ISMG Studio

at Black Hat USA 2025

Black Hat USA 2025: Security in the Age of AI

You simply can't have a cybersecurity conversation these days without mentioning artificial intelligence. Attendees at Black Hat USA 2025 in Las Vegas recognized the vast potential of AI technology - from emerging threats from deepfakes and spear-phishing to "fighting AI with AI" through advanced systems for managing security operations, identities and more.

We at ISMG.Studio have preserved some of the best insights so we can share them here with you in this exclusive compendium. Once again, ISMG captured the key themes at Black Hat and expert perspectives on issues shaping the cybersecurity landscape. Video interviews with CEOs, CISOs, government leaders, investors, researchers and attorneys are all featured here. In addition to AI, you'll find insights on secure enterprise browsers, application security, nation-state threats, the latest ransomware threats and threats to critical infrastructure.

Within these pages, you'll find insightful interviews by our seasoned editorial team - an in-depth view of the latest information and thought leadership from this landmark event. Get a glimpse of the future of cybersecurity - today.

Enjoy

Tom Field
Senior Vice President, Editorial
ISMG

Visit us online for more ISMG at Black Hat USA 2025 coverage:

ISMG.Studio

Video Interviews

“It's all about resilience. How do you understand the threat, prepare for it, be able to respond to it and then recover so that you can mitigate and drive down risk?”

Jen Easterly

Former Director, CISA, and Strategic Advisory Board Member, Huntress

Nick Biasini
Head, Outreach, Cisco Talos

Identity-Based Attacks - When MFA Isn't Enough

Cisco Talos' **Nick Biasini** on MFA Bypass Tactics and Role of AI in Identity Security

Identity has become the primary battleground in cybersecurity, with attackers increasingly specializing in credential theft and MFA bypass techniques. Nick Biasini, head of outreach at Cisco Talos, warns: "the attention on identity is not going anywhere; if anything, it's just going to get worse."

> "Identity is the name of the game right now."
>
> - Nick Biasini

In this video interview with Information Security Media Group at Black Hat USA 2025, Biasini also discussed:

- Why passwordless authentication could introduce new risks;
- Insights from Cisco Talos' latest Incident Response Threat Analytics report findings;
- The role of agentic AI in offensive cyber operations.

WATCH ONLINE

Closing Security Gaps in 5G Basebands and Open RAN

Penn State University Researchers on the Need for Smarter Security Testing

Proprietary hardware, intricate protocols and modular architectures in 5G basebands and open RAN create new opportunities for attackers, making specialized, architecture-aware testing essential, said **Tianchang Yang** and **Ali Ranjbar** of Pennsylvania State University.

WATCH ONLINE

How the CyberArk Deal Boosts Palo Alto Networks' Platform

Forrester's **Allie Mellen** on How M&A Strategies Broaden Vendor Portfolios

Palo Alto's $25 billion purchase of CyberArk fills a crucial identity gap in its platform strategy. Allie Mellen, principal analyst at Forrester, says the move reflects surging demand for integrated cybersecurity platforms and positions the company to better compete in a multi-cloud security market.

WATCH ONLINE

Study Finds Politicians Are More Likely to Share Your Data

Virginia Tech's **Alan Michaels** on Risks of Political Campaign Data-Sharing Practices

Some political campaigns shared supporter emails without consent, often within the same party. This fueled donation-driven messaging over policy discussion and raised concerns about voter privacy and data protection, said Alan Michaels, professor and director at Virginia Tech.

WATCH ONLINE

The Looming Threat of AI Agent-Powered Attackers

MITRE Researchers **Dotter** and **Russo** on How AI Is Reshaping Threats, Cyber Defenses

AI-powered agents are no longer theoretical - they're actively being deployed, say MITRE researchers Gianpaolo Russo and Marissa Dotter. They discuss how these autonomous systems are transforming both offensive operations and defensive strategies.

WATCH ONLINE

Human-Validated AI: Cutting Noise, Building Trust

Critical Start's **Chris Carlson** on AI's Role in Alert Response

AI is reshaping security operations, but trust, governance and human oversight remain essential. "The human in the driver's seat is the most important discussion around AI today," says Chris Carlson, chief product officer at Critical Start.

In this video interview with Information Security Media Group at Black Hat USA 2025, Carlson also discussed:

- How Critical Start's Trusted Behavior Registry addresses alert fatigue challenge;
- How the OCSF standard improves data normalization for better AI outcomes;
- Critical Start's long-term vision for MDR service and its platform capabilities.

WATCH ONLINE

> "The human-validated approach is that area of responsibility and trustworthiness that we apply to the use of AI within our platform."
>
> - Chris Carlson

“A lot of the companies in the market today want to bundle and sell together as many products as they can. But making sure that it's good for the analyst experience and the identity security users is paramount.”

Allie Mellen

Principal Analyst, Forrester

Shadow AI Creates Data Security Blind Spots at Scale

Cyera's **Kayla Williams** Discusses Data Loss Prevention and Model Integrity Risks

Shadow AI systems operating without authorization create critical security vulnerabilities that traditional controls cannot detect, exposing sensitive data and creating new attack vectors organizations struggle to identify, said Kayla Williams, field CISO at Cyera.

In this video interview with Information Security Media Group at Black Hat USA 2025, Williams also discussed:

- How data classification and governance serve as foundational AI security controls;
- Customer experiences discovering unauthorized AI systems through beta testing programs;
- The upcoming DataSec AI event in Dallas featuring industry professionals and real-world case studies.

WATCH ONLINE

> "The thing that companies don't realize is they already have AI in house. Whether they're aware of it or not, AI has crept in and it's shadow AI."
>
> - Kayla Williams

The CISO Role Is Evolving in AI and Zero Trust Era

Zscaler Global CISO **Sam Curry** on the Changing Demands of Cybersecurity Leadership

The responsibilities of a modern CISO extend far beyond preventing breaches. For Sam Curry, Zscaler's global CISO, the role now requires both strategic security leadership and technical vision.

WATCH ONLINE CyberEdBoard

Offensive AI Drives More Convincing Cyberattacks

Ethical Hacker **Mishaal Khan** on Deepfakes, Voice Cloning and OSINT

Artificial intelligence is boosting social engineering attacks. Voice cloning and deepfake videos and better open-source intelligence are creating more believable scams, said Mishaal Khan, ethical hacker and co-author of the book "The Phantom CISO."

WATCH ONLINE

Shadow AI and Compliance Gaps Put Enterprises at Risk

BLodgic's **Brennan Lodge** Calls for Proactive GRC Frameworks to Secure AI Systems

Organizations embracing AI without proper governance, risk and compliance controls face significant vulnerabilities from hallucinations, prompt injection attacks and shadow AI implementations that lack oversight, said Brennan Lodge, founder of BLodgic.

WATCH ONLINE

Anti-Cheat Tactics Offer Ransomware Defense Lessons

Researchers **Collins** and **Muench** on Zero Trust, Memory Hiding and Delayed Bans

Gaming anti-cheat systems operate in environments where attackers have full control, creating sophisticated defenses that could revolutionize enterprise cybersecurity and ransomware protection, said University of Birmingham's Ph.D. Researcher Sam Collins and Assistant Professor Marius Muench.

WATCH ONLINE

Generative AI Drives Surge in Unstructured Data Risks

Thales' **Todd Moore** on Blind Spots Created by AI-Driven Unstructured Data Growth

Generative AI is fueling a rapid rise in unstructured data, creating critical security blind spots. Todd Moore, global vice president of data security at Thales, shares why visibility and classification are essential to protect sensitive data across multi-cloud, hybrid and on-premises environments.

In this video interview with Information Security Media Group at Black Hat USA 2025, Moore also discussed:

- Why external key management is critical to maintaining data control on cloud platforms;
- The looming threat of quantum computing on current encryption algorithms;
- Why strong AI governance requires policies focused on data and identity protection.

WATCH ONLINE

> "Visibility is power. It is the normalizing factor. There are a lot of companies out there that are working to give that visibility, along with Thales, in all the places your data may be."
>
> - Todd Moore

“What will be transformative is when you start seeing the decision-making of the human being handed off to machine reasoning. Large language models have this incredible dual nature, to not only ingest natural language, but also use that and create more machine-readable types of code or tunnel scripting.”

Gianpaolo Russo

Head, AI and Autonomous Cyber Operations, MITRE

Organizations Must Focus on Adversary Behaviors, Not Vulnerabilities

Tidal Cyber's **Rick Gordon** and **Frank Duff** Call on the Need for Threat-Led Defenses

Traditional security approaches fail because they focus solely on vulnerabilities rather than adversary behaviors after initial access, said Tidal Cyber's CEO Rick Gordon and Chief Innovation Officer Frank Duff. Threat-led defense starts with understanding which adversaries target organizations.

In this video interview with Information Security Media Group at Black Hat USA 2025, Gordon and Duff also discussed:

- The convergence of offensive security and defensive security capabilities;
- How their MITRE backgrounds inform Tidal Cyber's threat-informed defense platform;
- The evolution from point solutions to unified continuous threat exposure management.

WATCH ONLINE

> "Threat-led is the opposite direction. We start with understanding who's attacking us with what, which of those behaviors we can defend against, which of those we cannot."
>
> - Rick Gordon

How Flaws in Dell Firmware Could Help Compromises Persist

Philippe Laulheret of Cisco Talos on Vulnerabilities in ControlVault Firmware

Security flaws in Dell's ControlVault firmware allowed attackers to run code on the chip, extract stored secrets and alter its behavior. By chaining these exploits, they could send malicious data to Windows components, said Philippe Laulheret, senior vulnerability researcher at Cisco Talos.

WATCH ONLINE

Strengthening Cyber Defense for Underserved Sectors

Former CISA Chief **Easterly** on AI-Driven Security and Public-Private Partnerships

Jen Easterly, former director of CISA and now a strategic advisory board member for Huntress, is focusing on boosting cyber resilience for small and medium enterprises. These organizations often face sophisticated attacks but lack the resources to defend themselves.

WATCH ONLINE

Board Responsibilities in a Cybersecurity Crisis

Allison Jetton of Jetton Law on Legal Complexities of State-Sponsored Incidents

Nation-state cyberattacks create unique legal challenges for boards, says Allison Jetton, founder of Jetton Law. From multi-jurisdictional notifications to ransomware payment bans, she explores how boards must navigate legal and regulatory complexities when nation-state actors target organizations.

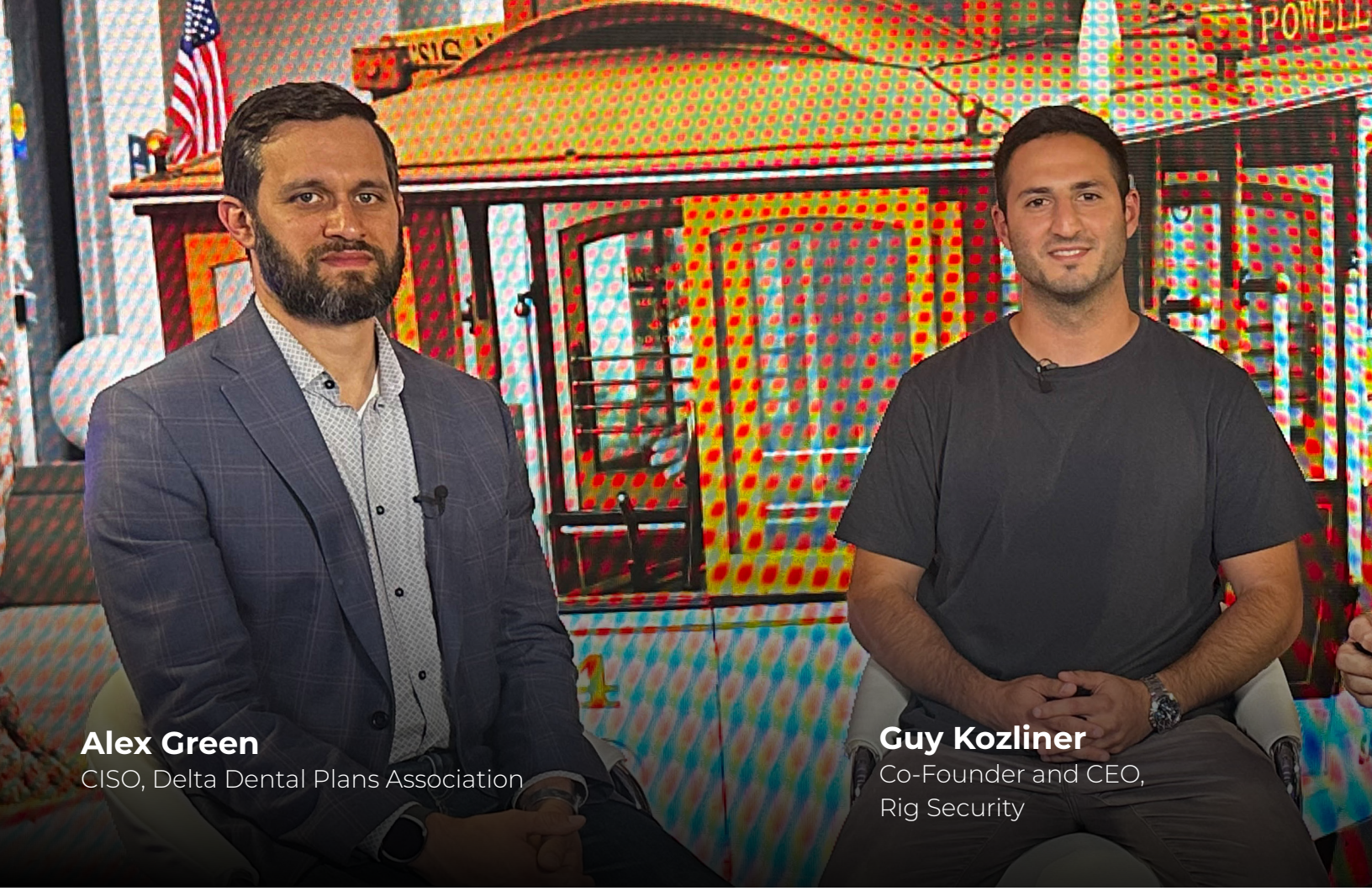
WATCH ONLINE

Security Flaw in TeleMessage Risks Exposure of Text Messages

Dentons' **Doug Henkin** on Encryption Gaps, Embedded Passwords in Message Archives

Financial firms and government agencies adopted TeleMessage to archive off-channel messages for compliance. Doug Henkin, partner at Dentons US, said the messaging platform introduced security flaws that exposed sensitive communications and created risks for both institutions and their clients.

WATCH ONLINE



Surge in Identities Drives Need for Dynamic Security

Rig Security's **Kozliner** and DDPA's **Green** Push forContext-Driven Identity Platforms

The explosive rise of human and non-human identities, accelerated by AI, is straining outdated security models. Security experts say organizations must adopt dynamic, behavior-driven solutions to detect and neutralize identity-based threats before they disrupt business operations.

In this video interview with Information Security Media Group at Black Hat USA 2025, Alex Green, CISO, Delta Dental Plans Association, and Guy Kozliner, co-founder and CEO, Rig Security, also discussed:

- The complexity of mapping relations between human and non-human identities;
- The need for contextual awareness to spot unusual behavior;
- Why security products must deliver fast deployment and minimal user friction.

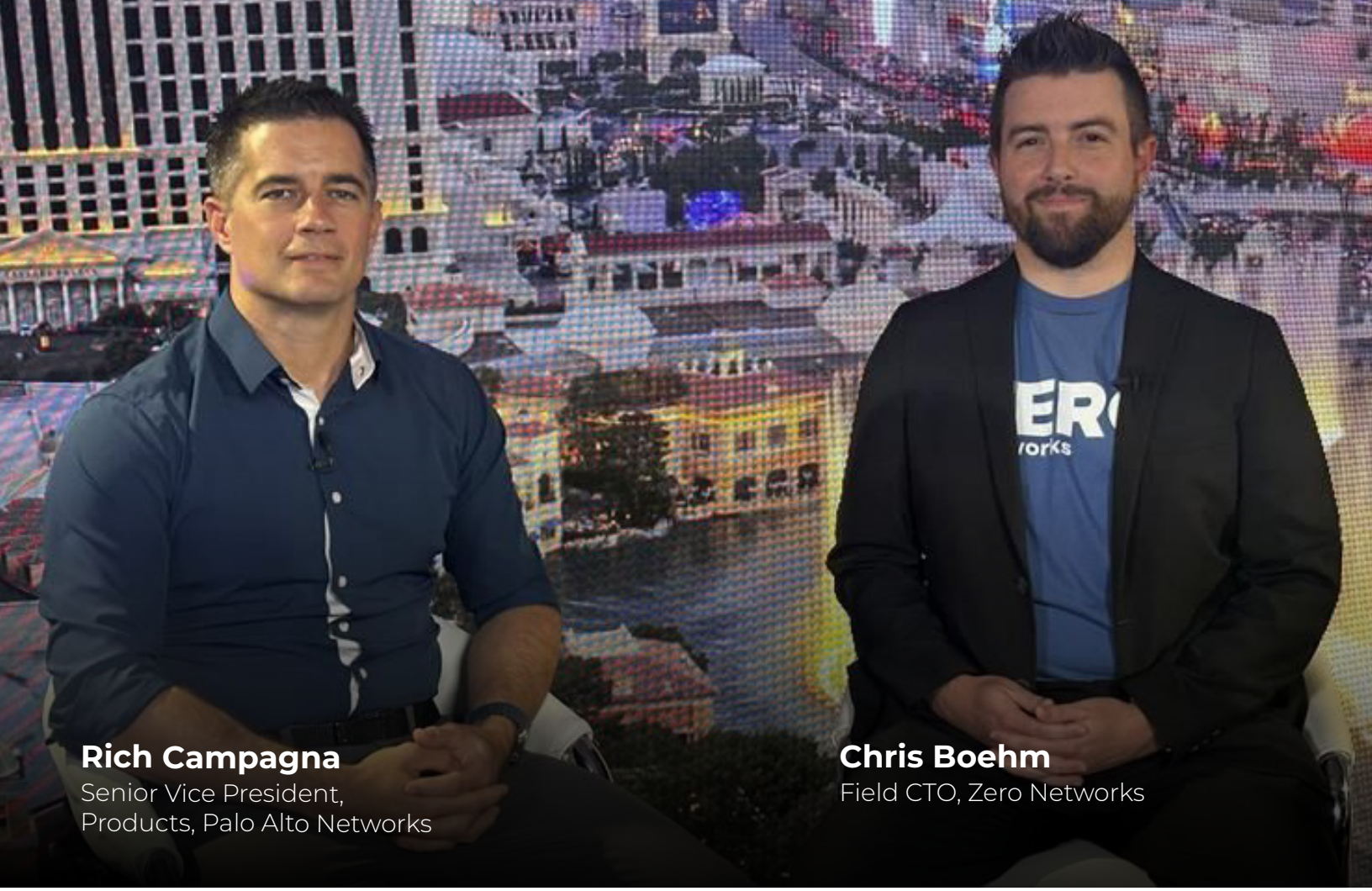
WATCH ONLINE

> "My thought is focusing on behavioral analysis - deciding what an identity is - and that way we can better ascertain how to track deviations and what might be a malicious identity or malicious use of an identity."
>
> - Alex Green

“You can imagine that it's in the business interests of a company to hold these types of data. If your company is harvesting your data to build something that takes over your job, maybe you have incentive to poison that data.”

Ben Sawyer

Associate Professor, Industrial Engineering and Management Systems, University of Central Florida



Combining Microsegmentation With Layer 7 to Stop Threats

Palo Alto Networks, Zero Networks Execs on Mitigating Lateral Spread of Ransomware

Rich Campagna, senior vice president at Palo Alto Networks, and **Chris Boehm**, field CTO at Zero Networks, describe how their companies joined capabilities to combine microsegmentation with Layer 7 inspection to protect critical assets and maintain security policies across hybrid environments.

In this video interview with Information Security Media Group at Black Hat USA 2025, Campagna and Boehm also discussed:

- How dynamic asset tagging streamlines hybrid policy management;
- Strategies to direct critical application traffic through advanced inspection;
- Reducing the blast radius by verifying user and device activity continuously.

WATCH ONLINE

> "The challenge with implementing microsegmentation has always been this complexity around identifying assets."
>
> - Rich Campagna

“Endpoint security gives you more control to reduce the dwell time.”

Vedang Parasnis
Cloud Platform Software Engineer, Intel Corporation

Service Providers Are Risking Security for User Retention

Bell Labs' **Siddharth Rao** on the Need for Stronger Safeguards in Account Recovery

Many service providers are prioritizing usability over security in account recovery to retain users. Siddharth Rao, senior security research scientist at Nokia Bell Labs, says this trade-off exposes systems to threats through vulnerable recovery channels and inconsistent policies.

In this video interview with Information Security Media Group at Black Hat USA 2025, Rao also discussed:

- How physical access and stealth tactics enable adversaries to exploit vulnerabilities;
- Why fully automated account recovery fails to address critical edge cases;
- The need for multifactor authentication tools, such as YubiKeys, in recovery flows.

WATCH ONLINE

> "There are two aspects to this. One is overly strict security policies, and the other aspect is the design problems ... there are also inconsistencies in practice. The problem is the whole approach."
>
> - Siddharth Rao

AI Agents: The New Security Wild Card

Palo Alto Networks' **Kevin Kin** on Agent Versus User Behavior Challenges

The increased prevalence of AI agents is creating new security challenges and making it harder for defenders to distinguish between agent and user behavior, said Kevin Kin, global vice president at Palo Alto Networks. He discusses how the industry has reached a new maturity in AI-powered security.

In this video interview with Information Security Media Group at Black Hat USA 2025, Kin also discussed:

- Why zero trust models and privileged access management are more critical than ever;
- Lessons learned from the IBM partnership and QRadar-to-SOC migrations;
- Strategies for addressing shadow AI usage while encouraging organizational adoption.

WATCH ONLINE

> "I think for practitioners and defenders, it's hard to differentiate what is agent behavior versus user behavior, and how do you identify that?"
>
> - Kevin Kin

“Some things may not be patchable, and so we've got to get to an infrastructure where if new, unexpected vectors of attack come, we can still weather them.”

Sam Curry
Global CISO, Zscaler

“The company also evaluates concentrations of cyber risk, and we can decide to reduce our presence in a given industry on that basis.”

Jacob Ingerslev
Head, Cyber and Tech Underwriting, Tokio Marine HCC

The AI Arms Race: When Attackers Adapt in Real Time

Mimecast's **Jason Morgan** on Defending the Human Layer Against Generative AI Threats

Gen AI is lowering the barrier for cyberattacks, enabling adversaries to launch sophisticated, adaptive attacks in real time. Cybersecurity must evolve beyond protecting inboxes and providing point solutions to securing the entire human layer, said Jason Morgan, distinguished architect at Mimecast.

> "We're coming to a point where we're going to get into an arms race with AI attacks."
>
> - Jason Morgan

In this video interview with Information Security Media Group at Black Hat USA 2025, Morgan also discussed:

- The role of deepfake technology in multi-vector intrusion campaigns;
- Cost-effective adoption of AI-powered defense strategies;
- Mimecast's responsible AI framework and ISO 42001 certification process.

WATCH ONLINE

Coinbase CSO: Crypto Security Demands Fast, Flexible Defense

Coinbase's **Philip Martin** on How Attackers Are Spending Months on Crypto Exploits

"The attackers are willing to invest time, effort and expense in attacking cryptocurrency companies because that's where the money is," says Philip Martin, chief security officer at Coinbase, warning that defenders must stay agile to counter increasingly targeted and sophisticated threats.

In this video interview with Information Security Media Group at Black Hat USA 2025, Martin also discussed:

- Why insider threats are harder to detect than outside attacks;
- The importance of tabletop exercises and threat modeling in strengthening incident response capabilities;
- Coinbase's bounty program targeting cyberattackers.

WATCH ONLINE

> "We've seen attackers spend months preparing, staging, researching or buying zero-days to spend them on attacks on us and other cryptocurrency exchanges."
>
> - Philip Martin

Why AI Security Needs Continuous Red Teaming

NIST's **Apostol Vassilev** Explains Need for Dynamic Response, Not Static Testing

As AI models grow in scale and power, leading to even more unpredictable outcomes, security teams are grappling with how to defend technologies that some experts can't begin to fully comprehend. Cyber response teams are exploring the practice of continuous red teaming, said NIST's Apostol Vassilev.

In this video interview with Information Security Media Group at Black Hat USA 2025, Vassilev also discussed:

- Information overload as an attack vector;
- The challenges of validating complex, natural language inputs;
- Combining traditional cyber practices with AI-specific measures.

WATCH ONLINE

> "You have to apply proactively red teaming to change the state of your model such that attackers will have difficulty finding the latest adversarial prompts that will attack your specific instance."
>
> - Apostol Vassilev

Island Browser Enables Secure, Responsible AI Use

VP and Field CTO **Michael Leland** on Guarding Sensitive Data in AI Workflows

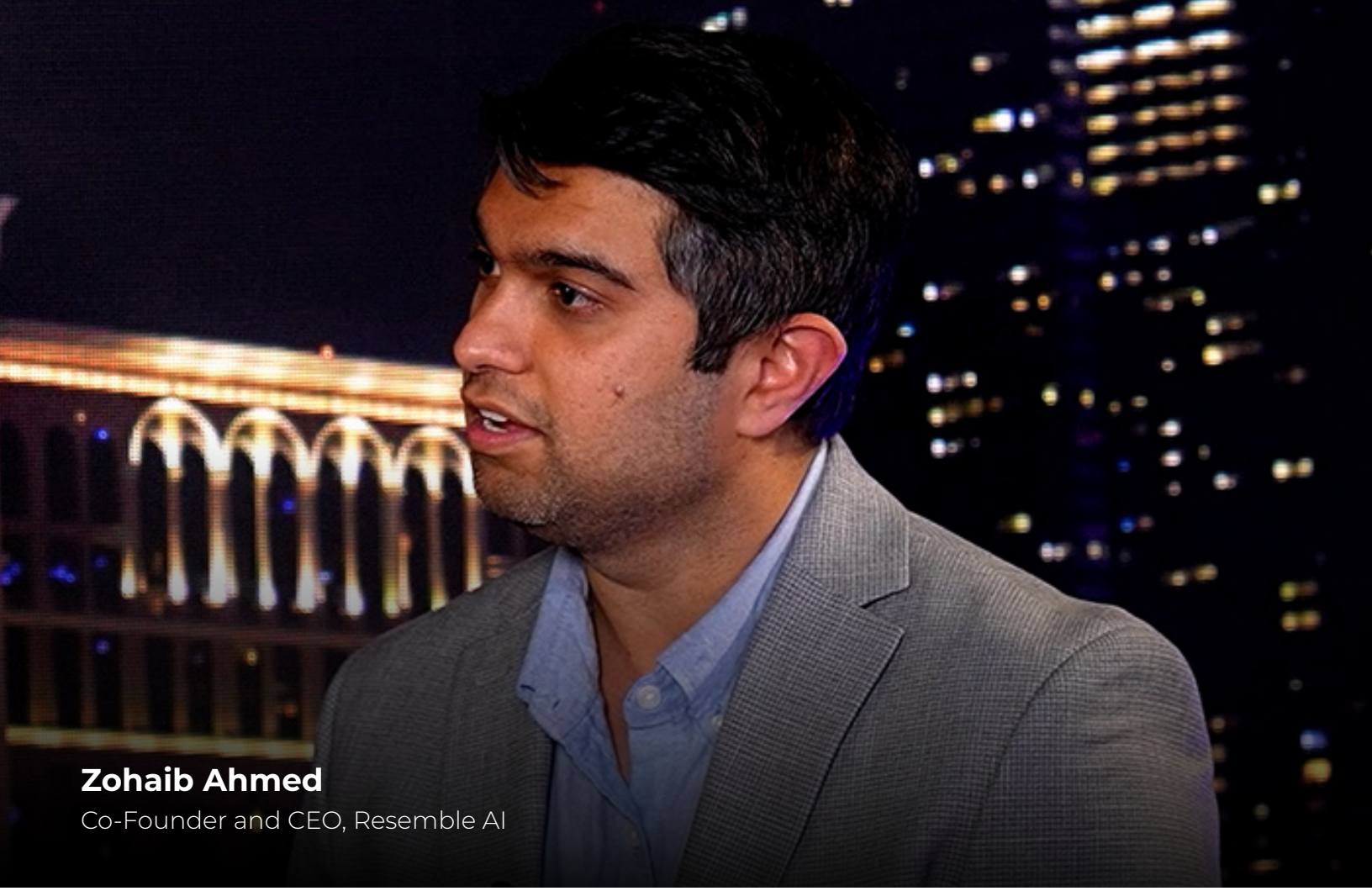
The Island Enterprise Browser operates at the presentation layer, where work happens, to monitor AI use, enforce policies and protect sensitive data, said Michael Leland, vice president and field CTO at Island.

In this video interview with Information Security Media Group at Black Hat USA 2025, Leland also discussed:

- Safe AI use through policy enforcement at the presentation layer;
- Detection and control of shadow AI in both sanctioned and unsanctioned apps;
- How dynamic device posture checks adjust permissions in real time.

WATCH ONLINE

> "Once you start using AI to index your internal files, you start learning more and more about the data ... you actually have access to knowledge."
>
> - Michael Leland



Synthetic AI Voices Are Gaining Human-Like Imperfections

Resemble AI CEO **Zohaib Ahmed** on the Rising Threats of Synthetic Voice Realism

Synthetic voices have reached Hollywood quality, but the next leap is in conversational AI that mimics human imperfections. Zohaib Ahmed, co-founder and CEO of Resemble AI, shares how adding natural pauses, tonal shifts and verbal quirks makes synthetic AI voices more realistic.

In this video interview with Information Security Media Group at Black Hat USA 2025, Ahmed also discussed:

- The challenges of controlling numerous individual attributes in voice generation;
- How open-source generative AI models are giving threat actors all the advanced tools they need - with no guardrails;
- Watermarking as a future standard for content authenticity.

WATCH ONLINE

> "Most people can't tell between AI voices and real voices. There was a study done by the University of Florida in 2024, where 73% of the people failed in determining whether a voice was AI or not."
>
> - Zohaib Ahmed

AI Deepfakes Fuel Faster, Cheaper, Targeted Attacks

Mindgard's **Peter Garraghan** on Synthetic Media Tools Being Used to Commit Fraud

Deepfake technology has evolved into a powerful tool for both innovation and exploitation. The combination of vast online data and advanced AI models allows synthetic content to be produced quickly, at low cost and with high personalization, said Peter Garraghan, CEO and CTO at Mindgard.

In this video interview with Information Security Media Group at Black Hat USA 2025, Garraghan also discussed:

- Cases of reputational damage and financial crime from deepfake attacks;
- The role of neural networks and training data quality;
- The human element and security protocols as key defense.

WATCH ONLINE

> "Whether it's voice, video or image, they can all be problematic because it's not how sophisticated it is. It's the timing. If I can get someone at a moment of weakness ... that's enough."
>
> - Peter Garraghan

TETRA Flaws Expose Critical Infrastructure Risks

Midnight Blue's **Jos Wetzels** on TETRA's Design Flaws and Probable Attacks

Researchers found encryption weaknesses and design flaws in TETRA, the radio system used by law enforcement and critical infrastructure, that allow interception and malicious traffic injection. Midnight Blue's Jos Wetzels says exploiting these flaws could disrupt essential services.

In this video interview with Information Security Media Group at Black Hat USA 2025, Wetzels also discussed:

- Packet injection attacks on OT networks using TETRA;
- Weaknesses in proprietary industrial wireless protocols;
- Limitations of current security standards and certifications.

WATCH ONLINE

> "Know what you buy. If you buy this technology and you rely on a certain security layer, you need to either fully know how it works or you need to get an independent assessment to be able to ascertain that the level of security you assume it provides is actually provided."
>
> - Jos Wetzels

How Insurers Use Threat Intelligence to Reduce Losses

Tokio Marine HCC Targets Vulnerabilities Before They're Exploited

With ransomware incidents at record highs, Tokio Marine HCC integrates darkweb monitoring, vulnerability scanning and incident data into its underwriting process to help clients close gaps and lower the chance of costly breaches.

In this video interview with Information Security Media Group at Black Hat USA 2025, **Ingerslev** and **Bovicelli** discussed:

- How darkweb intelligence and vulnerability scans inform underwriting decisions;
- Ways that incident data improves detection of high-risk clients and overlooked assets;
- Strategies to help policyholders remediate weaknesses before an attack.

WATCH ONLINE

> "One of the things we look at is the number of victims on leak sites. That's a pretty good indicator. Then we overlay that with the average payment rate of people who pay the extortion."
>
> - Jacob Ingerslev

Rethinking Software Supply Chain Security

Cyfinoid's **Shrivastava** Calls for Greater Visibility Over Software Security Risks

Software supply chain security is all too often viewed through a narrow lens, focused mostly on code dependencies and Software Bill of Materials. But the devil remains in the details and risks can emerge from overlooked areas, said Anant Shrivastava, founder and chief researcher at Cyfinoid.

In this video interview with Information Security Media Group at Black Hat USA 2025, Shrivastava also discussed:

- Broader software supply chain risks;
- Challenges with tracking and software visibility;
- Tools to improve awareness and management.

WATCH ONLINE

> "SBOM is not a security solution. SBOM is an inventory. As an inventory, how can we leverage the inventory to solve problems which are not just security-based?"
>
> - Anant Shrivastava

Risk and Liability Fears Are Stalling Enterprise AI Adoption

Honeywell's **DeLuccia** Offers Practical Steps to Address Barriers to AI Adoption

Organizations struggle to implement AI at enterprise scale because of basic fears that extend beyond technical issues. It often comes down to fundamental questions about the nature of AI and organizational accountability. "If I turn it on, am I liable for it?" asks Honeywell's James DeLuccia.

In this video interview with Information Security Media Group at Black Hat USA 2025, DeLuccia also discussed:

- Why psychological barriers slow enterprise AI deployment;
- The need for robust data governance before implementing AI systems;
- How technical confusion fuels legal and operational risk.

> "There is a fear around its [AI] existence a little bit and people don't know, 'If I turn it on, am I liable for it? Or is it liable for itself? And if it is, how do I deal with that?'"
>
> - James DeLuccia

WATCH ONLINE CyberEdBoard

Third-Party Risk Set to Reshape AI Security

Lytical Ventures' **Taylor Margot** on Autonomous Agents and New AI Defenses

As AI shifts toward autonomous agents, organizations face growing exposure from third-party systems. Strong permissioning, data orchestration and new defenses are essential to protect against opaque and potentially costly security risks, said Taylor Margot, partner at Lytical Ventures.

WATCH ONLINE

AI Worker Digital Twins Pose New Insider Threats

Researchers Say AI Bots Blur Lines Between Identity, Consent and Cyber Defense

As generative AI programs continue to evolve, they are introducing new threats to the modern workplace. Digital twins, once confined to industrial systems, now enable hyper-realistic copies of actual employees to mimic vocal patterns, behaviors and even pick up on decision-making trends.

WATCH ONLINE

How Endpoint Tools Block DNS Data Exfiltration at Scale

Intel's **Vedang Parasnis** on Securing DNS at Endpoints to Reduce Dwell Time

Vulnerabilities in domain name systems are exploited for data exfiltration and remote command-and-control operations. Vedang Parasnis, cloud platform software engineer at Intel, explains how endpoint security closes this gap with speed, accuracy and reduced attacker dwell time within systems.

WATCH ONLINE

ISMG Studio

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
info@ismg.io

Sales & Marketing

North America: +1-609-356-1499
APAC: +91-22-7101 1500
EMEA: + 44 (0) 203 769 5562 x 216

BANK INFO SECURITY® · CAREERS INFO SECURITY® · CU Just for Credit Unions INFO SECURITY

Data Breach TODAY · HEALTHCARE INFO SECURITY · GOV INFO SECURITY® · infoRisk TODAY

CyberEd.io · FraudToday.io · PaymentSecurity.io · DeviceSecurity.io · CyberEdBoard

OT.today · AIToday.io · CIO.inc · ATHENA · CYBER THEORY · Xtra mile LIFECYCLE MARKETING

QC MEDIA · SUMMIT · custom events · roundtables · NULLCON · hardwear.io Hardware Security Conference and Training · ISMG Studio

ISMG

902 Carnegie Center · Princeton, NJ · 08540 · ismg.studio