# Success Plan℠ for Splunk

**You made the investment – now get the most out of it.**

Formerly < aditum >

Splunk is a truly revolutionary product that can transform your organization based upon the platform's analytic capabilities. The precise value of Splunk has been well documented in over 1,000 case studies worldwide, across (3) key use cases:

| | |
|---|---|
| Security & Compliance | • 70% to 90% faster detection, triage and investigation of security events (more time for Security Analysts to perform threat hunting)<br>• Up to 90% reduction in compliance reporting time |
| IT Operations | • 70% to 90% reduction in incident investigation time and root cause analysis<br>• Up to 20% increase in capacity utilization |
| Application Development | • Up to 90% reduction in time to discover pre-production defects<br>• Up to 50% improvement in time-to-market |

The data above is indisputable: Splunk can provide transformational value to both middle-market as well as enterprise organizations. As with any IT solution, and Splunk is certainly no different, proper time and commitment is required for users to attain that value. There are several hurdles that customers commonly face that can prevent them from achieving these desired results with Splunk:

- Many system administrators and security engineers are over-burdened, wearing too many hats, neglecting to invest the proper time in Splunk
- Organizations may lack specific in-house Splunk subject matter expertise, resulting in the failure to fully develop the capabilities of Splunk
- Experienced Splunk Admins may move on from an organization, leaving the Splunk environment significantly neglected, or in the worst case, as shelfware

## For organizations with strained resources struggling to adopt and take ownership of Splunk, SP6 has developed the Success Plan℠ for Splunk.

The Success Plan℠ for Splunk:

- Relies on ongoing technical involvement, in the form of scheduled, monthly touches between your company's admin, engineers or Splunk power users, and an SP6 Splunk SME.
- Is based upon a series of specific, prescriptive, focused tasks
- Allows customers to leverage SP6's IT and security domain expertise, not simply product expertise
- Drives greater results for your business across IT, Security and App Dev (depending upon your Splunk use).

This Plan is designed to address issues common across all customers, who universally need help with:

- Use case development: "We think this is possible. What do you think? How do we achieve this?"
- Technical use of Splunk: administrating role-based access control, on-boarding new data, writing complex queries, developing dashboards and alerts
- General security operations consulting: "What should we be doing to make our environment more secure?"
- Data interpretation: making sense out of machine data and finding value in it.

**Customers who make the time investment and truly take ownership of the platform will realize outsized gains.**

# SP6's Success Plan℠ for Splunk

SP6's Splunk SME's are complete product experts, with experience engineering the tool and using it as analysts. Many other consulting firms provide services around tool configuration, but that is only part of what customers need. Our value-add is that we bring in both security engineering and security analyst experience, to advance the usage and value of the Splunk platform. We also have domain experts with extensive experience in IT Monitoring and DevOps.

## Monthly Cadence Calls with SP6's Splunk SME's

It's important to note that this Plan is not simply a pre-purchased 'bucket of hours', but rather a structured monthly program that ensures that your Splunk investment gets the ongoing attention that will drive desired business value.

| | |
|---|---|
| Month 1 | **Reducing Alert Fatigue (Tuning Reports and Alerts)**<br>• When Professional Services is delivered, PS develops queries (core Splunk) or turns on out-of-the-box correlation searches (Splunk ES). **It's critical that these queries be tuned to reduce unnecessary alerts and prevent alert fatigue on your security or IT Ops team.**<br>• This is especially critical with Splunk ES customers. Tuning Splunk ES to produce the most actionable results possible is part of the on-going administration of any SIEM. Working directly with our SP6 Splunk SMEs, we will empower your admins with the tools to take on this challenge themselves as well as provide assistance with the particularly difficult use cases. |
| Month 2 | **Developing Use Cases**<br>• For Security use cases, examination of Splunk's OOTB (out-of-the-box) security use cases from free apps available on Splunkbase, including the Splunk Security Essentials app.<br>• Provide insight into the value of specific security use cases, and advice regarding what other organizations are doing to meet their security challenges.<br>• Advice and technical assistance implementing use cases. SP6 Splunk SME's can help identify what data is needed for a given use case, how to get it, and how to produce the desired results with it. |
| Month 3 | **Developing SPL Queries**<br>• SP6 Splunk SME's will conduct live sessions with your admins and interested power users to develop their skills and confidence with using Splunk's query language (SPL).<br>• Ahead of this exercise, SP6 Splunk SME's will conduct a discovery of what use cases might have an immediate benefit for your team and guide your admin through developing these use cases themselves. |
| Month 4 | **Improving the Efficiency of Splunk SPL**<br>• Review end user queries, alerts, and reports to ensure searches are designed to best practices and perform as expected.<br>• **Poorly written queries can result in slow response time, failure to populate data models, and in some cases can completely bring down your Splunk environment.**<br>• This exercise simultaneously provides your team with more efficient searches, as well as the knowledge transfer to continue to build skills and competencies to optimize searches themselves in the future. |
| Month 5 | **Training your Admin for Splunk Care and Feeding**<br>• SP6 Splunk SME's will advise your admin on the best practices for keeping Splunk performant as more data, users, and queries are added to the platform.<br>• Your admins will learn all of the tools and techniques SP6 Splunk SME's use to troubleshoot problems and monitor a Splunk environment – including btool, the Monitoring Console, and License Usage reports. |
| Month 6 | **Dashboard and Report Creation**<br>• SP6 Splunk SME's will conduct live sessions with your admins and interested power users to develop their skills and confidence with building dashboards and reports in Splunk with real use cases and real data.<br>• Your admin will be enabled to build rich, effective visualizations and create the workflow within a dashboard you desire. |
| Month 7 | **Discovery of Additional Technology Integration**<br>• Over the life of a Splunk deployment, there will be new IT products to integrate with Splunk.<br>• SP6 Splunk SME's will help your admin find the best way to integrate new data sources or platforms with Splunk, and provide advice on how best to leverage this data. |

| | |
|---|---|
| Month 8 | **Utilize New (Or Unknown) Features in Splunk**<br>• There are a lot of apps and add-ons available in Splunk and new ones are being added every day.<br>• SP6 Splunk SME's will advise your admin on apps, add-ons or new features with Splunk itself that may benefit your organization. They can also advise on when it may be the right time to move into other Splunk products such as Enterprise Security or User Behavior Analytics.<br>• Often times there are overlooked add-ons and features that can provide immense value, things such as: Lookup Editor, LDAP (AD) Search, HTTP Event Collector, Indexed Extractions, or Splunk Metrics. |
| Month 9 | **Repurposing Data**<br>• Often times, **data ingested for one particular team or one particular use case can be very valuable for other teams.** Authentication data ingested for security can provide application usage statistics to DevOps. Network events ingested for infrastructure debugging can be trace logs for the security team.<br>• **SP6 Splunk SME's will examine how data already being ingested into Splunk (*and already paid for*) can be re-purposed for other critical uses within the customer's organization.**<br>• The end result is additional value for your organization with little to no additional costs. |
| Month 10 | **Executive Dashboard Development**<br>• Many organizations ultimately desire a high level, single pane of glass view of what's going on in their environment.<br>• SP6 Splunk SME's will help your team identify what matters in your environment and how best to display it at an "Executive" level.<br>• These dashboards can help track progress with your team's goals over time, identify where things may be lagging, and really tie together all the valuable data in your logs. |
| Ongoing and given attention to as needed | **Assistance with Splunk Care and Feeding**<br>• Troubleshooting and remediating performance issues, warnings, alarms, and errors.<br>• Debugging data input issues and data quality problems.<br>• Splunk upgrades, as well as app and add-on upgrades.<br>• Guidance on managing Splunk storage and retention.<br>• Other admin-related tasks as identified and needed. |

**Please Note:** The following represent prescriptive activities that form the basis of the ongoing Success Plan℠ for Splunk. They are listed in the order in which SP6 feels makes the most logical sense and adds the most value. However, this is not a rigid sequence. Our program is built upon a flexible model that allows our Splunk SME's to pick and choose, based upon specific customer needs and requests, what component of the program is performed in any given month.

This Plan is not a stand-alone service; meaning it can only can be attached to a recent SP6 Professional Services engagement with the customer. Why? It's critical that prior to engaging in this program, that SP6 has spent hands-on-keyboard time in the customer environment, in order to really understand the customer's starting point, environment and objectives.

| Program Guidelines | |
|---|---|
| > 20 GB daily data ingestion | Twice per month 60-minute web conference<br>(4) hours of total service time including work performed outside of these calls |
| > 50 GB daily data ingestion | Please consult with SP6 to determine Success Plan℠ time requirements<br>Customer may also want to consider SP6's Managed Splunk Services |