Technical Primer: Managed Detection and Response

A technical overview of what you'd get with our MDR service and SOC analysts

Rapid7's Managed Detection and Response (MDR) service offers a combination of expertise and technology to detect dynamic threats quickly across your entire ecosystem, powered by Rapid7's purpose-built technology stack, threat intelligence infrastructure, and our Security Operations Center (SOC) experts. The purpose of this document is twofold: 1) To provide a technical overview of how the service works, and 2) To describe the Onboarding and Implementation process.

Event Collection

During the onboarding process, Rapid7's MDR team will assist you in deploying the Insight Agent, a lightweight agent that sends endpoint event data to a data collector sitting behind your firewall. The purpose of this collector is to continuously gather real-time events from numerous log sources in the environment, including security event sources from a variety of network and security devices, such as firewalls, intrusion detection and prevention systems, DNS servers, cloud hosting environments, enterprise cloud applications, and security information and event management tools (SIEMs). This data is then synchronized with other event sources that include Active Directory to acquire user and permission details, which are then passed along with endpoint logs (user activities, endpoint data, and local logs on assets with the Insight Agent). This data is sanitized to remove any noisy log data, encrypted, and sent to Rapid7's Insight cloud.

The agents and collector are provided by Rapid7 and installed by the customer. Updates are automatically pushed from Rapid7 to the collector and agents as needed.

Threat Detection

Throughout your onboarding onto the Insight cloud and the MDR service, our team is also learning about your network. Later, we'll perform a Compromise Assessment to further develop our intimate understanding of your environment. This enables our team to spot possible threats earlier when your event data is analyzed against our external threat intelligence and validated by the SOC team.

Possible threats are identified using multiple threat detection methods, including:

- **User Behavior Analytics (UBA):** Analyzes user behavior and applies a series of heuristic and analytic rules to detect abnormalities such as compromised credentials, lateral movement, and other malicious behavior.
- **Attacker Behavior Analytics (ABA):** Analyzes endpoint behaviors to cross-reference against known attacker tactics, techniques, and procedures to find unknown attackers earlier in the attack chain.
- **Deception Technologies:** Set decoy technology assets (honeypots, honey users, and honey credentials) to find attackers and prevent them from infiltrating deep into the network.
- **Threat Intelligence:** Combines knowledge across research, threat intel, and the security community to continuously update rules and analytics capabilities to identify malicious activity in the customer's environment.

- **Threat Hunting:** MDR Hunter analysts leverage metadata collected by the Insight Agent to proactively hunt for persistent malware, historical application execution, unusual processes and network communications, Powershell invocation, ingress authentications, potentially unwanted programs or applications, and per-system anomalies that may be indicative of compromise or potential vulnerabilities.

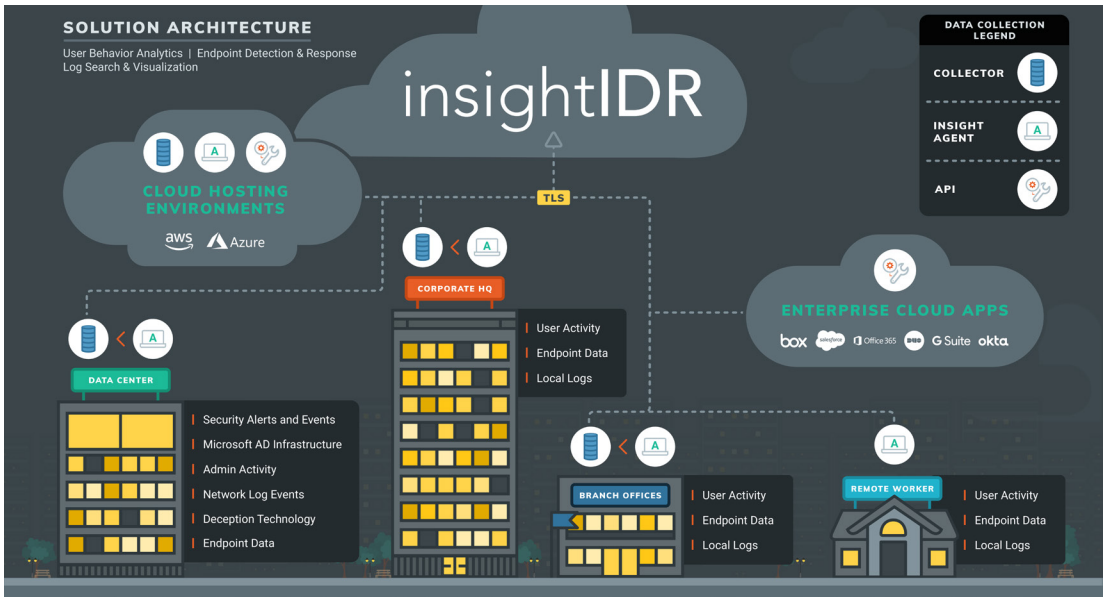

Figure 1: The InsightIDR solution architecture

Threat Reporting

Once a threat has been identified, the Rapid7 SOC validates the threat and prioritizes it as a Findings Report, which includes containment, remediation, and mitigation guidance. Alerts involving critical network assets are given higher priority, such as a file server with sensitive information, a workstation that processes PCI information, key cloud services such as Salesforce or Office 365, or the workstation of someone who deals with company secrets.

Because Rapid7 MDR has visibility into user endpoints to validate alerts, the Findings Reports sent to you are extremely accurate and are validated to show what poses an actual threat to the business. The data gathered from the endpoint agents are also used for the on-demand acquisition of forensic artifacts for the purpose of analysis and Incident Escalation. These include:

Suspicious User Authentication Activity

- Simultaneous authentications from multiple countries
- User logging into a device for the first time
- Brute-force attacks

Suspicious Account Management Activity

- Account password resets
- New account creation
- Account privilege escalations

Attacker Tools, Tactics, and Procedures

- Reconnaissance
- Credential harvesting
- Lateral movement
- Suspicious applications or scripts
- Traditional and web-based malware and backdoors
- DNS queries to a recently registered domain
- Honeypot activity

Remediation Recommendations

Once a threat has been identified, your Rapid7 Customer Advisor will reach out to your designated point of contact and include a Findings Report in your Services Portal. For non-critical threats, easy-to-follow instructions are provided so that your team can contain and remove the threat, and protect against similar attacks in the future. You are able to execute containment actions from within deep links in the Findings Report and via InsightIDR.

Incident Escalations

MDR Responder analysts are able to scope and help you respond in the event of an Incident Escalation. This seamless pivot into Incident Escalation is possible due to the forensic data collected by the Insight Agent, and it minimizes the time to contain an attacker or the damage from a breach.

ONBOARDING OVERVIEW

Each customer is assigned a Rapid7 Onboarding Project Manager, as well as other onboarding resources for the deployment, set-up, and implementation of the MDR service, including the deployment of the Insight Agent, collectors, and InsightIDR. Implementation of Managed Detection and Response typically takes 8 weeks, depending on the customer's environment and their availability to deploy agents and provide the required information to Rapid7.

Kickoff Call

Implementation begins with a kickoff call with the customer's assigned MDR resources. The team will explain the deployment process, including what to expect from Rapid7, and answer any questions you may have.

Information Gathering

Rapid7 MDR will require detailed information on your business, network, and processes so the team can understand priority assets and response paths when we detect anomalous activity. For example, this includes your company's Incident Response process, network architecture, identity and location of critical assets and employees, preferred communication method, and contact information. Through the information-gathering process, the team learns crucial details about your environment that are later used to validate and prioritize threats and suggest appropriate remediation steps.

Deployment of Collectors and Endpoint Agents

Based on the information gathered from the kickoff call, the MDR team will provide instructions on where and how the collector and endpoint agents should be deployed. The Rapid7 MDR team can monitor, investigate, and offer containment suggestions against remote users and high-risk assets in real time. Through our endpoint detection, our team of expert threat detection analysts are able to identify even the most stealthy intruder behaviors by correlating events captured from behavioral analytics in InsightIDR with human analysis from our expert SOC analysts.

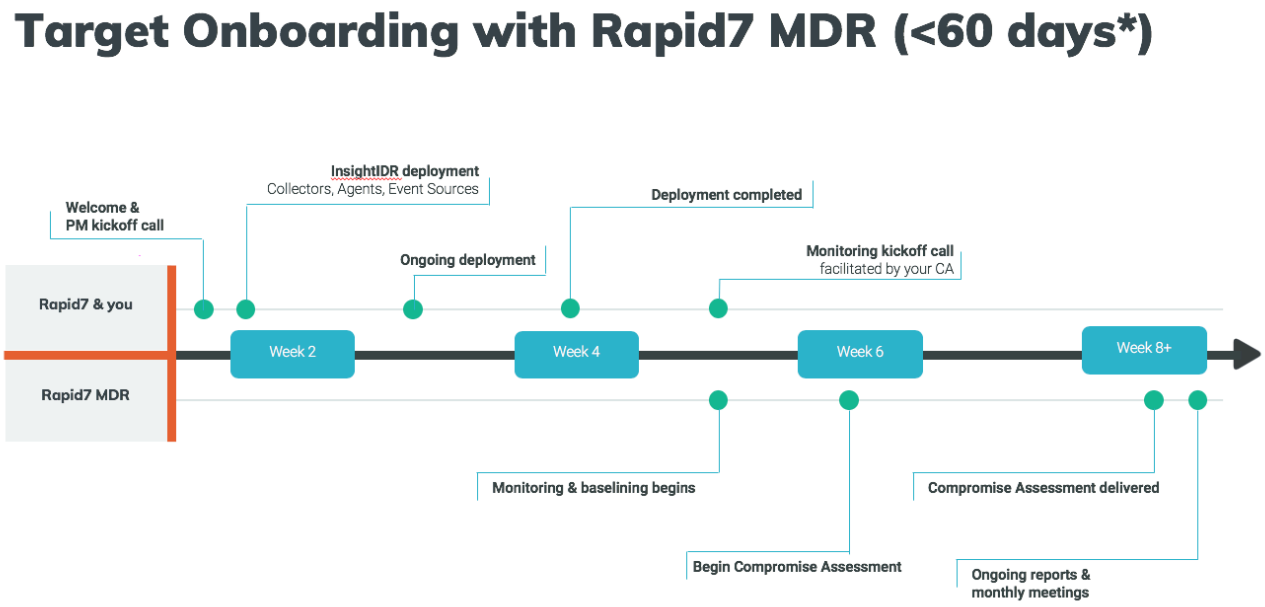

Figure 2: Target onboarding timeline for the MDR service
for small asset customers

We encourage you to deploy endpoint agents to your entire environment as quickly as possible for the best results; however, we require the Insight Agent to be deployed to at least 80% of your environment to consider deployment complete. You may decide to deploy additional endpoint sensors at any time, even after the service has launched. Once deployed, the agent will automatically provide data to the Rapid7 SOC for analysis.

Testing and Tuning

The Managed Detection and Response team tests and tunes the service as part of the implementation process and at an ongoing cadence to ensure that the correct data is continuously collected and sent to Rapid7. This includes new detections and configurations of your instance of InsightIDR. The team will work with each customer to ensure that any issues are promptly resolved.

ONGOING ANALYTIC RESPONSE SERVICE

Data is gathered and analyzed continuously, enabling customers to respond to threats much faster than they do today. In addition, anything learned from malicious behaviors caught in one customer's environment are immediately applied to all other relevant customer situations. With machine learning and ongoing research and analysis of new malware and threat detection techniques, the Managed Detection and Response service is continuously improving our ability to detect emerging threats for you and your team.

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. Over 7,800 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations.

To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

Support

call +1.866.380.8113

Customer Portal