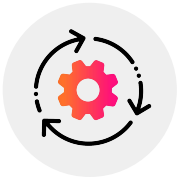
OnDemand Services Catalog – SOAR, Mission Control

Services. What you need. When you need it.

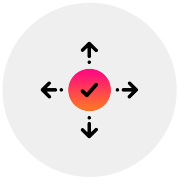
Services Available at Every Stage of Your Splunk Journey

Plan



Implement

Use/Adopt



Optimize/Scale

Tasks: Splunk Intelligence Management			
(Page 2) • Scaling and Architecture Planning • Configuration Guidance • Data Readiness • Use Case / Response Planning • Content Management Planning	*(Page 2)* • Configuration Support • Application Integration Support • Post Implementation Review	*(Page 3)* • Install / Upgrade Planning Guidance • Playbook Assistance • Playbook Design Guidance • Workbook Implementation Assistance • Content Management Assistance	*(Page 4)* • Playbook Review • Integration Feature Request • Security Integrations Review • Upgrade Readiness Assessment • Response Review • Performance Review

Services above do not address your specific need or question?

Leverage Ask an SOAR Expert (General Consultative Service)

Additional OnDemand Splunk Product Catalogs:

- Splunk Core - Enterprise, Splunk Cloud
- Enterprise Security (ES), User Behavior Analytics (UBA)
- Splunk Intelligence Management
- Splunk IT Service Intelligence (ITSI)
- Observability Cloud, Infrastructure Monitoring, Application Performance Monitoring, Log Observer
- Splunk Synthetics
- On-Call

General Consultation & Planning Tasks

Task Name	Task Descriptions	Credits
Ask a SOAR Expert	Conduct a consultative session to answer adoption and Splunk best practice questions related to Splunk SOAR products • Assist Customer with Splunk best practices approach to adoption	5
Scaling and Architecture Planning	Review and advise on how to expand/scale the SOAR environment or select a new SOAR architecture based on performance and reliability requirements. Additional planning tasks may be required to finalize decisions, such as "Data Readiness", "Use Case/Response Planning", "Content Planning", and/or “Security Integrations Review.	10
Configuration Guidance	Guidance for Splunk SOAR configurations related to one (1) of the options below: • Cluster management and expansion • Warm/Standby Configurations • Backing up or restoring Splunk SOAR	5
Data Readiness	Deep-dive data planning session for preparing to get data into SOAR properly, such as outlining requirements for mapping key value pairs (CIM to CEF mapping). Recommend this session after the "Scaling and Architecture Planning" task as it will reference the defined high-level architecture.	10
Use Case / Response Planning	Gather and validate use case requirements for workbooks and playbooks. Recommend this session after the "Scaling and Architecture Planning" task which defines high level architecture requirements of the environment to be considered in use case planning.	5
Content Management Planning	Assist with content management implementation planning by helping define playbook CICD pipeline. For example, GIT repository configuration, continuous development, repo usage, naming, data, etc. The number of topics that can be reviewed in each planning session will depend on the complexity of each topic. Recommend this session after "Scaling and Architecture Planning" which defines high level architecture requirements used in the deep dive content management planning session.	5

Implementation Tasks

Task Name	Task Descriptions	Credits
Configuration Support	Conduct a consultative session to support the adoption of one (1) integration / configuration for SOAR products • Source code management (SCM) configuration • Credential vault configuration • LDAP/SAML2/OpenID configuration • Warm Standby • Backup configuration	5
Application Integration Support	Configuration of one (1) of the following Splunkbase applications or Technical Add-ons aligning to an existing Customer SOAR implementation: • EWS for Exchange, LDAP, SAML configurations, Splunk application installs, ServiceNow (unidirectional), Splunk Remote Search configuration, Event forwarding from Splunk, Chat tools (Slack, teams).	5
Post Implementation Review	Review of an existing, previously implemented Splunk SOAR 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	10

Use/Adopt Tasks

Task Name	Task Descriptions	Credits
Install/Upgrade Planning Guidance	Provide guidance for an upcoming installation or upgrade of one (1) SOAR instance within the Customer environment. Topics may include reviewing steps for installation or upgrade, validating an installation or upgrade plan, outlining considerations, answer questions for clarification, etc.	10
Playbook Assistance	Assistance with troubleshooting, optimizing or developing a playbook or custom function. For new playbook development guidance, the session is typically after the "Playbook Design" task or utilizes an existing community playbook example. New playbook development may include assistance with one (1) playbook up to ten (10) design blocks and provide guidance on how to document and define the playbook and action integrations. For assistance troubleshooting and optimizing a playbook, the session may include guidance on how to test and debug issues with a playbook, customer specific function and action execution using SOAR best practices and techniques	20
Playbook Design Guidance	Assistance documenting the outlined requirements typically gathered in the "Use Case/Response Planning" task into a use case solution design diagram. This includes assistance designing one (1) playbook and provide feedback and guidance on how to design a playbook using inputs, interactions, action, and artifacts process. This may include: • Steps and procedures aligned to standard incident response frameworks • Assistance creating and preparing a visual diagram that outlines the decisions, actions, integrations, and steps to be performed Playbook examples may include: • IP enrichment, Splunk search workflow, Create or update ticket process, Block network address (domain or URL)	10
Workbook Implementation Assistance	Assistance creating a SOAR Workbook that includes requirements typically gathered in the "Use Case/Response Planning" task for SOAR case management. This may include: • Assistance designing one (1) workbook and provide guidance on how to design the workbook using Splunk's case management workflow process utilizing response phases and tasks. • Steps and procedures aligned to standard incident response frameworks • Assistance creating and preparing a visual diagram that outlines the phases, tasks actions and playbooks needed to perform the response tasks • Demonstrate how to build a workbook in a SOAR product Workbook examples may include: • Rare process investigation • Execution investigation • Phishing investigation	20
Content Management Assistance	Assist with content management implementation by helping configure into the SOAR environment. For example, GIT repository configuration, continuous development, repo usage, naming, data	10

Optimize/Scale Tasks

Task Name	Task Descriptions	Credits
Playbook Review	Conduct a consultative session to review one (1) existing playbook and provide improvement feedback. Out of Scope: • Splunk will not make changes to the playbook for Customer	10
Integration Feature Request	Conduct a consultative session to define feature request and gather necessary Customer requirements.	2
Security Integrations Review	Review and discuss integrations with Splunk premium security solutions Enterprise Security (ES), SOAR, and Splunk User Behavior Analytics (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	10
Response Review	Conduct a consultative session to discuss Splunk SOAR response utilization and how to maximize use of the SOAR product. This may include a demo of features, or possible future integrations, or response models related to one (1) of the following topics: • Case management, Threat intelligence, Breach readiness, Vulnerability management	10
Performance Review	Consultative session to discuss Splunk SOAR platform performance. This may include: • Capacity planning • Improvement of platform resources • Action/playbook performance and/or data ingestion	10
Upgrade Readiness Assessment	Assess Customer environment to validate it is adequately prepared for a version upgrade. • Applies to Splunk SOAR products • 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	10

Splunk-Led Tasks

The tasks outlined in the section below are not accessible for customers to initiate directly. They can only be opened by a Splunk employee. If you would like to learn more about these tasks, please reach out to your Splunk account team.

Category	Task Name	Task Descriptions	Credits
Use / Adopt	Technical Use Case Actions	Guidance with technical use case implementation. OnDemand, Splunk employee, and Customer will agree to the technical use case implementation scope based on the credits allocated in the request and may include consultative planning sessions or assistance with use case development topics, such as onboarding priority data sources, forwarder, technical add-on, and product feature configurations, integrations, building searches and dashboards. This task is not available to open in the OnDemand portal and can only be opened by a Splunk employee. *During the working session, Splunk OnDemand Consultant may gain access to your environment to execute specific work to accelerate the completion of a task. Customer will provide verbal consent and access to Splunk, constituting agreement between Splunk and Customer for such access.*	10, 20, or 30
Use / Adopt	Admin Assistance	Guidance with admin technical onboarding & readiness. OnDemand, Splunk employee, and Customer will agree to the technical onboarding & readiness scope based on the credits allocated in the request and may include consultative planning sessions or assistance with topics, such as data onboarding, data management, search best practices, user management, forwarder management, managing apps, Monitoring Console/Cloud Monitoring console, clustering, security and encryption. This task is not available to open in the OnDemand portal and can only be opened by a Splunk employee. *During the working session, Splunk OnDemand Consultant may gain access to your environment to execute specific work to accelerate the completion of a task. Customer will provide verbal consent and access to Splunk, constituting agreement between Splunk and Customer for such access.*	10, 20, or 30

Terms and Conditions

All OnDemand Services are annual subscriptions unless agreed otherwise. OnDemand Service Credits ("Credits") can only be used for items specifically listed in this Service Catalog and not for any other purpose. The number of Credits corresponding to the service items you request will be deducted from your total Credits purchased. Credits are made available on a quarterly basis and are only available for use during the corresponding quarter (Credits expire at the end of the quarter and any unused quarterly Credits do not carry forward, and there are no refunds for Credits not used). Quarters are based on calendar quarters (starting January 1, April 1, July 1, October 1 respectively). When an annual subscription starts during a calendar quarter, Credits available during the first and last partial quarters will be prorated accordingly.

The number of Credits listed for a service item establishes the number of hours of service we will perform for such service item, as follows: Two (2) Credits provides service for up to (2) hours; Five (5) Credits provides service for up to (4) hours; Ten (10) Credits provides service for up to (8) hours; Twenty (20) Credits provides service for up to (16) hours; and Thirty (30) Credits provides service for up to (24) hours. However, if the work required for an item takes longer than the aforementioned designations, Splunk reserves the right to require the use of additional Credits, and Splunk reserves the right to make such determination.

SPLUNK MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS FACT SHEET. These OnDemand Services 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 OnDemand Services. 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.