RAPID7

SERVICE OVERVIEW

Managed Detection and Response

Stop nefarious activity and accelerate your security maturity with hands-on, 24/7/365 monitoring, threat hunting, and tailored security guidance.

TABLE OF CONTENTS

Introduction to MDR

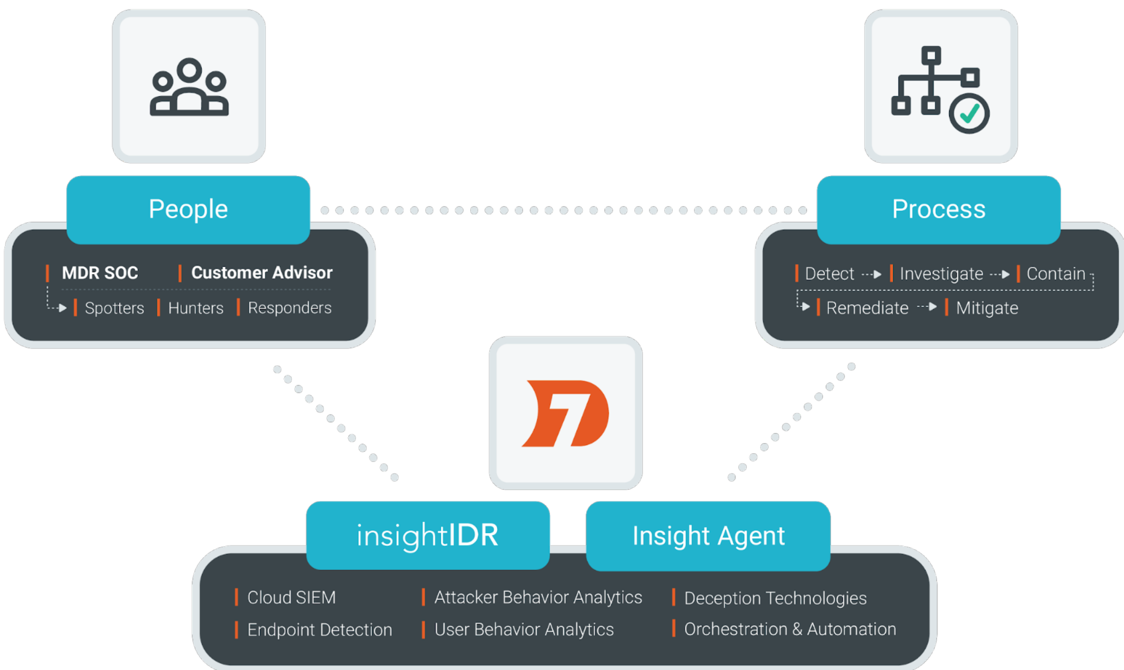
Rapid7's Managed Detection and Response (MDR) service offers a combination of expertise and technology to detect dynamic threats quickly across your entire ecosystem. Our MDR service provides hands-on, 24x7x365 threat monitoring and hunting customized to your business profile, powered by Rapid7's purpose-built technology stack. This includes the Rapid7 Insight cloud and Threat Intelligence infrastructure, in addition to our Security Operations Center (SOC) experts who work to help you remediate risks quickly, so you can accelerate your security maturity.

This document outlines Rapid7's MDR service.

Rapid7's MDR Approach

At its core, Rapid7's MDR service is a strategic partnership that allows your business to strengthen your security program maturity as it relates to threat detection and response. Rapid7 MDR extends your existing team to detect, investigate, report, and recommend response actions to threats in your network. We do this through 24x7x365 monitoring by a team of security experts, leveraging proven cloud SIEM technology, cutting-edge endpoint technology, and world-leading threat intelligence to stay ahead of attackers. When engaging with this service, you'll gain a true security partner who can provide the mentorship and guidance necessary to simplify the complexities of cybersecurity and help you securely advance your business.

Our focus on advancing your current maturity level in incident detection and response layers our industry experts, workflow processes, and technology to implement our three-pronged approach:



People

Your environment is monitored 24x7x365 by world-class SOC analysts, each with years of experience building detection and response programs, and hunting for and validating threats.

SOC Analysts leverage specialized toolsets, malware analysis, tradecraft, and forward-looking collaboration with Rapid7's Threat Intelligence researchers to make detection and remediation of threats possible. The Threat Intelligence researchers are constantly monitoring our MDR customer environments, as well as the global threat landscape to enhance the MDR team's detection methodologies.

These teams are augmented by your Customer Advisor (CA), who is your interface with the Rapid7 SOC and Threat Intelligence teams. Your CA will provide suggestions on managing your technical environment while offering tailored guidance and recommendations specific for your business to accelerate your security maturity.

Technology

The Rapid7 Managed Detection and Response service is powered by the Rapid7 Insight cloud, with endpoint data collected from the Insight Agent, a lightweight yet powerful software you can install on any asset—whether in the cloud or on-premises—to collect endpoint data from critical and remote assets across your IT environment.

The data passed to the analyst team by the Insight Agent allows the MDR analysts to get as close to the attacker as possible and perform endpoint investigations and threat hunts with system-level visibility. Combined with our Gartner-ranked cloud SIEM, InsightIDR, this endpoint data is parsed against real-time threat intelligence insights from the Rapid7 customer base and sophisticated behavioral analytics (tuned with an in-depth understanding of your business) to uncover threats across your internal network and cloud services.

Additionally, InsightIDR allows the MDR SOC team to integrate feeds from your existing security infrastructure, giving the Rapid7 MDR team even greater visibility into possible threats across your environment. As a customer of Rapid7 MDR, you'll have full access to InsightIDR, giving you visibility into the product and investigations and the ability to learn from the tool.

Process

Our expertise and technology reveals its true power when a threat is detected. Our MDR SOC analyst team uses a series of detection methodologies to validate each threat by gathering context related to the alert from your endpoints and logs to assess severity. Then we'll only report the true, real threats and suspicious lateral movement, and provide prioritized recommendations (e.g. containment, remediation, and mitigation actions) for your team in the form of a Findings Report. The result: MDR customers quickly identify and respond to attacker activity without wasting time investigating a mountain of false alerts.

What You Can Expect

Rapid7's approach ensures that there is full visibility and an organized response to incidents that occur in your environment. This encompasses four areas of service delivery with Rapid7 MDR:

Incident Detection & Validation

- 24/7/365 Monitoring
- Proactive Threat Hunting
- Initial Compromise Assessment
- Investigations of Threats and Alerts
- Alert Validation

Technology Access

- Full Access to InsightIDR Capabilities
  - SIEM
  - UBA
  - ABA
  - EDR
  - Deception Technologies
- Deployment Assistance Included
- No Additional Data Charges

White Glove Service

- Named Customer Advisor
- Threat Intelligence Team
- Custom Threat Profile
- As-it-happens Findings Reports
- Monthly Hunt Reports
- Monthly State of Service Reports
- As-it-happens Proactive Threat Reports

Incident Response & Escalations

- Process for Containment, Remediation and Mitigation of Threats
- Two Incident Escalations Included
- Slas for Threat Notification

Your Advantages With Rapid7 MDR

Rapid7's MDR offering goes far beyond the capabilities of traditional Managed Security Service Providers (MSSPs), who often provide incomplete technology solutions without the required expertise to manage the systems and provide guidance. Our belief in delivering the Rapid7 MDR service is to be more than a vendor, and for our team to do more than just alert you of threats. Counter to the Rapid7 MDR offering, the typical MSSP rarely offers threat hunting, and the experience is an impersonal one-size-fits-all approach that merely focuses on detection of malware and sending sterile tickets rather than a strict focus on advancing your security program. For more detailed analysis, please review our Rapid7 MDR vs. MSSP comparison brief.

Rapid7's Managed Detection and Response (MDR) service provides customers with five key advantages:

1. Improved Security Maturity

Rapid7 MDR is positioned to meet our customers at any level of security maturity and help accelerate that maturity, not just manage a SIEM. The team—from SOC analysts to your Customer Advisor—takes the time to truly understand your business processes, environment, and industry so they can provide customized guidance at each interaction point with the MDR service. This includes tailored reporting and recommendations, with remediation and mitigation strategies that align your investment in MDR with long-term security improvement across all 20 CIS critical controls. We go above simply looking at detection and response, with advice and mentorship from your Customer Advisor.

2. Powerful Agent and SIEM Technology

MDR is powered by the Rapid7 Insight cloud, with data fed from the Insight Agent to perform endpoint investigations and hunt for threats in your environment. This lightweight Agent unifies data collection for the MDR team to effectively view and correlate endpoint data, including: detailed asset information, Windows registry information, file version and package information, running processes, authentication information, local security and event logs, and more.

This is data is encrypted at rest and in transit as it's sent to InsightIDR for log correlation and investigation. Combined, the Insight Agent and InsightIDR provide the MDR team system-level visibility to spot real-time detections on the endpoint—the closest point to the attacker. As a customer of the MDR service, your team will have direct access to your instance of InsightIDR, giving you full transparency into our service and the ability to interact with the MDR team. Customers and their teams now have a single provider for both MDR services and SIEM/EDR technology.

3. Leading Threat Intelligence

Customer defenses leverage Rapid7's primary threat intelligence on attacker behaviors and common indicators of compromise, all powered by Rapid7's Managed Threat Intelligence Engine, cybersecurity research projects, vulnerability disclosures, insights from our customer endpoints, and Rapid7 SecOps Services engagements. In addition, Rapid7 leverages top third-party threat intelligence from security partners in the community, most notably Rapid7's involvement as an Affiliate member of the Cyber Threat Alliance (CTA) with Board and Committee seats.

4. World-Class Managed Services Team

The global MDR SOC teams are composed of security experts with unparalleled experience—both red team and blue team—with an assigned, primary high-tier analyst who becomes a subject matter expert in your user behavior, endpoints, and networks. Your analyst uses this in-depth knowledge of attacker tools, tactics, and procedures to catch malicious activity early in the attack lifecycle and validate each potential threat. Each of our SOC analysts acts as an extension of your security team and tailors the MDR service specifically to your industry and your business. This includes threat hunting, validation of threats, and guidance (e.g. containment, remediation, and mitigation recommendations) for only true threats.

5. Included Incident Escalation

Rapid7 offers two (2) Incident Escalations per year, giving MDR customers the ability to engage skilled personnel rapidly in the event of a compromise.

MDR Customer Engagement Model

The Rapid7 MDR team consists of multiple functional groups working together to ensure you receive world-class incident detection and response, providing 24/7 monitoring, unsurpassed service, and contextualized reporting that delivers real value.

We pride ourselves on becoming a true extension of customer teams through attentive service, visibility into our backend systems, and by providing a named resource (your Customer Advisor) whom you can reach out to for all things related to security.

Customer Advisor

Your **Customer Advisor (CA)** acts as a trusted advisor/ consultant. He or she should be considered an expert in your environment and a knowledgeable resource who can help your organization advance more securely. Customers Advisors will help your security team jointly manage the deployed cloud instance of InsightIDR while contextualizing alerts, investigations, and analysis.

Your CA is your main point of contact for the Rapid7 MDR service. This person has deep knowledge of your organization and works with you as a strategic security partner, from initial technology deployment through incident remediation. Having risen through the ranks of technical service delivery and customer success, each CA brings domain expertise, technical acumen, and white glove customer service. As such, customers often leverage their CAs as security experts to ensure their CISOs and board members are prepared to address any changes in the threat landscape.

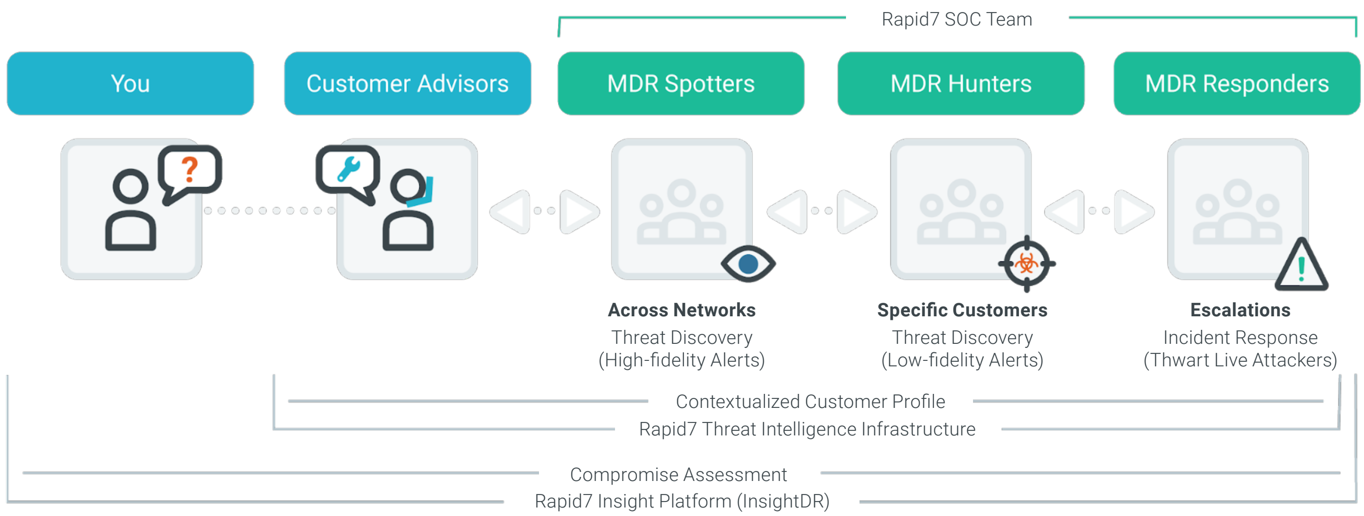
Throughout the service, your CA will communicate with you frequently via your preferred communication method and cadence, though never less than once a month. Typical communications provide updates on service delivery, walk you through Findings Reports, and assist you with reaching your security goals. Alternatively, you can proactively reach out to your named CA, or call the Customer Advisor hotline, whenever you'd like to chat about the service or your environment.

As part of the monthly check-in, Rapid7 will provide metrics and context surrounding analysis activities performed by the MDR analysts, technology health, and findings summaries. These reports serve as an at-a-glance overview of MDR activities. Additionally, the CA provides context for your MDR service and what any reports or threat intelligence insights mean for you and your business.

MDR SOC

Our SOC implements a three-tiered approach to ensure we have coverage for high- and low-fidelity alerts and can identify unknown threats through hunts in your environment. Together, the MDR SOC teams of world-class analysts maintain 24/7/365 vigilance of your network, from alert validation through in-depth forensics and malware analysis of your network and users. Our combination of these roles provides optimal coverage for all threats and attacker challenges.

- **Spotters** triage alerts across all customers to validate and report on high-fidelity indicators generated from InsightIDR (SIEM, EDR, UBA, ABA, deception technology), as well as the SOC's proprietary tools. Spotters typically monitor for simple threat intelligence matches and Attacker Behavior Analytics. Spotters typically have 2–4 years of experience validating and hunting for threats.
- **Hunters** are assigned to individual customer clusters to ensure a deep understanding of each of their customers' environments and threat profiles. Hunters are responsible for validating and reporting on lower-fidelity, technology-generated indicators like UBA and ABA alerts, as well as conducting monthly threat hunts. Hunters typically have 4–7 years of experience validating and hunting for threats.
- **Responders** support threat monitoring, hunting, and are responsible for leading incident escalations by providing advanced remediation and mitigation recommendations gleaned from deep analysis of evidence and malware. Additionally, these individuals assist in developing customer-specific detections (e.g. specific types of activities happening in the network) and work alongside our Threat Intelligence team to write new threat detections. Responders have 7+ years of cybersecurity experience, including incident response.



Threat Intelligence Team

Rapid7's **Threat Intelligence team** supports the SOC and CAs with analysis and new detections. Our MDR Threat Intelligence team are the vigilant researchers working on your behalf to identify new attacker trends before you are impacted. Our Threat Intelligence analysts provide customers and SOC analysts with the surrounding context needed to defend against threats with new detection mechanisms for vulnerability exploits and attack campaigns.

Additional Members of Rapid7's Team

A unique value point for Rapid7's MDR service is the strength and expertise of our employees who work with your organization to advance your security maturity. Throughout your service, you may come in contact with many of our excellent team members, including:

- **Account Executives:** Your introductory point of contact for all presale needs. The Account Executive takes the time to understand your business challenges, explains how our technology works to solve them, and proposes solutions to help accelerate your security maturity.
- **Project Managers:** The Deployment Project Manager leads MDR deployment coordination between Rapid7 and you, the customer. This person is responsible for ensuring a seamless experience during the deployment phase and can address any issues that arise during the deployment process.
- **Deployment Consultant:** Rapid7's InsightIDR solution specialist who is responsible for implementing and configuring the InsightIDR solution and for confirming configuration of all other related technology (e.g. log sources, event sources, collectors, etc.).
- **Customer Success Manager (CSM):** A Rapid7 CSM is assigned to your account for the entirety of your relationship with Rapid7. The CSM is an internal advocate who ensures your team's success by facilitating the best use of Rapid7 solutions and driving resolution on technology-related issues and requirements. This person is also your point of contact for adopting new Rapid7 solutions or expanding your solution coverage.
- **Security Operations Center (SOC) Manager:** Rapid7 SOC managers oversee and manage Rapid7 SOC operations, analyst teams, and MDR's internal infrastructure to ensure your ongoing success and coverage of your environment.

MDR Technology Overview

The Rapid7 MDR service leverages our InsightIDR solution to provide comprehensive protection against intruders in your internal network, devices, and cloud services. Additionally, the MDR SOC integrates event sources from your existing security infrastructure, granting the Rapid7 MDR team greater visibility into threats across your environment.

Customer-Deployed Software and Configuration

Insight Agent

The universal Insight Agent is lightweight software you can install on any asset—whether in the cloud or on-premises—to automatically collect data from endpoints (even those from remote locations that rarely join the corporate network) to enable the Rapid7 MDR team to have real-time visibility to identify malicious activity on your endpoints.

The endpoint agent enables our analysts and behavioral analytics tools to get as close as possible to the attacker, with the complete set of evidence needed to assess a threat. Each agent can be leveraged to perform on-demand containment actions to quarantine an endpoint asset or kill a process. We recommend deploying the Insight Agent on all endpoints, but require deployment on at least 80% of applicable assets using your existing software management processes in order to deliver service.

Rapid7 assigns deployment resources to work with you for the initial deployment of the Rapid7 MDR technology stack and ensure your event sources are configured for optimal coverage.

Insight Collector

The Insight Collector is responsible for receiving log data and agent data from your environment. All collected data is compressed and encrypted before being forwarded to the Insight cloud. The Collector also acts as a proxy for endpoint agents to reduce bandwidth constraints and increase endpoint scalability.

InsightIDR

Rapid7 MDR provides full access to jointly manage your InsightIDR instance, including access to functionality such as investigations, log search, dashboard cards, and reporting. Your team can also establish custom alerts in InsightIDR. Please note, however, that Rapid7 will be unable to act on these custom alerts beyond the monitoring that MDR typically covers. Your team should not modify or close out alerts within InsightIDR without first contacting your CA to ensure the Rapid7 MDR team maintains complete visibility.

InsightIDR also ingests data from multiple event sources, each configured in InsightIDR to create a unique log in Log Search. The standard MDR subscription includes 13 months of hot, immediately searchable log data and storage. Longer term retention is fully available to meet your business and compliance needs. Since the Insight architecture runs in the cloud, no external hardware is required for storage.

Event Sources

You are required to connect logs for four foundational event sources to the Insight Collector(s): Active Directory (for Windows assets), DHCP, DNS, and LDAP directory services (or equivalent as agreed upon with Rapid7). Rapid7 will validate connectivity and processing once deployment is complete. Rapid7 will also perform ongoing monitoring to evaluate the health of the technology stack and provide you with notifications when a failure or issue is identified.

Deception Technology (optional)

InsightIDR comes included with honeypots, honey users, honey credentials, and honey files designed to identify malicious behaviors using fake assets, users, credentials in memory, or files.

Rapid7 Cloud Technology Architecture and Capabilities

Insight Cloud

Responsible for all log management, data processing, enrichment, and storage of customer data aggregated from each endpoint with the Insight Agent. Each customer instance on the Insight cloud is isolated from other instances.

InsightIDR

Rapid7's purpose-built cloud SIEM for incident detection and response combines real-time threat intelligence insights with a deep understanding of your environment and sophisticated behavior analytics to identify threats. InsightIDR aggregates endpoint behavior, user behavior, and log history in a single solution offering a comprehensive view of the core technical environment.

Rapid7 Threat Intelligence Infrastructure

Primary Rapid7-developed intelligence paired with additional third-party sources to enrich the attack detection and response processes in near real time. This intelligence is fed back into the InsightIDR solution to update the behavioral analytics and detections within the product. A full review of Rapid7's Threat Intelligence infrastructure can be found here.

Services Workflow and Process

Rapid7's Managed Detection and Response service engagement is provided in four phases:

1. Detection

Rapid7 MDR leverages pre-built detections in InsightIDR combined with our threat intelligence engine and proactive threat hunting to identify both known and unknown threats before they can cause material impact. See all detection methodologies.

Rapid7 InsightIDR, in turn, leverages thousands of pre-built detections to identify intruder activity, cutting down false positives and enabling analysts to only alert you to true threats.

Additionally, InsightIDR baselines all users and actions to augment pre-defined rules to better detect anomalous and concerning activity. These behavior analytics detections are bolstered with:

Intruder traps

Honeypots, honey users, and honey credentials—built alongside our industry-leading offensive security/hacking team (pen testers) and knowledge from the Metasploit Community—to understand how best to plant traps attackers couldn't resist interacting with.

Explicit attack behavior indicators

InsightIDR uses advanced analytics to detect compromised users/assets that don't require an established baseline of behavior to trigger. One example is the ability to detect spear phishing attempts where the domain has been spoofed (i.e. rapid7.co instead of rapid7.com).

Additional data sources

InsightIDR integrates with your third-party offerings to identify suspicious processes, URLs, hosts, and IPs.

2. Investigation and Validation

Rapid7 validates alerts based on two key factors: attacker intent and observed capability. By combining adversary threat intelligence and knowledge of attack tools, Rapid7 determines the risk and potential impact of each incident and delivers that context in detail.

Each critical alert triggered by InsightIDR is manually triaged by our expert SOC analyst team to ensure validity. Our multi-layered process weeds out benign events, allowing our MDR team to **only report threats that are actually considered malicious** and need direct actions to be taken. This enables our team to produce near 0% false-positive reports and offer actionable guidance with tailored recommendations for your team to take on confirmed threats, including direct containment from within the reports and InsightIDR.

3. Reporting

Once alerts are investigated and verified, our SOC analysts produce a **Findings Report** delivered via the Customer Services Portal (with alerts via email or phone call, per the customer's request). This report is a summary of the incident with detailed evidence of the threat, recommended containment actions, remediation guidance, and mitigation recommendations.

The following additional reports are provided on a one-time, monthly, or an ad-hoc basis based on actions in your environment:

Compromise Assessment (one-time basis upon deployment)

The Compromise Assessment report contains any detected active or historic compromises, potential avenues for future breaches, and remediation and mitigation recommendations.

Service Reports (monthly)

Rapid7 will provide you with metrics and context for analysis activities performed by the MDR analysts, as well as technology health and findings summaries. These reports serve as an at-a-glance overview of MDR activities.

Hunt Reports (monthly)

Hunt Reports contain metrics and findings related to proactive threat hunts using analyzed data from our endpoint metadata and forensics collected by the Insight Agent to identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies.

Threat Intel Report (ad hoc)

A highly targeted analysis that leverages the power of our threat intelligence infrastructure, including Project Heisenberg, Project Sonar, and third-party threat intel with a global footprint to monitor and detect patterns in the wild. Many of these findings could impact your environment; we'll use this information to develop rules to scan your environment, which can be used to perform more real-time asset hardening.

Threat Intel Research Report (ad hoc)

This report is generated by the Threat Intelligence team and can include information on the threat landscape, activity observed in the wild, industry trends, and behavior of specific actors. Often these reports are requested for key briefings, to help prepare teams for potential attacks, and to focus resources on critical risks.

Incident Escalations Reports (in the event of an escalation)

In the event we need to escalate a breach into Incident Escalation, our team keeps you informed of our progress through various reports detailed in phase 4 below.

4. Escalation (On-Demand)

In the event of a validated breach during or after the Compromise Assessment and during the monitoring phase of your contract duration, Rapid7 will contact you with the option to exercise one of your **two (2) Incident Escalations each year** included in your MDR service per your contract, per the service level objectives outlined below:

ESCALATION ACTIVITY	TIME TO ACTION
Time to Begin Escalation	1 hour from initiation of incident escalation
Communications and Updates	Daily updates, along with a daily debrief of the day's investigation results and progress. Substantial findings will be communicated regularly as they are discovered
Incident Escalation Report	Within 2 business days from completion of investigation

An Incident Escalation is a technical process handled by the Managed Services SOC. An Incident Escalation is triggered when a customer is compromised. All investigation activity is conducted remotely and limited to examination of data obtainable by the InsightIDR Insight Agent and platform. Disk forensics are not included as part of an Incident Escalation.

Rapid7 MDR allocates SOC analysts for each Incident Escalation event. Activities performed during an Incident Escalation include:

- **Remote technical analysis and incident scoping:** The MDR team leverages Rapid7 cloud services and the Insight Agent to perform a remote incident investigation and scope attacker activity.
- **Daily reporting:** Rapid7 will provide a daily status report during the duration of the Incident Escalation detailing new findings and recommendations.
- **Final report:** At the conclusion of the Incident Escalation, Rapid7 will provide a final report detailing attacker activity supported by evidence with remediation and mitigation recommendations.

Unlike Incident Response services offered through the Rapid7 Global Services team, the investigation and output for Incident Escalations is done remotely and is limited to examination of data obtained by the Insight Agent and InsightIDR. If your incident falls outside the scope of an Incident Escalation (e.g., pre-dating the start of your MDR service, on-site help is needed, data collected outside of InsightIDR or the Insight Agent), or you wish to escalate more than two (2) incidents per year, Rapid7 will offer Incident Response services at a daily or weekly rate, as applicable per a separate Incident Response Services contract. You can work with your Account Executive to purchase an Incident Response retainer or to engage Rapid7's Incident Response services at the time of the incident for an hourly time and materials rate.

Escalation Protocol

Should a threat require an incident escalation detected by the Rapid7 MDR team, your Customer Advisor will request authorization to execute the incident escalation and additional analysis and reporting will begin. Additionally, in the event your team identifies an internal security incident and requires Rapid7 Incident Escalation assistance, you can contact your CA to begin the Escalation process.

Once you have transitioned to Incident Escalation, the Managed Detection and Response team and Rapid7 Incident Escalation teams will analyze the security incident to identify the scope of compromise, affected systems and accounts, malware used by the attacker, and attacker command and control channels.

A complete workflow outline is available here.

MDR Service Deliverables

Compromise Assessment

Following completion of the Deployment phase, Rapid7 will conduct a Compromise Assessment prior to your MDR service initiation to ensure there is not active malicious activity in your environment or evidence of previous compromise(s). Additionally, the Compromise Assessment allows our SOC analysts to familiarize the Rapid7 team with your security environment and provide actionable recommendations to bolster your security posture, and—if enacted—reduce the risk of future compromise.

The Compromise Assessment appraises your environment to validate evidence of attacker infiltration, active or historic compromises, potential avenues for future breaches, and actionable steps for remediation and mitigation, including:

- **Operating system-specific malware persistence mechanisms and process injection methods:** We review currently running processes, scheduled tasks, and common hiding places to detect anomalies in behavior and communications.
- **Attacker lateral movement:** We apply threat intelligence and User Behavior Analytics to uncover the attacker pathway in real time by analyzing common attacker behaviors, including compromised credentials and ingress from suspicious locations.
- **Common attacker tools:** We find evidence of attacker activity, including modified registry keys or executable files left behind, to validate suspected compromise.
- **Indicators derived from investigations:** We evaluate an exhaustive list of compromise indicators, such as privileged user account anomalies, or suspicious registry changes. InsightIDR detections are constantly updated with IoCs from MDR investigations, Incident Escalations, pen testers, Incident Response team engagements, and Rapid7-hosted events (e.g. Capture the Flag challenges) to improve the product's capabilities to detect anomalous activities.
- **Environment-specific considerations:** We take the time to understand your environment and the relationships between users, hosts, and processes (UHP) to identify any artifacts in the kill chain.

A sample Compromise Assessment Report can be viewed here.

Findings Reports

For each validated incident in your environment, within one (1) hour of validating that incident, Rapid7 will produce a Findings Report containing:

- Investigation details
- Written analysis
- Incident criticality
- Containment recommendations (how to contain the endpoint or user)
- Remediation recommendations (how to resolve this finding)
- Mitigation recommendations (potential ways to prevent future recurrence)

A sample Findings Report can be viewed here.

Monthly Service Reports

On a monthly basis, Rapid7 will provide you with metrics and context for analysis activities performed by the MDR analysts, as well as technology health and findings summaries. These reports serve as an at-a-glance overview of MDR activities. The Customer Advisor will review this monthly recap summary with all stakeholders of MDR on the scheduled monthly call to make recommendations to reduce risk over time.

A sample Monthly Service Report can be viewed here.

Threat Hunt Reports

Each month, Hunter SOC analysts leverage the Rapid7 Insight Agent to collect metadata from multiple locations on your endpoints to proactively identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies. The findings of these proactive threat hunts will uncover unknown threats in your environment and present data from the MDR analyst's forensic acquisition including, but not limited to:

- Evidence of threats from MDR-curated indicators of compromise
- Remote access solutions
- Cloud storage solutions
- Potentially unwanted programs (PUPs)
- Administrator utilities
- PowerShell invocation
- Webshell activity
- Lateral movement
- Ingress authentication
- Server Message Block (SMB) egress
- Potentially vulnerable open ports

A sample Hunt Report can be viewed here.

Threat Intelligence Reports

When Rapid7's Threat Intelligence infrastructure or third-party threat intelligence partners identify new vulnerabilities or detection patterns, the Rapid7 team will publish a detailed analysis of the threat to inform you of the findings. The purpose of this report is to help you better understand the global risk environment. The MDR team leverages this information to develop rules to scan your environment.

A sample Threat Intel Research report can be viewed here.

Incident Escalation Reporting

In addition to the reports provided by Rapid7 for each threat identified in your environment, Rapid7 MDR offers resources to help with up to two (2) incident escalations per year when it's recommended to remove attackers from the environment.

For Incident Escalations, Rapid7 will work with your team to identify a scope specifically tailored to the identified threats, and continue to remotely investigate and provide detailed reports during and at the conclusion of the escalation, including:

- **Remote technical analysis and incident scoping:** Rapid7 will leverage the Insight cloud and the Rapid7 Insight Agent to perform a remote investigation of the incident and scope attacker activity related to the incident.
- **Daily reporting:** Rapid7 will provide a daily status report during the duration of the incident escalation detailing new findings and recommendations.
- **Final report:** At the conclusion of the Incident Escalation investigation, Rapid7 will provide a complete report detailing all attacker activity, supported by evidence and recommendations to remove the threat from your environment.

Service Level Objectives (SLOs)

Alert Priority

The Rapid7 Threat Intelligence team and the MDR SOC work closely together to tune detections and ensure they are as high-fidelity as possible. In addition to tuning alerts to minimize alert noise, Rapid7 also assigns an internal priority for all alerts. This internal priority ensures that the alerts generated by high-fidelity detections and likely to result in a Critical or High criticality are highlighted for expedited SOC triage and investigation.

The Rapid7 MDR SOC triages Critical and High priority alerts in the order of severity to ensure the most pressing threats are identified and that remediation, mitigation, and containment guidance is offered. This allows the team to reduce the likelihood an attacker will gain a foothold and perform malicious activities, while also reducing the burden on our SOC team to investigate benign and false-positive alerts over actual suspicious or malicious events.

Alert Validations

The Rapid7 MDR SOC determines event criticality during the course of an investigation into an identified event. It is not possible to assign criticality before the scope of the event is determined.

Validation is defined as the Rapid7 MDR SOC performing initial triage and investigation to determine, with a high degree of confidence, that the event is non-benign and requires customer communication.

SEVERITY LEVEL	EXAMPLE BEHAVIORS	TIME TO NOTIFICATION	TIME TO FINDINGS REPORT
Critical	An incident created via non-commodity malware deployed via spear phishing, social engineering, zero-day exploitation, or strategic web compromise, specifically targeted towards a target or organization.	Within one (1) hour of validation; Ongoing communications as they become available, but at a minimum, every 4 business hours. Significant findings will be communicated as they are identified.	Within 24 hours upon completion of investigation.
High	An incident created using targeted off-the-shelf software backdoor deployed via spear phishing, social engineering, or strategic web compromise. Planned and targeted, but using common malware.	Within one (1) hour of validation; Ongoing communications as they become available, but at a minimum, every 4 business hours. Significant findings will be communicated as they are identified.	Within 24 hours upon completion of investigation.
Medium	An incident created using common threat malware, typically non-specifically targeted, but rather opportunistic and automatic.	Within eight (8) hours of validation; Ongoing communications as they become available, but at a minimum, every 8 business hours. Significant findings will be communicated as they are identified.	Within 24 hours upon completion of investigation.
Low	An low-risk threat, not capable of remote code execution, credential harvesting, or data theft (e.g. spam email delivering adware).	Within eight (8) hours of validation; Ongoing communications as they become available, but at a minimum, every 8 business hours. Significant findings will occur as they are identified.	Within 24 hours upon completion of investigation.

Insight Cloud Uptime

Rapid7 MDR leverages the Insight cloud, Rapid7's industry-leading security platform, to deliver the MDR service. As such, the uptime availability of this technology reflects that of Rapid7's overall Insight cloud Service Level Agreement.

Customer Advisor Response Times

Your Customer Advisor is held to the following SLOs for notifications and responses to inquiries from your team:

- One (1) hour to proactively reach out to you for validated critical or high severity threats by phone to provide the relevant details quickly while the SOC team generates a Threat Report.
- Two (2) business hours to respond to an urgent request from your team at the discretion of your Customer Advisor.
- One (1) business day to respond to a non-urgent request from your team at the discretion of your Customer Advisor.

Incident Escalation Procedure

In the event of an Incident Escalations, the Rapid7 MDR team will begin the Incident Escalation within one (1) hour once you have approved the escalation.

90 Day Success Plan

We work with our customers to deploy as quickly as possible to shorten the time to value, and as such we rely on our customers to ensure all necessary tasks are completed on their end. All required actions are outlined in the deployment timeline below; customers with smaller asset counts can often experience a shorter timeline in launching the MDR Service.

30/60/90 Day Success Plan

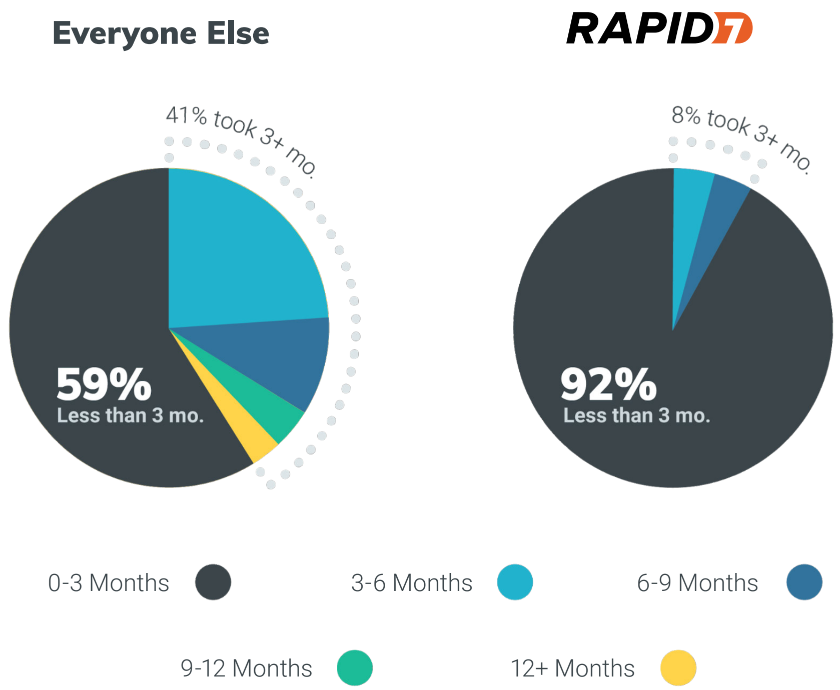
Customers should expect the following for 30/60/90 day milestones and operational results as a Rapid7 MDR customer:

MILESTONES	OPERATIONAL RESULTS
30 DAYS	
• Welcome email • Access to InsightIDR • Deployment kickoff call • Agent deployment completed • Collectors and foundational event sources configured	• Deployment completed • Product training and education completed
60 DAYS	
• Learn environment/start building threat profile • Start monthly meetings and reviews	• Product baselining • Compromise Assessment completed • Threat hunting now active • Log search available across all sources • All pre-build alerting is active
90 DAYS	
• Continue operational cadence and continued monitoring	• Monthly alert roll-up • Proactive threat hunt findings • Threat intelligence review • Quarterly goal review • Open Q&A and engagement with Rapid7 experts

MDR Technology Deployment

InsightIDR SaaS Advantage

As the only true SaaS SIEM on the market today, InsightIDR deploys faster then competing SIEM solutions. With this advantage, our team is able to stand up our MDR service within weeks.



Source: Gartner Peer Insights

Customers that already have the Insight Agent deployed in their environment significantly reduce the level of effort required to be 100% optimized as a Managed Services customer.

MDR Launch Phases

Rapid7 MDR Onboarding in broken into three distinct phases, including:
One (1) week of initiation activities ("Initiation")
Four (4) weeks of deployment activities ("Deployment")
Four (4) weeks of hunt/baselining activities ("Baselining")

Once Deployment, Baselining, and the Compromise Assessment are completed, Rapid7 will commence the monitoring and threat assessment phase ("Monitoring") as an ongoing service delivery.

Initiation Phase

The Initiation phase will introduce you to the setup and launch team, which includes a Project Manager, Operations Coordinator, and Security Consultant. The team works with your Rapid7 onboarding Project Manager to start the onboarding process.

TASK	MDR MILESTONES	DURATION	DETAILS
1.1	Welcome Email to Customer from Managed Services	1 day	Onboarding Team will send
1.2	Set up Customer in InsightIDR Portal	1 day	Customer will receive Log In details for InsightIDR via email
1.3	Set up Customer in Customer Portal	1 day	Customer will now have access to Customer Portal to access Site Survey
1.4	Enable Support Credentials	1 day	Enable support credentials for Customer
1.5	Welcome Email to Customer from Operations Manager	1 day	Introduces Project Manager and sends link for Kick Off Meeting Calendar options
1.6	MDR Kick Off Call	1 day	Define specific roles and responsibilities of the customer during the deployment and ongoing engagement phase
1.7	Complete Site Survey	1 day	If not already completed in PreSales, the Project Manager will ask you to complete a site survey

Initiation→ Deployment

To move from Initiation to Deployment, the following checkpoints must be completed:

- Configuration of InsightIDR and the Customer Portal
- Introductory Managed Services Kickoff Call
- Site Survey Response Submitted to the Customer Portal

Your MDR service kickoff call will include:

- Managed Services and Technology Delivery Overview
- Customer Engagement Model
- Defining Your Incident Escalation Process with Rapid7

Deployment Phase

Deployment phase is split into two stages:

- InsightIDR Setup with Collectors and Agents Deployed
- Validation of InsightIDR Setup

During your deployment, Rapid7 will provide one to two days of remotely dedicated time with our deployment consultant to assist in configuring your event and log sources into the platform service. During this stage, the Rapid7 deployment team will also help your team set up dashboards inside the InsightIDR product.

Following this, the Rapid7 team will provide best practices training and help configure advanced configurations in the InsightIDR dashboards. It is important to ensure you're following the recommended deployment requirements for successful deployment.

InsightIDR Setup Collectors, Agent, Event Sources

TASK	MDR MILESTONES	DURATION	DETAILS
2.1	Set Up Collector(S)	1 day	Use the wizard in InsightIDR to set up first Collector
2.2	Deploy Rapid7 Insight Agent to All Servers and Workstations	2 weeks	Deploy Agents using Token Installation
2.3	Configure all Foundational Event Sources	2 weeks	DHCP, LDAP, DNS & AD required for MDR Service
2.4	Deployment Event Sources	2 days	Customer will be invited for 1 or 2 full days with the Deployment Consultant to configure and validate all Event Sources and prerequisites. It is also an opportunity for training and education on InsightIDR

Validate InsightIDR Setup

TASK	MDR MILESTONES	DURATION	DETAILS
3.1	Verify Collectors & Agents	2 days	Deployment must be to at least 80% of asset environment
3.2	Configure/Validate Event Sources	2 days	
3.3	Custom Event Source Syslogs	2 days	
3.4	Set Up Deployment Phase Artifacts	2 days	
3.5	Set Up Custom Alerts, Dashboards	2 days	
3.6	Log Search Overview	1 day	

Deployment→ Baselining

There are two major prerequisites to move from Deployment to Baselining during onboarding:

1. Four foundational event sources configured

- Domain name system ("DNS")
- Active directory ("AD")
- Dynamic host configuration protocol ("DHCP")
- Lightweight directory access protocol ("LDAP") (collectively, the "event sources")

2. Minimum of 80% of your environment covered by the Rapid7 Insight Agent

Baselining Phase

Your Rapid7 Customer Advisor (CA) will take over for the Rapid7 Deployment team and introduce the next phase of onboarding: Baselining. The Customer Advisor will be your primary contact onwards in connection with the MDR service and the platform service.

TASK	MDR MILESTONES	DURATION	DETAILS
4.1	Monitoring Kickoff Call	1 hour	CA invites the Customer to a Monitoring Kick Off call to introduce the next phase of the Service. The CA will explain the reports that Customer will receive on an ongoing basis and set-up communications protocols and processes as defined by the Customer.
4.2	Set up Customer in Security Operations Center ("SOC") Tool		
4.3	SOC Notified Customer Ready for Baselining	1 day	
4.4	SOC Analyst Assigned	1 day	
4.5	Baselining Period	2 weeks	
4.6	Findings Report Created (if applicable)	1 hour	During Baselining, if malicious threats are found (such as an active malware event or if SOC notices the presence of an adversary) a Findings Report will be created for each threat as soon as they are discovered.
4.7	Hunt Period	2 weeks	
4.8	Deliver Compromise Assessment	1 day	This report contains any detected active or historic compromises, potential avenues for future breaches, and prioritized remediation and mitigation recommendations.

Baselining→ Monitoring

After the first two (2) weeks of MDR monitoring, InsightIDR will be configured to understand typical user, asset, and account behaviors. At the completion of Baselining, InsightIDR will understand the interactions between IP addresses, machines, and the user accounts on those machines. This baseline also starts to identify regular users from service accounts and admin accounts.

Additionally, at the end of the Baselining phase, Rapid7 MDR delivers a Compromise Assessment report that identifies and validates potential or present threats to your system environments, and will be continuously monitored using the platform service and other tools.

Monitoring Phase/Ongoing Service Delivery

Once Baselining is complete, your environment will be monitored by the Rapid7 MDR SOC, commencing the ongoing Monitoring phase. At this point, Rapid7 will deliver Findings Reports within 1 hour of a validated threat being confirmed.

TASK	MDR MILESTONES	DURATION	DETAILS
5.1	Service Reports	Monthly	Rapid7 will provide you with metrics and context surrounding analysis activities, technology health, and findings summaries for an at-a-glance overview of MDR activities.
5.2	Hunt Reports	Monthly	Our analysts leverage the Rapid7 Insight Agent to collect metadata from multiple locations on your endpoints to identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies.
5.3	Threat Intel Reports	Ad-hoc	Highly targeted analysis that leverages the power of Rapid7's threat intel infrastructure (Project Heisenberg, Project Sonar, 3rd-party threat intel) to develop rules to scan your environment and perform real-time asset hardening.
5.4	Finding Reports	Ad-hoc	Findings reports provide written analysis, criticality, raw details, remediation recommendations, suggested containment actions, and mitigation recommendations for each validated incident.

APPENDIX

Detection Methodologies

Rapid7 MDR SOC employs a multi-layered approach to detect malicious activity across the attack chain for both known and unknown threats. Each detection through InsightIDR is validated by our SOC analysts to ensure we only pass true threats in our reports. This section will outline our detection methodologies, the role of InsightIDR in our threat detection, and the deliverables you can expect from the MDR team.

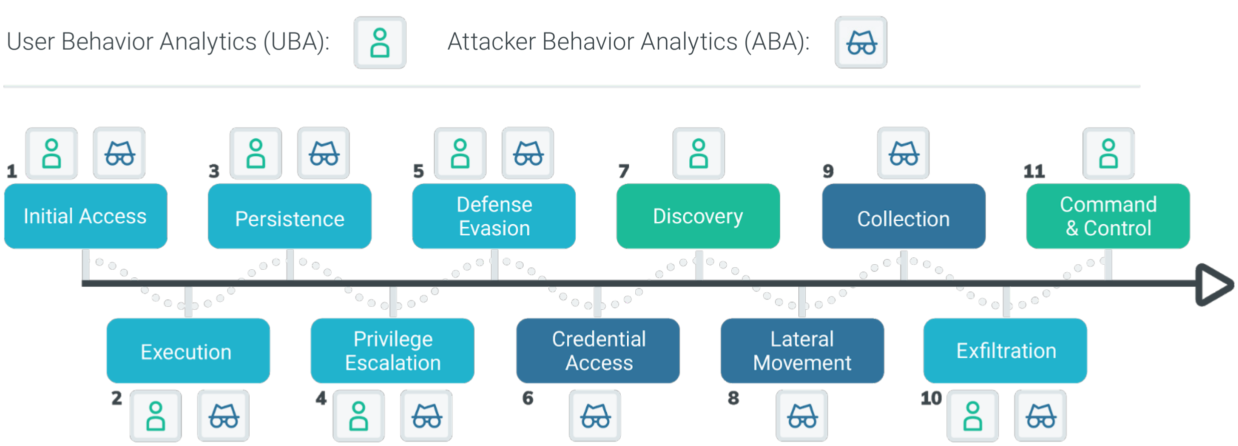
In order to have complete coverage, the InsightIDR technology integrates with your existing network and security stack to collect and query endpoints through the Insight Agent and endpoint scan. Beyond the alerts identified by InsightIDR, the MDR team also runs regular threat hunts in your environment and curates custom Threat Intelligence.

Behavior-based Detections

For our SOC team, detecting threats using InsightIDR is a core differentiator for Rapid7's MDR service, and it lays the foundation for advancing your security program's maturity by overlaying behavior-based detection methodologies.

The detection our team provides across the attack chain stems from a combination of User and Attacker Behavior Analytics, endpoint data, and deception technology.

Rapid7 MDR Aligns to MITRE ATT&CK Framework



Effective implementation of user- and deviation-based detection methodologies requires deep visibility into endpoints, network metadata, authentication/authorization events, and logs, coupled with purpose-built technology and subject matter expertise provided by the Rapid7 SOC.

User Behavior Analytics (UBA)

User Behavior Analytics (UBA) enables our SOC team to more easily determine whether a potential threat is an outside attacker impersonating an employee or an actual employee who presents some kind of risk, whether through negligence or malice.

UBA connects activity on the network to a specific user as opposed to an IP address or asset. This is then compared against a normal baseline of event activity for that user. Once collected and analyzed, it can be used to detect the use of compromised credentials, lateral movement, and other malicious behavior.

Our SOC leverages these UBA indicators to dynamically prioritize and rank alert criticality based on the presence or absence of notable behaviors associated with the alert by:

- **Detecting unknown threats** based on single occurrences, or groups of notable events based on specific user behaviors or deviations from known-good baselines.
- **Detecting insider threats** based on groups of notable events describing the sequence of events typically associated with information theft by an authorized party.
- **Associating user behaviors** based notable events to alerts and investigations to improve the validation and investigation analyst workflows.
- **Providing the data needed to associate technical evidence** with human understandable behavior for threat reporting.

InsightIDR provides our SOC team with a technological advantage by utilizing our proprietary attribution engine with models that are purpose-built to detect behaviors indicative of true threats, while sorting out users who may be doing unusual tasks but are not actually compromised or performing malicious actions. Many traditional SIEM solutions claim to utilize UBA detections, but SIEM engines aren't built for real-time attribution, unlike Rapid7's InsightIDR technology. This is because users and assets constantly move around in a modern network architecture, leading to an engine that cannot accurately map events to entities.

Attacker Behavior Analytics (ABA)

Attacker Behavior Analytics (ABA) applies Rapid7's existing experience, research, and practical understanding of attacker behaviors to generate investigative leads based on known attacker tools, tactics, and procedures (TTP). These include:

- Malware, malware droppers, maldocs, and fileless malware (opportunistic and targeted)
- Cryptojacking (stealing CPU cycles to mine cryptocurrency)
- Pen testing and attack tools
- Suspicious persistence
- Anomalous data exfiltration
- New attacker behavior

ABA detection methods are constantly updated by MDR SOC investigations, combined with Rapid7's research and threat intelligence analysts to extract key behaviors from threats identified in our customer environments. After performing research on related attacks and behaviors, we craft new ABA detections that are deployed across all MDR customers to simplify and accelerate detection and reduce the time to remediation. These sources include:

- MDR customers
- The Metasploit Community
- Project Heisenberg (our honeypot network)
- Project Sonar (our internet-side scanning project)
- Incident Response engagements
- InsightIDR customers sharing intel
- Rapid7's Threat Intelligence team and community (e.g. Cyber Threat Alliance)

Other key advantages include:

- **Found once, applied everywhere:** Your security team gets the benefit of the learnings from other MDR customer investigations. When our SOC team finds new attack methodologies—either by way of our SOC, threat intelligence team, or Rapid7 research—those TTPs are updated in InsightIDR and applied to all MDR customers and investigations
- **Detections based on behaviors, not signatures:** Through InsightIDR, our SOC team is armed with high-fidelity endpoint data to identify novel variations of new attacker techniques.
- **High-fidelity alerts grant context to take action:** Alerts include context from our analysts and threat intel teams, so you can make better decisions, remediate the problem, mitigate risk, and contain the alert from directly inside your Findings Report.
- **Constantly evolving ABA detections:** Whenever possible, the alert will detail known, recent adversary groups using a similar technique in a confirmed attack.

As a key advantage of our cloud deployment model, our detections are updated automatically to our entire user population—including MDR customers—after a thorough prototyping, testing, and validation process. All new indicators are applied to one month's historic data so your environment is instantly protected.

Threat Intelligence-based Detections

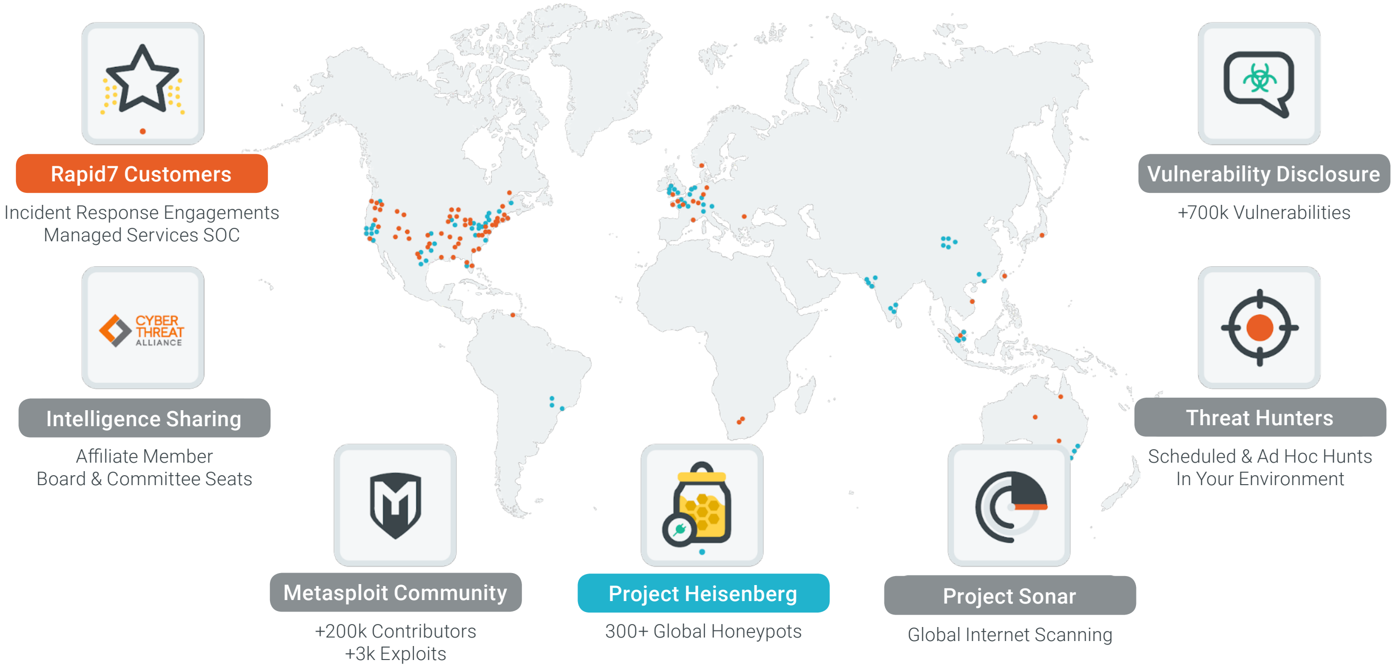
Rapid7 leverages proprietary threat intelligence derived from research, previous investigations and monitoring findings, as well as third-party sources. The MDR Threat Intelligence team is responsible for maintaining this intelligence and working alongside our SOC analysts to constantly apply threat detection and incident response learnings across all MDR customer environments.

Rapid7's Threat Intelligence team brings expertise and data sources from the public sector, private sector, and open sources to fuel threat detection and incident response.

- **Strategic threat intelligence** is provided per industry sector and is aimed at decision-makers to help shape strategies to prevent threats from materializing.
- **Tactical threat intelligence** is applied in our attacker behavior analysis methodologies and leverages complex rules to generate investigative leads across multiple event sources and over time.
- **Operational threat intelligence** is provided by way of proactive threat reports and indicates the likelihood of an impending attack. Our reports include mitigation recommendations to increase resilience against specific threats to your organization.
- **Technical threat intelligence** in the form of indicators of compromise are applied across our customer base. The Rapid7 Threat Intelligence team actively maintains the quality of the technical threat intelligence to ensure fidelity, context, and timeliness for our MDR threat analysts.

Rapid7 Research and Threat Intelligence Sources

We're committed to openly sharing security information that not only helps the entire cybersecurity community to learn, grow, and address issues in the security world, but also to improve our products and detections. Below are the common sources that lead to Rapid7's security expertise and intelligence advantage:



- **Rapid7 customers:** Our detections are enhanced from learnings across our 1MM+ customer endpoints, MDR customers, and Incident Response engagements.
- **Intelligence sharing:** Rapid7 is part of the Cyber Threat Alliance (CTA), a community of security research organizations with a mission to improve cybersecurity cooperation to improve defenses against cyber adversaries. Rapid7 is an Affiliate member of the CTA with Board and Committee seats.
- **Metasploit Community:** Metasploit is the world's most-used penetration testing software used to uncover weaknesses in defenses with over 3,000 exploits and over 200,000 active contributors.
- Project Heisenberg **Cloud:** A collection of over 200 low-interaction, global honeypots distributed both geographically and across IP space. The honeypots offer the front end of various services to learn what other scanners are up to (usually no good), and to conduct "passive scanning" to help enhance our understanding of attacker methods.
- Project Sonar: A security research project by Rapid7 that conducts internet-wide scans across different services and protocols to gain insight into global exposure to common vulnerabilities.
- **Pen test engagements:** Rapid7 service engagements allow us to leverage real-world experiences of our engineers and investigators gathered over thousands of pen tests.
- **Vulnerability disclosure:** Rapid7 publishes our data for free to encourage scientists, engineers, and anyone else interested in the nature and form of the internet to make their own discoveries.

Human Validation

All events are validated by our SOC analyst team prior to reporting any alert to you. With human validation from our Spotters or Hunters, our MDR service removes benign, unnecessary, or redundant alerts from your Findings Reports.

Threat Hunting

Rapid7's MDR team leverages Insight Agent data and specialized views to perform scheduled and ad-hoc threat hunts in your environment. The nature of the hunts varies over time and is based on trends in the threat landscape. The results of these hunts are sent to your team in the form of the monthly Hunt Reports.

Requirements for Successful Deployment

To get the most out of your MDR deployment, Rapid7 encourages you and your team to adhere to the following responsibilities:

- Designate and assign a project manager or similar to work with Rapid7 for your deployment.
- Designate and assign a primary point of contact and escalation path for reporting incidents.
- Complete a Deployment Survey prior to starting the Deployment phase.
- Ensure availability of deployed technology on site, including: Insight Collector, log sources, optional deception technology, and Insight Agent; as well as their ability to report to Rapid7 infrastructure.

Additionally, Rapid7 will take on the following requirements to ensure a smooth deployment process:

- Provision the Rapid7 cloud services in the technology stack for your environment.
- Designate and assign a Customer Advisor to support your security maturity and be your trusted point of contact for all things MDR.
- Designate and assign a Customer Success Manager.
- Designate and assign a Rapid7 Project Manager.
- Provide adequately trained/certified staff to conduct the service including:
    - Working with your appointed project manager to schedule meetings and tasks.
    - Assist you with subject matter expertise to deploy the various required and optional technology stack components.
    - Monitor your environment 24x7x365 in accordance with Rapid7's MDR detection methodologies and within the scope of the visibility provided by the technology stack.

During Initiation, Deployment, and Baselining Phases, Rapid7 will complete the following deliverables:

- Supported event sources
- As-built guides
- Findings Report
- Monthly State of Service
- Monthly Hunt Report
- Site survey

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. 7,800 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our website, check out our blog, or follow us on Twitter.