elastic | The Search AI Company

2025 SIEM Buyer's Guide

Key considerations when selecting your next SIEM

Propel detection, investigation, and response by modernizing security operations

Enterprise transformation is being driven by trends like the rise of AI, the growth of cloud services, and the need for data-driven decision-making. These dynamics are eroding traditional defenses and deepening the cyber skills gap.

How should your SOC adapt?

elastic.co

Modern SIEM is more important than ever

Your security operations team serves the central role in achieving your mission. Empower them to excel with modern SIEM capabilities that enhance their effectiveness:

Flexible deployment: Stay agile with a SIEM that scales easily and supports multi-cloud, hybrid, and on-premises architectures.

Full visibility: Gain a unified view across your entire attack surface, with a SIEM that eliminates blind spots and enables instant analysis of efficiently retained archives.

Advanced analytics: Move beyond traditional methods with cutting-edge analytics that accelerate detection, investigation, and response.

Insights and guidance: Arm analysts with relevant context, AI-driven recommendations, and built-in playbooks to make smarter, faster decisions.

Automation: Automate manual workflows to reduce dwell times and improve team productivity and morale.

Extended protection: Fortify defenses by deploying native endpoint and cloud security technologies or integrating third-party technologies.

Consider your unique needs

Whether you're replacing a SIEM or starting with a clean slate, you're in the right place. To select your next SIEM, weigh your organization's priorities, your team's skills and processes, and the right defenses for your attack surface.

Read on to explore key considerations and our related SIEM guidance.

elastic

Your organization

Ensure that your next SIEM deftly adapts to the needs of your organization.

Key considerations	SIEM guidance
What are your crown jewels — and who wants them?	Does your organization have financial assets that could be swiped? Trade secrets that competitors might fancy? Systems that could be ransomed? PII that could be sold? Critical infrastructure that an adversary could sabotage? Understanding how the threat landscape intersects with your organization's areas of exposure — and appetite for risk — is vital for establishing priorities. Consider your risk matrix and how your overall strategy should guide your SIEM investment
Is your SOC an accelerator or a blocker?	Security operations teams must support key initiatives while keeping attackers at bay. Achieving both requires the agility of an open and transparent SIEM. Closed security products often lack the integrations to automate workflows and the flexibility to evolve with your business — breaking processes, causing tool bloat, and slowing analysts. To stay nimble, guard against the constraints of: • Not-invented-here syndrome • Limited integrations with modern technologies • Inflexible licensing (e.g., per use case, per byte) • Closed code Unlock innovation with a solution that offers the versatility to expand to new use cases. Ensure that its licensing allows you to adapt as your needs change, scaling up and down and adopting new features. Look for a record of rapid roadmap advancement, a thriving user community, and broad interoperability with the enterprise technologies of tomorrow.
Are you concerned about vendor lock-in?	Vendor lock-in is a recipe for frustration. Choosing a solution with flexible licensing — including a free tier, ideally — helps organizations retain control. Product interoperability is a vital bulwark against vendor lock-in. This is true not just for SIEM, but also adjacent capabilities, like threat intelligence feeds and platforms, AI technologies, and SOAR functions. As such, only select solutions that work well with others. Cloud infrastructure is another path to potential lock-in. SIEM deployment options vary, with limited IaaS vendor options and hit-or-miss support for hybrid and multi-cloud architectures. Ensure that your next SIEM offers options that will meet your evolving digital resiliency and compliance needs.

elastic

Your team and processes

Empower analysts to make a positive impact.

Key considerations	SIEM guidance
Does your SOC attract and retain talent?	70% of organizations face heightened risk due to staffing issues, and experienced practitioners remain scarce, especially in AI/ML and cloud security[1]. Analysts typically change roles every 18 months — and backfilling and ramping them takes 6–12 months[1]. Develop your team's skills — and augment them with AI — to empower practitioners to contribute in new ways. Modern SIEMs surface relevant context, insights, and guidance on an intuitive UI, lowering the new analyst learning curve and helping seasoned personnel achieve more. Expand your recruiting pool by choosing a SIEM with a large and growing user base, and strong product momentum, too. Boost retention by addressing a key cause of analyst burnout: the stress of excessive cognitive load. Equip analysts to make fast, accurate decisions, as detailed in the next row.
How seamlessly can your team address threats?	Organizations need a SIEM that can keep pace with practitioners. Unfortunately, most security teams must still navigate a patchwork of tools and datasets. To connect and streamline disjointed workflows, the SIEM should: • Minimize context switching with a single pane of glass for all relevant data • Enable immediate, unified searching of all data tiers (e.g., hot, cold, frozen), without bulk data rehydration • Guide practitioners with actionable playbooks and AI assistance • Automate mundane and tedious tasks like alert triage • Prioritize investigation and response efforts according to risk • Foster collaboration with case management, RBAC, and workflow connectors for Elastic and third-party security tools
How do you implement standard operating procedures?	Mature SOCs operate with detailed procedures for key processes, like attack containment, evidence collection, and reporting. A SIEM should help teams codify these practices in playbooks and provide a path to incrementally automate them. Operationalizing processes from scratch requires time and expertise, so look for a SIEM that provides expert-written investigation guidance and AI-powered assistance. To facilitate collaboration and centralize associated artifacts (e.g., alerts, data, notes) the solution should also provide a mature case management function.

1. ISACA, 2023

elastic

How do you plan to harness generative AI?	Look for a platform that enables effective and secure use of AI: **Model-agnostic:** Ensure control over cost, speed, accuracy, and privacy by opting for a solution that allows you to choose and switch between multiple leading models and model providers. **Retrieval-augmented generation (RAG):** Choose a SIEM that equips public large language models (LLMs) to perform as if trained for your team using RAG, which instantly and securely enriches user prompts with relevant context gathered from private stores (e.g., alerts, asset criticality, user risk score). **Comprehensive visibility:** Access to context from across your attack surface improves the accuracy of LLM-generated responses, especially regarding complex, multi-vector attack scenarios. **Scalability:** Verify that generative AI features scale well to meet the demands of the real world, with production-level data volumes and complex queries. **Granular privacy controls:** To prevent accidental release of sensitive data, confirm the ability to anonymize or redact sensitive data by default and as needed, with document- and field-level control.
What are your automation plans?	Legacy products hinder automation with proprietary code, limited APIs, and other barriers to interoperability. Choose a SIEM engineered for automation from the inside out to ensure that it can smoothly connect with the tools in your ecosystem. Look for an API-first strategy, open code, and semi- and fully automated response actions for native and third-party technologies. Such capabilities facilitate data sharing, workflow orchestration, and automated response, bolstering program effectiveness. Many programs should also consider the security orchestration, automation, and response (SOAR) capabilities that the SIEM enables, whether via natively developed, bolt-on, or integrated functions. In our experience, most organizations are best served by a solution that offers both a core set of built-in SOAR capabilities and a deep roster of integrations with third-party SOAR platforms (e.g., Tines, Swimlane, Torq, ServiceNow SecOps, TheHive). Taking this approach allows you to adopt SOAR features as you see fit and then evolve with the system of your choice.
How do practitioners coordinate with other teams?	Investigating and responding to an incident — particularly one impacting the wider business — often entails working with adjacent teams, such as IT and Legal. To streamline collaboration, the SIEM must interface well with incident and task management tools (e.g., Jira, ServiceNow ITSM). To facilitate secure and compliant data sharing, it should provide fine-grained role-based access controls (RBAC) that allow admins to specify which data sources and individual fields different users can access. Additionally, by integrating SIEM with observability tools, security teams can gain insights from infrastructure and application performance, enabling faster root-cause analysis and more effective collaboration with teams like DevOps and IT Operations.

elastic

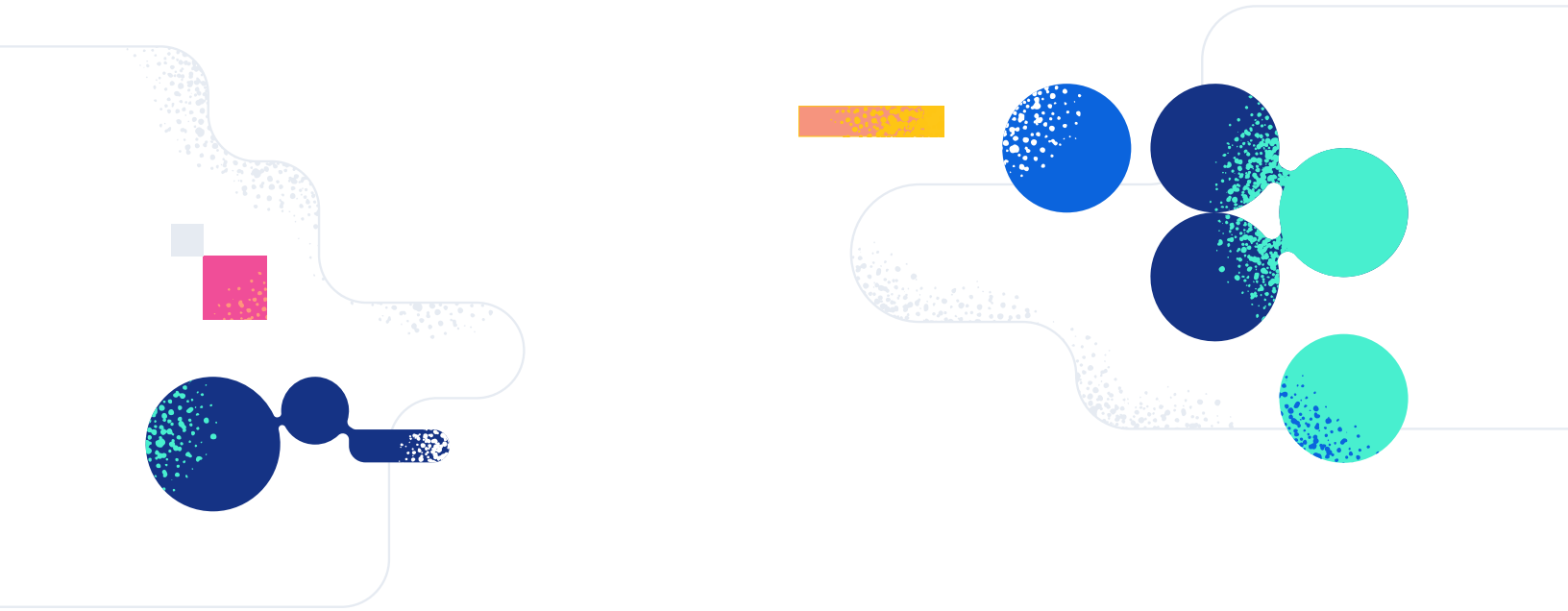
Your attack surface

Gather all of your security-relevant data for holistic analysis.

Key considerations	SIEM guidance
Which data sources matter — now and soon?	Achieving the visibility critical to overcoming today's adversaries is difficult but crucial, necessitating interoperability across vendors and technologies. The conglomerates claiming to be able to provide all necessary visibility via a closed portfolio aren't being realistic. The SIEM must centralize relevant data, whatever its volume, variety, or velocity. It should normalize this data with an open schema (e.g., CEF, ECS, OCSF) and preserve a raw copy for unstructured search and subsequent analysis. Prebuilt integrations simplify onboarding of new data sources. Disregard connector counts and instead assess overlap with your current and prospective tools. Also review the velocity of new integrations and commitment to maintaining existing integrations. For specific technology domains, dig further: • **Cloud infrastructure and applications:** Does the SIEM provide visibility across IaaS and PaaS technologies? Cloud workloads? Containers and orchestration tools? Can analysts access metrics, application traces, and CI/CD logs? • **Host telemetry:** Can analysts access rich host activity and system metrics? Can they perform ad-hoc inspection? • **Network activity and flow:** Does the SIEM enable uniform analysis across disparate network devices, cloud technologies, and hosts? • **User activity and context:** Does the SIEM correlate user data from a wide set of sources and enrich it for swift analysis? Does it identify privileged users, risky users, etc.? • **IoT and OT data:** Does the SIEM support common IoT and OT data formats? • **Third-party context:** Does the SIEM facilitate SecOps, threat intelligence management, vulnerability management, and attack surface management by enriching data with threat intelligence, vulnerabilities, asset data, and other context? Can CTI analysts use the same platform?
How often do you need to onboard new data sources?	No SIEM provides out-of-the-box support for each of the several dozen security technologies deployed in a typical enterprise SOC, so choose a solution that enables custom data sources to be integrated without extensive effort and expertise. Ideally, the solution can create and validate custom data integrations with generative AI, significantly reducing the manual effort required to keep pace with your evolving technology stack. If this process remains largely manual, is documentations strong? Are existing integrations proprietary or open? How readily can you borrow from and collaborate with other community members? Will you need to burn consulting hours for each integration? How long does it take to create and validate a custom data integration? Hours or days — or just minutes with generative AI?

elastic

Are technology or licensing issues limiting how much data you can centralize?	The limitations of legacy SIEMs can impede data collection and analysis, reducing visibility and slowing SecOps workflows. Technological complexity is the first culprit. Solutions that must renormalize data for every query are inherently inefficient. Likewise, legacy SIEMs are notoriously poor at scaling collection and analysis, and data spikes and high-volume sources compound these issues. Inflexible pricing (e.g., per-device, per-user, per-byte) put every customer in the same rigid boxes — regardless of risk profile, executive priorities, or compliance needs — limiting SOC flexibility. Security teams must be able to quickly analyze all of their data, without undue complexity, artificial licensing limits, or other obstacles.
How long do you need to retain actionable data?	As a threat lingers, risk rises — and if they can outlast the logs of their initial attack, sealing off entry points and eliminating footholds becomes a marathon of guesswork. Unfortunately, storage costs bring many organizations to discard data prematurely. Some SIEMs allow customers to reduce storage expenses by moving less frequently accessed data to off-platform archives. The most advanced of these options, Elastic's frozen tier, enables direct and seamless querying of all data. But most SIEMs require bulk data rehydration and can't natively search archives, delaying analysis by hours and raising costs. To bolster security, not just compliance, don't settle for unsearchable archives. The SIEM's data management options must allow the SOC team to: • Correlate logs stored across clouds and geos without the delays and costs of data backhaul • Optimize data retention, performance, and costs to meet the needs of the tiered SOC • Search years of archives in minutes to uncover lurking threats and novel exploits



elastic

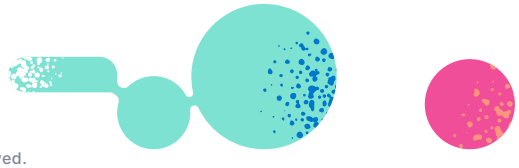
Your defenses

Tackle any conceivable security operations use case.

Key considerations	SIEM guidance
How do you thwart signatureless attacks?	Advanced analytics complement high-fidelity alerting by uncovering unknown threats through signatureless techniques such as entity analysis, machine learning (ML), behavioral analytics, and statistical analysis. These approaches offer key advantages over traditional methods: • Improve detection accuracy by analyzing vast volumes of data to spot malicious activity overlooked by traditional methods. • Mitigate threats by empowering practitioners to take proactive measures to reduce the likelihood and impact of security incidents. • Enhance team efficiency by automating data engineering and threat prioritization so analysts can stay ahead of critical threats. To evaluate the user and entity behavior analytics (UEBA) capabilities of a SIEM, consider the following: • Avoid unplanned costs by confirming that the SIEM doesn't require duplicating data into a separate UEBA store. • Most security teams aren't staffed with data scientists, so the SIEM should provide production-ready ML jobs for common use cases and an intuitive tool for creating custom ML jobs. • For optimal performance, the solution should offer both supervised and unsupervised ML. • Analysts should be able to access insights easily, without constant tab switching. • The solution should present actionable insights that it can readily explain. Also consider data visualization. Beyond the basics, pursue a SIEM that provides intuitive interfaces for exploring data, imbued with relevant insights, guidance, and context. Also look for specialized visualizations — for example, to correlate data, view system commands and processes, and examine cloud posture.
How do you intend to automate threat detection? *(Next page)*	Sophisticated campaigns are increasingly common, and commodity attacks are multiplying, too. Unfortunately, traditional signature-based detection methods tend to miss threats, generate false-positives, and break. A SIEM should ship with a robust library of field-tested detection rules — created and maintained by security experts — to spot adversary tools, tactics, and procedures. These rules help customers efficiently implement and strengthen automated threat detection. Risk-based alert prioritization helps focus analysts on the most concerning threats, lessening alert fatigue (the top challenge for 35% of security teams) and enabling automation.

elastic

How do you intend to automate threat detection?	Though not yet commonplace, generative AI is already beginning to revolutionize alert triage. Look for a solution that can holistically assess a large set of alerts with AI. By analyzing alerts within the context of other suspicious activity — rather than as a series of one-off events — AI-driven alert triage reduces adversary dwell time and related risk. Choose a SIEM that aligns prebuilt detections with the MITRE ATT&CK® framework because automating detection in a strategic manner reduces risk and alert fatigue. The solution should help detection engineers test new rules before implementation and then facilitate automated red teaming. During initial usage and regularly thereafter, someone should be assigned to monitor rule performance and update rule exceptions.
Do you have a threat hunting practice?	Siloed data and slow queries shouldn't impede threat hunters. Choose a SIEM that can quickly drill into all data and pivot on the fly. Initiate hunts with evidence-based hypotheses generated by prebuilt ML jobs. Prebuilt investigation queries, host inspection capabilities, and other features should also support hunters. Further accelerate analysis with contextual threat intelligence and AI-generated insights.
Are prevention, detection, inspection, and response capabilities deployed across all host systems?	A handful of first-party SIEM agents go beyond collecting data, offering endpoint security capabilities, such as: • Secure endpoints against ransomware and malware • Protect cloud-based resources like virtual machines, containers, and serverless workloads from threats • Detect threats with on-host analytics • Inspect systems with osquery • Invoke endpoint-based response actions
What are your compliance requirements?	Adhering to the regulatory and compliance frameworks and standards that apply to your organization will help you avoid needless fines, downtime, and reputational harm. Look for a SIEM that provides data integrations for the compliance-relevant technologies in your environment. The solution should expedite development of custom integrations with an open schema and AI assistance. Compliance reports are literally yesterday's news, so pursue real-time compliance monitoring and a path to proactive enforcement. To support this shift, choose a SIEM that can alert on violations and respond with autonomous or analyst-invoked actions. To inform compliance stakeholders, look for flexible and intuitive visualizations and building tools. If critical systems like point-of-sale terminals or development servers are part of your compliance footprint, consider your needs for file integrity monitoring (FIM), malware detection, and related endpoint security features. Finally, ensure that the SIEM you choose meets your specific security and compliance requirements.



elastic

SIEM success checklist

Each customer will have unique needs and priorities, but consider beginning with these requirements, gleaned from numerous successful SIEM projects.

Data ingestion and normalization

- The solution enables ingestion from all security-relevant data sources, including cloud infrastructure and applications, hosts, network devices, users, IoT and OT, and more.
- The solution offers prebuilt integrations with numerous data sources and regularly releases new integrations.
- The solution normalizes data with an open source schema.
- The solution efficiently retains data in an actionable form to support threat hunting, incident investigation, and compliance across years of archives.

Detection and prevention

- The solution offers diverse automated detection methods and provides a robust set of prebuilt rules.
- The solution spots hidden threats with advanced analytics.
- Prebuilt analytics are open (not a black box) and adaptable to customer environments.
- The solution offers fast real-time and historical analytics.
- Customers can easily customize and create detections to suit specific environments and use cases.
- The solution maps detection techniques to MITRE ATT&CK.
- The solution applies preventative capabilities to eliminate clearly identified threats and minimize analyst workload.

elastic

Investigation, hunting, and response

The solution expedites investigation and response by surfacing relevant insights, guidance, and context.
The solution enables analysts to search data in near-real-time.
The solution enables ad-hoc host and cloud workload inspection .
Analysts can search years of data without major loss of efficiency.
The solution provides case-management to facilitate collaboration, evidence gathering, and record keeping.
The solution enables autonomous and analyst-triggered response actions.
The solution offers core SOAR capabilities and integrates with third-party systems to streamline cross-organizational workflows.

Deployment architecture

The solution supports deployment on-premises, in the cloud, and in hybrid and multi-cloud architectures.
The solution enables security teams to meet data residency requirements while preserving unified visibility.
Fine-grained role-based access controls (RBAC) reduce risk, support compliance, and facilitate cross-org collaboration.
The solution supports multiple tenants (e.g., organizational lines of business, regions) with a single management layer.
The solution offers data management capabilities to support efficient long-term storage of actionable data.

elastic

Build the SOC of tomorrow with Elastic Security

Powered by the Elastic Search AI Platform

AI-driven security analytics is the future of SIEM.

Eliminate blind spots

- Gather data with prebuilt integrations and build custom connectors in minutes with AI.
- Efficiently retain years of instantly searchable archives.
- Analyze data where it lives, without the costs and complexities of backhaul.
- Choose your infrastructure (on-prem., hybrid, multi-cloud, and SaaS) and adapt as your needs evolve.

Strengthen defenses

- Harness research-driven detection rules from Elastic Security Labs.
- Ease SIEM migration by converting detection rules and data queries with AI.
- Solve key use cases with turnkey ML and tackle new use cases with custom ML.
- Equip hunters with user and entity risk scores.
- Extend protection with native and third-party endpoint and cloud security.

Accelerate SecOps workflows

- Holistically analyze alerts and guide analysts with Attack Discovery.
- Elevate analysts with AI assistance and expert-written investigation guides.
- Ground AI in private context, harnessing your choice of LLMs.
- Simplify operations with one platform for security, observability, and search.

elastic