splunk> | data SOLUTIONS

The Splunk Guide to SIEM Replacement

Table of contents

1. Why should I replace my SIEM solution?

2. Why Splunk?

3. Replacing a traditional SIEM with Splunk

4. What can I do today to prepare for a SIEM replacement?

5. Business case: Managing the cost of change

6. Managed service provider SIEM replacement scenarios

7. SIEM solution design

8. Introducing Splunk Professional Services

9. The Splunk SIEM replacement approach

Splunk Enterprise Security is a market-leading security information and event management (SIEM) solution with powerful capabilities. Splunk has a best-in-class professional services organization that exists to support customers in maximizing their ROI from Splunk. After delivering hundreds of successful SIEM replacements, we feel confident that there's something here for organizations of any size and maturity. In this document we'll cover:

- Why organizations might decide to replace their SIEM solution
- The considerations of total cost of ownership, total cost of change, time to value and ultimately, value itself
- Splunk's powerful SIEM capabilities
- How to replace a SIEM with Splunk's best practices and replacement methodology
- How to prepare for a SIEM replacement
- SIEM design considerations
- SIEM replacement scenarios and best practices specific to managed service providers (MSPs)
- Success stories, next steps and calls to action

We're excited to share what we've learned about the process and to partner with you on your SIEM replacement journey.

1. Why should I replace my SIEM solution?

Security operations require a modern SIEM solution to power the SOC of the future. The key capabilities include:

- Achieving comprehensive visibility by making sense of data noise
- Empowering accurate detections with context
- Fueling operational efficiency through unified detection, investigation and response workflows

These features are a baseline for successfully detecting and responding to emerging threats. Without these capabilities, organizations must rely on disparate point detection systems, which results in an untenable level of manual labor.

So if the SIEM is so key, why would we replace it?

There are plenty of reasons why an organization might decide to replace its existing platform, and most of them have to do with *value*. Value is the return for using a technology over and above the amount invested. If you spend a dollar on a technology and get two dollars out of using it, you're getting one dollar of value. Usually this value-based decision is the result of some combination of the factors below, including:

- Product functionality
- Total cost of ownership (TCO), including factoring in the total cost of change (TCC) and value realization
- Vendor relationship

Let's break each of these down in a little more detail, so we're working from the same definitions.

> *We're going to reuse a few acronyms repeatedly in this document; let's make sure we're aligned on their definitions before we move on:*
>
> - *TCO: Total cost of ownership*
> - *TCC: Total cost of change*
> - *ROI: Return on investment*
> - *TTV: Time to value*

Product functionality

This one is easy: If your current SIEM is outdated, the vendor likely has not invested in ensuring the technology keeps up with the pace of innovation and the evolving threat landscape. It may no longer provide what you need in order to mitigate the risks to your business. Alternatively, a homegrown solution that worked well when you were a startup may have started to outlive its usefulness, and you're rubbing up against its technical limitations. Whatever the reason, if the product isn't cutting the mustard, it's time to start evaluating your options. The Gartner Magic Quadrant — a series of market-leading research reports on technology providers — is a good place to start for most organizations.

Total cost of ownership (TCO)

Risk is a magical concept. At its most basic, the theory of business risk stipulates that if a threat to your business presents one dollar of material risk, spending two dollars to mitigate said risk doesn't make a whole lot of sense. Your SIEM technology is not immune to this logic. If, based on your own business risk analysis, the TCO of owning and running a SIEM is greater than the price you think is logical to pay, you really have two options:

- Increase the value (usually in the form of amount of financial risk mitigated) that your SIEM is providing — we'll discuss value realization in more detail later
- Reduce the TCO of your SIEM

Notice we said "reduce the TCO," not "reduce the license cost." This is because TCO consists of more factors than just the cost of the solution. How you calculate TCO will depend on your organization, but some fairly common factors which may play into it are:

- Technology cost
- People cost
- Process cost

Let's explore these concepts briefly, so we have an idea of how to think about TCO.

Technology cost

This factor is deceptive. Certainly, the cost of your SIEM license might feel high, but so is the cost of the additional point solutions — firewalls, endpoint protection, secure email gateways and more — that you may need, depending on missing product functionality. Additionally, there is the cost of outages, which occur when the technology doesn't perform as expected or it is hard to configure for resource efficiency. There's also the people cost of engineering and integrations if the product(s) make tasks like onboarding data sources (or configuring new correlations) overly time consuming and burdensome — or even worse, so simple that they lack the fidelity to provide any value; meaning our old friend, risk, starts to rear its head.

Many organizations feel like they need to invest in different technologies in order to reduce TCO, so consolidation becomes a key concept. Consolidation means taking two tools — Tool A and Tool B, with each tool covering 50% of a use case — and then moving to a single tool to achieve 100% coverage of the use case in question. This is almost always substantially more cost effective, and could be achieved by increasing the coverage of Tool A to 100%, or doing the same with Tool B. It could also be achieved by moving to a completely new tool, i.e., Tool C, which brings something new to the table. Although all of these moves will be likely to incur some level of cost of change, this one time capital expenditure (CapEx) can often easily pay for itself in terms of long term reduction of operating expenses (OpEx).

Splunk Lantern, Splunk's use case realization guide, is a great place to start to understand the use cases covered by Splunk's security portfolio with its use case explorer. For security-specific correlations, you can check out the Splunk research team's security content portal.

When thinking about different combinations of use cases, consider that technology use cases exist outside the world of security. If you can procure a tool that supports both your security business objectives and those of another team (e.g., ITOps, observability), you can achieve substantial cost of ownership gains by consolidating tools and leveraging efficient data pooling.

No matter how you calculate technology cost, the following principles can help guide your decision making:

- Consider product costs holistically, rather than focusing on a single license cost.
- Consider the impact of technology cost on people cost.
- Consider the power of consolidation.

People and process cost

People and process costs are strongly interlinked, so we've combined them into one section. This is because the total cost of a person's time is closely linked to the time it takes for them to complete a process, like alert triage.

Again, this can be a bit more involved than it first appears. The most basic way to think about people cost is to consider the cost of a SOC analyst's time. Take the below scenario where:

- A SIEM generates 1000 alerts per day
- An analyst needs 10 minutes (m) to triage an alert
- An analyst has eight available hours in a day, comprising 480 minutes a day

We can also write this out as a simplified textual algorithm:

Alerts (1000) x Analyst Time to Triage 10m = 10,000m

If the above is true, this means that in our scenario we need 20.8 analysts to cover a single day's alert triage. Let's call it 21, since 0.8 of an analyst doesn't translate to the real world.

Alerts (1000) x Analyst Time to Triage 10m = 10,000m

10,000m / 480 (Analyst Daily Available Minutes) = ~21 Analysts per Day

If we need 21 full-time employee (FTE) analysts per day, and the fully loaded, *daily* cost of an analyst is $500, this means we need to spend $10,500 a day to keep on top of our alert triage.

Alerts (1000) x Analyst Time to Triage 10m = 10,000m

10,000m / 480 (Analyst Daily Available Minutes) = ~21 Analysts per Day

FTE Fully Loaded Cost ($500) x 21 Analysts per Day = $10,500

Now consider the impact of false positives or other confounding factors on these numbers. Let's say, for your 10,000 alerts, 80% (8000) of these are low-fidelity detections. This is a pretty normal number for your average organization. By nature, low-fidelity detections are noisy and have high false positive (FP) rates. Let's assume the FP rate for these low-fidelity detections is 50% (4000) of the 80% (8000) total low-fidelity detections, and 40% of all total daily alerts. This would mean that the below calculation is true:

40% of 10,000 = 4000 FP Alerts

4,000m / 480 (Analyst Daily Available Minutes) = ~9 Analysts per Day

FTE Fully Loaded Cost ($500) x 9 Analysts per Day = $4500

If 40% of your alerts are low-fidelity false positives, you would end up spending $4500 a day to triage false positives. Reducing this number of false positives through superior fidelity detections — or a meta-alerting paradigm like risk-based alerting (RBA) — could therefore substantially reduce your people cost.

In the real world, calculating analyst cost is a bit more complicated than this. Analysts don't cost the same amount, triaging an alert is only step one of a chain of possible investigations and all alerts don't come in at an even, daily rate, etc. Nevertheless, this should help illustrate the concept that managing your people cost can be an important factor for managing TCO.

You can apply this same concept of measuring people cost to the other personas interacting with your SIEM, such as engineering cost, which might be impacted *negatively* by the cost of getting data in (GDI) — typically influenced by the complexity of onboarding new data sources — or be impacted *positively,* through the implementation of a detection as code (CI/CD) methodology for efficiently and effectively managing detections, or through automation.

Total cost of change (TCC)

The total cost of change describes all of the costs you incur when moving to a new technology such as a SIEM. The cost of implementation is only one element of TCC. Education and value realization are also critical elements and should be factored in. When we use the term value realization in this context, we're talking about the time it takes to achieve the business use cases which drove the decision to purchase a technology in the first place, such as achieving detection and response capabilities against defined threats in order to mitigate business risk.

> *Splunk's Professional Services team produces a phase-based implementation plan, which covers initial implementation as well as long-term value realization. Value realization is key to realizing the ROI associated with an investment.*

TCC is important to understand, because if you decide that the best way to reduce TCO is to combine use cases or to replace a SIEM entirely, the process of moving to that new SIEM will incur a cost. The time that it takes for the reduction in TCO to be equal to, or greater than, the TCC is the time it takes to achieve a positive ROI. For example, if your current TCO is $1,000,000 per annum, your TCC to move to a new SIEM is $300,000, and the TCO of the replacement SIEM is $700,000, you will recoup the cost of the move over the course of the first year post-change, breaking even at the end of the year, and then from that point will achieve positive ROI. Only your business can judge what the appropriate time horizon is to achieve this positive ROI.

You should also consider the factors below:

- Lower TCC is good, but only in the context of the TCO. It doesn't make sense to lower TCC only to increase TCO at an equivalent amount, since TCO is an ongoing cost and TCC is a one-time cost.
- Lower TCO is good, but if the TCC associated with that option is so high that it makes the possibility of a move challenging — *or* the ROI time horizon is so long that it's outside of the range of acceptability to your business — then that move is no good.
- Lower TCO with manageable TCC tends to be a sweet spot for a SIEM replacement, especially when partnered with other improvements, like product functionality and value realization.
- When managing TCC, factor in education and value realization. Achieving technical implementation of a technology without enabling your teams to use it, and without achieving some or all of the use cases you purchased the technology for, can result in an extended ROI time horizon and negative savings. Don't focus on cost, but instead on the value extracted in return for your spend.

Vendor relationship

When choosing a SIEM vendor, product capability and cost are essential factors. But one key consideration that's often overlooked is the type of relationship you'll be building with the vendor you're working with. When looking at different SIEM solutions, find out whether or not the vendor has a methodology for value realization based on your organizational needs. This is going to be a critical ingredient for your achievement of ROI and value.

> *Splunk's Professional Services team works with customers to produce a customized value realization roadmap which drives down time to ROI, and drives up value.*

2. Why Splunk?

Splunk helps make organizations more resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions and accelerate digital transformation. Splunk helps security, IT and engineering teams deliver these outcomes with comprehensive visibility, rapid detection and investigation and optimized response, all at the scale necessary for the world's largest digitized organizations.

Splunk Enterprise Security

Splunk has paved the way in advancing SIEM and security analytics. Our innovations have helped thousands of customers outpace adversaries. As an industry-defining SIEM and security analytics solution provider, only Splunk has been named a leader by multiple analysts, earning the distinction of a hat trick.

Splunk Enterprise Security is the trusted choice for SOCs around the globe. Its powerful capabilities deliver comprehensive visibility, empower accurate detection with context and fuel operational efficiency. Powered by an extensible platform and assistive AI-driven capabilities, Splunk Enterprise Security ensures analytics at scale for continuous security monitoring and cost-effective data optimization. With this foundation, you can detect what matters, investigate holistically and respond rapidly.

Realize comprehensive visibility

Splunk's data-powered platform with assistive AI capabilities offers unmatched, comprehensive visibility by seamlessly ingesting, normalizing and analyzing data from any source at scale. It offers continuous monitoring and correlation across security tools regardless of deployment — on-premises, cloud or hybrid — to help maximize attack-surface coverage. Find threats with comprehensive search and use Splunk AI Assistant to translate searches into SPL to save time. Splunk's custom alert actions feature makes it simple to take fast action. These custom alerts can be set to varying levels of granularity based on a variety of conditions, such as data thresholds, trend-based conditions and behavioral pattern recognition like brute force attacks and fraud scenarios.

Splunk Enterprise Security ensures cost-effective data optimization by ingesting only data critical to security use cases. Users have the flexibility to store and access their data, including at the edge, based on data tiering. This reduces forensics and compliance storage costs for added savings.

Empower accurate detection with context

Risk-based alerting (RBA) within Splunk Enterprise Security drastically reduces alert volumes by up to 90%. RBA uses the Splunk Enterprise Security correlation search framework to collect risk events into a single risk index. Events collected in the risk index create a single risk notable when they meet specific criteria, so you can stay focused on imminent threats that traditional SIEM solutions might miss. This boosts productivity and ensures the threats you're detecting are high fidelity.

The Splunk Threat Research Team delves deep into detection engineering, providing you with 1,700+ out-of-the-box detections so you can find and remediate threats faster. These detections align to industry frameworks like MITRE ATT&CK, NIST CSF 2.0 and Cyber Kill Chain®. Splunk also provides a machine learning toolkit to accelerate your ability to uncover threats with anomaly detection.

With Splunk Enterprise Security, you can enhance your security program with customizable dashboards, visualizations and reports. For example, you can operationalize the MITRE ATT&CK framework with a visualization matrix that highlights the tactics and techniques observed in risk events to save time when investigating. Additionally, you can discover the scope of an incident and respond accurately using the Threat Topology visualization. With the enhanced risk analysis dashboard, security analysts can monitor user entity risk events from detections across RBA and behavioral analytics.

Fuel operational efficiency

Centralize workflows and unify processes across detection, investigation and response to fuel SOC operational efficiency and stop breaches with Mission Control, an integral feature of Splunk Enterprise Security. Mission Control unifies your workflows, strengthened by automated playbooks infused with threat intelligence that brings together and normalizes data source scoring. This enables you to streamline SOC processes by adhering to predefined templates to reduce manual effort and pivoting between disparate tools.

You can achieve an appreciable increase in operational efficiency with Splunk's unified platform for data aggregation, analysis and automation. Additionally, Splunk is vendor-neutral so can support any number of use cases, enabling you to build what you need. You can leverage a thriving partner network of 2,200+ partners to create custom apps and seamlessly integrate existing tools, plus increase SOC efficiency by collaborating with the Splunk Answers community and tapping into Splunkbase's 2,800+ partner- and community-built apps.

Gain control of regulatory risks

As compliance requirements become increasingly complex, Splunk enables you to collect, search, monitor and analyze data using a centralized solution. You can rapidly meet requirements around log management and long-term log storage and use the Splunk compliance apps — PCI, GDPR, Essentials for Industrial Control Systems and more — for insight into your organization's compliance status.

Our suite of products aligns to the various requirements for the SOC of the future, including those outlined above. These products include:

- Splunk Enterprise: Data Analytics and Investigations Platform
    - Scalable data analytics platform; supports IT, security and fraud use cases for zero trust architectures
    - Ability to ingest a broad range of structured and unstructured data
    - Comprehensive partner ecosystem; includes zero trust solutions to support integration, as well as rapid data source onboarding and normalization

- Splunk Enterprise Security: Security Information and Event Management (SIEM)
    - Extensive security monitoring and detection use case library, supported by Splunk Security Essentials (SSE) and Enterprise Security Content Update (ESCU)
    - Key frameworks to support the enrichment and contextualization of asset and identity data, risk scoring and security posture in support of zero trust objectives
    - Risk-based alerting (RBA) helps with advanced risk scoring and multi-indicator detections aligned with the MITRE ATT&CK framework. Looks across zero trust controls for a sequence of activity that could indicate malicious behavior
- Splunk User and Entity Behavior Analytics (UEBA)
    - Out-of-the-box, unsupervised machine learning for advanced behavioral detection and automatic identity resolution
- Splunk SOAR: Security Orchestration, Automation and Response (SOAR)
    - Comprehensive case management, incident investigation, orchestration and automation to respond to security and service incidents across a zero trust architecture

3. Replacing a traditional SIEM with Splunk

There's never been a better time to swap your traditional SIEM for a SOC of the future. Splunk Enterprise Security, Splunk's flagship SIEM, sits at the core of Splunk's security suite, boasting powerful features and capabilities for decreasing time to value and increasing rapid ROI.

Out-of-the-box use cases

Splunk Enterprise Security ships with over a thousand out-of-the-box (OOTB) use cases, supplemented by threat detections and content updates from Splunk Security Essentials, mapping to modern detection frameworks including MITRE ATT&CK. Splunk Enterprise Security, combined with Splunk Professional Services, makes it easy to map legacy SIEM use cases to these OOTB use cases and achieve extremely rapid TTV.

Risk-based alerting

Risk-based alerting (RBA) provides teams with a unique opportunity to pivot resources from traditionally reactive functions to proactive functions in the SOC. As alert fidelity and true positive rates increase, analysts' resources can be shifted to higher impact tasks like threat hunting or adversary simulation, empowering SOCs to build up the skill sets of their analysts and prepare them for any threats they might encounter.

The RBA methodology is very similar to what you're most likely already doing in Splunk Enterprise Security. It uses nearly all of the existing frameworks within Splunk Enterprise Security, but includes a few optimizations that dramatically increase efficiency and general security maturity within the SOC.

The benefits of RBA include:

- Creating more time for high-value activities in your security organization like threat hunting, adversary simulation and security content development
- Aligning with cybersecurity frameworks like MITRE ATT&CK, the Lockheed Martin Kill Chain, and CIS2
- Meeting and exceeding security audit requirements resulting in a much smoother audit season
- Reducing low-fidelity, time-consuming alert volume by 50-90%

Managing TCC and TCO with RBA

RBA can help SOC teams bring the number of alerts they're triaging under control. If you followed the examples we gave in section one for calculating the cost of an alert, you can probably guess that using RBA to manage and consolidate low-fidelity alerts into high-fidelity detections will help rapidly and dramatically reduce SOC operating expenses, driving down TCO.

What you may not have considered is that implementing a meta-alerting paradigm like RBA can also drive down TCC. It does this by providing a framework for rapid testing and promotion of new correlation searches with much lower stakes.

RBA Example

Let's consider the following example. In a standard correlation frame where one detection equals one alert, a specific value will be applied to a security event to create a trigger. This means if you create a detection for failed logins, you could configure trigger threshold A to trigger an alert after five failed attempts and trigger threshold B to trigger an alert after 10 failed attempts. If a user or computer fails to log in six times with threshold A, an alert would be created for the event. However, if you implemented threshold B instead, no alert would be generated, even in the face of a likely attack.

This is quite high stakes — if the alert threshold is too high, false negatives will be a common occurrence; but if the number is too low, analysts will be spammed with false positives.

Fortunately, with RBA, you can rapidly iterate on alerts based on the corresponding risk. For example, if there's a low risk score attributed to an alert via Splunk's risk framework F, most of the events associated with the false positives would skip your analyst's queue. As you gain confidence in the fidelity and relevance of the alert and the accuracy of the threshold configuration, you can increase the risk score as needed. Once you understand your business risks and threat model, you can start to utilize risk modifiers to set a multiplier against your risk generation based on the importance of the target user or computer.

RBA Summary

RBA allows you to reduce TCO and TCC when replacing a SIEM by enabling you to turn low-fidelity alerts into aggregated high-fidelity meta alerts. This reduces the number of alerts your analysts need to triage and allows your security engineering team to more rapidly implement the use cases your business needs to drive value.

> *For more information on all things RBA, consider reading Splunk's Essential Guide to Risk Based Alerting (RBA).*

Incident management

Incident management refers to the ability to manage alerts in a ticketing system. This allows analysts and other stakeholders to easily collaborate on investigations, assign tickets, and report on and document investigation outcomes.

When considering product functionality, a robust incident management dashboard allows analysts to work in a unified view without toggling between multiple screens and tools. There's also a high degree of cohesion with other SOC tools, including Splunk SOAR and UBA.

When considering cost, incident management allows an analyst to use a single platform, rather than external third party ticketing systems, which helps keep down the TCO of a SIEM platform. This is due to both reducing license costs through consolidating on a single tool and reducing engineering costs of ongoing integration between multiple systems.

Splunk Security provides options for incident management that allow for consolidation into a single tool based on your preferred analyst incident management workflow, helping you achieve superior outcomes.

Splunk Enterprise Security and Splunk SOAR

Splunk Enterprise Security provides the incident review dashboard for incident management. Splunk SOAR also provides its own case management dashboard. Both of these capabilities provide rich feature sets, and can add significant value depending on your organization's preferred SOC operating model. SOAR can exist in the backend to provide automation only ("headless mode"), or become the incident management system of choice for a SOAR-oriented SOC, ingesting alerts directly and seamlessly from Splunk Enterprise Security.

Mission Control is a feature of Splunk Enterprise Security for cloud users globally and provides a unified, simplified and modernized security operations experience for your SOC. Mission Control provides a "best of both" single-pane-of-glass view into Splunk Enterprise Security and Splunk SOAR. This seamless integration reduces the time analysts spend getting the information they need, by presenting a single work surface to detect what matters, investigate holistically and respond intelligently, and by enriching events with contextual information to reduce follow up investigation time. Because the Splunk Security Portfolio leverages automation to enrich events and automate actions, a move to using Splunk for Case Management can drive down TCO by reducing time spent on repeated low grade manual analyst tasks.

> *Splunk Professional Services can help architect the right case management approach for your organization and assist with the documentation of analyst workflows and runbooks required to make use of your new SIEM platform. This helps to manage the TCC associated with a move to a new case management workflow.*

Automation

Native SOAR Integration

Splunk SOAR is Splunk's security orchestration, automation and response solution. Splunk Enterprise Security integrates natively with Splunk SOAR. This means getting up and running with Splunk Enterprise Security and Splunk SOAR is fast and easy.

Assets and identities

Splunk Enterprise Security comprises several frameworks, including the Asset and Identity (A&I) framework.

Splunk Enterprise Security uses an asset and identity system to correlate asset and identity information with events to enrich and provide context to your data. This system takes information from external data sources to populate lookups, sets of reference data stored in Splunk, which Enterprise Security correlates with events at search time. This ability to utilize contextual information at search time dramatically enhances the contextualization and fidelity of alerts.

Threat Intelligence

Another Splunk Enterprise Security framework is the Threat Intelligence (TI) framework.

As a Splunk Enterprise Security administrator, you can correlate indicators of suspicious activity, known threats, or potential threats with your events by adding threat intelligence to Splunk Enterprise Security. Adding threat intelligence enhances your analysts' security monitoring capabilities and adds context to their investigations.

Splunk Enterprise Security includes a selection of threat intelligence sources. Splunk Enterprise Security also supports multiple types of threat intelligence so that you can add your own threat intelligence.

This ability to natively ingest an array of threat intelligence sources out of the box, means you can integrate your existing threat intelligence subscriptions and easily bring in open source data to tailor your correlations to your organization's threat model, ensuring you bring rapid value from your threat intelligence feeds.

Splunk Machine Learning

Splunk Enterprise Security utilizes the Splunk Machine Learning Toolkit app to help your data scientists and security engineers rapidly develop and implement enterprise-grade machine learning. The Splunk Machine Learning Toolkit is available for both Splunk Enterprise and Splunk Cloud Platform users through Splunkbase. It acts as an extension to the Splunk platform and includes machine learning SPL search commands, macros and visualizations.

Splunk Security Essentials

To ensure you can get rapid ROI from your SIEM solution with Splunk, Splunk provides a free app. Splunk Security Essentials allows you to easily map your business requirements and data sources to Splunk's library of over 1700+ out-of-the-box security detections.

Splunk's Professional Services team utilizes Splunk Security Essentials in their use case workshop engagements. App functionality allows you to own and iterate on the output of these engagements yourself, or use your own use case planning as input for analysis.

4. What can I do today to prepare for a SIEM replacement?

So, you've decided to replace your SIEM. Great! If you're still deciding which vendor you should use, and biding your time until the right point in your organization's budget cycle, there are still many steps you can and should take in the lead up to kicking off your SIEM replacement transformation. In this section we'll cover some key considerations for before and during your engagement with vendors as you continue your SIEM replacement journey.

Gather requirements

This is a great time to consider your requirements. Whether it's in your SIEM RFP or in your conversations with vendors, you will need to articulate what your solution needs to do to meet your business objectives.

Here's a checklist to help you get started with thinking about your SIEM requirements:

- **What are the functional requirements?** What business problems are you looking to solve and what do you need the replacement SIEM to do that your current SIEM does not?
- **What are the non-functional requirements?** Uptime, reliability, scalability, etc., that you need in order to provide a resilient solution in line with your business's risk appetite?
- **What is your timeline?** When do you need the new SIEM to be in place? Is your current license expiring, or is there an MSP you need to get away from?
- **What are the business use cases you are trying to address?** Will the technical use cases come over from your old SIEM, or will you start with a fresh, "green field" approach? Creating a use case inventory of your current coverage will drive any use case mapping exercises.
- **Do you need other security technologies in the future, such as SOAR?** Consider the possible future requirements of your business, rather than just the requirements you have now.

- **What are your key data sources?** If you partner with Splunk Professional Services to plan your implementation, they will need to know your key data sources alongside your business use cases to optimize your onboarding strategy.
- **What are your data volumes?** Being able to share this information with vendors as accurately as possible will ensure you can get timely, accurate license estimates.
- **What regulatory requirements will you need to meet with your new solution?** Do any of these mandate that retain data for a certain period of time?
- **What are the required integrations with your other technologies?** If you partner with Splunk Professional Services, they will need to understand your integrations to accurately scope and plan your implementation.

Identify stakeholders

As you gather your requirements, you will inevitably run into additional stakeholders. These are all the individuals and teams who have a stake in your SIEM solution. Some of these are obvious, such as your budget decision-maker and head of security. Less obvious are the other teams who may wish to utilize your new SIEM solution for other use cases, in the interest of TCO reduction and business spend optimization. If other stakeholders will be joint users of the platform, start thinking about how that usage will be shared or prioritized.

Define your budget

After you've gathered your requirements and aligned your stakeholders, you need to define your budget. This will help you to define an appropriate data tiering and routing and filtering strategy, and will help your vendor determine the most cost-effective solution for your business.

Engage the Splunk team

It is never too early to start talking to vendors. Engaging Splunk early can help ensure you have an accurate understanding of the available technologies, and can accurately forecast the potential cost of your new solution.

5. Business case: Managing the cost of change

Introduction

Cost of change, or TCC, refers to the cost of any business transformation. When calculating the investment case for a new technology, the cost of change is factored into the TCO over an appropriate period, typically three or five years. If a technology costs $100,000 to implement in year one, but enables cost savings of $70,000 annually for five years over a five-year term, then it is a logical business decision to accept that TCC.

Cost of change vs. new operating cost

TCC refers to the total cost of making a change. The operating cost of your new solution refers to the cost you expect to incur once the change — in this context a SIEM migration — has been made. When considering the business case of any potential cost of change, you should weigh it against the new operating cost of your planned solution.

Typically, transformation projects such as implementing a new SIEM are considered CapEx, while the subscription license and maintenance costs of the SIEM, once implemented, will be considered OpEx.

Your organization may have a preference for considering the cost of change as a CapEx or OpEx expenditure. Work with your vendor to understand how any license or services costs can be packaged in order to work with your organization's budget.

Calculating potential post of change

In order to accurately estimate the cost of change, you will first need to have a clear understanding of your requirements.

Elements that will comprise your cost of change might include:

- The cost of reskilling your security analysts and engineers to work with your new SIEM
- The cost of any professional services required to design, implement and advise on your new SIEM
- The cost of any data migration or dual forwarding
- The effective dollar cost of any additional business risk incurred during the transition, as you redirect resources to focus on this project engineering work rather than standard operational engineering work
- Any crossover of license between your traditional and replacement SIEM
- The cost incurred by your procurement, legal and other teams in working with your replacement SIEM vendor

Managing cost of change

Now you know what the cost of change is, you understand why you want to keep it as low as possible.

Actually, that's not entirely accurate. We want the cost of change to be as low as possible, while also maximizing the ROI associated with the new solution. If your new solution will save you significant expense every day you use it, wouldn't it make sense to spend a little more to achieve that savings faster? We will dive deeper into finding that balance in this section on managing cost of change.

Reducing cost of change

How can you reduce the upfront cost of change? Let's consider the options one by one:

- **Effective planning:** The number one way to manage cost of change is to prepare. Any data you gather and document now will save time spent with Professional Services interviewing and identifying your requirements. The more up front and articulate you can be, the lower the cost of services will need to be.
- **Getting it right the first time, quickly:** It can be tempting to attempt to DIY your SIEM replacement. Repeated experience in our Professional Services organization has shown partnering with Splunk is one of the fastest and most reliable ways to migrate your SIEM. Failing to complete a SIEM migration because you attempted to do it without supervision, or with an unaccredited organization, is the fastest way to balloon your cost of change.
- **Building your skills:** Enabling yourself and your teams on the new SIEM will help them get up to speed quickly and allow them to help with implementation activities. This can reduce the scope of work for Professional Services, lowering overall cost. At Splunk, we offer courses and training through Splunk Education to help you meet your Splunk skills goals.
- **Be selective:** If you don't need to migrate your data, don't need your traditional SIEM use cases and don't need all of your data to be kept in hyper-performant storage, then Splunk can help reduce the scope of migration services.

Increasing ROI

Reducing cost of change is important, but ultimately this SIEM replacement project needs to both reduce costs *and* realize value. Only your organization can make a judgment on what spend is most effective. Make sure that rather than setting arbitrary limitations on cost of change, you are considering it in the context of your TCO over an appropriate period. If spending more now will save more over a three-year term due to increased ROI and value realization, it is likely worth the up-front investment.

6. Managed service provider SIEM replacement scenarios

Introduction

Managed service providers (MSPs) are ubiquitous in the modern security space. Sometimes referred to in this context as managed security service providers (MSSPs), they provide SOC services that address one or more of the following areas, among others:

- Threat detection and monitoring
- SIEM engineering
- Incident response
- Vulnerability management
- Compliance monitoring and reporting

Typical use cases for MSPs in the SIEM space might include:

- Lowering TCO by externalizing one or more SOC function
- Bootstrapping a net-new SOC capability

To understand how MSPs can lower TCO, it is helpful to consider the MSP business model. An MSP will rarely have only a single customer. Instead, MSPs leverage efficiencies of scale, training teams and designing security platforms based on a consistent methodology. MSPs manage each customer's service using this total capability for a lower cost than the customer would need to spend in-house on the service. This means that using an MSP has the potential to be an efficient exchange for both the provider and the customer. Most organizations that are not in the business or running a security service would have to invest a substantial amount to create their own SOC. Why do this when you can leverage the capacity of an organization that does this as their bread and butter?

On the other side of the coin, by understanding how an MSP can leverage scale to create value, you can also see that there is an incentive for an MSP to take a scalable approach. This means that the level of customization for your specific organizational needs may vary. You may find that once you start approaching a higher level of maturity, you struggle to get the level of specificity required by additional levels of maturity, though this depends on the nature of the service provider.

The decision of whether or not to use an MSP is typically a decision based on a sliding scale between cost and customization, and your organization's relationship with current and potential MSP providers. Factors can change over time; however, the good news is that whether you are an organization considering outsourcing capabilities to an MSP, or want to bring some or all of your MSP's capabilities in-house, Splunk has product features, professional services capabilities and the experience to support your move while keeping the TCC manageable.

Splunk Professional Services has worked with many customers to support insourcing of existing MSSP capabilities through leveraging our tried-and-tested SIEM replacement approach, product capabilities and domain expertise.

Whether you are creating a greenfield SOC or expanding existing capabilities, Splunk Professional Services can assist with designing and implementing Splunk RBA to maximize in-house analyst efficiency and quality of life and control TCO.

Splunk Professional Services has experience discovering and translating common MSP metrics with Splunk solutions through a process of use case mapping and rationalization:

- Framework coverage (e.g. MITRE ATT&CK, compliance)
- Risks mitigated
- Use cases implemented
- Alerts remediated

Help architect around the complexity of multiple business units using multi-tenancy, RBAC, service-level based design, automation, data tier classification, CI/CD process definition and more.

Insourcing

Insourcing a subset or the totality of your MSP's SIEM estate can be a big change. How big of a change depends on whether you are:

- Insourcing end-to-end SOC capability and creating a net-new internal SOC, or
- Insourcing a subset of SOC capability, such as Tier 2 (advanced) detection and monitoring

Clearly, insourcing an entire SOC capability and creating a SOC from scratch is a larger project than insourcing a subset of MSP functionality into an existing SOC. Let's treat these as two different scenarios and discuss how Splunk Professional Services can help.

A. In house: Insource everything

Insourcing your entire security capability is a big decision, but one many organizations make once they reach a certain size or maturity. Although TCO can be a big reason for insourcing, most organizations we work with choose to insource their entire security operations capability because they want a level of quality and relevance that they are struggling to get from the MSP market.

There are a few big decisions you'll need to make along the way:

- Will you keep the same KPIs and OKRs as you set for your MSP, or will you define your own? For example, number of alerts triaged is a common SLA for an MSP, but can be less useful for your internal capability.
- Will you attempt to migrate your MSP's use cases into your insourced SIEM platform? This can depend on whether you owned the previous SIEM, or whether your MSP managed it as a "black box" — without you having any insight into the underlying configurations. If the former, you can export and map the use cases to your replacement SIEM. If the latter, your MSP may not want to share their intellectual property, given that your relationship is ending, and you may need to start from the ground up.
- Will you need to migrate data from your MSP's solution? Depending on the contract you had with the MSP, this may not be possible, or may have an additional price tag.

The Splunk Professional Services approach

Splunk Professional Services has experience designing, implementing and documenting these transformations and can help you plan for insourcing from an MSP environment.

When moving to an insourced SOC, you have the opportunity to create a platform based entirely on your own requirements. This means Splunk can work with you to design a best-practice approach entirely tailored to your organizational needs.

B. Hybrid: Insource a subset

The good news is that if you're insourcing a subset of functionality into an existing SOC, you only have to add the capacity to perform that subset of capabilities, which will naturally have a lower TCC than doing everything. The challenge is that you will need to continue to work with your MSP with your new hybridized environment, which means your systems and runbooks need to be able to handle a multi-team approach.

When you're moving a subset of your MSP's capabilities in house, such as advanced detection and monitoring, or SOC engineering, you also need to consider that the reports and metrics your MSP provides to you to prove their value are likely not the same as the metrics that your business will expect from your internal SOC team. Where an MSP may rely on metrics like MTTR, MTTA and number of alerts triaged, your internal stakeholders may be more interested in the results of your more tailored internal investigations and insights into your progress in increasing risk mitigation and detection coverage.

The Splunk Professional Services approach

Splunk Professional Services can help with configuring a hybridized MSP environment. The team has experience designing, implementing and documenting relevant activities, as well as extensive experience working in hybrid MSP environments.

Architecting for success

- **Current state evaluation — Optimization checks:** If you are taking on a portion of responsibility for your security service, you will want to ensure that you understand both the current state of the SIEM platform's configuration, as well as a roadmap to achieve any optimizations required to increase value in any proposed future-state configuration. If the SIEM has been previously owned by an MSP, you may wish to verify that it is configured to best practice, and identify any gaps. Splunk Professional Services can perform this gap analysis and check whether existing SIEM configurations adhere to best practice.
- **System design:** When moving to a hybridized SOC, you will most likely also need to hybridize your SIEM. Even if you continue to use the same SIEM platform as your MSP as a co-tenant, you will still need to consider the new integrations and configurations your team needs to support your part of the security service. Splunk Professional Services can help produce a design that describes the new elements of this solution, and communicate these to your internal and external stakeholders, including your MSP. If you are planning to run two separate SIEM solutions, one internal and one external, Splunk Professional Services can assist with producing a design that describes the integration between your two systems, as well as performing the actual integration.
- **RBAC:** In order for multiple teams to leverage the same platform, you will need to plan a resilient and scalable index and RBAC design. Splunk manages access at the data layer through the use of these indexes and an RBAC model.
- **Workflows:** You will need to architect a case management platform design that supports your requirements. If your internal team requires different access to your MSP, you may need to create a multi-tenancy style RBAC model around not just your data, described above, but also your alerts. You can achieve this using Splunk Mission Control, and Splunk Professional Services can assist with creating a best-practice architecture supporting this objective, and documenting this alongside your planned case management workflows

Use cases and reporting

Use cases: Splunk can assist with providing a use case implementation roadmap during our Use Case Workshop, which can help define a collaborative approach with your MSP. Splunk Professional Services can solicit input from your internal teams, or from a combination of your organization and the MSP, to ensure that any roadmap is mutually agreeable, as well as aligned with best practices for rapid and consistent value realization.

Splunk Professional Services can also assist with implementing a subset of new use cases alongside your SOC team, to ensure you are able to build the skills needed to take on your new responsibilities as part of the insourcing project.

Reporting: When moving a subset of SOC functionality to sit internally, you will need to provide your own reports on the activities of your internal teams and no longer simply rely on reporting provided by your MSP. Splunk can assist with configuring reports and dashboards that tell the story you need, in order to communicate the results provided by your new internal SOC capability to key stakeholders.

Outsourcing

A. Fully managed service: Outsource everything

The purpose of a fully outsourced MSP is to remove the burden of security operations from your team. This means that there shouldn't be too much for you to consider when it comes to designing the solution. You will need to gather your requirements and share these with the MSP, and consider how you want to approach contracting with them, setting the appropriate KPIs and SLAs to meet your business requirements. Of note, the more stringent the SLAs, the higher the cost is likely to be.

Splunk works with a variety of approved partners to provide Managed Security Services for customers. If your organization is itself an MSP, Splunk Professional Services can help you design a performant and scalable solution for supporting multiple customers using Splunk. Take a look at the Splunk Content Manager app to see how you can manage content across multiple Splunk platforms today.

B. Hybrid: Outsource a subset

The same as outsourcing everything, but with an additional requirement to design the points of interaction and integration between your on-premise SIEM and your new MSP.

7. SIEM solution design

Designing a replacement SIEM doesn't just mean taking what you did before and replicating it with a new technology. Moving between SIEMs is an inflection point that you can utilize to optimize your SIEM platform and analyst experience, and ultimately drive superior outcomes at a lower TCO.

In this section, we provide an introduction to some of the many topics and concepts you will need to understand and engage with in order to create a blueprint for your future SIEM model.

To discuss any of these in more detail, please contact Splunk Professional Services. We can provide you with guidance and best practice solutions tailored to your specific requirements.

Data migration, dual forwarding and cutovers

Introduction

Moving between SIEMs means there will inevitably be a cutover period as you migrate from one technology to the next. These migration paradigms can take many different forms, but we most commonly see two — dual forwarding and "big bang."

Organizations must also decide whether to attempt to migrate the data out of their traditional SIEM or start afresh in their new SIEM, often referred to as a "greenfield" scenario.

There is no one best approach, and the right way to make this transition will depend on your organization's business priorities and objectives.

Data migration

Data migration refers to the act of taking some or all of the data stored in your traditional SIEM and pushing it into your replacement SIEM. Typically, this will be achieved by forwarding data from your traditional SIEM to your replacement SIEM.

Advantages

This approach can help decrease the amount of time needed for dual forwarding, reducing cost. It achieves this by helping you meet data retention requirements in your new SIEM more quickly. For example, if your regulator specifies that you must retain 100 days of data for critical devices in your SIEM tool, you would have to maintain 100 days of dual forwarding. If you migrate your data from your legacy to your replacement SIEM, you can reduce the time needed to meet this regulatory requirement. Additionally, this may allow your replacement SIEM to utilize a broader period of historical data in correlations, improving alert fidelity.

Challenges

Although data migration may sound like the obvious choice, there are some substantial challenges:

- If your traditional SIEM contains a substantial quantity of stored data, moving this to your new SIEM may incur substantial network costs. In the case of moving to an IaaS-hosted SIEM, check your cloud provider's data ingress costs, as these could be significant when migrating large quantities of historical SIEM data.
- The format of the data stored in your traditional SIEM is unlikely to be the same format as the data stored in your replacement SIEM. This means that although you can often send the data from your traditional SIEM into your replacement SIEM and store it, it may require additional custom effort to make the data usable alongside the data being sent to your replacement SIEM directly.

Ensure you are thoughtful about when to use a long period of historical data for correlations. It is quite rare for correlations to cover periods of time significantly longer than 30 days, although there may be exceptions for specific correlations covering low and slow activity such as beaconing, data exfiltration or long term denial-of-service (DoS).

Dual forwarding

Dual forwarding describes the scenario where an organization moves from a traditional to replacement SIEM over a controlled period of time, in order to ensure constant business coverage. This is achieved by setting data sources, or data source forwarders, to send to two or more locations.

Dual forwarding can be useful if a company policy or regulator demands that a certain time period of retained data must exist in a SIEM, and you do not plan to attempt a data migration.

In the context of a SIEM replacement based on a move to Splunk, dual forwarding will typically mean setting your data sources to send to both your traditional SIEM and to Splunk for a period of time. Once you have enough data in your Splunk solution to meet data retention requirements, or to prove security control functionality to a level acceptable to your business, data forwarding to your traditional SIEM can be switched, and the traditional SIEM can be decommissioned.

Advantages

The benefit of this approach is that it ensures that your business does not lose security coverage and meets any data retention requirements, ultimately reducing business risk.

Challenges

The downside is that it can be time- and resource-intensive, and may mean paying the simultaneous licensing cost of two solutions for a window of time.

Deciding whether to select this approach means comparing the value of the potential risk to your business to other approaches against the higher cost of a dual forwarding approach.

Dual forwarding is the most common approach Splunk Professional Services sees in the field, as most organizations prioritize resilience over cost savings during their SIEM transformation.

Store-and-forward

When migrating from a traditional SIEM, an alternative to dual forwarding is "store-and-forward" configurations. In a store-and-forward scenario, rather than setting your data sources to send to both your traditional and replacement SIEM simultaneously, you instead set your traditional SIEM to both store data and forward it on to Splunk.

Advantages

The advantage of this approach is that it is relatively simple to configure, reducing engineering effort and associated cost.

Challenges

The disadvantage of this approach is that once data has been processed by a traditional SIEM, it is typically no longer in its original format. Splunk brings huge value to customers through its app store, Splunkbase, which works with a community of developers and vendors to ensure data can be easily ingested and utilized in its standard format. Sending data from a traditional SIEM will typically mean these parsers cannot be used, and custom parsing needs to be created. Although this activity can often be performed quickly and easily by Splunk Professional Services, or by your organization's own team of Splunk administrators, this is time and effort that could be saved by selecting an alternative migration paradigm.

Second, although configuring a store-and-forward setup is relatively easy, it doesn't remove the need to cut data sources across at some point. Since a data source forwarded from another SIEM likely will not be in the same format, there may be additional work needed once the source itself is cut across to ensure it is being sent correctly.

Although store-and-forward used to be a common migration strategy, it is increasingly rare to see organizations use it to show rapid ROI in their new SIEM solutions, rather than simply using it as a security data storage tool.

Big bang cutovers

A "big bang" cutover describes the scenario where, rather than setting data sources to dual forward between your traditional and replacement SIEM, you instead move them over directly. This type of cutover is typically performed in a condensed time frame to minimize the time period where your organization does not have security coverage in a single tool.

Advantages

Big bang cutovers have one significant advantage: They get you to your new SIEM as quickly as possible. This can be particularly useful in MSSP insourcing scenarios, discussed earlier, or in the situation where you need to migrate from your traditional SIEM before license overages or cutoffs are enforced by your existing vendor.

Additionally, if your traditional SIEM is non-functional, and you do not have a regulator that requires you to have ongoing security coverage, or a set time period of data retention, there is not much disadvantage to dropping it and moving on.

Challenges

The potential problem with a big bang approach is that it will, by nature, leave you with a period of time where a portion of your data sources are going into your traditional SIEM, and a separate portion are going into your replacement SIEM.

There are many implications of this, including:

- There will be no singular SIEM you can point to that contains all of the data associated with an incident, should one occur during the big bang migration.
- There will be no "single pane of glass" for analysts. They will be hopping between two tools until the migration is complete, which makes performing their job exponentially more time consuming and increases business risk.
- There will not be time to properly test and confirm data and use case functionality as data sources are cutover. Any time taken to properly test each data source during the migration will extend the cutover period and heighten the business impact.

Any decision around adopting a big bang approach should be based on a rational analysis of your organization's circumstances. You will be accepting some amount of risk, but there may be competing risks that mean this is still the most logical course of action, especially if you are starting from scratch after a failed implementation with your traditional SIEM.

Splunk can make big bang migrations easier, as it utilizes a schema-on-read data processing methodology. This means that data doesn't necessarily have to adhere to any specific schema at the point of ingestion, and searches and parsing can be created on top of historical data after the fact to ensure it is still usable. Many traditional SIEMs instead utilize a schema-on-write data processing methodology, which means any data source moved across during the migration that does not align to its expected schema would be rendered unusable for security correlation.

Data classification and storage

Introduction

In our blog on the topic, Splunk describes data classification as "the process of organizing data in groups based on their attributes and characteristics, and then assigning class labels that describe a set of attributes that hold true for the corresponding data sets. We can consider it one part of an overarching data management practice."

In a SIEM context, we use data classification to control TCO without impacting solution usability. This is achieved by dividing data into tiers and choosing a storage and workload profile appropriate to each tier.

For example, if you plan to ingest security-relevant data used for alerting, this would likely be considered high-tier data — data that you need to be able to search quickly and reliably. On the other hand, you may ingest data that is for regulatory purposes only, and does not need to be searched except in rare incident scenarios. In such a situation, this data would be allocated to a lower data classification tier.

High-tier SIEM data will typically be stored in a fast access data store. Lower-tier SIEM data will be stored in a slower access data store, or may be archived entirely.

Splunk provides options for all tiers of data storage and archival, including utilizing remote object stores with SmartStore.

S3 federated search

In addition to SmartStore, Splunk provides the ability to search S3 data using federated search. As well as searching across Splunk environments, Splunk federated search for Amazon S3 lets you search data in your Amazon S3 buckets from your Splunk Cloud Platform deployment.

Workload management

Splunk workload management allows you to separate search and ingest resources into pools for prioritization. This can be critical in resource-constrained environments to ensure that an expansion of your least important data sources and use cases does not impact your business resiliency.

The most common example of architecting around workload management is to propose an ingest and search model in which critical use cases such as SIEM, which may coexist with other lower-priority workloads such as business analytics, are always prioritized by the system. This means in a scenario where you cannot necessarily control the usage of the platform — for example, in a situation where you share a Splunk platform with the business analytics team, utilizing it as both a SIEM and a business analytics engine — you want to ensure that should the business analytics team decide to ramp up their ingest or usage of the platform, you are guaranteed that your own security ingest and workloads are not impacted.

Planning for cross-functional workload management can be complex, but is vital to ensure your resilience is not impacted and ensuring you are not forced to expand your SIEM licensing based on factors outside of your control.

Splunk Professional Services can assist with architecting for workload management.

Intermediate data lakes and data streaming

A trend we have encountered more and more recently, in scoping and designing SIEM migrations, is organizations implementing an intermediate layer between their data sources and their SIEM. These might include data lakes, data streaming services, or both.

Let's examine the most commonly quoted motivations and then discuss whether they stand up to scrutiny.

- **Resilience:** Increase resilience by adding a secondary data store. If for some reason data doesn't reach the SIEM and there is an incident or outage, this allows for another location storing this data.
- **Vendor lock-in:** Remove vendor lock-in through introducing an intermediate layer. This intermediate layer can be easily swapped out should migrating your SIEM become necessary.
- **Scalability:** Introducing an intermediate layer will better allow a solution to scale to multiple destinations.
- **Simplicity:** Managing an intermediate layer is easier to maintain in the long term, as your teams will only need one set of skills in case of changing SIEM vendors.
- **Cost savings:** Using an intermediate layer allows you to filter out the noise, and only input the data you truly need into your SIEM, saving on license costs.

We'll consider each of these arguments in turn.

- **Resilience:** Adding an additional layer adds more components that must be maintained and configured, resulting in higher TCO and potentially increased risk. If the intermediate layer fails, this decreases solution resilience, rather than improving it.
- **Vendor lock-in:** Adding an intermediate layer adds to the number of vendors you are working with, increasing the number of procurement touch points. It does not remove vendor lock-in. If the intermediate layer is purely free, open source software, you will have no enterprise level support in the event that you run into an issue, adding significant business risk.
- **Scalability:** Many modern SIEMs, including Splunk, can scale to several petabytes of ingest without the need for an intermediate layer.

- **Simplicity:** Adding an intermediate layer increases the number of technologies your team is accountable for. This will mean additional headcount or diluting your engineering teams skill profiles.
- **Cost savings:** Although intermediate layers can filter data, the additional burden of managing them can be significant. Additionally, because many intermediate layers break standard SIEM data ingestion paradigms, the added cost of rebuilding these rather than being able to rely on out-of-the-box content can be substantial. Splunk provides its own technologies to route and filter data, and provides mechanisms for data tiering that allow you to optimize the cost of your data in line with its usage. Finally, when adding an intermediate data store, you are effectively storing some or all of your data twice; this is unlikely to be cheaper than sending it to appropriately tiered data stores.

When designing for an effective migration to Splunk, try to consider the following for any proposed intermediate layer:

- Does the intermediate layer reduce or increase resilience? Does it do so at the expense of TCO?
- Will it break your replacement SIEM's out-of-the-box data ingestion, forcing you to rebuild parsers and detections at your own expense?
- Does the intermediate layer add scalability beyond what is possible with your replacement SIEM software?
- Does the intermediate layer actually simplify your software landscape, or does it introduce more skills requirements and administration touchpoints for your engineers?
- After you account for additional skills, configuration time, the cost of storing your data twice, the additional network impact, the additional hardware, software and support costs, etc., is the TCO of your design actually lower?

Although the desire for an intermediate layer is based on valid business logic, the above considerations highlight how this can add cost and reduce functionality, unless considered in the wider business context. Splunk Professional Services can help you plan for a SIEM migration that achieves your business objectives, and recommend intermediate solutions that meet your requirements where needed. In addition, Splunk provides a stream processor, Splunk Edge Processor, described in our next section.

Splunk Edge Processor

Splunk Edge Processor is a data processing solution that works at the edge of your network. Use the Edge Processor solution to filter, mask and transform your data close to its source before routing the processed data to external environments. This solution allows you to send data to the appropriate data tiers, helping optimize your deployment costs.

Summary

In this section we considered the impact of classifying data and storing it appropriately, and the potential mechanisms for doing so. For a much deeper guide on everything data and data tiering, see Splunk's Essential Guide to Data and Splunk's Data Tiering Playbook.

Multi-Tenancy

RBAC for data layer multitenancy

RBAC is the mechanism through which Splunk manages data level access rights.

We can utilize RBAC to provide appropriate data level access rights to a variety of teams in your organization, for example business users and security analysts who need access to different datasets.

RBAC can be used to support MSP scenarios, where both your organization and your MSP need different levels of access. RBAC can also be used to support multitenancy should you need to set up a platform such that multiple business units, or organizations can share a single environment without seeing each other's data.

If you are an MSP, RBAC enables you to run a security operations service for multiple customers from a single shared Splunk platform, giving role-based access to their data only.

Security service level cataloging

Overview

Service cataloging describes an approach to security based on service catalogs. In this context, a service catalog describes multiple levels of service, from which your customers — be they business units, if you run information security for an organization, or the organizations themselves if you are a managed service provider — may select. For example, you may decide to offer a catalog of service levels of different tiers like Bronze, Silver and Gold based on budgetary agreements or fees.

These service levels may have different KPIs, SLAs, accepted data volumes and more. For example, the Bronze level of service may provide for up to 30 triaged alerts per day, on up to 100GB of data, whereas the Silver level of service may provide for up to 100 triaged alerts on 500GB of data, with a guaranteed response SLA of five hours.

Service catalogs can be a useful way to ensure your business responds to the highest priority customers. Splunk can support service catalogs through a combination of data tiering, RBAC, workload management and appropriate tagging of alerts in Enterprise Security.

Splunk Professional Services can help you design a service catalog that addresses your business needs, both at the business level and by creating the right technical architecture to support it.

Hybrid SIEM and SIEM-of-SIEM architectures

A more recent trend in SIEM design is the use of multiple SIEM solutions in parallel. Although there can be varying motivations for this, most commonly it is because a vendor includes the pricing for their SIEM, often a public, cloud-based solution, as part of an enterprise license agreement (ELA). This licensing model makes it financially appealing to utilize a SIEM for some amount of security monitoring. A secondary motivation might be if a SIEM is specialized for a specific data source type, and is selected for that data source only.

Splunk can work with many other SIEM solutions in an effective "SIEM-of-SIEM" architecture. This means that should you decide to implement another SIEM for a specific use case, or because your procurement team has enforced its usage, Splunk can continue to exist as a parent-layer SIEM, taking alerts and output from low-level sub-SIEMs.

SIEM-of-SIEM architectures have the downside of being more complex than using a single vendor, but given the realities of today's complex environments, it is incumbent on vendors to facilitate customers' business requirements for integrated SIEM configurations.

Although each configuration is necessarily custom, and cannot currently be based on a pre-packaged solution, Splunk has a set of paradigms that can help enable these architectures:

- **RBA:** Can be used to help aggregate point alerts from disparate sub-SIEMs with Splunk as the SIEM-of-SIEMs
- **SOAR:** Can be used to support automation between various SIEM components, acting both to speed and automate response to security incidents and also as middleware between SIEM components, helping ensure all event states stay in sync when transposed between tools

- **Open platform:** Splunk makes it easy both to bring in and forward along data and alerts with open APIs. This makes Splunk's open platform the ideal point for centralization in a multi-SIEM architecture.

Although hybrid SIEM architectures are becoming more common, and can be accommodated and accelerated, it is worth thinking through the business logic of utilizing more than one SIEM, and considering whether this is truly driving down TCO and business risk. Organizations should think critically about whether the cost of maintaining knowledge and integration between these multiple platforms outweighs the benefits.

Multi-region federated search and alert forwarding scenarios

Overview

In case your Splunk deployment needs to span multiple regions, there are several technologies Splunk provides to help support keeping your analyses connected while meeting both regulatory requirements and business objectives.

Multi-regional orchestration

Organizations can face a variety of challenges that require they set up multiple separate Splunk instances. Although one reason may be legal requirements to keep data on location, sometimes the reason is even more challenging. Some organizations have a requirement to ingest data from ships or aircraft, which will by nature have very limited options for sending on telemetry. This may mean architectures that need to support intermittent alert forwarding, such as when a ship docks or a satellite passes overhead, and reliably make this information available to onshore analyst teams.

The good news is that Splunk SOAR can help support orchestration of alerts across multiple instances where needed, where these are required. The Splunk Content Manager app can help you support keeping content in sync across multiple regions. Splunk has already successfully helped several customers with architectures that achieve these objectives and more. We are happy to speak to you to see how we can help.

Data sovereignty

Data sovereignty refers to requirements — legal or otherwise — to keep data in a specific region. For example, a data sovereignty requirement might mean that all data associated with a given country must remain in that country. If your SOC team is based in the US, this might give you pause. This is where alert forwarding and federated search come in. While data itself may be barred from moving between regions, detections can typically still run locally, and alerts — which are not data but metadata — may be sent, providing they meet certain requirements.

Federated search

Splunk can support federated search topologies, in which multiple deployments of Splunk are searched from a central deployment. This allows for more complex architectures supporting business requirements, such as data sovereignty across multiple regions.

Alert forwarding

Alert forwarding refers to usage of Splunk Enterprise Security and Splunk SOAR to move alerts between Splunk environments, typically to move them into a centralized instance for further analysis.

Insider threat and audit

Occasionally, when we speak with organizations, they raise concerns about the idea of who is “watching the watchers.” That is, what if an analyst was themselves an insider threat? Wouldn't having access to all of an organization’s data mean they could cover their tracks?

Although some might argue that if you hire someone into an analyst role, you are accepting a degree of faith in that individual and accepting some business risk, this type of enhanced insider threat audit is possible in Splunk. Organizations can either utilize RBAC to ensure that analysts do not have access to Splunk platform level logs, or by forwarding data onto a separate Splunk instance.

SIEM and vulnerability management

Another question we occasionally receive from organizations is: Can we use Splunk for vulnerability management?

The answer is yes, absolutely, but wait — don’t throw out your vulnerability scanner just yet!

Splunk is excellent at storing vulnerability data to both provide context for alerts and engaging visualizations that help tell the story of that data. Both are a critical part of the vulnerability management lifecycle. That being said, Splunk itself is not a vulnerability scanner. You will still need to use a dedicated tool for this purpose, that will provide data as an input to Splunk and use configuration management software to perform updates and remediation.

Use case management

Implementing a new SIEM represents an opportunity to up-level management of your use cases. In this section, we’ll example some of key use case management practices and strategies, and how these can be implemented in Splunk.

Use case inventories

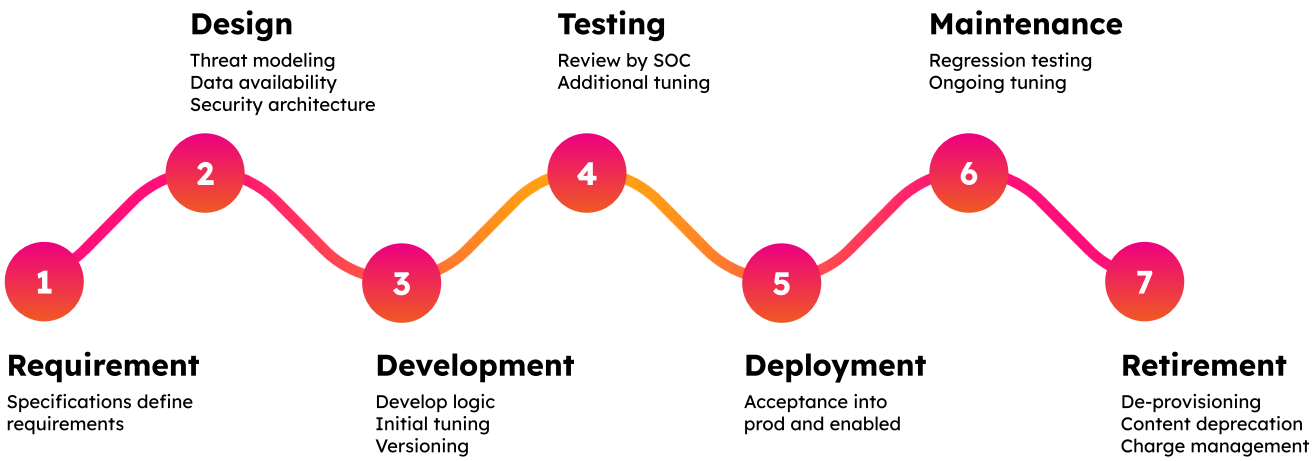
A use case inventory is a system for tracking and organizing your use cases. This can help you track coverage across multiple tools and ensure you have a single point of reference to articulate coverage to your stakeholders. An inventory could take the form of a shared spreadsheet, or leverage a dedicated use case management technology. In Splunk, you can utilize Splunk Security Essentials to map and manage use cases. As Splunk Security Essentials is a freely available Splunkbase app, there is nothing stopping you from using it to begin tracking and mapping use cases prior to a Splunk Enterprise Security implementation.

Use case lifecycle

When implementing a new SIEM, you have an opportunity to evaluate how your organization tracks and deploys use cases. Many organizations fall into the trap of continually adding technical use cases but not validating previously implemented use cases to ensure they are still functional and continue to provide value. This can cause use case bloat, which impacts system performance, resulting in low quality alerts, false positives, or worse still, false negatives as analysts assume coverage exists.

A use case lifecycle is a system for tracking a use case through various stages of its existence and ensures that a use case is providing continuous value or else is decommissioned. It can mitigate against the risk of use case degradation through ongoing testing, maintenance and decommissioning of use cases that are no longer relevant.

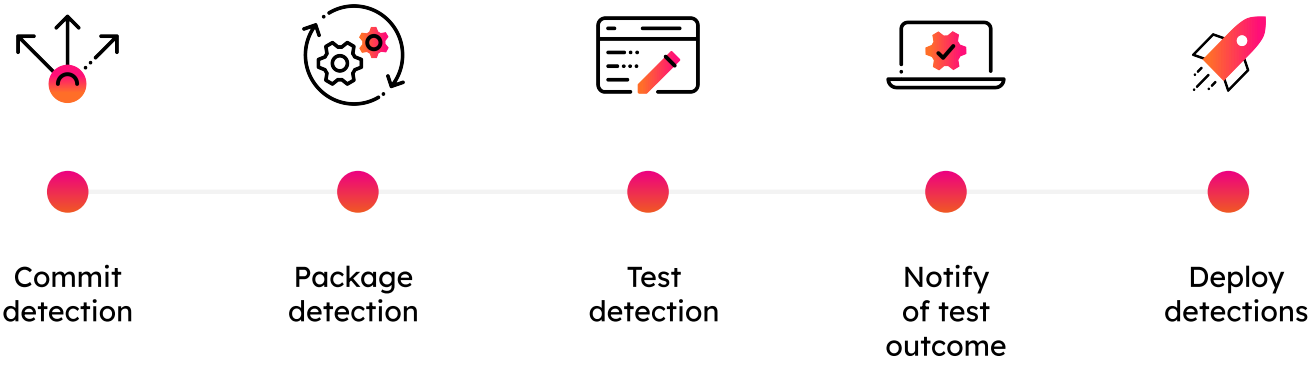
Splunk Professional Services can help design and document a use case lifecycle to meet your business requirements. These can be implemented through Splunk Security Essentials and CI/CD methodologies.



An example of a Splunk use case lifecycle

Detection as Code and CI/CD

Detection as Code refers to the practice of storing correlation searches not just as artifacts in a SIEM, but as code that can be version controlled and managed, just as you would software in a standard software development lifecycle. This practice makes detection management robust, scalable and supports the rollout of quality assured, tested detections.



Splunk supports detection as code methodologies out of the box. Splunk also provides a custom tool, content ctl, which makes the process of managing detection as code through CI/CD practices significantly easier, and supports atomic testing of detections through its Attack Range tool.

Path to Live

Path to Live refers to the practice of testing content in multiple staging environments before pushing to a primary production environment. This typically forms part of a use case lifecycle. Splunk facilitates this through Splunk Security Essentials and the CI/CD technologies outlined above, which can allow you to easily test content before pushing to production — even if that test environment is on premises and your production environment is based on Splunk Cloud.

SIEM migration patterns

On-premise SIEM to cloud SIEM versus SaaS SIEM to SaaS SIEM

There are some differences between migrating from an on-premise environment to SaaS versus going directly from a SaaS service to another SaaS service. Let's consider the impact these options might have on your SIEM replacement, from both business and technical perspectives.

On-premise to SaaS

When moving from an on-premise SIEM to a SaaS SIEM, you need to take into account the fact that you will be doing two transformations at once: a SIEM replacement and a cloud migration.

This adds a few considerations into the mix for your replacement project:

- You will need to carefully consider your order of operations. Moving to a cloud SIEM will mean decommissioning your on-premises hardware, setting up data forwarding out of your on-prem environment, and perhaps hardest of all for your teams: adapting a cloud-first mindset. This change may take time and the costs of reconfiguration, decommissioning and cloud enablement should be factored into your budget.
- You will need to consider data ingress and egress costs if you are migrating data from your on-premise SIEM to an IaaS platform. Be aware that you may incur additional data ingress or egress costs.
- You will check your limits. Even if you are moving from an on-premises SIEM to a cloud SIEM from the same vendor, remember that if you are moving to a SaaS platform, it's just that — a service. Just because you did something in your own environment, over which you had total control, doesn't mean it will be within the limits of your shiny new cloud environment. Limits exist to keep you safe and ensure your service is provided in line with what you paid for, but ensure you understand these limits before you make the move.

SaaS to SaaS

Moving from SaaS to SaaS simplifies things somewhat. You've got the business transformation of migrating to cloud out of the way, but there are still a few things to bear in mind:

- **Check rules on data.** Your existing cloud SIEM provider may not allow you to migrate data out of the platform, or may hit you with additional changes. You will need to read your SaaS service agreement to understand what is and isn't allowed.

8. Introducing Splunk Professional Services

Introduction

Splunk Professional Services consists of delivered expertise that helps you realize value sooner, optimize and enhance your Splunk instance and identify opportunities to unlock new capabilities from your investment.

The Splunk Professional Services value proposition

Splunk Professional Services delivers projects around the globe to organizations just like yours.

Splunk Professional Services at a glance

One team working together to achieve success for our customers!

1800+	5k+	1000+	91	110
Splunk Experts	**Accreditations**	**Projects Delivered Annually**	**Of Fortune 100**	**Countries**
Scale resourcing up and down on demand	Early access to new Splunk products	Direct access to Splunk Engineering and Support	Vast Certified partner delivery network	Proven Record Delivering Success

Splunk Professional Services creates offerings tailored to your organization, based on best-in-class packages with a track record of success. This flexible approach guarantees that we can quickly scope and quote, but can adapt to deliver in the way that's best for your organization.

	Splunk Enterprise Deployment	Data Sources	Splunk ES Deployment	Use Cases
Base	✓	7	✓	5-10
Standard	✓	9	✓	10-20
Premium	✓	9+	✓	20+

Splunk Enterprise Security Implementation Packages

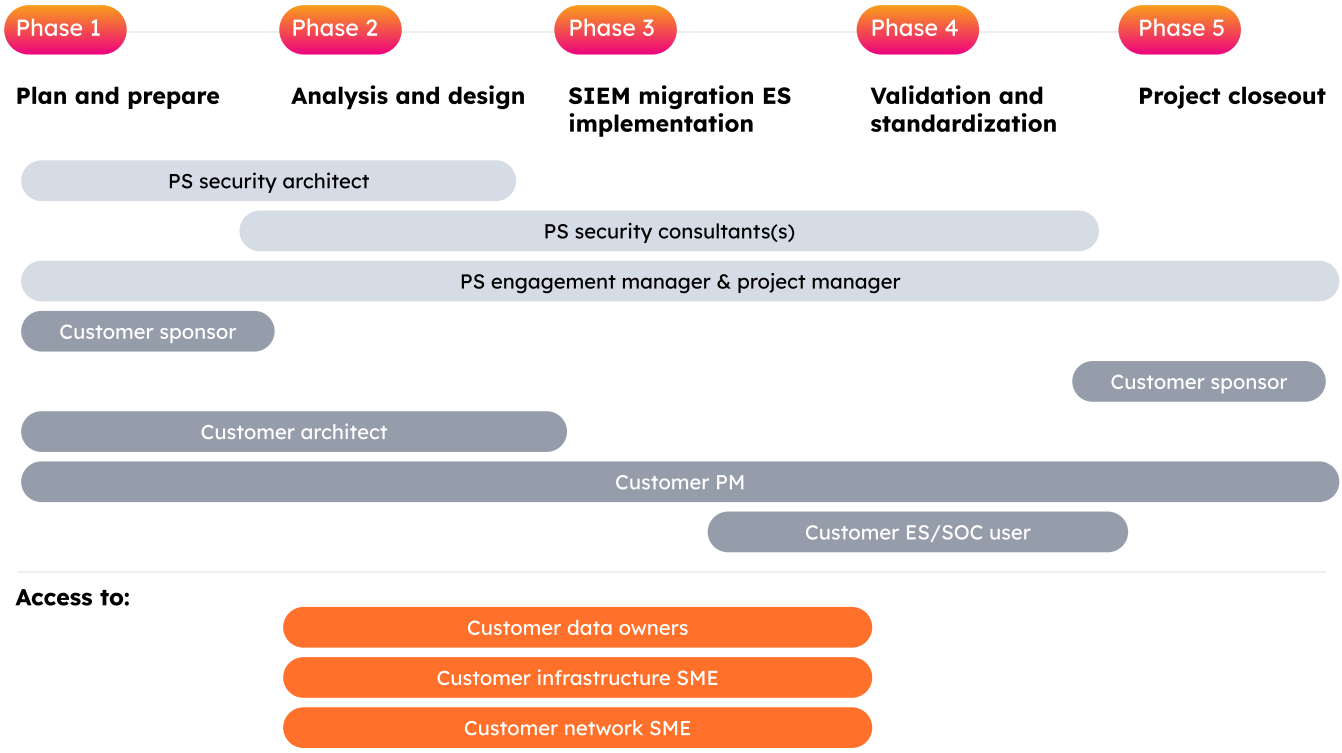
To get started with designing and implementing a world-class SIEM you can reach out to your Splunk team today, or use the Splunk website to contact Splunk Customer Success directly.

9. The Splunk SIEM replacement approach

Introduction to the Splunk Professional Services methodology

Our Splunk Professional Services team is highly efficient and can drive rapid TTV and overall value from Splunk-led SIEM replacement engagements. Our expert Professional Services team has delivered consistent success across hundreds of customer SIEM replacements and continues to evolve and optimize to handle any and all SIEM replacement engagements. Splunk Professional Services addresses SIEM replacement with a consistent methodology. This approach, which has demonstrated success on a global level, consists of the following high-level phases:

Let's take each of these in turn to understand their role in delivering a successful SIEM replacement.



A conceptual overview of Splunk Professional Services implementation phases

Plan and prepare

This engagement phase describes initial engagement planning activities. Depending on the scale of the engagement, the duration of this phase may vary.

This phase will typically cover the below activities:

- Define project methodology and ongoing cadence
- Agree on deliverable outline
- Create and agree on delivery plan
- Ramp up project and resourcing
- Kick-off calls

Analysis and design

This engagement phase describes the analysis of any existing solution and the design of the planned SIEM Solution. Splunk architects and project managers will work to gather and document requirements, then produce a Splunk best practice design to drive rapid TTV as well as long-term value realization. This phase is critical to a SIEM replacement project as it sets the foundation for success both for the Splunk

Professional Services team performing any downstream implementation activities, but also for the customer's long term value realization potential.

SIEM Replacement Workshop

A SIEM Replacement Workshop consists of both a Use Case Development Workshop and a SIEM Design Workshop. These can be broken up and completed separately, but as both are needed for a successful SIEM replacement, it is easiest to group them.

A Splunk Use Case Development Workshop is designed to:

- Perform discovery to analyze the current state and plan the future state of your SIEM environment
- Advise on best practices and approaches to realizing value against your business use cases with your new SIEM
- Create a phase-based use case roadmap and design, which supports both the immediate Splunk Professional Services led implementation and future long term customer-owned implementation

This workshop is a Splunk Professional Services architect-level activity, and is very strongly recommended as a part of any Splunk Professional Services led SIEM replacement.

Use case mapping

A Splunk Use Case Development Workshop achieves rapid TTV by enabling you to first understand the business use cases you are trying to address with your detection and monitoring strategy, then mapping a combination of Splunk out-of-the-box content and net-new custom content to achieve them. This mapping process can include any product in the Splunk security portfolio, including freely available apps such as Splunk Security Essentials or Splunk SOAR, depending on scope.
Splunk Professional Services brings extensive knowledge and experience of Splunk out-of-the-box use cases and their purpose, as well as recommendations on achieving rapid TTV against business requirements using this content. Where out-of-the-box content is not available, Splunk Professional Services can design a pattern to develop custom use cases that enable the customer, either by themselves or alongside Splunk Professional Services, to drive the development of custom content.

Like-for-like versus business-driven use case replacement

Like-for-like

When considering your approach to replacing an incumbent SIEM, many organizations naturally gravitate towards a strategy based around replacing their traditional SIEM in a like-for-like fashion. In this scenario, the logic goes, the replacement SIEM must first demonstrate that it can meet identical *technical* use cases and data ingest requirements to the previous SIEM before moving on to net-new content. This approach is often a mistake. Simply mapping the technical content from your existing SIEM on to Splunk Enterprise Security may be quick and easy; however, achieving fast and easy results does not necessarily mean a commensurate achievement of value.

Consider the following:

- You have replaced your traditional SIEM for a valid reason, such as unacceptable TCO or product functionality.
- You want to manage your TCC and keep this within acceptable limits. This means you cannot spend time on any activity that does not directly contribute to the generation of business value.
- Your new SIEM works differently than your old SIEM, including different, presumably superior methods for creating correlation search content or other technical use cases, and for managing and storing the appropriate data.

If these statements are true, then why would you want to replicate the content from a traditional SIEM solution when you know that this traditional SIEM has not provided the required business value? At the start of this segment we said that we are considering the like-for-like replacement of *technical* use cases. We stand by this statement, but that does not mean we should toss the wine out with the cork. Instead, we should look at the business-level use cases, sometimes also known as high-level use cases, which may well be as valid now as they were before.

	Use case levels	Examples
	Business requirements	Prevent unacceptable business risk, with ransomware as the largest source of business risk
High level business	Business level use cases	Detect and alert on ransomware
Low level technical	Technical use cases	**Correlation rule 1:** A Splunk ES Correlation Search detecting lateral movement through network logs
		Correlation rule 2: A Splunk ES correlation search detecting a specific log based IoC associated with ransomware from aggregated EDR logs
		Dashboard 1: A Dashboard showing ransomware incidents for all detections, etc.

The same can be said of data. The data you require to achieve use cases in your traditional SIEM is not necessarily the same data needed for your replacement SIEM use cases.

Business-driven

We've discussed why, when moving from a legacy SIEM to Splunk, you should consider disregarding your previous *technical* use cases; however, your business-level use cases may well be valid, and this is where Splunk Professional Services starts with our discovery process. Once we can understand the objectives you and your business are trying to achieve by implementing a SIEM solution, we can then map these high-level business use cases to low-level technical use cases in Splunk. This means we can utilize our out-of-the-box content and Splunk best practices to rapidly produce value against your business's objectives, rather than compromising your TCC by spending unnecessary cycles trying to replicate the content from your previous SIEM.

Ingest-driven SIEM versus use-case-driven SIEM

When implementing a SIEM, whether for the first time or as a replacement for an incumbent, you will need to evaluate your data strategy. Your data strategy is the long-term approach you choose to determine what data you will put into your SIEM, and how you will classify that data.

Ingest-driven

The default stance of many organizations is an ingest-driven data strategy. An ingest-driven strategy is one where the focus is first on bringing data into the platform. This is then followed by discovery and engineering of value driving applications of the data. This is the case for several common reasons:

1. **It's easy:** It's easy to start with big, obvious data sources and put them into your SIEM, then determine how to use the information. However, though this approach may make sense initially, it soon runs out of steam, since data alone cannot provide value. In the worst scenarios, the SOC is measured not on the value it provides, but instead on the quantity of new data it brings into the SIEM solution, increasing perceived "coverage" of the organization's technology estate.
2. **The SIEM is a service:** The SIEM is provided as a service to a series of business units. Because of the way this approach is sometimes structured, there is a separation between these business units and the SIEM service, and that results in the business units simply submitting their data to the SIEM, and then a separate security team realizing value from it. This process, although somewhat dysfunctional, is quite common.
3. **Compliance:** This is the most valid reason for an ingest-driven data strategy. Certain subsets of data may be labeled as required for compliance reasons, such as for regulations or audit requirements. In this situation, regardless of the usability of the data, it must be entered into the SIEM in order for the organization to avoid penalties.

Although these reasons can all be valid, situationally, following any of these ingest-driven data strategies creates a disconnect between the data itself and the security use cases that the SOC needs to support. Additionally, simply ingesting data without a valid understanding of how that data will be used in the SIEM to create value can generate costs without generating any actual security outcomes.

Splunk Professional Services can support a ingest-driven data strategy, and in some situations this may be advantageous, or even required — such as in a compliance scenario. Generally, however, the preferred approach is to instead operate on a use-case-driven data strategy.

Use-case-driven

In a use-case-driven data strategy, we instead orient our data ingestion priorities around their relationship with our prioritized use cases. In this scenario, we consider business requirements and map these requirements to business use cases. These high-level business use cases in turn drive low-level technical use cases, prioritized based on their value to the business and a list of known available data sources. Some of these available data sources may exist already in your incumbent SIEM, but some may not yet be ingested at all. This means we can prioritize our data source onboarding efforts in line with the outcomes that data is expected to drive for our business. It also ensures we have traceability of risk mitigation, from business requirements all the way to technical use cases, and can justify the data we are ingesting every step of the way.

Phase-based approach: Use cases and data

Use cases

The fastest value add that Splunk Professional Services can provide is helping the customer prioritize use case implementation in a standardized, phase-based approach, based on our expert knowledge.

As an example, for a customer whose top priority and business risk is detecting ransomware, we might have the following high-level phases:

- **Phase 1** – Critical use cases: We need to enable use cases associated with ransomware indicators of compromise, and bring in endpoint detection and response (EDR) data sources to enable identification of critical use cases in line with MITRE ATT&CK prioritizations.
- **Phase 2** – High priority use cases: We need to enable other, more complex use cases and bring in other data sources.

- **Phase 3** – Custom use cases: We need to create custom use cases to meet business requirements and onboard the associated data sources, including configuring machine-learning-based anomaly detection use cases specific to customer requirements.

These phases are always aligned to each customer's specific requirements, and Splunk Professional Services will produce a use case implementation roadmap that covers all identified phases. Splunk Professional Services typically only works with customers to implement phase one, as the goal is to deliver rapid TTV and build the skills needed within the customers' own teams to drive future progress. Please note, Splunk Professional Services does have the capability to deliver SIEM replacement projects end-to-end, inclusive of all phases, should this be a customer requirement.

Data

Splunk Professional Services can produce a phase-based roadmap of prioritized use cases, mapped to their associated prioritized data sources. This prioritization can be used to ensure that the data sources are brought on in sync with associated data sources. This may mean starting with a "big bang" approach, moving data sources from the incumbent SIEM, where you work with Splunk Professional Services to bring over all your data sources in an upfront migration phase, or it might mean a longer-term dual-forwarding based cutover scenario. Either way, Splunk Professional Services can ensure that you have a comprehensive strategy to bring in the right data at the right time to deliver rapid TTV and avoid wasted costs.

Scheduling

A typical schedule for a standard five-day Use Case Development Workshop might include an upfront day to perform discovery and include key senior customer stakeholders, such as the project sponsor. After a brief opening session with any customer participants, the remainder of the day will involve only the customer project team.

From a scheduling perspective, this might resemble the below:

Day 1

- First half: Discovery
- Second half: Advisory

Day 2

- First half: Advisory
- Second half: Documentation

Day 3

- First half: Advisory/Map and design content
- Second half: Documentation

Day 4

- First half: Advisory/Map and design content
- Second half: Documentation

Day 5

- Any remaining activities; present to customer project team for final draft input
- Documentation

The typical output from a Use Case Development Workshop is a customized, phased-based use case implementation roadmap document, mapped to your data sources.

RBA workshop

An RBA workshop is intended to support your SIEM implementation by designing for RBA. This can be conducted at the outset, or after you've proven success with your initial SIEM implementation. Splunk Professional Services can use the output of an RBA workshop to drive an RBA implementation, or you can utilize the output yourself to drive your own implementation, either with your teams or using a Splunk partner.

Typical outputs from an RBA workshop include an RBA implementation plan and roadmap.

SIEM design workshop

A subset of the SIEM replacement workshop, this workshop describes the design of all elements of the replacement SIEM solution.

Workshop topics may include:

- Asset and identity configuration
- Threat intelligence configuration
- Analyst case management workflow
- Dual forwarding
- Multitenancy
- Data classification
- Federated search
- Hybrid SIEM architectures
- Insider threat requirements

Planning your Splunk SIEM platform can mean thinking about a variety of architectural factors, and these factors can have a significant impact; so much so that we dedicated a section of this document to considering them.

Typical outputs from a SIEM design workshop include a SIEM design document.

Platform design workshop

This workshop designs the underlying Splunk platform that the Splunk SIEM will run on. This is a standard Splunk architecture workshop. It takes the appropriate Splunk Validated Architecture to meet customer scale and availability requirements, then builds it out into a customer-specific design. This process is just as important in a Splunk Cloud configuration, where considerations such as intermediate data-forwarding layers, cloud-to-cloud integrations and Admin Config Service based CI/CD models will need to be discussed, among others.

If the customer's platform is extremely simple — for example, a single, all-in-one node, or Splunk Cloud with cloud-to-cloud data sources only — these topics may be included as a part of the SIEM design workshop.

Typical topics covered may include:

- Selecting a customer-appropriate Splunk Validated Architecture based on requirements identified in this workshop, and any other upstream workshops
- Sizing
- Integration planning
- Intermediate forwarding layer planning, if applicable
- RBAC design
- Index and retention planning
- Edge processor design, if applicable

- Deployment server design

For Splunk Professional Services engagements of a sufficient scale, the final two items — RBAC design and index and retention planning — may be broken out into their own specific workshops.

Typical outputs from a platform design workshop include a Splunk platform design document.

SOAR platform design workshop

This workshop designs the underlying Splunk platform that the Splunk SIEM will run on. This is a standard Splunk architecture workshop, and takes the appropriate Splunk SOAR Validated Architecture that meets the customer's scale and availability requirements, and builds it out into a customer-specific design. To effectively leverage a security automation and orchestration solution, it should integrate seamlessly to ingest, triage, coordinate and respond effectively and efficiently.

Typical topics covered in this engagement include:

- Selecting a customer-appropriate Splunk SOAR Validated Architecture based on requirements identified in this workshop, and any other upstream workshops
- Sizing
- HA planning
- Integration planning
- Intermediate layer planning, if applicable; for example using Automation Brokers
- RBAC design

The typical output from a SOAR platform design workshop includes a SOAR platform design document.

SOAR response plan design workshop

Splunk can help you along your SOAR maturity journey and offers flexible packages for implementation of Splunk SOAR. The first stage is a design workshop. The Splunk Professional Services team works with the customer to choose the right implementation topology, then designs the appropriate response plans to address customer use cases. Response plans are logical constructs which address a use case, and are made up of modular, atomic playbooks.

The typical output from a SOAR response plan design workshop is a Splunk response plan design.

Build (Implementation)

SIEM implementation

Splunk's SIEM implementation approach provides end-to-end implementation.

This may include activities such as:

- Data onboarding and CIM compliance configuration
- Configuring the Splunk Enterprise Security App
- Configuring the Splunk Threat Intelligence Framework
- Configuring the Splunk Asset and Identity Framework
- Configuring Splunk use cases
- Providing knowledge transfer to your teams
- Configuring integrations

The typical output is a fully-configured Splunk SIEM implementation.

SOAR implementation

After the appropriate architecture model has been selected, Splunk Professional Services will provide the resources to install and configure Splunk SOAR and start the process of integrating the preliminary list of integrations for SOAR to ingest events, look up information and perform actions. This includes integrating SOAR with Splunk Enterprise Security.

The Splunk Platform team has identified three categories of playbooks:

- **Enrichment:** Perform the prep work before presenting to the analysts
- **Utility:** Supports the daily tasks the security teams perform
- **Autonomous:** completely automated response with human decision-making, if required

The SOAR team will work with you to leverage our library of playbook examples to deliver the security automation and orchestration capabilities to help security teams.

The typical output from a SOAR implementation is a configured Splunk SOAR deployment and one or more configured Splunk SOAR response plans.

Validate

Overview

This stage confirms the implementation has been completed in line with Splunk best practices.

The typical output from the validation stage is verification that the platform is implemented in line with Splunk best practices.

Project handoff

This stage covers the handoff from Splunk Professional Services to your teams. It involves sharing any final documentation and project wrap-up.

Typical outputs from this stage include a handover of any outstanding documentation, and a handoff for the customer to partner with Splunk's Customer Success team.

Splunk Professional Services flexible approach

We work with you

Splunk Professional Services follows a "work with you" approach. This means that we do not expect to operate your environment in a black box, or present your teams with a solution they don't understand. Every stage of our implementation is geared toward ensuring your teams get the knowledge and hands-on experience they need to be successful with Splunk. Where possible, we will work with your teams on implementation activities, and continuously collaborate with them to ensure that the final product meets their expectations and requirements, even as these evolve.

Flexible scoping

Splunk operates on a flexible scoping model. This means that packages are used to give structure to engagement scoping and ensure smaller organizations have cost-effective, predictable and off-the-shelf options. When we need to customize our approach to meet our customers where they are, we do; we can also scale our approach to the world's largest enterprise-grade customers and projects.

Prescriptive versus reactive support

Splunk Professional Services can take both a prescriptive and reactive support stance, depending on what best suits the needs of the customer. When we are prescriptive, we can help guide your teams toward the security models and frameworks that organizations of similar size and verticals rely on, that give a step up on their maturity journey. When our customers know what they want, we can switch to a more reactive support approach, taking customer requirements and flexing our approach in-line with what they need.

Timelines and parallel delivery

Splunk can provide parallel delivery with multiple consultants. This allows us to shorten timelines for implementation, should you discover you have a timeline you need to hit, such as the license on your previous SIEM running out.

We are able to achieve this by using Splunk project managers to oversee multiple work streams, ensuring parallel work is completed efficiently and without crossover.

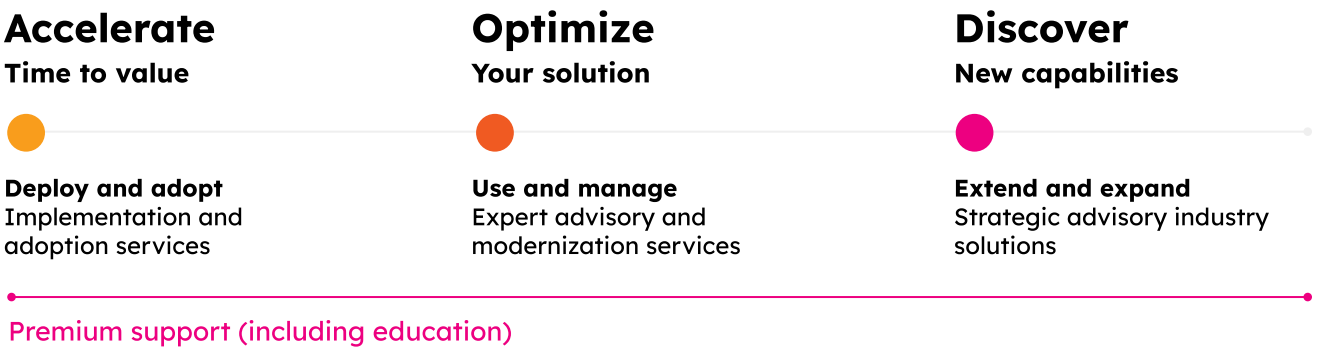
Please note, however, that consultants can't scale infinitely, so it is still important to plan your replacement well in advance to give yourself enough time to transition without substantial business risk.

Post-implementation value realization

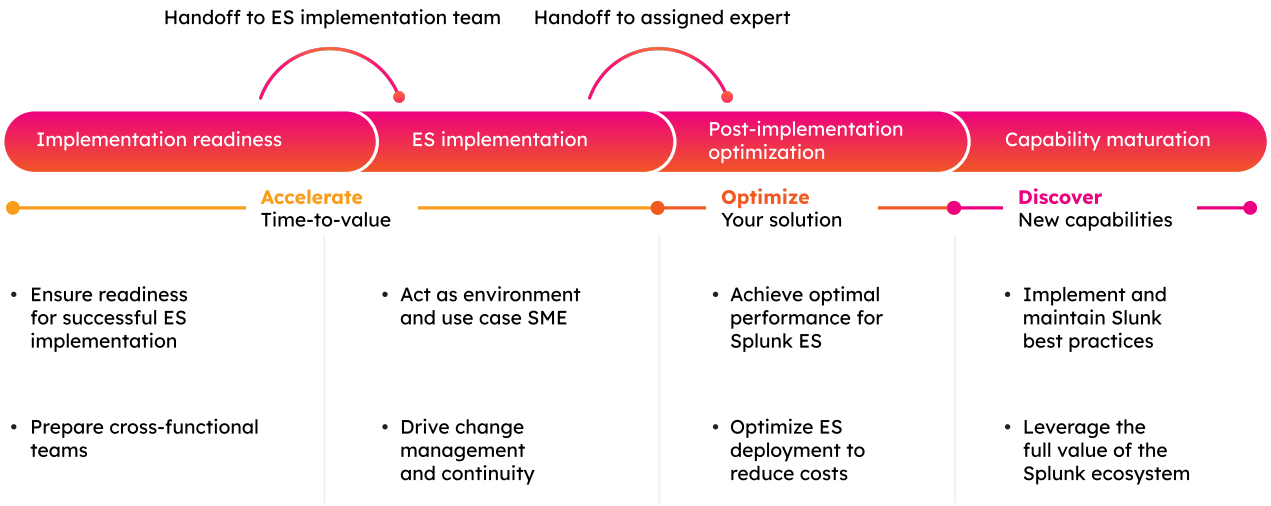
Splunk doesn't just provide implementation services. Both Splunk Professional Services and subscription model services can be utilized for value realization consultancy.

Partnering on your data journey

Maximize your Splunk investment at any point along your journey



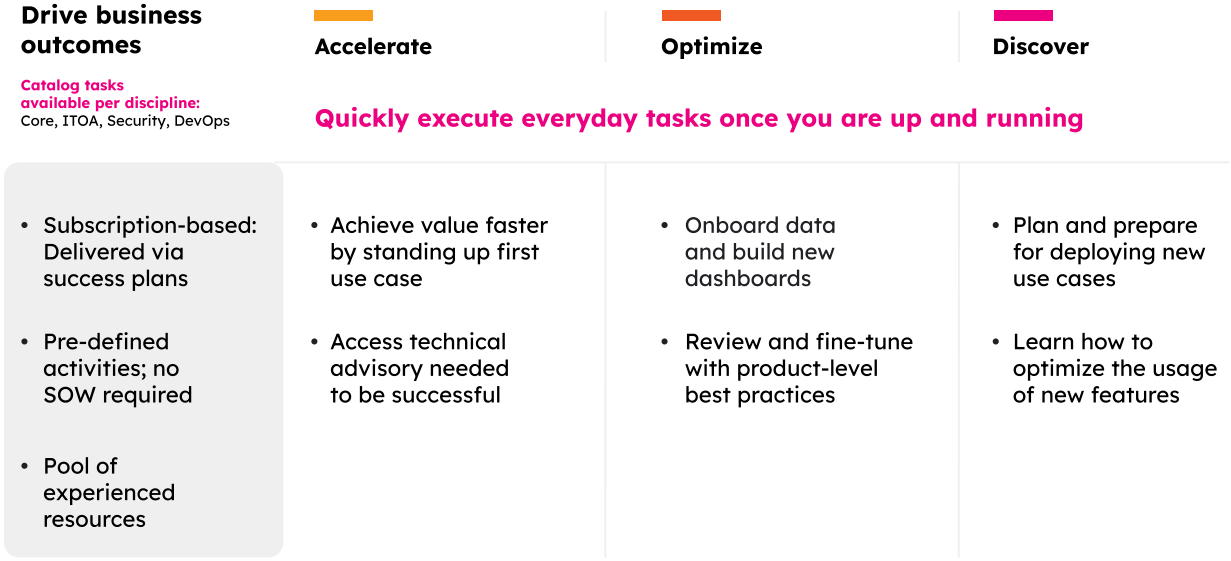
Splunk's premier subscription services offering is the Assigned Expert. This is a dedicated time period with a named expert Splunk resource who will help you unlock maximum value and return from your Splunk investment.



Splunk also provides OnDemand services, which operate on a credit-based subscription service. They can be used to rapidly achieve atomic tasks, without the need for a statement of work.

Deep Dive: On-demand service (ODS)

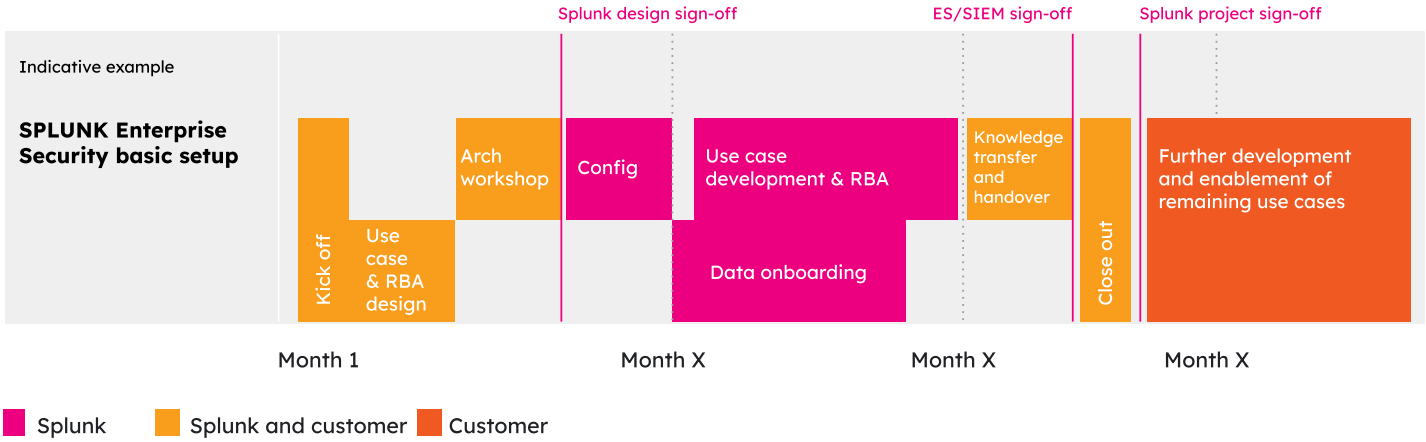
Execute common tactical activities, related to using and managing Splunk products



Putting it all together

As we've discussed, the Splunk SIEM replacement approach is flexible to each organization's needs. Although no two organizations are the same, we can visualize how the Splunk Professional Services phases, tasks and resources may align in a typical engagement to drive rapid value realization based on Splunk Professional Services' customer success focus and "work with you" approach.

Plan and prepare	Analysis and design	Build	Validate	Close out
• Project methodology and ongoing cadence	• SIEM migration workshop	• Implementation of agreed SIEM solution	• Execute agreed validation plan	• Complete project closeout checklist
• Agree deliverable outline	• Solution design	• Monitor progress against plan	• Remediate agreed issues	• Project sign off
• Create and agree delivery plan	• RBA design	• Onboard data sources		
• Project ramp up and resourcing	• Design documentation	• Implement correlation searches		
	• Detailed project plan	• Implement RBA		



Splunk PS and Customer Tasks by Phase

Appendix

Terms and Acronyms

Term	Description
SOC	Security Operations Center
TCO	Total Cost of Ownership
TCC	Cost of Change
TTV	Time to Value
Use Case	An application of a technology to solve a business problem. In Splunk PS we break this into high-level business use cases, and low-level technical use cases
FTE	Full-time employee
Fully loaded cost	The full cost of an FTE, including all associated costs and functions like HR, management, expenses, healthcare, etc.
Alert fidelity	In the context of a Splunk correlation search, alert fidelity refers to the likelihood that the search accurately identifies an accurate and specific security event
Low fidelity	Indicates that the search might generate non-specific alerts or false positives more frequently, requiring further investigation to confirm the actual threat
High fidelity	Indicates that the search is highly specific and that alerts generated are likely to highlight a true positive with little further investigation
False positive	An alert which inaccurately flags a security threat
False negative	An alert which inaccurately fails to flag a genuine security threat
Splunk Professional Services	Splunk Professional Services offers expert guidance to businesses, helping them implement and optimize Splunk solutions for security, IT operations and business intelligence, maximizing their return on investment
RBA	Risk-based alerting: A meta-alerting framework build on Splunk Enterprise Security
OOTB	Out-of-the-box: Usually in the context of functionality that comes built into a product
MTTR	Mean time to response: The average time taken to respond to incident
MTTA	Mean time to acknowledge: The average time taken to acknowledge or triage an incident
EDR	Endpoint detection and response: A software program that continuously monitors endpoints (devices like computers and servers) for suspicious activity, aiming to detect and respond to cyber threats like malware and ransomware in real time
SSE	Splunk Security Essentials: A free Splunkbase application which allows Splunk users to implement security use cases faster by using pre-built content that can be activated with a few clicks. Streamline implementation with built-in guidance and automation

Data lake	A data lake serves as a central repository for storing and managing all types of raw data, regardless of format or structure, allowing for flexible analysis and discovery of insights across diverse datasets
S3	Amazon S3, or Amazon Simple Storage Service: A highly scalable and cost-effective object storage solution offering industry-leading durability, availability and security for storing large volumes of data
Federated search	Splunk federated search enables seamless querying across multiple Splunk indexes and instances, regardless of their physical location, providing a unified view of data for comprehensive security and operational insights
SVA	Splunk Validated Architectures: Splunk Validated Architectures (SVAs) are proven reference architectures for stable, efficient and repeatable Splunk deployments
ACS	Admin Config Service: A cloud-native API that provides programmatic self-service administration capabilities for Splunk Cloud Platform. Splunk Cloud Platform administrators can use the ACS API to perform common administrative tasks without assistance from Splunk Support
Splunkbase	Identifying, ingesting and interpreting data correctly is a foundational step in the success of your Splunk security implementation that, if done correctly, will allow you to get the most value across your entire Splunk environment. To help you get this done correctly, you can use Splunk add-ons and apps, found in Splunkbase, to easily bring in new sources of information that expand your defense posture. Splunk's community of add-ons and apps are designed to make ingesting new data simple, efficient and accessible, as well as help you achieve your use cases faster.
Low and slow attack	A low and slow cyber attack aims to disrupt systems by sending minimal amounts of data over an extended period. These attacks mimic legitimate traffic, making them difficult to detect and potentially leading to resource exhaustion and service degradation
IaaS	Infrastructure as a service: Provides on-demand access to cloud-based infrastructure like virtual servers, storage and networking, allowing businesses to scale resources as needed without hardware management burdens. Most public cloud providers offer this service
SaaS	Software as a service: Offers ready-to-use, cloud-hosted applications accessible through a web browser. Businesses can subscribe to SaaS solutions, eliminating the need for software installation, maintenance and updates on their own infrastructure
Splunk Cloud	Splunk Cloud Platform delivers the benefits of award-winning Splunk Enterprise as a cloud-based service. Using Splunk Cloud Platform, you gain the functionality of Splunk Enterprise for collecting, searching, monitoring, reporting and analyzing all of your real-time and historical machine data using a cloud service that is centrally and uniformly delivered by Splunk to its large number of cloud customers, from Fortune 100 companies to small- and medium-size businesses
Splunk SmartStore	SmartStore is an indexer capability that provides a way to use remote object stores, such as Amazon S3, Google GCS, or Microsoft Azure Blob storage, to store indexed data

Meet your Splunk Professional Services Team

Consultant

Splunk Professional Services consultants are accredited and experienced in delivery of Splunk solutions. Splunk's consultants are aligned to a domain specialty and bring a background of industry knowledge. In a SIEM replacement scenario, that domain is security.

In a SIEM replacement, typical Splunk consultant tasks may include:

- Platform implementation
- SIEM implementation
- Use case implementation
- Splunk app development
- SOAR app development
- SOAR response plan (playbook) development
- Splunk Enterprise Security configuration
    - Splunk Enterprise Security app install and configuration
    - Risk based alerting (RBA) implementation
    - Assets and Identities configuration
    - Threat Intelligence configuration
- Knowledge transfer and handover to customer teams
- Conducting kickoff call

Architect

A Splunk Professional Services architect is an experienced domain specialist who conducts workshops, creates architectural designs and supports specialized implementation activities. Architect time allocation is typically frontloaded in a SIEM replacement project, however depending on the size and scale of a project they may also provide oversight and guidance for a project team throughout multiple project phases.

In a SIEM replacement, typical Splunk architect activities may include:

- Requirement breakdowns and technical input to the project timelines
- Conducting analysis and design phase workshops. These may include:
    - Use Case Workshop
    - SIEM Design Workshop
    - Platform Design Workshop
    - SOAR Platform Design Workshop
    - SOAR Response Plan (Playbook) Design Workshop
    - Index and Retention Planning Workshop
- Analyzing existing architectural patterns in Optimization Check engagements
- Providing oversight and guidance to extended project teams
- Creating high-level and low-level design documentation
- Knowledge transfer and handover to Splunk consultants and customer teams
- Conducting kickoff calls

Project manager

A Splunk Professional Services project manager (PM) is a critical component of a successful Splunk-led SIEM replacement project. Splunk PM time is a value multiplier, allowing architects and consultants to focus on the activities that they are trained and experienced in. Splunk PMs do not perform identical activities to your organization's internal PM team. Removing PM time allocation from a SIEM replacement may lower the dollar value of a Splunk Professional Services purchase, but will increase TTV and thus TCC disproportionately, typically increasing total costs overall.

In a SIEM replacement, typical Splunk PM activities may include:

- Defining the project methodology and communication cadence
- Creating and agreeing upon a delivery plan
- Working with customer stakeholders, including customer PMs, to ensure timely and appropriate flow of information
- Acting as a single point of contact with Splunk internal stakeholders to ensure flow of information to the customer, and avoid unnecessary repetition
- Assisting with resource project time planning and allocation
- Co-creating an implementation plan and timeline with the Splunk architect
- Managing check-in activities, such as daily standups
- Managing time-recording and status-reporting activities
- Creating and overseeing any proposed validation and testing plan
- Completing project closeout and signoff

Splunk Professional Services roles summary

Together, these roles produce a highly efficient team that can drive rapid TTV and overall value from Splunk-led SIEM replacement engagements. This model is always recommended by Splunk Professional Services, as it has shown consistent success and value realization across our customers SIEM replacements.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries.
All other brand names, product names or trademarks belong to their respective owners. © 2024 Splunk Inc. All rights reserved.