HUNTERS

SIEM BUYER'S GUIDE

For Small SOC Teams

Small SOC teams know the struggle:

Too many alerts, not enough time, and an endless parade of "silver bullet" promises. Every tool claims to revolutionize your SOC, promising better detection, fewer false positives, and that elusive goal: making security operations simple. But let's be real — if security operations were simple, you wouldn't feel like you're fighting fires all the time. You're not here for buzzwords or hype. You already know your SOC faces challenges like alert fatigue, fragmented insights, and a never-ending resource crunch. You also know that the wrong Security Information and Event Management (SIEM) can make those problems worse, not better.

These are the real questions that SOC managers and analysts need answered. And that's exactly why we created this guide. Whether you're exploring your first SIEM or replacing an outdated one, this guide cuts through the noise. ***It's designed to help small, resource-constrained SOC teams like yours make informed decisions, avoid common pitfalls, and find a solution that empowers your analysts to do more with less.***

Because when your SIEM works for you — not against you — you can move beyond survival mode and focus on what matters most: keeping your organization secure.

But how do you find the right one?

How do you choose a SIEM that fits your team's size, workflows, and budget?

Which features are *actually* useful for smaller teams managing a mountain of alerts?

MOST IMPORTANT

How can you ensure your new SIEM delivers real value — without just adding complexity to an already overburdened team?

TABLE OF CONTENTS

INTRODUCTION TO SIEM

A brief history of SIEM & its significance within an organization.

Cyber threats aren't going away, and no organization — big or small — is immune. Protecting your users and digital infrastructure has never been more critical, and that's where SIEM solutions step in. A good SIEM acts as the command hub of your Security Operations Center (SOC), helping you monitor, detect, and respond to threats across your environment.

But here's the catch: not all SIEMs are created equal. Finding the right fit means understanding how a solution aligns with your team's size, resources, and unique security challenges.

WHAT IS SIEM

Back in 2005, Gartner analysts Mark Nicolett and Amrit Williams coined the term "SIEM" to describe a *unified approach to security operations activities*. The concept grew out of two earlier approaches to security operations:

- **Security Information Management (SIM):** Focuses on collecting, analyzing, and reporting on data.
- **Security Event Management (SEM):** Monitors events to identify security threats.

WHY DID IT EMERGE?

Because security teams needed a better way to stay ahead of increasingly sophisticated threats. Essentially, SIEM technology was the response to a growing need for centralized security monitoring and incident management.

By pulling security data from every corner of an organization — endpoints, servers, networks, and applications — SIEM solutions provide a single pane of glass (collecting, analyzing, and correlating) for faster investigation and response.

THE EVOLUTION OF SIEM

SIEM technology has come a long way. What started as basic log management has evolved to meet the demands of today's complex environments. SIEM solutions have shifted from SQL-based data management to NoSQL, embraced big data, and adapted to the rise of cloud environments and data lakes.

Modern SIEMs are collections of finely tuned content — connectors, parsers, correlation rules, dashboards, and reports — all tailored to specific data stacks. This evolution has kept SIEMs relevant in an era where security teams face more data, more threats, and more complexity than ever before.

Throughout this evolution, SIEM has gone through several generations, continuously adapting to emerging threats, advancing technologies, and the ever-changing needs of modern businesses:

First-Generation SIEM (Early 2000s)

Focused primarily on log management and basic correlation, early SIEMs were built on SQL databases. While enabling centralized searching, these systems had limited scalability and struggled with real-time analysis, making them hard to scale and less effective in dynamic environments.

Second Generation (Late 2000s)

The second generation's introduction of more sophisticated data architectures allowed for better handling of high-volume data streams, enabling real-time analysis and correlation capabilities. These improvements significantly enhanced the ability of SIEMs to detect threats, but their primary value was in aggregating and normalizing common security monitoring data from technologies.

Third Generation (Early 2010s)

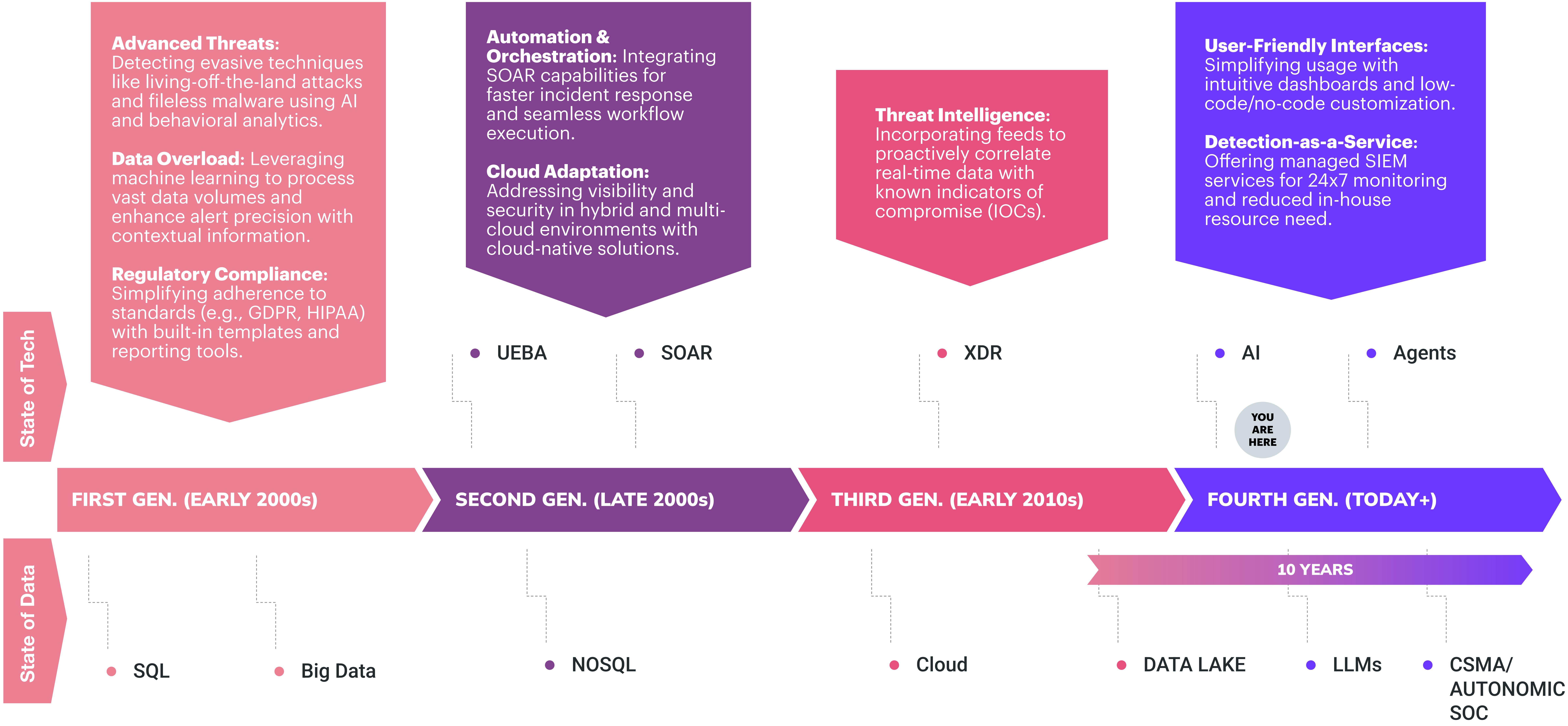
The third generation of SIEM embraced big data and NoSQL technologies, which allowed for greater scalability and more sophisticated analytics. Primitive machine learning and other analytics began to be incorporated into SIEM platforms, theoretically enhancing their ability to detect anomalies and evolving threats automatically. But compliance became the primary budget driver, leading to a stagnation of threat detection capabilities in favor of greater data acquisition scope and reporting frameworks.

WE ARE HERE!

Fourth Generation (Current)

Today's Next-Gen SIEM solutions are cloud-native, leveraging advanced analytics, artificial intelligence (AI), and security data lakes to provide more comprehensive and scalable security management. These modern SIEMs are designed to work in increasingly complex and hybrid IT environments, offering features like predictive security, autonomous threat response, and seamless integration with other security tools.

Key Drivers of Innovation in SIEM



State of Tech

State of Data

FIRST GEN. (EARLY 2000s)

Advanced Threats: Detecting evasive techniques like living-off-the-land attacks and fileless malware using AI and behavioral analytics.

Data Overload: Leveraging machine learning to process vast data volumes and enhance alert precision with contextual information.

Regulatory Compliance: Simplifying adherence to standards (e.g., GDPR, HIPAA) with built-in templates and reporting tools.

- SQL
- Big Data

SECOND GEN. (LATE 2000s)

Automation & Orchestration: Integrating SOAR capabilities for faster incident response and seamless workflow execution.

Cloud Adaptation: Addressing visibility and security in hybrid and multi-cloud environments with cloud-native solutions.

- UEBA
- SOAR
- NOSQL

THIRD GEN. (EARLY 2010s)

Threat Intelligence: Incorporating feeds to proactively correlate real-time data with known indicators of compromise (IOCs).

- XDR
- Cloud

FOURTH GEN. (TODAY+)

User-Friendly Interfaces: Simplifying usage with intuitive dashboards and low-code/no-code customization.

Detection-as-a-Service: Offering managed SIEM services for 24x7 monitoring and reduced in-house resource need.

- AI
- Agents

YOU ARE HERE

10 YEARS

- DATA LAKE
- LLMs
- CSMA/ AUTONOMIC SOC

WHY SIEM MATTERS

The role SIEM plays at the core of security operations.

The Role Of SIEM In Modern Cybersecurity

Cyberattacks aren't just more frequent — they're smarter, stealthier, and more damaging than ever before. As the threat landscape continues to evolve, SIEM has become a cornerstone of modern cybersecurity strategies. It plays a crucial role in helping organizations:

- **Detect Threats Early**

  By analyzing log data and correlating events across systems in real time, SIEM solutions help identify potential threats before they escalate. This early warning system is critical for staying ahead of increasingly sophisticated attacks.

- **Respond Quickly and Effectively**

  SIEM solutions provide valuable context around security incidents, enabling security teams to prioritize and respond to threats faster and more effectively. Integrated with technologies such as Security Orchestration, Automation, and Response (SOAR) and increasingly with native autonomic capabilities, SIEMs can even initiate automated responses to certain types of incidents, interrupting the attacker kill-chain and reducing the time it takes to mitigate threats.

- **Meet Regulatory Requirements**

  More industries are subject to strict regulatory requirements for data protection and security. SIEM solutions help organizations meet compliance standards by providing detailed reporting and audit trails.

- **Full Visibility Across the Entire Attack Surface**

  With the growing complexity of digital infrastructures that include cloud, on-premises, and mobile users, SIEM offers organizations a centralized view of their attack surface and security posture. This improved visibility allows for better threat detection, more efficient and cost-effective investigations, and a stronger overall security strategy.

From Reactive To Proactive Security

SIEM has come a long way from its humble beginnings in log management. Early systems were reactive by design — alerting teams only after something bad had already happened. Helpful? Sure. But game-changing? Not so much.

Fast forward to today, modern SIEM solutions are far more proactive thanks to advances in AI and machine learning. *Today's technology doesn't just wait for something to go wrong; it hunts down anomalies and sniffs out threats before they become full-blown incidents.*

Now, let's talk about the elephant in the SOC: the 24/7, always-on operations model. Once upon a time, this was hailed as the ultimate security strategy. But in practice? It's a budget-draining grind. The goal isn't just to keep watch — it's to work smarter, not harder. Reactive processes, endless alert investigations, and false positives galore? That's yesterday's news.

The real shift lies in letting automation handle the noisy stuff — triaging alerts, spotting patterns, and even initiating responses — while SOC analysts focus on the big-picture strategy. This isn't about replacing people; it's about empowering analysts with the equivalent of unlimited time and knowledge, giving them the support they need to focus on what matters most.

For smaller teams or resource-strapped businesses, proactivity doesn't mean gluing human eyes to dashboards 24/7. It means leveraging tools that provide early warnings, actionable insights, and (dare we say it) peace of mind.

Even if you're outsourcing to a Managed Detection and Response (MDR) provider, automation remains crucial. It ensures remote teams can do their job effectively and deliver consistent results — or higher levels of service. But here's the kicker: even the best MDR, or external provider, can't outperform the quality of the tools available to them. *At the end of the day, the tech stack is the foundation of both proactive and reactive success.*

Tackling Core Security Challenges

Time is the ultimate currency in cybersecurity. The faster your team can detect and respond to threats, the better your chances of stopping attackers in their tracks. But here's the problem: *security data is scattered everywhere — endpoints, network devices, cloud services, and beyond. Connecting the dots? Nearly impossible without the right tools.*

That's where SIEM solutions come in. By pulling all that disparate data into one centralized platform, a SIEM gives your team a complete picture of your environment. Suddenly, those random events that seemed harmless on their own start forming a pattern — a pattern that might just reveal a compromise in progress.

For small SOC teams, or teams with limited resources, modern SIEMs are more than just tools — they're lifelines. Automation and pre-built analytics act as force multipliers, doing the heavy lifting so your analysts can focus on what they do best. The right SIEM doesn't just sound the alarm; it hands your team the insights, automation, and functionality they need to investigate and respond with speed and precision.

Looking ahead, SIEM platforms aren't slowing down. They're doubling down on AI and automation to stay ahead of evolving threats. *Organizations that invest in modern SIEM solutions are future-proofing their operations, ensuring they can protect their data, systems, and reputation in a world that's only getting more complex.*

HOW TO EVALUATE SIEM SOLUTIONS

Key criteria to look for and mistakes to avoid.

Key Features To Look For

When evaluating SIEM solutions, picking the right one is about more than just checking boxes. It's essential to focus on features that meet both your current security needs and scale with your future growth. Here's what to keep an eye out for, the most critical elements:

Continuously Tuned Detections and Automation

One of the biggest advantages of a modern SIEM is the inclusion of pre-tuned detection rules that cover a wide range of attack vectors. Out-of-the-box detection rules are designed to catch common threats and correlate events across various security domains such as endpoints, cloud environments, networks, and identity systems. Look for SIEM solutions that provide investigation capabilities that automate scoring & prioritization, correlation, and enrichment for you. Additionally, evaluate SIEMs that include automation features like SOAR to reduce manual intervention and accelerate threat response times.

High-Fidelity Correlation Rules

Here's the thing: every SIEM promises correlation, but not all of them deliver. Reminder: aggregation is NOT correlation. High-fidelity rules help reduce false positives, ensuring that your security team spends less time chasing down benign alerts and more time focusing on real threats. The key is to find a SIEM that delivers detection content optimized for your environment and continuously adapts to evolving threats.

Search Capabilities That Are Easy to Use

Security Analysts need to search through large volumes of data across their IT infrastructure to investigate threats using specific keywords and search queries. Look for a SIEM that supports fast log searches within a UI that is simple and easy to use.

'AI-Native' Not 'Bolt-On AI'

An AI-Driven SIEM is better suited towards a small SOC team than a legacy SIEM retrofitted with AI features because it's built from the ground up with automation, advanced analytics, and efficiency in mind. Legacy SIEMs that attempt to bolt on AI capabilities often struggle with data silos, inefficient workflows, and outdated architecture that was never designed to handle modern security challenges. Unlike a legacy system playing catch-up, an AI-Driven SIEM continuously evolves with machine learning-driven insights, providing faster, more accurate detection and automatic investigation — all without requiring additional engineering or security expertise to maintain effectiveness.

Scalability Without Complexity

Growth shouldn't mean more headaches. The ability to scale security operations without adding complexity is crucial for organizations. A modern SIEM should allow you to ingest security telemetry from terabytes to petabytes of data without performance degradation.

A SIEM shouldn't just meet your needs today; it should set you up for success tomorrow.

Time To Value

LOOK FOR THIS

- ✓ **Streamlined, self-serve deployment & configuration**. A SIEM that doesn't require extensive onboarding, training, or professional services.
- ✓ **Performs playbook-less automation** to investigate and troubleshoot alerts.
- ✓ **Sensible, high-fidelity correlation capabilities - Out-of-the-Box (OOTB)**. Continuously tested and easy to tune.
- ✓ **Managed tuning services** to reduce manual labor required to refine correlation rules.
- ✓ **Always-on detection content**, OOTB and mapped to common security frameworks.

NOT THIS

- ☒ **Lengthy & complex setup**. Steer clear of SIEMs that require manual configurations, prolonged implementation cycles, and hidden dependencies on expert services or learning curves.
- ☒ **Limited detection content out-of-the-box** and tuning which isn't aligned to the skillset you have in house (e.g. too complex).
- ☒ **Includes a high number of professional services or requires specialized engineers** for deployment.
- ☒ **Narrow detection focus** with uneven coverage across your anticipated attack surface.

Learning Curve

LOOK FOR THIS

- ✓ **Adopts a robust universal language (SQL)** that is applicable across technologies, allowing direct transferability of queries and detections.
- ✓ **AI capabilities for simplification and explainability,** augmenting and supporting existing team.
- ✓ **Starts with answers, not questions.** Look for a SIEM that provides context rich alerts, with a high degree of explainability, rather than one that starts and ends with search. (Search adds value to an investigation, not a requirement to triage.)
- ✓ **Open data lake architecture,** neutral query language for search & detection, and OCSF for normalization framework - all of which are non-vendor proprietary and anti vendor lock-in.
- ✓ **Simple and user-friendly UI** with little to no learning curve from starter to power users.

NOT THIS

- ☒ **Use vendor specific query language** for search and detection.
- ☒ **Cater to large and mature security programs** with complicated use cases and specialized teams.
- ☒ **No AI functionality,** or existing functionality is very limited.
- ☒ **Require deployment and management by large, dedicated & specialized teams** of analysts and engineers.
- ☒ **Require professional services** to get up and running (and likely have steep learning curves).

Best-Of-Breed VS Portfolio

LOOK FOR THIS

- ✓ **Specialized exclusively in security incident and event management** that provides a best-of-breed solution and is purpose-built to address those specific needs.
- ✓ **Cutting-edge technology** and innovative software that will help you stay ahead of emerging threats and vulnerabilities.
- ✓ **Freedom from vendor lock-in,** able to operate without additional worry regarding the vendor.

NOT THIS

- ✕ **Solutions that shoehorn you into a consolidated portfolio** of mixed quality products, like endpoint, cloud, and network.
- ✕ **Deny you the freedom to choose** the most effective tools for your specific security requirements to tailor your approach to cybersecurity.
- ✕ **Spend more effort locking you into the ecosystem** rather than enabling interoperability, to prevent you from potentially switching to other solutions in the future.

Scalability

LOOK FOR THIS

- ✓ **Cloud-based solution vs. on-prem solution.** Can easily scale from gigabytes to hundreds of terabytes without degrading performance or availability.
- ✓ **Allows you to bring your own data lake** and has built-in data parsing for all supported integrations in every format.
- ✓ **Offers integrations that are mapped, parsed, and normalized** (ideally in a standard that is accepted across the industry - OCSF). Data source onboarding that doesn't require future editing of parsers, schemas, etc.

NOT THIS

- ✕ **Have limitations, or struggle to scale** as the volume of data increases, causing concerns about performance or availability.
- ✕ **Experience operational problems** like datasource delays, parse issues, or ingesters going down.
- ✕ **Don't provide access to specialized resources** that can quickly troubleshoot ingestion or datasource onboarding issues.
- ✕ Don't provide access directly to the data lake and the ingested raw data.

Threat Hunting

LOOK FOR THIS

- ✓ **Automatic investigation capabilities.** Get enhanced score and correlated alerts to help focus on what matters most.
- ✓ **Fast access to cybersecurity experts** that provide analysis of critical threats detected in your network.
- ✓ **Proactive hunting for globally emerging threats.**
- ✓ **Detailed reporting when a threat is found** with more than just recommendations for remediation. Look for a SIEM that provides details about what was found, the investigation steps that were taken, and what steps need to be taken next.

NOT THIS

- ☒ **Don't provide in-house expert services** that are highly skilled in incident investigation, proactive threat hunting, and security posture & hygiene reporting.
- ☒ **Offer a "one-size-fits-all"** reporting that will likely result in "one-size-fits-none."
- ☒ **Provides reporting that only includes recommendations for remediations** rather than including all the relevant information and details.

Pricing

LOOK FOR THIS

- ✓ **Pricing that's predictable, clear, and simple** to understand, without hidden costs or fees.
- ✓ **Transparent answers** on how many in-house analysts will be required to run the SOC.
- ✓ **Affordable access to cybersecurity experts** that provide rapid response, proactive threat hunting, and security posture reporting.

NOT THIS

- ☒ **Pricing models that are complicated** to understand, or full of "add-ons" for capabilities that should be included.
- ☒ **Consumption-based pricing models** that cause painful trade-offs due to high cost of data ingestion and retention.
- ☒ **Licensing models that don't align with your organization's needs.**

MAKING THE RIGHT CHOICE

How to align features and functionality to desired outcomes.

DON'T FALL FOR THE SHINY TOY SYNDROME

Let's be honest: it's easy to get distracted by flashy features and buzzword-filled promises. *But the true value of a SIEM doesn't come from its trendiest capabilities - it comes from how well it supports your business outcomes.* Compliance, operational efficiency, risk reduction - these are the results that actually matter.

The right SIEM won't just look good on paper. It will fit seamlessly into your workflows, deliver measurable ROI, and help your team defend the business while enabling strategic success. So skip the shiny toy syndrome and focus on solutions that work for you, not just ones that sound good in a sales pitch.

ALIGN SIEM CRITERIA TO ORGANIZATIONAL GOALS

Choosing a SIEM is about finding a solution that drives real results - balances the right features you need today, futures to come, and addresses your pricing requirements. *To ensure it delivers value, your SIEM should align with both your security goals and broader business objectives.* Here's what to aim for:

- **Early Threat Detection**

  Modern SIEMs are like a security early warning system. Using advanced analytics, AI, and correlation rules, they spot threats in real time, shrinking your window of exposure. The goal? Catch and mitigate incidents before they become full-blown escalations.

- **Efficient Incident Response**

  Data without context is just noise. A SIEM should centralize and contextualize your data, helping teams respond faster and smarter. With SOAR integrations, workflows are automated, saving valuable time and keeping your team focused on what matters.

- **Enhanced Threat Visibility**

  Blind spots are the enemy of effective security. A robust SIEM delivers centralized monitoring across on-premises, cloud, and hybrid environments, ensuring threats are visible no matter where they lurk.

- **Regulatory Compliance Without the Hassle**

  Compliance doesn't have to be a headache. Built-in reporting and data retention features help you meet standards like GDPR, HIPAA, and PCI-DSS, keeping your organization audit-ready while minimizing the risk of fines.

DRIVE BUSINESS OUTCOMES

A SIEM doesn't just strengthen your defenses; it powers your business. When implemented effectively, it drives outcomes that go beyond security, making your organization more efficient, cost-effective, and resilient. Here's how:

- **Operational Efficiency**

  Automating tedious tasks like log collection, normalization, and incident correlation frees your security team to focus on the bigger picture — think threat hunting and strategic planning instead of drowning in alerts.

- **Cost Optimization**

  SIEMs don't just save money by preventing costly breaches; they also consolidate tools and streamline operations. Modern solutions, especially cloud-based ones, offer predictable pricing that keeps your budget under control.

- **Risk Reduction**

  Breaches are bad for business — full stop. A well-tuned SIEM minimizes both the likelihood and impact of attacks, protecting sensitive data, maintaining customer trust, and ensuring your business keeps running smoothly.

- **Strategic Decision Support**

  Your SIEM isn't just a security tool; it's a strategic advisor. By delivering clear, actionable insights into your organization's security posture, it empowers executives to make smarter decisions about risk management and technology investments.

When your SIEM does its job, it doesn't just protect the business — it helps it thrive.

MAPPING FEATURES TO OUTCOMES

To ensure your SIEM investment achieves these goals and delivers outcomes, here's how features can directly contribute to that success:

OUTCOME	SIEM FEATURE(S)
Early Threat Detection	Real-time monitoring, user and entity behavior analytics (UEBA), machine learning-based anomaly detection.
Efficient Incident Response	Context enrichment, threat intelligence integration, SOAR, and remote response and automation capabilities.
Enhanced Threat Visibility	Multi-environment log aggregation, customizable dashboards, and advanced correlation rules.
Regulatory Compliance	Preconfigured compliance reporting templates, log retention policies, and audit trail management.
Operational Efficiency	Automated data ingestion and normalization, self-service onboarding, and low-code customization.
Cost Optimization	Flexible licensing, scalable cloud-based architectures, and efficient data processing (e.g., deduplication).
Risk Reduction	High-fidelity alerts, predictive analytics, and integrated playbooks for common attack scenarios.
Strategic Decision Support	Executive-level reports, security KPI tracking, and integrations with business intelligence tools.

FINAL THOUGHTS

Choosing the right SIEM isn't just another item on your to-do list — it's a decision that can shape the future of your security operations and, ultimately, your organization's resilience. For small SOC teams, the stakes are even higher. With limited resources and an ever-growing threat landscape, having strong, reliable technology at the core of your operations is critical.

A well-chosen SIEM solution can act as the backbone of your SOC, empowering your team to detect threats faster, respond more effectively, and scale with confidence. While price, and "shiny-features" may be tempting, they shouldn't outweigh functionality. A budget-friendly SIEM that lacks the features your team needs today will ultimately cost more in wasted time, missed threats, and burnout. Prioritize solutions that deliver measurable value — through automation, scalability, and seamless integration into your existing workflows. The goal is a SIEM that enhances your team's efficiency, reduces risk, and adapts as your organization grows.

As you evaluate your options, keep one thing at the forefront: your SIEM should work for you, not the other way around.

ABOUT HUNTERS

Hunters Next-Gen SIEM helps small security teams be more effective and efficient by automating the entire threat detection, investigation, and response process. Hunters deploys in days and eliminates repetitive work with out-of-the-box integrations and detection rules. High priority alerts are surfaced based on risk and confidence scoring, and similar alerts are clustered together, reducing alert triage by 80%. Customers can build an open, scalable data lake at a predictable cost, and bring their own data lake or leverage Hunters'. Team Axon provides rapid response to emerging threats, incident investigation, proactive threat hunting, and security posture and hygiene reporting.

Hunters was recognized as a Leader in the 2024 GigaOm Radar for SIEM and received an Honorable Mention in the 2024 Gartner Magic Quadrant for SIEM. Learn how companies like Booking.com, Snowflake, TheRealReal and Cimpress are leveraging Hunters to empower their security teams at *https://www.hunters.security.*

Hunters is backed by leading VCs and strategic investors including Stripes, YL Ventures, DTCP, Cisco Investments, Bessemer Venture Partners, U.S. Venture Partners (USVP), Microsoft's venture fund M12, Blumberg Capital, Snowflake Ventures, Databricks, and Okta.