TechNet indo-pacific

October 28-30, 2025 ◆ Hawai'i Convention Center

2025 INNOVATION SHOWCASE

AFCEA HAWAII

SIGNAL
AFCEA INTERNATIONAL MEDIA

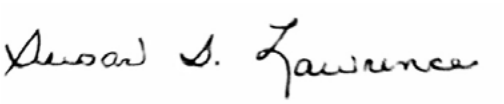
2025 TechNet Indo-Pacific Innovation Showcase

Within the Indo-Pacific region, the historic and contemporary nations in South Asia, specifically India, play a major role in shaping present and future discourses. The area has undergone a strategic shift that requires reliable connectivity between the Indian and Pacific Oceans. This three-day TechNet Indo-Pacific conference, hosted by AFCEA International and AFCEA Hawai'i, will reflect the expanded broader Asia view with participation from throughout the area, discussing defense policies and challenges and their relevance to both industry and government through this new lens.

The Innovation Showcase provides the opportunity for innovators in this space to demonstrate cutting-edge solutions so leaders can secure the region, supporting the "Sword & Shield: Ensuring a Secure, Free and Prosperous Indo-Pacific" theme for this year's TechNet Indo-Pacific conference.

Developing and integrating new technologies while strengthening global cooperation is essential to securing the Indo-Pacific region. AFCEA is determined to foster efficient and effective collaboration between industry and government to promote innovation in defense technologies. The companies and their innovative technologies below, ranging from cabling to zero-trust architectures, represent the future of Indo-Pacific defense.

Best wishes,



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

Table of Contents

INNOVATION SHOWCASE SUBMISSIONS

Submissions

Beyond the Checklist: Bridging Compliance and Operations for Federal Cyber Resilience

Brian "Stretch" Meyer, Field Chief Technology Officer •
brian.meyer@axoniusfed.com • Axonius Federal, Booth 631

ABSTRACT

With growing U.S. Department of Defense (DOD) mandates, such as DOD Instruction (DODI) 8510.01 – Risk Management Framework (RMF) for DOD IT, and increasing emphasis on programs like Continuous Monitoring (CONMON) and the Risk Management Framework, defense agencies face mounting pressure to strengthen their cybersecurity posture. Compliance is no longer about one-time audits—it requires sustained readiness in alignment with NIST SP 800-53 controls and DOW assessment processes.

This session will explore how DOD organizations can move beyond "checkbox compliance" toward a state of continuous readiness. We'll discuss strategies to reduce the attack surface through asset intelligence, protect mission data as it flows across joint and coalition environments, and automate compliance activities to meet evolving DOD requirements.

Most importantly, attendees will learn how Axonius helps bridge the gap between compliance and operations teams, transforming traditionally siloed groups into seamless partners. The result: security programs that are not only audit-ready for RMF and CONMON oversight, but also mission-focused, resilient and aligned with DOD cyber directives.

BIO: With more than 15 years of experience in the federal technology sector, Brian "Stretch" Meyer has built a distinguished career spanning the U.S. Department of Defense (DOD) and the intelligence community. As the field chief technology officer at Axonius Federal, he leverages deep technical expertise and strategic leadership to help government agencies tackle their most complex cybersecurity challenges.

Meyer's career is defined by his success in technical leadership and his deep federal experience. He has held key positions, including security services manager at major DOD agencies, where he had direct oversight of cybersecurity architecture and engineering divisions supporting the mission partner environment programs.

A U.S. Air Force veteran, Meyer played a critical role in engineering and securing mission-critical systems in theater, supporting Operation Inherent Resolve (OIR) and Operation Enduring Freedom – Afghanistan. His passion lies in translating mission needs into innovative cybersecurity solutions, ensuring federal agencies can strengthen their security posture in an evolving threat landscape.

WIDS in the Public Sector for Today's Threats

Joseph R. Salazar, Senior Product Marketing Manager • noe@sacocopr.com • Bastille Networks, Booth 543

ABSTRACT

Federal agencies and military organizations increasingly face mandates to secure their environments against wireless threats that operate beyond the reach of traditional controls. Policies from the Department of War and requirements under ICD 703 and NIST SP 800-53 explicitly call for wireless intrusion detection systems (WIDS) to monitor, detect and respond to unauthorized wireless activity in classified and mission-critical spaces. These requirements reflect the growing recognition that wireless technologies, such as Wi-Fi, Bluetooth, cellular, Internet of Things and others, have expanded the attack surface in ways that conventional endpoint, firewall and SIEM tools cannot address.

This session will explore how WIDS fulfills federal security requirements by providing visibility into the radio frequency (RF) spectrum. Attendees will learn how adversaries exploit the ubiquity and invisibility of wireless devices with demos and descriptions of attacks. Real-world scenarios, including advanced campaigns like the "Nearest Neighbor Attack," will highlight how both malicious insiders and unintentional device introductions can jeopardize security.

The presentation will conclude with guidance on evaluating WIDS platforms for compliance and mission readiness. We will review critical capabilities, including spectrum monitoring, wireless threat detection, device localization and policy enforcement, and show how these close the wireless visibility gap while strengthening layered defenses.

Key Takeaways:

- Awareness of the expanding wireless attack surface in the public sector
- Insights into RF-based tactics and equipment that target the wireless attack surface
- Understanding of WIDS solution capabilities
- Policies and guidance that support WIDS deployments
- Criteria for evaluating WIDS platforms to meet compliance and mission needs

BIO: Joseph Salazar is a seasoned cybersecurity professional with more than 20 years of experience in both military and civilian sectors. He is a retired major from the U.S. Army Reserves, where he served for 22 years as a counterintelligence agent, military intelligence officer and cybersecurity officer. Throughout his civilian career in cybersecurity, he has held numerous roles and co-authored a book on deception technology. He maintains the CISSP, CEH and EnCE certifications and is currently a senior product marketing manager at Bastille Networks.

Accelerating Decision Advantage: Embedding Modular AI Orchestration in the Indo-Pacific Enterprise

Bradley Zogopoulos, Deputy Director of Combatant Command Programs •
bradley.zogopoulos@bigbear.ai • BigBear.ai

ABSTRACT

In the Indo-Pacific theater, vast distances, contested domains and disparate systems strain command agility and decision cycles. Embedding a modular, vendor agnostic artificial intelligence (AI) orchestration capability early in mission architectures, via a lightweight middleware layer, empowers commanders and operators to dynamically integrate sensors, AI/ML models and analytics across domains in ways that they have never before been capable.

By prepositioning this orchestration framework:

- Connectivity interruptions become opportunities: models and data adapt in real time to contested or degraded networks.
- Stealthy force multipliers emerge: edge nodes reconfigure on demand and remotely to support allied UxVs, island command and control (C2) nodes or maritime intelligence, surveillance and reconnaissance (ISR) platforms.
- Decision clarity accelerates: fused outputs can be translated via large language model technology into digestible and actionable operational briefs, enhancing operational briefs, enhancing OODA loop velocity.
- Ecosystem agility scales: coalition partners, commercial partners and classified networks can be bridged without stovepipes.

This approach directly supports U.S. Indo-Pacific Command's "Sword & Shield: Ensuring a Secure, Free and Prosperous Indo-Pacific" mission, enabling integrated deterrence, resilient C2 and partner-ready AI advantage across sea, air, undersea and cyber domains. We'll illustrate these benefits through conceptual deployments involving maritime ISR, distributed sensor webs and allied force interoperability, showing how early adoption of orchestration translates to decisive operational scale and speed.

BIO: Bradley Zogopoulos is a U.S. Navy veteran and defense technology leader with more than 15 years of experience in electronic warfare, intelligence analysis and AI-enabled mission systems. He began his career as a cryptologic technician technical aboard the forward-deployed USS Mustin (DDG-89) in Yokosuka, Japan, where he served as electronic warfare supervisor supporting freedom of navigation operations and ISR patrols across the Indo-Pacific.

Following his service, Zogopoulos advanced red forces SIGINT analysis at the Office of Naval Intelligence and later supported the Defense Intelligence Agency's GALE program, driving adoption of critical intelligence platforms across the U.S. Department of Defense (DOD) and intelligence community.

Today, Zogopoulos is the deputy director of combatant command programs at BigBear.ai, where he leads the development and deployment of advanced AI/ML solutions for the DOD. His work includes orchestrating multi-INT platforms, enabling computer vision and predictive analytics at the edge, and delivering maritime domain awareness capabilities tailored for contested environments.

Zogopoulos brings a unique perspective shaped by both operational experience in the U.S. Indo-Pacific Command theater and hands-on leadership in applying AI/ML to accelerate decision advantage for U.S. and allied forces.

Bridging Detection and Decision: Operationalizing Threat Intelligence at Scale

Chris Cobucci, Principal Software Architect • chris.cobucci@vaeit.com • Brasi Tech, Booth 409

ABSTRACT

Traditional threat intelligence often arrives too late to influence incident response, leaving analysts burdened with manual lookups and reactive decision-making. This seminar explores a paradigm shift: operationalizing threat intelligence at the moment of data capture. By correlating and enriching streams from cloud, endpoint, VPN and network sources in real time, defenders can transform alerts into context-rich insights that drive faster triage, containment and mission alignment. The session will highlight how real-time context improves both technical workflows and strategic decision-making, from reducing analyst workload to maximizing existing infrastructure investments.

Attendees can expect to learn:

1. Limitations of traditional threat intelligence applications in cyber defense and how embedding contextual enrichment at the point of data capture redefines the utility of threat intelligence.
2. Approaches for applying real-time enrichment across diverse, high-volume, multi-vendor environments.
3. How real-time intelligence shifts workflows, resource allocations and readiness and both technical and leadership levels.

BIO: Chris Cobucci brings more than 25 years of expertise spanning network engineering and software development. He holds both a bachelor's degree and a master's degree in engineering science and mechanics from the Pennsylvania State University. His software engineering portfolio includes the development of mission-critical tools such as the Pentagon's primary tactical network troubleshooting, inventory, E911 and SOR application—still in use after 17 years. Cobucci has also designed a full-stack network assurance platform for the Missile Defense Agency, capable of validating more than 500,000 unique network flows; an offline engineering application for assessing and correlating disparate TDM telephony systems; and an event enrichment tool supporting both threat intelligence and network engineering. Currently, Cobucci focuses on systems engineering and software development for large-scale threat enrichment initiatives in highly complex environments.

Mission Assurance in the Age of Disruption: A Data-Driven Approach

Danny Everhard, Senior Solutions Engineer • deverhar@cisco.com • Cisco, Booth 1222

ABSTRACT

In today's contested and resource-constrained environments, maintaining digital mission resilience isn't optional—it's mission critical. This talk will explore how organizations operating in denied, degraded, intermittent and limited bandwidth (DDIL) environments can maintain continuity of operations using a combined approach with Splunk and Cisco's Comply to Connect (C2C). We'll walk through how real-time visibility, automated compliance and secure endpoint enforcement come together to protect and sustain operations at the edge. Attendees will see how Splunk's analytics capabilities, paired with C2C's zero-trust access control, can help ensure that mission-critical systems stay secure, compliant and functional, even when the network doesn't. Whether you're working in tactical edge environments or supporting enterprise-scale operations, this session will provide actionable insights for building cyber-resilient architectures in DDIL conditions.

BIO: Danny Everhard has 10 years of experience using Splunk, including three years supporting the U.S. Air Force/Space Force team at Splunk and now covering the Navy team. With a background as an Army interrogator, he ran sources and performed interrogations during his deployment to Afghanistan, sharpening his problem-solving skills under pressure. Everhard's technical expertise and military experience make him a valuable asset in both the information technology and defense sectors.

Security of Cabling

Jay Nusbaum, Senior Systems Engineer • Jay.Nusbaum@commscope.com •
CommScope / RUCKUS Networks, Booth 1300

ABSTRACT

This session will discuss which cabling solutions are ideal for supporting your network's security applications, such as surveillance, fire protection, building automation and more.

CommScope Systems Engineer Jay Nusbaum leads this educational session where he'll discuss the pros and cons of copper and fiber cabling solutions for security applications in several environments.

Whether you need to connect a sensor a few feet away or a camera that's across campus, the cabling solution will be as unique as your circumstances and requirements. Nusbaum will explore how to implement technologies and products such as Power over Ethernet, Fault Managed Power, extended-reach cabling and hybrid copper/fiber cables to achieve the transmission distances and application support you require.

This event will also examine the products and systems that help ensure your cabling infrastructure is protected and secure within the network—including inside- and outside-plant cabling. Nusbaum will discuss the roles of products such as armored cable, shielded cable, conduit, keyed and locked connector ports, and intelligent physical-layer management systems in securing a network's cabling.

BIO: Jay Nusbaum started in the industry as a technician in 1987 where he owned and operated an infrastructure installation company for 15 years. Nusbaum has been with CommScope since 2006 and is a senior systems engineer dedicated to the U.S. federal team.

Important Safety Tips for Implementing Wi-Fi 6E and 7

Brian Wright, Director of Systems Engineering • brian.wright2@commscope.com • RUCKUS Networks, Booth 1300

ABSTRACT

Many DOW entities are either currently implementing Wi-Fi for the first time or enhancing their deployment as users are migrated from primarily wired to wireless. This session will facilitate those efforts by highlighting recent changes in Wi-Fi standards, including Wi-Fi 6E (which adds the 6 GHz spectrum) and Wi-Fi 7. The focus of the session will be on transitioning from previous standards, Wi-Fi 5 and 6, paying attention to important changes that can affect deployment. We'll distinguish fact from fiction in 6 GHz Wi-Fi and help you plan for adoption of these newer standards.

During the session, we will explore the following key concepts:

- Intro: spectrum vs. standards
- 2.4 GHz, 5 GHz and 6 GHz technology comparison
- Challenges in 6 GHz wireless operation (that you might not know about)
- FIPS 140-3 and 6 GHz APs
- Switch/cable requirements for Wi-Fi 6E/7

The End of Tokens: Transforming Static Credential Risk

Derek Tracy, Mission Matter Expert • derek.tracy@dell.com •
Dell Technologies, Booth 1513

ABSTRACT

Many mission-critical systems still rely on bearer tokens for service-to-service authentication: static credentials that, once stolen, grant access from any location or device. This fundamentally breaks zero-trust principles. Attackers with one compromised service token can move laterally across networks, impersonate legitimate services and access coalition partner systems. Current service authentication often can't distinguish between legitimate software running on approved hardware versus malicious code using stolen credentials, a critical gap for joint operations across contested, degraded, intermittent and limited (DDIL) environments.

Quantum Helix (QHx) replaces static tokens with ephemeral, hardware-rooted identities unique to each software deployment. When a service starts, QHx generates cryptographically bound credentials tied to that specific process, on that specific machine, at that specific time. These short-lived credentials embed verifiable attestations about the runtime environment, software version and security posture. A transparent proxy handles mutual authentication and automatic rotation, and stolen credentials become worthless because they only work for one process, on one machine, for minutes not months.

This transforms security posture for military networks. Compromised credentials can't enable lateral movement because they're cryptographically locked to their origin. Every service interaction creates attribution trails showing exactly which software version, on which hardware, made which requests, essential for incident response and understanding adversary behavior. The system maintains security even when disconnected from central infrastructure, enabling resilient operations in contested environments. QHx retrofits onto existing systems through the proxy layer, delivering zero-trust architecture without rewriting mission applications, protecting joint and coalition operations across all domains.

Key takeaways of QHx:

- Eliminates static credential risk by replacing bearer tokens with short-lived, hardware-rooted identities
- Prevents lateral movement because credentials are cryptographically bound to a single process on a specific machine
- Enables real-time attribution of every service interaction, improving incident response and threat forensics
- Operates in DDIL environments without reliance on central infrastructure, ensuring mission continuity

Presented by:
M42, Dell Technologies and Sterling

BIO: Derek Tracy, a U.S. Marine Corps veteran, serves as mission matter expert at Dell Technologies, where he partners with U.S. Department of Defense (DOD) and intelligence community customers to maximize mission value and operational effectiveness from their technology investments. In this role, he provides strategic guidance to ensure software and hardware solutions deliver optimal outcomes for critical national security missions. Previously, as staff solutions engineer at VMware/Broadcom, Tracy served as lead solutions engineer for DOD and intelligence community accounts, where he was embedded as platform portfolio manager for the U.S. Army Software Factory, co-managing seven product teams and specializing in cloud-native software modernization on Kubernetes and DevSecOps for DOD missions.

Tracy's extensive platform architecture expertise, developed throughout his career, established him as a pioneer in federal cloud transformation and software modernization. He helped architect and build modern software factories across the DOD, including Kessel Run, Kobayashi Maru, Army Software Factory and the USMC Software Factory. Tracy also led the groundbreaking effort to create the DOD's first enduring cATO (Continuous Authorization to Operate) process for Kessel Run. Tracy architected and accredited multitenant solutions across NIPR, SIPR and JWICS security levels, managing complete installation efforts from design through ICD-503 accreditation for customers across the DOD and intelligence communities. His proven track record demonstrates his ability to deliver mission-critical hybrid-cloud solutions that meet the most stringent federal compliance and security requirements.

MESA Partner Networks: Cross-Domain Collaboration and AI Integration in the Indo-Pacific

Mark Drobena, Principal Product Manager • mark.drobena@everfox.com •
Everfox, Booth 1628

ABSTRACT

In the Indo-Pacific, mission success depends on the ability of partners to share information securely across organizational and national boundaries. Traditional approaches, such as point-to-point VPNs, COMSEC devices and dedicated circuits, introduce cost, delay and security exposure. These barriers limit both operators and artificial intelligence (AI)-enabled systems that rely on cross-domain access to trusted, multi-source data for timely decision-making.

The Multi-Enterprise Spanning Architecture (MESA), built on Trusted Thin Client (TTC) technology, represents a new evolution in cross-domain solutions. Rather than extending network perimeters, MESA interconnects independent TTC environments into a distributed partner network. Each organization maintains sovereignty over its infrastructure and data while selectively granting controlled access to trusted mission partners. This enables human operators to receive only the information they need, such as rendered outputs or pixel streams, while AI models and sensitive data remain protected from direct access or manipulation.

This interactive session will explore how mission partners can rapidly extend cross-domain collaboration, integrate AI and preserve sovereignty while strengthening interoperability across the region.

Key benefits for Indo-Pacific missions include:

- Strengthened Partnerships: Secure multilateral collaboration without exposing internal systems.
- AI-Ready Information Access: AI tools gain near-real-time, high-fidelity data from multiple partners while safeguarding models from manipulation.
- Operational Agility: Information-sharing timelines shrink from months to days, accelerating decision cycles.
- Resilient Security Posture: Zero-trust cybersecurity principles are upheld while enabling dynamic multi-partner operations.

BIO: Mark Drobena is a principal product manager at Everfox, where he leads the product strategy for Trusted Thin Client, Trusted Thin Client Remote and MESA. In this role, he is responsible for driving excellence across all aspects of the products and ensuring that

customers are engaged and delighted with the value and performance of their Everfox access products.

Drobena has more than 15 years of product, cybersecurity and leadership experience at software and information technology companies, including SAIC, Leidos, Forcepoint and the U.S. Army. In his previous roles, Drobena has managed engineering teams, information/exploitation operations and led cybersecurity and digital transformation for organizations.

Drobena holds a master's degree in information assurance from Northeastern University and has the CISSP certification from ISC2.

Rapidly Deployable 5G and Edge AI: Accelerating Decision Dominance Across the Indo-Pacific With iMERS

Aaryn Anderson, Senior Manager of Solutions • aaryn.anderson@insight.com • Insight Public Sector, Booth 1723

ABSTRACT

The vast and often disconnected environments of the Indo-Pacific region present significant challenges to rapid decision-making, secure data transfer and the deployment of advanced analytics at the tactical edge. Traditional networks struggle to support high-throughput, low-latency applications like artificial intelligence (AI) at the edge or to provide resilient communication during emergencies and deployments, leading to reduced mission agility and operational vulnerabilities. Effectively addressing these challenges requires cutting-edge solutions for secure, resilient communications and accelerated data-driven insights.

Insight's iMERS platform, integrated with private 5G capabilities, offers a transformative solution for "Sword & Shield: Ensuring a Secure, Free and Prosperous Indo-Pacific." iMERS is a compute platform for multi-network communications, including 4G/5G, SATCOM and MILSATCOM. This solution provides local 5G capability and bandwidth-optimized SATCOM backhaul, enabling AI at the edge and the extension of live virtual constructive training to the edge. It supports critical applications like Vcinity data acceleration, video processing, virtual/augmented/mixed reality solutions, and command and control (C2). Private 5G, a strategic modernization priority, further integrates mission-specific devices, secure data transfer, autonomous systems and edge compute for environments from military bases to forward operating bases (FOBs).

This integrated approach ensures uninterrupted connectivity and reliable performance even in challenging or austere conditions, overcoming Wi-Fi's limitations and supporting latency-sensitive applications. It enables bi-directional data transfer between command and tactical edge for critical assets like IAVA files, maps and inflight data ingest for analytics, while optimizing WAN bandwidth. By accelerating the understanding of complex scenarios through AI-enabled analytics and secure, resilient communications, this solution significantly enhances "mission readiness," "operational security" and the ability to "accelerate strategic advantage" across the Indo-Pacific. The platform's flexible, open architecture allows for multiple use cases and rapid reconfiguration, ensuring adaptability to evolving threats.

BIO: Aaryn Anderson is a strategic leader in public sector technology transformation, serving as senior manager of solutions at Insight Public Sector. With a career spanning complex engagements across federal, state and local government, Anderson brings deep expertise in aligning innovative solutions with mission-driven outcomes.

He has led high-impact initiatives supporting agencies where his work has focused on AI strategy, data governance, infrastructure modernization and cloud transformation. Anderson's leadership has been instrumental in shaping Insight's role as a trusted partner in public sector modernization, helping clients navigate procurement, compliance and service delivery challenges with precision and agility.

Anderson is a frequent collaborator with technology partners, driving joint planning and execution for national engagements, strategic planning sessions and innovation showcases. His ability to coordinate across stakeholders and deliver measurable outcomes has earned him recognition as a go-to public sector leader.

He continues to champion scalable, secure and future-ready solutions that empower public institutions to serve their communities more effectively.

AI and the Information Supply Chain

Mark Allen, Head of Solutions and Analytics • mark@legionintel.com •
Legion Intel, Booth 817

ABSTRACT

Militaries have understood the importance of logistics for millennia, best represented by the adage, "Amateurs talk strategy. Professionals talk logistics." Winning wars is often a function of effective supply chains—which side can move beans and bullets faster and more reliably.

Winning on today's battlefield or boardroom requires the same discipline to be applied to information. With AI, we must treat data, models and insights as supplies that flow through an "information supply chain." This discussion maps classic supply chain principles like demand forecasting, sourcing, quality control, inventory, routing and last-mile delivery to the production of decision-grade intelligence.

We will explore how to manage sources, provenance and policy; maintain a knowledge inventory; and design repeatable, auditable processes for information flow. The result should be a repeatable, auditable information logistics framework that increases tempo, reduces cognitive load and ensures leaders can exploit agent orchestration for real and impactful operational outcomes.

BIO: Mark Allen is a physicist-turned-analytics leader who earned his Ph.D. in physics from Stanford University and began his career with postdoctoral research before transitioning into data science and business analytics. He went on to serve as director of business analytics at Chegg, where he led teams of analysts and data scientists and helped drive operational improvements across key student services. In 2019, he co-founded FutureProof Technologies and served as its CTO, focusing on operationalizing climate change risk for financial professionals. Today, as head of solutions and analytics at Legion, he is involved in launching Legion's product, leveraging his robust background in analytics, technology and leadership.

Empowering the Indo-Pacific Warfighter: Intelligent Data Infrastructure for Rapid, Efficient and Cyber-Resilient AI and Mission Data

Jim Cosby, Chief Technology Officer • jim.cosby@netapp.com • NetApp, Booth 923

ABSTRACT

Federal agencies are experiencing exponential growth in mission-critical and artificial intelligence (AI) data, posing significant challenges in accessing, managing, processing and securing this information. This surge demands innovative technologies to optimize data by reducing its size, cost and processing time. In addition, escalating security threats from cyber attacks and ransomware require enhanced data access control methods to protect data and to reinforce zero-trust principles. In this session, we will delve into new technologies for storing, securing, managing and optimizing agency data across hybrid multicloud environments, including multidomain operations, to support a secure, free and prosperous Indo-Pacific region.

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. Cosby has focused on data management, storage and security for more than 20 years, including on-premises, hybrid and multicloud data fabric 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.

Asset Assessment: Understanding the Different Approaches of Asset Detection

Ronny Fredericks, Public Sector Chief Technology Officer •
gehron.fredericks@nozominetworks.com • Nozomi Networks, Booth 1102

ABSTRACT

All assets are not created equal. Some have differences in priority, functionality and accessibility. Ensuring they are being detected and monitored properly is essential for enhanced security monitoring. This session will explore the strengths and weaknesses of different asset detection approaches, including: passive, active, agents, hybrid and os/device fingerprinting.

BIO: Gehron "Ronny" Fredericks is the CTO - Public Sector at Nozomi Networks. He holds a master's degree in digital forensics and cyber investigation and an additional master's degree from the University of Maryland. Fredericks has more than 10 years of experience with unique operational technology experience from his time at leading energy provider Exelon Corporation as a senior security analyst in its security operations center and has also worked closely on the information technology side as a developer and technical operations manager in previous roles. Fredericks is currently a member of the Infragard – South Florida Members Alliance and the U.S. Secret Service Electronic Crimes Task Force.

Level Up: Implementing AI and Machine Learning Detection for Next-Generation Analytics Across All Levels of the Purdue Model

Ronny Fredericks, Public Sector Chief Technology Officer •
gehron.fredericks@nozominetworks.com • Nozomi Networks, Booth 1102

ABSTRACT

The Purdue Model framework organizes industrial control systems by layers. The best way to ensure a secure, free and prosperous Indo-Pacific is to monitor and detect all layers for inventory, threats, vulnerabilities and activity. This presentation will highlight different deployment techniques to ensure maximum visibility.

BIO: Gehron "Ronny" Fredericks is the CTO - Public Sector at Nozomi Networks. He holds a master's degree in digital forensics and cyber investigation and an additional master's degree from the University of Maryland. Fredericks has more than 10 years of experience with unique operational technology experience from his time at leading energy provider Exelon Corporation as a senior security analyst in its security operations center and has also worked closely on the information technology side as a developer and technical operations manager in previous roles. Fredericks is currently a member of the Infragard – South Florida Members Alliance and the U.S. Secret Service Electronic Crimes Task Force.

Seeing Through the Fog: Wireless Unified Visibility for OT and iOT

Ronny Fredericks, Public Sector Chief Technology Officer •
gehron.fredericks@nozominetworks.com • Nozomi Networks, Booth 1102

ABSTRACT

Wireless networks expand the potential attack surface for adversaries. Legacy devices were only seen on a wired network, but as more vendors opt for wireless connectivity, having visibility into those networks is critical. This session will cover detection of wirelessly connected devices via Bluetooth, Zigbee, LoraWAN, WirelessHART, cellular and Wi-Fi and what enhanced threat detection and alerting looks like during an attack.

BIO: Gehron "Ronny" Fredericks is the CTO - Public Sector at Nozomi Networks. He holds a master's degree in digital forensics and cyber investigation and an additional master's degree from the University of Maryland. Fredericks has more than 10 years of experience with unique operational technology experience from his time at leading energy provider Exelon Corporation as a senior security analyst in its security operations center and has also worked closely on the information technology side as a developer and technical operations manager in previous roles. Fredericks is currently a member of the Infragard – South Florida Members Alliance and the U.S. Secret Service Electronic Crimes Task Force.

Flexible by Design, Reliable by Demand: SATCOM Built for PACE

Rob Weitendorf, U.S. Representative • rob@paracomm-usa.com •
Paradigm, Booth 1300A

ABSTRACT

Modern missions demand satellite communications (SATCOM) that are more than just available; they must be reliable, resilient and flexible by design. In regions where forces operate across vast distances, contested environments and joint missions with allies, SATCOM becomes a critical enabler of command and control.

This session will examine why flexibility is the foundation of reliability in modern SATCOM and how it underpins mission assurance. From seamless switching across networks and profiles to multiple power options and resilience in GPS-denied or electronically contested environments, the next generation of platforms must endure where others have failed before. Intuitive, user-focused design and integrated intelligence, such as Paradigm's Interface Module (PIM), further reduce complexity, ensuring warfighters remain focused on the mission rather than the technology.

The discussion will highlight the key dimensions of flexibility required in a modern SATCOM architecture.

- Multi-waveform support to ensure interoperability with allies, backward compatibility and access to emerging high-throughput services.
- Multiband capability across Ku, Ka and X, giving operators the ability to select the frequency best suited to mission requirements.
- Integration with other transport layers from tactical radios to optical links, delivering redundancy and enabling resilient, blended networks essential for JADC2.
- Assured operations in GPS-denied environments, leveraging advanced timing alternatives, adaptive power control and anti-jamming techniques to maintain connectivity and protect operational security.

This flexibility transforms planning frameworks, such as PACE, into practical, mission-ready safeguards. For commanders and operators alike, SATCOM that is flexible by design and reliable by demand provides the assurance needed to maintain decision advantage and operational effectiveness in any environment.

BIO: Rob Weitendorf has many years of experience in the satellite communications industry, building extensive connections across the United States and conducting business within the U.S. government. He has joined as Paradigm's U.S. representative and continues the mission of showcasing Paradigm terminal solutions, which offer the world's most advanced SATCOM, made simple.

Enabling Spectrum Dominance: Real-Time Signature Management and Spectrum Situational Awareness

Jason Davis, Senior Research Scientist • jason.s.davis@peratonlabs.com •
Peraton, Meeting Room 2118

ABSTRACT

Spectrum dominance is reliant upon real-time understanding of the electromagnetic spectrum (EMS) and intuitive presentation of actionable information to commanders without reliance on subject matter experts. Spectrum situational awareness is inherent in requirements for signature management, dynamic deconfliction, emission control (EMCON) policy distribution and enforcement, and spectrum agility for reliable communications. Automated capabilities leveraging AI/ML solutions for distributed sensor orchestration, data aggregation and analytics are necessary to reduce the cognitive burden on the warfighter and to alert to emerging problems that impact survivability in the field.

The OSCAR (Operational Spectrum Comprehension, Analytics and Response) technology was developed to address current and emerging needs, including tactical use cases such as Blue Force Monitoring, EMS signature comprehension, adaptive network resiliency and real-time adaptive spectrum management. OSCAR utilizes a distributed network of passive radio frequency sensors, including vehicle-mounted and man-portable systems, enabling real-time spectrum comprehension while on the move, with intuitive representations and alert propagation into a Common Operating Pictures (COP). Automated workflows enable real-time EMCON alerts, signal localization and signature projections to inform physical and spectrum maneuvers. Further, autonomous spectrum analytics improve network robustness, rapid interference resolution and localization of unauthorized or adversarial signals activity.

OSCAR has been thoroughly tested over the past year at multiple DOW exercises and in U.S. Indo-Pacific Command (INDOPACOM) deployments. In these events, OSCAR was operated by U.S. Army personnel to evaluate capabilities for tactical use cases. Results demonstrated multiple deployment configurations, real-time signature comprehension, interference mitigation, signal of interest (SOI) geolocation, network assessment and EMCON policy adherence. Lessons learned from these events were utilized to improve OSCAR functionality for Army requirements.

This presentation will discuss the application of OSCAR for signature management and EMCON enforcement in tactical use cases. Results from prior test events and feedback from early adopters in INDOPACOM will be presented, along with discussion of lessons learned for spectrum dominance.

BIO: Jason Davis is a senior research scientist at Peraton Labs in Red Bank, New Jersey. Currently, Davis is the acting development manager and software architect on the Spectrum Integration System (SIS) project. Previously, he was a key member of the development team on Peraton's Operational Spectrum Comprehension, Analytics and Response (OSCAR) Solution for Dynamic Spectrum Management. In addition to his management and development responsibilities, Davis is an active participant and leader for recent test and training activities at U.S. Army bases including Cyberquest (Fort Eisenhower, 2024), NetModX (Fort Dix, 2024) and Lexington Green (Camp Shelby, 2025). Davis has more than 30 years of software development experience with domain expertise in test and measurement and wireless communications. He has a master's degree in electrical engineering from Drexel University and a bachelor's degree in electrical engineering from Stonybrook University. Davis has authored two patents related to testing techniques for location-based services.

AI and Identity: Use Identity Security as a Sword and Shield in Indo-Pacific AI MDO

Andrew Whelchel, Senior Solutions Engineer • andrew.whelchel@saviynt.com • Saviynt, Booth 730

ABSTRACT

Deploying artificial intelligence (AI) presents opportunities for acceleration of the mission of multidomain operations (MDO) in ways unimagined just a few years ago. Applying AI for accelerating the mission and reducing the cyber risk of the MDO digital space simultaneously can be a challenge. Identity security when integrated with the application of AI creates the opportunity to apply a simultaneous sword-and-shield approach (mission acceleration and cyber protection/reduction) to meet the needs of the Indo-Pacific AI MDO environment.

In enabling a simultaneous approach to meet MDO objectives via mission enablement and cyber defensive efforts (effectively sword and shield), organizations reap the benefits of application of AI for identity security as well as helping to secure AI with identity security. The simultaneous approach has dual respective benefits of reducing time for security decisions due to AI-informed risk information as well as risk reduction for AI systems in the theater.

Delivering the results from the simultaneous approach with AI and identity security first requires an identity security platform that has machine learning and agentic AI built into its core operating flows. Additionally, to meet the second part of the simultaneous approach (enabling AI mission for the theater), the identity security platform must have innate capabilities to aid the AI MDO through NPE protection of AI platforms and rapid data response through MCP server-enabled large language model platforms. When dually deployed approaches are available to organizations, they gain several capabilities including:

- Accelerate onboarding of mission resources and validate proper access using AI trust scoring models for risk
- Enable faster application onboarding in theater (even if disconnected) using agentic AI
- Provide NPE service principal access for authorization management of AI services in cloud and disconnected environments
- Integrate identity security MCP server for in-theater rapid data responses using cross-platform large language models in connected and disconnected environments

To meet the needs of the mission of MDO in the theater, AI needs to be optimized using identity security. When optimized, it will both improve speed of action for onboarding mission resources and accelerate AI in the mission by enabling protection of NPEs and identity security MCP server integration. As a part of the session, attendees will learn about key capabilities including accelerated resource onboarding using AI, faster application onboarding in theater (even if disconnected) using agentic AI, NPE authorization for AI services and identity security MCP server for accelerated data responses.

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 cybercrime prevention. At a prior role at Okta and the current role at Saviynt, focus is 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.

From Data to Decisions: Advancing Readiness With AIOps

Lee Koepping, Chief Technologist • lkoepping@sciencelogic.com •
ScienceLogic, Booth 737

ABSTRACT

In the contested Indo-Pacific, mission success depends on resilient, efficient and secure information technology (IT) ecosystems that adapt in real time. U.S. Department of War leaders face escalating cyber threats, increasingly complex hybrid infrastructures and the need to deploy and sustain capabilities at mission speed. Every second lost to blind spots, manual troubleshooting or fragmented systems can impact readiness and security.

This session will explore how modern AIOps and advanced observability are enabling the shift from reactive management to autonomous operations. By applying artificial intelligence (AI)-driven insights, machine learning and predictive analytics, leaders can improve situational awareness, streamline workflows and anticipate disruptions before they affect mission-critical services.

Participants will learn how unified observability platforms consolidate data across the enterprise to provide a single operational view. This empowers commanders and IT operators to act quickly and precisely whether defending against a cyber threat, optimizing resources or maintaining continuity in austere environments. The result is faster resolution of issues, reduced operational burden and the agility to redirect skilled personnel to higher priority mission tasks.

The discussion will also look toward the future of autonomous IT where self-healing systems, AI-supported decision-making and continuous optimization become force multipliers for mission readiness..

BIO: Lee Koepping, chief technologist at ScienceLogic, brings more than 30 years of experience in IT engineering and mission-aligned technology innovation, with a strong focus on the unique operational demands of federal and DOD environments. A U.S. Navy veteran with a background in naval intelligence, Koepping has a deep understanding of contested and denied domains and now leads ScienceLogic's technical strategy in the public sector. His work focuses on deploying AI-enabled solutions that drive situational awareness, predictive decision-making and cyber resilience at the edge. Koepping offers grounded insights into aligning industry innovation with operational imperatives, ensuring AI is secure, scalable and interoperable across U.S. and allied forces in the Indo-Pacific.

The Evolution of AI and Its Impact in Transforming Cyber at the Edge

Andres Giraldo, Director of Innovation • andres.giraldo@sealingtech.com •
SealingTech, Booth 842

ABSTRACT

SealingTech recognized that cyber operators could not wait for cloud-only solutions that fail to meet the realities of their missions. By taking the initiative to engineer an offline-capable generative artificial intelligence (AI) capability, we aimed to bridge the gap, giving defenders the same advantages of cutting-edge AI while operating in air-gapped, forward-deployed environments. This enables operators to act faster, make better decisions under pressure and stay ahead of adversaries in contested cyberspace. AI helps operators accelerate a hunt mission using natural language, reduce the overload from multiple defensive cyber tools and focus their time and energy on the activities that matter most to mission success.

During missions, cyber operators must rapidly process vast amounts of data, perform technical analysis and deliver actionable intelligence. In the world of defensive cyber operations, many operate in air-gapped, disconnected and contested environments. Delivering AI capabilities in these environments introduces unique engineering and operational challenges: optimizing performance without network connectivity, minimizing size, weight, power and cost (SWaP-C), and tightly integrating with mission-critical defensive cyber tools.

This presentation will discuss the challenges and necessary evolution of fielding an AI Cyber Hunt Assistant, from designing and fielding offline AI solutions for cyber missions, using SealingTech's Operator X as a case study. Operator X enables natural language interaction with cyber defense tools, empowering both junior and senior operators to triage threats, understand complex environments and generate mission reports.

Attendees will gain insights into:

- Evolution of its innovative AI integrations: How Operator X combines LLMs, RAG and its expanding suite of custom AI agents to interact directly with defensive cyber tools.
- Edge optimization challenges: Lessons learned adapting AI for forward-deployed missions, including reducing GPU vRAM consumption to enable a highly mobile, cost-efficient platform.
- Operational lessons: Insights from working directly with cyber defenders to identify workflows where AI meaningfully accelerates threat hunting and reporting.

The presentation concludes with a live demonstration and next steps for Operator X, showcasing how generative AI integrates with DOW cyber tools to augment the warfighter's mission needs, enabling them to rapidly understand mission environments and deliver actionable intelligence.

BIO: Andres Giraldo, director of innovation at SealingTech, is a highly accomplished cybersecurity professional renowned for his exceptional leadership and innovative contributions to the industry. Giraldo started his tenure at SealingTech as an intern. A proud U.S. Navy veteran, he earned a bachelor's degree in computer science from the University of Maryland Global Campus. He has been instrumental in driving innovative solutions for the DOD. He is known for his commitment to understanding his customers' unique requirements and tailoring solutions that align with their goals. Giraldo is a tenacious researcher who remains at the forefront of the ever-evolving cyber landscape. He is recognized for his ability to rapidly design, develop and bring solutions to market. In addition to his technical expertise, Giraldo is also deeply committed to mentoring and empowering the next generation of cybersecurity professionals.

Supply Chain Detection and Response: Defending Against Evolving Nation-State Threats

Ryan Sherstobitoff, Field Chief Threat Intelligence Officer •
rsherstobitoff@securityscorecard.io • SecurityScorecard

ABSTRACT

The Indo-Pacific threat landscape is undergoing a rapid transformation, driven by intensifying geopolitical tensions—particularly around the Taiwan Strait—and the increasing activity of state-aligned adversaries. Nation-state actors are moving beyond traditional, direct attack vectors and instead exploiting the weakest link: the supply chain. This evolution represents a strategic shift in targeting, leveraging the interconnectedness of modern ecosystems to achieve broader impact with greater stealth and deniability.

The supply chain in the Indo-Pacific is both wide and complex, encompassing entities ranging from advanced defense contractors and critical infrastructure providers to basic logistics and support suppliers. Each represents a potential entry point for compromise, creating an environment where a single exploited vendor can cascade risk across entire sectors. The lack of holistic visibility into these dependencies magnifies exposure, leaving both private and public organizations vulnerable to disruption, espionage and coercion.

Supply Chain Detection and Response (SCDR) emerges as a critical paradigm to address this evolving threat. By integrating continuous monitoring, advanced detection of anomalous activity across third-party and fourth-party networks, and intelligence-driven response playbooks, SCDR enables defenders to identify vulnerabilities before adversaries exploit them, disrupt campaigns targeting supplier ecosystems and strengthen overall resilience.

In the Indo-Pacific theater, SCDR offers a critical framework for shifting from reactive defense to proactive risk management. By bridging the gap between threat intelligence, operational security and strategic resilience, SCDR enables armed forces to safeguard mission readiness, protect defense-industrial supply chains and maintain operational superiority in the face of evolving nation-state threats.

In this presentation, we will explore the concept of SCDR and its implications for defenders—how it strengthens visibility, reduces risk and transforms supply chain security from a passive challenge into an active defense capability.

BIO: Ryan Sherstobitoff is SecurityScorecard's field chief threat intelligence officer, where he oversees the threat research, collections and intelligence teams. Prior to SecurityScorecard, Sherstobitoff was at McAfee Corporation where he led and contributed to nation-state threat research and analysis.

He is also the former chief corporate evangelist at Panda Security, where he managed the U.S. strategic response for new and emerging threats. Sherstobitoff is widely recognized as a security and intelligence expert throughout the country.

Powering Indo-Pacific Readiness: Elevating Digital Defense With ServiceNow

Adam Prem, Global Lead for Defense and Security Mission Solutions •
adam.prem@servicenow.com • ServiceNow

ABSTRACT

In the face of dynamic geopolitical shifts and escalating cyber threats, securing the Indo-Pacific demands a proactive, unified defense strategy. Aligned with the U.S. Indo-Pacific Command's (INDOPACOM's) priorities—enhanced deterrence, robust alliances and modernized capabilities—this session unveils how ServiceNow empowers defense organizations to build a resilient, adaptive digital shield.

The ServiceNow AI platform automates critical security and operations workflows to ensure faster, smarter responses. Key highlights include:

- AI-Driven Threat Response: Rapidly detect, contain and mitigate cyber threats with Security Incident Response, integrated with leading threat intelligence and SIEM tools.
- Vulnerability Prioritization: Streamline vulnerability detection, risk assessment and remediation to harden critical information technology (IT) environments.
- Operational Continuity: Automate IT service management and disaster recovery processes to maintain mission resilience during disruptions.
- Secure Collaboration: Enhance interoperability with secure, efficient knowledge-sharing across allied teams and partners.

Transform reactive strategies into proactive capabilities, and support a free, open and secure Indo-Pacific. Join us for actionable insights and real-world examples illustrating ServiceNow's role in driving digital defense excellence across the region.

BIO: Adam Prem is ServiceNow's global lead for defense and security mission solutions. He brings 23 years of experience in the IT consulting space, including time spent at Booz Allen Hamilton and Deloitte, supporting various DOD, defense logistics and state/local organizations. In his current role, he works with customers to develop and deploy new tactical and mission-related workflow solutions, specifically designed for defense and intelligence organizations across the globe.

Transforming IT and OT Security To Dominate INDOPACOM's Cyber Landscape

Robert Rash, Director of Outbound Product Management •
robert.rash@servicenow.com • ServiceNow

ABSTRACT

The Indo-Pacific's security challenges demand smarter, unified defenses for critical infrastructure and operational technology (OT). Aligning with the 2024 U.S. National Defense Strategy and U.S. Indo-Pacific Command's (INDOPACOM's) integrated deterrence framework, uniting information technology (IT) and OT security is vital to ensuring a secure, free and prosperous region. ServiceNow's artificial intelligence (AI) platform empowers defense organizations to blend operational precision with cutting-edge technology, delivering proactive, mission-ready solutions.

ServiceNow enables seamless collaboration across IT and OT teams, as well as between allied nations and coalition partners. By leveraging advanced AI and automation, our platform ensures real-time threat intelligence, orchestrated incident responses and synchronized security operations—critical for maintaining dominance in the region's dynamic battlespace.

In this session, we'll cover:

- Enhanced Domain Awareness: Achieve visibility into IT and OT assets with ServiceNow's CMDB, including industrial systems and SCADA networks. This capability identifies dependencies, uncovers vulnerabilities and prioritizes protection efforts across converged environments.
- Coordinated Response Automation: Use tailored security incident and vulnerability response solutions, complete with automated playbooks, to contain threats without disrupting mission-critical operations.
- Coalition-Ready Operations: Foster secure information-sharing and collective defense across INDOPACOM alliances, supporting the integrated deterrence strategy.
- Streamlined Compliance Management: Ensure adherence to defense standards, regulations and operational security with ServiceNow's automated and unified compliance tracking for IT and OT.

Real-world scenarios will illustrate measurable outcomes, including up to a 70% reduction in mean time to detection (MTTD) and 60% cuts in mean time to response (MTTR). ServiceNow delivers the tools to harmonize IT/OT security operations, ensuring resilience in critical missions.

Don't miss this opportunity to discover how ServiceNow transforms reactive defenses into proactive strategies, delivering the operational agility needed to shape the future of the Indo-Pacific. It's time to dominate today's threats and secure tomorrow's prosperity.

BIO: Robert Rash serves as the director of outbound product management, overseeing the market strategy and success of our operational technology management (OTM) solutions. His role includes formulating product strategies and road maps to ensure that the OTM offerings provide a superior solution for the management of operational technology assets. Rash has more than 20 years of OT industrial automation, engineering, programming and manufacturing experience. Prior to his engagement with ServiceNow in 2022, he specialized in process improvement and OT security for the manufacturing and utility sectors.

Unlock the Power of AI To Secure the Indo-Pacific: A Mission-Centric Approach

Adam Prem, Global Lead for Defense and Security Mission Solutions •
adam.prem@servicenow.com • ServiceNow

ABSTRACT

Artificial intelligence (AI) is revolutionizing defense operations, presenting unmatched opportunities to strengthen readiness in the Indo-Pacific. Yet, barriers like infrastructure gaps, security risks and integration challenges can hamper progress in this critical region.

ServiceNow is empowering the U.S. Department of Defense and its allies with secure, mission-ready AI solutions designed to overcome these challenges. Focused on scalable and seamless adoption, our platform fortifies defenses without adding complexity for warfighters.

Key capabilities include:

- Military-Grade Security: Utilize an Impact Level 5 cloud environment with mission-specific safeguards to protect sensitive data.
- Adaptive AI Deployment: Integrate generative AI and large language models at the application layer for flexibility, eliminating vendor lock-in while adapting to dynamic regional needs.
- Ethical AI Governance: Leverage human-in-the-loop governance to align AI use with U.S. Department of Defense policies, ensuring responsible and mission-assured deployment.

This session demonstrates how ServiceNow accelerates AI integration, enabling defense teams to overcome adoption hurdles, gain real-time insights and maintain tactical advantage in the information-driven battlespace. With ServiceNow, AI adoption isn't just about technology—it's about delivering impactful results to secure and empower a free, prosperous Indo-Pacific. Join us to discover how AI-backed resilience can secure the region's future.

BIO: Adam Prem is ServiceNow's global lead for defense and security mission solutions. He brings 23 years of experience in the IT consulting space, including time spent at Booz Allen Hamilton and Deloitte, supporting various DOD, defense logistics and state/local organizations. In his current role, he works with customers to develop and deploy new tactical and mission-related workflow solutions, specifically designed for defense and intelligence organizations across the globe.

AI-Powered Edge Computing for Mission Resilience in the Indo-Pacific

John Williams, Director of Government Programs • john.williams@tsecond.us •
Tsecond Inc., Booth 645

ABSTRACT

In the Indo-Pacific, mission success increasingly depends on the ability to collect, process and act on data at the tactical edge. Operating environments are often disconnected, denied, intermittent and limited (DDIL), making reliance on centralized cloud services impractical. To address this, we propose the deployment of Tsecond BRYCK AI Mini devices as a secure, ruggedized and portable solution for edge computing in contested environments. BRYCK AI Mini devices combine high-capacity storage, onboard compute and integrated GPU acceleration, enabling warfighters to run advanced AI/ML workloads, real-time video and image analytics, and cyber defense models directly in the field without dependency on external connectivity. Data collected at the edge can be processed, encrypted and selectively synchronized with the cloud once secure connectivity is restored, ensuring both operational continuity and data sovereignty. Our approach empowers defense and humanitarian missions alike—supporting ISR (intelligence, surveillance and reconnaissance), disaster relief coordination and cyber defense operations—with a scalable, modular platform that aligns with zero-trust security principles. The solution directly supports the conference theme, "Sword & Shield: Ensuring a Secure, Free and Prosperous Indo-Pacific," by enhancing decision-making speed, resilience against adversarial disruption and regional mission readiness. By combining the rugged portability of BRYCK AI Mini with AI-driven insights at the tactical edge, this innovation ensures that Indo-Pacific forces can operate with agility, autonomy and security—even in the most challenging and harsh conditions.

BIO: John Williams serves as the director of government programs at Tsecond Inc., a defense technology startup delivering breakthrough innovation in data mobility and edge artificial intelligence, serving defense, aerospace and industrial markets worldwide. In this role, he spearheads strategic growth initiatives and fosters key engagements with government and defense customers. Prior to joining Tsecond, Williams built decades of experience as a senior sales executive in the government and defense sectors at leading enterprise technology companies including Cloudera, Red Hat, Nutanix, Splunk and NetApp.

Intersection of Quantum, AI and Security

Gina Scinta, Deputy Chief Technology Officer •
Mary.Shiflett@ThalesTCT.com • Thales Trusted Cyber Technologies, Booth 1017

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

Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world-class encryption and key management for data at rest in data centers and cloud infrastructures.

From Intent to Action: A New Model for Military Networks

C. Tate Baumrucker, Principal Architect • tate.baumrucker@vaeit.com •
VAE Inc., Booth 409

ABSTRACT

Military networks operate at global scale, integrating heterogeneous technologies under dynamic mission demands. Intent-based networking (IBN) provides a model for aligning such infrastructures with high-level objectives, but current systems lack mechanisms to encode organizational hierarchy and mission variability. We propose a hierarchical, nested intent model that incorporates organizational constructs—such as location, tenant, mission type, priority and classification—as reference variables within IBN templates. Global intents define enterprise-wide requirements, while regional, mission and tactical layers refine or override inherited variables to reflect local constraints. This approach enables scalable configuration, consistent policy propagation and adaptive mission reconfiguration. Applied to defense networks, it supports coalition interoperability, reduces operator error and increases policy agility across distributed environments. Remaining challenges include automated conflict detection, scalable verification across heterogeneous devices and securing intent resolution pipelines. Embedding organizational constructs into hierarchical intent frameworks offers a foundation for deploying IBN in complex, mission-critical military networks.

Attendees can expect to learn:

1. How intent-based networking (IBN) can be adapted to handle the complexity of global, mission-driven defense networks
2. The role that hierarchical, nested intents can be used to achieve organizational structures (like mission type, priority, security) and enable policies to flow from global to tactical levels
3. Practical applications of policy inheritance and overrides within regional, mission and tactical layers
4. Ongoing challenges in applying IBN to DOW enterprises and missions

BIO: Tate Baumrucker is a seasoned technology executive with more than 30 years of experience designing and delivering secure, scalable and highly available networks and systems. A recognized expert in intent-based networking (IBN), AI-driven operations and automation, Baumrucker has led the development of global-scale operations support systems. Throughout his career, Baumrucker has successfully navigated complex, distributed and sensitive operational environments, earning a reputation as a trusted adviser to senior government, military and Fortune 500 leadership. In addition to executive leadership, Baumrucker is a published author on enterprise security and network architecture, sharing insights that continue to shape the field.

Smarter Intents, Stronger Networks: AI at the Core of IBN

C. Tate Baumrucker, Principal Architect • tate.baumrucker@vaeit.com •
VAE Inc., Booth 409

ABSTRACT

Intent-based networking (IBN) seeks to bridge high-level organizational objectives with low-level device configurations, yet existing systems struggle with ambiguity in natural language intents and lack sufficient grounding in operational realities. Current AI/ML-driven approaches often rely on synthetic datasets or narrowly scoped templates, limiting their ability to capture organizational complexity. This work proposes the integration of large-scale, real-world device configurations—spanning thousands of heterogeneous systems—with organizational artifacts such as security policies, standards documents and standard operating procedures into large language model (LLM) pipelines. By employing vector databases and retrieval-augmented generation (RAG), these models can retrieve and synthesize both technical precedent and institutional context during intent translation. Combing approaches can reduce semantic ambiguity by aligning intents with historical configuration practices, enforce policy compliance through the incorporation of organizational metadata and enable adaptive, explainable translations that evolve alongside both the network and the institution. Remaining challenges include scalable verification of AI-generated policies, mitigation of bias and adversarial manipulation and ensuring robust human-in-the-loop oversight. By unifying operational data with organizational knowledge in AI-enhanced translation pipelines, this research advances the state of IBN toward more trustworthy, verifiable and contextually grounded systems.

Attendees can expect to learn:

1. How LLMs enhanced with RAG can translate high-level intents into enforceable policies with greater accuracy
2. How training on real device configurations combined with organization artifacts can reduce ambiguity and reflect operational reality
3. Methods for generating network policies that evolve with changing configurations and organizational requirements while providing transparency to operators
4. Remaining challenges around verifying AI-generated outputs, mitigating bias and adversarial manipulation.

BIO: Tate Baumrucker is a seasoned technology executive with more than 30 years of experience designing and delivering secure, scalable and highly available networks and systems. A recognized expert in intent-based networking (IBN), AI-driven operations and automation, Baumrucker has led the development of global-scale operations support systems. Throughout his career, Baumrucker has successfully navigated complex, distributed and sensitive operational environments, earning a reputation as a trusted adviser to senior government, military and Fortune 500 leadership. In addition to executive leadership, Baumrucker is a published author on enterprise security and network architecture, sharing insights that continue to shape the field.

Versa Networks: Enabling Secure, Flexible Connectivity Across the Tactical Edge

Rob Kauffman, Senior System Engineer •
rkauffman@versa-networks.com • Versa Networks, Booth 1724

ABSTRACT

Versa Networks delivers a mission-ready secure SD-WAN and universal SASE platform purpose-built for the U.S. Department of Defense's shift toward zero trust. Our solution provides transport-agnostic connectivity across SATCOM, 5G, LTE, MPLS and broadband, enabling resilient, secure communications from the tactical edge to enterprise data centers and cloud environments. By converging networking and security functions—SD-WAN, next-generation firewall, micro-segmentation and secure access—into a single software platform, Versa reduces complexity, improves cyber resilience and lowers life-cycle costs. As the primary vendor for DISA's Thunderdome Zero Trust program, Versa brings proven defense experience that directly aligns with Indo-Pacific mission requirements for secure, interoperable and cost-effective C4I modernization.

BIO: Rob Kauffman is a senior system engineer at Versa Networks.

Operationalizing AI-Driven Zero-Trust Architectures for Mission Assurance in Contested Environments

Rob Bair, CISO in Residence • rbair@zscaler.com • Zscaler, Booth 1107

ABSTRACT

The Indo-Pacific region presents unique operational challenges that demand resilient solutions for secure, multi-domain collaboration in increasingly contested environments. As defense organizations accelerate adoption of artificial intelligence (AI) to enhance decision-making and operational overmatch, integration with robust cybersecurity frameworks such as zero-trust architecture (ZTA) is paramount to ensuring mission assurance. Deploying AI-driven capabilities at the tactical edge in disconnected, denied, intermittent and limited (DDIL) environments requires a meticulous balance between operational agility, cybersecurity assurance and interoperability across joint and coalition forces.

Rob Bair, leveraging more than 20 years of real-world expertise in government and military operations—including assignments at U.S. Cyber Command, the National Security Agency (NSA) and the National Security Council—offers a strategic perspective on using zero-trust principles to secure operational artificial intelligence (AI) systems in resource-constrained and contested domains. This session will explore how adaptive ZTA frameworks, coupled with AI, can enhance threat detection, strengthen decision-making cycles and mitigate risks across multi-domain operations.

Key topics addressed will include:

- Secure AI Deployment: Overcoming cyber and operational risks in DDIL scenarios using ZTA-integrated AI models
- Dynamic Interoperability: Ensuring coalition compatibility while maintaining secure data exchanges and real-time collaboration
- Ethical AI Use: Crafting deployment frameworks that balance operational effectiveness with ethical decision-making in military applications.
- Scaling Resilience: Lessons learned from national defense policy to integrate ZTA and AI at scale for enduring mission success regardless of emerging threats.

BIO: Rob Bair brings more than 20 years of government and U.S. Department of Defense information technology and cybersecurity experience to Zscaler. He brings a breadth of experience, including offensive cyber operations, red team and blue team (incident response and threat

hunt), SOC operations, threat intelligence and national-level policymaking. He has extensive knowledge of Department of Defense and intelligence community missions and activities (U.S. and foreign).

His service in the U.S. Navy included positions at U.S. Cyber Command, NSA, the U.S. Navy's Fleet Cyber Command, Joint Special Operations Command (JSOC) and various other Navy and joint military assignments. His final government position was director for intelligence programs (technical intelligence) and cybersecurity and operations policy (member of the team that developed Executive Order 14028) in the Executive Office of the President / National Security Council. He possesses a wide range of knowledge on critical infrastructure, U.S. and international policy and negotiation, the U.S. interagency, foreign policy and cryptography.

Prior to joining Zscaler, Bair was the executive director at Team Cymru, responsible for government sales and support, including threat hunt and malicious infrastructure. He has experience with FED, FFRDC, SLED, DOD, IC, DIB and national security focused customers.

Clarity Is the New Shield: Turning Data Into Mission Success

Drew Coyle, Staff Solutions Engineer • Acoyle@cribl.io • Cribl, Booth 925
Sybilla Robertson, Staff Solutions Engineer • Srobertson@cribl.io • Cribl, Booth 925

ABSTRACT

In today's Indo-Pacific environment, success depends on more than collecting data—it requires cutting through the noise to protect what matters and deliver clear, actionable insight where and when it is needed.

In this session, Cribl's Drew Coyle and Sybilla Robertson will discuss how agencies can strengthen mission outcomes by securely managing and routing massive data streams across hybrid, edge and cloud environments. They will share real-world perspectives on reducing tool sprawl, simplifying complex data pipelines and enabling trusted information-sharing across joint and coalition partners.

Attendees will walk away with practical strategies for defending critical assets, supporting compliance and improving readiness while lowering cost and complexity. The discussion will be interactive, encouraging participants to connect these lessons to their own challenges, with opportunities to continue the conversation at the exhibit booth for deeper technical dives.

BIO: Drew Coyle is a seasoned solutions engineer with more than a decade of experience supporting federal agencies in strengthening their cybersecurity and observability strategies. He began his career at Cisco, where he built a strong technical foundation in networking and security, before moving into roles at Area 1 Security, Agari and Proofpoint, helping government customers combat advanced threats and protect critical systems. Now at Cribl, Coyle partners with agencies to address their most pressing data challenges, enabling them to unlock the full potential of their telemetry to drive visibility, efficiency and mission success.

Sybilla Robertson is a cybersecurity expert with more than a decade of experience supporting the U.S. intelligence community and federal agencies. She began her career in national security, building a strong foundation in threat detection, data analysis and mission operations. Now in the private sector, Robertson serves as a public sector solutions engineer at Cribl, where she helps government teams unlock the power of their telemetry data to drive efficiency, visibility and informed decision-making. Her background across both government and industry makes her a trusted partner for agencies navigating today's complex threat landscape.

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, 140 chapters and 1,600 corporate members. For more information, visit afcea.org.