MDR Implementation & Onboarding

This Service ("MDR Implementation & Onboarding") may also be referenced as: Managed Detection & Response Implementation & Onboarding, Implementation and Onboarding, Onboarding, Implementation, Installation

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the *MDR Implementation & Onboarding* 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. These services are designed to ensure successful deployment and operational readiness for the Managed Detection and Response (MDR) service.

2. Scope of Services

The services include the following activities:

- Setup, configuration, and telemetry ingestion to ensure seamless service delivery.

2.1 Service Definitions and Parameters

- **SIEM Platform**
  - The SIEM solution in scope for Onboarding to the Binary Defense MDR services (e.g., Palo Alto Networks XSIAM, Google SecOps, Sumo Logic, etc.).
- **SIEM Vendor**
  - The provider of the SIEM Platform, responsible for the platform's software and infrastructure.
- **Business Hours**
  - Monday through Friday from 9:00am ET to 5:00pm ET

2.2 Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

Binary Defense Responsibilities:

- Kick-off call for onboarding and implementation planning
- Identification of telemetry sources and integrations

Client Responsibilities:

- Provision requisite access (web interface and API access) to in-scope SIEM and EDR platforms to deliver the MDR service
- Identification of telemetry sources and integrations

2.2.2. Governance Activities:

- Project plan for onboarding activities
- Governance calls as needed until onboarding is complete

2.2.3. Implementation Activities:

- Validate requisite access to in-scope SIEM and EDR platforms
- Validate telemetry onboarding
- Connect to the centralized BD monitoring platform
- Provision customer access to NightBeacon
- Threat Detection Engineering and Tuning

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 to in-scope SIEM or EDR platforms, as applicable.
- Assign a point of contact for coordination

- Configure Log Forwarding from Sources as Defined in the Planning phase
- Deploy endpoint agents where applicable (e.g., Vision)

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 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 SIEM and EDR access using Binary Defense owned authentication

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 support
- Configuration of unsupported third-party tools

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.