GlobalLogic®

Understanding the SOAR Canvas of Cybersecurity

Author by:
Nimasha Jain

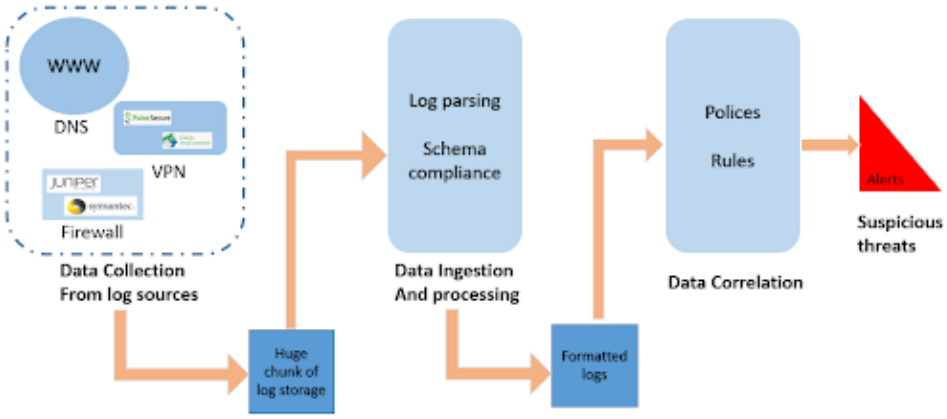
Contents

Cybersecurity is a huge term with many components, but a crucial element is dealing with threats. Threats are red flags to IT infrastructure (hardware and software) due to malicious activities. Security operation teams use Security Incident and Event Management tools to detect, analyze, process, and parse information in terms of traces, logs, and events to identify threats.

When there is an indefinite number of applications leading to indefinite logs, a Security Operation Center (SOC) cannot rely solely on manual effort. It would need many competent and reliable sources working in conjunction. Manual efforts may not be enough for threat intelligence and triaging, which makes Security Orchestration, Automation, and Response (SOAR) a prominent part of the cybersecurity picture to remediate suspected threats.

The SIEM Process

Security Incident and Event Management (SIEM) tools provide threat detection mechanisms that work on different log sources.



The SIEM process is intended to detect anomalies by performing the following steps:

1. **Data Collection:** Each device/piece of software leaves traces in the form of logs that are collected and stored in SIEM tools. The range of log sources varies from endpoints, antivirus software, cloud email, archives, identity and authentication, emails, and hardware devices like a router, etc. To have a competitive edge, SIEM tools need storage capabilities to collect an enormous amount of logs for a minimum period of time, which is provided by available cloud technologies.

2. **Data Ingestion:** When logs are collected, they are raw with huge chunks of information that require normalization. Logs are cleansed and normalized to make them ready for parsing and indexing, then used further for data enrichment. Logs are fed to parsing engines that make them schema-complaint and provide metadata fields for further traversal.

3. **Data Correlation:** Formatted logs are applied with policies and rules to raise alarms/alerts to determine a potential data breach, threat, attack, or vulnerability.

As per the process, we have an indefinite number of devices leaving traces that form the logs. Each is its own kind and is fed to parsing engines and rule engines to raise alarms. SIEM tools need further high-end SOAR for deep work to accomplish the following:

1. Simplify threat response workflows
2. Switch off the noise of false positive alerts
3. Provide actionable threat intelligence
4. Minimize Time to Respond (TTR)
5. Handle incidents
6. Manage forensics and vulnerability

Defining SOAR

Gartner defines Security Orchestration, Automation, and Response (SOAR) as "solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform."

SOAR combines incident response, automation workflow, and threat intelligence platforms. With SIEM's advanced platforms, SOCs will see a high number of alerts, but they won't be able to look into each one. SOAR platforms not only power SIEM tools to automate workflows on threat mitigation but also enhance User and Entity Behavior Analytics (UEBA) capabilities, which accelerate threat intelligence capabilities. The orchestration of alerts by automated workflows and incident responses enables businesses to take action on crucial threats. Some threats may just be noise, while others could be fatal to a whole organization's IT system.

Let's now move ahead to explore SIEM a little further and why it requires SOAR.

The SOAR Canvas

SOAR is divided into four core engines to do the deep work mentioned above:

1. **Workflow and Collaboration Engine**

   Playbooks are actions working in collaboration that look into suspicious activities that are flagged in the form of threats. There are pre-built or customized playbooks that can run multiple actions sequentially or concurrently, depending on the choice of the SOAR tool.

   For example, say a malicious Uniform Resource Locator (URL) is found in an employee email and identified during a scan. A playbook can be configured to block the email, alert the employee of the potential phishing attempt, and blacklist the sender's Internet Protocol (IP) address. SOAR tools can also trigger follow-up investigative actions by security teams if necessary.

2. **Ticket and Case Management Engine**

   Whenever a threat is reported, it is marked as an incident in an SIEM or third-party integration tool. At the same, it can also be marked as a case where analysts can attach the logs, summary, and investigative details for analysis. SOAR platforms provide the case management engine to drill down into any incident to draw vital details for a further course of action.

   Similarly, SOAR platforms are integrated with third-party platforms like JIRA and ServiceNow to raise tickets and attach the details from an SIEM's threat alerts.

3. **Orchestration and Automation Engine**

   Sometimes security orchestration and automation are used as synonyms, but they are actually different. Security orchestration integrates security tools, facilitates automation, and combines dashboards to increase the overall efficiency of SecOps teams. Security automation is the ability to execute a sequence of tasks related to security workflow without human intervention to decrease incident response times.

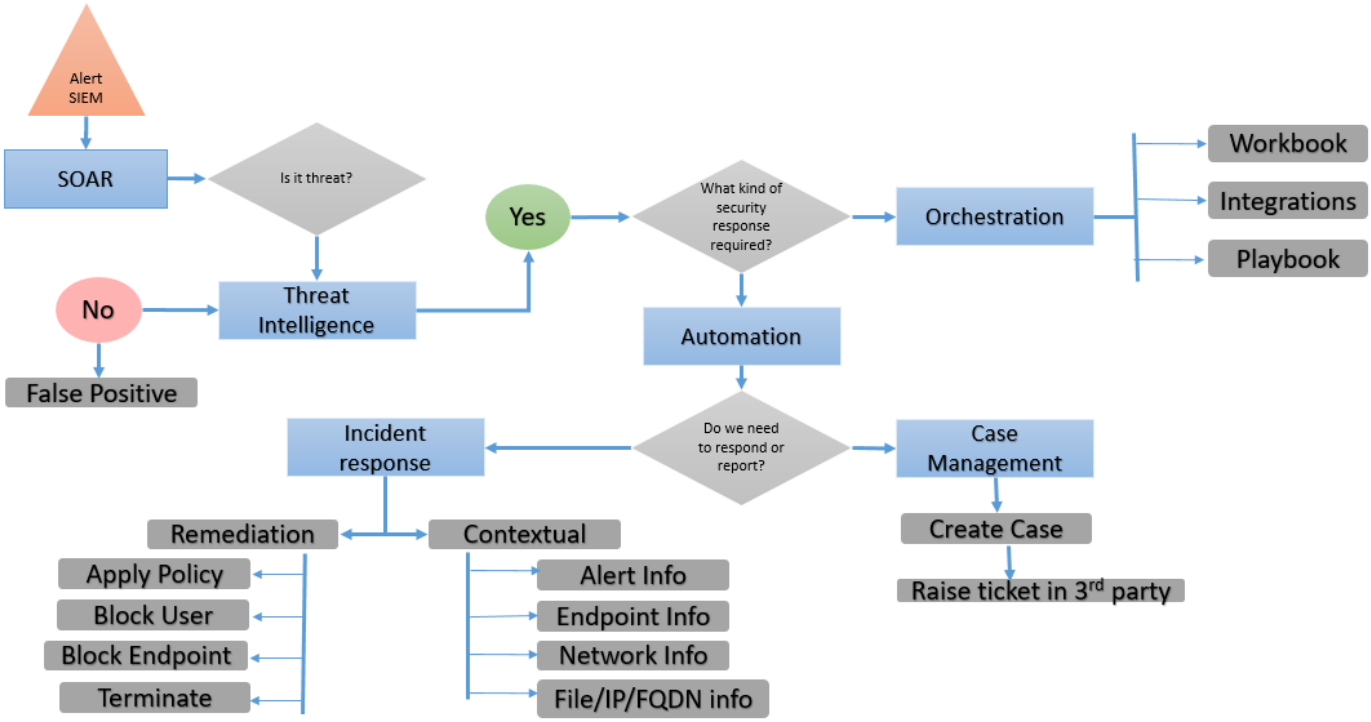
   It is the combination of orchestration and automation engines that enables incident response on third-party systems as well.

4. **Threat Intelligence Management Engine**

   SOAR tools are often either integrated or imbibed with User and Entity Behavior Analytics (UEBA) platforms to predict threat patterns in order to take proactive measures. It often decreases the time it takes to detect threats in SIEM.

Realizing the Full Potential of SOAR

As mentioned above about SOAR's four engines, it is becoming increasingly important to define SOAR platforms in a way that it is not only useful but efficient. The processes, operational metrics, and documented workflow along with supported technology integration lay the foundation for efficient SOAR usage. The diagram below shows the workflow and decision-making capabilities offered by SOAR.

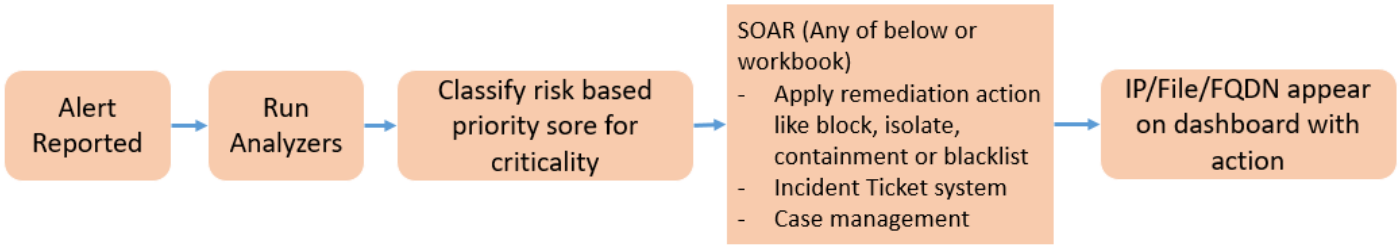


There are a few calls that systems need to make, such as "Is it a threat?" or "Does it require a report or a response?" These questions lead to decisions regarding how to use the full potential of SOAR, whether by automation or orchestration. Incident response engines offer a variety of actions to respond to threats. Remediation actions, such as applying policy to endpoints, blocking a user, adding a file hash, terminating a process, and blacklisting IP/FQDN are just a few measures that stop threats from going deeper into a system. A few enrichment actions like contextual actions that add more info to a device/endpoint/network make it easier for a security analyst to make decisions about suspicious activities.

SOAR Use Case Examples

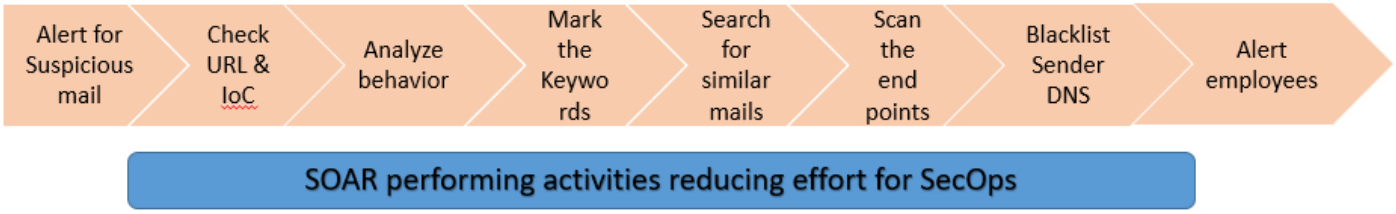
1. Malware Containments

As depicted in the flowchart below, alerts are reported by the SIEM and fed to SOAR platforms, which can be used by threat intelligence to give risk-based priority (RBP). RBP is one of the indicators that suggest analysts apply remediation actions on suspicious endpoints by blocking, isolating, containing, or blacklisting. These could be part of a workbook as well. After the actions are implemented, the suspicious endpoint can be checked in the respective dashboard.



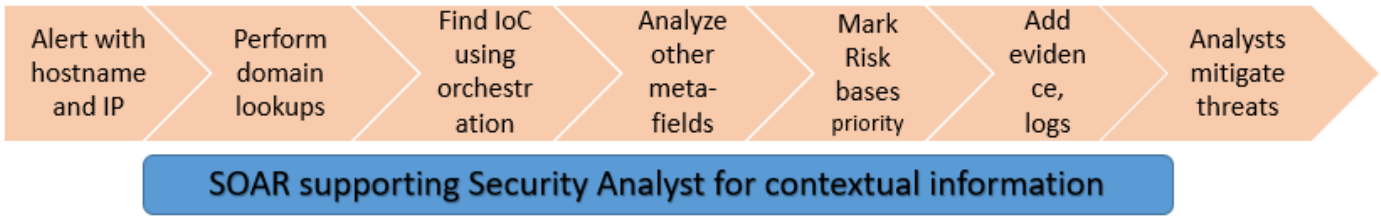
2. Phishing Emails

We all come across spam emails. Then there are emails with attachments that seem genuine but contain phishing scripts, which if executed on a machine would infect it with malware. If a suspicious mail is received, a SOAR platform runs a scan to identify the indicators of compromise, mark the keywords, and block the sender DNS. All the steps are automated in SOAR platforms, which are triggered by an alert received from SIEM, based on the rule configured.



3. Alert Enrichment

Most of security analysts' time is spent investigating alerts and digging deep for information, not responding to them. Enrichment actions can provide contextual information to draw conclusions about suspicious behavior. Alert enrichment actions like endpoint, device, and alert info, etc., enriches the information and adds evidence to the alerts.



Conclusion

SIEM led the cybersecurity industry for years, but it is not proactive enough to deal with threats. With the advancement of technology, cyber threats are advancing quickly. SOAR platforms need to mitigate threats before they form deep roots in computer systems.

SOAR uses alerts and develops responses based on automation or orchestration configurations. The cybersecurity canvas is getting more polished with the emerging SOAR trends of extended detection and response (XDR), which is similar to the latest tech stacks in cloud technology, AI, ML, and IOT, etc.

Enhancing security platforms with SOAR not only gives an edge to help businesses manage alerts but also empowers security analysts. The use of SOAR platforms accelerates the response time to SIEM alerts and crucial threats, and reduces the damage to IT systems.

About the Author

Nimasha is a Business consultant amalgamating her engineering understanding with a product role to deliver high quality, user centric products. She had evolved from automation engineer to product management roles donning various hats and working in multiple domains.

GlobalLogic®

GlobalLogic, a Hitachi Group Company, is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating our strategic design, complex engineering, and vertical industry expertise with Hitachi's Operating Technology and Information Technology capabilities, we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the automotive, communications, financial services, healthcare & life sciences, media and entertainment, manufacturing, semiconductor, and technology industries.



www.globallogic.com