The Difference Between SIEM and SOAR

If you have been involved in the IT and cybersecurity industry for a while, you have most likely come across the terms SIEM and SOAR before, but there is still much confusion by many professionals about what their specific uses and purposes are. So, what are they? What do they do? Are they the same thing? Do you need one, the other, or both within your security operations infrastructure? Below we will explain the basics behind them, their differences, and how they can work seamlessly together to accelerate security operations in terms of their incident response processes and tasks.

The Difference Between SIEM and SOAR

Most businesses already leverage SIEM technology as a core component of their security operations centers. SIEMs serve as a centralized collection point for the millions of log entries generated each day by applications, servers, endpoints, network devices and other log sources.

The SIEM manages a massive processing and storage infrastructure capable of receiving and processing these logs. From there, the SIEM correlates bits of related security information arriving from different sources to provide analysts with a comprehensive view into the security posture of the enterprise.

The major function of the SIEM is to assist in sifting through the proverbial haystack of security information to find the needles that indicate a security incident.

Once a SIEM detects a potential security incident, it may then alert administrators to the activity and/or trigger an automated response. The response toolkit of the SIEM normally consists of blocking activity, triggering vulnerability scans, gathering additional information and similar rudimentary actions. Security teams often manage playbooks that contain a set of response actions to carry out when the SIEM triggers alerts on certain types of security incidents.

Security orchestration, automation and response platforms take the response capabilities of a SIEM to the next level. SOAR solutions supplement, rather than replace, the SIEM. Those familiar with the robotic process automation trend that is currently driving digital transformation efforts in many business processes should think of SOAR as the application of RPA to the security operations center. It allows the cybersecurity team to extend its reach by automating the routine work of cybersecurity.

What is SOAR?

Security orchestration, automation and response (SOAR), terminology adopted by Gartner, is an approach to security operations and incident response used today to improve security operations efficiency, efficacy and consistency. To better understand what this means, let’s look at its components separately:

- **Security Orchestration** – the coordination of various desperate security tools and technologies being used within the tool stack (typically from various vendors) to seamlessly integrate and communicate with each other to establish repeatable, enforceable, measurable and effective incident response processes and workflows. People and processes must also be orchestrated properly to ensure maximum efficiency.
- **Security Automation** – the method of automatically handling tasks and processes without the need for manual human intervention, reducing the time these take by automating repeatable processes and applying machine learning to appropriate tasks. Automation usually takes place through the use of playbooks and runbooks (the former containing linear tasks, and the latter containing decision based conditional actions) to reduce or eliminate the mundane actions that must be performed.
- **Security Response** – the approach to addressing and managing the security incident once an alert has been confirmed, including triage, containment, remediation and more. Today, many actions, such as quarantining files and disabling access to compromised accounts, to name a few, are performed automatically, so incidents that once posed a real threat can be quickly resolved.

Why SIEM and SOAR Are Better Together

The incident response processes followed by security teams around the world are fairly standard. They might take the following steps:

1. Identify that a potential security incident is underway
2. Open a ticket in the organization’s incident tracking system and assign it to an analyst for review
3. Notify team members and trigger a call-in mechanism
4. Implement a firewall rule that temporarily quarantines affected systems while an investigation is underway
5. Query the SIEM for relevant information from affected systems
6. Poll external sources for supplemental information, such as IP address ownership and threat intelligence data
7. Analyze all the data and take appropriate action to eradicate the threat and recover operations

[source: https://biztechmagazine.com / https://www.dflabs.com]