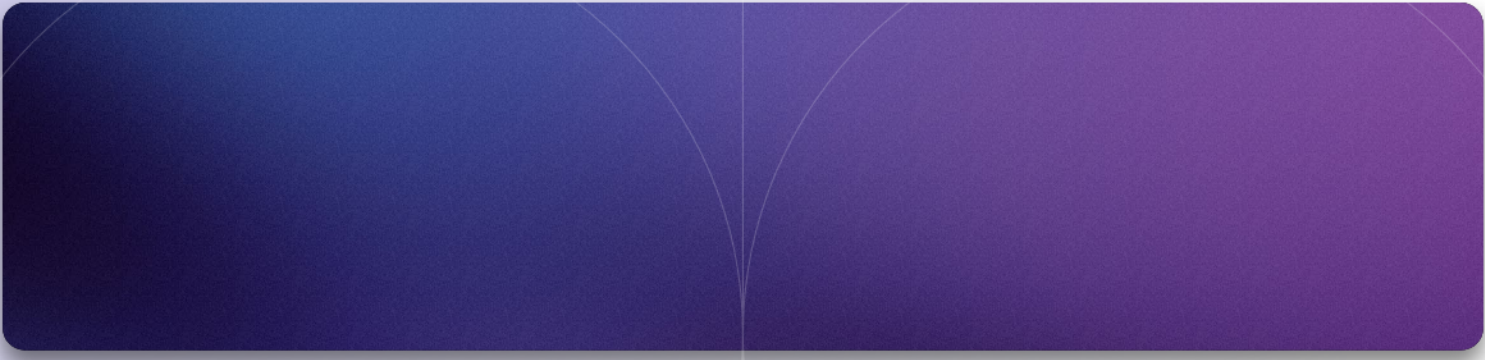




The Truth About SIEM: 5 Myths Standing Between You and Better Security Operations

White Paper



No single technology is more critical to effective security operations than **Security Information and Event Management (SIEM)**. SIEM lies at the center of every core workflow for security operations teams, from threat detection and hunting to triage and incident response. However, many organizations still harbor myths and suspicions around SIEM, based on poor experiences with legacy SIEM solutions, or an overall feeling that SIEM simply isn't made for them. These outdated impressions that SIEM is too complex, too slow, or too expensive prevent organizations from reaping the benefits and leveraging the transformative power of modern SIEM solutions.

Singularity AI SIEM is on the leading edge of autonomous SIEM solutions that break with the challenges of the past. AI SIEM offers a high-performance and user-friendly platform that helps security teams of all sizes to perform with speed, effectiveness, and maturity. Built as an extension of the Singularity platform, AI SIEM is particularly simple and straightforward to implement and use for existing SentinelOne customers.

Let's examine and debunk some common SIEM myths, and explore how AI SIEM provides an easy-to-use, AI-driven solution that maximizes productivity and security outcomes.

MYTH 1

Implementing SIEM is a Complex and Expensive Undertaking, Suitable Only for Large Enterprises

FACT

A modern, autonomous SIEM can start transforming your security operations in days, not months.

In the early days of SIEM, the products available on the market were more frameworks than solutions. The products worked well enough for addressing relatively simple compliance needs, but strained when they were scaled up to address more complex security operations use cases. Organizations were forced to perform complicated capacity planning exercises, develop custom parsing logic for many data sources, and deploy a complex array of physical appliances designed to collect, parse, analyze, and store massive streams of security data. To this day, many security leaders believe that SIEM solutions are too complex and expensive to design and deploy for all but the largest and most mature security teams.

Modern solutions like AI SIEM are designed to fit businesses of all sizes, dramatically simplifying implementation and ongoing management. AI SIEM is a seamless extension of the SentinelOne Singularity Platform, which is proven to power security operations with speed, scale, and simplicity for tens of millions of endpoints globally. AI SIEM dramatically streamlines implementation by delivering:

- **Cloud-Native Platform**
Cloud delivery provides organizations with effortless deployment and makes it easy to start small and scale up over time.
- **Seamless Extension of the Singularity Platform**
Existing SentinelOne customers benefit from a SIEM with familiar architecture, console, and agent, making implementation a snap.
- **Unified SIEM and EDR**
EDR is one of the richest and most useful sources of telemetry for today's security analysts. Unifying deep EDR telemetry with 3rd party SIEM data sources unlocks new and more sophisticated detection capabilities, while simplifying deployment and reducing total cost of ownership.
- **Plug-and-Play Connectivity**
AI SIEM leverages the existing SentinelOne agent for collecting Windows event logs, and provides an extensive array of options to connect with other 3rd party data sources. All data connectors are Open Cybersecurity Schema Framework-ready (OCSF), automatically normalizing data to make it simple to work with.
- **10GB/day of Data Ingestion at no Cost**
SentinelOne provides an entry-level ingestion capacity to get started, allowing existing SentinelOne customers to try AI SIEM today without any additional financial commitment.

These capabilities make AI SIEM accessible to businesses of any size, and particularly well suited for existing SentinelOne customers looking to implement a new SIEM or migrate from a SIEM that's not delivering the expected value.

MYTH 2

The More Data You Can Get into Your SIEM, the Better Results You'll Get

FACT

A little of the right data is a lot better than a lot of irrelevant data.

Perhaps no statement has created more SIEM chaos and inefficiency than: "It's a security log? Get it in the SIEM!" Many assume that dumping every possible log into your SIEM will lead to golden nuggets of security wisdom popping out the other side, but this approach more often yields piles of coal. Ingesting irrelevant or excessive data not only drives up costs to maintain and operate a SIEM, but also makes it harder for your security team to focus on real threats. Too much noise can obscure meaningful security insights, contributing to alert fatigue and poor decision-making.

SentinelOne's approach to SIEM is rooted in XDR principles, with a focus on bringing in relevant data that supports important security use cases and compliance requirements. Filtering out unneeded logs allows security teams to focus on actionable insights without overwhelming their infrastructure or their analysts. Key principles include:

- **Targeted Data Ingestion**
Align your SIEM data with specific security goals, bringing in only what's necessary.
- **Scale Use Cases as Your Team Matures**
As your use cases expand, so too can the amount of data ingested, but always in a controlled, meaningful manner.

SentinelOne makes it easy to start simply, and expand data ingestion over time, supporting the growing needs of your organization. This approach ensures that your SIEM delivers the highest possible value while keeping performance at optimal levels.

MYTH 3

SIEM Storage is Expensive, Complicated, and Slow

FACT

Modern cloud-native data lakes eliminate legacy expense and complexity.

The cost of storing and managing massive volumes of data has long been a pain point for organizations using legacy SIEM systems. Legacy SIEMs are built on enormous storage arrays, often with multiple tiers that provide varying levels of storage cost and performance. Data architects working under this model are forced to make painful tradeoffs: pay high costs to keep security data accessible in hot storage, or offload data to cheaper cold storage, but endure sluggish query speeds.

Thankfully, modern storage architectures are eliminating this source of pain. According to IDC's Worldwide Security Information and Event Management Forecast 2023–2027, “the traditional use of SIEM for log storage is quickly being replaced by security-specific data lakes that offer more efficient performance.”

SentinelOne's Singularity Data Lake (SDL) eliminates these storage concerns, offering infinite scalability and cost predictability by moving away from antiquated and expensive tiered storage towards a cloud-native data lake. AI SIEM is built on top of the Singularity Data Lake, allowing it to deliver:

- **Always-Hot Storage**
SDL eliminates cold storage delays while ensuring that data is always accessible and performant.
- **High-Performance at Scale**
SDL leverages a massively parallel query engine, delivering up to 100x faster performance than legacy systems.
- **Cost Efficiency**
SDL provides reasonable and predictable costs, removing the uncertainty and complexity traditionally associated with SIEM storage.

This results in a system that can handle structured and unstructured data at massive scale, providing 80% faster threat hunting and near-instantaneous query performance, all while reducing long-term storage expenses.

MYTH 4

Operationalizing a SIEM Requires a Full-time Team of Data Scientists and Detection Engineers

FACT

Modern SIEMs are turnkey solutions that come with expert insights and AI-powered analytics built-in.

One of the most important use cases for a SIEM is threat detection. SIEMs analyze signals across multiple security data streams to uncover and alert on attack activity that might not be clear looking at the data streams in isolation. Unfortunately, few SIEMs provided the continuous threat intelligence, streaming analytics, and detection logic needed to stay on top of rapidly evolving threats, leaving security teams on their own to develop and maintain effective threat detection within the SIEM framework.

AI SIEM provides up to date adversary context and detection by infusing the latest in global threat intelligence from Mandiant. Security teams, regardless of size or experience, can leverage out-of-the-box workflows and AI-driven threat detection without the need for specialized knowledge. AI SIEM delivers:

- **Built-in Detections and Dashboards**
Expert insights are continuously updated to detect emerging threats and guide organizations through detection and response workflows, allowing users to see immediate value.
- **Standards-Based Data Model**
All data is automatically normalized to the OCSF standard, providing a universal data model that makes complex security data from a variety of sources easy to understand.
- **Near Real-Time AI Analytics**
Enables rapid, autonomous threat detection without human intervention.

By embedding the most sophisticated detections and AI-powered contextual suggestions, SentinelOne empowers even lean teams to effectively operationalize their SIEM, achieving world-class threat detection without hiring additional personnel.

MYTH 5

It Takes a Team of Analysts with Decades of Experience to Get the Most From Your SIEM

FACT

AI and good UX improve effectiveness and efficiency dramatically.

The complexity of legacy SIEM systems made it difficult for less experienced analysts to fully leverage their capabilities. It puts a heavy burden on the analyst to know the right questions to ask in order to triage and understand an incoming threat. It required analysts to learn complex query languages in order to find answers to those questions. Finally, it left the analyst to come to their own conclusions about the optimal response to an emerging threat. Few organizations are able to hire and retain the kind of staff needed to execute these workflows in a consistent manner.

Generative AI is transforming the way security teams operate. IDC's Worldwide SIEM Forecast 2023–2027 report projects that “generative AI assistants will become a feature of the SIEM to improve security analyst efficiency.” AI SIEM, powered by **Purple AI**, makes this vision a reality, continuously learning and adapting to new threats, and coaching analysts on the optimal response.

- **AI Coaching**

Purple AI helps even less experienced analysts perform threat hunts and investigations, with reports showing a 128% increase in threat hunting efficiency and 80% faster investigations.

- **Hyperautomation**

No-code, API-based workflows allow teams to build and implement tailored responses quickly.

These features ensure consistent and effective responses across the team, regardless of experience level.

SentinelOne Customers Can Try AI SIEM Today

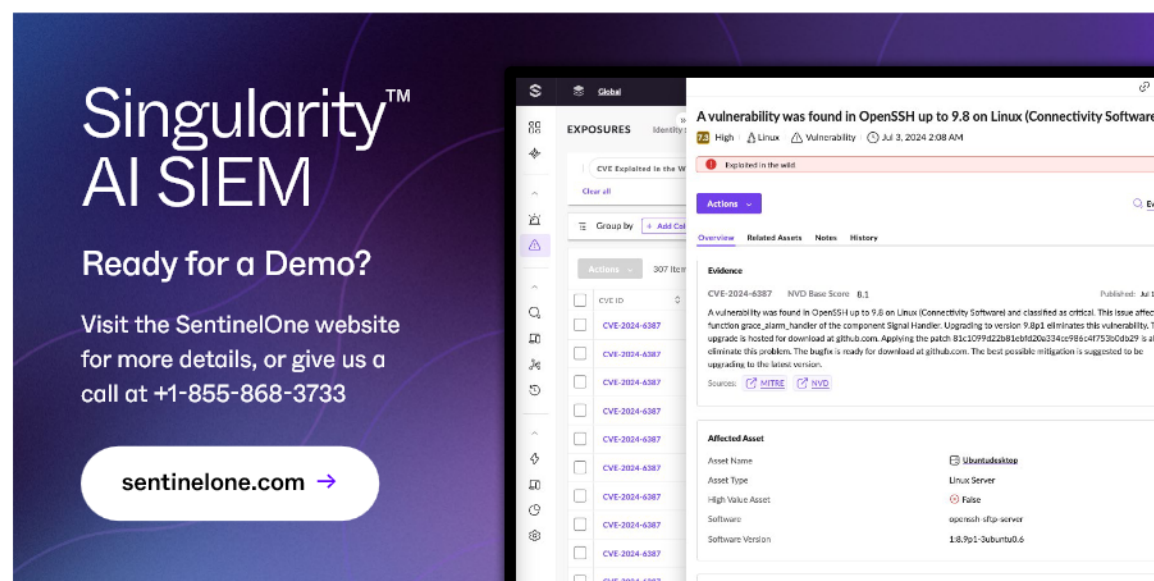
The myths surrounding SIEM adoption, implementation, and operationalization have kept many organizations from experiencing the full benefits of modern security operations. Singularity AI SIEM shatters these misconceptions, providing a unified, scalable, and AI-driven platform that empowers businesses of all sizes to enhance their security posture.

Curious about how AI SIEM will work for you? SentinelOne customers can take advantage of 10GB/day of data ingestion at no additional cost to see the power of AI SIEM first hand. Common initial use cases include:

- **Consolidate Windows event logs** to simplify compliance reporting.
- **Offload data from Splunk** to reduce costs and improve performance.
- **Integrate authentication and EDR data** for improved forensic investigations.

Organizations of all types are using AI SIEM to address these concerns and many more head-on, boosting the efficiency and effectiveness of their security teams.

Learn more: <https://www.sentinelone.com/platform/ai-siem/>



Innovative. Trusted. Recognized.



A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms



Record Breaking ATT&CK Evaluation
+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays



96% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity





Contact Us

techpartners@sentinelone.com

+1-855-868-3733

sentinelone.com

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

24_MKTG_Product_WhitePaper_010_SIEM_Myths_WP_r2_12052024

© SentinelOne 2024