NightBeacon AI

This Service ("NightBeacon AI") may also be referenced as: NB-AI, NightBeacon AI Platform.

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the NightBeacon AI offering ("Services") provided by Binary Defense. NightBeacon AI is delivered as a component of Binary Defense managed security services and is subject to your applicable Service quote and parent Service Description (the "Parent Service").

NightBeacon AI is Binary Defense's proprietary AI analysis platform. It augments Binary Defense SOC analysts with automated threat analysis, classification, and enrichment — accelerating alert triage and investigation while preserving human authority over escalation, containment, and response decisions. NightBeacon AI is included by default with eligible Parent Services. Clients may opt out at the organization level.

2. Scope of Services

NightBeacon AI delivers the following capabilities in support of Binary Defense managed security operations:

- **Automated Alert Classification:** Real-time scoring of eligible incoming alerts. Each output includes a malicious/benign classification, calibrated confidence score, and human-readable rationale, surfaced to Binary Defense SOC analysts to support triage prioritization.
- **Investigation Enrichment:** On-demand deeper analysis of alerts under active investigation. Outputs include MITRE ATT&CK technique mapping, attack context, similar-threat correlation, and recommended response actions, presented in a structured analyst dossier.
- **Specialized File Analysis:** Static and behavioral analysis of files submitted by Binary Defense SOC analysts, including executables (PE/ELF/Mach-O), PDFs, Office documents, SVG files, Windows shortcuts (LNK), MSI installers, compressed archives, and Windows

Event Log exports. Includes YARA-based malware scanning and SIGMA-based Event Log detection.

- **Email and Phishing Analysis:** Full email parsing including SPF/DKIM/DMARC validation, attachment scanning, URL and QR-code analysis, typosquat and homoglyph detection, domain age and GeoIP enrichment, and impossible-travel detection. Produces a phishing probability score with per-component breakdown. For phishing workflows, NightBeacon AI may pre-populate analyst response reports to accelerate review.
- **Universal Log and Network Capture Analysis:** On-demand analysis of structured log formats (JSON, XML, CEF, LEEF, Syslog, CSV, Key-Value, and raw text) and network captures (PCAP/PCAPNG/CAP). Produces IOC extraction and MITRE ATT&CK evidence.
- **Vishing (Audio) Analysis:** Analyst submission of phone-call recordings for transcription and analysis through the standard enrichment pipeline.
- **Sandbox Detonation (Deep Scan):** Isolated detonation of suspect files in a network-restricted sandbox environment with shellcode emulation. Produces extracted indicators, behavioral findings, and elevated risk scoring on confirmed threats.
- **Explainability:** Every verdict is accompanied by token-level justification, MITRE ATT&CK mapping, contrastive explanation (what would change the verdict), and a human-readable narrative.
- **Continuous Learning:** Binary Defense SOC analyst feedback drives ongoing model improvement through a synthetic-data training pipeline. No raw Client event data is stored in or used as training data for Binary Defense's AI models.
- **Per-Customer Tuning:** Per-customer false-positive tracking with auto-tuned thresholds. Customer-scoped suppression rules with expiration and audit logging.

2.1. Service Definitions and Parameters

- **NightBeacon AI:** Binary Defense's proprietary AI platform for automated security event analysis, classification, and enrichment, delivered as a component of Binary Defense managed security services.
- **Parent Service:** The Binary Defense managed security service (e.g., MDR, MEDR, or other) through which NightBeacon AI is delivered to the Client.

- **Quick Scan:** Automated classification of an eligible alert, producing a verdict, confidence score, and rationale.
- **Standard Enrichment:** Analyst-initiated deeper analysis of an alert under investigation. Includes MITRE ATT&CK mapping, attack context, response guidance, and a structured analyst dossier.
- **Deep Scan:** Sandbox detonation of a suspect file in a network-isolated environment, including behavioral monitoring and shellcode emulation.
- **Eligible Alert:** An alert that meets Quick Scan processing criteria, including (where applicable) priority threshold and Client opt-in status.
- **Verdict:** Classification of an alert as malicious or benign, derived from a calibrated probability score.
- **Confidence Score:** Calibrated probability output expressing model confidence in the verdict.
- **Analyst Feedback:** Disposition submitted by Binary Defense SOC analysts on NightBeacon AI outputs (e.g., true positive / false positive). Used as input to the Continuous Learning pipeline.
- **Synthetic Training Data:** Privacy-safe training data generated from analyst feedback patterns. Never derived from raw Client event data.
- **Business Hours:** Monday through Friday from 9:00am ET to 5:00pm ET.
- **Overages:** Client usage of the services (endpoints) is subject to audit and monitoring. If the number of endpoints exceeds the number of endpoints defined in the Service quote, the excess endpoints will be charged at the per-endpoint rate set forth in your quote at the time of the overages. Binary Defense will invoice overage fees monthly in arrears, based on Client's endpoints as of the last day of the fiscal month.

2.1.1. Options

- **Private Customer Model:** Customer-isolated model variant blended with the base model. Available as an opt-in tier.

- **Training Data Contribution Tier:** Opt-in, opt-out, or private-model tier governing whether analyst feedback derived from the Client's environment contributes to the Continuous Learning pipeline.

2.2. Planning, Governance, & Implementation

Planning, governance, and implementation activities for NightBeacon AI are performed in conjunction with the Parent Service.

2.2.1. Planning Activities

- NightBeacon AI is included by default in Parent Service onboarding. No separate planning activity is required unless the Client elects an opt-in option.

2.2.2. Governance Activities

- Access to NightBeacon dashboards displaying analyzed events, classification history, and analyst feedback activity.
- MITRE ATT&CK technique coverage visualization, updated continuously.
- NightBeacon AI activity included in periodic Parent Service reporting (cadence determined by the Parent Service level).
- Per-customer false-positive trend information available on request.

2.2.3. Implementation Activities

- Configuration of NightBeacon AI within the Client's environment is performed by Binary Defense as part of Parent Service onboarding.
- Opt-out configuration may be requested at any time by notifying Binary Defense.

2.3. Client Obligations & Assumptions

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

2.3.1. Obligations

Clients must:

- Maintain an active engagement in a Binary Defense managed security service that includes NightBeacon AI.

- Provide access to in-scope telemetry sources as required by the Parent Service.
- Notify Binary Defense in writing of any change to NightBeacon AI opt-in/opt-out preferences.

2.3.2. Assumptions

- NightBeacon AI is enabled by default for all eligible Parent Service clients.
- All services are delivered remotely.
- NightBeacon AI operates under a human-in-the-loop design — final escalation, containment, and response decisions remain with Binary Defense SOC analysts.
- Quick Scan eligibility may be limited by alert priority, Client opt-out status, or other operational criteria. Binary Defense reserves the right to suppress or skip Quick Scan on high-volume, low-fidelity events.
- Binary Defense may improve, tune, retrain, and update NightBeacon AI models at any time without prior notice, provided core service obligations remain met.

2.4. Privacy & Data Handling

NightBeacon AI is designed so that no raw Client event data is stored in, or used to train, Binary Defense's AI models. Training data is generated synthetically from analyst feedback patterns, not from Client events.

Privacy controls include:

- No retention of raw Client events in the training pipeline.
- Pattern-based sanitization of feedback signals (including but not limited to email addresses, IP addresses, identifiers, credentials, tokens, and connection strings) prior to any training-data generation.
- Synthetic data generation operating on Binary Defense infrastructure.
- Prompt-injection defenses applied to untrusted input before any LLM processing.
- Tenant-level training-data contribution controls (opt-in, opt-out, private model).
- Audit logging of model actions, analyst feedback events, and training operations.

2.5. 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:

- Autonomous containment, isolation, or remediation actions taken without Binary Defense SOC analyst approval.
- Interactive conversational AI access by Client personnel for ad-hoc investigation.
- Customer-controlled deployment or hosting of NightBeacon AI outside Binary Defense managed security services.
- Real-time malware reverse engineering.
- AI-generated legal opinions, attestations, regulatory filings, or expert-witness output.
- Configuration of unsupported third-party tools.

2.6. Service Level Targets and SLA Commitments

Service Component	SLA
Quick Scan Availability	24x7x365, asynchronous; does not block analyst triage workflow
Standard Enrichment	Available on demand to Binary Defense SOC analysts during Parent Service operations
Deep Scan	Available on demand; sandbox execution time varies by sample
Continuous Learning	Model retraining performed on a rolling schedule; specific cadence not warranted
Privacy Controls	Controls described in §2.4 maintained at all times

Alert triage, incident escalation, and other operational SLAs are governed by the applicable Parent Service Description and Detection and Escalation Service Level Agreement.

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.