Healthcare Institution

Active Threat Analytics – Premier

Cisco Active Threat Analytics helped this top U.S. university healthcare institution protect patient data and reassure concerned executives through superior threat detection performance.

Customer Profile

- A top-ranked American university healthcare institution
- Heterogeneous networking equipment
- Fledgling security operations program

Solution

- Cisco Active Threat Analytics Premier
- A proven incident response methodology that addresses security challenges within the university's heterogeneous environment
- Expert security professionals

Key Takeaways

- A 99 percent reduction in the average number of redundant security events and alerts
- An average of more than 93 monthly hours saved for customer analysts and investigators
- Incorporated FBI threat intelligence to protect the university during the holidays

Security Challenge

A top American healthcare institution (part of a renowned university) had executives who were uneasy with their network security given the increasing sophistication and proliferation of cyber attacks. These executives wanted to limit the possibility of a breach. Losing valuable data to cybercriminals poses a serious risk for patients and can damage the trust in the healthcare institution's brand. Additionally, strict healthcare regulations put added pressure on the executives to ensure the healthcare institution had a robust security infrastructure.

To protect against potential cyber attacks, the healthcare institution decided to build and improve its own security operations. However, building these proved to be challenging for several reasons.

The healthcare institution had numerous, disparate security technologies, and it was having difficulty piecing the equipment together effectively to secure its network. Furthermore, the healthcare institution lacked an adequate level of security professional staffing. This deficit in security resources made managing the healthcare institution's network and the vast number of daily security events it received far too time intensive.

Cisco Solution

Because acquiring advanced security while adhering to budgetary restraints was the healthcare institution's top executive concern, Active Threat Analytics Premier was the best solution. Active Threat Analytics Premier is the most thorough of the three tiers and offsets costs while still providing complete security visibility..

Where the healthcare institution previously struggled to effectively use its security technology, Active Threat Analytics Premier provides its proven incident response methodology and toolset. The service integrates Cisco technology with the healthcare institution's third-party software and equipment and collects all security-related network activity into OpenSOC, a big data analytics platform for aggregation and sophisticated analysis. From here, Active Threat Analytics experts provided advanced detection and targeted remediation recommendations.

With the focused incident detection provided by Active Threat Analytics Premier along with trained security experts, the healthcare institution was able to efficiently use their current staffing and resources to run an effective security program. This expertise, coupled with the service's advanced analytics and established methodology, help to enable the superior level of threat detection that the healthcare institution executives sought.

Business Outcomes

The healthcare institution saved resources and limited its exposure to cyber threats by not having to piece together complex security technology and build an in-house security operation center.

The threat detection accuracy of Active Threat Analytics alerts on approximately 5000 unique and tuned events per month in the healthcare institution's network. Of these thousands of events, only 32 incidents, on average, are confirmed for remediation. This accurate filtration reduced redundant customer investigations and false security alerts by ninety-nine percent.

The healthcare institution saved an average of more than 270 hours due to the support from Cisco investigators and analysts who focused on the healthcare institution's high fidelity events. Without Active Threat Analytics Premier, the limited and overcommitted healthcare institution security staff would have been forced to analyze these events. The time and resources saved allowed the healthcare institution's security team to focus on key business initiatives instead of constant, taxing threat monitoring.

About Active Threat Analytics

Cisco Active Threat Analytics (ATA) integrates deep expertise with cutting-edge technology, leading intelligence, and advanced analytics to detect and investigate threats with great speed, accuracy, and focus. Our expert investigators monitor customer networks 24x7 from our global network of state-of-the-art security operations centers, providing constant vigilance and in-depth analysis as a comprehensive security solution.

www.cisco.com/go/securityservices