



2024 MARITIME INNOVATION SHOWCASE

FEBRUARY 13-15, 2024 • SAN DIEGO, CALIFORNIA



SIGNAL
AFCEA INTERNATIONAL MEDIA

2024 Maritime Innovation Showcase

The Critical Decade for Maritime Modernization

Ensuring the world's allied navies can meet global security demands.

As global challengers threaten U.S. interests, we must continue to maintain maritime dominance—now and well into the future. From a historical perspective, a decade is but a moment. But at this moment, this *critical* decade, we must prepare our maritime forces for strategic dominance for many decades to come.

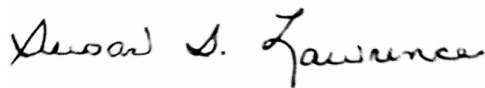
U.S. strategy emphasizes the joint force's combined capabilities in all domains—in concert with our allies, partners, industry and the entire U.S. government—to make the costs of aggression against our vital national interests prohibitive. We continuously build new partnerships and alliances while strengthening those we already enjoy.

For homeland security, whole-of-government cooperation is as vital as international partnerships are globally.

AFCEA International is doing its part to share information, build partnerships and find solutions in this critical domain, to include hosting this Innovation Showcase that provides companies the opportunity to demonstrate cutting-edge solutions to government representatives and potential industry partners. The showcase provides a platform for broad exposure to government, military and industry attendees.

It's imperative we discover and share the information, build the relationships and find the solutions that will help us plot a course during this critical decade, this moment in history, and together build the future of this vital domain.

Best wishes,



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

Table of Contents

Moveworks AI Enterprise CoPilot	
Peter Barrett, Director of Federal, Moveworks	9
Data Protection at the Edge	
Gina Scinta, Deputy Chief Technology Officer, Thales TCT	10
Quantum-Resistant Security	
Gina Scinta, Deputy Chief Technology Officer, Thales TCT	11
Zero Trust: Beyond the Buzzword	
Gina Scinta, Deputy Chief Technology Officer, Thales TCT	12
Build Winning Sales Plans for the Department of Navy	
Joh Slye, Senior Advisory Research Analyst, Deltek	13
Integration Solved: Sharing Our Blueprint for Zero-Trust Adoption	
Herb Kelsey, Project Fort Zero, Lead & Federal CTO, Dell Technologies	14
Using Flank Speed Teams to Create Service Requests	
Adam Prem, Manager, Solution Consulting, ServiceNow	15
How Generative AI Is Transforming Maritime Domain Awareness	
Chad Meley, Chief Marketing Officer, Kinetica	17
Decision and Data Dominance for the Warfighter	
Randy LeBlanc, Vice President, Data Analytics, Altair	18
Accelerated Product & Business Innovation with Altair Open Architecture Digital Engineering	
Keshav Sundaresh, Global Director of Product Management, Digital Twin and Model-Based Systems Engineering, Altair.....	19
Realizing Digital Modernization of Operational Platforms	
Michael Griesi, Senior Global Technical Account Manager, Altair.....	20
Designing for Sustainability—Women in Cybersecurity	
Teresa Duvall, Faculty Lecturer, Old Dominion University	21

The Zero-Trust Imperative: Building a Core of Security Around Mission-Critical Data Jim Cosby, Chief Technology Officer, NetApp.	22
Securely Delivering Information from Anywhere to Everywhere at the Speed of the Mission D.R. Carlson, Senior Director of Segment Marketing, Equinix	23
Next-Generation Navy Mobility Access-As-a-Service to Classified Data John Dunn, Senior Solutions Architect, Archon Division, Melissa Adams, Director, Archon Division, ID Technologies, LLC (CACI)	24
Don't Let the IO Blender Destroy Your AI Model Training Chris Zurich, Principal Systems Architect, WEKA Federal	26
Building Highly Resilient Defense Systems Using Agile at Scale Cynthia Ferreira, Federal Strategic Adviser, Scaled Agile, Inc.	27
Leveraging Satellite Communication to Achieve Mission Results Bob Beler, AVP Enterprise Sales, Allot	28
Artificial Intelligence: The Journey that Got Us Here and What's Next Bill Higgins, Vice President, watsonx Platform Engineering and Open Innovation Research IBM	29
Generative AI Equipment Maintenance Assist Bill Higgins, Vice President, watsonx Platform Engineering and Open Innovation Research IBM	30
Enabling Readiness With IBM Watsonx Bill Higgins, Vice President, watsonx Platform Engineering and Open Innovation Research IBM	31
DTEX InTERCEPT - Advanced Insider Risk Management Mike Rider, Senior Solutions Engineer, DTEX Systems.....	32
From Edge to Insight: Real-Time Data at the Tactical Edge Cuong Nguyen, Vice President, Public Sector, Aerospike	33

Accelerate Mission-Critical Decisions with KPMG Aperture Phillip Sutton, Director, Optimization and Simulation, KPMG	34
Innovations in Cloud Security for Mission Success Steve White, Field Chief Information Security Officer, Wiz.....	35
Workload Resiliency and Data Recovery Through Red Hat’s Software X Concept Tom Skradski, Application Platform Solution Specialist, Red Hat	36
Optimizing Data Security to Support the DoD’s JADC2 Strategy Chris Brow, Chief Technology Officer, Public Sector, Immuta.....	37
How to Increase Warfighter Efficacy Through Innovations in Edge Computing Andres Giraldo, Deputy Director, Product Development, Sealing Technologies (SealingTech) ...	38
Accelerated Data Access Impact on Naval Operations Russel Davis, Chief Operating Officer, Vcinity	40
Coalition Information Sharing During Great Power Competition Russ Smith, Field Chief Technology Officer, Zscaler.....	41
How to Operationalize the Executive Order on AI for the Department of Defense Toan Do, Vice President, Sales, Collibra	42
How to Speed Up Acquisition Lifecycles With the No. 1 CRM Matthew Jacobs, Digital Transformation Executive, David Nava, Principal Solution Engineer, Salesforce.....	43
Achieving Data Dominance: The Right Data, At the Right Place, At the Right Time—All the Time Gary Hix, Chief Technology Officer, Hitachi Vantara Federal	45
AI and Decision Advantage Terry Halvorsen, Vice President, Federal, IBM	46
T-Mobile U.S. and JMA’s role in the 5G Transformation of the Department of Defense Rishi Bhaskar, Senior Vice President and General Manager, Global Verticals & Partnership, JMA Wireless.....	47

Mission Assurance with Zero-Trust Privilege Access Service in the Maritime Environment	
Andrew Whelchel, Senior Solutions Engineer, Saviynt.....	48
Identity Trends Driving Zero-Trust Programs in the DoD	
James Imanian, Senior Director, U.S. Federal Technology Office, CyberArk.....	50
SOAR/Swimlane—Order from Chaos	
David Maphis, Cybersecurity Solutions Architect, Merlin Cyber	51
Enable Operational AI and Enhance Mission Readiness With Trusted Data	
Rick Taylor, Senior Solutions Engineer, Cloudera Government Solutions, Inc.	52
Private 5G—Be Your Own Mission IoT Mobile Operator	
Andrew Beaty, Chief Network Design Engineer/Chief Marine Corps Networks Design/Engineer, Global Maritime Defense Team, Ciena Government Solutions, Inc.	53
BMC Helix Edge	
Michael Alonso, Senior Solutions Engineer, BMC Software	54
Keeping It Simple—Breaking Down Cloud Misconfigurations	
Dilip Bachwani, Chief Technology Officer and Senior Vice President, Enterprise TruRisk Platform, Qualys	55
Securing Sensitive Data in a Connected World	
Lee Meadows, Lead Federal Systems Engineer, Sonatype.....	56
Enhancing Cybersecurity Measures in the Infrastructure Supply Chain	
John Loucaides, Senior Vice President, Strategy, Eclipsium.....	57
Decoding the Seas: How Observability Enables Better Decisions Faster	
Ken Wick, Solutions Engineer, Dynatrace	58
A Sailor’s Experience from Recruitment to Retirement with Adobe	
Michelle Woolford, Navy/USMC/4th Estate Account Director, Adobe.....	60
How Militaries Can Build, Buy and Deliver Capabilities in a Digital Age	
Adam Routh, PhD, Defense and Space Research Lead	
Lauren Dailey, Senior Manager, Deloitte.....	61

Submissions

Moveworks AI Enterprise CoPilot

Peter Barrett, Director of Federal, Moveworks • pbarrett@moveworks.ai

ABSTRACT

In an era defined by rapid technological advancement, the public sector faces unique challenges in bridging the gap between the needs of warfighters, civilians and contractors, and the technologies they employ on a daily basis.

Moveworks, which recently announced its FedRAMP Ready status, aims to be the first SaaS accredited IL5 (Impact Level 5) compliant AI solution that empowers public sector organizations to enhance operational efficiency while upholding the highest security standards. The company explores the pivotal role of AI in the public sector, emphasizing the unique requirements for handling sensitive and classified information and outlines what Department of Defense agencies can expect to achieve with the Moveworks solution.

By harnessing the power of AI, public sector organizations can streamline their operations, improve user experience and allocate resources more effectively. The IL5 secure solution offered by Moveworks promises to be a game-changer, enabling public sector entities to adapt to the demands of the digital age without compromising on security and compliance.

Moveworks provides an essential resource for those looking to leverage AI in the public sector while ensuring that critical information remains protected. Moveworks' cutting-edge IL5 secure AI solution represents a significant step toward a more efficient, secure and responsive public sector, ultimately benefiting both the personnel serving the nation and the citizens they serve.

BIO: Peter Barrett is a 30-year Washington, D.C., native who has spent his career focused on the public sector. For the past 5-plus years, his primary focus has been helping private enterprises, DiBs and public sector agencies embrace trusted, secure and scalable AI, ML and NLU technologies to drive mission success. His experience includes working with the world's most advanced large language models, like GPT-4, as well as generative AI applications for federal and enterprise environments.

Data Protection at the Edge

Gina Scinta, Deputy Chief Technology Officer, Thales TCT • Gina.Scinta@ThalesTCT.com

ABSTRACT

Core computing functionality commonly found in data centers and in the cloud is also being deployed at the edge—data protection capabilities must transition with that move.

However, many challenges often stand in the way of extending core-level security to the edge. Harsh environments, bandwidth-limited and disconnected sites, overrun or hostile scenarios and constraints related to size, weight, and power have made it difficult to employ the appropriate levels of security while allowing the kind of quick response needed at the edge.

True data protection extends to edge. From Thales TCT learn how to apply the same level of security deployed in the core and the cloud to edge environments. Topics include:

- How to contend with environmental and operational constraints at the edge
- How to extend your existing cybersecurity infrastructure to the edge
- Why supply chain security is critical at the edge

BIO: Gina Scinta is Thales TCT's deputy chief technology Officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC, and more. Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world class encryption and key management for data at rest in data centers and cloud infrastructures.

Quantum-Resistant Security

Gina Scinta, Deputy Chief Technology Officer, Thales TCT • Gina.Scinta@ThalesTCT.com

ABSTRACT

Quantum computing's impact is likely to be large—the potential computational power could render today's encryption algorithms obsolete. The White House's National Security Memorandum on Promoting U.S. Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems states that “America must start the lengthy process of updating our IT infrastructure today to protect against this quantum computing threat tomorrow.”

The memo continues by stressing that “[c]entral to this migration effort will be an emphasis on cryptographic agility, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards.”

The Quantum Computing Cybersecurity Preparedness Act also places similar emphasis on need for crypto-agile applications, hardware, and software. Keep in mind that even if a crypto-analytically relevant quantum computer is a decade away, bad actors can take note of potential vulnerabilities now, and exploit them later.

Thales TCT offers a way to start the transition to quantum-safe cryptography and key factors to consider when preparing for a quantum-safe encryption strategy:

- Know your risks—Learn how long-term data is subject to early attacks and about key initiatives that address the quantum threat
- Focus on crypto agility—Learn what to look for in a quantum-resistant crypto solution
- Start today—Learn how to design a quantum resistant architecture

BIO: Gina Scinta is Thales TCT's deputy chief technology Officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC, and more. Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world class encryption and key management for data at rest in data centers and cloud infrastructures.

Zero Trust: Beyond the Buzzword

Gina Scinta, Deputy Chief Technology Officer, Thales TCT • Gina.Scinta@ThalesTCT.com

ABSTRACT

Zero trust is not just another buzzword in a never-ending list of tech trends. The principles of zero trust eliminates the binary trust/don't trust approach applied to users and assets in yesterday's on-premises, perimeter-centric environments.

According to a recent survey, 100% of U.S. federal government agencies are storing sensitive data in third-party cloud, mobile, social, big data and IoT platforms, which inherently makes data vulnerable. Traditional perimeter protection does not protect off-premise data, which speaks to the need to take a zero trust approach to data security.

In fact, the White House has even issued guidance including the Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems and Executive Order 14028, which require agencies to develop a plan to implement a zero-trust architecture.

Thales TCT provides best practices for implementing a zero-trust architecture to protect the most sensitive of data and can address the top 5 things everyone should know about zero trust:

- The basics. What is zero trust and how does it apply to data security?
- Setting the stage. How digital transformation can make data vulnerable but also more secure.
- Getting to work. Tips for putting zero trust architecture into action.
- What about the cloud? How does cloud make implementing zero trust faster but more complicated.
- Pulling it all together. How to develop a long-term strategy to protect data throughout its lifecycle that maps to guidance such as CISA Zero Trust Maturity Model, OMB Zero Trust Strategy, DoD Zero Trust Reference Architecture, and NIST Zero Trust Architecture.

BIO: Gina Scinta is Thales TCT's deputy chief technology Officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC, and more. Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world class encryption and key management for data at rest in data centers and cloud infrastructures.

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 2024 can help you build a winning sales strategy. Deltek explores the Navy's FY 2024 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.

Integration Solved: Sharing Our Blueprint for Zero-Trust Adoption

Herb Kelsey, Project Fort Zero, Lead & Federal CTO, Dell Technologies •

Herb.Kelsey@dell.com

ABSTRACT

The growth of digital ecosystems has created a host of complex security concerns, particularly with data scattered across multicloud environments. While a robust security architecture is vital for business and operational continuity, the focus must expand to prioritize resiliency.

Additionally, in today's data driven environment, AI has become even more critical, further emphasizing the need for security and protection of data. The U.S. Department of Defense released a globally recognized reference architecture for zero trust, and organizations are embracing the approach to modernize and stay resilient. Yet determining where to start, prioritizing capabilities, progressing toward maturity and integrating it across multiple vendor products is complicated.

Dell Technologies is leading an ecosystem of technology partners to deliver a validated zero-trust solution. The recently announced Dell Technologies Project Fort Zero, built on the Department of Defense reference architecture, is designed to expedite frictionless zero-trust adoption. Discover how Dell Technologies will deliver a validated zero-trust solution and learn what that means for both private and public entities around the world.

BIO: Herb Kelsey is the Project Fort Zero team lead and Industry CTO Government at Dell Technologies. He has an extensive multi-decade career beginning as a GE trained engineer and manager, and subsequently as a successful software entrepreneur, an IBM trained architect, IBM's first CTO for cybersecurity and the chief architect for a Department of Defense's mission support agency's global portfolio. Kelsey supported the intelligence community around the world after the 9/11 attacks, designing secure clouds, securing networks and agency-wide mission infrastructures. He was deployed to create the operational watch for our National Counter Terrorism Center and invent analytics for social media intelligence. Kelsey participated in joint R&D activities, including the system that became IBM Streams. In the commercial arena, he has designed health care data analytics for the affordable care act, implemented cognitive solutions for IBM Watson and applied blockchain to secure software supply chains for globally distributed IoT devices.

Using Flank Speed Teams to Create Service Requests

Adam Prem, Manager, Solution Consulting, ServiceNow • adam.prem@servicenow.com

ABSTRACT

ServiceNow is working with PEO Digital to integrate ServiceNow's Employee Service Center and Virtual Agent directly within Flank Speed Teams. This better-together story brings best-of-breed technologies together to provide commercial-grade user experience and customer service to Navy and U.S. Marine Corps users.

Navy/USMC users would be able to:

- Access the ServiceNow virtual agent directly from Flank Speed Teams. They can raise support requests, self-service with knowledge articles or request to speak with a live agent without leaving Flank Speed Teams.
- Respond to the comments on tickets, approval requests and changes with actionable notifications within Flank Speed Teams.
- Receive status updates, e.g. approval updates, directly in Flank Speed Teams.
- Access their echelon-specific Employee Center portal directly within Flank Speed Teams. They can see pending tasks, check the status of open tickets, receive Navy/USMC-wide communications, launch a Teams chat and more via the embedded portal.
- Create, track, update or even close Universal Request directly from Flank Speed Teams. This empowers agents to initiate a Teams chat with the user and import the same in Universal Request.

Navy/USMC Service Desk Agents would be able to:

- Initiate a Flank Speed Teams chat with an employee from a ticket, then to copy the chat transcript back to the ticket as a comment.
- Chat to Call provides service agents with the ability to initiate a meeting on an incident, task or universal request, directly in Flank Speed Teams.
- Quickly respond to significantly disruptive events (major incident management, or MIM) affecting the business which require cross-team collaboration and communication to broader organization.
- Embed portions of the MIM Workbench directly into a Flank Speed Teams conference call to provide shared understanding of the Incident and upcoming communication tasks.

BIO: Adam Prem is a manager of solution consulting for ServiceNow, working to enable digital transformation across the Department of Navy and Marine Corps. He brings 23 years of experience in the IT consulting space, including time spent at Booz Allen Hamilton and BearingPoint/Deloitte supporting various DoD, Defense Logistics and state/local organizations. In his current role, he works with customers to understand the benefits of moving to cloud-based and Software-as-a-Service solutions and leveraging ServiceNow's enterprise applications to achieve successful business and tactical outcomes. Prem has a deep understanding of how DoD organizations operate, from an IT implementation and program management perspective. 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.

How Generative AI Is Transforming Maritime Domain Awareness

Chad Meley, Chief Marketing Officer, Kinetica • cmeley@kinetica.com

ABSTRACT

The integration of generative AI (Gen AI) in maritime domain awareness marks a pivotal shift in situational understanding. Leveraging finely tuned Large Language Models (LLMs), Gen AI assimilates and processes vast troves of data points from maritime and air domains, surpassing human capacities. Through sophisticated algorithms, it creates a unified, comprehensive common operating picture that allows for real-time analysis and prediction, enabling proactive responses to potential threats and improving navigation safety. Gen AI's transformative impact is evident in its ability to amalgamate billions of disparate data points, providing unprecedented situational awareness crucial for maritime operations' efficacy and security.

BIO: Chad Meley is an executive at Kinetica. His experience includes more than 20 years as a leader in SaaS, big data, advanced analytics for early-stage software companies and large, established leaders alike. Prior to joining Kinetica, Meley was vice president of product marketing at Teradata, where he played a key role in repositioning Teradata during the rise of big data and the cloud to its current leadership position. Meley has also held a variety of leadership roles centered on data and analytics with Electronic Arts, Dell and FedEx. He holds a doctorate from the University of Florida, where his dissertation was on Applied Artificial Intelligence, an MBA from the Rawls College of Business at Texas Tech University, and a B.A. in economics from the University of Texas.

Decision and Data Dominance for the Warfighter

Randy LeBlanc, Vice President, Data Analytics, Altair • rleblanc@altair.com

ABSTRACT

In the dynamic landscape of modern warfare, the Altair RapidMiner platform emerges as a transformative catalyst, playing a pivotal role in the Navy's data strategy. The platform addresses the challenges posed by the exponential growth of data, positioning itself as a cornerstone for achieving data and decision dominance.

Altair RapidMiner integrates skill-appropriate tooling and data analytics upskilling, becoming a medium for decision dominance in data-intensive environments. Its unique importance lies in the ability to advance enterprise data capabilities across the Business Mission Area and Warfighting Mission Area. Through advanced data integration, analysis and visualization tools, the platform fosters collaboration in the joint domain environment.

The key is Altair RapidMiner's ability to accommodate users of varying skill levels, from SMEs to developers, addressing challenges such as an analytics skills gap and centralization of data. It promotes a collaborative approach, recognizing SMEs as the best developers of decision systems, even if they lack coding or development skills.

The platform transcends complexity barriers, enabling orchestration, analysis and actionable intelligence derived from data. Positioned at the cornerstone of the Navy's digital transformation, it empowers personnel to harness the power of data in pursuit of information dominance.

Altair RapidMiner aligns with essential requirements for the Navy, ensuring security, scalability and availability. Adherence to zero-trust principles, compatibility with modern authentication and authorization standards, and connectivity to enterprise data fabrics make it a robust solution. The platform's unique ability to transition between authoring modalities and provide explainable AI sets it apart as an invaluable tool for the warfighter.

In summary, Altair RapidMiner offers the Navy a comprehensive solution for achieving data and decision dominance. With secure access, multi-persona authoring, built-in upskilling, and trust-building through explainable AI, the U.S. Navy will enhance its advantage in the battlefield by leveraging the full spectrum of data producers and consumers at the speed of war.

BIO: Randy LeBlanc developed Altair's Center of Excellence enablement methodology for the Altair RapidMiner platform. In his career, he has run global customer success teams and global software development teams for industry leading companies with a focus on high performance computing and artificial intelligence.

Accelerated Product & Business Innovation with Altair Open Architecture Digital Engineering

Keshav Sundaresh, Global Director of Product Management, Digital Twin and Model-Based Systems Engineering, Altair • keshavs@altair.com

ABSTRACT

Altair showcases how digital engineering is driving the automation of product and business decisions—from planning, design and manufacturing to operation and maintenance across industries. Digital twin enables a living and breathing system combining multiple data streams (digital “threads”). These data streams are used to create a digital representation of the elements and dynamics of assets to improve collaboration, information access, and decision-making. The presentation will focus on Altair Digital Engineering benefits, real-world applications, and business impact.

BIO: Keshav Sundaresh brings nearly 20 years of customer success and engineering experience to his role of global director of product management, digital twin and model-based systems engineering at Altair. In his role, he’s responsible for technical thought leadership, strategy and driving the development of integrated software solution offerings that enable open, traceable, collaborative and holistic digital twin/thread.

Sundaresh has held several leadership roles during his 17+ year tenure at Altair and prior to joining the company, he was a design engineer for new product development at Bharat Fritz Werner Ltd. He holds a bachelor’s degree in engineering from Visvesvaraya Technological University in India.

Realizing Digital Modernization of Operational Platforms

Michael Griesi, Senior Global Technical Account Manager, Altair • mgriesi@altair.com

ABSTRACT

The DoD Digital Engineering Strategy envisioned a future where prototypes and testing are optimized in a virtual environment, and data is leveraged across a dynamic lifecycle. In support, the U.S. Navy and Marine Corps Digital Systems Engineering Transformation Strategy astutely highlighted the need to design, deliver and sustain platforms under restrictive budgets and aggressive deadlines. While it may seem the vision and challenges are at odds, that future is now.

Altair Engineering is currently solving this conundrum. By merging physics-based modeling and data analytics across high-performance computing environments, complex environments such as Airborne RADAR electromagnetic field distortion caused by operational deformation can be predicted and optimized quickly and efficiently, while establishing a predictive digital thread across the system's lifecycle.

BIO: Michael Griesi received B.Sc. and M.Sc. in electrical engineering focused on signal integrity from the University of South Carolina. Griesi's 20 years of experience spans a broad background in electromagnetics, ranging from design, test and measurement, debug and repair, simulation, validation, and automation in digital high speed, wireless, and passive RF applications, across DoD, DoE, aerospace, telecommunications, computer aided engineering (CAE) and high bandwidth electrical interconnect industries. Today, Griesi is a senior global technical account manager at Altair Engineering focused on high-frequency electromagnetic applications in the aerospace and defense industry, passionate about empowering engineering organizations with diverse technical disciplines to innovate and optimize efficiently through digital modeling.

Designing for Sustainability—Women in Cybersecurity

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

ABSTRACT

How do we attract and maintain women into the field of cybersecurity? How do we address the gap from academia to being hired in the cybersecurity field in a sustainable manner? When the forcing functions are cyber attacks on our financial systems or national security systems, we won't be looking to see who is female or male in filling the position. We will want the best and brightest. It's not a question of if these attacks are going to happen, rather it is when and how often. The time to act is NOW.

BIO: Teresa Duvall is a faculty lecturer at Old Dominion University's School of Cybersecurity. She is internship director, School of Cybersecurity, Coastal Virginia Commonwealth Cyber Initiative (COVA CCI) liaison. She sits on AFCEA International's Board of Directors and a life member. She sits on AFCEA Hampton Roads' chapter as the vice president of education, Women's Outreach leader and past president.

The Zero-Trust Imperative: Building a Core of Security Around Mission-Critical Data

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

ABSTRACT

Zero trust is a paradigm shift in cybersecurity. According to Randy Resnick, director, Zero Trust Portfolio Management Office, Office of the DoD CIO: “It is a new way, it is the only way, that we can protect our data from adversaries going forward.”

Providing zero-trust data and network security in the field and with foreign partners can pose a challenge, both conceptually and practically. Finding zero-trust accreditable and scalable solutions for the verification of data and assets that may be detached from physical locations requires a new set of technology. These technologies should permit and include secure but seamless sharing of data between partners while granting only conditional access to data and networks. NetApp showcases what progress has been made in this field, strategic foresight, foreseeable demand for the integration of devices and users in numbers and quality and potential new approaches and solutions.

BIO: Jim Cosby is currently a chief technology officer for U.S. Public Sector and Partners for NetApp. Cosby has more than 25 years of engineering and technical sales experience supporting a variety of public sector and commercial customers. Cosby has focused on data management and security for more than 20 years, including on-premise and hybrid multi-cloud technologies. He has a passion for teaming with customers, partners and colleagues to drive great outcomes to solve technical challenges and win.

Securely Delivering Information from Anywhere to Everywhere at the Speed of the Mission

D.R. Carlson, Senior Director of Segment Marketing, Equinix • dcarlson@equinix.com

ABSTRACT

There is a growing federal focus on the physical security of government data centers, and the adoption of hybrid multi-cloud strategies that explore vendor-neutral data center options. By leveraging software-defined networking, cloud adjacent storage and interconnection capabilities, government agencies can dynamically deliver services in a hybrid multi-cloud environment, while at the same time, enabling legacy applications to operate in a cloud-like fashion efficiently and rapidly delivering mission-critical data to the warfighter.

BIO: D.R. Carlson is the senior director of segment marketing for the Americas for Equinix, focusing on joint value propositions and go-to-market strategy with Equinix's largest partners. Carlson works extensively with the Equinix Government Solutions team to provide tailored solutions to the state and local government agencies.

Prior to joining Equinix, Carlson served as vice president for Neovera (Equinix New Partner of the Year 2017), and Oratium. At Oratium, he built messaging for companies, trained Ted speakers and prepared executives for keynote speeches.

Next-Generation Navy Mobility Access-As-a-Service to Classified Data

John Dunn, Senior Solutions Architect, Archon Division and Melissa Adams, Director, Archon Division, ID Technologies, LLC (CACI) • jdunn@idtec.com and madams@idtec.com

ABSTRACT

Government agencies have experienced a sharp increase in the requirements for employees to work from home, or in disparate facilities. While remote work might be a newer concern, securely extending network access to contractors has been a long-standing battle. As the Navy is mobilizing remote access to its network there are some key challenges:

1. Limited availability of government-issued devices
2. Difficult contractor compliance and audit
3. Building classified work areas is time & cost prohibitive
4. Lower productivity due to personnel having to commute to approved classified workspaces

To solve these challenges, a compelling use case emerges from various federal agencies pursuing Commercial Solutions for Classified (CSfC) systems. This opens a door of opportunity for a future government shared data environment operating on an Access-as-a-Service (A3S) model to government end users. A3S, as a use case, benefits the Navy by maximizing capital investment while reducing time to delivery for organizations needing flexible, affordable, secure access to classified networks in locations where no such access exists. Backdoor virtual private network (VPN) tunneling through firewalls for the purpose of remote access can all but be eliminated. CSfC distribution can provide direct domain-controlled access to applications and data delivered in a way that is easier to manage and more secure than tunneling.

The internet affords global connectivity but is highly untrusted and serves as an adversarial data supply route to take advantage and disrupt Naval interests using cyber toolkits. However, the costs advantages available by using the global internet resources cannot be ignored and must continue to be used in creative ways for the Navy to maintain its information dominance.

The Navy's network infrastructure has been built-up/out over the years with significant investment to enable secure information transfer. The capabilities these networks bring to bear are tremendous. Still, this network infrastructure is not without gaps and needs for improvement. For example, the need for mobility was never greater than when COVID-19 presented a huge risk to society and the missions of the entire Department of Defense (DoD). What information inhibiting event will be next?

While the Navy has made tremendous strides to improve its ability to operate more autonomously across land and sea, there is still much work to be done to fill gaps. Consider the fact that a sizable portion of sailors, Marines and DoD civilians must move between facilities to perform their duties and access classified

information. Most buildings are simply not prepared to meet classified security standards. The impact to the Navy is waste of valuable personnel time and energy that could otherwise be spent focusing on Navy mission requirements.

What if a minimal investment in a CSfC distribution back-bone, compared to the significant costs and man-hours spent to maintain current stove-piped networks, was applied across a small community of interest (COI)? Such a pursuit could facilitate and enable classified data communications to almost any need in the Navy or DoD as a whole.

BIO: John Dunn is a senior solutions architect in the Archon Division of ID Technologies. He is responsible for technical engagements with customers designed to uncover digital information challenges and presents alternative computing solutions to the Department of Defense (DoD) and federal agencies. Dunn has vast experience in the National Security Agency (NSA) Commercial Solutions for Classified (CSfC) program, for which Archon is a Trusted Integrator and CSfC product manufacturer. He is a distinguished military veteran with more than 23 years of combined military service in both the U.S. Marine Corps and U.S. Army. He also served as a DoD civilian in the role of chief technology officer for the Joint Communications Support Element (JCSE) located at MacDill Air Force Base, Florida, which is a subordinate command to the U.S. Transportation Command. As a DoD civilian, Dunn was the sole author for the requirements coordination document for a tactical communications system that drove one of the most popular designs for military expeditionary communications kits still used today. He has worked for commercial industry for the past 9+ years focusing on cross domain, CSfC, Virtual Desktop Infrastructure (VDI), cybersecurity and data center solutions. Dunn has a Bachelor of Science and Master of Science Degree in computer information systems and a master's in business leadership.

Melissa Adams serves as the client relations director in the Archon Division of ID Technologies, supporting the Navy and civilian agencies. With more than three years at Archon, she specializes in deploying and implementing solutions through the NSA's Commercial Solutions for Classified Program (CSfC), of which Archon is a Trusted Integrator and CSfC product manufacturer. Adams excels in building and nurturing client engagements by understanding the unique mission requirements of the Department of Defense (DoD) and Federal Agencies.

With more than two decades in the technical industry, Adams has extensive experience, particularly in serving the federal government with a specialized emphasis on data center and enterprise solutions. At Dell Technologies, her focus centered on the Department of Justice working in close collaboration with the Federal Bureau of Investigation. Her tenure at VMware saw her in the role of Senior Engineering Manager, guiding an international team of engineers.

Adams holds a Bachelor of Arts degree in psychology and is the proud daughter of a U.S. Navy veteran and naval aviator.

Don't Let the IO Blender Destroy Your AI Model Training

Chris Zurich, Principal Systems Architect, WEKA Federal • chris.zurich@weka.io

ABSTRACT

According to one of the largest surveys of AI practitioners, data infrastructure is the most significant hurdle to AI success, with 32% of respondents saying it is their top challenge. During AI and GenAI pipeline operations—including ingestion of data, pre-processing, embedding, retuning and then extensive validation/backtesting—IO patterns are widely varied and may lead to an IO blender issue, a situation where different workloads consisting of transactional and streaming IO contend with a sub-optimal performance level.

The IO blender impacts time-to-results in generative AI by reducing the utilization of the compute GPU and CPU. We show actual IO blender effects on model performance and how you can avoid them and showcase the metadata management challenges at AI scale that can also affect model performance. Finally, we share some practical tips for how to get maximum utilization for your existing AI infrastructure.

BIO: Chris Zurich has spent more than 20 years successfully architecting and executing enterprise class storage solutions in the DoD/IC. As a principal systems architect at WEKA, he is responsible for working with customers to help solve their most pressing HPC, AI and ML challenges.

Building Highly Resilient Defense Systems Using Agile at Scale

Cynthia Ferreira, Federal Strategic Adviser, Scaled Agile, Inc. •

cynthia.ferreira@scaledagile.com

ABSTRACT

The use of lean-agile management techniques is becoming increasingly popular in the government sector, especially in the context of the Department of Defense. Scaled Agile aims to provide insights and best practices for implementing agile methods in government systems, focusing on large hardware systems. Agile techniques need sustained leadership and best practices in defense.

Scaled Agile can teach how to apply SAFe to manage massive systems. It will also cover the additional roles, artifacts and events needed for this purpose. SAFe's usage in government to support building highly compliant systems is highlighted, along with understanding agile roles, artifacts and events that assist in large systems development.

Leveraging Satellite Communication to Achieve Mission Results

Bob Beler, AVP Enterprise Sales, Allot • bbeler@allot.com

ABSTRACT

The modern U.S. Navy relies heavily on cutting-edge, next-gen advanced IT to achieve its daily missions and maintain its global superiority. These IT characteristics reflect the evolving nature of naval warfare, emphasizing the importance of information security, connectivity and adaptability to execute mission-critical tasks. That being said, satellite communication plays a significant role in achieving each mission's required results.

BIO: Bob Beler has more than 21 years of experience within the infrastructure and security solutions provider verticals, including numerous C-level leadership roles along the way. Before joining Allot, where he currently serves as its North America AVP of Enterprise Sales, Beler was responsible for CompuCom's (a billion-dollar VAR within the United States and Canada) Enterprise Business Development and Sales Strategy organization. Before that, Beler served as the vice president of sales at Axiomatic (an Identity & Access Management Security company) for several years. Beler was also the founder and president of a Chicago-based value-added reseller, Information Systems Group Inc. (ISG), for more than 16 years. He holds a Bachelor of Arts from DePaul University in Chicago.

Artificial Intelligence: The Journey that Got Us Here and What's Next

Bill Higgins, Vice President, watsonx Platform Engineering and Open Innovation Research, IBM • billh@ibm.com

ABSTRACT

Artificial intelligence (AI) is advancing at an unprecedented pace, reshaping the world as we know it. One of the most revolutionary breakthroughs came in 2012, when a team from the University of Toronto triumphed in the ImageNet competition, unveiling the power of Artificial Neural Networks/Deep Learning. Today, it is these very same Artificial Neural Networks that are creating machines capable of human-like proficiency in image recognition and language comprehension. These great strides in AI are progressing at an astounding exponential rate beyond anyone's expectations. The world was especially taken by surprise with the release of ChatGPT in November 2022. AI experts had always believed that language comprehension would be the "final frontier" of AI, and would be decades, if not centuries, away. Now, no one can afford not to be aware of what is happening in the world of AI.

BIO: With more than 22 years of computer science and software engineering expertise, Bill Higgins leads IBM's Watson AI platform team, responsible for common foundational ML model training and serving capabilities for Watson applications, core services like NLP, speech and vision, and developer APIs and SDKs. Although his current focus is on helping organizations transform around AI, his previous work included innovations in demo and development tools, design language advancements and private cloud technology. Higgins has multiple publications, enabling clients to adapt to an ever-changing world so that they can continue to succeed in the marketplace by serving their users better and with continuously improving their operational competence. Higgins has a Bachelor of Science in computer science from Penn State University and resides in the Raleigh, North Carolina, area.

Generative AI Equipment Maintenance Assist

Bill Higgins, Vice President, watsonx Platform Engineering and Open Innovation Research, IBM • billh@ibm.com

ABSTRACT

Generative AI based Equipment Maintenance Assistant (EMA) is a capability that can reduce mean time to repair (MTTR), reduce troubleshooting time, recommend actions (for parts, materials, tools), address knowledge gap created by an aging workforce, and improve first-time to fix (FTTF) rate.

Technicians in the maintenance shop spend 80% of their time searching for the information on how to complete the work ticket. This is assuming they are experienced and know where to look. To add to this challenge, there is 70% turnover among the experienced technicians. This vastly impacts the ability to get critical equipment ready to support the mission. Learn how generative AI can accelerate availability and support mission readiness.

BIO: With more than 22 years of computer science and software engineering expertise, Bill Higgins leads IBM's Watson AI platform team, responsible for common foundational ML model training and serving capabilities for Watson applications, core services like NLP, speech and vision, and developer APIs and SDKs. Although his current focus is on helping organizations transform around AI, his previous work included innovations in demo and development tools, design language advancements and private cloud technology. Higgins has multiple publications, enabling clients to adapt to an ever-changing world so that they can continue to succeed in the marketplace by serving their users better and with continuously improving their operational competence. Higgins has a Bachelor of Science in computer science from Penn State University and resides in the Raleigh, North Carolina, area.

Enabling Readiness With IBM Watsonx

Bill Higgins, Vice President, watsonx Platform Engineering and Open Innovation Research, IBM • billh@ibm.com

ABSTRACT

watsonx is IBM's next-generation AI and data platform that provides the most transparent, responsible and governed technology required to enable defense domain users to scale and accelerate the value of AI with trusted data across the Naval enterprise. Based on the best open technologies available, watsonx is designed to improve data access, apply controls, cut costs and create value.

BIO: With more than 22 years of computer science and software engineering expertise, Bill Higgins leads IBM's Watson AI platform team, responsible for common foundational ML model training and serving capabilities for Watson applications, core services like NLP, speech and vision, and developer APIs and SDKs. Although his current focus is on helping organizations transform around AI, his previous work included innovations in demo and development tools, design language advancements and private cloud technology. Higgins has multiple publications, enabling clients to adapt to an ever-changing world so that they can continue to succeed in the marketplace by serving their users better and with continuously improving their operational competence. Higgins has a Bachelor of Science in computer science from Penn State University and resides in the Raleigh, North Carolina, area.

DTEX InTERCEPT - Advanced Insider Risk Management

Mike Rider, Senior Solutions Engineer, DTEX Systems • mike.rider@dtexsystems.com

ABSTRACT

Most Insider Risk solutions for federal entities fail to provide the contextual insights needed to proactively understand, identify and mitigate insider risk before exfiltration (i.e., left of boom). The result is high rates of false positives and time spent on non-threatening alerts. DTEX is different, affording contextual behavioral insights on where and how insider risks move across the Insider Threat Kill Chain along with the opportunity of time to enforce early mitigation.

In 2017, DTEX was awarded a two-year Rapid Innovation Fund by DISA to research and develop a solution to automate the detection of lateral movement, flag unusual use of legitimate credentials and alert on situations of multiple, simultaneous login attempts and other anomalous user behaviors outlined in CNSSD 504. The successful completion of this project in 2019 led to the development of the DTEX InTERCEPT platform which combines the capabilities of a NITTF compliant UAM tool and UBA in an all-in-one lightweight, cloud-native platform. InTERCEPT provides contextual intelligence across data, machines, applications and people to surface and address early warning behavioral indicators of intent.

BIO: Mike Rider is a senior solutions engineer with DTEX Systems with more than 22 years' experience in cybersecurity. In this role, he works closely with DoD, the intelligence community (IC) and federal agencies to develop, modernize and/or enhance their Insider Risk/Threat security programs, enabling them to proactively understand, identify and mitigate insider risk before exfiltration.

Prior to joining DTEX, he held similar roles at Menlo Security, Tanium and Forcepoint G2CI supporting DoD, the IC, and federal civilian agencies. Additionally, he served in the U.S. Navy and Navy Reserve for nearly 21 years, retiring as a cryptologic warfare officer in April 2022. Some of his noteworthy assignments include the White House Communications Agency, the National Security Agency, Joint Special Operations Command and U.S. Strategic Command.

Rider holds a Master of Arts in strategic intelligence and a Bachelor of Science in information technology management from the American Military University.

From Edge to Insight: Real-Time Data at the Tactical Edge

Cuong Nguyen, Vice President, Public Sector, Aerospike • cnguyen@aerospike.com

ABSTRACT

In the fast-paced world of modern data-driven operations, the ability to harness real-time insights at the tactical edge is critical. Whether in the fields of defense, emergency response or critical operations, minimizing latency to ensure immediate access to data are not just important; they are essential for effective and efficient decision-making.

- The Tactical Edge Unleashed
- Edge to Insight Journey
- Real-Time Data Optimization

BIO: Cuong Nguyen is a visionary leader serving as the vice president and head of the Public Sector team at Aerospike. With a profound belief in the transformative power of data to tackle the world's most urgent challenges, his leadership is dedicated to empowering government agencies to harness the potential of real-time data.

In his role, Nguyen oversees all facets of business creation that support the Department of Defense, intelligence community, civilian agencies and state and local entities. With more than three decades of experience in the federal market, Nguyen has been a driving force in assisting agencies to leverage cutting-edge AI/ML solutions across tactical edge, cloud and core systems. His efforts have been instrumental in combating fraud, providing critical situational awareness and enhancing the battlefield advantage for our warfighters. The impact of these endeavors is felt in "real-time" mission outcomes, where every moment counts.

Accelerate Mission-Critical Decisions with KPMG Aperture

Phillip Sutton, Director, Optimization and Simulation, KPMG •

phillipsutton@kpmg.com

ABSTRACT

For the Department of the Navy, making faster, more informed decisions is more critical than ever to maintaining its edge in today's great power competition. Advances in technology infrastructure and advanced analytics have created an immediate opportunity for the Department of Defense (DoD) to connect and accelerate the readiness of people, supplies and systems at levels never possible before. KPMG Aperture helps the U.S. Navy and Marine Corps integrate program data across echelons and geographically disparate locations to develop analytical insights to make data-driven, defensible decisions for resource allocations, from people to parts across time and space, to increase readiness and efficiency across the enterprise. KPMG Aperture is a modular, open-source and customizable decision support solution powered by pre-built accelerator enabled through existing cloud or on-prem infrastructure and tailored for complex, mission-critical DoD environments. Armed with advanced decision support, the Navy and Marine Corps can make mission critical decisions, faster.

BIO: Phillip Sutton is a director within KPMG Lighthouse, KPMG's Center of Excellence for Data, Analytics and AI and leads the development of Modeling, Simulation, and Digital Twin Analytics solutions for the U.S. federal government. In his role, Sutton assists federal agencies in creating analytical solutions to address complex challenges and improve the decision-making processes. With more than 10 years of experience as an operations research analyst and data scientist, Sutton has worked on various challenges, including workforce planning, capability development, acquisition & sustainment, and supply chain & logistics. He holds a master's degree in operations research from George Mason University and is a Certified Analytics Professional (CAP) from the Institute for Operations Research and Management Science (INFORMS).

Innovations in Cloud Security for Mission Success

Steve White, Field Chief Information Security Officer, Wiz • steve.white@wiz.io

ABSTRACT

In January 2023, the Department of the Navy (DoN) and DoN CIO established a major cloud modernization objective: to optimize the Information Environment for Cloud.

Achieving mission success in this era of rapid cloud adoption requires rethinking how organizations approach security, as traditional security tools often lead to blind spots and alert fatigue. Wiz shows how to meet the changing needs of the mission and growth of the cloud, sharing how organizations of every size are adopting Wiz's agentless security solution to ensure readiness in the cloud by gaining complete visibility into their multi-cloud environment and accurate risk prioritization using a security graph.

BIO: Steve White is a field CISO at Wiz, working with organizations in the public sector to dramatically improve their cloud security outcomes. White has worked across all technology areas over the last 25 years. During his career, White has worked as a CSO/CISO (Mangata Networks and ForgeRock), a field CISO (Oracle and Pivotal/VMware), vice president of IT (Young Life), and held a variety of senior security leadership roles at companies, including Microsoft, Amazon, and Sonos. White has a passion for transforming security and infrastructure/operations organizations using modern cloud-native, agile and DevOps principles. Complementing his civilian career, White is a retired U.S. Air Force officer, serving 29 years across active duty, Guard and Reserve, with his last 14 years in cyberspace leadership roles.

Workload Resiliency and Data Recovery Through Red Hat's Software X Concept

Tom Skradski, Application Platform Solution Specialist, Red Hat •

skradski@redhat.com

ABSTRACT

While the Navy has shown vast improvements in building tactical applications and systems iteratively, it continues to struggle with routine deployment via DevSecOps. This keeps the Navy from putting cutting-edge technologies in the hands of the warfighter.

Red Hat's Software X concept fixes this problem by providing the Navy and USMC with a secure, resilient and modular platform that is horizontally and vertically scalable that also decouples the software layer from the hardware layer. This enables the development, testing and deployment of "forever" software baselines; a continuously versioned software baseline over an independently evolving hardware baseline. The concept gives the Navy and Marine Corps a tactical platform with port/starboard resiliency via advanced workload orchestration and data redundancy through software defined storage. Further, Software X is installable on many legacy hardware sets. This means tactical platforms can deploy the concept without waiting for costly and time-consuming hardware updates and the warfighter can take advantage of new software capabilities at the speed of development.

BIO: Tom Skradski is the application platform solution specialist covering the Navy and Marine Corps for Red Hat. He has worked in DoD as a software engineer, cyber analyst, integrator and eventually with NIWC Lant as a lead engineer with CANES at PMW 160. He holds bachelor's and master's degrees from the University of Illinois at Springfield and currently lives in Charleston, South Carolina.

Optimizing Data Security to Support the DoD's JADC2 Strategy

Chris Brown, Chief Technology Officer, Public Sector, Immuta • chris.brown@immuta.com

ABSTRACT

The need for data-driven decisions is increasingly essential to maintain battlefield superiority across land, air, sea and space. Yet, enabling warfighters to quickly access data for decision-making requires rethinking how data is managed, governed and secured. It must be fast to access but only accessible by the right people at the right time.

To achieve this goal of information superiority, the Department of Defense (DoD) has outlined two key lines of effort (LOEs): (1) establishing the data enterprise, and (2) modernizing Mission Partner Information Sharing. To successfully enable these two LOEs, the DoD must optimize its data security strategy in order to manage data security policies at scale, meet requirements for zero trust mandates, and operate in a federated data mesh architecture.

Learn from Chris Brown, public sector CTO of Immuta, about:

- How Zero Trust and Data Mesh support the goals of JADC2
- Why efficient data security will be necessary to implement the goals of JADC2
- How the Navy can automate the discovery, tagging and securing of data while integrating with existing enterprise data governance tools

BIO: Chris Brown is currently the chief technology officer for public sector at Immuta. He is an experienced strategic IT leader, helping organizations deliver on their digital transformations. As a thought leader, Brown has served as a trusted adviser to large federal agencies to develop and implement agency cloud migration strategy, lead the development and delivery of a data governance strategy and architect large analytic programs for national security agencies. While at Immuta, Brown has focused on helping federal agencies increase the speed of data-driven decisions through data governance best practices.

How to Increase Warfighter Efficacy Through Innovations in Edge Computing

Andres Giraldo, Deputy Director, Product Development, Sealing Technologies (SealingTech) • andres.giraldo@sealingtech.com

ABSTRACT

SealingTech provides modular edge computing servers to the Department of Defense (DoD) for various use cases, including cyber fly-away kits, tactical edge computing kits, AI/ML edge device applications and more. SealingTech aims to advise the Sea Service community on the latest industry innovations that can enhance warfighters' speed, efficacy and mission success.

We demonstrate how SealingTech's rapid prototyping, end-user feedback and Other Transaction Authorities (OTAs) have enabled us to design and quickly field the latest technological advancements throughout the DoD. SealingTech's edge compute servers and fly-away kits, highlighting how they can reduce the time necessary to achieve mission readiness.

Additionally, our team shares insights from automating software deployments to edge devices by demonstrating SealingTech's new rapid deployment touchscreen for edge devices. This touchscreen enables users to monitor, administer and redeploy the software stack on edge servers in an optimized manner as easily and quickly as it is to install an app on a cellphone. By automating and optimizing these processes, we significantly reduce the time necessary for teams to become mission-ready and further enhance their ability to perform effectively and efficiently in mission-critical environments.

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

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

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

One of Giraldo's key strengths lies in his unwavering dedication to understanding each customer's unique requirements. He engages closely with various stakeholders to gain insight into their cyber rapid response kit needs, allowing him to tailor solutions that align with their goals.

This personalized approach has earned him the trust and respect of clients and team members, who recognize his commitment to ensuring their security and success.

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

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

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

Accelerated Data Access Impact on Naval Operations

Russel Davis, Chief Operating Officer, Vcinity • rdavis@vcinity.io

ABSTRACT

Information access and awareness drive timely and appropriate decision making for every mission and are critical for minimizing time-to-action.

The Defense Department strives to share data across services, organizations, departments and even coalition partners under the Combined Joint All-Domain Command and Control (CJADC2). Yet, moving and accessing data is problematic, particularly as sensor data volume grows at a rate for which communications networks cannot keep pace. This challenge is further compounded as distance (latency) increases and traditional network performance dramatically decreases.

This has been a significant issue for the Navy, where the primary means of communications for ships at sea is via MIL-SAT communications at very low bandwidths. While there are now more options to access COMSAT networks in low Earth orbit (LEO) that provide multiple times the bandwidth of the legacy satellites, those networks cannot be fully utilized due to the impact of latency with standard protocols like TCP/IP or UDP.

Vcinity has a solution that mitigates the negative effect of latency on data access and transfer over moderate to high latency networks from shore-to-ship or ship-to-ship. In addition, Vcinity shows how data at a remote location can be accessed by users or applications over any IP-based network in near real-time without having to transfer the data first. These capabilities are enabled by Vcinity's unique approach to achieve data throughput at ~95% of the available bandwidth, regardless of distance.

Learn how to improve your security posture by eliminating unnecessary data movement, reduce cybersecurity risks associated with copy management and better protect data in flight by both encrypting, as well as splitting it, over several paths and reassembling at the remote site. Vcinity has partnered with Dell Technologies to create solutions that operate in standard rack mount servers for the data center and edge solutions that can be deployed to mission end points including shipboard use.

BIO: Vcinity COO, Russel Davis, brings more than 25 years' experience in management, operational and technical leadership at organizations ranging from start-ups to Fortune 500 companies.

Prior to joining Vcinity, Davis was co-founder and COO of a well-funded venture that developed telecommunications hardware and the service platform managing NFC devices and transactions for transportation and payment systems. He also served as CTO and vice president of product development for CIC (a public company) and director of services for Everex Systems (acquired by FPG), as well as working in field services engineering management at Centel Information Systems (acquired by Sprint) and for the U.S. Navy.

Coalition Information Sharing During Great Power Competition

Russ Smith, Field Chief Technology Officer, Zscaler • rsmith@zscaler.com

ABSTRACT

Carl von Clausewitz, the 17th century military strategist, spoke on the importance of lines of communication (LOC) while observing Napoleon. Those observations are as relevant today, in all warfighting domains, to include the cyber domain. As Clausewitz wrote, the LOC was necessary to move critical supplies to the frontline as well as provide an egress route for forces moving away from the frontline. Securing LOCs is paramount, especially when those “supplies” include sensitive warfighter information.

Every military branch has incorporated LOCs into its own domain operational art for mission success. The Army establishes ground LOCs, the Navy must secure sea LOCs, and the Air Force identifies air LOCs into and out of the area of operations (AOR). In the cyber domain, this concept is also very relevant. Zero trust, as a cybersecurity paradigm, enables cyber operators to securely move critical information around the battlefield, to include to and from our coalition partners, and everywhere it is needed for mission success. Zscaler addresses zero trust as the critical enabler to establish cyber LOCs. Additionally, a high-level architecture is described to rapidly on-board coalition partners to give military planners the agility needed for today’s great power competition.

BIO: Russ Smith is a field CTO supporting Zscaler’s DoD Team. He joined Zscaler after a 30 year Air Force career, culminating as the deputy chief information officer at the U.S. Special Operations Command. During his post-military career, he was a research analyst with the Institute for Defense Analyses, the vice president of the cyber practice at SAIC, and a security account lead at Accenture Federal Systems. Smith holds Masters Degrees in systems technology (Joint Command, Control, Communications and Computers) from the Naval Postgraduate School and in Military Operational Art and Science from Air University, and a B.S. in computer information science from Bloomsburg University of Pennsylvania. He is also certified as an Information Systems Security Professional, Project Management Professional, Chief Information Officer and Chief Information Security Officer.

How to Operationalize the Executive Order on AI for the Department of Defense

Toan Do, Vice President, Sales, Collibra • toan.do@collibra.com

ABSTRACT

With the recent executive order on safe, secure and trustworthy AI and the DoD Data, Analytics and AI Adoption Strategy, the DoD and its component agencies need to create steps to implement these policies. Collibra explores key AI risks, limitations that come along with AI and an AI framework you can start using today, outlining and exploring four fundamental steps to operationalize the executive order including:

- Proposing use cases: AI algorithms require regulatory approvals with internal stakeholders. Approvers need to understand the need and the legal, ethical and compliance implications.
- Identifying data: What data is used? Who has access to this data? Is it the most accurate source of data? Continuous assessment of the data as the appropriate source, especially as new data sets enter the enterprise's data corpus.
- Developing Models: Development of models involves the data and the algorithm itself. Developers must make sure the data is compliant and that bias is eliminated. Developers must understand data sharing rules and sovereignty and implement necessary privacy controls.
- Monitoring results including continuous assessment of the model: Have better data sources emerged and are the results yielding the intended outcome as proposed?

Finally, the company shares lessons learned and best practices from others in commercial regulated industries, so you can learn from others who faced similar challenges.

BIO: Toan Do brings his leadership experience and industry knowledge of data management, security, and analytics to the U.S. federal government, where he helps the largest agencies understand data to better inform their decisions in the most critical missions.

How to Speed Up Acquisition Lifecycles With the No. 1 CRM

Matthew Jacobs, Digital Transformation Executive, and David Nava, Principal Solution Engineer, Salesforce • matthew.jacobs@salesforce.com and dnava@salesforce.com

ABSTRACT

When stakeholders across the entire acquisition ecosystem are united under a single view, collaboration is seamless, insights are derived faster and acquisition cycles are streamlined.

Learn how Defense organizations and best-in-class industry organizations use a centralized platform to increase speed to innovation and improve supply chain resiliency.

Salesforce offers:

- Strategies that leading agencies employ to shorten acquisition lifecycles.
- Solutions that help address common challenges.
- Live demo of Salesforce Acquisition Relationship Management capabilities for defense organizations.

BIO: Matthew Jacobs is a consistently high-performing executive leader with deep experience across technology, system integration, financial management and supply chain. He draws on his professional experience and training with the U.S. Navy, Department of Defense and the most prestigious technology and consulting firms to help clients solve their most complex challenges.

David Nava was commissioned as an ensign in the U.S. Navy in 1999 via the University of Washington's NROTC program. He earned his Naval Flight Officer wings in 2000 and selected EA-6B Prowlers. Nava flew with Electronic Attack Squadrons VAQ-133 and VAQ-140 out of NAS Whidbey Island Washington, and deployed in support of Operations Northern Watch and Enduring Freedom.

In 2012 he was assigned to the U.S. Naval War College for back-to-back tours as a military professor in the War Gaming Department. Nava completed his military career at the Naval War College, retiring as an O-4 in July 2019 after serving for 20 years.

A year prior to retiring, Nava discovered Salesforce through a LinkedIn connection and took advantage of its veteran support programs to begin learning the platform. He was able to gain experience by volunteering as a system administrator for veteran-focused nonprofit organizations.

Three months prior to his transition date, Nava leveraged the DoD Skillbridge program to participate in a professional internship with a consulting firm that specializes in implementing Salesforce. At the conclusion of the internship upon his retirement, Nava was offered a full-time role as a solution architect. He accepted and began his second career, in the Salesforce ecosystem.

A year later, Nava received an offer to work at Salesforce and was hired as a senior solution consultant. Eight months later he was internally recruited to Global Public Sector, where he currently works as a lead solution engineer on the Department of Defense team.

Nava now has 16 technical certifications and mentors military members, veterans and spouses who are interested in transitioning to roles in the Salesforce ecosystem.

Achieving Data Dominance: The Right Data, At the Right Place, At the Right Time—All the Time

Gary Hix, Chief Technology Officer, Hitachi Vantara Federal •

gary.hix@hitachivantarafederal.com

ABSTRACT

Data Dominance has the capacity to transform naval operations and create competitive advantages for U.S. national defense. Hitachi Vantara Federal Chief Technology Officer Gary Hix delves into strategies for achieving faster access to data, and proposes solutions for improving data availability, ensuring that naval personnel have seamless access to vital information when and where it is needed most. Furthermore, the company can highlight the importance of enhancing data quality and fostering trust in the information at hand, underlining the necessary reliability and accuracy of mission-critical data sources. A key aspect to success is the elimination of data siloes, advocating for a cohesive data ecosystem that facilitates collaboration and maximizes the value derived from naval data assets from edge to core to cloud.

BIO: Gary Hix is the chief technology officer for Hitachi Vantara Federal, a wholly owned subsidiary of Hitachi Vantara. With more than a decade of experience as a trusted adviser for federal civilian, defense and intelligence agencies, and 25 years in the IT industry, Hix is known for his ability to solve government IT challenges and for his deep understanding of the information technology mandates facing federal agencies today. Responsible for architecting, implementing and maintaining custom technology solutions for customers, Hix is passionate about storage and data protection helping Hitachi Vantara Federal customers implement meaningful IT outcomes that better business and society.

Prior to joining Hitachi Vantara Federal, Hix served as a program architect at IBM's Cloud Services Division, where he was responsible for a \$500 million cross brand sales strategy. Earlier in his career, he held the role of channel technology executive at Novus Consulting Group, where he oversaw a \$16 million book of business, ongoing presales and delivery of new solutions.

Hix has developed patents for management complexity factors delivering services in an IT environment and tier-based data management storage solution.

AI and Decision Advantage

Terry Halvorsen, Vice President, Federal, IBM • Terry.Halvorsen@ibm.com

ABSTRACT

Terry Halvorsen, former DoN CIO and DoD CIO, now a vice president for federal at IBM, examines AI for government from his unique perspective. He discusses the importance of really understanding how to use AI within government systems to get the best results, focusing on having a good process when implementing AI, such as preparing the data, ensuring auditability and proper use cases. In addition, he considers not just why government agencies need to start looking at this new technology, but also different at ways to buy the technology within the government acquisition system.

BIO: Terry Halvorsen serves as vice president federal client development for IBM's U.S. Federal Market organization. Halvorsen spent more than three decades with the federal government in senior and influential roles, including as the Chief Information Officer (CIO) for the Department of Defense (DoD) and CIO for the Navy. Most recently Halvorsen served for two years as general manager for IBM's U.S. Federal Market technology organization. Before joining IBM, Halvorsen was CIO and executive vice president for IT and mobile for Samsung Electronics. In addition to his civilian government career, Halvorsen also served as an Army intelligence officer during Operation Just Cause in Panama and Operation Desert Storm in Kuwait and Iraq. Halvorsen's work in the government has been recognized twice with a Federal Computer Week Federal 100 award, in 2010 as the senior civilian at the Naval Network Warfare Command on its Cyber Asset Reduction and Security initiative, and in 2016 as DoD CIO on cloud computing and the Joint Regional Security Stacks. He has also received both the Meritorious and the Distinguished Presidential Rank Award for exceptional performance as a senior executive in federal service. Halvorsen holds a bachelor's degree in history from Widener University and a master's degree in educational technology from the University of West Florida. He is a Rotary International Paul Harris Fellow and an Excellence in Government Leadership Fellow.

T-Mobile U.S. and JMA's role in the 5G Transformation of the Department of Defense

Rishi Bhaskar, Senior Vice President and General Manager, Global Verticals & Partnership, JMA Wireless • RBhaskar@jmawireless.com

ABSTRACT

The U.S. government and the Department of Defense (DoD) are investing heavily to bring telecommunications leadership back to the United States. The government has allocated hundreds of millions of dollars to various programs across various agencies, such as the National Telecommunications and Information Administration in the Department of Commerce, to bring 5G to operational scenarios for the DoD and the enterprises. JMA Wireless offers key initiatives and opportunities, and details the role service providers can play to drive success in this digital transformation.

BIO: Rishi Bhaskar is the senior vice president and general manager of global verticals and partnerships for Syracuse, New York-based JMA Wireless. Bhaskar joined the company in November 2021.

Bhaskar is a business leader living at the crossroads of 5G, enterprise, cloud, and Software as a Service (SaaS), responsible for strategic alliances and global verticals. He previously led the Global Hyperscale business at Ericsson, spending six years there in various leadership roles as his realm of responsibility grew. He joined Ericsson to lead all Public Sector business and then expanded to full profit & loss responsibility for Ericsson's Energy and Public Sector verticals. Bhaskar oversaw strategy development, solution development, sales, marketing, delivery, alliances and go-to market execution.

Before joining Ericsson, Bhaskar was responsible for strategy development and execution of Public Safety broadband go-to market plans across Motorola's North America customer base, including state and local government, federal governments and utility customers. Bhaskar was responsible for double digit growth in Motorola's LTE business.

Prior to his tenure at Motorola Solutions, Bhaskar served as an assistant vice president of alliances and business development at Alcatel-Lucent. Bhaskar led all indirect sales and business development for Alcatel-Lucent's non-carrier markets focusing on government, energy and transportation.

Mission Assurance with Zero-Trust Privilege Access Service in the Maritime Environment

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

ABSTRACT

In the maritime environment, speed of mission execution is essential to success. Yet, this speed cannot sacrifice security of operations and put mission assurance at risk. To assure success in the joint maritime environment, the zero-trust capabilities for privileged access that are cloud ready and support a disconnected edge can make the difference for mission success. As part of zero-trust capabilities, privileged access-as-a-service enables rapid and secure access to operational resources while maintaining flexibility to operate disconnected when required. This has the effect to create organizational speed and agility while minimizing risks to operate full speed to the mission.

A zero-trust privileged access service addresses specific challenges found in the joint maritime environment. Some of these challenges include how to do risk reduction for administrative access to systems in the maritime operations environment and how to ensure limited access when operational access to systems is required. To meet these challenges, privileged access controls provide rapid secure access and operational risk reduction to systems access for the maritime joint environment.

The cloud-capable zero-trust privilege access service must provide these capabilities to address these challenges to enable success to meet the mission:

- Provide requestable (no-standing) access to maritime operational systems for privileged access to systems. This requestable access includes non-repudiation using AAL3 MFA for requestors and approvers to the operational systems.
- Secure access to the edge systems for administrative access for different operating systems and application platforms with each of these establishing recording of access and commands for cyber ML/AI threat analytics.
- Provide zero-trust JIT (just in time) access to the operational systems such that user credentials have reduced cyber risk because they do not exist up until the point of mission need.
- Enable cyber mission integration to ICAM for converged platform operations for AAL3 MFA authentication and federated user profiles to support the joint maritime environment.

Swift and secure access to maritime operational systems via zero-trust privileged access service solution is required for the future success of the joint maritime mission. The zero trust capabilities described here outline means to support connected and disconnected environments when needed. Validation of the use case for attendees will include technology demonstration and the use case details mapping the capabilities described to the requirements of the mission.

BIO: Andrew Whelchel (CISSP-ISSAP, ISSEP, CAP, CCSP, CSSLP) started in information security and IAM immediately after graduation from the University of Memphis, supporting identity and access management managing Microsoft Identity for U.S. federal customers. He later transitioned to network infrastructure security and then to consumer identity protection in the role at RSA Security and most recently at Okta and Saviynt. At RSA Security supporting financial services, health care, federal and other customers, he focused on identity risk analytics and integration of identity fraud intelligence for cybercrime prevention. At Okta and in his current role at Saviynt, he focuses on protecting employees and business partner identities for public sector agencies to reduce cyber risk while also accelerating capabilities for cloud transformation. Contributions include work as a contributor on the NIST 1800-3 ABAC (Attribute Based Access Control) standard and speaking events on identity access management and security.

Identity Trends Driving Zero-Trust Programs in the DoD

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

james.imanian@cyberark.com

ABSTRACT

New identities, new environments and new attack methods require a modern adaptive cyber defense to secure the DoD's most valuable resources. The threat landscape continues to dramatically evolve and more than half of CISOs (52%) feel they are not completely prepared for the cyber risks to their mission.

Employees and third-party vendors work from anywhere and from ubiquitous devices. Hybrid and cloud environments are massively complex for an organization to secure, while human and machine identities can be assigned high-risk permissions to become a "privileged user" AND a potential mission threat. Additionally, increased attack vectors, such as AI-fueled ransomware and complex software supply chain attacks, are constantly growing in sophistication.

CyberArk provides insights on:

- Recent hacks effecting government organizations
- Identity threat detection and response
- An identity security approach that delivers measurable cyber risk reduction

BIO: James Imanian is an executive with more than 30 years of experience in aviation and cyberspace operations as well as risk management in these areas. In his role as the first leader of CyberArk's U.S. Federal Technology Office, Imanian is tasked with advising federal customers on the latest threat landscape and how the CyberArk technology platform aligns to meeting their mission requirements.

Imanian brings to CyberArk a valuable "customer first" perspective from his experience as the Navy staff's CIO, CISO for Guidehouse, and deputy CIO for the F-35 Joint Program Office. He is excited to contribute to CyberArk's mission's success as it aligns with his passion for defending our nation against advanced cyber threats.

SOAR/Swimlane—Order from Chaos

David Maphis, Cybersecurity Solutions Architect, Merlin Cyber •

dmaphis@merlincyber.com

ABSTRACT

A brief discussion regarding the challenges, strategies and techniques of getting cybersecurity tools to work together and provide value in the new zero-trust world.

BIO: David Maphis has been in the Information Technology field for more than 30 years. From working on the core of the internet in the 1990s to designing data center processing systems for the public sector, he has always worked at the cutting edge of technology. He has committed himself to helping to bring these technologies to the public. Currently his focus is on cybersecurity tool rationalization, integration and automation. He maintains MerlinCyber's Zero Trust lab to provide demonstrations of zero-trust technologies to customers.

Enable Operational AI and Enhance Mission Readiness With Trusted Data

Rick Taylor, Senior Solutions Engineer, Cloudera Government Solutions, Inc. •

rtaylor@cloudera.com

ABSTRACT

Security and readiness are tightly interconnected, and success on the global stage requires the Navy to be experts in both. Threats will continue to evolve and get more complex, while advancements including GPUs and generative AI lower the bar for adversaries in terms of cost, complexity and time. While status quo was never really the optimal approach, it's now no longer even an option. The Navy can greatly accelerate and enhance operational readiness by capitalizing on commercial best practices vs. building bespoke capabilities.

Learn how a proven, scalable and secure Open Data Lakehouse architecture, supporting generative AI and Open Source Large Language Models, will help the Navy more quickly identify, adapt and respond to evolving threats. Time is of the essence.

BIO: Rick Taylor is a senior solution engineer at Cloudera Government Solutions Inc. (CGSI). Taylor has been supporting the intelligence community and the DoD community since 2004.

Private 5G—Be Your Own Mission IoT Mobile Operator

Andrew Beaty, Chief Network Design Engineer/Chief Marine Corps Networks Design/Engineer, Global Maritime Defense Team, Ciena Government Solutions, Inc. •
abeaty@ciena.com

ABSTRACT

The advent of 5G technology has revolutionized the way we communicate and connect with each other. The communications industry has been at the forefront of this transformation, providing cutting-edge solutions to meet the ever-increasing demand for faster, more reliable and secure wireless networking. Ciena Government Solutions provides innovative packaging of a 5G cell site into an outdoor travel kit that can be quickly moved and deployed remotely to stand up a secure mobile network at the tactical edge. This solution is differentiated using protected N79 spectrum; with a N79 Private 5G network, agencies become their own cellular wireless service provider (SP). As a wireless SP, your agency can enhance its network security by managing “what” and “who” can access the network. Agencies provide personnel with commercially available mobile devices that support the N79 band (with a spectrum policy change) and control user access by issuing subscriber identity modules (SIMs) or digitally embedded SIMs (eSIMs) to authorized users so that only the agency’s mobile devices can access the private network.

Our 5G solution has multiple use cases and is amenable to the tactical edge as well as being able to upgrade in-building local area networks (LANs), distributed antenna systems (DAS), and Wi-Fi networks with a network specifically designed for U.S. government and NATO partners. Fast track your implementation by letting the us build – and even manage – these 5G networks for you using low-cost Commercial Off the Shelf (COTS) technologies and User Equipment (UE).

BIO: Andrew Beaty works at Ciena Government Solutions, Inc. as the chief network design engineer/chief Marine Corps networks design/engineer for Ciena’s Global Maritime Defense Team. Beaty hails from Alpharetta, Georgia, and became a U.S. Marine in 2006. After attending Basic Training at MCRD Paris Island, he served in Washington D.C., Camp Pendleton, Okinawa and the Philippines. After leaving the Marine Corps he received a degree in computer engineering and electrical engineering from the Georgia Institute of Technology.

BMC Helix Edge

Michael Alonso, Senior Solutions Engineer, BMC Software • Michael_Alonso@bmc.com

ABSTRACT

BMC Helix Edge discovers, collects, aggregates and analyzes operational technology (OT) data at the point of inception to enable anomaly detection, predictive maintenance and digital twin simulation in a unified, enterprise-wide view. BMC Helix Edge is deployed at the edge of the network and interacts with physical devices, sensors, actuators, and other Industrial Internet of Things (IIoT) objects to enable:

- Anomaly detection
- Predictive maintenance
- Edge asset inventory
- Edge asset lifecycle management

BIO: Michael Alonso is a senior solutions engineer at BMC Software and has been for the past 23 years. Alonso has covered the Navy during his tenure and was instrumental in the Naval Enterprise Service Desk and SMIT's adoption of BMC Helix ITSM SaaS solution at Navy.

Keeping It Simple—Breaking Down Cloud Misconfigurations

Dilip Bachwani, Chief Technology Officer and Senior Vice President, Enterprise TruRisk Platform, Qualys • dbachwani@qualys.com

ABSTRACT

Monitoring, alerting, immutable configurations are simple strategies that lead to security success. But why are we our own worst enemy?

Qualys offers solutions on:

- The persistent issues of insecure configurations such as IAM, alerting, monitoring logging and encryption
- Misconfigurations that are consistently exploited in the real world
- The why AND how to addressing all of the above

BIO: As the Chief Technology Officer and Senior Vice President of the Enterprise TruRisk Platform, Dilip Bachwani is responsible for leading global product development, data and platform engineering, DevOps, site reliability engineering, cloud operations and customer support across Qualys' broad security product portfolio. Bachwani joined Qualys in 2016 to drive Qualys' own internal digital transformation efforts and has been instrumental in helping scale the technology and organization in support of the company's accelerated product growth and transformation into a unified security platform.

Prior to joining Qualys, Bachwani served in multiple engineering leadership roles at various mid-sized and large organizations to build and deliver complex, scalable, distributed enterprise SaaS products and big data cloud platforms. Bachwani has a bachelor's degree in electronics engineering from the University of Mumbai and a master's degree in computer science from Ball State University.

Securing Sensitive Data in a Connected World

Lee Meadows, Lead Federal Systems Engineer, Sonatype • lmeadows@sonatype.com

ABSTRACT

In an era where open source software components are ubiquitous in public sector applications, the vulnerability of sensitive data to exploitation poses a critical challenge. The growing and ever-evolving threat from adversaries capable of identifying, infiltrating and disrupting federal applications underscores the imperative need for secure development environments. Lee Meadows, Sonatype Air-Gapped Environment (SAGE) Lead Federal Systems Engineer, explores the benefits of air-gapped solutions within federal agencies, delves into best practices to safeguard against threats and discusses how the SAGE can help with secure software development.

Key Takeaways:

1. **Understanding the Landscape:** Navigate the challenges posed by open source software components and the vulnerabilities they introduce to public sector and DoD applications.
2. **Security Imperative:** Recognize the critical importance of secure development environments in the face of a dynamic and evolving threat landscape.
3. **Air-Gapped Solution Benefits:** Explore the benefits of implementing air-gapped solutions to create high quality software—meeting the most stringent security requirements.
4. **SAGE in Action:** Discover how SAGE serves as a game-changer, contributing to secure software development and elevating the overall security posture.

BIO: With more than two decades in IT, Lee Meadows currently serves as the lead federal systems engineer at Sonatype, specializing in supporting DoD and intelligence clients with the SAGE product, allowing them to utilize Sonatype's tools and data in the highest security air-gapped networks.

As a seasoned professional, Meadows previously served as a senior principal engineer for BAE Systems and senior software engineer for Lexis Nexis supporting SIGINT systems in the intelligence community. He has not only demonstrated technical prowess but has also shared insights as a dynamic speaker at industry forums, bringing a unique perspective shaped by hands-on experience. Excited about shaping the narrative of IT innovation in protecting the nation's software supply chain, Meadows continues to contribute to the evolving landscape.

Enhancing Cybersecurity Measures in the Infrastructure Supply Chain

John Loucaides, Senior Vice President, Strategy, Eclipsium •

john.loucaides@eclipsium.com

ABSTRACT

Unveiling the intricate layers of IT assets within our digital infrastructure supply chain, Eclipsium delves into the complexities of cybersecurity. From processors relying on firmware and microcode to diverse interfaces connecting various components, such as graphics cards, storage, network interface cards and remote management interfaces, each element comes with its dependencies and updates. The pervasive software presence encompasses the operating system, device drivers, applications and shared libraries, creating a nested landscape of updatable technologies. Embracing the philosophy of “Turtles all the way down,” this paradigm prompts questions about quantifying supply chain risks and addressing potential backdoors or vulnerabilities, especially if updates become unavailable.

Drawing on his firsthand experience in researching and coordinating the disclosure of significant platform-level vulnerabilities, both within the USG and beyond, John Loucaides unravels technical issues surrounding supply chain cybersecurity. He sheds light on common problems, methods for identification and strategies to preemptively safeguard against unforeseen challenges. Incorporating insights into firmware updates, end-of-life considerations, component vulnerability scanning, integrity checks and sanitization/destruction processes, Loucaides emphasizes the pragmatic use of both open source and commercial tools. While acknowledging the impossibility of achieving perfection, attendees will gain a renewed sense of optimism and actionable solutions amidst the evolving landscape of cybersecurity.

BIO: John Loucaides has extensive history in hardware and firmware threats from experience at Intel and the U.S. government. At Intel, he served as the director of advanced threat research, platform armoring and resiliency, PSIRT, and was a CHIPSEC maintainer. Prior to this, he was technical team lead for specialized platforms for the federal government.

Decoding the Seas: How Observability Enables Better Decisions Faster

Ken Wick, Solutions Engineer, Dynatrace • jenn.deuterman@dynatrace.com

ABSTRACT

In the ever-expanding landscape of information, where volume and variety exponentially increase, sea services face the critical task of deciphering it all at the speed of mission. Observability is a key tool that enables sea services to not only manage but truly comprehend the intricacies of their IT environments.

In this challenging maritime environment, Dynatrace champions the way as the leading observability solution, seamlessly delivering precise answers and intelligent automation at the speed of mission. It provides sea services with the capability to dynamically explore and map dependencies across their entire IT ecosystem, encompassing the vital components of legacy systems and hybrid/multi-cloud services essential for the seamless execution of naval operations.

Within this context, Dynatrace doesn't just serve as an observability solution; it becomes the compass guiding sea services to enable better decisions faster. By navigating the intricate IT landscape, Dynatrace facilitates a quicker understanding of dependencies, ensuring that sea services can make informed decisions swiftly, a critical capability in the dynamic maritime environment.

Securing these intricate systems is paramount to the mission's success, and a zero trust (ZT) architecture becomes the linchpin in achieving this objective. Dynatrace plays a pivotal role in helping sea services realize the goals of a ZT architecture. Through AI-enabled continuous observability, analytics, automation and orchestration—the 6th and 7th pillars of the ZT Defense model—Dynatrace provides robust support in fortifying cyber defenses. Many advanced security threats are initially observed by way of anomalous behavior in day-to-day interactions, both machine to machine and user to application. Dynatrace automatically baselines the environment, and leverages AI to determine issues at machine speed.

Dynatrace showcases how sea services IT leaders are leveraging AI-Driven observability for:

- Full-Stack Observability/Visibility within applications and infrastructure
- Continuous Monitoring, Baselining, and Anomaly Detection
- Automated problem resolution at scale with root cause analysis
- Achieving zero-trust architecture objectives
- User experience monitoring real and synthetic

BIO: Ken Wick is a solutions engineer supporting the Department of Defense and intelligence community. As a solutions engineer, Wick leverages his extensive technical background to provide guidance to his customers regarding Dynatrace capabilities, architectures and best practices for observability and monitoring.

Prior to joining Dynatrace in 2023, Wick dedicated his career in support of the federal government as a technology strategist, engineer and consultant across DoD, IC and civilian organizations. Wick's previous employment includes Microsoft, Booz-Allen & Hamilton, and NetIQ/Attachmate.

Wick is based in the Denver, Colorado, metro area.

A Sailor's Experience from Recruitment to Retirement with Adobe

Michelle Woolford, Navy/USMC/4th Estate Account Director, Adobe •

woolford@adobe.com

ABSTRACT

Within the DoD, it is crucial to recruit the right talent to meet mission-critical objectives. The problem is that the DoD is competing for the same talent as the private sector. The proper digital experiences enhance the ability to attract and retain that talent for the long haul.

Adobe is currently working across the DoD for the following ways to improve digital experiences:

- **Recruitment:** Personalize relevant candidate experiences across online & offline channels to build trust, expand outreach, drive candidate engagement, and enhance brand.
- **Hiring & Onboarding:** Reduce paper and manual HR process with digitized and automated workflows, collaborative work management and signatures for speed-to-mission.
- **Retention:** Engage and develop employees to ensure robust support of the mission, increase job satisfaction and empower employees with personalized intranet and eLearning platforms.
- **Retirement:** Streamline offboarding & maintain a positive post-employment experience by supporting retirees with relevant benefits and continued connection.

BIO: Michelle Woolford represents Adobe as the Navy, Marine Corps and 4th Estate account director. She has spent 8 years navigating the cutting edge of Adobe's software solutions for use cases across recruitment, eLearning, digital forms, zero trust and more.

Woolford can delve into the intricacies of Adobe's software, exploring alignment to the Navy's mission and demonstrating how these tools can revolutionize creative workflows.

How Militaries Can Build, Buy and Deliver Capabilities in a Digital Age

Adam Routh, PhD, Defense and Space Research Lead, and Lauren Dailey, Senior Manager, Deloitte • adrouth@deloitte.com and ldailey@deloitte.com

ABSTRACT

Military power is becoming increasingly digitally enabled. The latest fighter aircraft, tanks and satellites are equal parts network hubs and sensors as they are weapons or reconnaissance capabilities. Software underwrites just about everything a military does, like it underwrites nearly everything else in today's data-driven world. While sophisticated military tools like exquisite fifth-generation fighter aircraft, autonomous drones and advanced cyber capabilities will likely define much of the modern battlefield, success in deterring war and protecting the security of nations will require equally sophisticated abilities to build, buy and deliver those combat resources.

To be sure, the responsiveness of a nation's defense industrial base and a military's ability to procure, deploy and sustain operations in contested environments are key measures of how capable a nation's military is. While many militaries are well-aware of the need for digitally advanced combat and combat-support capabilities, the way these militaries and their departments and ministries of defense build, buy and deliver those resources may be less accustomed to the increasingly digital character of our world. Developing capable, modern militaries requires placing as much emphasis on the value of software, intellectual property and digital systems for supplying and sustaining military operations as it does on weapon systems.

As militaries continue to embrace the role of software, they also should confront how software is disrupting the ways they build, buy and deliver military capabilities. Confronting this disruption can affect everything from partners to processes.

- **Build:** When it comes to software-defined systems, militaries may need to amplify their efforts in looking outside traditional defense industrial base companies to find the solutions they need because critical software is often commercial and produced by a variety of companies, not just a few known prime contractors.
- **Buy:** These changes to the defense industrial base can also affect a military's buying power. When it comes to software or other emerging technologies (e.g., drones, satellite communications, artificial intelligence) shaping combat, militaries may not be the only, or even the largest, consumer. Meaning, often militaries no longer have the buying influence that comes with being a monopsonist.
- **Deliver:** Once new capabilities are built and acquired, a military needs to deliver them. The return of strategic competition and peer adversaries may place new strains on existing military logistics practices and tools. Developed in recent decades around efficient logistics, modern military threats and commercial supply chain fragility require militaries to shift logistics practices from what is most efficient (speed) to what is most effective.

Each new challenge could require militaries to better leverage information of all types. The expansion of the defense industrial base can be helped by knowing which company can produce the right solutions. It also requires knowing how to align incentives so that a company wants to do business with the military. Finally, detecting supply chain or logistics vulnerabilities may require deep insights into suppliers,

Four strategies can help address the disruptions in how militaries build, buy and deliver for the digital age. Consider the following:

1. **Out with the defense industrial base, in with the defense industrial network:** Militaries should broaden their aperture to identify more providers of tools and services, and then align interests with new commercial providers to create new partnerships that could allow militaries to move beyond the familiar industrial base to a more effective industrial network.
2. **Buying for the digital age:** To buy increasingly digital systems, militaries should first assess their buying power in the context of industry incentives and innovations to better understand their place in the market. Militaries should then adjust procurement culture and develop new tools to ensure they can acquire what they need when they need it.
3. **From efficient to effective combat logistics:** Efficient logistics should be replaced with effective logistics, requiring militaries to develop the practices, partnerships, and tools for more resilient supply chain and logistics operations.
4. **From Open Source to Everything-as-a-Source:** Militaries must be able to leverage more information than ever before to create strategic and operational insights, mitigating the risks of producing potentially harmful publicly available information themselves. More than adopting new tools, militaries should consider changing culture and processes too.

BIO: Adam Routh, PhD, is the defense and space research lead for Deloitte's Center for Government Insights and Deloitte's space practice. His research areas include the future of warfare and emerging space activities. His analysis has been featured on ABC News, The John Batchelor Show, and I24 News and published in National Review, The Hill, The National Interest, Space News, The Space Review, Real Clear Defense and Defense News among other outlets.

Prior to Deloitte, Routh worked at the Center for a New American Security, served as a team leader with the U.S. Army's 75th Ranger Regiment. Routh received a PhD in defense studies from King's College London.

Lauren Dailey is a senior manager who specializes in defense innovation and acquisition in Deloitte's Government & Public Services (GPS) Defense, Security and Justice (DS&J) sector. As a recognized expert in Other Transaction Authorities (OTAs), she leads the Non-traditional Innovation & Acquisition team, advises the Government Futures team and supports clients across the DoD in digital transformation. She is currently the program manager for the Army Acquisition Tech Services contract. Prior to Deloitte, she served as the COO of Second Front Systems. In her role, she managed the company's operations, helping the government access

venture-backed technologies developed by the private sector. Dailey also served as the senior director, Pathways, at the Defense Innovation Unit Experimental (DIUx). In this position, she developed a first-of-its-kind rapid acquisition mechanism called the Commercial Solutions Opening (CSO) that leverages OTAs to execute fast, flexible and collaborative deals with top-tier technology companies across the country. As a result of her work, DIUx deployed more than \$180 million to more than 60 companies in areas as diverse as machine learning, autonomy and commercial space. Dailey oversaw the award of the first ever production OTAs in DoD. She set and managed the innovative acquisition strategy for DIUx, which aims to fundamentally change the way the Department of Defense does business.

Prior to her position at DIUx, Dailey served as the special assistant to the principal deputy assistant secretary of the Army (Acquisition, Logistics, and Technology). In that capacity, she advised and supported the principal deputy across the full spectrum of policy and oversight matters concerning Army acquisition—including operations of a 6,000-person organization managing more than 600 Army weapon systems programs and contracts totaling more than \$70 billion. In this capacity, she helped develop and promulgate the Department's acquisition reform proposals included in congressional legislation. She also previously served as the special assistant to the deputy assistant secretary of the Army (Procurement), focusing on oversight of all Army procurement operations and the development of the Army contracting workforce.

Dailey holds a Master of Science in commerce and a Bachelor of Arts, both from the University of Virginia, and holds a Project Management Professional (PMP) certification.

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.

