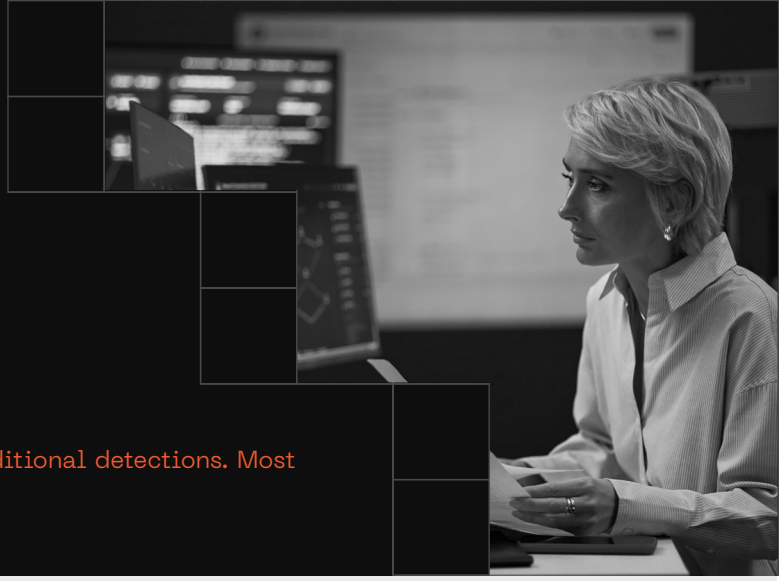
DATASHEET

# Managed Threat Hunting

Modern attackers blend into normal activity and slip past traditional detections. Most teams lack the time to proactively hunt.



## Stop waiting for alerts. Start hunting.

HYPOTHESIS-DRIVEN

100% US-BASED THREAT HUNTERS

NO ADDED HEADCOUNT

### Human Driven Hunting Tuned To Your Environment

Managed Threat Hunting provides proactive, hypothesis-driven threat hunting across your environment using your existing security platforms to surface stealthy activity that signature- and indicator-based detection misses.

| APPROACH | CADENCE | DELIVERY | TEAM |
|---|---|---|---|
| Hypothesis-driven hunts | Continuous, closedloop | Fully managed, zero overhead | 100% US-based threat hunters |

## Why advanced threats stay hidden.

### See what your tools can't

Surface attacker activity that slips past signature-based and automated detection, before it becomes an incident.

### Shrink attacker dwell time

Catching suspicious behavior early limits lateral movement, privilege escalation, and the cost of a breach.

### Coverage without the overhead

No hypotheses to define and no working sessions to attend. We run the hunts; you get the outcomes.

# Proactive threat hunting that scales with you.

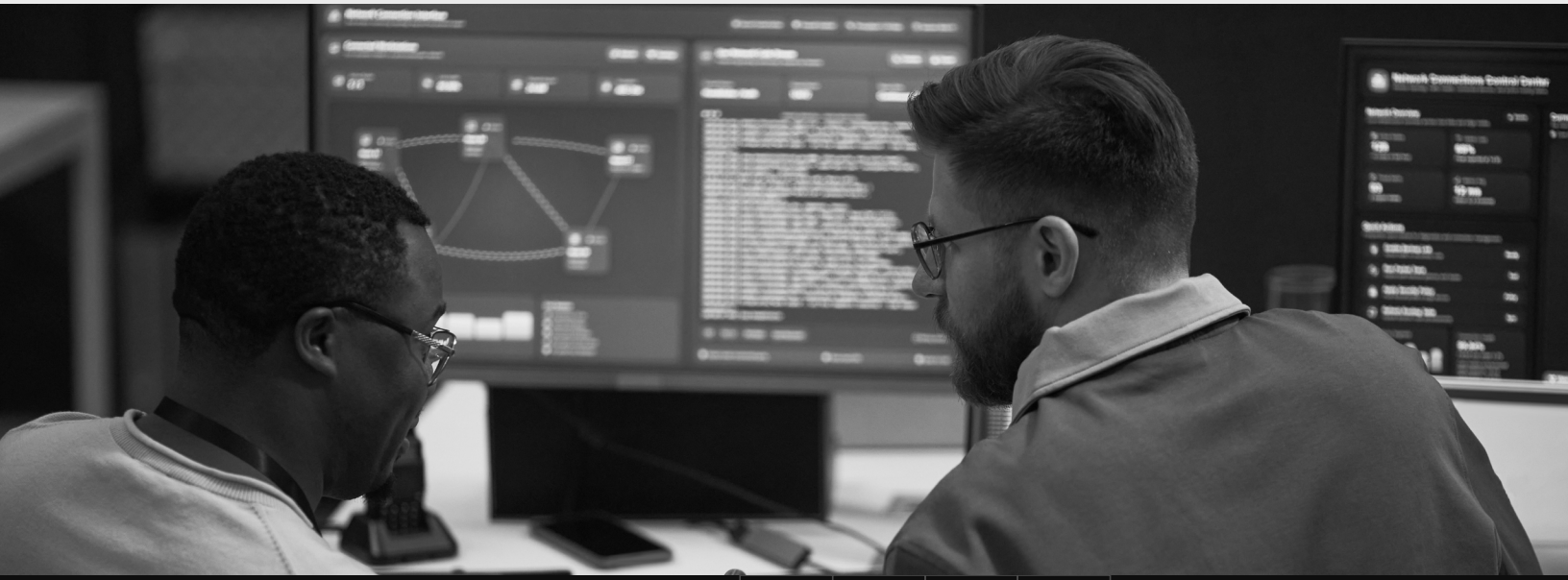
Managed Threat Hunting provides proactive, hypothesis-driven threat hunting across your environment using your existing security platforms. Binary Defense develops and executes structured, hypothesis-based hunts that proactively search for attacker behaviors and tactics, techniques, and procedures (TTPs), surfacing stealthy activity that signature- and indicatorbased detection misses.

Hunts are informed by threat intelligence feeds, security blogs and trust groups, sandbox and malware analysis, and internal lab research. Findings are analyzed by experienced threat hunters, with escalations delivered alongside context and recommended next steps to support response.

Managed Threat Hunting delivers scalable, repeatable hunting coverage that surfaces confirmed, actionable findings consistently across environments.

## Beyond IOC queries.

Indicator-based searches only match what someone has already seen and fingerprinted. Hypothesis-based hunting targets attacker behaviors and TTPs, surfacing novel and evolving threats before they have a known signature.



# Five ways coverage compounds.

### Threat-Informed Hunting

- Hunts developed using current threat intelligence and emerging attacker techniques
- Uncover stealthy behavior that evades traditional monitoring
- Continuously reprioritized by relevance and risk.

### Pattern & Anomaly Detection

- Identify unusual behaviors, linked events, and activity patterns across your environment
- Surface anomalies and visibility gaps that may indicate real risk.

### Trained Threat Hunters

- Expert analysts with advanced malware analysis and security investigation experience
- Apply threat intelligence, intuition, and real-world experience to uncover hidden threats
- Provide clear, actionable guidance to support investigation and response
- 100% US-based team delivering consistent, high-quality analysis.

### Expert Analysis & Escalation

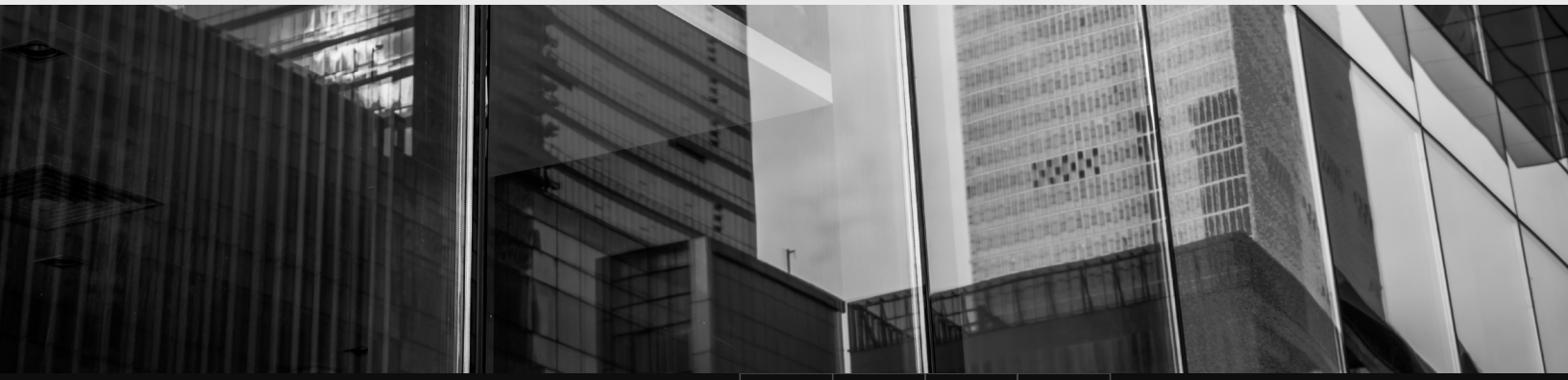
- Findings reviewed and validated by experienced threat hunters
- Confirmed or high-risk activity escalated with context and recommendations to guide response.

### Scalable Coverage Across Your Environment

Threat hunts executed across your in-scope platforms using repeatable methodologies
Broad, consistent coverage that requires no ongoing involvement from your team.

# A six-step hunt lifecycle.

Managed Threat Hunting follows a structured, six-step process developed and executed entirely by Binary Defense threat hunters.



| | |
|---|---|
| 1 | **Threat Hunting Hypothesis**<br>Hunters synthesize intelligence from threat intel feeds, security blogs and trust groups, sandboxes and malware samples, and internal lab research into a structured, testable hypothesis. |
| 2 | **Threat Research & Modeling**<br>Hunters perform deep research on the identified threat, including lab-based attack replication in Binary Defense's Red Lab to validate observed behavior and understand attacker TTPs firsthand. |
| 3 | **Hunt Development**<br>Structured, hypothesis-driven hunt logic is built in target query languages (KQL, SPL, Sigma/YARA) and version-controlled in Binary Defense's Master Detection Engineering repository. |
| 4 | **Scalable Hunt Execution**<br>Hunts run in your environment against your relevant security tools and specific context, including historical tuning, known benign patterns, prior hunt results, and historical findings. Execution is automated, repeatable, and guided by threat prioritization. |
| 5 | **Client-Specific Analysis & Escalation**<br>Results are validated by experienced threat hunters against that environment-specific context to separate real risk from benign activity. Confirmed, actionable findings are escalated to the NightBeacon CMD, and all findings are documented in tickets for cross-team visibility. |
| 6 | **Ongoing Re-Execution & Feedback Loop**<br>Relevant hunts are re-run as threats persist or evolve. Insights are shared with detection engineering, Analysis on Demand, and SOC analysts, and outcomes directly reprioritize the hypothesis queue, creating a closed loop that continuously improves coverage. |

| | |
|---|---|
| ↻ | It's a loop, not a line. Outcomes from Step 06 feed back into Step 01. Validated findings and insights reprioritize the hypothesis queue, so coverage compounds and grows sharper for your environment over time. |

# Hunts run on the tools you already have.

Managed Threat Hunting is delivered through supported SIEM and EDR APIs, enabling visibility across your environment using the tools you already have in place. Primary platforms are EDR-based and provide the deepest hunting coverage. Secondary platforms enrich hunts; a supported EDR is required for threat hunting.

| | Primary: EDR-based |
|---|---|
| x | SentinelOne |
| x | Microsoft Defender for Endpoint |
| x | Palo Alto Networks Cortex XDR |

| | Secondary: SIEM & Data Sources |
|---|---|
| x | CrowdStrike NG SIEM |
| x | Google SecOps |
| x | Palo Alto Networks Cortex XSIAM |
| x | Microsoft Sentinel |
| x | Splunk |
| x | Sumo Logic |
| ~ | CrowdStrike Falcon EDR* |

* CrowdStrike Falcon EDR is supported only when EDR events are available in the CrowdStrike NG SIEM.

# Hunts run on the tools you already have.

Managed Threat Hunting shifts your posture from waiting on signals to actively searching them out, and the gains compound the longer it runs.

| | |
|---|---|
| Reacting to alerts after they fire | → Proactively uncovering threats across your environment before they escalate |
| Blind spots and unknown dwell time | → Reduced time to detection and broader visibility into stealthy activity |
| A backlog of unverified signals | → Confirmed, actionable findings escalated with context and recommended next steps |
| Hunting that competes for your team's time | → Scalable coverage with no added headcount and no ongoing involvement |
| One-time engagements that go stale | → Coverage that compounds as the closed-loop process makes every hunt sharper over time |

## The Bottom Line

Managed Threat Hunting ensures your organization is not just reacting to alerts, but actively uncovering threats across your environment. By combining structured methodologies, expert analysis, and scalable delivery, you gain the visibility and insight needed to reduce risk and improve security outcomes over time.

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, including earlier threat detection, faster response, and stronger long-term security posture

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


BINARY DEFENSE