Scope of Service

Rapid7 Managed Vector Command

Rapid7's Managed Vector Command Offering is a continuous red teaming service provided by Rapid7. This Service offers an ongoing, proactive defense strategy to simulate real-world threat actors targeting your ("you", "Customer", "your organization", "your environment") organization. Through integrating Rapid7's industry-leading vulnerability management, attack surface monitoring, and expert penetration testing, we help identify, exploit, and report critical vulnerabilities before malicious actors can leverage them.

Vector Command is an advanced adversarial group combining automated technology with expert human oversight to continuously monitor and assess your external attack surface. When vulnerabilities or misconfigurations are identified, the Vector Command service attempts to exploit these weaknesses to demonstrate their potential impact, providing your security team with actionable intelligence to prioritize the most critical risks. The service simulates real-world attack tactics, including multi-vector attack chains, to reflect how actual threat actors would approach breaching your organization.

Key Features of Vector Command:

1. Continuous External Attack Surface Monitoring:
   - Ongoing identification of new and existing assets and potential exposures across your attack surface, focusing on internet-facing assets.
2. External Vulnerability Identification & Exploitation:
   - Regular evaluations to identify misconfigurations or exposures, followed by attempted exploitation to demonstrate their potential impact.
3. Noise Reduction through Focused Reporting:
   - Reporting only on vulnerabilities that result in successful breaches ensures your security team focuses on the most relevant threats.
4. Monthly Electronic Social Engineering Campaigns:
   - Opportunistic phishing and other electronic social engineering tactics aimed at breaching your organization's perimeter, simulating real-world tactics.
5. Zero-Day and N-Day Vulnerability Monitoring:
   - Continuous monitoring for critical vulnerability releases affecting your external software, along with validation of patch effectiveness against these threats.
6. Post-Breach Threat Actor Emulation:
   - In a breach, Vector Command will emulate real-world threat groups' techniques, tactics, and procedures (TTPs), allowing your security team to test and improve detection and response capabilities.
7. Real-Time Platform Reporting:
   - Access to an intuitive reporting platform that highlights vulnerabilities and potential attack paths as they are discovered and exploited.
8. Reassessment of Remediated Vulnerabilities:
   - Verification that previously remediated external vulnerabilities remain secure and are no longer exploitable.

9. Monthly Findings Summary Reporting:
    - A monthly report that includes reported findings, remediation guidance, affected assets, and post-compromise breach activities.

This service is designed to keep your organization one step ahead of attackers, ensuring that your security team can effectively respond to and mitigate the most significant risks.

By working as your partner to understand your business goals, network, and assets, Rapid7's goal is to deliver the peace of mind, focus, and consistency that customers expect from a managed service while ensuring our customers maintain visibility into program activities and deliverables enabling them to effectively communicate and report on their security posture internally.

This document outlines the scope of Rapid7's Vector Command service which includes:

- Rapid7 Managed Team
- Rapid7 Supporting Teams
- Rapid7 Technology
- Service Deliverables
- Cybersecurity Advisor (CA) Engagement
- Continuous Red Team Operations
- Customer Service Interaction
- Joint Responsibilities
- Appendix

Rapid7 Managed Team

Vector Command Cybersecurity Advisor

Your Vector Command Cybersecurity Advisor ("CA") will collaborate with you to understand your goals concerning how Vector Command fits within your security program. The knowledge gained from these discussions will drive the contextual output of your program deliverables. During monthly meetings with your CA, there will be an opportunity for continuous feedback, resulting in holistic program development. This helps adapt existing policies and procedures to maximize our joint risk remediation efforts. Throughout service delivery, your CA will communicate remediation and mitigation improvements using specific and adaptive reports and periodic business reviews.

Red Team Operators

The primary objective of the Managed Red Team Operators is to perform testing against your approved external network attack surface to identify high-impact vulnerabilities and breach perimeter defenses. Successfully exploited vulnerabilities and breaches into your organization will be documented through detailed reporting on the Vector Command platform. These reports will include comprehensive insights into your attack surface, potential risks, and the steps used to exploit the vulnerabilities. Rapid7's Red Team operators will work in a team model, with each member of the team focused on their area of expertise: external network penetration testing, emergent threat validation, phishing simulation, and post-compromise breach assessment.

Rapid7 Supporting Teams

Threat Intelligence and Research Team

Rapid7 technology is heavily influenced by our Threat Intelligence and Research Team to better help you defend against the changing landscape of malicious attackers' ability to attack your environment.
Our Rapid7 Threat Intelligence and Research Team identifies new attacker trends across the global threat landscape and uses these findings to enhance our product offering. Primarily leveraging information from Rapid7's Metasploit Project, the most used pen testing tool for offensive security, and Project Sonar, an internet-wide survey across different services and protocols, to gain insights into global exposure to common and new exploitable vulnerabilities. Rapid7's research team monitors new emerging threats for 0-days and N-days most likely to be abused by malicious actors for initial access. Rapid7's Red Team operators collaborate with the Threat Intelligence and Research Team to assess emergent threats against your exposed external attack surface.

Rapid7 Technology

Platform	Description
Vector Command Attack Surface Management	Your service includes a single instance of Vector Command for your entire organization. The Attack Surface Management (ASM) solution will be the primary tool used by Rapid7's team to perform asset discovery and reconnaissance of your external attack surface. All of your security team users will be assigned to and will have access to all data stored within this single instance.
Vector Command Reporting Portal	Your service includes a single instance of the Vector Command Reporting Portal. Rapid7's Red Team operators will provide service deliverables through the Vector Command Reporting Portal, as defined in the service deliverables section of this document below.
Customer Portal	Communication with your Cybersecurity Advisor and technical support tickets should be raised via the Rapid7 Customer Portal at insight.rapid7.com/login.

Service Deliverables

Rapid7 will provide you with the following Vector Command deliverables during the term of your Vector Command service. These include:

Deliverable	Description
Vector Command Red Team Findings	When Rapid7 successfully exploits a vulnerability, a new finding will be opened in your Vector Command reporting portal. Findings may include an overview of the vulnerability, detailed steps Rapid7 took to exploit the vulnerability, the impact of successful exploitation, severity rating following NIST guidelines, affected assets or users, and remediation guidance. When a new finding is published, a specified employee or email distribution list will be notified via email.
Vector Command Breach Timeline	In the event of a successful breach of an asset or application, Rapid7's Red Team Operators will include a breach timeline within the current monthly report. This breach timeline will provide an overview of initial access activities and post-exploitation activities performed by Red Team operators. Information provided is to assist your organization in tracking Rapid7's activity, providing an opportunity for your team to assess if the actions were discovered by your security tooling or telemetry.
Vector Command Findings Status Dashboard	The Vector Command portal provides a dashboard view of all findings identified and reported on by the team, providing a high-level view of the number of findings and severity rating associated with them. This allows your team to view all findings identified in one view, providing a high-level view of current findings.
Vector Command Monthly Report Exports	Findings, attractive assets, breach report summaries, phishing campaign summaries, and Emergent Threat Response (ETR) reviews performed by Rapid7 will be captured in monthly reports. These monthly reports are living documents, with new content being added and made visible to your organization throughout each month. At the end of each month, your organization can export these results and assessment notes into a Word (.doc) or PDF file.

Cybersecurity Advisor Engagement

During the term of your Vector Command service, you will regularly engage with your CA. Your CA will be available to answer any questions about your service and advise you on how to advance your security maturity.

Outlined below are frequent interaction touchpoints that your team will have with your CA:

Communication	Frequency	Method	Description
Customer Requested Meeting	Ad-Hoc, requested through Online Support Portal and subject to	Online Customer Portal, phone or screen share	Meeting with CA to address concerns or questions regarding the service.

	CA availability		
Customer Questions	Unlimited, Ad-hoc	Online Customer Portal	You may leverage the customer portal to request help or to voice concerns and questions related to the Vector Command service.
Monthly Meeting	Scheduled Monthly	Virtual	Your CA will meet monthly to review findings, recommendations, asset approvals and discuss any requirements regarding your interaction with the Vector Command Service.
Periodic Business Review (PBR)	As Requested, Ad Hoc	Virtual	The Periodic Business Review is scheduled with your entire Rapid7 account team to provide a holistic review of your security program and partnership with Rapid7. During the PBR, your CA will summarize service performance and present recommendations for further advancing your maturity.
Detailed Finding Review	As Requested, Ad Hoc	Virtual	You can leverage the Customer Portal to request a detailed review of a specific finding within the month it was opened. Your CA will assess the request and schedule a meeting with an appropriate member of the Red Team operators to discuss the finding in-depth.

Activating Your Vector Command Service

Rapid7 will begin the Vector Command service after the initial completion of the following onboarding steps:

1. Your assigned Cybersecurity Advisor will schedule an initial kickoff call with you and your team to explain Rapid7's Vector Command platform and services.
2. Input of your seed assets into the ASM platform (Discovery Seeds), allowing discovery to begin.
3. Once discovery has completed, approve discovered assets for ongoing vulnerability scanning and Red Team Operations. In order for Red Team operations to begin, you must approve assets within ASM. Approved assets must be assets owned by your organization. For further information, see *Customer Service Interaction* within this Scope of Service.

Continuous Red Team Operations

Rapid7 will perform ongoing Continuous Red Team ("CRT") operations against your approved external network attack surface, with the objective of identifying vulnerabilities of substantial impact and breaching your perimeter defenses. Key components of Rapid7's CRT are ongoing exploitation attempts against external network services, electronic social engineering campaigns, and post-compromise breach simulation.

External Network Assessment

Rapid7's skilled Red Team operators will leverage automated tools and manual analysis to assess your organization's external network (internet-facing) assets for exploitable vulnerabilities and misconfigurations. You are responsible for using Attack Surface Management (ASM) to define and approve your organization’s scope for ongoing external network testing. Approved assets will be collected on the first day of each month for both automated vulnerability scanning and Rapid7’s Red Team operator’s penetration testing activities.

Rapid7’s Red Team operators will only report vulnerabilities that they were able to successfully exploit with an identifiable impact to the organization. Vulnerabilities that could not be exploited by the Red Team, such as those with mitigating factors, lacking exploit primitives, or requiring other vulnerabilities not present in the attack chain, will not be reported as a finding to your organization. However, they may surface under the Red Team report ‘attractive assets’ category, which provides an overview of assets that the Red Team operators found interesting during their ongoing assessment.

Electronic Social Engineering

Rapid7 will conduct ongoing electronic social engineering campaigns. Campaigns are opportunistic, simulating adversaries targeting multiple companies with the same campaign. Red Team operators will perform phishing campaigns with the goal of breaching your organization’s perimeter or externally exposed applications. Tactics used during electronic social engineering may include, but are not limited to:

- Phishing for usernames and passwords.
- Phishing tactics that capture authenticated sessions to bypass Multi-Factor Authentication (MFA) controls.
- Phishing with Command and Control (C2) payloads to establish remote access on compromised assets.
- Targeted vishing tactics as a secondary exploitation step to a phishing campaign.

Social Engineering activities conducted by Rapid7’s Red Team operators will be recorded in Vector Command’s reporting portal. Successful campaigns will be recorded as new findings in the Vector Command reporting portal, including detailed information about the campaign with screenshots of successful exploitation.

Post-Compromise Breach Simulation

In the event that Rapid7 is able to compromise an asset in your environment, Rapid7’s Red Team operators will perform post-exploitation exercises in the form of a Post-Compromise Breach simulation. Post-compromise breach simulation will assist your organization in understanding the impact of the compromised asset or application, as well as additional vulnerabilities which could be discovered through the compromised asset. Post exploitation activities may include, but are not limited to:

- Execute a payload to establish Command and Control (C2) access on the compromised asset.
- Assessment of services, configurations, and Active Directory domain trust relationships within the internal network, with the goal of performing privilege escalation and lateral movement in the internal network.
- Establish persistence on the compromised asset and hosts laterally moved to.

Post-compromise breach simulation activities can assist your organization in understanding the following, through real-world exploitation attempts:

- The impact of the compromised asset, such as if the asset has trust relationships to other hosts in the internal network, is properly segmented in the network, or contains sensitive data valuable to malicious actors.

- The effectiveness of your defense-in-depth strategy, such as visibility provided by network and endpoint telemetry, as well as prevention technology that may block post-exploitation activities.

Successful breaches into your organization, as well as post-exploitation activities performed, will be recorded in the Vector Command portal. The breach log entries will assist your organization in confirming Rapid7's activities. The activity log can be used to compare the visibility provided through your organization's telemetry, as well as your security team's response to the breach.

Customer Service Interaction

The following section outlines activities your organization must perform to ensure you receive the most value out of services set forth by this Scope of Service.

ASM Asset Approval

Rapid7's Attack Surface Management technology will attempt to identify external exposures pertaining to your organization. You are responsible for reviewing discoveries and approving assets for ongoing Red Team operations.You are responsible for ensuring approved assets are owned by your organization and that Rapid7 is authorized to perform testing against the asset. Approved asset lists will only be picked up on the first day of each month by Rapid7's scanning engine and Red Team operators. You are responsible for approving new assets in-scope for testing prior to the start of each month. During the onboarding phase, after approving your assets, you will be provided with a one-time button to begin testing activities outside of the standard monthly cadence.

Allowlisting External Scanning Engines

To allow easy attribution of Rapid7's InsightVM scanning and initial exploitation attempts, activities will be conducted from known IP address ranges provided by your Cybersecurity Advisor. Rapid7 requires you to allowlist these IP addresses on your Intrusion Prevention Systems (IPS) to prevent automated blocking of scanning activities.

If Rapid7 identifies a vulnerability that is exploitable, the vulnerability will also be assessed from an IP outside of the allowlisted range to assess protections provided by your organization's IPS.

Electronic Social Engineering Operations

Rapid7's Red Team operators will perform ongoing reconnaissance to identify email addresses to phish within your organization. You are responsible for providing your Cybersecurity Advisor with a list of email addresses that are not to be targeted in Social Engineering campaigns.

Use the Vector Command reporting portal to identify Rapid7's Social Engineering operations conducted. Review your email gateway and security solutions to determine the effectiveness of phishing emails sent by Rapid7's team. If emails are blocked, you may choose to release them to employees to assess the effectiveness and impact of the phishing operation.

Assumed Post-Compromise Breach Simulation

Rapid7’s social engineering campaigns may leverage payloads which attempt to evade endpoint and network security controls, with the objective of performing Post-Compromise Breach Simulation activities as set forth in this Scope of Service. Your organization may choose to intentionally execute these payloads on an asset of your choosing to conduct an ‘assumed breach’ operation. This will allow your organization to assess your defenses against the crafted payload, as well as your visibility into post-compromise breach simulation activities.

Finding Status Management

You are responsible for reviewing findings opened in the Vector Command reporting portal. When your team has remediated a finding, you are responsible for updating the finding’s status in the Vector Command reporting portal.

Joint Requirements For Ensuring Success

To ensure your organization realizes the full value of Rapid7 Vector Command, both parties must share in the responsibilities and requirements of the partnership for the effective delivery of the service:

Rapid7 Responsibilities and Requirements

	Responsibilities and Requirements
1	Monitor your external environment as outlined in this Scope of Service, with the visibility provided by Rapid7’s Vector Command technology stack (ASM, InsightVM) and in conjunction with Red Team Operator’s manual activities.
2	Provide a security advisor (“Cybersecurity Advisor”) as the point-of-contact for the Vector Command relationship and to help accelerate your organization’s security maturity.
3	Provide a team of Red Team Operators to conduct an ongoing assessment of your organization’s perimeter exposures and defenses, as outlined in this Scope of Service.
4	Deliver service deliverables outlined in this Scope of Service within the Vector Command reporting portal.
6	Notify you of any Cybersecurity Advisor or service delivery changes.

Your Responsibilities and Requirements

	Responsibilities and Requirements
1	Acknowledge, accept, and adhere to all requirements and actions outlined in this Scope of Service.
2	Provide a list of out-of-scope email addresses and employees for social engineering operations. Notify your Cybersecurity Advisor of any changes to this list.
3	Review asset discoveries in Rapid7's ASM platform. Approve assets owned by your organization, which Rapid7 is authorized to conduct Red Team operations against.
4	Allowlist Rapid7's external scanning engine IP addresses.

Additional Terms

This Scope of Service is governed by the Rapid7 terms available at https://www.rapid7.com/legal/terms unless the parties have a fully executed agreement which supersedes such standard terms. Any responsibilities and/or actions not explicitly defined in this Scope of Service are not considered part of the Rapid7 Managed Vector Command Advanced service. Rapid7 may modify this Scope of Service at any time by posting a revised version here, which modifications will become effective as of the first day of the calendar month following the month in which they were first posted.

Exclusions

Full visibility of your internal attack surface is provided as part of our Surface Command, Exposure Command and Incident Command products and is not included with Vector Command or Vector Command Advanced. Connectors installed from the Rapid7 Extension Library are intended to enable dynamic discovery of registered domains and public IP networks via integrations with your IT management systems. If a customer is only licensed for Vector Command and Vector Command Advanced (and not separately licensed for additional Surface Command functionality through another offering), the customer acknowledges and agrees that they are only permitted to install Connectors to systems that manage their public/external domain and network space.

Vector Command SKUs include the following licenses:

- CAS - enables Vector Command-specific features such as testing approvals & PlexTrac reporting (the original name of Vector Command was Continuous Assessment Service, or CAS)
- ASM - Attack Surface Management, which includes:
    - EASM - enables external attack surface discovery services
    - CAASM - enables unified external and internal attack surface UI and connectors.Vector Command customers are provided with connectors solely for purposes of the upcoming Dynamic Discovery Seeds feature, which will leverage integrations with domain and network management tools (e.g., Markmonitor and NetBox) to automatically synchronize registered domains and managed public IP address spaces.