sumo logic | Continuous Intelligence Platform™

SOLUTIONS BRIEF

# Cloud SOAR

Modernize your SOC with progressive automation, orchestration and insightful decision-making

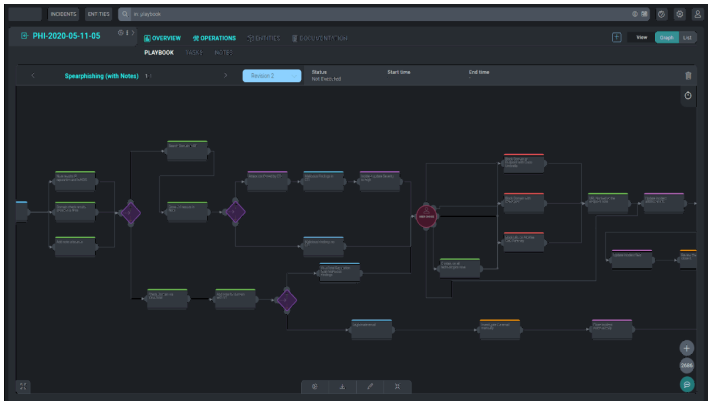
Sumo Logic Cloud SOAR improves SOC productivity, increases visibility, enhances incident response and helps security professionals make insightful decisions

## Accelerating SecOps processes

Cyber security is no longer a human-scale problem. To efficiently combat the evolving threat landscape, SOC teams must unify people, process and technology.

Sumo Logic paves the way for modernized security operations with cutting-edge technologies, such as Cloud SOAR, that provide customers with a comprehensive cloud-native security solution.

Driven by the mission for constant innovation, Sumo Logic leverages modern applications, architectures and cloud-native infrastructure to help SOC teams achieve greater levels of cyber resilience.



## Solution Benefits

**Minimize response time:** Improves your standard operating procedures for fast response by using playbooks and Supervised Active Intelligence to suggest relevant processes for specific use cases.

**Focus on real threats:** Reduces false positives, provides accurate alert enrichment, deduplicates similar incidents and automates time-consuming tasks.

**Measure success and improve collaboration:** Makes it easy to manage the escalation process and enables analysts to work simultaneously on incidents. Provides detailed incident reports with related IOCs, timeline and corrective actions.

**Easily orchestrate your tools:** Integrates with hundreds of technologies with our Open Integration Framework and allows you to create custom integrations with almost no coding experience required.

## Make the most of automation with Open Integration Framework

Using security automation is easy. Sumo Logic's Open Integration Framework defines all integrations at the action level, not as one monolithic file. It enables users with limited coding experience to easily add actions to existing integrations without the need to modify existing code. The execution of each integration is performed in a unique Docker container and easily configured from within the integration file, providing additional security and eliminating the risk of conflicting libraries.

The Sumo Logic team develops the connectors you need, but you can easily develop integrations having access to the API code.

## Get automated SOPs up and running fast with App Central.

In app central you can find playbooks, integrations and use cases to easily start your own processes. You can select playbooks you would like to use as a starting point for building your standard operating procedures changing whatever you want, including integrations.

## Advanced incident management

The Cloud SOAR advanced Triage allows you to handle suspicious events that require deeper analysis outside the context of an incident. This is the key differentiator between Sumo Logic and other SOAR vendors as it allows you to handle the last mile of inside and outside the context of the incident.

Advanced Triage helps reduce the number of false positives and other red flags raised by an elevated number of suspicious events that have to be inspected.

### Advanced triage

- Automated investigation of relevant IOCs and re-classification of incidents, based on the results of the Triage
- Specific cyber and non-cyber info-gathering processes (e.g., financial transactions, credit cards, admin logins and IoT network activity)
- Significantly reduced false positives and duplicated events

### Supervised active intelligence & SecOps dashboard

- Analysis of alarms before they are converted into incidents
- Tasks and user choices assigned are ordered by time and prioritization in the SecOps dashboard
- Cloud SOAR offers playbook recommendations, providing the most suitable ways to respond to incidents

## Case management and War Room

### Manage all aspects of the incident case management

We provide in-depth information in hundreds customizable case management fields.

### War room

War Room provides a complete and detailed picture of a specific incident process in one single page and analysts can easily view everything that happened in a specific incident in chronological order.

### Segregation of duties with highly granular RBAC

Cloud SOAR offers granular role-based access control (RBAC). The profiles can be defined and customized depending on the particular role at hand, both for general and incident profiles.

### Data breach regulations

Case management is a relevant and sensitive component as data breaches are subject to control by the authorities, and there are regulations that highlight the importance of the evidence that is acquired and managed.

## Customizable dashboards, reports, and KPIs

### Dashboards and KPIs

Our dashboards make it easy to gain an overview of the platform, and you can also easily customize dashboards to include the data relevant to your workflow processes, job functions, timeframes and characteristics.

### Fast and customizable reports

Cloud SOAR provides configurable reports, enabling you to build customizable KPI reports in your own template, generate reports in different formats, as well as access advanced reporting with visual dashboards.

## Excellent support

Before implementing a SOAR solution, the first thing to do is to determine the type of operational processes that are suited for your organization and identify which technologies need to be orchestrated. Sumo Logic is here to partner with you to share a proven knowledge base of numerous articles and playbooks to fully leverage the Cloud SOAR capabilities. You are not alone; we are here for direct support, as well as through our partners, to empower you to tap into the full power of the solution.

## About Sumo Logic

Sumo Logic is the pioneer in continuous intelligence, a new category of software, which enables organizations of all sizes to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,100 customers rely on Sumo Logic to build, run, and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy. For more information, visit www.sumologic.com.

sumo

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

**www.sumologic.com**