2023 ITS7 AGENDA

FOR MORE INFORMATION ON THE BELOW SPEAKERS VISIT:
insiderthreatsummit.com/2023speakers

DAY 1 - Wednesday, March 22nd

8:00 AM -8:45 AM
KEYNOTE SPEAKER
Michael Orlando, *Director of NCSC at ODNI*
Mitigating Counterintelligence Risk & Insider Threats: How to Convince CEOs to Invest in Prevention
Mr. Orlando will discuss today's counterintelligence threat landscape and the latest insider threat trends and mitigation best practices from his perspective as the leader of U.S. Government's counterintelligence and security community. He will also discuss ways for insider threat practitioners to make the best business case to corporate leaders for investing in robust insider threat detection and prevention.

8:45 AM - 9:30 AM

Gunner Newquist, *Client Advisor, Strider Intel*

Protecting Your Vulnerable Employees from Nation State Actors

Today, Nation State Actors (China, Iran, Russia) are interested in more than our military capabilities and intent. They are specifically interested in disruptive technologies such as Artificial Intelligence (AI), Quantum Science and Nano Technology. Becoming a global industry leader, in any of these fields, will create economic statecraft advantages. Although still interested in DOD intentions and capabilities, the global economy requires Nation State Actors to aggressively compete in the development of disruptive technologies.

As players in the Great Power Competition, Nation State Actors are actively recruiting insiders to acquire Western talent and IP to develop disruptive industries critical to their ability to compete globally.

How should you respond? By protecting your vulnerable employees who are at risk of being exploited as Managed Insiders. Raised awareness, clear governance and enhanced monitoring provide a solid foundation to understand the risk of Insiders, managed by Nation State Actors, to our collective strategic edge.

9:30 AM - 9:45 AM

COFFEE BREAK

9:45 AM - 10:15 AM

Henry Nelson, *Deputy for Enterprise Program Management at DITMAC, DCSA*

From Infancy, to Maturity

The Evolution and Advancement of DoD Insider Threat Programs. This briefing will focus on new initiatives within the DoD Insider Threat Management and Analysis Center (DITMAC) and how they enhance existing enterprise capabilities to detect, deter, and mitigate risk from insiders.

10:15 AM -11:00 AM

Aaron Cordova, *Chief Technical Officer, Koverse, Inc.,*
An SAIC Company

Eliminating One Class of Insider Threats with a Zero Trust Approach to Data

Access to sensitive data remains a central issue in guarding against insider threats. Often the coarse granularity of access controls results in organizations either overprotecting and physically siloing data, or inadequately protecting it by giving individuals access to entire datasets when only a portion is required for a particular job – especially within IT departments. In this session, Aaron discusses how advanced Zero Trust data security models, conceived and used across National Defense and Intelligence Communities, can solve precise data access requirements for all organizations in highly regulated industries. We'll examine how organizations can prevent elevation of privilege, trace user activity, and combine ephemeral information about users' equipment and spatiotemporal circumstances into access control decisions. Lastly, Aaron will share how fine-grained access control has been used in several real-world cases to combine sensitive data to identify potential insider activity risks.

11:00 AM - 11:45 AM
Mohan Koo, *Chief Technology Officer of DTEX Systems*
Rajan Koo, *Chief Customer Success Officer and Head of i3 Investigations & Engineering, DTEX*
Armaan Mahbod, *Director i3 Insider Threat Investigations and Intelligence, DTEX*
SINK or SWIM?
Too many insider threat programs are drowning in an overload of poor quality data that lacks sufficient context to proactively mitigate risk. Learn how a Top 3 Global Bank, Top 3 US Energy Provider and a large Federal Government agency have transformed their insider programs by addressing data quality. Also, learn about MITRE's new data-driven Insider Threat Framework initiative and how you can support it.

11:45 AM - 12:45 PM
LUNCH BREAK

12:45 PM - 1:30 PM
Charlie Sowell, *CEO at SE&M Solutions LLC*
Quantum Trust™ - Thinking beyond Trusted Workforce 2.0
The Federal Government is well into the Trusted Workforce 2.0 transformation. The USG is also beginning to highlight the challenges and opportunities arising from quantum computing and artificial intelligence. Insider Threat and Security community members like DCSA are beginning preparing for a post-quantum and AI-enabled world

now. The Quantum Trust world will feature a hyper-individualized, data-rich, AI-enabled operating environment. Quantum Trust decisions will be faster, better-informed, and more equitable than anything we could institute today. This presentation is designed to generate thoughts and debates about the future of U.S. security clearances and will compare what other countries are doing now.

1:30 PM - 2:00 PM

Damien Weiss, Splunk

Using Machine Learning to Find the Hidden, and Ease Analyst Burden

Analysts are overwhelmed by the amount of data that is being generated by their UAM systems. Additionally, computer savvy insiders use wildly unpredictable methods to exfiltrate data that can be missed when looking with more traditional means. Luckily, some ML models offer relief to both of these problems by looking through the figurative hay stack and showing analysts a collection of needles for further investigation. In this conversation is, as always, the question of how UEBA can help and how ML assisted UEBA becomes a real detection machine.

2:00 PM - 2:30 PM

Dr. Michael Gelles, *Managing Director, Deloitte Consulting LLP*

Building Holistic Insider Threat Programs: Mitigating Physical and Logical Threats: Data Exploitation to Workplace Violence

Building Holistic Insider Threat Programs: Mitigating Physical and Logical Threats: Data Exploitation to Workplace violence. Addressing how organizations can become more proactive versus reactive while looking at the challenges faced by current insider threat programs. This presentation will also review the lessons learned from the evolution of insider threat tactics over the past 30yrs.

2:30 PM - 2:40 PM

COFFEE BREAK

2:40 PM - 3:25 PM

Grace Clemente, *Senior Director, Insider Threat & Counterintelligence at Anduril* with Nik Seetharaman, *& Chief Information Officer (CIO) at Anduril Industries*

Building Insider Threat Programs at Advanced Defense Technology Companies: Finding Anomalous Behavior on Weapons Systems and the Infrastructure That Builds Them
Detecting sophisticated insider threats in environments dealing with advanced or emerging technology requires a rethinking of traditional counterintelligence paradigms.

Leaders in these organizations must corral cross-functional teams from across business boundaries to synthesize disparate data points into high signal context that proactively stops or rapidly detects malicious insiders. Analysts must speak the language of IT and cybersecurity teams, whose systems they must integrate into their behavioral analytics pipelines.

In this two-part session, Grace Clemente and Nik Seetharaman will relay their experiences building insider threat programs focused on protecting the intellectual property of advanced spaceflight and defense technology companies, and the characteristics of what makes a modern insider threat program successful. They'll also discuss lessons learned and practical recommendations for protecting critical infrastructure, weapons systems, and autonomous vehicles against adversaries who may do them harm.

3:25 PM - 3:55 PM
Shibu Thomas, *Worldwide Consulting Sales Engineer, Insider Threat/Risk and Analytics Global Governments at Forcepoint*
Success Stories in a Never-ending War
Shibu will feature actual Insider Threat/Risk success stories from real-world wins, some of which have been covered in the media. ITS7 is focused on concepts, best practices and thought leadership on how to combat the unique Insider Threat/Risk problems that organizations face today. This talk is meant to be encouraging and will highlight the outcomes of the concepts and strategies that have been discussed and implemented over the years, all of which have produced undeniable victories.

3:55 PM- 4:40 PM
OPEN- PANEL DISCUSSION with
- **Mr. Tim Sullivan, *DLA Intelligence, Security Division Chief***
- **Mr. Camilo Bolanoeslava, *DLA Insider Threat Program Manager***
- **Mr. Sherif El-Shazly, *DLA Insider Threat Program IT Lead***
- **Mr. Philip LaGamba, *DLA Cyber Insider Threat Analyst***

Discussion: Mitigation Strategies: A Defense Agency Approach

It is common knowledge that having a fully compliant Insider threat Program (InTP) doesn't necessarily translate into its mitigation effectiveness. The Defense Logistics Agency (DLA) was the first Defense Agency to reach Fully Operating Capability (FOC). However, some of the biggest challenges the DLA InTP has faced are related to the multi-organizational approach for mitigation strategies. Through some case studies, this panel aims to generate discussion focused on the different types of mitigation strategies, that despite being framed by the same policy, vary/evolve significantly by agency/company.

4:45 – 8:00 PM

NETWORKING RECEPTION

Join us in the OCEAN VIEW BALLROOM, TOP FLOOR where you will be treated to the best views of Monterey Peninsula, great company, food and beverages. Don't forget your drink tickets!

End of Day 1

FOR MORE INFORMATION ON THE BELOW SPEAKERS, VISIT:
insiderthreatsummit.com/2023speakers

DAY 2 - Thursday, March 23rd

7:00 AM -8:00 AM
Check-in and Networking with Breakfast

8:00 AM -8:45 AM
KEYNOTE SPEAKER

Terry Carpenter, *Chief Technology Officer (CTO) of DCSA*

Artificial Intelligence is Critical for National Security

Learn how the Defense Counterintelligence and Security Agency is experimenting with AI and developing plans to integrate into missions responsibly. Hear insights from Terry Carpenter, CTO of DCSA will share his learning and insights on accelerating the adoption of AI-based systems and managing the inevitable resistance to change that comes with using digital technologies.

8:45 AM - 9:30 AM
Steve Layne, *Chief Executive Officer (CEO) of Red Vector*

Threats – Risks – Trust, A pragmatic approach to the challenges

A pragmatic view of the age-old concerns of organizational risk caused by individual behaviors and how risk identification can lead to threat reduction and elimination. Illumination and insights on approaches and solutions that have proven to be effective at mitigation and increasing organizational trust.

9:30 AM - 9:45 AM
COFFEE BREAK

9:45 AM - 10:30 AM

Dr. Leissa Nelson, *Industrial-Organizational Psychologist and Project Director with the Defense Personnel and Security Research Center (PERSEREC), Office of People Analytics (OPA)*

Global Insider Threat Certification: A Program to Support Professionalization of the Insider Threat Workforce.

A discussion of certification, training, and analyst tools developed by the Threat Lab to support counter-insider threat professionals. She will discuss competencies and certification, and publicly available tools such as a guide to Structured Professional Judgment tools, a handbook for analysts and other products developed by PERSEREC's Threat Lab.

10:30 AM -11:15 AM

Nathan Verrill, *Edge AI Lead & Research Fellow at SAIC*

AI Synesthesia: Data Fusion Techniques for Pattern Recognition & Anomaly Detection

Geiger Counters are an example of machine synesthesia and sonification—translating non-audio data into representations we can hear. The variations in spacial, temporal, amplitude, and frequency resolution are perceived by humans three times faster than a visualization of the same data. So what happens when we fuse multiple types of data, sonify it, and process it with algorithms modeled after music and human speech?

This multi-sensory presentation will explore the intersection of sonification, artificial intelligence, music information retrieval, and natural language processing. The experience will inspire the audience to further discuss how these techniques might be applied to insider threat use cases, including anomaly detection, behavioral analytics, and patterns of life.

11:15 AM - 12:00 Noon

Dr. Frank L. Greitzer, *President and Principal Scientist at PsyberAnalytix, LLC | Consultant, Cogility Software*

Implementing Proactive Insider Threat Assessment: Research and Operational Perspectives

Insiders who destroy, steal, or leak sensitive information pose a serious threat to enterprises. An insider threat is an individual with authorized access to an organization's systems, data, or assets, and who intentionally (or unintentionally) misuses that access in ways that harm (or risk) these assets. Insider risk assessment is a wicked/hard problem: the research and operational communities have come to realize that it is a human problem. Spanning two decades, a strong theme of my research has been to

develop insider threat models that integrate relevant human behavioral and psychological factors with technical factors associated with host and network cybersecurity monitoring systems.

The presentation will provide an overview of this research on socio technical factors and the continuing challenges to understand and characterize cyber and behavioral indicators of insider threat risk. A comprehensive ontology of Sociotechnical and Organizational Factors for Insider Threat (SOFIT) provides a foundation for this whole-person, predictive analytic approach that seeks to get “left of harm.” The talk will review recent research characterizing the dynamic nature of insider threat indicators and their relationships, with implications for devising threat assessment models and effective mitigation strategies.

12:00 PM - 1:00 PM
LUNCH BREAK

1:00 PM - 1:30 PM
Tony Waller, *Principal Sales Engineer, DoD and Special Programs, Netscout*
Network-Centric Risks and Mitigation Techniques for Insider Threats
Attendees will gain insights into different types of insiders and their motivations along with associated threats. NETSCOUT will review and participate in an open discussion of recent insider threats that have resulted in criminal prosecution. You will learn how to use a network-centric approach for identification of insider threats and see differences between log and packet-based approaches for analyzing insider activity. Leave this talk having gained a better understanding around a TECHOPS process for proactively addressing and mitigating the insider threat. Receive one (1) CPE credit for use with ISC2 by attending this discussion.

1:30 PM - 2:15 PM
Stephanie Jaros, *Insider Risk Professional*
Leveraging Social Sciences to Forecast Insider Risk in an Uncertain Economy
Since Executive Order 13587 was signed in 2011, we have had the opportunity to build insider risk programs during a period of relative economic stability. As we all do our best to continue prioritizing security in this current uncertain economy, insider risk professionals cannot stand on the sidelines as leaders make enterprise-level policy and

staffing decisions. Instead, we must leverage our expertise and forecast insider risks. The social sciences are well-suited to this challenge and in this briefing Stephanie will share theories and practices that will help us better protect our colleagues and our organizations as we navigate the future through organizational cooperation and integration.

2:15 PM - 2:45 PM

Julian Claxton, *Managing Director, Jayde Consulting*

I spy with your little eye: How employees can use behavioural intelligence to detect insider threats.

Despite heavy investment in physical, electronic, and cyber security, insider threat actors continue to undermine protective security controls. Could this be because organisations place too much emphasis on software platforms to detect anomalous behaviour?

Although software plays an essential role in the detection of insider threat acts, its use often overlooks the fundamental core of an organisation's well-being - social interaction. The conveying of information between two or more people, be it verbal or non-verbal, can reveal a treasure trove of valuable intelligence. It can inform of a person's emotional state, whether they are focused and committed, their intent, and myriad other indicators - all of which in context, can be used to identify emerging threats.

The presentation addresses key behavioural indicators of malintent that are often best revealed through face-to-face interaction. It will reference case studies and anecdotal evidence to demonstrate that 'intelligence' exists. We just need to teach our employees how to identify and report it, to better combat insider threats.

2:45 PM - 2:55 PM

COFFEE BREAK

2:55 PM - 3:40 PM

CLOSING KEYNOTE SPEAKER - Joshua Crumbaugh, *Chief Executive Officer (CEO) of PhishFirewall | Author | Ethical Hacker*

Creating Your Own Insider Threat: You are Your Own Worst Enemy

Every day, thousands of organizations are unknowingly exposing themselves to more insider threats due to inadequate security awareness models. This is often because the

training is not engaging, and tests are designed to trick rather than educate users. On top of that, there are often harsh consequences for those who engage with cyber threats. This type of environment only serves to breed threats instead of mitigate them. In this speech, Joshua Crumbaugh, founder and CEO of PhishFirewall, will discuss why traditional punitive security awareness approaches are counter-productive and how organizations can leverage AI tools to emphasize positive reinforcement techniques. He will explain how data analysis and behavior analytics can be leveraged to detect anomalies and create an engaging and supportive environment that encourages users to understand the importance of security.

Crumbaugh will also explore how organizations can use this approach to reduce the risk of insider threats and create a more secure environment. By the end of this speech, attendees will understand the danger of ineffective cyber security that relies on punitive measures and unengaging training models, and how it leads to an uncaring attitude towards the organization's cyber defenses. They will also have the knowledge on how to build effective training programs that engage users and provide holistic behavior analytics built around actually reducing organizational breach risks.

3:45 PM - 4:45 PM

OPEN-PANEL DISCUSSION

- **Brad Morris,** ***Chief Technology Officer at Advanced Onion***
- **Christopher Augustine,** ***Deputy for Operations at DITMAC, DCSA***
- **Michael Swan,** ***GSRS/Google***
- **Stephanie Jaros,** ***Insider Threat Professional***

Discussion: **Offensive Communities and Organizational Linchpins.**

End of day 2