augustschell

CASE STUDY

U.S. Airport Authority Leaves No Data Behind, Enhances Security Using Splunk Threat Intelligence

Executive Summary

A U.S. airport authority responsible for two regional airports had installed Splunk, but wasn't using it to their full benefit. The customer was processing data for two very active locations with many control lines, which created a significant amount of federated data across regions. With the customer's location being one of the busiest airport regions in the country, the sobering truth that they rely on data to be operational every day of the year was causing considerable fear of a critical system going down, and even more harrowing, the possible repercussions. To increase their visibility and resilience, it was time to find a better way to manage data.

Business Impacts

- ✓ Congested storage issues eliminated
- ✓ Practical use of Splunk adjusted to address relevant use cases
- ✓ Splunk Enterprise Security provided greater insight into security operations
- ✓ Robust training prepared the customer's security team to operate and manage their Splunk environment autonomously

Challenges

- » Dual locations with a multitude of kiosks, control lines, and endpoints overall were creating large amounts of disparate data.
- » A lack of a centralized platform made it hard to make data relevant to the security and operations of the airport.
- » A considerable amount of PII originating from credit cards was being processed without the proper security controls in place.
- » The security team needed the proper threat intelligence capabilities to foresee future threats.

Solutions

Primary:

- » Splunk Enterprise Security

Supporting:

- » Cleaned up full storage to enable proper indexing
- » Enabled security capabilities relevant to use cases

U.S. Airport Authority Must Enter the Modern Era of Data and Security

A U.S. airport authority operating two regional airports was met with significant obstacles in maximizing their use of Splunk. They'd reached storage capacity and needed to install Splunk Enterprise Security in order to address the use cases most relevant to their business.

"The agency had many control lines," Eric Nicholson, Splunk Systems Engineer at August Schell said. "Their federated data was everywhere across regions and they needed a consolidated platform to help visualize and aggregate the schema."

The customer needed to optimize and tune their use of Splunk, as well as gain better visibility into their data from across the enterprise in order to achieve a healthier security posture.

Storage Clean-Up, Splunk Enterprise Security Implementation, and Necessary Training

In order to prepare the customer for a Splunk Enterprise Security install, August Schell first had to address their storage capacity issue.

"When I first went in, the customer had Splunk, but it wasn't indexing because their storage was totally full," Nicholson said. "I started by getting all of that cleaned up."

Beyond their initial storage issue, the customer was simply dealing with mass amounts of data that needed to be modernized from a management and security perspective.

"It was important to us to convey to the customer that with all of the PII they were processing, security couldn't be an afterthought, and Splunk Enterprise Security needed to be set up to help them be more proactive," Cory Conway, Director of Big Data Solutions & Services at August Schell said.

The key to making the customer's use of Splunk as impactful as possible was in getting systems up and running and disabling unnecessary use cases. "They were using Splunk for performance monitoring, but they actually needed it on the security side," Nicholson explained.

The environment was optimized while the data relevant to their use cases was gathered. Next, ASE implemented Enterprise Security to improve the customer's ability to swiftly detect and respond to potential attacks, whether internal or external.

The engagement was concluded with comprehensive Splunk ES training offered to the customer's security team to ensure they were properly onboarded and prepared to manage the environment.

Achieving a Fully Functional Splunk Environment That Addresses Essential Use Cases

"Before August Schell went in, Splunk wasn't working for the agency at all. They just weren't having success," Nicholson recalled. "My goal was to help them achieve a fully functional environment that matched their specific use cases and could be operated by their security team with ease."

Without a consolidated platform for visualizing security-relevant information, an airport processes a dangerous aggregation of data, and securing it is critical to effectively operating in the modern era. August Schell ensured the customer was secure, properly configured, and set up to realize swift ROI.

"We wanted the customer to know that we're here for them beyond the initial engagement," Conway said. "We advised them to consider adding additional data into Splunk, such as sensor data, active directory, routing information, and metro data. As they add use cases, they'll be able to visualize flow and know when they need to scale or consider additional protections."

There are many ways to use Splunk from unique perspectives. As use cases are added, a more detailed operational picture of facilities and endpoints gets painted, ultimately aggregating points throughout the entire environment; this is what ASE made possible for the airport authority.

Want to learn more about Splunk? Read our case study "Agency of U.S. Government Opts for Splunk Over Legacy SIEM, Overcomes Perilous Security Vulnerabilities" which covers Splunk, Splunk Enterprise Security, and scaling your SIEM.