Cloud SIEM Enterprise

Learn about Cloud SIEM Enterprise (CSE).

Cloud SIEM Enterprise (CSE) is a cloud-based SIEM that provides the following functionality:

- Collection of log and event data from your infrastructure and applications, on-premise and in-cloud.
- Correlation of the collected data to winnow down the volume of info you need to sift through to investigate issues.
- A rich interface that analysts and admins can use to investigate security issues and administer CSE itself.
- Integration with the Sumo Logic platform.

- CSE Rules

Learn about CSE rules, rules syntax, and how to write rules.

- About CSE Rules
- Write a Match Rule
- Write a Threshold Rule
- Write a Chain Rule
- CSE Rules Syntax
- CSE Built-In Rules

- CSE Schema

Learn about CSE Schema v3, schema attributes, and schema models

- Schema Attributes
- Attributes You Can Map to Records
CSE Record Types

Username and Hostname Normalization

**CSE Sensors**

CSE Sensors collect log and event data from your infrastructure and applications.

- Windows Sensor Overview
- Windows Sensor Installation
- Windows Sensor Configuration Settings
- Windows Sensor Troubleshooting
- Network Sensor Deployment Guide
- Network Sensor Troubleshooting
- Cloud Sensor Guide
- Log Sensor Troubleshooting

**Integrations**

- Insight Enrichment Server
- Send Data from Sumo Logic to CSE

**Match Lists**

Learn about creating a Match list and their usage in the rules.

- Create a Match List
- Match Fields Reference
- Standard Match Lists