DARKReading RESEARCH

AUGUST 2022

State of Cybersecurity Research Report: Sharing the Burden, the Defenders' Perspective

GoSecure

Executive Summary

For years, midsize businesses mostly had two choices for security: go it alone with an in-house infosec team or turn critical tasks of defense and response over to a security service provider. The former places the entire burden on the organization's own defenders, who are frequently underbudgeted and understaffed relative to the risks and compliance requirements they face in today's challenging, dynamic threat environment. The latter can mean turning over responsibility — and control — to a third party that may not be fully aligned with the organization's goals and strategies.

Now a third option is emerging — one that is proving especially effective for resource-challenged, security-minded organizations, particularly those in highly regulated verticals: sharing the security burden with a trusted partner. Managed security services providers (MSSPs) — and managed detection and response (MDR) providers in particular — can be a force multiplier for overburdened teams, but only if the organization is willing and prepared to engage in such cooperative security relationships.

A new study commissioned by GoSecure and conducted by Dark Reading shows how security professionals continue to wrestle with key areas of information security, particularly defense and response-related disciplines that require a high degree of skilled human interaction. The research reveals how organizations parcel out precious resources to protect their critical assets, how they're dealing with shortfalls in budget and bandwidth, and where defenders can benefit from assistance safeguarding the business. The data demonstrates the value of combining focused, in-house security resources with robust, third-party managed security services to improve overall security posture across all levels of the business.

Key Findings

Going It Alone: Most midsize organizations employ five or fewer full-time security staffers. In 38% of cases, those small teams manage all of their company's security tasks.

Pressure Points: Limited budgets and inadequate staffing top the list of obstacles most detrimental to the effectiveness of in-house security teams.

Sluggish Response: Over four in ten respondents said resolving their latest breach took between one day and one week; one in six said it took weeks or months to respond and rectify the fallout from the attack.

On the Legal Hook: Some 87% of in-house security teams are now responsible for data protection requirements included in industry-specific regulatory compliance mandates.

The Look of Success: Practitioners are looking to MSSPs to help them lower overall risk (56%), expand capabilities for protection, defense, and response (53%), and increase their security maturity (48%).

Introduction: Confronting a Growing Security Gap

When it comes to developing and maintaining robust cyber-defense, detection and response capabilities, organizations are at a distinct disadvantage. Many have grown too complex to simply outsource everything to an IT-managed services generalist with a basic, bolt-on security practice. These same firms typically lack the support staff and infrastructure sufficient to safeguard their rapidly expanding roster of critical technologies.

A recent survey by research firm Vanson Bourne finds that 61% of in-house practitioners lack skills to properly tackle security issues — up from 52% in 2020. That's a problem, particularly for the growing number of midsize firms staring down enterprise-grade cyber threats and risks. According to the European Union Agency for Cybersecurity (ENISA), more than 80% of in-house professionals now process critical data, making cybersecurity imperative for firms of any size. While the majority of midsize businesses rolled out new technology in the wake of the COVID-19 pandemic — mostly remote access and cloud solutions — fewer than 10% implemented any additional measures to secure these new solutions, ENISA finds.

The biggest infosec challenges for organizations in this segment center around complex tasks, as well as those that require the highest level of expert cybersecurity skills and human interaction. Our research shows practitioners are putting a brave face on their overall security posture, while also recognizing significant shortcomings in their approach to safeguarding the organization at large.

These security professionals in the Dark Reading research represent small to midsize teams. With decent skills in basic infosec blocking and tackling but less mastery of more sophisticated controls and strategies such as threat prioritization or incident detection and response. Most safeguard the entirety of their company's critical assets with only meager resources and little outside help. For those efforts, they rate themselves about a C+.

The findings make a compelling case for enlisting the assistance of ancillary security services, particularly third-party managed security services firms that offer MDR. By sharing the cybersecurity burden with an MDR provider, security leaders can augment the capabilities and capacity of in-house teams, reduce alert fatigue, hasten detection and response, and increase security sophistication, all while maintaining control of the organization's overall infosec priorities, goals, and strategies.

Unlike more general managed security service providers, which face many of the same capacity and capability challenges as the broad-based security teams they were designed to supplant, MDR offerings are tightly focused on risks and outcomes that directly affect the business. MDR providers specialize in understanding security events from all sources at scale and turning that telemetry into rapid, real-time threat detection and incident response.

Because they provide a specialized proficiency — a blend of human and technical facilities — that's largely beyond the scope of most security teams, MDR providers deliver help right where the research shows practitioners need it most.

Small Teams, Big Challenges

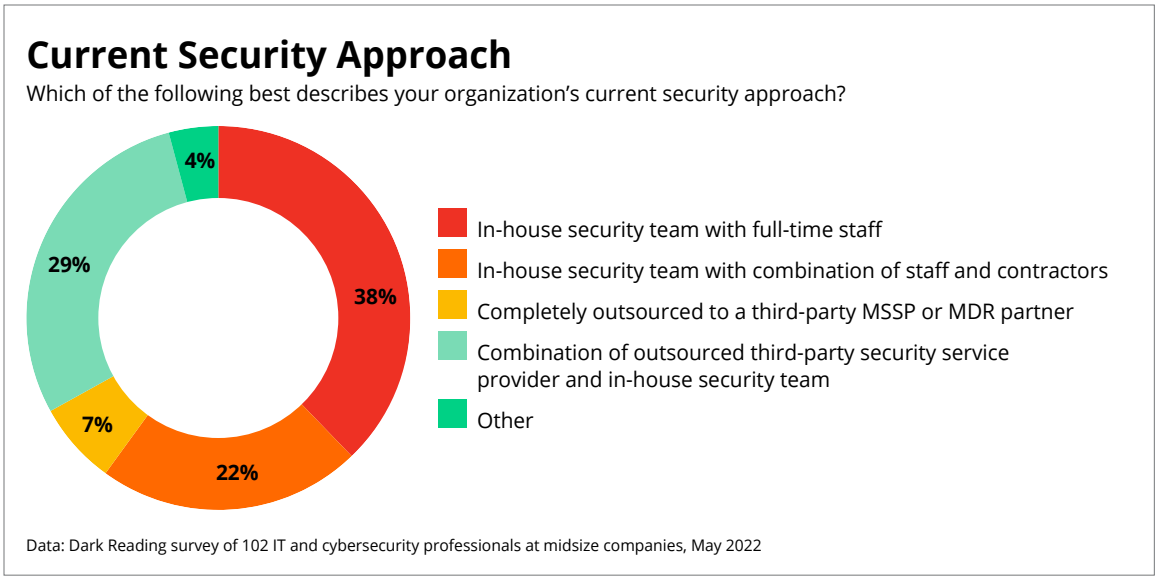
Over the past decade, a guiding IT truism has emerged: All businesses are now technology businesses. Indeed, the eras of cloud computing, digitization, and digital transformation have democratized technological benefits once reserved for large enterprises. Even small businesses now have robust web applications, complex partner and supply-chain connections, remote workers and branch offices, and troves of cloud-connected product and financial and client data.

With these big-business capabilities came big-business problems — most notably how to protect it all from attackers roused by the prospect of ripe new data sources, keen to exploit perceived weaknesses in defenses.

Smaller firms expanded their technology footprint by an order of magnitude; their security capabilities, not as much. Many fail in their efforts to effectively detect and react to threats because they lack focus, expending much of their finite energy on wide-ranging, generic security monitoring and data collection while ignoring meaningful, more nuanced analysis. The gap is a product of scale.

More than half of the respondents we polled say they have five or fewer security staffers. With those relatively small teams, 38% are managing all of their company's security tasks in-house while 51% use some combination of staffers, contractors, and managed services partners **(Figure 1)**.

Figure 1.



Just a handful (7%) outsource security completely to a third-party security services specialist.

In this environment of small teams facing sizeable responsibilities, in-house practitioners offer a tepid assessment of their capabilities. Just under half of our survey respondents (46%) rate their organization's overall security posture a passable 3 on a scale of 1 to 5. The share of security professionals in this middle ground, a group with clear room for improvement, outnumbers those with self-assessment scores of "very good" and "excellent" combined. Meanwhile, 1 in 10 characterize their defenses as "fair" or "poor."

A collection of organizational pressures — such as finances and staffing, along with a host of inconsistent capabilities and spotty overall protections — weighs heavily on the security sophistication of these beleaguered security teams. Asked to consider the factors most detrimental to their security teams, the majority (56%) cite limited budgets **(Figure 2)**. Nearly as many (48%) say inadequate staffing while about a third (31%) call out the growing roster of regulatory compliance requirements. Other notable concerns include poor visibility into systems and data (28%), alert fatigue (25%), and poor collaboration with other stakeholders (21%).

Security leaders also have a limited budget for enterprise-grade issues, which forces them to make difficult choices regarding coverage priorities — focusing meager resources in some areas while forsaking others. A slim majority expresses high confidence in basic disciplines such as email and endpoint protections, but that confidence wanes in more complex, labor-intensive areas such as vulnerability and risk assessment, asset inventory and configuration management, identity management, compliance, secure app development, and supply chain audits **(Figure 3)**.

Figure 2.

Adding pressure and complicating the mix of responsibilities for defenders, compliance requirements represent a significant additional burden. The vast majority of respondents (87%) say their organization must expend precious security resources to ensure compliance with a type of security-related industry or governmental regulation — the most common being the healthcare industry's Health Insurance Portability and Accountability Act (HIPAA) privacy rules, retailers' Payment Card Industry Data Securi-

ty Standard (PCI DSS) which governs credit card transactions, and the European privacy guidelines known as the General Data Protection Regulation, or GDPR **(Figure 4)**.

All common regulatory edicts have detailed requirements for data defense and incident response protocols. If the ramifications of getting hacked aren't sobering enough,

Figure 3.

Handling Security Disciplines

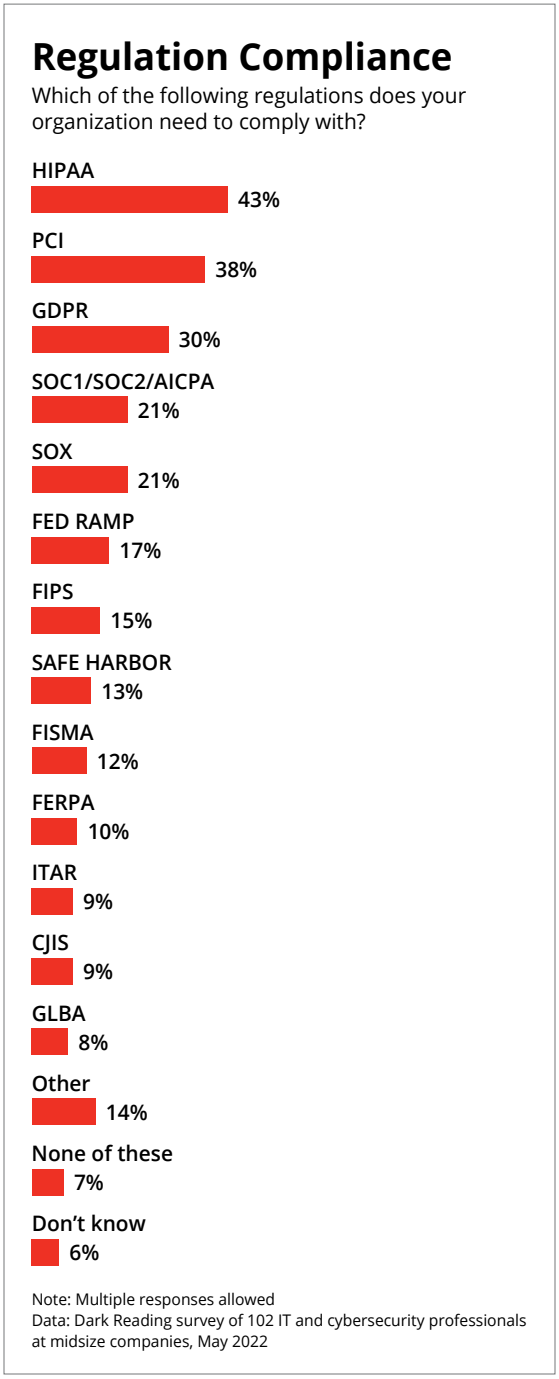
Rate your organization's current handling of the following security disciplines.

	Excellent	Very good	Good	Fair	Poor	N/A
Endpoint protection, detection, and response	23%	33%	30%	9%	1%	4%
Post-delivery email protection	23%	31%	31%	6%	5%	4%
Pre-delivery email protection	23%	38%	22%	9%	4%	4%
Security awareness training	18%	30%	35%	14%	2%	1%
Data backup, continuity, and disaster recovery	17%	31%	38%	7%	4%	3%
Network protection, detection, and response	16%	35%	38%	7%	1%	3%
Identity and credential management	16%	29%	39%	10%	3%	3%
Regulatory compliance	15%	38%	31%	7%	2%	7%
Asset security posture/patch status	15%	31%	37%	12%	1%	4%
Vulnerability scanning/ management	14%	27%	43%	9%	4%	3%
Comprehensive asset inventory	14%	33%	26%	19%	2%	6%
Asset configuration/change management	13%	27%	36%	11%	9%	4%
Cloud applications and data protection	12%	33%	32%	11%	1%	11%
AppDev platform and code security	11%	23%	31%	13%	6%	16%
Threat modeling/risk management	8%	24%	37%	10%	13%	8%
Third-party/supply chain auditing	7%	19%	35%	19%	10%	10%

Data: Dark Reading survey of 102 IT and cybersecurity professionals at midsize companies, May 2022

running afoul of any data security regulatory compliance measure can come with steep fines and other significant statutory penalties. For smaller organizations, the double jeopardy can be financially devastating.

Figure 4.



Environmental Hazards

Even with all the obstacles they face, many practitioners have done a fair job maintaining focus in their environments. In fact, 62% of professionals had 10 or fewer solutions deployed. Still, those with a collection of tools on the higher end of that scale might benefit from extra skilled human support for monitoring, management, and maintenance to effectively provide defenses — including detection and response capabilities. More than 1 in 4 security practitioners surveyed (26%) say they've suffered a breach in the past two years, and another 14% say they might have been breached or aren't sure. More bracing than the share of respondents falling victim to attacks are the events that followed such breaches.

In a realm where damage from intruders can happen within minutes, those that have been breached concede incident response often took days. Out of the respondents, 4 in 10 say resolving their latest breach took between one day and one week, and 1 in 6 say it took weeks or months to respond and rectify the fallout from the attack. Exacerbated by the poor response times, these attacks most frequently resulted in the loss of intellectual property, disruptive effects of ransomware, and exposure of customer data.

Respondents understand that such a protracted dwell time between initial breach and subsequent detection, response, and recovery is inadequate. In a stack ranking of desirable improvements, improving detection and response time rated the highest **(Figure 5)**. Following closely near the top of the list of critical improvements for defenders were gaining the ability to continuously monitor the environment for threats and establishing a system of prioritization for vulnerabilities once found.

This trio of top goals has two things in common. All three are table stakes for moving foundational security teams toward greater maturity and true infosec sophistication, and all three demand a judicious combination of tools, controls, automation, and human expertise often beyond the scope of resource-strapped defenders in organizations.

Figure 5.

Priorities to Improve Security Team Efficiency

Thinking about improving your security team's efficiency and effectiveness, please rank the following actions in priority order from highest to lowest.

	RANK
Improving detection and response time	1
Maintaining continuous monitoring	2
Prioritizing vulnerabilities	3
Automating asset discovery/change management	4
Reducing actionable alerts	5
Lowering manual labor requirements for security analysts	6
Generating useful reports and dashboards	7

Note: Rank is based on a weighted score. Answers are weighted and scores are the sum of all weighted counts.
Data: Dark Reading survey of 102 IT and cybersecurity professionals at midsize companies, May 2022

Working in Tandem

With budget and staffing pressures increasing and critical responsibilities rising, security decision-makers are exploring ways to leverage force multipliers in the form of security services partners to improve their posture and practices. The research shows the areas where they need the most help in stark relief. Security disciplines that are the most complex and labor-intensive top the list for those looking to share the burden. Scanning, prioritizing, and managing vulnerabilities are top of mind, as are continuous monitoring and the management of asset inventories and configurations.

Many security leaders have taken the initial steps necessary to augment their security capabilities through services partnerships. Interestingly, 4 in 10 respondents say they already work with a third-party security partner, and another 7% are considering such a relationship.

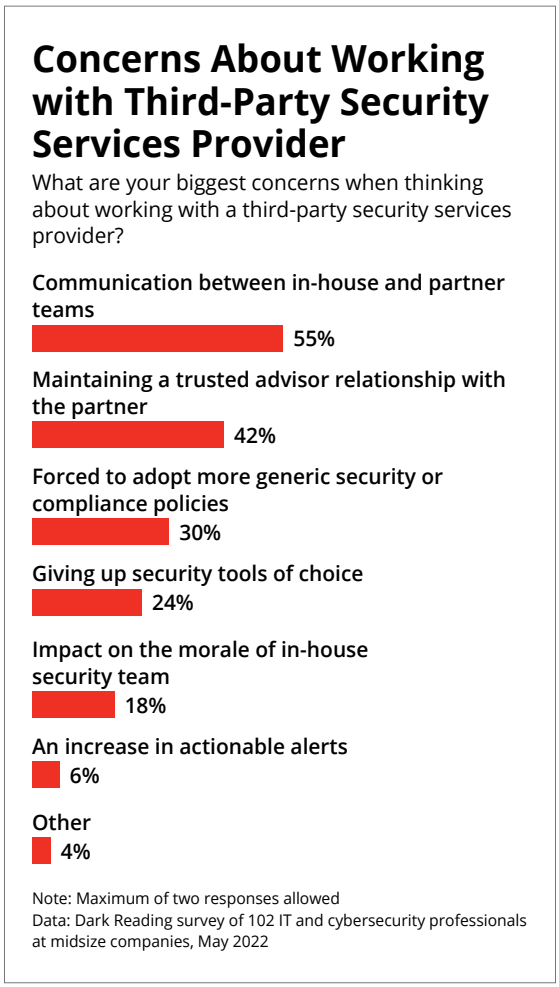
What do they look for in such cooperative arrangements with a security service provider? Security decision-makers surveyed say they want a collaborative relationship with a trusted advisor. They want a durable foundation built on communication and trust. And they look for a managed service partner that will handle critical disciplines like continuous, automated monitoring, detection and response, and freeing in-house security teams to focus on big-picture goals and strategies that best support the unique aspects of their business **(Figure 6)**.

Choosing a partner is driven by the desire to augment capacity and capabilities in the security professionals' known areas of weakness. Top services selection criteria include integrated threat intelligence, risk assessment and management, and expertise in advanced areas of cybersecurity technology **(Figure 7)**.

At a tactical level, security leaders need a security services expert to help them root out vulnerabilities, speed detection and response, and generally, improve their overall security posture **(Figure 8)**.

Metrics for success in a collaborative security services provider arrangement mirror

Figure 6.



the above requirements. The end game for most respondents is to lower overall risk and expand capabilities for protection, defense, and response (56% and 53%, respectively). Better regulatory compliance and a measurable increase in overall security sophistications are also important.

Conclusion: The Benefits of Sharing

Making the case for working collaboratively with a specialized provider of managed security services starts with understanding the depth and breadth of such offerings and their crucial role in strengthening the overall security posture and sophistication of an organization. Managed security services providers with a featured managed detection and response offering give their clients access to the power of a modern security operations center (SOC) delivered remotely as a service. Full-featured MDR offers rapid detection, analysis, and response via threat mitigation and containment.

According to the most recent cybersecurity workforce study by the International Information System Security Certification Consortium, organizations would need to grow their security workforce by 65% to effectively defend critical assets at such a high level on their own.

In an environment where the number of available skilled cybersecurity professionals is down and the costs for recruiting and keeping staff are way up, that's a tall order for most midsize organizations. Leveraging third-party managed detection and response (MDR) gives organizations the ability to affordably access skills and talent they'd otherwise be unable to source.

As a result, managed security relationships are becoming more common among even the most sophisticated infosec professionals, research by McKinsey & Company shows. Trusted third parties are increasingly integral to the successful integration of multiple defenses across the cyberstack. Such systemic security improvement is powering the global managed security services market from $22.8 billion in 2021 to a projected $43.7 billion by 2026, a CAGR of 14%, according to industry analysts at Marketsandmarkets.

Still, organizations taking advantage of outsourced security services remain the exception. Our research shows that 44% of respondents are not currently working with such partners. This demonstrates opportunity for security teams to bolster their secu-

Figure 7.

Importance of Factors When Considering Managed Security Services

When thinking about managed security services, how important would each of the following be to your organization?.

	Extremely important	Very important	Of average importance	Of little importance	Not important at all	N/A
Collaboration/teamwork with our internal security teams	37%	50%	10%	1%	0%	2%
Knowledge transfer, coaching, and mentoring for staff	33%	39%	20%	4%	1%	3%
Integrated threat intelligence	29%	52%	13%	3%	0%	3%
Integrations with our existing security tools	29%	48%	17%	2%	0%	4%
Providing optimum technical capabilities	28%	52%	14%	2%	0%	4%
Dashboard/portal with visibility into security posture and reporting	28%	50%	15%	4%	0%	3%
Integrations with our existing platforms	28%	43%	15%	8%	0%	6%
Help understanding our overall security risks and maturity	26%	55%	11%	3%	2%	3%
Developing a security roadmap	26%	40%	23%	8%	2%	1%
Expertise with our specific regulatory compliance requirements	21%	46%	23%	4%	0%	6%
Adherence to our security framework of choice	19%	39%	31%	3%	0%	8%
Expertise within our vertical industry	19%	35%	36%	5%	1%	4%
Vendor custom playbooks/runbooks to define managed activity support	12%	40%	31%	9%	2%	6%

Data: Dark Reading survey of 102 IT and cybersecurity professionals at midsize companies, May 2022

rity posture and competitively differentiate themselves from their peers with advanced security.

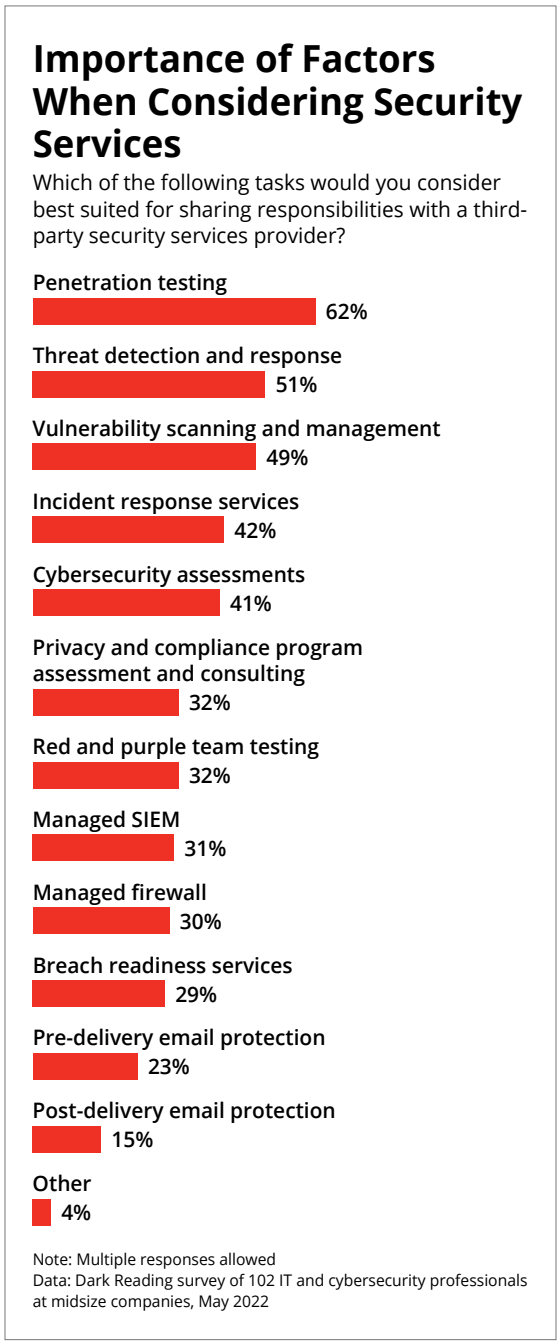
By 2025, analyst firm Gartner predicts fully half of organizations "will be using MDR services for threat monitoring, detection and response functions that offer threat containment and mitigation capabilities." With managed detection and response, "telemetry is analyzed within the service provider's platform using a range of techniques," Gartner notes. "This process allows for investigation by experts skilled in threat hunting and incident management, who deliver actionable outcomes."

When considering an MSSP services partner, consider the following core capabilities as part of the selection process:

The Human Element

As noted throughout our research, the tasks that demand skilled human interaction present defenders with their biggest challenges. One of the most important benefits of engaging an MSSP is access to cybersecurity experts who act as an adjunct to the in-house infosec team. The best partners will ensure that the right people understand the client's business and infrastructure and are always available to advise, assist, and take the most appropriate action when trouble arises. That's key for practitioners we polled — 87% say collaboration with internal security teams is the most important feature of working with an MSSP.

Figure 8.



Always on the Hunt

Continuous monitoring and automated alerts are table stakes for managed security services offerings today — with many making MDR a key solution. In the case of MDRs, this 24/7 visibility sharply focuses on the events, actions, and behaviors that indicate threat and compromise. In addition to threat hunting, MDR providers can synthesize information about the client's environment with current threat intelligence data to deliver a dynamic, prioritized snapshot of security posture and status along with advice for mitigating risks.

Maintaining continuous monitoring and prioritizing threats are top priorities for security team improvement in our research, behind only improving detection and response time. The combo also addresses one of the main tasks our respondents most want to share with an MSSP, namely threat detection and response (51%).

Automation and Machine Learning

Skilled human analysts and practitioners are the fuel for successful MDR engagements. But the depth and breadth of visibility and data collection required to support effective detection and response capabilities would quickly overwhelm even the best security teams if not for a robust technology stack. Automation and a judicious use of machine learning play a key role for MDRs, helping the analysts convert reams of aggregated and archived log data into actionable results.

Adaptability

The threat landscape confronting today's businesses is ever-changing, as are the security policies and processes built to address it. It's vital, therefore, that an MSSP partner be able to scale and flex with the dynamic needs of the client. That means adjusting configurations and settings — at the firewall, in email, or on the endpoint — as new threats emerge and business needs evolve. This is especially important in the realm of regulatory compliance, where critical, industry-specific requirements must be inherent to the security strategy.

Adaptability is crucial to the security professionals we polled with 1 in 3 saying that being forced to adopt more generic security or compliance policies is among their biggest concerns when considering a third-party security services provider. Meanwhile, 32% indicate they could use the help of a services partner to improve their privacy and regulatory compliance efforts.

All of this dynamic capability must reside on a core technology platform sturdy enough to handle exponential growth in the amount of data being collected, analyzed, and stored as the organization — and the threats it faces — evolve and expand.

Cloud and SaaS Savvy

Rare is the organization today that doesn't store and process a sizable portion of its data in the cloud. Yet, our research finds only 45% of respondents feel their ability to protect cloud systems was very good or excellent; 12% say it was fair or poor and 11% say they weren't sure. This exposes a real need among organizations. While a pure MDR offering may not cover all of the bases in the cloud on its own, more advanced MSSPs augment their detection and response services with as-a-service add-ons covering areas such as vulnerability, firewall, and security information and event management (SIEM). These tightly integrated, cloud-capable managed service options help form a holistic safety net and ensure reliable protection for all applications, data, and infrastructure — no matter where they reside.

"In the cybersecurity industry, you can never have enough resources to assist with threat detection," said Cass Information Systems CISO Erica Wilson in a 2021 eBook titled Seven Experts on Transitioning to Managed Detection and Response. "By having the ability to extend your staff with a trusted partner that can provide additional analytics and faster response times to security events in your environment, you are working toward a more mature security program."

Survey Methodology

GoSecure commissioned Dark Reading to research cybersecurity detection and incident response activities as part of the overall security strategy for small and midsize business organizations with between 250 and 5,000 employees. The survey queried 102 IT and cybersecurity managers and executives on perceptions, strategies, and tactics related to security administration, team organization, capabilities, capacity, and propensity to engage outsourced security services partners.

The survey was conducted online in May 2022. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database. Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing U.S. privacy laws.

Twenty-three percent of the respondents are from organizations with 499 or fewer employees, 29% work at organizations that employ between 500 and 999 workers, and 22% represent firms with between 1,000 and 2,499 employees. The remaining 26% represent businesses with between 2,500 and 4,999 employees.

The survey queried respondents with job titles that include chief information officer (CIO), chief information security officer (CISO), other security executive (CSO, VP/SVP Security), head of information security or cybersecurity, head of product team or product manager, VP engineering, IT management and staff, DevSecOps management, SOC manager, application security team member, and security architect.

Respondents' organizations represent more than 20 vertical industries, including government and defense, technology, banking and financial services, education, healthcare, engineering, construction, insurance, and manufacturing.

About

GoSecure

For over 10 years, GoSecure has been a recognized cybersecurity leader, delivering innovative managed security solutions and expert advisory services. GoSecure Titan® managed security solutions deliver multi-vector protection to counter modern cyber threats through a complete suite of offerings that extend the capabilities of our customers' in-house teams. GoSecure Titan Managed Detection & Response (MDR) offers a best in class mean-time-to-respond, with comprehensive coverage across customers' networks, endpoints and in-boxes. GoSecure Titan MDR is the cornerstone of our suite of managed solutions which also includes options to keep systems and applications up to date and in compliance with GoSecure Titan Vulnerability Management as a Service, ensure that firewalls are maintained and working at peak efficiency with GoSecure Titan Managed Firewall and comprehensive visibility across technologies and environments with GoSecure Titan Managed SIEM.

Through expert Advisory Services, GoSecure helps customers test, assess and improve. With a focus on combining the best of technology with skilled people, GoSecure has become the trusted cybersecurity advisor to organizations of all sizes, across all industries. As one of the most skilled and experienced teams in the industry, we deliver solutions as an extension of your IT operations.

To learn more, please visit: https://www.gosecure.net.