



# H-ISAC™

HEALTH - ISAC



## TIC Overview of 2018

In 2018 the H-ISAC Threat Intelligence Committee (TIC) continued to peruse the cyber threat landscape for the health and public health (HPH) sector and engaged in strategic direction for the ISAC community to anticipate and prepare for threats.

The WeeSecrets and Mattermost platforms have taken off this year, closing 2018 with ~1,275 H-ISAC users. This number increases every day, as more members discover the benefits (and fun!) of secure chatting with other members. Mid last year, the Credparser and BiMeta capabilities were added to H-ISAC membership offerings. To date, CredParser has ingested 10B+ credentials and found 1.8M unique credentials. BiMeta has found 33M imposter domains. Any member currently not receiving this offering and would like to, please email [contact@h-isac.org](mailto:contact@h-isac.org).

The automated IOC sharing through Soltra has 252 members participating and the Anomali / Threatstream has 75 members receiving the TLP Amber Trusted Circle and the TLP White/Green Trusted Circle has increased to 783 participants.

The TIC conducted eight major briefings in 2018, as well as the TLP Amber in-person sessions at the Spring and Fall Summits. TIC webinar briefings drew up to 839 attendees. Some briefing highlights included the following:

- Meltdown/Spectre (280 attendees)
- SamSam
- RDP Shop
- Struts2
- Magecart

The TIC sends out Threat and Vulnerability Bulletins on new critical or high-risk vulnerabilities that might affect H-ISAC members. Some examples of these from 2018 include bulletins sent regarding WebEx vulnerabilities, emergency patches for Internet Explorer and vulnerabilities affecting Adobe. In addition to covering important vulnerabilities, last year's threat bulletin topics ranged from the recent uptick in activity from TheDarkOverlord, to changes in malware capabilities (ex. Evolution of Emotet capabilities,) to large scale breaches (ex. Marriott,) to indictments issued by the Federal Government, such as APT 10.

The TIC is a closed H-ISAC working group comprised of member volunteers. Members who actively share and answer questions on the Amber Listserv may be asked to participate in the TIC. Be sure to attend the next briefing where the TIC will be discussing a framework to help analysts assess news sources for validity in an efficient manner, which will help when analysts need to keep up with the news cycle and update their leadership.

## Top 10 Health Related Cyber Events for January:

[The 10 Biggest U.S. Healthcare Data Breaches of 2018](#)

[Private data of more than 82 million US citizens left exposed](#)

[Senators Push for Data Breach and Privacy Legislation Following Marriot Breach](#)

[DHS and FBI published a joint alert on SamSam Ransomware](#)

[30 Percent of Healthcare Databases Exposed Online](#)

[How To Protect Healthcare Records In A Zero Trust World](#)

[Government Hackers Assault Hundreds Of 'Secure' Google Accounts With Evil Phishes](#)

[Unsafe medical devices allowed into global markets harm patients, investigation reveals](#)

[How big data is redefining the CEO, CFO and COO roles](#)

[6 CISO Resolutions for 2019](#)

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](mailto:contact@h-isac.org)



# H-ISAC Spring "Whole-in-One Community" Summit



**Call For Papers is now Open**  
Through January 18th

Recent Summit feedback shows Members want to hear more "how" and less "why."

Drive your message to the Whole Community of fellow health sector partners.

Share your usable case studies of techniques, implementation tips and best practices for overcoming trending challenges.

Be a "Course Master" and innovative leader willing to share with, and learn from, your peers.

\*\*Any presentation involving an H-ISAC member and a vendor is considered a "Sponsorship" and should be submitted by the vendor under the "Sponsor" category, not "Member" or "Other". Abstracts submitted in the wrong category will be declined and will not be considered by the H-ISAC Content Planning Committee.

Please submit all inquiries to [summit@h-isac.org](mailto:summit@h-isac.org)

## More Upcoming Global Events:

### H-ISAC CyberRx IoMT Executive Symposium April 15-16 in Munich, Germany

This event includes networking opportunities and a tour of the IBM Watson IoT Tower and industry demos.

More information here <https://h-isac.org/hisacevents/cyberx-iomt-executive-symposium/>



### H-ISAC CyberRx EU Council Meeting and Workshop February 5th in London, England

CPE's may be available to attendees. You must self-certify with an organization such as ICS2 or ISACA. More information here <https://h-isac.org/hisacevents/h-isac-cyberx-biotech-pharma-workshop-london/>

## H-ISAC Israel Showcase & Innovation



**April 8-13**  
in Tel Aviv, Israel

The week includes a 2-3 day showcase of Israel cybersecurity and digital innovators, a 1 day workshop covering cybersecurity topics and opportunities to tour Israel.

### Who should attend?

- Healthcare organization CIO, VP of IT and CISOs and senior cybersecurity leadership.
- Spouses are welcome. Separate fee will include tours and activities.

More information here <https://www.regonline.com/registration/Checkin.aspx?EventID=2551847>

## Shared Services Spotlight:

### H-ISAC 2.0 Questionnaire Released for Shared Risk Assessments

After extensive review and member input, H-ISAC Shared Services provider Prevalent has begun collecting vendor assessment due diligence using the new H-ISAC 2.0 questionnaire. As of December 2018, all new and renewed vendor assessments will be conducted using 2.0. As part of the renewal process, vendors will receive a refresh letter notifying them that it is time to renew their assessment due diligence, and provide instructions on the renewal process.

Note that vendor re-assessments will not automatically be provided as they are collected. The decision was made to make re-assessments available to members at their request. It was determined that this would allow members to more effectively manage their vendor assessment work load. Prevalent will provide a list of all re-assessments as they are received and are available for member review.

For more information on the H-ISAC 2.0 Questionnaire and services offered by Prevalent, please email [contact@h-isac.org](mailto:contact@h-isac.org).