Agenda

All Summit Sessions will be held in the Parthenon Ballroom on the 2nd floor, BL level (unless noted).

Summit presentations will be posted via the following URL, ***https://cyber-defense.sans.org/resources/summit-archives,*** *typically within five business days of the Summit. An email will be sent to all attendees once live.*

Portions of the Summit may be video-recorded. These videos may be used for marketing or other purposes, but will not be available for distribution or viewing on demand at this time.

Tuesday, August 11

8:00 - 9:00am

Registration & Coffee

Breakfast Pastries Provided

(LOCATION: PARTHENON BALLROOM FOYER)

9:00 - 9:45am

The Current Reality: Defending a Compromised Network

Dr. Eric Cole*, Fellow, SANS Institute*

Designing and securing a network is very complex. With detailed requirements to support all of the latest devices, mobile computing, cloud services and the portability requirements of data, current networks are very porous, very difficult to secure and very compromised. When people hear about networks being compromised, they should not be surprised. Networks directly connected to the Internet are compromised and should be the new baseline for designing and building out security. The question that has to be answered is how to implement security based on the assumption that security is more than just setting up and protecting perimeters. In this talk, Dr. Cole will share real life examples of security solutions that work to protect current environments that might be already compromised. Attendees will learn how to drive this new thought process into decision makers and solutions covering data protection, network design and network monitoring.

9:45 - 10:30 am

Insider Threat Detection: Identifying Your Vulnerabilities Before the Bad Guys Can

Roccie Soscia*, Deputy to Director of Counterintelligence, Lockheed Martin*

As a global security, aerospace, and information technology company, focused on national security, Lockheed Martin takes an aggressive and proactive stance to ensure the safety of its 113,000 employees and integrity of its information and products. Physical and information security have long been major contributors in Lockheed Martin's ability to accomplish its broad mission. To ensure a security posture fully responsive to evolving threats, Lockheed Martin established the Counterintelligence Operations and Corporate Investigations (CO/CI) in 2011 to proactively and comprehensively identify and mitigate risks associated with theft of Lockheed Martin's intellectual property and trade secrets. In 2013, CO/CI launched an Insider Threat Detection Program that looks for indicators identifying employees at a higher risk of being targeted by foreign intelligence services. Join Roccie Soscia to learn about this program and the significant upside it's creating.

10:30 - 11:00am

Networking Break and Vendor Expo

(LOCATION: PARTHENON BALLROOM FOYER)

11:00 - 11:45am

How Not to Fail at Cyber Defense

***Mark Burnette**, CPA, CISA, CISSP, CISM, CGEIT, QSA, Partner, LBMC Security & Risk Services*

Whether we want to admit it or not, many organizations' security programs are failing despite the best efforts of security champions. In this talk, Mark will provide analysis on why so many programs are failing, and provide a list of "Do's and Don'ts" to help you ensure that your security program doesn't suffer the same fate. Attendees will leave this talk with a clear action plan for implementing a successful Cyber Defense program and avoiding the pitfalls that have hampered many security programs. Without a strong strategic approach to cyber defense (which will be provided in this talk), tactical efforts will not have the intended impact on risk reduction.

11:45am - 12:15pm

Surprisingly Successful: What Really Works in Cyber Defense

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

Every day, headlines trumpet the latest "largest breach ever." But rarely do we hear about the companies that avoided breaches and the security processes, controls and technologies that worked to either prevent incidents or to quickly detect and minimize damage. There are actually a lot of success stories out there, where skilled security professionals increased the effectiveness and/or the efficiency of their security programs. This talk will highlight several real-world, "what worked" case studies and identify the common success factors. Each case study includes measurable results and metrics across areas such as detecting advanced targeted threats, reducing the cost of vulnerability scanning while increasing the reach, reducing application vulnerabilities and other areas.

12:15 - 1:30pm

Lunch & Learn

presented by

THREATSTREAM®

Social Threat Intelligence (STI)

***Trevor Welsh**, Principal Security Strategist, ThreatStream*

Social has changed many aspects of information security. Fascinatingly, enterprise has been slow to embrace community sourcing security intelligence. Trevor Welsh of ThreatStream will present on Social Threat Intelligence (STI). This talk will detail how STI exists today, and how it might exist tomorrow. Trevor will also detail how enterprise can best take advantage of STI in a sensible, secure way.

1:30 - 2:15pm

Adaptive Monitoring and Detection for Today's Landscape

***Jamie Murdock**, CISO, Binary Defense Systems*

Current monitoring and detection programs have become stale and outdated. It takes more than a SIEM and an incident response plan that hasn't been reviewed in years. Although it is impossible to say that a company can't get breached, it is possible to detect and respond to attacks. This talk will focus on the importance of a good monitoring and detection program that can adapt quickly to an ever-changing threat landscape by utilizing penetration testing, threat intelligence, and incorporating this all into a responsive incident response plan.

2:15 - 3:00pm

Views from the Incident Response Trenches

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

What breed of cyber warrior stands between your network's data and the hands of the attacker? The incident responder works under the constant pressure of an impossible mission: to detect critical incidents before the organization suffers significant loss and to return "faster-than-yesterday" business operations to full functionality. SANS surveyed this "tempered-by-fire" community of professionals to pinpoint what works now, where improvements are needed and what challenges currently face IR within organizations today. The increasing sophistication and prevalence of attacks seen by IR teams may surprise you. Join us to gain insight from the 2015 SANS IR Survey into life in the IR trenches.

3:00 - 3:30pm

Networking Break and Vendor Expo

(LOCATION: PARTHENON BALLROOM FOYER)

3:30 - 4:15pm

Game Changer: Identifying and Defending Against Data Exfiltration Attempts

***Ismael Valenzuela** – Lead, Foundstone IR/Forensics; Technical Practice Manager, Intel Security & Community SANS Instructor*

Accept that you are getting compromised, because that's the only truth. Now, you are ready to change the definition of winning, and it's not about preventing compromise anymore. Your new objective is to prevent attacker's success. And you win every time you prevent the attackers from accomplishing their goal, which, in most cases, involves data exfiltration. In this talk, Ismael Valenzuela will provide a better understanding of how you can redefine the game and start winning by exploring the following questions: how do attackers exfiltrate data? And more importantly, how can you identify and defend against those techniques?

4:15 - 5:30pm

The Cyber Defense program at SANS Institute is on a mission to find the 2015 Ultimate Cyber Defender. This engaging and exciting challenge will allow participants to compete via online at the Cyber Defense Summit, and at other regional training events. The Challenge pits security professionals against each other by asking them to answer a series of cybersecurity questions that every cyber defender should know. Everyone who participates in the Ultimate Cyber Defender Challenge has the potential of winning, but only one Ultimate Cyber Defender will emerge from a group of contestants from the online, Summit and regional events. Successful contestants from the online, Summit and regional competitions will win an all-expenses-paid trip to San Diego to participate in the finals. The final "battle royale" will take place in San Diego (Oct 23) and will be similar to the regional events, but much more difficult.

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.

Wednesday, August 12

8:00 - 9:00am

Registration & Coffee

Breakfast Pastries Provided

(LOCATION: PARTHENON BALLROOM FOYER)

9:00 - 9:45am

Hope You Never See These Guys Again: Lessons Learned from the FBI Cyber Task Force

***Scott Augenbaum**, Supervisory Special Agent, Federal Bureau of Investigation*
***Victor Rodriguez**, Special Agent – Cyber Task Force, Federal Bureau of Investigation*

It's a really bad day when Special Agents Scott Augenbaum and Victor Rodriguez of the Federal Bureau of Investigation's Cyber Task Force show up at your organization and inform you that the crown jewels of your organization (money, intellectual property, PHI or PII) are gone forever. Scott and Victor have been working together for close to nine years, and they have seen threats morph and severely impact numerous organizations. In this talk, they will take the lessons they have learned from hundreds of data breaches and acts of Cyber Crime and provide you with what they have learned so you can best protect your organization's infrastructure. They'll offer a number of common technical, managerial and incident response mistakes that could have saved a number of organizations from becoming victimized. They have one goal, and that's to keep you from having the answer the next door they knock on.

9:45 - 10:30am

Business Email Compromise: The Next Billion Dollar Problem

***Donald "Mac" McCarthy**, MyNetWatchman*

New social engineering techniques driven by business email compromise are costing businesses hundreds of millions of dollars per year. Every business is a target and attack success rates are alarmingly high. These techniques are undetected by antivirus, firewalls, IDS sensors and the latest advancements in email security (SPF, DKIM). It's essential that organizations adopt the proper business procedures to validate the authenticity of any email communications used to initiate financial transactions in order to avoid becoming the next victim. Attendees will leave this talk with a better understanding of the threat and strategies to defend against it.

10:30 - 11:00am

Networking Break and Vendor Expo

(LOCATION: PARTHENON BALLROOM FOYER)

11:00 - 11:45am

Continuous Ownage: Why You Need Continuous Monitoring

***Eric Conrad**, Senior Instructor, SANS Institute*

Repeat after me: "I will be breached." Most organizations realize this fact too late, usually when 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 even months. The attacks are continuous, and the monitoring must match. This talk will help you face this problem and describe how to move your organization to a more defensible security architecture that enables continuous security monitoring.

11:45am - 12:15pm

Offense Must Inform Defense: Why Proper Incident Response is SO Important!

Jonathan Ham, Certified Instructor, SANS Institute

Despite your best defensive efforts, you've been breached, because there was something you missed. That happens. Maybe it was a patch you didn't get applied yet. Maybe it was a 0-day. Maybe your network architecture wasn't quite right. But what is most important now is to learn from the mistake. You need to understand how and why the breach occurred, so you can make sure it doesn't happen again. Come find out how to run an incident to ground!

12:15 - 1:30pm

Lunch & Learn

presented by

Prevent - Detect – Respond

***Derrick Masters**, Security Analyst, A+ Network+ FCNSA GSEC, Infogressive*

We all want to prevent 100% of attacks, but most SANS attendees know that isn't realistic given today's threat landscape. We will discuss technologies and services that increase prevention rates, help with detection when your defenses fail, and how we respond when it really hits the fan.

1:30 - 2:15pm

The Power of the Human Shield in Cyber Defense

***David Cawley**, Senior Manager, Information Security, Intuit*
***Rinki Sethi**, Director – Information Security, Intuit*

Our product development teams, employees and customers are often the first line of defense to keep an organization secure and must be armed with relevant security skills. Enlisting these groups is a must in helping to prevent or respond to security incidents in an ever-advancing threat landscape. There are new and innovative ways to educate and enable both your employees and customers to prevent incidents including collaboration and gamification. Rinki Sethi and David Cawley will discuss the journey at Intuit to rally the organization into battle.

2:15 - 3:00pm

Active Defense: Gaining Visibility Into Your Network

***Robert M. Lee**, Co-Founder, Dragos Security*

Active defense is the process of monitoring for, responding to, and learning from threats. It is not about hack-back, it is simply taking an active approach to defense. The key to being able to implement an active defense is building on the proper foundations of security, including the proper architecture and maintenance of the network as well as the appropriate use of passive defenses such as firewalls and anti-malware systems. This talk will present a framework to discuss the activities that contribute to cybersecurity and a strategy for an active defense. It will focus on a key step that contributes to security within a network: asset identification. Understanding the assets, the network itself, and being able to establish baselines of normal activity are all critical components of security. With a good understanding of the network itself and through gaining true network situational awareness, it is possible to implement the style of defense that is required for countering advanced threats.

3:00 - 3:20pm

Networking Break and Vendor Expo

(LOCATION: PARTHENON BALLROOM FOYER)

3:20 - 4:05pm

Top 10 Dashboards

***Craig L. Bowser**, Sr. Security Engineer, Dept. of Energy*

Dashboards are a critical capability of a Security Information Event Monitor (SIEM), as they are able to display the near real time status of the health, operational availability, security posture and compliance level of networks of all sizes. While there are numerous papers, blog posts and examples of dashboards that provide deep insights, specific security alerts or complicated compliance metrics for your network, I wanted to create a list of dashboards that provided a solid starting point for Security Operation Centers to use when they installed their first SIEM. These are suggested quick-win, industry-agnostic dashboards, which were chosen because of their ease of implementation and simple graphical presentation that provide SOC personnel an initial view into the security posture of a network.

4:05 - 4:50pm

Building Out a SOC

***Randy Marchany**, CISO, Virginia Tech*

This talk discusses the components that need to be in place to build a SOC. Some of the components include your Continuous Monitoring, sensitive data protection, and policy structure. This talk shows examples of how these components can be built using existing information and tools within your organization.

4:50 - 5:00pm

Closing Remarks

***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.