Summary

Splunk is only valuable to the extent that it is (a) properly administered on the back end and (b) leveraged by end users with the necessary knowledge of the tool. It's capable of delivering incredibly powerful analytics value, yet most organizations lack either the in-house skill set or bandwidth (or both) to take proper advantage of this power. Given how critical a SIEM's security detections are to an organization's cyber defenses, organizations need to get the most out of Splunk. SP6 ensures that success and value occur.

SP6 was able to significantly:

- ✓ Increase the ROI of the organization's Splunk investment.
- ✓ Educate and empower internal staff to properly implement and manage security detection.

Back to Back Winner 2023 & 2024
splunk> AMER Professional Services PARTNER OF THE YEAR

CASE STUDY

VALUE ACCELERATION PROGRAM FOR SPLUNK (CO-MANAGED SPLUNK SERVICES)

SP6
SYSTEMS MADE
Secure. Compliant. Resilient.

The Problem

A large healthcare system had purchased and implemented Splunk for three years with little to show for it. Despite having deployed both Splunk Enterprise and Splunk's Enterprise Security (ES) SIEM, this organization had an extremely low level of value realization.

- Splunk was only being used as a log repository rather than an **analytics tool** to leverage those logs.
- Despite having Splunk's SIEM (Enterprise Security) in place for those three years, this organization hadn't enabled a single security detection – not one!
- **This was an incredible misuse of Splunk.**

Hurdles

The roadblocks this organization faced are far too common:

- **Overcommitted personnel.** Splunk's best practices suggest that any organization ingesting over one terabyte (TB) of data daily needs a full-time Splunk Administrator to manage the platform. This platform management can include both the care and feeding of Splunk – including the integrations that feed data into Splunk and data normalization – as well as content development for users. Content development can include the configuration of available out-of-the-box alerts, dashboards, and reports, as well as the creation of custom content. Splunk Administrators may also be responsible for tuning queries to reduce false-positive alerts and other critical functions depending upon the knowledge level of users.
- This organization had a single technology team member dedicated to supporting Splunk, ***but at only 5% of that person's time***. Given their **1.3 terabytes of daily data ingest,** and the requisite need for a full-time Splunk Admin, **this organization was massively under-resourced**.
- The individual responsible for supporting Splunk was extremely eager, but as the primary administrator of four other tools, he didn't have the necessary bandwidth to generate effective use of – and results from – Splunk.
- **Organizational overcommitment.** This organization had a habit of overloading technology and security staff with project work. There is an adage: "When everything is a priority, nothing is a priority." That was certainly the case here, as there was a commitment to many projects but lack of progress on most.

Solution

This organization turned to SP6 for assistance. Specifically:

- SP6 was asked to provide co-management of the organization's Splunk environment.
- This was not a full outsourcing arrangement; rather, SP6 was leveraged to provide both strategic guidance and tactical hands-on engineering of Splunk, assisting the organization's employee.
- SP6 was not providing Security Analyst (monitoring) functions of an MSSP. SP6 was assisting with Splunk administration so that the organization's **own security analysts** could be much more effective.
- **The goal:** Drive the intended outcomes of Splunk. Leverage Splunk as a SIEM for security detection and not simply log management.

SP6 understood that this organization's employees were stretched across a multitude of projects and responsibilities. As such, SP6 adopted a "Crawl, Walk, Run" approach. While SP6 was capable of running at a fast pace, the customer was not. To remedy this, yet still **pull forward Splunk use and value**, SP6 employed their #1 Core Value: Drive Successful Outcomes, Iteratively and Often. This was accomplished in the following manner:

- The customer made it clear that they were in no position to "boil the ocean" but were adamant in wanting to see more value out of Splunk for security detection.
- The starting point SP6 was working with: the customer had zero security detections (correlation searches) enabled in Splunk Enterprise Security.
- SP6 employed an **iterative approach** similar to that used in agile software development. While in the software development domain, it's common for small improvements to be made through bi-weekly sprints, SP6 established monthly objectives in collaboration with this customer. This is the basis of **SP6's Outcomes Based Approach: establishing achievable monthly goals, accomplishing them, and establishing the next series of commitments.**
- The CISO at this organization asked for three things in month one:
  - Establish a first set of four security detections.
  - Ensure that those detections were extremely tuned to reduce false positives, not wanting to overrun his security analyst team with false positive security alerts.
  - Create an executive dashboard with specific information that is important to the CISO.

Results

After co-managing this organization's Splunk environment for 18 months:

- **SP6 closed a major security and compliance risk related to password security.**
  This organization's infrastructure team had disabled their password auditing enforcement, so SP6 built a unique dashboard showcasing the percentage of employees setting non-compliant passwords. The dashboard revealed that 20% of employees were using improper passwords, which prompted the organization to reinstate password auditing.

Continued

Results, *continued*

- **SP6 prevented the possibility of major HIPAA violations.**
  It was discovered that some employees were forwarding work emails — potentially with sensitive patient data — to external email addresses. To combat this, SP6 created a security detection to alert the organization whenever employees forwarded an email to external and private email addresses.
- **SP6 created and implemented 32 correlation searches in Enterprise Security as well as 20 scheduled searches.**
  These searches were tuned to prevent false positives and excess noise.
- **SP6 dedicated, at times, 50% of our time to providing knowledge transfer to an already capable Splunk administrator.**
  Despite their advanced capabilities, this administrator regularly came to SP6's experts with how-to questions for solving certain problems within the organization.

Customer Feedback

> You have ***always*** delivered. I've always been happy.

> We've had a ***positive experience*** — even with different engineers.

> The weekly cadence has gone well. We get something done ***every week***.

About SP6

SP6 is a niche services firm with expertise in both Security Analytics and Cybersecurity Compliance. In Security Analytics, SP6 has one of North America's largest and most competent Splunk services teams in North America. SP6 offers both project-based Professional Services and the Value Acceleration Program for Splunk, a fractional co-management model. In the field of Cybersecurity Compliance, SP6 provides consulting expertise with NIST security frameworks such as NIST CSF, 800-171 and 800-53. These services include security and compliance gap assessments, remediation advisement around missing or failed security controls, outsourced Compliance as a Service, and Continuous Controls Monitoring through our ASCERA software product.