3 Critical Success Factors For Choosing a New SIEM

While no solution can prevent all attacks, some security information and event management (SIEM) solutions can detect intrusions and anomalous activity better than others. Many SIEM solutions require specialized expertise to customize and maintain the system — or are too costly for ingesting, analyzing, and maintaining all the logs that might help your teams discover what happened; when, where, and how it happened; and which credentials were involved.

Combating these challenges requires a system equipped with pre-built rules, behavioral models, timelines, and the suggested investigation steps to find the true gems of discovery amidst the noise of alerts.

There are a lot of SIEMs in the marketplace from which to choose. But how do you distinguish between SIEM vendors to find the right fit for your organization?

Here are the three main success factors to consider when selecting a new SIEM:

1. Keep up with a high volume of threats buried in a sea of noisy alerts

Ever-increasing attack surfaces, personnel shortages, and other factors are driving organizations to look for ways to improve their security posture. SIEM is a great solution for enhancing visibility and overall security, but many are overly complicated and don't deliver the desired results.

Many organizations see significant limitations with their current SIEM. Some see it as a log management platform not purpose-built for security, offering only limited security capabilities and visibility into incidents. Other complaints include excessive alerts, false positives, and considerable expense, and that it demands expert-level skills to manage.

As a Next-gen SIEM, Exabeam uses a behavior-based approach to threat detection, investigation, and response (TDIR). Leveraging industry-leading behavioral models, Exabeam creates histograms to automatically baseline "normal" behavior of users and devices to detect, prioritize, and respond to anomalies based on risk. By aggregating all relevant events and assigning them a risk score, Exabeam weeds out the noise. Exabeam Fusion SIEM is proven to boost analyst productivity and detect threats missed by other solutions.

2. Scale detection, investigation, and response with advanced analytics and security visibility

According to the 2022 Verizon Data Breach Investigations Report, the number of breaches involving compromised credentials is a whopping 93% — and nearly all have involved lateral movement. Detecting lateral movement from device to device — let alone from device, to cloud, to on-premises resources — is nearly impossible without robust behavioral models and fact-based correlation rules.

Exabeam integrates with hundreds of security solutions and thousands of log sources, and offers more than 1,900 behavioral rules and models, and threat intelligence to deliver world-class TDIR. Focusing on high-value events, improving attack chain visibility with MITRE ATT&CK coverage, and use-case enrichment of events offer your team more focused, accurate, and repeatable results.

3. Get a holistic view of an incident and automate mitigations to speed resolution

Legacy SIEMs struggle to keep up with expanded threat vectors and the pace of attacks. With limited correlation, analytics, search, and visualization capabilities, organizations are either overmatched or forced into manual workflows with limited success. Automation plays a key role in improving productivity and ensuring repeatable results if an investigation is warranted.

Through natural language querying, context-enhanced parsing, and data presentation, Exabeam improves analyst efficiency and effectiveness from detection to response. Fusion SIEM offers 1,900 pre-built correlation rules and 750 pre-built models, allowing less-skilled employees to manage it — thus enabling ROI, decreasing costs, and strengthening the ability to hire. With nearly 8,000 parsers — more than four times the industry average — as well as the ability to easily create new ones in minutes, Fusion SIEM can quickly absorb new data sources, parse them with a common information model (CIM), and enrich events with context from threat intelligence to bring you security-relevant events and alerts.

	exabeam	Legacy SIEMs
Detection Content		
Behavior-Based Models to Detect Abnormalities	750+ Behavioral Models	X
Detection Rules to Detect Known Threats	1,800+	✓
Integrated Commercial-Grade Threat Intelligence	✓	X
Detection Content Mapped to Use Cases	✓	X
Investigative Automation		
Automatically Generated Smart Timelines	✓	X
ML-Based Alert Prioritization	✓	X
Pre-Built Watchlists for Risky Users and Entities	✓	X
Log Management		
3rd Party Vendor Integrations	550+ 3rd Party Integrations	~400 3rd Party Integrations on Average
Search Query Builder Assistant	✓	X
Up to 10 Years of Searchable Data Without Rehydration	✓	X
Deployment Architecture		
Fully Cloud Native	✓	Partial
Multitenant	✓	✓
Integrated SIEM + UEBA + SOAR	✓	Partial

Conclusion

To address today's security problems, you need solutions developed by security people for security people. Instead of expensive legacy "multi-purpose" tools whose claim to fame is "efficient indexing" and "fast searches," choose a tool that finds the threats other tools miss.

Some competitor SIEMs are not equipped to detect lateral movement or understand the behavior of high-risk assets or users. Events aren't filtered into high-value timelines; their correlation and reporting are manual and require skilled professionals.

Your team needs to know what to look for, and that is impossible for modern attacks that have been designed to evade detection methods based on correlation rules. Some solutions offer only a bunch of noisy correlation rules that generate expensive false positives, while the true attacks are not detected.

Get a solution that leverages all the latest cloud technologies for data ingestion, storage, and powerful analytics. Exabeam prepackages log parsers, rules, correlations, integrations, reports, and threat intelligence.

According to the 2022 Forrester Total Economic Impact™ (TEI) Study of Exabeam Fusion SIEM, after deploying Exabeam:

- Security operations teams gained a centralized view of their ecosystem that allowed them to more quickly review and investigate security alerts and incidents.
- One team saw a more than a 70% drop in the number of incidents that needed to be investigated.
- Another firm was assessing the ability to provide more security coverage with less-experienced staff.
- Customers experienced quicker recognition and response to internal and external attacks, and reduced financial losses.
- An organization no longer needed costly third-party incident response services to pull information for legal defense. The CISO reported saving more than $100,000 for just the investigation component for one event.
- Customers realized cost savings from transition to the cloud, reduced cost of system management, and reduced downtime.

Insights from Exabeam helped one team see a greater than 70% drop in the number of incidents that needed to be investigated.

Exabeam customers realize an ROI of up to 245% over six months

Based on the 2022 Forrester Consulting TEI Study of Exabeam Fusion SIEM

Exabeam provides customers with pre-built rules, timelines, and suggested guidelines for purpose-built security investigation to defend against the endless threats posed by attacks such as ransomware, phishing, and brute force attacks. We are leading the industry with solutions to help you constantly adapt to the evolving world of cyberthreats.

Whether it's malicious insiders, compromised insider credentials abused by Lapsus$, or zero-day attacks from nation-states or organized crime, Exabeam helps your team to keep up with the growing number of daily threats via our cloud-native solutions and security tactics focused on generating incident resolutions, consistently and repeatedly.

No SIEM can prevent all attacks, but some detect them better than others. Choose a solution that includes advanced analytics capabilities with machine learning and security models that separate the real threats from the noise, clearly indicating what is abnormal behavior and needs to be investigated.

Get an Exabeam Fusion SIEM demo today, and think of us when it's time to renew!

Uplevel Your Team

Everyone is short of employees these days, and security operations teams are certainly no exception. One way to help address skillset shortages is automation, and Exabeam Fusion requires much fewer skills than its competitors.

And if you are in an organization fortunate enough to have highly skilled security pros, doesn't it make more sense to better utilize their skills? Free up your security team to do more value-add tasks.

The Forrester Consulting TEI Study found that the Exabeam customers they interviewed unanimously said that they could operate more effectively with less-skilled employees.

They worried less about employee churn, and more about recruiting people with the right aptitude for the job. As a result, they could fill positions faster, with a shorter ramp time.

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now →