sumo logic

2025 Security operations insights

Three-quarters of security leaders need something new in SIEM

A SECURITY EXPERT'S GUIDE TO REEVALUATING YOUR ORGANIZATION'S SIEM
SECURITY INFORMATION AND EVENT MANAGEMENT

RESEARCH CONDUCTED AND VERIFIED BY UserEvidence

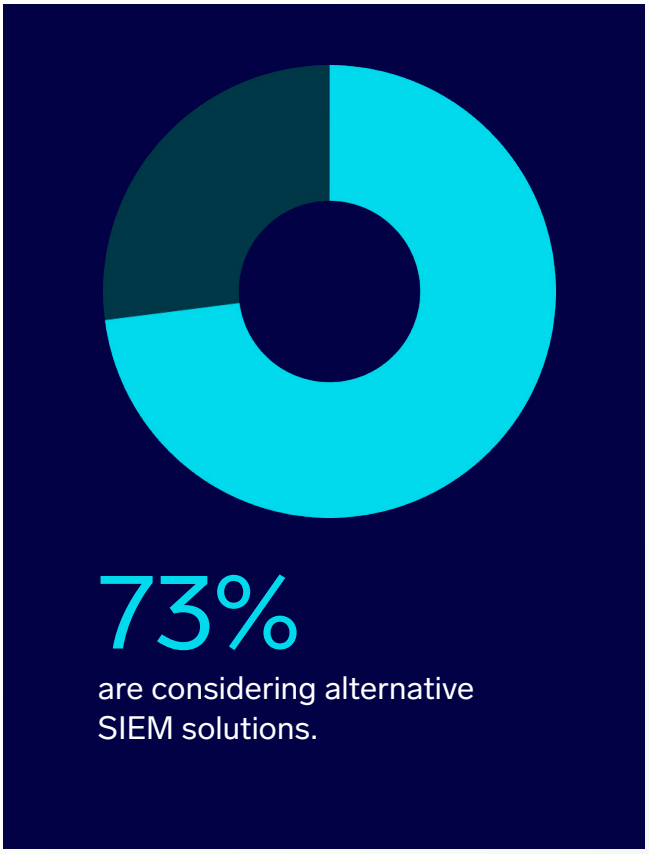
What's inside?

How SIEM is changing and what security leaders are looking for

Entering 2025, many organizations that raced to become digital natives now face the consequences of letting security become an afterthought. They encounter three converging pressures: AI-accelerated attacks, sprawling cloud telemetry that overwhelms analysts, and budgets that tighten even as expectations climb. The gap between what defenders must see and what many SIEMs surface widens—fueling alert fatigue, blind spots, and soaring storage bills. This survey zeroes in on how practitioners feel that strain and which capabilities they believe will close it.

At the same time, advances in AI are quietly reshaping both the threat landscape and the way defenders work. Automated tools now help attackers generate convincing phishing messages, probe cloud footprints at scale, and adapt techniques more quickly than manual monitoring can follow. On the flip side, security teams are beginning to rely on their own AI-driven analytics to sift through ever-growing log volumes, suppress routine noise, and surface the signals that matter. This mutual acceleration puts modern SIEM solutions—those built to blend rich data collection with embedded, adaptive analytics—squarely at the center of any serious security strategy.

Traditional SIEMs were never designed for today's flood of telemetry. Enterprises now need a cloud-scale SIEM that doubles as a security data lake, layers advanced detection on that data, and pairs every alert with an embedded automation service (SOAR) to streamline investigation and trigger rapid, consistent response.



This report will explore the findings from our research, sharing why and how security leaders are reevaluating their tech stack, the components of SIEM success, and the innovations shaping the security landscape next.

Why buyers are turning to new solutions in SIEM and SOAR

34%

of respondents identified enhancing threat detection and response as their top cybersecurity priority for the next 12 months.

93%

of respondents consider the SIEM approach relevant for safeguarding their organization.

Thirty-four percent of survey respondents say their number-one security priority for the coming year is to enhance threat detection and response.

That urgency explains why SIEM and SOAR now function as a combined imperative: SIEM delivers the visibility and analytic depth to spot trouble, while SOAR drives the playbooks that turn those insights into consistent, rapid action. Teams increasingly view the two as inseparable; what was once a bolt-on platform is becoming core functionality. In fact, 84 % of respondents rate integrated SOAR inside their SIEM as important or extremely important for automating responses to future complex threats.

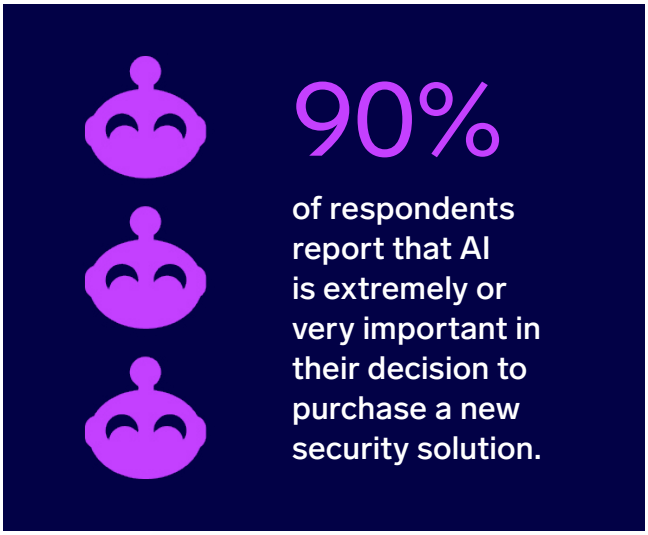
Yet even strong confidence doesn't lock customers in. Among leaders who feel "very confident" that their current SIEM can adapt over the next three to five years, 75 % are still evaluating alternative solutions—proof that meeting today's detection-and-response mandate is only the baseline, not a guarantee of long-term loyalty.

Let's unpack why leaders are looking elsewhere and how they should evaluate potential solutions.

The top four reasons for reevaluating the SIEM stack

Which factors play the largest role in convincing security leaders to consider an alternative solution? Respondents cite four key areas that most impact their confidence in the future of their SIEM solution.

1. Artificial intelligence



Seven out of 10 security leaders say that AI impacts their confidence in their current SIEM solution, the most common response by 30%. It follows that, of the organizations considering switching SIEM solutions, 90% report that AI is extremely or very important in their decision to purchase a new security solution, whether SIEM or an alternative.

AI offers massive potential to support and streamline security, from more intelligent alerts to automated response.

Over 70% of respondents struggle with alert fatigue and false positives—and many participants reported receiving over 10,000 alerts daily. Naturally, noise reduction is a high-priority improvement area for respondents, making the need to use AI for more accurate alerting and more efficient response all the more pressing.

2. Cloud-native

The second most common factor limiting security leaders' confidence in their SIEM solution is cloud-native capabilities (38%). Respondents prefer cloud-native platforms due to their scalability and ease of deployment, among other benefits. These advantages stand out when compared to traditional security options like XDR or standalone SOAR, which can be more specialized or limited in scope.

Key advantages of a cloud-native solution include:

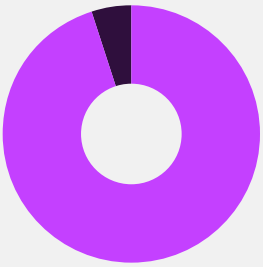
- Elasticity and scalability. These platforms can seamlessly scale up or down based on the organization's needs to handle large volumes of data from diverse sources without performance degradation. This flexibility will aid adoption of more cloud-based and distributed architectures.
- Real-time analytics and updates. Cloud-native SIEM solutions help organizations stay ahead of evolving threats by delivering security analytics and updates in real time, with no need for manual patches or upgrades.
- Unified view. Cloud-native platforms offer a holistic view of the security landscape, aggregating data from multiple cloud environments, on-prem infrastructure, and remote users in one place.
- Seamless integration and automation. A cloud-native SIEM platform like Sumo Logic can integrate with a range of cloud services and platforms, allowing organizations to unify security operations and automate responses, all within a single platform.

Research backs up these benefits: Nearly four out of 10 security leaders would consider changing their solution due to the agility and comprehensive coverage cloud-native SIEM makes possible. Of those considering changing their solution, the majority say they're evaluating cloud-native platforms.

3. The pace of innovation

A growing number of security leaders—more than one-third in this study—say the break-neck speed of security-tech innovation is already eroding their confidence in the SIEMs they run today . AI now reshapes attack techniques every quarter, compliance rules tighten almost as fast, and cloud services spin up new log sources weekly; a SIEM that can't absorb fresh analytics and automated playbooks at that cadence quickly turns from asset to liability.

They highlight three accelerators behind the gap: AI-powered detection methods evolving faster than static rule sets, automation frameworks raising expectations for near-instant containment, and continuously updated cloud stacks that demand new integrations on short notice. If a vendor can't push updated behavior models, detection content, and API hooks in lock-step with these changes, defenders are left working with yesterday's view of today's threats—an untenable risk for any modern SOC.



95%

of organizations looking to switch SIEM solutions cite vendor lock-in as a key concern in reassessing their security needs.

4. The role of vendor lock-in when considering solutions

Flexibility—not feature sprawl—is the currency of modern security. Nearly 95 % of teams eyeing a new SIEM list vendor lock-in as a primary reason for reevaluating their stack. When a single mega-suite controls ingestion, analytics, automation, and pricing, you lose the leverage to pivot as threats, budgets, and architectures change. Switching later becomes complex and costly, especially after custom content, data schemas, and workflows become entangled with proprietary tooling.

The risk goes beyond economics. One-size-fits-all vendors tend to optimize for retention rather than rapid innovation, shipping incremental updates while niche attackers evolve daily. Point solutions that embrace open standards—such as OpenTelemetry for log, metric, and trace collection—let you keep pace by integrating new data types or detections without rewiring the whole stack.

SIEM is not the place to compromise. Security leaders who treat it as a best-of-breed investment secure three enduring advantages:

- **Negotiating power**—you can replace or augment any layer without ripping out the core.
- **Continuous innovation**—specialized vendors live or die by keeping their detection and response tech ahead of attackers.
- **Operational fit**—teams tailor workflows to their environment instead of conforming to rigid platform assumptions.

In short: refuse "good-enough" platforms that trade short-term convenience for long-term constraint. Choose a SIEM that stays open, scales with you, and gives your team—not your vendor—the final word on how security evolves.

Taken altogether, these needs spell out the next phase of modern security operations:

Data is not just collected, but intelligently connected to drive faster insights, more informed decisions, and proactive security management.

The search for the right SIEM

As security leaders weigh their current tools against the competition, SIEM is very much alive. Organizations just need to choose the right SIEM, even and especially if they've had their current solution for a while. Nearly three-quarters (72%) of respondents who say they are considering an alternative solution have had their current solution for three years or longer.

Before investing significant budget and time in a new SIEM solution, enterprises must undergo a sufficient evaluative process to ensure the next one meets their needs. Use this five-step checklist to guide your process:

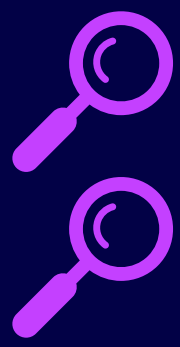
01 Data collection: Are you collecting the right logs?

The challenge with log collection is aggregating various disparate data sources accurately and efficiently. That's why most new entrants to the SIEM market get the vast majority of their data from their own endpoint solutions, and only their own endpoint solutions; they miss the bigger picture.

Cloud-native SaaS solutions offer scalability and speed, which should be top priorities for SIEM log collection. Look for features like comprehensive source integration, real-time data ingestion, and log storage and data retention.

02 Data transformation: How is data transformed in your SIEM?

After collection, the SIEM transforms the data into a usable format for analysis and next steps. Data transformation involves normalization, enrichment, and correlation processes. When evaluating your SIEM, consider factors like effectiveness of normalization, performance and scalability, contextual data integration, accuracy and relevance, and impact on detection and response.



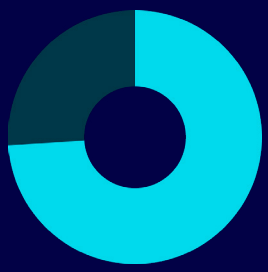
Log management use cases

The majority of respondents rely heavily on log management for compliance and forensic investigations.

03 Advanced analytics: Does your SIEM offer advanced analytics?

A solution is only as good as the ability to search the most data possible. Many solutions limit the amount of data to 30 days—while an attack dwell time can be three times longer.

Modern advanced analytics capabilities in a SIEM solution use machine learning (ML) to analyze large volumes of data and identify patterns that traditional methods might miss. Over time, these models enhance threat detection by adapting to new threat patterns.



74% of respondents said that having UEBA in their SIEM for proactively identifying future security anomalies was critical in their future plans.

A strong UEBA solution continually baselines every user, asset, and service; applies unsupervised machine learning with peer grouping to surface genuine anomalies; attaches context-rich, explainable risk scores; and routes findings straight into automated playbooks across on-prem, cloud, and SaaS environments. It should normalize logs into a universal schema for real-time streaming analytics, merge related anomalies into a single insight mapped to MITRE ATT&CK, support open APIs and sandboxed rule testing, and provide AI-assisted investigations that keep models fresh and noise low—so analysts can focus on the threats that truly matter.

04 Investigation: Does your SIEM offer effective investigation?

After a threat is flagged, your SIEM should pivot instantly into investigation mode—enriching every alert with real-time threat-intelligence context. Integrated feeds (via STIX/TAXII or vendor APIs) let the platform correlate fresh IOCs and MITRE ATT&CK TTPs against internal telemetry so analysts see where an event fits in the global attack landscape and why it matters. It's a capability practitioners now deem essential: 85 % of respondents rate out-of-the-box threat-intelligence integration in their SIEM as "extremely" or "very" important for staying ahead of future threats.

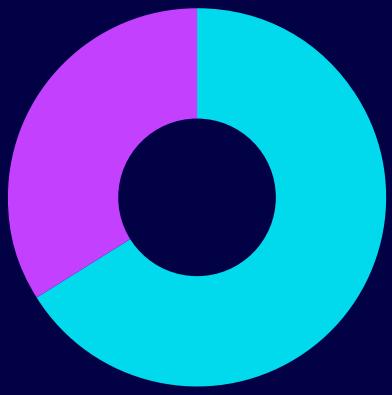
With that enrichment in place, best-practice investigation criteria expand to include: pinpointing the initial point of compromise, layering contextual intel and confidence scores, prioritizing alerts, triggering SOAR-driven automated triage, and aggressively reducing false positives—all while giving hunters the TTP-level detail they need for deeper searches across the environment.

05 Facilitating response

Evaluate SIEM response capabilities like customizable dashboards, role-based access controls, automated reporting, compliance tracking, incident response workflows, automation and orchestration (SOAR) of repetitive tasks, and post-incident reviews.

Top cybersecurity priorities

(next 12 months)



34%
Enhancing threat detection & response

19%
Modernizing infrastructure

18%
Achieving compliance

17%
Expanding security to new technologies

12%
Optimizing cost while maintaining security

The acceleration of digital transformation and the future of SIEM

As we've seen, most enterprise security leaders are considering or actively pursuing new SIEM solutions, and digital transformation is fueling this transition. Next, let's unpack how SIEM is changing and what organizations need to succeed in the future.

Diverse data telemetry for the modern security operation center

Receiving threat and security data from different kinds of environments is a key ingredient to digital transformation. So it comes as no surprise that 90% of respondents report that supporting data sources from multi-cloud and hybrid-cloud environments is extremely or very important for their SIEM as part of their digital transformation.

This flexibility is a foundational feature of the modern, intelligent security operations. Organizations can address the growing need to collect and manage telemetry from diverse sources in two primary ways:

Leverage open standards for data collection

Organizations should prioritize SIEM solutions that are compatible with modern, open standards for data collection, such as Open Telemetry (OTel). OTel has become the new de facto standard for vendor-agnostic agents, capable of collecting logs, metrics, and traces across a variety of environments. This standard simplifies data integration from multiple cloud platforms and provides the flexibility to transform and route data to multiple destinations as needed.

Going forward, proprietary collection mechanisms will struggle to keep pace with the needs of modern, cloud-driven infrastructures. Open standards empower organizations to decouple their telemetry collection from specific vendors and remain adaptable and scalable as their infrastructure evolves.

Future-proof security ops through data normalization

SIEM solutions that excel in data parsing, normalization, and mapping to a common schema or data model support enterprise needs for telemetry from diverse sources. Writing detections directly against raw logs as they are ingested from different security tools is brittle and labor-intensive to maintain. Replacing one security solution with another requires rewriting rules in the new vendor's log format, leading to operational bottlenecks, and nuanced vendor log formats make correlation complex.

When organizations normalize data into a consistent schema, they can maintain and enhance detections regardless of changes in the underlying security tools or cloud providers. This approach also upholds robust correlation across disparate data sources because the SIEM can process normalized data consistently, regardless of the vendor's log format.

Organizations should select SaaS-based SIEM platforms that offer built-in support for these tasks to alleviate the burden on in-house security teams and stay up to date with evolving data formats and security challenges.

Respondents mentioned training and skill gaps as a barrier to fully leveraging advanced SIEM capabilities.

Scalability to accommodate growing security needs

As organizations grow and change, so do their data and security needs. Naturally, our research uncovered that larger organizations report more frequent scalability issues. Compared to other SIEM features, respondents also indicate overall dissatisfaction with SIEM scalability. These findings reflect the need for flexible data-handling capabilities and illustrate the importance of scalability to unlock the next wave of SIEM. Data only continues to grow, which indicates that scalability will keep growing in importance, too.

Respondents indicate high satisfaction with log ingestion and search speed, and low satisfaction with integration and scalability.

Scalability is at the core of Sumo Logic's cloud-native platform. As organizations grow, the elastic architecture seamlessly scales to accommodate expanding log data, security events, and analytics without impacting performance. The ability to auto-scale ensures that customers experience consistent and reliable performance, no matter the data volume.

This flexibility also comes at a manageable cost with Sumo Logic's pay-as-you-grow model. As the data scales and requirements fluctuate, organizations only pay for the capacity they need.

Sumo Logic in action

One large enterprise customer transitioned from a traditional SIEM to Sumo Logic. As the business grew, so did the complexity and volume of their security data, especially from multi-cloud environments.

With Sumo Logic, the organization could ingest and analyze massive amounts of data in real time, while still maintaining high-speed query performance across their logs and metrics. As a result, their security team has significantly reduced mean time to resolution (MTTR) and stayed agile in responding to threats across various environments.

"After an exhaustive review of many industry SIEMs, we did a full integration testing of three solutions, and at the end of the day, we decided to partner with Sumo Logic. I'll tell you right now, it's the best decision we ever made. Sumo Logic ticked all the boxes for our requirements in a single solution. It provided flexibility in the platform for our security team to do non-traditional things for security monitoring."

James Morris, Vice President, Cyber Services and Technology NoAM N/A Regulatory Audit and Compliance, Threat Detection and Investigation Response, SRG
"Cloud Infrastructure Security SIEM Log Analytics" Professional Services, MSSP

Advanced analytics

Advanced analytics is an essential feature to enable proactive threat detection in modern SIEM solutions. Three-quarters of respondents report that having UEBA in their SIEM for proactively identifying future security anomalies was extremely or very critical. This trend holds true across industry and company size.

Sumo Logic leverages UEBA as a crucial layer. The platform continuously monitors and analyzes the behavior of users, devices, and applications within the environment. Sumo Logic UEBA can then detect subtle deviations from normal behavior that could signal potential security threats, including insider attacks, compromised accounts, or advanced persistent threats (APTs).

ML algorithms aid in baselining normal user activity and flagging unusual patterns such as access to sensitive files at odd hours or attempts to bypass security protocols. Sumo Logic customers have early warnings for anomalies—which signature-based or rule-based detection methods would otherwise miss—before they escalate into serious breaches.

Sumo Logic drives exceptional ROI

44%
of users report outstanding returns

67%
of users see significant value

This is the future of SIEM, and these capabilities allow organizations to step forward with confidence in their security strategy.

Emerging technological innovations and investments in SIEM

The security landscape is changing for better and for worse—as cyber threats grow more sophisticated, technology to respond to these threats is advancing in kind. Here's how two key innovations and approaches to SIEM are changing the direction of enterprise investments—and how Sumo Logic enables both.

How AI and automation are shaping SIEM investment

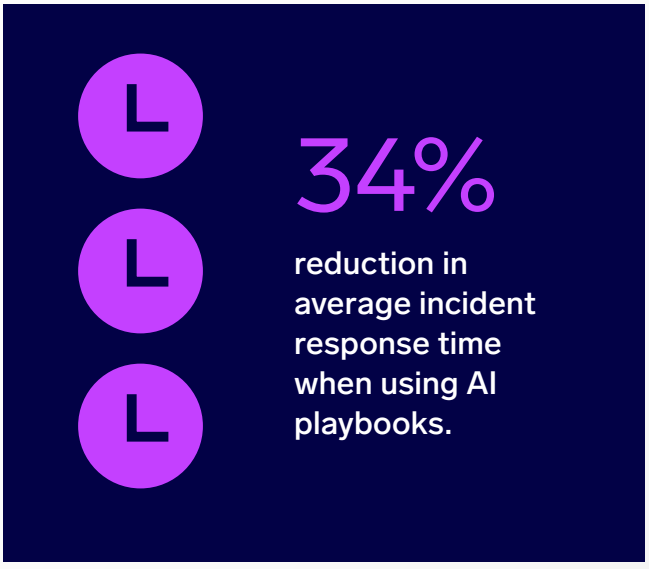
Enterprises that are actively searching for their next SIEM are likely to be on the cutting edge of artificial intelligence in security.

Alert fatigue is pushing buyers toward platforms that behave like AI co-analysts, not mere log collectors. The strongest signal from the survey is clear: respondents say an integrated automation layer (SOAR) inside the SIEM is essential for handling future, more complex threats. In their own words, they want a system that correlates events in real time, explains why they matter, and launches first-step remediation automatically—so human analysts begin every investigation several moves ahead.

Emerging technologies—especially LLMs and AI—play a complementary role in next-generation SIEMs, rather than acting as a complete replacement. LLMs can analyze textual data at an unprecedented scale, so AI-powered SIEMs can efficiently process vast amounts of security data and detect threats with greater accuracy.

The result?

More sophisticated threat detection, pattern recognition, and anomaly detection without overwhelming security teams. With respondents sharing that their top priorities are threat detection accuracy and achieving real-time response capabilities, this advancement couldn't be more timely.



AI-powered SIEM progression

Stage 1: Operational automation (today's baseline)

Most mature SOCs have already automated large portions of detection and response—log normalization, correlation, enrichment, ticket creation, and even basic containment actions such as disabling accounts or quarantining hosts. The business case is straightforward: cut the roar of false positives, drive minutes-not-hours mean-time-to-respond, and free analysts from repetitive swivel-chair tasks. Budgets in 2025 continue to flow toward technologies that combine rules-based logic with lightweight machine-learning models to suppress duplicate alerts, map events to MITRE ATT&CK, and trigger playbooks through an embedded automation service (SOAR). Teams at this stage focus on reducing alert volume, shrinking analyst touch-time per incident, and closing more incidents without escalation.

Stage 2: Analyst-assistive AI (near-term advantage)

The next leap replaces static playbooks with deeper AI that guides investigations in real time. Natural-language summarization, unsupervised anomaly detection, peer-group analysis, and contextual risk scoring converge to hand analysts a "why this matters" narrative instead of a raw event stream. These models automatically pivot across logs and threat-intelligence feeds, highlighting kill-chain progression and suggesting the next best query. By translating complex patterns into plain language and offering one-click hunts, AI off-loads cognitive load, accelerates triage, and effectively elevates Tier-1 analysts to tackle cases that once demanded senior expertise. Organizations here emphasize faster investigation dwell times, higher analyst productivity, and sharper incident accuracy as false-positive rates drop.

85%

of respondents rate out-of-the-box integration of threat intelligence feeds in their SIEM to stay ahead of future threats as extremely or very important.

Stage 3: Organization-tuned intelligence (strategic differentiator)

Ultimate maturity comes when security teams train domain-specific language and behavior models on their own telemetry, business logic, and historical incident data. These tailored models learn the organization's unique attack surface—custom SaaS apps, industry regulations, insider-risk profiles—so they can forecast likely intrusion paths, score anomalies against business impact, and recommend countermeasures aligned with internal workflows. Continuous fine-tuning on fresh data closes the feedback loop, automating remaining edge cases, exposing subtle lateral movement, and orchestrating fully customized response sequences. At this level, the payoff is proactive risk reduction—blocking novel techniques before damage occurs and giving defenders a durable, attacker-informed security advantage.

How Sumo Logic helps—and where to invest

Eight out of 10 respondents agree that current SIEM solutions effectively leverage AI-driven analytics to anticipate and mitigate future threats. But there's significant opportunity for more growth.

What AI-driven analytics should organizations pay attention to? For a start, they should look for entity-centric detections. Whether an event of interest comes from user accounts, non-human service accounts, or systems, effectiveness requires correlating these events across the attack life-cycle or kill chain back to an entity. Analysts can then see what happened and when. While legacy solutions still struggle with this view, AI will continue to push anomaly detection forward for higher fidelity alerts and lower false-positive rates.

Security leaders should also look for AI-driven features and outcomes we've already discussed, from predictive threat modeling and automated incident response to false positive reduction and threat intelligence integration.

Detection engineering moves security from reactive to proactive

Detection engineering revolves around precision, automation, and adaptability in threat detection and response. Given the evolving threat landscape, Sumo Logic sees detection engineering as a structured and iterative process that allows security teams to fine-tune detections, reduce noise, and enhance contextual awareness.

Here's how Sumo Logic approaches it:

1. Logs-first approach

Detection engineering starts with comprehensive log collection from cloud environments, on-prem infrastructure, and SaaS applications.

By normalizing and enriching logs, security teams can extract actionable signals from raw data.

2. AI-driven analytics and correlation

Sumo Logic applies machine learning to detect patterns, anomalies, and potential threats.

Behavioral analytics and UEBA help distinguish normal vs. suspicious activities.

3. Cloud-native SIEM for agile rule development

Custom rule creation enables teams to define detections that match their specific threat models.

Security teams can iterate and refine detection logic based on real-world attack data.

Cloud-native architecture ensures fast rule deployment and updates without operational overhead.

4. Reducing noise through automation

Correlation and suppression reduce false positives, surfacing high-fidelity alerts.

Entity-Centric Detection aggregates signals across users, endpoints, and applications for context-aware detections.

AI-assisted investigation helps analysts understand and respond to alerts faster.

5. Threat intelligence integration

Sumo Logic ingests multiple threat intelligence feeds, enhancing detection coverage with up-to-date IOCs (Indicators of Compromise).

Detections can be automatically enriched with contextual threat intelligence to prioritize response efforts.

With these steps taken, organizations can set up detection engineering as a cycle: analysts test and validate feeds, developing better rules and signals as they build.

How Sumo Logic supports emerging Intelligent SecOps

Investment in Intelligent SecOps allows enterprises to consider cybersecurity throughout the development process—not just when a threat occurs. It merges speed and agility with security and reduces the bottlenecks of older security models.

Sumo Logic's SIEM facilitates collaboration between these three teams by offering a unified platform that breaks down traditional silos. The platform offers real-time visibility across cloud and on-prem environments to ensure all teams can access the same security insights.

Sumo Logic fosters collaboration through:

- Integrated, customizable dashboards. Every team gets distinct insights they need from the same data sources. Research respondents reinforce the importance of these features, emphasizing the need for more customizable dashboards and reporting features in their SIEM.
- Continuous monitoring and logging. Teams can monitor security events and application performance logs within the same platform and work together to secure applications during development and after deployment.
- Automated workflows and playbooks. Sumo Logic enables creation of automated workflows that incorporate security checks into the development pipeline. The result is a security-by-design approach that supports DevSecOps in addressing vulnerabilities before they hit production.
- Intelligent SecOps paves the way for a proactive and advanced approach to security. Sumo Logic unifies logs, metrics, and security analytics to enable DevSecOps collaboration and secure modern, cloud-native environments.

Take the ROI of your SIEM from status quo to excellent

Just half of respondents rate the ROI of their SIEM solution as good. Security teams need features that allow them to work better:

Powerful correlation that cuts through alert overload and surfaces only real incidents.

Automation that eliminates repetitive tasks and gives analysts the freedom to focus on meaningful projects.

A SIEM with these features enables you to prevent burnout, keep talent engaged, and make the security team look like heroes. Prove the value of your investment by empowering your team and protecting your business.

Invest in cybersecurity that scales and adapts with our cloud-native platform—book a demo to see how our proactive monitoring can protect your organization when you need it most.

See SIEM in action

Methodology

Sumo Logic commissioned the independent market research agency UserEvidence to conduct the 2025 Security operations insights survey.

Who Are the Survey Respondents?

The study surveyed over 500 IT and security leaders from enterprise organizations.

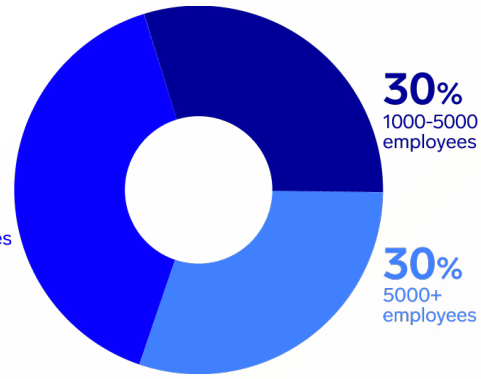
Four out of 10 respondent organizations have up to 1,000 employees, three out of 10 have between 1,001-5,000 employees, and three out of 10 have more than 5,000 employees.

Three-quarters of respondents come from organizations in the IT sector, while 7% come from manufacturing, 5% from financial services, and 4% from retail.

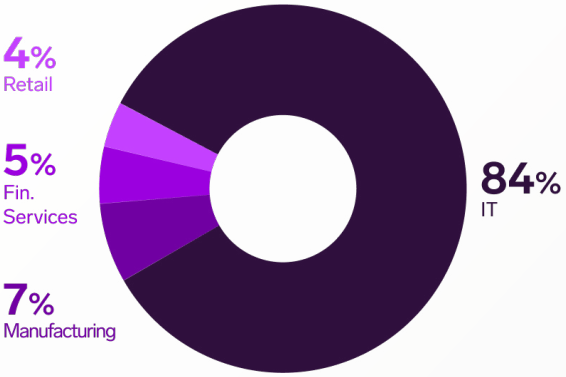
Survey respondents primarily hold security leadership roles, with over half serving as director of IT or security manager (33%) or information security manager (21%). Other top titles include security engineer (8%), chief security officer (7%), and chief security architect (4%).

On their digital transformation journey, half are taking a hybrid (SaaS) approach (49%), 24% are going through cloud migration, and 11% have moved to the cloud using legacy architecture.

Organization size

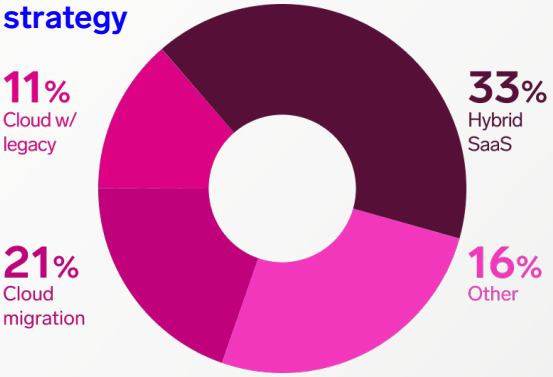


Industry



Job title

Digital strategy



UserEvidence

UserEvidence is a software company and independent research partner that helps B2B technology companies produce original research content from practitioners in their industry. All research completed by UserEvidence is verified and authentic according to their research principles: Identity verification, significance and representation, quality and independence, and transparency. All UserEvidence research is based on real user feedback without interference, bias, or spin from our clients.

UserEvidence Research Principles

These principles guide all research efforts at UserEvidence—whether working with a vendor's users for our Customer Evidence offering, or industry practitioners in a specific field for our Research Content offering. The goal of these principles is to give buyers trust and confidence that you are viewing authentic and verified research based on real user feedback, without interference, bias, and spin from the vendor.

Principle 1 — Identity verification.

In every study we conduct, UserEvidence independently verifies that a participant in our research study is a real user of a vendor (in the case of Customer Evidence) or an industry practitioner (in the case of Research Content). We use a variety of human and algorithmic verification mechanisms, including corporate email domain verification (i.e., so a vendor can't just create 17 gmail addresses that all give positive reviews).

Principle 2 — Significance and Representation

UserEvidence believes trust is built by showing an honest and complete representation of the success (or lack thereof) of users. We pursue statistical significance in our research, and substantiate our findings with a large and representative set of user responses to create more confidence in our analysis. We aim to canvas a diverse swatch of users across industries, seniorities, personas - to provide the whole picture of usage, and allow buyers to find relevant data from other users in their segment, not just a handful of vendor-curated happy customers.

Principle 3 — Quality and Independence

UserEvidence is committed to producing quality and independent research at all times. This starts at beginning of the research process with survey and questionnaire design to drive accurate and substantive responses. We aim to reduce bias in our study design, and use large sample sizes of respondents where possible. While UserEvidence is compensated by the vendor for conducting the research, trust is our business and our priority, and we do not allow vendors to change, influence, or misrepresent the results (even if they are unfavorable) at any time.

Principle 4 — Transparency

We believe research should not be done in a black box. For transparency, all UserEvidence research includes the statistical N (number of respondents), and buyers can explore the underlying blinded (de-identified) raw data and responses associated with any statistic, chart, or study. UserEvidence provides clear citation guidelines for clients when leveraging research that includes guidelines on sharing research methodology and sample size.