Agenda

All Summit Sessions will be held in the Capitol Ballroom (unless noted).

All approved presentations will be available online following the Summit at ***https://files.sans.org/cyberdefense2014****.*
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Tuesday, August 19

9:00-9:05 am

Welcome & Opening Remarks

Dennis Scandrett*, Director - Cyber Defense, SANS Institute*

9:05-9:40 am

Prevent, Detect, Respond: A Framework for Effective Cyber Defense

Security is now a mainstay of boardroom discussions. However, many organizations remain frustrated and confused by what it takes to implement effective security. The number of breaches is increasing at an exponential rate, and it seems that the more organizations spend on security, the worse the problem gets. The fundamental problem is an organizational lack of a unified framework for building security solutions that work. In this engaging talk, Dr. Cole will outline the triple threat of security solutions that focus on what really matters: prevention, detection and response. Organizations must recognize that prevention is ideal, but some attacks will be successful, and effective security is built off of timely detection. However, detection without response has minimal value, so attendees will leave with a framework of metrics to evaluate effectiveness.

Dr. Eric Cole*, Fellow, SANS Institute*

9:40-10:25 am

Think Like the Bad Guys: Emerging Threats and How to Thwart Them

Todd McCall and Scott Augenbaum spend a lot of time with bad guys. They're in a unique position to tell you what the current threat landscape really looks like and the shape of the dark clouds on the horizon. Learn what law enforcement experts know about who's targeting your organization's systems, how, and why – and most importantly, how you can outsmart them.

Todd McCall*, Special Agent in Charge – Memphis Division, Federal Bureau of Investigation*
Scott Augenbaum*, Special Agent – Memphis Division, Federal Bureau of Investigation*

10:25-10:45 am

Networking Break & Vendor Expo

10:45-11:30 am

Taking Control: Using the Critical Security Controls as a Blueprint

With grim headlines about dramatic breaches becoming more of the rule than the exception, defending your cyber environment can feel like an impossible task. Many organizations have found success – and sanity – using the Critical Security Controls as a blueprint. Better news still – many of the benefits accrue from just four of the controls. Panelists share their results and lay out a plan that your organization can emulate.

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

Panelists: ***Dr. Eric Cole****, Fellow, SANS Institute*
Rick Doten*, CISO, DMI*
Jack Nichelson*, Global Information Security & Network Manager, GrafTech Intl.*

11:30 am-12:15 pm

OODA Security

If you can't prevent a breach entirely, then you need to be able to detect it as early as possible to reduce the resulting damage. IT baselining is one method that can give you an advantage over attackers, enabling earlier detection to mitigate the impact. This session will outline simple but powerfully effective techniques anyone can use.

***Kevin Fiscus**, Certified Instructor, SANS Institute and Founder, Cyber Defense Advisors*

12:15-1:15 pm

Lunch & Learn Presented by

Symantec™

The Integration Point for Cyber Security

The complexity and challenges of today's cyber security environment demand a coherent and unified security platform that carefully balances the awareness of internal and external risks. In this session, you will take a close look at how Symantec can help you achieve this perfect balance with a comprehensive, holistic approach to security that combines security best practices, security experience and security intelligence to build a robust security services platform for the cyber-aware enterprise.

***Efrain Ortiz**, Director - Market and Technology Innovation, Symantec Corporation*

1:15-2:00 pm

Accelerate Your SOC Deployment

As threats escalate, more organizations are finding the need to gain visibility into what is happening on their networks. This session discusses how to fast-track the stand-up of a Security Operations Center, including, people, process and technology.

***Holly Ridgeway**, Chief Information Security Officer, PNC Financial Services Group*

2:00-2:45 pm

Will The Real Next Generation Security Please Stand Up?

At Gartner in 2003, John Pescatore first published the phrase "Next Generation Firewall" to describe how the network security market needed to react to the Slammer/Blaster class of advanced attacks causing extensive damage back then. As punishment for that, he will moderate a panel of network security vendor experts to drill down into what today's "Next Generation" network security products really can and cannot do in detecting and mitigation today and tomorrow's advanced targeted attacks. The increased targeting, evasion and complexity of attacks, combined with increased business use of mobility and cloud-based IT has changed the game once again.

Come armed with questions and be prepared to join in a lively discussion on What Works in Network Security.

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

Panelists: ***Tom Hartig**, Security Engineer, Check Point Software Technologies*
***Justin Kallhoff**, CEO, Infogressive, Inc*
***Ryan Petersen**, Sales Engineer, FishNet Security*

2:45-3:05 pm

Networking Break & Vendor Expo

3:05-3:50 pm

Six Ways to Identify Targeted Attacks

Most organizations are drowning in alerts and threat information. How do you prioritize which alerts warrant your attention? This session will give real-life examples of techniques that advanced actors have used that would indicate a targeted attack. Learn what to look for when scanning alerts that signal that you are being targeted.

***Jason Rebholz**, Senior Consultant, Mandiant (A FireEye Company)*

3:50-4:30 pm

Developing Cyber Threat Intelligence

One of the issues facing many organizations is obtaining usable, accurate, timely, and tailored Cyber Threat Intelligence (CTI). CTI is required for organizations in order to maintain situational awareness on the internal and external threat environment that they operate in. Particularly problematic is that within the IT Security industry several services, while purported to be an advanced cyber threat intelligence source, use mostly open source intelligence with little value add analysis and intelligence built into the product by the vendor. This talk will discuss how to obtain CTI from a variety of open sources, including feeds from vendors, and creating your own enhanced by other sources with the appropriate people-process-technologies. As well, some of the issues and challenges faced within an organization attempting to develop a CTI capability for internal use or as a product offering will be discussed.

***Adrien de Beaupre**, Certified Instructor, SANS Institute*

4:30-5:15 pm

Incident Response: How to Fight Back

Highly public breaches at companies such as Target, Evernote and Living Social, which collectively compromised more than 200 million customer records, are pushing many organizations to develop in-house incident response (IR) capability to prevent these kinds of data breaches.

Incident response teams, typically operating under a formalized incident response plan, are designed to detect, investigate and remediate organizational assets in the event of a critical incident. SANS conducted a survey focused on the current state of incident response during May and June 2014, polling security professionals from over 19 industries and various sized companies and organizations. The goal of this survey was to get a clearer picture of what IR teams are up against today—the types of attacks they are seeing and what defenses they have in place to detect and respond to these threats. This presentation discusses the highlights of the survey results as well as some best practices in justifying a dedicated IR team and maturing in-house response capabilities.

***Alissa Torres**, Certified Instructor, SANS Institute*

5:15-6:00 pm

Antivirus is *NOT* Dead: Extending Infosec to Deal With Advanced Persistent Threats

Armchair quarterbacks that say antivirus is "dead" because it doesn't stop advanced persistent threats make two fundamental errors. First, they ignore traditional threats, and second they fail to adapt to deal with advanced persistent threats. Instead of ignoring the change of an evolving threat landscape, we must both continue to defend against traditional threats, and adapt to protect against advanced persistent threats.

This talk presents a framework drawn from communities that have dealt with both types of threats in a variety of different circumstances. Emphasizing the defensive and offensive components of detection and deterrence, this talk examines how to extend existing technologies to protect against advanced persistent threats, while not ignoring traditional threats.

***Michael Murr**, Certified Instructor, SANS Institute*

Thank you for attending the SANS Summit.

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.

Agenda

All Summit Sessions will be held in the Capitol Ballroom (unless noted).

*All approved presentations will be available online following the Summit at **https://files.sans.org/cyberdefense2014**.*
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Wednesday, August 20

9:00-9:45 am

Follow the Money: VC Investment Trends Predict the Future of Cyber Defense

Venture capital firms are shrewd observers of the cybersecurity landscape, backing the products and innovators they think are most likely to revolutionize the space. Veteran investor Peter Kuper will share his thoughts on the most promising emerging trends and areas of growth in cyber security based on where the money's flowing.

***Peter Kuper**, Partner, In-Q-Tel*

9:45-10:30 am

Continuous Monitoring and Real-World Analysis

Repeat after me: I WILL be breached. Most organizations realize this fact too late, usually after a third party informs them months after the initial compromise. Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match.

Modern threats require a paradigm shift in the way we perform analysis and monitoring. This talk will help you face the problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring.

***Seth Misenar**, Principal Instructor, SANS Institute*

10:30-11:00 am

Networking Break & Vendor Expo

11:00-11:45 am

Mind the Gap: Building a Bridge from Intrusion to Detection

So you convinced your organization to implement all the latest, greatest commercial tools for detecting advanced malware, and you trained your entire organization on behaviors to avoid. But there's a gap between the introduction of malware and the delivery of signatures by commercial security products. And attackers are getting smarter and smarter, with phishing techniques designed to fool even the most astute users. This talk will use real-world examples to discuss how you are being targeted and to demonstrate how to bridge the gaps using custom detection signatures.

***Bart Hopper**, Information Security Analyst, Volunteer Corporate Credit Union*

11:45 am – 12:30 pm

Cyber Exploits: Improving Defenses Against Penetration Attempts

Sometimes the best defense is a good offense. In this presentation, LBMC will provide a real-world view of how the company's security penetration testers break in to computer systems. The session will include case studies of actual successful attacks and will demonstrate how the target's defenses were inadequately designed, and what organizations really SHOULD be doing to protect themselves from external and internal compromise. Participants in this session will leave with a list of practical action items that can be completed to improve their defensive posture and reduce their organization's risk of attack.

***Mark Burnette**, Partner, LBMC Security & Risk Services*

12:30-1:30 pm

Lunch & Learn Presented By

Infogressive, a Fortinet platinum partner, will discuss next-generation firewall technology. Learn how Fortinet products can improve your organization's security and simplify your network for a fraction of the cost of other manufacturers.

***Justin Kallhoff**, CEO, Infogressive, Inc.*

1:30-2:15 pm

Security Awareness Metrics: Measuring Human Behavior

Security awareness is nothing more than another control designed to reduce risk, specifically human risk. This session will discuss the different ways organizations are effectively measuring human risk, which methods are proving to be the most successful, and steps you can take to have successful metrics for your awareness program.

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

2:15-3:00 pm

Delivering Security From The Cloud: Turning a Risk into a Weapon

Every time IT begins to use new technologies to deliver business services, security inevitably ends up having to use those same methods to deliver security controls. This will be true with business use of Software/Platform and Infrastructure as a Service cloud offerings, just as it proved true with the PC, client/server, web services and mobile technology waves. For example, Gartner has predicted that by 2016 more than 25% of enterprises will be using cloud-based delivery of web security controls. In this session John Pescatore will take a What Works look at how cloud-based security services are already being used by large and small enterprises to secure use of mobile devices and SaaS/IaaS use. He will also provide a forecast of trends in these areas, and detailed case studies and decision frameworks for taking advantage of cloud-based delivery of security controls and services.

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

3:00-3:20 pm

Networking Break & Vendor Expo

3:20-4:15 pm

SIEM Evolution: Threat Intelligence, Big Data, Application Monitoring

Despite some media noise to the contrary, SIEM is a pivotal technology that provides security visibility today and it is likely to hold the same role for the next two to three years. SIEM operations can be significantly improved with the use of threat intelligence, all the while the technology evolves towards more use of big data-inspired approaches and covers more applications and use cases.

***Dr. Anton Chuvakin**, Research VP - Security and Risk Management, Gartner*

4:15-5:00 pm

Back to Basics: Five Steps to a Secure Future

Cyber security is not that difficult – IF organizations take the time to lay a secure foundation before building out a security program. Without the proper fundamentals in place, all the security in the world will have minimal value in protecting an organization. The core foundations needed for success are 1) asset inventory; 2) configuration management; and 3) change control. Most breaches that have occurred are caused by organizations overlooking these core areas. In this talk, Dr. Cole will outline the 5 steps to a secure future. Students will walk away with an actionable blueprint for protecting their organizations.

***Dr. Eric Cole**, Fellow, SANS Institute*

Thank you for attending the SANS Summit.

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.

EXHIBITORS

Check Point Software Technologies Ltd. (www.checkpoint.com), the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization.

FireEye® has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection against the next generation of cyber attacks. The FireEye platform provides real-time, dynamic threat protection without the use of signatures to protect across the primary threat vectors, including web, email, and files.

Founded in 2006, **Infogressive** is a managed security services company focused on reducing risk by building defense-in-depth networks and implementing best practices. We accomplish those goals by combining our exceptional technical talent with industry leading technologies. Please visit www.infogressive.com or e-mail sales@infogressive.com for more information.

LBMC Security & Risk Services is a national leader in healthcare IT security, healthcare compliance/consulting, and managed security services (MSS). We have helped guide federal healthcare security requirements and are respected experts to government agencies and healthcare industry groups. As a result, we understand at a deep level how to implement and maintain compliance with complex healthcare IT security frameworks in healthcare organizations and other industries with strict privacy and security requirements.

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.