Sumo Logic Professional Services

sumo logic

Cloud SIEM for Service Providers

Overview

Sumo Logic's Professional Services Cloud SIEM for Service Providers ("Cloud SIEM for Service Providers") is designed for Service Providers new to Sumo Logic. Sumo Logic shall work with the Service Provider to deploy Cloud SIEM on a single tenant, as set forth below, while also enabling Service Provider personnel to manage and use Cloud SIEM as a Service Provider to support their clients. The Cloud SIEM for Service Providers is to be delivered in partnership with the Service Provider via working sessions, during which configuration and enablement activities are performed. The specific activities to be performed by Sumo Logic and the Service Provider are set forth below.

Activities

Sumo Logic shall assist the Service Provider with the following activities, using an iterative approach that leverages Sumo Logic's best practices and techniques:

Topic	Sumo Logic Activities	Service Provider Activities
Service Provider Orientation	• Conduct project kickoff. • Review success criteria and desired outcomes. • Provide engagement overview and timelines.	• Participate in project kickoff. • Create accounts in the Sumo Logic Partner and Training Portals. • Complete Sumo Logic Cloud SIEM self-paced courses.
Discovery and Design	• Discuss collection strategies. • Review data sources and collection options with specific recommendations. • Provide recommended design for metadata. • Discuss and advise on Service Provider targeted use cases. • Provide guidance on Service Provide multi-organization authentication strategy.	• Identify data sources to be included in the scope of the engagement, limited to eight (8) distinct sources. • Provide input and validate metadata design. • Provide use cases for the design of custom rules. • Configure Role Based Action Control ("RBAC"). • Develop a multi-organization authentication strategy.

Topic	Sumo Logic Activities	Service Provider Activities
Data Onboarding	• Conduct working sessions to provide configuration guidance for the collection of up to eight (8) distinct sources. • Conduct working sessions to provide guidance and enablement for the design and configuration of data partitions. • Conduct working sessions to provide guidance and enablement for data normalization and data parsing, including the configuration of up to three (3) custom parsers.	• Attend and participate in working sessions. • Configure and deploy collectors for the ingestion of data sources within the Service Provider environment. • Configure data partitions. • Validate configuration of collectors, partitions and parsers.
Content Development	• Implement standard Cloud SIEM dashboards, designed to provide details on records, signals and insights. • Conduct working sessions to provide enablement and guidance on how to tune Cloud SIEM detection rules. • Create up to a total of five (5) Cloud SIEM custom rules and/or Automation Service action nodes. • Integrations within Automation Service action nodes shall be limited to Cloud SIEM Certified Integrations • Review available APIs and terraform modules. • Provide API and terraform examples for managing multiple organizations.	• Cloud SIEM administrators attend working sessions related to the tuning of Cloud SIEM detection rules. • Provide desired use cases for Cloud SIEM rules and/or Automation Service action nodes within six (6) weeks of project kickoff. • Validate configuration of dashboards, rules and action nodes.
Knowledge Transfer & Project Closeout	• Conduct knowledge transfer session and project closeout session. • Provide the following project documentation: source configurations, tuning recommendations, list of parsers, list of dashboards, list of queries, and recording of knowledge transfer session.	• Cloud SIEM administrators and end users attend and participate in the knowledge transfer and project closeout session.

Expert Services Activities

Following completion of the Deployment Activities set forth above, Sumo Logic will provide up to five (5) hours of expert services ("Expert Services") per month for six (6) months. Expert Services are to provide guidance and configuration assistance to the Service Provider. The Expert Services hours must be used by the Service Provider monthly and any unused hours remaining at the end of each month will expire, without refund, adjustments, or credits. For the avoidance of doubt, the Expert Services hours cannot be moved from one month to be consumed in a different month.

Timeline

The Cloud SIEM for Service Providers Deployment Activities are intended to be executed in a continuous motion and completed within twelve (12) weeks of project kickoff. If the project extends beyond twelve (12) weeks, and the delay is due to a lack of Service Provider participation, Sumo Logic may require a paid project change modification.

Assumptions

- Cloud SIEM shall be deployed for one Sumo Logic tenant.
- Service Provider shall provide timely access to personnel required for Sumo Logic to perform its obligations hereunder (including subject matter experts familiar with security, compliance, and operational requirements of the Service Provider).
- Service Provider personnel to timely complete all recommended Sumo Logic self-paced training prior to participating in any design and/or configuration activities.
- Assistance by Sumo Logic for collection of data sources is limited solely to sources documented within the Sumo Logic Application Catalog.
- Sumo Logic will not access and/or perform configuration work within Service Providers' non-Sumo Logic environments and/or systems. For clarity, Service Provider, and its client as applicable, are responsible for the installation and configuration of collectors.
- SSO functionality requires a Sumo Logic Enterprise Package subscription. For the avoidance of doubt, if the Service Provider does not have an Enterprise Package subscription SSO shall not be enabled.
- SSO functionality shall require the Customer to use an identity provider supported by Sumo Logic.
- Professional Services shall be performed exclusively on a remote basis.

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
855 Main Street, Redwood City, CA 94603

www.sumologic.com