NightBeacon Command

This Service ("NightBeacon CMD") may also be referenced as: NightBeaconCMD, CMD, NightBeacon Response Portal, NB CMD.

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the NightBeacon CMD offering ("Services") provided by Binary Defense. NightBeacon CMD is a multi-tenant, cloud-hosted (SaaS) service that delivers Binary Defense's AI-assisted security operations capabilities to Clients through a customer web portal and a developer API. Through CMD, Clients receive AI-driven alarm enrichment, agentic threat hunting across their connected security platforms, incident management, investigation workflows, and on-demand deep-scan analysis of suspicious files — all in the quantities, tiers, and volumes defined in, and subject to, your quote through which you purchased the Services.

NightBeacon CMD is delivered as a hosted SaaS service accessed at the Binary Defense-issued tenant URL through the CMD web portal and/or the CMD API. No client-side software installation is required. The Service includes access to the CMD web portal, the CMD API, the underlying NightBeacon analysis engine, configured connectors to Client telemetry sources, and the managed support functions described below.

2. Scope of Services

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

- Tenant provisioning on the NightBeacon CMD SaaS platform, with the user counts, connector counts, and feature tier identified in the applicable quote.
- Access to the CMD web portal for alarm review, incident triage, investigation tracking, agentic hunting, deep-scan submissions, reporting, and tenant administration.
- Access to the CMD API for programmatic submission of security events, logs, files, and payloads; retrieval of structured enrichment results; and integration with Client SIEM, SOAR, ticketing, or custom pipeline tooling, subject to tier and rate-limit policies.

- Configured platform connectors for ingestion and on-demand query of Client SIEM, EDR, identity, cloud, email, network, threat-intelligence, and ticketing systems, subject to tier and the supported-connector list.
- AI-assisted alarm enrichment and recommendation on telemetry the Client has authorized CMD to analyze.
- Agentic Hunting AI for natural-language hunt authoring across launch-validated connectors.
- Deep Scan service for submitted file artifacts, including sandbox detonation, shellcode emulation, and LLM-driven review.
- Incident and investigation workspaces, including artifact attachment, analyst notes, and exportable reports.
- Branded PDF reporting and scheduled report generation.
- Portal-managed notifications (email and webhook) for alarms, incidents, and investigation events.
- Ongoing updates to the CMD portal, AI prompts, hunt recipes, connector adapters, and detection logic, deployed automatically without Client action.
- 24/7/365 availability of the CMD portal, subject to the platform availability targets in the Master Service Agreement.
- Detection and Escalation service levels for any Binary Defense-monitored offering consumed through CMD are governed by the applicable Detection and Escalation SLA.
- Acceptance of in-portal service tickets and notification of Clients regarding new investigations or incidents through CMD.
- Tuning of AI behavior, suppression of noisy or low-fidelity alarms, and adjustment of hunt recipes by Binary Defense as needed.
- **Credit Use:** Annual credits are provisioned upon Order Form execution and are replenished on an annual basis, unless otherwise specified in the Order Form. Annual credits are available for use during the annual term and do not carry over beyond the annual term specified in the Order Form. Credits will be deducted according to actual

use of each action type based on the table below. Unused credits expire at the end of the subscription term and are non-refundable.

Action	Credits
Quick Enrich (API)	1
Full Enrich (API)	30
Deep Scan (API)	75
Alarm ingested	3
NB Enrichment	5
Assistant AI query	10
AI Hunt run	150

- **Credit Consumption**. An AI action consumes the credits associated with its action type only when the action is executed by CMD to a result state that delivers analytical value to Client. Specifically:
- **No credit consumption for:** requests rejected before execution (invalid input, expired credentials, exceeded rate limits, unauthorized connector access); user-cancelled actions cancelled before substantive execution begins; or actions that fail due to a Binary Defense-side platform error, outage, or system timeout.

- **Credit consumption for:** actions that execute through to completion, regardless of the count of findings returned (a Hunt that runs the full pipeline and returns zero matches still consumed compute and is billable); and actions that complete with partial platform success (e.g., a Hunt where one connector returned results and another timed out at the connector vendor).

- Mid-execution failures caused by Client-side or third-party platform conditions outside Binary Defense's control (connector vendor outages, connector-vendor rate limits, credential expiry mid-Hunt) are billable if substantive execution had begun.

- Disputes regarding credit consumption may be raised through the support channel within thirty (30) days of the action; Binary Defense will review CMD's execution log for the action and reverse credit consumption where the action did not deliver analytical value.
- **Overage Handling:** If Customer's usage exceeds the annual contracted Credits in the applicable Order Form, the following terms apply:

- Overage Rate. Credits consumed above the annual contracted amount are billed at the contracted Credit rate plus twenty percent (20%).
- Overage Cap. Overage usage is permitted up to twenty-five percent (25%) of the annual contracted Credits. Usage beyond this cap requires execution of a new Order Form and purchase of additional Credits before further usage is permitted.
- Billing Cadence. Binary Defense will invoice overage fees monthly, based on Customer's actual calendar-month consumption, in accordance with the applicable Order Form.

2.1. Service Definitions and Parameters

- **NightBeacon CMD (CMD):** The Binary Defense-hosted, multi-tenant SaaS service for alarm review, incident and investigation workflows, agentic hunting, Deep Scan submission, reporting, connector administration, and service ticket management. CMD is accessible through the CMD web portal and the CMD API.
- **NightBeacon Analysis Engine:** The Binary Defense-hosted backend that performs ML classification, LLM enrichment, and orchestration. CMD consumes the engine on Clients' behalf through the CMD web portal and the CMD API; the engine itself is not directly addressable by Clients.
- **CMD API:** The Binary Defense-published REST API that provides programmatic access to CMD's enrichment, alarm, and Deep Scan capabilities. Requests are authenticated with an API key issued at provisioning, scoped to the Client's tenant, and subject to the same data scopes, suppression rules, and Advisory Output framing as the CMD web portal. Concurrency, throughput, and request-size limits are documented in the CMD API reference.
- **Tenant (Organization):** A logical isolation boundary within CMD. Each Client receives at least one tenant. Multi-tenant Clients (MSSPs) may have a parent tenant and one or more sub-customer tenants.
- **Connector:** A configured, credentialed integration between a Client-owned platform (SIEM, EDR, identity provider, ticketing system, threat-intelligence service, etc.) and CMD. Connectors are read-only by default and limited to the data scopes the Client authorizes.

- **Alarm:** A normalized event surfaced into CMD from a connected platform or from Binary Defense detection, presented to the Client with AI-generated enrichment and recommendation.
- **Incident:** An analyst-curated grouping of one or more related alarms representing a security event requiring tracking through resolution.
- **Investigation:** The analytic review of an alarm, incident, or analyst-initiated query, with attached artifacts, evidence, and conclusions, persisted in CMD.
- **Hunting AI (HuntAI):** The agentic hunting capability inside CMD that translates Client hypotheses into platform-native queries (FQL, KQL, SPL, S1QL, UDM, etc.) and executes them across launch-validated and admin-preview connectors. HuntAI-generated queries are executed on Client's behalf based on Client-supplied hypotheses; Binary Defense makes no warranty as to the performance impact, data scope, or completeness of AI-generated queries on Client platforms, and unintended side effects of query execution (including platform rate-limit violations, latency, or over-broad results) shall not constitute a breach of this Service Description or the Agreement, provided Binary Defense uses commercially reasonable efforts in maintaining the HuntAI capability.
- **Deep Scan:** The on-demand analysis service for files submitted through CMD, producing sandbox detonation results, optional shellcode emulation, and an AI-generated review.
- **Launch-Validated Connector:** A connector that has passed Binary Defense's full validation gates (setup, credential validation, adapter execution, frontend rendering, telemetry, and end-to-end tests). Customer-visible support for agentic hunting is generally available.
- **HuntAI Admin Preview Connector:** A connector whose customer-visible setup and HuntAI routing exist, but which remains under monitored preview pending tenant validation and benchmark gates.
- **User:** A named, authenticated individual provisioned into a CMD tenant with one of the supported roles (BD admin, MSSP admin, MSSP analyst, Customer admin, Customer analyst).

- **MFA (Multi-Factor Authentication):** Time-based one-time password (TOTP) second factor enforceable at the tenant level for local users. SSO-backed users satisfy MFA through the Client's identity provider.
- **SSO (Single Sign-On):** Optional federated authentication via the Client's identity provider, supported through the CMD identity broker.
- **Supported Connector:** A platform integration that Binary Defense maintains an adapter for, and on which Binary Defense makes a good-faith effort to ensure CMD will function as expected, including testing for connector-vendor API changes. The current supported connector list is published in CMD documentation and may evolve as adapters are added, promoted, or deprecated.
- **EOL (End-of-Life):** The status of a connector, API version, or browser no longer supported by its vendor. Binary Defense supports vendor-supported connector API versions and modern evergreen browsers; legacy versions are supported on a best-effort basis up to one year past vendor EOL.
- **Suppression / Low-Value Alerts:** Binary Defense reserves the right to suppress, disable, or convert to background reports any high-volume, low-fidelity events to preserve analyst focus and platform performance.
- **Advisory Output:** AI-generated enrichment, hunt queries, and Deep Scan reviews are advisory and analytical in nature. The Service is a decision-support tool; final operational, investigative, and response decisions remain with Client.

2.1.1. Options

The Service is delivered in tiered packages identified in the Client's quote:

- **Tier 1 — NB Enrichment:** API-driven alarm enrichment with an enrichment-metrics dashboard inside CMD. No incident or investigation workflows.
- **Tier 2 — NB Response:** Full AI-SOC experience — alarms, incidents, investigations, agentic hunting, Deep Scan, reporting, and connector management for a single tenant.
- **Tier 3 — NB Response MSSP:** Multi-tenant Tier 2 with parent / sub-customer hierarchy, MSSP analyst roles, and white-labeling controls. MSSP Clients are solely responsible for entering into appropriate agreements with their sub-customers governing the use of

CMD and any white-labeled version thereof. Binary Defense has no contractual relationship with, and no liability to, sub-customers; all claims arising from sub-customer use of CMD must be brought against the MSSP Client, not Binary Defense.

Add-on options that may be enabled per quote include additional connector seats, additional Deep Scan submission volume, additional report scheduling, and white-label branding (Tier 3). All tier and add-on selections are governed by the quote; opt-in modules outside the quote require a written change order.

2.2. Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties

- Binary Defense provisions the Client tenant (or parent + sub-customer tenants for MSSP) and issues initial admin credentials.
- Client identifies in-scope platforms for connector configuration, designates initial admin users, and confirms whether SSO will be used at go-live.
- Binary Defense and Client jointly confirm tier, user count, connector count, ingestion volume, and Deep Scan submission volume against the quote.

2.2.2. Governance Activities

- Binary Defense maintains the supported-connector list, AI prompts, hunt recipes, and detection logic as part of the platform.
- Client tenant admins govern user provisioning, role assignment, MFA enforcement, SSO configuration, connector credentials, suppression rules within their authority, and notification routing for their own tenant.
- MSSP tenant admins additionally govern sub-customer creation, sub-customer user assignment, and white-label branding within their parent scope.

2.2.3. Implementation Activities

- **Tenant Provisioning:** Binary Defense creates the Client tenant on the CMD platform.
- **Identity Setup:** Client provisions the initial admin user(s); admins then provision additional users, configure roles, and (optionally) enable organization-wide MFA enforcement and / or SSO.

- **API Credential Provisioning:** Where the Client elects to use the CMD API, Binary Defense issues API key(s) to the Client's designated technical contact. Client integrates the API into its SIEM, SOAR, ticketing system, custom pipeline, or other consuming tooling; integration design, development, testing, deployment, and ongoing maintenance are Client responsibilities.
- **Connector Configuration:** Client tenant admins configure connectors through the CMD onboarding workflow by supplying credentials and authorizing the requested read-only scopes for each platform. Binary Defense validates the connector and confirms agentic execution is enabled where applicable.
- **Notification Routing:** Client configures email recipients and / or webhook destinations for alarms, incidents, and investigation events.
- **Initial Tuning:** Binary Defense and the Client jointly tune suppression rules, alarm routing, and report templates as appropriate for the tier.

2.3. Client Obligations & Assumptions

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

2.3.1. Obligations

- Provision and maintain authorized administrator and analyst users in CMD, and remove access for users who no longer require it.
- Provide and maintain valid, scoped credentials for each connector the Client elects to integrate with CMD, and rotate credentials in accordance with Client's internal policies.
    - Authorize only the data scopes Client intends Binary Defense to access through CMD. Connectors are read-only by default; any write or respond capability is opt-in and explicitly scoped at connector setup. CMD distinguishes two classes of write capability: Telemetry write-back (e.g., pushing incidents or comments into Client's ticketing system via the connected ServiceNow or Jira connector). This is enabled by Client at connector setup and constrained by the API scopes Client grants to the connector credentials.
    - Active response actions on Client systems (e.g., endpoint containment via the connected EDR, user disablement via the connected identity provider, session revocation). These actions are governed by a CMD Playbook, a versioned, status-

controlled automation definition that Client activates within CMD. Each active Playbook identifies the permitted action types, authorization conditions (including any required analyst confirmation), and escalation contacts, and is auditable through CMD's execution log. No active response action shall be taken on Client systems except through an active CMD Playbook authorized by Client.

- Maintain the configuration and licensing of Client-owned source platforms (SIEM, EDR, identity, ticketing, etc.) such that the configured connectors continue to function.
- Use a supported, evergreen browser to access CMD.
- Where MFA is required by Client policy or by the tenant mfa_required setting, ensure users complete MFA enrollment.
- Submit only files for Deep Scan that the Client has the legal right to submit and analyze.
- Not submit PHI, PCI cardholder data, Social Security numbers, biometric identifiers, classified or export-controlled material, plaintext passwords or secrets, children's data, or any other data restricted under the Agreement.
- Provide and maintain accurate authorized contact information for tenant administration, billing, and service notifications.

2.3.2. Assumptions

- Service is delivered remotely as a SaaS web application.
- English is the default language of delivery and of the user interface.
- Client is responsible for the licensing, configuration, and maintenance of Client-owned source platforms and identity providers integrated with CMD.
- Binary Defense is responsible for the availability and ongoing maintenance of the CMD SaaS platform itself, including the underlying NightBeacon analysis engine and platform infrastructure, on a commercially reasonable efforts basis. Binary Defense will implement reasonable technical and organizational security measures for the CMD platform consistent with industry standards.
- Connector vendor APIs are subject to change by their vendors. Binary Defense is not responsible for delivery interruptions caused by vendor API deprecations or rate-limit

changes outside Binary Defense's control, but will make a good-faith effort to maintain compatibility within the supported window.

- Connector capability tiers (launch-validated, HuntAI admin preview, adapter implemented, deferred) and the underlying supported-connector list may change over time as adapters are added, promoted, or deprecated.
- AI-generated enrichment, hunt queries, and Deep Scan reviews are decision-support outputs. Client is responsible for the final disposition of any alarm, incident, investigation, or response action.
- Binary Defense is not responsible for the timing of any product roadmap transitions, deprecations of preview features, or changes to non-launch-validated connectors.
- Resale, white-labeling, sublicensing, or service-bureau use of the Service outside the contracted MSSP tier is not permitted under this Service Description and requires a separate written agreement.

2.4. 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, on-premises deployment, or any non-SaaS delivery of CMD.
- Custom connector development for platforms not on the supported-connector list.
- Active blocking, automated containment, or remediation actions executed on Client systems by Binary Defense.
- Forensic-level endpoint or memory analysis beyond what the Deep Scan service produces.
- Any legal support, e-discovery, or expert witness work.
- Real-time alerting configuration outside CMD's in-platform notification capabilities.
- Direct Client access to Binary Defense's internal correlation, detection-engineering, or model-training infrastructure.
- Development of custom AI prompts, custom ML models, or custom hunt recipes outside the standard tuning process.

- Ingestion of, or analysis on, data from platforms or scopes the Client has not authorized through a configured connector.
- Hard uptime guarantees, service credits, or refunds beyond those expressly stated in the Master Service Agreement; the Service is otherwise provided on a commercially reasonable efforts basis.
- Service in languages other than English unless explicitly contracted.

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.