Managed Endpoint Detection & Response

This Service ("Managed Endpoint Detection And Response for EDR") may also be referenced as: MEDR

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the *Managed Detection and Response (MDR) for EDR* offering ("Services") provided by Binary Defense and in the quantities and volumes defined in, and subject to, your quote through which you purchased the Services. MDR for EDR is a multi-faceted managed security service designed to deliver continuous threat detection, investigation, and response support through a combination of SOC Monitoring and EDR Detection Management, as further described below. The service also includes MDR Implementation & Onboarding to ensure successful deployment and operational readiness, as further described below.

2. Scope of Services

The MDR offering provides a defense-in-depth approach to security monitoring, analysis, and threat response:

- **SOC Monitoring:**
  - Continuous 24x7x365 monitoring of client environments for alert triage, threat detection, and incident escalation.
- **EDR Detection Management:**
  - The comprehensive process of creating, deploying, testing, tuning, and maintaining detection rules within supported platforms, including custom rule development based on emerging threats and client-specific requirements.
- **MDR Implementation & Onboarding:**
  - Setup, configuration, and telemetry ingestion to ensure seamless service delivery.
- **Analysis on Demand (AoD) (Optional Add-On):**
  - Expert investigative support for suspected security incidents. The AOD team is not 24x7 and will begin work during normal business hours, M-F 9am-5pm ET.
- **Threat Intelligence on Demand (TIoD) (Optional Add-On):**

    - Client-submitted Requests for Information (RFIs) are fulfilled with actionable threat intelligence developed by Binary Defense analysts.
- **Cortex XDR Platform Management (Optional Add-On):**
    - Ongoing platform configuration, policy management, and system optimization for Palo Alto Networks Cortex XDR deployments.
- **BDVision (Optional Add-On):**
    - Includes *Vision* endpoint protection and visibility.

Each sub-service is defined in a corresponding Service Description (referenced rather than duplicated)

2.1 Service Definitions and Parameters

- **RFI (Request for Information)**
    - A client-submitted inquiry regarding threat actors, vulnerabilities, or adversary tactics.
- **Per Quarter**
    - A standard calendar quarter (Jan–Mar, Apr–Jun, Jul–Sep, Oct–Dec).
- **Endpoint**
    - A physical or virtual device monitored under the service.
- **Investigation**
    - A review of suspicious alerts to assess severity and determine disposition (e.g., true positive, false positive, or benign).
- **Overage**
    - Usage beyond scoped metrics (e.g., endpoints, RFIs, ingest volume); may result in additional charges.
- **Business Hours**
    - Monday through Friday from 9:00am ET to 5:00pm ET

2.1.1. Options

- **Analysis on Demand (AoD) (Optional Add-On):**
    - Adds expert investigative support for suspected security incidents.
- **Threat Intelligence on Demand (TIoD) (Optional Add-On):**
    - Adds client-submitted Requests for Information (RFIs) for actionable threat intelligence.
- **Cortex XDR Platform Management (Optional Add-On)**

    - Adds platform support for Palo Alto Networks Cortex XDR platform.
- **BDVision (Optional Add-On):**
    - Adds BDVision offering to MEDR.

2.2 Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

- Kick-off call for onboarding and implementation planning
- Access provisioning for EDR

2.2.2. Governance Activities:

- Access to NightBeacon dashboards and incident timelines
- Monthly or quarterly reporting (based on service level)
- Governance calls or QBRs may be included for certain tiers or clients

2.2.3. Implementation Activities:

- EDR integration and tuning
- ServiceNow (SNOW) access setup for AoD and TIoD (if selected)

2.3 Client Obligations & Assumptions

2.3.1. Obligations:

The below shall not limit or diminish Client's obligations under the Agreement.

Clients must:

- Provide access and grant permissions to in-scope EDR platforms, as applicable.
- Provide and maintain valid UI and API credentials with appropriate permissions for all in-scope SIEM or EDR platforms requiring management. Service delivery is contingent upon continuous availability of these credentials.
- Notify Binary Defense of new detection requests and process them through the detection engineering team
- Not alter or modify any detections deployed or managed by Binary Defense without approval from Binary Defense.

- Assign a point of contact for coordination
- Submit RFIs via SNOW and provide context (if selected)

2.3.2. Assumptions:

- All services are delivered remotely
- English is the default language of service
- Customer infrastructure is stable and accessible
- Client licenses and owns supported platforms, except in any instance where Binary Defense owns the platform and the customer is purchasing the right to use the platform.
- Timely Client responsiveness is expected for engagements
- Binary Defense reserves the right to suppress, disable, or convert to reports for any high-volume, low-fidelity alerts (e.g., false positives, extraneous information, etc.)
- Binary Defense requires connectivity to our centralized monitoring platform or SOAR to enable 24x7 monitoring, meet service level agreements (SLAs), and ensure comprehensive investigative capabilities.
- Binary Defense SOC analysts require streamlined EDR access using Binary Defense owned authentication
- Detection rules created by Binary Defense remain the intellectual property of Binary Defense unless otherwise agreed

2.4.1 Exclusions

Unless specifically set forth in this Service Description or reasonably related thereto as jointly determined by the parties, such activities are excluded, including, for example:

- Onsite incident response or support
- Strategic threat assessments outside scope of TIoD (if selected)
- Any legal support or expert witness work
- Real-time malware reverse engineering
- Remediation beyond host isolation and account lockout where applicable
- Configuration of unsupported third-party tools

2.5 Service Level Targets and SLA Commitments

Service Component	SLA
SOC Monitoring	24x7x365 alert triage and escalation per priority in accordance with the Detection and Escalation Service Level Agreement
AoD Acknowledgment	Initiated during business hours (M–F, 9am–5pm ET)
TIoD Acknowledgment	Within 4 business hours (M–F, 9am–5pm ET)
TIoD Response	Within 72 business hours (M–F, 9am–5pm ET) when information is available to Binary Defense
Investigation Delivery	Through NightBeacon, timelines depend on priority and scope

See the applicable Service Description for each Service for more information.

3. Terms and Conditions

The Services described herein are subject to the Binary Defense Terms and Conditions, unless you have a separate written agreement in place with Binary Defense ("Agreement"). In the event of a conflict, this Service Description shall control unless otherwise expressly agreed in writing.