CENTRIPETAL

CASE STUDY

FINANCIAL SERVICES ORGANIZATION OPERATIONALIZED RELEVANT THREAT INTELLIGENCE IN REAL TIME

OCTOBER 2022 | CENTRIPETAL.AI

CENTRIPETAL

For financial services companies and institutions, it's becoming increasingly challenging to protect infrastructure and payment systems against evolving and complex cyber-attacks and fraud. The cost of a breach to a financial organization averages $5.97 million, the second highest of any industry.

In 2022, 74% of financial institutions experienced one or more ransomware attacks, and 63% of those institutions paid the ransom.

THE CHALLENGE

This particular financial services firm was aware that they faced a high risk of cyber attacks and wanted to ensure both the privacy of their customers' records and integrity of their networks.

With data centers spread across the United States, it had become impossible for the firm to manage attacks on their infrastructure. They not only needed situational awareness of specific threats to their company, but also a way to correct the high noise-to-signal ratio from misleading and inaccurate sources of threat intelligence monopolizing the security team's time.

The organization's security team required a solution that allowed operationalizing relevant threat intelligence in real-time.

THIS INCLUDED:

- Fully correlated cyber threat intelligence data continuously updated in near real-time
- The ability to automatically filter out noise and false positives against billions of indicators of compromise (IOCs)
- Comprehensive data and analytics to build an enhanced security information and event management (SIEM) threat dashboard

THE SOLUTION

The financial services company worked with Centripetal to manage the sources and types of threat intelligence used to defend their network.Doing so allowed the security team to focus on delivering rapid incident response and real-time visibility into the threat landscape of all their datacenter locations.

The Centripetal solution provided sophisticated packet filtering combined with real-time threat intelligence feeds and analytics capabilities. This meant large dynamic policies, with millions of rules enabled, containing high fidelity indicators to actively protect the network in real-time without degradation to network performance or user experience. With these capabilities in place, analysts could detect threats that had previously gone unnoticed.

Leveraging criticality ratings, confidence, tags, and deep contextual associations to define granular policies for alerting and blocking, the firm was able to operationalize threat intelligence and deliver immediate enforcement of dynamic threat indicators.

With real-time feedback now available to the Security Operations Center team, they could conduct network research; IOCs could be identified and attributed to activity on known internal network hosts in multiple locations. With this real-time information and insights, Incident response teams were able to target their efforts on the most severe and urgent security incidents.

THE RESULTS

The solution the Centripetal team deployed provided the firm with fully correlated inbound and outbound data. This allowed the organization to spot previously undetected outbound network threats with a level of visibility and control that they did not have previously.

The financial services firm was also able to identify malicious hosts on their network, and without disruption, block any outbound communications to known bad actors. The solution allowed the security team to react faster to threat data, ultimately regaining control of their network and keeping their data secure.

ABOUT THE COMPANY

This financial services firm is a constant target of adversarial groups. Given that they play a key role in the global economy, the organization places a strong emphasis on ensuring their enterprise is protected and that their data is safe.

Learn more about how CleanINTERNET® and Centripetal can proactively protect your organization.

LEARN MORE

CENTRIPETAL