RAPID7 TECHNICAL PRIMER

Managed Detection and Response

Rapid7's Managed Detection and Response is the only managed threat detection and incident response service that identifies nearly 100% of threats across the customer's entire environment and provides remediation recommendations to stop the breach. The purpose of this document is twofold: 1) To provide a technical overview of how the service works, and 2) To describe the implementation process.

TECHNICAL OVERVIEW

There are five components to the Managed Detection and Response service: event collection, event analysis, threat notification, remediation recommendations, and incident response.

Event Collection

As shown in Figure 1, a data collector sitting behind the customer's firewall continuously gathers real-time events, from both numerous log sources in the environment and from endpoint agents deployed as a part of the Managed Detection and Response (MDR) service. The analysis process sanitizes the noisy log data to track only meaningful security activity events and sends it to Rapid7's secured cloud. Data is encrypted before it is pushed from the collector to the cloud.

At a minimum, the collector synchronizes with the customer's Active Directory to acquire user and permissions information. The collector can also receive and process logs from a variety of network and security devices, including firewalls, intrusion detection and prevention systems, DNS servers, and security intelligence and event management tools (SIEMs).

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

Event Analysis

Once in the cloud, the customer data, combined with external threat intelligence, is analyzed. Possible threats are identified using multiple threat detection methods, including:

- **User behavior analytics:** Managed Detection and Response analyzes user behavior and applies a series of heuristic and analytic rules to detect abnormalities and risky behaviors.
- **Attacker behavior analytics:** Rapid7's deep expertise and continuous research in attacker behavior is unparalleled in the industry. Leveraging the knowledge and experience of Rapid7's security researchers, Managed Detection and Response defines rules against which the data is run to identify attacker behavior. These attacker analytics allow Rapid7 to create a series of intruder traps–such as honeypots and honey users–that provide accurate, low-noise detection of intruder behavior.

- **Threat intelligence feeds:** Rapid7 continuously gathers its own threat intelligence and uses this information to identify malicious activity in the customer's environment.

Threat Notification

Once a threat has been identified, the Rapid7 Security Operations Center (SOC) validates the threat and prioritizes it. During the implementation process and through regular customer update meetings, Rapid7's Managed Detection and Response team learns the customer's network and which assets are important–an investment that helps us prioritize what is of importance to our customers. Threats 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 used by someone who deals with company secrets.

Because Managed Detection and Response has the ability to reach down to the customer's endpoints to validate alerts, the alerts sent to the customer are nearly 100% accurate and positive. The endpoint agents are also used for on-demand data acquisition to gather forensic artifacts for the purpose of analysis and incident response.

Types of suspicious activity and risk factors that can be detected include, but are not limited to, the following:

- Exploitable mobile devices on the network
- Simultaneous authentications from multiple countries
- Account privilege escalations
- Account password resets
- Brute-force attacks
- DNS queries to a recently registered domain
- Honeypot user connections
- Lateral movement
- Attacker tools, tactics, and procedures
- Traditional and web-based malware and backdoors

Remediation Recommendations

Once a threat has been identified, a Rapid7 threat assessment manager contacts the customer. A complete analysis of the threat is provided, including what happened, which systems were impacted, and related evidence. For non-critical threats, easy-to-follow instructions are provided so that the customer can remove the threat and protect against similar attacks in the future.

Incident Response

For more complex attacks that involve removing a live attacker, the threat assessment manager may recommend that the customer use Rapid7's Incident Response (IR) professionals to remediate the threat. Managed Detection and Response includes a number of IR service hours so that, if required, Rapid7's IR team can immediately begin incident response work without requiring a separate contract. This seamless pivot into Incident Response minimizes the time to contain an attacker and the damage from a breach.

Rapid7's world-class Incident Response team has successfully completed over 2,000 investigations, including for 25% of the Fortune 100. On average, our team members have 15 years of experience investigating breaches of all sizes and across many industries. They are skilled in network analysis, forensics, and malware analysis, and in quickly remediating data breaches.

Bios of some of Rapid7's leading Incident Response team members are included on the last page of this document.

The Rapid7 Managed Detection and Response service is delivered from our Security Operations Center (SOC) located outside of Washington DC in Alexandria, VA. The facility is staffed 24/7 with world-class threat detection and incident response analysts. The facility has multifactor access controls, round the clock physical security monitoring, redundant and backup power, and Internet services.

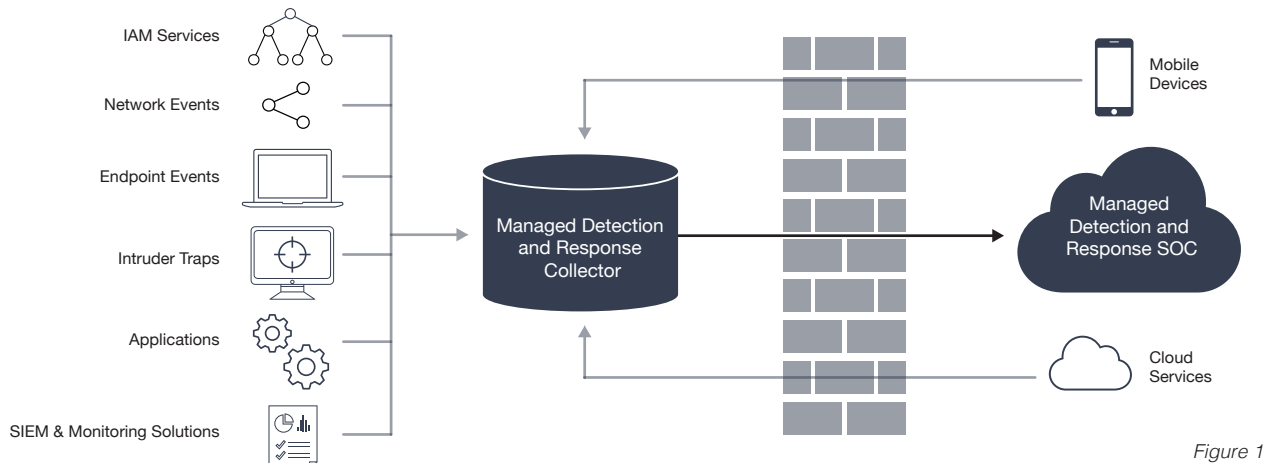

Figure 1

IMPLEMENTATION

Each customer is assigned a Managed Detection and Response team consisting of a deployment manager and a threat assessment manager who will work with the customer throughout their service period. Implementation of Managed Detection and Response typically takes 1 to 3 weeks, depending mainly on the customer's environment and their availability to provide the required information to Rapid7.

Kickoff Call

Implementation begins with a kickoff call with the customer's dedicated Managed Detection and Response team. The team explains the deployment process, tells customers what to expect from Rapid7, and answers any questions they may have.

Information Gathering

The Managed Detection and Response team will require information on the customer's business, network, and processes. For example, they will ask questions about the 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 the customer's environment that is 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 customer, the Managed Detection and Response team will provide instructions on where and how the Managed Detection and Response collector and endpoint agents should be deployed. Managed Detection and Response can monitor, investigate, and contain attacks against remote users and high-risk assets in real time. Through its endpoint detection, it sniffs out even the most stealthy intruder behaviors.

Testing and Tuning

The Managed Detection and Response team tests and tunes the service as part of implementation and on an ongoing basis to ensure that the correct data is continuously collected and sent to Rapid7. 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, learnings from one customer 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.

Customers receive a monthly report on activity generated from the Managed Detection and Response service. The reports show the number of alerts investigated, key findings, and monthly trends.

The customer may decide to deploy additional endpoint sensors at any time, even after the service has launched. Once deployed, the agent will automatically check in and begin sending data to Rapid7's SOC.

INCIDENT RESPONSE

Customers are advised to use their Incident Response hours included in the Managed Detection and Response service during complex attacks, particularly those that involve a live attacker. Rapid7 Incident Response Services provide access to the experience and technical expertise to accelerate incident investigation and containment. Our teams can work together with in–house teams for all stages of incident response, from analysis and detection through containment, remediation, and cleanup. Rapid7 Incident Response teams are made up of industry–leading experts with 15 years of experience in incident response of all sizes. Our team will help you with all aspects of the response through to incident remediation and cleanup. Customers benefit from a single point of contact who is ultimately responsible for coordinating, communicating, and reporting on all aspects of incident response activities. Incident management includes all aspects of threat detection, documenting findings, and collaborating to devise appropriate remediation activities.

ABOUT RAPID7

With Rapid7, technology professionals gain the clarity, command, and confidence to safely drive innovation and protect against risk. We make it simple to collect operational data across systems, eliminating blind spots and unlocking the information required to securely develop, operate, and manage today's sophisticated applications and services. Our analytics and science transform your data into key insights so you can quickly predict, deter, detect, and remediate attacks and obstacles to productivity. Armed with Rapid7, technology professionals finally gain the insights needed to safely move their business forward. Rapid7 is trusted by more than 5,800 organizations across over 110 countries, including 37% of the Fortune 1000. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

RAPID7 MANAGED DETECTION & RESPONSE TEAM MEMBER BIOS

Wade Woolwine

Wade is responsible for defining and managing Rapid7's threat detection and incident response initiatives. Prior to joining Rapid7 he played an integral part in building Mandiant's Managed Defense business unit. His team there was responsible for incident response, performing intelligence management, systems/technology integration, and research and development on new threat detection and incident response techniques. In the course of his career Wade has helped build AOL's application security capability, and has served as a threat detection and incident response analyst in a number of different government agencies. When not delivering world-class services for employers and customers, Wade spends time speaking at various infosec conferences, as well as contributing to the security community at large through working groups like OWASP and NoVAHackers.

Tim Stiller

Tim's primary focus areas include incident response, forensics, malware analysis, automation engineering, and development. He previously worked for Mandiant's Managed Defense Team as an Incident Analyst, where he responded to a variety of malware-based threats and developed an arsenal of automated tools to aid in hunting efforts. Tim holds multiple certifications including the CISSP, CEH and ECS.

Jordan Rogers

Jordan is a consultant at Rapid7 responsible for building out the Program Development, Table Top Exercise, Breach Readiness Assessment, and Forensic programs. Prior to joining Rapid7 Jordan worked for HALOCK Security Labs acting as a lead consultant for their Incident Response and Forensics practice, where helped design their forensics lab, wrote incident response and forensics, templates and policies, performed table top exercises, breach readiness assessments, litigation forensics support, first responder training, and malware analysis. Prior to HALOCK he was a federal contractor working with RSA Netwitness and Security Analytics with full packet capture and log correlation. He was responsible for deploying the solution, training the clients, and assisting with investigations. When Jordan is off the clock he enjoys speaking, training, and volunteering at infosec conferences across the globe. Jordan also assists with open source projects such as OpenStack and Gentoo as well as various malware research groups. He has also been contacted by Good Morning America regarding the research he has done with friends during his free time.