sumo logic

How to calculate the ROI of Cloud SOAR

Learn how to get the best ROI out of your SOAR investment

Table of contents

Introduction

There's more to making the most out of your security orchestration, automation and response (SOAR) investment than simply deploying it in your environment. As sophisticated as it is, SOAR still needs to be run, monitored and directed by humans.
In this white paper, we'll teach you how to maximize the return on investment (ROI) of your SOAR solution, including leveraging the strengths of Sumo Logic Cloud SOAR.

Finally, we'll personalize your ROI by showing exactly how SOAR elevates the efficiency of your security operations center (SOC).

sumo logic

What kind of ROI should I expect from a SOAR solution?

The Cloud SOAR Open Integration Framework (OIF) allows you to easily integrate your existing architecture—even independently—so you can obtain the ROI described in this document.

The ROI of SOAR differs by the organization and how it is used. But, achieving ROI for SOAR boils down to the following elements:

- **Improved time management and productivity**: By automating repetitive tasks, analysts will have more free time on their hands to prioritize work and improve efficiency.
- **Enhanced threat hunting capabilities**: SOAR's machine learning engine improves SOC threat detection by providing a thorough analysis of a threat which allows the cyber team to make insightful decisions.
- **Increased efficiency**: Thanks to automation, you'll get more things done with fewer resources. SOCs can better allocate their resources and analysts can focus on tasks that matter.
- **Improved employee retention**: Security professionals don't have to manually handle menial tasks.

To get the most out of SOAR, companies must first strategically assess the nature of their security operations. Integrating SOAR will help you get more done in a shorter amount of time and with fewer resources. Companies that receive thousands of alerts every day will recoup their investment through SOAR's progressive automation.

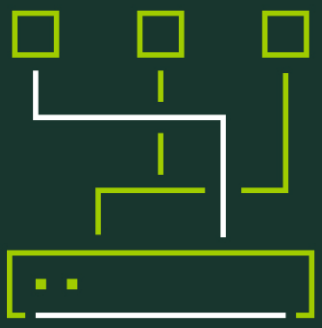
How does automation impact the ROI of SOAR?

The evolution of cyber threats has stimulated the progression of technology used in cybersecurity environments. The zero-tolerance SOCs have for security breaches has given birth to setting clear and concise rules and instructions that every security team member must follow. That's what marked the genesis of standard operating procedures (SOPs).
However, as cyber threats continue to grow, merely following SOPs is not enough. Organizations must be quicker than criminals and effectively implement SOPs while using the full potential of their resources.

SOAR automates crucial parts of the incident response process. Here is how the incident management and response process would go with and without the implementation of SOAR.

sumo logic | Continuous Intelligence Platform™

How does automation impact the ROI of SOAR?



Action	With SOAR	Without SOAR
Alert analysis and triage of false positives	The analyst has to manually manage disparate tools and should add all collected information into a report.	The process of alert validation to playbook activation can be completely automated and SOAR can create incidents only when real threats are detected.
Incident assignment	Incidents are assigned through the ticketing system by manually collecting information from different tools. Analysis of the information collected is not straightforward.	SOAR assigns incidents to a specific user or group of analysts by adding all the essential information in the case manager providing the cyber team with all necessary information.
Playbook activation	If the cyber team has written procedures it has to follow them by managing several tool interfaces. If the procedures are not there, they must improvise based on their specific knowledge and skills.	SOAR generates playbook recommendations based on the type of alert helping the analyst to activate SOPs.
Manage every task inside SOPs	The cyber team must manage disparate tools by following written instructions (if these exist).	Easily orchestrate all your technologies and automate time-consuming tasks with progressive automation.
Execute specific instructions when a manual task happens	Analysts must manually accomplish the process with all tasks concatenated to another specific task.	Advanced Cloud SOAR triggers can be automatically hooked to manual tasks performed by users.
Active search and analysis of relevant alerts	The analyst has to manually search specific types of alerts, analyze incoming syslog messages and convert them into objects,retrieve threat feeds from various external repositories, analyze external databases, etc.	You can use several types of daemons to schedule processes that, according to a chosen schedule, are automatically activated to execute tasks of any nature.
Report creation	Analysts have to manually collect information and build a report.	Incident detailed reports are created automatically.

sumo

sumo logic

How can SOAR improve efficiency and consistency?

SOAR allows for numerous benefits including:

- **Alert analysis:** Thanks to SOAR you can use daemon's unique capability to improve automation rules and decide which type of alert you want to manage with SOAR. In addition, SOAR suggests which process has to be activated.
- **Easy visualization of processes**
  Using playbooks to visualize and improve SOPs will avoid confusion and ensure that practitioners are working from the most recent version of a SOP. Update the SOP regularly and include the date of the last update and the version number.
- **Add as many additional controls as you want.** Without SOAR, an analyst can perform a finite number of tasks because time is short and it is necessary to rationalize forces. With SOAR it is possible to use automation to avoid repetitive tasks for the operators. One of our customers has an alert investigation procedure that foresees 82 actions that SOAR carries out at the same time.
- **Decision making**: A crucial part of the procedures are the decisions to be made. Thanks to automation you can efficiently and quickly collect all the information that will ensure insightful choices.
- **Containment:** Before responding to a threat by taking containment action, it is essential to do a quick and thorough investigation and have the ability to easily verify the outcome. SOAR allows you to make well-informed decisions, orchestrate containment tools, and automatically assign checking tasks to make sure everything is working properly. At that point, analysts can close the incident.
- **Reporting:** Thanks to SOAR it is possible to automatically create extremely detailed and customized reports.

SOAR as a technology applies automation in the conventional workflow processes of security teams. This means that tasks that were once handled manually will now be able to be run automatically with the same or even better degree of quality.

Some SOPs can be very time-consuming and can disrupt the workflow of security professionals. For example, repetitive tasks such as generating reports or managing various tools., This is why incorporating a solution that can automate repetitive and low-risk tasks can be highly beneficial for the SOC.

Time plays an essential role in cybersecurity. Growing cyber threats leaves no room for potential mishaps, and with every minute cyber attackers spend breaching your security defenses, the bigger the damage is that is inflicted on the organization.

Let us explain the simple math behind SOAR's integral role in improving your standard operating procedures:

Automating certain tasks: SOAR automates certain SOPs, such as generating and sending reports. This relieves analysts from their duty of doing these repetitive tasks and allows them to redirect their expertise to other tasks of greater importance.

Make the most out of your resources: Given the fact that the cybersecurity field is undergoing a shortage of skilled analysts, the quicker you are at effectively seeking out every aspect of your workflow processes, the better you will deal with unexpected cyber threats.

Orchestrate different tools: SOAR allows you to orchestrate your security tools into a seamless response platform, and thanks to playbooks, security analysts can have a better overview of their SOPs in a visually accessible manner. In this case, choosing a vendor which can guarantee a full open integration framework is mandatory.

SOAR takes much of the burden off your analysts' shoulders by automating SOPs, but the true value of SOAR goes beyond improving SOPs.

Quantifying your SOAR investment

In addition to the qualitative benefits of SOAR, you can also calculate the time if saves.

Besides defining structured processes that all analysts have to follow, SOAR allows you to decide whether each action should be triggered automatically or handled manually.
In over 10 years of experience in this field, we have noticed that analysts spend the most time in the enrichment and decision-making phases. This means they spend a lot of time analyzing all the information collected via different tools. Taking this into account, we have crafted Sumo Logic Cloud SOAR around the premise of helping analysts spend more time on critical assignments and less time on tasks that can very easily be automated.

When it comes to the ROI of investing in SOAR, we've been able to pinpoint two distinctive phases where SOAR plays a particularly important role in easing the job for analysts:

1. Enrichment
2. Decision making & containment

sumo logic

1. Enrichment

In the enrichment phase, every action is pointed toward collecting information that will afterward have to be analyzed, such as:

- Malicious IP Geolocation
- Reputation IP/URL/Malicious crimes
- Compromised user info retrieval
- Detonation suspicious attachments
- Detonation of malicious attachments
- Who is of malicious IP/URL
- IOC search on CTI

Example of a playbook of only enrichment actions

Depending on the type of threat and on your tools, all enrichment actions are different. They are collected from different sources, which leaves the analyst with the tedious task of making the collected data readable. When it comes to the options analysts have in the enrichment phase, the number of manually managed enrichment actions per incident is often limited, which isn't the case with SOAR. SOAR allows analysts to trigger actions sequentially, indicating as input to the next action the output of the previous one, or making it possible to trigger actions simultaneously.

We have considered the following timeframe for the execution of each enrichment action. We have taken into consideration the best scenario for the execution of the manual process, which includes accessing the tool, changing every time, and therefore having several interfaces for executing specific actions. We have also mapped out the worst-case scenario for the SOAR part.

Assumptions on time management of shares with or without SOAR

Enrichment	Manual processing (seconds)	SOAR processing (seconds)	SAVED TIME (seconds)
Average time to manage enrichment actions	**65**	**5**	**60**

2. Decision making & containment

For the decision-making and containment phases, we have underlined the following actions to be carried out for each incident:

Assumptions for every incident	Manual processing (seconds)	SOAR processing (seconds)	SAVED TIME (seconds)
1 Note creation with results of enrichment phase	**180**	**17**	**163**
1 Send email notification	**210**	**4**	**206**
1 Detailed incident reports with related IoCs, timeline, and corrective actions executed	**415**	**3**	**412**
1 Decision making: with SOAR, all the information is in the same place, and without SOAR you have to read reports in different formats.	**900**	**60**	**840**
1 Containment action	**30**	**3**	**27**
Manual tasks	We considered the same amount of time for manually executing the tasks in Cloud SOAR even though they are easier to execute thanks to the well-structured data previously collected from the past actions.		

SOAR is an extremely flexible tool and it is possible to select which alerts to manage with it and which to continue to manage manually.

Therefore it is possible to calculate the ROI over several phases because the level of knowledge of the platform grows progressively with time, thus affecting the initial phase of adoption for the following reasons:

- The number of processes managed with SOAR increases with time.
- The number of enrichment actions for each process increases as the security stack grows, allowing enrichment actions to be added to all the playbooks already created.
- Analyst knowledge improves over time through training and simulation

sumo logic

Assumptions	Description
A= number of Standard Operating Procedures managed with SOAR (number of playbooks)	Total number of SOPs for which SOAR is used to enrich incidents
B= Average weekly number of incidents per type of threat	Each alarm has a different response process, you have to consider the average number of alarms per process.
C= AxB Total number of incidents to manage weekly	Obtained by multiplying the number of playbooks by the average number of accidents per type.
D= Average number of IoCs involved in every incident	Each enrichment action must be activated for each Indicator of compromise (IoC) involved in the incident.
E= CxD Total number of IoCs to investigate	Obtained by multiplying the total number of incidents by the average number of IoCs involved in every incident.
F= Average number of enrichment actions per SOPs	Represents the number of enrichment actions performed for each playbook.
G= ExF Total number of enrichment actions for all incidents	Obtained by multiplying the total number of IoCs to investigate by the average number of enrichment actions per playbook.

3. Saved time in 3 Phases

Below is an explanation of the three phases that SOAR uses to consolidate your SOPs via automation. Each phase allows the SOC team to gradually increase the role of automation in processes, starting from SOPs to non-incident use cases as well.
When you implement a SOAR, three to five playbooks are usually selected as a starting point and then you can implement other processes.
In this use case, we have considered the following phases:
Phase 1: Start the project
Phase 2: Consolidate and add other playbooks
Phase 3: Add other playbooks and extend SOAR use to other non-incident processes

Parameters	Phase 1	Phase 2	Phase 3
Number of SOPs managed with SOAR****	5	20	50
Average weekly number of incidents per type of threat*	14	12	10
Total number of incidents to manage weekly*	**70**	**240**	**500**
Average number of enrichment actions per SOP***	10	12	14
Total number of enrichment actions for all incidents	**700**	**2880**	**7000**

*We considered a decrease in the average number of incidents per type as the number of processes increased.
**Although the number of IoCs involved is on average greater than one, we have been conservative.
*** We have considered an increased number of enrichment actions as processes are consolidated over time, adding more technologies.
**** Number of Standard Operating Procedures = Number of Playbooks

Annual ROI	Phase 1	Phase 2	Phase 3
Total amount of saved time to investigate and respond to every incident annually	2.412hours /100.5 days	8.719hours /363.3 days	19.103 hours /795.9 days
% of saved time	94%		

How we calculated ROI - Final consideration

To calculate the total amount of saved time to investigate and respond to every incident annually, we have multiplied the number of enrichment actions by the time spent by an analyst in performing them and we have added the number of incidents assumed in a year multiplied by the assumptions made in the decision making & containment chapter described above. As you can see in phase one alone you can save 100.5 days to handle only an average of 70 weekly incidents.

sumo logic

Would you like to have your personalized ROI report?

To quantify the unique value of adopting Cloud SOAR, contact us, and together with the Business Value Office, we will work together to give you a Business Value Assessment (BVA) report based on your real parameters.

SOAR adoption facilitates ROI growth by:

Implementing an actionable incident response (IR) plan
Reducing implementation time, converting existing SOPs in automation processes (playbooks)
Implementing industry best practices extending their usage to cybersecurity

Automate & optimize SecOps
Creating reusable IR workflows (playbooks), leverage standardization
Hint: Start from the most common type of attacks (Phishing, Ransomware, DDoS, Malware, Intrusion)

Change of analysts' mindset
Invest in your human resources, providing dedicated training on SOAR with real-life simulations
Focus on automation improvements, Governance and well-informed Decisions making

Reduce inefficiency with progressive automation in four steps
With automation you can save a lot of time. Here is our advice on how to use it:

1. Full automation just for enrichment, notification, and escalation first
2. Remediation Actions & Triggers after analyst supervision (user choices and automatically assigned manual tasks that will appear in the SecOps Dashboard)
3. Report creation

After these three steps you will be able to push the automation to the maximum:

4. Improve threat hunting & threat Investigation using other playbooks, nested playbooks, triggers, and daemons (threat pull)
5. Implement automatic triage and playbook activations

For this reason, the more you use Cloud SOAR the more your ROI will grow.

sumo logic

Summary

In the end, the ROI of your SOAR investment comes down to your ability to extract the benefits that SOAR as a technology has to offer. SOAR improves incident response time, replaces analysts when it comes to manual and repetitive tasks, and applies automation in critical segments of SecOps that additionally aid SOC teams in incident investigation and remediation. In addition, the data collected, all actions taken, and processes activated on each specific incident are simple and clear to view in chronological order in the War Room. This allows the cyber team to save additional time in analyzing incidents. These benefits alone guarantee a solid return on investment, but it all comes down to the degree to which you utilize SOAR's unique capabilities.

The time for SOAR is here, Its automation and orchestration capabilities are only going to be more in demand in the cybersecurity industry. Ultimately, the more you understand how to leverage SOAR's benefits, the more you will be able to maximize the ROI of your SOAR investment. And that starts by learning which areas of your security posture SOAR help strengthen.

Learn more

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

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700

305 Main Street, Redwood City, CA 94603