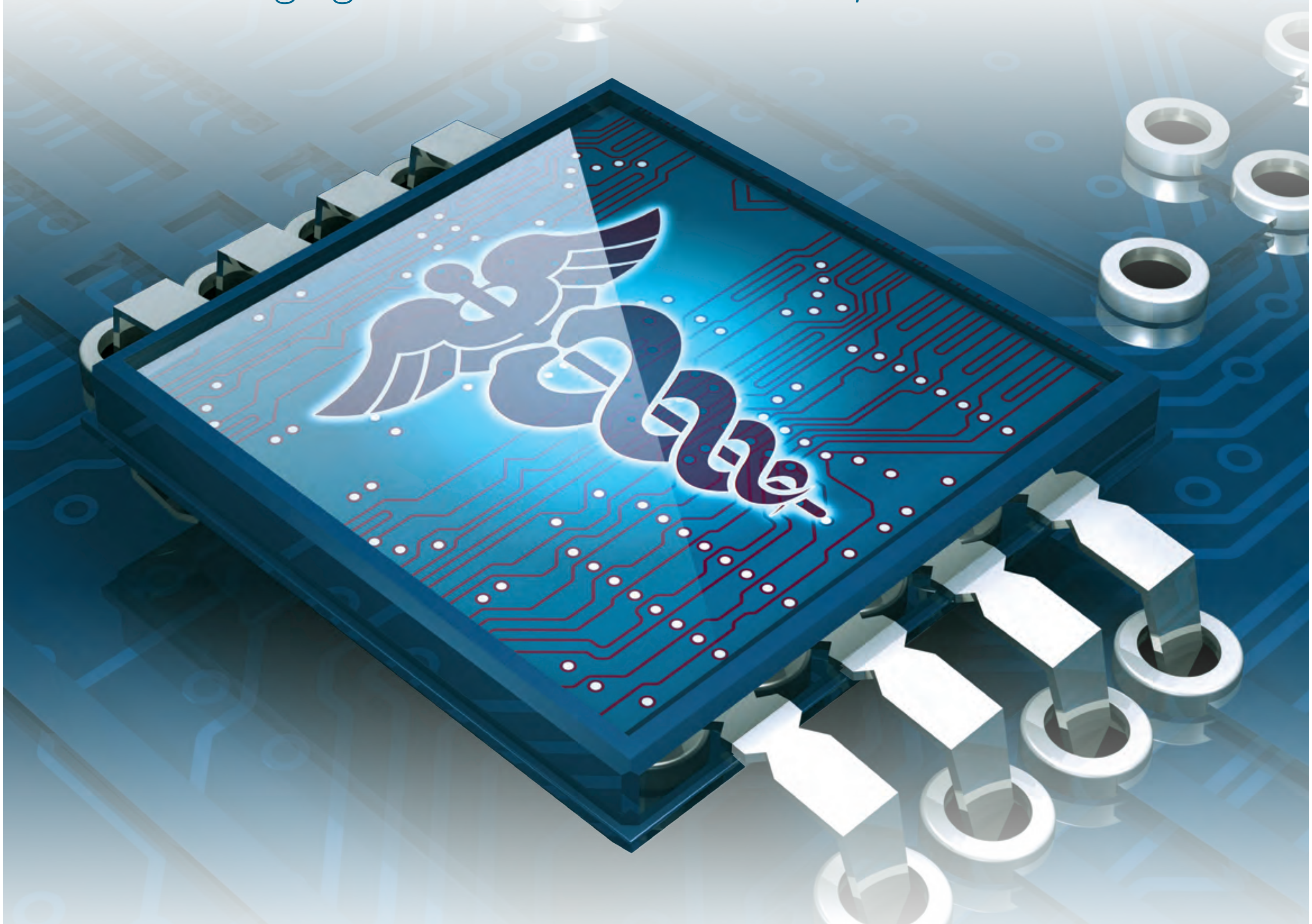
Healthcare CYBER SECURITY SUMMIT

Emerging Trends & Best Practices for Healthcare



Program Guide

Summit Chairman: Jim Routh, CISO, Aetna & Board Member, NH-ISAC

Follow @SANSInstitute on Twitter

Join the conversation #HealthcareSummit

SANS NH-ISAC

Agenda

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

*Summit presentations will be posted via the following URL - **https://files.sans.org/summit/healthcare2015**.*
An email will be sent to all attendees once the slides are live on the website, typically about 5 business days after the event.

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, May 12

8:00 - 9:00am

Registration & Coffee

Pastries Provided

(LOCATION: INTERNATIONAL FOYER)

9:00 - 9:50 am

Healthcare at the Speed of Hacking

***David Kennedy**, Founder, TrustedSec, LLC, Co-Founder & CTO, Binary Defense Systems*

The healthcare industry is unique based on the types of systems that need to remain protected and are, at the same time, difficult to secure (loss of life, etc.) This update to last year's top-rated presentation at the HC-ISAC Summit illuminates the techniques being used by hackers, and most importantly, points out how vulnerable we are in the medical field. Healthcare IT security is years behind other industries. This briefing covers our recently completed assessments and the alarming trends we see consistently across the industry.

9:50 - 10:20am

Networking Break & Vendor Expo

(LOCATION: INTERNATIONAL FOYER)

10:20 - 11:00am

How To Give A Winning Security Briefing That Leads To Management Action

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

What is the difference between a presentation to management that leads to management approving projects/action you envision vs a presentation that leads to their confusion or worse to their conclusion that the CISOs communication skills are inadequate? Technical speakers often make a series of blunders that devalue their presentation in the eyes of senior executives and managers in other parts of their organizations. This briefing illuminates many of those errors, in a relatively humorous way, and then shows you the one technique that is more powerful than any other in moving management to action, before concluding with a brief segment on handling very tough questioners.

11:00am - Noon

Adjusting Controls Based on Changes in Threats For Risk-Driven Information Security in Healthcare

***Jim Routh**, CISO, Aetna & Board Member, NH-ISAC*

In this updated version of the 2014 Summits other top-rated briefing Aetna CISO Jim Routh introduces a fundamentally new approach to the drivers for an effective information security program for the healthcare industry using risk management practices and technology portfolio management practices. Jim is one of the growing numbers of information security leaders migrating into the healthcare industry applying risk- driven information security practices in an industry driven historically by a complex web of regulatory requirements at the federal, state and local levels. He will provide specific examples of adjusting controls to address threats from emerging technologies. Security programs need to anticipate and prepare for risks and make real-time adjustments to controls based on shifts in threat trends to make the most efficient and cost-effective use of scarce resources.

Noon - 1:15 pm

LUNCH & LEARN

Presented by

VERACODE

A CISO's Perspective on Talking to the Board About Cybersecurity

***Chris Wysopal**, CTO, Veracode*

The role of the CISO is dramatically changing as business and technology are becoming interwoven with one another. Learn how to be less nerdy when talking to the board, which key metrics to use when describing your risk posture, and how to provide context about why today's risks are different.

LUNCH & LEARN

Presented by

IONIC SECURITY

Data control and Protection at the Molecular Level – How to succeed in the age of Social, Mobile, Analytics, Cloud (S.M.A.C)

***Alain Sergile**, V.P. Product Marketing, Ionic Security*

In a world where data proliferation and collaboration is exploding and new technologies are enabling the individual before the business can, learn how businesses can regain visibility and retain control of their sensitive information and data while saying yes to their employees and the business.

1:15 - 2:00pm

The Monster Under Your Bed is More Afraid of You Than You Are of It

***Nikolay Chernavsky**, CISSP, CISM, CRISC, Director of Information Security, Amgen*

This talk will look into the rise of nation-state sponsored threat actors from a different vantage point. There is no shortage of publically available information on cyber security incidents involving Russia and China. The term "cybersecurity threat" has become nearly synonymous with Russia or China. This talk will offer a different perspective on the current situation and what healthcare organizations can do about it. It's a provocative conversation, led by Belorussian-born Nikolay Chernavsky, who has spent the last couple years analyzing Emerging Markers to help you to understand and align your strategy in Emerging Markets. His perspective is different from that of people who spent most of their lives in United States. Participants will be able to hear another story that will likely change perceptions and will certainly influence enterprise's strategy for doing business in Emerging Markets.

2:00 - 2:45pm

Cyber Threats to the Healthcare Sector: FBI Response and Information Sharing

***Brett Leatherman**, Assistant Section Chief, Cyber Outreach Section, Cyber Division, Federal Bureau of Investigation*

FBI Cyber Division describes its responsibilities, resources, and outreach efforts with regard to cyber threats to the healthcare sector. Recent major intrusions highlight the fact that targets of cyber intrusions are most frequently private company networks and data that can directly impact the financial and physical security of U.S. citizens. As such, the FBI recognizes the cyber threat cannot be adequately addressed—that the FBI cannot fulfill its mission to identify, pursue, and defeat national security and criminal cyber threats—without the inside knowledge and voluntary cooperation of the private sector.

2:45 - 3:15pm

Networking Break
(LOCATION: INTERNATIONAL FOYER)

3:15 - 4:00pm

A Look at the Healthcare Threat Landscape with Lessons from First Responders

Col. Barry Hensley*, CTU Executive Director, Dell SecureWorks*

Leveraging alert data compiled from over 4000 customers, we will show how multiple industry verticals compare to the healthcare industry and highlight differences where they occur. Then, using information collected during incident response and advanced threat hunting engagements, we will share some insights into common tactics, techniques, and procedures observed in the past year and identify examples of security controls that will help detect and prevent such attacks.

4:00 - 4:15pm

Closing Remarks

Jim Routh*, CISO, Aetna & Board Member, NH-ISAC*

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.

4:15 - 5:30pm

Networking Reception
(LOCATION: INTERNATIONAL FOYER)

Sponsored by

Deloitte.

Wednesday, May 13

8:00 - 9:00am

Breakfast Panel

Presented by

INAUTH hp Sonatype

Start the second day of the Healthcare Summit with breakfast sponsored by Inauth, HP Voltage Security and Sonatype. They will each give a brief presentation followed by networking with your healthcare security colleagues.

9:00 - 9:45am

How Security Practitioners can Influence Business Leaders

Jim Routh, *CISO, Aetna & Board Member, NH-ISAC*

Jim Routh delves deeper into exactly what management and board members need to understand to make the right decisions to create a secure cyber environment in healthcare organizations of all types and sizes. Jim will share several techniques applied and identify what works well and not so much offering specific examples.

9:45 - 10:15am

Networking Break

(LOCATION: INTERNATIONAL FOYER)

10:15 - 11:00am

From the Front Lines:
An Insiders' Story About Inter-Company Cooperation in Responding To Cyber Attacks

MODERATOR:

Alan Paller, *Director of Research, SANS Institute*

PANELISTS:

Nikolay Chernavsky, *CISSP, CISM, CRISC, Director of Information Security, Amgen & Board Member, NH-ISAC*
Jeanie Larson, *CISM, CISSP-ISSMP, CRISC, ACISO, Stanford Health Care & Board Member, NH-ISAC*
Jim Routh, *CISO, Aetna & Board Member, NH-ISAC*

An insider's look at cyber security sharing practices from three different healthcare firms and how the whole is more resilient than each individual company as a result of sharing information on threat trends, indicators of compromise, threat actor intent, effective controls, ineffective controls and emerging practices. The information sharing of an ISAC differs from any other type of information sharing in making the industry more resilient and this inside story will highlight several examples of how the industry is improving.

11:00 - 11:45am

Using an Open-Source Threat Model for Prioritized Defense

James Tarala*, Senior Instructor, SANS Institute*

Threat actors are not magic and there is not an unlimited, unique list of threats for every organization. Enterprises face similar threats from similar threat sources and threat actors – so why does every organization need to perform completely unique risk assessments and prioritized control decisions? This presentation will show how specific, community-driven threat models can be used to prioritize an organization's defenses – without all the confusion. James Tarala will present a new, open, community-driven threat model that can be used by any industry to evaluate the risk that faces them. Then he will show how to practically use this model to prioritize enterprise defense and map to existing compliance requirements facing organizations today. Whether you are part of a multinational pharmaceutical corporation or a 30-bed care facility, you will be able to use this model to specifically determine a prioritized defense for your organization.

11:45am - 12:30pm

Healthcare Industry Control Frameworks: Key Decisions for CISOs and CSOs

MODERATOR:

Alan Paller*, Director of Research, SANS Institute*

PANELISTS:

Cliff Baker*, CEO, Meditology*
Scott Breece*, VP of Security & CISO, Community Health Systems*
Jim Routh*, CISO, Aetna & Board Member, NH-ISAC*

Every healthcare CISO and CSO has to address the fundamental question of what role industry control frameworks play in the information security program and which ones matter most. Alan Paller will moderate this panel of healthcare CISOs and CSOs who will discuss how they made their decisions on the frameworks most appropriate for their organizations and what factors were considered in the decision-making process. Healthcare specific vs. cross industry, U.S. centric vs. International, vendor specific or standards board.

12:30 - 1:30pm

LUNCH & LEARN

Presented by

Skycure
Smart Security for Smart Devices.

The Most Dangerous Security Holes in Your Mobility Policy

Adi Sharabani*,*
CEO and Co-Founder of Skycure

Hackers are finding new ways to steal data and infiltrate healthcare organizations daily. A number of trends are driving the need for mobile threat defense, including the ubiquity of mobile devices among doctors, nurses and patients, BYOD, and the rise of cyber attacks. Attend this lunch and learn to hear from Adi Sharabani, CEO of Skycure, the leader in mobile threat defense, the best practices on how to avoid mobile attacks and secure both BYO and corporate-owned devices. The session will also include a live demo of an ethical hack in which Adi will hack any iOS or android device in less than 60 seconds.

LUNCH & LEARN

Presented by

SOPHOS Infogressive, Inc.
Aggressive Information Security

Prevent - Detect - Respond

Donald Sanders*,*
Director of Operations, Infogressive

We all want to prevent 100% of attacks, however 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. #BOOM.

1:45 - 2:30pm

SOLUTIONS SESSION

Presented by

SURFWATCH
CYBER IN SIGHT

Physician, Heal Thyself: Using Familiar Data Collection and Analysis Approaches to Treat Cyber Like a Disease

***Jason Polancich**,*
Founder and Chief Architect, SurfWatch Labs

The healthcare industry is used to data-heavy analysis to find resilient solutions and to reduce risk. In fact, Patient Safety Organizations (PSO's) were created to study what bad things happen (and how and to whom) over time in order to help prevent them and to make healthcare a safer place overall. However, when it comes to cybersecurity, this commitment to data collection and analysis is almost nonexistent.

Cyber defense is dominated by tactics - lever-pulling and button-pushing at an operator level. It's the never-ending cycle of react, retreat, get hit again. Most healthcare organizations cannot say with any certainty how the cybersecurity tools or resources align with their specific cyber problems. They don't know what cybercrime affects them most, least or what's trending over the last quarter. They don't know the areas where they should increase/decrease spend and focus. This approach would never be taken by a surgeon, who would study data and historical information with the goal of improving or innovating on existing tactics when something has failed.

In this session, Jason Polancich, Founder and Chief Architect of SurfWatch Labs, will explore why the traditional approach to cybersecurity is failing and how healthcare organizations can improve their security strategy and long-term resiliency by treating cyber like a disease.

SOLUTIONS SESSION

Presented by

Vorstack

Getting the Most Value from Your TIP Implementation – It's That Easy

MODERATOR:
***Anne Bonaparte**, CEO & President, Vorstack*

PANELISTS:
***Paul Calatayud**,*
CISO, Surescripts

***Nikolay Chernavsky**,*
Director of Information Security, Amgen & Board Member, NH-ISAC

***Scott Jantzer**,*
CISO, St. Luke's Hospital

NH-ISAC released its Threat Intelligence Platform (TIP) that enables its members to anonymously share threat information as a community effort. The NH-ISAC platform leverages Vorstack ACP and Soltra to create a common ground for fighting threats across the healthcare industry. The combined solution enables you to ingest STIX messages and publish them back to the community. In this session, a panel of industry leaders will share their experiences implementing the NH-ISAC TIP, describe the value they received from the solution, and explain how they expect to participate with in the NH-ISAC Trusted Circles going forward.

2:30 - 3:15pm

Third-Party Governance Done Right

***Brenda Ward**,*
Director of Global Information Security (GIS), Aetna

This talk will feature a mature 3rd-party security governance process implemented for Aetna that adds risk-based security controls to a robust compliance program that address the risks of third parties hosting member health information and providing web portal access or mobile access. Brenda Ward is the Global Information Security Director for the 3rd-party security governance program and has implemented five security specific controls across hundreds of third parties that address things like software security maturity and risks, authentication of users, encryption of data in transit and at rest, using frameworks from the financial services industry. Brenda leads a vendor ISAC community to share cybersecurity intelligence and best practices with the vendors to improve their cyber resiliency.

Adding Resiliency to Software Reduces Risk and Improves Productivity

***Tim Tompkins**,*
Director, Global Information Security Innovation, Aetna

Chief Security Architect Tim Tompkins, from Aetna, will provide an overview of his award-winning software security program that leads the healthcare industry in maturity measured by BSIMM (www.bsimm.com). Tim designed and implemented a dozen controls to be integrated with the software development and acquisition processes that include threat modeling, open source component lifecycle management, security frameworks (reusable code), static analysis for developers that is easy to use, dynamic scanning in QA, penetration testing, and perimeter vulnerability scanning. Tim uses a curriculum developed specifically for over a dozen stakeholder groups (developers, DBAs, architects, project leads, etc.) that is delivered electronically and includes an advanced program for security mavens that certify developers on software security practices at a green, brown and black belt level of expertise. Tim will share information on the results of the program through key performance indicators that include the productivity gains from the program.

3:15 - 3:40pm

Networking Break
(LOCATION: INTERNATIONAL FOYER)

3:40 - 4:30pm

One Size Doesn't Fit All

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

PANELISTS:
***Steve Bartolotta**,*
VP & CISO, Community Health Network of Connecticut

***Jeanie Larson**,*
CISM, CISSP-ISSMP, CRISC, ACISO Stanford Health Care & Board Member, NH-ISAC

***Reid Stephan**,*
Director, IT Security, St. Luke's Health System & Board Member, NH-ISAC

Information sharing is vital for any healthcare organization, but can feel overwhelming for small organizations with limited resources. What can smaller organizations learn from healthcare giants? Does being small provide benefits of agility and speed of decision-making? How can smaller providers maximize their efficiency to ensure big-time cybersecurity?

Securing Health Data in the Mobile Ecosystem

***Tim Tompkins**,*
Director, Global Information Security Innovation, Aetna

Mobile Security Architect Eileen Bridges will describe her mobile security program for consumers and for enterprise users and how Aetna has addressed the data protection requirements with a focus on ecosystem and application level controls for mobile applications. Eileen has over a decade of experience developing mobile applications and applying effective security controls to protect the data from ecosystem level threats. Eileen uses a mobile risk engine to determine a risk score for each application user depending on attributes from the device and the user of the device that tells the application how much functionality to provide. This is an example of behavioral based authentication that improves both the risk and the customer experience vs. conventional binary authentication controls (user ID & password). Eileen will describe how important it is to protect the brand for consumer applications by obfuscating the mobile binaries and scanning mobile app stores to identify copycat applications that infringe on the brand and apply malware to mobile users.

4:30 - 5:30pm

A Healthy Perspective:
What Healthcare Cybersecurity Leaders Learned From Other Industries

MODERATOR:

***Steve Katz**, President, Security Risk Solutions LLC*

PANELISTS:

***Jeanie Larson**, CISM, CISSP-ISSMP, CRISC, ACISO Stanford Health Care & Board Member, NH-ISAC*
***Jim Nelms**, CISO, Mayo Clinic*
***Matt Pocchia**, Information Security Executive*
***Frank Price**, VP & CISO, CVS Caremark*

While some leaders in healthcare cyber security worked their way up through the ranks of healthcare organizations, many cut their teeth in very different industries. Whether they started out in the military, banking and financial services, or elsewhere, our panelists will share the ways their experience helped them bring innovative thinking to careers in healthcare, and the challenges of making the leap.

5:30pm

Closing Remarks

***Jim Routh**, CISO, Aetna & Board Member, NH-ISAC*

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

AGARI

Akamai

cigital

DELL SecureWorks

Deloitte.

hp

INAUTH

IONIC SECURITY

RISKIQ

Skycure
Smart Security for Smart Devices.

skyhigh

SOLTRA

Sonatype

SOPHOS

Infogressive, Inc.
Aggressive Information Security

SURFWATCH
CYBER IN SIGHT

VERACODE

Vorstack