FORTINET

acora
Led by Experience

SOAR Through Implementation

Table of Contents

Executive Summary

Security operations teams face the challenge of maintaining the longevity of their security infrastructures against the evolving threat landscape and operational complexities. New threats are more dynamic and attacks are more sophisticated. Organizations often add point products to address a specific type of threat, which leads to multivendor infrastructures that are difficult to control and have limited product integration within their security stack. In many cases, the technologies used to defend teams from cyberattacks are not fully utilized because of the sheer number of steps it takes for an analyst to execute a response. High alert volumes and cybersecurity talent shortages also contribute to slow response times and increase the risk of human error. All of these factors can lead to fragmented responses, complex manual workflows, decentralized processes, and the inability to truly streamline team collaboration efforts. With security orchestration, automation, and response (SOAR) solutions, teams can optimize operations, reduce alert fatigue, and provide consistency throughout processes. The key to successful implementation is to look at current processes to determine those that will most benefit from SOAR.

An estimated 3.5 million cybersecurity jobs will go unfulfilled globally in 2021.[1] As a result, 42% of responders report to be suffering from cybersecurity fatigue, and 93% of those individuals are experiencing 5,000 or more alerts per day.[2]

The Need for Advanced Automation

Every day, security analysts have to quickly make decisions to identify alerts that are real threats vs. false positives. Although analysts are making major decisions multiple times a day, they aren't always able to complete threat investigations. Many analysts are simply overwhelmed by the vast number of alerts. More than 50% of organizations experience 5,000 alerts per day and 17% have 100,000 per day.[3] Just deciding which alert to investigate can be a challenge. The problems are exacerbated by the extensive number of technologies used to counter cyber threats. Although the need for automation is evident, it's not enough. SOAR solutions fully maximize automation by centralizing management, controlling across multiple security stack products, and streamlining procedures.

Managing Success While Reducing Risk

Once a security team reaches the point where it can no longer address advanced security concerns manually and are exploring or have acquired a SOAR solution, they must tackle the challenge of implementation. Before a SOAR solution is deployed, key areas should be addressed. Every organization has different best practices, initiatives, and security concerns, so teams will have different priorities that affect how they build out orchestration and automation. Without a plan in place, the magnitude of security tasks that could benefit from orchestration and automation can create its own set of difficulties. To successfully administer SOAR, it's important to know what defined manual processes are already in place. Then a balanced, risk-driven prioritization approach can be divided up into stages. Recognizing the processes that are required to complete a repetitive manual function will become the foundation of mapping out the initial workflows that could be accelerated using a SOAR solution.

Although each organization might have their own unique processes, teams can maximize SOAR by fundamentally zeroing in on essential operations that are well understood. Initially, teams should look at processes that pose the highest risk or that delay crucial response times. While assessing the processes that are most essential, teams also should highlight the most beneficial processes to automate. For example, if there are an unmanageable number of phishing alerts, this is a process that should be automated. Lastly, teams should review their existing automation and how it's configured within their day-to-day operations. Identifying simple tasks that are already automated and why leads to opportunities to examine processes that could be expanded upon.

This initial automation of workflows often starts relativity simply, such as automating a SIEM alert. Over time, more complex workflows like threat hunting can be automated. It's important to focus on supporting analysts in completing tasks consistently, while responding at machine speed to potential cyber-induced risk. To support teams, Fortinet provides a Best Practice Service bundle that showcases areas where security teams can anchor Fortinet resources for fast deployments and long-term scalability.

Implementing Automation to Phishing Investigations and Response

Phishing has become one of the most common cyber threats. When left unchecked, it can have devastating consequences for organizations. Although essential, phishing investigations and response processes produce high alert volume and repetitive lengthy manual workflows. Phishing alerts also can remain masked under hundreds of alerts. This alert overload is tied to increased cyber risk because when investigating alerts, there needs to be consistency. Phishing alerts are a good candidate for orchestration and automation. Investigation is essential and has defined workflows. And it can be implemented in a semiautomated capacity. If a user submits a suspected phishing attempt or it's detected by technology, analysts must complete a series of manual steps to confirm if it is a false or true positive. The steps start with reviewing the body and header of an email, which can lead to further investigation. Because of the volume, sophistication, and lack of dedicated solutions for phishing, teams often only monitor an inbox. The sheer volume of this workflow alone can lead to human error and burnout.

With a SOAR solution, phishing investigation and response can be automated through the power of automated alert enrichment. Teams can search every vector to identify if other alerts have the same indicators and how other individuals were targeted with phishing emails. In this way, teams can quickly zero in on threats related to a specific bad actor. The sender can easily be blocked and all attachments quarantined. SOAR not only implements full and semiautomation but also includes various technologies that might have been underutilized within the workflows of analysts, such as sandbox tools. Because SOAR can automate complex phishing investigation processes consistently, organizations can move from a reactive to proactive approach to threat response.

Phishing has become one of the most common cyber threats. When left unchecked, it can have devastating consequences for organizations.

Mitigate False Positives and Threats Simultaneously

At a company that has healthy cyber hygiene, users may update their passwords every 90 days. However, the constant changes can result in errors, particularly when users forget their login information. Password-related errors cause an organization's security information and event management (SIEM) tools to send countless alerts to the security team. Analysts have to determine whether an alert is a false positive from a failed employee login attempt or a true positive alert. Spending time investigating false positives keeps analysts from dealing with the threats that matter.

To investigate an alert, analysts must check if the Internet Protocol (IP) address is internal or external. If it's internal, they need to confirm that the user is truly an internal employee who merely forgot their password. Then the analyst must manually close out the alert and document their actions. If it's an external IP address, the analyst must confirm the reputation to be malicious, which requires further investigations. The analyst has to determine if the user has been seen across multiple alerts, gained access to internal systems, and if any indicators of a breach exist.

Whether positive or negative, investigating password alerts increases costs. Because the repercussions of a breach can be severe, password alerts are another good use of SOAR. It can cover the foundational elements that are assessed during the mapping of workflows and can take advantage of artificial intelligence (AI) for some of the automation and orchestration. Automating these workflows into playbooks that tackle each of the initial steps of a potential brute force attempt isn't complicated. It can help reduce false positives by including a series of steps that verify if the user is internal, malicious, and their immediate intent. Depending on the SOAR solution, analysts also can take advantage of an AI-driven recommendation engine that can quickly identify alerts that have the same IP address, username, and criteria.

With a SOAR solution, analysts can automate alert enrichment to extract decision-based data. That data is added to a repository of indicators that is submitted to threat-intelligence feeds. Indicators that do not have previous data can be automatically applied to a sandbox tool for further investigation. The data also can be used for historical correlation, other investigations, or linked to different alerts. Having information that goes beyond whether an IP address has a bad or good reputation helps analysts focus on relevant threats.

With a SOAR solution, analysts can automate alert enrichment to extract decision-based data.

Manage Threat Intelligence With Efficiency

To do their jobs, cybersecurity teams have to acquire extensive amounts of data from multiple sources, sift through it, and segregate relevant information that could prevent a breach. Refining this information requires monotonous manual steps that take up valuable time and slow incident response. Cybersecurity can't be proactive when teams constantly are working in reaction mode. Having vital intelligence determines the actions an analyst can take while hunting for threats or during a response, so automation and management with a SOAR solution is becoming a foundational cybersecurity component.

Fortinet has designed a security operations center (SOC) automation model that caters to every stage of SOC maturity. It is structured to help security teams take advantage of the capabilities in the Fortinet Security Fabric based on their current investment in analysts and activities within their SOC teams. Fortinet FortiSOAR works at the peak of the framework. It is ideal for mature security teams that require the advanced capabilities of SOAR to help them do more with less.

[1] Steve Morgan, "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021," Cybercrime Magazine, October 24, 2019.

[2] "Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020," Cisco, 2020.

[3] Ibid.

www.fortinet.com

April 29, 2021 9:48 PM

ebook-soar-implementation

957935-0-0-EN