Security Assigned Expert Services Datasheet

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

Security Challenges

- Reduce risks
- Security, Safety and Compliance
- Protect Intellectual Property and Brand
- Monitor and Detect Threats
- Enterprise Visibility
- Cost, Feasibility and Scale

Offering Benefit

- Work with an expert to tailor detections to your environment
- Alignment of Enterprise Security (ES) capabilities to organizational goals
- A security expert familiar with your data, org structure, and requirements
- Understand your security posture

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.

Security Assigned Expert ("AE")

- Splunk Security Accredited Specialists
- 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 the Splunk Security Suite.
- Knowledgeable in Splunk features, functions, and operations.
- Skilled technical expert for planning, implementation, and optimization of your business and technical use cases.

Security Program Facets

Splunk can assist you with technical adoption and use of Splunk security products for a variety of security business use cases:

Business Use Cases	Definition
Security Operations	One or many program facets of security operations (e.g., SOC) Deep analysis and investigation
Forensics	Deep analysis and investigation
Threat Hunting	Hunting for IOCs, APTs, and TTPs
DevSecOps	Secure coding, management, and software development life cycling
Insider Threat	Internal threats from employee, service, or partner organizations
Threat Intelligence	Collection, integration, and management of IOCs/IOAs
Risk Management	Assessment of threat likelihood and impacts to manage risk
Vulnerability Management	Identification and dissemination of threats and exploits
Physical Ops	Physical security environment; badge readers, camaras, & IoT
Administration	Change, config, and system management
Detection Engineering	Security engineering of operational technologies and capabilities
Governance	Policy and process, inventory, and accountability
Compliance	Compliance policies, regulations, controls, and requirements
Cloud Security	Cloud provider security products, services, and capabilities
Data Onboarding	Assist in bringing new data into Splunk and aligning it ot the CIM

Technical Ability

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

Splunk Security Product Questions

- What operational, security monitoring, and investigative opportunities does my data provide?
- How can I efficiently build alerts and tune my searches?
- How do product features integrate into my larger security processes?
- How can my team accelerate their development and become product experts?

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.

Specialist Product Focus

The Security AE service spans a broad range of technical activities to enable the adoption of features and functionality for Enterprise Security, Behavioral Analytics, Intelligence Management, and Security Essentials with a focus of driving business goals and objectives. Activities may include the following items (listed to the right).

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".

Enterprise Security

Specialist Activities	Features
· Dashboard Optimization · Data Readiness Review · Data Onboarding and Hygiene · Data Model Optimization · Data Normalization and CIM Mapping · Incident Review Customization · Mitre Framework Visualization · Risk-based Alerting Enablement & Tuning · Search Optimization · Targeted Workshops & Discussions · Threat Hunting and SPL Best Practices · Threat Intelligence Ingestion · Upgrade Readiness · Use Case Development · Use Case Planning	· Adaptive Response Actions · Assets & Identities · Machine Learning Toolkit · Notable Events Risk Based Alerting · Splunk Technical Add-Ons · Threat Intelligence Framework · Workflow Actions

User Behavioral Analytics

Specialist Activities	Features
· Architecture Planning · Customize UBA · Data Source Validation · ES Integrations · Features & Functions · Threat & Anomaly Tuning	· Anomaly detections · Machine Learning · UBA Monitoring

Intelligence Management

Specialist Activities	Features
· Data Readiness · ES Integration · Features & Functions · Indicators & KV Stores · Indicator Tagging · Intelligence Feeds · IOC & IOA Enrichment · Mitre Integration · Threat Intelligence Tuning	· Intel Workflows · Intelligence Sources · Managed Connectors · TruSTAR Unified App **Enclaves** · Custom Enclave · Intel Source · Sharing Group · Splunk Threat Activity · Workflow Destination

Security Essentials

Generalist Discussion
· Data inventory · Data Journey Tips · MITRE ATT&CK Content · Use Case Recommendations

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.