



TechNet Augusta

August 19–22, 2024 | Augusta Marriott at the Convention Center | Augusta, GA

2024 SOLUTIONS SHOWCASE



AFCEA TechNet Augusta 2024 Solutions Review

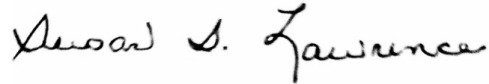
For good reason, the theme of this year's TechNet Augusta event is "transform, align, accelerate for pacing challenges." The U.S. Army continues its journey of massive modernization — a once-in-a-generation undertaking — for more unified warfighting toward superiority and the solutions cited in these pages from our industry partners align with that effort.

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 build 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.

The content is as inspiring to read as it is informative.

Best wishes,

A handwritten signature in black ink that reads "Susan S. Lawrence". The signature is written in a cursive, flowing style.

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

President and CEO
AFCEA International

Problem Statements

Problem Statements from Concepts and Analysis Division (CAD)

Integrated Counter UAS Using Non-Kinetic Technologies

Problem Statement: What cyberspace\EMSO capabilities currently exist or are under development that can deny or defeat the full range of adversary UAS threats to lessen the reliance on costly interceptor projectiles?

Cross-Domain Counter Autonomy

Problem Statement: What cyberspace\EMSO capabilities currently exist or are under development that enable cross-domain counter autonomy efforts to confuse the sensors or poison data, attack via cyber methods, EW, or efforts to cause the human operator to lose trust in the system?

Problem Statements from Army Capability Manager Electromagnetic Warfare (ACM EW)

Electromagnetic Warfare Data Flow in a Degraded Environment

Problem Statement: How does the Army tag, pass, and store EW-relevant data at the tactical edge to ensure availability to all required stakeholders in an EMS-degraded environment?

Adopt Machine Learning (ML) Techniques for Electromagnetic Attack to Optimize Unknown Signals

Problem Statement: How can the Army rapidly adopt ML-enabled EA technique optimization for unknown signals with minimal hardware/platform additions?

Problem Statements from Army Capability Manager Networks and Services (ACM NS)

High Throughput, Low Latency, On the Move, Line of Sight (LOS) and Beyond Line of Sight (BLOS) Communications

Problem Statement: What are you working on for high throughput, low latency, SATCOM as well as on-the-move BLOS and LOS solutions?

Minimize Data Footprint Over Low Bandwidth Connections

Problem Statement: What are you working on to enable dispersed command posts with a low digital signature?

Problem Statements from Army Capability Manager Cyber (ACM CY)

Cyberspace Operations in Multi-Domain Operations

Problem Statement: As the Army focuses its efforts from Strategic to Tactical Cyberspace Operations, how does the Army support the integration of Cyberspace Operations into Multi-Domain Operations? What leading edge industry solutions can support Cyberspace Solutions at the tactical edge?

Data Analytics at the Tactical Edge

Problem Statement: To support the Army of 2030 and beyond, analytical capability of Big Data Platforms, will be needed at the tactical edge. How do advances in AI/ML, reduced compute/storage form factors, and the increase of data from sensors enable commanders by turning data into decisions in a degraded and congested environment?

Problem Statements from Army Capability Manager Tactical Radios (ACM TR)

Tactical Radios and Assured Positioning, Navigation, and Timing

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

Portable Waveforms for Core C2

Problem Statement: Provide methods to achieve core C2, including assured voice (verbal communication at range with globally available spectrum while defeating jamming and direction-finding threats) and limited messaging for digital fires and PLI/COP. Solutions should be available across existing software defined radio capabilities.

Problem Statements from Requirements and Integration Division (RID)

Economy of Force

Problem Statement: How can future technologies eliminate the amount of personnel required to install, operate, and maintain network transport, as well as lessen the number of individuals necessary to manage, monitor, and secure/defend the unified network and data services?

Information Advantage

Problem Statement: How can the Army leverage emerging technologies that allow it to shape relevant actor attitudes, perceptions, and behaviors through target audience engagement, information dimension analysis and assessment, information production and delivery, and the concealment of critical operations and information?

Table of Contents

A Commander’s-Intent-Driven Network to Enable Cyberspace Operations from the Tactical Edge and Beyond	
Andrew D. Stewart, National Security and Government Senior Strategist for Cybersecurity, Cisco Systems, Inc.	10
Utilizing AI to Unlock Data Essential to Mission Success	
Marlin McFate, Federal CTO, Cohesity	11
Mission Edge Data — A Realized Solution for Flightline and Beyond	
Brendan Harris, Director, ISR Solutions, Dell Technologies	13
Cyberspace Operations in Multi-Domain Operations	
Eric Cobb, Principal Solutions Architect, Elastic.....	14
Data Analytics at the Tactical Edge	
Eric Cobb, Principal Solutions Architect, Elastic	16
ExtraHop — Optimizing SATCOM Bandwidth and Spend Through Network Traffic Analysis	
Mike Guyton, Senior Solutions Engineer, ExtraHop.....	17
The Role of NDR in Your Security Strategy	
Mike Guyton, Senior Solutions Engineer, ExtraHop.....	18
Controlling/Displaying Multiple Domains on a Single Display Set	
Gerald Oliver, Product and Business Development Manager, High Sec Labs.....	19
Ensuring Reliable, Resilient Space and Cyber Domains with a DataOps Approach	
Frank Reyes, Software and Infrastructure Capabilities Leader, Maximus	20
Leveraging Cyber Resiliency Solutions to Protect Critical Data and Assets with NetApp	
Jim Cosby, Chief Technology Officer, NetApp	22
The Multi-Domain Cyber Imperative: Building a Core of Security around Mission-Critical Data	
Jim Cosby, Chief Technology Officer, NetApp	23
Electromagnetic Warfare Data Flow in a Degraded Environment	
Jeff Fleming, Technical Cloud Account Executive, Oracle.....	24

Oracle Roving Edge DDIL Analytics	
Jeff Fleming, Technical Cloud Account Executive, Oracle.....	25
Cyberspace Operations in Multi-Domain Operations	
Jim Smid, DoD/Intel Field CTO, Palo Alto Networks	26
A Holistic Approach to Machine Learning for Electronic Warfare	
Aaron Mihalik, Principal Engineer, Parsons.....	27
Mastering the Information Environment to Deliver Information Advantage	
Dr. Dave Dickey, Senior Intelligence Analyst, Peraton	28
Emerging Technologies to Deliver Information Advantage	
Dr. Paul Lieber, Chief Data Scientist, Cyber Mission, Peraton	30
Cyber Decision Advantage	
George Alder, Senior Systems Engineer, Peraton	32
Distributed Edge Cyber Operations	
George Alder, Senior Systems Engineer, Peraton	35
Data Analytics for Decision Dominance at the Edge	
Derek Thurston, Associate Principal Architect, RedHat.....	38
Equipping The Warfighter With Actionable Insights via Intelligent Automation	
Bill Roberts, Deputy Chief Technology Officer, Riverbed	39
Enabling AI/ML at the Tactical Edge	
Jay Meil, Vice President, AI, SAIC.....	40
Speed the Tactical Data Analytics and AI Mission with ZSP Identity Security at the Edge	
Andrew Whelchel, Senior Solutions Engineer, Saviynt.....	42
Transforming the U.S. Army Network Workforce: A Future-Focused Approach to Automation and Efficiency	
Brian Tetreault, Account Executive, ServiceNow	44

Digitally Transform Security Operations for Improved Cyber Defense	
Scott Flynn, Security Operations Advisory Solution Consultant, ServiceNow.....	46
Data Analytics at the Tactical Edge	
Joe Hagan, Staff Solutions Engineer, Splunk.....	48
Data Protection at the Tactical Edge	
Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies	49
Intersection of AI and Security	
Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies	50
Best Practices for Data in Transit Encryption	
Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies	51
Algorithm Evolution	
Thomas Clark, Program Manager, X Technologies	52

Submissions

A Commander's-Intent-Driven Network to Enable Cyberspace Operations from the Tactical Edge and Beyond

Andrew D. Stewart, National Security and Government Senior Strategist for Cybersecurity, Cisco Systems, Inc. • andrewst@cisco.com

ABSTRACT

As the U.S. Army makes the network its top priority to enable operations, commanders must ensure they are prepared and equipped to improve the readiness of their units. Today's modern, leading-edge, commander's intent-driven software-defined network will support the Army's ability to impose its will at the tactical edge.

BIO: Andrew D. Stewart is a national security and government senior strategist for cybersecurity at Cisco Systems, Inc. He works across Cisco's Global Government practice but focuses primarily on national defense and intelligence. He served almost 30 years in the U.S. Navy, where he last served as the chief of cyber operations for Fleet Cyber Command/U.S. TENTH Fleet. He also served as the commanding officer and program manager of the Navy Cyber Warfare Development Group (NCWDG).

Utilizing AI to Unlock Data Essential to Mission Success

Marlin McFate, Federal CTO, Cohesity • marlin.mcfate@cohesity.com

ABSTRACT

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

Key topics include:

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

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

BIO: Before joining Cohesity, Marlin McFate was the federal chief technology officer (CTO) at Riverbed Technologies, where he brought more than 25 years of engineering, leadership and technology experience leading technical initiatives. He is a strategic and supportive voice for customers, partners and team members, and helped ensure successful solution delivery. In his role, he explored emerging technologies, advised on development, and recommended strategies through research and collaboration with business and technology leaders across the company and public sector organizations.

Prior to taking on the role of CTO, McFate was the technical director of the Advanced Technology Group in the Office of the CTO, responsible for being the subject matter and industry expert to the world's largest and most complex customers. As well as at Circadence, as a software engineer, solutions architect and ending as its systems engineering manager leading the engineering teams for commercial and government business units.

An empathetic and engaged leader, McFate refuses to limit himself to the more traditional constructs of the C-suite. As an Army veteran, he is a self-taught technologist and transformed his personal technical curiosity into one of the leading voices in the federal IT community. He makes himself readily available and accessible to colleagues, partners and customers to tackle some of the most difficult challenges in IT, breaking down difficult concepts to empower integrated teams and helping government customers achieve mission success.

Mission Edge Data — A Realized Solution for Flightline and Beyond

Brendan Harris, Director, ISR Solutions, Dell Technologies • Brendan.Harris@Dell.com

ABSTRACT

Air superiority is critical in driving missions' success for the U.S. armed forces through unrelenting force, as well as unparalleled intelligence gathering. The challenges faced with data gathering is how to effectively get the materials off the combat aircraft and processed in a timely manner.

In this session, Dell will discuss how it developed a solution that provides edge processing of F-35 data (via the RAPIDS edge solution). The solution allows for data to be globally accessible by Crowd-Sourced Flight Data enterprise architecture, which is now being cloud-enabled and enhanced for real-time streaming data analytics.

Moreover, it's a platform by which data is optimally managed & governed for AI and big data analytics. The solution provides aircrew and analysts the prompt access to data to support sortie debrief, tailored "shot sheets" and view of cockpit video displays. The data also supports tactical intelligence activities for electronic warfare (EW) signals exploitation and rapid reprogramming efforts under the umbrella of Electromagnetic Battle Management (EMBM). It has transformed the data lifecycle process, shaving hours—even days—over the legacy baseline. Codenamed CHEETAS-SAFARI, the system is being proliferated across many DoD platforms, including B-52, ICBM, Hypersonic missiles and the F-22.

BIO: Brendan Harris, based in McLean, Virginia, is a director of ISR solutions at Dell Technologies, bringing experience from previous roles at Jacobs and the U.S. Air Force. Harris holds a Master of Science in national security strategy from the National War College. With a robust skill set that includes leadership, Air Force, top secret, defense, public speaking and more, Harris contributes valuable insights to the industry.

Cyberspace Operations in Multi-Domain Operations

Eric Cobb, Principal Solutions Architect, Elastic • eric.cobb@elastic.co

ABSTRACT

In the landscape of the modern warfighter, data is a strategic asset. Data drives decisions and decisions drive outcomes. Access to data at the tactical edge for the warfighter and at the strategic level for decision-makers is imperative, and it is this integration of multi-domain operations that is essential for maintaining superiority in modern warfare, where the convergence of cyber and physical domains is increasingly critical.

The Elastic Search AI Platform can ingest, store and analyze petabyte-scale data from virtually any source, and is fully deployable in disrupted, disconnected, intermittent and low-bandwidth (DDIL) environments. At the tactical edge, Elastic's real-time analytics, integrated AI/ML capabilities and scalable architecture enable rapid and informed decision-making, ensuring operational effectiveness and resilience no matter the domain. In the broader multi-domain context, Elastic's cross-cluster search (CCS) capability enables the Army to establish a true global data mesh. By bringing the question to the data and eliminating the need for data backhaul, data remains at the tactical edge while enabling decision-making at higher echelons.

The Army is already standardizing on the Elastic Search AI Platform for its Unified SIEM (U-SIEM) initiatives, and the platform is well-suited to meet the aim of Unified Network Operations (UNO) to reduce operational complexity through machine learning and artificial intelligence. Benefits of the Elastic Search AI Platform at the tactical edge include:

- **Real-Time Data Aggregation and Analysis:** Ingest, search and analyze large volumes of data from various sources quickly.
- **Monitoring and Alerts:** Real-time monitoring with customizable alerts for rapid threat detection and response.
- **Machine Learning:** Support for a wide range of out-of-the-box machine learning models for anomaly detection, outlier detection, natural language processing, pattern analysis, classification and vector search, as well as support for many more 3rd-party machine learning models for more specific use cases.
- **Scalability and Flexibility:** Fully deployable at scale in DDIL environments.
- **Visualization and Dashboards:** Out-of-the-box dashboards and intuitive self-service dashboard creation for real-time data visualization, aiding decision-making.

- **System Integration:** Seamless integration with many existing Army systems, ensuring comprehensive situational awareness.
- **Data Mesh:** Cross-cluster search eliminates the need for data backhaul and brings the question to the data, enabling decision-making across multiple domains.

BIO: Eric Cobb is a principal solutions architect at Elastic, the Search AI company. Prior to joining Elastic, Cobb spent 12 years with the Cybersecurity and Infrastructure Security Agency (CISA, formerly NPPD) supporting programs with the charter to protect critical federal networks and infrastructure. At Elastic, Cobb works closely with Army personnel to solve critical data collection and analysis needs.

Data Analytics at the Tactical Edge

Eric Cobb, Principal Solutions Architect, Elastic • eric.cobb@elastic.co

ABSTRACT

In modern IT environments, data can quickly become overwhelming, reducing the effectiveness of analysts and warfighters as they struggle to identify the critical information for timely, effective analysis and response. The Elastic Search AI Platform provides out-of-the-box ML-backed anomaly detection, pattern analysis, outlier detection and change point detection capabilities to surface critical anomalies in an otherwise insurmountable mountain of data.

Elastic also provides ML capabilities for classification (i.e. tagging), natural language processing, multilingual semantic search, vector search and many more solutions. In addition to advanced AI/ML capabilities, the Elastic Search AI Platform provides an easy and effective means of creating data visualizations through a drag-and-drop user interface, shortening the time to insights. Utilizing AI/ML and visualizations to process data reduces the time necessary for critical data understanding, but data is not useful if it cannot be effectively collected and accessed in all environmental conditions; Elastic's platform will run on virtually any compute/storage form factor, and fully supports deployment in DDIL environments.

BIO: Eric Cobb is a principal solutions architect at Elastic, the Search AI company. Prior to joining Elastic, Cobb spent 12 years with the Cybersecurity and Infrastructure Security Agency (CISA, formerly NPPD) supporting programs with the charter to protect critical federal networks and infrastructure. At Elastic, Cobb works closely with Army personnel to solve critical data collection and analysis needs.

ExtraHop — Optimizing SATCOM Bandwidth and Spend Through Network Traffic Analysis

Mike Guyton, Senior Solutions Engineer, ExtraHop • mikeg@extrahop.com

ABSTRACT

The intent of this abstract is to help communicate the mission value of network packet analysis in optimizing limited SATCOM bandwidth and spend. This abstract highlights the following:

- How the U.S. Army can optimize existing bandwidth through network visibility
- How the U.S. Army can lower SATCOM costs by using network visibility to right size bandwidth

BIO: Mike Guyton spent 14 years active duty Air Force working on securing mission networks and data. Today he supports ExtraHop's DoD and IC customers with their Network Detection Response and Network Performance Management challenges.

The Role of NDR in Your Security Strategy

Mike Guyton, Senior Solutions Engineer, ExtraHop • mikeg@extrahop.com

ABSTRACT

ExtraHop will cover the top five capabilities that help organizations gain the full value of NDR and help them expand current SIEM/SOAR and EDR solutions into a true XDR approach. Benefits of an XDR approach will address the personnel challenges faced by the U.S. Army Cyber today. When done right, XDR will improve cyber defense operations and lessen the number of individuals necessary to manage, monitor and secure/defend the unified network and data services.

BIO: Mike Guyton spent 14 years active duty Air Force working on securing mission networks and data. Today he supports ExtraHop's DoD and IC customers with their Network Detection Response and Network Performance Management challenges.

Controlling/Displaying Multiple Domains on a Single Display Set

Gerald Oliver, Product and Business Development Manager, High Sec Labs •

gerald.oliver@highseclabs.com

ABSTRACT

Today's battlespace leverages multiple sensors, intelligence systems and unclassified news feeds to gain the best possible understanding of the environment in which U.S. warfighters will be engaging the enemy. The KVM Combiner allows feeds to be combined, scaled and displayed on single or dual monitors. Up to eight feeds can be brought into a single KVM Combiner and the operator controls how they are displayed to meet the current operational situation (a single source displayed or up to eight systems displayed simultaneously). Bringing multiple systems together on a single display allows the Operator to compare different feeds and gain the best possible situational awareness of the battlespace.

With the KVM Combiner, a single set of peripherals (mouse, keyboard, display) controls up to eight systems of different security domains. The KVM Combiner displays systems simultaneously while enforcing security isolation between the systems. Complex and dedicated hardware is integrated into KVM Combiner to prevent data leaks between domains. Having this ability in a tactical environment reduces the need for multiple displays, keyboards and control devices, thus reducing the setup time and weight of equipment being transported. Within a tactical vehicle, the KVM Combiner allows the operator to display multiple feeds simultaneously on a single screen, saving valuable space in an already cramped environment.

The KVM Combiner can receive feeds in multiple formats and is offered in commercial and military rugged variants. The rugged variants are deployed for vehicle operation and forward operation centers. This functionality also finds a home in the intelligence community. Having multiple feeds displayed side-by-side allows for change analysis, battle damage assessment and comparing ELINT with overhead photo collection assets, among other tasks. The KVM Combiner allows virtually unlimited display possibilities over a multitude of systems, while enforcing data isolation across different security domains.

BIO: Gerald Oliver is a retired naval intelligence officer with an engineering background. Upon transitioning from the military, Oliver went to work for a military contractor focused on tactical computing systems for Army platforms on the move. Recently Oliver transitioned to High Sec Labs to oversee its manufacturing facility, which designs, certifies and builds a multitude of cybersecurity hardware. He maintains several certifications, including his CISSP and PMP.

Ensuring Reliable, Resilient Space and Cyber Domains with a DataOps Approach

Frank Reyes, Software and Infrastructure Capabilities Leader, Maximus •

efrainreyes@maximus.com

ABSTRACT

The Army is coming off the heels of 25+ years of counterinsurgency operations where soldiers needed to extend communications platforms to the tactical edge—easy to do in uncontested environments. Now, in a time of competition and potentially preparing for conflict with an advanced adversary, the requirements and capabilities have changed significantly.

We can no longer assume we have communication and information dominance. The Army is now competing for information dominance across networks while operating on land, sea, air, cyber and space. Technology has created interdependent relationships between domains, so access or lack of access in one domain can have effects in others. For example, mission assurance across land, sea and air demands reliable, resilient data access from the space and cyber domains.

In the same way airborne and paratrooper forces rely on parachute riggers to pack, maintain and ensure their reliable deployment, operators and decision-makers need to know they can rely on the space and cyber domains for successful multidomain operations.

Parachute riggers have a motto — “Be sure, always” — illustrating the criticality of their role: if a parachute fails, it means their fellow soldier’s life is at risk. The same principle applies to the space and cyber domains: for successful integration of cyberspace operations into multidomain operations, the Army needs data interoperability, network intelligent systems and commercial failover mechanisms to be sure, always. Network-intelligent systems are critical for multidomain operations so data-driven applications can understand what’s happening in the environment and respond to maintain mission operations. Designing network-intelligent systems requires a strong data management and governance foundation to synthesize and standardize unstructured data, manage data across disparate systems, and provide real-time visibility into mission-critical data for data-driven decision-making.

Similarly, commercial failover for space and cyber technologies requires end-to-end workflow management and significant technical expertise to ensure tools and solutions are developed, deployed, and maximized for reliability and resiliency.

As a large systems integrator with JAB-authorized platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS), and software-as-a-service (SaaS) solutions, Maximus brings decades of data management experience across the federal government to meet Army needs for data interoperability, network-intelligent systems and commercial failover in the space and cyber domains. By integrating advanced technologies

with a DataOps approach to data pipelines, Maximus continuously improves data quality throughout the data lifecycle for accurate, consistent and reliable data across domains.

Maximus' operations approach to managing data, software, and infrastructure solutions is critical for ensuring operators and decision-makers have access to the right data at the right time across the space and cyber domains, thus ensuring a reliable, resilient cyberspace for multidomain operations.

BIO: As a business leader and technologist, Frank Reyes works closely with federal government customers to understand their challenges and deliver appropriate solutions. Reyes oversees Maximus's development of secure hybrid cloud solutions and cloud native applications to ensure that agencies provide their services in a modern and secure way.

Reyes helps customers realize the value of their cloud investment by envisioning the landscape before migration and during implementation. His ability to develop the cloud roadmap, architect and implement solutions, and accelerate positive outcomes has served agencies, including the Department of Homeland Security and Department of Defense.

Reyes' skill as a business leader is reflected in his ability to build teams, communicate the value of technical concepts, and connect with stakeholders. His programs have grown because of his technical and interpersonal capabilities.

Previously at Amazon Web Services, Reyes supported public sector technology transformation programs focused on secure computing and accelerated cloud adoption. Other positions included serving as a technology policy advisor to the Committee on Homeland Security in the U.S. House of Representatives and as a civilian employee in the Department of the Navy working on combat system software.

Reyes attended Florida International University, where he studied industrial systems engineering, and holds a graduate certification from Massachusetts Institute of Technology in cybersecurity policy. He is a member of ACT-IAC and serves at the Policy Lead for the Cybersecurity Supply Chain Risk Management Acquisition Working Group, as well as an active member in the FBI's InfraGuard. Reyes holds technical certifications for SAFe® 5 Agilist, AWS Well-Architected Proficient, AWS Partner - Technical, AWS ML for Business and ML Production Operations, AWS Solutions Architect - Associate, AWS Cloud Practitioner.

Leveraging Cyber Resiliency Solutions to Protect Critical Data and Assets with NetApp

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

ABSTRACT

With the reality of today's cyber threat landscape, a data-centric, layered defense approach using a zero-trust security architecture around critical data is key. In this session, learn how NetApp's built-in security capabilities, including cyber vaults and autonomous AI, can be leveraged as an effective cyber resiliency strategy against cyber forces and other threats.

BIO: Jim Cosby is a chief technology officer (CTO) at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on data management, storage and security for more than 20 years, including on-premises, hybrid and multi-cloud data fabric technologies, which include multi-domain operations and foreign mission environments. Cosby has a passion for teaming with agencies, customers, partners and colleagues to drive winning outcomes, and he thrives on helping customers architect optimal, cost-efficient and secure data management solutions using NetApp technology.

The Multi-Domain Cyber Imperative: Building a Core of Security around Mission-Critical Data

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

ABSTRACT

With today's multi-domain data sharing requirements and cyber threat landscape, a data-centric layered defense approach using a zero-trust security architecture around critical data is key. According to Randy Resnick, director, Zero Trust Portfolio Management Office, Office of the DoD CIO: "It is a new way, it is the only way, that we can protect our data from adversaries going forward."

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

BIO: Jim Cosby is a chief technology officer (CTO) at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on data management, storage and security for more than 20 years, including on-premises, hybrid and multi-cloud data fabric technologies, which include multi-domain operations and foreign mission environments. Cosby has a passion for teaming with agencies, customers, partners and colleagues to drive winning outcomes, and he thrives on helping customers architect optimal, cost-efficient and secure data management solutions using NetApp technology.

Electromagnetic Warfare Data Flow in a Degraded Environment

Jeff Fleming, Technical Cloud Account Executive, Oracle • jeff.fleming@oracle.com

ABSTRACT

Oracle is a data company that spends hundreds of millions of dollars a year on research and ways to enhance how users can interact with their data. The Oracle database ingests all types of data from all types of sensors, and with configuration, can easily integrate all that data, regardless of the type or sensor origin. From those relationships, commanders get analysis and decision support.

Once data is consolidated into a repository, your organization is ready for the next step: self-service analytics. Oracle Analytics delivers complete self-service analytics in an intuitive user interface built for everyone, from business users to data scientists. Available in the cloud, on-premises, or as a hybrid deployment, Oracle Analytics uses machine learning and artificial intelligence to uncover hidden insights and generate instant visualizations.

All of this can be done forward, in a DDIL environment on Oracle's roving edge infrastructure. Oracle edge infrastructure comes in two smaller form factors, the Ultra, which is a 7-pound backpackable device, and the RED, which is a 2U server in a ruggedized faraday cage case that weighs about 80 pounds and comes with GPUs. These devices talk between each other and to the enterprise tenancy, over any transmission device with an RJ-45 connector; SATCOM, 5G, wired internet, SINGARS with an RJ-45 dongle and more.

BIO: Jeffrey Fleming is a technical cloud account executive at Oracle Government Defense & Intelligence with expertise in tactical compute solutions supporting forward commanders, regardless of communications availability. When Fleming is not doing Oracle things, he is a traditional Army National Guard soldier with 21+ years of service. His first 14 years was as a signal officer (25A) at all levels within an IBCT doing tactical communications, after that he stood up a cyber protection team, and is currently the G6 for the IL ARNG, and the officer in charge of the Army National Guard's cyber exercise, Cyber Shield.

Oracle Roving Edge DDIL Analytics

Jeff Fleming, Technical Cloud Account Executive, Oracle • jeff.fleming@oracle.com

ABSTRACT

Army commanders are overwhelmed in data saturated environments, causing delayed decision making and data fatigue that is crushing their staffs — especially when forward deployed in contested environments, where high quality communications allow access to powerful clouds or rear support assets. Now, more than ever, forward decision assistance that can operate standalone with a minimal signature is critical to survivability and lethality.

Oracle roving edge infrastructure provides small form factor compute/storage for use in fully disconnected environments. If connection becomes available, the devices can synchronize to other connected units or big enterprise cloud, if desired. Oracle's smallest form factor, the Ultra, provides high-performance computing (HPC) optimized shapes for AI/ML applications when GPUs aren't available. Oracle's larger device, the RED, comes with up to three GPUs to support significant disconnected compute capability forward.

With Oracle, the interface between the enterprise and edge are the exact same. Before units deploy, S6/G6 shops can build out the required support packages for each unit in their enterprise cloud, and then issue edge devices when the unit is deploying. If a device is lost or destroyed, the original configuration remains in the cloud and can easily be re-provisioned and sent forward. To support mission changes, or critical device loss and needing to bump devices to support the mission, each device has plenty of storage to store pre-configured load outs to shift the applications from one mission set to another.

BIO: Jeffrey Fleming is a technical cloud account executive at Oracle Government Defense & Intelligence with expertise in tactical compute solutions supporting forward commanders, regardless of communications availability. When Fleming is not doing Oracle things, he is a traditional Army National Guard soldier with 21+ years of service. His first 14 years was as a signal officer (25A) at all levels within an IBCT doing tactical communications, after that he stood up a cyber protection team, and is currently the G6 for the IL ARNG, and the officer in charge of the Army National Guard's cyber exercise, Cyber Shield.

Cyberspace Operations in Multi-Domain Operations

Jim Smid, DoD/Intel Field CTO, Palo Alto Networks • jsmid@paloaltonetworks.com

ABSTRACT

The Army's integration of Cyberspace Operations into Multi-Domain Operations (MDO) involves leveraging advanced technologies and strategic planning to enhance operational effectiveness across all domains. At the tactical edge, where bandwidth and resources may be limited, Palo Alto Networks' solutions are designed to be efficient and effective. Our solutions are optimized for performance in constrained environments without compromising on security effectiveness. Robustness and reliability are critical, ensuring continuous operation even in challenging conditions where units operate in dynamic and potentially hostile environments.

At Palo Alto Networks, we know that cyber as a domain has to be fully integrated into the commander's operational picture like fires, aviation or any other asset. The fight in cyberspace can be readily managed and executed through security orchestration, automation and response as key tenets to protecting and defending the digital domain. This space can be well defended through an array of sensors that collect information and then, through AI-enabled orchestration, we can automate a series of programmed and dynamic responses to remediate the impact of the threat and even deploy countermeasures to fend off future attacks. Modern solutions to the problem enable us to thwart these attacks regardless of vector — traditional network infrastructure, modern 5G, or even on innovative platforms like the XM30, airborne platforms or in the connections between sensors and shooters. Commanders have a unified picture of their complete battle plan, from the phase lines in their mission to IP addresses in their networks — all at the speed of electrons.

BIO: Jim Smid has spent more than 25 years in the technology space. He brings background across many technologies, creating solutions and products for the federal and managed service markets. He started his career in software development, scripting, automation and operations. Prior to Palo Alto Networks, Smid spent 13 years as CTO for Iron Bow Technologies, focused on developing and deploying solutions for the federal government. From 2004 to 2008, Smid managed the engineering team focused on the Army and DoD agencies for EMC Corporation. During his tenure, Smid used his security and scripting background to create automated STIG scripts used by EMC in hundreds of deployments throughout the DoD.

Prior to working with the federal government, his background is in operations and solutions working in software development, telecommunications, service providers and managed services.

A Holistic Approach to Machine Learning for Electronic Warfare

Aaron Mihalik, Principal Engineer, Parsons • Aaron.Mihalik@parsons.us

ABSTRACT

Electronic warfare (EW) is in a constant state of change, driven by evolving adversarial capabilities, advancements in hardware platforms and the rapid growth of machine learning (ML) capabilities. Electronic attack (EA) techniques are particularly sensitive to these underlying developments. The Army must adopt a comprehensive strategy that addresses these challenges while rapidly deploying cost-effective solutions using existing hardware.

At Parsons, our approach to ML solution development—including our EW and EA products—is influenced by three interconnected areas:

- **Core Research and Development:** We drive advancements in electromagnetic signal analysis and response optimization through focused research initiatives. This includes advanced model architectures, efficient hardware integration and innovative data generation techniques. Our research extends to enhancing model robustness, addressing data scarcity and optimizing performance in tactical environments.
- **Model Lifecycle Management:** We integrate cloud-based development with tactical deployment, enabling collaborative iteration and continuous improvement. Additionally, we are developing standards for compact frameworks and integration methods to provide integration paths for model deployment into existing hardware with minimal modifications.
- **Continuous Evaluation and Demonstration:** Our state-of-the-art integration facilities provide testing and evaluation on Army platforms to ensure real-world effectiveness. These laboratories are low-risk venues for rapid prototyping and demonstration using realistic data sets. This collaborative environment provides for rapid feedback loops, swift determination of capability viability and continuous improvement.

This holistic approach enables us to stay at the forefront of EW and EA capabilities, ensuring that our solutions evolve as rapidly as the threats they counter. By combining cutting-edge research, flexible deployment strategies and rigorous evaluation processes, we provide the Army with adaptive, efficient and effective tools to maintain spectrum dominance in an ever-changing operational landscape.

BIO: Aaron Mihalik is a Parsons technical fellow specializing in applied AI/ML solutions with applications in spectrum-enabled operations. He has more than 20 years of experience leading and supporting programs within Department of Defense organizations, having fielded software and hardware projects in areas including audio analytics, natural language processing and physics-based modeling and simulation. As a senior technical advisor and AI/ML subject matter expert, he supports various AI/ML projects throughout Parsons, bringing innovative solutions to complex defense challenges.

Mastering the Information Environment to Deliver Information Advantage

Dr. Dave Dickey, Senior Intelligence Analyst, Peraton • dave.dickey@peraton.com

ABSTRACT

The Challenge

The U.S. government (USG) is largely outspent by competitors/adversaries in content creation and message dissemination in the information environment (IE) and existing approaches have proven insufficient due to resource and time constraints. The USG is outspent on information operations in the order of billions of dollars and the deluge of adversary misinformation and disinformation (including full-time broadcast media with locally tailored content, online news, syndicated content and BotNets) is challenging to track and assess.

The Solution

Peraton's Operationally Dynamic Information Network (ODIN) provides comprehensive analysis and assessment of the IE. ODIN leverages an array of AI-enabled data capabilities, combined with social scientific research, integrated into a single, cloud-based platform. ODIN leverages a full suite of AI-enabled tools, including machine learning (text and pixel-based), natural language processing (NLP), large language models (LLMs), and geospatial data visualization. These capabilities are integrated into a single platform to drive analysis and assessment using secure, IL5 cloud-based platform (AWS/Azure). ODIN also includes cross-domain (IL6/IL7), cloud-based capability to integrate intelligence and operational data.

Further, ODIN is designed to integrate world-class, social-scientific research derived from on-the-ground networks across the globe to inform LLMs, assess shifts in target audience attitudes/behaviors, including surveys, focus groups and elite samples.

Flexible human-machine teaming options include a range of SMEs like social scientists, data scientists, CULADs, statisticians, MISO professionals and market communication experts. Reach-back analytic support to answer quick-turn RFIs and customized reporting requirements is available as well as embedded assessment SME support to coordinate requirements and complete classified assessments.

ODIN key outcomes include:

- Full spectrum OIE analysis and assessment, integrated on a single platform
- Cross-domain data streams in a secure cloud environment, feeding AI-enabled solutions
- Examination of millions of friendly and adversary messages/OIE activities
- Rapid, interactive RFI response mechanisms to address dynamic shifts in the IE

ODIN has provided operational insights across multiple combatant commands, including INDOPACOM, CENTCOM, EUCOM, and Combined Joint Task Force Operation Inherent Resolve (CJTF-OIR). Outputs include hundreds of reports and a multitude of customized dashboards for analysis of the IE and access to the AskODIN LLM for rapid responses to information requests.

BIO: Dr. Dave Dickey manages the ODIN analytic cell in Peraton's Cyber Mission Sector and oversees analytic projects across multiple Combatant Commands. Dickey has spent his academic and professional career focusing on issues of foreign policy and national security. Dickey spent more than a decade as a senior analyst for the intelligence community and has broken new ground with the fusion of statistical modeling and qualitative evaluation allowing decision-makers to better anticipate future outcomes. His analytic leadership has provided mission-critical insights and strategic communications guidance for U.S. decision-makers on issues ranging from violent extremism to great power competition challenges.

Emerging Technologies to Deliver Information Advantage

Dr. Paul Lieber, Chief Data Scientist, Cyber Mission, Peraton •

paul.lieber@peraton.com

ABSTRACT

The Challenge

Information advantage no longer favors detailed understanding of online content; rather objective holistic looks at context. In the modern battlespace, information activities almost always precede, join or follow physical environment ones, and Army technology approaches seeking to understand actor attitudes, perception and behaviors must embrace this reality.

The introduction of advanced artificial intelligence (AI) and machine learning (ML) automated technologies only compounded this requirement, as the volume of information, complexity of source type and attempts to deceive multiplied exponentially. This includes adversary exploit of traditional and outdated assessment criteria for measures of effectiveness (MoE), where seeming success derived from data declaring false wins. As the Army and others play catch up in these areas, literally billions of dollars are spent every year in outdated target audience engagement, analysis, assessment and content delivery, campaigns and efforts unfortunately also ripe with Type 1 or Type 2 error based MoE.

The Solution

Emerging technologies can mightily assist if they are postured to address the new Army information advantage mission. These technologies can and should emphasize semi-automated data integration and tagging, the purposeful fusion and joint consideration of formerly disconnected information across information operations, cyber, signals and human intelligence domains, respectively. Importantly: there is no need for Army to purchase additional data sources, rather maximize existing collection capability and partners in new ways. As an example, current API based technologies are better employed as sources of information, not as standalone and costly entities.

Army AI and ML models should be purposefully implemented into traditional workflows to:

- a) streamline analysis processes
- b) maximize historical data to train AI and ML models
- c) simulate, predict and advise on future phenomena.

Data strategy and knowledge management plans should ensure—whenever possible—every Army data point can—in some aspect—be assessed against all other relevant ones on a target audience of interest. Full data provenance is required to locate source information, validate and justify relationships, also yield true data confidence. Technology must provide this.

Instead of narrative analysis, there is, for example, a wealth of potential knowledge in applying technologies to assess actor network structure formation, shift and dissolution, which combine to explain the ebbs and flow of a target audience genus also their information sharing and behavioral preferences on a topic of interest. Looking wider and via pattern of life exploration, significant anomalies in a large data space featuring multiple -INTs can point to adversary attempts to test new techniques, throw false breadcrumbs, fool impact measures of effectiveness, or preface a much bigger item of note.

Importantly, by Army adopting new approaches focused less on content-based intervention and more on contextual understanding, footprint and activity significantly lessens. With less touchpoints, this naturally helps protect mission integrity and lowers outreach and data collection costs writ large.

In tandem, better and more deliberate insertion of partner agency and nation efforts and capability is also underutilized at present and should be remedied. It is now a lot easier to comply with zero-trust architecture requirements when considering partner contributions, with almost every cloud environment adhering to it by default to include deliberate access controls by use type and group. These environments should replace legacy on-premises ones, whenever possible.

Peraton is already adopting all these information advantage approaches on several of its efforts, to include at Army Cyber's Information Advantage Enterprise, where thoughtful and considered integration of relevant target audience data across numerous spectrums occurs. These are supported—via Peraton Labs and others—by advanced AI and ML model creation, testing and application to expedite Army analyses and processes.

BIO: Dr. Paul Lieber is Peraton's chief data scientist for its Cyber Mission Sector, where he provides executive level strategic guidance on data solutioning, methodology and best practices. He likewise serves as an associate research scientist at the University of Maryland, co-leading an OUSD-P sponsored effort on Operations in the Information Environment assessment. Formerly COLSA's chief scientist, Lieber functioned as the command writer for two USSOCOM Commanders and strategic communication advisor to the commander of Special Operations Command-Australia.

Within academic environs, Lieber was a full-time member of the graduate faculty at Joint Special Operations University, Emerson College, University of South Carolina, and the University of Canberra, respectively. Within these roles, he taught across the entire strategic communication and influence curriculum, with a research emphasis on social media-based persuasion and methodological design. He possesses nearly 100 combined publications and lectures on these topics.

Cyber Decision Advantage

George Alder, Senior Systems Engineer, Peraton • george.alder@peraton.com

ABSTRACT

The Challenge

All national power is designed to create effects in the land domain, whether directly or indirectly, through economic, diplomatic and when necessary, military means. The operational domains of land, maritime, air, space and now cyberspace, must converge to produce these effects. However, traditional industrial-age approaches must now give way to fully integrated, multi-domain operations (MDO) to dynamically synchronize and focus these effects in a rapidly changing and chaotic environment.

Integration and synchronization across the strategic, operational and tactical levels of war are essential to ensure a unified effort toward national strategies and the commander's Intent. This requires agile and adaptable management of campaigns, operations, battles and engagement plans to achieve mission objectives in a complex and dynamic operational environment.

A crucial foundation for all MDOs is the freedom of maneuver within the information environment, which encompasses cyber operations, electronic warfare and information warfare activities. These functions are interdependent and reinforcing. Information advantage capabilities must support sensing, shared situational awareness and command & control, even under degraded conditions while remaining resilient, survivable, and adaptable in an all-hazard environment.

While the Department of Defense (DoD) seeks to leverage the latest AI/ML commercial capabilities, these solutions often fall short in operational environments that involve the application of lethal force and require safety-critical systems. Finally, MDO necessitates that information be shared with mission partners at the speed of battle to achieve mission objectives across contested areas.

The Solution

To tackle these challenges, Peraton has developed a comprehensive approach called Cyber Decision Advantage (CDA). Leveraging five decades of multi-sensor data fusion experience and the latest AI/ML technologies, our solution is designed to be fully extensible and scalable across all echelons and operational environments.

We achieve rapid and dynamic mapping of Cyber Mission Relevant Terrain (MRT-C) by analyzing all source intelligence, including the fusion of multiple ISR sensor types. Raw data is processed using conventional data fusion algorithms and deep neural networks, which encode and store embeddings in a vector database. This processed information is then used to assess features, entities, situations, and impacts, preserving complex relationships in a graph database.

These data stores build, populate, and dynamically update a cyber knowledge graph (CKG) of blue, gray and red cyberspace. Starting with MITRE ATT&CK and its adversary emulation platforms (STIX/TAXII) for struc-

tured data sources, the dynamic CKG is managed by in-memory knowledge graph databases, supporting continuous updates with threat intelligence feeds, real-time attack data, and vulnerability scanning results.

AI/ML analysis is used to develop MRT-C, overlaying mission relevance over the CKG. This analysis also produces defensive/offensive TTP mapping. Integrating MRT-C with AI/ML adds a crucial layer, using tools like Project Deepdive (DARPA) or KRYSTAL to analyze the CKG, identifying mission-relevant attack paths, potential pivot points, and exploitable vulnerabilities, considering dynamic factors like adversary resources and network configurations.

Finally, multiple courses of action (CoAs) are presented based on mission parameters, creating an automated mission plan through machine reasoning. Predictive analysis uses known TTPs, such as the MITRE ATT&CK Framework for Offensive TTPs and MITRE Engage for Defensive TTPs. Leveraging MITRE Engage for defensive TTPs and AI/ML analysis for offensive-defensive pairings automates CoA generation. Tools like DeepMind's AlphaStar, evolved with reinforcement learning, can simulate red team-blue team engagements within the CKG, suggesting optimal offensive moves and countermeasures. AI-powered planning algorithms like hierarchical temporal planners (HTPs) can translate optimal CoAs into executable mission plans. Tools like EUROPA (NASA) or OPTIC planner (Army Research Lab) can dynamically create attack sequences, resource allocation strategies, and contingency plans based on predicted adversarial responses and potential collateral damage.

CDA informs defensive cyber operations internal defense measure (DCO-IDM) by predicting actions by specific threats against critical information assets and providing CoAs for DCO response actions to neutralize active threat actors. For offensive cyber operations (OCO), arsenal capabilities are mapped to adversarial vulnerabilities to provide dynamic CoAs.

Integration across the information environment is further supported by other Peraton capabilities, such as the Operational Spectrum Comprehension, Analytics, and Response (OSCAR) Solution for Dynamic Spectrum Management and the Operationally Dynamic Information Network (ODIN) for information operations. Using a common multi-sensor data fusion framework, these capabilities can be integrated across MDO and with mission partners through information-sharing techniques.

BIO: George Alder, a seasoned senior systems engineer, boasts more than three decades of extensive experience in planning, architecting and engineering mission-critical processes for the Department of Defense. His impressive career spans roles at prestigious organizations such as Peraton, U.S. Africa Command (USAFRICOM) and the 38th Cyber Engineering Group. Alder's profound expertise lies in information technology, cyberspace solutions and military doctrine.

Currently serving as a senior enterprise architect at Peraton, Alder supports the Air Force, Space Force and DoD activities by developing advanced architecture artifacts and products. His specialization in mission engineering, command & control, cyberspace operations, and cybersecurity—including zero trust and identity management—underscores his pivotal role in shaping strategies for high-level defense programs.

Before joining Peraton, George made significant contributions at the 38th Cyber Engineering Group, where he served as a cyberspace systems engineer. His leadership was instrumental in integrating cyberspace mission requirements for Air Mobility Command and Air Education and Training Command. During his tenure at USAFRICOM as the chief enterprise architect, he established critical IT governance and enterprise architecture programs, facilitating the migration of legacy systems across Africa. Alder 's earlier career includes impactful roles as a joint systems engineer and software systems engineer at the 38th Engineering Installation Wing.

Alder holds a Bachelor of Science in electrical engineering from the Thomas J. Watson College of Engineering and Applied Science. His certifications from the DAU in Systems Engineering and the ISC2 in Information Systems Security Engineering & Cloud Security further validate his expertise.

With a career marked by innovation, leadership, and technical excellence, Alder remains a driving force in the realm of defense and cybersecurity. He is dedicated to delivering secure, balanced solutions through the effective integration of people, processes and technology.

Distributed Edge Cyber Operations

George Alder, Senior Systems Engineer, Peraton • george.alder@peraton.com

ABSTRACT

In the evolving battlefield, data plays a crucial role, necessitating advanced analytical capabilities at the tactical edge to support multi-domain operations (MDO). This abstract explores how technological progress enables efficient data analytics at the tactical edge, converting extensive data into actionable insights. Given its integration with all other C5ISR data and assets, the cyberspace domain is uniquely positioned to deploy analytics platforms that safeguard capabilities and enhance sensor and source fusion.

The Challenge

While big data platforms play a crucial role in handling and analyzing the vast data volumes produced in contemporary military operations, existing big data architectures have notable limitations. These architectures necessitate transmitting data back to a central cloud service, resulting in decision-making delays due to network latency issues caused by congestion or disruptions. Additionally, bandwidth constraints contribute to high data transfer expenses and restricted network availability in remote areas. Security and scalability are also challenges, given the risk of single points of failure and resource-intensive processes.

MDO demand analytical capabilities akin to those found in big data platforms, complemented by cutting-edge AI/ML technologies. Edge analytics tackles these requirements by processing data near its source. This approach enhances real-time decision-making, minimizes latency & bandwidth usage, strengthens security & privacy and offers cost-effective scalability. Leveraging the computational power of edge devices, edge analytics distributes the processing load, mitigating challenges associated with centralized big data analytics.

However, successful implementation of edge analytics necessitates a deliberate and well-considered approach that provides seamless information sharing and machine reasoning capabilities between fixed and maneuver units, including mission partners. Compute and storage platforms should be adaptable and configurable to accommodate diverse environments and connectivity, enabling self-forming networks. These platforms ought to host a broad array of AI/ML and data fusion algorithms, which can be dynamically updated to adapt to changes in the operational context. Additionally, it's recognized that decentralized data fusion systems may yield inconsistent and corrupted indicators due to the propagation of redundant information. To address these challenges, advanced data fusion techniques, such as covariance intersection, must be employed to ensure the reliability of derived indicators.

The Solution

To address these challenges, Peraton developed a tiered architecture approach called Distributed Edge Cyberspace Operations (DECO). Building on five decades of multi-sensor data fusion experience and leveraging the latest AI/ML technologies, our solution offers a fully extensible and scalable framework across all echelons and operational environments while ensuring secure access to cyberspace. The integrated tiered model aligns with the strategic, operational, and tactical levels of war as well as the portfolio-, program- and dev-team levels of the scaled agile framework. Integration with operational planning teams (OPT) aids

in planning campaigns, operations, battles and engagements, as well as in the algorithmic preparation of the battlespace. The tiered AI model development and deployment architecture consists of central cloud locations, intermediate locations, and edge nodes. Central sites support big data analytics & learning, data aggregation, data processing, model training, evaluation and model repository. Intermediate locations, including agency data centers and edge servers, focus on fine-tuning constraints, performance optimization, and deployment management. Finally, edge devices such as edge nodes, IoT devices, and sensors support model inference, local data collection, real-time decision-making and provide feedback to higher tiers.

Technology Overview

Functional specialists like software developers, AI engineers and data scientists prefer environments that simplify the underlying infrastructure using cloud and API services. However, this can impede optimal design by limiting performance, efficiency, scalability and extensibility beyond this infrastructure. To effectively support edge capabilities, a comprehensive systems engineering approach is necessary to leverage the full spectrum of leading technologies. This allows functional requirements to be allocated across these technologies, ensuring systems are designed to best meet mission needs.

The DECO approach is supported by adaptive computing technology tailored to the compute and storage needs at each architectural tier. This includes centralized cloud services with conventional GPU accelerators and newer AI inference engines, as well as high-performance edge nodes equipped with AI engines, FPGA accelerators and SmartNICs. These edge nodes offer composable hardware that can be adapted for fine-tuning and inference models, with FPGA capabilities significantly reducing the attack surface by eliminating memory and storage vulnerabilities. Open-source scalar and vector processors, such as RISC-V designs, can be instantiated in FPGAs, enabling complex processing capabilities to be tailored for specific needs in an adaptable and agile manner.

Security technologies like physically unclonable function (PUF) utilize manufacturing variations in integrated circuit production to establish a “silicon fingerprint,” offering immutable verification of edge node identities. This technology can also secure cryptographic keys, creating a vault accessible only within the device post-secure boot. Inline memory encryption also ensures confidential computing by partitioning data-in-use (DIU) for virtual machines and containers.

Storage technologies like 100G Remote Direct Memory Access (RDMA) over Converged Ethernet (ROCE), reduce CPU overhead by enabling direct access to storage arrays via PCIe and high-speed Ethernet. OPAL NVMe self-encrypting drive (SED) standards ensure encryption of multi-tenant storage and protect Data at Rest (DAR).

Adaptive Compute Systems on a Chip (SoC) provide revolutionary capabilities at the edge, offering processing systems, programmable logic, AI engines, digital signal processing (DSP), high-speed networking exceeding 400G, advanced cryptography, and security functions in a single device. These technologies can be implemented in a standard PCIe server card or a VPX platform aligned with sensor open system architecture (SOSA).

When properly integrated, these technologies have the potential to innovate microservice analytical services for sensor fusion, AI/ML, and machine reasoning. Implemented within a cohesive total systems design, this approach can provide a substantial operational advantage over adversaries.

BIO: George Alder, a seasoned senior systems engineer, boasts more than three decades of extensive experience in planning, architecting and engineering mission-critical processes for the Department of Defense. His impressive career spans roles at prestigious organizations such as Peraton, U.S. Africa Command (USAFRICOM) and the 38th Cyber Engineering Group. Alder's profound expertise lies in information technology, cyberspace solutions and military doctrine.

Currently serving as a senior enterprise architect at Peraton, Alder supports the Air Force, Space Force and DoD activities by developing advanced architecture artifacts and products. His specialization in mission engineering, command & control, cyberspace operations, and cybersecurity—including zero trust and identity management—underscores his pivotal role in shaping strategies for high-level defense programs.

Before joining Peraton, George made significant contributions at the 38th Cyber Engineering Group, where he served as a cyberspace systems engineer. His leadership was instrumental in integrating cyberspace mission requirements for Air Mobility Command and Air Education and Training Command. During his tenure at USAFRICOM as the chief enterprise architect, he established critical IT governance and enterprise architecture programs, facilitating the migration of legacy systems across Africa. Alder's earlier career includes impactful roles as a joint systems engineer and software systems engineer at the 38th Engineering Installation Wing.

Alder holds a Bachelor of Science in electrical engineering from the Thomas J. Watson College of Engineering and Applied Science. His certifications from the DAU in Systems Engineering and the ISC2 in Information Systems Security Engineering & Cloud Security further validate his expertise.

With a career marked by innovation, leadership, and technical excellence, Alder remains a driving force in the realm of defense and cybersecurity. He is dedicated to delivering secure, balanced solutions through the effective integration of people, processes and technology.

Data Analytics for Decision Dominance at the Edge

Derek Thurston, Associate Principal Architect, RedHat • dthursto@redhat.com

ABSTRACT

By using artificial intelligence/machine learning (AI/ML) at the edge to perform real-time data processing and analysis, ML models can process vast amounts of data in real-time, filtering out the “noise,” to provide commanders with actionable insights swiftly. This includes the identification of patterns, an ability to predict outcomes and the optimization of resource allocation.

Edge devices can operate independently, maintaining functionality even when network connectivity is disrupted, ensuring continuous data processing. Using Army developed ML decision models, edge devices can prioritize and send critical data when an opportunity arises, ensuring commanders receive the most pertinent information.

Red Hat Device Edge provides a variety of deployment options for a consistent and secure platform to run AI/ML workloads at the edge, the datacenter and in between. Specifically, for edge deployments, containerized applications and functions-as-a-service using “OpenShift Serverless” reduce the amount of compute, memory and storage required to process data to the smallest necessary for the mission workload.

By utilizing Red Hat Device Edge and ML, real-time compute requirements can be reduced and the influx of data from sensors can be reined in, providing commanders in the Army of 2030 and beyond to turn data into actionable decisions effectively, even in degraded and congested environments.

BIO: Derek Thurston is an associate principal solution architect at Red Hat and has been working with open source software since the mid ‘90s. After graduating from a small merchant marine college in coastal Maine, Thurston landed a job in the “IT Department” at a naval architecture firm in Arlington, Virginia, where he started using Linux. Thurston has worked with SGI and HP/UX systems and did his part to help save the world by converting COBOL programs to four-digit years in the late 1990s. Having worked with a variety of public and private sector entities, he has spent more than 25 years helping customers find the right open source tools and technologies.

Equipping The Warfighter With Actionable Insights via Intelligent Automation

Bill Roberts, Deputy Chief Technology Officer, Riverbed •

william.roberts@riverbed.com

ABSTRACT

As missions become more distributed, today's warfighters operate in increasingly complex IT environments. To operationalize data and make the most effective decisions, more and more commands turn to intelligent automation, which combines artificial intelligence (AI), correlation and analytics to streamline repeatable processes with minimal human intervention. This technology equips warfighters with actionable insights across an organization's entire IT ecosystem, leading to enhanced efficiency, productivity and user satisfaction.

To tackle these challenges, the concept of "shifting left" has become more crucial than ever. This approach focuses on resolving issues at the fastest speed and lowest technical level possible to enhance productivity and minimize dependency on specialized knowledge.

Key Takeaways:

- How to "shift left" and reduce the time and resources needed to detect, analyze, and resolve network performance issue
- How to scale up your IT team's ability to meet support demand by analyzing large volumes of cross-domain data, freeing staff to focus on the most critical needs
- How to utilize automation to prioritize alerts with actionable insights, reducing overall alert volume while speeding response time for issues impacting mission readiness

BIO: Bill Roberts serves as the deputy CTO at Riverbed Technology for the U.S. Department of Defense. Roberts is a trusted advisor for Riverbed DoD customers to help ensure mission success by realizing the optimum value from Riverbed solutions and advocating for the customer within Riverbed, driving product change to meet customer needs. Roberts has more than 20 years of experience in the IT industry specializing in networking, integration, automation and service management working with DoD, intelligence community, civilian government, as well as private sector customers. Roberts started his IT career in first level technical support, progressing into escalation support and support management before moving to professional services implementation consulting and project management positions, finally transitioning to pre-sales engineering.

Enabling AI/ML at the Tactical Edge

Jay Meil, Vice President, AI, SAIC • jason.t.meil@saic.com

ABSTRACT

SAIC's Tenjin enables warfighters to sense, make sense and act in near real-time, denied degraded intermittent and limited (DDIL) bandwidth environments. It provides artificial intelligence, machine learning (AI/ML) and data analytic capabilities in DDIL environments using SAIC's Edge Services Architecture (ESA), a lightweight, open architecture that is flexible and adaptable to support distributed operations for the Army of 2030 and beyond. Developed using ESA, Tenjin is small form factor deployable software that performs sub-second aggregation and fusion of real-time data at the edge. It hosts multiple AI models, including object detection, entity recognition and speech to text, enabling rapid threat to targeting decision making through automated tagging, classification, and aggregation at the source. It also provides a visualization of AI model effectiveness to ensure confidence in dynamic operational environments.

Tenjin automates data tagging using streaming attribute-based access control (ABAC) to secure data for U.S. and coalition partners, avoiding the need for manual intervention and cross domain solutions (CDS). Tenjin includes two approaches to improving AI models and performance at the edge. First, it provides easy-to-use no-code tools to rapidly create AI models in the field without special hardware, cloud or network access. These models are immediately deployable in multiple formats, including ARM64, x86/64 and Web Assembly. Second, it performs inference on real-time edge data, evaluating and analyzing new sensor information to automatically improve performance of its edge-deployed AI/ML algorithms. For example, inference could adapt AI models to the current terrain or weather conditions.

Tenjin provides real-time monitoring and instant alerts on environmental changes or emerging threats, enabling real-time data-informed decision making. To do this, Tenjin uses SAIC's AI Feature Importance model to identify actionable data or other priority information, such as algorithm outputs or fused sensor data. It then prioritizes transmission of critical data, optimizes the type and amount of total data transmitted, and sends data on the best network path using an Auto Primary Alternate Contingency and Emergency (PACE) algorithm. Before transmission, all data is compressed and encrypted to minimize bandwidth consumption.

Using Tenjin, SAIC:

- Reduced transmission of required sensor data from the edge by 74% using AI Feature Importance
- Performed vehicle classification in 10 ms using fused sensor data on microcontrollers with digital signal processing (DSP)
- Displayed classification in remote vehicle in DDIL environment in less than 1 second
- Synchronized 2.5K data records per second over Bluetooth

BIO: Jay “Wizard” Meil is vice president of artificial intelligence (AI) and chief data scientist at SAIC, where he leads AI technical strategy and oversees solutions that enable rapid decision-making at scale in support of multiple intelligence disciplines and command, control, communications, computers, cyber, intelligence, surveillance, and reconnaissance (C5ISR). He also chairs SAIC’s AI Council. Outside of SAIC, Meil is on the Security Industry Association (SIA) AI Advisory Board, has been invited to be a member of the National Institute of Standards and Technology (NIST) U.S. Artificial Intelligence Safety Institute Consortium, and advises Congressional committees on topics related to AI.

Meil is a recognized subject matter expert in the application of machine learning to analytical tradecraft, all source intelligence, open source intelligence and C5ISR. He serves as a technical advisor to numerous intelligence organizations within the intelligence community (IC) and Department of Defense (DoD).

Meil has led cross-functional teams who have designed, built and deployed deep learning models to support federal government customers in complex missions of national importance, with the ultimate objective of making the nation safe against peer and near-peer threats. In addition to the IC and DoD customers, he has supported civilian agencies including the Department of Homeland Security.

As an SAIC research fellow (emeritus) and now an SAIC technical fellow, Meil is focused on three areas:

- Building data models and integrating common taxonomies to identify objects of interest across service components and combatant commands
- Integrating multi-modal intelligent decision support systems into command and control operations
- Applying AI algorithms in identity intelligence, information warfare, information operations and unconventional warfare (I2/IW/IO/UW) operations.

Meil is a frequent participant in research panels and industry discussions on the impact of AI on national security, including with the John Hopkins University Applied Physics Laboratory; the Center for Security in Politics at UC-Berkeley on behalf of DARPA; CERN’s OpenLab and Quantum Technology Initiative; the European Geosciences Union; the Atlantic Council Scowcroft Center for Strategy and Security; the Potomac Officers Club; and AFCEA International.

Speed the Tactical Data Analytics and AI Mission with ZSP Identity Security at the Edge

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

ABSTRACT

The joint multi-domain environment of today brings a new pace of information faster than ever before. This multidomain environment drives a complex data saturation that propels the need for data access capability in cloud resources at the edge. This data at the edge though has potential for operational advantage, comes with new risk challenges to maintain speed of the mission. These data assets (such as AI/ML outcomes) when harnessed with zero-standing privilege (ZSP) identity security brings the field operator the potential to mediate the risk of operating the edge data analytics while leveraging that data for competitive overmatch.

Key to success of harnessing edge data analytics is not just about the data itself but more specifically about engaging the data with ZSP identity cyber protection so that the edge analytics data moves safely to the commander, leader and soldier at the speed of necessity. Fundamental to providing ZSP identity cyber protection at the edge is the ability to swiftly and securely onboard users and NPEs (non-person entities) using least privilege to hybrid cloud data analytics resources operating at the edge. As part of this capability, the ZSP identity cyber protection enables speedy and secure zero-trust access to accelerate data analytics at the edge in way that also survives disconnected scenarios.

Delivering on challenges of data analytics at the edge requires a ZSP identity cyber protection with durable disconnected survivability that is accessible from cloud core to the tactical edge. The ZSP identity security enables edge data analytics brings capabilities to the multi-domain theater including:

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

Data analytics at the edge using ZSP identity security enables rapid access to hybrid cloud and edge assets to support the multi-domain mission. The capabilities included and described as part of this session include details of the capabilities, durable ICAM architecture and operational use case scenarios to hasten the assurance of success of the mission.

BIO: Andrew Whelchel (CISSP-ISSAP, ISSEP, CCSP, CGRC, CSSLP) started in information security and IAM immediately after graduation from the University of Memphis, supporting identity and access management managing Microsoft Identity for U.S. federal customers. Later work transitioned to network infrastructure security and then to consumer identity protection in the role at RSA Security and most recently at Okta and Saviynt. At RSA Security supporting financial services, health care, U.S. federal and other customers, there was focus on identity risk analytics and integration of identity fraud intelligence for cybercrime prevention. At a prior role at Okta and the current role at Saviynt, focus is on protecting employees as well as 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.

Transforming the U.S. Army Network Workforce: A Future-Focused Approach to Automation and Efficiency

Brian Tetreault, Account Executive, ServiceNow • brian.tetreault@servicenow.com

ABSTRACT

The U.S. Army's unified network demands a highly skilled workforce to manage its vast and complex infrastructure. However, traditional, labor-intensive approaches limit agility and scalability. We explore how next-generation technologies can revolutionize the Army's network operations by significantly reducing personnel needs.

We propose leveraging automation across key network functions:

- **Installation and Maintenance:** Automating device setup and configuration minimizes manual effort for installation teams. Integration with advanced request and dispatch systems streamlines maintenance activities, reducing reliance on manual processes.
- **Real-Time Network Visibility and Proactive Management:** Real-time data analysis can predict and prevent network issues, minimizing reactive troubleshooting and personnel workload. Automated workflows can trigger self-healing mechanisms or dispatch technicians only when necessary.
- **Enhanced Network Security with Reduced Manpower Burden:** Automated threat detection and response systems can significantly reduce the workload on security personnel. Integration with a centralized security platform can further reduce manpower needs for security management.

These automated functionalities empower a leaner, more efficient Army network workforce by:

- **Reducing Manual Workloads:** Automating repetitive tasks frees up personnel time for strategic initiatives like network optimization and security planning.
- **Improving First-Time Resolution Rates:** Enhanced knowledge management systems empower technicians to resolve issues efficiently on the first attempt, reducing repeat dispatches.
- **Data-Driven Decision Making:** Real-time network data can guide informed decisions for resource allocation, optimizing network performance and cost-effectiveness.

By embracing automation, the U.S. Army can achieve a future-proof network workforce characterized by efficiency, agility, and a focus on mission-critical tasks.

BIO: Brian Tetreault is an account executive for ServiceNow, working to enable digital transformation across the U.S. Army. He brings 10 years of experience in the IT consulting space, including time spent at Ernst & Young supporting various commercial, DoD and state/local organizations. In his current role, he works with customers to understand the benefits of moving to cloud-based and Software-as-a-Service solutions and leveraging ServiceNow's enterprise applications to achieve successful business and tactical outcomes. Tetreault has a deep understanding of the way DoD organizations operate, from an IT implementation and program management perspective. He is a certified ServiceNow System Admin.

Digitally Transform Security Operations for Improved Cyber Defense

Scott Flynn, Security Operations Advisory Solution Consultant, ServiceNow •

scott.flynn@servicenow.com

ABSTRACT

ServiceNow Security Operations (SecOps) streamlines security processes, reduces manual workload and enhances the efficiency and effectiveness of security teams, allowing organizations to maintain a robust security posture with fewer resources. Leveraging ServiceNow SecOps can optimize the mission in support of Gabriel Nimbus, RCCs and NECs by automating security processes and centralizing data into a single source. SecOps significantly amplifies the productivity and effectiveness of security teams. This enables them to manage a larger volume and greater complexity of security tasks without a proportional increase in team size, making it a powerful force multiplier in cybersecurity management.

Join us to learn how these capabilities can transform how the Army manages, monitors, and secures/defends a unified network.

- **Automation of Security Processes:** ServiceNow automates the incident response process, from detection to remediation. Automated workflows reduce manual effort and speed up resolution times.
- **Vulnerability Management:** Automatic scanning and assessment of vulnerabilities, combined with prioritization based on asset criticality and threat context, streamline the patch management process.
- **Unified Platform:** A centralized platform for security operations, integrating various security tools and processes into a single interface. This reduces the complexity and the need for multiple specialized roles.
- **Machine Learning and AI:** Leverage machine learning and artificial intelligence to detect anomalies, predict potential threats and suggest remediation actions. This proactive approach reduces the manual effort required for threat hunting.
- **Orchestration Capabilities:** ServiceNow orchestrates workflows across different security tools and systems, ensuring that tasks are completed efficiently without human intervention. This reduces the manual workload on security analysts.
- **Common Control System:** Security teams can view and manage all security incidents, vulnerabilities, and threats from a single dashboard, improving visibility and control.

BIO: Scott Flynn began his career enlisting in the U.S. Army in 1991, at 17, into the Signal Corp as a 29V. Supporting secure, global IT operations in South Korea, the Pentagon Army Tech Control and Army Operation's Center, Flynn was honorably discharged in 1996. For more than 30 years, Flynn has supported the secure global communications of the U.S. Army, Navy, Marine Corps, Air Force, White House Communications Agency, Department of State, and several other U.S. intelligence agencies focusing specifically on cybersecurity and RMF via ICD-503. He has a bachelor's degree in information technology and a master's degree in cybersecurity. Certified in several network disciplines, Flynn holds a CISSP certification as well as ServiceNow's CSA.

Data Analytics at the Tactical Edge

Joe Hagan, Staff Solutions Engineer, Splunk • johagan@splunk.com

ABSTRACT

When it comes to AI & ML, we all have grandiose ideas of what this future looks like—and we can all agree a future with more C-3PO and less Agent Smith is ideal. Until reality catches up to science fiction, we are bottlenecked by our compute capabilities. These limitations, coupled with data storage capacity, are compounded even more so at the tactical edge.

Splunk has been providing machine learning at the tactical edge since 2015 via our Machine Learning Toolkit (MLTK) and since 2020 with our Data Science and Deep Learning (DSDL). Deploying Splunk at the tactical edge allows users to leverage prebuilt containers for TensorFlow, PyTorch and various data science, NLP and machine learning libraries. Using predefined Jupyter Lab Notebooks workflows, DSDL enables rapid model development, testing and deployment all within Splunk. You can even leverage GPUs for intensive training tasks and deploy models on CPU or GPU containers.

BIO: Joe Hagan is a staff solutions engineer at Splunk, with a solid foundation in cybersecurity. He holds both a master's and a bachelor's degree in the field. Hagan has been working in the Information Technology field since 2004. He's served in various technical roles within DoD/IC spaces since 2009, gaining valuable experience in addressing unique challenges in critical national security environments.

Hagan has been a Splunk enthusiast since first touching the platform in 2011, he created GoSplunk.com in 2015, and officially joined the mothership that is Splunk in 2019. He's leveraged his background and practical knowledge to accelerate his customers through their Splunk maturity journey and continues to do so to this day.

Data Protection at the Tactical Edge

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies •

Gina.Scinta@ThalesTCT.com

ABSTRACT

Core computing functionality commonly found in data centers and in the cloud can now be deployed at the tactical edge—data protection capabilities must transition with that move.

For example, military operations at edge often require unique situational data to be shared with coalition partners and must utilize core-level security protocols like zero trust to ensure data is only shared on a need-to-know basis.

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

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

- How to securely share CUI, SBU data with coalition partners
- How to contend with environmental and operational constraints at the edge
- How to extend your existing cybersecurity infrastructure to the edge
- Why supply chain security is critical at the edge

BIO: Gina Scinta is Thales TCT's deputy chief technology officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC and more.

Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world class encryption and key management for data at rest in data centers and cloud infrastructures.

Intersection of AI and Security

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies •

Gina.Scinta@ThalesTCT.com

ABSTRACT

Artificial intelligence (AI) is rapidly transforming our world, from the way we work to the way we interact with machines. But with this immense power comes immense responsibility. As AI becomes more sophisticated, so too do the potential security risks.

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

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

BIO: Gina Scinta is Thales TCT's deputy chief technology officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC and more.

Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world class encryption and key management for data at rest in data centers and cloud infrastructures.

Best Practices for Data in Transit Encryption

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies •
Gina.Scinta@ThalesTCT.com

ABSTRACT

High speed networks are the critical foundation that supports many of an agency's most vital communications and operations. However, this foundation is at risk of surveillance and attack by increasingly sophisticated cyber criminals and well-funded nation states.

These network connections, if unprotected, are proving to be highly vulnerable, leaving sensitive assets exposed. So, what is the best way to protect network traffic? Encrypt everywhere—between data centers and headquarters to backup and disaster recovery sites, whether on premises or in the cloud.

Attend this session to learn about the best practices for data in transit encryption including how to:

- Protect against common network threats such as eavesdropping, fiber-tapping, harvest and decrypt
- Deploy high speed encryption from the core to the cloud to the edge
- Improve performance
- Mitigate the quantum threat
- Address zero-trust requirements

BIO: Gina Scinta is Thales TCT's deputy chief technology officer (CTO). In this role, Scinta serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Scinta also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC and more.

Scinta has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Scinta served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world class encryption and key management for data at rest in data centers and cloud infrastructures.

Algorithm Evolution

Thomas Clark, Program Manager, X Technologies • thomas.clark@x-technologies.com

ABSTRACT

Algorithm Evolution: In this presentation, we empower system owners and leaders to navigate the algorithm evolution and threat landscape while exploring the transition to SHA384 and quantum-resistant algorithms, emphasizing the importance of crypto-agility in maintaining security in the face of rapid technological advances. Insights from a previous AE migration provide a practical perspective on algorithm evolution as we discuss our AE framework that mitigates risk and increases confidence. This presentation aims to prepare clients for the rigors of zero-trust maturity and equip stakeholders to fortify their defenses against the ever-changing threats of the digital world. Finally, we discuss how a modernized public key infrastructure (PKI) enables Zero Trust in a strategic and tactical environment.

BIO: Thomas Clark is an industry leader in public key infrastructure (PKI), a senior technical leader and future technology strategist with extensive experience in government contracting, specializing in the PKI office. Currently leading the future technology cell, he has dedicated his career to driving innovation and ensuring the highest standards of security and efficiency in the digital landscape.

With a background in both technology and leadership, he successfully managed complex projects, aligning them with strategic goals and ensuring they meet the rigorous demands of the modern digital environment. His passion for technology is matched only by his commitment to foster collaboration and growth within his teams.

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

