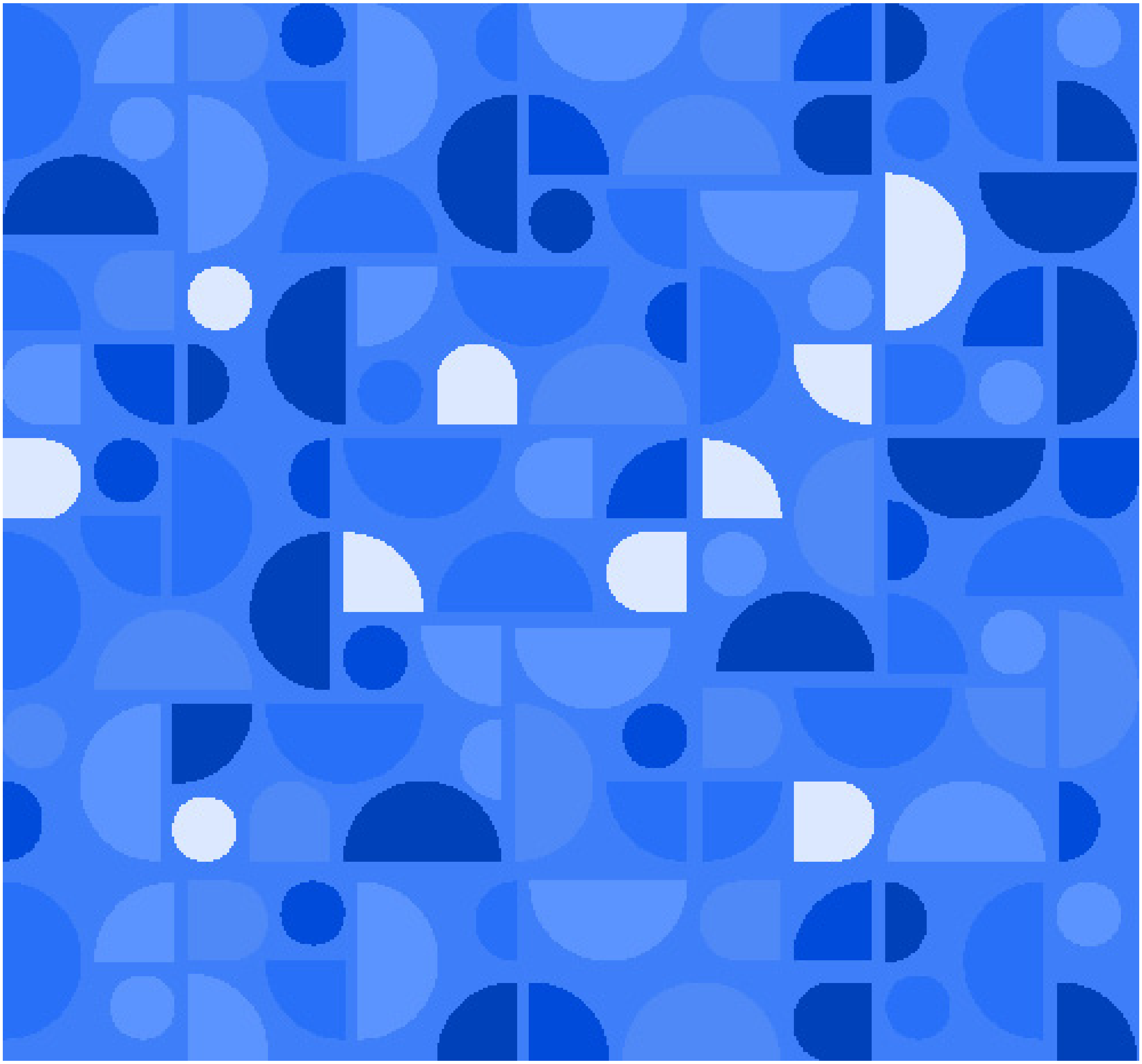

The Modern SIEM Evaluation Guide

How to select a SIEM that meets your security needs without significant overhead.

Blumira

Blumira.com

The Blumira Modern SIEM Evaluation Guide

A SIEM (Security Information and Event Management) platform is a necessary centralization tool that manages security event information across disparate security platforms. SIEMs centralize this data in order to investigate and detect threats, prevent attacks, and provide reporting for incident remediation and compliance. With cybersecurity threats at an all-time high, it is crucial to select a SIEM that fits your organization's needs. No two SIEM solutions are created equal and making the wrong choice can result in unpredictable costs, burdensome maintenance, and significant overhead.

When a SIEM platform is put in place, it will not automatically detect all possible malicious activity within an organization. While many SIEM platforms do come preconfigured with a certain set of alerts, dashboards, and reports, these pre-set tools still need to be customized. Each environment is completely unique and a SIEM must be properly configured to be tailor-fit to its environment.

A SIEM will be one of the most customized aspects of your security architecture. As your network changes, new software is added, or new behavior is seen, your SIEM must continue to be updated and fine-tuned. This is why it is crucial to understand what to look for when evaluating SIEM solutions to find the platform that will best fit your unique security needs without demanding significant time and resources.

In this guide, you'll learn

- What to expect from a SIEM platform and why it is crucial to your organization's security strategy.
- Common challenges with the traditional SIEM approach.
- Key considerations for modern SIEM.
- The complete set of evaluation criteria to consider in order to select a SIEM that fits the unique security challenges of your business.
- What a sophisticated, modern SIEM with low overhead looks like in practice.

SECTIONS

Why Do You Need a SIEM?

A SIEM platform provides a centralized location to understand the activities in your IT environment. SIEMs aggregate complex, disparate security systems in order to investigate and detect threats, prevent and remediate attacks, and provide reporting for incident response and compliance. In the event of a breach, a SIEM is crucial in helping understand what happened, help prevent it in the future, and ensure your organization adheres to compliance and data security regulations.

In today's ever-evolving cybersecurity climate, businesses face more threats than ever before. Finding the right SIEM is crucial in protecting against the latest risks and equipping your organization with a robust security strategy.

What Should You Expect From a SIEM?

Traditionally, SIEMs have served a few key security functions, namely, providing a historical view into security events for audit and compliance, researching potential security threats to an organization, and detecting threats within the organization.

Your SIEM should provide and centralize:

- Malware Control
- Boundary Defenses
- Access Controls
- Accessible Use Monitoring (AUP)
- Application Defenses
- Compliance and Audit Data Requirements
- Monitoring and Reporting
- Deployment and Infrastructure Activation
- Network and Host Defenses
- Network and System Resource Integrity

Challenges With the Traditional SIEM Approach

Although SIEMs have existed for decades, up until recently, they came with considerable pitfalls. Deploying and managing these systems is often expensive, complex and inefficient. Consider the following challenges when evaluating a legacy SIEM solution.

Time-Intensive

Legacy SIEMs are complicated to deploy and difficult to manage. Not only do users of these systems have to manually build, monitor and modify rule sets, they also have to manually collect, configure and maintain threat intelligence feeds. All of this work puts a significant strain on internal resources and makes it nearly impossible for an organization to scale its threat detection and response.

Requires Costly Expertise

The process of configuring and deploying a traditional SIEM requires an organization to either hire or contract expensive, expert security resources. In a recent study on SIEM, 40% of respondents said a lack of skilled staff was the biggest hurdle in maximizing the value of their SIEM platform. Without a specialized in-house security team or network of experts, it is nearly impossible to install a traditional SIEM. But the need for experts doesn't end at deployment. In a legacy system, although threats are identified, the data must be interpreted in order for an organization to know how to respond. Without a team of experts, a legacy SIEM will not fully protect an organization from security risks.

Inefficient & Unactionable

Traditional SIEM solutions have a significant infrastructure footprint, driving data consumption that can lead to unpredictable costs and energy inefficiency. Organizations using these systems will also often experience a high volume of false positive alerts that require dedicated security resources to review, leading to alert fatigue. Lastly, when a legacy SIEM surfaces a known threat, response is often delayed until a security expert can assess the situation, rendering the threat temporarily unactionable and exposing the organization to vulnerabilities.

Key Considerations for Modern SIEM

Traditional SIEMs' reliance on manual, rule-based implementation, threat detection, and maintenance have made them impossible to scale and incomprehensive in today's ever-evolving security environment. Although some SIEM platforms have advanced to address current cybersecurity challenges, there are still significant variations between SIEMs in their deployment options, automation offerings, and overall efficacy. When considering a modern SIEM, it is essential to ask the following questions.

Deployment

Today, 54% of organizations have SIEM deployed on-premises. SaaS SIEM solutions can significantly lessen infrastructure footprint, manageability, and cost, making it important to investigate if a cloud-based SIEM solution is right for you.

- Does the service require significant product-specific training in order to deploy and manage?
- Is the service delivered as a SaaS platform, limiting the infrastructure footprint?
- Does the service integrate with your existing technology stack?

Automation

- Does the service include broad threat intelligence feed coverage without requiring manual configuration or third-party licensing?
- Does the service automatically begin detecting threats as soon as it starts receiving security events and logs?

Automation (cont)

- Does the service limit the need to manually create rule sets?
- Does the service automatically block new threats discovered using next-generation firewall dynamic block lists?

Efficacy

- Does the service detect lateral movement using honeypot technology?
- Does the service limit false positive alerts?
- Does the service integrate with next-generation firewalls to automate the blocking of known threats?
- Does the service provide community-based threat intelligence to block known threats?
- Does the service provide actionable playbooks to follow when threats are detected?
- Does your solution retain logs for one year and include backups?

Comprehensive SIEM Evaluation Criteria

Your organization's security needs are as unique as your product offering. A modern SIEM should work for you, not against you, to centralize and automate the detection, remediation, and reporting of cybersecurity threats. The following questions are designed to help you find a SIEM that will provide maximum protection against security risks while minimizing the effort required from your organization.

Deployment & Configuration

- Does the solution integrate and work with your existing products?
- Can the SIEM be deployed in a matter of hours?
- Does the solution centralize and retain logs as a cloud-delivered platform?

Threat Detection

- Is security event information automatically correlated?
- Does the solution provide correlated threat intelligence from multiple threat feeds?
- Does the service reduce the noise of false-positive alerts associated with legacy SIEM products?
- Does the service detect lateral movement using Honeypots?

Automation

- Does the solution have the capabilities to automated security response capabilities when a cybersecurity threat is detected?
- Does the solution automate the blocking of community detected threats?
- Does the solution integrate with next-generation firewalls using dynamic IP blocklist capabilities?

Remediation Playbooks

- Does the solution have configurable alerting, including out-of-band notification capabilities such as SMS and voice call?
- Does the solution automatically prioritize detected suspicious activity and threats?
- Does the solution provide actionable response playbooks that can be completed by any IT professional?

Reporting, Analytics & Compliance

- Does the solution provide pre-populated dashboards?
- Does the solution provide simple reporting capabilities?
- Does the solution provide reporting capabilities for compliance purposes?

Blumira: A Modern, Highly Automated SIEM

Preconfigured so you don't need a security team to run it

A centralized SOC without the need for an actual SOC, the Blumira platform is a highly-automated SIEM solution that provides rapid threat detection, prevention and response without the need for an expert security team. We believe that all businesses should have access to best-in-class security software, which is why our pricing is not only affordable, but also predictable.

Our cloud-based platform can be deployed in hours and starts delivering results in days without the need to invest in third-party tools, infrastructure or extra people. Blumira is preconfigured to detect attacks and each actionable finding comes with clear remediation guidance specifically designed for easy execution by the team you have today.

The Blumira Platform is Preconfigured to:

Collect and Centralize Security Events

Applications and security tools across your environment connect with Blumira's virtual sensor to collect and stream security events, logs and alerts straight to Blumira's cloud service.

Rapidly Detect Cybersecurity Threats

Security event information is correlated and threat intelligence is applied to detect known and suspected cybersecurity threats. Backend automation and fine-tuned alerting increase the effectiveness of threat detection while reducing the noise of false-positive alerts. Virtual Honeypot(s) are deployed with the click of a button to detect lateral movement across your environment.

Provide Guided and Actionable Remediation Playbooks

Notifications are sent when suspected and known security threats require manual intervention. Guided and actionable remediation playbooks enable any member of your organization to easily respond and stop the security threat, even when the responder might not have security expertise.

Rapidly Detect Cybersecurity Threats

Security event information is correlated with threat intelligence to quickly detect known and suspected cybersecurity threats. Backend automation and fine-tuned alerting increase the effectiveness of threat detection while reducing the noise of false-positive alerts. Virtual Honeypot(s) are deployed with the click of a button to detect lateral movement across your environment.

Automate Remediation

When known cybersecurity threats are detected, automated remediation capabilities can implement blocking rules to stop active threats without manual intervention.

Report on Security Findings and Activities

Pre-populated dashboards and reporting help organizations understand the security threats found within their environment and the actions they need to take in order to adhere to compliance regulations.

> “Blumira does the heavy lifting to pare down the overwhelming amount of data from logs into actionable events. That allows us to focus on revenue enhancing activities for our internal team. We could probably have a full-time person doing just log management. Instead, we are spending, on average no more than 2 to 3 hours a week, taking action on the most serious threats”
>
> – **Michael Cross**, Chief Information Officer, Greenleaf Hospitality Group

Security threats are constantly evolving and traditional SIEMs are unable to keep pace. Unscalable solutions that require immense effort from expensive teams of security experts prevent even the largest of enterprises from achieving a robust cybersecurity program. When assessing which SIEM product to choose for your organization, it is crucial to understand each solutions’ deployment and configuration options, the extent to which it automates threat detection, if it provides playbooks for remediation, and whether or not its’ reporting is comprehensive enough for your needs.

Blumira’s cloud-based easy-to-use platform provides an all-in-one tool to effectively protect your organization from evolving and new security risks without the need to hire an expensive team. Our mission is to provide affordable, comprehensive security solutions to organizations of all sizes -- without complication or overhead.

Ready to Get Started?

Get your free account with Blumira and secure your Microsoft 365 environment in minutes. No credit card required.

Sign Up Free