Microsoft Security

State of the SOC

Unify Now or Pay Later: What New Research Reveals

Contents

Foreword by Rob Lefferts 3

The modern SOC: An operation at a breaking point 4

The strategic imperative: Unifying for a resilient defense 10

The roadmap to resilience 14

Unify now or pay later 16

Appendix: About the research 17

Foreword: An inflection point for the SOC

Security operations are at a real inflection point. The signal we see every day—and the data in this report—show how fragmentation and manual work erode resilience while adversaries continue to accelerate. Many teams still stitch insights across double-digit consoles, and nearly half of alerts never get investigated—gaps attackers have learned to exploit. Sophisticated threats like ransomware or business email compromise now move in minutes, compressing the window to contain intrusions.

The path forward is evolving to a predictive SOC—one that anticipates attack paths and measures risks, shifts posture before an attacker can exploit, and uses AI agents to turn intent into coordinated action at machine speed. In practice, that means predictive graphing to surface likely pivot paths and prioritize the fixes that matter, real-time coordinated defense to shrink dwell time, and agentic assistance that reasons over context and orchestrates multi-step workflows so experts can pivot from reactive defense to proactive threat hunting, stopping novel attacks before they cause damage.

The findings that follow quantify today's hidden taxes and lay out a pragmatic roadmap to measurably better outcomes. Our commitment is simple: keep elevating defenders with technology that is both faster and safer—from endpoints to cloud workloads and the servers and data they protect—so you can anticipate and stop attacks with confidence.

Rob Lefferts

Corporate Vice President,
Threat Protection

The modern SOC: An operation at a breaking point

The modern security operations center (SOC) is at a breaking point, not from a lack of effort, but from an operational model that creates too much friction. New research from Microsoft and Omdia reveals a clear performance gap between fragmented security tools and a unified, AI-driven approach.

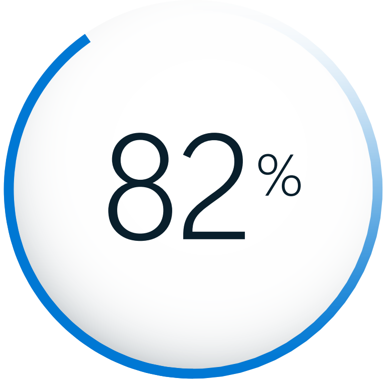
Microsoft processes more than 100 trillion security signals every day.[1] This massive scale trains AI models that detect emerging threats and correlate attack patterns across endpoints, identities, and cloud—intelligence no fragmented toolset could generate alone.

[1] Microsoft Digital Defense Report 2025, page 6, Microsoft, October 2025.

1 The fragmentation challenge

Fragmented tools and disconnected data present the modern SOC's most significant operational challenge. With teams juggling an average of **10.9 security consoles**, analysts must pivot between interfaces and manually reconstruct context. This not only slows investigations but dramatically increases the risk of missing critical signals buried in the noise.

This problem is compounded by incomplete data ingestion into the central Security Information and Event Management (SIEM) platform. Our research found that only **~59% of security tools** push data to the SIEM via API, leaving critical gaps. As a result, an astonishing **82% of SOCs** still ingest data manually several times per week, creating bottlenecks that erode operational efficiency.



of SOCs still ingest data manually several times per week or more.

For more detail, see figures 1 and 2

CISO takeaway: Unify or face rising rates of compromise

Fragmentation directly degrades key performance metrics like Mean Time to Acknowledge (MTTA) and Mean Time to Resolve (MTTR). The only sustainable way to remove this friction is to unify tools and workflows into a single, integrated SOC platform for faster, more accurate detection and response.

2 The hidden tax of manual toil

Behind every alert triaged and every threat investigated lies a hidden tax on analyst time: the grind of manual data aggregation, correlation, and data plumbing. This repetitive routine is a significant drain on the SOC's most valuable resource—its human experts.

According to our findings, **66% of SOCs** report that analysts spend over **20% of their week**—the equivalent of a full day—on manual data aggregation across tools. Rather than acting on insights, analysts spend one-fifth of their week assembling and cleaning data—delaying the very analysis that drives proactive defense.

This is time that could be spent on activities that directly impact the security bottom line; our research shows that **~75% of SOCs** allocate three or more full-time employees to the critical workstreams of detection engineering and threat hunting, yet their capacity is consistently eroded by manual toil.

20%

of an analyst's week—one full workday in five—is lost to manual toil.

For more detail, see figures 3 and 4

CISO takeaway: Automate to elevate

Manual toil drains SOC capacity and effectiveness, diverting critical resources from high-value risk reduction. Unified platforms with embedded AI automate routine tasks, empowering experts to focus on what matters most and significantly improving MTTA and MTTR.

3 The security signal storm

SOCs face a paradox: they're flooded with data yet starved for actionable insight. The relentless surge of alerts creates a deafening noise that obscures the true signal. Instead of empowering defenders, this torrent of low-fidelity alerts fragments analysts' attention, accelerates burnout, and heightens the risk of overlooking genuine threats. The challenge isn't just volume—it's clarity.

Our research paints a stark picture of this "security signal storm." An estimated **46% of all security alerts** are false positives. This means nearly half of the alerts an analyst investigates provide no value, stretching capacity thin and breeding alert fatigue. The consequence is dire: leaders report that **42% of alerts** go uninvestigated simply due to capacity constraints.

42%

of all security alerts go uninvestigated, allowing preventable breaches to slip through.

For more detail, see figures 5 and 6

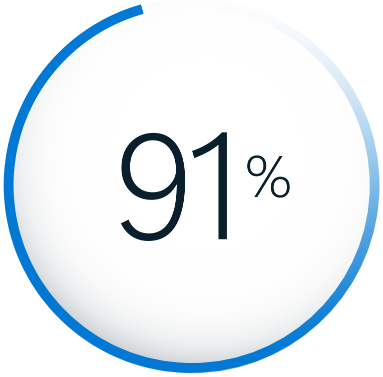
CISO takeaway: Prioritize with precision

Ignored alerts aren't just missed opportunities—they're unhandled risks and potential breaches. An integrated, AI-driven platform helps SOCs cut through the clutter, frees analysts from repetitive triage, and reduces fatigue. Unified data and end-to-end visibility enable AI-driven optimization—fine-tuning detections, tightening controls, and strengthening defenses. The result: sharper focus, stronger security, and maximum impact from human expertise.

4 The business cost of operational gaps

When SOC teams are stretched thin by tool fragmentation and manual toil, the consequences create quantifiable business risk. This risk manifests as financial loss from downtime, reputational damage, and strategic scrutiny at the board level as resilience metrics like MTTA and MTTR are examined.

Our research confirms the direct link between these operational gaps and business-disrupting events. A staggering **91% of security leaders** confirm that operational gaps have directly caused a serious incident. This is not an occasional failure but a chronic condition, with **56% of leaders** reporting it happened **more than five times** in the past year alone.



of leaders confirm operational gaps translate directly into serious, business-disrupting security incidents.

For more detail, see figure 7

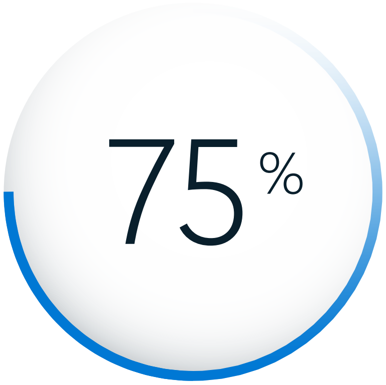
CISO takeaway: Elevate your SOC

The true cost of an inefficient SOC is measured in breaches. Transform your SOC from a cost center to a strategic business enabler by modernizing its operational model with automation and consolidation.

5 The blind spot of detection bias

As attackers pivot, security teams often concentrate on what they know best: refining detections for familiar threats. This creates a "detection bias," a trend our research confirms: **52% of true positive alerts** are linked to known vulnerabilities. While a tactical necessity for managing overwhelming alert volumes, this reactive posture leaves blind spots for the novel tactics, techniques, and procedures (TTPs) adversaries use to slip through the cracks.

This detection bias stifles the SOC's evolution. It directs resources toward tuning rules for known threats, suppressing detection engineering for emerging risks. This, in turn, erodes capacity for the proactive threat hunting required to find unknown threats. Security leaders are acutely aware of this vulnerability: a striking **75% are concerned** their SOC cannot keep pace with new and emerging threats.

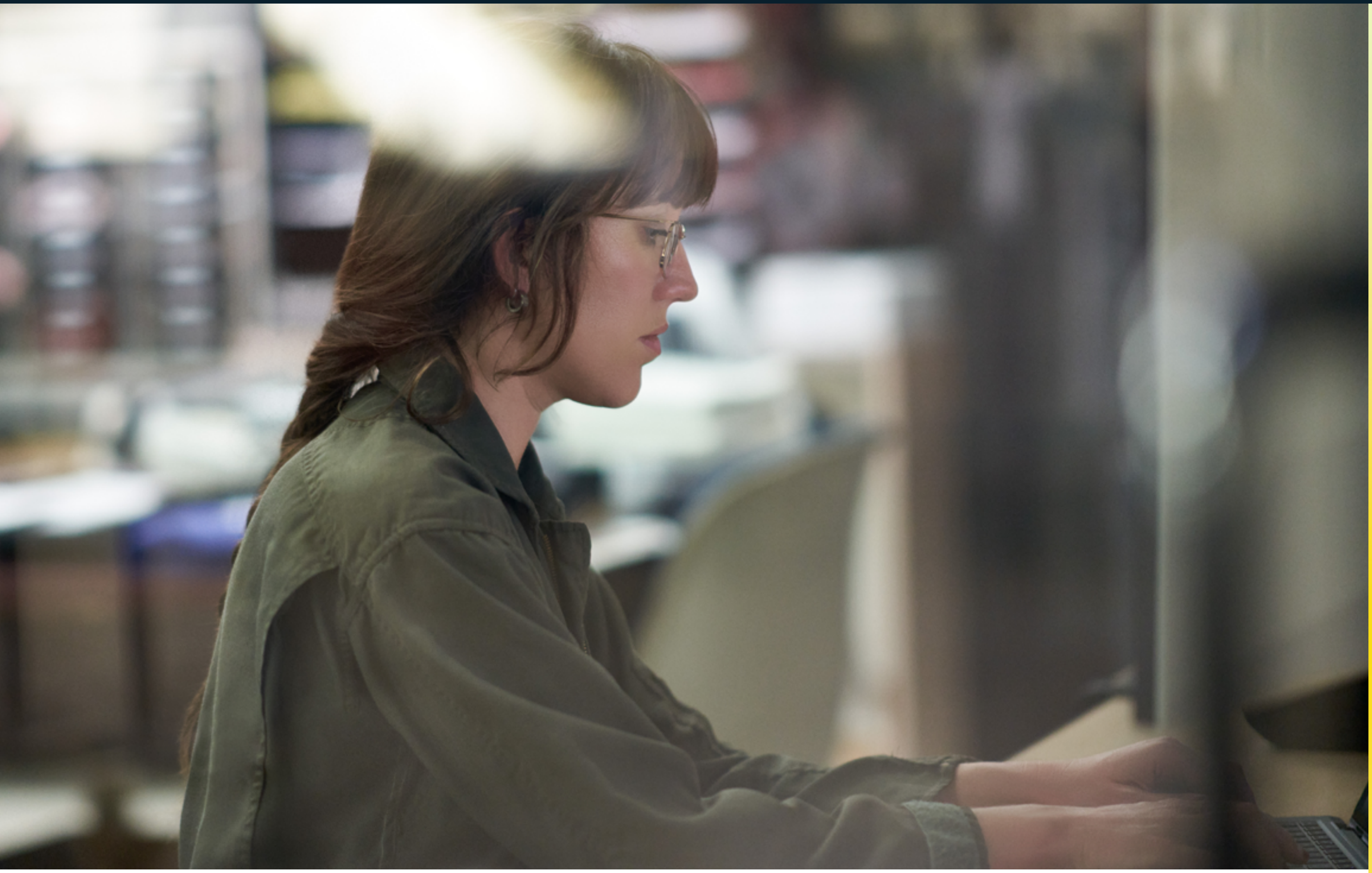


of security leaders fear they are losing the race against new and emerging threats.

For more detail, see figure 8

CISO takeaway: Detect beyond known threats

To detect beyond known threats, shift from manual work to proactive hunting. A unified platform enables this by automating routine tasks and correlating alerts, freeing analysts to focus on stopping emerging threats before they cause harm.



The strategic imperative: Unifying for a resilient defense

AI and automation are already delivering measurable wins in the modern SOC. Leaders are starting with the highest-impact opportunities—automating routine tasks, streamlining triage, and reducing noise—to combat fragmentation and manual toil. This shift from abstract concept to practical solution is well underway.

More than 97% of identity attacks are password attacks.[2] This core failure of fundamentals makes identity the most critical control point for defense—a vulnerability that can only be sealed by unifying identity and endpoint security.

[2] Microsoft Digital Defense Report 2025, page 16, Microsoft, October 2025.

1 The mandate for AI and automation

Our research confirms this momentum. An overwhelming **majority of security leaders (76%)** believe that most routine Indicator of Compromise (IoC) lookups could and should be automated. Furthermore, **90% or more** expect AI to deliver a moderate to significant reduction in manual effort across all SOC workflows. This is a clear mandate: automation is not a luxury, but a necessity.

However, the most insightful finding is not if leaders want AI, but *how* they want to deploy it. When asked about deploying SOC-focused AI agents, **64% of leaders** want a "studio" environment to build their own custom agents, compared to just 35% who favor pre-built, out-of-the-box tools. This preference reveals a sophisticated understanding of AI's potential and its risks. Leaders are not looking for a magic black box; they are looking for a powerful, governable capability they can customize to their unique environment.

64%

of leaders want to build their own AI agents, demanding control, not just automation.

For more detail, see figures 9, 10 and 11

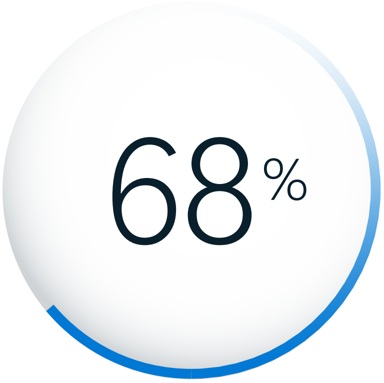
CISO takeaway: Integrate AI for impact

Bolting AI onto fragmented tools severely limits its potential. AI's true power is realized not as an add-on, but when deeply embedded within a unified platform with comprehensive data access. This transforms AI from a mere feature into the intelligent foundation of your security operations.

2 The SIEM’s next evolution: From centerpiece to integrated platform

The SIEM has long served as the visibility backbone of the SOC. Its foundational importance is undeniable, with our research showing that, on average, **45.8% of an organization's security data** resides in its SIEM. However, this same statistic reveals a critical limitation: with over half of security data living elsewhere, a standalone SIEM cannot connect the dots of a sophisticated attack.

Security leaders recognize this need for evolution. This is powerfully reflected in our research: **68% of leaders** state that it is critical their SIEM comes from their top security vendor. This is not about brand loyalty; it is a strategic demand for deep, native integration.



of leaders demand their SIEM comes from their top vendor, prioritizing integration over fragmentation.

For more detail, see figures 12 and 13

CISO takeaway: Evolve your SIEM

A standalone SIEM is no longer sufficient against modern, multi-domain attacks. Unified SIEM + XDR architectures, built on a security data lake, are critical. This integrated approach delivers the broader telemetry and deeper analytics essential for scalable automation and effective AI.

3 The KPI playbook: Turning gaps into gains

For security leaders focused on improving critical KPIs, the current state of the SOC is a major obstacle. Our research shows teams are treading water, splitting their time between **reactive tasks (48%)** and **proactive work (52%)**. This balance prevents the essential shift toward proactive defense that leaders demand.

The playbook for turning operational friction into strategic momentum is clear: unify tools to improve MTTR, automate triage to reduce backlogs, and integrate investigation workflows to lower MTTD/MTTA. This path forward explains why nearly **89% of leaders** are confident they can materially improve their KPIs, signaling a readiness for a new operational model where automation frees teams for high-value strategic work.

89%

of leaders are confident they can improve key security metrics, signaling a readiness for change.

For more details, see figures 14 and 15

CISO takeaway: Optimize your SOC

Improving security KPIs isn't about working harder; it's about enabling your team to work smarter. The most significant and sustainable gains come from a systemic shift to a single, integrated SOC platform.

The roadmap to resilience

The future of the security operations center isn't just about scaling—it's about simplifying, unifying, and empowering. The journey from a fragmented, reactive posture to a cohesive, intelligent, and resilient one is a strategic imperative. The next 12 months offer a clear opportunity to begin this transformation, guided by three simple but powerful principles: **Unify signals. Embed AI. Let humans hunt.**

More than 40% of ransomware attacks now involve hybrid components.[3] This reality proves that a Predictive SOC requires a unified platform that delivers seamless visibility and defense across cloud, identity, and on-premises environments, eliminating the gaps that fragmentation creates.

Drawing from these research findings and our experience securing the world's largest enterprises, this roadmap outlines a practical, phased approach to building the modern SOC.

1

Near term

(0–90 days)

Foundational wins

2

Mid term

(90–180 days)

Operational alignment

3

Long term

(180–365 days)

Strategic resilience

[3] Microsoft Digital Defense Report 2025, page 28, Microsoft, October 2025.

Phase 1: Near term (0–90 days)—Foundational wins

Focus on these four actions to reduce noise, automate repetitive tasks, and give your team back valuable time.

Expand API ingestion: Connect critical data sources to your SIEM via API for more complete and timely data.

Automate low-hanging fruit: Automate IoC lookups and alert enrichment to reduce analyst fatigue and accelerate triage.

Enforce alert quality: Set and enforce quality thresholds on alert sources to cut low-fidelity noise.

Deploy quick-win playbooks: Use automated playbooks for common triage and response scenarios to reduce backlogs and improve MTTR.

Phase 2: Mid term (90–180 days)—Operational alignment

The goal now is to break down silos by aligning tools, data, and workflows.

Establish a unified queue: Normalize data from all sources to create a single source of truth for investigations and eliminate console pivoting.

Embed AI assistants: Integrate AI assistants into analyst workflows to streamline decision-making, summarize incidents, and suggest response actions.

Invest in detection engineering: Dedicate analyst time to build and refine analytics for hunting both known and emerging threats.

Phase 3: Long term (180–365 days)—Strategic resilience

The focus now shifts from operational efficiency to strategic resilience, transitioning the SOC from a reactive to a predictive operation.

Implement continuous exposure management: Gain an attacker-centric view of your environment to proactively identify and mitigate risk.

Activate cross-domain correlation: Use ML-powered correlation to detect subtle, low-and-slow attack patterns across your entire digital estate.

Measure and refine: Track KPI improvements quarterly to justify investments and continuously refine your security strategy with data.

Unify now or pay later

The data are clear: fragmented security portfolios drain analyst capacity with manual toil, create blind spots, and leave organizations exposed to preventable threats.

The path forward is a unified SOC platform that embeds AI to automate routine tasks, cut through noise, and surface critical threats. This transforms the SOC from a reactive defense center into a proactive one—built not just to respond to threats, but to anticipate them.

The journey starts with a commitment to unification—the cornerstone of the modern security operations model.

↗ Learn more about unified security operations

↗ Explore Microsoft Sentinel

Share report with a colleague

Appendix: About the research

This study examines how security operations centers are evolving in response to increasing threats, tool sprawl, and the promise of AI-powered automation. The research explores where SOC teams are today, how they're measuring success, and what strategies are driving better outcomes.

The study, commissioned by Microsoft, was conducted by Omdia from June 25 to July 23, 2025. Survey respondents (N=300) included security professionals responsible for SOC operations at mid-market and enterprise organizations (750+ employees) across the United States, United Kingdom, and Australia/New Zealand.

Figure 01

How many distinct security management consoles (e.g., those associated with SIEM, EDR, XDR, NDR, SOAR, threat intel platforms, etc.) does your SOC team actively use in support of their daily activities? (Percent of respondents, N=300)

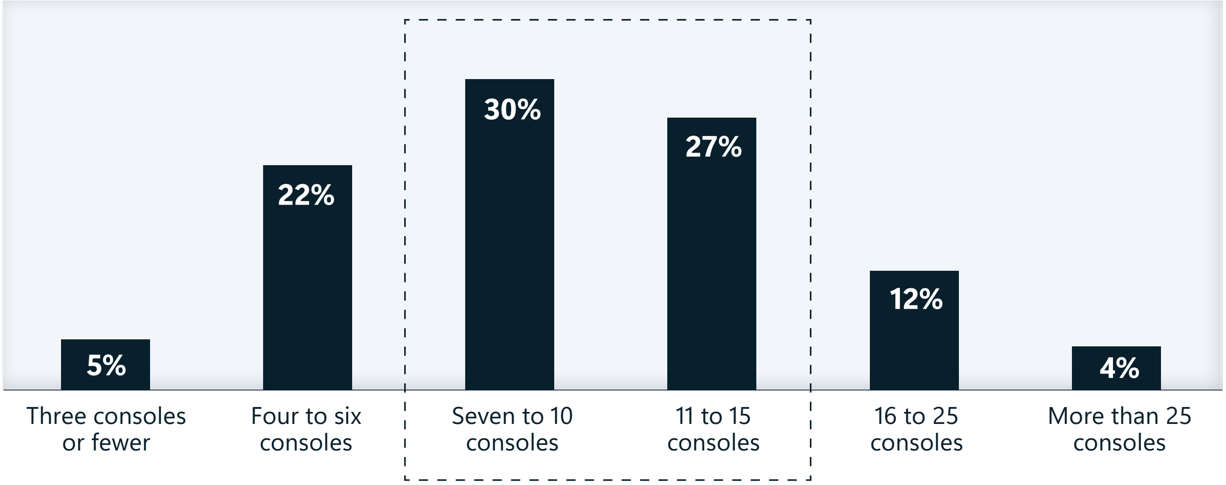
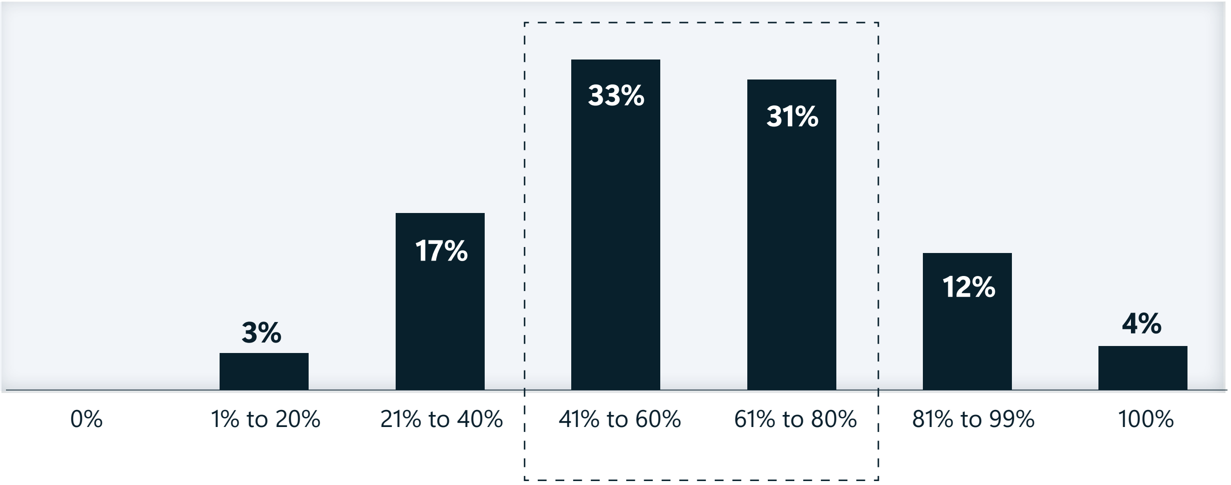


Figure 02

For the security tools deployed throughout your organization that have available APIs, approximately what percentage are currently feeding data into your SIEM? (Percent of respondents, N=300)



How often does someone on the SOC team need to manually track down data and ingest it into the SIEM because it's not automatically ingested? (Percent of respondents, N=300)

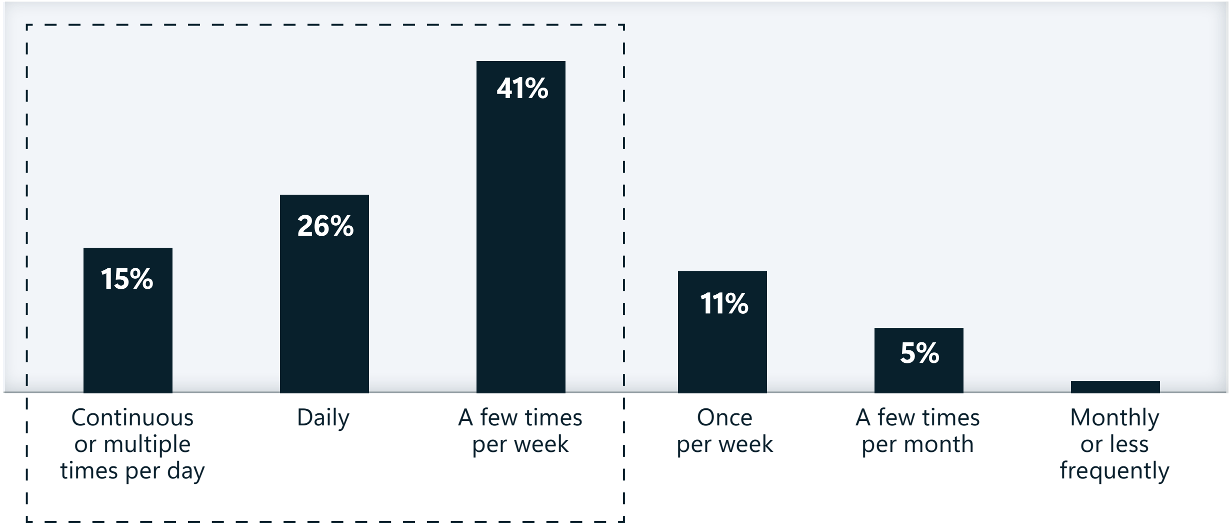


Figure 03

In a typical week, approximately what percentage of time does a typical SOC analyst spend manually correlating/aggregating data across different security tools to support their activities? (Percent of respondents, N=300)

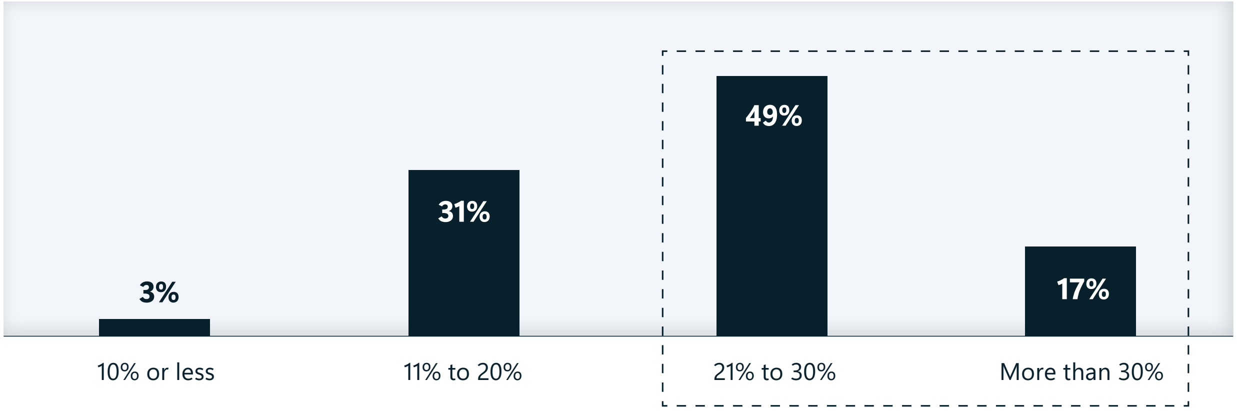


Figure 04

Approximately how many full-time equivalent (FTE) employees within your SOC are allocated to detection engineering? How many are allocated to hunting for IoCs based on threat intelligence? (Percent of respondents)

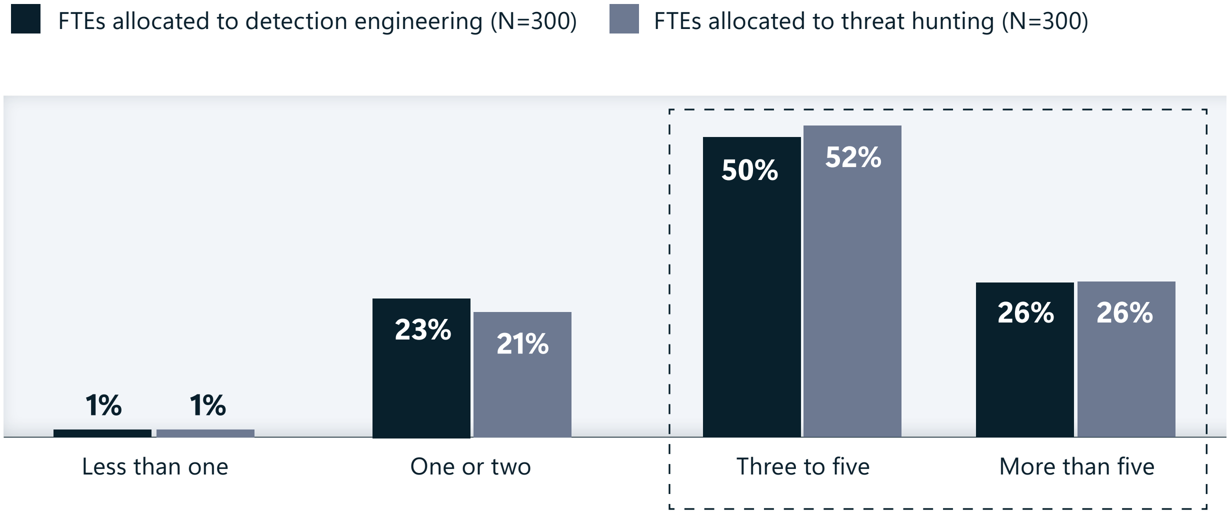


Figure 05

What percentage of the overall volume of security alerts do you believe are false positives (i.e., they are not an indication of an actual issue that warrants investigation)? (Percent of respondents, N=300)

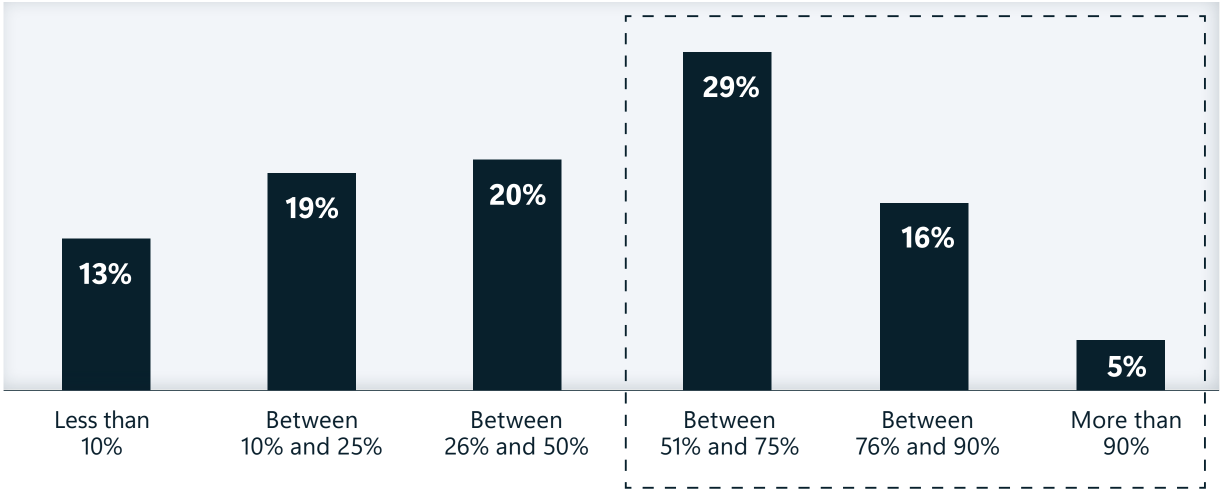


Figure 06

What percentage of the overall volume of security alerts do you believe your SOC staff ignores/ closes without investigation due to volume constraints? (Percent of respondents, N=300)

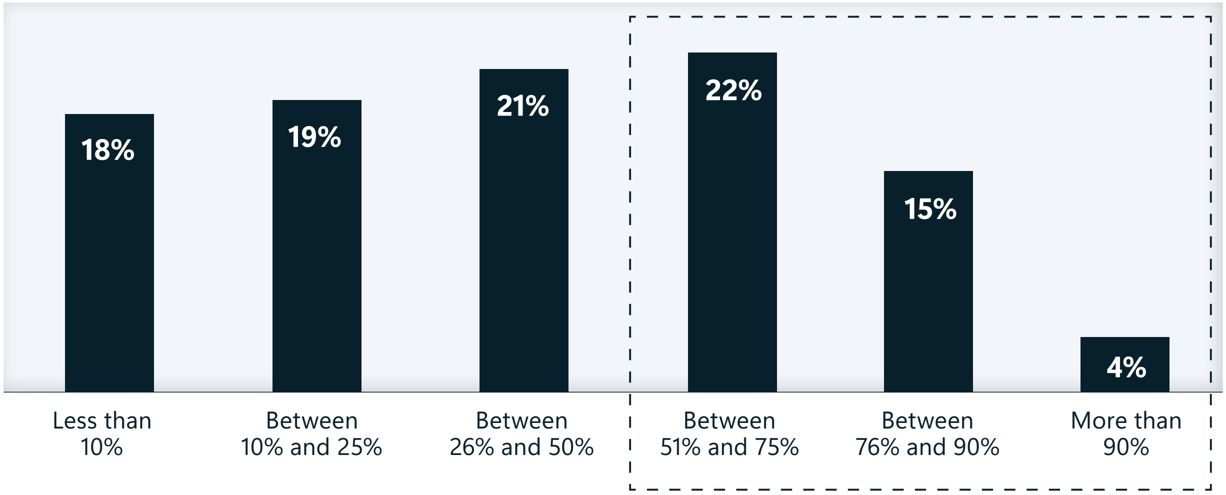


Figure 07

How many times in the past year do you think a security alert has waited in the queue/been ignored due to bandwidth and ended up being an indicator of a serious incident that could have been prevented if it had been addressed right away? (Percent of respondents, N=300)

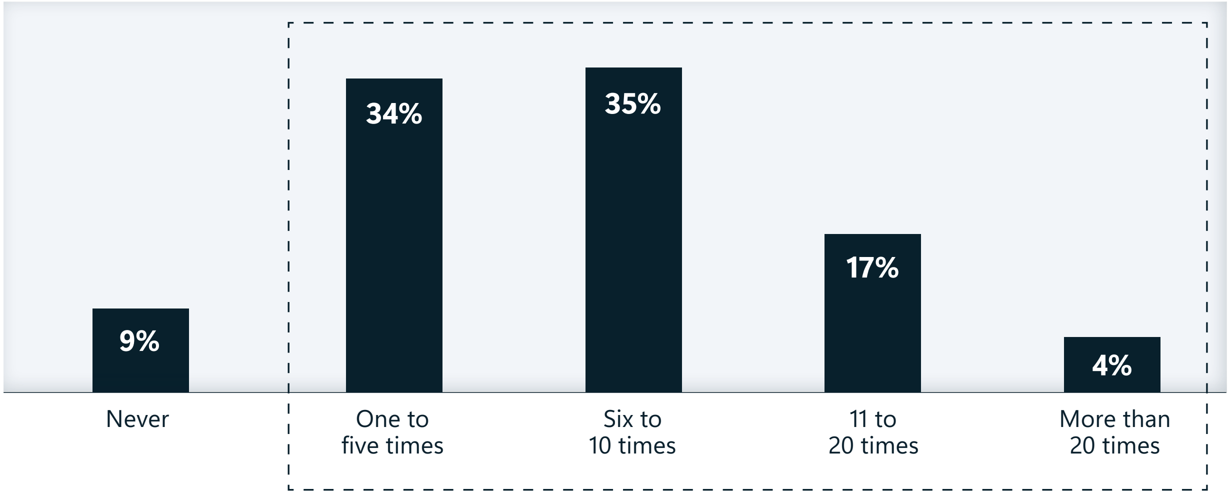
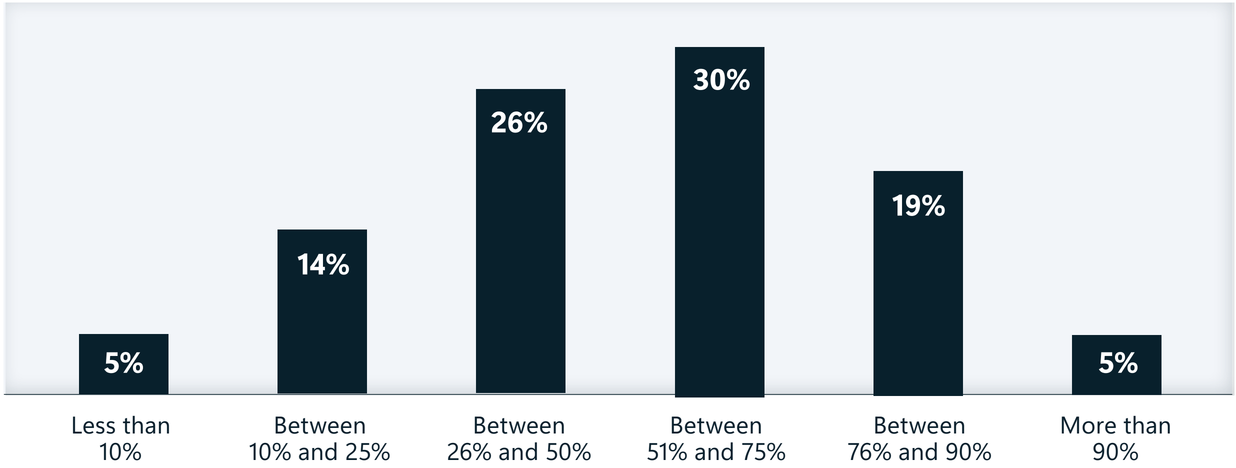


Figure 08

Considering just the true positive/high-fidelity alerts the SOC team handles, what percentage would you say are associated with a known vulnerability (as opposed to an emerging one)? (Percent of respondents, N=300)



How concerned are you that your SOC is not discovering new and emerging threats/vulnerabilities quick enough to manage enterprise risk effectively? (Percent of respondents, N=300)

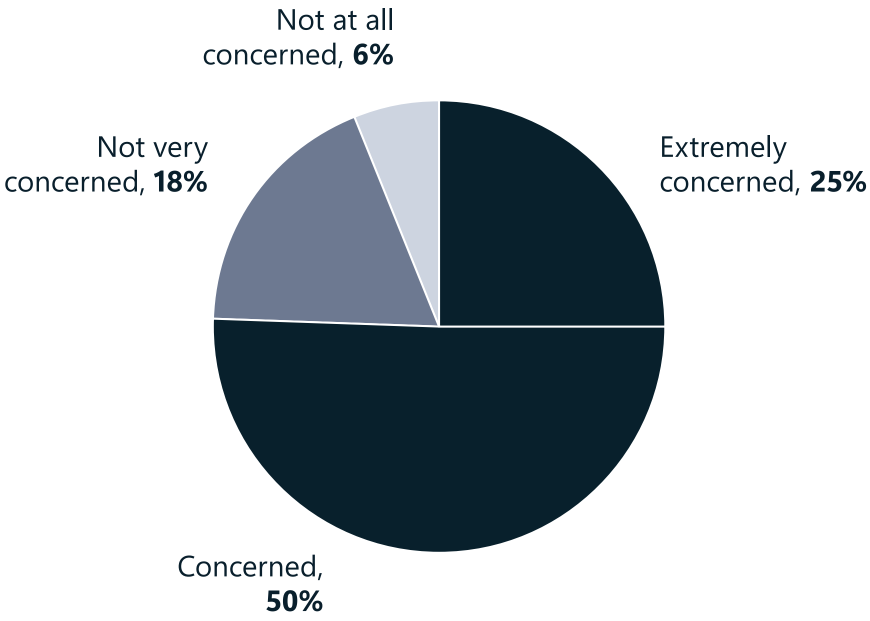


Figure 09

What percentage of IoC lookups within your organization do you estimate could be automated with the right tools? (Percent of respondents, N=300)

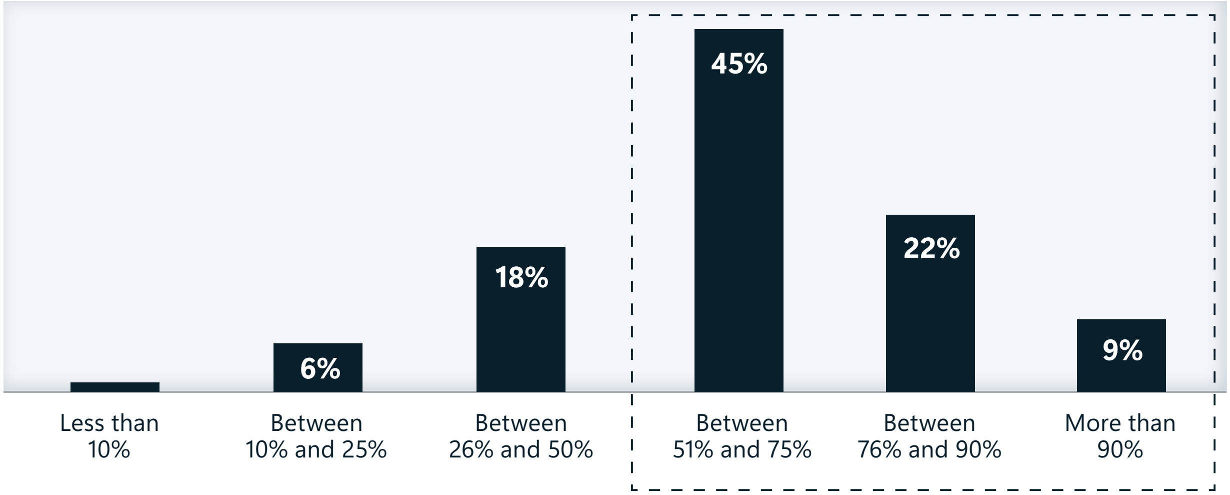


Figure 10

What level of impact do you believe innovations in AI and automation within security tools will have on reducing the amount of manual effort required in the following areas over the next few years? (Percent of respondents, N=300)

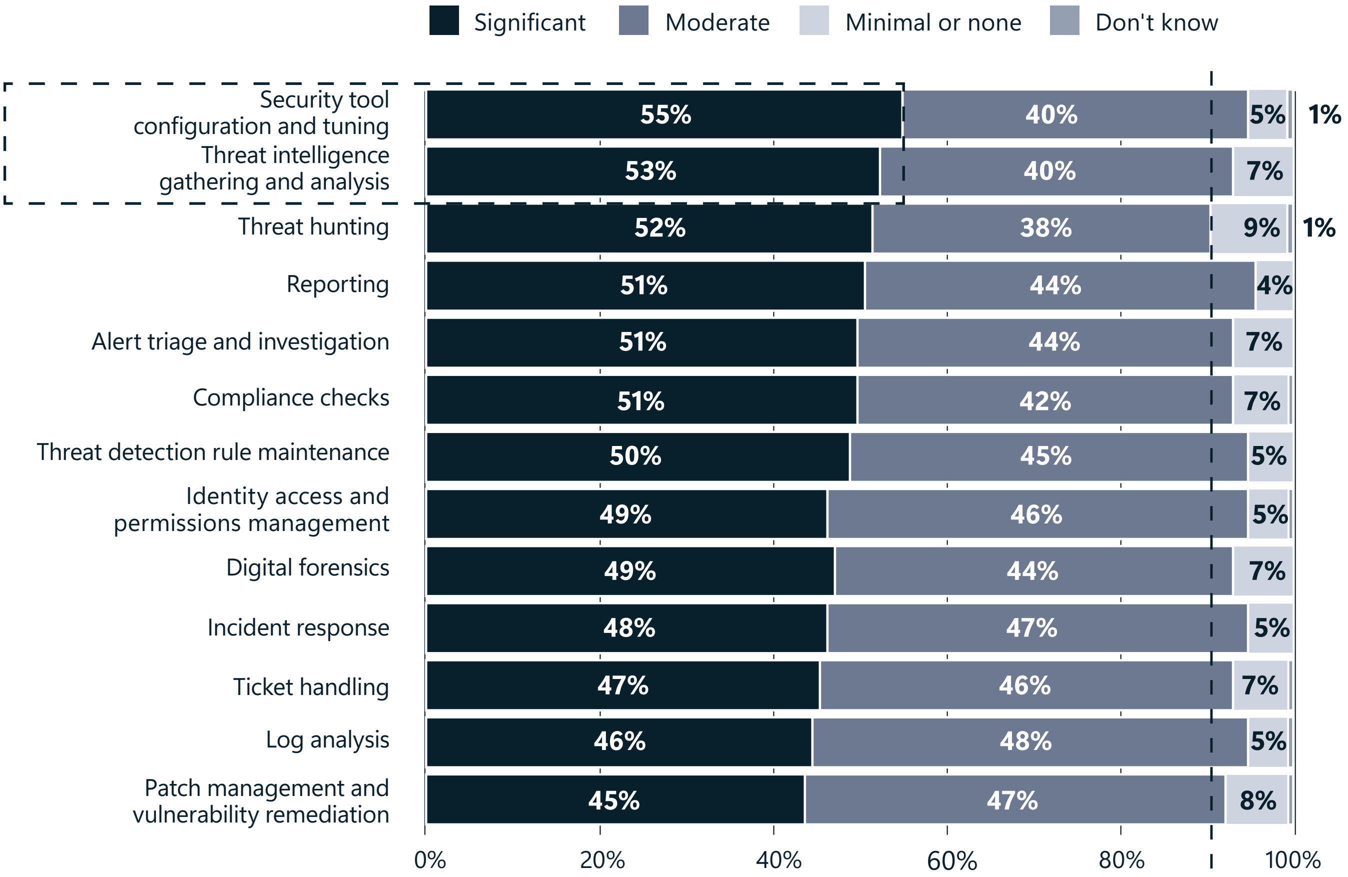


Figure 11

Generally speaking, which best describes how your organization wants to deploy SOC-focused AI agents? (Percent of respondents, N=300)

SOC teams seek flexibility in AI agent deployment

Respondents report a preference for the ability to build their own agents in a studio environment (vs. pre-built agents) by a nearly 2:1 margin.

A studio approach resonates both at the C-level (70%) and along middle managers/practitioners (75%) vs. directors-VPs (43%).

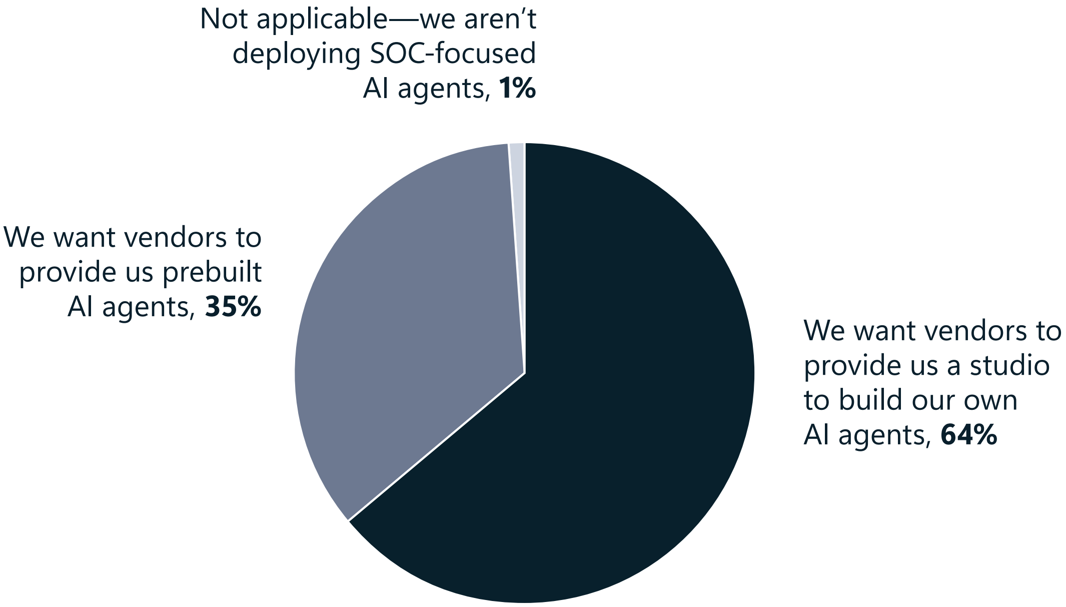


Figure 12

Thinking about your entire security data set, what approximate percentage typically resides in each of the following locations? (Mean percentage of data)

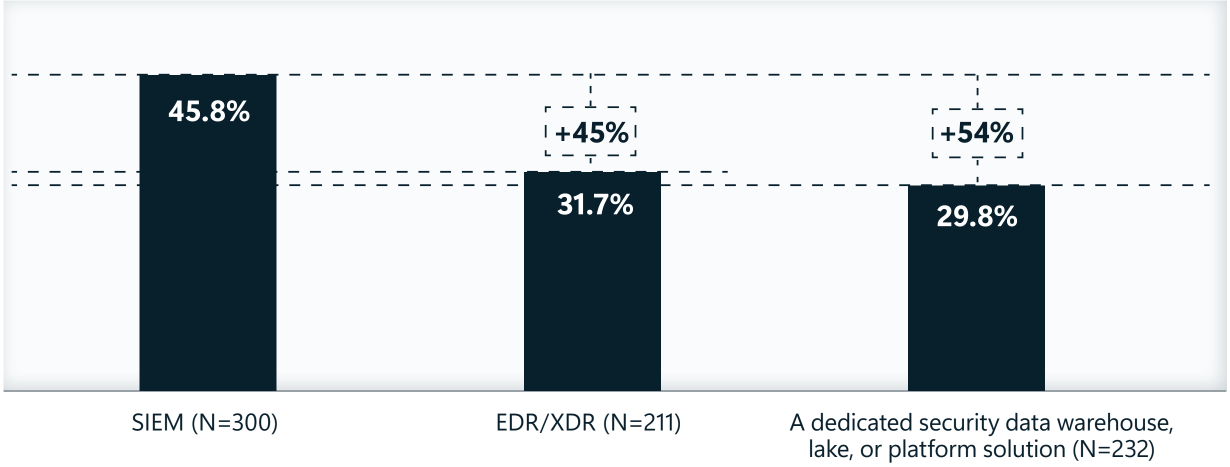
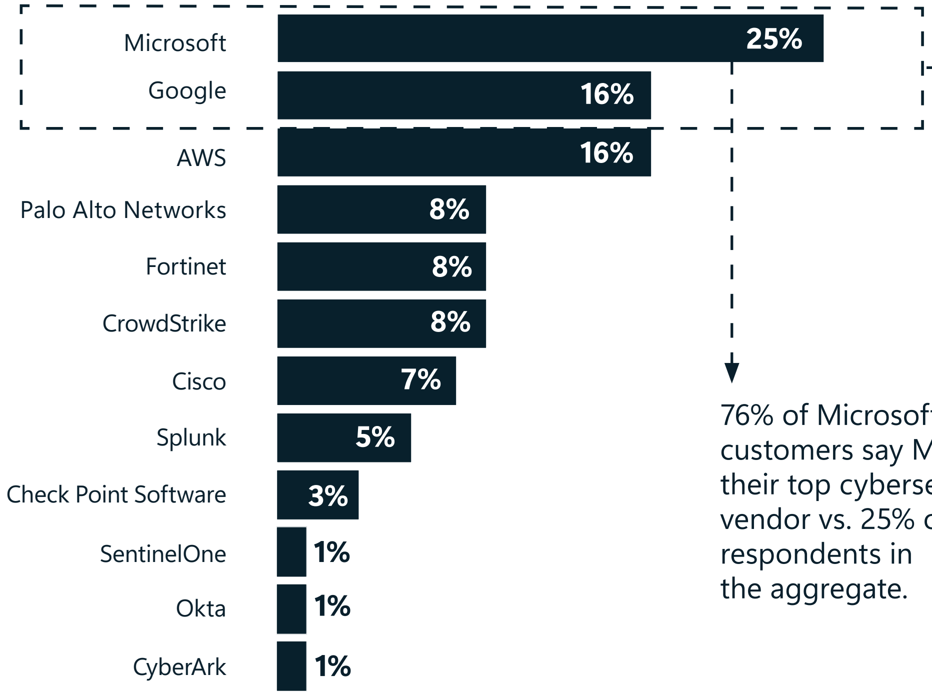
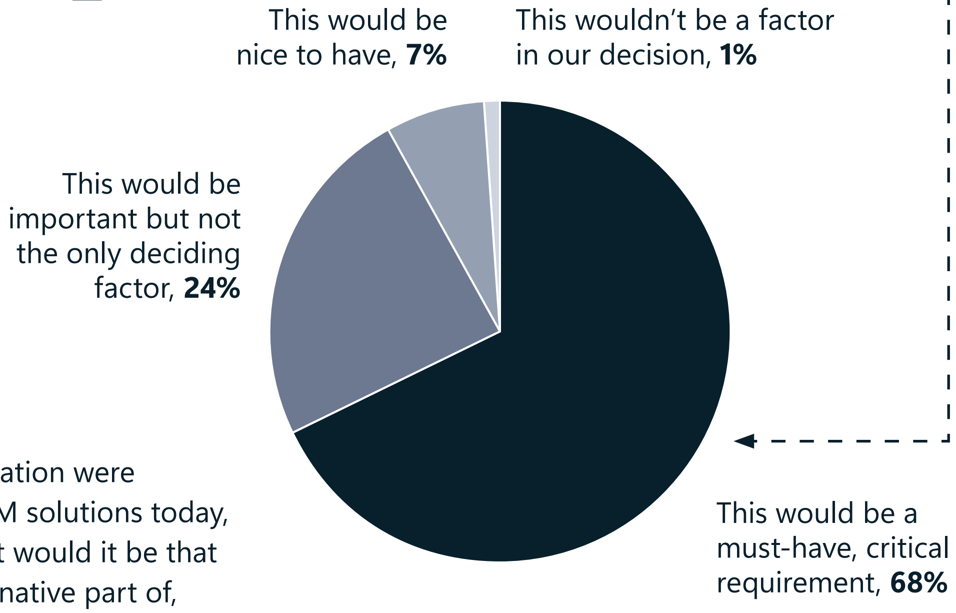


Figure 13

Who would you say is your organization’s top vendor of cybersecurity technologies?
(Percent of respondents, N=300)



76% of Microsoft Sentinel customers say Microsoft is their top cybersecurity vendor vs. 25% of respondents in the aggregate.



If your organization were evaluating SIEM solutions today, how important would it be that the SIEM be a native part of, and provided by, your most critical security tool vendor?
(Percent of respondents, N=300)

Figure 14

Consider the typical SOC practitioner at your organization and estimate the percentage of time they spend on reactive tasks versus proactive tasks. (Mean, N=300)

SOC teams tend to split their time equally between reactive and proactive tasks

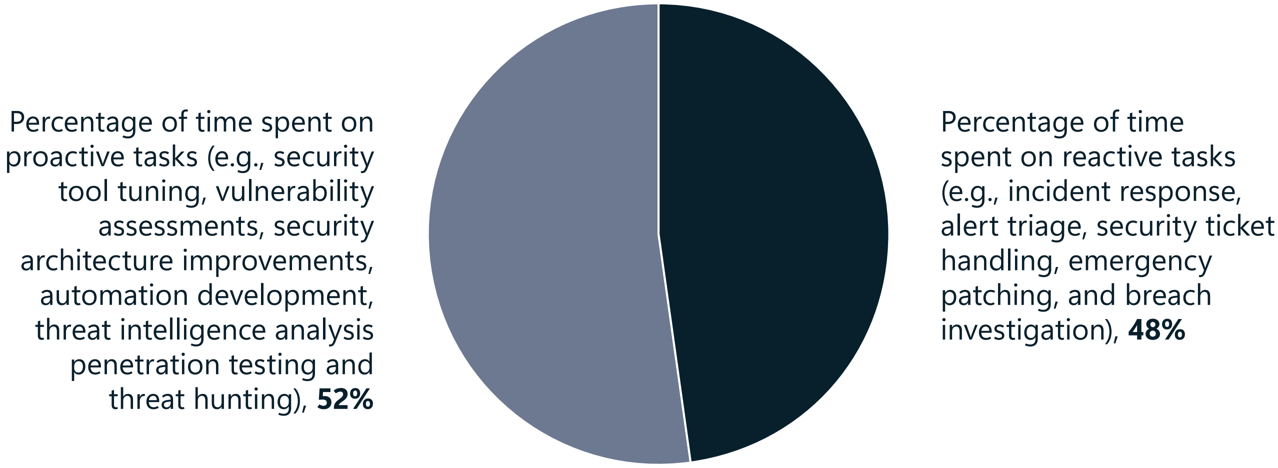
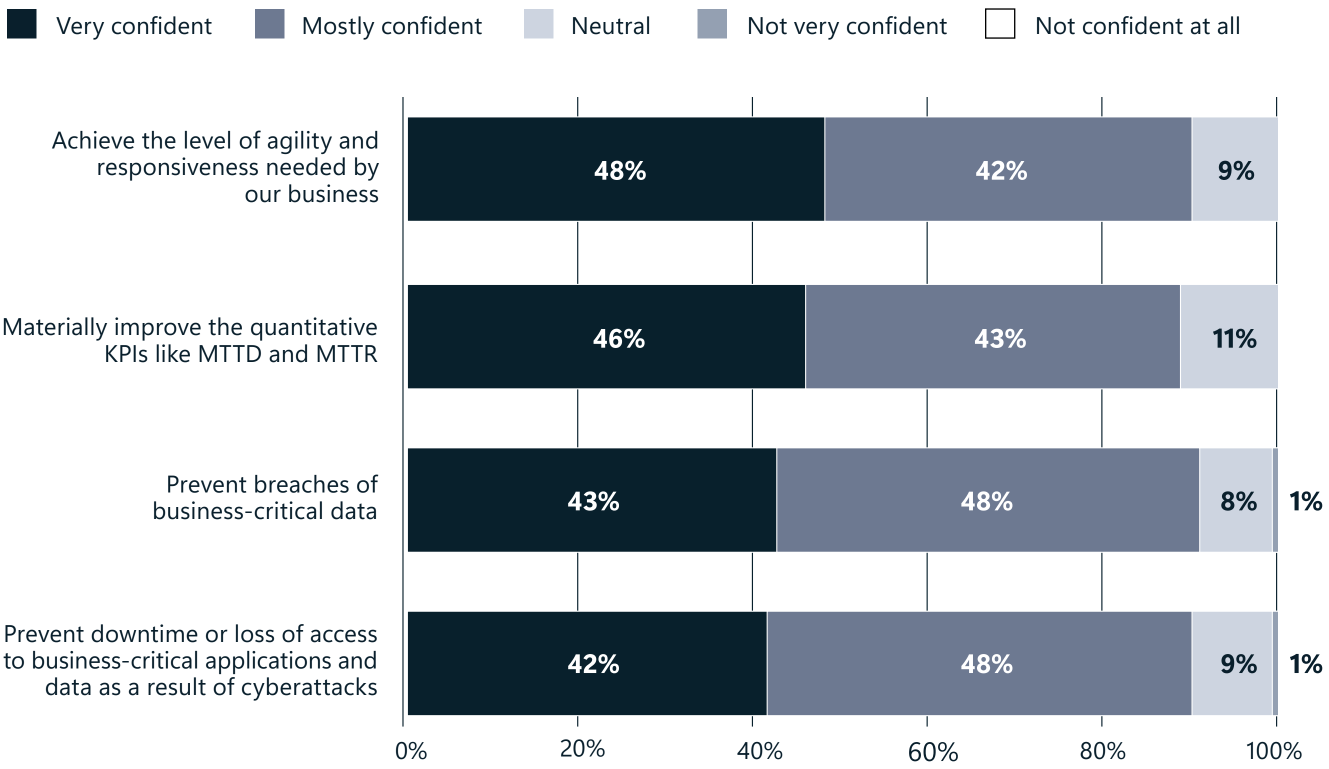


Figure 15

SOC teams are confident in their ability to execute in the future

Looking ahead over the next 12 months, how confident are you in your SOC team's ability to...
(Percent of respondents, N=300)


Very confident
Mostly confident
Neutral
Not very confident
Not confident at all
Achieve the level of agility and responsiveness needed by our business
Materially improve the quantitative KPIs like MTTD and MTTR
Prevent breaches of business-critical data
Prevent downtime or loss of access to business-critical applications and data as a result of cyberattacks