WHAT IS SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)?

A relatively new platform for data security is Security Orchestration, Automation, and Response—better known as SOAR.

Security teams often use the terms SOAR and SIEM interchangeably. (SIEM refers to System Information and Event Management.) But these practices are two separate security solutions with complementary capabilities. In fact, both tools work hand-in-hand so well that SecOps teams often use the technologies in tandem to optimize their security operation centers.

Let's take a look at SOAR and what it can do for you.

SIEM functions at a glance

To fully understand SOAR, it's helpful to start with what it is not: SIEM. SIEM solutions focus on:

- Log data storage
- Threat intelligence
- Data aggregation
- Threat detection
- Notification

Users in highly regulated industries also use SIEM software's ability to store and organize log data as

proof of compliance with government regulations and security standards.

The SIEM process

All of this is done with the end goal of gaining near real-time insights into what's happening in an enterprise's security ecosystem from one single point-of-view. Common SIEM tasks include:

- Collecting log data from many internal sources
- Aggregating and normalizing the data
- Analyzing the data to detect possible cybersecurity breaches
- Sending alerts or utilizing established protocols to shut down a security incident

The challenge of SIEM tools lies in the final step of the process, which often requires a team of security engineers and analysts to continually tweak software alerts. This step is human-resource intensive: it can require many man-hours of continuously managing rules and uses cases, ensuring that normal activities are not mixed up with suspicious ones.

A properly tuned SIEM, run by a properly staffed security department, can be critical to an organization's detection and incident response capabilities. However, manual remediation challenges and other shortcomings of existing SIEM solutions have left a hole: how should SecOps teams manage and respond to endless alarms from too much data?

Enter SOAR.

What is SOAR?

SOAR platforms are a collection of software solutions and tools designed to browse a broad range of sources and collect:

- Security threats
- Data
- Alerts

SOAR tools then analyze this disparate data through a combination of human and machine learning to understand and prioritize incident response activities.

Traditionally, a human would have to review, remediate, and standardize a variety of actions into a digital workflow to define incident response procedures. But that process takes a lot of resources and introduces human error. SOAR solutions can define your incident response procedures for you, by combining a variety of data tasks including:

- Data gathering
- Case management
- Standardization
- Workflow
- Analytics

This format can then be handled by automated machine-driven activities.

Let's look at the three security tasks that comprise SOAR:

Orchestration

Orchestration is the act of integrating a wide array of technologies and connecting security tools, both security-specific and non-security specific, in order to make them work together while improving security incident response times.

That means SOAR solutions can perform much more than ingesting and analyzing alerts from your SIEM system. SOAR solutions can also ingest and analyze alerts from:

- User and entity behavior analytics (UEBA)
- Threat intelligence platforms
- Incident response platforms
- Intrusion detection and prevention systems (IDPS)
- A whole host of others

Having multiple security solutions often from multiple vendors can improve the overall security of your data. Yet it often results in more alerts, including false alerts, as well as the time spent by dedicated and highly-trained staff to investigate each one.

Automation

Automation is the machine-driven execution of security operations-related tasks. Tasks that were previously performed by humans can be performed and standardized by SOAR solutions:

- Automation steps
- Decision-making workflow
- Enforcement actions
- Status checking
- Auditing capabilities

With SOAR, these tasks are no longer a drain on manual resources.

Response

Now, security orchestration is pulling in and analyzing alerts from across your IT infrastructure. Repetitive manual tasks are automatically designed and handled.

That free time means security teams can focus on actual security incidents and resolutions. SOAR allows analysts to collaborate on incidents by extending their analysis further than SIEM's log data, further allowing these analysts to determine remediation for potential vulnerabilities to prevent further attacks. SOAR tools also include case management modules. These modules are useful in communicating learnings and delivering threat intelligence, further improving proactive response times to future attacks.

SOAR use cases

In the relatively short time SOAR platforms have been around, security teams have utilized these tools in creative ways to achieve more in less time, while still allowing for human decision-making when it's most critical. A few examples of the most common use cases for SOAR are:

- Phishing emails
- Malicious network traffic
- Streamlining vulnerability management
- Meeting service level agreements
- Case management

SOAR example

Let's look at phishing emails as an example. SOAR is perfectly positioned to enable automatic triage and examination of suspected malicious emails.

Over the past several years, many high-profile data breaches have resulted from carefully crafted phishing emails which have made it one of the most critical issues faced by security teams. If a suspicious email is received, SOAR can extract artifacts such as header information, email addresses, URLs, and attachments.

You can then use your various tech integrations to analyze this data. If determined malicious, the SOAR platform can take automated or semi-automated actions to contain the threat. Security teams define the next actions. In this case, next steps could be:

- Quarantine or delete the email
- Search and delete other instances of the email in other user's accounts
- Block IP addresses or URLs
- Ban executables from running
- Quarantine the user's workstation

Using SOAR to examine and respond to an organization's individual uses cases like phishing emails can reduce investigation times from hours to minutes by automatically containing the attack while minimizing risk to the organization. When SOAR is implemented well and built on top of strong and accurate data, it will allow security teams to streamline their security operations centers by reducing the load of low-level security events consuming their time.

Additional resouces

For related reading, explore these resources:

- BMC Security & Compliance Blog
- Security Analytics: An Introduction
- SIEM vs Log Management: What's the difference?
- Tracing vs Logging vs Monitoring: What's the Difference?
- AIOps Machine Learning: Supervised vs Unsupervised