VECTRA

GLOBAL REPORT

2023 State of Threat Detection

The Defenders' Dilemma

Executive Summary

Today's security operations center (SOC) teams are tasked with protecting the organization from progressively more sophisticated, fast-paced hybrid cyberattacks.

Detecting, investigating and stopping advanced cyberattacks at speed and scale is becoming increasingly unsustainable with the complexity of technology SOC teams have at their disposal. A perfect storm of an ever-expanding attack surface, highly evasive and emerging attacker methods, and an increasing SOC analyst workload is resulting in a vicious spiral of more for SOC teams.

In this independent global study of 2,000 SOC analysts, we dive headfirst into the challenges SOC analysts face.

What we conclude: threat detection is fundamentally broken.

This report uncovers a major disconnect between SOC analysts' effectiveness and threat detection tool efficacy. While many SOC analysts believe their tools are effective, a number of concerned analysts admit the same technology hampers their ability to effectively defend the organization from cyberattacks.

Alert noise and time spent on alert triage are increasing. Detection blind spots and false positives are growing, and SOC analyst alert fatigue, burnout and turnover are at a tipping point. The industry remains at a 3.4 million person talent deficit, and all signs indicate it will only get worse.

With the stakes this high – and the demotivating, manual demands of work wearing SOC teams down – many analysts are considering leaving their roles or are "quiet quitting", adding to an already existing security skills gap and leaving remaining analysts at the company faced with even more work.

Today's threat detection and response is broken, and it's pushing humans to the brink. Is it time for organizations to rethink traditional industry approaches to threat detection and start holding vendors accountable for the efficacy of their signal? **This research indicates "yes" because attackers are winning.**

71%

Nearly three-quarters (71%) of analysts admit the organization they work in may have been compromised and they don't know about it yet.

97%

Most (97%) of analysts worry they'll miss a relevant security event because it was buried in a flood of security alerts.

67%

SOC teams receive an average of 4,484 alerts per day, and over two-thirds (67%) of them are ignored.

67%

67% of security analysts are considering or actively leaving their jobs, citing factors like stress, lack of leadership empathy and poor-quality security alerts.

41%

41% agree that security vendors flood analysts with pointless alerts because they are afraid of not flagging a breach.

63%

70%

66%

A majority of SOC analysts say the size of their organization's attack surface (63%), the number of security tools (70%) and alerts (66%) they manage have significantly increased in the past three years.

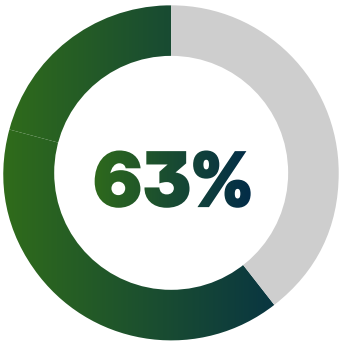
VECTRA

SECTION ONE

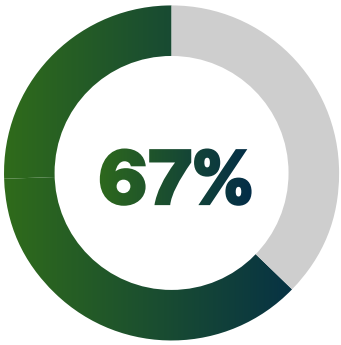
More Attack Surfaces, More Alerts, More Costs

SOC analysts sit on the front lines in the ongoing battle against cyberattacks.

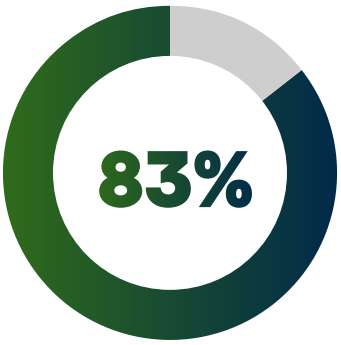
They have a critical job: to effectively detect, investigate and respond to threats as quickly and efficiently as possible. The longer they leave a potential adversary inside the corporate network, the more lasting damage that adversary could cause. But defenders are increasingly challenged by three core factors: the size of the organization's attack surface, the number of security alerts they receive, and their increasing workloads. This "spiral of more" threatens defenders' ability to be successful at their job.



Nearly two-thirds (63%) of respondents say the size of their attack surface has increased in the past three years



Security analysts are unable to deal with over two-thirds (67%) of the daily alerts they receive



83% of these alerts are false positives and not worth their time

Nearly two-thirds (63%) of respondents say the size of their attack surface has increased in the past three years, while 27% say it has increased significantly. 61% of analysts also point to surging volumes of vulnerabilities impacting their organization during this period. Investments in digital and cloud-based technologies during the pandemic are behind much of this expansion. But while digitalization has helped to drive productivity and improve customer experience, it also provides attackers with more opportunities to target an organization. This is especially true when in-house skills fail to keep pace with digital investments. There's increasing demand for analysts to uplevel their cloud knowledge, as 61% of respondents admit they don't have the necessary skillset and expertise to defend the organization's expanding cloud footprint.

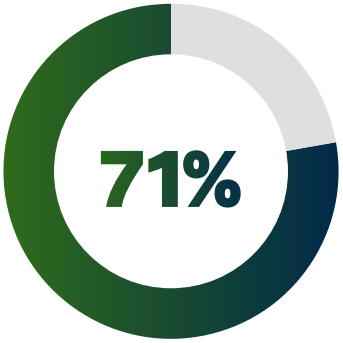
At the same time, existing tools are failing to effectively prioritize events for further investigation, increasing the workload on already stretched teams. **SOC teams receive 4,484 alerts each day on average**. Analysts spend nearly 3 hours (2.7) each day manually triaging alerts, a figure rising to more than 4 hours a day for 27% of respondents.

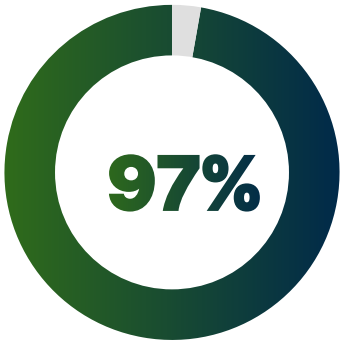
Manual alert triage costs organizations approximately $3.3bn annually in the US alone[1]. On average, **security analysts are unable to deal with over two-thirds (67%) of the daily alerts they receive**. What's more, they say **83% of these alerts are false positives and not worth their time**. This barrage of alerts has more than an adverse effect on analyst productivity. Hidden is a sea of alerts, which allows attackers to easily blend in and slip under the radar by masking themselves in "normal" activity. This problem shows no signs of stopping, with two-thirds (66%) of respondents saying the number of alerts they receive is increasing, and increasing alerts means rising costs.

[1]Calculated based on 115,573 security analysts earning an average salary of $48 per hour, and spending 83% of their 2.72hrs (2.26 hours based on 83% of alerts being benign) a day triaging false security alerts for 260 days a year.

SECTION TWO

More Tools, More Blind Spots, More Burnout





71% of SOC analysts admit the organization they work in has likely been compromised and they don't know about it yet – while 84% think it's at least possible. In other words, with the tools they have today, analysts do not have the confidence to say they can spot the signs of an attack in progress and protect their organization. This is at odds with most analysts who currently claim tools are effective, suggesting a contradiction that brings organizations' approaches to security into question.

At the same time, **nearly all (97%) SOC analysts worry about missing a relevant security event because it's buried under a flood of alerts**, while almost half (46%) worry about this every day. A combination of blind spots and high-volume false positives means that enterprises and their SOC teams are struggling to contain cyber risk. Without visibility across the entire IT infrastructure, from OT to endpoints and beyond into cloud environments, organizations simply won't be able to spot even the most common signs of an attack such as lateral movement, privilege escalation or cloud account hijacking.

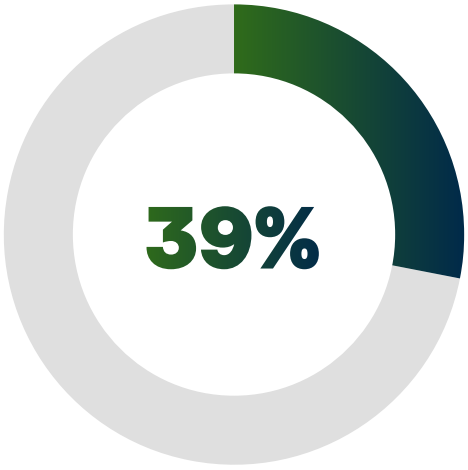
YET, THE VAST MAJORITY OF SOC ANALYSTS SURVEYED DEEM THEIR TOOLS "EFFECTIVE" OVERALL:

Intrusion Detection Systems (IDS)	**91%**
Endpoint Detection and Response (EDR) tools	**90%**
Network Detection and Response (NDR) tools	**90%**
Extended Detection and Response (XDR) tools	**90%**
Security Information and Event Management (SIEM) tools	**91%**
Security Orchestration, Automation, and Response (SOAR) tools	**91%**
Cloud Security Posture Management (CSPM) tools	**91%**
Antivirus software	**91%**
Firewalls	**91%**

The data suggests a major disconnect between SOC analysts' attitudes about the tools they use to detect and respond to cyber-incidents, and their acknowledgment of security blind spots. While many analysts deem their technologies effective, they are still facing an increasing number of alerts, and go on to admit that the same tools mentioned above are adding to a lack of visibility and uncertainty, as well as alert overload.

THE CHALLENGE IS LAID BARE BY ADDITIONAL FINDINGS THAT SHOW ANALYSTS LACK COMPLETE VISIBILITY INTO THEIR IT ENVIRONMENTS. DESPITE SOC ANALYSTS' BELIEF THEIR TOOLS ARE "EFFECTIVE," THREE-QUARTERS CLAIM THEY DON'T HAVE FULL VISIBILITY INTO:

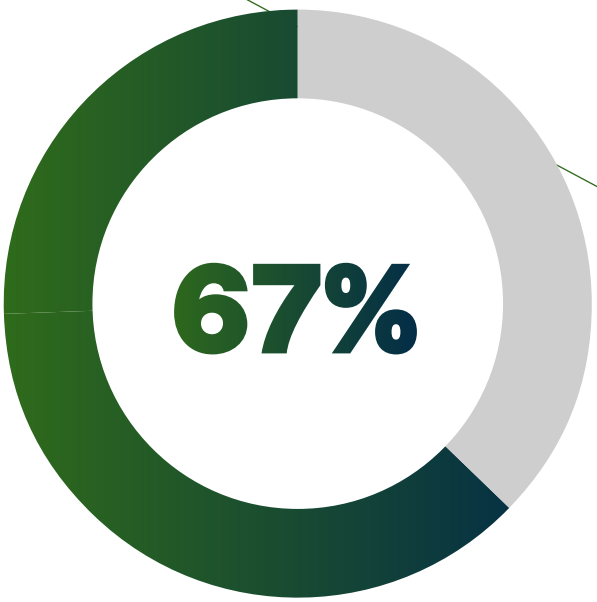
This shows SOC analyst expectations for their security tools are simply too low. By accepting that their security tools are effective as they are, SOC teams are setting themselves up to fail. Despite analyst's claims that tools are effective, a **significant proportion of the same analysts blame their tools for creating too much "noise" (39%)**. What's more, the sheer amount of noise generated by security alerts is having a very human cost on SOC analysts. Alert overload is pushing analysts out the door and exacerbating the security skills shortage.



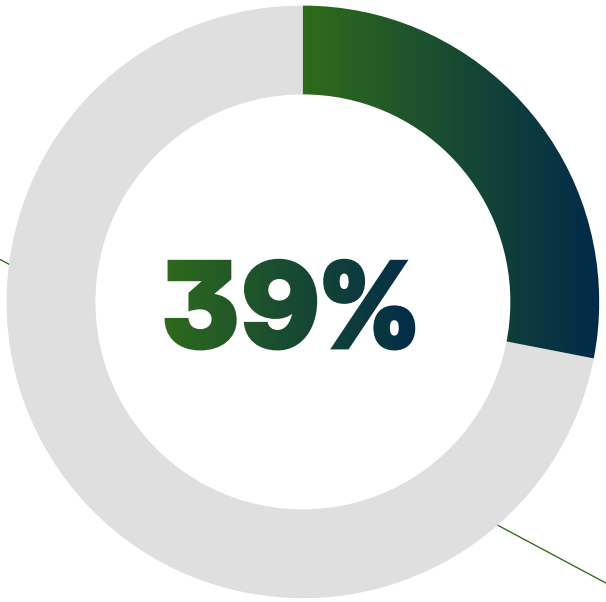
A significant proportion of the same analysts blame their tools for creating too much "noise" (39%)

The cybersecurity industry has been suffering from a major skills shortfall for years. Estimates put the shortage of workers globally at 3.4 million. The battle to attract and retain talent is becoming fiercer, and it is worsened by day-to-day stresses and frustrations that can be traced back to poor signal efficacy. That's bad news for organizations because it can create a vicious cycle of workplace stress and resignations that may be difficult to resolve.

No two security analysts are the same. But many enter the profession for similar reasons. Some want to "make a difference" (49%) and protect people from cyberattacks (48%). Others are drawn to cybersecurity for the intellectual challenge (43%) and the opportunity to proactively hunt for cyberthreats every day (47%), although these opportunities can be extinguished by manual processes, alert overload and poor tooling. There is also a significant number (49%) who simply want a solid income. But many analysts over-burdened by ineffective technology come to realize that there are easier ways to make similar sums.



Two-thirds (67%) are considering leaving or are actively leaving their jobs



Spending too much time sifting through poor quality alerts (39%)

Despite three-quarters (74%) of respondents claiming the job matches their expectations, **two-thirds (67%) are considering leaving or are actively leaving their jobs**. Of these, almost a quarter (24%) are looking for another analyst role, but a fifth (20%) are leaving the profession entirely. That should ring alarm bells for organizations. More than half (55%) of analysts claim they're so busy that they feel like they're doing the work of multiple people. What's more, 50% of security analysts are so burned out they are tempted to "quiet-quit." Analysts are clearly stretched, and the industry can't afford to see them leave the profession.

The fewer analysts there are to go around, the more stretched teams will be and the higher the stress levels and workload for those who stay. In turn, that could prompt even more individuals to change jobs or careers.

Many of the reasons analysts give for considering leaving their jobs can be linked to the problems highlighted above. They complain of **spending too much time sifting through poor quality alerts (39%)**, working long hours, and feeling "mind-numbingly" bored in the role (32%). All of which chimes with the problems of alert overload driven by poor tooling and manual processes. More than one-third of respondents also cite constant workplace stress (35%), burnout (34%) and the role's impact on their mental health (32%).

More than a third (35%) claim the organization's leadership simply doesn't understand security. This means that SOC teams may not always be given the right tools they need to do their jobs efficiently.

It's greatly concerning that over half (52%) of the industry professionals we spoke to believe that working in the security sector is not a viable long-term career option. AI and automation can only do so much. We still need a critical mass of security workers to interpret data, launch investigations, and take remedial actions based on the intelligence they are fed.

SECTION THREE

More Inefficiencies, More Ineffectiveness, More Breaches

This research indicates that SOC analysts believe the measure of effectiveness is based on whether or not a security tool flags a threat event and triggers an alert.

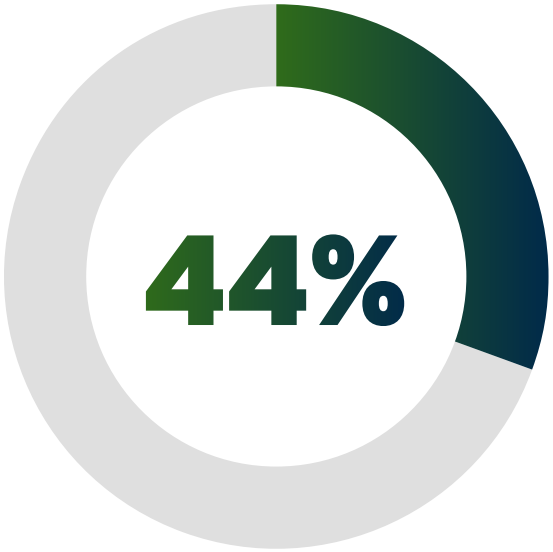
This needs to change. Without addressing the broken security model and redefining how we measure the effectiveness of security tools, the situation is only going to get worse as alert volumes increase.

The first step is changing how analysts measure effectiveness. Currently, most measure SOC maturity via factors like reduced downtime (65%), time to detect, investigate and respond (61%), breaches prevented (61%), and the number of tickets dealt with (60%). But it's debatable how useful prioritizing the continuous measurement of such metrics is if the organization is breached unknowingly on a continual basis.

As previously noted, 71% of security analysts admit the organization they work in has likely been compromised and they don't know about it yet – while 84% think it's at least possible. At the same time, nearly all (97%) SOC analysts worry about missing a relevant security event because it's buried under a flood of alerts, while almost half (46%) worry about this every day.

Clearly, SOC analysts have a confidence problem. These two findings alone beg the question: how confident is the SOC team when it comes to knowing when and where an attacker has compromised the organization the moment they become compromised? This research suggests the need for a Security Confidence Index (SCI) that assesses threat visibility, detection accuracy and analyst workload effectiveness.

Perhaps if a Security Confidence Index metric existed, organizations would hold their vendors more accountable for attack surface visibility, detection accuracy and analyst productivity. We are not there yet, because **less than half (44%) of respondents agree that vendors should take greater responsibility for alert signal accuracy**, while 41% believe alert overload is the norm because vendors are afraid of not flagging something that could turn out to be important.



Less than half (44%) of respondents agree that vendors should take greater responsibility for alert signal accuracy

Less than half (40%) of analysts say they're tired of vendors selling new products that increase alert volumes rather than improve threat efficacy. A similar proportion (39%) claim the tools they use are increasing the workload rather than reducing it.

Vendors aren't solely to blame though – the entire decision-making process must also be re-evaluated. Almost two in five (38%) claim that security tools are often purchased more as a box ticking exercise to meet compliance requirements. And nearly half (47%) wish that other IT team members would consult with them before investing in new products. Of the analysts considering leaving or actively leaving their role, a third (34%) claim they don't have the necessary tools to secure their organization. The industry as a whole needs to stop making the same mistakes and buying tools that hinder analysts and add to their workload.

Conclusion

We've seen in this report how a "spiral of more" is threatening to overwhelm SOC analysts. While threat actors have an ever-greater attack surface to target, and an increasing number of techniques to do so, defenders are struggling with excessive alert noise and IT complexity. As a result, they spend hours triaging alerts and still run the risk of missing legitimate attacks amidst the noise.

Although many analysts believe their tools are effective, they also admit to major visibility gaps. A majority even claim they've likely already been unaware of a breach. This can't continue. Many blame the tech vendors or a lack of consultation with security teams prior to tools being purchased. The stress and demotivation this creates is causing many to rethink their careers, which could have a devastating long-term impact.

Organizations must focus on the things they can control. This does not include the corporate cyberattack surface, which will continue to grow as digital investments are leveraged to advance productivity, innovation, and efficiency. Nor can SOC teams address the booming threat landscape: attackers will always look for new ways to outwit defenders.

However, what organizations can control are the signal and burnout challenges currently impacting SOC analysts. It's time to recognize that effective security in the SOC doesn't mean simply detecting possible threat events – it means accurately detecting and prioritizing real attacks. That's why organizations need to demand signal clarity from their security vendors. The more effective the attack signal, the more cyber-resilient, efficient and effective the SOC becomes.

Vectra AI Perspective

For the past decade, cyber security defense centered on what is known. Threat detection methodologies across people, processes and technology have relied heavily on signatures, anomalies, and rules to see and stop cyber criminals from infiltrating the organization and exfiltrating data. The problem with this approach is that it's broken. As enterprises shifted to hybrid and multi-cloud environments, embracing digital identities, digital supply chains, and ecosystems — security, risk, and compliance leaders, architects and analysts are continuously faced with more. More attack surface for attackers to exploit and infiltrate. More methods for attackers to evade defenses and progress laterally. More noise, complexity and hybrid cloud attacks and incidents

We call this the "spiral of more" and as organizations shift more applications and data to the cloud, the bigger the spiral becomes and the faster it accelerates, creating more challenges for SOC teams. Amid the spiral of more, threat detection and response has become more complex and less effective. The fact of the matter is that there are simply too many disparate, siloed tools creating too much detection noise for a SOC analyst to manage. To make matters worse, attackers thrive on noise because it makes it easier for them to infiltrate an organization, blend in and progress unseen. The measure of security tool effectiveness is NOT whether or not a tool detects and alerts a possible threat event. That only overwhelms analysts and puts them at risk of missing something important.

SOC teams spend an inordinate amount of time on manual mundane tasks like maintaining signatures, tuning detection rules, and triaging hundreds if not thousands of alerts a day only to find they've spent hours chasing false positive after false positive, while real attacks fly under the radar. This system is broken. Today's approach to threat detection and response is simply not sustainable. Analysts are forced to cover a growing attack surface, with security tools spitting out an increasing volume of imprecise alerts.

> *Today's approach to threat detection and response is simply not sustainable. Analysts are forced to cover a growing attack surface, with security tools spitting out an increasing volume of imprecise alerts.*

Still, as the threat landscape expands and evolves, security teams are sold more threat detection tools, creating more noise and facilitating more unseen attacks – resulting in more breaches – so they deploy more tools – creating more noise – and the vicious spiral continues. As an industry, we cannot continue doing what has always been done, making the same mistakes, feeding the same spiral. If we are to break the spiral, we need to provide SOC teams with the one thing they continue to lack – signal. When it comes to breaking the spiral of more the only "more" security needs is more effective signal. It is time security vendors are held accountable for the efficacy of their signal.

Signal clarity is the difference between time spent on manual, mundane tasks and time spent investigating and responding to real attacks. We argue the vendor that delivers the most accurate signal will earn the trust and confidence of the SOC team. The more effective the threat signal, the more cyber resilient, efficient, and effective the SOC becomes.

About Vectra AI

Vectra AI is the leader in AI-driven threat detection and response for hybrid and multi-cloud enterprises. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single platform. The Vectra AI Platform with patented Attack Signal Intelligence™ empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks in 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 March-April 2023 study commissioned by Vectra and carried out by Sapio Research. Sapio surveyed 2,000 IT security analysts working at organizations with more than 1,000 employees across the US (200), UK (200), France (200), Germany (200), Italy (200), Spain (200), Sweden (200), the Netherlands (200), Australia and New Zealand (200), and Saudi Arabia and the United Arab Emirates (200).

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