Putting Healthcare-Specific Threat Intelligence to Work

Healthcare organizations are a prime target for cyberattacks. The continuum of care makes for a complex and varied landscape of users, devices, applications, and workflows that attackers can use as entry points into the network. Attackers can also threaten the disruption of critical life-saving services to carry out ransomware attacks. All of this activity generates data that can be used to hunt down attackers and stop them in their tracks.

Every industry has general indicators of compromised data, but healthcare organizations need quality data that is specific to their environment to help reduce the time to detect and respond to threats.

The Challenge: Getting Data That's Useful for a Varied Landscape

Identifying threats in the healthcare organization is a considerable challenge. From handheld tablets to magnetic resonance imaging (MRI) machines, from electronic health records to telehealth platforms, the scope and variety of the landscape requiring protection is broad. Then there's legacy medical devices and operational technology that can't easily be secured or upgraded, leaving the organization and its patients constantly vulnerable.

To further complicate matters, healthcare organizations are vulnerable to a variety of motives and targeted by every type of attacker. Nation-state threat actors may target research data or clinical trials data, while financial crime groups target physicians for tax or direct deposit fraud. Busy users may inadvertently leave data vulnerable while others abuse their privileges when they see an opportunity. The list goes on.

Threat intelligence can help security analysts track down threats in the environment, but that data often only tells part of the story. Organizations get disparate pieces of data, making it difficult to turn that data into something cohesive that can be useful in their analysis.

How to Gain Visibility and Control

Threat intelligence is actionable insights into vulnerabilities and the threat actors that exploit them. A strong, healthcare-specific intelligence source ensures that you can detect the latest industry attacks, threats, and motives targeting healthcare. It can be used proactively to detect attacks as they happen and reactively to see if you've already been compromised.

Healthcare-specific data can be obtained from organizations like Health Information Sharing and Analysis Center (H-ISAC). But there is no better threat intelligence than your own data—that's critical because if you know your own environment well, you can pick out the anomalies. In fact, biomedical and telehealth and other systems make it easy for you to monitor, detect, and respond because of the standardized nature for which they operate. Using your own data, you can easily detect and respond to deviations from normal behavior.

One way to obtain the visibility you need to make sense of threat intelligence is through network monitoring. Whether health IT solutions are in the cloud or on-premises, an analyst or security team must monitor the environment in real time and respond to any threats to their information systems, patients, and data.

A security information and event management (SIEM) platform provides visibility, integrates with threat intelligence, and alerts on the threats. The LogRhythm NextGen SIEM Platform offers comprehensive, single-pane-of-glass visibility into legacy systems and cloud-based solutions. The platform easily integrates with existing technology, including EHR systems, biomedical devices, and telehealth systems. LogRhythm can help bridge threat detection and response by correlating healthcare-specific threat intelligence with the event logs generated by patient care systems. LogRhythm provides contextual information to make threat intelligence actionable, enabling you to quickly respond to threats and avoid disclosure requirements.

Our Threat Intelligence Services (TIS) is an easy-to-use integration that operationalizes threat intelligence. TIS enables organizations to rapidly add and configure a variety of threat feeds, including H-ISAC and other threat intelligence sources specific to healthcare. We use Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) to integrate threat intelligence into our platform.

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.

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.

To see how LogRhythm can help solve the unique challenges of leveraging threat intelligence to protect the healthcare IT environment, schedule a demo today.
logrhythm.com/demo

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

www.logrhythm.com