Agenda

All Summit Sessions will be held in the Press Room (unless noted).

*All approved presentations will be available online following the Summit at **https://files.sans.org/securityleadership2014**. An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.*

Wednesday, April 30

8:00-8:45 am

Registration

8:45-9:00 am

Welcome & Introduction

***Frank Kim**, Summit Chairman, SANS Institute*

***John Pescatore**, Director of Emerging Security Trends, SANS Institute*

9:00-9:45 am

Keynote Address:

Security Leadership: A Framework for Taking Control

The threat landscape can feel like a carnival funhouse: constantly shifting, twisting and turning, with terrifying surprises around every turn. True leadership in information security requires more than just adequately thwarting threats as they arise. The most effective security leaders create a framework for being relentlessly proactive in improving their organizations' security. Learn how to leverage the Critical Security Controls to decrease your risk of enduring a data breach, and hear real-world examples of organizations who've seen measurable results using this framework.

*Speaker: **Tony Sager**, Director, SANS Institute*

9:45-10:45 am

CISO 101: Lessons Learned From Higher Education

In this session, a panel of CISOs from colleges and universities will weigh in on their biggest challenges, their must-have security policies, and their favorite security controls and frameworks. The panel will also explore best practices for communicating with executive management regarding the risks, costs and consequences of data breaches, and the process for establishing business cases that get security initiatives funded.

*Moderator: **Larry Wilson**, CISO, UMASS*

*Panelists: **David Escalante**, Director of Computer Policy & Security, Boston College*
***Sherry Horeanopoulos**, CISA, Information Security Officer, Fitchburg State University*
***David J. Sherry**, CISSP CISM, Chief Information Security Officer, Brown University*

10:45-11:00 am

Networking Break & Vendor Expo

11:00-12:00 pm

A Secure Investment: What Leading VCs Think About the Future of Cyber Security

Threats continue to evolve and innovative security solutions continue to be in high demand. In previous waves of threats, small startup security companies delivered that innovation and often grew rapidly to become trusted enterprise security technology suppliers. Will that be true in this wave, or will developments such as cloud, mobility, software defined networks, etc. change the security markets in radical ways? A panel of experienced investors in security companies will discuss these and other issues.

Moderator: ***John Pescatore****, Director of Emerging Security Trends, SANS Institute*

Panelists: ***Greg Dracon****, Partner, .406 Ventures*
Jeff Fagnan*, Partner, Atlas Venture*
Rick Grinnell*, Managing Director, Fairhaven Capital Partners*

12:00-1:15 pm

Lunch & Learn

presented by

VIEWFINITY

Adaptive Security Strategies via Bi-lateral Network to Endpoint Threat Response

Mr. Shtilman will discuss his perspective regarding the need for smarter, more agile security solutions that not only detect and respond to threats, but also include the required forensics that allow organizations to adapt and fine-tune the security infrastructure when an unfortunate breach occurs. He will explore the options available for further leveraging core endpoint security technology to harness attacks before they permeate an IT infrastructure. Mr. Shtilman will discuss how using advanced endpoint security agents that collaborate bi-laterally (endpoint-to-network security solutions) regarding suspicious behavior offers key visibility and purposeful forensics that help catalog and adapt threat intelligence mechanisms to remediate and protect against threats.

Speaker: ***Leonid Shtilman****, CEO, Viewfinity*

1:15-2:15 pm

2014 Security Trends: Attacks Advance, Hiring Gets Harder, Skills Need Sharpening

Last year began with Advanced Targeted Attacks from China and ended with headlines of insider disclosure of sensitive NSA information and yet another "World's Largest" credit card breach. What will 2014-2016 bring? John Pescatore will present the results of SANS' studies on attack, vulnerability and security technology trends, along with the results of the SANS 2014 Security Salary Survey. Join the discussion and learn about the evolving trends and how to best deal with them when you get back to work.

Speaker: ***John Pescatore****, Director of Emerging Security Trends, SANS Institute*

2:15-2:55 pm

Building Awareness: A Guide to Establishing a Successful Information Security Education Program

This talk will explain the process of building the key support, funding, policy and staffing undertaken by Michigan Tech to develop, measure and maintain an effective campus-wide security awareness presence. It will cover the key steps of educating executives, selecting tools, staffing, categorizing and measuring risk, through implementation, support, and analytics with the goals of producing more secure behavior in our users and the ability to measure the success of the program.

Speaker: ***Dan deBeaubien****, Chief Technology Officer, Michigan Technological University*

2:55-3:15 pm

Your Security Awareness To-Do List

After hearing about the success of Dan and his team at Michigan Tech, you're probably fired up to kick your own security awareness program into high gear. Learn the top three things you can do right away to transform your users from vaguely aware to relentlessly security-focused.

Speaker: ***Lance Spitzner****, Training Director, SANS Securing The Human Program*

3:15-3:30 pm

Networking Break & Vendor Expo

3:30-4:15 pm

The Regulatory Landscape: How Changes Will Affect Your Security Program

This session will discuss how the changing legal/regulatory landscape will impact your company's security efforts, including:

- Federal data security legislation
- State legislation
- Foreign regulatory efforts
- NIST Framework
- Litigation in federal and state courts

The session will also address challenges in compliance, including how the security and legal teams can communicate better about cybersecurity risks and threats, to protect the company from cyber risks while also managing its litigation risks.

Speaker: ***Jason M. Weinstein****, Partner, Steptoe & Johnson, LLC*

4:15-5:00 pm

Improving Assurance Through Metrics: A Practical Case Study

Show up to a security presentation and walk away with a specific action plan. In this presentation, James Tarala, a senior instructor with the SANS Institute, and Jack Nichelson, the Global Information Security & Network Manager at GrafTech International, will be presenting on making specific plans for information assurance metrics in an organization. Clearly this is an industry buzzword at the moment when you listen to presentations on the Critical Security Controls, NIST guidance, or industry banter). Security professionals have to know that their executives are discussing the idea. So exactly how do you integrate information assurance metrics into action in an organization and actually achieve value from the effort. Learn what efforts are currently underway in the industry to create consensus metrics guides and what initial steps an organization can take to start measuring the effectiveness of their security program. Small steps are better than no steps, and by the end of this presentation, attendees will have a start integrating metrics into their information assurance program.

Speakers: ***Jack Nichelson****, Global Information Security & Network Manager, GrafTech Intl.*
James Tarala*, Senior Instructor, SANS Institute*

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

All Summit Sessions will be held in the Press Room (unless noted).

All approved presentations will be available online following the Summit at ***https://files.sans.org/securityleadership2014****. An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.*

Thursday, May 1

8:00-9:00 am

Registration

9:00-9:45 am

A Well-Oiled Machine: How Advance Auto Parts Integrates Security Across the Organization

Advance Auto Parts, the largest automotive aftermarket parts provider in North America, recently completed a massive acquisition. The company they acquired was privately held, and had not previously been subject to PCI compliance or any other security controls that have long been the standard at the publicly traded Advance Auto Parts (NYSE: AAP). Hear from their CISO as he discusses the challenges of integrating and securing legacy and acquired systems while keeping the business running at top speed.

Speaker: ***Joel Yonts****, CISO, Advance Auto Parts*

9:45-10:45 am

Taking Risks to Manage Risk:
Using Technology Portfolio Management to Design New Controls for Emerging Technologies

Chief Information Security Officers have evolved as information risk managers dealing with emerging technologies like social networks, mobile applications, analytics on vast amounts of data and cloud services. Aetna's CISO Jim Routh will share his perspective on the pressing need to take risks in order to more effectively manage risks using an approach of selecting specific emerging technology solutions to create new controls to use with emerging technologies.

Speaker: ***Jim Routh****, Chief Information Security Officer, Aetna*

10:45-11:00 am

Networking Break & Vendor Expo

11:00-11:45 am

Convincing Management to Increase Your Security Budget

Imagine if a business line manager went to the CEO and said "I need $1M to launch a new product. I can't tell you what good things will happen if we do, but really bad things will happen if we don't, though I can't tell you when the bad things will happen." Doesn't sound like a winning strategy, does it? Yet, that is what most CIOs and CEOs hear from security managers asking for budget increases. Come hear the founder of SANS, Alan Paller, describe real-world examples of how successful CISOs have convinced management to fund proactive steps to increase security. At the end of the session, you'll be armed with better tactics and evidence to convince management that new security initiatives will lead to concrete and meaningful benefits to the business and its customers.

Speaker: ***Alan Paller****, Director of Research, SANS Institute*

11:45 am-12:30 pm

IR Team Leadership in 2014: How to "Level Up" Your IR Team

Organizations' IR policies focus on the NIST IR PICERL process (PICERL – Preparation, Identification, Containment, Eradication, Recovery and Lessons learned). Most organizations tend to focus their IR teams on of C, E, or R and lightly touching on the others in their policy. As a result, the larger picture - the context they operate within – might not be fully explored. This presentation ties together all the elements into a complete narrative, walking the attendees through the entire incident response process. Attendees will develop a greater appreciation of their role as a leader, the role of their IR team, and their relationship with the larger organization. While leadership may think their team might consider their role is confined to some, but not all, of those phases. IR teams should be involved in all phases to a greater or lesser degree. And in doing so IR teams expand our own capabilities and contribute to the development of a stronger and more flexible team.

Speakers: ***David Kovar****, Manager, Ernst & Young*
Rob Lee*, Fellow, SANS Institute*

12:30-1:15 pm

Lunch

1:15-2:00 pm

Interview Smarter: Using Social Science to Hire the Right People

When interviewing, have you ever had trouble understanding a bullet point on a resume? Perhaps you are a manager and interviewing a highly skilled technical candidate? There are methods and techniques that you can use and have no technical understanding of the answer. This talk will discuss the use of a psychological phenomenon known as "cognitive load" in a practical application along with analysis of a real world interview. We will examine how to place a candidate under cognitive stress and some tips for analyzing the results.

Speaker: ***Richard Porter****, Certified Instructor, SANS Institute*

2:00-3:00 pm

Dynamic Enterprise Security Governance

In large, multi-state utilities, establishing a strategic security governance plan is essential in developing a single view of the enterprise security state that is protecting critical energy infrastructure assets, sensitive business information, and meeting multiple security and privacy mandates. A dynamic governance plan also helps establish firm command and control over defenses, personnel, costs, and threats and aids in protecting customer data and assuring shareholders that protections and risk management strategies are implemented. Join Christopher Peters as he outlines Entergy's strategic approach to enterprise security governance and the critical role it has played with supporting ICS security efforts.

Speakers: ***Chris Peters****, VP, NERC Compliance and Critical Infrastructure Protection, Entergy*
Tim Conway*, Technical Director of ICS & SCADA Programs, SANS Institute*

3:00-3:15 pm

Networking Break & Vendor Expo

3:15-4:15 pm

Aligning Your Defenses with Today's Evolving Threats

Defenders are in an arms race against hackers who are continuously evolving their attack vectors and methods to take advantage of our current weaknesses. Many have fallen into today's "Crown Mentality" trap, and due diligence has been reduced to simply doing what everyone else is doing. To get ahead, we need to gain an understanding of current threats and attack vectors, and realign our defenses accordingly. This presentation reviews some of the most current headline-grabbing attacks and discusses defenses to provide real risk mitigation.

Speaker: ***Paul Henry****, Senior Instructor, SANS Institute*

4:15-5:00 pm

What Every CISO Should Know: Lessons Learned from Financial Industry CISOs

The financial industry will always be the most attractive target for both cybercriminals and "helpful" legislators. Financial services firms also are usually among the first to try out new technologies, such as cloud, mobility, big data, etc, for financial gain. These factors have meant that CISOs in the financial vertical are usually the first to encounter and manage/mitigate new risks and new compliance demands. The panel of experienced CISOs will detail key lessons learned and answer your questions about the major coming challenges they see.

Moderator: ***John Pescatore****, Director of Emerging Security Trends, SANS Institute*

Panelists: ***Paul Davis****, CSO, ThreatGRID*
Mark Graff*, Chief Information Security Officer, Nasdaq OMX*
Nasrin Rezai*, SVP, Chief Technology Risk Officer. State Street Bank*

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.