SentinelOne®

Is SIEM Really Dead? Or Has It Just Evolved?

Go Beyond Next-Gen with AI SIEM

White Paper

Introduction

Across an ever-changing cybersecurity market landscape, technology's evolution is the only constant. Vendor consolidation occurs alongside endless jockeying for competitive advantage and the echoes of ever-louder marketing hype. For buyers, the number of capabilities that must be part of every "enterprise-grade" security stack continues to grow yearly. This means that security infrastructures become more complex, integrating and correlating data is increasingly difficult, and security analysts' jobs get harder and harder.

Yet threats keep rising in volume and sophistication, and the costs and losses associated with data breaches inevitably reach new all-time highs on an annual basis.[1] Amid these formidable challenges, it's no surprise that many stakeholders in the field of cybersecurity are looking for change.

Because security information and event management (SIEM) platforms serve as the cornerstone technology for mature security operations (SecOps) programs, housing the data that's their lifeblood and enabling detections, threat hunting, and operational intelligence, it's also unsurprising that this market category is in the crosshairs.

In 2024, a set of mergers and acquisitions (M&As) that took place in rapid-fire succession further upended the SIEM space. Just hours after LogRhythm, which had struggled to adapt its products for a cloud-first world, announced its impending merger with Exabeam,[2] best known for its high-quality user behavior analytics (UEBA) product, Palo Alto Networks announced plans to acquire IBM's entire QRadar software-as-a-service (SaaS) business.[3] These developments took place only a few months after Cisco had completed its acquisition of Splunk.[4]

For several prominent thought leaders and industry analysts, the M&As signaled the death of SIEM as a market category. Google Cloud's Anton Chuvakian wrote on X that all three SIEM tools had "died" that day, and his words were echoed by several others. Of IBM's sale of QRadar, Forrester analyst Allie Mellen proclaimed that it was "the biggest concession of a SIEM vendor to an XDR vendor so far" and signaled "a sea change for the threat detection and response market," such that "security buyers may finally be getting the SIEM alternative they've been seeking for years."[5]

While we agree with Mellen that large-scale changes in the security analytics market are afoot, we don't believe that XDR can or will be the primary SecOps tooling in enterprise-grade security programs. We also agree that security buyers may finally be getting access to a better option than traditional SIEM, but we don't believe that an alternative tool or solution will play this role.

Instead, we're confident that an entirely new category of SIEM is about to emerge, one that (finally) delivers on the promise that SIEM has had since Gartner first gave it its name back in 2005.

[1] IBM Security, Cost of a Data Breach Report 2024, July 2024.

[2] Thoma Bravo Press Release, "LogRhythm and Exabeam Announce Intent to Merge, Harnessing Collective Innovation Strengths to Lead the Future of AI-Driven Security Operations," May 2024.

[3] Forrester Research Featured Blog, "IBM Surrenders SIEM While PANW Tries to Gain Ground on Tech Titans," May 2024.

[4] Cisco Press Release, "Cisco Completes Acquisition of Splunk," March 2024.

[5] Forrester Research Featured Blog, "IBM Surrenders SIEM While PANW Tries to Gain Ground on Tech Titans," May 2024.

The Evolution of SIEM and Security Analytics Platforms

SIEM was born out of consolidating two previously separate technology categories, security information management (SIM) and security event management (SEM). Vendors brought these tools together to increase real-time visibility across corporate networks and expand IT environments. This need resulted from growing awareness that the firewall-centric, perimeter-based models that were then standard for securing networks were inadequate to defend against increasingly sophisticated threats.

As it became increasingly apparent that intruders able to circumvent the firewall's traffic filters had nearly unlimited access to devices on the network—and as internet connectivity exploded—intrusion detection systems (IDS) grew in popularity. These tools can monitor network traffic for evidence of known malicious activity but cannot block threats independently. In addition to requiring security analysts to manually intervene to act upon the alerts they generated, IDS tools tended to be noisy. The static detection rules early IDS solutions relied on were often a poor match for the varied and increasingly complex nature of attacks, leading to high false positive rates. Correlating the security alerts that IDS generated with those created by antivirus software and firewalls promised to yield a clearer picture of what was taking place on the network—enhancing visibility and detection accuracy simultaneously.

This is the role that SIEM was created to fill. In essence, it was intended to be a centralized place where data from other solutions could be gathered, normalized, correlated, and made available to security teams for analysis.

First-generation SIEM solutions had notable shortcomings, including a lack of scalability, cumbersome processes for ingesting data, setting policies, managing alerts, generating reports, and general user-unfriendliness. Nonetheless, they became standard and central in enterprise-grade security operations centers (SOCs) because their ability to bring log and telemetry data together proved invaluable for multiple purposes.

What SIEM was Built to Enable

Compliance

Regulatory mandates such as HIPAA, PCI-DSS, and the Sarbanes-Oxley Act (SOX) all have reporting requirements that demand a centralized logging solution. While it might theoretically be possible to meet these requirements by gathering the data manually, it's certainly not easy, especially when the number of hosts and security tools involved gets larger. Problems of scale become even more acute if an organization is subject to multiple compliance rules. SIEM has been promoted as a solution to these reporting challenges since its inception, and the reality is that these capabilities are still required by regulators and needed by enterprises.

Detections

Centralizing security alerts, logs, and telemetry data from across the organization's technology environment should—at least, in theory—enable security analysts to understand everything occurring within it. Funneling this information into a single place enables unified visibility since alerts can be correlated across different data sources, enriched with threat intelligence, and prioritized for remediation. Such visibility makes it possible to identify the patterns indicating an in-progress attack, even as they span various devices, systems, and assets. This accelerates threat detection while improving its accuracy.

Threat Hunting

As a centralized repository of security-related information from across the enterprise, the SIEM can function as a master archive of everything that's taken place there. This makes it possible to investigate suspicious activities and search for active threats that may have ongoing access to the environment. If an incident is known to have occurred, the SIEM houses historical data that can be used for subsequent forensic analysis.

Analytics

By combining data from diverse sources into a single repository, SIEM platforms provide an efficient access point for analytics. The goal is to save the time and manual effort involved in bringing the information together, making it possible to identify patterns and behavioral trends in real-time.

Response

First-generation SIEM platforms typically relied on integrations with other security tools to initiate responses to the alerts and notifications they generated. Still, these extensive integrations had the potential to streamline incident response workflows. More recently, SIEM vendors have added integrations with (or built-in capabilities resembling) orchestrated response platforms to introduce automation into these workflows.

The centralization of data that SIEM was created to enable has become more important for modern enterprises confronting explosive growth in the amount of security data available across highly distributed and cloud-centric IT ecosystems. If anything, it has become more important since threat actors have perfected the art of hiding the traces of their presence amidst the noise that comes from high false positive alert volumes.

Misalignment Between SIEM Offerings and Market Needs

What made SIEM challenging to build at the time of the category's inception was that storing large amounts of data was expensive, querying large data stores was computationally intensive, and integrating security tooling from multiple vendors proved all but impossible. Versions of these issues continue to be a problem for SIEM users to this day—as well as for the enterprise decision-makers tasked with choosing solutions.

All of them relate to challenges in operationalizing data. These challenges underlie the vast majority of the complaints that SIEM's end users have, as well as the reasons that analysts like Mellen give for SIEM's "death" within the market.

In particular, there tend to be issues with:

- **Data ingestion and retention costs:** This is a significant problem for SecOps programs, and it has existed for a long time. The more data a SIEM platform can ingest and leverage, the more accurate the detections can be. In recent years, however, and especially with the move to the cloud, volumes of events, telemetry, and log data have ballooned. Most SIEM vendors have moved their storage to the cloud as well. In the cloud, storage is inexpensive, but ingress and egress costs are high, so the problem of "more data, higher costs" persists. These cost considerations create an unwelcome tradeoff between staying on budget and optimizing visibility and detection effectiveness. Data retention costs create a similar challenge: threat hunting is more detailed and comprehensive when more historical data is available for analysis, but keeping security data tends to raise costs.

- **Performance:** Security analysts have long cited slow query speeds as a major source of frustration when working with SIEM platforms. When data architectures aren't optimized for rapid retrieval, alert triage, and threat hunting can take a long time—a major problem when accelerated response is key for mitigating damage from active threats and preventing initial intrusions from becoming breaches.

  Data duplication, which is commonly used in traditional SIEM data architecture designs, speeds up queries, since they're then being run on smaller subsets of data copied into summary indexes, but adds the costs (and performance bottlenecks) that come with copying the data. When data is stored in multiple places, especially on-prem, data ingestion and retrieval can slow to a crawl. This problem gets exacerbated as data volumes grow.

- **Confusing workflows with multiple, difficult-to-navigate dashboards.** Traditional SIEM platforms have never been known for user-friendliness. Security analysts have long struggled to correlate events across multiple dashboards, to understand complex query languages, and to make sense of large volumes of alerts streaming across their consoles. In addition, maintaining these systems is complex, requiring expertise in configuration and rule-building, typically involving extensive custom coding. Because these processes are so time-consuming, they often leave resource-constrained teams without the time they need for activities like threat hunting that allow for proactive risk reduction. And when solutions are painful to work with, it only adds to the challenge of recruiting and retaining talent, which is already a major issue for an industry where there's a global workforce shortage of nearly 4 million professionals.[6]

[6] World Economic Forum, Bridging the Cyber Skills Gap, 2025.

- **Integrations.** This goes along with data normalization and standardization. Despite the fact that security decision-makers voice a strong preference for a platform approach over point products in their solution stacks,[7] the reality is that most organizations maintain at least some legacy tools and systems, with single-vendor security stacks remaining the exception, not the rule. This means that there's nearly always a need to ingest data from third-party solutions, and the better a SIEM solution is able to do this, the more comprehensive the visibility and detections it can deliver.

  However, integrating telemetry data from other vendors' tools is often difficult and laborious—if it is possible at all. Cybersecurity vendors often have a vested interest in making sure that this continues to be the case (achieving lock-in with customers), even if it works against the "bigger picture" goal of building more resilient defenses. Often, also, when vendors offer larger numbers of integrations, the quality and accuracy of detections suffer, particularly when—as is often the case—discrepancies in data types and formats make it difficult or impossible to correlate across various sources.

These difficulties persist among users of first-generation SIEM platforms to this day, and they continue to inhibit SecOps teams from building effective threat detection and triage workflows.

Importantly, SIEM platforms have historically been lacking in automated response capabilities. To empower defenders to take immediate action against newly detected threats, SIEM vendors have built integrations with security orchestration, automation, and response (SOAR) platforms that allow users to create playbooks that can automatically initiate response actions when threats are detected. Implementing SOAR, however, creates many of the same integration and data management challenges that SIEM platforms themselves confront—in many cases, doubling the inconvenience while increasing demands for time, expertise, and manual effort (to build out playbooks and workflows).

Many of these shortcomings have resulted in frustrated SIEM users looking for a new way of achieving centralized operational visibility and control. Meanwhile, business decision-makers have been feeling mounting pressure from boards to mitigate real-world risks and improve security posture without greatly increasing budgets. This amplifies the enterprise's need for both effectiveness and efficiency in a SIEM solution.

Meeting Tomorrow's Needs: Moving Beyond Legacy and Next-Generation SIEM

Cybersecurity vendors have been striving to solve the challenges with traditional legacy SIEM for more than a decade now. They've sought to build newer solutions that are faster, more scalable, easier to operate, and better suited to modern cloud computing environments. Often, these efforts have taken the form of next-generation SIEM platforms, typically featuring machine learning (ML) and AI for more accurate threat detection, built-in automated response capabilities, and connectors that enable the ingestion of log data from SaaS apps and cloud infrastructures. These are welcome developments, to be sure, but don't go far enough.

A new approach to SIEM must still be able to serve all of the use cases that this technology was initially intended to address. However, it must also remove the obstacles that have long frustrated the security analysts who use these platforms. Alerting must be accurate, not excessive. Data must be comprehensive and complete but easily searchable. The SIEM must harness the full efficiencies that cloud-native architectures provide. The SIEM must be engineered to serve as the cornerstone for autonomous SOC operations.

[7] S&P Global Market Intelligence, Tectonic shifts in the SIEM landscape create disruption in the market, May 2024.

This means there is a need for revolutionary transformation in how data is stored (data architecture) and how analysts interact with data (dashboards and query languages). Meeting these challenges requires solving the following:

- **Scalability:** Traditional SIEM solutions were built on top of legacy databases or query/analytics engines like Elasticsearch, which were designed for indexed, text-based content, and these don't scale well for analytical workloads. Instead, a solution that can seamlessly store and rapidly search large volumes of structured, semi-structured, and unstructured telemetry and event data is needed.
- **Cost control:** Cost has long been traditional SIEM users' number one pain point because longer data retention improves investigation, triage, threat hunting, response, and even compliance, but it also raises cost concerns. When data growth outpaces budgets, stakeholders find themselves torn between supporting robust SecOps programs and reigning in expenses. Understanding what took place in a real-world breach situation usually requires more than 14 or 30 days' worth of historical data.
- **Flexibility and integration:** Seamlessly integrating all the tools that comprise modern security stacks remains a challenge for most traditional SIEM solutions. Raw logs are difficult to search and understand, and ingesting data from multiple vendors' tooling often demands time and expertise in building custom integrations, which may remain brittle or of limited use.
- **The elimination of data silos:** Data is only valuable when it's accessible for use, but without a centralized data strategy and highly usable repository, the same data ends up getting duplicated for use by different tools. This adds costs, inhibits visibility, and renders it impossible to make decisions on the basis of full situational awareness.

Making it easier (and more pleasant) for security analysts to interact with data requires:

- **An intuitive natural language interface** that empowers every analyst to run complex queries using easy-to-understand conversational inputs.
- **Accelerators for threat hunting** so simple tools and guides can reduce hunting cycle times from hours to minutes.
- **Support for collaboration** with unified data access and threat intelligence that's easy to share.

One key difference between the model we're describing here and the first-generation SIEM is the backend data architecture that supports it. What's needed is an innovative data storage architecture that can operate at low cost and high performance and scale. It must be able to ingest data from a broad array of first- and third-party sources, including apps, infrastructure, devices, security tooling, and cloud services. A centralized data lake architecture can provide comprehensive visibility at speed and scale. The ability to normalize data to the Open Cybersecurity Schema Framework (OCSF) and the Open Telemetry (OTel) standards supports true interoperability. Such standardization supports detection, streaming, retention, and query and analytics engines. This data architecture must support high-performance analytics and real-time detection, which should be available through a single console, one intentionally designed to give end users (i.e., security analysts) the great experiences that we've all come to expect as consumers.

This isn't just a list of all the functionalities that SIEM should have, but it isn't at present. Instead, this vision of the future of SIEM has already been realized and is available today in the form of **Singularity AI SIEM**, the industry's fastest AI-powered SIEM, converging SIEM, XDR, and automation capabilities in a single, cloud-native platform.

Singularity AI SIEM: The Future of SIEM Is Already Here

Enterprise security teams that have long been dissatisfied with the costs and sub-standard data enrichment (leading to time-consuming manual investigations and alert fatigue) that come along with traditional SIEM platforms now have an alternative. Singularity AI SIEM is a highly autonomous solution built on a cloud-native SaaS architecture and leveraging cutting-edge AI and automation to transform the security analyst's role from one that's full of monotonous tasks and hands-on investigations to one involving systems supervision and optimization.

Singularity AI SIEM was architected to drive operational efficiency and effectiveness by using rich, unfiltered data to drive autonomous operations and immediately mitigate critical threats. Tasks requiring human input are seamlessly augmented with AI, empowering analysts of all skill levels to confidently perform threat hunting and investigations.

Singularity AI SIEM's Cloud-Native SaaS Architecture:

- A columnar database offers unparalleled scalability, making it possible to retain 100% of data for deeper insights
- A massively parallel query engine leveraging container technology breaks down complex queries into fast-running tasks and swiftly aggregates results
- OCSF-compatible data ingestion makes it possible to bring in all the data—structured and unstructured
- Real-time threat detection upon ingestion
- Always-on hot storage ensures that data is always accessible with good performance, even for older historical data

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2024 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Industry-leading ATT&CK Evaluation

+ 100% Detections. 88% Less Noise.
+ 100% Real-time with Zero Delays
+ Outstanding Analytic Coverage, 5 Years in a Row

Gartner Peer Insights

95% recommend SentinelOne

Endpoint Protection Platforms reviews for SentinelOne Singularity Platform

FedRAMP

TEVORA PCI DSS Attestation HIPAA Attestation

SentinelOne

Contact Us

sales@sentinelone.com
+1-855-868-3733

sentinelone.com

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.