verizon

MANAGED DETECTION AND RESPONSE +

1. GENERAL
1.1 Service Definition
1.2 Service Implementation
1.3 Service Features
2. SUPPLEMENTAL TERMS
2.1 Customer Responsibilities
2.2 User Based Licensing
2.3 Volume Based Licensing
2.4 License Enforcement
2.5 Export Control
2.6 Third Party Warranties
2.7 Consent
2.8 Restriction on Encryption Functionality in India
3. SERVICE LEVEL AGREEMENT
4. FINANCIAL TERMS
4.1 Service Commitment
4.2 Rates and Charges
5. DEFINITIONS

1. GENERAL

1.1 **Service Definition.** Managed Detection and Response (MDR) helps identify, detect and respond to cyber threats by collecting the data required for advanced analytics and providing the platform needed for response. MDR combines endpoint detection and response (EDR), User and Entity Behavior Analytics (UEBA) and threat hunting services with security operations center triage, escalation and response by MDR analysts resulting in 24x7 protection for Customers.

1.2 **Service Implementation.** Verizon will provide Customer with a welcome kit that describes the initial information and resources Customer will need to implement MDR including agreed upon Fully Supported data sources. Fully Supported data sources are defined as data sources that have been previously fully configured and tested and available to be quickly implemented. Customer will designate a point of contact to make decisions and take appropriate actions related to the MDR service (including but not limited to, coordinating meetings with the MDR service delivery team and identifying the appropriate internal resources for configuration and implementation calls) and work with the MDR service delivery team to resolve certain issues that arise during implementation. Based upon review of the welcome kit, both parties will choose a project kickoff date. The project kickoff date must take place within 3 months of the purchase date of MDR. The project kickoff date marks the beginning of phase I of the MDR service implementation. Phase I consists of Verizon implementation of up to ten (10) Fully Supported Data Sources. Phase II of the MDR service implementation will implement the remaining agreed upon data sources. The Verizon service delivery team will defer billing for the 30 days after the project kickoff date to allow for Phase I of the MDR service implementation and allow Customer time to prepare network devices and free up required resources as necessary. The Verizon service delivery team will only monitor alerts generated during the implementation period for tuning purposes and no threat analysis or other services will be performed until RFO.

1.3 **Service Features**

1.3.1 **Data Identification and Ingestion.** MDR collects log data through a remote ingestion node (RIN). Customer may choose non-managed (On-Premises RIN; Customer Cloud RIN) or fully managed (Public Cloud; Private Cloud) RIN to deploy.

1.3.1.1 **On-Premises RIN.** The on-premises RIN consists of software that Customer will install on the Customer network via a physical or virtual machine. Customer will be remotely guided through the installation process and will provide the host server for the remote ingestion node. Customer should configure the ingestion node with additional disk space to prevent data loss when connection to the MDR platform is interrupted. Customer should not filter or modify data from standard vendor configurations so that the MDR platform can parse it properly.

1.3.1.2 **Customer Cloud RIN.** Customer cloud RIN is a Customer managed service extending RIN services to Customer's cloud environments such as AWS, GCP or Azure.

1.3.1.3 **Public Cloud RIN.** Public cloud RIN is a fully managed RIN that collects logs from Customer's cloud services such as an endpoint detection or secure web gateway cloud service.

1.3.1.4 **Private Cloud RIN.** Private cloud RIN is a fully managed RIN that provides the ability for concentration of log sources on Customer private cloud premises.

1.3.2 **Detection.** The MDR detection methods combine several techniques, including but not limited to, analytics with threat hunting and incident management.

1.3.2.1 **Analytics.** Analytics includes:

- Correlation logic which combines logs from various sources with Threat Intelligence and additional customer context to identify attack patterns that are hidden when looking at individual log messages and is monitored and tuned based on real world data.
- Threat intelligence from Verizon's threat intelligence database which includes access to industry intelligence from Verizon's telecommunications operations and incident response team.
- UEBA leads that are used to modify risk levels on correlated events and help analysts pinpoint changes in behavior by a user or device.

1.3.2.2 **Threat Hunting.** MDR proactively hunts through Customer's log data to identify threats. The threat hunting is performed by Verizon MDR analysts, leads generated by the UEBA included in MDR and the latest Threat Intelligence to help identify current threats and previously unidentified threats.

1.3.2.3 **Incident Management Component.** MDR analysts actively monitor the MDR violation queue, which uses a risk analysis engine to identify users or devices posing the highest risks to Customer environments. Customers will have visibility into the violation queue and can assign cases to MDR analysts for investigation and response.

1.3.2.3.1 **Security Incident Classification.** Verizon classifies Security Incidents into 4 categories of criticality:

Criticality	Description
High	A Security Incident that is likely to have a significant impact on the confidentiality, integrity or availability of the customer's environment.
Medium	A Security Incident that may have an impact on the confidentiality, integrity or availability of the customer's environment.
Low	A Security Incident that is unlikely to have an impact on the confidentiality, integrity or availability of the customer's environment.
None	The Security Incident is informational.

verizon

1.3.2.3.2 **Security Incident Notification.** Verizon will identify Security Incidents on the Customer Portal. Verizon will also provide notification of Security Incidents to Customer as provided in Section 3 of this Agreement.

1.3.3 **Response and Containment.** In the event of a Security Incident, MDR analysts will respond by investigating the incident and handing it off to Customer for remediation. MDR analysts may also take containment actions if required in the MDR analyst's discretion.

1.3.3.1 Supported MDR containment actions are restricted to accounts or devices that have user or asset context only so that MDR analysts are not modifying unknown devices, and include:

- Quarantining a host.
- Blacklisting file hashes.
- Removing persistence via registry key modifications (when available and supported by EDR agent).
- Initiating virus scans.

1.3.3.2 **Response and Containment Hours.** Responses and containment are limited to three hours of MDR analyst time per incident. Incidents requiring response and/or containment time greater than three hours or further investigation can be contracted separately with Customer's incident response vendor of choice or Verizon's Rapid Response Retainer service.

1.3.4 **Support.** Verizon provides Client Security Engineers (CSE) as the Customer's primary points of contact for technical security service management support. Based upon a weekly number of hours identified in the applicable Order, CSEs will conduct Customer training, review changes to the Customer environment, and run and review monthly incident reports. Verizon also provides Security Services Advisors (SSA) as the Customer's primary points of contact for day-to-day non-technical support, including but not limited to: Customer onboarding, Phase I and Phase II implementation and ongoing MDR service communications during the term of the Service. MDR also includes cyber security consultants who perform recurring, Customer specific SIEM assessments to tune threat content, identify and onboard new or unparsed log sources, and monitor and configure integrations with Customer's user or asset repositories for more accurate alert context. Security consultants will provide Customer specific focus hours on a weekly basis identified in the applicable Order.

1.3.5 **Customer Management Portal.** Customers can manage Security Incidents and receive support via the Customer Portal.

1.3.6 **Log Data Availability, Retention, and Rehydration**

1.3.6.1 Logs collected by the MDR service are retained in storage for the below described times so they are available for querying via the Customer Portal.

- **Hot Storage.** Online storage of logs collected by MDR and available in the Customer Portal for 30 days.
- **Warm Storage.** Online storage of logs collected by MDR and available in the Customer Portal for 90 days (60 days after the 30 days Hot Storage).
- **Cold Storage.** Offline or inactive data collected by MDR which can be accessed upon request for up to 365 days. Cold store data can be retrieved within 10 business days of a request through the Customer Portal and is subject to data volume restrictions.

1.3.6.2 **Rehydration of Data.** Data that is requested from Cold Storage is subject to the following:

- Customer can request a maximum of 2TB of total data volume per year.
  - Total data volume is calculated as follows: "Volume of data requested" x "number of days available within Customer Portal" = "Total data volume available" (e.g., If a Customer requests 10MB of data to be available for 7 days, then this request utilizes 70MB of total data volume).
- Customer can request up to two queries per calendar year.

- Customer may request more than two queries per calendar year or more than 2TB of total data volume per year under a separate invoice/order. Requests greater than 2TB of total data volume per year will be billed according to the fee structure provided in Section 4 below.
- Customer can request an export of log data at the end its Service Commitment or upon notice to terminate, however, the foregoing conditions still apply.
  - Customer agrees that exported log data will be delivered in raw data source format, and will only be available for external download for a period of 7 days following receipt of Customer's request.
  - Exported log data will not be visible or accessible via the Customer Portal.

2. SUPPLEMENTAL TERMS

2.1 **Customer Responsibilities.** Customer is responsible for obtaining, operating and maintaining any equipment, software and ancillary services needed to connect or otherwise use the Services, including but not limited to hardware, software and networking equipment. Customer is also responsible for maintaining the security of the equipment, Customer account, passwords and files. Customer is responsible for ensuring that appropriate data is being sent to Verizon, for the purpose of providing the MDR services.

2.2 **User Based Licensing.** Verizon will calculate Customers' data volume estimate for user based pricing based upon previous MSS industry analysis that assumes 1.5 events per second per user at 677 bytes per message. Verizon reserves the right to perform tuning or disable log sources if a Customer's license levels purchased are exceeded. Verizon may also filter or exclude data sources that put the Customer data capture beyond the expected data volume per user. If a tuned data set does not meet Customer requirements, additional users can be purchased or the licensing model can be converted to volume based licensing.

2.3 **Volume Based Licensing.** Volume based licensing will be calculated based on Customer's monthly aggregate data volume.

2.4 **License Enforcement.** For both volume based and user based licensing, license utilization will be evaluated before new devices are onboarded to verify license levels are appropriate. In the event that a customer exceeds its license level for two months in any 12 month period by less than 30%, Verizon will work with the customer to either (i) increase Customer's entitlement level or; (ii) identify and, if necessary, decrease log sources that will bring the license level back into compliance with Customer's purchased license level. In the event that a customer exceeds its license level by greater than 30% in one month in any 12 month period, Customer will have a period of no more than 15 days to be brought back into compliance with its license level. After 15 days, Verizon reserves the right to disconnect log sources or discontinue log capture until license levels are adjusted or log capture issues are corrected to be in compliance with purchased license level. In the event that Customer is on track to exceed monthly license levels by more than 50%, Verizon reserves the right to disconnect log sources or discontinue log capture until license levels are adjusted or capture issues are corrected to be in compliance with purchased license level. After three months of overages in any 12 month period, Verizon will disable log sources to bring capture below license levels and will refuse additional log sources until additional licenses are purchased.

2.5 **Export Control.** Customer will not use the MDR Service to store or transfer any technology or technical data controlled for export under applicable export control laws, including but not limited to the U.S Export Administration Regulations or the U.S. International Traffic in Arms Regulations.

2.6 **Third Party Warranties.** For any third party products and/or services incorporated as part of the MDR Service, Customer will receive only the warranties offered by such third party either directly to Customer or to the extent Verizon may pass through such warranties to Customer.

2.7 **Consent.** Customer consents to Verizon's collection and use of data and threat intelligence collected in connection with provision of the MDR services for use in an aggregated and anonymized form with Verizon's portfolio of security services to improve threat detection.

2.8 **Restriction on Encryption Functionality in India.** Prior to connecting any encryption equipment to Verizon Facilities in India, Customer must obtain prior evaluation and approval from the relevant telecom authority.

3. **SERVICE LEVEL AGREEMENT.** The Service Level Agreement (SLA) can be found at: www.verizon.com/business/service_guide/reg/managed_detection_and_response_sla.pdf.

4. **FINANCIAL TERMS**

4.1 **Service Commitment.** The Service Commitment is for a one year, two year or, three year term.

4.2 **Rates and Charges.** Customer will pay the non-recurring charges (NRCs), monthly recurring charges (MRCs) and annual recurring charges (ARCs) as set forth in the applicable Agreement. Unless expressly indicated otherwise, all NRCs will be invoiced upon Commencement Date and the initial MRCs or ARCs will be invoiced upon Service Activation Date. Requests greater than 2TB of total data volume per year (identified earlier in Section 1.3.6.2) will be billed at $220 per additional TB.

5. **DEFINITIONS.** The following definitions apply to MDR, in addition to those identified in the Master Terms.

Term	Definition
24x7	Non-stop service, 24 hours a day, seven days a week, 365 (366) days a year, independent of time zones and local or international public holidays.
Customer Portal	An online portal where Customer can have a near real time view on the Security Incidents being processed, and where they can view the company's security posture and effectiveness of the devices and services at various levels.
Device	A device, appliance, software application or a system which has been approved by Verizon for security monitoring.
Log	A collection of various IT, network, application, and security related information created by devices.
Ready for Operations (RFO)	The date that Verizon (1) completes phase I of MDR service implementation; and (2) commences Security Incident monitoring.
Security Incident	A security incident is a single or a series of unwanted or unexpected, adverse events that have a significant probability of compromising business operations and threatening security.
Threat Intelligence	Strategic, tactical, and operational intelligence used to develop applied detection policies and perform multi-factor Security Incident correlation, so that only those threats that pose a significant risk are identified.