MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2017

APRIL 3-5, 2017 | OMNI ORLANDO RESORT AT CHAMPIONSGATE | CHAMPIONSGATE, FL

70+ SESSIONS | 10 WORKSHOPS | 7 DYNAMIC TRACKS | 3 CO-LOCATED SUMMITS

CISO LEADERSHIP SUMMIT
April 2, 2017

CLOUD SECURITY SUMMIT
April 6, 2017

RISK MANAGEMENT SUMMIT
April 6, 2017

EARN UP TO
47 CPEs
WITH OUR WORLD PASS

FEATURED KEYNOTES

CORY DOCTOROW
Author, Blogger
Electronic Frontier Foundation & Boing Boing

RICH MOGULL
Chief Executive Officer
Securosis

JIM ROUTH
Chief Security Officer
Aetna

CRAIG SMITH
Founder
Open Garages;
Research Director
Rapid7

#INFOSECWORLD

FOR AGENDA UPDATES VISIT: INFOSECWORLD.MISTI.COM

BROUGHT TO YOU BY

MIS|TI™
TRAINING INSTITUTE

EVENT SPONSOR

Hewlett Packard Enterprise

PLATINUM SPONSORS

LIEBERMANSOFTWARE

Malwarebytes

GOLD SPONSORS

Check Point
SOFTWARE TECHNOLOGIES LTD

CYLANCE

MIS|TI™ PRESENTS

InfoSecWorld
Conference & Expo 2017

en-tre-pre-neur-ship

noun

1. The willingness to take risks and develop, organize and manage a business venture in a competitive global marketplace that is constantly evolving.

The infosec space is constantly changing, and today's security practitioners have no choice but to become more entrepreneurial about finding solutions to problems, not just at a technical level, but at a management and leadership level. InfoSec World 2017 Conference & Expo provides practitioners with the ideal forum for learning about the latest advances and most cutting-edge strategies for ensuring optimal security within their organizations, despite the progressive threat landscape. Join your peers from around the globe for two and a half days of learning, peer sharing, networking and hands-on education.

CONFERENCE HIGHLIGHTS

EXPO HOURS: MONDAY, APRIL 3 5:00 PM - 6:30 PM | TUESDAY, APRIL 4 11:30 AM - 6:15 PM | WEDNESDAY, APRIL 5 8:00 AM - 11:00 AM

NETWORKING EVENTS: MONDAY, APRIL 3 5:00 PM - 6:30 PM | TUESDAY, APRIL 4 4:45 PM - 6:15 PM | WEDNESDAY, APRIL 5 9:30 AM - 11:00 AM

NETWORKING

InfoSec World isn't JUST about the in-depth breakout sessions. We know networking is just as important, which is why this year we are holding THREE networking receptions. Plus, we've added huddle spaces around the Expo floor to help facilitate even more informal brainstorming with your peers.

ONE-ON-ONE LEADERSHIP STRATEGY SESSIONS

Are you valued for your leadership as much as your security skills? Explore how to recognize your leadership value in a private, one-on-one coaching session customized for you. Spend twenty minutes with Michael Santarcangelo, Founder of Security Catalyst, to assess your situation and determine your best next step as a security leader. Known for his leadership and communication development, Michael elevates leaders and accelerates their journeys, infused with the mindset of success. And he's offering his services to you – complimentary for conference attendees.

BOOK SIGNINGS

Each year a new break-through book is released in the infosec industry, and we have the authors of the latest titles! Meet and greet with these authors and bring home a signed copy of their books. This year's book signings include titles from keynote speakers Craig Smith and Cory Doctorow, as well as Raef Meeuwisse, Director of Cybersecurity and Data Privacy Governance at Cyber Simplicity Ltd.

HANDS-ON

Want to get down into the nitty gritty of mainframes, threat hunting or malware analysis? This year we have more hands-on sessions and workshops than ever before. Join us for an extra day or two to get full access to our experts in our pre- and post- conference workshops and get all of your toughest questions answered. Plus earn extra CPEs while you're at it!

KEYNOTE SPEAKERS

MONDAY, APRIL 3, 8:30 AM - 9:30 AM

RADICAL REMODELING: RENOVATING SECURITY FOR TODAY'S PROBLEMS AND TOMORROW'S OPPORTUNITIES

Rich Mogull, Chief Executive Officer, Securosis

The practice of information security is in the midst of the most tumultuous changes in our history. As threats become global socioeconomic challenges, we are adopting new technologies at a pace never before seen. Security professionals face the unenviable challenge of protecting decades' worth of decisions while building a safe foundation as we transition into a world dominated by cloud and mobile technologies. This keynote will lay out a roadmap for adapting your security for current requirements while still preparing yourself for the future.

TUESDAY, APRIL 4, 8:30 AM - 9:30 AM

REBOOTING THE AUTO INDUSTRY: WHEN SECURITY AFFECTS SAFETY

Craig Smith, Founder, Open Garages; Research Director, Rapid7

We are surrounded by 2-ton IoT devices on wheels. The auto industry has rapidly evolved in the last five years; vehicles now have phone apps for remote control, built-in Wi-Fi hot spots, heads-up displays, lane correction systems and other Advanced Driver Assistance Systems. These convenience and road safety features are in high demand, but they also introduce cybersecurity concerns.

Automakers are now software companies, and this talk will address some of the cybersecurity-related issues faced by the transportation industry. Mr. Smith will share techniques currently used by hackers and show some of the security defenses being put into place. You will see the vulnerabilities of vehicles on the road today, as well as take a peek into the future of fully autonomous cars.

TUESDAY, APRIL 4, 1:30 PM - 2:30 PM

1998 CALLED AND IT WANTS ITS STUPID INTERNET LAW BACK…BEFORE IT DESTROYS THE WORLD

Cory Doctorow; Science fiction author, activist, journalist and blogger; Electronic Frontier Foundation & Boing Boing

In 1998, Congress passed the Digital Millennium Copyright

CO-LOCATED SUMMITS 8 CPEs

CISO LEADERSHIP SUMMIT

SUNDAY, APRIL 2

SPONSORED BY

Hewlett Packard Enterprise

Presenters: **Michael Santarcangelo,** Founder, Security Catalyst; **Bhavesh Bhagat,** Co-Founder, Confident Governance

Are you valued as much for your leadership as you are for your technical skills? Most security leaders (reluctantly) say "no." In this interactive summit you will gain access to universal insights and frameworks that you can use to accelerate your journey.

No decoder ring required. It's not designed only for security—which is why it is the right, powerful approach to address and advance security leaders. The key of this effort is to connect leadership, communication, and the security mindset for success. Attend this summit to learn and practice how to advance your leadership journey.

- Debunking leadership misconceptions
- Five essential elements for exceptional leadership and communication
- Mastering the rapid velocity of change in the CISO world by leveraging core principles
- Finding your unique leadership path

CLOUD SECURITY SUMMIT

THURSDAY, APRIL 6

Presenters: **Andrew Hay,** CISO, Data Gravity; **Jason Wood,** Hunt Team Operations; **John Menerick,** Gap, Inc.

Cloud computing has had a huge impact on IT, but in many ways security has fallen behind IT. While we were busy watching our network IDS, technology moved out of the datacenter and to cloud providers. Companies have hundreds—if not thousands—of connected cloud services where organizational data resides. Just because the data isn't hosted internally, security can't shirk responsibility for its protection.

This interactive summit will help attendees work through common cloud-based challenges and offer expert insights for managing operations, provider relationships, testing the security of your data in the cloud and more.

- Adapting your operations for the cloud
- Migrating business data into the cloud
- Incident response in the cloud
- Generating your own file-based cyber threat intelligence (CTI)

RISK MANAGEMENT SUMMIT

THURSDAY, APRIL 6

Presenters: **Jack Jones,** Co-Founder and EVP, R&D, RiskLens; **Ron Wormer,** Director of CyberSecurity Studies, Bellevue University; **Evan Wheeler,** Vice President, Operational Risk, Depository Trust & Clearing Corp. (DTCC)

As with any other aspect of operating a business, managing cyber risk well is predicated on making informed decisions, and then executing reliably within the context of those decisions. Unfortunately today, too many security teams still don't understand how to effectively translate technical security issues into risk language the business can use.

During this summit we'll disprove some of the myths about what risk is and what it isn't. Attendees will walk away with new tools and methodologies that will help them align security and risk with business goals, and help elevate security as a strategic and trusted partner.

- Fundamentals of risk management
- Recognizing, avoiding and correcting analytical mistakes
- Improving the quality of risk measurement
- Communicating risk analysis results to management

Act, which made it a felony to reconfigure any system that has digital rights management (DRM) in it. While this began as a way to keep people from changing their DVD players to be region-free, now it's an all-purpose tool for maximizing profits for any software enabled gadgets and systems: just insert the minimum viable DRM between the customer and your business model, and anything that disrupts the model is a felony.

Worse: any security vulnerability in a DRM-encumbered system is potentially helpful to people who want to bypass the DRM, so courts (and legal advisors) treat vulnerability disclosure as a potential felony.

So DRM has metastasized: it's in everything from voting machines, to phones, tablets, and computers.

Combine the new reach of computerized devices with the legal jeopardy for security researchers who audit them and we're hurtling towards The Internet of Things on Fire That Spy on You and Destroy Your Life.

The Electronic Frontier Foundation is working on the Apollo 1201 project, whose objective is to kill all the DRM in the world, forever, within a decade. Attend this talk to hear about the project and how it will affect the security industry.

WEDNESDAY, APRIL 5, 8:30 AM - 9:30 AM

THE THREE "Ts" OF SECURITY: TALENT, TOOLS & TECHNIQUES: WHICH IS MOST IMPORTANT FOR CISOs?

Jim Routh, Chief Security Officer, Aetna

The diversity of threats facing the healthcare industry are now similar to what the banking industry has dealt with for decades: skilled nation state threat actors and criminal fraud syndicates. Mr. Routh will share examples of specific controls implanted in innovative ways that add trust to email, allow teams to monitor privileged users and help operations and security teams migrate from binary authentication to behavioral-based authentication.

This keynote will explore the relationship between cybersecurity and privacy, identifying the most effective principles and techniques for leading a risk-driven cybersecurity program.

PRE- AND POST-CONFERENCE WORKSHOPS

PRE-CONFERENCE WORKSHOPS

ONE DAY **8 CPEs**

SATURDAY, APRIL 1

W1 DEVSECOPS SYMPOSIUM

Bill Burns, Chief Trust Officer and VP, Cloud Business Transformation, Informatica; **Mahesh Kandru,** Application Security Architect, Informatica; **Shannon Lietz,** Director of DevSecOps and Chief Security Architect, Intuit; **Jayne Groll,** COO, DevOps Institute; **Alan Shimel,** Founder and Editor-in-Chief, DevOps.com; **Chris Hawley,** Founding Partner, Blackrock 3 Partners; **Ron Vidal,** Partner, Blackrock 3 Partners; **Lawrence Embil,** Miami-Dade County; **Rob Schnepp,** Partner, Blackrock 3 Partners; **Ben Tomhave,** Security Architect, New Context

1. Lessons learned forming a DevSecOps program
2. Culture hacking lessons needed to succeed in building safer software
3. Building a SecDevOps program to help with cybersecurity resources shortage
4. Improving security operations by leveraging orchestration, automation and DevOps practices
5. Incident Management System as a framework for solving high-severity problems
6. Tools and processes that enable the further blending of development, operations and security roles
7. Building a roadmap for integrating security into DevOps
8. Measuring the transition of an application behavior from normal to malicious while lowering false positives
9. Implementing an end-to-end security lifecycle from visibility and detection to responses and remediation in an immutable infrastructure
10. Changing human behavior and organizational culture to better account for security

TWO DAYS **16 CPEs**

SATURDAY, APRIL 1 - SUNDAY, APRIL 2

W2 MAINFRAME SECURITY: HANDS-ON AUDIT AND COMPLIANCE HANDS-ON

Philip Young, Founder, Level 6 Security

- z/OS operating system basics
- Understanding z/OS operating system paradigms
- Mainframe security auditing
- RACF/Top Secret/ACF2 security review
- TSO and UNIX security
- VTAM hardening
- CICS security and exploitation
- System enumeration

Day 1 - Mainframe Basics

- Mainframe history
- Operating system introduction
- z/OS basics
- System startup
- Security

Day 2 - Networking/Patch Management

- Networking
- Patching/patch management
- CICS
- Auditing

Requirements:

Participants must bring a laptop capable of running a virtual machine. See website for technical details and requirements.

W3 RED VS. BLUE TEAM TECHNIQUES WITH HUNT TEAMING HANDS-ON

Larry Spohn, Senior Principal Security Consultant, TrustedSec
Paul Koblitz, Senior Principal Security Consultant, TrustedSec

Day 1

- Introduction to attacker techniques
- Common methods for exploitation
- Methods for persistence and evasion
- Lateral movement and pivoting
- Circumventing security defenses
- Understanding attacker mindsets
- Performing an adversarial simulation
- Simulated attack scenario on live network

Day 2

- Developing a common defense
- Introduction to hunt teaming
- Performing a hunt team exercise
- Tools, tricks and free scripts!
- Identifying threats on the network and at the endpoint
- Using existing technology in the network
- Defending the network – live network defense

Requirements:

Participants must bring their own laptop. See website for technical details and requirements.

ONE DAY **8 CPEs**

SUNDAY, APRIL 2

W4 HOW TO PREPARE FOR, RESPOND TO AND RECOVER FROM A SECURITY INCIDENT

John Pironti, President, IP Architects, LLP

A risk-based and business-aligned approach to design, implementation and operation of comprehensive and proactive defensive programs and capabilities can be easily introduced, sustained and matured within organizations of any size or complexity. This workshop will explore a risk-based and pragmatic approach to defending information infrastructure and data assets.

- Module 1: Key elements of an information risk profile
- Module 2: Threat and vulnerability analysis
- Module 3: Key elements of a vulnerability management program
- Module 4: Pay me or you lose your data! – five key considerations when preparing for a ransomware incident
- Module 5: Key considerations for business resiliency

POST-CONFERENCE WORKSHOPS

HALF DAY **5 CPEs**

WEDNESDAY, APRIL 5

W5 MALWARE ANALYSIS 101 - MALWARE DETECTED, NOW WHAT? HANDS-ON

Paul Lewis, VP Technology Risk, T&M Protection Services
Kyle Poppenwimer, Sr. Digital Forensic Examiner, T&M Protection Services

Through basic malware analysis, learn how to identify business critical threat intelligence, respond to security incidents and strengthen security defense systems. This workshop will teach attendees the basics of both static and behavioral malware analysis utilizing real-world malware samples.

- Configure an isolated virtual environment to safely dissect and analyze malware
- Learn what makes malware malicious, how it spreads and what it does behind the scenes
- Analyze actual malware embedded in Microsoft Office files and Adobe PDF files
- Analyze real malicious portable executable files
- Perform behavioral analysis of real-world malware samples
- Identify and document indicators of compromise (IOCs) and drive threat intelligence

This is an entry level malware analysis course. Attendees will need to be comfortable navigating Microsoft Windows. A very basic understanding of a Linux environment is a plus.

Requirements:
Participants must bring their own laptop. Prior to the workshop, participants will need to download and install VMware Workstation Pro (Windows) or VMware Fusion (Mac OS X). See website for technical details and requirements.

W6 LEVERAGING CASB TO TAME YOUR CLOUD

George Gerchow, VP Security & Compliance, Sumo Logic

The Cloud Access Security Broker (CASB) market is the hottest market in security tools today and for good reason.

CASBs deliver a central point of monitoring and control across network services for cloud services, enabling organizations to find discover in the cloud, monitor their usage and prevent further activity.

This interactive workshop will cover deployment details, specific use cases and requirements to consider when choosing a CASB, and provide recommendations for ensuring the proper controls are in place for SaaS-based business applications.

Be prepared to:

- Learn about the CASB landscape
- Discuss what CASBs really do
- Look at deployment models and architecture
- Walk through SaaS-based application use cases
- Deploy a CASB solution

W7 BINARY EXPLOITATION 101 HANDS-ON

Lilith Wyatt, Security Engineer, Cisco ASIG

This class will explain exactly what an exploit is, the tools and skills needed to create one, and the theory of what is going on “under the hood” during the course of an exploit. Participants will view a live demonstration of the development of a buffer overflow and hear a detailed explanation of the process from beginning to end.

- Metasploit (msfvenom in particular)
- Linux memory management and layout
- Fuzzing (Mutiny fuzzing framework and sulley)
- Basic buffer overflows
- Linux memory protections (ASLR, DEP, Fortify Source)
- Advanced exploitation techniques (encoding/ret2libc/Egg hunters/ROP)

Prerequisites:
Familiarity with C programming, x86 Assembly, and a bit of Python. This is an advanced class for those wishing to hone their skills.

Recommendation:
Participants should bring a laptop that can run VMware Workstation, VMware Fusion or Virtualbox. See website for technical details and requirements.

W8 KEYS TO CREATING AN EFFECTIVE CYBERSECURITY CULTURE

Dr. Jane LeClair, President, Washington Center for Cybersecurity Research & Development

This workshop will provide participants with an understanding of the key components in establishing an effective cybersecurity culture within their organizations. Cybersecurity is more than independently functioning hardware and the people that operate it; rather, it is about the synergy that must be created within an organization that combines people, processes and technology into a capable, high-functioning operation.

- The role of technology
- Policies and processes that serve as guidelines
- New learning opportunities to offer
- Identifying key roles in the organization’s culture

ONE DAY **8 CPEs**

THURSDAY, APRIL 6

W9 CRAFTING AN EXCITING AND EFFECTIVE SECURITY TRAINING AND AWARENESS PROGRAM

George Dolicker, CISO, INC Research

This workshop will discuss key factors to successfully develop and deploy a balanced information security program that will increase compliance within your particular regulatory environment, and result in improved employee behaviors that are more resistant to both internal and external attacks.

- Identifying and meeting the individual training needs of your varied audience
- Evolving your message as your organization evolves and matures
- Separating arcane topics from the things everybody needs to know
- Delivering messages in stand-up, PowerPoints, posters, videos and publications
- Turning good sources of ideas, hints, tips and guidance into quality programs
- Developing programs on a shoestring
- Making the message memorable

W10 INTRODUCTION TO THREAT HUNTING WITH ELK

HANDS-ON

Fred Mastrippolito, President & CEO, Polito, Inc.
Ben Hughes, Senior Security Engineer, Polito, Inc.

- Introduction to log monitoring and analysis
  - Security Information and Event Management (SIEM)
  - Different types of event logs
  - Log ingestion, indexing and searching
  - Log correlation and enrichment using additional data sources
  - How network perimeter and endpoint security logs complement each other
- Introduction to threat hunting
  - Where threat hunting fits into your security program
  - Proactive monitoring/hunting vs. dead box forensics
  - Understanding the malware kill chain
  - The role of threat intelligence
  - Identifying and hunting for Indicators of Compromise (IOCs)
- Relevant tools including mostly open source or otherwise free tools:
  - ELK stack (popular open source log management platform)
  - Sysmon (free Microsoft Sysinternals endpoint logging tool)
- Threat hunting with logs
  - How to search logs to find anomalous/malicious events
  - How to build and use dashboards, automation and alerting capabilities
  - How to integrate threat intelligence feeds and enrich data

Requirements:
Participants must bring a Windows, Mac, or Linux laptop with at least 6 GB and a web browser. See website for technical details and requirements.

CONFERENCE AT-A-GLANCE

TECHNICAL LEVEL DESIGNATIONS

▁ LOW ▄ MEDIUM █ HIGH

Tools & Demos
Information Protection
Management & Strategies
Threat Management
Governance, Risk & Compliance
Operations & Applied Security
Security Roundtables*

*To enable an interactive learning environment these roundtable sessions are limited to 30 attendees on a first-come, first-served basis.

	TOOLS & DEMOS	INFORMATION PROTECTION	MANAGEMENT & STRATEGIES	THREAT MANAGEMENT	GOVERNANCE, RISK & COMPLIANCE	OPERATIONS & APPLIED SECURITY	SECURITY ROUNDTABLES*
MONDAY, APRIL 3, 2017							THIS TRACK SPONSORED BY Hewlett Packard Enterprise
7:30 AM - 8:30 AM	*Registration and Continental Breakfast*						
8:30 AM - 9:30 AM	**WELCOME KEYNOTE** Radical Remodeling: Renovating Security for Today's Problems and Tomorrow's Opportunities, presented by ***Rich Mogull***						
9:30 AM - 9:45 AM	Tech Spotlight presented by HP						
9:45 AM - 10:00 AM	*Refreshment Break*						
10:00 AM - 10:50 AM	A1 Ninja Looting Like A Pirate *William Lumpkin* ▄	B1 Data Protection - How to Sleep Better at Night *Steven Sheinfeld* ▁	C1 Management Hacking 101: Leading High Performance Security Teams *Tom Eston* ▁	D1 Launch, Detect, Evolve: The Mutation of Malware *Adam Kujawa* ▄	E1 Watch Out! Yet Another Regulator Is Asking Questions! *Randy Sabett* ▁	F1 Incident Response: The First 48 *Nick Selby* ▁	G1 Protecting Dollars for Pennies: Improving Organizational Security with Effective, Inexpensive Solutions *Kevin Johnson* ▁ *This session ends at 11:30 AM*
11:00 AM - 11:50 AM	A2 Pentesting Yourself to DEBT *Chris Nickerson* ▄	B2 Do You Have a Mega Breach Brewing? *Raef Meeuwisse* ▁	C2 Late-breaking session	D2 Applying Analytics to Cyber Threat Intelligence *Steve Orrin* ▄	E2 Insider Risk: Attacking the Threat From Within *George McBride* ▄	F2 Behavioral Analysis Using DNS, Network Traffic and Logs *Josh Pyorre* █	
12:00 PM - 1:15 PM	*Networking Lunch,* sponsored by Lieberman Software						
1:15 PM - 2:05 PM	A3 Everything is Code: Why Should You Worry About Software Security and Coding Standards? *Dan Creed* █	B3 Late-breaking session	C3 It's Not If, But When: How to Create Your Cyber Incident Response Plan *Lucie Hayward & Michael Quinn* ▁	D3 Developing a Threat and Vulnerability Management Program: A Pentester's Perspective *Robert Thibodeaux* ▄	E3 Vendor Vetting: Who's Touching Your Stuff? *Angie Singer Keating & Connie Mastovich* ▁	F3 Application Security: From the Ground Up *James Jardine* ▁	G2 Risk vs. Threat: Threat Intelligence Exposed *Kristy Westphal* ▄ *This session ends at 2:45 PM*
2:15 PM - 3:05 PM	A4 Scouting AWS Accounts for Security Gaps *Loïc Simon* █	B4 Secure Development for the Cloud *Randall Brooks* ▄	C4 I Have Phish I's For You *Mike Saurbaugh* ▄	D4 Forensics and Discovery Obligations vs. International Privacy Law *Darrin Reynolds* ▁	E4 Self-Audits: Applying User Context to Activity Anomalies *Leslie Lambert* ▄	F4 Late-breaking session	
3:05 PM - 3:20 PM	*Refreshment Break*						
3:20 PM - 4:10 PM	A5 The Exploits Used in Ransomware Campaigns *Brad Antoniewicz* █	B5 Secure Data Logistics: How Information Security Can Learn from Armored Cars *Chris Ensey & David Etue* ▁	C5 Cutting Through the Security Analytics Hype *Stu Bradley* ▄	D5 Late-breaking session presented by Cylance	E5 An Aflac Case Study: Moving a Security Program From Defense to Offense *Tim Callahan* ▁	F5 Rise of Cyber Hunting: Not Falling Victim to Undetected Breaches *Kris Lovejoy* ▄	G3 Securing Innovation *Kerry Matre* ▁ *This session ends at 4:45 PM*
4:15 PM - 5:00 PM	Panel: Cyber Liability Insurance: Misinformation Everywhere! moderated by ***Jake Kouns***						
5:00 PM - 6:30 PM	*Opening Party in the Expo*						
TUESDAY, APRIL 4, 2017							
7:30 AM - 8:30 AM	*Continental Breakfast*						
8:30 AM - 9:30 AM	**KEYNOTE ADDRESS** Rebooting the Auto Industry: When Security Affects Safety, presented by ***Craig Smith***						
9:40 AM - 10:30 AM	A6 Everything I Know About Security I Learned from Watching Kung Fu Movies *Paul Asadoorian* ▄	B6/B7 Your Data was Breached, Now What? An Interactive Incident Response Tabletop Experience *Diana Kelley & Ed Moyle* ▄	C6 Becoming Bi-lingual: Community Cybersecurity as a Business Impact *Summer Fowler* ▁	D6 Corporate Cannabis: Lessons Learned in Modeling a Controversial Threat Profile *Grant Sewell* ▄	E6 Late-breaking session	F6 Mutiny on the Bounty: Handling Security in a Bug Bounty World *Kevin Johnson* ▁	G4 IoT Security and Its Impact on Your Job *Chad Childers* ▁ *This session ends at 11:10 AM*
10:40 AM - 11:30 AM	A7 Excuse Me, Server, Do You Have the Time? *Brian Cardinale* █		C7 Late-breaking session	D7 The Details of Forensic Case Studies *Bill Dean* ▄	E7 Creating a Relevant Cyber Security Governance Framework: Supporting Business Digital Transformation *Dominic Vogel* ▁	F7 Getting Off the Back Foot – Employing Active Defense *Rafal Lós* ▄	
11:30 AM	*Expo opens*						
12:00 PM	*Lunch in the Expo*						
1:30 PM - 2:30 PM	**KEYNOTE ADDRESS** 1998 Called and It Wants Its Stupid Internet Law Back...Before It Destroys the World, presented by ***Cory Doctorow***						
2:30 PM - 2:40 PM	Tech Spotlight						
2:40 PM - 3:00 PM	*Refreshment Break in the Expo*						
3:00 PM - 3:50 PM	A8 Late-breaking session	B8 Pi in the Sky: The Push Towards Cloud-Based Applications *Nicholas Takacs* ▄	C8 Fast, Cheap or Good? How a Fortune 500 Picked All Three in Assessing Enterprise to Cloud Application Migration Risks *Jon-Michael Brook* ▁	D8 Threat Modeling Wearables by 2019 *David Lindner* ▄	E8 Moving Mountains Through Measurement *Chris Clymer, Jack Nichelson & Jason Middaugh* ▁	F8 Victory in 100 Battles: How to Perform a Successful Asset Inventory *Chris Poulin* ▄	G5 The Technology is Worth 5% *Joshua Marpet & Scott Lyons* ▄ *This session ends at 4:15 PM*
4:00 PM - 4:50 PM	A9 Abnormal Behavior Detection in Large Environments *David Kennedy* ▄	B9 Late-breaking session	C9 Information Security Assessments: Building Bridges Instead of Making Enemies *Jaret Preston* ▁	D9 Facing Emerging Threats - Evolving from Penetration Testing to Capability Effectiveness Testing *Paul Rohmeyer* ▁	E9 Case Study: Atlassian's Journey Through CSA Certification *Craig Davies* ▁	F9 The Phishing Kill Chain *Ira Winkler* ▄	
4:45 PM - 6:15 PM	*Networking Reception in the Expo*						
WEDNESDAY, APRIL 5, 2017							
8:00 AM - 8:30 AM	*Rise'n Shine Breakfast in the Expo*						
8:30 AM - 9:30 AM	**KEYNOTE ADDRESS** The Three T's of Security: Talent, Tools & Techniques, presented by ***Jim Routh***						
9:30 AM - 11:00 AM	*Refreshment Break in the Expo; Enjoy Mimosas while we announce Passport-to-Prizes!*						
10:30 AM - 11:20 AM	A10 Hacking Blockchain *Konstantinos Karagiannis* ▄	B10 Patients Have Lost Patience for Data Breaches *Ray Potter* ▁	C10 What We Learn from Hackers ... and the Government *Erez Liebermann & Andrew Pak* ▁	D10 Social Engineering: It's Not Just for Suckers Anymore *Erich Kron* ▁	E10 Cyber Liability Insurance 101 - What You Should Know Before and After a Breach *Brian Kelly* ▁	F10 Dealing with Cyberextortion, Ransomware and Other Bad Stuff *Ben Rothke* ▁	G6 Is Enterprise Resiliency the New Security Strategy? *Gary Sheehan* ▁ *This session ends at 11:45 AM*
11:30 AM - 12:15 PM	Panel: You're in a Leadership Position, Now What? moderated by ***Michael Santarcangelo***						

MONDAY, APRIL 3

10:00 AM – 10:50 AM

A1 NINJA LOOTING LIKE A PIRATE

William Lumpkin, Sr. Information Janitor, Data Housekeeping Services

- How to hunt for data repositories and apply search techniques
- Security issues that exist in media- or multimedia-driven environments
- The positive and negatives of collecting this information

10:00 AM – 10:50 AM

B1 DATA PROTECTION - HOW TO SLEEP BETTER AT NIGHT

Steven Sheinfeld, Vice President, Internal Assurance Services, Rite Aid Corp.

- Consequences of not properly protecting customers' and associates' personal information
- The regulatory environment surrounding data protection
- Selecting a data security framework that fits your company's business and culture

10:00 AM – 10:50 AM

C1 MANAGEMENT HACKING 101: LEADING HIGH PERFORMANCE SECURITY TEAMS

Tom Eston, Manager, Penetration Testing, Veracode

- Techniques for hiring the right team members
- Understanding your role as a leader: coaching and motivation methods
- Improving communication and maximizing the performance of a technical team to achieve results

10:00 AM – 10:50 AM

D1 LAUNCH, DETECT, EVOLVE: THE MUTATION OF MALWARE

Adam Kujawa, Head of Malware Intelligence, Malwarebytes

- New malware tactics researchers and analysts are confronting daily
- How cyber criminals are using Crypters to evade detection
- How to proactively protect your business from future challenges

10:00 AM – 10:50 AM

E1 WATCH OUT! YET ANOTHER REGULATOR IS ASKING QUESTIONS!

Randy Sabett, Vice Chair, Privacy & Data Protection Practice, Cooley LLP

- Discuss which regulators have typically involved in cybersecurity (e.g., HHS and FTC)
- Address the areas of privacy and cybersecurity often at issue
- Determine how to deal with regulator inquiries

10:00 AM – 10:50 AM

F1 INCIDENT RESPONSE: THE FIRST 48

Nick Selby, Operations & Applied Security, Secure Ideas

- The key roles that must be filled
- The crucial strategies that drive the IR visibility - by hook or by crook
- Whack-a-mole post-incident clean up

10:00 AM – 11:30 AM

G1 PROTECTING DOLLARS FOR PENNIES: IMPROVING ORGANIZATIONAL SECURITY WITH EFFECTIVE, INEXPENSIVE SOLUTIONS

Kevin Johnson, CEO, Secure Ideas

- Dive into today's new and complex security issues
- Learn new techniques to prevent breaches
- Discover how to inexpensively monitor and alert for security issues

11:00 AM – 11:50 AM

A2 PENTESTING YOURSELF TO DEBT

Chris Nickerson, CEO, LARES

- How technical debt is created during a pentest and how it relates to testing debt
- Potential guidelines to use that can reduce or eliminate debt
- How to test in a collaborative manner to increase the security of a program

11:00 AM – 11:50 AM

B2 DO YOU HAVE A MEGA BREACH BREWING?

Raef Meeuwisse, Director Cybersecurity & Data Privacy Governance, Cyber Simplicity Ltd

- How to tell if your organization is vulnerable to a mega breach
- How to socialize the risk without appearing sensationalist
- How to change cyber behaviors and organizational cultural obstacles to mitigate risks

11:00 AM – 11:50 AM

C2 LATE-BREAKING SESSION

11:00 AM – 11:50 AM

D2 APPLYING ANALYTICS TO CYBER THREAT INTELLIGENCE

Steve Orrin, Chief Technologist, Intel Corp.

- How to make sense of the various technologies and approaches to threat intelligence and analytics
- How to have better-informed risk tolerance discussions
- How to better set security priorities, develop capital and operational expenditure budgets, and identify potential security solutions and practices

11:00 AM – 11:50 AM

E2 INSIDER RISK: ATTACKING THE THREAT FROM WITHIN

George McBride, Vice President, Stroz Friedberg

- Necessary components of an insider risk management program
- Specific legal and human resource considerations
- Recent technical advancements

11:00 AM – 11:50 AM

F2 BEHAVIORAL ANALYSIS USING DNS, NETWORK TRAFFIC AND LOGS

Josh Pyorre, Security Researcher, OpenDNS/Cisco

- Methods of performing behavioral analysis to observe and create a baseline in any environment
- New methods of BA to apply to monitor and secure networks

1:15 PM – 2:05 PM

A3 EVERYTHING IS CODE: WHY SHOULD YOU WORRY ABOUT SOFTWARE SECURITY AND CODING STANDARDS?

Dan Creed, Security & Infrastructure Management, Morgridge Institute for Research

- How SWAMP can help with writing, testing and delivering secure code
- Developing the policy and procedures to make code security part of your culture is also critical
- A look at threat vectors and the current landscape of tools to mitigate those threats

1:15 PM – 2:05 PM

B3 LATE-BREAKING SESSION

1:15 PM – 2:05 PM

C3 IT'S NOT IF, BUT WHEN: HOW TO CREATE YOUR CYBER INCIDENT RESPONSE PLAN

Lucie Hayward, Managing Consultant, Kroll
Michael Quinn, Associate Managing Director, Kroll

- Understand the difference between an event and an incident, and why the distinction is important
- Learn how to build out your Incident Response Team (IRT) and who should be included
- Experience a walk-through of a cyber incident scenario and discuss possible actions and outcomes

1:15 PM – 2:05 PM

D3 DEVELOPING A THREAT AND VULNERABILITY MANAGEMENT PROGRAM: A PENTESTER'S PERSPECTIVE

Robert Thibodeaux, Security Operations Director, DefenseStorm

- Current threat actors and see a cyber kill chain and exploit example
- Insider view of the network
- Open source tools for building a threat and vulnerability program

1:15 PM – 2:05 PM

E3 VENDOR VETTING: WHO'S TOUCHING YOUR STUFF?

Angie Singer Keating, CEO, Reclamere, Inc.
Connie Mastovich, Senior Security Compliance Analyst, Reclamere, Inc.

- The security impact of thorough vendor vetting
- How to effectively use information security questionnaires and pre-screening questionnaires
- How to build a strong business associate agreement

1:15 PM – 2:05 PM

F3 APPLICATION SECURITY: FROM THE GROUND UP

James Jardine, CEO, Jardine Software

- Understand why an AppSec program is critical to the organization
- Identify first steps and goals of an AppSec program
- Help identify resources and how the entire organization relates to the program

1:15 PM – 2:45 PM

G2 RISK VS. THREAT: THREAT INTELLIGENCE EXPOSED

Kristy Westphal, Senior Manager, Charles Schwab

- Risks versus threats and what threat intelligence should really accomplish
- The correct size of the TI program to support requirements
- Reporting opportunities

2:15 PM – 3:05 PM

A4 SCOUTING AWS ACCOUNTS FOR SECURITY GAPS

Loïc Simon, Principal Security Consultant, NCC Group

- Strategy to follow when assessing the security of AWS accounts
- Scout2 and how to use some powerful non-default options of Scout2
- Uncommon IAM-related security risks

2:15 PM – 3:05 PM

B4 SECURE DEVELOPMENT FOR THE CLOUD

Randall Brooks, Engineering Fellow, Raytheon

- What happens when applications are moved to the cloud?
- How do cloud technologies such as elasticity, containers and microservices come into play?
- How does one get started with applying application security to cloud?

2:15 PM – 3:05 PM

C4 I HAVE PHISH I'S FOR YOU

Mike Saurbaugh, Director, Technical Alliances, PhishMe

- Investigate potential successful phishing campaigns
- Learn the "I's" of a successful phishing incident response program
- Immersion, incident response, investigation, intelligence, integration
- Be better prepared to organize, analyze and respond to phishing

2:15 PM – 3:05 PM

D4 FORENSICS AND DISCOVERY OBLIGATIONS VS. INTERNATIONAL PRIVACY LAW

Darrin Reynolds, Owner/Chief Privacy Officer, Reynolds Privacy, LLC

- Legal landmines to consider during a security incident or other litigation
- Strategies that allow organizations to hit both targets with a single shot and avoid consequences of non-compliance and violation of international law
- Tactical measures or technical tools available to address this situation

2:15 PM – 3:05 PM

E4 SELF-AUDITS: APPLYING USER CONTEXT TO ACTIVITY ANOMALIES

Leslie Lambert, Chief Security and Strategy Office, Gurucul

- Why traditional security methods cannot detect these attacks
- What alternative protections are available and how effective they are
- The definition of "self-audit" and how it works to help detect account compromise

2:15 PM – 3:05 PM

F4 LATE-BREAKING SESSION

3:20 PM – 4:10 PM

A5 THE EXPLOITS USED IN RANSOMWARE CAMPAIGNS

Brad Antoniewicz, Security Researcher, OpenDNS/Cisco

- Ransomware can be defended against and identified early in the attack chain
- It is possible to automate a defense with a few simple tools
- Exploits used to deliver ransomware contain clues about their authors

3:20 PM – 4:10 PM

B5 SECURE DATA LOGISTICS: HOW INFORMATION SECURITY CAN LEARN FROM ARMORED CARS

Chris Ensey, Chief Operating Officer, Dunbar Armored
David Etue, Vice President for Managed Services, Rapid7

- How concepts from armored logistics can be applied to data protection
- Ways to use data tagging, classification, encryption and other security tools to create data telemetry
- How to use open source intelligence without breaking the bank

3:20 PM – 4:10 PM

C5 CUTTING THROUGH THE SECURITY ANALYTICS HYPE

Stu Bradley, Vice President, SAS Institute

- How to evaluate whether security analytics can be a force multiplier to current detection/response efforts
- Why you should be skeptical of claims of predictive analytics
- Which key components of an analytics initiative are often overlooked

3:20 PM – 4:10 PM

D5 LATE-BREAKING SESSION

presented by Cylance

3:30 PM – 4:20 PM

E5 AN AFLAC CASE STUDY: MOVING A SECURITY PROGRAM FROM DEFENSE TO OFFENSE

Tim Callahan, Senior Vice President, Global Security Chief Security Officer, Aflac

- Three proven methods to show the strategic value of moving from a traditional defensive in-depth posture to an offensive approach
- Alternative forms of internal data, internal system intelligence and external intelligence sharing
- The importance of distinguishing intelligence from information or data and how this analysis process can include manual, human analysis, or a system analytics engine for parsing information

3:20 PM – 4:10 PM

F5 RISE OF CYBER HUNTING: NOT FALLING VICTIM TO UNDETECTED BREACHES

Kris Lovejoy, President, Acuity Solutions

- Steps to take for a successful cyber hunting mission
- How security architecture and traditional security operators can bear a greater portion of hunting efforts
- How to empower the cyber hunters and achieve greater ROI

3:20 PM – 4:45 PM

G3 SECURING INNOVATION

Kerry Matre, Sr. Manager, HPE Security Portfolio, HP

- What IT innovations cause weaknesses that attackers can exploit?
- How can we effectively plan to deploy new IT innovations securely?
- How should we prioritize addressing innovation risk vs. fighting traditional external and internal threats?

4:15 PM – 5:00 PM

PANEL: CYBER LIABILITY INSURANCE: MISINFORMATION EVERYWHERE!

Moderator: Jake Kouns, CISO, Risk-Based Security

- Available types of coverage
- Underwriting, pricing, legal and claims
- Cyber insurance "gotchas" and risk management services

TUESDAY, APRIL 4

9:40 AM – 10:30 AM DEMO

A6 EVERYTHING I KNOW ABOUT SECURITY I LEARNED FROM WATCHING KUNG FU MOVIES

Paul Asadoorian, CEO, Security Weekly & Offensive Countermeasures

- What your teacher may be reluctant to teach you
- The consequences of taking shortcuts in your training
- The "soft" skills that will more likely than not lead you to victory

9:40 AM – 11:30 AM

B6/B7 YOUR DATA WAS BREACHED, NOW WHAT? AN INTERACTIVE INCIDENT RESPONSE TABLETOP EXPERIENCE

Diana Kelley, Executive Security Advisor (ESA), IBM Security
Ed Moyle, Director of Thought Leadership and Research, ISACA

- Tabletop exercise on how to strategically approach a post-breach investigation and response
- Consequences of high-stakes decisions about response that can impact your organization
- How to respond when surprises arise

9:40 AM – 10:30 AM

C6 BECOMING BI-LINGUAL: COMMUNITY CYBERSECURITY AS A BUSINESS IMPACT

Summer Fowler, Technical Director, Carnegie Mellon University Software Engineering Institute

- Effective measures and metrics when communicating cybersecurity posture
- Best practices in communicating cybersecurity to senior management
- Lessons learned in cybersecurity crisis communications

9:40 AM – 10:30 AM

D6 CORPORATE CANNABIS: LESSONS LEARNED IN MODELING A CONTROVERSIAL THREAT PROFILE

Grant Sewell, Manager, Global Information Security Strategy

- Barriers and obstacles observed in creating a threat profile
- Unique threats and actors identified to the industry
- Indicators and metrics to determine exposure; key controls that support a secure environment

9:40 AM – 10:30 AM

E6 LATE-BREAKING SESSION

9:40 AM – 10:30 AM

F6 MUTINY ON THE BOUNTY: HANDLING SECURITY IN A BUG BOUNTY WORLD

Kevin Johnson, CEO, Secure Ideas

- Pros and cons of bug bounties for individuals partaking and organizations evaluating bug bounties
- How organizations can determine if they need a bug bounty program
- Necessary skill sets for individuals to participate in a bug bounty program

9:40 AM – 11:10 AM

G4 IOT SECURITY AND ITS IMPACT ON YOUR JOB

Chad Childers, Consultant, Ford Motor Co.

- Learn from early and recent incidents to help avoid repeating the same mistakes
- Lists of common controls and risk decision guidelines
- Projects and needs for future IoT security research and development

10:40 AM – 11:30 AM

A7 EXCUSE ME, SERVER, DO YOU HAVE THE TIME?

Brian Cardinale, Senior Penetration Tester, Veracode

- Common developer bad practices and real-life examples of predictable tokens
- How to identify time-based tokens during black box testing in active and passive fashion
- Methodology on reversing tokens to interact with protected resources or defeat protections

10:40 AM – 11:30 AM

C7 LATE-BREAKING SESSION

10:40 AM – 11:30 AM

D7 THE DETAILS OF FORENSIC CASE STUDIES

Bill Dean, Senior Manager, LBMC

- How digital forensics provides value
- Details of tools and approaches to be successful, including commercial and open source forensics tools
- Case studies of success

10:40 AM – 11:30 AM

E7 CREATING A RELEVANT CYBER SECURITY GOVERNANCE FRAMEWORK: SUPPORTING BUSINESS DIGITAL TRANSFORMATION

Dominic Vogel, Chief Security Strategist, Cyber.SC

- Digital transformations are magnifying cybersecurity challenges
- We have a pressing need for formal guidance to help with cybersecurity challenges
- Practical steps for establishing relevant governance that aligns with and supports business strategy

10:40 AM – 11:30 AM

F7 GETTING OFF THE BACK FOOT – EMPLOYING ACTIVE DEFENSE

Rafal Lós, Director of Solutions Research & Development, Optiv

- A clear definition of active defense and its role in the modern enterprise security program
- The practical application of threat intelligence to enhance and enable enterprise security
- Optimizations of the cyber threat intelligence lifecycle and framework

3:00 PM – 3:50 PM

A8 LATE-BREAKING SESSION

3:00 PM – 3:50 PM

B8 PI IN THE SKY: THE PUSH TOWARDS CLOUD-BASED APPLICATIONS

Nicholas Takacs, Chief Technology Officer, Bethlehem Area School District

- Capabilities and flexibility of the Raspberry Pi architecture
- Processes for scaling the technology within an enterprise
- Framework for "selling" the capabilities to upper management

3:00 PM – 3:50 PM

C8 FAST, CHEAP OR GOOD? HOW A FORTUNE 500 PICKED ALL THREE IN ASSESSING ENTERPRISE TO CLOUD APPLICATION MIGRATION RISKS

Jon-Michael Brook, Principal, Guide Holdings, LLC

- A deep dive into the CSA's Cloud Controls Matrix
- How publicly available tools are useful in assessing cloud risks
- Successful processes and techniques used by a Fortune 500 company for risk identification and mitigation

3:00 PM – 3:50 PM

D8 THREAT MODELING WEARABLES BY 2019

David Lindner, Vice President of Solutions, nVisium

- History and future of wearables
- Security of wearables
- Threat landscape of wearables and common attacks against wearables

3:00 PM – 3:50 PM

E8 MOVING MOUNTAINS THROUGH MEASUREMENT

Chris Clymer, Director of Security, MRK Technologies
Jason Middaugh, Director of Infrastructure, Cliffs Natural Resources
Jack Nichelson, Director, IT Infrastructure & Security, Chart Industries

- How to show security progress and present to senior leadership
- Real-world security metrics: Identifying and using easily collected data
- Aligning with existing organizational metrics

3:00 PM – 3:50 PM

F8 VICTORY IN 100 BATTLES: HOW TO PERFORM A SUCCESSFUL ASSET INVENTORY

Chris Poulin, Research Strategist, IBM X-Force

- How to overcome analysis paralysis and start with asset tracking, data discovery and continuous awareness
- Tools available and skills required to build and maintain an effective asset inventory
- How to optimize an identity and access control program around assets and applications

3:00 PM – 4:15 PM

G5 THE TECHNOLOGY IS WORTH 5%

Scott Lyons, VP Business Development, Warcollar
Joshua Marpet, SVP Compliance and Managed Services, CyberGRC

- Learn to distinguish (and communicate the difference) between a tool, a product and a service
- The signs of a company with a good product, and more importantly, an amazing implementation
- Figure out which products are investable, and utilize that to your benefit at the negotiating table

4:00 PM – 4:50 PM

A9 ABNORMAL BEHAVIOR DETECTION IN LARGE ENVIRONMENTS

David Kennedy, Founder, Principal Security Consultant, TrustedSec LLC

- Learn techniques for defending against some of the most common attack vectors
- Understand how to identify abnormal behavior in the network
- Catch early warning indicators of compromise within your infrastructure

4:00 PM – 4:50 PM

B9 LATE-BREAKING SESSION

4:00 PM – 4:50 PM

C9 INFORMATION SECURITY ASSESSMENTS: BUILDING BRIDGES INSTEAD OF MAKING ENEMIES

Jaret Preston, Information Security Officer, Caterpillar

- How to partner with independent facilities and baseline expectations of security
- Awareness and engagement opportunities
- How to focus on risk awareness and not non-compliance

4:00 PM – 4:50 PM

D9 FACING EMERGING THREATS - EVOLVING FROM PENETRATION TESTING TO CAPABILITY EFFECTIVENESS TESTING

Paul Rohmeyer, Associate Professor, Stevens Institute of Technology

- The value of introducing realistic, time-bound drills and tests
- Enhancement of test team activities to mimic realistic adversary tactics
- Effective governance and oversight mechanisms to embed capability effectiveness testing in enterprise risk management practices

4:00 PM – 4:50 PM

E9 CASE STUDY: ATLASSIAN'S JOURNEY THROUGH CSA CERTIFICATION

Craig Davies, Head of Security, Atlassian

- The benefit of adhering to Cloud Security Alliance (CSA) guidelines over competing standards
- How companies can improve processes, techniques and policies as a result
- How "automating everything" can help companies operate with a high degree of efficiency and security

4:00 PM – 4:50 PM

F9 THE PHISHING KILL CHAIN

Ira Winkler, President, Secure Mentem

- Understand the complete phishing lifecycle and kill chain
- Understand how technology is a failsafe for poor awareness
- How to implement kill chain analysis for other areas of awareness

WEDNESDAY, APRIL 5

10:30 AM – 11:20 AM

A10 HACKING BLOCKCHAIN

Konstantinos Karagiannis, CTO, BT Americas

- The basics of how blockchain and variants work
- The risk of current/proposed blockchain applications in digital assets, identity, verifiable data and smart contracts
- How to modify blockchain to protect cryptocurrencies and newly emerging adaptations of the technology

10:30 AM – 11:20 AM

B10 PATIENTS HAVE LOST PATIENCE FOR DATA BREACHES

Ray Potter, CEO, SafeLogic

- Assess the security compliance levels of deployed technology in your organization
- Distinguish between compliant and non-compliant encryption to determine whether Safe Harbor is in effect
- Develop a strategy to ensure that only compliant technology is approved for future use

10:30 AM – 11:20 AM

C10 WHAT WE LEARN FROM HACKERS ... AND THE GOVERNMENT

Erez Liebermann, Chief Counsel, Cybersecurity & Privacy, Prudential Financial
Andrew Pak, Trial Attorney, Computer Crimes and Intellectual Property, Department of Justice

- What the government has learned from talks with hackers
- How information sharing is affected by new legislation
- The government's new directive about hacking investigations

10:30 AM – 11:20 AM

D10 SOCIAL ENGINEERING: IT'S NOT JUST FOR SUCKERS ANYMORE

Erich Kron, Security Awareness Advocate, KnowBe4

- The latest techniques designed to social engineer users
- Best practices for training users not to fall for social engineering attacks
- Technical and non-technical solutions to address threats

10:30 AM – 11:20 AM

E10 CYBER LIABILITY INSURANCE 101 - WHAT YOU SHOULD KNOW BEFORE AND AFTER A BREACH

Brian Kelly, Chief Information Security Officer, Quinnipiac University

- Overview and understanding of cyber liability insurance policies
- Risk analysis perspectives
- Resources available through cyber liability policy before and after a breach

10:30 AM – 11:20 AM

F10 DEALING WITH CYBEREXTORTION, RANSOMWARE AND OTHER BAD STUFF

Ben Rothke, Senior eGRC Consultant, Nettitude

- Different types of attacks, attacker targets and patterns, and ransomware
- Maximizing cyberdefense effectiveness to avoid being a victim
- Countermeasures and best practices to avoid ransomware

10:30 AM – 11:45 AM

G6 IS ENTERPRISE RESILIENCY THE NEW SECURITY STRATEGY?

Gary Sheehan, Chief Security Officer, ASMGi

- Discuss key resiliency concepts, strategies and techniques
- Understand how security impacts and complements enterprise resiliency
- Discover how to contribute to their organization's resiliency strategy

11:30 AM – 12:15 PM

PANEL: YOU'RE IN A LEADERSHIP POSITION, NOW WHAT?

Moderator: Michael Santarcangelo

- Leadership vs. management
- The startup mindset
- Real-world experiences as a new leader coming from an individual contributor role

EXPO

EXPO HOURS

Monday, April 3, 5:00 PM - 6:30 PM
Tuesday, April 4, 11:30 AM - 6:15 PM
Wednesday, April 5, 8:00 AM - 11:00 AM

EVENT SPONSOR

Hewlett Packard Enterprise

Hewlett Packard Enterprise
www.hpe.com
Hewlett Packard Enterprise is an industry leading technology company that enables customers to go further, faster. With the industry's most comprehensive portfolio, spanning the cloud to the data center to workplace applications, our technology and services help customers around the world make IT more efficient, more productive and more secure.

PLATINUM SPONSORS

LIEBERMANSOFTWARE™

Malwarebytes

GOLD SPONSORS

Check Point SOFTWARE TECHNOLOGIES LTD

CYLANCE

SILVER SPONSORS

DARKTRACE

GRSEE Make Cyber Secure Again

KnowBe4 Human error. Conquered.

LogRhythm® The Security Intelligence Company

PHISHLABS

QUALYS® CONTINUOUS SECURITY

Join 1,000+ of your peers and top infosec vendors in the Expo, the heart of InfoSec World's networking community.

NETWORKING EVENTS

Monday, April 3, 5:00 PM - 6:30 PM
Tuesday, April 4, 4:45 PM - 6:15 PM
Wednesday, April 5, 9:30 AM - 11:00 AM

DON'T MISS! Tech Update Sessions
Stop by the Tech Theatre located in the center of the Expo hall to hear brief overviews on the latest trends and solutions from some of the best infosec vendors today.

SHOWCASE YOUR ORGANIZATION

Ready for three days of face-to-face time with infosec decision makers from around the world? This year's InfoSec World program has more Expo time than ever before, which means more time in front of the people you want to talk to most. If you are interested in exhibitor or sponsorship opportunities at InfoSec World, please contact one of our Sales Directors:

CJ OLIVERI at coliveri@misti.com
or (508) 532-3609 (for Vendors A-L)

MIKE ALESSIE at malessie@misti.com
or (203) 209-6574 (for Vendors M-Z)

PACKAGES & PRICING

PACKAGE	CPEs	INCLUDES	TIER 1 Until Jan 29	TIER 2 Jan 30 - March 26	TIER 2 After March 27
✓BEST VALUE InfoSec World Pass **SAVE** up to $1580	47*	Access to conference sessions, keynotes, one workshop/summit per time slot, all lunches and Expo	$3695	$3895	$4095
Main Conference	18	InfoSec World conference sessions, keynotes, lunch on Monday and Tuesday and Expo	$1795	$1995	$2195
Government Employees and Association Members *(10% off Main Conference Fee)*	18	InfoSec World conference sessions, keynotes, lunch on Monday and Tuesday and Expo	$1615	$1795	$1975
CISO Leadership Summit	8	Summit sessions and lunch	$995	$1095	$1195
Risk Management Summit and Cloud Security Summit	8	Summit sessions and lunch	$895	$995	$1095
Half-day Workshop	5	Half-day workshop and lunch on Wednesday	$445	$495	$595
One-day Workshop	8	One-day workshop and lunch	$795	$895	$995
Two-day Workshop	16	Two-day workshops and lunch on both days	$995	$1095	$1195
Expo Only	0	Access to the Expo and select sessions	$0	$0	$75

*Earn up to 47 CPEs depending upon workshop/summit selection.

INFOSEC WORLD PASS – EARN UP TO 47 CPEs!

Take advantage of all the top-notch learning available at InfoSec World at a substantially reduced rate! With the **InfoSec World Pass**, you have the freedom to attend as many optional workshops and/or summits as you can fit into your schedule. And of course you get InfoSec World sessions, keynotes and the Expo – all at a discounted price. It's an offer too good to pass up!

(One workshop or summit per time slot. You will only receive the workshop/summit materials for the specific workshop/summit you attend.)

GROUP DISCOUNTS AVAILABLE!

When two people from your organization attend InfoSec World, a third person can attend at half price! The discounted registration must be of equal or lesser value. All registrations must be made and paid for at the same time, cannot be combined with any other discount offer and cannot be used on previous registrations. Please call Customer Service at 508-879-7999 ext. 501.

REGISTRATION & TRAVEL INFORMATION

Top reasons to stay at the Omni Orlando Resort at ChampionsGate:

Convenience: Don’t stress about transportation to and from the conference. Everything you need will be in one location including all conference sessions and networking events, as well as after conference entertainment including onsite restaurants and recreation (including two world-class gold courses).

Networking: Don’t miss a minute of networking when you stay at the Omni. Enjoy three onsite receptions and then continue your peer-to-peer brainstorming after hours at one of the many hotel bars or pool.

Leisure: After a day packed with keynotes, breakout sessions and Expo time, you might be ready to unwind. Hang out by the pool, participate in walk-out golf, relax at the spa or take the complimentary shuttle to the Walt Disney World Theme Parks.

Book your room online at infosecworld.misti.com/hotel

GENERAL INFORMATION

THREE EASY WAYS TO REGISTER

Our Customer Service Department looks forward to answering your questions and making the registration process easy and fast. Call today to reserve your seat.

Web infosecworld.misti.com

Email customerservice@misti.com

Call 508-879-7999 ext. 501

You can also register through your MISTI Sales Consultant.
Important: When registering, have your registration code ready, found on the mailing panel of this brochure.

FEES

All fees must be paid in advance in US dollars. The conference fee includes admission to sessions, conference materials (excluding optional workshops/summits), continental breakfasts, refreshments, lunches and receptions. All workshop/summit fees include lunch and materials for the workshops/summits you attend. (See pricing schedule on page 14).

THE MISTI HIGH-YIELD/NO-RISK GUARANTEE

If you attend the conference and feel you did not benefit from it, simply tell us why on your organization’s letterhead and you will receive full credit toward another MISTI program.

CONTINUING EDUCATION CREDITS

Conference attendees are eligible to receive 18 hours of credits for the conference, 16 for two-day workshops, 8 for one-day summits and workshops and 5 for half-day workshops.

CANCELLATIONS, TRANSFERS AND SUBSTITUTIONS

A full refund, less a $195 administrative fee, will be given for cancellations received 15 days or more before the event. Tuition is non-refundable for cancellations made 14 days or less before the event. You may, however, transfer your tuition to another MISTI course, less a $195 administrative fee. Transfers are valid for 12 months from the time of initial cancellation. Substitutions are welcome at any time. Those who do not cancel before the conference date and who do not attend are responsible for the full non-refundable, non-transferable tuition. To cancel, call Customer Service at 508-879-7999 ext. 501.

ACCOMMODATIONS

The conference will be held at the Omni Orlando Resort at ChampionsGate, where a block of discounted rooms at the special conference rate of **$225.00 per night** has been reserved on a space-available basis until **March 9, 2017**. We also have a limited number of rooms at the prevailing government per diem rate. After that date, reservations may be made on a space-available, regular-rate basis. To be assured this discounted room rate, we urge you to make your reservations early. To book now, call 407-390-6664 and mention MIS Training Institute to receive the special conference rate.

Omni Orlando Resort at ChampionsGate
1500 Masters Boulevard, ChampionsGate, FL 33896
407-390-6664

To Book Your Room Online: infosecworld.misti.com/hotel

NATIONAL REGISTRY OF CPE SPONSORS

MIS Training Institute is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

Field of Study: Information Technology

MIS|TI™ PRESENTS

# InfoSecWorld

Conference & Expo 2017

APRIL 3-5, 2017 | OMNI ORLANDO RESORT AT CHAMPIONSGATE | CHAMPIONSGATE, FL

70+ SESSIONS | **10** WORKSHOPS | **7** DYNAMIC TRACKS | **3** CO-LOCATED SUMMITS

CISO LEADERSHIP SUMMIT
April 2, 2017

CLOUD SECURITY SUMMIT
April 6, 2017

RISK MANAGEMENT SUMMIT
April 6, 2017

PRE- AND POST-CONFERENCE WORKSHOPS

EARN ADDITIONAL CPEs!

EARN UP TO
47 CPEs
WITH OUR WORLD PASS

W1 DEVSECOPS SYMPOSIUM

W2 MAINFRAME SECURITY: HANDS-ON AUDIT AND COMPLIANCE HANDS-ON

W3 RED TEAM VS. BLUE TEAM TECHNIQUES WITH HUNT TEAMING HANDS-ON

W4 HOW TO PREPARE FOR, RESPOND TO AND RECOVER FROM A SECURITY INCIDENT

W5 MALWARE ANALYSIS 101 - MALWARE DETECTED, NOW WHAT? HANDS-ON

W6 LEVERAGING CASB TO TAME YOUR CLOUD

W7 BINARY EXPLOITATION 101 HANDS ON

W8 KEYS TO CREATING AN EFFECTIVE CYBERSECURITY CULTURE

W9 CRAFTING AN EXCITING AND EFFECTIVE SECURITY TRAINING AND AWARENESS PROGRAM

W10 INTRO TO THREAT HUNTING WITH ELK HANDS-ON

SAVE when you register before January 29th!

MIS|TI™
TRAINING INSTITUTE

#INFOSECWORLD

Keep checking the InfoSec World website for updates and exciting additions!

INFOSECWORLD.MISTI.COM