OnDemand Services Catalog – Enterprise Security (ES) and User Behavior Analytics (UBA)

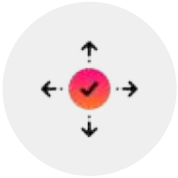
Services. What you need. When you need it.

Services Available at Every Stage of Your Splunk Journey

Plan

Implement

Use/Adopt



Optimize/Scale

Tasks: Enterprise Security (ES), User Behavior Analytics (UBA)			
(Page 2) • Use Case Advisory Discussion • Enterprise Security Framework and Architecture Diagram Creation Assistance • Data Readiness • Security Maturity Guidance	***(Page 3)*** • Post Implementation Review	***(Pages 3-4)*** • Dashboard, Report, Correlation Search Assistance • Getting Started with Security Cloud Suite • Getting Started with Behavioral Analytics (BA) Service • Data Model Review • Enterprise Security Assets and Identities Planning or Assistance • Data Source Review • Index and Retention Review	***(Page 5)*** • Enterprise Security/UBA Technical Assessment • Upgrade Readiness Assessment • Scaling Advisement & Expansion Readiness Assessment • Security Integrations Review

Services above do not address your specific need or question?

Leverage Ask a Security Expert (General Consultative Service)

Additional OnDemand Splunk Product Catalogs:

- Splunk Core - Enterprise, Splunk Cloud
- SOAR, Mission Control
- 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 Security Expert	Consultative session to answer adoption and Splunk best practice questions related to Security Premium Solutions, including Enterprise Security and UBA. • Assist Customer with Splunk best practices approach to adoption	5
Use Case Advisory Discussion	Consultative session to review 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 and UBA data models.	5
Enterprise Security Framework and Architecture Diagram Creation Assistance	Review the ES Splunk environment and advise in creating a detailed diagram specific to security architecture aspects. Architecture aspects include data flows, business architecture, and one (1) Enterprise Security framework diagram, such as the Notable Event, Threat Intelligence, Risk Analysis, and Adaptive response.	5
Data Readiness	Review data readiness related to Security Premium Solutions, including Enterprise Security and UBA. • Topics may include Common Information Model (CIM) data mapping, technical addons, and implementing data governance strategies.	10
Security Maturity Guidance	Consultative session to identify strategic and tactical security monitoring goals and provide guidance on immediate and longer-term next steps. Provides Customer with recommendations on how to meet their immediate and long-term security monitoring objectives, leveraging applicable features within the in-scope products (Enterprise Security, Splunk Security Analytics for AWS, Mission Control). This service may include: • Assets/Identities Review: o Discuss Customer approach to assets/identities, compared to Splunk (and industry) best practices o Advise Customer on how to leverage assets/identities to prioritize security events and investigations • Use Case Advisory Review: o Review current alerting configurations and compare to Customer monitoring goals o Identify use case gaps based on Customer requirements o Overview of risk-based alerting and how it can be leveraged within Customer security monitoring workflow • Case Management Review: o Review Customer's current incident response/case management process o Advise on Splunk best practices for how to leverage Splunk product(s) for case management and response (if applicable) Out of Scope: • This is an advisory session. Implementation/configuration is out of scope for this task Customer Required Information: • Applicable Customer processes and configurations	5

Implementation Tasks

Task Name	Task Descriptions	Credits
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	10

Use/Adopt Tasks

Task Name	Task Descriptions	Credits
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.	5
Enterprise Security Assets and Identities Planning or Assistance	Assistance with Splunk Enterprise Security Assets and Identifications functionality and best practices. This may include one (1) of the following: • Planning Assistance - discuss Enterprise Security Assets and Identities functionality and best practices and provide guidance on identified source(s) to use for asset and identity identification and considerations to factor, such as how to format the data and save the scheduled search to populate the assets and identities • Configuration Assistance - guidance on configuring or tuning Assets and Identities, such as scheduled searches to populate lookup or data model, and processing steps for applicable data source(s), such as, onboarding, normalization, expansion, enrichment, and usage	10
Dashboard, Report, Correlation Search Assistance	Assistance with creating or tuning a dashboard, report, or correlation search. Assistance may include guidance on improving configurations and structure of search queries, xml, reports, dashboards, and visualizations. Customer Required Information: • Associated data exists and has been onboarded and normalized • Acceleration is already enabled for underlying / associated Data Model	5

Use/Adopt Tasks continue on following page

Task Name	Task Descriptions	Credits
Getting Started with Security Cloud Suite	Consultative session to help Customers get started with the Splunk Security Suite. This task focuses on introduction to and leveraging of Splunk best practices for the Splunk Security Suite and may include: An overview of Splunk Security Essentials: • Verify pre-requisite App and platform configuration • Introduction to Use Cases, filtering views, bookmarking and managing content, how to create of custom content, using Analytics Advisor, and using Data Inventory and Data Availability A Use Case advisory review: • Advise on Role Based Access Control (RBAC) for Splunk Core • Advise on Use Cases that can be addressed with Splunk Core from Splunk Security Essentials • Advise on data requirements, which may include firewall, IDS/IPS, Vulnerability Scanner, Windows and Linux Security and Event logs, Antivirus Malware • Walk through the creation of one (1) alert and creation of an associated email action for that alert Case Management: • Introduction to Mission Control • Introduction to Cloud SOAR (if purchased as add-on) Suggest next steps, where to go for additional information, common tips and tricks to quickly get started with Security Cloud Suite. Out of scope: • This task does not include configuration	10
Getting Started with Behavioral Analytics (BA) Service	Consultative session to help Customer with initial configuration of Behavioral Analytics service. This service may include: • Install and configure Splunk Connect for Mission Control • Import Assets and Identities data from Splunk ES on Splunk Cloud Platform into BA service • Configure Windows event logging for proper BA ingestion • Getting data into the BA service • Configuration validation and supportability walkthrough	5
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.	10
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	10

Optimize/Scale Tasks

Task Name	Task Descriptions	Credits
Security Integrations Review	Review and discuss integrations with Security Premium Solutions including Enterprise Security, SOAR, 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	10
Splunk Enterprise Security/UBA Technical Assessment	Discuss Splunk Enterprise Security/UBA performance. • Topics may include capacity planning, improvement of search performance and data ingestion.	10
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 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	10
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	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.