HOUSTON, TX

SUMMIT: NOV 14-15

SANS Healthcare CYBERSECURITY SUMMIT

Program Guide

@SANSInstitute #SANSHealthcare

Welcome to the SANS Healthcare Cybersecurity Summit! These are challenging times in healthcare information security, but we are here with a team of technical experts to provide you the tools and information to improve your organization's information security. Over the next two days, we will have in-depth talks form top incident responders and forensics experts as well cutting edge research in application whitelisting and malware detection. We want you to take the skills and knowledge you obtain at this Summit to better secure your organization.

James Tarala

Take this opportunity to introduce yourself to those sitting around you, join one of the many conversations during breaks, engage with our expert speakers during our many networking breaks, ask questions during Q&A sessions, and weigh in on Twitter #SANSHealthcareSummit and @ SANSInstitute.

Looking forward to a great Summit!

Sincerely,

James Tarala,
Healthcare Cybersecurity Summit Chair

Agenda

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

All approved presentations will be available online following the Summit at
https://files.sans.org/summit/healthcare2016
An e-mail will be sent out as soon as the presentations are posted, typically within five business days of the event.

Monday, November 14 – Protecting Healthcare Data

8:00-9:00am **Registration & Coffee** (LOCATION: LEGENDS PRE-FUNCTION AREA)

9:00-9:45am

Healthcare in the Cyber Bullseye:
How to Gain Top Management Support for Your Programs

30 months ago, the FBI issued one of its rare "Private Industry Notifications" (PIN) for CEOs in hospitals, health insurance and other health care organizations. It said "increased cyber intrusions into health care organizations is likely" because the "healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors." Intrusions did increase and defenses continue to be insufficient to meet the risk of cyber attacks. You already know that improvements are needed, and in many cases you know what needs to be done. But how do you get top management to support your programs? This fast-paced briefing shows the key errors CISOs make when briefing boards of directors and top managers, and provides real-world examples of what works in and keeping top management aware and engaged so they will support your new initiatives.

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

9:45-10:30am

Making Best Practice Common Practice in the Healthcare Industry

The slogan for the Center for Internet Security,"Making Best Practice Common Practice," came from an observation. The vast majority of cyber problems that plague us today could have been prevented by actions, technologies and policies that are already known or already exist in the marketplace. The challenge is that you can't find those "best practices" on your own to learn from them. Or even more likely, you are overwhelmed by the "fog of more" – competing expert opinions, vendor claims, and regulatory or compliance requirements.

Through the lens of a 35-year career at the National Security Agency, and now with the non-profit Center for Internet Security,Tony will share his observations about the threats that we all face; the ways that we can identify, share, and sustain best practices to manage risk; how these best practices apply to the healthcare industry; and the new models of open, collaborative action that will be required for success.

***Tony Sager**, Senior VP & Chief Evangelist, Center for Internet Security*

10:30-11:00am **Networking Break and Vendor Expo** (LOCATION: LEGENDS V & VI)

Monday, November 14 – Protecting Healthcare Data

11:00-11:45am Solutions Session

(LOCATION: LEGENDS I)

presented by

cybereason

Hacking the Hacking Team

Do you wonder what a hack looks like from the hacker's perspective? Now you can find out. Join our session for an in-depth look at the tools, techniques and procedures that were used to hack the Hacking Team. You'll learn how the attackers deployed an APT against the organization, why hackers are increasingly using these threats against enterprises and how companies can best detect these complex threats.

***Richard Harlan**, Solutions Engineer*

(LOCATION: LEGENDS II)

presented by

SPIRION™

Can Data Classification Improve Data Security?

Discussion of findings from a comparative study recently published by Poneman on the "Business Impact of Business Security on US Companies" focused on the interrelationship between InfoSec Data Classification best practices and post-breach costs incurred by organizations. Anybody who is responsible for data security, privacy or data governance should attend.

***Gabriel Gumbs**, VP of Product Strategy, Spirion*

11:45am-12:30pm *Cyber-Hygiene and Standards of Care: Practical Defenses for Healthcare*

There is no question that healthcare organizations are struggling to stop attacks. The healthcare industry has been regulated by cybersecurity standards and laws since 2001, yet today they seem to be the one vertical industry regressing, rather than making progress defending their information systems.

In February of 2016, the California Attorney General, Kamala Harris recommended that "the 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

In this presentation James Tarala, contributor to the CIS Critical Security Controls, will discuss standards of cyber security care for healthcare organizations and why the CIS Critical Security Controls are quickly becoming the standard of cyber security care for all US healthcare organizations. He will also share practical tips for implementing these controls in a healthcare setting and overcoming the barriers to implementation. Attendees should expect to leave the presentation with practical advice for using these controls to stop even the most advanced attacks in their organization.

***James Tarala**, Principal, Enclave Security; Senior Instructor, SANS Institute*

12:30-1:30pm Networking Luncheon and Vendor Expo (LOCATION: LEGENDS V & VI)

Monday, November 14 – Protecting Healthcare Data

1:30-2:15pm	***Security Awareness: Understanding and Managing Your Top Three Human Risks*** The key to managing your human risk is first identifying and then prioritizing your risk factors. After working with hundreds of organizations, Lance Spitzner will discuss the three most common human risks he finds in organizations, and what you can do to effectively manage and measure them. Key points you will learn include: the concept of "cognitive overload" and how every behavior has a cost; the key elements in a human risk analysis; how to determine the behaviors that will mitigate your top human risks; and how to effectively communicate and measure those behaviors. ***Lance Spitzner****, Director, SANS Securing the Human*
2:15-3:00pm	***Whitelisting: It's Just Good Medicine*** Cybercrime. Hacktivism. Nation-states. Lucrative ransomware. In addition to caring for and restoring human life, the healthcare industry continues to find itself on the front lines of cyberattack. The stakes are real and require effective prevention strategies to stay out of the headlines. McElroy demonstrates how whitelisting is a true prevention strategy through use cases on application whitelisting relevant to healthcare. He'll share best practices and strategies for implementation. Come learn how utilizing better preventative medicine maintains the long-term health of your systems. ***Rick McElroy****, Security Strategist, Carbon Black*
3:00-3:30pm	**Networking Break and Vendor Expo** (LOCATION: LEGENDS V & VI)
3:30-3:45pm	***Healthcare Provider Breaches and Risk Management Road Maps: Results of the SANS Survey on Information Security Practices in the Healthcare Industry*** The number of attack surfaces continues to rise as the use of mobile medical- and health-related apps grows and as electronic health records (EHR) become ever more embedded in clinical settings. As this survey shows, many attacks stem from insiders with access, whether through simple negligence, malicious intent or just plain curiosity. James will highlight key findings of the survey, so you can boost your immunity to breaches. ***James Tarala****, Principal, Enclave Security; Senior Instructor, SANS Institute*

Monday, November 14 – Protecting Healthcare Data

3:45-4:30pm

Ransomware in Healthcare: Attack Vectors and Prevention Tips

The business model behind crimeware has changed. Cyber attackers are turning to ransomware due to advances in attack distribution, anonymous payments, and the ability to reliably encrypt and decrypt data. Ransomware incidents impact the quality of care that clinical facilities can provide, costs money in remediation efforts, and hurts their reputation as competent providers of care.

In this session, Matt Mellen, a former Information Security Lead at a hospital network in California, will discuss strategies healthcare organizations can take to stop ransomware. Drawing from his first-hand experience responding to ransomware, combined with the latest developments in cyberattack prevention at Palo Alto Networks, Matt will explain how ransomware is penetrating healthcare organizations, along with practical steps you can take to prevent exposure to this type of cyberattack.

Matt Mellen*, Security Architect – Healthcare, Palo Alto Networks*

4:30-5:15pm

Prediction 2017: "I Survived a Ransomware Attack in my Cloud!"

Just as other malware has graduated from endpoints to bigger targets, ransomware attacks increasingly threaten sensitive and valuable assets beyond desktops: server, data center, and cloud resources. Ismael Valenzuela, Head of Intel Security's Foundstone Incident Response team, GSE and SANS Instructor, will discuss ransomware lessons learned in different industries and how to pre-empt, contain, and mitigate these evolving invasions.

Ismael Valenzuela*, Head of Intel Security's Foundstone Incident Response team, GSE and SANS Instructor*

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.

Tuesday, November 15 – Detecting and Responding to Healthcare Breaches

8:00-9:00am	**Registration & Coffee** (LOCATION: LEGENDS PRE-FUNCTION AREA)
9:00-9:45am	***FBI Perspective: Cyber Threats to the U.S. Healthcare and Public Health Sector*** Cybersecurity professionals in the public health sector are facing growing threats as social hacktivism, financial fraud, and ransomware adversaries plot to disrupt the brand, patient privacy, and even lifesaving technology. FBI Executive, Jon Ford, will discuss emerging threats, risk assessment, and incident response to the evolving cyber security landscape. Attendees will learn the FBI perspective on cyber threats to the U.S. healthcare and public health sectors. ***Jon Ford****, Principal to NSA and U.S. Cybercommand, Federal Bureau of Investigation*
9:45-10:30am	***Break in Case of Emergency: Lessons from Healthcare Investigations*** Recent intrusions affecting healthcare companies by targeted actors necessitates an understanding of how preventative and detective controls can be leveraged to more quickly contain and eradicate threats. Using lessons learned from a recent investigation, Kerr will present a case study that outlines some of the challenges faced by modern healthcare organizations, the role of incident response expertise and methodologies, and explains some of the most important controls that can effectively prevent or more quickly identify threats within an environment. ***Devon Kerr****, Manager – Incident Response, MANDIANT, A FireEye Company*
10:30-11:00am	**Networking Break and Vendor Expo** (LOCATION: LEGENDS V & VI)
11:00-11:45am	***Healthcare Incident Response: The Five Stages of Loss and Grief*** Are you prepared to cope with healthcare data loss? Many of us have suffered a breach or loss of data, or know someone who has. Data loss and HIPAA breaches affect us all differently. It's not a matter of if but when you will suffer from a loss of data. Join Brandon as he helps develop strong coping skills and practical ways to lessen the pain of data loss in a healthcare environment by comparing the five stages of loss and grief to real-world healthcare incident response scenarios. ***Brandon McCrillis****, Senior Information Security Consultant, Rendition InfoSec*

Tuesday, November 15 – Detecting and Responding to Healthcare Breaches

11:45am-12:15pm

2016 Application Whitelisting vs. Anti-Malware Survey Results: A Panel Discussion with Leading Experts

For years, organizations have implemented traditional anti-malware as their core defense at the endpoint. Although most organizations indicate that more than 95% of their endpoints are running some form of anti-malware software, breaches are still occurring at these same organizations. More organizations are considering application whitelisting software as an alternative to traditional anti-malware software. Interestingly, many organizations are reporting that after implementing application whitelisting, the usefulness and need for anti-malware is declining. This, along with other pertinent findings from a recent application whitelisting survey, will be discussed. The panelists will also offer practical suggestions for choosing endpoint defenses, promoting user acceptance of application whitelisting, and project implementation do's and don'ts.

MODERATOR: ***James Tarala**, Principal, Enclave Security; Senior Instructor, SANS Institute*

PANELISTS: ***Mike Haag**, Director – Advanced Threat Detection & Research, Red Canary*
***Rick McElroy**, Security Strategist, Carbon Black*
***Kelli Tarala**, Principal, Enclave Security*

12:15-1:30pm Lunch & Learns

(LOCATION: LEGENDS I)

presented by

SailPoint

Unstructured Data within the Cyber Kill Chain

Join us as we take a look at how cyber criminals are leveraging unstructured data environments as one of their primary exploits to gain access to your most sensitive information. We will also discuss how you can address this problem and close out this extremely open security flaw.

***Bryan Whorton**, Sales Executive, Sailpoint*

1:30-2:15pm

How You Stack Up: Examining the Security Landscape of Three Hospitals

Every organization takes a different approach to information security, always wondering if their efforts are considered "enough." While there are no definitive answers, understanding the strategies your peers are using and the resulting degree of success can always help. In this session, Haag walks you through the security postures of three hospitals ranging in size from a small regional hospital to a 550-bed health facility. You will learn about the solutions and processes they have relied on to secure their own organizations, and how those investments have performed to date.

***Mike Haag**, Director – Advanced Threat Detection & Research, Red Canary*

Tuesday, November 15 – Detecting and Responding to Healthcare Breaches	
2:15-3:00pm	***EHR Vulnerability Reporting – A Cause for Concern?*** In 2015, 84% of all U.S. hospitals were utilizing a basic electronic health records (EHR) system, as government incentives meant to drive EHR adoption and their use have generally been successful. Yet, the very systems designed to store, process, transmit, and maintain electronic protected health information (ePHI), while shepherding in a promising new era of accessibility and the sharing of medical data, are also providing additional opportunities for theft and fraud. In this presentation, Greg Porter of Allegheny Digital will discuss the current state of EHR security vulnerability reporting, the use of "Certified Health IT Products," and noteworthy testing observations. He will conclude by providing attendees with practical considerations for developing an EHR-focused assessment program to identify and monitor software and configuration-based weaknesses. ***Greg Porter****, Founder, Allegheny Digital; Instructor, SANS Institute*
3:00-3:20pm	**Networking Break and Vendor Expo** (LOCATION: LEGENDS V & VI)
3:20-4:05pm	***How to Determine the Significance of a Security Incident*** Security incidents are common. But only a few of them constitute "data breaches" or other significant compromises of security. These panel members will share the wisdom they have gained by evaluating incidents in healthcare and other industries. ***Meredith Harper****, Chief Information Privacy & Security Officer, Henry Ford Health System* ***Rick Kam****, President/Co-Founder, ID Experts* ***Erika Riethmiller****, Director, Corporate Privacy-Incident Program, Anthem, Inc.*
4:05-4:50pm	***Security and Privacy: Birds of a Feather, or Different Species?*** This session will look at the ways in which privacy and security are parts of the same puzzle of compliance and overall confidentiality. Some would argue that they are siblings, others that they are at best distant cousins. This session will shed some light on how each process area has developed and how, since both functions are somewhat young, they share many of the same growing pains. At the same time, the way in which each is perceived within the corporate structure can be very different, and we will discuss that and its effect on the particular program. We will look at reporting relationships, discuss where the most effective programs reside, and understand the key elements that make these two functions equal, but perhaps different. This will be an interactive session with the audience answering some of their own questions, and the speaker presenting challenges and theories for consideration. ***Mark Williams****, Principal Systems Security Officer, Blue Cross Blue Shield of Tennessee*
4:50-5:00pm	***Closing Remarks, Plan of Action and Next Steps*** ***James Tarala****, Principal, Enclave Security; Senior 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.

@SANSInstitute **#SANSHealthcare**