binalyze!

THE BINALYZE 2026 STATE OF THE SOC REPORT

PUNCHING THROUGH THE INFORMATION AVALANCHE

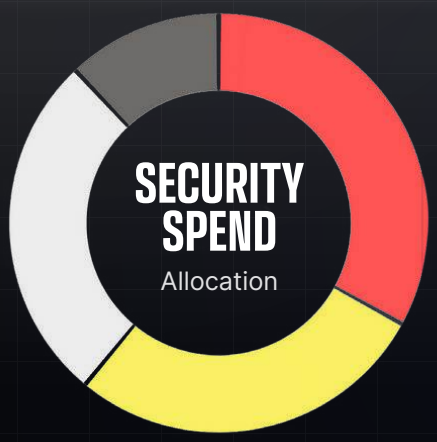
Inside: how SOC teams under pressure can turn the tide.

EXECUTIVE SUMMARY

SOCs are organizations' first and last line of defense. But a transforming threat landscape risks overwhelming them. Modern attacks are faster and more powerful than anything SOCs have faced before, spreading between systems faster than teams can respond. And SOCs must track a constant avalanche of new technologies, regulations and information.

Without the right X factor, SOC teams will be buried. Proactive threat hunting can stem the flood of alerts and put teams on the front foot, but can stretch already under-resourced teams thinner and thinner. AI presents both threats and opportunities, but can easily swamp teams in information without granting understanding. And regulation can support best practice and protect reputations, but also easily act as a crutch or create perverse incentives.

WHERE ARE SECURITY BUDGETS SPENT?



SOC operations — alert monitoring, triage & response	33%
Maintaining governance, risk & compliance	28%
Threat hunting	27%
Other	12%

Source: 400 US and UK CISOs and senior IT leaders, organizations with 500+ employees

These are not insurmountable odds. A truly empowered team will hold the most powerful weapon of all: the truth. Facing every decision armed with real-time truth on demand, they can meet regulatory demands while ensuring they are truly protecting the business.

For instance, adding context to information empowers teams to act based on a full understanding of the facts, without wasting time on irrelevant data. Embedded, accessible forensic-grade visibility means teams with a live view of new and emerging threats can hunt and triage effectively and confidently, instead of being forced into reaction.

KEY FINDINGS

AN AVALANCHE OF ALERTS

2,047

alerts received by SOCs every day, on average.

THE AGE OF IGNORANCE

$5.1m

average annual cost of undiscovered vulnerabilities.

BLINDED, NOT ILLUMINATED

91%

of SOCs are suffering from information overload.

PROTECTION OR PRISON?

74%

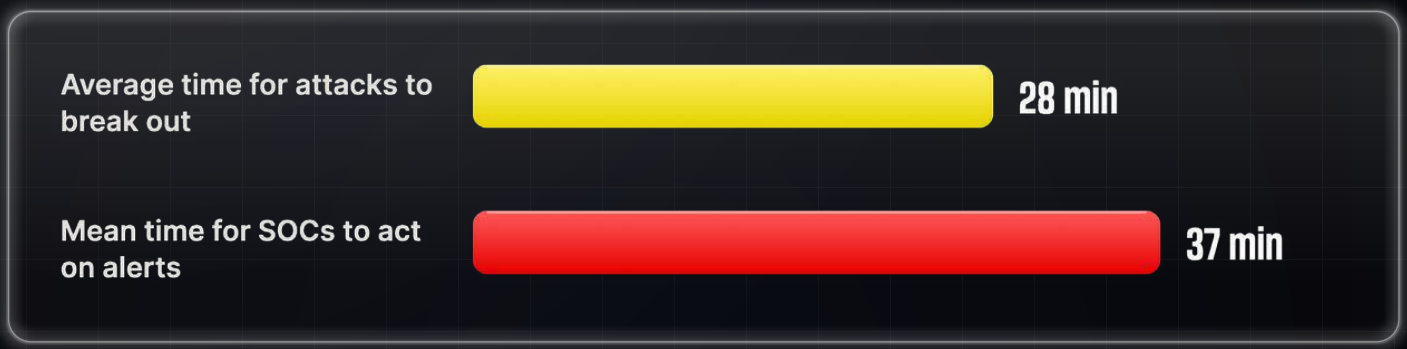
of CISOs have had projects refused because they “weren’t deemed necessary” to meet compliance.

Each finding points to the same root problem: SOCs are forced into a reactive posture, fighting symptoms instead of causes. Speed alone cannot close the gap when the volume of alerts, the depth of hidden risk and the burden of compliance all rise together.

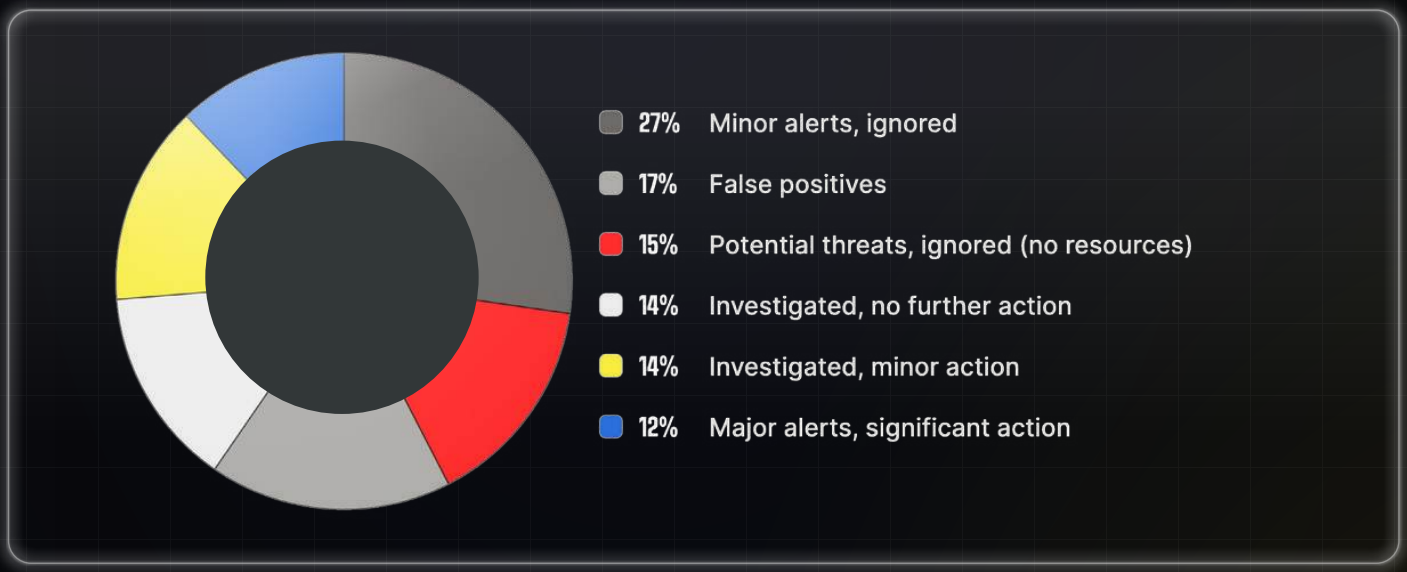
The rest of this report explores three fronts: alert overload, the data flood, and regulation. And how SOCs can switch from defense to a confident, proactive offense.

PART ONE TURNING THE TIDE ON ALERT OVERLOAD

Speed is of the essence. Alerts have to be triaged and acted on before attacks break out from a compromised endpoint into the wider environment and start causing havoc. This is not happening.



Defenders are forced to leave gaps in their knowledge. Of more than 2,000 daily alerts, over 1,200 are ignored or false positives, and more than 300 potential threats are ignored due to a lack of resources.



37 > 28

THE VERDICT
Triage is slower than breakout. On average, attacks always break out first.

15%

OF SOCS
take more than an hour to act on an alert.

TARGET SIZE MATTERS

2,047
ON AVERAGE
alerts a day across all SOCs

1,356
SMALLER ENTERPRISES
500–999 employees, per day

3,115
LARGER ENTERPRISES
5,000+ employees, per day

This is an acknowledged problem, and the industry has been talking about it for years. The clear answer is automated triage. But most SOCs do not trust automation built on telemetry alone, because telemetry is not ground truth. Without forensic-grade evidence underneath it, automation inherits the very blind spots it was meant to remove.

STANDING AGAINST THE STORM OF VULNERABILITIES

SOCs are facing a storm of vulnerabilities. Both identified and undiscovered. Rising costs are inevitable. To prevent this, enterprises need resilience that runs parallel to finding and patching. Damage from vulnerabilities can still be mitigated with a threat hunting program.

290

NEW VULNERABILITIES

On average, enterprises identified 290 new vulnerabilities in the past year.

172

UNDISCOVERED

But estimate 172 more went undiscovered.

$5.1M

THE COST

Undiscovered vulnerabilities cost on average $5.1 million a year.

This proactive approach also reduces the risk that enterprises fall victim to vulnerabilities that should be solved problems. Alongside intelligence sharing, it improves outcomes for all organizations.

57% of organizations have suffered a breach thanks to a vulnerability another organization had already suffered and reported.

Without this approach, SOCs will find themselves trapped with rising alerts and vulnerabilities. Teams will face the worst of both worlds: resigned to missing alerts and breaches, yet at the same time paranoid that a major breach will go unchecked.

56% of CISOs: “I am paranoid that I’ll miss an alert signifying a major breach.”

73% of CISOs: “It’s inevitable there will be blind spots as we can never cover everything.”

SOCs recognize the need for a proactive approach. They believe they are investing heavily in threat hunting. And they understand the impact on effectiveness and reducing fatigue. The question is, is this happening?

77% of CISOs: "Our SOC would be more effective if we were more proactive."

81% of CISOs: "The only way to prevent alert fatigue is to hunt down and deal with threats earlier."

62% of CISOs: "Our SOC focuses almost entirely on alerts and triage, instead of prevention and intelligence."

76% of CISOs: "I want to invest more in threat intelligence, but I have too many other demands on my budget."

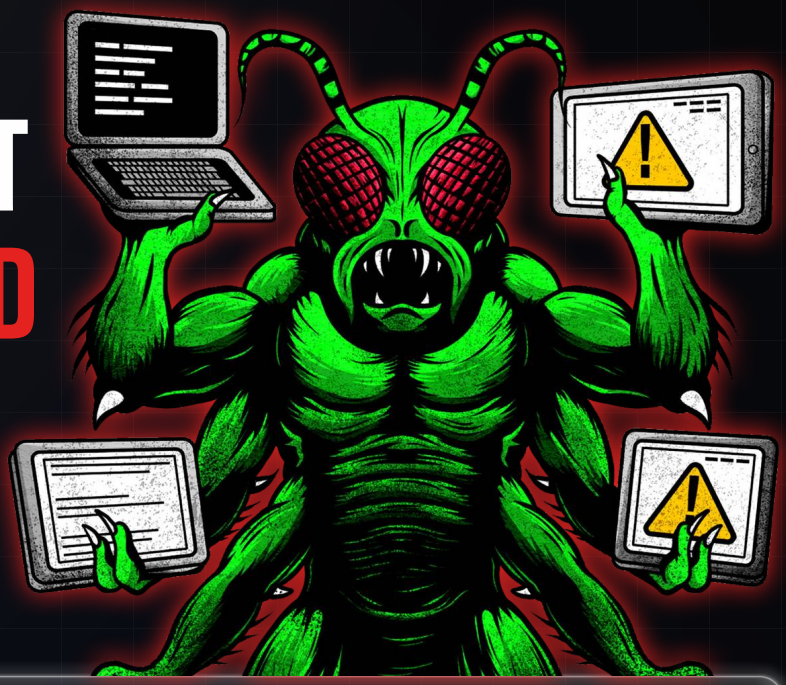
THE CHALLENGE IS CLEAR

The greatest impact will be making tools more accessible. Specialist hunters are in high demand, and cannot be everywhere at once. Removing or reducing this barrier will reduce the pressure on teams and budgets, and allow for effective threat hunting. Effective hunting is constant and consistent. Not an occasional or even regularly scheduled activity where threats have time to fester and grow in between hunts. It is comprehensive, leaving no dark corners for threats to lurk in: hunting for suspicious activity and unidentified exposures, not only for attackers lying in wait.

Threat hunting teams need tools and approaches that maximize their effectiveness and help them find the truth behind the threat. That reduce time spent pivoting across disconnected tools and evidence, or on repetitive manual tasks. That give a way for investigative findings to improve broader SOC detection and resilience. And that empower investigative experience to scale consistently across teams.

PART TWO

RISING AGAINST THE DATA FLOOD



It is inevitable. As the threat landscape grows and new technologies like AI create data at never-before-seen scale, SOCs face a flood of threat information.

86% of SOCs: "We are dealing with more data, from more sources, than ever before."

AI has definitely contributed. Used by attackers, it means threats arrive in a greater volume and scale than ever before. But even defensive AI contributes: the deluge of information it creates in identifying and attempting to mitigate potential alerts still needs to be understood.

The all-too-predictable outcome? More threat data. And a larger workload for analysts attempting to parse it all.

25%
GROWTH
in available threat data over the past 12 months.

27%
INCREASE
in analysts' workloads over the past 12 months.

+1 week
THE REALITY
analysts are working an extra week per month.

This information overload is already affecting SOCs. Not only with a higher workload. But by making it harder to spot the genuine threats.

INFORMATION OVERLOAD IS HERE

91% OF CISOS
say their organizations suffer from information overload.

77% OF CISOS
have missed warnings and vulnerabilities because of it.

47% FOR NEARLY HALF
it's a regular or constant issue.

Worse, SOCs aren't even getting the information they need. All this data still doesn't help analysts understand what they're facing, make informed decisions, or have confidence in their actions.

Because volume is only half the problem. Quality is the other. Garbage in, garbage out applies as much to a SOC as to any other data operation: decisions are only ever as good as the evidence beneath them, and no amount of AI will rescue an answer built on shallow or stale data.

The distinction that matters is not how much data reaches the SOC, but whether that data is investigation-ready: complete, contextual, and searchable by analysts and by the AI tools working alongside them. Evidence that was previously out of reach until an incident was escalated to a specialist team needs to be available, and usable, from the first alert. Get that right and each new source becomes an asset rather than another contributor to the overwhelm.

64% OF SOCs: "I don't want alerts; I want information about the threats I face and the data at risk."

65% OF SOCs: "When we act on an alert, it's impossible to have the full context of what data is at risk."

60% OF SOCs: "Even with all the information at our disposal, I don't have 100% confidence in our decision-making."

AI is contributing to the information flood. This would be a worthwhile trade-off if it made triage and investigation more effective. Currently, results are mixed.

CISOS WHO CANNOT COMPLETELY TRUST THREAT TRIAGING:

79% NOT USING AI
cannot completely trust their threat triaging

67% USING AI TO TRIAGE
cannot completely trust their threat triaging

71% OF CISOS
"AI should be powerful for triage, but I don't think it's used correctly."

The challenge isn't only using AI correctly. It's having all the necessary resources, from technology to training to skilled people, to provide complete clarity of incoming data, and offer trusted insights.

34% of SOCs have all the resources and skilled people they need.

42% say high demand means they can't hire enough people – even when they have the resources to do so.

With the right tools and processes, SOC teams can make the data explosion work for them. Validating before escalating, to reduce escalation pressure and burnout. Scaling investigation capability while freeing up senior investigators to focus on those threats that need deep expertise. And building clarity so teams have the right picture, from the outset, every time.

Knowing what data is the most critical will be a crucial element of this. For instance, current AI and other tools can provide a wealth of information on telemetry. Where data is moving from and to; in what volumes; and who has access.

But to make the right decisions, teams need context: what is the data, how valuable is it, what are the consequences of a breach?

With the right approach, SOCs can soar above the data flood: understanding the truth of what happened and acting with confidence at every stage.

PART THREE

KEEPING REGULATION AN ALLY, NOT THE ENEMY

Regulation is a powerful ally for SOCs. It encourages best practice, supports communication and understanding, and protects organizations, their partners and customers.

If it encourages simple box-ticking and performative audits over action that will genuinely improve security and safety, organizations need to question the regulation's aims, or their own approach.

CISO VIEWS ON REGULATION

"Regulation is more focused on protecting organizational reputations than on protecting people." **72%**

"I'm worried increasing regulations will fill our time with tick-box exercises instead of improving security." **65%**

"From a compliance perspective, it's safer to follow the same actions as every other organization–even if that isn't best." **64%**

"I feel under pressure to be always-prepared for audits that wouldn't help improve or future-proof our security." **63%**

The answers suggest CISOs and regulators don't see eye to eye. CISOs are even divided among themselves.

"I DON'T BELIEVE THAT OUR PRIORITIES AS A SECURITY TEAM AND REGULATORS' PRIORITIES MATCH UP."

40% AGREE

40% DISAGREE

Time spent on compliance is not time wasted if it improves security and accountability. The worst-case scenario is spending time that doesn't improve security, safety or compliance.

22% of CISOs' time is spent proving compliance.

44% of that time is "wasted" - around 4 hours every week.

The wrong approach to regulation can affect entire organizations. Focusing on strict compliance instead of the purpose of regulation, protecting individuals and organizations, can prove a drag on security itself.

74% of CISOs have had security projects refused because they "weren't deemed necessary" to meet compliance.

What could regulators do better? Many of the challenges above are for organizations to solve. And the nature of regulation means it can only ever react to new developments in security and advances by attackers. Instead, regulation should focus on behavior. Encouraging best practice in organizations and covering institutional weak spots in industries.

54 weeks

CISOs say regulators are 54 weeks behind the curve.

54% OF CISOS:

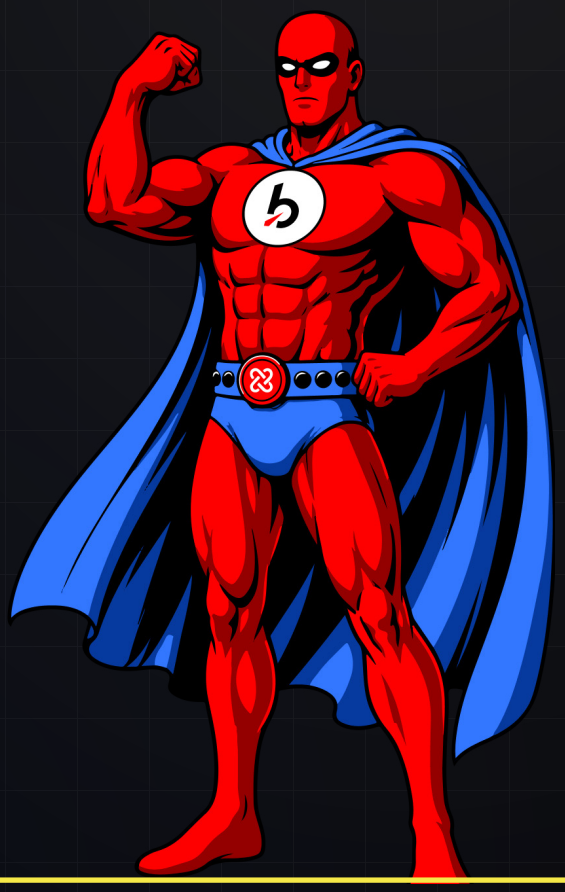
"Current regulations don't do enough to encourage intelligence sharing."

To prosper in the brave new world of cybersecurity, CISOs and SOCs need to meet regulators' demands while protecting themselves; their customers, partners and employees; and their reputations.
This means giving regulators what they need. Answers. Fast, confident, defensible answers.

A framework that provides evidence and investigative clarity on demand will help CISOs prove compliance before it's questioned. Without spending days or weeks of their time auditing and dragging attention away from security.

CONCLUSION

EMPOWERING THE ENTERPRISE'S MIGHTIEST HEROES



Modern enterprises face an overwhelming force. Threats are evolving and multiplying. AI is uncovering new vulnerabilities, and even acting on them, at record speed. Regulation is racing to keep up with a constantly changing landscape. And competition for the skills to combat this is fierce.

The SOC is the first and last line of defense. But it has to set its own terms. Relying on alerts to stop every attack before it breaks out is already a losing battle. Information overload will inevitably bury SOC teams. And regulation cannot substitute for constantly adapting tactics and strategies.

To succeed, we must take the fight to the enemy. Proactive threat hunting will allow us to stop threats before they can take root. And help gather intelligence that makes future attacks harder or identifies attackers outright.

Focusing on context will let us find the truth in data: bringing understanding instead of an information overload. And concrete evidence with investigative clarity will give regulators what they need, when they need it. Freeing teams to concentrate on the true goal of making everyone safer.

With the right tools and frameworks, SOC teams can unleash their true abilities. And prove themselves more than a match for a rapidly evolving threat environment.

TO LEARN MORE ABOUT HOW BINALYZE CAN HELP LEVEL UP THE SOC, VISIT: MSSP.BINALYZE.AI

METHODOLOGY

This report is based on a Sapio Research survey of 400 CISOs and senior IT leaders responsible for managing the SOC in their organizations. Respondents were based equally in the US and UK. Research was performed in Q2 2026.