ANOMALI

GUIDE

Don’t Get Blown Away by the SIEM Storm:

AI-Powered Security Operations to the Rescue

Don’t Get Blown Away by the SIEM Storm:

AI-Powered Security Operations to the Rescue

There’s a lot of turbulence happening in the SIEM market. Your favorite product just got bought (Splunk junk in the Cisco trunk), merged (“ExRhythm”), or sold for parts (RIP QRadar).

All this turbulence may have you wondering about the future landscape, the impact of these changes on your organization and if it’s time to reassess your security stack.

In these rough seas, it’s tough to predict whether an acquiring company will have the same objectives, vision, and roadmap as the original vendor. Which puts you in an interesting bind:

- Will they continuously improve visibility and threat protection?
- Will they be as agile (if they ever were) in keeping pace with your needs and the evolving threat landscape?
- Will your product even exist in two years?

Whether your ability to execute is directly impacted by recent mergers and acquisitions or you are preparing for a renewal, now is a fortuitous time to proactively evaluate your needs for threat detection, investigation, and response and the solutions required to meet them.

The million-dollar question: **Is your current SIEM working for you?**

Here are five requirements you need to stay afloat amidst the SIEM maelstrom.

1. Comprehensive threat visibility across all attack surfaces

It’s critical to be able to query data from every source in your ecosystem — switches, firewalls, email, network traffic, databases, DNS, cloud, and more. Most SIEMs fall short in this area.

Looking back, the original purpose of SIEM was to consolidate data from multiple log sources (firewall traffic, detection systems, switches, routers, and so on) to facilitate analysis. In 2005, when the term

"SIEM" was first coined, there was no easy way to sift through these volumes of data to extract actionable intelligence. Manual analysis was tedious and time-consuming. SIEM was the answer for automating log collection and analysis.

The challenge with SIEM has always been collecting and consolidating logs from thousands of products from hundreds of vendors — a mountain of machine-generated data. However, in recent years, the complexity has compounded.

The types of data and the number of tools and vendors have increased by orders of magnitude. Moreover, bad actors have developed more sophisticated, multi-faceted attack techniques that have the potential to leave data trails in multiple security environments.

To achieve the coverage required for a comprehensive defense, companies have had to bolt on specialized tools tailored for specific entry points and log sources. As the complexity mounted, SIEM has become only one component in the mix, as opposed to the security umbrella it was in its original incarnation.

If this situation sounds familiar, you're not alone. The good news is that you can reframe the turbulent SIEM market as an inflection point — the perfect opportunity to adopt a modernized solution that delivers on the SIEM's original intention.

Anomali is that solution. It provides connectors for virtually every device and product on the market, giving you unprecedented and unparalleled visibility. It's the SIEM for today's elastic ecosystem.

2. Ability to search hundreds of billions of events over years in seconds

The attacks are coming that fast and furious and you need to keep up. Searching historical log data with ease and efficiency is necessary for pinpointing suspicious activity and matching those findings with IoCs. However, most SIEM vendors don't provide access to historical datasets, hindering your ability to investigate incidents that occurred before a specific date (either when the SIEM was first deployed or an arbitrary default time period).

Even with access to historical logs, searching with legacy SIEMs is time-consuming and arduous. It often requires complicated queries and may take hours or days to get results — plenty of time for an attack to gain traction.

The Anomali AI-Powered Copilot gives you ready access to search all data as warm data from as far back as you like, using natural language queries instead of proprietary query language. Ask a simple question, such as "Were there any logins from this IP range between July and September of 2020?" and get answers almost instantaneously.

3. Containing costs amidst the rising tide of threat intel

With the volume of attacks increasing exponentially, the surge in data volume presents two additional challenges: rising costs and the need for intelligent data prioritization and filtering.

Most of the biggest SIEM vendors charge exorbitant rates for data ingress, storage, ingest, predictive analytics, and workload processing. Some have revenue models directly tied to data volume, disincentivizing them from helping customers optimize data ingestion. This can force a perilous tradeoff between comprehensive visibility and budgetary limitations.

Another stumbling block with legacy SIEMS is the difficulty of extracting actionable insights from vast datasets. It's tedious to sift through massive data volumes from diverse sources to pinpoint critical information.

The ideal solution involves automated data prioritization. This empowers you to focus your analysis on the most relevant data. It also optimizes storage and processing costs to ensure efficient resource allocation.

Anomali stores all of your data — including rich historical data — in an unlimited Security Data Lake. This data is always hot and immediately retrievable.

Of course, a giant pool of data is only as useful as the answers you can extract from it. Anomali helps you distill it down to only the data that matters. Copilot is always there, helping you search across petabytes of data in mere seconds.

4. Empower junior analysts to do the work of senior analysts

A recent report found that over 40% of companies struggle to fill critical cybersecurity roles, particularly in research and malware analysis. This issue is compounded because many SIEM products require senior analysts who understand extensive engineering concepts, such as data modeling, search heads, and clusters.

But it doesn't have to be that way.

Anomali's intuitive AI-Powered Security Operations Platform makes data analysis fast and easy, empowering new team members to operate as effectively as senior analysts. It lets you do more with less — slashing analysis time by half, boosting team efficiency, and reducing cost.

5. Leverage AI across the entire threat detection, investigation, and response lifecycle

AI is transforming the way we detect, analyze, and respond to threats. And it's not a single-purpose tool: AI enhances multiple aspects of threat management, making our defenses smarter and more adaptive.

Not only does AI simplify search with natural language, it can take threat hunting to a whole new level. Imagine reviewing a suspicious file on one of your endpoints and having an adjacent sidebar on the screen alert you in real time that the filename matches a zero-day exploit. AI makes this possible.

You can use AI to understand the nuances of your environment and effortlessly build machine language models from users' behavior patterns or typical data flow. It can also reduce alert fatigue. Contextual awareness enables it to distinguish between a genuine threat and a false positive, ensuring that you only receive and spend time addressing alerts that matter.

But AI isn't just about defense — it's about resilience. AI can help defend against increasingly common AI-powered threats. These threats use machine learning to adapt and evolve, making them harder to detect and neutralize with traditional methods. Anomali's AI-Powered Security Operations Platform keeps you one step ahead, using its own sophisticated algorithms to outsmart malicious AI.

The bottom line

The SIEM market's turbulent landscape presents the perfect opportunity to adopt a modernized umbrella solution that delivers on the intention of the original SIEM but is better equipped to meet the new clouds on the horizon. It's time to evaluate, adapt, and ensure your organization (and your resume) is equipped to handle today's cybersecurity challenges with the best tools available. Don't get lost at sea. It's time to Be Different.

Learn more about the leading AI-Powered Security Operations Platform

Schedule a live product demo or visit anomali.com to discover how Anomali can help you leave the SIEM market chaos in your rearview mirror. Experience Security Operations Done Differently.

Be Different. Be the Anomali.

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, SOAR, TIP, and XDR 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 the Anomali AI-Powered Security Operations Platform.