BINARY DEFENSE

ExtraHop Managed NDR

This service ("ExtraHop Managed NDR") may also be referenced as: ExtraHop, mNDR, 360 Managed NDR, EH

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the **ExtraHop Managed NDR (mNDR)** – *Essential or Apex* offering ("Services"), all in the quantities and volumes defined in, and subject to, your quote through which you purchased the Services. Binary Defense provides managed network detection and response (NDR) through ExtraHop Reveal(x) as part of its 360 Managed NDR program. This service delivers 24/7/365 threat detection, monitoring, and alert triage across the Client's network infrastructure as described below.

Please note that Binary Defense provides configuration, visibility, and alert handling support for the ExtraHop platform, while ExtraHop is responsible for the performance and availability of its underlying software and infrastructure.

2. Scope of Services

The Services include:

- 24/7/365 monitoring and alert triage via the ExtraHop platform
- Access to the ExtraHop Client portal
- Management and health monitoring of the ExtraHop platform instance
- Detection and response aligned to Binary Defense's use-case library as determined by Binary Defense
- Alert investigation and escalation aligned with Binary Defense-established MDR workflows
- Integration of ExtraHop telemetry into Binary Defense's broader monitoring ecosystem

Offering Tiers:

Essential:

- Continuous monitoring and alert triage
- Basic alert investigation and escalation support
- Health monitoring of ExtraHop sensor performance
- Access to platform dashboards, alerts, and reports
- Monthly threat summary reporting

Apex:

Includes all capabilities from Essential, plus:

- Enhanced detection tuning and enrichment
- Use-case alignment to client-specific threat models
- Custom investigation logic and response guidance
- Bi-weekly review of platform detections and recommendations
- Quarterly Threat Review with Binary Defense security advisors

2.1 Service Definitions and Parameters

- **NDR (Network Detection and Response)**
  - Security monitoring of network traffic to detect anomalous or malicious behavior using behavioral analytics and threat intelligence
- **Essential**
  - Baseline level of service including monitoring, alert triage, and reporting
- **Apex**
  - Advanced service tier including tailored threat modeling, deeper investigation support, and advisory reporting
- **Overages**
  - Client usage of licensed metrics (e.g., traffic volume in GBs, license count) is subject to audit and monitoring, and may incur additional charges per Binary Defense's then-current rate at the time of overage. Binary Defense has the right to immediately invoice for such overages.
- **Client Portal**
  - Access provided to ExtraHop's Reveal(x) platform interface for visibility into network events, detections, and telemetry
- **Monitoring Coverage**
  - 24/7/365 alert ingestion and triage

Client acknowledges and agrees that the ExtraHop products ("ExtraHop Products") are subject to ExtraHop's standard terms and conditions set forth at https://cloud-assets.extrahop.com/legal/customer-terms-and-conditions.pdf (as may be amended by ExtraHop from time to time), unless Client and ExtraHop enter or entered into a separate written agreement ("ExtraHop Agreement"). Client further acknowledges that ExtraHop and not Binary Defense will be responsible for performance and delivery of the ExtraHop Products in accordance with the ExtraHop Agreement. Binary Defense is not responsible and disclaims all liability, for ExtraHop, the ExtraHop Products, or ExtraHop's performance or delivery of the ExtraHop Products.

2.1.1. Options

- Service Tier Selection
  - Clients may select between Essential or Apex based on their quote and threat coverage needs
- Quarterly Threat Reviews (Apex only)
  - Optional advisory sessions to review detections, suppression opportunities, and tuning outcomes
- Overage Review
  - Additional capacity or licenses may be purchased if usage exceeds quoted limits

2.2 Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

- Onboarding kickoff with Binary Defense and Client security/IT teams
- Platform provisioning and access credential delivery (ExtraHop-managed)
- Review of service tier, quote details, and responsibilities

2.2.2. Governance Activities:

- **Essential:** Monthly summary of significant detections and alerting trends
- **Apex:** Quarterly Threat Review and alignment to client risk model

2.2.3. Implementation Activities:

- Configuration of ExtraHop sensors and Reveal(x) instance
- Tuning of alerts and detection policies based on service tier
- Integration of alert telemetry into Binary Defense MDR processes

2.3 Client Obligations & Assumptions

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

2.3.1. Obligations:

- Provide necessary access to the network for ExtraHop sensors
- Maintain infrastructure compatibility for ExtraHop deployments
- Provide contact info for escalation and reporting workflows
- Accept ExtraHop's terms and conditions (Customer Agreement) with respect to ExtraHop's Products

2.3.2. Assumptions:

- Service will be conducted remotely
- Client agrees to terms and licensing usage audits for ExtraHop services
- English is the standard language of service delivery
- Binary Defense is not liable for failures in ExtraHop's performance or availability of ExtraHop's Products

2.4 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 deployment or support
- Configuration of third-party systems or tools not explicitly stated
- MSSP-style active blocking or firewall management
- Support for unmanaged ExtraHop instances not provisioned by Binary Defense
- Any legal support or expert witness work
- Binary Defense does not provide warranties or guarantees on ExtraHop's software performance

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.