sumo logic | Continuous Intelligence Platform™

Accelerate SecOps using Cloud SOAR Open Integration Framework

Customize and easily add new integrations to your existing security tools and Cloud SOAR

Flexibility, customizability, and ease of use are three highly relevant factors in modern SecOps. This is what Open Integration Framework (OIF) is all about.

With the open integration philosophy adopted by Cloud SOAR, you can:

- Easily connect and integrate disparate technologies
- Customize integrations and adapt them to your environment
- Boost the automation of repetitive tasks with full control

The Sumo Logic Community Portal, provides an open and cooperative ecosystem, where you can find and share integrations and playbooks for tackling specific bespoke use cases.

Key benefits of OIF

- Faster integration development
- Easily extend existing and develop new integrations
- Designed to minimize technical knowledge required
- Use of built-in and third-party libraries
- Integrations executed in Docker containers
- Custom integrations can be easily shared between users
- Increased openness and community involvement
- Share knowledge and integrations with Sumo Logic's Cloud SOAR Community Portal
- Unique incident response capabilities without the need for complex coding

The importance of Open Integration Framework in cybersecurity

OIF is one of the core components of Cloud SOAR. It fundamentally changes the way integrations are being used in the platform. It allows you to develop connectors and operate with external technologies. All of this ultimately helps you improve your cybersecurity posture while enjoying a more user-friendly experience.

OIF is based on open APIs for defining integrations within Sumo Logic Cloud SOAR.

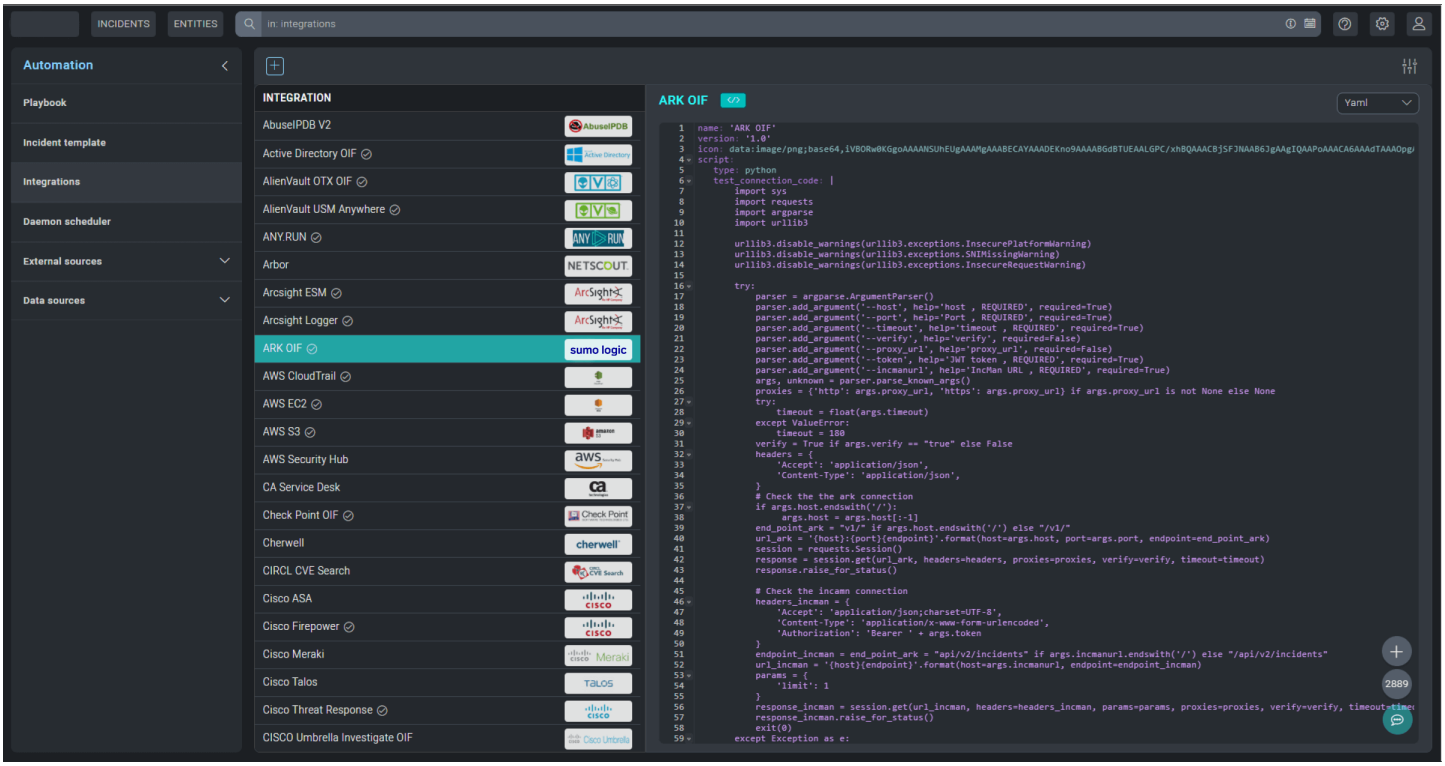
What are the standard scripting languages supported?

Sumo Logic allows both users and developers to define integrations in multiple standard scripting languages, such as Perl, Python, Powershell, and Bash, all wrapped into YAML configuration for optimal flexibility. Integrations in Cloud SOAR are structured in a modular way. This means Cloud SOAR defines all integrations at the action level, not as one monolithic file.

Can you easily add new integrations?

Yes, adding new integrations in Cloud SOAR is a seamless process that doesn't require complex coding. You can extend the capability of integrations at any time, and organizations can easily modify the existing integrations with the new functionalities Cloud SOAR provides for maximized customizability.

The execution of each integration is performed in a unique Docker container and is easily configured from within the integration file, providing additional security and eliminating the risk of conflicting libraries.



Can you create your own integration or modify the existing one?

Yes, you can easily develop integrations and access to the API code. Plus, once you're done, you can share the integrations with us and we can test them for you. Then, when the integration is ready, we'll publish it on our portal.

Can teams create their own integrations?

Yes, they can. Cloud SOAR's OIF allows you to build your own integrations from the ground up. This function is great for a team with developers, system integrators, and MSSPs. In any case, you can create and manage playbooks with no significant coding experience required.

Can you write your own custom scripts in Cloud SOAR?

Yes, Cloud SOAR allows you to write custom scripts that appear as usable actions that can be manually invoked or used within the playbooks. Usually, custom scripts are used for incident enrichment, specific investigation activities, custom data processing, or escalations. They can be manually executed by the operators as part of an ad hoc investigation step.

How do I create an integration?

Cloud SOAR allows you to create integrations with different security tools due to its OIF philosophy. The creation of the integration is enabled via the Docker containers. By creating an integration definition container via the OIF, you can upload individual action files. Then, you can code the action in the integration action file by using one of the supported scripting languages.

Lastly, the user is free to choose the Docker container they want their integration to be executed in, using different types of third-party libraries in the process.

Supervised Active Intelligence (SAI) and machine learning

The Supervised Active Intelligence applies OIF machine learning to historical responses to threats and recommends relevant playbooks and paths of action to help you respond more effectively to future threats. In short, SAI helps:

- Assess new incidents based on unique and shared indicators and their relevance to historically recorded incidents
- Construct a model of organizations threat landscape based on recorded historical incidents
- Suggest appropriate actions and playbooks by using its algorithm based on similar and related threats

- Prioritize threats that have greater relevance by assigning them with higher urgency
- Identify parent incidents and correlate incidents based on similar demographics
- Intervene in the process of triage

The Automated Responder Knowledge (ARK) does not require any knowledge. ARK learns from the experiences and actions of your security team and becomes smarter and more effective as time goes on.

What kinds of actions can be created via OIF?

Besides the definition of actions that can be inserted as steps into playbooks, OIF allows you to create seven different types of actions:

- Enrichment
- Scheduled
- Containment
- Notification
- Custom
- Automatically assigned tasks
- Machine or user choices

All these actions can be customized and adjusted according to the needs of the organization.

Specific emphasis should be placed on scheduled actions, which enable you to implement new use cases by defining steps in a playbook that can be executed multiple times until a specific condition is met or the scheduling time expires.

Make the most of automation

In order to improve your standard operating procedures, you can easily add automatic or manual execution actions, choices and tasks to playbooks, but these are other uses of automation:

- **Daemons** are defined as scheduled processes that are activated to execute particular actions. Daemons silently work in the background without disrupting the original workflow of the task. When integrations are created via the OIF in Cloud SOAR they include the action type “daemon.” They can be run as a Daemon or a scheduled service, automatically creating incidents based on the results of a predefined query.
- **Cloud SOAR triggers** allow developers to monitor specific manual events performed by the operators and automatically take actions whenever the event is performed.

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