sumo logic | Continuous Intelligence Platform™

WHITE PAPER

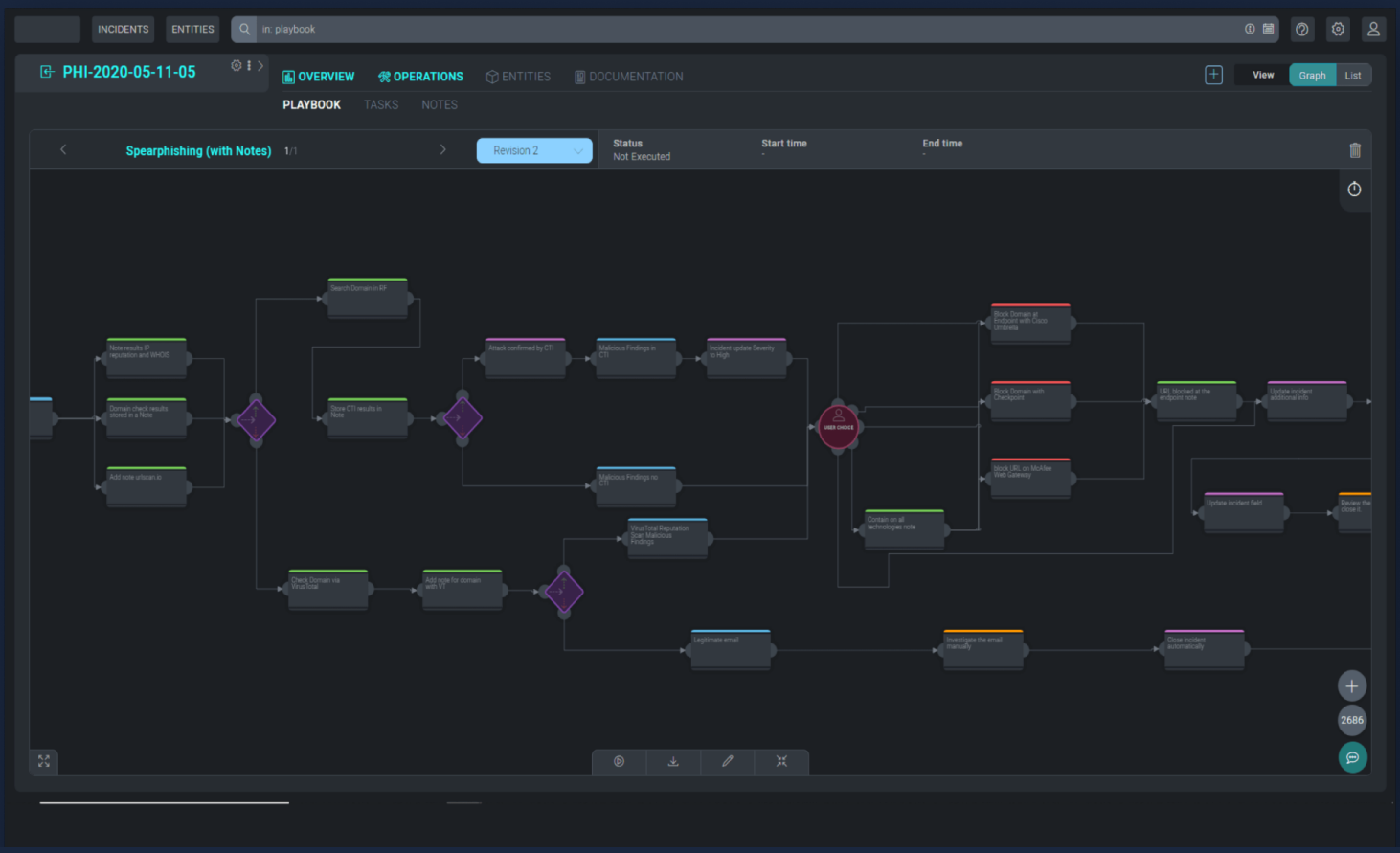
SOAR 101: an A-to-Z guide

Learn the fundamentals of SOAR, how SOAR elevates SecOps, and how to choose the right SOAR solution for your needs

Introduction

SOAR, short for security orchestration, automation and response, is a relatively novel solution in the cybersecurity industry. Many don't yet understand its full value.

In this white paper, we will address the fundamentals of SOAR, dive deeper into security automation, how SOAR fits in a typical security operations center (SOC), and how SOAR elevates your SecOps.



What is SOAR?

SOAR is a solution that allows companies to collect data regarding threats and alerts. By automating tasks, it helps analysts respond to threats in less time.

A term coined by Gartner, SOAR describes three distinctive software capabilities:

- Orchestration includes all the technologies that assist with the resolution of cyber threats.
- Automation describes the process of using machine learning to automate particular areas of security operations.
- Response refers to security incident response, measuring how an organization responds to threats.

Even though SOAR may appear to be complex, it is fairly straightforward to use, as it was created with the intention of instantly helping security professionals. With the implementation of SOAR, the natural workflow of SecOps remains unaltered, yet it is drastically improved. SOAR allows SOC teams to respond faster to cyber threats, recognize false positives by detecting patterns, and free time for analysts to focus on more relevant threats that require in-depth expertise.

How does SOAR affect the way a SOC team operates without altering the core of their SecOps? SOAR blends into the environment where it is deployed by integrating with a wide range of security tools. Instead of requiring security professionals to adapt to the way it operates, SOAR allows security professionals to preserve their workflow while benefiting from its automation capabilities.

How is SOAR different from SIEM?

This is a commonly asked question, as many confuse SOAR with the popular cybersecurity solution known as security information and event management (SIEM). Once a SIEM detects an event, SOAR takes over.

A SOAR platform is typically incorporated in a SOC to increase the efficacy of the security professionals working within the SOC. SOAR uses automation and orchestration to help organizations pinpoint real cyber threats, eliminate false positives, and respond to actual danger by drastically improving the incident response time.

SIEM, on the other hand, provides security analysts with enhanced visibility across the entire organization. SIEM allows analysts to better understand the context of incoming threats by providing automated insights to speed investigation processes and automatically triage alerts.

SOAR collects data from a SIEM and other tools, and uses its machine learning engine to respond to threats and carry out low-risk tasks (like documenting the process of analyzing an alert) without the need for human interaction. SOAR typically ingests alerts, enriches and investigates them via the orchestration of several tools.

This is why, with SOAR, analysts have more time to focus on higher priority assignments, rather than having to manually check every alert as it arrives in real-time, which is the case with those SOCs that rely only on SIEM.

Does SOAR replace SIEM?

SOAR and SIEM are two different technologies. The value in SIEM lies in collecting and aggregating security information, including:

- Collecting data from endpoint detection and response (EDR), network detection and response (NDR), intrusion detection system (IDS), firewall, identity access management (IAM), threat intelligence, etc.
- Centralizing data aggregation & storage
- Leveraging machine learning algorithms to accelerate threat detection at cloud scale
- Providing enhanced visibility to seamlessly monitor multi-cloud, hybrid, and on-premise architectures
- Detecting/identifying threats using correlation & rules
- Analytics, audit, compliance & threat hunting

More advanced SIEM solutions also have investigative workflows and automated insights. However, once SIEM stores the aggregated data, its job is done. And to be able to replicate SOAR's behavior and differentiate between normal and suspicious alerts, SIEM requires constant tweaking, which is performed by security analysts and engineers. But while SOAR has the upper hand in this area, and can autonomously distinguish between normal and potentially malicious alerts, SIEM is better at generating large volumes of data regarding security alerts.

So, rather than having to choose between SIEM and SOAR, the wise thing to do would be to combine the strengths of these two very different technologies and leverage their benefits by unifying them in a singular SOC platform.

By working together, SOAR will be able to react to every alert generated by SIEM in a timely and effective manner.

Why is SOAR becoming increasingly prevalent in the cybersecurity industry?

So far, we mentioned that SOAR utilizes orchestration and incorporates automation in SecOps. Now, we're going to explain just how these features benefit organizations, SOCs, MSSPs, and CISOs as well:

- **Resolve the alert fatigue problem:** Many organizations receive thousands of alerts daily, and SOCs often don't have the manpower to properly assess every one of them. The huge volume of alerts inevitably leads to an overload of work for analysts, who are unable to keep up with the never-ending flood of alerts. By leveraging security automation, SOAR addresses low-risk alerts, repetitive tasks, and false positives.
- **Address the skill shortage issue:** The number of daily alerts is rising, and sadly, the number of skilled security professionals is decreasing. However, SOAR directly addresses this issue by increasing productivity, allowing SOC teams to accomplish more by doing less.
- **Drastically decrease incident response time:** SOC teams that don't rely on the most contemporary technology and are not stacked with the most skilled analysts are often too slow in analyzing alerts. SOAR allows security professionals to decrease their response time to cyber threats with fully or semi-automated responses.
- **Elevate the efficiency of standard operating procedures (SOPs):** SOAR automates many time-consuming tasks, such as orchestration of several tools, generating reports and documentation. This relieves analysts from the duty of having to manually perform these tasks and allows them to focus their expertise on more important assignments.

SOAR acts as an all-in-one solution simultaneously reinforcing different aspects of a SOC. Gartner believes that in 2022 over 30% of all SOCs with over five members will rely on SOAR to connect all aspects of their security platform.

How does SOAR affect the incident response efficiency of one SOC?

We already mentioned that SOAR improves the incident response time of an average SOC team. Here's how it is done:

- Respond to threats within minutes instead of hours: SOAR uses its automation capability to get to the bottom of incoming alerts. Major companies get bombarded with thousands of threats every

day, and without SOAR, answering every one of those alerts can take days, and sometimes even weeks.
- SOAR presents a quick visual representation with every relevant characteristic of an alert. Given that SOAR tells apart normal from suspicious alerts, it only notifies analysts if there is an unprecedented, complex issue it can't resolve with the knowledge it already has.

Instead of sifting through endless data, SOAR automatically presents fundamental tasks that analysts can take care of and automatically collects the most relevant pieces of information regarding a threat, allowing analysts to make well-informed decisions. The analysts control all the assigned tasks and manually execute actions and user choices in their own SecOps dashboard.

SOAR retains the course of action taken to remediate complex threats, thus increasing its ability to provide recommended actions when similar threats appear in the future. SOC teams need a defined set of written instructions to achieve optimal results. SOAR establishes pre-defined playbooks and effective standard operating procedures.

For each action added to the playbook, you can decide if it should be fully automated or manually executed. This is progressive automation.

How does progressive security automation function?

Security automation is often a subject of some of the most heated debates among security professionals. To automate or not to automate? But before answering that, let's delve into the idiosyncrasies of security automation:

- **Detecting and resolving false positives:** Due to its machine learning engine, SOAR is capable of differentiating false positives from actual threats. The reason why security automation is called progressive is that the engine itself is programmed to accumulate knowledge from the characteristics of different types of threats it encounters, and SOAR uses that knowledge whenever an alert with a familiar pattern occurs.
- **Adjustable degree of automation:** By configuring documented procedures of a playbook, analysts have full autonomy to choose which circumstances they want SOAR to fully automate and which areas they want to include human intervention.
- **Security automation frees up analyst time:** SOAR's security automation revolves around utilizing machine learning to apply full or semi-automation to workflow processes. Given that many of the day-to-day processes of many SOCs are repetitive, automating those repetitive processes spares a lot of time that would be unnecessarily spent if those processes were handled manually by analysts.
- **Addresses the increasing volume of alerts:** Automation resolves the flood of low-risk alerts in a regulated manner, while complying with GDPR and NIST regulations. This allows analysts to focus on mitigating more malicious threats or document playbooks.

While many are skeptical of automation, SOAR has a machine learning engine that is controlled by analysts and engineers. SOAR automation operates in the way analysts orchestrate it, not the other way around.

Even if you choose automation to take part only in low-risk processes, that would still be extremely helpful for your SOC team, as it will alleviate the burden of having to spend their time handling menial and repetitive tasks unnecessarily.

The role of SOAR in cybersecurity

SOAR improves incident response time and boosts the productivity of analysts, in some cases by tenfold, by automating thousands of menial and mundane tasks.

Here is the role SOAR plays in a typical SOC environment:

- **Force multiplier:** SOAR feeds on the abilities of other technologies and is created with the sole purpose of increasing the efficacy of a SOC environment. This means that SOAR doesn't replace other technologies, yet, it acts as a force multiplier and allows them to exceed their capabilities.
- **Connective tissue:** SOAR interacts with other technologies, such as SIEM, and builds on the knowledge extracted from such technologies to allow security professionals to make better incident-related decisions. SOAR also allows everyone on the SOC team to have a better understanding of the security strategy by offering a customizable dashboard that can be used to improve the communication among SOC members and also follow a wide range of valuable KPIs.
- **False positive detector:** Thanks to its machine learning engine, the SOAR triage and Supervised Active Intelligence (SAI) functions can successfully differentiate normal from suspicious activity and tell apart real threats from false positives. This feature is valued by analysts, in particular, as it frees their time from having to manually check every alert. Especially the ones that are low-risk and probably don't pose a threat to the organization.
- **Useful playbooks:** Thanks to its automation capabilities, SOAR allows clients to create documented playbooks which will allow them to fully or semi-automate repetitive and menial tasks. And, given that companies receive thousands of alerts on a daily basis, most of which fall into the category of low-risk alerts, this makes the presence of SOAR's automation an invaluable asset to every SOC team.

How does SOAR fit into a security network?

Regardless of the size of the organization, SOAR fits into every environment seamlessly and integrates well with both internal and external applications and technologies. SOAR allows clients to create bidirectional integrations with hundreds of security technologies.

Our own Cloud SOAR solution is particularly easy to integrate with, because it adopts an Open Integration Framework (OIF) philosophy, which allows clients to create their own integrations with little coding experience. This allows SOAR to easily work within the environment of which it is deployed and make an immediate impact.

Why is improved incident response time such a valuable aspect of what SOAR offers?

SOAR drastically improves a SOC's response time to incidents. Shortening the breach time reduces the ability of hackers and other malicious actors to cause damage to an organization.

By connecting the expertise of top security professionals, technologies, and processes, SOAR speeds analysis and response. For instance, combining the strengths of SOAR and SIEM allows security operations to be drastically more efficient in detecting and resolving cyber threats.

Advanced SOAR solutions use machine learning to read the characteristics of threats. Whether the analyst labeled the alert as a false positive or an actual threat, SOAR retains the course of action taken. This helps SOAR detect the patterns of security alerts and predict a successful response, thanks to its machine-learning engine. It's much easier to recognize the real threats when SOAR takes care of the thousands of alerts that are only meant to confuse analysts and waste their time while the real threats go by undetected.

Is SOAR a replacement for other security technologies?

As a force multiplier, SOAR boosts the productivity of SOC teams, allowing security professionals to make well-informed decisions and vastly improve response time. SOAR works with a SOC's existing security tools to connect and improve each one's potential. Instead, SOAR should be understood as the binding force that connects the dots in a SOC environment and improves the potential of every tool it interacts with.

By connecting the expertise of top security professionals, technologies, and processes, SOAR speeds analysis and response. For instance, combining the strengths of SOAR and SIEM allows security operations to be drastically more efficient in detecting and resolving cyber threats.

Is SOAR just for large organizations or it is also for small and medium enterprises?

SOAR is immediately useful for larger organizations with established SOC environments, many tools, and a number of security analysts. However, because all organizations benefit from streamlined procedures and faster response times, scalable SOAR solutions help growing organizations. Managed security service providers (MSSPs) can also help smaller organizations take advantage of the benefits of SOAR.

Choosing the right SOAR solution: What makes Cloud SOAR stand out from the competition

While there are some standard features among various SOAR platforms, like orchestration and automation, SOAR solutions differ. Sumo Logic's Cloud SOAR is focused on innovation and features a tested platform that integrates with other essential security technologies:

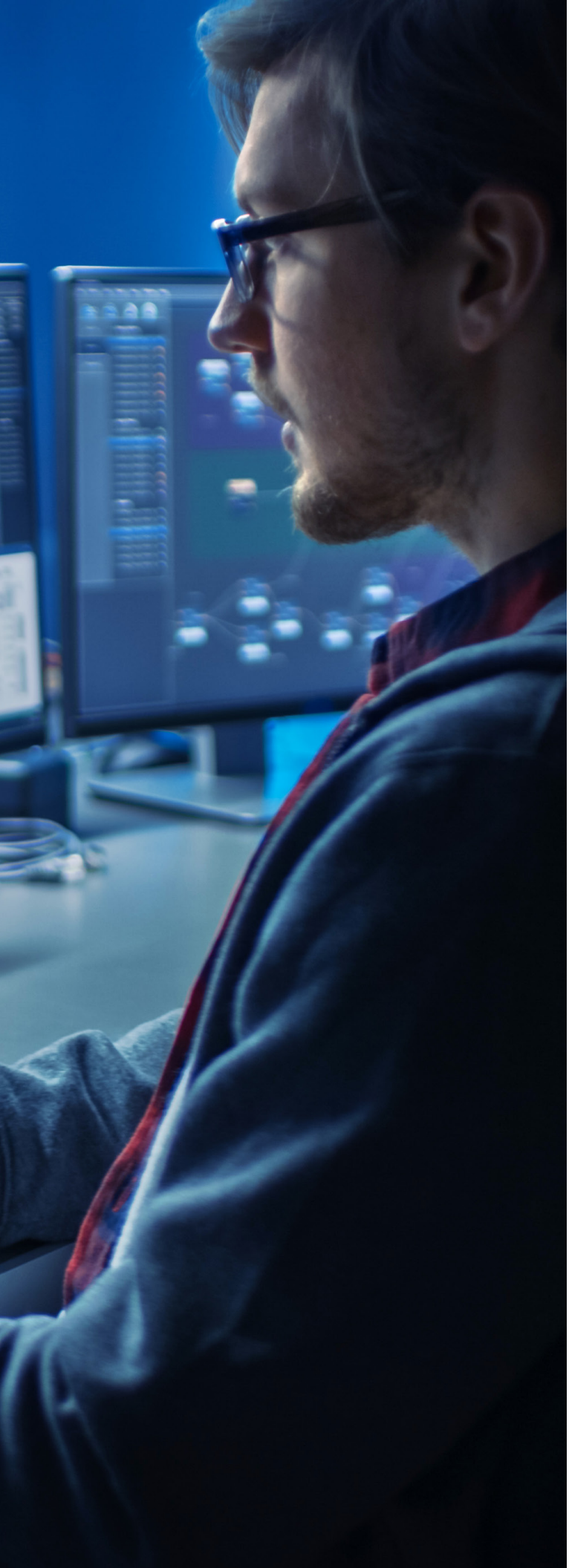
- Scalable, cloud platform leveraging ML/AI
- Automated workflow processes across all tools, with built-in or customized playbooks
- The most open SOAR platform—hundreds of connectors to other tools, thousands of automated actions
- Part of Sumo Logic's complete security portfolio--including security monitoring and analytics and Cloud SIEM

Summary

In this white paper, we discussed some of the fundamental aspects of SOAR technology. We took a closer look at how SOAR operates, as a novel technology, how it is different from SIEM, and how SOAR fits into the entire cybersecurity puzzle of modern SOCs.

We delved into what SOAR brings to the table and why it is considered a vital asset of every high-functioning SOC, and we placed a special emphasis on security automation and its invaluable contributions to next-gen security operations.

And lastly, we discussed the key differentiators of Sumo Logic's Cloud SOAR and why it is considered a pioneer in SOAR technology.



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.

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

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 08/2021