proofpoint.

CUSTOMER STORY

Large Financial Institution Reduces Risk, Streamlines Incident Response and Protects from Advanced Threats

The Challenge

- Verify, prioritize and respond to suspected security threats in a timely and cost-effective manner

The Solution

- Proofpoint Threat Response

The Results

- Reduced average response time from hours to minutes
- Immediately eliminated false alarms
- Cut down on unnecessary PC reimaging by more than 80%

The Company

A large, high-profile financial services company has recently seen an increase in targeted cyber attacks. The company has a high volume of proprietary data and customer information in its data centers. And it has mission critical systems that require virtually 100% uptime.

The company has dedicated incident response teams and has invested in a wide variety of network security products. These include traditional and next-generation firewalls, a security information and event management (SIEM) platform and advanced malware detection platforms. Their heterogeneous environment includes networking equipment from Cisco, Juniper, Palo Alto Networks and Check Point, as a result of several recent corporate acquisitions.

The Challenge

Effective analysis requires additional context

The company has numerous certified security professionals on staff. However, the manual effort required to investigate each incident has affected the team's ability to respond quickly. This gives attacks time to cause significant damage before they can be remediated or contained. With each incident, the team must gather multiple pieces of data from various sources, which is a slow and laborious process. This information is then analyzed. This analysis includes cross-referencing data from a variety of external feeds (geolocation, reputation and WHOIS data) to understand the extent, severity and intent of the attack.

False positives increase response costs
Investigating and responding to incidents that are ultimately determined to be "false positives" has become a significant burden to the team. It limits their ability to identify true security attacks that cause damage. And it exposes the company to data loss or damage from benign events that turn out to be wild goose chases. What's more, the unnecessary reimaging of PCs has huge cost and productivity implications for end users and IT.

Advanced detection tools increase incident volumes Recently, the company deployed a FireEye solution to help identify and mitigate advanced persistent threats (APT) and zero-day attacks. Soon after, the staff discovered that they were able to identify a variety of malware exploits and attack traffic that had been previously undetected. This increased the overall volume of incidents that had to be dealt with by an already overextended team.

"Proofpoint Threat Response provides an immediate way to automate, prioritize and respond to security incidents in a way we never imagined possible. The old manual processes of researching each incident is automatically taken care of, giving our team the ability to focus on dealing with critical security incidents and immediate response."

Director of Incident Response

Limited response options
After investigating the threats detected by FireEye, the incident response team struggled to implement appropriate responses. They often used their existing security infrastructure to block the attacks and follow-on communication channels (command and control—CNC). Responding to an incident often required coordinating with the network operations team through the use of a ticketing system. This handoff delayed the response by hours, days and sometimes even weeks, depending on the load of the network team and their availability. And many of the serious attacks were discovered outside of normal business hours.

Heterogeneous infrastructure compounds the issue
The team faced one final problem. They needed to figure out how to effectively update multiple security devices from multiple vendors with consistency and accuracy. They were challenged with proprietary syntax from their security devices. This caused periodic misconfigurations and ineffective responses. Or even worse, it inadvertently took critical business systems offline.

The staff needed a solution that could quickly analyze and respond to threats by adjusting infrastructure policies across a variety of vendor devices. And it needed to happen in near real-time, with accuracy and little or no human intervention.

"Proofpoint gives our incident response team a platform that automatically collects additional context for every security incident. This dramatically reduces the time it takes to prioritize and swiftly respond, while enabling our team to contain bad actors enterprise wide."

CISO

The Solution

The Incident Response team chose the Proofpoint Threat Response threat management platform to help them respond quickly and effectively to the growing volume of security incidents. A key factor in their decision was the fact that it provided support for their existing security event sources, including their SIEM and FireEye WebMPS. And it supported their diverse range of firewalls from a variety of vendors.

The payoff

The company implemented Proofpoint Threat Response, and they were immediately able to respond to security incidents with a higher degree of accuracy and confidence. This gave them the ability to protect their people from a variety of advanced attacks.

Eliminating the enemy of time

Threat Response helped the team by collecting data for every security incident. This included reputation, WHOIS and GEO location for all external IP/hostnames, along with any identified command and control networks IP addresses.

Threat Response also collected additional data for internal IP addresses/hostnames. This includes Active Directory (AD) mappings, login activity and AD group memberships. This capability gave the team more clarity about the intended attack target and potential exposure. It provided dynamic, targeted data gathering that was specific to each security incident. And it eliminated the manual, time-consuming data-gathering tasks the team was handling for each security incident.

Reducing false positives

Using the PC data collection feature in Threat Response, the team dramatically reduced false positives and eliminated unnecessary PC reimaging. This feature enabled remote collection of specific indicators of compromise (IOC) from a user's PC. These indicators were then compared with the security incident to determine if that PC was compromised. And now the team can quickly identify which systems require remediation vs. systems that are false positives. This eliminates the costly and productivity impact of PC reimaging.

Taming incident volumes

The volume of incidents dramatically increased after implementing FireEye's advanced malware detection product. But Threat Response helped to prioritize the important incidents, eliminate false positives and automate critical responses. The team also defined automatic, real-time responses to block access to identified malware callback destinations. This eliminated a significant amount of their typical response workload. And they were able to gather PC data and automatically determine if it was compromised. This gave the team an immediate way to prioritize confirmed incidents vs. false positives.

Seamless and timely responses

The Proofpoint solution was integrated with the existing security infrastructure devices (Palo Alto Networks, Check Point and Cisco firewalls). This resulted in a dynamic security policy within each device that reacts to current threats targeting the company. Now when a response is taken (for example, blocking multiple CNC addresses), the device update is immediate. This eliminates the previously painful process of attempting to coordinate across multiple disparate teams.

The network operations teams liked the fact that the Proofpoint solution was not directly adjusting security policies, and instead relied on object groups used in predefined rules that were already in place. Every change is audited and notifications are generated so all teams are satisfied that the solution does not impact their existing compliance controls.

Heterogeneous changes with accuracy

Threat Response gave the team the ability to connect with their variety of security equipment. It ensured that a response to block IP addresses, hostnames and URL reported in security incidents was deployed consistently. And the team didn't have to define multiple UI or CLI commands, but instead relied on the natural device language capabilities of Threat Response.

After installing Proofpoint Threat Response, the response time to contain newly detected threats has been reduced from what was often hours, days, or even weeks, down to minutes or seconds.

The Results

After installing Proofpoint Threat Response, the response time to contain newly detected threats has been reduced from what was often hours, days, or even weeks, down to minutes or seconds.

The Proofpoint platform has enabled the incident response staff to implement workflows that ensure new threats are quickly prioritized and addressed

- Threats that are clearly malicious attacks are handled automatically by the Proofpoint platform
- Incidents that require additional research are given the attention needed in a timely manner
- The incident response team's productivity and ability to respond to critical incidents and lower false alarm research has dramatically improved

With the ever-increasing list of supported detection systems, threat feeds and enforcement devices supported by Proofpoint, the team can now take advantage of new technologies quickly. This makes Proofpoint Threat Response a key component of their expanding network protection efforts.

LEARN MORE

For more information, visit **https://www.proofpoint.com/us/products/threat-response**.