insider threat

2017 SUMMIT

PROGRAM

March 29 - 30
Hyatt Regency
Monterey, CA

Information Security
Cyber Security
Privacy Risk
Identity Management
Operations Security

Hosted by Tech Regiment

insider threat

2017 SUMMIT

AGENDA - DAY 1
Wednesday, March 29

6:30 AM - 8:00 AM	**CHECK-IN & NETWORKING with Continental Breakfast**
7:45 AM - 8:00 AM	**WELCOMING REMARKS** Michael Sorrento, Director of Defense Manpower Data Center (DMDC)
8:00 AM - 8:45 AM	**KEYNOTE PRESENTATION - Fighting the Insider Threat: Plugging the Leak in the Digital Fence** Dr. Paul Vixie, CEO of Farsight Security
8:50 AM - 9:35 AM	**Data Breaches *Will* Happen. Be Defined by How You Recover.** Antonio Rucci, Director, Information Security & Threat Intelligence at Information International Associates, Inc.
9:35 AM - 10:25 AM	**Insider Threat: the Human Inside the Machine** Dan Dzenitis, Vice President of Business Development at Digital Reasoning
10:25 AM - 10:35 AM	**COFFEE BREAK - Sponsored by LexisNexis**
10:35 AM - 11:20 AM	**Financial Drivers for Insider Threat** Jeffrey Huth, Vice President of Product Strategy at U.S. Information Services – Government Information Solutions at TransUnion
11:20 AM - 12 NOON	**Inside the Cuckoo's Egg** Ryan Meeks, Human Factors Consultant and Insider Threat Expert at Frazer-Nash Consultancy
12 NOON- 1:00 PM	**LUNCH BREAK - hosted by Boeing** Coastal Lunch - Soup, Salad, Niman Ranch Pork Loin, Northern Salmon, Dessert and Beverages
1:00 PM - 1:45 PM	**Modeling Resilience** Wayne Lloyd, Federal CTO & Technical Director, CISSP at RedSeal
1:45 PM - 2:30 PM	**Using Data to Thwart the Insider Threat** Jason Rowe, Counterintelligence Integration Contract Program Manager for General Dynamics Mission Systems
2:30 PM - 2:40 PM	**BREAK**
2:40 PM - 3:10 PM	**Subversion from Within: The Ultimate Insider Threat** Cynthia Irvine, Distinguished Professor and Director of CISR at Naval Postgraduate School; Cyber Security Hall of Fame, 2015 Inductee
3:10 PM - 3:20 PM	**BREAK**
3:20 PM - 4:10 PM	**OPEN-PANEL DISCUSSION and Audience Engagement: Detect. Deter. Mitigate.** Gregg Seitz - Vice President and Co-Founder of Rhodes Edge Dr. Ellick Chan - Senior Associate, Statistical & Data Sciences Department at Exponent Michael Reith - Sales Engineer at Equifax Michael Lipinski - CISO and Chief Security Strategist at Securonix
4:10 PM - 5:00 PM	**Cyber Situational Awareness** Bob Palmer, VP, Solutions and Innovation at SAPNS2 with Timothy Evans, Co-Founder and Vice President of Strategy at Adlumin, Inc.
5:00 PM - 8:30 PM	**NETWORKING RECEPTION - Sponsored by Advanced Onion**

insider threat

2017 SUMMIT

AGENDA - DAY 2
Thursday, March 30

7:00 AM - 8:00 AM	**REGISTRATION & NETWORKING with Continental Breakfast**
8:00 AM - 8:30 AM	**WELCOMING REMARKS** Paul Temple, CEO of Advanced Onion and Tech Regiment
8:30 AM - 8:50 AM	**Using Theories of Attribution and Process Loss to Predict Conditions for Better Analysis** Captain Ryan Kelly, Information Systems Management Officer at Naval Postgraduate School
8:50 AM - 9:00 AM	**COFFEE BREAK - Sponsored by LexisNexis**
9:00 AM - 9:40 AM	**Find the Lipsyncer in a Choir of Hundreds: Identify the Insider Threat** Neil Carmichael, Director, Insider Threat Program at National Archives and Records Administration
9:40 AM - 10:20 AM	**Insider Threat Specialist: The New Breed of Analyst** Michael Caimona, Director of Strategy at Boeing
10:20 AM - 10:30 AM	**COFFEE BREAK - Sponsored by LexisNexis**
10:30 AM - 11:20 AM	**Privileged Users, Friends or Foe: A Security and Operations Perspective** Bill Johnson, CEO of TDi Technologies
11:20 AM - 12 NOON	**The Enemy Within: Detecting and Mitigating Insider Threats** Brian Vecci, Technical Evangelist at Varonis
12 NOON - 1:00 PM	**LUNCH BREAK - sponsored by A10 Networks** Tusca Lunch - Soup, Salad, Seared Halibut, Roasted Chicken Cacciatore, Desserts and Beverages
1:00 PM - 1:45 PM	**Identity Proofing and Multi-factor Authentication to Combat Insider Threats** Patrick Clancey, Vice President, Solutions and Strategy at Morphotrust
1:45 PM - 2:30 PM	**Insiders and Immune Systems - When Rules and Signatures Don't Work** Justin Fier, Director of Cyber Intelligence and Analytics at Darktrace
2:30 PM - 2:40 PM	**BREAK**
2:40 PM - 3:10 PM	**The Visible Attack Surface – What it is and Why it Matters** Kevin Flynn, Director of Products at Skybox Security
3:15 PM - 4:00 PM	**OPEN-PANEL DISCUSSION and Audience Engagement** Michael Pozmantier, Co-founder & Managing Director of the EdgeTech Group at Ratio Innovation Management Christian Grijalva, Chief Technologist at GCE Derick Smith, CEO of Ipso Microelectronics Robert Rounsavall, President & Chief Security Strategist of Trapezoid
4:00 PM - END	**Q&A / Audience Engagement and Closing Comments** • Check out sponsor giveaways • Pick up signed Certificates of Completion for 20 hours toward Continuing Professional Education Credits (CPE's) • Drop off Evaluation Forms at check-in table • Inquire about early sign-ups for Insider Threat Summit, 2018 (iTS4)!

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 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.

The 3rd annual Insider Threat Summit (iTS3) will discuss personnel security issues including information security, privacy risk management, cyber security challenges and capabilities, continuous evaluation of privileged identities and technical physical security considerations. With a newly developed and heightened awareness of insider threats, we have been brought together for one main purpose:

To better understand security challenges in order to better defend against insider threats.

iTS3 GOAL

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

iTS3 FOCUS

- Cyber security challenges & capabilities including personnel security issues
- Detection and deterrence of insider threats
- Continuous evaluation of privileged identities
- Ethical physical security considerations

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

DAY 1 SPEAKERS
OPENER and KEYNOTE

WELCOMING REMARKS

7:45 AM - 8:00 AM
Michael Sorrento
Director of
Defense Manpower
Data Center (DMDC)

BIOGRAPHY

Mr. Sorrento, a member of the Senior Executive Service, currently serves as the Director of the Defense Manpower Data Center (DMDC), a high performing operational support organization reporting to the Under Secretary of Defense for Personnel and Readiness. DMDC maintains the central repository of 50 million records for military, civilians, retirees, family members, and selected contractors. It is also the central point in the Department of Defense (DoD) for contract data. DMDC's four major business lines include: benefits and entitlements, identity management, decision support and personnel security/assurance. Over 250 employees and 800 on-site contractors work in Monterey, CA, Arlington, VA, or one of three satellite offices in Germany, South Korea, and Boyers, PA. Additionally, DMDC supports the operations of over 2,000 sites issuing ID cards and over 100 bases using its base access control system around the world, a truly world-wide operation. DMDC's mission directly supports the security of DoD's networks, facilities and personnel across the enterprise for identification of potential fraud and abuse, personnel policies and programs, the delivery of the right benefit to the right person at the right time, and most importantly the DoD's goal of a life-time relationship with its members and their families.

Mr. Sorrento began his federal career in 1990 with the Small Business Administration's Disaster Loan Program. He served in numerous supervisory, management and executive roles prior to being promoted to the Senior Executive Service in 2010. During his career with SBA, Mr. Sorrento was detailed for several lengthy field duty assignments to assist victims of disaster in their recovery efforts including the September 11, 2001 terrorist attacks, the Northridge earthquake and several hurricanes.

Mr. Sorrento was selected to the position of DMDC Director in November 2016, his third SES appointment within DoD. He previously held the position of Director, Cyber Capabilities and Compliance, AF CIO from September 2014 – November 2016... ...and Chief Information Officer, Assistant Secretary of the Air Force for Financial Management and Comptroller from October 2010 – August 2014.

KEYNOTE

8:00 AM - 8:50 AM
Paul Vixie
Chief Executive Officer
at Farsight Security

BIOGRAPHY

Paul Vixie was responsible for BIND from 1989 to 1999, and is the author of a dozen or so IETF RFC documents about DNS. He also started the first anti-spam company (MAPS), and was the founder and later president of the first U.S.-based commercial Internet Exchange (PAIX). Today he serves as CEO of Farsight Security, home of the Security Information Exchange (SIE) and the world's leading Passive DNS database (DNSDB). He is also co-inventor of the DNS Response Rate Limiting (RRL) and Response Policy Zone (RPZ) feature-sets now in widening use. He received his Ph.D. from Keio University in 2011, and was inducted into the Internet Hall of Fame in 2014.

Fighting The Insider Threat: Plugging The Leak In The Digital Fence

According to the 2016 U.S. State of Cybercrime Survey, 27% of electronic crime events were suspected or known to be caused by insiders. An employee, contractor or partner in your supply chain is leaking intellectual property and other sensitive data -- intentionally or accidentally -- from your organization. How do you determine motive, control your data and mitigate this risk? In this keynote presentation, Internet pioneer and Farsight Security CEO and Cofounder Dr. Paul Vixie will provide an overview of the insider threat as well as recommend tools, techniques and policies organizations can put in place to better protect against this critical cyberthreat.

DAY 1 SPEAKERS CONTINUED

8:45 AM - 9:35 AM
Antonio Rucci
Director, Information Security and Threat Intelligence at Information International Associates, Inc.

Data Breaches *Will* Happen... How You Recover Defines Your Company

Ransomware is No Joke! You've heard it many times before, and you'll continue to hear “it’s not a matter of if, but when…” you will at some point experience a data breach. Whether directly or indirectly, your measure for success will be built on your ability and speed to respond, recover and restore operations, minimizing impact to your customers, employees, intellectual property, industry reputation and ultimately your ROI. Throughout this talk, I’ll walk you through some proactive administrative, technical, and security operations to consider as you build out your disaster recover planning strategies.

Wait, What? You’re NOT building a D/R Strategy? I know, it’s usually an after-thought, but it’s much easier than you might think. We will review some fairly straight-forward things to consider to help better prepare your organization for that late Friday afternoon when things begin going sideways. Ransomware can really take a toll on organizations when they are ill-prepared. Some of the vendors in the next room over will become your best friends when that day comes. Invest a little time to ensure you are able to recover from and reconstitute your data in the unfortunate event there is catastrophic failure.You’ll walk away with a wealth of resources and building blocks to give you and your company a leg up!

9:35 AM - 10:25 AM
Dan Dzenitis
Vice President of Business Development at Digital Reasoning

Insider Threat: The Human Inside the Machine.

Actions by trusted insiders can result in serious and costly damage to sensitive information, national security interests, and place human lives in danger. Thus the requirement to continuously monitor for insider threats has become a top priority for agencies and organizations. Whether threats arise unwittingly by vulnerable employees, or maliciously by nefarious individuals that are becoming more proficient at their art, it is becoming increasingly difficult to detect and circumvent the next data or security breach. With the assistance of machines, the threat landscape is now changing. Going beyond keywords, lexicons and simple searches, and leveraging investments in big data and their information packed data lakes, artificial intelligence is now being used to uncover human behaviors and intent. AI is leveraging current investments in access detection and bringing together a situational perspective that was previously unthinkable.

DAY 1 SPEAKERS CONTINUED

10:35 AM - 11:20 AM
Jeffrey Huth
Vice President of Product Strategy at U.S. Information Services, Government Information Solutions at TransUnion

Financial Drivers for Insider Threat

Financial stress can happen to anyone for a variety of reasons. Seeking relief from financial stress, an employee may choose to perform some illicit activity as an insider with the hope of monetary gains. In this session we will examine some of these stressors and present the results of a financial profiling study performed on government employees.

11:20 AM - 12:00 NOON
Ryan Meeks
Human Factors Consultant and Insider Threat Expert at Frazer-Nash Consultancy, Ltd.

Inside the Cuckoo's Egg

Technological developments and an increasing reliance on cyber networks in recent years have redefined the risks associated with malicious insider threats. Regardless of the environment though, insider threat remains a ‘people problem;’ affected by a myriad of complex socio-cultural, organisational and behavioural influences. Key to effective management is an understanding of the intricacies of insider threat psychology that underpin malicious motivation, something that most organisations are struggling to achieve. This presentation will outline the psychological effects,... ...environmental and personal influences and catalysts affecting insider threat, and provide an overview of why understanding the insider psychology is essential to achieve ‘next generation’ safety and security.

1:00 PM - 1:45 PM
Wayne Lloyd
Federal CTO & Technical Director, CISSP at RedSeal

Modeling Resilience

Today’s networks and digital systems must mirror the “military sand table” for effective mission planning and educational purpose. Networks must become an ongoing model of visibility and understanding through quantifiable measurement; a living tract of landscape that lets you continuously and quickly grasp where your high value assets are, how they are at risk and prioritize real-time actionable intelligence of how they can be protected and what must be remediated first. Simply put, “You can’t manage what you can’t measure.”

- State of the Nation – Current state, what we’re seeing, what we know.
- What’s Next? – What cyber chaos lies ahead?
- How Do We Win? - Management through performance based measurement, the only way to win the war.

1:45 PM - 2:30 PM
Jason Rowe
Counterintelligence Integration Contract Program Manager for General Dynamics Mission Systems

Using Data to Thwart the Insider Threat

Insider Threat is more than a tool. General Dynamic Mission Systems' multi-stage approach to Insider Threat looks at the entire organization, builds upon existing capabilities, integrates best of breed software, ensures compliance with legal, privacy and civil liberties issues, and leverages subject matter experts in all related disciplines to deliver a robust solution for each customer. Our modular solution to Insider Threat ensures each organization obtain only those services that the needs of their program require to detect, deter and mitigate insider threats including espionage, sabotage, fraud, and workplace violence.

2:40 PM - 3:10 PM
Cynthia Irvine
Distinguished Professor of Computer Science at the Naval Postgraduate School and Cyber Security, Hall of Fame 2015 Inductee

Subversion from Within: The Ultimate Insider Threat

Suppose an adversary was on the development team for a highly sophisticated military system. What kind of damage could be wrought? For decades, subversion from within has been considered a serious threat. Today, as our supply chains span the globe, the threat of subversion has become more palpable, as well as more complex. When dealing with an intelligent adversary, can we address the subversion threat?

3:20 PM - 4:10 PM
OPEN-PANEL DISCUSSION and AUDIENCE ENGAGEMENT

Gregg Seitz
Vice President and Co-Founder of Rhodes Edge

Dr. Ellick Chan
Senior Associate, Statistical and Data Sciences Department at Exponent

insider threat
2017 SUMMIT

Michael Reith
Sales Engineer at Equifax

Michael Lipinski
CISO and Chief Security Strategist at Securonix

Detect. Deter. Mitigate.

Panel members will be challenged by some hard-to-answer questions. ***We welcome you to bring your own questions, issues and ideas to the conversation.*** Below are some examples of the topics this panel will be addressing from their equally diverse and deep-rooted backgrounds.

1. Best practices for managing false positives and false negatives in large data sets. Problem: tight match logic limits false positives (noise) but also may exclude relevant results (faint signal) and results (signals) .

2. Translating online (web content) data (unstructured & alias) to the offline (physical world) using attribute data and digital signatures. Where to start: the relevant content or the individual?

3. Data: Volume, Velocity, Variety and Veracity

DAY 1 SPEAKERS CONTINUED and RECEPTION

4:10 PM - 5:00 PM
Bob Palmer
VP, Solutions and Innovation
at SAPNS2

4:10 PM - 5:00 PM
Timothy Evans, J.D., LL.M.
Co-Founder & Vice President
of Strategy at Adlumin, Inc.

Technology innovations to support near real-time anomaly detection and behavioral analysis of insider threat.

Insider threat detection and mitigation has driven new requirements for High Performance Data Analytics that differ from other missions in two aspects: speed and complexity. We will discuss emerging technologies which can enable new approaches and help to execute complex algorithmic methods including graph analysis, machine learning, event stream processing, natural language processing, “fuzzy search” and time series analysis. We’ll also cover new hardware innovations in FPGA (field programmable gate arrays) targeted on acceleration of netflow analysis in order to identify and mitigate threats in near real time.

5:00 PM - 8:30 PM
NETWORKING RECEPTION hosted by Advanced Onion

Advanced Onion, Inc. will be hosting the 3rd annual Insider Threat Summit’s networking reception. The reception is open to all registered attendees and is located in the Conference Center foyer and terrace. 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 unique opportunity of sharing similar interests with Insider Threat Summit presenters, fellow attendees, prospective partners and future employees.

Thank you Advanced Onion!

ADVANCED ONION
LAYERS OF TECHNOLOGY

Advanced Onion (AO) is a Service Disabled Veteran Owned Small Business (SDVOSB) and a California Certified Disabled Veteran Business Enterprise (CA DVBE). As a technology and business services company they specialize in systems integration, cyber security, privacy risk mitigation and personnel identity management. AO delivers unique solutions to commercial and government customers with a focus on Federal, State and local governments.

advancedonion.com

f /advancedonion
@advancedonion
in Advanced Onion, Inc.

8:00 AM - 8:30 AM
Paul Temple
CEO of Advanced Onion
and Tech Regiment

Welcome to iTS3, Day 2!

iTS3 moderator, Paul Temple, will say a few words about the methodologies behind iTS3, including:

- Event highlights
- Upcoming events that will dig deeper into some of these highly relevant issues, such as Data Sciences....
- Important announcements

8:30 AM - 8:50 AM
Captain Kelly Ryan
Information Systems
Management Officer at the
Naval Postgraduate School

Insider Threat Research Briefing on Cognitive Psychology

A briefing on Ryan Kelly's research, which is focused on the cognitive psychology of insider threat analysts who seek out insider threats to cyber security. His work uses theories of attribution and process loss to predict conditions for better insider threat analysis.

8:50 AM - 9:35 AM
Neil Carmichael
Director, Insider Threat Program
at National Archives and
Records Administration

Find the Lipsyncer in a Choir of Hundreds: Identify the Insider Threat

Today's Insider Threat can hide under the voluminous amount of data or "noise" within an organization. It is very similar to identifying someone who is lip-syncing or singing softly during a choral concert, when they are hidden among many other voices. How do you identify the Insider Threat within your organization? How can you use your people, processes, and policies to mitigate, detect and deter our lip-syncing singer or Insider Threat? You need to find ways to attenuate the noise with strategies that allow your program to detect and deter the threat, while using organization policies with a measure of accountability.
You cannot ignore the human side of the Insider Threat equation! So, how do you reduce the normal noise created across your infrastructure? Learn how one Federal agency took advantage of the policies and procedures that already existed across the organization to mitigate their own Insider Threat risk.

DAY 2 SPEAKERS CONTINUED

9:35 AM - 10:25 AM
Michael Caimona
Director of Strategy at Boeing

Insider Threat Analysts: Investing in Tradecraft

As the private and public sectors solidify their technology approaches to combat insider threats, a new discipline of analytic tradecraft is emerging. Insider Threat Analysts are being exposed to new data sources, new threat vectors and new methods of concealment daily. In order to meet the growing challenges facing security organizations, we must invest in this new breed of analyst to further develop their methodology, approaches and skill sets. Immersive scenario-based training simulations are a way to prepare the new cadre of analysts for their evolving roles.

10:35 AM - 11:20 AM
Bill Johnson
Founder and CEO of TDi Technologies

Privileged Users, Friends or Foe: A Security and Operations Perspective

IT organizations are increasing their budgets each year to monitor real time and latent activities that occur on servers, routers, switches and other enterprise-wide devices to prevent a corporate data breach. These tools collect logs of data on devices but are often limited in monitoring a... ...specific device and human interactivity performed by Privileged Insiders, the enterprise administrators who have unrestricted access to critical corporate data and employee credentials.

A breach of a corporation's data assets by malicious insider activity is the most common yet most elusive. An effective approach is Proactive Monitoring and control of all the activity, human and machine performed by these Privileged Insiders, which has benefits for both IT & OT security/operations policies. This session will discuss the policies and proactive initiatives an organization should consider to protect against enterprise insider threats and enhance security/operations for both IT & OT.

11:20 AM - 12:00 NOON
Brian Vecci
Technical Evangelist at Varonis

The Enemy Within: Detecting and Mitigating Insider Threats

Ransomware is both scourge and savior. While it's not typically considered an insider threat, it acts from the inside, using insider identities, encrypting files that insiders have access to on endpoints and file shares. Learn how organizations are using ransomware to identify and confront vulnerabilities that expose them to rogue employees, abusive administrators, and hackers.

DAY 2 SPEAKERS CONTINUED

1:00 PM - 1:45 PM
Patrick Clancey
Vice President, Solutions and Strategy at Morphotrust

Identity Proofing and Multi-factor Authentication to Combat Insider Threats

This session will explore the use of strong proofing and multi-factor authentication tools to augment traditional Identity and Access Management (IAM) and Security Information and Event Management (SIEM) systems utilized to combat insider threats. Discussion of authenticators, credentials, and assertions will all be explored in the context of identity assurance as a flexible, enabling capability.

1:45 PM - 2:30 PM
Justin Fier
Director of Cyber Intelligence and Analytics of Darktrace

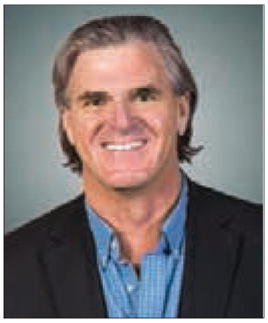
Insiders and Immune Systems - When Rules and Signatures Don't Work

Over two years after the Snowden leak, organizations are still struggling to reconcile the need for competitive, information-sharing cultures with security requirements. Insider threat is a major challenge because our organizations are full of them – and these people do not need to have malicious intent to do lasting damage. The reality is that you cannot trust every insider to make the right decision 100% of the time. As networks get bigger and more unpredictable, spotting the needle in a growing haystack gets harder. Genuine innovations in science and technology are changing the security paradigm however. Today, immune system technology is quickly becoming the de facto insider threat defense technology, deployed over 1,000 installations globally.

In this session, learn how companies with living 'immune systems' are able to:

- Visualize 100% network activity graphically, from high-level overviews to forensic detail required for in-depth investigations
- Detect emerging threats, without requiring to train the immune system in advance
- Immediately identify abnormal behaviors, based on bespoke knowledge of individual networks and users – not broad assumptions
- Derive instant value that protect against a whole spectrum of internal threats – not just threats that fit a specific known pattern
- Apply lessons of government intelligence to today's private-sector defense challenge

DAY 2 SPEAKERS CONTINUED



2:40 PM - 3:10 PM
Kevin Flynn
Director of Products at Skybox Security

The Visible Attack Surface – What it is and Why it Matters

During this session, you will learn what makes up the layers of the attack surface and how gaining visibility to Indicators of Exposure (IOEs) can shrink it and more effectively contain incidents from insider threats. Understand how network modeling and simulation can be used to visualize and analyze the attack surface and how to measure IOEs such as vulnerability density, remediation latency and network zoning compliance. Identify the best strategies for targeted elimination of IOEs. Comprehend the business impacts of using IOEs, such as response time improvements and risk reductions, as well as how CISOs are empowered when company executives can see the attack surface to better understand both internal and external threat exposures.

- What makes up the layers of the attack surface and IOE?
- How can network modeling and simulation be used to visualize and analyze the attack surface?
- How to best measure IOE such as vulnerability density, remediation latency and network zoning compliance?
- What are the business impacts of using IOE, such as, response time improvements and risk reductions; how are CISOs empowered when company executives can see the attack surface and understand threat exposures?
- How can IOEs be used to better understand and secure hybrid IT environments (physical, virtual and cloud)?

DAY 2 SPEAKERS
OPEN-PANEL DISCUSSION

3:20 PM - 4:20 PM
OPEN-PANEL DISCUSSION, AUDIENCE ENGAGEMENT and Q&A

Michael Pozmantier
Co-founder & Managing Director of the EdgeTech Group at Ratio Innovation Management

Derick Smith
CEO of Ipso Microelectronics

Christian Grijalva
Chief Technologist at GCE

Robert Rounsavall
President & Chief Security Strategist of Trapezoid

Physical and Logical Access to Firmware, Hardware and Software Represent the Insider Vulnerabilities to Data.

Panel members will be challenged by some hard-to-answer questions. ***We welcome you to bring your own questions, issues and ideas to the conversation.*** Below are some examples of the topics this panel will be addressing from their equally diverse and deep-rooted backgrounds.

1. Robust identity management (IdM) as a security enhancer
2. Effective use cases of data science applications for security in detecting anomalous insider behavior
3. Solidifying irrefutable digital identity to online interaction; how it eliminates a variety of threats
4. Consideration about the monetizing of insider threat via the dark web

SPONSORED STUDENTS

Oscar Ramirez
Computer Science,
Hartnell College

Michèle Marchese
IT Security,
Western Governors Univ.

Steven Willey
Network Security,
Hartnell College

Remberto Nunez
Computer Science,
Hartnell College

A huge thank you goes to Advanced Onion and MorphoTrust for sponsoring local students to attend the 3rd Annual Insider Threat Summit (iTS3). The knowledge and connections they gather from this event are priceless! iTS3 gives them a chance to share their fresh perspectives with seasoned professionals, while hearing from top security leaders and threat experts from all over the world.

Past Insider Threat Summit's have allowed students to enjoy experiences such as dining with the CA State CISO, networking with speakers and sponsors from DARPA, DSS, DMDC, NPS, HPE, Boeing and Cisco (to name a few), interviewing with KSBW Action News, adding their insights to open-panel discussions and much more. Some students have even been ***hired directly out of college.***

If you have internships available or would like to connect with these students for job opportunities, please contact the iTS3 event coordinator, Mia Medeiros at the Check-In Table for the best way to connect.

Happy Networking!

ADVANCED ONION
LAYERS OF TECHNOLOGY

SAFRAN
MorphoTrust USA

insider threat

2017 SUMMIT

SPONSORS

Thank you sponsors for your expertise and support! You have succeeded in making iTS3 an outstanding event for all participating parties. 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!

Digital Reasoning

TransUnion

DARKTRACE

SECURONIX

ADVANCED ONION
LAYERS OF TECHNOLOGY

FARSIGHT SECURITY

REDSEAL

VARONIS

EQUIFAX

Exponent

BOEING

GENERAL DYNAMICS
Mission Systems

TD

SAFRAN
MorphoTrust USA

rhodes edge INC

SKYBOX SECURITY
Total Visibility. Focused Protection.

GCE

NS2
SAP NATIONAL SECURITY SERVICES

A10

TRAPEZOID
Firmware Integrity Management

OTCXN

LexisNexis

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.

California, like most areas, needs security solutions and experts to directly respond to issues. There's been a chain of critical reactions due to cyber security mandates put in place by the CA Governor's office in 2016 after accusations were made by State lawmakers stating the CA Department of Technology **officials are failing to keep state agencies secure**. They were deemed vulnerable to insider threats and hacks. California, a leader in the world of technology, is not the only location in the "hot seat." 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, 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.

Hosted by:

TECH REGIMENT

insiderthreatevents.com

For more information on upcoming events please contact us:

@techregiment events@techregiment.com techregiment.com