COMCAST ENTERPRISE SERVICES
PRODUCT SPECIFIC ATTACHMENT
MANAGED DETECTION & RESPONSE SERVICES

ATTACHMENT IDENTIFIER: Managed Detection & Response Services, Version 1.0

The following additional terms and conditions are applicable to Sales Orders for Managed Detection & Response Services ("MDR Services") ordered under an Enterprise Master Service Agreement:

DEFINITIONS

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Master Service Agreement.

"**Customer-Provided Equipment**" or "**CPE**" means the hardware appliance or other endpoint device installed at the Service Location.

"Estimated Availability Date" means the target Service Commencement Date for the Service.

"MDR Platform" means the MDR cloud platform provided by Comcast, including malware protection, detection and remediation solutions, endpoint detection and response solutions, device discovery and control solutions, identity and directory management security solutions, and other solutions offered by Comcast to Customer, together with the software underlying products and services.

"MDR Solution" or "Solution" means the MDR Platform together with the Asset Components, and all updates thereto. For the avoidance of doubt, the Solution shall be deemed Licensed Software under the Agreement.

"MDR Vendor" means the third-party provider, supplier or licensor of the MDR Platform.

"Service(s)" means the Managed Detection and Response Services which may also be referred to as MDR Essentials, MDR Enhanced, and/or MDR Complete, as applicable.

ARTICLE 1. SERVICES

This attachment shall apply to MDR Services. A further description of the Services is set forth in Schedule A-1 hereto, which is incorporated herein by reference.

ARTICLE 2. PROVIDER

The Services shall be provided by Comcast or one of its applicable subsidiaries or affiliates (**"Comcast"**).

ARTICLE 3. SERVICE PROVISIONING INTERVAL

Following acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Service on or about the Estimated Availability Date; provided, however, that Comcast's failure to provision Service by said date shall not constitute a breach of the Agreement.

ARTICLE 4. SERVICE COMMENCEMENT DATE

Comcast shall inform Customer when the Service is available ("Availability Notification"). Charges for the Services shall begin to accrue on the Service Commencement Date. The Service Commencement Date shall be the earliest of: (a) the date on which Customer confirms receipt of and concurrence with the Availability Notification; (b) five (5) business days following the date of the Availability Notification; or (c) the date on which Customer first uses the Service.

ARTICLE 5. TERMINATION; PORTABILITY

5.1 The charges set forth or referenced in each Sales Order have been extended to Customer in reliance on the Service Term.

Termination Charges.

A. Subject to Section 5.1(C), in the event that Service is terminated following Comcast's acceptance of the applicable Sales Order, but prior to the Commencement Date, Customer shall pay Termination Charges to one hundred and twenty percent (120%) of costs and expenses incurred by Comcast in provisioning or preparing to provision the Service.

B. Subject to Section 5.1(C), in the event that Service is terminated on or following the Commencement Date, but prior to the end of the

applicable Service Term, Customer shall pay Termination Charges equal to a percentage of the monthly recurring charges remaining for the unexpired portion of the then-current Service Term, calculated as follows:

i. 100% of the monthly recurring charges with respect to months 1-12 of the Service Term; plus
ii. 80% of the monthly recurring charges with respect to months 13-24 of the Service Term; plus
iii. 65% of the monthly recurring charges with respect to months 25 through the end of the Service Term; plus
iv. 100% of any remaining, unpaid non-recurring charges.

Termination Charges shall be immediately due and payable upon cancellation or termination and shall be in addition to any and all accrued and unpaid charges for the Services rendered by Comcast through the date of such cancellation or termination.

C. Termination Charges shall not apply to Service terminated by Customer as a result of Comcast's material and uncured breach in accordance with the Master Service Agreement.

5.2 Additional Termination Right. In addition to, and without limiting Comcast's other termination rights under the Agreement, in the event that any of Comcast's rights, licenses or authorizations to provision the Services, or any component thereof, terminate, cease, or expire, in whole or in part, Comcast may, at its sole option: (a) terminate the Services or affected component(s) thereof, or (b) replace the Services or affected component(s) thereof with substantially similar services.

5.3 Service Upgrades. Customer may upgrade or downgrade MDR Service without incurring Termination Charges, provided that: (a) the modified Service (the "**Modified Service**") must assume the remaining Service Term of the existing Service (an "**Existing Service**"), but in no event less than twelve (12) months; (b) Customer submits a Sales Order to Comcast for the Modified Service and that Sales Order is accepted by Comcast; and (c) Customer agrees to pay the applicable monthly recurring charges for the Modified Service commencing with the upgrade or downgrade, as applicable.

ARTICLE 6. CUSTOMER PORTAL

Comcast provides the Customer with a password-protected web portal ("**Portal**"), which Customer will be required to access to operate and view information regarding the Service. Customer may have the option to use the Portal to enter changes to the Customer's Service settings and configurations, subject to the availability of self-service settings and configurations, as determined by Comcast in its sole discretion.

ARTICLE 7. ADDITIONAL SERVICE TERMS

In the event that Comcast is obligated to indemnify the Customer under the Master Service Agreement as a result of any infringement of a U.S. patent or copyright related to Comcast Equipment or Licensed Software, including the MDR Solution, and such Comcast Equipment or Licensed Software, including the MDR Solution, is provided by a third party, Comcast's indemnification obligation is conditioned on Comcast having the right to indemnification from the MDR Vendor with respect to the MDR Solution, or other third party provider for any other applicable Comcast Equipment or Licensed Software, and the Customer's sole and exclusive remedy against Comcast and the MDR Vendor is limited to the pass through to the Customer of any amounts of damages applicable to the Customer that Comcast is able to recover pursuant to Comcast's agreement with such MDR Vendor or other third party provider. To the extent that the Customer, Comcast and/or any other customer of Comcast pursues claims against an MDR Vendor or other third-party provider, then any damages applicable to the Customer that are actually received from such MDR Vendor or other third-party provider related to such claims shall be allocated equitably among all affected parties.

ARTICLE 8. TECHNICAL SPECIFICATIONS; SERVICE LEVEL AGREEMENT

The technical specifications applicable to the Services are set forth in Schedule A-1 hereto ("Service Descriptions and Technical Specifications").

PRODUCT-SPECIFIC ATTACHMENT

MANAGED DETECTION & RESPONSE

SCHEDULE A-1
SERVICE DESCRIPTIONS AND TECHNICAL SPECIFICATIONS

The Services will be provided in accordance with the service descriptions and technical specifications set forth below:

1. Definitions

1.1 "**Asset(s)**" means a single system that is connected to a Customer network or under Customer management such as a server, laptop or virtual machine where the Asset Component of the Solution has been installed and is connected to the MDR Platform.

1.2 "**Asset Component(s)**" means the software components of the Solution that can be downloaded to Assets.

1.3 "**Content**" means any of Customer's data gathered through the provision of the offering or made available by Customer for use in connection with the Offering. These data may be stored within Comcast and the Customer's environments, within the MDR Platform, or a combination.

1.4 "**Customer Data**" means Customer data and information which is uploaded to, processed by and/or stored within the Solution via Customer's use of the Solution, directly or via Comcast's operation of the Solution on behalf of Customer.

1.5 "**Documentation**" means the written and/or electronic end user or technical documentation, including but not limited to documents, images, recordings and/or videos specifying the functionalities of the Solution provided or made available by Comcast or the MDR Vendor, including through Comcast's or the MDR Vendor's website or otherwise, as updated by Comcast or the MDR Vendor from time-to-time.

1.6 "**MDR Platform**" means the MDR cloud platform provided by Comcast, including malware protection, detection and remediation solutions, endpoint detection and response solutions, device discovery and control solutions, identity and directory management security solutions, and other solutions offered by Comcast to Customer, together with the software underlying such products and services.

1.7 **"MDR Services"** means the operation, management, and support using the MDR Platform by Comcast on behalf of or for the benefit of Customer.

1.8 "**MDR Solution**" or "**Solution**" means the MDR Platform together with the Asset Components, and all updates thereto. For the avoidance of doubt, the Solution shall be deemed Licensed Software under the Agreement.

1.9 "**MDR Vendor**" means the third-party provider, supplier or licensor of the MDR Platform.

1.10 "**Managed Services**" mean the delivery, operation, management, support or use of the Solutions by Comcast on behalf of or for the benefit of Customer, as and to the extent made available by Comcast.

1.11 "**SOC**" means Comcast's Security Operations Centers.

1.12 "**System Data**" means information compiled by the Services in connection with Customer's use of the MDR Platform, including but not limited to cybersecurity attack data, contextual data, detections, indicators of compromise, and Customer Data.

2 Service Description

2.1 **General.** The Service is a managed security service, which provides customers with access to a cloud-hosted security information and event management, detection, and response platform. The MDR Platform performs detection and response functions as well as other features depending on the service tier licensed from Comcast. The Comcast MDR Platform and MDR Services work together to detect, investigate, contain and disrupt cybersecurity risks and threats in the customer's IT environment. The MDR Services assist in containing and disrupting threats that the Comcast

SOC can detect using Customer Data analyzed by the MDR Platform. The MDR Services are intended to contain and disrupt cybersecurity attacks, but do not remediate Asset configuration issues, hardware or software version levels or hardware and software errors and vulnerabilities. Customers are responsible for mitigating any underlying root-cause vulnerabilities that made the threat possible, such as device configuration hardening, patching old versions of software, or vulnerabilities related to people, process or technology, that may have allowed the attack to occur.

2.2 **Managed Services.** The Comcast SOC will monitor cybersecurity attack alerts based on a 24/7x365 basis and respond to cybersecurity attacks identified from such alerts based on the settings and configurations for Customer's Service and the cybersecurity attack severity classification assigned by the MDR Solution.

2.3 **Service Offerings.** Comcast offers three versions of the Service, MDR Essentials, MDR Enhanced, and MDR Complete, which are described below.

(i) **MDR Essentials.** This Service includes customer support, threat investigation and containment and data archiving.

(ii) **MDR Enhanced.** MDR Enhanced includes the features described for MDR Essentials above with the addition of custom detection rules.

(iii) **MDR Complete.** MDR Complete includes the features described for MDR Enhanced with the addition of custom Security Orchestration and Automated Response ("SOAR") automations and threat hunting.

2.4 **Optional Features.** During the applicable Service Term, Customers may purchase, as made available by Comcast and subject to additional fees, the following optional features:

(i) Vulnerability scanning – Scan of the Customer's the network to discover and prioritize active vulnerabilities for remediation. Gain visibility into Customer's IT assets. Continually assess and prioritize Customer's critical vulnerabilities for remediation.

(ii) Extended Data Retention – Extends MDR data retention period from default 60 days to 365 days.

(iii) Security review – Personalized review of MDR performance. Options include Monthly Incident Report, a Quarterly Security Posture Report or a Quarterly review of Critical Security Controls.

(iv) Dedicated Security Team – Assignment of a dedicated Comcast SOC personnel.

3 Service Requirements

3.1 **General Requirements.** In order to provide the Services to Customer, Customer's Assets must have Internet connectivity. If the Internet connectivity is terminated for any Asset or is unavailable for any reason at any time (and even if the Asset Components installed by Customer otherwise continue to operate), the Services will be inoperable or impaired, including without limitation, the Asset Components' inability to communicate with the MDR Platform.

3.2 **Customer Responsibility.** Comcast's ability to provide the Service is contingent upon Customer's compliance with the following responsibilities related to the installation, use, support and maintenance of the Service, and Comcast will not be responsible for any failure of the Service as a result of Customer's failure to fulfill the same:

(i) Provide Comcast necessary technical and contact information required to provision the MDR Solution and Managed Services to Customer;

(ii) Participate in Comcast's Service activation and verification processes, and perform any testing required by Comcast in connection therewith;

(iii) Setup and maintain an account within the MDR Solution and the Portal, including if applicable, setting up secondary users with appropriate privileges;

(iv) Ensure Customer is able to access the Portal and MDR Solution;

(v) Manage service settings for the Service to the extent such settings are self-managed through the MDR Solution or Portal, as determined by Comcast from time to time in Comcast's sole discretion;

(vi) Installing the MDR Platform software components on Customer's Assets with Comcast's guided installation assistance and strictly in accordance with Comcast's instructions (for the avoidance of doubt, Customer shall

not install the Asset Components on Customer Assets in excess of any quantities or other limitations set forth in a Sales Order); and

(vii) Provide Comcast with all license or access keys, credentials and permissions, obtain all rights, licenses, consents and authorizations, and take all such other actions necessary, in order for Comcast to access, use, operate, and manage the MDR Solution, and as otherwise necessary for Comcast's performance of the Managed Services.

3.3 **Customer Consent.** Customer acknowledges and agrees (a) the MDR Solution connects to and communicates with the Customer's systems and environment, including the Assets, (b) that Assets collect and transmit data (including, without limitation, System Data) from the MDR Platform, and that Comcast and/or MDR Vendor will have access to such data through the MDR Solution, and (c) the MDR Solution may communicate with Customer's Assets, systems and environment to initiate responses to cybersecurity attacks. Customer expressly consents to such activity in connection with the Service. Customer further authorizes Comcast to (i) access and transmit, (ii) perform remote analysis of, and (iii) use, modify, and distribute any System Data in connection with the Services.

3.4 **Notifications; Requests for Information.** Comcast will notify Customer when conducting a cybersecurity investigation classified as critical or severe. Comcast may on behalf of the customer respond to a cybersecurity event by making changes to the Customer's environment. Comcast will notify customer of actions or changes in response to its investigation. Comcast may not have sufficient information from the Customer Data to determine if an event is benign or malicious during MDR monitoring and investigation and may send Customer a Request for Information (RFI). If Customer does not respond or if the detection rule is the responsibility of the customer, then Comcast may close the investigation.

4 License to MDR Platform; Restrictions

4.1 **License Grant.** With respect to the MDR Solution, the license to the Licensed Software set forth in Section 2.6 of the General Terms and Conditions shall be further limited such that the license is non-sublicensable and such use shall be solely in accordance with the Documentation and the terms of the Agreement.

4.2 **License Restrictions.** In addition to and without limiting the restrictions in Section 2.6 of General Terms and Conditions, Customer may not (and shall not permit or cause any third party to) do any of the following: (a) modify, disclose, alter, translate or create derivative works of the MDR Solution (or any components thereof) or any accompanying Documentation; (b) license, sublicense, resell, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the MDR Solution (or any components thereof) or any Documentation; (c) disassemble, decompile or reverse engineer the MDR Solution (except to the extent and for the express purposes authorized by any and all applicable federal or state laws or regulations); (d) use the MDR Solution in any illegal way, in violation of any law or regulation or third party property or personal right, including, to store or transmit infringing, libelous or otherwise unlawful or tortious material, or material in violation of third-party property, personal or privacy rights; (e) use the MDR Solution to knowingly store or transmit any viruses, software routines or other code designed to permit unauthorized access, to disable, erase or otherwise harm software, hardware or data, or to perform any other harmful actions; (f) copy, frame or mirror any part or content of the MDR Solution; (g) access or use the MDR Solution to build a competitive product or service, or copy any features or functions of the MDR Solution; (h) interfere with or disrupt the integrity or performance of the MDR Solution; (i) attempt to gain unauthorized access to the MDR Solution or their related systems or networks or to another user account; (j) disclose to any third party or publish in any media any performance information or analysis relating to the MDR Solution without consent of Comcast; (k) remove, alter or obscure any proprietary notices in or on the MDR Solution or accompanying Documentation, including copyright notices; or (l) probe, scan or test the vulnerability of the MDR Solution, or take any action in an effort to circumvent the Services; test the vulnerability of the MDR Solution, breach the security or authentication measures on the MDR Solution, or take any action that imposes an unreasonable or disproportionately large load on the infrastructure of the MDR Solution, such as a denial of service attack.

4.3 **Export Compliance.** Without limiting Article 9.11 of the General Terms, the MDR Solution and any components of the MDR Solution made available to Customer by Comcast are subject to the U.S. Export Administration Regulations, the UK Export Control Act 2002 and other relevant export control and economic sanctions laws. Customer agrees to comply with all such laws and regulations as they relate to access to and use of the MDR Solution by Customer. Customer shall not access or use the MDR Solution in any jurisdiction in which it is prohibited under U.S. or other

applicable laws or regulations (a "**Prohibited Jurisdiction**"). Customer represents, warrants and covenants that (a) Customer is not named on any U.S. government list of persons or entities prohibited from receiving U.S. exports, or transacting with any U.S. person, (b) Customer is not a national of, or a company registered in, any Prohibited Jurisdiction, and (c) Customer shall comply with all applicable laws regarding the transmission of technical data exported from the U.S. and the country in which Customer or Assets are located. Notwithstanding the foregoing, Customer acknowledges and agrees that Customer may not use the Service outside of the United States.

5 Additional Limitation of Liability; Disclaimers

5.1 COMCAST MAKES NO EXPRESS OR IMPLIED WARRANTY OR GUARANTEE THAT THE SERVICES WILL (A) IDENTIFY, REMEDIATE OR RESOLVE EVERY, SECURITY RISK, INCIDENT, THREAT OR CYBERSECURITY ATTACK, (B) BE ERROR-FREE (INCLUDING WITH RESPECT TO CYBERSECURITY ATTACK CLASSIFICATION AND/OR FALSE POSITIVES), (C) CORRECTLY PRIORITIZE INCIDENTS, THREATS OR ATTACKS, OR (D) SATISFACTORILY ACCOMPLISH OR PERFORM CYBERSECURITY ATTACK RESPONSE OR THREAT HUNTING. CUSTOMER ACKNOWLEDGES THAT THE SERVICE CONSTITUTES ONLY ONE COMPONENT OF CUSTOMER'S OVERALL SECURITY PROGRAM AND IS NOT A COMPREHENSIVE SECURITY SOLUTION; INSTEAD, THE SERVICE IS INTENDED TO IDENTIFY AND RESPOND TO EXISTING KNOWN CYBERSECURITY ATTACKS. CUSTOMER ACKNOWLEDGES THAT THE SERVICES PROVIDED ARE MERELY A TOOL FOR CUSTOMER TO USE IN ORDER TO ASSIST IN SUCH IDENTIFICATION AND RESPONSE EFFORTS. CUSTOMER ACKNOWLEDGES THAT THE CUSTOMER IS SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SERVICES, AND FOR ANY RELIANCE THEREON. TO THE MAXIMUM EXTENT PERMITTED BY LAW CUSTOMER WAIVES ANY AND ALL CAUSES OF ACTION OR CLAIMS AGAINST COMCAST, ITS PARENTS, AFFILIATES AND ITS AND THEIR SUPPLIERS AND LICENSORS ARISING THEREFROM OR RELATING THERETO. COMCAST CANNOT AND DOES NOT WARRANT THE RESULTS THAT MAY BE OBTAINED BY THE USE OF THE SERVICES. COMCAST'S ABILITY TO PROVIDE THE SERVICE MAY BE CONTINGENT ON CUSTOMER PROVIDING ACCURATE AND TIMELY INFORMATION TO COMCAST. CUSTOMER ACKNOWLEDGES AND AGREES THAT (1) CYBERSECURITY ATTACK DETECTIONS, ALERTS, AND RESPONSES MADE BY THE MDR SOLUTION, AND (2) THE SOC'S REVIEW AND RESPONSE TO SUCH ALERTS MAY BE CONTINGENT ON THE CUSTOMER'S SETTINGS AND CONFIGURATIONS OF THE SERVICES, INCLUDING THE MDR SOLUTION.

6 System Data Customer acknowledges and agrees that (a) as between Customer and Comcast, Comcast shall retain the rights to all System Data collected in conjunction with the Services, and (b) Comcast may use such System Data for security, product, and operations management, and/or for research and development.

7 Anonymized Data Customer acknowledges and agrees that Comcast and/or its suppliers or licensors, including the MDR Vendor, may monitor, collect, use and store fully anonymous, aggregated statistics and/or data regarding use of the Solutions ("**Anonymized Data**") for their business purposes (including, but not limited to, improving the Services and creating new features) and such Anonymized Data shall not be considered Customer Data or System Data, provided that (a) the data cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual or Customer, and (b) Comcast or its applicable supplier or licensor (i) has implemented technical safeguards that prohibit reidentification of the information, (ii) has implemented business processes that specifically prohibit reidentification of the information, (iii) has implemented business processes to prevent inadvertent release of anonymous information, and (iv) makes no attempt to reidentify the information

8 Privacy, Data Security and Content

8.1 **Privacy.** To the extent that Comcast MDR Service processes personal data about any individual in the course of providing the Service, the terms of Comcast's Privacy and Information Security policies located at https://business.comcast.com/privacy shall apply.

8.2 **Data Security.** Comcast shall implement appropriate technical and organizational measures to protect Content from accidental or unlawful destruction, loss, or alteration, unauthorized disclosure of, or access to Service. Such measures

may include, as appropriate (a) the encryption of Content; (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 Service.

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

8.4 **Confidentiality.** Comcast shall maintain the confidentiality of all Customer data and information provided to them in connection with the MDR Services and shall use such information only as necessary to perform the Services. The intellectual property rights therein, are and shall remain the sole property of the Customer.

8.5 **Comcast shall retain the rights to all System Data it develops in conjunction with the MDR Services**

9 MDR Installation and Configuration

9.1 Customer shall provide to Comcast complete and accurate contact information and scoping information including, without limitation, a list of names and email addresses for provisioning the MDR Solution and any other information requested by Comcast. Upon receipt of complete and accurate Customer contact and Services scoping information:

(i) Comcast will enable Customer access to the MDR Platform and will provide an initial default configuration.

(ii) Comcast will make MDR Platform software available to Customer electronically, via download from a secured website or other means as determined by Comcast.

9.2 Comcast will make three (3) attempts to schedule a call with Customer to complete the Services on-boarding process and to obtain any additional information required from Customer. If Comcast attempts to schedule an on-boarding call are unsuccessful, Comcast may terminate the applicable Sales Order (subject to applicable Termination Charges set forth in Article 5).

9.3 **MDR Subscription Fees.** For each service tier, customers license the number of Assets they want Comcast to monitor. Assets are defined as computer hosts running a workstation or server operating system on which the customer installs the MDR software. MDR subscription fees are based on the volume of Assets. Comcast may impose a minimum number of Assets at its own discretion. Comcast reserves the right to charge Customer additional surcharge fees if Customer installs the MDR software on a greater number of Assets than licensed. The MDR Service may be purchased without the need for other Comcast products or services, although Comcast may choose to offer promotional discounts from time to time in combination with other products and services.

10. Automated Threat Response

Comcast MDR Service can initiate actions that contain attacks against customer Assets or compromised user accounts (Automated Threat Response) in response to a validated cybersecurity threat. To be eligible for Automated Threat Response, customers must subscribe to the MDR Enhanced or MDR Complete service tier and install the MDR SOAR tool. To contain users via Active Directory, Customer must allow the SOAR tool to connect with their Lightweight Directory Access Protocol ("LDAP") domain.

To take automated containment actions on Assets, customers must also install MDR Platform endpoint software. To enable the MDR SOC to perform post-containment forensic investigation on Assets, customers must allow network connections from contained assets to the MDR Platform. Customer is responsible for taking action to remove an Asset from MDR quarantine.

The Automated Threat Response service is designed to take real time action in the customer's production

environment and can disrupt users, endpoints, and business operations. By enabling the Automated Threat Response service, Customer has read, understands, and agrees to the following:

Customer grants Comcast permission to take the recommended response action in Customer's production environment via automated threat response. While the Comcast SOC strives to identify and contain all threats, there is no guarantee that automated threat response will catch and contain all threats in the customer environment.

Comcast will not be held liable for any actions performed by automated threat response. In no event shall Comcast or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information) arising out of the use of, or inability to use, software, service, or capabilities related to action taken by the automated threat response service, even if Comcast has advised Customer of the possibility of such damages.

11. **Data Ingest Fair Use**

Customer is subject to a monthly data ingest fair use limitation, which Comcast may charge to Customer if it exceeds the data ingest fair use limitation specified in the Fair Usage table below.

Data ingest fair use shall be calculated in the aggregate, and not based on MDR Platform data ingest by individual Assets.

"Fair Use" or "Fair Usage" means the total data that a given customer may send to the MDR Platform for processing.

Fair Usage	MDR Essentials	MDR Enhanced	MDR Complete
Monthly Data Ingest (aggregated)	200 TB	240 TB	260 TB

12. **Response Times - Service Level Objectives**

The Service Level Objective (SLO) refers only to the Response Time by a MDR Service analyst to an Investigation and is dependent on the MDR Service ordered by Customer. "Response Time" means the elapsed time between the reported detection time by the MDR Platform and the time a MDR Services SOC analyst first annotated the event. Response Time does not include the time to conduct a RFI Investigation. SLOs are non-credit bearing objectives that Comcast endeavors to meet for Response Time.

MDR Service	MDR Essentials	MDR Enhanced	MDR Complete
SLO	Standard	Advanced	Advanced

MDR Investigation Type	Standard Response Time (within 90%)	Advanced Response Time (within 90%)
Malicious/Suspicious	2 hours	1 hour
Mitigated/Blocked	4 hours	2 hours

An "Investigation" occurs when the MDR Platform triggers a detection rule based on activity in a Comcast customer's environment and when a Comcast SOC analyst or its authorized suppliers annotates one or more events as an Investigation. Comcast MDR does not provide an SLO for unmanaged events that do not create an Investigation.

Comcast and its authorized suppliers will triage all MDR Investigations to determine whether the activity is benign or malicious. Comcast will prioritize detections based on a combination of the likelihood of malicious activity and the potential impact of the detected activity. Comcast's Investigation SLO is to begin investigation promptly in accordance with the following:

Investigation Priority	Time to Begin Investigation
Critical	15 minutes
High	1 hour
Medium	12 hours
Low	48 hours

Critical – an event in Customer's environment which contains behavior that highly correlates to tactics, techniques, and procedures utilized by threat actors. Critical alerts require immediate response and are the highest priority for the Comcast analysts to review.

High – an event in Customer's environment which contains behavior that often correlates to tactics, techniques, and procedures utilized by threat actors and are prioritized for MDR analyst review.

Medium – an event in Customer's environment which contains behavior that can correlate to tactics, techniques, and procedures that may be utilized by threat actors, but overlaps with normal administrator or user activity and requires MDR analyst review.

Low – an event in Customer's environment which contains behavior that infrequently correlates to tactics, techniques, and procedures utilized.