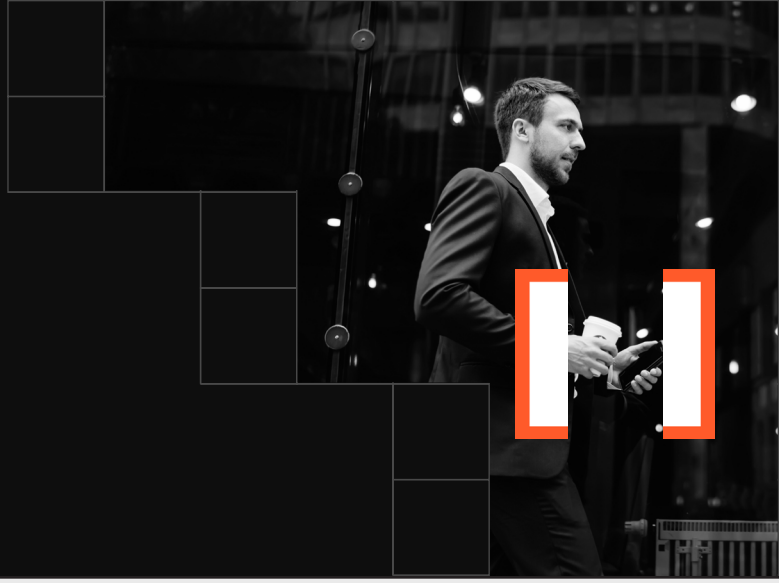
DATASHEET

NightBeaconAI



Faster Decisions. Fewer Missed Threats. AI You Can Explain.

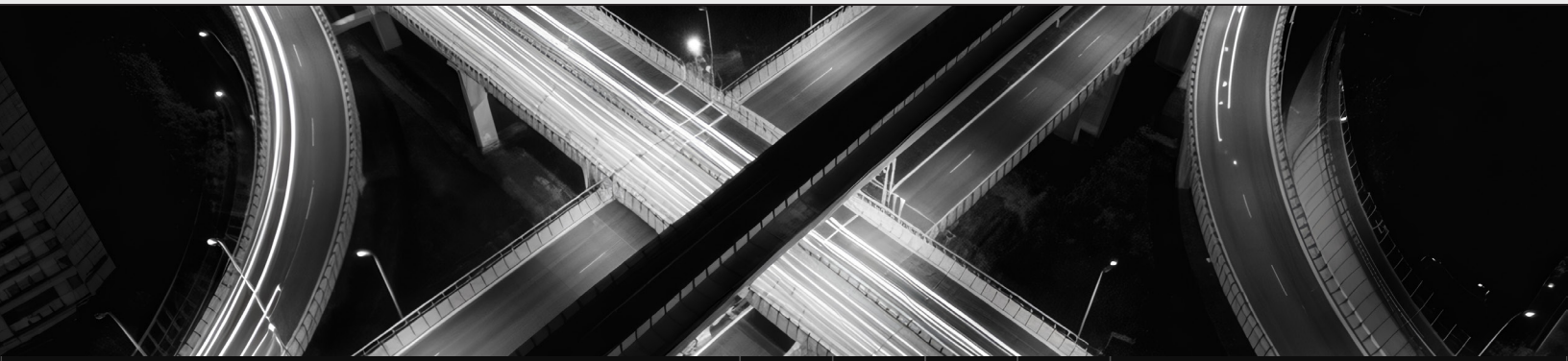
NightBeaconAI is Binary Defense's purpose-built AI engine: trained on real threats and real analyst decisions inside a live MDR operation, not built in a lab. It takes the flood of raw alerts hitting your environment and turns them into evidence-backed investigations our analysts can act on immediately. NightBeaconAI powers our SOC analysts, so you get the outcome: faster detection, defensible verdicts, and a SOC that gets sharper every shift.

~30%	35%+	~46%	<10 min
MTTR Reduction	More Alerts Processed	Faster Summerization	Research to Production Detection

The Problem We Solve For You

SOC teams are drowning in alerts. Attackers aren't waiting.

The average attacker breakout time is now 29 minutes: the window between initial access and lateral movement. Traditional SOCs lose that window to alert triage: sorting noise from signal, chasing context across tools, and writing up what happened. NightBeaconAI collapses that work so our analysts spend their time on decisions, not data collection. You get answers inside the window that matters.



How The Engine Works Inside Our SOC

From raw alert to finished investigation, in seconds

Every alert your environment generates reaches our SOC already scored, contextualized, and grounded in how real analysts respond to real threats. Three layers do the heavy lifting before a human ever picks it up.

1 Classify	2 Fuse	3 Investigate
Deep-Learning Model A classifier fine-tuned on proprietary threat intel and years of live MDR data scores every event malicious vs. benign. Not a generic model. Not a lab: the decisions our own analysts have made in production. Tge benefit: Every alert arrives pre-triaged, not raw.	**Signal Fusion Ensemble** NightBeaconAI blends multiple detection layers into one confidence score. When layers agree, we act fast. When they conflict, we surface the disagreement rather than bury it. The benefit: Fewer false positives, fewer missed threats.	**Agentic Investigation Pipeline** What takes an analyst ~45 minutes to investigate manually, our SOC resolves in minutes: cross-reference, deobfuscate, map to MITRE ATT&CK, synthesize a verdict autonomously. The benefit: Finished investigations, not alerts to sort.

Every action our analysts take is visible. Nothing executes without human approval: NightBeaconAI augments our analysts, it never replaces them.

Works With What You Already Have

No rip-and-replace. Your stack stays exactly as it is.

When a new alert needs more context, our analysts don't stop to go find it. NightBeaconAI reaches back into your connected systems automatically, pulls what it needs, and hands our SOC a higher-confidence determination before a human decision is required. That speed is what closes the gap between when a threat enters your environment and when we act on it.

We support 100+ connectors today. If you don't see yours, let us know. New connectors are added weekly.

One analyzer per file type. No hex editors. No manual reverse engineering. No time lost.

Every file and email your environment produces gets analyzed by a dedicated NightBeaconAI module before it reaches our analysts. They walk into every investigation already knowing what the file does, how it behaves, and where it maps on MITRE ATT&CK.

Executables (PE / ELF / Mach-O) Static disassembly, API call analysis, packer signature detection, shellcode emulation, and sandbox detonation. The engine spins up a container, detonates the file, and monitors its behavior in a live environment.	**Office Documents** Macro decompilation, VBA source exposure, and DDE attack detection.
Email QR code extraction from headers, attachment analysis, domain age flagging on recently registered sites, and a dedicated business email compromise investigation workflow.	**SVGs** 55 pattern-based detections across 7 categories, Shannon entropy analysis, and payload decoding.
PDFs Embedded JavaScript and launch action detection.	**Archives** Hidden payload detection and compression bomb identification.
LNK Shortcuts Suspicious target and icon spoofing analysis.	**MSI Installers** Embedded script detection.
Windows Event Logs 4,000+ SIGMA detection rules via Hayabusa.	

Every analyzer feeds the same explainability layer, so our analysts escalate on evidence your team can see and verify, not a verdict they have to trust.

Every Verdict Is Defensible

Not a black box. A glass box.

Every CISO eventually has to explain their AI to the board. NightBeaconAI answers that before they have to: every alert gets a grade and a reason, so our analysts escalate on evidence they can stand behind, and you get a clear record of every call we made.

> "It's malicious because of X. Remove X and it would be benign."
> Contrastive analysis: what tipped the call, and what would flip it

LIME/SHAP	Attention
Token-level reasoning See exactly which words, patterns, and indicators drove the classification: not just what the model concluded, but what it paid attention to.	**Weighting visualization** A visual breakdown of what the model weighted in each event so any score can be challenged and understood.
MITRE/ATT&CK	**Attention**
Mapped automatically Every finding maps to specific ATT&CK techniques, exported as Navigator layers with heatmap visualization.	**Report-ready write-up** Every escalation ships with a complete threat narrative: evidence and reasoning already written, ready to drop into your tickets and reports.

Our analysts escalate on evidence, not instinct. You get a clear picture of what happened: not a closed ticket.

Tuned to you

Most AI tools go static the day they deploy. NightBeaconAI doesn't: every analyst decision across every Binary Defense deployment sharpens the model protecting you.

- Per-customer false-positive tracking with automatic threshold adjustment, so alerts in your environment get more accurate over time.
- Customer-specific suppression rules with expiration and audit logging, so known-good activity stops creating noise without permanently hiding anything.
- You inherit every investigation our SOC has ever run. This week's coverage is better than last week's.

Private by architecture

When a CISO asks "is my data training your model?" the answer is no: enforced by design, not policy.

- No customer event is ever stored or used as training data. Full stop.
- Analyst feedback generates synthetic variations that carry the learning signal without exposing any underlying event content.
- The engine improves from collective SOC expertise across every deployment: never from your raw telemetry.

Attackers don't wait for an analyst to finish enriching a ticket, which means seconds count. NightBeaconAI processes every event the moment it enters the pipeline, handing our SOC analysts alerts already classified, deobfuscated, correlated across 80+ threat intelligence sources, and mapped to MITRE ATT&CK. By the time a human is in the loop, the work is done.

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