exabeam

Guide

The 5 ~~Lies~~ Claims a SIEM Vendor Should Never Make

And they do!

A SIEM is a very established technology with a mature set of vendor products. However, with that maturity, the SIEM is a victim of scope creep. Over the years, new capabilities, edge requirements, and delivery models have resulted in a product that barely resembles Version 1. The complexity of today's SIEM is legendary (well-documented, well-understood), a byproduct of this explosion in scope.

While the evolution of the SIEM has resulted in a product that is far more powerful today than at its conception, vendors have overstated, overhyped, and over-promised about its capabilities. Many users have been burned — here are the five claims you need to watch out for.

1. More data means better security

SIEMs have been around for over 15 years and are an important part of many security strategies. A common trend is to increase log volume and add multiple sources with the goal of missing nothing, but oftentimes, threats are still missed and attackers are still getting through. During this, your organization will incur increasing costs for log storage and processing which will likely benefit your SIEM vendor a lot more than you.

2. SIEMs are excellent at detection

SIEMs have been around for over 15 years and are an important part of many security strategies. A common trend is to increase log volume and add multiple sources with the goal of missing nothing, but oftentimes, threats are still missed and attackers are still getting through. During this, your organization will incur increasing costs for log storage and processing which will likely benefit your SIEM vendor a lot more than you.

3. SIEMs let you see the entire picture

SIEMs are completely dependent on the SOC analysts and SIEM engineers building rules and running queries. Most organizations can have between 20 and 200 rules, but we know that there are thousands of different threat indicators of compromise in the data. Missed events (false negatives) represent blind spots in your security posture. Many SOCs have been distracted by metrics and operational efficiency because of the shortcomings of SIEMs.

4. Correlation rules are amazing

Peak SIEM performance and return are dependent on the SOC team building and managing rules. Adding more data doesn't reveal any additional threat intelligence without necessary rules; it is just more expensive. The SOC of the future needs to understand the importance of moving away from the dependency on rules by adopting tooling that helps them do their job. By adding both intelligent analytics and automation to your SIEM, you can have over 90% coverage of the threat spectrum with the right log sources. Simultaneously, you will enjoy minimal false positives, automated event timelines, and alerts prioritized by severity.

5. SIEMs eliminate the manual and repetitive work

SOC teams' time should be spent investigating and responding to events and alerts, but they are often buried in repetitive tasks such as identifying false positives and reporting them, writing rules for event escalations, and queries/pivot tables.

Although SIEMs can provide significant business value as log management, business operations, and analysis tools, they do not deliver great value in their original purpose of detecting threats. And overall, they often don't truly help the SOC team do their job.

Exabeam Fusion

As the leading Next-gen SIEM and XDR, Exabeam Fusion provides a cloud-delivered solution for threat detection and response. Exabeam Fusion combines behavioral analytics and automation with threat-centric, use case packages focused on delivering outcomes. Exabeam Fusion is modular, we can augment your legacy data lake or SIEM deployment with XDR, or replace your SIEM entirely. It's your call.

Exabeam Fusion provides the following benefits: Industry-leading behavioral analytics to detect threats other tools miss

- Advanced alert triage capabilities — 83% of analysts report the ability to triage twice as many alerts as a legacy SIEM
- Faster threat detection and response, as much as 50% faster
- Built-in automation with predefined workflows and checklists to improve analyst productivity
- Advanced SOC functionality with threat-centric, use-case packages to deliver specific, desired outcomes
- Metrics to show whole analyst team improvement in Mean Time to Detect, supporting your SLAs

To learn more about how Exabeam Fusion can help, **request a demo today.**

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Operations Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm.

For more information, visit exabeam.com

exabeam