

The Race to Support Overwhelmed Security Teams With XDR and SOC Modernization

Dave Gruber | Principal Analyst

ENTERPRISE STRATEGY GROUP

MARCH 2024

Research Objectives

Security operations grow more difficult each year due to issues like the persistent threat landscape, a growing attack surface, and the volume and complexity of security alerts. Additionally, many SOC teams remain understaffed and lack advanced security operations skills. To address these challenges, CISOs are open to evaluating new technologies in areas like advanced analytics for threat detection and process automation for incident response.

Additionally, many organizations are considering security operations tools consolidation. These efforts will likely lead to the proliferation of security operations and analytics platform architecture (SOAPA) strategies. SOC technology consolidation and integration efforts are aimed at improving security efficacy, reducing operational overhead, and building a SOC technology architecture that can keep up with the pace and scale of hybrid IT.

Threat detection and response priorities include operationalizing threat intelligence, improving the integration of asset management data with security operations, and improving alert triage and prioritization. This indicates that existing SOC operations activities are inadequate, and organizations will subsequently spend accordingly to address current limitations.

To gain further insight into these trends, TechTarget's Enterprise Strategy Group surveyed 374 IT and cybersecurity professionals at organizations in North America (US and Canada) responsible for or involved with security operations technology and processes.

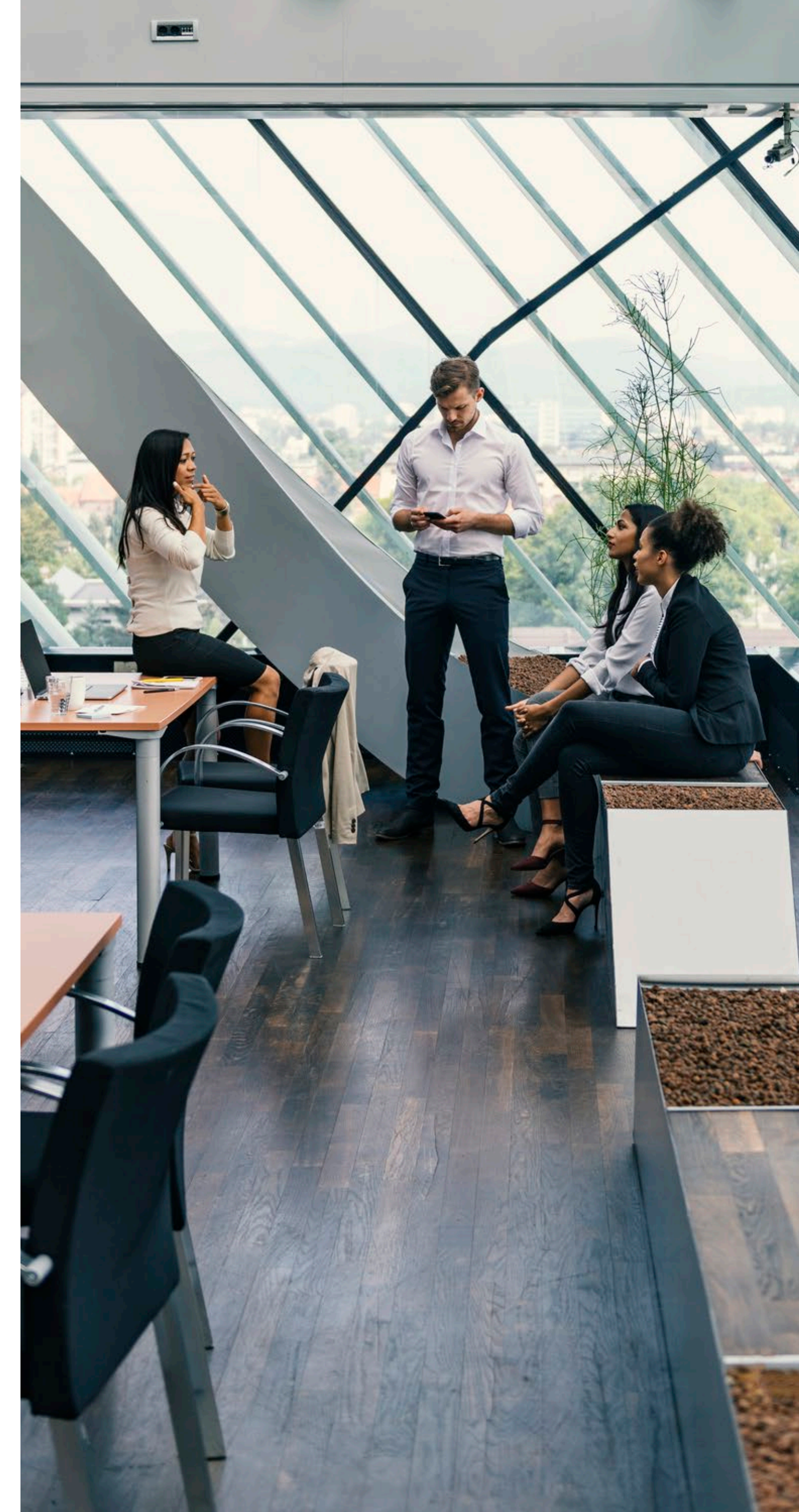
THIS STUDY SOUGHT TO:

..... **Examine** the people, processes, and technology strategies supporting security operations modernization as well as challenges encountered.


..... **Identify** key requirements and expectations for both products and managed services for XDR and SOC modernization.

..... **Determine** current perceptions of and roles for XDR as a component of security operations modernization efforts.

..... **Explore** strategies used to automate triage, speed investigations, and find unknown threats.



KEY FINDINGS



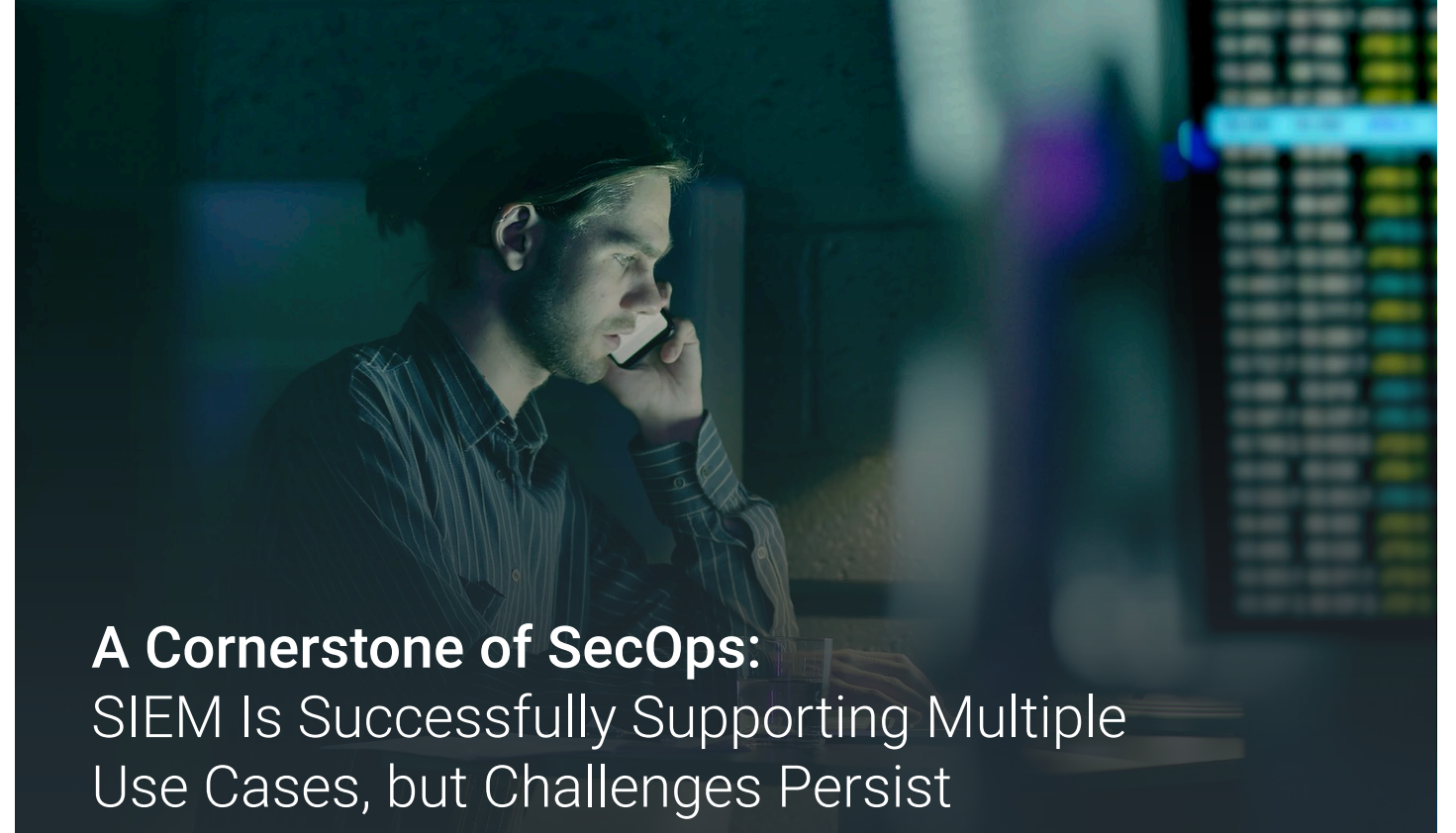
The State of SecOps:
Despite Some Improvement, Security Teams Still Struggle to Keep up With IT Investments

PAGE 4



Security Tools and Data Stack:
Consolidation Initiatives Continue, as Siloed Tools and Data Persist

PAGE 9




A Cornerstone of SecOps:
SIEM Is Successfully Supporting Multiple Use Cases, but Challenges Persist

PAGE 13




The State of XDR:
XDR Is Maturing and Perceptions Are Changing

PAGE 16



Automation and GenAI:
Automation Is a Priority, Beginning With the Basics

PAGE 21



The People Behind Security:
Hybrid Staffing Models Are the 'New Norm'

PAGE 25



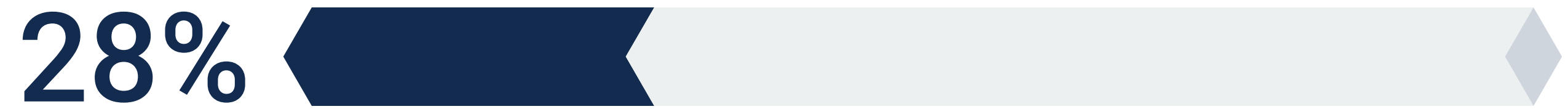
The State of SecOps:

Despite Some Improvement, Security Teams Still Struggle to Keep up With IT Investments

Security Operations Continue to Challenge Many Organizations

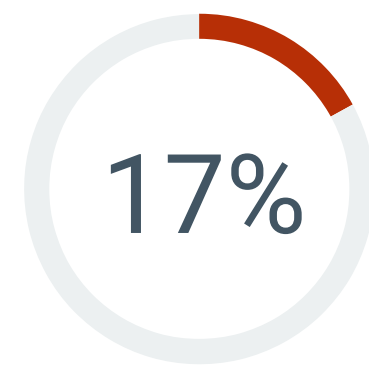
While some improvement is reported, almost half (45%) of organizations say they still struggle with their security operations program. When asked why, the five most common reasons included a growing, changing attack surface; a changing threat landscape; the increasing volume and complexity of security alerts; an overwhelming amount of security data to collect and process; and difficulty keeping pace with the operational needs of SecOps technologies.

Maybe most concerning is that when asked what the greatest, primary security operations challenges were, first on the list was that cybersecurity teams spend most of their time addressing high-priority issues, leaving little to no time to make strategy and process improvements. Indeed, while investments continue to be made to address many of these challenges, progress in resolving them is slow.

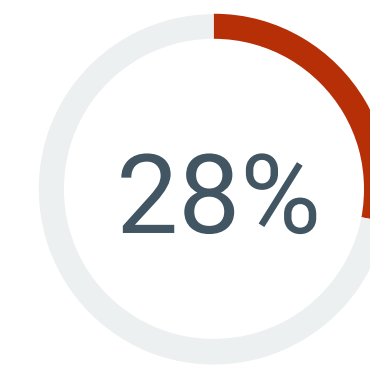


of organizations believe their cybersecurity team spends most of its time **addressing high-priority/emergency issues** and not enough time on strategy and process improvement.

Level of security operations difficulty today versus two years ago.



Security operations are significantly more difficult today than they were two years ago



Security operations are somewhat more difficult today than they were two years ago

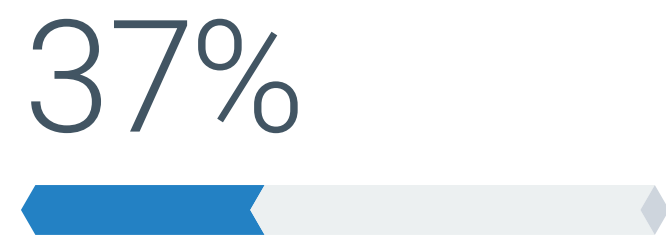
Top five reasons security operations are more difficult than they were two years ago.



The attack surface is continuously growing, changing, and evolving



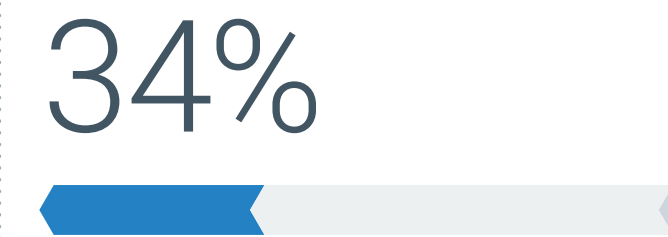
The threat landscape is evolving and changing rapidly



The volume and complexity of security alerts have increased



We collect and process more security data today than we did two years ago



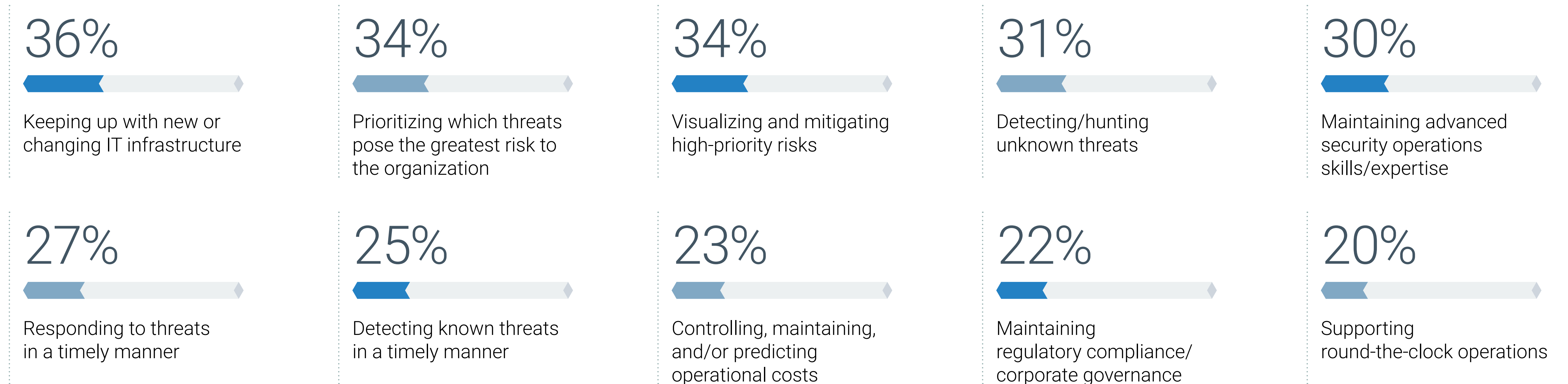
It is difficult to keep up with the operational needs of security operations technologies

Weakest SecOps Areas Include Keeping Pace With IT Infrastructure, Lack of Risk Perspective, and Complex Investigations

As the pace of change within IT infrastructure races forward, security teams often struggle to keep up. With a more complex infrastructure to protect, and continuing silos of operating infrastructure, prioritizing which threats pose the greatest risk across the organization is a weak point for many. A more integrated, comprehensive risk perspective is also needed to visualize and mitigate high-priority risks.

Meanwhile, many struggle to maintain the advanced security operations skills and expertise required to detect and investigate modern threats.

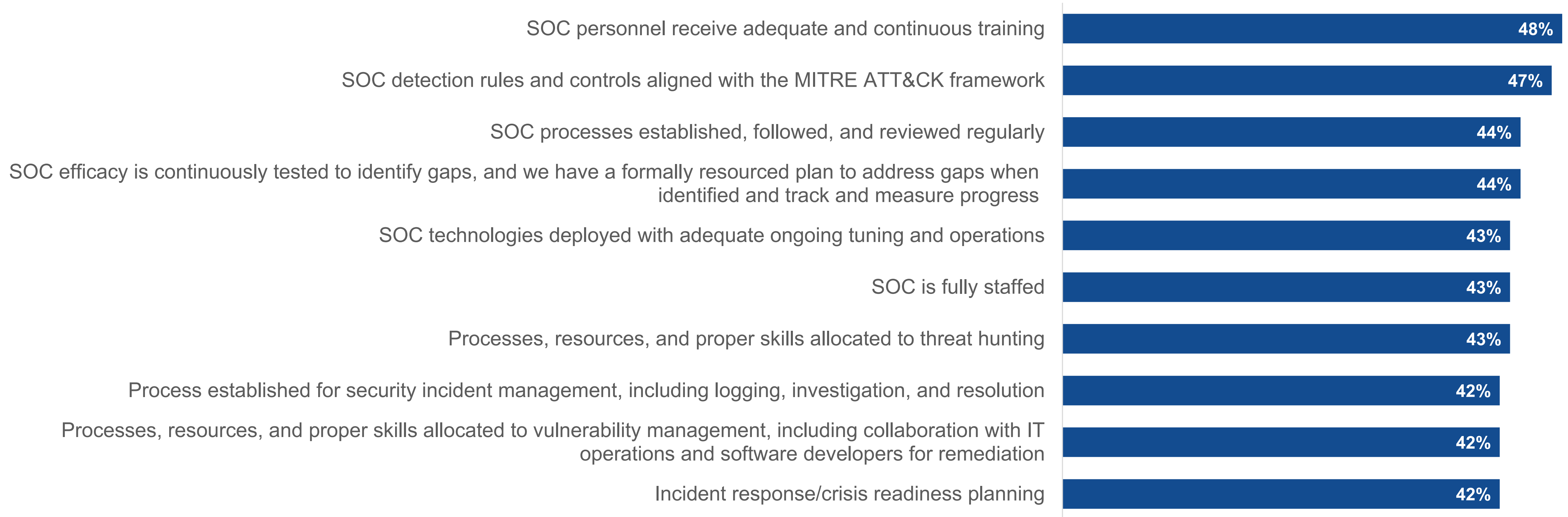
Weakest areas of security operations.



Where Do Organizations Need to Work on Their SOCs?

Security teams have an overwhelming amount of work to do to improve their security operations centers. When asked to rate the status of their organization’s SOC across a number of areas, the four most commonly identified as needing more work were operationalizing SOC personnel training, aligning SOC detection rules and controls with the MITRE ATT&CK framework, testing SOC efficacy to identify and address gaps, and formalizing, following, and regularly reviewing SOC processes.

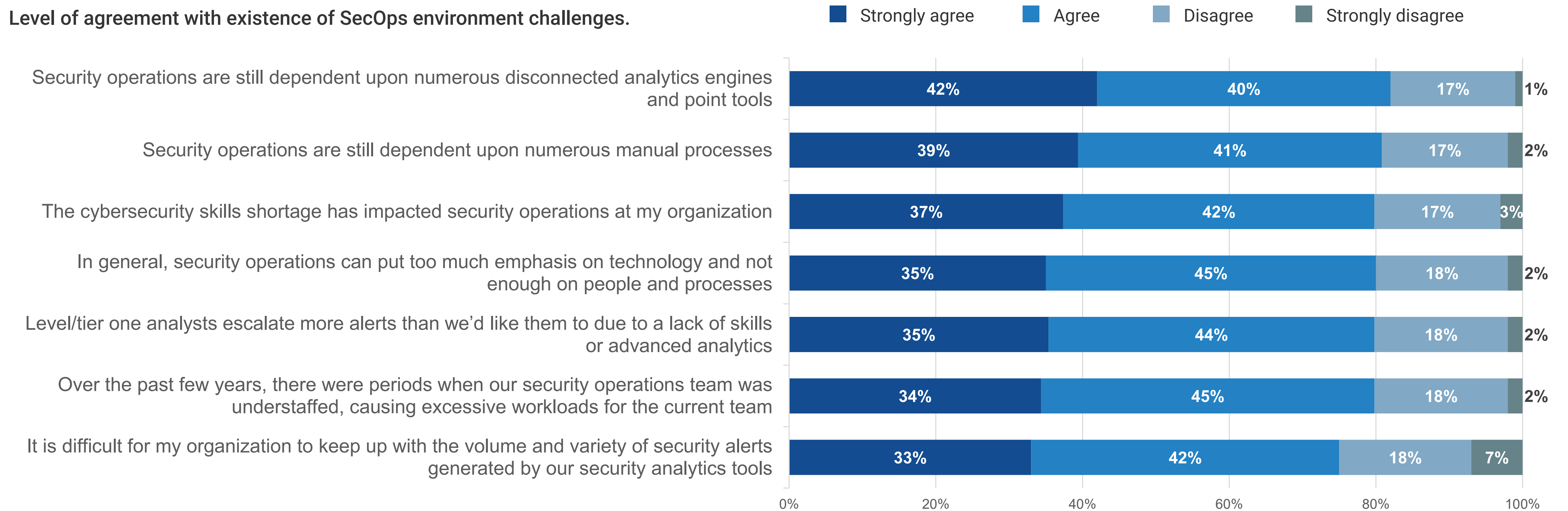
Top ten aspects of security operations centers that need work.



Common SecOps Challenges Include Overabundance of Alerts and Manual Processes, Compounded by Understaffing

With 75% of organizations reporting difficulty in keeping up with the volume and variety of security alerts generated by their many security tools, and 79% of organizations reporting that their tier one analysts are escalating more alerts than they'd like due to a lack of skills or advanced analytics, modernizing security operations is a key priority for many. Security leaders also report that there have been periods of time over the past few years when their security operations teams were understaffed, with 79% reporting continuing cybersecurity skills challenges. This study further surfaces the need to apply more automation across security operations, with 80% of organizations reporting that their security operations are still dependent on numerous manual processes, and 82% of organizations reporting that they are still dependent on numerous, disconnected analytics engines and point tools.

Level of agreement with existence of SecOps environment challenges.



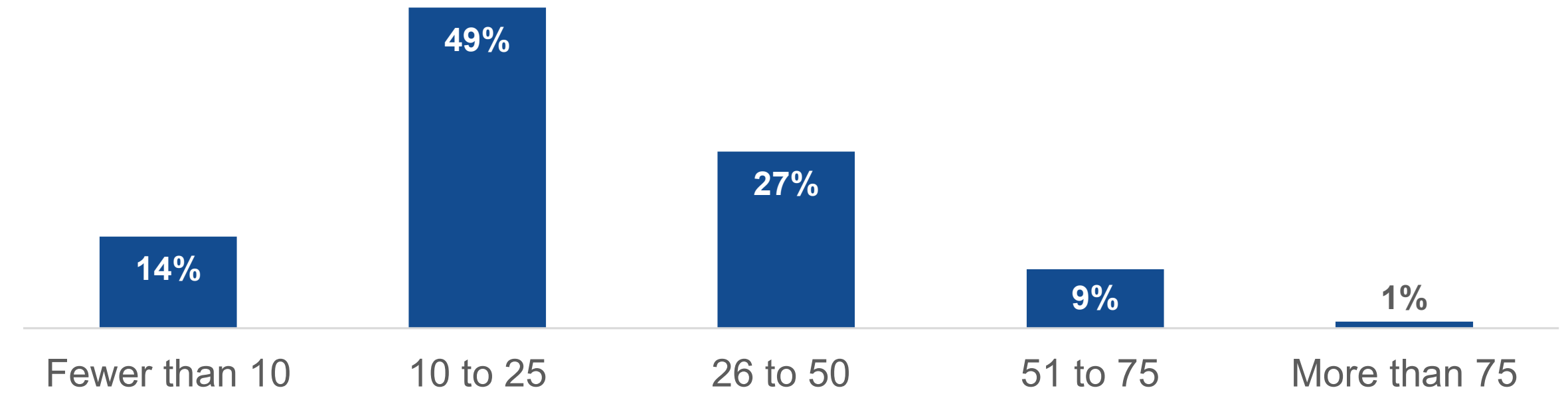
The image depicts a digital cityscape composed of numerous glowing, three-dimensional cubes. Each cube is illuminated with a blue and red light, suggesting data or network activity. The cubes are arranged on a dark blue background with a grid of white lines and red circuit-like paths. A prominent feature is a large, glowing red padlock icon on the top surface of a central cube, symbolizing security or data protection. The overall aesthetic is high-tech and futuristic.

Security Tools and Data Stack:
Consolidation Initiatives Continue, as Siloed
Tools and Data Persist

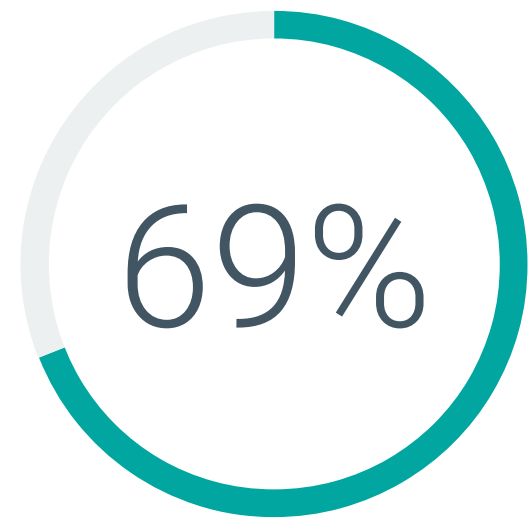
An Overabundance of SecOps Tools Continues, Driving Consolidation Initiatives

Organizations are seeing a continuing proliferation in security tools. Specifically, more than one-third (37%) report using in excess of 25 unique technologies to support SecOps. It follows then that consolidation initiatives are prevalent for more than two-thirds (69%) of organizations. In parallel, as the adoption of new security tools continues, consolidation is an important component of an ongoing, long-term strategy required to continuously optimize security operations.

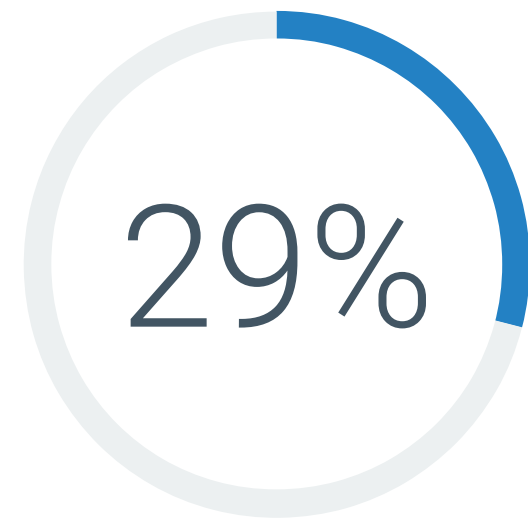
Number of tools and technologies used for security operations.



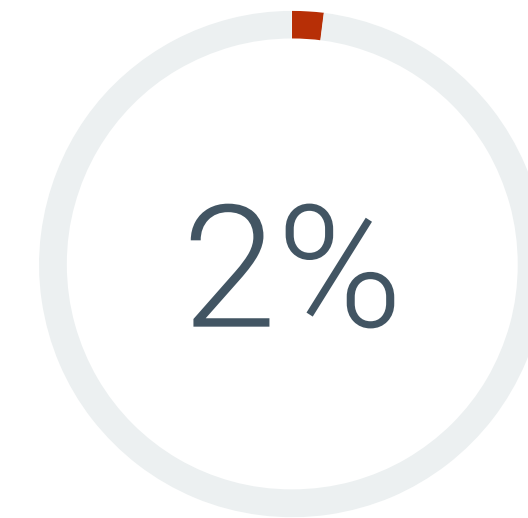
Consolidation plans for SecOps tools.



We are **actively** consolidating/integrating our security operations tools



We are **considering** consolidating/integrating our security operations tools

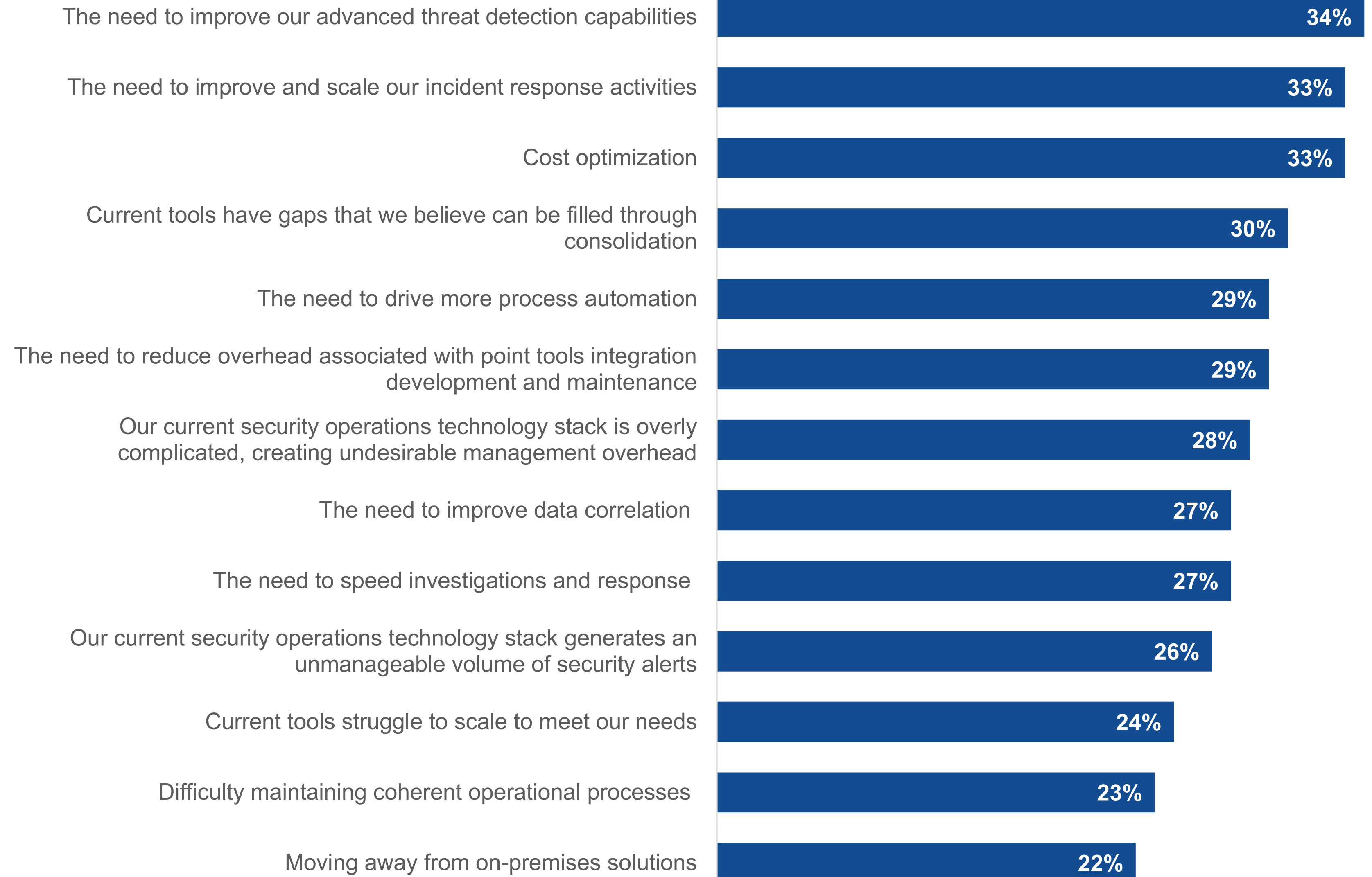


We have **no plans** to consolidate/integrate our security operations tools

SecOps Tool Consolidation Drivers

Specific consolidation objectives are most often focused on improving advanced threat detection and incident response, together with lowering or optimizing both the outright tools costs and the costs associated with integration development and maintenance. Others see opportunities to close gaps in coverage and reduce alert volume through further consolidation.

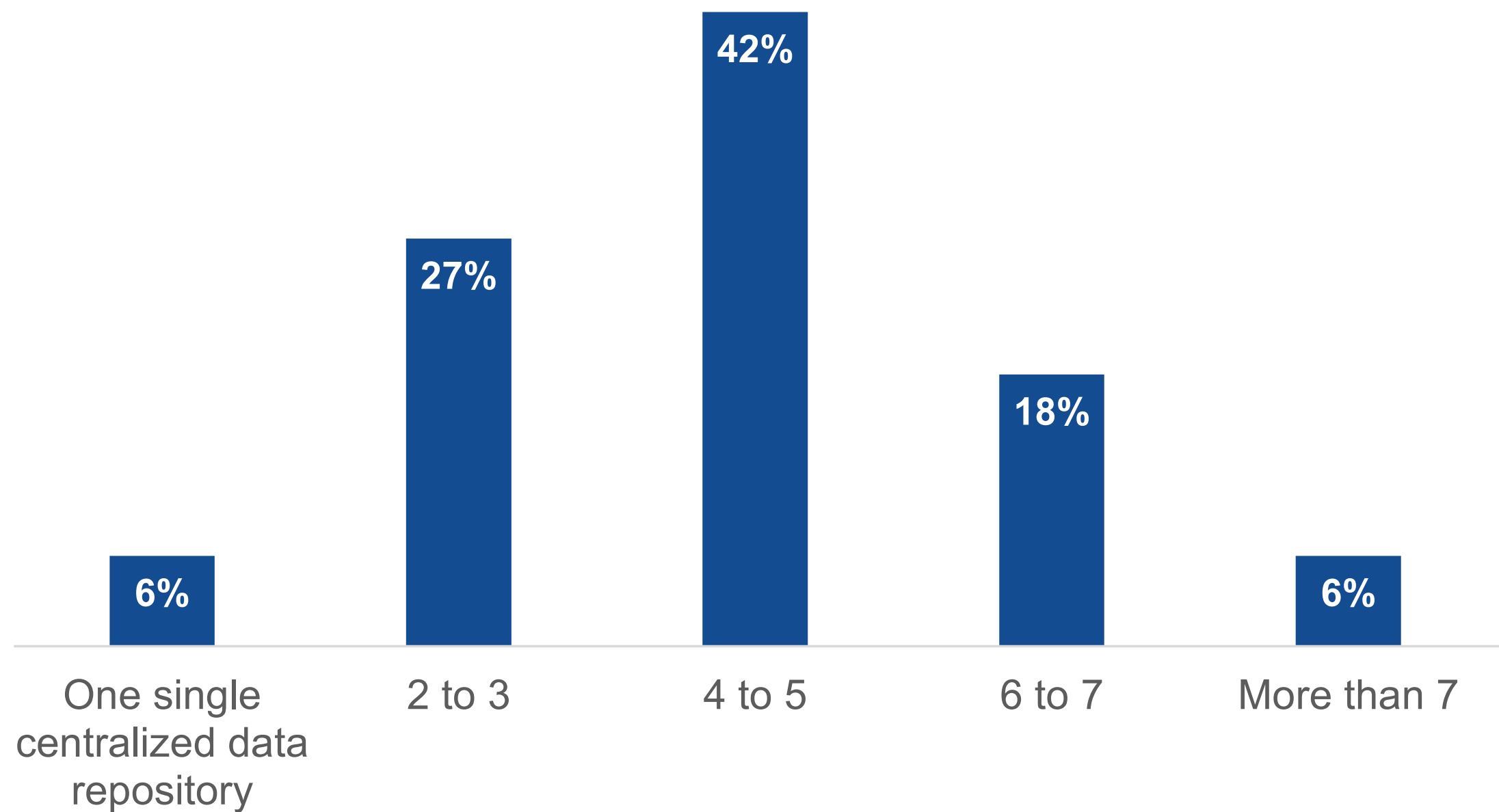
Drivers for SecOps tools consolidation.



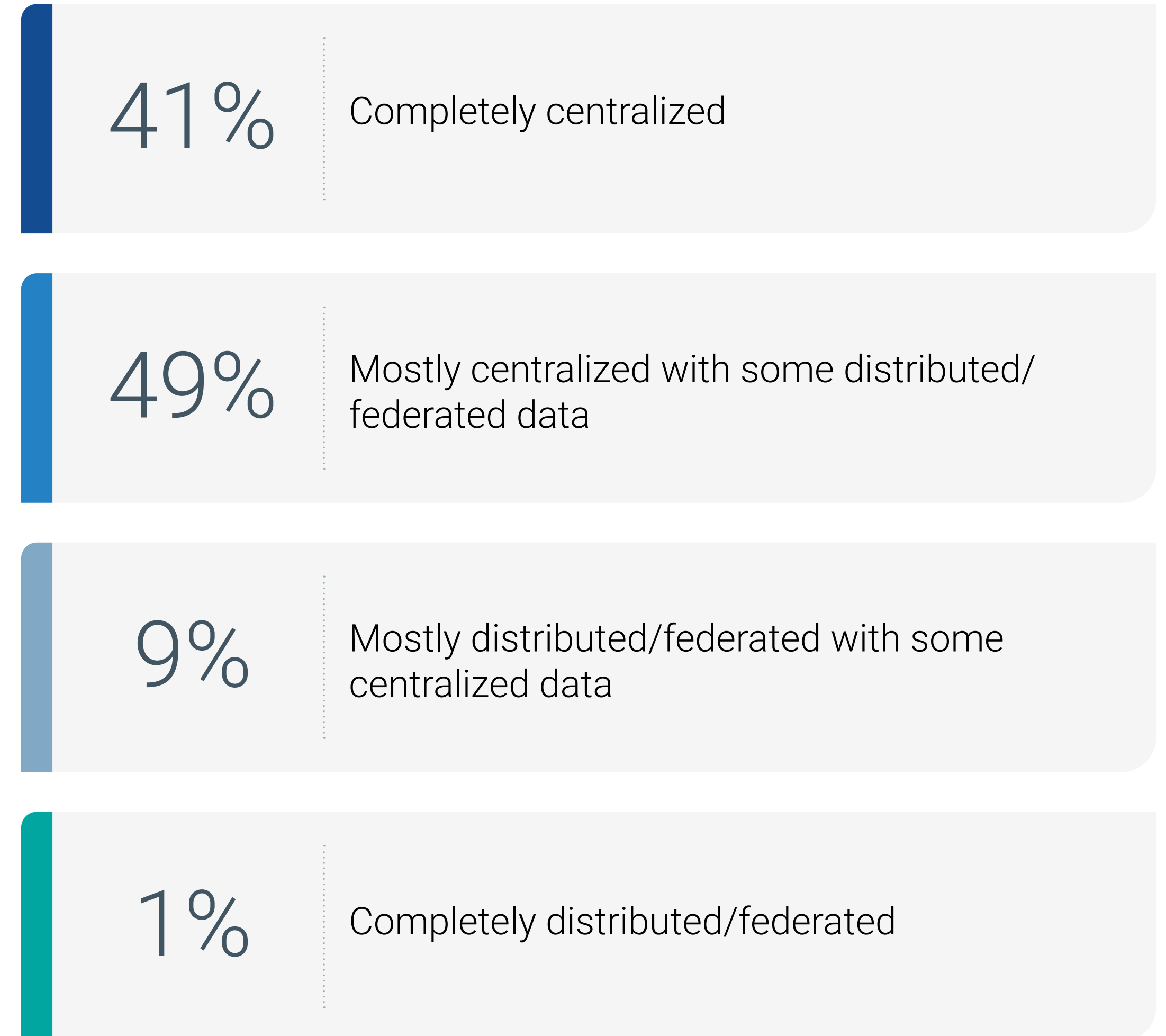
Most Desire Data Consolidation

Aligned with tools consolidation initiatives, a more centralized security data strategy is the vision for most. However, progress is slow, as demonstrated by the two-thirds of organizations currently maintaining four or more security data repositories. Looking ahead, a federated security data architecture could be a more realistic operating model for most, as tools, platforms, and architectures continue to evolve over time.

Number of security data repositories.



Current security data strategy.



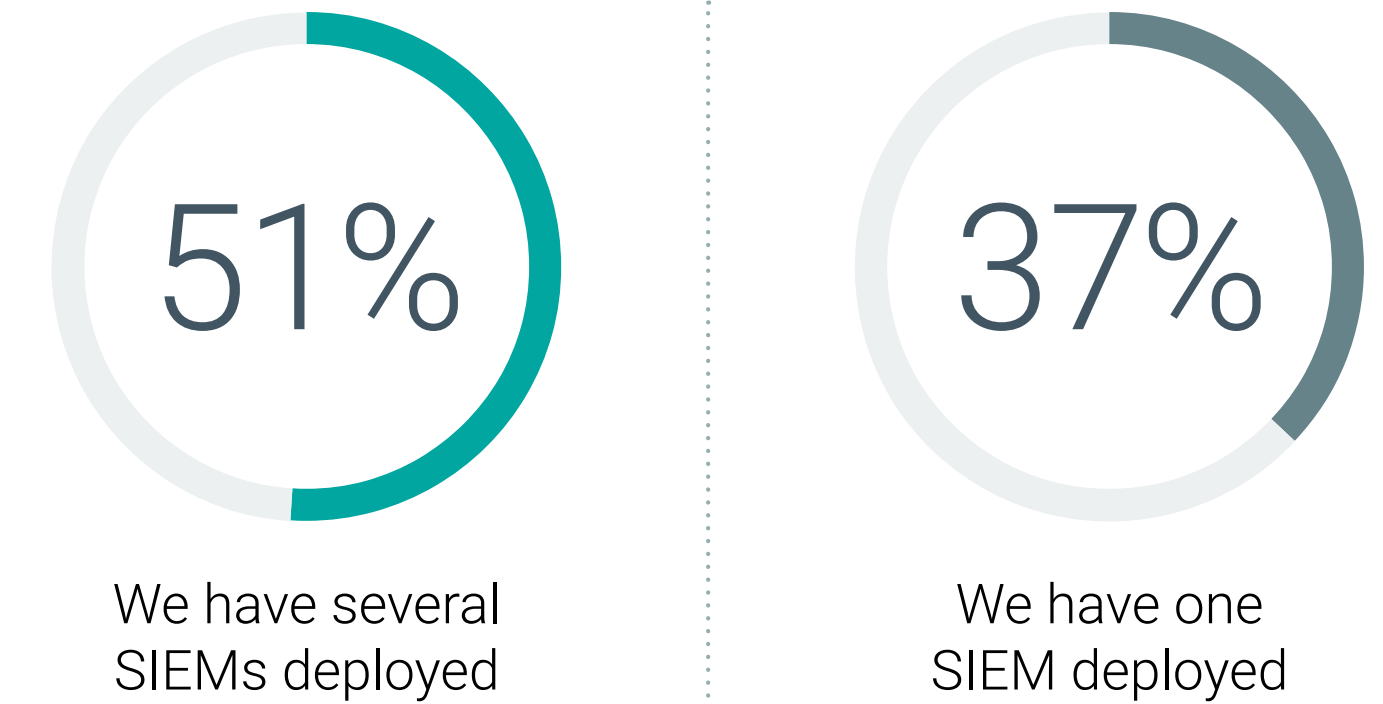
A man with a beard, wearing a striped shirt, is shown in profile, talking on a mobile phone. He is sitting at a desk in a server room or data center. In the background, there are several computer monitors displaying data, with one monitor on the right showing a grid of yellow and blue cells. The lighting is dim and blue-toned, typical of a server room.

**A Cornerstone of SecOps:
SIEM Is Successfully Supporting Multiple
Use Cases, but Challenges Persist**

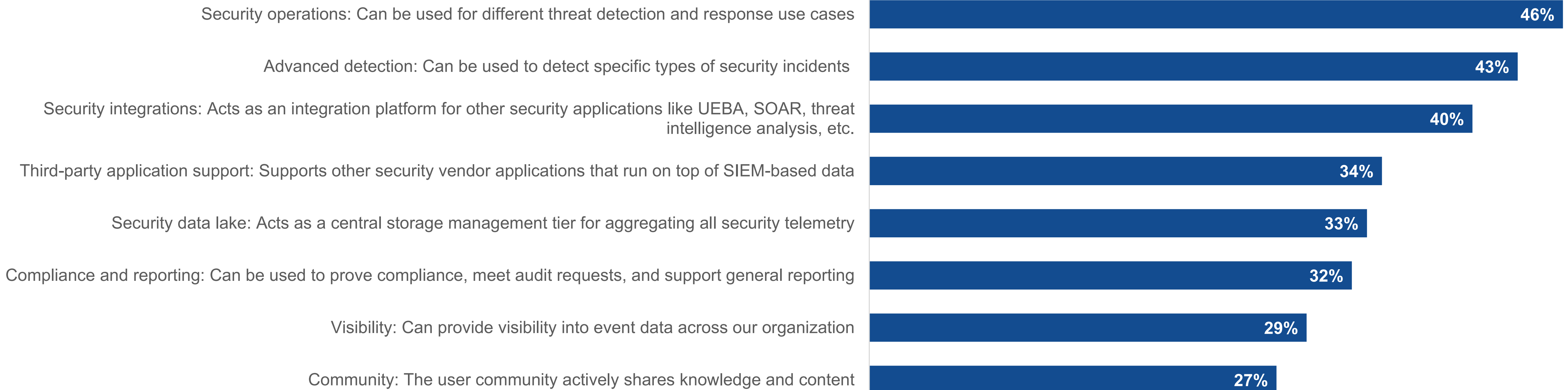
SIEM Usage Is Prolific, and Using More Than One SIEM Is Common

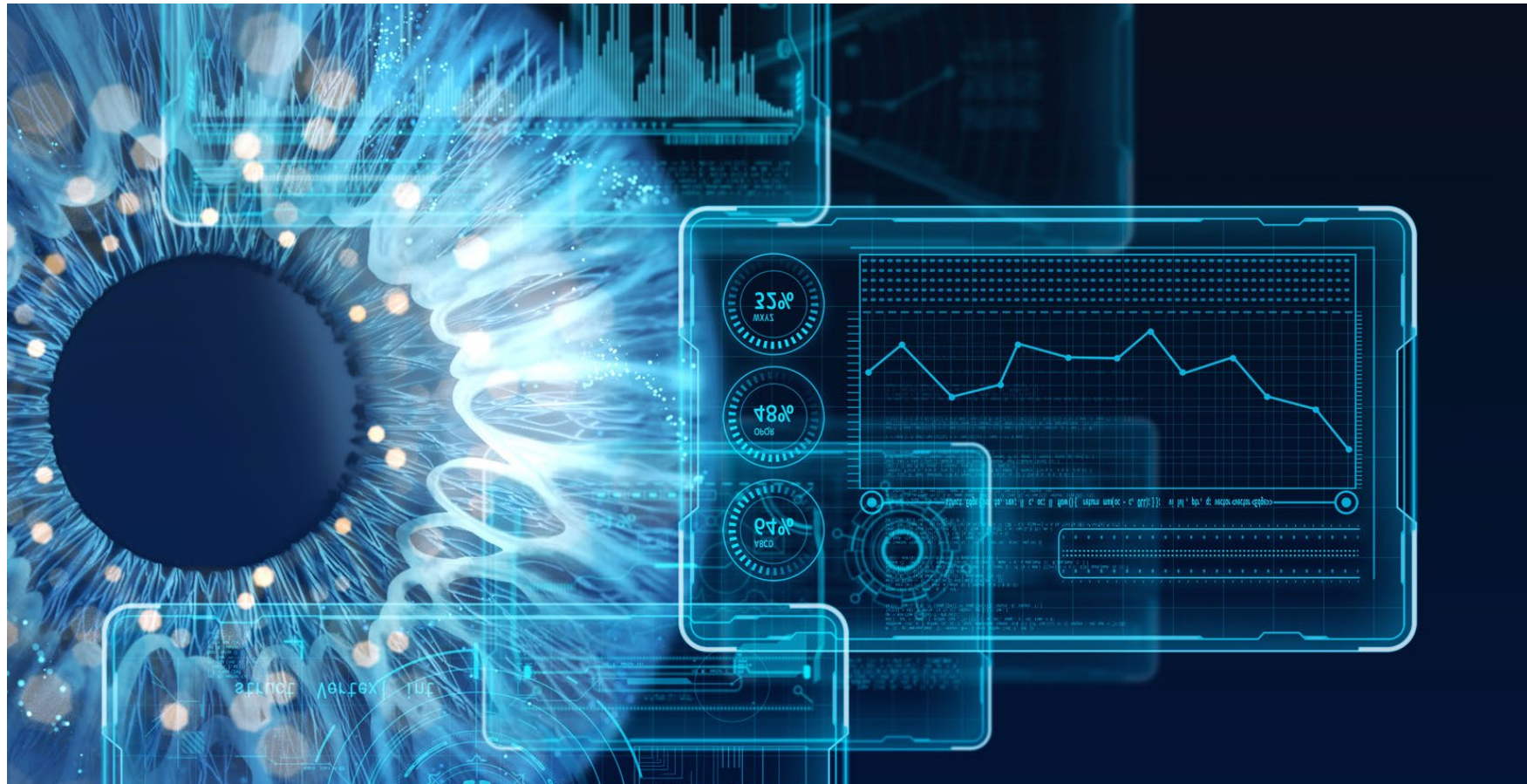
As the basis of data consolidation strategies, security information and event management (SIEM) has become a cornerstone of security operations infrastructure. Indeed, more than half (51%) of organizations report having several deployed, with another 37% having at least one SIEM deployment. While parallel data strategies exist for many, including XDR and custom data lakes, most still see value in continuing SIEM investments despite reported operational challenges. Fortunately, new SIEM operating models have emerged, enabling many to leverage SIEM through an as-a-service model or through a managed service provider, breaking down operational barriers of the past. Additionally, organizations find many valuable attributes in SIEM platforms, most commonly supporting different threat detection and response use cases, providing advanced detection capabilities, and serving as an integration platform for other security applications such as UEBA, SOAR, and threat intelligence analysis, among others.

SIEM deployment status.



Most valuable attributes of SIEM.

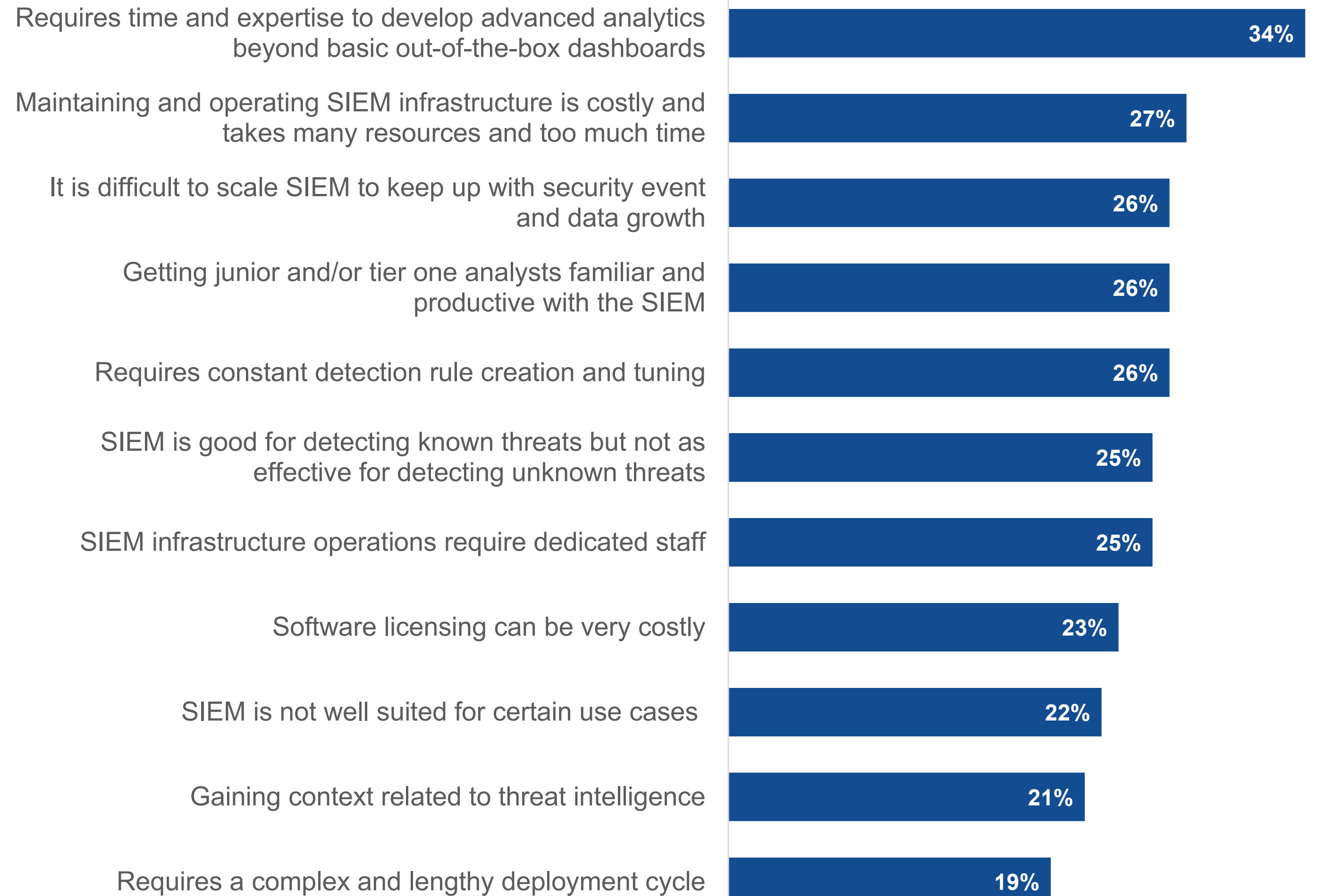




SIEM Challenges Persist

Following all this value are challenges associated with the deployment, management, and maintenance of the SIEM environment. Yet the value surely outweighs the challenges as organizations continue to invest in and leverage SIEMs for many use cases in support of security and IT operations and regulatory and compliance efforts.

Most challenging attributes of SIEM.



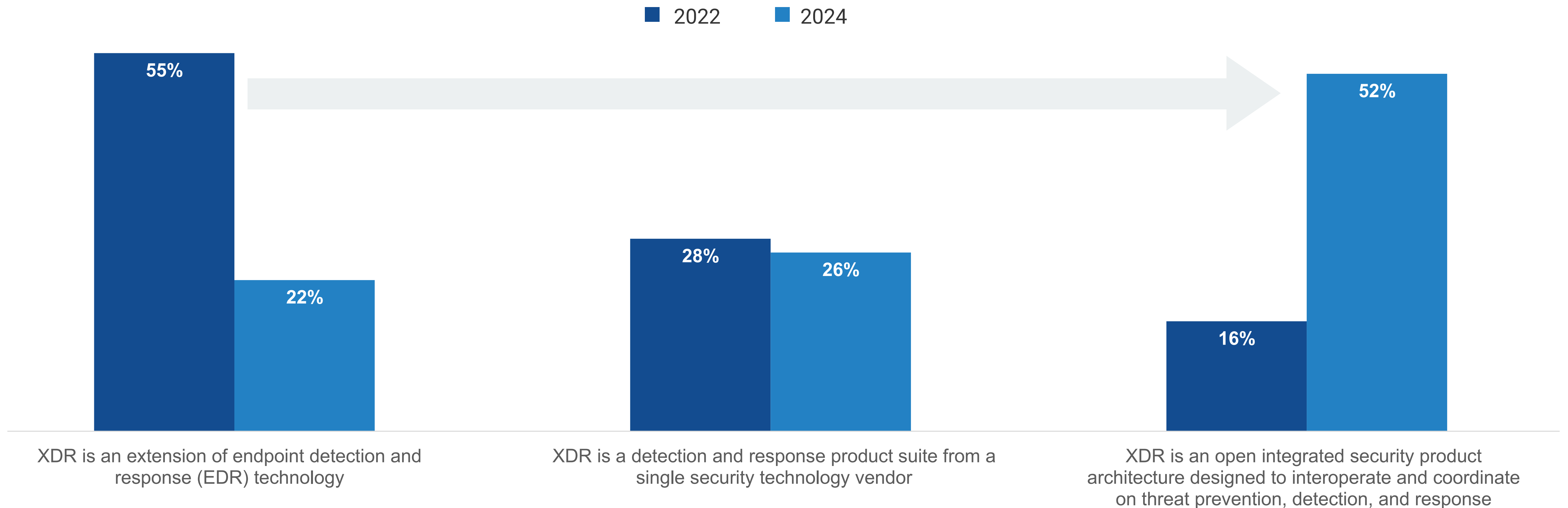


The State of XDR: XDR Is Maturing and Perceptions Are Changing

The Evolving Definition of XDR

After years of massive confusion around the official definition of XDR, the current perspective has now evolved from an early-days view of “an extension to EDR” to “an open, integrated security product architecture designed to interoperate and coordinate on threat prevention, detection, and response.” This move reflects an extensive investment by security vendors upgrading the scope and capabilities of XDR as well as the more practical usage experiences of security operations teams, as XDR has been utilized in support of an expanding attack surface and a more advanced threat landscape.

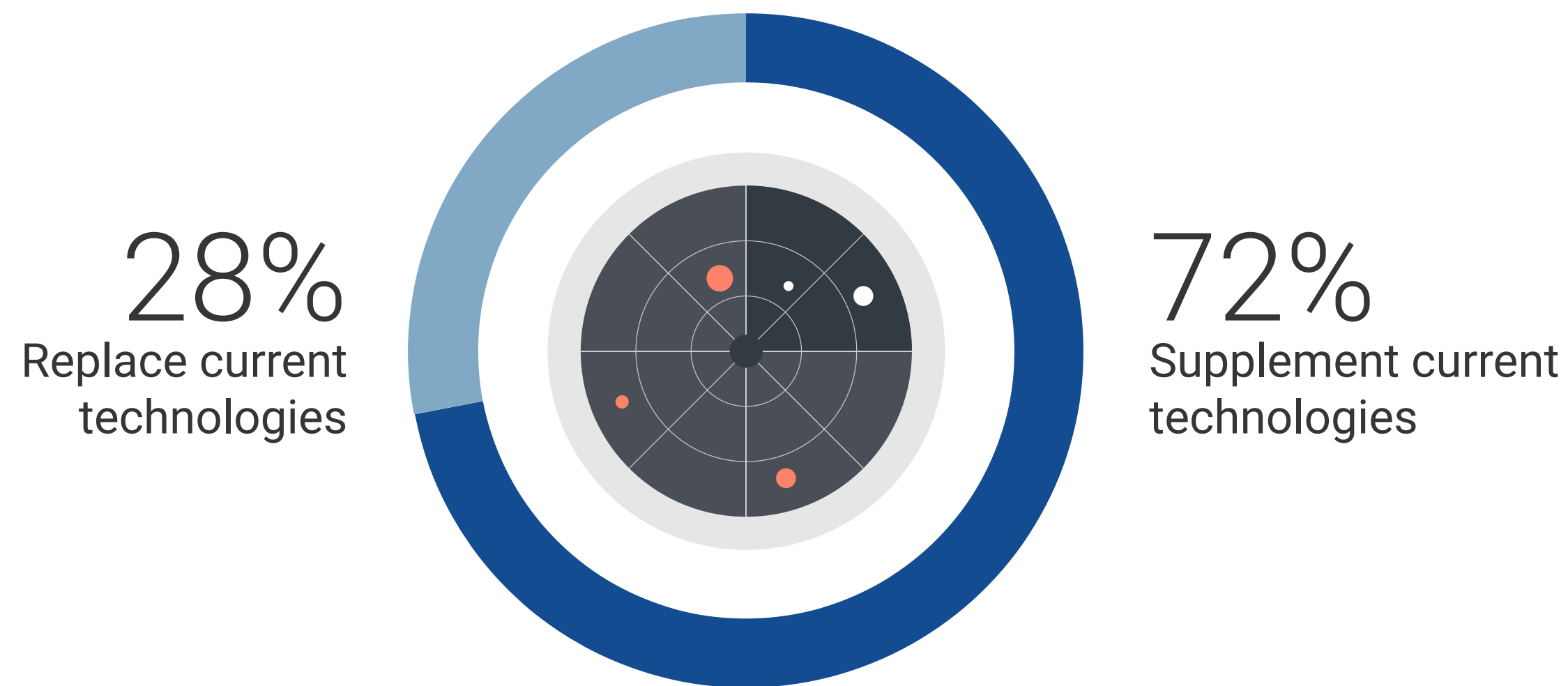
Closest alignment with organizations’ definition of XDR.



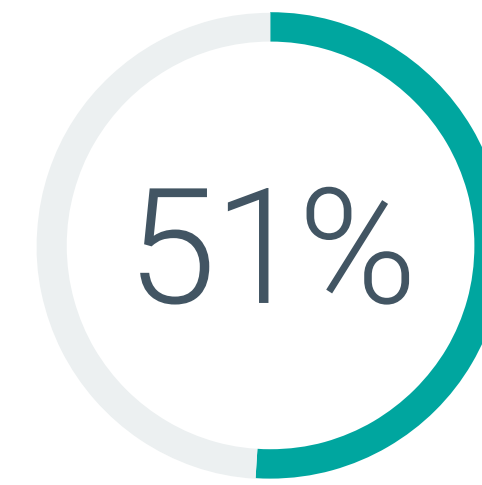
XDR as a Supplement

Once thought of as a possible SecOps panacea, XDR is now considered supplemental to other SecOps tools. As the use of other detection and response tools continues, specialized “DR” solutions will be loosely coupled in a federated XDR model. This will enable security teams to detect advanced attacks using XDR and then drill down leveraging specialized vector-specific tools in support of investigations or forensics activities. XDR and SIEM will further work together in support of the many use cases SIEM supports beyond XDR.

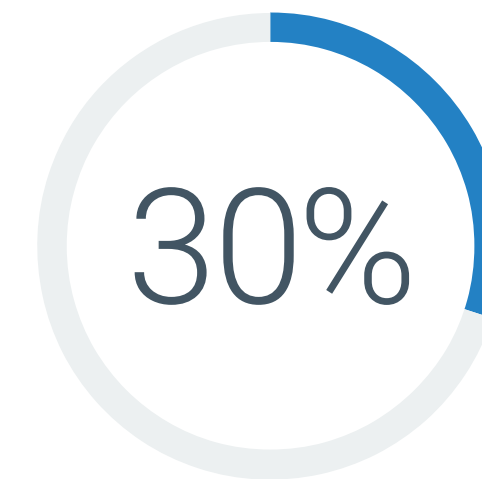
Expected impact of XDR on security operations environment.



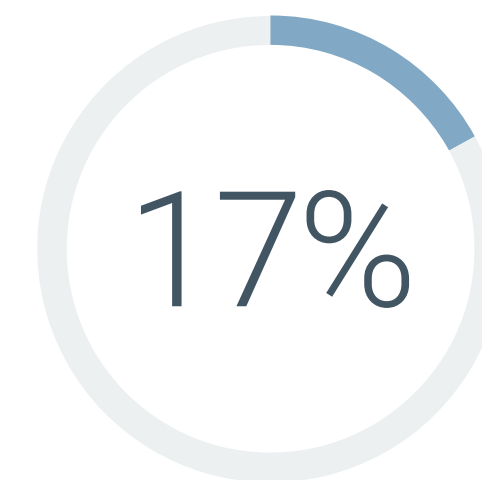
How specialized threat detection and response technologies are expected to integrate with XDR over time.



Specialized threat detection and response technologies will **remain independent and be loosely coupled** with XDR in federated architecture



Specialized threat detection and response technologies will **become part of XDR**



Specialized threat detection and response technologies and XDR will **come together by sending logs and alerts to a SIEM platform**

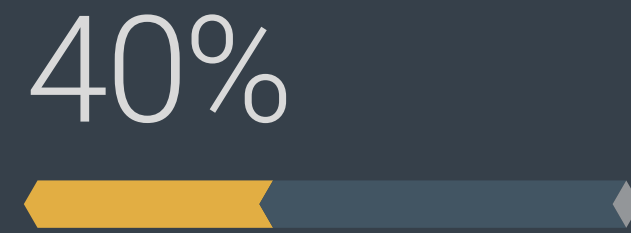
What Problems Is XDR Solving?

From the early days of XDR's introduction, Enterprise Strategy Group's research has shown that the top use case for XDR is consistently the need to investigate advanced threats, followed by the need to support threat detection and response for cloud resources. This latest iteration of the research validates that despite the change in XDR's definition and how XDR helps to solve security operations problems, the objectives remain the same. Current approaches are seen as cumbersome, complex, costly, noisy, lacking scalability, and lacking the ability to effectively detect and support the investigation of advanced threats. This sets a big agenda for XDR that will require continuing investment from every XDR vendor to succeed.

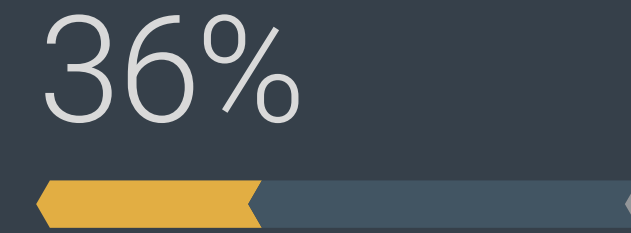


of organizations believe **XDR improves their ability to correlate threat and vulnerability information** to better prioritize remediation actions.

Threat detection and response challenges driving XDR interest and spending.



Current tools aren't effective at detecting and investigating advanced threats



Specific gaps in cloud detection and response capabilities



Current tools require too many specialized skills



Current tools aren't effective at correlating alerts, causing us to struggle to keep up with alert triage



Current tools aren't integrated well, making threat detection and response too cumbersome



Current tools approach is too complex to use and manage



Current tools aren't scaling to handle our growing attack surface



Current tools approach is too costly

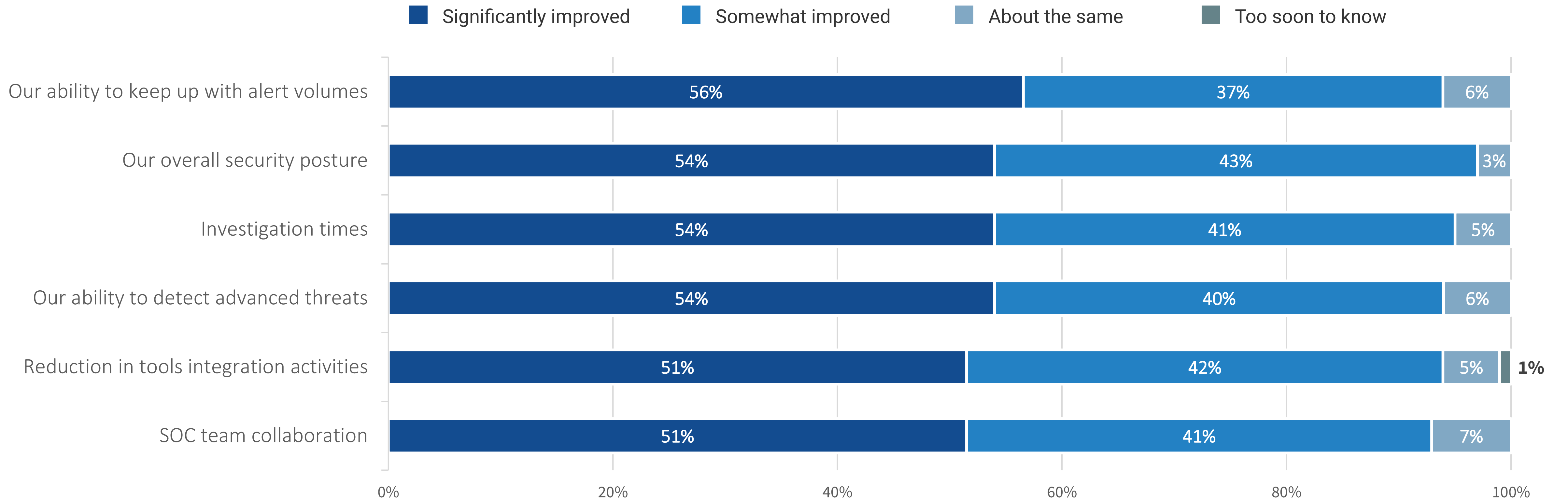



Can't develop and implement detection rules fast enough to keep up

XDR Is Delivering Value

For many, XDR solutions are contributing to both efficacy and efficiency improvements. Looking at how and where XDR has improved security outcomes over the past 18 months, at least half of organizations report that XDR has **significantly** improved several key areas of security operations. These measurable enhancements include the ability to keep up with alert volumes and detect advanced threats, improved overall security posture, improved investigation times, a reduction in tools integration activities, and better SOC team collaboration.

Areas in which XDR has produced measurable improvements.



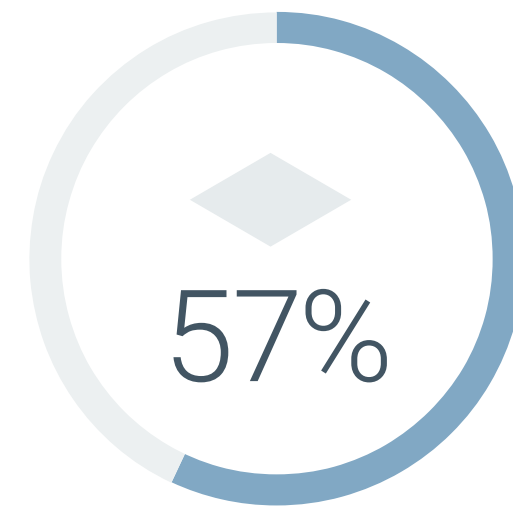


Automation and GenAI:
Automation Is a Priority,
Beginning With the Basics

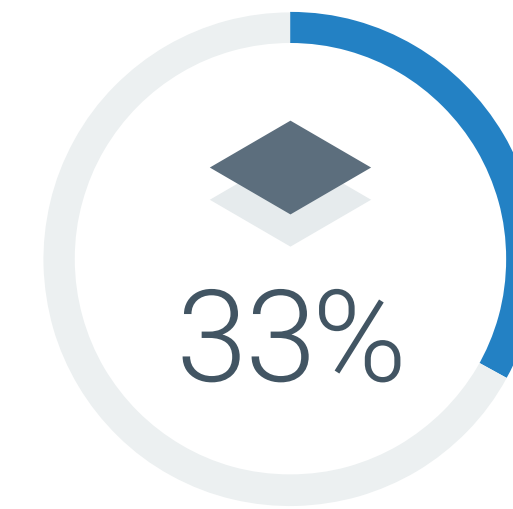
Using More Automation in SecOps Is a Priority, Starting With the Basics

Automation is an ongoing theme across security operations; however, implementation strategies vary widely. With 88% reporting the use of automation within security operations processes, security leaders understand that more processes need to be automated to scale their security programs. There are multiple approaches to incorporating automation into security programs, including formal SOAR tools actively in use by a subset of security teams being broadly deployed across many processes and tools. More popular is the use of integrated automation features included within individual security tools, though generative AI (GenAI) technology is emerging as a tool to help save time and provide rapid value.

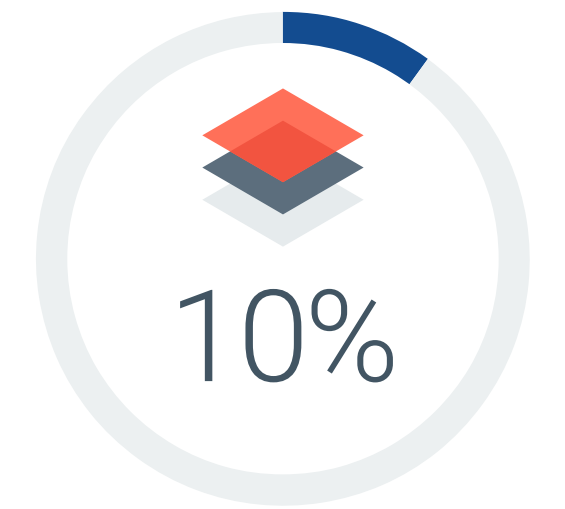
Primary focus of automating security operations processes.



Automating processes associated with **level/tier one analysts** (i.e., alert enrichment, alert prioritization, alert triage support, etc.)

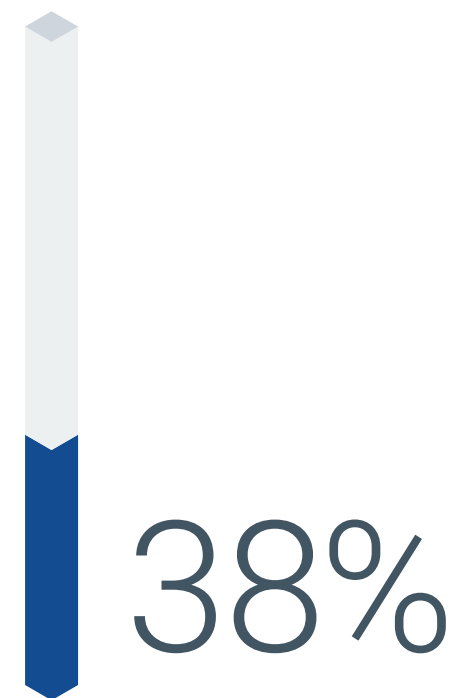


Automating processes associated with **level/tier two analysts** (i.e., data collection for security investigations, investigation runbooks, etc.)

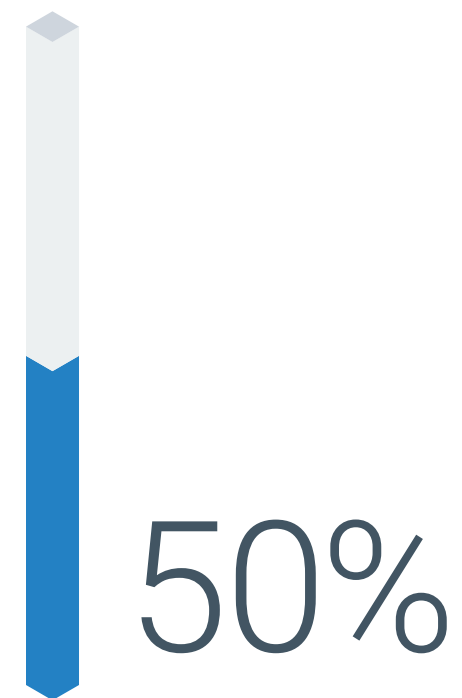


Automating processes associated with **level/tier three analysts** (i.e., runbooks for forensic analysis, runbooks for threat hunting, etc.)

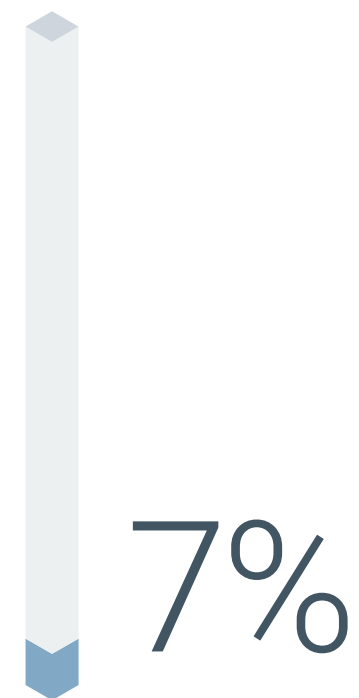
Has your organization automated security operations processes?



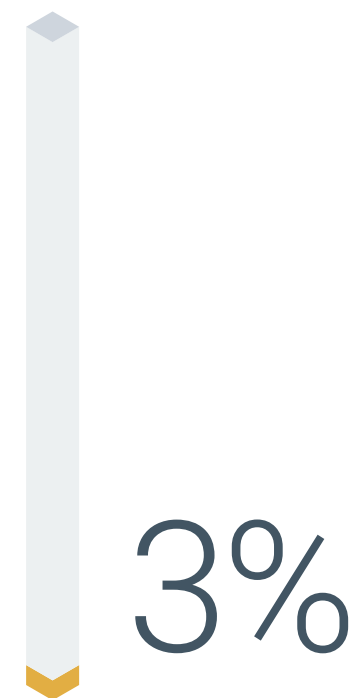
Yes, extensively



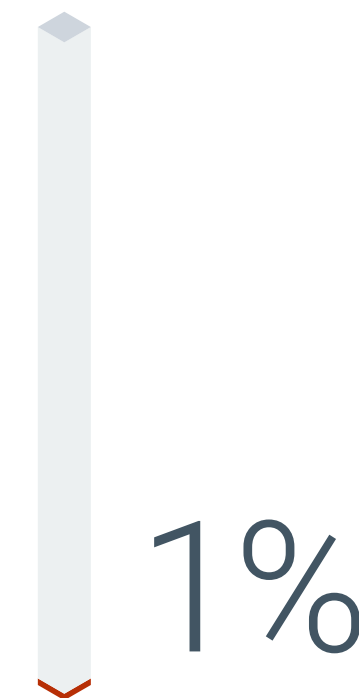
Yes, somewhat



No, but we are in the process of doing so



No, but we are planning to do so



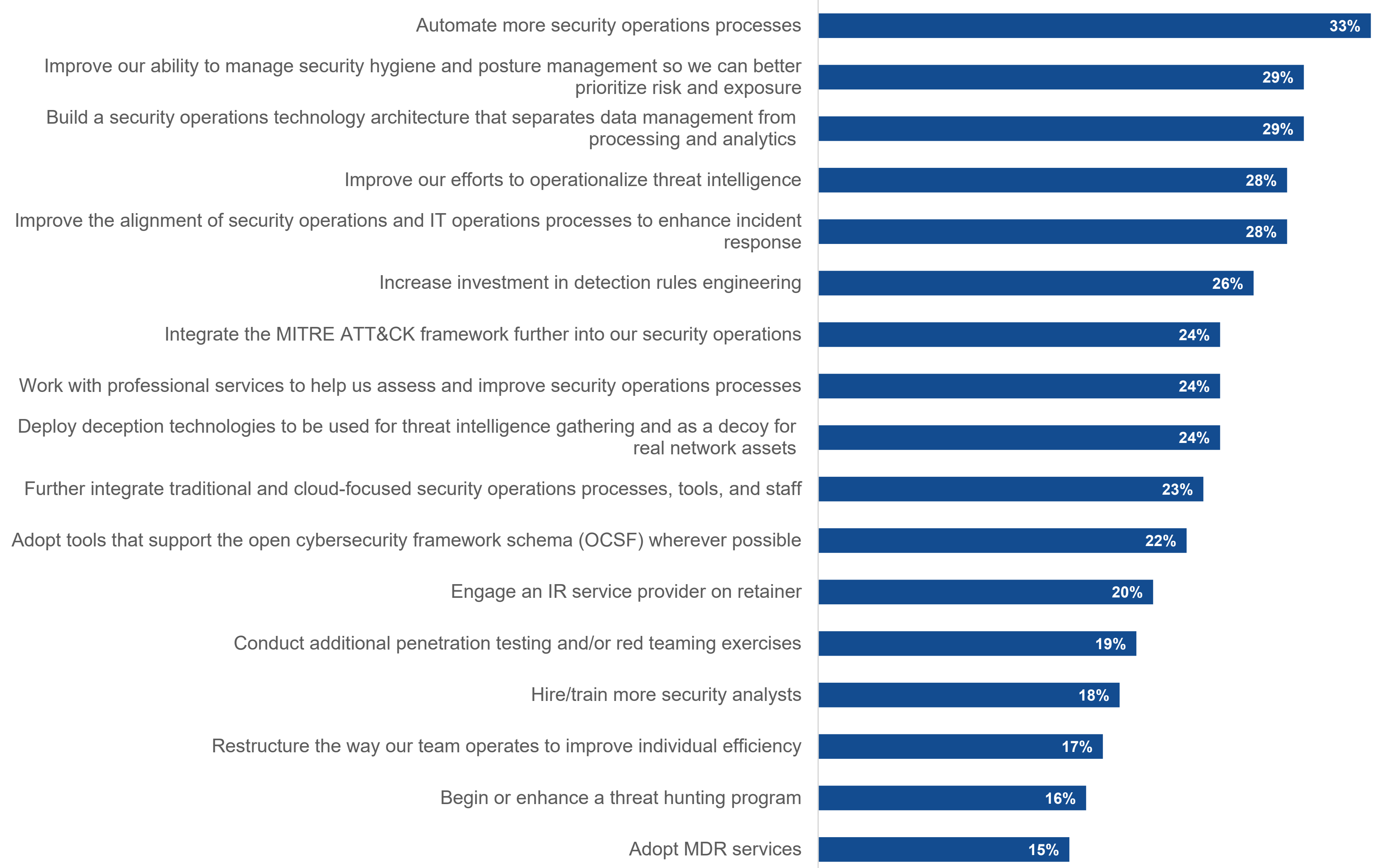
No, but we are interested in doing so

But where are early automation investments happening? Early investments in automation are aimed at helping more junior security personnel become more productive. Thinking about the many challenges associated with alert enrichment, prioritization, and triage, automation investments should be prioritized here first to relieve stress on the security operations functions and help scale the organization's capabilities. This is especially important for those who find themselves caught in the firefight, with no time to improve processes and strategies.

Automation Is a Clear SecOps Priority

Looking at the big picture surrounding security operations, when asked what actions their organizations will take over the next 12 to 18 months to improve, automating more security operations processes was the most common response. With the continuing growth of both threats and the attack surface, security teams can no longer gain the scale they need by hiring more analysts. More processes must be automated to scale the operation. Other actions organizations are likely to take to improve their security operations posture include improving security hygiene and posture management to better prioritize risk and building a SecOps architecture to separate data management from data processing and analytics.

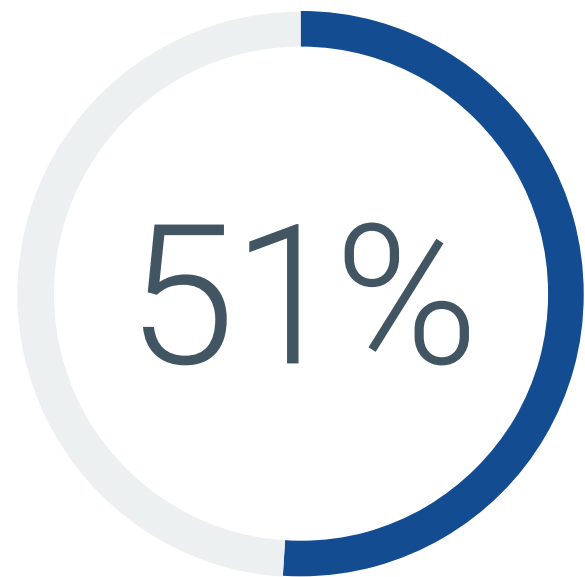
Actions organizations will take to improve security operations.



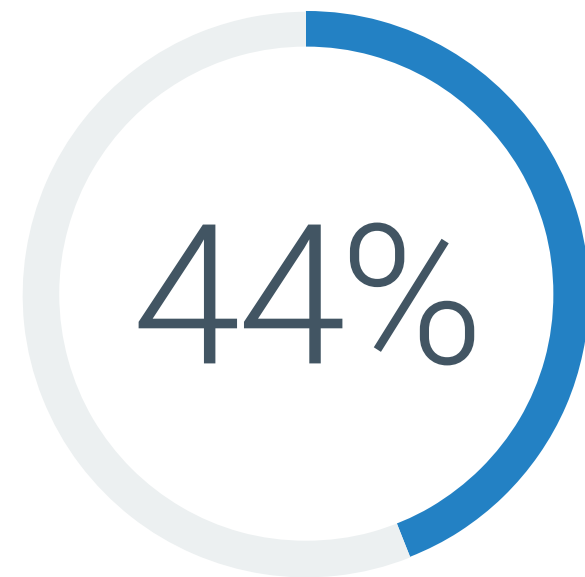
Most Are Optimistic That Generative AI Will Improve SecOps

Organizations see promise in the application of GenAI throughout the SecOps process. More than half (51%) believe that GenAI will be used in support of many SecOps use cases in the coming 12 to 18 months, while an additional 44% see at least a few security use cases for GenAI. While still early days, as vendors employ GenAI within existing security tools, security operations personnel will begin to formulate how and where GenAI can save time, add clarity, help scale the operation, and contribute to improving key metrics. As a form of automation itself, GenAI should redefine what's possible using automation, enabling organizations to further automation objectives with less overhead required to tightly define specific processes prior to automation.

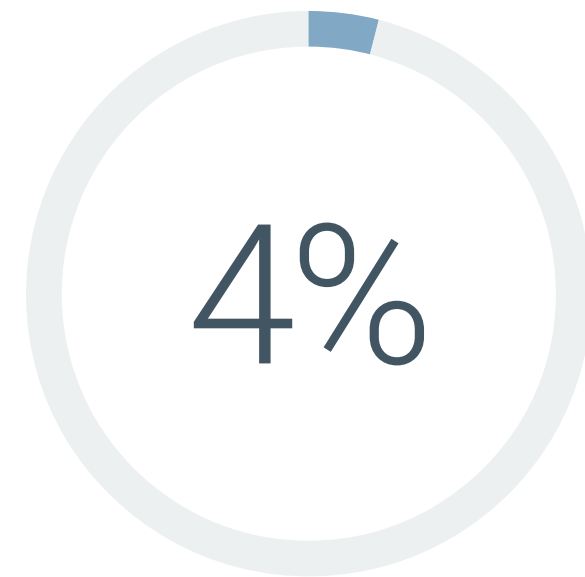
Perspective on importance of GenAI capabilities for security operations.



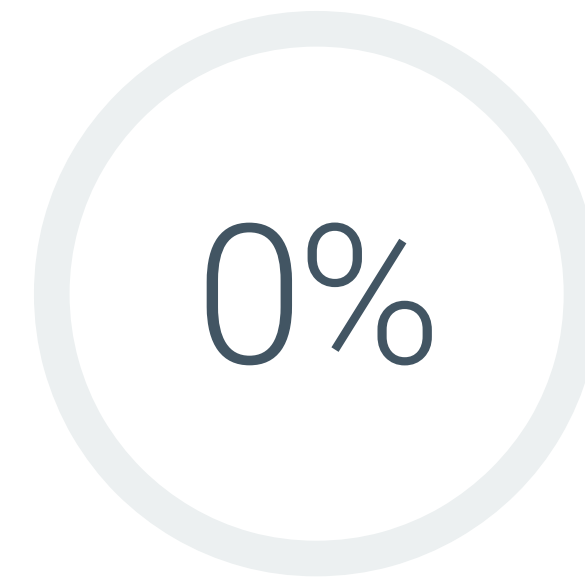
I believe generative AI will be used for **many** security operations use cases over the next 12 to 18 months



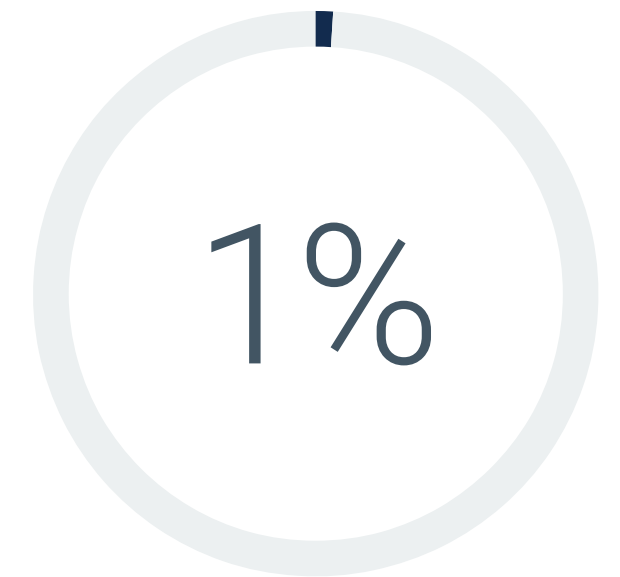
I believe generative AI will be used for **a few** security operations use cases over the next 12 to 18 months




My organization **plans to test** generative AI for security operations, but I don't anticipate that it will become part of our security operations in the next 12 to 18 months



My organization has **no plans** to adopt generative AI for security operations in the next 12 to 18 months



It's too soon to tell

A man and a woman are standing in a control room, looking at a laptop. The man is wearing a light blue shirt and glasses, and the woman is wearing a dark blazer. They are surrounded by large screens displaying network diagrams and data. The screens show various labels like 'ENT 03', 'ENT 04', 'ENT 05', 'PATH 1', 'PATH 2', 'PATH 3', 'PATH 4', 'PA-30', 'PA-31', and 'ORK 034'. The overall atmosphere is professional and technical.

**The People Behind Security:
Hybrid Staffing Models
Are the 'New Norm'**

Managed Service Providers Are Widely Utilized, and More Usage Is Planned

As security leaders struggle to scale their security operations program, exacerbated by the security skills shortage, a combination of internal, full-time personnel and third-party services are needed for most. Indeed, 82% are currently leveraging managed service providers for some or all of their security operations program, with 42% planning to significantly increase usage over the coming 12-24 months and another 42% planning to slightly increase investment over the same timeframe. And managed service providers are offering more than just experts, also helping accelerate overall security program development, implement best practices, and upgrade the technology stack.

Does your organization currently or plan to use managed services for security operations?



- **41%** Yes, we do so for **a majority** of our security operations
- **41%** Yes, we do so for **a portion** of our security operations as an extension of our internal resources
- **12%** Yes, but only in **a limited capacity** as an extension of our internal resources

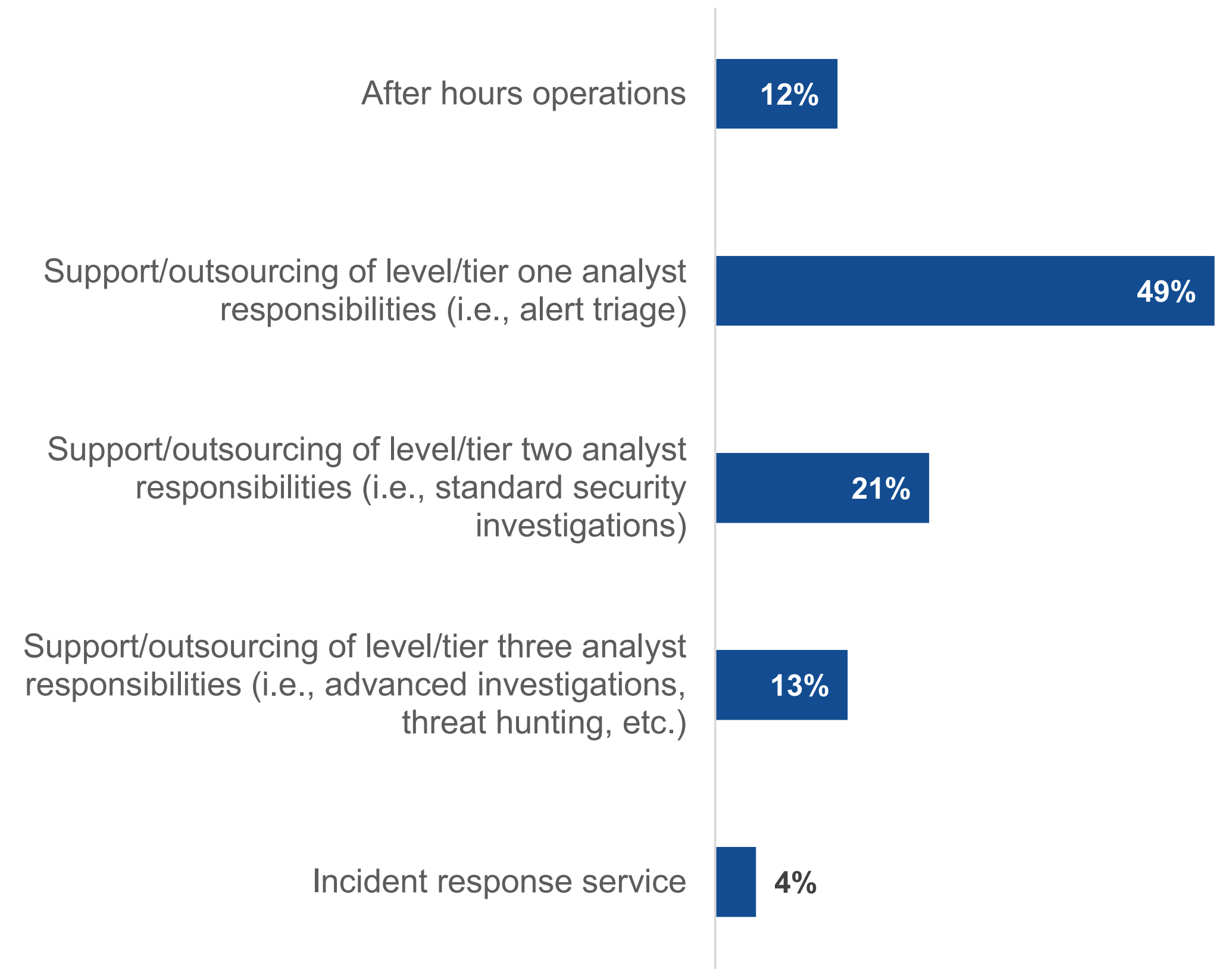
Usage plans for managed services to support security operations.



- **42%** We will increase our use of managed services for security operations **significantly**
- **42%** We will increase our use of managed services for security operations **slightly**

While managed service providers are helping in many ways, almost half (49%) are focused on supporting level/tier one analyst responsibilities, often freeing up resources to focus in other areas. Slightly more than one-third (34%) of organizations are leveraging managed service providers to support tier two and tier three analyst responsibilities, including advanced investigations, threat hunting, and more.

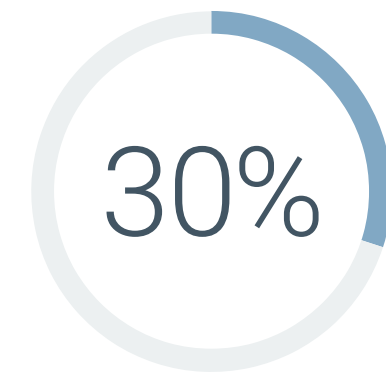
Security operations role/task for which organizations most heavily rely on managed security service providers.



Cloud SecOps Is Still a Work in Progress for Most Security Teams

When it comes to cloud security operations, many organizations are still ramping up, often depending on cloud-specific knowledgeable resources for support. This is evident in the fact that only 30% of organizations report their SOC completely owns all aspects of cloud security; in other words, 70% of organizations depend on separate cloud SecOps teams to secure cloud infrastructure. This continues to be a challenge for the industry, as the pace of cloud infrastructure development and innovation has left many security professionals caught without the level of knowledge they need to understand and investigate threats in the cloud. This should solidify cloud SecOps as an important agenda for all security teams, and Enterprise Strategy Group recommends hybrid operating models to accelerate cloud skills development for core security personnel.

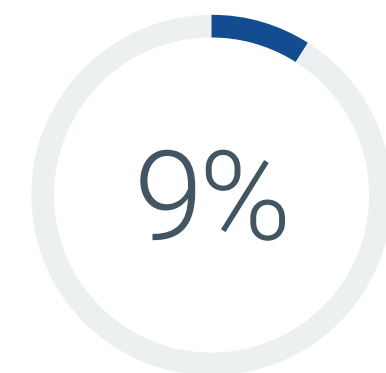
SOC support structure for cloud security operations.



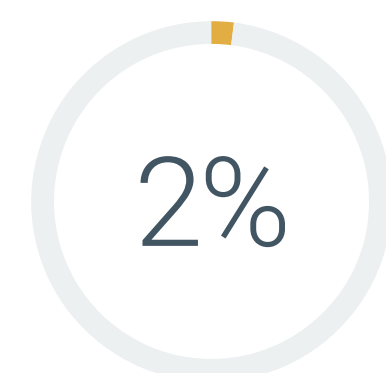
My organization's SOC has **complete ownership** of cloud security operations



My organization's SOC has a **major role** in cloud security operations but maintains a collaborative relationship with a dedicated cloud team (i.e., developers, operations, security, etc.) in this area



My organization's SOC has a **minor role** in cloud security operations, but these responsibilities are mostly owned by a dedicated cloud team (i.e., developers, operations, security, etc.) in this area



My organization has a **dedicated cloud team** (i.e., developers, operations, security, etc.) that owns cloud security operations independent of the SOC

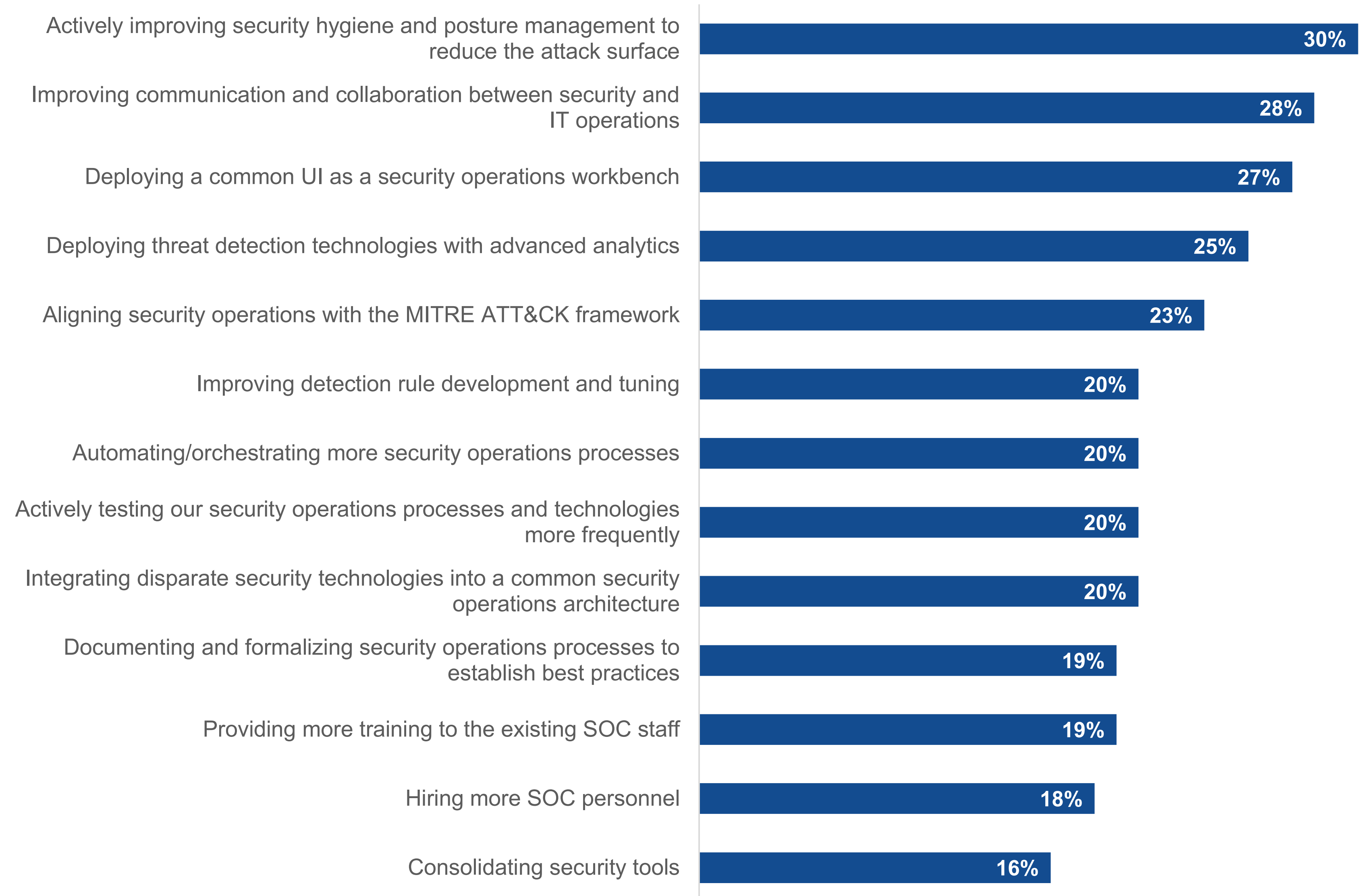
Action Plan for Improving Security Operations

What are the actions security teams think would most improve security efficacy and operational efficiency?

Atop the list is improving security hygiene and posture management to reduce the attack surface. This should not come as a surprise, given that the top challenge reported in this research is the changing attack surface. The next anticipated action involves improving communication and collaboration between security and IT operations teams. While the disconnect here has been palpable for many years, it's exciting to finally see a desire to actually invest in improving this gap.

Finally, and likely more challenging for most, is the desire for a common UI as a security operations workbench. "Platformization" is happening, so this objective may actually be within reach as security solution providers continue to aggregate and centralize operations consoles across the many security tools. Enterprise Strategy Group believes that consolidation initiatives will help security teams discover the power of more integrated security platforms, coming closer to providing a common workbench.

Most beneficial actions for improving security efficacy and operational efficiency.





ABOUT

Trend Vision One is where security pros start their day. It is a full-spectrum SOC platform that speeds up investigations by surfacing the highest priority, actionable alerts, and automating complex response actions. Your teams spend less time on tedious, repetitive tasks, and more time on high value, proactive security work like threat hunting and detection engineering.

Correlate events across endpoint, server, email, identity, mobile, cloud workload, OT, network, global threat intelligence feeds, and robust third-party integrations for complete context with XDR - only from Trend. High-fidelity detections show you the entire chain of attack, from root cause to full scope of the incident, while native response capabilities leave attackers with nowhere to hide. Advanced SOC tools let you predict the attacker's next move, so that you're always one step ahead.

[LEARN MORE](#)

[BOOK A MEETING](#)

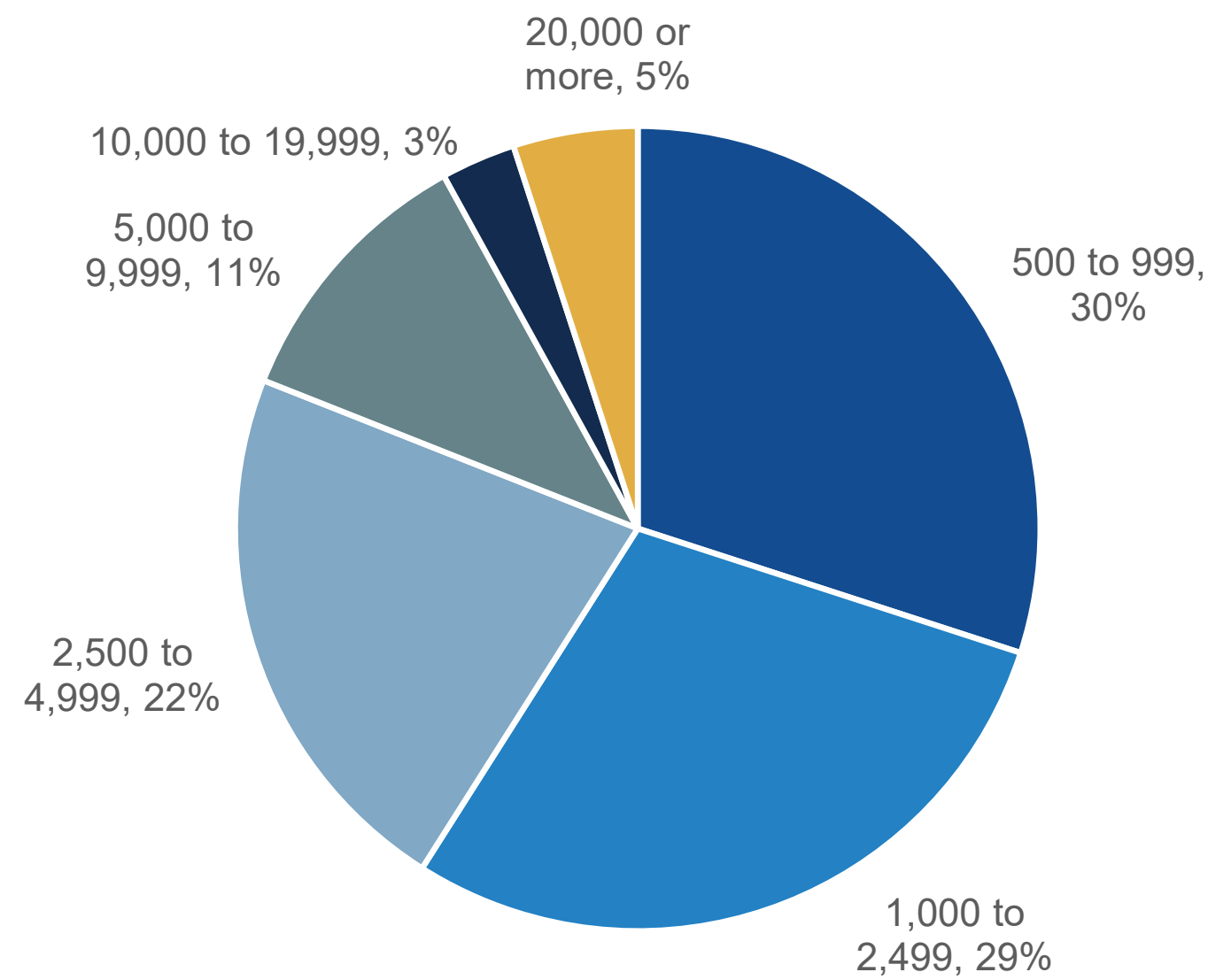


RESEARCH METHODOLOGY AND DEMOGRAPHICS

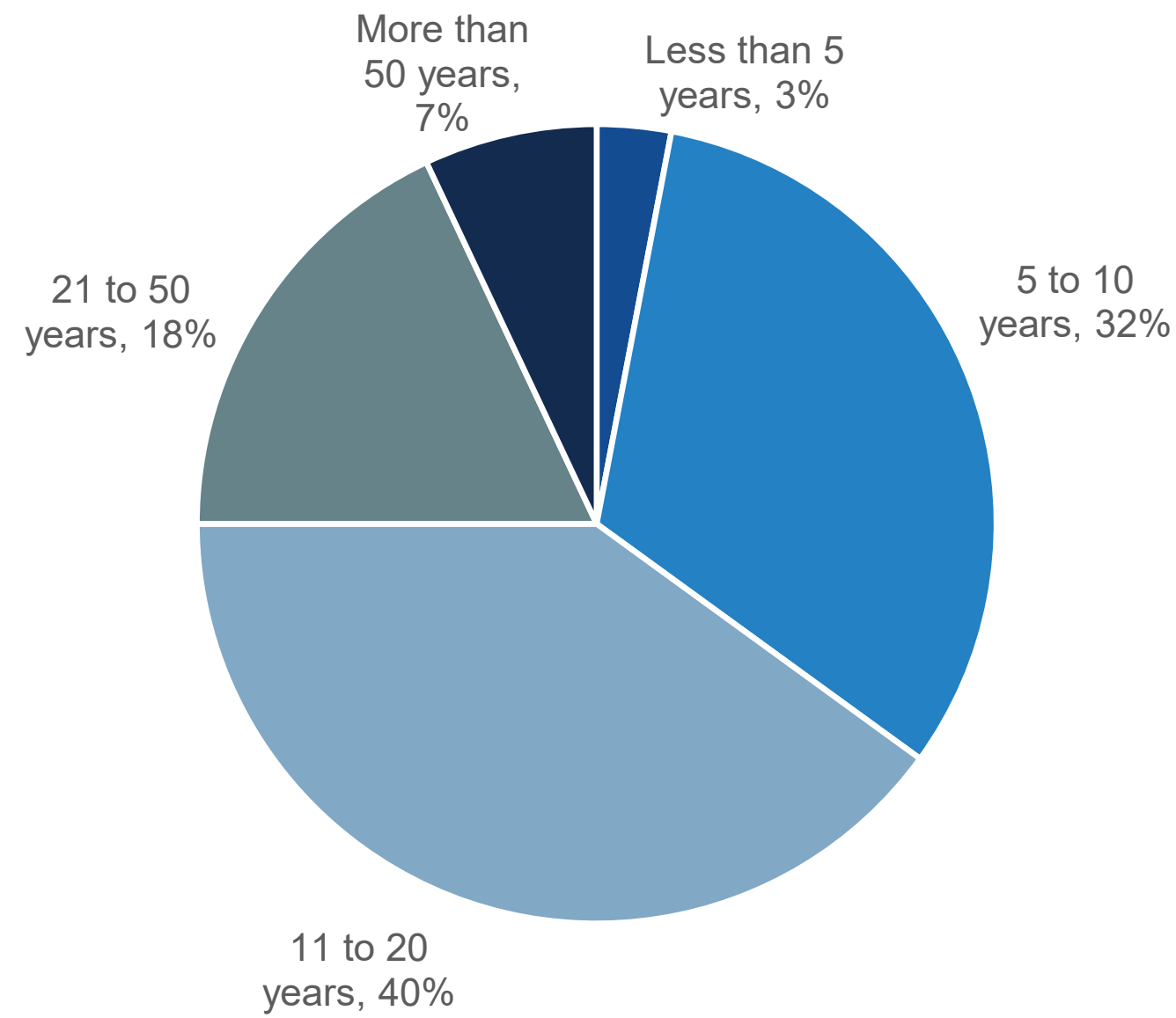
To gather data for this report, TechTarget’s Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between January 10, 2024 and January 23, 2024. To qualify for this survey, respondents were required to be responsible for or involved with security operations technology and processes. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 374 IT and cybersecurity professionals.

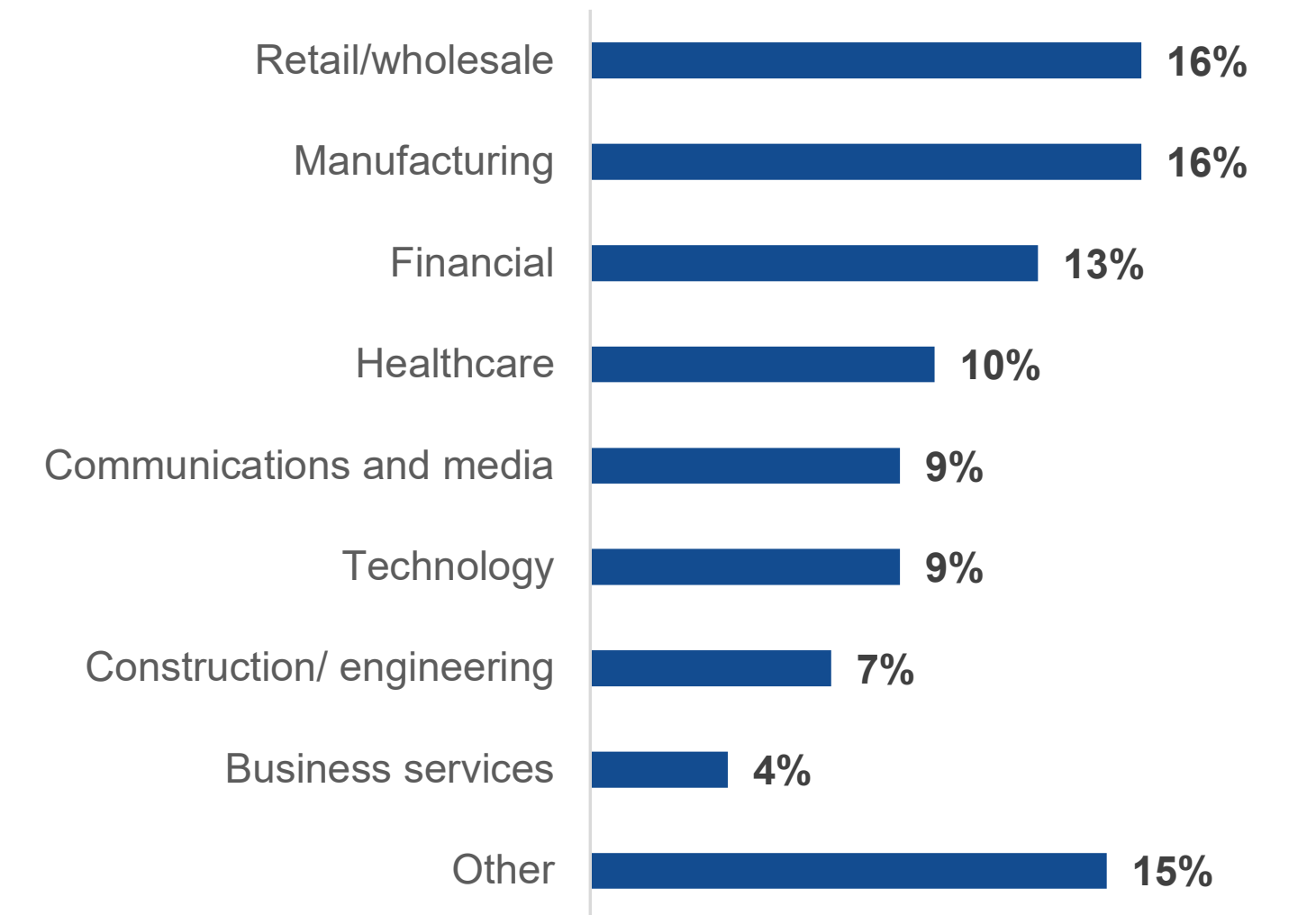
Respondents by number of employees.



Respondents by age of organization.



Respondents by industry.



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2024 TechTarget, Inc. All Rights Reserved.