next-gen SIEM and SOAR: a powerful duo against cyber threats

jack henry™

contents

introduction

With the growth of cybersecurity and an ever-changing marketplace, there's been an explosion of acronyms in the tech industry. Two of these acronyms, SIEM and SOAR, have evolved over the decades and in how they continue to adapt to today's cybersecurity challenges.

SIEM and SOAR are causing substantial confusion in the IT community. The high signal-to-noise ratio of traditional SIEM (Security Information and Event Management) solutions, combined with systemic staffing shortages, have impelled a new generation of SIEM complemented by SOAR (Security Orchestration, Automation, and Response) functionality.

What's the difference between next-gen (NG) SIEM solutions and SOAR, and how do the new requirements of NG SIEM compare or contrast to the capabilities of a SOAR platform?

It's imperative that we first define what capabilities must be met by a SIEM solution to be considered NG. Then we will explore SOAR, and how both SIEM and SOAR can work together.

history of SIEM

One of the first true SIEM solutions to appear in the market was *Intellitactics* in the late 1990s. The product category at the time was referred to as network security management (NSM). Later, the term was replaced with the phrase SIEM (by Gartner in 2005).

The traditional, first-generation SIEM solutions quickly began to prove challenging for talent-starved institutions. They had few internal cybersecurity professionals who certainly didn't have time to sit in front of an SIEM day in and day out tuning, creating content rules, or validating false positives while looking for false negatives.

The term "event (or alert) fatigue" became a challenge, giving rise to a new market of MSSPs (Managed Security Service Providers) that followed by taking over the burden of monitoring.

MSSPs offered hope by acting as a triage for level 1 and level 2 event analysis for institutions unable to staff an internal security operations center (SOC).

First-generation SIEM solutions started out as log aggregators, powered by relational databases, capping their ability to provide real-time response. The introduction of correlation engines began to give intelligence to first- generation SIEM. The goal was to address the event fatigue problem caused by false positives and to create an equation (A + B + C is related to the same event and = something bad).

Despite the introduction of correlation engines, SIEM still fell short of expectations. SIEM technologies were unable to aggregate and correlate all log and event data from on-premises and cloud workloads, SaaS (Software-as-a- Service) solutions, and system and network data. Nor could they provide the capability to perform automated response for detected threats.

NG SIEM: a smarter detective

This brings us to today's NG SIEM.

In order to qualify as an NG SIEM, the solution needs to leverage NOSQL databases, such as Hadoop, Elastic, Spark, and other technologies that weren't available in the early part of the 21st century. Data warehouses that were used by first-generation SIEM solutions included MySQL, PostgreSQL, MSSQL, and even Oracle. They overwhelmed the backend and rendered them unusable over time, preventing institutions from sending any new raw event data to their SIEM unless it was absolutely necessary.

During the last two decades, data science has matured at an evolutionary pace, removing the need for false positive-prone pattern-matching engines, also referred to as signatures. NG SIEM solutions incorporate machine learning (ML) capabilities to leverage supervised and unsupervised models to cluster events together and identify anomalies from learned behavior. This helps prevent overwhelming the analyst by deafening them with too much noise.

One of the most prevalent themes to become part of the daily narrative in SecOps (security operations) is the concept of applying context to security to determine if an event should be considered a true positive. This is the idea that the SIEM solution should be able to take its understanding of a given asset and apply context to an event affecting that asset, if it is indeed relevant.

For example, an event may trigger from an NDR (network detection and response) solution that an Apache buffer overflow attack was detected that may be real, but the target IP address is running Windows and the IIS web server. Context in this case would not apply, despite it being a real attack, saving an analyst time in having to further investigate.

By incorporating more intelligence into the traditional SIEM, which makes it aware of not just asset information but also the learned behaviors of users in the environment, it gives NG SIEM the capability to apply UEBA (user entity behavior analytics). NG SIEM solutions don't simply identify an event as being "bad or good." Using ML models, they assign a type of score to an event. When that score exceeds a specified threshold, it's presented to the analyst for further analysis.

more ML awareness

Early SIEM solutions typically presented events by categorizing them into tables of high, medium, or low severity without much more context than the potential severity of the event. Using UEBA, an NG SIEM can quickly identify anomalous behavior when, for example, an employee suddenly demonstrates behavior not previously seen by the SIEM (such as logging onto the corporate VPN on Sunday at 2 a.m. when the individual has never previously logged into the VPN outside of work hours).

Because early SIEM products didn't have much in the way of asset and infrastructure awareness, they were incapable of identifying lateral movement following a foothold by cybercriminals. Conversely, NG SIEM solutions are now capable of tracking the lateral movement of cybercriminals as they pivot from one asset to another in an on-premises or cloud network.

Just like in the investigation of a crime scene, the primary job of an investigator is to piece together the events against an established timeline. Timeline generation of related events is a hallmark capability of NG SIEM solutions that previously had to be reconstructed manually by analysts.

The most powerful capability added to an NG SIEM is the capability to perform automated responses to known threats that are predefined by incident response playbooks.

Unlike their first-generation SIEM solutions, NG SIEMs can pull event data from applications and systems. They can also stack workflow automation on top of orchestration, such as pushing response actions to devices like firewalls or IPSs (intrusion prevention systems) in response to detected threats.

This makes NG SIEM similar in capability to SOAR technology. And this is why there's the current confusion in the market.

Finally, NG SIEM solutions have integrated threat hunting capabilities, allowing analysts to uncover suspicious activity and vulnerabilities in their environment, as well as monitor threat intelligence feeds to uncover potential issues, adversaries, and indicators of compromise.

detection and resolution in cybersecurity

Before we turn our attention to SOAR, it's important to first introduce the concepts of mean-time-to-resolution (MTTR) and mean-time-to-detection (MTTD).

MTTR first originated in deskside/IT support and signified the duration of when a problem ticket was first reported and subsequently resolved by a technician. Cybersecurity analysts have also adopted MTTR. Its meaning remains the same except that MTTR in cybersecurity defines the span of time between when a confirmed cybersecurity incident is first triaged to when it's eventually resolved.

MTTD refers to when cybercriminals first employ the tactics and techniques used to obtain a foothold on a target network to when they're eventually detected by a network or endpoint security control.

SOAR and NG SIEM: a powerful partnership

SOAR was conceived to help address the SIEM challenge of event/alert fatigue and the global talent shortage in cybersecurity for institutions to effectively staff a SIEM deployment.

SOAR streamlines what were once manual tasks as a way of removing human error from the MTTR/MTTD loop through automation and orchestration, powered by incident response playbooks, while reducing the tediousness and overtaxing nature of threat analysis.

Unlike NG SIEM, SOAR is an integration platform that glues an institution's numerous SecOps tools together and automates them using incident response playbooks that can be executed automatically or with a single click by a SOC analyst. SOAR also facilitates case management with a purpose-built issue tracking system for collecting security event analysis and response workflows.

The best way to compare NG SIEM and SOAR platforms is to think of SIEM solutions as systems of record and SOAR platforms as systems of action. This doesn't remove the need for a SIEM.

Instead, when combined with SOAR, an NG SIEM is more effective in reducing MTTD/MTTR. It also addresses the challenge of inadequate staffing and lowers the high signal-to-noise ratio common in many SOCs.

NG SIEM + SOAR: Leveraging the advances in NG SIEM and SOAR technology will help identify and stop the presence of potentially malicious and harmful behavior, which can help prevent a data breach or service disruption.

SOAR via NG SIEM

SOAR and NG SIEM can work together to stop threats while keeping operations running smoothly.

As expected, the collision of the SOAR and NG SIEM worlds is occurring as NG SIEM companies began acquiring SOAR companies with the objective of integrating SOAR capabilities into their SIEM platform or expanding the integration between the two.

NG SIEM platforms that integrate SOAR capabilities because of the necessity to support NG SIEM functions will not incorporate all of the capabilities of a dedicated SOAR platform. Adding playbooks and automated response to an NG SIEM will certainly improve the automated response and orchestration offered by a dedicated SOAR solution.

SOAR also integrates into existing workflows, helping to make network management more efficient and automated. NG SIEM is intelligent software, just like SOAR. But NG SIEM is prone to generating more alerts than a team can respond to. NG SIEM that incorporates SOAR will help to reduce the number of alerts and make workflows more manageable.

leveraging SIEM and SOAR to proactively protect against cyber threats

Cyber attacks can often only be detected through a holistic view and analysis of varying events occurring on your network.

It's more important than ever to gain a comprehensive view of your entire institution. Aggregation and correlation of events across all systems and networks provides management with better visibility of potential cyber threats.

More visibility leads to a better assurance that your security controls are effective, which will lower your risk profile and reduce your total cost to mitigate cyber threats. Leveraging the advances in NG SIEM and SOAR technology will help identify and stop the presence of potentially malicious and harmful behavior, which can help prevent a data breach or service disruption.

Simply put, the best solution to industry-wide struggles with threat detection and response is to increase efficiency using NG SIEM and SOAR together.

connect with next generation technology

Learn more about our cybersecurity solutions.

For more information about Jack Henry, visit jackhenry.com.

jack henry™