VECTRA

Global Report

2023 State of Threat Detection

The Defenders' Dilemma

EXECUTIVE SUMMARY

Today's security operations (SecOps) teams are tasked with protecting progressively sophisticated, fast-paced cyberattacks. But detecting, investigating, and stopping advanced cyberattacks at scale and speed is becoming increasingly unsustainable with the complexity of people, processes and technology SecOps teams have at their disposal. A perfect storm of an ever-expanding attack surface, highly evasive and emerging attacker methods, and increasing SOC analyst workloads is resulting in a vicious spiral of more for SOC teams.

In this report – based on an independent global study of 2,000 SOC analysts – we dive headfirst into the spiral of more that SOC analysts face.

Is threat detection 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 concerned number of analysts admit the same technology hampers their ability to effectively defend the organization from cyberattacks.

Alert noise and triage increasing

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.

SecOps teams facing high demands

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

SecOps model is broken

Today's SecOps model is broken, and it's pushing humans to the brink. This research indicates that organizations need to rethink traditional approaches to threat detection and start holding security vendors accountable for the efficacy of their signal.

KEY FINDINGS

90% OF SOC ANALYSTS BELIEVE THEIR SECURITY TOOLS ARE EFFECTIVE, YET:

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.

63/70/66%

SOC analysts report the following having increased in the past 3 years: 63% say the size of their organization's attack surface has grown, 70% report the number of security tools they leverage has increased, 66% say the amount of alerts they manage have significantly increased.

67%

SOC (Security Operations Center) teams receive an average of 4,484 alerts per day, but can't deal with over two-thirds (67%) of them.

97%

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

41%

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

67%

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

SECTION ONE

More Attack Surfaces, More Alerts, More Costs

KEY FINDINGS

- Manual alert triage costs organizations approximately $3.3bn annually in the US alone
- SOC teams receive **4,484 alerts each day on average**
- Security analysts are unable to deal with over two-thirds (67%) of the daily alerts they receive, with 83% reporting that these alerts are false positives and not worth their time

67%

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

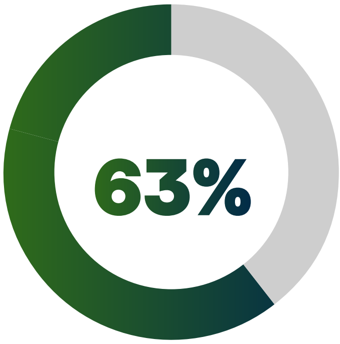
83%

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

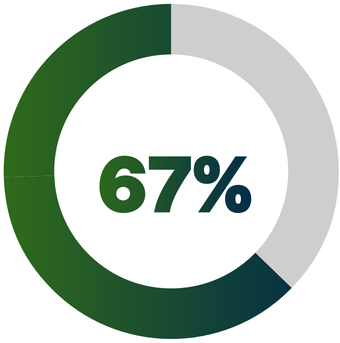
Security analysts sit on the front lines in the ongoing battle against cyberattacks.

They have a critical job: to 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:

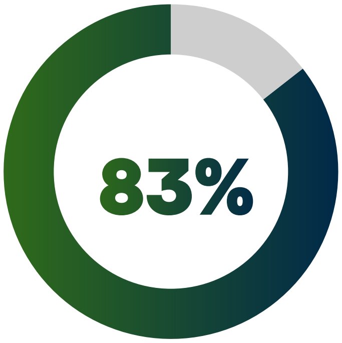
- The size of the organization's attack surface
- The number of security alerts they receive
- Their increasing workloads



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

This "spiral of more" threatens defenders' ability to be successful at their job.

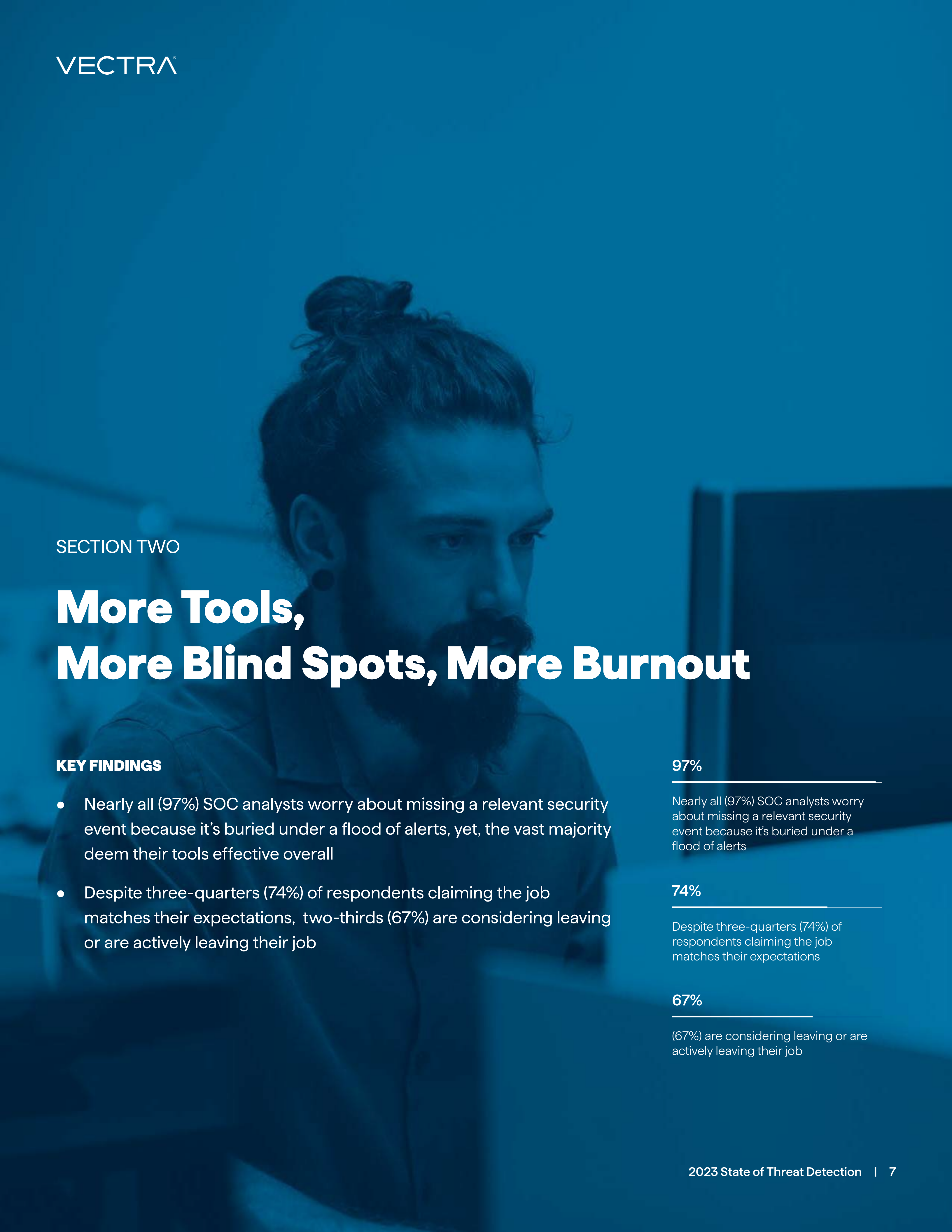
Nearly two-thirds (63%) of respondents say the size of their attack surface has increased in the past three years, while 27% say it has increased significantly. 61% of analysts also point to surging volumes of vulnerabilities impacting their organization during this period. Investments in digital and 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 opens up more opportunities for attackers, with 61% of respondents admitting they don't have the necessary skillset 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 SecOps teams.

Responding 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. 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, allowing attackers to 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

KEY FINDINGS

- Nearly all (97%) SOC analysts worry about missing a relevant security event because it's buried under a flood of alerts, yet, the vast majority deem their tools effective overall
- Despite three-quarters (74%) of respondents claiming the job matches their expectations, two-thirds (67%) are considering leaving or are actively leaving their job

97%

Nearly all (97%) SOC analysts worry about missing a relevant security event because it's buried under a flood of alerts

74%

Despite three-quarters (74%) of respondents claiming the job matches their expectations

67%

(67%) are considering leaving or are actively leaving their job

97%

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 a high volume of false positive alerts mean that enterprises and their SecOps 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.

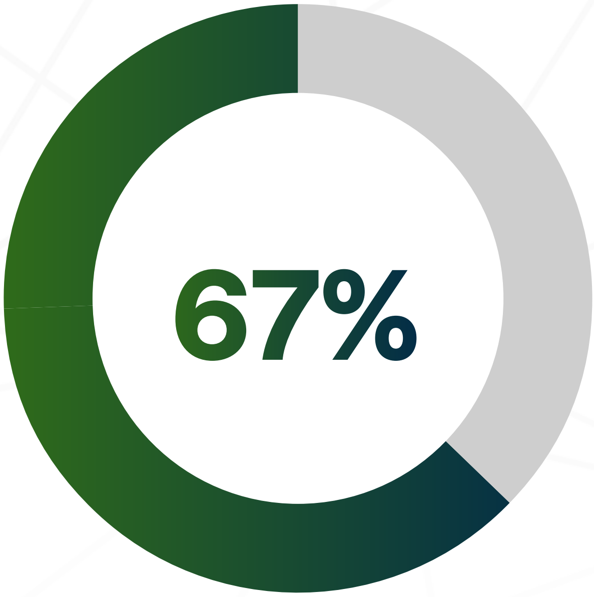
YET, THE VAST MAJORITY OF SOC ANALYSTS SURVEYED DEEM THEIR TOOLS "EFFECTIVE" OVERALL:

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%

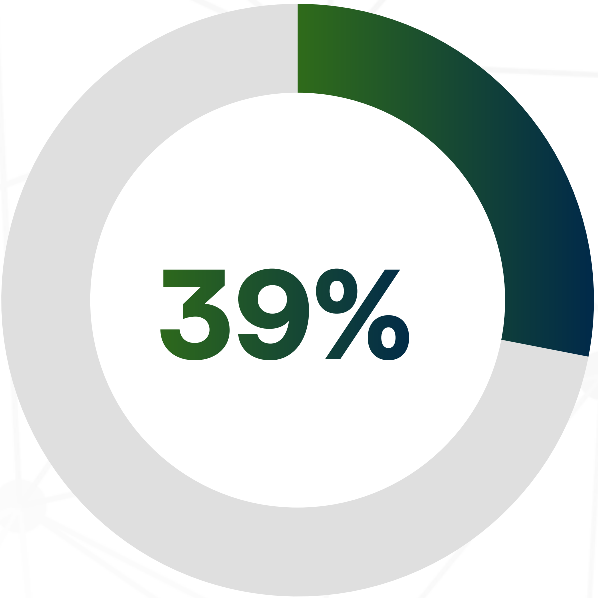
While many analysts deem their technologies effective, they are still facing an increasing number of alerts, and go on to admit that the same tools mentioned above are adding to a lack of visibility and uncertainty, as well as alert overload.

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

Endpoints	**76%**
On-premises and cloud-based networks	**75%**
Identity systems	**75%**
SaaS environments like Microsoft 365	**75%**
Public cloud environments	**73%**
Private cloud environments	**76%**
IoT (Internet of Things) environments	**76%**
OT (Operational Technology) environments	**76%**



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



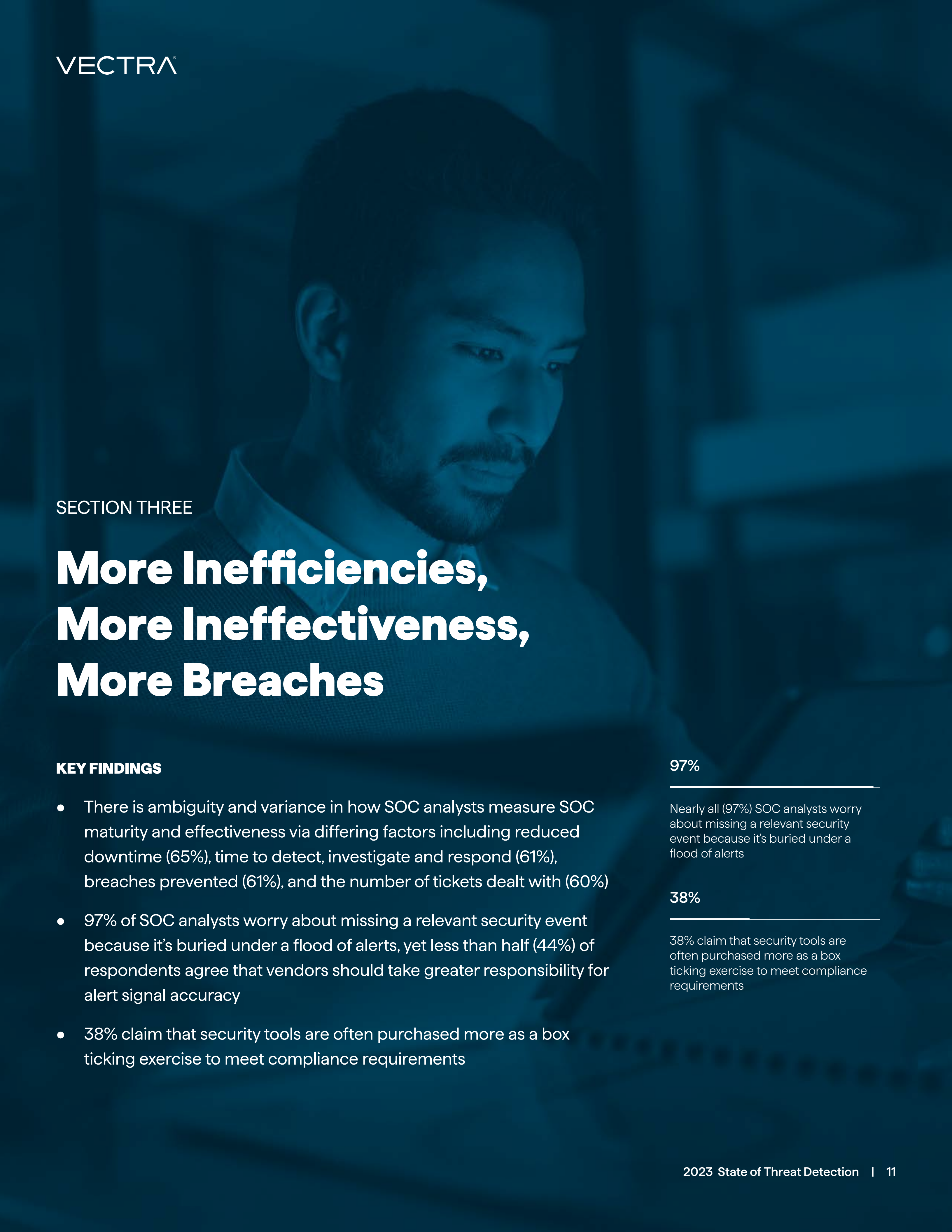
Spending too much time sifting through poor quality alerts (39%)

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 burnt out they are tempted to "quiet-quit." Analysts are clearly stretched, and the industry can't afford to see them leave the profession.

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 SecOps processes. Respondents also cite constant workplace stress (35%), burnout (34%) and the role's impact on their mental health (32%), which long hours of repetitive, mundane work could certainly contribute to.

More than a third (35%) claim the organization's leadership simply doesn't understand security. This means that SecOps 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

KEY FINDINGS

- There is ambiguity and variance in how SOC analysts measure SOC maturity and effectiveness via differing factors including reduced downtime (65%), time to detect, investigate and respond (61%), breaches prevented (61%), and the number of tickets dealt with (60%)
- 97% of SOC analysts worry about missing a relevant security event because it's buried under a flood of alerts, yet less than half (44%) of respondents agree that vendors should take greater responsibility for alert signal accuracy
- 38% claim that security tools are often purchased more as a box ticking exercise to meet compliance requirements

97%

Nearly all (97%) SOC analysts worry about missing a relevant security event because it's buried under a flood of alerts

38%

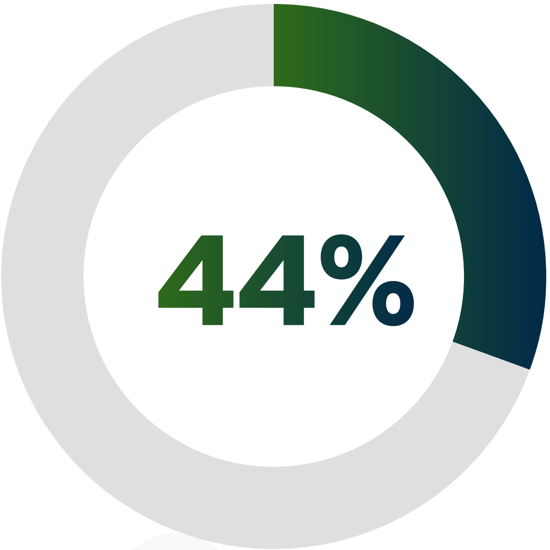
38% claim that security tools are often purchased more as a box ticking exercise to meet compliance requirements

Without addressing the broken security model and redefining how we measure the effectiveness of security tools, the situation will only 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.

Nearly all (97%) SOC analysts worry about missing a relevant security event because it's buried under a flood of alerts, yet **less than half (44%) of respondents agree that vendors should take greater responsibility for alert signal accuracy** and 41% believe alert overload is the norm because vendors are afraid of not flagging something that could turn out to be important.

Vendors aren't solely to blame – 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.



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

CONCLUSION

These findings prove that a "spiral of more" is overwhelming SOC analysts. While threat actors have never had a greater attack surface to target or number of techniques to do so, defenders are struggling with excessive alert noise and IT complexity. As a result, hours are spent triaging alerts while still running the risk of missing legitimate attacks.

Although many analysts believe their tools are effective, they also admit to major visibility gaps. 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 are 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 ever-expanding corporate cyber-attack surface or booming threat landscape, as hackers will always be looking for new ways to outwit defenders.

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

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 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 March-April 2023 study commissioned by Vectra AI 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.