NightBeacon CMD Implementation & Onboarding

This Service ("NightBeacon CMD Implementation & Onboarding") may also be referenced as: CMD Implementation & Onboarding, Implementation and Onboarding, Onboarding, Implementation, Installation.

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the NightBeacon CMD Implementation & Onboarding 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.

NightBeacon CMD Implementation & Onboarding is a professional services engagement that provides a Binary Defense implementation engineer who works directly with the Client to enable rapid adoption of NightBeacon CMD and to shorten ramp-time to expertise and value realization. It is a required component of every NightBeacon CMD purchase, delivered in the hour allotment described in Section 2.1.1.

Relationship to the NightBeacon CMD Service Description. This engagement complements, and does not replace or alter, the onboarding activities included in the NightBeacon CMD Service Description ("CMD SD"). Capitalized terms used but not defined herein have the meanings given in the CMD SD. Where this Service Description and the CMD SD address the same activity, the CMD SD's allocation of responsibilities governs; this Service Description adds engineer-led guidance and acceleration of those activities.

2. Scope of Services

Delivered by the assigned implementation engineer, up to the contracted hours, the Services include:

Onboarding kickoff and implementation planning.

Guided identity setup, including provisioning of users and roles and, where elected, organization-wide MFA enforcement and/or SSO.

Hands-on assistance configuring Connectors to Client telemetry sources through the CMD onboarding workflow, and validating telemetry ingestion.

Guidance on CMD API key issuance and initial use, where the Client elects to use the CMD API.

Assistance configuring notification routing (email and/or webhook).

Initial tuning of suppression rules, alarm routing, and report templates, conducted jointly with the Client.

Administrator and analyst enablement across the CMD capabilities included in the Client's tier (alarm review, incident and investigation workflows, agentic hunting, Deep Scan, and reporting).

A go-live checkpoint and value-realization review.

2.1 Service Definitions and Parameters

NightBeacon CMD Implementation & Onboarding (the "Engagement")

A professional services engagement of Binary Defense implementation engineering, delivered remotely, that accelerates the Client's adoption of NightBeacon CMD. The hour allotment provided is identified in the quote, as described in Section 2.1.1.

Implementation Engineer

The Binary Defense engineer who works directly with the Client to deliver the activities defined herein.

NightBeacon CMD (the "Platform")

The Binary Defense-hosted, multi-tenant SaaS service onto which the Client is being onboarded, as defined and governed by the CMD SD.

Business Hours

Monday through Friday from 9:00am ET to 5:00pm ET.

2.1.1 Implementation Hours

Implementation engineering is provided in the allotment identified in the Client's quote:

NightBeacon CMD: ten (10) hours, required with and automatically added to every NightBeacon CMD purchase.

Multi-tenant (MSSP): forty (40) hours, covering onboarding of the parent and its sub-customer tenants.

Additional time: available in ten (10) hour increments beyond the applicable allotment, subject to a separate quote or written change order, whether to complete an implementation that requires more time or to support a customer or MSSP with adoption, troubleshooting, or knowledge transfer.

2.2 Planning, Governance, & Implementation

2.2.1 Planning Activities & Responsible Parties

Binary Defense Responsibilities:

Kickoff call for onboarding and implementation planning.

Identification, jointly with the Client, of telemetry sources and Connector integrations in scope.

Client Responsibilities:

Provision requisite access (web interface and API access) to in-scope security platforms to enable Connector configuration with NightBeacon CMD.

Identification of telemetry sources and integrations.

Designate a point of contact and the initial administrator user(s).

2.2.2 Governance Activities

Project plan for onboarding activities.

Governance and checkpoint calls as needed until onboarding is complete.

2.2.3 Implementation Activities

Guide provisioning of Client access to NightBeacon CMD, including SSO or native MFA enrollment.

Work alongside Client tenant administrators to configure Connectors and validate telemetry ingestion; coordinate Binary Defense Connector validation where applicable.

Assist with CMD API key issuance and initial calls where the Client elects to use the CMD API.

Assist with notification routing for alarms, incidents, and investigation events.

Conduct initial tuning of suppression rules, alarm routing, and report templates jointly with the Client.

Deliver administrator and analyst enablement for the capabilities included in the Client's tier.

Conduct a go-live checkpoint to confirm operational readiness.

2.3 Client Obligations & Assumptions

2.3.1 Obligations

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

Clients must:

Provide access to in-scope SIEM, EDR, identity, or other security platforms, as applicable, for Connector configuration.

Assign a point of contact for coordination.

Provision and maintain authorized administrator and analyst users in CMD.

Provide and maintain valid, scoped credentials for each Connector the Client elects to integrate.

Configure log forwarding from sources as defined in the Planning phase.

Respond in a timely manner and complete Client-side activities within the Engagement window.

2.3.2 Assumptions

All Services are delivered remotely.

English is the default language of service.

The Engagement is delivered during Business Hours, in the hour allotment described in Section 2.1.1.

Customer infrastructure is stable and accessible.

Client licenses and owns supported source platforms; NightBeacon CMD is owned by Binary Defense and the Client is purchasing the right to use the Platform.

Timely Client responsiveness is expected for the Engagement.

Ongoing availability, maintenance, and operation of the Platform are governed by the CMD SD, not by this Service Description.

The Services are professional services delivered on a commercially reasonable efforts basis, and Binary Defense does not warrant any particular outcome, timeline, or result. AI-assisted enrichment, hunt queries, tuning recommendations, and Deep Scan reviews are advisory and analytical in nature; final operational, investigative, and response decisions remain with the Client, as further described in the NightBeacon CMD Service Description.

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 and any non-SaaS or on-premises deployment.

Configuration of unsupported third-party tools and custom Connector development for platforms not on the supported-connector list.

Design, development, testing, deployment, or ongoing maintenance of the Client's CMD API integrations, which remain Client responsibilities under the CMD SD.

Ongoing platform operation, monitoring, and tuning after the Engagement, which are governed by the CMD SD and any applicable Detection and Escalation SLA.

Ongoing Managed Detection and Response (MDR) monitoring and 24x7 SOC services.

Implementation hours beyond those contracted in the applicable quote.

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.