sumo logic | Continuous Intelligence Platform™

WHITE PAPER

2022 Enterprise SOAR Buyer's Guide

Your guide to evaluating security orchestration, automation and response (SOAR) solutions

Introduction

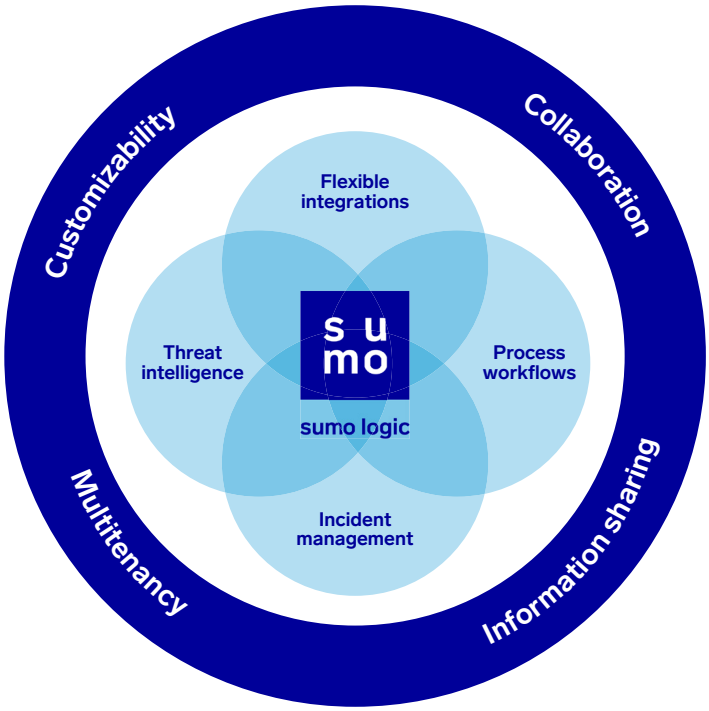
Modern SOAR solutions should be flexible enough to adapt to any use case, including those outside the traditional security operations space. This document evaluates choosing SOAR solutions informed by working with customers, developing unique solutions, and information from leading industry analysts.

This guide covers SOAR as a transformative technology in the cybersecurity industry and provides the information you need to make an informed decision based on your requirements.

Whether you're new to SOAR or you're looking to change your current SOAR vendor, this guide will help you align your needs with the right SOAR solution. Since SOAR can significantly impact your security operations center (SOC), it is essential to understand the available options to make the best decision for the right SOAR solution.

What is SOAR?

Even though no two SOAR platforms are entirely alike, they should all possess core functions and capabilities. Depending on your set of problems and goals, some of these functions and capabilities may be more important than others. Start by deciding which of these functions are most important in achieving your defined objectives. This will allow you to focus your evaluation of each SOAR solution based on the functions and capabilities which are most important to your organization.



Core functions

Flexible integrations

Whether commercial, open-source, or developed in-house, any viable SOAR solution must be flexible enough to support many security products. However, the likelihood that all the organization's security products will be supported by default is low. For that reason, it is crucial that a SOAR solution is flexible and allows customers to easily create bidirectional integrations with security products that are not supported by default.
The methods used to support this type of flexible integration may vary but could include scripting languages such as Perl or Python, APIs, or proprietary methods. Whatever the chosen method, it should be easy to implement and not involve a steep learning curve on the user's part.

Bidirectional integrations are crucial in supporting full automation and orchestration. However, in some cases, the customer may not require full bidirectional functionality. It may only be necessary for some security products to support the data ingestion from the security product to the SOAR platform. These unidirectional integrations are generally for the customer to create in cases where full bidirectional integration is not required. For this reason, a SOAR platform should support common methods of data ingestion, such as Syslog, database connections, APIs, email, online forms, and data standards such as CEF, OpenIOC, and STIX/TAXII.

Process workflows - Playbooks

One of the key benefits of a SOAR solution is the playbooks which allow you to orchestrate actions and automate time-consuming tasks in streamlined processes. They are force multipliers by taking care of repetitive tasks via automation. To produce these benefits, a SOAR solution must be flexible in implementing workflow processes without limitations.

Playbooks codify process workflows within a SOAR solution. The implementation of these workflows must be flexible enough to support almost any process that may be enhanced. Workflows should support the use of both built-in and custom integrations, and the creation of manual tasks that need to be completed by an analyst. Allowing control to pass between the automation engine and an analyst, SOAR provides flexibility and enables automation to continue beyond the first point at which human decision is required.

Building workflows should not require programming knowledge. You can easily add actions into playbooks to define standard operating procedures. Every type of attack has to have specific processes to investigate alerts and remediate incidents, and SOAR supports analysts uniformly by following the same procedures. Since workflows are at the heart of a SOAR solution's automation and orchestration activities, extra focus should be placed on flexibility and ease of use. Workflows that are difficult to build or complex to understand by a wide range of users will cause confusion and sub-optimal performance during an incident.

Incident management

Incident response is a complex process. Orchestration and automation of security products provide apparent value to any security program. Still, to maximize the time and monetary investment, a comprehensive SOAR solution should include additional features to manage the complete incident response and management lifecycle. This should consist of basic case management functionality, such as tracking cases, recording actions taken during the incident, and reporting critical metrics and KPIs.

However, a SOAR solution's incident management capabilities should not consist solely of case management functionality. To properly manage the entire incident management lifecycle, a SOAR solution should also provide the following features:

- Phase and objective tracking
- Detailed task tracking, including assignment, time spent, and status
- Asset management, tracking all physical and virtual assets involved in the incident
- Evidence and chain of custody management
- Indicator and sample tracking, correlation, and sharing
- Document and report management
- Time and monetary effort tracking

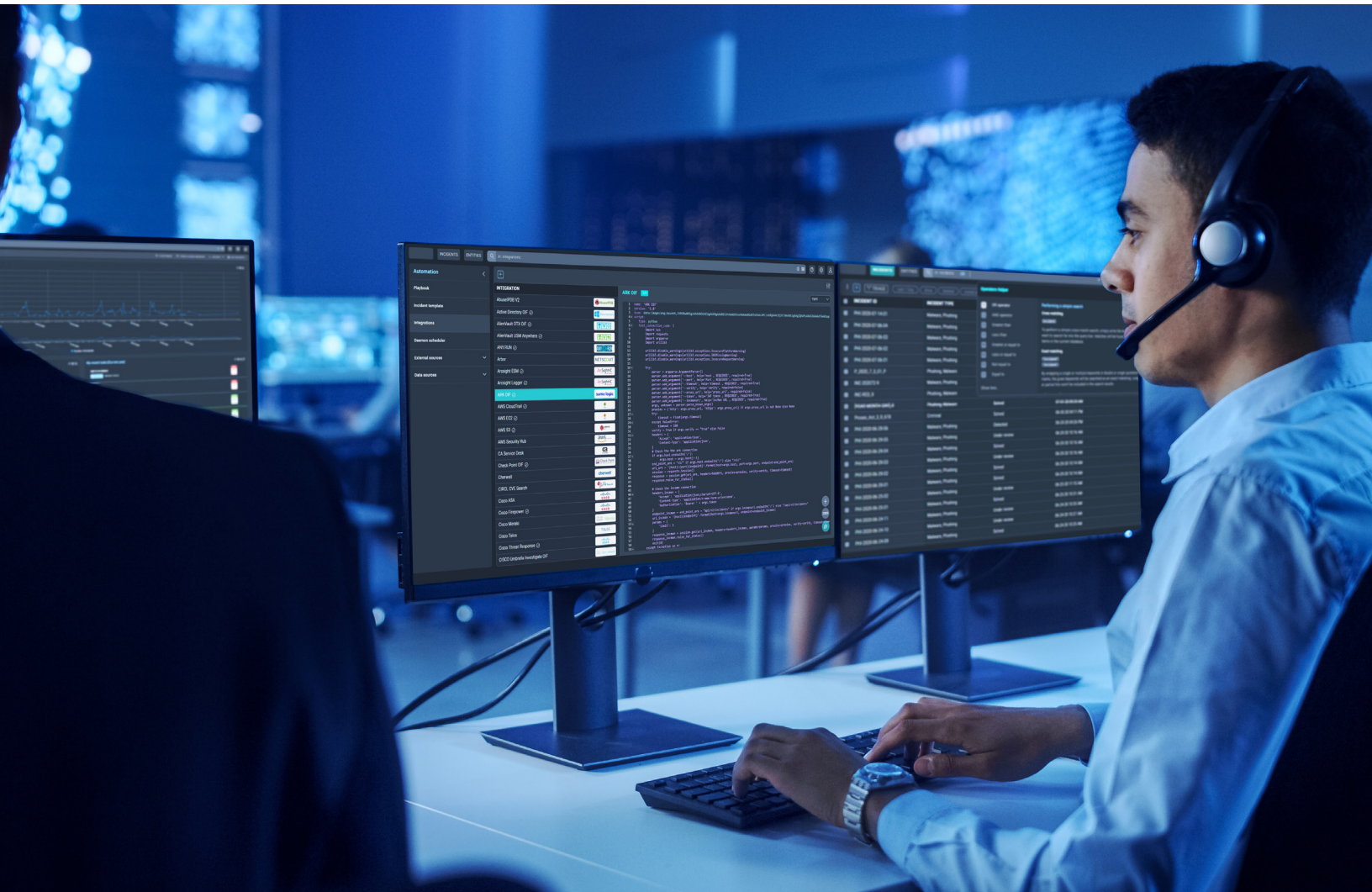
Threat intelligence

Actionable threat intelligence is a critical component in effective and efficient incident response. While simple threat intelligence feeds still provide some value and should be supported by a SOAR solution, to be truly effective in today's threat landscape, threat intelligence must go above and beyond simple feeds. As discussed in the previous section, tracking indicators and samples, such as IP addresses, URLs, malware samples, and TTPs is a critical component of incident management. However, to become actionable threat intelligence, these indicators must be surrounded with further context. Because a SOAR solution has access to the indicators and the rest of the incident information which can provide additional context, it is in a unique position to gather actionable threat intelligence.

A SOAR solution must go beyond simply gathering threat intelligence. A proactive security program requires threat intelligence to be properly correlated to discover attack patterns, potential vulnerabilities, and other ongoing risks to the organization. This correlation should be done automatically, and it should be immediately apparent if an ongoing incident may share common factors with any previous incidents.

Nowadays, threats are increasing in number, and it is essential to have more than one threat intelligence security solution to enrich alerts and identify with greater certainty if the threat is real.

Having all the information in one place is critical for analysts to make informed decisions during the incident response process. Many proactive security programs now include various forms of threat hunting, actively looking for attacks and patterns that



automated methods may not detect. To facilitate this process, threat intelligence and correlated events should be displayed in an easy-to-understand visual manner to allow analysts to effectively analyze the information.

Core capabilities

Customizability

No two security programs are alike; this is especially true when you cross vertical lines. For a SOAR solution to be effective, it should be the single tool on top of the security stack. A "one-size-fits-all" approach to SOAR will leave customers with a solution that does not adequately address all their use cases, forcing customers to look to other tools to supplement the gaps.

A SOAR solution must be flexible in its implementation, the data it collects, and how it integrates with other security tools (discussed in more detail in the following section). A SOAR solution should be implemented in a manner optimized for CSIRT teams, as well as SOCs, MSSPs, and security teams. Data input from many sources, including machine to machine, email, user submissions, and manual input should be supported. The importance of security metrics means customers should customize the values available in the solution and what attributes are tracked. Higher customizability of the SOAR solution will result in greater ease of use and a better fit for the customer, and substantially increased ROI.

Collaboration and information sharing

Incident response is not a one-player sport. Response to a security incident will likely include multiple individuals and potentially multiple teams and even organizations. To be effective in a team environment, a SOAR solution must support seamless collaboration and information sharing between team members in a controlled manner. Those with authorization should have instant access to the status of the incident they are collaborating on and any information gathered and other actions performed by team members. Team members should also have the ability to communicate securely within the SOAR platform, providing an out-of-band communication mechanism when other mediums may not be trusted.

Collaboration and information sharing must also be possible outside of the organization itself. This is especially true in the context of threat intelligence. Open sharing of threat intelligence, when possible, is a critical tool in fighting cybercrime. There are numerous avenues available to share threat intelligence: open, closed, and industry-specific. The majority of these threat intelligence sharing programs utilize one of the open standards for threat intelligence, such as STIX/TAXII, OpenIOC, or MISP. A SOAR solution should support both the ingestion and sharing of threat intelligence information via these common standards in a controlled and secure manner.

Multitenancy

Many large enterprises have multiple internal security teams performing unique sets of tasks. In some instances, it may not be appropriate for some internal teams to access the data collected by other internal teams. MSSPs are also beginning to turn to SOAR solutions as a force multiplier and require stringent segregation of customer data.

In either case, it is not cost-effective to deploy an individual SOAR solution for each team or customer. A SOAR solution must be capable of supporting multiple instances on a single host, providing accurate data segregation and access controls for each tenant's information.

SOAR vs. Orchestration and Automation

The number of vendors who have begun to include elements of orchestration and automation (O&A) capabilities in their platforms has increased dramatically over the past year. This has caused some confusion regarding which products are competitors of existing SOAR solutions and complementary solutions that offer O&A capabilities (non-SOAR solutions).

When you begin to compare these two categories, there are two significant differentiators. Non-SOAR solutions tend to focus on O&A within their product or within a similar product space. Their focus on one particular product space makes them capable of addressing advanced use cases in that product space. However, they typically do not support use cases outside of that space. On the other hand, a SOAR solution should perform O&A across many different product spaces in one cohesive solution.

The other significant differentiator between SOAR and non-SOAR solutions is their ability to perform other "response" (the R in SOAR) and incident management functions. Whereas a SOAR solution should perform these other response functions, a non-SOAR solution is typically limited in this regard.

Reliability of automation in SecOps

Given that automation is relatively new, many security professionals are still skeptical of its abilities. Still, after having some time to analyze the benefits of applying automation in everyday security operations, those doubts slowly fade away.

The benefit of automation in SOAR is that it is 100% adjustable. You can instruct SOAR to halt and leave things to the analysts at any point in the automated procedure. The level of customization in automating procedures allows analysts to decide which tasks they want to be fully automated and which tasks should include human intervention.

Ultimately, the role of automation in security operations is to ease the burden of security professionals by automating low-risk, repetitive, and time-consuming tasks. We strongly believe that

automation has reached the level of maturity necessary to carry out such tasks effectively. And in the future, it will only continue to become a more reliable and integral part of SecOps.

What kind of security operations can be automated?
SOAR can be instructed to automate any security operation. But in practice, the most common types of security operations that are automated by SOAR are the ones that are most repeatable and time-consuming.

For instance, a potential phishing attack analysis follows a similar procedure that repeats almost every time. From tracking the geolocation to analyzing the IP reputation, these procedures are time-consuming and repeatable every time there is an alert of a phishing attack. But if you instruct SOAR to analyze this alert, it will successfully notify analysts to the degree of danger.

Even though SOAR is constantly innovating and its progressive automation is getting stronger, it still uses caution, and its application now revolves mainly around repetitive security operations. But even if automation is applied to repetitive tasks, it still provides value to security professionals, as these tasks are often the most numerous and time-consuming ones.

Is there a downside to automation in security operations?
No. The only downside is the fear that automation would one day replace humans in security operations. But in reality, automation cannot ever be completely autonomous. It relies on human commands to carry out processes, which is one reason why automation will never replace humans. It will only serve to make them more efficient.

Defining the problem

Here are a few of the fundamental questions that should be answered before evaluating any SOAR solution:

What is the problem we are trying to solve?
A SOAR solution can solve a variety of problems, some better than others. It is crucial to define which problems are most important for your organization to solve. Some of the most common problems organizations look to a SOAR solution to solve are:

- Too many alerts to handle with available staff
- Lack of qualified staff to fill positions
- Repetitive, manual processes requiring large amounts of the staff's time
- Lack of incident management capabilities
- Undocumented standard operating procedures (SOPs) or inconsistent processes
- Inability to record and generate metrics
- Need to comply with regulations, standards, and best practices

Once the problems have been identified, each solution can be evaluated for how well it solves these problems.

How will success be measured?
The answer to this question is closely tied to the previous question, and ideally, you should identify at least one measurement of success for each identified problem. Any measurement should be as clear, objective, and easy to measure as possible. For example, suppose one of the organization's problems is trying to solve an unacceptably high time to respond to an alert. In that case, you may decide to measure success by reducing the average time to respond to alerts.

Once you have defined what you will measure, define the goal you wish to achieve for each measurement. In other words, if we implement this solution, what is the outcome we expect to achieve? To effectively measure success, goals should be SMART: Specific, Measurable, Attainable, Relevant, and Time-based. Goals that do not meet all five criteria are unlikely to give you an accurate measure of the success of your project. For example, a goal may be to reduce the average time to respond to alerts by 50% over the next year.

Other questions to consider before beginning your research and evaluation:

- What are the critical SOPs to improve?
- Who is conducting incident response today?
- What is the timeline, and when do I want to implement the solution?
- Is there a budgeted initiative to reduce costs and time for incident management resolution?
- Which features are must-haves? Which are nice to have?
- Which integrations are must-haves? Which are nice to have?
- What are the technical and implementation requirements?
- How many users do I need?

With the answers to these critical questions thoroughly defined, documented, and shared with the entire evaluation team, you should be ready to begin an evaluation of SOAR solutions that will provide you the best solution that perfectly aligns with your organization's specific needs.

Evaluation criteria

Defining a core set of questions to ask each SOAR vendor is critical for obtaining an accurate, unbiased comparison of each solution. This process may be as formal as creating an RFI or RFP to send to each vendor, or as informal as a list of questions that will be asked during a product demo. In either case, the questions should be established and agreed upon before the first solution is evaluated.

Questions should focus on determining how well each solution will meet the project goals you defined at the beginning of this process. If you have not yet established your project goals,

see this guide's section, "Defining the Problem". Some general questions about the solution and the vendor (discussed in additional detail in the next section) may be appropriate as well.

Most mature SOAR solutions will provide a core set of features, such as a GUI workflow editor or ingestion of common protocols such as Syslog. If any of these core functions are critically important for your use case, it may make sense to ask more detailed questions regarding these functions. However, in general, questions regarding these functions, such as "Do you support Syslog?" are unlikely to differentiate the solutions in a meaningful way.

With that in mind, here are some common questions that should provide some meaningful differentiation between SOAR solutions to assist in your evaluation:

General

- What problems does the solution solve?
- How does the solution solve these problems?
- What are the solution's primary differentiators?
- What are some of the most common use cases current customers have implemented? What are some of the most unusual use cases current customers have implemented?

Automation & Orchestration

- Does the solution allow human decisions to be made at critical junctions? How?
- How does the solution orchestrate actions between different integrations?

Implementation

- How is the solution implemented?
- How long does it take until the solution can be fully operational?

Incident management

- What incident management capabilities does the solution provide?
- How does the solution support team collaboration and information sharing?
- Does the solution support evidence management?

Integrations

- What product integrations does the solution support?
- How many of your 'must-have' integrations are on the list?
- Are your specific integration use cases supported? (i.e., can you perform the actions you need?)
- What is the process for getting a new integration added?
- Is it possible to modify the integrations and see the code?
- Are there any limits?

Pricing

- What are the pricing models?
- What is included in the base price and what is considered an 'add-on'?
- Are professional services or consulting required to get up and running with the solution?

Reporting and visualization

- Does the solution provide the ability to generate custom reports and metrics?
- Does the solution support customizable dashboards or other visualizations?
- Does the solution allow you to record and report on custom attributes?

Vendor evaluation

A SOAR solution should be considered a long-term investment. The rip-and-replace cost will be high once a SOAR solution is deployed and integrated into the security process. For this reason, it is important to evaluate the vendor of the SOAR solution, along with the solution itself. The vendor chosen should provide both a leading SOAR solution and responsive customer service for the foreseeable future.

Questions to ask a SOAR vendor
Here is a list of common questions that can be used to provide meaningful differentiation between SOAR vendors:

- How do you provide post-sales customer support? When is support available?
- What is the process for customer feature requests?
- Who are your competitors?
- Do you offer any professional services or other services?
- Is there a library of playbooks available to start adapting to my environment?
- How does the company contribute to the security community?

Summary

The purpose of this guide is to help organizations understand what SOAR is, what core functions and capabilities an organization should expect from a SOAR solution, and how to define what criteria should be used when evaluating SOAR solutions to best meet an organization's challenges. Objectively evaluating which vendor has the best solution is a

process tailored to each organization's requirements. Although this guide has suggestions for common questions that may be beneficial when evaluating SOAR solutions, each organization must consider what questions will be most impactful based on the problems they are trying to solve.

To learn how Sumo Logic's Cloud SOAR solution can accelerate your SecOps processes, visit: https://www.sumologic.com/solutions/cloud-soar/

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.

s u

Continuous Intelligence Platform™

m o

sumo logic

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

www.sumologic.com

Updated 09/2021