NATIONAL INSIDER THREAT SPECIAL INTEREST GROUP

INSIDER THREAT SYMPOSIUM & EXPO AGENDA

Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland
September 10, 2019

PREMIER SPONSOR

Veriato

Vendors Exhibiting

MATHCRAFT SECURITY TECHNOLOGIES, INC.

INSIDER THREAT DEFENSE GROUP

Dtex systems

TransUnion

haystax

AC GLOBAL RISK

solarwinds government

SECURONIX

Jazz Networks

ORACLE National Security

Capgemini

CODE42

splunk>

observe it

CYBERHAVEN

INSIDER THREAT SYMPOSIUM SPEAKER AGENDA

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

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

KEYNOTE Speaker # 1 **8:05am To 8:35am**
Defense Intelligence Agency
Robert Carpenter
Chief, Insider Threat Division

Presentation Title
Building Upon The National Insider Threat Task Force Standards

Presentation Abstract
The Defense Intelligence Agency has a well-established Insider Threat Program that has played a major role in helping identify, understand and respond to anomalous workforce behaviors that are indicative of potential insider threats. This program has experienced a number of changes since its inception during 2009, and these changes were aimed at better addressing the dynamic problem set that the insider threat creates. Mr. Carpenter will share insights about the Defense Intelligence Agency' Insider Threat Program, including its strategy moving forward.

Speaker # 2 **8:40am To 9:10am**
U.S. Department Of Homeland Security / Cybersecurity & Infrastructure Security Agency
Daniel Abreu
Deputy Associate Director for Security Programs

Presentation Title
Securing Critical Infrastructure From Insider Threats

Presentation Abstract
The Cybersecurity and Infrastructure Security Agency (CISA) partners with industry and government to understand and manage risk to the Nation's critical infrastructure. One of the risks that CISA supports its partners in mitigating is insider threat. Given the inherent institutional knowledge, insiders have the ability to significantly disrupt operations if proper mitigating measures are not in place. CISA provides organizations with capabilities that support their efforts in mitigating this risk. Daniel will provide an overview of CISA and the resources it makes available free of cost to public and private sector partners to mitigate insider threats.

Speaker # 3 **9:15am To 9:45am**
Naval Information Warfare Center Atlantic
David T. Lang, CSEP, CGEIT, CRISC
Lead Functional Architect & Senior Technical Advisor
Navy Insider Threat Program

Presentation Title
Counter Insider Threat Strategy: Engineer The Insider Threat Program, Not The Tools

Presentation Abstract
Almost every day I get e-mail touting the latest innovations for counter Insider Threat tools. Big data analysis, user activity monitoring, enterprise data aggregation, security information and event management, and more. Yes, there are a lot of great tools out there, but what do you need? What is your operational concept? What are you protecting? How big is your enterprise? How big is your staff? What technical expertise do you have available?

This presentation will provide a systematic approach to engineering and architecting your Insider Threat Program so you can select the tools that fit your organization and operational concept.

BREAK
9:45am To 10:00am

Speaker # 4 **10:05am To 10:35am**
Dell Technologies
Tim Kirkham
Director Of Global Security Investigations & Insider Risk

Presentation Title
Insider Risk Management At The Corporate Level

Presentation Abstract
Lessons Learned From Developing Insider Threat Programs In Fortune 100 Companies

---

Speaker # 5 **10:40am To 11:30am**
Veriato
Patrick Knight
Senior Director Cyber Strategy & Product Management

Presentation Title
Troll Farms: Converting Insiders To Insider Threats

Presentation Abstract
Troll farms have become a commercial service for entities to affect public sentiment and incite unrest through sophisticated disinformation and psychological operations tactics for the modern era. Successes can be measured by affecting the actions of only a few of the targeted individuals. Combined with targeted campaigns via social media to sow anti-government sentiment and other activist emotions, trusted insiders could be turned into the next major insider threat.

LUNCH – NETWORKING
11:30am To 1:00pm

Speaker # 6 **1:00pm To 1:30pm**
Penn State University Homeland Security Program
Nicholas Eftimiades
Assistant Teaching Professor, Homeland Security Program

Presentation Title
Chinese Economic Espionage: Insider Threats & Operational Methods

Presentation Abstract
American industry is poorly prepared to contend with the insider threat stemming from China's whole of society approach to economic espionage, theft of intellectual property, technology, and trade secrets. This briefing presents findings on insider threats, their targets, motivations, and operational tradecraft. Conclusions are drawn from analyzing a data set of 447 cases of Chinese espionage. China's intelligence activities targeting the US industry are conducted by a wide range of organizations including state-owned enterprises, private companies, individuals, and some universities, as well as the country's intelligence services. The targets of China's espionage correlate to the priority technologies identified in core government strategies, suggesting a centrally directed but distributed 'whole of society' approach to intelligence activity. The level of espionage tradecraft ranges from quite poor to professional, even within organizations; cyber espionage is the exception, showing standardized techniques and practices. The views expressed in this briefing do not reflect Penn State University or the U.S. Government.

Speaker # 7 **1:35pm To 2:05pm**
DoD Insider Threat Management & Analysis Center
Dr. Gallagher Senior Behavioral Science Advisor

Presentation Title
User Activity Monitoring Results In The Department of Defense: Trends & Response

Presentation Abstract
This presentation will explore how the Department of Defense (DoD) has responded to Executive Order 13587 and National Insider Threat Task Force (NITTF) Minimum Standards requirement to establish user activity monitoring on its networks. It will detail the insider threat trends that have emerged thus far from those monitoring activities. Finally, it will discuss how the DoD is adapting to better address these trending threats now and in the future.

BREAK
2:05pm To 2:20pm

Speaker # 8 **2:25pm To 2:50pm**
Equifax
Courtney Healey
Insider Threat Program Manager

Presentation Title
Adapting & Evolving: Lessons Learned From Changing Security Landscapes

Presentation Abstract
Whether you are building an Insider Threat Program or have one long-standing, there are consistent challenges in collecting the information and support you need to be successful. While there is no silver bullet that works for every organization, we would like to share both successes and failures we have had with organizational structure, data, tools, and executive support.

Speaker # 9 **2:55pm To 3:25pm**
TransUnion
Jon Mark Harrington, CFE
Director, Global Insider Threat & Data Loss Prevention Program
Cyber Threat and Intelligence
Global Technology-Information Security

Presentation Title
Winning Hearts & Minds: Countering Insider Threats Goes Beyond InfoSec

Presentation Abstract
Building and then honing an industry-leading Insider Threat Program involves more than high-tech information security tools. It takes close relationships, buy-in, and actual participation from other key company components as well as senior executives.

If one transitions from the government, and is new to the private sector, the environment can seem very different. Where should one begin? One approach involves engaging the tactical, operational and strategic levels, simultaneously. In doing so, there are several do's and don'ts about which to be mindful. For example, a do - maintain a consistent message - have a message - on all three levels; a don't – maintain a matter-of-fact demeanor, especially with senior executives. There are many competing priorities - making money or feeling more like a family than a corporation.

The Insider Threat Professional must formulate their security strategy by sincerely considering these competing priorities and using them to win the hearts and minds of key individuals who will facilitate the program's success.

Speaker # 10 **3:30pm To 4:00pm**
Oracle National Security Group
Patrick Sack
Chief Technologist Officer (CTO)

Presentation Title
Protecting Cloud Data From Insider Threats

Presentation Abstract
As we've seen in recent major Cloud breaches, the insider threat (employees, ex-employees, etc) can lead to catastrophic data loss for banks, government, and other institutions. Predicting and monitoring a malicious insider's "authorized" activity on data is extremely difficult, yet paramount. We will explore the attack vectors insiders have on data in the cloud and the unique protections needed to secure it.

CLOSING REMARKS
4:05pm To 4:20pm

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
CEO Insider Threat Defense Group, Inc.
Insider Threat Program Development / Management Training Course Instructor
Insider Threat Analyst, Vulnerability Assessor & Mitigation Specialist
Phone: 888-363-7241 / 561-809-6800
www.nationalinsiderthreatsig.org
www.insiderthreatdefense.us

NITSIG LinkedIn Group:
https://www.linkedin.com/groups/12277699

Follow Us On Twitter:
@InsiderThreatDG