Summary

A large university system with over 35,000 faculty and students has a significant (3+ terabyte of daily log data) and complex Splunk deployment being used for a wide variety of purposes: application availability, information security, and data compliance.

This University had significant issues supporting Splunk which prevented them from achieving optimal value.

SP6 was able to significantly:

- ✓ Improve compliance tied to data retention regulations.
- ✓ Drive down the cost of Splunk licensing at renewal.
- ✓ Reduce organizational risk tied to the University always being one resignation away from lack of Splunk management (and the consequences to compliance, security, IT operations and DevOps).
- ✓ Reduce the cost and complexity of managing Splunk (through less time spent on platform administration).

splunk> 2023 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

Like many organizations, the client had a sole employee managing Splunk who was highly technical and proficient in certain areas (Linux administration and network engineering). However, Splunk was not this employee's core capability. Despite being responsible for Splunk, this employee didn't know the solution very well.

This part-time Splunk administrator had inherited the system from a prior admin who happened to be a developer that took on Splunk responsibilities. In doing so, this prior admin over-engineered Splunk. There were many unnecessarily complex, custom-built components with little documentation.

Because Splunk was not within this employee's core capabilities, and because they were managing an environment that was developed outside of best practices, the employee struggled to effectively manage the platform. Key challenges included:

- Data integrations — which are critical to log aggregation, compliance, and analytics — would break, and there was no understanding as to why (or how to remediate).
- Dropped data integrations posed significant risks, as the data being collected:
  - Was required for statutory compliance purposes.
  - Was no longer available for security detections or systems troubleshooting.
- At some point, the individual responsible for managing Splunk left the University.
  - There was an absence of in-house expertise to (a) manage Splunk's engineering and (b) ensure the platform worked efficiently.

These Problems Are Not Unique

The three biggest issues with this organization are quite common:

- A mission-critical system is **single threaded** through one individual, risking a complete lack of platform management when the employee leaves the organization.
- Splunk is **not this individual's core competency**, yielding poor engineering and use.
- The employee is responsible for managing other systems and tools, **leaving inadequate time to support Splunk**.

CASE STUDY

VALUE ACCELERATION PROGRAM FOR SPLUNK (CO-MANAGED SPLUNK)

Solution

The University decided to partially outsource Splunk administration to SP6 through SP6's Value Acceleration Program for Splunk. They did this in conjunction with hiring another employee to own the system internally. The intent was to:

- Have one of the University's most mission-critical technology solutions co-managed by Splunk experts.
- No longer be single threaded and vulnerable to internal staff changes.
- ***As a result, get optimized value from Splunk through better engineering and use.***

SP6 deployed their **Objectives Based Methodology**. This approach starts with the identification and prioritization of needs that promise the highest organizational impact, before flowing to execution.

SP6 also provided an assigned Splunk SME that is dedicated (part time) to the customer. This helped the University benefit from not only expertise, but from **consistent, intimate knowledge of their systems**.

Results

Through the expertise of SP6 Splunk experts who were assigned to deliver part-time, monthly services on behalf of the University, SP6 was able to:

- **Ensure Data Compliance**
  Integrations are now stable and report legally required data to the University's data store.
- **Significantly Reduce Future License Costs by Up to 40% (~$300,000)**
  The University was leveraging Splunk's workload licensing model (SVCs). Prior to SP6's involvement, poor engineering and misconfigurations caused searches to run improperly. This significantly and unnecessarily drove up server utilization, and therefore costs. After being consolidated and re-engineered by SP6, server utilization — the basis of the University's compute-based SVC license — was reduced by 40%.
- **De-Risk the University's Compliance, Security, IT Ops, and DevOps Operations**
  The Splunk platform is no longer reliant upon a single individual. Regardless of staff turnover, proper data collection and analytics — which are the foundation of compliance detections, security detections, and accelerated IT and application troubleshooting — will continue. This provides better systems availability.
- **Provide Knowledge Transfer and User Education**
  The University is on their third in-house Splunk Admin in as many years, and SP6 is helping up-skill that staff member. SP6's intent is not for the University to be reliant upon our service, but to enable them to achieve the same results in a 'teach a man to fish' manner.

  In addition, the University has over 1,000 users with access to Splunk, many of whom didn't initially understand the tool or how to effectively use it. SP6 held weekly training sessions on "How To" with Splunk, resulting in more efficient use of the solution and greater self-sufficiency.

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.