



TechNet Augusta

August 15–18, 2022 | Augusta Marriott at the Convention Center | Augusta, GA

2022 SOLUTIONS SHOWCASE



AFCEA TechNet Augusta Solutions Review

Welcome to TechNet Augusta and the 2022 Solutions Review.

Good cybersecurity is no longer enough, nor is operating in a silos. The U.S. Army is undergoing a massive modernization effort — a once-in-a-generation undertaking — for more unified warfighting toward superiority. All the Army's modernization focus areas are important, particularly Designing and Deploying a Unified Network. Warfighters are at the forefront of a new kind of competition and conflict, and the role they play is absolutely vital to national and global security — today and into the future.

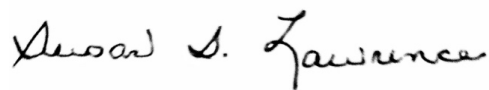
The Army Cyber Center of Excellence sought solutions to address emerging and existing challenges. Dozens of abstracts address the Problem Statements. This Solutions Review Compendium complements the event and helps builds engagement.

The abstracts cover many complex challenges the Army faces not only on land but also in the air and in cyberspace. The Solutions Review offers industry the opportunity to engage and respond to pressing problems. Companies were invited to offer solutions to the following areas:

1. Non-Traditional Waveforms for Information Advantage (IA)
2. The Unified Network - An Operational Requirements Perspective
3. High Capacity Beyond Line of Sight (BLOS) (e.g., Low Earth Orbit (LEO) / Medium Earth Orbit (MEO) [LEO/MEO] / Geostationary Earth Orbit (GEO)) Communications
4. Command, Control, Communications, Computers, Intelligence, Surveillance and reconnaissance/ Electronic Warfare (C4ISR/EW) Modular Open Suite of Standards (CMOSS) Compliant Capability
5. Tactical Radios and Assured Positioning, Navigation, and Timing
6. Tactical Radios and Post-Quantum Cryptography
7. Small Form-Factor Long Range Sensor and/or Antenna
8. Dynamic Spectrum Management
9. Radio Frequency Obscuration
10. Ingesting sensor feeds from multiple enclaves to a central platform

The Army strategy calls for a force “capable of conducting multi-domain operations as part of an integrated Joint Force in a single theater by 2028 and ready to conduct multi-domain operations across an array of scenarios in multiple theaters by 2035.” This includes doctrine, training, materiel, leader development and education, personnel, facilities, policy — and solutions offered by industry partners.

Best wishes,



Lt. Gen. Susan S. Lawrence, USA (Ret.)

President and CEO
AFCEA International

Problem Statements

Army Capabilities Manager Networks & Services

Non-Traditional Waveforms for Information Advantage (IA)

Problem Statement: Army migration of Data Analytics, Machine Learning, and Artificial Intelligence Solutions in Army Enterprise Data Centers (AEDCs) that will allow distribution of information between the enterprise level and the tactical edge. Today the Army is unable to access, share, and interpret the data across warfighting functions required to ensure commanders have the ability to exploit the power of current and emerging data analytics.

Why It's Important: The Army requires Integrated Enterprise Network/Integrated Tactical Network "Big Data" solutions that help achieve a global, standards-based environment with enduring goals of making data visible, accessible, understandable, trusted, interoperable, and secure. The Army continues to operate in increasingly complex, highly dynamic environments. The speed of decision-making will be critical to our ability to fight and win against peer adversaries in congested and contested environments. On the Multi-Domain battlefield, information is an instrument of National Power and data is a strategic asset. Seamless access to Army data at echelon, when readily shared, increases readiness, enhances modernization efforts, and ultimately impacts mission effectiveness across all warfighting functions.

Title: The Unified Network — An Operational Requirements Perspective

Problem Statement: The Army has a requirement to design, operate and maintain a unified network to counter emerging threats, enable new forms of maneuver and allow the commander to fully leverage capabilities across echelons to execute Multi-Domain Operations. As maneuver formations become cloud enabled, the ability to ensure reliability of communications while leveraging common data hosted both on premises at the unit and off premises in a cloud environment, with no loss of continuity, is essential. Essential elements of the Unified Network include:

- Data Centric
- Transport Agnostic
- Planned, managed and secured by Unified Network Operations
- Cloud enabled

Army Capabilities Manager Tactical Radios

High Capacity Beyond Line of Sight (BLOS) (e.g., Low Earth Orbit (LEO) / Medium Earth Orbit (MEO) [LEO/MEO] / Geostationary Earth Orbit (GEO)) Communications

Problem Statement: High Capacity Beyond Line of Sight (BLOS) (e.g., Low Earth Orbit (LEO) / Medium Earth Orbit (MEO) [LEO/MEO] / Geostationary Earth Orbit (GEO)) Communications

Why It's Important: This will provide expeditionary, mobile, beyond line of sight (BLOS) communications with increased bandwidth and low latency in order to provide the Warfighter enhanced transport for Mission Command Systems (to include sensor data).

Command, Control, Communications, Computers, Intelligence, Surveillance and reconnaissance/Electronic Warfare (C4ISR/EW) Modular Open Suite of Standards (CMOSS) Compliant Capability

Problem Statement: The Army is required to execute Mission Command (MC) and Warfighter Functions during Multi-Domain Operations (MDO). As a result, Army vehicles and other platforms are laden with radios, video displays, sensors, electronic warfare tools, antennas, and other vital communication technologies, each with its own power draw and platform footprint. At the core, these C4ISR/EW systems use many of the same building blocks, but they are not shared or distributed between systems (e.g., amplifiers, filters, processors). The C4ISR/EW Modular Open Suite of Standards (CMOSS) was developed to facilitate consolidation of these disparate systems into a common ruggedized chassis, described as the CMOSS Mounted Form Factor (CMFF). The Army requires a materiel solution for the CMFF to facilitate convergence of warfighting capabilities. Solutions should be packaged as a CMOSS compliant chassis system with physical specifications (standards) for capability cards. For capability cards, we would like to have a standard proposed if the company is unable to capture the other capability functions. CMFF solutions should be available for various environments e.g. chassis-concept integration solutions for use on a Stryker, Abrams, or Bradley in order to provide Commanders with the ability to use current warfighting capabilities. The solution should be adaptable for use in the Command Post (CP) environment.

Why It's Important: CMOSS would improve the ease of operation, maintenance, and sustainment of current Warfighting capabilities. CMFF minimizes the need for platform specific integration and allows the fielding of subsequent capabilities (i.e. circuit cards/modules) without the need of any additional cabling or mounts.

Tactical Radios and Assured Positioning, Navigation, and Timing

Problem Statement: Provide methods for Tactical Radio networks to distribute, validate, utilize, refine, and improve trust for Positioning, Navigation, and Timing information.

Why this is important: Potentially provides options to increase both Assured-PNT and network system resiliency by increasing integration of planned capabilities and maximizing A-PNT/Network investments. Potentially informs future requirements.

Tactical Radios and Post-Quantum Cryptography

Problem Statement: Provide methods to modernize CMOSS Modular Form Factor – Capability Card Assemblies for Post-Quantum Cryptography at the chassis level.

Why this is important: Informs Industry and mission partners of desired operational characteristics and potentially provides initial assessment of feasibility. Potentially informs future requirements.
Army Capabilities Manager Electronic Warfare

Small Form-Factor Long Range Sensor and/or Antenna

Problem Statement: The Army requires long-range electronic warfare (EW) sensors and/or antenna built in a small deployable form-factor that can achieve ranges greater than 40 kilometers.

Why this is important: All echelons need to be able to detect, identify, and geolocation electromagnetic spectrum (EMS) signatures at significant distances to provide friendly and adversary situational awareness to enable lethal and non-lethal targeting capabilities in large areas of operations.

Dynamic Spectrum Management

Problem Statement: The Army needs the ability to dynamically adapt and adjust friendly electromagnetic spectrum use and the accompanying signature in order to adjust to and mitigate electromagnetic interference while providing a real time EMS visualization of current EMCON conditions.

Why this is important: Understanding and controlling the Army's electromagnetic signature and mitigating interference is critical to command post survivability.

Radio Frequency Obscuration

Problem Statement: Army command posts need the ability to emulate key assets and the associated locations with the intent to confuse and deceive adversary foreign intelligence collection and targeting cycle. Enemy electromagnetic spectrum detection and location equipment is confused by the obfuscation of actual friendly emissions, locations, and intent.

Why this is important: The ability to obscure and slow down enemy's targeting cycle is critical to command post survivability.

Army Capabilities Manager Cyber

Ingesting sensor feeds from multiple enclaves to a central platform

Problem Statement: What capabilities exist to enable secure data transport between open and closed networks to facilitate the ability to gain situational understanding given sensor data streams originate across multiple enclaves?

Why this is important: In order to gain a comprehensive cyber situational understanding of the battle-field, it is imperative to have a common operating picture that is fed by streaming data from all applicable sensors across multiple enclaves. This understanding of how adversary actions will impact the functionality of friendly networks, allows battle staffs to identify weak links, develop contingencies, and target adversarial capabilities to stop disruptive effects. This process requires that an adequate cross-domain solution exists that allows for a continuous stream of data from identified sensors to the repository in order to identify impacted nodes/links in real time.

Table of Contents

Cybersecurity Threats in Classified Environments	
Mike Maice, Chief Technology Officer, Archon Products	12
Building Toward a Zero-Trust Architecture	
Imran Umar, Zero Trust Director, Booz Allen Hamilton	14
Data Management: A Foundational Pillar for Data Modernization, Data Literacy, Data Sharing and Analytics/AI	
Skip Farmer, Principal Sales Engineer, Collibra	16
Data Mesh and Mission Command	
Anthony Zech, Data and AI COE Director, ECS	18
The Need for Automated Data Security	
Nancy Patel, Vice President of Public Sector, Immuta	20
Phantom	
Tim Solie, SISO and Executive Cyber Consultant. Phase II	22
Modular Detachment Kit	
Ryan Lathan, Senior Lead Engineer, Booz Allen Hamilton	24
Securing the Warfighter Workforce Everywhere	
Michael Slavinsky, Solution Engineer and Michael Rider, Senior Federal Systems Engineer, Menlo Security	26
Dynamic Spectrum Management Using Operational Spectrum Comprehension, Analytics and Response (OSCAR)	
Ryan Tortorich, Ph.D., Senior Research Scientist, Peraton Labs	28
Auto-PACE	
Ross Osborne, Managing Partner, Phase II	29
Centralized Identity Driven Zero Trust	
Josh Brodbent, RVP, Public Sector Solutions Engineering, BeyondTrust	30
Rethinking Sensor Collection Strategies Through Security at Scale Principles	
Mike Sexton, Director, Threat Hunt and DFIR, Booz Allen Hamilton	31

Universal Data Distribution	
Rick Taylor, Senior Solution Engineer, Cloudera Government Solutions, Inc.	33
Stop Lateral Attacks — Micro-Segmentation for DoD Zero-Trust Architecture	
Samuel Bickham, Federal Systems Engineer, Illumio	34
Visibility Fabric Architecture for Directing Data to Central Analytics Platform	
Craig Reynolds, Senior Director, Government Solutions, Keysight Technologies	35
Ingesting Sensor Feeds From Multiple Enclaves to a Central Platform	
Daniel Haas, Director of Growth, Cyber Mission Sector, Peraton	36
How the Army Is Currently Ingesting Sensor Feeds From Multiple Enclaves to a Central Platform	
Steve Liviccori, Client Executive-Army, VMWare	38
Infrastructure as Code to Enable the Unified Network	
Matthew Perry, Senior Director, DevOps Enablement, World Wide Technology	39
Act Globally Defend Locally: Ingesting Sensor Feeds Across MDO	
Kyle Tsao, Army Account Manager, World Wide Technology.....	40
Two Key Requirements of the Unified Network are Visibility and Control	
Mark Parker, VP of Business Development, CodeMettle	41
Zero Trust — Challenges and Opportunities	
Ron Fodor, Operations Manager, HII.....	43
The Unified Network — An Operational Requirements Perspective	
Jason Hogan, Director, Cyber Operations, IOMAXIS.....	44
Criticality of Security Posture Validation Across Multi-Domain Operations	
Craig Reynolds, Senior Director, Government Solutions, Keysight Technologies	45
Voice Network TDM Elimination	
Jon Marcy, President & CEO, Netmaker Communications, LLC	47

Automating the Edge-Based Unified Network	
Rich Gallant, Director of Software Sales, NexTech Solutions	48
Accelerate the Mission with the Unified Network and Zero-Trust Identity Access	
Andrew Whelchel, Senior Solutions Engineer - Federal, Saviynt	49
Muti-Domain Operations with Autonomous Networks	
Eddie Kempe, Solutions Consultant, ServiceNow	51
Predictive Analytics and Auto-remediation of Future Network Issues in a Hybrid Environment	
Brandon Virgin, Chief Technology Officer, SliceUp, Inc.	52
The Orchestration and Automation of Environments as a Service	
Greg Conley, President, Technical Systems Integrators, Inc.	54
Top 5 Ways to Comply with the National Security Memo on Improving Cybersecurity of National Security Systems	
Gina Scinta, Deputy Chief Technology Officer, Thales TCT	56
The Unified Network — An Operational Requirements Perspective	
Rodney Hess, Solution Engineer, Veritas	57
Leveraging the Army Investment in Hybrid Cloud	
Jonathan Hardin, Staff Solution Engineer, VMWare	58
Leveraging Zero Trust and Strong Authentication Across Unified DoD Networks	
Alex Antrim, Senior Solutions Engineer, Yubico, Inc.	59
The Unified Network — An Operational Requirements Perspective	
Patrick Perry, Director of Emerging Technology, Zscaler	61

ABSTRACTS

Cybersecurity Threats in Classified Environments

Mike Maice, Chief Technology Officer, Archon Products • ksamarin@idtec.com

ABSTRACT

As technology advances, cybersecurity breaches in classified military environments have grown exponentially. In this submission, we cover the following topics:

- Mobile device threats in secure work environments
- Building rapid device deployment timelines
- Importance of cybersecurity training for military personnel

In 2019, research found that 24% of all enterprise mobile devices were prone to threats not including out-of-date software. Securing company and organizational data are no longer about physical security; they are about digital protection. In a world where mobile devices are essential in many fields, there is a heightened risk of network vulnerability.

ID Technologies' Archon ZV secure laptop or phone is a CSfC-compliant endpoint built on a Dell laptop or on mobile devices Samsung S20 and the Pixel 5, used for secure access to multi-domains. They provide end users with the ability to securely operate in classified environments with a hardened infrastructure—ensuring military operations are afforded the highest levels of security.

A secure RTOS and custom mobile OS provide military-grade security for the unique requirements of cyber operations. The first-ever turnkey mobility solution meets CSfC program requirements, provides an excellent end user experience and operates efficiently in diverse locations and challenging conditions.

The Archon ZV solution enables government agencies, private sector enterprises and law enforcement organizations to protect data and critical infrastructure against attacks by cybercriminals and cyberterrorists. The scalability, cost-effectiveness and ease of use of this system allow federal customers to deploy new systems directly from the factory in a matter of minutes as opposed to hours or days as required by legacy solutions.

Archon Cloud Fabric, a part of the Archon Suite, is an enterprise gray cloud fabric solution that provides last-mile transport to those critical end-users. Insufficient bandwidth undermines video conferencing and collaboration applications, frustrates users, prevents the adoption of time-sensitive analytics, and can derail “cloud-first” initiatives. When paired, the Archon Suite enables secure cloud connectivity virtually anywhere globally. This enterprise-class solution has been built from the ground up to scale to support any size organization featuring factory configuration and remote certificate renewals.

BIO: As the Chief Technology Officer for Archon Products, Michael Maice is responsible for overseeing and advising on the strategy for Archon product development, as well as evaluating new technologies to be integrated into the Archon product platform. Prior to joining the team, Michael spent 20 years in the U.S. Army as a chief warrant officer and the CTO of the Joint Communication Support Element, as well as his industry experience as the chief innovation officer for a ruggedized hardware manufacturer.

Michael's mission-first perspective brings an understanding of the challenges and missions that our most important customers face daily.

Building Toward a Zero-Trust Architecture

Imran Umar, Zero Trust Director, Booz Allen Hamilton • umar_imran@bah.com

ABSTRACT

Threat actors continue to bypass traditional perimeter security defenses, prompting organizations to shift to a zero-trust mindset where cybersecurity designs focus on protecting an organization's data and access to that data, versus relying on protecting the network from a breach.

This data centric cybersecurity approach requires developing a comprehensive data tagging and labeling strategy where the criticality of an organization's data is fully understood, allowing for policy rules and enforcement to occur as users and systems try to access that data. Two key factors should be used to determine user or system access to that data, including identifying the user/system via an identity, credential and access management (ICAM) solution and examining the device's posture (e.g., antivirus status, patching status, encryption status).

The combination of the identity and device posture allows for granular decision making and policy enforcement for accessing data. Modernization of visibility and analytics for an organization's on-premises, hybrid, and/or multi-cloud environment and its remote workforce is just as important as the implementation of conditional-based access to data and workloads. To keep pace with advancing threats and distributed users and workloads, organizations need a distributed data analytics architecture to process logs as close as possible to the source, while centralizing visibility of relevant events and alerts to analysts and operators.

Booz Allen is helping the DoD, intelligence community, civil and commercial organizations modernize their current brownfield environments to incrementally move toward a zero-trust architecture (ZTA), including assessing their current zero-trust maturity, identifying gaps, developing roadmaps and implementing new solutions. This submission outlines how organizations can incrementally move toward a ZTA by:

1. Moving away from traditional VPN architectures to Secure Access Service Edge (SASE) solutions to enforce conditional-based access for remote users, while optimizing performance (i.e., direct to cloud).
2. Moving away from traditional centralized security stacks to software defined-wide area network (SD-WAN) and customer edge security stacks (CESS) to simplify management, improve performance and apply conditional-based access and micro-segmentation at the application layer for on-premises users.
3. Moving away from centralized data lakes and analytics to distributed data analytics to optimize detection, reduce costs and improve the information provided to defense cyber operations (DCO) analysts in a hybrid, multi-cloud environment.

BIO: Imran Umar is a senior solution architect at Booz Allen Hamilton, serving Booz Allen's defense and civil clients. In this role, he applies expertise to lead service offerings related to cybersecurity and infrastructure engineering. Imran works to advance the adoption and fusion of concepts such as zero trust, machine learning and artificial intelligence to improve cyber resiliency. His experience spans the commercial, civil and the defense sectors, and he has been a trusted advisor for Department of Defense (DoD) customers. For his DoD customers, Imran led a team of cybersecurity engineers to modernize legacy security operations through the adoption of advanced analytics to detect cyber threats and security orchestration, automation and response capabilities to accelerate defenses. He also oversaw a team of engineers who were critical in the development and release of DoD's zero-trust reference architecture. Before joining the firm, Imran led the engineering and design of Verizon's high-speed backbone network and helped automate the configuration and hardening of their critical infrastructure. Imran earned a Master's degree in information and telecommunication systems, with a focus on cybersecurity, from Johns Hopkins University, and a Bachelor's degree from George Mason University.

Data Management: A Foundational Pillar for Data Modernization, Data Literacy, Data Sharing and Analytics/AI

Skip Farmer, Principal Sales Engineer, Collibra • emily.mariea@collibra.com

ABSTRACT

The Department of Defense operates in a highly complex data landscape with zettabytes of data residing in hundreds, if not thousands, of disparate data sources spread across an on-premises, hybrid and multi-cloud environment. Data management is a foundational pillar for overcoming data silos, improving data literacy (understanding of data), fostering data collaboration and enabling data integrity at scale. Moreover, it is critical for implementing the Federal Data Strategy, driving successful cloud migration and data modernization initiatives as well as democratizing the use of high quality and trustworthy data that is easily discoverable, certified for use and fully traceable for analytics and AI use.

In this submission, a domain expert in data management shares best practices for building a comprehensive data management strategy and leveraging data cataloging, data governance, data quality and privacy to enable and support mission-critical use cases. It covers key topics that will aim to address:

- How to break down data silos by capturing, reconciling and managing metadata (data about your data) for intra and cross-agency use.
- Create a unified view of data assets without moving the data.
- Empower data citizens (data producers and consumers of data) to easily discover, understand and collaborate with data.
- Leverage data cataloging to speed analytics, AI governance and AI model building.
- How to implement access to trusted data at scale.
- How to expedite cloud data migration with end-to-end data lineage and impact analysis by prioritizing datasets for migration, understanding impact of migration on upstream and downstream systems, etc.
- Understand the relationship between physical and logical data assets and gain visibility into the lineage (provenance) of data and systems.
- Enable adaptive data governance and analytics including understanding the policy implications against all assets individually and in aggregate.
- Implement comprehensive data privacy policies to prevent unintended release and disclosure of data as well as easily identify, classify and protect sensitive data.
- Leverage granular privilege management (identity, attributes, permissions, etc.) to govern the access to, use of, and disposition of data.

- Enable comprehensive security and data classification, such as creating customizable classifications, record management, etc., in accordance with DoD standards.
- How to scale data quality across large and diverse databases, files, streaming data, data lakes and data warehouses.
- Real-world use cases from across government and commercial enterprises.

BIO: Skip Farmer is a strategic field engineer focused on helping agencies unlock the power of their data. Most of his roughly 28 years in technology has focused on data management solutions within public sector agencies. His unique experience as a chief architect and distinguished engineer has helped him to share a vision on architectural plans, goals and strategies for agencies while helping to navigate through governance and policy requirements.

Data Mesh and Mission Command

Anthony Zech, Data and AI COE Director, ECS • anthony.zech@ecstech.com

ABSTRACT

The requirements of operating in a distributed, global fashion require data solutions that are also distributed and globally discoverable, visible and standards-based. A globally distributed solution requires an approach that is decentralized and flexible while using standard toolsets that enable seamless operations from tactical edge to cloud, across warfighting functions. The requirements of global and warfighting function distribution are why traditional methods of establishing data lakes or warehouses do not work.

Legacy approaches experience further issues when teams or functions need to evolve data to meet operational requirements. Traditional approaches generate rigid data dependencies controlled by a central team that result in accumulated technical debt when organizations attempt to modernize infrastructure elements. This rigidity is a result of the lack of organizational alignment and flexibility centralized teams have. Distributed teams encourage mission-type command approaches and closely align data generation and sharing. Centralized, monolithic approaches create static organizational structures that evolve slowly due to institutional inertia and coordination requirements.

Data meshes and distributed but query-able data stores address the issues of flexibility and responsiveness while preserving capability in communication disadvantaged environments. A data mesh is a distributed approach to data storage and access that shifts data storage and access responsibilities to data producers while preserving centralized metadata repositories on data structure and identity and access management that enable organization-wide data access. This conceptualizes data as a product of information-generating organizations, empowering them to evolve data production while maintaining backward compatibility.

Importantly, this approach decouples data storage and production from potentially unreachable central repositories. This approach can still leverage the advantages of the cloud — in fact, data meshes can more flexibly use cloud resources than legacy approaches. Data meshes can include legacy applications, but are typically built on microservices leveraging Kubernetes and containers. Using this approach for applications allows organizations to decouple applications from infrastructure.

Kubernetes and container infrastructure allow applications to run locally and in the cloud when available. Automatic service discovery and services built on APIs standardized via a data mesh metadata repository enable capability to gracefully and automatically expand and contract as resources become available. A data mesh paired with the decentralized data query capabilities of Elasticsearch allows access to data across the world when available. It also will gracefully degrade when communication pathways become unavailable due to operational or adversarial reasons.

In this model, the data mesh implementation provides documented and discoverable ways to access data securely while Elasticsearch's distributed search capabilities provide the capability to get access to

data from across the world that is transparent to users. A data mesh model with distributed search moves responsibility for providing data to the producers of the data itself. This is a model that is distributed and is more flexible for users while also reflecting organizational structures. Crucially for the military, it is a more survivable model and one that will be far more effective in a contested information space while still preserving global visibility.

BIO: Anthony “Tony” Zech is the Data and AI Community of Excellence director at ECS. Tony is in charge of building a community of practice for Data and AI at ECS to support ECS’ many customers. Previously at ECS, he oversaw cyber analytics and architectures to secure customer environments in defense, government, and the private sector. Before joining ECS, Tony worked as a systems engineer at Forescout Technologies in the Operational Technologies (OT) Business Unit. In this role, he helped organizations secure critical cyber assets at the heart of their missions. Prior to Forescout, Tony worked at Cargill, a major agricultural manufacturer, leading analytics and orchestration for the Cargill Security Operations Center. Tony served as an active duty U.S. Marine officer in intelligence and cybersecurity, deploying in support of Operation Iraqi Freedom, Operation Enduring Freedom and other operations in the Middle East. He continues in this role in the Reserves, currently serving on the Joint Staff as the Reserve Deputy Director for Collection Management (J26). Tony holds a Bachelor of Science in international relations from the U.S. Naval Academy and a Master of Science in business analytics from the University of Minnesota.

The Need for Automated Data Security

Nancy Patel, Vice President of Public Sector, Immuta •

jenn.deuterman@immuta.com

ABSTRACT

As the U.S. Army continues to build toward cloud enterprise architectures and move away from legacy platforms, these systems increasingly require automated data security to be readily available across the force. Policies, regulations, laws, classification rules and other protections must be implemented and enforced effectively to ensure that the right data is going to the right people, with the right access and for the right reasons.

Applying and enforcing unified data standards across the community for industry, intelligence, defense, federal, state and foreign partners is not realistic, but the need for data protection and data handling is an element of common concern. With the move toward an interoperable landscape, mission analysts, data consumers and the warfighter require seamless access to data.

Leveraging a data management platform at the data layer built to accelerate unified network operations and multi-domain operations (MDO) for data access across multiple data sources is essential to how the Department of Defense will automate digital policy management and enable data access at the speed of mission. In addition, it is inevitable the Army will face disrupted, intermittent, and limited (DIL) network connectivity when deployed or on the move. As PEO-C3T works with the Network-Cross Functional Team (N-CFT) to modernize the network, the data will continue to require protection, namely to release and/or redact information at the appropriate level, when the network becomes available. To effectively complete this work, the Army requires data management and analytic tools that create an effective balance between local and distributed computing storage.

Additionally, endpoint security capabilities must reduce reliance on network-based controls and mature identity, access and asset management to reduce insider threat. Immuta understands the complexity of disconnected operations, and the transition from disconnect to connected environments. Immuta can be provisioned down to the tactical network cloud and can grant access to data in the same manner, whether the system is disconnected or connected. The IC, U.S. military, and foreign partners will in many ways continue to maintain standalone information systems, but true digital integration will require a unity of effort for software and hardware within a common digital ecosystem in which information is collaboratively and continuously analyzed without burdening the customer with the management and data exchange between systems.

As the central point for data access, Immuta makes data available, discoverable and secure, and ensures that policies can be created or changed rapidly. Immuta understands and is equipped to empower any Army Cloud Initiative, be it at the AIE (AC2SP), DAIS, the Army's Enterprise Cloud Management Agency (ECMA), and PEO-C3T's Tactical Cloud Infrastructure. Immuta can bridge the data governance community to easily share and protect data between platforms such as ADVANA and JADC2, to include partner coalition networks, ensuring that information is accessible at the tactical edge and in a highly contested environment. With Immuta, the Army can leverage an automated data access governance platform that protects our national security intelligence information and provides the principles, policies, processes, frameworks, tools, metrics, and oversight required to effectively manage data at all levels, from creation to disposition.

BIO: Nancy Patel is the vice president of Public Sector at Immuta, a leader in cloud data access and data security control. She has expertise in engineering, security, ethics and law. With more than two decades of experience in cybersecurity, data analytics and the public sector, Nancy is an industry veteran who also brings extensive experience in software development and systems engineering.

Phantom

Tim Solie, SISO and Executive Cyber Consultant, Phase II • tim.solie@p2sc.net

ABSTRACT

For years, the U.S. Army has focused on developing the perfect waveform. By the time the waveform is ready for use, it is normally five to 10 years behind the threat or commercial capabilities that have out-paced the developmental program. Phantom offers a shift in paradigm in a ready-now solution focused not on development but on providing immediate impact.

A combination of three existing products, Phantom is ready for testing and employment immediately, and delivers a transport environment that is waveform agnostic, lightweight, secure and randomly diverse in path selection providing a true multi-path, hiding in plain sight networking capability. It enables the rapid insertion of commercially developed waveforms (e.g. 3G/LTE/5G, SatCom) reducing costs and getting the capability in the hands of the commander now with visibility and extensibility to all endpoints and connections at every layer of mission command and Multi-Domain Operations.

NOOB is a commercially available product, providing protection through use of a holomorphic blockchain platform leveraging non-Euclidean geometries and quaternions. NOOB is unique in its approach to create and use multiple flexible ledgers, tailorable to mission structures or security requirements. The ledgers define roles allowing or denying the end-user authorization to see/input data, define types of data, establish data functions, tokenize the data and securely transmit the token in unsecure environments. The data in the token is ciphertext protected. The ciphertext is discarded if a single bit is corrupt, protecting the data in motion and at rest. The end recipient will only be able to open the data packets and assemble the message if they possess the base credentials and the unique security credentials. The multiple ledgers support data taxonomies to deliver multi-level classification environments (e.g. coalition). Ridgeback elevates the role of a network defender to network warrior, allowing them to see, block and maneuver against adversaries in the network.

Operating at the Data-Link Layer (Layer 2) and Internet Protocol (Layer 3) of the OSI model, Ridgeback sees all network traffic and characterizes intent based on packet protocols, network intentions and packet function. Ridgeback provides IOT device visibility for everything connected to the network, continuous attack surface scanning and risk assessment, policy enforcement and reporting and automatic policy enforcement. Ridgeback is agentless, with no bandwidth overhead, allowing defenders to see all IOT devices in the environment, clearly identifying blue space, authorized devices, adversarial probing of the network, and identification, investigation and detachment of unwanted devices. Ridgeback network defenders fight in the network by blocking adversary reconnaissance and lateral movement and placing phantoms and decoys to force adversaries to identify their intentions in reconnaissance. Defenders either disconnect or maneuver them to an observation area by meaconing or deception targets. cQure is a HEMP protected path diversifier utilizing a unique bonding algorithm to scramble tokenized sensitive data bit-by-bit across up to 4 seemingly randomized communication pathways (any ethernet-based medium available) transmitted through VPN tunnels virtually eliminating any man-in-the-middle data interceptions or manipulation. Phantom's algorithm then reassembles the data at known, trusted endpoint(s) (e.g. Regional Hub Nodes).

BIO: Col. Tim Solie, USA (Ret.) has supported the C5ISR community for more than 20 years, focused on the development of Army Battle Command Systems, military tactical and enterprise networks, systems integration and capability development for cyberspace, electronic warfare, and has conducted message delivery for information operations. At the field-grade level, Tim has worked in the 101st Airborne Division, USTRANSCOM, USCENTCOM, USCYBERCOM and HQDA G-3/5/7 operating computer networks, developing doctrine and policy, programming funding and developing special capabilities.

Modular Detachment Kit

Ryan Lathan, Senior Lead Engineer, Booz Allen Hamilton • lathan_ryan@bah.com

ABSTRACT

Modular Detachment Kit (MDK) is a hardware, software, vendor agnostic approach to delivering an open architecture, integrated solution that enables decentralized global command and control (C2), securely connecting sensors, decision makers and effects. Leveraging modular, scalable, decentralized capability modules, MDK distributes a common operating picture across the joint, all domain spectrum and establishes remote voice and data communications to positively control any military operation from any location. It provides solutions for distributed sensor fusion, tactical datalink (TDL) and voice communications, supplying an open architecture for data processing and sharing. It also extends early warning coverage and connections to C2ISR systems, minimizing sensor gaps in the common operating picture.

The MDK Communications Module is a deployable, tailorable, self-sufficient radio package containing integrated mission systems and maintenance support capabilities. It is a compact, agile, scalable and deployable transit case, vehicular or fixed facility configurations, while employing local or remote maintenance monitoring. This module provides everything necessary to establish a communications mission system to provide C2 connectivity without requiring external support apparatus or on-site crypto storage.

Using advanced concepts, modular assemblies, and automated monitoring systems, the MDK-F module employs high reliability electronics that drastically reduce the beyond line of sight (BLOS) radio system footprint. The MDK Datalink Module provides a forward deployed, datalink gateway for employment within line of sight of datalink networks. It enables the extension of coverage of individual datalink networks, injection of sensor feeds into the radio frequency datalink network, and management/monitoring of performance of multiple datalink networks from a consolidated location.

As a small add-on capability, the datalink module is intended to be positioned with forward forces to enhance battlespace awareness, while enabling remote datalink transport to connect to higher and lateral theater C2 organizations and forces. As a component of the modular MDK suite, a Maintenance/Management Module can be added to a deployment package as a site's mission systems footprint increases to require a formal maintenance operations center (MOC) or communications focal point (CFP). It provides positional equipment to establish a MOC/CFP and acts as an administrative and maintenance system that centralizes real-time monitoring capabilities for effective management and situational awareness of C2 enterprise systems, remote sensors, and communication sites. This module also provides remote maintenance capabilities to troubleshoot computer or network-based systems, allowing the ability to actively recognize and troubleshoot communications interruptions from a centralized location — a vital benefit for remote sensor sites with fewer personnel assigned, or for locations where resources are secured in separate locations. MDK enables warfighters to manage the operational environment and local assets, as well as collaborate with distributed forces and critical C2 nodes.

BIO: Ryan Lathan has been with Booz Allen for almost 16 years, while simultaneously serving as a lieutenant colonel in the Georgia Air National Guard as the chief of maintenance and director of communications for an Air Force Control and Reporting Center. He is currently the solution architect and lead engineer for Booz Allen's Modular Detachment Kit (MDK), a hardware, software, vendor agnostic approach to delivering an open architecture, Integrated Operations and Training solution that enables decentralized global Battle Management Command and Control (BMC2) operations, securely connecting sensors, decision makers, and shooters. Ryan leads the network architecture design and circuit action coordination for the stand-up of the BC3 facility, including creating necessary circuit action requests and coordinating the procurement, logistics, and installation of required equipment. Routinely performs engineering site surveys in Southwest Asia combat zones to determine installation requirements, assess current technologies, coordinate allied support agencies, and obtain site-specific technical information, including information assurance data. He provided on-site engineering change request approvals for primary command and control, intelligence, surveillance, and reconnaissance facility installation, including designing and managing systems installation, activation, and cutovers. He has coordinated and analyzed all aspects of design, including shelter and power requirements, equipment selection, bandwidth and routing allocations for theater distribution of remote radar sensors, Ethernet networks and radio control systems. He has served as project engineer for major BLOS radio projects providing civil and military en-route ATC services at 15 unmanned sites for the Ministry of Transport and Civil Aviation (Afghanistan) and the State Civil Aviation Department (Turkmenistan). Ryan led a multidisciplinary engineering team, developing country-wide architecture, backbone network, satellite routing schemes, equipment elevations, detailed cabling and wiring diagrams. He has performed site surveys, coordinating land use and supporting site and system integration planning and activation to deliver BLOS radio systems.

Securing the Warfighter Workforce Everywhere

Michael Slavinsky, Solution Engineer and Michael Rider, Senior Federal Systems Engineer, Menlo Security • john.lee@menlosecurity.com

ABSTRACT

The U.S. Army has embarked on a digital transformation at all echelons. Top of mind across Army leadership are emerging cybersecurity challenges faced by adversaries. Digital transformation during the COVID-19 pandemic added to the complexity and threat exposure landscape as the Army workforce transformed with more soldiers, civilians, contractors and vendors operating as a hybrid workforce. This post-pandemic situation presents challenges to Army cyber leadership coupled with major geo-political events. This new normal Army workforce, coupled with stated objectives within the Army's Unified Network goals, implies that Army users, devices, applications and data are moving toward a cloud-focused approach for application access.

Legacy security solutions such as virtual private networks (VPN) coupled with strong authentication have traditionally been leveraged for secure connections between remote users and mission-critical applications. However, the explosion of remote workers has shown the limitations of VPNs, creating major bottlenecks that negatively affected application performance. A key challenge for Army leadership is providing distributed employees and vendors with the unhindered secure access to internal web applications, data and other enterprise resources needed to do their jobs, without expanding the surface area for bad actors to target.

A key solution to this challenge is the Menlo Private Access (MPA) solution, which grants secure access to mission-critical Army applications without requiring VPN clients and 3rd party security agents. The MPA solution leverages Menlo Security's Isolation Core Technology to create a rendered image of an application on an endpoint device directly in the user's browser. This zero-trust network access approach eliminates a bad actor's ability to directly interact with the application through the power of an approved cloud-enable Isolation platform.

Founded in 2013 in Palo Alto, California, Menlo Security has more than 300 customers, including eight of the 10 largest banks in the world. Menlo's Isolation Core has also been successfully deployed via the Defense Information Systems Agency's (DIS's) Cloud Based Internet Isolation (CBII) solution to 2 million DoD employees and contractors. More than 50 million threats are being eliminated per month by CBII.

BIO: Michael Slavinsky is a solution engineer at Menlo Security. As a U.S. Coast Guard veteran, Michael has more than 20 years of experience working as a cybersecurity engineer, along with 7 years as a solution engineer with the U.S. Army. He holds a Bachelor of Science in information systems and several professional and technical certifications, including CISSP, Azure, AWS, CISA, and hands-on experience supporting Army commands.

Michael Rider is the senior federal systems engineer at Menlo Security. He retired from a career with the U.S. Navy and has been working in the federal and defense IT/cybersecurity space for more than 21 years, with most of that time serving as an information systems technician and a cryptologic warfare Officer in the Navy and Navy Reserve for nearly 21 years. Some of his noteworthy military assignments include tours at the National Security Agency, U.S. Strategic Command, White House Communications Agency and Joint Special Operations Command. Prior to joining Menlo Security in October 2021, Mike worked at Tanium for 2 years and Forcepoint/WebSense for 7 years. At both companies, he held roles in sales engineering and technical account management supporting federal customers.

Dynamic Spectrum Management Using Operational Spectrum Comprehension, Analytics and Response (OSCAR)

Ryan Tortorich, Ph.D., Senior Research Scientist, Peraton Labs •

ryan.tortorich@peratonlabs.com

ABSTRACT

As the electromagnetic spectrum becomes more and more critical to Army and adversary operations, it is necessary to better understand and visualize the electromagnetic environment as well as dynamically control friendly emitters under various conditions.

This need is further amplified by the increasing demand for spectrum resources at home and abroad, especially with respect to commercial spectrum auctions such as AWS-3, AMBIT, EMBRS and future shared bands.

Naturally, this introduces the need for intelligent and dynamic spectrum management systems that can easily monitor and quickly adapt to changes in the electromagnetic environment. To address this need, Peraton Labs is developing the Operational Spectrum Comprehension, Analytics and Response (OSCAR) system. OSCAR provides a simple automated dynamic spectrum planning and monitoring capability used to plan spectrum usage, deconflict spectrum requests, and push configurations to radios, while also dynamically reacting to and avoiding interference in real time with a mature RF sensor network.

BIO: Ryan Tortorich is a senior research scientist at Peraton Labs and program manager of the OSCAR program. He has been supporting and managing DoD research and development efforts covering many domains for more than 8 years. His prior work involved development of sensing solutions for hardware security applications, assessment of cyber physical security vulnerabilities and solutions, and analysis of high-power microwave coupling and effects. In his current role, he is focused on developing solutions to better harness the electromagnetic spectrum in congested and contested environments including dynamic spectrum management/access, improved spectrum situational awareness, and support for modern electronic warfare testing and training.

Auto-PACE

Ross Osborne, Managing Partner, Phase II • ross.osborne@p2sc.net

ABSTRACT

The OSCAR system was developed as a solution to current and future needs for efficient spectrum management and utilization, including support for dynamic behavior in congested or contested environments. OSCAR is a flexible web-based application designed to support test and training range activities as well as provide new capabilities for in theater operations. In the planning phase, OSCAR provides an integrated portal for Spectrum Managers to streamline and simplify their daily activities, such as making and approving frequency authorization requests, visualizing the electromagnetic operating environment (EMOE), and refining mission plans. OSCAR works within the current spectrum management workflow, incorporating inputs from external planning and management tools (e.g. SXXI, SPEED, UNO Planner) and standard record forms as its core source of authoritative information.

BIO: Ross Osborne the managing partner of a Virginia-based CVE Verified SDVOSB providing IT/telecommunications/cyber services and solutions and marketing and strategy support to the U.S. government.

Centralized Identity Driven Zero Trust

Josh Brodbent, RVP, Public Sector Solutions Engineering, BeyondTrust •

escanlan@beyondtrust.com

ABSTRACT

Zero trust is about knowing who is doing what within your network and ensuring that in the event of anomalous activity, you can control and limit threats to the network. Applying the granularity of Privileged Access Management (PAM) to achieve zero-trust objectives ensures all access is appropriate, managed and documented, regardless of how the perimeter has been redefined. To stay agile, agencies must leverage zero-trust principles to never trust, always verify, and only allow access when contextual parameters are met. Leveraging PAM and robust identity security strategies enables agencies to move from a network-based approach to a data centric approach to defending systems.

This submission helps to understand:

- Why Privileged Access Management (PAM) is essential to mission critical DoD initiatives
- How to enable IT teams with a centralized management, reporting and analytics console that provides unmatched visibility and control over privileged access activity
- Perspectives on data centric security to defend agency systems and the path to secure modernization using least privilege.

BIO: Josh Brodbent is the RVP of Public Sector Solutions Engineering at Beyond Trust and has more than 20 years in IT experience and has architected identity and privilege access management solutions for more than three million user accounts. He joined BeyondTrust in 2018 as a senior solutions engineer and was quickly selected to lead the team. Prior to BeyondTrust, Josh was a senior solutions architect for Quest Software. He began his career by founding a managed service provider (MSP) at age 12. He held multiple industry certifications by age 14, making him the youngest in the nation to do so. That MSP went on to become successful, and ultimately his launching point into Public Sector architecture and support.

Rethinking Sensor Collection Strategies Through Security at Scale Principles

Mike Sexton, Director, Threat Hunt and DFIR, Booz Allen Hamilton •

saxton_michael@bah.com

ABSTRACT

Organization's data needs are not slowing down. In fact, 71% of organizations today feel their data is growing at a concerning rate. Federal organizations are facing the challenge of defending enterprises at the multi-million endpoint scale and traditional approaches to security fall apart at the size of government. This requires new methods for collecting and detecting threats at the petabyte to exabyte scale.

Organizations, such as the U.S. Army, are not immune to this challenge, but rather more susceptible as the needs of the networks must always match the needs of the warfighter. Multi-cloud environments, micro-services, and observability, logging, and tracing will only add to the Army's need for a broader strategy to providing a common operating picture for situational understanding. As more data is moved to the cloud, especially multiple cloud environments, careful consideration should be given to how data is used and transported. Centralized platforms provide a tremendous opportunity for long-term searches, yet operational teams struggle to gather timely and necessary information due to the volume of data stored.

To meet the needs of both operational security operations teams and commander's requiring real-time information, while also meeting the needs of having long-term storage, moving to a federated data model provides a new approach to gathering real-time data while offering the speed necessary for results in real time. A federal data model exists where data is stored in the individual locations where the data is created, while only bringing back information necessary for the questions being asked. Also called, cross-cluster searching, this approach lets organizations leave data where it is and orchestrate a search spread across all the locations and return results.

The data can still be shipped to a central location; however this approach allows operations analysts to access the data when they need it without delays. In addition to cross-cluster searching, new capabilities exist to analyze, detect and alert on data en-route to a central platform in real time. Following an approach, we refer to as "Bringing the Detection to the Data, Not Data to the Detection," teams can have access to real-time information while data is streaming, vice waiting for data in a central platform to decompress, index and be available for searching. This streaming detection capability can provide situational understanding at the time the event is happening as detection is abstracted from the remainder of the shipping and storage process.

Finally, this federated process allows for multi-enclave searching by only needing to transport the question or query to the other enclaves, rather than attempting to move all data centrally. As data is moved it can't be analyzed in stream, and as described above, stored or alerted on based on Information criticality requirements.

BIO: Mike Saxton is the director of Booz Allen's adversary-informed defense business and leads the federal threat hunt and digital forensics and incident response (DFIR) team. As a cyber expert with more than 20 years of experience, Mike has led and worked on multiple programs across various client spaces focused on improving security operations, incident response and forensics. Mike rejoined Booz Allen in 2019. In his earlier tenure at the firm, he was a deputy program manager for the U.S. Army's Global Security Operations Center. Mike has established and rebuilt multiple cybersecurity programs and developed first-of-a-kind, innovative approaches to rapid detection and response to cyber threats. In addition, he has helped clients establish their cybersecurity strategy and vision. Mike has also served as chief information security officer (CISO) at Georgetown University. Mike holds an M.S. in cybersecurity from the University of Dallas and a B.A. in intelligence studies from American Military University. He is certified as an information security manager (CISM).

Universal Data Distribution

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

rtaylor@cloudera.com

ABSTRACT

The U.S. Army needs a reliable, scalable data transport mechanism to deliver sensor data from origination through all points of consumption — at the edge, on-premise and in the cloud — in a simple, secure, universal and scalable way. The data transport architecture should provide guaranteed delivery, even in contested or denied, disrupted, intermittent or limited bandwidth (DDIL) environments. These requirements can be addressed by a Universal Data Distribution (UDD) architecture. UDD provides a wide range of extensible capabilities ranging from real-time data ingestion, edge processing, transformation and routing through to descriptive, prescriptive and predictive analytics.

UDD provides the capability to connect to any data source anywhere, with any structure, process it, and reliably deliver prioritized sensor data to any destination. Data can be securely shared across on-premises, public cloud, hybrid cloud environments and multiple enclaves. The movement of data across multiple enclaves is facilitated by utilization of any DoD-approved cross domain solution. Once the architecture is set up to ingest sensor data from thousands of endpoints into the UDD, the system can scale up or out based on mission requirements. In fact, one of our customers is ingesting data from more than 100,000 endpoints.

The UDD can act as a neutral, bidirectional, data movement engine between sensors and any of the Army's data platforms. Sensor data from thousands of end points can provide valuable operational insights about threats and vulnerabilities resulting in improved battle space awareness. UDD is designed with ease of use in mind. Data transfer requirements are instantiated using a low code environment to specify and automate reliable data movement. UDD offers a flow-based, low-code development paradigm that provides the best impedance match with how developers design, develop, and test data distribution pipelines. With more than 400 connectors and processors, UDD enables a broad range of data distribution capabilities. Mission specific, custom processors can also be developed as needed. These data distribution flows can be version controlled into a catalog where operators can self-serve deployments to different runtimes.

Cloudera UDD provides secure, universal, hybrid and streaming data distribution enabling the Army to effectively manage data flows and sensor feeds. Cloudera's technology solutions enable organizations to capture, store, analyze and act on any data at massive speed and scale with our Cloudera Data Flow (CDF), Cloudera Data Platform (CDP) and Cloudera Machine Learning (CML) solutions. CDF is the enabling technology for the UDD architecture. Cloudera solutions are built upon proven open source components and open standards with wide industry adoption, they are readily implemented and straightforward to integrate with other platforms. These capabilities and solutions ultimately enable U.S. military and civilian leaders and analysts with the real-time and predictive insights they need to meet their objectives, and support the mission. CDF, CDP and CML provide a comprehensive data ecosystem for security and governance of mission data, as well as a rich toolset for its operational use. Cloudera technologies are accredited in the IC and DoD communities.

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

Stop Lateral Attacks — Micro-Segmentation for DoD Zero-Trust Architecture

Samuel Bickham, Federal Systems Engineer, Illumio • samuel.bickham@illumio.com

ABSTRACT

The DoD/DISA Zero-Trust Reference Architecture (ZTRA) specifically calls out micro-segmentation. Micro-segmentation under the Applications and Workloads Pillar of Zero Trust divides your network into smaller segments, i.e., ring fences, to reduce the attack surface by making these segments cloaked or invisible. In addition to Micro-segmentation, the DoD ZTRA document references the need for “improved visibility control.” Before you can micro-segment, you must see what you want to protect! In this interesting program, you will learn about the three ways Illumio can stop the spread of cyberattacks and malware through zero-trust micro-segmentation.

BIO: Sam Bickham is a commensurate cybersecurity, network engineer, solution architect and web application developer possessing a unique combination of deep-dive technical understanding, creativity and communication skills. He is experienced working with the federal government, software developers and engineers at every level. Sam is focused on delivering high-end problem solving, succinct and versatile communication to stakeholders, C-level executives and end-user training environments. He is fluent in the language of design for LAN/WAN, data-center, virtualization, collaboration and security at all levels. He has a passion achievement of long-term organizational goals, maximizing efficiency and client satisfaction.

Visibility Fabric Architecture for Directing Data to Central Analytics Platform

Craig Reynolds, Senior Director, Government Solutions, Keysight Technologies •

craig.reynolds@keysight.com

ABSTRACT

To combat security threats in the operational environment, cyber operations and cyber protection teams rely on a wide variety of security solutions to protect networks from cyber attacks and traffic anomalies. These tools require a variety of data sources, including logs. But an ongoing critical need is the packet data itself. To enable access of critical packet data to a central platform, the program will need to deploy an intelligent high availability security visibility architecture that supports both inline and out-of-band packet processing across a distributed infrastructure.

Keysight recommends implementing the following best practices to create maximum data capture, data analysis and network survivability during normal operations but more importantly under cyber-attack:

- Create a passive out-of-band visibility architecture to enable high speed packet capture and continuous monitoring.
- Access and direct the data from physical, virtual and cloud environments.
- Aggregate the signals for a unified feed to the data analysis platform, tools and personnel.
- Replicate signals to allow for one-to-many distribution of the data everywhere it is required.
- Tag traffic to identify source origination.
- Perform protocol inspection, SSL decryption and analysis for intelligent filtering and tool optimization.

BIO: Craig Reynolds leads the government sector business for Keysight's Network Applications and Security solutions group, which provides network test and visibility solutions for validating, optimizing and securing networks for government agencies worldwide. Craig has extensive experience in high-tech business strategy, M&A and program/product management. Craig holds a Master of Science degree in technology commercialization from the University of Texas' McCombs School of Business, and a Bachelor of Science in mechanical engineering from Texas A&M University.

Ingesting Sensor Feeds From Multiple Enclaves to a Central Platform

Daniel Haas, Director of Growth, Cyber Mission Sector, Peraton •

gkmety@peraton.com

ABSTRACT

Evolving into the future fighting force, the U.S. Army must use data as the critical component in determining the outcome of military operations. Success in the operating environment hinges on the ability of Army decision-makers to have real-time information available to realize decision dominance. Supporting the need for real-time data means the Army must operate on a common data fabric leveraging speed, security and simplicity at every echelon while understanding the dynamics and complexity of its globally distributed systems. The resulting benefit is an information repository with agility, scalability and integrity while operating in contested operating environments.

Starting with the fundamental question of “what decision(s) is our data supporting?” should drive how the Army organizes to become a data-centered fighting force. A common data fabric reduces data silos from stove-piped legacy systems and enables the integration, management and distribution of trusted and secure data in real time to geographically dispersed users in any location regardless of enclave or classification levels. However, this only solves how to make data visible, accessible, secure and interoperable. Data must be parsed, classified, aggregated, tagged, stored and secured for users to recognize the content, context, and applicability of data and then link it to other data elements for exploitation and meaningful reporting.

Applied in Army cyberspace operations, data ingested from the DODIN-A creates searchable repositories, regardless of the domain, to enable knowledge of incidents for comparison against Army prioritized threats/vulnerabilities with relevant data. High volume feeds are accomplished via API's allowing real-time ingestion and bulk uploads from Army sources, which includes historical data in cloud-based containers or cleansed datasets from isolated networks. Data inputs are fed into and processed in seconds in a natural language processor (NLP) analysis engine providing the performance and scalability required to cover large amounts of data input. Defenders can customize these NLP engine-identified objects of information based on past and future threats. The objects are tagged to create data sets of information for analysts and threat hunters at any skill level. Identified observables automatically move to the attribution layer of the fabric and are enriched using the previously identified NLP objects through organizational, third-party, free, open, paid and customer-provided threat intelligence sources. Next, a secondary NLP engine begins processing the combined event and enriched data. This secondary NLP process is key to being able to increase the accuracy of the enriched threat data. Data used for analytics is stored in a separate graph container. This container holds data for analytics and metrics, both visually and as data for correlation with previous and future events. The service also directs data required for queries into a searchable database.

At the time of the first observation by an analyst or threat hunter, the data fabric has already gathered threat research information, reducing time-intensive research and correlation allowing for optimized operations. A new approach to security against modern and evolving threats requires new thinking. By breaking through the data silos, leveling the playing field and enriching data at machine speed, this new approach transforms organizations' security posture.

BIO: Daniel Haas completed a 30-year career as an officer of U.S. Marine Corps in 2018 with his final assignment as chief of staff for U.S. Marine Corps Forces Cyberspace Command. He transitioned to industry, where he continued working to develop the nation's cyber capabilities by supporting the U.S. Air Force's cyber infrastructure, and pairing the capabilities of Northrop Grumman, and subsequently Peraton, with the mission-critical needs of various DoD and other U.S. government organizations. Dan is currently a director of growth in Peraton's Cyber Mission Sector.

How the Army Is Currently Ingesting Sensor Feeds From Multiple Enclaves to a Central Platform

Steve Liviccori, Client Executive-Army, VMWare • sliviccori@vmware.com

ABSTRACT

The Army needs to be ready to engage and deliver, consistently, regardless of mission or locale. To do so, capability needs to be flexible enough to meet a variety of requirements, without over complicating delivery to the operating forces. The software-defined evolution enables the Army to do just that. Regardless whether the mission takes the Army local, overseas or even to the cloud, software-defined solutions like automating the use of virtual cloud networks create a means to deliver consistent capability that are hardware/transport agnostic. This is no futuristic strategy however, the Army currently owns and operates capabilities on Army-owned, infinitely scalable, multiple hybrid-cloud platforms that automate the ingesting of sensor feeds (ISR/FMV) from multiple enclaves to a central platform since 2016. The Army's ability to ingest sensor data at carrier scale is no different than how all four 5G U.S. carriers are using VMWare's multi cloud networking technologies.

BIO: Steve Liviccori is the client executive focused on supporting the U.S. Army at VMWare, where he has helped to modernize the Army, space, missile, AVN, intelligence and cyber for the past 19 years, the last 9 years at VMWare.

Infrastructure as Code to Enable the Unified Network

Matthew Perry, Senior Director, DevOps Enablement, World Wide Technology •
matthew.perry@wwt.com

ABSTRACT

WWT's outcome-based approach to agile development, DevSecOps and Infrastructure as Code can help transform the way U.S. Army teams build, run and operate services. We focus on capturing iterative feedback to guide decisions, reduce risk, and produce impactful outcomes to ever-changing mission requirements. Along the way, we upskill Army teams to own those solutions long after they've been built.

Our briefings, workshops and assessments can help you make sense of the DevOps landscape. From evaluating your current strategy, accelerating the adoption of DevOps practices, or executing on work identified in your backlog — WWT can streamline your DevOps journey.

- DevOps Briefing
- DevOps Assessment
- DevOps Envisioning Workshop
- Infrastructure Automation Workshop

Policy as Code Engineering and Enablement Infrastructure as Code and automation enable innovation, productivity and help reduce costs when adopted. Leverage our team's experience to enhance and enable your team.

- Infrastructure as Code Accelerator
- Continuous Delivery of Infrastructure Accelerator
- GitOps for Infrastructure Teams
- Infrastructure as a Service
- Strategic Resourcing Services Consulting Services

Our expert consultants can assist your development and operation teams in the guidance and long-term adoption of Agile, DevOps and Cloud at scale.

COMPAY INFORMATION: At WWT, we see DevSecOps as the combination of people, process, and technology to enable continuous delivery of value and security to the Army's mission. Infrastructure as Code is an effective DevSecOps practice for creating and managing infrastructure in a descriptive model by utilizing modern software development techniques. Army Commands will benefit from these practices by gaining a shared knowledge of infrastructure and replicating these systems in a repeatable and maintainable fashion. When combined with Continuous Integration and Continuous Delivery practices, Infrastructure as Code (IaC) allows for changes to be tested, verified, and deployed automatically to streamline the Unified Network.

Act Globally Defend Locally: Ingesting Sensor Feeds Across MDO

Kyle Tsao, Army Account Manager, World Wide Technology • kyle.tsao@wwt.com

ABSTRACT

Developing a comprehensive situational awareness capability requires the ability to connect sensor data from multiple domains across the enterprise. In the DoD, this effort is complicated by decentralized data sources, tactical networks experiencing intermittent communications and, of course, multi-domain networks at various classification levels. While traditional approaches to situational awareness typically involve a data lake approach that requires selective forwarding of data to centralized locations, valuable insights could be lost because data is typically restricted by classification domain and not all the data is accessible.

WWT will show a new approach for situational awareness and data analytics that can provide more comprehensive access to data across the department as well as allow for powerful analytics designed to identify adversaries and provide better awareness. A consistent scalable platform enabled by a cross-domain solution creates the foundation to rapidly ingest data across multiple domains for faster analysis, rapid application updates through the CI/CD pipeline and simplified training and operations requirements. Additionally, emerging concepts like federated machine learning will allow the development and training of powerful AI/ML models without the need to move large amounts of data to a centralized location through congested networks yet maintain security and data protection of data at various classification levels. This statement does a deep dive in to these concepts for data aggregation across networks and discuss this new paradigm. We will include lessons learned from our efforts with a DoD Customer.

COMPANY INFORMATION: At WWT, we see DevSecOps as the combination of people, process, and technology to enable continuous delivery of value and security to the Army's mission. Infrastructure as Code is an effective DevSecOps practice for creating and managing infrastructure in a descriptive model by utilizing modern software development techniques. Army Commands will benefit from these practices by gaining a shared knowledge of infrastructure and replicating these systems in a repeatable and maintainable fashion. When combined with Continuous Integration and Continuous Delivery practices, Infrastructure as Code (IaC) allows for changes to be tested, verified, and deployed automatically to streamline the Unified Network.

Two Key Requirements of the Unified Network are Visibility and Control

Mark Parker, VP of Business Development, CodeMettle •

mark.parker@codemettle.com

ABSTRACT

Two key requirements of the Unified Network are Visibility and Control. The ability to see, understand and control the dynamic network environment to enable decisions and support a data centric fight. In addition, artificial intelligence and machine learning must be incorporated into these elements to enable better and faster decisions.

How CodeMettle approaches the elements of the Unified Network:

- Data centric: Facilitates access to the right data at the right time to enable decisions, analysis, and actions.
- Transport agnostic: Securely uses any available transport mechanism to ensure a resilient and robust ability to deliver data centricity.
- Planned, managed and secured by Unified Network Operations: UNO is the capability that will enable the network from the edge to the enterprise to ensure that signal operations support operations by tailoring bandwidth, spectrum, latency, etc., to enable commanders to see and act at speed.
- Cloud enabled: Control is the key to ensuring today's networks and data can become cloud enabled by using the power and resiliency of the cloud.

The UNO's capability to provide users with the control necessary to shape and decide what network elements and data reside where will ensure continuity of operations through DIL environments, while maximizing the power of the cloud when operations permit. By unifying network operations around transmission, network, and data across echelons, CodeMettle seeks to provide commanders with the necessary visibility and controls to ensure the network resiliency required for Multi-Domain Operations.

Background: CodeMettle was established in 2009 to simplify the management of the most complex networks. Our intuitive software packages consolidate fragmented data, processes and operations into one unified NetOps capability that is secure and scalable from the edge to the enterprise. Our capabilities enable and facilitate effective, efficient and unified network operations that support end-to-end service management and operations to provide situational awareness of localized, fragmented, and inconsistent networks. These secure software products enhance collaboration for better responsiveness and provide the necessary data to the right operators, at the right time, for effective decision-making and problem resolution. An open NetOps framework provides a universal and common approach to achieving end-to-end visibility and vertical and horizontal information flows allow commanders at all echelons access to necessary data in near real time in disconnected, intermittent and latent (DIL) and congested/contested networks. Distributed information management and exchange convergence of tactical, operational and strategic enterprise network information at any echelon with automated machine-to-machine connections that utilize native compliance to

various standards (e.g., VICTORY and MORA, CMOSS, SOSA, ISA, Flexible Terminal/Modem Interface, Network Health API, etc.)

Automation and orchestration reduce cognitive load and execute operational tasks in seconds with repeatability, consistency, and predictability. Unified NetOps picture relevant data and interfaces managed in a single dashboard with context.

BIO: Mark Parker builds long-lasting relationships with military decision-makers and value-add partners while representing the viewpoint of the customer across the company. Mark brings extensive knowledge of Army communications systems from the tactical to enterprise level. Prior to CodeMettle, Mark served in the U.S. Army for 28 years in various leadership positions at all levels. He served as a signal officer in Operations Uphold Democracy, Enduring Freedom, Iraqi Freedom, New Dawn and United Assistance. Mark holds a Bachelor's degree in business administration from Georgia Southern University, a Master's Degree in information technology from the University of Maryland, and a Master's Degree in strategic studies from the U.S. Army War College.

Zero Trust — Challenges and Opportunities

Ron Fodor, Operations Manager, HII • ron.fodor@hii-tds.com

ABSTRACT

The zero-trust framework shatters the archaic perceptions of how to operate securely. It provides freedom and security of movement across networks, not just within the one with a strong security perimeter. While most people believe zero trust is a better security framework than the “walled garden” approach, there are several issues that need to be addressed before zero trust becomes reality. Governance, policy, funding and the technical implementations of a zero-trust architecture require substantial work and investigation before we can realize the benefits and move beyond the paradigm of “trusted” networks to a more resilient and robust security architecture.

BIO: Ron Fodor is an embedded software engineer turned operations manager for one of the largest government contractors. His responsibilities include directing the future of our cyber capabilities.

The Unified Network — An Operational Requirements Perspective

Jason Hogan, Director, Cyber Operations, IOMAXIS • jhogan@iomaxis.com

ABSTRACT

IOMAXIS provides mission-critical solutions to complex infrastructure requirements, including multi-domain information systems, cybersecurity operations, telecommunications infrastructure, cross-domain solutions and managed attribution infrastructure. Delivering mission-critical infrastructure(s) across the globe requires a proven partner capable of securing data and ensuring resiliency with a robust, no-fail information and communication technology system.

To retain information dominance and ensure network survivability, IOMAXIS incorporates artificial intelligence and machine learning (AI/ML) models as combat force multipliers at the tactical edge, including our cloud-native virtualized fully-instrumented 5G core which can cross connect additional non-3GPP network extension(s) to provide the critical capabilities necessary for information dominance in congested and contested data environments. Our scalable test and innovation network (TIN) solution is a distributed, zero-trust network that rapidly conducts live, virtualized and constructive based test and evaluation. Its cloud-native virtualized core was designed as data centric and transport agnostic; providing the ability to integrate emerging technologies such as 5G and beyond wireless networks that align to zero trust principles. This supports the establishment of a standardized, integrated security architecture that sets the foundation for the Unified Network.

TIN integrates a DevSecOps framework; a management lifecycle approach that combines application planning, delivery and monitoring approaches under a single framework. Part of the allure of DevSecOps is that it can speed up many steps in the software development lifecycle (SDLC) and ensure continuous code integrations and updates are handled at the ever-increasing speed of the information environment. This enables the Joint forces to maneuver, counter (through implementation of rapidly fielded capabilities) and prevail in the non-linear conflicts of tomorrow. Additionally, this allows the Joint forces' capabilities to sustain, extend, and expand the reach of both defensive and offensive actions.

BIO: Jason Hogan is the director of cyber operations within IOMAXIS. His tech lead, Kim Cooper, a pioneer in Army cyber operations, brings unparalleled insight to all aspects of MDO operations. Jason recently retired from 22 years of service in the Army and has held multiple leadership positions in military intelligence and cyber from combat mission force team lead to commander for ARCYBER's detachments in support of JFHQ-C (AFCYBER) and JFHQ-C (FLEETCYBER). He is a graduate of the NSA's JOCCP and has a background in offensive cyber operations and expeditionary cyber operations. His focus continues to be enabling the nation's cyber warriors.

Criticality of Security Posture Validation Across Multi-Domain Operations

Craig Reynolds, Senior Director, Government Solutions, Keysight Technologies •
craig.reynolds@keysight.com

ABSTRACT

A typical gap we see in adopting a zero-trust approach for the unified network is the lack of security performance testing, zero-trust architecture validation and breach and attack simulation. Incomplete or lack of validation leaves blind spots when it comes to evolving the unified network, especially as new digital technologies with cloud, edge, and the distributed battlefield in general. For example, for the unified network to provide data centric services in a zero-trust architecture, testing must first be done to ensure that the any user can be properly authenticated to access any data required, and only the data they have permission to access, from any location.

Keysight's solutions provide high fidelity traffic, threat scenarios and intelligence to ensure your zero-trust architecture is protecting the network properly. Keysight's CyPerf is a first instantly scalable and elastic agent-based test solution for zero trust in hybrid, distributed cloud networks. It recreates every aspect of a realistic workload across a variety of physical and cloud environments to deliver insights into end user experience, cybersecurity posture and performance bottlenecks of distributed networks.

Test agents send application and attack traffic simultaneously through hybrid networks, security devices and zero-trust implementations to validate scalability, performance and security efficacy. Keysight Threat Simulator is a SecOps tool that safely performs targeted, configurable, realistic, current attack scenarios focused on the Mitre Att&ck Framework where results can be trended and easily combined with other data points to successful build, refine and evolve a cybersecurity model. This allows the SecOps team to assess the unified networks overall defensive cyber posture and ensure network and endpoint tools are configured properly.

Finally, to combat security threats in the operational environment, cyber operations teams and cyber protection teams rely on a wide variety of security solutions to protect networks from cyberattacks and traffic anomalies. These tools require a variety of data sources including logs, but an ongoing critical need is the packet data itself. To enable access of critical packet data to a central platform, the program will need to deploy an intelligent high availability visibility architecture that supports both inline and out-of-band packet processing across a distributed infrastructure.

Keysight recommends implementing the following best practices to create maximum data capture, data analysis, and network survivability during normal operations but more importantly under cyberattack:

- Create a passive out-of-band visibility architecture to enable high speed packet capture and continuous monitoring.
- Perform protocol inspection, SSL decryption, and analysis for intelligent filtering and tool optimization.
- Utilize an inline data analysis architecture to maximize network uptime and improve security efficiency.
- High availability deployment for security resilience and faster network recovery.

BIO: Craig Reynolds leads the government sector business for Keysight's Network Applications and Security solutions group, which provides network test and visibility solutions for validating, optimizing and securing networks for government agencies worldwide. Craig has extensive experience in high-tech business strategy, M&A and program/product management. Craig holds a Master of Science degree in technology commercialization from the University of Texas' McCombs School of Business, and a Bachelor of Science in mechanical engineering from Texas A&M University.

Voice Network TDM Elimination

Jon Marcy, President & CEO, Netmaker Communications, LLC •

jon.marcy@ucnetmaker.net

ABSTRACT

The DoD CIO published a directive memorandum in the spring of 2021 requiring all PSTN and DSN use of PRI trunking to be decommissioned within the DoD by Oct. 1, 2023. This has been extended to March 1, 2025. In preparation for this, legacy TDM end office solutions are going to have to be replaced with Voice over IP (VoIP) capabilities that will be supported over the DoD Information Network (DODIN).

The Army is considering moving as many as 80% of their unclassified voice users to MS Teams, creating what will be a hybrid VoIP environment. One of the key issues that needs to be addressed before this transition is the requirement to support 9-1-1 calling in compliance with Next Generation 9-1-1 (NG911) standards.

Netmaker Communications has created an architectural framework that provides the necessary strategy to deliver this capability within the Army.

BIO: Jon Marcy has more than 35 years of experience in the telecommunications field working for Contel, GTE, BBN, Verizon and Nortel Networks before starting his own telecommunication company. Today, Netmaker Communications is a multi-million-dollar private company delivering business class telecommunications throughout the mid-Atlantic area of the United States. Jon holds a BSIT degree in telecommunications and is an active member with the SIP Forum and NENA.

Automating the Edge-Based Unified Network

Rich Gallant, Director of Software Sales, NexTech Solutions •

rich@nextechsol.com

ABSTRACT

NexTech Solutions (NTS) sees automation as an emerging requirement in the DoD and military sectors, thanks to rapid prototyping, deployment, validation and sustainment advancements in technology. NTS' MANTLE suite of applications has been developed specifically with our tactical users in mind, with the goal to provide a cloud-like experience at the edge by enabling one of the core components that makes the cloud so valuable — automation.

As networks expand and with complexity growing exponentially, MANTLE focuses on providing an easy-to-use UI that will enable, even in a DDIL environment, our communicators to quickly and efficiently build and configure the infrastructure needed to support edge-based operations. Using the same methodologies that exist within enterprise automation tools and cloud-based applications, MANTLE can create a network and virtual infrastructure in minutes, rather than hours or days, and eliminate human error associated with such tasks. In addition to critical core infrastructure, MANTLE has also been developed to support growing edge capabilities, our Android EUDs, and ATAK devices. Through a similar process, MANTLE can quickly provision and configure Android-based devices in support of our mission partners. Our goal is to bring this capability into the unified network and provide a true cloud-to-edge experience by solving one of the more difficult challenges that exist — automating edge-based infrastructure.

COMPANY INFORMATION: For the last nine years, NexTech Solutions (NTS) has supported the tactical community by bringing in new capabilities and advancing the warfighter's effectiveness at the edge through IT. In recent times, NTS has put a significant focus on addressing a particular gap that exists, making the tactical edge infrastructure easier to use and more cloud-like in support of a true cloud-to-edge model. With that came the creation of our software, MANTLE, which was created to solve a specific problem of automating the creation of edge-based infrastructure in a DDIL (Denied, Disrupted, Intermittent, and Limited) environment. MANTLE and our MANTLE Mobile solution are software applications that are used to automate the provisioning of networking, compute, and EUDs to ensure continuity of a unified network.

Accelerate the Mission with the Unified Network and Zero-Trust Identity Access

Andrew Whelchel, Senior Solutions Engineer - Federal, Saviynt •

andrew.whelchel@saviynt.com

ABSTRACT

The modern operational theater operates in a contested joint environment. In this environment, speed and security of access across the unified network mean the difference in operational success. When fully leveraged, the unified network enables new forms of maneuver across the joint environment. To assure success, rapid access to data across the cloud and edge to the unit enable maximum agility for the commander, leader, and soldier to operate with reliability of communications and engage the data for the multi-domain enabled mission. As a part of this capability, identity least-privilege access to attributes enables rapid and secure access to these resources while minimizing risks to operate at full speed of the mission.

The unified network employed with cloud-enabled identity access addresses key challenges found in accessing data across multi-domain data fabrics from command post to contested edge. Some of these challenges include how to conduct data access validation in a contested environment, how to sustain reliable AI/ML data access in a potentially disconnected environment, and disengaging data access if needed for data disposition. To address these challenges, cloud-enabled identity access and identity security controls combine to provide needed agility and security for data access across multiple domain operations.

Delivering on these challenges requires a cloud-enabled identity access capability set that is accessible from operations planning to edge theater operations. The cloud-enabled identity access for the unified network innovative approach addresses these challenges by enabling the following for the mission:

- Provide data access authorization capability across the unified network from AI/ML and dynamic sources that can drive rapid data access decisions in a joint contested environment. This data access operates with the option of disconnected or connected environments and maintains an identity chain of access audit trail needed for cyber assurance of the mission.
- Provide a zero-trust approach for access by leveraging governance requests and risk reviews of data attributes (ABAC attributes) in the unified network and use as authorization for access to abstracted data and data products for the mission.
- Create secure data access path for operational integration of data analytics across data fabrics (e.g. secured, MPE, et al.) using identity access for common data presentation from the command post to edge field environment (such as CMFF).

Rapid and secure data access via a unified network with cloud-based identity access is necessary for the future success of the execution of information warfare for the joint multi-domain mission. The capabilities described here would leverage all the data security functions and identity controls to provide rapid and agile access to the unified network data to succeed in the joint multi-domain mission.

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

Multi-Domain Operations with Autonomous Networks

Eddie Kempe, Solutions Consultant, ServiceNow • holly.horton@servicenow.com

ABSTRACT

A unified network that is extensible, survivable, reliable and agile is achievable by leveraging a dynamic service catalog that provides resource fulfillment based on available resources (physical, logical, and virtual), end-to-end visibility, machine learning that supports self-healing and dynamic routing based on mission requirements, service level quality, and resource availability. This is also referred to as an Autonomous Network.

Mission packages, services that are required by connecting network resources, can be designed and fulfilled based on performance, cost, availability and security. The ability to provide such service orchestration requires a common network asset data model. This single source of truth can provide network resource attributes (capability, configuration, location) that are utilized in the fulfillment of the specific service in the network. This is also referred to as Intent in Autonomous Networks. This same source of truth, Network Asset Inventory, can be leveraged to provide service model event correlation and root cause analysis that provide real-time visibility into the quality/health, performance, security, vulnerability and utilization in the network.

Workflows providing decision support, humans in the loop, and full automation for action and remediation can be driven by this network intelligence. Bringing the cycle back to Service Orchestration, service affecting conditions can promote actions, humans in the loop or fully automated, to remediate any degradation or loss in network connectivity. Going back to the Service Orchestration, Services can be designed by primary, secondary, and tertiary priorities (configurable policies) that can enable a self-healing, survivable capability. In the commercial telecommunications industry, this approach is often referred to as a fully autonomous network. ServiceNow, along with its technology ecosystem, provides a common fabric that enables deployment, management, and automation required to support the Multi-Domain Operational requirements of the Unified Network.

BIO: Eddie Kempe has more than 20 years of experience in IT with a subject matter expertise in Infrastructure Architecture. He is a U.S. patent holder in the field of quality of service and has presented his research in this field at industry events, including Cisco Live! Eddie holds CCDE #20110003, CCIE #8374 and CISSP certifications. He completed his MBA from Washington University in St. Louis and holds a Bachelor of Science in mathematics from the University of Texas at Dallas.

Predictive Analytics and Auto-remediation of Future Network Issues in a Hybrid Environment

Brandon Virgin, Chief Technology Officer, SliceUp, Inc. •

basia@sliceup.com

ABSTRACT

To operate and maintain continuity and reliability in hybrid, on-premise and multi-cloud environments, a wealth of data must be collected, correlated and understood in real time. Traditional tool sets must be brought to bear, data that is currently collected must be utilized and when necessary, new data sources must be collected. Application monitoring is the form of distributed tracing that provides insight into each segment of a multi-tier environment. This capability is available for microservices, multi-tier and monolithic applications. Each segment of the application is monitored to note deviations from typical performance. Understanding the typical performance of each segment provides the ability to know when things are behaving in an anomalous manner.

However, it is not enough to know when two nodes are communicating with each other in a less performant manner than normal. If possible, the root cause must be identified and the problem resolved automatically. The slow down or failure source can come from many sources. Each must be understood, and monitored, and a fix or warning needs to be generated to reflect their failure. The network that resides between the nodes is an area that must be analyzed, which is where the SliceUp system excels.

Since networks consist of many different layers of redundant equipment, a system to analyze the combination of data from these devices is required. The SliceUp system is designed to easily ingest and analyze multiple data sources to understand the Layer 3 and Layer 2 paths that end nodes take to communicate. Once all the endpoints, in the cloud or on premise, are known and the latency of each of the segments is measured and analyzed, sources of any slowdowns or failures can be quickly isolated and understood from statistical analysis. With that narrowed focus, all relevant metrics (from the relevant devices) such as CPU, memory, disk, fan speed, power usage, interface utilization and many others can be evaluated to show statistically significant variations from their norms, quickly identifying the root cause of the issue. Even this analysis is not complete.

Some issues result from software problems or changes or something else that is not as well defined as a metric. Each of the relevant devices will also generate log files. These log files are varied and can even be from custom applications. A typical approach to understanding these files is to parse them from libraries of parsers or to write regex parsers. This is a rigid method that is expensive to set up and prone to being

out of date. SliceUp uses a dynamic method to parse combined with an ML meta-model to locate any anomalies e.g. root cause issue from the relevant devices or cloud logs. Finally, the networks that connect these devices can often be tunnels within tunnels. SliceUp analyzes routing tables, traceroutes and historical latency to identify any path changes that might be both hidden and the root cause of any issues.

BIO: Brandon Virgin is the CTO of SliceUp, where he leads the efforts to deliver predictive analytics for network performance issues in hybrid and multi-cloud environments. He has more than 20 years of networking industry experience and holds a patent for work on normalizing network performance indexes. He helped architect several of the world's largest networks for companies such as Sprint. He achieved his CCIE in August 2000. Brandon was a founding member of the Analytics Center of Excellence (ACE) at Cisco Systems, using predictive analytics internally at Cisco to enhance the service line of business. Before that, Brandon was the founder and CTO of LogSense, which was recently sold to Sumologic, being the architect of the Application Performance Management solution.

The Orchestration and Automation of Environments as a Service

Greg Conley, President, Technical Systems Integrators, Inc. •

gconley@tsieda.com

ABSTRACT

The need for infrastructure access is exploding. Whether hosted on-premises, in the cloud, or in a hybrid environment, the teams responsible for executing the strategy have the need to access infrastructure, data and application resources quickly. Their goals and expectations depend on it.

TSI customers balance speed and innovation with governance and control through an Environments as a Service approach. End users access pre-built blueprints containing all the resources for the environments they need, while administrators control how the resources in those blueprints are used. Whether to support application development, QA testing, network labs, testing labs, training and exercise ranges, or simply IT operations, TSI customers provide self-service access to the infrastructure and workflows their teams need while enhancing productivity and security. TSI's AgileWARE®, powered by Quali CloudShell, provides self-service access to complex network environments with a mix of physical and virtual components.

As such it provide for a variety of distinct use cases:

- Cyber testing, training, and exercises
- Network development and test
- Network certification
- Training in general

TSI's Environment as a Service approach is a new way to provision and access infrastructure — one that actually fits the needs of the enterprise. By abstracting away complexity and providing self-service access to infrastructure and workflows, TSI customers are equipped to optimize the value of their infrastructure investments while incorporating legacy, present and future assets.

TSI ties its intelligent orchestration and automation framework with a new PCIe based network fabric (less than 200ns server to server latency) which, when combined, offer an incredible ability to recompose high performance compute infrastructure as required for the job at hand while totally eliminating the PCIe to Ethernet translation layer in your network. Automation and speed are key — we have to do things faster and with greater accuracy.

BIO AND COMPANY INFORMATION: Greg Conley is President of TSI. Its environments as a service automation framework combined with physical/virtual resources allow customers to have standardized environments accessed by a single pane of glass for all aspects of lab, range, and infrastructure deployment, consumption, and lifecycle management. This environment is provided to end users through a self-service web portal for execution of multiple workflows and tasks. AgileWARE COTS technology is currently being successfully utilized by DISA, Cisco Systems, Verizon, USPACOM, and many other commercial and DoD entities. Videos and White Papers are available at www.tsieda.com.

Top 5 Ways to Comply with the National Security Memo on Improving Cybersecurity of National Security Systems

Gina Scinta, Deputy Chief Technology Officer, Thales TCT •

mary.shiflett@thalestct.com

ABSTRACT

On January 19, 2022, the White House issued a National Security Memorandum (NSM) to improve the cybersecurity of national security, Department of Defense and intelligence community systems. Under the memorandum, National Security Systems (NSS) must employ network cybersecurity measures equal to or greater than those required of federal civilian networks in Executive Order 14028, which was issued in May 2021. EO 14028 and the NSM are both key initiatives in the Biden administration's effort to protect federal IT systems — cloud-based, on-premises, or hybrid — from the raft of security hacks and ransomware attacks plaguing U.S. infrastructure.

Policy compliance can often be a daunting process, especially when it comes to cybersecurity. This presentation teaches the top 5 ways to comply with the NSM on improving cybersecurity of NSS and outlines 5 key requirements in the NSM to achieve compliance with these requirements by applying best practices for:

1. Cloud Security
2. Zero-Trust Architecture
3. Multifactor Authentication
4. Data-at-Rest and in-Transit Encryption
5. Quantum Resistant Cryptography

BIO: Gina Scinta is Thales TCT's Deputy Chief Technology Officer (CTO). In this role, Gina 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. Gina also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC, and more. Gina has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Gina 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.

The Unified Network — An Operational Requirements Perspective

Rodney Hess, Solution Engineer, Veritas • rodney.hess@veritas.com

ABSTRACT

This discussion focuses on solutions that comprise the industry's most comprehensive, compliant and secure resiliency platform and leveraged a multi-layered and comprehensive strategy structured around the National Institute of Standards and Technology (NIST) methodology identify, protect, detect, respond, and recover. When it comes to an organization's backup ecosystem, agencies should keep in mind the following best practices:

- Learn how to protect IT systems and safeguard data integrity
- Understand what solutions can help monitor and mitigate threats and vulnerabilities
- Explore options for rapid and complete cross-system restoration and develop a plan to optimize your environment for recovery

BIO: Rodney Hess has worked in the information technology industry for more than 30 years. He began his career designing and installing systems for organizations as they implemented local area networks and shared storage. While serving as an engineer for the U.S. Customs Service, he traveled to U.S. border locations installing and maintaining local area networks and mainframe computer terminals. Rodney has continued to support federal government organizations during stints at Dell-EMC, Oracle and now Veritas. He provides the technical framework to assist federal organizations as they develop strategies to efficiently store, manage and protect their most critical asset — data. As an engineer at Veritas, Rodney enables customers to easily protect, visualize and migrate their data to and from the cloud.

Leveraging the Army Investment in Hybrid Cloud

Jonathan Hardin, Staff Solution Engineer, VMWare • jhardin@vmware.com

ABSTRACT

Missions can change. Threats to national security don't wear homing beacons. The Army needs to be ready to engage and deliver, consistently, regardless of mission or locale. To do so, capability needs to be flexible enough to meet a variety of requirements, without over complicating delivery to the operating forces. The software-defined evolution enables the Army to do just that. Regardless of mission takes, the Army local, overseas or even to the cloud, software-defined solutions create a means to deliver consistent capability, hardware/transport agnostic.

Capability (network, security policies, device and device configuration, etc.) is built and delivered in a consistent, pre-validated/secured manner through mechanisms such as infrastructure as code. Mission scenarios can be validated against existing or future capability through concepts such as digital twin.

Mission commanders have these such concepts, as well as artificial intelligence (AI) & machine learning (ML), to make real-time, dynamic (as mission dictates), data driven decisions. Manage and account for network operations for your actual enterprise, regardless of operating domain. This is no futuristic strategy however, the Army currently owns the capabilities to deliver an efficient, modern and cyber effective unified network. Such concepts not only unify network operations, visibility, and management, but the Army and its partners as a whole.

BIO: Jonathan Hardin is the VMWare DoD Staff Solution Architect.

Leveraging Zero Trust and Strong Authentication Across Unified DoD Networks

Alex Antrim, Senior Solutions Engineer, Yubico, Inc. • alex.antrim@yubico.com

ABSTRACT

Defense Department IT professionals have practiced a defense-in-depth strategy for years, relying on a series of firewalls for fundamental security against predicted and known threats. However, in today's post COVID-19 world, the attack surface is changing as network access is moved away from traditional perimeter-based security to cloud-based security, making the former security strategy increasingly irrelevant as a way to protect networks, data and intellectual property.

That's especially true given the proliferation of privileged accounts that give users the ability to access sensitive data and applications, including ubiquitous devices, like smartphones and tablets, that allow access to Department of Defense (DoD) networks. Together, these avenues of access have one vulnerability in common — the username-and-password login process.

What's the single wall that's blocking nation states, rogue actors and cyber criminals from hacking email accounts? The log-in screen, with potentially weak authentication methods that result in a vulnerable cyber defense strategy. Firewalls are no longer effectively serving that purpose. Instead, remote identity proofing, access management, and strong authentication are quickly becoming the new bulwark against cyberattacks. As the DoD moves to securely make data and resources available to service members and employees around the globe, the need for strong authentication that is device agnostic is crucial. Modern phishing-resistant authentication protocols must be employed by end users regardless of the device being used to access data and resources. This is accomplished by leveraging a multi-protocol external hardware authenticator, effectively bridging tried and tested PKI over to FIDO2, while still supporting legacy authentication on air-gapped networks. A unified network requires a strong foundation of identity and authentication to meet zero trust and securely provide data-centric resources to the warfighter.

Strong authentication is required across all of the top use cases in the DoD: bring your own device (BYOD), privileged users and administrators, non-CAC eligible employees and dependents, and shared devices at the tactical edge. Each of these is supported by a multi-protocol, multi-factor, AAL3 hardware authenticator like the YubiKey. This session will describe the value of modern authentication for and how multi-protocol authenticators can support a wide range of use cases for the DoD. You'll also hear how the confluence of world events and federal government directives enhanced the evaluation and piloting of CAC-alternative authenticators.

BIO: Alex Antrim is a senior solutions Engineer at Yubico, Inc., where he assists DoD customers in developing and implementing strong multi-factor authentication solutions to protect their information technology assets and data. He helps customers develop strategies for topics such as identity proofing, identity and credential lifecycle, authentication, authorization and compliance. Alex has more than 15 years of experience in various cybersecurity domains, especially in the areas of secure architectures, PKI and identity in a zero-trust environment. Prior to Yubico, Alex was the lead cyber engineer supporting NAVSEA in the development of the U.S. Navy's next- generation afloat platform network architecture. Alex holds a Certified Information Systems Security Professional (CISSP) certificate and a Masters in cybersecurity and information assurance from National University. He is currently serving as a senior chief petty officer in the U.S. Navy Reserve.

The Unified Network — An Operational Requirements Perspective

Patrick Perry, Director of Emerging Technology, Zscaler • dwarren@zscaler.com

ABSTRACT

The Army has a requirement to design, operate and maintain a unified network to counter emerging threats, enable new forms of maneuver and allow the commander to fully leverage capabilities across echelons to execute Multi-Domain Operations. As maneuver formations become cloud-enabled, the ability to ensure reliability of communications while leveraging common data hosted both on-premises at the unit and off-premises in a cloud environment, with no loss of continuity, is essential. Essential elements of the Unified Network include: To optimize the unified network strategy, the Army must approach domains of operating and securing the network as any other battlefield terrain, and abstract the concepts away from the idea of how it “builds and maintains” the network as a terrain.

Viewing a zero-trust architecture as an overlay of the network terrain is the only way to fully unify all aspects of the network and optimize data flows and security at the same time. A truly cloud native, Secure Service Edge (SSE) solution is designed to do just that.

BIO: As Director of Emerging Technology, Patrick Perry is responsible for the alignment of usable and secure Zscaler capabilities providing dynamic, mission-focused capability with tailored operations to the Department of Defense (DoD) and intelligence communities (IC). Patrick recently retired from the Army as a Signal Corps chief warrant officer 4 after 21+ years of service. Patrick’s experience over the last 15 years has been with the U.S. Special Operations community. Throughout his career, he has served as the Chief Technical Advisor to senior military leaders as well as performed both network and security engineer positions. He specialized in developing innovative and emerging technology solutions to both strategic and tactical missions globally. Patrick holds degrees from the University of Oklahoma and University of Maryland University College, as well as industry certifications including 2 x CISCO Certified Internet Expert (CCIE) and a CISSP. He is married to a career Army Signal Officer currently serving on active duty and they have five children.

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 www.afcea.org

