

Cybersecurity leaders face unprecedented challenges as generative AI introduces new risks and threats. Having robust managed detection and response systems in place is crucial for securing digital assets while leveraging GenAI to further corporate goals.

Cyber-Resilience in the GenAI Era Through Effective MDR Implementation

April 2025

Written by: Craig Robinson, Research Vice President, Security and Trust

Introduction

As generative AI (GenAI) has entered everyday nomenclature, this evolutionary technology's potential risks and threats are causing leaders in cybersecurity, risk and compliance, and the C-suite to question whether their organizations are properly prepared to secure their digital assets while using GenAI to further corporate goals. In short, every C-suite leader and board member should be wondering whether their organization has the right structure to succeed in the GenAI era.

Ensuring the proper structure is in place often starts by realizing that success will likely require good partners. There is no magic "do-over" button to press if ransomware gangs steal or maliciously encrypt the data that feeds GenAI capabilities. The right cybersecurity pieces must be in place, and they must then run with operational effectiveness and efficacy.

Figure 1 shows the mix of ingredients that organizations utilize to remain cyber-resilient. With 41% of the average spending mix going to security service providers, CISOs need to ensure that these providers have the technology acumen to navigate the rough seas that sophisticated attacks cause. Service providers with industry-specific regulatory and compliance knowledge can help an organization chart a secure course in uncertain times.

AT A GLANCE

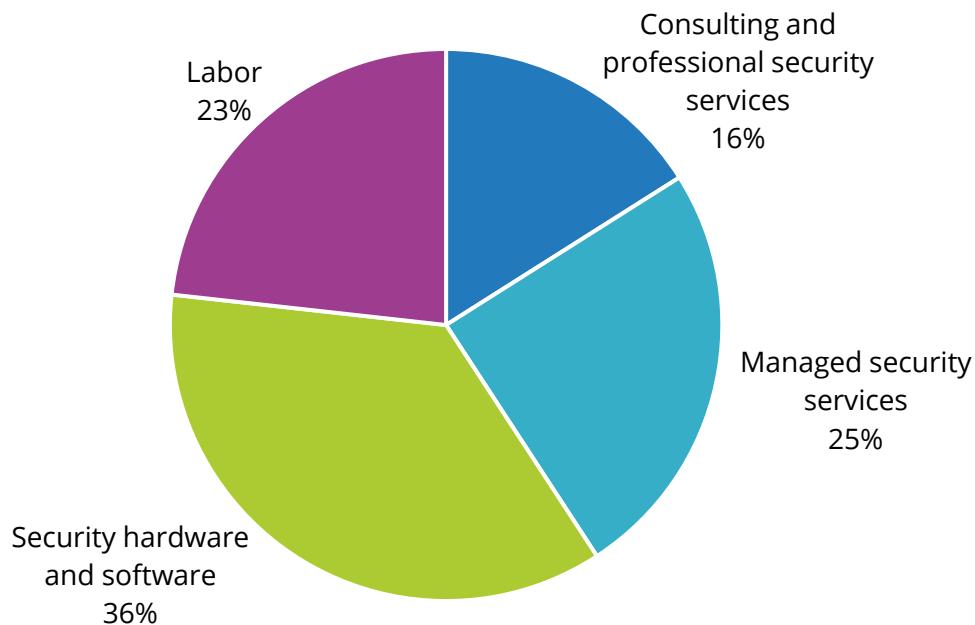
KEY TAKEAWAY

When utilizing a security service provider, organizations must evaluate the capabilities of and the collaboration that occurs with both the service provider and the technology partners it wraps its services around.

FIGURE 1: **Breakout of Cybersecurity Budget**

Q *Approximately what percentage of your organization's total cybersecurity budget is spent on the following broad categories?*

IT and cybersecurity budget influencers



n = 1,123

Source: IDC's Global Security Services Survey, November 2024

How to Address the Shortage of Qualified Cybersecurity Professionals

Any CISO or CIO leading a cybersecurity program will agree that it hurts when a competitor poaches a seasoned, well-performing team member. Exceptional talent is hard to find, even harder to retain, and disruptive to the organization when they leave.

The growing use of managed security services reflects the need for stable staff, hardware, and software to protect the ever-growing digital surface. As automation and AI increasingly handle or aid the many tasks a cybersecurity professional is responsible for, human intuition must evolve to another level. When evaluating outside service providers to supplement or replace in-house practitioners, organizations need to judge how well the provider's team will be able to perform its tasks.

Does the provider and its cybersecurity specialists understand the organization's industry? For example, there is a big difference between securing restaurant payments and securing the electrical grid in a municipality. Add the extra dimensions of privacy and compliance needs, and it becomes clear that the human expertise necessary to protect an enterprise remains an important factor, regardless of whether the provision of that expertise occurs internally or externally.

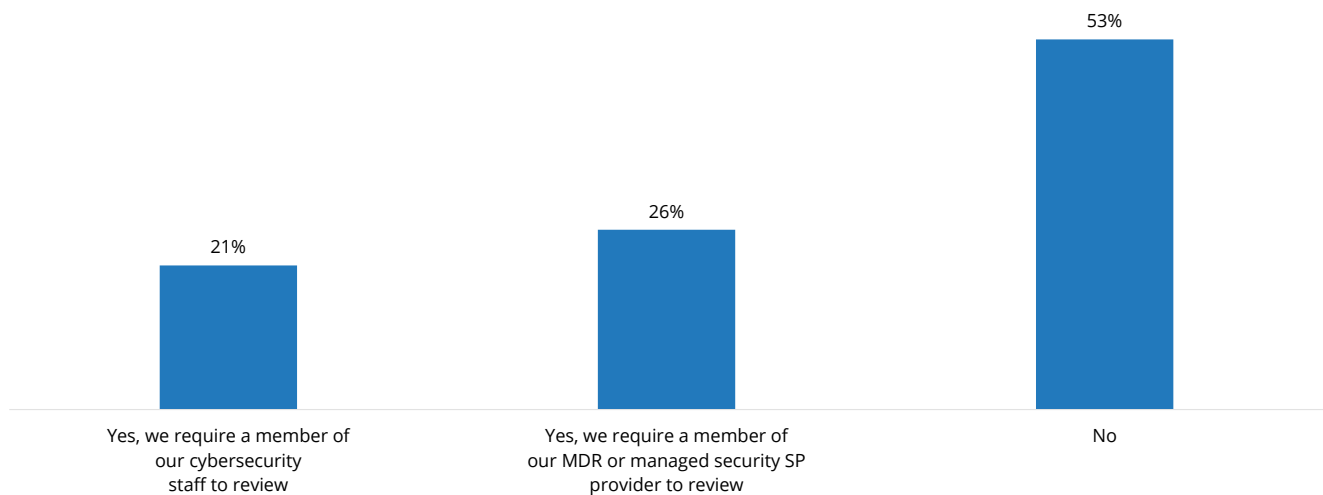
Human-in-the-Loop

The takeaway is that it is not a binary choice between human review and AI or other automation capabilities. The type of technology that service providers use to detect and respond to cyberattacks matters, especially in the critical managed detection and response (MDR) and managed extended detection and response space. Managed security services providers (SPs), global systems integrators (GSIs), and pure-play MDR providers will apply an increasing amount of technology, which buyers of these services need to thoroughly evaluate.

Figure 2 shows that only 53% of organizations stated that they do not require a human to review an investigation before closing it. This highlights a rough parity between those willing to trust the technology mix to close the loop in an investigation and those that do not. It is fair to say that organizations are fully automating their approach to threats they perceive as less severe, whereas potentially more severe attacks require a higher level of expertise.

FIGURE 2: **How Organizations Approach Cybersecurity Investigations**

Q Does your organization require a human-in-the-loop to review any cybersecurity investigation before it is closed?



n = 1,123

Note: Respondents indicated that their organization primarily uses managed security service/MDR providers for its detection and response needs.

Source: IDC's Global Security Services Survey, November 2024

The ideal situation would be to have a security operations center (SOC) analyst who has world-class cybersecurity tools at their disposal and understands an organization's industry and region.

The 24 x 7 x 365 need for organizations to protect their digital assets, together with staffing shortages and the need to raise their overall cybersecurity maturity levels, has propelled the growth of MDR services.

What to Look for in a Cybersecurity Provider

It is important to recognize a percolating trend in modern SOCs. There is recognition that there are too many tools in the mix and, therefore, too many vendors. Many of these tools are nonintegrated, unmonitored, or unmanaged. Organizations should review their existing tools and service providers to streamline their portfolios.

Security leaders should seek out several key characteristics as they add or replace current service providers and cybersecurity tools. In detail:

- » **ROI:** IDC research shows that who the CISO reports to is shifting from the CIO to the COO or CEO. While CISOs must still be concerned about traditional speeds and feeds, they must now also address ROI, reduced or mitigated risk, compliance, and operational resilience.
- » **Threat intelligence:** Threat intelligence feeds can help attribute cyberattacks to specific threat groups, allowing for targeted responses and remediation. Applying this capability to the core speeds and feeds metrics makes technology-focused leaders take note. The information that CEOs and COOs care about impacts the need for quality proactive threat intelligence. Understanding the risks to the enterprise requires new intelligence sources, such as geopolitical and targeted threat intelligence, that reference how bad actors may target different personas in the business. CEOs and COOs are also interested in recognizing and mitigating industry- and region-specific threats.
- » **Partners:** The adage "no one knows it all" offers lessons for cybersecurity software and service providers. Collaborations between service providers that have the business acumen and technology providers that have the required technical pedigree can make for a good partnership. Nearly every cybersecurity technology provider is investing in GenAI use cases. When evaluating GSI or managed security SP capabilities, organizations must consider providers' collaborations with cybersecurity technology suppliers. Have they developed industry-specific solutions? Have they noted subtle regional differences?
- » **Adjacent capabilities:** Complexity is the enemy of cybersecurity. Yes, there is a need for some organizations, especially larger ones with complex digital infrastructures, to have a defense-in-depth or best-of-breed operational model. However, even within these large and complex environments, it is important to review the vendor mix and look for opportunities to consolidate. The same rule applies to the technology stacks that service providers work with. Does the underlying cybersecurity technology provider have a history of either internally developing solutions or externally investing in smaller companies that come up with the latest and greatest cybersecurity solutions?

The Benefits of MDR

A trusted GSI or managed security SP can help guide, supplement, and elevate the CISO's cybersecurity program as well as provide some respite to these issues. It is also important for organizations to take advantage of outside providers whose core competencies lie in helping firms maintain an even keel and in elevating programs to meet advanced threats. The tactical issues of running a 24 x 7 x 365 SOC will always exist and require considerable time from senior security leadership. Offloading some of the issues CISOs face to an industry-aligned MDR provider is a recognized approach to the problem. The benefits of utilizing an MDR provider include the following:

- » **Efficacy:** Outcomes matter. MDR services focus on detecting, stopping, and responding to cyberattacks. Their core competencies around four of the six pillars of the NIST cybersecurity framework — identify, protect, detect, and respond — allow CISOs and other cybersecurity leaders to work on more strategic initiatives, such as the recover pillar, which is rapidly gaining attention as cyber-resilience becomes a board-level discussion item.
- » **Efficiency:** The glory days of annual double-digit percentage growths in the CISO's cybersecurity budget are largely behind us. The economic reality is that no geographic region is sustaining significant economic growth to help fuel higher-than-normal budget growth for cybersecurity. The details of which areas organizations allocate cybersecurity costs to are almost as important as the amount of scarce dollars they allocate. This is where a managed security service such as MDR comes in. The consumed value compared with the subscription cost is significant when considering the human resources, tools, integration, maintenance, and internally developed IP necessary to replicate an MDR service's capabilities.
- » **Aces in their places:** Organizations should ask themselves the following questions: Is monitoring, detecting, and rapidly responding to cyberattacks a core competency? Are they really good at it? These questions are important because for many, the answer to at least one is likely no. Ask any aspiring cybersecurity practitioner what their next job goal is, and it is likely not to be a tier 1 or a tier 2 SOC analyst. Architecture, incident response, pen testing, and red teaming exercises will be at the top of the list. Chasing down another false positive that a poorly tuned SIEM kicks out gets old, real fast.
- » **Future proofing:** How many organizations had a publicly available GenAI service on their radar before November 2022? Such offerings have radically changed the capabilities that nation-state actors and other criminally motivated cybersecurity miscreants have at their fingertips. In response, those who defend the enterprise now also have new GenAI-related capabilities they can use, at least theoretically. But does the team use these capabilities? Do they work? Are they integrated? What about the next new capability? Are security operations future proofed?

Last, although many may consider detection and response needs to be tactical requirements rather than strategic C-level discussion items, this notion is false. With more CISOs reporting to COOs or CEOs, ideas around resilience are becoming top of mind for these personas. A zero-day attack should cause the opening of incident response playbooks. Will the organization's response be to mount a practiced, prepared posture? There is a greater likelihood of the organization initiating a forward-looking and proactive posture if it is not busy fighting the fires of modern SOC operational issues.

Considering HCLTech and Google Security

HCLTech's Universal Managed Detection and Response (UMDR) service is designed to provide comprehensive threat detection and response capabilities. A significant aspect of this service is its strategic collaboration with Google Cloud

Security. The partnership leverages HCLTech's industry-specific cybersecurity background with Google's scalable security solutions to deliver a robust, AI-driven security offering that addresses the complex needs of modern enterprises.

HCLTech UMDR, powered by Google Security, offers a unified approach to threat detection and response, integrating various security components into a comprehensive solution and allowing for seamless data ingestion from multiple sources. This integration provides centralized visibility and real-time analytics crucial for identifying and mitigating potential threats across different environments, including on premises, cloud, and hybrid.

Key aspects include:

- » **Ubiquitous ingestion:** UMDR can ingest data from any source, ensuring comprehensive coverage and centralized visibility. This capability is essential for identifying potential threats across diverse environments.
- » **Speed and scale:** The service analyzes data in real time, utilizing continuous analytics to provide actionable insights. This rapid analysis helps quickly identify and mitigate threats, reducing the potential impact on business operations.
- » **Strong investigations:** UMDR empowers security analysts by prioritizing critical threats and providing tools for in-depth investigations. This focus on high-priority threats ensures that analysts can respond effectively to the most significant risks.
- » **Collaboration:** The service promotes close collaboration between HCLTech and its customers, facilitating integrated decision-making processes and enhancing an organization's overall security posture.
- » **Superior skill sets:** Organizations benefit from the expertise of HCLTech's security professionals, including SecOps advisors, threat hunters, and detection engineers. These experts bring knowledge and experience to the table to provide strong security support.
- » **AI-driven technology:** The service can detect elusive cyberadversaries using advanced ML algorithms. This AI capability enables real-time threat intelligence and automated response, keeping organizations ahead of potential threats.
- » **Enhanced threat detection and response:** Google Security brings robust security automation capabilities to the UMDR service. By integrating Google's Security Operations suite, HCLTech can offer proactive threat detection and effective response measures. This integration allows for real-time monitoring and rapid response to emerging threats, so organizations can maintain a strong security posture.
- » **Fusion Platform integration:** HCLTech's Fusion Platform, powered by Google Security, provides a modular operating model that offers flexibility and end-to-end capabilities. It enables the convergence of IT and operational technology (OT) cybersecurity operations and can handle complex environments, including OT, industrial control systems, hybrid clouds, identity and access management, endpoints, networks, and applications.
- » **Comprehensive security coverage:** This includes advanced threat detection, end-to-end incident life-cycle support, and proactive threat hunting. The collaboration also enhances the service's ability to provide real-time threat intelligence and automated response, which are critical for maintaining business continuity in the face of cyberthreats.

Other noteworthy features of HCLTech's UMDR service are its AI-driven technology and automated response capabilities, which accelerate crucial InfoSec metrics, such as mean time to detect and mean time to respond. This rapid response reduces potential damage and downtime, ensuring business continuity.

Challenges

MDR providers are adding GenAI capabilities to their tool chests at a breakneck pace. There is little doubt that Google Cloud Security will continue to invest in the technical capabilities that HCLTech can utilize in its MDR offering. The challenge for HCLTech will be to balance the technical capabilities of GenAI use cases with its industry knowledge and apply them both in a cohesive manner.

Conclusion

Organizations must prioritize robust cybersecurity measures to counter evolving threats. The integration of superior skill sets and AI-driven technology can significantly enhance threat detection and response capabilities. Strategic collaborations, such as those with leading managed security providers, offer comprehensive security solutions that leverage advanced technologies and expertise. Success in the GenAI era will require CISOs to be picky about the companies they use to provide them with crucial cybersecurity products and services to ensure cyber-resilience within their organizations. However, CISOs and other security leaders must also ensure that their partner's partners also have a track record of success.

Success in the GenAI era will require CISOs to be picky about the companies they use to provide them with crucial cybersecurity products and services to ensure cyber-resilience within their organizations.

About the Analyst



Craig Robinson, Research Vice President, Security and Trust

Craig Robinson is a research vice president within IDC's Security and Trust research practice, focusing on managed security services and integration. Coverage areas include Managed Detection and Response services, Cyber-Resilience, and Incident Readiness and Response services. Craig delivers unparalleled insight and analysis, leveraging his unique practitioner experience leading diverse IT teams across several industries. This expertise positions him to provide valuable thought leadership, research, and guidance to vendors, service providers, and clients worldwide.

MESSAGE FROM THE SPONSOR

As cyber threats evolve in complexity, Managed Detection and Response (MDR) services are essential for modern organizations. MDR integrates advanced threat detection and incident response capabilities, enhancing overall cybersecurity. By leveraging AI-driven insights, MDR solutions offer real-time visibility into potential threats across various environments, enabling swift identification and mitigation of risks. Incorporating MDR into cybersecurity strategies ensures organizations can manage the dynamic cyber landscape, maintain operational resilience, and protect valuable data assets effectively.

HCLTech Universal Managed Detection and Response (UMDR), powered by Google Cloud Security, enhances threat detection capabilities through proactive vulnerability identification and real-time threat assessment. The collaboration between HCLTech and Google Cloud Security reflects a forward-thinking approach to cyber resilience, combining deep expertise with state-of-the-art technology. To learn more about the partnership, visit:

<https://www.hcltech.com/google-cloud>



The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. CCPA