BINARY DEFENSE

EDR Detection Management Service Description

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the **EDR Detection Management** 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. EDR Detection Management is a detection engineering service that provides expert creation, deployment, and continuous tuning of endpoint detection and response rules across enterprise EDR platforms. The Service includes rule optimization and threat-aligned detection strategies, all as described below.

2. Scope of Services

The Services provided under this Service Description include the following core components:

Core Service Components

1. **Detection Rule Tuning** – Regular optimization of existing detection rules to reduce false positives and improve threat coverage
2. **Multi-Platform EDR Support** – Unified detection management across supported EDR platforms
3. **Detection Lifecycle Management** – End-to-end management including creation, testing, deployment, monitoring, and retirement of detection rules
4. **Threat-Aligned Detection Strategy** – Development of detection rules aligned with current threat intelligence and client-specific risk profile

2.1. Service Definitions and Parameters

- **Detection Management:** The comprehensive process of creating, deploying, testing, tuning, and maintaining detection rules within supported EDR platforms.
- **Access Requirements:** Web interface and API access must be granted by Client to the EDR Platform for detection management.
- **Supported EDR Platforms with Full Detection Management:**

  - **Cortex XDR:** Complete BIOC (Behavioral Indicators of Compromise) and Correlation rule management
  - **Microsoft Defender for Endpoint:** Custom analytic rules within Microsoft Sentinel or custom rules within Microsoft Defender for Endpoint depending on Sentinel availability.
  - **SentinelOne:** Custom storyline active response (STAR) rules and deep visibility queries
- **Limited Support Platform:**
  - CrowdStrike Falcon: Detection Engineering will create and tune Custom IOAs (Indicators of Attack) within the CrowdStrike Falcon platform, subject to platform-specific limitations.

2.1.1 Options

- Additional SKU required for custom detection development.

2.2. Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

Binary Defense Responsibilities:

- Conduct initial EDR platform assessment and capability review
- Document existing detection rule inventory and coverage gaps
- Develop detection strategy roadmap aligned with Client security objectives
- Establish detection naming conventions and documentation standards

Client Responsibilities:

- Provide complete inventory of deployed EDR platforms and versions
- Provide requisite access to EDR platforms to deliver the service
- Identify key stakeholders and technical contacts
- Define priority assets and critical business processes requiring protection
- Communicate specific compliance or regulatory detection requirements

2.2.2. Governance Activities:

1. **Regular Service Reviews:** Quarterly reviews of detection effectiveness, false positive rates, and coverage metrics
2. **Detection Lifecycle Reviews:** Annual assessment of detection rule relevance and retirement recommendations

2.2.3. Implementation Activities:

- **Phase 1 – Platform Integration**
  - Validate API credentials and connectivity for all supported EDR platforms
  - Establish secure communication channels between Binary Defense and Client EDR platforms
  - Configure necessary permissions and access controls
  - Document platform-specific limitations and capabilities
- **Phase 2 – Baseline Assessment**
  - Inventory existing detection rules and configurations
  - Identify coverage gaps based on MITRE ATT&CK framework
  - Assess current false positive rates and detection effectiveness
  - Implement tuning or retirement of existing high false positive or ineffective rules
  - Prioritize initial detection development requirements
- **Phase 3 – Initial Detection Deployment**
  - Deploy priority detection rules based on assessment findings
  - Implement foundational detection coverage for critical attack techniques
  - Establish baseline tuning parameters
  - Configure alerting and notification workflows
- **Phase 4 – Operational Transition**
  - Transition to steady-state detection management operations
  - Implement ongoing tuning and optimization processes
  - Establish regular review and reporting cadences
  - Complete knowledge transfer and documentation

2.3 Client Obligations & Assumptions

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

2.3.1. Obligations:

- **Credential Provisioning:** Client must provide and maintain valid UI and API credentials with appropriate permissions for all EDR platforms requiring management. Service delivery is contingent upon continuous availability of these credentials.
- **Platform Licensing:** Maintain active licensing and support agreements for all EDR platforms included in service scope
- **Detection Modification:** Client must not alter or modify any detections deployed or managed by Binary Defense without approval from Binary Defense.
- **Change Notification:** Provide minimum 30-day advance notice of any planned EDR platform changes, upgrades, or migrations

- **Technical Contact Availability:** Maintain designated technical contacts available for detection validation and approval processes
- **Testing Environment:** Provide access to non-production environment for detection testing when available
- **Incident Context:** Share relevant incident data and threat intelligence to inform detection development priorities
- **Timely Feedback:** Respond to false positive reports and tuning recommendations within 5 business days
- **Platform Documentation:** Provide access to vendor documentation and support channels as needed

2.3.2. Assumptions

- Client has appropriate licensing levels for custom detection creation on all platforms
- EDR agents are properly deployed and functioning across the client environment
- Client infrastructure can support the processing requirements of custom detection rules
- Network connectivity between Binary Defense and client EDR platforms remains stable
- Client will participate in regular service review meetings and provide feedback
- Detection rules created by Binary Defense remain the intellectual property of Binary Defense unless otherwise agreed to in writing
- Client understands that detection effectiveness depends on proper EDR agent deployment and configuration
- Platform API functionality remains consistent with documented 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:

- EDR platform installation, configuration, or administration
- Endpoint agent deployment, troubleshooting, or maintenance
- Incident response or forensic analysis activities
- Any legal support or expert witness work
- Detection development for unsupported EDR platforms or technologies
- Custom integration development or API programming beyond standard detection management
- Performance tuning or optimization of EDR platform infrastructure
- Training or certification of client personnel on EDR platforms

- 24x7 emergency detection development (unless included in selected service option)
- Recovery or recreation of detection rules lost due to client platform issues
- Detection development for platforms where API access is not provided
- Compliance audit support or regulatory reporting
- Threat hunting or proactive threat discovery services
- Management of prevention policies or endpoint hardening configurations
- Detection rules requiring custom platform modifications or vendor engagement
- Support for end-of-life or unsupported EDR platform versions

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.