



DATASHEET

Co-Managed Platform

Maximize the Value of Your Security Tool Investments and Unlock Visibility with Binary Defense's Expertise

Deploying, maintaining, and monitoring SIEMs, XDR, and EDR platforms can be tedious and challenging without the resources and expertise to optimize fully. At Binary Defense, we collaborate with your organization to provide a tailored, Co-Managed Platform solution that maximizes the usability and value of your data, effectively reducing blind spots and enhancing your security operations and posture. Our personalized Co-managed Platform solution not only lowers costs and simplifies security operations but also fortifies your security stance with a custom detection strategy, continuous tuning, and 24x7x365 monitoring to safeguard against threats. Our 24x7x365 SOC leverages NightBeacon CMD, our AI-driven SOC workbench, pairing machine-speed analysis with U.S.-based analysts who own every decision to deliver Managed Detection and Response. Bi-directional sync keeps every Situation aligned with your SIEM or SOAR automatically, so your team keeps working where they already live and nothing drifts out of sync.

150+
SIEMs

have been successfully deployed
by the Binary Defense team of experts

Key Features:

Tailored Deployment

- ◆ Our experts collaborate with your team to pinpoint essential logs and eliminate unnecessary noise, thereby reducing SIEM costs.
- ◆ Tailored automation and playbooks are developed to streamline response to alerts.
- ◆ Areas of improvement are identified, and recommendations are provided to close security gaps, enhancing your long-term security posture.

Ongoing Tuning

- ◆ Ongoing policy and alarm tuning to reduce false positives
- ◆ Security posture and risk management reviews
- ◆ Security alarm enrichment with recommended triage and remediation steps

Personalized Detections

- ◆ A core set of Binary Defense Detections gathered from years of intelligence is deployed to the SIEM
- ◆ Expert detection engineering team works with you to create, deploy, and tune a personalized detection strategy that meets your needs and is constantly reviewed based on our Threat Intelligence and emerging threats.

Continuous Monitoring

- ◆ Peace of mind with 24x7x365 monitoring, alert triage and threat investigation
- ◆ Binary Defense experts helps with updates/upgrades, health checks, troubleshooting, and engaging with third-party vendors

NightBeacon CMD in Our SOC

Binary Defense runs NightBeacon CMD, our AI-driven SOC workbench, inside our own 24x7x365 SOC, layered onto the platform you already own. Related alarms auto-correlate into one verdict-ready Situation before an analyst opens a ticket, so investigation starts with roughly 80% of the work already done.

Detection content is authored in NightBeacon CMD, then deployed into your own SIEM in its native query language. Every verdict shows its evidence and reasoning, mapped to MITRE ATT&CK: a glass box, not a black box. NightBeaconAI does the analysis; our U.S.-based analysts own every decision.

Work With What You Have

While not exhaustive, these are the key technologies we frequently integrate with and support. Our platform works alongside the tools your team already relies on delivering stronger outcomes without disruption.

	Implementation	Detections	Tuning	Management	SOC Monitoring	Managed Threat Hunting	Premium Threat Hunting
SIEMS							
Sentinel	✓	✓	✓	✓	✓	✓*	✓*
Palo Alto Networks Cortex XSIAM	✓	✓	✓	✓	✓	✓*	✓*
Splunk		✓	✓	✓	✓	✓*	✓*
Sumo Logic	✓	✓	✓	✓	✓	✓*	✓*
Google SecOps	✓	✓	✓	✓	✓	✓*	✓*
CrowdStrike NG					✓	✓*	✓*
ExtraHop			✓	✓	✓		✓*
Add-On							
Cribl		✓	✓	✓			
EDRs							
CrowdStrike		✓	✓		✓		✓
Sentinel One		✓	✓		✓	✓	✓
Microsoft Defender		✓	✓		✓	✓	✓
Palo Alto Networks Cortex XDR	✓	✓	✓	✓	✓	✓	✓

*These are considered secondary threat hunting sources that are used to enrich threat hunts. A supported EDR is required for threat hunting.

Table Definition Key

Implementation

Deployment of a SIEM within a customer environment from the ground up. Includes identifying and onboarding log sources, integrating SIEM alerts into the Binary Defense environment, and performing initial tuning to ensure optimal visibility and performance.

Detections & Tuning

Continuous refinement and application of Binary Defense's threat-informed detection strategy to enhance alert fidelity and minimize false positives.

Management

Ongoing administration of the SIEM or EDR platform, including updates, upgrades, health checks, troubleshooting, and coordination with third-party vendors. Includes continuous tuning and applying Binary Defense's threat-informed detection strategy.

SOC Monitoring

Binary Defense's 24x7x365 monitoring service, where SOC analysts provide real-time analysis and response for all SIEM and EDR alerts to detect and mitigate threats promptly.

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