sumo logic | Continuous Intelligence Platform™

Key considerations when implementing a SOAR

SOAR makes humans more efficient

The role of automation in SOAR is to ease the burden of cybersecurity organizations by automating low-value repetitive behavior.

Automation allows SOC teams to accelerate their threat hunting processes, improve incident response time, and successfully resolve the skill shortage problem that is particularly prevalent in the cyber security industry.

How to launch a security automation process in five steps

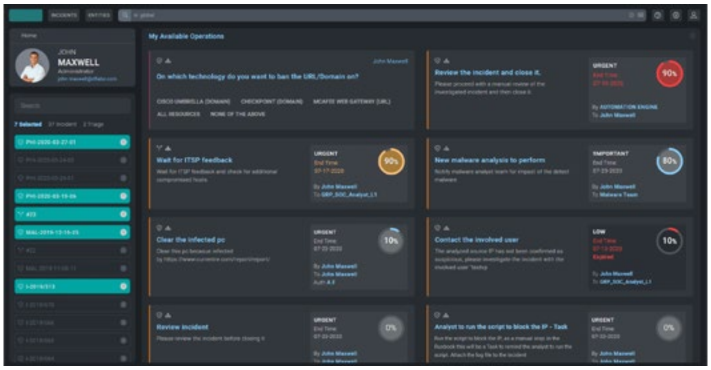
1. Identify standard operating procedures (SOPs)
2. Analyzing the tools that need to be orchestrated within the processes
3. Improve SOPs using playbook logic
4. Leverage progressive automation & supervised active intelligence
5. Harness the Sumo Logic experience

Step 1: Identify standard operating procedures (SOPs)

The first thing to do before starting an automation project is to analyze the current Standard Operating Procedures (SOPs) present in the company, or start by downloading playbooks from APP central, selecting playbooks you would like to use as a starting point for building your SOPs, changing whatever you want, including integrations.

Step 2: Analyzing the tools that need to be orchestrated within the processes

The second step is to analyze the tools that need to be orchestrated within the processes in order to perform investigations and create notifications and containment actions.



Verify existing API connectors & create the missing ones

There are over 1500 actions in the community that could be orchestrated in streamlined processes. However, via Sumo Logic's unique Open Integration Framework, you can easily extend, modify, or create a new one with almost no coding experience required.

Create daemons to be more proactive

Users are free to create daemons of any nature, and via daemons, they can analyze the content of a mailbox, incoming Syslog messages, databases external to Cloud SOAR, and also retrieve indicators of compromise (IOC) from threat intelligence.

Step 3: Enhance SOPs using playbook logic

You can easily add automatic or manual execution actions, choices and tasks.

Via playbooks, you have the ability to control every phase of security processes (enrichment, notification, customization, escalation, choice, and containment). CISOs and SOC managers are free to customize playbooks in whichever way they deem most beneficial to their needs.

Step 4: Progressive automation & Supervised Active Intelligence

Alert triage & automatic incident creation

Thanks to the capabilities of Supervised Active Intelligence, the process of alert detection to playbook activation can be completely automated. Supervised Active Intelligence automates crucial parts of the incident response process, such as:

- Triage of false positives
- Validation of incidents
- Delegation of incidents to a group of users or to a specific analysts
- Related playbook recommendations based on the type of threat

Additionally, via progressive automation, users can customize the application of automation in their SecOps and decide which actions they want to automate and which ones they want to manually execute.

Playbooks in actions

Automation in playbooks: It's essential to decide how every action of the process should be executed. In this area, we can identify three types of actions that can be inserted into a playbook:

- **a. Fully automated actions:** Actions that are performed directly by SOAR without the need for human intervention. From our experience, these kinds of actions are mainly those revolving around the investigation and enrichment of alarms.
- **b. Manually executed actions & user choices:** Actions that require the assistance of an analyst. All these actions appear in the SecOps dashboard and they are orchestrated after being manually approved by analysts.
- **c. Tasks:** In this case, these are tasks that the analyst has to perform manually and not through orchestration. The assigned task can be created automatically by the playbook itself or by the supervisor.

SecOps dashboard, Case manager and War Room

Your analysts will work differently. They have all tasks in one place such as automatically assigned actions, user choices, and playbook recommendations. They can use the search query bar to easily customize the viewing perspective, and choose which data they want to see.

Supervised Active Intelligence

Analysts can control all the assigned tasks, manual execution actions and user choices in their own SecOps dashboard. Furthermore, the addition of the concept of Supervised Active Intelligence helps analysts by providing recommendations on which playbooks should be activated for that particular type of incident.

MITRE ATT&CK simulation to improve visibility

By creating appropriate test incidents, you can activate enrichment actions that take data from MITRE and present it to the users, allowing them to improve the processes accordingly.

Automated & fully customizable reports

Instead of manually verifying characteristics of a potential threat that could take hours, SOAR's fast-paced incident reports allow analysts to have access to vital information in a matter of minutes.

Step 5: The Sumo Logic experience

How can we help you in starting an automation project?

- **Analyst training and change of mindset**
  Modern-day analysts spend their time drowning in manual tasks. However, thanks to automation, they can direct their time and effort on more challenging initiatives, such as process governance, managing escalation, and making well-informed decisions regarding high-priority projects.

- **Professional services and training**
  Sumo Logic's experienced professional services can support and make your SOAR implementation as smooth as possible by providing different onboarding packages.

We can support you in:

- Configuration of Cloud SOAR based on your specific needs
- Creation of custom playbooks

We also offer an extensive catalog of training for the different users involved with Cloud SOAR. Our expert team of security professionals is at your service at all times.

Other Q&A about Automation

Does SOAR replace human intervention?

SOAR does not replace humans, it simply makes them more efficient by taking care of repetitive and time-consuming tasks, allowing analysts to concentrate on critical initiatives.

Is there a downside to automation in security operations?

No, there isn't. Security automation was designed to overcome the deficiencies of manual operations and its only purpose is to ease the job of analysts without inflicting any negative effects on the operations.

About Sumo Logic

Sumo Logic Inc., (NSDQ: SUMO) 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 around the world 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.

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

www.sumologic.com

Updated 02/2022