Tuesday, February 13, 2024

12:10 PM - 12:30 PM

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

Adam Routh, Ph.D.

Defense and Space Research Lead

Deloitte

Lauren Dailey

Senior Manager

Deloitte

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,transporters, and adversary needs and activity. All of this requires militaries to adjust how they take advantage of the information-rich modern world.

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.

Thursday, February 15, 2024

11:10 AM - 11:30 AM

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

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. In this talk, we will discuss the 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 US government and NATO partners. Fast track your implementation by letting the us build – and even manage – theses 5G networks for you using low-cost Commercial Off the Shelf (COTS) technologies and User Equipment (UE).

Tuesday, February 13, 2024

10:40 AM - 11:00 AM

AI and Decision Advantage

Terry Halvorsen

VP, Federal

IBM

Abstract:

Terry Halvorsen, former DON CIO and DoD CIO, now a VP for Federal at IBM, will examine AI for government from his unique perspective. He'll discuss the importance of really understanding how to use AI within government systems in order to get the best results. There will be a focus on having a good process when implementing AI, such as preparing the data, ensuring auditability, and proper use cases. In addition, he will consider not just why government agencies need to start looking at this new technology, but also different ways to buy the technology within the government acquisition system.

Tuesday, February 13, 2024

11:10 AM - 11:30 AM

Decoding the Seas: How Observability Enables Better Decisions Faster

Ken Wick

Solutions Engineer

Dynatrace

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.

In this presentation you will learn 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

Tuesday, February 13, 2024

11:40 AM - 12:00 PM

Integration Solved: Sharing Our Blueprint for Zero Trust Adoption

Herb Kelsey

Project Fort Zero Team Lead & Industry CTO Government

Dell Technologies

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 US 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 towards 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 US 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.

Tuesday, February 13, 2024

12:40 PM - 1:00 PM

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

D.R. Carlson

Senior Director, Segment Marketing for the Americas

Equinix

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.

Tuesday, February 13, 2024

1:10 PM - 1:30 PM

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

Jim Cosby

CTO, Public Sector and Partners

NetApp US Public Sector

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. In this session we’ll discuss 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.

Tuesday, February 13, 2024

1:40 PM - 2:00 PM

Building Highly Resilient Defense Systems Using Agile at Scale

Cynthia Ferreria, Ph.D.

Federal Strategic Advisor

Scaled Agile, Inc.

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. This presentation 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.

The presentation will explain 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.

Tuesday, February 13, 2024

2:10 PM - 2:30 PM

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

Melissa Adams

Director, Archon Division

ID Technologies, LLC

John Dunn

Senior Solutions Architect, Archon Division

ID Technologies, LLC

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 Agency's 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 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 manhours 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. During this technical presentation we will explore the concept of a next generation Access-As-a-Service (A3S) to Classified Data to fill communications gaps in the future.

Tuesday, February 13, 2024

4:30 PM - 4:50 PM

Innovations in Cloud Security for Mission Success

Steve White

Field CISO

Wiz

Abstract:

In January 2023, the Department of the Navy 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. In this session, attendees will learn how to meet the changing needs of the mission and growth of the cloud. Wiz will share 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. Learn how you can build and operate in the cloud with confidence and accelerate your cloud adoption with Wiz's continuous risk and compliance assessment. This presentation is brought to you by Wiz, an approved software provider for the U.S. Navy.

Wednesday, February 14, 2024

9:40 AM - 10:00 AM

Build Winning Sales Plans for the Department of Navy

John Slye

Senior Advisory Research Analyst

Deltek

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.

In this session, we will explore Navy's FY 2024 funding priorities and unpack procurement and contract spending trends including how small businesses stack up. We will also address:

• Navy's top issues and priorities

• Preferred contract vehicles and top contractors

• Opportunity highlights and potential project leads

Wednesday, February 14, 2024

10:10 AM - 10:30 AM

Designing for Sustainability -- Women in Cybersecurity

Teresa Duvall

Faculty Lecturer

ODU School of Cybersecurity

Abstract:

How do we attract and maintain Women into the field of Cybersecurity. How do we address 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." Teresa Duvall – ODU School of Cybersecurity and COVA CCI

Wednesday, February 14, 2024

10:40 AM - 11:00 AM

Data Protection at the Edge

Gina Scinta

Deputy Chief Technology Officer

Thales Trusted Cyber Technologies

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. Attend this session to learn how to apply the same level of security deployed in the core and the cloud to edge environments. We will discuss topics including:

• 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

Wednesday, February 14, 2024

11:10 AM - 11:30 AM

Using Flank Speed Teams to Create Service Requests

Adam Prem

Manager, Solution Consulting

ServiceNow

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 USMC 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.

Wednesday, February 14, 2024

11:40 AM - 12:00 PM

Coalition Information Sharing During Great Power Competition

Russ Smith

Field CTO

ZScaler

Abstract:

Carl von Clauswitz, the 17th century military strategist spoke on the importance of Lines of Communication (LOC) while observing Napolean. Those observations are as relevant today, in all warfighting domains, to include the cyber domain, as it was then. 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 their 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. This session will address zero-trust as the critical enabler to establish Cyber Lines of Communication. 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.

Wednesday, February 14, 2024

12:10 PM - 12:30 PM

Accelerate Mission-Critical Decisions with KPMG Aperture

Phillip Sutton

Director, Optimization and Simulation

KPMG

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 US 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, in order 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 US Navy and Marine Corps can make mission critical decisions, faster.

Wednesday, February 14, 2024

12:40 PM - 1:00 PM

Optimizing Data Security to Support the DOD's JADC2 Strategy

Chris Brown

Public Sector Chief Technology Officer

Immuta

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.

In this talk, you hear from Mr. 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

Wednesday, February 14, 2024

1:10 PM - 1:30 PM

Accelerated Product & Business Innovation with Altair Open Architecture Digital Engineering

Keshav Sundaresh

Global Director, Product Management - Digital Twin and Model-Based Systems Engineering

Altair

Abstract:

Altair will discuss 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.

Wednesday, February 14, 2024

1:40 PM - 2:00 PM

SOAR/Swimlane - Order from Chaos

David Maphis

Cyber Security Solutions Architect

Merlin Cyber

Abstract:

A brief discussion regarding the challenges, strategies and techniques of getting cyber security tools to work together and provide value in the new Zero Trust world.

Wednesday, February 14, 2024

2:10 PM - 2:30 PM

BMC Helix Edge

Michael Alonso

Senior Solutions Engineer

BMC Software

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

Wednesday, February 14, 2024

4:00 PM - 4:20 PM

Accelerated Data Access Impact on Naval Operations

Russel Davis

Chief Operating Officer

Vcinity, Inc.

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 will present 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 will discuss 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 percent of the available bandwidth, regardless of distance.

This session will dive into 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 datacenter and edge solutions that can be deployed to mission end points including shipboard use. Ready to arm your command with the necessary tools and intel for mission success? We hope to see you in this session to learn how Dell and Vcinity can give you real-time, secure connectivity and control of your data—regardless of where and when your mission takes you.

Thursday, February 15, 2024

9:40 AM - 10:00 AM

How to Speed up Acquisition Lifecycles with the #1 CRM

Matthew Jacobs

Executive, Digital Transformation

Salesforce

David Nava

Principal Solution Engineer

Salesforce

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.

In this session you will:

- Hear strategies that leading agencies employ to shorten acquisition lifecycles.

- Learn about solutions that help address common challenges.

- See a live demo of Salesforce Acquisition Relationship Management capabilities for defense organizations.

Thursday, February 15, 2024

10:10 AM - 10:30 AM

Realizing Digital Modernization of Operational Platforms

Michael Griesi

Technical Account Manager, High-Frequency Electromagnetics

Altair

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 US 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. Join this presentation to learn how 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.

Thursday, February 15, 2024

10:40 AM - 11:00 AM

Identity Trends Driving Zero Trust Programs in the DOD

James Imanian

Senior Director, US Federal Technology Office

Cyberark

Abstract:

New identities, new environments and new attack methods require a modern adaptive Cyber Defense to secure 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.

Join our session for insights on:

• Recent hacks effecting government organizations

• Identity threat detection and response

• An identity security approach that delivers measurable cyber risk reduction

Thursday, February 15, 2024

11:40 AM - 12:00 PM

How to Increase Warfighter Efficacy Through Innovations in Edge Computing

Andres Giraldo

Deputy Director, Product Development

SealingTech

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. In this presentation, we aim to advise the Sea Service community on the latest industry innovations that can enhance warfighters' speed, efficacy, and mission success.

We will 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. We will provide a brief overview of SealingTech's edge compute servers and fly-away kits, highlighting how they can reduce the time necessary to achieve mission readiness.

Additionally, our team will share 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 cell phone. 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.