

DATASHEET

Managed Detection and Response

Decisions, Not An Alert Queue

Binary Defense detects and isolates threats early in the attack lifecycle. Our analysts bring an attacker's mindset, monitoring your environments 24x7x365 as an extension of your team. They work in NightBeacon CMD, the AI-driven SOC workbench behind our MDR, which correlates related alarms into one verdict-ready Situation so investigation starts with roughly 80% of the work already done. Every event gets triage, full MITRE ATT&CK-mapped analysis, and tactical mitigations your team can act on.

Precision Threat Intelligence

The Binary Defense SOC is your early warning system, scanning your infrastructure around the clock for the activity and anomalies that signal danger. NightBeacon CMD unifies that telemetry across 130+ connectors, scans it against 8,700+ malware rules, and enriches every alarm with ARC Labs research and MITRE ATT&CK context, so what matters surfaces as one correlated Situation, not scattered alerts.

- 24x7x365 monitoring, detection, analysis, and response capability that operate as an extension of your team.
- Event triage, notification, MITRE ATT&CK analysis, tactical mitigations, documentation, and reporting.
- Find threats faster, with greater consistency and accuracy, across your entire attack surface, before they can cause damage.
- Cuts through endless alerts in NightBeacon CMD to separate real threats from noise, enriching alerts with context and working with you to validate every step.
- Analysis on Demand for level 2-3 forensics and attack reconstruction.
- Threat Intel On Demand gives you targeted, quarterly insights into the threats that matter most, so you can stay ahead of attackers and act before risk turns into impact.
- Known IOCs and static signatures are continuously applied in NightBeacon CMD, strengthening your environment's resilience against attacks.
- Provides guided responses with actionable advice to contain and remediate specific threats, advising organizations on the right steps to take.

"Binary Defense differentiates itself from other providers via its deep understanding of how attackers operate... and its approach to detection, investigation, and response."
Forrester Wave: Managed Detection and Response 2025

For Teams Who Won't Compromise

Our Approach:

- Attack-mindset drives defense-in-depth
- Human insight + adaptive tech = stronger defense
- NightBeaconAI makes our analysts faster, never a black box that replaces them
- Alarms are the unit of detection, Situations are the unit of work
- You bring your security tools, we amplify their impact
- An out-of-the-box solution tailored to your unique needs and challenges
- We think differently when it comes to MDR, building around what's best for you

NightBeacon CMD, AI-Driven SOC Workbench

> Binary Defense runs NightBeacon CMD in its own 24x7x365 SOC, with U.S.-based analysts in the driver's seat, owning every decision. MDR clients get machine-speed analysis and human-owned outcomes.

HOW WE DELIVER MDR

Our analysts in the driver's seat

We run NightBeacon CMD inside our own 24x7x365 SOC. NightBeaconAI does the analysis at machine speed; our analysts own every decision and stand behind every outcome.

Built and trained in a live SOC

NightBeaconAI is trained on years of real analyst decisions across a large, diverse client base. It sharpens every shift, operational signal a tool-only vendor cannot copy.

Detections that run in your own SIEM

Detection content is authored and versioned in NightBeacon CMD, then deployed into your own SIEM in its native query language across 9 platforms. When a rule fires, the alarm returns tied to the exact rule that raised it, so noise and outcomes score per rule and feed continuous tuning.

WHAT MDR CLIENTS GET

Faster detection and response

Related alarms auto-correlate into one verdict-ready Situation before an analyst opens a ticket, so our SOC decides in minutes, not after 20 to 40 minutes of manual context assembly.

Human-owned decisions

Nothing reaches you without a human reviewing it, standing behind it, and owning the outcome. High-impact actions are always analyst-approved.

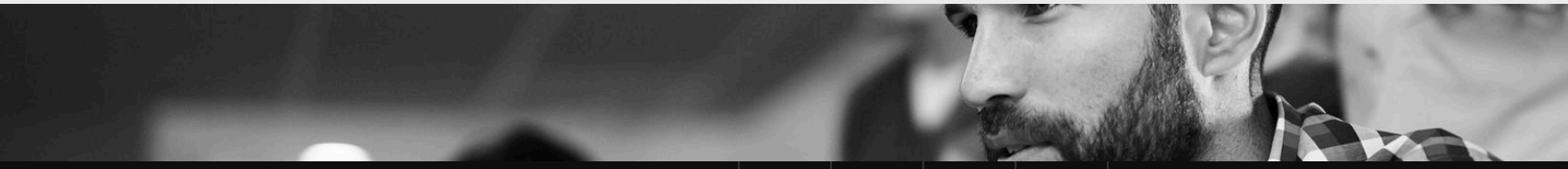
Glass-box explainability

Every verdict shows its evidence and reasoning, mapped to MITRE ATT&CK. Findings you can defend to a board, an auditor, or a cyber-insurer.

~80%	~46%	24x7x365	130+
Of the investigation pre-built before an analyst engages	Faster Situation summarization for the client write-up	U.S.-based analysts who own every decision	Connectors unifying your whole stack

"I haven't seen another product that combines the visibility that Binary Defense MDR offers with the response times of the SOC."

Mike Saunders, Principal Consultant in Information Security



Two Ways We Deliver MDR

Turnkey MDR and Platform Management are the two subset delivery methods of MDR. Both run in our 24x7x365 SOC on NightBeacon CMD, with our analysts owning every decision. The difference is whether we stand up and run the underlying stack for you, or layer onto the stack you already own.

Turnkey MDR

Subset delivery method of MDR

Binary Defense delivers Turnkey MDR by fully managing your SIEM and security operations end to end. We take care of implementation, detection engineering, continuous tuning, and 24x7 monitoring so your security program produces real results without adding operational burden.

Our analysts and engineers handle deployment, threat-informed detection strategy, ongoing tuning, and 24x7 coverage protecting you against the latest emerging threats, with every Situation investigated and decided in NightBeacon CMD.

Your client experience is NightBeacon CMD. You log in to the same surface our analysts work from: Situations with the full evidence trail, MITRE ATT&CK mapping, and coverage reporting. There is nothing for your team to stand up, tune, or maintain, and no queue to manage.

Platform Management

Subset delivery method of MDR

Already invested in a SIEM or XDR platform? We layer onto it. Binary Defense handles implementation, detection engineering, continuous tuning, and 24x7 SOC monitoring across platforms like Sentinel, Palo Alto Networks Cortex XSIAM, Google SecOps, Sumo Logic, and more.

Detection engineering runs both directions. We author and govern detection content in NightBeacon CMD, then deploy it into your own SIEM in its native query language across 9 platforms. When a rule fires, the alarm flows back with lineage to that exact rule, so noise and outcomes are measured per rule.

Your team keeps access and ownership. We bring the expertise, the coverage, and the 24x7 eyes. You keep the visibility and control, and the platform you already paid for starts working the way you expected it to.

Built Around Your Program

Co-Managed SIEM and XDR

enriches your security investments to deliver maximum ROI and increase security maturity, with NightBeacon CMD unifying your stack across 130+ connectors

Security Orchestration and Automation

enables deep integration while allowing you to retain full ownership of data, with NightBeacon CMD connectors read-only by default and response actions analyst-approved

Ability to Scale

as your business grows

Flexible Engagement Models

focused on driving security objectives

Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our blog for the latest insights, or follow us on LinkedIn.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com



BINARY DEFENSE