CASE STUDY

Financial Services Customer Relies on Vertek for High-performance and Proactive Cybersecurity Protection

SUMMARY

This Vertek customer offers flexible, private-label mortgage origination solutions to credit union customers. The financial organization manages the mortgage origination process, so credit unions don't have to contend with margin pressures, increasing competition, and demanding regulatory requirements associated with the loan process. As a financial-based lending institution, this customer is a target rich environment for security breaches and attracting bad actors. The company is entrusted to keep customers' personal information secure and is required to meet compliance requirements including PCI-DSS.

CHALLENGES

Primary challenges customer was facing:

- Lack of internal security expertise - A small internal IT department struggled with performing threat detection and threat remediation
- Target-rich environment - The customer was frequently targeted for cyber attacks, including countless email phishing scams
- No proactive threat-monitoring and breach detection capabilities - The organization could not proactively detect, track, and respond to threats in a reliable manner
- Primarily manual and reactive compliance process - A mostly manual compliance report creation process was time-consuming and costly
- Budget Limitation - The VP had a limited budget and headcount to accomplish IT and security tasks

> *The constant barrage of cyber attacks targeted at our users via email phishing was impossible for us to contain on our own. We also didn't have the proper expertise internally at the time to analyze the attacks or prioritize their risk.*
>
> *– VP of Information Technology*

SOLUTION

The company selected Vertek as their expert Managed Detection Response (MDR) partner. Vertek leverages the award-winning AlienVault® USM® platform to log and aggregate security and event data from their critical assets on an ongoing basis. Vertek's solution offering, Managed Threat Intelligence (MTI), couples both Managed SIEM and 24/7 SOC-as-a-service.

356 Mountain View Drive
Colchester, VT 05446
802.764.4599
hello@vertek.com

RESULTS

The company believes that Vertek's Managed Threat Intelligence delivery model backed by AlienVault is an excellent fit and is meeting the company's security needs, compliance obligations, and budgetary requirements. The solution has helped 'fill the gap' in terms of the customer's limited internal cybersecurity staff. The organization now has expert resources and best-of-breed tools delivering a comprehensive threat monitoring solution at a fraction of the cost of building the service themselves.

Because Vertek's MTI solution, couples both Managed SIEM and 24/7 SOC-as-a-service, the system continuously scans the customer's complete IT infrastructure - protecting critical systems, networks, and applications. Vertek's analysts monitor the system and have access to the broadest threat vectors and effective defenses, so when suspicious behaviors or exploits are spotted, the organization is confident knowing they have proactive protection and immediate response, no matter what..

3.8 million +

average number of events per day normalized by Vertek's SOC

90%

or better alarm detection maintained since SOC

> *"Each month, Vertek provides monthly security readouts that help keep the team in check and communications lines open "*
>
> *– IT Manager*

Making compliance simpler

Vertek's managed security solution maps to the NIST Cybersecurity Framework (CSF) which helps the company automate much of its compliance processes with a high level of confidence. The solution's security controls, procedures, and SOC reporting go above and beyond traditional reporting tools to maintain compliance. Vertek's security team also provides monthly security readouts, reporting, and analytics helping the internal team manage their compliance process in a much more coordinated and streamlined way.

Optimizing protection with continuous monitoring and management

The mortgage-origination team also likes that Vertek's security team regularly optimizes the company's SIEM platform to minimize false alarms and improve the system over time. Vertek analysts write customized correlation rules according to the customer's environment. They also manage new assets, as needed, and changing workloads to better detect routine and more sophisticated multi-stage attacks that would have otherwise gone undetected.

Vertek's white-glove approach

The Managed Threat Intelligence solution is a combination of people, process and technology. Under the hood of MTI is a solutions company with over 30 years of experience providing critical operations services to Tier 1 carriers and Large Enterprises. Leveraging US-based certified security expertise, armed with hardened SOC BPM capabilities, IR tools, and its own enhanced proprietary threat intelligence feeds, Vertek's Security Operations Center provides continuous front-line threat visibility and actionable remediation guidance.