ANOMALI

GUIDE

Five Essential Features For Your Next SIEM

Five Essential Features for Your Next SIEM

In the ever-escalating battle of digital wits, Security Information and Event Management (SIEM) solutions must continually evolve to stay ahead of the adversaries. As the pervasive use of AI enables attacks to become more sophisticated, the right SIEM can make the difference between a swift response and a costly breach.

Selecting a SIEM is far more complex than reading product reviews. It's a multi-step journey that starts with an evaluation of your current technology stack, your budget, and your team's preferences. Many enterprises select a vertical security stack from a single vendor to address multiple needs. Others are platform agnostic and choose best-of-breed solutions that require some level of integration.

A recent wave of M&A in the SIEM market adds another level of uncertainty. If these consolidations affect your current SIEM, you may be wondering if these newly formed entities will maintain the same vision and agility in the face of rapidly evolving threats… or whether their solutions will even exist a few years down the road.

Because the SIEM is the cornerstone of your cyber defense strategy, you need to perform a detailed analysis to understand the pros and cons of the alternatives. This guide is designed to help you simplify your decision-making process by identifying the five most important factors to consider when comparing solutions and vendors.

Advanced Analytics and Threat Detection

The heart of any SIEM lies in its analytical capabilities. Seek solutions with robust correlation features that can link external threat intelligence with internal telemetry, enabling swift identification and remediation of potential threats. Advanced analytics, including attack-surface management (ASM) correlation and behavioral analysis, are essential for detecting sophisticated attacks.

Integration with threat intelligence feeds is crucial for staying ahead of emerging threats. Opt for a SIEM that gives you access to the largest repository of threat curated intel available. User and entity behavior analytics (UEBA) is another essential feature that helps detect insider threats and anomalous behavior that might indicate a breach.

Integration and Compatibility

A top-tier SIEM solution should seamlessly integrate with a wide array of log sources, including operating systems, network devices, applications, and cloud services. Look for an open platform that supports hundreds of feeds to maximize visibility across your entire IT/security infrastructure.

Moreover, ensure the SIEM offers robust APIs and customization options, allowing it to integrate smoothly with your existing security tools and third-party solutions. Be sure to confirm that it's compatible with your preferred deployment model, whether on-premises, cloud-based, or hybrid, and can be implemented within weeks rather than months.

Compliance and Reporting

Ensure your chosen SIEM can help meet regulatory and compliance requirements relevant to your industry. Built-in reporting templates and capabilities that are easily accessible to compliance auditors can streamline the audit process, allowing your IT and security staff to focus on their core responsibilities.

Look for robust, customizable reporting features and dashboards that can be tailored to different stakeholders' needs. Creating and scheduling reports for various audiences, from operations analysts to C-level executives, is critical for transparency and accountability.

Ease of Use and Deployment

An intuitive, user-friendly interface is essential for efficient navigation, rule configuration, and data interpretation. Look for solutions that support natural language queries, reduce dependency on complex query languages, and boost analyst productivity.

Consider the ease of deployment and ongoing maintenance. Solutions offering streamlined setup, automated updates, and minimal manual intervention can save significant time and resources. Assess the availability of training resources, documentation, and customer support to ensure a smooth adoption process.

Scalability and Performance

One of the most important characteristics of an effective SIEM is its ability to grow with your organization. It is highly unlikely that your needs will ever decrease. To the contrary, anticipate continually escalating data volume, additional log sources, and higher event throughput. As you shop for alternatives, consider data storage costs and the ease of integrating new devices, endpoints, and log sources.

Performance is equally critical. Your SIEM should offer real-time analysis and alerting, leveraging production-level AI to process data swiftly and respond to queries promptly. This ensures that your security team can react to threats in real time, minimizing potential damage.

Consider a cloud-native solution, as it will most likely provide the agility needed to scale quickly and efficiently without compromising performance.

Empowering Your Cybersecurity Strategy

Selecting the right SIEM solution is pivotal in strengthening your organization's cybersecurity posture. By focusing on scalability, integration capabilities, advanced analytics, ease of use, and compliance features, you can choose a SIEM that meets your current needs and adapts to future challenges.

Anomali scales without compromising performance and is a fraction of the cost of other solutions. It is compatible with every log source in your environment, ensuring complete visibility. Moreover, Anomali lets you search through petabytes of logs — even rich historical data — in seconds. Its generative AI-based Copilot supports natural language queries, flattening the learning curve and slashing analysts' workload by half.

When you select Anomali as your Security Operations Platform, you get curated access to the largest global threat intelligence repository, coupled with ETL, SIEM, SOAR, TIP, UEBA and XDR capabilities. It is quick to deploy, features an intuitive user interface, and costs a fraction of other SIEM solutions.

Ready to elevate your security operations further? Schedule a demo of Anomali to see how our cloud-native, AI-Powered Security Operations Platform can transform your organization's cybersecurity posture.

Security Operations Done Differently.

Anomali is the leading AI-Powered Security Operations Platform that delivers mind-blowing speed, scale and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, XDR, SOAR, and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

Request a demo to learn more about AI-Powered Security Operations Platform.

ANOMALI