Security Orchestration Automation and Response ("SOAR") Assigned Expert Services Datasheet

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

SOAR Challenges

- Alert Fatigue
- Siloed Security Products
- Lack of Processes
- Tedious and Repetitive Tasks
- Extended MTTD and MTTP

Splunk has you covered with Assigned Expert ("AE")

The mission of the Assigned Expert ("AE") is to help Splunk customers win with proactive planning and advisement. They start with understanding your business goals, requirements, and environment and aligns a set of planned technical activities and prescriptive product-focused roadmaps with the objective to guide successful outcomes.

Key Features	Benefits
Splunk SOAR Architecture Design Review	Lower risk to address business objectives, performance, and scalability
Use Case Management and Playbook Design	Expert guidance to orchestrate and automate response plans
Proactive Risk Assessment and Tune-Up Workshops	Mitigation and reduction of environment risks
Customer Environment Familiarity	A single resource to deliver services vs. variable resourcing
Tailored Technical Guidance	Optimization/augmentation of customer resources through Splunk best practices
Provides Splunk Project Technical Oversight and Guidance	Increased efficiencies and continued assistance throughout the year to reduce risk

Offering Benefit

- Orchestrate security responses across your technology stack
- Leverage best practices to build reusable automation
- Enable analysts to focus on advanced investigations
- Reduce Mean Time to Respond (MTTR)
- Leverage I2A2 methodology

.

Delivery Process

Your journey starts with our delivery framework, which includes a set of activities with detailed outputs and coalesces the information into a prescriptive product-focused roadmaps with the objective to guide successful outcomes.

SOAR Assigned Expert

- Splunk SOAR Accredited Specialist
- Product Feature & Capability Expertise
- Technical advisory; product solutioning

Bringing value to you organization:

- Product specialist with an advisory focus on the capabilities and features of SOAR.
- Knowledgeable in Splunk features, functions, and operations.
- Skilled technical expert for planning, implementation, and optimization of business and technical use cases.

Technical Ability

A SOAR AE is a certified Splunk Consultant with additional domain knowledge in one or more of the Splunk SOAR suite products. They bring product knowledge and real-world experience to strengthen security initiatives spanning multiple business verticals and use cases.

SOAR Product Questions

- What are the best practices for SOAR playbook development?
- How to size and tune my SOAR environment?
- How to develop SOAR apps?
- How to navigate the SOAR journey: from use case, to design, to playbook?
- How to integrate SOAR playbooks with 3rd party apps?
- How to update my notables from SOAR?

Tailored Technical Guidance

An assigned expert works regularly with your team, learning your environment to provide guidance tailored to address your organizational goals and business objectives. They can assist with tactical issues like troubleshooting and configuration, or focus on more strategic issues like architecture, design, and integration. One of an AE's primary goals is to verify that you understand not just the outcome and direction, but the why behind it.

AE Availability

AEs proactively share technical knowledge through strategic and operational planning sessions, and deliver services aligned to their expertise in accordance with the terms and conditions, as outlined below. Splunk may revise and update these services from time to time without notice.

Direct access to the applicable AE shall be made through regularly scheduled remote sessions, on-site visits, or ad hoc remote requests with best effort response within 48 hours. AE access is limited to local business hours in the region where the resource is located unless otherwise agreed upon.

If required for your environment an AE is available with a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance as a "Cleared AE".

Product Focus

SOAR AE service spans a broad range of technical activities to enable the adoption of features and functionality for Splunk SOAR with a focus of driving business goals and objectives. Activities commonly include the following items.

SOAR

Specialist Activities	Features
· Build Playbook/Customer Specific Function · Playbook Optimization · Debug Playbook · Architecture Planning · Configuration Guidance · Data Readiness · Response Planning · Content Planning · Application Integration Assistance · Performance Review · Upgrade Readiness Assessment · Integration Feature Request · Scaling Advisement & Expansion Readiness Assessment	· Notable Events Forwarding · Risk Based Alerting · Threat Intelligence Framework · Workbook Actions Design

Resilience, let's build it together

Splunk Customer Success offers end-to-end success capabilities for each step of your resilience journey to accelerate time to value, optimize your solutions and discover new capabilities. We offer professional services, education and training, success management and technical support, surrounding you with the expertise, guidance and self-service success resources needed to drive the right outcomes for your business. For more information contact your Splunk account team or email us at sales@splunk.com.

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 datasheet, and not for any other purpose. AES annual subscription is available in two levels of dedication depending on the scale and complexity of the Customer. AES includes Customer shared direct access to AES for up to an average of eight (8) hours per week for "quarter time" or sixteen (16) hours per week for "half time" which is the level of dedication purchased. Unless otherwise mutually agreed to in writing, AES will be delivered remotely.

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, Splunk AE 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. Additionally, 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 DATASHEET. 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 Datasheet 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 Datasheet. However, the agreement noted above does not apply to the extent there is a separate, mutually signed agreement for or includes Professional Services.

Dedication Level and Availability:

The annual subscription entitles Customer to the following:

- Standard AE: Customer is entitled to two (2) on-site services selections. Each on-site visit will be for a maximum duration of 5 consecutive business days, unless mutually agreed to between the parties.
- Cleared AE: Customer is entitled to up to an average of 50% of dedicated hours on-site at customer location or local Sensitive Compartmented Information Facility (SCIF). Each on-site visit will be for a maximum duration of 5 consecutive business days, unless mutually agreed to between the parties.

AEs proactively shares technical knowledge through strategic and operational planning sessions and deliver services aligned to their expertise, in accordance with the terms and conditions, as outlined above. Splunk may revise and update these services from time to time without notice. AEs assists multiple customers during local business hours. Direct access to the applicable AE shall be made through regularly scheduled remote sessions, on-site visits, or ad hoc remote requests with best effort response within 48 hours. AEs access is limited to local business hours 8:00 am to 5:00 pm Monday through Friday in the region where the AE is located unless otherwise agreed upon. AE access is not available during local holidays, weekends, and planned time off. For any immediate requests while the AE is out of the office during a normal working day, Customer may open an OnDemand Services request if they are entitled.

Availability of non-English and cleared assistance is based on Splunk resource availability and may not be available in all regions.