augustschell

CASE STUDY

Agency of U.S. Government Opts for Splunk Over Legacy SIEM, Overcomes Perilous Security Vulnerabilities

Executive Summary

An independent agency of the U.S. government was using an aged SIEM and struggled to transition from a security posture built for reactivity rather than proactivity. The customer was focused on searching for old threats rather than emerging threats and experienced major scalability problems as a result of using a legacy system to monitor a massive network.

Challenges

- The legacy SIEM lacked proper hygiene, causing maintenance and auditing to suffer
- Security emphasis was on old threats as opposed to new and emerging threats
- With one of the largest networks in the federal government, the aged SIEM suffered from scalability problems

Solutions

Primary:

- Splunk

Supporting:

- Splunk Enterprise Security

Business Impacts

- ✓ The customer successfully swapped a problematic, legacy SIEM for a modern one.
- ✓ By adding Splunk ES, the customer gained full visibility into machine data generated from security technologies, resulting in a much stronger security posture.
- ✓ A shift from reactive security to proactive security was achieved.
- ✓ Scalability problems were eliminated.

U.S. Federal Agency Suffers the Effects of a Legacy SIEM

A department of the U.S. government was striving to migrate to a more modern, proactive security posture. A fundamental truth of the modern threat landscape is the reality that eventually, a breach will come to pass. With this in mind, this particular agency wanted to reach a state of operations which emphasized prevention as much as possible, as well as finding threats before they become problematic. It was time to transition from reactivity to proactivity.

With the legacy system came poor security hygiene. It wasn't well maintained and use cases hadn't been monitored or audited for an extensive period of time, putting the focus on old threats rather than new and emerging ones. The agency also ran an overwhelmingly massive network. Coupled with an aged SIEM, scalability was a considerable problem.

Swapping a System on Its Last Leg for the Cutting-edge: Splunk

Erika Horton, Splunk Architect at August Schell recalled: "When I got on board, the customer already had Splunk deployed, so we had to review the current installation and make sure everything was configured properly for the scale of the environment."

Following the initial review, data hygiene had to be examined to ensure proper onboarding. When updating a legacy SIEM with Splunk, it's of utmost importance to ensure data has been onboarded properly. It has to be correctly extracted and formatted for the CIM data model, which is a data normalization abstraction in

between core Splunk and Splunk ES, to make the data usable across a broad variety of use cases.

"While we were looking at their data hygiene, they were continually bringing on new data sources and use cases. So, the other challenge was doing all of this activity on a production system. We had to go back and walk through the installation, configuration, and data onboarding while still bringing on new data sources," Horton explained.

Tackling Splunk Enterprise and Taking a SIEM from Old to New

With the initial configuration review complete, it was time to hit the ground running with bringing legacy SIEM use cases into Splunk. "It was all about walking the customer through their security use cases from their legacy SIEM and translating those over to the new SIEM. That process was intensive, and we had to complete the validation of the requirements," Horton said.

Each rule or use case in an existing SIEM has to be accounted for. Its purpose, whether it's still needed, and the best way to deploy it within an enterprise security context are all critical considerations. While everything is a rule in a legacy SIEM, perhaps in ES it's configured as a dashboard rather than a notable event. Because of these nuances, individual use cases must be evaluated in order to determine the best method for visualization in ES, then translated and built out.

"We had to avoid replication of work, too," Horton said. "Some things had already been built out, so if they had an old SIEM use case for account lockout, and we're building a rule, but they already did that in core Splunk, we had to validate their SIEM uses cases against the core Splunk work they'd already done and merge all of that together."

Finally, ASE completed the migration of the indicator of compromise list for threat data from other Splunk systems to the customer's enterprise security systems. "Their intelligence team had their own Splunk search head upon which they maintained lists of threat data, whether bad URLs, email addresses, or IP addresses," Horton explained. ASE created a custom solution that would allow for the automatic migration of threat data lookups from original search head onto the ES search head. "They needed to be maintained at a single point of truth, but also still be utilized at the ES framework," Horton stated.

Federal Agency Goes Modern with Splunk, Optimizes Usage, and Strengthens Security Posture

In the end, swapping out the legacy SIEM for Splunk was an arduous process with rewarding results. The customer realized a complete SIEM upgrade by optimizing their initial Splunk installation, followed by a successful migration process which ensured all security data was amalgamated into one place.

The customer was even able to make custom content available within enterprise security, enabling tailored dashboards and visualizations. With the help of Erika Horton, they merged the content into the Splunk ES navigation, eliminating the need to constantly leave the ES app to access it.

The agency's users were also coached on how to create more efficient searches, keep the platform healthy, and find bad searches. ASE provided a comprehensive knowledge transfer and product training session to ensure their new SIEM would operate successfully long after the close of the engagement.

"I was glad to make the customer happy, and they have plenty of potential to extend their use of Splunk even further and improve their infrastructure overall when they're ready. We could work with them to achieve better utilization of virtualization, or enable larger, broader, disaster recovery. At the project's close, the customer was satisfied with their outcomes, and they definitely have the opportunity to continue to optimize," Horton concluded.