USE CASE

ANOMALI

Healthcare/Hospital Systems

Keeping patients and their data safe

Use Case Summary

This organization is a large (20,000+ employees, 30+ person cybersecurity team) mid-Atlantic healthcare provider that needed to optimize its SIEM deployment along with other security controls. This was particularly challenging given the unique security considerations around sensitive patient data and the critical nature of healthcare services. Their security operations center routinely spent hours combing through alerts and running searches that would time out or produce inaccurate results. These inefficiencies led to high turnover within the technical staff and an increased risk to staff and patients due to delays in mean-time-to-detect IOCs.

Security Considerations

Healthcare providers are a particularly tempting target for attacks due to their heavy use of critical technologies (not just back-end systems but devices connected to patients) and the fact that hospitals cannot afford a moment of downtime.

- PHI (personal health information) protection
- Encryption of data at rest and in transit
- Access Controls - monitoring and enforcement of users access policies
- Data Loss Prevention - detect and prevent unauthorized data transfers or leaks of PHI
- Medical (IoT) Device Security - log and event monitoring, anomaly detection (unauthorized access, breaches, etc.), incident response
- Phishing/Email Security - analysis of email gateways, web proxies, user and network behavior, altering and incident response, data correlation
- Ransomware/Malware Protection - threat intelligence integration, data encryption monitoring, incident forensics, integration with endpoint security
- Incident Response and Recovery - incident triage, automated response actions, threat intelligence integration, post-incident analysis, and reporting
- Insider Threat Detection - data loss prevention, access control monitoring, alerting and incident response, IAM integration, audit trails, and forensics
- Cloud Security - centralized monitoring, real-time threat detection, alerting and incident response, data loss prevention, multi-cloud integration

Compliance Mandates

Healthcare is a heavily regulated sector with both financial and human impacts that can result from a breach. Anomali provides a multi-layer defense to respond to and facilitate adherence to compliance mandates.

HIPAA

Support for auditing, logging, and reporting

Audit Trails

Anomali offers comprehensive auditing trails and reporting to support healthcare-specific mandates

Personas Goals

Practitioner Goals

As a SOC Manager, my concern is the effectiveness of my security infrastructure and the ability of those controls to capture threat information across an unusually broad array of devices in a timely manner. Keeping up with continuous threats is a real challenge (particularly given the critical nature of our business). Mapping that in an actionable way to my internal attack surface is a fundamental challenge, and ensuring that my organization is aware of and able to respond to threats in a way that is timely and relevant is an area I often struggle against.

CISO Goals

As the CISO, I am ultimately responsible for the success of both our patient's welfare and our organization's security investments. I need to persuade executive management and our board of directors of the importance of investing in rapid-response solutions that are adaptable enough to manage a highly dynamic and diverse threat environment and provide an immediate and actionable perspective on how this affects our internal potential attack surface. And everything I describe needs to be done in business terms.

Anomali contribution

Anomali architected a solution that would solve for three main outcomes:

- Improved Alert Fidelity - lowering MTTR and raising team effectiveness
- Search simplification to allow for faster security searches across data
- Integration of threat intelligence into existing tools to improve consistency across the security organization

The organization deployed the Anomali Security Operations Platform, ingesting high-value logs from their EDR, Firewalls, and internal network, as well as connecting the Anomali Intelligence library to their perimeter controls. This gave them a dataset that would provide relevant results in the case of a security incident. During the POC, they were targeted by a ransomware group, KillNet, which specialized in DDOS style attacks. Using Anomali, this organization pinpointed a list of the known KillNet IOCs, and was able to push those to the perimeter controls in a matter of minutes, resulting in the prevention of over 1700 DDOS attempts during the two-week period. Additionally, the organization leveraged Anomali's natural language capabilities to continuously query and confirm no KillNet traffic had made its way into their internal networks.

Use Case Outcomes

Stopping attackers in their tracks

- Immediate correlation of external threats to internal telemetry
- Distribution of known threat vectors to perimeter defenses, preventing over 1700 DDOS attacks
- Ability to track KillNeet across their entire organization

This is an excellent example of Anomali's value-add; identify the threat, define its relevance, and immediately strengthen your security posture. Through the use of generative AI, threats can be automatically stopped and information disseminated across both the organization and the broader healthcare ecosystem (through ISACs) to prevent further attacks.

Anomali Capabilities

Anomali Security Analytics

Anomali Security Analytics gathers security telemetry from various security controls, such as endpoints, firewalls, cloud platforms, proxies, and DNS. This data is stored in a scalable cloud-native data lake, ensuring efficient storage and significantly reduced costs.

CoPilot

Anomali's generative AI solution, Copilot, enables immediate prioritized security responses based on detected threats, enhancing the speed and efficiency of incident response from cybersecurity analysts. Incorporating AI into the Anomali Security Operations Platform significantly accelerates product performance.

ThreatStream

As a high-performance threat intelligence product, ThreatStrream curates and enriches raw data from hundreds of diverse sources of threat intelligence, including Anomali Labs curated feeds, open-source OSINT feeds, specialized premium feeds, and information sharing and analysis (ISAC) centers.

Anomali is headquartered in Silicon Valley and is the Leading AI-Powered Security Operations Platform that is modernizing security operations. At the center of it is an omnipresent, intelligent, and multilingual Anomali Copilot that automates important tasks and empowers your team to deliver the requisite risk insights to management and the board in seconds. The Anomali Copilot navigates a proprietary cloud-native security data lake that consolidates legacy attempts at visibility and provides first-in-market speed, scale, and performance while reducing the cost of security analytics. Anomali combines ETL, SIEM, XDR, SOAR, and the largest repository of global intelligence in one efficient platform. Protect and drive your business with better productivity and talent retention.

ANOMALI