Rapid7 Managed Services Guidebook

Table of Contents:

What is Rapid7 Managed Services?

The mission of Rapid7's MDR service is to leverage our experts to collaboratively advance each customer's cybersecurity decision-making and maturity through our tailored guidance. We pride ourselves on becoming a true extension of our customer's security team. Our goal is to partner together to enhance our customer's ability to detect and respond to threats with hands-on 24x7x365 monitoring, threat hunting, incident response, and customized security guidance to stop malicious activity and strengthen each customer's security posture.

This guidebook is designed to help you understand Rapid7's Managed Services as a whole and describe the teams working behind the scenes to make all of our Managed Services work together.

Services

Managed Application Security

With increased requirements for testing web applications, it is crucial to ensure applications are configured, scheduled, and scanned on a consistent basis. Thus, prioritizing the risks most susceptible to exploitation by real threat actors, and reducing vulnerabilities found in your runtime applications are critical. It is also important to test for business logic flaws and other attacks not covered by automated scanners, which requires the experience of experts and practitioners who understand the real risk. Using Rapid7's award-winning application security software AppSpider and attack intelligence, our team of experts continuously test and provide remediation guidance so you can be confident that your applications are secure -- now and moving forward.

Managed Detection and Response

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.

Managed Vulnerability Management

Rapid7's Managed Vulnerability Management (Managed VM) Program provides a comprehensive picture of threat exposures and global criteria for risk prioritization to facilitate timely remediation across your environment. Rapid7 Managed VM is tailored to help you build, operationalize, or advance your current security program by implementing our proven three-pronged approach covering Technology, Security Expertise, and Process. Rapid7 Managed VM provides your team tailored recommendations to manage, execute, and optimize remediation across your environment — cloud, virtual, remote, local, and containerized infrastructure — to strengthen your overall security posture and lower your risk exposure.

The Managed Services Team

Rapid7's Managed Services consist of multiple teams working together to help you improve your organization's security posture. You may be assisted by all or some of these teams, depending on the services you have purchased.

All Services

Customer Advisor

Your Customer Advisor (CA) is your main point of contact for Rapid7 Services. You may have one or more assigned CAs depending on the number of organizations and services This named resource works with you as a strategic security partner through ongoing security consultation to guide your organization's security maturity, and should be considered an expert in your environment and a knowledgeable strategic resource who can help your organization advance more securely. They are your gateway to the many teams behind the scenes, from the MDR SOC to the Managed Operations teams. Customer Advisors work closely together to discuss best practices so your organization gets the benefit of the collective knowledge of all CAs. Your CA may be located in our LA, Austin, or Alexandria offices in addition to our remote CAs spread throughout the globe. You will be given a direct line of communication to your CA through phone calls, emails, and regularly scheduled meetings to provide updates on service delivery, reporting, metrics, technology health, and ensure that we are addressing your security goals. CAs are available during normal business hours by

Customer Success Manager

Your Customer Success Manager (CSM) is assigned to your account for your entire relationship with Rapid7. Your CSM is an internal advocate who ensures your team's success by facilitating the best use of Rapid7's solutions and driving resolution on technology-related issues and requirements. They are also your point of contact for adopting new Rapid7 solutions or expanding your solution coverage. Your CSM may be located in Boston or Austin and you will be given a direct line of communication through phone calls, emails, and regularly scheduled check-in meetings.

Support Engineers

Throughout your relationship with Rapid7, you may work with the Rapid7 Support team for assistance with product related concerns. Your CA can help you determine whether to leverage the Support team.

opening up a Support ticket assigned to your CA. During non-business hours, a member of the CA team is on-call for security emergencies.	

MVM and MAS

Managed Operators

Rapid7's Managed Operations team works behind the scenes to ensure that day-to-day operations run as smoothly as possible. The team is engaged right from the beginning of your journey with Rapid7, through standing up your console and making sure all supporting infrastructure is set up and configured correctly.

Once you and your Customer Advisor (CA) have agreed upon a scanning cadence, the Managed Operations team will take over the configuration, monitoring, verification, and troubleshooting of these scans. They will also collaborate with your CA to help set up detailed and understandable reports, providing insight into vulnerabilities and remediation advice to help you securely advance. The Managed Operations teams are located in our Belfast and Arlington Security Operations Centers (SOC).

MDR

Security Operations Center	Incident Responders
After deployment is complete and all monitoring requirements have been met, your environment will be assigned to one of our Security Operations Center (SOC) Pods staffed by our world-class analysts. These pods of analysts ensure that each customer receives continuous 24x7x365 monitoring coverage for high- and low-fidelity alerts. This pod model enables our SOC team to more thoroughly scale to ensure your environment is vigilantly monitored and our team can better identify known and unknown threats to your business, such as our monthly threat hunts. The MDR analysts are located in our Arlington, Dublin, and Melbourne SOCs.	Rapid7's expert Incident Response (IR) Consultants have conducted hundreds of investigations and have decades of experience responding to compromises of all sizes and severity. These include small-scale opportunistic threats, corporate phishing attacks, credential theft, ransomware attacks, and sophisticated state-sponsored campaigns. Our professionals complement their expert analysis with knowledge of multiple, industry-leading technology platforms for rapid response and incident scoping. Our consultants are located throughout the US and are available 24x7x365 to help our customers. Rapid7's IR team is found within the Managed Services department under the Detection & Response (D&R) Practice.

Threat Intelligence Team

Rapid7’s Threat Intelligence team supports the MDR SOC and CAs with analysis and new detections. Our Threat Intelligence team of researchers identifies new attack trends across the global threat landscape and uses these findings to create in-product detection mechanisms for new vulnerabilities, exploits, and attack campaigns. The Threat Intelligence Team is located in our Arlington office.