

Sumo Logic Professional Services

Cloud SIEM Upgrade Quickstart

Overview

Sumo Logic's Professional Services Cloud SIEM Upgrade Quickstart ("Cloud SIEM Upgrade Quickstart") is designed for existing customers that have already deployed the Sumo Logic platform and are currently ingesting the required log data for a Cloud SIEM deployment. Sumo Logic shall work with Customer to deploy Cloud SIEM using existing log data sources within the Sumo Logic platform, while also enabling Customer personnel to effectively manage and use Cloud SIEM, as set forth below. The Cloud SIEM Upgrade Quickstart is to be delivered in partnership with Customer via working sessions, during which configuration and enablement activities are performed.

Activities

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

Topic	Sumo Logic Activities	Customer Activities
Discovery and Design	<ul style="list-style-type: none">• Conduct project kickoff.• Discuss and advise on Customer use cases by conducting interviews with Customer.	<ul style="list-style-type: none">• Participate in project kickoff.• Provide use cases for the design of custom rules.
Data Onboarding	<ul style="list-style-type: none">• Conduct working sessions to provide guidance and enablement for data normalization and data parsing, including the configuration of up to three (3) custom parsers.	<ul style="list-style-type: none">• Attend and participate in working sessions.• Validate data normalization and data parsing.

Topic	Sumo Logic Activities	Customer Activities
Content Development	<ul style="list-style-type: none"> 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 ten (10) Cloud SIEM custom rules and/or Automation Service action nodes. <ul style="list-style-type: none"> - Integrations within Automation Service action nodes shall be limited to Cloud SIEM Certified Integrations. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Conduct knowledge transfer session and project closeout session. Provide project documentation, including: source configurations, tuning recommendations, list of parsers, list of dashboards, and list of queries, and recording of knowledge transfer session. 	<ul style="list-style-type: none"> Cloud SIEM administrators and end users attend and participate in the knowledge transfer & project closeout session.

Timeline

The Cloud SIEM Upgrade Quickstart is expected to be executed in a continuous motion and completed within six (6) to ten (10) weeks of project kickoff. If the project extends beyond that timeline, and the delays are due to a lack of Customer participation, Sumo Logic may require a paid project change modification.

Assumptions

- Cloud SIEM shall be deployed for one Sumo Logic Organization (“Sumo Org”).
- Customer shall provide timely access to Customer personnel required for Sumo Logic to perform its obligations hereunder (including subject matter experts familiar with security, compliance, and operational requirements of Customer).
- Customer personnel to timely complete all recommended Sumo Logic self-paced training, prior to participating in any design and/or configuration activities.
- This deployment shall use existing data sources already configured for collection within the Sumo Logic platform. The collection of additional data sources is not included in the scope of the Cloud SIEM Upgrade Quickstart.
- Sumo Logic shall not access and/or perform configuration work within Customer’s non-Sumo Logic environments and/or systems. For clarity, Customer is responsible for the installation and configuration of collectors.
- Professional Services shall be performed exclusively on a remote basis.

