Splunk Professional Services Catalog

This catalog of Splunk Professional Services is provided for informational purposes only and Cisco and the Customer will discuss and agree on the specifics of the Services to be provided during the Services Term as well as any associated limitations or prerequisites (if any) at the Services kick-off.

Activity Name	Activity Description
Risk-Based Alerting Implementation Success	
Taking advantage of risk-based alerting (RBA), through Splunk Enterprise Security, will greatly empower and maximize the efficiency of your SOC. Splunk's RBA Implementation Success offering allows you to successfully deploy, adopt and realize value faster with standardized risk and risk incident rules as the foundation to building a more resilient enterprise with Splunk. If you are already leveraging Splunk Security Orchestration, Automation and Response (SOAR) or in the process of implementing it, Splunk has developed a Risk Notable Playbook Pack, to be deployed with Splunk SOAR, specifically tailored to enrich and triage alerts generated through the RBA methodology, allowing your team to work smarter and respond faster to alerts.	
Services	• RBA workshop and discovery • Build & Configure risk incident rules • Configured risk and risk incident rules • Risk modifier framework • RBA maturity roadmap • RBA operational runbooks • Knowledge Transfer with security team • Implement and configure SOAR Risk Notable Playbook Pack (if applicable)
Security Use Case Development Workshop	
Whether you are working on an initial deployment or maturing your security monitoring, the Splunk Enterprise Security Use Case Development Workshop can help. This workshop helps you increase the effectiveness of your security monitoring, identify ways to improve your security posture, and refine your monitoring strategy to better align with your business priorities. Our experts aid in identifying and customizing the security queries (use cases) to maximize the opportunities to improve your security posture, align with your enterprise needs and risk priorities.	
Services	• Use Case Development Workshop
SIEM Replacement Assessment	
Our consultants support the replacement of legacy SIEM products across the globe and are ready to lead your replacement. We have developed a framework for identifying the critical steps and timelines of the significant stages in a replacement project. In our Replacement Implementation Workshop, customers will work with us to develop a customized migration plan.	
Services	• Identify use cases to be implemented in your new environment • Develop a dual environment data feed plan • Evaluate data sources and map data requirements to use cases • Provide a customer network architecture recommendation for the new Splunk environment • Evaluate custom integration requirements (workflows, ticketing, etc.)

	• **Conduct integration planning for existing Splunk instances already running in your organization** • **Deliver a high-level project plan with timelines and estimated levels of effort required**

Fraud Analytics Success

The Splunk Fraud Analytics (SFA) Service Offering covers all activities required to deploy the SFA application, onboard data, and implement alerting, and build visualizations for fraud-relevant information. This Professional Services offering is for implementation of the Splunk Fraud Analytics application and is separate from the implementation of Splunk Enterprise Security (requirement for SFA). Our experts may perform the activities described below for the planning and implementation of Splunk Fraud Analytics.

Services	• **Implementation Planning Workshop**: Identify key fraud use case(s) and applicable data sources. This session will inform the work to be performed for the duration of the engagement. • **Data Onboarding Assistance:** Splunk experts will assist with data onboarding, CIM compliance, and applicable data model configuration. • **Asset and Identity Review and Configuration:** Splunk experts will help you with categorizing and prioritizing your internal assets and identities for better fidelity and context within configured alerts and dashboards. • **Use Case Review and Tuning Session:** Splunk experts will work with you to review the configured detections and alerts to ensure they are providing the expected results. • **Visualization Review Session:** Splunk experts will work with you to review the included visualizations/dashboards to ensure they are populating correctly and modify if necessary. • **Risk Based Alerting Configuration Services:** Splunk experts will ensure Risk Based Notables are configured and alerting as expected, and assist you with further configuration and tuning, as necessary, of Risk Based Alerting functions.

Splunk Observability Implementation Success

Splunk's Observability Implementation Success offering is a comprehensive service designed to ensure You are successful in Your implementation of Splunk Observability and to accelerate adoption and time to value. Our Cisco Splunk Consultants will architect and configure your Infrastructure Monitoring (IM) and/or Application Performance Monitoring (APM) environment with the latest best practices, quickly and effectively. The offering is available The various packages (Small, Medium, Large, and X-Large) which are designed to meet your organization's size and goals and which can apply to both simple and complex environments, helping Your organization along Your resilience journey.

Services	• **Discover and Design –** Our experts will engage in a kickoff with your team to discuss current business and technical requirements, validation of use cases to be deployed, and understand your technologies and tools. We'll go through an Architecture and Implementation Planning Workshop (not in Small package) to build a customized implementation plan, including steps, prerequisites, and the best possible configurations for your deployment, whether its Splunk IM and/or Splunk APM. • **Configure and Implement -** Build out your Splunk environment with a Splunk Certified Consultant aligned to the implementation plan. For Splunk IM, we'll go through a configuration and automation exercise of your infrastructure and service emitters. For Splunk APM, we'll run auto and/or manual instrumentation of applications. For our larger engagements, we'll conduct use case workshops and find new ways to evolve your enterprise resilience.

	• **Knowledge Transfer and Documentation** – As we go through the engagement, our experts will work with your team to ensure they understand the processes to continue to develop and evolve your organization's ability to take advantage of Splunk IM and/or APM.

Splunk Observability Smart Start

Services to accelerate your transition to Splunk Observability, to assist teams with onboarding to Observability by using best methodologies and best practices for faster adoption of the Observability suite. The onboarding process will allow consumers and the monitoring team to help develop a more effective, intuitive process to help adopt the Observability monitoring tool efficiently, faster and ensure you get it right first time. Leveraging people, processes and the Observability Suite to shorten your time to value and maximize business impact. Splunk Observability onboarding process provides Expert Services to help you transition to Splunk Infrastructure Monitoring, Splunk Application Performance Monitoring (APM), Browser/Mobile RUM, Log Observer and Synthetic monitoring to meet your business objectives. The implementation will be performed on a sample set of infrastructure, services and applications in order to define the customized Smart Start Onboarding processes to meet your business requirements

Services	• Creation of a structured custom onboarding plan tailored to your requirements and business objectives. • Creation of documented standardized onboarding process and flows using best practices and methodologies. • Creation of detailed self-service resources within your environment for each step of the onboarding process from consumer requirements, getting data in, to creating teams, dashboards and detectors. • Sample Implementation of the Observability products to put the Onboarding process into practice. • Custom use case implementation. • Assisting monitoring and CoE teams to onboard consumers efficiently and rapidly showing faster ROI. • Increasing value of the Splunk Observability deployment. • The onboarding process can be tied in to use Configuration as code support via Terraform. • Training recommendations & End user workshops.

Splunk Observability Solution Replacement Success

Splunk Observability Solution Replacement provides Expert Services to help you transition to Splunk Infrastructure Monitoring (IM) and/or Splunk Application Performance Monitoring (APM) to meet your business objectives. Jump start your Splunk Observability adoption journey and accelerate your transition to Splunk IM and/or APM following Splunk Best Practice methodologies with Splunk experts providing technical expertise and guiding you through the challenges of an observability solution replacement with a successful deployment. The solution replacement packages are sized to suit small businesses through to large enterprises. Modular and expandable, the Services can be customized to precisely suit your specific needs.

Services	• Architecture and Existing Observability Solution Review Workshop. • Creation of a migration plan based on your environment, use cases and end users to enable a smooth deployment and transition. • Assistance reconfiguring new or existing emitters and metrics pipelines to gather infrastructure and service metrics for Splunk IM. • Assistance instrumenting and updating your application code and code annotations to work with Splunk APM. • Recreation of existing business critical visualization and alerting content with custom dashboards, detectors and notification policies. • Assistance with content creation for end users to assist their transition to Splunk Observability Solution.

	• Security and governance best practice review and configuration. • Configuration as code support via Terraform. • Advanced Analytics with SignalFlow query language. • Training recommendations & End user workshops.

Splunk Observability Value Assessment

Splunk Observability Value Assessment provides Expert Services to achieve maximum value from your Splunk Observability solution, focused on recognizing additional value, and improving adoption through best practice as well as help you realize the value required from Splunk Infrastructure Monitoring and/or Splunk Application Performance Monitoring solution against your business objectives. The value assessment packages are sized to suit small businesses through to large enterprises. Modular and expandable, the Services can be customized to precisely suit your specific needs. During an Observability Value Assessment our Splunk Experts will partner with you to and provide guidance on best practices to achieve improved value and insight from your observability use cases. The Service offers Use Case Optimization, Configuration Reviews and Recommendations.

Services	• Review of current Architecture and Deployment of Splunk Observability products • Review can include metrics instrumentation, APM instrumentation, chart and dashboard use cases, detectors, outbound integrations and troubleshooting workflows. • Suggestions based on best practices to improve value from current instrumentations, dashboards, detectors and troubleshooting workflows. • Updates on any new platform features and functionals and how they may be used to gain additional insight or improve end user experience. • Executive presentation of findings and recommendations. • Guidance on achieving additional value by using advanced functionality such as built in detector conditions, advanced SignalFlow Analytics or managing content as code via Terraform. • Identification of additional data sources and use cases to provide additional insights and value. • Recommendations and guidance to onboard additional data sources and implement new use cases while following industry standard best practices. • Optimization of existing use cases such as excessive noise reduction, misfiring detectors, readability improvements, dashboard optimization and adjusting metadata to make the data you send more useful and meaningful.

Splunk Cloud Migration Success

The Splunk Cloud Migration Success Offering will take a holistic review of your Splunk architecture and Splunk deployment best practices to determine the migration path to Splunk Cloud. We provide guidance and expertise to not only migrate your deployment, but also to optimize it for Splunk Cloud. The Splunk Cloud Migration Success Offering is designed for Splunk customers who are looking to minimize downtime and minimize the time it takes to migrate to Splunk Cloud. Additionally, this Migration is targeted to customers who need to preserve their Splunk Historical Data in the original format, want to implement a Splunk deployment to best practices and have already on-boarded data and custom-built applications.

Services	• Planning Services include Resourcing, Platform Checklist, Kickoff Meeting, Assess Data Source. • Delivery and Execution Services include Architecture Review, Optimize for Cloud, Provision Cloud stack, Start Cloud, Data Migration, Customer content migration, Cut Over, stabilize. • Completion Services include Tuning

Splunk Enterprise/Cloud Implementation Success

The Splunk Enterprise/Cloud Implementation Success Offering provides new customers with the foundation to deliver performance and scale to their end users. Leveraging the latest best practices, our Splunk Accredited Consultants, Solutions Architects, and Delivery Managers will work with you to implement the best deployment of Splunk for your needs.

Services	Depending on the package size purchased, the following services may be delivered: • Planning Services include Resourcing, Platform Checklist, Kickoff Meeting, Assess Data Source • Create a customized Implementation Plan outlining Architecture, Use Cases, Data, and Success Criteria • Install and Configure Best-Practice Splunk Data Collection Architecture • Collect Data in to Splunk • Discuss Splunk Storage and Security Model, Apply Security Model to Data in Splunk • Integrate Key Configuration Points with Source Control • Consult to Determine Requirements and Success Criteria • Understand Data and Extract Knowledge from Understood Data • Apply Tags and Expand Naming Conventions for Easier Searching • Search Data from a Central Location, Create Alerts Based on Important Data • Build Reports and Drilldowns for Operations, Security, Business Analytics, and Executives • Install a SplunkBase App, or Create a Custom App

Optimization Check

As you onboard data and users into your Splunk environment, it's valuable to look under the hood to ensure your searches and dashboards are still operating at peak performance. Whether you are preparing for an upgrade, re-architecture, scale-out, or are simply not seeing the speed you expect of searches and dashboards, this offering can help. This offering includes a review of architecture, configurations, knowledge objects, data governance and use cases. Leveraging best practices, our Splunk experts will ensure your users and administrators receive the experience they expect.

Services	• Review of Splunk Architecture and Configurations (Indexers, Search Heads, configuration points) • High-Level Performance Assessment (Splunk performance metrics, slow or skipped searches, bottlenecks) • Deep-dive Assessment of Data Sources (Input configurations, Field Extractions, Lookups, KV Store, and Data Models) • Audit of Deployed Apps / Technical Addons and their configuration • Audit existing searches to identify inefficient searches and provide recommendations • Review search and indexing capacity against current and projected requirements • Review known or identified environmental, performance, or stability issues • Identify any features that could be utilized to optimize the Customer's experience • Review an agreed subset of existing dashboards - provide Customer with feedback and best practices • Audit data retention and security settings, reviewing data source ownership and permissions in place

Splunk Enterprise Security Implementation Success

The Splunk Enterprise Security (ES) Implementation Success Offering comes in three sizes – Basic, Standard, and Premium – to provide the capabilities that will optimize the implementation and TTV within your environment.

Basic Offering -Basic is designed for customers with more internal resources dedicated to the Splunk project. Internal Splunk Admins and Users will receive informal training from the Splunk Accredited Consultant and will complete tasks remaining after Splunk Professional Services finishes their work.
Standard Offering -For customers looking for more support during the initial installation but are confident that ongoing maintenance and optimization of Splunk will be handled well by internal resources, build upon the services offered in Basic with our Standard offering.
Premium Offering-This is designed for customers who recognize the opportunity for additional business value beyond the set of initial use cases. With the Premium offering, additional services beyond Standard are included, such as ongoing architectural, workshop, and optimization assistance, plus staff augmentation to meet additional use case and outcome needs.

Services	• Planning: -Workshop with a Solutions Architect to develop a plan for implementation. • Installation: Deploy Splunk Enterprise in your environment; On-board seven or nine essential data sources; Install Splunk Enterprise Security; Deploy and optimize 7 to 18+ use cases (correlation searches) for your environment; Optimize out-of-the-box content. • Training: Provide remote over-the-shoulder training for your Splunk Admins; Complete a walk-through of ES functionality for your staff; Review best practices for on-boarding data; Review best practices for creating correlation searches. • Coordination A Delivery Manager tracks your path to success

Splunk ITSI Implementation Success

Splunk IT Service Intelligence (ITSI) Implementation Success is designed for new installations in Splunk Cloud or on-prem environments. The offering is designed for customers who are new to Splunk IT Service Intelligence (ITSI). This Professional Services offering helps customers successfully configure elements such as Services, KPIs, adaptive thresholds, anomaly detection, predictive service health, and event analytics to gain greater visibility and insights into the health of their monitored services and devices. Splunk onboarding packages are sized to suit small to large businesses all the way up to enterprise level. Modular and expandable, the prebuilt offerings can be customized to precisely suit Your specific requirements and goals.

Services	• Comprehensive Requirements Gathering Session - Collect and document high level business goals and objectives. Create a plan to leverage ITSI to meet these goals. • Service Identification Workshop - Splunk Architect will work with customers and stakeholders to identify, collect, prioritize, and document services, associated requirements, and process workflows. • Service Decomposition Workshop - Identify service KPIs and dependencies to effectively monitor service health. Identify required data sources and importance. • Data Onboarding and Validation - Validate proper onboarding of data sources required to populate KPIs and provide a plan of how to onboard any missing data according to Splunk best practices. • Installation and Configuration of IT Service Intelligence Application - Splunk Professional Services will follow best practices and standard methodologies for the installation and configuration of ITSI and other required apps and add-ons. • ITSI Events Analytics Workshop – Gather requirements and discuss desired outcomes. Identify alert data sources, alert actions, and integrations. Develop an implementation plan to achieve goals.

Splunk SOAR Implementation Success	
Security Automation, Orchestration and Response (SOAR) is changing the world of security operations, incident response, governance, and threat intelligence enablement. The Splunk SOAR Implementation Success Offering has been packaged to match the needs and maturity of the customer's security program.	
Services	Every customer is different, so Splunk have a unique sizing model to provide flexibility to Your needs. The base service provides the following services: • Kick Off meeting to align goals, resources and timelines. • An Architecture Review Workshop to identify the right Splunk SOAR Validated Architecture to meet the Customer's needs. • The installation, configuration of the SOAR instance. • The integration of the customer's Enterprise or Enterprise Security instance(s) to enable data exchange between the two platforms, and the configuration of up to an initial list of up to 5 app integrations in SOAR. • The delivery of Customer specific Knowledge transfer sessions to help with the identification of the right use cases, playbooks and workbooks. • The co-development of a selected response plan into a set of up to 5 playbooks and/or workbooks.
Splunk UBA Implementation Success	
Splunk User Behavior Analytics (UBA) is a machine learning-powered solution that delivers the answers you need to find unknown threats and anomalous behavior across users, endpoint devices and applications. It not only focuses on external attacks but also the insider threat. Its machine learning algorithms produce actionable results with risk ratings and supporting evidence that augment security operation center (SOC) analysts' existing techniques for faster action. The Splunk Professional Services UBA Implementation Success offering is designed for customers looking to incorporate a solution using machine learning and anomaly detection analytics in their security operations center to prevent, detect and respond to cyber attackers in today's security landscape.	
Services	This Professional Services offering is for Splunk UBA only. The following activities may be performed for the Standard offering of Splunk UBA: • Implementation Planning Workshop: Spend time with a Splunk Solutions Architect to discover requirements and customize a project plan that will define the work to be performed for the duration of the project. There is project coordination and success tracking by the Splunk Project Manager. • Configuration Services: A Splunk Accredited Consultant will utilize best practices for installing Splunk UBA while executing the project plan. They will ensure all UBA required data sources are coming into UBA and are normalized correctly. • Use Case Review Sessions: Once data is in place for the recommended baseline period and use cases are enabled, the Consultant will operationalize and tune Splunk UBA use cases. • Knowledge Transfer Sessions: Professional Services will conduct sessions to demonstrate the implementation and document administrative items. Best practices will be communicated and shared on the overall administration of the application.