



H-ISAC™

HEALTH - ISAC



H-ISAC is excited to announce our **10 YEAR ANNIVERSARY!**

In 2010 it was rare to hear the words health care and cyber security paired in the same sentence. However, with the advent of the passing of the Electronic Records Act and the advance of technology in health, including medical devices, along with the evolution of the threat landscape, looking back, how naïve we were. The H-ISAC had humble beginnings but over the last ten years we have grown tremendously and have done great things. We are truly a global community. We are very proud to have played a role in making the health sector more secure and addressing cyber and physical security and the role they play in patient safety. Thank you to all of our members and partners who add value to the organization every moment of every day. We look forward to working together with all of you into the next decade and beyond.



High Scores at H-ISAC “Up Your Game” Fall Summit in San Diego!

Starting with in-person meetings for many of our working groups and a gorgeous evening reception for new members and first time attendees, it was a full week of network building and sharing. The keynote speaker, Michael Pfeffer, MD, FACP, shared a doctor’s perspective to the transition from paper to digital. Lunchtime comic relief from technical comedian Don McMillon had the room rolling. Suzanne Schwartz, Deputy Director for the US Food and Drug Administration, led an interactive and dynamic Medical Device Town Hall. In breakout sessions, members and vendor partners shared everything from how to build a threat and vulnerability assessment program to IT best practices learned from going through a divestiture transition, and a panel discussion on how to break through to the board—just to name a few. Between sessions, members honed their incident response skills working together under pressure before the “bomb” exploded in the Escape Room set up by Living Security.



H-ISAC has become known for great networking events and this Summit did not disappoint. The Arcades and Charades Game Night offered a tentful of digital and retro games—including a life-sized Operation Game—for attendees to really interact. True gaming nerds gathered around tables of board games which lasted well into the night. The finale networking event was a fabulous dinner cruise on the San Diego Bay thoroughly entertained by a dueling pianists who managed to get everyone singing to requested songs. The Spring Summit theme is Strike Back, so the events should prove memorable. Learn more about upcoming summits at <https://h-isac.org/events/>.



Top 10 Health Related Cyber Events for January:

[Atlassian scrambles to fix zero-day security hole accidentally disclosed on Twitter](#)

[US Indicts 'Evil Corp' Hackers With Alleged Russian Intelligence Ties](#)

[Snatch Ransomware Reboots Windows in Safe Mode to Bypass Antivirus](#)

[TrickBot gang is now a malware supplier for North Korean hackers](#)

[New Ransomware Spotted Targeting Health, Tech Orgs Via Supply Chain](#)

[Ryuk Ransomware Likely Behind New Orleans Cyberattack](#)

[Emotet Trojan is Inviting You To A Malicious Christmas Party](#)

[RSA Keys Found in IoT Medical Devices, Implants Prone to Attack](#)

[British Hacker Accused of Blackmailing Healthcare Firms Extradited to U.S.](#)

[Apple Opens Its Invite-Only Bug Bounty Program to All Researchers](#)

H-ISAC is pleased to publish a monthly member newsletter. It is designed to bring events and other important ISAC information to your attention. If there is something you would like to see included please email: contact@h-isac.org



The H-ISAC Threat Operations Center (TOC)

With the newly formed H-ISAC Threat Operations Center up and running for several months now, it is a good time provide members an overview of their TOC and its mission toward supporting and edifying H-ISAC membership.



We thought the term Security Operations Center (SOC) was creating some confusion due to the nature of what a traditional SOC does. Most people believe a SOC monitors firewalls and intrusion detection systems and then responds to potentially harmful events or hunts for threats within an organization's networks. Threat Operations Center (TOC) more accurately describes what we do – we act as the hub for information sharing, plus we monitor many sources for threats and provide timely threat intelligence for H-ISAC members.

The TOC was stood up to assist and augment the membership community to protect themselves from potential attacks that may cause harm to their organization, brand, and most importantly their patients.

A typical day at the TOC begins with aggregating current events that are relevant to both Cyber and Physical threats that may affect the Healthcare sector. The remainder of the day is variable in nature and may encompass crafting threat and vulnerability bulletins, monitoring chatter across multiple communication channels, working with intelligence partners to identify and assist potential victims of cyber-crimes, hosting threat briefings, attending intelligence training and events, and other various research activities.

Zach Nelson, Intelligence and Operations Team Lead at H-ISAC, comes to the TOC with 9 years of experience in the Healthcare industry learning numerous roles within the IT department of Orlando Health in Central Florida, mostly within the Cyber Security team. His experience includes assisting the procurement and implementation of SOAR and Threat Intelligence Platforms within their SOC. When asked what he would like the H-ISAC membership to know about the TOC, Zach says "We would like our members to know we exist to assist in enriching their membership experience. As we build on the foundation of the identity created, we welcome the thoughts and opinions of our members to assist in bringing to fruition a more robust partnership that will help guide us into the future."

The 2020 vision for the TOC includes launching products that will enhance and streamline the membership experience, providing members the capability of tailoring their experience and the information they receive towards their relevant individual interests. Events will include extensive training with intelligence partners to offer our members opportunities that will assist in expanding knowledge within their intelligence programs. The team also envisions a global presence with staff coverage that will eventually be represented throughout the world. Members are encouraged to drop a note to your TOC – to share, ask questions, provide suggestions, etc. at soc@h-isac.org.

Call for Participants - Hobby Exercise

The February 12th exercise in Washington D.C. will highlight and address cybersecurity challenges impacting the HPH sector; educate the sector and government on the issues faced by the HPH sector and how H-ISAC can, and is, addressing them; and more. Interested persons please email contact@h-isac.org.

An H-ISAC Navigator Webinar

A Sign of the Times: **VALIMAIL**

Automated communications fraud and what you can do to stop it.

January 22nd at 12PM EDT.

Visit our [events page](#) for more information.

Connect with H-ISAC Around the Globe!

Find a Security Workshop near you!



- UK-London**—February 5: H-ISAC Security Workshop
- USA-Florida**—March 4: H-ISAC Analysts Security Workshop
- India-Chennai**—March 27: H-ISAC Security Workshop
- Singapore**—March 31—April 2: APAC H-ISAC Summit
- USA-Massachusetts**—April 7: H-ISAC Security Workshop
- USA-Georgia**—April 13: H-ISAC Security Workshop
- USA-Florida**—May 11-13: 2020 H-ISAC Spring Summit
- USA-Maryland**—June 9: H-ISAC Security Workshop

Important Upcoming Summit Deadlines

- APAC Summit Call for Papers closes January 10**
- Spring Summit Call for Papers closes January 20**



Find these and other upcoming events on our [Events page](https://h-isac.org/events/)