The Cost of Not Taking Your SIEM to the Next Level

How to get ahead of a fast-moving threat landscape

ANOMALI

PROBLEM 1:

The Direct Cost of a SIEM Solution

Poor Scalability

Significant investments in infrastructure or additional licensing costs are always amplified for enterprises undergoing digital transformation. A lack of scalability for a security information and event management (SIEM) solution often limits views of past events, providing an incomplete picture of potential threats.

Lack of Historical Context

This is a major issue for most SIEMs. When you need to analyze data going back several months or years, you'll find that most SIEMs either cannot deliver historical data that far back, or it is slow and expensive to access archived materials.

The average cost of a SIEM solution exceeds

$1M ANNUALLY[1]

—and that's only license and hardware costs.

[1] Schoenbaum, Dan. 2022. "The Average SIEM Deployment Costs $18M Annually... Clearly, It's Time for a Change!" *Medium.*

PROBLEM 2:

The Effect of Poor Performance on Security Analysts

Alert Fatigue

SIEMs generate a large number of alerts, including false positives (flagging benign events as malicious), false negatives (missing actual security incidents), or low-priority events. The level of noise can easily overwhelm security teams, making it difficult to identify the signal of genuine threats.

Complex Configuration and Maintenance

Setting up and maintaining a SIEM is complicated and time-consuming, requiring expertise in configuring log sources, creating correlation rules, and continuously ensuring the system is up to date. A complex user experience also hinders its adoption, limiting its use for non-technical staff who need to interact with SIEM data.

Absence of Actionable Context

A SIEM's reliance on rules and signatures to identify security events provides limited external context about generated alerts. This lack of actionable context leads to an incomplete or inaccurate understanding of the severity and impact of an incident, making it challenging for security analysts to identify advanced threats in a complex, dynamic environment.

Limited Automation and Response Capabilities

While SIEM systems provide alerting capabilities, they often lack robust automation and response features, particularly when facing complex correlation requirements. SIEM systems are also limited in their abilities to provide monitoring and threat detection in cloud-based environments, requiring manual investigation and response to alerts. This is both time-consuming and prone to human error.

> False positives can run as high as
>
> **99%**
>
> adding a high level of stress to a security analyst's work.[2]

[2] *Alahmadi, Bushra A., Louise Axon, and Ivan Martinovic. 2022. "99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms." 31st USENIX Security Symposium (USENIX Security 22).*

PROBLEM 3:

The Organizational Impact

Incomplete Data Collection

SIEM solutions rely on log data from various sources, but they may not collect all relevant logs and can fail to capture critical information due to limitations in log sources, network configurations, or compatibility issues. This leaves blind spots in the security monitoring process.

Storage Limitations

Storage costs, log retention policies, and log normalization can create obstacles that result in incomplete log data for analysis. This has significant implications for both threat analysis and actionable insight.

Security teams can no longer indulge in response times that can be measured by a calendar.

Inability to Handle Large-Scale Data

SIEM technologies often struggle to handle the volume and velocity of data generated by modern networks and systems. Slow response times can lead to delays in processing and analyzing data, making security teams potentially miss time-sensitive security events.

Limited Threat Intelligence Integration

While SIEM solutions often incorporate threat intelligence feeds, their integration and updating processes with other security elements such as intrusion detection systems, firewalls, or vulnerability scanners may not be seamless (if they exist at all), leading to outdated or ineffective threat intelligence.

What's the answer to all these problems?

A real-time solution that provides actionable visibility by integrating external intelligence information with internal attack surface information is mission-critical for any enterprise subject to cyber threats.

Uplevel Your SIEM with Anomali

SIEMs still have a critical role to play in the security framework of any organization. However, you need a more forward-leaning approach to stay ahead in the modern threat landscape while maximizing the value of your non-trivial SIEM investment. This requires thinking along three vectors: Actioned Visibility, Automated SecOps, and an Optimized Cyberstack.

LEARN MORE

Actioned Visibility

Security teams must take immediate action across all security telemetry and supply chains to address potential threats before they move into execution mode. This requires visibility beyond the scope and reach of traditional SIEM solutions, including threat and attacker insights augmented with curated and peer intel. This delivers context that goes far beyond current SIEM storage limitations while reducing cycle times from weeks to minutes.

Automated SecOps

By implementing workflows supported by AI engines that automate routine analyst tasks such as intelligence analysis, trigger investigations, security gap identification, and security posture updates, analysts are in a much better position to separate the signal from the noise, handle threat detection with precision and context, and reduce the stress associated with unsustainable workloads.

Optimized Cyberstack

You want to optimize the value of your security infrastructure to understand risk exposure, prioritize security investments, and capture and share intelligence to security controls to identify attacker TTPs and prevent breaches. Most enterprises have a number of specialized stand-alone security solutions that are not fully integrated with external defense resources such as ISACs or MITRE ATT&CK. Integrating dynamic data sources into an actionable framework is a genuine force multiplier, enabling analysts to deliver a significant impact.

An approach leveraging these three vectors via Anomali is used in some of the most demanding security environments across a broad range of industries. To learn more, please visit www.anomali.com/product.

LEARN MORE

ANOMALI

"Creating actionable intelligence and then acting on it is the most effective tool that we have to defend ourselves against all classes of cyber adversaries, from nation states to hacktivists."[3]

— Chip Stewart
Former Chief Information Security Officer,
State of Maryland

[3] *Anomali. 2023. "A CISO Perspective: From Threat Landscape Insights to Transformation Programs | May 2023."*