augustschell

CASE STUDY

Healthcare Organization Faces a Network in Severe Disarray, Optimizes Splunk Enterprise Security to Regain Control

Executive Summary

A large healthcare conglomerate had many diverse users and systems utilizing their network, ranging from tablets and specialized hardware in hospital rooms to guest access for customers and vendors. Given the amount and variety of network activity taking place, the customer struggled to gain a comprehensive view of sources of events, and increasing complexity was beginning to compound the problem. Further, with the ever-evolving threat to healthcare and PHI, it's no secret that this sector is one of the most frequently attacked. Unfortunately, healthcare organizations often end up paying for targeted attacks such as ransomware because lives are quite literally on the line. The customer feared that without better controls and visibility, they could be next.

Challenges

- Diverse users and systems connected to the network created a complex environment
- A wide, varied amount of activity made accurately tracking activity difficult
- Due to constantly changing IP addresses and shifting users, discerning malicious activity from harmless events was challenging for the Security Operations Center (SOC)

Business Impacts

- ✓ The security team was given the wherewithal to more efficiently investigate events.
- ✓ Network complexity was reduced by putting the right tools in place to simplify understanding diverse activity.
- ✓ The customer was able to successfully refine and optimize their use of Splunk to more easily identify legitimate security events.
- ✓ False positives were eliminated, thanks to tailored correlation searches.

Solutions

Primary:

- Optimized Splunk Enterprise Security

Supporting:

- Implemented additional correlation searches to narrow down users
- Created two-tiered alert system that allowed distinction between alerts and events

Large Healthcare Customer Contends with Chaotic Network Environment

A large healthcare organization was contending with a chaotic network environment—their network was being used by many users and systems, creating complexity that made identifying potential malicious activity and finding its sources difficult. Further, the use of multiple logging tools and a lack of an optimized alert system was generating an amount of false positives that wasn't manageable for their SOC.

"They had a lot of users and systems using their network, from tablets and specialized hardware in hospital rooms to guest access to their network via customers, vendors, and contractors," Andy Kaylor, Systems Engineer at August Schell recalled.

The customer needed to make the most out of their use of Splunk while ensuring their security team could keep up with the alerts being generated and respond to them appropriately.

Maximizing the Impacts of Splunk Enterprise Security

Kaylor said, "When I first began working with our customer, they already had a fully functioning Splunk environment collecting their data, and they had ES installed, configured, and working reasonably well. What I came to help with was working on additional correlation searches and other supporting Splunk configurations to help them narrow down users."

While the customer was familiar with the fundamentals of Splunk, the diversity of users and systems connected to their network made tracking sources of activity challenging—their use of Splunk needed to be refined. If a bad actor or indicative behavior took place, identification response became difficult because IP addresses changed and users shifted constantly. Determining whether activity was malicious and tracking down relevant users and systems was becoming a distracting challenge due to unmanageable complexity.

Improving Integration Between Splunk and Their Ticketing System, Managing Disparate Logging Tools

After identifying the primary security issues the customer was struggling with, Kaylor set out to enhance the integration between Splunk incidents and the customer's ticketing system. "They wanted to make sure if something happened and a ticket got opened, based on the rules of the correlation search and rules that cause triggers, that additional incidents wouldn't be generated," Kaylor explained.

One of the keys to using incident review successfully is tailoring correlation searches to eliminate false positives. For instance, if the customer had three operators on an eight-hour shift and 400 alerts are generated, they'd be facing an unmanageable amount of incidents and become distracted from events that could actually be malicious. When using Splunk Enterprise Security, finding a way to achieve balance and a system that can realistically be dealt with by staff is key. "They had a basic framework, but I was able to help them refine it and make additions that would result in a better, more reliable system," Kaylor said.

The next part of the process was focused on dealing with multiple tools detecting malicious behavior. "We got them into a place where they weren't generating new incidents for issues that already had tickets open, which was a win. But, when you're using several different tools, some particular event might hit an external load balancer, come to a firewall, a web server, then an app server, anti-virus… it triggers all of those tools." Since different tools log events differently, the customer needed a system to keep track of individual entities and triggers to correlate new issues back to existing tools based on shared information. "You don't know they're connected unless you have another event," Kaylor explained.

ASE worked with the customer to create a system with two tiers of alerts: initial alerts, plus combined alerts to indicate what happened and related incident triggers. Based on related rules, it became possible to determine if events were related to the same action, or if possible attacks were the same entities.

Empowering Security Operations to Quickly and Efficiently Resolve Problems

When it comes to security operations, organizations need to enable analysts to quickly and efficiently find and resolve problems. By focusing their efforts and making sure they're equipped with all of the knowledge that's available to them, improving efficiency of the customer's SOC was a success. "Some of what we were doing was writing additional searches, and that was really important. To make all of that work with intermediate stacks, we had to work together on writing external Python code in addition to normal Splunk enhancements," Kaylor concluded.