elastic

SIEM Buyer's Guide for the Modern SOC

Key considerations when selecting your SIEM solution

Accelerating digital transformation demands modern security operations

Enterprise transformation is accelerating, as reflected by dynamics like digitization, work-from-anywhere models, and cloud-based services. The impacts for security teams are profound, altering the attack surface, reducing the efficacy of traditional security approaches, and exacerbating the cyber skills gap.

What do these dynamics mean for risk — and how does that change security operations?

What security operations teams need

Your team is the single most important driver in the success of your security program, but technologies like SIEM also play an essential role. Achieving success requires overcoming the limitations of previous solutions by:

Expanding visibility: Organizations need visibility across their holistic attack surface. Only open, vendor-agnostic approaches scale successfully and reduce the swivel-chair phenomenon experienced by analysts. The answer is a security operations platform that supports any technology in your environment.

Detecting in depth: Overcome the limitations of traditional solutions by applying diverse analytical models (e.g., machine learning, behavioral, statistical) against rich data to detect and respond rapidly.

Slowing attackers: 89% of companies have been damaged before responding to a detected attack, according to a recent ESG report. Why? Because triaging an event, building an investigation, and forcefully responding remain highly human-centric workflows. Intelligently automating these processes can slow attackers while expediting analysis.

Building for scale: Data isn't slowing down, and there aren't enough analysts to shrink the skills gap. Any solution must therefore address both trends. Simplifying the analyst workflow while allowing them to leverage all data is crucial to success.

Going beyond cloud-native: Cloud-native is a common term. However, almost every organization leverages more than one cloud provider and still others have hybrid deployments. Does your security approach take this into account while also addressing data sovereignty requirements? And does it do so in a cost-efficient manner without moving data around?

Understanding your unique needs

Whether you aim to replace an existing solution or select your organization's first SIEM, you're in the right place. Selecting a SIEM for your organization requires assessing your situation from multiple angles. You'll need to consider your organization's priorities, your team's composition and processes, and the evolution of your attack surface — as well as how to best protect it.

Read on to explore key considerations about your situation and resulting guidance to weigh in your evaluation criteria.

Organization

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

Key considerations	SIEM guidance
What are your organization's crown jewels — and who might want them? What are your greatest areas of exposure? Which risks are business-critical and which can you accept?	Does your organization have financial assets that could be swiped? Systems that could be ransomed? Health records that could be sold? Intellectual property that a competitor might fancy? Critical infrastructure that an adversary could sabotage? Reviewing how the global threat landscape intersects with your organization's areas of exposure — and appetite for risk — is a key step for establishing priorities for your investment. Review your risk matrix and consider how your overall security strategy should shape your SIEM priorities.
Are you safeguarding employees everywhere they work? Has expedited cloud transformation caused new blind spots?	If the COVID-19 pandemic required your organization to suddenly shift to remote work, you may still be adjusting security practices to catch up. Transformation remains on the fast track for most businesses, so take stock. Do your defenses reflect your technology stack of today — or yesterday? Can you keep pace by quickly adding new cloud data sources? How strong are your endpoint protections? Do you have deep visibility into email and application activity? With just a click or two, can you inspect and take action on remote hosts? Don't lose sight of the risk posed by a return to the office. For use cases that require data from physical security (e.g., entry, location monitoring) and connected office technologies (e.g., printers, HVAC), choose a SIEM that makes it easy to ingest and normalize custom data sources.

elastic

Are security teams struggling to support new corporate initiatives?	Security teams must keep attackers at bay while enabling key organizational initiatives. Succeeding at both requires the agility enabled by an open and transparent SIEM. Unfortunately, closed security products often lack the integrations to automate workflows and the adaptability to evolve with your business. Consequently, they tend to cause tool bloat, break processes, and slow analysts. To stay nimble, guard against the constraints of: · Closed code · Not-invented-here syndrome · Inflexible licensing (e.g., per use case, by ingestion) Power new digital initiatives and support the success of Security, DevOps, and IT teams by choosing a SIEM that excels at monitoring the enterprise stack of tomorrow, including cloud infrastructure, workloads, and applications. Your priorities will continue evolving in the years ahead, of course. To get a sense for how well a given SIEM might grow to power new use cases, look for a track record of rapid roadmap advancement, a fast-growing integrations ecosystem, and a flourishing user community.
Does your organization experience significant fluctuations in business activity?	Are your company's sales highly seasonal, with surges that test the limits of your operating capacity? Does it sometimes expand into new markets or acquire established businesses? Hackers exploit stressful situations, so when the going gets tough, your SOC needs to be ready. Choose a SIEM with the scalability to rise to the challenge and the versatility to pivot to new use cases. As your needs evolve, adapt with SIEM licensing that makes it easy to scale up and down. Licensing should never get in the way of good security practices, so make sure it won't tie your hands when you need to be quick on your feet.
Are you concerned about vendor lock-in?	Vendor lock-in is a recipe for ineffectiveness and frustration. Gain control by choosing a solution with flexible licensing (including a free tier, ideally) that minimizes vendor lock-in. The deployment options of legacy SIEMs vary, with hit-or-miss support for hybrid and multi-cloud architectures and limited say over IaaS vendors. Confirm that your next SIEM offers a range of deployment options that will meet your needs for years to come.

elastic

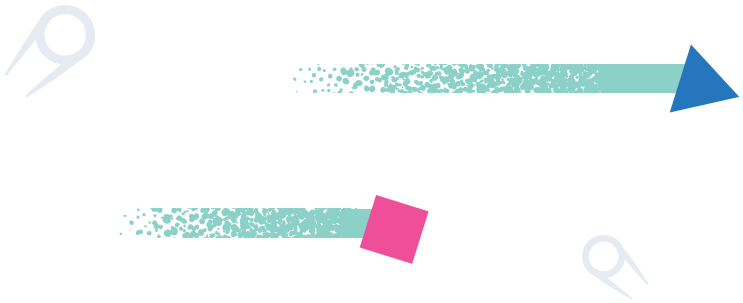
Your team

Empower each analyst to experience the satisfaction of making a positive impact with their work.

Key considerations	SIEM guidance
Does your organization struggle to recruit and retain skilled security personnel?	57% of organizations are impacted by the cyber skills gap, per a 2021 ISSA/ESG survey, preventing many organizations from being able to fully staff their security teams, particularly with specialists in investigation, cloud computing security, and application security. Increased workloads are amplifying burnout, causing the average security analyst to change employers every 18 months. Backfilling these positions takes 3-6 months (ISACA, 2019) and preparing even seasoned new-hires requires longer still. When choosing a SIEM, consider how to advance and retain your present practitioners and expand your recruiting pool. Ambitious analysts relish the opportunity to level up their skills to tackle important challenges — and don't want to be stuck in mundane work with obsolescing tools. As such, favor solutions with these two leading indicators: demonstrable product momentum and fast-growing user communities.
How much energy do your practitioners invest in detection and response vs. patching together technologies?	Security teams need a SIEM that's fast, intuitive, and can be seamlessly integrated with other technologies. Unfortunately, many security teams must still marshal a patchwork of tools and data silos. This dynamic steepens the learning curve for junior analysts, hampers experienced practitioners, and reroutes personnel from core SecOps functions. To boost SOC efficacy and morale, the solution should: · Delight analysts with a fast, intuitive, and powerful UI that allows them to clear away distractions and perform at their best · Simultaneously search all data tiers (e.g., hot, cold, frozen archives) — with structured and unstructured queries — several times faster than legacy technologies · Prioritize alerts and provide guidance and context for how to qualify and investigate detected behaviors · Streamline day-to-day analyst tasks by linking workflows with third-party technologies · Enable rapid remediation across your environment via semi- or fully automated response actions.

elastic

Do you have a threat hunting practice?	Scattered datasets and prolonged query times shouldn't stand in the way of your threat hunting program. Choose a SIEM that can quickly drill into a vast trove of environmental data and pivot on the fly. Automatically enrich this data with threat intelligence to surface context that further accelerates analysis. To help analysts see the signals amongst the noise, leverage prebuilt ML jobs that provide hunters evidence-based hypotheses for spotting threat activity like zero-day malware and social engineering. Built-in investigation queries and host inspection capabilities should support hunting activities.



Your processes

Enterprise transformation breaks existing SecOps processes, so choose a SIEM equipped to standardize and streamline organizational processes.

Key considerations	SIEM guidance
To what extent do you document and apply standard operating procedures?	Your organization likely already has documented processes for handling security incidents, such as procedures for evidence collection, cross-team collaboration, and board-level reporting. Whether these practices are currently detailed in a workflow system or simply a shared document, they reflect hard-won wisdom that's worth preserving. A SIEM should provide a built-in case management function that facilitates collaborative investigation and response and centralizes associated alerts, data, and notes. A SIEM should also enable your team to operationalize procedures in a playbook for investigation and response. This function should enable practitioners to incrementally automate routine steps, evolving into runbooks. Documenting (and later automating) investigation and response takes significant time and expertise, so look for a SIEM that provides a significant set of prebuilt playbooks/runbooks.

What tasks have you automated? Which would you like to automate next?	Legacy solutions were not designed with automation in mind. If APIs exist, they are typically limited to very specific functions. Some might also not be able to create automation workflows directly within their ecosystem, or interact with third-party RESTful services. If your team has already put in the work to automate some of its procedures, your next SIEM shouldn't require you to rework them from scratch. These automations should fit into any existing automation ideas or plans that you have lined up.
Do you use a dedicated platform for orchestration and automation?	If your security team operates a standalone security orchestration, automation, and response (SOAR) tool, your SIEM should integrate without hassle. If SOAR is still on the horizon for your organization, many SIEMs offer bolt-on SOAR capabilities and a select few deliver natively integrated SOAR. Look for seamless integration with the SIEM, because for a high-functioning SOC, these capabilities are inextricable.
How do security practitioners collaborate with other teams? Do these teams have a ticketing system with which your SIEM should integrate?	Investigating and responding to an incident — particularly one that impacts the wider business — typically entails working with colleagues on adjacent teams, such as IT and Legal. To streamline collaboration with peers outside SecOps, the solution should interface well with existing incident and task management tools (e.g., Jira, ServiceNow ITSM).

elastic

Your attack surface and protection needs

Consider the possibilities unlocked by the power to analyze all of your security-relevant data. Tackle any conceivable SecOps use case by exploring data from across your technology.

Key considerations	SIEM guidance
Are scaling challenges stemming from technology or licensing problems limiting which data you can centralize?	Without direct access to security data, practitioners have to fly blind. Yet many organizations often drop valuable data before it's even analyzed, reducing the breadth and depth of monitoring and detection efforts and eliminating visibility vital to response. Technological constraints with legacy technologies are the first culprit. Such solutions are notoriously poor at scaling both collection and analysis. Data spikes and high-volume data sources tend to compound these issues. Upon successfully centralizing data, new headaches related to analyzing such large datasets appear. Licensing constraints also often put the organization at risk by forcing security practitioners to evaluate which of their data to drop rather than centrally store and analyze (e.g., Which endpoints should we leave exposed? Can we get by without flow data?). The one-size-fits-nobody licensing models of many vendors (e.g., per-device, per-user, per-ingested or stored bit) place every customer in the same rigid box, regardless of their risk profile, executive priorities, or governance requirements — degrading their operational capacity. Security teams need to establish an entirely different set of expectations for their SIEM. They should aim for a platform that can quickly search and analyze all of their data, without unnecessary complexity or artificial licensing limits.
What data sources do you need to be able to employ — now and in the future?	Defenders must protect an attack surface ballooning from the growth of the digital economy, the vanishing of the perimeter, and other dynamics. In asymmetrical contrast, their adversaries can prod for weaknesses and test a succession of attack vectors. For most SOCs, achieving the visibility necessary to fight back has long been a pipe dream. Fortunately, blind spots and data silos are no longer inevitable. To establish control across your attack surface, the SIEM should centralize all security-relevant data — from your cloud infrastructure and applications, hosts, neworks, users, files, you name it — regardless of volume, variety, or velocity. It should enable uniform analysis by normalizing data with an open schema (e.g., CEF, **ECS**) and preserve a raw copy to enable unstructured search.

What data sources do you need to be vable to employ — now and in the future?	Prebuilt data integrations simplify the onboarding of new data sources. Disregard connector counts and focus instead on the overlap between the data sources that matter to your organization and the integrations shipped with each solution. Prioritize support for tomorrow's enterprise stack and be wary of solutions that excel with traditional tools but struggle with modern technologies. Criteria to consider for establishing visibility across various types of data: · **Host activity and context:** Does the solution provide access to system data via the best available tooling? Can analysts swiftly access system state (e.g., temperature) or perform ad-hoc queries (e.g., list currently running processes)? · **Cloud infrastructure and apps:** Does the solution support hybrid and multi-cloud environments with cross-vendor visibility into IaaS and PaaS technologies? Cloud workloads? Applications? Cloud access security brokers (CASBs)? Does it support the security posture of your containers and orchestration tools? · **Network activity and flow:** Does the solution normalize disparate network data — regardless of vendor and device type — to enable uniform analysis of data from network devices, cloud technologies, and hosts? · **User activity and context:** Do prebuilt integrations streamline the centralization of user access and authentication data? Can responders quickly view relevant context? Does the solution facilitate the analysis of privileged users, risky users, etc.? · **IoT and OT data:** Does the solution provide strong support for custom data sources and common IoT and OT data formats? Does it operate with a schema that allows data to be prepared for visualization and detection? · **Observability data:** Can practitioners tap into metrics, application traces, and CI/CD logs within natural SecOps workflows? Does the solution provide visibility across hybrid and multi-cloud environments? Can Observability teams safely be granted access to data in the SIEM? · **Third-party context:** Can you quickly onboard threat intelligence, vulnerability data, and other context? Does the solution utilize it to automate threat detection and accelerate incident response? Can the teams responsible for these datasets manage them in the same platform?
How often do you need to add new data sources?	The average enterprise uses 70+ security products. No SIEM provides out-of-the-box support for each one, so assess the complexity of building new integrations. Assess the associated documentation. Find the code used in other data integrations. Consider how readily you can collaborate with another community member. Are you going to need to burn consulting hours for each integration?

How many months or years of data do you need to retain for hunting, incident response, and compliance purposes? For how long do you need to keep this data ready for analysis?	Security teams need to be able to: · Retain actionable data for years, and search it in seconds to uncover long-dwelling threats and markers of newly discovered exploits, leveraging a wide range of storage options, including low-cost object stores like AWS S3. · Align data management with the needs of the tiered SOC, applying flexible licensing to balance retention length, performance, and cost. · Uniformly analyze information stored across multiple clouds without the delay and expense of data backhaul. Access to this wealth of activity and context eliminates blind spots and data silos, reduces alert fatigue, and arms practitioners to stop threats. The longer a threat is allowed to linger, the greater the potential destruction. Further, the adversaries most motivated to maneuver until accomplishing their mission — advanced persistent threats (APTs) — are also the best equipped to do so. It can be astonishing — even for security practitioners — to see how a major incident can unfold for months or even years, with a threat continuously operating in the environment and inflicting damage throughout. When a threat manages to outlast the logs that would reveal their attack from its first steps, incident responders have a much harder time fully extricating them. Without a full record, sealing off entry points and eliminating footholds becomes a marathon of guesswork and whack-a-mole. Storing data is expensive, so data management policies must balance retention, performance, and affordability. Unfortunately, the cost-prohibitive licensing models of many vendors force customers to unnaturally shorten retention periods and banish archives to distant silos. Some vendors also charge for each search of these archives or pass along the data transit charges incurred by the clunky workarounds required to do so. Most SIEMs allow customers to reduce costs by programmatically moving data to off-platform archives, but such workarounds hamstring responders with slow, clunky queries. In the heat of battle, time is short, so while marooning data in inaccessible buckets may suit the needs of auditors, it doesn't help responders.
How do you thwart zero-day exploits and other signatureless attacks?	Advanced analytics are a vital tool for exposing unknown threats presented by vendor attacks like SUNBURST, zero-day exploits like **Log4Shell**, and other vectors. Hackers attack weaknesses, so multi-layered detections are key. As such, advanced analytics are a complement to high-fidelity alerting, not a replacement. For optimal performance, the SIEM should offer the flexibility of both supervised and unsupervised machine learning.

How do you thwart zero-day exploits and other signatureless attacks?	With signatureless protections powered by machine learning, behavioral analytics, statistical analysis, and other methods, advanced analytics uncover threats that previously evaded notice. Focus your review on how well the analytics work and whether they're ready for production right out of the box. Beyond visualization basics like data charting and correlation, pursue a SIEM that provides intuitive interfaces for exploring data, imbued with relevant guidance, insights, and context. To more readily wield key technologies, look for purpose-built visualizations for correlating disparate data sources, viewing Linux system commands and process trees, examining cloud posture, and more.
How do you intend to automate threat detection over time?	Common attacks are more numerous than ever and sophisticated campaigns are multiplying, too. Clearing the decks requires the power of automated threat detection. Unfortunately, the signature-based detection methods of old school SIEMs tend to miss many adversaries, generate burdensome false-positives, and break. A modern SIEM should ship with a robust library of field-tested detection rules — created and maintained by security experts — to continuously flag adversary tools, tactics, and procedures. These rules help customers establish a baseline of detection far more quickly than would otherwise be possible. Alert prioritization helps focus analysts on the most concerning threats, lessening alert fatigue (the top challenge for 35% of security teams) and enabling automation. But in practice, it's sometimes more a Magic 8-Ball than a magic bullet. Be wary of vendors that overhype the precision of alert prioritization and underplay the work your team will need to put in to get it right. Look for a SIEM that aligns prebuilt detection rules with a framework such as MITRE ATT&CK® because automating threat detection requires a methodical approach. Incrementally broadening automated detection decreases mean time-to-detect (MTTD), reducing susceptibility to attack and freeing practitioners to tackle tasks requiring human intuition and skill. The solution should help detection engineers test new rules before implementation and facilitate red team automation to confirm continuing operation. Although activating a prebuilt rule is typically a one-click affair, the SOC would be wise to assign someone to monitor rule performance and update rule exceptions during the first couple weeks and on a regular cadence thereafter.

Do you have prevention, detection, inspection, and response capabilities deployed across all of your host systems?	For most first-party SIEM agents, collecting data is the only order of business. But a handful of SIEM agents go further, offering some combination of the following capabilities: · Secure hosts from a broad range of ransomware and malware families. · Detect threats with on-endpoint analytics. · Inspect systems with osquery. · Respond with actions like process suspension and host isolation.
What are your compliance considerations?	Nearly every organization must adhere to one or more regulatory and compliance frameworks and standards. To avoid unnecessary fines, business downtime, and reputational harm, consider these controls when choosing your next SIEM. Attaining comprehensive visibility across security and IT infrastructure is part of almost every plan. Prioritize solutions that provide prebuilt data integrations for the compliance-relevant technologies in your environment and enable streamlined development of custom integrations (including an open-data schema) for other technologies. Also account for related requirements such as data sovereignty and data masking. Be wary of vendors that require an extra subscription to access audit logs. Achieve compliance faster with a solution that offers open detection logic and response actions, rather than withholding the details of "proprietary" protections. Are systems like point-of-sale terminals or development servers a major part of your compliance footprint? Consider your organization's needs for integrated data collection and inspection, file integrity monitoring (FIM), and malware detection. Compliance reports are literally yesterday's news, so pursue real-time compliance visibility, and eventually, proactive enforcement. If compliance stakeholders want to be kept current, look for flexible dashboarding. To support the shift toward enforcing compliance controls, prioritize solutions with the horsepower to alert in real-time on notable violations and respond with autonomous or analyst-invoked actions.

elastic

SIEM requirements checklist

The below table reflects the best practices gleaned from numerous successful SIEM deployments. Specific customer deployments might differ in the priorities of requirements and likely include other needs.

1	Data ingestion and normalization	The solution must enable the ingestion of security-relevant data sources, representing cloud infrastructure, workloads, applications, servers and endpoints, network devices, users, etc.
2		The solution should offer out-of-the-box integrations with as many security-relevant data sources as possible, especially those that represent a growing part of your attack surface.
3		Solution must be adaptable to new data sources that may be unique to the organization.
4		Data must be uniformly normalized to enable aggregation and analytics.
5		The solution must retain data in an actionable form for years to aid with deep insights and analytics, and allow compliance with applicable requirements.
6	Detection and prevention	Solution must provide out-of-the-box detection capabilities
7		The solution must apply advanced analytics to spot hidden threats
8		Solution must include preventative capabilities to eliminate clearly identified threats and minimize analyst workload
9		Analytics capabilities must be transparent (not a trust-me black-box) and adaptable to customer environments
10		Solution must offer real-time and retrospective analytics to identify threats
11		Customers must be able to customize and create rules to suit specific environments and use cases
12		Solution must map detection techniques to well known frameworks (i.e. MITRE ATT&CK)

elastic

13	Investigation, hunting, and response	Solution must accelerate analyst workflows by surfacing risk insights and context (e.g., threat intelligence, vulnerabilities) throughout investigation and response.
14		Solution must allow analysts to search in near-real-time to give hunters and incident responders a richer understanding of the threats.
15		Solution must facilitate real-time inspection of impacted endpoints and cloud workloads.
16		Analysts must be able to search years of data for attacker activity without significant loss of efficiency.
17		Solution must offer case-management capabilities to help analysts collaborate.
18		Solution must enable autonomous and analyst-triggered response actions to minimize threat impact.
19		Solution should offer built-in security orchestration and automation capabilities and integrate with third-party systems to streamline cross-organizational workflows.
20	Deployment architecture	Solution must support deployment on-premises, in the cloud, and in hybrid and multi-cloud architectures, to meet evolving business needs.
21		Solution must support data residency guidelines with regional cloud deployments.
22		All key capabilities should be available from a single pane of glass.
23		Role-based access controls (RBAC) should support appropriate security.
24		Solution must be able to support multiple tenants (e.g., organizational lines of business, regions) with a single management layer.
25		Solution must offer appropriate data management capabilities to support long-term storage and analysis needs while optimizing costs

Build the SOC of tomorrow

There's a lot to consider when searching for the right SIEM vendor. View a day in the life of a security analyst to learn how **Elastic Security for SIEM** powers the modern SOC.

elastic