VECTRA

REPORT

# 2024 State of Threat Detection and Response:

## The Defenders' Dilemma

# Executive Summary

In this independent global research study, we interviewed 2,000 cybersecurity professionals who are involved in security with their organization or influence decisions on security. The purpose of the research is to gain an in-depth understanding about the challenges their organizations face each day when detecting, investigating, and responding to cyber attacks. To do this, the interviews included responses from security engineers, security analysts, security operations center (SOC) leaders, CISOs and other security team members that work in organizations with at least 1,000 employees based in APAC, North America, Europe, or the Middle East.

The data presented provides insight into current threat detection, investigation and response practices. This includes uncovering how effective and efficient technology is working to help SOCs stop attacks, what needs improvement, details about SOC workload, AI adoption and where desired outcomes are or aren't being met. This report also references additional data that was previously presented in the 2023 State of Threat Detection Report to showcase how the areas covered are improving, staying the same, or compounding further.

# What we conclude:

**No change, no change.** The promise of consolidation and platformization has yet to take hold as 71% of respondents have more than 10 detection and response tools in place, 45% have more than 20 tools, and 98% still rely on SIEM — begging the question: does the SOC have a threat detection problem, or an attack signal problem? No doubt, tools and SIEM have proven effective at detecting potential threats — alerting thousands per day, but are they effective at delivering the SOC an accurate attack signal? This research indicates the answer is "No."

More SOC practitioners believe they are losing the battle detecting and prioritizing real threats. SOC practitioners cite a growing dissatisfaction with the tools they currently have in place. Often, their security stack contains too many tools that are siloed and increase SOC workload rather than reduce it. Moreover, practitioners cite an increasing distrust of vendors, believing their tools can be more of a hindrance than help in spotting real attacks. Alert noise and false positives remain top challenges, and practitioners are disillusioned with vendors who they feel flood them with pointless alerts to avoid responsibility for a breach.

SOC practitioners exhibit a sense of optimism around the promise of AI. Nearly all SOC practitioners (97%) have adopted AI tools and 85% say their level of investment and use of AI has increased in the last year, which has had a positive impact on their ability to identify and deal with threats.

The data shows that practitioners clearly see how AI-powered threat detection, investigation and response tools are helping. In fact, many are already experiencing positive outcomes from AI by way of reduced workloads, feelings of burnout and tool sprawl brought on by legacy approaches. As many practitioners take steps toward an AI-powered SOC, the hope is that current frustrations will ease as siloed legacy tools are replaced by AI-powered tools capable of delivering an accurate attack signal.

# Key Findings

VECTRA


Nearly three-quarters (71%) of SOC practitioners worry every week they will miss a real attack buried in a flood of alerts.


62% of SOC practitioners say security vendors flood them with pointless alerts to avoid responsibility for a breach.


More than half of SOC practitioners believe they cannot keep pace with the increasing number of security threats.


71% of SOC practitioners say vendors need to take more responsibility for failing to stop a breach.


SOC teams receive an average of 3,832 alerts per day, 62% of them are ignored.


50% of SOC practitioners say their security tools are more hindrance than help in spotting real attacks.


55% say more effective security tools would help ease their SOC workload.


89% of SOC practitioners will be using more AI-powered tools over the next year to replace legacy threat detection and response.


75% of SOC practitioners say AI has reduced their workload in the past 12 months.

VECTRA

# Table of Contents



SECTION 1

# Can SOC teams keep pace with attacks?

# Keeping pace with the increasing amount of security threats means security practitioners need to be confident in their defenses.

They need to know that the right resources are in place — both by way of tools and staff to stop and respond to threats that enter their environment. Without a high level of confidence in either area, attackers gain an advantage.

**64%** 64% of security practitioners say they have the right number of analysts in their SOC.

**71%** Nearly three-quarters (71%) of SOC practitioners worry every week they will miss a real attack buried in a flood of alerts.

↓ Down from 97% in 2023

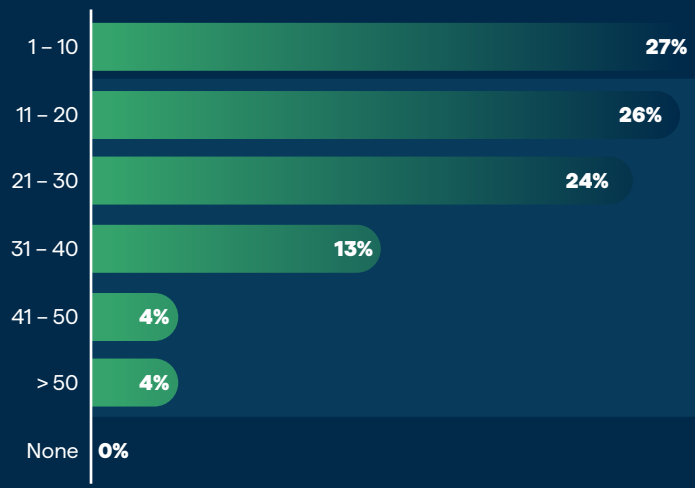
**51%** 51% of SOC practitioners believe they cannot keep pace with the increasing number of security threats.

↑ Up from 35% in 2023

Overall, SOC practitioners are more confident in their defenses than a year ago, in fact the number of practitioners who worry they'll miss or overlook a malicious true positive event because it was buried under a flood of security alerts (71%) is down 26% from 2023 when almost all practitioners (97%) had this concern. In addition, while 51% of respondents still believe it's likely that their environment is already compromised — that number is also down from 71% in 2023. With SOC confidence trending in the right direction, why do many feel they're still losing the battle against real threats? Is it the number of tools they have to manage, the constant alerts and noise, or perhaps a lack of trust in vendors?

To zero in on tools, one of the challenges SOCs are up against is the number of tools in their security stack being used to detect, prioritize and stop threats. In fact, 71% of SOC practitioners have more than 10 tools in place and 45% have more than 20 tools.

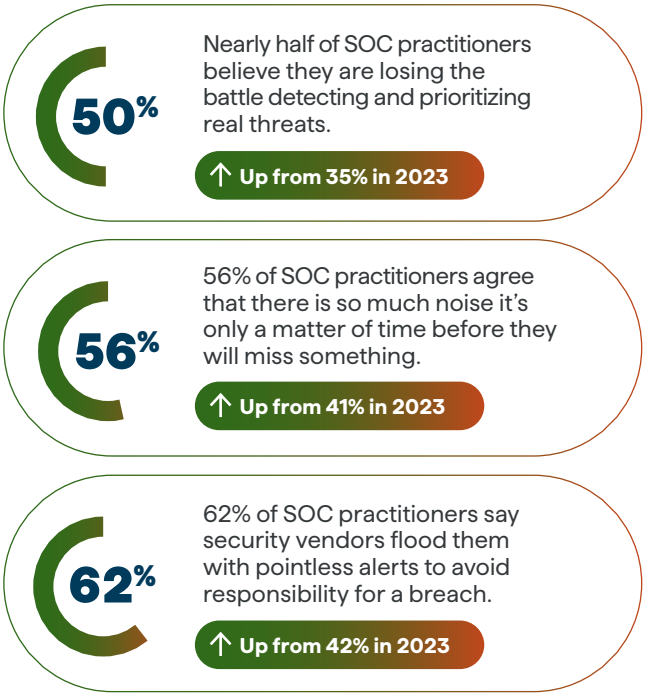
## How many tools, if any, are you using to help you detect, prioritize, and stop threats?




**71% of SOC practitioners have more than 10 tools in place to detect, prioritize and respond to attacks. 45% have more than 20 tools.**

**71%**

This could be the result of security teams attempting to solve for exposure gaps from expanding hybrid attack surfaces (65% currently defend hybrid environments), emerging attacker methods and any new security use cases that regularly arise. It could also be from a lack of tool consolidation yet to take hold in many of today's SOCs. How do these landscape trends translate to the overall effectiveness of their current tools?




The findings show that SOC practitioners are concerned that the tools they use will eventually cause them to miss an important alert, and that security vendors in general are part of the problem. Practitioners know that their tools will alert on thousands of events whether malicious or not, but there's no way for every alert to be addressed. This puts practitioners in a tough position because they don't have time to address each and every alert; however, they can't claim their tools didn't alert them when they miss a true positive event that was overlooked. Are they losing trust? According to the research, nearly half (47%) of practitioners do not trust their tools to work the way they need them to work, while 54% say the tools they work with actually increase the SOC workload instead of reduce it.

Does the lack of confidence and trust in tools have practitioners seeking alternatives? The study shows that 62% of teams have either recently adopted or are exploring extended detection and response (XDR) solutions. Now expressing a lack of confidence around their current threat detection tools, and the skepticism they have towards vendors — 57% of SOC practitioners say they are tired of empty promises from vendors and how they sell products that require constant tuning — security professionals are open to seeking tools that match the current demands inside the SOC.

## Is this the beginning of a shift?

## Takeaway

Talented SOC teams with confidence in their ability as defenders feel limited by the tools and lack of threat signal to help them identify real threats. There's an increased sense that they can't keep pace with attacks while threats remain buried in a flood of noise and pointless alerts, leaving them frustrated with the approach from vendors.

SECTION 2

# How do SOC teams feel about their tools?

# How is the decreasing confidence security practitioners have in their current tools impacting the overall SOC competence seen across the industry?

We just saw how many tools teams are using to detect, prioritize and respond to attacks (71% have more than 10 tools, while 45% have over 20 tools), and looking further into the frustrations practitioners have when operating with their current stack shows how existing tools are creating additional challenges rather than helping SOCs effectively secure their organization. One of the main challenges being that over three-fourths (77%) of SOC teams say they push aside important security tasks more than twice a week so they can tune, monitor, and maintain existing security tools. Some teams even say this is a daily occurrence.

50% of SOC practitioners say their security tools are more hindrance than help spotting real attacks.

↑ Up from 40% in 2023

57% of SOC practitioners say jumping between security tools is wasting hours of their time every week.

↑ Up from 40% in 2023

60% of SOC practitioners say a lot of our security tools are bought as a "box ticking" exercise for compliance.

↑ Up from 39% in 2023

The increase in tool dissatisfaction isn't just targeted at the tools themselves, but also at security vendors. SOC practitioners aren't afraid to call out vendors who they feel are selling alerts to limit accountability when an attack transpires or simply just create too much noise that causes more work for analysts.

60% of SOC practitioners say vendors are selling threat detection tools that create too much noise and too many alerts.

↑ Up from 39% in 2023

81% of SOC practitioners spend more than 2 hours per day digging through / triaging security events and alerts.

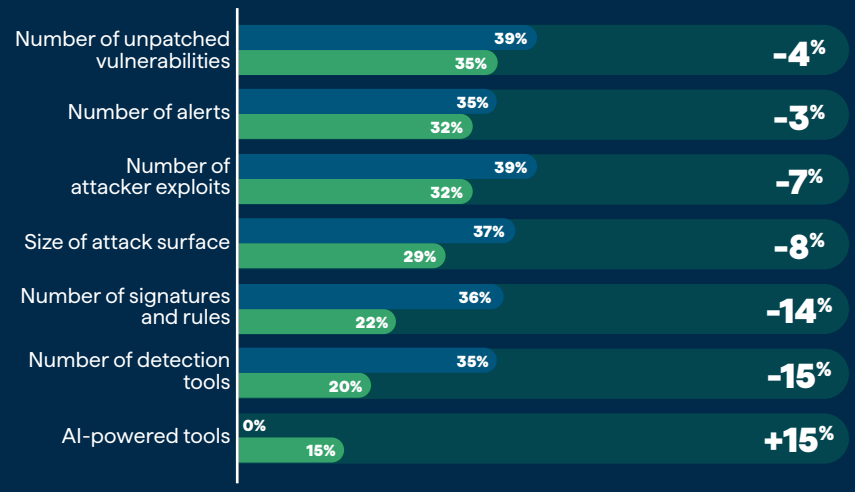
↓ Down from 83% in 2023

71% of SOC practitioners say vendors need to take more responsibility for failing to stop a breach.

↑ Up from 43% in 2023

**When evaluating the data to see what is most negatively impacting practitioners' ability to identify and deal with threats, it's not just tools that present a challenge.** In fact, practitioners place blame squarely on the fundamentals, where tools are a piece of, but not the whole story. Bad hygiene, alert noise and attacker exploits are all top causes for concern. Attack surface size also plays a role. Interestingly though, concerns around all of these areas are down slightly compared to a year ago even with a growing sense that vendors need to take more responsibility. Maybe this is a result of practitioners continuing to adapt as they gain experience addressing challenges across always-changing hybrid environments? However, when it comes to vendors, they might simply be fed up with a lack of a partnership they're experiencing to help solve security challenges across the board? Take alert noise as an example — a widely known distraction that pulls analysts away from addressing real threats, yet vendors continue to create tools that generate an unmanageable amount of alerts.

## To what extent, if any, have the following negatively impacted your ability to identify and deal with threats?



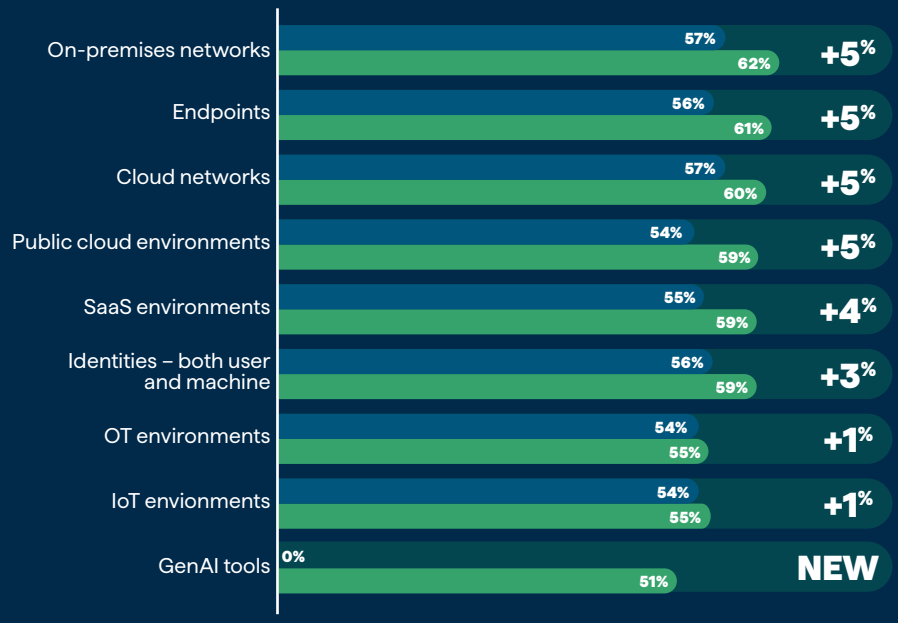

2023 Research Data

2024 Research Data

And in terms of having the correct information about each attack surface — practitioners express that visibility across hybrid environments is improving in small amounts as well.

In fact, 77% of practitioners feel their current suite of tools provides adequate protection against today's growing hybrid attack landscape.

## How would you rate your visibility into the following environments?

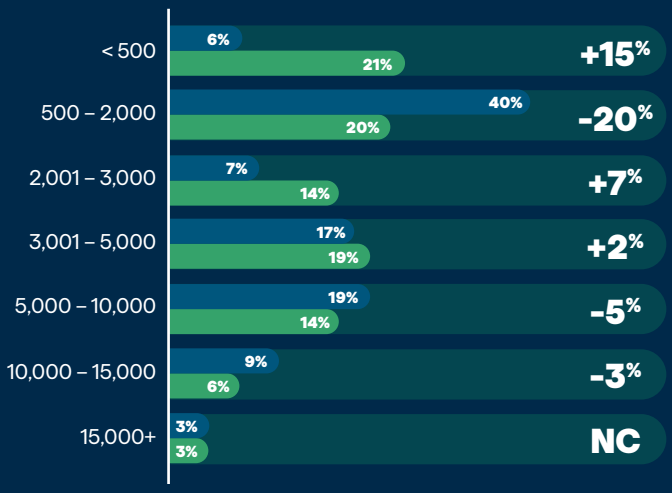



2023 Research Data

2024 Research Data

**Even with evidence that certain areas in the SOC are trending in a positive direction, SOC practitioners are still operating under conditions with unmanageable alert volume**. While down from last year, the average number of alerts teams receive is still too high for them to address on a daily basis — meaning there are plenty of detections that could possibly be signaling a true threat or attack, that go unaddressed simply because there's not enough time or the right tooling to help analysts prioritize them. Practitioners state that realistically, they are still only able to deal with 38% of the alerts they receive, while they would classify 16% of them as "real attacks."

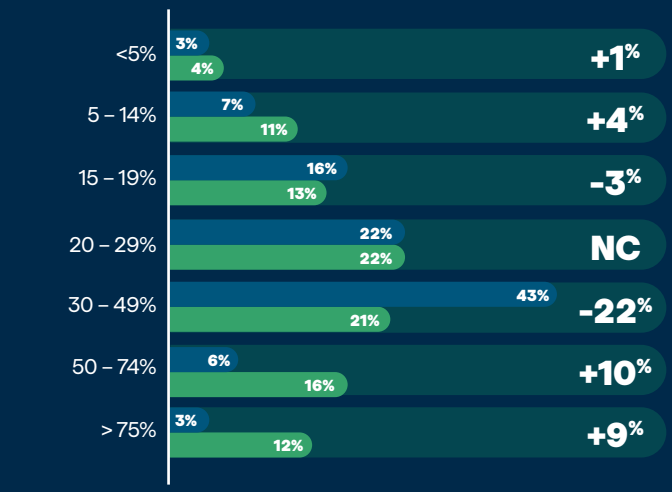
## Typically, how many security alerts per day does your SOC team receive?




2024 Mean: **3832**

2023 Mean: **4484**

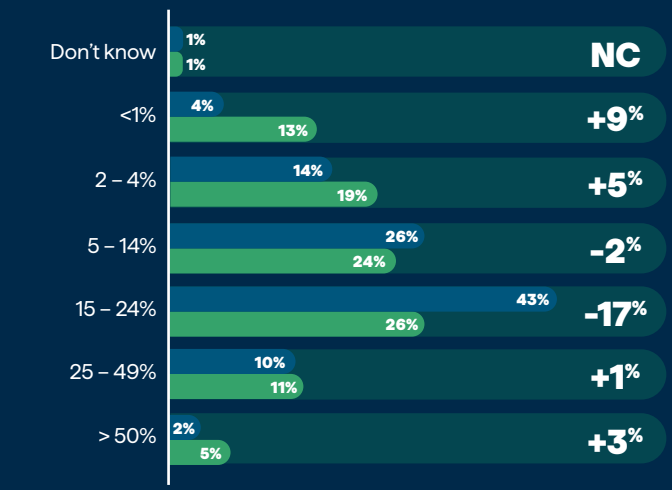
## Realistically, what percentage of these security alerts can you deal with per day?




2024 Mean: **38%**

2023 Mean: **32%**

## What percentage of the security alerts you receive are "real attacks"?




2024 Mean: **16%**

2023 Mean: **16%**

2023 Research Data

2024 Research Data

Seeing year-over-year data remain the same when it comes to alert accuracy (16% of alerts being real attacks) is also an indicator that alert fidelity or the threat signal SOCs are getting from their tools isn't improving. A trend that's also reflected in the sentiment among practitioners who utilize SIEM (98% of respondents) for threat detection and response. Where they cited the top three ways to improve alert volume, workload, and accuracy revolve around the lack of signal.

## What areas of SIEM could be improved?

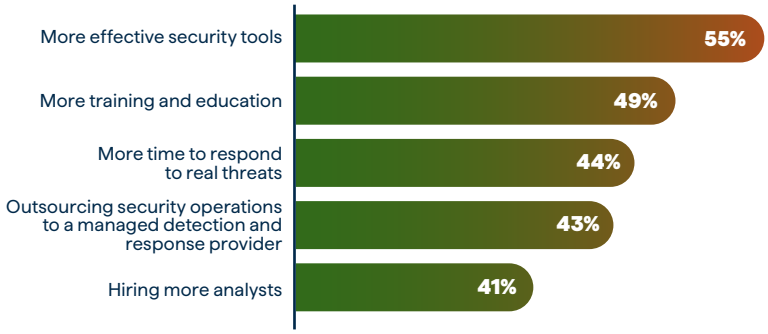
58% report the quality of data going into SIEM

53% report threat signal efficacy

46% report time required to manage

With data highlighting dissatisfaction surrounding current security tools, vendor trust, signal accuracy, and expressing slight improvements in visibility and alert volume — what do SOCs feel would be most helpful to ease their workload?

## What scenarios would best help ease the workload in your SOC?




Confidence in their defense ability, skills, and teams — ensuring SOC competence according to practitioners is rooted in tools, training, and time.

**Are they planning to fill these gaps, and where are they looking?**

## Takeaway

Security practitioners are no longer willing to accept that their tools are holding them back. They are tired of jumping between tools, wasting time on alerts, and want vendors to own more accountability when incidents occur. Usage of legacy technology remains high among SOCs, but they want technology partners who can help prioritize real attacks.

SECTION 3

# SOC teams are optimistic about AI, but vendors have work to do

## As previously stated, well over half (62%) of organizations are either exploring or have adopted XDR — solutions heavily focused on the use of AI to detect and respond to threats.

The data also shows that AI adoption and use in the SOC is expanding as practitioners gain optimism and trust around the technology.

85% of SOC practitioners say their level of investment and use of AI has increased in the last year.

67% of SOC practitioners say AI has had a positive impact on their ability to identify and deal with threats.

89% of SOC practitioners will be using more AI-powered tools over the next year to replace legacy threat detection and response.

In addition to these figures, 97% of SOC practitioners reported that they have adopted AI, with 73% saying the number of AI-powered security tools they use has increased significantly over the past year. Gaining trust and optimism could be a result of SOC practitioners experiencing real-world outcomes and value with tools utilizing AI versus the lack of trust in other tools.

75% of SOC practitioners say AI has reduced their workload in the past 12 months.

73% of SOC practitioners say AI has reduced feelings of burnout in the past 12 months.

75% of SOC practitioners say AI has reduced the number of tools they use for threat detection and response.

## Interestingly, data from the 2023 report shared that 67% of SOC practitioners were considering leaving their job at the time due to burnout they were experiencing.

The fact that SOCs are experiencing reduced workload and feelings of burnout could be a good sign for the increasing cybersecurity workforce gap that has reportedly reached 4.8 million workers[1]. The sentiment around AI also seems to be heading in a more positive direction than the ones SOC practitioners have for legacy tools that many feel are more of a hindrance than help.

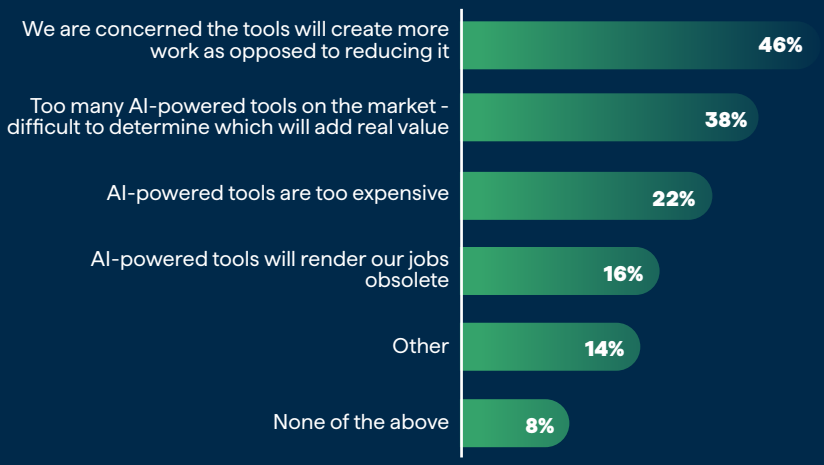
[1]ISC2 Research: 2024 Cybersecurity Workforce Study.

With that in mind, of the 97% of practitioners who have adopted AI, the number who invest to a greater extent is much smaller — currently sitting at 39%.

Certainly, a much smaller portion, however, it does show that security organizations are actively investing in and deploying AI in their security stack. In fact, 89% say they will be using more AI-powered tools over the next year to replace legacy threat detection and response, yet 61% have not yet invested in a broad-based AI strategy.

**Do practitioners have concerns or reservations that are holding up AI being fully operationalized in the SOC?**

## Why is deployment and implementation not happening in your organization?

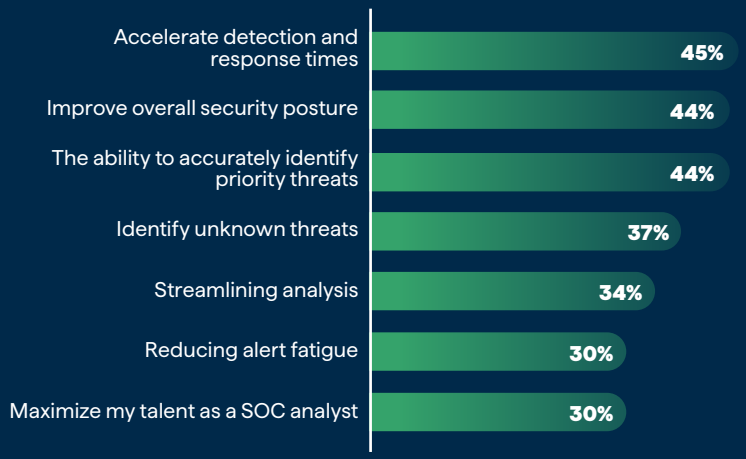



While only a small amount of practitioners have concerns related to cost or the idea that AI could potentially replace their jobs, almost half of practitioners (46%) expressed concerns that adding another tool will create more work.

Perhaps understandable considering the overall sentiment expressed around their legacy tools doing exactly that. Practitioners recognize that they have gaps that current tools struggle to address. They also recognize that the right AI solution can deliver threat signal efficacy to help accurately identify and respond to threats, reduce workloads, and even replace legacy threat detection and response tools, however, they want to know which AI solutions will add real value.

**What specifically do SOC practitioners see as the most important benefits of AI-powered security tools?**

**Which of the following, if any, do you think are the most important benefits AI-powered security tools offer to SOC teams?**




Shown here, practitioners see value specifically in how AI can improve efficiency, efficacy, and posture.

Practitioners want to be sure that the AI solutions they deploy can deliver accurate threat signal that will speed up detection and response times. A reasonable ask considering that 45% of SOC teams already have over 20 tools to manage. And while practitioners see how AI can reduce the number of tools (75% reported that to be the case), it still takes strategy, planning and resources to rip and replace solutions. To move beyond the disconnect between SOCs and the tools they use, vendors will have to work harder in order to earn the trust of practitioners who are struggling with threat detection and response. Even if the technology problem can be greatly improved with AI, it's going to take the people behind that technology to earn back trust.

## Takeaway

SOCs are investing in AI-powered tools and will continue to use more over the next year to replace legacy threat detection and response. There are some reservations around adding new tools, which comes from past experiences where vendors don't deliver on promises. Practitioners want to be certain about the value that AI will add, but express optimism around attack signal accuracy that solutions utilizing AI can provide.


# Conclusion

## Diving into this year's data alongside the findings from a year ago provide helpful insight about the specific areas limiting effective threat detection and response.

We now know more about where security practitioners feel confident in their defenses, and as we saw across this year's data — what areas they feel need improvement. Interestingly, the sentiment across the different disciplines of security practitioners whether at the CISO level or those who live and breathe day-to-day life in the SOC didn't show much of a discrepancy among responses. So, what is the current state of threat detection and response?

In some areas, little has changed. Things like alert volume remain unmanageable, but practitioners exude more confidence in their defenses overall. However, over half of the respondents feel they can't keep pace with today's attacks even though they feel they have the right number of analysts available in the SOC. And that's where the disconnect begins to surface. The data clearly suggests that the tools being used for threat detection and response along with the vendors who sell them aren't holding up their end of the deal. Tools are more of a hindrance than help in many cases, while vendors continue to deliver a flood of "pointless alerts" and in the eyes of practitioners simply "need to take more responsibility for failing to stop a breach." Practitioners are ultimately held responsible for the security of their organization but feel that their vendor partners don't have their back even though this scenario isn't necessarily by design.

Reading between the disconnect presents an opportunity for vendors to improve upon tools and deliver a more effective integrated attack signal. One that helps SOCs know where they should be spending time and resources to address real threats. In addition, there's room for vendors to work more closely with security teams to help them address threat detection challenges. There's also an opportunity for practitioners to accelerate detection and response times by incorporating newer methods, which many are already doing with the growing use of AI in their stack.

Looking ahead, tracking AI adoption and usage across SOC teams will continue to provide key insights about how emerging threats are addressed. As we saw, a high majority (89%) of the practitioners surveyed said they will be using more AI-powered tools over the next year to replace legacy threat detection and response. A broad statement yet it will be interesting to see which areas are either replaced or improved with the use of AI as adoption increases. Teams shared how they believe AI delivers an attack signal that helps identify and prioritize threats, accelerate response times, and reduce alert fatigue, however, removing the existing disconnect may come down to how security vendors work to add value beyond just the technologies they sell.

# Recommendations

# Vectra AI recommendations based on findings

## 1 Move away from siloed tools and prioritize an integrated attack signal

As we saw in the research, there are too many confident teams with the right amount of skill and expertise that still can't keep pace with attacks. 71% of practitioners have over ten tools to detect, prioritize, and respond to attacks while 98% of teams still utilize SIEM for the same purpose. This suggests that there are too many potentially siloed signals across enterprise SOCs. Utilizing tools such as XDR enables an integrated attack signal alongside legacy technologies such as SIEM or on its own across hybrid attack surfaces. This is a seamless way to improve the quality of data that the SOC receives from a more accurate signal. This approach also removes the exposure gaps, latency, and noise that make it so difficult for to prioritize attacks.

## 2 As an industry, we need to hold vendors more accountable – and vendors need to take more responsibility

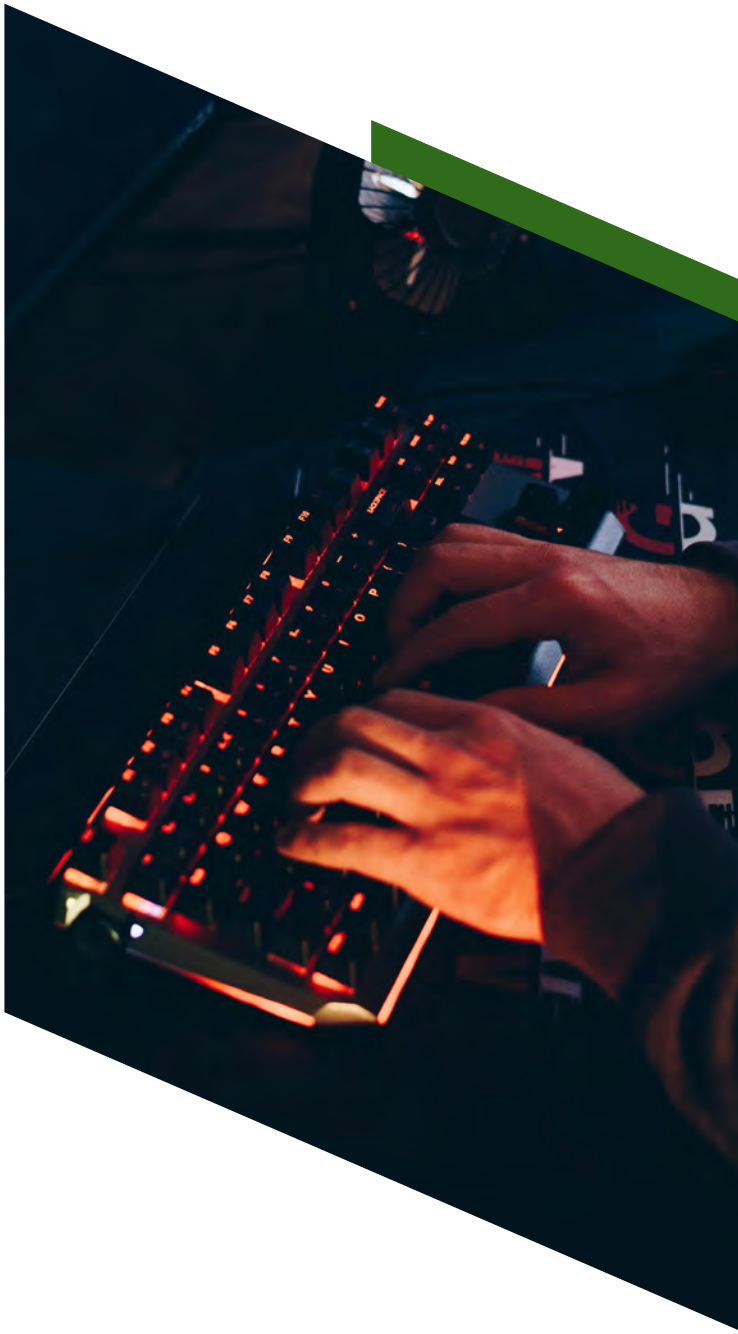
Practitioners buried in alert noise are in a difficult position. There's not enough time or resources to address all of them and it's the practitioners who are on the hook if a real attack gets overlooked. As we saw in the data, practitioners stated that they are only able to realistically deal with 38% of alerts and that 16% of the alerts they receive are real attacks (same as a year ago). Alert fidelity isn't improving, and practitioners are right — vendors should own more responsibility. It doesn't help practitioners when tools alert on "everything" because it just sets them up to eventually miss something important. Attack signal accuracy with a prioritized view of what needs attention can help SOCs get away from manual alert triage so they can focus on defending against critical activity. Having to address 3,832 alerts on average each day isn't helping practitioners focus on what's urgent. Rather, ask vendors how they use AI to help prioritize those alerts for you, so critical events aren't missed and teams aren't constantly swimming through alerts and noise.

## 3 Understand exactly what outcomes you want delivered from your AI solutions

89% of practitioners state they will be using more AI-powered tools over the next year to replace legacy threat detection and response. However, there is some hesitation to add new tools because current tools haven't delivered. There's also concern because the market is saturated with tools claiming "AI" which makes it difficult to know which will add real value. One way to cut through the noise is to know exactly what you want from your AI solution up front. For threat detection and response, this could be determining that your XDR is equipped with a signal that truly arms defenders. Does it integrate across all your hybrid attack surfaces and automatically analyze attacker behavior? Does it deliver a threat urgency score and feed that data into a workflow that makes it easy for the SOC to digest and utilize? Does it have manual, automated, and managed response actions that make it easy to stop attacks in progress? These callouts barely scratch the surface of what AI can do from a threat detection and response standpoint, but focusing on these areas will help go beyond the hype and find the right AI tool.

# About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai



# Methodology

This report is based on a June 2024 study commissioned by Vectra AI and carried out by Sapio Research. The study was conducted among 2,000 individuals involved in cybersecurity with their organizations or who influence decisions on cybersecurity, working in organizations with at least 1,000 employees and based in North America (500), Europe (850), APAC (400), and the Middle East (250).

For more information please contact us at info@vectra.ai. Refer to **vectra.ai** for more information.