augustschell

CASE STUDY

# Arizona Municipality Vulnerabilities Contend with Unsuccessful Splunk Implementation

## Executive Summary

You know the story, a major US City in Arizona, spent big to bring in Splunk and get things going, but with changing priorities and some kicking the can they ended up with dreaded shelf-ware and an improperly tuned Enterprise Security Installation. They were forced to continue security operations with their existing tools for an entire year without visibility into its inner workings.

## Challenges

- The original Splunk implementation was improperly configured, rendering it unusable
- Comprehensive visibility into security operations was lacking due to the limitations of current tools
- The customer felt hesitant to work with a new consultant after a poor initial experience with another provider

## Solutions

### Primary

- Splunk

### Secondary

- Splunk Enterprise Security

## Business Impacts

- ✓ The customer received an entirely new Splunk infrastructure.
- ✓ Trust and communication between August Schell and the customer were established.
- ✓ By adding and properly configuring Splunk ES, the customer gained a much better picture of their organization-wide security activities, resulting in a stronger security posture.
- ✓ A long-term relationship came of the engagement, allowing the customer to consult August Schell regularly for additional tips and assistance through minor hiccups.

### Arizona Metropolis Reluctant After an Improper Splunk Implementation

A city of Arizona had previously partnered with a consultant for both managed Splunk and Enterprise Security. Unfortunately, after the consultant left the customer, they quickly came to find that Splunk was not implemented correctly, and were left with a nonfunctioning solution that wasn't contributing to their security strategy. Their Splunk environment remained unused for about a year before August Schell was engaged. The customer's security team didn't feel optimistic about engaging a new services firm after having a poor experience the first time around. Ultimately, they decided to search for a consultant with the necessary expertise to bring their environment back to life.

"They were a little nervous to give Splunk another shot, not because they doubted the solution itself, but because of the misconfigured environment, and this was completely understandable. I made sure they knew that I wasn't leaving until their Splunk environment was working properly," Eric Nicholson, Certified Splunk Architect at August Schell.

## Rethinking a Haywire Splunk Environment, Designing a New Infrastructure for a Favorable Outcome

The customer's goal was to use their Security Information and Event Management (SIEM) system for security monitoring and visibility. While they had other tools available to them, using Splunk to gain a more comprehensive view of their security operations was desired.

"The first week was really focused on redesigning the architecture and deploying the new core infrastructure. We were also focused on onboarding all their data sources properly into this new infrastructure," Nicholson recalled.

Splunk ES also had to be reinstalled, as well as the add-ons required to go along with it, after numerous technical issues surfaced while Nicholson and the engineering team were working on reducing roles and upgrading the software.

"It was a little tricky, but we worked through the issues, ultimately resulting in a solid core search head – a core component of Splunk. Plus, all the apps and add-ons were successfully updated to their most recent versions, and we verified that they were all working properly," he said.

The engagement concluded with the finalization of the new infrastructure, complete with a brand new Splunk search head. The engineers took extra time to perform health checks and review logs to make certain that the infrastructure was solid and running without issues.

"We were not going to let them run a Splunk environment that wasn't going to benefit them again," Nicholson said. "We tripled checked everything and made sure the deployment was a complete success."

## City in Arizona Puts an Unsuccessful Deployment Behind Them and Enjoys a Rock Solid Splunk Environment

When the engagement came to a close, the IT team representing the municipality was pleased with their new infrastructure and looked forward to being able to streamline their security operations.

"The biggest challenge was making the customer feel comfortable with the knowledge I had to make sure they were going to be good to go. They were nervous, especially the first week. I felt that the engagement was about the customer more so than the technology. I was confident in my Splunk expertise, but what I was really dedicated to was gaining their trust," Nicholson said.

August Schell was able to make recommendations for go-forward Splunk engagements, such as regular health checks, additional dashboards, and onboarding additional data sources, such as firewalls or a cloud environment. Since the conclusion of this project, Nicholson has kept in touch with the customer to ensure continuous success, and has helped out with several remote engagements.

"Things have been going really well. In fact, we're the envy of many state and local government agencies here in Arizona. Our Splunk environment has been rock solid... and major kudos to you for getting us there."

-Sr. Information Security Architect, Arizona Municipality

Contact August Schell at 301.838.9470 or inforequest@augustschell.com to learn more!