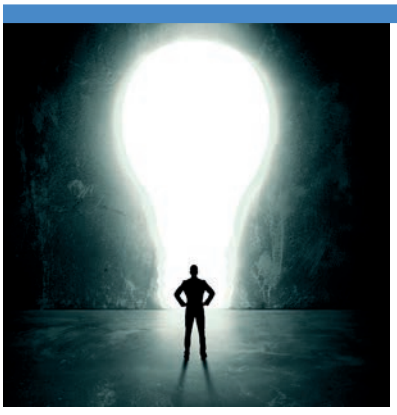
insider threat

2016 SUMMIT

PROGRAM



Information Security

Cyber Security

Operations Security

March 29 - 30
Hyatt Regency Hotel & Spa
Monterey, California

Hosted by Tech Regiment

insider threat

2016 SUMMIT

AGENDA - DAY 1
Tuesday, March 29

6:30 AM - 8:00 AM	**REGISTRATION OPENS & NETWORKING BREAKFAST - sponsored by DarkTrace**
7:55 AM - 8:00 AM	**WELCOMING REMARKS** Paul Temple, CEO of Advanced Onion and Tech Regiment
8:00 AM - 8:50 AM	**KEYNOTE PRESENTATION - Are You Ready?** Chris Grijalva, Division Director for Physical Security and Law Enforcement, and Senior Intelligence Officer at Defense Manpower Data Center (DMDC)
8:50 AM - 9:00 AM	**BREAK**
9:00 AM - 9:40 AM	**Case Study: How Insider Threat Unfolded in Livingston County, MI** Rich Malewicz, Deputy County Administrator/CIO at Livingston County, MI
9:40 AM - 9:50 AM	**BREAK**
9:50 PM - 10:35 PM	**Cyber Security - Exploring the Threat Landscape** Maj. General (Ret.) Earl Matthews, Vice President, Enterprise Security Solutions HP Enterprise Services, U.S. Public Sector for Hewlett-Packard Enterprise
10:35 AM - 11:20 AM	**Insider Threat Specialist: The New Breed of Analyst** Michael Caimona, Director of Strategy for Boeing Integrated Information Systems (IIS)
11:20 AM - 12 NOON	**Making Behavioral Analytics Work in the Real World** Karthik Krishnan, VP of Product Management at Niara
12 NOON- 1:00 PM	**LUNCH BREAK - hosted by Boeing** Build your own sandwich with fresh deli selections, spreads and breads with Chef's dessert
1:00 PM - 1:45 PM	**"All your attacks belong to insiders" – A Modern People, Process, and Technology Approach to Combating Insider Cyber Attacks** Kenneth Sean Patrick, Senior System Security Engineer at Vectra Networks
1:45 PM - 2:30 PM	**How Do You Connect the Invisible Dots?** Alison Ryan, Vice President of Business Development at Reservoir Labs
2:30 PM - 2:40 PM	**BREAK**
2:40 PM - 3:25 PM	**Recent DARPA Sponsored R&D Advances the State-of-the-Art in Cyber Security** Dr. Raymond Richards, I2O Program Manager at DARPA
3:25 PM - 4:10 PM	**Innerworkings of the Defense Security Service Mission** Michael M. Buckley, Chief, Defense Insider Threat Management and Analysis Center Implementation Counterintelligence Directorate, Defense Security Service (DSS)
4:10 PM - 4:20 PM	**BREAK**
4:20 PM - 5:20 PM	**OPEN - PANEL Discussion and Audience Engagement** Peter Ateshian with NPS, Andrew Smith from Advanced Onion, Samantha Leach from Expressworks and Dr. Christopher Williams from Exponent
5:30 PM - 8:30 PM	**NETWORKING RECEPTION - Sponsored by HP Enterprise and FireEye**

insider threat

2016 SUMMIT

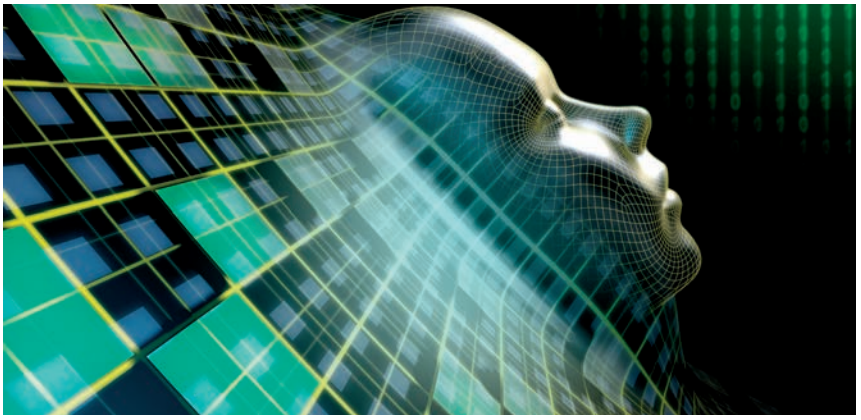
AGENDA - DAY 2
Wednesday, March 30

6:30 AM - 8:00 AM	**REGISTRATION & NETWORKING BREAKFAST - sponsored by PaloAlto Networks**
7:55 AM - 8:00 AM	**WELCOMING REMARKS** Paul Temple, CEO of Advanced Onion and Tech Regiment
8:00 AM - 8:50 AM	**KEYNOTE PRESENTATION - When the Insider Threat Has Authority Over You** Antonio Rucci, Owner & Principal at Insider Threats Consulting
8:50 AM - 8:55 AM	**BREAK**
8:55 AM - 9:40 AM	**The Whole Person Risk Model for Insider Threat** Bryan Ware, President and CTO of Haystax
9:40 AM - 9:50 AM	**BREAK**
9:50 AM - 10:35 AM	**Man in the Middle Role Based Access for Applications** Rick Simmons, Director, Federal Software Sales at Brocade
10:35 AM - 11:20 AM	**Building a Practical Insider Threat Program and Making It Work** Gaby Friedlander, Co-Founder and CTO of ObserveIT
11:20 AM - 12 NOON	**Insiders and Immune Systems – When Rules and Signatures Fall Down** Nicole Eagan, CEO of Darktrace
12 NOON - 1:00 PM	**LUNCH BREAK - sponsored by LogRhythm** Build your own sandwich with fresh deli selections, spreads and breads with Chef's dessert
1:00 PM - 1:45 PM	**Scoring the Insider / Evaluating the Risk** Mark Sheppard, Federal CIO & Yvonne Phillips, Senior Statistical Modeler - Government from LexisNexis
1:45 PM - 2:30 PM	**Understanding BitCoin - The Fuel Powering the Underground Economy** Anshu Gupta, Director of Information Security at HelloSign
2:30 PM - 2:40 PM	**BREAK**
2:40 PM - 3:25 PM	**Insider Threat Detection: Defending from Actors within the Network** Stephen Marker, Deputy Director of Technology, General Dynamics Mission Systems
3:25 PM - 4:10 PM	**Today's "Identity Crisis" and National Security: Pinpointing Threats Using Multiple Characteristics of Identity** Patrick Clancey, Director of Federal Programs at MorphoTrust
4:10 PM - 4:20 PM	**BREAK**
4:20 PM - 5:20 PM	**OPEN - PANEL Discussion and Audience Engagement - Human & Technological Patterns of Risk** Earl Matthews from HPE, Tammy Torbert with HPE Security, Karthik Krishnan of Niara and Bryan Lee with Palo Alto Networks
5:30 PM - END	**Q&A / Audience Engagement and Closing Comments** Vendor giveaways and Certificates of Completion for 20 hours toward Continuing Professional Education Credits (CPE's)

insider threat

2016 SUMMIT

OVERVIEW



Tech Regiment events are unique in that they are solution-focused, vision-driven and strategically geared to meet the needs of attendees. We 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 & commercial audiences. Through carefully selected presentations and networking opportunities there is an endless amount of value at Tech Regiment events.

The 2016 Insider Threat Summit (ITS2016) will discuss personnel security issues including 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.

ITS2016 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.

ITS2016 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.

8:00 AM - 8:50 AM
Chris Grijalva
Director for Physical Security and Law Enforcement, and Senior Intelligence Officer at Defense Manpower Data Center (DMDC) at Defense Manpower Data Center (DMDC)

Are You Ready?

A presentation about the broader definition of insider threat to include everyday actions that increase or decrease threat. This includes a discussion about what happens when an event occurs at an organization and how to better prepare to recover. Also, included in the discussion will be some of the unforeseen consequences and lessons learned from the massive data breach at the Office of Personnel Management.

BIOGRAPHY - Christian "Chris" Grijalva is the Division Director for Physical Security and Law Enforcement at DMDC. Chris also serves as the organization's Senior Intelligence Officer with responsibility for all classified operations support to the Intelligence Community. He has over 20 years of enterprise information technology (IT) experience with a degree in International Cyber Forensics and a certification as a Lean Six Sigma Master Black Belt.

Chris began his career in the Department of Defense at DMDC in 1993 as an intern. After nine months he was hired on in a permanent position as a system engineer and served as lead engineer implementing solutions supporting the Gulf War (Operation Desert Shield/Desert Storm) post-war operations and biometrically enabled access control systems. In 2000, Mr. Grijalva was selected to fill the role of Deputy Director of IT Operations. In this capacity, he lead all enterprise IT implementations and strategic direction. Starting in 2006, Chris moved again to become the Chief Technology Officer for a few years during which time he served as the acting CIO for a year.

At the end of 2009 Mr. Grijalva was named the Division Director of Identity Services and assumed responsibility for all globally deployed DMDC systems including the Common Access Card (CAC) program, Defense Biometric Identification System (DBIDS/IACS) and the Non-Combatant Evacuation Operation Tracking System (NTS). When the earthquake and subsequent tsunami hit Japan in 2011, the NTS solution, Mr. Grijalva and his team were called upon to manage the evacuation accountability and tracking of US persons out of Japan. Most recently, Mr. Grijalva led the architecture and implementation of the Identity Matching for Enterprise Security Analysis (IMESA) system. This system was developed and implemented in response to the directive and recommendation stemming from the Ft. Hood and Washington Navy Yard incidents. IMESA has had a tremendous impact to security by identifying over 4000 wanted felons that were accessing DoD facilities flagging nearly 40k fraudulent and invalid ID cards in its first year of operation. Chris and his team have also been at the forefront the Department's pilot programs for the Continuous Evaluation effort. Chris is currently the DoD technical lead on behalf of the DoD CIO in support of mitigations related to the OPM data breach.

9:00 AM - 9:40 AM
Rich Malewicz
CIO / CISO of
Livingston County, MI

Case Study: How Insider Threat Unfolded in Livingston County, MI

Learn first-hand of how insider threat management software was used to detect and mitigate a series of insider threats at a local government county. This discussion will go over the chain of events involved in a real-life insider threat incident, how to detect early indicators of insider threat by monitoring user behavior, and the key components of a user-centric security program based on user behavior analytics.

9:50 AM - 10:35 AM
Maj. General (Ret.) Earl Matthews
Vice President, Enterprise Security Solutions, U.S. Public Sector, Hewlett Packard Enterprise

Cyber Security-Exploring the Threat Landscape

Cyber attacks have become more organized, advanced, persistent and adaptive. It is imperative for government organizations to be prepared to meet these dire challenges and still meet current user's demands and compliance requirements. This session will explore the tactics attackers use at the front lines of cyber warfare, as well as some of the best practices for preparation and response.

Presenation highlights include:
- It is no longer enough to focus on only protecting infrastructure...

... continued

- We need to proactively protect the interactions between users, applications and data across any location or device.
- Why enterprises can't keep up: legacy technologies, skills, shortage, new style of IT and lack of visibility
- What we have learned in the trenches: cyberspace is an asymmetrical theater, "perimeter" is not about your network, rethink the human element

10:35 AM - 11:20 AM
Michael Caimona
Director of Strategy for Boeing Integrated Information Systems (IIS)

Insider Threat Specialist: The New Breed of Analyst

As industry and government continue to establish programs to counter the growing insider threat challenge, security professionals are inundated with new technology and policy. However, at the core of any successful insider threat program are the talented analysts charged with wading through fields of new data and evaluating critical risk factors, behavioral indicators and technical activity. The tradecraft of the Insider Threat Specialist is emerging and requires broad experience and a cross-discipline approach. Developing this new cadre of analysts is equal to, if not more critical than implementing policy and deploying state-of-the-art technology.

11:20AM - 12 NOON
Karthik Krishnan
Vice President of Product Management at Niara

Making Behavioral Analytics Work in the Real World

Global patterns of known good and bad are no longer sufficient to detect and investigate modern attacks. Real-time threat detection and prevention, even if leveraging machine learning and analytics, are noisy, prone to false positives and add to the alert white noise. Many of the attacks are already on the inside of the network and often manifest themselves as originating from legitimate users and hosts even if they have been compromised. In addition, negligent and malicious insiders are hard to unearth. Too often any signals that would indicate an anomaly are often weak and difficult to spot.

In this session, we will demonstrate practical ways in which behavioral analytics techniques can be used to detect and investigate compromised users, entities and malicious insiders. Topics will include:

- Innovative frameworks for how user behavior analytics can be flexibly applied to diverse data sources to detect privilege escalation, command and control, internal reconnaissance, lateral movement, abnormal resource access and exfiltration
- How user behavior analytics has to be combined with "global" or "cross enterprise" analytics to more reliably link anomalies to malicious intent and reduce false positives
- How entity risk profiles can be built to thread a needle across multiple "weak signals" to potentially identify a larger attack underway
- How detection alone is not sufficient without having the forensic context necessary to investigate
- Real world examples of how user behavior analytics, global analytics and forensic context can come together to help detect and investigate modern attacks

1:00 PM - 1:45 PM
Kenneth Sean Patrick
Senior System Security Engineer at Vectra Networks

"All your attacks belong to insiders" – A Modern People, Process, and Technology Approach to Combating Insider Cyber Attacks

Modern cyber attacks are perpetrated from an insider's perspective whether they be from an external attacker who has penetrated the perimeter or a trusted person on the inside. Cyber attackers steal credentials and passwords to bypass traditional defenses and use insider privilege to affect information systems, networks and cyber operations. Traditional insider threats leverage the same processes to impact organizations as external cyber attackers. The good news is there's an overlap in the investment in the people, process and technology controls used to combat both types of attackers.

In this session we will explore the insider threat challenge and discuss a people, process and technology set of concepts in creating a proper security management program to detect and avert insider cyber attacks. The talk will include:

- Comparison of an insider attack versus the Carbanak APT attack
- Enterprise vs. tactical environments and the need for proper information-assurance controls
- Challenges with the shift from "need to know" to "responsibility to provide"
- An approach to combat insider attacks through a synergistic people, process and technology approach
- Modern network and host-based advanced cyber analytic approaches
- Combining human produced, physical security and cyber information to increase the probability of detection

1:45 PM - 2:30 PM
Alison Ryan
Vice President of Business Development at Reservoir Labs

How Do You Connect the Invisible Dots?

An obfuscated attack, such as the systematic, but distributed scraping of data by an insider, relies on hiding individual attack actions within a broader pattern of normal activity. In hindsight, the individual attack dots are easy to connect, but as the attack unfolds, the common purpose of the individual's actions - what truly distinguishes the attack from normal activity - remains invisible. Traditional workflows rely on finding suspicious dots and then using a mix of automated and human analysis to run the meaning of those dots to ground. In practice, this method fails for two reasons: (1) insiders can craft their actions to subvert signature-based detection methods, thus denying analysts even a starting point for investigation, and (2) the process of piecing together the broader purpose of an attack from the individual actions requires painstaking analysis. We will share Reservoir Labs' open, unsupervised learning approach to this challenge.

2:40 PM - 3:25 PM
Dr. Raymond Richards
I2O Program Manager at Defense Advanced Research Projects Agency (DARPA)

Recent DARPA Sponsored R&D Advances the State-of-the-Art in Cyber Security

Dr. Richards will present an overview of R&D sponsored by the DARPA Information Innovation Office (I2O) in the...

...continued

area of cyber security. As much of the world-wide economy has moved into cyberspace, protecting and assuring information flows over networks has become a priority. Most networks today rely on the successive discovery of vulnerabilities and deployment of patches to maintain security. Even after patching, new vulnerabilities are often introduced in successive releases, and may even be introduced by the patches themselves. The I2O cyber R&D portfolio is largely focused on changing this paradigm through a variety of methods such as heterogeneity, formal methods proofs, secure code generation and automation.

3:25 PM - 4:10 PM
Michael Buckley
Chief, Defense Insider Threat Management and Analysis Center Implementation Counterintelligence Directorate, Defense Security Service (DSS)

Innerworkings of the Defense Security Service (DSS) Mission

In this session there will be a detailed overview of:
- The DSS Mission
- Insider Threat Policy Landscape
- Executive Order 13587
- National Insider Threat Policy
- NISPOM Conforming Change #2
- Insider Threat Implementation
- Industry
- Measured Expectations
- DSS CDSE Tools, Training, and Resources
- Defense Insider Threat Management and Analysis Center (DITMAC)
- What it is, and what it isn't
- Relationship with Industry

4:20 PM - 5:20 PM
OPEN-PANEL DISCUSSION and AUDIENCE ENGAGEMENT

Samantha Leach
Senior Change Consultant at Expressworks International

Andrew Smith
Business Requirements Analyst at Advanced Onion

Peter Ateshian
Faculty Associate - Research Department of Electrical and Computer Engineering for the Graduate School of Engineering and Applied Sciences at Naval Postgraduate School (NPS)

Dr. Christopher Williams
Associate Technology Development at Exponent

Human & Technological Patterns of Risk

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, yet deep-rooted backgrounds.

1. Accidental vs. Intentional threats... what are the "tells" in a potentially threatening employee? How can you tell there is an instability?

2. Obviously, there is a lot of training needed to create a more secure cyber / infosec culture? What should some of the key elements be to start this process?

3. These events are pretty rare (though way more frequent than we like), so how can we appropriately apply data science techniques to predict these outcomes; what sort of things do we need to be "measuring?"

4. Should there be a breakdown of the age-group of people that actually click malicious links--is it a generational problem?

5. What sort of information/data do you think can be collected that describes an insider threat (such as Alexis and Hasan types).

5:30 PM - 8:30 PM
NETWORKING RECEPTION

Hewlett Packard Enterprise (HPE) and FireEye will be hosting the 2nd 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 HPE and FireEye!

Hewlett Packard Enterprise

Hewlett Packard Enterprise (HPE) provides world-class IT, technology, products, solutions and services to enterprises and government agencies. HPE helps customers transform to a digital enterprise—integrating cloud applications and mobile workplaces with enhanced security and the ability to gain deeper insights into their enterprise.

FireEye
SECURITY REIMAGINED

FireEye (FEYE) is a leader in cyber security, protecting organizations from advanced malware, zero-day exploits, APTs, and other cyber attacks. FEYE has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks.

8:00 AM - 8:50 AM
Antonio "Tony" Rucci
Owner & Principal,
Insider Threats Consulting

When the Insider Threat Has Authority Over You

More often than not, we focus on the Insider Threat within our organization as an employee, partner or someone we've brought inside our "Circle of Trust." For many of those situations, there is a methodical process for reporting and addressing those potential threats. However, what about those Insiders with authority over us in particular circumstances? What if it's someone in the C-Suite and you're in a small company? What if it's the very person you would elevate a complaint to otherwise? What about unique situations where your hands are tied, or you feel compelled to take matters into your own hands? There are some unique situations out there. I'll address a few cases and illustrate some of the challenges that exist, making it difficult to "solve it with software." Seldom is there an "easy answer."

BIOGRAPHY - Antonio A. Rucci (Tony) is a Fellow with with National Cyber Security Institute, Excelsior in Washington, D.C, sponsored by the National Security Agency. He has more than 32 years of counterintelligence and security experience as a retired Counterintelligence Special Agent and US Army Warrant Officer, of 21 years. Following his dream, Tony started a couple of his own companies, /Root Technology and Insider Threats Consulting. With a core emphasis on secured networking, critical infrastructure protection, data center planning, design and efficiencies, /Root exceeded all expectations and was approached for acquisition in 2014.

During his years as an agent, he is proud to have investigated espionage cases and serve as a Computer Crimes Investigator, protecting our national interests. His final assignment was to serve as the Counterintelligence Operations Officer for the Director of Security at The White House. Tony left The White House upon his retirement in December 2004 but continues to serve the US Intelligence Community and national security efforts in his current capacity in Reno, Nevada. He speaks regularly on topics, such as critical infrastructure protection, spear phishing, social networking and insider threats while serving on multiple Security Advisory Boards. Currently he is an Advisory Board Member for the Nevada Secretary of State, Silver Flume and the University of Nevada. He is on the Advisory Board for the Computer Science and Engineering & Cyber Security Center and is a Fellow at the National Cyber Security Institute, Washington DC, sponsored by the NSA.

Tony and his wife Pam are "proud empty nesters" and reside in sunny Reno, NV. They have one adult son and a beautiful three year old grand baby!

8:55 AM - 9:40 AM
Bryan Ware
President, Analytics and Chief Technology Officer at Haystax

The Whole Person Risk Model for Insider Threat

Many current inside threat tools and capabilities are inherently forensic in nature, detecting a derogatory event after it has occurred. Additionally, many current systems are limited to specific data domains, working either User Activity Monitoring or Personnel Security Data, but not both. This presentation will describe a “whole person” approach to insider threat, blending data from a variety of sources. Additionally, this presentation will describe an approach for identifying high-risk personnel, based on data applied to a quantitative model before derogatory actions take place.

9:50 AM - 10:35 AM
Rick Simmons
Director, Federal Software Sales at Brocade

Man in the Middle Role Based Access for Applications

Software is purpose-built to meet defined functional requirements and put into production with the mindset that other systems will cover all, or nearly all, aspects of security. In the case of software for web applications the traditional security infrastructure of firewall and IPS/IDS is being augmented with next generation firewalls and occasionally web application firewalls with improved results. The...

...continued

approach in this presentation will reveal how to check permissions for every user that requests access to any portion of a web application. This granular approach is proven in the Intel Community to block insider threats that otherwise would have occurred when relying substantially on PKI.

10:35 AM - 11:20 AM
Gaby Friedlander
Co-Founder and CTO of ObserveIT

Building a Practical Insider Threat Program and Making It Work

The use of insider threat management software has grown dramatically over the last two years, but we’ve only started to scratch the surface of innovation. This presentation will not only show you where insider threat technology is today, but also where it’s headed over the next 18 months. You will see what’s capable with leading insider threat software and how it can be applicable for your organization.

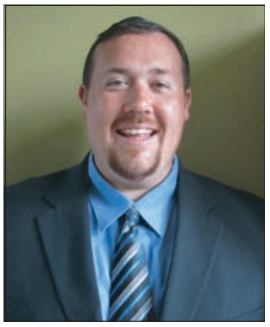
11:20 AM - 12 NOON
Nicole Eagan
Chief Executive Officer of Darktrace

Insiders and Immune Systems – When Rules and Signatures Fall Down

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 750 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 anomalies, 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



1:00 PM - 1:45 PM
Mark Sheppard
Federal CIO at LexisNexis

Yvonne Phillips
Senior Statistical Modeler, Government at LexisNexis

Scoring the Insider / Evaluating the Risk

The number of 5 Million Clearances may go up or down, but truth remains that a platform is needed to evaluate WHICH of the masses deserves an unplanned reinvestigation. The system of choice needs to be based on the Adjudicative Standard 13 rules and consider the FIS Level 5 guidance. The solution must scale, be cost effective and review everyone frequently. LexisNexis has leveraged their decades of expertise in creating industry standard models in government, banking, insurance, and risk screening solutions to create A-TIP. The LexisNexis A-TIP scoring model is in use today with many agencies for their Continuous Evaluation and Insider Threat risk mitigation programs and provides the way forward.

1:45 PM - 2:30 PM
Anshu Gupta
Director of Information Security at HelloSign

Understanding BitCoin - The Fuel Powering the Underground Economy

As new digital crypto currencies like BitCoin have come forth, so have been use cases where they have been used to fund and fuel criminal enterprises. This presentation "Understanding BitCoin - The fuel powering the underground economy" is intended as a technical primer for security and compliance professionals to understand the internals of "BitCoin" and be aware of the security issues in the use of digital currencies. You'll become better prepared to address any security and compliance challenges as businesses adopt the use of the digital currencies as means of payment for goods and services. This presentation will also delve into some of the recent high profile security issues around BitCoin that have been covered in the media including Mt. Gox, Silk Road, CoinCut, BitStamp among others.

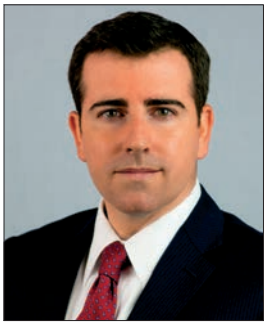
2:40 PM - 3:25 PM
Stephen Marker
Deputy Director of Technology at General Dynamics Mission Systems

Insider Threat Detection: Defending from Actors within the Network

Establishing an effective defense to insider threats requires proactive identification of adverse behaviors within the enterprise. However, the operation of this capability must...

... continued

be based upon legal authorities, governance and policy. General Dynamics presents our successful 7-step process to establishing a robust insider threat detection capability, along with a five-tiered architecture and emerging technologies to detect, deter and mitigate potential threats.



3:25 PM - 4:10 PM
Patrick Clancey
Director of Federal Programs at MorphoTrust

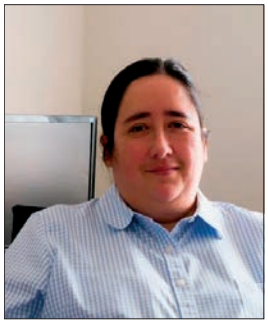
Today's "Identity Crisis" and National Security: Pinpointing Threats using Multiple Characteristics of Identity

When it comes to securing our nation, the ability to quickly identify individuals who may pose a threat, and verify with confidence that individuals are who they claim to be, is of paramount importance. There are three primary characteristics that comprise our identity: something we have (i.e., our driver license or passport), something we know (i.e., our mother's maiden name) and something we are (i.e., our face, fingerprints, DNA, etc.). The more characteristics captured and verified, the lower the risk and higher the degree of confidence we can have in an individual's identity. How does this work? Today's cloud-based identification and authentication solutions enable fast, accurate verification through multi-modal biometrics and authenticating our most trusted proof-of-identity documents – driver licenses and passports. These systems offer the benefits of a hosted environment, are quick to deploy and offer the flexibility to add more modes and capabilities as needs change and new advancements are available. Learn how these technologies work and how the combination of multiple characteristics reduces risk and threats to our country in many situations.

4:20 PM - 5:20 PM
OPEN-PANEL DISCUSSION andAUDIENCE ENGAGEMENT

Earl Matthews
Vice President, Enterprise Security Solutions, U.S. Public Sector, Hewlett Packard Enterprise

Karthik Krishnan
Vice President of Product Management at Niara



Tammy Torbert
Worldwide Solutions Architect, US Public Sector for HPE Security

Bryan Lee
Unit 42 – Threat Intelligence Analyst at Palo Alto Networks

Securing Business Outcomes with Cybersecurity

In the course of our engagements with customers across the globe, we find organizations can fit in three broad categories:

- Those who have a long-term strategic cyber plan based on delivering business outcomes
- Those who confuse tactical “activity” with outcomes
- Those who have their heads in the sand

This session will help both executives and technical leadership connect and integrate cyber security with proper business outcomes. Once defined, the adoption of cyber infrastructure choices, people and processes become clearer and more achievable.

Thank you sponsors for your expertise and support! You have succeeded in making the 2nd annual Insider Threat Summit an outstanding event for all participating parties. We are excited at the level of support and dedication to highly relevant insider threat topics and we are privileged to be able to bring you all together to meet these security challenges head on!

Hewlett Packard Enterprise

FireEye
SECURITY REIMAGINED

observe it

LexisNexis

Haystax Technology

VECTRA
Security that thinks

niara

DARKTRACE

SECURONIX

ADVANCED ONION
LAYERS OF TECHNOLOGY

GENERAL DYNAMICS
Mission Systems

BROCADE

paloalto networks

sas

Exponent

expressworks

exabeam

LogRhythm

VARONIS

BOEING

MorphoTrust USA

splunk>

GCE
Global Connections to Employment, Inc.
An Affiliate of Lakeview Center, Inc.

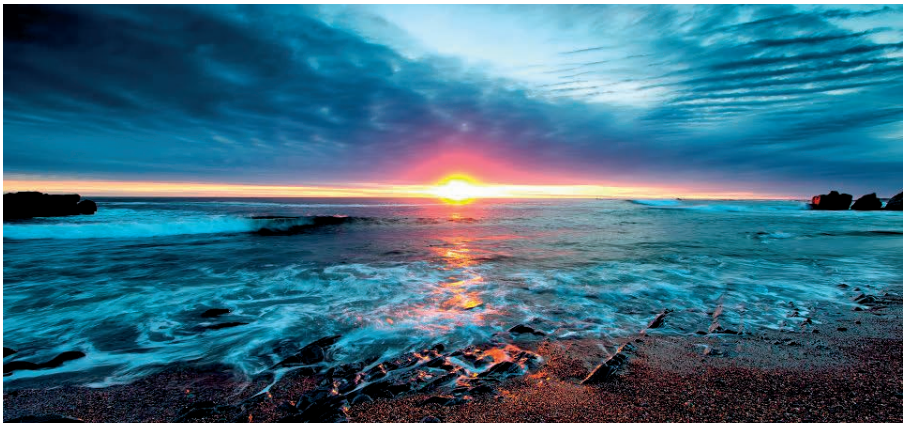
ClearShark
fierce technology solutions

Reservoir Labs

insiderthreatevents.com

#insiderthreatsummit

@threatevents



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.

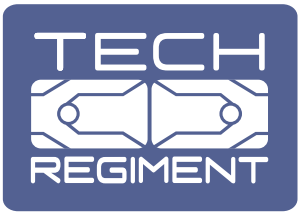
California, like most areas, needs security solutions and experts to directly respond to issues such as those brought up in recent hearings by the Members of the Assembly Committee on Privacy and Consumer Protection and Select Committee on Cybersecurity. There's been a chain of critical reactions put in place by the CA Governor's office 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. The result was the near immediate resignation of the CA CISO and CIO. California is not the only location in the "hot seat," **this is a world-wide issue 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 **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.

NOTES

Hosted by



For more information on upcoming events please contact us:

@techregiment events@techregiment.com techregiment.com