Cortex XDR Platform Management Service Description

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the **Cortex XDR Platform Management** offering ("Services") as described below and in the quantities and volumes defined in, and subject to, your quote through which you purchased the Services.

Cortex XDR Platform Management is a technical administration service that provides ongoing platform configuration, policy management, and system optimization for Palo Alto Networks Cortex XDR deployments. The Service includes access to Binary Defense's Systems Engineering team for platform administration, configuration updates, and technical support, all as described below.

2. Scope of Services

Binary Defense will deliver ongoing operational management of the Client's platform, including proactive monitoring, tuning and custom detections engineering. This service is designed to maintain platform health, optimize detection efficacy, and ensure visibility into the Client's security environment through custom and vendor-curated use cases, all as further described below.

Core Service Components

1. **Platform Administration and Configuration** - Management of Cortex XDR tenant settings, user access controls, and system configurations
2. **Policy Management and Optimization** - Creation and maintenance of security policies, exception rules, and detection configurations
3. **System Health Monitoring** - Regular platform health checks, performance monitoring, and capacity planning
4. **Update and Patch Coordination** - Coordination of platform updates, agent version management, and feature enablement
5. **Technical Reporting** - Platform utilization reports, configuration audits, and optimization recommendations

2.1. Service Definitions and Parameters

- Platform – Refers to the third-party platform solution deployed, cloud hosted or on-premise in the Client environment (e.g.,Palo Alto Cortex XDR).

- Platform Vendor – Refers to the third-party platform service provider (e.g., Palo Alto) through which Client procures the Platform.

- Custom Use Case – A detection rule or logic tailored to a specific need, threat scenario, or asset unique to the Client, created based on capabilities and access provided.

- Ruleset Tuning – Modifying detection logic, thresholds, and correlations to reduce false positives/negatives and adapt to environmental changes.

- Out-of-the-Box (OOTB) Rules – Default detection content provided by the platform vendor.

- Overage – Usage that exceeds the contracted metrics such as ingest volume (GB/day), license count, or endpoint quantity. Billed at then-current rates. Binary Defense reserves the right to audit Client usage and invoice overages accordingly when applicable.

2.1.1. Options

N/A

2.2. Planning, Governance, & Implementation

N/A

2.2.1. Planning Activities & Responsible Parties:

Binary Defense Responsibilities:

- Document current Cortex XDR configuration and deployment architecture
- Review existing policies and identify optimization opportunities
- Establish platform management procedures and change control processes
- Create platform administration runbooks
- Define regular maintenance windows and update schedules

Client Responsibilities:

- Provide Cortex XDR tenant access with appropriate administrative permissions
- Designate technical contacts for platform change approvals
- Define change management windows and blackout periods
- Communicate business requirements for platform configuration

- Approve platform changes and policy modifications

2.2.2. Governance Activities:

1. **Platform Reviews**: Review of platform health, utilization metrics, and configuration changes
2. **Optimization Sessions**: Analysis of policy effectiveness and tuning recommendations
3. **Platform Assessments**: Comprehensive platform review and roadmap planning
4. **Vendor Liaison Services**: Coordination with Palo Alto Networks for support escalations

2.2.3. Implementation Activities:

- **Platform Assessment**
- **Access and Integration**
- **Standardization**
- **Operational Transition**

2.3 Client Obligations & Assumptions

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

2.3.1. Obligations:

- **Administrative Access**: Provide and maintain administrative access to Cortex XDR tenant with appropriate role permissions
- **License Maintenance**: Maintain active Cortex XDR licensing for all endpoints under management
- **Change Approval**: Review and approve platform changes within 3 business days of recommendation
- **Maintenance Windows**: Provide approved maintenance windows for platform updates and configuration changes
- **Technical Contacts**: Maintain current technical contacts for platform-related communications
- **Asset Documentation**: Provide accurate endpoint inventory and deployment requirements
- **Vendor Relationship**: Maintain active support agreement with Palo Alto Networks
- **Infrastructure Requirements**: Ensure network connectivity and infrastructure support platform requirements

2.3.2. Assumptions

- Client maintains active Cortex XDR licensing and Palo Alto Networks support
- Platform is currently deployed and operational
- Client has completed initial agent deployment to endpoints
- Network infrastructure supports platform management requirements
- Client will approve recommended configuration changes in a timely manner
- Binary Defense will have continuous API access to the platform

- Client maintains responsibility for incident response and security operations
- Platform meets minimum version requirements for API management
- Client supports pairing the Cortex XDR gateway with the BD Multi-Tenant environment

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:

- Cortex XDR agent deployment or endpoint installation
- Security incident response or investigation
- Threat hunting or security monitoring
- SOC services or alert management
- Endpoint remediation or malware removal
- Network infrastructure management
- Operating system administration or patching
- Application management or troubleshooting
- Data recovery or backup services
- Compliance auditing or certification preparation
- End-user training or certification
- License procurement or contract negotiation
- Custom software development beyond platform configuration
- On-site support or physical intervention
- Management of non-Cortex XDR security tools
- Forensic analysis or litigation support
- Architecture design or major platform migrations

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.