Siemplify

No Threat Left Behind

How Castle Ventures Investigates Alerts Others May Have Missed

Castle Ventures

Newark, New Jersey

Information security consulting

www.castleventures.com

Organizations engage managed security services providers (MSSPs) for a variety of reasons, from device management to detection and remediation of threats from inside and outside the company.

Tasked with preventing and responding to threats of all kinds by its compliance-conscious clients, Castle Ventures, an information security consulting company in the Northeast US, needed a way to more efficiently manage a high volume of SIEM alerts, effectively respond to insider threats and better document incident response processes for auditors.

Challenges

Like most companies providing managed security services, Castle Ventures manages a variety of disparate technologies for its clients. The result is a deluge of SIEM alerts on a daily basis that, at times, would overwhelm its 15 security analysts. Being able to filter through all of the alerts, piece together related ones to tell a story and separate real threats from the noise was a persistent challenge for the organization.

In addition, Castle Ventures' client roster is primarily made up of organizations in the healthcare, financial services and higher education fields. These companies have stringent regulatory requirements they must meet and look to their partners, like Castle Ventures, to provide documentation that demonstrates adherence to HIPAA and PCI regulations.

ALERT FATIGUE
High volume of SIEM alerts

DISPARATE POINT TOOLS
Management and investigation across multiple technologies is time-consuming and manual

COMPLIANCE DOCUMENTATION
Need to demonstrate incident response processes to auditors

Siemplify's security orchestration and automation platform allowed us to focus our efforts and actually solve a problem that other tools regarded as noise.

— Arthur Hedge, President and Co-Founder

Solutions

Castle Ventures began searching for a security orchestration and automation solution that could help them streamline alerts, manage a wide variety of client security stacks and provide robust compliance reporting.

"From addressing the massive amount of alerts we get to being able to more efficiently answer auditors, improving our ability to respond to the various needs of our clients was the primary goal," said Arthur Hedge, president, Castle Ventures.

After exploring multiple security orchestration solutions, they selected Siemplify based on the integration and reporting capabilities of the platform paired with the overall flexibility of the support team.

Using Siemplify, Castle Ventures is able to streamline alerts, focus its analysts' tasks through a robust workbench, consolidate related alerts into cases that help the team build a full storyline for security events and deliver the visibility and compliance documentation their clients require.

Wins

Castle Ventures experienced the full power of Siemplify in investigating and remediating threats that have the potential to be overlooked or missed.

One of its clients, a midsize investment bank, trusts Castle Ventures with monitoring for internal security issues that can come from downloading malicious software to PCs and other routine activities. Castle Ventures' analysts review executables daily for this client and manage a variety of endpoint solutions as part of the overall environment.

In one instance, an analyst noticed the source of a recent download was questionable.

"The source was a German website, which I thought was odd since the request came out of Brazil," said Hilsabeck. "By investigating it through Siemplify, we found that the host was a known source of ransomware and that it had spread to another PC."

What was particularly challenging about this case is no single security tool in the stack was able to detect the malware or identify other PCs where it had spread. Had the analysts needed to rely on piecing together the story manually via the individual technologies, the malware would have likely continued to proliferate throughout the client's environment.

Instead, Siemplify's contextual grouping and orchestration capabilities enabled Castle Ventures' team to quickly identify the download as malicious, conduct a rapid and thorough investigation and solve the issue quickly. And, because all of the necessary information was delivered through a holistic workbench, Hilsabeck was prompted to recall he had seen this particular source host before, further speeding up the incident response process.

CASTLE VENTURES USES SIEMPLIFY TO...

ORCHESTRATE
Manage ecosystem of disparate customer technologies

INVESTIGATE
Build a full threat storyline through contextual grouping of alerts

AUTOMATE
File hash lookups, firewall traffic monitoring and other data gathering activities

RESPOND
Address insider threats throughout a customer's ecosystem from a single console

PROVIDE VISIBILITY
Demonstrate incident response processes to meet compliance requirements

Siemplify allows me to eliminate some of the noise. Having the single pane of glass that centralizes everything means I can be more efficient and focus on the activities that will truly keep our customers' data safe.

— Tyler Hilsabeck, Security Engineer, Castle Ventures