FORTINET

What Really Matters When Selecting a Security Information and Event Management Solution

Extracting Usable Intelligence from High Alert Volumes

Table of Contents

FORTINET

Executive Overview

As the attack surface expands and the threat landscape accelerates and becomes more complex, lean security teams can no longer keep up with the deluge of alerts and other information generated by their security devices. To address these challenges, security leaders look to security information and event management (SIEM) solutions to correlate data and perform automated analysis. Security leaders are challenged in terms of time and resources, so the SIEM they choose must be easy to implement and highly accurate, while offering a low total cost of ownership (TCO) by automating time-consuming, manual workflows. This is particularly true for security leaders in midsize organizations. The SIEM must also enable business-driven prioritization, extending monitoring beyond individual devices to the business services they power.

On average, an organization's security operations center (SOC) receives over 10,000 alerts per day, but an analyst can only realistically investigate 20 to 25 of them.[1] SIEM must focus attention on the right alerts.

Addressing Skyrocketing Security Event Volume and Velocity

Security leaders in midsize organizations have an uphill struggle. The volume and velocity of threats are overwhelming their understaffed teams, with the number of security events generated by a growing multitude of devices, applications, and users far exceeding what they can track and manage. In order to keep up, security leaders are turning to SIEM solutions. Data aggregation, correlation, and analysis enables security teams to reduce the amount of time required to identify and respond to potentially suspicious behavior.[2]

Security leaders also see SIEM solutions as the means for addressing compliance requirements by streamlining the process of compliance audits and reporting.

Companies have deployed products from up to 70 different security vendors.[3] A SIEM solution can ingest and correlate data from many devices, allowing an organization to consolidate their monitoring efforts.

4 Key Requirements for Highly Effective SIEM Solutions

A SIEM solution that addresses these needs must not only maximize the effectiveness of the security operations center (SOC) but also shorten the time to value for lean security teams. Following are four key requirements that security leaders need to heed when evaluating SIEM solutions:

1. Collect data from every device and scale to store it efficiently

A proliferation of security products adds complexity on myriad fronts. When addressing new and evolving threats, organizations commonly focus on acquiring best-in-breed solutions. In order for a SIEM solution to be effective, it must communicate with each of these. To do so, a SIEM must provide comprehensive application programming interface (API) capabilities that support a wide range of IT, identity security, and other devices throughout the organization, and even into the cloud. This facilitates the ingestion of data across the entire security infrastructure. Bandwidth-constrained security teams do not have time or resources to build manual API connections with each device. SIEM solutions must by and large be ready to go right out of the box.

They also must be able scale cost-effectively, in order to store the huge volume of data they ingest. For this reason, high-performance, distributed processing, storage, and search are essential.

31%

of organizations ignore over half of security alerts due to inadequate automated data aggregation and analysis.[4]

2. Deliver context-based insight

Of course, raw information is of limited value. One fundamental function of a SIEM is automated data aggregation, correlation, and alerting. The same wealth of data that can overwhelm analysts becomes invaluable when properly organized. This is particularly the case for security teams from midsize organizations.

A SIEM solution must be capable of performing the preliminary analysis, including contextual enrichment, necessary to ensure that security analysts are provided information that is actionable. Here, security leaders need to look for SIEM solutions with robust rule sets, advanced analytics, such as user and entity behavior analytics (UEBA), as well as additional context from other sources.

Other key capabilities include the flexibility to receive and process data from devices across the network, the ability to learn the topology of the protected network and the relationship of users to it, and integrated machine learning (ML) that uses this wealth of information to make informed threat decisions. All these lead to high-fidelity identification, which ensures that alerts are relevant and do not overwhelm or waste the time of SOC analysts.

A SIEM can distill over a billion alerts a week into a manageable number of high-impact alerts using data aggregation and integrated machine learning.[5]

3. Automate as much as possible

The cybersecurity skills gap means that only 28% of organizations have the ability to adequately staff their security teams.[6] Security leaders from midsize organizations are especially impacted in this regard. And as the skills shortage is expected to grow, these challenges will only worsen. SIEM solutions should offer various ways to automate workflows—not only those associated with log collection and policy enforcement but also those used to manage event response. Although security orchestration, automation, and response (SOAR) has become a buzzword in the industry, there is certainly value to defining the alert handling process, from validation to containment to remediation. In the midst of a potential emergency, it's better that everyone knows what they are supposed to do. Further, once the process is defined, customizable levels of automation allow organizations to offload activity to the systems themselves to the degree they become comfortable doing so.

Monitoring and workflow automation must also include compliance obligations and reporting. The regulatory landscape is rapidly expanding, forcing organizations to deal with various data protection regulations. These include regional regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA); industry-specific privacy laws such as the Payment Card Industry Software Security Framework (PCI SSF) and the Health Insurance Portability and Accountability Act (HIPAA); and government data security guidelines such as those from the National Institute of Standards and Technology (NIST) as well as regulations such as the Federal Information Security Management Act (FISMA). Achieving and maintaining compliance requires regular compliance reports, which create a significant burden for security teams when compiled manually. A SIEM solution should reduce this burden through automated data collection and compliance report generation.

57%

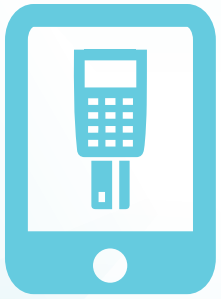
of security leaders name a reliance on manual processes as one of their top three security concerns.[7]

4. Monitor business services, not just devices

Many SOCs have visibility into incidents on a device basis, such as a firewall detecting malicious traffic from a compromised server, a device reporting evidence of a malicious process, or even an access point that has stopped reporting status entirely. In these cases and many others, the ability to understand the context and the relationships between impacted devices is crucial to differentiating between a critical event and a less important one.

For example, an alert that a wireless access point is down requires a response. However, the priority of the issue depends on context. While the loss of a hotel's guest network may be an annoyance, the loss of an access point used to manage guest check-ins or one used by the payment processing system in the hotel restaurant can be a more significant issue.

In this case, security leaders must have the ability to understand relationships between devices—and the impact of these relationships on the ability to provide user-facing services—as well as understanding the functions of the devices themselves. Often, the ability to understand these relationships is what makes a SIEM capable of appropriately prioritizing events and alerts for the security team.



A single mobile or web payment can cross 35 different technology systems.[8] Business context is crucial for identification of important alerts.

Conclusion

An expanding attack surface, accelerating threat landscape, and a scarcity of skilled cybersecurity professionals demand technologies that provide real-time visibility and control across the entire network. The ideal SIEM speeds incident detection and response and demonstrates compliance, all while reducing complexity in the SOC. This requires the ingestion and correlation of huge amounts of data in order to provide high-fidelity threat identification and ideally automate the appropriate response.

[1] Barbara Filkins, "An Evaluator's Guide to NextGen SIEM," SANS Institute, December 6, 2018.

[2] Ibid.

[3] Ofer Schreiber, "The Good & Bad News About Today's Cybersecurity Investment Landscape," Dark Reading, July 25, 2018.

[4] Jon Oltsik, "Dealing with Overwhelming Volumes of Security Alerts," ESG Blog, March 3, 2017.

[5] Evan Schuman, "SIEMple evolution: The future for a cloud-based SIEM," SC Magazine, July 11, 2019.

[6] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens (ISC)²: Cybersecurity Workforce Study, 2018," (ISC)², 2018.

[7] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[8] "CIOs Reveal Rapid Growth In Technology Makes It Hard To Adapt," The Millennium Alliance, March 7, 2019.

www.fortinet.com

456630-0-0-EN

October 20, 2019 10:34 AM

eb-security-information-event-management