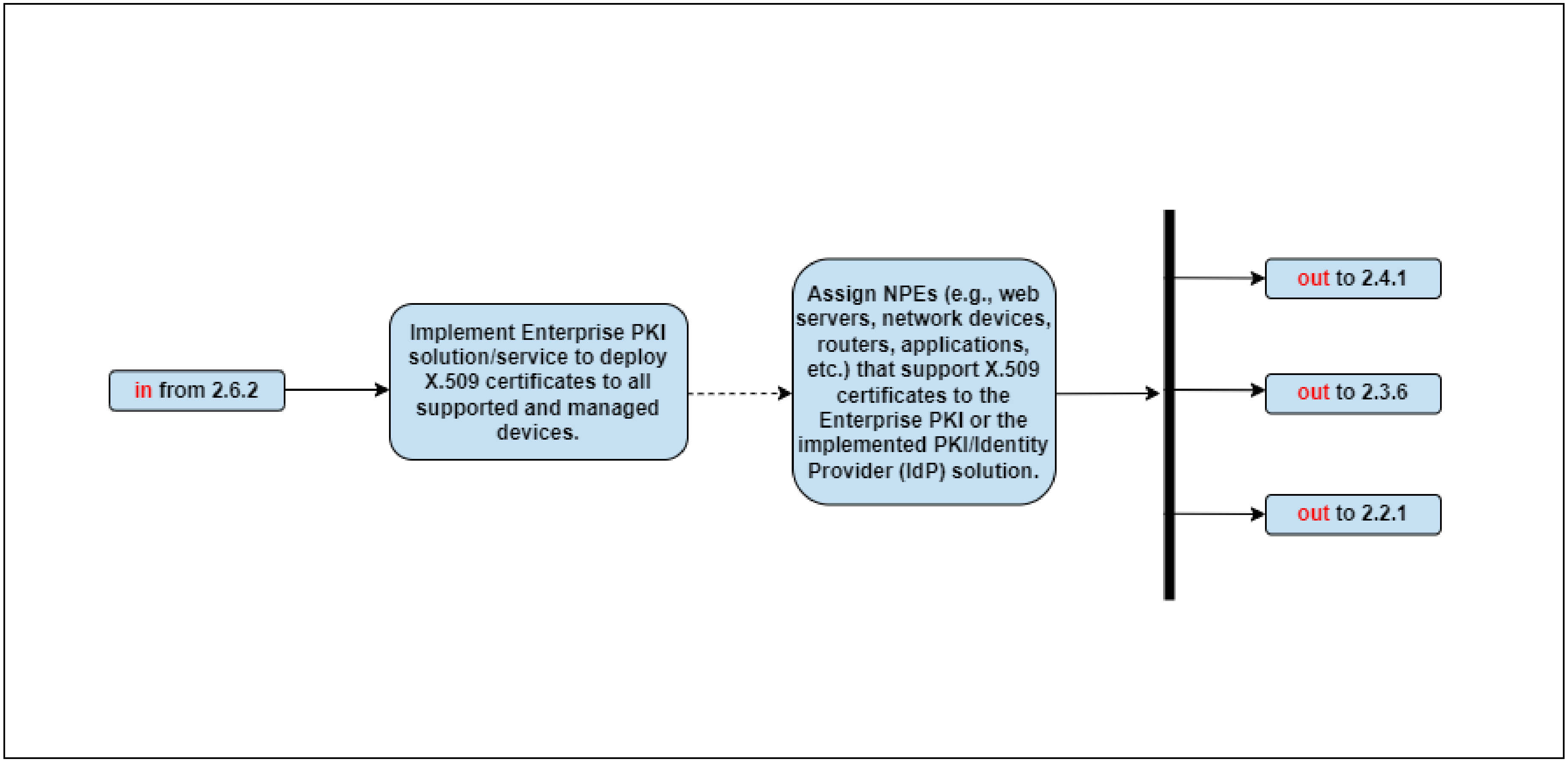

in from 2.6.2
Implement Enterprise PKI solution/service to deploy X.509 certificates to all supported and managed devices.
Assign NPEs (e.g., web servers, network devices, routers, applications, etc.) that support X.509 certificates to the Enterprise PKI or the implemented PKI/Identity Provider (IdP) solution.
out to 2.4.1
out to 2.3.6
out to 2.2.1

Figure D-7: Implementation Tasks for Activity 2.1.2 — *Non-Person Entity (NPE) and Public Key Infrastructure (PKI), Device Under Management*

Activity 2.4.1 Deny Device by Default Policy

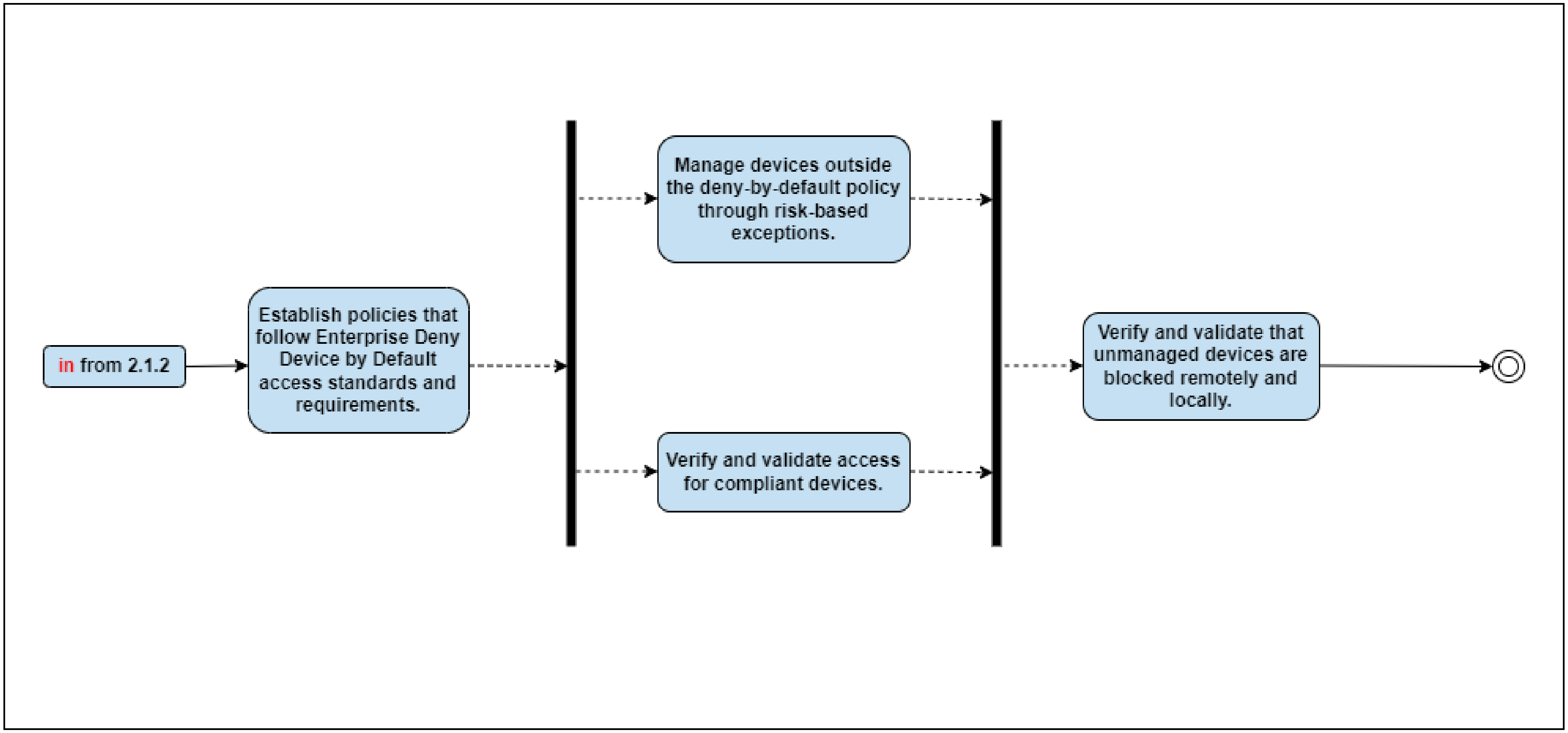

in from 2.1.2
Establish policies that follow Enterprise Deny Device by Default access standards and requirements.
Manage devices outside the deny-by-default policy through risk-based exceptions.
Verify and validate access for compliant devices.
Verify and validate that unmanaged devices are blocked remotely and locally.

Figure D-8: Implementation Tasks for Activity 2.4.1 — *Deny Device by Default Policy*

Activity 2.5.1 Implement Asset, Vulnerability, and Patch Management Tools

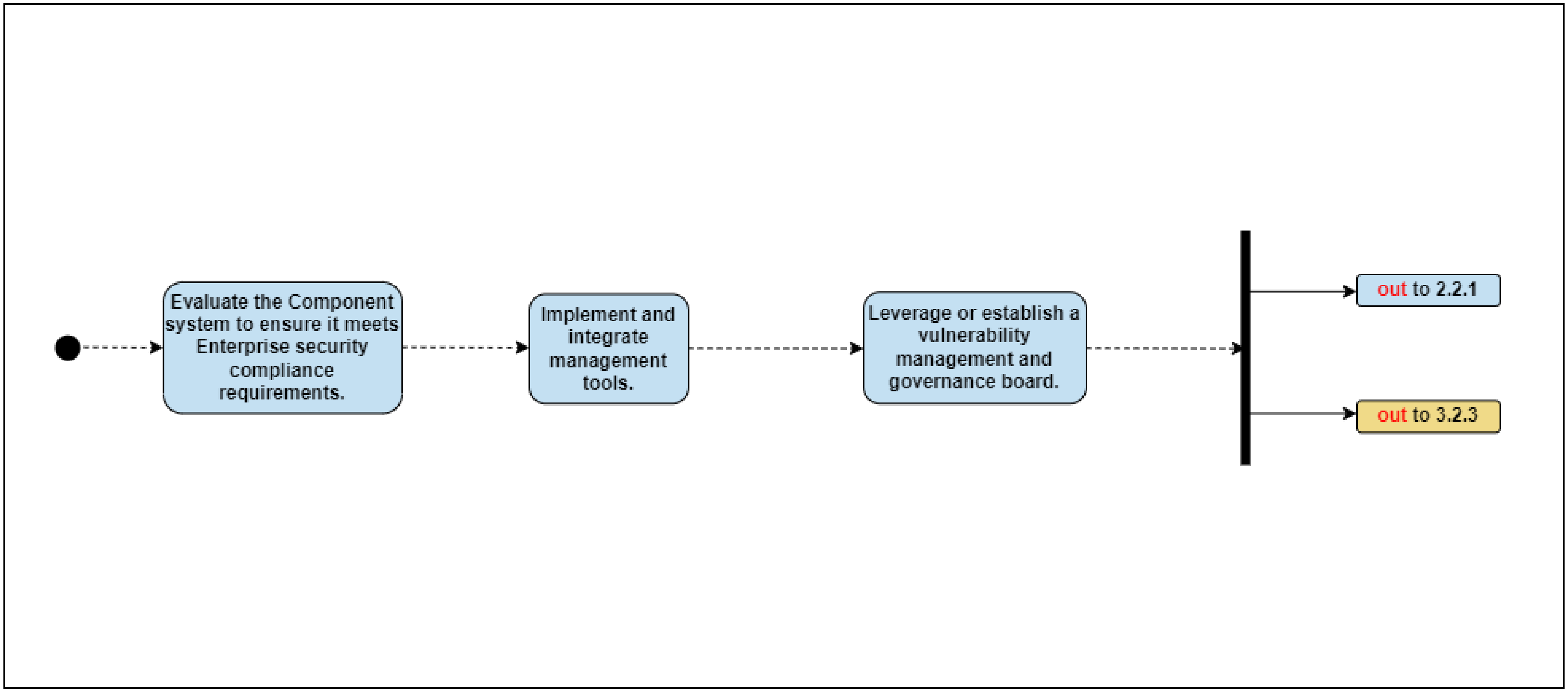

Evaluate the Component system to ensure it meets Enterprise security compliance requirements.
Implement and integrate management tools.
Leverage or establish a vulnerability management and governance board.
out to 2.2.1
out to 3.2.3

Figure D-9: Implementation Tasks for Activity 2.5.1 — *Implement Asset, Vulnerability, and Patch Management Tools*

Activity 2.6.1 Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools

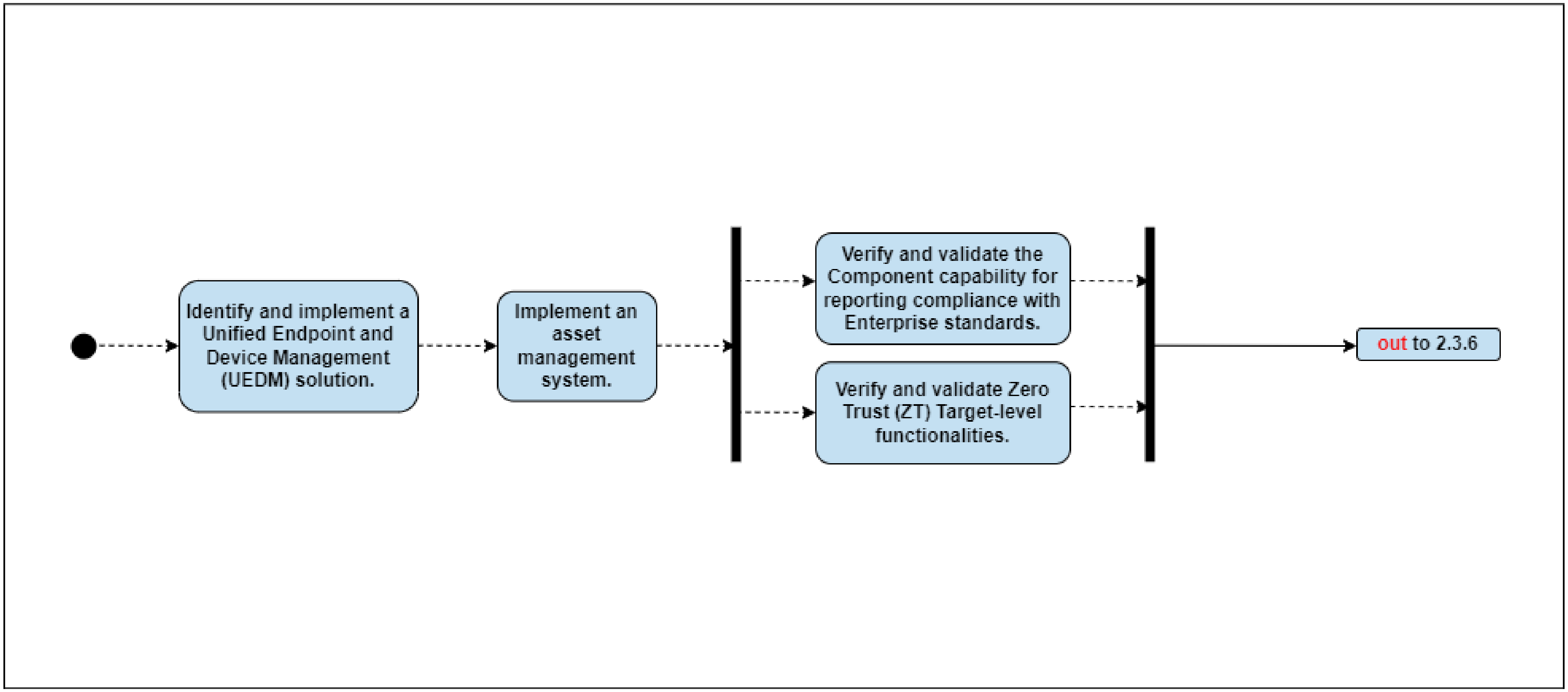

Identify and implement a Unified Endpoint and Device Management (UEDM) solution.
Implement an asset management system.
Verify and validate the Component capability for reporting compliance with Enterprise standards.
Verify and validate Zero Trust (ZT) Target-level functionalities.
out to 2.3.6

Figure D-10: Implementation Tasks for Activity 2.6.1 — *Implement Unified Endpoint and Device Management (UEDM) or Equivalent Tools*

Activity 2.6.2 Enterprise Device Management (EDM) Part 1

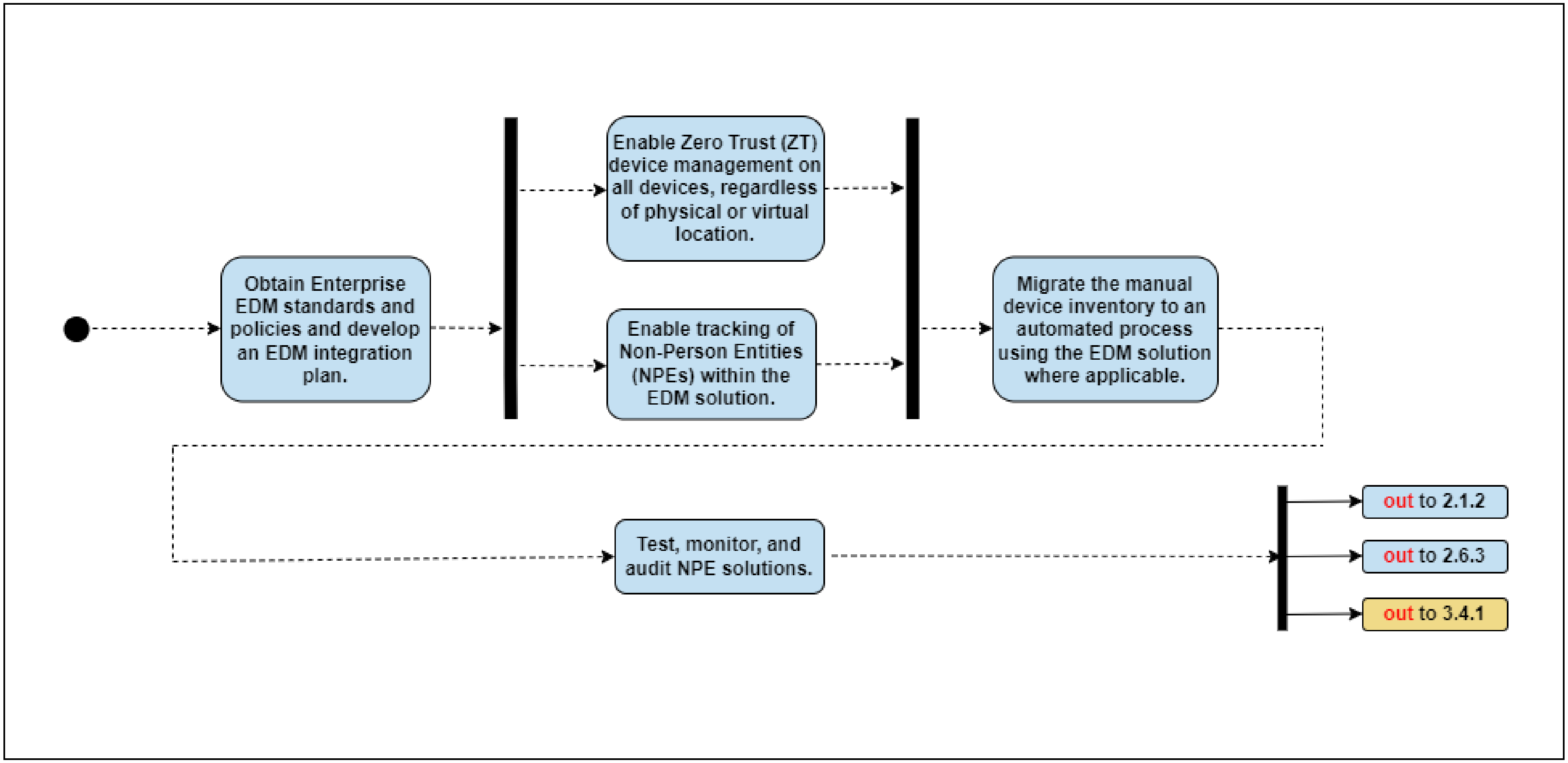

Obtain Enterprise EDM standards and policies and develop an EDM integration plan.
Enable Zero Trust (ZT) device management on all devices, regardless of physical or virtual location.
Enable tracking of Non-Person Entities (NPEs) within the EDM solution.
Migrate the manual device inventory to an automated process using the EDM solution where applicable.
Test, monitor, and audit NPE solutions.
out to 2.1.2
out to 2.6.3
out to 3.4.1

Figure D-11: Implementation Tasks for Activity 2.6.2 — *Enterprise Device Management (EDM) Part 1*

Activity 2.7.1 Implement Endpoint Detection and Response (EDR) Tools and Integrate with Comply-to-Connect (C2C)

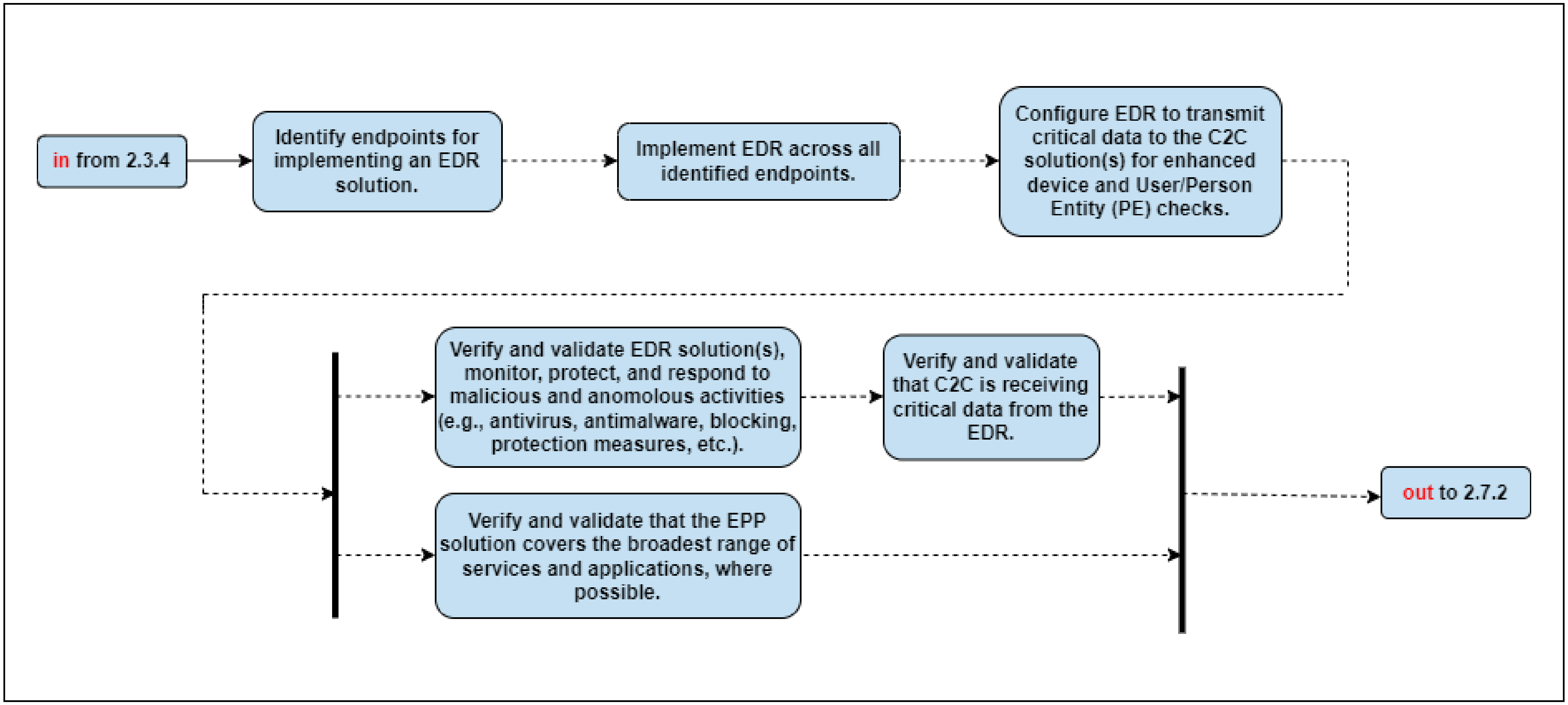

in from 2.3.4
Identify endpoints for implementing an EDR solution.
Implement EDR across all identified endpoints.
Configure EDR to transmit critical data to the C2C solution(s) for enhanced device and User/Person Entity (PE) checks.
Verify and validate EDR solution(s), monitor, protect, and respond to malicious and anomolous activities (e.g., antivirus, antimalware, blocking, protection measures, etc.).
Verify and validate that C2C is receiving critical data from the EDR.
Verify and validate that the EPP solution covers the broadest range of services and applications, where possible.
out to 2.7.2

Figure D-12: Implementation Tasks for Activity 2.7.1 — *Implement Endpoint Detection and Response (EDR) Tools and Integrate with Comply-to-Connect (C2C)*

Activity 3.2.1 Build Development, Security, and Operations (DevSecOps) Software Factory Part 1

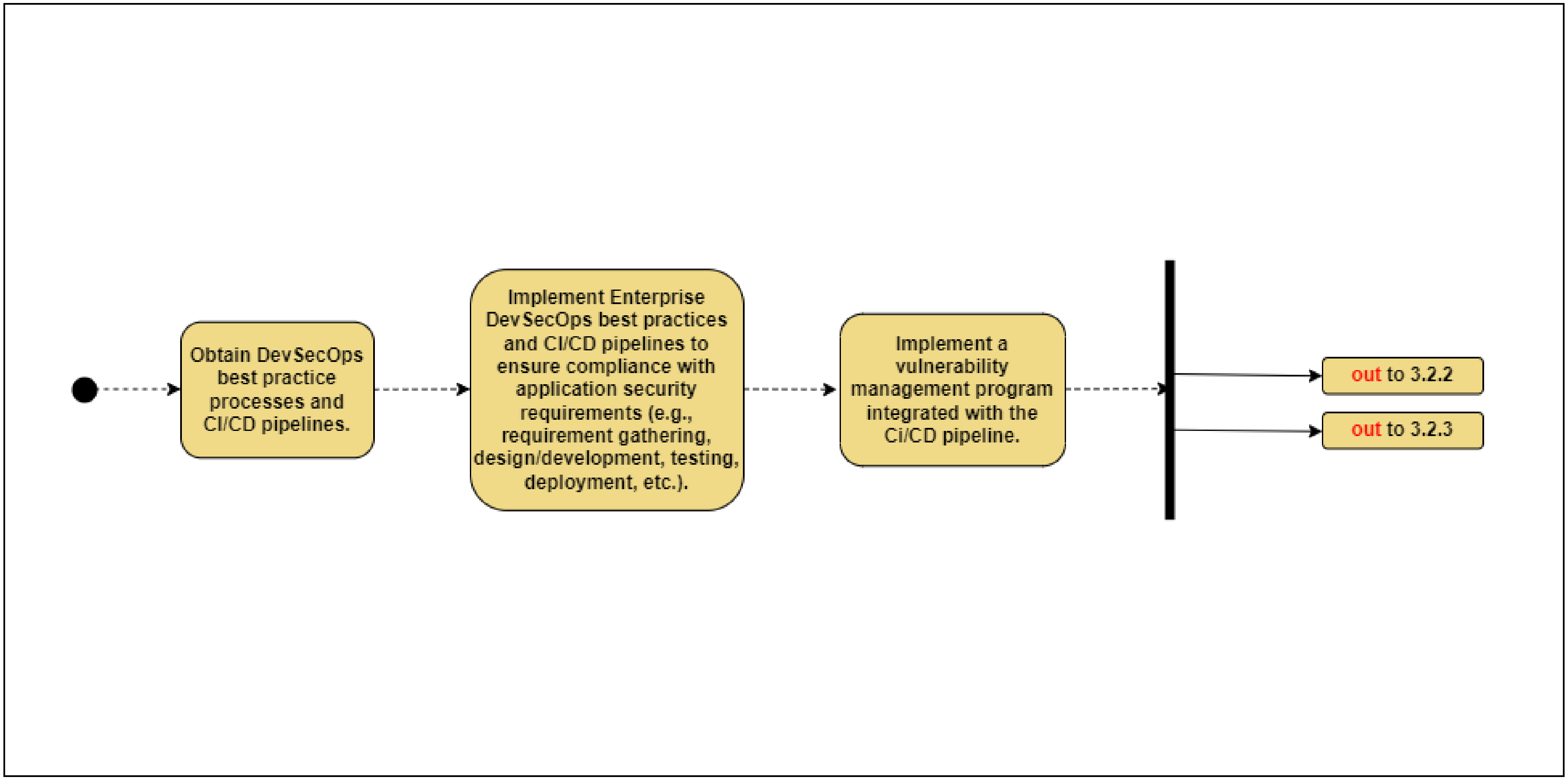

Obtain DevSecOps best practice processes and CI/CD pipelines.
Implement Enterprise DevSecOps best practices and CI/CD pipelines to ensure compliance with application security requirements (e.g., requirement gathering, design/development, testing, deployment, etc.).
Implement a vulnerability management program integrated with the Ci/CD pipeline.
out to 3.2.2
out to 3.2.3

Figure D-13: Implementation Tasks for Activity 3.2.1 — *Build Development, Security, and Operations (DevSecOps) Software Factory Part 1*

Activity 3.2.2 Build Development, Security, and Operations (DevSecOps) Software Factory Part 2

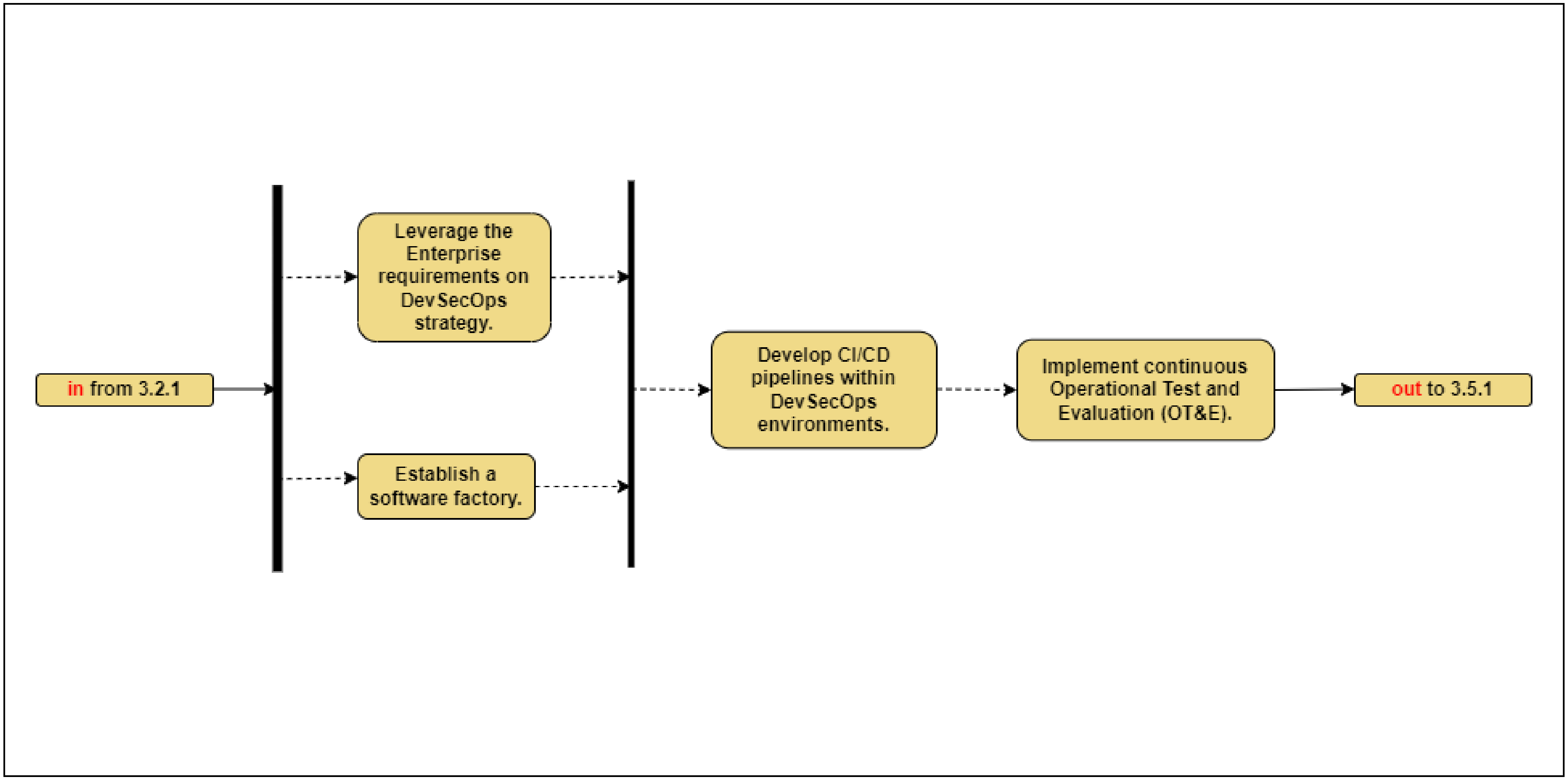

in from 3.2.1
Leverage the Enterprise requirements on DevSecOps strategy.
Establish a software factory.
Develop CI/CD pipelines within DevSecOps environments.
Implement continuous Operational Test and Evaluation (OT&E).
out to 3.5.1

Figure D-14: Implementation Tasks for Activity 3.2.2 — *Build Development, Security, and Operations (DevSecOps) Software Factory Part 2*

Activity 3.3.1 Approved Binaries and Code

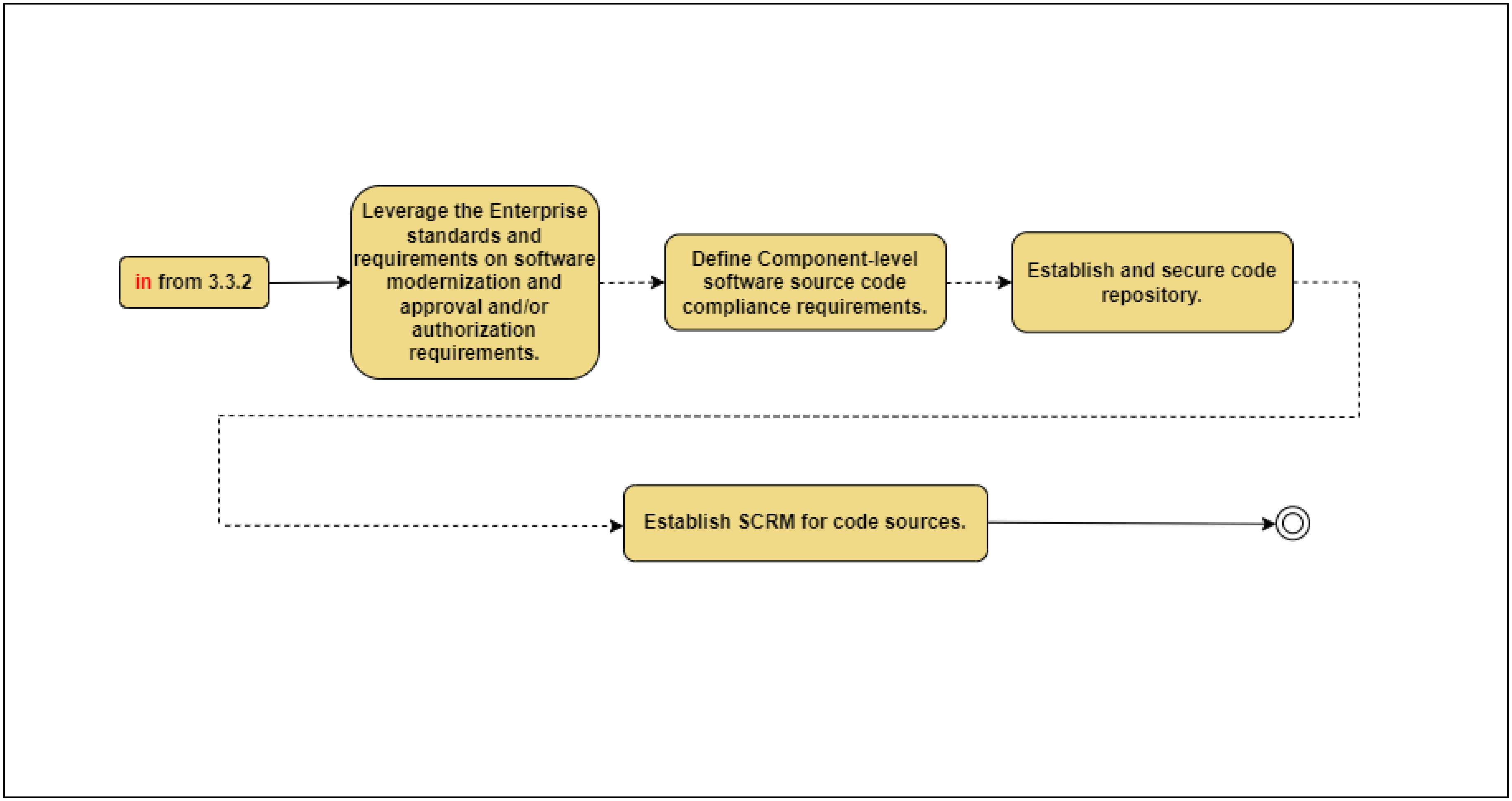

in from 3.3.2
Leverage the Enterprise standards and requirements on software modernization and approval and/or authorization requirements.
Define Component-level software source code compliance requirements.
Establish and secure code repository.
Establish SCRM for code sources.

Figure D-15: Implementation Tasks for Activity 3.3.1 — *Approved Binaries and Code*

Activity 3.3.2 Vulnerability Management Program Part 1

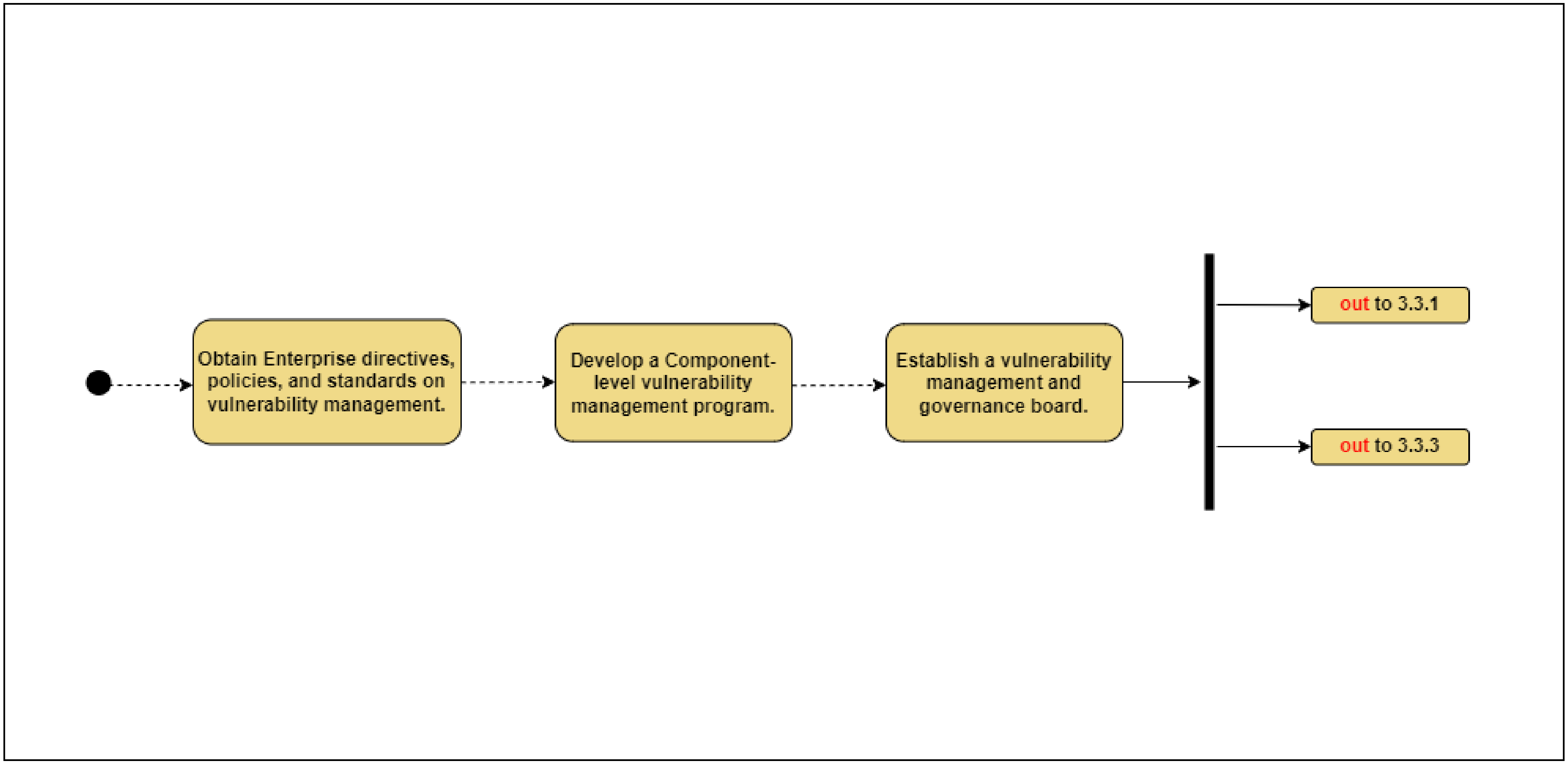

Obtain Enterprise directives, policies, and standards on vulnerability management.
Develop a Component-level vulnerability management program.
Establish a vulnerability management and governance board.
out to 3.3.1
out to 3.3.3

Figure D-16: Implementation Tasks for Activity 3.3.2 — *Vulnerability Management Program Part 1*

Activity 3.4.1 Resource Authorization Part 1

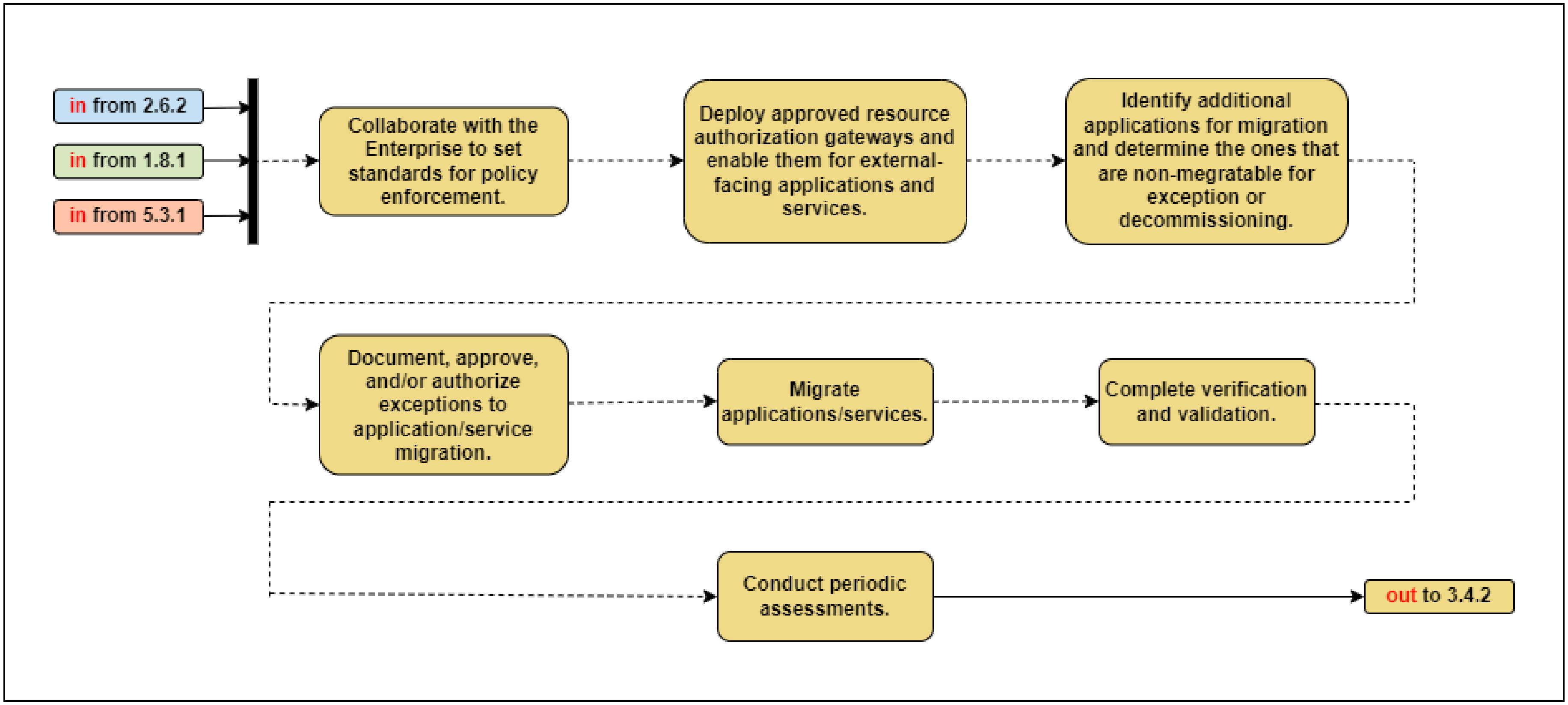

in from 2.6.2
in from 1.8.1
in from 5.3.1
Collaborate with the Enterprise to set standards for policy enforcement.
Deploy approved resource authorization gateways and enable them for external-facing applications and services.
Identify additional applications for migration and determine the ones that are non-megratable for exception or decommissioning.
Document, approve, and/or authorize exceptions to application/service migration.
Migrate applications/services.
Complete verification and validation.
Conduct periodic assessments.
out to 3.4.2

Figure D-17: Implementation Tasks for Activity 3.4.1 — *Resource Authorization Part 1*

Activity 3.4.3 Software-Defined Compute (SDC) Resource Authorization Part 1

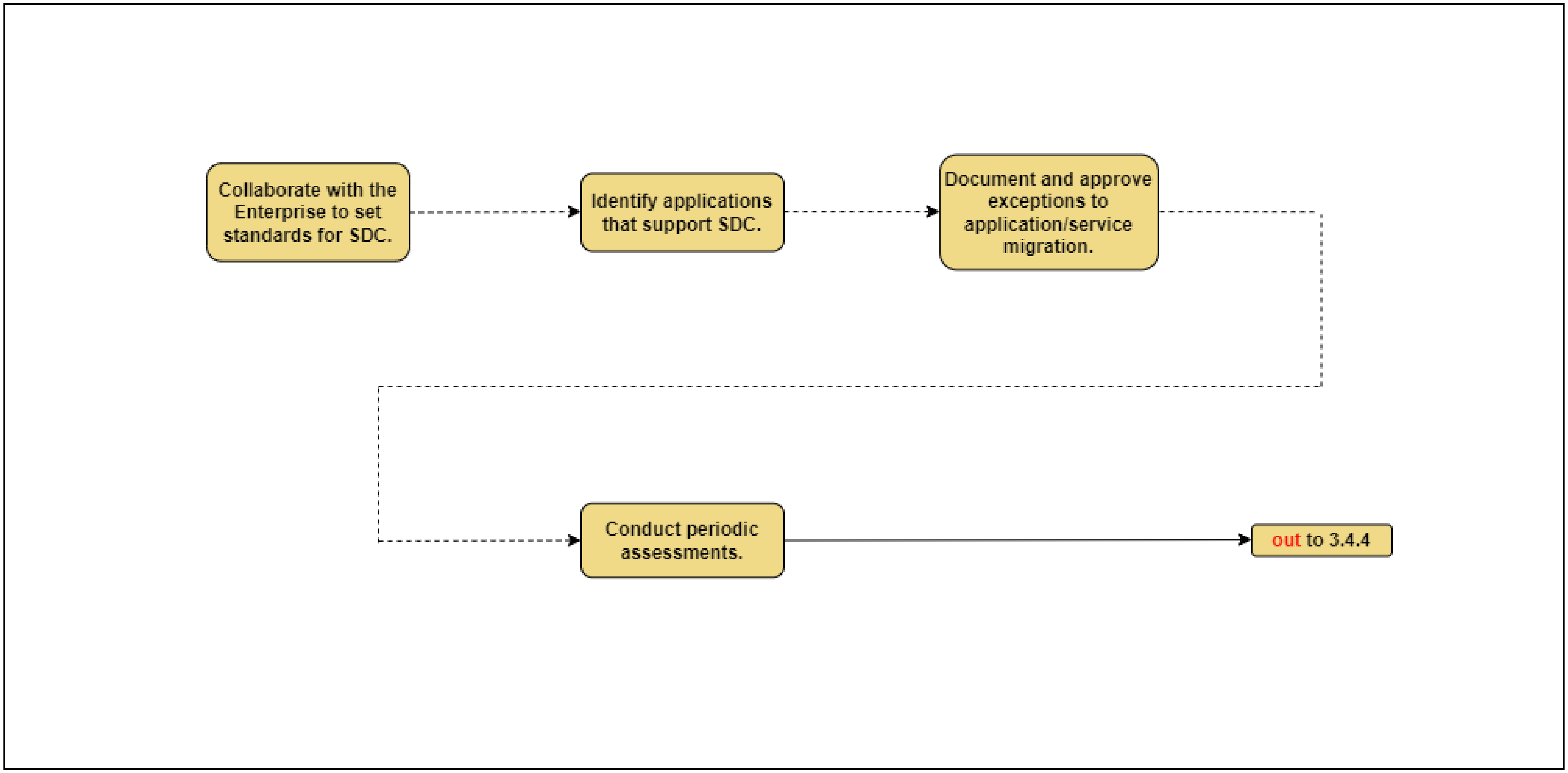

Collaborate with the Enterprise to set standards for SDC.
Identify applications that support SDC.
Document and approve exceptions to application/service migration.
Conduct periodic assessments.
out to 3.4.4

Figure D-18: Implementation Tasks for Activity 3.4.3 — *Software-Defined Compute (SDC) Resource Authorization Part 1*

Activity 4.2.1 Define Data Tagging Standards

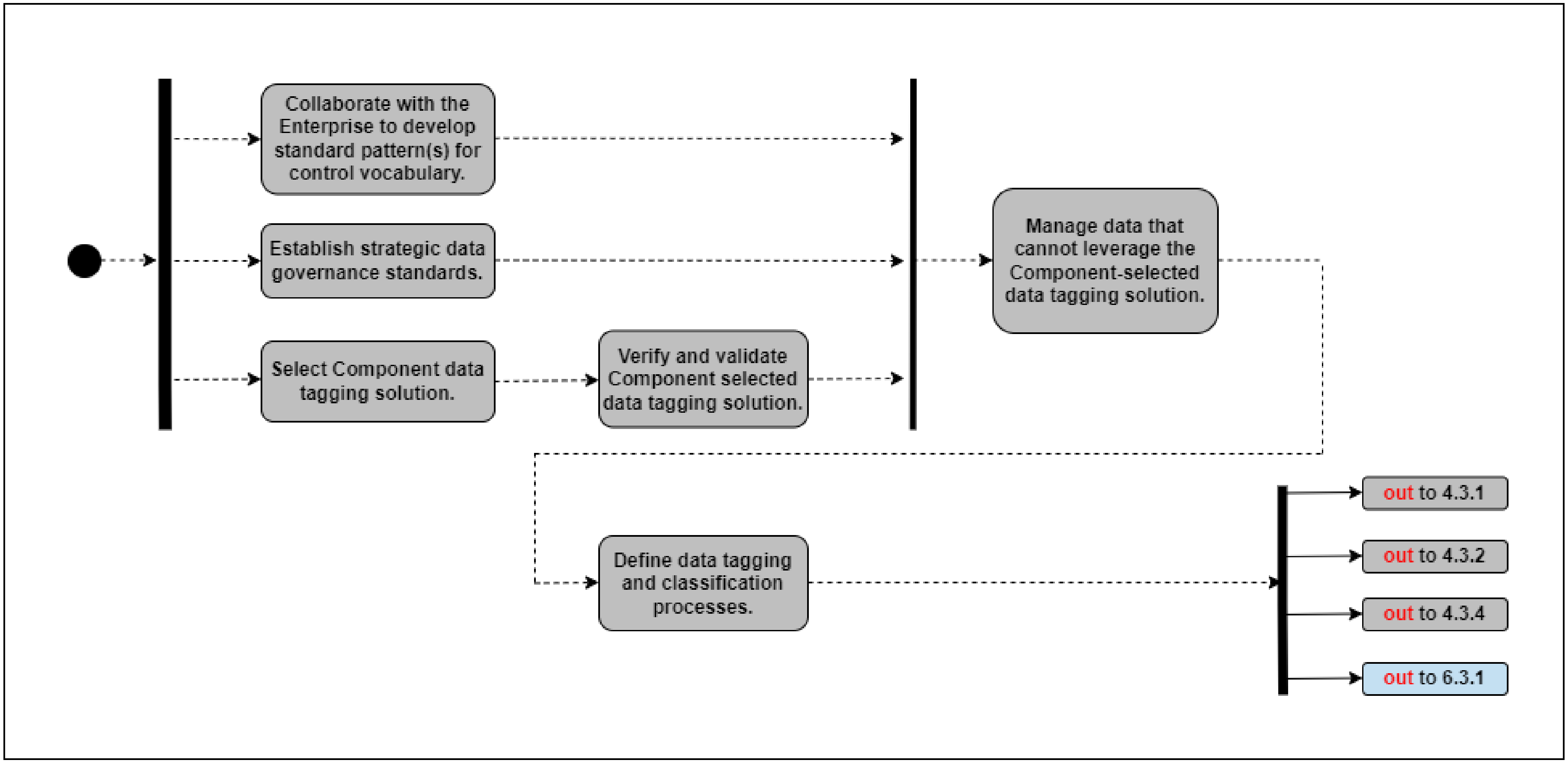

Collaborate with the Enterprise to develop standard pattern(s) for control vocabulary.
Establish strategic data governance standards.
Select Component data tagging solution.
Verify and validate Component selected data tagging solution.
Manage data that cannot leverage the Component-selected data tagging solution.
Define data tagging and classification processes.
out to 4.3.1
out to 4.3.2
out to 4.3.4
out to 6.3.1

Figure D-19: Implementation Tasks for Activity 4.2.1 — *Define Data Tagging Standards*

Activity 4.2.2 Interoperability Standards

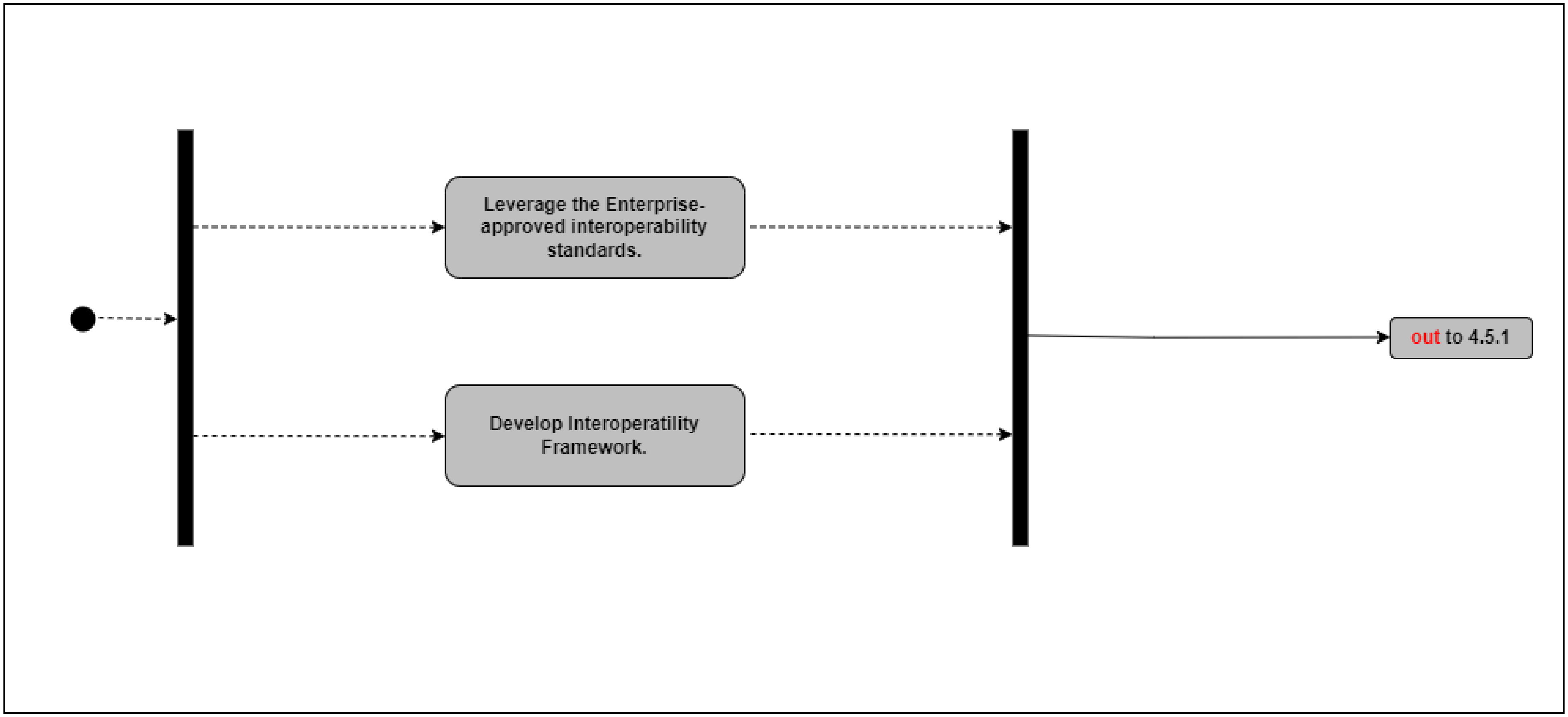

Leverage the Enterprise-approved interoperability standards.
Develop Interoperatility Framework.
out to 4.5.1

Figure D-20: Implementation Tasks for Activity 4.2.2 — *Interoperability Standards*

Activity 4.3.1 Implement Data Tagging and Classification Tools

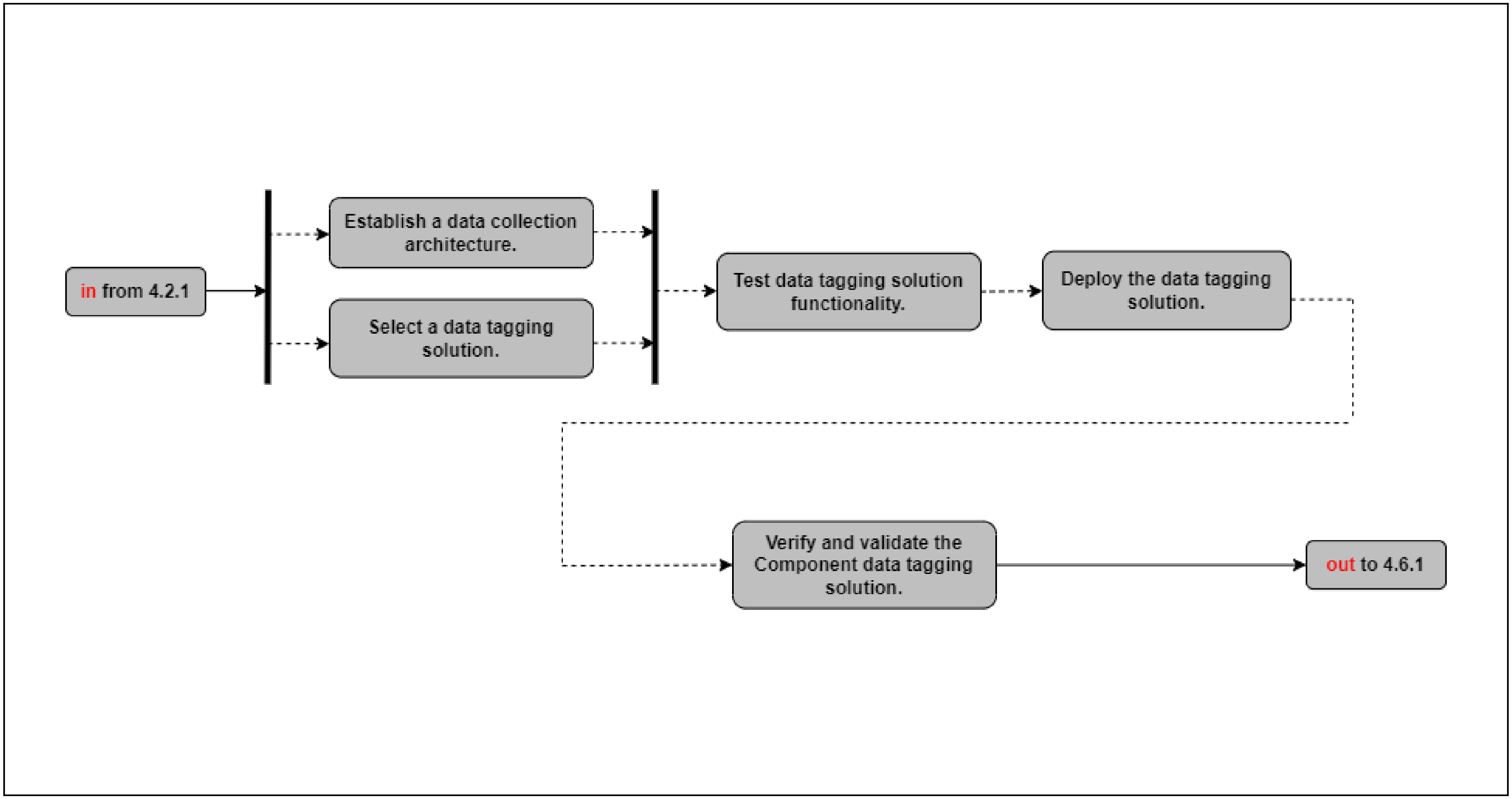

in from 4.2.1
Establish a data collection architecture.
Select a data tagging solution.
Test data tagging solution functionality.
Deploy the data tagging solution.
Verify and validate the Component data tagging solution.
out to 4.6.1

Figure D-21: Implementation Tasks for Activity 4.3.1 — *Implement Data Tagging and Classification Tools*

Activity 4.4.3 File Activity Monitoring Part 1

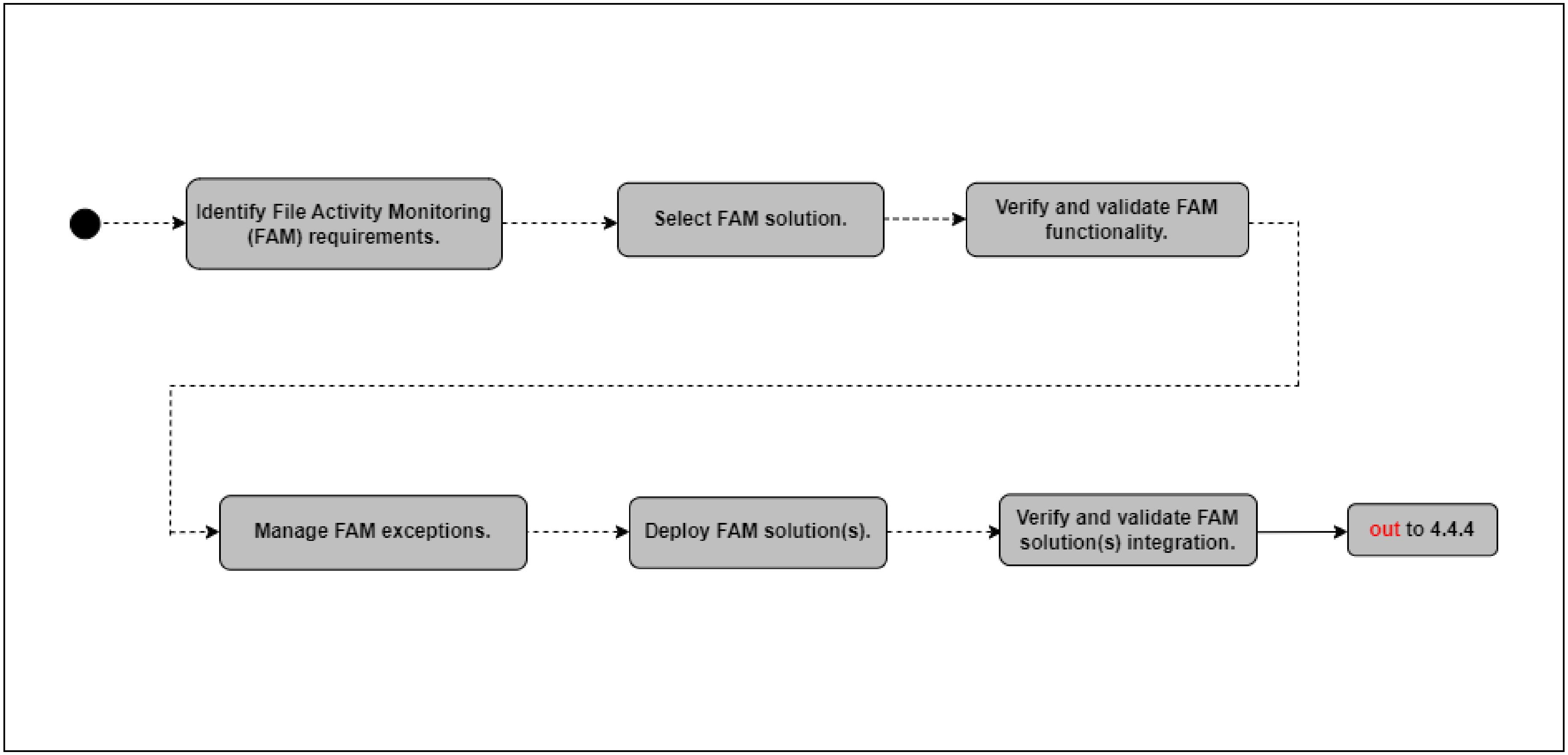

Identify File Activity Monitoring (FAM) requirements.
Select FAM solution.
Verify and validate FAM functionality.
Manage FAM exceptions.
Deploy FAM solution(s).
Verify and validate FAM solution(s) integration.
out to 4.4.4

Figure D-22: Implementation Tasks for Activity 4.4.3 — *File Activity Monitoring Part 1*

Activity 4.5.1 Implement Data Rights Management (DRM) and Protection Tools Part 1

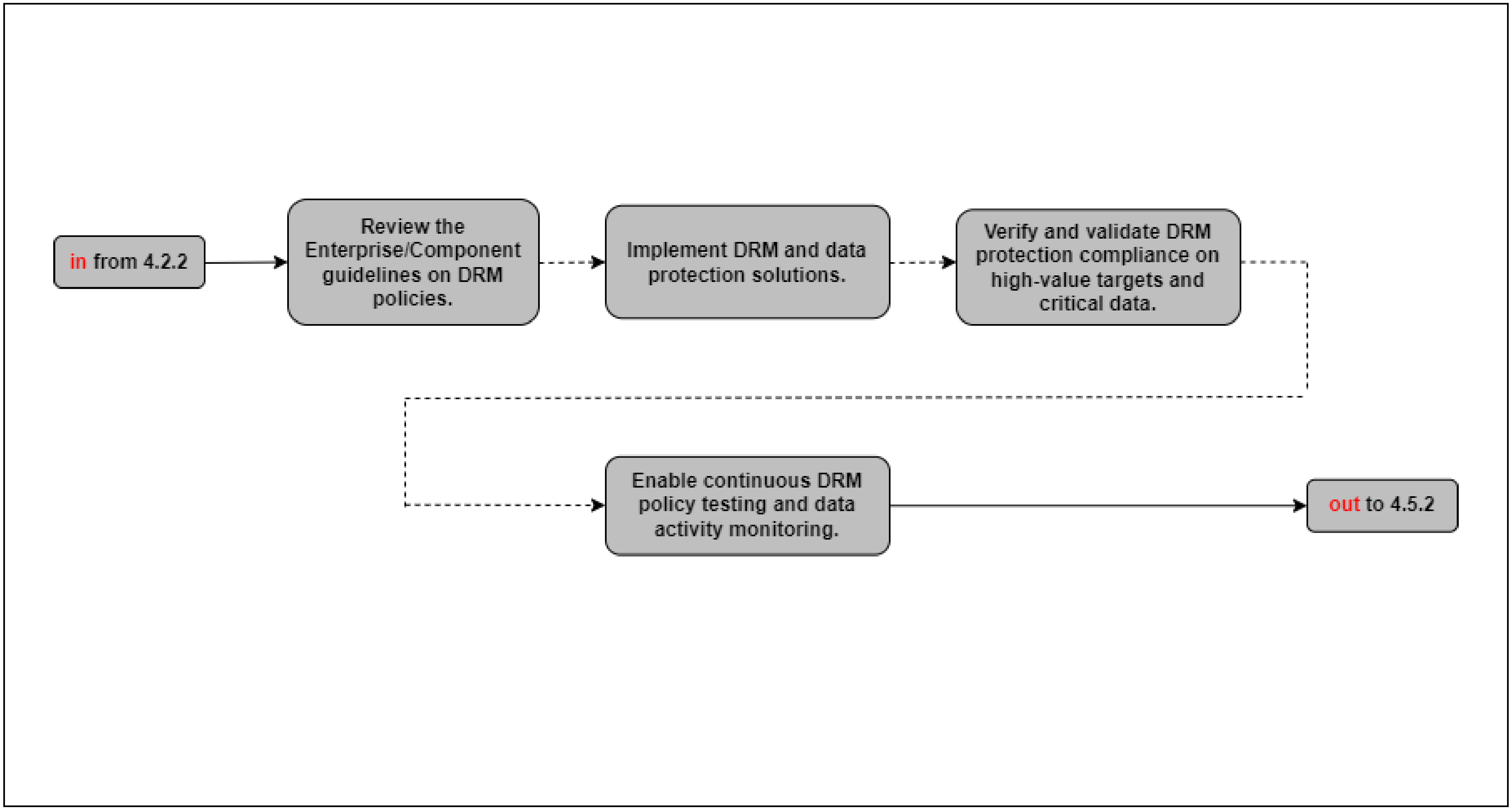

in from 4.2.2
Review the Enterprise/Component guidelines on DRM policies.
Implement DRM and data protection solutions.
Verify and validate DRM protection compliance on high-value targets and critical data.
Enable continuous DRM policy testing and data activity monitoring.
out to 4.5.2

Figure D-23: Implementation Tasks for Activity 4.5.1 — *Implement Data Rights Management (DRM) and Protection Tools Part 1*

Activity 4.6.1 Implement Enforcement Points

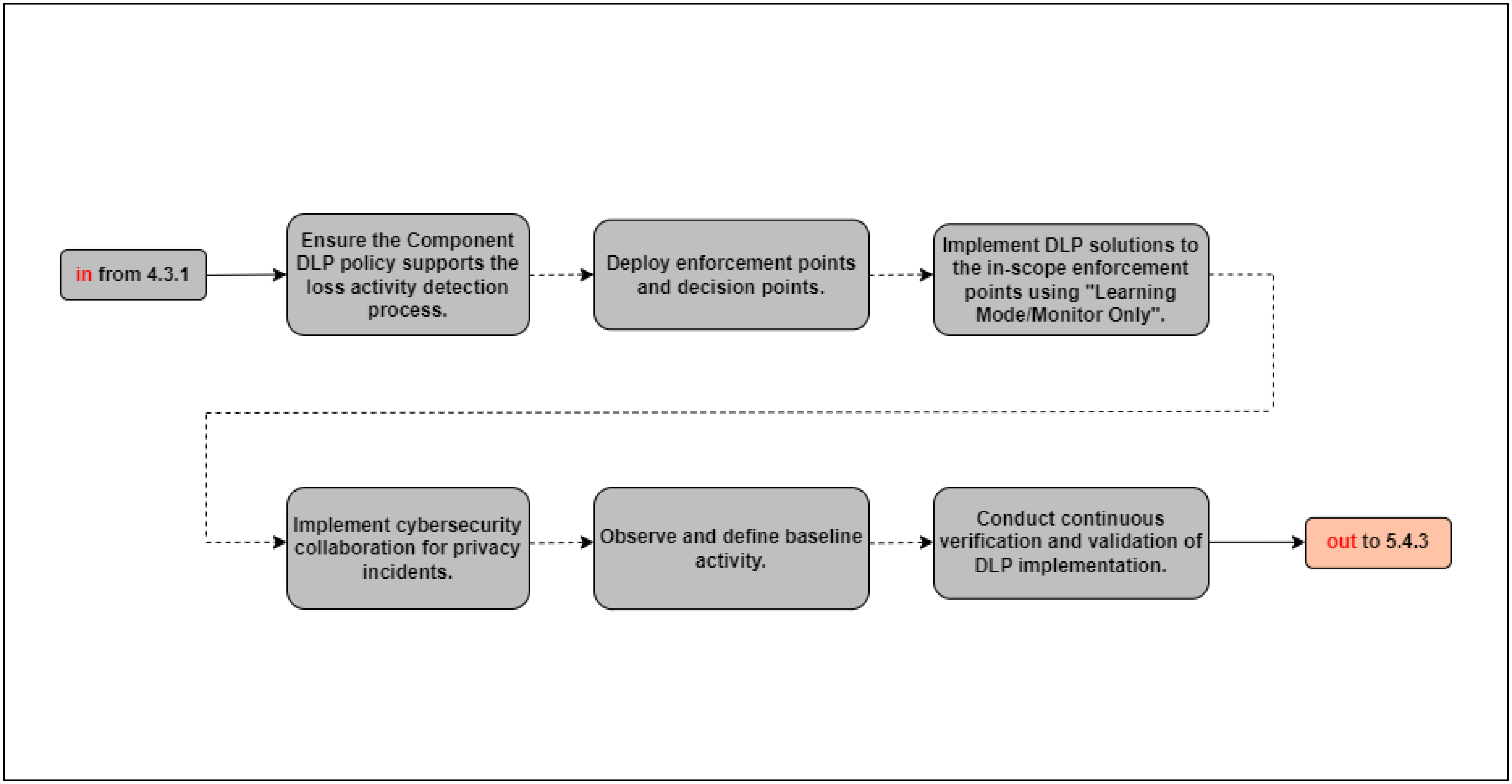

in from 4.3.1
Ensure the Component DLP policy supports the loss activity detection process.
Deploy enforcement points and decision points.
Implement DLP solutions to the in-scope enforcement points using "Learning Mode/Monitor Only".
Implement cybersecurity collaboration for privacy incidents.
Observe and define baseline activity.
Conduct continuous verification and validation of DLP implementation.
out to 5.4.3

Figure D-24: Implementation Tasks for Activity 4.6.1 — *Implement Enforcement Points*

Activity 5.1.2 Define Granular Control Access Rules and Policies Part 2

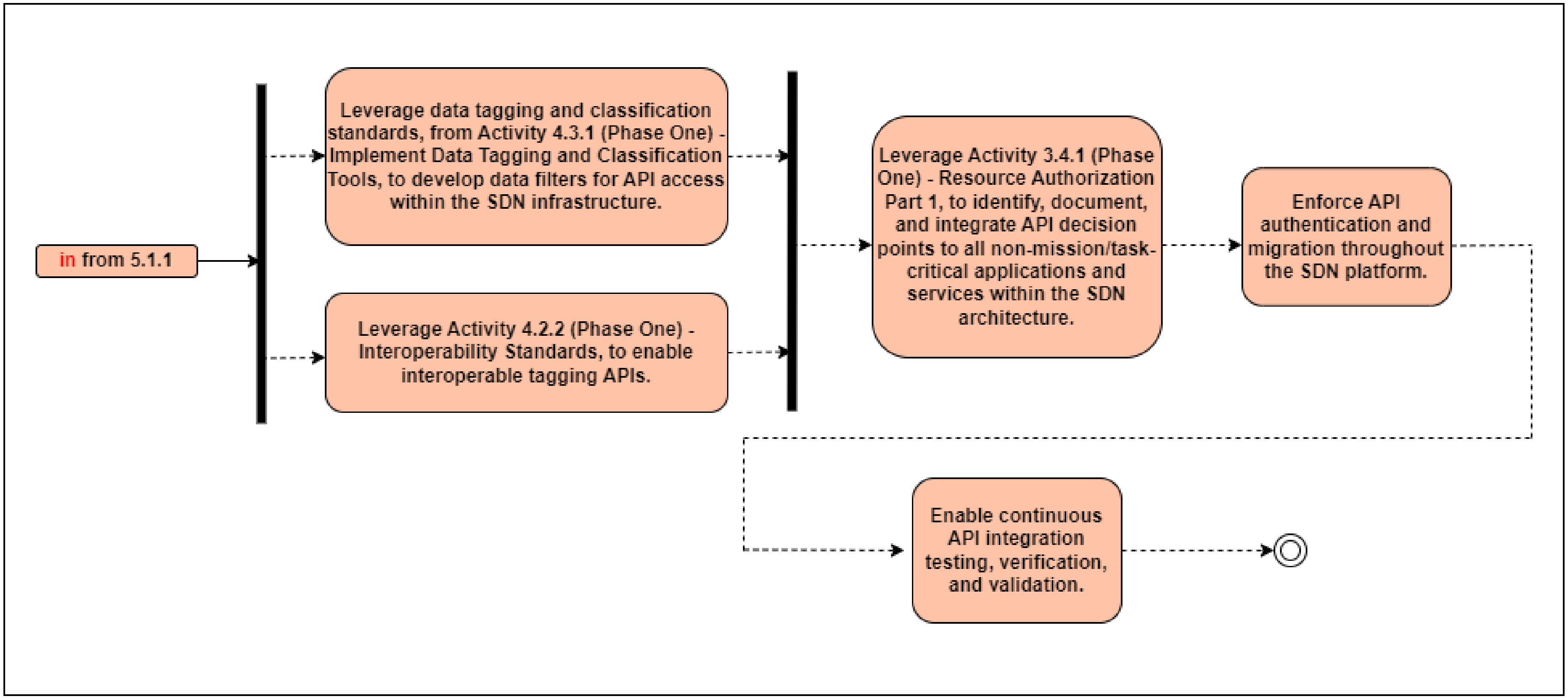

in from 5.1.1
Leverage data tagging and classification standards, from Activity 4.3.1 (Phase One) - Implement Data Tagging and Classification Tools, to develop data filters for API access within the SDN infrastructure.
Leverage Activity 4.2.2 (Phase One) - Interoperability Standards, to enable interoperable tagging APIs.
Leverage Activity 3.4.1 (Phase One) - Resource Authorization Part 1, to identify, document, and integrate API decision points to all non-mission/task-critical applications and services within the SDN architecture.
Enforce API authentication and migration throughout the SDN platform.
Enable continuous API integration testing, verification, and validation.

Figure D-25: Implementation Tasks for Activity 5.1.2 — *Define Granular Control Access Rules and Policies Part 2*

Activity 5.2.2 Implement Software-Defined Networking (SDN) Programmable Infrastructure

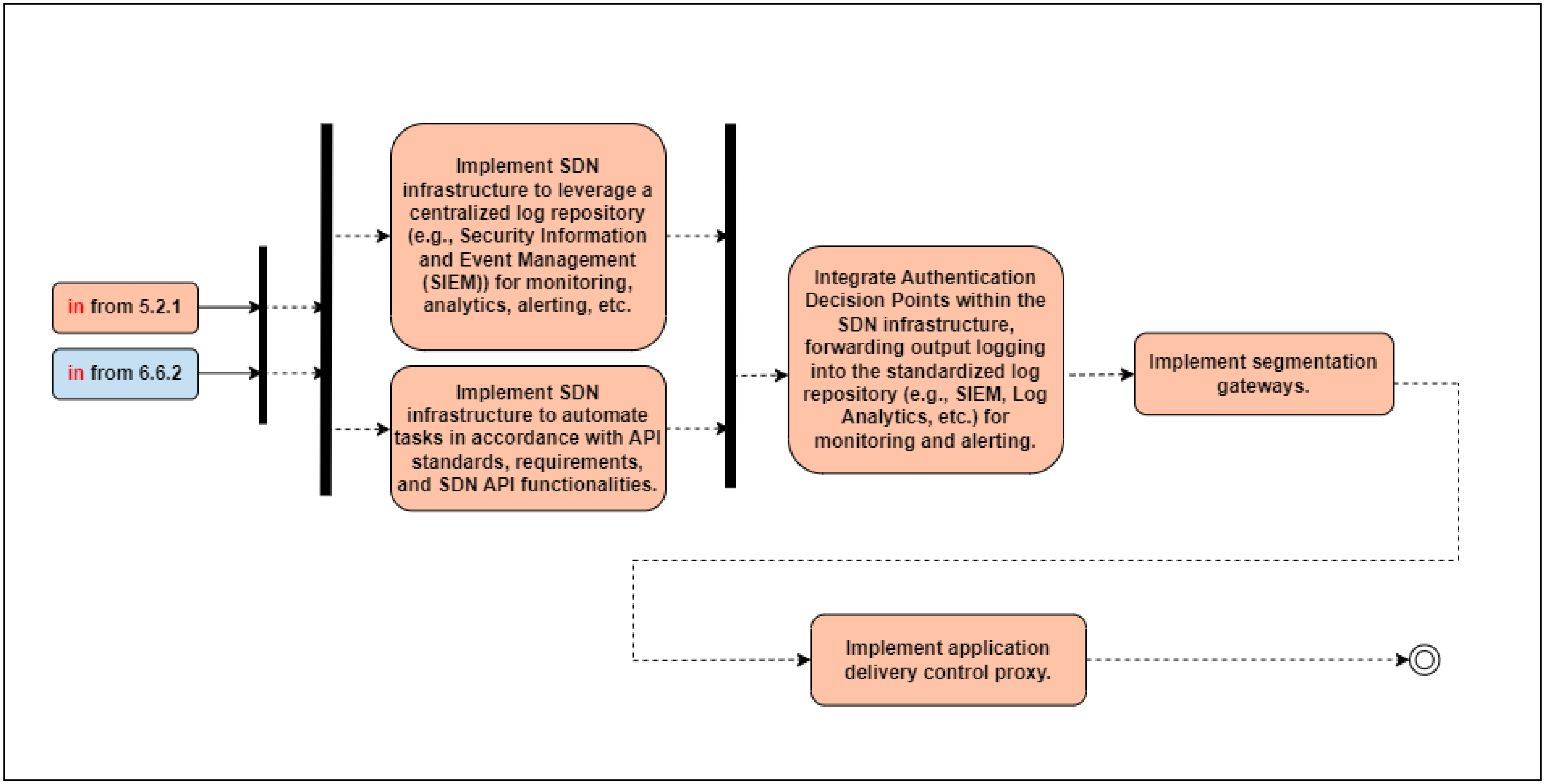

in from 5.2.1
in from 6.6.2
Implement SDN infrastructure to leverage a centralized log repository (e.g., Security Information and Event Management (SIEM)) for monitoring, analytics, alerting, etc.
Implement SDN infrastructure to automate tasks in accordance with API standards, requirements, and SDN API functionalities.
Integrate Authentication Decision Points within the SDN infrastructure, forwarding output logging into the standardized log repository (e.g., SIEM, Log Analytics, etc.) for monitoring and alerting.
Implement segmentation gateways.
Implement application delivery control proxy.

Figure D-26: Implementation Tasks for Activity 5.2.2 — *Implement Software-Defined Networking (SDN) Programmable Infrastructure*

Activity 5.3.1 Datacenter Macro-Segmentation

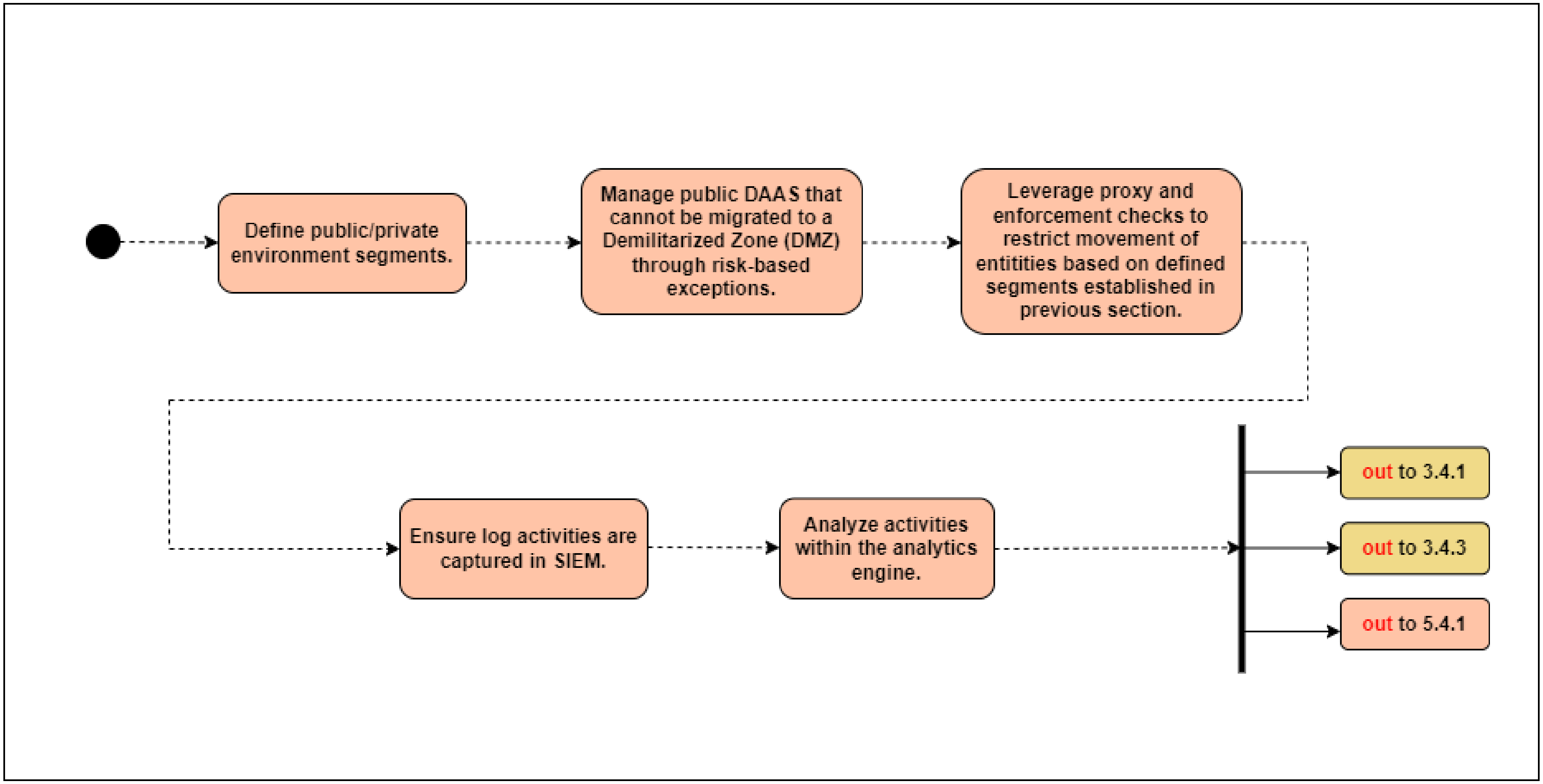

Define public/private environment segments.
Manage public DAAS that cannot be migrated to a Demilitarized Zone (DMZ) through risk-based exceptions.
Leverage proxy and enforcement checks to restrict movement of entitities based on defined segments established in previous section.
Ensure log activities are captured in SIEM.
Analyze activities within the analytics engine.
out to 3.4.1
out to 3.4.3
out to 5.4.1

Figure D-27: Implementation Tasks for Activity 5.3.1 — *Datacenter Macro-Segmentation*

Activity 5.4.1 Implement Micro-Segmentation

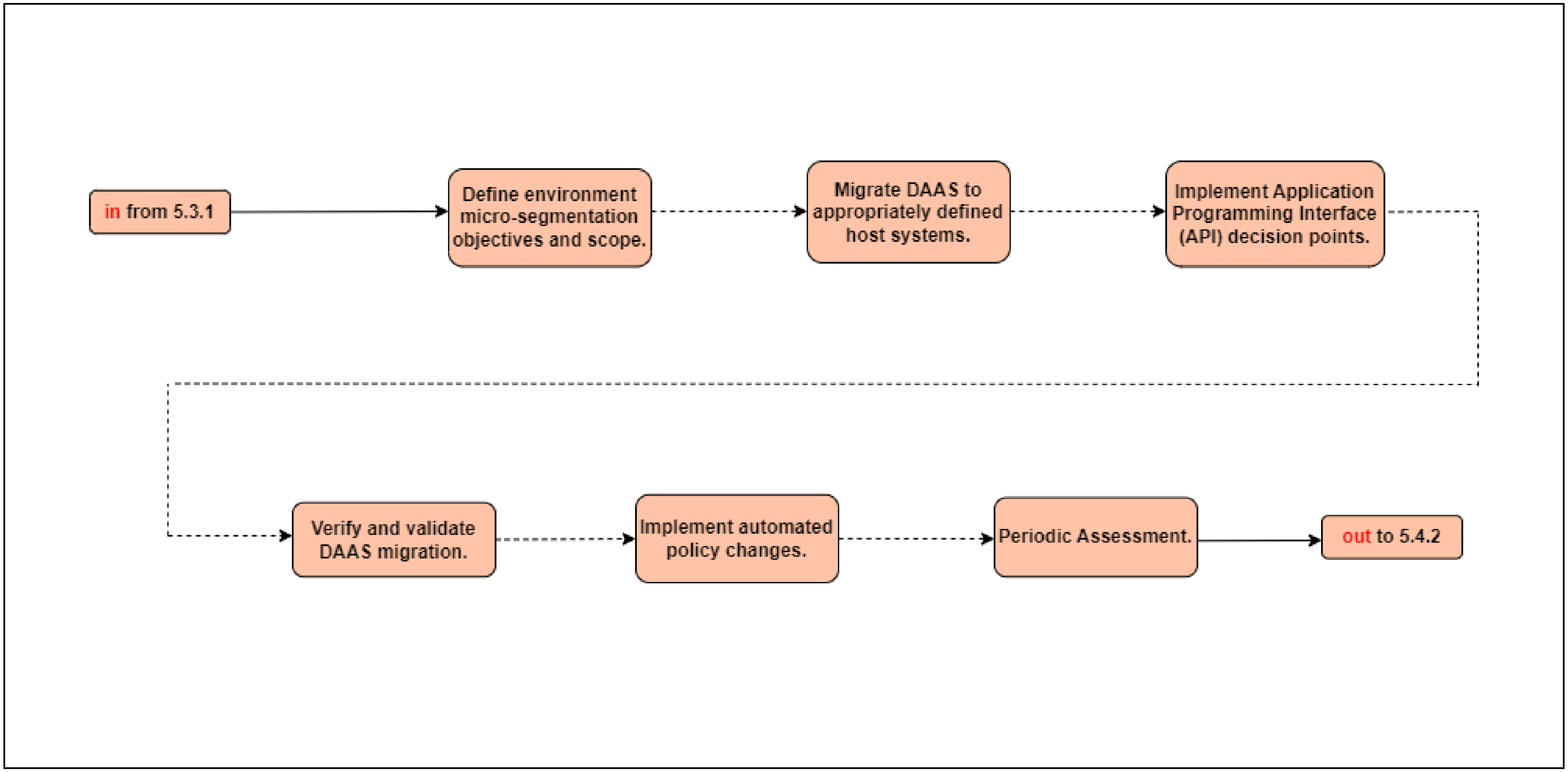

in from 5.3.1
Define environment micro-segmentation objectives and scope.
Migrate DAAS to appropriately defined host systems.
Implement Application Programming Interface (API) decision points.
Verify and validate DAAS migration.
Implement automated policy changes.
Periodic Assessment.
out to 5.4.2

Figure D-28: Implementation Tasks for Activity 5.4.1 — *Implement Micro-Segmentation*

Activity 6.1.2 Organization Access Profile

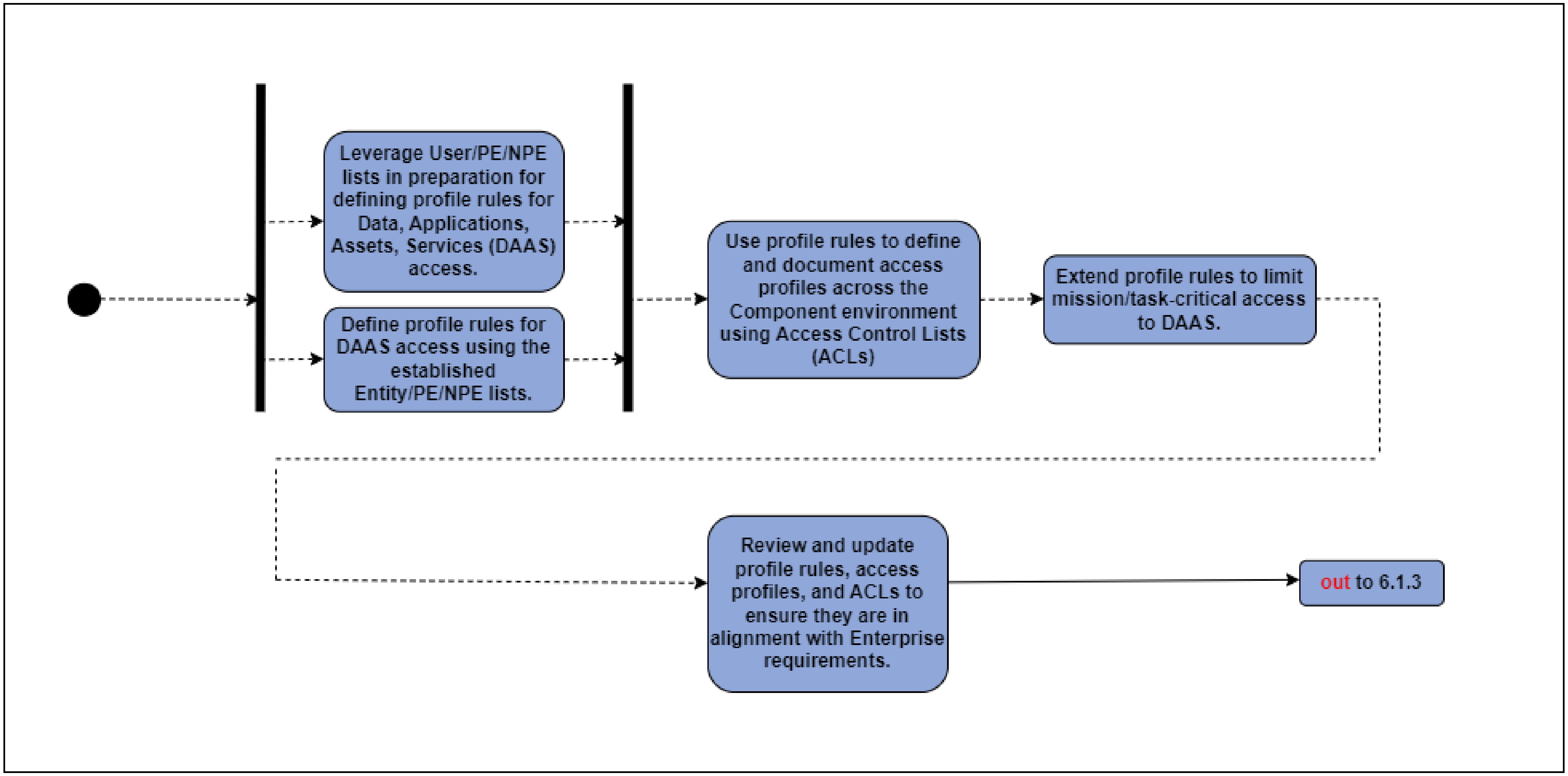

Leverage User/PE/NPE lists in preparation for defining profile rules for Data, Applications, Assets, Services (DAAS) access.
Define profile rules for DAAS access using the established Entity/PE/NPE lists.
Use profile rules to define and document access profiles across the Component environment using Access Control Lists (ACLs)
Extend profile rules to limit mission/task-critical access to DAAS.
Review and update profile rules, access profiles, and ACLs to ensure they are in alignment with Enterprise requirements.
out to 6.1.3

Figure D-29: Implementation Tasks for Activity 6.1.2 — *Organization Access Profile*

Activity 6.5.2 Implement Security Orchestration, Automation, and Response (SOAR) Tools

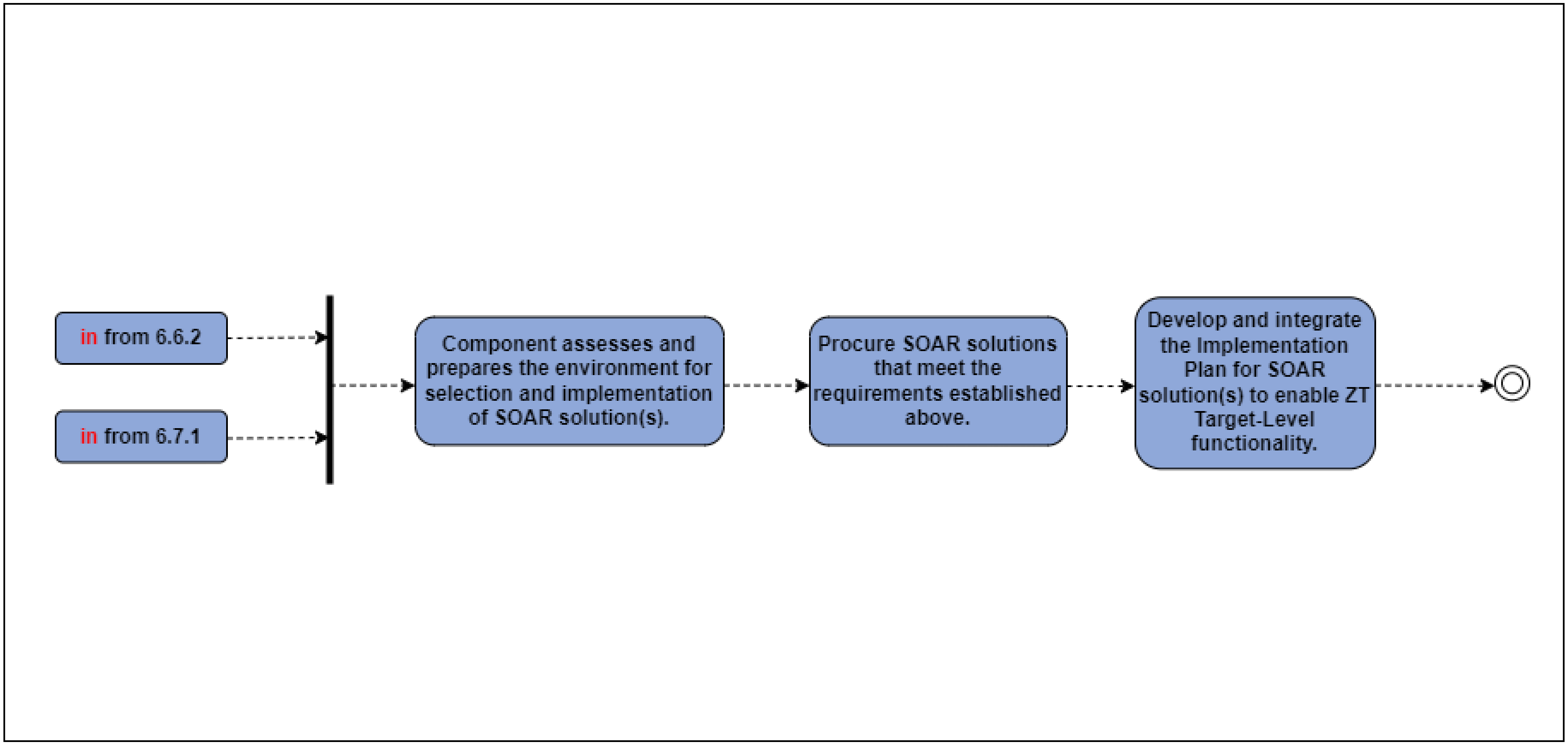

in from 6.6.2
in from 6.7.1
Component assesses and prepares the environment for selection and implementation of SOAR solution(s).
Procure SOAR solutions that meet the requirements established above.
Develop and integrate the Implementation Plan for SOAR solution(s) to enable ZT Target-Level functionality.

Figure D-30: Implementation Tasks for Activity 6.5.2 — *Implement Security Orchestration, Automation, and Response (SOAR) Tools*

Activity 6.6.2 Standardized Application Programming Interface (API) Calls and Schemas Part 1

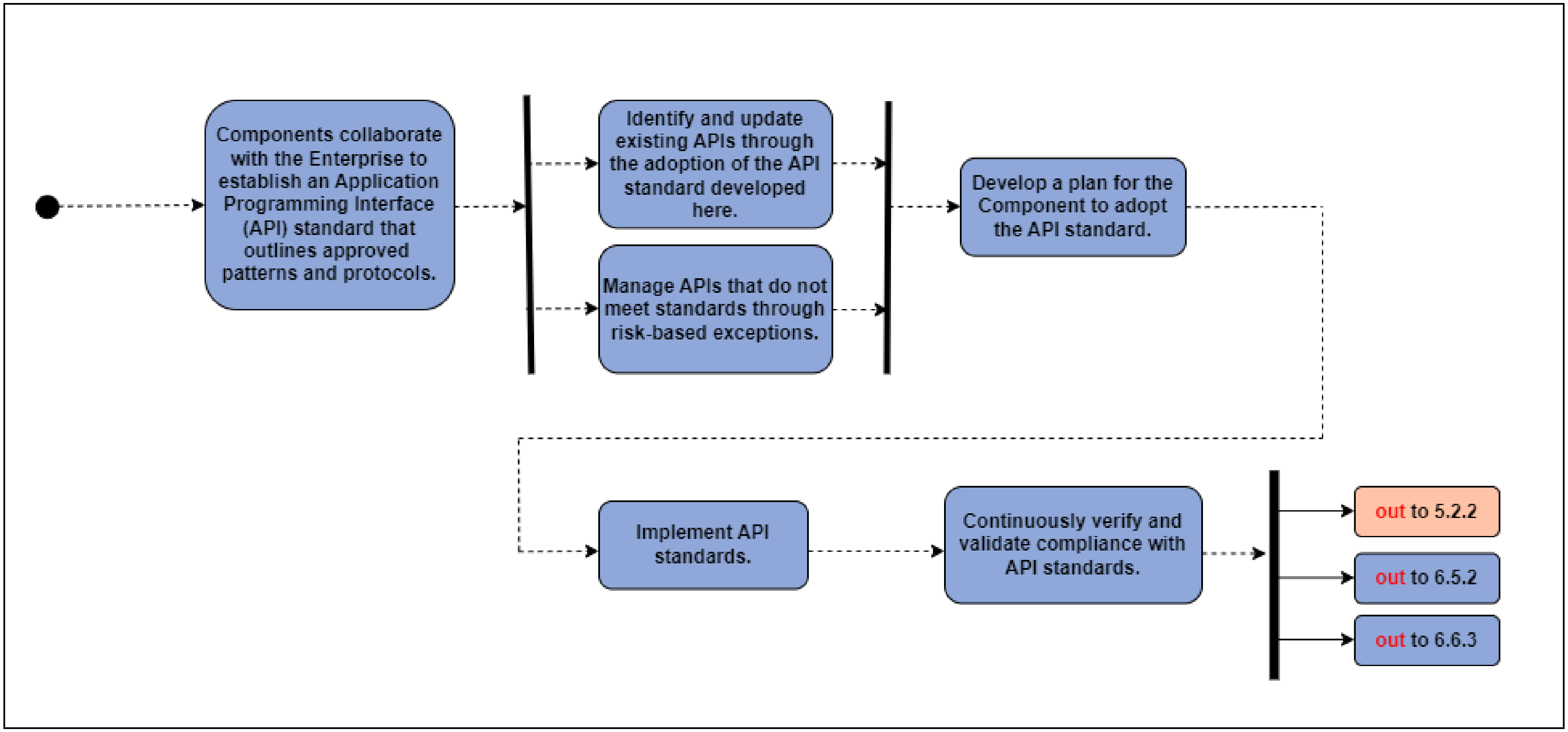

Components collaborate with the Enterprise to establish an Application Programming Interface (API) standard that outlines approved patterns and protocols.
Identify and update existing APIs through the adoption of the API standard developed here.
Manage APIs that do not meet standards through risk-based exceptions.
Develop a plan for the Component to adopt the API standard.
Implement API standards.
Continuously verify and validate compliance with API standards.
out to 5.2.2
out to 6.5.2
out to 6.6.3

Figure D-31: Implementation Tasks for Activity 6.6.2 — *Standardized Application Programming Interface (API) Calls and Schemas Part 1*

Activity 6.7.1 Workflow Enrichment Part 1

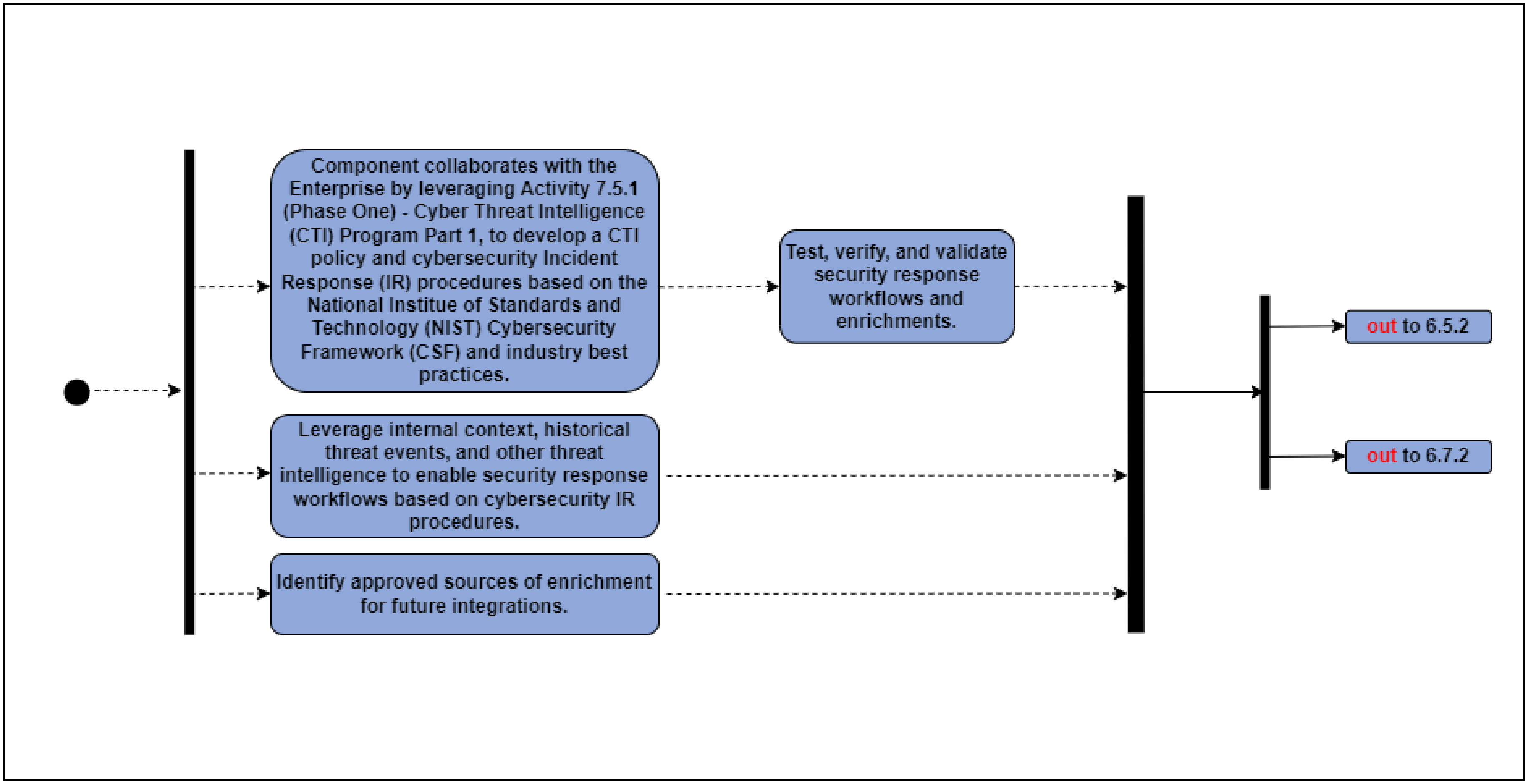

Component collaborates with the Enterprise by leveraging Activity 7.5.1 (Phase One) - Cyber Threat Intelligence (CTI) Program Part 1, to develop a CTI policy and cybersecurity Incident Response (IR) procedures based on the National Institue of Standards and Technology (NIST) Cybersecurity Framework (CSF) and industry best practices.
Test, verify, and validate security response workflows and enrichments.
Leverage internal context, historical threat events, and other threat intelligence to enable security response workflows based on cybersecurity IR procedures.
Identify approved sources of enrichment for future integrations.
out to 6.5.2
out to 6.7.2

Figure D-32: Implementation Tasks for Activity 6.7.1 — *Workflow Enrichment Part 1*

Activity 7.1.2 Log Parsing

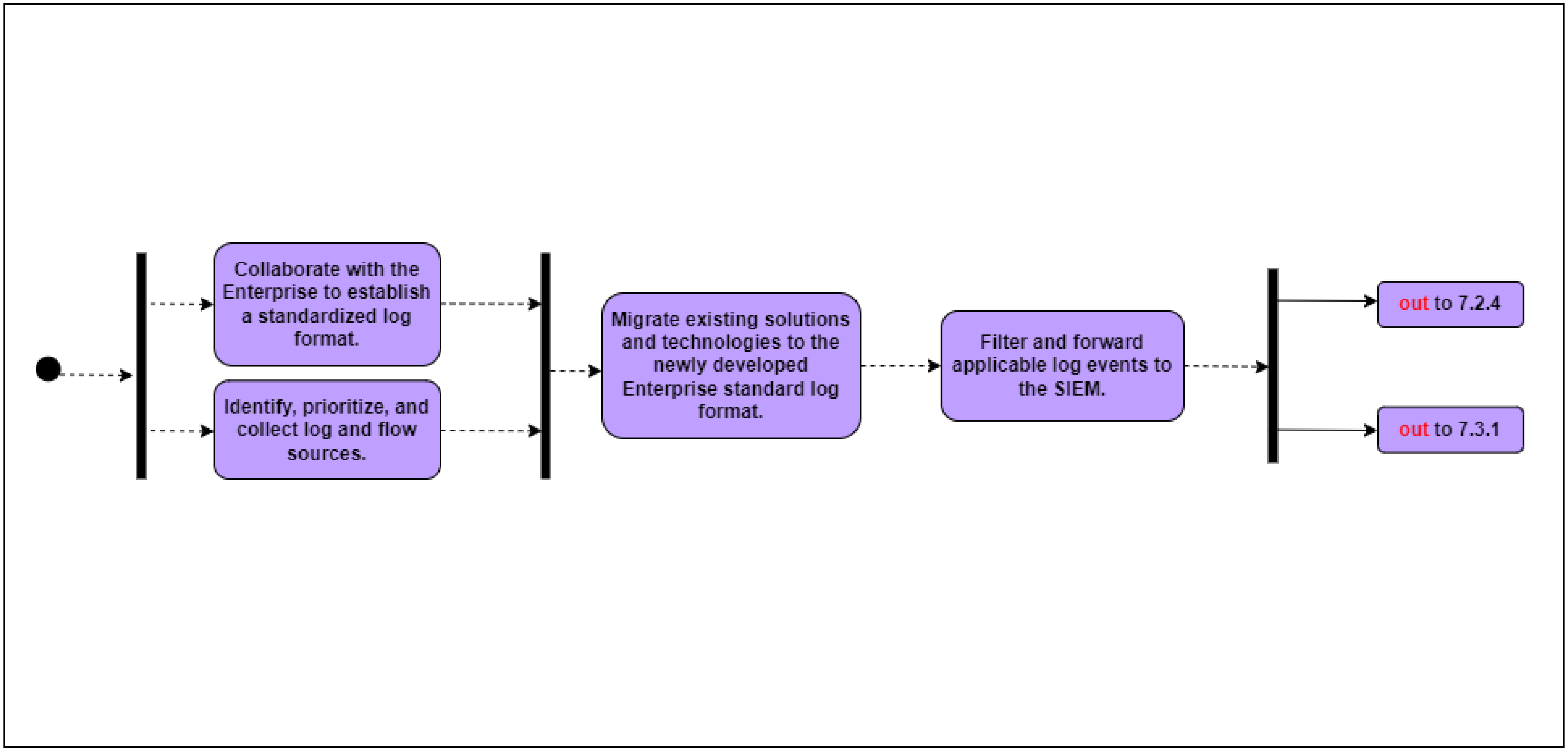

Collaborate with the Enterprise to establish a standardized log format.
Identify, prioritize, and collect log and flow sources.
Migrate existing solutions and technologies to the newly developed Enterprise standard log format.
Filter and forward applicable log events to the SIEM.
out to 7.2.4
out to 7.3.1

Figure D-33: Implementation Tasks for Activity 7.1.2 — *Log Parsing*

Activity 7.2.1 Threat Alerting Part 1

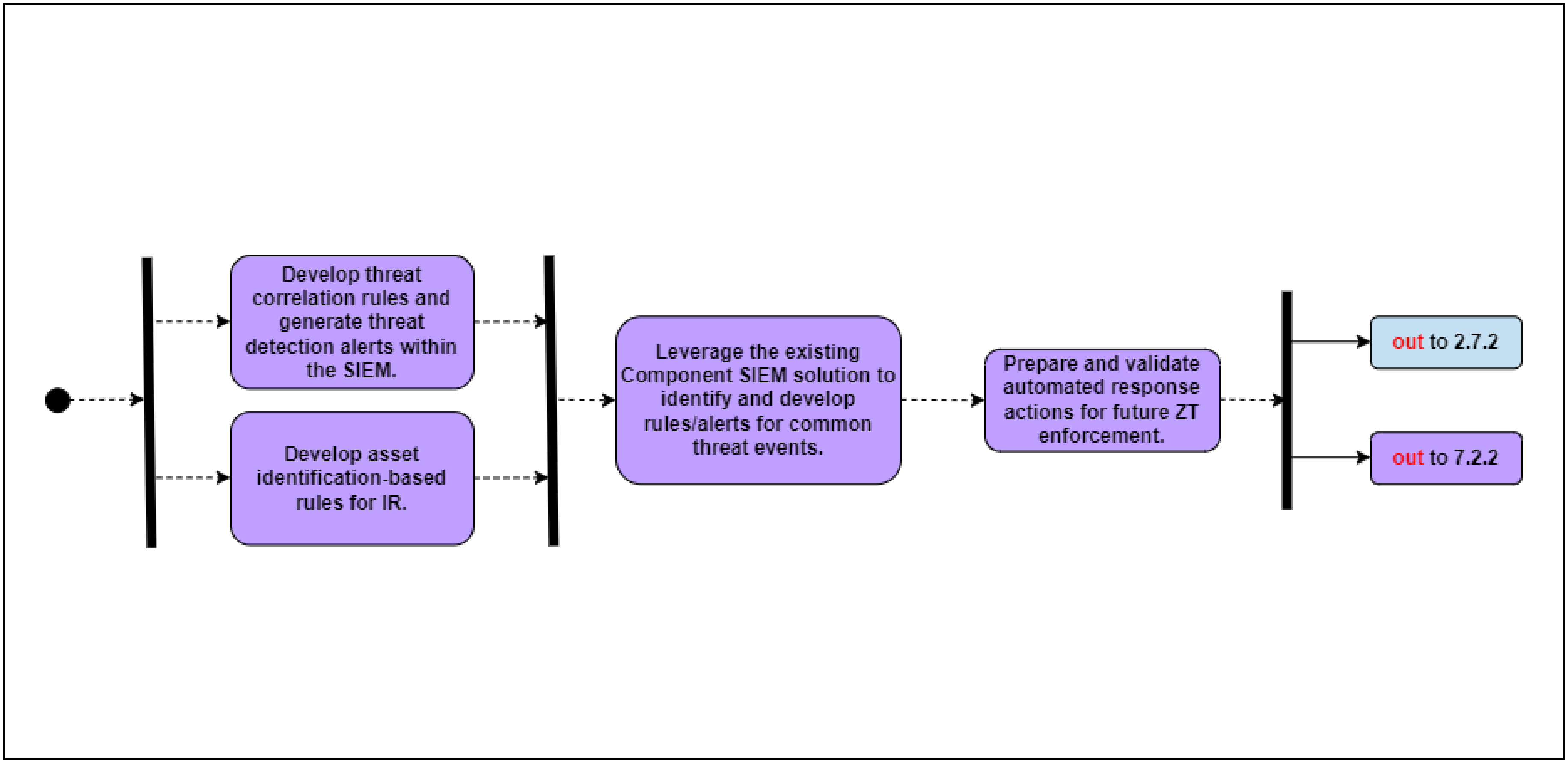

Develop threat correlation rules and generate threat detection alerts within the SIEM.
Develop asset identification-based rules for IR.
Leverage the existing Component SIEM solution to identify and develop rules/alerts for common threat events.
Prepare and validate automated response actions for future ZT enforcement.
out to 2.7.2
out to 7.2.2

Figure D-34: Implementation Tasks for Activity 7.2.1 — *Threat Alerting Part 1*

Activity 7.2.4 Asset ID and Alert Correlation

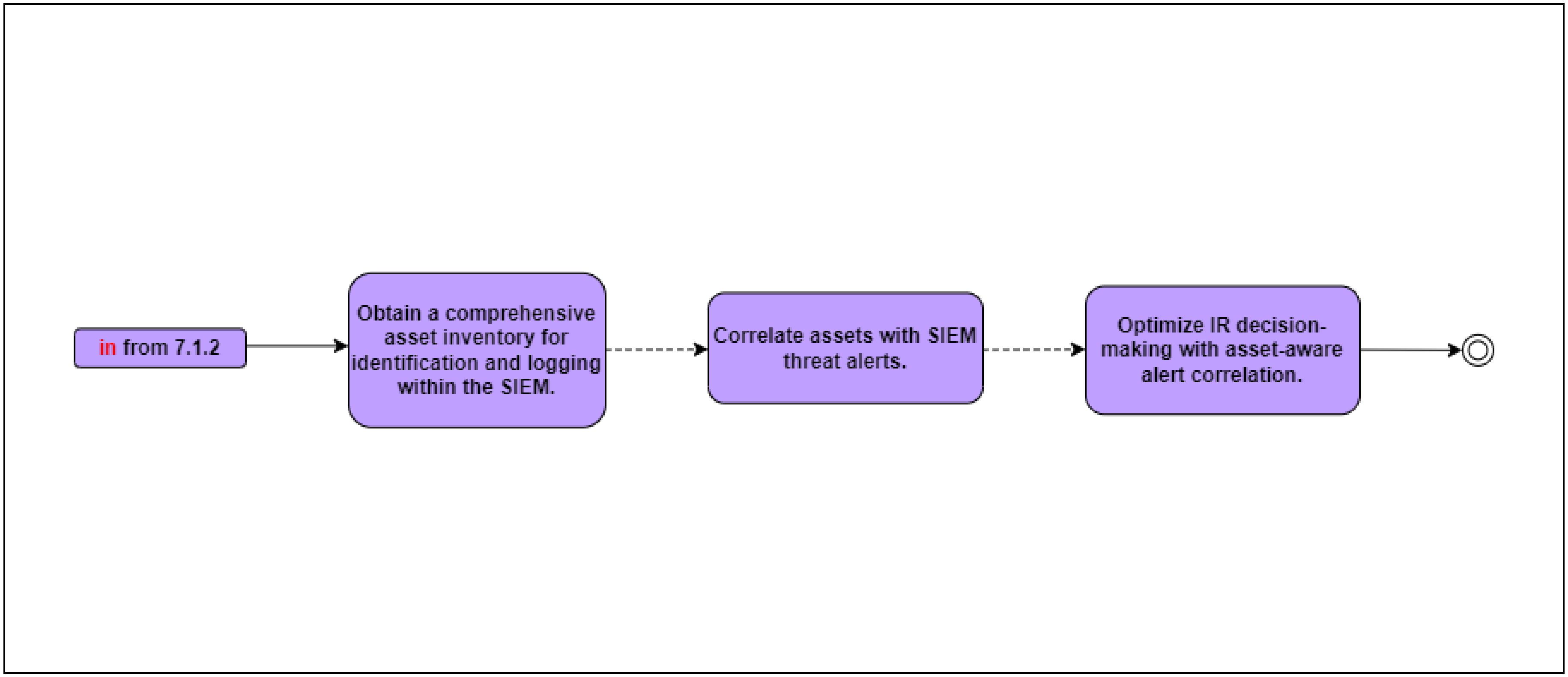

in from 7.1.2
Obtain a comprehensive asset inventory for identification and logging within the SIEM.
Correlate assets with SIEM threat alerts.
Optimize IR decision-making with asset-aware alert correlation.

Figure D-35: Implementation Tasks for Activity 7.2.4 — *Asset ID and Alert Correlation*

Activity 7.3.1 Implement Analytics Tools

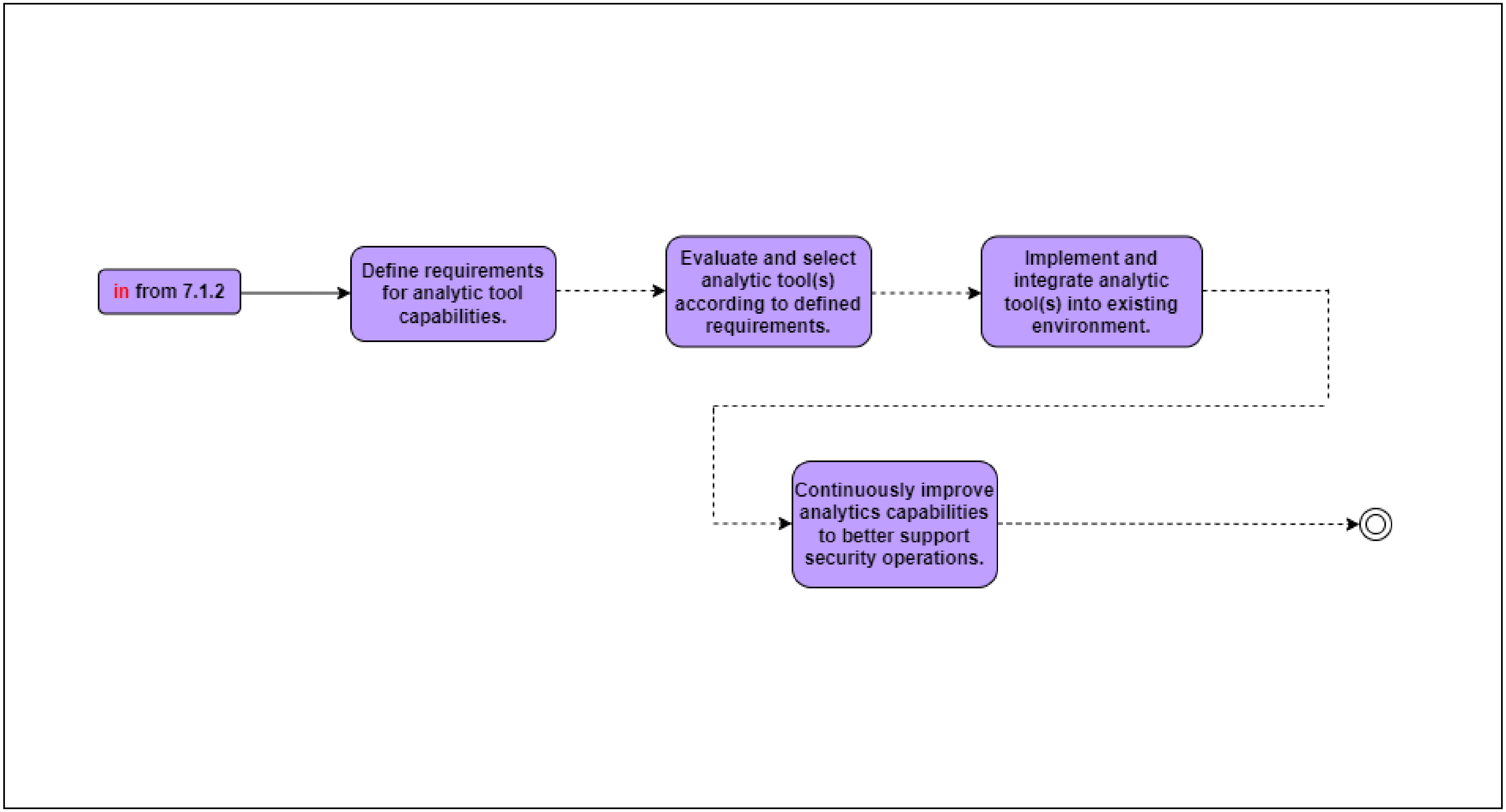

in from 7.1.2
Define requirements for analytic tool capabilities.
Evaluate and select analytic tool(s) according to defined requirements.
Implement and integrate analytic tool(s) into existing environment.
Continuously improve analytics capabilities to better support security operations.

Figure D-36: Implementation Tasks for Activity 7.3.1 — *Implement Analytics Tools*

Activity 7.5.1 Cyber Threat Intelligence Program Part 1

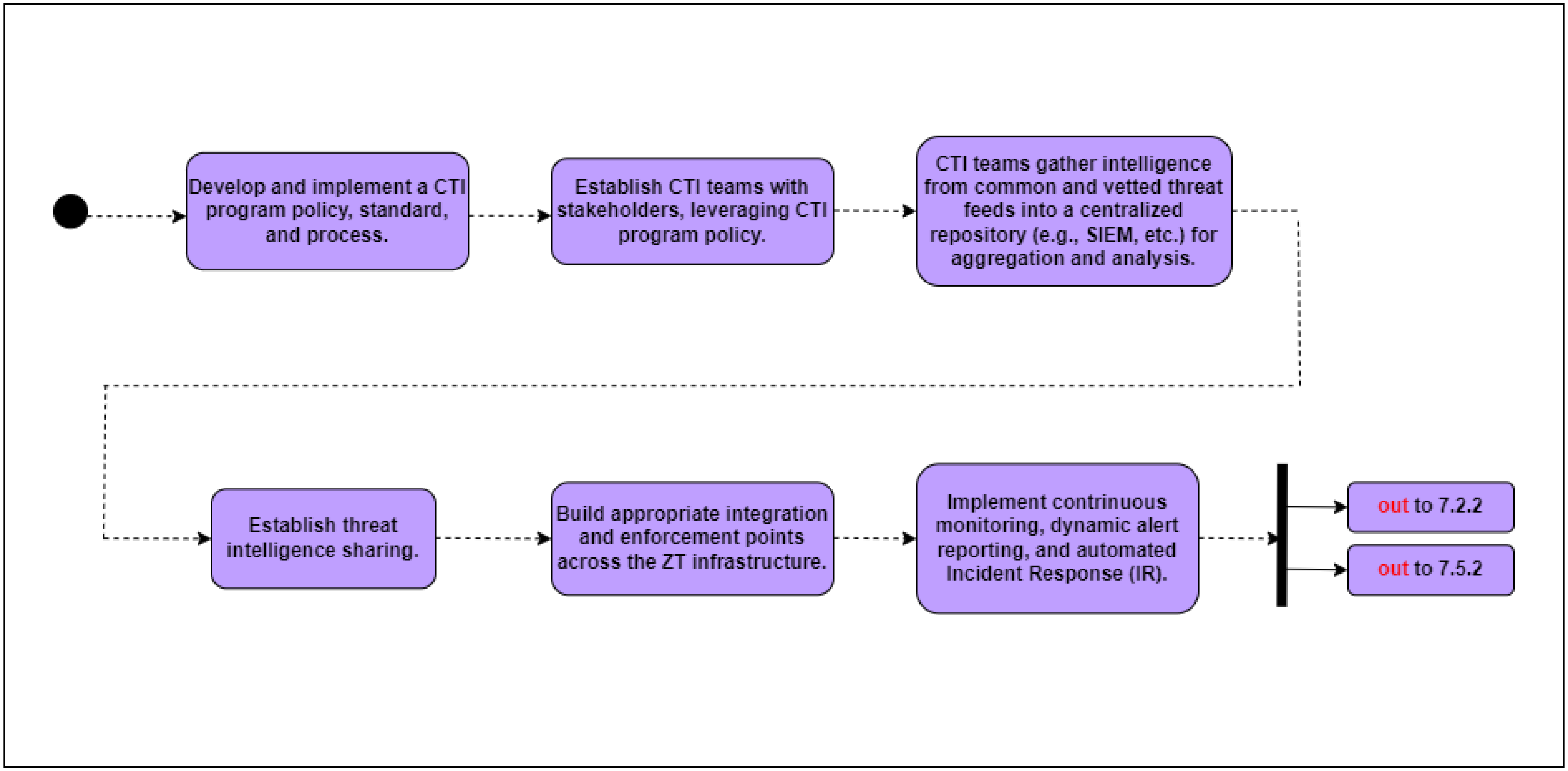

Develop and implement a CTI program policy, standard, and process.
Establish CTI teams with stakeholders, leveraging CTI program policy.
CTI teams gather intelligence from common and vetted threat feeds into a centralized repository (e.g., SIEM, etc.) for aggregation and analysis.
Establish threat intelligence sharing.
Build appropriate integration and enforcement points across the ZT infrastructure.
Implement contrinuous monitoring, dynamic alert reporting, and automated Incident Response (IR).
out to 7.2.2
out to 7.5.2

Figure D-37: Implementation Tasks for Activity 7.5.1 — *Cyber Threat Intelligence Program Part 1*