Sumo Logic Professional Services

sumo logic

Cloud SOAR Quickstart with One Playbook

Effective Date: August 15, 2023

Overview

Sumo Logic's Professional Services Cloud SOAR Quickstart with One Playbook ("Cloud SOAR Quickstart") is designed to deploy incident response, orchestration and automation, and threat intelligence management capabilities within Sumo Logic Cloud SOAR ("Cloud SOAR"), as set forth below. The Cloud SOAR 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	• Conduct project kickoff. • Review incident triggers, such as alerts and signals, for playbook execution. • Gather requirements and document design for one (1) playbook based on use cases and workflow design provided by Customer. • The playbook shall be limited to a maximum of twenty (20) actions, utilizing out of the box integrations.	• Participate in project kickoff. • Provide use case for the design of one (1) playbook. • Provide a documented workflow design to be implemented within the playbook, including selection of technologies and actions to orchestrate. • Identify sources of applicable alerts and signals. • Ensure SOC Subject Matter Experts (SMEs) are available to work with Sumo Logic staff.
Technical Onboarding	• Configure Role Based Access Control ("RBAC") and Single Sign On ("SSO") within Cloud SOAR. • Conduct working session(s) to provide guidance for the installation and registration of the automation bridge. • Deploy out-of-the-box dashboards and reports.	• Provide SAML identity provider information for SSO configuration. • Provide design guidance for RBAC configuration. • Allocate a virtual machine for the installation of the automation bridge. • Provide API credentials for the configuration of connectors with external technologies to be used in the Playbook.

Topic	Sumo Logic Activities	Customer Activities
Playbook Development	• Conduct working sessions to provide guidance and enablement for playbook deployment. • Create and implement one (1) playbook, as selected and designed during Discovery and Design. • Create up to two (2) custom actions for an existing, out of the box integration.	• Attend working sessions to provide configuration input and validate the development of the playbook. • Conduct operational testing and validation of the playbook.
Knowledge Transfer & Project Closeout	• Conduct knowledge transfer and provide documentation for the one (1) playbook.	• Cloud SOAR administrators, SOC analysts and SOC engineers attend the knowledge transfer session.
Enablement	• Conduct up to three (3) 2-hour knowledge transfer and enablement sessions for administrators, SOC analysts and SOC engineers.	• Cloud SOAR administrators, SOC analysts and SOC engineers attend knowledge transfer and enablement sessions.

Timeline

The Cloud SOAR Quickstart is expected to be executed in a continuous motion and completed within eight (8) to twelve (12) weeks of project kickoff. If the project extends beyond the timeline, and the delays are due to a lack of Customer participation, Sumo Logic may require a paid project change modification.

Assumptions

- Cloud SOAR shall be deployed for one Sumo Logic Organization ("Sumo Org").
- Customer personnel shall complete a Cloud SOAR discovery questionnaire prior to project kickoff.
- 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.
- Customer shall provide a virtual machine(s), using a Sumo Logic supported operating system, for the Sumo Logic Automation Bridge.
- Sumo Logic shall not access and/or perform configuration work within Customer's non-Sumo Logic environments and/or systems.
- 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