TechNet indo-pacific

October 22-24, 2024 ◆ Hawai'i Convention Center

2024 INNOVATION SHOWCASE

AFCEA

AFCEA HAWAII

SIGNAL

AFCEA INTERNATIONAL MEDIA

2024 TechNet Indo-Pacific Innovation Showcase

I noted in my President's Commentary column in the October issues of SIGNAL Magazine that in August, the Lowy Institute, an independent think tank in Sydney, Australia, released a report on "The Great Game in the Pacific Islands."

Pacific Islanders, the report cited, have found their region, previously undervalued by "larger powers," to be a focal point for strategic competition. We know well that China is expanding its diplomatic reach and targeting strategically important countries and sectors to pursue its agenda and attempt to impose its signature coercive tactics outside of international norms to extend its influence regionally for the benefit of the Chinese Communist Party.

Australia, the United States and other partners in democracy also are stepping up diplomatic efforts. But governments can't solve the technology issues alone, which is why submissions by our industry support partners, such as the ones offered in this compendium, are so important.

The Innovation Showcase provides the opportunity for leaders in this space to demonstrate cutting-edge solutions so that the region can remain "Free-Open-Secure," which is the theme for this year's TechNet Indo-Pacific conference. Those three words are important to the region. For our friends and partners in the Indo-Pacific, the future is not a game.

Best wishes,

Susan S. Lawrence

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

Table of Contents

INNOVATION SHOWCASE SUBMISSIONS

Innovation Showcase Submissions

The New Network Landscape: Transitioning to Wi-Fi6E and Wi-Fi7

Rick Macchio, Consulting Systems Engineer, CommScope •
rick.macchio@commscope.com

ABSTRACT

Many DoD 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-Fi7. The focus of the session will be on transitioning from previous standards, Wi-Fi5 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

BIO: Rick Macchio graduated with a B.S. in electrical engineering from the U.S. Naval Academy in 1987. After five years as a surface warfare naval officer, he transitioned into a career of supporting federal IT efforts as a contractor with Booz Allen & Hamilton as well as a systems engineer for multiple startup networking and security companies since the 1990s.

Defend AI at the Hybrid DDIL Edge with ZSP Identity Security

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

ABSTRACT

The joint multi-domain environment in the Pacific region carries new and more complex challenges. To meet these challenges, defense organizations bring a new pace of AI innovation to mission systems at the edge faster than ever before. These AI capabilities, though offering potential for operational advantage, come with new risk challenges that must be addressed to maintain the drive at the speed of the mission. These AI mission assets when equipped with zero standing privilege (ZSP) identity security provides the operator the ability to mitigate the risk of AI at the edge while still leveraging that AI asset for operational overmatch.

Essential to the success of AI assets at the edge is not just about the execution of AI itself, but rather about application of ZSP identity cyber protection to the AI asset for maximum force multiplier impact. As part of the hybrid edge capability, the ZSP identity cyber protection ensures speedy and secure zero standing privilege access to accelerate AI at the edge while supporting disconnected (DDIL) scenarios.

Meeting challenges of AI cyber protection at the edge requires ZSP identity cyber protection with durable disconnected survivability (DDIL) that is available from cloud to the tactical edge. The ZSP identity security enables edge AI capabilities in the joint domain theater including:

- Provide access authorization to data sets, AI hyperparameters and AI analytics products operating at the tactical edge
- Enable cyber risk remediation through removal of access authorization due to cyber threat or end of mission
- Provide durable ICAM services enabling access to AI edge services and data even in disconnected environments

The capabilities included and described as part of this session include ZSP identity security capability details, DDIL ICAM architecture and operational use case scenarios to hasten the assurance of success of the edge AI mission.

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, his focus is on protecting employees as well as business partner identities for public sector agencies to reduce cyber risk and accelerate capabilities for cloud transformation. Contributions include work as a contributor on the NIST 1800-3 ABAC (Attribute Based Access Control) standard and speaking events on identity access management and security.

Empowering the Cyber Warfighter: AI Solutions to Safeguard Data

Andres Giraldo, Director, Product Development, SealingTech •
andres.giraldo@sealingtech.com

ABSTRACT

This session will explore how large language models (LLMs) and retrieval augmented generation (RAG) can be leveraged to augment cyber defense capabilities. Andres Giraldo, SealingTech's director of products, will highlight how AI agents can seamlessly integrate and interact with defense information systems, empowering cyber defenders in their efforts to safeguard critical data. Attendees will gain insight into cutting-edge AI technologies that enhance the capabilities of both junior and senior cyber defenders. These tools enable quick understanding of complex data and mission environments, allowing cyber defenders to rapidly deliver actionable intelligence to leaders. A demonstration will showcase how cyber defenders can be empowered to utilize open and secure AI technology to stay ahead of adversaries.

BIO: Andres Giraldo is a highly accomplished cybersecurity professional renowned for his exceptional leadership and innovative contributions to the industry. As the director of product development at Sealing Technologies (SealingTech), he has been an invaluable asset, driving groundbreaking solutions for the U.S. Department of Defense (DoD).

Before joining SealingTech, he proudly served in the U.S. Navy and earned a bachelor's degree in computer science.

Giraldo started his tenure at SealingTech as an intern and advanced quicky by displaying exceptional leadership capabilities and fostering a culture of innovation and collaboration. By encouraging open communication and creativity, he has consistently enabled his team and colleagues to deliver cutting-edge solutions for the DoD's cybersecurity needs.

One of Giraldo's key strengths lies in his unwavering dedication to understanding each customers' unique requirements. He engages closely with various stakeholders to gain insight into their cyber rapid response kit needs, allowing him to tailor solutions that align with their goals. This personalized approach has earned him the trust and respect of clients and team members, who recognize his commitment to ensuring their security and success.

As a tenacious researcher, Giraldo remains at the forefront of the ever-evolving cyber landscape. He continuously expands his knowledge, ensuring his clients receive state-of-the-art technology to counter the threat actors in the cyber realm. Giraldo's true expertise shines through in his ability to rapidly design, develop and bring solutions to market. His adept problem-solving skills and efficiency have earned him a reputation as a go-to professional for tackling even the most complex cybersecurity challenges.

With a profound understanding of cybersecurity software and technologies, Giraldo consistently optimizes tools to enhance the efficiency of the cyber warfighter. He is always on the lookout for opportunities to improve existing hardware and software while simultaneously creating new, cutting-edge solutions tailored explicitly to the needs of the cyber defense sector.

Beyond his technical prowess, Giraldo is also deeply committed to mentoring and empowering the next generation of cybersecurity professionals. He actively participates in industry events, sharing his expertise and experiences to inspire others to make a positive impact in the cybersecurity field.

Best Practices for Implementing Quantum-Resistant Security

Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies •
Mary.Shiflett@ThalesTCT.com

ABSTRACT

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

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

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

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

BIO: Gina Scinta is Thales TCT's deputy chief technology officer (CTO). In this role, Scinta servesas 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.

Revolutionizing Network Connectivity—Software-Defined Unified Transport Network (SD-UTN)

Wade Lehrschall, Distinguished Architect, IronBow • wade.lehrschall@ironbow.com

ABSTRACT

Software-Defined Unified Transport Network (SD-UTN) offers a transformative solution for unifying underlay transport networks and Software-defined Wide Area Network (SD-WAN) overlays. This approach eliminates the problem of disjointed wide area networks (WANs) in larger enterprise environments, which often results from scaling proprietary solutions across complex WAN architectures. It is an issue that frequently affects larger federal agencies as they modernize to address an expanding set of mission use cases. SD-UTN enables a unified WAN architecture by leveraging the best modern technologies and solutions in the right places across a diverse and complex WAN landscape.

This whitepaper discusses how SD-UTN simplifies WAN integration, management, and routing policies, ensuring optimal business and mission outcomes.

BIO: Wade Lehrschall has 25 years of experience in networking, software development, post-sales consulting and pre-sale consulting supporting various customers in the U.S. federal domain. He has helped to design, implement and sustain some of the largest and most complex networks and IT systems in the federal government. He provides technical leadership and direction from our chief strategy office to help customers achieve business and mission value through technology adoption. Lehrschall is a triple CCIE with extensive background in modern networking approaches with a focus on multi-domain SDN, SASE, ZTNA, multicloud, WAN and zero trust architectures.

Operating Through the ‘Unknown Unknowns’

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

ABSTRACT

Enabling the warfighter to work and interact from anywhere, on any device like they are in HQ is critical to meeting the needs and expectations of this generation of airmen, soldiers, sailors and Marines. Even at the edge they should be able to utilize IT systems for tactical and core business functions even when they are in delayed/disconnected, intermittently-connected, and low-bandwidth (D-DIL) environments.

This session will detail how a platform approach to workflow enables consistency of use and resilience of data no matter where the user is deployed. Learn how to:

- Eliminate the need for manual efforts like spreadsheets and pen and paper forms while in the field
- Provide consistent HR and IT support to warfighters no matter where they are
- Ensure mission and business efforts continue even when Internet connection is lost and continue seamlessly when connectivity is regained

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.

Prem has a deep understanding of how U.S. Department of Defense organizations operate, from IT implementation and program management perspectives. He spent 8 years within the Naval Information Warfare Systems Command (NAVWAR) program offices, managing the engineering, configuration, risk, program and acquisition of systems and applications deployed on U.S. Navy ships. He is a certified ServiceNow System Admin, holds certifications from Program Management Institute (PMI) for Program Management and Risk Management, and obtained a Certificate for Leadership and Management from Wharton School, Aresty Institute of Executive Education.

Agile Combat Support—Deploying Open and Secure Software to the Edge

Marc Boswell, Air Force Mission Systems and Programs, Red Hat •

maboswel@redhat.com

ABSTRACT

Data is the lifeblood of the kill chain. Getting data from the tactical edge to command and control elements, securely and resiliently, is a linchpin for battlefield success. Iron Bow, Pacstar, and Red Hat recently upgraded Agile Combat Platform (ACP) edge kits to use Red Hat Enterprise Linux (RHEL). The ACP is a complex set of communications infrastructure operating on small form factor hardware, providing secure, reliable and resilient communications at the forward deployed battlefield edge.

RHEL is a flexible platform that supports the deployment and management of workloads in small resource-constrained devices in challenging field locations, such as edge kits. RHEL delivers a DoD-ready software distribution open and secure solutions that enhance security, ensuring the protection of sensitive information. Its scalability adapts to changing demands, optimizing resource utilization. This tool empowers the U.S. Air Force to efficiently extend computing capabilities to remote locations, ultimately strengthening mission success and readiness. This enterprise application platform provides an edge-optimized operating system built from RHEL and Red Hat Ansible® Automation Platform for consistent Day 1 and Day 2 management of hundreds to thousands of sites and devices pulling data from the battlefield. Red Hat automation capabilities enable teams to sustain and maintain software patches and updates for mission workloads at the edge- both disconnected and connected - keeping systems protected anywhere.

BIO: Marc Boswell has more than 30 years of air, nuclear and cyber operations experience, inside and outside of the U.S. Air Force. Commissioned in 1985, Boswell spent 8 years in SAC’s ICBM operations community, including commanding the wing’s Alternate Command Post. In 2009, Boswell was tasked with owning the operations plan to complete the IOC stand up and facility move of the 609th Coalition Air Operations Center, Al Udeid Air Base, Qatar. In 2017, Boswell was mobilized again as the AFCENT A2Y to lead the JWICs systems and targeting operations and sustainment the AFCENTCOM AOR. In 2018, Boswell was mobilized to assist the USAFE A6 staff in preparation for conflict in the EUCOM AOR under the European Defense Initiative. Boswell holds a senior missile operations designator and a master cyber operations designator, an AOC cyber operations certification, and was the non-kinetic effects DO for his unit. Boswell retired from the USAF in October 2019.

Boswell moved from IBM to Red Hat in 2020, after nearly 8 years as IBM’s lead software architect for USAF and joint programs. At Red Hat, Boswell oversees business development and program capture activities for the USAF, USSF, USSTRATCOM, USTRANSCOM, USINDOPACOM and USEUCOM. Boswell holds several technical certifications and is a CISSP, with technical expertise in routing, switching and cybersecurity systems. Boswell also has worked at Cisco, Bell Atlantic Data Solutions Group, and American Power Conversion. Boswell holds a top secret security clearance with SCI talent/keyhole eligibility.

Fortifying Federal Security: Implementing Zero-Trust and Cross-Domain Solutions in the Indo-Pacific Theater

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

ABSTRACT

Former VMware End User Computing Division, now Omnissa, will discuss topics surrounding the ever-evolving landscape of the Indo-Pacific region and the need for robust, secure and resilient IT infrastructure, which have never been more critical. As nations and military forces collaborate to address the unique challenges posed in this volatile area, the ability to communicate securely, quickly and continuously is paramount. Omnissa is at the forefront of providing cutting-edge solutions tailored to meet the stringent requirements of federal agencies and military operations.

This session will delve into the core principles and practical applications of zero-trust architecture (ZTA), cross-domain solutions (CDS), and multi-level security (MLS) systems, specifically designed to enhance the security posture of federal operations in the Indo-Pacific theater. Attendees will gain insights into how these technologies can be integrated to create a fortified, agile, and responsive IT environment.

BIO: Chris Betz is a highly accomplished end user computing technology strategist and a federal CTO inside the EUC VMware Field Technology Office (FTO). Betz has supported federal customers his whole career, now spanning 30 years. With an impressive professional background, Betz's expertise spans multiple roles and federal industries. Before rejoining VMware EUC (Now Omnissa), he held the position of account CTO at Dell Technologies, where he successfully managed large-scale multi-cloud architectures and played a crucial role in implementing enterprise solutions for end user computing. During this time, Betz collaborated closely with VMware as a subsidiary of Dell Technologies, further enhancing his understanding of the VMware ecosystem. Prior to his tenure at Dell Technologies, Betz served as the lead engineer for the VMware Army team, where he dedicated several years to aligning VMware technologies with the unique needs of public and private Sector customers. In total, Betz has dedicated the past 14 years of his career to working with Omnissa, showcasing his unwavering commitment to the company and its customers.

The Rise of Wireless Threats: Protecting Classified Information from Invisible Wireless Attacks

Dr. Brett Walkenhorst, Chief Technology Officer, Bastille • noe@sacocopr.com

ABSTRACT

The U.S. Department of Defense has long recognized the risks associated with wireless capabilities, prompting policies to exclude electronic devices from secure areas, whether stationary or forward-deployed. Today, those risks are greater than ever, driven primarily by three factors: 1) the ubiquity of wireless-capable devices, 2) the invisibility of the signals they send, and 3) the vulnerability of the protocols they utilize.

For the malicious insider, the first two drivers are sufficient to cause significant damage. The ubiquity (and affordability) of wireless technology lowers the barrier to entry for would-be attackers, putting powerful tools into the hands of less sophisticated actors than ever before. The invisibility of the signals those devices send allows such attackers to act without fear of detection. Until recently, robust solutions to this problem were not available, but today, we can and must do better in bringing visibility to the invisible wireless attack surface.

For the unwitting insider, the unintentional introduction of electronic devices can be just as damaging due to the third driver: vulnerability. To date, almost 3,000 wireless-related CVEs (common vulnerabilities and exposures) have been published in the NIST database with ever-increasing numbers in recent years. These numerous vulnerabilities represent a fraction of what could potentially be exploited. With low-cost hardware and openly available code repositories that implement various attacks, the barrier to entry is lower than ever, enabling bad actors to compromise an insider's electronic devices in numerous ways. Today, every well-meaning person with access to classified information has the potential to unintentionally introduce compromised electronic devices into secure spaces where they become as dangerous to the security of classified information as the malicious insider.

This presentation will examine various wireless devices and threats, including how smartphones become sophisticated surveillance devices against their own users; Wi-Fi pineapples emulate trusted networks, capture devices, and steal credentials; Bluetooth peripherals are appropriated for data exfiltration; IoT devices become unwitting pawns in network-based attacks; and many more. Additionally, we will review hardware and software tools used to conduct wireless attacks and explore how they lower the barrier to entry, making such attacks more feasible to a larger group of bad actors.

Finally, we will present a wireless detection and localization system and discuss its use in identifying and alerting on malicious wireless devices and behaviors. We will review the system architecture, highlight key system components, and discuss analytics tools that are used to bring visibility to the increasingly problematic and invisible wireless attack surface.

BIO: Dr. Brett Walkenhorst is chief technology officer at Bastille, where he leads R&D efforts to enhance product performance and add new capabilities. He has more than 20 years of experience as a technology leader in RF systems and signal processing. Prior to Bastille, he led and executed R&D efforts at Lucent Bell Labs, GTRI, NSI-MI Technologies, Silvus Technologies and Raytheon Technologies. His experience includes RF system design, communications systems, antenna design/testing, radar, software-defined radios, geolocation and related topics. He has authored more than 70 publications, including papers, articles and reports, has taught numerous graduate, undergraduate and professional short courses, and has served as an expert witness on multiple occasions. He is a senior member of IEEE and has served as the chair of the Atlanta Chapter of the IEEE Communications Society.

To the Edge and Beyond: Solving the Growing Demand for Extended Distance Network Devices

Jay Nusbaum, Systems Engineer, Enterprise Networks, CommScope •
Jay.Nusbaum@CommScope.com

ABSTRACT

Ever since the development of PDS in the early 80s, network designers have looked for ways to extend the network and reach devices in far-away spaces in the building. The original method of extending the network was the IDF closet, and it has surely stood the test of time, but the network's utility and importance has grown as the list of IP devices has expanded exponentially, so network designers now need to extend the network into every nook and cranny of the building and surrounding campus.

In this session, we'll discuss future applications that will broaden this demand, and the three best methods of extending the network, reaching further and further than ever before: Hybrid Powered Fiber, Building Edge Infrastructure, and Extended Reach Category Twisted Pair with larger gauge pairs.

The presentation will cover:

- Applications driving this growing demand today and in the future
- Challenges and deployment considerations
- Use cases

BIO: Jay Nubaum has more than 37 years in the industry, the last 18 years with CommScope. Nubaum concentrates on supporting the federal team as well as support territory in the Northeast, United States.

Great Power Information Sharing for Great Power Competition

Russ Smith, Field CTO, Zscaler • rsmith@zscaler.com

ABSTRACT

Breaking down barriers between silos of critical information is key for success in today's Great Power Competition. These barriers, or perimeters, are built around information to ensure information is protected. The zero-trust cybersecurity architecture breaks down those perimeters while greatly enhancing security. The Department of Defense is leveraging cloud service providers (CSP) to embrace this "perimeterless" cybersecurity of a zero-trust architecture. Modern zero-trust architectures must be designed, deployed and operated in a manner that keeps pace with the ever changing threat landscape. Relying on cloud hosted applications and data, while accessing those applications through ubiquitous terrestrial, cellular or satellite transport, is a force multiplier to "fight tonight" if necessary. This presentation will cover the intersection of zero-trust security with 5G cellular transport to deliver cloud-based coalition applications and information to deployed warfighters for success in Great Power Competition.

BIO: Russ Smith is a field CTO supporting Zscaler's Defense, Systems Integrators and Higher Education teams. Russ joined Zscaler after a 30-year Air Force career culminating as the deputy chief information officer at the U.S. Special Operations Command. During his post-military career, he was a research analyst with the Institute for Defense Analyses (IDA), where he researched and made recommendations for improved protection of controlled unclassified information within the Defense Industrial Base. Additionally, he was the vice president of the cyber practice at SAIC as well as a security account lead at Accenture Federal Systems.

Smith holds a Master of Science in systems technology (Joint Command, Control, Communications and Computers) from the Naval Postgraduate School and a Master of Science in military operational art and science from Air University, and a Bachelor's in computer information science from Bloomsburg University of Pennsylvania. He is certified as an information systems security professional, project management professional, chief information officer and chief information security officer.

Software X

Josh Mills, Account Executive, Red Hat • jomills@redhat.com

ABSTRACT

Red Hat will provide an overview of Red Hat's alternative CANES/Agile Core Services design that simplifies the existing architecture by collapsing the infrastructure and application layers in the existing system into a single consolidated platform where containers and virtual machines operate side-by-side. The concept, known as Software X, decouples the hardware from the software and enables over-the-air delivery of core CANES and ACS services. Further, the design and prototype are designed to be installable on HW1.2 and later shipsets during a 30-day availability period.

CANES/ACS Solution:

CANES is partnering with Red Hat Consulting to design and build a proof-of-concept of the Software X concept at NIWC LANT using representative CANES HW1.2 from the USS Champlain.

The Software X strategies include:

- 30-day Backfit Capability: Enables rapid deployment to the fleet on CANES HW 1.2 baselines and newer.
- Rapid Capability Delivery: Push CANES/ACS updates to the fleet in hours, not weeks or months or years. Permits the fielding of an MVP and evolving that baseline dynamically based on fleet feedback.
- Hardware Agnosticism: Modular design deployable to existing legacy hardware already installed on platforms
- New hardware stacks.
- Mix of legacy/new hardware.
- ZTA Enablement: Providing CANES as a service via App Arsenal allows PMW 160 to implement ZTA strategies gradually and push atomic changes quickly and incrementally to a single fleet-wide software baseline.
- Modular Data Centers: Distributing data and applications across multiple points shipboard and simultaneously across geographically dispersed data centers can help ensure continued service in the event of a disaster.

BIO: Josh Mills has been with Red Hat for more than four years. Prior to Red Hat, Mills worked at Gartner for 8 year and HPE for 7.5 years, where he supported Navy and Marine Corps customers in the Pacific AOR. He holds a secret clearance and is a former Naval officer.

Shifting to Highly Assured Data-Centric Security (HADCS)

Keith Strini, Chief Technical Strategist, DOD/IC, Dell • keith_strini@dell.com

ABSTRACT

In the evolving landscape of digital security, we need a revolutionary framework designed to tackle the complexities of data-centric security across modern IT infrastructures. The focus needs to be on building Highly Assured Data-Centric Security (HADCS), which goes beyond traditional perimeter-based security models by shifting the focus to securing the data itself, irrespective of where it resides or how it travels. At the core of this framework there are several advanced technologies that aim to provide end-to-end protection for sensitive data.

These include:

1. **Identity-Native Security:** This emphasizes leveraging hardware-backed identities and cryptographic keys that are fused with the devices and workloads. Each entity interacting with the system—whether a device, workload, or user—carries a root of trust anchored in tamper-resistant hardware.
2. **Post-Quantum Cryptography (PQC):** The near horizon mission need to integrate post-quantum cryptographic techniques, which provide resilience against emerging quantum computing threats. This ensures that sensitive data remains secure, even in a future where quantum attacks become feasible.
3. **Zero-Trust Architecture (ZTA):** The operation under a zero-trust model, which assumes that no entity—whether inside or outside the network—should be inherently trusted. Each interaction within the system requires continuous verification, ensuring a robust layer of security around all data exchanges.
4. **Federated Trust and Governance:** The framework should facilitate secure data sharing across decentralized environments, allowing organizations to maintain control over their data while collaborating securely with external partners.

In this session, we will explore how a framework could combine these cutting-edge technologies to create an ecosystem where data is secured through an integrated, highly automated, and scalable security solution. The session will highlight use cases and discuss how to future-proof systems by adopting HADCS in industries ranging from national defense to critical infrastructure, ensuring that organizations are equipped to meet the security challenges of tomorrow.

BIO: Keith Strini serves as a technical strategist and mission subject matter expert supporting Dell Federal mission-program business. Strini brings his solutions architect experience, with a demonstrated history of working in the computer software industry, to assist federal customers to solve their complex mission-environment challenges. Strini is skilled in DOD/IC operations, CBRNE, cloud consulting (AWS, GCP, Azure, vSphere), networking and architecture-based enterprise systems engineering.

Strini served as the principal engineer responsible for several game-changing efforts across the DoD and IC. Strini built the National Geospatial-Intelligence Agency (NGA) GeoInt Services environment that consisted of AWS C2S and on-premise SIPR clouds and the original "ATO in a Day" implementation that served as the basis of the continuous ATO process in place around the DoD.

Strini is the principal engineer responsible for Kessel Run's Global AOC operational environment spanning five geographies and implemented the first-ever cATO in the DoD under the same effort.

Strini is the principal engineer responsible for Kobayashi Maru's Global Space Operations Center (SpOC) operational environment spanning our FVEY partner (SpOCs). Strini used to build out both the USAF logistics cloud effort (BESPIN) and the Army Futures Command (AFC) software factory and delivered capabilities ranging from edge computing to biological weapons detection and warning systems for the JPEO Chemical, Biological, Radiological, Nuclear, and explosive (CBRNe) office.

Strini served as a technology analyst for Navy PEO C4I, responsible for guiding legacy to modernization migrations to cloud initiatives and served as a senior technical advisor to Defense Threat Reduction Agency (DTRA), Joint Science and Technology Office (JSTO), and Army RDECOM. Strini architected, developed and executed software fielding across the Joint Services both CONUS and OCONUS (Korea, Japan, Europe, and the Middle East).

Intersection of 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. But with this immense power comes immense responsibility. As AI becomes more sophisticated, so too do the potential security risks.

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

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

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.

Streamline Operation Planning, Execution and Reporting

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

ABSTRACT

Coordinating operations is a multi-faceted effort involving logistics, personnel management and communication, scenario planning, reporting and more. This session will approach operations planning as a strategic effort to be managed like any other business portfolio.

Learn how automation of workflows can impact all phases of the operation planning process.

- **Planning and Objectives:** Align operation objectives with mission goals and prioritize exercises based on readiness, risk, and resource availability.
- **Design and Scenario Development:** Cross functional workflows improve collaboration and process accountability.
- **Preparation:** Gain visibility into asset status and track and allocate resources through the same interface used for planning.
- **Execution:** Track results and milestones even in disconnected environments.
- **Assessment and Debrief:** Quickly generate reports and provide dashboards that also highlight opportunities for continuous improvement for future operations.

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.

Prem has a deep understanding of how U.S. Department of Defense organizations operate, from IT implementation and program management perspectives. He spent 8 years within the Naval Information Warfare Systems Command (NAVWAR) program offices, managing the engineering, configuration, risk, program and acquisition of systems and applications deployed on U.S. Navy ships. He is a certified ServiceNow System Admin, holds certifications from Program Management Institute (PMI) for Program Management and Risk Management, and obtained a Certificate for Leadership and Management from Wharton School, Aresty Institute of Executive Education.

edgeCore: A Digital Twin Solution Built on a Proven Data Mesh to Ensure Decision Dominance in a Dynamic Battlespace

Jacques Jarman, Chief Growth & Federal Operations Officer, Edge Technologies • jacques.jarman@edge-technologies.com

ABSTRACT

In the INDOPACOM AOR, our forces face significant mission and logistical challenges due to vast distances and a sophisticated threat environment. Adversaries target supply chains and logistics networks with advanced kinetic and digital tactics. To counter these threats, the U.S. must achieve decision dominance by integrating real-time situational awareness across all mission and logistics functions—such as weapon systems, mission planning, fuel, supplies, equipment and power. A major challenge is providing decision-makers with timely, actionable information amid an overload of data often stored in redundant, siloed data warehouses and data lakes across various agencies and coalition partners. This fragmentation makes it difficult for warfighting communities ranging from special ops, C2, ISR and even combat support functions such as logistics planning to access critical, actionable information swiftly, hampering their ability to respond to rapidly evolving threats.

BIO: Jacques Jarman is the chief growth and federal operations officer at Edge Technologies. Jarman is a technical business executive focused on setting corporate direction and facilitating all aspects of government operations to meet the needs of edge's customer base. With more than 25 years of experience addressing situational awareness, data integration, big data and emerging AI & digital twin technologies, Jarman is a recognized subject matter expert and invited AFCEA, NDIA, TechConnect speaker. Jarman holds a Bachelor of Science from Virginia Tech.

Hitchhikers Guide to API Security for AI Based Apps

Paul Deakin, Principal Solutions Engineer, F5 Networks • p.deakin@f5.com

ABSTRACT

As AI workloads increasingly rely on APIs for seamless integration and functionality, ensuring their security, monitoring and discovery become critical. APIs serve as the backbone for data exchange, model deployment and real-time decision-making in AI systems. However, this creates unique challenges across the DoD, such as safeguarding sensitive data, mitigating potential attack vectors and managing complex API ecosystems.

In this presentation, we will explore why DoD environments need robust API security measures, effective monitoring to ensure performance and compliance, and reliable discovery methods to track and manage evolving APIs in AI workflows, highlighting strategies to overcome these challenges.

BIO: Paul Deakin is a principal solutions engineer working with the DoD group primarily with the U.S. Air Force at F5, a company focused on delivering industry-leading solutions for application delivery analytics and security. He has 20 years of experience in the technology industry, with 9 years in the security environment, including leadership roles in directing large-scale projects; and implementation of software/hardware in complex environments; exposure to a wide variety of businesses including insurance, manufacturing, government, aerospace, financial, and healthcare. He holds a master’s degree in computer science and is an F5 Certified Solution Expert in security and cloud.

XD Vision

Michael Blake, Technical Fellow, Owl Cyber Defense • mblake@owlcyberdefense.com

ABSTRACT

Witness an exclusive unveiling of XD Vision, the next-generation cross domain solution (CDS) from Owl Cyber Defense. Soon to be certified and approved for deployment, XD Vision is the world's first and only CDS designed for secure, multi-domain audio (VoIP) and video (VTC & FMV) collaboration. XD Vision combines RTB-compliant security with an elegant, user-friendly interface, empowering operators and commanders to communicate seamlessly across secure network domains.

BIO: With more than 25 years of hands-on experience in the software industry, Michael Blake is a visionary IT professional known for driving the planning, architecture, deployment and management of cutting-edge smart systems. His expertise extends to incorporating the latest technologies, including cyber defense, to develop innovative solutions. Blake has played a pivotal role in the acquisition of the ACS business unit by DC Capital, integrating it into Owl Cyber Defense's SPAC. As chief architect and technical fellow at Owl, he has a team of 30 professionals and oversees product roadmaps, sales strategy, technical engagements with certification boards and corporate strategy.

WHAT IS AFCEA?

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