Security Operations Center Monitoring

This Service ("Security Operations Center Monitoring") may also be referenced as: SOC Monitoring

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the SOC Monitoring offering, a core component of the Managed Detection & Response (MDR) service bundle, all in the quantities and volumes defined in, and subject to, your quote through which you purchased the Services.

2. Scope of Services

The Services include 24x7x365 oversight of Client environments by the Binary Defense Security Operations Center (SOC). This includes real-time visibility into security events, threat activity, and anomalous behavior across endpoints, networks, cloud workloads, and other critical assets, all as described below.

Included capabilities:

- Real-Time Alert Triage and Validation
- Threat Detection and Correlation
- Incident Escalation and Notification
- Dashboards and Reporting

2.1. Service Definitions and Parameters

- **SOC Monitoring Coverage**
  - 24x7x365 coverage for alert triage and response, subject to the Detection and Escalation service levels as outlined in the Detection and Escalation SLA.
- **Investigation**
  - A review of suspicious alerts to assess severity and determine disposition (e.g., true positive, false positive, or benign).

- **Endpoint limit**
  - As defined in your quote. If Client exceeds 5% over the defined endpoint limit, overages will be billed pro rata through the remaining term.
- **SLAs follow the Detection and Escalation SLA**

  - P-1: Critical, phone/email notification

- P-2: High, email notification
- P-3: Medium, email notification
- P-4: Low, email notification

2.1.1. Options

N/A

2.2. Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

N/A

2.2.2. Governance Activities:

- Access to BD Platform dashboards and incident timelines
- Quarterly reporting
- Governance calls or QBRs may be included for certain tiers

2.2.3. Implementation Activities:

- N/A (Covered by Implementation Service Description)

2.3 Client Obligations & Assumptions

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

2.3.1. Obligations:

Customer must:

- Provide streamlined SIEM and EDR access using Binary Defense owned authentication
- Complete Welcome Kit documentation provided during onboarding
- Complete SOC Questionnaire documentation provided during onboarding

2.3.2. Assumptions

- All Services are delivered remotely
- English is the default language of Service delivery
- 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.

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
- Real-time malware reverse engineering
- Any legal support or expert witness work
- Remediation beyond host isolation and account lockout where applicable
- 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.