splunk> turn data into doing

PROFESSIONAL SERVICES

Assigned Expert – Services Description Catalog

Make us an extension of your business. Obtain an Expert. Reap the rewards.

Services Available at Every Stage of Your Splunk Journey

Hand-off

Plan	Implement	Use/Adopt	Optimize/Scale
Core and Platform			
• **Architecture & Implementation Planning Workshop** • **Cloud Migration Assessment** • **Data Source Assessment** • **SmartStore (S2) Preparedness & Planning Workshop** • Use Case Advisory Discussion • Architecture Diagram Creation • Workload Management Planning Workshop • Workflow Management Planning Workshop	• Assist with Implementation Services • Knowledge Transfer to Partner or Splunk Implementation Services • Technical Oversight & Guidance over Implementation Services • Post Implementation Review • Workload Management Implementation Guidance • Workflow Management Implementation Guidance	• **Mentoring of Customer Staff** • Build a Simple Dashboard • Build a Complex Dashboard • Assist with Data On-Boarding • Data Source Review • Index and Retention Review • Build/Debug Search • Create a Drilldown, Workflow, Macro/ Tag/Eventtype • Build a Lookup • Create/Manage Indexes • Extract a New Field	• **Splunk Core Technical Assessment** • Upgrade Readiness Assessment • Scaling Advisement & Expansion Readiness Assessment • Forwarder Health Check • Search or Dashboard Optimization
Security Suite			
• **Architecture & Implementation Planning Workshop** • **Enterprise Security Use Case Development Workshop** • **Phantom Use Case Development Workshop** • **SIEM Replacement Workshop** • Use Case Advisory Discussion • Architecture Diagram Creation • Data Readiness	• Assist with Implementation Services • Knowledge Transfer to Partner or Splunk Implementation Services • Technical Oversight & Guidance over Implementation Services • Post Implementation Review • Splunk Application Integration for Phantom • Splunk Enterprise Security Use Case Implementation Guidance	• **Mentoring of Customer Staff** • Data Model Review • Asset Identification • Data Source Review • Index and Retention Review • Splunk Phantom Configuration Guidance	• Enterprise Security/UBA Technical Assessment • Upgrade Readiness Assessment • Scaling Advisement & Expansion Readiness Assessment • Security Integrations Review • Report or Dashboard Optimization • Splunk Phantom Application Integration Feature Request
ITOA			
• **ITSI Service Model Requirements and Implementation Plan** • **Prescriptive Use Case Workshop – Data Driven Intelligence (Service Insights)** • **Prescriptive Use Case Workshop – Data Driven Intelligence (Event Management)** • **Prescriptive Use Case Workshop – Infrastructure Troubleshooting & Monitoring** • **IT Ops Modernization Workshop** • Use Case Advisory Discussion • ITSI Service Design Review	• Assist with Implementation Services • Knowledge Transfer to Partner or Splunk Implementation Services • Technical Oversight & Guidance over Implementation Services • Post ITSI Implementation Review	• **Mentoring of Customer Staff** • ITSI KPI Identification and Configuration Review for Existing Customers • ServiceNow / Remedy Service Desk Integration Review with ITSI • ITSI KPI Adaptive Threshold Review and Anomaly Detection	• ITSI Technical Assessment • ITSI KPI Base Search Review • ITSI Content Pack Implementation Assessment

***Bold** = Recommended for onsite service (up to 5 days for each service). Non-Bold = Recommended for remote service (up to 8 hours for each service). The number and complexity of the Services that can be performed are dependent upon time available within the Assigned Expert subscription level purchased.

Services above do not address your specific need or question?

Ask the Expert Anytime (General Consultative Service)

Core and Platform Assigned Expert Services

Category	Service Name	Service Descriptions	Location
General Consultative	Ask an Expert	Expert consultative session on Splunk best practices questions related to adoption activities for Splunk Enterprise or Splunk Cloud (does not include Premium Solutions). • Assist the Customer with Splunk best practices on Splunk's "out-of-the-box" functionality and UI based configurations. • Assist the Customer with advanced Splunk best practices and adoption activities which may include HA/DR, multi-site, migrations, and other advanced configurations.	Remote
Use/Adopt	Build a Simple Dashboard	Build dashboard to utilize ingested Splunk data in a visual format. This service may include: • Up to four (4) unique charts or panels • Based on a single (1) new search and existing searches • Up to two (2) Customer specific dashboard inputs (i.e. text boxes or drop-down lists) Out of Scope: • Does not include sub-searches, commands that require sub-searches, custom visualizations, JavaScript modifications, or CSS customizations. Assumptions: • Data already exists in the system (no data onboarding or field extractions) • Dashboard is built in XML and not Splunk's Universal Dashboard Framework (UDF) Customer Required information: • Detailed description of search and dashboard requirements	Remote
Use/Adopt	Build a Complex Dashboard	Build dashboard to utilize ingested Splunk data in a visual format. This Service may include: • Up to eight (8) unique charts or panels, which may include underlying scheduled searches or reports to provide dashboard content • May include Customer specific dashboard inputs (i.e. text boxes or drop-down lists) Out of Scope: • Does not include sub-searches, commands that require sub-searches, custom visualizations, JavaScript modifications, or CSS customizations. • Dashboard is built in XML and not Splunk's Universal Dashboard Framework (UDF) Assumptions: • Data already exists in the system (no data onboarding or field extractions) Customer Required information: • Detailed description of search and dashboard requirements	Remote
Optimize / Scale	Search or Dashboard Optimization	Review and troubleshoot up to five (5) searches, reports, data models, or dashboards in accordance with Splunk best practices. This service may include: • Advise on Splunk best practices for visualizations and workflows • Advise on search re-use and Splunk best practices around building optimized searches, reports, data models, or dashboards • Troubleshoot and tune existing searches, reports, data models related to a dashboard • Coach the Customer on Splunk best practices for review of performance for other searches, reports, data models, or dashboards. The number of searches, reports, data models or dashboards that can be reviewed will depend on the complexity of each search. Out of Scope: • Does not include custom visualizations	Remote

Category	Service Name	Service Descriptions	Location
Use/Adopt	Assist with Data On-Boarding	Assist the Customer with getting new data sources ingesting into Splunk. This Service may include: • Build necessary props & transforms to enable Splunk best practices for new data onboarding • Build necessary inputs.conf configurations necessary to onboard data • Assist with deploying app Out of Scope: • Does not include field extractions which can be requested separately Customer Required information: • Example dataset & data definition	Remote
Plan	Workload Management Planning Workshop	Feature Objective: Workload Management is a Splunk Enterprise feature that optimizes resource efficiency across Splunk Search Heads. This service is a consultative discussion to assist the Customer architect and distribute resource allocation pools for search efficiency across Splunk Enterprise Search Heads (does not include planning around Splunk Cloud or Premium Solutions). This Service may include: • Operational review of Splunk infrastructure • Splunk search performance review • Knowledge transfer of feature behaviors and capabilities • Advise on strategy to implement workload management • Advise on configuration practices Out of Scope: • Does not include implementing Workload Management or application development Assumptions: • Splunk Search Heads are in place and configured • RBAC is configured, users are onboarded and active • MC is setup and running • Customer user has admin privileges to the environment	Remote
Plan	Workflow Management Planning Workshop	Feature Objective: Workflow Management is a Splunk Enterprise feature that automates actions from events to interact with web resources that reduce the number of steps taken to either investigate or take an action on an event. This service is a consultative discussion to assist the Customer architect and configure workflows based on event types that enable interaction between Splunk and web resources. This Service may include: • Review Customer data sources pertinent to their Web Resource solution which may include SNOW, IP Lookup, or an agreed upon Web Resource solution • Review Customer web resources leveraging Workflow actions • Knowledge transfer of feature behaviors and capabilities • Advise on strategy to implement workflow management • Advise on configuration practices Out of Scope: • Does not include implementing Workflow Management or application development Assumptions: • Splunk Search Heads are in place and configured • Customer user has admin privileges to the environment	Remote

Category	Service Name	Service Descriptions	Location
Implement	Workload Management Implementation Guidance	Feature Objective: Workload Management is a Splunk Enterprise feature that optimizes resource efficiency across Splunk Search Heads. This service provides Customer guidance through the implementation of Workload Management (WLM) for up to three (3) resource pools and up to five (5) rules across Customer Splunk Enterprise Search Heads (does not include planning around Splunk Cloud or Premium Solutions). This service may include: • Guides Customer through creating resource pools based on applications or users • Monitor hardware and search performance based on resource pools • Guides Customer on the monitoring of search pool metrics and resource pool tuning adjustments based on search pool behavior Out of Scope: • Splunk does not implement Workload Management on behalf of the Customer Assumptions: • Workload Management Planning Workshop has been executed • The cgroups at the OS level are already configured	Remote
Implement	Workflow Management Implementation Guidance	Feature Objective: Workflow Management is a Splunk Enterprise feature that automates actions from events to interact with web resources that reduce the number of steps taken to either investigate or take an action on an event. This service guides Customer through creating and configuring up to three (3) Workflow actions based on eventtype across Customer Splunk Enterprise. Out of Scope: • Splunk does not implement Workflow Management on behalf of the Customer Assumptions: • Workflow Management Planning Workshop has been executed	Remote
Use/Adopt	Build a Search	Assist with building or debugging simple searches of indexed Splunk data. This service may include: • Build a single (1) search with up to three (3) data sources Out of Scope: • Does not include sub-searches or new data model creation Assumptions: • Data already exists in the system (no data onboarding or field extractions) Customer Required information: • Detailed description of search requirements	Remote
Use/Adopt	Create a Drilldown	Assist with creation of a drilldown on an existing dashboard to provide deeper data visibility • Add up to five (5) drilldowns to existing dashboard Customer Required information: • Current dashboard and drilldown definition	Remote
Use/Adopt	Create a Macro, Tag, or Eventtype	Assist Customer with creation of knowledge objects to facilitate the index of data • Create up to five (5) macros, tags, or eventtypes • Assumes search already defined Customer Required information: • Definition of items to be created	Remote
Use/Adopt	Create Workflows	Enable interactions between indexed or extracted data to other web sources • Create up to five (5) workflows • Limited to one (1) field per workflow Customer Required information: • Data source type, target of workflow action, fields to be provided to target	Remote

Category	Service Name	Service Descriptions	Location
Use/Adopt	Build a Lookup	Create lookup tables to enrich indexed data • Create a single csv or kv store-based lookup • Enable automatic lookups if required Customer Required information: • Csv to be used for lookup, sourcetype to be used, linked values within data sources	Remote
Use/Adopt	Create/Manage Indexes	Creation of indexes to organize ingested data within Splunk for searching • Create up to five (5) indexes • Manage retention and access policies for up to five (5) indexes • Assist with deployment of app Customer Required information: • Index names and retention and access requirements	Remote
Use/Adopt	Extract a New Field	Assist the Customer to properly extract particular fields from datasets, leveraging Splunk best practices. This Service may include: • Extract up to five (5) new fields via regular expression(s) or key values Customer Required information: • Example dataset & data definition and field names required	Remote
Plan	Use Case Advisory Discussion	Consultative discussion to identify additional use cases or review of completed Data Source Assessment (DSA) executed to determine key technical requirements, identifying current progress, and outline of next steps. • May include review of requirements, determination of additional data sources, and underlying architecture changes required. • This task covers Splunk Enterprise only (not premium solutions)	Remote
Optimize / Scale	Forwarder Health Check	Analyze and recommend remediation of abnormal forwarder behavior. • Analyze abnormal forwarder behavior such as 'altogether missing', 'some missing' or 'slow throughput' • Provide recommendations on remediation required and ongoing monitoring configurations for critical inputs • Advise on Splunk best practices for forwarder configuration including event breaker, indexing discovery and site failover • Includes up to four (4) forwarder types	Remote
Plan	Architecture Diagram Creation	Create an Architecture Diagram illustrating Customer's Splunk implementation	Remote
Optimize / Scale	Scaling Advisement & Expansion Readiness Assessment	Review existing Splunk environment for proposed scaling activities. • Review project technical readiness against the Customer-documented requirements Briefly assess the following to determine the feasibility of using the current environment for expansion: Splunk architecture, High-level performance, Data onboarding	Remote
Implement	Post Implementation Review	Review an existing, previously implemented Splunk environment and provide performance feedback and recommendations. • Review and provide Splunk best practice recommendations for additional use cases implemented by the Customer • Provide recommendations for additional data source configurations created by the Customer	Remote
Use/Adopt	Data Source Review	Review existing data onboarding procedures and configurations and compare to Splunk best practices. This may include identifying issues with: • Splitting of data into individual events • Multi-line merge settings • Parsing of date/timestamps, time zone settings • Truncation of long events Splunk will advise on the importance of proper data onboarding, recommended applications from Splunkbase, and adhering to the Splunk Common Information Model ("CIM") where possible.	Remote

Category	Service Name	Service Descriptions	Location
Use/Adopt	Index and Retention Review	Consultative discussion to define a strategy for index definition and data retention. This Service may include: • Advise on retention strategy in alignment with the Customer audit and compliance requirements. • Advise on time and size-based retention capabilities • Advise on data archiving and restoration recommendations • Advise on access control recommendations	Remote
Optimize/ Scale	Upgrade Readiness Assessment	Assess the Customer environment to validate it is adequately prepared for a version upgrade. This service may include: • Checks for adequate hardware provision, deprecated features and known issues • Identify possible App compatibility issues • Advise on Splunk best practices for upgrade procedures and workflows • Provide recommendations and remediation activities required	Remote
Plan	Architecture & Implementation Planning Workshop	Review the customer requirements and produce Architecture Recommendations, list of data sources, and Implementation Plan. Activities: • Review Customer use cases to identify data sources and their associated data on-boarding methods • Document Customer requirements in Architectural Recommendations per Splunk best practices • Identify Technology Add-ons required • Identify Splunk Apps applicable to Customer use cases • Identify data enrichment requirements based on Customer use cases and data sources • Document anticipated tasks, estimated duration, Customer pre-requisites, and dependencies in Implementation Plan	Onsite
Optimize/ Scale	Splunk Core Technical Assessment	This workshop is designed to provide a comprehensive review of the customer's Splunk environment to validate the customer's deployment remains sustainable, stable and ready to scale. Activities: • Discovery: An account review and discussion of the current environment, indexing volume, data sources, architecture, primary use cases and outstanding issues. • Diagnostics: Configuration and monitoring of the Management Console (MC) to conduct the assessment. • Architecture review: Review and document Splunk instances, configurations, hardware specifications and OS settings to verify they adhere to Splunk best practices. • Server configuration: Review Splunk resource utilization, instance and application configuration, consistency, deployment server configuration, and internal error analysis. • Data lifecycle inspection: ○ Collect – Validate that data is being collected and processed at the forwarder tier efficiently in accordance with Splunk best practices. ○ Index – Review indexing performance, index sizing and storage retention settings. ○ Search – Audit stagnant running and inefficient searches and provide search optimizations. • Optimization techniques: Provide optimization techniques on data onboarding, searching, dashboards, application deployment and Splunk best practices. • Inventory review: Review of inventory for dashboards, saved searches and reports to identify unused knowledge objects and content. • Security review: Review of security settings, authentication, role-based access controls and Splunk role capabilities. This assessment is not designed to provide recommendations for optimization of Splunk premium products, such as Splunk ITSI or components of the Splunk Security Operations Suite.	Onsite

Category	Service Name	Service Descriptions	Location
Plan	Cloud Migration Assessment	This workshop is designed to provide a pragmatic approach to help migrate the customer's environment to Splunk so the customer can minimize downtime while also leveraging the customer's architecture to align to and access Splunk Cloud. The workshop will evaluate the customer's on-premise Splunk installation for Migration to Splunk Cloud which will result in a roadmap that provides guidance, Splunk best practices and requirements for migrating to Splunk Cloud. Activities: • Assessment of current on-premise environment • Migration plan for current Apps, configurations, and indexed data • Migration plan for data collection architecture Pre-Requisite: • Customer has already deployed a functional Splunk infrastructure running and already on-boarded data and custom-built applications	Onsite
Plan	Data Source Assessment	Conduct interviews with customer staff to determine additional opportunities for required data sources using Splunk's Data Source Assessment Tool. Activities: • Execute DSA • Review Technical Requirements	Onsite
Plan	SmartStore (S^2) Preparedness & Planning Workshop	Work with customer to assess storage requirements and plan for use of Amazon S3 compatible storage using Splunk SmartStore. This service may include: • Review validation of S3 storage location and compatibility with required API calls • Perform retention planning / cache sizing • Evaluate searches with eye to paradigm shift • Document cutover plan, including data sizing requirements and transfer methodology (i.e. Amazon Snowball) • Document recommended ongoing monitoring plan	Onsite
Use/Adopt	Mentoring of Customer Staff	Augment the customer team's efforts by utilizing Splunk SME's expertise in a tailored interaction to align to customer business initiatives and use cases. • The assigned SME will arrive onsite and spend one work week (five (5) business days) with the customer's team to work through challenges and coach the customer team on implementing Splunk best practices to resolve them.	Onsite

Security Suite Assigned Expert Services

Category	Service Name	Service Descriptions	Location
General Consultative	Ask an Expert	Consultative Session to answer adoption and Splunk best practice questions related to Security Premium Solutions, including Enterprise Security, Phantom, and UBA. • Assist Customer with Splunk best practices approach to adoption	Remote
Plan	Use Case Advisory Discussion	Review of a Security use case roadmap executed with the Splunk Customer Success Manager ("CSM")" or Sales team to determine key technical requirements, identify current progress, and outline of next steps. • This may include reviewing a previously executed Prescriptive Value Path (PVP) session and discussing technical next steps, such as requirements and architectures, identifying data sources, discussing Customer specific use case content, and recommended tuning to reduce false positives. • This task covers Security Premium Solutions, including ES correlation searches, Phantom playbooks/runbook definitions, and UBA data models.	Remote
Implement	Splunk Enterprise Security Use Case Implementation Guidance	Provide guidance to Customer with creating and tuning one (1) "out of the box" ("OOTB") use case for Enterprise Security. This may include: • Review existing OOTB correlation search • Guide Customer through tuning the OOTB correlation search in accordance of Splunk best practices • Validate the subsequent SPL performance Out of Scope: • Splunk does not implement the use case on behalf of the Customer Assumptions: • Use Case Advisory Review has been previously executed	Remote

Category	Service Name	Service Descriptions	Location
Use/Adopt	Asset Identification	Consultative session to assist Customer with identifying sources suitable for population of assets and identities. • Up to ten (10) sources per session Customer Required Information: • Customer currently ingested data sources in Splunk • Access to data being considered for onboarding into Splunk architecture	Remote
Optimize / Scale	Report or Dashboard Optimization	Help with modification and tuning of editable dashboards/panels that are contained within a component of the Splunk Security Operations Suite. • Assistance with up to four (4) unique charts or panels Out of Scope: • Does not include sub-searches, commands that require sub-searches, custom visualizations, javascript modifications, or CSS customizations. Assumptions: • Dashboards have been created and associated data exists and has been onboarded and normalized • Acceleration is already enabled for underlying / associated Data Model	Remote
Use/Adopt	Data Model Review	Consultative walkthrough of the Data Model Audit dashboard within Enterprise Security, and guidance on Splunk best practices for active and inactive data models.	Remote
Optimize / Scale	Splunk Phantom Application Integration Feature Request	Consultative session to define feature request and gather necessary Customer requirements.	Remote
Implement	Splunk Application Integration for Phantom	Configuration of one (1) of the following Splunkbase applications or Technical AddOns aligning to an existing Customer Phantom implementation: • EWS for Exchange, LDAP, SAML configurations, Splunk application installs (Phantom App on Splunk and Splunk app for Phantom), ServiceNow (unidirectional), Splunk Remote Search configuration, Event forwarding from Splunk, Chat tools (Slack, teams).	Remote
Use/Adopt	Splunk Phantom Configuration Guidance	Guidance for Splunk Phantom configurations related to one (1) of the options below: • Cluster management and expansion • Warm/Standby Configurations • Backing up or restoring Splunk Phantom	Remote
Plan	Architecture Diagram Creation	Create an Architecture Diagram illustrating Customer's Splunk implementation	Remote
Optimize/ Scale	Scaling Advisement & Expansion Readiness Assessment	Determine if the current as-built Splunk environment is fit for purpose for the next phase of the project. • Review project technical readiness against Customer-documented requirements • Assess the following to determine the feasibility of using the current environment for expansion: Splunk architecture, High-level performance, Data onboarding	Remote
Implement	Post Implementation Review	Review of an existing, previously implemented Splunk environment and provide performance feedback and recommendations. • Review and provide Splunk best practice recommendations • Provide recommendations for use case required data source configurations created by Customer	Remote
Use/Adopt	Data Source Review	Review existing data onboarding procedures and index usage within the Splunk environment. Splunk will review Customer data onboarding configurations and procedures and compare to Splunk best practices. This may include identifying issues with: • Splitting of data into individual events and multi-line merge settings • Parsing of date/timestamps • Truncation of long events Splunk will advise on the benefits of Splunk best practice data onboarding, utilizing applications from Splunkbase, and adhering to the Splunk Common Information Model ("CIM") where possible.	Remote

Category	Service Name	Service Descriptions	Location
Use/Adopt	Index and Retention Review	Consultative discussion to define strategy for index definition and data retention. • Advise retention strategy in alignment with Customer audit and compliance requirements. • Advise on time and size-based retention capabilities • Advise on data archiving and restoration recommendations • Advise on access control recommendations	Remote
Plan	Data Readiness	Review data readiness related to Security Premium Solutions, including Enterprise Security, Phantom, and UBA. • Topics may include Common Information Model (CIM) data mapping, technical addons, and implementing data governance strategies.	Remote
Optimize/ Scale	Security Integrations Review	Review and discuss integrations with Security Premium Solutions including Enterprise Security, Phantom, and UBA. • Integrations may include communications between two (2) Splunk premium solutions, or between one (1) Splunk premium solution and a third-party system, such as an external ticketing system • Includes discussion around Threat Intelligence feeds and Splunk best practices	Remote
Optimize/ Scale	Splunk Enterprise Security/UBA Technical Assessment	Discuss Splunk Enterprise Security/UBA performance. • Topics may include capacity planning, improvement of search performance and data ingestion.	Remote
Optimize/ Scale	Upgrade Readiness Assessment	Assess Customer environment to validate it is adequately prepared for a version upgrade • Applies to Splunk Security Premium Solutions including Enterprise Security, Phantom, and UBA. • Includes checks for adequate hardware provision, deprecated features and known issues • Identify possible App compatibility issues • Advise on Splunk best practices for upgrade procedures and workflows • Provide upgrade dependency recommendations and remediation activities required	Remote
Plan	Architecture & Implementation Planning Workshop	Review the customer requirements and produce Architecture Recommendations, list of data sources, and Implementation Plan. Activities: • Review Customer use cases to identify data sources and their associated data on-boarding methods • Document Customer requirements in Architectural Recommendations per Splunk best practices • Identify Technology Add-ons required • Identify Splunk Apps applicable to Customer use cases • Identify data enrichment requirements based on Customer use cases and data sources • Document anticipated tasks, estimated duration, Customer pre-requisites, and dependencies in Implementation Plan	Onsite

Category	Service Name	Service Descriptions	Location
Plan	Enterprise Security Use Case Development Workshop	This workshop is designed to increase the effectiveness of security monitoring and identify ways to improve security posture by configuring security use cases aligned to improving security posture, align business needs, and the prioritization of identified risks. Activities: • Gain mutual understanding of customer priorities and needs used to prioritize use case content • Review use case content to identify candidate use cases o Review Splunk Enterprise Security Use Cases o Review identified priorities and potential use cases o Identify unaddressed use cases and document mapping to Splunk out-of-the-box functionality o Identify data sources required for use case implementation	Onsite
Plan	Phantom Use Case Development Workshop	This workshop is designed to identify and develop SOAR use cases Activities: • Brief health and architectural assessment of current on-premises environment. • Review of current prioritized use case and playbook roadmap • Mutual selection of one (1) use case from the prioritized list	Onsite
Plan	SIEM Replacement Workshop	This workshop builds on the Use Case Development Workshop and is designed to identify the critical steps and timelines of the significant stages in a SIEM replacement project, culminating in a customer specific migration plan. Activities: • Identify use cases to be implemented in customer’s 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 customer specific integration requirements (workflows, ticketing, etc.) • Conduct integration planning for existing Splunk instances already running in the customer’s organization	Onsite
Use/Adopt	Mentoring of Customer Staff	Augment the customer team’s efforts by utilizing Splunk SME’s expertise in a tailored interaction to align to customer business initiatives and use cases. • The assigned SME will arrive onsite and spend one work week (five (5) business days) with the customer’s team to work through challenges and coach the customer team on implementing Splunk best practices to resolve them.	Onsite

ITOA Assigned Expert Services

Category	Service Name	Service Descriptions	Location
General Consultative	Ask an Expert	Consultative session to answer adoption and Splunk best practice questions related to IT Premium Apps (primarily ITSI) • Assist Customer with Splunk best practices approach to adoption	Remote
Plan	Use Case Advisory Discussion	Review of an ITOA use case roadmap executed with the Splunk Customer Success Manager ("CSM")" or Sales team to determine key technical requirements, identify current progress, and outline of next steps. • This may include reviewing a previously executed Prescriptive Value Path (PVP) session and discussing technical next steps, such as requirements and architectures, identifying data sources, discussing Customer specific use case content, and recommended tuning.	Remote

Category	Service Name	Service Descriptions	Location
Use/Adopt	ITSI KPI Identification and Configuration Review for Existing Customers	Assist with reviewing one (1) service and up to ten (10) associated KPIs which may include sourcing, thresholding, and anomaly detection configurations.	Remote
Optimize/ Scale	ITSI KPI Base Search Review	Review and optimization of KPI Base Search.	Remote
Use/Adopt	ServiceNow / Remedy Service Desk Integration Review with ITSI	Review requirements and design of out-of-the-box ServiceNow or Remedy integration.	Remote
Implement	Post ITSI Implementation Review	Elected check-in following the completion of previously implemented Services in order to review performance and provide recommendations. • Review and provide Splunk best practice recommendations for additional use cases implemented by the Customer • Provide recommendations for additional data source configurations created by the Customer	Remote
Plan	ITSI Service Design Review	Review of one (1) service model for the addition of an additional service. • Identify up to ten (10) dependent subservices.	Remote
Use/Adopt	ITSI KPI Adaptive Threshold Review and Anomaly Detection	Review Splunk best practices and procedures on how to determine candidates, settings, and operational requirements. • Review of up to three (3) services	Remote
Optimize/ Scale	ITSI Content Pack Implementation Assessment	Review the Customer’s environment in preparation of one (1) content pack functional capability installation. • Review Customer environment to identify known risks prior to content pack implementation • Configure and tune environment if applicable and if time allows	Remote
Optimize/ Scale	ITSI Technical Assessment	This workshop is designed to assess the Customer’s Splunk ITSI environment in order to identify inefficiencies and optimize ITSI features. • Recommend changes to improve ITSI environment, such as guidance on unused features or released product enhancements • Performance enhancement guidance related to current ITSI architecture configuration • Review potential integration requirements with other common 3rd party tools • Provide guidance on optimization techniques • Review Notable Event Aggregation Policies and provide recommendations for enhancements • Review configuration of thresholds and anomaly detection values	Remote

Category	Service Name	Service Descriptions	Location
Plan	ITSI Service Model Requirements and Implementation Plan	Provide a workshop in order to identify business service and event analytics models for the purpose of increasing business service visibility, reduce event noise and resolution time, and improve operational efficiency. Activities: • ITSI product walkthrough • Identify Technology Add-ons required • Perform architecture review of ITSI environment • Service Identification Workshop to identify services which can be monitored using ITSI and prioritize such services considering business values and Customer's ability to instrument • Service Decomposition Workshop to identify KPIs of the service and sub services and identify data sources required • Services Data Review of data identified in the Service Decomposition Workshop for validation of applicability and identify issues which may require action before utilization • Document proposed tasks, estimated duration, Customer pre-requisites, and dependencies in Implementation Plan Proposal. • Operational requirements workshop to define: ○ Operational workflows ○ Service Analyzer and Deep Dive requirements ○ Integrations ○ Glass tables, reports, dashboards • Review workshop results and provide customer with implementation approach guidance.	Onsite
Plan	Prescriptive Use Case Workshop – Data-Driven Intelligence (Service Insights)	Requirement definition session to define and prioritize the services, KPI's, impact management aspects, thresholding and visualizations. This workshop includes identification, a decomposition session, blueprinting the visualizations by persona data, and a stakeholder presentation to display the proposed service model. Activities: • Engagement kickoff meeting with stakeholders • Use Case Workshop(s) • Persona Visualization workshop • Design Service Model • Stakeholder presentation Pre-Requisites: • Prescriptive Value Path (PVP) assessment and roadmap must be completed by the Splunk Customer Success Manager (CSM) or Sales team prior to executing this workshop. Must have Splunk Enterprise & ITSI installed, configured and operational in Production.	Onsite
Plan	Prescriptive Use Case Workshop – Data-Driven Intelligence (Event Management)	The Event Management Workshop is designed to define objectives associated with leveraging Customer's infrastructure and associated alerts. Activities: • Engagement kickoff meeting with stakeholders • Use Case Workshop(s) • Persona Visualization Workshop • Stakeholder presentation of Event Management Model Pre-Requisites: • Prescriptive Value Path (PVP) assessment and roadmap must be completed by the Splunk Customer Success Manager (CSM) or Sales team prior to executing this workshop. Must have Splunk Enterprise & ITSI installed, configured and operational in Production.	Onsite

Category	Service Name	Service Descriptions	Credits
Plan	Prescriptive Use Case Workshop – Infrastructure Troubleshooting & Monitoring	The Infrastructure Monitoring Workshop is designed to define objectives associated with monitoring Customer's cloud and server environments, and operationalizing the Customer's physical and virtual environments. Customer may select one (1) of the Infrastructure Troubleshooting & Monitoring use cases to be covered during the workshop (i.e. Infrastructure Troubleshooting, Server/OS Monitoring, Cloud Monitoring, Container Monitoring, or Virtualization Troubleshooting, etc...). Activities: • Engagement kickoff meeting with stakeholders • Use Case workshop(s) • Persona Visualization Workshop • Stakeholder presentation of Monitoring Model Pre-Requisites: • Prescriptive Value Path (PVP) assessment / use case roadmap must be completed by the Splunk Customer Success Manager (CSM) or Sales team prior to executing this workshop. Must have Splunk Enterprise & ITSI installed, configured and operational in Production.	Onsite
Plan	IT Ops Modernization Workshop	The IT Ops Modernization Workshop is designed to discover both business and technical requirements that provides customers with the ability to transition from older legacy technologies, consolidate tools, and provide the highest service availability. This workshop will review Customer objectives and requirements for the deployment. Activities: • Review of Customer objectives ○ Consult to determine requirements, success criteria, and priorities ○ Understand tools consolidated and replaced in order to design solution requirements • Architect a Solution ○ Design Splunk best-practice Splunk architecture ○ Identify necessary out-of-the-box and Splunkbase application integrations available for third party/non-Splunk solutions ○ Deliver Splunk ITOPs Modernization replacement solution • Develop a phased deployment plan	Onsite
Use/Adopt	Mentoring of Customer Staff	Augment the customer team's efforts by utilizing Splunk SME's expertise in a tailored interaction to align to customer business initiatives and use cases. • The assigned SME will arrive onsite and spend one work week (five (5) business days) with the customer's team to work through challenges and coach the customer team on implementing Splunk best practices to resolve them.	Onsite

Terms and Conditions

Assigned Expert Services ("AES") are annual subscriptions unless expressly agreed otherwise, and consumption of such subscription can be used only for items specifically listed in this Service Catalog, and not for any other purpose. One (1) AES annual subscription includes AES services for up to twenty-five (25) Business Days (a "Business Day" is one day's work, up to eight (8) hours in that day). The annual subscription only entitles Customer to two (2) Onsite services selections. Each Onsite services selection is limited to no more than five (5) Business Days of work and must be provided in consecutive day increments.

Splunk's ability to deliver these Services is dependent upon the Customer's full and timely cooperation with Splunk, as well as the accuracy and completeness of any information and data the Customer provides to Splunk. Depending on the complexity of Customer's requirements, additional Splunk implementation services may be necessary at additional cost. Splunk reserves the right to make such determination. There are no refunds or credits for any subscription days not used. SPLUNK MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS FACT SHEET. All of the AES engagements are governed by the Configuration and Implementation Services Agreement (**"C&I Services Agreement")** [**http://www.splunk.com/en_us/legal/professional-services-agreement.html**] except for the payment, refund and credit terms identified above shall control for the AES. In this FACT SHEET all mentions of "Customer" shall refer to the party in the applicable C&I Services Agreement or services agreement with Splunk. All references to SOWs in the C&I Services Agreement mean this FACT SHEET. However, the agreement noted above does not apply to the extent there is a separate, mutually signed agreement for or includes Professional Services.