TechNetCyber

INNOVATION SHOWCASE 2026

JUNE 2-4, 2026 | BALTIMORE CONVENTION CENTER, BALTIMORE, MARYLAND

80 AFCEA 1946 2026

SIGNAL
AFCEA INTERNATIONAL MEDIA

2026 TechNet Cyber Innovation Showcase

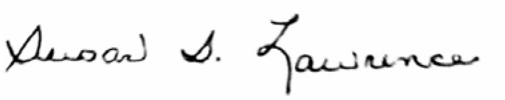
Dominating the Digital Battlespace: Confidence, Speed, Precision

As we face persistent attacks and simultaneous sophisticated campaigns that threaten political, economic and security interests, it is more important than ever to focus on delivering the right cyber power. To stay ahead of our adversaries, we must collaborate and bring together policy, strategic architecture, operations, command and control, and joint capabilities to thrive in the digital environment.

AFCEA International invites industry leaders, government officials and academia partners to convene at its annual TechNet Cyber conference to engage in meaningful discussions and share cutting-edge solutions. The Defense Information Systems Agency, U.S. Cyber Command and U.S. Department of War (DOW) chief information officer will lead the conversations, and the industry experts who have shared their solutions in this compendium will demonstrate the technologies and advancements enabling the United States to maintain its cyber edge.

The innovative solutions presented during the three-day AFCEA flagship event will respond to three problem statements raised by DOW partners and government representatives related to agentic artificial intelligence, automated authority to operate and zero trust in contested and disconnected environments. By giving industry professionals a chance to share their cyber solutions at the event's *SIGNAL* Innovation Showcase, we hope to spur the development of solutions that aid warfighters at the tactical edge and defend against today's cyber threats.

Best wishes,



Lt. Gen. Susan S. Lawrence, USA (Ret.)
President and CEO
AFCEA International

Table of Contents

AGENTIC AI

AUTOMATED AUTHORITY TO OPERATE (ATO)

ZERO TRUST IN CONTESTED AND DISCONNECTED ENVIRONMENTS

Submissions

Agentic AI

Opportunity Statement: DISA is exploring the adoption of agentic artificial intelligence (AI) to orchestrate and automate defensive cyber operations across a diverse ecosystem of security tools, data sources and operational workflows. While AI agents offer transformative potential to accelerate threat detection and response, the industry lacks mature standards for agent interoperability, secure integration and governance. We are seeking to understand how industry partners are implementing agentic AI today—specifically, what interoperability protocols are proving effective, how industry is integrating existing authentication and authorization solutions to ensure least-privilege access for agents within a zero-trust architecture, and what frameworks exist for governing autonomous actions in high-stakes operational environments.

Why this is Important: Agentic AI represents a fundamental shift from passive automation to autonomous systems that can reason and act on behalf of human operators. Without established standards and proven governance frameworks, we risk deploying agents that could introduce security vulnerabilities, produce unreliable outcomes or operate outside their intended scope. Understanding how industry is solving these challenges is critical for the agency to harness the power of agentic AI effectively and lead in its secure adoption.

AI on the Cyber Frontline: Strategic Impacts on DOD Operations and OPSEC

Joe Ford, SE Manager, Office of the CTO, Check Point Software Technologies •
JoeFord@checkpoint.com

ABSTRACT

Artificial intelligence (AI) is rapidly transforming the U.S. Department of Defense's (DOD's) approach to cyberspace, enabling faster threat detection, autonomous response and enhanced decision-making across joint all-domain command and control (JADC2) environments. This session will examine the strategic implications of AI integration into DOD cyber operations over the next five years, with a particular focus on its impact on operational security (OPSEC). As AI systems ingest and act on vast volumes of data, new vulnerabilities emerge—ranging from adversarial manipulation and data poisoning to inadvertent exposure of sensitive mission patterns. Designed for DOD cyber leaders and technologists, this discussion will explore how AI is reshaping cyber defense postures, force readiness and OPSEC practices, while highlighting the ethical and strategic challenges of maintaining trust and accountability in an increasingly autonomous battlespace.

BIO: Joe Ford is a technical professional with more than 30 years of experience in selling information technology (IT) and security solutions to U.S. government agencies and Fortune 500 companies, with expertise in infrastructure, security, backup, virtualization, wireless, storage and business systems across public and private sectors. He demonstrates strong leadership and collaboration skills, successfully guiding technology implementations and achieving FedRAMP authorization for a government security platform. Ford focuses on driving ROI and sustainable growth by reducing operational costs, forming strategic alliances and leading teams to deliver complex solutions efficiently. He is a top performer with deep knowledge of technology and security landscapes, adept at complex enterprise sales and communicating effectively with high-level executives. Ford consistently exceeds sales targets and engages in public speaking, social media and thought leadership to build influential industry relationships.

AI-Driven Threat Detection at the Speed of the Network: A Live End-to-End Demo

Aaron Boteler, CTO, CloudCurrent • aaron@cloudcurrent.biz
Evan Powell, Founding CEO, DeepTempo • evan@deeptempo.ai

ABSTRACT

Modern adversaries move faster than signature-based and rule-driven defenses can react, and they move through networks: hybrid IT, OT and cloud environments whose operational reality is invisible to most detection stacks. This session demonstrates how a fully integrated AI-native detection and visualization pipeline closes that gap in real time, grounded in the network and operational picture that makes findings actionable.

Evan Powell (DeepTempo) and Aaron Boteler (CloudCurrent) walk attendees through a live demonstration running against a realistic simulated network environment purpose-built for this talk. DeepTempo's LogLM, a vertical foundation model trained exclusively on security telemetry, ingests raw telemetry from hybrid IT, OT and cloud environments to produce high-fidelity behavioral findings such as reconnaissance, lateral movement, C2 activity and exfiltration, without signatures, rules and per-environment retraining.

Those findings are passed through CloudCurrent's VStrike fusion layer, which correlates them with network topology and multisource telemetry to place every detection in its operational context: which assets, segments, mission systems and adversary pathways are actually in play. The enriched, network-aware findings are then surfaced through Vigil (vigilsoc.org), an open-source platform started by DeepTempo, delivering fully interactive visualizations that let operators step through attack timelines, map activity to MITRE ATT&CK and understand not just that an attack occurred but where on the network, how it propagated and why it matters to the mission.

Attendees will leave with a clear picture of how AI-native detection, network-grounded fusion and open cyber visualization combine into a practical, deployable stack that DOD and government cyber teams can evaluate, adopt and extend today.

Key Takeaways:

- How foundation models detect adversary intent, not just anomalies, across encrypted IT and OT traffic
- How the VStrike fusion layer grounds AI findings in network topology and operational context, turning detections into mission-relevant intelligence
- How open cyber visualization (Vigil) gives operators a continuous operational picture of adversary activity across the network
- A proven, deployable stack aligned with DISA and U.S. Cyber Command modernization priorities

BIO: As the CTO of CloudCurrent and the visionary architect behind the vStrike Platform, Aaron Boteler brings more than 25 years of elite engineering experience to the intersection of cyber-security and signals intelligence (SIGINT). His career is defined by a deep-seated expertise in embedded and full-stack domains, where he has pioneered the development of high-fidelity geospatial tools and immersive rendering solutions specifically for the intelligence community.

Boteler's work is rooted in a fundamental mission: solving the "pervasive awareness" crisis within the IT, OT and cyber arenas. By bridging the gap between complex data and human intuition, he created vStrike to serve as a sovereign visualization layer that transforms fragmented data into a collaborative, mission-critical dashboard. Under his leadership, the platform has evolved into an industry-leading asset health and monitoring solution, delivering a level of operational clarity and proven insight that is currently unmatched in the marketplace.

Evan Powell is founder and CEO of DeepTempo, building the intelligence layer for machine-speed cybersecurity, which includes the LogLM foundation model for extremely accurate and easy-to-use threat prediction and detection and Vigil, a leading open-source AI SOC project that has grown very quickly in 2026.

Previously, he co-founded StackStorm, the leading open-source SOAR project, which is now a Linux Foundation project, as well as several other companies and open-source projects that achieved mass adoption in large enterprises and service providers.

Advancing Security Operations Through Agentic AI: Balancing Automation With Human Oversight

Mark Maglin, VP DOW Cybersecurity Strategy, ECS Federal • mark.maglin@ecsfederal.com

ABSTRACT

As organizations face exponentially growing alert volumes and increasingly sophisticated cyber threats, the traditional SOC model has reached its practical limits. This Innovation Showcase demonstrates how ECS Federal successfully deployed agentic AI to transform its security operations while maintaining critical human oversight and decision-making authority.

ECS Federal's 24/7, multitenant SOC analysts were processing more than 2,500 alerts per analyst per month, making a hire-to-keep-up model operationally and economically unfeasible. The organization faced three critical operational challenges.

- Limits of Existing Automation: ECS had maximized the practical limits of its SOAR technology. While effective for enrichment and response actions, SOAR lacked the ability to reason through complex investigations or safely auto-close benign alerts
- Alert Overload and Analyst Fatigue: Benign alerts consumed disproportionate analyst time, displacing focus from genuine threats, leading to fatigue and operational inefficiency
- Inconsistent Manual Triage: Human-driven triage produced variable outcomes requiring standardized, auditable processes

The Agentic AI Solution

Rather than replacing human analysts, ECS Federal implemented agentic AI agents as an autonomous investigative layer designed to provide analysts with leverage. The solution conducts deep, contextual investigations while delivering decision-ready investigation reports with clear conclusions and supporting evidence.

ECS integrated AI agents directly into its existing workflows moving alerts from detection systems through SOAR, to the AI agent for autonomous investigation, with outcomes fed back into ServiceNow for centralized case management and auditability.

Defending Against AI-Enabled Offensive Attacks

AI is increasingly being leveraged by adversaries to craft more sophisticated and automated attacks, including highly convincing phishing campaigns, advanced malware and even autonomously executed cyber warfare.

Agentic AI defenses address these threats by:

- Matching speed and scale

- Deep contextual investigation, which is essential when AI-powered attacks adapt their behavior to avoid detection
- Consistent, auditable analysis

Human-in-the-Loop Safeguards

Critical to this implementation is the preservation of human decision-making authority. The AI agent system enhances analyst effectiveness by standardizing triage in a repeatable, auditable manner while ensuring transparency. Each alert arrives with clear conclusions, supporting evidence and rich context, improving trust and decision quality.

Results

- Tier 1 Alert Auto-Closure Rate: 70% of alerts automatically closed safely without analyst involvement.
- Investigation Response Time:100% of alerts investigated immediately upon creation
- Scalability Achievement: Broke the SOC scalability ceiling
- Headcount Efficiency: Scaled SOC operations 20% without adding headcount

Qualitative Outcomes

- Scalable solution to combat AI-generated attacks
- Improved Analyst Effectiveness and Retention: No negative impact to SLA. With queues cleared and workloads more manageable, analysts experienced less burnout and greater job satisfaction.
- Enhanced Strategic Focus: Focus on higher-value work like threat hunting, detection engineering.
- Investigation Depth: Context and evidence-gathering exceeded what analysts would typically perform during initial triage

Conclusion

The ECS Federal case demonstrates that agentic AI, when implemented thoughtfully with human-in-the-loop controls, can dramatically enhance security operations without sacrificing the judgment and accountability that only human analysts can provide. This phased approach—from virtual agent implementation through autonomous task execution—positions organizations to achieve significant operational improvements while maintaining essential human oversight.

BIO: Mark Maglin is the vice president for DOW cybersecurity at ECS Federal, where he leads business development and manages a portfolio of cybersecurity managed services. Maglin has lead enterprise-wide deployments and delivered security-as-a-service for the DOW and U.S. Army, integrating multiple vendor security tools into a single integrated cyber defense platform delivered as a service. Maglin has provided enterprise program management, acquisition, financial management and systems engineering support to DOW intelligence community customers for acquisition of full life cycle support for major ACAT IT systems. Prior to his industry career, Maglin served in the U.S. Navy for more than 23 years.

Machine-Speed Conflict: What Internet-Scale Data Reveals About Threat Actor Evolution

Nishawn Smagh, Director of Intelligence, GreyNoise Intelligence • shawn@greynoise.io

ABSTRACT

GreyNoise telemetry indicates that cyber adversaries are gaining access to vulnerabilities prior to public disclosure. The research indicates that threat actors employ AI-assisted reconnaissance and machine-speed exploitation, compressing vulnerability weaponization timelines from weeks to hours. Most significantly, it reveals that attacker behavior itself offers predictive signals. An analysis of 216 malicious activity spikes from the GreyNoise Global Observation Grid revealed that 80% preceded CVE disclosures by up to six weeks.

This presentation summarizes 12 months of internet-scale threat telemetry from GreyNoise's Global Observation Grid, revealing fundamental shifts in adversary structures, motivations and operational tactics. Through analysis of billions of malicious observations, we document the industrialization of cyber operations—where threat actors operate as distributed automation ecosystems rather than individual operators.

The key takeaway is that attacker behavior offers predictive signals, providing defenders with an actionable early warning window. Defense must evolve comparably, leveraging automation, behavioral analytics and predictive intelligence derived from internet-scale observation.

BIO: Nishawn Smagh is the principal intelligence liaison and a senior executive at GreyNoise Intelligence, where he leads collaboration with global government and enterprise partners to enhance their ability to detect, understand and respond to advanced cyber threats. Drawing on decades of operational experience, he helps organizations strengthen both their offensive and defensive capabilities, advising on how government and commercial enterprises can counter sophisticated adversaries, defend critical networks and outpace rapidly evolving APT tradecraft. In his role at GreyNoise, Smagh connects real-world threat activity to actionable intelligence, helping partners detect and disrupt adversary operations at speed and scale. His mission is to empower operators and decision-makers with the insights needed to anticipate change and build resilience in an increasingly contested digital domain. A retired U.S. Air Force intelligence officer with 25 years of service, Smagh most recently served as director of intelligence for the Cyber National Mission Force at U.S. Cyber Command, leading intelligence operations for a 2,000-member joint command charged with deterring, disrupting and defeating malicious cyber actors. Throughout his Air Force career, Smagh commanded at the squadron, group and wing levels, leading intelligence operations across multiple global theaters. His decorations include the Defense Superior Service Medal, two Legions of Merit, the Bronze Star Medal and the Defense Meritorious Service Medal. Smagh is a graduate of the U.S. Air Force Academy and holds master's degrees in international relations and management. He completed professional military education at the U.S. Army Command and General Staff College and undertook

senior development education at the Congressional Research Service, Library of Congress, where he supported congressional oversight and policy analysis on national security issues. At GreyNoise Intelligence, Smagh brings deep operational and intelligence leadership to the private sector, helping partners bridge the gap between strategy and execution to anticipate threats, enhance detection and response.

From Automation to Autonomy: Governing Agentic AI in Defensive Cyber Operations

Jason Malnar, Lead Cybersecurity Solutions Architect, Merlin Cyber •
jmalnar@merlincyber.com

ABSTRACT

DISA has identified a critical challenge: while agentic AI has the potential to transform defensive cyber operations, the industry lacks proven standards for interoperability, secure integration and governance. Merlin Cyber addresses this gap with a lab-validated autonomous SOC architecture that operationalizes agentic AI across real-world, multivendor environments.

This solution moves beyond rule-based automation by deploying an AI SOC analyst capable of ingesting threat intelligence, executing cross-platform threat hunts, enriching findings, assessing severity and blast radius, and generating response recommendations. In testing within a federal lab environment, the system reduced threat detection-to-response time from hours to under five minutes while decreasing analyst triage workload by up to 80%.

The architecture integrates multiple security platforms—including EDR, orchestration, threat intelligence, asset intelligence and ITSM—through API-driven interoperability and a normalized data model. This enables agents to operate consistently across heterogeneous environments, including multi-EDR deployments.

To align with zero-trust principles, all agent actions are governed through least-privilege access using scoped API credentials and strict tenant-level authorization boundaries. Autonomous actions are controlled through a just-in-time (JIT) human authorization gate, supported by a predefined action framework and AI-generated rationale for every recommendation. All decisions and actions are logged end to end, producing an auditable chain aligned to NIST 800-53 (AU, SI, IR) controls.

This session provides a practical implementation-focused perspective on agentic AI, demonstrating how interoperability, authorization and governance challenges can be solved today using commercially available technologies. Merlin Cyber's approach offers DISA a validated model for securely adopting agentic AI within high-stakes operational environments.

BIO: Jason Malnar is a lead cybersecurity solutions architect at Merlin Cyber, bringing more than 20 years of federal IT experience across cybersecurity, enterprise infrastructure and mission-driven technology modernization. His career includes roles as federal account executive at SentinelOne, senior solutions engineer at Nutanix and systems and virtualization lead at the U.S. Department of Energy headquarters—a trajectory that has given him rare fluency in both

the security and infrastructure sides of the house and a sharp understanding of how the two must converge to enable and protect the mission. Additionally, Malnar is a National Institute of Standards and Technology (NIST) published author on trusted cloud infrastructure. A veteran of the U.S. Air Force and Operation Enduring Freedom, Malnar brings the same discipline and mission focus to the civilian sector that defined his military service.

Agentic AI, Multisource Fusion and the Hidden Strain on Analytical Infrastructure

Antonio Ibáñez, Solutions Architect, Ocient National Security Solutions •
tibanez@ocient.com

ABSTRACT

Cyber defense practitioners routinely operate in environments where insight depends on fusing data from many sources. Traditionally, this fusion process has been driven by human analysts who pace their queries, apply judgment to partial results and decide when an answer is sufficient for the task at hand. Agentic AI changes that dynamic. Rather than serving as a passive assistant, an AI agent can autonomously decompose an analytical objective, explore multiple hypotheses in parallel, validate assumptions and iteratively refine results. While this shift offers clear productivity benefits, it also introduces a new and often overlooked challenge: query and compute amplification at the backend data infrastructure layer. Agentic workflows are exploratory, iterative and nondeterministic by design. They do not naturally account for cost, contention or system-level constraints unless those considerations are explicitly surfaced.

This talk examines how agentic AI exposes architectural assumptions that were reasonable in human-paced analytics but fragile under autonomous, machine-paced fusion. It discusses why common mitigations—such as semantic layers, data governance and specialized analytical engines—improve correctness and trust but do not by themselves limit workload amplification. It also explores how fragmented analytical environments, where different systems are used for historical, real-time, geospatial or graph analysis, can unintentionally increase agent orchestration complexity and query fan-out. Finally, the session outlines emerging architectural principles for supporting agentic workloads responsibly. The goal is not to replace human judgment but to enable the infrastructure supporting autonomous agentic workflows to be reliable, governable and mission ready as analytic velocity increases.

BIO: Antonio (Tony) Ibáñez is a solutions architect for Ocient National Security Solutions. In his role, Ibáñez helps deliver public-sector organizations' solutions for their most difficult data analysis challenges. A veteran of companies such as SGI, DDN Storage, Cleversafe, IBM and Cohesity, Ibáñez has more than 20 years of experience architecting and sustaining large-scale systems for government agencies and national security organizations.

Beyond the API Key: Securing the Mission-Critical Shift to Autonomous AI

Brandon Iske, Principal Solutions Architect, Okta • brandon.iske@okta.com

ABSTRACT

As the U.S. Department of War races to integrate LLMs and autonomous agents into scientific workflows, traditional security is hitting a breaking point. Legacy API keys and manual OAuth flows weren't built for the speed of the mission; they create "over-permissioned" risks that stall innovation and complicate audits in high-security environments.

This session introduces Cross App Access (XAA), an emerging identity-first standard that treats AI agents as first-class identities. By leveraging the Identity Assertion JWT Authorization Grant (ID-JAG) extension to OAuth 2.0, XAA replaces static permissions with dynamic, task-specific authority.

We will explore how a unified security fabric—integrating XAA with other industry standards like the Shared Signals Framework and Model Context Protocol (MCP)—dramatically reduces risk and time to respond to security challenges. Attendees will learn to eliminate the identity gap, ensuring that AI-driven discovery scales securely across the enterprise for both warfighters and their autonomous counterparts.

BIO: Brandon Iske is a principal solutions architect focused on enabling federal government and strategic accounts at Okta. He is passionate about strengthening our nation's cybersecurity and user experience through identity-focused IT modernization and cyber best practices. Before joining Okta, Iske worked for more than a decade in government public service to deliver and secure joint U.S. Department of Defense enterprise capabilities in endpoint security, mobile management, identity and access management, and zero-trust architecture at the Defense Information Systems Agency. He earned a bachelor's degree in computer science from the University of Nebraska at Omaha. He is also a National Science Foundation CyberCorps Scholarship for Service alumnus and an Okta certified professional.

Agentic AI, Accountable Operations: Governing Private AI in Mission-Critical Workflows

Alexei Ivanov, Federal Chief Technology Officer, Pegasystems • Alexei.ivanov@pega.com

ABSTRACT

Agentic AI promises faster threat detection, response and decision-making, but ungoverned autonomy introduces unacceptable risk in defense and cyber environments. In this session, we explore how industry is implementing agentic AI within accountable operational frameworks, where agents collaborate across tools yet remain constrained by policy, oversight and audit. Attendees will learn how workflows, case management and agent interoperability patterns provide the missing control plane for deploying autonomous AI in high-stakes environments. The discussion focuses on practical governance models that ensure autonomous actions are explainable, repeatable and aligned to mission outcomes, allowing organizations to scale AI safely without sacrificing operational trust. Rather than replacing human decision-making, agentic AI becomes a governed participant in enterprise operations, operating with clarity about responsibility, authority and accountability.

Attendees will leave with a clear, practical framework for harnessing their own AI investments with the Pega platform, deploying agentic AI not as an unchecked force but as a governed digital worker within the operational guardrails that defense and cyber missions require.

BIO: As the federal CTO, Ivanov supports Pega's U.S. federal clients across civilian, DOD and intel accounts. Over the past 15 years, he has helped many agencies (federal and state) innovate and transform using Pega technology. As CTO, he works closely with customers and prospects as a trusted adviser and a Pega technologist to help deliver on mission-critical programs and initiatives.

Accelerate and Secure the Mission With Identity Security for AI

Andrew Whelchel, Lead Solutions Engineering – Federal, Saviynt •
andrew.whelchel@saviynt.com

ABSTRACT

Agentic AI introduces a new operational paradigm where autonomous agents orchestrate defensive cyber operations across heterogeneous environments. However, the absence of mature standards for interoperability, identity governance and secure integration creates significant risk. AI agents must interact with multiple tools, data sources and privileged systems, often requiring dynamic, machine-to-machine access. Without robust identity controls, these agents may operate with excessive privileges, lack accountability or execute unintended actions. Traditional identity and access management (IAM) models are not designed to handle non-human identities at scale, particularly those capable of autonomous decision-making within zero-trust architectures. Delivery at this scale rather requires an identity security for AI approach that provides identity security assurance for AI agents operating in the joint all-domain environment.

By delivering zero trust via identity security for AI (specifically for AI agents) for joint all-domain operations missions, organizations gain benefits as they leverage identity security for AI capabilities that enable missions and defend against cyber threats to the AI operating plane. These organizations reap mission benefits from their AI operations, mitigating contested security risks and ensuring mission continuity. These benefits result from using identity security for AI, enabling accelerated risk reduction and executing a compressed time-to-enforcement for zero trust for the AI agents.

When organizations deliver identity security for AI agents, they accelerate the mission and safely operationalize agentic AI with several essential capabilities, including:

- Non-Human Identity Governance: Life-cycle management for AI agents, including creation, modification and decommissioning.
- Dynamic Least-Privilege Access: Context-aware authorization that adapts to agent behavior, mission context and risk posture.
- Policy-Based Access Control: Fine-grained enforcement using attribute-based and risk-adaptive controls aligned to zero-trust principles.
- Auditability and Accountability: Full traceability of agent actions with immutable logs for compliance and forensic analysis.
- Autonomous Governance Controls: Guardrails that constrain agent behavior within predefined operational and ethical boundaries.

Agentic AI has the potential to transform cyber defense operations, and its success depends on establishing strong identity-centric governance. By extending identity security capabilities to AI agents, an organization can enforce least privilege, ensure interoperability and maintain accountability within a zero-trust framework. This

approach mitigates risks associated with autonomous systems while enabling scalable, secure adoption of agentic AI in mission-critical environments. As part of this session, attendees will learn about key capabilities, including identity security for AI for agent registration, policy enforcement for AI agents and ensuring audit requirements in the joint all-domain environment for AI agents.

BIO: Andrew Whelchel (CISSP-ISSAP, ISSEP, CAP, CCSP, CSSLP) started in information security and IAM immediately after graduating from the University of Memphis, supporting identity and access management and managing Microsoft Identity for U.S. federal customers. Later, the role transitioned to network infrastructure security and then to consumer identity protection at RSA Security and, most recently, at Okta and Saviynt. At RSA Security, supporting financial services, health care, U.S. federal and other customers, the focus was on identity risk analytics and integration of identity fraud intelligence for cyber crime prevention. In prior roles at Okta and current roles at Saviynt, the focus is on protecting employees' and business partners' identities for public-sector agencies to reduce cyber risk and accelerate cloud transformation capabilities. Contributions include serving as a contributor on the NIST 1800-3 ABAC (attribute-based access control) standard and speaking engagements on identity access management and security. Currently, studies are at Augusta University in pursuit of the master of arts degree in intelligence and security studies.

Operator X: Optimizing Agentic AI for High-Stakes Environments

Nathan Delgado, Director of Software Products, SealingTech ·
nathan.delgado@sealingtech.com

ABSTRACT

This presentation covers the challenges and evolution of SealingTech's groundbreaking AI platform: Operator X™.

Operator X uses large language models (LLMs) and retrieval-augmented generation (RAG) to enhance the efficiency and effectiveness of the cyber warfighter. To address the unique security requirements of cyber operations, SealingTech prioritizes a fully air-gapped architecture, ensuring that sophisticated agentic capabilities remain effective at the tactical edge without reliance on external connectivity.

To address the U.S. Department of War's (DOW's) need to operate across a diverse ecosystem of tools, Operator X utilizes the model context protocol (MCP) for agentic workflows. This approach moves away from rigid, one-off integrations toward a flexible architecture enabling a standardized, interoperable bridge between agents and diverse data sources. To facilitate governance in high-stakes environments, Operator X incorporates a human-in-the-loop framework, with live feedback and explained reasoning ensuring oversight of agentic action.

The presentation will share how Operator X continues to evolve and expand its capabilities based on mission needs and a rapidly shifting technology environment. Optimizing Operator X for deployment in disconnected, resource-constrained environments presents significant R&D challenges compared to traditional cloud-enabled AI. Innovations in architecture design, model evaluation and context window management enable a mobile solution that delivers elite reasoning capabilities at the edge.

By bridging the gap between resource-heavy AI and the disconnected warfighter, SealingTech ensures that defenders can hunt adversaries more effectively and efficiently in any challenging environment.

BIO: Nate Delgado is a distinguished product leader at the forefront of artificial intelligence and cybersecurity innovation. As the director of software products at Sealing Technologies (SealingTech), a Parsons Corporation company, his team is building the first AI cyber analyst designed specifically for offline environments. Prior to SealingTech, Delgado scaled global managed detection and response (MDR) programs serving Fortune 500 clients and led the product team at a cut-

ting-edge malware analysis software company. Delgado comes to SealingTech with a proven track record of leading complex AI and machine learning products, including advanced threat hunting capabilities for major federal agencies. His commitment to advancing the field extends to the next generation where he actively mentors cybersecurity students through university programs across the United States. He holds a bachelor of arts degree in economics from the University of Southern California (USC).

Agentic AI at Mission Scale: Identity-Enforced, Zero-Trust Autonomous Cyber Defense for the Department of War

Pete White, Senior Advisory Solution Consultant, Security Operations, ServiceNow •
pete.white@servicenow.com

ABSTRACT

Adversaries are accelerating. Attack surfaces are expanding. Analyst capacity cannot keep pace. DISA's exploration of agentic AI for defensive cyber operations is not a technology evaluation; it is a mission imperative.

ServiceNow, together with its recently acquired identity governance platform Veza, delivers a production-proven, governance-ready foundation for agentic AI across the full defensive cyber life cycle.

ServiceNow's security operations platform provides the orchestration layer the U.S. Department of War needs. Rather than replacing existing tools, it integrates across SIEMs, EDR platforms, threat intelligence feeds and asset repositories through certified integrations and an open API framework. AI agents operating within this layer can consume signals from any authorized source, reason across correlated context and execute response workflows within a single, auditable system of action, including agent-to-agent interactions with non-ServiceNow agents, fully aligned to zero-trust mandates.

Veza solves the hardest piece of the agentic puzzle: least-privilege enforcement for non-human identities. Veza's graph-based identity security platform defines, enforces and continuously verifies the authorization boundaries within which AI agents operate, scoping every agent to specific data sources, tools and actions based on mission role.

This is operationally enforced zero trust for the agentic era.

Governance is built in, not bolted on. ServiceNow's workflow engine applies human-in-the-loop checkpoints calibrated to action risk, with every agent decision logged and attributable to specific authorization chains, meeting FISMA and DISA STIG evidentiary standards.

Open interoperability. Identity-enforced least privilege. Auditable autonomous action. ServiceNow and Veza answer DISA's core questions.

BIO: Pete White is a senior advisory solution consultant, security operations at ServiceNow. He is a CISSP certified information security specialist with more than 20 years of experience in securing enterprises.

Intersection of Quantum, AI and Security

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies •
gina.scinta@thalestct.com

ABSTRACT

Artificial intelligence (AI) is rapidly transforming our world from the way we work to the way we interact with machines. Once AI is able to utilize the power of quantum computing, the results—both good and bad—will be immeasurable. As AI becomes more sophisticated, so too do the potential security risks.

This session will discuss the critical issues at the intersection of quantum, AI and security. The speaker will explore:

- Countering malicious use of AI systems by actors with ill intentions, such as criminals, terrorists or hostile states.
- Adversarial attacks on AI, such as attempts to fool or manipulate AI systems by exploiting their vulnerabilities or limitations.
- Protection of the massive amounts of data used by AI systems to learn and improve their performance.
- Using AI to enhance cybersecurity, such as preventing cyber attacks, optimizing security processes and improving security resilience.
- Deploying quantum-resistant security to protect data at the heart of AI

BIO: Gina Scinta is Thales TCT's deputy chief technology officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission-critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC and more. Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world-class encryption and key management for data at rest in data centers and cloud infrastructures.

Leveraging Wiz Security To Enable Adoption of Agentic AI for Defensive Cyber Operations

Chris Saunders, Director of Public Sector Sales Engineering, Wiz Inc. •
chris.saunders@wiz.io

ABSTRACT

As the U.S. Department of War (DOW) transitions toward agentic AI to automate defensive cyber operations (DCO), the primary challenge shifts from model performance to architectural trust and governance. At Wiz, we're building a platform that directly supports DISA and the DOW's vision for agentic AI in DCO. Our approach delivers sophisticated automation, secure integration and strong governance across all your security tools and data.

Wiz offers a mature, agentic AI-ready platform to orchestrate and automate DCO, ensuring interoperability, secure integrations with engrained zero-trust principles and robust governance for autonomous actions in high-stakes environments. Wiz provides a comprehensive security and governance framework that enables DISA to deploy autonomous agents with confidence. By leveraging our industry-leading Cloud Native Application Protection Platform (CNAPP) and AI-Security Posture Management (AI-SPM), Wiz provides the "connective tissue" required to orchestrate agents across diverse security tools while enforcing zero-trust principles and autonomous guardrails.

Wiz addresses the lack of mature standards around AI by providing complete visibility. Our security graph maps every AI agent, its underlying large language model (LLM), privileges granted and the specialized tools/APIs it invokes into a single pane of glass. This allows DISA to visualize the "blast radius" of an agentic workflow across disparate DCO tools.

Our Wiz Integrations Network (WIN) creates an open ecosystem, bringing together more than 140 security tools and data sources. This enables the ability to orchestrate workflows and automate remediation across your existing security stack (e.g., SIEM, EDR and SOAR), ensuring the built-in multiagent orchestration remains transparent and auditable.

In a zero-trust architecture, an AI agent is a non-human identity. Wiz differentiates by integrating directly with existing authentication and authorization (AuthN/AuthZ) solutions to analyze agent permissions. We identify "overprivileged agents" that have broader system access than their defensive mission requires, enabling the DOW to enforce strict identity bindings and prevent lateral movement if an agent is compromised via prompt injection or logic manipulation. We further enforce secure integration by monitoring service accounts for least-privilege access suggesting changes to overly privileged accounts, strengthening AuthN/AuthZ.

Wiz integrates with identity security solutions like CyberArk and Linx Security for just-in-time access, directly supporting a robust zero-trust architecture. Our platform builds multilayered defense, continuously verifying and authorizing every interaction.

Wiz offers an AI bill of materials, which tracks the lineage of agents, including the model context protocol (MCP) servers. This framework provides DISA and the DOW with a standardized method to govern the supply chain, ensuring only approved, vetted agents are permitted to execute actions in high-stakes environments.

Beyond static configuration, Wiz provides runtime AI security. We monitor agent behavior for deviations from intended operational workflows, such as an agent attempting to exfiltrate data or modify firewall rules outside of its defined mission parameters. This provides the human-in-the-loop governance necessary for high-stakes DCO, where autonomous actions must be reconciled against real-time security policies. This means critical automated remediation actions can be reviewed and approved by people through interactive messaging, ensuring transparency and accountability. Features like approval requests and workflow variable governance help restrict sensitive data flow, providing policy-driven oversight and avoiding "black box" automation worries.

Our blue AI agent and green agent concepts use agentic principles to automate threat investigation, assign verdicts and create dynamic remediation plans with human validation.

BIO: Chris Saunders is a sales engineering leader with 26 years of professional experience working in the federal government space to ensure mission-critical solutions are delivered to meet security and compliance outcomes. He has a penchant for collaborating with sales and engineering teams to develop technical strategies and drive customer outcomes.

Advancing Secure, Autonomously Driven Cyber Defense Through Agentic AI

Isaiah Akers, Senior Cloud Computing Application Architect, Booz Allen Hamilton •
akers_isaiah@bah.com

ABSTRACT

As cyber threats evolve in speed and sophistication, defensive operations must shift from reactive alert-based workflows to proactive, autonomous cyber defense. This requires the adoption of end-to-end, defense-in-depth solutions powered by AI. Advanced methods disrupt the adversary, eliminating their AI advantage. Agents automate mitigations, accelerate identification and automate manual workflows so that organizations can execute security operations at machine speed.

To meet this charter, Booz Allen is advancing agentic identification and mitigation by integrating autonomous detection engineering capabilities (Booz Allen's Vellox RangerTM), which automates the creation and tuning of detection logic while interfacing directly with endpoint detection and response (EDR) platforms for proactive mitigation. This enables SOC teams to surface malicious behaviors, continuously refine detection coverage and orchestrate rapid, machine speed mitigations before threats can propagate.

Second, we are adding agents directly into the SOC to increase operational velocity and reduce analyst workload. Through partnerships, like our work with Andesite, we are introducing mission-tailored agents that autonomously execute key SOC workflows, correlating alerts, triaging events, validating indicators and initiating response actions. These agents act as intelligent teammates that extend human capacity while standardizing and accelerating end-to-end SOC processes.

Finally, we are ensuring agents operate securely and safely by anchoring them within our secure AI architecture and trusted control plane. This includes enforcing least-privilege access, providing guardrails on autonomous actions, enabling auditability across agent decisions and integrating with zero-trust-aligned authentication and authorization frameworks. This governance layer ensures agents remain both operationally effective and tightly bounded, allowing organizations to adopt agentic AI with confidence—even in high stakes or contested mission environments.

Together, these advancements demonstrate how secure, mission-aligned agentic AI can transform defensive cyber operations—delivering precise, rapid and reliably governed autonomy at enterprise scale.

BIO: Isaiah Akers is a senior cloud computing application architect with Booz Allen.

From Snapshot to Signal: Governed Agentic AI for Continuous ATO

Bobby Tuohy, VP, Product and Platform Strategy, Cav AI • bobby.tuohy@cavhq.ai

ABSTRACT

The U.S. Department of War is in the midst of the most significant platform modernization cycle in a generation. Programs across the services are racing to field autonomous systems, attritable platforms and AI-enabled capabilities at unprecedented speed. The defense industrial base is scaling rapidly to meet this demand, with new entrants and commercial technology companies accelerating delivery timelines that traditional defense programs measured in decades.

But there is a bottleneck no one is talking about: every one of these systems must receive an authority to operate before it can be deployed. And the ATO process has not kept pace with the speed at which systems are now being built.

The problem compounds further as these modernized platforms increasingly rely on open-source software, third-party AI libraries and commercial components. Each dependency introduces supply chain risk that must be evaluated against RMF controls, yet the current compliance model has no mechanism to continuously assess third-party risk at the speed these components evolve.

Vulnerabilities appear daily. Dependencies update weekly. The compliance picture remains static.

The consequences are not just operational delays. When authorizing officials cannot see the current security posture of a system because the evidence is months old and manually assembled, they face an impossible choice: slow the mission by withholding authorization or accept risk they cannot fully quantify. In practice, AOs are routinely forced to accept unnecessary or even unknown risk, not because the underlying system is insecure, but because the compliance process cannot give them the visibility they need to make an informed decision.

This session examines a fundamentally different model: continuously computing compliance posture from live operational data using a governed agentic AI architecture. We will walk through how a deterministic integration layer can ingest raw security telemetry, resolve it into canonical entities and emit structured compliance evidence without manual intervention, and how an agentic layer above it can evaluate system state, identify control gaps and propose compliance claims that human operators review and approve before they take effect.

This is not a theoretical framework. I will share production outcomes from federal deployments where this approach reduced ATO timelines by 75–96%, including environments spanning NIPR, SIPR and JWICS. We will address the governance challenge that DISA has rightly raised around agentic AI: how to ensure least-privilege access, auditability and accountability when autonomous systems reason about compliance in high-stakes operational environments.

I hope attendees will take away three things: an understanding of how entity-claim data models enable traceable, machine-verifiable compliance findings; a practical framework for integrating governed AI agents into existing RMF and eMASS workflows; and a clear picture of what continuous ATO looks like when compliance infrastructure moves at the speed of platform delivery, not the speed of paperwork.

BIO: Bobby Tuohy is vice president of product and platform strategy at Cav, an AI-powered cyber compliance platform serving U.S. defense agencies and critical infrastructure, and founder of Blackthorn Strategies, an engineering and product firm focused on RF, electronic warfare and AI-enabled systems. He previously led product at Flashpoint, a global threat intelligence company, and founded the supply chain venture studio at 25madison. A decorated U.S. Navy veteran with tours across signals intelligence and special operations, Tuohy holds an MBA and master's degree in engineering from Harvard and a bachelor's degree from the United States Naval Academy.

Automated Authority to Operate (ATO)

Opportunity Statement: The traditional ATO process is slow and labor intensive. DISA is looking for technologies that will assist in automating both the package creation and package review process. Any solutions must integrate with existing tools, like eMASS, and the RMF process.

Why this is Important: DISA is continually working to accelerate solution delivery to warfighters while staying ahead of an increasingly complex cyber landscape. To meet that, we need to reduce compliance bottlenecks while maintaining cybersecurity rigor.

AI-Native Solutions To Expedite Authorization Processes, Utilizing Latest Developments in Technology With No Sacrifices to Security

William Liu, Co-Founder and CTO, Ironmist ·
will@ironmist.co

ABSTRACT

Problem: Defense software teams spend months on compliance rework for findings that could have been caught during development. Authorizing officials' (AO) teams chase manual evidence, perform redundant assessments and wade through incomplete artifact packages, stretching ATO cycles to 18-plus months at more than $1 million per system. As a consequence, mission owners receive outdated software and operate below their potential.

Solution: Ironmist is a continuous compliance platform that replaces manual, document-based ATO processes with automated compliance assessment and evidence generation built directly into the software delivery pipeline. Unlike traditional compliance tools that treat authorization as a separate, periodic activity, Ironmist embeds security controls from the first line of code through continuous monitoring as code changes, automatically producing the machine-verified evidence that AOs and assessment teams need without slowing delivery.

BIO: William Liu is the co-founder of Ironmist, a continuous authorization platform that replaces manual ATO processes by embedding compliance directly into the software delivery pipeline, compressing more than 18-month authorization cycles to weeks so secure, mission-ready software reaches the warfighter faster. Liu has deep experience building software products under demanding regulatory and performance constraints, from regulated fintech to large-scale consumer platforms. His conviction: security and speed are not a trade-off. Previously the co-founder and CTO of Sanlo, Liu has shipped products across PlayStation and Electronic Arts and has scaled engineering teams through two successful exits: Playfish and Earnest.

From Compliance Bottleneck to Continuous Readiness: AI-Driven ATO Automation With Integrated Risk, Security and CORA Dashboards

Tom Bean, Advisory Solution Consultant, Risk, ServiceNow •
tom.bean@servicenow.com

ABSTRACT

The traditional ATO process was built for a slower era. Manual workflows, fragmented tools and point-in-time assessments consume months of mission time while risk accumulates in the gaps between reviews. For most organizations, cybersecurity compliance runs as a separate discipline, disconnected from the enterprise IT systems, workflows and data that actually reflect real risk posture. The result is an artifact-dependent process that lags reality by design.

For U.S. Department of Defense organizations operating under persistent threat, that lag is unacceptable. Compliance latency is operational risk.

ServiceNow transforms ATO from a periodic administrative burden into a continuous, AI-accelerated mission capability. It does this from within the enterprise, embedding cyber risk management directly into the same platform that manages IT operations, service delivery and infrastructure. Authorization evidence is generated by live operational data, not assembled after the fact.

When cybersecurity is integrated into the enterprise IT fabric, continuous authorization becomes achievable. AI continuously aggregates live operational data, tracks control status across the environment and surfaces emerging risk, collapsing review cycles and enabling authorizing officials to make faster, better-informed decisions. ATO becomes a state of continuous preparedness, not a finish line that organizations cross and then fall behind.

Commanders, ISSMs and authorizing officials operate from real-time dashboards that translate live enterprise data into actionable risk intelligence. Because the platform connects to the systems that run the organization, not periodic artifact submissions, the risk picture is current, not historical. Leadership sees a consolidated boundary-level view of posture scored against CORA readiness and JFHQ-DODIN priorities. When conditions change, the platform surfaces what is at risk and where to act first.

ServiceNow accelerates the process you already have, from inside your own enterprise. AI handles evidence aggregation, gap analysis and remediation prioritization, freeing cybersecurity professionals to focus on mission-critical decisions rather than administrative overhead. Bringing cyber automation into your enterprise

IT environment eliminates the handoffs, translation layers and time delays that make traditional compliance unsustainable at operational tempo.

Integrated with eMASS, ACAS, STIG tooling, CMDB and ITSM, ServiceNow serves as the AI orchestration layer that connects cyber risk management to the living enterprise. Existing investments are amplified. Evidence is derived from operational reality. Authorization posture reflects the environment as it actually exists, continuously.

Attendees will leave with a clear picture of how embedding AI-driven cyber automation within the enterprise shifts cyber readiness from a compliance exercise to a persistent operational advantage, enabling faster capability delivery and a stronger defensive posture across the DODIN.

BIO: Tom Bean is a risk management solution consultant at ServiceNow with a strong track record in enterprise software sales. He specializes in governance, risk and compliance (GRC), covering risk management, policy, compliance and audit solutions. Bean brings a background in data management and federal policy that has fueled consistent sales performance, including a 300% quota attainment that earned him top 1% recognition and multiple industry awards. He is known for crafting compelling narratives and uncovering data-driven insights that demonstrate clear value to customers. Collaborative by nature, Bean blends creativity and analytics to deliver results that resonate across technical and executive audiences. He is currently focused on exploring AI-driven innovation in the GRC space.

Delivering Continuous ATO With Security Control Management

Kendall Moore, Co-Founder and CTO, Sicura • kendall@sicura.us

ABSTRACT

To counter fast-moving adversaries, security controls for mission-critical IT infrastructure must be continuously adapted to changes in the threat landscape, technology and user actions. The federal government has traditionally relied on authority to operate (ATO) to keep pace with change; however, the process to obtain certification is often slowed by siloing between tools, fragmentation between security and DevOps teams, and overreliance on manual workarounds to navigate the space between them. As teams navigate these challenges, the warfighter waits for delivery. Adding further challenges, systems often fall out of date in the three years between ATO exercises, increasing the risk of vulnerabilities and leaving warfighters unable to access the latest technology.

Security control management (SCM) provides a paradigm shift. By providing end-to-end compliance automation and integrating with key security and agile workflows, SCM transforms ATO certification from a static compliance exercise into a continuous cycle of enforcement, where the RMF becomes an agile workflow that delivers for the warfighter at the pace of the mission.

DevOps engineer Kendall Moore lived these challenges while obtaining ATO for complex infrastructure at NSA and supporting key intelligence community contracts. These experiences led him to become the co-founder of Sicura, a platform purpose-built to deliver SCM in highly secure environments.

In this talk, Moore will detail his lived experience navigating the back-and-forth between security and engineering teams that slowed down the ATO process and the real-world consequences that slowed down delivery when mission engineers were prevented from working until ATO was complete.

Moore will also break down how SCM delivers continuous ATO (cATO). Moore will cover key pillars of SCM and how these automate steps of the RMF. These include customizable security policies that map ATO requirements with specific system attributes, artifact delivery that integrates with DevOps workflows and existing GRC tools such as eMASS, automated remediation, continuous monitoring and flexible deployment across hybrid and air-gapped environments. Additionally, Moore will provide examples and outcomes from real use cases of cATO deployment, including with U.S. Army DevCom.

Attendees will leave this talk with perspective on how cATO can accelerate certification timelines from months and years to days and weeks, while reallocating engineering labor toward mission-critical problem-solving. Moreover, they will have a framework to reset expectations for compliance as a process that hardens infrastructure every day, not only during certification exercises.

BIO: Kendall Moore is the CTO and co-founder of Sicura, a platform providing security control management for mission-critical IT infrastructure. Moore specializes in translating compliance policies into effective workflows, product and engineering leadership, and continuous delivery. As a DevOps engineer at NSA, Kendall's experience with slow and static authorization-to-operate processes led him to co-create a platform to automate compliance. That platform became Sicura, and today Moore leads the product, engineering and technical delivery of the platform. Previously, he served as a senior DevOps consultant at Onyx Point Inc. Moore obtained a master's degree in bioinformatics from the University at Buffalo and a bachelor's degree in computer science from the State University of New York at Oswego.

Cryptographic Discovery as an ATO Accelerant: Operationalizing ACDI Tooling and PQC Road Maps for DOW System Owners

Aaron Faulkner, Co-Founder, Tychon • aaron.faulkner@tychon.io

ABSTRACT

The U.S. Department of War's (DOW) ATO process increasingly demands evidence of cryptographic hygiene, yet most system owners lack systematic visibility into where classical cryptography lives in their environments, what CNSA 2.0 compliance requires of them or what a credible post-quantum cryptography (PQC) transition will cost.

Drawing on direct operational experience deploying automated cryptography discovery and inventory (ACDI) tooling across U.S. Army programs worldwide, this session delivers a practitioner's guide to integrating cryptographic discovery into the ATO life cycle. Topics include standing up ACDI tools in operational DOW environments, translating discovery outputs into eMASS plan of action and milestones (POA&M) entries aligned to FIPS 203/204/205 and CNSA 2.0, building system-level PQC cost estimates for program leadership and structuring a PQC transition road map that integrates with existing risk management framework processes.

Attendees will leave with an operational playbook grounded in real Army engagements, for using cryptography discovery as an ATO accelerant rather than a compliance burden and for giving system owners the data they need to brief, resource and execute the transition to PQC.

BIO: Aaron Faulkner is an ICIT fellow and co-founder of Tychon, a platform focused on automated cryptography discovery, inventory and post-quantum readiness. He works with government and private-sector organizations to help them understand and manage cryptographic risk as they prepare for the transition to quantum-resistant security. Previously, Faulkner served as cyber practice lead at Accenture Federal Services, where he was responsible for cybersecurity strategy and delivery across major federal missions and for launching the firm's first global post-quantum cryptography business unit.

Combating Compliance Drift: Automating Continuous Enforcement With Ansible

George Nalen, Manager, Automation and Engineering, Tyto Athene •
george.nalen@gotyto.com

ABSTRACT

Even after achieving an authority to operate (ATO), systems begin to drift from their approved security baseline almost immediately. Configuration changes, patching, and operational demands introduce inconsistencies that are difficult to track and even harder to correct using manual processes.

This session focuses on how to combat compliance drift by automating continuous enforcement of security controls using off-the-shelf tools like Ansible and the Ansible Lockdown project. George Nalen will demonstrate how to implement compliance as code, continuously validate system configurations and remediate drift in real time.

Attendees will learn practical approaches to maintaining alignment with STIGs and security baselines, reducing audit friction and supporting ongoing authorization efforts in zero-trust environments.

BIO: George Nalen is a long-time technologist and automation advocate with more than two decades of experience across the IT spectrum. From early days in tech support and Linux administration to leading teams and designing enterprise automation strategies, he has seen firsthand how complex—and often manual—compliance processes can become. Since 2019, Nalen has led the Ansible Lockdown project, focusing on turning compliance into something repeatable, scalable and actually usable by engineering teams. His work centers on using off-the-shelf tools like Ansible to bring security and operations closer together without adding unnecessary complexity.

Automated Authority To Operate (ATO)

Greg McCullough, Vice President, Booz Allen Hamilton • mccullough_greg@bah.com

ABSTRACT

Attackers now operate at the speed of AI. Every vulnerability and every device provides even the most basic adversary with a point of entry into networks to disrupt operations or steal intellectual property. As cyber defense and IT operations teams work to incorporate AI to close those gaps more quickly, it's critical that they take control of their networks and everything on them. AI-enabled continuous compliance now makes it possible to manage and secure environments more effectively than ever before. Booz Allen's Vellox Navigator™ provides AI-assisted controls implementation, near real-time controls assessment support and detailed risk mitigation assistance to autonomously interpret and control enterprise compliance in real time.

BIO: Greg McCullough is a Booz Allen vice president leading the transformation of the cyber compliance business.

Zero Trust in Contested and Disconnected Environments

Opportunity Statement: How can industry enable scalable, policy-driven zero-trust enforcement across classified and unclassified networks when operating in denied, degraded, intermittent or limited (DDIL) environments?

Why this is Important: DISA is responsible for securing the U.S. Department of War Information Network (DOWIN). As cyber threats from peer adversaries increase, centralized trust models break down in contested environments. DISA needs:

- Distributed identity and access control
- Edge-based policy enforcement
- Continuous authentication without constant cloud reachback

This directly supports resilient command and control (C2) and joint all-domain operations.

Securing Federal Defense: Check Point's AI-Powered Alignment With DOD Zero-Trust Architecture

Joe Ford, SE Manager Federal, Check Point Software Technologies •
joeford@checkpoint.com

ABSTRACT

The U.S. Department of Defense's June 2024 Zero Trust Overlays establishes a comprehensive road map for federal agencies to achieve zero-trust maturity by fiscal year 2027. This session demonstrates how Check Point Software Technologies' Infinity Platform delivers AI-powered security capabilities directly aligned with all seven DOD zero-trust pillars: user; device; applications and workloads; data; network and environment; automation and orchestration; and visibility and analytics.

Discover how Check Point's ThreatCloud AI powers more than 2 billion daily security decisions with 99.8% malware block rates. Quantum-safe encryption protects against future threats, and Infinity AI Copilot automates incident response. Federal security professionals will learn practical implementation strategies for accelerating zero-trust adoption, reducing complexity and achieving measurable cybersecurity outcomes that protect critical defense assets while simplifying operations across multicloud environments.

BIO: Joe Ford is a technical professional with more than 30 years of experience in selling IT and security solutions to U.S. government agencies and Fortune 500 companies, with expertise in infrastructure, security, backup, virtualization, wireless, storage and business systems across public and private sectors. He demonstrates strong leadership and collaboration skills, successfully guiding technology implementations and achieving FedRAMP authorization for a government security platform. Ford focuses on driving ROI and sustainable growth by reducing operational costs, forming strategic alliances and leading teams to deliver complex solutions efficiently. He is a top performer with deep knowledge of technology and security landscapes, adept at complex enterprise sales and communicating effectively with high-level executives. Ford consistently exceeds sales targets and engages in public speaking, social media and thought leadership to build influential industry relationships.

Implementing DOD Data-Tagging and Classification for IL-6 Environments

Greg Colla, Chief Technical Officer, Janusnet • greg.colla@janusnet.com

ABSTRACT

As the U.S. Department of Defense accelerates adoption of data-centric security and zero-trust architectures, precise data-tagging and classification have become foundational to protecting national security information.

This session examines the practical implementation of manual data-tagging at the enterprise endpoint to meet DOD requirements for handling classified and controlled information within Impact Level 6 (IL-6) environments.

Attendees will gain actionable insight into applying DODM 5200.01, Volume 2, which governs information classification and marking to ensure consistent, compliant handling of data across classified domains. The session also clarifies the role of DOD minimum essential metadata (MEM)—the mandated set of metadata elements that enables secure data discovery, sharing and access control across DOD systems.

Using real-world examples, the discussion demonstrates how effective metadata tagging and classification markings improve interoperability, mission assurance, auditability and operational resilience across both connected and air-gapped IL-6 environments.

Designed for cybersecurity professionals, system architects and program managers, this session provides a clear framework for aligning endpoint tagging solutions with DOD classification and metadata requirements, enabling trusted collaboration while strengthening data protection across defense networks.

BIO: Greg Colla is the chief technology officer at Janusnet, where he leads the development of secure, compliant information-sharing platforms for government, defense and enterprise organizations. His work focuses on turning complex security and compliance requirements into practical, mission-ready solutions that enable trusted communication across email, documents and enterprise systems in high-consequence environments.

Zero Trust at the Tactical Edge: Enforcing Policy in Contested and Disconnected Battlespaces

David Herbst, Director of Solutions – Federal, Mattermost •
david.herbst@mattermost.com

ABSTRACT

Joint and coalition forces are increasingly forced to fight through denied, degraded, intermittent and limited (DDIL) environments where traditional, centralized trust models cannot keep pace with peer adversaries. Zero-trust principles offer a path forward but only if identity, access control and policy enforcement can operate at the edge—across classified and unclassified networks—without assuming reliable cloud reachback or pristine transport. In this context, the question is not whether to adopt zero trust but how to implement it in a way that survives jamming, disruption and isolation while still protecting critical data and mission systems.

This session will explore how industry can support DISA and the broader DOD in advancing distributed identity, edge-based policy enforcement and continuous authentication in contested environments. From a Mattermost perspective, the discussion will focus on what it takes to push decision-making and enforcement closer to the tactical user, synchronize policy across echelons and domains, and maintain resilient command and control and joint all-domain operations even when links are unstable or partially severed. The objective is to outline practical design and governance principles that help commanders and cyber defenders treat zero trust not as a centralized service but as a distributed warfighting capability that can endure in the realities of modern conflict.

BIO: David Herbst is a federal sales engineer at Mattermost, recognized as an AI/ML innovator and a strategic leader in federal and defense technology. With more than 15 years of experience, Herbst has driven high-stakes technology operations in some of the most secure environments, spearheading complex cloud migrations and orchestrating large-scale infrastructure initiatives with flawless execution. He is known for applying advanced AI/ML approaches—such as natural language processing and multimodal data fusion—to solve the nation's toughest security challenges and deliver transformative mission results. Herbst's track record spans winning and executing multimillion-dollar federal contracts, which combines his deep technical expertise with strategic business insight to accelerate growth and ensure mission success. Prior to his role at Mattermost, Herbst held key positions at leading companies, including Virtualitics, Primer.ai, Rebellion Defense, Descartes Labs and Exeter Government Services, where he continu-

ously led technical programs and solutions architecture across federal agencies and defense organizations. His skills include ETL, data analysis, artificial intelligence, machine learning and executive-level technology leadership. Herbst holds a bachelor's degree in defense systems management with a concentration in acquisition program management from Defense Acquisition University and has formal training in electronic systems technology from Air University, U.S. Air Force Institute of Technology.

Jarzombek has more than 30 years focused on software security, safety and quality in embedded and networked systems and enterprise IT. He is a Certified Secure Software Lifecycle Professional (CSSLP) and project management professional with an MS in computer information systems, a BA in computer science and a BBA in data processing and analysis.

Built for Disruption: Zero Trust in Contested and Disconnected Operations

Chris Betz, Federal CTO, Omnissa • betzc@omnissa.com

ABSTRACT

Zero-trust strategies are often designed around persistent connectivity, assuming continuous access to centralized policy engines, cloud control planes and real-time data exchange. Military and government operations rarely have that advantage. In contested, degraded or fully disconnected environments, those assumptions break down, creating gaps in enforcement, visibility and control at the exact moment they are needed most.

This session focuses on how zero trust must be implemented to operate through disruption, not around it. When connectivity is limited or unavailable, security decisions cannot rely on constant reach back to centralized infrastructure. Instead, trust must be continuously evaluated and enforced locally using device posture, identity context and session state—ensuring security controls remain intact at the tactical edge.

Omnissa will outline a practical, operational approach to extending zero trust into these environments by embedding policy enforcement directly into endpoints, access workflows and controlled execution environments. This allows DOD components to maintain least-privilege access, reduce credential exposure and limit lateral movement—even when operating offline. When connectivity is restored, telemetry and policy state are synchronized to support auditability, compliance and broader situational awareness.

Attendees will learn how to:

- Shift enforcement from network-dependent controls to device, identity and session-based decision points.
- Maintain policy-driven access and compliance posture during intermittent or disconnected operations.
- Reduce reliance on static credentials and centralized infrastructure in contested environments.
- Preserve mission continuity and security assurance without requiring persistent connectivity.

This session reframes zero trust as an operational capability built for the realities of modern defense, designed to function in denied, degraded, intermittent and limited (DDIL) environments, while delivering a cloud-operating model across on-prem and fully disconnected deployments.

BIO: Chris Betz is the chief technology officer for Omnissa Federal, where he works closely with government customers, executive leadership, product teams and field organizations to align technology strategy with mission outcomes. With more than 30 years of experience across the IT spectrum, Betz brings a practitioner's perspective shaped by roles spanning help-desk

support, systems administration, engineering, architecture and executive leadership. Betz began his career serving eight years in the U.S. Army as a signal support systems specialist, where he built the technical foundation that launched his career in IT. That experience continues to influence his focus on resilient, mission-ready systems designed to operate in contested, degraded and disconnected environments. Throughout his career, Betz has remained focused on customer success, helping organizations modernize IT, improve digital employee experience and strengthen enterprise security. He brings deep expertise across the Omnissa platform, including unified endpoint management, identity and access, automation and Horizon virtual desktop infrastructure, developed through years of hands-on work with enterprise and federal customers. In his current role, Betz leads technology strategy for Omnissa's federal business, helping agencies deploy secure, scalable solutions that balance flexibility with control while supporting evolving zero trust and compliance requirements.

Splunk as a Service: Zero-Trust Monitoring for Classified and Disconnected Mission Environments

Kevin Dorsey, Director, Federal Solutions Development, Optiv + ClearShark •
kdorsey@clearsharkinc.com

ABSTRACT

Learn how Optiv + ClearShark has radically changed how the U.S. Department of War (DOW) and intelligence community can solve the ever-expanding data challenges. Through an exclusive partnership between Splunk, AWS and Optiv + ClearShark, organizations in our nation's most sensitive mission environments now have access to a proven solution set and a disruptive procurement method enabling the quickest on-ramp to achieving complete zero-trust monitoring. Optiv + ClearShark's flexible services model addresses both the technical and operational dimensions of zero trust at the edge: pre-engineered deployment architectures reduce time-to-mission readiness, while SLO-bound engineering support and advanced support services ensure sustained operations so mission owners can focus on outcomes rather than infrastructure. Learn how SPLaaS is enabling the fastest on-ramp to zero-trust compliance monitoring in the nation's most sensitive environments.

BIO: Kevin Dorsey is an accomplished SIEM engineer building the future of Splunk Enterprise in the DOW/intelligence community space.

Dominate the Digital Disconnected Edge With Zero Trust and Identity Security

Andrew Whelchel, Lead Solutions Engineering – Federal, Saviynt •
andrew.whelchel@saviynt.com

ABSTRACT

Deploying modern zero trust demands more than just MFA and microsegmentation to meet today's mission at the disconnected edge. Zero trust for accelerating the mission becomes an even greater challenge in a contested and disconnected environment, where the tyranny of distance (or just disconnection) stretches normally resilient systems to their limits. Identity security, when enabled with artificial intelligence (AI), enables scalable zero-trust authorization access for users and non-person entities (NPEs) across connected and DDIL environments down to OT endpoints.

By delivering zero trust via AI-enabled identity security for command and control (C2) and joint all-domain operations missions, organizations gain benefits as they leverage identity security to enable missions and defend against cyber threats across disconnected and DDIL environments. These organizations reap mission benefits from device and user trust validation at the edge, mitigating contested security risks and ensuring mission continuity. These benefits result from using identity security with AI in the DDIL environment, enabling accelerated risk reduction and executing a compressed time to enforcement for zero-trust policies.

Delivering zero-trust at-the-edge outcomes requires an identity security solution with an AI platform that is ready to deploy at the edge, can extend to edge OT endpoints and operate using a rapidly deployable ICAM platform. When deployed with these key elements, they gain several capabilities, including:

- Enable distributed identity access using DDIL-enabled ICAM with AI-enabled identity security.
- Establish data and attribute-based edge policy enforcement for C2 and joint all-domain operation mission applications.
- Provide continuous authentication service with strong MFA (using CAC where available) to sustain the mission while connected and disconnected.
- Assure auditability and deferred synchronization during disconnected state, as mission networks adapt and ensure safety and security before reconnection.

To ensure the mission at the edge's needs are met, identity security with AI must be delivered as an ICAM solution down to the person, NPE risk reduction and OT edge cyber protection. When integrated and optimized, these elements will improve the speed of action for onboarding mission personnel and non-person entities and ensure data-centric protection of mission partner resources. These outcomes will be in addition to providing operational capability to ensure audit compliance, even when disconnected, and information assurance before connecting to the enterprise network. As part of this session, attendees will learn about key capabilities, including accelerated identity security-based onboarding in a disconnected environment, managing data-centric edge policy enforcement, providing continuous authentication services with MFA when disconnected and assuring audit requirements in any environment, connected or not.

BIO: Andrew Whelchel (CISSP-ISSAP, ISSEP, CAP, CCSP, CSSLP) started in information security and IAM immediately after graduating from the University of Memphis, supporting identity and access management and managing Microsoft Identity for U.S. federal customers. Later, the role transitioned to network infrastructure security and then to consumer identity protection at RSA Security and, most recently, at Okta and Saviynt. At RSA Security, supporting financial services, health care, U.S. federal and other customers, the focus was on identity risk analytics and integration of identity fraud intelligence for cyber crime prevention. In prior roles at Okta and current roles at Saviynt, the focus is on protecting employees' and business partners' identities for public-sector agencies to reduce cyber risk and accelerate cloud transformation capabilities. Contributions include serving as a contributor on the NIST 1800-3 ABAC (attribute-based access control) standard and speaking engagements on identity access management and security. Currently, studies are at Augusta University in pursuit of the master of arts degree in intelligence and security studies.

Top 5 Best Practices for Achieving Target Zero Trust at the Edge

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies •
gina.scinta@thalestct.com

ABSTRACT

As mission systems increasingly extend beyond centralized data centers to the tactical edge, achieving target-level zero trust becomes increasingly complex. Edge environments—ranging from forward-deployed units to IoT-enabled platforms and disconnected or intermittently connected systems—introduce unique constraints around latency, bandwidth and physical security. These conditions demand that zero-trust principles be enforced as close to the point of data generation and decision-making as possible. Agencies must extend the same protections used in the core and cloud to the tactical edge to enable identity verification, continuous monitoring and policy enforcement.

Attend this session to learn about the best practices for achieving target-level zero trust at the edge. The speaker will outline the top five tips for developing a repeatable framework to accelerate adoption.

BIO: Gina Scinta is Thales TCT's deputy chief technology officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission-critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC and more. Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world-class encryption and key management for data at rest in data centers and cloud infrastructures.

Zero Trust in Contested and Disconnected Environments

Bob Agans, Project Manager – Multi-Partner Environments, Booz Allen Hamilton. •
agans_bob@bah.com

ABSTRACT

As U.S. forces encounter intensifying cyber pressure from peer adversaries, the limitations of perimeter-centric security architectures become stark—especially when warfighters must operate with denied, degraded, intermittent or limited (DDIL) connectivity. Operators need to be able to securely send data back to other stakeholders, obfuscate data in transit to protect against data-sniffing attacks and have a local chat capability. This requires a nontraditional solution that delivers the flexibility and speed required for forward operations. Here is the good news: advancements in distributed enforcement demonstrated with advanced zero-trust (ZT) technology show how integrated microsegmentation, application-aware security, defensive cyber operations and conditional access can be deployed across multiple enclaves, enabling mobility and resilience in forward environments. Complementary tactical innovations—such as modular ZT kits that collapse multiple security tools into a unified transport agnostic platform—provide autonomous microsegmentation and failover necessary for mission continuity when disconnected. These developments emphasize the need for data-centric security, where protections travel with the data itself to enforce access, context and sensitivity constraints regardless of network state or transport. The outcome is a ZT posture purpose-built for contested operations—one that protects command and control, ensures coalition and mission partner interoperability and sustains secure data access across joint all-domain operations even when the network fights back.

BIO: Bob Agans is a Booz Allen project manager for multi-partner environment efforts supporting DISA.

Senior Solutions Architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world class encryption and key management for data at rest in data centers and cloud infrastructures.

WHAT IS AFCEA?

AFCEA is a member-based, nonprofit association for professionals that provides highly sought-after thought leadership, engagement and networking opportunities. We focus on cyber, command, control, communications, computers and intelligence to address national and international security challenges. The association has more than 30,000 individual members, 138 chapters and 1,600 corporate members. For more information, visit afcea.org.