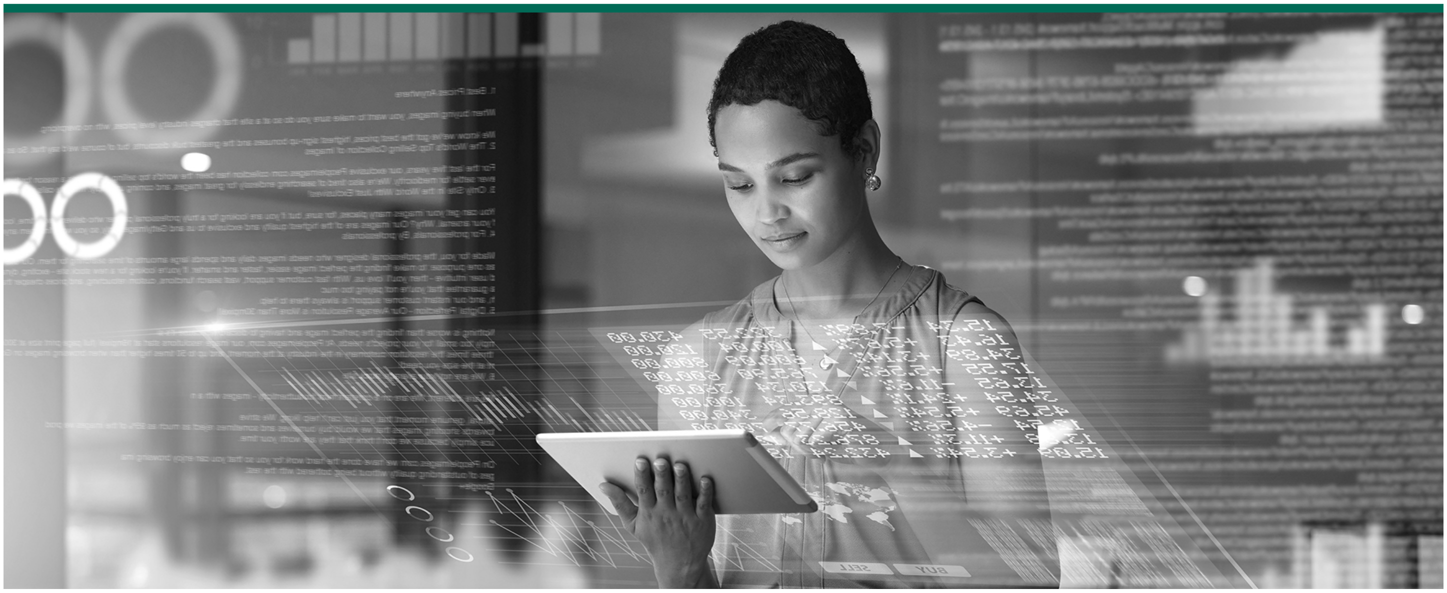
WHITE PAPER (ALERT LOGIC)

SIEM SOLUTIONS FOR SECURITY

What Vendors Won't Tell You

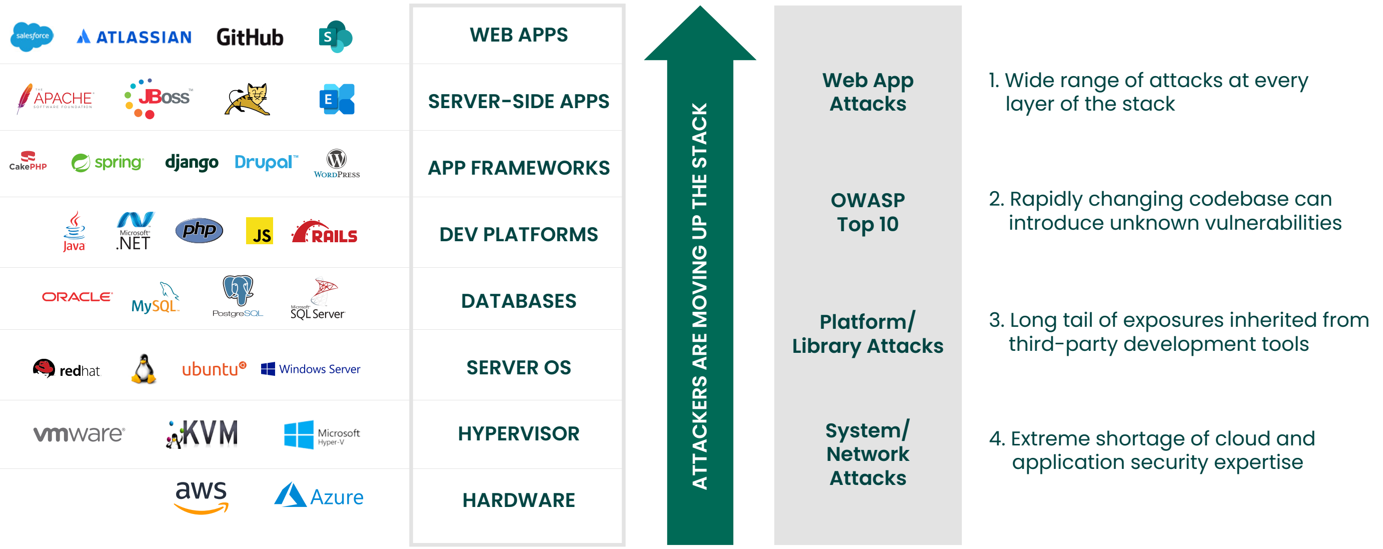


Security information and event management (SIEM) solutions have been around for more than a decade. These solutions promise a holistic view of what is happening in near real-time across an organization's IT estate by ingesting log and event data generated by assets across an organization's infrastructure. Once the data is collected, correlation rules (also called rule sets) are applied to detect and categorize threats. When a rule is matched, an alert is triggered, indicating a security incident needs to be investigated. Given that the data is centralized, the SIEM also may be used to investigate security incidents, eliminating the need to log into dozens of consoles.

For many organizations, SIEMs appeal to their optimistic sense of what is possible. Unfortunately, the full cost and resource burden often isn't realized until after purchase. For security professionals and strategists, it's important to understand these challenges as well as recognize there are other ways to achieve the desired security outcomes.

Modern Threats Require Insight Beyond Basic SIEM Capabilities

To identify threats, a SIEM is only as good as its inputs and detection rules, which originally were designed for on-premises environments. Admittedly, they have evolved somewhat over the years, but still have challenges (and hefty price tags) when it comes to cloud security. One of these areas is securing web applications, which are a prime target for threat actors looking to gain access, build footholds, and move laterally. According to the Verizon 2022 Data Breach Investigations Report, web application attacks are the number one attack vector as they have been for many years.



1. Wide range of attacks at every layer of the stack
2. Rapidly changing codebase can introduce unknown vulnerabilities
3. Long tail of exposures inherited from third-party development tools
4. Extreme shortage of cloud and application security expertise

SIEM TOOLS ARE CHALLENGED WHEN TASKED WITH PROVIDING FULL STACK VULNERABILITY DATA AND INSIGHT

To protect against web application attacks, an organization should purchase a web application firewall (WAF), deploy it, send data to the SIEM, and write new rules. This holds true for all additional security controls added to protect against modern threats.

Constant Tuning for Accurate and Actionable Insights

In the initial stages of a SIEM deployment, there will be a set of rules for common use cases. When a rule is matched, an alert is triggered, indicating a security issue to be investigated. However, the volume of alerts can become overwhelming, making the task of investigating each of them nearly impossible. Twenty-five percent of respondents to a 2022 study reported a lack of contextual information as one of their primary SIEM challenges. The problem is there is little-to-no context about alerts, so every alert is treated with the same level of criticality. Eventually, the security team is drowning in a sea of alerts, causing alert fatigue which allows attacks to slip by because analysts ignore the alerts.

This is where the ongoing maintenance burden comes into play, as SIEMs require constant tuning. Correlation rules need to be tweaked, and new ones need to be written to increase accuracy and reduce the number of alerts to investigate. Tuning must be done by someone with strong expertise. If an organization lacks the expertise, outsourcing and/or third-party expertise may be required. This tuning is critical to begin filtering out some of the noise to find the needles in the haystack as well as creating actionable items for those responsible for remediation. While tuning will help reduce some noise and surface the riskiest activity, it won't uncover all the risks. To prioritize the potential threats, additional content, including advanced analytics, is needed. For some vendors, this addition context and analytics capabilities comes at an added cost.

Costly Analytics Necessary for Context

The obvious goal for organizations is to block all known bad activity and allow known good activity. However, it's the "suspicious" or unknown activity that can be substantial.

The SIEM may offer a User Behavioral Analytics (UBA) or a User and Entity Behavioral Analytics (UEBA) module to enrich large data sets and use data models to add context and prioritize the alerts. Some vendors call this combination Next-Generation SIEM, which requires additional infrastructure and professional services for deployment, as well as another technology that will require tuning. In many cases, it also requires the most advanced support level due to the solution's complexity. Next-Generation SIEM or SIEM with UEBA is necessary to gain valuable insights by providing the following detection methods:

- Signatures and rules that detect known malicious patterns such as exploits against vulnerabilities or transactions that violate specified parameters.
- Anomaly detection that compares real-time activity against baselines to flag unusual behavior such as HTTP requests and responses with characteristics beyond the established normal range.
- Machine learning that detects new threats and improves detection accuracy without being explicitly programmed where to look by iteratively using computer-generated algorithms. Machine learning is particularly good at detecting multi-stage, multi-vector attacks that don't match existing signature patterns or anomaly parameters. In addition, it can help overcome the fragility of SIEM rules that do not have proper maintenance.

SIEM Alerts Require Interpretation and Triage

A critical and often overlooked factor in achieving SIEM value is the requirement for interpreting and triaging events and alerts. Once threats are detected, organizations require clear event and incident information to understand their potential impact, triage, and respond with remediation. According to the 2022 SIEM Security Report, 41% of organizations cite lack of skilled staff as their number one challenge to maximizing value of their SIEM. If you lack security experts to turn detection into response, a SIEM will not help you. In-house security analysts — who are in short supply — are an expensive SIEM cost component that is frequently overlooked.

Understanding the Full Cost Burden of SIEM

SIEM is a powerful platform, requiring substantial investment of time and money to implement, configure, learn, use, and keep current. Many SIEM initiatives simply fail to launch, while others grossly exceed planned budgets and timelines. Although a SIEM's average cost is up to $10,000 per month, the cost to be fully operational, including implementation and software maintenance fees, can be significant and out of reach for mid-size organizations. Additionally, an organization's storage, network, and compute infrastructure will need to accommodate growth as SIEM use matures. Professional services are typically required to stand up a SIEM and often throughout its lifetime for ongoing updates, new rules, new assets, and changing workloads.

Operationalizing SIEM Reveals More Resource Burdens

A SIEM typically prioritizes threats detected to help the security analyst focus on issues of most concern. Yet, expertise is still required to triage and respond to incidents as they arise and refine and tune detection rules.

The bulk of the ongoing effort required for a SIEM is to monitor and investigate identified alerts. Security and IT staff typically waste 25% of their time investigating unreliable alerts, while actual breaches go undetected for an average of 277 days.

Once you evaluate the costs and commitment required to implement a SIEM, consider your alternatives for improving your security posture. While SIEMs are a more traditional approach, they usually only benefit organizations with a well-staffed internal security team. A SIEM alone is not the best solution for monitoring threats against web applications and cloud environments. Analytics and additional effort are generally required which are cost prohibitive and resource intensive for most mid-size organizations.

Alternatives to Achieve Necessary Outcomes

Every organization wants to increase their security while reducing risk and costs. Security leaders would be wise to understand what outcomes they want and where they may have gaps to achieve those outcomes. In many cases, organizations come to realize they either don't have the expertise to fully understand how to solve their security and compliance problems, or they know exactly what to do but don't have the time or the staff to deliver the security outcomes they need.

An alternative approach to improve security posture is managed detection and response (MDR). With MDR, customers are quickly alerted about what incidents matter and what to do about them. The MDR solution provider enables organizations to achieve their outcomes by providing:

- Platform/technology to collect data to various third-party sources
- Security expertise to analyze and enrich data
- Remediation guidance
- Constant tuning to reduce false positives
- Community defense and rapid protection for critical threats by actively tracking new vulnerabilities and emerging threats across their large install base

These functions enable organizations to achieve continuous, around-the-clock monitoring with a predictable pricing model at a fraction of the cost of owning a SIEM.

Fortra's Alert Logic, a pioneer in MDR, provides managed threat detection as a service, fully deployed and operational in days with predictable monthly subscription costs. The service monitors your IT environment and uses advanced analytics to identify threats. It includes all the necessary behind-the-scenes efforts such as: implementation and maintenance of monitoring systems like WAF and IDS, their integration with the threat detection analytics, and the everyday use of rules and alerts. Our global security operations center investigates alerts and provides meaningful insight and remediation advice. Alert Logic can help you sidestep the SIEM money pit by using a modern solution that quickly provides results at a fraction of the cost and with greater predictability for your budget.