



# TechNet Augusta

August 18–21, 2025 | Augusta Marriott at the Convention Center | Augusta, GA

## 2025 SOLUTIONS SHOWCASE





# AFCEA TechNet Augusta 2025 Solutions Review

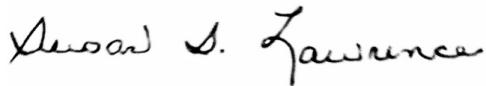
The theme of this year's TechNet Augusta conference is "non-kinetic dominance in multidomain operations." This event allows leaders and innovators to discuss the procurement challenges faced by the military, government and industry in a time of uncertain budgets and runaway technology advances. The U.S. Army continues to explore the intricacies of the cyber domain, and the solutions cited in these pages from our industry partners align with the effort to secure non-kinetic dominance.

The Army Cyber Center of Excellence is seeking solutions to address emerging and existing challenges. Presented with problem statements, dozens of companies have produced abstracts to provide solutions to the challenges. This Solutions Review Compendium complements the event, offering industry the opportunity to respond to the Army's pressing issues.

The abstracts cover many complex challenges the Army faces, from securing data infrastructure to utilizing artificial intelligence in multidomain operations. The top solutions will be presented in the engagement theater at TechNet Augusta.

The content offers a wide range of unique perspectives and solutions, inspiring future innovation.

Best wishes,

A handwritten signature in black ink that reads "Susan S. Lawrence". The signature is fluid and cursive, with the first name "Susan" and last name "Lawrence" clearly legible.

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

# Problem Statements

**Problem Statement 1:** How can technology act as a surrogate for threat transceiver(s) that can receive RF-enabled cyber attacks and can demonstrate battle damage because of the RF-enabled cyber attack? Transceiver(s) must be able to support C2, UAS control and data links.

---

**Problem Statement 2:** How can technology import and ingest data from multiple feeds, sources and formats? Does the tech aggregate and analyze data? Can tech create and have interactive (filters) digital display to inform users of mission-relevant atmospheric, information and data?

---

**Problem Statement 3:** How can technology ingest data from multiple sensors, geo tag data and aggregate for analysis? Can technology do predictive analysis based on preconditioned filters? Can this technology integrate data into mission command systems?

---

**Problem Statement 4:** How does the Army tag, pass and ensure EW-relevant data at machine speed ISO EW OPs to ensure availability to all required stakeholders in an EMS degraded environment?

---

**Problem Statement 5:** How can the Army rapidly adopt ML-enabled EA technique optimization for unknown signals with minimal hardware/platform additions?

---

**Problem Statement 6:** Many modern solutions require integration with multiple vendor technologies to achieve optimal results. To foster innovation and accelerate the delivery of capabilities, we are exploring opportunities for collaborative experimentation. Specifically, how willing would your organization be to participate in joint experimentation activities with other vendors—potentially including sharing nonproprietary data and test environments—to demonstrate the interoperability and combined value of your respective solutions? What mechanisms or agreements would be necessary to facilitate such collaboration while protecting your intellectual property?

---

**Problem Statement 7:** What challenges are you (the vendor) facing while integrating AI with your technologies (e.g., data/compute requirements, security and trust, integration or implementation, cost)?

---

**Problem Statement 8:** Recent conflicts have shown that transmission security (TRANSEC), the ability to protect and mask the data path, is equally as important as COMSEC, since unprotected RF transmission is easily jammable and being used by aggressors for targeting. What is industry doing to ensure radio and other communication systems developed for the force are outfitted with TRANSEC capabilities that meet today's and future threats?

---

**Problem Statement 9:** What technology exists, or is in development, that the Army has not yet experimented with that could act as a "game-changer" for assured voice and data communications at echelon?

---

**Problem Statement 10 – Information Advantage:** How would your company's solution provide the Theater Information Advantage Detachment (TIAD) with a unified tools and integrated systems platform to manage and operate its information activities within an assigned theater? Specifically, how would the solution address and support data sensing/collection, data management, advanced analytics (AI/ML applications), data visualization, comprehensive cybersecurity, and monitoring and influence of the information environment to support the TIAD's contribution to Army multidomain operations (MDO)?

---

**Problem Statement 10 – DCO:** To what extent can you develop a solution that leverages AI/ML to proactively enhance mission network defense by providing an agentless capability to emulate realistic peer/near-peer adversary tactics, techniques and procedures (TTPs) for access to people, processes and systems, while simultaneously augmenting cyberspace defenders in the tactical environment with intelligent threat identification and data movement analysis—encompassing both vertical and horizontal data flow across the mission network and its mission partner environment (MPE)?

# Table of Contents

From Data to Decision: Operationalizing Mission Intelligence Across Systems and Environments	
Michael Chappell, CTO, Appian .....	11
Utilizing AI To Achieve Advantage Over Cyber Adversaries	
Joseph J. Wingo, Director of DOD Strategy, Armis .....	12
Built for Trust, Not Just Speed: Delivering Secure and Compliant Software at Mission Pace	
Philip Brooks, Solutions Architect, Chainguard .....	13
Secure Foundations: Hardening the Open-Source Supply Chain for AI Applications	
Mike Barretta, Solutions Engineering Manager, Chainguard.....	14
Standardize To Secure: Adopting Secure Software Baselines for the Mission	
Natalie Somersall, Principal Field Engineer, Chainguard .....	15
Navigating the Quantum Era: A Proactive Approach to Post-Quantum Cryptography	
Phil Brown, Chief Architect, Army, Defense Agencies and Special Operations Forces, Cisco....	16
Cole Engineering Services	
Stuart Armstrong, CTO, Cole Engineering Services Inc.....	18
From Data Chaos to Clarity: Powering Army Missions With Unified, Actionable Intelligence	
Josh Brunvoll, Senior Solutions Engineer, Cribl .....	19
Hacked From Above: Stopping Adversaries Who Launch Attacks From the Cloud	
Jeff Worthington, Public Sector Executive Strategist, CrowdStrike .....	20
Information Advantage at the Edge: Multimodal Search in a Tactical Form Factor	
Sean MacKirdy, Area Vice President, DOD, Elastic.....	22
Enabling MPE and ACE: Decision Dominance With AI/Gen AI Data Integrity	
John N. Carbone, Ph.D., Senior Technical Director and Chief Solutions Architect, Everfox .....	24
Zero-Trust Application Access and LLM Guardrails for Multidomain Operations and Tactical Data Analytics	
Jim Togher, Major Account Manager, F5.....	26



From Data to Decisive Action: Google’s Security Solution for Multidomain Operations Bailey Marshall, Customer Engineer, Google Public Sector .....	27
Beyond the Hype: Practical AI Integration in Security Automation for Defense Environments Brent Kelley, Principal Solution Architect, GuidePoint Security .....	28
The Role of Special Operations EW and Cyber Activities in Great Power Competition Herm Hasken, Founder and CEO, HighGround Advisors .....	30
Securing the Mission Edge: Zero-Trust AI for Cyber Resilience in Multidomain Operations Jessica Dapelo, Founder and CEO, Jessica Dapelo Enterprises Inc.....	31
Quantum Threats and AI Defense: Future-Proofing National Security Jessica Dapelo, Founder and CEO, Jessica Dapelo Enterprises Inc.....	32
Partnering for Mission Success: How Juniper Mist AI and Marvis Can Enhance Warfighter Communications and Support Non-Kinetic Dominance Michael Maice, Strategic Advisor, DOD, Juniper Networks .....	33
Defending Gray Cyberspace for Combat Power at Echelon Adam Rogge, Senior Account Director, Lumen .....	36
AI Data Challenges Agencies Face and How To Secure, Optimize and Expedite AI Data Operations With Intelligent Data Infrastructure To Ensure Non-Kinetic Dominance Jim Cosby, CTO, NetApp .....	37
Empowering Non-Kinetic Dominance With Unified Data Ingest, Optimization and Classification Using Intelligent Data Infrastructure Jim Cosby, CTO, NetApp .....	38
Enabling DOD Agency Non-Kinetic Dominance by Using Intelligent Data Infrastructure To Unify, Secure, Optimize and Expedite Data Operations Across Hybrid Multicloud and Multidomain Operations Environments Jim Cosby, CTO, NetApp .....	39
Onebrief Collaborative Planning Platform Matthew Work, Head of Growth, Army, Onebrief.....	40
Peraton Dave Dickey, Ph.D., Senior Analyst, Peraton .....	41

Peraton—AI	
Jeff Berlet, CTO, Peraton .....	43
Peraton—DCO and OCO	
Jeff Berlet, CTO, Peraton .....	45
Future of Threat Hunting	
Tim Singletary, Director of Emerging Technologies and Solutions, Peraton .....	46
AI-Driven Security Fortification and Attack Surface Reduction	
Russ Andersson, COO, RapidFort .....	48
An Architecture for Adversarial AI-Enhanced Red Team Simulation, Testing and Defense	
Christopher Yates, Principal Chief Architect, Red Hat .....	50
An Architecture for Decision Advantage	
Christopher Yates, Principal Chief Architect, Red Hat .....	51
Harnessing Disparate Data: Red Hat's Integrated Approach to Ingestion, Analysis and Visualization	
Derek Thurston, Associate Principal Solution Architect, Red Hat.....	52
Wireless Fingerprints: How Evolving Tech Redefines Battlefield Risks	
David Baldwin, Cybersecurity Engineer, Savannah River National Laboratory.....	54
Accelerate the MDO Mission With Secure NPEs for Theater AI Operations	
Andrew Whelchel, Lead Solutions Engineering, Federal, Saviynt.....	55
Mission-Ready ITops: Leveraging Generative AI for Operational Advantage Across the DOD	
Matt Carter, Solutions Architect, ScienceLogic.....	57
The Making of Operator X: The GenAI Platform To Transform Cyber at the Edge	
Nate Delgado, Software Product Owner, SealingTech.....	59
Achieving Decision Dominance: How ServiceNow Empowers Mission Command Through Data-Driven Insight	
Michael Longoria, Senior Account Executive, U.S. Army, ServiceNow .....	61
Empowering the Theater Information Advantage Detachment (TIAD) With a Unified Platform for Multidomain Information Dominance	
Michael Longoria, Senior Account Executive, U.S. Army, ServiceNow .....	63



Overcoming Barriers to Trusted AI Integration for Mission Advantage	
Nathan Bernache, Senior AI Specialist, Solution Consulting, ServiceNow .....	65
Strengthening Decision Superiority Through Unified, Mission-Relevant Data	
Rick Camensky, Federal Sales Director, ServiceNow .....	66
Turning Complexity Into Clarity: Unifying Asset, Operational and Strategic Data To Drive Mission Outcomes	
Andrew Scherer, IT Transformation Solution Sales Manager, Federal, ServiceNow .....	67
Operational Awareness Through Data Aggregation, Analysis and Interactive Visualization With SolarWinds	
Scott Pross, Vice President Technical Solutions, Monalytic, SolarWinds .....	69
Certify Once, Secure Always: Fast-Tracking Trusted Software to the Mission Edge	
Bryan Whyte, Director, Solutions Engineering, Sonatype .....	70
Information Advantage: Deny the Adversary Everything, Deny Ourselves Nothing	
Jeanne Falick, Observability Advisor, Splunk .....	71
Information Dominance in the Modern Battlespace	
Eric Hennessey, Solutions Architect, Splunk .....	72
Modernizing RMF Compliance Through Automation and Agentic AI	
Fawad Siraj, Co-Founder and CTO, stackArmor .....	73
Modernizing the Army's Data Pipeline To Ensure High Velocity Data-Driven Decision-Making From the Enterprise to the Edge	
Sean Applegate, CTO, Swish Data .....	75
Intersection of Quantum, AI and Security	
Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies .....	77
Best Practices for Data in Transit Security, Thales TCT	
Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies .....	78
Bringing Air-Gapped AI to the Tactical Edge for Sensor Fusion and Decision Dominance	
Raj Iyer, Ph.D., President, Tsecond.ai .....	79
Real-Time Data for Mission Analytics	
Carmelo McCutcheon, CTO, VAST Federal .....	80
VDetect	
John Eubank, Founder and CEO, 10x National Security .....	82

**Submissions**

# From Data to Decision: Operationalizing Mission Intelligence Across Systems and Environments

**Michael Chappell, CTO, Appian** • michael.chappell@appian.com

## ABSTRACT

Modern defense leaders face a persistent challenge: How to transform the vast amounts of siloed, incongruent, dispersed datasets into mission-relevant decisions and timely action.

While advancements in hardware and software have made us more efficient at aggregating and analyzing increasingly complex datasets, the end goal remains the same: Drive outcomes through informed, rapid decisions.

In complex, multi-echelon, geographically dispersed processes like C2, the ability to act on real-time intelligence can mean the difference between success and failure on the battlefield.

This session will explore how combining data fabric with artificial intelligence (AI) analysis and process orchestration enables continuous adaptation—so workflows evolve as new intelligence emerges or mission needs change.

Attendees will gain insight into how to:

- Unify data from diverse sources and formats without migration.
- Surface mission-relevant insights with dashboards, filters and AI-powered analysis.
- Operationalize intelligence through agile workflows that adapt in real time.
- Maintain mission dominance across distributed and disconnected environments.

Ideal for mission owners and defense technologists, this session demonstrates how to align data, analytics and processes—powered by AI—to accelerate decision-making and deliver mission outcomes in dynamic operational environments.

**BIO:** As CTO, defense at Appian, Michael Chappell leads the company's U.S. Department of Defense (DOD) portfolio, with a particular focus on the U.S. Army. Before joining Appian, he served as assistant program executive officer for the CIO at the Army's PEO Enterprise Information Systems, where he directed technical strategy and product domains spanning AI, cloud and cybersecurity. With more than 18 years of experience supporting DOD and federal agencies, Chappell has led the development of advanced data analytics platforms and advised Army CIO leadership on enterprise information technology (IT). Since 2010, he has supported the Army in contractor roles, including as a global solutions architect at Ernst & Young, where he spearheaded data quality efforts, and at Accenture, where he specialized in analytics and IT infrastructure. Chappell holds a degree in mechanical engineering from Virginia Tech.

# Utilizing AI To Achieve Advantage Over Cyber Adversaries

**Joseph J. Wingo, Director of DOD Strategy, Armis** • joseph.wingo@armis.com

## ABSTRACT

The U.S. Department of Defense (DOD) must leverage AI/ML models to not only collect data from across the operational environment but also operationalize that data into decision quality information made available to operators at the right time and place to achieve effects over an adversary. In the world of defensive cyberspace operations, Armis stands as the industry leader in utilizing AI/ML capabilities to achieve advantage over cyber adversaries.

**Agentless network terrain mapping:** Deep understanding of each and every network asset and its corresponding vulnerabilities is the foundational bedrock of cyber defense. An “agentless” approach ensures that profiles of networked operational technology and Internet of Things devices that can’t install an agent are still captured and accounted for. Additionally, agentless capabilities ensure that vulnerabilities aren’t missed due to a bad or nonexistent client install.

**Persistent visibility:** Reliance on scheduled scans to gain network and asset visibility is a critical weakness of legacy cybersecurity tools. Scans are a snapshot in time and often fail to capture devices that do not have proprietary clients installed correctly. Agentless and persistent visibility ensures that all devices and their associated security profiles are updated in real time, resulting in enhanced visibility into vulnerabilities and adversary movement in a network.

**Attack Path Mapping:** Armis generates a “digital twin” based on its deep understanding of your network and then utilizes AI models to correlate vulnerabilities in network terrain with known adversary attack vectors to identify the most likely points of ingress and lateral movement across your network. This information is graphically displayed and provides alerts and recommended actions to cyber defenders, allowing them to focus efforts on reducing real-world risk. Because this Attack Path Map is based off of real-time, agentless asset data, operators can eliminate “blind spots” caused by legacy scan/client-based systems and operate with confidence.

**BIO:** Col. Joe Wingo (Ret.) is the director of DOD strategy for Armis and additionally acts as the CTO for Armis’ DOD products. Before Wingo’s retirement on January 1, 2024, he served as the director of operations, 16th Air Force (Air Forces Cyber) and Joint Force Headquarters-Cyber, Joint Base San Antonio-Lackland, Texas.

# Built for Trust, Not Just Speed: Delivering Secure and Compliant Software at Mission Pace

**Philip Brooks, Solutions Architect, Chainguard** • [philip.brooks@chainguard.dev](mailto:philip.brooks@chainguard.dev)

## ABSTRACT

Warfighters rely on fast, adaptable digital capabilities—from artificial intelligence on the edge to real-time logistics orchestration. But the software meant to accelerate the mission often carries hidden fragility: bloated containers, untraceable dependencies and brittle security controls that struggle under scrutiny.

To meet U.S. Department of Defense security expectations and support rapid accreditation, many teams turn to “debloating” images after the fact. This may shrink artifacts, but it also breaks reproducibility, introduces hidden risk and slows trusted delivery.

This session challenges that model. Instead, we’ll explore how building software with a secure-by-construction approach—minimal, verifiable images from the source—aligns directly with NIST 800-190, DISA STIGs for containers and Kubernetes, FIPS validation paths, and emerging DevSecOps compliance patterns.

Attendees will leave with a clear understanding of why post-build “hardening” techniques often fall short under compliance frameworks, how container image design decisions directly impact alignment with standards like NIST 800-190, DISA STIGs and FIPS, and why a secure-from-source pipeline offers a more reliable path to trusted, accreditable software. Whether you’re delivering zero-trust infrastructure or deploying machine learning at the tactical edge, this talk will arm you with a modern, standards-aligned framework for building and delivering secure software at mission speed.

**BIO:** Philip Brooks is a solutions architect at Chainguard, focused on helping public sector organizations secure their software supply chains from the ground up. With a background as a systems and DevOps engineer supporting the U.S. Department of Defense, Brooks brings practical, real-world experience implementing secure, automated and compliant infrastructure at scale. At Chainguard, he works closely with federal teams to simplify container security and improve software provenance. Brooks is passionate about enabling secure-by-default environments through modern tooling and open-source innovation.

# Secure Foundations: Hardening the Open-Source Supply Chain for AI Applications

**Mike Barretta, Solutions Engineering Manager, Chainguard •**

mike.barretta@chainguard.dev

## ABSTRACT

As the U.S. Department of Defense (DOD) scales up its use of artificial intelligence (AI)—from battlefield edge computing to strategic decision automation—there’s a growing blind spot: the security of the open-source software these systems rely on.

Modern AI stacks are assembled from thousands of open-source components: machine learning libraries, software development kits, orchestration tools and more. But few programs track where this code comes from or how it’s built and are unprepared to manage the volume of known vulnerabilities they contain. That’s a critical oversight. Threat actors are already exploiting weak links in the open-source ecosystem, and the DOD’s AI initiatives are not immune.

This session examines the challenges and corresponding solutions concerning risks to the open-source software supply chain of AI applications. We’ll discuss the hidden risks in modern AI development, why securing the base layers of the software stack is essential to trustworthy AI and what a secure-by-default pipeline looks like in practice.

**BIO:** Mike Barretta leads Chainguard’s public sector solutions engineering team, focused on helping ensure the federal government receives its fair share of the future. Barretta has worked across civilian, defense and intel programs in a variety of roles—software developer, data scientist, solution architect—for a variety of organizations—system integrators, consulting companies, software vendors—with the common purpose of creating and championing technologies and techniques for simplifying the extraction and utilization of information from lots of data.

Having witnessed the ever-increasing threats to those systems, Barretta is now focused on methods and mitigations to secure them.



# Standardize To Secure: Adopting Secure Software Baselines for the Mission

**Natalie Somersall, Principal Field Engineer, Chainguard •**

natalie.somersall@chainguard.dev

## ABSTRACT

The rise and increased prevalence of software supply chain attacks, the strengthened security requirements of compliance frameworks and the speed and complexity of automated software development and build processes have all driven the need for open-source standardization, often called golden image or base image programs.

But while DevOps and security teams recognize how critical open-source standardization is, few feel comfortable tackling a large and fragmented challenge like open-source software delivery, especially across diverse and disparate mission needs.

Join a fun-filled presentation to hear real-world stories about best practices and common pitfalls that you should be on the lookout for when adopting or building a golden image program.

Audience members will walk away with a clear understanding of the right change management milestones to keep in mind, the critical implementation criteria and the most compelling use cases to make developers more productive and deliver secure open-source software from the start.

**BIO:** Natalie Somersall is a principal field engineer at Chainguard, focused on helping public sector organizations secure their software supply chains. She has spent her career supporting national security and public service missions—designing, building and leading complex systems in highly regulated environments at a major systems integrator.

Her path has taken her through roles in project management, systems engineering and education, giving her a broad perspective on how to solve hard problems in high-stakes environments. Somersall is passionate about empowering engineers to build secure, resilient systems that serve the mission—and about advancing diversity and inclusion across the technology community.

# Navigating the Quantum Era: A Proactive Approach to Post-Quantum Cryptography

**Phil Brown, Chief Architect, Army, Defense Agencies and Special Operations Forces,**  
**Cisco** • philipbr@cisco.com

## ABSTRACT

Cisco is actively engaged in developing and implementing post-quantum cryptography (PQC) to secure its networks, applications and data against the emerging threat posed by quantum computing, which could act as a “game-changer” for assured voice and data communications at echelon to secure data. The company’s comprehensive strategy focuses on a seamless and proactive transition from classical cryptographic methods to quantum-resistant algorithms, emphasizing the protection of boot integrity, control plane integrity and data plane integrity across its infrastructure. Cisco collaborates closely with leading organizations such as the National Institute of Standards and Technology (NIST) and the Internet Engineering Task Force (IETF) to validate and integrate standardized PQC algorithms into its solutions, ensuring interoperability and robust security. Rather than an immediate overhaul, Cisco advocates for a phased, incremental deployment approach, integrating hybrid cryptographic models that combine classical and quantum-safe techniques during the transition period. This includes evaluating the impact of PQC on both existing and future networking hardware, ensuring that its routers, switches and security appliances can seamlessly support new cryptographic primitives. Furthermore, Cisco is developing quantum-resistant software products, including crypto software libraries that support NIST’s PQC algorithms and protocol standards.

Cisco has been actively developing and deploying post-quantum trust anchors designed to resist attacks from large-scale quantum computers, with new quantum-safe editions of Secure Boot and Cisco Trust Anchor Technologies, implementing the new NIST PQC standards, anticipated soon. Notably, some existing products, such as the Cisco 8100 router, Cisco Catalyst 9500 network switch and Cisco Firewall 4215, already provide quantum-safe secure boot using hash-based signatures, a precursor to the NIST-approved LMS, with Cisco PQC hardware based on the new NIST standards expected to be available in late 2025 or 2026. Beyond hardware and software, Cisco is evolving its cloud-native security solutions and zero-trust architectures to incorporate quantum-resistant authentication and encryption, aiming to protect sensitive data in transit and at rest. The company is also a founding member of the Linux Foundation’s Post-Quantum Cryptography Alliance, including the Open Quantum Safe project, to facilitate agreement on standards implementation and smooth the transition. To accommodate new algorithms, Cisco is working on incorporating PQC algorithms into transport protocols like TLS, SSH and IKEv2, in parallel with IETF’s efforts to release key standards.

**BIO:** Phil Brown is a retired U.S. Army chief warrant officer and currently serves as the chief architect for Army, Defense Agencies and Special Operations Forces at Cisco. With a distinguished 20-year career in the Army, Brown's diverse assignments spanned various roles, with a primary focus on tactical operations. He spent much of his service with the 101st Airborne Division and managed two regional hub nodes as a network engineer, ensuring mission-critical communications in demanding environments.

Brown's journey in the communications and technology field began in 1999, when he earned his first Cisco certification. Over the past 25-plus years, he has cultivated a deep expertise in networking and technology, continuously evolving alongside advancements in the field. In his current role at Cisco, Phil leverages his military and technical experience to design innovative solutions that meet the unique needs of defense and special operations communities.

Outside of work, Brown is passionate about mentoring others in the technology and military communities, sharing his knowledge to inspire the next generation of leaders in both fields.

# Cole Engineering Services

**Stuart Armstrong, CTO, Cole Engineering Services Inc. • [stu.armstrong@cesicorp.com](mailto:stu.armstrong@cesicorp.com)**

## ABSTRACT

The rapid proliferation of artificial intelligence (AI) across defense applications demands new strategies to shorten development timelines while maintaining rigorous performance and security standards. This presentation explores how high-fidelity simulation environments can be leveraged to accelerate the design, training and validation of AI algorithms, focusing on two use cases: training AI models for object detection and developing AI agents capable of reasoning through complex courses of action (COA).

For object detection applications, simulation offers the ability to generate large, diverse and precisely labeled datasets under controlled conditions, mitigating the cost and security challenges associated with real-world data collection. By synthetically varying environmental conditions, sensor characteristics and target presentations, developers can expose algorithms to edge cases and rare events that are impractical to capture otherwise.

In the realm of cognitive agents, simulation provides a sandbox for modeling dynamic operational environments where AI systems can iteratively explore COA options, learn from outcomes and refine decision-making processes without operational risk. This approach not only accelerates development cycles but also enhances confidence in AI performance prior to deployment.

**BIO:** Stu Armstrong is the chief technology officer at Cole Engineering Services Inc., where he leads the integration of cutting-edge technologies—including AI/ML, AR/VR/XR and 5G edge computing—into training and simulation systems supporting the U.S. Department of Defense and allied missions.

With more than two decades of experience in defense modeling and simulation, Armstrong has worked extensively across both the U.K. and U.S. defense sectors, specializing in transitioning innovative research into operational capabilities. He was instrumental in securing and delivering the U.S. Army's Synthetic Training Environment, one of the largest and most ambitious modernization efforts in military simulation.

Armstrong oversees CESI's internal research and development portfolio, drives strategic technology partnerships and sponsors corporate initiatives focused on quality and process excellence, including CMMI and ISO compliance. His career highlights also include pioneering the world's first augmented reality rehabilitation system for wounded veterans and developing augmented reality training systems for complex naval operations.

He is passionate about building high-performing technical teams and fostering a culture of purpose-driven innovation that bridges emerging technologies with real-world mission success.

# From Data Chaos to Clarity: Powering Army Missions With Unified, Actionable Intelligence

**Josh Brunvoll, Senior Solutions Engineer, Cribl** • [jbrunvoll@cribl.io](mailto:jbrunvoll@cribl.io)

## ABSTRACT

Today's U.S. Army faces an overwhelming volume and variety of data—from battlefield sensors and intelligence, surveillance and reconnaissance platforms to cyber intel and open-source feeds. This session explores how modern, vendor-neutral data architectures can help the Army unify fragmented sources, enrich data in real time and visualize insights through dynamic, mission-tailored dashboards. Attendees will learn how to accelerate decision-making, enhance situational awareness and build a real-time common operating picture—all without overhauling existing infrastructure.

**BIO:** Josh Brunvoll is a senior solutions engineer at Cribl, leveraging seven years of experience in big data and more than three years as a Cribl customer in the federal contracting space. Before joining Cribl in October, he led initiatives that integrated complex data tools to enhance decision-making and operational efficiency. With a deep understanding of data challenges from both the customer and engineering perspectives, Brunvoll now helps organizations optimize their observability pipelines and maximize the value of their data with Cribl's innovative solutions.

# Hacked From Above: Stopping Adversaries Who Launch Attacks From the Cloud

**Jeff Worthington, Public Sector Executive Strategist, CrowdStrike •**

jeff.worthington@crowdstrike.com

## ABSTRACT

As the U.S. Army accelerates digital transformation and embraces cloud-first initiatives, adversaries are exploiting gaps across hybrid environments—leveraging the cloud plane not just as a target, but as a launchpad for broader attacks. Modern cyber actors—especially nation-states like China and Russia—are adept at exploiting misconfigurations, abusing federated identity and establishing persistent access through cloud-native services that bypass traditional perimeter defenses.

In this session, CrowdStrike will examine how adversaries weaponize the cloud to move laterally between cloud and on-premise information technology (IT) assets, using the cloud control plane as a vector to escalate privileges, execute reconnaissance and disrupt mission-critical operations. We'll highlight real-world threat actor tradecraft, provide insight into how the U.S. Department of Defense's (DOD's) attack surface has evolved and discuss how the convergence of zero-trust principles with cloud-native security can close critical gaps.

Attendees will gain:

- A threat-focused understanding of adversarial activity in cloud environments
- Insights into cross-domain attacks that begin in the cloud and target on-premise assets
- Best practices to harden identity, protect workloads and operationalize threat intelligence across hybrid deployments

Cloud is not just infrastructure; it's a warfighting domain. Defending it requires continuous visibility, identity enforcement and a proactive, threat-informed posture.

**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 the nation's most vital information network across the globe.

Worthington 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 both Presidents Bush and Obama.

His leadership and executive operational experiences include information security, IT governance and strategy, network/systems operations, and implementation/integration of robust enterprise systems and services.

# Information Advantage at the Edge: Multimodal Search in a Tactical Form Factor

**Sean MacKirdy, Area Vice President, DOD, Elastic • [sean.mackirdy@elastic.co](mailto:sean.mackirdy@elastic.co)**

## ABSTRACT

As the U.S. Department of Defense (DOD) accelerates efforts to operationalize Combined Joint All-Domain Command and Control (CJADC2)—as well as its service-specific implementations such as the U.S. Army's Project Convergence—the need for interoperable, scalable and edge-capable data capabilities has never been greater. Central to achieving this vision is the ability to conduct multimodal search (MMS) across diverse, distributed and often disconnected data environments.

The Ukraine conflict has underscored the urgency of enabling small, mobile, tactically resilient nodes that can operate under constant threat from drones, long-range fires and electronic warfare attacks. Elastic's Edge Kit delivers critical capabilities in these denied or degraded conditions by enabling real-time search and analytics at the tactical level, without dependence on persistent reachback or cloud access.

Elastic will demonstrate how its MMS platform can be deployed at the tactical edge in a form factor as small as a carry-on-approved “Edge Kit,” mirroring the design and scale of systems already deployed by cyber protection brigades. This compact solution, leveraging a ruggedized server with integrated NVIDIA GPUs, brings the power of high-performance computing, search and AI inference directly to the warfighter, enabling decision dominance at the speed of relevance.

Unlike traditional keyword-based tools, MMS fuses disparate modalities, text, imagery, audio and video, into a unified search experience. This cross-domain capability is essential for modern operations, where mission-critical insights are often hidden within nontraditional data types or siloed repositories. Whether analyzing dense policy documents, full-motion video from ISR platforms or training archives, warfighters can now derive actionable insights through intuitive, AI-enabled search capabilities.

To bring this vision to life, Elastic will showcase a forward-leaning demonstration of an integrated MMS solution using its industry-leading vector database and a locally hosted large language model, all running on the Edge Kit itself. This “art of the possible” demonstration illustrates how CJADC2-aligned forces can unlock operational insights across all data types, enabling faster kill chains, better coordination across echelons and smarter use of scarce bandwidth.

By bridging the gap between core enterprise capabilities and tactical edge needs, Elastic provides a powerful enabler for the DOD's data-centric modernization strategy. This solution enhances mission effectiveness, accelerates data-to-decision timelines and supports the broader objectives of CJADC2, Project Convergence and cross-domain mission integration, ultimately empowering a more agile, informed and resilient joint force.

**BIO:** Sean MacKirdy has more than 25 years of experience in the information technology industry. His career began in software development and Unix systems administration, moved to high-performance computing with Silicon Graphics, then transitioned to sales and sales leadership with Cisco. In his nearly 18 years at Cisco, MacKirdy worked in the U.S. public sector for 12 years and in country leadership outside of the United States in Cisco's emerging markets group for six years.

In the years since leaving Cisco, MacKirdy was the vice president of digital transformation for a SLED-focused partner in the Rocky Mountain region (Advanced Network Management); sales director for the U.S. Air Force and COCOMs at Splunk; and, most recently, sales leader for the U.S. DOD at Cohesity. Today, MacKirdy leads Elastic's DOD efforts. He is passionate about connecting customers with the right technology portfolio to solve problems in the spaces of predictive analytics, AI and machine learning, data fusion and more.

# Enabling MPE and ACE: Decision Dominance With AI/Gen AI Data Integrity

**John N. Carbone, Ph.D., Senior Technical Director and Chief Solutions Architect, Everfox** • john.carbone@everfox.com

## ABSTRACT

As artificial intelligence (AI) and machine learning (ML) expands across defense, intelligence community and multidomain mission partner operations, AI data and models must support complex distributed multiclassification missions. Therefore, model ingestion, data integrity, data flow enforcement and data access become especially complex. Missteps can dramatically affect lives and mission and simultaneously increase the attack surface. This interactive discussion explores how to accelerate AI, generative AI (GenAI) and agentic AI employment to support and secure the progressive use of AI/ML across heterogeneous distributed multiclassification missions at the enterprise and the edge.

### What attendees will learn:

Challenges and solutions for enabling AI/GenAI/agentic AI/ML solutions to support distributed multiclassification missions; enabling rapid, distributed, cross-domain access, administration and model adaptation for AI, GenAI and agentic AI platforms; threat removal for AI, GenAI and agentic AI tools, platforms and data pipelines; and unidirectional flow enforcement for high-threat AI, GenAI and agentic AI deployment.

**BIO:** For 37-plus years, John Carbone has served the defense industry as an engineering fellow, chief science adviser, technology director, chief engineer for innovation, chief data scientist and academia for eight years as an adjunct professor of applied AI (including AI ethics and security) and data science. Carbone currently serves as senior technical director and chief solutions architect at Everfox LLC, while developing and teaching transformational master's and Ph.D. curriculum on applied artificial intelligence, self-learning machines and applied data science at Baylor and Southern Methodist University. Carbone has also been selected for insights and spoken on multiple AFCEA TechNet AI and mission partner environment (MPE) panels and DAFITC Tech Talks.

His national and international innovations and patents were instrumental in forging bridges between high-performance computing and big data/cloud warfighting architectures, C5ISR enterprise, non-kinetic ISR algorithms, MESH comms architecture, UAV sensor fusion, JADC2 dominance-focused 5G designs, dynamic DDIL comms, AI cognition, space C2 and recent space-based SDWAN and cross-domain cybersecurity, each enabling rapid fielding of vital weapon systems across ground, sea, air and space and MPE.

Lastly, Carbone has authored 100-plus AI, engineering and data science publications and books, including AI-based cybersecurity, mining big data to improve national security, multidisciplinary systems engineering and applied cyber physical systems, to name a few. His newest AI book by Springer Publishing discusses nuances of chatbots and large language models, “AI Chatbots: The good, The Bad, and The Ugly.”

Carbone’s Research:

[https://scholar.google.com/citations?user=evH9\\_poAAAAJ&hl=en](https://scholar.google.com/citations?user=evH9_poAAAAJ&hl=en)

<https://www.researchgate.net/profile/John-Carbone-3>

# Zero-Trust Application Access and LLM Guardrails for Multidomain Operations and Tactical Data Analytics

**Jim Togher, Major Account Manager, F5 • [j.togher@f5.com](mailto:j.togher@f5.com)**

## ABSTRACT

Join this session to explore how the U.S. Army can enhance application security at the Tactical Operations Center (TOC), in the cloud and at the tactical edge through the implementation of zero-trust application access (ZTAA). Learn how ZTAA goes beyond traditional zero-trust network access (ZTNA) by integrating identity-aware access controls, contextual security policies and continuous monitoring to safeguard both legacy and modern applications, including those powered by large language models (LLMs).

We'll also discuss how to protect critical data analytics in degraded and congested environments, ensuring that data is turned into decisions even under challenging conditions. Learn how ZTAA can mitigate threats like prompt injections and LLM data leakage, while optimizing performance and reducing GPU costs. Discover how industry leader F5 is enabling the Army to secure tactical applications and data in a multidomain environment.

### Key Topic Areas Covered:

- **Zero-Trust Application Access (ZTAA):** Exploring identity-aware access controls, contextual security policies and continuous monitoring to protect both legacy and modern applications at the tactical edge.
- **Integration of ZTAA in Multidomain Operations:** How ZTAA supports secure application access at the TOC, in the cloud and across the tactical edge, ensuring seamless operations in degraded and congested environments.
- **Securing Large Language Models (LLMs):** Protecting LLM-based applications from threats such as prompt injections and data leakage, ensuring integrity and confidentiality.
- **Tactical Data Analytics Protection:** Safeguarding critical analytics in multidomain environments, turning data into actionable decisions even in degraded and congested settings.
- **Optimization and Cost Reduction:** Reducing GPU costs while maintaining high performance, security and real-time decision-making in data-intensive tactical operations.

**BIO:** Making a difference in the government community with a focus on supporting the mission. Mentoring and growing a diverse team that fulfills all aspirations with equality. Adopting to technology changes and their impact. Continuing to have fun and learn in life with family and friends.



# From Data to Decisive Action: Google's Security Solution for Multidomain Operations

**Bailey Marshall, Customer Engineer, Google Public Sector • [bnmarshall@google.com](mailto:bnmarshall@google.com)**

## ABSTRACT

Google's integrated security solutions empower the theater information advantage detachment (TIAD) to achieve superior information advantage in support of U.S. Army multidomain operations (MDO). The core of this solution is Google SecOps, providing a unified platform for data sensing, collection and management from diverse cyber and information environment sources. Enriched by Google Threat Intelligence (GTI), the platform offers advanced analytics using AI/ML for proactive threat detection, behavioral analysis and secure generative AI applications for rapid insight extraction from vast datasets. Interactive data visualization within SecOps provides critical atmospheric and actionable intelligence. Comprehensive cybersecurity is delivered through Google Cloud's robust infrastructure, GTI's intelligence and continuous validation by Mandiant Security Validation. Crucially, this integrated approach supports monitoring and influencing the information environment by correlating cyber and information activities, informing influence operations and overcoming intelligence overclassification barriers—all vital for decisive action in MDO.

**BIO:** Bailey Marshall is a cybersecurity professional and U.S. Army veteran with experience managing cyber operations, information technology and security analysis for the U.S. Department of Defense (DOD) and joint agencies. She brings nearly a decade of practice directly managing network teams, planning and executing cyber operations, and developing security strategies in both the private and public sectors. She is always ready to demonstrate that age is just a number when it comes to what young cyber professionals can bring to the table.

As a customer engineer with Google Public Sector, her ability to translate technical methodologies into digestible concepts makes Marshall well-equipped to empower teams of all backgrounds. Her work in this role predominately entails creating customized security solutions to support government and military organizations. She is a team-oriented spearhead for emerging technology with hands-on execution experience with in-depth defense strategies, zero-trust implementation and offensive security.

Marshall has previously served as a security consultant for Mandiant, has been a curriculum developer and instructor for cybersecurity courses within the DOD and is a cybersecurity and information technology adjunct at SNHU.

# Beyond the Hype: Practical AI Integration in Security Automation for Defense Environments

**Brent Kelley, Principal Solution Architect, GuidePoint Security •**

brent.kelley@guidepointsecurity.com

## ABSTRACT

In today's rapidly evolving cybersecurity landscape, the integration of artificial intelligence with security automation platforms presents both unprecedented opportunities and unique challenges, particularly for defense and intelligence organizations. As a no/low code automation platform focused on enabling customers to automate their most critical workflows, Tines has encountered and addressed several key challenges when incorporating artificial intelligence (AI) capabilities into our technology stack.

This presentation will explore how Tines approaches AI not as a standalone solution but as another form of automation—one that enhances human decision-making rather than replacing it. We'll examine the technical and operational hurdles encountered when integrating AI into a platform that serves organizations with stringent security requirements and how these challenges have shaped our implementation strategy.

Specifically, we'll address four critical challenge areas:

- **Extracting Actionable Intelligence:** The difficulty in delivering AI-powered insights that genuinely enhance security operations rather than adding noise. We'll demonstrate how Tines has developed AI features that provide contextual intelligence within automation workflows, allowing security teams to make more informed decisions with less cognitive overhead.
- **Technology Stack Integration:** The technical challenges of integrating with the appropriate AI technology stack while maintaining the platform's security posture and performance. This includes architectural decisions that enable AI capabilities without compromising the core automation engine that customers rely on.
- **Use in Classified Environments -** The unique challenges of AI adoption in classified and cleared environments, where data sovereignty and security clearance requirements create additional layers of complexity. Our "Bring Your Own AI" approach allows organizations to leverage AI capabilities while maintaining complete control over their sensitive data—a critical requirement for defense customers.
- **AI Adoption Risks -** The critical challenges of managing supply chain risks associated with AI models and their training data.

We'll examine how organizations must evaluate the provenance of AI models, secure the software development life cycle when incorporating AI components and implement controls to prevent unintended model

behaviors or data exposures. We'll contrast common industry practices with Tines' approach to securing the AI supply chain while maintaining the integrity of automation workflows in high-security environments.

Throughout the presentation, we'll demonstrate practical examples of how AI can be effectively integrated into security workflows to augment human analysts, provide new insights into security data and create more intuitive interfaces for interacting with automation systems—all while maintaining the security and control requirements essential in defense environments.

By sharing these challenges and our approaches to solving them, this talk aims to provide security leaders with a practical framework for evaluating and implementing AI-enhanced automation in their own organizations, particularly in environments where security cannot be compromised.

**BIO:** Brent Kelley is a principal solution architect at GuidePoint Security.

# The Role of Special Operations EW and Cyber Activities in Great Power Competition

**Herm Hasken, Founder and CEO, HighGround Advisors •**

herm.hasken@hgadvisoryteam.com

## ABSTRACT

National security strategy is underpinned by the concept of “integrated deterrence,” which assumes both tactical and strategic dominance of all domains, including cyber. This requires the SOF and cyber communities to gain access and subsequent custody of an adversary’s most critical assets, credibly threatening unacceptable costs to those assets in order to “create dilemmas,” as the secretary of defense recently stated. In the event of escalation, the United States requires both cyber and electronic warfare (EW) capability to reduce the adversary’s ability to project force or deny access (A2/AD) to mission-critical terrain in order to deliver precision kinetic and non-kinetic effects. The best means by which this can be accomplished is through strategic cyber reconnaissance and immediate delivery of cyber/EW tools provided by the cyber and EW industry and its U.S. government partners.

**BIO:** Herm Hasken served more than 20 years in the U.S. Army as a military intelligence officer, with more than half that time in the SOF community, with his last assignment as the command liaison officer (LNO) from Joint Special Operations Command to director, National Security Agency (JSOC LNO at NSA). He has seven deployments from Desert Storm to Bosnia to Operation Enduring Freedom and Iraqi Freedom, where he earned two bronze stars supporting counter terrorism operations in Afghanistan.

After retirement from active duty, Hasken served another 10 years as a senior civilian intelligence officer in the Defense Intelligence Agency, assigned to U.S. Special Operations Command and U.S. Cyber Command, serving as the director of the U.S. SOCOM Cryptologic Office, U.S. Cyber Command director of exercises and training (J71), and later as senior adviser to the Cyber Command J3 for Special Operations planning and integration.

Upon leaving federal service, Hasken provided staff support to the presidential transition team, contributing to the White House national strategy and policy on cyber warfare and cybersecurity. He became a partner at MarkPoint Technologies, developing and delivering private industry’s most advanced body-worn, handheld and vehicle-mounted electronic detection and electronic warfare equipment to the SOF community.

MarkPoint was acquired in March 2023. Since then, Hasken has begun another chapter as a senior adviser to several small cyber and electronic warfare companies. He has also volunteered time as visiting lecturer at the George Bush Graduate School for Public Policy and Diplomacy, Texas A&M University.

# Securing the Mission Edge: Zero-Trust AI for Cyber Resilience in Multidomain Operations

**Jessica Dapelo, Founder and CEO, Jessica Dapelo Enterprises Inc. •**

[jessica@jessicadapeloenterpriseinc.world](mailto:jessica@jessicadapeloenterpriseinc.world)

## ABSTRACT

As military operations grow increasingly reliant on interconnected systems and AI-enabled platforms, cybersecurity at the mission edge becomes both a vulnerability and a critical advantage. In this presentation, Jessica Dapelo, CEO of Jessica Dapelo Enterprises Inc., explores how zero-trust architecture combined with explainable AI can transform cyber defense across multidomain operations. Drawing from more than 15 years of experience in national security, AI governance and critical infrastructure protection, Dapelo offers a roadmap for building adaptive, intelligence-driven defenses that secure warfighter networks from supply chain to sensor.

The session will focus on operationalizing zero-trust principles in dynamic environments, leveraging AI to detect and mitigate threats in real time and reinforcing decision superiority at the tactical edge. Case studies will highlight implementations supporting the U.S. Department of Defense (DOD), DHS and emergency management agencies, emphasizing how policy, culture and technology must align to maintain resilience in an evolving threat landscape. Attendees will gain practical insights into architecting resilient, AI-augmented cyber systems that protect mission integrity and enhance strategic readiness.

**BIO:** Jessica Dapelo is the founder and CEO of Jessica Dapelo Enterprises Inc., a woman-owned small business specializing in zero-trust cybersecurity, AI-driven risk management and national security consulting. With more than 15 years of executive leadership experience, Dapelo is a trusted adviser to U.S. government agencies, including the U.S. Department of Defense and Department of Homeland Security. She holds active DOD and DHS clearances and a TS Facility Clearance. A recipient of the AFCEA International 40 Under Forty Award, Dapelo is an internationally recognized speaker on AI security, digital transformation and critical infrastructure resilience.

# Quantum Threats and AI Defense: Future-Proofing National Security

**Jessica Dapelo, Founder and CEO, Jessica Dapelo Enterprises Inc. •**

jessica@jessicadapeloenterpriseinc.world

## ABSTRACT

As quantum computing rapidly advances, it poses both unprecedented opportunities and significant risks to national security. Quantum algorithms have the potential to break current cryptographic systems, undermining the confidentiality, integrity and availability of critical information infrastructures. This presentation explores the emerging quantum threats and their implications for cybersecurity, with a particular focus on how artificial intelligence (AI) and zero-trust security frameworks can be leveraged to anticipate, detect and mitigate these risks.

Attendees will gain insight into the evolving quantum landscape, the vulnerabilities it introduces to existing defense mechanisms and the urgent need to develop quantum-resistant encryption protocols. The session will highlight innovative AI-driven approaches for real-time threat detection and adaptive risk management that can future-proof critical national infrastructure. Practical strategies for integrating quantum-safe solutions within existing cybersecurity architectures will also be discussed, empowering organizations and government agencies to stay ahead of adversaries in an increasingly complex threat environment.

Join us to understand the intersection of quantum computing, AI and cybersecurity—and discover how to build resilient defenses that protect our nation’s digital future.

**BIO:** Jessica Dapelo is a seasoned executive leader and founder of Jessica Dapelo Enterprises Inc., a certified woman-owned small business, specializing in cybersecurity, AI governance and zero-trust frameworks. With more than 15 years of experience, Dapelo is recognized for her expertise in AI-driven risk management and digital transformation, supporting federal agencies, including the U.S. Department of Defense and Department of Homeland Security.

Dapelo is an accomplished speaker and thought leader, having presented at major industry conferences such as the Joint Engineer Training Conference (JETC), SAE International and the Cybersecurity Technology & Management Alliance (CTMA). In 2025, she will deliver key presentations at the Waste Management Conference, the SAE Conference in Portugal and the Ransomware Summit. Dapelo’s innovative work has earned her the prestigious AFCEA International 40 Under Forty Award for STEM leadership.



# Partnering for Mission Success: How Juniper Mist AI and Marvis Can Enhance Warfighter Communications and Support Non-Kinetic Dominance

**Michael Maice, Strategic Advisor, DOD, Juniper Networks • [mmaice@juniper.net](mailto:mmalice@juniper.net)**

## ABSTRACT

The TechNet Augusta 2025 theme, “Non-Kinetic Dominance in Multi-Domain Operations,” highlights the vital role of superior information capabilities in achieving mission objectives. We understand that foundational to this dominance is the unwavering assurance of voice and data communications for every warfighter. The increasing complexity of modern military networks and the dynamic nature of tactical environments place immense strain on dedicated signal personnel. In this context, the U.S. Army seeks transformative approaches—not just new hardware, but innovative ways to enhance the capabilities of its existing expert workforce and ensure they have the best possible tools.

Juniper Mist AI and Marvis—a collaborative approach to augmenting the signal corps: Juniper Networks believes a significant opportunity to address these challenges lies in Juniper Mist AI, an AI-native networking platform featuring the Marvis™ Virtual Network Assistant. We envision Mist AI and Marvis not as a replacement but as a powerful AI-driven augmentation for the Signal Corps, akin to providing each unit with tireless, specialized AI assistants focused 24/7 on network health and performance. This collaborative, AI-driven operational model aims to shift network operations from a reactive stance to one that is proactive and predictive, with an acute focus on the warfighter’s end-user experience. Our goal is to help augment human teams, ensuring critical communications are consistently available, reliable and optimized to support their mission.

Key capabilities and potential benefits—AI-powered support for your teams: We believe Juniper Mist AI, with Marvis as its intelligent interface, offers tangible benefits by acting as a supportive extension of the U.S. Army’s signal force:

1. **Proactive & Predictive Assurance—Enhancing Vigilance:** Like a dedicated expert partner, Mist AI leverages advanced machine learning to help proactively identify anomalies (e.g., degrading Wi-Fi, faulty cables, misconfigured VLANs) and predict potential issues before they impact mission-critical services. This preemptive capability, including support for self-driving remediations, can significantly contribute to uptime and reliability, ensuring warfighters have the connectivity they need.
2. **Unparalleled User Experience Focus—Aligning With Mission Intent:** Marvis is designed to help ensure the network understands and delivers on the intent of the communication, directly supporting the warfighter. Rather than just monitoring devices, it provides deep insight into the actual quality

of experience for soldiers using voice, video and data applications, striving to meet and maintain service-level expectations (SLEs) critical for operational demands.

3. **AI-Powered Root Cause Analysis—A Force Multiplier for Troubleshooting:** When issues arise, Marvis can act as an instantly available support tool, providing rapid and accurate root cause analysis, potentially reducing troubleshooting times by up to 90%. Its natural language interface allows personnel to ask, “What is affecting the comms link to Unit X?” and receive clear, actionable answers, helping to reduce cognitive burden and the need for deep expertise at every point.
4. **Enhanced Operational Agility and Supporting the Mission—Streamlining for Success:** By helping to automate routine tasks, providing AI-validated configuration guidance and offering a centralized cloud-managed dashboard (including FedRAMP-authorized Juniper Mist Government Cloud instances), Mist AI can simplify network deployment and management. This aims to free up dedicated signal personnel to focus on strategic, higher-value tasks that directly support the warfighter.

Supporting non-kinetic dominance through collaborative AI-human teaming: By working to transform network operations and augment human expertise with tireless AI capabilities, Juniper Mist AI can help provide the robust, resilient and adaptive communications backbone essential for non-kinetic dominance. Our aim is to empower the U.S. Army with a network that is more autonomous, easier to manage and significantly more reliable, ensuring information flows seamlessly to support the warfighter’s decision-making and operational success at every echelon.\

An invitation to collaborate and experiment: Juniper Networks is deeply committed to supporting the Army’s mission. We welcome the opportunity to partner with the Army and explore how Mist AI and Marvis can act as a powerful force multiplier. We propose collaborative experimentation to validate its efficacy in real-world Army scenarios, showcasing its potential to deliver truly assured communications and contribute significantly to the Army’s information advantage in multidomain operations. We sincerely invite discussions at TechNet Augusta 2025 to explore how this transformative technology can best serve the warfighter.

**BIO:** Michael Maice is a retired U.S. Army warrant officer and technology leader with a direct perspective on modern military communications. His experience spans military deployments to the Middle East and private-sector leadership at Juniper Networks, Archon (a CACI company) and Klas, giving him a practical understanding of delivering mission-critical capabilities in complex environments.

During his military career, Maice served with the 18th Airborne Corps, the Joint Communications Unit and the Joint Communications Support Element. This firsthand experience provided him with deep insights into tactical networking requirements and the operational imperatives of assured communications. He is a recognized thought leader, contributing to publications and podcasts on military technology and secure communications, including CSfC.

At TechNet Augusta 2025, Maice will discuss “Partnering for Mission Success: How Juniper Mist AI & Marvis Can Enhance Warfighter Communications and Support Non-Kinetic Dominance.” Drawing on his expertise with Juniper’s AI-Native Networking Platform, particularly Mist AI and

the Marvis Virtual Network Assistant, he will present a vision for how AI-driven solutions can augment the Signal Corps, acting as specialized AI assistants working alongside dedicated personnel.

His presentation will focus on shifting network operations from reactive to proactive and predictive, prioritizing the warfighter's end-user experience. Michael will explore how a collaborative AI-human teaming approach can provide the robust, resilient and adaptive communications backbone essential for non-kinetic dominance and empowering the warfighter. He welcomes a discussion on how transformative technologies can best serve the Army's mission and enhance soldier capabilities.

# Defending Gray Cyberspace for Combat Power at Echelon

**Adam Rogge, Senior Account Director, Lumen** • [adam.rogge@lumen.com](mailto:adam.rogge@lumen.com)

## ABSTRACT

The U.S. Department of Defense (DOD) struggles to perform functional mission analysis, map, sensor and conduct defensive cyberspace operations for key cyber terrain of defense critical infrastructure (DCI), commercial critical infrastructure (CCI) and its supply chain. In most cases, the DOD does not own and cannot monitor these types of gray cyberspace terrain in real time, yet is reliant upon the terrain for mission assurance. Lack of battlespace awareness may lead to loss of operational availability of mission systems and reduced combat power.

Lumen operates the most peered network of any provider, has more than 2,200 data center connections, ~340K global fiber miles, 4M quantum fiber locations in 16 CONUS states, ~163K on net fiber buildings globally and has more than a 350-plus Tbps global backbone capacity. Additionally, Lumen owns and operates approximately 95% of the DISA backbone. In summary, Lumen can see gray cyberspace the DOD relies upon.

Attendees will learn how Lumen network telemetry is a game-changer for the U.S. Army to provide continuous monitoring, cyber threat intelligence, threat hunting and cyber adversary clearing assistance of DCI, CCI and supply chain friendly gray cyberspace, underwriting combat power at echelon.

**BIO:** Adam Rogge, based in Colorado Springs, Colorado, is a senior account director at Lumen Technologies, focused on meeting Army, Air Force, Space Force and joint operational needs. Immediately prior to joining Lumen, Rogge served in the federal civil service for the U.S. Space Force Delta 6, charged with defensive cyberspace operations for space mission systems. Rogge also concurrently serves in the Colorado National Guard.

# AI Data Challenges Agencies Face and How To Secure, Optimize and Expedite AI Data Operations With Intelligent Data Infrastructure To Ensure Non-Kinetic Dominance

**Jim Cosby, CTO, NetApp** • [jim.cosby@netapp.com](mailto:jim.cosby@netapp.com)

## ABSTRACT

AI data is growing at ever-increasing rates for federal agencies and is becoming more challenging to manage, scale, process and secure. This demands new technologies that optimize data by reducing the size, cost and time to process and manage. At the same time, security threats from cyber and ransomware attacks are constantly increasing, which is demanding stronger data access controls, protection, backup and recovery methods. In this session, we will discuss new capabilities around storing, securing, managing and optimizing AI data, as well as ways to optimize productivity and cost levels helping ensure non-kinetic dominance for the warfighter and multidomain operations environments.

**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 U.S. Department of Defense agencies. Jim has focused on data management and storage security for more than 20 years, including on-premise and hybrid multicloud intelligent data infrastructure technologies, which include multidomain operations and foreign mission 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 NetApp technology.

# Empowering Non-Kinetic Dominance With Unified Data Ingest, Optimization and Classification Using Intelligent Data Infrastructure

**Jim Cosby, CTO, NetApp** • [jim.cosby@netapp.com](mailto:jim.cosby@netapp.com)

## ABSTRACT

Mission and warfighter data is constantly growing for federal agencies and is becoming more challenging to access, process, store and manage in an effective 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 cyber resilient security controls against ransomware attack and must remain flexible to share data across multiple coalition partners. Join this session to learn how NetApp's intelligent data infrastructure and data fabric can integrate efficiency, AI security and flexibility to enable non-kinetic dominance for the warfighter environments as well as multidomain operations.

**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 U.S. Department of Defense agencies. Jim has focused on data management and storage security for more than 20 years, including on-premise and hybrid multicloud intelligent data infrastructure technologies, which include multidomain operations and foreign mission 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 NetApp technology.

# Enabling DOD Agency Non-Kinetic Dominance by Using Intelligent Data Infrastructure To Unify, Secure, Optimize and Expedite Data Operations Across Hybrid Multicloud and Multidomain Operations Environments

**Jim Cosby, CTO, NetApp** • [jim.cosby@netapp.com](mailto:jim.cosby@netapp.com)

## ABSTRACT

Federal agency data is growing at ever-increasing rates and becoming more challenging to access, secure and manage in a timely manner. These challenges are demanding new methods and technologies that can optimize data by assessing, classifying and reducing the footprint, cost and time management. In addition, data must be shared across agencies, coalitions, applications, users and networks regardless of data type. At the same time, security threats from cyber and ransomware attacks are ever increasing, which is demanding stronger data access controls, protection, backup and recovery methods. Join this session to learn how intelligent data infrastructure can enhance data efficiency, security, optimization and flexibility across any hybrid multicloud and across multidomain operations to help ensure non-kinetic dominance.

**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 U.S. Department of Defense agencies. Jim has focused on data management and storage security for more than 20 years, including on-premise and hybrid multicloud intelligent data infrastructure technologies, which include multidomain operations and foreign mission 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 NetApp technology.

# Onebrief Collaborative Planning Platform

**Matthew Work, Head of Growth, Army, Onebrief** • [matthew.work@onebrief.com](mailto:matthew.work@onebrief.com)

## ABSTRACT

Onebrief empowers teams to seamlessly move from planning to execution by delivering real-time, collaborative workflows in a single, secure platform. Purpose-built for dynamic and distributed environments, Onebrief synchronizes data, automates routine processes and enables multiple contributors to update plans, maps, briefings and orders simultaneously, so every stakeholder always operates from the latest information. With robust version control, instant updates that cascade across all products and proven interoperability, Onebrief transforms complex planning cycles into agile, coordinated action, helping organizations execute faster and smarter, together.

Onebrief is deeply committed to fostering innovation and accelerating capability delivery through collaborative experimentation, with interoperability as a core pillar of the platform. Onebrief provides APIs built to OpenAPI specifications, enabling seamless integration with a wide variety of government and commercial systems. The platform already links to key U.S. Department of Defense tools such as VJOC, Maven Smart System, Power BI and C2IE, and is routinely integrated into joint exercises and planning environments, including events requiring the blending of solutions from multiple vendors. Onebrief's microservices architecture, modular design and proven history of working alongside government and industry partners make us eager and well-positioned to engage in joint experimentation activities, including sharing nonproprietary datasets and establishing shared test environments to demonstrate interoperability and collective value.

In a recent example, Onebrief played a pivotal role in PACIFIC SENTRY 25 by delivering unified, real-time collaboration across the entire operational enterprise, integrating both ashore and afloat units for the first time. It became the PACFLT Headquarters staff's tool of choice for planning and workflow, supporting key events and facilitating faster, more effective decision-making at scale. During the exercise, Onebrief was identified by both PACFLT and USINDOPACOM Joint Force headquarters as a "sustain," one of only three technology solutions highlighted for enduring value, and enabled subordinate units to experience and demand its capabilities for future events. Its live sync, cross-domain accessibility and ability to propagate changes instantaneously empowered planners and commanders to focus on strategy over administration, ensuring execution remained synchronized across large, dispersed teams. Onebrief's proven interoperability laid the foundation for its selection as the core staff workflow solution for upcoming exercises around the globe.

**BIO:** Matthew Work is Onebrief's Army head of growth and an Army special operations forces veteran.



**Dave Dickey, Ph.D., Senior Analyst, Peraton** • dave.dickey@peraton.com

## ABSTRACT

In an era defined by information deluge, fragmented data landscapes and rapidly evolving operational challenges, decision-makers face unprecedented hurdles in maintaining strategic superiority. Recognizing these challenges, Peraton created IRIS: the Integrated Realtime Information System. IRIS is purpose-built to resolve these problems by unifying disparate data sources and transforming vast information streams into actionable intelligence that drives rapid, informed decision-making.

Key Enhancements Tailored To Address Core Challenges:

- **Unified Analytics Dashboard:** Tackling the challenge of fragmented intelligence, IRIS consolidates diverse information—from traditional open sources, global news and social media feeds to tactical human intelligence—into a single, intuitive dashboard. This centralized view minimizes cognitive overload by enabling operators to spot trends and anomalies without switching between multiple systems.
- **Advanced Geospatial and Visual Analytics:** In response to the need for contextual clarity, IRIS integrates interactive, Plotly-powered maps and dynamic visualizations. By providing geospatial context to real-time events—such as conflict zones, protest movements and emerging hotspots—IRIS allows decision-makers to quickly interpret complex data, reducing the risk of information gaps.
- **Real-Time Data Integration and Alerting:** Designed to overcome delays in data processing and integration, IRIS automatically fuses feeds from sources like ACLED, IGMA and ORB. Its real-time alerting and notification system ensures that critical changes in the operational environment are immediately communicated, enabling proactive responses to evolving threats.
- **Enhanced Decision Support Capabilities:** To counteract the limitations of siloed data analysis, IRIS leverages advanced machine learning algorithms and predictive analytics. These tools anticipate emerging trends and potential flashpoints, providing decision-makers with actionable forecasts that support adaptable strategic planning.
- **Improved Collaborative Tools:** Addressing the challenge of disjointed interagency communication, IRIS incorporates secure, integrated collaboration features. These tools foster real-time information sharing and joint analysis across agencies, ensuring that critical insights are disseminated swiftly and efficiently during fast-paced operations.
- **DoD IL5 Compliant Architecture:** Built on Azure Government's robust framework, IRIS meets stringent DOD Impact Level 5 standards, guaranteeing the secure management of sensitive data in high-risk environments while maintaining the pace and accuracy required for modern warfare.
- **Customizable and Adaptive Interface:** Recognizing that each operational theater presents unique challenges, IRIS offers a modular and configurable interface. Users can tailor dashboards, reports and alert criteria to align with specific problem statements—whether addressing data overwhelm, integration delays or analytic bottlenecks—ensuring that every operational need is met.

**BIO:** Dave Dickey oversees the ODIN analytic cell, including assessments for information warfare in Peraton's cyber mission sector. Dickey serves as a lead for analysis and assessments for the operational planning, implementation and assessment services (OPIAS) task order and co-launched Peraton's Operationally Dynamic Information Network (ODIN). Dickey's expertise includes intelligence analysis, foreign policy and the incorporation of artificial intelligence (AI)-enabled methods such as machine learning and generative AI into analysis. Dickey spent over a decade focused on violent extremism and great power competition across a variety of USG customers, including the U.S. intelligence community, U.S. Central Command (USCENTCOM), U.S. Special Operation Command (USSOCOM) and U.S. Indo-Pacific Command (USINDOPACOM). Dickey holds a Ph.D. in international relations with a focus on alliance dynamics and power transition.

# Peraton—AI

**Jeff Berlet, CTO, Peraton** • jeff.berlet@peraton.com

## ABSTRACT

Artificial intelligence (AI) is revolutionizing cybersecurity by enabling faster, more accurate and scalable methods for detecting and responding to threats. In domains like threat hunting, red teaming and malware analysis, AI plays a critical role in identifying sophisticated attacks, simulating adversarial behavior and uncovering malicious artifacts.

### Threat Hunting

1. Threat hunting is the proactive search for hidden threats that evade traditional security tools. AI enhances this process by:
  - a. Anomaly Detection: Machine learning models can baseline normal user, device and network behavior, flagging deviations suggestive of insider threats or advanced persistent threats (APTs).
  - b. Event Correlation: AI analyzes massive log data to correlate events across time and systems, revealing subtle indicators of compromise (IOCs).
  - c. Threat Intelligence Parsing: Natural language processing (NLP) tools extract IOCs from unstructured sources like threat reports or forums, enriching hunt hypotheses.
  - d. Prioritization and Noise Reduction: AI ranks suspicious activities by potential impact, helping analysts focus on critical signals over false positives.

### Red Teaming

2. Red teaming emulates real-world adversaries to test an organization's defenses. AI improves red teaming by:
  - a. Automated Reconnaissance: AI scrapes and interprets open-source intelligence (OSINT) to gather target details at scale.
  - b. Phishing Automation: Language models generate context-aware spear phishing emails, increasing success rates in social engineering simulations.
  - c. Adaptive Attack Simulation: Reinforcement learning enables agents to mimic adversarial behavior dynamically, adjusting tactics based on defender responses.
  - d. Malware Mutation: AI can generate polymorphic payloads that bypass signature-based defenses by automatically altering structure and behavior.

## Malware Forensics

3. Malware analysis involves understanding how malicious software behaves. AI enhances both static and dynamic analysis:
  - a. Malware Classification: Deep learning models classify malware families from binary data, op-code sequences or API call logs with high accuracy.
  - b. Behavior Clustering: AI detects patterns in sandbox-executed malware, grouping samples with similar behavior to streamline analysis.
  - c. Obfuscation Detection: AI models trained on code syntax or graphs uncover structural similarities between obfuscated variants.
  - d. Signature Generation: Tools powered by AI assist analysts in crafting YARA rules or behavioral signatures for new threats.

## Conclusion:

AI significantly improves efficiency, scalability and depth in cybersecurity operations. While challenges like explainability and adversarial manipulation remain, its integration into threat hunting, red teaming and malware analysis is rapidly becoming essential for modern cyber defense.

**BIO:** Jeff Berlet is the chief technology officer for Peraton's Cyber Mission Sector. In this role, Berlet leads the internal research and development activities, solution development, technical workforce development and external engagement with industry partners for Peraton's cybersecurity, electronic warfare and information operations programs. Berlet has more than 20 years of experience within Peraton's heritage companies, including Perspecta, Vencore, The SI Organization and Lockheed Martin. He previously held positions as director, chief engineer, chief technology officer, chief information officer, program manager, lead solution architect and a range of systems engineering roles. Earlier in his career, Berlet worked in a variety of engineering and information technology positions for Eli Lilly and Sun Microsystems.

Berlet previously served as a technical director in Peraton's Space and Intelligence Sector, where he developed technical solutions for the U.S. Space Force, Air Force Space Command and classified space customers. Berlet recently served as the chief engineer for the company's largest classified intelligence program, and he previously supported several cyber programs in the United Kingdom in chief engineer and program manager roles.

Berlet has earned several professional certifications, including International Council on Systems Engineering (INCOSE) Expert Systems Engineering Professional (ESEP), Lean Six Sigma Black Belt, Scaled Agile Framework (SAFe) Agilist, Information Technology Infrastructure Library (ITIL) Foundation, Enterprise Architect Center of Excellence (EACOE) Enterprise Architect and Project Management Institute (PMI) Program Management Professional (PMP). Berlet is an officer and past president of INCOSE Chesapeake Chapter, and he is a graduate of Penn State University (B.S. in computer engineering) and University of Pennsylvania (M.S. in computer and information sciences).

# Peraton—DCO and OCO

Jeff Berlet, CTO, Peraton • [jeff.berlet@peraton.com](mailto:jeff.berlet@peraton.com)

## ABSTRACT

Innovative solutions are needed to meet the dynamic and complex requirements of defensive cyber operations (DCO) and offensive cyber operations (OCO). These innovative solutions must be aligned with current and future mission objectives, deliver operational efficiency through automation and artificial intelligence (AI), and interoperate with existing DCO and OCO architectures and systems. To maximize investments in innovation and deliver efficiencies in operations and support dramatically scaled-up operations to match the threats from near-peer adversaries, defenders and cyber warriors require solutions, including experiential “train as you fight” techniques, tactics and procedures (TTPs) and predictive course of action (COA) generation. As our adversaries continue to advance their cyber capabilities, our nation’s DCO and OCO missions will only be successful if we provide “intel enrichment” to the operations floor and integrate intel, cyber, electronic warfare, information warfare capabilities, best practices and subject matter expertise.

**BIO:** Jeff Berlet is the chief technology officer for Peraton’s Cyber Mission Sector. In this role, Berlet leads the internal research and development activities, solution development, technical workforce development and external engagement with industry partners for Peraton’s cybersecurity, electronic warfare and information operations programs. Berlet has more than 20 years of experience within Peraton’s heritage companies, including Perspecta, Vencore, The SI Organization and Lockheed Martin. He previously held positions as director, chief engineer, chief technology officer, chief information officer, program manager, lead solution architect and a range of systems engineering roles. Earlier in his career, Berlet worked in a variety of engineering and information technology positions for Eli Lilly and Sun Microsystems.

Berlet previously served as a technical director in Peraton’s Space and Intelligence Sector, where he developed technical solutions for the U.S. Space Force, Air Force Space Command and classified space customers. Berlet recently served as the chief engineer for the company’s largest classified intelligence program, and he previously supported several cyber programs in the United Kingdom in chief engineer and program manager roles.

Berlet has earned several professional certifications, including International Council on Systems Engineering (INCOSE) Expert Systems Engineering Professional (ESEP), Lean Six Sigma Black Belt, Scaled Agile Framework (SAFe) Agilist, Information Technology Infrastructure Library (ITIL) Foundation, Enterprise Architect Center of Excellence (EACOE) Enterprise Architect and Project Management Institute (PMI) Program Management Professional (PMP). Berlet is an officer and past president of INCOSE Chesapeake Chapter, and he is a graduate of Penn State University (B.S. in computer engineering) and University of Pennsylvania (M.S. in computer and information sciences).

# Future of Threat Hunting

**Tim Singletary, Director of Emerging Technologies and Solutions, Peraton •**

tsingl01@peraton.com

## ABSTRACT

Large, resourceful nations have dominated warfare throughout history, whether kinetic-based and large armies were involved or covertly and cyber-related. These large nations had the resources both intellectually and economically to sustain the advantage in warfare (and cyber warfare). In today's cyber landscape, just like the guerilla warfare from past conflicts, small, dedicated groups can inflict significant damage on larger countries with a keystroke. With the growing interconnected world, the cascading effect of a single attack can wreak havoc on societies and economies around the world.

At the core of the problem is the lack of visibility and understanding of the millions of data streams that move into and around organizations' networks every day. Current security systems can only process a fraction of these streams in real time. Other security systems rely on IOCs (indicators of compromise) to trigger an alert, which could require hours of human review to determine. The majority of these IOCs are either signature or behavioral-based. If one indicator of the attack is dropped during the analysis phase, the IOC may be missed altogether. Compounding this is that most adversaries are aware of the measures most organizations use to detect threats. Attackers can simply avoid these by varying the attack not to trigger the pattern that causes the IOC to cause an alert. A simple technique is to "stage" the attack from multiple sources or multiple destinations, never creating a single session to execute an attack. Even newer detection methods using state-of-the-art artificial intelligence (AI) have already been proven not to be reliable. Attackers simply send unassociated attack data with the actual attack data to "train" the AI to look for a different signature, pattern or behavior.

Solution:

As cyber threats grow more frequent, sophisticated and damaging, organizations need more than just passive monitoring—they need real-time intelligence, rapid response and proactive defense.

Designed for agility and precision, Peraton's threat hunting capability, ThreatBoard, is a game-changer in cyber threat intelligence (CTI), detection and mitigation. Its state-of-the-art AI and machine learning (ML) capabilities analyze vast amounts of diverse threat data, helping organizations uncover stealthy, persistent and fast-evolving attacks—all from a single, unified dashboard.

ThreatBoard automates the ingestion and synthesis of cyber threat data, transforming fragmented information into a cohesive, real-time operational picture. By mapping relationships among IOCs, threat actors, malware and attack campaigns, analysts can spot patterns faster, predict adversary moves and disrupt attacks before they escalate. The result? Reduced detection and response time, lower analyst fatigue and a more resilient cybersecurity posture.

**BIO:** Tim Singletary is the director of emerging technologies and solutions within the strategic innovation business unit at Peraton. He manages and leads Peraton's portfolio of internal research and development, proof of concepts and client pilots. Singletary connects with federal agencies to advise on defensive cybersecurity architectures, workflows, tools, controls and standards. He oversees Peraton's ThreatBoard capability, an autonomous, data-centric platform for cyber threat intelligence, threat management and threat hunting.

Singletary has 25-plus years of experience in the analysis, design and management of information system security and defensive cyber operations. Some of his extensive experience is with the U.S. Army Regional Computer Emergency Response Team (RCERT-Europe), the U.S. Air Force Research Laboratory (AFRL) in Rome, New York, and several large Fortune 500 companies.

# AI-Driven Security Fortification and Attack Surface Reduction

**Russ Andersson, COO, RapidFort • russ@rapidfort.com**

## ABSTRACT

Artificial intelligence (AI) is creating a multipronged software security challenge because it is being used to exploit software vulnerabilities, while at the same time, AI coding assistants are increasing the volume of software that must be defended. AI code is not inherently more insecure; merely, the volume of it is significantly increasing code base sizes quickly, often without adequate oversight, and thus increases attack surfaces, which leads to security risks and CVE exploitation. RapidFort's experience founding the concept and tooling enabling flow defending highlights four developments relevant to AI coding and its implications for AI.

### **AI Weaponization Is Increasing the Threat Landscape:**

AI is increasing the rate, severity and volume at which software vulnerabilities can be exploited. Software vulnerability exploits have increased 400% year over year and are now the primary attack vector for cloud software. We will profile industry statistics that illustrate this trend.

### **Increased Volume and Velocity Code Releases:**

AI vibe coding is increasing the volume of code being developed, potentially overwhelming security teams. We will profile industry statistics that illustrate this trend.

### **Vulnerability Remediation Windows Are Shrinking:**

Because adversaries weaponize vulnerabilities in 72 days but companies patch in 45 days, this gap provides a window of opportunity responsible for 84% of breaches. Time is everything in cybersecurity.

### **The Need for Flow Defending:**

Flow defending is a term whereby security defenses are built into the software development workflow using highly automated and often AI-based tooling to protect and patch software before it gets deployed, thus closing the software window. It is the complement to the so-called vibe coding enabling AI-generated software to be secured rapidly. State-of-the-art tooling, often AI-based, is able to examine workloads to prioritize and remediate risks automatically.

To address these challenges and the evolving AI-driven threat landscape, RapidFort integrates AI-driven vulnerability intelligence directly into SDLC workflows, enabling teams to tame AI's output, focus on true mission-critical risks and maintain a near-zero CVE state from code commit through live container runtime.



**BIO:** Russ Andersson co-founded RapidFort to pioneer container security that scales with modern DevOps. As COO, he drives product innovation and community collaboration, having led multiple defense customers through FedRAMP and CMMC readiness with AI-driven, run-time-aware security solutions.

# An Architecture for Adversarial AI-Enhanced Red Team Simulation, Testing and Defense

**Christopher Yates, Principal Chief Architect, Red Hat** • [cyates@redhat.com](mailto:cyates@redhat.com)

## ABSTRACT

Artificial intelligence (AI) and machine learning are critical capabilities in the near term to provide depth and breadth of active cybersecurity to increase systems readiness and enhance resilience. In this talk, we will demonstrate and discuss a cybersecurity architecture that provides accelerated alerting, investigation, resolution, reconstitution and remediation. This architecture will discuss maturity models to proceed from traditional human-ops to machine-augmented human decision-making and on to fully autonomous cyber resilience. We will address model training, deployment, management and integration to instrument and automate the full life cycle of systems infrastructure and capabilities across the cyber terrain and measures for control to ensure AI guard rails.

**BIO:** Christopher Yates has worked with the U.S. Department of Defense and U.S. federal government for more than a decade within Red Hat, modernizing information systems and assisting in the adoption of open-source technologies.

# An Architecture for Decision Advantage

**Christopher Yates, Principal Chief Architect, Red Hat • cyates@redhat.com**

## ABSTRACT

Modern doctrine like CJADC2 demands rapid deployment of force and infrastructure to support dynamic, emerging conflict capabilities in an evolving battlespace. This requires the ability to quickly, efficiently and effectively field and operate information systems across traditional enterprise, cloud and edge environments, and ingest and share data across agencies, allies and coalition partners, within a heterogeneous infrastructure environment. In this talk, we will demonstrate an architecture that enables the elasticity, scalability and dynamic agility necessary to ensure readiness and robustness for warfighting systems within the modern CJADC2 construct.

Automation is the foundational capability necessary to quickly, accurately and efficiently deploy, operate and maintain the sophisticated, modern information systems that are necessary to achieve and maintain advantage. Readiness and resilience are critical within the battlespace. Automation is necessary to accelerate the full life cycle of systems from the software development life cycle through to system deployment, scaling and retirement.

Red Hat solutions offer automation for system configuration and operation, providing consistent behavior to permit full cloud elasticity and management capabilities within and across traditional data centers, cloud service providers and edge deployed environments. Whether managing simple web services, complex microservice architectures or sophisticated AI/ML workloads and applications, Red Hat offers automation to enable DevSecOps behaviors and infrastructure as code that supports and enables advanced cybersecurity capabilities for zero-trust architectures, including network microsegmentation, workload resilience and robustness to deliver and maintain decision advantage across heterogeneous networking, hardware and software vendor solutions anywhere.

**BIO:** Christopher Yates has worked with the U.S. Department of Defense and U.S. federal government for more than a decade within Red Hat, modernizing information systems and assisting in the adoption of open-source technologies.

# Harnessing Disparate Data: Red Hat's Integrated Approach to Ingestion, Analysis and Visualization

**Derek Thurston, Associate Principal Solution Architect, Red Hat •**

dthursto@redhat.com

## ABSTRACT

Red Hat offers a robust suite of solutions that directly address the challenge of ingesting, aggregating, analyzing and visualizing data from a multitude of disparate sources and formats. By leveraging a foundation of open-source innovation, Red Hat provides the enterprise capabilities to transform a chaotic influx of information into a clear, interactive and mission-critical digital display.

At the core of Red Hat's offering is Red Hat Integration, a comprehensive set of tools designed to connect diverse applications and data streams across hybrid cloud environments. This suite of technologies is adept at handling the initial problem of importing and ingesting data from multiple feeds and in various formats. It employs enterprise integration patterns to create a unified view of data, regardless of its origin or structure. Key components like Red Hat build of Apache Camel provide more than 200 pre-built connectors, enabling seamless communication with a vast array of systems and data sources. For real-time data feeds, Red Hat AMQ, which is based on Apache Kafka and ActiveMQ, offers a high-throughput, low-latency messaging platform. Furthermore, Debezium, a tool for change data capture, allows for the streaming of updates from databases in real time.

Once ingested, the challenge shifts to aggregation and analysis, a task for which Red Hat's portfolio is equally well-equipped. Red Hat OpenShift, the company's enterprise Kubernetes platform, serves as a powerful foundation for deploying and managing a wide range of database and data analytics tools from both Red Hat's partners and the open-source community, including Apache Spark and Kafka. This allows organizations to build a data aggregation strategy that best suits their needs, whether it involves data consolidation into a central repository or data federation for real-time, on-demand access. For high-speed data processing and analysis, Red Hat Data Grid provides an in-memory, distributed NoSQL datastore, enabling rapid querying of large datasets.

To address the need for an interactive digital display with filtering capabilities, Red Hat leverages Grafana, an interactive data visualization and observability platform. Red Hat OpenShift can utilize Grafana, or other third-party visualization dashboards, to create dynamic dashboards that present complex data in an easily digestible format. These dashboards can be customized with various visualizations and interactive filters, allowing users to drill down into the data and gain mission-relevant insights. This empowers users to move beyond static reports and actively explore the information that is most critical to their objectives.

Red Hat provides a layered, integrated approach to solving the modern data challenge. From the initial ingestion and integration of disparate data sources to the final interactive visualization of mission-critical information, Red Hat's open-source-based solutions offer the flexibility and power to turn data overload into a decisive advantage.

**BIO:** Derek Thurston is an associate principal solution architect at Red Hat and has been working with open-source software since the mid '90s. After graduating from a small merchant marine college in coastal Maine, Thurston landed a job in the IT department at a naval architecture firm in Arlington, Virginia, where he started using Linux. Thurston has worked with SGI and HP/UX systems and did his part to help save the world by converting COBOL programs to four-digit years in the late 1990s. Having worked with a variety of public- and private-sector entities, he has spent more than 25 years helping customers find the right open-source tools and technologies.

# Wireless Fingerprints: How Evolving Tech Redefines Battlefield Risks

**David Baldwin, Cybersecurity Engineer, Savannah River National Laboratory •**

david.baldwin@srnl.doe.gov

## ABSTRACT

Over the past three decades, technology has undergone remarkable transformations, notably in terms of miniaturization and the introduction of advanced capabilities, such as wireless connectivity, smart devices and computerization of phones. In today's digital age, a multitude of portable devices, utilized by both the military and consumers, seamlessly integrate with smartphones and feature wireless functionality. While these advancements offer significant convenience and efficiency in low-risk environments, they necessitate robust safeguards and thorough analysis when users face genuine adversarial threats. This article delves into the array of risks posed to operators by contemporary geolocation tactics and wireless exploitation. It also explores the expanded attack surface introduced by smartphones in critical operations. The focus is on how adversaries can leverage these technologies to compromise the security and privacy of users, highlighting the necessity for stringent protective measures. The article aims to provide a comprehensive understanding of the vulnerabilities associated with modern smart devices in high-stakes scenarios and offers insights into mitigating these risks to enhance operational security. From potential location tracking to the exploitation of wireless communications, the integration of smart technology presents a multifaceted challenge that requires continuous vigilance and innovative solutions.

**BIO:** David Baldwin is a cybersecurity engineer at the Savannah River National Laboratory. His current work specializes in reverse engineering, threat assessment and vulnerability analysis of medical devices and smart-enabled technology.

# Accelerate the MDO Mission With Secure NPEs for Theater AI Operations

**Andrew Whelchel, Lead Solutions Engineering, Federal, Saviynt •**

andrew.whelchel@saviynt.com

## ABSTRACT

The multidomain environment operating for information advantage brings artificial intelligence (AI) theater decision processing and data sensors integration into AI at rates not seen ever before. This presents potential information overmatch opportunities but does require identity cybersecurity attached to AI and theater data analytics matching the speed of the mission in new ways not attempted before.

Essential to success of harnessing the AI and theater data analytics is ability to operate at speed of the mission, particularly with regards to identities, specifically NPEs (non-person entities). This new tooling available for operating at the edge presents the opportunity to accelerate decision processes as well as provide more precise operational outcomes in the field. To deliver these outcomes at the speed of the mission, NPEs must operate securely by applying zero standing privilege to those identities that control and direct the AI and data analytics program capabilities.

Delivering on these outcomes of secure NPEs for AI and data analytics requires an identity security capability with the ability for disconnected resiliency. This identity security brings information advantage capabilities to the theater including:

- Accelerate authorization to AI and data analytics in theater through NPE principles
- Enable cyber risk controls to provide acceleration of deployment of AI and data analytics
- Provide NPE authorization services enabling access to AI data, AI operations and data analytics products even during theater disconnected scenarios

For AI and data analytics in the theater to deliver the speed of the mission, NPEs must be secured with faster authorization and durable security cyber controls for access. The capabilities included as part of this session include details on rapid NPE access authorization, disconnected with hybrid ICAM architecture and demonstration of operational use case scenarios for access to AI and data analytics in theater for information advantage.

**BIO:** Andrew Whelchel (CISSP-ISSAP, ISSEP, CAP, CCSP, CGRC, CSSLP) started in information security and IAM immediately after graduation from the University of Memphis, supporting identity and access management managing Microsoft identity for U.S. federal customers. Later

work transitioned to network infrastructure security and then to consumer identity protection in the role at RSA Security and most recently at Okta and Saviynt. At RSA Security supporting financial services, health care, U.S. federal and other customers, there was focus on identity risk analytics and integration of identity fraud intelligence for cyber crime prevention. In the prior role at Okta and the current role at Saviynt, the focus was on both protecting employees as well as business partner identities for public-sector agencies to reduce cyber risk as well as accelerate capabilities for cloud transformation. Contributions include work as a contributor on the NIST 1800-3 ABAC (Attribute Based Access Control) standard and speaking at events on identity access management and security.



# Mission-Ready ITOps: Leveraging Generative AI for Operational Advantage Across the DOD

**Matt Carter, Solutions Architect, ScienceLogic** • [matt.carter@sciencelogic.com](mailto:matt.carter@sciencelogic.com)

## ABSTRACT

In today's multidomain operational environment, the U.S. Army and broader U.S. Department of Defense (DOD) must process, synthesize and act on vast volumes of information from a growing number of sources. Generative AI is emerging as a strategic asset, transforming information technology operations (ITOps) into intelligent systems that enhance readiness, resilience and mission execution.

This session will explore how generative AI enables rapid ingestion and analysis of data from diverse, mission-critical feeds—structured, unstructured, real-time and historical. We will showcase how AI-driven platforms aggregate and contextualize this information, enabling interactive displays with real-time filters and situational overlays that empower commanders, analysts and support personnel with decisive insights.

Attendees will gain insight into:

- **Data Integration at Scale:** How generative AI ingests and correlates data from sensors, systems and classified/nonclassified networks to enable unified situational awareness
- **AI-Driven Workflow Automation:** How automating ITOps tasks improves tempo, reduces human error and frees up personnel for strategic decision-making
- **Interactive Operational Displays:** How digital dashboards with AI-enhanced filters provide mission-relevant visibility tailored to roles and command priorities
- **Operational Agility in Uncharted Scenarios:** How AI can detect anomalies, predict system failures and propose courses of action—even in unanticipated environments

Conclusion:

Generative AI is more than technological evolution; it is an operational imperative. For the U.S. Army and DOD, it provides the cognitive edge required to outpace threats, secure infrastructure and dominate the information environment. Join us to see how AI-driven ITOps is reshaping the way the military prepares, operates and adapts at mission speed.

In today's multidomain operational environment, the U.S. Army and broader DOD must process, synthesize and act on vast volumes of information from a growing number of sources. Generative AI is emerging as a strategic asset transforming ITOps into intelligent systems that enhance readiness, resilience and mission execution.

**BIO:** Matt Carter is a technologist supporting the DOD with deep expertise in secure IT operations, cloud infrastructure and mission-aligned automation. As a solutions architect at ScienceLogic, Carter serves as a subject matter expert in artificial intelligence for IT operations (AIOps), with a specialized focus on the use of generative AI to transform operational visibility, resilience and decision-making across DOD networks.

Carter works directly with IT leaders and mission stakeholders across the DOD to align AI capabilities with real-world operational demands. He leads efforts to deliver measurable improvements in situational awareness, incident response and infrastructure performance by deploying platforms that convert complex, multidomain data into actionable intelligence. His mission-first approach ensures that generative AI and automation are not just technical enhancements but strategic enablers of faster, smarter and more resilient operations.

Prior to ScienceLogic, Carter served as a systems analyst at 1901 Group, where he specialized in VMware, Linux, AWS and large-scale network monitoring. His background includes system deployment, requirements analysis and hybrid IT operations, giving him firsthand insight into the tactical and technical challenges of modern military IT environments.

Carter brings a strong technical foundation and an unwavering commitment to mission assurance, delivering resilient, adaptive and intelligence-driven IT operations that enable sustained mission success.

# The Making of Operator X: The GenAI Platform To Transform Cyber at the Edge

**Nate Delgado, Software Product Owner, SealingTech •**

nathan.delgado@sealingtech.com

## ABSTRACT

This presentation covers the challenges and evolution of SealingTech's groundbreaking generative AI (GenAI) platform: Operator X.

Operator X uses large language models (LLMs) and retrieval-augmented generation (RAG) to enhance the efficiency and effectiveness of the cyber warfighter. Its direct integrations with U.S. Department of Defense (DOD) cyber tools help defenders stay ahead of adversaries and ensure the resilience of defensive operations.

SealingTech prioritizes meeting customers where they are, by integrating with and enhancing their tool sets and existing systems. This focus presents the challenge of tailoring AI for defensive cyber operations while maintaining a form factor that excels at the edge.

The team selected an agentic approach, developing agents optimized for integration with DOD tools—yet flexible enough to continuously improve functionality while adapting to evolving models. The presentation will explore how these challenges were overcome and how the solution evolved from a paradigm of fixed LoRAs to one of adaptable reasoning.

Optimizing Operator X for deployment in SealingTech's varied customer environments presented significant challenges, particularly concerning mobility and cost. Given the high price of AI-capable GPUs due to their vRAM consumption, a traditional server design posed a barrier to fielding the platform on forward-deployed missions.

The presentation will share how optimizing the selection of models via a custom testing pipeline resulted in a 3x decrease in vRAM requirements, enabling an exceptionally mobile solution.

Operator X continues to evolve and expand its reach and capabilities based on the warfighter's mission needs. The presentation will conclude with next steps for Operator X, highlighting its key position within SealingTech's Cyber Hunt Kit platform.

**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 specifi-

cally 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's degree in economics from the University of Southern California (USC).

# Achieving Decision Dominance: How ServiceNow Empowers Mission Command Through Data-Driven Insight

**Michael Longoria, Senior Account Executive, U.S. Army, ServiceNow •**

michael.longoria@servicenow.com

## ABSTRACT

Today's fast-paced, threat-filled operational landscape necessitates rapid, confident and decisive responses. Unfortunately, too often, disconnected data, sensor and alert noise, and manual processes create a fog that can delay critical decisions. Downstream, this puts mission success and warfighter safety at risk.

To overcome these challenges, ServiceNow delivers a mission-ready, resilient AI platform that transforms complex, distributed data into actionable insight. Whether in garrison or at the tactical edge, the AI platform supports multidomain operations by unifying information from a wide range of sources (which could include UAVs, cyber feeds and ground systems) into a single, intelligent system built for action.

The AI platform enriches current data streams with contextual value, such as mission-relevant geospatial tagging, to further enhance decision clarity. Even in denied, degraded, intermittent or limited (DDIL) environments, commanders maintain access to a continuously updated common operational picture once connectivity is restored.

Through built-in intelligence and flexible filters, the AI platform enables predictive analysis based on key mission indicators, such as movement patterns, threat activity or sustainment thresholds, empowering faster, more informed decisions. These insights can be directly integrated into mission command workflows, triggering alerts, updating task statuses and driving coordinated responses across dispersed units.

Thanks to its low-code design and open integration framework, the ServiceNow AI platform connects seamlessly with existing U.S. Army systems, simplifying modernization without the need for major infrastructure changes. The result is a more agile, responsive command environment where data flows to the right people at the right time to support decisive action.

Don't miss this session to see how intelligent data fusion and mission-ready workflows can sharpen decision advantage, bringing speed, clarity and control to today's contested battlespace.

**BIO:** Michael Longoria is a driven and competitive sales executive with a proven record of achieving objectives in fast-paced, technical environments. With 14-plus years of military

and technology sales experience, he has applied strong problem-solving, organizational and interpersonal skills to IT management, customer service, public speaking, negotiation, project management and cybersecurity. Longoria is a proven leader experienced in building cross-functional teams and has excelled in complex, diverse and austere multicultural environments. He is committed to the success of prospective and current clients to better achieve the realization of their organization's mission-critical priorities and key initiatives. His key attributes include a proven track record of successful prospecting, mutually beneficial negotiations and strong relationship growth. Longoria is experienced in developing rapport, building relationships and influencing high-ranking, key decision-makers. He excels both independently and as a team player, proficient at creating effective presentations and developing opportunities to drive organizational quotas. He has a passion to further his own education in the field of technology. He is always looking for opportunities to better himself while helping those around him reach their fullest potential.

# Empowering the Theater Information Advantage Detachment (TIAD) With a Unified Platform for Multidomain Information Dominance

**Michael Longoria, Senior Account Executive, U.S. Army, ServiceNow •**

michael.longoria@servicenow.com

## ABSTRACT

ServiceNow's AI-enabled platform equips the U.S. Army's Theater Information Advantage Detachment (TIAD) with a comprehensive, mission-ready solution to manage, integrate and execute information activities across a theater of operations. Aligned with TIAD's operational focus, this unified platform supports all critical functions: data sensing and collection, secure data management, advanced analytics, visualization, cybersecurity and influence within the information environment.

Key Capabilities Include:

- Automate data sensing and collection using ServiceNow's Integration Hub and edge connectors to ingest structured and unstructured data from multidomain sensors, open-source intelligence and allied systems complete with geotagging and normalization to support a unified data architecture.
- Manage data securely and collaboratively through life cycle governance, tagging and federation features, ensuring data integrity and accessibility across joint and coalition partners.
- Generate advanced analytics and insights with AI/ML models that correlate indicators across the information environment, enabling predictive insights, pattern detection and sentiment analysis to assess adversary narratives and operational risk.
- Visualize mission-relevant data through real-time, role-specific dashboards powered by Performance Analytics, giving commanders and operators the situational awareness needed to act with precision.
- Enforce comprehensive cybersecurity with embedded zero-trust architecture, continuous monitoring and automated compliance to safeguard sensitive data and maintain mission assurance.
- Integrate information operations through a single interface for campaign planning, messaging workflows, influence assessment tracking and automated reporting.

This integrated, scalable approach empowers the TIAD to deliver theater-level information advantage in support of U.S. Army multidomain operations (MDO), synchronizing informational power with kinetic and non-kinetic effects across all domains.

Join us to explore how ServiceNow enables TIADs with a unified, secure AI platform for sensing, analyzing and acting on information, supporting influence, agility and decision dominance in the modern battlespace.

**BIO:** Michael Longoria is a driven and competitive sales executive with a proven record of achieving objectives in fast-paced, technical environments. With 14-plus years of military and technology sales experience, he has applied strong problem-solving, organizational and interpersonal skills to IT management, customer service, public speaking, negotiation, project management and cybersecurity. Longoria is a proven leader experienced in building cross-functional teams and has excelled in complex, diverse and austere multicultural environments. He is committed to the success of prospective and current clients to better achieve the realization of their organization's mission-critical priorities and key initiatives. His key attributes include a proven track record of successful prospecting, mutually beneficial negotiations and strong relationship growth. Longoria is experienced in developing rapport, building relationships and influencing high-ranking, key decision-makers. He excels both independently and as a team player, proficient at creating effective presentations and developing opportunities to drive organizational quotas. He has a passion to further his own education in the field of technology. He is always looking for opportunities to better himself while helping those around him reach their fullest potential.



# Overcoming Barriers to Trusted AI Integration for Mission Advantage

**Nathan Bernache, Senior AI Specialist, Solution Consulting, ServiceNow •**

nathan.bernache@servicenow.com

## ABSTRACT

Generative artificial intelligence (GenAI) and agentic AI are evolving rapidly. Despite their potential, these capabilities have yet to be fully realized in operational environments given the tremendous speed of advancements. Key barriers, such as infrastructure constraints, lack of enterprise-grade security and limited application-level integration, continue to slow progress and prevent these technologies from delivering their full value in mission environments.

At ServiceNow, we're addressing these challenges with a secure, mission-aligned AI platform designed to help the U.S. Army adopt AI with confidence. Our approach enables trusted, scalable AI integration while aligning with U.S. Department of Defense security requirements, without adding risk or complexity for warfighters.

Key AI challenges, such as data readiness, compute demands and trust, are addressed through our optimized architecture:

- **Security-first AI:** Leveraging IL5 commercial cloud environments with strict access controls and mission-specific use case approval
- **Flexible AI adoption:** Modular LLMs and GenAI capabilities integrated at the application layer—no need for prompt engineering or vendor lock-in
- **Human-in-the-loop governance:** Ensures ethical, auditable AI use aligned with Army policies and mission assurance

This session will discuss key lessons learned. Successful AI integration isn't just about the tech; it's about meeting mission needs without adding operational burden.

Join us to learn how you can overcome common barriers to AI adoption, gaining real-time insight, accelerating decisions and maintaining the tactical edge in an increasingly information-driven battlespace.

**BIO:** Nathan Bernache is a senior AI specialist in solution consulting.

# Strengthening Decision Superiority Through Unified, Mission-Relevant Data

**Rick Camensky, Federal Sales Director, ServiceNow •**

richard.camensky@servicenow.com

## ABSTRACT

In today's dynamic and contested battlespace, the U.S. Army faces an urgent need to make faster, smarter decisions across increasingly distributed operations. Yet, warfighters and commanders alike are often hindered by fragmented data environments, disparate formats and delayed access to mission-critical information.

In this session, attendees will learn how to transform structured, unstructured and streaming data into actionable insight to support the Army's drive for decision dominance, greater interoperability and enhanced cyber readiness. We will explore a secure, scalable data integration approach that seamlessly ingests and aggregates information from sensors, systems and external partners into a single, unified operating picture.

Attendees will discover how this solution's real-time data access and AI-powered analytics empower commanders to rapidly detect anomalies, understand operational conditions and act decisively in time-sensitive environments. Leveraging ServiceNow's Workflow Data Fabric and Platform Analytics, the AI platform delivers interactive dashboards with mission-relevant filters, drilldowns and natural language processing to streamline information synthesis and reduce cognitive load.

By implementing this future-ready approach, attendees will learn how to unlock new levels of mission agility, resilience and overmatch in today's complex operational environments. The session will highlight key capabilities that support faster, more informed decision-making, including:

- Seamless data integration and ingestion from diverse sources
- Intelligent data aggregation and interactive visualization
- AI-powered analytics and anomaly detection
- Natural language processing for enhanced human-machine dialogue

Join us to explore how this solution-oriented approach can transform your ability to achieve decision dominance in today's contested battlespace.

**BIO:** Rick Camensky is an experienced federal sales director with a demonstrated history of success. He is skilled in enterprise software, security, go-to-market strategy and the importance of strategic partnerships.

# Turning Complexity Into Clarity: Unifying Asset, Operational and Strategic Data To Drive Mission Outcomes

**Andrew Scherer, IT Transformation Solution Sales Manager, Federal, ServiceNow** •  
andrew.scherer@servicenow.com

## ABSTRACT

The U.S. Army faces a growing volume of information that often exceeds the capacity of current systems to manage it effectively. At the same time, leaders are under increasing pressure to use resources more wisely while keeping pace with shifting priorities. Meeting these expectations takes more than simply collecting data. What is needed are systems that can make sense of complexity in ways that support real-time decision-making and inform long-term planning.

This session explores how a unified digital platform can connect data across IT systems, operational networks and business processes to support a wide range of Army missions. A connected approach helps the Army move beyond siloed tools and outdated reporting by giving leaders a clearer understanding of what they have, how it is being used and where adjustments are needed to keep operations aligned with mission demands.

The discussion will focus on how an integrated platform supports mission-critical decisions through capabilities that:

- Aggregate data from multiple systems and format into a single, trusted operational view ★
- Surface cost savings and reduce risk through automation and intelligence-driven insights ★
- Deliver real-time visibility into usage, life cycle status, performance and alignment to mission priorities ★
- Simplify compliance and audit readiness by connecting operational data with policy and governance requirements ★
- Deliver interactive dashboards with filters that help users surface mission-relevant data, assess current conditions and support planning based on real-time operational context ★
- Leverage built-in AI to accelerate decision-making and introduce emerging agentic AI capabilities that can act on behalf of users based on context and mission relevance

Finally, the bullets marked with a star (★) highlight capabilities delivered through ServiceNow solutions that have already been adopted across the Department of the Army. These capabilities are delivered through software asset management and hardware asset management, both of which play a key role in strengthening the Army's ability to manage its assets efficiently and in line with operational and policy requirements. Because these solutions are already in use at scale, Army commands can build on the existing investment without incurring additional licensing costs. This accelerates time to value and helps reduce operational burden.

**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-plus years of selling IT services directly to both the U.S. Department of Defense (DOD) and civilian agencies. Andrew'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.

# Operational Awareness Through Data Aggregation, Analysis and Interactive Visualization With SolarWinds

**Scott Pross, Vice President Technical Solutions, Monalytic, SolarWinds •**

scott.pross@solarwinds.com

## ABSTRACT

In complex and dynamic cyber environments, mission success depends on the ability to rapidly ingest, analyze and act upon data from a diverse range of sources simultaneously.

SolarWinds delivers a comprehensive observability and IT operations platform that empowers military and cyber operations with scalable data ingestion, advanced analytics and interactive visualization capabilities. SolarWinds technology is designed to import and normalize structured and unstructured data from multiple feeds, including logs, metrics, events, configuration data and telemetry from both cloud-hosted and self-hosted environments. In this session you will learn:

1. The SolarWinds approach to providing a unified operational view of disparate aspects IT operations through flexible APIs, native integrations and support for industry-standard formats (e.g., syslog, SNMP, NetFlow, RESTful data sources).
2. How SolarWinds ingests data and employs intelligent analytics and correlation to identify anomalies, trends and mission-relevant patterns. Real-time processing enables proactive detection of system performance issues, network threats and cyber hygiene gaps across U.S. Army IT infrastructures.
3. Ways SolarWinds further enhances operational decision-making by providing customizable dashboards with interactive filters, enabling users to drill down into mission-relevant operational performance without unnecessary fluff. These digital displays can be tailored to specific operational roles, command levels or geographic areas of interest—helping commanders, warfighters and analysts maintain situational awareness, prioritize threats and ensure continuity of operations.

When you attend this session, you will get a deep dive into SolarWinds architecture, offering modular, scalable and secure performance, which aligns perfectly with the Army Cyber Center of Excellence's goals of cyber readiness, data-driven decision-making and resilient mission command.

**BIO:** Scott Pross is the vice president of technical solutions at Monalytic, a SolarWinds subsidiary.

# Certify Once, Secure Always: Fast-Tracking Trusted Software to the Mission Edge

**Bryan Whyte, Director, Solutions Engineering, Sonatype** • [bwhyte@sonatype.com](mailto:bwhyte@sonatype.com)

## ABSTRACT

Mission assurance in the modern digital domain requires more than secure code; it demands automated trust, traceability and speed in how software is delivered to the warfighter. As threats increase and systems become more complex, the Department of the Army needs scalable approaches to mitigate supply chain risk while accelerating capability delivery.

This session will explore how a “Certify Once, Use Many Times” strategy, anchored by SBOM automation, vulnerability intelligence and SWFT integration, can dramatically streamline the secure acquisition and reauthorization of COTS software. Drawing on Sonatype’s experience supporting IL6 environments and U.S. Department of Defense (DOD) software factories, we will illustrate how a centralized SBOM registry, AI-enriched validation workflows and policy-enforced governance can replace redundant manual reviews, shorten ATO cycles and elevate trust across interconnected systems.

Attendees will walk away with a reference architecture for SBOM-driven supply chain security, a path to align with EO 14028 and NIST 800-218, and real-world insight into how DOD teams are deploying these practices today to protect the mission, without slowing it down.

**BIO:** After earning a master’s degree in electrical engineering, Bryan Whyte spent more than 20 years developing software applications to test hardware systems such as torpedoes, circuit boards and digital subscriber line (xDSL) modems. During this time, he also contributed to product development for both embedded and distributed enterprise applications.

In 2015, Whyte joined IBM Security as a technical pre-sales engineer, specializing in the AppScan tool suite for static, dynamic and mobile application security testing. With a growing interest in advancing his cybersecurity expertise, Whyte earned the Certified Information Systems Security Professional (CISSP) certification, broadening his proficiency in the field.

In 2019, Whyte joined Sonatype, recognizing that the rapid growth of open-source software had made software composition analysis a critical component of application security.

# Information Advantage: Deny the Adversary Everything, Deny Ourselves Nothing

Jeanne Falick, Observability Advisor, Splunk • [jfalick@cisco.com](mailto:jfalick@cisco.com)

## ABSTRACT

To enable information dominance in contested, multidomain environments, Splunk's unified platform equips mission forces with the power to sense, understand and act faster than the adversary. It fuses real-time data from tactical sensors, ISR feeds, cyber assets and open-source intelligence, then applies advanced AI/ML to uncover hidden patterns, detect anomalies and predict mission-impacting events before they happen. Dynamic topology maps and intuitive dashboards give commanders a real-time, theater-wide view of mission systems, application health and infrastructure performance—connecting data to decisive action. Built with U.S. Department of Defense-grade security, the platform delivers continuous cyber monitoring, rapid threat detection and prioritized remediation to maintain resilience under pressure. This is full-spectrum observability—arming Army units with the agility, insight and speed needed to dominate the information environment and accelerate multidomain operations.

**BIO:** Jeanne Falick serves as an observability advisor at Splunk, partnering with leaders across the Department of Defense and national security community to advance mission outcomes through data-driven resilience and operational efficiency. With more than two decades of experience working alongside federal and enterprise organizations, Falick brings a strategic lens to complex challenges at the intersection of technology and defense.

Her work centers on surfacing high-impact use cases where observability can streamline operations, strengthen cyber posture and enhance decision advantage. Falick holds a master's degree from Rutgers University and is based in North Carolina's Research Triangle Park.

# Information Dominance in the Modern Battlespace

**Eric Hennessey, Solutions Architect, Splunk • [erhennes@cisco.com](mailto:erhennes@cisco.com)**

## ABSTRACT

In modern military operations and C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) environments, decision superiority depends on the rapid and accurate synthesis of vast amounts of data from diverse sources. This presentation explores how a robust data analytics platform can ingest, normalize and analyze data from a wide range of structured and unstructured sources, including sensor feeds, SIGINT, battlefield reports, logistics systems and open-source intelligence (OSINT). Emphasis will be placed on the platform's ability to handle heterogeneous data formats (e.g., JSON, XML, CSV, video, text and geolocation data) and to unify them into a cohesive model in near real time for clear presentation.

We will discuss how advanced analytics, including machine learning and geospatial correlation, enable actionable insights that enhance situational awareness, support predictive maintenance and drive informed command decisions.

**BIO:** Eric Hennessey is a solutions architect at Splunk for IT and observability solutions supporting national defense accounts. He has more than 30 years of experience in IT operations and infrastructure management in both the public and private sectors and served 27 years in the U.S. Air Force and Air National Guard. He joined Splunk in January 2016.



# Modernizing RMF Compliance Through Automation and Agentic AI

**Fawad Siraj, Co-Founder and CTO, stackArmor • fawad@stackarmor.com**

## ABSTRACT

Meeting RMF requirements under NIST SP 800-37 Rev. 2 remains a significant challenge for U.S. Army cybersecurity teams, often requiring manual, time-consuming documentation efforts and ongoing control validation across complex environments. These burdens not only slow down system authorization but also strain limited security resources post-deployment.

A modernized approach is emerging: one that integrates authorization artifacts as code, aligns with DevSecOps pipelines and embeds compliance directly into infrastructure deployment. By automating the generation and maintenance of critical documentation—such as system security plans (SSPs) and control implementation statements—teams can reduce errors, increase traceability and maintain alignment with evolving configurations.

Furthermore, the integration of agentic AI enables intelligent, continuous monitoring tasks across the system life cycle, dramatically reducing the need for manual oversight or expanded workforce support. By autonomously validating system changes, performing real-time risk assessments and generating audit-ready evidence, agentic AI minimizes the human effort required to maintain RMF compliance. This not only ensures sustained alignment with control baselines but also mitigates the need to hire additional personnel for routine compliance tasks. To build confidence and trust in agentic AI, its actions are fully traceable, auditable and aligned with established RMF workflows—providing transparency and assurance to cybersecurity teams and authorizing officials. The result is a leaner, more efficient security operation that maintains readiness and compliance while allowing existing teams to focus on mission-critical objectives.

**BIO:** Fawad Siraj, CTO and co-founder of stackArmor, a Tyto Athene Company, is a seasoned cloud solutions architect with more than 15 years of experience in systems engineering, infrastructure modernization and secure systems development. Since co-founding stackArmor in 2016, Siraj has been instrumental in shaping the company's technical vision and driving the strategic delivery of its innovative cloud services, particularly in support of public-sector and regulated industry clients. Under his leadership, stackArmor has become a recognized authority in accelerating FedRAMP, StateRAMP and U.S. Department of Defense compliance through its pioneering ThreatAlert® Security Platform and ATO on AWS Accelerator, helping customers reduce risk and time to compliance.

Siraj leads stackArmor's technological development and strategic planning, identifying and evaluating evolving technologies and industry trends to maintain a competitive edge. His

leadership and vision contributed to Tyto Athene's 2025 acquisition of stackArmor, recognizing the company's groundbreaking work in cyber, compliance and cloud automation. Together, they deliver cost-efficient digital infrastructure that accelerates the mission of government and defense customers through secure innovation and automation.

Before founding stackArmor, Siraj held technical roles at Northrop Grumman and Smartronix. He has a bachelor's degree in computer science from George Mason University. He is an active thought leader in cloud security and compliance, regularly engaging with stakeholders, partners and industry forums to promote secure cloud adoption.

# Modernizing the Army's Data Pipeline To Ensure High Velocity Data-Driven Decision-Making From the Enterprise to the Edge

**Sean Applegate, CTO, Swish Data • [sapplegate@swishdata.com](mailto:sapplegate@swishdata.com)**

## ABSTRACT

The U.S. Army today operates across a sprawling enterprise defined by legacy systems, disparate databases, stovepiped networks and sensors. This fragmentation leads to excessive data duplication, delayed sharing and persistent challenges in connecting critical information across silos, including logistics, personnel, sustainment and intelligence. These structural inefficiencies impede the Army's ability to conduct timely, data-driven decisions at scale, which is a fundamental requirement in multidomain operations and strategic readiness missions.

Despite investments in enterprise initiatives, such as the Army Data Platform (ADP), Army Vantage, CJADC2 and ARDAP, the service faces hurdles with inconsistent APIs, variable data quality and limited analytics capabilities. Domain experts often lack modern tools, AI/ML integration and coordinated frameworks to derive predictive insights. Meanwhile, network complexity and environmental conditions slow the flow of data, inhibiting real-time battlefield decision dominance.

To break through, the Army must modernize its data pipeline by transforming from monolithic, network-centric architectures into a layered, event-driven data-centric ecosystem comprised of loosely coupled systems that work seamlessly together.

First, it is critical to extract canonical data directly from siloed systems via open APIs, publishers and data integration providers. Second, the data must flow into a globally distributed DDIL-capable data mesh architecture to empower domain-aligned data "products" that are trusted, governed, discoverable, shareable and democratized for teams to easily use. Third, the Army must put the data to work in edge to enterprise event-driven applications and data lakes for analytical insights, automated workloads and agentic operations.

This presentation will outline and discuss the approaches that the Army can take to build out this streamlined stack enabling democratized data ops and how it enables distributed teamwork and speed of relevance. It aligns with Army digital transformation and the Unified Data Reference Architecture (UDRA), supporting zero-trust security, self-service discovery and multilevel decision support. By democratizing data products and integrating analytics/ML the Army gains resilient, near-real-time insight into global multidomain operations. The mission demands nothing less than a data architecture that accelerates decision advantage and collaboration in an increasingly competitive environment.

**BIO:** Sean Applegate serves as chief technology officer for Swish, where he leads innovation strategy, solutions and services. Applegate is passionate about delivering life cycle services to ensure clients realize maximum value for technology investments. Prior to joining Swish, Applegate spent nine years with Riverbed Technology, helping large enterprises understand, optimize and control performance of global IT architectures. He filled several technical leadership roles at Riverbed, including senior director of the portfolio solutions group and public sector technology strategist. Before Riverbed, Applegate worked with several OEMs doing business in the public sector. He has also worked as a technology consultant and served as an active-duty U.S. Marine.

# 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 is able to utilize the power of quantum computing, the results—both good and bad—will be immeasurable. As AI becomes more sophisticated, so too do the potential security risks.

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

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

**BIO:** Gina Scinta is Thales TCT's deputy chief technology officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission-critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC and more.

Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, she 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 Data in Transit Security, Thales TCT

**Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies •**

Mary.Shiflett@ThalesTCT.com

## ABSTRACT

High-speed networks are the critical foundation that supports many of an agency's most vital communications and operations. However, this foundation is at risk of surveillance and attack by increasingly sophisticated cyber criminals and well-funded nation states. These network connections, if unprotected, are proving to be highly vulnerable, leaving sensitive assets exposed.

So, what is the best way to protect network traffic? Encrypt everywhere, between data centers and headquarters to backup and disaster recovery sites, whether on premises or in the cloud.

Attend this session to learn about the best practices for data in transit encryption, including how to:

- Protect against common network threats, such as eavesdropping, fiber-tapping, harvest and decrypt
- Deploy high-speed encryption from the core to the cloud to the edge
- Improve performance
- Mitigate the quantum threat
- Address zero-trust requirements

**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, she 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.

# Bringing Air-Gapped AI to the Tactical Edge for Sensor Fusion and Decision Dominance

**Raj Iyer, Ph.D., President, Tsecond.ai • [raj.iyer@tsecond.us](mailto:raj.iyer@tsecond.us)**

## ABSTRACT

As artificial intelligence (AI) transforms the battlefield and far-edge DDIL operational environments, the fusion of compute and storage at the edge has become a mission imperative to achieve decision dominance in multidomain environments. Tsecond is a Silicon Valley defense startup focused on building hardware solutions to move AI inferencing to the tactical edge rather than moving large volumes of edge data to the enterprise for analysis. Tsecond's BRYCK AI product line offers an innovative family of ruggedized, low SWaP, high-capacity data AI edge inferencing platform that can transform how the U.S. Army moves, processes, analyzes and acts upon large volumes of unstructured data, such as videos to achieve key operational insights. These standalone, completely air-gapped units are built to deliver actionable intelligence directly at the edge without reliance on network connectivity or cloud infrastructure. With this technology, soldiers and commanders now have access to AI at the tactical edge in a fully secure solution. Tsecond's proprietary and patented technology enables us to condense high-density storage, high-end computing and GPUs/ AI accelerators needed for AI inferencing, all inside a small form factor while at the same time reducing the power needs and reducing heat and electromagnetic signatures.

**BIO:** Raj Iyer serves as the president of a Silicon Valley-based defense startup called Tsecond.ai, where he leads all aspects of the company's growth in the federal business. Previously, Iyer served as the Army's first chief information officer at the Pentagon, driving digital transformation and providing oversight to the Army's \$18 billion cyber and IT budget. Iyer brings more than 30 years of technology experience, most of them in the defense industry, both inside and outside of the government. He received the secretary of the Army's Superior Civilian Service Medal in 2023.

# Real-Time Data for Mission Analytics

**Carmelo McCutcheon, CTO, VAST Federal • [carmelo@vastfederal.com](mailto:carmelo@vastfederal.com)**

## ABSTRACT

This presentation addresses Problem Statement 3 posed by the Army Cyber Center of Excellence (CCoE): “How can technology ingest data from multiple sensors, geotag data and aggregate for analysis? Can technology do predictive analysis based on preconditioned filters? Can this technology integrate data into mission command systems?”

Our solution demonstrates a comprehensive end-to-end data analytics pipeline specifically designed for mission-critical military applications, leveraging the VAST data platform as the foundational infrastructure integrated with Apache Spark, Trino query engine and Apache Superset. This architecture directly addresses the U.S. Army’s need for real-time sensor data processing, geospatial intelligence and seamless integration with existing mission command frameworks.

### Technical Architecture Overview:

The implemented solution features a four-stage pipeline architecture that begins with direct sensor data capture through high-throughput ingestion mechanisms capable of processing multiple sensor formats simultaneously. Raw sensor streams flow through automated triggers and database functions for initial data quality assurance and normalization, ensuring consistent data structures before entering the transformation layer.

Apache Spark serves as the primary ETL engine, performing complex data transformations, feature engineering and real-time geospatial tagging operations on streaming sensor inputs. The VAST database provides unified storage, database and stream processing capabilities in a single all-flash system optimized specifically for AI and analytics workloads required in tactical environments.

### Predictive Analytics and Mission Integration:

The system integrates Trino’s distributed SQL query engine running natively on VAST’s serverless compute infrastructure, enabling high-performance interactive analytics on massive datasets without data movement penalties. This integration supports both real-time and historical data queries, facilitating predictive analytics through machine learning models that adapt to evolving operational conditions.

Preconditioned filtering capabilities are achieved through configurable data preprocessing pipelines that implement automated anomaly detection, data normalization and feature selection processes. Mission command system integration is facilitated through RESTful APIs and standardized military data formats, enabling seamless incorporation of analytical outputs into existing C2 frameworks used by the Army Cyber Center of Excellence.



#### Visualization and Decision Support:

Apache Superset interfaces with Trino and the VAST database to provide interactive dashboards and mission-critical insights to command personnel. The visualization layer supports real-time monitoring of sensor networks, predictive threat assessments and geospatially aware tactical displays that enhance situational awareness for commanders operating in contested environments.

Performance evaluations demonstrate the system's ability to process high-velocity sensor streams with sub-second latency while maintaining data accuracy and supporting concurrent analytical workloads, making it well-suited for deployment in mission-critical environments requiring continuous monitoring and intelligent decision-making capabilities.

This unified architecture eliminates traditional data silos and reduces operational complexity by providing a single platform for storage, processing and analysis, directly supporting the Army's multidomain operations requirements and cyber electromagnetic activities as emphasized at TechNet Augusta.

**BIO:** Carmelo McCutcheon is a seasoned technology leader with a proven track record of driving innovation and growth in the technology sector, particularly in AI/ML, cloud computing and cybersecurity. As the public sector CTO at VAST Data Federal, he leverages his expertise to simplify complex technology solutions for customers, focusing on optimizing AI/ML workloads and securing AI/ML environments to meet stringent federal standards. McCutcheon is responsible for driving the company's technology vision and ensuring its solutions not only meet but exceed the rigorous security and compliance standards required by federal government partners. Additionally, he serves as a key adviser to the company's leadership and board, helping shape the strategic direction of VAST Data Federal to support mission-critical federal missions and maintain its reputation as a trusted provider of secure, high-performance data infrastructure.

# VDetect

**John Eubank, Founder and CEO, 10x National Security** • [john@10xnatsec.com](mailto: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 U.S. Department of Defense (DOD) and intelligence community 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.

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.



## 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, 139 chapters and 1,600 corporate members. For more information, visit [www.afcea.org](http://www.afcea.org)

