aws marketplace

WHITEPAPER

Learn how to streamline security with SOAR

A SANS Whitepaper

Written by: Christopher Crowley
Contributor: Temi Adebambo

AWS Marketplace introduction

In the "Learn How SOAR Helps You Streamline Security While Improving Your Defenses Against Cyber Attacks" webinar, SANS and AWS Marketplace explored how security orchestration, automation, and response (SOAR) streamlines your security tasks on a unified platform and improves your defenses. If you missed the webinar, you can watch it **here** on-demand.

In this whitepaper, SANS senior instructor Christopher Crowley discusses the benefits, objectives, and challenges of SOAR. He provides an overview of the shifting cybersecurity operations automation paradigm and how adjusting operational workflows to develop use cases with a team-based approach can simplify the adoption of a SOAR-focused strategy.

AWS will share how you can build and deploy a SOAR strategy with solutions from independent software vendors in AWS Marketplace.

Learn more about the featured solutions for SOAR that can be accessed in AWS Marketplace:

Sumo Logic

IBM

Vectra

Whether you are securing endpoints, identifying vulnerabilities, or safeguarding sensitive data, you can find the security software and security tools you need on AWS Marketplace to enhance protection for your entire Amazon Web Services (AWS) environment with compatible security solutions.

Learn more by visiting AWS Marketplace ›

SANS

Analyst Program

Whitepaper

Learn How SOAR Helps You Streamline Security While Improving Your Defenses Against Cyber Attacks

Written by **Christopher Crowley**

Contributor: Temi Adebambo

August 2022

aws marketplace

Introduction

SOAR stands for security orchestration, automation, and response. It is essentially writing automations, which has been possible with information systems for decades. So how is SOAR a departure from what we've done to date? The short story is that cybersecurity automations are distinct enough to warrant their own tool. Automation development is often designed to work with systems operating normally and as planned. Cybersecurity deals with systems that are behaving unexpectedly and deviating from intended or authorized actions. Handling the unexpected requires a distinct approach to automations, and SOAR tools are designed to help cybersecurity professionals construct these automations.

SOAR is not a new concept, but recent technological developments make it easier for organizations to reap the benefits of automations despite staff shortages. The challenge with most tools, including SOAR, is understanding their strengths and then deploying them in the most productive way possible. This paper will discuss the benefits and objectives of SOAR, as well as implementation challenges and their resolutions, when integrating this tool with Amazon Web Services (AWS).[1] Read on to learn how to accomplish these benefits.

Defining SOAR

Let's start with some basic definitions of the words that make up the SOAR acronym. *Security* is the restriction of a system to its intended use and the protection of the confidentiality, integrity, and availability of that system. *Orchestration* is the automated configuration, coordination, and management of computer systems and software.[2] *Automation* is the technology by which a process or procedure is performed with minimal human assistance.[3] In this paper, the somewhat academic distinction between automation and orchestration will largely be discarded.

Instead, we focus on the consolidated objective of automation and orchestration in the context of cybersecurity operations—that is, gluing systems together to perform collection of data from multiple systems, aggregation of related data, performance of repeatable tasks on behalf of cyber professionals, and guidance of workers through complicated sequences and decision making. This is the standard work of cybersecurity staff, and SOAR is intended to help you increase performance accuracy and precision, as well as to accomplish tasks more quickly. *Accuracy* is being correct, and *precision* is being exact and consistent in that exactitude. These are attributes we aspire to be in our work: accurate, precise, and fast. This is what SOAR provides us.

---

[1] This paper mentions product/solution names to provide real-life examples of how security tools can be used. The use of these examples is not an endorsement of any product/solution.

[2] "Orchestration (computing)," https://en.wikipedia.org/wiki/Orchestration_(computing)#cite_note-Erl-1

[3] "Automation," https://en.wikipedia.org/wiki/Automation

The last word to define in the SOAR acronym is *response*. We respond to problems in our information systems. In cybersecurity, response is fairly complicated. We often call this "incident response" or "incident handling." This adds the notion of an incident, which is an issue or a problem. The situation is that we often don't know if it is an actual incident at the start of our response, so we need initial validation and verification after we have been given a clue that we need to start our response. That initial clue is either in the form of an alert (derived from our SIEM or some other tool designed to notify) or a report, perhaps from a person, such as a customer or an employee noticing that something is not behaving according to expectations.

Response, then, is our effort to perform initial verification, short-term mitigation, fundamental root-cause analysis, business continuity in the face of actual incidents, and long-term enhancement of our systems to be more resilient to issues.

Here's where SOAR technology can provide assistance: uncertain signals, minimal initial clarity, requirements for verification, correlation of data from many systems, rapid responsive actions that may impact our business operations, detailed analysis, and long-term remediation. Let's take a look at what you can do to make the most of SOAR technologies.

Benefits and Objectives

When you think of what SOAR does for you, think of an analyst equipped with a multitude of widgets to accomplish the repetitive and routine—and even some things an analyst wouldn't necessarily think of until someone suggests that it is a good idea. Don't think of a fully automated assembly line to build automobiles.

The value proposition that accompanies SOAR is straightforward: It reduces the human effort of performing tasks (which lend themselves to automation), facilitates the fusion of data between multiple systems, and guides the analyst on the journey of exploring uncertain situations.

SOAR provides enhanced repeatability, precision, and accuracy as well as a corresponding increase in speed, because the human analyst doesn't need to manually perform the tasks.

SOAR provides enhanced repeatability, precision, and accuracy as well as a corresponding increase in speed, since the human analyst doesn't need to manually perform the tasks.

Maturity increases because repeatability increases. A likely improvement is that repeatability will highlight what can and can't be done, with a corresponding increase in capability due to clear understanding of capability deficiencies.

Workflow—interconnected sequences of actions—can be defined in terms of modular actions that can be performed. The common approach to developing a workflow is to consider possible scenarios, then fill in details about what could be done and what additional information might be useful in each scenario. After running through a scenario with an automation tool, an analyst will likely identify additional steps to perform. This information can be captured in the SOAR tool, and the workflow can then be updated for the next scenario.

This repetition and workflow enhancement cycle is both a benefit and an objective of a SOAR tool. The SOAR tool serves as a knowledge management tool. It aggregates the collective wisdom of the analysts performing the work through updates and revisions. Further, it facilitates expression of management agreements with constituents to do things in a very specific way.

Let's explain this via an example. The paper will identify specific implementations in AWS later, but it's useful to illustrate the circumstance here. Assume there's an Amazon Machine Instance (AMI) where a specific event was flagged by an alert via a SIEM detection. An incident is declared, and investigation proceeds. This AMI is related to an important service. Cybersecurity staff thinks it's a good idea to collect a snapshot of the system, so it pauses the instance to do so. That's suboptimal from the organization's perspective because that has an operational impact. Instead of operating in an ad hoc, pause-then-collect approach, let's think about how to do this with a SOAR tool.

Prior to the incident, the cybersecurity team discusses using a SOAR routine for containment of AMIs should there ever be an incident. Organizational AMI priority levels are determined, and autoscaling and warm-pool strategies are defined for the varying application priorities. A method for establishing adequate Amazon Elastic Compute Cloud (Amazon EC2) pool resources is defined when pausing an instance is required in a cybersecurity-directed action. Instead of manually pausing and collecting an AMI, a cybersecurity containment routine is enacted, and the appropriate steps are performed to assure ongoing availability of resources prior to pausing the AMI. This is the objective of our deployment.

If you take this approach, you can collect the wisdom of the professionals who created the application architecture to begin with. You can harness the thoughts of the cybersecurity staff who want to protect the information resources, utilize your vendor technologies for detection and response in a cloud-native fashion, and leverage the native capabilities of the AWS resources.

Cybersecurity Operations Automation Paradigm

To accomplish alerting from systems, cybersecurity professionals typically discuss use case development or detection engineering. There is a shade of difference between them, but the overall intention is to configure systems to correlate enough data elements to identify when there is a security incident that needs to be addressed. Organizations may lack the staff to investigate every single event that triggers an alert, so reducing false positive alerts and prioritizing alerts is key. There are many strategies and techniques involved in this prioritization and selection of alerts. Use case development and detection engineering are fundamental efforts by cybersecurity teams because they maximize the true positive alerts to notify them when there is in fact an incident that needs to be addressed.

Please note: Hunting is considered an additional critically important element of security operations, but it isn't addressed beyond this mention because it is not intended to be automated or orchestrated in a repeatable fashion. Hunting is an ad hoc, responsive, exploratory, developmental, flexible, creative effort. A closely related act that is sometimes also labeled as "hunting" involves historical analysis with new indicators of compromise (IoCs), and this process can certainly be automated and orchestrated—for example, searching through the last 30 days of DNS logs for a domain that was newly identified as hosting malware over the past month. That's a case of historical analysis, not hunting. Hunting involves not exactly knowing what you're looking for, but nonetheless seeking indications of incidents. Historical analysis is looking in old data for newly identified IoCs.

Developing a workflow that ingests ideas for use cases and detections, performs the appropriate assessment of available data, implements the detection in a system(s) to alert when there is a problem, and then monitors the performance of those alerts to tune and optimize them going forward is an absolute necessity for security operations. If you don't have this workflow in place, a brief version of the recommended sequence is the following: one scenario of interest is selected and decomposed into a story line (potentially separate into distinct use cases), data artifacts are identified, and detection opportunities are identified (how to differentiate problems from the normal). Next there is enrichment through correlation with related internal data or external threat intelligence, test scenario development and technical implementation, and performance assessment and review, revision, or retirement.

Developing a workflow that ingests ideas for use cases and detections, performs the appropriate assessment of available data, implements the detection in a system(s) to alert when there is a problem, and then monitors the performance of those alerts to tune and optimize them going forward is a highly recommended practice for security operations.

This workflow isn't intended to be implemented in the SOAR tool, but the technical implementation of these actions is appropriate for the utilization of a SOAR. If this sequence (or a similar use case creation workflow) isn't already part of security operations, the team's operational method should be adjusted to refocus its emphasis on a workflow that has a repeatable, team-based approach to developing use cases (or engineer detections) that is documented and refined on an ongoing basis. Once this adjustment is made, embracing an automation and orchestration operational paradigm is greatly simplified.

Who is responsible for this use case development pipeline? The cybersecurity staff have the fundamental responsibility for it, but they will need to collaborate closely with IT systems architects, administrators and engineers. They'll also need input from risk management and audit teams to set priorities. Business continuity planners can provide substantial insight on how to implement remediations for cybersecurity incidents. The recommendation is to consolidate incident handling and containment, eradication, and recovery efforts to the same actions taken for business continuity plans.

The challenge is that cybersecurity staff members are often working a large queue of tickets, consulting on high-priority projects, and handling the unexpected. So, how can they make time to implement a new technology and shift the fundamental way of working?

The resolution is multifaceted, but straightforward. First, identify at least one, but preferably two cybersecurity team members to be responsible for the SOAR technology operational improvement for the long term. Train these people in workflow development and provide them with diagraming and modeling software so they will be able to sketch and formalize the sequence of actions they'll need to implement in the SOAR tool. Often, the tools provide a visualization of the SOAR sequence—a WYSIWYG sequence development tool. Having an additional tool to empower people to think in workflows, actions, tasks, and decisions is extremely useful. The people working on this project should have a thorough understanding of cybersecurity practices and attack techniques and consider their agenda and objective to be the expansion of capability with the relentless pursuit of efficiencies and improvements. The role requires both technical acumen and a drive to improve things.

The people who are tasked with orchestrating and automating face another challenge: the legacy of solutions that were "good enough" at the time and never get addressed fundamentally. The aphorism "Nothing lasts longer than a temporary fix" is exceedingly true in the information technology domain. The old, uncoordinated, broken workflows that are present aren't going to be magically repaired by a SOAR tool. But, the tool's purchase and implementation represent a phenomenal opportunity to reconcile those misaligned sequences of effort.

Another challenge that comes along with implementing a SOAR tool is educating staff on its power. Here's a simple analogy that is relatable for almost everyone:

> People are generally trained to drive a car on the public road. There are stop signs, yellow lights, and other drivers. Imagine then if you were invited to drive a race car. You might not understand how to turn it on! Compared to a regular car, a race car has different objectives and challenges and requires related but differently applied skills. It's no longer about being considerate and moving to the right when a faster car wants to pass you. It's about being faster in every corner, out-positioning other drivers, and maintaining the fastest lap times.

Likewise, your SOAR-enabled staff may have a bit of an adjustment to absorb the newfound power of the SOAR technology. Solving the challenges heretofore about not having access are but an implementation sequence away.

Now there's another challenge: People who embrace automation must accept turning control of systems over to the computer to automatically perform actions that previously were controlled by them. How can we develop confidence that the automation tool can maintain security of the data and sustain access? The answer is straightforward: testing. We test, test, test, and test some more. We develop small tasks, test them, and gain confidence in specific and constrained circumstances. Then we expand the contexts in which we automate and test some more. See Figure 1.

The real key here is to develop another workflow, and this is often referred to as *DevSecOps*. Coordination with IT teams for authorized containment actions is a great example. What do cybersecurity teams do that isn't just a standard move/add/change actions? Truth is, almost nothing. We perform standard move/add/change actions, but in the midst of uncertainty in challenging situations. Mimicking the IT move/add/change actions might help them to formalize and enhance maturity in their own processes.

This makes sense, because this is the operating model for cloud deployments generally. It should be the model for internal IT systems, but few organizations have accomplished a mature DevSecOps pipeline. Let's turn our attention to AWS to explore specific tools.

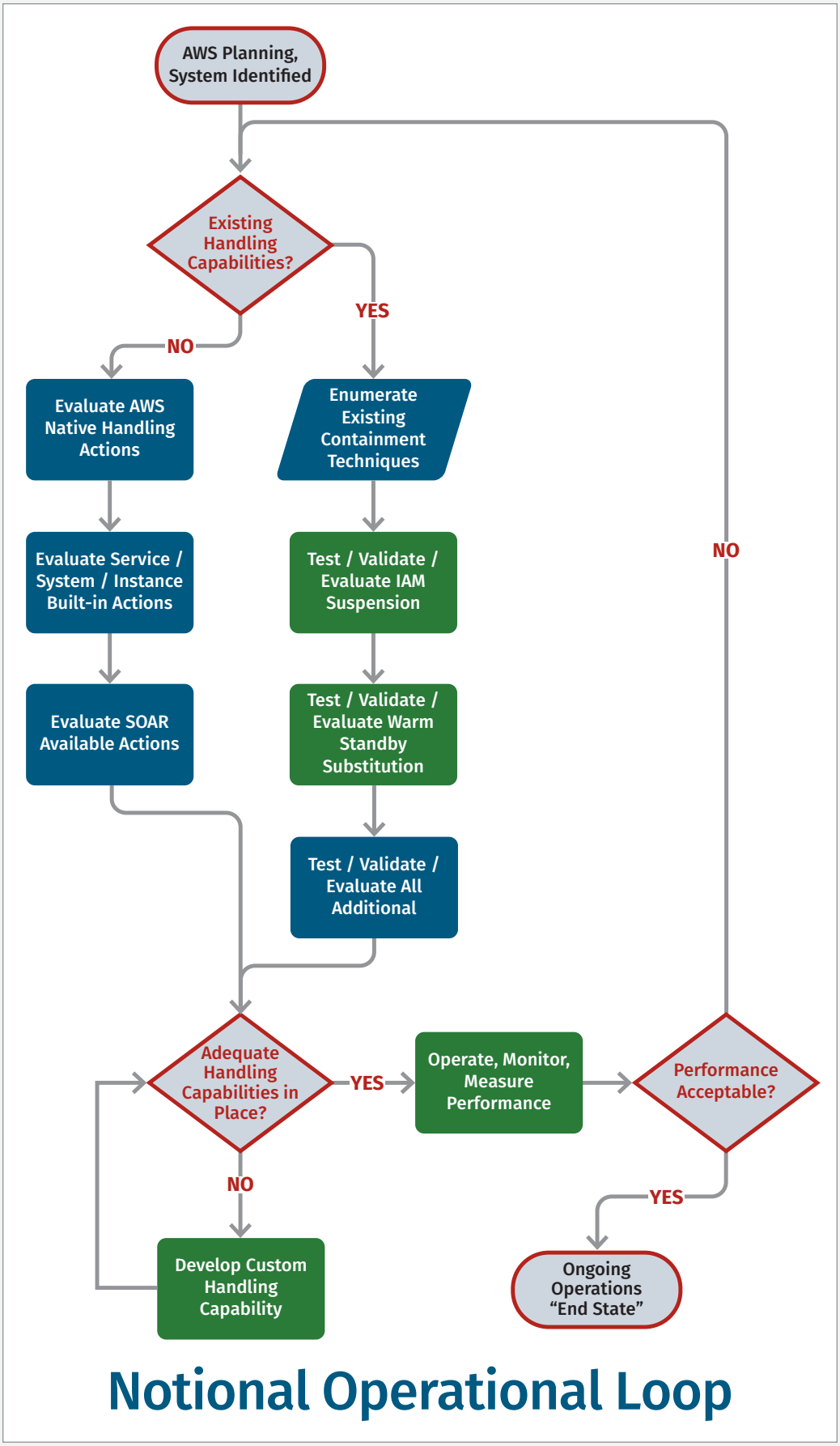


Figure 1. Workflow

Native SOAR Capabilities in AWS

First, it's important to acknowledge the extent of automatable and orchestration capability native to AWS. We'll start with fundamental components that can be automated and move on to the automations that are natively in place. After, we'll explain what the AWS Marketplace is and highlight a few products that can assist with the automation effort.

First, be sure you're matching the security offering to the appropriate AWS product. There are a multitude of product categories[4] this paper won't discuss SOAR use within—for example, machine learning, satellite services, robotics, or blockchain. The principles discussed here are applicable, but tuning the SOAR to be optimal requires the nuance of those domains of expertise. We will discuss the fundamental service offerings in the context of SOAR, such as Amazon EC2, AWS Lambda, Amazon Simple Storage Service (Amazon S3), and Amazon VPC.

The security and compliance documentation section lists 18 native offerings. Figure 2 is a snapshot of these offerings as of July 2022.

The AWS Artifact tool is available to start from compliant deployments, such as ISO and AICPA service-oriented control. You can identify non-compliance with the specifications via AWS Audit Manager. This can be automated to perform assessments and reporting as needed.

Logging is a fundamental action that is necessary to enable in some cases, but it's more important to use the available data to monitor your AWS deployments. Unless the task is specifically transferred to a third party, it is still your responsibility to review the activity on your deployed resources for unauthorized activity. Tracking this activity through logs is a baseline action. Automation to assure the logging was collected is recommended and straightforward to implement. This paper previously described a workflow for use case development, starting with a scenario of what might go wrong and then looking for data sources to help to identify when that's happening.

These logs are part of that portfolio of data. Orchestration can utilize this data, by selectively retrieving it only when it is relevant to a scenario of interest. The primary services for collecting logs are AWS CloudFront access logs, Amazon CloudWatch, and AWS CloudTrail logs. These can be configured on a number of services. Each service has distinct items collected, so be conscientious to understand the distinctions between the exact fields collected in Amazon S3 logs and Amazon VPC Flow Logs, for example.

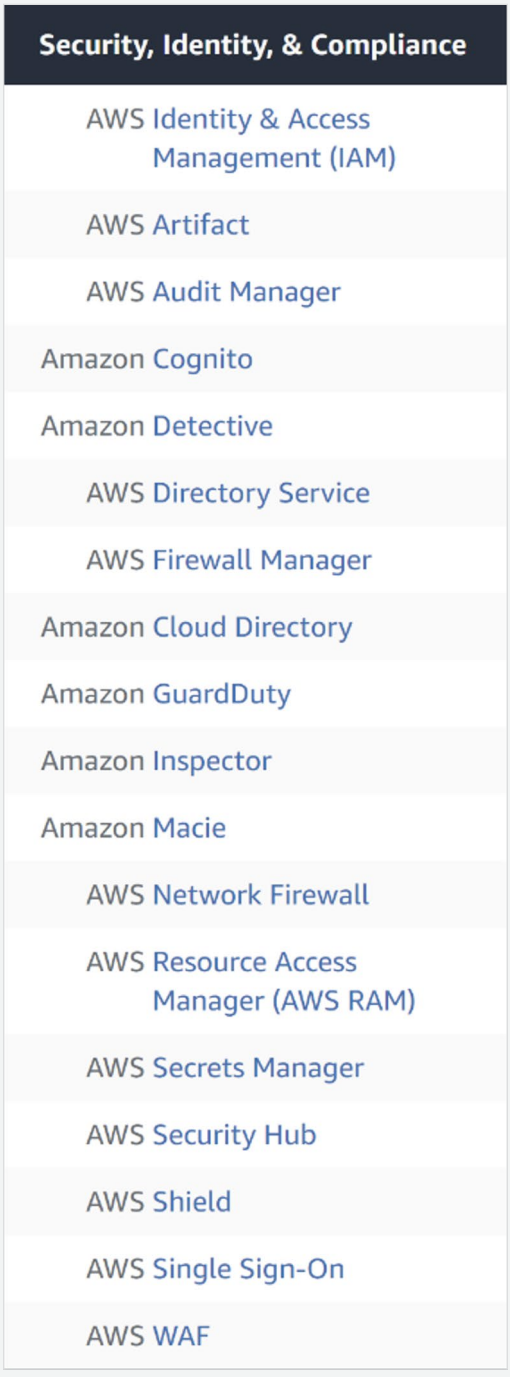


Figure 2. AWS Documentation Page: Security, Identity, Compliance

[4] "AWS Documentation," https://docs.aws.amazon.com/index.html

AWS Identity and Access Management (IAM) is a critically important facet of your security portfolio. Because cloud resources are available to anyone connecting to them, the IAM authentication and configuration is frequently the only thing that prevents a bad actor from accessing your important resources. Brute forcing passwords is a common attack that can be identified and shunned.

Perhaps you want some help with this review of data? One available place to start is Amazon Grafana. While not specifically a cybersecurity tool (we'll identify a few of those later), it can help with visualization and relationships within logs. Of course, there's an AWS Managed Grafana service available if you don't want to deploy Grafana on your own. AWS Management Console and AWS Resilience Hub are primarily operationally focused. Amazon Macie is a cybersecurity focused web application intended to help cybersecurity professionals address protection requirements.

AWS Security Hub is intended to be the singular collector of information for your AWS deployment. It assists with the identification of issues and assists with alerting. This is intended to help with fundamental concerns such as the aforementioned brute force attempts.

Using native capabilities, much of the standard incident handling playbook could be automated. Take the example of a weak password allowing unauthorized access to an account. Let's consider the scenario, starting from receipt of an alert from AWS Security Hub identifying potentially unauthorized account access. An analyst would review the presented data, make a decision about the likelihood of the account access being authorized or not, and take appropriate containment actions.

Let's consider the sequence involved. First, it is generally considered best practice for more restriction earlier in the incident-handling sequence, so an account with an even moderate concern of being affected would be temporarily suspended. The suspension would be applied while investigation proceeds. Current authentication data would be collected in an orchestrated fashion for the account across various AWS resources as well as related resources such as email, domain, VPN, and VPC authentications. Since this isn't an insider scenario, the communication channels available (email, chat/messaging, and SMS) would receive automated messaging indicating the account has been suspended due to suspicious activity and would remain suspended until final review is completed, which should not take longer than some duration (likely 120 minutes). The message would indicate that if the account is determined to be compromised, it would require some sequence for identification and subsequent release.

Similar coordinated workflows would be developed for the following events: compromised Amazon EC2 instances, AWS Lambda functions (or any hosted code or machine instances) suspected of receiving unauthorized code updates, suspected unauthorized data access, or employees suspected of unauthorized data access. In these scenarios, we can identify the likely workflow of activity and then map out what we can simply automate using native capabilities in AWS: activate standby capability, pause suspected instance, snapshot, review, decide, remediate (as needed).

Because you're likely busy already and don't want to have to program this sequence yourself, it's reasonable to consider if a SOAR tool has been configured and deployed already within AWS that will help you to quickly accomplish this sort of orchestration and automation.

The SOAR solutions offered directly within AWS Marketplace may be few, but the SOAR market is a niche cybersecurity product. An AWS Marketplace search for SOAR (performed on July 7, 2022[5]) turned up 45 hits. Not all are specifically SOAR solutions, although they all have relevance to cybersecurity. There are other vendor solutions that work with AWS, to be sure, but those are 45 matches for SOAR specifically within AWS Marketplace.

When your team already knows a tool, it might be best to simply continue to use that tool and retain the already developed capabilities. If you can leverage the cloud-native instance of that which has already been integrated and tested by the vendor, then this represents a low-drag strategy for keeping your team's skillset and minimize the deployment overhead for new territory.

A few examples of the SOAR-specific products include Splunk SOAR (which many people still refer to as Phantom), IBM QRadar SOAR, and Sumo Logic SOAR. Each has its distinctive SOAR capabilities, available via AWS Marketplace.

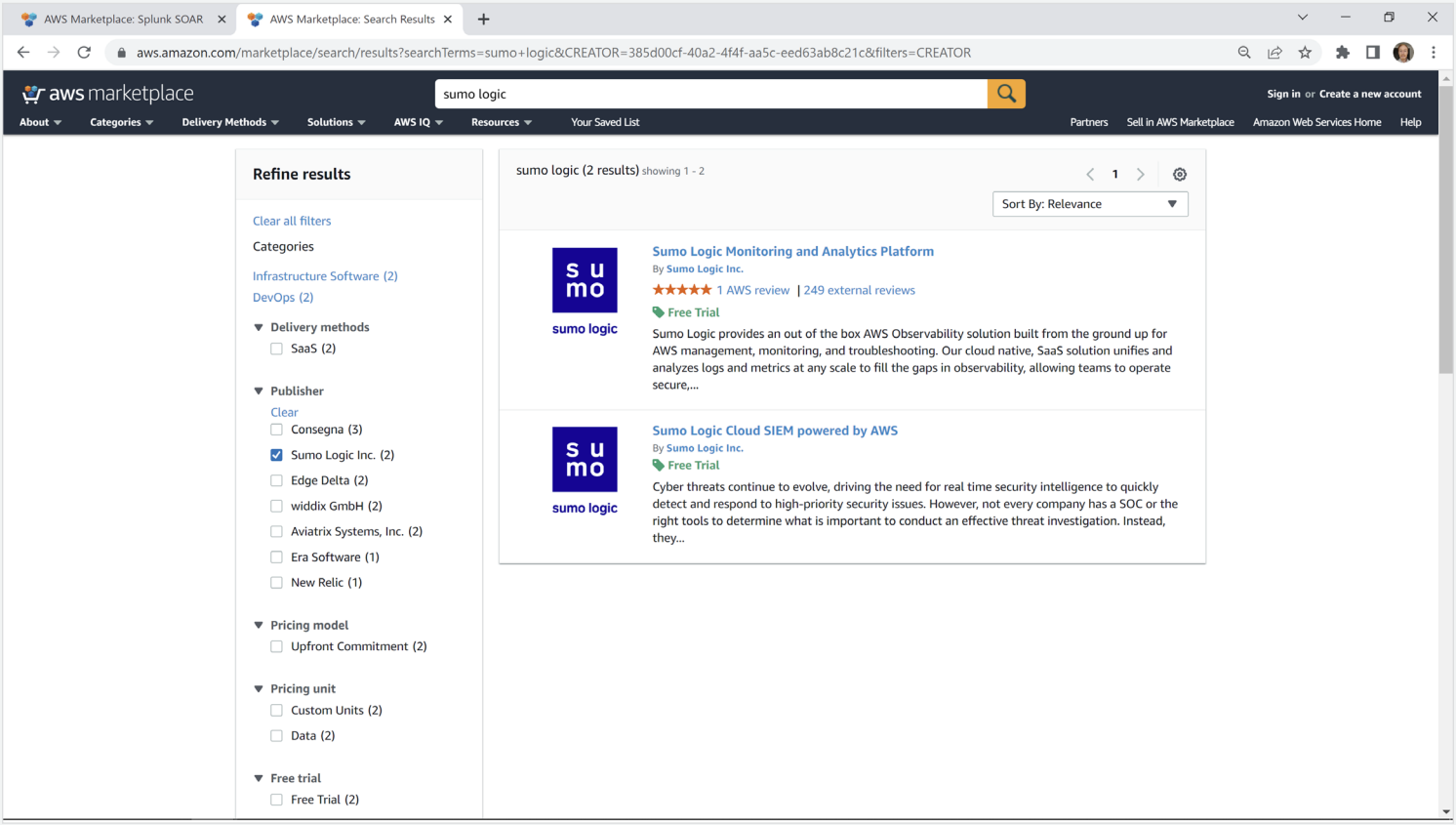


Figure 3. Sumo Logic SOAR in AWS Marketplace

[5] https://aws.amazon.com/marketplace/search?searchTerms=SOAR&sort=AVERAGE_CUSTOMER_RATING-DESCENDING&pageSize=50

Next Steps

If your organization performs cybersecurity duties, even if it isn't consolidated into an operational SOC, then you should consider effective ways to drive toward repeatability, accuracy, precision, expedience, and stable transitions as team members join and depart from the cybersecurity team.

This paper provided guidance on the orchestration, automation, and response that is captured and bundled within SOAR tools. The most fundamental aspect of deploying and using a SOAR tool, however, is outside of the tool itself. Workflows around use case development and the mature performance of investigation and response are what make a SOAR tool effective for your organization.

While it would be optimal if your team is already mature operationally and can effortlessly absorb a new tool such as SOAR to make it even better, the team may have weaknesses that need to be remedied. The SOAR tool is seen as a technology to provide those remedies.

This may be seen as an opportunity to get well, but the right approach is to use the SOAR deployment as an opportunity to take a renewed approach to health and wellness within your cybersecurity operations. Leveraging solutions provided in AWS Marketplace to expedite that renewal is an optimization if your organization is using AWS to host solutions.

Sponsor

SANS would like to thank this paper's sponsor:

aws marketplace

sumo logic

Discover how Sumo Logic helps you extend the effectiveness of your SOC

Discover, implement, and optimize security automations with AWS services and third-party solutions

SOAR is not a new concept, but recent developments in technology offerings make it easier for organizations to reap the benefits of automations despite staff shortages. The challenge with most tools, including SOAR tools, is understanding their strengths and then deploying them in the most productive way possible. Explore the benefits and objectives of SOAR, as well as implementation challenges and their resolutions when integrating this tool with Amazon Web Services (AWS).

How AWS customers are leveraging Sumo Logic to implement SOAR

Sumo Logic Cloud SOAR improves SOC productivity, increases visibility, enhances incident response, and helps security professionals make insightful decisions. Key features include:

- Threat focus that leverages machine learning to significantly reduce false positives and duplicate events to keep organizations prepared when real threats strike.
- Tool orchestration that connects disparate tools to fully automate incident response and leave time-consuming, manual tasks behind—plus, automating incident response boosts the efficiency of the entire team.
- Better collaboration by automating the full incident lifecycle to ease the burden on security analysts, while helping to successfully pinpoint real threats and coordinate an effective response across tools and team members.
- Customizable reports and dashboards with relevant templates that create greater visibility for KPIs and make collective improvements across the SOC team.

Why use AWS Marketplace?

AWS Marketplace is a digital software catalog that makes it easy to find, try, buy, deploy, and manage software that runs on AWS. AWS Marketplace has a broad and deep selection of security solutions offered by hundreds of independent software vendors, spanning infrastructure security, logging and monitoring, identity and access control, data protection, and more.

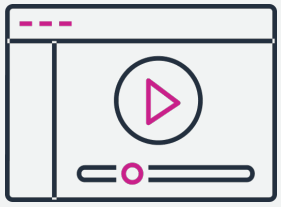
Customers can launch pre-configured solutions in just a few clicks in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with entitlement options such as hourly, monthly, annual, and multi-year contracts.

AWS Marketplace is supported by a global team of solutions architects, product specialists, and other experts to help IT teams connect with the tools and resources needed to streamline migration journeys to AWS.

How to get started with SOAR security solutions in AWS Marketplace

Security teams use AWS native services and seller solutions in AWS Marketplace to help build automated, innovative, and secure solutions to address relevant use cases and further harden their cloud security footprint.

The following resources can help you get started:



Watch the Webinar

Learn how SOAR helps you streamline security while improving your defenses against cyber attacks.

View On-Demand

Discover Solutions

Find the tools you need to implement security orchestration, automation, and response (SOAR) in AWS.

Visit AWS Marketplace

Talk to an Expert

Get connected with a solution architect that can share best practices and help solve your business challenges.

Get Connected