Scope of Service

Rapid7 Managed Detection and Response (MDR Elite)

The Rapid7 MDR service is delivered as a collaboration between Rapid7 and the customer ("you", "your team", "your organization", "your environment"). The mission of Rapid7's MDR service is to leverage our experts to collaboratively advance your cybersecurity decision-making and maturity through our tailored guidance.

We pride ourselves on becoming a true extension of your security team. Our goal is to partner together to enhance your 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 your security posture.

Any responsibilities and/or actions not explicitly defined in this Scope of Service are not considered part of the Rapid7 MDR Elite service. Additional details can be seen in the MDR Responsibilities Matrix.

All terminology not defined in this document can be viewed at: services.help.rapid7.com/docs/mdr-terms.

Joint Requirements For Ensuring Success

To ensure your organization realizes the full value of Rapid7 MDR, it is critical that both parties share in the responsibilities and requirements of the partnership for effective delivery of the MDR service:

Rapid7 Responsibilities and Requirements

	Responsibilities and Requirements
1	Monitor the customer's environment in accordance with the detection methodologies outlined in this Scope of Service and with the visibility provided by the Rapid7 MDR technology stack (InsightIDR & Insight Agent), and in conjunction with the event sources configured in InsightIDR from the customer environment.
2	Provide a knowledgeable information security professional with subject matter expertise in Rapid7 products to assist with the deployment of required and optional product features.
3	Provide a named security advisor ("Customer Advisor") as the point-of-contact for the MDR relationship and help to accelerate the customer's security maturity.
4	Perform Remote Incident Response engagement in addition to standard alert and incident investigations.
5	Provisioning and ongoing management of Rapid7 cloud services in the technology stack.
6	Delivery of all reports via the Rapid7 Services Portal in accordance with this Scope of Service.
7	Notify the customer to any Customer Advisor or service delivery changes to Rapid7 MDR.

Customer Responsibilities and Requirements

	Responsibilities and Requirements
1	Acknowledge, accept, and adhere to all requirements and actions outlined in this Scope of Service
2	License all endpoints within the in-scope environment(s). The in-scope environment(s) must be 'logically separated' from any other out-of-scope environments.
3	Designate a Point-of-Contact to work with Rapid7 for deployment and onboarding.
3a	Complete the Solution Alignment survey prior to starting the deployment.
3b	Complete the Service Activation Request form prior to being placed in service.
3c	Provide Rapid7 with relevant documentation (i.e., policies, procedures, diagrams, flow charts, etc.) so the MDR service can fit seamlessly into your process, including an escalation path for reporting incidents.

4 **Deploy Insight Agents** to all workstation, desktop, and server assets in the in-scope environment(s) and **connect all Insight Agents** to InsightIDR.
- Assets without the Insight Agent deployed will not be fully supported by the MDR service.
- Performing a Compromise Assessment and Monthly Threat Hunts require deployment of Insight Agents to at least 80% of the in-scope environment.

4a Ensure the Rapid7 Insight Agent is up to date. The Rapid7 MDR service supports the current version of the Agent and up to two previous versions as signified by a change in either the ones (x), tenths (y) or hundredths (z) of a version (x.y.z).

5 Allocate and configure **Insight Collector(s)**. At least one Insight Collector must be provisioned. The collector is required in order to:
- Collect the event sources described in 6 and 7.
- Proxy connections from 'on premise' InsightAgents to the Insight Platform.

6 Connect **all available recommended data sources** to InsightIDR for each in-scope environment and ensure availability and connectivity to Rapid7 infrastructure for all MDR technology and Event Sources.

6a For organizations that have Microsoft Windows domains, send the **Windows Security event logs** from each domain controller to InsightIDR using one of the supported methods. Without this event source, many of Rapid7 MDR's UBA detections will not be supported.

6b For organizations that have Microsoft Windows domains, Microsoft Azure AD Domain Services, or Amazon AWS Domain Services, connect at least one **LDAP event source** for each domain. Without this event source, Rapid7 MDR will not have vital contextual information about users in your environment.

6c Connect all supported **DHCP** log sources to InsightIDR. Without this event source, Rapid7 MDR's SOC may not be able to accurately attribute network traffic to the appropriate assets in your environment.

6d Connect all supported network logs - **DNS, firewall, VPN,** and **Web Proxy** - to InsightIDR, particularly those network devices at your Internet egress points. These log sources are extensively used for real-time threat detection, hunting, and investigations.

6e Connect all supported **Cloud Service** logs to InsightIDR. These log sources are extensively used for real-time threat detection, hunting, and investigations.

6f Deploy **Insight Network Sensors** in your environment to analyze and log network traffic data.

6g Set up **Honey Credentials, Honey Users, Honey files** and **Honeypots**.

7 Connect **any other security-relevant event sources** to InsightIDR
Note: All connected event sources may be leveraged for investigation and incident response purposes. Not all event sources will be used for real-time threat detection or hunting. For more detail, see 'Event Sources'.

8 Notify Rapid7 to any personnel, technology, event source, or point-of-contact changes or modifications.

9 Configure the InsightIDR instance in accordance with the recommendations from Rapid7's deployment team and Customer Advisors.

10 Review alerts that are not in-scope for the MDR service. These alerts will **not** be reviewed by the MDR SOC. See 'Alert Review Limitations' appendix for details.

11 Respond to 'Requests for Information' (RFIs) from the MDR SOC regarding specific alerts. These requests may be sent via e-mail or as cases in the Support Portal. The MDR SOC requires additional feedback from the customer in order to accurately assess these alerts.

Security Expertise

The MDR team is composed of a named **Customer Advisor,** the customer's **MDR SOC "Pod"**, and the **Rapid7 Threat Intelligence Team**.

Customer Advisor

Your **Customer Advisor ("CA")** is the main point-of-contact for the Rapid7 MDR service. This named resource works with your team as a strategic security partner—from initial technology deployment through incident remediation and ongoing security consultation—to shepherd your organization's security maturity. Your CA will be assigned to your organization at the time of your Service Delivery Kickoff call.

Throughout the service your CA will frequently communicate with your team to provide updates on service delivery, reporting, metrics, technology health, and ensure we are helping you address your security goals. Additionally, each CA is aligned to your assigned MDR SOC Pod ("Pod") to maintain constant communication and understand all relevant knowledge pertaining to investigations and incidents.

MDR SOC Pod

Your organization's environment will be assigned to one of our **SOC Pods** staffed by our world-class analysts to ensure continuous 24x7x365 monitoring coverage for real-time alert investigation, threat hunting, and incident response. Pods are comprised of three levels of Security Analysts and managed by a Pod Lead:

Analyst	Distribution	Description
Associate Analyst	3 per Pod	Responsible for alert triage and investigation and threat hunting.
Analyst	2 per Pod	Responsible for alert triage and investigation, threat hunting, alert tuning, and supporting Remote Incident Response engagements.
Senior Analyst	1 per Pod	Responsible for alert tuning, threat hunting, leading Remote Incident Response engagements, training other analysts, and handles escalated investigations.
Pod Lead	1 per Pod	Manages the SOC teams. Responsible (along with the named Customer Advisor) for the MDR service delivered to their team's assigned customers.

Threat Intelligence Team

Rapid7's **Threat Intelligence team** supports the MDR SOC and CAs with threat analysis and detections for new vulnerabilities, exploits, and attack campaigns found via their research. These new detections are added as detections for all MDR customers.

MDR Technology

The Rapid7 MDR service is powered by InsightIDR, Rapid7's own threat-focused Cloud SIEM, Endpoint Detection and Response (EDR), and User Behavior Analytics (UBA) solution, to provide comprehensive protection against intruders in your organizations internal network, devices, and cloud services. InsightIDR and the MDR SOC leverage the Insight Agent and other event sources from your existing security infrastructure to ensure visibility into threats across the environment.

A full list of all Rapid7 cloud technologies and customer-deployed software leveraged by the Rapid7 MDR service can be viewed at services.help.rapid7.com/docs/mdr-terms.

InsightIDR Instance Set-Up

By default, the MDR Elite service includes a single instance of InsightIDR for your entire organization. All log sources will be onboarded to this single instance. Additionally, all Insight Platform users (on both InsightIDR & Services Portal) will be assigned to, and will have access to, all data stored within this single instance.

In some cases, your business may want to deploy the MDR service to multiple 'organizations' as separate InsightIDR instances to provide separate visibility and reporting across these 'logically separated' organizations (such as business units). Details on the MDR service delivery for additional organizations can be provided in an additional Addendum titled "*Scope of Service Addendum - Additional Organizations*".

In-Scope Environment for MDR

Rapid7 MDR requires licensing and deployment of the Insight Agent across your organization's entire environment to have the best coverage and monitoring of malicious activity. In certain instances, your team may choose to license a partial portion of your environment for MDR ("in-scope") as long as this environment meets the qualifications of a 'logically separated' environment. For example, an Internet-facing production data center that is separate from your corporate IT end-user environment. Or your environment may include multiple subsidiaries with logically separate IT infrastructures.

In these situations, Rapid7 recommends that your organization deploy our MDR service to all of your environments for the following reasons:

- Attackers often move laterally within an organization from one environment to another, and without a full deployment to all environments we may be unable to detect or respond to the full scope of an attack.
- If traffic/activity from 'out of scope' environments is logged by 'in scope environments', this causes additional detection and response work for the MDR SOC that your business is not licensed for.

However, Rapid7 MDR will still support only a subset of their logically separated environments if required by your team. When determining if one or more environments are 'logically separated' and therefore can be considered in-scope, consider the following criteria:

- Do the environment(s) have their own authentication and access control infrastructure? Specifically, do they have their own Windows domain?
- Are the environment(s) on a network that are logically segmented from the in-scope environment(s)?
- Does the environment(s) serve a distinctly different purpose than other environments? For example, a production data center (versus a corporate IT end user network).
- Do the environment(s) have their own Internet egress points?

If the in-scope environment(s) meets the criteria above **and** your team accepts the risk of a limited deployment of the Insight Agent in their in-scope environment, we can consider this a partial deployment and exclude other 'out of scope' environment(s) from MDR licensing and deployment.

Detection Methodologies

Below are the detection methodologies employed by the Rapid7 MDR to detect anomalous and malicious activity:

Detection Method	Description
User Behavior Analytics (UBA)	InsightIDR creates a baseline of normal user activity within your environment and generates alerts when there is a deviation.
Attacker Behavior Analytics (ABA)	InsightIDR applies behavioral analytics to generate alerts, built from our experience and understanding of attacker tools, tactics, procedures, and methodologies.
Network Traffic Analysis (NTA)	InsightIDR detects intrusions or other potential security events on your network through traffic analysis.
Threat Intelligence Detections (Intel)	Proprietary threat intelligence indicators derived from research, previous investigations, MDR monitoring findings, and third-party sources.
Threat Hunting	The MDR team performs monthly forensic analysis based on Insight Agent data and other log sources to identify unknown threats in your environment based on emerging trends in the threat landscape. Threat hunting requires deployment of the Insight Agent to at least 80% of your logically separated environment.

Event Sources

InsightIDR supports a wide range of security-relevant event sources. These event sources are leveraged by the MDR SOC as described in the table below. Specifically:

- **Real-time detection**: These sources are processed by our threat detection engine and may generate real-time alerts that are reviewed by our 24x7x365 SOC.
- **Threat Hunting**: Data from these sources are aggregated and leveraged by analysts when performing monthly threat hunts.
- **Investigation**: Data from these sources may be leveraged to accurately attribute other activity to an asset or user, and to provide other useful context data in the course of investigating alerts or performing Remote Incident Response.

Source	Real-time Detection				Threat Hunting	Investigation	
	UBA	ABA	NTA	Intel		Asset/User Attribution	Log Search
Insight Agents	✓	✓		✓	✓	✓	✓
Active Directory	✓	✓		✓	✓		✓
VPN Logs	✓	✓		✓	✓		✓
Cloud Services Logs	✓	✓		✓	✓		✓
Deception Technology	✓						✓
DNS Logs		✓		✓	✓		✓
Firewall Logs		✓		✓	✓		✓
Web Proxy Logs		✓		✓	✓		✓
Insight Network Sensor			✓	✓			✓
DHCP						✓	✓
LDAP						✓	
All Other Log Types							✓

See the full list of event sources supported by InsightIDR: insightidr.help.rapid7.com/docs/insightidr-event-sources.

Data Retention Policy

MDR offers your organization unlimited data ingestion into InsightIDR with access to 12 months hot storage and one month cold storage. Your team can add or remove event sources with no incremental data charges, with exception to Insight Agents which must be licensed and deployed to as much of your entire environment as possible. Exporting data is possible, but must be set up on a separate S3 bucket instance managed by your team and limited to a go-forward basis.

Deployment and Configuration Tasks

We encourage your team to begin the deployment as soon as possible by self-deploying InsightIDR in your environment. If deployment assistance is requested, Rapid7 will assign a Product Consultant to work with your team to ensure a successful and timely deployment. To expedite this deployment process, we ask that your team also elect a Project Manager to expedite the process.

Deployment Process

The Rapid7 InsightIDR product can be deployed with or without the assistance of a Rapid7 Product Consultant. After purchasing Rapid7 MDR, you will be sent a welcome email that explains your options for both self-deployment and scheduling time with a Rapid7 Product Consultant ("Deployment Sessions").

While you have the option to complete deployment on your own and go directly into service, an enablement session with a Product Consultant is still highly encouraged.

If you opt to work with a Product Consultant, Rapid7 recommends that you begin deployment on your own and then work with a Product Consultant to complete any outstanding items, answer questions, and get enablement on the product.

Deployment Sessions

Upon completion of the pre-deployment tasks, your team can leverage remote deployment assistance with a Rapid7 Product Services Consultant. This assistance should not to exceed 3 sessions, but can be reviewed on a case-by-case basis for complex environments.

During the Deployment Session(s), your assigned Rapid7 Product Consultant will assist your team with any remaining InsightIDR deployment related tasks, including the configuration of Collectors, event sources and product settings. Rapid7 will not assist the customer with agent roll-outs. Custom integrations, additional deployment time, training, and other services are not included in the Deployment Sessions and must be purchased separately.

Activating your MDR Service

In order to activate your MDR service, you must fill out a Service Request Form to provide Rapid7 with information regarding your environment. You will be provided with a link to this form in your welcome email. Once you have completed this form and had a kickoff meeting with your Customer Advisor, your service will begin.

InsightIDR Access

Rapid7 MDR has the right to access your InsightIDR instance as necessary to deliver service/support. A list of users who have access to Rapid7 InsightIDR can be seen inside the product. Your team is required to add users for your organization to InsightIDR; Rapid7 will not add users for your organization to InsightIDR once the Deployment Phase is completed. In the case that all of your organization's existing Insight Platform Admins are no longer with the organization, someone from your organization must provide Rapid7 a written request for access.

Compromise Assessment

Once your team has deployed the Insight Agent to 80% or more of endpoints in your in-scope environment, a Compromise Assessment will be performed.

Deliverable	Frequency	Description
Compromise Assessment	One-time	After deployment, Rapid7 MDR will evaluate whether there is malicious activity in your network or evidence of previous compromise(s). This report contains any detected active or historic compromises, potential avenues for future breaches, and prioritized remediation and mitigation recommendations.

If the Compromise Assessment finds that there is currently a compromise or detected malicious activity, Rapid7 will suggest that you utilize one of your Remote Incident Response engagements.

Validation of Alerts

When a threat is detected, your assigned Pod of analysts will act as an extension of your team, manually validating each detection by gathering context from your endpoints and logs to assess the severity. Validation is defined as

the Rapid7 MDR SOC performing initial triage and investigation to determine with a high degree of confidence that the event is non-benign and requires a communication to your security team.

Threat Findings and Reporting

Rapid7 MDR service reports are delivered via the Rapid7 secure file transfer system located in the Rapid7 Services Portal. These include:

Deliverable	Frequency	Description
Findings Report	Ad-hoc, after validated attacker activity	Provides written analysis ("attack storyboard"), criticality, raw details, remediation and mitigation recommendations, and suggested containment actions at the conclusion of each validated incident investigation. Rapid7 will notify the customer of any malicious activity ("incident") discovered via your preferred method within the timeframes outlined in the 'Response Times'.
Hunt Reports	Monthly	Once your compromise assessment is complete, you will begin receiving monthly hunt reports. These reports provide metrics and findings related to endpoint forensic analysis activities performed by the MDR analysts. Our analysts leverage the Rapid7 Insight Agent to collect metadata from multiple locations on the customer's endpoints to identify persistent malware, historical application execution, unusual processes and network communications, and per-system anomalies.
Monthly Service Reports	Monthly	Provides metrics and context surrounding analysis activities, technology health, and findings summaries for an at-a-glance overview of MDR activities.
Quarterly Service Reports	Quarterly	Provides metrics and context surrounding analysis activities, technology health, and findings summaries for an at-a-glance overview of MDR activities for the customer.
Threat Intelligence Reports	Ad-hoc, MDR finds new attack patterns	Provides a highly targeted analysis of new and emerging threats to inform the customer of the findings based on Rapid7's Threat Intelligence infrastructure or third-party threat intelligence partners.

Response Actions

You have the option to enable the Active Response service capability. Active Response gives your security program immediate response capabilities—initiated by our MDR experts—to stop attacks and contain confirmed threats in your environment. Details on the 'Active Response' service capability for MDR Elite customers can be provided in an additional Addendum titled "Scope of Service Addendum - Active Response".

Customer Advisor Engagement

During the course of your MDR service, your team will engage with your assigned CA. This resource is available to answer any questions about the MDR service and offer security advisorship to advance your security maturity.

Customer Advisors are available during normal business hours by phone and email. During non-business hours, a member of the CA team is on-call via the CA Hotline if malicious activity is detected in your environment.

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

Communication	Frequency	Method	Description
Monthly Meeting	Scheduled Monthly	Online, Phone, or Screen Share	• Review monthly hunt reports • Address questions about alerts • Walk through threat intel reports • Build custom alerts or other use cases • Answer questions related to the current program

Request For Information (RFI)	Ad-Hoc, when SOC analysts need additional details	Email from CA to Customer	When an incident is identified and the MDR SOC needs additional context (input from you), your CA will reach out via email to ask for more information to assist the investigation. (Ex. user running an abnormal process that we must confirm is related to malicious activity or intentional).
Findings Report Communication	Ad-Hoc, with Findings Report	Phone and/or Customer Portal	CA notifies you of a validated incident and presents remediation recommendations.
Quarterly Service Review	Quarterly	Online, Phone, or Screen Share	CA will walk through a summary of the service for the quarter and present customer recommendations for how to further advance your security maturity.
Customer Requested Meeting	Ad-Hoc, requested through Online Support Portal	Online, Phone, or Screen Share	You request a meeting to address concerns or questions regarding the service, technology, or alerts with your CA -- both for Rapid7 MDR or outside of Rapid7 advice.
Customer Questions	Unlimited, Ad-Hoc	Online Support Portal	You can leverage the online Support Portal to request help or voice concerns/questions.

Remote Incident Response

Remote Incident Response ("Remote IR") engagement is a technical response process handled remotely by the Managed Services SOC team. The customer is allotted two (2) Remote IR engagements per contract year.

Customers will be able to invoke a Remote IR for any incident discovered -- by the customer or the Managed Services SOC -- in the in-scope environment at any time after contract execution. An 'incident' is defined as 'a confirmed or reasonably suspected compromise of customer systems or data'. An 'in-scope environment' is one in which the customer has either deployed or is licensed to deploy the MDR service. This would include all systems for which an Insight Agent license has been purchased, and all common cloud services used by customer users.

In the event of a validated security incident, the customer will have the option to exercise a Remote IR engagement per the service level objectives outlined below:

Activity	Definition
Remote Technical Analysis & Incident Scoping	Analysis of any data source including data generated by the Insight Agent, and other analysis techniques to include full disk forensics.
Communications & Updates	Daily verbal debrief of the day's investigation results and progress. Substantive findings (such as increase in incident scope or impact) will be communicated regularly as discovered. Written weekly Summary Status Reports will be produced if engagement exceeds a week.
Remote Incident Response Report	This report will provide an overview of the Incident and a retrospective to include an executive summary, findings details, analysis, root cause, and recommendations, within 10 business days from completion of investigation

Additionally, you may use a Remote Incident Response engagement to test your MDR security control during a Penetration Testing engagement (through Rapid7 or otherwise). Details are available in the Appendix section titled, "MDR Reporting During Penetration Testing".

Service Level Objectives

Response Times

The following response times are included as a part of the Rapid7 Managed Detection and Response service:

Investigation Validation Response Time

Based on the level of severity of an incident, the MDR team will alert you per the response times outlined in the table below. It should be noted, criticality of an event is determined by the Rapid7 MDR SOC during the course of an investigation into an identified event. It is not possible to assign criticality before the scope of the event is determined and the incident is validated.

Severity	Example behaviors	Target time to notification	Time to Findings Report
Critical	An incident created via non-commodity malware deployed via spearphishing, social engineering, zero-day exploitation, or strategic web compromise, specifically targeted towards a target or organization.	Within one (1) hour of validation; Ongoing communications as they become available, but at a minimum, every 4 hours. Significant findings will be communicated as they are identified.	Findings Report will be posted in the Services Portal within 24 hours upon completion of investigation
High	An incident created using targeted off-the-shelf software backdoor deployed via spearphishing, social engineering, or strategic web compromises. Planned and targeted, but using common malware.	Within one (1) hour of validation; Ongoing communications as they become available, but at a minimum, every 4 hours. Significant findings will be communicated as they are identified.	Findings Report will be posted in the Services Portal within 24 hours upon completion of investigation
Medium	An incident created using common threat malware, typically non specifically targeted, but rather opportunistic and automatic.	Within eight (8) hours of validation; Ongoing communications as they become available. Significant findings will be communicated as they are identified.	Findings Report will be posted in the Services Portal within 24 hours upon completion of investigation
Low	An low-risk threat, not capable of remote code execution, credential harvesting, or data theft. (ex: Spam email delivering adware).	Within eight (8) hours of validation; Ongoing communications as they become available. Significant findings will occur as they are identified.	Findings Report will be posted in the Services Portal within 24 hours upon completion of investigation

Customer Advisor Response Times

The Customer Advisor team is held to the following response times for notifications of validated threats:

Trigger	Time to Action	Method	Action
Critical Severity Threat	Up to 1 hour after posting the RFI	Phone	Proactively reach out to the customer for validated critical severity threats by phone to provide relevant details while the SOC generates a Findings report.
High Severity Threat	Up to 1 hour after posting the RFI	Phone	Proactively reach out to the customer for validated high severity threats by phone to provide relevant details while the SOC generates a Findings report.
Medium Severity Threat	Up to 1 hour after posting the RFI	Email	Proactively reach out to the customer for validated medium severity threats by email to provide relevant details while the SOC generates a Findings report.
Low Severity Threat	Up to 1 hour after posting the RFI	Email	Proactively reach out to the customer for validated low severity threats by email to provide relevant details while the SOC generates a Findings report.

The following are response times to inquiries from your team:

Response Trigger	Time to Action	Action
Urgent Request	2 business hours	Reactively respond to an urgent request from the customer's team. Urgency is based on the discretion of the Customer Advisor team.
Non-urgent Request	24 business hours	Reactively respond to a non-urgent request from the customer's team. Urgency is based on the discretion of the Customer Advisor team.

Remote Incident Response

Each Remote IR is governed to the response times outlined below:

Action	Time to Action
Remote IR Trigger	Remote IR will begin as requested by the customer, or once any investigation performed by the MDR SOC exceeds 8 hours.
Time to begin Remote IR	1 hour from customer request/approval to initiate Remote IR.

Technology Uptime

Rapid7 InsightIDR and the Insight Platform, which powers the MDR service, follows the same uptime availability reflected by Rapid7's overall Insight Platform Service Level Agreement.

Additional Terms

This Scope of Services contract is governed by Rapid7's standard Master Services Agreement available at https://www.rapid7.com/legal/terms/ unless the parties have a fully executed Master Services Agreement which supersedes such standard terms. Any changes in materials or scope of work as defined in this document must be agreed upon in writing by the customer and Rapid7. Customer deployed software and related services are governed by the Rapid7 Terms of Service available at https://www.rapid7.com/legal/terms.

Signature

The undersigned has read, understands, and agrees to the Rapid7 MDR Scope of Service (including Appendix).

Company	**Hidalgo County**	Title	**County Judge**
Signature	Richard F Cortez	Name	**Richard F. Cortez**
Date	3/14/22		

Rapid7

DocuSigned by:
F14E329C654B4E7...

10-Mar-2022

General Counsel

Peter Kaes

APPROVED BY COMMISSIONERS COURT ON: 3/8/22

APPENDIX

MDR Responsibilities Matrix

	Rapid7	Main POC	Security & IT	C-Suite
Initiation Phase				
Complete Site Survey		✓	✓	
Define internal remediation escalation path(s) for MDR reporting		✓		
Set up customer in InsightIDR	✓			
Enable customer in customer's services portal	✓			
Deployment Phase				
Deployment Intro call	✓	✓		
Download and install Collectors		✓		
Deploy Insight Agent to all servers and workstations		✓	✓	
Deploy Insight Network Sensor(s)		✓	✓	
Install Orchestrator and workflows		✓	✓	
Configure event sources				
Configure all required event sources	✓	✓		
Optional - Configure recommended event sources (if available); Ex. Firewall, VPN, Web Proxy	✓	✓		
Firewall rules complete		✓		
Deploy Deception Technologies				
Deploy honeypots		✓	✓	
Deploy honeycredentials		✓	✓	
Deploy honeyfiles		✓	✓	
InsightIDR walkthrough	✓	✓		

	Rapid7	Main POC	Security & IT	C-Suite
Service Delivery Phase				
Service Delivery Kickoff call	✓	✓		
Compromise Assessment *(If in Full Service)*	✓			
Customer Advisor communication process				
Monthly Meeting	✓			
Quarterly Meeting	✓			
Availability for Board and Executive calls (optional)	✓	✓		✓
Ad-Hoc Calls	✓	✓	✓	

	Rapid7	Main POC	Security & IT	C-Suite
Service Delivery Phase (Continued)				
24x7 environment monitoring				
Investigate MDR ABA, UBA, & NTA alerts	✓			
Validate investigated alerts to remove false positives (including RFI confirmation from the customer when needed)	✓			
Validate alerts and remove false positives from Customer's custom alerts and 3rd party alerts		✓	✓	
Detail malware and/or malicious activity analysis	✓			
Attack storyboarding	✓			
Write and assemble Findings Reports detailing any verified suspicious or malicious activity	✓			
Outreach to Customer ensure Findings Report and all recommendations are understood	✓	✓		
Initial Containment (one or the other)				
Without Active Response set up		✓		
With Active Response set up	✓			
Additional remediation & mitigation actions		✓	✓	
Monthly Threat Hunting *(If in Full Service)*				
Analyze historical data	✓			
Threat hunting	✓			
Threat reporting	✓			
Remediation & mitigation actions performed		✓	✓	
Threat Intelligence				
Monitor global attacks and vulnerabilities	✓			
Share research and findings in Threat Intel reports	✓			
Add Threat Intel findings to monitoring detections	✓			
Remediation & mitigation actions performed		✓	✓	
Remote Incident Response (Remote IR)				
Suggestion for Remote IR if a breach is confirmed	✓	✓	✓	
Acceptance of Remote IR		✓		
Scoping of breach	✓			
Reporting of findings	✓			
Presentation of findings	✓			
Remediation & mitigation actions performed		✓	✓	

Technology-Dependent Service Limitations

Some aspects of the Rapid7 MDR service may be degraded as described below if technology deployment or coverage requirements are not fully met.

Service Limitations of a Partially Deployed Environment

Rapid7 MDR recommends full deployment of Insight Agents to all in-scope assets. However, for a partial deployment of the Insight Agent to the environment your organization understands, agrees, and accepts the limitations and risk of service degradation. Specifically, the following aspects of the MDR service are unavailable to assets without the Insight Agent installed:

Detection Aspect	Limitation
Attacker Behavior Analytics	A significant portion of MDR's threat detection power lies in the ability to detect specific events (file system changes, network connections, process start/stop) on each of the assets. This data can only be provided by the Insight Agent.
Manual Human Threat Hunting	The MDR monthly threat hunts rely on the endpoint agent to collect the data in scope for threat hunts. Assets without the Insight Agent will be excluded from threat hunts. Threat hunting requires deployment of the Insight Agent to at least 80% of the in-scope environment.
Threat Intelligence matching	All executable processes run on any asset with the Insight Agent are matched against known threat intelligence. Assets without the Insight Agent will not have running processes matched against threat intelligence.
Alert validation and Remote IR investigations	MDR's incident investigations rely on the Insight Agent to collect data for analysis. Assets without the Insight Agent will be out of scope for both the typical validation process conducted by the SOC team for an alert as well as any Remote IR investigation.
Local authentications and group membership changes	The Insight Agent is required to identify authentications using local accounts, such as a local administrator account, and is required to identify local group membership changes (ex: user added to local administrators group). Assets without the Insight Agent will be excluded from local authentication and UBA, where UBA is the act of tracking per-user and per-system actions to build statistical models of user activity and identify anomalies.
Attacker ingress detection	The most common methods of compromise are via Phishing (malicious emails) and malicious web sites, both of which require end-user interaction to succeed. As the majority of internet browsing and email activity occurs on end-user workstations, Rapid7 is unable to identify initial methods of compromise and lateral movement from those systems to servers and other critical assets without the Insight Agent.

Alert Review Limitations

Rapid7 MDR reviews real-time alerts based on event sources described above. The following limitations are part of the MDR service related to event sources configured in InsightIDR:

Alert Source	Limitation
Third party alerts	These alerts (listed at https://docs.rapid7.com/insightidr/third-party-alerts) are not reviewed by the MDR SOC and do not generate alerts for the MDR SOC team to investigate. These log sources are used only for informational purposes to add fidelity and evidence during an investigation performed by the MDR SOC analysts.
Custom InsightIDR alerts	Alerts you add are not reviewed by the MDR SOC. It is up to you to review these alerts.

MDR Reporting During Penetration Testing

Many MDR customers integrate routine penetration testing into their holistic security strategy to perform end-to-end evaluations of all cyber security measures, including prevention, detection, and response. As an integral aspect of your cyber security controls, MDR works on your behalf to identify malicious activity, provide initial containment actions (if Active Response is enabled), and guide your team with detailed remediation and mitigation steps.

Penetration Test Communications to Rapid7 MDR

Communication Prior to Penetration Test

Rapid7 encourages your team to communicate upcoming or ongoing penetration testing to your CA. If you do choose to communicate details of upcoming penetration tests to your CA, you agree to provide:

- Beginning and end dates of penetration test
- Systems, networks, or subnets in scope
- Whether the test is a 'blackbox or no knowledge', 'limited knowledge', or 'full knowledge' test

You may also opt to not inform your CA as part of your testing regimen.

Communication During a Penetration Test

During the course of your Penetration Test, your CA will communicate Findings Reports or Requests for Information generated by the MDR SOC with a request to clarify whether MDR findings are related to penetration test activities.

Upon confirmation of penetration tester activity, MDR analysts will continue to monitor for related testing activities and use additional context provided by your team (or determined through analysis), to differentiate between penetration tester activity and potential attacker actions. As such, it is required that your team acknowledge if there is pen testing activity happening in the in-scope environment if MDR detects the test.

Once confirmed, you will be asked which engagement model you prefer ('no further notifications' or 'rollup', see below). The default for Rapid7 MDR reporting for Penetration Testing is 'no further notifications' which means your team will not be alerted to further security testing activity.

It is required that your team notifies your CA at the conclusion of the penetration test; following the completion of scheduled penetration testing activities and review of the MDR deliverables generated by the test, your CA will work with your team to identify detection gaps, if any, and additional measures to assist in adding context to findings.

Service Delivery Considerations

Should the scope of attacker activity increase beyond MDR's initial findings (or you communicate to your CA that a penetration test is taking place), we will ask you to choose one of the following options:

Option 1: Roll Up Reporting (Preferred)

Once Rapid7 identifies a Pen Tester in your environment, Rapid7 will only provide an initial notification on events related to security testing. Following initial notification and confirmation that findings are associated with ongoing penetration testing activities, the MDR team will continue to disposition related alerts as "SECURITY_TEST" and deliver our findings as an aggregate 'roll-up' report which lists which alerts the SOC would investigate had this been a real attack. You are required to specify "Roll Up" reporting as the default is 'no further notification' to further security testing activity.

Upon request, Rapid7 can review specific detection and response gaps (if applicable), however, Rapid7 is not responsible for performing gap analysis on customer's penetration test reports. In order for Rapid7 to address potential detection gaps, your team **must** provide Rapid7 with specific examples of penetration test activity for which Rapid7 did not generate alerts. Rapid7 **requires** the following information for the specific examples**:**

- Description of the activity and/or tools used
- Timestamp(s) of the activity
- Associated asset name(s) and IP address(es)
- Associated account(s)

Roll Up reporting contains the following deliverables:

- An aggregate 'roll-up' report of all alerts generated by the penetration test activity.

Option 2: "Purple Team Exercise"

You may want our SOC to treat the penetration test as an actual attack with all the resulting deliverables and updates. This type of engagement is considered a 'purple team exercise'. Rapid7 can support this 'purple team exercise' upon request; however, the 'purple team exercise' is subject to the following requirements listed below.

Note: Rapid7 MDR reserves the right to refuse the 'Purple Team Exercise' in rare instances when the MDR team is performing concurrent breach responses and/or currently performing a Purple Team Exercise.

Customers are required to:

1. Notify your Customer Advisor at least **two weeks** prior to the desired date of the purple team exercise.
2. Attend a kick-off call with your Customer Advisor and a member of the MDR Incident Management Team to discuss the scope of the penetration test, as well as agree upon the rules of engagement.
3. Timeline for the Penetration Test must be **limited to under seven (7) days** from the confirmation of the Pen Testing activity to the end of the engagement. Rapid7 reserves the right to not continue providing real-time reporting relating to the Pen Test after these 7 days.
4. Your organization agrees to retain an **external party** to perform the red team portion of the security testing. **Rapid7 MDR does not provide red team services for MDR purple team exercises.** Customers can, however, choose to retain penetration testing services through the Rapid7 Consulting Services at a cost.
5. Your organization agrees to **use one (1) of their allotted Remote IR engagements** due to the amount of SOC resources required to respond to penetration test activity.
6. Your team agrees to **take all recommended containment and/or remediation actions in a timely manner** to simulate an active response to these attacks. If Active Response is enabled, Rapid7 will perform actions to contain the threat as it relates to the Active Response service. Performing response actions in real-time will result in a more accurate simulation of an attack and subsequent response. It should be understood that taking remediation steps on production systems may impact business operations. Additionally, this protects the MDR SOC against 'unbounded' engagements that impact Rapid7's service delivery to all customers. If you are unable or unwilling to take the appropriate actions, Rapid7 MDR reserves the right to immediately cancel the exercise and will provide a **Roll Up Report** at the conclusion of the testing.

Purple Team Exercise reporting contains the following deliverables:

- All Remote Incident Response deliverables.

RAPID7 MUTUAL NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (the "Agreement"), effective as of the date of the last signature below (the "Effective Date"), is made by and between Rapid7, Inc., a Delaware corporation with a principal place of business at 120 Causeway Street, Suite 400, Boston, MA, 02114 ("Rapid7") and the company signing this Agreement ("Company"). The parties agree to be bound by the following terms and conditions concerning a potential or existing business relationship ("Purpose").

1. *Confidential Information*. "Confidential Information" means information that the Disclosing Party (as defined herein) considers to be proprietary and/or confidential, which may include, but is not limited to, trade secrets, discoveries, ideas, concepts, know-how, techniques, designs, specifications, drawings, diagrams, data, strategic and development plans, business plans, market reports, business activities and operations, reports, studies and other technical, financial and business information, including information concerning the Disclosing Party's employees and strategic partners ("Confidential Information"). The party disclosing Confidential Information shall be referred to herein as the "Disclosing Party" and the party receiving such information shall be referred to as the "Receiving Party."

2. *Exceptions*. Confidential Information does not include information that the Receiving Party can show: (i) was in the Receiving Party's possession on a non-confidential basis prior to disclosure by the Disclosing Party; (ii) was or became a part of the public domain without breach of this Agreement by the Receiving Party; (iii) was disclosed to the Receiving Party from a third party without an obligation of confidentiality; or (iv) was independently developed by the Receiving Party without the use of the Confidential Information.

3. *Non-disclosure Obligations*. The Receiving party shall: (i) only use Confidential Information for the Purpose: (ii) use reasonable care to protect the Confidential Information against unauthorized use, publication or disclosure, and in no event less than the same degree of care as it would employ with respect to its own Confidential Information; (iii) restrict access to the Confidential Information to those employees and agents who have a need to know such information to carry out the Purpose and who are bound by a duty of confidentiality no less protective of the Disclosing Party's Confidential Information than this Agreement; and (iv) not cause or permit reverse engineering of any Confidential Information or recompilation or disassembly of any products which are part of the Confidential Information received by it under this Agreement.

4. *Required Disclosure*. The Receiving Party may disclose Confidential Information if required by law, provided the Receiving Party uses diligent efforts to minimize disclosure, notifies the Disclosing Party prior to such disclosure (if legally permitted), and cooperates with the Disclosing Party in the event the Disclosing Party elects to legally contest such disclosure.

5. *Ownership; Disclaimer*. All Confidential Information provided under this Agreement shall remain the sole property of the Disclosing Party. Neither party acquires any intellectual property or other right under this Agreement, except as set forth herein. All Confidential Information and materials furnished hereunder are provided "as is," and Disclosing Party shall have no liability for Receiving Party's use thereof.

6. *Return of Information*. Upon the Disclosing Party's Request, the Receiving Party will promptly deliver to the Disclosing Party or destroy all Confidential Information, except that the Receiving Party may retain one copy of the Confidential Information to the extent necessary to comply with its legal obligations, and provided that any such copy shall remain subject to the terms and conditions of this Agreement.

7. *Applicable Law*. The Receiving Party shall comply with all applicable laws and regulations in relation to any Confidential Information received from the Disclosing Party.

8. *Remedies*. The parties acknowledge that a disclosure in violation of this agreement may cause irreparable harm and agree that either party may seek equitable relief in addition to other remedies available at law or in equity.

9. *Independent Development*. Notwithstanding anything herein to the contrary, the restrictions on disclosure and use set forth herein shall not restrict or limit the right of the Receiving Party to independently design, develop, acquire, market, service, or otherwise deal in, directly or indirectly, products or services competitive with those of the Disclosing Party, provided that the Receiving Party has not violated its obligations under this Agreement in connection with such development.

10. *Term and Termination*. This Agreement shall be effective from the date the last signature is affixed to this Agreement and shall continue until terminated by either party upon written notice. Confidential Information disclosed during such discussions shall be protected from disclosure under the terms of this Agreement for a period of 3 years from the date of disclosure, except that Confidential Information that constitutes a trade secret or personal information will continue to be protected under the terms of this Agreement for so long as such information remains a trade secret under applicable law.

11. *Miscellaneous*. (a) This Agreement binds and inures to the benefit of the parties and their successors and assigns; (b) this Agreement shall be construed in accordance with and governed for all purposes by the laws of the State of Texas, excluding its choice of law provisions, and each party consents and submits to the jurisdiction and forum of the state courts in Hidalgo County, in the State of Texas for all questions and controversies arising out of this Agreement; (c) this Agreement supersedes all prior discussions and writings and constitutes the entire agreement between the parties with respect to the subject matter hereof; (d) this Agreement may not be modified except by a writing signed by both parties; (e) should any provision of this agreement be found unenforceable, the remainder shall still be in effect; (f) this Agreement shall be binding upon and shall inure to the benefit of the parties hereto and their successors and permitted assigns; (g) any failure to enforce any provision of this Agreement will not constitute a waiver of that provision; and (h) this Agreement may be executed in two or more counterparts, each of which is deemed to be an original, but all of which constitute the same agreement.

IN WITNESS WHEREOF, and intending to be legally bound hereby, the parties hereto have caused this Agreement to be duly executed and delivered by their respective duly authorized officers as of the date set forth below.

Company: **Hidalgo County**

Signature: Richard F Cortez

Printed Name: **Richard F. Cortez**

Title: **County Judge**

Date Signed: 3/14/22

Address: **101 E. Cano, 2nd Floor, Edinburg, Texas 78539**

Rapid7

DocuSigned by:

Signature: F14E329C654B4E7...

Printed Name: Peter Kaes

Title: General Counsel

Date Signed: 10-Mar-2022

APPROVED BY COMMISSIONERS COURT ON: 3/8/22

Rev 07/20

RAPID7 INSIGHT PLATFORM TERMS OF SERVICE

This Terms of Service (the "Agreement"), effective as of the date of the last signature below (the "Effective Date"), is made by and between Rapid7 LLC (for customers located in the United States) or Rapid7 International Limited (for customers located outside the United States) (as applicable, "Rapid7") and the customer signing this Agreement ("Customer"). The parties agree to be bound by the following terms and conditions in connection with the subscription to and use of Rapid7 Services as defined herein.

1. DEFINITIONS

1.1. *Customer Data* means all data made available by Customer to Rapid7 for use in connection with the Service. This data may be stored within the Customer's environment, within the Rapid7 environment, or a combination of both.

1.2. *Documentation* means the documentation for the Service generally supplied by Rapid7 to assist its customers in their use of the Service, including user and system administrator guides, manuals and the software functionality specifications.

1.3. *Order Form* means Rapid7's order form or other ordering document signed or referenced by Customer and Rapid7 or its authorized reseller which identifies the specific Service ordered, the Volume Limitations, and the price agreed upon by the parties.

1.4. *Service* means the subscription service identified on an Order Form and further described herein.

1.5. *Subscription Term* means the term identified on an Order Form during which Customer has a subscription to the Service. Subscription Term will include the initial term as well as any renewal terms.

1.6. *Volume Limitations* means the capacity indicated on the Order Form, including, as applicable, unique assets, applications, number of scans, gigabytes, or workflows.

2. SOFTWARE LICENSES

2.1. *Access to Service*.

(a) During the Subscription Term, Rapid7 grants Customer a non-exclusive, non-transferable, non-sublicensable right to use and access the Service: (i) solely for Customer's internal business purposes; (ii) within the Volume Limitations; and (iii) as described in this Agreement. The parties also agree to be bound by any further license restrictions set forth on the Order Form.

(b) Access to the Service may require software to be downloaded or installed locally on Customer systems. If applicable, Customer must allow the downloaded and locally deployed software to integrate with such programs and devices necessary to provide data to the Service. In such an event, Rapid7 grants to Customer a worldwide, royalty-free, non-exclusive, non-transferable, non-sublicensable license to such software during the Subscription Term solely for the purpose of using the Service. In the event Customer decides to transmit its data without encryption, the Customer assumes all risks for failure to encrypt.

(c) In the event that the Service is used in excess of the Volume Limitations, following a reasonable notification period by Rapid7, Customer shall be liable for, and Rapid7 reserves the right to invoice for, the fees for such excess usage at Rapid7's then current list rates, or as otherwise set forth on the Order Form, notwithstanding the limitation on liability in Section 6.2 of this Agreement.

2.2. *Restrictions*. Except as may be expressly permitted by applicable law, Customer will not, and will not permit or authorize third parties to: (i) reproduce, modify, translate, enhance, decompile, disassemble, reverse engineer, create derivative works of the Service, or merge the Service into another program; (ii) resell, rent, lease, or sublicense the Service or access to it including use of the Service for timesharing or service bureau purposes; (iii) circumvent or disable any security or technological features or measures in the Service; nor (iv) access the Service in order to build a competitive product or service, for competitive analysis, or to copy any ideas, features, functions or graphics of the Service. Customer is responsible for its employees' compliance with this Agreement. If Customer identifies a vulnerability in the Service, all information and analysis regarding the vulnerability must be disclosed through the Rapid7 contact form, found at www.rapid7.com/disclosure/.

2.3. *Use by Affiliates*. Subject to the Volume Limitations, Customer may make the Service available to its Affiliates under these terms, provided that Customer is liable for any breach of this Agreement by any of its Affiliates. "Affiliate(s)" means any entity now existing that is directly or indirectly controlled by Customer. For purposes of this definition "control" means the direct possession of a majority of the outstanding voting securities of an entity.

2.4. *Customer Systems*. Customer represents and warrants that it has the appropriate authorizations from the owner of the networks, systems, IP addresses, assets, and/or hardware on which it deploys the Service, or which it targets, scans, monitors, or tests with the Service.

2.5. *Evaluation Licenses*. If Customer's access to the Service is for a trial or evaluation only, then the Subscription Term shall be thirty days, or the term specified on the Order Form. Customer may not utilize the same Service for more than one trial or evaluation term in any twelve month period, unless otherwise agreed to by Rapid7. Rapid7 may revoke Customer's trial or evaluation access at any time and for any reason. Sections 5 (Limited Warranty) and 9.1 (Indemnification) shall not be applicable to any evaluation or trial license.

3. FEES AND PAYMENT TERMS

3.1. If Customer is purchasing the Service through a Rapid7 authorized reseller, then the fees shall be as set forth between Customer and reseller and the applicable fees shall be paid directly to the reseller and Section 3.2 shall not apply.

3.2. Customer agrees to pay the fees, charges, and other amounts in accordance with the Order Form. All fees are nonrefundable, unless otherwise stated herein. Customer shall be responsible for remitting all taxes levied on any transaction under this Agreement, including, without limitation, all federal, state, and local sales taxes, levies and assessments, and local withholding taxes in Customer's jurisdiction, if any, excluding, however, any taxes based on Rapid7's income. In the event Customer is required to withhold taxes from its payment or withholding taxes are subsequently required to be paid to a local taxing jurisdiction, Customer is obligated to pay such tax, and Rapid7 as applicable, will receive the Order Form payment amount as agreed to net of any such taxes. Customer shall provide to Rapid7 written evidence that such withholding tax payment was made.

4. CONFIDENTIALITY

4.1. *Confidential Information*. Confidential Information. "Confidential Information" means information provided by one party to the other party which is designated in writing as confidential or proprietary, as well as information which a reasonable person familiar with the disclosing party's business and the industry in which it operates would know is of a confidential or proprietary nature. A party will not disclose the other party's Confidential Information to any third party without the prior written consent of the other party, nor make use of any of the other party's Confidential Information except in its performance under this Agreement. Each party accepts responsibility for the actions of its agents or employees and shall protect the other party's Confidential Information in the same manner as it protects its own Confidential Information, but in no event with less than reasonable care. The parties expressly agree that the terms and pricing of this Agreement are Confidential Information. A receiving party shall promptly notify the disclosing party upon becoming aware of a breach or threatened breach hereunder and shall cooperate with any reasonable request of the disclosing party in enforcing its rights.

4.2. *Exclusions*. Information will not be deemed Confidential Information if such information: (i) is known prior to receipt from the disclosing party, without any obligation of confidentiality; (ii) becomes known to the receiving party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing party; (iii) becomes publicly known or otherwise publicly available, except through a breach of this Agreement; or (iv) is independently developed by the receiving party without use of the disclosing party's Confidential Information. The receiving party may disclose Confidential Information pursuant to the requirements of applicable law, legal process or government regulation, provided that, unless prohibited from doing so by law enforcement or court order, the receiving party gives the disclosing party reasonable prior written notice, and such disclosure is otherwise limited to the required disclosure.

5. LIMITED WARRANTY

5.1. *Service Warranty*. Rapid7 warrants that, during the Subscription Term: (i) the Service will conform, in all material respects, with the applicable Documentation; and (ii) it will not materially decrease the overall functionality of the Service. For any breach of the above warranty, Rapid7 will, at no additional cost to Customer, use commercially reasonable efforts to provide remedial services necessary to enable the Service to conform to the warranty. Customer will provide Rapid7 with a reasonable opportunity to remedy any breach and reasonable assistance in remedying any defects. If Rapid7 is unable to restore such functionality, Customer may terminate the applicable Order Form and receive a pro rata refund of the fees paid for the terminated portion of the then-current Subscription Term. Rapid7 makes no warranty regarding third party features or services. The remedies set out in this subsection are Customer's sole remedies for breach of the above warranty.

5.2. *Disclaimer*. **RAPID7 DOES NOT REPRESENT THAT THE SERVICE WILL BE UNINTERRUPTED, ERROR-FREE, OR WILL MEET CUSTOMER'S REQUIREMENTS. EXCEPT FOR THE WARRANTY STATED HEREIN, RAPID7 MAKES NO OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS. RAPID7 MAKES NO WARRANTY THAT ALL SECURITY RISKS OR THREATS WILL BE DETECTED BY USE OF THE SERVICE OR THAT FALSE POSITIVES WILL NOT BE FOUND.**

5.3. *Orchestration Disclaimer*. **Customer is responsible for implementing appropriate internal procedures and oversight to the extent it utilizes the configuration of workflows and processes, including but not limited to containment actions, quarantine actions, kill processes and similar functionalities ("Orchestration and Automation Functionality"). EXCEPT FOR THE WARRANTY IN SECTION 5.1, THE ORCHESTRATION AND AUTOMATION FUNCTIONALITY IS MADE AVAILABLE BY RAPID7 ON AN "AS-IS" BASIS TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW. Rapid7's Orchestration and Automation Functionality is not designed, intended or licensed for use in hazardous environments or other applications where a malfunction could cause property damage or personal injury, and Rapid7 specifically disclaims any liability in connection with any such use. Customer assumes all risks in using third-party products or services in connection with the Orchestration and Automation Functionality.**

6. **LIMITATION OF LIABILITY**

6.1. *Exclusion of Certain Damages*. **NEITHER PARTY WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE.**

6.2. *Limitation on Amount of Liability*. **NEITHER PARTY WILL BE LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE TOTAL AMOUNT PAID OR PAYABLE BY CUSTOMER TO RAPID7 HEREUNDER DURING THE TWELVE MONTHS IMMEDIATELY PRIOR TO THE EVENT GIVING RISE TO LIABILITY, EXCEPT THAT THE LIMITATION IN THIS SECTION 6.2 SHALL NOT APPLY TO: (I) VIOLATIONS OF A PARTY'S INTELLECTUAL PROPERTY RIGHTS BY THE OTHER PARTY; OR (II) A PARTY'S EXPRESS INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT.**

7. **TERM**

7.1. *Term*. This Agreement will continue in effect until otherwise terminated in accordance with Section 7.3 below. The Subscription Term will automatically renew for an additional one year term at the rate listed on the applicable Order Form unless (i) otherwise indicated on the Order Form or (ii) either party provides the other with written notice of its election not to renew at least 30 days prior to the anniversary date. In connection with any renewal term, Rapid7 reserves the right to change the rates, applicable charges and usage policies and to introduce new charges, upon providing Customer written notice thereof (which may be provided by e-mail) at least 60 days prior to the end of the then-current Subscription Term.

7.2. *Suspension of Service*.

(a) In the event that Customer is using the Service to engage in illegal activity, and/or Customer's use of the Service is causing immediate, material and ongoing harm to others, Customer agrees that Rapid7 may suspend Customer's access to the Service, and shall promptly notify Customer of such suspension (which may be made by email or telephone). In the event that Rapid7 suspends Customer's access to the Service, Rapid7 will use commercially reasonable efforts to limit the suspension to the offending portion(s) of the Service and work with Customer to resolve the issues giving rise to the suspension of Service. Customer agrees that Rapid7, acting in good-faith, shall not be liable to Customer nor to any third party for any suspension of the Service for the above reasons under this Section 7.2.

(b) In addition to the foregoing, Rapid7 also reserves the right to suspend Customer's access to the Service upon notification, without having to terminate this Agreement or any Order Form, if Customer is more than thirty days late with respect to any payments due hereunder. Upon such suspension, Customer shall still be liable for all payments that have accrued prior to the date of suspension and that will accrue throughout the remainder of the Subscription Term. Rapid7 will not be obligated to restore access to the Service until Customer has paid all fees owed to Rapid7.

7.3. *Termination*. Notwithstanding the foregoing, either party may terminate this Agreement or any Order Form: (i) immediately in the event of a material breach of this Agreement or any such Order Form by the other party that is not cured within thirty days of written notice thereof from the other party or, if such breach is incapable of cure, immediately upon written notice; or (ii) immediately if the other party ceases doing business or is the subject of a voluntary or involuntary bankruptcy, insolvency or similar proceeding, that is not dismissed within sixty days of filing. Either party may also terminate this Agreement upon no less than thirty days' prior written notice to the other party for any reason if at such time there are no outstanding Subscription Terms then currently in effect. All rights and obligations of the parties which by their nature are reasonably intended to survive such termination or expiration will survive termination or expiration of this Agreement and each Order Form. Except as expressly provided herein, termination of this Agreement by either party will be a nonexclusive remedy for breach and will be without prejudice to any other right or remedy of such party.

7.4. *Effect of Termination*. Upon any termination or expiration of this Agreement or any applicable Order Form, Rapid7 shall no longer provide the applicable Service to Customer and Customer must cease using the Service and send no further Customer Data to Rapid7. Termination of this Agreement or an Order Form shall not relieve Customer of its obligation to pay all fees that have accrued or have become payable by Customer hereunder. Customer agrees that following termination of Customer's account and/or use of the Service, Rapid7 may

immediately deactivate Customer's account and that following a reasonable period not to exceed 90 days, shall be entitled to delete Customer's account and all Customer Data from the Service.

8. **OWNERSHIP; USE OF CONTENT; OBLIGATIONS**

8.1. *Customer Data*. Customer retains ownership of all right, title, and interest in and to all Customer Data, and Customer is solely responsible for all Customer Data. Rapid7 does not guarantee the accuracy, integrity, or quality of such Customer Data. Except as provided in this Agreement, Customer shall be solely responsible for providing, updating, uploading, and maintaining all Customer Data. Rapid7 may use Customer Data solely as necessary to: (i) provide the Service to Customer; (ii) in an anonymized and aggregated form that does not or cannot be used to identify Customer or any Customer Data, to generate statistics and produce reports; and (iii) collect data and analytics about use of the Service in order to continue to improve the development and delivery of the Service.

8.2. *Rapid7 Service*. Rapid7 retains ownership of all right, title, and interest in and to all intellectual property in and about the Service.

8.3. *Customer Obligations*. Customer shall not: (i) upload or otherwise transmit, display, or distribute any Customer Data to the Service that infringes any trademark, trade secret, copyright or other proprietary or intellectual property rights of any person; (ii) upload or otherwise transmit to the Service any material that contains software viruses or any other computer code, files, or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment; or (iii) interfere with or disrupt the Service.

9. **INDEMNIFICATION**

9.1. *By Rapid7*. Rapid7 will indemnify, defend, and hold harmless Customer from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys' fees) arising out of a third party claim that Rapid7's technology used to provide the Service infringes or misappropriates any patent, copyright, trade secret, or trademark of such third party. Notwithstanding the foregoing, in no event shall Rapid7 have any obligations or liability under this Section arising from: (i) use of any Service in a manner not anticipated by this Agreement or in combination with materials not furnished by Rapid7; or (ii) any content, information, or data provided by Customer or other third parties. If the Service is or is likely to become subject to a claim of infringement or misappropriation, then Rapid7 will, at its sole option and expense, either: (i) obtain for the Customer the right to continue using the Service; (ii) replace or modify the Service to be non-infringing and substantially equivalent to the infringing Service; or (iii) if options (i) and (ii) above cannot be accomplished despite the reasonable efforts of Rapid7, then Rapid7 may terminate Customer's rights to use the infringing Service and will refund pro-rata any prepaid fees for the infringing portion of the Service. THE RIGHTS GRANTED TO CUSTOMER UNDER THIS SECTION 9.1 SHALL BE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR ANY ALLEGED INFRINGEMENT BY THE SERVICE OF ANY PATENT, COPYRIGHT, OR OTHER PROPRIETARY RIGHT.

9.2. *By Customer*. Customer will indemnify, defend, and hold harmless Rapid7 from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys' fees) arising out of a third party claim regarding Customer's: (i) use of the Service in violation of this Agreement or applicable law; or (ii) breach of the representations and warranties made in Sections 2.4 and 11.2 of this Agreement.

10. **AVAILABILITY; DOWNTIME; SUPPORT**

10.1. *Downtime*. Subject to this Agreement and the Service Level Agreement located at https://www.rapid7.com/legal/sla/, Rapid7 shall use commercially reasonable efforts to provide the Service twenty-four hours a day, seven days a week throughout the Subscription Term. Customer agrees that from time to time the Service may be inaccessible or inoperable for various reasons, including: (i) equipment malfunctions; (ii) periodic maintenance procedures or repairs which Rapid7 may undertake from time to time; or (iii) causes beyond the control of Rapid7 or which are not reasonably foreseeable by Rapid7, including interruption or failure of telecommunication or digital transmission links, hostile network attacks or network congestion, or other failures (collectively "Downtime"). Rapid7 shall use commercially reasonable efforts to provide twenty-four hour advance notice to Customer in the event of any scheduled Downtime. Rapid7 shall have no obligation during performance of such operations to mirror Customer Data or to transfer Customer Data. Rapid7 shall use commercially reasonable efforts to minimize any disruption, inaccessibility, and/or inoperability of the Service in connection with Downtime, whether scheduled or not.

10.2. *Support Services*. Rapid7 shall provide support during any Subscription Term, or else as otherwise set forth on the applicable Order Form subject to Rapid7's support policy, located at https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-customer-support-guidebook.pdf.

10.3. *Product-Related Professional Services*. Unless otherwise provided on an Order Form or SOW, Customer is responsible for installing and configuring any Service. Rapid7 may provide Customer certain professional services, such as installation, configuration, consulting, training, and external scanning, if and as specified on an Order Form or a separate SOW executed by the parties ("Professional Services"). Professional

Services will be invoiced upon execution of the SOW. All changes to an SOW must be approved by both parties in writing. Rapid7 shall have sole discretion in staffing the Professional Services and may assign the performance of any portion of the Professional Services to any subcontractor; provided that Rapid7 shall be responsible for the performance of any such subcontractor. Customer will have a non-exclusive, non-transferable license to use any deliverables or other work product developed by Rapid7 in the performance of the Professional Services, which are delivered to Customer, upon Customer's payment in full of all amounts due for such deliverables or work product. Rapid7 retains ownership of all information, software, and other property owned by it prior to this Agreement or which it develops independently of this Agreement and all deliverables and work product compiled or developed by Rapid7 in the performance of the professional services.

10.4 *Professional Services Rescheduling*. To the extent Customer purchases Professional Services, Customer may reschedule the Professional Services up to ten business days prior to the start of the Professional Services at no cost. If Customer reschedules the Professional Services with less than ten business days' notice, Customer will forfeit the portion of the Professional Services equal to the number of days that were rescheduled without the required notice. If Customer reschedules the Professional Services after they have begun, Customer will forfeit five days of Professional Services, or the number of days remaining on the Professional Services, whichever is fewer. Customer will also be responsible for any expenses incurred by Rapid7 due to such rescheduling. If performance of the Professional Services is delayed by Customer's acts or omissions, including Customer's failure to meet the requirements set forth in an SOW, Customer will forfeit the duration of such delay from its Professional Services time.

11. DATA PRIVACY

11.1. *Personal Data*. To the extent that Rapid7 processes personal data about any individual in the course of providing the Service, Customer agrees to Rapid7's Data Processing Addendum, located at www.rapid7.com/legal/dpa/.

11.2. *Data Privacy*. Customer represents and warrants that Customer has obtained all necessary rights to permit Rapid7 to collect and process Customer Data from Customer, including, without limitation, data from endpoints, servers, cloud applications, and logs.

11.3. *Data Security*. Rapid7 shall implement appropriate technical and organizational measures to protect Customer Data from accidental or unlawful destruction, loss, or alteration, unauthorized disclosure of or access to Customer Data. Such measures may include, as appropriate (a) the encryption of Customer Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services; (c) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of Customer Data.

12. GENERAL PROVISIONS

12.1. *Miscellaneous*. (a) This Agreement shall be construed in accordance with and governed for all purposes by the laws of the State of Delaware (for customers located in North America), or England & Wales (for customers located outside of North America), each excluding its respective choice of law provisions and each party consents and submits to the jurisdiction and forum of the state and federal courts in the State of Delaware (for customers located in North America) or London, England (for customers located outside North America) all questions and controversies arising out of this Agreement and waives all objections to venue and personal jurisdiction in these forums for such disputes; (b) this Agreement, along with the accompanying Order Form(s) constitutes the entire agreement and understanding of the parties hereto with respect to the subject matter hereof and supersedes all prior agreements and undertakings, both written and oral; (c) this Agreement and each Order Form may not be modified except by a writing signed by each of the parties; (d) in case any one or more of the provisions contained in this Agreement shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provisions of this Agreement but rather this Agreement shall be construed as if such invalid, illegal, or other unenforceable provision had never been contained herein; (e) Customer shall not assign its rights or obligations hereunder without Rapid7's advance written consent; (f) subject to the foregoing subsection (e), this Agreement shall be binding upon and shall enure to the benefit of the parties hereto and their successors and permitted assigns; (g) no waiver of any right or remedy hereunder with respect to any occurrence or event on one occasion shall be deemed a waiver of such right or remedy with respect to such occurrence or event on any other occasion; (h) nothing in this Agreement, express or implied, is intended to or shall confer upon any other person any right, benefit, or remedy of any nature whatsoever under or by reason of this Agreement, including but not limited to any of Customer's own clients, customers, or employees; (i) the headings to the sections of this Agreement are for ease of reference only and shall not affect the interpretation or construction of this Agreement; (j) terms in an Order Form have precedence over conflicting terms in this Agreement, but have applicability only to that particular Order Form; and (k) this Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

12.2. *Injunctive Relief*. Notwithstanding any other provision of this Agreement, both parties acknowledge that any breach of this Agreement may cause the other party irreparable and immediate damage for which remedies other than injunctive relief may be inadequate. Therefore, the parties agree that, in addition to any other remedy to which a party may be entitled hereunder, at law or equity, each party shall be entitled to seek an injunction to restrain such use in addition to other appropriate remedies available under applicable law.

12.3. *Relationship of the Parties*. Rapid7 and Customer are independent contractors, and nothing in this Agreement shall be construed as making them partners or creating the relationships of principal and agent between them, for any purpose whatsoever. Neither party shall make any contracts, warranties, or representations or assume or create any obligations, express or implied, in the other party's name or on its behalf.

12.4. *US Government Restricted Rights*. US Government Restricted Rights. This Section applies to all acquisitions of the Service by or for the US federal government, or by any prime contractor or subcontractor (at any tier) under any contract, grant, cooperative agreement, or other activity with the federal government for the Government's end use. The Service are "commercial items" as that term is defined at FAR 2.101. If Customer is an Executive Agency (as defined in FAR 2.101) of the U.S. Federal Government ("Government"), Rapid7 provides the Service, including any related technical data and/or professional services in accordance with the following: If a right to access the Service is procured by or on behalf of any Executive Agency (other than an Executive Agency within the Department of Defense (DoD)), the Government is granted, in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Computer Software), only those rights in technical data and software customarily provided to Rapid7's customers as such rights are described in this Agreement. If a right to access the Service is procured by or on behalf of any Executive Agency within the DoD, the Government is granted, in accordance with DFARS 227.7202-3 (Rights in commercial computer software or commercial computer software documentation), only those rights in technical data and software that are customarily provided to Rapid7's customers as such rights are described in this Agreement. In addition, DFARS 252.227-7015 (Technical Data – Commercial Items) applies to technical data provided by Rapid7 to an Executive Agency within the DoD. Note, however, that Subpart 227.72 does not apply to computer software or computer Service documentation acquired under GSA schedule contracts. Except as expressly permitted under this Agreement, no other rights or licenses are granted to the Government. Any rights requested by the Government and not granted under this Agreement must be separately agreed in writing with Rapid7. This Section 12.4 of the Agreement is in lieu of, and supersedes, any other FAR, DFARS, or other clause, provision, or supplemental regulation that addresses Government rights in the Service.

12.5. *Force Majeure*. Other than payment obligations hereunder, neither party will be liable for any inadequate performance to the extent caused by a condition that was beyond the party's reasonable control (including, but not limited to, natural disaster, act of war or terrorism, riot, global health crisis, acts of God, or government intervention), except for mere economic hardship, so long as the party continues to use commercially reasonable efforts to resume performance.

12.6. *No Reliance*. Customer represents that it has not relied on the availability of any future version of the Service or any future product or service in executing this Agreement or purchasing any Service hereunder.

12.7. *Notices*. Unless specified otherwise herein, (i) all notices must be in writing and addressed to the attention of the other party's legal department and primary point of contact and (ii) notice will be deemed given: (a) when verified by written receipt if sent by personal courier, overnight courier, or when received if sent by mail without verification of receipt; or (b) when verified by automated receipt or electronic logs if sent by email. When sent by email, notices to Rapid7 must be sent to notices@rapid7.com.

12.8. *Publicity*. Customer acknowledges that Rapid7 may use Customer's name and logo for the purpose of identifying Customer as a customer of Rapid7 products and/or services. Rapid7 will cease using the customer's name and logo upon written request.

12.9. *Compliance with Law*. Each party agrees to comply with all applicable federal, state, and local laws and regulations including but not limited to export law, and those governing the use of network scanners, vulnerability assessment software products, encryption devices, user monitoring, and related software in all jurisdictions in which systems are scanned, scanning is controlled, or users are monitored.

12.10. *Links and Third Party Content*. Customer agrees that Rapid7 shall not be responsible for applications, services, software, or other products supplied by a third party (excluding those delivered as part of the Service) that Customer chooses to use with or integrate with the Service, even if such third-party service interoperates with a Service.

Signature page follows.

Rapid7 and Customer have caused this Agreement to be executed by their duly authorized representatives as of the Effective Date.

Customer: **Hidalgo County**

Signature: Richard F Cortez

Printed Name: **Richard F. Cortez**

Title: **County Judge**

Date Signed: 3/14/22

Address: **100 E. Cano, 2nd Floor**

Edinburg, Texas 78539

APPROVED BY
COMMISSIONERS COURT
ON: 3/8/22

Rapid7

Signature: DocuSigned by: F14E329C054B4E7...

Printed Name: Peter Kaes

Title: General Counsel

Date Signed: 10-Mar-2022

EXECUTED as of the day and year first written above.

APPROVED BY COMMISSIONERS' COURT ON March 08, , 2022 .
Agenda Item No. 84848 **Executive Office:** _____

VENDOR:
ABC Company

John Doe, Title

APPROVED AS TO FORM:
Office of the Criminal District Attorney,
Ricardo Rodriguez, Jr.

APPROVED BY
COMMISSIONERS COURT
ON: 3/8/22

COUNTY:
COUNTY OF HIDALGO

ATTEST:

Hon. Richard F. Cortez, County Judge

Arturo Guajardo, Jr., County Clerk

COMMISSIONERS COURT
HIDALGO COUNTY, TEXAS

ATTACHMENTS:
(If Applicable)

SUPPLEMENTAL SIGNATURES:
(If Applicable)