



WEST2025 INNOVATION SHOWCASE

JANUARY 28-30, 2025 • SAN DIEGO, CALIFORNIA



SIGNAL
AFCEA INTERNATIONAL MEDIA

WEST 2025 Innovation Showcase

The Future is Now: Are We Advancing Operational Capabilities That Pace the Threat?

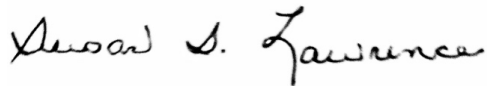
Sea Service leaders today confront profound and rapidly changing threats in a landscape of increasingly complex challenges. During this three-day WEST 2025 conference, experts will one, explore the depths of the unique issues our warfighters confront, and two, work to answer the conference theme question: “are we advancing operational capabilities that pace the threat?”

Some of those answers could be unveiled during the “Innovation Showcase” sessions, during which innovators will demonstrate cutting-edge solutions.

And speaking of innovators, experts who speak at AFCEA International conferences continually stress the value of innovation in this digital age. The consensus is that we must align strategy and resources to enable the rapid integration of new technologies, operational concepts and training to continually adapt those changing threats and to fight and win the race for emerging technologies. We absolutely must give our warfighters and decision-makers the edge in solving the challenges.

AFCEA continues to do its part to share information, to build partnerships and to find the answers, including hosting these Innovation Showcase presentations and preparing this compendium. A lot of work needs to be done and there are many challenges to overcome to promote faster, more efficient and effective collaboration across our government and among multiple governments. And the content on these pages is an optimal place to start.

Best wishes,



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

Table of Contents

From Legacy Data to Next-Generation Data Architecture for Digital Transformation Samuel Chance, Lead Solutions Architect, Altair	10
Boosting Tactical Network Performance and Cyber Resilience with a Modern Approach to Testing Cade Nelson, Sales Engineer, Aposite Technologies.....	11
Buzzwords Meet the Battlespace: How AI/ML, Network Centric Warfare and Contested Logistics Come Together at the Data Level Rear Adm. Christian 'Boris' Becker (Ret.), Founder & President, Silvergate Consulting, AtomBeam Technologies	12
The Impact of Holographic Visualization on Military Operations Wally Haas, Founder & President, Avalon Holographics.....	14
Identity Security: Eliminate Privilege Escalation as Part of Your Zero Trust Strategy James Ebeler, Vice President, Technology Solutions, Emergent360 Brendon Kruk, Enterprise Account Manager, BeyondTrust, BeyondTrust, Inc. & Emergent360	15
A Comparative Study of RF Power Meters for Digitally Modulated Signals in Military Applications Russell Buttriss, Applications Engineer, Bird Electronic Corporation	16
Achieve Mission Efficiency in the Software Supply Chain at the Speed of the Battle John Savio, Executive Director, Public Sector and Defense, Black Duck Software	17
Broadcom: Unified Data Management Burt Wagner, Data Solutions Architect, U.S. Federal, Broadcom	18
The ABCs of Software Supply Chain Security: Starting with XZ and Finding the Y Connor Wynveen, Solutions Engineer, Chainguard	19
AI in the Trenches: Leveling Up Cyber Talent and Defending our Critical Infrastructure Aaron Rose, Security Architect Manager, Check Point Software Technologies	20
Understanding the Risks, the Rewards and our Relationship with Artificial Intelligence—A CISO's Perspective Cindi Carter, Global Chief Information Security Office, Check Point Software Technologies.....	21

Bladerunner is Here Now!
David Robertson, Director, Federal Engineering, Check Point Software Technologies. 22

Harnessing the Power of AI to Manage the Implementation of a Zero-Trust Framework
David Robertson, Director, Federal Engineering, Check Point Software Technologies 23

Navigate the Challenges of Air-Gapped Environments With Modern Day Defense Shared Intelligence
David Robertson, Director, Federal Engineering, Check Point Software Technologies 24

Harnessing the Power of Generative Adversarial Networks: Creating and Detecting Deepfakes in the Era of Synthetic Media
Michele Boland, Global Technologist, Office of the CTO, Check Point Software Technologies 25

5G Secure Wireless with Post Quantum Cryptography
Ron Malenfant, Head of 5G Strategy and Architecture, Ciena & IncrediTek..... 26

Revolutionizing Naval Operations with Generative AI
Rick Taylor, Senior Solutions Engineer, Cloudera..... 27

Utilizing AI to Unlock Data Essential to Mission Success
Marlin McFate, Public Sector CTO/CISO, Cohesity..... 28

Colvin Run Networks: The IRONCLAD Initiative
Nikhil Shenoy, CEO & Founder, Colvin Run Networks 29

CommScope: Extending the Network
Jay Nusbaum, Systems Engineer, Enterprise Networks, CommScope..... 30

Transitioning to Wi-Fi 6e & 7
Rick Macchio, Consulting Systems Engineer, CommScope..... 31

Bridging the Data Divide: Advancing Mission Readiness and Cyber Resilience in Maritime Operations through Strategic Data Management
Derek Gleich, Manager, Solutions Engineering, Cribl 32

Advancing Operational Capabilities While Adversaries Target Your Identity
James Imanian, Senior Director, U.S. Public Sector Technology Office, CyberArk Software..... 33

Driving Mission Readiness: Empower Federal Missions With Trusted AI Justin Swansburg, VP, Applied AI & Technical Field Leads, DataRobot	34
Build Winning Sales Plans for the Department of Navy John Slye, Senior Advisory Research Analyst, Deltek	35
Building Brilliant Machines Zac Staples, CEO & Founder, Fathom5	36
Risks to AI Adoption for U.S. Sea Services Parth Vakil, Vice President, Global Field Engineering, HiddenLayer	38
Hunted Labs: Securing the Software Supply Chain Hayden Smith, Chief Technology Officer & Co-Founder, Hunted Labs	39
Industrial Defender—Operational Technology: Protecting Cyber Resilience and Operational Continuity Alex Bagwell, Chief Revenue Officer, Industrial Defender	41
Innovative Ways to Solve Tech Debt for Federal Customers—Hardware as a Subscription (HWaaS) Wade Lehrschall, Distinguished Architect, Iron Bow Technologies	42
Mission-Focused WAN Modernization—Software-Defined Unified Transport Network (SD-UTN) Wade Lehrschall, Distinguished Architect, Iron Bow Technologies	43
Building an AI-Enabled Foundation for Electronic Warfare Collection, Process and Exploitation J. David ‘TUBA’ Britt, Vice President, Defense Technology & Innovation, ManTech	44
Automation, AI and Scalability: A New Era in DoD Cyber Risk Management Brian Recore, Systems Engineer, Merlin Cyber.....	46
Treating Platform as a Product for Resilient Delivery of Software to the Warfighter Hannah Hunt, Distinguished Technical Fellow, MetroStar Systems.....	48
Integrated Respirator Information System Joe Early, Senior Director, R&D Solutions, MetroStar Systems	49

Traditional Software Composition Analysis (SCA) Is Not Enough: Protecting Mission-Critical Software	
Bryan Whyte, Director, Solutions Engineering, MFGS Inc. & Sonatype.....	51
Make Your Artificial Intelligence Analytics More Accurate by Leveraging an Effective ETL Process	
Chris Kelly, Big Data Solutions Sales, MFGS Inc.....	52
The Operational Data Interop Imperative—Architecting an Intelligent Data Infrastructure to Share and Secure Critical Data to Ensure Mission Operation Advancement	
Jim Cosby, Chief Technology Officer, NetApp	53
The Multi-Domain Data and Information Sharing Conundrum—Building an Effective and Secure Data Information Sharing Architecture to Provide Collaborative Mission Execution	
Jim Cosby, Chief Technology Officer, NetApp	54
The Zero-Trust Data Centric Challenge—Building a Functional Data Centric Sharing Architecture with Effective Zero-Trust Controls to Drive Operational Advancement	
Jim Cosby, Chief Technology Officer, NetApp	55
Protecting Technological Innovation: Educating the Next Generation of Cyber Risk Management Professionals	
Rafael Diaz, Ph.D., Graduate Program Director, School of Cybersecurity, Old Dominion University	56
Internships Are One Great Idea, So What Other Innovative Ideas Can We Explore?	
Teresa Duvall, Faculty Lecturer, School of Cybersecurity, Old Dominion University.....	57
Fortifying Federal Security: Implementing Zero Trust and Cross-Domain Solutions\Multi-Level Security Solutions	
Chris Betz, Chief Technology Officer, Federal, Omnisia.....	59
Ocean Wave-Powered Underwater Charging	
Priscilla Prem, CEO & Founder, Pittsburgh Coastal Energy	60
Introducing The Risk Operations Center: Orchestrating the Elimination of Mission-Critical Cybersecurity Risk	
Richard Seiersen, Chief Risk Technology Officer, Qualys	61
Software X	
Tom Skradski, Application Platform Solutions Specialist, Red Hat	62

Generative AI for the Cyber Warfighter	
Andres Giraldo, Director of Innovation, Sealing Technologies Inc.	63
Securing Information Anywhere	
Richard Streeter, Operations Director, Sertainty	64
Operating Through the “Unknown Unknowns”	
Adam Prem, Global Lead, Defense and Security Mission Solutions, ServiceNow	65
Meeting the Speed of Mission with Generative AI	
Thomas Calabrese, Certified Technical Architect, ServiceNow	66
Revolutionizing the Intelligence Cycle Through Innovation	
Vincent Nguyen, Business Development and Enablement Manager, Starboard Maritime Intelligence Inc.	67
Best Practices for Implementing Quantum-Resistant Security	
Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies	69
Intersection of Quantum, AI and Security	
Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies	70
SAP and UiPath, Better Together: Navigating Innovation in Navy ERP Modernization	
Jonathan Moak, Vice President, Federal, UiPath Inc.	71
Modernizing Defensive Cyber Operations—the AI Imperative	
Zachary Vaughn, Director, Federal Security Engineering, Vectra AI	73
Deploying Containers and Virtual Machines in Kubernetes for Future-Ready Naval Operations	
Greg McPhee, Federal Solutions Architect, Veeam	74
The Future and Innovation of Navy Base Communications: Merging Industry Best Practices and Technologies with Navy Culture	
Dominic Bonaduce, Senior Product Strategy Manager, Verizon	75

Submissions

From Legacy Data to Next-Generation Data Architecture for Digital Transformation

Samuel Chance, Lead Solutions Architect, Altair • schance@altair.com

ABSTRACT

Digital transformation requires a next-generation data architecture that enables pervasive artificial intelligence and autonomous information systems to maintain competitive advantage. Standards-based, machine understandable knowledge graph technology and associated methodologies provide the way forward. This presentation articulates the characteristics, advantages and applications of knowledge graph technology and how it changes today's transactional workflow paradigm to increasingly autonomous behaviors.

Boosting Tactical Network Performance and Cyber Resilience with a Modern Approach to Testing

Cade Nelson, Sales Engineer, Apposite Technologies • cade@apposite-tech.com

ABSTRACT

The rapid evolution of digital networks and cybersecurity threats pose significant challenges to defense organizations and civilian agencies whose success hinges on reliable communication systems and robust cybersecurity defenses. Validating the performance of these mission-critical systems under real-world conditions is essential—but often difficult. This session will introduce a modern, easy-to-use approach to performance testing that empowers government agencies and the military to evaluate and optimize networks in a controlled, repeatable lab environment before deployment.

During this session, we will explore how to:

- Simulate real-world network impairments like latency, bandwidth constraints and adverse weather.
- Generate high-scale, realistic traffic to measure performance metrics and validate Quality of Service (QoS).
- Combine legitimate application traffic with simulated malicious attacks to strengthen cyber defenses.

Reliable, repeatable testing can harden tactical communications, validate DDoS defenses and optimize network performance. Join us to learn how our technologies are enabling a new era of secure, resilient, and high-performing mission-critical systems for today's complex threat environment.

BIO: Cade Nelson has been in the networking business since 1996, when he was hired as employee number 56 at Earthlink Networks. He has held positions as Senior Network Engineer, Systems Integration Engineer and Product Engineer at many tech companies. Nelson has been called the “Swiss army knife” of Apposite Technologies, where he wears many hats, from product engineering to product development.

Buzzwords Meet the Battlespace: How AI/ML, Network Centric Warfare and Contested Logistics Come Together at the Data Level

**Rear Adm. Christian ‘Boris’ Becker (Ret.), Founder & President, Silvergate Consulting
AtomBeam Technologies • boris.b@atombeamtech.com**

ABSTRACT

The concept of network centric warfare (NCW) has been pivotal in shaping military strategy since at least the 1990s, certainly following the publication of Joint Vision 2010 by the Joint Chiefs of Staff. At its core, NCW transforms data from the edge into actionable information and from there into knowledge with which commanders at the core can then take action directly or enable action closer to the edge. As we reflect on the journey from JV 2010, Sea Power 21 and other looks to the future that is now our present’s past, it’s important to examine the evolution of NCW and its impact on modern warfare.

In military operations, logistics is not simply a support function; it is a critical pillar that underpins success. As Gen. Omar Bradley famously stated, “Amateurs talk tactics, professionals study logistics.” The principle of logistics is ever relevant in the Indo-Pacific Command area of responsibility, which encompasses more than 100 million square miles. In contested logistics environments, where adversaries may attempt to disrupt supply lines, real-time data analysis and secure information flow become paramount for mission success. Effective management and transmission of data are crucial for maintaining supply chains, coordinating troop movements, and ensuring operational readiness. By leveraging cutting-edge technologies currently used in sectors like oil and gas or mining, we can apply innovative data-centric solutions to the government space. This approach will revolutionize contested logistics, providing needed improvements in challenging environments.

Atombeam Technologies directly addresses these issues by revolutionizing how the military can move, use, store and secure data with its innovative Data-as-Codewords technology. Fundamentally, data management is the cornerstone of AI-enabled NCW in support of contested logistics. To transform these buzzwords into meaningful battlefield realities, we must first revolutionize their foundation: data.

Learn from retired Navy Rear Adm. Chris ‘Boris’ Becker, Board Member of Atombeam Technologies and former commander of the Naval Information Warfare Systems Command about:

- What NCW is and how has it progressed from Joint Vision 2010 to modern day
- How artificial intelligence and machine learning evolved in military applications focused on NCW
- Why data management is crucial in contested logistics and how can lessons from commercial industries be applied to military operations

BIO: Board Member of Atombeam Technologies, retired Rear Adm. Christian ‘Boris’ Becker has

more than 30 years of distinguished service in the U.S. Navy and led high-performing organizations in advanced technology and defense sectors. He graduated from Boston University in 1987 with a B.S. in electrical engineering. As the former Commander of the Naval Information Warfare Systems Command (NAVWAR), he oversaw an 11,000-person global organization responsible for the Navy's digital, cyber and space systems. After retiring from the Navy, Becker transitioned to industry, serving as a senior advisor, C-level executive and board member in space and information technology companies. He is the founder and president of Silvergate Consulting and sits on the board of Atombeam Technologies.

The Impact of Holographic Visualization on Military Operations

Wally Haas, Founder & President, Avalon Holographics •

wally.haas@avalonholographics.com

ABSTRACT

Holographic visualization used to be “the future.” Now it’s quickly becoming the present. What does that mean for military operations?

Our game-changing display delivers a powerful user experience and superior visualization capabilities that enables military and defense teams to engage with mission data like never before. Immersive, intuitive and incredibly detailed, holographic displays sharpen decision-making and increase situational awareness.

BIO: Wally Haas is a successful serial entrepreneur with more than 25 years in high technology industries. Haas has a bachelor’s degree in electrical engineering from the University of Calgary. His career has led him to work in St. John’s, Ottawa, and the United Kingdom, and he has traveled extensively, collaborating with customers in North America, Europe and Asia. Haas has worked for companies such as Nortel, PMC-Sierra and AMCC, focused on semiconductor design for optical networking. When Haas moved to Newfoundland and Labrador for family reasons, he founded Avalon Microelectronics to continue his career and passion for semiconductors. Without the need for any venture capital, Haas grew the company to 31 people and nearly \$4 million in annual revenue. Avalon Microelectronics sold to Altera (now part of Intel) in 2010 after less than 5 years of effort. In 2015, Haas founded Avalon Holographics and has led a team of more than 70 people since then.

Identity Security: Eliminate Privilege Escalation as Part of Your Zero Trust Strategy

James Ebeler, Vice President, Technology Solutions, Emergent360 and Brendon Kruk, Enterprise Account Manager, BeyondTrust, Inc. • jebeler@emergent360.com and bkruk@beyondtrust.com

ABSTRACT

The ever-growing threat of cyber attacks faced by the Department of Defense are almost always the result of exploitable privilege as the key technique required to escalate access and move laterally.

A higher degree of privileged access protection is required to reduce and eliminate privilege exploitability. Identity-based policies to enforce the principle of least privilege are required in all threat vector contexts, granting users the minimum level of access necessary for their roles, without reducing speed or capabilities.

A complete identity, credential and access management (ICAM) solution is critical to the foundational phase of any zero-trust architecture effort. Join us for a discussion around BeyondTrust and Emergent 360 integrated ICAM solution that is comprehensive, cost-effective, simple to manage, easily accessible and sustainable.

BIO: James Ebeler is the Vice President Technology Solutions at Emergent 360. Ebeler brings more than two decades of experience developing strategy and technology for go-to-market and branded solutions across the Department of Defense (DoD), including posturing IT Solutions to deliver successful client outcomes. Prior to joining Three Wire, Ebeler was the Chief Technology Officer for the Department of Defense at Iron Bow Technologies and within the U.S. Army. Ebeler has specific expertise as a technical leader for establishing policy, guidance, planning and functional advocacy to create organizational technology roadmaps. He also has experience in many technical solutions surrounding zero-trust architecture and enterprise IT as a service.

Brendon Kruk, Enterprise Account Manager, has more than 10 years of U.S. federal government experience. DOJ, DOL, Air Force, Army, CoCom experience with DevSecOps and large Identity and Access Management (ICAM), zero trust, FICAM, cross-domain, cyber programs and mainframe solutions. Extensive current contacts across the DoD and fed.

A Comparative Study of RF Power Meters for Digitally Modulated Signals in Military Applications

Russell Buttriss, Applications Engineer, Bird Electronic Corporation •

RButtriss@BirdRF.com

ABSTRACT

Modern military communication systems increasingly rely on digitally modulated signals, necessitating accurate RF power measurements to ensure operational efficiency and regulatory compliance. Traditional RF power meters like the Bird 4410A, designed for continuous wave and frequency-modulated signals, exhibit significant inaccuracies when measuring complex digital modulation schemes due to their reliance on conventional diode detector technology. This paper presents a comprehensive comparison between the legacy Bird 4410A and the advanced Bird 4480A digital power meter, which employs Schottky diodes operating in the square law region to provide accurate average power measurements independent of modulation format. Through rigorous testing, including side-by-side measurements with a thermal power meter as a reference, we demonstrate the limitations of the 4410A and the superior performance of the 4480A across multiple modulation types, including amplitude modulation (AM) and quadrature amplitude modulation (QAM). Our findings underscore the critical need for military systems to adopt modern power meters capable of accurately handling digitally modulated signals, thereby enhancing communication reliability and system integrity.

BIO: Russell Buttriss is an Applications Engineer at Bird Electronic Corporation in Solon, Ohio, specializing in the use of in-line directional power meters to accurately measure true average power and assess antenna match characteristics in advanced communication systems—particularly those utilizing complex modulation schemes in military contexts. He also provides hands-on instruction in RF fundamentals and antenna line sweeping techniques using frequency domain reflectometers, training technicians and field operators.

Before joining Bird Electronic Corporation, Buttriss served as a Radio Operator in the United States Marine Corps. His military service included two deployments supporting flightline operations and later served at Quantico, Virginia, as Platoon Sergeant of the Communications Platoon supporting The Basic School. After his military service, he earned a Bachelor's degree in electrical engineering from Cleveland State University, graduating with honors.

Combining a strong military background with deep technical expertise and academic achievement, Buttriss applies a practitioner's insight and an engineer's precision to address complex RF and communications challenges.

Achieve Mission Efficiency in the Software Supply Chain at the Speed of the Battle

John Savio, Executive Director, Public Sector and Defense, Black Duck Software •

jsavio@blackduck.com

ABSTRACT

It is critical to deliver software capabilities to the warfighter with high quality, security and safety, while reducing cycle time and costs. Hear how Black Duck is working with the Department of Defense to achieve continuous authority to operate and to accelerate capability delivery within the software supply chain. We'll discuss our role within the RAISE process and how we are enabling them to get mission critical upgrades to the fleet faster than ever.

BIO: John Savio is a seasoned technology leader with extensive expertise in leading public sector software teams and fostering innovation in software solutions. As Executive Director of Public Sector and Defense at Black Duck Software, Savio leads efforts to help government agencies and systems integrators create software that is secure, of high quality and safe for mission-critical applications that support the warfighter. With more than three decades of experience, he is passionate about delivering solutions that meet the unique needs of public sector clients, combining strategic insight with a deep understanding of technology trends.

Broadcom: Unified Data Management

Burt Wagner, Data Solutions Architect, U.S. Federal, Broadcom • burt@broadcom.com

ABSTRACT

Is your data EVERYWHERE, and you can't use it all together? Even if you could, what analysis could you do? What about AI/ML? Broadcom's Unified Data Management (UDM) solution can help centralize your data, perform myriad analyses, create AI and ML models and even proactively distribute these products where they're needed most.

BIO: Burt Wagner has been supporting DoD and intelligence community customers as a data architect for more than 20 years. He has depth in data governance, data security, advanced analytics and AI/ML, as well as an advanced degree in data science.

The ABCs of Software Supply Chain Security: Starting with XZ and Finding the Y

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

ABSTRACT

The software supply chain faces increasingly sophisticated attacks, from malicious backdoors in critical open-source projects to exploited vulnerabilities in widely used dependencies. High-profile incidents like SolarWinds, Log4Shell, XZ and the recent npm compromise underscore a troubling trend: hidden threats are becoming harder to detect and mitigate.

For years, security professionals in the federal industry have asked, “Can you determine whether open-source contributors are linked to adversary nations or known threat actors?” The XZ backdoor turned this fear into reality. While solving the challenge of verifying every contributor is daunting, the question remains: what can we do today to protect our software supply chains?

This session emphasizes getting the basics (the ABCs) of software supply chain security right. We’ll dive into practical strategies for building truly minimal container images—ensuring they are up-to-date, secure by default, and with a minimal attack surface—so your organization spends less time patching vulnerabilities and more time mitigating risks.

BIO: Connor Wynveen is a solutions engineer at Chainguard serving the public sector market. With a decade of experience in the public sector, Wynveen has focused most recently on advancing organizations’ container security and DevSecOps practices. During his six years as a systems engineer at Booz Allen Hamilton, he supported more than a dozen DoD programs in managing their technical baselines and integrating emerging technologies.

AI in the Trenches: Leveling Up Cyber Talent and Defending our Critical Infrastructure

Aaron Rose, Security Architect Manager, Check Point Software Technologies •
arose@checkpoint.com

ABSTRACT

As artificial intelligence (AI) continues to revolutionize cybersecurity, it's no longer just a tool—it's a force multiplier. This session explores how leveraging AI can elevate the skills of cybersecurity practitioners at all levels, from entry-level analysts to seasoned experts, creating a more agile and effective workforce capable of responding to sophisticated threats. We'll also dive into the responsible use of generative AI, addressing the critical need to protect sensitive data like PII and organizational assets. Attendees will gain insights into how AI can be used to both enhance human talent and shore up defenses, while navigating the ethical challenges that come with integrating these powerful tools into everyday cybersecurity operations.

BIO: Aaron Rose is a Cybersecurity Evangelist, Security Architect Manager and a member of the Office of the CTO at Check Point Software Technologies. As a subject matter expert in artificial intelligence and application security, Rose has dedicated his career to securing organizations and their resources beyond the traditional network firewall. Passionate about making cybersecurity education accessible to all, Rose actively engages as a guest lecturer, mentors students and assists in the development of cybersecurity courses. An avid international traveler, Rose spent three months in Tel Aviv, Israel, training with Check Point's research and development teams at the company's global headquarters.

Understanding the Risks, the Rewards and our Relationship with Artificial Intelligence—A CISO’s Perspective

Cindi Carter, Global Chief Information Security Office, Check Point Software Technologies • cindic@checkpoint.com

ABSTRACT

Today, every company (and CISO) is confronting questions about how artificial intelligence (AI) will apply to them and their industries. Whether it means a significant pivot in their operating models or an opportunity to scale and broaden their offerings, all organizations must assess their readiness to deploy AI responsibly without perpetuating harm to their stakeholders and the world at large. In this talk, Cindi Carter will share thought-provoking, actionable advice on this topic for all audiences.

BIO: Cindi Carter is a global, multi-industry Cybersecurity and Information Technology Executive who consistently delivers the optimal outcome. As a transformational leader from startups to enterprises, she excels at building cybersecurity practices in highly regulated industries, turning strategic goals into action, and highly collaborative engagement to lead the organization in managing cyber risk. At Check Point Software Technologies, Carter is a Global Chief Information Security Officer in the Office of the CISO, leading Check Point’s Healthcare Center of Excellence, where human safety is essential to care. With more than two decades in the health care and financial industries, Carter’s purpose is deeply rooted in human safety, bringing together the capabilities that protect the security and privacy of each individual. Carter is the founding president of Women in Security – Kansas City 501(c)(3), was honored in SC Media magazine’s “Women to Watch in Cyber Security,” and was featured in Cybersecurity Venture’s book, “Women Know Cyber: 100 Fascinating Females Fighting Cybercrime.” She presents at conferences worldwide, holds several recognized IT, security, and project management certifications and has a Master of Science degree in Information Technology.

Bladerunner is Here Now!

David Robertson, Director, Federal Engineering, Check Point Software Technologies •
droberts@checkpoint.com

ABSTRACT

We are now living in a “post-real society” where voice, pictures and videos can be faked. Learn about how artificial intelligence-based technological advancements are impacting us and the latest countermeasures.

The presentation is a fun and fast-paced review of the newest AI-based threats and countermeasures.

- a. Current State of the art of voice, photo and video cloning
- b. AI bias, hallucinations and other risks
- c. Criminal use of AI tools
- d. AI and business countermeasures necessary to combat new threats

BIO: David Robertson is a globally recognized evangelist and director of federal engineering at Check Point Software Technologies. Over the course of more than two and half decades, Robertson has been instrumental in supporting the cybersecurity mission of the Department of Defense and assisting civilian agencies in enhancing their knowledge and environments to effectively address the evolving global security challenges they encounter.

Harnessing the Power of AI to Manage the Implementation of a Zero-Trust Framework

David Robertson, Director, Federal Engineering, Check Point Software Technologies •
droberts@checkpoint.com

ABSTRACT

The Department of Defense Zero Trust Overlays proposes a security framework that aligns with security controls to zero-trust capabilities, activities and outcomes. The framework will aid the Department of Defense in transitioning from a trusted environment model to a zero-trust, AI-model architecture. Let us engage in a thorough discussion on strategy encompassing the identified zero-trust controls and explore how automation and orchestration can facilitate a secure and safe environment with AI.

BIO: David Robertson is a globally recognized evangelist and director of federal engineering at Check Point Software Technologies. Over the course of more than two and half decades, Robertson has been instrumental in supporting the cybersecurity mission of the Department of Defense and assisting civilian agencies in enhancing their knowledge and environments to effectively address the evolving global security challenges they encounter.

Navigate the Challenges of Air-Gapped Environments With Modern Day Defense Shared Intelligence

David Robertson, Director, Federal Engineering, Check Point Software Technologies •
droberts@checkpoint.com

ABSTRACT

The Department of Defense encounters global challenges that require a strengthened security posture, primarily stemming from stringent compliance requirements. The imperative to safeguard classified data and secure cross-agency threat intelligence sharing requires both a comprehensive solution and a tailored approach. In response to these challenges, David Robertson will explore the advantages of a private threat cloud designed for air-gapped environments, ensuring data privacy, compliance and scalable threat protection.

BIO: David Robertson is a globally recognized evangelist and director of federal engineering at Check Point Software Technologies. Over the course of more than two and half decades, Robertson has been instrumental in supporting the cybersecurity mission of the Department of Defense and assisting civilian agencies in enhancing their knowledge and environments to effectively address the evolving global security challenges they encounter.

Harnessing the Power of Generative Adversarial Networks: Creating and Detecting Deepfakes in the Era of Synthetic Media

Michele Boland, Global Technologist, Office of the CTO, Check Point Software Technologies • mboland@checkpoint.com

ABSTRACT

The rapid evolution of deepfake technology has ushered in a new era of innovation and risk, where artificial intelligence can convincingly manipulate reality. This presentation delves into the dual-edged nature of Generative Adversarial Networks (GANs)—the very framework that enables the creation of highly convincing synthetic media and serves as a powerful tool in its detection. Attendees will gain deep technical insight into how GANs operate, through a hands-on demonstration showcasing the step-by-step creation of a deepfake video. In parallel, Micki Boland will unveil how the same adversarial architecture that creates these forgeries can be leveraged to detect them, using cutting-edge GAN-based detection methods. By exploring the generative-discriminative paradigm, this session will reveal the intricate balance between offensive and defensive AI techniques in the cybersecurity landscape. With deep technical details and practical insights, this talk aims to equip cybersecurity professionals and researchers with a thorough understanding of GAN-driven deepfake generation and detection, providing new perspectives on defending against this growing threat. Join as we decode the adversarial game of deception and detection in this digital realm we live in.

BIO: Micki Boland is a global technologist and cyber warrior with Check Point Software Technologies Office of the CTO. A leader, innovator and practitioner with more than 20 years in ICT, cybersecurity and emerging technology innovation with expertise in financial, health care, energy and high-tech manufacturing sectors, Boland holds ISC2 CISSP, Master of Science in technology commercialization from the University of Texas at Austin, and MBA with global security concentration from East Carolina University.

She recently completed MIT No Code AI and Machine Learning Building Data Science Solution certificate program. Boland is a United States Army veteran. Boland frequently writes cybersecurity articles for Cybertalk.org, has contributed to articles for WSJ, Dark Reading, Silicon Angle, Decipher, Security Boulevard, and speaks frequently with the broadcast media and radio shows regarding cybersecurity and emerging technology, the global threat landscape, tips and resources for enterprise organizations and consumers, Dark Web research, Deepfake technologies and threats, cybercriminal gangs, cloud security, and DevSecOps. Her focus over the last few years is AI-based proactive threat intelligence (ML/NN/deep learning), and generative AI, helping organizations adopt GenAI without trading off security and ways to leverage GenAI to stay ahead of the adversary.

5G Secure Wireless with Post Quantum Cryptography

Ron Malenfant, Head of 5G Strategy and Architecture, Ciena & IncrediTek •

malenfa@ciena.com

ABSTRACT

Ciena and IncrediTek have joined forces to develop an innovative secure 5G solution, 5G Secure Wireless with post quantum cryptography. By leveraging purism secure U.S.-made end user devices and a 5G American-made RAN, this solution delivers enhanced security to a secure 5G deployment, ensuring government operations can adapt and thrive in today's fast-paced digital world. Our solution harnesses the power of an adaptable 5G architecture and post quantum cryptography (PQC) to deliver tailored solutions and capabilities designed to meet unique operational requirements. We will cover end-to-end arch from 5G UE to RAN and MEC, 5G AI enablement, 5G Core and slicing and the disaggregation of the 5G RAN and virtualization along with Ciena 5G Transport and X-Haul 5G carrier class features. We will also cover the 5G tactical use cases, ship to shore, ship to ship, campus and base secure deployments.

BIO: Ron Malenfant is an industry expert in mobility and IoT and presently Head of 5G Strategy and Architecture for the Sales CTO organization at Ciena and also on the 5G Americas Board of Governors driving 5G adoption and innovation. Malenfant is focused on 5G mobility and building new markets for Ciena and driving mobility into existing markets in DoD/federal, Enterprise and MNO and MSO markets. Prior to Ciena, Malenfant was Vice President at JMA Wireless focusing on strategic accounts building out private 5G and CBRS markets and initial insertions into DoD private 5G opportunities. Prior to JMA, Malenfant was with Cisco for 22 years leading and building mobility, 3G/4G/5G CBRS and Wi-Fi along with IoT, smart cities and mobile security solutions and development. Malenfant has developed industry innovation such as the connected athlete where the player, fan and coach experience has been increased through the use of on body sensors, analytics, mobility and IoT which was showcased at CES along with a Tier 1 MNO and the NFL. Malenfant has spoken at many conferences and workshops globally around 5G, IoT, connected vehicles and smart cities.

Revolutionizing Naval Operations with Generative AI

Rick Taylor, Senior Solutions Engineer, Cloudera • rtaylor@cloudera.com

ABSTRACT

The Navy's reliance on artificial intelligence (AI) and machine learning (ML) continues to grow, transforming operations in areas like Condition Based Maintenance Plus (CBM+) and supply chain management. Generative AI (Gen AI) offers unprecedented potential to further revolutionize naval capabilities.

This talk explores how a secure, robust and scalable data platform delivers AI as a Service and empowers the Navy to harness the power of Gen AI.

By addressing critical challenges such as data security, model governance and operational efficiency, our solution enables cost effective development and deployment of robust Gen AI applications.

Key platform features should include:

- **Robust Security and Governance:** Ensuring the protection of sensitive data and maintaining control over AI-generated content.
- **Model Management:** Streamlining the development, deployment, and monitoring of AI models.
- **Optimized Performance:** Delivering high-performance AI inference at the edge.
- **Seamless Data Integration:** Facilitating access to diverse data sources for training and inference.

AI and Gen AI are only as good as the data. It's important for the Navy to ensure data is clean, unbiased, trusted and available. Trusted, high-quality data inputs are essential to drive quality data outputs (AI products). Data movement capabilities address the first mile problem from ship-to-ship and ship-to-shore, including in DDIL situations.

Cloudera provides support for the entire data lifecycle from data ingestion through Gen AI, AI and ML. By leveraging Cloudera and capitalizing on data mesh capabilities available at different classifications in CANES, the Navy can unlock the full potential of Gen AI, driving innovation and operational excellence across the fleet.

BIO: Rick Taylor is a Senior Solutions Engineer at Cloudera Government Solutions Inc. (CGSI), supporting our U.S. Navy and Marine Corps partners and customers. He has worked closely with the intelligence and the DoD communities since 2004. Prior to joining Cloudera in 2016, Taylor was a technical staff member at Schlumberger. He later provided systems engineering expertise to a broad range of IC, DoD and commercial customers at Sun Microsystems and Oracle.

Utilizing AI to Unlock Data Essential to Mission Success

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

ABSTRACT

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

Key topics include:

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

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

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

Colvin Run Networks: The IRONCLAD Initiative

Nikhil Shenoy, CEO & Founder, Colvin Run Networks • Nikhil@colvinrun.com

ABSTRACT

The IRONCLAD initiative develops and deploys prototypes of a cutting-edge multi-cloud machine learning operations (MLOps) platform tailored for the U.S. Navy's unique operational needs. Leveraging the combined expertise of Colvin Run Networks, Google Cloud and Noctua Technology, this project will integrate advanced artificial intelligence (AI) and machine learning capabilities into a secure, scalable multi-cloud environment. The primary objectives include establishing a multi-cloud architecture, implementing secure cloud foundations and deploying three initial use cases:

- Drone Identification Vision Model
- Translation Model for Coalition Communications
- Anomaly Detection Model.

Additionally, the project will enhance the platform with generative AI for intelligence analysis and predictive maintenance models in subsequent phases, with edge deployed 5G as a capstone use cases for deployable AI.

The IRONCLAD SBIR changes the game for NAVWAR networking, connectivity, software and AI/ML-enabling operations for the Navy. Colvin Run Networks' commitment is anchored in delivering a future-proof application that serves immediate NAVWAR needs while establishing a solid foundation for Navy-wide adoption.

BIO: Nikhil Shenoy serves as Founder and CEO of Colvin Run Networks Inc., where he has led multiple DoD SBIR initiatives focused on data analytics platforms and services. His career spans roles at leading organizations including Goldman Sachs, where he worked as a quantitative strategist for credit & equity derivatives trading, and Procter & Gamble, where he led data-driven finance and marketing initiatives for major consumer brands.

Prior to founding Colvin Run Networks in 2018, Shenoy oversaw the design and development of an innovative workplace IoT platform at Kastle Systems, a national managed security technology company. His analytics work there proved foundational to their building occupancy data service, which was featured in Bloomberg as a key indicator of workplace dynamics.

Shenoy brings deep expertise in defense technology through his active involvement in key industry organizations. He serves on the AFCEA International Technology Committee and is a board member focused on emerging technology applications for the National Defense Industry Association (NDIA) Electronics Division. His thought leadership includes publications in defense journals, such as his work on improving operational readiness in Phalanx, and frequent speaking engagements at DoD conferences and events.

CommScope: Extending the Network

Jay Nusbaum, Systems Engineer, Enterprise Networks, CommScope •

Jay.Nusbaum@CommScope.com

ABSTRACT

Ever since the development of PDS in the early 1980s, 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 into the future
- Challenges and deployment considerations
- Use cases

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

Transitioning to Wi-Fi 6e & 7

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-Fi 7. The focus of the session will be on transitioning from previous standards, Wi-Fi 5 & 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
- Recommendations

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. As a Consulting Systems Engineer, he advises numerous customers on network architecture and associated technology.

Bridging the Data Divide: Advancing Mission Readiness and Cyber Resilience in Maritime Operations through Strategic Data Management

Derek Gleich, Manager, Solutions Engineering, Cribl • dgleich@cribl.io

ABSTRACT

In the maritime domain, the exponential growth of operational, intelligence and cyber data presents unique challenges to existing infrastructure, budgets and data management strategies. As fleets and shore-based facilities deploy a growing array of sensors, platforms and security systems, maritime operations must deliver actionable, data-driven insights in increasingly resource-constrained environments. These insights are essential for enhancing threat detection, improving situational awareness, ensuring compliance, and maintaining fleet readiness and mission effectiveness. Meeting these demands requires innovative solutions to eliminate data silos and inefficiencies inherent in traditional workflows.

Advancing Operational Capabilities While Adversaries Target Your Identity

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

ABSTRACT

As agencies face increasing threats from adversaries, the need to protect sensitive identities while advancing operational capabilities has never been more critical. This session explores the intersection of identity security and operational resilience in government, highlighting how agencies can safeguard against targeted attacks without compromising mission effectiveness. From emerging threats to actionable solutions, attendees will gain insights into balancing security priorities with evolving operational demands.

Here you'll learn:

- Best practices for fortifying identity security while maintaining operational agility
- How to anticipate adversaries' evolving tactics and develop a proactive defense posture
- How to extend privilege controls to the endpoint to mitigate risk, and protect your existing investments
- Guidance on ensuring the efficiency, continuity and integrity of your agency's mission

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

Driving Mission Readiness: Empower Federal Missions With Trusted AI

Justin Swansburg, VP, Applied AI & Technical Field Leads, DataRobot •

justin.swansburg@datarobot.com

ABSTRACT

The Sea Service community has faced increasing challenges in operational readiness, resource optimization, logistics and cybersecurity amid rapidly evolving technology and complex missions. Advanced data-driven solutions are now critical to achieving mission success and resilience.

Join DataRobot for an engaging session exploring how the Department of the Navy can leverage generative AI to address mission-critical challenges. Discover practical strategies, real-world use cases, and valuable lessons from successful AI implementations across the armed forces. Attendees will learn how to operationalize AI to enhance decision-making, streamline operations, and drive measurable mission impact—all while ensuring compliance with security standards.

BIO: Justin Swansburg is the VP of Applied AI & Technical Field Leads at DataRobot. He has extensive experience working with DoD customers and has deployed advanced AI applications that blend predictive AI with generative AI, including time series forecasting, predictive maintenance and readiness use cases. He also has hands-on expertise in running smaller language models locally for deployment on ships, aircraft or remote military bases with limited connectivity. Additionally, his applied research on implementing guardrails and safety measures for large language models (LLMs) ensures that AI solutions are effective and secure.

Build Winning Sales Plans for the Department of Navy

John Slye, Senior Advisory Research Analyst, Deltek • johnslye@deltek.com

ABSTRACT

The Navy acquisition environment continues to adapt to address the department's multiple modernization realignment efforts and meet evolving objectives. Understanding the Navy budget landscape for FY 2025 can help you build a winning sales strategy.

Deltek explores the Navy's FY 2025 funding priorities and unpacks procurement and contract spending trends, including how small businesses stack up. They also address:

- Navy's top issues and priorities
- Preferred contract vehicles and top contractors
- Opportunity highlights and potential project leads

BIO: John Slye is a Senior Advisory Research Analyst at Deltek, where he brings more than 20 years of experience in federal, state and local market analysis to serve clients with insight into the policy, technology and buying trends impacting companies competing for government business. He came to Deltek through its acquisition of INPUT in 2010. Prior to Deltek/INPUT, Slye was a federal account manager with CDW Government (CDW-G), developing IT solutions for government agencies spanning federal civilian and defense agencies and state and local governments. Previously, Slye held several positions in consulting, business analysis and systems integration in the telecommunications industry with Verizon, UUNet and American Management Systems. His experience in public procurement and industry analysis began in the early 1990s as a research associate at the Heritage Foundation, where he led the use of data mining to analyze federal funding trends. Slye holds an MBA from George Mason University and a bachelor's degree in political science from the State University of New York at Oswego.

Building Brilliant Machines

Zac Staples, CEO & Founder, Fathom5 • zac@fathom5.com

ABSTRACT

Fathom5, a Texas-based defense innovation firm specializing in tactical-edge AI infrastructure, succeeded in delivering the Navy's first program-of-record deployment of artificial intelligence to a warship. Under the government direction of NAVSEA, Fathom5 refactored the legacy codebase for Enterprise Remote Monitoring (ERM) to create a modern AI hosting environment aboard USS Fitzgerald. This ERM tactical platform as a service (PaaS) hosts predictive analytics that make maintenance recommendations to sailors via a direct interface to the ship's maintenance planning system.

In addition to ERM, Fathom5 has announced that its patented ARIA technology has been chosen for the 2024 National Security Innovation Network (NSIN) Propel Maritime Digital Defense Accelerator. ARIA, a cyber-resilient machinery control architecture, enhances the security of machinery endpoints against advanced, persistent cyber threats, addressing potential vulnerabilities in Navy warships. This selection allows Fathom5 to collaborate with Department of Defense stakeholders and demonstrate ARIA's potential to bolster cybersecurity for maritime defense. Participation in the accelerator aims to secure a pilot test within a Navy program, facilitating integration into the fleet and broader commercial deployment.

This achievement follows other Fathom5 advancements, including launching its flagship platform, TempestOS, and continuing to innovate on cutting edge technology at the intersection of AI and grease. Fathom5 is setting new standards for industrial resilience and national security.

BIO: Zac Staples is the Founder and CEO of Fathom5, an Austin, Texas-based technology company dedicated to designing secure infrastructure for AI-powered machines that transform industrial resilience and drive defense innovation. Since founding Fathom5 in 2018, Staples has championed cyber-resilient designs and innovative solutions for the most complex operational technology challenges. Under his leadership, Fathom5 has reached significant milestones, including deploying AI aboard U.S. Navy warships—a pioneering achievement in defense technology—and holds 17 patents for advanced actuators and cybersecurity. His commitment to blending next-generation technology with legacy systems has positioned Fathom5 as a trusted partner in national defense and industrial innovation.

Staples' distinguished career began with more than two decades of service in the U.S. Navy, where he held key roles across various assignments and ultimately served as the Director of the Center for Cyber Warfare at the Naval Postgraduate School. He led a team of PhDs, graduate students and technical staff in this role, focusing on cutting-edge research and development to bolster the Navy's cyberspace capabilities. His team also established the Engineering Enclave for Maritime Security—a first-of-its-kind lab focused on electronic reliability and cybersecurity for shipboard navigation and control systems. In recognition of his contributions, he was honored with the Secretary of the Navy's "Innovation Catalyst" award in 2017, a testament to his pioneering work in digital and cyber defense.

Staples' experience in the Navy is foundational to Fathom5's mission and strategic direction. He brings a rare combination of tactical knowledge and a forward-looking approach, blending high reliability with advanced technology to protect critical infrastructure and support national security. At Fathom5, Staples and his team specialize in secure infrastructure, operational technology and AI-based solutions that empower organizations to operate safely and effectively in high-stakes environments. Their flagship platform, TempestOS, is at the forefront of AI enablement at the tactical edge, safeguarding mission-critical operations for the U.S. Navy and other industrial leaders. By merging agile prototyping, rigorous cybersecurity measures and expertise in operational systems, Fathom5 enables clients to outpace emerging threats and set new standards for innovation delivery in highly regulated environments.

Staples' vision for Fathom5 extends beyond individual projects. He believes in a future where secure, intelligent technology underpins industrial resilience, and his work emphasizes bridging traditional infrastructure with cutting-edge cyber defense to ensure security and operational excellence. His leadership values are rooted in integrity, mission-focused innovation and the pursuit of excellence, driving Fathom5 to create meaningful advancements that support both industry and national security.

Beyond his work with Fathom5, Staples actively contributes to the defense and technology communities, sharing insights and offering his expertise in AI enablement for critical infrastructure. He graduated from the U.S. Naval Academy with a B.S. in engineering and holds an M.A. in international relations from the Naval Postgraduate School.

Risks to AI Adoption for U.S. Sea Services

Parth Vakil, Vice President, Global Field Engineering, HiddenLayer •

pvakil@hiddenlayer.com

ABSTRACT

Artificial intelligence (AI) is becoming its own “arms” race and for good reason. With the advent of large language models (LLMs), the applicable use cases for AI technology have exploded and global actors are participating in innovating AI capabilities as well as AI exploitation.

According to the [Information Technology & Innovation Foundation](#), “The United States has been at the forefront of AI innovation. ... However, China has emerged as a formidable competitor over the past decade. And the narrative that China is merely a ‘copycat’ is false and outdated. China’s strong academic institutions and innovative research, particularly from Tsinghua University, has [sic] produced the majority of China’s top AI start-ups. ... China now produces more AI research than the United States, and it is rapidly closing the performance gap with U.S. LLMs.”

With the adoption of AI significantly increasing, safeguarding the integrity of our AI assets is mandatory. Not only from China and traditional state actors, but from non-state threats.

Traditional security solutions are not designed to address adversarial AI attack vectors. Protecting the AI assets we build and trust requires an AI native approach rooted in AI security research. With more than 30 research blogs, 20+ conference talks, 40+ CVEs, 60+ vulnerabilities and 10+ patents filed, HiddenLayer’s SAI Team has set the bar for AI security best practices. In this presentation, we’ll provide an overview of what we’ve learned.

BIO: Parth Vakil is the Vice President of Global Field Engineering at HiddenLayer, where he brings deep expertise in data and AI. His extensive experience provides him with a keen understanding of organizations’ journeys in safeguarding these critical assets. In his previous role at Databricks, Vakil led a field engineering team and was instrumental in establishing the company’s public sector vertical. Earlier in his career, while at the Naval Research Lab, Vakil contributed significantly to teams deploying mission-critical systems on Navy platforms to enhance national security. He holds a Master of Science in electrical engineering from the University of Maryland, College Park.

Hunted Labs: Securing the Software Supply Chain

Hayden Smith, Chief Technology Officer & Co-Founder, Hunted Labs •

hayden@huntedlabs.io

ABSTRACT

Join Hayden Smith, Co-Founder and CTO of cybersecurity company Hunted Labs, as he addresses the increasingly urgent challenge of securing software supply chains, particularly within government and defense environments. While open source software supports much of our commercial applications and a surprisingly high percentage of public- and defense-related infrastructure, we're often blind to the work of coders who inadvertently—and in some cases, deliberately—insert malicious code that have the potential to undermine our national security. Such vulnerabilities, misconfigurations and threats can be buried in software and are often impossible for cybersecurity professionals to detect.

Drawing on his decade-long experience supporting the U.S. Department of Defense and intelligence agencies, Smith will discuss how AI can locate and address these software vulnerabilities, provide unified threat management, secure software assets across public and private organizations to thwart determined threat actors leveraging open source software as an attack vector.

This session will offer an overview of the current threat landscape, along with actionable takeaways for applying AI and enhanced visibility tools to harden software supply chains and protect organizations against sophisticated threats and attacks. Smith will explore strategies for empowering enterprises and agencies to counter adversarial incursions and maintain a strong cybersecurity posture across digital ecosystems.

Attendees will gain practical knowledge on advanced defensive measures—from real-time risk assessment to code-level threat identification—that align with the unique requirements of government infrastructure. The insights will better prepare attendees to detect vulnerabilities and will raise awareness of the growing challenges posed by open source software and nation-state actors looking to do harm.

BIO: Hayden Smith is Co-Founder and Chief Technology Officer at software security company Hunted Labs, a Red Cell Partners incubation. A battle-tested software engineer, Smith spent a decade in defense intelligence, most recently serving as Senior Director of Field Services at Anchore, where he helped U.S. government, intelligence community (IC) and Fortune 500 clients secure their software supply chains. While at Anchore, Smith built the DoD's first software factory—DoD Platform One. During his time with Platform One, he helped design, architect and deliver the container-hardening pipelines that secured 500+ images into Iron Bank. He later oversaw a larger team of Anchore solutions architects across various Platform One value streams.

Prior to joining Anchore, Smith worked at Booz Allen Hamilton, serving federal and IC customers on cybersecurity and DevOps programs. While at Booz Allen, Smith also led the cybersecurity team for testing and assessing the U.S. Air Force's Global Positioning Systems Next Generation Operational Control System (GPS OCX). It was his experience working in these challenging cyber environments that inspired Smith to co-found Hunted Labs, which leverages artificial intelligence and machine learning to give organizations unprecedented end-to-end visibility into their software supply chains so they can quickly identify and eliminate threats.

Through its product, Entercept™, Hunted Labs, born out of Red Cell's Cyber Practice, provides customers with command and control over their software supply chain. With features like Threat-to-Code™, which hunts for risks and vulnerabilities within codebases, Entercept gives customers comprehensive visibility into their software supply chain's attack surface—from source code repositories to runtime Kubernetes environments—to help them determine the affected blast radius if a breach occurs. In addition, the platform provides AI-driven reconnaissance that actively investigates open source software to alert customers of potentially malicious contributors; and a threat-aware code assistant that automates threat hunting, prioritizes action against dangerous vulnerabilities, and expedites remediation.

Industrial Defender—Operational Technology: Protecting Cyber Resilience and Operational Continuity

Alex Bagwell, Chief Revenue Officer, Industrial Defender •

abagwell@industrialdefender.com

ABSTRACT

Continued cyber threats increasingly target the operational technologies (OT) that underpin maritime and critical infrastructure. These systems are vital for day-to-day operations and protecting them requires heightened vigilance to ensure cybersecurity and operational resilience. Safeguarding critical infrastructure demands securing entry points, hardening systems and monitoring for suspicious changes.

Industrial Defender's OT asset management platform provides complete visibility into OT environments, delivering granular monitoring with sensors to all OT cyber activity. In OT, managing cyber assets has traditionally been a challenge due to their cyber-physical nature, high stakes and demanding operational requirements—where traditional IT approaches risk disrupting critical processes. Industrial Defender has developed its sensors and monitoring approach to be safe for cyber-physical operations while delivering comprehensive, detailed, and accurate asset information.

Complete visibility from Industrial Defender empowers organizations to harden their systems by addressing vulnerabilities, misconfigurations and potential openings that could threaten operational continuity. Through continuous monitoring, the platform identifies risks to security posture, detects and alerts to changes in the environment and stays on top of suspicious behavior. It also enables teams to self-audit and standardize as needed across common frameworks and standards, with detailed reporting aligned to industry benchmarks and hardening requirements. This ensures systems remain in trusted states while adhering to policies like MOSAICS requirements.

As a trusted partner to the U.S. government, Industrial Defender empowers federal agencies with the visibility needed to secure critical infrastructure. By enabling detailed asset monitoring and assessing systems against hardening best practices, the platform strengthens the defense, reliability and operational continuity of vital cyber systems.

BIO: Alex Bagwell is Chief Revenue Officer (CRO) at Industrial Defender, while also spearheading the company's federal organization and collaborating closely with U.S. government operations on their OT security needs.

With more than a decade of experience selling SaaS and on-premises solutions, Bagwell has worked extensively with cyber and physical security teams across OT/ICS, IoT and IT environments. In previous executive sales roles, he drove go-to-market strategies focused on revenue growth and successfully managed global security sales teams. His expertise lies in building scalable processes and fostering strong partnerships to achieve sustainable growth.

Bagwell's leadership and deep understanding of the security landscape have made him a trusted advisor in the public and private sectors.

Innovative Ways to Solve Tech Debt for Federal Customers—Hardware as a Subscription (HWaaS)

Wade Lehrschall, Distinguished Architect, Iron Bow Technologies •

wade.lehrschall@ironbow.com

ABSTRACT

As federal IT modernization accelerates, Hardware-as-a-Subscription (HWaaS) emerges as a pivotal Network-as-a-Service (NaaS) offering tailored for federal agencies. Iron Bow's HWaaS bridges the gap between modern NaaS capabilities and the specific operational requirements of federal contracts, addressing hardware ownership concerns while promoting continuous innovation. This session explores how HWaaS empowers federal organizations to tackle tech debt, navigate the complexities of hardware procurement, and maintain flexibility in rapidly evolving technology landscapes. Attendees will gain insights into leveraging HWaaS to drive modernization and unlock new efficiencies.

What You'll Learn:

- The benefits of HWaaS as a federal-focused NaaS solution.
- How HWaaS resolves tech debt and simplifies hardware ownership issues.
- Actionable strategies to modernize federal networks with scalable, subscription-based models.

BIO: Wade Lehrschall has more than 25 years of experience in networking, software development, post-sales consulting and pre-sale consulting supporting various U.S. federal customers. He has helped 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.

Mission-Focused WAN Modernization— Software-Defined Unified Transport Network (SD-UTN)

Wade Lehrschall, Distinguished Architect, Iron Bow Technologies •

wade.lehrschall@ironbow.com

ABSTRACT

The Software-Defined Unified Transport Network (SD-UTN) represents a groundbreaking solution to unify underlay transport networks and Software-Defined Wide Area Network (SD-WAN) overlays. It addresses the challenges of disjointed WANs in large, complex enterprise environments—an issue particularly prevalent in federal agencies modernizing for diverse mission use cases. By integrating the best modern technologies and solutions, SD-UTN provides a cohesive WAN architecture that simplifies integration, management, and routing policies. Attendees will learn how SD-UTN empowers organizations to optimize their WAN environments, reduce operational complexity, and achieve optimal outcomes for business and mission-critical operations.

What You'll Learn:

- The limitations of traditional WAN architectures in federal environments.
- How SD-UTN resolves disjointed network challenges and supports mission-critical applications.
- Best practices for simplifying WAN integration and management.

BIO: Wade Lehrschall has more than 25 years of experience in networking, software development, post-sales consulting and pre-sale consulting supporting various U.S. federal customers. He has helped 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.

Building an AI-Enabled Foundation for Electronic Warfare Collection, Process and Exploitation

J. David 'TUBA' Britt, Vice President, Defense Technology & Innovation, ManTech •
jenks.britt@mantech.com

ABSTRACT

To manage an electromagnetic footprint in spectrum-denied environments, electronic warfare (EW) systems must be able to process and exploit signals in a congested electromagnetic environment to quickly deliver decision-worthy actions, which may counter active threats or optimize, scale and prioritize self-generated electromagnetic signals. Signals footprint adaptability and speed of decision making will be essential in countering complex electronic attacks while also remaining one step ahead of adversaries in future battlespaces.

ManTech's Defense Chief Technical Officer, J. David Britt, offers a framework discussion that is foundationally based upon a model-based systems engineering (MBSE) digital ecosystem (DEE) running an AI-enabled data ingestion platform. This framework can be ported to an appropriately resourced small form-factor asset for use in the field or directly connected to raw data collections for on-site, timely analysis. The data ingestion platform should be an agnostic, multi-tenant, multi-access AI-enabled data management environment that supports integration of data labeling by deploying an autonomous AI-enabled labelling toolset. This framework depends on the quick-labelling service to then feed the AI-enabled signals analysis module. The signals analysis module then rapidly provides signal analysis, advanced labelling, feature extraction and differential signal processing. The combination of data handling and analysis aids signals labeling, process feature engineering, dataset generation and anomaly detection leading to quicker decision information. Britt will speak to this framework and guide the audience through important MBSE processes and ecosystem considerations while also laying the foundation for development of this AI-enabled signals processing and analysis sandbox.

BIO: J. David Britt orchestrates the enhancement of ManTech's innovative capabilities and technology solutions. Britt actively identifies and leads innovative program transformation, develops innovation timelines and manages innovation and technology goals alignment with ManTech's broad business objectives.

Britt joined ManTech in 2019 as a Program Manager leading ManTech's largest portfolio of work for the Navy Segment, where he leads ManTech's engineering support efforts for NAVSEA and NAVAIR. A U.S. military veteran, Britt served for more than 25 years in the Navy as a naval Flight Officer from the Maritime Patrol community. His latest assignment was serving as the major program manager for the U.S. Navy's

Secure Cloud Pilot effort for U.S. Fleet Forces Command and OPNAV N2/N6. He also served as the Chief Technical Officer (N6) of the P-8 Poseidon/P-3 Orion programs.

Britt earned a Master of Science in systems engineering analysis from the Naval Postgraduate School and a Bachelor of Science in chemistry from the U.S. Naval Academy. He has extensive flight test experience as a Navy Flight Officer and program manager for NAVAIR and OPNAV including executive experience in Washington, D.C. while serving for the Undersecretary Secretary of Defense, Personnel and Readiness.

Automation, AI and Scalability: A New Era in DoD Cyber Risk Management

Brian Recore, Systems Engineer, Merlin Cyber • brecore@merlincyber.com

ABSTRACT

The U.S. Department of Defense (DoD) is at the forefront of defending a vast and increasingly complex digital infrastructure. As threats evolve, so must its approach to cybersecurity. Modernizing its cyber risk management strategy is crucial to protecting cloud systems, hybrid environments, containers and IoT devices in an era of ever-expanding attack surfaces. To meet these challenges, the program needs enhancements such as real-time scanning, seamless integration of new technologies like DevSecOps pipelines, and scalable solutions that ensure all assets are covered. These advancements will not only strengthen defenses but also position the DoD to anticipate and neutralize future threats effectively.

Automation and smarter integration can revolutionize how vulnerabilities are managed, reducing the time from detection to resolution from weeks or months to mere hours. By adopting automated remediation and integrating with tools like SIEMs and IT Service management (ITSM) platforms, the DoD can transform its workflows for greater efficiency and precision. Advanced threat intelligence, intuitive reporting, and AI-driven insights will enable proactive responses to complex threats such as zero-day vulnerabilities and advanced persistent threats (APTs). Furthermore, ensuring alignment with frameworks like RMF and STIGs, while leveraging AI and machine learning to predict and counter emerging vulnerabilities, will keep the DoD ahead of its adversaries.

The Qualys TruRisk Platform embodies this vision, delivering a comprehensive solution to enhance DoD cybersecurity capabilities. It combines real-time vulnerability detection with automated remediation, streamlining processes and reducing response times. With built-in scalability and coverage for cloud, hybrid, and OT environments, the cloud-native TruRisk Platform adapts to the DoD's dynamic needs. Its AI-powered risk assessments and actionable insights empower the DoD to prioritize and address critical vulnerabilities, ensuring a secure and resilient infrastructure in the face of evolving threats.

Summary Points

- Scalability and Real-Time Scanning: Manage increasing data volumes and diverse environments.
- Automation and Integration: Reduce detection-to-resolution time from weeks to hours with ITSM platform integration.
- AI-Driven Threat Response: Leverage dynamic updates and predictive analytics for proactive cybersecurity.
- Qualys TruRisk Benefits: Enhance cyber risk management with scalable and intelligent solutions tailored for evolving threats.

BIO: Brian Recore is a seasoned Systems Engineer with 25 years of experience in the IT industry. He has a proven track record of designing, implementing and managing complex systems for organizations of all sizes. Brian's expertise includes cloud computing, network architecture, cybersecurity and data management. He is known for his ability to lead technical teams, communicate effectively with stakeholders, and deliver results that exceed expectations.

But Recore is not just a Systems Engineer; he is also an avid ultra-runner. He has completed numerous ultra-marathons, including the notoriously challenging Western States 100-Mile Endurance Run and the Badwater 135. Recore's passion for running has not only kept him physically fit but has also honed his mental toughness, discipline and perseverance—qualities he brings to every project he undertakes.

Treating Platform as a Product for Resilient Delivery of Software to the Warfighter

Hannah Hunt, Distinguished Technical Fellow, MetroStar Systems •

hhunt@metrostar.com

ABSTRACT

Delivering Platforms as a Service (PaaS) with a “platform as a product” mindset is essential for enabling resilient and scalable software delivery to the warfighter. This approach prioritizes human-centered design (HCD), robust governance and continuous improvement to ensure platforms meet the dynamic operational needs of defense environments. By treating PaaS as a product, development teams focus on delivering value through intuitive developer interfaces, seamless integrations and built-in capabilities such as security, compliance, and observability. This fosters a standardized yet adaptable framework for deploying mission-critical software with speed and reliability. Adopting DevSecOps practices within the PaaS ecosystem enhances automation and reduces time-to-delivery while ensuring operational resilience against cyber threats. Additionally, a product-focused strategy encourages feedback-driven iterations, empowering developer teams to align platform capabilities with emerging warfighter demands. Ultimately, treating PaaS as a product drives efficiency, innovation and mission readiness in delivering software solutions for modern defense operations.

BIO: Hannah Hunt serves as a Distinguished Technical Fellow at MetroStar Systems in the Defense Business Unit, where she supports technical delivery across MetroStar’s defense customers. As a 2021 Forbes 30 under 30 winner in the Enterprise IT category, Hunt previously served as the Chief Product and Innovation Officer at the Army Software Factory and previously served as Chief of Staff for the U.S. Air Force’s Software Factory Kessel Run. At the Army Software Factory, Hunt led the development and delivery of a cohesive suite of products “by soldiers, for soldiers” and evangelized agile acquisitions and DevSecOps in the Army.

Integrated Respirator Information System

Joe Early, Senior Director, R&D Solutions, MetroStar Systems • jeary@metrostar.com

ABSTRACT

ActionStreamer's IRIS (Integrated Respirator Information System) offers a groundbreaking solution for enhancing situational awareness, safety, and operational efficiency in hazardous and confined environments. Designed to address the complex challenges faced by Navy personnel, the IRIS system integrates wearable technology with live-streaming and data-capture capabilities, providing command teams with real-time visibility of an officer's perspective.

In high-risk scenarios such as inspections aboard vessels, submarine maintenance or damage control in confined spaces, IRIS enables seamless communication and improved decision-making by streaming live footage directly from the field to command centers. The system enhances safety by allowing remote experts to guide personnel in navigating confined, hazardous, or oxygen-depleted areas, reducing exposure risks and improving mission outcomes.

Beyond operational utility, IRIS revolutionizes training and post-mission review processes for Navy officers. By capturing first-person footage of real-world scenarios, the system creates a robust visual archive for training exercises and post-event analysis. Officers can review authentic footage to refine techniques, analyze decision-making processes, and prepare for similar future challenges. This capability fosters a deeper understanding of operational environments, accelerating learning curves and enhancing readiness across the fleet.

MetroStar's integration with IRIS establishes a comprehensive monitoring system for hazardous operations. The Mission Analysis Ecosystem processes real-time data through AI/ML capabilities, enabling predictive maintenance and automated risk assessment. By fusing multiple data streams, including video and environmental sensors, the system provides commanders with enhanced situational awareness. Operating through MetroStar's DoD-compliant Onyx Platform, this integration reduces repair times by 66% and significantly improves aircraft availability. The streaming platform ensures reliable communication in confined spaces, enabling seamless collaboration between field personnel and remote experts.

The IRIS system's unique blend of real-time streaming, data capture and usability in hazardous and confined environments positions it as a vital asset for improving Navy operations and training effectiveness, ensuring mission success and safeguarding personnel.

BIO: Joe Early is the Senior Director of R&D Solutions at MetroStar, where he focuses on innovative integration of machine learning, data science and AI technologies. In this role, he develops executive tech and operations strategies, leads research initiatives and drives open-source software collaboration efforts. Early brings a visionary approach to technology leadership, with expertise in strategic planning, executive management and adoption of emerging technology.

Prior to joining MetroStar, Early served as the Deputy Chief Technology Officer at Cornerstone Defense, where he led strategic solutions and organic technology innovation. His experience also includes significant roles in the defense sector, notably as the Chief Data Officer and Chief Digital Officer for the F-35 Joint Program Office. In these positions, he spearheaded data-enabled strategies, analytics governance and digital transformation initiatives across the enterprise.

Early's career highlights include F-35 lead on the Mad Hatter project partnered with Air Force's Kessel Run, where he revolutionized software development in military aviation and successfully deprecated more than \$150 million a year in legacy software spending. His experience spans various aspects of defense technology, from operational test and evaluation of naval aircraft to enterprise modernization and transformation.

A former Naval Flight Officer and current Navy Reservist, Early has served more than 15 years in the U.S. Navy, specializing in E-2D and E-2C Hawkeye aircraft Joint and Combined C4ISR operations. He holds expertise in military strategy, government digital transformation, maritime operations and naval aviation. He is a proud graduate of University of Virginia and holds two Master's Degrees.

Traditional Software Composition Analysis (SCA) Is Not Enough: Protecting Mission-Critical Software

Bryan Whyte, Director, Solutions Engineering, MFGS Inc. & Sonatype •

bwhyte@sonatype.com

ABSTRACT

As the Department of Defense leverages advanced technology to maintain mission-critical readiness, the software landscape continues to evolve. With open-source software downloads exceeding 6.6 trillion in the past year, innovation has accelerated—but so have risks to the DOD’s software supply chain, including open-source malware and “persistent risk.”

In this session, Sonatype and MFGS Inc., will demonstrate how integrating Sonatype’s software supply chain management solutions with OpenText Fortify delivers a powerful, end-to-end approach to software supply chain security. Together, we’ll explore how to:

- **Enhance DoD Cybersecurity Compliance:** Use OpenText Fortify’s application security tools in tandem with Sonatype’s Software Bill of Material (SBOM) Manager and SCA solutions to streamline compliance with mandates such as NIST SP 800-218 and CISA guidelines.
- **Strengthen Threat Detection:** Leverage Fortify’s Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) capabilities alongside Sonatype’s automated security checks and open-source malware detection to eliminate vulnerabilities throughout the software development lifecycle.
- **Achieve Full Lifecycle Security:** Integrate Fortify’s security testing with Sonatype’s automated dependency management to address risks early and continuously monitor software quality.
- **Improve Software Integrity Across the Mission:** Ensure secure, well-maintained components are deployed across DOD projects, safeguarding operational success.

Join us to learn how the synergy between Sonatype and OpenText Fortify help modernize software supply chain management, reduce risk, and support the DOD’s mission to secure national defense initiatives.

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

In 2015, Whyte joined IBM Security as a Technical Pre-Sales Engineer, specializing in the AppScan tool suite for Static, Dynamic and Mobile Application Security Testing. With a growing interest in advancing his cybersecurity expertise, Whyte earned the Certified Information Systems Security Professional (CISSP) certification, broadening his proficiency in the field.

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

Make Your Artificial Intelligence Analytics More Accurate by Leveraging an Effective ETL Process

Chris Kelly, Big Data Solutions Sales, MFGS Inc. • chris.kelly@mfgsinc.com

ABSTRACT

Effective tools leveraged in the Extract/Transform/Load (ETL) process will prepare content to be analyzed with AI and LLLMs. These tools should include the following:

- **Extraction:** The process begins with the need to extract data from extensive sources, including structured databases, unstructured documents, and multimedia files. ETL processes should ensure that data is extracted efficiently and accurately, regardless of its format or complexity.
- **Transformation:** During the transformation phase, various techniques should be applied to clean, normalize, and enrich the extracted data. This includes:
 - *Textual Analysis:* Applying natural language processing (NLP) techniques to extract keywords, entities and semantic meaning from text data.
 - *Audio/Video Analysis:* Employing speech-to-text conversion, speaker identification and sentiment analysis to extract insights from audio and video content.
 - *Image Analysis:* Utilizing image recognition and computer vision techniques to extract visual information and metadata from images.
- **Loading:** The transformed data is then loaded into the AI knowledge base, making it readily available for further analysis and insights.

BIO: Christopher (Chris) Kelly supports Big Data Information Management and Governance software and artificial intelligence solutions sales to the U.S. government civilian, DoD and classified market segments for MFGS Inc. Kelly combines solutions expertise, partner capabilities and innovative technologies to address the information lifecycle and business solution needs of Federal customers, as well as the large system integrators that support them.

Kelly has been in the imaging, document management, process automation, record management and information lifecycle management discipline for almost three decades and has contributed to the transformation that has positioned big data technologies and AI at the crossroads between regulatory compliance, business efficiency and transparency.

The Operational Data Interop Imperative— Architecting an Intelligent Data Infrastructure to Share and Secure Critical Data to Ensure Mission Operation Advancement

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

ABSTRACT

Effective data sharing across mission coalition partners and allies can be incredibly challenging in today's defense arena. Different technologies and types of data have driven siloed, unique infrastructures that do not play well together. Learn in this session how to architect a unified data sharing backbone and fabric that has built-in AI and intelligence to provide security, efficiency and flexibility for mission operation advancement from edge to core and across hybrid multi-clouds for any agency.

BIO: Jim Cosby is currently a CTO at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on Data Management and Storage Security for more than 20 years, including on-premise and hybrid multi-cloud intelligent data infrastructure technologies, which include multi-domain operations and 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.

The Multi-Domain Data and Information Sharing Conundrum—Building an Effective and Secure Data Information Sharing Architecture to Provide Collaborative Mission Execution

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

ABSTRACT

The U.S. Department of Defense agencies all utilize state of the art data sharing technologies. However, some commands have chosen their own unique technology and infrastructure that does not always communicate or share data effectively. In addition, maintaining security levels of data across disparate technologies for data is cumbersome and often ineffective. Join this session to learn how to architect an Intelligent Data Infrastructure that leverages AI to effectively secure and share data across data fabrics and data backbones for multiple partners and allies while ensuring optimal efficiency, security, and flexibility to drive strong mission outcomes.

BIO: Jim Cosby is currently a CTO at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on Data Management and Storage Security for more than 20 years, including on-premise and hybrid multi-cloud intelligent data infrastructure technologies, which include multi-domain operations and 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.

The Zero-Trust Data Centric Challenge— Building a Functional Data Centric Sharing Architecture with Effective Zero-Trust Controls to Drive Operational Advancement

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

ABSTRACT

Today there are multiple mission partner environments that need to securely share data across coalitions to enable Joint All-Domain Operations for partners and allies. There are major limitations existing today due to unique and separate data technologies implemented by the different agencies and countries. Additionally, security of data must be maintained while sharing and should leverage the latest security and AI capabilities to protect sensitive information. Join this session to learn about an intelligent data infrastructure that provides true hybrid multi-cloud data sharing with built-in AI driven security and zero-trust capabilities to ensure safe and effective mission execution and advancement.

BIO: Jim Cosby is currently a CTO at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on Data Management and Storage Security for more than 20 years, including on-premise and hybrid multi-cloud intelligent data infrastructure technologies, which include multi-domain operations and 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.

Protecting Technological Innovation: Educating the Next Generation of Cyber Risk Management Professionals

Rafael Diaz, Ph.D., Graduate Program Director, School of Cybersecurity, Old Dominion University • rdiaz@odu.edu

ABSTRACT

Technological innovation is integral to military leadership across the Department of Defense (DoD), permeating nearly every facet of its operations. As digital transformation advances, technologies such as cloud computing, advanced communication networks and cyber-physical systems continue to expand exponentially, enabling efficient data exchange within the information and communication technology (ICT) supply chain. However, this rapid growth also enlarges the cyberattack surface and exposes new vulnerabilities. Consequently, contractors and subcontractors in the Defense Industrial Base (DIB) must adhere to stringent frameworks like the Cybersecurity Maturity Model Certification (CMMC) and adopt zero-trust Architectures (ZTA).

A highly skilled workforce is essential to ensuring compliance and transitioning across a broad spectrum of certifications, thereby safeguarding the ICT supply chains critical to innovation. This presentation highlights the role of Old Dominion University's School of Cybersecurity in preparing students to support the DIB. Through a curriculum enriched with hands-on experiential learning, extensive virtual labs, and the integration of Artificial Intelligence, the program equips students with the skills to analyze information critically, evaluate diverse perspectives, and make sound, informed decisions. By emphasizing critical thinking and decision-making, the School of Cybersecurity cultivates leaders capable of defending ICT supply chains and advancing innovation within the defense sector.

BIO: Rafael Diaz, Ph.D., is Professor, Commonwealth Cyber Initiative and ODU AI Teaching Fellow. Diaz serves as the Graduate Program Director—School of Cybersecurity, Interim Graduate Program Director—School of Supply Chain, Logistics, and Maritime Operations Director of Supply Chain Cybersecurity Research.

Internships Are One Great Idea, So What Other Innovative Ideas Can We Explore?

Teresa Duvall, Faculty Lecturer, School of Cybersecurity, Old Dominion University •
tduvall@odu.edu

ABSTRACT

The persistent gap between the influx of university graduates with degrees in cybersecurity and other STEM fields and the hiring challenges faced by the government and defense contractors and agencies underscores a critical workforce issue. Despite the high demand for skilled cybersecurity professionals, for example, organizations are unable to hire suitable candidates. This abstract proposes innovative ideas to bridge the gap between the students graduating with a degree in cybersecurity and the challenge that companies and the government face with trying to hire these students. Internships are one great idea, so what else can we do?

BIO: Teresa Duvall is a native of Harbor Creek, Pennsylvania. She graduated from the Pennsylvania State University and commissioned an ensign via Officer Candidate School. Duvall was a plank owner in the Information Professional Community; she served as Commanding Officer at Naval Computer and Telecommunications Station Puget Sound, Washington. She retired from Naval Network Warfare Command as Deputy CIO; completed a Master of Science Degree in the management of information technology with honors from the University of Virginia's McIntire School of Commerce and returned five years later to serve as a senior civil servant at the same command. She served at U.S. Fleet Cyber Command as Supervisor, IT Specialist and Mission Integration Division Head for the Navy Authorizing Official.

In addition to her Naval career, she was employed in industry at CACI International as Director, Naval Programs Enterprise Services Division and Cyber Division.

As faculty at Old Dominion University, Duvall is a lecturer in the School of Cybersecurity. She is the Internship Director for all cybersecurity students and a liaison with the Coastal Virginia Commonwealth Cyber initiative. She is called upon to present at cyber conferences with a focus on women in cybersecurity.

Duvall owns a small Disabled Veteran/Woman owned business, Solutions TBD LLC and is a consultant for ValidaTek Inc.

She served in the nonprofit arena as Chapter President of AFCEA Hampton Roads and currently serves as the chapter's Women's Outreach chair with support to the Maritime IT Summit. She was selected to serve AFCEA International on the Board of Directors.

Other degrees include a Master of Arts Degree in national security and strategic studies from Naval Command and Staff College and a Master in Education and Human Development from George Washington University. Duvall is Project Management Professional (PMP) certified.

The Navy awarded Duvall the Superior Civilian Service Medal, the highest honorary award the Chief of Naval Operations may bestow on a civilian employee in the Department of the Navy, and the Meritorious Civilian Service Medal. She was the recipient of the Department of Defense Chief Information Officer Information Technology Award for Excellence in her leadership role in Operation Triton Bastion. She was recognized as one of the prestigious AFCEA/USNI Copernicus Award winners for her sustained superior performance in cyber and IT. AFCEA International recognized Duvall with the Chairman's Superior Performance award, Leadership Award and Women's Appreciation Award to recognize her achievements to further the careers of women.

Fortifying Federal Security: Implementing Zero Trust and Cross-Domain Solutions\ Multi-Level Security Solutions

Chris Betz, Chief Technology Officer, Federal, Omnisca • betzc@omnisca.com

ABSTRACT

In the ever-evolving landscape of all regions across the globe, the need for robust, secure and resilient IT infrastructure has never been more critical. As nations and military forces collaborate to address the unique challenges posed by these volatile areas, the ability to communicate securely, quickly and continuously is paramount. Omnisca 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, cross-domain solutions and multi-level security (MLS) systems, specifically designed to enhance the security posture of federal operations. 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 currently a Federal CTO inside the EUC Omnisca 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 Omnisca), 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 Omnisca, showcasing his unwavering commitment to the company and its customers.

Ocean Wave-Powered Underwater Charging

Priscilla Prem, CEO & Founder, Pittsburgh Coastal Energy •

priscilla.prem@pghcoastal.com

ABSTRACT

Pittsburgh Coastal Energy is an early-stage hardware startup using ocean waves to charge underwater systems while submerged. At-sea systems such as unmanned underwater vehicles (UUVs) rely heavily on battery power for operational energy, which imposes significant limitations on their mission duration, stealth capabilities and weight and size dimensions. Our mission is to expand undersea capabilities for UUVs and other naval systems by delivering underwater battery charging solutions to enhance long-duration stealth, ensure protection against storms, and offer operational flexibility for unmanned systems, thus providing strategic advantages unobtainable with other energy generation technologies.

BIO: Priscilla Prem is the founder and CEO of Pittsburgh Coastal Energy, an early-stage hardware startup developing underwater charging solutions for unmanned submersible systems. She is currently pursuing her PhD in chemical engineering at the University of Pittsburgh where she invented the company's core technology—the Polar Ionic Nanogenerator (PING)—to provide operational energy for naval applications. As a U.S. Navy veteran, Prem is dedicated to enhancing the Navy's mission readiness to confront evolving threats to national security through advanced wave energy solutions. Through Pittsburgh Coastal Energy, she aims to empower critical operations for unmanned systems with extended mission duration and greater stealth capabilities. Her commitment reflects the company's vision to transform how naval forces achieve sustained, resilient and adaptable underwater operations.

Introducing The Risk Operations Center: Orchestrating the Elimination of Mission- Critical Cybersecurity Risk

Richard Seiersen, Chief Risk Technology Officer, Qualys • rseiersen@qualys.com

ABSTRACT

The Department of Defense (DoD) faces significant challenges managing risks across its vast infrastructure, the Department of Defense Information Network (DoDIN), and the varied divisions of its uniformed services. With interconnected and dynamic threats spanning cyber and operational domains, the DoD would benefit from a comprehensive, mission-aligned risk management approach.

ROC's comprehensively orchestrate (prioritize, remediate, mitigate) risk sourced from:

- Full-Stack Security Telemetry (asset, threat, vulnerability, identity)
- Hybrid Infrastructure (IT, OT, Cloud Native)
- First and Third-party Data Sources

Attendees will leave this session with an understanding of how and why a ROC is necessary for today's digitally and AI transforming enterprise. Likewise, they will get exposure to a modern platforming approach for powering your ROC called Enterprise TruRisk Management (ETM).

BIO: Richard Seiersen is the Chief Risk Technology Officer at Qualys. He has held CISO roles at GE, Twilio, LendingClub and was the Chief Risk Officer for Resilience. He is the co-author of How to Measure Anything In Cyber Security Risk (core curriculum for the DoD CISO program out of Carnegie Mellon University) and The Metrics Manifesto: Confronting Security With Data.

Software X

Tom Skradski, Application Platform Solutions Specialist, Red Hat •

tskradsk@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.

Generative AI for the Cyber Warfighter

Andres Giraldo, Director of Innovation, Sealing Technologies Inc. •

andres.giraldo@sealingtech.com

ABSTRACT

This session covers how large language models (LLMs) and Retrieval-Augmented Generation (RAG) are transforming defensive cybersecurity capabilities. SealingTech, a trusted mission partner to cyber protection teams across the Department of Defense (DoD), is developing a generative AI solution designed to enhance the efficiency and effectiveness of the cyber warfighter.

The presentation will highlight how AI agents can seamlessly integrate with defense information systems to empower cyber defenders in protecting critical data. Attendees will discover cutting-edge AI technologies that enhance information awareness, enabling both junior and senior cyber defenders to rapidly understand complex mission environments and deliver actionable intelligence to decision-makers.

The session will include a demonstration showcasing our Operator X Generative AI project interacting with DoD cyber tools to stay ahead of adversaries and ensure the resilience of defensive operations.

BIO: A highly accomplished cybersecurity professional renowned for his exceptional leadership and innovative contributions to the industry, Andres Giraldo, Director of Innovation, started his tenure at SealingTech as an intern. A proud U.S. Navy veteran, he earned a Bachelor of Science 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, Andres is also deeply committed to mentoring and empowering the next generation of cybersecurity professionals.

Securing Information Anywhere

Richard Streeter, Operations Director, Sertainty • rich.streeter@sertainty.com

ABSTRACT

The phrase “securely move any information from anywhere to anywhere” was introduced in DoN CIO’s 2022 Capstone Design Concept and continues to be referred to as “The One Goal” for the Navy’s Information Architecture. The Capstone document went so far as to say “satisfying this goal transforms the DoN IE into a warfighting mission enabler.” Unfortunately, if this goal were achievable with the current network-based data security tools, data would have been secure for the past 30 years. Achieving this goal without a revolutionary shift in how networks operate or how cryptography is applied is simply unrealistic.

The often overlooked and unspoken truth about “data security” is that it primarily involves securing the computer, network or communications infrastructure that controls the data file. While the file itself may or may not be encrypted, most of the success or failure in protecting the data depends on the success or failure of securing the infrastructure surrounding the data file. Think of these as the rings surrounding a generic piece of data, depicted in any graphic illustrating defense in depth.

Returning to the concept of “securely move any information from anywhere to anywhere,” if we were to compare cyber operations to chess, data files would be similar to the king. They are both the most valuable and, potentially, the weakest piece. Defending the king is paramount, even while also simultaneously trying to attack the opponent’s king. Sertainty will present a technology that injects an internal self-defense mechanism into data files. Imagine, in chess, the ability to teleport to any square on the board when in check. In the real world, this technology grants data files the ability to control final access to the internal data—no longer relying on the security of the computer, network, communications process or even the root-level user. This makes the secures the information in the file anywhere—satisfying the “One Goal”.

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

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 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.

Meeting the Speed of Mission with Generative AI

Thomas Calabrese, Certified Technical Architect, ServiceNow •

thomas.calabrese@servicenow.com

ABSTRACT

The pace of change in the mission space is relentless, and it will only continue to accelerate. To meet the needs of our sailors and civilians, leaders must leverage technology such as generative artificial intelligence (GenAI) to securely advance operational capabilities and enhance mission outcomes.

This session will detail how Now Assist, ServiceNow's GenAI suite of skills, supports human interactions for mission outcomes tied to:

1. Employee/warfighter self-service (GenAI-powered search, Virtual agent)
2. Developer productivity (Text-to-code and Flow generation)
3. ServiceNow agent productivity (Summarization and text generation)

Our session will include a demonstration of these specific use cases of Now Assist, and the powerful impact the solutions can have on mission readiness.

BIO: Thomas Calabrese has 16 years of IT experience supporting commercial and government organizations. He was introduced to the ServiceNow platform 9 years ago while working at PlayStation and uses his process expertise and platform knowledge to help government customers. He is currently an Advisory Solution Consultant and a Certified Technical Architect at ServiceNow. In this role, he is dedicated to advancing the digital capabilities of the United States Navy, aligning its operational speed with that of leading commercial enterprises.

Revolutionizing the Intelligence Cycle Through Innovation

Vincent Nguyen, Business Development and Enablement Manager, Starboard Maritime Intelligence Inc. • vincent.nguyen@starboard.nz

ABSTRACT

The evolving threat landscape in maritime security demands innovative solutions that can outpace adversarial tactics. Starboard Maritime Intelligence, a state-of-the-art platform, redefines the intelligence cycle by enhancing maritime domain awareness (MDA) and enabling cross-border collaboration. Designed to address transnational challenges like drug trafficking, IUU fishing and vessel-based crimes, Starboard integrates advanced analytics, automated anomaly detection and real-time data sharing to support actionable intelligence.

Leveraging collaboration with the United Nations Office on Drugs and Crime (UNODC), the Pacific Fusion Centre (PFC) and the Pacific Transnational Crime Coordination Centre (PTCCC), Starboard supports multinational information-sharing efforts vital for operational coordination. By fusing encounter algorithms, oceanographic data, and automated alerting systems—such as identifying anomalous vessel behavior in cable protection zones—Starboard empowers users to transition from detection to enforcement swiftly and securely.

Aligned with the conference theme, “The Future is Now: Are We Advancing Operational Capabilities That Pace the Threat?” Starboard demonstrates how cross-cutting data within its platform can integrate seamlessly into the intelligence cycle, enabling decision-makers to analyze high-risk patterns, assign response assets and mitigate threats across the Pacific and beyond. Through partnerships with regional stakeholders, including nations involved in U.S. INDOPACOM exercises, Starboard showcases its ability to strengthen maritime security and operational readiness in a dynamic and interconnected world.

BIO: Vincent “Vinnie” Nguyen is a maritime leader with more than 23 years of experience in data analytics, maritime security and capacity building, honed through a distinguished career in the U.S. Navy and U.S. Coast Guard. As a former naval trainer and instructor, Nguyen specializes in analyzing high-level data, developing strategic policies and forging cross-border partnerships to enhance maritime domain awareness and global security. His international experience spans the Asia-Pacific, the Americas and beyond. He holds a Master’s Degree in international relations and affairs focusing on Asia-Pacific Public Policy and environmental security from the University of San Francisco and a Bachelor’s Degree in military and diplomacy studies from Hawaii Pacific University. His expertise is further supported by his certifications in Project Management and advanced language skills in Chinese and Vietnamese.

Current Focus: As the Business Development and Enablement Manager for North America at Starboard Maritime Intelligence, with additional responsibilities in the Asia-Pacific (APAC) region, Nguyen is committed to advancing Starboard's mission to provide innovative maritime intelligence solutions. His focus includes combating illegal, unreported, and unregulated (IUU) fishing, securing maritime critical infrastructure and enhancing biosecurity through strategic collaborations with the United States, Canada and international partners.

Experience:

- Principal Consultant & Owner – The Nguyen Solutions: Led consultancy engagements with notable organizations, including the United States Agency for International Development (USAID) Sustainable Fish Asia Project, WildAid Marine, Global Fishing Watch, IMCS Network and Skylight at the Allen Institute for Artificial Intelligence.
- Maritime Law Enforcement and International Affairs Officer – U.S. Coast Guard: Directed maritime security operations and managed international partnerships to enhance global maritime law enforcement, focusing on the Asia-Pacific and the Americas. Oversaw projects in data analytics, emerging technology for the maritime domain, fisheries enforcement, emergency disaster response, and cybersecurity within the Maritime Transportation System.
- International Affairs and Data Analytics Specialist (Asia-Pacific) – U.S. Navy: Specialized in data analysis and international relations, focusing on the Asia-Pacific region to support U.S. military objectives and strengthen cross-border collaborations.

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

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

- Utilize crypto inventory tools to learn where and how encryption is currently deployed within an agency's infrastructure
- Prioritize existing infrastructure for a migration to post-quantum cryptography
- Deploy crypto-agile solutions for PKI, data-at-rest and in-transit, and identity and access management
- Apply a Cryptographic Bill of Materials (CBOM)

BIO: Gina Scinta is Thales TCT's Deputy Chief Technology Officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company such as the collaboration with National Institute of Standards and Technology's 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.

Intersection of Quantum, AI and Security

Gina Scinta, Deputy CTO, Thales Trusted Cyber Technologies •

Mary.Shiflett@ThalesTCT.com

ABSTRACT

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

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

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

BIO: Gina Scinta is Thales TCT's Deputy Chief Technology Officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company such as the collaboration with National Institute of Standards and Technology's 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.

SAP and UiPath, Better Together: Navigating Innovation in Navy ERP Modernization

Jonathan Moak, Vice President, Federal, UiPath Inc. • jonathan.moak@uipath.com

ABSTRACT

In today's rapidly evolving defense landscape, the Department of the Navy faces critical Enterprise Resource Planning (ERP) challenges that hinder efficiency and mission readiness. This session explores how the synergy between SAP and UiPath's cutting-edge technology is revolutionizing the Navy's approach to ERP modernization.

We'll delve into the Navy's journey toward standardizing and unifying business processes through ERP Modernization, highlighting the crucial role of enterprise-wide intelligent automation in bridging the gap between legacy systems and a modernized ERP platform.

Discover how UiPath's AI-powered Business Automation Platform, combined with SAP, enables the Navy to optimize existing processes, reduce customizations and ensure a smooth transition with minimal disruption to operations.

Key focus areas include:

- Leveraging automated process discovery for accelerated mapping
- Implementing a singular automation platform across all migration phases
- Utilizing AI-driven automated testing for efficient migration
- Achieving a "Clean Core" through strategic automation
- Exploring advanced AI capabilities such as digital assistants and intelligent document processing to drive transformation

This session will provide valuable insights for functional and financial management components within the Department of the Navy, demonstrating how this innovative approach not only streamlines modernization but enhances operational efficiencies, improves decision-making processes and ensures readiness in the face of evolving challenges.

BIO: Jonathan Moak is the Vice President for Defense at UiPath, where he is responsible for the oversight and management of all sales, revenue operations and the implementation and execution of the company strategy for the Department of Defense.

Moak was previously a Vice President in the Global Public Sector Business Unit at Salesforce, where he developed and directed go-to-market plans to execute customer acquisition strategies focused on cloud adoption and software-as-a-service solutions.

He joined Salesforce following his tenure performing the duties of the Assistant Secretary of the Army for Financial Management and Comptroller. Prior to his appointment, he served as a defense consultant in the Government and Public Sector practice of Deloitte Consulting LLP.

Moak earned a Bachelor of Science in biology at the University of Alabama at Birmingham, a Master of Business Administration at Norwich University and a Master of Science in business analytics from the University of Virginia.

He has significant experience in the military, federal civil service and the private sector leading business transformation programs that drive enterprise impact by focusing on the intersection of mission, business, data and technology. Additionally, Moak is a combat veteran and a distinguished military graduate still serving as an infantry officer in the Army National Guard. He has deployed to the CENTCOM and AFRICOM theaters.

Modernizing Defensive Cyber Operations—the AI Imperative

Zachary Vaughn, Director, Federal Security Engineering, Vectra AI •

zvaughn@vectra.ai

ABSTRACT

Cyber defenders and incident responders have largely been detecting and reacting to human-driven attack efforts—even large-scale offensive cyberattacks are being launched and managed by human operators. Offensive use of artificial intelligence is expanding and with it the speed and scale at which attackers can operate necessitates defensive security tools capable of responding in kind.

Sophisticated attacks prey upon rigid architectural and political boundaries separating infrastructure, identity, software and platform resources and exploit the deficit of human responders relative to vast amounts of data produced requiring inspection and correlation.

Defenders need tools that ‘think’ like attackers.

A true security-led AI platform must act as an all-seeing, dispassionate and tireless observer of all interactions across multiple networks to drastically reduce the mean-time-to-detection and mean-time-to-response for defensive cyber operators, incident responders and analysts, providing them immediate context and narrative around the types of indicators and how they play a part of potentially larger attack campaigns

Vectra can operate at scale, drastically reducing the previously manual and reactive tasks of attributing seemingly disaggregated signals and attributing them back to the participating or impacted systems, identities and services.

- Smoke and Mirrors: Not all AI and ML are equal when it comes to security.
- Focusing on ‘right-of-boom’ is a losing proposition. Real-time analysis and correlation across multiple domains empower defenders to mitigate threats as they occur.
- Perimeter defenses alone are not enough; NGFW, EDR and similar technologies continue to be bypassed.
- Specific use cases and scenarios where AI/ML are best suited to realize meaningful results.
- Supporting existing DCO efforts without additional complexity and friction.

BIO: Zachary Vaughn is the Director of Federal Security Engineering and has been assisting U.S. federal agencies adopt and implement transformative technologies for more than 18 years. Most recently Vaughn participated in multiple working groups and prototypes of functional zero-trust architectures to support critical systems and infrastructure. Prior to joining Vectra AI, Vaughn helped architect and deploy systems and services used by millions of people globally leveraging technologies such as network and identity threat detection and response, access and identity management, network and application security and virtualization.

Deploying Containers and Virtual Machines in Kubernetes for Future-Ready Naval Operations

Greg McPhee, Federal Solutions Architect, Veeam • gregory.mcphee@veeam.com

ABSTRACT

This presentation explores the deployment of both containers and virtual machines (VMs) within Kubernetes environments, highlighting the benefits and challenges associated with this approach. By leveraging Kubernetes, naval operations can gain greater data flexibility, scalability and resilience. The presentation will cover key concepts, new implementation strategies and early adopter use cases, providing a comprehensive understanding of how containers, VMs and Kubernetes can be harnessed to enhance naval capabilities and ensure future readiness.

BIO: Greg McPhee is an accomplished Federal Solutions Architect with more than two decades of experience in the technology industry. Currently, he holds a position at Veeam/Kasten, where he has been applying his extensive expertise to help government clients bridge the gap between on-premises solutions and hybrid multi-cloud offerings.

McPhee gained significant experience as a Senior Systems Engineer at SolidFire Inc., which was later acquired by NetApp. He also held senior roles at AMD and Riverbed Technology, where he specialized in federal and commercial sales engineering. McPhee has built a reputation for his technical acumen and ability to deliver impactful presentations and product demonstrations.

Based in the Washington, D.C., metro area, his career has been defined by his dedication to mission continuity and his commitment to providing robust and innovative data protection solutions to his clients. His deep understanding of technology infrastructure and IT operations continues to benefit organizations aiming to modernize their IT systems and capabilities.

The Future and Innovation of Navy Base Communications: Merging Industry Best Practices and Technologies with Navy Culture

Dominic Bonaduce, Senior Product Strategy Manager, Verizon •

dominic.bonaduce@verizon.com

ABSTRACT

Current Navy communications technology has brought a need for enhanced base modernization, replacing antiquated phone systems, and redefining the perception of soldier mobility. Imagine a base that has an infrastructure that has enhanced interoperability, flexible enough to work with current technologies (inside plant and outside) while providing a roadmap for the Navy to move to a new, modernized platform with minimal constraints.

Verizon can not only provide the products and services in this journey, but true expertise in evolving the journey—conception to activation to servicing, with a trusted partner.

Learn more about how base modernization utilizing private networks and fixed wireless access technology along with Network as a Service (NAAS) and the concept of Software Defined Networking (SD WAN) can help the Navy modernize base communications.

BIO: Thomas Dominic Bonaduce is a Senior Product Strategy Manager where he focuses on commercial paths for new and emerging technology developed at Verizon, focusing on dual-use capabilities across enterprise and public sector domains. Previously, he was the Director of Operations at the United States Department of Transportation and senior advisor to the U.S. Secretary of Transportation. A Native of Southern California, Dominic now resides in Washington D.C.

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.

