Cisco Managed Threat Defense Service

Cisco Managed Threat Defense (MTD) Service helped this top American university defend against known intrusions, zero-day attacks, and advanced persistent threats.

Snapshot

Customer Profile

- Consistently ranked amongst the top American universities
- Teaching hospital
- Heterogeneous network equipment
- University executives concerned with security situation

Solution

- Cisco Managed Threat Defense Service
- Completely outsourced and managed security service
- Rapidly detects and responds to security events by analyzing network traffic, evaluating security telemetry, and using global intelligence

Key Takeaways

- Provided boardroom-level data and observations
- Identified 71 confirmed breaches in a 2 week period, providing clear remediation steps
- Incorporated threat intelligence from the FBI that kept the university safe from cyberattacks during the winter holiday

`Security Challenge

With a threat landscape that's growing more and more complex, organizations need new and innovative security solutions. But to keep those solutions working with the network environment and optimized, security experts who can continually monitor software and equipment are needed so that you can address the threats of today and the future, not the threats of last month.

Security threats are becoming so advanced and complex that it is hard to keep up, and finding the right security experts is difficult. When these security experts are found, hiring them can be very expensive.

A top American university (teaching hospital) was faced with a competitive security talent landscape and was struggling to parse the mountains of security data with which it was presented. The university realized that it needed to explore big data analysis techniques and correlation tools to monitor network activity in new ways. They also faced a heterogeneous equipment environment, making integrating equipment and delivering actionable insights even more difficult.

A security conversation was being held in the boardroom at the university. Heads of the school were concerned with the possibility of a breach and dealing with compliance issues relating to the sensitive student and medical data entrusted to them.

Cisco Solution

Cisco sees the networks in a way that many cannot, from end to end in a way that helps customers to protect themselves. Cisco brought its security experts to the university to collaborate on a solution that would fit the customer's needs. These experts integrated Cisco products with third-party software and equipment that enables the production of usable insights. This solution is onsite and managed by Cisco.

MTD Service captures full packet-level data and extracts protocol metadata to create a unique profile of a network and monitors it against up-to-date community and Cisco intelligence. Machine learning algorithms and predictive analytics are further used to detect behavior that stands out from normal network operations.

The real value for the university is that MTD sorts through mountains of data to find the targeted threats requiring vigilance and remediation. MTD separates the actionable intelligence from the chatter, showing the university how to remediate threats, providing:

- Network security monitoring
- Network anomaly detection
- Analysis of metadata
- Security intelligence feeds
- Sandboxing

All of these things together enable rapid response to potential threats.

Outcomes

The results were immediately apparent. MTD armed the chief information security officer with boardroom-level data and observations about security investments and the efficacy of its controls. MTD demonstrated the operational threats they were encountering with far greater visibility, and allowed the CSO to steer controls to where the threats were aimed.

The results have been compelling: In the last 2 weeks of the summer, Cisco MTD staff analyzed nearly 300,000 events, but notified the university about only 71 of those events. Those 0.02 percent of the event load were confirmed breaches requiring the university to remediate them. In each case, Cisco MTD investigators provided detailed mitigation and remediation steps, intimately fitted to their knowledge of the university's capabilities and network.

The superior MTD protection comes largely from Cisco information. Reliable threat intelligence enables discovery of threats in almost real time. As an example, Cisco MTD incorporated threat indicators released by the FBI after a December breach. While university students and staff were enjoying the holidays, MTD vigilantly hunted through the university network to spot the threats, alerting security staff if anything was found. This teamwork and tight cadence has enabled the university's security team to progressively speed its detection and remediation of cyberattacks, rendering employees, patients, and staff safer by the day.

Learn more about Cisco Managed Threat Defense Service or other Cisco Security Services.