splunk> turn data into doing

PROFESSIONAL SERVICES

# Splunk Security Cloud Success

Success approaches for common Security Use Cases for your critical business operations

The Splunk Security Cloud Success offering focuses on providing a quick realization of value across two different pathways. This offering is designed to apply Splunk best practices, provide recommendations for improvement, and accelerate your journey into Splunk Security Cloud. Depending on the version selected, it may include a Maturity Review/Security roadmap session, Data Onboarding Review session, Security Essentials review session, Configuration assistance session, and Case Management workflow session.

## Accelerate Your Success

These services are backed by Splunk experts, ensuring consistent and quality delivery, architecture, training, and ongoing sustainment for Splunk in your enterprise.

## Business Challenge

Security organizations today are challenged to cull through the mountains of data at speed and scale to manage your business and minimize risk within the environment. This requires a shift in focus from day-to-day technology operation to leveraging technology to enable desired business outcomes. You need support from your key technology partners and vendors. They must have a deep understanding of your business objectives and how to align to tactical goals to ensure that your critical initiatives are realized and return the quickest possible time to value.

## Splunk Solution

Our Experts will help you gain visibility into your security operations by implementing at least one recommended Use Case from scratch or continue to implement pre-built content developed during the Splunk Autobahn. This offering is intended to enable you to implement initial standard use cases, as quickly as possible. For more advanced configurations, such as utilizing Machine Learning Toolkit (MLTK), 3rd party integrations, complex Asset and Identity configurations, please contact Splunk for a customized implementation solution.

## Success Offering Benefits

This offering is specifically designed to provide expert Security guidance and an accelerated time to value with Splunk Security Cloud. We're here to help and ensure your success by providing:

- **Faster Innovation:** Utilizing Splunk Cloud with Out-of-the-Box security content enables you to focus on what matters most.
- **Quicker Time to Value:** Using Splunk Cloud and our proven service delivery model, you will be up and running quickly.
- **Enhanced Security Posture and Maturity:** By quickly realizing value, you obtain needed security visibility across your enterprise faster. The Maturity Review aligns your objectives and strategy with tactical needs, increasing the overall Security Posture and Maturity of your Security Operations.

## Offer Details

Splunk Security Cloud Standard is limited to Use Cases that utilize Splunk Enterprise but includes the Security Essentials App along with predefined services and best practices. Our Experts may perform the following activities for Splunk Security Cloud Standard (depending on the number of Protected Devices):

- **Maturity Review / Security Roadmap**: This session will be used to define the work to be performed for the duration of the engagement. Whether you have journeyed through a Proof of Value or you are a new customer, we will use this time to determine your current capabilities and align those with your goals as well as create a customized implementation roadmap.
- **Security Essentials Guided Walkthrough:** A curated journey through the Security Essentials app which will include discussions on the included use cases, how to manage (filter / create / bookmark) the included content, utilizing data availability and introspection.
- **Data Onboarding Review Session**: This session validates the data required to fulfill the requirements of the various use cases that have been picked for implementation along with a detailed plan of how to obtain this data.
- **Data Onboarding Assistance:** Assist with data onboarding with standard security data sources, as noted in stage 1 of the Security Data Journey within Splunk Security Essentials. Activities will include advisory services on normalizing the data, deploying the appropriate Technology Add-on(s) and ingesting the required data into the platform.
- **Use Case Advisory Discussion:** Review available use cases based on customer data sources and advise on essential detections to improve customer security posture based on the capabilities of Splunk Enterprise only.
- **Configuration Services**: Assist with configuration of Splunk Security Essentials, along with the creation of one alert (detection) and email workflow within Splunk Enterprise.
- **Use Case Development Workshop for 10,000+ Protected Devices:** Multi day workshop focused on aligning security with the capabilities of Splunk Enterprise and basic alerting.

**Security Cloud Plus Details**
Security Cloud Plus includes everything in Standard listed above. Additionally, our Experts may perform the following activities for Splunk Security Cloud Plus (depending on the number of Protected Devices):

- **Data Onboarding Assistance:** Assist with data onboarding with standard security data sources, as noted in stages 2 through 6 of the Security Data Journey within Splunk Security Essentials. Activities will include advisory services on normalizing the data, deploying the appropriate Technology Add-on(s) and ingesting the required data into the platform.

- **Enterprise Security:** Full Security Incident and Event Management (SIEM) capability with Splunk Enterprise Security (ES). Includes ES implementation and configuration for all essential ES frameworks (e.g. assets / identities, threat intelligence), as well as Risk Based Alerting configuration guidance.

- **Enterprise Security Content Updates**: This session will discuss using analytic stories and more advanced detections included in the regularly updated content pack.

- **Use Case Development Workshop**: Multi-day workshop focused on aligning security monitoring use cases with your strategic and tactical objectives to harness the power of Enterprise Security.

- **Advanced ES Configuration:** Configure risk annotations and risk factors to leverage Risk Based Alerting (RBA) in Enterprise Security. Assist with additional applicable visualizations, advanced assets and identity configuration (third-party sources, advanced categorization, and prioritization).

**Assigned Expert included for 10,000+ Protected Devices**
The mission of the Assigned Expert is to help you win with proactive planning and management. They guide you in the planning, coordination, implementation, and optimization of your Splunk investment to address specific business needs.

- **Key Features**:
  - Splunk Project Technical Oversight & Guidance
  - Transformation & Scale Advisement
  - Proactive Risk Assessments
  - Tune Up Workshops

| | Security Cloud Edition* | |
|---|---|---|
| | Standard | Plus |
| Project Kickoff | ✓ | ✓ |
| Security Essentials Walkthrough | ✓ | ✓ |
| Configuration Services | ✓ | ✓ |
| Data Onboarding Review Session | ✓ | ✓ |
| Data Onboarding Assistance | ✓ | ✓ |
| Maturity Review and Roadmap | ✓ | ✓ |
| Use Case Advisory | ✓ | ✓ |
| Use Case Development Workshop | ✓ | ✓ |
| ES Content Updates | - | ✓ |
| Enterprise Security Review and Configuration | - | ✓ |
| Advanced ES Configuration | - | ✓ |
| Assigned Expert | - | ✓ |

*Services delivered is dependent on # of Protected Devices

## Enhanced Implementation Services

If you require assistance with some of the more advanced features of Enterprise Security like:

- Configuring the Machine Learning Tool Kit
- Predictive analytics that are not part of the out of the box configurations
- Hybrid deployments (mix of Splunk Cloud and existing on-prem)
- Design and configuration of complex workflows
- Replacement of an existing monitoring / SIEM platform or tool
- Migration of any data

- Additional data integration and/or development outside of Active Directory for Assets and Identities

Please contact your Splunk Sales Representative or send an email to cs-sales@splunk.com to engage with us on any of these additional services.

## Splunk Professional Services

We are here to help you get the most out of your Splunk products. Our services are backed by Splunk experts, who provide consistent and quality service delivery, architecture guidance, training, and ongoing support. Take your Splunk environment to the next level and achieve continual optimization, enhanced processes, and active collaboration.