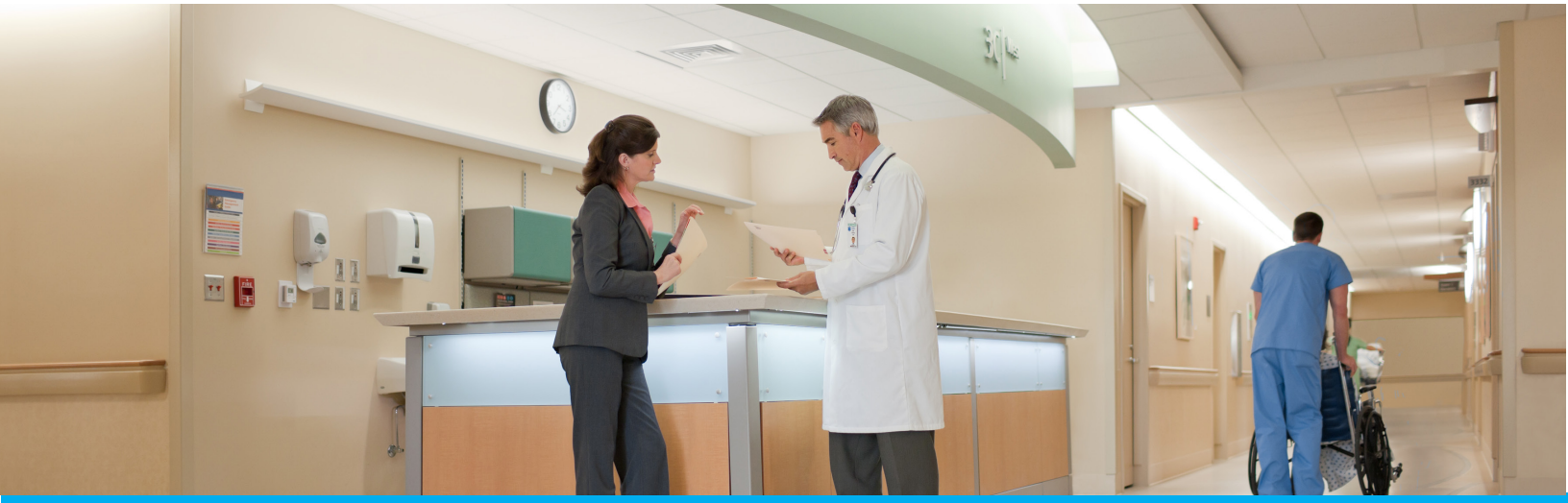
American Hospital

Active Threat Analytics – Premier



Cisco Active Threat Analytics Premier helped this hospital smoothly transition to a new managed security service and reduced the hospital's number of security alerts to a manageable level.

Customer Profile

- An American Hospital
- Dissatisfied with current managed security services
- Anxious about switching to either a new service or a do-it-yourself option

Solution

- Active Threat Analytics Premier
- Filtered security alerts and provided customized remediation recommendations
- Offered services as a layer on top of current capabilities to ease the transition to a new managed security service

Key Takeaways

- Potential for replacing the rest of the hospital's managed service with ATA Premier capabilities
- Less time responding to false alerts
- Improved overall security posture and protection from breach with more advanced managed security capabilities

Security Challenge

Effectively securing sensitive healthcare information is a top priority for this American hospital, which encountered challenging industry regulations and sophisticated cyber attacks. In such an environment, advanced security operations are a necessity.

However, this hospital was dissatisfied with its current managed security service because the service lacked key analytical capabilities and had an automated, rather than customized, process by which alerts were detected and delivered to the hospital. As a result, the hospital received too many alerts. Furthermore, the root causes of these numerous alerts were difficult to pinpoint because the service was outsourced to employees who recommended solutions with prepared scripts.

The hospital's executives were knowledgeable about security and understood that it should be a top priority. These executives knew that they needed to change their hospital's cyber security infrastructure but were uncertain about how to proceed. Building its own advanced security capabilities threatened an increased risk of breaches during the time it took to implement a new solution, while replacing their current provider to an entirely new managed security service was seen as risky and untested.

Cisco Solution

Active Threat Analytics Premier provides the most advanced security analytics capabilities to-date. This made Active Threat Analytics Premier the best solution for the healthcare company because it needed the best available filtration for false-positive security alerts that slowed its operations and burdened its security staff.

Active Threat Analytics separates confirmed incidents from thousands of daily security events by using advanced analytics: deterministic rules, statistical anomaly detection, and data science centric parameters. These analytics' approaches, in conjunction with Active Threat Analytics Premier full packet capture, create a unique network profile that is monitored against up-to-date community and Cisco intelligence and used to provide customized remediation recommendations.

What made Active Threat Analytics Premier even more appealing to the hospital was how Cisco was able to provide additional analytics capabilities without removing the hospital's current managed security service. This solution avoided exposing the hospital to increased security risk during a transition that would have occurred had the company built its own capabilities or switched to an unproven competitor service.

Business Outcomes

By first adopting Active Threat Analytics Premier as an add-on, the hospital gained additional time to consider next steps for upgrading its security infrastructure. Now, the hospital is positioned to continue adopting the entirety of the Active Threat Analytics Premier capabilities and start replacing its other managed service.

Active Threat Analytics Premier combines analytics, people, technology, and intelligence to provide an upgraded security service to the hospital. The speed and accuracy of threat detection coupled with the focus on the hospital's network with continuous 24-hour monitoring, full packet inspection, and proactive threat hunting with big data capabilities provides a level of vigilance not met by the former managed security service.

These capabilities decrease the hospital's risk of security breach and save valuable time and resources, which the company's security professionals can instead apply to core business functions.

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