augustschell

CASE STUDY

Federal Agency Leaves Ineffective SIEM Behind, Rapidly Gains Power to Visualize Environmental Data

Executive Summary

A federal agency had been running a product for networking analysis and threat intelligence for a few years, but had become dissatisfied with its cost and lack of integration into other tools they were using. They needed a better solution that would provide visibility into their IT environment. Further, due to the classified nature of the agency, while they required support in installing a new SIEM, their consultant of choice would not be permitted to interact with their systems directly or view their network.

Challenges

- The customer struggled to aggregate live data from all network devices
- Active directory reporting was a major priority in order to execute on location-based correlation, but their current solution didn't provide the capabilities
- Visibility into security events was lacking, putting their environment at risk
- The classified nature of the agency introduced interactive limitations for their chosen technology consultant

Business Impacts

- ✓ The customer successfully installed Splunk Enterprise, which provided a comprehensive view of their organization-wide IT and network activities.
- ✓ Active-passive mirroring provided reassurance that potential outages would not render Splunk inoperative.
- ✓ Several agency team members were trained on Splunk.
- ✓ The customer was set up to be able to run Splunk successfully for the foreseeable future, as it was configured to encompass upcoming requirements.

Primary Solution

- Splunk Enterprise

Federal Agency Grapples with Their SIEM's Lack of Integration, Sets Sights on Better Visibility of IT Systems in a Highly Classified Environment

A federal agency had been running a SIEM product for several years, but struggled with its lack of integration with other tools, as well as the high cost. They experienced difficulty in getting additional data into the product, plus, they'd been upgrading and replacing some of their network hardware, and getting data from the new devices into was just as arduous.

The customer recognized the need for a new SIEM solution, as bringing together live data from all network devices was a priority.

Taking Advantage of Location-based Correlation, Overcoming the Limitations of a Highly Classified Network

"They also wanted to be able to do active directory reporting, especially correlations between log on and whether or not people should be logging on from their given location. Location-based correlation, making sure that users haven't been compromised, was really important to the customer, so using Splunk was a no-brainer," Warren Myers, Consulting

Engineer at August Schell said. "Plus, the agency planned to install Splunk Enterprise Security to enhance their security posture and improve their position of defense."

This particular customer faced a unique challenge, and so did Myers as a result. Their network was classified top secret, which meant that Myers and his team would not be able to physically touch any equipment or systems.

"I had to tell employees what to type and where to put things," Myers recalled. "Then there was the second environment that was being put up on the classified network, and I wasn't allowed to look at that either. I was up to the challenge, though, especially because I trusted the power of Splunk."

Installing Splunk, Setting Up Active-Passive Mirroring, and Reviewing How-Tos

With the goals of the customer in mind, the August Schell Splunk engineering team was ready to begin the installation. At the project's beginning, the customer was migrating a considerable amount of their hardware to Nutanix devices, so the installation began with working alongside Nutanix engineers in order to get Splunk set up and built.

"The first day was spent getting the two VMs we needed built. One on the network I was dealing with, and one on the second one. Then we worked to transfer over Splunk apps, including the Splunk App for Windows Infrastructure, as someone else replicated the process by video conference in another building," Myers recalled.

Day 2 kicked off with configuration. Myers worked with the customer to load licenses and ensure that Splunk would be ready to go and collect data. They began pointing a number of products already installed in Splunk to confirm that it was in fact collecting data.

Next, it was time for troubleshooting network issues and opening up more firewall ports between different locations.

"Not all at once, but stretched over a couple days, until we got to where the syslog collector colocated on the Splunk server, which was the customer's objective," Myers explained.

The agency wanted to be able to automatically pick Splunk back up in the event that their site goes down, so the ASE team also spent time setting up active-passive mirroring for the VMs between two different locations, ensuring that if one site goes down, there's a backup DNS to rely on.

Myers and his team also worked closely with the customer to share how-tos, best practices, and tips for Splunk. Not being able to interact with their systems directly created positive outcomes—the customer had to do searches and build reports and dashboards according to Myers' guidance, and build their own skillset as a result.

Usable Data and ROI Generated. IT Staff Educated. Potential Exploits Identified

"Without being able to see what the customer was doing, we were still able to accomplish their mission, and that's a major attestation to Splunk, as well as our engineering team," Myers said. "Because of the limitations introduced by the classified nature of the agency, by the end of the engagement, the customer had three or four personnel who had gotten the hang of the data they were bringing into Splunk from their environment and devices."

As soon as the team pointed data (particularly syslog data) at Splunk and got Splunk forwarders on Windows machines, the customer was getting usable data into Splunk. Rapidly, they were able to visualize machine data, make sure appropriate firewall rules were in place, and identify problems they suspected existed, but couldn't previously identify.

"The big upshot was, they were seeing a return on the time investment once we got it set up, which took a couple days, inside of 10-12 minutes. With some of the planning and structure we did early on, they won't have to do a lot of extra management later to add new things to their environment," Myers said.

Ultimately, the customer was set up to encompass all of their current use cases, as well as what could be reasonably anticipated for the coming months. They went from limited visibility to a comprehensive view of IT systems, and are now able to address problems in a more proactive fashion.

"Going from where they were to seeing problems that could be flagged immediately was a major win," Myers concluded.

51 Monroe Street, Suite 1802
Rockville, MD 20850
301.838.9470 | www.augustschell.com