Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

The Impact of XDR in the Modern SOC

Dave Gruber, Senior ESG Analyst
Jon Oltsik, Senior Principal ESG Analyst, ESG Fellow

NOVEMBER 2020

CONTENTS

Research Objectives

Threat detection and response is a core component of modern security programs, driving investment in tools to improve visibility, efficacy, and efficiency. As organizations commit to and extend EDR, NDR, or other security analytics solutions in support of broad threat detection and response programs, new opportunities arise for XDR. Organizations can increase business agility when threats are better understood and controlled. Rapidly and effectively correlating threat data across multiple threat vectors leads to increased threat visibility, more rapid and automated response and mitigation, and a reduced dependence on highly skilled security analysts.

More telemetry is generally desired, but correlation and analysis is a heavy lift. Most organizations can see value in combining threat data from multiple threat vectors to provide context and accelerate detection and response; however, most lack the expertise and tools to correlate data, often leading to the reactive elimination of point threats without understanding broad attack campaigns. Additionally, many organizations don't have SIEMS today or don't have the resources to learn, configure, or operate a SIEM successfully. In order to gain insight into these trends, ESG surveyed 388 IT and cybersecurity professionals at organizations in North America (US and Canada) personally responsible for evaluating, purchasing, and managing detection and response strategies, processes, and technologies.

THIS STUDY SOUGHT TO:

Examine the people, process, and technology utilization in security teams throughout their journey to master threat detection and response.

Understand buyer preferences, concerns, and conflicts related to XDR solutions and architecture.

Determine current buyer perception of XDR concepts and potential business outcomes.

Identify key value points, required metrics to back them up, and what's expected from vendors to rationalize the sale of an XDR solution.

Back to Contents

Research Highlights

ORGANIZATIONS SEE XDR AS A PATH TO INCREASED SECURITY EFFICACY.

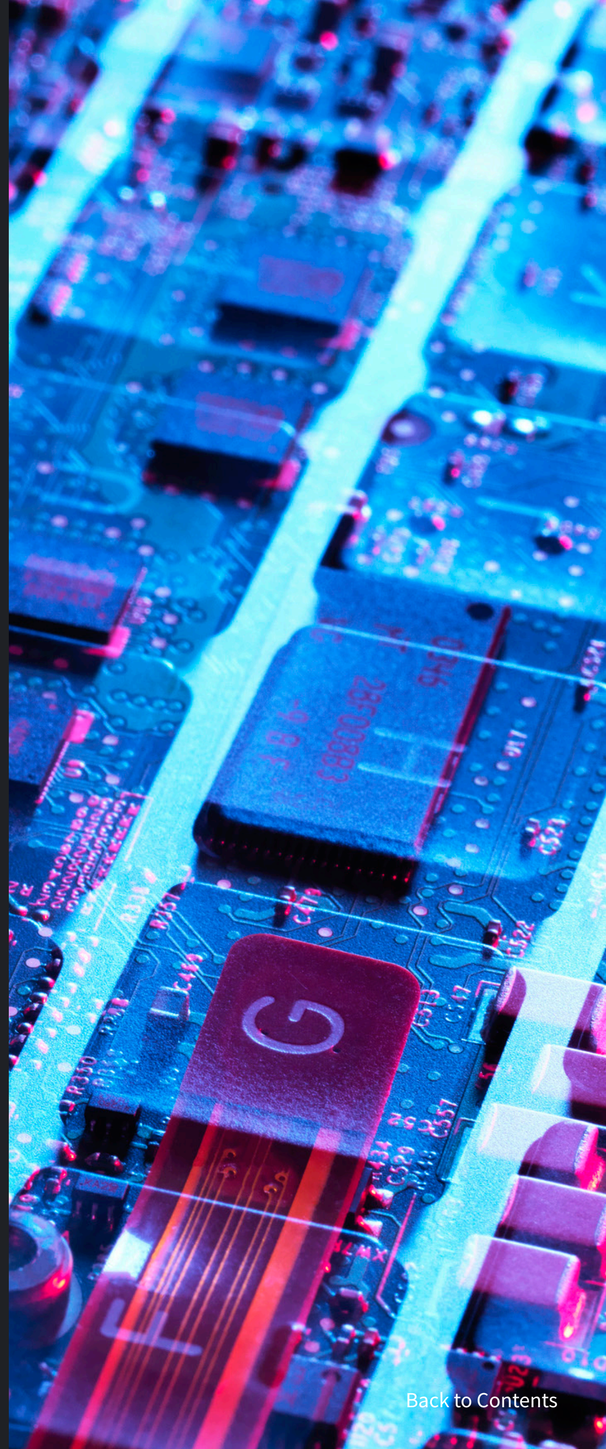
Threat detection and response goals include improving detection of advanced threats, increasing automation tasks, and improving the mean time to respond (MTTR) to threats. Organizations see XDR as a potential path to helping them detect, identify, and understand complex attacks across the kill chain.

DATA INGEST IS A MAJOR CHALLENGE FOR MOST.

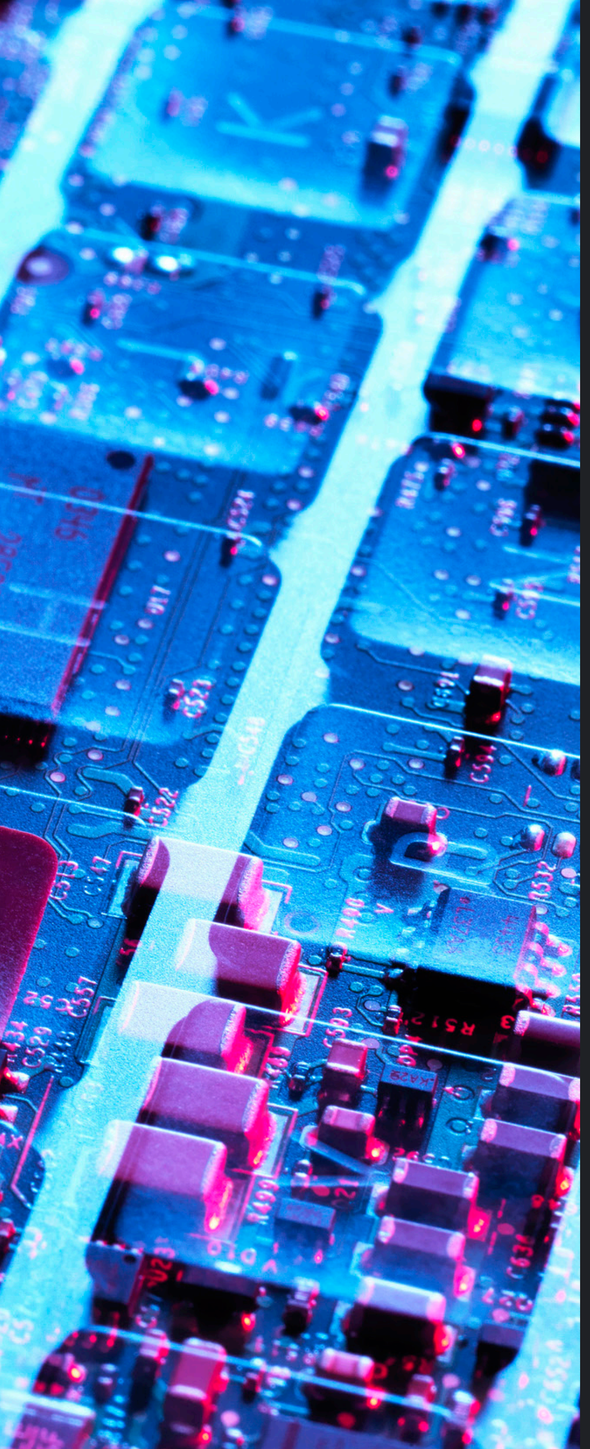
Cybersecurity analytics and operations depend upon collecting, processing, analyzing, and acting upon security data. To accommodate the volume, velocity, and variety of security data, XDR technologies must be anchored by a modern data pipeline that can collect and process security data at scale across hybrid IT.

XDR MUST EXTEND SIEM CAPABILITIES IN THE NEAR TERM.

When looking at all the tools used today for threat detection and response, more than half of respondents say that their SIEM is one of their three most valuable tools. XDR can not only improve threat detection and response, but can also help modernize, integrate, and automate security operations processes.



Back to Contents



XDR MUST INCLUDE COMPANION MDR SERVICES.

Managed detection and response services (MDR) are becoming mainstay components of most modern security programs. More than half of organizations believe that an MDR provider can do a better job at threat detection and response than they can alone.

CLOUD DETECTION AND RESPONSE REMAINS A GAP, AND A GOOD STARTING PLACE FOR XDR.

When thinking about where to start with XDR initiatives, 43% of respondents say their organization would focus on implementing an XDR solution in support of adding threat detection and response capabilities for cloud-based workloads and SaaS applications. Additionally, nearly half would be willing to replace individual controls with integrated XDR solutions.

THE XDR MOVEMENT COULD BE ATTRACTIVE FOR MOST ORGANIZATIONS.

More than two-thirds of organizations expect to make XDR investments in the next 6-12 months. Aside from a dedicated budget, XDR funding could come from elsewhere like the SOC technology budget, the EDR budget, or even the SIEM budget.

Back to Contents

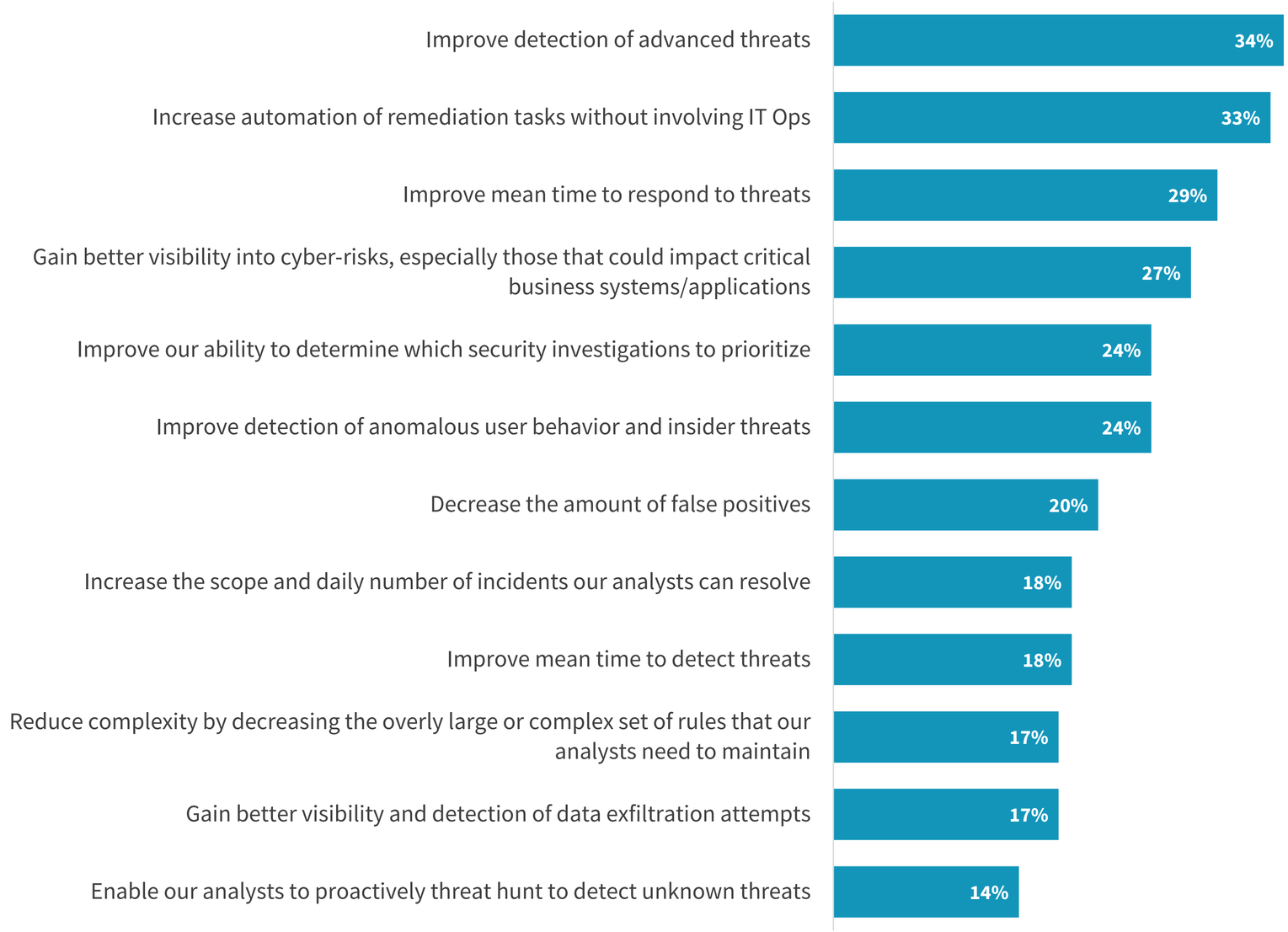
Organizations see XDR as a path to increased security efficacy.

Organizations Need Threat Detection and Response Improvements

Security teams continue to struggle in fundamental areas like detecting and responding to threats as quickly as possible. This indicates that existing solutions aren't working well, so it's not surprising that threat detection and response goals include improving detection of advanced threats (34%), increasing automation tasks (33%), and improving the mean time to respond (MTTR) to threats (29%).

Simply stated, SOC teams need better threat detection and response efficacy, especially as it relates to unknown threats that move laterally across networks over time.

Top areas of TDR focus.

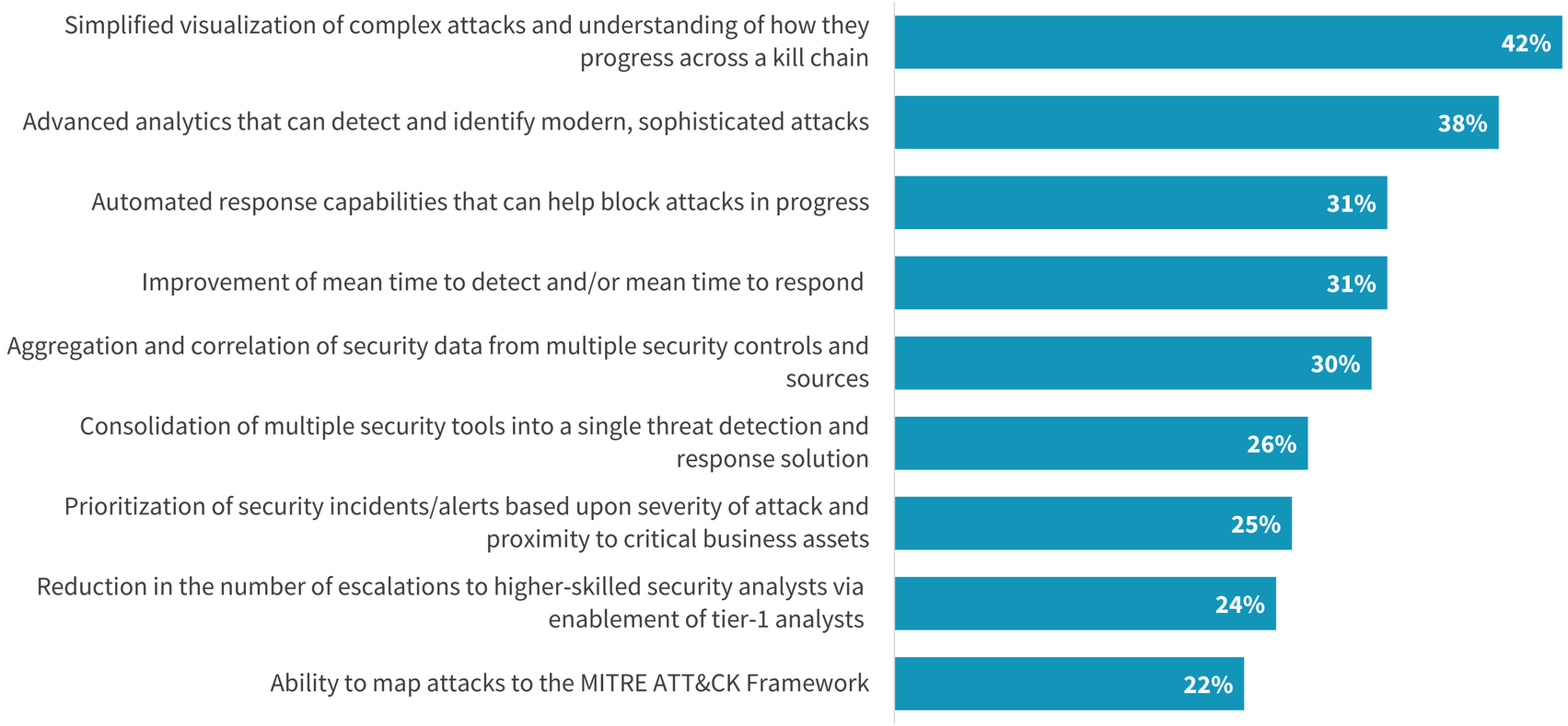


Back to Contents

Therefore, Detecting Complex Attacks Is an XDR Priority

Organizations see XDR as a potential path to helping them detect, identify, and understand complex attacks across the kill chain. For most, this means investing in a solution with simplified visualization across the attack chain, and advanced analytics capable of correlating signals from many sources. Nearly one-third (31%) of organizations also want automated response capabilities. This will be especially effective if XDR solutions can block attacks and update rule sets across endpoints, networks, servers, and cloud-based workloads.

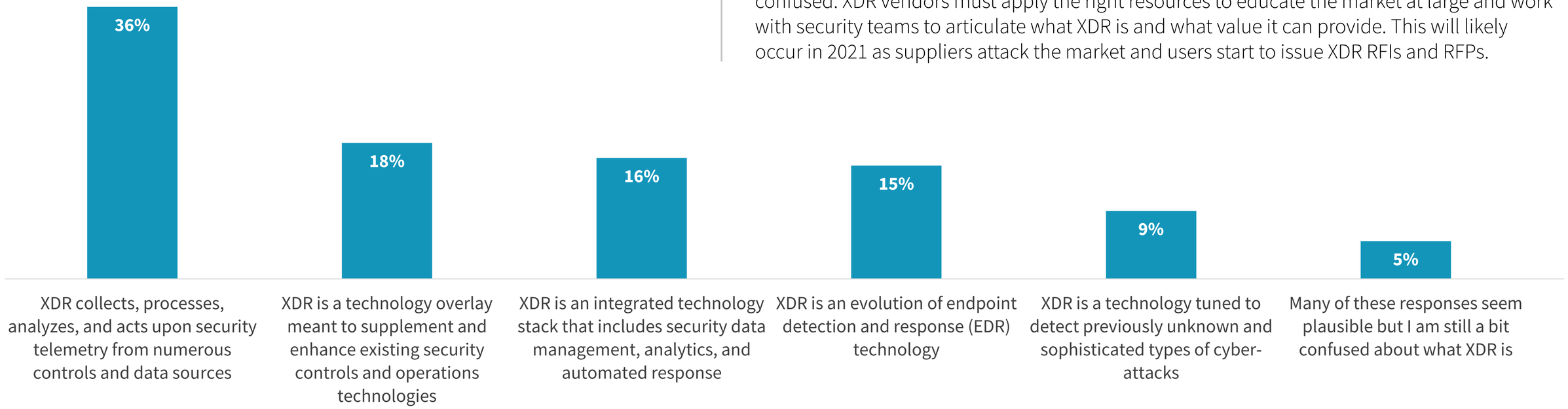
Most appealing XDR capabilities.



Back to Contents

> ***XDR technology may help*** *organizations overcome these challenges, but cybersecurity professionals aren't clear about just what XDR is."*

Perceptions of XDR.



Expectations of XDR Vary Widely

The research clearly points to problems around threat detection and response using existing security controls and management tools. XDR technology may help organizations overcome these challenges, but cybersecurity professionals aren't clear about just what XDR is.

The plurality of respondents (36%) see XDR as a consolidated security data pipeline used for collecting, processing, and analyzing data from numerous controls and sources. Others perceive XDR as a technology overlay (i.e., software) meant to supplement existing controls, or an integrated technology stack, or even an evolution of endpoint detection and response (EDR) technology.

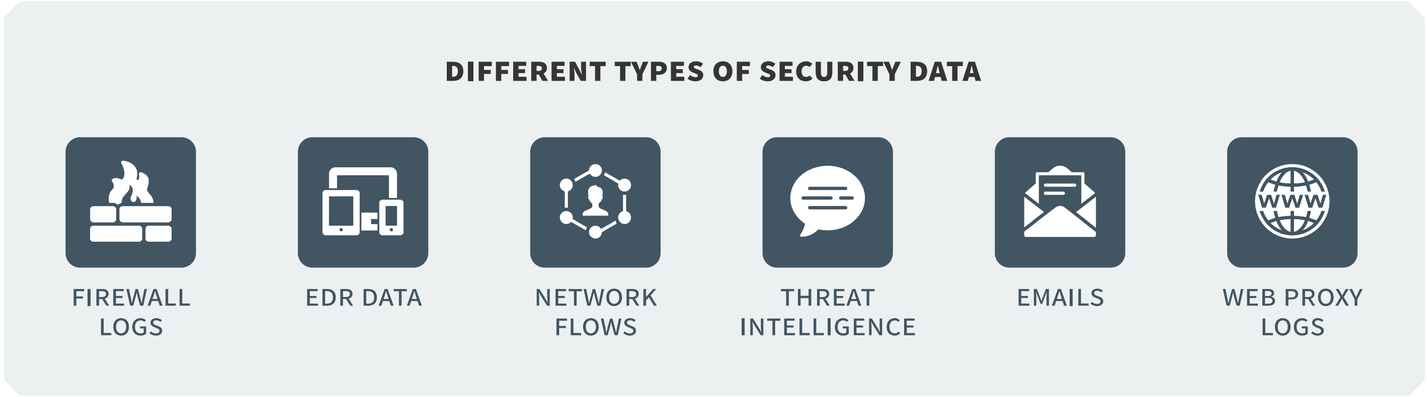
In fact, XDR is all these things and more today, but the data indicates that users remain confused. XDR vendors must apply the right resources to educate the market at large and work with security teams to articulate what XDR is and what value it can provide. This will likely occur in 2021 as suppliers attack the market and users start to issue XDR RFIs and RFPs.

Back to Contents

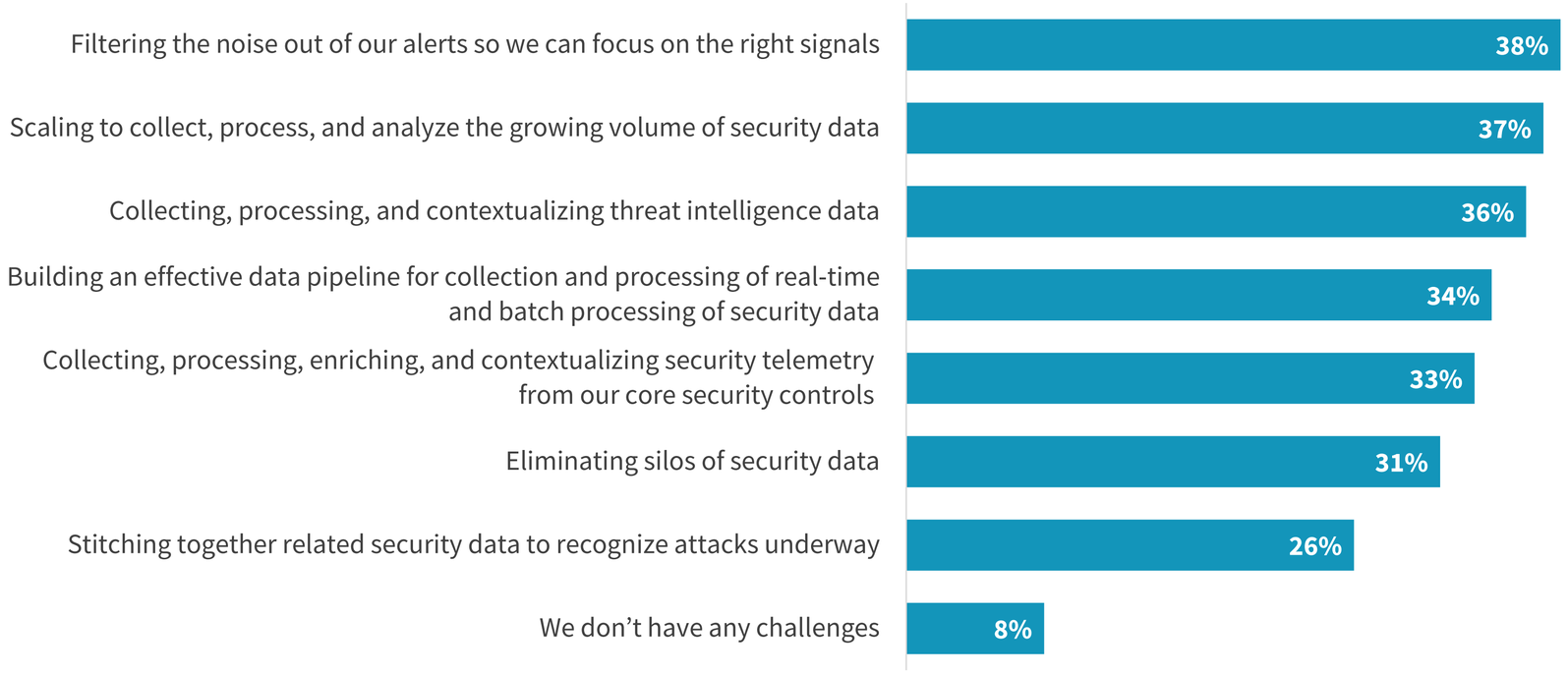
Data ingest is a major challenge for most.

Data Issues Plague Most Organizations

Cybersecurity analytics and operations depend upon collecting, processing, analyzing, and acting upon growing volumes of security data. What types of data? Firewall logs, EDR data, network flows, threat intelligence, emails, web proxy logs, and many other telemetry sources. The ESG research indicates that organizations encounter many issues with security data management like filtering out noisy alerts (38%), scaling the data pipeline (37%), collecting/processing/contextualizing threat intelligence (36%), and building an effective data pipeline for stream and batch processing (34%).

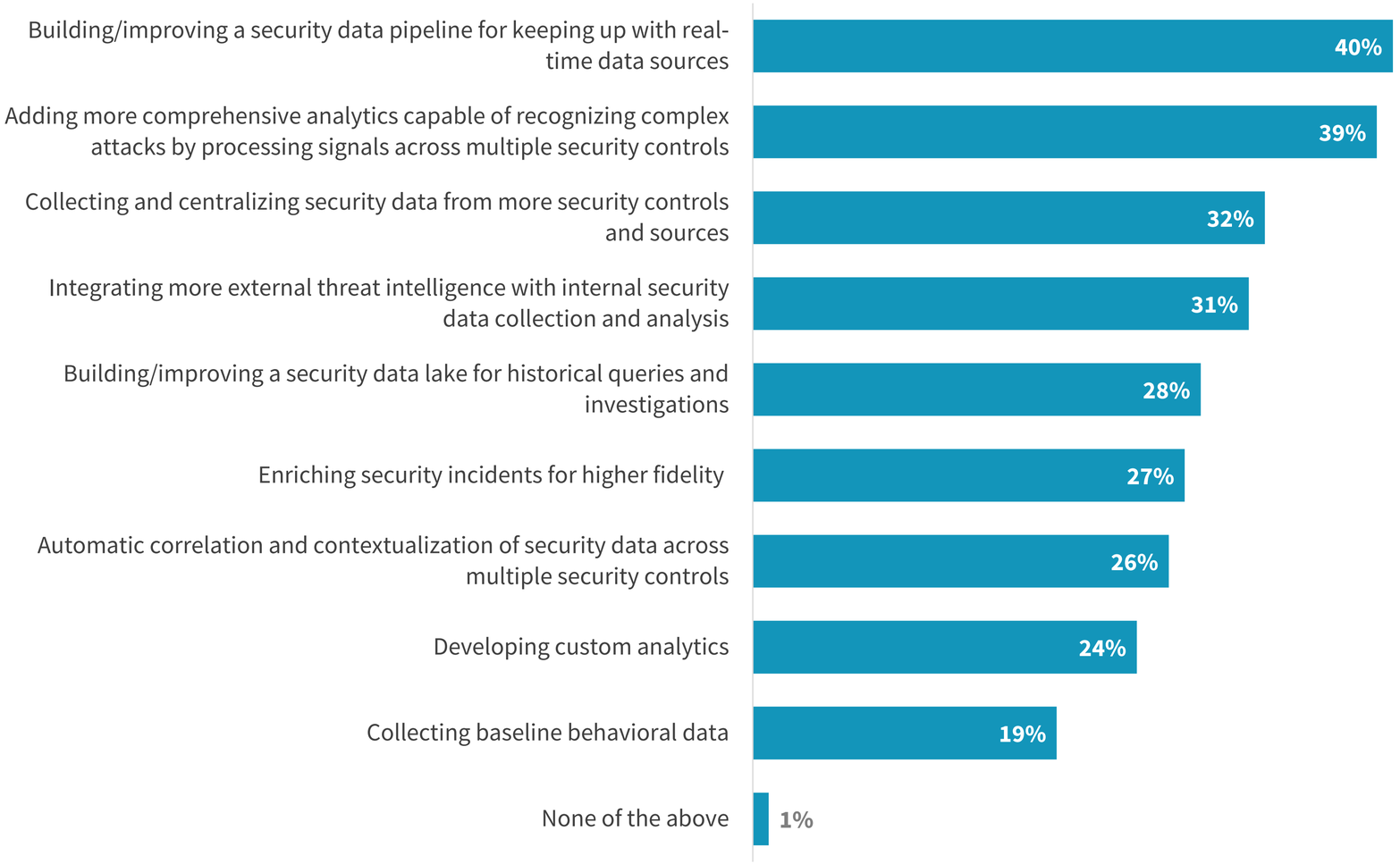


Top challenges stemming from security data and alerts.



Back to Contents

Security data pipeline investment priorities.



XDR Must Address the Security Data Pipeline

To overcome data management issues and potential data bottlenecks, organizations are building/improving their security data pipeline (40%), processing/analyzing signals across multiple security controls to detect complex attacks (39%), and collecting/centralizing more security data from various sources (32%). This represents a lot of engineering work scaling the data pipeline.

To accommodate the volume, velocity, and variety of security data, XDR technologies must be anchored by a modern data pipeline that can collect and process security data at scale across hybrid IT. Lacking this capability, XDR solutions must be built on top of open source and commercial log management systems or cloud-based databases and storage offerings.

Back to Contents

XDR must extend SIEM capabilities in the near term.

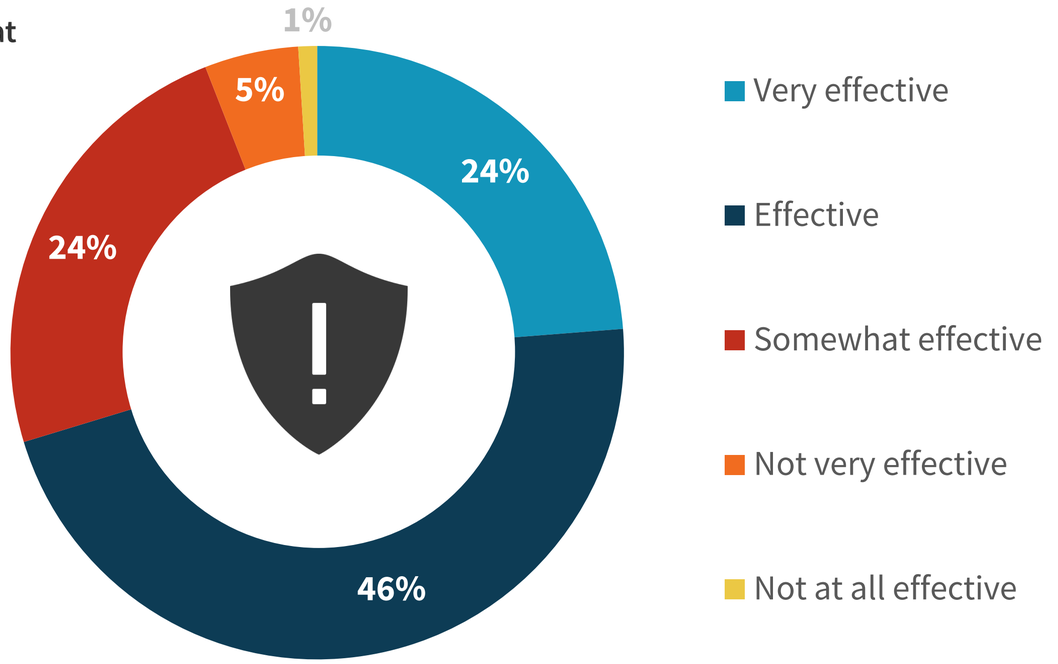
SIEM Is both Popular and Deemed Effective for Security Operations

When looking at all the tools used today for threat detection and response, 58% say that their SIEM is one of their three most valuable tools. This may not be a surprise, given that SIEM is the predominant mechanism for consolidating, storing, correlating, and reporting on security data. Users claim their organizations find that EDR, NDR, and threat intelligence platforms are also effective for security operations.

Even among those who don't identify SIEM as one of their three most effective TDR tools, 71% still view the technology as being very effective or effective at threat detection and response.

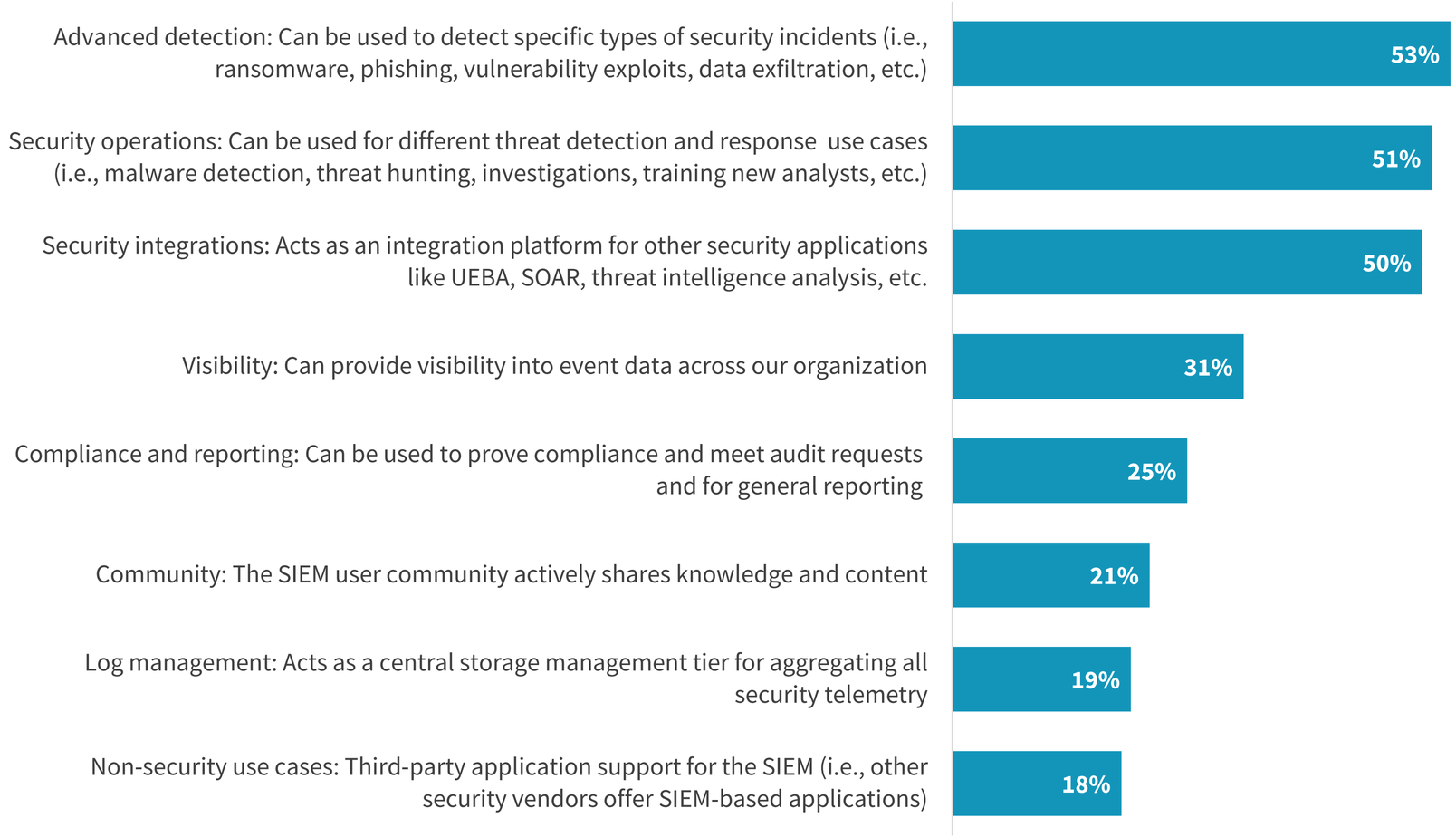
> ***58% of respondents identify SIEM*** *as one of their organization's most effective threat detection and response tools."*

Effectiveness of SIEM for threat detection and response.



Back to Contents

Most valuable SIEM attributes.



SIEM Is a Core SOC Platform Today…

At least half of security professionals said the most valuable attributes of their SIEM include its ability to help with advanced detection of specific types of security incidents (ransomware, phishing, vulnerability exploits, data exfiltration, etc.); its ability to be used for different threat detection and response use cases (malware detection, investigations, threat hunting, training new analysts); and its ability to integrate data from other security applications like UEBA, SOAR, and threat intelligence. This seems to indicate that SIEM technology anchors many SOCs today.

Back to Contents

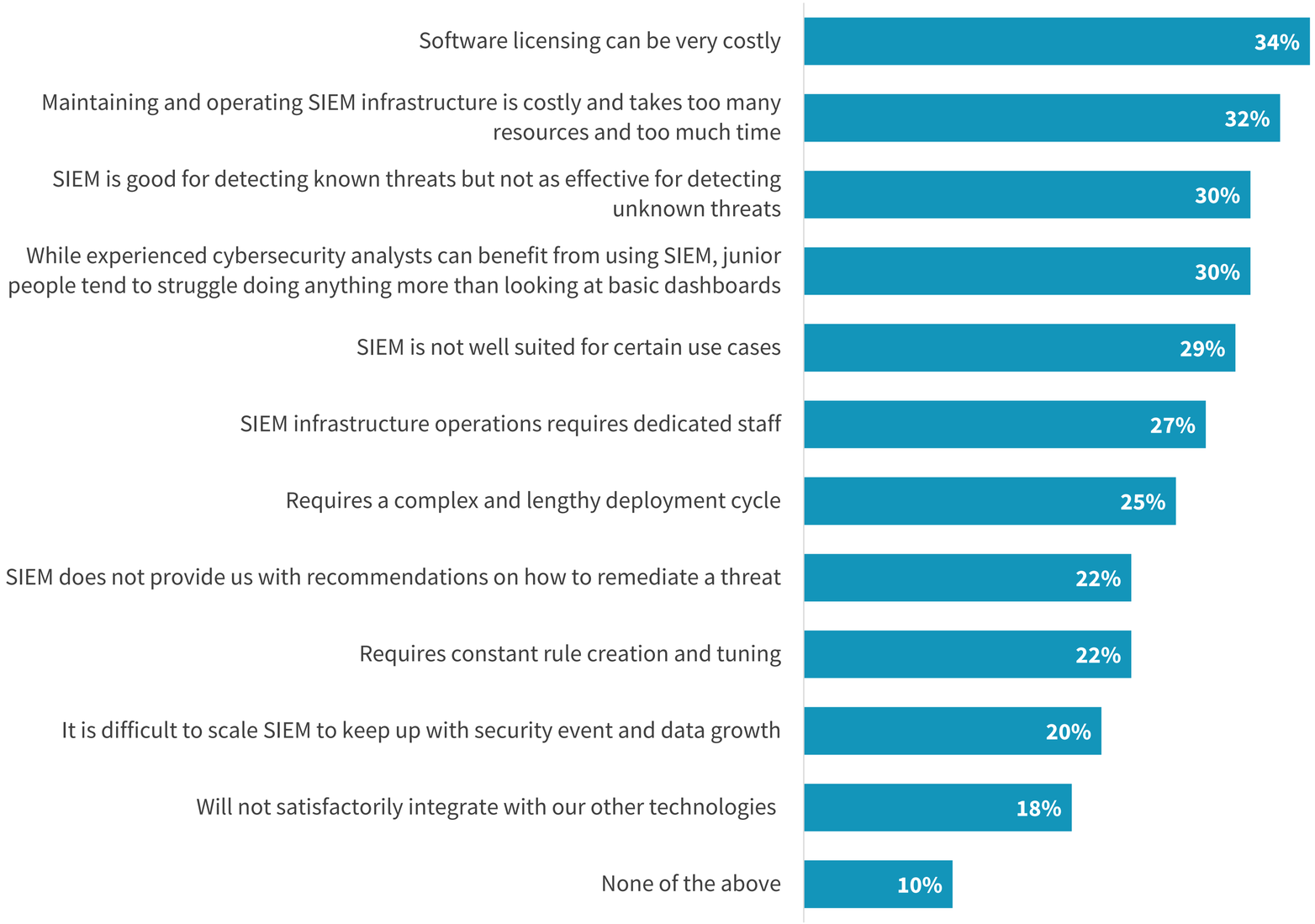
…But SIEM Still Creates Many Challenges

Despite some of the positive attributes of SIEM, many organizations admit that SIEM can be costly and complex. For example, 34% say SIEM licensing can be costly, while 32% lament that maintaining and operating SIEM infrastructure is costly, requiring a lot of resources and time to operate. Furthermore, 30% say that while experienced analysts can benefit from SIEM, junior analysts struggle with SIEM learning curves.

What's most telling here is that 30% of organizations feel that, while SIEM can be effective at detecting known threats, it is not as effective at identifying unknown threats.

This graphic can be seen as a microcosm of the state of security operations. Tools are costly, complex, and ineffective at detecting unknown and sophisticated threats that move laterally across networks and cloud-based workloads. Therefore, CISOs are desperately seeking solutions that improve security efficacy while easing the cost and complexity of security operations. This is where XDR may fit.

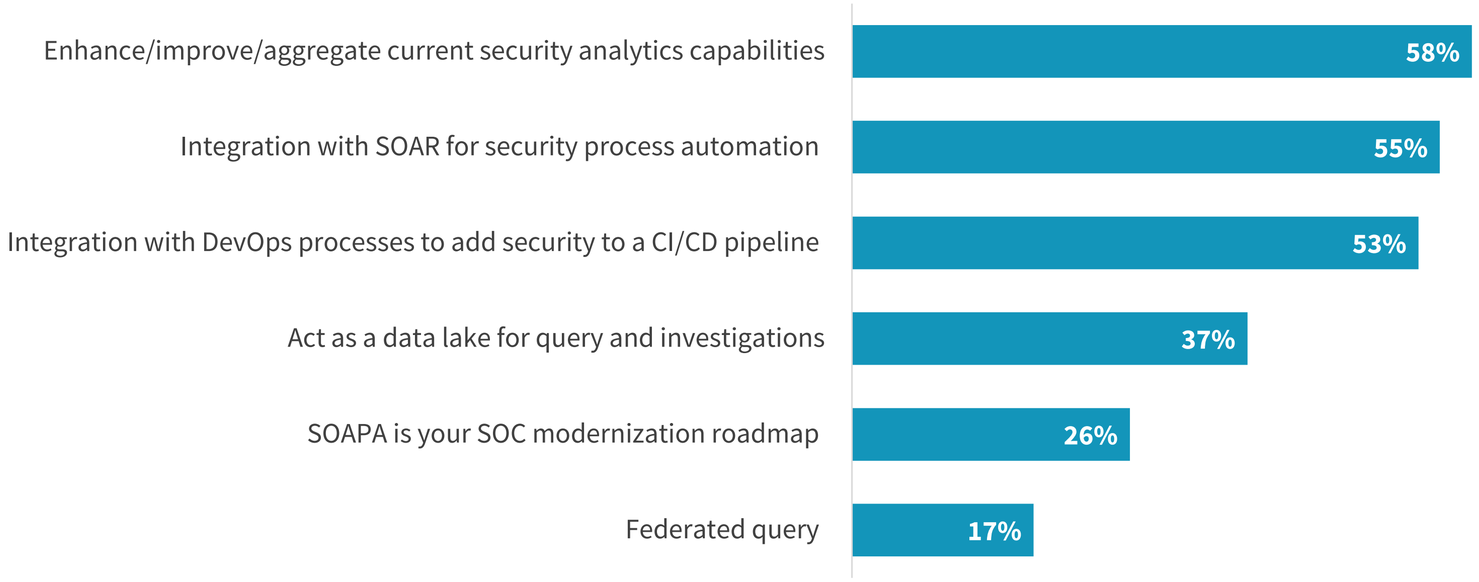
Biggest SIEM challenges.



Back to Contents

> ***More than half of survey respondents*** *believe XDR could play a role in improving current security analysts' capabilities…"*

Perceptions of XDR.



XDR Could Have a Central Role in SOC Modernization

The prior data can be seen as a microcosm of the state of security operations. Tools are costly and complex and are ineffective at detecting unknown and sophisticated threats that move laterally across networks and cloud-based workloads. Therefore, CISOs are desperately seeking solutions that improve security efficacy while easing the cost and complexity of security operations.

More specifically, more than half of survey respondents believe XDR could play a role in improving current security analysts' capabilities, integrating with SOAR for security operations process automation, and integrating with DevOps processes to add security to the CI/CD pipeline.

In this way, XDR can not only improve threat detection and response but can also help modernize, integrate, and automate security operations processes. In this way, XDR could become a SOC modernization catalyst.

Back to Contents

XDR must include companion MDR services.

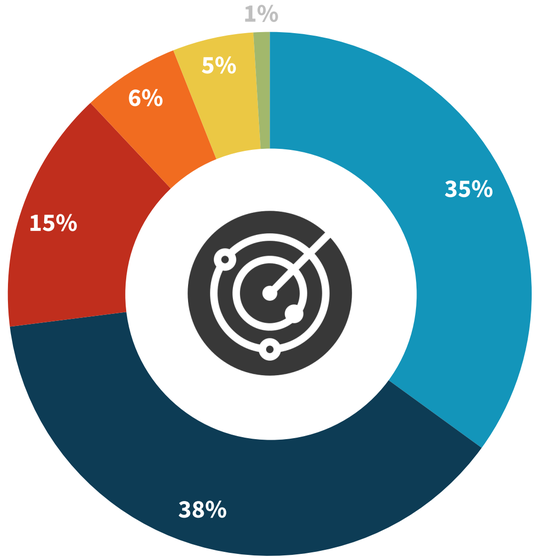
MDR Has Become a Core Component of Most Security Programs

Managed detection and response services (MDR) are becoming a mainstay component of most modern security programs, with 73% of organizations either already using an MDR provider or actively working on a project to adopt MDR services.

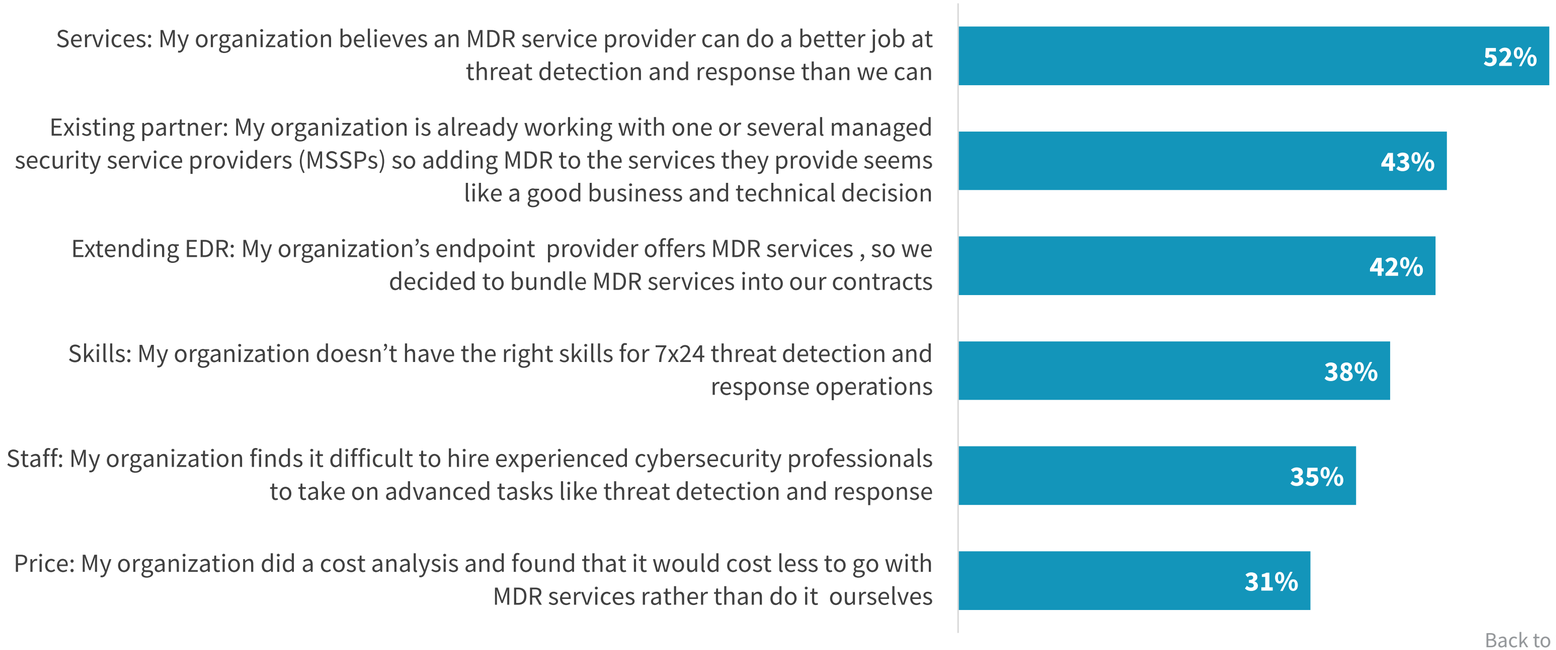
Why are organizations flocking to MDR? Simply stated, because they need help. More than half believe that an MDR provider can do a better job at threat detection and response than they can alone. Additionally, 43% added MDR to an existing MSSP contract, 42% began procuring MDR via their endpoint provider, 38% see MDR as a means for skills augmentation, and 35% need MDR services for staff augmentation.

The data seems to indicate that XDR technology alone is not enough; security professionals need hands-on help.

Plans for MDR services.



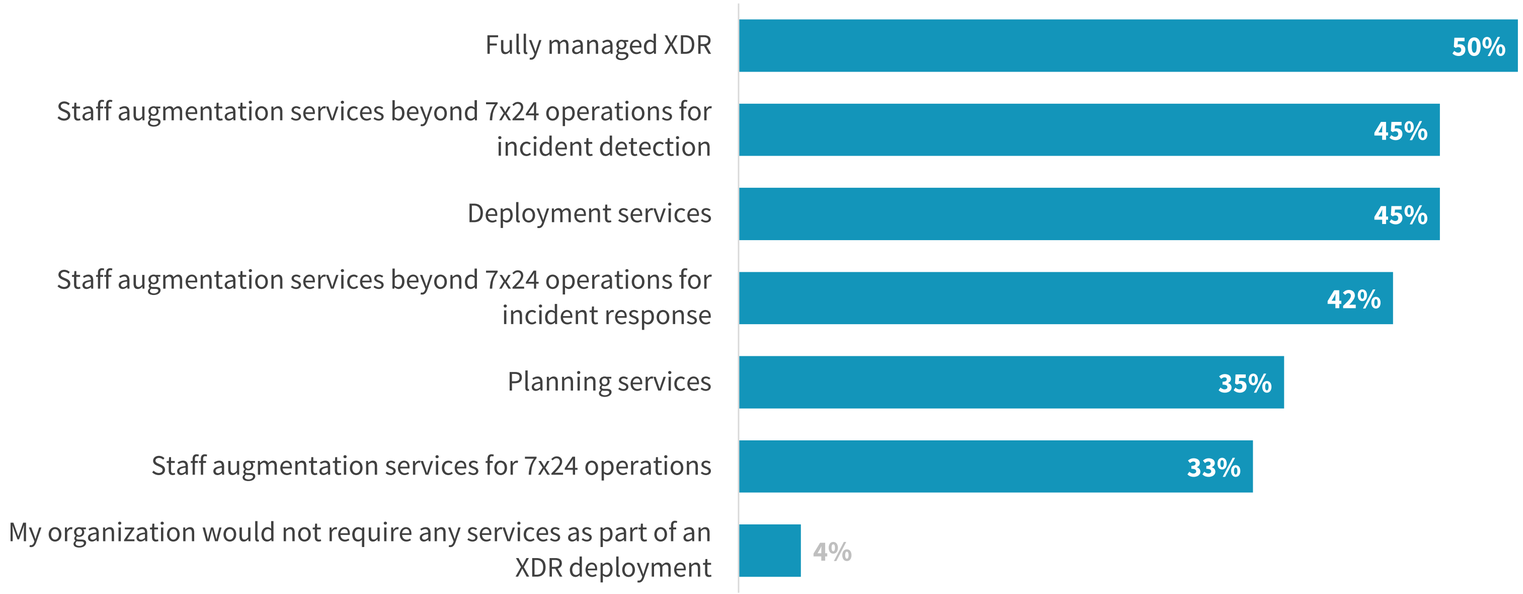
Primary drivers behind MDR



Back to Contents

> ***Half of all respondents*** *are interested in fully managed XDR."*

MDR services of interest.



Half Will Consider Managed XDR

The data seems to indicate that XDR technology alone is not enough, and security professionals need hands-on help. So, what about managed XDR? This seems like an appealing alternative to in-house XDR operations, with half of all respondents interested in fully managed XDR. Other popular services include staff augmentation beyond 7x24 security operations for threat detection (45%), XDR deployment services (45%), and staff augmentation beyond 7x24 security operations for incident response (42%).

Given these broad requests for services, XDR technology providers must partner with enterprise-class MSSPs or offer a full menu of services.

Back to Contents

Cloud detection and response remains a gap, and a good starting place for XDR.

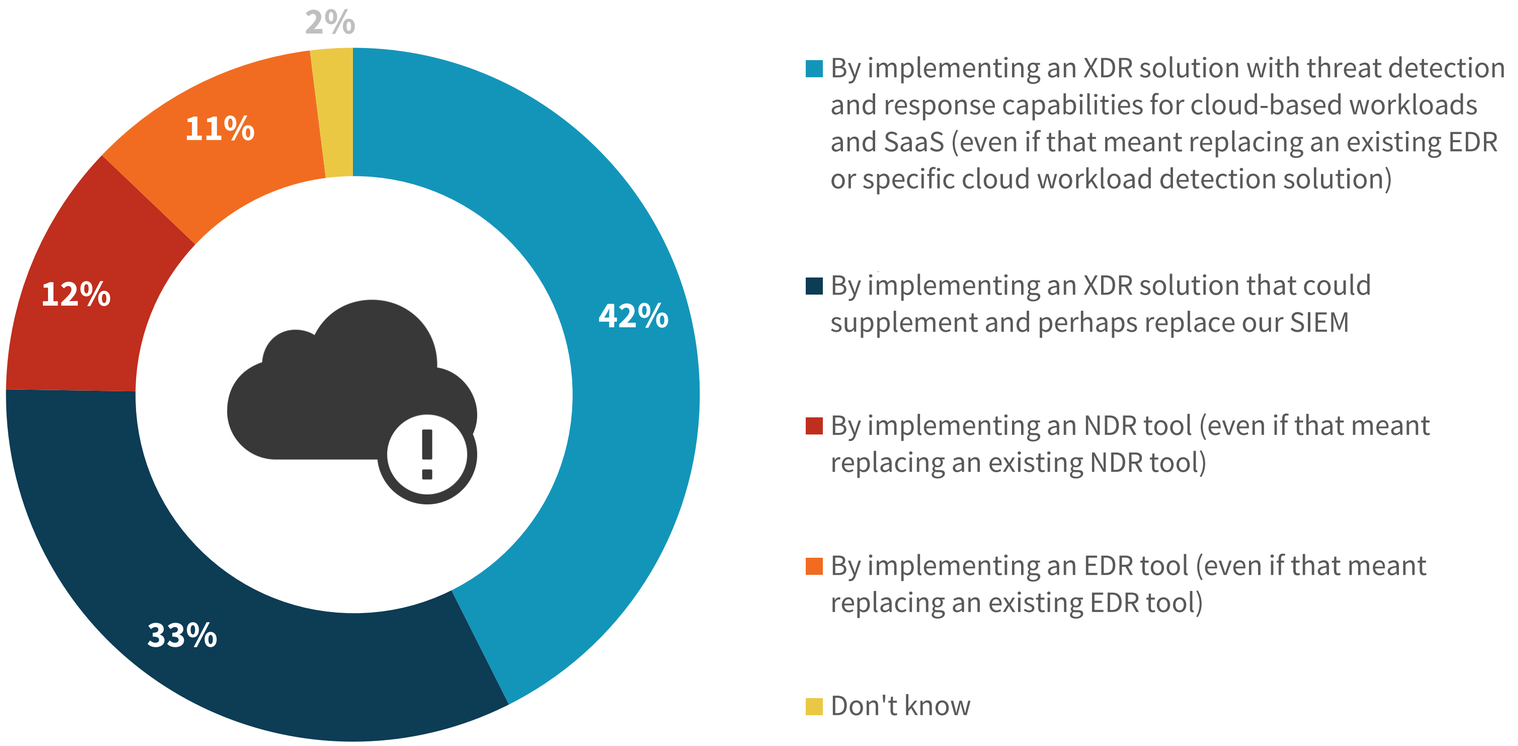
XDR Could Start with Cloud Visibility or SIEM Supplementation

When thinking about where to start with XDR initiatives, 43% say that they would focus on implementing an XDR solution in support of adding threat detection and response capabilities for cloud-based workloads and SaaS applications. This indicates that many organizations have cloud security blind spots and may struggle to detect things like adversary exploits, malware downloads, or anomalous behavior associated with cloud-based workloads and SaaS applications.

It is also noteworthy that one-third say they would start an XDR project by supplementing or perhaps replacing SIEM. As previously noted, SIEM is a foundational SOC technology so it's likely most organizations will add XDR to SIEM to improve alert fidelity, help junior analysts triage incidents, or supplement SIEM correlation rules with advanced analytics for threat detection.

> ***43% say that they would focus on implementing*** *an XDR solution in support of adding threat detection and response capabilities for cloud-based workloads and SaaS applications."*

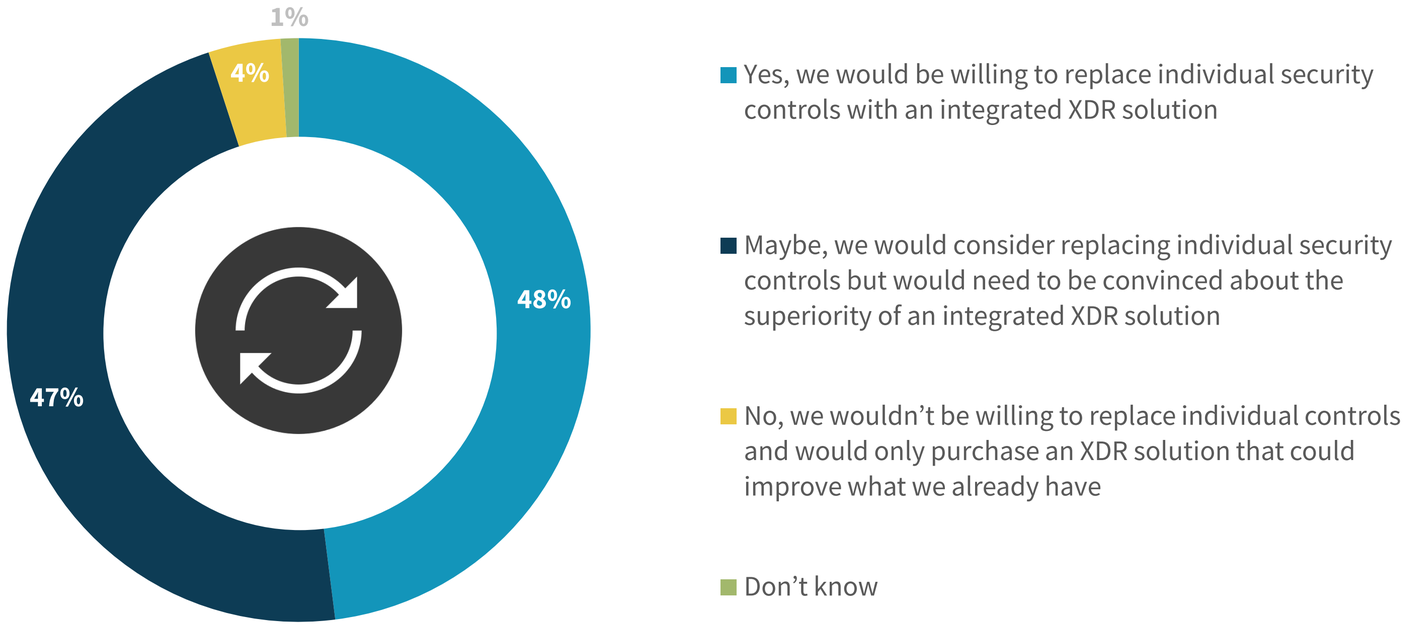
Likeliest starting point for XDR projects.



Back to Contents

> ***Nearly half (48%)*** *would be willing to replace individual controls with integrated XDR solutions.”*

Willingness to replace existing security products for XDR implementation.



XDR Could Replace Existing Technologies Over Time

Once organizations begin XDR projects, they could grow organically and replace existing security bedrock technologies like EDR, NDR, SIEM, and SOAR over time. In fact, nearly half (48%) would be willing to replace individual controls with integrated XDR solutions while another 47% would consider replacing individual controls but would need to be convinced about the superiority of an integrated XDR solution.

While this data strongly suggests that organizations want tightly integrated SOC solutions, tools replacement won’t be easy. CISOs must assess their existing security portfolios, identify technology and processes weaknesses, and then create XDR projects that start by addressing their biggest challenges. Tools replacement must be guided by detailed planning, SOC best practices, and XDR reference architectures.

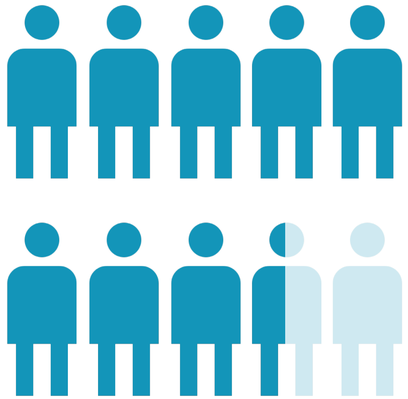
The XDR movement could be attractive for most organizations.

XDR Adoption Is Moving Fast!

With more than 80% of organizations planning increased investments in threat detection and response technologies, it's clear that security teams are experiencing acute pain. The research indicates that XDR could be part of these plans, as 23% are already working on an XDR project, while 70% could establish a formal XDR budget within the next 6 -12 months. Aside from a dedicated budget, XDR funding could come from elsewhere, like the SOC technology budget, the EDR budget, or even the SIEM budget.

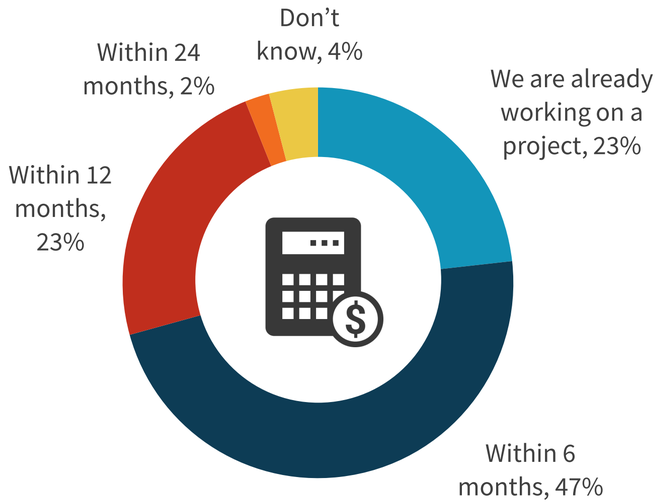
With more than a third willing to dedicate net-new XDR funding, solution providers that can clearly articulate an XDR vision and strategy should prosper in 2021.

Increased budget planned for TDR over next 12-18 months.

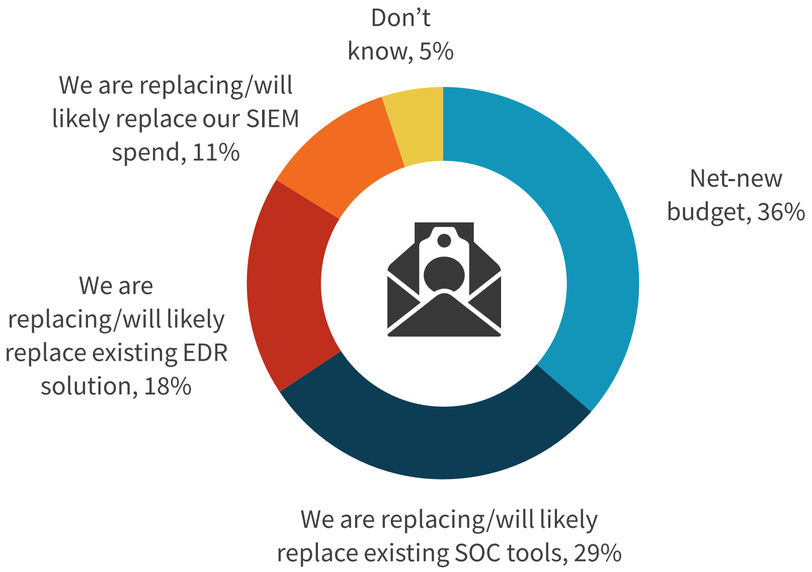


83%
will increase TDR spending.

Plans for formal XDR budget.



Source of XDR funding.



Back to Contents

cybereason®

Cybereason is the champion for today's cyber defenders, with future-ready protection that ends attacks on the endpoint, across the enterprise, and everywhere the battle is waged. Cybereason provides future-ready attack protection to unify security from the endpoint, to the enterprise, to everywhere. The Cybereason Defense Platform combines the industry's top-rated detection and response (EDR and XDR), next-gen anti-virus (NGAV), and proactive threat hunting to deliver context-rich analysis of every element of a malicious operation (Malop™). The result is an operation-centric approach that eliminates alert fatigue and ends cyber attacks from endpoints to everywhere.

LEARN MORE

About ESG

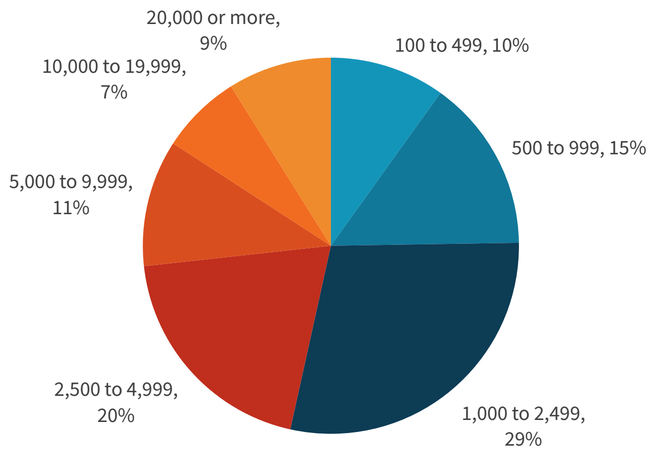
Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

Research Methodology

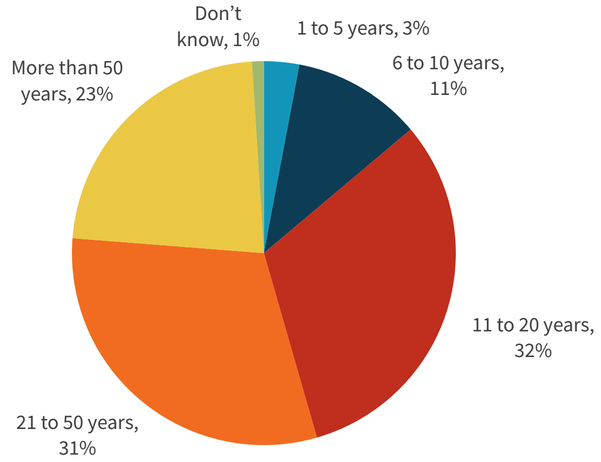
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between October 6, 2020 and October 13, 2020. To qualify for this survey, respondents were required to be IT and cybersecurity professionals personally responsible for evaluating, purchasing, and managing detection and response strategies, processes, and technologies. 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 388 IT and cybersecurity professionals.

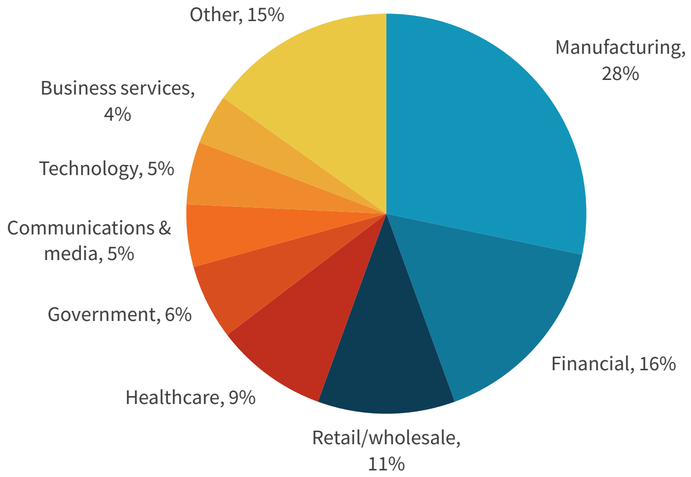
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



Back to Contents