SHARING SINCE 2010

Health-ISAC™

*Collaborating for Resilience in Healthcare*

# Resilience is in our DNA

ANNUAL REPORT 2023

## CONTENTS

# Resilience is in the DNA of the Health-ISAC Community

## ABOUT ISACs

Information Sharing and Analysis Centers (ISACs) are non-profit, mainly private sector, member-driven organizations specific to the critical infrastructure sectors and subsectors. ISACs, established in 1998, help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. This is accomplished by collecting, analyzing, and disseminating timely actionable threat information to their members and providing members with tools to mitigate risks and enhance resiliency. ISACs have broad reach within their sectors, communicating critical information far and wide to maintain sector-wide situational awareness, and collaborate with each other through the National Council of ISACs.

## ABOUT HEALTH-ISAC

Health-ISAC — a non-profit, private sector, member-driven organization — plays an essential role in providing situational awareness around cyber and physical security threats to the Health Sector so that companies can detect, mitigate, and respond to ensure operational resilience. Health-ISAC connects thousands of health security professionals worldwide to share peer insights, real-time alerts, and best practices in a trusted, collaborative environment. As the go-to source for timely, actionable, and relevant information, Health-ISAC is a force-multiplier that enables health organizations of all sizes to enhance situation awareness, develop effective mitigation strategies and proactively defend against threats every single day.

## ABOUT HEALTH-ISAC'S MEMBERS

Health-ISAC membership connects a diverse body of Health Sector organizations to form one community focused on improving health and saving lives. We are better together!

**Globally, Health-ISAC Members include:**

Academic Medical Centers
Biotechnology/Genomics
Blood and Organ Banks
Consumer Health
Electronic Health Record System Providers
Health Delivery Organizations
Hospice
Insurance Companies
Laboratories
Medical Device Manufacturers
Medical Group Purchasing Organizations
Medical Material Manufacturers and Distributors
Medical Research & Development Centers
Medical Technology
Pharmaceutical Manufacturers
Pharmacies
Radiological Centers
Telehealth Providers

# Welcome from the President and CEO

Denise Anderson
President and CEO Health-ISAC

*"DNA orchestrates the complex dance of life and resilience is in our DNA."*

Deoxyribonucleic acid (DNA) was first discovered in 1869 by Swiss biochemist Frederich Miescher. In 1953 a group of researchers uncovered the double helix structure of DNA and the important role it played in genetics by giving it the ability to pass biological instructions through replication. In 1990 the Human Genome project, an initiative to map the human genetic code with its 3.2 billion letters, began. By 2003, the project was completed. The study of DNA has evolved rapidly in less than 200 years, and we are now looking at advancements such as therapeutics designed for an individual based upon his or her genetic makeup.

Likewise, we have seen the evolution of technology and threats. The first computer virus came out in the early 1970's. Fifty years later we face not just viruses and worms, but myriad threats such as Distributed Denial of Service (DDoS), Drive-by downloads, Zero-Days, Phishing, Ransomware, Spyware, Exploit kits, and Wiperware, to name a few. We're not just facing script kiddies in basements, but sophisticated cyber armies funded by nation states.

When you look at the amazing complexity of humans and incredible resilience we have as a species, it is interesting to note that each of the trillions of cells that make up our bodies contain the same 3 billion base pairs. These trillions of cells are replicated from just one pairing, that of our biological mother and our biological father during fertilization.

While the DNA may be the same in each cell, there are 200 different types of specialized cells — cells with specific functions, such as red blood cells that carry oxygen throughout the body and white blood cells that fight infection — where unique proteins allow the cell to perform certain defined tasks. When the body faces a threat, such as a disease, each cell carries on its task with some cells, such as white blood cells, taking point. An intricate, coordinated incident response, if you will.

Over the ages, humans as organisms have adapted to their environments and have taken on or dropped traits, such as wisdom teeth, that are no longer used and could potentially cause harm through impaction or infection. We also have innate instincts such as the fight or flight reaction that becomes finely honed with each threat or perceived threat encounter. You could say that we have assessed risks to our survival and have adapted as a result.

Our bodies with their incident response and risk assessment for survival could be the code for how we adapt as organizations in the face of threats. Looking at the threats, determining the risk, using basic infrastructure that shapes our protective measures and adapting as required, and then responding in a coordinated, informed, collaborative way, enhances our ability to survive — to be resilient. DNA orchestrates the complex dance of life and resilience is in our DNA.

I hope you will enjoy seeing how all of us contributed over 2023 to keep the Health Sector resilient.

Denise Anderson

**Denise Anderson**
President and CEO
Health-ISAC

*"Our bodies with their incident response and risk assessment for survival could be the code for how we adapt as organizations in the face of threats."*

# Message from the Board Chair

Brian D. Cincera
Board Chair Health-ISAC

Health continues to be among the most targeted sectors for criminal actors. While our industry is dedicated to saving and improving lives, attackers steal resources, disrupt operations, divulge personal information, steal intellectual property, counterfeit medicines, and divert lifesaving medical supplies for personal gain. 2023 marks another year in which attacks continue to grow in sophistication and complexity.

Health-ISAC is a community bonded by its human health mission through operational resilience, and as such, is focused on delivering unparalleled visibility to the cyber and physical threat landscape, real-time sharing of preventive and responsive intelligence, and creating a community that collectively shares its successes and solutions to its challenges.

Health-ISAC continues to grow. Our community grew by more than 100 new organizations in 2023, and we now connect over ten thousand analysts globally to share and receive vital threat information. The Threat Operations Center (TOC) expanded its reach, adding European staff and new external intelligence partners. TOC analysts observed a rising number of vulnerabilities and notified 1106 vulnerable health organizations, many of whom were not Members.

Working groups produced six white papers to share with the sector on topics ranging from vulnerability management to biometrics and identity management. Members created five new working groups during the year, including NIS2 Implementation and Physical Security.

We also had a number of 'firsts'. The inaugural APAC Summit in Singapore commenced in March, quickly followed by the first annual European Hobby Exercise in Dublin, Ireland. We launched a Threat Analyst internship program with local universities, operating out of the newly relocated Threat Operations Center in Orlando, Florida. We will continue to expand this program, not only to develop a cyber workforce but to ensure members can benefit from it as well. In addition, the ISAC, along with the American Health Information Management Association® (AHIMA), implemented a certification program with an initial course designed specifically for health professionals entitled *Introduction to Information Security and Cyber Threat Intelligence*.

The Health-ISAC Board of Directors is committed to ensuring that Health-ISAC is an integral and valuable part of the global Health sector.

Resilience is in our DNA as an organization. The Annual Report serves as a time capsule for 2023. Take pride in knowing the health sector has been strengthened through your participation and the collective collaboration, interactions, and sharing within our community.

Brian Cincera

**Brian D. Cincera**
Health-ISAC Board Chair
SVP and CISO Pfizer

## BOARD OF DIRECTORS

**Tarik Rahmanovic**
Sr. Principal Scientist, AbbVie

**Anahi Santiago**
CISO, ChristianaCare

**Scott Nichols**
Global Product Security Leader, Danaher

**Brad Carvellas**
VP and CISO, The Guthrie Clinic

**TJ Bean**
CISO, HCA Healthcare

**Gregory Barnes**
CISO, Highmark Health

**Roisin Suver**
AVP, Cyber Threat Intelligence, Humana

**Michael McNeil**
SVP and Global CISO, McKesson

**Nancy Brainerd**
Senior Director, Product Security, Medtronic

**Terence Rice**
VP, IT Risk Management and CISO, Merck & Co.

**Rishi Tripathi**
CISO, Mount Sinai Health System

**Brian D. Cincera**
SVP and CISO, Pfizer

**Dirk de Wit**
Head of Product Security, Philips

**Sahan Fernando**
CISO, Rady Children's Hospital and Health Center

**Dr. Hans-Martin von Stockhausen**
Principal Key Expert Cybersecurity, Siemens Healthineers

*In Memory of a mentor, advisor and friend of Cybersecurity and Health-ISAC*

Photo ISMG

Steve Katz 1942-2023
Health-ISAC Board Advisor
2017-2023

# A Growing Global Community

## THE VALUE OF COLLABORATING FOR RESILIENCE

In 2023, Health-ISAC Member organizations operated in over 140 countries, constituting a global reach across 71% of the world. Health-ISAC participated in over 181 media events and conducted a Cyberthreat Landscape Tour in 12 cities in Europe, spreading the word about collaborating for resilience in healthcare. 108 new Member organizations joined Health-ISAC's community throughout the year, and the 95% retention rate shows the value gained from collaboration in this community.

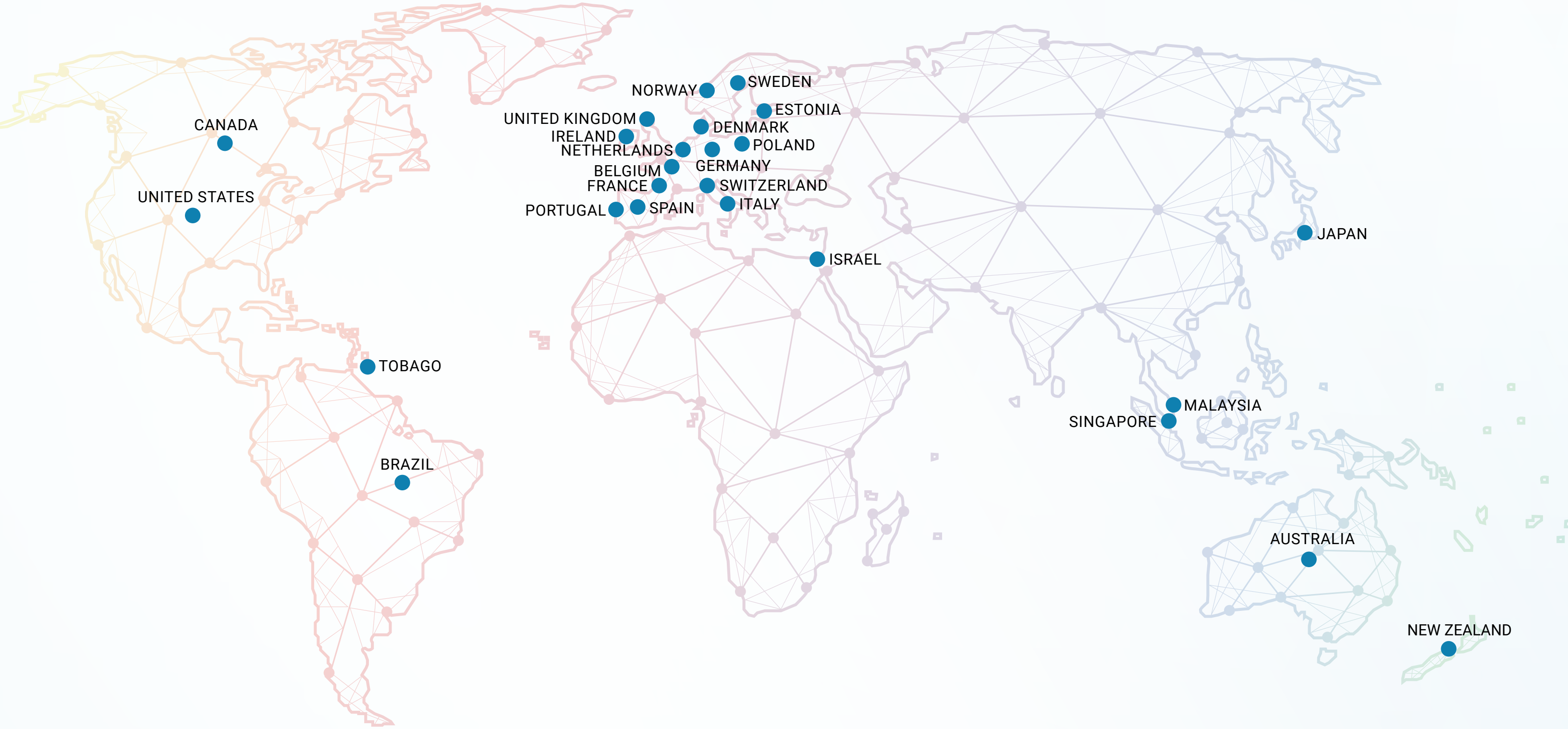
*“Honestly, I feel like you're doing great and providing great value. I can't think of more to do.”*

Medical Device Manufacturer

*“We get tremendous value from our Health-ISAC membership.”*

Chief Security Officer (CSO)
Pharma/Biotechnology

## Global Member  Headquarter Footprint



# 2023

## By The Numbers

**80**

Speaking events by Health-ISAC's leadership

**108**

New Member Organizations joined Health-ISAC

**10,000+**

Security Professionals in the Network Globally

**8,000+**

Followers on LinkedIn a 25% increase

**#1**

Ranking On LinkedIn in Post Engagements

**#2**

for total and new followers (among other ISACs)

**900**

Member Check-ins

**16**

Number of countries that held events

**140+**

Countries Represented

**95.1%**

Member Retention

**250,000+**

People had access to TLP Green & White Bulletins through Health-ISAC including Members, industry partners, and associations.

# A Collaborative Structure for Resilience

Members of the Health-ISAC community have the opportunity to connect with others in health security from around the world. Through daily chats, deep-dive discussions, and Member-presented experiences at global events, Members can collaborate and share rich, actionable information with their peers. Health-ISAC's Member Engagement Team serves as the central hub, providing access to services, tools, and information that enable everyone to engage fully within the community.

> *“Honestly, this is outstanding. I'm at a loss for words; I'm blown away with Health-ISAC being such an amazing value.”*

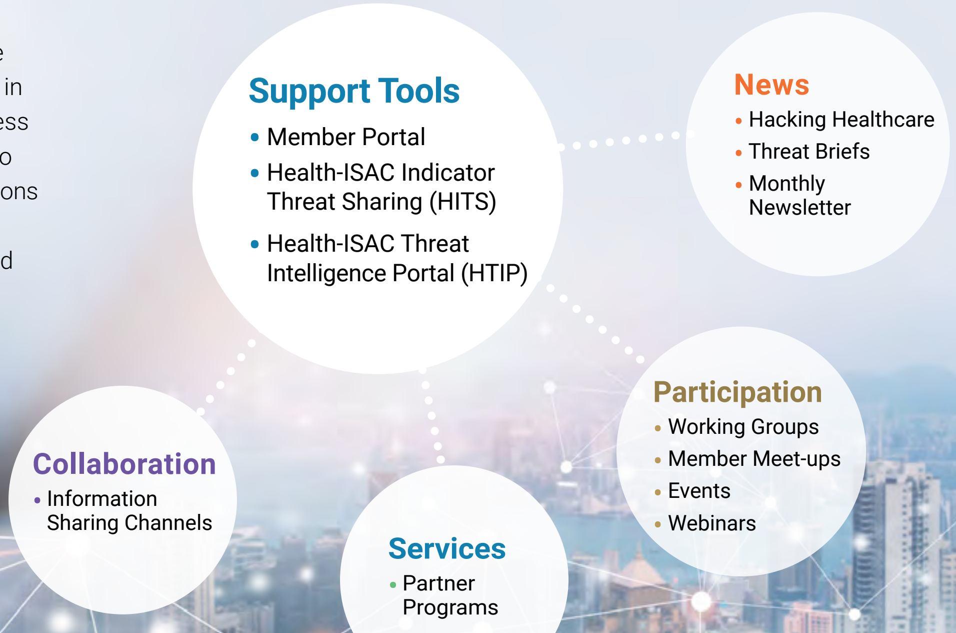
A prospective member's reaction
after hearing the Membership Benefits

> *“The freebies that Health-ISAC provides is amazing. Secure chat platform, Member portal, working groups that create best practices and whitepapers, educational opportunities, Member-hosted workshops, and tabletop exercises, four annual Summits: APAC, Europe and 2 in the US.”*

David Anderson, Member

## *Health-ISAC systems work together to connect the community*

In 2023, Health-ISAC made significant upgrades to Its technology to better serve and connect the community. These enhancements have resulted in improved real-time collaboration and better access to resources. Members now have more control to personalize their experience and manage notifications within the Member Portal. The Designated Point of Contacts for each organization have the added ability to add or remove their team members.



**Support Tools**
- Member Portal
- Health-ISAC Indicator Threat Sharing (HITS)
- Health-ISAC Threat Intelligence Portal (HTIP)

**News**
- Hacking Healthcare
- Threat Briefs
- Monthly Newsletter

**Participation**
- Working Groups
- Member Meet-ups
- Events
- Webinars

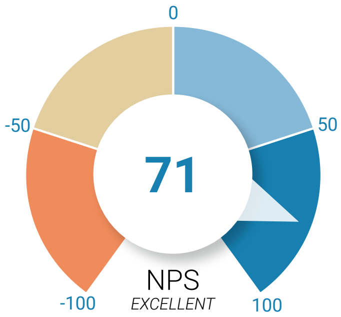
**Services**
- Partner Programs

**Collaboration**
- Information Sharing Channels

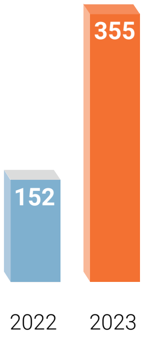
## *Health-ISAC Annual Member Satisfaction Survey*

Health-ISAC received an outstanding response from its members through the second annual Membership Survey in 2023. Health-ISAC was rated with a Net Promoter Score of 71, signifying a high level of satisfaction and willingness to recommend membership to others.

Net Promoter Score



Number of Responces

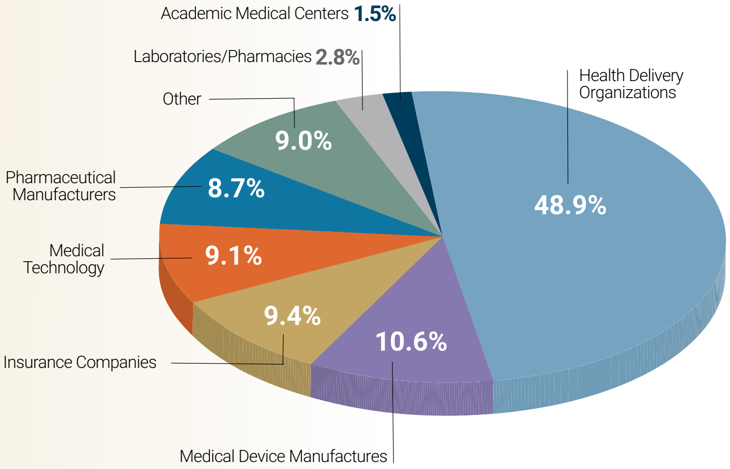


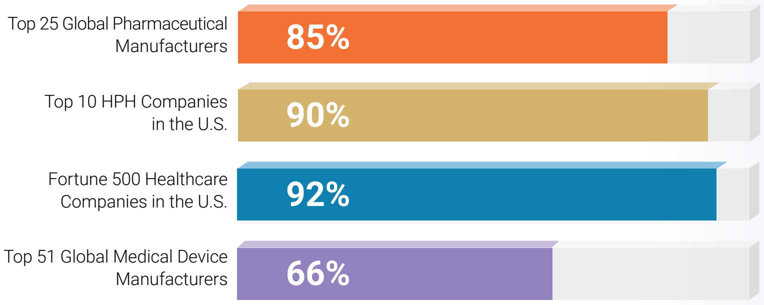
## *Diverse Member Composition across the Health Sector*

Health-ISAC connects security professionals within a large range of health organizations, from a regional clinic to a global health system, from a medical school to a medical device manufacturer.

> *"I really like the sharing of knowledge and the ability to ask questions and get responses from other organizations."*
>
> Health Provider

Member Composition





## *Leaders in the Industry*

Health-ISAC Membership represents different sizes and sections of the Health ecosystem, from <$1M annual revenue to $250B in annual revenue. The more Health Sector organizations that collaborate within Health-ISAC, the more resilient the global Health Sector is.

**900**
Number of Member Check-ins

**10,000+**
Health-ISAC Members connect on the secure chat platform

**18,000**
Average weekly secure chat messages

**72**
Webinars delivered in 2023

# The DNA of Actionable Data

**Health-ISAC's Threat Operations Center (TOC)** provides in-depth and wide-reaching analysis of actionable cyber and physical threat intelligence to Members. Members use this information for timely action against phishing, ransomware, and other threats. The TOC produces actionable intelligence, including pre-public alerts, targeted alerts, vulnerability & threat bulletins, benchmarking surveys, situational awareness & physical security reports, daily cyber headlines, and webinar discussions for up-to-the-minute updates on current threats. TOC analysts work with intelligence partners to monitor events and assess additional opportunities to provide value to membership.

## RESILIENCE BY THE NUMBERS

**1,044**
Targeted Alerts

**54**
Threat Intelligence Bulletins

**11**
Cyber Incidents

Achieved
**100%**
Of Member organizations connect to HTIP, Health-ISAC's Threat Intelligence Portal

**56**
Physical Security Threat and Incident Bulletins for Members & Employees

**91%**
Of Members subscribe to the Physical Security Daily Reports and Alerts

**2,973**
(248 Average)
Member Attendees at the Monthly Threat Briefings

**8**
TOC Spotlight and Hot Topics threat and vulnerability webinars presented to Members

**29**
Vulnerability Bulletins to Members

**33**
Geopolitical Alerts / Strategic Intelligence

*"The ability to draw on a multitude of organizations globally 24/7 is really important where an attack on one member organization is probably going to have impact on others."*

Tony Clarke, SVP of IT Digital Operations, ICON

# 57%

Member organizations have adopted the new automated Health-ISAC Indicator Threat Sharing platform (HITS)

Shared over

# 7,343

Member-to-Member Indicators of Compromise (IOCs)

# 1 🔒

Pre-public vulnerability notifications shared with Members from security researchers and technology vendors

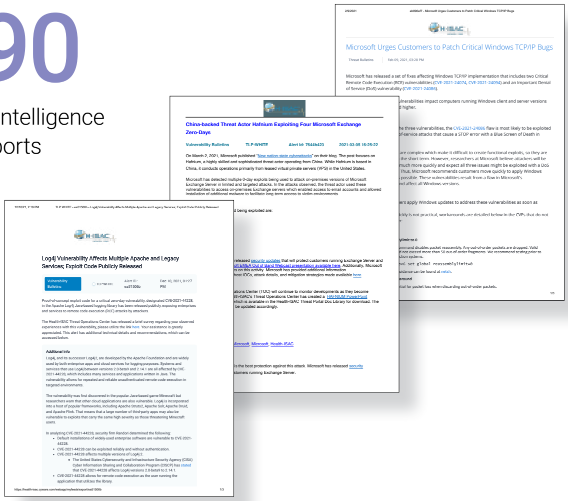
# 16

Member-initiated best practice surveys

> *“This is a great community and a great service. I rely on Health-ISAC to keep me "in the know" so I do not have to go hunting for threat briefs or vulnerability advisories. Even though I'm a member of other ISACs, Health-ISAC is by far the best value and the one group I rely on for my job.”*
>
> Healthcare Provider

# 190

Finished Intelligence Reports



2/9/2021 eb890ef7 - Microsoft Urges Customers to Patch Critical Windows TCP/IP Bugs

Microsoft Urges Customers to Patch Critical Windows TCP/IP Bugs

Threat Bulletins | Feb 09, 2021, 03:28 PM

Microsoft has released a set of fixes affecting Windows TCP/IP implementation that includes two Critical Remote Code Execution (RCE) vulnerabilities (CVE-2021-24074, CVE-2021-24094) and an Important Denial of Service (DoS) vulnerability (CVE-2021-24086).

ulnerabilities impact computers running Windows client and server versions d higher.

he three vulnerabilities, the CVE-2021-24086 flaw is most likely to be exploited of-service attacks that cause a STOP error with a Blue Screen of Death in

are complex which make it difficult to create functional exploits, so they are the short term. However, researchers at Microsoft believe attackers will be much more quickly and expect all three issues might be exploited with a DoS Thus, Microsoft recommends customers move quickly to apply Windows possible. These vulnerabilities result from a flaw in Microsoft's nd affect all Windows versions.

ers apply Windows updates to address these vulnerabilities as soon as

ickly is not practical, workarounds are detailed below in the CVEs that do not r:

ylimit to 0

ommand disables packet reassembly. Any out-of-order packets are dropped. Valid d not exceed more than 50 out-of-order fragments. We recommend testing prior to ction systems.

```
v6 set global reassemblylimit=0
```

uidance can be found at netsh.

around

tial for packet loss when discarding out-of-order packets.

1/3

China-backed Threat Actor Hafnium Exploiting Four Microsoft Exchange Zero-Days

Vulnerability Bulletins TLP:WHITE Alert Id: 7644b423 2021-03-05 16:25:22

On March 2, 2021, Microsoft published "New nation-state cyberattacks" on their blog. The post focuses on Hafnium, a highly skilled and sophisticated threat actor operating from China. While Hafnium is based in China, it conducts operations primarily from leased virtual private servers (VPS) in the United States.

Microsoft has detected multiple 0-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. In the attacks observed, the threat actor used these vulnerabilities to access on-premises Exchange servers which enabled access to email accounts and allowed installation of additional malware to facilitate long-term access to victim environments.

d being exploited are:

released security updates that will protect customers running Exchange Server and oft EMEA Out of Band Webcast presentation available here. Additionally, Microsoft s on this activity. Microsoft has provided additional information host IOCs, attack details, and mitigation strategies made available here.

ations Center (TOC) will continue to monitor developments as they become lth-ISAC's Threat Operations Center has created a HAFNIUM PowerPoint hich is available in the Health-ISAC Threat Portal Doc Library for download. The be updated accordingly.

icrosoft, Microsoft, Health-ISAC

is the best protection against this attack. Microsoft has released security stomers running Exchange Server.

12/10/21, 2:19 PM TLP WHITE - ea51506b - Log4j Vulnerability Affects Multiple Apache and Legacy Services; Exploit Code Publicly Released

Log4j Vulnerability Affects Multiple Apache and Legacy Services; Exploit Code Publicly Released

Vulnerability Bulletins | TLP:WHITE | Alert ID : ea51506b | Dec 10, 2021, 01:27 PM

Proof-of-concept exploit code for a critical zero-day vulnerability, designated CVE-2021-44228, in the Apache Log4j Java-based logging library has been released publicly, exposing enterprises and services to remote code execution (RCE) attacks by attackers.

The Health-ISAC Threat Operations Center has released a brief survey regarding your observed experiences with this vulnerability, please utilize the link here. Your assistance is greatly appreciated. This alert has additional technical details and recommendations, which can be accessed below.

Additional Info

Log4j, and its successor Log4j2, are developed by the Apache Foundation and are widely used by both enterprise apps and cloud services for logging purposes. Systems and services that use Log4j between versions 2.0-beta9 and 2.14.1 are all affected by CVE-2021-44228, which includes many services and applications written in Java. The vulnerability allows for repeated and reliable unauthenticated remote code execution in targeted environments.

The vulnerability was first discovered in the popular Java-based game Minecraft but researchers warn that other cloud applications are also vulnerable. Log4j is incorporated into a host of popular frameworks, including Apache Struts2, Apache Solr, Apache Druid, and Apache Flink. That means that a large number of third-party apps may also be vulnerable to exploits that carry the same high severity as those threatening Minecraft users.

In analyzing CVE-2021-44228, security firm Randori determined the following:

- Default installations of widely-used enterprise software are vulnerable to CVE-2021-44228.
- CVE-2021-44228 can be exploited reliably and without authentication.
- CVE-2021-44228 affects multiple versions of Log4j 2.
  - The United States Cybersecurity and Infrastructure Security Agency (CISA) Cyber Information Sharing and Collaboration Program (CISCP) has stated that CVE-2021-44228 affects Log4j versions 2.0-beta9 to 2.14.1.
- CVE-2021-44228 allows for remote code execution as the user running the application that utilizes the library.

https://health-isac.cyware.com/webapp/myfeeds/export/ea51506b 1/3

SecOps Stories: Cyber Threat Intelligence, Artificial Intelligence, and Risk
AMGEN

## CYBER THREAT INTELLIGENCE, STRATEGIC INTELLIGENCE, AND PHYSICAL SECURITY

### *Targeted Alerts*

Health-ISAC's Threat Operations Center (TOC) published 1,044 Targeted Alerts in 2023 to Member and non-member organizations in the health sector. Targeted Alerts warn organizations of high risks specific to their network—including things like vulnerable servers, cybercriminals selling access to their networks, stolen intellectual property, and compromised credentials.

**Top 5 Targeted Alerts in 2023**

1. DICOM Exposure
2. Targeted DDOS Mitigation - Killnet
3. Compromised Credentials and Infrastructure
4. MoveIT Vulnerabilities
5. Remote Desktop Protocol (RDP) Exposure.

### *Member Best Practice Surveys*

Health-ISAC conducted 16 surveys in 2023, capturing Member feedback in a variety of useful and timely topic areas. Survey results help all Members determine what is state-of-the-art and what would be considered best-practice for operational areas. Survey topics come from the Members and a few examples are listed here:

- Email Phishing
- Cybersecurity Frameworks
- Security Risk Assessments
- SIEM Product Usage
- Identity & Access Management
- Active Shooter Training
- Threat Actor Tracking
- Passive IoT/Medical Device Monitoring Tools
- Endpoint Patch Remediation
- Internship Program

The number of Targeted Alerts sent in 2023 **increased by 281%** over the number sent in 2022.

# The DNA of Actionable Data *Continued*

### *Internship Program*

In line with Health-ISAC's ongoing commitment to developing talent and partnering with the local community in Orlando, Florida, the internship program allows University of Central Florida students to benefit from hands-on training and experience. In 2023, Health-ISAC sponsored two Threat Analyst interns and a Cyber Security Research intern. The interns supported monitoring and analyzing security threats in the health sector, actively engaged in ongoing projects and research, and contributed to content creation.

### *Biweekly Geopolitical Watchlist, Enhanced with Deep-Dive Analytics*

Health-ISAC provides a biweekly snapshot of the geopolitical issues that could impact the delivery of healthcare globally. In 2023, the TOC added Collaborative Deep-Dive Analytics and strategic deep-dives into complex geopolitical developments that affect the global health sector. These reports examine geopolitical developments and provide a healthcare-specific analysis of events as well as resilience recommendations.

A few examples include:

- Semiconductor Shortage and Strategic Importance Drive Western Subsidy Programs
- Assessment of Cyberspace Solarium Commission 2.0 Report and U.S. Critical Infrastructure Security
- The Supply Chain Impacts of the European Union's Pharmaceutical Reform
- Risks and Opportunities of Increased Arctic Access.

Geopolitical Implications of the G-20 Summit

The Supply Chain Impacts of the EU's Pharmaceutical Reform

Risks and Opportunities of Increased Arctic Access

### *External Collaboration*

In 2023, Health-ISAC worked with external partners, including industry associations, goverments and law inforcement agencies around the world. Some of these contributions included:

- World More Than a Password Day - Spearheaded by the Global Cyber Alliance, Health-ISAC joined a coalition of nonprofit organizations to promote Common Guidance on Passwords
- Health-ISAC partnered with the American Health Information Management Association (AHIMA) to develop an entry level training program designed to up-skill employees to perform basic cybersecurity functions as a cost-effective answer to address the staffing and talent shortages in the industry. In 2023, the first course was launched – Cyber Threat Intelligence (CTI) and more courses are in development.
- The American Hospital Association (AHA) and Health-ISAC continued to partner and collaborate on a number of initiatives, including intelligence sharing, Member outreach, and strategic reporting.
- Health-ISAC joined Microsoft & Fortra as co-plaintiffs on a federal civil action designed to disable cyber-criminal infrastructure using Cobalt Strike to distribute ransomware targeting the health sector.

GLOBAL CYBER ALLIANCE

AHIMA

American Hospital Association™

Advancing Health in America

Microsoft

> *"Being a member of the community has been one of the best decisions our organization has made. It's paid back tenfold in the short amount of time we've been members and it's allowed us to share with the community just as much as we are taking information from the community and build those bonds that will allow healthcare to be effective for our patients"*
>
> Krista Arndtt, CISO,
> United Musculoskeletal Partners

# The DNA of Actionable Data *Continued*

## *New Health-ISAC Threat Operations Center*

Health-ISAC moved to a new Headquarters office in Orlando, Florida. The move places Health-ISAC's Threat Operations Center (TOC) in a centrally located position for talent access as well as access by Members for workshops and training. Close proximity to universities and health organizations also makes it opportune for student internships and collaboration. The office configuration was built with a high-tech design perfectly suited for a Threat Operations Center. Health-ISAC is hosting Member visits and more at the new location.

> *"You are doing a good job and the community aspect is strong."*
>
> From a Laboratory/Pharmacy

## Global Threat Intelligence

In 2023, Health-ISAC's community of 10,000+ global threat intelligence analysts collaborated and exchanged ideas on topics ranging from internal phishing campaign tests, assessing AI, red team/purple team vendor recommendations, to scam calls directed to individuals (at home), and leveraging secure SMS communications with patients.

### TOC Spotlight webinars included:

- "A Primer on ChatGPT and Large Language Models"
- "Cyber Security Issues and Challenges with Large Language Models (LLM) like ChatGPT"
- "ChatGPT & LLMs: Regulation and Risks"
- "Lockbit Ransomware Attack"
- "IANS InfoSec Budget Benchmark Report: Focus on Healthcare"
- "Decoding HTTP/2 Rapid Reset Zero-Day (CVE-2023-44487) Exploited"

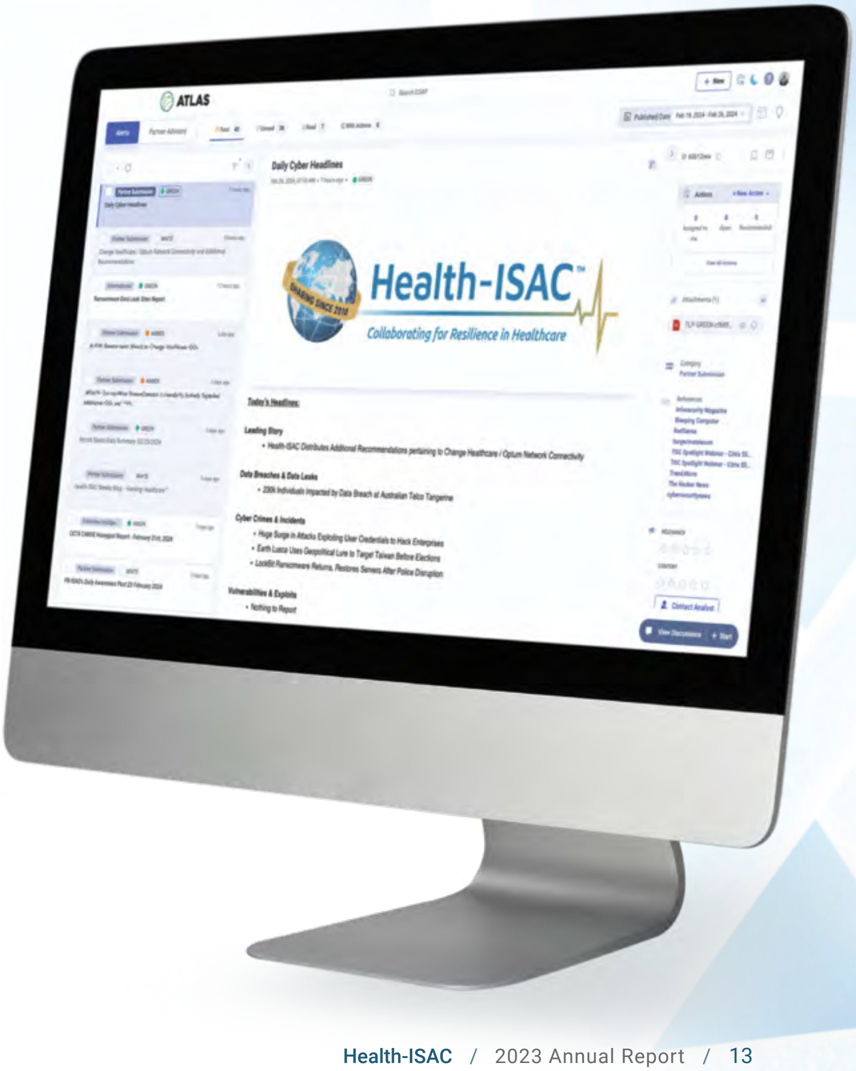
## ATLAS

Working with Cyware, Health-ISAC created ATLAS, a platform to facilitate ISAC-to-ISAC sharing through the click of a button and enhance information sharing across all critical infrastructure sectors. ATLAS speeds up analyst productivity and introduces fewer errors — enabling ISAC-to-ISAC sharing without relying on copy and paste, which was the modus operandi for over 20 years.

Today, ATLAS is used by over 20 organizations — a dozen ISACs, several ISAOs, and several international CERT teams. Analysts can share content, make it available to all ISACs (and ISAOs), and import information easily into their own platforms.

Health-ISAC will continue to expand the capabilities of ATLAS and recruit more information-sharing communities to broaden cross-sector collaboration and bring more timely threat intelligence to Health-ISAC Members.

> *"We haven't been members for long, but the information and resources are invaluable."*
>
> Healthcare Provider



Daily Cyber Headlines

Today's Headlines:

Leading Story

- Health-ISAC Distributes Additional Recommendations pertaining to Change Healthcare / Optum Network Connectivity

Data Breaches & Data Leaks

- 230k Individuals Impacted by Data Breach at Australian Telco Tangerine

Cyber Crimes & Incidents

- Huge Surge in Attacks Exploiting User Credentials to Hack Enterprises
- Earth Lusca Uses Geopolitical Lure to Target Taiwan Before Elections
- LockBit Ransomware Returns, Restores Servers After Police Disruption

Vulnerabilities & Exploits

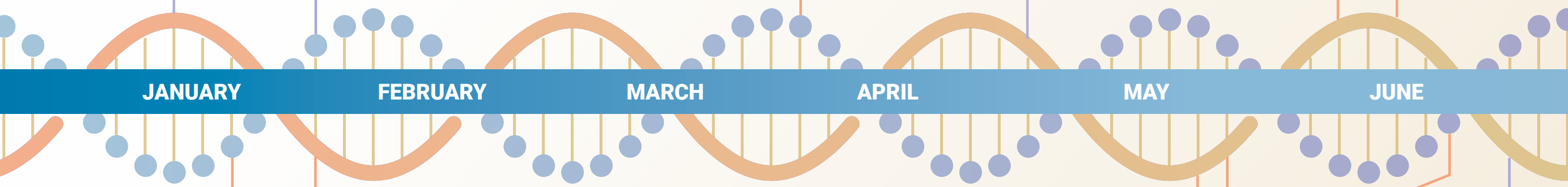
- Nothing to Report

# Top Incidents and Vulnerabilities of 2023

Health-ISAC's Threat Operations Center (TOC) disseminated over a thousand Vulnerability, Threat, and Incident bulletins throughout the year. Below captures a selection of the most prevalent incidents and vulnerabilities during 2023.

● *Purple highlights indicate Physical Threats*

● *Orange highlights indicate Cyber Threats*



**1/16/23**
**Physical Security Report** Tens of Thousands Impacted by Severe Weather in California

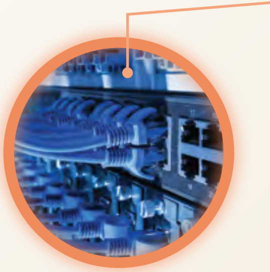
**1/25/23**
**Threat Actors** Using Remote Monitoring and Management Software For Persistent Access on Victim Networks

**2/2/23**
**Physical Security Report** Protests Over Pharmacies Selling Abortion Pills

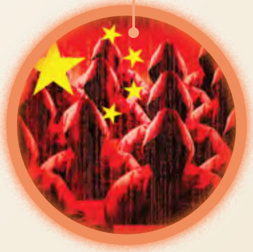
**2/3/23**
**Hacktivist Group Killnet DDoS** Attacks Actively Targeting Healthcare Organizations

**4/3/23**
**3CX Software Vulnerability** Creates Cascading Supply Chain Attack Impacts

**5/1/23**
**Widespread exploitation** of critical Zyxel firewall flaw



**5/22/23**
**Remote Code Execution** Vulnerabilities Impacting Cisco Small Business Series Switches



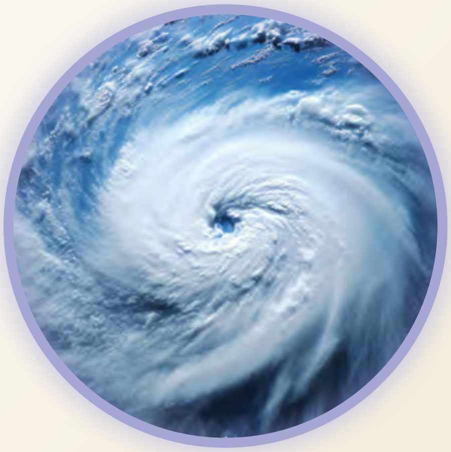
**5/24/23**
**China State-Sponsored Cyber Actor** Living off the Land to Evade Detection

**6/1/23**
**Progress MOVEit** Transfer Critical Vulnerability Actively Exploited; impacts thousands of organizations globally

**6/12/23**
**Fortinet FortiGate** SSL VPN Critical Remote Code Execution (RCE) Flaw

**6/21/23**
**Hacktivist Group PHOENIX** Targeting European Ambulance System

**6/28/23**
**Physical Security Bulletin** Canadian Wildfire Smoke Drifts into Northeast



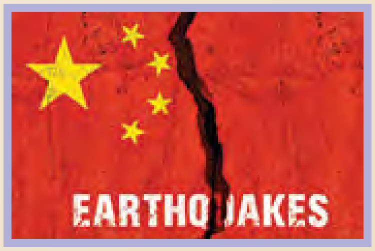
**7/14/23**
**Hurricane Calvin** Becomes First Major 2023 Hurricane in the East Pacific

**10/6/23**
**Global NetScaler** Gateway Credential Harvesting Campaign

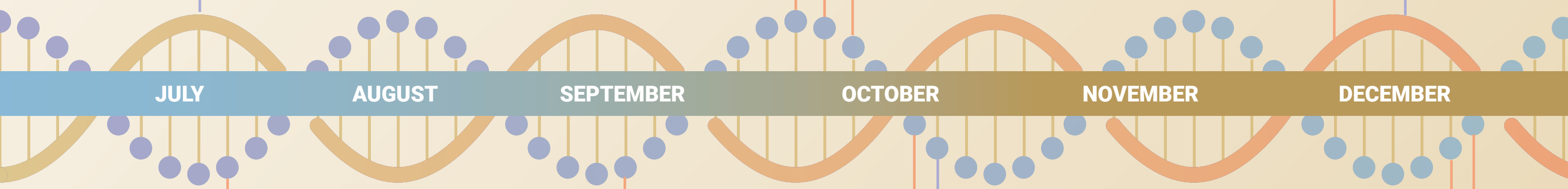
**10/9/23**
**Israel and Palestine War** Expected to Cause Increase in Cyber Activity

**10/10/23**
**Widespread Web Server Vulnerability** HTTP/2 Rapid Reset Exploited to Cause Denial of Service

**12/5/23**
**Adobe ColdFusion** Vulnerability Exploited for Access to Government Infrastructure



**10/19/23**
**Physical Threat Bulletin** Earthquake in Rural China



**7/18/23**
**Critical Vulnerabilities** Impacting Citirx ADC and Citrix Gateway

**9/19/23**
**QR Code Phishing** Attacks Used to Steal User Credentials

**10/16/23**
**Atlassian Confluence Vulnerability** Actively Exploited for Initial Access to Enterprise Networks

**10/18/23**
**Physical Security Bulletin** Protests Erupt In Response To Israel-Hamas War

**12/21/23**
**Member Reports Fake Websites** Targeting Colleagues in Region

**10/26/23**
**INC Ransomware** New Group Targeting Healthcare

# Industry Collaboration, Training & Awareness

## Health-ISAC provided ample preparedness and resilience opportunities for Members in 2023

### *Training*

- Held a two-day Leadership Development course presented and sponsored by Cisco Secure at both the Spring and Fall Americas Summits, where rising CISO Members learned valuable skills.
- Provided the new CTI Analyst Training at the Fall Americas Summit, where Analysts from ten Member organizations increased their knowledge, skills, and abilities.

### *New CyberThreat Intelligence (CTI) Training Program*

In 2023 Health-ISAC offered its first CTI Training during the Fall Americas Summit. Over 45 Members applied for the training. Thanks to a sponsorship from Cyware, 10 Members were selected from a pool of 45 applicants to receive a complimentary, all-expenses-paid professional development opportunity.

### *Webinars*

In 2023, Health-ISAC held 72 webinars to keep Members abreast of current trends. Some examples include:

- "Healthcare Security - View from the Cloud by Google"
- "Insights from 10 Years of Data Breach Monitoring" by RiskRecon, a Mastercard Company
- "Latest Cybersecurity Threats to the Healthcare and Cloud Sectors"
- "Google Discusses the Latest Threat Landscape Trends Impacting the Healthcare and Cloud Sectors"

### *Workshops*

Health-ISAC facilitated 21 global workshops with topics focused on:

- Life Sciences, Biotechnology, Biopharma
- Cyber Theat Landscape
- Incident Response and Information Sharing
- Legal & Regulatory Cybersecurity Issues
- Third-Party Risk Management
- Supply Chain, IT, and OT Security
- Artificial Intelligence/Machine Learning

> *"This is my first Health-ISAC workshop, I really enjoyed it. I would love to attend additional events in EMEA. Great work! Very enjoyable and love the networking elements!"*
>
> From a Dublin, Ireland workshop attendee

### *Exercises*

Members participated in seven preparedness and resiliency exercises with scenarios that focused on the world's geopolitical and economic climate and resulted in threat actors targeting the Health Sector.

**Just some of the Health-ISAC Exercise highlights include:**

- Health-ISAC conducted its fourth annual Americas Hobby Exercise in Washington, DC.
- The first annual Health-ISAC European Hobby Exercise was held in Dublin, Ireland and hosted by ICON.
- Custom Table Top Exercises created for the benefit of Health-ISAC Members to test their internal incident response processes.
- Four internal drills to test and improve staff preparedness and resiliency using scenarios designed to impact daily operations.

## *Insights and analytics were shared within the health sector to increase resilience.*

The exercise series explored challenges and opportunities facing the resiliency of the health sector due to the increasingly interconnected nature of cyber and physical systems and interdependencies.

TLP:WHITE APRIL 2022

Health-ISAC Preparedness & Resiliency Exercise Series After-Action Report 2022

ordr | MedSec | proofpoint

Health-ISAC

2023 State of Cybersecurity for Medical Devices and Healthcare Systems

FINITE STATE Securin Health-ISAC

Joint research project from Health-ISAC, Finite State, and Securin discovers nearly 1,000 vulnerabilities spanning 966 medical products.

Healthcare Heartbeat Quarterly Report provides observations of ransomware, cybercrime trends, and malicious actor forum postings that could potentially impact health sector organizations

TLP:WHITE Quarterly Threat Brief

Healthcare Heartbeat

2023: Q3

Cybersecurity Trends and Threats in the Healthcare Sector

Health-ISAC

## *CISCO LEADERSHIP TRAINING*

*"Blessed to be a part of this program with so many talented leaders! Thanks to Health-ISAC and Cisco for putting this program together to equip rising leaders with the skills needed to make a difference. 2 days of challenging leadership training with an InfoSec spin. I left with a new network of leaders to collaborate with and many takeaways to continue to grow along my journey!"*

Erik Gregg, Information Security Manager, Health First

*"I distinctly remember being told this program would change my life, and I can confidently say this is true. Thank you to the staff at Health-ISAC, Cisco, and everyone who made this a reality for us. It was a privilege to be chosen to attend, and I can't wait to pay it forward to other aspiring leaders. The friendships we made this week are so great!"*

Krista Arndt, CISO, United Musculoskeletal Partners

# Strengthening Resilience in Europe

## Expanding the team to foster a connected community centered on regional cyber and physical threats

Health-ISAC's mission in Europe is to foster a connected community and forum that centers on the cyber and physical threats to healthcare within the region. In 2023, Health-ISAC added two new positions located in Europe, a Threat Intelligence Analyst and a European Operations Director. Health-ISAC was also a founding member of the European Council of ISACs which was launched in 2023.

### *European Healthcare Cyber Threat Landscape Tour*

The tour was held between May and October 2023 in the following twelve cities:

- Zurich, Switzerland
- Milan, Italy
- Rome, Italy
- Helsinki, Finland
- Stockholm, Sweden
- Warsaw, Poland
- Berlin, Germany
- Lisbon, Portugal
- Barcelona, Spain
- Madrid, Spain
- Prague, Czech Republic
- Vienna, Austria

These events were free, half-day workshops covering relevant topics, specifically NIS2, Ransomware, Incident Response, and Information and Vulnerability Sharing.

**185 total attendees across all events**

**51 companies registered**

> *"It was a pleasure for us to have you here. Thanks to Health-ISAC and all participants; this workshop equipped us with practical and effective ideas for all of us to improve our information security posture."*
>
> Barcelona attendee

Ubiquiti Employee: Theft, Ransom, Press
Supply Chain
Credit Cor
West Roc
March/Sept. IBM CarePath & Nuance
Hacktivists
DDoS –
bulance Service, September Financial Institutions
Crimi
de Barcelona March 2023; ClOP Ra
stem
could make $100

**Vasileios Mingos**
European Operations Director

### *Inaugural Hobby Europe Exercise Health-ISAC*

The first annual Hobby Europe table top exercise was on April 20 in Dublin, Ireland.

– Large-scale cybersecurity incident scenario

– Over 30 participants, multiple organizations

# Contributing to Global Health Sector Resilience

> *"Cyber threats know no borders. Cybersecurity is a global problem and the more we can coordinate and collaborate together as one in the world's healthcare community, patient care will be safer and more resilient."*
>
> Denise Anderson, President & CEO, Health-ISAC

**Health-ISAC contributes to the sector by:**

- **Sending Targeted Alerts** to non-members to warn organizations of high risks specific to their networks.
- **Supporting the Cyber Working Group of the Health Sector Coordinating Council** (HSCC CWG) by:
  - Providing resources and financial funding
  - Contributing staff support to HSCC CWG initiatives.
  - Donating partial funding for the 2023 Cybersecurity for the **Clinician Video Training Series**
- **Publishing white papers** to share the newest best practices throughout the sector.
- **Producing and dispersing alerts and threat briefings** for non-members.
- **Interfacing with government officials and law enforcement** to educate them on issues and sector activities. In 2023 contributed to efforts to disrupt the Cobalt Strike Botnet.
- **Assisting critical infrastructure cross-sector collaboration** by contributing staff resources and technological support to the National Council of ISACs (NCI), which celebrated its 20th Anniversary in 2023.

# Collaborating for Resilience and Security in Medical Devices

## MEDICAL DEVICE SECURITY

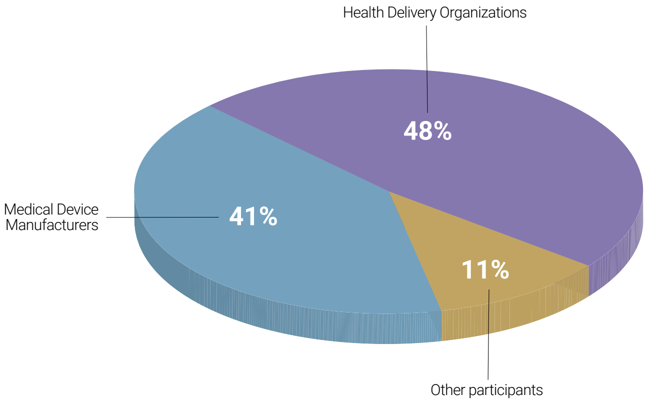
Health-ISAC is the only organization that brings together Medical Device Manufacturers and Health Delivery Organizations to support the security of Medical Devices within Healthcare. This collaboration is done through the Medical Device Security Council (MDSC) with 432 participants from 156 organizations, supporting over 140 countries around the globe.

> *"I like how open the community is. If there's something my company is struggling with, I can ask other MDMs and they're very open and very helpful, as well as hearing from the HDOs and the Insurers on how their processes work. The entire healthcare industry is playing catch-up; medical devices specifically and legacy devices. Not only do we need to comply with FDA requirements, we need to comply with customer requirements, so hearing from the customer is a good aspect as well."*
>
> Craig Foust, Manager, Device Security,
> Zoll Medical Corporation

### *Key Accomplishments in 2023:*

- Established the Health-ISAC Software Bill of Materials (SBOM) Repository in partnership with Cybeats to improve software component transparency and reduce time to patch vulnerabilities.
- Shared over a dozen medical device public advisories.
- Moderated two FDA Town Halls at Health-ISAC Summits
- Published Shared Responsibility whitepaper.
- Published Medical Device Customer Vulnerability Scanning whitepaper.
- Increased MDSC membership by 20% and monthly participation by 42%
- Demonstrated an overview of Daggerboard at the 2023 Spring Summit. DaggerBoard is an open-source vulnerability scanning tool developed by the New York Presbyterian infosec team that ingests Software Bill of Material (SBOM) files and outputs results in a human-readable format. Daggerboard is available for community use.
- Hosted four medical device roundtables at two Health-ISAC Summits.
- Performed community outreach through speaking engagements and podcasts.
- Signed a Memorandum of Understanding (MOU) with the Food and Drug Administration (FDA)'s Center for Devices and Radiological Health (CDRH)

## Medical Device Security Council Composition



*"Medical Device patching is always a big issue; how we defend our networks. Every device is different, every manufacturer is different, every environment you put the device into is different."*

Tom Mustac, Senior Director & Head of Systems, Cloud & Biomed Security
Mt Sinai Health System

### *2023 Health-ISAC SBOM Studio launched in partnership with Cybeats*

The Health-ISAC SBOM Studio, powered by Cybeats, launched in November 2023, and is a unique platform that allows medical device manufacturers (MDMs) to share medical device software information with health organizations that use the devices. This initiative is the first of its kind in any critical infrastructure sector, and it serves the greater community by promoting transparency. The platform will meet the FDA's regulatory guidance on an ongoing basis and reduce the level of effort health organizations need to make to understand vulnerabilities and patching requirements for the thousands of medical devices in their environments. The Health-ISAC SBOM Studio is a valuable tool for increasing transparency and making the sharing of security information easier and more efficient.

# Committees and Working Groups

The Member community comes together through committees, working groups, and councils to lead discussions and drive solutions for the industry. Work product items include: white papers, creating resource libraries and templates, presenting at events, and networking to share best practices.

> *"You get actionable takeaways that you can apply in your own business so you can achieve your goals."*
>
> Russell Johnson
> North Mississippi Health Services
> IAM WG and Risk Management WG

### *Health-ISAC Working Groups*

- Cybersecurity Analytics
- Cyber Threat Intelligence Program Development
- Cybersecurity Awareness and Training
- Diversity and Inclusion
- Identity and Access Management
- Incident Response (Joint Working Group with HSCC)
- Information Protection
- Information Security Risk Management
- IT Mergers, Acquisitions, Integration, and Divestitures
- Pharma and Healthcare Insider Threat
- Provider
- Purple Team
- Regional Tensions
- Security Architecture
- Security Engineering
- Social and Political Risks to Healthcare
- Software Security
- Third Party Risk Governance

### Health-ISAC New Working Groups in 2023

- Email Security
- NIS2 Implementation
- OT Security
- Physical Security (*see callout box*)
- Vulnerability Management

### Health-ISAC Committees

- Business Resilience
- Identity
- Threat Intelligence
  Health-ISAC Councils
- European
- Medical Device Security

> *"The biggest advantage of being in a working group is to understand and learn from each other's experiences as well as best practices."*
>
> Sethu Raman
> Organon

## *Special Interest Group*

Health-ISAC created a new Trailblazer Special Interest Group (T-SIG) program exclusively for Members of Small and Medium-sized Businesses in the health sector.

The program has three key components: a moderated secure-chat forum, a Member portal group, and a monthly T-SIG webinar series.

> *"It's a think tank where people bring their challenges, their thoughts, and discuss them in a safe environment to move the needle in a positive direction."*
>
> Tom Mustac
> Mt Sinai Health System

> *"The working groups are not just looking at what others are doing, but it is looking at what's coming on down the road."*
>
> Phil Alexander
> North Mississippi Health Services

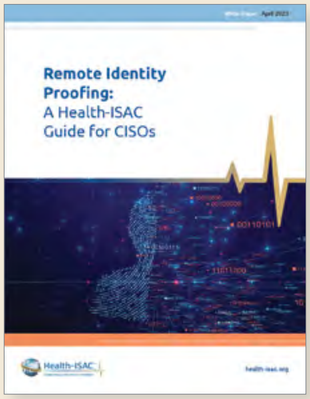
## Physical Security Working Group

The Physical Security Working Group is a place for health physical security professionals to come together and discuss challenges in regard to the safety and security of organizational personnel, patients, and constituents. While the group's primary focus is workplace violence and all aspects of health facility management that pertain to the prevention, mitigation, and handling of acts of aggression, the discussions also include elements of emergency preparedness and response, including natural disasters. The goal is to ensure that health facilities are prepared for emergencies whether they arise from workplace violence, acts of aggression, or unforeseen natural disasters.

Learn more about Working Groups:
**https://h-isac.org/committees-working-groups/**

## *2023 White Papers*

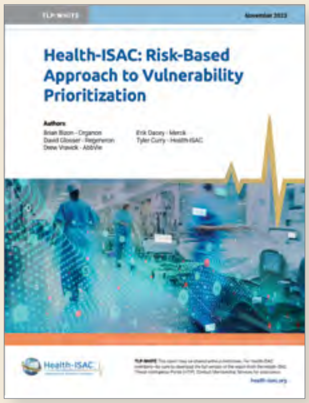
Health-ISAC Committees and Working Groups published six whitepapers in 2023 to connect Members and other Health organizations to actionable best security practices in the following areas:



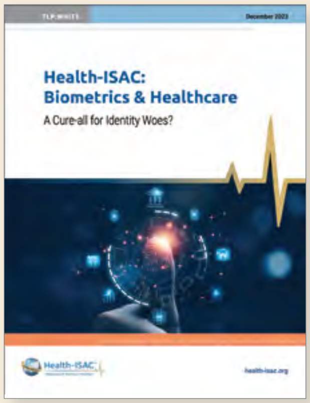
Remote Identity Proofing – A Health-ISAC Guide for CISOs

Improving Medical Device Security by Moving From Shared to Defined Responsibility
Health-ISAC

Defined Responsibility RACI

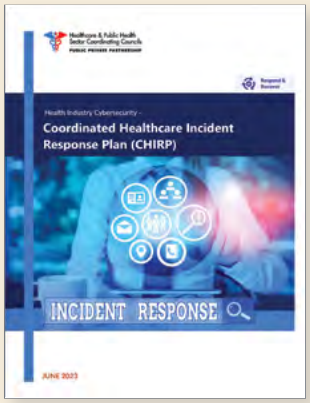

Health-ISAC: Risk-Based Approach to Vulnerability Prioritization
Health-ISAC

Risk Based Approach to Vulnerability Prioritization


Health-ISAC: Biometrics & Healthcare
A Cure-all for Identity Woes?
Health-ISAC

Health-ISAC: Biometrics & Healthcare, A Cure-all for Identity Woes?

Information Sharing Best Practices – updated*



Coordinated Healthcare Incident Response Plan

* The 2023 updates feature several additions, including a new information sharing type — Threat Defender Content and Resources Sharing, thoughts on legal protections with respect to information sharing & GDPR, and new case studies to provide solid examples of good information sharing.

# Global Collaboration for Resilience in Health

## HEALTH-ISAC GLOBAL SUMMITS

Health security subject matter experts gathered to share and learn from each other across the globe to strengthen the health sector. 2023 welcomed the inaugural APAC Summit in Singapore. Health-ISAC Summits are 'must attend' events full of informative sessions often led by Members and provide numerous networking opportunities.

> *"I'm hearing new ideas, fresh ideas; seeing things I hadn't thought of."*
>
> Edwin Drayden, Member

### March

**APAC Summit:** *Inaugural*

Singapore

Representing 4 continents, 75 attendees from 8 countries engaged in person at Health-ISAC's inaugural Asian Pacific Summit.

### May

**Spring Americas:** *Strike Back!*

Tampa, FL

A total of 613 attendees representing 9 countries, 37 states, and 210 companies connected in the Spring. 80 people attended virtually.

### October

**European Summit:** *Gateway to Security*

Dubrovnik, Croatia

Health-ISAC's third European Summit commenced in Dubrovnik, Croatia. 102 people attended in person, representing 18 countries.

### November

**Fall Americas:** *S'More Sharing with Health-ISAC*

San Antonio, TX

622 attendees represented 137 organizations from across the globe. Of those, 49 were virtual attendees, and 295 were first-time attendees!

## ANNUAL MEMBER AWARDS

### The Routhy Award

The Routhy Award was created in 2018 to honor first Chairman of the Board, Jim Routh, and is awarded yearly to honor other influential forces within health and the information security profession.

**The Routhy Award went to Anahi Santiago, ChristianaCare**

### The Hero Award

The Hero Award recognizes one Member each year who represents excellence in information sharing.

**The Hero Award was presented at the Fall Americas Summit.**

### The Securitas Award

The Securitas Award is presented to an individual or team from a Member organization judged to best exemplify collaboration, information sharing, active membership, and increased value to the cybersecurity community in the European region. 2023 was the inaugural year for this award. The Securitas Award was presented at the Health-ISAC European Summit.

**The Securitas Award went to Eva Telecka, MSD**

> *"As the new CISO for an organization hesitating over the benefit of Health-ISAC Membership, I convinced some team members to attend the 2022 Fall Americas Summit, and now they are fighting over who gets to attend the next Summit."*
>
> Sara Hall, CISO,
> Teladoc Health Inc.

> *"Great session on using a framework to speak to your board. It's not just some esoterica; it is applicable and practical information we can immediately take back to work and apply."*
>
> David Anderson, Member

# Complimentary and Discounted Solutions for Member Resilience

Health-ISAC engages with vetted service providers who embody the mission of increasing Health Sector resiliency against all hazards. This unique, solution-based community provides Members with exclusive cost-effective security solutions, offers Members valuable opportunities to evaluate security services with less risk, and expands Member security awareness.

> *“Mastercard is proud of our association with Health-ISAC... It’s about thinking big, bringing in different perspectives and moving fast. It’s about taking ownership, setting high standards, and then consistently delivering. Together, we build for the future, not just for today. As perfectly demonstrated in Portugal at the European Summit in October, Health-ISAC provides a unique setting for all Members to learn and strive for improvement in our collective practices and we look forward to remaining an active part of this valuable community”*

Steve Brown, Director Cyber Resilience,
Cyber & Intelligence Solutions – Europe

> *“Google Cloud was the first and only cloud organization to join Health-ISAC as an Ambassador partner last year. Since then, we've elevated this relationship to new heights. Our deep collaboration has allowed us to overcome challenges, solve problems, and create new opportunities in the healthcare industry. We are proud to team up with the Health-ISAC community to help build a stronger, more resilient healthcare ecosystem”*

Taylor Lehmann, Director, Office of the CISO,
Google Cloud

Google Cloud

mastercard

## AMBASSADOR PROGRAM

The Ambassador program was established to promote and accelerate the acceptance of a simple message — that a more secure and resilient health sector can be created by expanding a community for sharing threats, incidents, and best practices. Health-ISAC's Ambassador program is home to two well-known global brands that can reach health security audiences worldwide.

In 2023, the health community continued to face increased attacks, particularly the weaker and under-resourced hospital community. Threat actors took advantage of stretched budgets to exploit this weakness and demand higher ransomware payments.

During this time, the Ambassador program shifted from a consultative relationship to a more practical one, benefiting both Health-ISAC and its Members. The two Ambassador leaders — Mastercard and Google Cloud — provided thought leadership and useful tools for Health-ISAC's global security community. Cryptocurrency fraud tracking and cloud-based SIEM technology were among the newer solutions available to Members.

Health-ISAC also organized cyber threat landscape workshops in 12 European cities to educate its Members. Both Ambassadors participated in and supported these events by promoting them to customers or sharing hands-on thought leadership and best practices.

Learn more about the Ambassador Program: https://h-isac.org/ambassador/

## COMMUNITY SERVICES

Community Services providers offer their services to Health-ISAC Members at reduced fees or, in some cases, at no cost. In 2023, these 15 vested stakeholders shared their expertise across the Membership community at our Summits and in well-attended monthly lunchtime webinars exclusive to Membership. By providing unique solutions to Members, Community Service Providers increase resiliency for all Members across the health ecosphere, regardless of resource depth.

Learn more about Community Services: https://h-isac.org/community-services/

AHIMA

CENSINET

CYBEATS

GLOBAL CYBER ALLIANCE

RED SIFT

SAFEGUARD CYBER

SecurityRisk ADVISORS

AppOmni

CYWARE

flare

FINITE STATE

Prevalent

quad9

Security Scorecard

TOURO UNIVERSITY

# Building Awareness of Health Sector Threats

Health-ISAC was featured in news stories approximately every three days in 2023, showing an impressive 330% increase in media coverage as compared to the previous year. This remarkable achievement demonstrates that Health-ISAC is a reliable and authoritative source for health security information.

## Spreading the word about health and medical device physical and cyber security

Health-ISAC subject matter experts spoke about the threat landscape and best security practices across the globe in 2023.

### SME Speaking Sessions:

*"The PowerPuff Girls of Information Sharing - Joining Forces To Protect The Universe!"* panel at the 35th Annual FIRST Conference in Montreal

Health-ISAC President and CEO testifying at the United States Congress

*"Medical Technology Security Innovation"* at Cyber Future Foundation Summit

*"ACCE CE/IT Symposium on Securing IoMT Proactively "*

*"Medical Device Cybersecurity Program"* at Heartland Biomedical Association Symposium

*"From Hacked to Hero: Cyber State of the Union"* panel at ViVE

*"The Changing Medical Device Regulatory Environment"* at AMI eXchange

*"Information Sharing – Sounds like a good idea but where do I start and how do I get the approvals?"* Copenhagen CyberCrime Conference 2023

AHIMA23
CONFERENCE
OCTOBER 8-10, 2023
Baltimore Convention Center BALTIMORE, MD
Virtual | OCTOBER 26-27, 2023

*"Scoping the Cyberthreat Landscape & Staying Safe On-Line"* at AHIMA 23

*"Securing Increasing Threats to Critical Infrastructure"* Cyber Future Foundation panel (Davos, Switzerland)

### Podcasts:

*Addressing Cybersecurity Challenges in a Post-Pandemic World* in Risk Never Sleeps podcast

Build Diverse Teams or Die in Unspoken Security Podcast with Zerofox

*The Rise of Virtual CISO Neighborhood Watch with Health-ISAC* in Data Protection Gumbo Podcast - Episode 219

*The Genesis of Information Sharing* in Shot of Cyber podcast

### Media Mentions:

HIPAA JOURNAL THE HILL BECKER'S HOSPITAL REVIEW yahoo! finance asiaone EIN NEWS a digital news provider

## Media Mentions, Articles, and Blogs

In 2023, media reached out to Health-ISAC to comment on security events affecting the Health sector. A few of these titles are listed here:

THE WALL STREET JOURNAL.

*Healthcare Governance Body Warns Hospitals Face Debilitating Cyberattacks*
in **The Wall Street Journal**

Microsoft News

*Inside the Fight Against Hackers Who Disrupted Hospitals and Jeopardized Lives*
in **Microsoft News**

WSJ PRO CYBERSECURITY

*Biotech CEO Gets Hands-On After Cyberattack to Protect*
in **The Wall Street Journal Pro Cybersecurity**

*The Impact of the Israel-Hamas Conflict on U.S. Healthcare Cybersecurity*
in **Express Healthcare Management**

BANK INFO SECURITY

*Could Middle Eastern Cyberwarfare Spill Into Health Sector?*
in **Bank InfoSecurity**

GOV INFO SECURITY

*Medical Device Makers Taking a New Approach to Cybersecurity*
in **GovInfo Security**

ITBrief AUSTRALIA

*Concentric AI to debut autonomous data security at Health-ISACs 2023 Summit*
in **ITBrief Australia**

CNN

*Microsoft, Hospital Group Use Court Order To Disrupt Ransomware Attacks Aimed At Health Sector*
in **CNN**

HEALTHCARE INFO SECURITY

*Chinese, North Korean Nation-State Groups Target Health Data*
in **Healthcare InfoSecurity**

healthsystemCIO.com helping improve healthcare since 2010

*Sharing Cyber Incidents Makes Us All Stronge* in **HealthSystemCIO**

HEALTHCARE INFO SECURITY

*Authorities Warn Health Sector of Attacks by Rhysida Group*
in **Healthcare InfoSecurity**

TechTarget HEALTH ITSECURITY xtelligent HEALTHCARE MEDIA

*Researchers Observe 59% Spike in Medical Device Security Vulnerabilities*
in **HealthIT Security**

BANK INFO SECURITY

*Health-ISAC on Situational Awareness and Other Critical Concerns*
in **Bank InfoSecurity**

**56**
Media Mentions

**55**
Interviews

**6**
Press Releases

**95**
Speaking Sessions

**212**
**Total Media**

Health-ISAC, Inc.
226 North Nova Road, Suite 391
Ormond Beach, Florida 32174

Drève Richelle 161 M Box 57
1410 Waterloo, Belgium

**Health-ISAC.org**

Health-ISAC's mission is to empower trusted relationships in the global healthcare industry to prevent, detect, and respond to cybersecurity and physical security events so that Members can focus on improving health and saving lives.

## DON'T MISS THE UPCOMING 2024 SUMMITS

| APAC | Spring Americas | European | Fall Americas |
|---|---|---|---|
| March 19 – 21 | May 20 – 24 | October 15 – 17 | December 2-6 |
| **Cape Schanck, Victoria, Australia** | **Orlando, Florida** | **Athens, Greece** | **Phoenix, Arizona** |

Joining Health-ISAC as a Member strengthens not only your own organization, but also increases the resiliency of the global health sector. To discover more, send an email to CONTACT@h-isac.org