Enterprise Strategy Group | Getting to the bigger truth.™

ESG RESEARCH REPORT

The rise of cloud-based security analytics and operations technologies

By Jon Oltsik, Senior Principal Analyst

December 2019

Contents

List of Figures

Executive summary

Report conclusions

ESG conducted an in-depth survey of 406 IT and cybersecurity professionals concerning their organizations' collection and/or analysis of security data in support of information security management strategy. Survey participants represented midmarket (100 to 999 employees) and enterprise-class (1,000 employees or more) organizations in North America (United States and Canada).

Based upon the data gathered as part of this project, the report illustrates:

- **Organizations have broad and diverse security analytics and operations objectives.** Cybersecurity professionals want security analytics and operations improvements in a number of areas like managing vulnerability, acting upon threat intelligence, and increasing the efficiency of the security data pipeline. CISOs must consider this extensive list as they modernize SOCs, aligning them with the threat landscape, growing attack surface, and evolving business requirements.
- **External changes and internal inefficiencies make security analytics and operations difficult.** Security professionals find it challenging to keep up with the cyber-threat landscape and the growing IT attack surface driven by initiatives like cloud computing, digital transformation, and IoT. At the same time, security operations centers (SOCs) struggle with disconnected point tools, manual processes, and a global cybersecurity skills shortage.
- **The security data pipeline continues to grow in volume and complexity.** Nearly one-third of organizations collect substantially more data to support cybersecurity analytics and operations today than they did 2 years ago, while more than half are retaining data online for longer periods of time than in the past.
- **IT is evolving from SIEM to SOAPA.** Seventy percent of organizations have a security event and information management (SIEM) system in place, and use SIEM for monitoring the security of cloud-based workloads, detecting known cyber-attacks, and producing reports for regulatory compliance. While SIEM continues to play a central security operations role, SOC teams are supplementing SIEM with tools for threat detection/response, investigations/query, threat intelligence analysis, and process automation/orchestration.
- **Staffing and skills shortages lead inevitably to managed services.** Three-quarters of respondents agree that the cybersecurity skills shortage has impacted their organization's security analytics and operations effectiveness, and more than two-thirds say it is difficult to recruit and hire additional SOC staff.
- **SOCs will have a "cloudy" future.** Many organizations are moving on from on-premises security analytics and operations technologies, as more than half now prefer cloud-based security analytics/operations solutions or would consider cloud-based security analytics/operations solutions on a case-by-case basis. Some will "lift and shift" on-premises tools to the cloud, some will replace on-premises tools with cloud-based alternatives, and some will supplement on-premises SOC technologies with cloud-based tools.
- **Organizations are incorporating machine learning and automation/orchestration into their technology plans.** More than half of organizations are adopting technologies featuring security analytics machine learning algorithms while nearly two-thirds are utilizing new technologies for process automation/orchestration.

Introduction

Research objectives

Security analytics and operations can be complex, requiring highly skilled professionals and detailed processes. To overcome these issues, security teams tend to deploy an array of security analytics tools and technologies to collect, process, analyze, and act upon growing volumes of security telemetry. Despite this investment, however, many organizations continue to find it difficult to manage cyber risk or detect and respond to cyber incidents.

How can CISOs address these issues and develop effective security analytics and operations processes? In order to get more insight into these trends, ESG surveyed 406 IT and cybersecurity professionals at organizations in North America (US and Canada) involved with the planning, implementation, and/or operations of their organization's information security policies, processes (including purchase decisions), or technical safeguards and familiar with their organization's collection and/or analysis of security data in support of information security management strategy. Among other questions of interest, this study sought to answer:

- What do organizations anticipate will be their primary objectives regarding security analytics and operations over the next 12 months?
- How do cybersecurity professionals view the cybersecurity analytics and operations landscape compared with 2 years ago? For those who believe it is more difficult today, what are the primary reasons?
- How has the amount of data organizations collect to support their information security activities changed in the last 2 years?
- Of all the data types organizations use for security analytics/operations, which three types are most important for their overall security mission?
- What types of security analytics and operations tools do organizations use on a regular basis?
- How active are organizations in terms of integrating disparate security analytics and operations tools to form a more cohesive security software architecture?
- What are/will be the primary use cases for SIEM? What are the most valuable attributes of SIEM?
- How difficult is it for organizations to recruit and hire cybersecurity staff specifically for analytics and operations?
- Do organizations use managed security services for any aspect of security analytics and operations? How will this usage change over the next 12-18 months?
- How are organizations using or considering public cloud-based security analytics and operations technology?
- Do organizations leverage or plan to leverage machine learning technologies for security analytics and operations? Have organizations deployed or do they plan to deploy technologies designed for security analytics and operations automation and orchestration?

Survey participants represented a wide range of industries including manufacturing, financial services, healthcare, communications and media, retail, government, and business services. For more details, please see the Research methodology and Respondent demographics sections of this report.

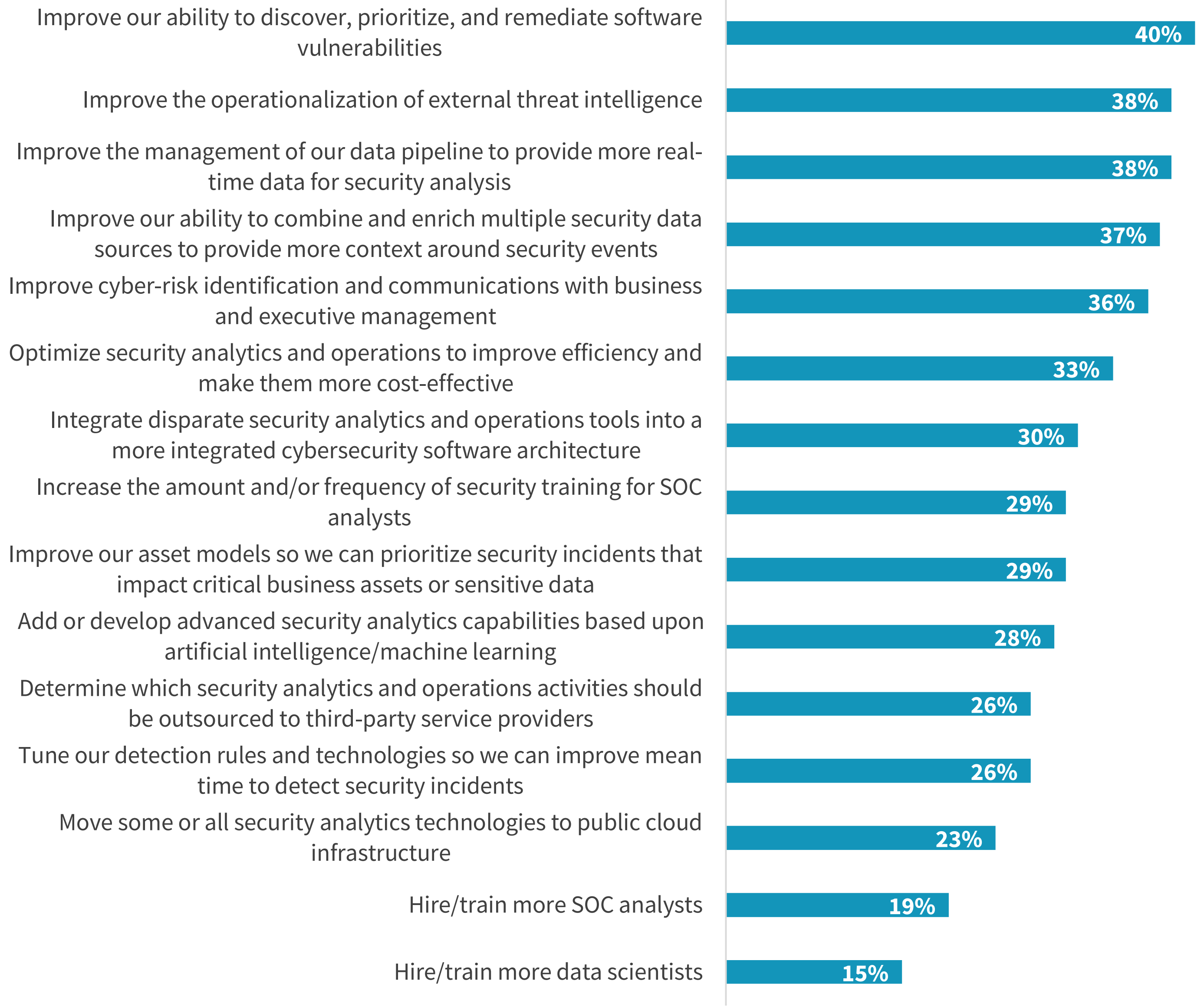
Research findings

Organizations have broad and diverse security analytics and operations objectives

Organizations have a lot of work ahead with security analytics and operations. According to Figure 1, the most prioritized objectives for cybersecurity analytics and operations over the next 12 months are improving software vulnerability discovery/prioritization/remediation (40%), operationalizing threat intelligence (38%), and enhancing the management of security data pipelines for real-time security analytics. CISOs should take note that the list of objectives includes risk, threat, operational, and even business metrics. While tactical adjustments may help, organizations should really be thinking about long-term SOC strategies.

Figure 1. Security analytics and operations objectives are varied

Over the next 12 months, which of the following would you say are your organization's primary objectives regarding security analytics and operations? (Percent of respondents, N=406, multiple responses accepted)



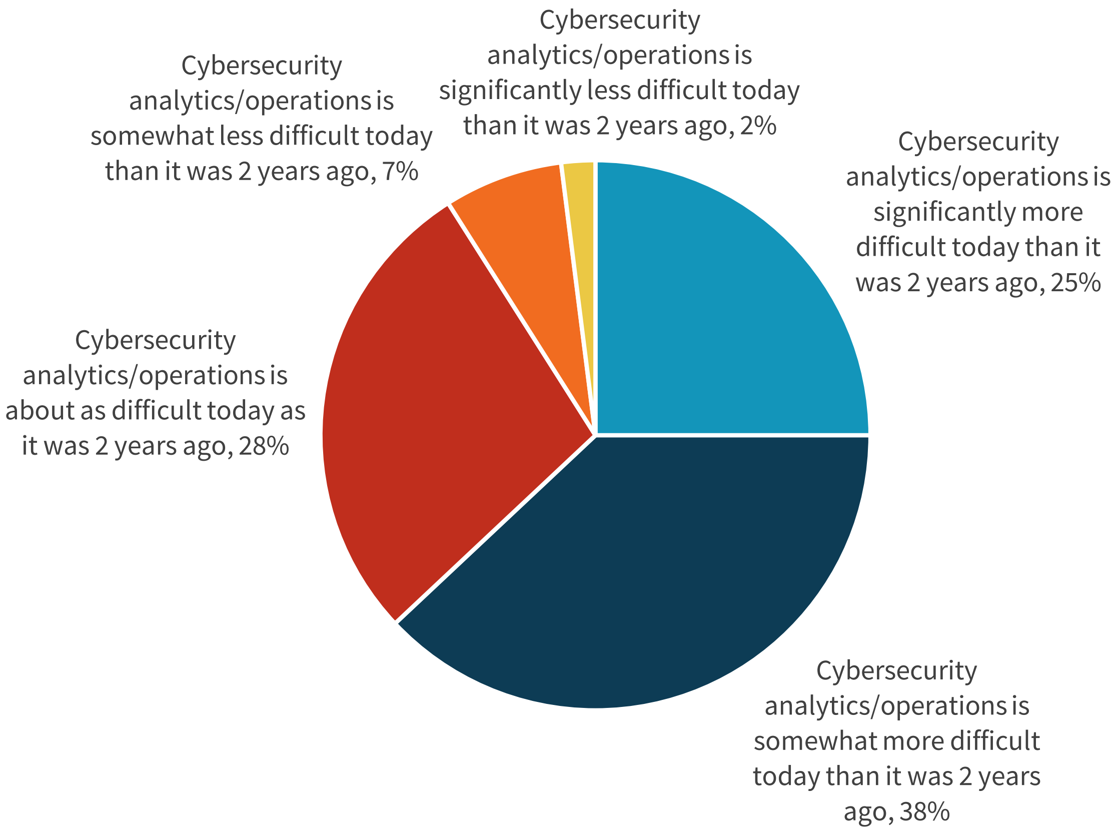
Source: Enterprise Strategy Group

External changes and internal inefficiencies make security analytics and operations difficult

The cybersecurity landscape in general continues to get harder for organizations to control and manage in the face of an increasing number of attack vectors, as well as the level of sophistication of the attacks themselves, and this complexity extends to the area of security analytics and operations. In fact, nearly two-thirds (63%) of respondents claim that security analytics and operations is more difficult for their organization today than 2 years ago (see Figure 2).

Figure 2. The security operations landscape is growing in complexity

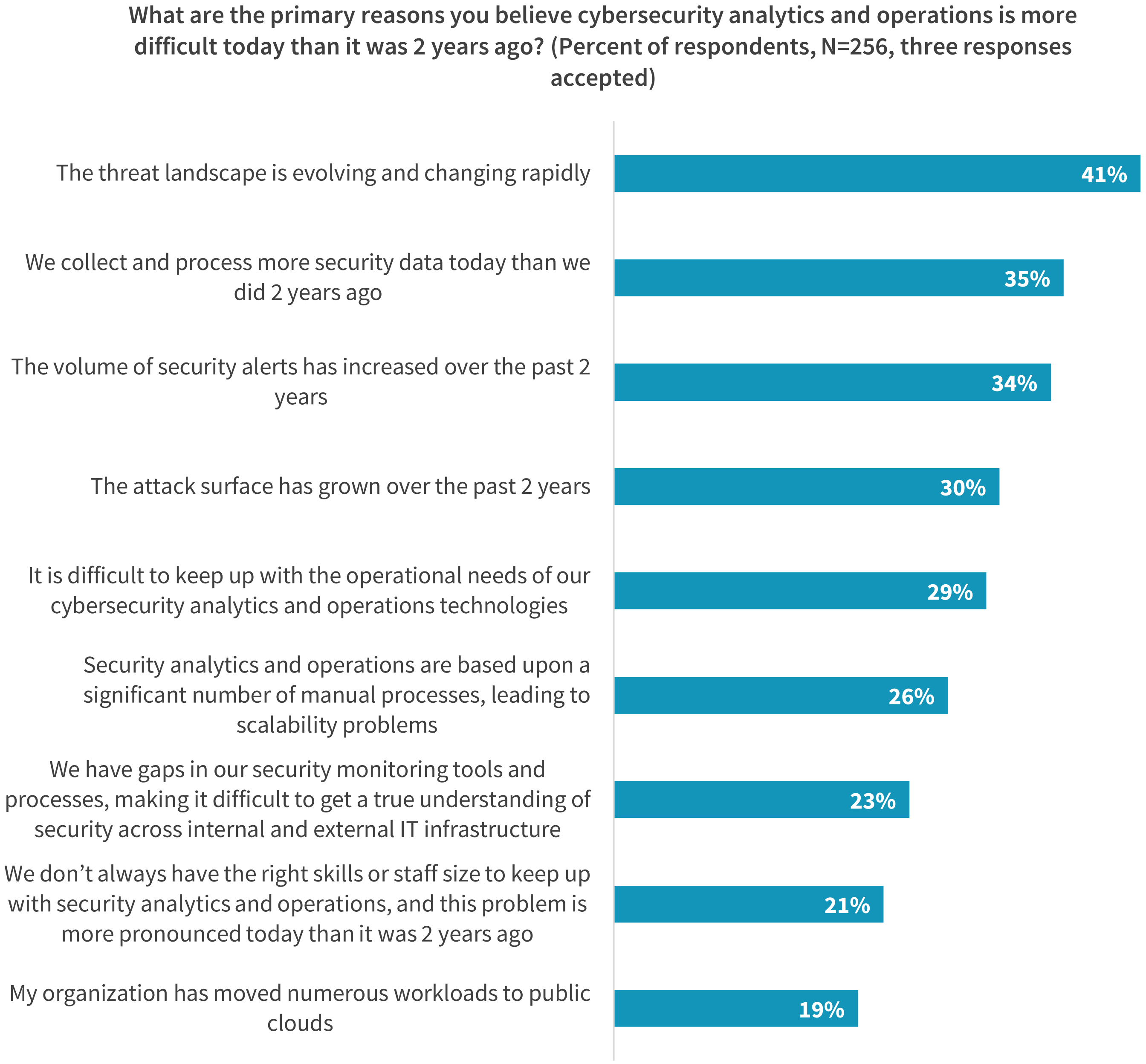
Which of the following best describes your opinion about cybersecurity analytics and operations? (Percent of respondents, N=406)



Source: Enterprise Strategy Group

Of those respondents who believe security analytics and operations are more difficult than 2 years ago, 41% believe this is the case due to the evolving and changing threat landscape, 35% say they collect and process more security data today than 2 years ago, 24% claim that the volume of security alerts has increased over the past 2 years, and 30% point to a growing attack surface (see Figure 3). CISOs must scale security operations to address the threat landscape and growing attack surface, while adopting modern security and data management technologies to help them tackle growing data and alert volumes.

Figure 3. Changing threat landscape and security operations model

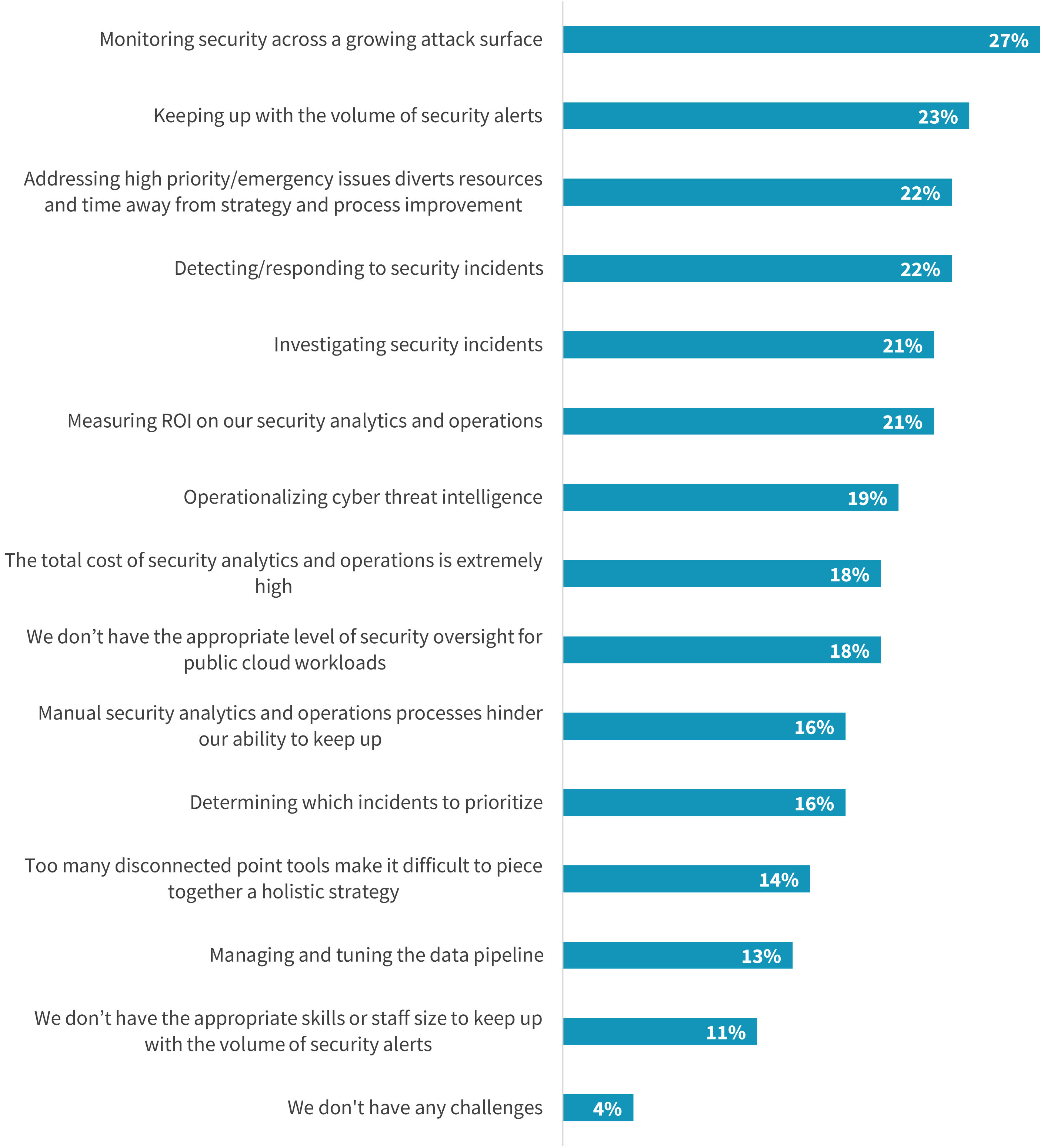


Source: Enterprise Strategy Group

Respondents were also asked to identify their primary security analytics/operations challenges. Once again, according to Figure 4, security professionals point to a growing attack surface and keeping up with the volume of security alerts. Alarmingly, 27% say that the cybersecurity team spends most of its time addressing cybersec emergencies, leaving them little time to work on strategy or process improvement. This constant cycle of security “firefighting” can result in employee burnout and high attrition rates, and without process improvement, cybersecurity analytics and operations performance will only degrade over time.

Figure 4. Keeping up with threats and alerts are the most common security analytics and operations challenges

Which of the following would you say are your organization’s primary challenges regarding security analytics and operations? (Percent of respondents, N=406, three responses accepted)



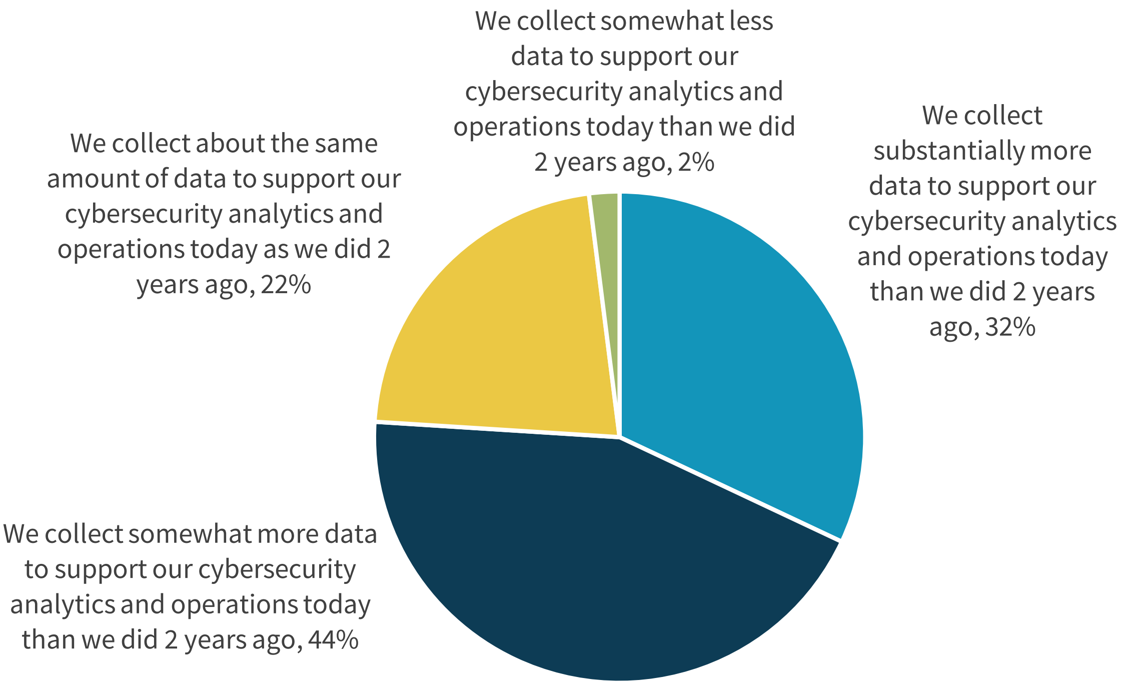
Source: Enterprise Strategy Group

The security data pipeline continues to grow in volume and complexity

Security analytics and operations depends upon collecting, processing, analyzing, and acting upon growing volumes of diverse security data sources. In fact, when respondents were asked to think about the amount of data their organization collects to support all its information security activities, such as risk management, regulatory compliance, incident detection/response, and security analysis/forensics, nearly one-third (32%) reported their organizations collect *substantially* more data to support cybersecurity analytics and operations than they did 2 years ago, while another 44% collect somewhat more data (see Figure 5). Additionally, 52% of organizations retain security data for longer periods of time than they did in the past. Security data growth and retention periods are driving the requirement for scalable high-performance security data pipelines, but many organizations don't have the right data management skills within their cybersecurity teams.

Figure 5. Organizations are collecting more security data and retaining it for longer

How has the amount of data your organization collects to support its information security activities changed in the last 2 years? (Percent of respondents, N=406)

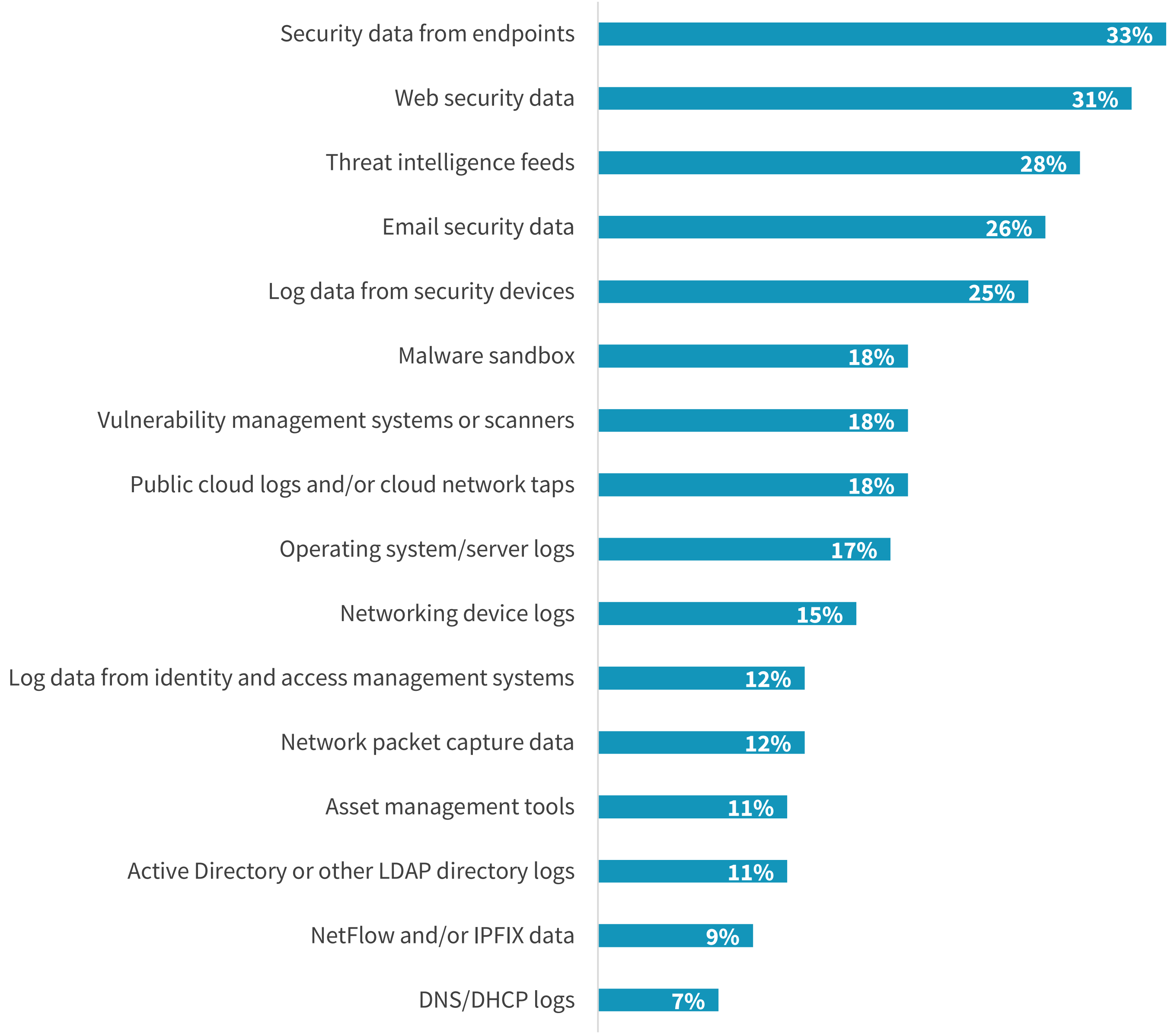


Source: Enterprise Strategy Group

Which data sources are most important for security analytics/operations? Based upon ESG's research, it appears that the focus is on incident detection. As seen in Figure 6, respondents pointed toward security data from endpoints, which can indicate compromised systems; web and email security data, which are common threat vectors; threat intelligence feeds, which are used to compare internal alerts with security data "in the wild;" and log data from security devices, such as network perimeter firewalls, IDS/IPS, and proxies. Other data like DNS, identity, and directory logs are likely used as part of investigations.

Figure 6. Wide range of important security telemetry

Of all the data types your organization uses for security analytics/operations, which three types would you say are the most important for your overall security mission? (Percent of respondents, N=406, three responses accepted)



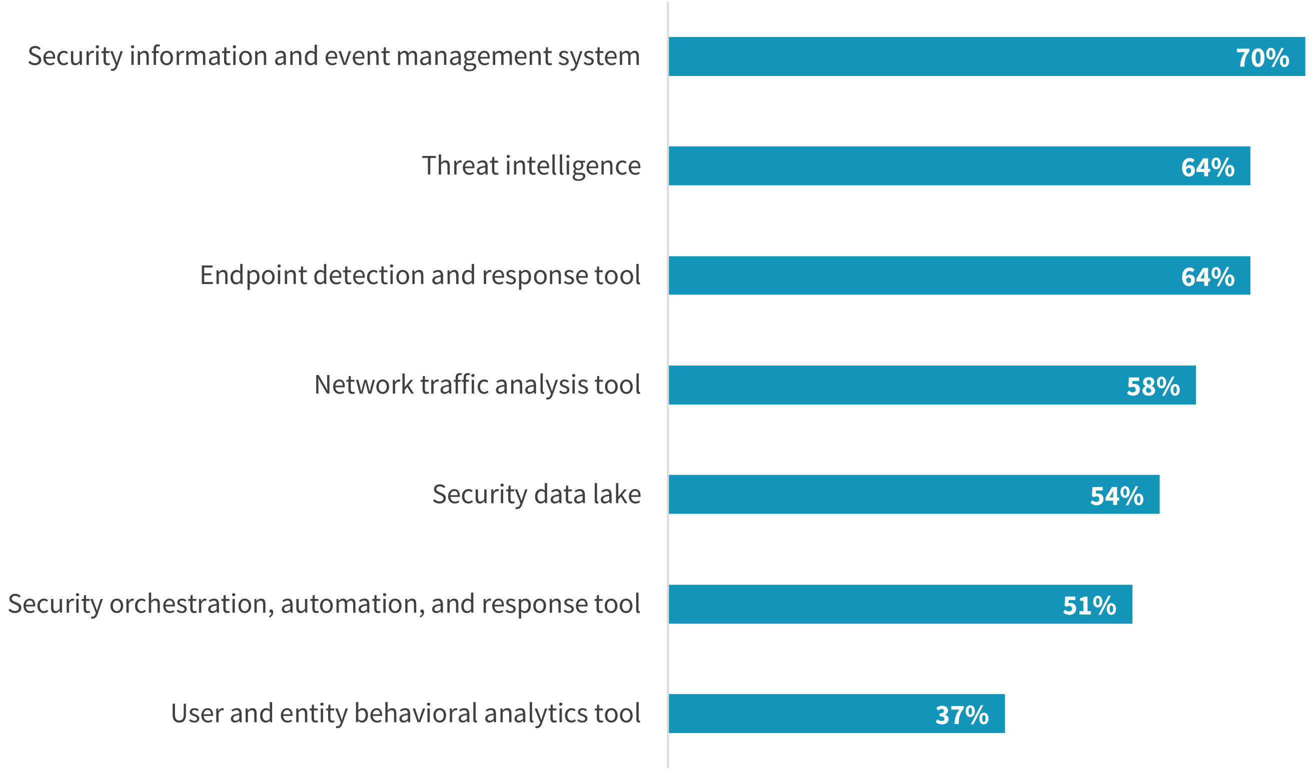
Source: Enterprise Strategy Group

IT is evolving from SIEM to SOAPA

When it comes to the activities and processes in place to support security analytics and operations, what types of tools are organizations using on a regular basis? According to Figure 7, nearly three-quarters (71%) of organizations use SIEM today as well as an assortment of other security technologies like threat intelligence feeds/analytics (64%), EDR (64%), and network traffic analysis tools (58%). While each tool provides valuable data analysis, it is difficult for security operations center (SOC) teams to piece together a holistic view of enterprise security across an assortment of disconnected point tools.

Figure 7. SIEM, threat intelligence, and EDR are the most commonly used security analytics and operations tools

Which of the following types of security analytics and operations tools does your organization use on a regular basis? (Percent of respondents, N=406, multiple responses accepted)



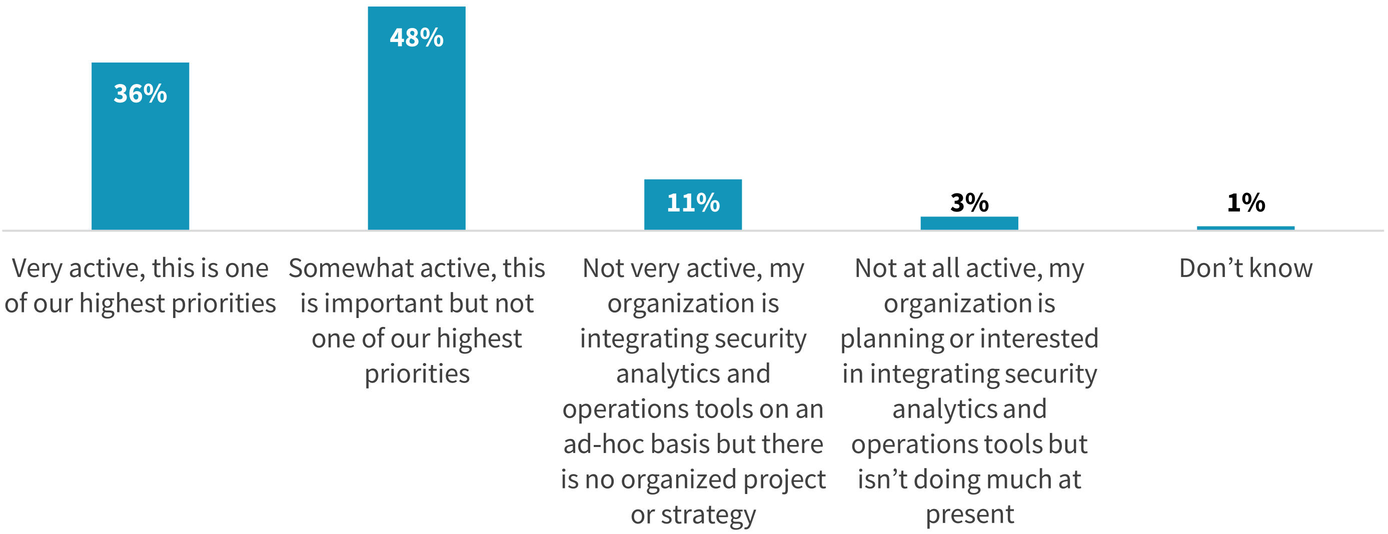
Source: Enterprise Strategy Group

To overcome this limitation, 36% of organizations are very active regarding integrating security tools into a common security analytics and operations platform architecture (SOAPA), while 48% are somewhat active in this area (see Figure 8). CISOs want unified SOAPA to help them improve SOC efficacy and efficiency.

82% of organizations are committed to moving large volumes of workloads and applications to the public cloud (see Figure 9). This increases the attack surface and introduces new oversight and skills requirements in security operations centers.

Figure 8. Many organizations are prioritizing integrating disparate security analytics and operations tools

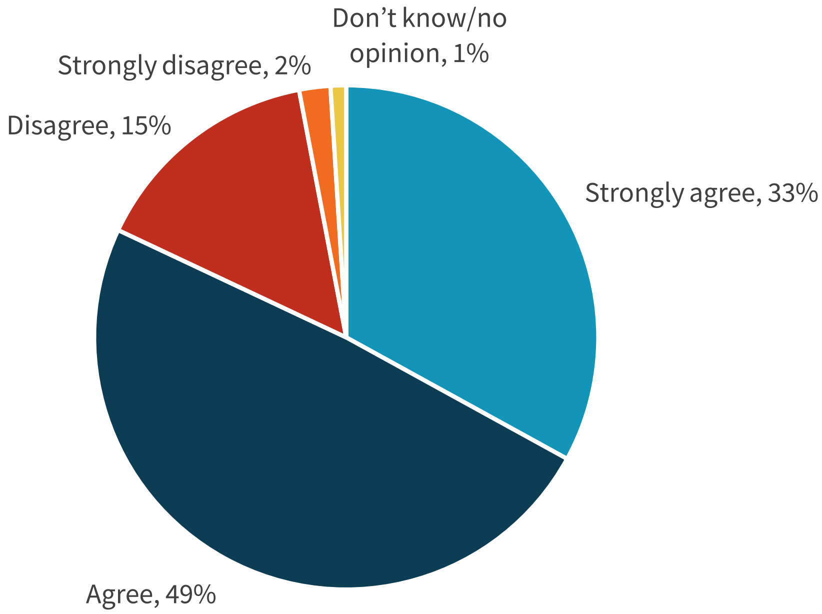
How active is your organization in terms of integrating disparate security analytics and operations tools together to form a more cohesive security software architecture? (Percent of respondents, N=406)



Source: Enterprise Strategy Group

Figure 9. SIEM is on a collision course with cloud services

Do you believe your organization is committed to moving a large volume of workloads and applications to the cloud? (Percent of respondents)

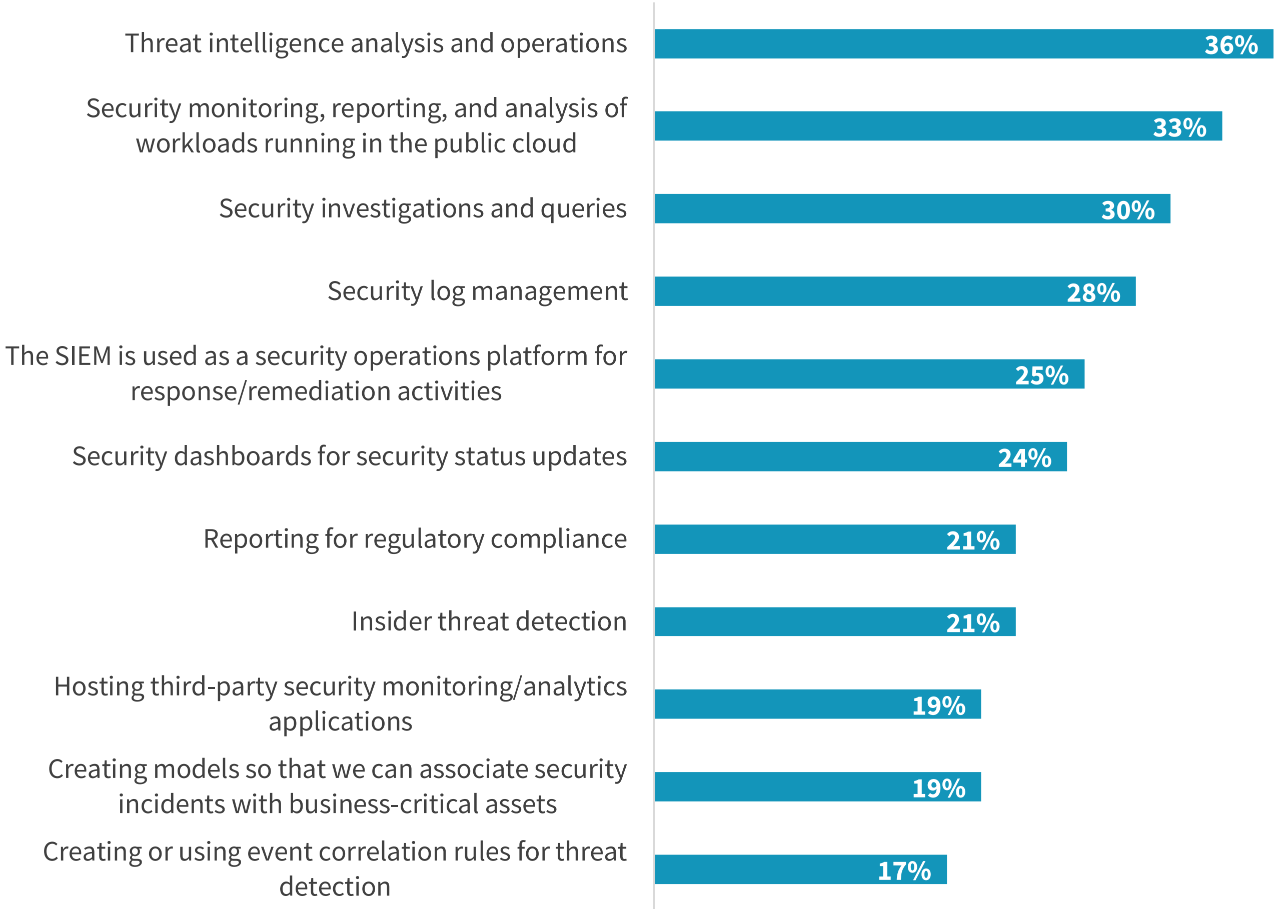


Source: Enterprise Strategy Group

So what are organizations leveraging SIEM platforms looking to accomplish? More than one-third (36%) of respondents say one of their organization's current and likely SIEM use cases involves threat intelligence analysis and operations (see Figure 10). Based on the fact that the majority of organizations are committed to moving large volumes of workloads and applications to the public cloud, it makes sense that 33% of respondents claim that SIEM systems are or will be used for security monitoring, reporting, and analysis of workloads running on public cloud platforms. CISOs must gauge whether existing SIEMs have the scale, performance, and analytics to keep up with cloud-based security data collection, processing, and analysis needs.

Figure 10. Most common SIEM use cases are threat intelligence synthesis, cloud monitoring, and investigations

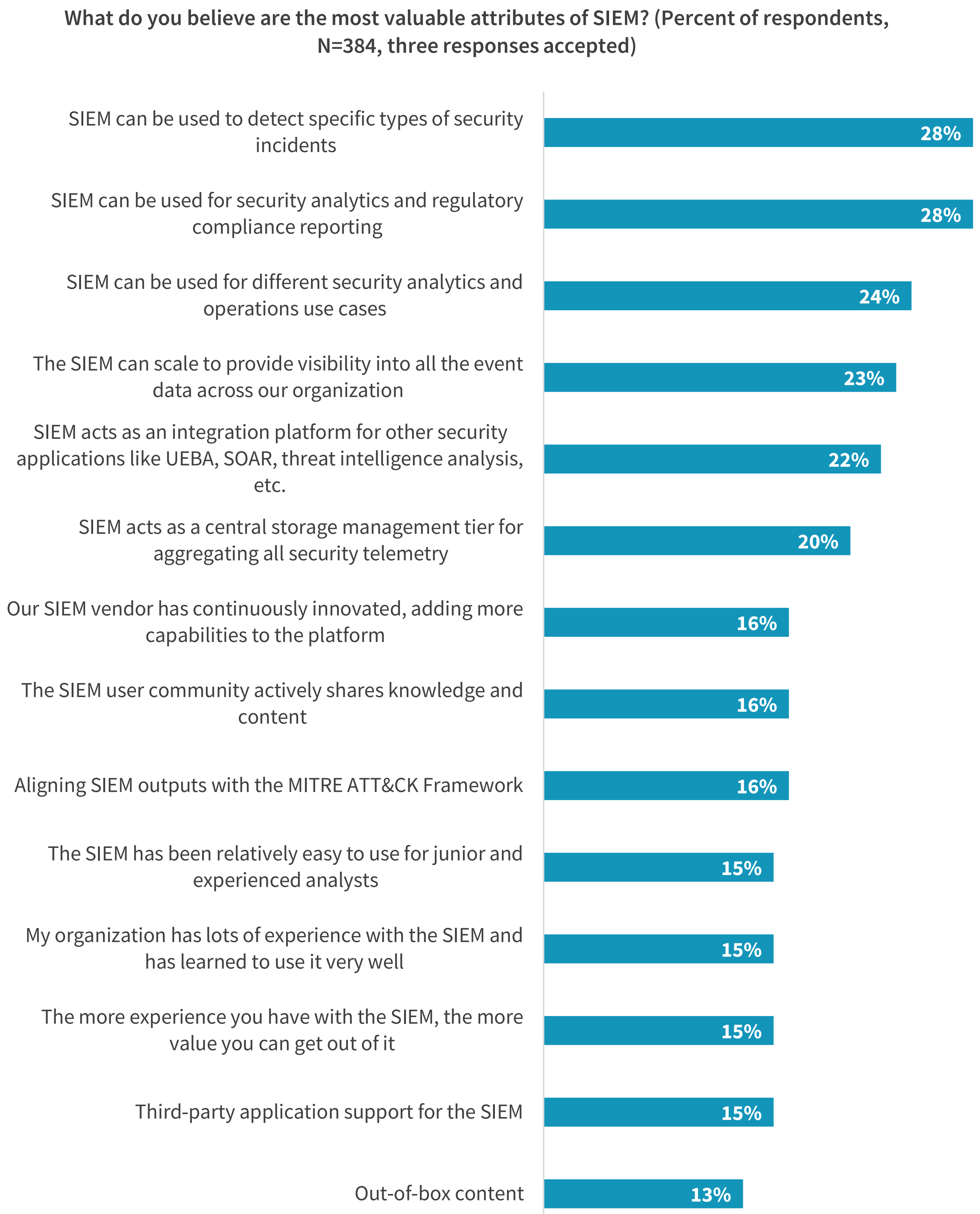
What are/will be the primary use cases for your organization's SIEM? (Percent of respondents, N=384, three responses accepted)



Source: Enterprise Strategy Group

Based on the wide variety of current and potential use cases associated with SIEM, many obviously see it as a valuable security operations asset. For example, SIEM is especially useful for detecting certain types of known incidents using correlation rules, and it is often seen as a Swiss Army knife for a variety of use cases, including security and regulatory compliance reporting (see Figure 11).

Figure 11. More than one-quarter view threat detection and compliance reporting as key SIEM value propositions



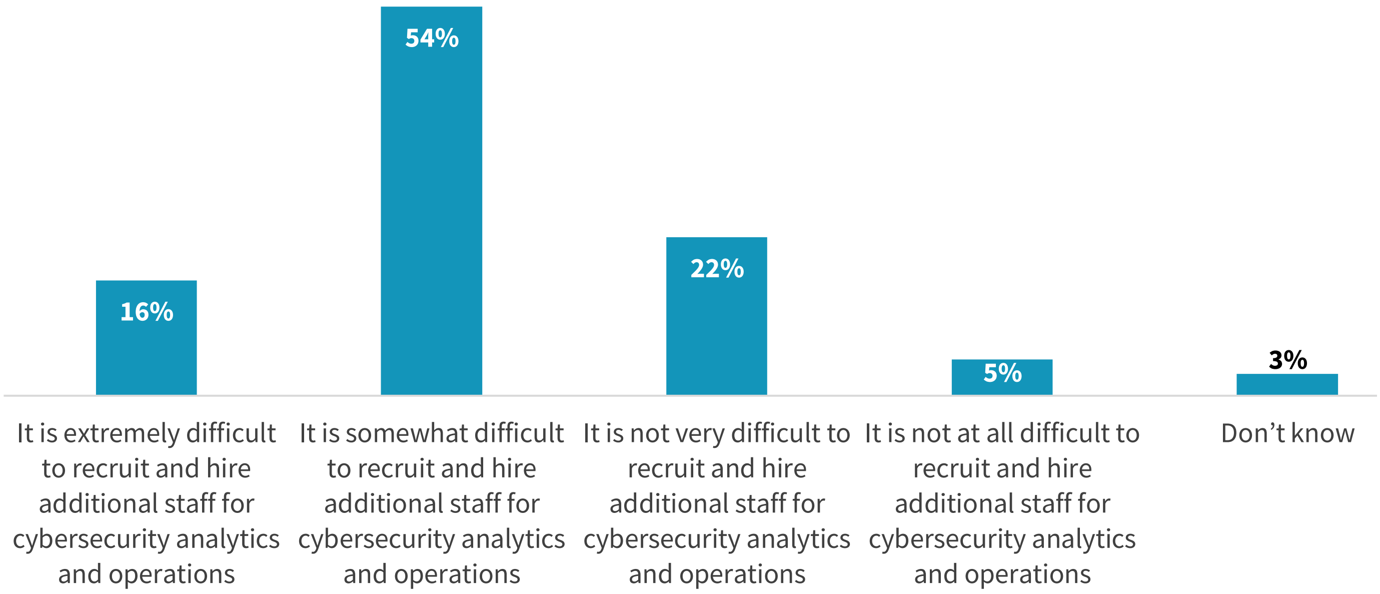
Source: Enterprise Strategy Group

Staffing and skills shortages lead inevitably to managed services

ESG research has been tracking the ongoing global cybersecurity skills shortage over the course of several years, and the data indicates that nearly three-quarters (74%) of organizations claim that this trend has directly impacted them.[1] Does this personnel deficit extend to their ability to effectively support security analytics and operations technologies and activities? Unfortunately, it does, according to Figure 12, as more than two-thirds (70%) of respondents say that it is extremely (16%) or somewhat (54%) difficult for their organization to recruit and hire SOC personnel in this climate.

Figure 12. More than two-thirds say it is difficult to recruit and hire additional SOC staff

When your organization actively recruits and hires cybersecurity staff specifically for analytics and operations, how would you characterize this effort? (Percent of respondents, N=406)



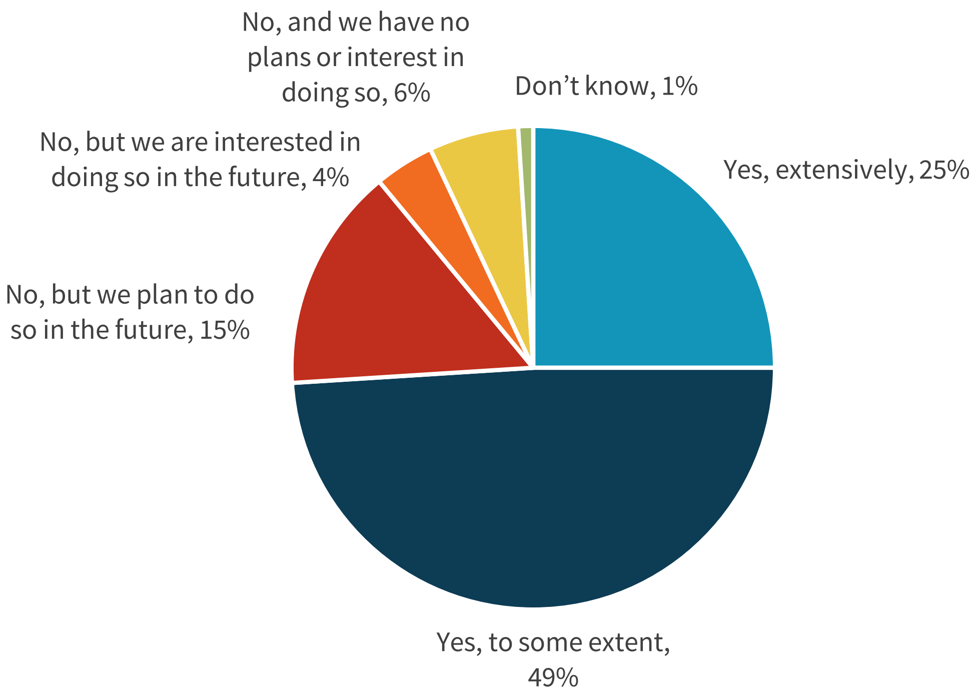
Source: Enterprise Strategy Group

To bridge the personnel gap, most organizations are turning to managed security services. Indeed, according to Figure 13, nearly three-quarters (74%) of organizations already use managed services for security analytics and operations in some capacity. Managed security services also have a strong future, as 91% of organizations will increase their use of managed security analytics and operations services in the next 12 to 18 months (see Figure 14). Smart CISOs will include SOC technologies and managed services as part of a cohesive and comprehensive SOC strategy.

[1] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2018*, April 2019.

Figure 13. Majority of organizations use security analytics managed services

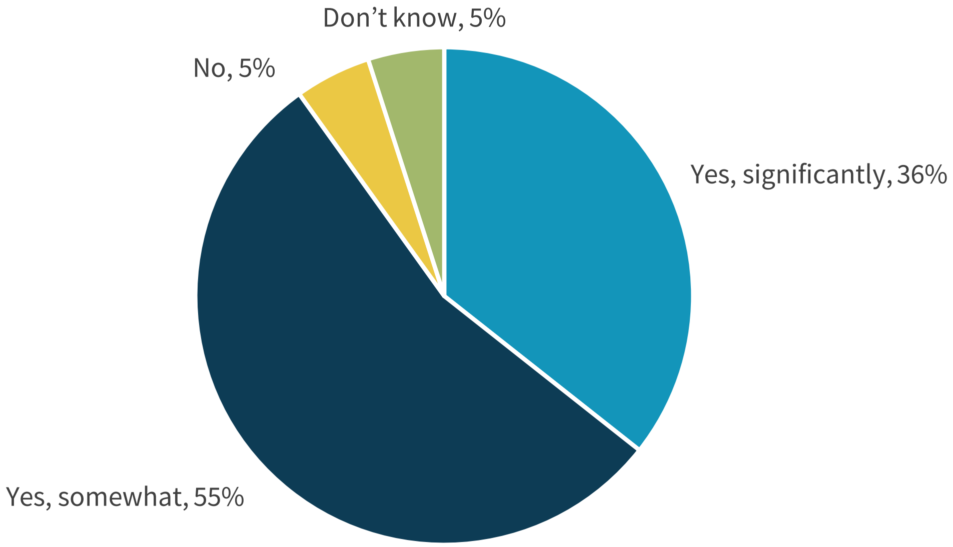
Does your organization use managed security services for any aspect of security analytics and operations? (Percent of respondents, N=406)



Source: Enterprise Strategy Group

Figure 14. Most expect to increase use of security analytics managed services

Will your organization increase its use of managed security analytics and operations services over the next 12 to 18 months? (Percent of respondents, N=377)



Source: Enterprise Strategy Group

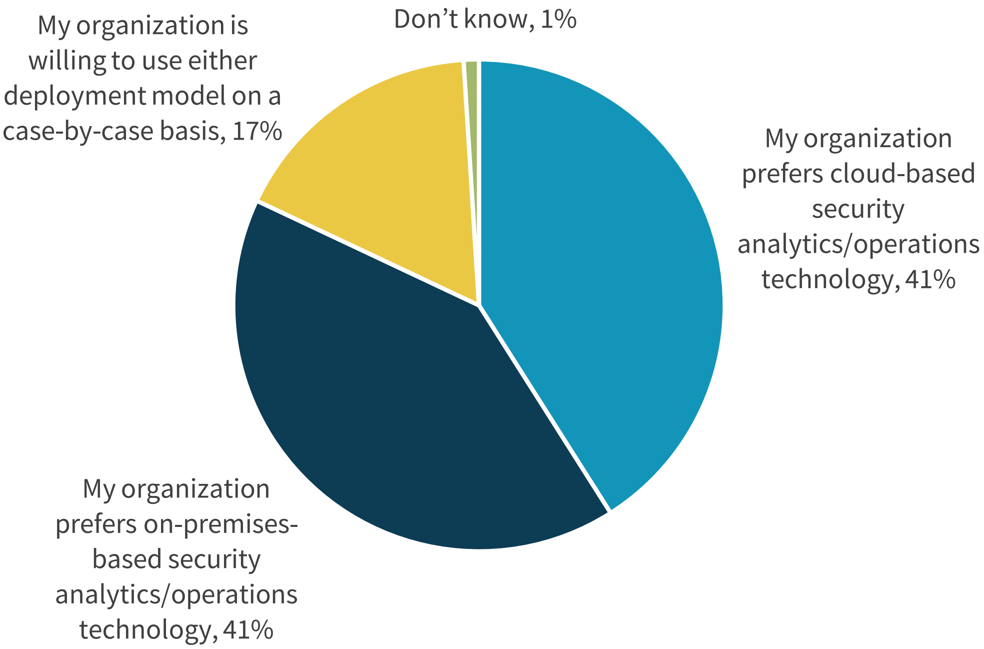
SOCs will have a ‘cloudy’ future

In the past, many security professionals eschewed cloud-based security analytics and operations tools, opting instead for the oversight and control associated with on-premises tools. Slowly but steadily, this behavior is shifting. Forty-one percent of survey respondents claim that their organization prefers cloud-based security analytics/operations technology today while another 17% are willing to consider cloud-based options on a case-by-case basis (see Figure 15).

Why the changing preference for cloud-based security? Cloud-based security analytics/operations technologies offer massive processing/storage scale and attractive pricing models while eliminating the cost and operational overhead associated with on-premises solutions.

Figure 15. No deployment model preference between cloud and on-premises

In general, which of the following options is most appealing to your organization? (Percent of respondents, N=406)



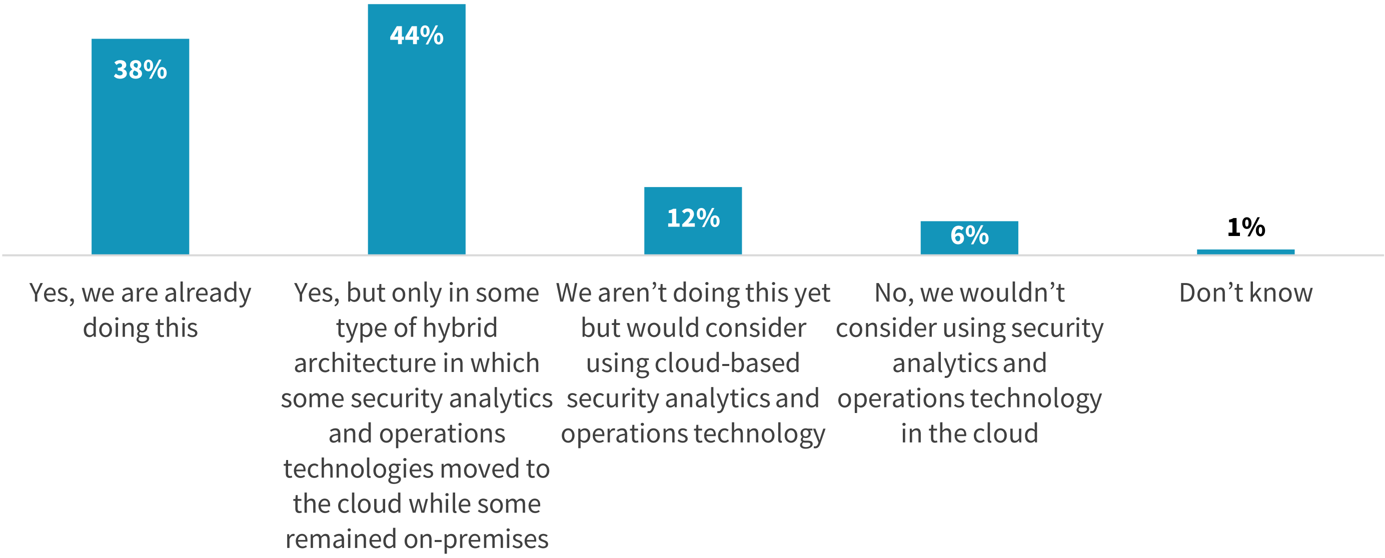
Source: Enterprise Strategy Group

Security professionals are actively moving security analytics and operations technologies to the public cloud: 38% are already using public cloud-based security analytics and operations technologies, 44% are willing to do so in a hybrid environment, and 12% would consider using cloud-based security analytics and operations technologies in the future (see Figure 16).

Cloud-based security analytics technology strategies follow diverse paths. Figure 17 reveals that 38% of organizations will move some or all existing security analytics technology infrastructure to the cloud in a “lift and shift” approach to SOC strategy. Alternatively, 36% plan to replace on-premises security analytics technologies with native cloud-based alternatives, while 23% will supplement on-premises analytics technologies with cloud-based capabilities.

Figure 16. Broad use of cloud-based security technologies

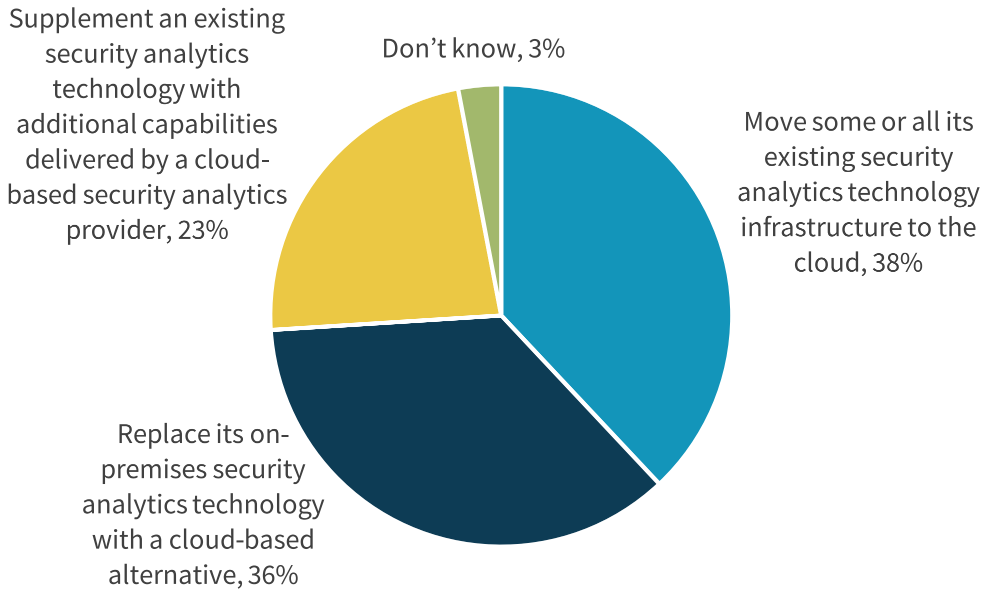
Is your organization considering using public cloud-based security analytics and operations technology (i.e., collect, process, and analyze security telemetry using cloud-based rather than on-premises infrastructure)? (Percent of respondents, N=406)



Source: Enterprise Strategy Group

Figure 17. Alternative strategies for cloud-based security analytics technology skew toward movement and replacement

Which of the following best describes your organization's likeliest security analytics and operations strategy with regards to public cloud services? (Percent of respondents, N=379)

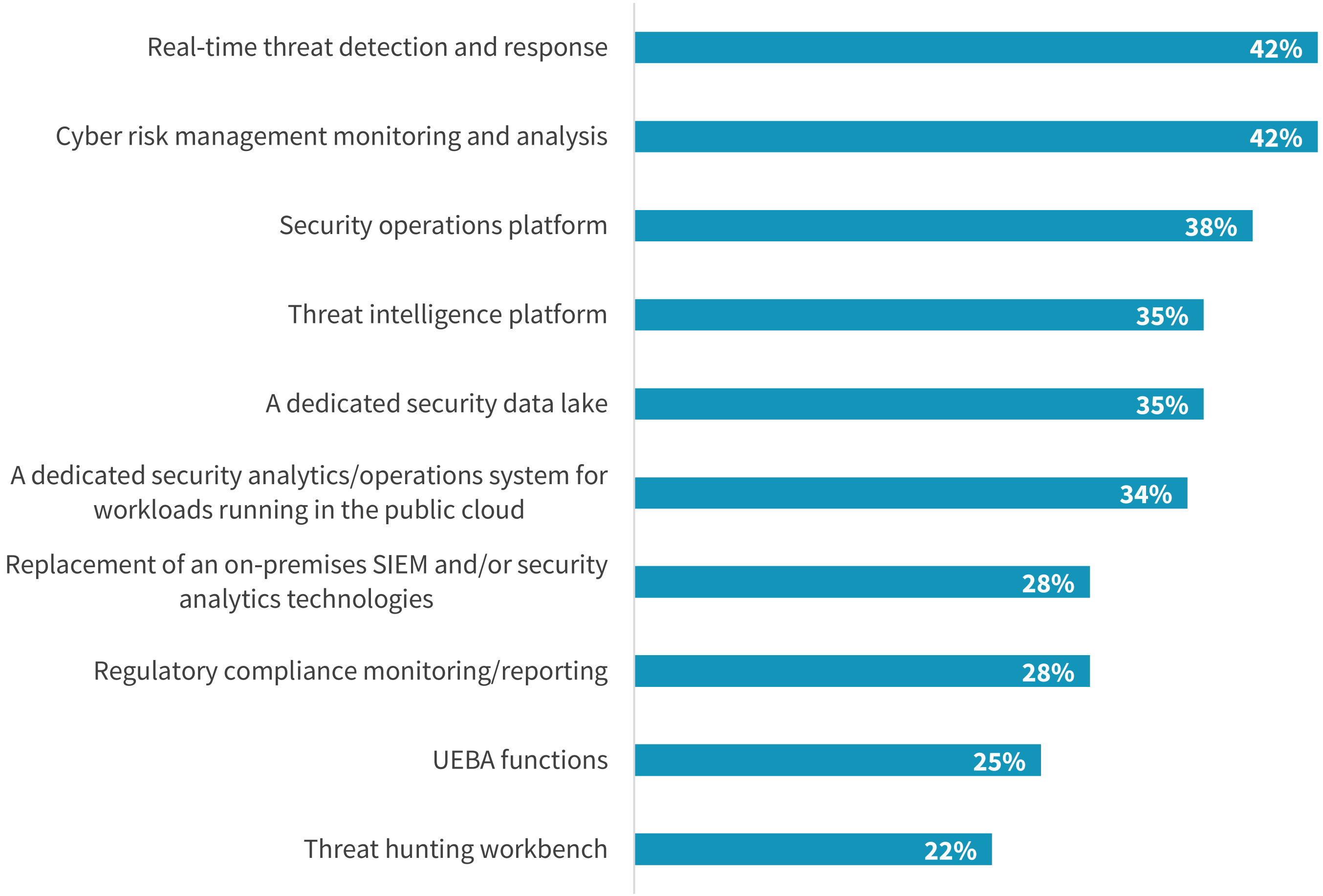


Source: Enterprise Strategy Group

When asked about current and potential cloud-based security analytics use cases, respondents provided an array of responses. According to Figure 18, more than four in ten organizations see these services as a way to provide real-time threat detection and response capabilities and/or monitor and analyze cyber risk management. Additionally, more than half like the platform aspect of cloud, viewing these services as an opportunity to support security operations (38%) and/or threat intelligence activities (35%). All roads seem to lead to cloud-based security analytics in the near future. Organizations must inventory current SOC technologies, map their strengths and weaknesses with emerging requirements, and craft an intelligent migration that includes cloud-based security analytics technologies and supporting managed security services.

Figure 18. Real-time TDR and cyber risk monitoring are the most common cloud-based security operations technology considerations

For which of the following use cases is your organization using – or would your organization consider using – cloud-based security analytics? (Percent of respondents, N=379, multiple responses accepted)



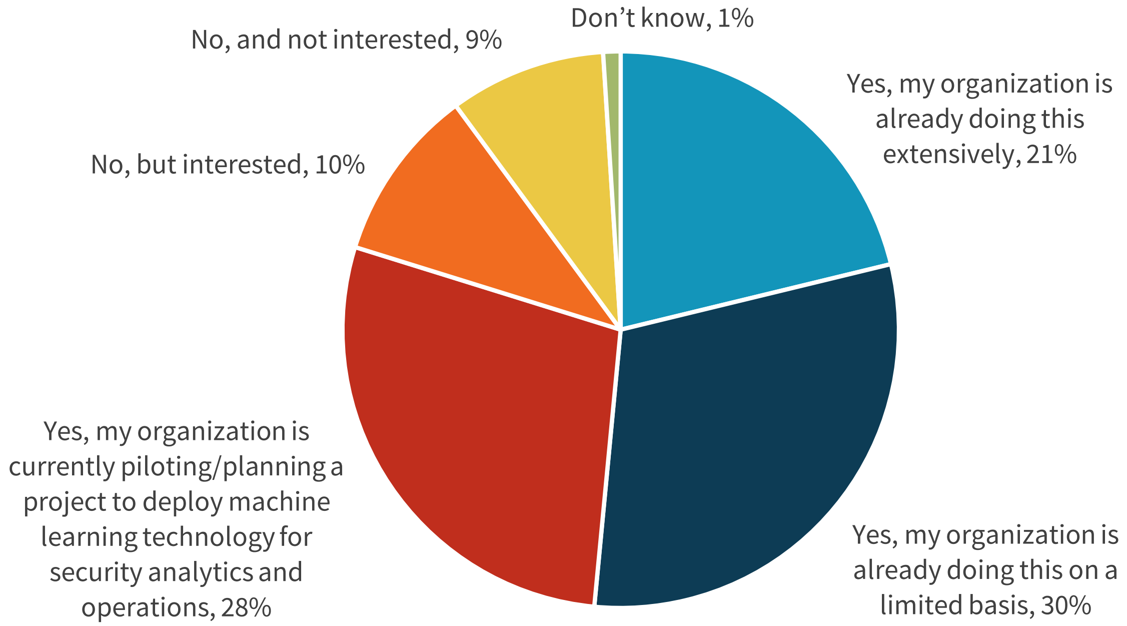
Source: Enterprise Strategy Group

Organizations are incorporating machine learning and automation/orchestration into their technology plans

Aside from managed services, security professionals want their security analytics and operations technology to help address their growing workload. More than half (51%) of organizations are already using machine learning technologies today while another 38% are piloting machine learning technology, planning a machine learning project, or interested in deploying machine learning technology in the future (see Figure 19).

Figure 19. Machine learning widely used for security analytics and operations

Does your organization leverage – or does it plan to leverage – machine learning technologies for security analytics and operations? (Percent of respondents, N=406)



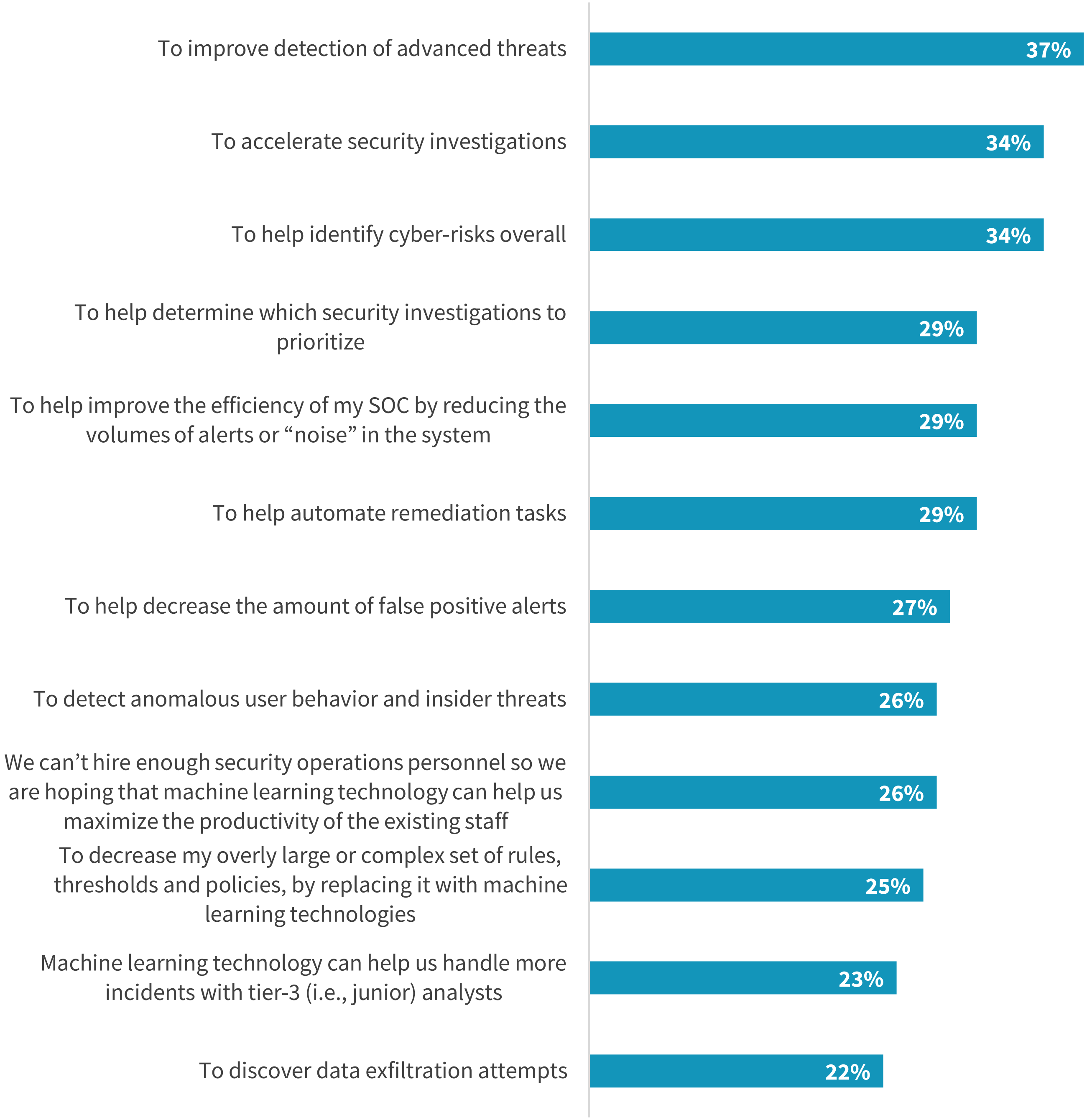
Source: Enterprise Strategy Group

The top use cases for machine learning technology are improving advanced threat detection, accelerating security investigations, and identifying cyber-risks (see Figure 20).

Many organizations remain cautious of machine learning technologies, and they will likely supplement rather than replace existing layers of defense. Nevertheless, machine learning will gain incremental traction within the SOC. Rather than blind faith in algorithms, CISOs must develop the expertise necessary to deploy, operate, and fine-tune machine learning technologies to achieve a "force multiplier" effect on security operations.

Figure 20. Primary reasons for machine learning are acceleration and accuracy improvements

What are the primary reasons for your organization's usage of or interest in machine learning to support analytics and operations? (Percent of respondents, N=363, multiple responses accepted)

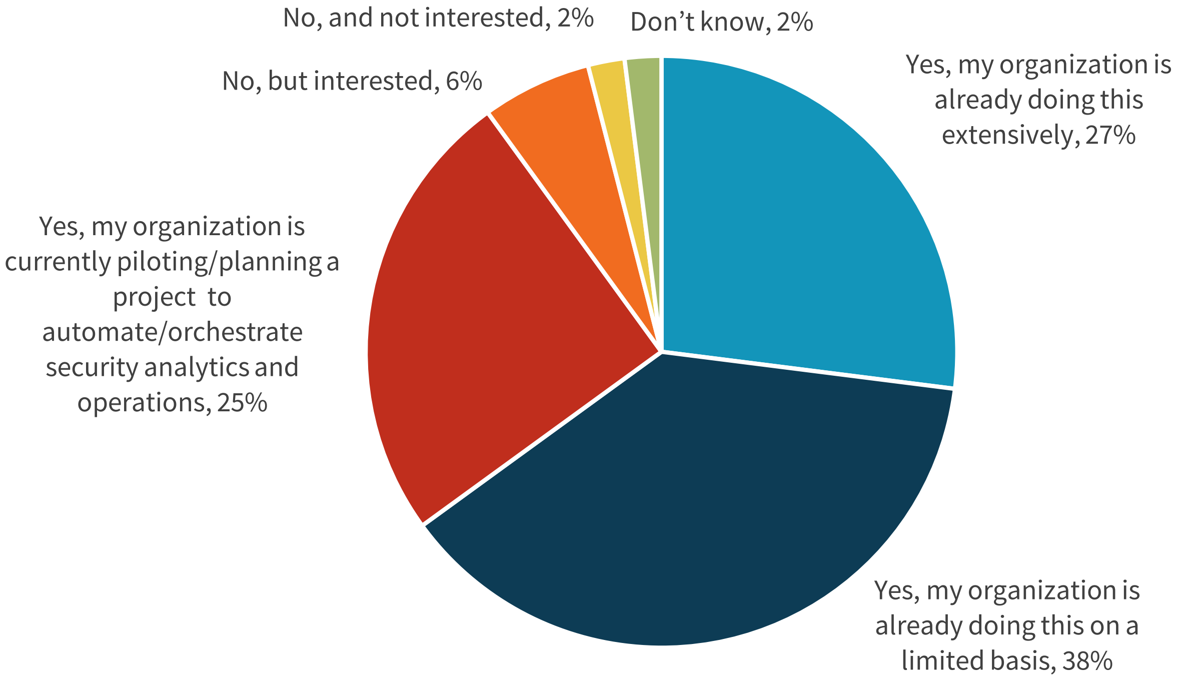


Source: Enterprise Strategy Group

Similar to machine learning, many organizations need help with security operations process automation and orchestration. To address this requirement, 27% of organizations have deployed technologies for security analytics/operations automation and orchestration extensively while 38% have done so on a limited basis (see Figure 21). Another 31% are piloting security operations automation/orchestration technology, planning a project, or interested in doing so.

Figure 21. Most use security operations automation and orchestration to some extent

Has your organization deployed – or does it plan to deploy – technologies designed for security analytics and operations automation and orchestration? (Percent of respondents, N=406)



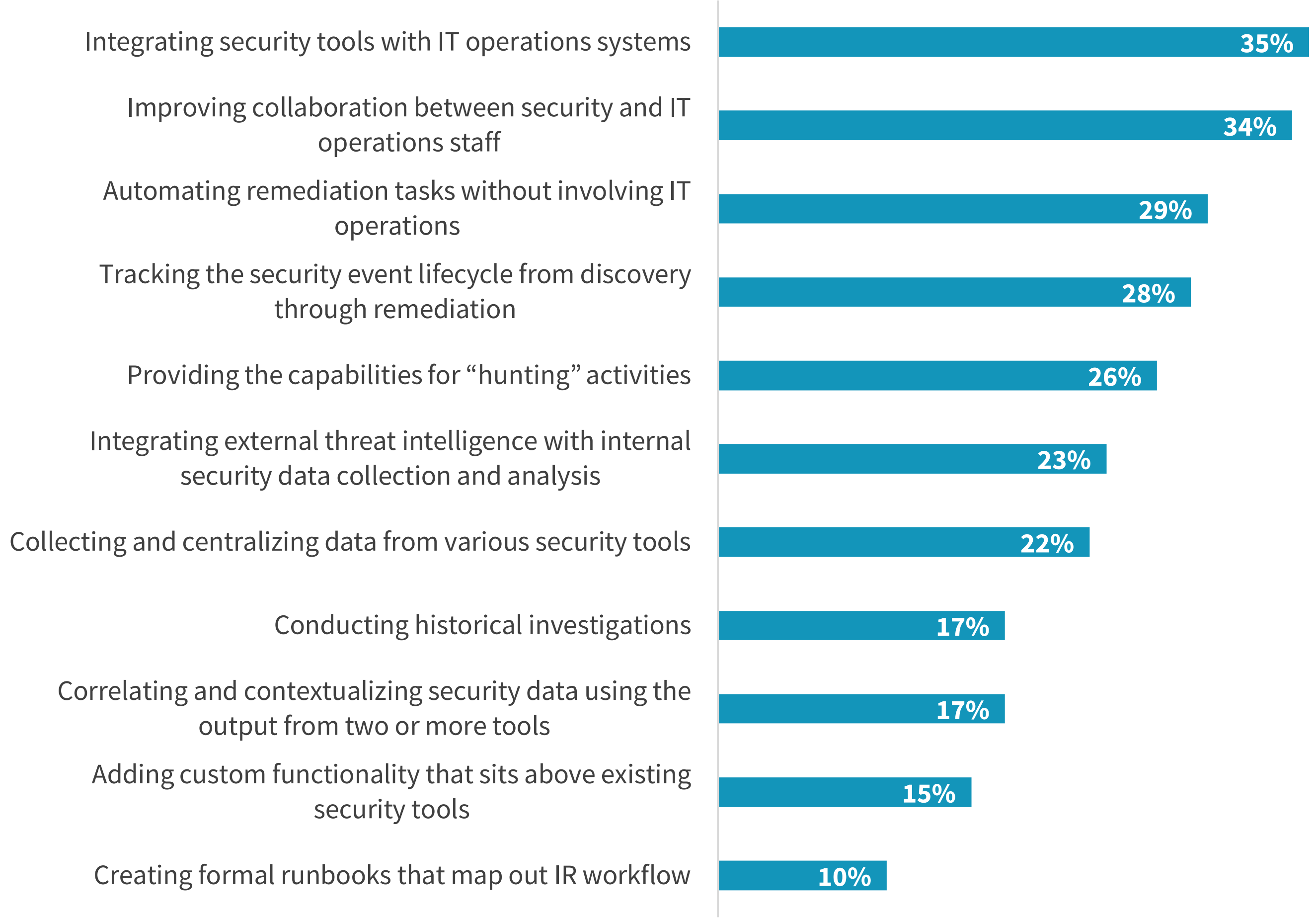
Source: Enterprise Strategy Group

The top use cases for machine learning technology are integrating security and IT operations technologies, improving collaboration between security and IT operations, automating remediation tasks, and tracking security event lifecycles (see Figure 22).

Security operations process automation should start with process assessment and an evaluation of all tasks associated with a workflow. CISOs should establish best practices by streamlining and optimizing manual processes and then (and only then) applying technologies for process automation.

Figure 22. Top use cases for security operations automation and orchestration bridge security and IT operations

What types of tasks are or would be the top priorities for security operations automation/orchestration? (Percent of respondents, N=366, three responses accepted)



Source: Enterprise Strategy Group

Conclusion

Based upon the data presented in this report, ESG reached several conclusions on the current and future state of security analytics and operations. Security analytics and operations requirements are diverse and rapidly changing. Organizations must keep up with dynamic cyber-threats across a growing attack surface, including public cloud infrastructure and new device types. This goal is simply “mission impossible” using disconnected point tools, manual processes, and a SOC team with limited personnel and skills. CISOs must address SOC deficiencies with long-term and comprehensive strategies that can improve security efficacy, bolster operational efficiency, and support business objectives.

Security analytics and operations depend upon access to large volumes of real-time and historical data. To collect, process, analyze, and act upon gigabytes, terabytes, and even petabytes of security data, organizations must implement scalable high-performance data pipelines while establishing best practices for security data management. This process starts by defining and fine-tuning security analytics and operations objectives and then working backward to identify critical security data sources, understand data pipeline requirements, and measure results. Large organizations must ensure that security teams have appropriate data management skills so they can build and operate security data pipelines at scale.

The data collected as part of this research project paints a clear picture: Security technologies are moving to the cloud to address the scale, cost, and complexity of security analytics and operations. CISOs must plan for this cloud migration so they can create a security operations and analytics platform architecture (SOAPA) that helps them prevent, detect, and respond to security incidents across hybrid IT infrastructure.

Finally, ESG’s research presented in this report represents a cry for security analytics and operations help. To address the scale and scope of security operations along with the ongoing cybersecurity skills shortage, SOC managers will lean on artificial intelligence, security process automation, and managed services moving forward. Once again, CISOs need a detailed plan on how these elements will augment the SOC staff, supplement and improve SOC processes, and better safeguard critical business assets.

Research methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between August 14, 2019 and August 25, 2019. To qualify for this survey, respondents were IT or security professionals involved with the planning, implementation, and/or operations of their organization's information security policies, processes (including purchase decisions), or technical safeguards. Additionally, these respondents had to be familiar with their organization's collection and/or analysis of security data in support of information security management strategy. 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 406 cybersecurity decision makers.

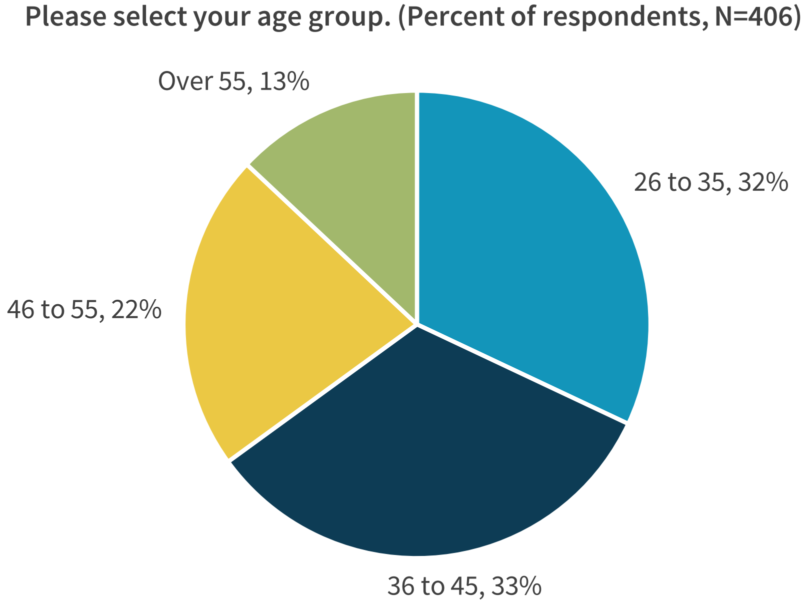
Please see the Respondent demographics section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Respondent demographics

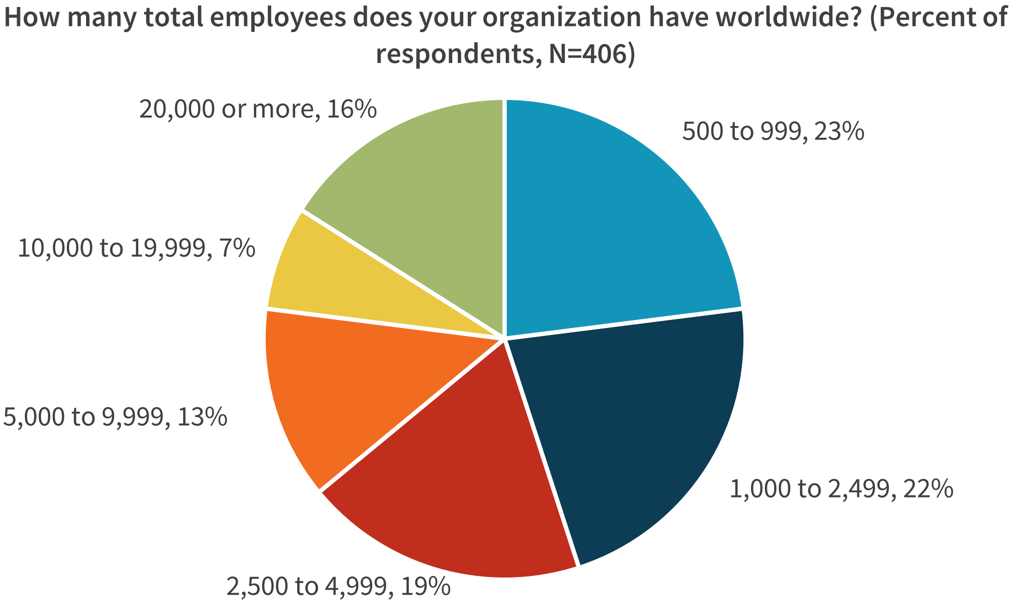
The data presented in this report is based on a survey of 406 qualified respondents. Figure 23 through Figure 26 detail the demographics of the respondent base, both at an individual and organizational level.

Figure 23. Survey respondents by age



Source: Enterprise Strategy Group

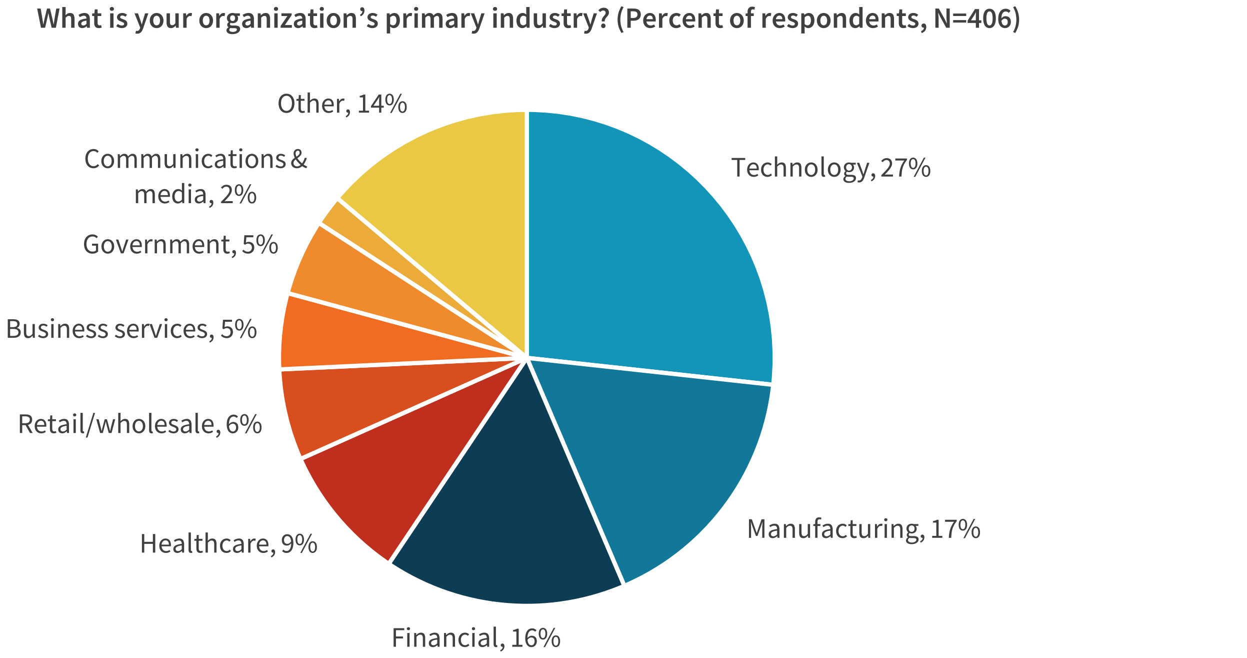
Figure 24. Survey respondents by number of employees



Source: Enterprise Strategy Group

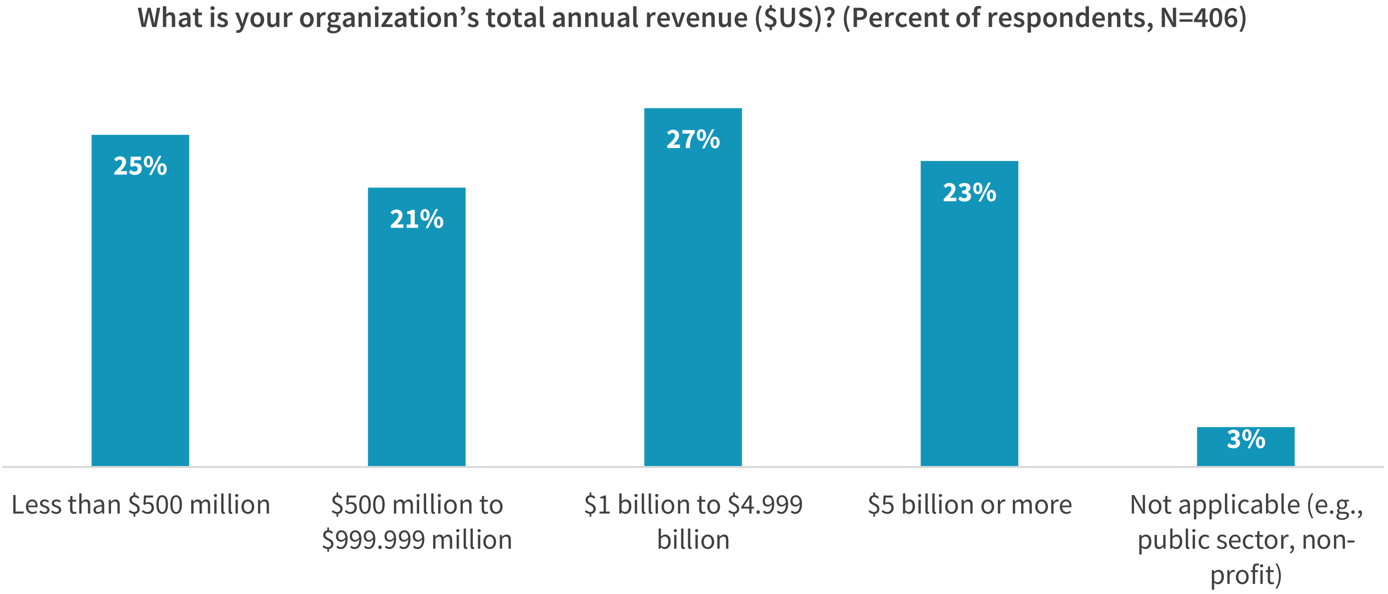
Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified responses from individuals in 25 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 25.

Figure 25. Survey respondents by industry



Source: Enterprise Strategy Group

Figure 26. Survey respondents by annual revenue



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com   ✉ contact@esg-global.com   ☎ 508.482.0188