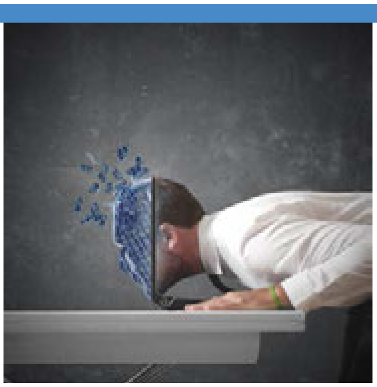
insider threat

2015 SUMMIT

PROGRAM

Information Security



Cyber Security

Operations Security

March 16 - 17
Hyatt Regency Hotel & Spa
Monterey, California

Hosted by Advanced Onion and Tech Regiment

insider threat

2015 SUMMIT

AGENDA - DAY 1
Monday, March 16

7:30 AM - 8:30 AM	**REGISTRATION**
8:30 AM - 8:50 AM	**WELCOMING REMARKS** Paul Temple, CEO of Advanced Onion and Tech Regiment
9:00 AM - 9:50 AM	**KEYNOTE PRESENTATION - AT THE CORE OF INSIDER THREAT** Michele Robinson, CA State Chief Information Security Officer (CISO), California Information Security Office
10:00 AM - 10:50 AM	**WHO DO YOU TRUST?** Chris Grijalva, Director for Physical Security and Law Enforcement at Defense Manpower Data Center (DMDC)
11:00 AM - 11:50 AM	**PRACTICAL COMPUTER NETWORK ANALYSIS AND DISCOVERY: STORIES FROM SCINET and SC'14** Eric Dull, Technical Director at Cray, Inc.
11:50 AM - 12:50 PM	**LUNCH BREAK -** Sponsored by Norse Corp.
1:00 PM - 1:50 PM	**DISRUPTING THE ATTACK CHAIN AND PREVENTING INSIDER THREATS** Tim Treat, Blogger, IT Operations and Cyber Security Professional at Palo Alto Networks
2:00 PM - 2:50 PM	**SAFEGUARDING, FROM THE ENEMIES PERSPECTIVE** Maj. General (Ret) Earl D. Matthews, Vice President, Enterprise Security Solutions HP Enterprise Services, U.S. Public Sector for HP-ES
3:00 PM - 3:50 PM	**OPEN-PANEL DISCUSSION - VIRTUALIZATION AND BRING YOUR OWN DEVICE (BYOD) CYBER PLANNING** Bob Goodwin, Cybersecurity Analyst and Chris Gaucher, Director of Cybersecurity and Privacy, Deputy CIO for Operations from Naval Postgraduate School (NPS), Scott Clark, Software Chief Technology Officer, Federal at Brocade, Oliver Tavakoli, Chief Technical Officer of Vectra Networks and Mohan Koo, CEO and Founder of DTEX Systems
4:00 PM - 4:25 PM	**CHANGING THE CYBER PARADIGM** Rich Heimann, Chief Data Scientist at L-3 Data Tactics
4:30 PM - 5:00 PM	**Q&A - AUDIENCE ENGAGMENT / CLOSING COMMENTS** Paul Temple, CEO of Advanced Onion and Tech Regiment
5:00 PM - 8:00 PM	**NETWORKING RECEPTION -** Sponsored by HP Enterprise Services

insider threat

2015 SUMMIT

AGENDA - DAY 2
Tuesday, March 17

8:15 AM - 8:25 AM	**OPENING STATEMENTS** Paul Temple, CEO of Advanced Onion and Tech Regiment
8:30 AM - 9:20 AM	**KEYNOTE PRESENTATION - MIND THE GAP – SECURING THE PRIVATE CLOUD** Chris Kemp, Founder of Nebula and OpenStack, former CTO at NASA
9:30 AM - 10:00 AM	**ANOMALY DETECTION ALGORITHMS FOR DETECTING INSIDER THREAT** Ellick Chan, Ph.D., Senior Associate, Technology Development and Dr. Adam Rowell, Senior Engineer, Technology Development both from Exponent
10:10 AM - 10:50 AM	**UTILIZING NEXT GENERATION INFORMATION FUSION FOR INSIDER THREAT ANALYSIS** Brian Clark, VP Product Development at Objectivity
11:00 AM - 11:50 AM	**A MODERN METHODOLOGY FOR DETECTING CYBER ATTACKS** Oliver Tavakoli, Chief Technical Officer of Vectra Networks
11:50 AM - 12:50 PM	**LUNCH BREAK -** Sponsored by LexisNexis
1:00 PM - 1:50 PM	**ENSURING SECURITY IN A DATA DRIVE ENTERPRISE** A.J. Shipley, Senior Director, Product Security at NetApp
2:00 PM - 2:50 PM	**PROTECTING YOUR INFORMATION AND YOUR ENTERPRISE** Matthew Toth, Principal Security Engineer at Symantec
3:00 PM - 3:50 PM	**OPEN-PANEL DISCUSSION - COUNTERING INSIDER THREAT** David Schwab, Program Manager for Physical Access and Law Enforcement and Chris Grijalva, Director for Physical Security and Law Enforcement both from Defense Manpower Data Center (DMDC), Benji Hutchinson, Senior Director at MorphoTrust, David Yachnin, Security Analytics, USPS Hewlett-Packard Company and Rob Buzby, Business Development Director and DOD Cyber Lead at SAPNS2
4:00 PM - 4:50 PM	**PRACTICAL INSIDER RISKS FROM THE CORPORATE SECTOR** Josh Ablett, CISO & SVP of Product Management at Dtex Systems
4:50 PM - 5:00 PM	**CLOSING COMMENTS** Paul Temple, CEO of Advanced Onion and Tech Regiment

The Insider Threat 2015 Summit 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, 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.

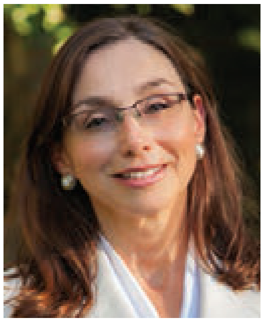
The event is hosted by Advanced Onion and Tech Regiment who have been on the forefront of some of the most innovative threat mitigation projects in support of government and private industry leaders. By coming together, our solution-based discussions and exchanges of ideas will aid in our overall understanding in countering this costly problem from various forms of insider threats. Ultimately, our goal is to provide a forum of key security-focused leaders who can share, enlighten and stimulate your security know how, so you can meet your challenges head on.

The summit presentation and open panel discussions will be on the following topics of interest:

Cyber threat, detection, security and mitigation

Personnel security threat mitigation, including continuous evaluation (CE) of privileged identities

Technical physical security threat measures and advancements including unique supportive data models



DAY 1 - KEYNOTE SPEAKER
9:00 AM - 9:50 AM
Michele Robinson
CA State Chief Information Security Officer (CISO) at the California Information Security Office

At the Core of the Insider Threat

Technology and the Internet have changed the World ecosphere. It has also changed what you need to know about insider threats. Michele will walk through an examination of insider threat occurrences, their root causes and consequences. The examples and lessons may surprise audiences, as they transcend what is traditionally known about behavioral theory and characteristics of insiders at risk.

BIOGRAPHY

Michele Robinson was appointed Director of the California Office of Information Security (OIS) and State Chief Information Security Officer (CISO) by Gov. Jerry Brown in May 2013. Robinson joined OIS in 2007 and assumed the position of Acting Director in February 2013, where she served as the liaison to federal, State and local government on cyber security policies and issues. From 2010 to 2013, she served as Deputy CISO and was responsible for managing the day-to-day operations of OIS and the statewide information security program, including enterprise policy development, disaster recovery planning, incident management, and compliance. From 2007 to 2010, Robinson served as Assistant CISO managing the statewide enterprise incident management program and effecting several significant policies. Prior to joining OIS, Robinson served as the CISO and Privacy Officer for the California Unemployment Insurance Appeals Board (CUIAB) for nearly 5 years.

Prior to her appointment with CUIAB she worked for the Department of Consumer Affairs (DCA) for 8 years, serving on policy development, new program implementation, business process reengineering and system design and integration committees, and representing DCA and its constituent board and bureau programs at task force meetings, board meetings and special meetings with control agencies and members of the Legislature. Robinson has 10 years of experience in the finance and credit industry where she has held manager, supervisor, and fraud investigator positions. She holds a Bachelor of Science in information systems from the University of San Francisco, and CISSP, CISM, CIPP/US, and CIPP/IT certifications.

10:00 AM - 10:50 AM
Chris Grijalva
Director for Physical Security and Law Enforcement at Defense Manpower Data Center (DMDC)

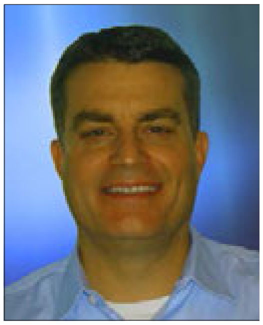
Who Do You Trust?

This presentation will discuss the human and sociological factors around insider threat and how those factors might be able to be detected and mitigated. A brief description of the recent shifts in ideology and how that can and may affect your business and operation. Lastly, a high level look at what the Department of Defense is doing in the area of insider threat.

11:00 AM - 11:50 AM
Eric Dull
Technical Director at Cray, Inc.

Practical Computer Network Analysis and Discovery: stories from Scinet and SC'14

SCinet is the high-bandwidth network that supports the SC technical conference and exhibit hall. SC'14 had the largest network to date, with 1.2 terabits per second reaching the show floor and 11,000 devices using SCinet's 32,000 publicly-routable IP addresses. Securing this network posed a number of challenges.... This talk will discuss these challenges, how the network security team overcame these obstacles, Cray's role in the network security team and share interesting analytic results from the conference.



1:00 PM - 1:50 PM
Tim Treat
Blogger, IT Operations and Cyber Security Professional at Palo Alto Networks

Disrupting the Attack Chain and Preventing Insider Threats

This presentation discusses the Insider Threat problems that plague legacy cyber security technologies as well as new approaches available to counter Insider Threats. The innovations and approaches discussed include practical application and user enablement techniques that are ready for implementation to protect organizations at every stage of the Cyber Attack Chain, including Insider Threat.

2:00 PM - 2:50 PM
Maj. General (Ret) Earl Matthews
Vice President, Enterprise Security Solutions HP Enterprise Services, U.S. Public Sector for HP Company

Safeguarding, From the Enemy's Perspective

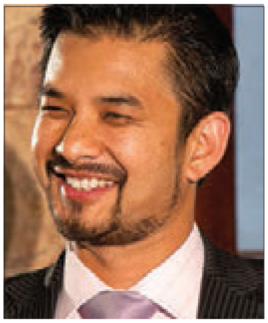
The cost of cybercrime for an organization has escalated to $12.7 million a year compared to $3.8 million in 2010. And recovering from a data breach has increased from 14 days (2010) to 48 days (2014). Hackers are becoming more sophisticated and specialized, spending more money on building up their arsenals and coalitions that span criminal, activist, and nation-state players. Find out how to safeguard your government organization by changing the way you invest in and think about security: from the perspective of the enemies targeting you.

3:00 PM - 3:50 PM
OPEN-PANEL DISCUSSION

Robert Goodwin
Cybersecurity Analyst at Naval Postgraduate School (NPS)

Scott Clark
Software Chief Technology Officer - Federal at Brocade

Chris Gaucher
Director of Cybersecurity and Privacy at Naval Postgraduate School (NPS)



Mohan Koo
CEO and Founder of DTEX Systems

Oliver Tavakoli
Chief Technical Officer of Vectra Networks

Virtualization and Bring Your Own Device (BYOD) Cyber Planning

In the near future the number of mobile devices will be approximately 10 billion, that is 1.5 devices per person in the world! That fact is no different for enterprise environments, like those represented here today, in how they secure their hosted organizations. Having a substantial mobile program, allowing for BYOD, presents significant security concerns to all organizations.

BYOD challenges most traditional security models that protect the perimeter of an organization by muddying what we currently define as the perimeter and by limiting an organization's ability to control the software image of such devices. The overall intent of this panel is to discuss the risks of BYOD and Virtualization, and talk about the potential methods to address the risks and security challenges.

DAY 1 SPEAKERS AND NETWORKING RECEPTION

4:00 PM - 4:25 PM
Rich Heimann
Chief Data Scientist at
L-3 Data Tactics

Changing the Cyber Paradigm
Forget the Needle in the Haystack...
Focus on the Hay!

The new paradigm is not looking for the needle, but is finding the difficult-to-find patterns in the hay. Rule based cyber analytics is the starting line NOT the finish line.

4:30 PM - 5:00 PM
Paul Temple
CEO of Advanced Onion
and Tech Regiment

AUDIENCE ENGAGEMENT / Q & A
CLOSING COMMENTS

Paul Temple, will be closing the first day and welcoming all attendees to the networking reception. This would be a great time to address any questions or concerns you would like to share.

5:00 PM - 8:00 PM
NETWORKING RECEPTION

HP Enterprise Services (HP-ES) will be hosting the Insider Threat Summit's networking reception. The reception is open to all registered attendees and is located in the Conference Center Foyer, Terrace and Courtyard. There will be excellent food, tasty beverages and plenty of good company.

We welcome you to enjoy this unique opportunity to meet the presenters and fellow attendees in an optimal setting for sharing similar interests.

Thank you HP-ES!

It's what we do. HP creates new possibilities for technology to have a meaningful impact on people, governments and society. With the broadest technology portfolio, HP delivers solutions to customers' most complex challenges, including managing insider threats. HP's flexible and scalable solutions will help you address ever changing landscapes.

DAY 2 - KEYNOTE SPEAKER
8:30 AM - 9:20 AM
Chris Kemp
Founder and Chief Strategy Officer at Nebula, and former CTO of NASA

Mind the Gap – Securing the Private Cloud

In today's computing environment, two IT security domains exist—"pre-cloud" and "public cloud"—each providing application owners with different set of security challenges. In the gap between these two domains lie the new security challenges of setting up a "private cloud."

In the "pre-cloud" domain of IT infrastructure, virtualization and enterprise data centers, IT has established processes, accreditations, certifications, governance and compliance rules named all kinds of acronyms including FISMA, NERC CIP, NIST 800-53, HIPAA, PCI-DSS, IRS 1075, MAS TRM and SOX, and even professional ones such as CISSP and CASP.

In the "public cloud" domain, organizations that operate software in the cloud have a completely different "attack surface" with a completely different set of security considerations. Efforts such as FedRAMP have attempted to tackle this domain. They have had to build very different processes to operate software securely in this domain.

In the intersection of the "pre-cloud" and "public cloud" security practices and expertise lays an area where "private clouds" exist. In this gap are new security challenges that aren't exclusively found in either "pre" or "public" cloud domains.

During his talk Chris will reflect on "pre-cloud" security and compare that to security requirements in the "public cloud." He will discuss the challenge that today's organizations have when building a secure private cloud where they cannot solely rely on established "pre-cloud" security processes and controls nor can they count on integrating only those processes and controls that exists for the "public cloud" today.

BIOGRAPHY

Chris C. Kemp is an entrepreneurial executive with a passion for igniting innovation in high-tech organizations. He is the Chief Strategy Officer of Nebula, Inc., a company Chris founded after serving for five years in various roles at NASA. Chris also co-founded the OpenStack project.

As the Chief Technology Officer for IT at NASA, Chris was responsible for pioneering work in cloud computing, open source, and open government. Chris served on the Cloud Computing Executive Steering Committee, and chaired the Cloud Standards Working Group. Previously, he served as the CIO of NASA Ames Research Center in Silicon Valley where he forged partnerships with Google and Microsoft and helped create Google Moon, Google Mars, and Microsoft World Wide Telescope. He was responsible for NASA's Nebula Cloud Computing Project and co-founded the OpenStack project. Prior to joining NASA, Chris helped create the third largest online community Classmates.com, was the founding CEO of the leading webbased vacation rental platform Escapia (AWAY), and, as the founding CEO of Netran, developed the first online grocery shopping platform for Kroger, the world's largest grocery store chain.

DAY 2 SPEAKERS

9:30 AM - 10:00 AM
Dr. Adam Rowell
Senior Engineer Technology Development of Exponent

Ellick Chan, Ph.D.
Senior Associate, Technology Development of Exponent

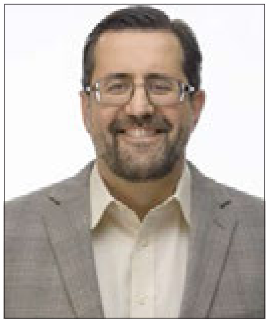
Anomaly Detection Algorithms for Detecting Insider Threat

Anomaly detection is a technique to identify behavior that deviates from the norm. In the case of insider threat or system breaches, the behavior of a user can deviate dramatically from normal usage. In this talk, we discuss several technical machine learning-based approaches to analyze data for anomalies. We briefly discuss the theoretical foundations of the techniques and compare their efficacy in several real-world use cases in detecting buried explosives and mining medical datasets. We also highlight several difficulties in working with high dimensional data and the challenges involved in processing and mining the data.

10:10 AM - 10:50 AM
Brian Clark
VP Product Development at Objectivity

Utilizing Next Generation Information Fusion for Insider Threat Analysis

With the increase in security threats globally (cyber and physical including terrorism, financial fraud, intellectual property and insider threats such as Snowden) that compromise security, it is crucial to be able to understand and discover potentially dangerous behavior and communications in real-time. Utilizing next generation information fusion, which focuses on finding and creating key associations between data, organizations can be used to develop better and more accurate or timely insight through enriched information.



11:00 AM - 11:50 AM
Oliver Tavakoli
Chief Technical Officer
of Vectra Networks

A Modern Methodology for Detecting Cyber Attacks

Fundamental shifts in the nature of computing are forcing IT and Security teams to evolve their approach to protecting their key assets. IT must support and secure an increasingly powerful and diverse set of end-user devices, operating systems, and applications. At the same time, traditional security solutions have become increasingly out of touch in virtualized data centers where east-west endpoint-to-endpoint communications account for more than 80% of traffic. These fundamental shifts in the attach surface of the modern network have created the ideal environment for cyber attackers, who have perfected the art of low-and-slow attacks that quietly spy, spread, and steal within a victim network.

In this session we will investigate how these changes impact the security of the enterprise network, and will introduce a modern methodology for protecting your critical assets and thwarting sophisticated cyber attacks. The talk will include:

- An analysis of how the enterprise attack surface has changed in the past 3 years
- An analysis of recent breaches, and what they have in common
- Requirements for securing mobile and virtualized devices
- Proposing a generic methodology for automating the detection of persistent attacks in any network

1:00 PM - 1:50 PM
A.J. Shipley
Senior Director, Product
Security at NetApp

Ensuring Security in a Data Drive Enterprise

As organizations become data-drive entities, many are rapidly moving to a much more dynamic, services based model in response to growing demands for faster creation and delivery of services to end customers. This approach requires stringent Data Control that addresses business needs, meets information technology requirements, and, above all, protects data from unauthorized access or manipulation from inside or outside the organization. That last – and most important – requirement means keeping regulated data safe by ensuring it is encrypted and unreadable by unauthorized users while simultaneously securely storing the information without impacting ongoing operations or reducing availability.

2:00 PM - 2:50 PM
Matthew Toth
Principal Security Engineer
at Symantec

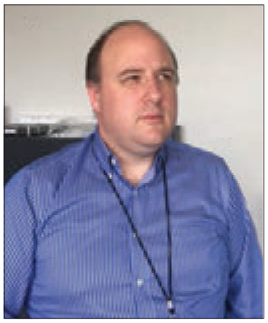
Protecting Your Information and Your Enterprise

Here we take a look into what makes up an Insider and how to better detect them and help protect your information. Presentation highlights: What makes up an insider? Where is your data and who is using it? What we have learned from insider breaches.

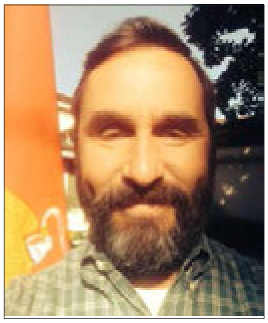
3:00 PM - 3:50 PM
OPEN-PANEL DISCUSSION

Chris Grijalva
Director for Physical Security and Law Enforcement at Defense Manpower Data Center (DMDC)

Benji Hutchinson
Senior Director at MorphoTrust



David Schwab
Program Manager for Physical Access and Law Enforcement at U.S. Department of Defense (DoD)



Rob Buzby
Business Development Director and DOD Cyber Lead at SAP NS2

David Yachnin
Security Analytics, USPS
Hewlett-Packard Company

Counter Insider Threat

In today's climate, a significant amount of cyber security concerns have shifted from outside bad actors to inside bad actors. There are many concerns about how policy and technology will answer the needs for security executives and IT Managers to counter the insider threat problem.

4:00 PM - 4:50 PM
Josh Ablett
CISO & SVP of Product Management at Dtex Systems

Practical Insider Risks From the Corporate Sector

Based on recent risk assessments, Dtex has identified a number of alarming data points in how insiders utilize technology resources important to the public and private sectors.

This ranges from utilizing hacking tools and pirated software to bypassing security controls and violating policies. Whether intentional or accidental, the failure of existing controls and technologies can leave any type of organization exposed.

4:50 PM - 5:00 PM
Paul Temple
CEO of Advanced Onion and Tech Regiment

CLOSING COMMENTS

Paul Temple will be closing the event with some choice words. If you missed any part of our event, have any questions you would like addressed or concerns you would like to share, please be sure to stay for this brief and informative recap.

> No one is ever completely secure and everyone has one thing in common, vulnerability.

SPONSORS

Thank you sponsors for your exp ertise and support! You have helped make the first annual Insider Threat Summit an outstanding event for all participating parties.

PLATINUM SPONSORS

hp

Dtex systems

VECTRA™
Security that thinks.™

GOLD SPONSORS

paloalto networks.

BROCADE

Objectivity

NORSE

L3

Symantec.

MorphoTrust USA

nebula.

Exponent

LexisNexis

VARONIS

NS2 NATIONAL SECURITY SERVICES. | SAP

MarkLogic

NetApp

OWASP
Open Web Application Security Project

HOSTS

ADVANCED ONION
LAYERS OF TECHNOLOGY

TECH REGIMENT

Insider Threat Summit's hosts Advanced Onion and Tech Regiment are both headquartered on the Monterey Peninsula. By holding the Insider Threat Summit on the Monterey Peninsula, 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.

Significant progress is being made to enhance the technology industry on the Monterey Peninsula, which is quickly becoming the **information security (InfoSec) hub** of the nation. The Insider Threat Summit creates an optimal setting for networking and provides a unique platform to build your presence on the Monterey Peninsula and beyond. In addition, 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 excellent community and hope you find your stay to be rewarding, and you leave stimulated by new information and prospects.