BridgerWise Research

Sponsored by TandemTrace

AI in the SOC

European Practitioner Survey 2026

Adoption, Automation and Operational Impact

Research Report

March 2026

BridgerWise Research

Sponsored by TandemTrace

AI in the SOC

European Practitioner Survey 2026

82 %

82 % expect **AI usage in the SOC to increase** in the next 12 months

46 %

~~Cutting down~~ false positives rate is **#1 priority**

64 %

Automated Alert Triage would deliver the **most value** for SOCs

24 %

24 % of alerts are **ignored or closed** without investigation

65 %

Majority of SOCs don't count with **dedicated threat hunters**

#1

Context switching and **tool fragmentation** is the biggest operational challenge

TABLE OF CONTENTS

INTRODUCTION

Security Operations is going through one of its **most significant transformations** since the **early days of automation and the rise of SOAR platforms**. Today, AI is increasingly present in the SOC, shaping how alerts are triaged, how investigations unfold, and how analysts spend their time.

Yet despite the constant discussion around AI in cybersecurity, much of the publicly available data and commentary reflects a very specific perspective: the U.S. market.

Most industry statistics, surveys, and benchmark reports are heavily weighted toward North American organizations. While they often include responses from other regions, European voices tend to represent only a small fraction of the data. As a result, the narrative around SOC challenges, priorities, and technology adoption often fails to capture the operational realities faced by security teams across Europe.

This gap is precisely what motivated this research.

At **BridgerWise Research**, we set out with a simple goal: **to better understand the state of AI adoption in European Security Operations** and to provide SOC professionals with a clearer picture of how their peers across the region are approaching this transition.

To do this, we conducted an anonymous survey of security professionals working in and around SOC environments across Europe. While more than 100 professionals initially engaged with the survey, responses were carefully cleaned and validated, resulting in over 50 qualified submissions. While this may appear modest at first glance, it represents a meaningful dataset in a field where many global reports include even less responses from outside the United States.

The findings presented in this report highlight an important reality: **while alert fatigue and alert overload are frequently cited as the defining challenges of the SOC, they are only part of a much broader operational picture.**

Security teams across Europe are balancing increasing detection volumes, analyst capacity constraints, growing infrastructure complexity, context switching, false positives and mounting pressure to operationalize automation and AI. At the same time, organizations are still navigating practical questions around trust, implementation, and the real operational value of AI-driven technologies.

As one respondent noted:

> **Everyone is talking about reducing alerts (fatigue), but with AI we should be able to turn up the noise, while the SOC evolves into a more strategic role.**

Another practitioner captured challenges that are very much European:

> **NIS2 reporting SLAs expectations require us to quickly triage and identify root cause and blast radius, prioritizing root cause analysis and report generation.**

These voices reflect the broader theme that runs throughout this report: AI is already part of the SOC, at least in terms of considerations, but its role, maturity, and impact vary widely between organizations.

For some teams, AI is already embedded in triage and detection workflows. For others, it remains a capability under evaluation, constrained by concerns around reliability, transparency, regulations, or operational integration. What is clear, however, is that **the SOC is entering a new phase of transformation**, one where AI is no longer a distant concept but an emerging operational layer.

Our intention with this report is not simply to present statistics. Instead, we aim to provide European security professionals with three things:

- **Visibility** into how their peers across the region are approaching AI.
- **Context** around the operational pressures shaping SOC priorities.
- **Benchmarks** that help teams understand where they stand within this evolving landscape.

We hope the insights in this report help SOC leaders, analysts, and security practitioners better understand the trajectory of Security Operations in Europe, and the role AI will play in shaping the next generation of the SOC.

Ignacio Sbampato
Partner
BridgerWise

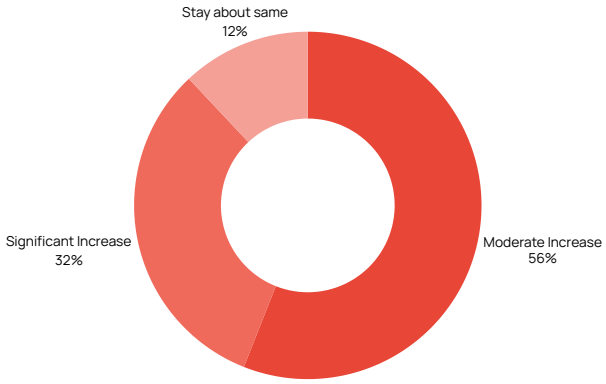
KEY FINDINGS

1 1/3 of SOCs expect their AI usage to significantly increase this year

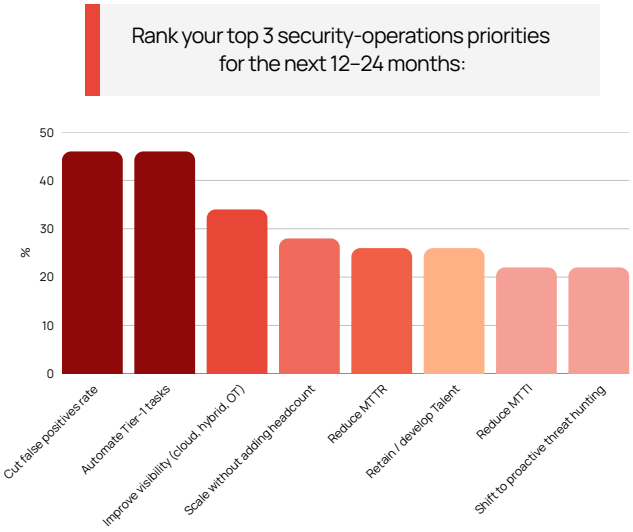
The majority of respondents are looking into adopting AI further in the next 12 months, with 32 % reporting a significant increase, and more than 50 % seeing a moderate one ahead of them.

2 Reducing False Positives and Automating Tier-1 Tasks are the highest priorities for SOCs in the next 12 months

Close to 50 % of respondents have reported that cutting down the number of false positives as well as automating partially or fully the work currently handled by their Tier 1 analysts are the biggest priorities for them at the moment.



How do you expect your organisation's AI usage in security operations to change in the next 12 months?



3 24 % of alerts are ignored or closed without investigation

SOC teams report being unable to investigate at least 1 in 4 alerts, with 18 % of them reporting they are suppressing more than half of them. There's no clear relationship between alert volume and ignored alerts, suggesting that this is driven more by process inefficiencies and tooling fragmentation than pure volume alone.

4 Alert noise is limiting detection visibility

Majority of SOC teams are operating with limited EDR and Network telemetry, with close to half of them reporting also that they would welcome higher visibility into the Cloud and Identity dimensions if noise wouldn't be an issue. Interestingly, **teams that restrict detections most frequently are also the ones wanting the broadest telemetry coverage.**

5 **AI & Automation adoption is growing, but operational maturity varies widely**

Around 50 % of respondents report using SOAR-driven automated playbooks and/or ML-based anomaly detections, with 24 % using some level of AI-driven automatic alert triage. Despite that, the majority of those that have those use cases implemented are still dealing with high false positive rates and a need for further automation.

6 **Enterprise SOCs and MSSPs are pursuing different AI strategies**

The segmentation analysis reveals clear differences between SOC operating models. MSSPs are focusing on false-positive reduction, playbook automation and MTTR reduction more than Enterprises, where we find a greater interest in automating Tier-1 tasks, implementing investigation assistants and detection rule tuning and coverage expansion.

7 **Smaller organizations face more operational strain**

When analyzing the responses by company size, the smaller organizations receive **more alerts on average** and also **ignore significantly more alerts**. Their priorities reflect this pressure due to a greater focus on **false-positive reduction** and stronger need to **scale without adding headcount**. Meanwhile, larger organizations are looking more into Threat Hunting, Measuring SOC effectiveness and Cloud visibility.

ABOUT THE SPONSOR

TandemTrace is a European cybersecurity company specializing in an **Agentic AI platform for Security Operations**. Their solution focuses on threat detection, investigation and hunting, based on autonomous agents that can perform full alerts triage and root-cause analysis, hypothesis-driven threat hunting, providing comprehensive results for SOC analysts to remediate security issues and respond to breaches.

Their platform also identifies false positives and attack surface blindspots, and includes additional functionality to perform AI-assisted investigations and initiate hunts supported by the **TandemTrace** autonomous agents.

TandemTrace is available in **Cloud** and **on-premises** deployments and it is compatible with the most common SIEM and XDRs, like **Splunk, ElasticSearch, QRadar, Microsoft Sentinel** and **Crowdstrike.**

AI & AUTOMATION IN THE SOC

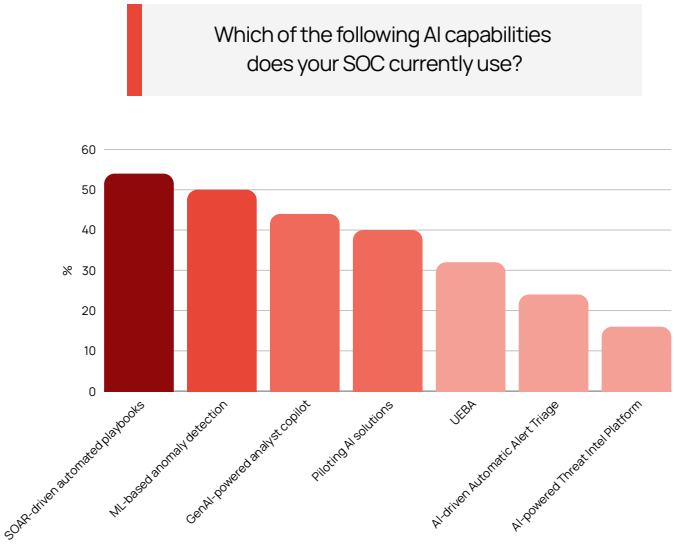
Automation in the SOC did not start with AI. Over the past decade, security teams have relied on a range of automation approaches including **SIEM correlation rules**, **detection-as-code pipelines**, **automated enrichment workflows**, and **SOAR playbooks**.

Many organizations also developed internal scripting and data engineering pipelines to automate enrichment, rule deployment, and investigation tasks. These approaches laid the operational foundation for the more advanced AI-driven capabilities now emerging in security operations.

More recently, advances in machine learning and generative AI have introduced new approaches to automation within the SOC, particularly in areas such as alert triage, investigation assistance, and analyst productivity.

Within our research, the most common use cases when it comes to automation and AI are:

1. SOAR-driven automated playbooks (54 %)
2. ML-based anomaly detection (50 %)
3. GenAI-powered analyst copilot (44 %)



While several AI-enabled capabilities are already present in many SOC environments, fully automated workflows remain relatively rare. AI adoption doesn't necessarily mean automation maturity.

For example, 24 % of respondents report using AI-driven alert triage, while the majority of them continue to rank false positives and automation as their primary concern. **Moreover, 12 % report having no AI capability whatsoever.** This suggests that most organizations are still experimenting with AI-assisted workflows rather than relying on autonomous systems.

To better understand how AI adoption varies across the industry, we compared responses between enterprise SOC teams and managed security service providers.

The following sections will explore AI & Automation in the SOC further.

a Differences between SOC operating models

The analysis reveals **meaningful differences** between enterprise SOCs and managed security service providers (MSSPs). Enterprise teams report higher adoption of anomaly detection and automated playbooks, while MSSPs are more frequently evaluating or piloting new AI solutions.

Moreover, at least one third of enterprises are already having some level of AI-driven alert triage automation.

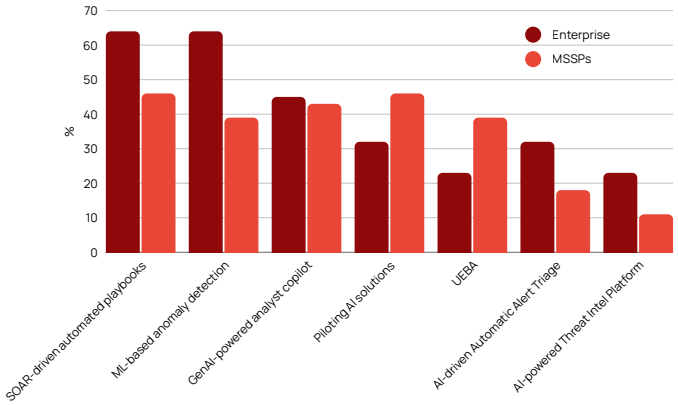
The Enterprise reality contrasts with the situation of MSSPs, where almost half of them are currently evaluating or piloting new AI solutions due to their lower current adoption.

The adoption of SOAR doesn't necessarily mean better automation, as those that report having SOAR-driven automated playbooks are as likely to report insufficient automation as a challenge than those that don't have SOAR in place.

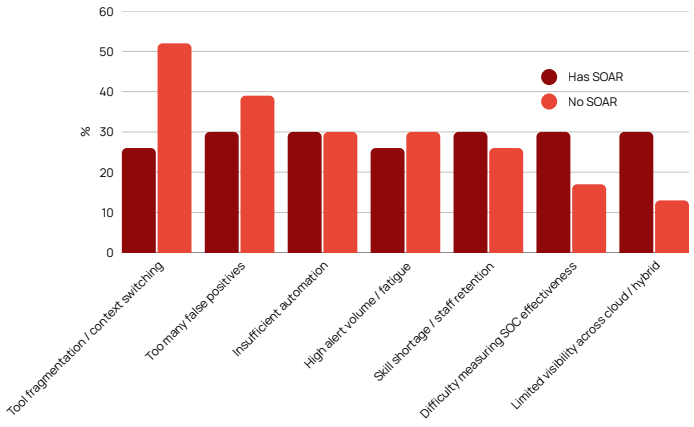
Consequently, **respondents that report already using SOAR-driven automated playbooks are also among those most likely to prioritize false-positive reduction and Tier-1 automation in the coming year**. This suggests that the introduction of automation does not necessarily eliminate operational pressure, and may instead highlight additional opportunities for workflow optimization.

Reducing False Positives and Automating Tier-1 Tasks are the highest priorities for SOCs in the next 12 months

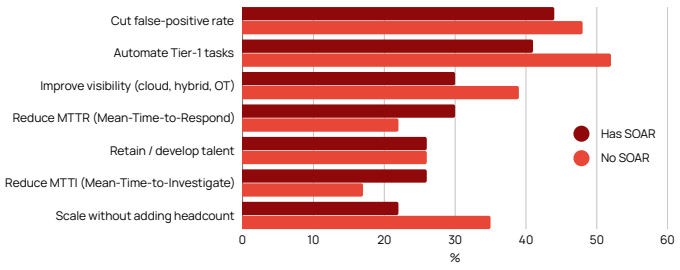
Which of the following AI capabilities does your SOC currently use?



Top 3 operational challenges (Split based on SOAR availability)



Top 3 security-operations priorities for the next 12–24 months (Split based on SOAR availability)



b What SOCs want AI to solve

Automated alert triage and prioritization is where majority of SOCs would expect AI to deliver most value for them (64 %, consistent across MSSPs and Enterprises), followed by **investigation assistance in context and root-cause analysis** (54 %, more likely among Enterprises) and **playbook automation & response orchestration** (44 %, more likely among MSSPs).

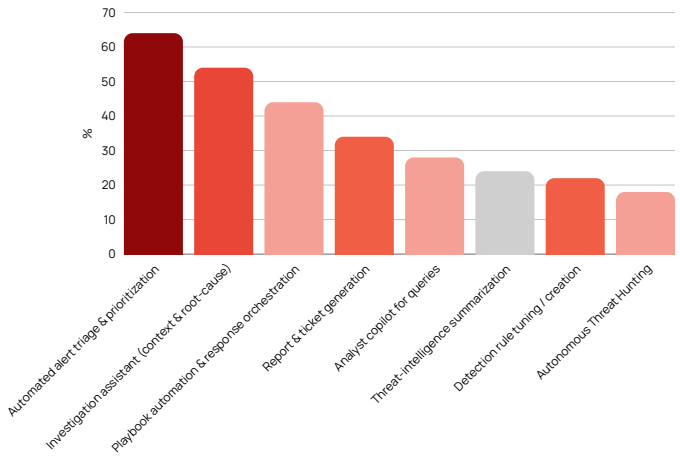
Alert triage and prioritization, investigation, and response orchestration are all time-consuming tasks traditionally handled by Tier-1 and Tier-2 analysts

One of the clearest differences between enterprises and MSSPs appears **in detection engineering**. While more than one third of enterprise SOCs see detection rule tuning as a valuable AI use case, only 11% of MSSPs prioritize it. This reflects different operational priorities: enterprises tend to focus on improving internal detection capabilities, while MSSPs prioritize scalable operational workflows.

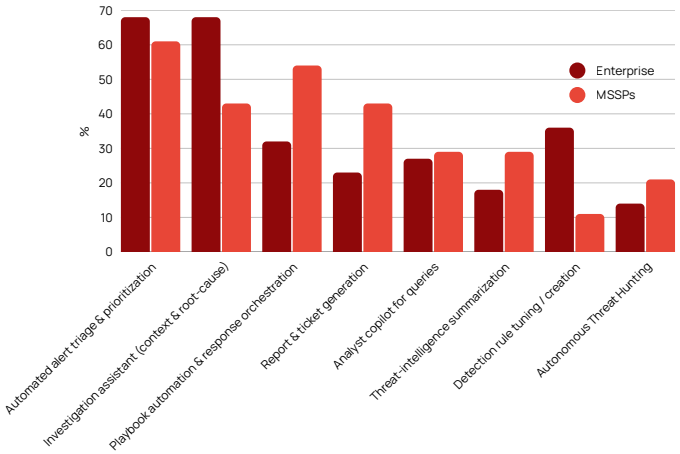
Another one is in **Report & Ticket generation**, where 43 % of MSSPs highlight this as an AI use case that will deliver more value compared to 23 % in the case of Enterprises. As MSSPs support multiple customers, prioritizing the need to reduce the workload related to reporting is expectable.

Finally, **Autonomous Threat Hunting** is more relevant for MSSPs than the creation and tuning of detection rules (21 %), **something we explore in a specific section further down this report.**

Which AI use-cases would deliver the most value in your SOC?

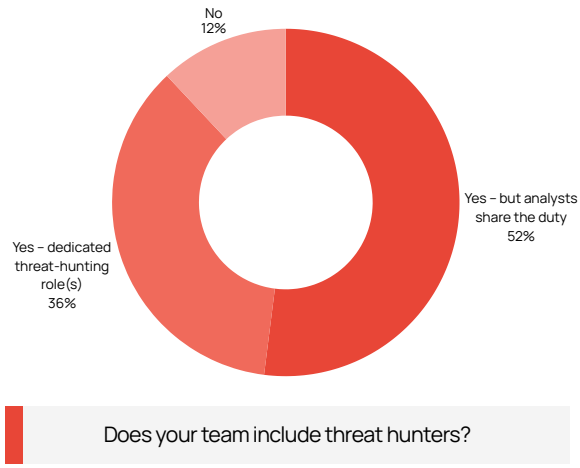


Which AI use-cases would deliver the most value in your SOC?
(Split Enterprise vs. MSSP)



C Threat hunting as the next step in SOC maturity

Threat hunting capabilities are present in many SOC environments, but they are often not dedicated roles. **Only about one third of organizations report having dedicated threat hunters**, while in most cases the responsibility is shared among analysts with other operational duties. This is lower than one would expect, considering the benefits it could bring are known and supported by data (IBM, Cost of a Data Breach Report 2025)



Dedicated threat hunters are significantly more common among MSSPs, as **only 18 % of the enterprise SOCs report having them**. In the majority of the cases, threat hunting is an activity that analysts with other responsibilities are performing.

This comes as no surprise as 61 % of organizations cite skilled staffing shortages as a primary barrier to success in this area (SANS 2025 Threat Hunting Survey).

When looking at priorities for the next 12–24 months, **roughly one quarter of organizations report plans to shift toward more proactive threat hunting.** However, fewer respondents (1 in 5) identify threat hunting as a primary AI use case, suggesting that many teams still view automation and triage improvements as more immediate priorities.

When it comes to priorities for the next 12-24 months, a shift to proactive threat hunting is reported by almost 1 in 4 organizations, consistently across MSSPs and Enterprises. Yet, only 1 in 5 consider it as an AI use case that can deliver the most value, below the top cases mentioned above.

This gap suggests that threat hunting remains a longer-term capability for many SOC teams. Operational pressures such as alert volume, false positives, and staffing shortages appear to limit the resources organizations can dedicate to proactive detection activities.

Survey results also suggest that many SOC teams operate with limited telemetry due to alert noise. This constraint further limits the ability to conduct proactive threat hunting, as effective hunting typically requires broad visibility across endpoints, networks, and identities.

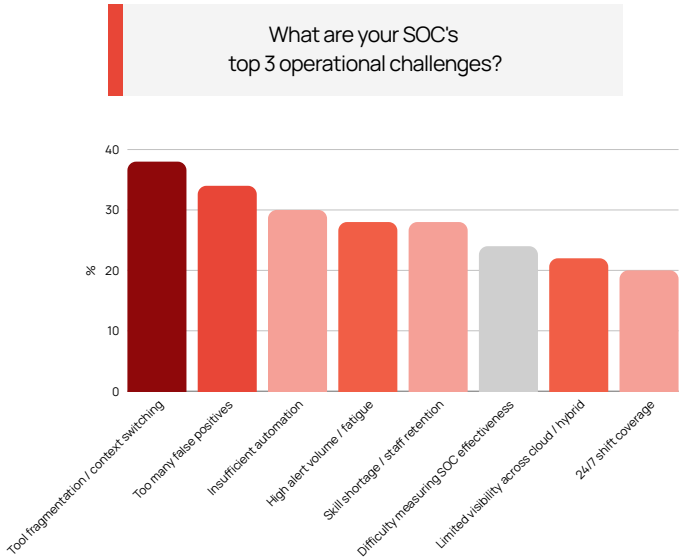
As automation and AI begin to reduce the time analysts spend on triage and investigation, some organizations may gain the operational capacity required to invest more heavily in proactive threat hunting.

OPERATIONAL CHALLENGES

Security operations centers face a wide range of operational challenges, many of which go beyond the commonly cited issue of alert fatigue. **The survey results suggest that structural operational issues - such as tool fragmentation, false positives, and limited automation - often create more friction for analysts than the sheer volume of alerts itself.**

"High alert volume / fatigue" came only 4th, with 28 %, in our survey, followed closely by "Skill shortage / staff retention", and the difficulties of measuring SOC efficiency.

These findings suggest that the biggest operational challenges in the SOC are not necessarily related to alert volume itself, but rather to the workflows and processes required to triage and investigate alerts efficiently.



Analysts often need to pivot between multiple platforms during investigations, including SIEM, endpoint telemetry, threat intelligence feeds, and ticketing systems. **This constant context switching increases investigation time and reduces the overall efficiency of SOC workflows**. In this survey, tool fragmentation and context switching emerged as the most frequently cited operational challenge, surpassing even alert fatigue, which is often considered the defining problem of the SOC.

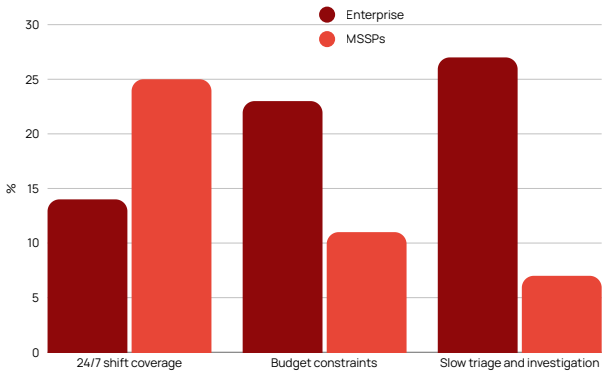
> **Everyone is talking about reducing alerts (fatigue), but with AI we should be able to turn up the noise, while the SOC evolves into a more strategic role.**

Now, when we review those results one level lower, looking into identifying those challenges that are more common for Enterprises or MSSPs, the reality is that the top 2 remain the same. It's not alert fatigue, as usually mentioned, that causes more issues for SOC professionals: **it is the need to manage too many tools**, regularly switching context when triaging or investigating, and the high number of false positives that their detections are causing.

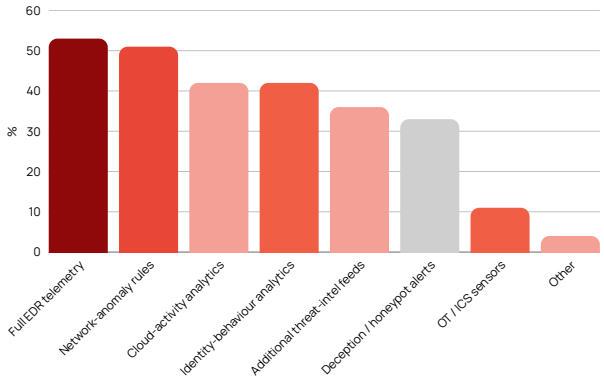
The **main difference** between enterprise SOCs and MSSPs is when it comes to **24/7 shift coverage, budget constraints and the speed of triage and investigation**. MSSPs are the ones highlighting the span of their coverage twice as much as enterprises, while the latter highlights "slow triage and investigations" 4 times as much as MSSPs, and budget more than double.

Noise is also another issue that SOCs face, as many of them limit detections or telemetry sources. **More than half of respondents would enable full EDR telemetry if it wouldn't generate that many additional alerts and false alarms**, followed closely by others: network-anomaly rules (51 %), cloud-activity analytics (42 %) and identity-behaviour analytics (42 %).

What are your SOC's top 3 operational challenges?
(Split MSP & Enterprise)



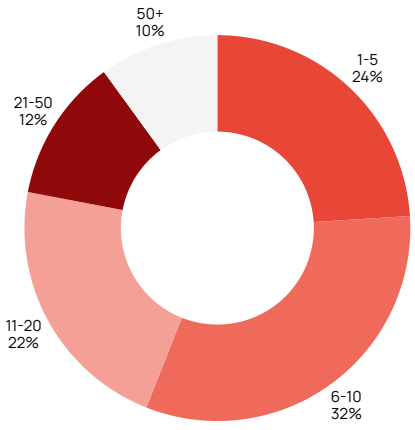
If noise were no longer an issue, which detections would you enable?



This takes relevance when we consider that the respondents need to deal with a large number of distinct security tools feeding alerts into their systems, and more than half of them are ignoring or closing alerts without investigation regularly.

Another recurring challenge highlighted by respondents is the difficulty of measuring SOC effectiveness. While metrics such as mean time to detect (MTTD) or mean time to respond (MTTR) are commonly used, they often fail to capture the full complexity of security operations.

Several respondents indicated that measuring analyst productivity, detection coverage, or the real impact of automation remains difficult, making it challenging for organizations to evaluate the effectiveness of their SOC investments.



How many distinct security tools feed alerts into your SOC / SIEM today?

The survey results also show that operational challenges are not evenly distributed across organizations. **Smaller SOC teams report receiving more alerts on average and ignoring a larger share of them**, reflecting the difficulty of scaling security operations without increasing headcount

These operational challenges help explain why automation and AI have become such prominent priorities for SOC teams. Many of the most frequently cited problems - context switching between tools, manual investigation steps, and high volumes of low-quality alerts - are **precisely the areas where organizations expect AI to deliver operational improvements.**

REGULATIONS & COMPLIANCE

Regulatory requirements play a particularly significant role in European security operations. Frameworks such as NIS2, DORA, and the upcoming AI Act introduce new expectations around incident reporting, accountability, and the governance of automated systems.

Despite this, the impact of European regulation on SOC operations is rarely examined in global cybersecurity research, which tends to focus primarily on North American organizations. That is why we made this a core part of our research, where we asked participants which compliance challenges concern them the most when deploying AI in the SOC.

The respondents have highlighted that the **explainability and auditability of the decisions made by AI are among their top concerns**, as 2 out of every 3 answered this is a current compliance challenge for them.

Their worries don't end there: liability for automated actions, where the data is stored and potential supply-chain risks from the AI vendors were chosen by half of respondents. **Compliance-related concerns are top in the mind of European SOCs.**

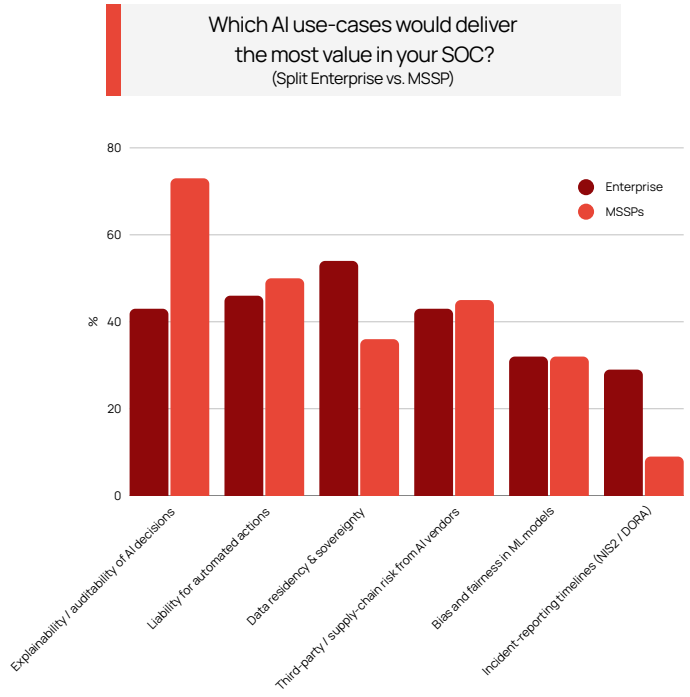
When we dig deeper, the results show that the situation differs significantly between enterprises and MSSPs.

- The biggest compliance challenge for enterprises is the Explainability & Auditability of AI decisions (73 %), while MSSPs only cited it as such in 43 % of the responses
- For MSSPs, the main challenge is Data Residency & Sovereignty (more than half of respondents). This is significantly lower with Enterprises (1 in 3)

Liability for automated actions is highlighted by half of the organizations, as well as third party and supply-chain risk from AI vendors (around half of respondents in those cases from both enterprises and MSSPs). This reflects an emerging challenge for organizations deploying AI-driven automation: **determining accountability when security decisions are made or influenced by automated systems.**

Liability for automated actions is highlighted by half of the organizations, as well as third party and supply-chain risk from AI vendors (around half of respondents in those cases from both enterprises and MSSPs). This reflects an **emerging challenge** for organizations deploying AI-driven automation: **determining accountability when security decisions are made or influenced by automated systems.**

The way these concerns are ranked is not surprising as enterprise SOCs are regularly audited, internally and externally, and accountability and explainability are highly relevant in those cases. In the case of MSSPs, as they need to handle customer data, cross-border concerns are among their biggest ones.



Incident-reporting timelines introduced by regulations like NIS2 and DORA have not been cited as relevant by enterprises, but almost 1 in 3 of MSSPs have highlighted as a concern, likely reflecting the operational complexity of managing regulatory reporting across multiple client environments.

The participants had an additional option in this particular question: to select that they have no concern and they feel well prepared. **None of the participants selected it**. However, around half of the respondents said that they are **Somewhat** to **Very Confident** when it comes to their current or planned AI tools meeting regulatory requirements.

> **EU regulations like NIS2 and DORA drive my SOC strategy by mandating ultra-fast incident reporting (eg, DORA's 4-hour initial alerts vs. NIS2's 24 hours) and rigorous third-party risk management, forcing automated detection, real-time logging, and supply chain audits as core priorities. The AI Act further requires explainable AI triage for high-risk detections to ensure compliance during automated Tier-1 handling.**

Due to the above, EU Regulations are strong drivers for accelerating the adoption of AI in MSSPs, with more than 40 % citing it that way. On the other side, 1 in 4 of the respondents refer to regulatory uncertainty as a barrier slowing or preventing AI adoption in their organization.

European regulations appear to have a dual effect on AI adoption in the SOC. While compliance requirements encourage automation and explainable AI capabilities, regulatory uncertainty around emerging frameworks such as the AI Act also introduces hesitation for some organizations.

FUTURE OUTLOOK: OUTCOMES, BARRIERS AND THE NEXT PHASE OF AI IN THE SOC

Taken together, the survey findings suggest that AI adoption in security operations is being driven less by technological experimentation and more by operational necessity.

Security teams across Europe are increasingly turning to automation and AI as a way to reduce context switching and the number of alerts, accelerate investigations, and scale operations without proportionally increasing analyst headcount.

While fully autonomous SOC workflows remain rare, AI-assisted operations are quickly becoming a foundational capability in modern security operations environments.

1 Early Outcomes of AI Adoption

Organizations that have already deployed AI capabilities are primarily using them to support analyst workflows rather than replace human decision-making. The most common use cases identified in the survey - **automated alert triage, investigation assistance, and response orchestration** - focus on reducing the time analysts spend on repetitive tasks such as alert validation, enrichment, and investigation.

This aligns closely with the operational priorities reported by respondents, where reducing false positives and automating Tier-1 tasks were among the most frequently cited goals for the next 12 months. In practice, AI appears to be delivering incremental improvements in SOC efficiency rather than radical automation.

However, the results also highlight an important point: **the presence of AI capabilities does not necessarily translate into operational maturity yet.** Many organizations that already use anomaly detection or automated playbooks still report a significant number of alerts as well as investigation workload. This suggests that AI is often introduced as one component of a broader automation strategy rather than as a complete solution to SOC challenges.

These early improvements, however, are often incremental. **The survey results show that while AI can reduce investigation workloads, organizations still face structural challenges that limit how far automation can be operationalized.**

2 Barriers to Operationalizing AI

Despite growing interest and early adoption, several barriers continue to slow the operationalization of AI in security operations.

One of the most frequently cited challenges relates to **trust and accountability** (half of the respondents). Many organizations remain cautious about allowing automated systems to make security decisions without human oversight, particularly when those decisions may affect containment actions, incident prioritization, or customer environments. Concerns around explainability and auditability are particularly strong in European organizations operating under increasingly strict regulatory frameworks.

Several barriers slowing AI adoption are not technological but organizational. Budget constraints and competing priorities were each cited by more than 40% of respondents as factors delaying AI initiatives.

Integration complexity is another barrier. SOC environments often rely on a diverse set of tools, telemetry sources, and workflows. Introducing AI capabilities into this ecosystem requires integration across SIEM, EDR, threat intelligence platforms, and ticketing systems, which can create additional operational overhead.

Regulatory uncertainty also plays a role, as we have covered above. While some organizations view European regulatory frameworks as drivers for automation and improved monitoring capabilities, others report that evolving regulations - particularly around AI governance and data handling - introduce additional complexity when deploying new technologies.

Together, these factors contribute to uneven levels of AI maturity across SOC environments.

3 Expanding Detection Without Expanding Noise

One of the most interesting patterns emerging from the survey is a paradox faced by many SOC teams. On one hand, respondents report deliberately limiting detection rules or telemetry sources in order to control alert noise and maintain manageable workloads. On the other hand, many also indicate that they would enable broader telemetry - such as full EDR visibility, network anomaly detection, and identity analytics - if alert volume were not a constraint.

This suggests that operational capacity, rather than detection capability, is often the limiting factor in modern SOC environments.

AI-driven automation may play an important role in resolving this tension. By improving alert prioritization and reducing investigation overhead, AI has the potential to allow organizations to expand detection coverage without overwhelming analysts.

In this sense, AI may not only reduce analyst workload but also enable organizations to expand detection coverage without overwhelming SOC teams.

4 The Next Phase of Security Operations

Looking ahead, organizations overwhelmingly expect AI usage in the SOC to grow. More than half of respondents anticipate a moderate increase in AI adoption over the next 12 months, while one third expect a significant increase. Notably, no respondent indicated that AI usage would decrease.

This trajectory suggests that AI capabilities will increasingly become embedded within core SOC workflows rather than existing as separate experimental tools.

As automation improves triage and investigation efficiency, many organizations may also gain the operational capacity to invest more heavily in proactive security practices such as threat hunting, detection engineering, and security analytics.

In this sense, AI may play a role not only in improving operational efficiency but also in enabling a shift in how security teams allocate their time: **from reactive alert handling toward more proactive detection and security engineering activities**.

Ultimately, the findings of this research point toward a gradual but meaningful evolution of the SOC. AI will reshape the work of analysts, becoming an operational layer that augments human expertise, helping security teams manage growing volumes of telemetry and increasingly complex environments.

The next generation of security operations will likely combine human analysis, automated workflows, proactive practices like autonomous threat hunting , and AI-assisted decision-making to create SOC environments that are both more scalable and more resilient.

METHODOLOGY & DEMOGRAPHICS

This report is based on an online survey conducted between the months of February and March (2026). The objective of this survey was to collect insights from cybersecurity professionals in the Security Operations function about their views on the current state of AI in this space, as well as its future adoption.

The survey was designed based on prior qualitative interviews with a small number of practitioners, and included multiple choice, ranges and numeric questions, as well as open-ended ones for additional context on specific topics.

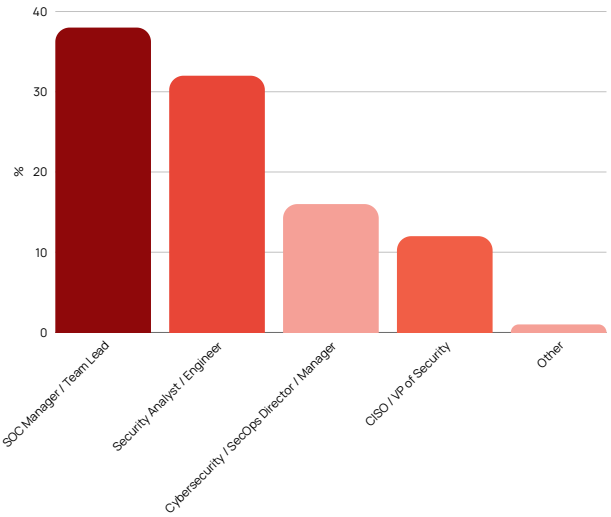
The questionnaire was completely anonymous to ensure data confidentiality, as no personally identifiable information was requested as part of the survey.

Participants were invited to participate directly, ensuring their profile was compatible with the theme of the research. All participants work in Europe.

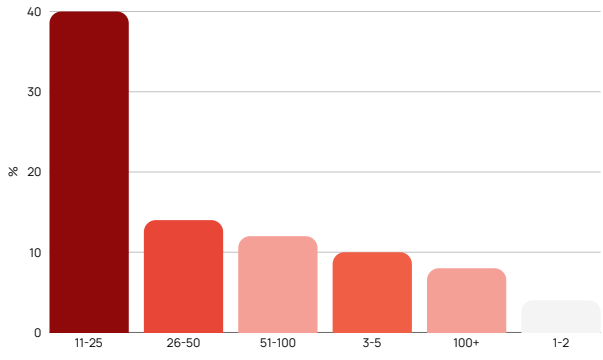
Only the answers from those that completed the whole questionnaire were considered for the final research. Some questions have not been included in the final report.

The research is therefore based on self-reported data and may include biases. Participants were not compensated for this survey.

What best describes your current job role?



How large is your SOC / security-operations team (including outsourced staff)?



ABOUT BRIDGERWISE

BridgerWise Research was founded to bridge the gap between cybersecurity innovation and strategic business decision-making in Europe.

We provide investors, vendors, and enterprise buyers with the market intelligence they need to navigate one of the world's most dynamic and complex technology sectors.

Our research combines deep technical understanding with commercial acumen, delivering insights that drive confident investment and procurement decisions.

Visit **research.bridgerwise.com** for more information.

ACKNOWLEDGEMENTS

We want to thank the support received from **Marcel Velica**, **Almog Ohayon** (TandemTrace), and the members of **BridgerWise's CISO Advisory Network.**