Siemplify

Taking Security Operations to a New Level

How Choice Solutions Automates 98% of Its Tier 1 Tasks

Choice Solutions

Overland Park, Kansas

Managed security services and business process automation

choicesolutions.com

Challenges

Choice Solutions has a broad base of 2,500+ seat clients, many of whom initially signed on for its expertise in virtualization and data centers. As the business expanded to include managed security services, the company began to face the same staffing roadblocks its clients were coming to them to solve. Finding experienced security talent that could hit the ground running using the outputs from its AlienVault SIEM was the primary challenge.

For Choice Solutions' existing bench of security analysts, playbooks presented a challenge of their own. Processes were all manual and, at times, steps were missed. These existing processes often meant that analysts couldn't get to the root cause of an alert before having to move on to the next one.

STAFFING
Not enough experienced talent available

PROCESS
Manual, sometimes incomplete, runbooks

ALERT VOLUME
Too many alerts, not enough detail

Solutions

Choice Solutions began searching for an automation solution to help its team more quickly analyze and triage alerts, better identify false positives and make its analysts more effective. "I didn't want my analysts to have to learn the back end for a bunch of different technologies," said Brad Horsley, Chief Technology Officer, Choice Solutions. After looking at a variety of options, the team selected Siemplify based on its platform's robust integration with, and support of, AlienVault.

In deploying Siemplify, Choice Solutions is able to ensure its security analysts have a holistic workbench to manage all of their day-to-day tasks. Each analyst gets a prioritized list of cases, and playbooks populate into each ticket so every team member has a clear to-do list at all times.

Siemplify also enabled Choice Solutions to make improvements in standardizing its processes through the platform's standard playbooks as well as its own customized playbooks.

With Siemplify, we can confidently go to our customers with findings, which solidifies our position as their security company.

— Brad Horsley, Chief Technology Officer

Wins

The Siemplify security orchestration and automation platform has allowed Choice Solutions to make the analysts it has more effective and speed up the on boarding process when new analysts are hired by significantly reducing the learning curve.

Within six months of beginning use of the platform, Choice Solutions was able to automate 98% of its Tier 1 tasks. This has helped the Tier 1 team members learn faster and become effective more quickly, which allows them to step up into Tier 2 more often.

The organization has also been able to maintain, and even improve, its effectiveness with a smaller Tier 1 bench, allowing Choice Solutions to put those dollars back toward the company's bottom line.

And, the analysts have been able to solve some previously puzzling tickets, including one that had been open for three months. Once Siemplify was deployed, the team was able to close this ticket in just four days thanks to contextual grouping of alerts, which brought together all of the relevant alerts into a single case. From there, the team was able to apply the automated playbooks and quickly resolve the case.

> **Our analysts love the platform. There's been a renewed interest in pushing to a new level. Siemplify has absolutely been the right security orchestration and automation solution for us.**

By the numbers:

98% of Tier 1 tasks automated

34% savings on Tier 1 staffing

10X ability to scale

> **What sets Siemplify apart is the ability of their platform to actually do what it promises. Our analysts can truly work from a single console and the contextual grouping brings together all the alerts we need to handle a case so we don't have to go searching.**
>
> — Brad Horsley, Chief Technology Officer