TELOS ACA™

Telos®

Telos ACA for Healthcare

High-value data, legacy systems, and connected medical devices make hospitals and other healthcare organizations targets of attack.

The healthcare industry has been a growing target of opportunity for cyber criminals around the globe. Due to the financial and reputational impact of leaked HIPAA information, cyber criminals will leverage medical institutions through the use of ransomware. According to the U.S. Federal Bureau of Investigation (FBI), healthcare accounted for the highest number of ransomware attacks in 2021 among all critical infrastructure sectors, with 148, or nearly 25% of all breaches reported.[1] Healthcare organizations are actively targeted for the high monetary value and relatively easy accessibility of personal healthcare information.[2] These organizations require a new proactive strategy to counteract cyber-based threats.

The major difficulties for healthcare organizations are; the complexities of their IT systems, medical devices, and remote access; the requirement to have confidential patient data accessible for staff, both on-site and via remote access; and outdated technology. To effectively update technology, healthcare institutions need to ensure that all of their medical equipment and IT systems are updated and can be properly configured. Additionally, employees need to be trained on the new equipment to ensure consistent processes and patient care. All of these factors deoptimize daily operations and patient support during the installation period.

Healthcare Organizations Exposed to Risk and Threats

Unfortunately, due to the complexities of updating technology systems and integrating new cybersecurity solutions to support them, the majority of healthcare organizations choose not to pursue enhancements to their current infrastructure. The logistical confinement results in various access points remaining vulnerable to cyber threats, and with the requirement to make patients' health information accessible to various departments, HIPAA-covered information is always at risk.

Challenges:

Healthcare organizations have legacy systems and internet-connected medical devices that increase attack surfaces and the risk of breaches and malware

Litigation, criminal charges, the expense of ransomware and extortion, disruption to operations, patient safety, and reputational damage are all risks of vulnerable systems

Solution:

Proactive cyber threat intelligence that enables healthcare organizations to understand the hacker ecosystem surrounding their infrastructure

Actively target cybercriminals and cross-examine the identified threats with the organization's data traffic

Empower the organization to focus their resources on threat response and ensure that all personal healthcare information remains secure

The healthcare industry continues to have the highest average cost per data breach and that is because cyber criminals understand that these organizations are willing to pay. In 2021, a data breach in healthcare cost, on average, US $10.1 million, in comparison to the global average data breach, at US $4.35 million.[3] As healthcare continues to be targeted, cyber criminals' attack methods have been refined and updated. Ransomware had become more accessible due to the ransomware-as-a-service technology that cyber criminals employ, enabling non-technical criminals the opportunity to employ ransomware as well. As cybercriminals continue to evolve and employ new methods to successfully acquire monetary gain, the healthcare industry needs to evolve and employ new cybersecurity methods.

[1] *FBI, 2021 Internet Crime Report*
[2] *Advisory Board, "What hackers actually do with your stolen medical records" (3/1/2019)*
[3] *IBM, Cost of a Data Breach Report 2022*

Connected medical devices are just one factor in today's healthcare technology environments that are expanding the attack surface and creating vulnerabilities. Proactive cyber threat intelligence alerts security professionals in real time to IT and OT threats.

The Solution: Proactive Cyber Threat Intelligence

An excellent way to provide cybersecurity without hiring new employees or consultants is to implement a solution-as-a-service through a third-party vendor. Employing a cyber analytics service that enriches and analyzes all traffic transmitted in andout of your systems to hunt for malicious activity and identify cyber threat vectors provides subject matter expertise without requiring restructuring within the organization. Additionally, this will create a sustainable solution that is not impacted by positional shifts within the company. Cyber analytics will be able to monitor both IT and operational technology (OT). This ensures that any creative methods used to gain access through connected medical equipment are identified and mitigated. A solution of this scale will be able to ingest the data, successfully illuminating the hacker ecosystem.

The Telos Advanced Cyber Analytics solution is a service that will mitigate these risks. Telos' solution will enable the customer to know in real-time what malicious activity is occurring, resulting in the cyber attack being stopped before any significant damage and financial impact occurs to the organization. Additionally, by implementing the security solution, the risk of class action for negligence is mitigated due to the organization taking all necessary steps to implement cybersecurity principles to both IT and OT systems. Telos Advanced Cyber Analytics will mitigate the risk of a data breach, malware, operation disruption, reputational damage, or long-term litigation expenses.

Learn more at
www.telos.com/telos-advanced-cyber-analytics/

Telos® Solutions that **empower** and **protect** the enterprise.™

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 | 1.800.70.TELOS | 1.800.708.3567 | info@telos.com | www.telos.com