Executive Summary for CISOs: Current and Emerging Healthcare Cyber Threat Landscape

Announcements | TLP:WHITE | Alert Id: 6d48fae8 | 2024-02-21 14:28:59

Health-ISAC, in partnership with The American Hospital Association (AHA), has published the annual **Executive Summary for CISOs: Current and Emerging Healthcare Cyber Threat Landscape**. For 2024, the annual report includes sections on physical security, geopolitical activity, Threats to Medical Devices and Threats in Operational Technology (OT). New this year, the CISO Exclusive Market Summary, offers a comprehensive overview of global cybersecurity product trends based on the purchasing decisions of C-Suite executives across various industries.

The intent of the report is to raise awareness for senior leaders of the threats facing modern health organizations. The report can help influence cybersecurity budget and investment decisions for senior leaders and practitioners in the healthcare sector by providing an overview of the current cyber threat landscape and cybersecurity market projections moving into 2024. These market insights should illuminate global trends in cybersecurity solution purchasing, allowing C-suite executives and other decision-makers to make the most well-informed decisions.

In addition to the CISO Cybersecurity Market Summary, this version of the Health-ISAC Current and Emerging Healthcare Cyber Threat Landscape report for 2024 presents a condensed version of the key developments observed by Health-ISAC and its members in 2023, giving senior leaders a brief yet meaningful synopsis of the threat environment facing their organization going forward.

Report Source(s): Health-ISAC

Release Date: Feb 22, 2024 (UTC)

Tags: Health-ISAC Annual Threat Report, CISO Executive Summary, ATR, Health-ISAC Annual Threat Assessment, AHA, European Union (EU), APAC

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

HICP:

The Health Industry Cybersecurity Practices (HICP) refer to a set of guidelines and recommendations developed by the U.S. Department of Health and Human Services (HHS) to help healthcare organizations improve their cybersecurity posture. The HICP was created in response to the increasing threat of cyberattacks and data breaches in the healthcare sector, which has been a target for cybercriminals due to the sensitive and valuable nature of healthcare data.

The HICP resources are aimed at helping healthcare organizations of all sizes, including small, medium, and large entities. It provides practical and actionable guidance for managing and mitigating cybersecurity risks in healthcare environments, with a focus on five key cybersecurity threats: ransomware, phishing, loss or theft of equipment or data, insider threats, and attacks against connected medical devices.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.