NATIONAL INSIDER THREAT SPECIAL INTEREST GROUP

INSIDER THREAT SYMPOSIUM AND EXPO AGENDA

Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland
October 19, 2018

PREMIER SPONSOR

Veriato

Vendors Exhibiting

DIGITAL GUARDIAN

INSIDER THREAT DEFENSE
Insider Threat Risk Mitigation Experts
www.insidertheatdefense.us
www.nispomcc2training.com
888-363-7241

GEMINI DATA

EXEC SECURITY
TSCM TECHNICAL SERVICES

systems dtex

MATHCRAFT
SECURITY TECHNOLOGIES, INC.

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

SIMS SOFTWARE

AVESHKA

exabeam

TransUnion

observe it

HID

FORCEPOINT

solarwinds federal

Jazz Networks

leidos

INSIDER THREAT SYMPOSIUM SPEAKER AGENDA

NITSIG ITSE Registration
7:00am To 7:45am

NITSIG ITSE Opening:
7:45am To 8:00am (NITSIG Board Members Opening Remarks)

KEYNOTE Speaker # 1 **8:05am To 8:35am**
William R. Evanina
Director, National Counterintelligence and Security Center

Presentation Title / Overview
The Importance Of Addressing The Insider Threat With An Insider Threat Program
No matter how good your perimeter defenses are, you must always contend with the problem of the insider--malicious or otherwise. Insider threat actors have a comparative advantage over others in the arena of critical infrastructure. They have access to facilities, systems or networks that terrorists and nation-state threat actors typically do not have. They know how to do damage in nuanced ways, not just relying on remote-access cyber, but using digital technologies. Insiders may also be unwitting, compromising information or security through negligent or lax practices (i.e., clicking on the spear phishing link). Continually advancing technology enhances malicious insiders' ability to exploit large quantities of sensitive information. It may be difficult to stop an insider who is determined to steal, leak, or sell information. A malicious insider may also put personnel, equipment and facilities at risk through acts of terrorism, workplace violence, or sabotage. Holistic Insider Threat Programs—whether in the public or private sector—are in a much better position to proactively identify abnormal activity and to minimize potential damage when it occurs. They are able to identify and analyze anomalous activity, using multiple data sources, and refer the matter to the proper authority for mitigation and/or response. Ideally, Insider Threat Programs will get ahead of an unauthorized disclosure, by closing potential security gaps and/or identifying personnel who need assistance, before any damage occurs.

Speaker # 2 **8:40am To 9:10am**
Daniel Costa
Lead Of The Insider Threat Technical Solutions Team
CERT National Insider Threat Center

Presentation Title / Overview
A Framework To Effectively Develop Insider Threat Controls
The CERT Insider Threat Center will present a framework for organizations to consider as they first attempt to identify insider threats to critical assets and second as they develop, implement and measure the effectiveness of technical and nontechnical controls and detection capabilities. Actual incidents of insider harm will be presented to demonstrate control development using the framework.

Speaker # 3 **9:15am To 9:45am**
Patrick Knight
Senior Director Of Cyber Strategy And Technology
Veriato

Presentation Title / Overview
Assessing Your Insider Threat Program's Maturity
Just because nearly every organization is aware of insider threats, they don't all address the problem in the same way. And yet, there are industry-recognized best practices that, in total, can be used to properly establish and maintain an Insider Threat Program. In this educational session, join Patrick Knight from Veriato, as he uses the findings from an Insider Threat Program Maturity Model survey to help you:

- Identify just how mature is your organization's program.
- Spot the common challenges every organization faces – and learn how to overcome them.
- Learn how to mature your program to one that's consistently aligned with the needs of your organization.

BREAK
9:45am To 10:00am

Speaker # 4 **10:05am To 10:35am**
Davita N. Carpenter, M.B.A., SHRM-SCP
Vice President, Human Resources / Employee Care / Compliance / Ethics / EEO Officer
Novetta Inc.

Presentation Title / Overview
Insider Threat Program: Is Human Resources At The Table And Engaged?
The presentation will focus on Human Resources (HR)' level of engagement and commitment to the Insider Threat Program. The gathering and sharing of employee information is essential for the success of an Insider Threat Program. Equally important is protecting employee's privacy and civil liberties. If you are asking "How can HR be successful in this role?", this presentation is for you.

Speaker # 5 **10:40am To 11:30am**
Dr. Liza Briggs
Social Scientist
US Marine Corps HQ Intelligence Department

Presentation Title / Overview
Social Science And Insider Threat: Being The Insider's Outsider
Social Science perspectives uncover gaps, address unintended impacts and provide assessment and analytic capabilities that advance Insider Threat Program objectives. Dr. Briggs will discuss examples of common dynamics, challenges and tools relevant to Insider Threat Programs, while highlighting the application of Social Science methods and tools.

LUNCH – NETWORKING
11:30am To 1:00pm

Speaker # 6 **1:00pm To 1:30pm**
Dr. Max Alexander
Chief Technology Officer, Digital Transformation / Defense and Intelligence
Aveshka, Inc.

Presentation Title / Overview
Conducting User Activity Monitoring With Your Existing Network Infrastructure
The presentation focuses on using your existing network infrastructure to conduct user activity monitoring. This presentation is designed for organizations just starting to implement User Activity Monitoring and Insider Threat Programs within their organizations. It provides a basis for achieving an initial operating capability until other tools and infrastructure can be implemented, or allows the organization to tune their existing tools to achieve a maximum return on investment if no other tools will be purchased.

Speaker # 7 **1:35pm To 2:05pm**
Tammy Smith
Operations Manager, Office of Security
Office Of The Comptroller Of The Currency

Presentation Title / Overview
Office of the Comptroller of the Currency (OCC) Insider Threat Program Team Approach
The Department of Treasury has the main responsibility of Insider Threat Program monitoring. As a bureau OCC has a responsibility of employee safety that the Treasury program does not monitor at the departmental level. Mrs. Smith will discuss examples of OCC collaboration of the Crisis Management Team approach in dealing with the security challenges and departmental dynamics when having responsibility of over 70 sites of across the United States.

Speaker # 8 **2:10pm To 2:40pm**
Alan Small
President Of The Maryland Chapter Of The Association of Certified Fraud Examiners
Morgan State University Internal Management Auditing And Investigations
Certified Internal Auditor (CIA) / Certified Fraud Examiner (CFE)
Certified Instructor With The Maryland Police Training Commission For Fraud Investigation For Law Enforcement

Presentation Title / Overview
Insider Threat Vulnerabilities And Fraud
Insider Threat Vulnerability (ITV) creates a pathway for the opportunist to access targeted sources of records from an inventory of files arranged into categories that contain operating footprints of organizational plans exposing the weaknesses of the internal control environment. An opportunist will take advantage of these weaknesses.

In all organizations, internal and external threat exposure can result in fraud and originates with underdeveloped business control practices. These exposures drive the heartbeat of every organization affecting hiring, communications, financial management, taxes, procurement, and physical plant, security, transportation, and food services operations. Such vulnerabilities weaken financial stability and become insider threats to the going concern opportunities for business success. A prescription of internal auditing and fraud assessment may serve businesses well to minimize the effects of these threats.

BREAK
2:40pm To 3:00pm

Speaker # 9 **3:05pm To 3:35pm**
Mark Riddle
Principal For CUI Program Oversight
Information Security Oversight Office
National Archives and Records Administration

Presentation Title / Overview
Protecting Controlled Unclassified Information (CUI)
Background On Protecting CUI - On November 4, 2010, the President signed Executive Order 13556, Controlled Unclassified Information. The Executive Order established a government wide CUI Program to standardize the way the executive branch handles unclassified information that requires protection. It designated the National Archives and Records Administration (NARA) as the Executive Agent to implement the program. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office.

The requirements for the protection of CUI provide a set of "minimum" security controls for contractor information systems upon which CUI is processed, stored on, or transmitted through. These security controls must be implemented at both the contractor and subcontractor levels based on the information security guidance in NIST Special Publication (SP) 800-171: Protecting Controlled Unclassified Information In Non-Federal Information Systems And Organizations.

The CUI protection requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. Failure to implement the security controls to protect CUI, would be a breach of contract.

For an Insider Threat Program to be robust and effective, it must be built upon an established security foundation within an organization. The NIST SP 800-171 covers many security controls that can support Insider Threat Risk Mitigation.

This presentation will provide the attendees with an overview of the CUI Program, its origins, and review the safeguarding elements found in the CUI implementing directive 32 CFR Part 2002.

Speaker # 10 **3:40pm To 4:15pm**
Jim Henderson
Insider Threat Risk Mitigation Expert
NITSIG Founder / Chairman
CEO Insider Threat Defense, Inc.

Charles Patterson
President, Exec Security TSCM Services / Patterson Communications, Inc.

Presentation Title / Overview
Data / Information Using The Malicious Insider Playbook Of Tactics - Insider Threats Made Easy - James Bond 2018
Is Your Government Agency Or Business Being Bugged With Spy Gear?
The news during the week of August 12, 2018, reported that former White House employee Omarosa Manigault Newman used a Spy Pen to record conversations within the White House. Manigault Newman has dodged questions about how she made her recordings, but current and former White House staffers are reportedly concerned that she used a pen that looks like a typical writing tool but can actually record audio.

This presentation / demonstration will focus on understanding simple techniques and spy gear that "Malicious Insiders" can use to exfiltrate data and other valuable information from within an organization. These techniques have successfully been used to exfiltrate sensitive business information during Insider Threat Risk Assessments. Understanding the "Malicious Insiders Playbook" of options is critical.

Mr. Patterson specializes in providing electronic privacy protection through technical surveillance countermeasures (TSCM) inspections, providing security sweeps for electronic surveillance, listening devices, and technical cyber threats.

INSIDER THREAT DISCUSSION PANEL
4:15pm To 4:50pm

CLOSING
4:50pm To 5:00pm

EXPO E-MAIL OPT-OUT NOTICE
The Expo will have many great vendors showcasing a variety of Insider Threat Risk Mitigation solutions and services.

If you do not wish to receive a follow up e-mail message(s) from vendors with their company information, please send an e-mail to: jimhenderson@nationalinsiderthreatsig.org.

Please specify "Opt-Out Expo E-Mails" in the subject line.

The NITSIG hopes you find this event very informative. Please send your comments to: jimhenderson@nationalinsiderthreatsig.org

Contact Information
Jim Henderson, CISSP, CCISO
Founder / Chairman Of The National Insider Threat Special Interest Group
Phone: 888-363-7241 / 561-809-6800
www.nationalinsiderthreatsig.org