ManageEngine
Log360 Cloud

DATASHEET

Security Orchestration, Automation, and Response (SOAR)

Native engine and mature workflows

Modern SOC teams are equipped with detection tools and handle a high volume of alerts and detections, yet triage fatigue leads to delayed responses. Investigation and remediation steps are often scattered across multiple platforms, slowing down containment efforts.

Analysts move between SIEM, EDR, identity, cloud, and ticketing systems to gather context and execute actions, repeating the same enrichment and remediation steps for every critical alert instead of focusing on deeper threat analysis.

Log360 Cloud's native SOAR capability closes this gap by transforming isolated response actions into orchestrated, end-to-end workflows that investigate, decide, and remediate threats in a centralized platform.

Native SOAR in Log360 Cloud

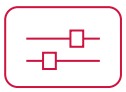
Log360 Cloud SOAR is built into the SIEM, not bolted on. It leverages a native orchestration engine to automate investigation and response across security tools, identity platforms, endpoints, and cloud services.

Key capabilities at a glance

60+ default playbooks with a visual playbook builder

15+ marketplace integrations and 400+ supported actions

Low-code automation with visual flow controls



Custom functions using Python and Deluge

Single playbook for investigation, decision-making, remediation, and notification

How it works

SOAR Workflow

01

Trigger

Alerts, detections, or incidents generated by Log360 SIEM feed into the SOAR engine. Analysts can manually trigger the playbooks or automate them.

Investigation

Alerts are enriched with threat intelligence, endpoint context, identity data, and historical behavior patterns. This provides analysts with complete situational context before making response decisions.

02

03

Decision Logic

Branching conditions evaluate severity, risk score, and confidence level. Parallel task execution ensures faster triage without waiting for sequential steps.

Response and Containment

Actions such as disabling users, isolating endpoints, blocking IPs or domains, and removing persistence are executed. Stakeholders are notified immediately to maintain visibility and coordination.

04

05

Closure and Audit

Every action is documented with a detailed response trail for traceability. This ensures compliance reporting and simplifies post-incident reviews.

Core components of SOAR in Log360 Cloud

01 Native orchestration engine

- Built on Zoho Qntrl Circuit
- Enterprise-grade workflow orchestration
- Visual, drag-and-drop playbook design
- Full state management from start to end

02 Logic and flow control

- Branch, parallel, wait, batch, and termination states
- Enables conditional execution and decision-making
- Supports simultaneous investigation steps for faster outcomes

03 Integrations and actions

- Pre-built integrations with:
  - Endpoint security platforms
  - Identity providers
  - Cloud services
  - Threat intelligence sources

04 Custom functions

- Extend playbooks with Python or Deluge
- Handle unique logic, parsing, or business rules
- Reusable sub-playbooks for consistency

05 Playbook library

- Ready-to-use response templates
- Fully customizable and version-controlled
- Faster deployment with standardized workflows

Use cases and challenges addressed

Use cases & challenges addressed	How SOAR helps
Triage fatigue	Automates enrichment across endpoint, identity, and threat intelligence sources Runs investigation steps in parallel and reduces analyst effort for repetitive tasks.
Fragmented response workflows	Orchestrates actions across multiple tools from a single playbook. Executes coordinated containment steps and ensures consistent response every time.
Delayed containment	Initiates immediate containment actions based on structured investigations to improve mean time to respond (MTTR).
Inconsistent incident handling	Enforces standardized, repeatable playbooks. Captures every action for audit readiness and strengthens SOC maturity over time.

Use case example

This usecase demonstrates the different aspects of a playbook broken down into:

Enrichment

Investigation analysis

Response

Okta Identity Compromise Response

An Okta identity compromise occurs when an attacker gains access to a user's account often through stolen credentials, MFA fatigue attacks, phishing, or session hijacking. Once suspicious identity behavior is detected, the playbook automatically performs structured enrichment, risk validation, and coordinated containment to prevent further unauthorized access.

1. Enrichment

User Enrichment

- Check privileged group membership and critical app access.
- Detect newly enrolled MFA factors.

IP Enrichment

- Check IP/ASN reputation and prior related alerts.

Login History Analysis

- Identify new IP, ASN, location, or device anomalies.

2. Investigation (Decision Block – True Positive Indicators)

Escalate as True Positive if:

- Privileged user shows new location/ device login.
- Suspicious IP reputation score.
- MFA factor added within 24 hours.
- Behavioral anomaly detected (MFA bypass, credential misuse).

3. Response

- Create incident and document anomaly indicators.
- Enforce password reset.
- Remove newly enrolled MFA factor.
- Block malicious IP/ASN.
- Terminate active Okta sessions.

ManageEngine
Log360 Cloud

About Log360 Cloud

ManageEngine Log360 Cloud, a unified cloud SIEM solution with integrated CASB capabilities, helps enterprises secure their network from cyberattacks. With its security analytics, threat intelligence and incident management capabilities, Log360 Cloud helps security analysts spot, prioritize and resolve threats in both on-premises and cloud environments. The solution is highly scalable and helps drive down infrastructure and storage costs.

For more information about Log360 Cloud, visit www.manageengine.com/cloud-siem/.

Sign-up for free

Get a personalized walk-through