Fortifying Cyber Defenses with MDR

A definitive guide to critical managed detection and response capabilities

MANDIANT®
NOW PART OF Google Cloud

EBOOK

Introduction

Detection and response are critical cyber defense functions for organizations of all sizes and industries However, budget and resource constraints often limit their capabilities, which puts them at greater risk.

To help organizations reduce risk, a managed detection and response (MDR) service provider can:

- Supplement internal capabilities,
- Fill critical gaps, or
- Provide a complete end-to-end detection and response function.

But not all MDR providers are equal, and many do not offer the required skills and expertise to ensure organizations are well-protected against the threats that matter most.

According to Gartner, an MDR provider is "a breed of detection and response service, one that helps you accelerate maturity by being turnkey, one that brings expertise, evolution and development. Something that can be part of a wider detection and response strategy or stand up on its own. MDR provides outcomes that reduce cyber security risk in your organization." [1]

To optimize their cyber defense capabilities, security leaders and teams must ask the right questions to confidently evaluate MDR providers:

- What is the mix of threat intelligence, detection capabilities, threat hunting, investigation, response actions and customer communication the MDR provider offers?
- How broad, deep, and useful are the provider's intelligence and human expertise?
- How consistent and scalable are their offerings?
- Are they available through software-as-a-service (SaaS) offerings or as fully managed services?

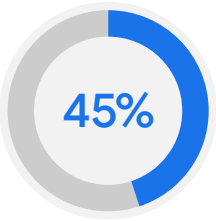
1 Gartner (June 11, 2020). Is MDR just Another Acronym that means Managed Security?

Common Challenges Facing SOC Teams

High Numbers of False Positives…

… limit an organization's ability to detect intrusions quickly.

According to IDC, 45% of alerts are false positives, and 35% of security analysts report that they ignore alerts if the queue is too full.[2] Security engineers are often forced to manually stitch together data from disparate systems, taking time away from trying to make sense of data and identify malicious behavior. Without advanced automation and analytics technologies, organizations cannot effectively scale data collection, processing and analysis.

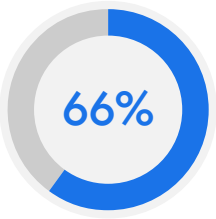


of alerts are false positives

Lack of Timely, Relevant Intelligence…

… required to understand the most critical threats at any given time.

According to Forrester, organizations subscribe to an average of 7.5 threat intelligence feeds.[3] Furthermore, the recent SANS CTI Survey reports that 66.5% of organizations disseminate cyber threat intelligence internally through spreadsheets, slides and documents.[4] However, organizations must operationalize that intelligence to ensure that the right threat details are seen by the right people. Otherwise, it becomes harder to effectively monitor, triage and prioritize alerts. It also becomes more difficult to investigate and reconstruct events to determine the scope of a breach and to find adversaries that have evaded technical controls.



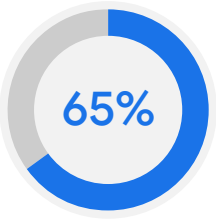
of organizations disseminate threat intelligence through spreadsheets

Shortage of Cyber Security Skills…

… puts organizations at a disadvantage.

The international cyber security organization (ISC)² reports in its 2021 Cybersecurity Workforce Study that the global cyber security workforce needs to grow 65% to effectively defend organizations' critical assets.[5] Skills such as cyber threat hunting require expertise and resources that few individual organizations can maintain on their own without proper training programs. This makes it hard to find, train and retain security analysts with essential skillsets.

A properly equipped and empowered MDR can address these challenges.



growth in global workforce needed to effectively defend critical assets

2 IDC (January 2021). The Voice of the Analysts.
3 Forrester (March 23, 2021). The Forrester Wave™: External Threat Intelligence Services, Q1, 2021.
4 SANS (January 2021). 2021 SANS Cyber Threat Intelligence (CTI) Survey.
5 (ISC)₂ (2021). Cybersecurity Workforce Study, 2021.

Reducing Mean-Time-to-Detect with MDR

Mean-time-to-detection (MTTD) is a measurement of how long an attacker "dwells" in a network before being detected. Mandiant research shows that the global median dwell time across organizations decreased from 56 days in 2019 to 24 days in 2020[6]—which, while trending in the right direction, is still far too long.

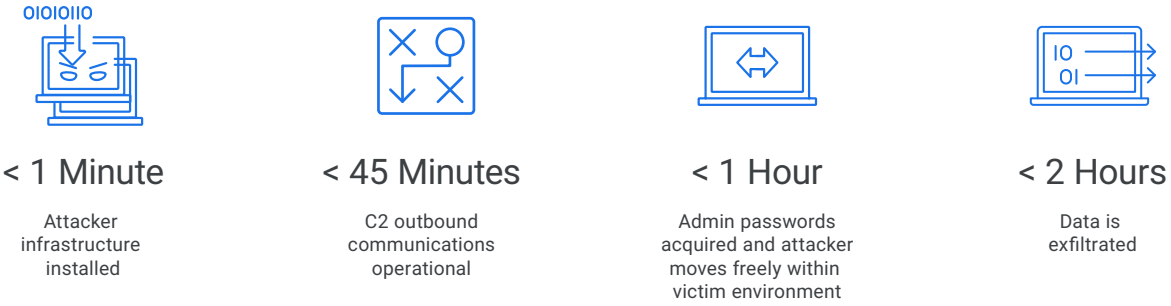


FIGURE. What can happen in the first two hours of dwell time.

An MDR provider with quality threat intelligence and deep threat hunting expertise can significantly reduce an organization's MTTD and minimize the business impact of a breach. Better service capabilities enable security experts to focus on threats that matter and root out emerging attacks.

Reduced detection and response times represent the ability of security teams to reduce risk and are one measure of cyber security maturity.

6 Mandiant (2021). M-Trends 2021.

Critical Components of Effective Detection and Response

The most effective approach to MDR is a combination of technology and expertise. Industry research and analyst perspectives support this notion and highlight several components for effective detection and response: threat intelligence, threat detection, threat hunting, investigations, remediation and response and a solid customer support model.

Threat Intelligence

The Intelligence function feeds directly into every other cyber defense function, from providing indicators of compromise (IOCs) that can be used to develop use cases within the Detect function, providing guidance to build mission-critical Hunt function activities and developing adversary emulation to test security controls.

Threat Detection

Threat detection includes enhancing contextualization and providing detection analytics through automation and machine learning. As a result, organizations gain a clearer picture of threats to the environment and a more comprehensive view of the environment itself.

Threat Hunting

Threat hunting is a proactive cyber defense activity used to identify active threats within the environment. It includes advanced capabilities such as insider threat identification, deception tactics and threat modeling exercises.

Investigation

Investigation blends threat intelligence, automation and correlation with human analytical skills and experience. The combination of analyst-driven investigations with correlated event data gathered by automated defense technologies ensures that providers can deliver fast, scalable response activities.

Remediation and Response

Remediation and response focuses on returning business to normal after a compromise. A response team's actions must match the scope of the attack. Capabilities such as containment should be augmented with automation and orchestration to drive faster remediation of incidents and minimize impact.

Customer Support Model

An MDR provider should serve as an organization's cyber defense partner. The customer support function should understand the organization's needs, act as an advisor and contributor to their SOC team and offer a dedicated expert or team of on-demand experts.

Critical Components of Effective Detection and Response

Expert Threat Intelligence: Gain the Upper Hand in the Fight Against Cyber Attacks

Effective threat Intelligence, the core of all detection and response activities, depends on two factors:

- Intelligence integration
- Credibility and quality of sources

Building the Foundation of Detection and Response through Integration

Expert intelligence is best activated and used at a foundational level to guide security monitoring. It provides visibility into the cyber threats most relevant to the organization and prioritizes the detection of those threats. Threat intelligence should be integrated across tools and processes for:

Precise threat hunting
Using data on active advanced persistent threat (APT) groups and current, relevant attacks, threat hunting teams can identify both active compromises and evidence of past (undetected) incidents.

Activity prioritization
Threat intelligence helps IT and security groups determine patch and upgrade priorities based on the potential impact of the threats most likely to target the organization.

Informed monitoring
Security engineers who know where to look, what to monitor for and when to alert security analysts of activities tied to active APT groups.

Refined security strategy
As adversary targets and tactics continually shift, intelligence empowers security operations groups to update their strategy and maintain their security posture.

Confident, capable incident response
Intelligence bolsters incident response teams' ability to scope and rapidly contain breaches and prevent repeat attacks.

Up-to-date security validation
Effective validation efforts incorporate the latest adversary tactics, techniques and procedures (TTPs) to ensure controls and operations can stop an attack or reduce its impact.

Importance of Varied, Credible Threat Intelligence Sources

A quality MDR vendor should have a broad set of intelligence sources operationalized into comprehensive, actor-specific playbooks that inform detection, investigation and response activities. Their sources should include:

Breach intelligence from real-world incident response engagements

Adversary intelligence obtained by expert researchers

Machine intelligence from deployed security products

Operational intelligence from security operations centers managed by the service provider

Questions to Ask MDR Providers:

- What intelligence sources do you use beyond simple data feeds?
- Can your threat intelligence reveal who is targeting our industry? And how?
- How well do you align threat intelligence to relevant industry attack frameworks such as MITRE ATT&CK and NIST?
- Is your threat intelligence completely transparent and available to your customers?

Critical Components of Effective Detection and Response

Detection: Accelerate, and Augment Threat Visibility through Automated Technologies

Extended detection and response (XDR) provides visibility into telemetries across an organization. However, it greatly increases the amount of data monitored and tends to further stress overextended, resource-constrained security operations—even when offered as a managed service. An advanced technology platform that can enable the growing volume of data to be processed and analyzed at scale.

To cover all possible threat vectors, XDR can include telemetry collection: alerts, events and logs from endpoint, network, cloud and OT/IoT/IIoT devices, and more. Again, while valuable, this can also lead to higher volumes of data, creating further challenges. Automation and machine learning can help normalize, enrich, and analyze data coming in from multiple sources.

Automated defense technologies offer several detection benefits:

- Minimize the risk of human bias in the monitoring and triage process
- Accelerate detection at scale across all integrated technologies to enable rapid response
- Maintain correctly prioritized customer interactions with transparent communication

Questions to Ask MDR Providers:

- How many sources of telemetry are ingested (for example, endpoint, network, cloud, email, OT/IoT/IIoT)?
- Can you work with customers' technology stacks, or do you use a proprietary stack?
- Do you regularly update and maintain your data science models?
- Do you use cyber threat intelligence to help automate detection or enhance remediation

Single- or Multi-Vendor Option?

- **Single vendor:** Requires deployment of its proprietary technology and point solutions
- **Multi-vendor**: Supports the customer's existing technology and is equipped to deliver detection and response across multiple telemetries

Critical Components of Effective Detection and Response

Threat Hunting: Stop Attacks before Impact with Intelligence, Human Expertise and Automation

An example is SUNBURST, a covert backdoor that was distributed by a software update as a result of a supply chain attack on one organization's widely used IT management software. The adversary used multiple techniques to evade detection across the entire attack lifecycle, enabling them to operate within both public and private organizations around the world for over 15 months.

Stealthy attacks force mature MDR providers to go beyond sweeping the environment against new indicators of compromise (IOCs) to a more continuous, expert-led function. More accomplished providers adopt both automated and human-led hunting strategies to adapt to changes in the threat landscape and attacker behavior. This approach allows MDR providers to systematically reduce an organization's threat exposure through proactive detection and enables them to identify security control gaps.

Threat hunting, a differentiating facet among MDR service providers, should be reviewed with these traits in mind:

- **Flexible:** Demonstrable adaptability to adversaries' changing TTPs.
- **Scalable:** Automation of data collection and preparation to improve effectiveness and efficiency.
- **Intuitive:** Expert threat hunters in place to proactively search for covert signs of active or unknown compromises across multiple telemetries including endpoint, network, cloud and OT/IoT/IIoT.
- **Industry framework-compatible:** Mapping to frameworks such as MITRE ATT&CK enables analysts to see which controls may have been subverted and take decisive action based on attacker motives even when technology detections fail or attackers use new or unknown behaviors.

Questions to Ask MDR Providers:

- How do you define threat hunting and how do you find unknowns in the environment?
- How do you hunt for threats beyond searching for common IOCs?
- How often do you hunt for threats?
- Are your threat hunting capabilities human-led or automated, or a combination of the two?
- Which threat vectors are covered by your hunting efforts?

Critical Components of Effective Detection and Response

Investigation: Lead with Intelligence for Rapid, Scalable Response

Top-tier providers have experts conduct comprehensive investigations using an intelligence-led approach. They combine analyst-driven investigations with correlated event data gathered by automated defense technologies to deliver fast, scalable response activities. Providers should make analyst actions and findings directly available to customers.

Investigations should be conducted through a comprehensive, iterative process that scopes incidents well enough for providers to answer:

- What happened?
- How did it happen?
- What do we know about the actors behind this activity?
- What should be done to respond to this activity?
- What should be done to prevent it from happening again?

An MDR provider's investigation capabilities are distinguished when they:

- **Continually update investigative reports:** The provider should deliver context needed to fully understand the scope of the attack, help assess risk and impact and recommend remediation strategies.
- **Communicate transparently:** The provider must render and communicate an in-depth understanding of the TTPs based on reliable threat intelligence and their expert analysis.
- **Produce comprehensive investigative reports:** The provider should report findings that include a timeline of attacker behavior supplemented with evidence, an interpretation of attacker activities based on threat research and data analysis and attributed threat intelligence for necessary context.

The most robust providers offer highly specialized services such as:

- Malware analysis
- Forensic analysis
- Intelligence gathering
- Incident response

Questions to Ask MDR Providers:

- What type of information do you provide beyond reporting alerts?
- How effectively do your reports convey the context around likely threats and correlated activity?
- What sort of evidence do you provide to establish the identity, methodology and attack timeline of suspected threat actors?
- How do you scale detection and customize response actions for individual customers?

Critical Components of Effective Detection and Response

Focused, Definitive Response: Remediate the Specific Attack to Reduce Its Impact

Response and remediation services are critical to minimizing attack impacts and rapidly returning operations to normal. Reliable MDR providers should offer a broad range of response capabilities and adjust actions based on the type of attacks their customers experience. They must assure their customers that investigations are thorough and assess the full extent of a compromise.

A full-service MDR provider should offer these response and remediation capabilities:

Containment

Appropriate actions must be taken to disrupt the attacker and limit their access to the environment. Remote containment is dependent on each client organization's endpoint security tools.

Eradication/Remediation

Understanding the full extent of the compromise is critical. The MDR provider may have to work with the customer to remove any residual attack infrastructure and restore secured system configurations.

Enhancement/Fortification

With information from the investigation, MDR providers can recommend defense strategies to prevent or withstand future attacks with the same TTPs.

Questions to Ask MDR Providers:

- What range of response services do you provide?
- What types of remediation do you recommend beyond "wiping the box"?
- How will your analysts collaborate with our internal team?
- Which response actions are taken by your team, and which are our responsibility?
- What incident response capabilities do you offer to extend your base service?

Critical Components of Effective Detection and Response

Customer Support: Gain Confidence through a Reliable, Flexible Partnership

Security professionals are looking for more than an MDR service provider; they want a true cyber security partner. Their ideal MDR partner offers a dedicated customer support team that understands their unique SOC environment and amplifies the capabilities of their security team, both as advisor and contributor. Organizations also need flexibility and on-demand access to a dedicated expert or a pool of experts who augment specific functions.

31.5% of survey respondents consider "Excellent Customer Support" an important factor when evaluating MSSP and MDR providers.[7]

IDC'S MSSP AND MDR SURVEY (MAY 2020)

An MDR provider that offers reliable customer support delivers unique and differentiated cyber security knowledge and skills to address challenges facing security teams.

MDR providers should deliver:

- Experience across a broad range of technologies such as OT, IoT and cloud.
- Technical experience and specialized services to aid investigations, such as:
  - Malware analysis
  - Forensic analysis
  - Intelligence gathering
  - Onsite incident response

7 IDC (September 2020). IDC Marketscape: Worldwide Managed Security Services 2020 Vendor Assessment.

The customer support models of top tier MDR providers include:

- **Knowledge and skills drawn from years of experience:** Experience refers to direct involvement with cyber attacks and the aftermath of a compromise, which may involve response, remediation and advanced forensic analysis. Specialized support team skills should include:
  - SOC expertise
  - Deep analysis capability to fully understand the adversary
  - Forensics and malware reverse engineering
  - Threat hunting
  - IR expertise
- **Transparency through accessibility:** Attacks don't sleep, which means that the CISO or SOC manager often feel like they can't either. Data connectivity through APIs, full visibility into environments and 24x7 access to world-class experts adds tremendous value to security operations and the MDR-SOC partnership.
- **Ability to use automation and machine learning:** These capabilities enable accelerated detection and swift response. MDR providers that can quickly operationalize and scale the latest intelligence and attacker TTPs to protect customers stand out.

Questions to Ask MDR Providers:

- What is your customer support model?
- What does collaboration between our teams look like?
- What activities are taken to enhance our overall security posture? How frequently?
- What options are available to further enhance security (i.e., assessments, attack simulation, validation)?

Comprehensive MDR Coverage with Mandiant Managed Defense

The combined power of intelligence, expertise and automation in Mandiant Managed Defense delivers unique, differentiated and high-demand cyber security capabilities, knowledge and skills to SOC managers and their security teams. It minimizes many critical SOC challenges with:

- A dedicated onboarding team to ensure smooth implementation from day one
- A dedicated Managed Defense consultant who becomes part of the client's security team and acts as their conduit and incident handler
- An early knowledge advantage through world-leading threat intelligence that delivers advanced detections and notifications of ongoing adversary activity from the latest frontline experiences
- The ability to integrate disparate data types with Mandiant technology and gain a cohesive, single vantage point to secure their environment
- A combination of skilled threat hunting and proprietary Mandiant intelligence to help discover and identify headline-worthy threats, adversaries and vulnerabilities.

The full benefits of Mandiant Managed Defense extend to the C-Suite. Executive leadership gains peace of mind, knowing that their SOC managers and security teams understand the threats that matter to their organization. They become more confident in their ability to secure and defend their organization, critical assets and people.

Google Cloud

For more information visit cloud.google.com
MD-EXT-EB-US-EN-000435-02