CASE STUDY

Holding Company Stops Phishing and Data Exfiltration With a Single Platform

The Challenge: Need a Centralized Security Solution Across Multiple Business Units

A large holding company needed to centralize their security efforts. Across the multiple business units the holding company managed there were a variety of different security tools, but no way to achieve centralized security visibility across all tools. Additionally, the company didn't just have one Windows log feed, they had many Windows log feed, one for each business unit.

The holding company reviewed next-generation SIEM solutions, prioritizing cloud SIEM solutions that have strong UEBA capabilities in order to thwart stealthy threats. The security team knew that attackers are often already inside an environment before they are detected, and that behavioral analytics pinpoint advanced attacks better than a rules-based approach.

Initially the company spent months trying to get IBM QRadar to work in their environment but found the capabilities and pricing to be less than favorable for their organization's goals.

The Solution: Securonix for Phishing and Data Exfiltration Prevention

The company chose Securonix Next-Gen SIEM due to its superior UEBA capabilities and true cloud-native, SaaS architecture. Due to their company structure, they started out by bringing in 50 log sources from across their many business units, with many data sources repeated across each business unit.

With Securonix Next-Gen SIEM and UEBA in place, the SOC started to detect and respond to their biggest vulnerability, phishing emails. Phishing emails was their biggest concern because the company doesn't have a consumer-facing website as a result of being a holding company. One of the only ways for attackers to get in is through a phishing email.

The holding company knew that it was easy for attackers to take advantage of free 30-day trials from various domain registrars, so they used a two-policy set up that focused on looking for newly registered domains. The policy would check whether the sending domain was less than 45 days old. Previously thousands of alerts would have been generated, but with this new policy only 5-10 possible malicious events were detected and investigated by the security team. This two-policy setup wasn't available with any other SIEM they reviewed, even Splunk. The two-policy setup was a game changer for their security posture.

The next major use case the security team worked on was data loss prevention. They leveraged policies in Securonix Next-Gen SIEM to detect data exfiltration attempts which they were previously blind to. Behavior-based rules were a huge help in detecting and responding to data exfiltration events.

The Business Impact: Blind to Perfect Visibility Without a Complex Setup

This company benefited from the flexibility of the Securonix Next-Gen SIEM solution to find and stop cybersecurity threats that they were blind to previously. They finally had a next-generation SIEM solution that could centralize visibility across all of their business units while not requiring a large security operations team. They are able to detect and stop phishing and data exfiltration events across their business units using a solution that is customizable to their unique needs.

On top of their successes in stopping many phishing and data exfiltration events, the holding company praised Securonix support. The security administrator running the solution believes that, "their support has been the best feature Securonix brings to the table."

Company Profile

This large consumer packaged goods holding company manages many of the household brands you know and love from the grocery store. As a Fortune 500 company, they are frequently targeted by attackers. Therefore, they like to buy best-of-breed security technologies.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.