

TechNetCyber

INNOVATION SHOWCASE 2025

MAY 6-8, 2025 | BALTIMORE CONVENTION CENTER, BALTIMORE, MARYLAND



SIGNAL
AFCEA INTERNATIONAL MEDIA

2025 TechNet Cyber Innovation Showcase

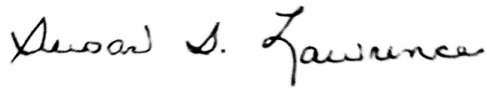
Focus on The Cyber Edge

We know all too well that cyber enhances situational awareness and allows more informed planning and decision-making. As I write in my President's Commentary in the May issue of *SIGNAL* Magazine, in addition, offensive cyber operations disrupt enemy command, control, communications, intelligence, surveillance, reconnaissance and logistics, effectively hindering an enemy's ability to coordinate and execute missions.

Fortunately, the U.S. government recognizes the challenge, as do many of our industry partners working hard every day to devise the solutions to safeguard the digital domain.

At TechNet Cyber, and in the pages of this compendium, AFCEA International continues to do our part in helping find solutions for warfighters at the tactical edge and across the department, as well as for first responders, homeland security personnel and the intelligence community. And we help give voice to the industry partners through the event's *SIGNAL* Innovation Showcase to highlight their proposed solutions to identify the threats, challenges and the technology gaps facing our national security and defense community—and ultimately, find the right cyber solutions to execute their missions successfully.

Best wishes,

A handwritten signature in black ink that reads "Susan S. Lawrence". The signature is written in a cursive, flowing style.

Lt. Gen. Susan S. Lawrence, USA (Ret.)

President and CEO
AFCEA International

Table of Contents

UNIFYING OPERATIONS

An AI Application's Journey to Production: Software Supply Chain Fundamentals Connor Wynveen, Solutions Engineer, Chainguard	9
AI Enabled Cypher Security Steven Matherne, Area Vice President, Defense & Heath, AT&T Government Solutions	10
Unifying Operations: A Common Operational View for DISA Using Ciena's Blue Planet Peter Briscoe VP, Head of Pre-Sales Blue Planet, Ciena	11
Utilizing AI to Unlock Data Essential to Mission Success Marlin McFate, Public Sector CTO/CISO, Cohesity.....	12
Empowering the Warfighter with Modernized AI and Data Centric Security for Any Agency Hybrid Multi-Cloud Environment Including Multi-Domain Operations Jim Cosby, Chief Technology Officer, NetApp	13
Operator X: Transforming Cyber Defense with GenAI Nate Delgado Software Product Owner, Sealing Technologies	14
Intersection of Quantum, AI and Security Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies.....	15
Securing AI for National Defense: Mitigating Risks with the OWASP LLM Top Ten Bill Church, Chief Technology Officer, F5.....	16
Using AI to Enhance Service Delivery and CX in the DoD 4th Estate: How DISA Leverages ServiceNow Telecom Service Management Shadeh Ardani, Senior Solution Sales Executive, ServiceNow.....	17
Platform AI Capabilities to Enhance Security and Unify Security Operations Scott Havlak, Advisory Solution Consultant, Security Operations, ServiceNow	19
Delivering Improved Enterprise Services with a Unified AI-Powered Platform Approach Jeremy Westerwiller, Senior Solutions Consultant, ServiceNow.....	21

MANEUVER THE DOMAIN

Revolutionizing Cyber Hunt Operations at the Edge With Portable, High-Performance Solution

Richard “Trey” Howard, Senior Software Engineer, Omni Federal 24

RAVID (Randomized Automated Virtual Infrastructure Defense)—An End-to-end Automated, Stealth, Moving Target Defense Architecture

Harris Nussbaum, Cybersecurity Expert, Tyto Athene, LLC 26

Pre-Emptive Threat Intelligence: Disrupting Adversary Operations Before They Strike

Noah Plotkin, Solutions Engineer, Silent Push 28

Unlock the Threat: Apply Storyboarding to the Cyber Arena

Aaron Boteler, Chief Technology Officer & Principal Engineer, CloudCurrent LLC 29

Advanced Cyber Deception—The Future of Cyber Defense

Sreenivas Gukal, Ph.D., Chief Product Officer, Acalvio Technologies..... 31

ZeroLens: Enhancing Cyber Deception and Threat Intelligence for Dynamic Network Defense

Terry Dunlap, Senior VP, Corporate Strategy & Development, NetRise 33

Maneuvering the Domain: Deception-Enhanced Endpoint Defense for the Federal Enterprise

Rick Friend, Manager, Cybersecurity Solutions & Architecture

Brian Recore, Cybersecurity Solutions Engineer, Merlin Cyber 35

DEVSECOPS TRANSFORMATION

A Structured Approach to DevSecOps Transformation

Andrew Scherer, IT Transformation Solution Sales Manager, Federal, ServiceNow 38

Accelerating DevSecOps: Consolidated Machine Identity Security and Code Signing

James Imanian, Senior Director, U.S. Federal Technology Office, CyberArk Software 40

DevSecOps Transformation

Manisha Morris, President & CEO, MSM Technology, LLC 41

DevSecOps—Operationalized

Rich Streeter, Operations Director, Sertainty Federal Systems..... 44

DevSecOps Transformation

Joe Jarzombek, CSSLP, Cybersecurity Solutions Program Manager, Acquired Data Solutions . 46

DevSecOps: A Foundation for Consistency, Speed and Security

Cory Blankenship, Senior Security Engineer, GuidePoint Security 48

Building a Resilient DevSecOps Framework for DISA and the DoD

Zach Bennefield, Federal Security Strategist, Tenable 49

UNDEFINED

The Hidden Threat: Managing Third-Party and Machine (Non-Human) Identities in a Zero-Trust World

Frank Briguglio, Federal CTO and Global Public Sector Strategist, Sailpoint. 52

The Evolving Digital Battlefield: Counter State-Backed Cyber Operations in the Cloud Era

Jeff Worthington, Public Sector Executive Strategist, CrowdStrike..... 54

How Proactive IT With DEX Tools Help Improve Employee Experience (or Something Close to That)

Bill Musson, Senior Technical Sales Engineer, Nexthink Inc. 55

VDetect

John Eubank, Founder & CEO, 10x National Security 56

Best Practices for Implementing Quantum-Resistant Security

Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies..... 58

Best Practices for Insider Risk Management

Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies..... 59

High Assurance Data Security in the Era of Complex Integration

Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies..... 60

Submissions

UNIFYING OPERATIONS

An AI Application's Journey to Production: Software Supply Chain Fundamentals

Connor Wynveen, Solutions Engineer, Chainguard • connor.wynveen@chainguard.dev

ABSTRACT

Speed and security are often at odds. Early prototype efforts typically prioritize functionality to quickly demonstrate mission value. In an era with unprecedented access to data, data scientists and developers have an incredible ability to build applications that empower analysts and decision makers, support war-gaming simulations and address a plethora of other critical use cases.

Open-source software is ubiquitous, comprising roughly 80% of many application code bases. While these building blocks accelerate time-to-mission value, a significant majority of security vulnerabilities are found within them. This can lead to the misconception that open source is inherently insecure. But what if open-source software isn't fundamentally flawed—instead, the challenge lies in how we integrate and manage it?

This presentation will follow the lifecycle of a notional Retrieval-Augmented Generation (RAG) AI application, demonstrating how a few intentional choices and best practices can mean the difference between an application successfully fielded in production and one that gets trapped in a security risk reduction black hole. We will focus on the following software supply chain security fundamentals:

1. Using minimal, hardened, multi-stage container images: Learn how using minimal and hardened multi-stage container images can reduce known vulnerabilities (CVEs) by 90-99%.
2. Dependency management: Explore current open-source consumption practices, the challenges they bring and the solutions available today to mitigate these risks.
3. Release cadence: Understand why regularly rebuilding your application is a critical capability and how establishing a consistent release cadence can drive both speed and security.

BIO: Connor Wynveen is a solutions engineer at Chainguard, helping public sector organizations strengthen their software supply chain security and DevSecOps practices. With a decade of experience in the public sector, he has worked extensively on secure software delivery, container technology and mission-critical systems.

Previously, as a systems engineer at Booz Allen Hamilton, Wynveen supported a range of space and ground systems, including the Kobayashi Maru software factory. His work focused on managing technical baselines and integrating emerging technologies through digital engineering.

AI Enabled Cypher Security

Steven Matherne, Area Vice President, Defense & Health, AT&T Government Solutions •

sm2693@att.com

ABSTRACT

Mr. Matherne will describe the AT&T use of and vision for artificial intelligence (AI) technologies. The promise of AI to be the most powerful toolset in generations for expanding knowledge, increasing prosperity and enriching the human experience, must be taken seriously. This emerging technology will be the foundation of the innovation economy leading to reduced operational costs while simultaneously providing a source of enormous power for countries that harness them. AI is fueling competition between governments and companies racing to field it. It is being employed by nation states as non-kinetic applications to pursue their strategic ambitions. In U.S. military parlance, the term “kinetic” refers to missiles or other traditional types of weapon systems that physically engage targets, whereas non-kinetic tools can include cyber, electronic warfare and other means of attack. When these non-kinetic tools are equipped with AI we have a potential strategic game changer. AI is not a single piece of hardware or software, but rather a constellation of technologies that depend on interrelated elements that can be envisioned as a stack. AI requires talent, data, hardware, algorithms, applications and integration.

BIO: Stephen Matherne serves as the AVP - Defense & Health, leading the organization supporting DoD and Department of Veterans Affairs customers. Matherne is responsible for the strategic alignment of AT&T solutions and support organizations with U.S. governmental priorities, as well as thought leadership for internal and customer organizations. In his current role, Matherne leads the AT&T Federal Solutions - Defense & Health organization, supporting all AT&T DOD and Defense customer programs as well as the Department of Veterans Affairs. Matherne joined the company in 2004 and has held numerous technical and leadership positions throughout his time at AT&T.

Prior to assuming his current role, Matherne served as the AVP - Federal Civilian, where he led the organization supporting the Federal Healthcare, Natural Resources and General Government verticals; and previously served as the Chief Architect for the AT&T Government Solutions - Civilian & Intel organization.

Before joining AT&T, Matherne held leadership roles in engineering and product management with Comsat International, Teleglobe and Sprint Corporation. Mr. Matherne holds a Bachelor of Science degree in Electrical Engineering from the University of Virginia and is a graduate of the ACT-IAC Partners Program.

Unifying Operations: A Common Operational View for DISA Using Ciena's Blue Planet

Peter Briscoe VP, Head of Pre-Sales Blue Planet, Ciena • pbriscoe@blueplanet.com

ABSTRACT

The Defense Information Systems Agency (DISA) operates one of the largest network infrastructures in the world supporting critical missions and operations globally. The Department of Defense Information Network (DODIN) is an environment comprised of a collection of multi-layer, multi-vendor devices providing connectivity to the applications and services that ensure mission success for the warfighter and all of those who support them.

Ciena's Blue Planet portfolio offers a comprehensive set of capabilities that provides a "Common Operating Picture" enabling end-to-end visibility across the collection of devices in the DODIN network infrastructure. Blue Planet Inventory can store all end customer services and how they are linked to each piece of infrastructure allowing it to automate the root cause of outage and restoral process. By integrating with DISA's current processes, Blue Planet can aggregate and target operational data sets, allowing for a holistic view of the network. This Common Operating Picture will allow DISA to gain layer-to-layer visibility, tracking the status and performance of various network layers, from physical infrastructure to virtualized services. This enables DISA to proactively identify and address issues, ensuring a seamless user experience for mission success. Including Blue Planet Inventory and Orchestration into DISA's operations, the organization can leverage AI-driven insights and automation to enhance interactions at the helpdesk.

BIO: Peter Briscoe is the VP Global Head of Pre-Sales at Ciena, where he leads a team of more than 40 professionals focused on helping customers achieve transformative automation with software solutions. With more than three decades of experience in software innovation and business development, including leadership roles at Ericsson and Amdocs, Briscoe has a deep understanding of the telecommunications industry and its technical and business challenges. Briscoe has a proven track record of creating and executing product strategies and roadmaps that align with customers' long-term automation objectives, delivering value-added outcomes.

Utilizing AI to Unlock Data Essential to Mission Success

Marlin McFate, Public Sector CTO/CISO, Cohesity • marlin.mcfate@cohesity.com

ABSTRACT

In today's ever-evolving digital landscape, the intersection of AI technologies and cybersecurity is paramount for ensuring robust data research and data resiliency. This session delves into the innovative utilization of AI to augment user data research and forensics capabilities while bolstering cyber defenses.

Key topics include:

- **AI-Powered Data Research:** Explore how AI technologies, utilizing machine learning (ML), large language models (LLM), neural networks and deep learning are harnessed to enhance user data research processes. Understand the nuances of ML applications and the time considerations involved in training models.
- **Cyber Resiliency Foundations:** Discover the pivotal role of cyber resiliency, where protection, response and recovery strategies form the bedrock of defense mechanisms. Learn how AI contributes to cyber resiliency by reducing vulnerabilities and mitigating threats.
- **Innovative Solutions:** Introduce cutting-edge advancements such as neural and GenAI, tailored to address contemporary cybersecurity challenges. Delve into the significance of staying up to date with the latest AI developments, ensuring relevance and efficacy in combating emerging threats.
- **AI-Driven Data Analysis:** Uncover the capabilities of AI models, such as Cohesity Turing and GAIA, in analyzing vast datasets for actionable insights. Witness how these solutions facilitate efficient data retrieval, vectorization and metadata creation, enabling seamless analysis without extensive training requirements.
- **Mitigating Risks:** Explore strategies to reduce AI-related hallucinations, inaccuracies and other drawbacks ensuring the reliability and integrity of findings. Understand the importance of validating AI-generated insights through cohesive methodologies and rigorous scrutiny.

Attendees will gain valuable insights into leveraging AI technologies for comprehensive data research and bolstering cyber resiliency measures. By harnessing the collective power of advanced AI solutions, agencies can navigate the complexities of modern cybersecurity landscapes with confidence and efficacy.

BIO: Marlin McFate is an Army veteran and an experienced technologist focused on mission success. McFate brings more than 20 years of engineering, leadership and technology experience leading long-term technical initiatives. He serves as Public Sector Chief Technology Officer and Chief Information Security Officer for Cohesity. In his current role, he explores emerging technologies and recommends strategies, through research and collaboration with business and technology leaders across the company and public sector organizations. He is a strategic and supportive voice for customers, partners and team members, ensures successful secure solution delivery and advises on the direction of Cohesity's research and development of its AI/ML powered data security and management solutions.

Empowering the Warfighter with Modernized AI and Data Centric Security for Any Agency Hybrid Multi-Cloud Environment Including Multi-Domain Operations

Jim Cosby, Chief Technology Officer, NetApp • cosby@netapp.com

ABSTRACT

Mission and warfighter data is constantly growing for federal agencies and is becoming more challenging to access, store, manage and process in a timely and secure fashion. This challenge requires new methods and technologies to optimize data by reducing the footprint, cost and time to manage. It also requires enhanced security controls against cyber attacks and must remain flexible to share data across multiple coalition partners. Join this session to learn how innovative intelligent data infrastructure can integrate AI security, efficiency and flexibility to enable dominate outcomes for the warfighter environment as well as Multi-Domain Operations (MDO) and Mission Partner Environments (MPE).

BIO: Jim Cosby is currently a CTO at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on Data Management and Storage Security for more than 20 years, including on-premise and hybrid multi-cloud intelligent data infrastructure technologies which include Multi-Domain Operations and Mission Partner Environments. Cosby has a passion for teaming with agencies, customers, partners and colleagues to drive winning outcomes and he thrives on helping customers architect optimal, cost-efficient and secure data management solutions using innovative technology.

Operator X: Transforming Cyber Defense with GenAI

Nate Delgado Software Product Owner, Sealing Technologies •

nathan.delgado@sealingtech.com

ABSTRACT

As nation-state offensive cyber operations increase, the DoD Cyber Mission Forces (CMF) and hunt forward teams face more complex environments and tasks, while being provided less training prior to missions. They often operate in offline environments with limited or no connectivity to the internet, increasing the challenge of completing complex engineering and analysis tasks.

This session covers how large language models (LLMs) and retrieval-augmented generation (RAG) can be used in a generative AI solution designed to enhance the efficiency and effectiveness of the cyber warfighter. The presenter will highlight how AI agents can seamlessly integrate with defense information systems to empower cyber defenders in protecting critical data. Attendees will discover cutting-edge AI technologies that enhance information awareness, enabling both junior and senior cyber defenders to rapidly understand complex mission environments and deliver actionable intelligence to decision-makers.

The presentation will feature SealingTech's current development, Operator X, a groundbreaking generative AI platform purposely built to interact with DoD cyber tools to help cyber defenders stay ahead of adversaries and ensure the resilience of defensive operations. An overview of current and future use cases of generative AI for cyber defense will be provided. Additionally, the session will explore how Operator X can automate tedious, repetitive, time-consuming tasks, allowing cyber operators to focus on mitigating network threats.

Three Learning Objectives:

- Participants will learn the various use cases for Operator X
- Grasp the powerful potential behind an agentic approach to combining LLMs with a RAG pipeline for cyber defense
- Understand how this new capability levels the knowledge playing field between junior and senior operators

BIO: Nate Delgado is a distinguished product leader at the forefront of artificial intelligence and cybersecurity innovation. As software product owner 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 cutting-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 in economics from the University of Southern California (USC).

Intersection of Quantum, AI and Security

Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies •

Mary.Shiflett@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 can use 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 cyberattacks, 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.

Securing AI for National Defense: Mitigating Risks with the OWASP LLM Top Ten

Bill Church, Chief Technology Officer, F5 • b.church@f5.com

ABSTRACT

As the Department of Defense integrates AI into mission-critical operations, securing these workloads is no longer optional—it's imperative. This session explores the OWASP LLM Top Ten, the most pressing security risks facing AI-driven systems and their implications for national security. Attendees will gain insights into real-world adversarial threats, supply chain vulnerabilities and strategies for mitigating risks while maintaining operational effectiveness. Learn how to fortify AI deployments against manipulation, data poisoning and prompt injection attacks to ensure AI remains a force multiplier rather than a liability.

BIO: Bill Church is a Chief Technology Officer for F5 Public Sector, where he has covered federal customers and their unique security needs for more than 15 years. Church has been in the information security space since 1998, both as customer consultant and engineer. He was dropped in the deep end of a dot com website in the early 2000s in the days of Code Red and Nimda and had to learn security the hard way. Church is a firm believer in “know thy enemy and know thy self” you can't effectively secure yourself if you don't understand how the bad guys think.

Using AI to Enhance Service Delivery and CX in the DoD 4th Estate: How DISA Leverages ServiceNow Telecom Service Management

Shadeh Ardani, Senior Solution Sales Executive, ServiceNow •

holly.horton@servicenow.com

ABSTRACT

Join us to learn how ServiceNow is empowering DISA to redefine service delivery and CX- ensuring seamless, efficient and mission-ready operations for the DoD 4th Estate.

Delivering seamless, mission-critical services across the DoD 4th Estate and across the Department of Defense as a whole, requires a customer-centric approach to service management—one that prioritizes cost-reduction, operational efficiency and effective customer experience (CX). However, legacy processes require personnel to “swivel chair” across different systems, screens and applications—as well as depending on specific resources with legacy knowledge. This often adds costs, creates service bottlenecks, fragmented communication and inconsistent support. Finally it degrades mission readiness.

This session explores how ServiceNow’s current deployments with Service Bridge and Telecommunications Service Management (TSM) are transforming service delivery in service of DISA’s mission today. ServiceNow unifies service management across DoD agencies, improves transparency and enables real-time collaboration between service providers and mission partners.

Key topics include:

- **Proactive Service Management for Mission Readiness:** Leveraging AI-driven analytics and predictive insights to prevent service disruptions before they impact operations.
- **Bridging the CX Gap in Service Delivery with AI:** How Service Bridge enhances communication between service providers and end-users, ensuring greater visibility and faster issue resolution.
- **Automating and Standardizing Requests Across the 4th Estate:** Eliminating silos with a unified, automated approach to service requests, reducing wait times and improving response accuracy with service bridge.
- **End-to-End Visibility and Proactive Issue Resolution:** Providing real-time insights into service performance, enabling predictive analytics to prevent outages before they occur.

By modernizing its telecom service management framework, DISA is achieving:

- **Faster Response and Resolution Times:** Automation reduces delays, ensuring mission-critical services remain operational.
- **Improved Service Accuracy and Compliance:** Standardized processes minimize errors and enhance adherence to DoD regulations.
- **Scalability for Future Needs:** A flexible, cloud-based platform that adapts to evolving mission demands and emerging technologies.

BIO: Shadeh Ardani is a Federal ServiceNow solutions specialist based in the Washington, D.C., region as part of ServiceNow's Public Sector division. Ardani has spent her career supporting the DoD and its agencies in the realm of IT and helping them achieve quicker mission outcomes with digital transformations. Currently, Ardani is focused on improving operational challenges and bringing service delivery solutions to the DoD in support of modernizing government systems for all diverse missions.

Platform AI Capabilities to Enhance Security and Unify Security Operations

Scott Havlak, Advisory Solution Consultant, Security Operations, ServiceNow •

holly.horton@servicenow.com

ABSTRACT

ADISA faces critical challenges that most peer-sized organizations are encountering across the public and private sectors: Improving customer interactions, notifying users with timely operationally impacting communication and ensuring customer issues are managed accurately to resolution. However, DISA faces this complex paradigm with a no-fail mission that is nation-critical.

The challenges DISA faces of service delivery, at the Helpdesk level and across customer information systems and workflows, can be optimized through the deployment of an AI platform approach for operational transformation. This nature of deployment has the potential to revolutionize DISA's Security Operations.

Within the context of cyber operations—by leveraging advanced AI capabilities, such as the platform could streamline the detection, management and resolution of security incidents and vulnerabilities. This means that threats can be identified and addressed more efficiently, reducing the risk of breaches and ensuring a more secure environment.

We propose an approach that unifies IT and Security Operations, fostering better collaboration and coordination between teams.

An AI-first integrated platform approach delivers capabilities that enhance DISA's overall security posture and operational efficiency in several important ways:

1. **The power of the platform:** Operationalizing service delivery on a single enterprise-grade platform. that unites AI, data and workflows builds scale, trust and efficiency – and reduces cost. DISA can seamlessly harness data for better business outcomes and organizational success. With this vision, DISA can break -down silos, seamlessly connecting people, systems and processes with enterprise-wide digital workflows. In approaching a platform, DISA can consider a customer-centered platform that empowers customers, employees and partners with modern, consumer-grade experiences. This service delivery must also conform to the data models, security and compliance posture that is designed for DOD operations. This approach accelerates time-to-value, unleashes agility and unlocks innovation.
2. **Transform Enterprise Security Operations with AI:** Security operators manage multiple applications, sometimes more than 50 or 100. Unifying operations on a single AI-leading platform helps security teams scale faster, smarter and more efficiently, enabling and automating critical collaboration of data and process between IT, security and risk to more quickly and effectively respond and remediate threats. It brings in security and vulnerability data from your existing tools and uses intelligent workflows, automation and a deep connection with IT to streamline security responses.
 - **Efficient Incident Assessment and Prioritization:** AI accelerates the process of assessing and prioritizing security incidents, enabling teams to focus on the most critical threats first.

- **Rapid Contextual Insights:** AI provides concise summaries and contextual insights on threats, helping security teams understand incidents quickly and accurately.
 - **Natural Language Processing:** The use of natural language queries allows for improved resolution notes and expedited investigations, significantly reducing incident closure times.
 - **Threat Hunting:** The use of natural language queries empowers teams to proactively identify and isolate advanced threats that may bypass traditional security measures.
 - **Automated Triage:** AI helps in automating the triage process, reducing the time spent on manual analysis and allowing for faster response to incidents.
 - **Performance Analytics:** AI-driven analytics provide insights into security operations, helping organizations anticipate trends and improve their response strategies.
3. **Platform Operational Efficiencies:** Being able to communicate accurately and in a timely manner to resolve security threats and vulnerabilities is imperative in DISA's environment. A delay could impact the wide range of enterprise services that DISA provides to their customers. Leveraging the following capabilities of ServiceNow's platform offers substantial operational efficiencies and unifies Security and IT Operations:
- **Integrate Data Sources:** Combine data from various security tools and platforms to create a comprehensive view of security incidents and vulnerabilities.
 - **Utilize Predictive Intelligence:** Implement machine learning algorithms to analyze historical data and predict potential security threats, enhancing proactive measures.
 - **Centralized Dashboards:** Use dashboards to visualize data and track security incidents from detection to resolution, ensuring all team members have access to the same information.
 - **Automate Reporting:** Automate the generation of reports to provide insights into security performance and incident trends, facilitating better decision-making.
 - **Continuous Improvement:** Regularly review and refine processes based on performance analytics to ensure that the security operations remain effective and responsive to new threats.
 - **Enhanced Analyst Productivity:** Streamlines the incident review process, allowing analysts to focus on critical tasks by delivering instant summaries of relevant information.

BIO: Scott Havlak is an Advisory Solution Consultant for Security Operations at ServiceNow. During his career Havlak has proposed and delivered a broad range of cybersecurity consulting services and solutions to hundreds of Fortune 500 companies, U.S. federal, state and local government entities and large privately held enterprises. Havlak's previous work experience includes sales, consulting and IT positions at Synack, Palo Alto Networks, Mandiant, FireEye, RSA, Qualys, SecureWorks (LURHQ Corporation), AGCO and the San Francisco Museum of Modern Art. Havlak is a cum laude graduate from the University of Florida with a degree in accounting and successfully passed the uniform certified public accountants exam.

Delivering Improved Enterprise Services with a Unified AI-Powered Platform Approach

Jeremy Westerwiller, Senior Solutions Consultant, ServiceNow •

holly.horton@servicenow.com

ABSTRACT

The Defense Information Systems Agency (DISA) faces significant challenges in unifying back and front offices operations, including the helpdesk, to better support and inform their customers using efficient, cost-reducing and intuitive technologies.

DISA provides a critical and complex scope of services through an operational envelope that has is challenged by multi-domain operations plus siloed teams, systems and data. In this context, it can be challenging for DISA to support and inform the warfighter at the speed of need.

Leveraging artificial intelligence (AI) across the enterprise in a unified fashion offers DISA the possibility to deliver exceptional customer support as a unified agency in furtherance of a nation-critical mission.

A unified approach of customer service delivery founded on AI, connected to data, delivering experiences through a modern and intuitive workflow empowers DISA to proactively support all corners of the organization, ultimately leading to enhanced speed, reduced cost and a fundamentally superior experience for all customers, especially the warfighter.

Within the context of the cyber domain: we will discuss how AI can recognize anomalies in the network to improve detection and resolution. We will demonstrate how a unified customer and IT support systems provide targeted and automated communications to improve customer visibility while proactively providing Tier 0 support. Additionally, we will explore how AI can be leveraged by agents and customers to speed up resolutions times and improve self-service capabilities.

An AI-first approach that consolidates operational data to leverage a more unified technology deployment to the helpdesk, customer information systems: the back and front offices operations – DISA will be able to improve visibility, increase operational excellence, reduce cost and improve experiences while aligning to White House initiatives.

We will examine the following three use cases:

1. Maximizing the accuracy and effectiveness of AI-first solutions by mitigating data silos and inconsistent insights. Different teams may implement AI solutions independently, leading to fragmented data storage and analysis. This lack of integration prevents a holistic view of operations, reducing the effectiveness of AI-driven decision-making and support. Powerful and purposeful AI requires the ability to leverage data across teams to automate outcomes. Without data integrated into unified system, AI may fail to communicate across departments and its promises.
2. Delivering unified and proactive services. Many teams within DISA are challenged with reactive service management due to fragmented front and back-office operations. This leads to inefficiencies, delayed issue resolution, increased cost and decreased user satisfaction. By consolidating data into a unified platform, organizations can create cross-department AI solutions to proactively detect, prevent and resolve problems while providing automated communication with the customer. By providing AI access to real-time data to conduct predictive analytics, organizations can shift from reactive troubleshooting to proactive service delivery. Unified operation ensures seamless communication and engagement between DISA delivery teams and customers, enabling faster resolutions and improved experiences.
3. Delivering consistent, accurate and actionable experiences at mission speed. Siloed AI implementations can degraded levels of automation, responsiveness and service quality across different touchpoints. This inconsistency increases cost-of-delivery and causes delays as it forces employees to adjust to different workflows, manage tasks across inefficient workflows and navigate frustration operational scenarios. This inconsistency also frustrates the customer in service delivery when their visibility, self-service efforts and experiences change from system to system. Ultimately this reduces trust in AI interactions and hinder overall operational effectiveness – negating the investment value in modernization. Unified operations across the enterprise can drive a more consistent experience to improve effectiveness, efficiencies and engagement.

BIO: Jeremy Westerwiller is a Senior Solutions Consultant at ServiceNow and is an experienced professional with a demonstrated history of working in the software industry and holding leadership roles while attached to results driven organizations. Westerwiller has a strong understanding of Scrum framework and experience as a DevOps manager with a unique ability to effectively guide organizational goals by bridging the communication gap between business and technical personnel. Knowledgeable in Scrum, Software Development Lifecycle (SDLC), AWS and IBM cloud environment, software deployment, SSAS, database management, JIRA, data science, requirements gathering, user experience, security, IT architecture and web accessibility. Westerwiller has advanced soft skills with the technical education and experience required in today's corporate environment. Westerwiller earned a Bachelor of Science in information science from the University of Maryland.

Submissions

Maneuver the Domain

Revolutionizing Cyber Hunt Operations at the Edge With Portable, High-Performance Solution

Richard “Trey” Howard, Senior Software Engineer, Omni Federal •

richard.howard@omnifederal.com

ABSTRACT

The Department of Defense (DoD) faces increasing challenges in safeguarding its networks from sophisticated cyber threats. For securing edge networks in particular, approaches considered best practice for securing centralized cloud-based networks are often not appropriate. This poses a significant challenge to DoD organizations operating in Edge environments, as the required approach in responding to an attacker's tactics, techniques and procedures are often significantly different than for traditional cloud-based networks. Edge networks, a specific sub-type of DoD enterprise networks, are best protected with specialized solutions designed explicitly for defense at the Edge.

Join us for this educational segment where we describe the lessons learned in building for edge defense via our development of REDHOUND, a new cyber hunt kit offering by Omni Federal. Built specifically to address the unique challenges posed by edge environments, REDHOUND delivers successful mission outcomes by bringing the fastest performance speeds, the lowest power usage, a very small form factor and the latest technology in a modular and transportable kit. A comprehensive solution, REDHOUND provides all the software and hardware needed for Edge Missions – for today and for the future.

Attendees of this session will gain valuable knowledge including:

- Understanding the key differences between defending cloud-based enterprise networks and Edge enterprise networks.
- Learning about the specific cybersecurity challenges posed during edge missions.
- Experiencing the unique lessons our cybersecurity team learned through both their former careers as cyber operators and their current careers as solutions developers - and how this shaped our development of REDHOUND.
- Developing an understanding for why Omni adopted novel approaches in building our REDHOUND solution to address the key needs of Edge mission requirements for today's and tomorrow's Edge networks.

BIO: Richard “Trey” Howard is a veteran of the networking, cybersecurity and infrastructure space. Howard is a subject matter expert in software engineering with more than 12 years of experience in delivering cybersecurity software solutions, system architecture, development workflows and full stack applications. His background includes work developing cybersecurity solutions in edge environments for federal customers. He has extensive experience as a Senior Software Engineer and proven ability to develop tailored edge solutions that are effectively future-proofed and foster continuous improvement and development. Prior to joining Omni, Howard held various roles at leading DoD software providers, including CACI, Technica and Booz Allen Hamilton.

RAVID (Randomized Automated Virtual Infrastructure Defense)—An End-to-end Automated, Stealth, Moving Target Defense Architecture

Harris Nussbaum, Cybersecurity Expert, Tyto Athene, LLC •

harrisn@mindpointgroup.com

ABSTRACT

RAVID addresses the pressing challenge of outdated, static cybersecurity infrastructures that expose organizations to predictable and exploitable threats. Traditional models rely on fixed endpoints and constant network configurations, making it easier for adversaries to detect, target and breach critical systems. Inspired by historical shifts in military strategy—from stationary defenses to agile, stealth-enabled operations—RAVID redefines cyber defense by emphasizing mobility and dynamic obfuscation across the entire digital landscape.

At its core, RAVID implements a multi-layered Adaptive Moving Target Defense (AMTD) strategy that continuously reorients network pathways, infrastructure and applications. This approach leverages stealth networking techniques—such as rotating network routes, decoupling control and data planes and eliminating static IP addresses—to transform the network from a vulnerable threat plane into an active shield. Additionally, orchestrated API-driven failover mechanisms ensure that endpoints and virtualized storage are not fixed targets but are dynamically repositioned to preempt adversarial attacks.

By integrating cost-effective commercial and open-source tools, RAVID not only extends the lifespan of legacy systems but also creates a resilient, self-healing infrastructure. This proactive defense model drastically reduces the attack surface and minimizes the window of opportunity for cyber threats. In doing so, RAVID sets a new standard for cybersecurity—one where continuous adaptation and stealth are central to maintaining a robust defense in the face of an ever-evolving threat landscape.

BIO: Harris L. Nussbaum Jr. is a seasoned cybersecurity expert with a distinguished career spanning military and civilian domains. With nearly three decades of experience, he has been at the forefront of designing and implementing advanced defense strategies, including pioneering work in stealth networking and moving target defense. Nussbaum has led multiple high-profile initiatives to modernize security infrastructures, integrating innovative network architectures that ensure continuous system invisibility and rapid adaptation to evolving threats.

His extensive background includes serving in critical roles within the intelligence community, where he developed methodologies that leverage mobility and obfuscation to preempt enemy exploitations of some of our most critical secrets. Nussbaum's expertise bridges the gap between theoretical research and practical, scalable solutions—transforming legacy systems into dynamic, resilient architectures. His work has not only enhanced the security posture of military operations but has also empowered commercial organizations to proactively safeguard their digital environments against sophisticated adversaries.

Pre-Emptive Threat Intelligence: Disrupting Adversary Operations Before They Strike

Noah Plotkin, Solutions Engineer, Silent Push • nplotkin@silentpush.com

ABSTRACT

Threat actors rely on well-structured infrastructure to conduct cyber operations, including reconnaissance, malware distribution and command-and-control (C2) activities. By understanding how adversaries build, manage and evolve their infrastructure, defenders can shift from reactive response to proactive disruption—denying adversaries the operational environments they depend on. This talk will explore key methodologies for identifying and tracking adversary infrastructure, including fingerprinting hosting patterns, leveraging WHOIS and DNS records and detecting behavioral signatures that expose attacker operations.

Using Sapphire Sleet, a North Korean APT group, as a case study, we will examine how adversaries strategically age domains, rotate infrastructure and exploit hosting providers to evade detection. By analyzing their evolving tactics and operational shifts, we'll demonstrate how DoD cyber defenders can apply pattern-based intelligence to preemptively uncover new infrastructure before it becomes fully operational.

Silent Push enables this level of proactive threat hunting through its ability to track adversary infrastructure at scale, leveraging first-party DNS telemetry, real-time scanning and behavioral fingerprinting to detect pre-weaponized attack infrastructure. By integrating these techniques, defenders can significantly reduce blind spots, identify adversary campaigns earlier and strengthen their ability to disrupt emerging threats in alignment with DoD cyber defense objectives.

Attendees will leave with actionable methodologies for real-time infrastructure tracking, allowing them to move beyond traditional intelligence gathering toward the active disruption of adversary operations.

BIO: Noah Plotkin is a Solutions Engineer at Silent Push, specializing in cyber threat intelligence (CTI) and adversary infrastructure tracking. With experience in intelligence-driven cybersecurity solutions and strategic consulting, he helps enterprise and government organizations build and enhance threat intelligence programs by delivering actionable cyber threat intelligence that improves detection, response and overall security posture. His expertise spans proactive intelligence methodologies, large-scale threat analysis and integrating advanced CTI solutions into security workflows to counter evolving cyber threats.

Unlock the Threat: Apply Storyboarding to the Cyber Arena

Aaron Boteler, Chief Technology Officer & Principal Engineer, CloudCurrent LLC •
aaron@cloudcurrent.biz

ABSTRACT

VStrike provides a critical solution for DISA's imperative to modernize its static networks and implement robust deception strategies. At its core, VStrike delivers continuous, real-time analysis of network traffic and sensor data, a fundamental capability for identifying malicious actors and bots exploiting static network vulnerabilities. Operators can now establish baseline network behaviors and detect subtle deviations that reveal anomalies and sophisticated threats that attempt to blend into normal operations.

This foundational real-time visibility seamlessly transitions into VStrike's advanced 3D mapping and detailed data capture, further enhanced by its storyboarding capabilities. These features are pivotal in streamlining the deployment of deception technologies. With centralized management across cloud, DevSecOps, IT and OT infrastructure, VStrike provides the actionable intelligence necessary to create realistic false targets and decoys. These strategically placed decoys effectively redirect adversaries, disrupt their operations, deplete their resources and grant stakeholders valuable time to strengthen their defenses.

The efficacy of this integrated approach was vividly demonstrated during the NNSA/DOE Imperial Catfish Cyber Exercise. VStrike distinguished itself as the only solution capable of accurately identifying and animating the Red Team's maneuvers as they gained network control. This unique capability stemmed from its ability to synthesize actionable threat intelligence visuals by consolidating data feeds from multiple vendors—including traffic and hardware alerts—and overlaying them onto a dynamic 3D physical map. This real-world success underscores VStrike's ability to translate complex data into clear, actionable situational awareness.

Ultimately, VStrike's storyboarding feature acts as the culmination of its capabilities, transforming raw data into actionable insights. This empowers DISA to deploy defensive countermeasures rapidly, significantly hindering adversarial efforts and providing operators with the necessary time to reinforce network defenses. By facilitating a shift from a static security posture to one that is adaptive, agile and centered on deception and proactive threat detection, VStrike significantly enhances DISA's ability to counter evolving cyber threats and ensure a secure, resilient network. In essence, VStrike provides a comprehensive, end-to-end solution for modern cyber defense

BIO: Aaron Boteler is a CTO/Principal Engineer at CloudCurrent LLC with more than 25 years of experience in embedded and full stack engineering. He has expertise in project/team leadership, product rollout/sustainment and customer interfacing. This expertise includes a wealth of experience in high-speed 3D rendering, geospatial, packet processing, complex UIs, stream-processing and collaborative platform development. He holds two patents in applying DSP concepts to packet processing.

Advanced Cyber Deception—The Future of Cyber Defense

Sreenivas Gukal, Ph.D., Chief Product Officer, Acalvio Technologies •

sgukal@acalvio.com

ABSTRACT

In 2024, Google announced the first zero day detected by AI. Amazon cyber chief C.J. Moses said that AWS saw a billion cyber threats a day driven by AI. University researchers published papers on how generative AI can come up with AI agents to create exploits based on just CVE descriptions. We are in the new age of AI-driven attacks and the attacks will only get worse.

Advanced Cyber Deception (ACD) is ideal for active cyber defense against both N-day and zero-day attacks. Deception is the only security technology that allows introducing new entities into the network to create enticing false opportunities for the attacks to target, at every step of the attack progression. ACD has progressed far beyond honeypots of the old – deceptive entities now include any type of endpoint in the network, applications, document and data repositories. Deception also extends to identities, in identity repositories such as Active Directory or Cloud IAM directories and on endpoint credential caches, cloud services such as secrets managers, Kubernetes clusters etc. With AI integrated into every aspect of deception technology, ACD is easy to use and very effective in high-fidelity early threat detection.

Automated Moving Target Defense (AMTD) based on cyber deception is the paradigm shifting technology to address AI-driven attacks. Join this session to learn about the advances in deception technology to address evolving threats.

1. Layered deception – multiple independent layers of deception that change to address different threat scenarios to provide a very effective moving target defense.
2. Just in time deception that is automatically deployed as response actions to confirm low priority alerts by other security solutions.
3. Dynamic deception that keeps changing the network neighborhood.
4. Identity deception that is pervasive – endpoints have many credential stores that attackers can steal from for lateral movement and privilege escalation. NSA and five eyes intelligence agencies recently published a paper on the attacks against Active Directory and how deception is the only effective way.
5. Perception-changing deception – living off the land and increasingly living off the cloud, attacks leverage native legitimate tools and cloud services. By deploying deception in these tools and services, attacker perception can be changed without actually changing the network.

BIO: Sreenivas Gukal, Ph.D., is a co-founder and the Chief Product Officer at Acalvio Technologies and the author on more than a dozen patents in cyber deception. Acalvio is a leader in autonomous cyber deception technologies, arming enterprises against sophisticated cyber threats including APTs, insider threats and ransomware. Its AI-powered Active Defense Platform, backed by 25 patents, enables advanced threat defense across IT, OT and cloud environments. Additionally, the Identity Threat Detection and Response (ITDR) solutions with Honeytokens enable zero-trust security models.

Prior to founding Acalvio, Gukal held senior R&D positions at Informix, Microsoft and CA Technologies, where he pioneered development of high-performance data stores. Gukal holds a doctorate and master's degree in computer science from the Georgia Institute of Technology, Atlanta, Georgia.

ZeroLens: Enhancing Cyber Deception and Threat Intelligence for Dynamic Network Defense

Terry Dunlap, Senior VP, Corporate Strategy & Development, NetRise •

terry.dunlap@netrise.io

ABSTRACT

The static nature of enterprise networks leaves them vulnerable to increasingly sophisticated adversaries who rapidly adapt their attack techniques. The DoD must integrate automated deception strategies that disrupt adversarial operations while capturing real-time threat intelligence to regain decision dominance and impose actual costs on cyber threats.

ZeroLens, a cutting-edge capability within the NetRise platform, transforms cyber defense by automating vulnerability identification and enabling adaptive deception at scale. By analyzing exploitable weaknesses in firmware, embedded systems and compiled binaries, ZeroLens enables defenders to:

- Identify and weaponize vulnerabilities that lure adversaries into interacting with false targets.
- Automate zero-day exploit detection and reachability analysis to predict adversarial attack paths.
- Feed real-time threat intelligence into defensive countermeasures, enabling faster remediation and adaptive security responses.

This talk will explore how ZeroLens supports DISA's mission to maneuver the cyber domain, leveraging deception technologies to impose tactical and operational costs on adversaries. ZeroLens allows decision-makers, cyber operators and threat hunters to turn exploitation attempts into intelligence opportunities with the tools needed to outpace, mislead and counteract cyber threats in real-time.

BIO: Being arrested at 17 years old (circa 1985) for hacking with a Commodore 64 and a 300 baud U.S. Robotics modem didn't stop Terry Dunlap from:

- Obtaining a top-level security clearance with the U.S. government (2001)
- Working offensive cyber operations with the U.S. National Security Agency (2002)
- Launching Tactical Network Solutions to provide offensive cyber capabilities (2007)
- Spinning out ReFirm Labs to reverse engineer IoT firmware (2017)
- Selling ReFirm Labs to Microsoft for more than \$20 million (2021)

- Launching Gray Hat Academy to teach cybersecurity pros how to think and act like a hacker (2023)
- Becoming SVP of Corporate Strategy & Development with NetRise (2024)

Every setback is just another steppingstone toward success. No matter where you start or the obstacles you face, your journey is defined by resilience, adaptability and the relentless pursuit of growth. He hopes his story shows that with the right mindset and determination, even the most unexpected paths can lead to remarkable outcomes. Keep pushing, keep learning and never underestimate where your passion can take you. Want to chat about your journey?

Maneuvering the Domain: Deception-Enhanced Endpoint Defense for the Federal Enterprise

Rick Friend, Manager, Cybersecurity Solutions & Architecture • rfriend@merlincyber.com

Brian Recore, Cybersecurity Solutions Engineer, Merlin Cyber • Brecore@merlincyber.com

ABSTRACT

Federal agencies face adversaries who increasingly bypass traditional EDR endpoint defenses by abusing techniques like syscall manipulation, credential harvesting and living-off-the-land (LotL) binaries. These threats often operate under the radar, bypassing and exploiting traditional security control measures. While preventive controls remain essential, agencies must pair them with deception-based detection to impose costs on the adversary, buy time for defenders and support timely corrective actions.

This session focuses on how embedded endpoint deception—such as false credentials, decoy connections and dissolvable identity traps—can expose malicious activity in real time and generate high-confidence alerts. Tailored for the mission needs of the Department of Defense and federal civilian agencies, the approach supports a layered defense strategy that enhances visibility, enables more agile response and creates operational space to outpace the adversary.

Key Session Takeaways:

- Understand how attackers bypass EDR using techniques like syscall manipulation and credential harvesting—and why static defenses are no longer enough.
- Learn how endpoint deception enhances detection, using false credentials and decoy assets to expose attacker behavior without relying on signatures or agents.
- Explore agent and agentless deception technologies that adapt to each host without impacting performance or visibility. • Discover how deception accelerates response, reduces dwell time and supports faster, more confident deployment of corrective controls.

BIO: Rick Friend, a CISSP-certified cybersecurity professional at Merlin Cyber, draws on more than two decades of federal cybersecurity experience, including service in the U.S. Army with multiple combat tours. Holding a Top-Secret SCI clearance, he focuses on implementing zero-trust architectures to proactively shield organizations from evolving threats. Friend has shared his insights on vulnerability and risk management at numerous cybersecurity panels, leveraging real-world expertise in high-stakes government environments. With a special interest in preventing adversaries and mitigating ransomware, he consults with organizations to defend their most critical assets.

Brian Recore is a Systems Engineer with more than 25 years of experience in the IT industry. He has designed, implemented and managed complex systems for organizations of all sizes, with expertise ranging from cloud computing and network architecture to cybersecurity and data management. Recore leaves an impact with his technical team leadership, stakeholder communication and results that exceed expectations.

Submissions

DevSecOps Transformation

A Structured Approach to DevSecOps Transformation

Andrew Scherer, IT Transformation Solution Sales Manager, Federal, ServiceNow •
holly.horton@servicenow.com

ABSTRACT

For DISA and other DoD organizations, embracing a DevSecOps mindset isn't just a shift in methodology—it's a strategic necessity. The goal is clear: delivering capabilities at the speed of need, supporting the warfighter and serving a no-fail nation-critical mission. Successful transformation requires a structured approach, balancing agility, security and operational efficiency.

This journey follows five key steps:

1. **Leadership Alignment & Cultural Shift** – Secure executive buy-in, foster collaboration and empower champions.
2. **Define a Roadmap & Structure the Transformation** – Establish a DevSecOps Center of Excellence (CoE), take a phased approach and standardize the toolchain.
3. **Identify & Prioritize Target Programs for Transition** – Use a maturity model to assess readiness and prioritize high-impact applications.
4. **Implement Agile Governance & Continuous Improvement** – Track performance, measure KPIs and optimize workflows.
5. **Scale & Sustain the Transformation** – Embed security into development pipelines, automate compliance and foster a culture of learning.

The DevSecOps Journey

Leadership:

DISA leadership plays a critical role in driving DevSecOps by aligning initiatives with strategic objectives and ensuring transparency at every stage across teams and domains. A well-defined governance model brings development, security and operations teams together under a unified framework, breaking down internal silos and fostering collaboration. Identifying DevSecOps champions across teams accelerates adoption, encourages innovation and creates a structured way to surface and refine new ideas. With leadership commitment and a culture ready for change, the next step is to establish a clear roadmap for execution, setting the foundation for a scalable and sustainable transformation.

Center of Excellence:

A DevSecOps Center of Excellence (CoE) brings together key stakeholders from development, security, IT operations and compliance to establish policies and governance. Role-based access controls help maintain accountability and security. Taking a phased approach is the most effective strategy—starting with small pilot projects, refining processes based on early results and expanding as successes build. Standardizing the toolchain is also essential, incorporating CI/CD, security scanning and automated testing to improve

workflows and accelerate software delivery. Meanwhile, agile management practices keep teams aligned, adaptable and compliant throughout the transformation.

Identify Programs:

Choosing the right programs to transition first is key. A maturity model helps assess readiness and provides a structured way to evaluate potential candidates. Applications with frequent deployments, high change rates, or cloud-native architectures are good starting points, while mission-critical systems benefit from automation to strengthen security and resilience. Enterprise architecture principles help identify application dependencies, address technical debt and prioritize modernization. A standardized evaluation framework guides decisions by balancing business goals, feasibility and risk.

Governance:

As DevSecOps takes hold, agile governance and continuous improvement keep teams on track. Objectives and Key Results (OKRs) align efforts with long-term goals, while strategic planning helps teams stay flexible and responsive. Real-time monitoring tracks key metrics like deployment frequency and security compliance, while performance analytics identify bottlenecks and improve efficiency. Continuously measuring outcomes allows teams to refine their approach, strengthening DevSecOps maturity over time.

Scale and Sustain:

Once initial successes are in place, the focus shifts to scaling and sustaining DevSecOps. Repeatable templates and best practices help teams expand adoption across the organization. Security and compliance should be built into development pipelines (Shift Left Security) to catch vulnerabilities early. Automated risk assessments, vulnerability scanning and real-time threat intelligence strengthen security while reducing operational friction. Visibility into infrastructure, software dependencies and compliance status keeps governance aligned with DoD requirements.

A strong learning culture is key to long-term success. Ongoing training, knowledge-sharing and gamification keep teams engaged and drive continuous improvement. By combining automation, best practices and data-driven insights, organizations can accelerate DevSecOps adoption—delivering secure, high-quality software at mission speed. Starting small, demonstrating quick wins and scaling strategically will create lasting impact.

Conclusion

This approach empowers DISA and the DoD to achieve a DevSecOps transformation that's scalable, measurable and inherently secure. By integrating proven practices with automation and robust governance, organizations can accelerate software delivery, fortify security and streamline operations—all while adhering to rigorous DoD standards.

BIO: Andrew Scherer, based in Washington D.C., boasts 25 years of experience in the financial and federal sales domains. His impressive track record includes 18+ years of selling IT Services directly to the Department of Defense (DoD) and civilian agencies. Scherer's forte lies in crafting customized solutions that yield powerful outcomes, all while keeping a keen eye on budget constraints and return on investment (ROI).

His passion lies in collaborating with DoD clients to deliver enterprise-wide solutions that not only advance their mission but also equip them with world-class tools to enhance their work environment.

Accelerating DevSecOps: Consolidated Machine Identity Security and Code Signing

James Imanian, Senior Director, U.S. Federal Technology Office, CyberArk Software •
james.imanian@cyberark.com

ABSTRACT

In today's digital battlespace, adversaries relentlessly exploit machine identities as a weak point within DevSecOps. Securing personnel access alone is not enough. DevSecOps personnel must ensure all forms of machine identities they touch—workloads, containers, coding platforms, code signing, cloud—are protected. But can properly securing these machine identities actually make DevSecOps easier and faster?

Join us for an in-depth discussion on how you can experience accelerated DevSecOps across hybrid and multi-cloud environments through a battle-tested identity security with integrated machine secrets management. Learn how machine identity security is a force multiplier for DevSecOps, enabling secure automation, policy enforcement and rapid deployment of digital capabilities—all while reducing cyber risk and ensuring mission readiness.

BIO: James Imanian is an executive with more than 30 years of experience in aviation and cyberspace operations as well as risk management in these areas. In his role as the first leader of CyberArk's U.S. Federal Technology Office, Imanian is tasked with advising federal customers on the latest threat landscape and how the CyberArk technology platform aligns to meeting their mission requirements. Imanian brings to CyberArk a valuable "customer first" perspective from his experience as the Navy staff's CIO, CISO for Guidehouse and Deputy CIO for the F-35 Joint Program Office. He is excited to contribute to CyberArk's mission's success as it aligns with his passion for defending our nation against advanced cyber threats.

DevSecOps Transformation

Manisha Morris, President & CEO, MSM Technology, LLC •

mmorris@msmtechinc.com

ABSTRACT

MSM presents a strategic roadmap for DISA's DevSecOps transformation, engineered to deliver rapid capability deployment and fortified security through the seamless integration of immutable infrastructure and Continuous Authority to Operate (cATO) within a zero-trust framework. Our methodology employs a structured, five-phase approach, beginning with foundational alignment and a focused pilot initiative and advancing through collaborative design, automated security integration, rigorous validation and continuous optimization. We emphasize the development of a resilient DevSecOps pipeline, leveraging industry-leading tools for comprehensive code analysis, infrastructure vulnerability assessments and automated security testing. Recognizing the complexities of legacy systems, MSM provides tailored strategies for risk-prioritized transitions and the implementation of alternative zero-trust controls where full DevSecOps adoption is initially constrained.

Our approach is designed to empower DISA to achieve accelerated delivery, enhanced security posture and a culture of sustained improvement, ensuring mission success in an evolving threat landscape.

MSM Technology Response:

DISA's initiative to adopt DevSecOps and Agile practices is crucial for accelerating capability delivery and enhancing security. MSM understands that this transformation extends beyond technical implementation; it requires a fundamental shift in organizational mindset, particularly focusing on immutable workloads and Continuous ATO (cATO).

1. How Should an Organization Start? MSM's Approach: Strategic Foundation & Pilot Team with Emphasis on Immutability and cATO.

To initiate DISA's DevSecOps transformation, we recommend a foundational phase centered on strategic alignment, security and the establishment of immutable workloads. This entails conducting comprehensive workshops with stakeholders to establish a clear understanding of DISA's strategic goals and security requirements, with a specific focus on transitioning to serverless/container architectures and implementing Infrastructure as Code (IaC). From the outset, we prioritize aligning to DISA's Zero Trust architecture, ensuring security is embedded throughout the development lifecycle and integrating cATO by tracking security concerns, POA&Ms and bug fixes through Agile sprints and release pipelines.

Importantly, we advocate for starting with a pilot team, preferably a development team already familiar with Agile and DevSecOps principles and focusing on a project that can demonstrate the benefits of immutable workloads and cATO. This approach allows for controlled experimentation, rapid feedback and demonstrable success. We use tools like Jira Align to ensure the DevSec-

Ops transformation is aligned with strategic business goals and integrate code scanning tools like Veracode, SonarQube and Palo Alto Prisma Cloud into the pipeline. The direct impact of this approach is minimized risk, built internal expertise, the establishment of a strong foundation for scaling DevSecOps across the organization and a clear path towards achieving immutable workloads and cATO.

2. How Should the Transformation Process Be Structured? MSM's Approach: Phased Approach & Continuous Improvement with Detailed DevSecOps Pipeline Integration

MSM provides a strategic and effective approach for organizations to adopt DevSecOps through a phased and iterative methodology. This framework is firmly rooted in Zero Trust principles and is intrinsically linked with continuous improvement practices and a robust DevSecOps pipeline. The central goal is to achieve measurable security and operational results, with a specific focus on Continuous Authority to Operate (cATO) and the deployment of immutable workloads.

The transformation is structured into five distinct phases, offering a clear and progressive roadmap for implementation. This journey begins by establishing a secure foundation grounded in Zero Trust, followed by collaborative and secure design practices that embed security from the outset. The methodology then emphasizes automation-first security, leveraging advanced tools throughout the development lifecycle to ensure continuous security and cATO readiness. Subsequent phases prioritize rigorous validation and secure deployment, culminating in continuous optimization and governance to foster a culture of ongoing improvement.

Underpinning each phase is a comprehensive DevSecOps pipeline, integrating a suite of specialized tools for threat intelligence, security analysis, secure access, policy management, collaboration, code management, CI/CD, vulnerability management and infrastructure automation. This holistic approach ensures that security is seamlessly integrated into every stage of the software development lifecycle. MSM's structured transformation process delivers a comprehensive and actionable strategy, ultimately driving successful DevSecOps adoption and the realization of tangible, measurable enhancements in both security and operational efficiency.

3. How Should Target Programs for Transition Be Identified? MSM Approach: Risk Assessment & Strategic Value with Consideration for Legacy Systems

To identify target programs for transition, MSM recommends a risk assessment and strategic value approach, with a particular focus on minimizing complexity and maximizing existing expertise for the initial pilot phase and addressing the challenges of legacy COTS/GOTS applications. We advocate for prioritizing programs with high potential impact, such as those involving critical operations or sensitive data, ensuring the most critical missions benefit first.

However, for the initial pilot, we strongly recommend selecting programs with the fewest number of dependencies and interface requirements, effectively choosing less-complex programs. We also recommend selecting programs where the development teams are already familiar with DevSecOps best practices and platforms. Additionally, we suggest selecting programs already aligned with Agile principles or modern development practices and are deemed secure, further facilitating smoother transitions.

For legacy COTS/GOTS applications, we recommend assessing their compatibility with DevSecOps and exploring options for achieving immutable workloads through scripted installations and automated deployments. If full DevSecOps is not feasible, we suggest enforcing other zero-trust

functionalities like micro-segmentation, ICAM, encryption and API protections. We can conduct workshops with stakeholders to evaluate the strategic importance and feasibility of each program, ensuring alignment with DISA's overall objectives.

This targeted approach maximizes the return on investment, minimizes initial pilot complexity, leverages existing expertise and ensures that the DevSecOps transformation delivers tangible benefits to DISA's most critical missions, while also addressing the complexities of legacy systems.

BIO: Manisha Morris is the President and CEO of MSM Technology, LLC, a leading Woman-Owned Small Business dedicated to IT modernization, automation and emerging technology solutions for defense and federal agencies. Based in Quantico, Virginia, MSM Technology is distinguished for delivering secure, high-speed data access and operational excellence that empower the modern warfighter. With more than 30 years of experience in IT systems development, integration and modernization, Morris has been instrumental in advancing critical initiatives for agencies such as DHS, CBP, DOD and DISA.

DevSecOps—Operationalized

Rich Streeter, Operations Director, Sertainty Federal Systems •

rich.streeter@sertainty.com

ABSTRACT

DevSecOps brings software developers' skills and talents into the cybersecurity fight, which is a significant step forward. However, there are two key challenges.

First, developers have historically been excluded from cybersecurity efforts because protections—culturally and technologically—have been primarily network-centric. Second, most cyber threats target networks and, more specifically, the data they store. This raises an important question: If DevSecOps efforts were 100% successful, what percentage of total cybersecurity threats would be mitigated? If network security and application development tools remain static, the answer is: not much. However, moving beyond legacy toolsets opens up far more promising possibilities.

The most powerful tool for cybersecurity and data protection is cryptography. Traditionally, cryptography has been the exclusive domain of network and system engineers. Developers, on the other hand, work directly with the data that requires protection—utilizing, transforming and creating it. A fundamental truth in computing is that protected data must be decrypted when applications use it. Once an application completes its tasks, the responsibility for securing both the input and output data falls back to network or system resources, where encryption is applied. In essence, developers control the data, while network administrators protect it.

The problem? There is currently no widely implemented encryption technology that allows cryptographic protection to be applied effectively within applications. If such a technology existed, a broader concept of DevSecOps—one where developers play a direct role in data security—would already be the norm. Sertainty's innovation changes this dynamic by enabling developers to integrate cryptographic protections directly into applications, making data security a core part of DevSecOps.

If application developers could take responsibility for protecting the data their applications use—both inside and outside of those applications—it would bypass many systemic cybersecurity vulnerabilities. Sertainty's technology presents the first real opportunity for developers to bridge this gap.

Bottom line: If we want to empower the application development community to solve long-standing cybersecurity challenges, we must provide them with the right tools. Giving developers the ability to secure both the input and output data they handle is the ultimate goal of DevSecOps—and the key to stronger cybersecurity.

BIO: Rich Streeter is the Operations Director at Sertainty Federal Systems, spearheading technology introduction and integration since 2016. Before joining Sertainty, he spent 28 years in the intelligence community, splitting his time between being a Navy Reservist who spent 7 years as a cryptologist on active duty after 9/11 and as a contractor in the private sector providing technical and computing expertise. This combination provides a solid and balanced understanding of both requirements and roadblocks to satisfying those requirements, especially in terms of information security. Streeter holds a MS in management information systems.

DevSecOps Transformation

Joe Jarzombek, CSSLP, Cybersecurity Solutions Program Manager, Acquired Data Solutions • sjoejazz7@gmail.com

ABSTRACT

DevSecOps has evolved from DevOps by incorporating security into development and operational workflows. However, this retrofitted approach leaves critical gaps—it primarily focuses on application security, overlooks the security of deployment platforms and supply chain and treats operations security reactively rather than proactively. Our work addresses these limitations through a three-pronged approach that integrates comprehensive security and AI-driven automated risk assessment into the DevSecOps pipeline.

1. Unlike traditional DevSecOps, which emphasizes application security and operational monitoring, our approach extends security considerations to the deployment platform and supply chain, ensuring that infrastructure security is an integral part of the workflow. Additionally, rather than treating security operations as a static process, we position risk assessment as the driving force for security by using our innovative automated risk assessment technology. Automated risk assessment in the context of DevSecOps dynamically generates security requirements for secure operations and is continuously refined by interfacing with security intelligence, which focuses on emerging, relevant attack scenarios. These elements are processed in near real-time, feeding into an adaptive DevSecOps pipeline for continuous security management.
2. At the core of our approach is a novel AI-driven automated risk assessment system, which dynamically infers security risks from system models. This embeds Systems Engineering principles into DevSecOps, extending its scope beyond developers.
3. The entire assurance argument is managed as a knowledge graph alongside the DevSecOps pipeline, further enabling knowledge-based AI techniques to support structured security reasoning, traceability and compliance verification.

By integrating platform security, risk-driven requirements, intelligence-driven adaptation and AI-powered assurance, our approach transforms DevSecOps into a proactive, systemic and dynamic security framework that is deeply embedded in both the software and infrastructure lifecycle.

BIO: Joe Jarzombek is a Cybersecurity Solutions Program Manager for Acquired Data Solutions and serves as an SME on ICT SCRM Task Force Software Assurance Working Group; Member of CWE Advisory Board, CISQ Advisory Board and SAE G32 Cyber Physical Systems Security. Retired from Synopsis, he served as Director for Government and Critical Infrastructure Programs; Retired from Department of Homeland Security, he served as Director for Software & Supply Chain Assurance; retired USAF lieutenant colonel, he served in Office of Secretary of Defense as Director for Software Intensive Systems and Deputy Director for Software Assurance. While on exchange with the Canadian Department of Defense, he served as Project Manager and Systems Engineer for the CC-130 Electronic Warfare Self-Protection System.

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.

DevSecOps: A Foundation for Consistency, Speed and Security

Cory Blankenship, Senior Security Engineer, GuidePoint Security •

cory.blankenship@guidepointsecurity.com

ABSTRACT

Modern organizations face increasingly complex IT infrastructures, with platforms, services and applications spanning multiple environments. This complexity magnifies the challenge of ensuring consistent, rapid and secure deployments—principles central to a stable, scalable and secure infrastructure and the core of the DevSecOps methodology.

However, in environments where manual configurations are the norm and a development mindset hasn't been introduced, there are important questions which need to be addressed before teams can make the shift to a DevSecOps approach:

- “Where do we start?”
- “What tools do we use and what will those processes look like?”
- “What systems should we include and which should we begin with?”

Most importantly, “how do we help our team comfortably adopt a completely new approach to managing infrastructure?” Addressing these crucial questions is essential for a successful DevSecOps transition, which ultimately delivers significant long-term benefits. New infrastructure can be deployed quickly, the configurations can be more easily maintained and teams can simplify and standardize their deployment processes and thereby enhance the security of their infrastructure.

Please join me to discuss some practical steps for making this transition a reality for your team.

BIO: Cory Blankenship is the Senior Security Engineer, GuidePoint Security, Federal.

Building a Resilient DevSecOps Framework for DISA and the DoD

Zach Bennefield, Federal Security Strategist, Tenable • zbennefield@tenable.com

ABSTRACT

Without a comprehensive security strategy, integrating DevSecOps practices could expose critical systems to new vulnerabilities, undermining mission success. Adopting DevSecOps is critical to enabling DISA and its mission partners to rapidly develop and deploy capabilities while maintaining security at scale. However, transformation without security is a risk multiplier. Agencies need a proactive, continuous security framework that aligns with DevSecOps principles and ensures security is not an afterthought but rather an integrated, automated component throughout the software development lifecycle (SDLC) that also provides insight into your traditional IT security needs.

By incorporating continuous monitoring and risk-based vulnerability management into DevSecOps processes agencies can: Identify and prioritize risks in real time across development and production environments. Implement security-as-code, embedding security controls directly into CI/CD pipelines. Reduce attack surfaces by securing enclaves and microservices, ensuring that the transition to DevSecOps does not introduce security blind spots. Provide actionable insights to leadership and DevSecOps teams, enabling informed decision-making.

As a long-standing partner with DISA and the DoD and the technology provider powering the ACAS contract, Tenable has expanded its capabilities beyond vulnerability management to provide extended attack surface coverage with expansion into DevSecOps as a core component. By integrating Tenable Enclave Security, DISA can ensure that security keeps pace with agility, enabling a secure, resilient and effective DevSecOps transition. For organizations looking to adopt DevSecOps, the “shift-left” security mindset is critical. Tenable Enclave Security is a force multiplier, providing the visibility, automation and risk intelligence needed to securely accelerate DevSecOps adoption. As we move forward, integrating industry best practices with robust enclave security will ensure that DevSecOps delivers its full potential—faster innovation, enhanced security and mission success.

BIO: Zach Bennefield is the Federal Security Strategist at Tenable and a Professor at UMGC teaching graduate level cybersecurity courses. With 20 years of experience in information security, Bennefield has developed a strong expertise in risk detection, prioritization and remediation. Zach’s background as a Security Engineer and Security Analyst for the United States Navy has been instrumental in the creation of new technologies and initiatives at Tenable focused on supporting the unique cybersecurity challenges in the Department of Defense (DoD). Bennefield is a frequent speaker on cybersecurity topics, has authored numerous articles on compliance within the Department of Defense and is frequently sought after for advice on securing critical infrastructure. Bennefield is a creative thinker and innovative technology

leader who takes a great deal of pride in the security industry. He works to ensure that mission-critical goals are met through rigorous requirements analysis and a bottom-up mentality that elevates ideas from the field while giving back best practices to advance organizations' security programs.

Submissions
Undefined

The Hidden Threat: Managing Third-Party and Machine (Non-Human) Identities in a Zero-Trust World

Frank Briguglio, Federal CTO and Global Public Sector Strategist, Sailpoint •

frank.briguglio@sailpoint.com

ABSTRACT

In today's dynamic cybersecurity landscape, identity is the new perimeter and efficient identity security is critical to protecting Department of Defense (DoD) and federal government systems. As agencies continue to expand their reliance on third-party contractors, APIs, service accounts, RPAs and bots, the complexity of identity security grows, increasing the risk of cyber threats and operational inefficiencies.

This brief discussion explores how poor identity security practice leads to security gaps, inefficiencies and compliance risks, with a focus on real-world breaches of third-party software vendors in the government supply chain that exploited weak identity controls. We will highlight how overprivileged access, inadequate access governance and lack of visibility into machine identities create vulnerabilities that adversaries can exploit.

By adopting zero-trust principles and identity security best practices, federal agencies can streamline operations, reduce risk and ensure only the right people and machine identities have the right access at the right time. Attendees will gain practical insights on automating the identity lifecycle, enforcing least-privilege access and leveraging AI-driven monitoring to enhance both security and efficiency.

At the end of this session, you will have an understanding of what it takes to implement identity security frameworks that improve security, operational agility and compliance in alignment with DoD zero-trust strategies and federal mandates.

BIO: Frank Briguglio, CISSP, a seasoned cybersecurity expert with more than 28 years' experience in federal identity, credentialing and access management, public key infrastructure, NIST Security Frameworks and Directives and zero trust. He currently serves as the Federal CTO and Global Public Sector Strategist, where he provides global government customers with a profound understanding of government security and compliance standards and hands-on experience in designing, implementing and managing security solutions tailored to federal requirements, for example, he was the Lead Architect and Subject Matter Expert for a large government-wide cybersecurity program, Dept of Homeland Security (DHS) Continuous Diag-

nostics and Mitigation (CDM). He provides expertise to SailPoint leadership to align product portfolios with federal compliance standards and respond effectively to customer needs, for example, he represents SailPoint on the NIST Cybersecurity Center of Excellence Zero-Trust Architecture collaboration initiative.

Briguglio has been a notable voice in the cybersecurity community across the globe, sharing his expertise and insights at various speaking engagements focused on federal and public sector cybersecurity challenges and identity security. From keynote addresses to panel discussions, Briguglio has contributed to the collective knowledge of cybersecurity professionals and inspired others to enhance their security practices.

- NIST Cybersecurity Framework
- NIST/DoD Zero Trust Architecture
- Identity Governance and Administration
- Access Management and Dynamic Authorization
- Credentialing and PKI

The Evolving Digital Battlefield: Counter State-Backed Cyber Operations in the Cloud Era

Jeff Worthington, Public Sector Executive Strategist, CrowdStrike •

jeff.worthington@crowdstrike.com

ABSTRACT

Modern cyber adversaries, including state-backed actors like China, exploit identity-based attacks, cross-domain techniques and cloud-aware tradecraft to bypass traditional security controls. Increasingly, attackers target less protected areas such as SaaS platforms, business email infrastructure and unmanaged assets.

Cloud security threats are rising, with attackers abusing identity and access management (IAM) systems, single sign-on (SSO) and federated authentication to hijack sessions and escalate privileges. Business email compromise (BEC) tactics now involve email forwarding rule manipulation and OAuth abuse. Unmanaged assets, including abandoned cloud instances and orphaned accounts, provide footholds for lateral movement.

Threat actors employ stealth techniques like living-off-the-land (LOTL), advanced credential theft and cloud reconnaissance. Multi-stage cyber operations increasingly evade detection, while ransomware groups refine double extortion methods. During this briefing, you will learn how adversaries—particularly China—are leveraging these tactics today. We will cover their evolving methods and discuss strategies to counter these emerging threats.

BIO: Col. Jeff Worthington (Ret.), Public Sector Executive Strategist, sits on the Public Sector Executive Strategy Team at CrowdStrike where he provides strategic advisory services related to enterprise cybersecurity solutions for public sector organizations across federal, state and local higher education and health care. Prior to joining CrowdStrike, he served as the Chief Information Officer for the Joint Special Operations Command and Commander of the Army's only Signal Brigade in Europe and Africa, supporting two combatant commands across 110 countries. This capped a career of uniformed federal service spanning 30 years installing, operating, maintaining and defending our nation's most vital information network across the globe. He has extensive experience leading cyber, IT, network and communications teams at all levels of military service across the DoD and within both conventional and Airborne Special Operations units from the foxhole to the White House, where he provided direct communications and Emergency Action support to Presidents Bush and Obama. His leadership and executive operational experiences include information security, IT governance & strategy, network/systems operations and implementation/integration of robust enterprise systems and services.

How Proactive IT With DEX Tools Help Improve Employee Experience (or Something Close to That)

Bill Musson, Senior Technical Sales Engineer, Nexthink Inc. •

bill.musson@nexthink.com

ABSTRACT

In the Department of Defense (DoD), mission success relies on a seamless, stable and secure technology environment. Digital Employee Experience (DEX) is a strategic approach that enhances the workforce's interaction with technology, ensuring reliability and predictability across the enterprise. A strong DEX discipline proactively reduces technology disruptions by shifting IT operations from reactive troubleshooting to predictive, data-driven decision-making.

By enabling enterprise-wide visibility from the endpoint inward—rather than relying solely on data center extrapolation—DEX empowers IT teams to manage the DoD's vast infrastructure with real-time insights rather than just help desk ticket trends. This session will explore how AI, machine learning and modern automation can minimize technology friction, enhance operational readiness and allow military and civilian personnel to focus on their missions. Additionally, we will examine how these advancements can improve IT speed, quality and cost efficiency while strengthening cyber resilience across the DoD.

BIO: Bill Musson is a highly accomplished Senior Technical Sales Engineer with more than 25 years of experience delivering complex IT solutions, security structures and enterprise networks. Holding both CISSP and CCNA certifications, Musson excels in bridging the gap between technical expertise and strategic sales, consistently driving revenue growth within the federal sector. His career highlights include significant contributions to Nexthink, ServiceNow, Cisco and Splunk, where he served as a trusted advisor to DoD and intelligence community clients, demonstrating proficiency in areas such as cloud security, IoT solutions and digital employee experience platforms. Notably, he has a proven track record of developing and presenting compelling product demonstrations, collaborating on FedRAMP compliance and achieving consistent sales targets.

Prior to his federal sales roles, Musson successfully owned and operated ACTT Hawaii, demonstrating his entrepreneurial acumen and ability to build a multi-million dollar business. His extensive technical skill set, coupled with exceptional communication and negotiation abilities, positions him as a valuable asset in the technology sales landscape.

VDetect

John Eubank, Founder & CEO, 10x National Security • john@10xnatsec.com

ABSTRACT

10x National Security's VDetect is a next-generation enterprise data layer designed specifically for advanced intelligence and defense applications. VDetect seamlessly integrates diverse data streams, enabling real-time analytics, predictive insights and enhanced situational awareness. Leveraging cutting-edge machine learning, artificial intelligence and natural language processing (NLP), VDetect provides rapid, accurate and actionable insights by automatically identifying, labeling, categorizing and correlating data across vast networks and multiple security enclaves.

Engineered with an emphasis on flexibility, scalability and security, VDetect supports customized deployments, ranging from baseline operational monitoring to advanced analytics with tailored AI-driven data tagging, labeling and anomaly detection capabilities. Its sophisticated anomaly detection algorithms proactively identify threats and irregularities, significantly improving preemptive security measures and reducing response times. The platform is built to operate within stringent compliance standards, ensuring reliability, security and auditability for sensitive national security missions.

VDetect's unique modular architecture allows customers to select from multiple service-level agreements (SLAs), scaling from foundational capabilities to comprehensive, fully customized enterprise solutions. High-tier SLA options include specialized customizations, such as advanced algorithm training, bespoke data labelers and taggers, implementation of state-of-the-art AI tools and specialized integrations tailored to mission-specific requirements. With its robust design, agile integration capabilities and comprehensive data fusion functionality, VDetect significantly accelerates decision-making cycles, optimizes resource allocation and enhances mission effectiveness for defense and intelligence community stakeholders, ensuring operational superiority in dynamic threat landscapes.

BIO: John Eubank IV is an experienced executive and technology strategist with a proven record in leading innovative defense and cybersecurity initiatives. As Founder and CEO of 10x National Security, he specializes in delivering agile software engineering solutions tailored to the critical missions of national security and defense organizations. Eubank's extensive background includes guiding strategic growth and developing advanced technological frameworks like the Big Data Platform (BDP) and hyperconverged infrastructure automation solutions. Eubank has successfully led efforts across multiple high-profile Department of Defense (DoD) and intelligence community (IC) projects with organizations such as DARPA, DIU, Army, Air Force, Navy, Marine Corps and USCYBERCOM. His vision and leadership extend into initiatives such as VDetect, REDHOUND, Nexus Guard and VPipeline, highlighting his commitment to next-generation technologies such as AI-driven data analytics, quantum data processing and robust cybersecurity frameworks.

In addition to his professional endeavors, Eubank and his wife, Whitney, have actively contributed to educational philanthropy including: 1) Establishing the John and Whitney Eubank Maryland Promise Scholarship at the University of Maryland, aimed at empowering future leaders and innovators. 2) The John Eubank IV endowed Scholarship for Excellence in Business and Information Technology at Towson University. 3) numerous other philanthropic support initiatives to Veterans, Education, Health and financial empowerment initiatives.

Eubank holds deep expertise in building collaborative, forward-looking communities and has a passion for mentoring aspiring technologists and entrepreneurs dedicated to solving complex global challenges.

Best Practices for Implementing Quantum-Resistant Security

Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies •

Mary.Shiflett@ThalesTCT.com

ABSTRACT

Quantum computing's potential computational power will render today's widely deployed encryption algorithms obsolete. Both the National Security Memorandum on Promoting U.S. Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems and Quantum Computing Cybersecurity Preparedness Act stress the need to update IT infrastructure today to combat the quantum threat. Both policies emphasize the use of crypto-agile solutions to diminish transition time and enable seamless updates to new cryptographic standards.

In August 2024, NIST, academia and industry reached the milestone of releasing the first set of Post Quantum Cryptography (PQC) standards. This milestone is a result of many years of research, development, testing and collaboration. Now, federal agencies are tasked with moving to the next phase of getting standards-compliant, interoperable solutions deployed to combat the looming quantum threat.

Session attendees will learn about the best practices that federal agencies should follow when transitioning to quantum-resistant security including how to:

- Utilize crypto inventory tools to learn where and how encryption is currently deployed within an agency's infrastructure
- Prioritize existing infrastructure for a migration to post-quantum cryptography
- Deploy crypto-agile solutions for PKI, Data-at-Rest and in-Transit and Identity and Access Management
- Apply a Cryptographic Bill of Materials (CBOM)

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 cyber security 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.

Best Practices for Insider Risk Management

Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies •

Mary.Shiflett@ThalesTCT.com

ABSTRACT

Insider attacks are on the rise. According to a recent study, 83% of organizations have experienced at least one insider attack in the past year. And, 85% of cybersecurity leaders expect data loss from insider incidents to escalate in the next 12 months.

The U.S. federal government is not exempt from this trend. Insider threats come in a variety of forms—everything from malicious, covert actions of individuals within or connected to an agency, to the accidental loss or theft of data to the theft of an end-user device. Personnel with administrative privileges or adversaries that have maliciously obtained administrative privileges have the potential to inflict detrimental consequences and introduce significant risk to the agency's mission and national security.

Agencies can mitigate the risks from insider threats by merging traditional data security with insider threat detection to help prevent data breaches. Attend this session to learn how to apply best practices for insider risk management from the core to the cloud to the edge including:

- Automating the discovery of non-compliant, risky and malicious data access behavior anywhere
- Detecting compromised accounts and malicious insiders as soon as behavior changes
- Discovering and classifying sensitive data to reduce the risk of data exposure
- Encrypting data with granular access controls to define who, what, where, when and how data can be accessed
- Consolidating encryption keys to facilitate consistent security policies across your entire core-cloud-edge ecosystem

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 cyber security 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.

High Assurance Data Security in the Era of Complex Integration

Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies •

Mary.Shiflett@ThalesTCT.com

ABSTRACT

Enterprise architecture now contains innumerable integrations from the core to the cloud to the edge. Information assurance must not be compromised during the integration process. Best practices for data encryption and key management can be implemented through the use of automation eliminating the need for manual interaction and human error.

By utilizing APIs to automate processes, core policies can be seamlessly applied across the enterprise. For example, while DevSecOps teams can use dynamic and static application security testing to check the code and binaries for misconfigurations or the presence of known vulnerabilities, if the system does not have a consistent and centralized approach to key and certificate management, the DevSecOps configuration management and orchestration tools will be very difficult to trust.

Multi-cloud environments, for example, often result in the use of proprietary tools and APIs, which make it very challenging to orchestrate effective security controls. By implementing cloud key management—like BYOK/HYOK—the key lifecycle ownership remains in the hands of the cloud consumer and can be automated across the multi-cloud landscape to easily enforce enterprise-level security best practices.

Attend this session to learn how to leverage APIs through automation to ensure the highest level of data security enforced across the enterprise at application and data layer to achieve zero trust from the core to the cloud to the edge.

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 cyber security 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.

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.

