Monitor and Defend Medical Devices in Real Time

Healthcare providers rely on a wide variety of medical devices to diagnose, treat, and keep patients alive. These devices directly attach to patients and bridge them with the local computer network. Cyberattackers can use this direct link to endanger patients. As critical infrastructure, devices cannot be shut down if an attack is underway. And devices like magnetic resonance imaging (MRI) machines are significant investments that often outlive the operating system (OS) refresh cycle. Healthcare security teams must be able to detect and respond to attacks leveraging medical devices and do so in a timely manner.

The Challenge: More Devices, Less Control

The healthcare IT environment is growing increasingly complex due to the rising number and variety of medical devices, many of which represent blind spots on the network. The devices are governed by contracts and Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreements, which vary in their effectiveness and inclusion of mandated security controls. The organization has no way of knowing whether vendors are adhering to information security best practices.

To further complicate matters, medical devices are not conducive to traditional security measures. For example, up to 75% of biomedical devices do not use encryption on the network. That means data can be easily read on the wire. Attackers could also perform man-in-the-middle attacks and send commands directly to the device once they interpret the network protocol and switches.

Organizations may install software on assets that reside in the data center, such as a Picture Archiving and Communication System (PACS) server, and passively monitor data and collect logs from devices that have built-in logging capabilities. However, organizations cannot conduct vulnerability scanning or directly collect logs from devices like infusion/insulin pumps, vital monitors and drug compounders.

The number of devices requiring a passive monitoring approach are on the rise. eICUs, for instance, are being deployed to provide 24/7 care across multiple hospitals utilizing two-way cameras, smart alarms, and other technologies to share real-time patient data with practitioners. Physicians are also using consumer-based IoT devices like Google Glass to improve treatment.

But that's not all. An increasing number of non-critical IoT devices are also connecting to the network. These devices are enriched with patient health information (PHI) that must be protected under HIPAA. For example, smart displays in patient rooms can pull data from the EHR system, such as the patient's name and diet requirements, and provide easy access to documentation related to the patient's current health concern. These devices commonly lack authentication, as they are always-on systems integrated with physician/nurse scheduling systems. While not focused on keeping the patient alive, the IoT devices introduce a rapid growth of vendor-managed IoT devices that pose security risks to the organization and the patient's ePHI.

How to Gain Visibility and Control

Healthcare organizations must have the ability to passively monitor network-connected medical devices. This requires complete visibility to ensure that every device is monitored, the network can be properly segmented, and devices can be tied into the network access control system. Visibility is also key to reducing the time to detect and respond to an attack.

Network monitoring provides the network and application visibility healthcare organizations need to monitor and secure medical devices. Whether the solutions are in the cloud or on-premises, the network and the services must be monitored in real time from a centralized point. A security information and event management (SIEM) platform allows healthcare organizations to see the traffic flowing to and from all the devices in the IT environment.

The LogRhythm NextGen SIEM Platform offers comprehensive, single-pane-of-glass visibility into legacy systems and cloud-based solutions, including all the medical devices on the network. LogRhythm can help bridge detection and response for security threats by correlating that with health records violations and other healthcare operational technology, such as medical devices and physical security. As a result, LogRhythm enables you to quickly respond to threats, whether it's an attempt to remotely control a device or exfiltrate patient data.

The NextGen SIEM Platform also monitors cloud services for alignment to compliance requirements. LogRhythm's prebuilt Health Care Compliance Automation Module provides a comprehensive security framework that helps protect your patients and improve your organization's security posture. The module features capabilities to help you comply with HIPAA and HITECH guidelines, including:

- Analysis rules built to support healthcare to monitor your environment, staff, and vendors for risks and policy violations associated with HIPAA and HITECH guidelines.
- Investigation queries designed to answer and address key questions associated with investigations and regulatory requirements.
- Prebuilt reports that directly map to HIPAA directives.

When integrated with the NextGen SIEM Platform, LogRhythm NetMon provides the real-time visibility and security analytics you need to monitor your organization's entire network. NetMon delivers rich data and deep insights to help you detect and respond to advanced threats, including data exfiltration. NetMon integrates with Epic and other healthcare systems in your IT environment.

Security orchestration, automation, and response (SOAR) from LogRhythm RespondX helps healthcare organizations automate workflows and accelerate threat qualification, investigation, and response. In other words, SOAR enables you to identify and stop attacks faster — reducing the risk of a data breach and reaching HIPAA's 500-record threshold. The LogRhythm NextGen SIEM Platform provides everything you need to incorporate SOAR technology. It easily integrates with your current and future technologies so your team can accelerate response and remediation.

LogRhythm: More Than Technology

LogRhythm knows healthcare. We have deep expertise in healthcare workflows and the nuances of security operations in a health IT environment. This is evident in our Health Care Compliance Automation Module and deep integrations with other health IT systems, which are designed to help take some of the challenges out of securing your healthcare systems and data. We also integrate with a number of healthcare systems used in telehealth and telemedicine, such as MedSec, ORDR, and Armis. LogRhythm can also support legacy and current operating systems.

To see how LogRhythm can help solve the unique challenges of monitoring medical devices and protecting patient data, schedule a demo today.

logrhythm.com/demo

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301

www.logrhythm.com

©2020 LogRhythm Inc. | UC1450_Aug20