CASE STUDY

Financial Services Organization Sees Success with Smarter Threat Intelligence

ABOUT THE COMPANY

This Financial Services firm plays a key role in the global economy and they place an emphasis on ensuring their enterprise is protected as they are a constant target of many diverse adversary groups. Network security is a priority for this organization, as it must ensure that their data is safe.

THE THREAT LANDSCAPE

The threat landscape is forever expanding and adapting. Cyber threats have doubled from 2016 to 2017 with a 223% increase in traffic. In 2017, the number of detected security incidents soared to over 223 million, averaging 611,141 per day. With millions of malicious users hiding amongst billions of legitimate users, cybersecurity systems must be able to meet the breadth of today's cyber attacks. Without this solution in place, the next breach could be right around the corner.

One of the biggest factors in predicting breaches on a company's security stack is based upon which industry the organization is rooted in. Heavily regulated industries such as financial services have per capita data breaches that cost substantially higher than the overall mean. In fact, financial services organizations are consistently one of the top 10 industries targeted by threats like phishing attacks, URL and email malware attacks, and spam.

THE CHALLENGE

This financial services firm was unable to manage adversary changes to the infrastructure at their various data centers throughout the United States. The organization needed a way to gain situational awareness of specific threats to their company while correcting the high noise-to-signal ratio their security team saw from irrelevant or inaccurate sources of threat intelligence.

As a financial services organization, this company was aware of the high risk they faced from cyber attacks and wanted to ensure the privacy of their customers' records and integrity of their networks. This organization's security team needed a solution that provided fully correlated data of their network traffic as well as a way to operationalize relevant threat intelligence in real-time.

As a financial services organization, this company was aware of the high risk they faced from cyber attacks and wanted to ensure the privacy of their customers' records and integrity of their critical infrastructure.

The organization's security team needed an advanced solution that provided:

- Fully correlated cyber threat intelligence data that is constantly updated
- The ability to automatically filter out the noise and false positives against billions of IOCs
- Analytics and data to build an enhanced SIEM threat dashboard

Centripetal

THE SOLUTION

Centripetal provided a way for this organization to control what sources and types of threat intelligence are used to defend their network, this solution also allowed the security team to focus on delivering fast incident response and real-time threat landscape visibility for all datacenter locations.

Centripetal's sophisticated packet filtering combined with real-time Threat Intelligence feeds and analytics capabilities provided a way for this organization's security team to control what sources and types of threat intelligence are used to defend their network. Centripetal leverages criticality ratings, confidence, tags, and deep contextual associations to define granular policies for alerting and blocking. The Centripetal solution enabled the organization to input threat intelligence from their own research, open and private communities, and third party vendors for real-time protection of their network.

The solution provided the organization's security teams with the ability to focus their investigative resources to deliver faster-than-ever incident response and gain real-time visibility into the threat landscape over their multiple datacenter locations. In addition, it operationalized the threat intelligence to allow for immediate enforcement of dynamic threat indicators.

PERSISTENT THREATS REQUIRE PERSISTENT PROTECTION

Centripetal enables large dynamic policies with high fidelity indicators to actively protect the network in real-time. Centripetal's solution enforces cybersecurity policies with millions of rules, at full line rate and without degradation in network performance or user experience. Once deployed, the level of scale allowed for this company's analysts to detect threats that had previously gone unnoticed. Their previous cybersecurity system simply could not scale to meet their needs.

THREAT INDICATOR MATCHES

Centripetal provided real-time feedback to the Security Operations Center (SOC) team conducting research on the network. Indicators of compromise were identified and attributed to activity with known internal hosts on the network in multiple locations. This led to a faster collaboration on the severity of the incident and targeted efforts for the incident response team.

THE RESULTS

This financial services firm has seen continued and demonstrable success in protecting their network.

The current deployment allows for fully correlated data inbound and outbound. The combined solution enabled the organization to spot previously undetected outbound network threats and provided a level of visibility and control that they did not have with their previous security solutions. They were able to identify malicious hosts on their network and block outbound communications to known bad actors without disruption. The integration allowed the security team to react faster to threats and act according to threat data.

This Active Threat Blocking solution has enabled this customer to systematically regain control of their network and keep their data secure.