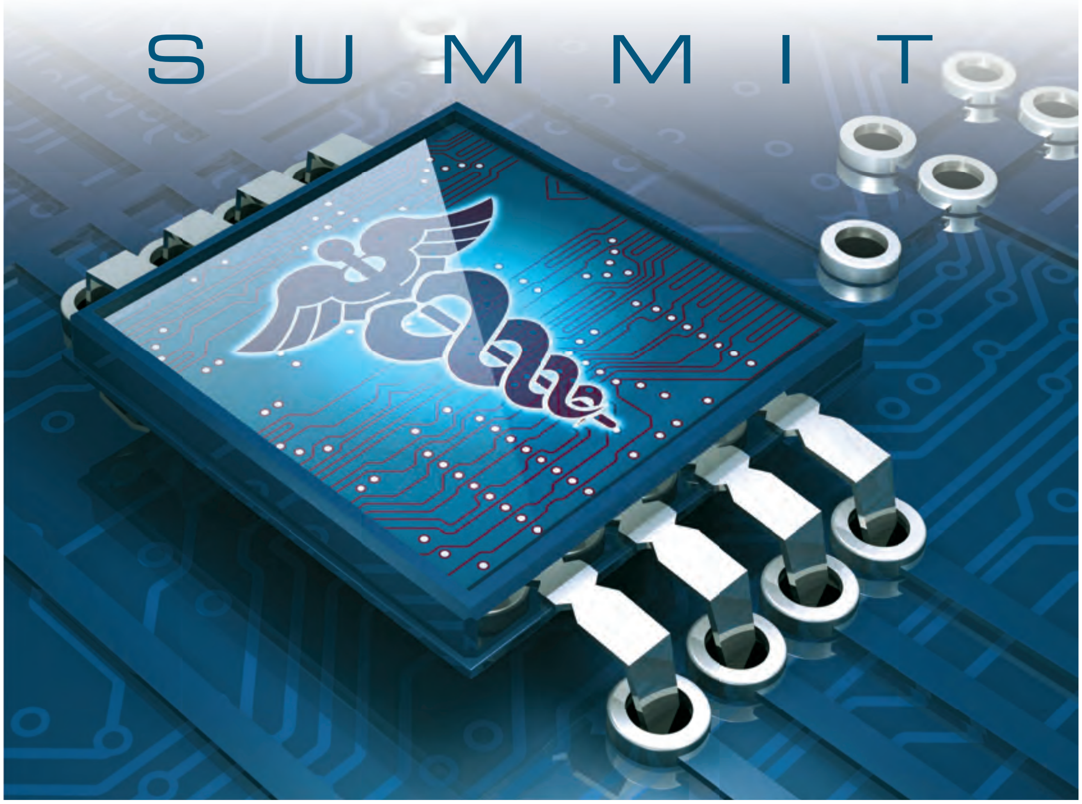
SANS

Healthcare CYBER SECURITY SUMMIT



Program Guide

Agenda

All Summit Sessions will be held in CA Thayer Ballroom (unless noted).

*All approved presentations will be available online following the Summit at **https://files.sans.org/summits/healthcare13**.*
You will receive an e-mail within approximately one week of the summit once presentations are posted.

Wednesday, October 23

8:00 - 9:00 am

Registration

9:00 - 9:45 am

Keynote Address
Disrupting Healthcare Organizations: New Data Customers, New Data Workflows

Medicine is the most knowledge-intensive industry facing the Big Data transformation. Change will require the engagement of a wide range of front-line doctors, nurses, pharmacists, and other clinical experts. In her work as a research scientist at Kaiser Permanente, Dr. Herrinton strives to increase the accessibility of medical data needed for quality improvement so that clinical stakeholders are empowered to prioritize data requests and act on data. She developed a crowd-sourcing platform toward this end, for which she received the prestigious Innovation Award from Kaiser Permanent Information Technology.

Medical care delivery and public health surveillance are also being transformed by changes brought by the Affordable Care Act, the electronic health record, mobility, and social media. Key trends include (1) the aging of the population; (2) the integration of public health with medicine; (3) the ubiquity of process measurement in care delivery; (4) the exchange of health data across institutions; (5) empowerment of patients and caregivers to act as members of the care team; (6) shifting of care out of medical facilities and into the home; (7) the creation of the Patient-Centered Medical Home; (8) shifting in payments from volume-based to quality-based; (9) shifting of insurance markets and competition; and (10) genomics and personalized medicine. Dr. Herrinton will discuss these trends in relation to the creation of new data customers and new data workflows.

Speaker: ***Lisa Herrinton, PhD****, Senior Research Scientist, Kaiser Permanente*

9:45 - 10:15 am

Results of the Inaugural SANS Health Care Security Survey

Is the industry ready, willing, and able to respond to the brave new world of electronic health care? Can health care as a whole keep up with advancing cyber threats? The first annual Health Care Security Survey will provide insight into your peers' security priorities, their biggest concerns about using cloud and mobile solutions, top industry security threats, and more. Be among the first to hear the results of this survey, and find out where your organization stands relative to the rest of the industry – and your competitors.

Speaker: ***Frank Kim****, Director, Kaiser Permanente*
Barbara Filkins*, Senior Analyst, SANS Institute*

10:15 - 10:35 am

Networking Break

10:35 - 11:05 am

Understanding Medical Device Vulnerabilities: A Case Study

Speaker: ***Billy Rios****,Technical Director, Cylance*

11:05 am - Noon

Emerging Health Care Security Threats

In 2012, the ten largest security incidents alone exposed over 1.8M patient records. Cybercriminals found that the information in medical information and billing systems was just as valuable as that in financial systems for use in identity theft and account fraud. This trend has accelerated in 2013 and we have also seen attacks against medical and pharmaceutical research systems looking to steal intellectual property as well as demonstrations of denial of service attacks against medical implants.

This panel will discuss the future of attacks against healthcare systems and networks, against the backdrop of both new threat trends and also new technology trends in healthcare IT, such as mobility, BYOD, use of cloud-based systems, etc. The panel will provide the perspective of both security managers in healthcare and national law enforcement.

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

Speakers: ***Special Agent Kristen McLeran****, Federal Bureau of Investigation*
Greg Porter*, CISSP, CISM, GCIH, Allegheny Digital*
Joseph Say*, Solutions Architect, Greater Houston Healthconnect*

Noon - 1:15 pm

Lunch On Own

1:15 - 2:00 pm

Medical Identity Theft: Response Considerations

The theft of protected health information shows no signs of slowing, as stolen medical identities are being used daily to engage in outright fraud. Activities range from illegally accessing a variety of medical services and procuring prescription drugs, to defrauding insurance providers and passing undue expense onto the consumer. Medical identity theft not only threatens the economics of our healthcare system, but also puts lives at risk and erodes patient trust.

This presentation will examine some of the means that criminals are using to obtain PHI, provide real-world instances of medical identity abuse, and conclude with key considerations for stemming the proliferation of medical ID fraud.

Speaker: ***Greg Porter****, CISSP, CISM, GCIH, Allegheny Digital*

2:00 - 2:45 pm

Protecting Regulated Data in the Cloud

All cloud vendors claim to be secure, but how can you be sure? What upfront security requirements should you demand of your cloud vendors? What security terms should you include in your contract? What security validation of the service should you perform before going live? What operational security reporting should you expect from your cloud and SaaS vendors? Learn about security controls, data monitoring and identity management approaches that may assist your own efforts in moving your applications and systems into the cloud.

Speaker: ***Tom Lunzer*** *and* ***Mike Wolfe****, Senior Security Architects, Blue Shield of California*

2:45 - 3:15 pm

Networking Break

3:15 - 4:15 pm

Solutions Session Presented by

TREND MICRO™

Securing Your Journey to the Cloud

Securing the Patient Portal

Healthcare organizations are beginning to understand that HITECH/HIPAA compliance and information security risk assessments are not one-time events and must be implemented as part of a continual security monitoring and remediation program.The impact of lapses in security can be staggering including financial harm, reputational damage, and loss of consumer confidence.

As such, healthcare organizations must continuously work to identify endpoint, network and web application weaknesses for EHRs and patient portals to defend against increasingly sophisticated external threats. In this session we will examine these issues and learn ways to successfully deploy patient portals and other EHR applications with robust security that minimize risk and regulatory exposure for your organization.

Speaker: ***Karl Gainey****, Senior Sales Engineer,TrendMicro*

4:15 - 5:15 pm

Panel: Top 5 Security Issues for Medical Devices

Driven by HIPAA most activity initially focused on health care applications and the electronic protected health information contained within. However, medical equipment has been often been impacted by malware exploiting unpatched software. More recently, exploits have detailed that can compromise personal medical devices and possibly even implants.

Vulnerabilities of the simplest nature continue to exist in medical devices, but there are other security issues around integrity of data, authentication and access control. FDA regulation and certification requirements often cited by manufacturers as an impediment to security improvements and health care organizations can't improve security on their own.

Moderator: ***Frank Kim****, Director, Kaiser Permanente*

Panelists: ***Steve Abrahamson****, Engineering Privacy and Security Leader Science and Technology, Organization, GE Healthcare*
Dale Nordenberg*, Co-Founder & Executive Director, Medical Device Innovation, Safety & Security Consortium (MDISS)*
Lynette Sherrill, *MCSE, CISSP, GSEC, Deputy Director -Health Information Security Division, Department of Veterans Affairs*
Daniel Silverstein*, Cyber Security Strategy Consultant, Kaiser Permanente*

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.

Thursday, October 24

9:00 - 10:00 am

Keynote Panel: Real-World Healthcare Cyber Security: The View from the Top

Join a panel of senior leaders from top healthcare organizations as they share their priorities for cyber security, their prognostications on emerging threats, and the truth about what keeps them up at night. Learn from their best practices and their pain points, and see how your cyber security plan stacks up.

Moderator: ***Frank Kim****, Director, Kaiser Permanente*

Panelists: ***Kevin DePeugh****, VP, Cyber Security, Kaiser Permanente*
Jim Routh*, CISO, Aetna*
Sherry Ryan*, CISO, Blue Shield of CA*

10:00 - 10:30 am

Networking Break

10:30 - 11:15am

National Health Cybersecurity Framework

Intelligence information is often called a "force multiplier," but in order to achieve that effect in cybersecurity, threat and vulnerability information needs to be shared. Too often that data, as well as best practices, guidelines, metrics, solutions etc., are trapped in organizational silos. In the healthcare industry, the National Health Information Sharing and Analysis Center was established under the National Infrastructure Protection Plan as a privately led sector-specific organization to establish and maintain collaborative frameworks for interaction and sharing between and among members and external partners.

The National Health Information Sharing and Analysis Center (NH-ISAC) Executive Director, Deborah Kobza is providing a national briefing on the National Health Cybersecurity Framework (health sector-focused version of the NIST Cybersecurity Framework (Presidential Executive Order), and the National Health Cybersecurity Response System. Health sector-defined working in collaboration with NIST, HHS, DHS, FBI, etc., the Health Framework incorporates cybersecurity leading practice and security situational awareness information sharing and response to support National Health Critical Infrastructure Resilience (Identify, Protect, Detect, Respond and Recover).

This session provides the opportunity to engage and participate with a "defining voice" and benefit from ongoing efforts and the National Health ISAC.

Speaker: ***Deborah Kobza****, CGEIT, Executive Director / CEO, The National Health ISAC (NH-ISAC)*

11:15 am - Noon

Case Study: BYOD in a Clinical Care Setting: A Case Study

On a recent visit to our house, my father asked to borrow a newspaper. I proceeded to extol the virtues of the modern digital age, going so far as to scoff at the very idea of print media, and then offered him my trusty mobile device. That spider never knew what hit it!!

This anecdote is an example of the most important step in developing a sound BYOD strategy – understand the requirements. In this session, we will discuss the various steps and considerations for successfully implementing mobile devices in a clinical care setting.

Speaker: ***Bill Dieringer****, AVP – IT Security, Ardent Health*

Noon - 1:15 pm

Lunch On Own

1:15 - 2:15 pm

HIE & Security

Successful Health Information Exchanges should improve the overall quality, cost and efficiency of the healthcare system. Organizations participating in a HIE are challenged to ensure that the data provided through the exchange is timely, accurate, understood, and secure. The data involved in the exchange process is very sensitive and there are regulatory and legal requirements to keep the data secure and available within the process. When preparing to create or participate in a HIE, each participating organization should ensure that appropriate legal requirements, security structure, and technical framework have been established to protect the confidentiality and integrity of the data, while offering appropriate protection to the participating providers/organizations.

This session will include discussion on a recommended approach for creating an overall security framework and security organizational structure to help minimize the risks for HIE participating members and to protect the shared data. It will conclude with a mini-panel of members of the Care Connectivity Consortium IT Security Workgroup, to discuss the security issues involved in the implementation of the CCC HIE.

Speaker: ***Carl Allen****, CISM, CRISC, Director of Information Systems Security and Deputy CISO, Intermountain Healthcare*
Bruce James*, Manager, IS Security Architecture, Intermountain Healthcare*

2:15 - 2:45 pm

Networking Break

2:45 - 3:30 pm

Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks in the Healthcare Sector

CERT's insider threat team, which was formed in 2001, has built an extensive library and comprehensive database containing hundreds of actual cases of insider incidents. This presentation will describe findings from our analysis of three primary types of insider incidents: IT sabotage, Theft of Intellectual Property, and Fraud. All CERT insider threat research focuses on both the technical and behavioral aspects of actual compromises. The presentation will describe who committed the crimes, their motivation, organizational issues surrounding the incidents, methods of carrying out the attacks, impacts, and precursors that could have served as indicators to the organization in preventing the incident or detecting it earlier. We will convey the "big picture" of the insider threat problem - the complex interactions, relative degree of risk, and unintended consequences of policies, practices, technology, insider psychological issues, and organizational culture over time.

Attendees will leave with an understanding of the scope of the insider threat problem, patterns to watch for that could signify increased risk, and proactive measures that they can put into place for prevention and detection of insider threats. Actual incidents from the Healthcare sector will be presented throughout the presentation to provide concrete examples and lessons learned.

Speaker: ***George Silowash****, CyberSecurity Threat and Incident Analyst, Cyber Enterprise and Workforce Management, CERT Program at Carnegie Mellon University's Software Engineering Institute*

3:30 - 4:30 pm

Have Tablet, Will Travel: How To Secure and Manage Mobile Solutions for Clinicians In The Wild

When you want to test your ability to secure and manage your mobile clinical device, just release it from the hospital to travel in the wild. This session will share Sutter's lessons learned on managing and securing mobile clinical tablets running mission critical EHR when PHI is stored locally, there's a rich set of other communications and clinical tools, and the patient bedside has now moved from the hospital to the home. Mobile healthcare solutions at the patient home are improving care and productivity and they're opening the door to new services. The solutions discussed in this session will make sure that we protect patient information while taking advantage of these new platforms and solutions.

This session will provide lessons learned from four years of managing 1,000+ clinicians and their devices travelling throughout Northern California. This journey includes changing device platforms, changing device management solutions, managing the transition through 3 generations of Android tablets, enabling the change from 3G to 4G, managing stolen devices, lost devices, recovered devices, and reporting to the data security office. If you have mobile clinical systems that have to travel out in the wild, this session will help you help them travel safely.

Speaker: ***Ed Elliott****, Technical Services Manager, and* ***Phil Chuang****, IS Director, Sutter Health Information Service - Sutter Care at Home*

Thank you for attending the Healthcare Cyber Security 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.

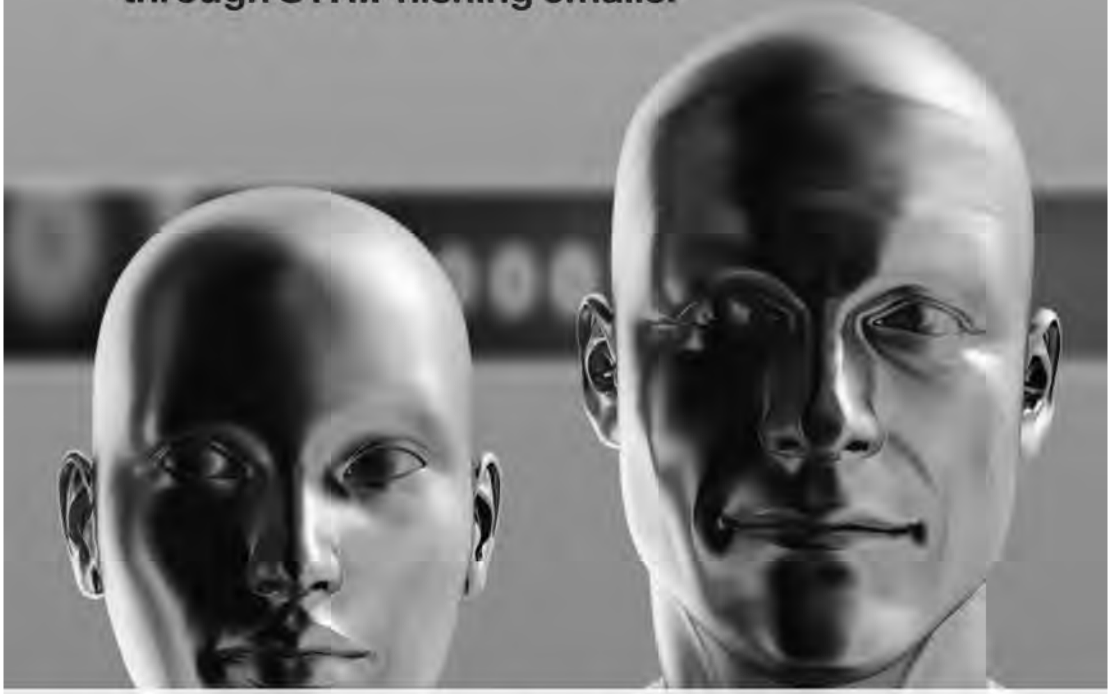
Exhibitor

TREND MICRO™

Securing Your Journey to the Cloud

Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With more than 25 years of experience, we're recognized as the market leader in server security, virtual security, and small business content security. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. Our solutions are powered by the cloud-based global threat intelligence of the *Trend Micro™ Smart Protection Network™* infrastructure, and are supported by over 1,200 threat experts around the globe.



How Are You Protecting Your

Data?

Network?

Systems?

Critical Infrastructure?

Risk management is a top priority. The security of these assets depends on the skills and knowledge of your security team. Don't take chances with a one-size fits all security certification. **Get GIAC certified!**

GIAC offers over 20 specialized certifications in security, forensics, penetration testing, web application security, IT audit, management, and IT security law.

"GIAC is the only certification that proves you have hands-on technical skills."
-Christina Ford, Department of Commerce

"GIAC Certification demonstrates an applied knowledge versus studying a book."
-Alan C, USMC

Learn more about GIAC
and how to *Get Certified* at
www.giac.org

GLOBAL INFORMATION ASSURANCE CERTIFICATION
GIAC
www.giac.org

NEW!
GIAC CERTIFICATION

GIAC MOBILE DEVICE SECURITY ANALYST
GMOB

Coming Fall 2013!
GIAC Mobile Device Security Analyst

Registration now open at www.giac.org

UPCOMING SUMMITS & TRAINING COURSES

2013

Pen Test Hackfest Summit & Training
Washington, DC | November 7-14

Asia Pacific ICS Security Summit
Singapore | December 2-7

2014

AppSec Summit & Training
Austin, TX | February 3-8

Cyber Threat Intelligence Summit & Training
Washington, DC | February 2014

Digital Forensics & Incident Response Summit & Training
Austin, TX | June 3-10

Industrial Control Systems Security Summit & Training
Orlando, FL | March 12-18

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**.

Visit **www.sans.org/summit** for detailed summit agendas as they become available.