Case Study: Caduceus Health

Sector: Healthcare

Caduceus, Inc. supports over 2,500 providers on the Athena Health service platform with services ranging from data entry, coding, claim error dashboard workflows, un-postable routing, interface management, live operator patient call, scheduling center, and business intelligence analytics with pop health reporting. Whether looking for an end-to-end outsourced revenue cycle or just segments of the workflow process, Caduceus provides a customized service solution while staying secure and at a reduced cost.

Objective: Providing a Secure Business Environment

As a vendor in healthcare, Caduceus is trusted with sensitive information and it is crucial to take the necessary precautions against cyber attack. With high volume of transactions related to billing and collections, data is moving fast across the network while also undergoing human interactions through intensive digital processing.

- Data security (PHI and PII) is a major requirement for both data-at-rest and data-in-motion
- Integration with multiple vendors imply that many entry points for attackers
- Constant turnover leads to potential for misuse of access privilege

Traditional point solutions for cyber security were focused on solving a part of the problem with defined boundaries while leaving the rest on other solution types.

Seceon’s Cyber Security Solution with aiSIEM

Unlike traditional SIEM, Seceon’s aiSIEM relies primarily on behavioral anomaly detection to identify early signs of intrusion. After the solution was rolled out, it took 2-3 weeks for Machine Learning to build a baseline pattern, which got further tuned over time.

- The platform could correlate unusual network behavior (ports scan, outbound/inbound request, data transfer etc) and user entity behavior through ML and AI
- Context was enriched with Threat Intelligence information on blacklisted domains, URLs and IP Addresses
- Threat Indicators were generated in real time with clear indications of Zero-Day Malware, Brute-Force Attack and Web Exploits
- Network Control Policies and Custom Alerts were configured based on specific conditions

Visible Difference with Seceon aiSIEM

1. Eliminated potential legal issues and revenue loss associated with data breach
2. Reduced unnecessary alerts (false positives) to a very manageable level with Automated Threat Detection and Remediation
3. Served as deterrent for potentially malicious insiders and careless users
4. Notified SOC Analysts and IT Management instantly upon policy violation and custom alert conditions
5. Unburdened IT staff and cut expenditure on outsourcing with significant automation

As one of the customer executives noted – *“Some tools we reviewed were presented as turnkey but they neglected to tell us that they need 15 people to turn the key. Seceon can handle the lion share of the work looking for breaches that happen within our system and has reduced our workload from security standpoint being able to assure that the patient data is secured”.*