

# Sumo Logic Professional Services Cloud SIEM Quickstart

## Overview

Sumo Logic’s Professional Services Cloud SIEM Quickstart (“Cloud SIEM Quickstart”) is designed for customers new to Sumo Logic. Sumo Logic shall work with Customer to deploy Cloud SIEM, while also enabling Customer personnel to effectively manage and use Cloud SIEM, as set forth below. The Cloud SIEM 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
<b>Discovery and Design</b>	<ul style="list-style-type: none"> <li>• Conduct project kickoff.</li> <li>• Review data sources and collection options with specific recommendations.</li> <li>• Provide recommended design for metadata.</li> <li>• Discuss and advise on Customer use cases by conducting interviews with Customer.</li> <li>• Provide design and configuration guidance for Role Based Access Control (“RBAC”) and Single Sign On (“SSO”).</li> </ul>	<ul style="list-style-type: none"> <li>• Participate in project kickoff.</li> <li>• Identify data sources to be included in the scope of the engagement, limited to eight (8) distinct sources.</li> <li>• Provide input and validate metadata design.</li> <li>• Provide use cases for the design of custom rules.</li> <li>• Configure RBAC and SSO.</li> </ul>
<b>Data Onboarding</b>	<ul style="list-style-type: none"> <li>• Conduct working sessions to provide configuration guidance for the collection of up to eight (8) distinct sources.</li> <li>• Conduct working sessions to provide guidance and enablement for the design and configuration of data partitions.</li> <li>• Conduct working sessions to provide guidance and enablement for data normalization and data parsing, including the configuration of up to three (3) custom parsers.</li> </ul>	<ul style="list-style-type: none"> <li>• Attend and participate in working sessions.</li> <li>• Configure and deploy collectors for the ingestion of data sources within Customer environment.</li> <li>• Configure data partitions.</li> <li>• Validate configuration of collectors, partitions and parsers.</li> </ul>

Topic	Sumo Logic Activities	Customer Activities
<b>Content Development</b>	<ul style="list-style-type: none"> <li>Implement standard Cloud SIEM dashboards, designed to provide details on records, signals and insights.</li> <li>Conduct working sessions to provide enablement and guidance on how to tune Cloud SIEM detection rules.</li> <li>Create up to a total of ten (10) Cloud SIEM custom rules and/or Automation Service action nodes.                             <ul style="list-style-type: none"> <li>- Integrations within Automation Service action nodes shall be limited to Cloud SIEM Certified Integrations.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Cloud SIEM administrators attend working sessions related to the tuning of Cloud SIEM detection rules.</li> <li>Provide desired use cases for Cloud SIEM rules and/or Automation Service action nodes within six (6) weeks of project kickoff.</li> <li>Validate configuration of dashboards, rules and action nodes.</li> </ul>
<b>Knowledge Transfer &amp; Project Closeout</b>	<ul style="list-style-type: none"> <li>Conduct knowledge transfer session and project closeout session.</li> <li>Provide project documentation, including: source configurations, tuning recommendations, list of parsers, list of dashboards, and list of queries, and recording of knowledge transfer session.</li> </ul>	<ul style="list-style-type: none"> <li>Cloud SIEM administrators and end users attend and participate in the knowledge transfer &amp; project closeout session.</li> </ul>

## Timeline

The Cloud SIEM 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 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.
- Assistance by Sumo Logic for collection of data sources is limited solely to sources documented within the Sumo Logic Application Catalog.
- 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.
- SSO functionality requires a Sumo Logic Enterprise Package subscription. For the avoidance of doubt, if Customer 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.

