Scope of Service

Rapid7 Vector Command Advanced

Rapid7 Vector Command Advanced is a continuous red teaming service provided by Rapid7, bundled with a single, goal based Internal Network Pentest and Segmentation test. This Service offers an ongoing, proactive defense strategy to simulate real-world threat actors targeting your ("you", "Customer", "your organization", "your environment") organization as well as the benefit of meeting industry standard penetration and segmentation testing needs. Through integrating Rapid7's industry-leading vulnerability management, attack surface management, and expert penetration testing, we help identify, exploit, and report critical vulnerabilities before malicious actors can leverage them.

Vector Command is an advanced adversarial exposure validation service combining automated technology with expert human oversight to continuously monitor and assess your attack surface and exploitable exposures. 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 Advanced:

1. Continuous Attack Surface Monitoring & Management:
    - 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 vulnerabilities and 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.
10. One time Internal Network Penetration Test and Segmentation test
    - Goal-Based Internal Network Penetration Test
        i. Testing to be achieved via virtual machine (vPTK) provided by Rapid7,which the customer will deploy to establish connectivity to the customer's internal network (See your Vector Command Specialist for Scope Details)
    - Attacks include but not limited to:
        i. Attempt to gain direct or indirect access to segmented network areas
        ii. Attempt to gain elevated access within customer environment
        iii. Attempt to gain access to customer sensitive data
        iv. Testing to be conducted remotely & during Rapid7 standard business hours
    - Network Segmentation Testing
        i. Testing of Segmentation Boundaries (See your Vector Command Specialist for Scope Details)
            1. Each boundary not to exceed a /21 CIDR (2,048 IP addresses)
            2. Rapid7's vPTK must be 'whitelisted' on any Firewalls silently dropping packets or the firewall rule set to DENY rather then DROP
        ii. Report services and ports exposed across boundaries
    - Remediation Validation
        i. Proportionally sized, single (1) remediation validation included to validate any findings corrected.
11. Internal Network and Segmentation Findings Report
    - Rapid7's final report provides an independent, point-in-time assessment of vulnerabilities from the perspective of a malicious actor. The final report consists of the following:
        i. Executive Summary, Key Findings and Recommendation, Threat Ranking Methodology, Assessment Storyboard, Findings and Remediation Guidance, Appendices
    - Rapid7's standard Final Report will go through a Quality Assurance (QA) process, with the final deliverable provided within ten (10) business days from the completion of services, unless otherwise agreed upon by the parties.
    - Additional Documentation Provided:
        i. Rapid7's Customer-Facing Document (CFD)
        ii. Rapid7's Letter of Attestation (LOA) Engagement Type and Date Conducted
        iii. Unless otherwise specified, a standard CFD and LOA will be delivered with the Final Report.
12. Debrief of pentest findings
    - Upon delivery of the final report, Rapid7 will conduct a debrief call to review the final report findings.

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 Advanced service which includes:

- Rapid7 Managed Team
- Rapid7 Supporting Teams
- Rapid7 Technology
- Service Deliverables
- Vector Command Specialist
- Project Manager (PM) Engagement
- Continuous Red Team Operations
- Customer Service Interaction
- Joint Responsibilities
- Appendix

Rapid7 Managed Team

Vector Command Specialist

Your Vector CommandSpecialist 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 Vector Command Specialist, 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 Vector Command Specialist will communicate remediation and mitigation improvements using specific and adaptive reports and periodic business reviews. The Vector Command Specialist will assist your team in navigating and approving assets in the external attack surface management portal, highlighting new assets or requesting updates to assets that need approval status changes.

Red Team Operators

The primary objective of the 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.

Pentest Project Manager

The primary objective of the Pentest Project Manager ("PM") is to ensure that the internal network and segmentation test is planned, scheduled, and conducted. The PM will engage with your team to review your goals for the internal network and segmentation test, ensure you are provided the virtual machine for testing, and manage the scheduling and delivery of your penetration test services. The PM will work in collaboration with the CA to ensure all parties are informed of the testing activities and associated meetings are arranged.

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.
Virtual Penetration Testing Kit (vPTK)	In order to deliver the Internal portion of Vector Command Advanced, Rapid7 will provide you with a virtual machine in the form of an ISO and/or OVA that should be deployed in your environment before the start of the internal network penetration test and segmentation test. This vPTK provides Network Connectivity into your internal Network for the Rapid7 Team to perform internal testing.
Customer Portal	Communication with your Vector Command Specialist 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 Advanced deliverables during the term of your 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.
Internal Network and Segmentation Testing Report	Rapid7's Final Report provides an independent, point-in-time assessment of vulnerabilities from the perspective of a malicious actor. The Final Report consists of the following: Executive Summary: ● Executive-Level Discussion of the Assessment, including the Objectives and Findings ● High-Level Overview of Scope ● Explanation of Constraints (If Applicable) ● Key Findings and Recommendations: ● Overview of up to Five Key Findings with Summarized Recommendations ● Threat Ranking Methodology: ● High-Level Overview of the National Institute of Standards and Technology (NIST) 800-30-based Risk Scoring Methodology Assessment Storyboard: ● Walkthrough of Multi-Step Exploitations to Help Customer Understand Risk ● High-Level Overview of penetration testing activities in the case of a minimal to no findings report to show work ● Findings and Remediation Guidance: ● Risk Scoring, Summary of Findings, and Validation Steps ● Detailed Recommendations

	● Links to Related References (If Applicable) Appendices: ● Scope and Rules of Engagement ● Requirements, Scope, and Assumptions ● Applicable Methodology ● Additional Documentation (If Applicable) Rapid7's standard Final Report will go through a Quality Assurance (QA) process, with the final deliverable provided within ten (10) business days from the completion of services, unless otherwise agreed upon by the parties.
CFDs and LOAs	Rapid7's Customer-Facing Document (CFD) is a high-level summary of a penetration test that describes Rapid7's methodology and provides the number of vulnerabilities per NIST 800-30-based risk rating discovered during the engagement. Rapid7's CFD consists of the following: ● Engagement Type and Date Conducted ● Number of Findings per Risk Rating ● Threat Ranking Methodology ● Reporting Methodology Rapid7's Letter of Attestation (LOA) states that Rapid7 has completed services as they are currently outlined in the SOW, and that testing was designed to provide the customer with an independent, point-in-time assessment from the perspective of a malicious actor in accordance with the Center for Internet Security (CIS) Controls, NIST, and additional guidelines, if applicable. Rapid7's LOA consists of the following: ● Engagement Type and Date Conducted ● Objectives ● Overview of Methodology and Areas Evaluated Unless otherwise specified, a standard CFD and LOA will be delivered with the Final Report.

Vector Command Specialist Engagement

During the term of your Vector Command Advanced service, you will regularly engage with your Vector Command Specialist. 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 Vector Command Specialist:

Communication	Frequency	Method	Description
Customer Requested Meeting	Ad-Hoc, requested through Online Support Portal and subject to Vector Command Specialist availability	Online Customer Portal, phone or screen share	Meeting with Vector Command Specialist to address concerns or questions regarding this service.
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 Vector Command Specialist 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 Vector Command Specialistwill 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 Vector Command Specialist will assess the request and schedule a meeting with an appropriate member of the Red Team operators to discuss the finding in-depth.
Internal Network & Segmentation Test Findings Report, CFD, and LOA Debrief	1x per contract	Virtual	PM, Vector Command Specialist and Internal Network and Segmentation Test Consultant will review and discuss the findings approximately 2-3 weeks after the completion of the test. .

Activating Your Vector Command Advanced Service

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

1. Your assigned Vector Command Specialist will schedule an initial kickoff call with you and your team to explain Rapid7's Vector Command Advanced 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.

Upon completion of the steps mentioned above, Rapid7 will then review your internal network and network segmentation testing actions as well as schedule testing with you. Internal network segmentation test will be conducted subject to availability of Rapid7 resources, at Rapid7 discretion. Testing to occur within the subscription window.

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.

Internal Network and Segmentation Testing

Goal-Based Internal Network Penetration and Segmentation Test

- Before the start of engagement Customers will deploy a virtual machine (vPTK) provided by Rapid7 to establish connectivity to your internal network. (vPTK placement to be discussed with your CA and Project Manager)
- Phase 1 – Network Segmentation Testing / Testing of Segmentation Boundaries
    - Package scope and boundary limits to be reviewed with your CA and Project manager upon onboarding.
    - Rapid7 will report on services and ports exposed across boundaries
- Phase 2 – Network Penetration Test
    - Testing will be goal based (your Rapid7 will provide you the allocation of days of service):
    - Attempt to gain direct or indirect access to segmented network areas
    - Attempt to gain elevated access within your environment
    - Attempt to gain access to your sensitive data
    - Testing to be conducted remotely & during Rapid7 standard business hours
    - Qualified personnel provided by Rapid7 will perform all work. Unless otherwise defined in the price quotation and SOW, Rapid7's responsibilities are limited to the work defined by this SOW and attached quotation.
    - All work to be conducted remotely & during Rapid7 standard Business hours.

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.

ASM Asset Categorizations

Within Rapid7's Attack Surface Management platform, you may classify assets with the following approval or disapproval categories:

Categorization	Description
Approved	You confirm this asset (IP and domain) is owned by your organization and that Rapid7 is authorized to perform full vulnerability scanning, penetration testing, and

	red teaming activities against the asset.
Not Allowed	You own this asset, but it is excluded from testing. External Attack Surface Management (EASM) discovery can still use this asset as a data point for finding other related external exposures.
Software as a Service (SaaS)	While these assets are part of your organization's attack surface, the underlying host operating system and software are managed by a third-party provider. Rapid7 is not authorized to perform direct penetration testing or CVE exploitation against the hosted software or infrastructure. However, Rapid7 is authorized to assess these assets for organizational risks, including: • **Misconfigurations:** Identifying settings that expose sensitive data or administrative functionality. • **Data Exposure:** Locating unprotected sensitive information accessible via the service. • **Identity Risks**: Testing authentication and conditional access using compromised employee credentials. • **Registration:** Identifying account registrations that could be leveraged as an initial entry point into your organization. SaaS will be assessed as a potential entry point into your organization, focusing on how an adversary can exploit identities and exposures in other attacks against assets you own.
Not Owned	This asset is not owned by your organization. It will be removed from future attack surface management discoveries, and will not be used as a data point for future attack surface management discoveries.

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 Vector Command Specialist. 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 Vector Command Specialist 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.

Scheduling Network and Segmentation Testing

Rapid7 will provide setup support during your initial onboarding. You will have the added benefit of a project manager available to support the scheduling and delivery of your internal network penetration test, segmentation test, and remediation validation. Please work with your CA and Project Manager as appropriate to provide any blackout dates testing cannot occur, the contact information of those from your team who will participate in setup and support of the testing, and deploy the vPTK prior to testing.

Note - Internal Network and Segmentation testing will be scheduled based upon Rapid7 availability with consideration of customer blackout dates. Scheduling will occur no sooner than 8 weeks from order placement date.

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 Vector Command Specialist 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 support team or service delivery changes.
7	Provide consultants with industry-standard training and certifications to effectively interact with your personnel and conduct the Services.
8	Provide the appropriate tools, when such are required, to perform the service.
9	Provide a dedicated Project Manager to facilitate the logistical details and work in conjunction with the CA to accelerate your organization's security maturity of the internal network and network segmentation testing activities.

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 Vector Command Specialist 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.
5	Prior to the internal network and segmentation test engagement: ● Designate a point of contact to work with Rapid7. ● Ensure all key network, security, or other Customer personnel are accessible as necessary for services. ● Provide Rapid7 with a list of relevant documentation (i.e., policies, procedures, diagrams, flow charts, etc.) necessary for the provision of services. ● Provide necessary access to the systems and applications in scope; including deployment of PTKs to necessary parts of the customer environment.. ● Work with the appointed Rapid7 Project Manager to schedule the internal network and

segmentation test.
- Work Hours: Services are performed between Rapid7 standard business hours, 8:30 AM to 5:00 PM local time, Monday through Friday, excluding nationally observed holidays, and in contiguous business days once commenced unless otherwise agreed upon in advance.

Rescheduling:
- Your team may request rescheduling the services up to ten business days' prior to the start of the services.
- Services may be rescheduled within 12 months of order placement, if testing is not completed within the 12 month contract period customer would forfeit such services.

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 & Disclaimers

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.

Customer warrants and represents that it is the owner of any network, systems, IP addresses, and/or computers upon which Rapid7 performs the Services ("Customer Systems"), or that Customer is authorized to instruct Rapid7 to perform Services on such Customer Systems pursuant to this Scope of Service. Customer shall indemnify and hold harmless Rapid7 for any claims by any third parties with respect to a breach of the foregoing warranty. Customer further understands that any customization (such as scripting)

provided by Rapid7 as part of a services engagement are provided for the current Customer environment and the current version(s) of in-scope products only. As such, any changes to the Customer environment or future Rapid7 product upgrades or updates may cause the customization to become incompatible, and any further customization required as a result of such changes is outside the scope of this SOW.

Offboarding

In the event that you choose not to renew your Vector Command services, an offboarding process will begin during your final active month. During this transition period, Rapid7's Vector Command managed services team will assist with exporting all monthly reports, letters of attestation, and findings in PDF format. On the final day of your contract, access to the Vector Command platform (including the Attack Surface Management and Reporting Portal) will be deactivated. Rapid7 will retain your attack surface management and penetration testing report data for up to ninety (90) days following contract termination, should your team require additional information.