Enterprise Strategy Group | Getting to the bigger truth.™

SOC Modernization and the Role of XDR

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

JUNE 2022

Research Objectives

Security operations demand massive scale to collect, process, analyze, and act upon massive amounts of data. Early XDR was anchored to two primary data sources: endpoints and networks. While this was an improvement on disconnected EDR and NDR tools, threat detection and response across enterprise organizations demands a wider aperture, including cloud workloads, threat intelligence feeds, SaaS applications, and identity and access management visibility. At the same time, in order to modernize security operations centers and keep up with the volume of security alerts, large organizations need advanced analytics to help automate tier-1 analyst tasks like triaging alerts, correlating alerts with IoCs, and preparing incidents for investigations.

In order to gain insights into these trends, ESG surveyed 376 IT and cybersecurity professionals at organizations in North America (US and Canada) personally responsible for evaluating, purchasing, and utilizing threat detection and response security products and services.

THIS STUDY SOUGHT TO:

Examine the people, processes, and technology supporting the modernization of security operations.

Determine the current perception and role of XDR as a component of security operations modernization efforts.

Identify key value points, metrics required to back up those value points, and what's expected from both products and managed services for XDR and SOC modernization.

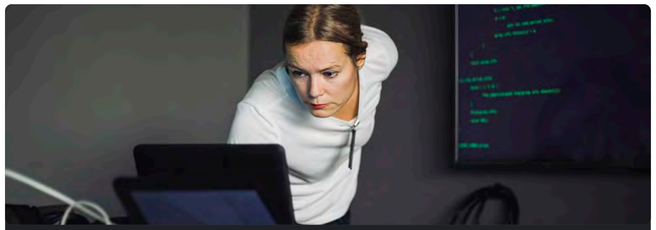
Explore strategies used to automate triage, speed investigations, and help organizations find unknown threats.

KEY FINDINGS

CLICK TO FOLLOW

Security operations remain challenging.

Increasing difficulty is due to the growing attack surface, dangerous threat landscape, and increasing use of cloud computing.



Security professionals want more data and better detection rules.

Despite the massive amount of security data in use, more is desired, as are better detection rules.

SecOps process automation investments are proving valuable.

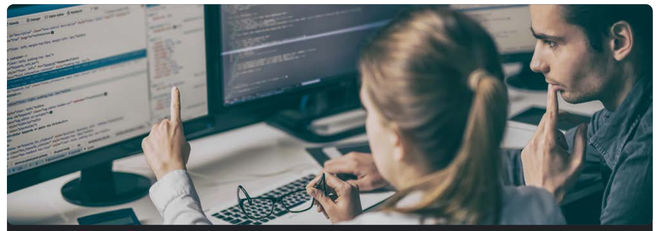
While implementation strategies vary, automation investments are paying off for most.

MITRE ATT&CK framework is proving valuable for most.

However, many are still figuring out how and where to apply it to gain value.

XDR momentum continues to build.

While there is confusion about what XDR is, investment in support of advanced threat detection is significant.



MDR is mainstream and expanding.

While use cases vary, MDR services are widely adopted across organizations of all sizes and maturity.

Back to Contents

Security Operations Remain Challenging

Security operations have become more difficult at most organizations over the past few years. Specifically, more than half (52%) of respondents believe their organization's security operations environment has become more difficult to manage over the last two years. This is due to factors such as the increasingly dangerous threat landscape, a growing attack surface, the volume and complexity of security alerts, and public cloud proliferation. Since these challenges will only accelerate in the future, many CISOs realize that current SOC strategies are inadequate. To cope with the increasing threat volume and IT scale/sprawl, organizations have several initiatives focused on SOC modernization.

52%

of organizations believe that security operations are more difficult today than they were two years ago.

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

The threat landscape is growing and changing rapidly,

41%

The attack surface has grown,

40%

The attack surface is continuously changing and evolving,

39%

The volume and complexity of security alerts has increased,

37%

The use of public cloud services has increased,

34%

"Organizations have several initiatives **focused on SOC modernization.**"

Back to Contents

Security Operations Are Impacted by the Global Skills Shortage

In addition to general security operations challenges, it's worth noting that 81% of organizations agree that security operations have been impacted by the global cybersecurity skills shortage. Typically, this leads to increasing workload on existing staff as well as staff attrition and burnout. Security professionals point to several areas where staff and skills are especially lacking, including security architects, security engineers, tier-3 analysts, and vulnerability assessment/prioritization analysts.

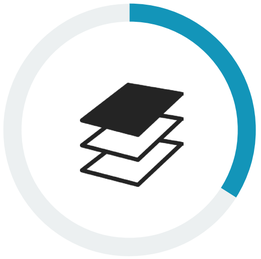
81%

of organizations agree that their security operations **have been impacted by the cybersecurity skills shortage.**

Most understaffed areas of security operations.

Security architect,
37%

Security engineers,
35%



Tier-3 analysts,*
34%

Vulnerability assessment/ prioritization analysts,
33%

** i.e., similar to tier-2 analysts but more experienced and focused on difficult/critical issues.*

Back to Contents

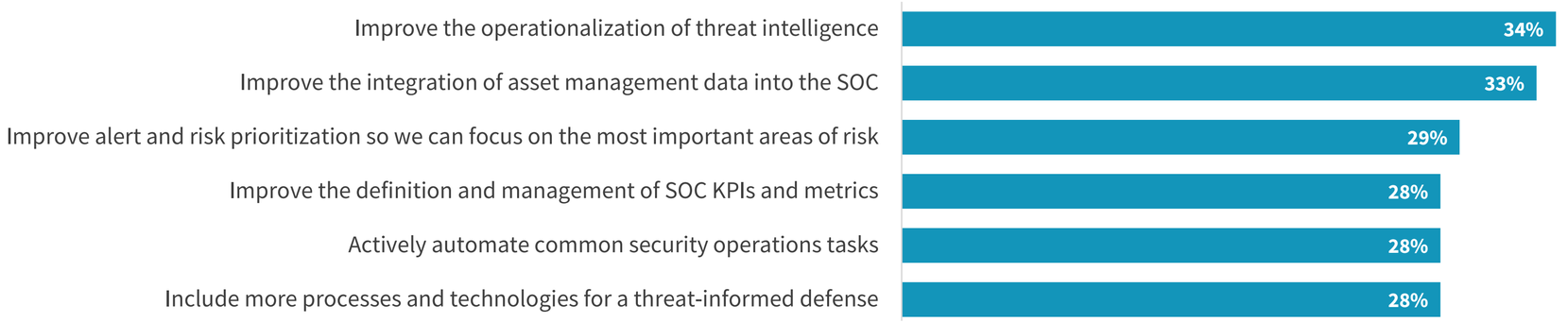
Near-term SOC Modernization Priorities

How do organizations plan to deal with increasingly difficult security operations environments, including insufficient staffing levels? SOC modernization is a key program initiative, with 88% of organizations increasing security operations spending this year. In the near term, SOC teams plan to focus their efforts on areas like improving the operationalization of threat intelligence, improving the integration of asset management data into the SOC, improving risk and alert prioritization, improving the definition and management of SOC KPIs, and automating common security operations tasks.

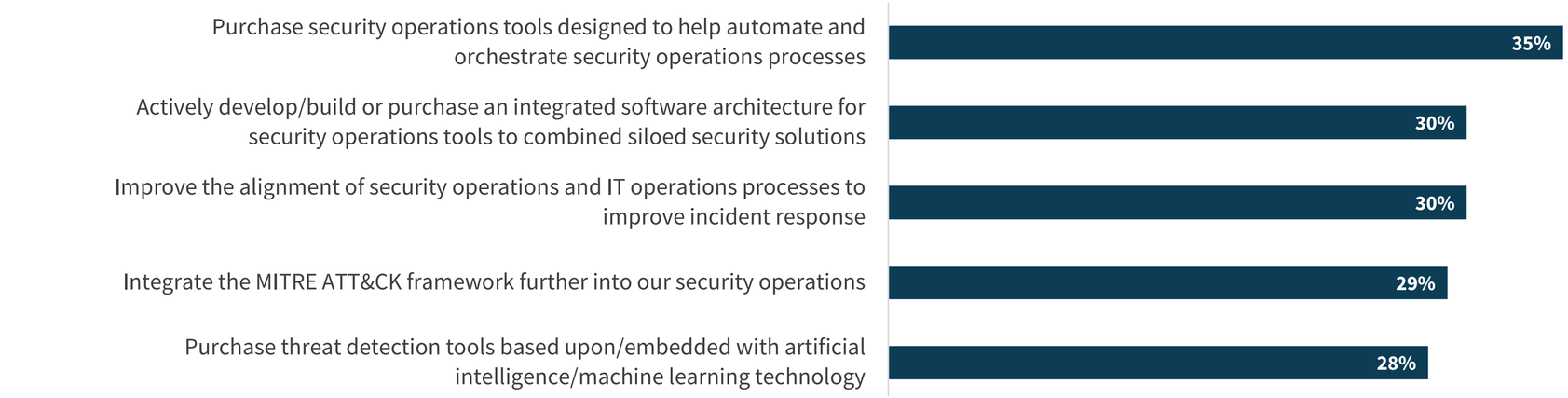
Moving forward, organizations will take many further steps toward SOC modernization such as purchasing security process automation tools, developing/building an integrated security operations and analytics platform architecture (SOAPA), improving the alignment of security and IT operations, further integrating the MITRE ATT&CK framework into security operations, and purchasing advanced analytics tools for threat detection.

These advancements will take time and may require security services support. Nevertheless, they should be seen as stops along a journey toward SOC modernization. The goal is creating a SOC that can offer the scale, performance, intelligence, automation, and manageability to prevent, detect, and respond to threats, manage risk, and support the organization's mission.

Expected SOC-focused objectives over the next 12 months.



Expected actions to improve security operations over the next 12-18 months.



Back to Contents

Security Professionals Want More Data and Better Detection Rules

Despite the Move to XDR, Endpoint Data Is Still Most Valued

Eight in ten organizations collect, process, and analyze security operations data from more than ten data sources. Security professionals believe that the most important sources are endpoint security data, threat intelligence feeds, security device logs, cloud posture management data, and network flow logs. While this seems like a lot of data, survey respondents actually want to use more data for security operations, driving the need for scalable, high-performance, cloud-based back-end data repositories.

80%

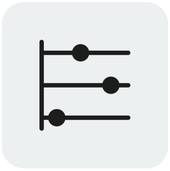
of organizations use more than 10 data sources as part of security operations.

> “Respondents actually want to use **more data for security operations.**”

Most important data sources for security operations.

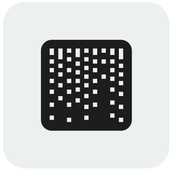
24%
Endpoint security data

21%
Threat intelligence feeds



20%
Log data from security devices

20%
Cloud security posture management systems



18%
NetFlow and/or IPFIX data, and/or VPC flow logs

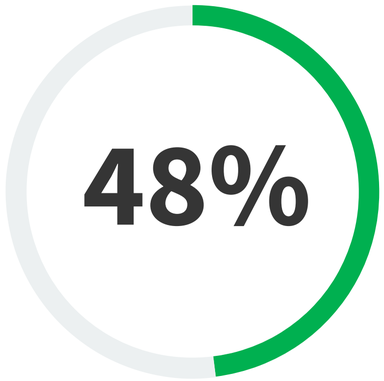
Back to Contents

Most Organizations Develop Their Own Custom Detection Rules

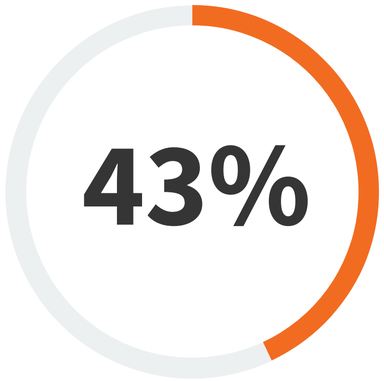
While vendors provide growing volumes of out-of-the-box content for threat detection, 91% of organizations supplement these efforts with their own detection engineering. In fact, SOC teams collect, process, and analyze a variety of security telemetry to help them determine detection weaknesses where custom rules are needed. Security teams customize vendor rule sets to meet their needs and develop custom rules to detect threats targeting their industry or organization. To support this trend, vendors must facilitate user network cooperation while embracing open standards such as Sigma and YARA with established industry support.

Extent of custom threat detection rules.

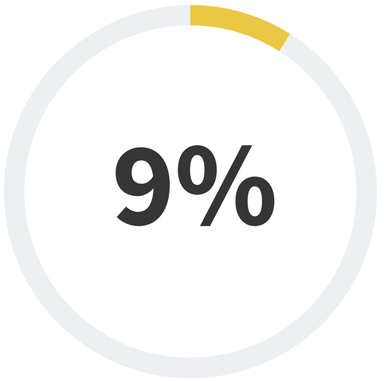
My organization develops a significant number of custom rules to supplement the detection rules provided by vendors



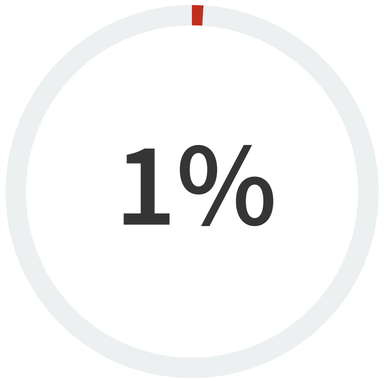
My organization develops some custom rules to supplement the detection rules provided by vendors



My organization may develop a small number of custom detection rules but mainly relies on those provided by vendors



My organization does not develop any custom detection rules and completely relies on those provided by vendors



Back to Contents

SecOps Process Automation Investments Are Proving Valuable

Many Organizations Have Realized Benefits from Security Process Automation, but Challenges Persist

Security process automation is popular, as evidenced by the 90% of organizations currently automating security operations processes, with 46% describing their automation efforts as extensive. Those engaged in security process automation report benefits like improved threat detection using playbooks, MTTR, and incident prioritization, as well as an ability to more quickly isolate infected assets. Given security operations challenges like the growing attack surface, alert storms, and the dangerous threat landscape, security process automation will continue and likely merge with IT process automation to deliver efficiencies across IT and security.

While security process automation remains popular and beneficial, it does come with some challenges. Nearly two in five (39%) organizations claim that their security operations team doesn't have the right programming skills to develop runbooks/workflows in SOAR tools, while 21% claim that their security operations processes are immature and in need of reengineering before they can be automated. In these cases, organizations need more to assess process workflows, looking for bottlenecks before moving on to automation. Those with limited programming skills should investigate low code/no code SOAR options or use the process automation functionality built into other operations tools.

Most commonly realized benefits from security operations process automation.

Improved threat detection using playbooks

51%

Improved mean time to respond

49%

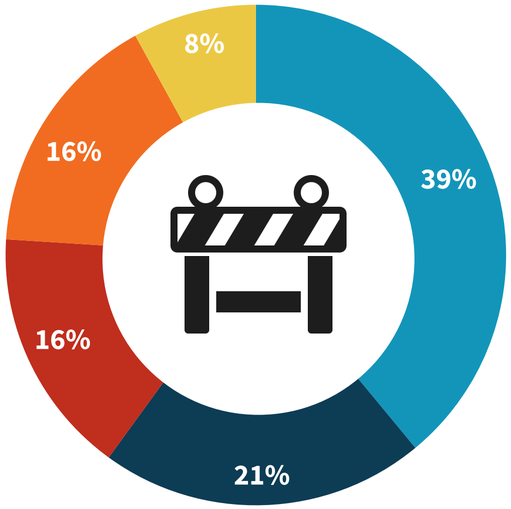
Improved incident prioritization

44%

More quickly isolated infected assets

44%

Biggest impediments to security operations process automation.



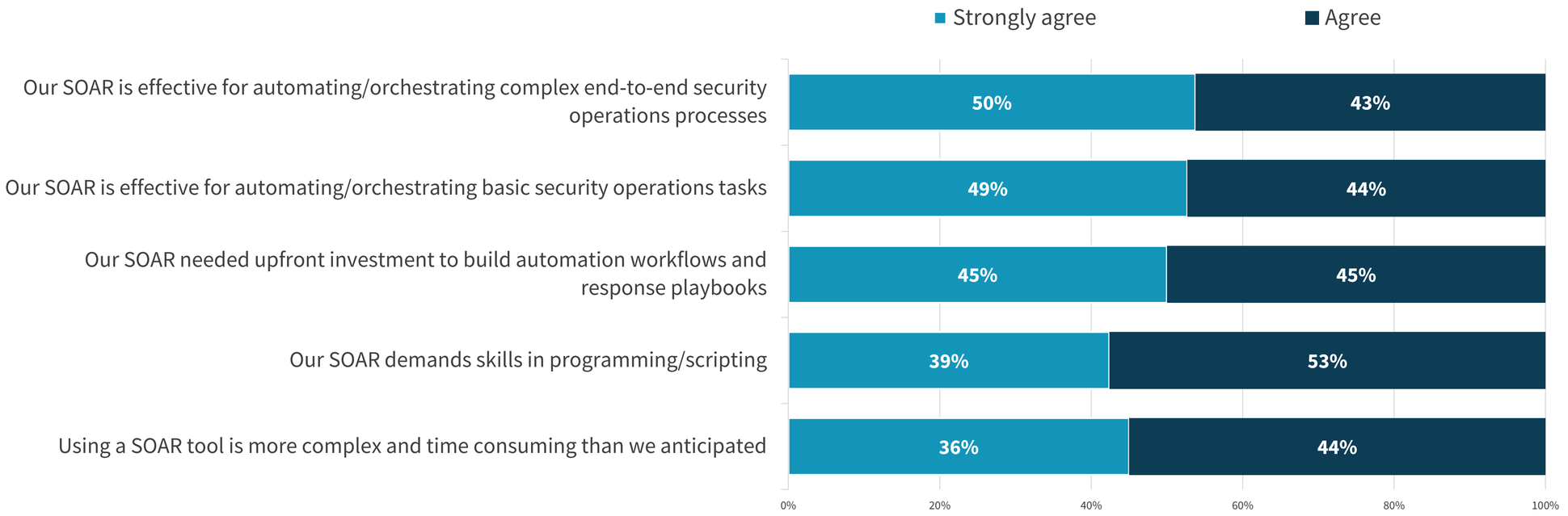
- Software development skills: Our security operations team doesn't have the programming skills to develop runbooks/workflows
- Process immaturity: Our security operations processes are relatively immature, so we would really have to reengineer them before proceeding to process automation
- Time: The security team doesn't have ample time to work on process automation
- Tools: Our organization doesn't have technologies, like SOAR, needed for security process automation
- No impediments

Back to Contents

SOAR Tools Can Produce Results with the Right Upfront Investments and Expectations

More than a quarter (29%) of organizations use some type of security orchestration, automation, and response (SOAR) tool for process automation. Use of SOAR can be beneficial: 93% of security professionals agree that their SOAR is effective for automating complex end-to-end security operations processes and for automating/orchestrating basic security operations tasks. SOAR doesn't come for free, however. Success depends upon some upfront planning, investments, and the right skills. For example, 90% of security professionals claim that SOAR needed upfront investment to build automation workflows and response playbooks, 92% agree that SOAR demands programming/scripting skills, and 80% agree that using a SOAR tool is more complex and time consuming than anticipated. Based on this data, organizations should recognize that SOAR should be viewed as a project, not a panacea. SOAR benefits can only be achieved with the right level of planning, training, and project management.

Sentiment for security orchestration, automation, and response (SOAR) tools.



"Use of SOAR can be beneficial."

Back to Contents

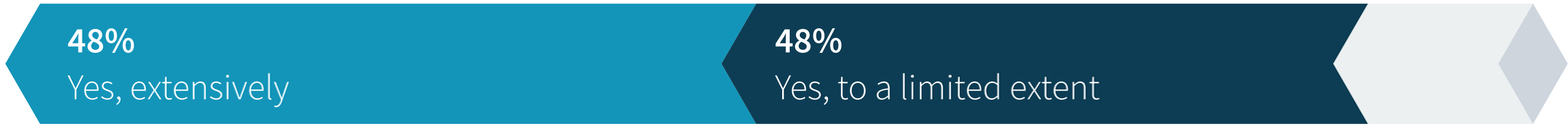
MITRE ATT&CK Framework Is Proving Valuable for Most

Most Organizations Use and See Value in the MITRE ATT&CK Framework for Security Operations

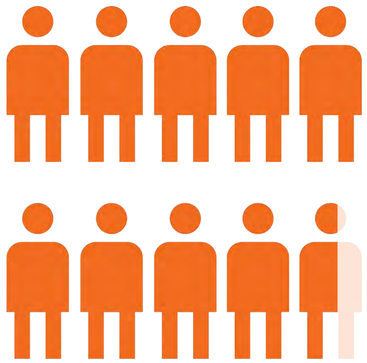
The MITRE ATT&CK framework has grown in popularity to the point that nearly nine in ten organizations use it to some extent today. As SOC managers look into the future, they see even greater MITRE utilization. In fact, 97% of security professionals believe that MITRE ATT&CK (and derivative projects) will be critical, very important, or important to their organization's security operations strategy.

Usage of MITRE ATT&CK framework for security operations.

Do organizations use the MITRE ATT&CK framework for security operations?



Importance of MITRE ATT&CK framework to security operations.



97%

of security professionals believe that MITRE ATT&CK (and derivative projects) will be critical, very important, or important to their organization's security operations strategy.

Back to Contents

MITRE ATT&CK Use Cases Flourish

MITRE ATT&CK has also become instrumental in a variety of security operations processes. Of those organizations embracing the MITRE ATT&CK framework, 38% use it to help them apply threat intelligence into their alert triage or investigations process, 37% use it as a guideline for security engineering, 35% use MITRE to better understand the tactics, techniques, and procedures of cyber-adversaries, and 34% use the framework to help them understand the full extent of attacks more quickly.

In these ways, organizations are operationalizing MITRE ATT&CK across threat prevention, detection, and response.

Ways in which organizations are utilizing MITRE ATT&CK framework.

To help us better apply threat intelligence to our alert triage and/or investigations processes,

38%

As a guideline for security engineering,

37%

To better understand the tactics, techniques, and procedures of cyber-adversaries,

35%

To help organizations more quickly understand the full extent of attacks,

34%

To make sure we are collecting the right data from the right data sources,

33%

> “MITRE ATT&CK has also become **instrumental in a variety of security operations processes.**”

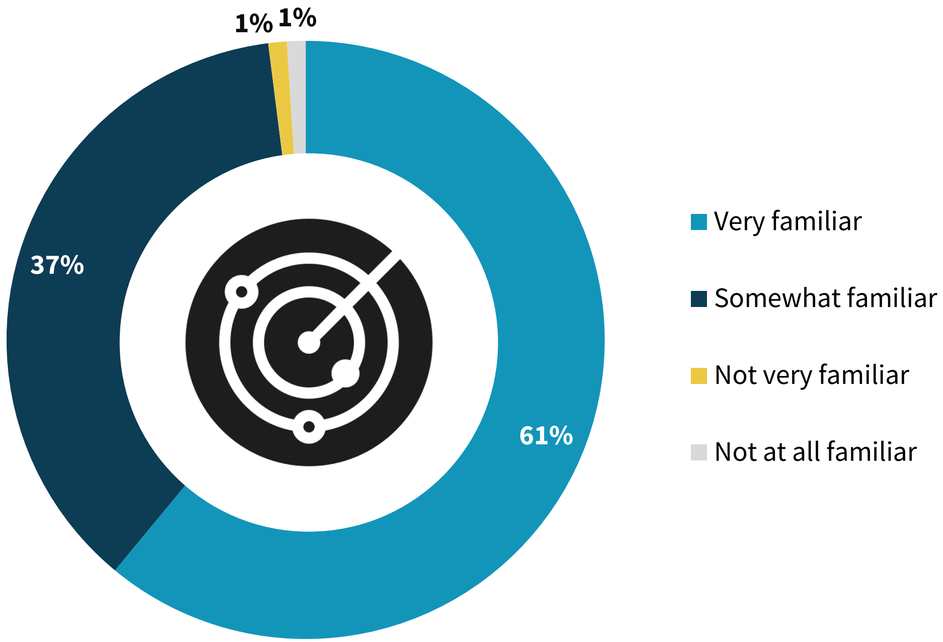
Back to Contents

XDR Momentum Continues to Build

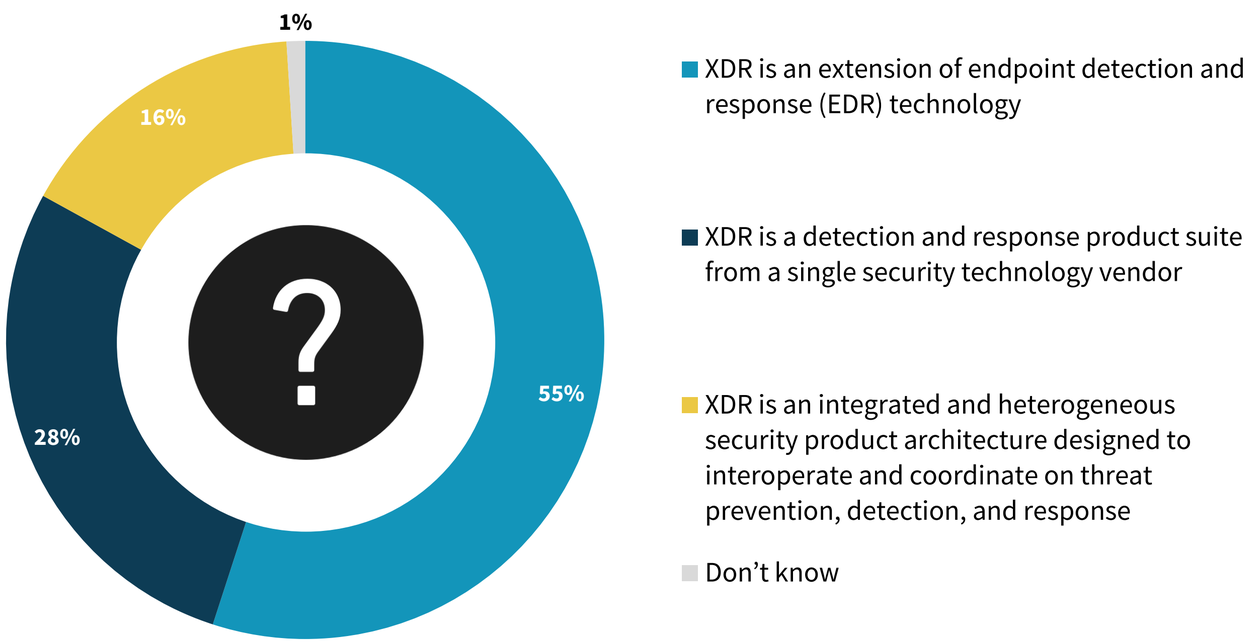
XDR Awareness Continues to Grow, though Most See XDR Supplementing or Consolidating SOC Technologies

While XDR has gained more industry attention, it remains an amorphous concept with different components and definitions. This is reflected by the fact that 61% of security professionals claim that they are very familiar with XDR technology. While this is an improvement from ESG's 2020 research (when only 24% of security professionals were very familiar with XDR), 39% are still only somewhat familiar, not very familiar, or not at all familiar with XDR. Users are also confused about what XDR is. While 55% of respondents say that XDR is an extension of EDR, 44% believe XDR is a detection and response product from a single security technology vendor or an integrated and heterogeneous security product architecture designed to interoperate and coordinate on threat prevention, detection, and response. It's safe to say that XDR remains a bit of a work in progress.

Familiarity with XDR technology.



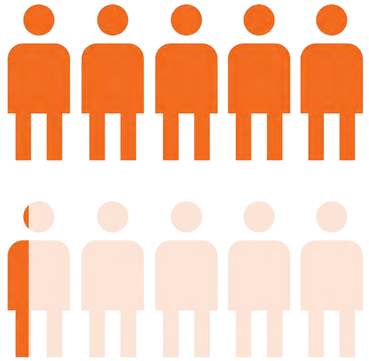
Organizational definitions of XDR technology.



Back to Contents

Most See XDR Supplementing or Consolidating SOC Technologies

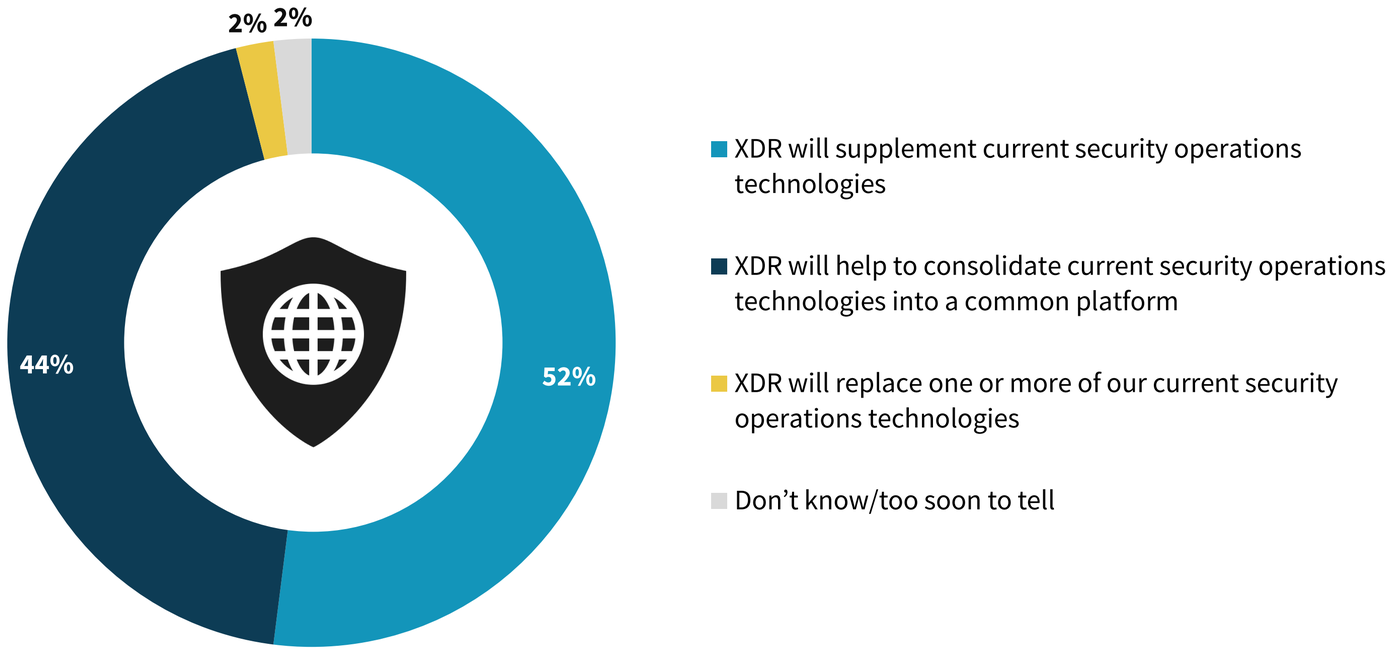
Along those lines, at this point, XDR is not seen as a potential replacement for SOC technologies like SIEM, SOAR, and TIP. Rather, more than half (52%) of security professionals believe XDR will supplement existing security operations technologies, while 44% see XDR as consolidating current security operations technologies into a common platform. Only 2% believe that XDR will replace any current security operations technologies.



MORE THAN HALF

of security professionals believe **XDR will supplement existing security operations technologies.**

Expected impact of XDR on security operations environments.



Back to Contents

Users Want XDR to Address Common Threat Detection and Response Challenges

Regardless of how XDR is defined, security professionals are interested in using XDR to help them address several threat detection and response challenges. XDR seems like an attractive option since current tools struggle to detect and investigate advanced threats, require specialized skills, and aren't effective at correlating alerts. In summary, CISOs want XDR tools that can improve security efficacy, especially regarding advanced threat detection. Additionally, they want XDR to streamline security operations and bolster staff productivity.

Security professionals seem to have a number of common XDR use cases in mind. For example, 26% of security professionals want XDR to help prioritize alerts based on risk, 26% seek improved detection of advanced threats, 25% want more efficient threat/forensic investigations, 25% desire a layered addition to existing threat detection tools, and 25% think XDR could improve threat detection to reinforce security controls and prevent future similar attacks. Clearly, users want XDR to fill gaps within the security stack while improving the efficacy and efficiency of threat detection and response.

Five most common challenges driving XDR interest.

51%

Current tools struggle to detect and investigate advance threats

38%

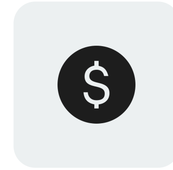
Current tools require too many specialized skills

36%

Current tools aren't effective at correlating alerts

35%

Specific gaps in cloud detection and response capabilities



32%

Current tools approach is too costly

Five highest priority XDR use cases.

26%

An XDR solution that could help prioritize alerts based on risk

26%

Improved detection of advanced threats

25%

More efficient threat/forensic investigations

25%

Layered addition to existing threat detection tools, aimed at identifying advanced or more complex threats

25%

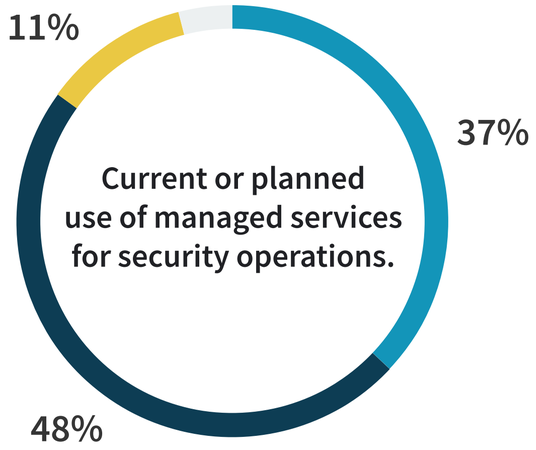
Using improved threat detection to reinforce security controls and prevent future similar attacks

Back to Contents

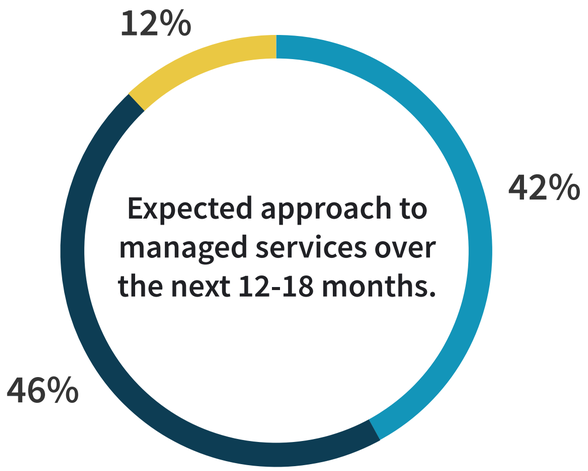
MDR Is Mainstream and Expanding

The Use of MDR Is Mainstream… and Increasing

Regardless of technology definitions or implementation strategies, ESG's data demonstrates one nearly universal truth: Organizations need help from service providers for security operations. Eighty-five percent of organizations use managed services for a portion or a majority of their security operations today. And of those utilizing managed security services, 88% will increase the use of managed services for security operations moving forward.



- We use managed services for a majority of our security operations
- We use managed services for a portion of our security operations
- We use managed services for security operations in a limited capacity



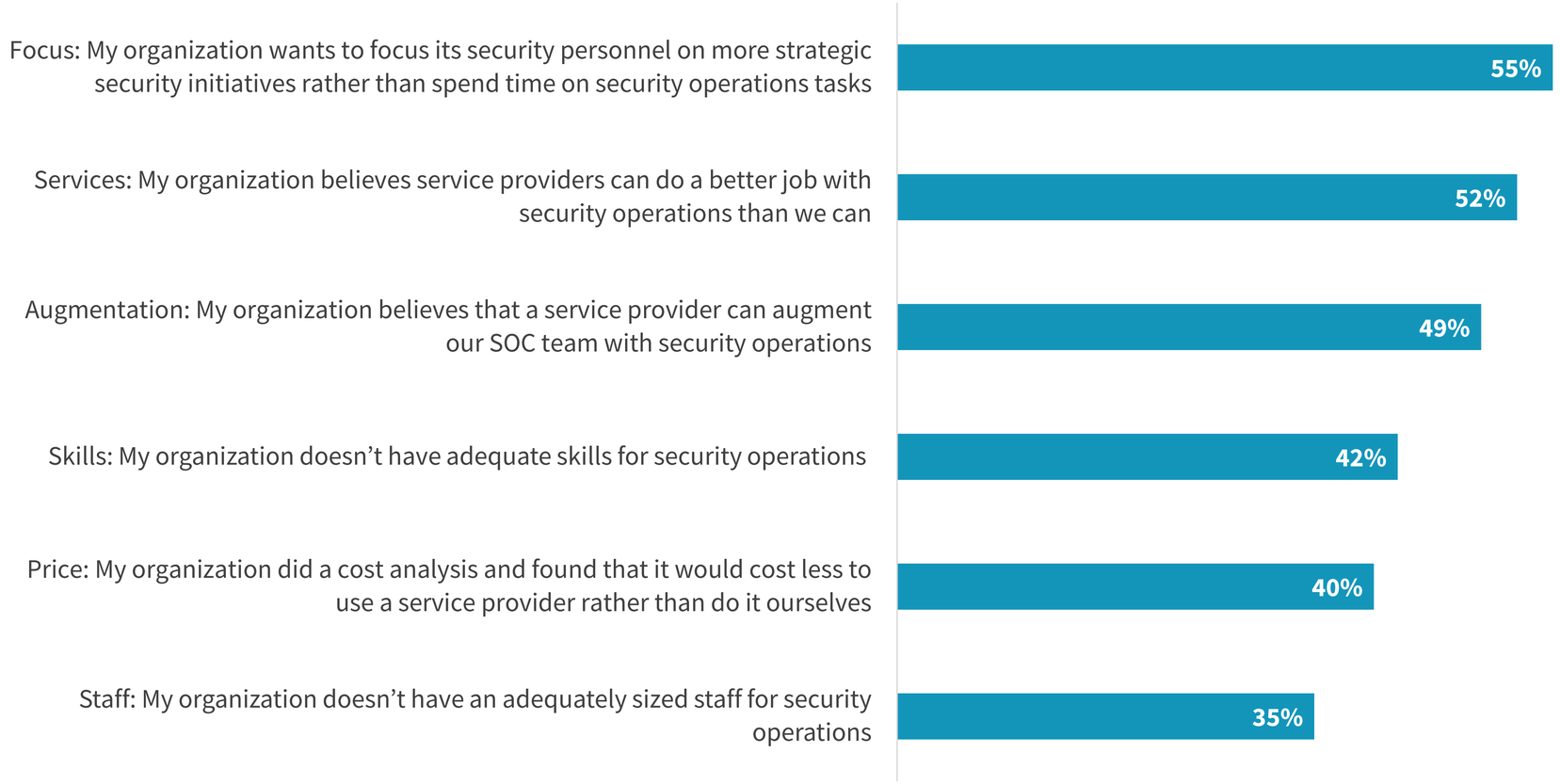
- We will increase our use of managed services for security operations significantly
- We will increase our use of managed services for security operations slightly
- We will maintain our current use of managed services for security operations

Back to Contents

MDR Helps Organizations Focus Security Efforts and Address Skills And Staff Shortages

Why do organizations need managed services for security operations? More than half (55%) want security services so they can focus security personnel on strategic security initiatives. Others believe managed service providers can accomplish things that their organization simply cannot, with 52% believing service providers can provide better security operations than their organization can, 49% saying a managed service provider can augment their SOC team, and 42% admitting that their organization doesn't have adequate skills for security operations.

Primary reasons behind usage of or plans for managed services for security operations.



Back to Contents

ABOUT ESG

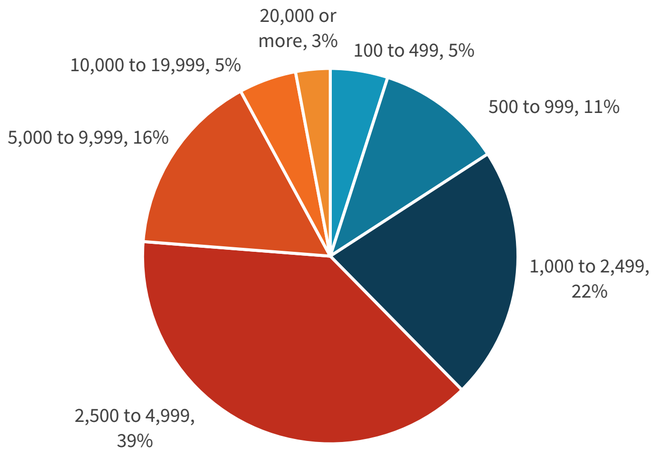
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology

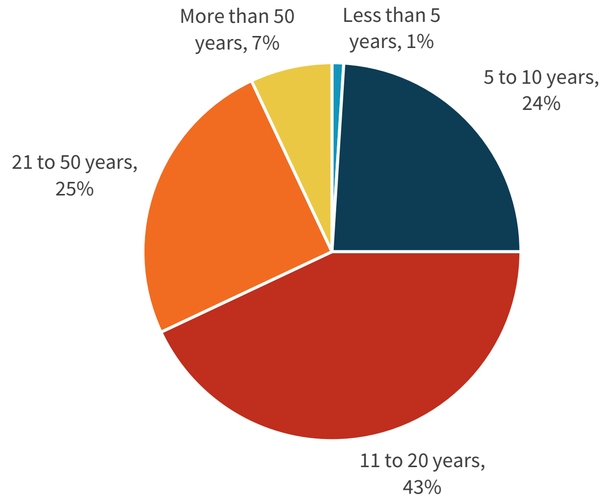
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between April 4, 2022 and April 15, 2022. To qualify for this survey, respondents were required to be IT or cybersecurity professionals responsible for evaluating, purchasing, and utilizing threat detection and response security products and services. 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 376 IT and cybersecurity professionals.

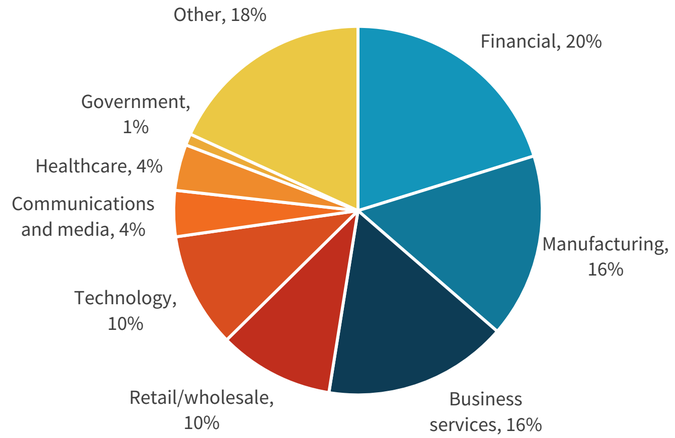
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



Back to Contents

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.