deepwatch

June 2022

RESEARCH REPORT

The State of the Modern SOC

Stronger Detection and Automation Pave the Way for Real-Time Response

Table of Contents

State of the Modern SOC

Introduction: State of the Modern SOC

Stronger Detection and Automation Pave the Way for Real-Time Response

INTRODUCTION

State of the Modern SOC

Stronger Detection and Automation Pave the Way for Real-Time Response

Executive Summary

Organizations both large and small face a cyber threat landscape that is complex and growing. Throughout the first half of 2022, sophisticated adversaries, an expanding attack surface, unavailability of skilled talent and even geopolitical turmoil have required organizations to stay particularly vigilant. While firewalls and defend-the-castle approaches remain part of defense-in-depth strategies, even mid-sized organizations now realize the need for 24/7/365 monitoring and response. Security operations centers (SOCs) used to exist only in larger enterprises, resourced with sophisticated in-house security teams. Today's attacks require even smaller organizations to stand up SOC capabilities in order to continue conducting business effectively.

Businesses of all sizes must be prepared to respond to disruptive cyber incidents at any time. But how equipped are they to detect such threats, and are they able to respond fast enough to stop these threats from doing actual damage? Deepwatch commissioned this report to examine these exact issues.

In this research, security professionals were asked about the hurdles they face in taking swift and effective response actions against cyber threats, and what effect that has on their businesses.

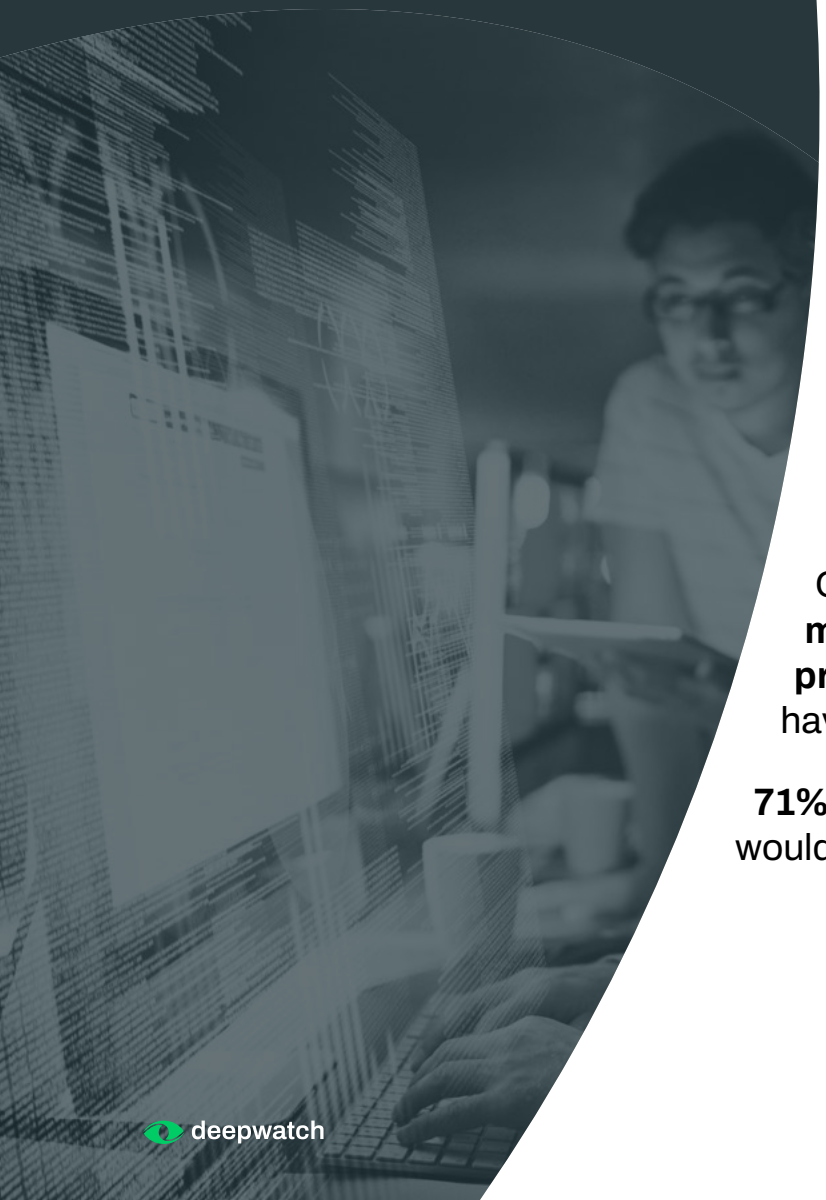
The resulting survey of over 300 security professionals brought to light how security teams are often outpaced by threat activity across an expanding attack surface. Most notably, the research found that 85% of security professionals attributed costly and preventable business impacts to insufficient response practices. Almost all security teams (93%) said they are working to reduce response times.

The findings section of this report unpacks the barriers to effective response and how security teams today plan to shorten the time to contain threats and address related issues.

KEY FINDINGS

State of the Modern SOC

Stronger Detection and Automation Pave the Way for Real-Time Response



Key Findings

Security professionals highlight **staffing challenges, alert quality, and organizational culture** as primary factors slowing down response.

38% of security teams don't have 24/7 SOC coverage.

Only 12% of security professionals are highly confident that their security alerts are adequate enough to respond quickly.

97% of security professionals state that more accurate alerting would increase confidence in implementing automated response actions.

With the need for better information on the detected threats, it may be no surprise that **66% of security professionals** are investing or planning to invest in XDR solutions.

Of those not planning to invest in XDR, **more than half (51%) of security professionals** say the reason is they don't have the expertise or staff to manage it.

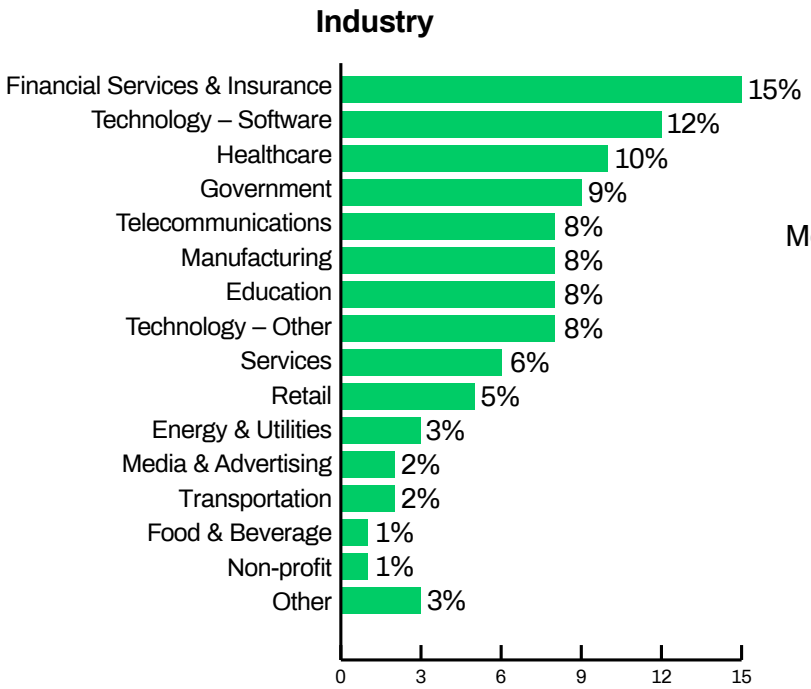
71% of security professionals said they would want XDR as a managed service.

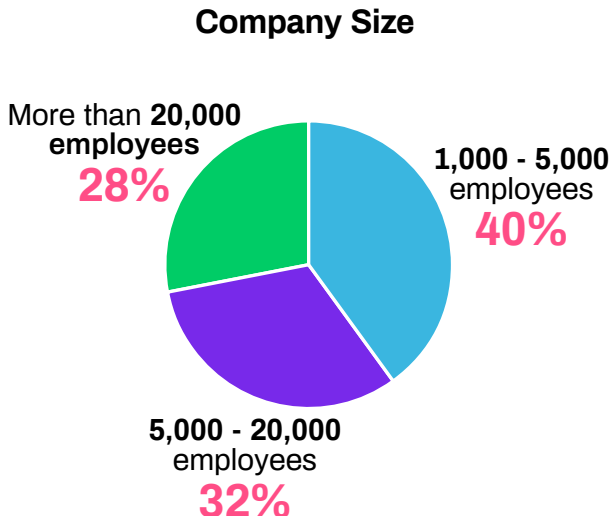
Methodology

On behalf of Deepwatch, Dimensional Research surveyed IT security professionals on a variety of questions and topics related to experiences and attitudes in security response, as well as areas of investments. Responses were captured between April 19 and 25th, 2022. The survey was fielded in English. A total of 304 qualified individuals completed the survey, all directly responsible for IT security at a company in the United States with more than 1,000 employees.

Demographics

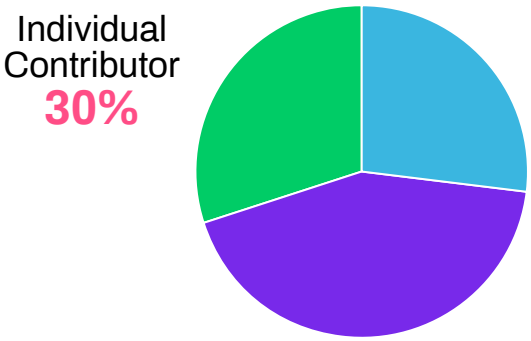
Participant Demographics



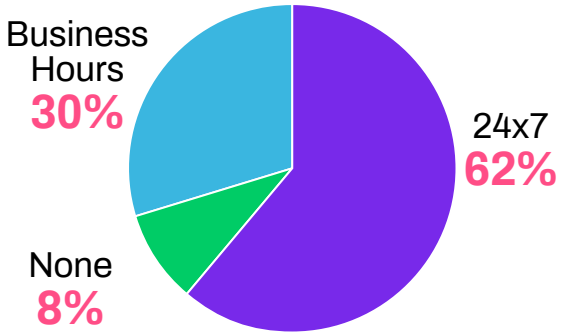


Demographics (cont'd)

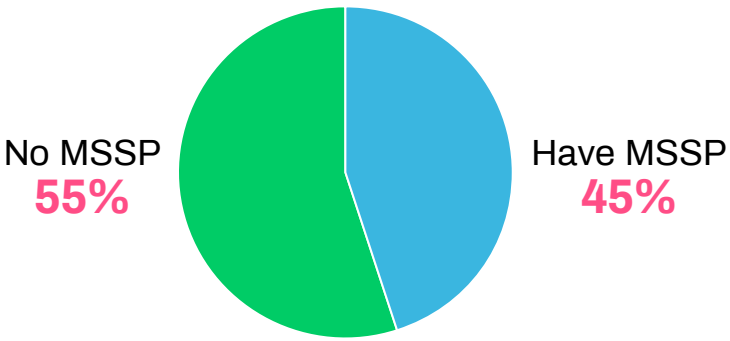
Job Level



Type of SOC



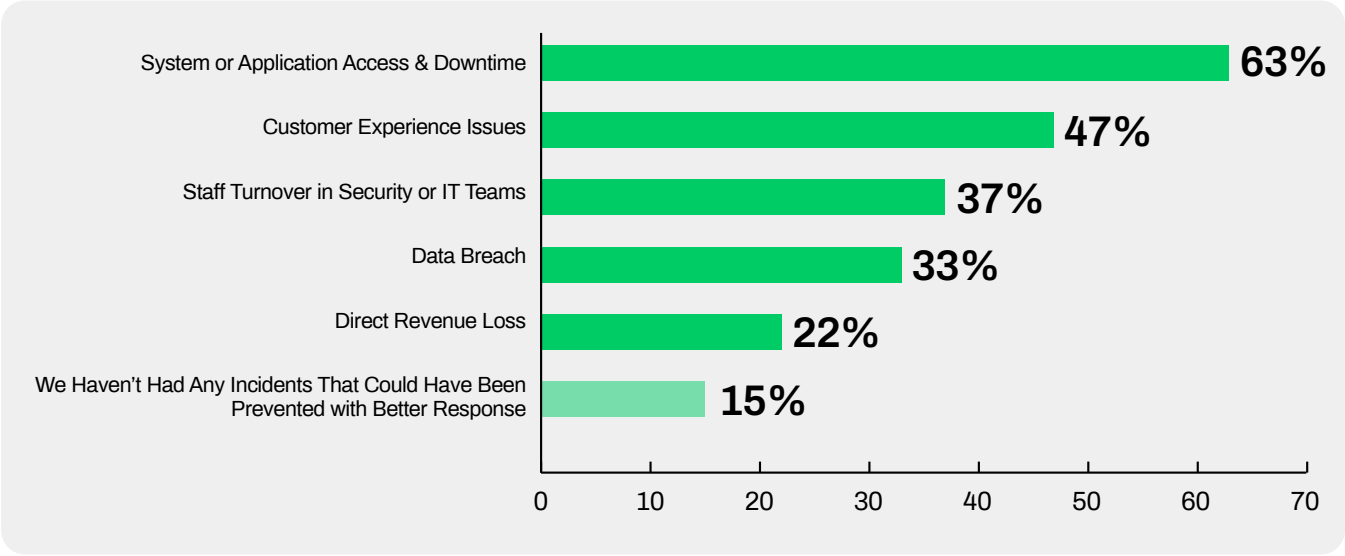
MSSP



Findings

85% of security professionals attribute preventable business impacts to insufficient response practices.

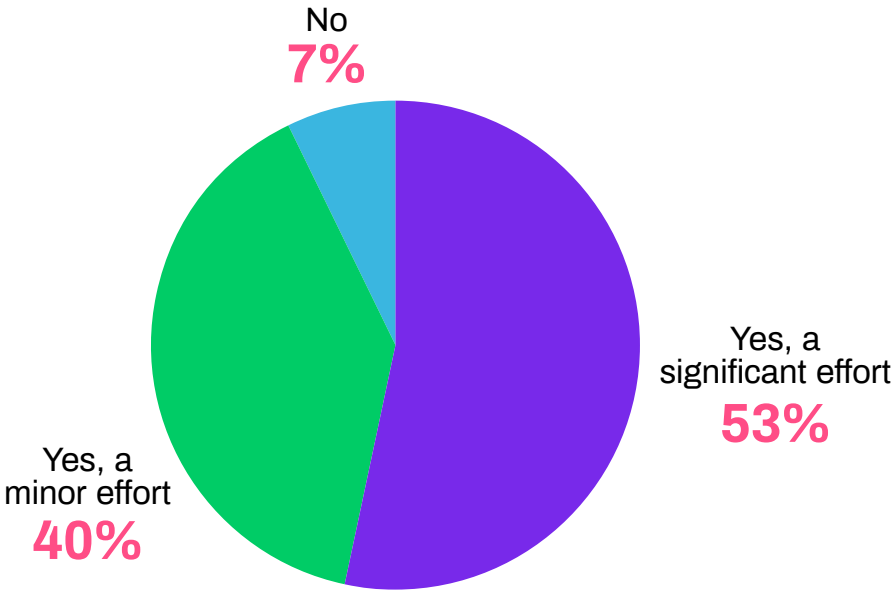
In the past few years, which of the following types of issues occurred at your organization that could have been prevented or minimized with better security response practices? Choose all that apply.



The inability to continue business operations, blocked access to systems or applications and negative impacts to customer experience were the top business impacts experienced by security professionals due to cybersecurity events. These are serious issues that could have long-term consequences on the business, and security professionals believe they could have been avoided with better security response practices.

Almost all (93%) of security professionals are working to reduce response times.

Is your security team making an effort to reduce response times?

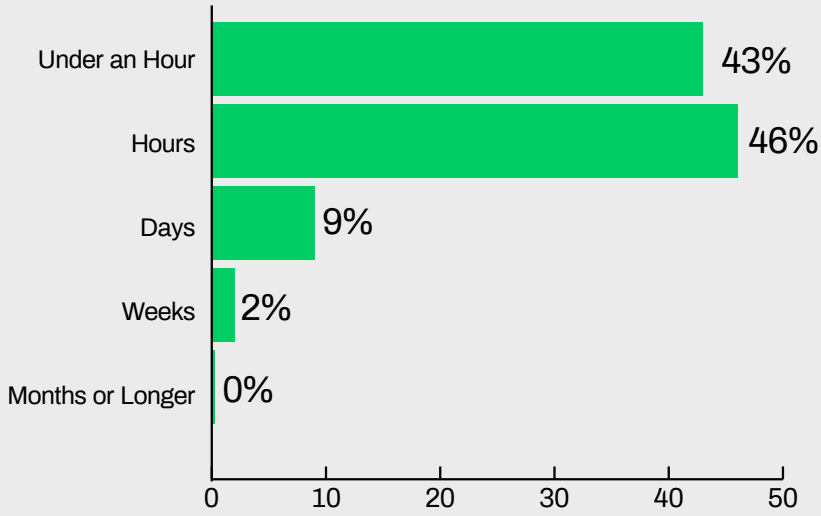


Security professionals say response to critical alerts should occur in less an hour, but less than half (43%) can respond that quickly.

Security teams are continually looking for ways to improve response times. Although response actions may vary, from isolating a host to blocking access for identities, security teams need to better understand the potential threat footprint and develop response actions that span the enterprise.

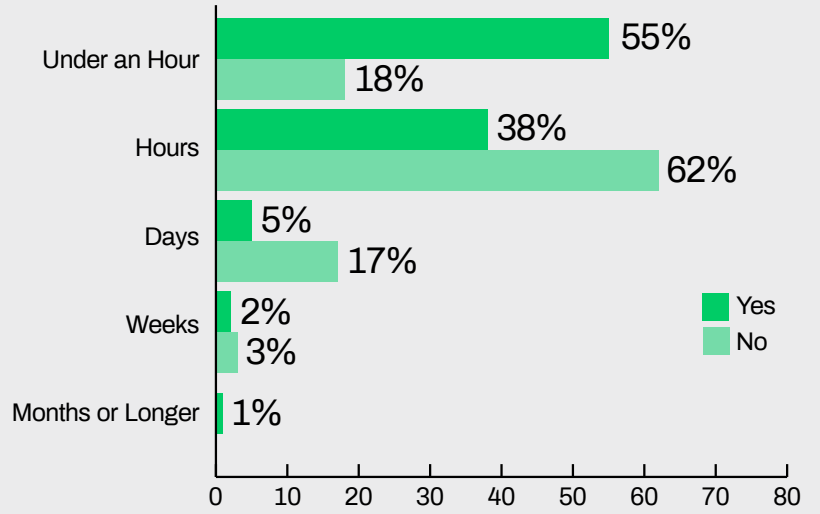
What is your organization's mean time to respond to security incidents with critical severity?

Choose the one answer that most closely applies.



What is your organization's mean time to respond to security incidents with critical severity?

"Is this fast enough?"



For critical severity threats, nearly all organizations are able to respond in hours or less, almost evenly distributed between those who could respond in less than an hour and those who needed multiple hours. However, 62% of those responding within hours acknowledge this is not fast enough. Even 18% of those responding in under an hour believe they aren't responding fast enough. Response times vary based on the nature of the identified threat, but even medium or low severity alerts require swift and precise response in order to minimize the impact on business.

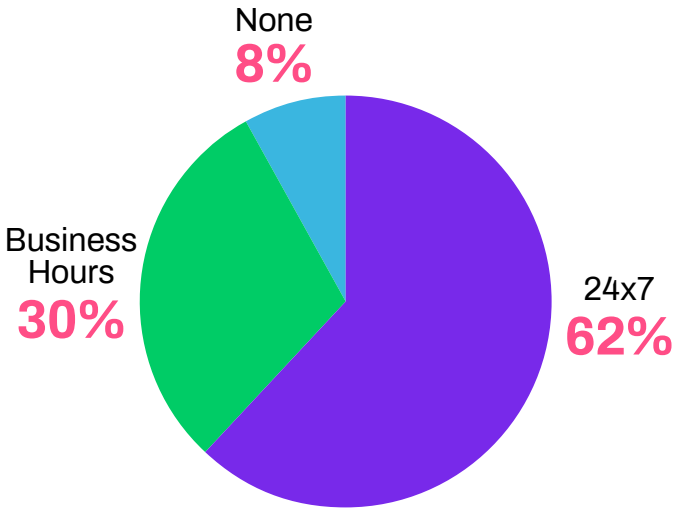
Security professionals highlight staffing challenges, alert quality, and organizational culture as primary factors slowing down response.

Security practitioners point to various factors that impact their response times, including the inability to run 24/7/365 security operations, difficulty in hiring/retaining skilled staff to monitor the environment, lack of actionable alerts, and challenges with organizational/security culture. Security leaders have leveraged tools like SIEM (security information and event management) to improve alert correlation, but this causes SOC analysts to have to deal with thousands of alerts on a monthly basis. Inability to get the full context from the alerts generated impacts the accuracy of response and response times.

38% of security teams don't have 24/7 SOC coverage

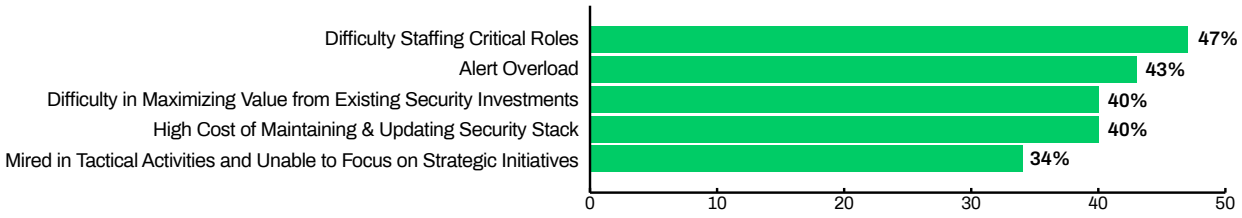
What type of security operations center (SOC) coverage do you have?

Although the majority of organizations have 24/7 monitoring and threat detection for their environments, that still leaves 38% of organizations unable to track threats outside of working hours. Today's threat landscape has evolved, with adversaries spread across the world, underscoring the need for protection around-the-clock.



Known challenges to security operations remain, with security professionals citing staffing issues and alert overload as their top challenges.

What current SOC or security operations challenges are faced by your security teams? Choose all that apply.

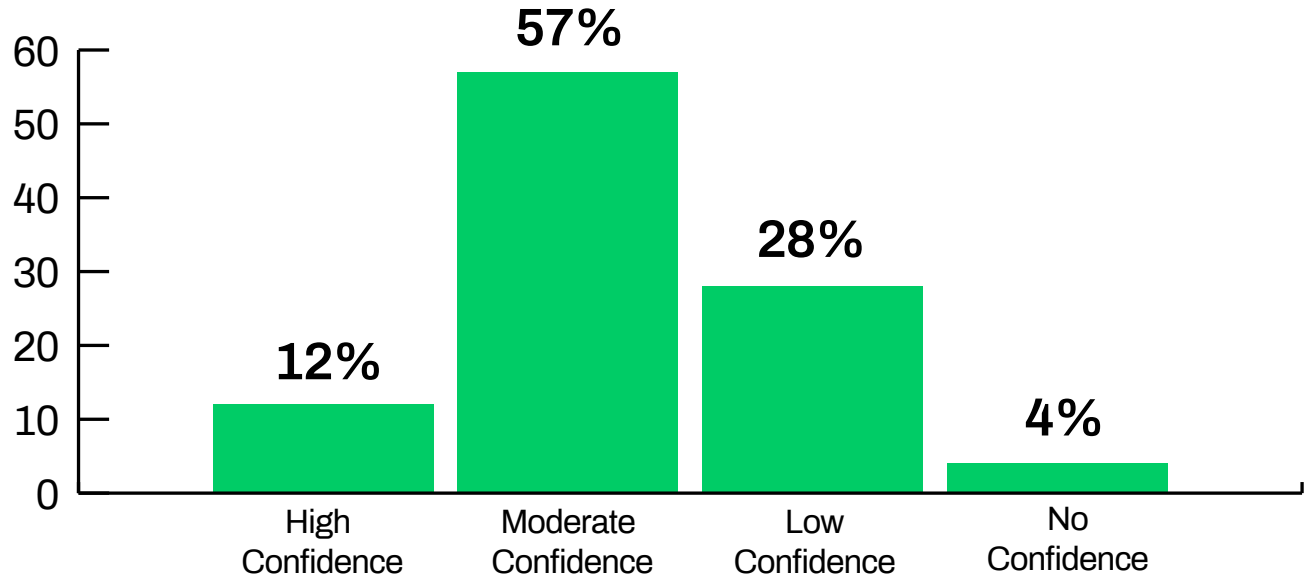


...continued from previous page

SOCs are strained, and even without a workforce shortage, many teams would still be getting way more alerts than they can handle. Staffing difficulties of course exacerbate that problem and this has compounding effects on the other challenges noted. SIEM and SOAR solutions are typically the first tools deployed to address these problems, but teams spend much of their time having to learn these tools and fine-tuning them before they can get any security value. These tools help with alert correlation and response, but with more sophisticated adversaries and newer techniques, a human element is still often required to review or confirm the work of automation platforms. While this is critical, it also slows the remediation process and proves to be difficult in many resource-strapped organizations.

Only 12% of security professionals are highly confident that their security alerts are adequate enough to respond quickly.

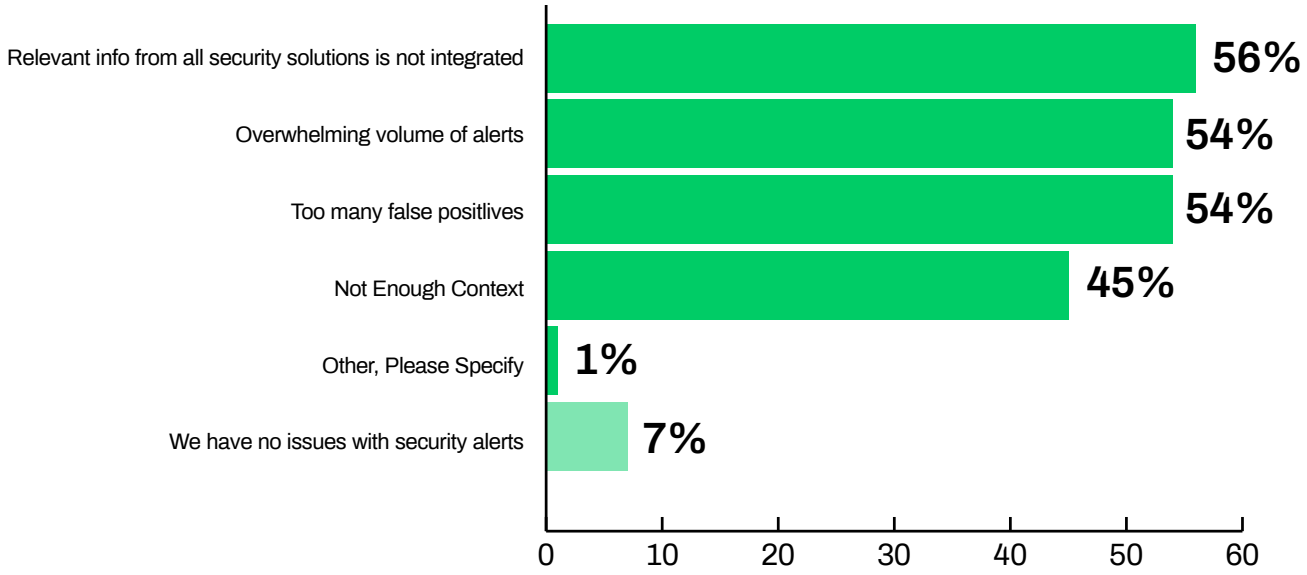
How confident are you that the security alerts your team receives provide enough information to enable quick, decisive response actions?



Insufficient alerts are one of the primary barriers to threat response and nearly one-third (32%) of security professionals have low to no confidence that the alerts contain enough information to respond. Alerts should be relevant, easy to understand and have the right contextual information. If the tools in the security stack aren't tuned correctly, security teams are left with meaningless or irrelevant alerts that create noise and don't add any value.

93% of security professionals report limitations with existing security alerts.

What issues exist with current security alerts that prevent your team from delivering quick, decisive response actions? Choose all that apply.

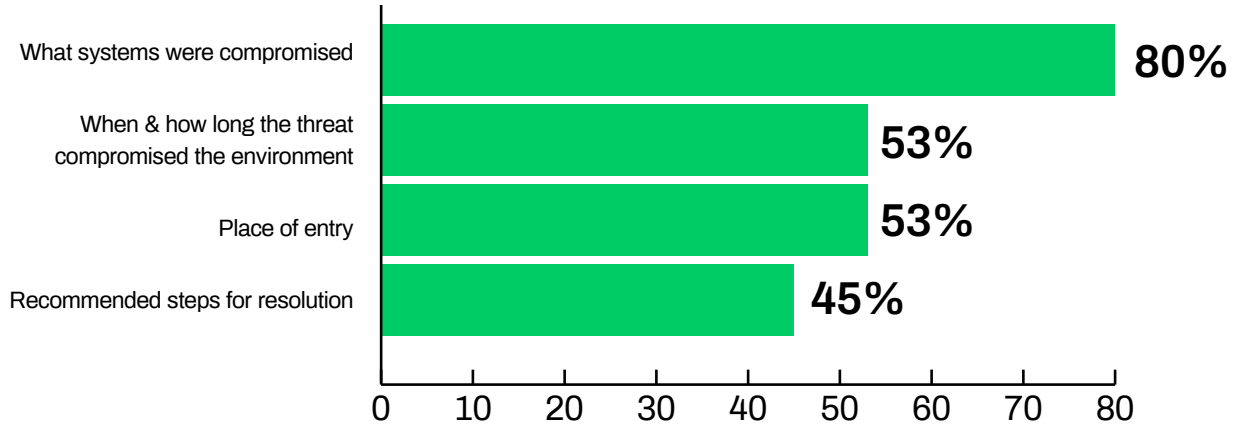


Imagine a scenario in which a Windows machine is compromised. It is infected through email, leading to a compromised identity communicating with a rogue IP address. This would generate different alerts for the host, email and firewall which typically would span over a period of several weeks without any correlation between them. In this instance, SOC analysts are left to make sense of all these different alerts to get a complete picture of the threat. In order to improve alert fidelity, it is critical that security teams get actionable alerts.

Alert fatigue cripples the SOC, and growing pressure to stay on top of everything often results in an overwhelming amount of alerts. Without the right resources, enabled by the right processes and technologies, identifying the alerts that actually need addressing is an insurmountable task.

Less than half (45%) of security professionals receive recommended actions in their security alerts.

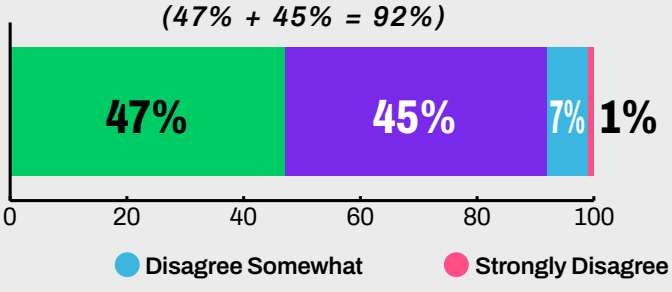
What information about a threat is typically incorporated into alerts used to evaluate security incidents?



Most alerts reviewed by security analysts include some data about the systems impacted and dwell time, but if the correlation isn't done correctly, these alerts do not provide a complete picture of the alerts nor the appropriate steps for resolution. In the end, inadequate alert information and poor correlation ends up slowing the response times.

92% of security professionals say they could respond to threats more effectively with details integrated from multiple security tools, versus multiple separate alerts (e.g. host, email and firewall).

We could respond much more quickly to threats if alerts included detail from mulitple perspectives (network, firewall, cloud, email, identity, etc.)



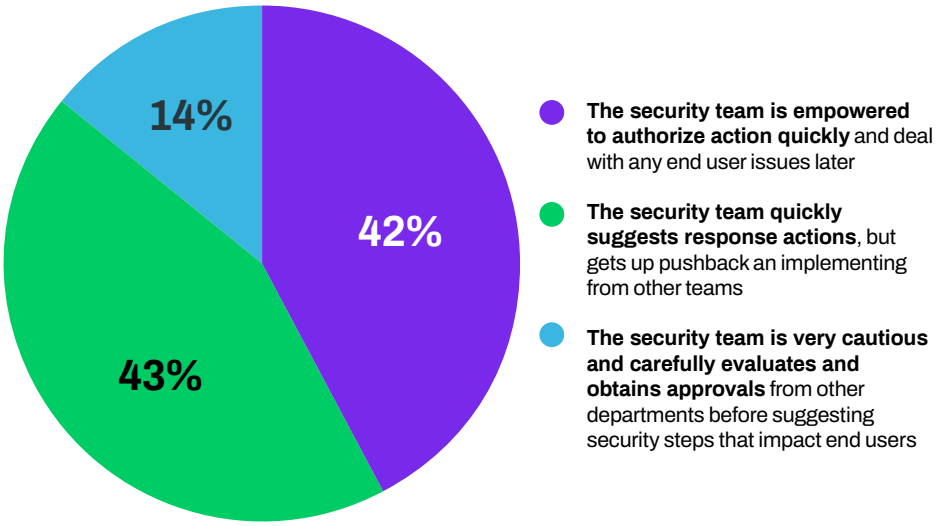
High-fidelity alerts enable better response. Security professionals want more information in the alerts they receive. Threat detection and threat analysis need to go beyond SIEM and SOAR capabilities and offer teams greater insight into risks throughout their environment. Alerts can be processed further through deduplication, enrichment and prioritization.

Alert deduplication is the process of reducing alert noise by organizing and grouping alerts. Alert enrichment removes false-positives and deduces actionable intelligence from alerts. SOCs can see a nearly 75% reduction in alerts through these processes. SOCs can then use advanced correlation and investigation to further reduce actionable alerts. SIEM based correlation can help reduce the actionable alerts by more than 90%

Culture and pushback from other departments also slow down the response process.

Which of the following statements best represents your company's culture towards taking a swift security action that could disrupt employees,customers or other end users?

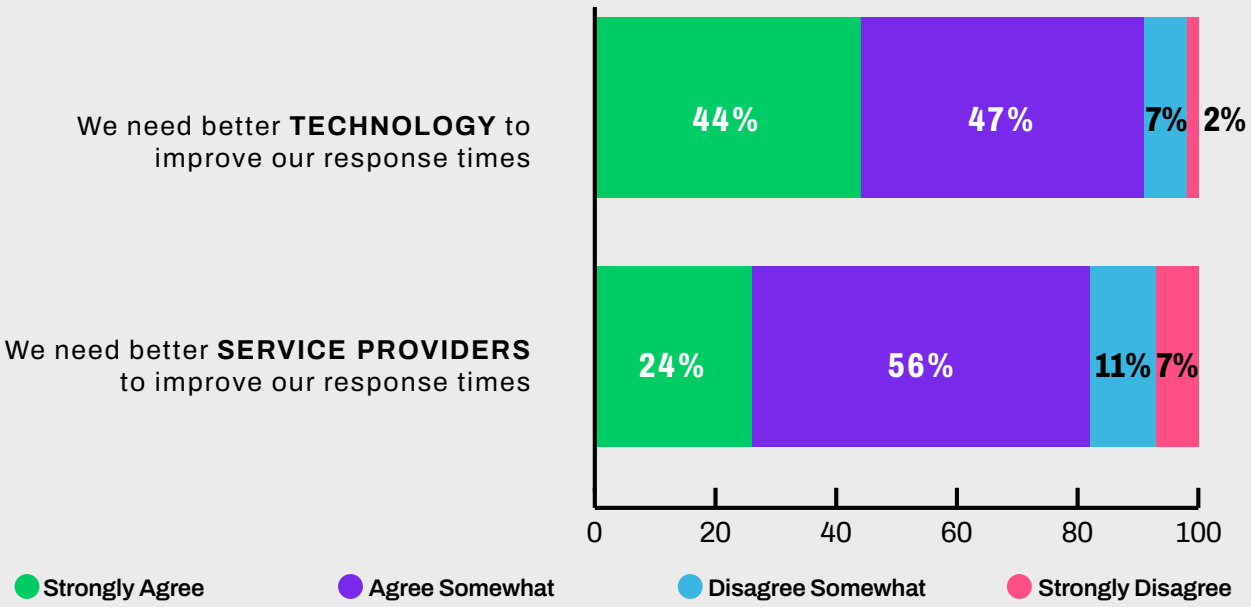
Sometimes other departments may block a suggested security action, potentially out of fear of disruption or skepticism that the detection actually poses a threat. Higher fidelity alerts may play a role here in providing more comprehensive and objective evidence of the threat, and therefore more confidence in implementing the recommended response action.



The Keys to Response

Most security professionals agree better technology (91%) and better service providers (80%) would improve response times.

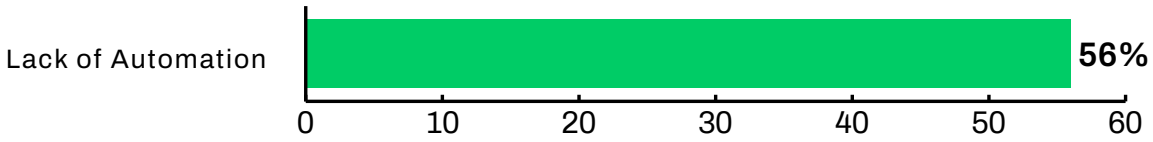
Please rate your level of agreement with each of the following statements.



Security leaders believe a combination of security technology and competent service providers can help improve response times. In addition to monitoring the environment 24/7/365, service providers can also aid in alert correlation, reduction in false positives, and threat detection. Security teams can work together with the service providers to implement response capabilities.

More than half (56%) of security professionals say “lack of automation” is a challenge to improving response times.

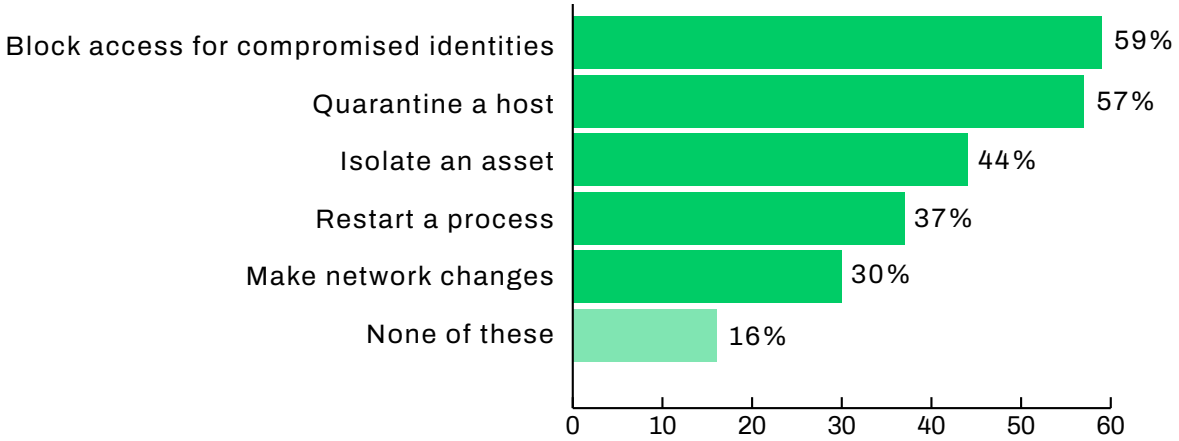
What challenges does your team face in improving response times to security threats once they have been detected? Choose all that apply.



Overall, lack of automation negatively impacts response times. However, the level of accepted automation varies for different organizations, as outlined in the next chart.

84% automate specific types of security response, although specific actions taken vary.

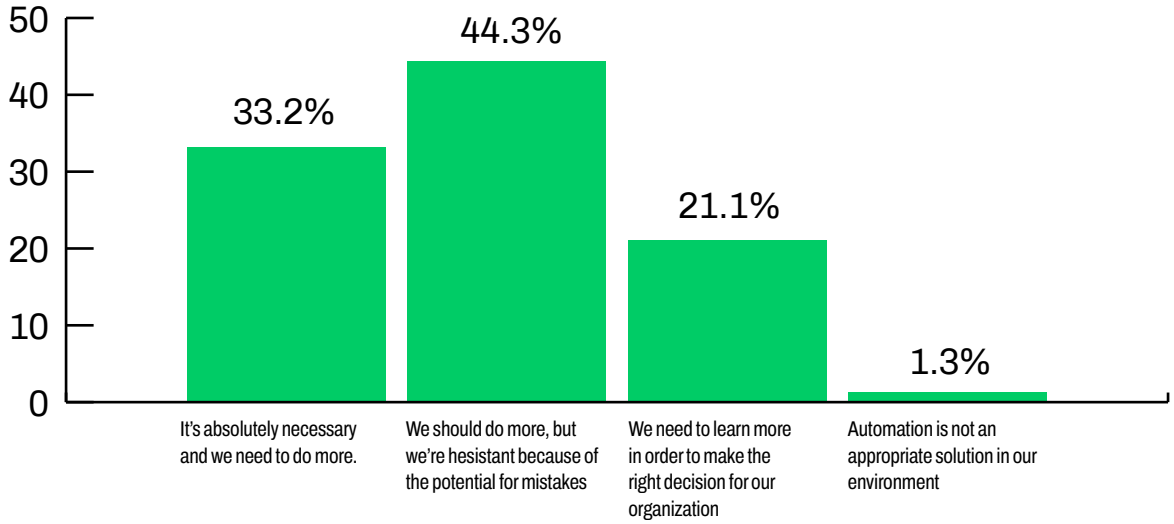
Does your company automate any of the following as part of security response? Choose all that apply.



Reauthorization and restricting access are the most common automation actions. In most cases, this type of automation is non-invasive and aimed at containing the threat rather than eradicating the threat. Most security leaders shy away from automating actions like restarting a process on a host or file roll back. Even then, in these cases automation is still restricted to a single host or identity and doesn't effectively contain threats that have spread across the network.

99% of security professionals believe they need more or want to learn more about automating security incident response in their organization.

What is your opinion about automating security incident response?

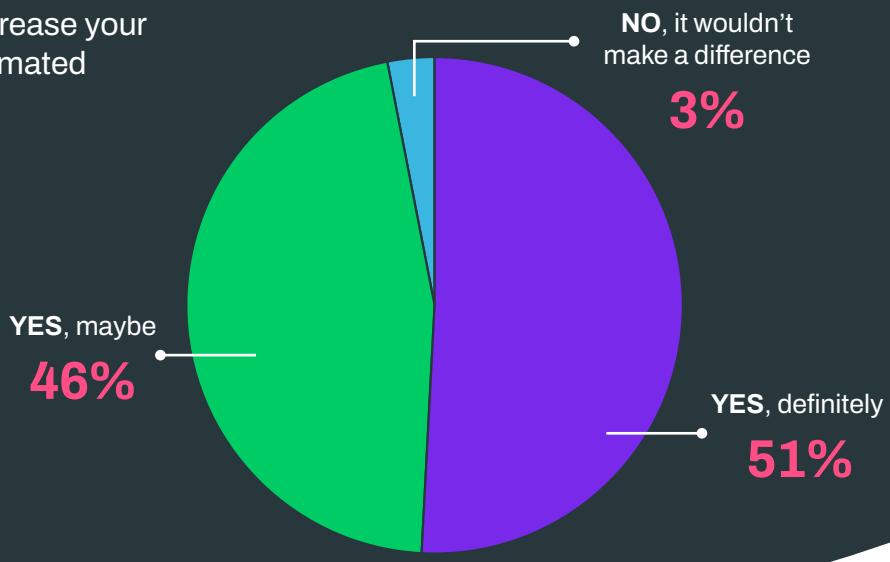


It's well understood that overreliance on human involvement contributes to slow response times. While nearly all (99%) of security professionals either believe they need to pursue more automation for security response (77%), or are exploring the possibility (21%), fear of making mistakes as a result of implementing automation is a key concern.

97% of security professionals state that more accurate alerting may increase confidence in implementing automated response actions.

Would more accurate alerting increase your confidence in implementing automated response actions?

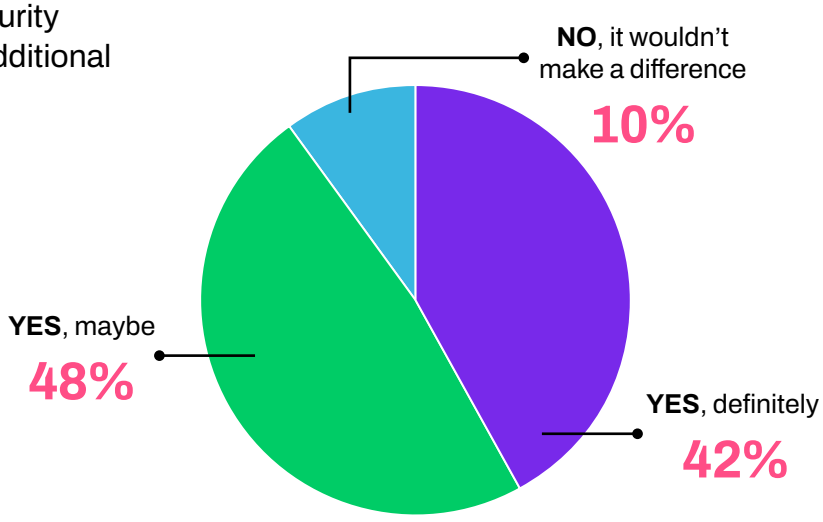
It is no surprise that the overwhelming majority of security professionals believe that accurate alerting, with the right contextual data and advanced correlation, will increase their confidence in implementing automated response actions.



90% of security professionals agree that better alerts would instill confidence in MSSPs managing more response actions on their behalf.

Would more accurate alerting increase your confidence in allowing a managed security service provider (MSSP) to manage additional response actions?

Even working with a managed security service partner, security professionals are faced with alert overload. Adding better correlation of alerts, and a complete picture of business risk, will help security leaders trust their service provider to take response actions on their behalf.



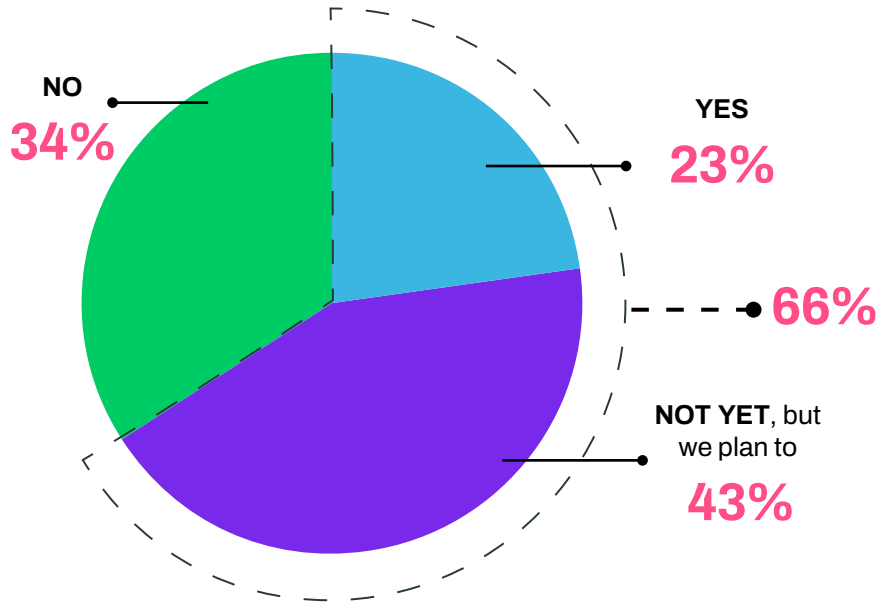
XDR Adoption is a Work in Progress

Extended Detection and Response (XDR) tools are aimed at solving the issues with alerting, threat detection and response across the environment. XDR adoption is driven mostly by large organizations but security leaders still struggle with the expertise and cost of implementing such solutions. Most security teams want XDR outcomes for their security programs, but without the complexity and cost, and therefore look for managed services partners to help them on their XDR journey.

With the need for better information on the detected threats, it may be no surprise that 66% of security professionals are investing or planning to invest in XDR solutions.

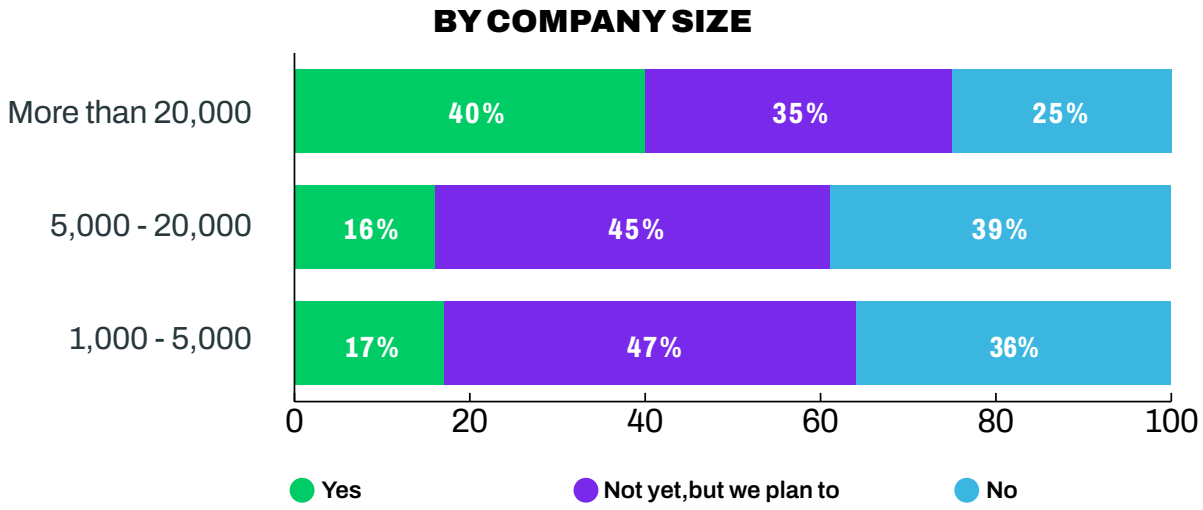
Has your organization's security team invested in any Extended Detection and Response (XDR) solutions?

With the promise of advanced alert correlation, better detection of threats, and automated response capabilities, it is no surprise that XDR adoption is top of mind for modern security leaders. However, organizations of all sizes face significant challenges in adopting XDR.



Large enterprise organizations are far more likely to have adopted XDR.

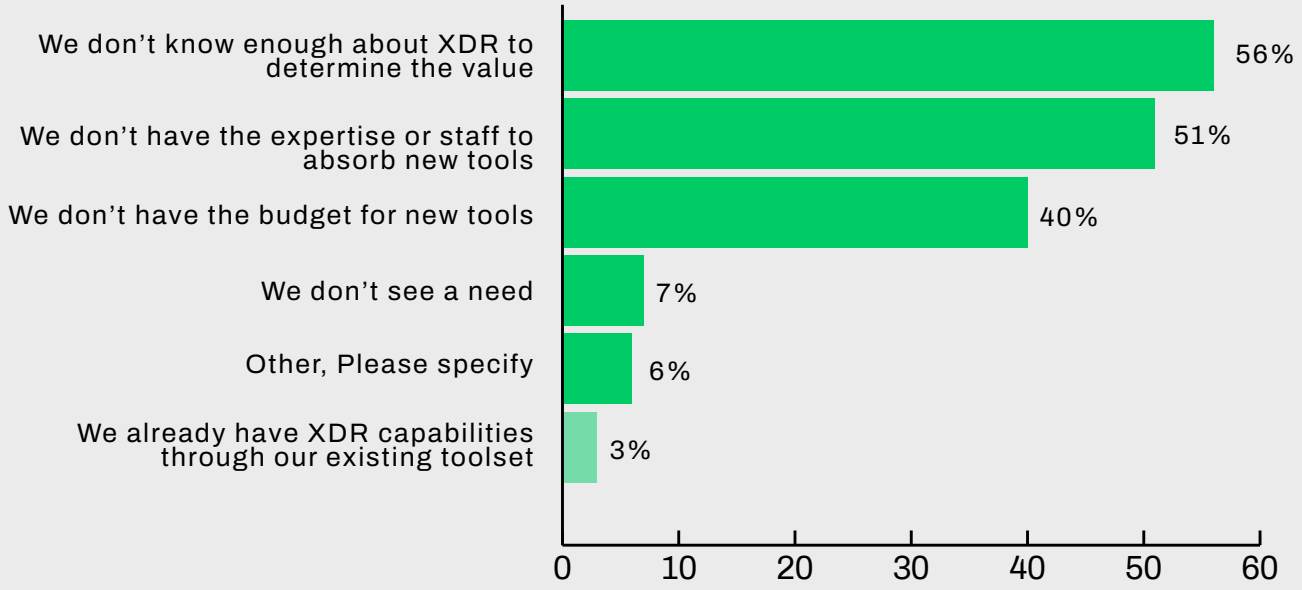
Has your organization's security team invested in any Extended Detection and Response (XDR) solutions?



Larger organizations with bigger security teams and skilled cyber security professionals have been leading the charge in XDR adoption. Smaller organizations want XDR outcomes for their security programs but lack the expertise, budget and ability to get the value from XDR tools outside of preconfigured options.

Of those not planning to invest in XDR, more than half (51%) of security professionals say the reason is they don't have the expertise or staff to manage it.

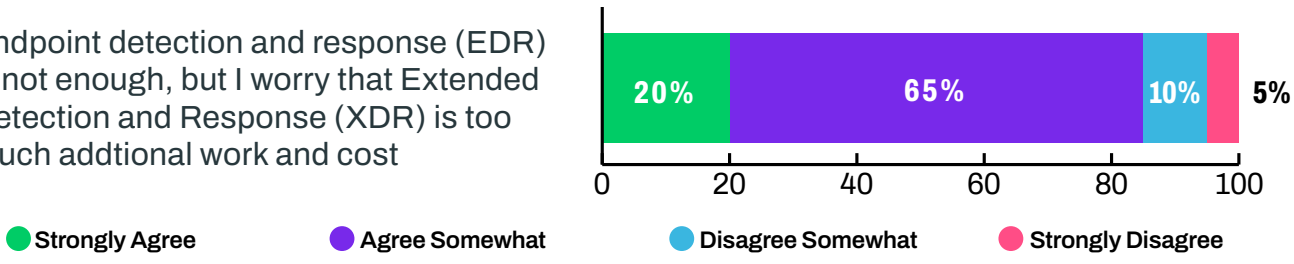
Why hasn't your organization's security team invested in any Extended Detection and Response (XDR) solutions? Choose all that apply.



While many are still learning about XDR, one of the main challenges for security teams is having the right people in order to manage it. Adopting new tools in the security stack means finding the skilled people who know how to configure and tune the tools, enable different use cases, and write custom content to get more value out of their investment.

While they recognize the need to go beyond the endpoint, 85% of security professionals said XDR is too much additional work and cost.

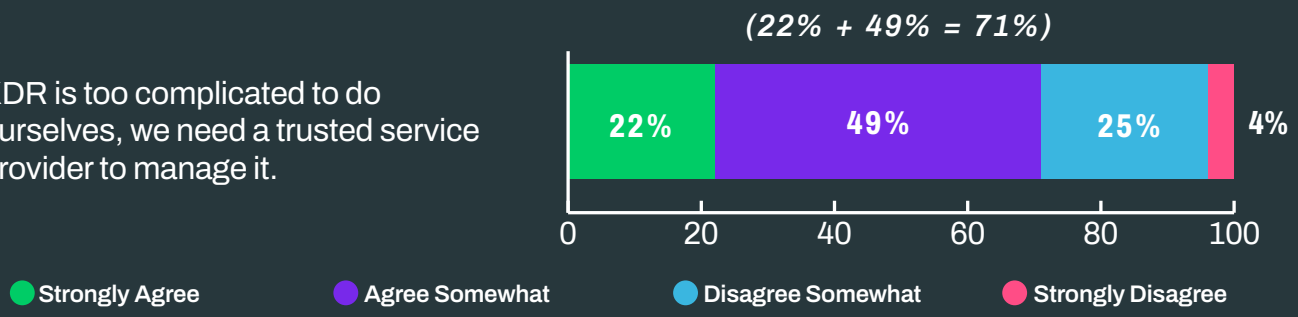
Endpoint detection and response (EDR) is not enough, but I worry that Extended Detection and Response (XDR) is too much addtional work and cost



Security leaders want XDR outcomes that they can't get from today's Endpoint Detection and Response (EDR) tools but still believe that XDR will be too much work and cost to realize the benefits of the investment.

71% of security professionals said they would want XDR as a managed service.

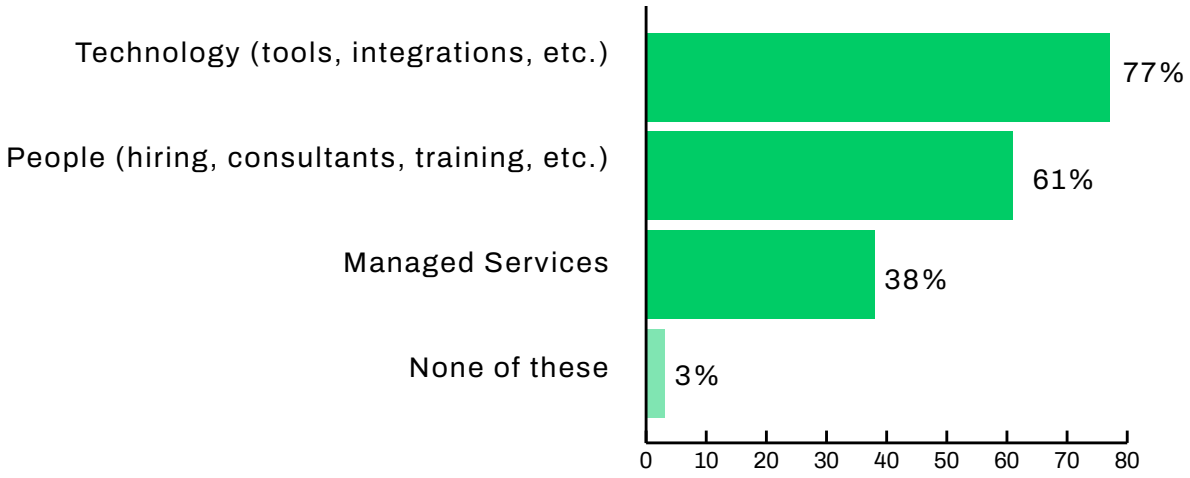
XDR is too complicated to do ourselves, we need a trusted service provider to manage it.



The complexity and cost of implementing and managing XDR tools has most security leaders looking to managed security providers to deliver the XDR outcomes to enhance their security program.

38% of security teams are prioritizing managed services for new spending.

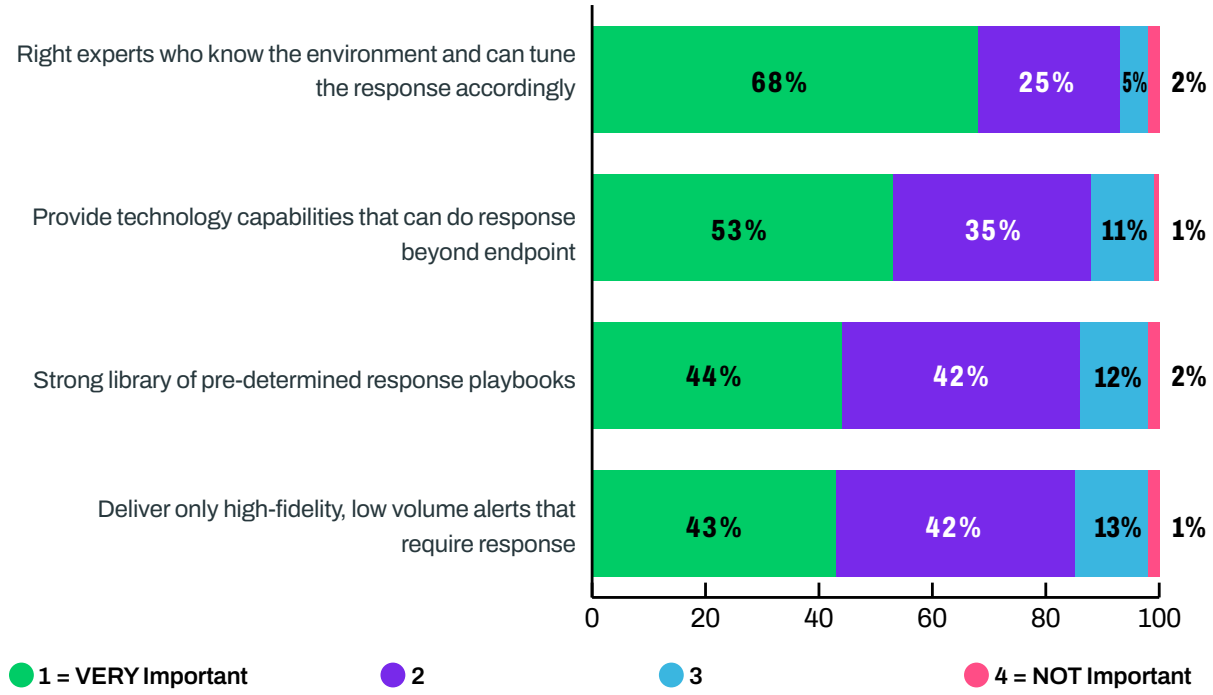
Which of the following is your security organization prioritizing for new spending? Choose all that apply.



With the combination of staffing challenges and a growing threat landscape, the desire for managed services should come as no surprise. More and more organizations seek a trusted partner to strengthen their security postures and fill gaps they are not able to address internally, particularly in providing protection 24/7, outside usual business hours.

Expertise and capabilities for response beyond the endpoint top the list of requirements for selecting a managed service provider to improve response, according to security professionals.

Imagine the scenario where your organization is considering a service provider to help improve security response. Please rate each of the following in terms of their importance to that decision. *Rate from 1 to 4 where 1 = VERY important and 4 = NOT important.*



Not all managed service providers are created equal. In order for security leaders to trust their managed security services partner, they need to see that the service provider has skilled professionals who know the customer's environment and can tune the current tools in the security stack to get the maximum value. The ability to demonstrate response capabilities beyond the endpoint (e.g. network, cloud, email, and identity) is also a critical requirement for security leaders before they can trust their provider to take response actions on their behalf and thereby improve response time to mitigate impact to the business.

Conclusion

Current insights from security professionals highlight specific challenges that are blocking SOCs from responding to threats in a timely enough manner to prevent negative impacts to the business. By identifying these issues, this report also highlights actionable opportunities to improve security operations and response strategies.

As the findings revealed, stronger detection capabilities can pave the way for automated response. To achieve that, people, processes and technologies can better align to enhance detection with security telemetry correlation, beyond just the endpoint. With more completeness in the detection data, there is more confidence in enabling real-time response through automation and managed service providers.

Automating defined response and mitigation actions eliminates the lag in response time due to dependence on security staff and cross-departmental resources. A managed detection and response partner with automated response capabilities and the right cybersecurity expertise can help speed response and free internal resources to focus on other issues and projects.

How Deepwatch Can Help

Deepwatch partners with its customers to speed detection and response, providing SOC capabilities and 24/7/365 protection. The Deepwatch SecOps platform leverages security telemetry across data sources to detect complex threats and provide complete real-time response – programmatically, customized to the customer's environment. Deepwatch security experts work in partnership with the customer's security team to identify and prioritize which response processes to automate, alleviating the short-term burden of automation in order to achieve the long-term benefit.

As a partner and extension of internal security teams, Deepwatch offers peace of mind and assurance that threats are rapidly and holistically addressed, unlocking a new level of security that supports business outcomes.

deepwatch

ABOUT DEEPWATCH

Deepwatch is the leader in managed security services, protecting organizations from ever-increasing cyber threats 24/7/365. Powered by Deepwatch's cloud-based security operations platform, Deepwatch provides the industry's fastest, most comprehensive detection and automated response to cyber threats together with tailored guidance from dedicated experts to mitigate risk and measurably improve security posture. Hundreds of organizations, from Fortune 100 to mid-sized enterprises, trust Deepwatch to protect their business.

Visit www.deepwatch.com to learn more.

CONTACT US

4030 W Boy Scout Blvd, Suite 550
Tampa, FL 33607
(855) 303-3033