insider threat

2018 SUMMIT

iTS4 PROGRAM

March 19 - 20

Marriott, Monterey, CA

Hosted by Tech Regiment, Inc.

insider threat

2018 SUMMIT

AGENDA - DAY 1
Monday, March 19

7:00 AM - 8:00 AM	**Networking Check-in with Continental Breakfast**
8:00 AM - 8:45 AM	**KEYNOTE Edward Snowden, the Ultimate Insider.** Steven Bay, Director-Threat Reconnaissance Unit, Security On-Demand; CISSP, Writer, Speaker
8:45 AM - 9:35 AM	**Data Driven Risk Indicators of Insider Threats** Jeffrey Huth, Vice President of Product Strategy at U.S. Information Services – Government Information Solutions at Transunion
9:35 AM - 10:25 AM	**Insider Threats Slipping Through the Cracks. "Whatcha Gon' Do 'bout it?"** Antonio "Tony" Rucci, Director, Information Security & Threat Intelligence at Information International Associates, Inc. (IIA)
10:25 AM - 10:35 AM	**COFFEE BREAK -** Please visit our sponsors, without them iTS4 would not be possible.
10:35 AM - 11:20 AM	**NCCoE: Increasing the adoption of standards-based cybersecurity technologies** Harry Perper, Chief Engineer, The MITRE Corporation Senior Cybersecurity Engineer, National Cybersecurity Center of Excellence at NIST
11:20 AM - 12 NOON	**The Intersection of Knowledge and Trust: Making "Need to Know" Work** Nat Bongiovanni, Chief Technology Officer at NTT Data Services
12 NOON- 1:00 PM	**LUNCH BREAK - hosted by Advanced Onion, Inc.** Head to the 10th floor to enjoy a complimentary networking lunch with the most breathtaking views of the Monterey Bay.
1:00 PM - 1:45 PM	**Where is your HITL?** Brandon Bean, Chief of Regional Support - West at Department of Defense
1:45 PM - 2:30 PM	**Killer Robots and Other Crazy Ideas** Chris Grijalva, Chief Technologist at GCE
2:30 PM - 2:40 PM	**BREAK**
2:40 PM - 3:10 PM	**Small Business Compliance with Controlled Unclassified Information (CUI) & Insider Threat Mitigation Requirements – A Primer** Kumar Gnanamurthy, Senior Vice President of iWorks Corporation
3:10 PM - 4:00 PM	**Forensic Investigations of Alleged Data Exfiltration** Dr. Adam Sorini, Managing Scientist and Dr. Dustin Burns, Scientist at Exponent, Inc.
4:00 PM - 4:10 PM	**BREAK**
4:10 PM - 5:30 PM	**KEYNOTE TRAINING WORKSHOP - Radically Cutting the U.S. Navy's Killchain - An Intrapreneurial DevOps Workshop** Warren Yu, Chief Learning Officer, Cebrowski Institute for Innovation at the Naval Postgraduate School
5:45 PM - 8:30 PM	**NETWORKING RECEPTION - Sponsored by Advanced Onion, Inc.**

insider threat

2018 SUMMIT

AGENDA - DAY 2
Tuesday, March 20

7:00 AM - 8:00 AM	**Networking Check-in with Continental Breakfast**
8:00 AM - 8:45 AM	**KEYNOTE PRESENTATION - Grandmothers, Gangsters, Guerrillas and Governments** KEYNOTE SPEAKER - Brian Contos, CISO and VP of Technology Innovation at Verodin
8:45 AM - 9:35 AM	**The Missing Link in Threat Mitigation - The Human Aspect of Motivation & Behavior** Brandon Porter, Assistant General Counsel *with* Juan Cole Vice President, Strategy and Solutions Consulting, Government Services, Equifax Inc.
9:35 AM - 10:25 AM	**Please refer to our website for this session information:** insiderthreatevents.com
10:25 AM - 10:35 AM	**COFFEE BREAK -** Please visit our sponsors, without them iTS4 would not be possible.
10:35 AM - 11:20 AM	**Evolving Threat Demands Evolving Response** Mr. Dean Clemons, Director of Cybersecurity Advisory Services for the US Public Sector region within DXC Technology
11:20 AM - 12 NOON	**Top 10 Epic Human Security Fails - Creating an effective security awareness culture.** Joshua Crumbaugh, Developer of the Human Security Assurance Maturity Model (HumanSAMM) and Chief Hacker at PeopleSec
12 NOON- 1:00 PM	**LUNCH BREAK** Head to the 10th floor to enjoy a complimentary networking lunch with the most breathtaking views of the Monterey Bay.
1:00 PM - 1:45 PM	**Federated Identity: The Foundation for Access Rights Management and Making "Need To Know" Work** Don Graham, Account Manager at Radiant Logic, Inc.
1:45 PM - 2:30 PM	**Benefits of a Cognitive AI based Insider Threat Prevention System** Dr. Venkat Rayapati, Founder &CEO of Cyber Forza, Inc.
2:30 PM - 2:40 PM	**BREAK**
2:40 PM - 3:10 PM	**A Whiskey Framework to Get Down and Dirty with Q&A** Nickolas Golubev, Chief of Engineering and Architecture at Advanced Onion, Inc.
3:10 PM - 4:00 PM	**Please refer to our website for this session information:** insiderthreatevents.com
4:00 PM - 5:00 PM	**CLOSING COMMENTS, Q&A** Paul Temple, CEO of Advanced Onion and Tech Regiment

insider threat

2018 SUMMIT

OVERVIEW

The 4th annual Insider Threat Summit (iTS4) will dig deeper and ask harder questions than ever before. Previous events thoroughly examined what an insider threat was. This year, iTS4 gets more technical, taking visions and turning them into focus, which can then immediately be utilized for a diverse landscape of solutions.

Presenters, attendees and sponsors are encourage to keep iTS4's format open and interactive. When it comes to insider threat topics, there is nothing one-sided about it. Participants are encouraged to share their challenges, solutions and previous experiences so everyone walks away with a greater knowledge base.

By coming together, our discussions, trainings and exchanges of ideas will aid in the overall understanding and ability to address how best to counter this costly problem that persists within various forms of insider threats.

iTS4 GOAL

To provide an open forum for key security-focused leaders who can share, enlighten and stimulate your security mindset, allowing you to meet challenges head on.

iTS4 FOCUS

- Cyber Security
- Personnel Security
- Ethical Security Considerations
- Detection and Deterrence of Insider Threats
- Continuous Evaluation of Privileged Identities

TECH REGIMENT

Tech Regiment's events are unique in that they are solution-focused, vision-driven and strategically geared to meet the needs of the attendees. They bring the industry's most relevant overarching topics and best-of-breed leaders from technology, data, security and cyber arenas to the Federal, State, local, educational and commercial audiences. Through carefully selected presentations and networking opportunities there is an endless amount of value at Tech Regiment events.

KEYNOTE SPEAKER

Steven Bay
Director-Threat Reconnaissance Unit, Security On-Demand; CISSP, Writer, Speaker

BIOGRAPHY

Steven Bay is the Director of Threat Intelligence at Security On-Demand, where he leads a team providing threat intelligence, hunting, and insider threat detection services. With over 15 years in cybersecurity, his career has spanned government, enterprise and consulting services. For a majority of his career, he served as an Analyst supporting the NSA via the US Air Force and Booz Allen Hamilton. While at Booz Allen, he served as Edward Snowden's boss just prior to Snowden's flight from the United States. Following his time supporting the agency, he designed and implemented information security programs for Fortune-500 companies and served as a CISO. He holds an MBA from Thunderbird School of Global Management and an MA in international relations from Webster University.

8:00 AM - 8:45 AM

Edward Snowden, the Ultimate Insider.

Having served as Edward Snowden's boss at the time Edward fled the country with millions of Top-Secret NSA documents, Steven will share his inside story of what happened with Snowden. His presentation will illustrate how Snowden matched the profile of a malicious insider and provide lessons learned and solutions focused on information security and insider threats.

8:45 AM - 9:35 AM

Jeffrey Huth
Vice President of Product Strategy at U.S. Information Services, Government Information Solutions at TransUnion

Data Driven Risk Indicators of Insider Threats

Insider risk programs use a combination of internal and external data on employees to highlight areas of risk. External data can show predispositions and stressors that might put someone at a higher risk of deciding to do something nefarious. In this presentation we will review our prior research and will provide updates on the best practices to use external data in insider risk programs.

9:35 AM - 10:25 AM

Antonio Rucci
Director, Information Security and Threat Intelligence at Information International Associates, Inc.

Insider Threats Slipping Through the Cracks. "Whatcha Gon' Do 'bout it?"

Your critical data… your corporate IP… your "secret sauce," and then, trust has been compromised. Someone has gone rogue; or was negligent. Either way, it's gone!

In the ensuing aftermath, you'll have to ask and address many hard questions… How did you get there? How did it happen? More importantly; What happened to the information? Where has it gone and ended up? How do you get it back? Can you get it back? How do you move forward? What could you have done to prevent it? What can YOU do?

We'll address these, and many other questions as we take a brief tour through several scenarios of the interrogatives of the Insider; addressing the Third-Order Effects and impact on things you may never be able to control, and maybe some which you can. Either way, it'll be an interesting, entertaining journey from old-school risks and threats to the cutting edge - IoT, Smart-Yet-Scandalous Technologies, yes, you guessed it… we're talking "Sex Toys." Oh, come on, I'm not the first one to talk about it! Maybe the first one here though! You'll stifle those chuckles when you see the results of years of dedicated research, and walk away with some how-to tips, and a smile.

10:35 AM - 11:20 AM

Harry Perper
Chief Engineer, The MITRE Corporation Senior Cybersecurity Engineer, National Cybersecurity Center of Excellence at NIST

NCCoE: Increasing the Adoption of Standards-Based Cybersecurity Technologies

Identity and access management is one of the pillars of cybersecurity that directly address the issues of insider threats. The NCCoE will discuss its identity and access management projects. The projects are based on standards based cybersecurity technologies.

The goal of this presentation is to convey the concepts the center has developed to integrate available technologies to address current identity and access management challenges.

11:20 AM - 12:00 NOON

Nat Bongiovanni
Chief Technology Officer at NTT Data Services

The Intersection of Knowledge and Trust: Making "Need to Know" Work

Multiple major compromises have occurred because people and/or devices had access to information that was not related to their function at all. A primary question should be "Why did they have access?"

This presentation will demonstrate an approach for your organization to implement "need to know" using Attribute Based Access Control (ABAC). ABAC cultivates the nuanced approach necessary to define who gets access to what in today's dynamic digital environment in contrast to the traditional Role Based Access Control (RBAC) methodology.

NTT DATA's ABAC methodology is designed to work in a dynamic environment where access to knowledge is governed by the "need to know" and granted to those who can be trusted.

1:00 PM - 1:45 PM

Brandon Bean
Chief of Regional Support - West at Department of Defense

Where is your HITL?

With machine learning taking the front seat in insider threat detection, organizations must ensure that they do not overlook the most vital part of the Insider Threat Detection Team: The Human-In-The-Loop (HITL). This presentation will look at the value of the HITL and provides vignettes where the HITL proved critical to the success of Insider Threat Detection.

1:45 PM - 2:30 PM

Chris Grijalva
Chief Technologist at GCE

Killer Robots and Other Crazy Ideas

A look at the potential future with regards to AI and Insider Threat. Exploring some possible near future scenarios and what the implications are.

2:40 PM - 3:10 PM

Kumar Gnanamurthy
Senior Vice President of iWorks Corporation

Small Business Compliance with Controlled Unclassified Information (CUI) & Insider Threat Mitigation Requirements – A Primer

Complying with government requirements for insider threat mitigation can be a daunting task, particularly for small businesses. Kumar Gnanamurthy will discuss DFARS compliance, insider threat monitoring, and loss prevention actions that small businesses can use to meet the government's requirements in manageable, cost-effective ways.

3:15 PM- 4:00 PM

Dr. Adam Sorini
Managing Scientist at Exponent

Dr. Dustin Burns
Scientist at Exponent

Forensic Investigations of Alleged Data Exfiltration

Exponent will present analysis techniques and tools employed to investigate cases involving alleged data exfiltration by one or more insiders, including discussion of the complexities of the analyses and questions that often arise during such forensic investigations.

4:10 PM - 5:30 PM

Warren Yu
Chief Learning Officer, Cebrowski Institute for Innovation at the Naval Postgraduate School

KEYNOTE WORKSHOP

Radically Cutting the U.S. Navy's Killchain - An Intrapreneurial DevOps Workshop

This provocative, disruptive discussion about improving our federal government's ability to manage change stems from the executive education of our nation's Admirals, Generals, and Senior civilian leadership. Condensed from 33 years to 90 minutes, this multimedia presentation uses digital storytelling and motion graphics.

Intended learning outcomes center around thinking, innovation, balance and how to sow a culture of *Learning.*

** Audience members should consult a physician beforehand if they possess health conditions like:*

- Heart trouble, high blood pressure, or motion sickness
- Infatuation with bureaucracy or an aversion to heretics
- Bodily control issues that may prevent them from properly bracing themselves during the presentation

***Rated R**

NOTES

continued notes section in back

5:45 PM - 8:30 PM, March 19th
NETWORKING RECEPTION

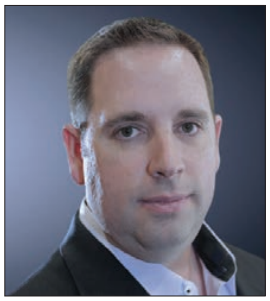
Advanced Onion, Inc. will be hosting the 4th Insider Threat Summit's networking reception. The reception is open to all registered attendees.

Located at the top of the Marriott downtown Monterey, in the Ferrantes Room on the 10th floor, the iTS4 reception boasts the best views of Monterey Bay!

There will be gourmet food, tasty beverages and like-minded company in an optimal setting for continuing discussions that were stimulated from the day's presentations.

We welcome you to enjoy this incredible opportunity of sharing similar interests with Insider Threat Summit presenters, fellow attendees, prospective partners and future employees.

Thank you Advanced Onion!



KEYNOTE SPEAKER

Brian Contos
CISO and VP of Technology Innovation at Verodin

BIOGRAPHY

Brian Contos has over two decades of experience in the security industry. He is a seasoned executive, board advisor, security company entrepreneur and author. After getting his start in security with the Defense Information Systems Agency (DISA) and later Bell Labs, Brian began the process of building security startups and taking multiple companies through successful IPOs and acquisitions including: Riptech, ArcSight, Imperva, McAfee and Solera Networks.

Brian has worked in over 50 countries across six continents. He is a strategic board advisor for multiple companies including Cylance and Appdome. He has authored several security books, his latest with the former Deputy Director of the NSA, spoken at leading security events globally and is a Distinguished Fellow with the Ponemon Institute. Brian frequently appears in the news and has been featured in CNBC, C-SPAN, Fox, NPR, Forbes, Wall Street Journal, The London Times and many others. He most recently appeared in a cyberwar documentary alongside General Michael Hayden (former Director NSA and CIA).

8:00 AM - 8:45 AM

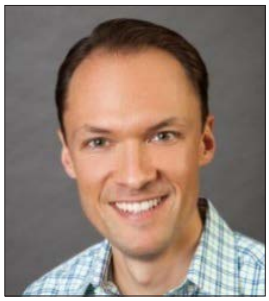
Grandmothers, Gangsters, Guerrillas and Governments

This presentation will explore threat actors including insiders, cybercriminals, hacktivists and nation-states. We will dissect how these actors operate and analyze their techniques to better understand what makes each group successful. This presentation will translate the “who, how and why” of cyberattacks. We will identify multiple “old school” and modern-day threat vectors and organize attacks by motives like financial and political. Each threat actor type will be explored in detail with real-life use cases and personal accountants based on my work in security in over 50 countries and 6 continents for the last 20 years.

insider threat

2018 SUMMIT

DAY 2 SPEAKERS



8:45 AM - 9:35 AM

Brandon Porter
Assistant General Counsel at Equifax Inc.

Juan Cole
Vice President, Strategy and Solutions Consulting, Government Services at Equifax Inc.

The Missing Link in Threat Mitigation - The Human Aspect of Motivation & Behavior

Unlike negligent employees who may accidentally cause a breach, malicious insiders make a choice to act based on personal life circumstances and motivations. An effective Insider Threat program requires a 360 view of personnel that integrates not only internal and contextual data but also relevant external data about an insider's activities. User behavior outside of the network or the work environment is sometimes the missing link in threat mitigation as it may be indicative of their likelihood to be a potential threat. Join us as we discuss the value and regulatory implications of leveraging 3rd party data, provide guidance on the use of the most-up-to-date available financial, employment and criminal data in continuous evaluation, and explore the possibilities of leveraging data-driven behavior insights as a missing link to mitigate insider threat.

insider threat

2018 SUMMIT

9:35 AM - 10:25 AM

Please refer to our website for this speaker session:
insiderthreatevents.com

10:35 AM - 11:20 AM

Dean Clemons
Director of Cybersecurity Advisory Services for the US Public Sector region within DXC Technology

Insider Threat: Evolving Threat Demands Evolving Response

Mr. Clemons' presentation will be a walk through the evolution of the insider threat and the commensurate technical response required to thwart the threat. The presentation will examine the evolution of countermeasures from single point monitoring through technical countermeasures built around context and insider behavior coupled with the analytics platforms that have shown merit in this space.

11:20 AM - 12:00 NOON

Joshua Crumbaugh
Developer of the Human Security Assurance Maturity Model (HumanSAMM) and Chief Hacker at PeopleSec

Top 10 Epic Human Security Fails - Creating an effective security awareness culture

This talk will outline the top 10 mistakes related to human security and why most companies are still failing. This will be followed up with actionable data derived from real-world training program successes and failures. Attendees will learn how to measure human risk accurately and most importantly how to remediate that risk.

Each mistake and misconception will come with a lesson learned, and these experiences can be used to create an effective security awareness program that will practically eliminate malware incidents. During the talk, I will review a case study of a business that was able to use these methodologies to take their non-weighted risk from 5. 7% to . 12% in less than 180 days. I will also discuss critical metrics and how to get the data you need to be successful in human security.

1:00 PM - 1:45 PM

Don Graham
Account Manager at Radiant Logic

Federated Identity: The Foundation for Access Rights Management and Making "Need To Know" Work

This year's conference features sessions from NIST/NCCoE outlining a framework for access rights management and from NTT Data Services discussing how we can make "Need to Know" work.

The NCCoE has developed an example implementation that demonstrates ways in which an organization can improve their information system security by limiting employee access to only the information they need to do their job, at the time they need it, and nothing more. NTT Data Services has developed an approach for organizations to implement "Need to Know" using Attribute Based Access Control (ABAC) to define who gets access to what in dynamic environments.

These approaches (and others) are all based on the premise that you have the identity foundation in place that allows you to authenticate the actors and understand their profile and contexts. Most organizations live in a decentralized, distributed, world where users and profile data are scattered across the enterprise.

This session will outline a strategy for leveraging your investment in existing identity sources to build a coherent, consistent identity that can be used across all IAM initiatives to ensure that actors are who they say they are and to provide granular access to only the things these actors should have access to. We will focus on reference implementations at NIST/NCCoE and NTT Data described previously but also provide a broader examples of the value of identity as the foundation and glue for IAM initiatives.

1:45 PM - 2:30 PM

Dr. Venkat Rayapati
Founder & CEO of
Cyber Forza, Inc.

Benefits of a Cognitive AI based Insider Threat Prevention System

Today's innovative workplace environment allows employees to easily gain access to an organization's critical and sensitive data. This innovation has increased the risk of insider threat from 11% to 40% over the last few years and organizations are now losing billions of dollars per year, some without knowing it. Insiders can attack in five separate ways: IT sabotage, fraud, intellectual property theft, organization security espionage and employee negligence, which result in organizations losing billions of dollars per year. We will discuss the benefits of implementing a Multi-layered cyber security defense approach to Detect, Identify and Prevent (DIP) with Cognitive AI at its core. This presentation will cover live use cases of insider threats include: Mission Critical Business Assets, Data Loss, Data Integrity, Data Forensics, IP Theft, Security Policies, Real Time Monitoring (RTM) and prevention. Practical internal threat prevention methods and use cases for the real world will be presented.

2:40 PM - 3:10 PM

Nickolas Golubev
Chief of Engineering and
Architecture at
Advanced Onion

A Whiskey Framework to Get Down and Dirty with Q&A

It's your turn, this session reverses the roles allowing the attendees to ask Nickolas challenging questions, or bring up pressing topics you and your team find yourself faced with. Bring a list of questions or ask him one big important one, as long as questions are kept within the realm of his expertise he will do his best to answer and provide his fresh perspective, insights and intelligent solutions. Nick specializes in the following areas:

- Cyber Security
- Risk Management Framework (RMF)
- System Compliance and Automation

LOCATION

Insider Threat Summit's host, Tech Regiment, is headquartered on the Monterey Peninsula where you will be strategically located near some of the leading defense, technology, medical, educational and scientific organizations within the Federal, State, local, commercial and educational arenas.

These are over-arching issues within each industry world-wide and everyone is vulnerable.

If anyone has the capability to fill holes in the online security community within California and beyond, it's the participants at the Insider Threat Summit. Building your presence on the Monterey Peninsula allows you to cement foundational relationships throughout a vast array of organizations who have secured excellent partnerships within the industry worldwide.

In addition to meeting your security needs, this amazing location boasts some of the richest history on the West Coast, as well as being saturated with world-class scenery, attractions, phenomenal restaurants and many other attractions. We are pleased you could make it to our fantastic corner of the world and hope you leave stimulated by new information and prospects.

insider threat

2018 SUMMIT

SUPPORTERS

Thank you sponsors for your expertise and support! We are excited at the level of your support and dedication to persistent insider threat topics. It is a privilege to bring you all together to meet these security challenges head on!

EQUIFAX

ADVANCED ONION
LAYERS OF TECHNOLOGY

TransUnion

Exponent

GCE

IIa Information International Associates

LexisNexis

CYBER FORZA

CONNECT···IO

AXIOMATICS FEDERAL

RADIANT LOGIC

RSA

POWDER RIVER
INDUSTRIES

DXC.technology

GD OPERATIONS

TECH REGIMENT

AXIDOME
PIVOTAL THINKING

NOTES

Hosted by:

TECH REGIMENT

insiderthreatevents.com

For more information on upcoming events please contact us:

@techregiment events@techregiment.com techregiment.com