TechNetCyber

INNOVATION SHOWCASE 2024

JUNE 25–27, 2024 | BALTIMORE CONVENTION CENTER, BALTIMORE, MARYLAND

AFCEA

SIGNAL
AFCEA INTERNATIONAL MEDIA

2024 TechNet Cyber Innovation Showcase

By strategic design, the theme for 2024 TechNet Cyber is “Outpacing the Threat: Alight, Adapt, Accelerate.” It is challenging to describe the sheer urgency of cyber cooperation needed across departments, agencies, industries and governments. TechNet Cyber serves as the center of gravity for a whole-of-government effort and our strategic industry partners play such a vital role in finding the solutions to meet global security challenges and successfully operate in a digital environment.

AFCEA International is doing its part to share information, build partnerships and find solutions in the critical digital domain, to include hosting this Innovation Showcase that provides companies the opportunity to demonstrate cutting-edge solutions to government representatives and potential industry partners.

The showcase provides a platform for broad exposure to government, military, fellow industry and academia attendees. It’s imperative we discover and share the information, build the relationships to realize that whole-of-government approach, which has practically become a way of life for the national security and defense community.

Yes, a lot of work still needs to be done and a lot of challenges overcome to promote faster, more efficient and effective collaboration across our government and among multiple governments. And the content on these pages and at a flagship event such as TechNet Cyber are optimal places to start.

Best wishes,

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

In an era of increasing requirements and constrained resources, the Department of Defense (DoD) must continue to embrace commercial innovation and the efficiencies it can provide. The Innovation Showcase is an opportunity for companies of all sizes to demonstrate groundbreaking solutions of interest to government and potential industry partners.

The Defense Information Systems Agency (DISA) Emerging Technology Directorate sought solutions to address emerging or existing challenges. TechNet Cyber participants submitted potential solutions for the following problem statements.

Generative AI

Problem Statement: The DoD is in the midst of an AI revolution — with an opportunity to positively impact how we work. Yet, the success of artificial intelligence (AI), machine learning (ML), generative AI (Gen AI) and other data-intensive models are linked to the quality of the data they ingest. The large amount of data that DISA ingests daily leads to fundamental problems with labeling data to train language learning models. DISA is looking for innovative solutions that will allow us to utilize cyber data to train language learning models with the goal of augmenting the capabilities of DISA's analysts by identifying known attacks and potential new zero-day attacks.

Why this is Important: The DoD needs to leverage accelerated data access solutions to establish a continuous data pipeline across global and hybrid data sources to feed AI models and analytics platforms. We need to understand the considerations for deploying future-ready AI programs and utilize AI models to effectively detect cyber log data threats and increase our analysts' capability in defending the DoDIN.

IT Investment Optimization (Technical and Business)

Problem Statement: Is the DoD/DISA using its invested IT to its full potential?

Why this is Important: With the hundreds of IT vendors that help to power DISA services and internal business operations, it is impossible to know all the terms and conditions of a given service or software. DISA must divest from technology that no longer efficiently and effectively solves the warfighter's problems. The agency must also determine if it currently offers redundant systems or tools that should be removed to simplify operations and reduce costs. DISA requires a detailed insight into its IT investment to measure its effectiveness and extract the best value for mission partners.

Measure What Matters—Key Performance Indicators

Problem Statement: Leaders and employees are expected to set broad-reaching goals -- but how is the agency measuring performance? How does DISA know if it has accomplished its mission?

Why this is Important: Key Performance Indicators starts with having something to measure first. If you can't measure it, then you can't track it. And if you can't track it, you won't achieve it or will achieve it most inefficiently. DISA must invest in scalable and repeatable tools to help leaders and individuals set objectives and measure key performance indicators to fully understand the agency's IT, program, and project investments.

Table of Contents

SUBMISSIONS ON GENERATIVE AI

Navigating the Risks: Strengthening DoD Supply Chains Against AI-Induced Vulnerabilities

By Jeremy Newberry, Cybersecurity Solutions Architect, Merlin Cyber 9

Data Management and Future Network Operations with AI/Gen AI/ML

Dean Brewster, Senior Director Product Line Management, Ciena 10

Using AI Agents and RAG to Augment the Cyber Warfighter

Ed Sealing, Founder & Chief Technology Officer, SealingTech 11

Querying Minds Want to Know: Can a Data Fabric Overcome the Data Agility Challenge Hindering Gen AI Potential?

Terry Dorsey, Senior Data Architect, Denodo 12

Generative AI for DCO: Why Timing and Signal are Key

Zachary Vaugh, Director, Federal Security Engineering, Vectra AI 13

Accelerate Your Generative AI using ZSP Identity Security to Reduce Risk and Speed the Mission

Andrew Whelchel, Senior Solution Engineer, Saviynt 14

Decoding the Hype: Practical Applications of Large Language Models in Cybersecurity

Yihua Liao, Senior Director, AI Labs, Netskope 16

Utilizing AI to Unlock Data Essential to Mission Success

Marlin McFate, Public Sector Chief Technology Officer and Chief Information Security Officer, Cohesity 18

Adobe & The Impact of Generative AI in Information Operations

Michelle Woolford, Adobe Account Executive, Carahsoft Technology Corp. 20

Intersection of AI and Security

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies 21

Identity and AI Trends Driving Zero Trust Programs in the DoD

James Imanian, Senior Director, CyberArk Solutions 22

Transforming Security Through Language Models

Jonathan Mullin, Chief Technology Officer, DCI Solutions 23

Cybersecurity in the Age of AI: Fusing Zero Trust with Universal Confidential Computing

Dwayne Hoover, Vice President, Solutions Engineering, Anjuna Security 25

Data Driven AI: Practical Advice for Successful Results

Ron Rintala, President & CEO, DataInFormation – Liberty Source 26

Enhancing Cybersecurity with Cloudera: A Generative AI Approach for the Department of Defense

Tej Tenmattam, Principal Solutions Engineer, Cloudera Government Solutions 27

Fully Trained Cyber AI Engine for Advanced Threat Detection

Eric Irizarry, Security Solutions Architect, MFGS, Inc. 29

Enhancing DoD's AI Threat Intelligence with Comprehensive Datasets

Tim LeMaster, Vice President, Worldwide Systems Engineering Lookout 30

VMware Private AI Foundation

Tommy Dammer, Senior Solutions Engineer, VMware, Broadcom 31

DataBee from Comcast Technology Solutions—Cracking the Code with OCSF: Making Machine Learning a Symphony of Success!

Scott Miserendino, Vice President of Engineering Cyber, Comcast 32

The New AI Data Frontier: How to Secure, Optimize and Expedite Data Operations for AI

Jim Cosby, Chief Technology Officer, NetApp 34

Securing Intellectual Assets: Real-Time Source Code Detection Using ML

Yi Zhang, Ph.D., Senior Manager, Software Engineering, Machine Learning, Netskope 35

SUBMISSIONS ON IT INVESTMENT OPTIMIZATION

Metrics That Matter: How to Analyze, Observe and Measure Agencywide Compute and Data Operations

Jim Cosby, Chief Technology Officer, NetApp 38

Maximizing IT Investment Potential: An Evaluation of DoD/DISA's Technology Utilization

Andrew Scherer, IT Transformation Solution Sales Manager, Federal, ServiceNow 39

DataBee from Comcast Technology Solutions—From Golden Shackles to Golden Age: Breaking the Dependency on Security Vendor-Specific Configurations

Jill Cagliostro, Director of Product Management, Comcast 41

Team Based Planning—A Framework for Modernizing Public Sector Program Funding

William Bunce, Value Stream Management Specialist, Broadcom 42

Embracing Hybrid Multi-Cloud Strategies for Enhanced Mission Efficiency and Cost Reduction

D.R. Carlson, Senior Director of Segment Marketing for the Americas, Equinix 43

SUBMISSIONS ON MEASURE WHAT MATTERS—KEY PERFORMANCE INDICATORS

ExaSwitch: A Revolutionary Solution for Cloudifying the Network

Jason Yoho, Senior Vice President, Public Sector Product and Technology, Lumen Technologies, Inc. 45

KPIs Or It Didn't Happen: Cyber Threat Intelligence Metrics and Efficacy

Jason Baker, Threat Intelligence Consultant, Research and Intelligence Team (GRIT), GuidePoint Security 46

Leveraging Data Analytics to Accelerate the OODA Loop for Enhanced Mission Outcomes in Adversarial Environments

Pragyansmita Nayak Ph.D., Chief Data Scientist, Hitachi Federal 47

Measure What Matters - Key Performance Indicators

Peter Barrett, Director, Federal, Moveworks, Inc. 48

SUBMISSIONS ON UNDEFINED TOPICS

Clearing the IT Fog of War

John Aron, Founder & CEO, Aronetics 50

Past, Present, Future of Appx Abuse

Will Burke, Chief Information Security Officer & Director of Cybersecurity, TSI. 51

Beyond Textual Rules: Revolutionizing DLP with Custom Classifier Training

Jason Bryslawskyj, Ph.D., Senior Machine Learning Scientist, Netskope 52

Quantum-Resistant Security

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies 54

Data Protection at the Edge

Gina Scinta, Deputy Chief Technology Officer, Thales Trusted Cyber Technologies 55

Submissions on

Generative AI

Navigating the Risks: Strengthening DoD Supply Chains Against AI-Induced Vulnerabilities

Jeremy Newberry, Cybersecurity Solutions Architect, Merlin Cyber •
jnewberry@merlincyber.com

ABSTRACT

The rapid integration of generative artificial intelligence (Gen AI) within the Department of Defense (DoD) presents novel vulnerabilities, particularly in the areas of supply chain management. Merlin Cyber addresses the dual-edge nature of AI deployment in defense contexts, highlighting how the automation and data-processing capabilities of AI can inadvertently expose the DoD to new forms of cyber threats. Specifically, the company addresses the unique risks that Gen AI introduces to the supply chain, including data poisoning, model theft and adversarial attacks, which can all undermine the integrity and security of critical defense operations.

Solutions pivot to robust remediation strategies tailored to the defense sector's needs, emphasizing alignment with the zero-trust architecture and the implementation of stringent National Institute of Standards and Technology cybersecurity frameworks. We will outline advanced methodologies for auditing and monitoring AI systems within supply chains to detect and mitigate risks early. Further, the presentation will explore the deployment of decentralized ledger technologies (DLTs) to enhance transparency and traceability in AI-driven processes, thereby securing the provenance of data and AI models used across the DoD.

BIO: Jeremy Newberry boasts a distinguished career spanning 25 years as a network and cybersecurity engineer, architect and strategist, focusing on federal and civilian markets. His extensive background includes hands-on experience in SOC and NOC operations, threat intelligence and cybersecurity. Newberry's forte lies not only in his broad expertise but also in his knack for storytelling, which he leverages to explain complex technical concepts for diverse audiences. As a consummate storyteller and technical evangelist, he excels at bridging the gap between technology and understanding.

Data Management and Future Network Operations with AI/Gen AI/ML

Dean Brewster, Senior Director Product Line Management, Ciena •
dbrewste@ciena.com

ABSTRACT

The Defense Information Systems Agency, or DISA, operates one of the largest network infrastructures in the world supporting critical missions and operations globally. The threat landscape is rapidly changing, and the network needs to be responsive and agile to provide network services where and when it is needed. The integration of artificial intelligence (AI) into network operations and planning can significantly enhance the responsiveness and agility of the network, making it more capable of adapting to changing needs and threats. Developing effective artificial intelligence and advanced analytics is dependent upon high-quality Data Management as the foundation.

Dean Brewster with Ciena, will discuss how large network operators employ Ciena's extensive experience in networking and software development to assist with collecting, organizing, validating and transforming the information about the network into a scalable and reliable source for future artificial intelligence.

This session will share insights on data management in the commercial networking industry and Ciena's own journey within the ML/AI/Gen AI areas. Ciena's experience in this area has led to the development of a platform that integrates and normalizes network data into data sets and creates a vendor agnostic, standards-based extensible datastore. This platform and the analytics developed enables Ciena to provide services to network operators for complex tasks such as network transformation of legacy technologies, fully utilizing existing equipment, and capacity planning all made possible by effective network data management.

Using AI Agents and RAG to Augment the Cyber Warfighter

Ed Sealing, Founder & Chief Technology Officer, SealingTech •
ed.sealing@sealingtech.com

ABSTRACT

Over the last 12 months, SealingTech has conducted research and development efforts into the use of large language models (LLMs) to augment the cyber workforce through retrieval augmented generation (RAG) and AI agents. In this talk, Ed Sealing, chief technology officer at SealingTech, will discuss some of the findings and use cases and demonstrate how AI Agents can interact with DoD cyber defense systems to augment cyber defenders.

BIO: Founder and Chief Technology Officer of Sealing Technologies LLC a Parsons Company, Ed Sealing's journey began when he enlisted in the U.S. Army at age 17. He rose to staff sergeant and served on a Computer Emergency Response Team in Kuwait and Iraq until 2006. Sealing received numerous awards during his military service, including the Bronze Star. After leaving the Army, he continued supporting the DoD as a federal contractor while pursuing his education. He earned an AAS in computer science from the College of Southern Maryland and a Bachelor of Science in cybersecurity from Capitol Tech University while gaining practical experience with various technology companies. Missing the teamwork and camaraderie from his military days, Sealing founded Sealing Technologies in May 2012.

Throughout his career, Sealing has been a steadfast advocate for increasing innovation and accelerating the DoD's cyber tools, both in uniform and as a DoD contractor. Sealing Technologies was acquired in 2023 by Parsons IMP, where Sealing continues to serve as the CTO, overseeing innovations in its hardware technology, artificial intelligence and defensive cyber solutions.

Querying Minds Want to Know: Can a Data Fabric Overcome the Data Agility Challenge Hindering Gen AI Potential?

Terry Dorsey, Senior Data Architect, Denodo • tdorsey@denodo.com

ABSTRACT

The Department of Defense (DoD) is committed to deploying future-ready artificial intelligence (AI) programs and harnessing the full potential of generative AI. To achieve this, it must address common obstacles that impede data agility, including data silos, legacy systems, regulatory compliance issues and diverse data formats from multiple sources. The solution lies in data fabric, a key enabler that connects disparate data sources, formats and structures. Enhanced by data virtualization, data fabric serves as a crucial foundation, securely facilitating easy access to and integration of structured and semi-structured data offering the promise of real-time accessibility. This empowers large language models (LLMs) and retrieval-augmented generation (RAG) with a simplified yet comprehensive view of the organization's informational landscape.

This session will explore how the integration of data fabric, RAG and LLMs can transform the delivery of information to non-technical data users. We will discuss essential platform capabilities necessary to realize a Gen AI-enabled future, including intelligent autonomous agents and on-demand enterprise data querying. Furthermore, in an era where access to LLMs is widespread and foundational models are universally used, we will demonstrate how data agility can provide a strategic decision-making advantage.

BIO: Terry Dorsey has amassed more than 30 years of experience in the information technology field. She currently holds the position of senior data architect and serves as North America's evangelist for Denodo, a leading provider of data virtualization technology.

Dorsey's educational background includes a bachelor's degree in applied mathematics from Carnegie-Mellon University, a master's degree in information science from the University of Pittsburgh and a master's degree in analytics from Harrisburg University of Science and Technology. Presently, she is pursuing a doctoral degree in data science at Harrisburg University, focusing on the application of machine learning and artificial intelligence to unstructured data leveraging graph theory and graph-based algorithms.

Prior to joining Denodo, Dorsey held positions in various industries, including consumer goods, manufacturing, health care, utilities and defense. Throughout her career, she has made significant contributions in the areas of business intelligence, software development and integration. Dorsey has also held enterprise-level architecture roles, where she played a pivotal role in driving practices for enterprise integration, minimizing disruption during cloud and ERP migrations, and spearheading the implementation of self-service analytics while managing costs for delivery. She has also been involved in architecting the technical implementation of AI and ML. Dorsey is experienced in streamlining strategic implementations leveraging data virtualization.

Generative AI for DCO: Why Timing and Signal are Key

Zachary Vaugh, Director, Federal Security Engineering, Vectra AI • zvaughn@vectra.ai

ABSTRACT

The DoD's significant challenge in managing the immense volume of data it collects daily is complicated by the enormous effort needed for proper data labeling for training language models to augment defensive cyber operations. To better assist and automate the need for such labeling, Vectra AI is able to identify all assets and user identities operating in environments and all associated threat detection information in real time using 150+ algorithms in its security-led AI&ML platform. This information, along with the post-process, enriched metadata, has all the necessary attributes and information necessary to properly train security-focused large language models to further assist in DCO efforts. Acting upon this highly effective output, we optimize accessing, cleansing and interpreting data to ensure a continuous pipeline from diverse global and hybrid sources. Our strategy includes integrating various data streams such as open source intelligence (OSINT), public datasets like Common Crawl and CICIDS with internally generated cybersecurity reports and logs into AI analytics platforms.

Clarity of signal is critical when considering AI model training approaches Dell Technologies has partnered with Vectra AI to provide a real-time network detection and response platform powered by true security-led AI comprised of supervised and unsupervised learning methodologies. Vectra AI's coverage is built to identify the behaviors associated with these consistent attacker activities, which enables confident identification of attackers without noise. Vectra aligns these detections to the associated entities observed on the network and their interactions, whether these are hosts, user identities or edge/IOT devices in real-time. This allows defensive cyber operators, analysts and incident responders more upfront context regarding the detections and any of the participating components without adding voluminous amounts of purely anomalous indicators to investigate and consume time and attention. This type of signal being utilized at-scale within DoD and IC agencies is key to ensuring that models being trained to assist and augment DCO activities are automatically being provided the proper attributes and context via initial, real-time AI & ML processing, which far outpaces human capacity. By adopting the combined capabilities of Vectra's cybersecurity platform and Dell Technologies' infrastructure, we tackle the labeling challenges using supervised (e.g., classifying), unsupervised (e.g., clustering), and semi-supervised learning techniques (e.g., bootstrapping, co-training). This approach improves scalability and adaptability but also enhances cyber threat detection, thereby protecting the integrity of the DoDIN and strengthening national security.

BIO: Zachary Vaughn has been supporting federal agencies for more than 17 years with network and identity threat detection and response, access and identity management, web and application security, and virtualization of key infrastructure.

Accelerate Your Generative AI using ZSP Identity Security to Reduce Risk and Speed the Mission

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

ABSTRACT

At the speed of rapidly shifting artificial intelligence (AI) models and data, the challenge remains for the joint mission on how to leverage generative AI in way to reduce risk and accelerate the mission. Generative AI, like machine learning and other AI models, depends on untampered data to ensure outcomes meet the needs of the mission. Risk further exists for outcome manipulation with improper access to models and training data pools.

To assure the success of the generative AI mission, identity security—particularly assurance of zero standing privilege—is crucial to the mission. Identity security, when aligning with the generative AI tools and data, ensures that the training data, models and AI response outcomes operate with reduced risk and speed of the mission. When employing zero standing privilege with generative AI systems, it empowers risk reduction for operators working with AI data and models as well as assures minimal access for NPE agents doing continuous deployment of the AI system. This session will enable integration of zero standing privilege into generative AI environment to provide speed of access via governed service agent access and facilitate insider threat mitigation resulting in generative AI that is focused on the success of the joint mission.

Attendees of this session will learn and apply new capabilities including:

- Learn the approaches to apply zero standing privilege against service principals and other NPE agents for access enforcement and insider threat mitigation in Azure OpenAI environment.
- Develop methods for implementation controls for zero standing privilege using identity security in your generative AI environment.
- Experience demonstration of existing operational zero standing privilege capabilities protecting service principals to rapidly mitigate cyber and insider threat risks against Azure OpenAI and similar environments.

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 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 the current role at Saviynt, focus is on protecting employees and business partner identities for public sector agencies to reduce cyber risk and 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.

Decoding the Hype: Practical Applications of Large Language Models in Cybersecurity

Yihua Liao, Senior Director, AI Labs, Netskope • yliao@netskope.com

ABSTRACT

The current fascination with large language models (LLMs) has ignited enthusiasm and skepticism in the tech community. While the hype is undeniable, how can cybersecurity professionals actually benefit from these models?

Our team embarked on a journey to answer this question. Utilizing an open-source model named Llama2, we fine-tuned it with a specialized knowledge base to explore a variety of applications within the cybersecurity landscape. The use cases ranged from employing chatbots for automating support queries to utilizing analytics for a deeper understanding of security stances and summarizing hefty threat reports into easily consumable information.

So, what worked and what fell short? This session aims to unpack these questions, providing attendees with concrete metrics and methodologies for evaluating the efficacy of LLMs in cybersecurity tasks. We will share the criteria for determining the success or failure of each use case, along with lessons learned from our trials and tribulations.

Specifically, the session will cover and demo:

- **Chatbots for Product Support:** Streamlining issue resolution by automating common queries.
- **Interactive Analytics:** Leveraging LLMs to gain granular insights into your security posture.
- **Threat Report Summaries:** Condensing complex reports into actionable intelligence.
- **Contextualizing Threats and Vulnerabilities:** Using LLMs to provide deeper insights into the threat landscape.
- **Dynamic Policy Recommendations:** Adapting to evolving threats through real-time, data-driven guidelines.
- **Documentation Quality Assurance:** Employing LLMs to enhance the accuracy and readability of internal documents.

By the end of the session, attendees will have a well-rounded perspective on the opportunities and challenges tied to the implementation of LLMs in cybersecurity. Moreover, the discussion will be geared toward offering actionable takeaways that you can apply in your cybersecurity endeavors.

Through this session, we aim to cut through the noise surrounding LLMs and provide a comprehensive guide for cybersecurity professionals looking to harness the power of generative AI. We welcome you to join us in demystifying the buzz and diving deep into the practicalities of LLMs for cybersecurity.

BIO: Yihua Liao, Ph.D., serves as the senior director of AI Labs at Netskope, where he leads a specialized team of machine learning scientists and engineers. He is at the forefront of innovation, applying cutting-edge machine learning technologies that span computer vision, natural language processing (NLP) and large language models (LLMs). Prior to his role at Netskope, Liao helmed data science teams at industry giants such as Uber, Facebook and Microsoft, tackling complex issues in security, fraud, and risk management. He earned his Ph.D. in computer science from the University of California, Davis.

Utilizing AI to Unlock Data Essential to Mission Success

Marlin McFate, Public Sector Chief Technology Officer and Chief Information Security Officer Cohesity • cmarlin.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 gen AI, tailored to address contemporary cybersecurity challenges. Delve into the significance of staying up to date with the latest AI developments, ensuring relevance and efficacy in combating emerging threats.
- AI-Driven Data Analysis: Uncover the capabilities of AI models, such as Cohesity Turing and GAIA, in analyzing vast datasets for actionable insights. Witness how these solutions facilitate efficient data retrieval, vectorization, and metadata creation, enabling seamless analysis without extensive training requirements.
- Mitigating Risks: Explore strategies to reduce AI-related hallucinations, inaccuracies and other drawbacks ensuring the reliability and integrity of findings. Understand the importance of validating AI-generated insights through cohesive methodologies and rigorous scrutiny.

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

BIO: 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, Marlin was the technical director of the Advanced Technology Group in the Office of The CTO as 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.

Adobe & The Impact of Generative AI in Information Operations

Michelle Woolford, Adobe Account Executive, Carahsoft Technology Corp.

• woolford@adobe.com

ABSTRACT

In today's information environment, the joint force commanders' ability to inform the public at the same pace as the media is complicated by the ability for anyone to produce content quickly and become instant journalists without validating facts or maintaining authenticity. Building and maintaining public trust, especially during military operations, is undermined by vast misinformation spread across multiple communications channels.

Part of the challenge is keeping pace with the demand for content from members of the military community and the public while delivering engaging experiences that can change perceptions and build support for military operations.

Generative AI has the potential to revolutionize information operations by enabling communicators at every level to produce and deliver highly personalized content at speed and scale. This transformative technology is being incorporated into digital media editing applications, web content management systems and data analytics platforms as an effective co-pilot to disseminate information rapidly. Simple text prompts and a few mouse clicks can generate high-quality messaging and summarize data to make informed decisions.

While Generative AI can advance information operations capabilities across the DoD, it can also be leveraged by our nation's adversaries to manipulate content and sow distrust. Efforts are being made across the technology industry to address the prevalence of misleading information online through the development of technical standards for certifying media content's source and history (or provenance). Procuring and deploying technology solutions that follow these standards and train their large language models (LLMs) based on commercially safe sources supports the responsible use of generative AI capabilities.

Join Adobe to explore how generative AI is shaping the information environment and how it is being incorporated today into image editing software, web content, and digital asset management systems to safely bring advanced capabilities across the DoD.

BIO: Michelle Woolford is the Adobe account executive for the U.S. Navy, Marine Corps and 4th Estate supporting the Adobe Digital Experience solutions. Throughout her career, Woolford has been solely dedicated to digital transformation within the Department of Defense (DoD). Woolford has passion around finding solutions to match the DoD mission objectives and modernization efforts. Through her team's alignment to the mission, she understands the value the correct tools can bring and the importance of building strategic partnerships.

Intersection of AI and Security

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

ABSTRACT

Artificial intelligence (AI) is rapidly transforming our world, from the way we work to the way we interact with machines. 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 National Institute of Standards and Technology 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, she 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.

Identity and AI Trends Driving Zero Trust Programs in the DoD

James Imanian, Senior Director, CyberArk Solutions • james.imanian@cyberark.com

ABSTRACT

New identities, environments and attack methods require a modern adaptive cyber defense to secure the Department of Defense's (DoD's) most valuable resources. Cyber defenders must also incorporate AI into their defensive capabilities as adversaries integrate AI into their attack tool set.

Employees and third-party vendors work from anywhere and on ubiquitous devices. Hybrid and cloud environments are massively complex for an organization to secure and human and machine identities can be assigned high-risk permissions to become vulnerable "privileged users." Moreover, avenues for attack, such as AI-powered ransomware and complicated software supply chain attacks, are constantly becoming more advanced.

Join our session for insights on:

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

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

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

Transforming Security Through Language Models

Jonathan Mullin, Chief Technology Officer, DCI Solutions • jmullin@dci-solutions.com

ABSTRACT

The power of generative artificial intelligence (Gen AI) is the ability to adapt to almost any data type, as long as there is enough data to build a statistical model upon which deep non-linear relationships can be established. This is a perfect for cybersecurity applications, which can generate an absolute deluge of data. Using this massive data resource learning models can create internal representations in lieu of hard labels used in traditional machine learning. The only limitation is traditional Gen AI approaches require billions of parameters and kilowatts of power to provide insight into cyber data.

Our approach at DCI solutions seeks to bridge the power of Gen AI with a scalable architecture capable of running on device not locked away in the cloud. CyFormer harnesses the power of AI for the purpose of transforming cybersecurity. CyFormer is powered by state-of-the-art AI models to defend against never-before-seen cyberattacks at both the network and host level. CyFormer covers all aspects of the cyber threat, both from inside and outside adversaries. The basis of our stance is not to rely on known threats of the past, but to model your network to find who can be trusted now and into the future. CyFormer applies seamlessly as part of any network architecture and is a flawless technology insertion into a zero-trust architecture providing visibility and analytics.

CyFormer is a signatureless agent that feeds off network data and learns what “normal” network behavior is for a customer. From there, the CyFormer model can identify activity outside the normal baseline, tag those activities and send alerts through JSON messaging.

CyFormer is custom built specifically to address the unique challenges of cyber data. Our models develop internal representations of each entity and their relationships, thus allowing a fast, scalable identification when unusual events happen. CyFormer can respond independently or via teaming with security professionals through reports explaining the reasoning for the alerts. This methodology helps to build deep trust while augmenting a security team to effectively investigate the vast scale of cyber data in a meaningful, systematic, and straightforward way.

DCI is now pushing the boundary of automated cyber defenses by combining CyFormer with reinforcement learning (RL) approaches. This combination is transformative. The combination of a language model to drive and inform the actions of the RL agent allows for a dynamic interplay between each allowing for both specialization of each model and teaming with a common goal.

CyFormer allowed us to move detection to the left of indicator of compromise (IOC), the combination of RL pushes remediation even further to the left denying adversaries the chance to even dwell in your environment.

BIO: Jonathan Mullin, Ph.D., has 20+ years identifying and delivering solutions for the DoD's most challenging problems in machine learning, high performance computing, quantum and material sciences, data science and cybersecurity. Using HPC and AI/ML to push what is possible and meet the government's unique challenges, unclassified and classified. He has 10+ years leading teams to deliver bespoke data analysis tools for a variety of unstructured and structured data sets. Work has focused on technical leadership and management of programs at academic institutions, startup companies, AFRL, NRL, ARL and the Army C5ISR Center of Excellence.

Cybersecurity in the Age of AI: Fusing Zero Trust with Universal Confidential Computing

Dwayne Hoover, Vice President, Solutions Engineering, Anjuna Security •
dwayne.hoover@anjuna.io

ABSTRACT

In an era marked by unprecedented data volumes and breakneck advancements in artificial intelligence (AI), government agencies face the dual challenge of harnessing this technology's unprecedented power while safeguarding sensitive information against never-ending and rapidly evolving threats.

This breakout session delves into the intersection of two cutting-edge concepts: zero-trust architecture and universal confidential computing, offering insights into how they synergize to bolster the security posture of government AI initiatives. By adopting by default zero trust—an approach that assumes that no entity, whether inside or outside the network, should be trusted, coupled with universal confidential computing—a new technology category emerges that offers cloud and application agnostic security and data privacy through a hardware-rooted trust. Now government agencies can establish a dominant security posture.

Join us as we explore practical strategies for implementing zero-trust principles alongside universal confidential computing to secure AI data processing and analysis workflows, ensuring data confidentiality, integrity and privacy at every stage. Discover how this holistic approach empowers government organizations to embrace AI innovation with resilience, trust and confidence, setting the stage for the future of the cyber mission.

BIO: Dwayne Hoover is the vice president of solutions engineering at Anjuna Security, where he helps customers secure data in every state to create a zero-trust environment for code and data. Before Anjuna, Hoover led global sales, service delivery and customer success teams across diverse industries, ranging from application security to observability. In addition, he's built and deployed many big data and analytics solutions for federal and commercial clientele as a consultant who pushed modernization. In his free time, he enjoys being terrible at golf, spending time with his family and hacking/exploring emerging technology.

Data Driven AI: Practical Advice for Successful Results

Ron Rintala, President & CEO, DataInFormation – Liberty Source •
ron.rintala@liberty-source.com

ABSTRACT

Artificial intelligence (AI) technology has been a valuable business tool for years, but since OpenAI launched ChatGPT in November 2022, interest in AI has soared—and that's putting technology partners under increasing pressure to make an investment in AI systems to keep their companies competitive and relevant.

However, without a clear understanding of the overall business strategy, a clear definition of what opportunity or business problem you are addressing, or how it will fit in with the rest of your technology architecture, an investment in AI will not yield the business outcomes you desire. In this discussion, we will discuss how to approach AI as a strategic enabler of business strategy and explain the necessary preparations you must make before deploying AI platforms in your organization. We will also provide answers to important questions:

- Why an effective AI solution is a strategy enabler, not a stand-alone initiative
- Why data is the key to success
- What defines effective data preparation

BIO: Ron Rintala is a globally recognized thought leader specializing in the practical application of data and analytics to drive significant measurable improvements in operations, sales and marketing, customer experience, technology and risk management for major financial services and insurance companies. Currently, Rintala is leading Liberty Source and the DataInFormation suite of products focused on mobilizing business leaders, data teams and analytics teams to drive pragmatic, impactful and scalable use cases aimed at the realization of AI/BI/ML value using high-feature, highly governed unstructured and structured data. Rintala has a BS in engineering from the U.S. Military Academy at West Point and a Juris Doctorate from the University of Denver Sturm College of Law.

Enhancing Cybersecurity with Cloudera: A Generative AI Approach for the Department of Defense

Tej Tenmattam, Principal Solutions Engineer, Cloudera Government Solutions •
ttenmattam@cloudera.com

ABSTRACT

The Department of Defense (DoD) is at the forefront of an AI revolution, seeking to harness the power of artificial intelligence (AI), machine learning (ML) and generative AI (Gen AI) to transform its operations. A critical challenge in this endeavor is the need for high-quality data to train language learning models, particularly in the context of cybersecurity. The Defense Information Systems Agency (DISA) faces a pressing issue with the vast amount of cyber data it ingests daily, which requires effective labeling to train models capable of identifying known attacks and detecting potential new zero-day threats.

Cloudera offers a comprehensive solution to this challenge, providing a platform that enables the DoD to establish a continuous data pipeline across global and hybrid data sources. By leveraging Cloudera's advanced data management and analytics capabilities, the DoD can accelerate data access and ensure the quality of data feeding into AI models. This is crucial for deploying future-ready AI programs that can effectively analyze cyber log data, enhancing the capabilities of DISA's analysts in defending the DoD Information Network (DoDIN).

Cloudera's platform supports the development and deployment of generative AI/LLMs, which can automate the process of data labeling and generate synthetic data for training models. This reduces the manual effort required and increases the efficiency of training robust language learning models. Furthermore, Cloudera's commitment to security ensures that sensitive data is managed and analyzed with the highest level of protection, maintaining the integrity of DoD's cybersecurity efforts.

In this presentation, we will explore how Cloudera's solution can be leveraged to address the DoD's challenges in utilizing cyber data for training language learning models. We will discuss the importance of a continuous data pipeline, the role of Gen AI in augmenting analyst capabilities and the considerations for deploying AI programs that are future-ready and effective in detecting and defending against cyber threats.

BIO: Tej Tenmattam is a dynamic leader with expertise in building and scaling software sales, presales and professional services organizations. With a strategic focus on organizational and business strategy, Tenmattam has a proven track record of driving growth and transformation in the technology sector.

Specializing in disruptive technologies and open-source solutions, Tenmattam excels in leveraging platforms like cloud foundry and infrastructure as a service (IaaS) to drive innovation. Their proficiency in cloud computing, big data analytics, AI/ML and data science enables them to deliver cutting-edge solutions that meet evolving business needs.

Fully Trained Cyber AI Engine for Advanced Threat Detection

Eric Irizarry, Security Solutions Architect, MFGS, Inc. • eric.irizarry@mfgsinc.com

ABSTRACT

Cybersecurity Landscape: The threat landscape is constantly evolving due to sophisticated cyber attackers and technological expansion. IoT devices, cloud computing and mobile tech create new attack vectors. These threats, often AI-driven, bypass traditional security. Proactive strategies like AI-based behavioral analytics are crucial for risk mitigation.

Threat-Informed Approach: To combat cyber threats, organizations need a global signal analytics approach. It uncovers malicious network traffic, identifies early attack signs and enhances defenses. Analyzing external internet traffic beyond organizational perimeters provides comprehensive threat visibility, minimizing blind spots and improving overall security efficacy.

BIO: Eric Irizarry is a security solutions architect with MFGS, Inc., where he provides pre-sales security solutions and technical support for DoD customers. Irizarry began his cyber career with CaterAir, Inc., where he excelled as a network engineer. With more than 20 years of IT and cybersecurity experience, his background spans network design and security architecture, risk assessments, vulnerability management, incident response and policy across government and commercial industries. He holds a variety of certifications (CISSP, CEH, CCNA).

Enhancing DoD's AI Threat Intelligence with Comprehensive Datasets

Tim LeMaster, Vice President, Worldwide Systems Engineering, Lookout •
tim.lemaster@lookout.com

ABSTRACT

The Department of Defense (DoD) has reportedly experienced a staggering 12,000 cyber incidents since 2015. This relentless assault from cybercriminals and nation-state actors on classified data and DoD systems is not just a security concern, but a direct threat to the critical infrastructure and the safety of U.S. citizens.

Artificial intelligence (AI) is a powerful tool for combating these ongoing threats, enabling insights to enhance threat detection and response capabilities. However, the DoD must build future-ready AI programs based on quality datasets that account for all data types, including mobile data.

In today's digital era, many government employees use mobile devices during work, whether agency-issued or employee-owned. With more than half of personal mobile devices targeted by phishing attacks in 2022, mobile data is a threat vector that must be considered when training AI models and increasing analysts' ability to defend critical DoD systems.

Over the last decade, Lookout has collected the world's most extensive mobile threat dataset, comprising telemetry from more than 210 million devices and 280 million apps and insights from more than 410 million URLs and 17,500 SaaS apps.

In this session, Tim LeMaster, Lookout's vice president, worldwide systems engineering, will:

- Discuss best data practices for strengthening AI models and improving their ability to identify and correlate cyberattacks.
- Highlight how mobile threat intel can strengthen the DoD's data pipeline and enable a better understanding of the latest criminal tactics threatening national security.
- Examine Lookout's mobile dataset to gain insights into the new tactics being leveraged by criminals.

BIO: Tim LeMaster is a veteran of the networking, cybersecurity and infrastructure space. He spent 14 years at Juniper Networks as the federal systems engineering director before coming to Lookout in December 2014. Before Juniper, he held various roles at General Dynamics and NET, ranging from network modeling to network operations. LeMaster also served 12 years in the U.S. Air Force. As the vice president, worldwide systems engineering at Lookout, he helps customers understand the mobile security threat landscape and how to address the threats.

VMware Private AI Foundation

Tommy Dammer, Senior Solutions Engineer, VMware, Broadcom •
tommy.dammer@broadcom.com

ABSTRACT

Broadcom and NVIDIA have collaborated to develop a joint generative AI platform called VMware Private AI Foundation with NVIDIA.

This joint Gen AI platform enables enterprises to fine-tune large language models (LLMs), deploy retrieval augmented generation (RAG) workflows, and run inference workloads in their data centers, addressing privacy, choice, cost, performance and compliance concerns. VMware Private AI Foundation with NVIDIA simplifies Gen AI deployments for enterprises by offering an intuitive automation tool, deep learning VM images, vector database and GPU monitoring capabilities.

Components of this platform

Here are the key components that enable organizations to securely harness the power of generative AI.

- **VMware Cloud Foundation**—VMware Cloud Foundation offers a full-stack scalable, software-defined architecture designed to deliver a self-service unified platform and leverage an automated IT environment that simplifies the deployment and management of all workloads utilizing VMs, containers and AI technologies. The versatility offered through this architecture enables cloud admins to utilize different workload domains, which can each be customized to support specific workload types, optimizing for workload performance and resource utilization, specifically GPUs.
- **NVIDIA AI Enterprise**—NVIDIA AI Enterprise is a secure, end-to-end, cloud native software platform that accelerates the data science pipeline and streamlines development and deployment of production-grade AI applications, including generative AI, computer vision, speech AI and more. NVIDIA NIM allows enterprises to run inference on a range from LLMs from NVIDIA models to community models.
- **Major Server OEM Support**—Major server OEMs such as Dell, Lenovo and HPE support this platform.

BIO: Tommy Dammer is the VMware by Broadcom senior solutions engineer, covering DoD 4th Estate Agencies. Prior to Broadcom, Dammer had a long career working for a joint service provider and other 4th Estate Agencies.

DataBee from Comcast Technology Solutions—Cracking the Code with OCSF: Making Machine Learning a Symphony of Success!

Scott Miserendino, Vice President of Engineering Cyber, Comcast •
scott_miserendino@comcast.com

ABSTRACT

Powerful tools exist today for artificial intelligence (AI) model creation and tuning, but the quality of the data used for training is highly coupled to the accuracy and reliability of models created from it. In a typical environment, nearly 80% of time spent on AI is in the data preparation phases. Considering the added complexity of data sources from a broad set of COTS, GOTS and custom tools the government employs across its infrastructure, the task of developing the data set seems daunting. It's time to unburden government data scientists and their partners so they can direct their focus to the valuable tasks of developing and applying AI to solve the cyber challenges of today and the future.

We'll cover the principles, practices, patterns and other opportunities that will help DISA create these critical data sets, despite the variety of sources. Going beyond simple log translation, data needs a defined standard to map to, it should be deduplicated, and it needs to be enhanced to identify unique users and devices since they may be referred to differently in various logs. We'll cover an example of data from different sources being transformed by DataBee and show how it becomes the ideal precursor for the AI model generation process.

By the end of the talk, we'll understand a roadmap for building a quality data source to base machine learning on, and how this standard can enable more collaboration and ultimately sharing of models across the DoD.

BIO: Scott Miserendino, Ph.D., leads DataBee's cybersecurity engineering, analytics and product development teams. He is responsible for building cybersecurity solutions based on DataBee's security data fabric. As a passionate leader, researcher and developer, he enables his team of data scientists and software engineers to solve some of the cybersecurity industry's hardest problems through the application and invention of cutting-edge technology.

Since 2017, he has overseen the development and operational deployment of multiple cybersecurity products. Prior to helping establish the DataBee product, Miserendino lead the engineering team for BluVector's advance network detection and response and automated threat hunting products. BluVector, a security startup spun out of Northrop Grumman, was acquired by Comcast in 2019. Dr. Miserendino has spent more than 10 years working on advance network sensors, cybersecurity analytics and various projects for the U.S. Department of Defense and intelligence community.

Miserendino earned a bachelor's degree in electrical engineering and mathematical sciences from Johns Hopkins University and a masters and doctorate in electrical engineering from the California Institute of Technology. He has published more than 10 scholarly papers, one book chapter, and holds three U.S. patents. He is a senior member of the Institute for Electrical and Electronic Engineers (IEEE).

The New AI Data Frontier: How to Secure, Optimize and Expedite Data Operations for AI

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

ABSTRACT

Artificial intelligence (AI) data is growing at ever increasing rates for federal agencies, and is constantly becoming more challenging to store, manage and process in a timely and secure fashion. New methods and technologies are evolving that can optimize data by reducing the footprint, cost and time to process and manage. At the same time, security threats from cyber and ransomware attacks are ever increasing, which is demanding stronger data protection, backup and recovery methods. In this session we will discuss new capabilities around storing, securing, managing and optimizing AI data across hybrid multi-cloud environments.

BIO: Jim Cosby is a CTO at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on data management, 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.

Securing Intellectual Assets: Real-Time Source Code Detection Using ML

Yi Zhang, Ph.D., Senior Manager, Software Engineering, Machine Learning , Netskope • yzhang@netskope.com

ABSTRACT

As enterprises transition their source code repositories to cloud platforms, the secure management of such intellectual assets is becoming increasingly vital. Recent incidents, like the unintended leakage of source code through conversational artificial intelligence (AI) models, underline the need for robust data privacy controls. This is especially true when AI-driven cybersecurity mechanisms are rapidly becoming the norm.

This session aims to educate attendees on the challenges and solutions in identifying source code within textual data—a crucial element for implementing effective data loss prevention (DLP) frameworks.

We will focus on a hands-on approach that involves utilizing machine learning techniques to classify source code. Specifically, attendees will learn how to:

1. Understand the complexities involved in programmatically detecting source code within text streams.
2. Choose appropriate algorithms and design an architecture for building a machine-learning classifier tailored for source code recognition.
3. Optimize the model for real-time execution, a necessity for immediate enforcement of source code policies in live environments.

Key takeaways from this presentation will include:

- Techniques for feature extraction using specialized code vocabulary.
- Guidelines for training a decision tree classifier, focusing on both accuracy and computational efficiency.
- Metrics and live examples to evaluate the model's real-time performance and effectiveness in preventing data leaks.

By the end of this session, attendees will have a clear roadmap for integrating machine learning-based source code classification into their existing DLP strategies. They will gain the theoretical knowledge and practical skills needed to safeguard their intellectual property in today's cloud-centric landscape.

BIO: Yi Zhang, Ph.D., serves as a distinguished machine learning scientist at Netskope's AI Labs, where she leverages more than two decades of expertise in machine learning and data science to address challenges in system reliability and security. Her research focus encompasses a range of critical areas, including malware detection, vulnerability analysis, sensitive data protection, time-series anomaly detection, behavior analytics and AIOps. Prior to joining Netskope, Zhang held key roles at leading research institutions such as GE Global Research and Qualcomm Silicon Valley Research, as well as security startups like Forescout. She received her Ph.D. in computer engineering from Carnegie Mellon University.

Submissions on

IT Investment Optimization

Metrics That Matter: How to Analyze, Observe and Measure Agencywide Compute and Data Operations

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

ABSTRACT

IT infrastructure and operations are rapidly increasing every day. The measurement of diverse compute and data elements in hybrid-multi cloud and multi-domain environments is becoming overwhelming to visibly observe and measure. Attend this session to learn about new technology that can span hybrid-multi cloud environments to assess and measure these elements to produce accurate metrics of utilization to help any agency accomplish their mission more efficiently and cost effectively.

BIO: Jim Cosby is a CTO at NetApp U.S. Public Sector and has more than 25 years of technology engineering and leadership experience supporting a variety of federal and Department of Defense agencies. Cosby has focused on data management, 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.

Maximizing IT Investment Potential: An Evaluation of DoD/DISA's Technology Utilization

Andrew Scherer, IT Transformation Solution Sales Manager, Federal, ServiceNow •
Andrew.Scherer@servicenow.com

ABSTRACT

The Defense Information Systems Agency (DISA) faces critical challenges in managing a vast array of IT services and software provided by numerous vendors. Given the complexity and diversity of these services, it can be challenging for DISA to maintain an up to date understanding of the terms and conditions of each vendor agreement. To ensure operational efficiency and effectiveness in supporting warfighter needs, DISA must proactively divest from outdated technologies that no longer meet these critical demands. Additionally, the agency faces the need to identify and eliminate redundant systems or tools that complicate operations and inflate costs.

This session will explore a strategic approach to addressing the technical and business imperatives in driving operational excellence, cost savings, compliance and risk reduction across IT investments. We will review how an integrated approach can allow DISA to gain comprehensive visibility into its IT asset portfolio, enabling detailed insights into each service and software application in use. We will demonstrate how software asset management will allow DISA to track and manage software licenses, compliance and expenditures, ensuring optimal utilization and adherence to contractual terms and conditions. Additionally, we will explore how application portfolio management facilitates application rationalization, identifying redundant or obsolete technologies, and enabling informed decision-making regarding technology divestment.

By leveraging this dual approach, DISA can streamline its IT infrastructure, reducing unnecessary costs and simplifying operations. The insights provided by this solution also empower DISA to measure the effectiveness of its IT investments accurately and ensure they align with the evolving requirements of mission partners. Ultimately, this strategic management of IT resources enhances operational readiness and delivers greater value, supporting the agency's mission to equip warfighters with the best possible technological tools in connected and disconnected environments.

We will examine the following three issues:

PROBLEM 1 - Complex Vendor Management and Compliance

Managing a myriad of vendor relationships and their associated contracts poses significant challenges. Each vendor agreement comes with its own set of terms and conditions, making it difficult for agencies to

maintain compliance and manage renewals efficiently. The complexity is compounded by the need to ensure that all contractual obligations are met while optimizing cost and service delivery. This scenario demands robust management tools that can automate and streamline vendor contract tracking, compliance checks, and the updating of contractual terms.

PROBLEM 2 - Optimization and Rationalization of IT Assets

Federal agencies are often saddled with outdated, redundant or simply underutilized IT systems and applications. This not only leads to increased operational costs but also hampers agility and effectiveness in mission-critical operations. The challenge is to identify and divest from these inefficient assets to streamline operations and focus resources on technologies that directly enhance capabilities and service delivery. Rationalizing the IT asset portfolio requires a strategic approach to assess each asset's value, usage, and impact on the agency's overall technological ecosystem.

PROBLEM 3 - Evaluation and Reallocation of IT Investments

The ability to effectively measure the performance and value of its IT investments is crucial for ensuring that these resources yield the best possible outcomes for mission partners. However, the absence of detailed insights into the effectiveness of these investments can lead to misallocated resources, underperforming technologies, and suboptimal support for critical operations. There needs to be a systematic method to evaluate each technology investment, ensuring that spending is aligned with strategic objectives and that adjustments can be made to adapt to changing mission needs and technological landscapes.

BIO: Andrew Scherer, based in Washington D.C., boasts 25 years of experience in the financial and federal sales domains. His impressive track record includes 18+ years of selling IT services directly to the Department of Defense (DoD) and civilian agencies. Scherer's forte lies in crafting customized solutions that yield powerful outcomes, all while keeping a keen eye on budget constraints and return on investment (ROI).

His passion lies in collaborating with DoD clients to deliver enterprise-wide solutions that not only advance their mission but also equip them with world-class tools to enhance their work environment.

DataBee from Comcast Technology Solutions—From Golden Shackles to Golden Age: Breaking the Dependency on Security Vendor-Specific Configurations

Jill Cagliostro, Director of Product Management, Comcast •
jillian_cagliostro@comcast.com

ABSTRACT

Once a security tool is fully deployed in the network and environment, it becomes near impossible to change vendors without significant operational impact. The impact is more than just replacing the existing solution, it's also updating all upstream and downstream integration points, such as custom detection content or log parsers. This leads to potential gaps in coverage due to limitations in the deployed tooling and the tools desired. Not to mention, those golden shackles really hurt the wallet, or security budget.

We'll cover the principles, practices, patterns and other opportunities that help DISA unshackle the golden handcuffs to get the full potential out of your IT investment by beginning your journey to a vendor agnostic approach to security. Leverage Zeek offerings via BluVector and standardizing to open-source detection formats like Sigma detections into your existing security tooling and operations. Learn how to leverage the metadata of Sigma Detections such as MITRE ATT&CK tags to chain together patterns of events. We'll cover an example of automating threat hunting activities to reduce the noise by chaining together Sigma Detections with Zeek logs in BluVector to look for evasive malware and modeling Advanced Persistent Threats.

By the end of the talk, we'll understand a roadmap for how we can transform into open architecture that's vendor agnostic, enabling the offboarding of redundant systems with ease. Enter the Golden Age of security operations by optimizing for your use cases, not which vendor was there first.

BIO: Jill Cagliostro is a customer-obsessed product leader in the security industry. Her deep understanding of customers' pain points comes from her own real-world experience in the SOC. She started her career at a large financial institution where she focused on operationalizing and architecting their enterprise SIEM solution and establishing their threat intelligence program. She brought her experience to Anomali, where she led the customer success team for the East & federal region. She pivoted to product manager to get closer to the product and ensure that product strategy aligns with customer needs at companies like Anomali, Recorded Future, Splunk and most recently DataBee where she is a director of product management. She is a "Double Jacket" having completed both her undergraduate and graduate studies at Georgia Tech in computer science and cybersecurity, respectively.

Team Based Planning—A Framework for Modernizing Public Sector Program Funding

William Bunce, Value Stream Management Specialist, Broadcom •
william.bunce@broadcom.com

ABSTRACT

When it comes technology in the DoD, it seems virtually everything has changed in the past couple years. Why is it that the way capital planning and funding are managed looks the same as it did decades ago? In many ways, teams are still working with a traditional capital planning and investment control model that emerged when client/server computing was all the rage. These legacy approaches are inefficient and wasteful and are fundamentally misaligned with the modern technologies and realities of today's DoD agencies. This session introduces a new approach to program planning, one that is focused on teams rather than projects. Find out why this new framework is vital, learn about the three pillars of success and get practical tips on getting started.

BIO: With more than 25 years of experience implementing IT in DoD, Bill Bunce helps DoD organizations optimize their IT portfolios to align business and IT goals using Value Stream Management. Value Stream Management extends beyond DevSecOps and operational roles to include capabilities and metrics that matter most to mission leaders.

Embracing Hybrid Multi-Cloud Strategies for Enhanced Mission Efficiency and Cost Reduction

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

ABSTRACT

With a multitude of IT vendors powering DISA services, understanding the terms and conditions of each solution becomes a challenge. Discover how DISA can best leverage software-defined networking, hybrid multi-cloud strategies, and interconnection capabilities to dynamically deliver services, efficiently operate legacy applications and rapidly deliver mission-critical data to the warfighter. Gain detailed insights into how vendor-neutral data center options can support DISA's IT investment for enhanced effectiveness, simplified operations and reduced costs.

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

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

Submissions on

Key Performance Indicators

ExaSwitch: A Revolutionary Solution for Cloudifying the Network

Jason Yoho, Senior Vice President, Public Sector Product and Technology, Lumen Technologies, Inc. • jason.yoho@lumen.com

ABSTRACT

Lumen introduces ExaSwitch™, a revolutionary network interconnection system that redefines the DoD's network infrastructure. ExaSwitch is engineered to route traffic between networks quickly and dynamically, eliminating the need for third-party intervention. Tailored to meet the evolving needs of the DoD community, it promises to reduce network costs, boost performance and agility, fortify security and streamline complexity.

ExaSwitch is a testament to Lumen's commitment to innovation, offering a high-performance, low-latency and scalable solution that enables cloud-native applications and services. With the ability to handle up to 400 Gbps of throughput per port, and support for a wide range of protocols and interfaces, such as Ethernet, IP, MPLS and VSLAN, ExaSwitch is poised to revolutionize the DoD's network infrastructure.

By harnessing Lumen's edge computing and network orchestration, ExaSwitch ensures unparalleled efficiency and security. It enables the DoD to deploy and manage network resources on demand, optimize network performance and reliability, and safeguard network traffic against cyber threats.

As the DoD embraces commercial innovation, ExaSwitch is poised to ensure they have access to the world's most advanced network. Witness ExaSwitch at the SIGNAL Innovation Showcase, where it will demonstrate new standards for situational awareness, operational excellence, and innovation within the DoD community.

BIO: Jason Yoho joined Lumen in 2023 as senior vice president to lead the Public Sector Product and Technology team. Yoho is a technology solutions leader with a 20-year career facilitating understanding and adoption of cloud technologies to transform customers' businesses. He is passionate about building high performance teams to define and deliver product stories that capture mindshare and delight customers. Trust, innovation and winning are Yoho's core operating values for cultivating success. He helped build and lead the global internet service provider organization at Sun Microsystems, which created the market for cloud managed services like disaster recovery, business continuity, data storage, identity management and network security. Yoho helped several startups define strategies and build plans for success, attracting more than $80 million in venture capital for data center management, cloud storage and big data markets. Before joining Lumen, Yoho was focused on helping the public sector architect and utilize the cloud for regulatory and compliance goals.

KPIs Or It Didn't Happen: Cyber Threat Intelligence Metrics and Efficacy

Jason Baker, Threat Intelligence Consultant, Research and Intelligence Team (GRIT), GuidePoint Security • allegra.novalis@guidepointsecurity.com

ABSTRACT

Despite entering our lexicon nearly two decades ago, objective measurements and metrics of cyber threat intelligence (CTI) remain ambiguous, highly variable or infrequently adopted. This inconsistency is in part due to varying business and information needs that drive disparate CTI programs, our failure to adopt a universal standard and an occupational culture that frequently "falls back" on U.S. intelligence community (IC) practices in lieu of independent doctrine. This presentation will seek to review contemporary CTI metrics and their purpose, identify deviations from the IC practices, explain common pitfalls that lead to issues in evaluating program efficacy, and review the "lifecycle" of CTI metrics in organizations of varying maturity levels. Attendees will leave with reliable measures to evaluate CTI program efficacy, awareness of issues to avoid and be empowered to pursue contemporary approaches to metrics, evaluation, and CTI program management.

To begin, we will present CTI metrics as a subcomponent of evaluation and feedback within the intelligence cycle and how they are applied to traditional IC all-source intelligence. We will separate the form and function of CTI from that of the IC, and explain how this disparity leads to issues in tracking and actionability of common CTI metrics. Next, we will explore best practices in CTI metrics as key performance indicators, measures of effectiveness, and measures of performance, with examples of how organizations can develop the complexity of their metrics over time. We will present metrics as a "ground-up" component of CTI programs and provide examples of "baking in" metrics and tracking mechanisms from program establishment through to full operational maturity. Finally, we will close with case studies that reflect the "lifecycle" of metrics, from intelligence requirements, through intelligence production and finally in documentation and evaluation. This portion will provide examples of both quantitative and qualitative evaluation as well as subsequent program modifications that they may inform.

BIO: Jason Baker is a threat intelligence consultant on GuidePoint Security's Research and Intelligence Team (GRIT), where he engages in threat intelligence program development, incident response investigations and threat intelligence research on behalf of the firm and its clients. His career background includes strategic intelligence analysis and intelligence program management in the private and public sector.

Baker joined the GuidePoint team from a Fortune 50 health care organization, where he worked as a senior cyber threat intelligence analyst responsible for enterprise analysis and support to incident response. Prior to that, Baker served 10 years in the U.S. Marine Corps and Department of Defense as a counterintelligence agent and strategic intelligence analyst, in military and civilian roles.

Leveraging Data Analytics to Accelerate the OODA Loop for Enhanced Mission Outcomes in Adversarial Environments

Pragyansmita Nayak Ph.D., Chief Data Scientist, Hitachi Federal •
pragyan.nayak@hitachivantarafederal.com

ABSTRACT

In the ever-evolving landscape of modern warfare and security challenges, the ability to effectively observe, orient, decide and act (OODA loop) is paramount for mission success. This abstract explores how harnessing data analytics, including generative AI, can accelerate the OODA loop and enable organizations to align, adapt and accelerate mission outcomes against adversaries. By integrating advanced data analytics techniques such as machine learning, predictive modeling and real-time data processing, organizations can enhance their situational awareness, rapidly assess threats and make informed decisions in dynamic environments. Moreover, leveraging data analytics enables proactive adaptation to changing circumstances, ensuring agility and resilience in the face of evolving threats. This talk will cover the tangible benefits of incorporating data analytics into the decision-making processes of defense and security organizations such as DISA, ultimately leading to more effective mission execution and a competitive edge against adversaries.

BIO: Pragyansmita Nayak, Ph.D., is the chief data scientist at Hitachi Vantara Federal (HVF). She explores the "Art to the Science" of solution architectures orchestrating data, APIs, algorithms and applications. She has more than 25 years of experience in software development and data science (analytics, machine learning and deep learning). She has led multiple projects for different federal government agencies (DoD/civilian) in the domain of federal accounting, operational analytics, data fabric, object storage, metadata management, records management and data governance.

She holds a Ph.D. in computational sciences and informatics from George Mason University (Fairfax, VA) and Bachelor's of Science in computer science from BITS Pilani (India). Her doctoral thesis focused on the application of machine learning techniques to estimate galaxy redshifts based on photomorphic information. She has published and presented at various technical events including WEST, AFCEA TechNet Cyber, NLIT, BrightTalk summits, guest lecture at GMU and GWU and organizer of the NOVA Deep Learning meetup.

Measure What Matters - Key Performance Indicators

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

ABSTRACT

Agency leadership teams should be tracking key performance indicators (KPIs) to help automate their automation roadmap by evaluating the current state of IT, identifying problem areas that need new innovation, and then measuring the outcomes of newly implemented solutions. By focusing on specific metrics for new solutions, Moveworks enables service teams to understand the addressable impact these new solutions can achieve by correlating service & processing times with natural language within service requests (tickets), which allows leadership teams to address problem areas based on data, not just opinions. This approach helps in setting objectives and measuring key performance indicators, ensuring that leadership and individuals can fully comprehend the agency's IT, program, and project investments, thus empowering the agency workforce to help drive mission success in the most efficient ways in their day-to-day operations.

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

Submissions on

Undefined Topics

Clearing the IT Fog of War

John Aron, Founder & CEO, Aronetics • john@aronetics.com

ABSTRACT

Don't lose control of security controls. When nine of 10 compliant organizations are successfully breached, and one-fifth of security practioners think that compliance is the answer, what does the four-fifths of remaining practioners denote, an education gap? What can be done among the STIGs, RMF and various existing tools to minimize risk and mitigate the adversarial threat?

Past, Present, Future of Appx Abuse

Will Burke, Chief Information Security Officer & Director of Cybersecurity, TSI •
wburke@tsiva.com

ABSTRACT

Appx deployment mechanisms have been abused in recent years as a method for threat actors to deploy code or gain initial access, most notably with the distribution of Emotet via the ms-appinstaller protocol in 2021. To protect end-users from this attack vector, Microsoft ultimately decided to deactivate the ms-appinstaller protocol from use in February 2022. After a review period, the ms-appinstaller protocol was reintroduced in August 2022, until it was unceremoniously re-de-activated in December 2023 after another spike of high-profile attacks. We couldn't help but ask ourselves, with the ms-appinstaller protocol disabled, how else is an APT supposed to stop, drop and open up shop?

Join us on a journey of intrigue and masterfully placed DMX puns as we dive into the Past, Present, Future of Appx abuse and reveal our methods to deploy malicious Windows applications without reliance on the ms-appinstaller protocol. After a review of the inner-workings, requirements and (default!) configurations necessary for appx deployment, we will walk through a range of techniques we developed that can leverage these mechanisms for phishing, to establish persistence and more. From there we have one more road to cross and will look at these techniques from a defender's perspective—highlighting how they can be detected and help you take control in your environment.

Some of these techniques are fun, some are just mean, most of them blend in with intended operations, and they all currently work in standard deployments of Windows 10 & 11 with Defender enabled. Whether you are on the offensive or defensive side they could provide some valuable tools for your toolbelt, so bring your whole crew as we open the world of appx.

BIO: Blending his experiences across 20 years in the intelligence and cyber fields, William Burke has found a passion for developing impact-driven offensive security programs and the personnel who lead them. Having previously served as an operator in the U.S. Air Force, as a co-founder of the Department of Homeland Security (DHS) Red Team, and as the deputy chief of vulnerability evaluations (VE) at the Cybersecurity and Infrastructure Security Agency (CISA), he is currently leveraging those skillsets to build and deploy cybersecurity programs as the chief information security officer (CISO) and director of cybersecurity at TSI. Throughout his time, he has also independently developed and taught graduate-level courses focused on offensive security methodologies and actively serves as a member of EC-Council's Certified Ethical Hacker (CEH) Practical scheme committee. He currently holds 15 industry certifications and a M.S. in security informatics from Johns Hopkins University.

Beyond Textual Rules: Revolutionizing DLP with Custom Classifier Training

Jason Bryslawskyj, Ph.D., Senior Machine Learning Scientist, Netskope •
bryslawskyj@netskope.com

ABSTRACT

The landscape of data loss prevention (DLP) is rapidly evolving, and machine learning offers a unique advantage in classifying files that contain sensitive information. Traditional DLP techniques often rely on textual rules, which might not be sufficient for handling complex, unstructured data. This presentation will provide a hands-on guide to implement machine learning-based file classification as a robust supplement to conventional DLP methods. By applying these techniques, participants can better safeguard data subject to PII, PCI and HIPAA regulations, among others.

Objectives

The primary goal of this session is to demystify the process of integrating machine learning classifiers into your existing DLP frameworks. Specifically, we'll introduce the Custom Classifier Training (CCT) approach. Attendees will learn how to:

- Train machine learning classifiers with minimal sample data
- Ensure data privacy during the machine learning training phase
- Quickly adapt classifiers to new data categories without expensive computational costs

Technical Deep Dive

The core of this session will be a technical walkthrough, aimed at enabling participants to independently implement the CCT methodology. We will delve into:

1. **Encoding Model:** Understand how to employ pre-trained deep learning models to extract high-quality feature vectors, or "embeddings," from your data samples.
2. **Approximate Nearest Neighbors Model:** Learn to leverage these embeddings to quickly retrain classifiers via an approximate nearest neighbor's algorithm, without demanding computational requirements.

Real-World Applications and Takeaways

We'll walk you through a case study—building an access card classifier with CCT. By the end, you'll understand:

- How to gather the minimum data required for effective classification
- Steps to preprocess and encode the image data
- Techniques for training and validating your classifier
- How to implement privacy safeguards during the process

Attendees will walk away with a well-defined roadmap for tackling their own DLP challenges, irrespective of their technical background or resource constraints. This session aims to provide the skills and confidence needed to implement tailor-made DLP solutions efficiently and economically.

BIO: Jason Bryslawskyj, Ph,.D., is a staff machine learning scientist at Netskope's AI Labs. Bryslawskyj started his career in the field of high energy nuclear physics, analyzing near-petabyte sized datasets at the Relativistic Heavy Ion Collider. He has more than a decade of experience applying machine learning to large scale datasets, focusing on signal analysis and computer vision. At Netskope, Bryslawskyj has been developing computer vision models for data loss prevention and phishing detection.

Quantum-Resistant Security

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

ABSTRACT

Quantum computing's impact is likely to be large—the potential computational power could render today's encryption algorithms obsolete. The White House's National Security Memorandum on Promoting U.S. Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems states that "America must start the lengthy process of updating our IT infrastructure today to protect against this quantum computing threat tomorrow." The memo continues by stressing that, "Central to this migration effort will be an emphasis on cryptographic agility, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards."

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

Attend this session to learn how to start the transition to quantum-safe cryptography. The speaker will provide a brief overview of the quantum threat and current initiatives within government and industry designed to mitigate the associated risks. Lastly, the speaker will discuss key factors to consider when preparing for a quantum-safe encryption strategy:

- **Know Your Risks**—Learn how long-term data is subject to early attacks and about key initiatives that address the quantum threat
- **Focus on Crypto Agility**—Learn what to look for in a quantum-resistant crypto solution
- **Start Today**—Learn how to design a quantum resistant architecture

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

Data Protection at the Edge

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

ABSTRACT

Core computing functionality commonly found in data centers and in the cloud is also being deployed at the edge—data protection capabilities must transition with that move. However, many challenges often stand in the way of extending core-level security to the edge. Harsh environments; bandwidth-limited and disconnected sites; overrun or hostile scenarios; and constraints related to size, weight and power have made it difficult to employ the appropriate levels of security while allowing the kind of quick response needed at the edge.

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

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

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

WHAT IS AFCEA?

AFCEA is a member-based, nonprofit association for professionals that provides highly sought-after thought leadership, engagement and networking opportunities. We focus on cyber, command, control, communications, computers and intelligence to address national and international security challenges. The association has more than 30,000 individual members, 138 chapters and 1,600 corporate members. For more information, visit afcea.org.