KROLL

Managed Detection and Response (MDR) Buyer's Guide

October 2022

Managed Detection and Response (MDR) Buyer's Guide

All organizations should have access to the skills needed to detect and contain threats. But, typically, only the very largest enterprises can afford the millions in annual staff and infrastructure investments required to maintain a Security Operations Center (SOC). Even then, large in-house teams often only see their own environments and may not have frontline visibility to the latest threat tactics and techniques, leading to gaps in incident response (IR) and containment capability. Small and midsized businesses often struggle to recruit and retain enough experienced analysts to keep their small workday teams at full strength.

These issues are exacerbated by the ongoing global talent shortage, alert fatigue, and the relentless pressure to secure an expanding attack surface rife with newly discovered vulnerabilities for threat actors to exploit.

Managed Detection and Response (MDR) services can help ameliorate these challenges by providing the people, processes, and technologies in a turn-key way to strengthen an organization's security posture and reduce its risk exposure. This buyer's guide assesses today's MDR market space and the key criteria for selecting a suitable MDR partner.

KROLL

Begin with the Target Outcomes

Your MDR provider search should begin with a disciplined self-assessment of the outcomes you want to achieve with an MDR service. In addition to preventing breaches, what other specific outcomes should you hope to achieve? Here are the key outcomes that justify the need for MDR:

High-Fidelity Detection

One drawback of the defense-in-depth approach to security has been the rapid proliferation of stove-piped security tools ingesting billions of events and churning out thousands of alerts daily. Many are false positives, which must still be triaged, investigated, and resolved by over-burdened security teams.

An MDR partner should be able to minimize this noise by continuously tuning and updating detection analytics and rulesets so that only true positive alerts are prioritized for investigation. They can also help identify and close gaps in your security architecture by correlating detection events to events reported in threat intelligence feeds or mapped to tactics, techniques, and procedures (TTPs) cataloged in the MITRE ATT&CK framework.

Minimizing Dwell Time

An MDR provider should help minimize attacker dwell time by rapidly identifying threats and indicators of compromise (IoCs) concealed within your endpoint, network, and cloud system telemetry. As evidence, they should convincingly demonstrate their ability to optimize metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) through multiple methods such as ongoing threat research, detection engineering, automation, and analyst training.

Remote Remediation

An MDR provider should also help prevent an initial intrusion from escalating into a catastrophic breach by moving swiftly to contain and remediate threats. This may include such tasks as terminating malicious processes, removing persistence mechanisms from the file system or Windows registry, and isolating compromised systems from the network.

Incident Response Support

Often organizations mistakenly wait until a breach is discovered to bring in IR experts. By this time, business interruption may have already occurred, and the goal is simply to understand what happened and limit further damage. If an intrusion is suspected, bringing in this expertise as quickly as possible can get you ahead of the game to contain the threat and identify related malicious activity in other systems. Having an IR team working hand-in-hand with the SOC team streamlines the threat investigation, remediation, and recovery processes. However, less advanced MDR providers today subcontract IR support to a third party, which can introduce unacceptable delays in response and remediation and can result in finger-pointing between the MDR vendor and its sub-contractor. Common causes for critical delays in these scenarios involve getting the IR team up to speed and having to deploy a new set of agents capable of running adequate remote live forensics. Look for an advanced MDR provider who can integrate their own experienced IR experts as part of the service.

Types of Providers

MDR is a growth market that many security firms are attempting to enter, so it's often helpful to consider how well a company's core business competencies align with its MDR claims.

Managed Security Service Providers (MSSPs)

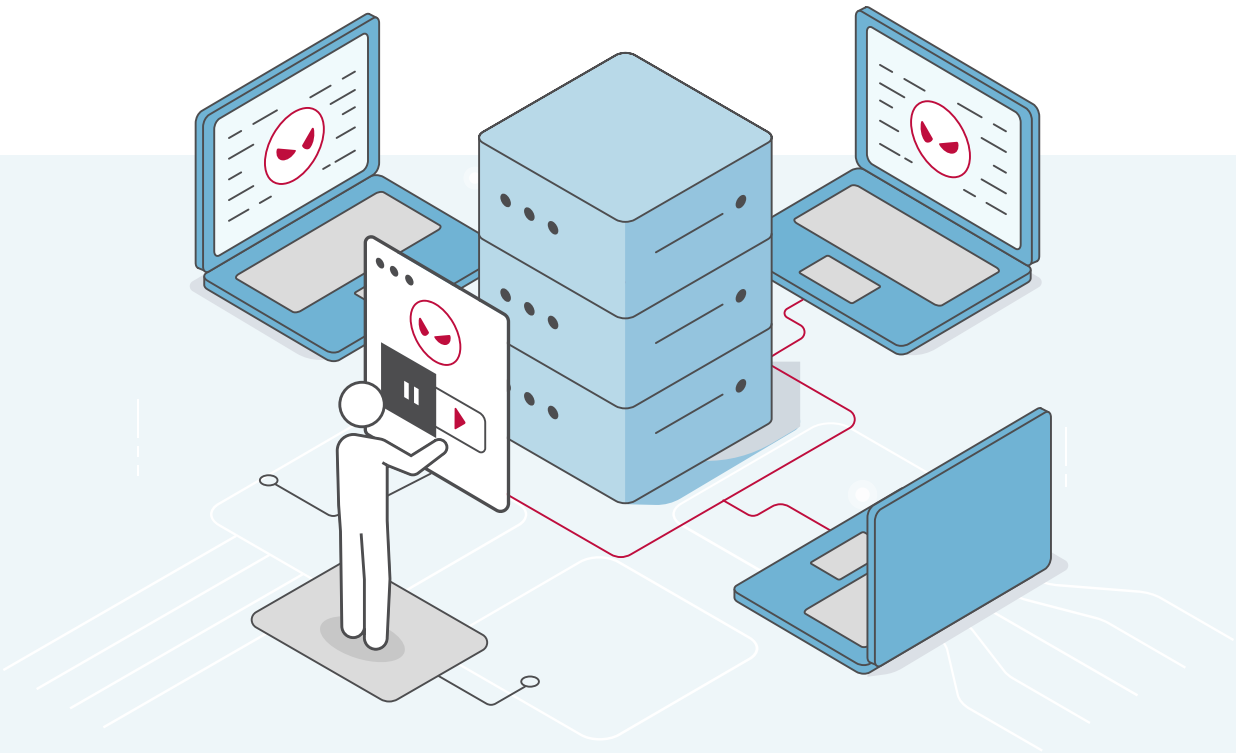
MSSPs have traditionally focused on monitoring and managing firewalls, virtual private networks (VPNs), endpoints, and other devices. By outsourcing these functions, clients can deploy a baseline security infrastructure without adding headcount. The cost avoidance benefits are somewhat offset by a shared security model that requires clients to manage and investigate the resulting alerts. Some mature MSSPs have accepted responsibility for alert management and orchestration in recent years. However, very few provide a comprehensive MDR solution that includes threat hunting, incident response, and remediation. Consequently, most MSSPs remain poorly positioned to deploy and manage a complex, multi-layered security stack that provides the enterprise-wide visibility necessary for effective detection and response.

Product vendors

In this model, clients outsource management and maintenance of the vendor's security products to their implementation and support teams. Products are often supplied on a subscription basis, enabling the client to avoid capital expenditures. Vendors of security information and event management (SIEM) platforms and endpoint detection and response (EDR) systems often promote their ability to develop and deploy customized detection and response rulesets to complement default "out-of-the-box" features. Others offer ancillary services to expand their reach by ingesting and correlating telemetry from other vendors' security tools. However, the intrinsic limitations of the product-centric approach impair their ability to detect and trace a kill chain across the enterprise attack surface or provide the proactive threat hunting, incident response, and remediation services required to meaningfully reduce a client's risk exposure. Over time, changes in the competitive product landscape may leave an organization stuck with an outdated or inferior solution without an easy migration path and continuity of services over the long term.

MDR providers

MDR is a natural evolution away from the historical focus on throwing alerts 'over the fence' for the customer's team to deal with. MDR service providers should act as a partner, working as an extension of your in-house security team, reducing or eliminating the operational workload of monitoring alerts around the clock and adding threat detection, investigation, hunting and response expertise so you can focus on other strategic aspects of your security program or business. MDR providers should be flexible enough to scale the detection and response work as your maturity evolves and needs change, while being transparent with their detections and response processes. Leading providers are technology agnostic, leveraging both proprietary methods and the native capabilities of each security tool to collect, correlate, and investigate alerts and telemetry from across the enterprise. Clients benefit from a multi-disciplinary approach to MDR that is inherently flexible, scalable, efficient, and effective for the long run.



Key Questions for Prospective MDR Partners

The following questions will help you evaluate MDR providers based on their maturity, scope of services, and alignment with the outcomes identified.

1 How long have you been offering dedicated MDR services?

It takes years to develop the people, processes, and technologies required to provide clients with a comprehensive MDR service. The answer will help you distinguish MSSPs and product vendors from pure-play MDR providers with mature offerings and reputations for proven performance.

It's important to distinguish early between those with a MSSP history and those with an actual MDR history. Providers with an MSSP history have had to move away from the typical approaches of "ticket counting", service level-driven monitoring and black-box approach. It's less throwing opaque alerts over the fence to the inhouse team and more about delivering key security outcomes.

MDR Providers should be poised to respond no matter what, all day every day. This shift in mindset means many MSSPs are behind pure play MDR providers in their ability to deliver high-touch engagement, high-fidelity threat detection across all areas of the environment (endpoint, network and cloud), and effective incident response.

Related Questions

In addition to SOC analysts, what other professionals are on staff to enhance the scope and quality of MDR service delivery? For example, does the vendor have malware engineers deconstructing zero-day malware? Are dedicated detection engineers available to update and refine rulesets based on changes to the threat landscape?

You can distinguish those that have really invested in their services by seeing if they have diverse skills sets across highly integrated teams.

2 What data sources and telemetry does your team monitor and analyze?

The answer will provide essential clues about the depth of the provider's detection and response capabilities. MSSP and product vendors are likely to focus only on a limited set of telemetry, impairing their ability to trace a kill chain. In contrast, experienced MDR providers routinely monitor telemetry and alerts across the digital estate, including endpoints, networks, cloud systems, and Software-as-a-Service (SaaS) using a unified threat management platform.

An MDR platform should integrate seamlessly with your existing technology stack (SIEM, EDR, NDR, Cloud, etc.). MDR providers should preserve the value of your current security investments where possible while providing the flexibility to incorporate new tools and technologies as your business and IT infrastructure evolve.

3 Indicate what level of response you provide as part of your standard MDR service. What role will your MDR team play in remediation and recovery?

Distinguishing whether an MDR provider will only go as far as containment rather than removing malware and understanding the root cause could make or break your business.

Under what circumstances will your MDR candidate take responsibility for actively containing and remediating an incident, or will they merely offer recommendations for you to implement?

- Critical response time can be squandered if solely you are responsible for executing and validating containment recommendations. Importantly, how does the provider support incidents that may involve unusual issues such as insider threats or mobile devices? Can the provider provide on-site or laboratory services for physical devices?
- Equally, if the provider is sub-contracting incident response to a third-party supplier, what level of business understanding, communication and timing should be expected? Consider eliminating providers that only offer minimum response and focus on those who will go beyond containment to understand the root-cause and remediate the threat.

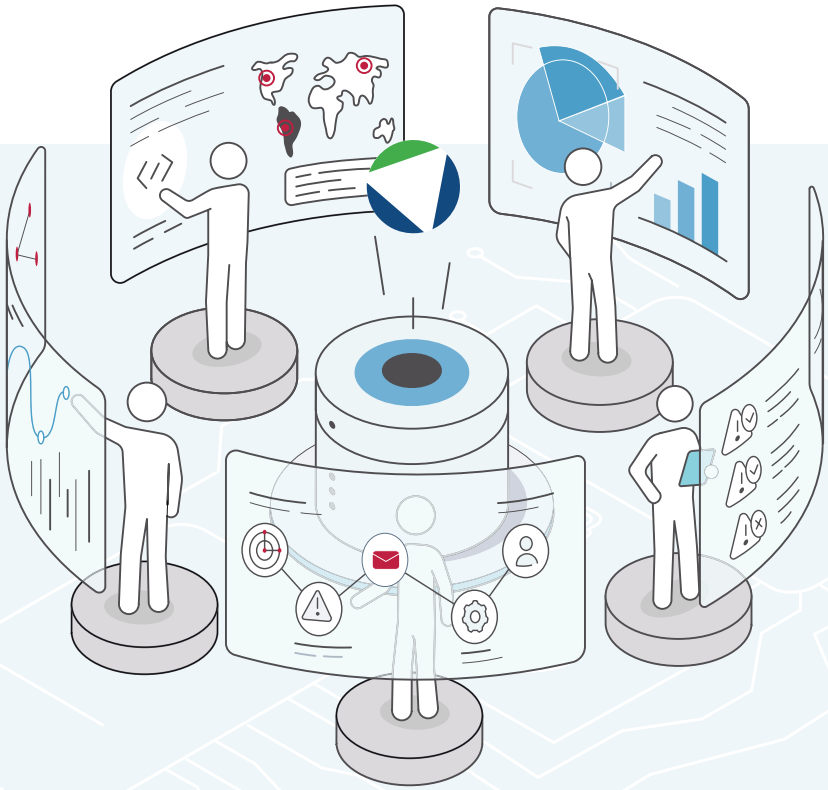
4 What is your methodology for introducing new use cases and achieving continuous improvements in detection accuracy?

Today, many traditional providers rely on the default detection rulesets included by their preferred EDR and SIEM product vendors. Some make minor modifications to those rulesets in response to new threat advisories.

Look for information around how the provider uses the MITRE ATT&CK framework and threat intelligence to tune these rules. Some will say they use this internally, but more proficient providers can provide you with a live mapping of your MITRE ATT&CK coverage to help you understand the scope of their services and demonstrate they are on top of your unique threat profile.

A Real-Life Example

Kroll has developed an agile process for continuously developing and tuning detection rulesets based on the latest threat intelligence. For example, on December 10, 2021, a critical vulnerability was discovered in a widely used Apache Log4j Java logging library that hackers could exploit to compromise tens of thousands of systems worldwide. That same day, the Kroll Applied Intelligence team notified clients of the vulnerability and provided recommendations to patch and ensure detection coverage. Shortly after, they had created 60 custom detection rules to ameliorate the threat for customers.



KROLL

5 How do you use threat intelligence and hunting to identify potential threats and inform your service delivery?

You should be able to lean on your MDR provider for ongoing insight into the latest threats that may impact your business, while also turning this intelligence into active detection, hunting and response efforts.

Threat intelligence needs to be wide enough as it is deep; wide enough to include a variety of organic, open-source, and proprietary sources but deep enough to identify not just known attacker indicators such as an IP address, internet domain, or file hash – referred to as Indicators of Compromise (IOCs), but actual methods and behaviors used by attackers – known as Tactics, Techniques and Protocols (TTPs). This kind of intelligence requires access to dark web forums, live incident response and forensic analysis, and exposure to both cybercriminal and nation-state level activity.

Key to this is ensuring the MDR provider has an adversary-driven mindset, or has teams beyond their core SOC that are engaging with live attacker campaigns and using this information to frequently update detections. This requires tight integration between threat intelligence analysts, malware analysts and detection engineers.

Many MDR services equate threat hunting with the reactive process of investigating high-risk alerts and incidents. In contrast, proactive threat hunting is a cyclical, hypothesis-driven process that assumes an undiscovered breach of an unknown type has already occurred. Threat hunters possess the experience and adversary mindset to ensure malicious activity and advanced persistent threats are surfaced, traced, and remediated efficiently. As noted in NIST Special Publication 800-53, public and private sector organizations should view proactive threat hunting as an "enhanced security requirement."

Ask your provider about the difference between ongoing threat monitoring across all of its customers and proactive, bespoke threat hunting tailored to your organization.

6 How do you ensure the transparency of your service delivery and processes?

Your MDR partner should be providing you with a nominated team, acting as the point of contact for both strategic security advice and service-related queries. This will enable you to stay informed about the overall service quality as well as the provider's view of your security posture. MDR providers should offer a service portal that acts as a unified view of alerts and incident activity across your digital estate, along with self-service features for tracking service requests, KPI-driven reporting and defined response playbooks.

Key Takeaways

Choosing an MDR partner begins with objectively defining what you want to achieve from the service. What gaps exist in your security program and skill sets? What outcomes are you hoping to realize?

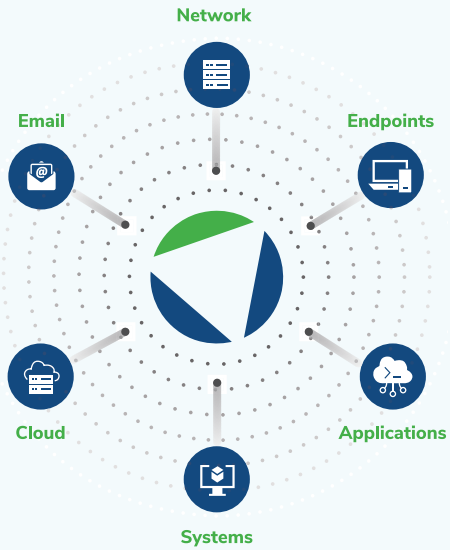
Having defined these expectations, you can begin assessing potential MDR partners. The questions above will help you distinguish candidates by type, service maturity, expected outcomes, global footprint, and much more. Once you have a short list, consider intangibles, such as the vendor's reputation in the industry, ancillary and related services, and degree of alignment with your business culture.

Kroll leverages its unrivaled IR experience and frontline intelligence to run a round-the-clock global MDR service providing active response using seasoned incident responders, not just monitoring analysts. In 2014, Redscan, now a part of Kroll, became one of the first full-service MDR providers, pioneering the approach of layering custom detection analytics and hunting procedures over the security tooling (EDR, SIEM, NDR etc.), investigating the threats and responding on behalf of the customer. Today, Kroll Responder is now one of the only solutions in the market that delivers MDR with what we call "Complete Response".

At Kroll, we believe the 'Response' aspect of MDR shouldn't leave you hanging. Our response goes as far as you need it to, closing the gap between merely containing the threat to actively removing it across all affected systems and quickly understanding the root cause, to ensure it doesn't happen again. Our Responder MDR service is backed by the same Kroll IR experts that handle thousands of high-profile breach investigations annually. We extend that service to our customers, which means they get the value of remote digital forensics and incident response without the additional cost.

Learn more about **Kroll Responder managed detection and response**

Kroll Responder at Work



1

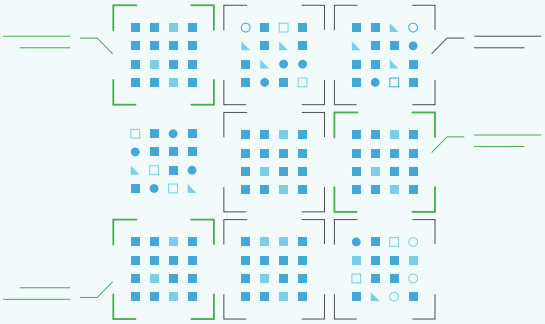
Telemetry & Intelligence

Telemetry is collected from across your networks, endpoints, and cloud environments, analysed using the latest machine learning and behavioural detection engines, then enriched with the latest threat intelligence.

2

Detection & Enrichment

Detections are correlated and then grouped together by common attributes to create 'cases' – providing a more complete overview of security events.



3

Investigation & Hunting

Cases are triaged by our 24/7 Security Operations experts, using initial findings to hunt deeper before escalating those requiring additional attention to Kroll's elite incident response team.

4

Response & Containment

Automated playbooks and human intelligence provide robust response and remediation capabilities around the clock to disrupt, contain and eradicate threats before they cause costly damages.

KROLL

TALK TO A KROLL EXPERT TODAY

North America
T: 877 300 6816

UK
T: 808 101 2168

Hong Kong
T: 800 908 015

Additional hotlines at:
kroll.com/hotlines

Singapore
T: 800 101 3633

Australia
T: 1800 870 399

Brazil
T: 0800 761 2318

Or via email:
CyberResponse@kroll.com

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.