

ThreatHunt™

Hypothesis-driven, human-led threat hunting across your clients' endpoint, network, identity, cloud, and SaaS telemetry — mapped to MITRE ATT&CK and delivered as a white-labeled report you take straight into your QBRs.

WHY IT EXISTS

Alert-only monitoring waits for a detection to trip. ThreatHunt goes looking before it does. Our Tier-3 analysts form a hypothesis about how an adversary would operate undetected inside an environment, then pursue it by hand through raw telemetry — surfacing the quiet footholds that never generate an alert: native-tool execution, dormant persistence, and identity abuse.

Beyond the endpoint. Falcon Adversary OverWatch hunts the endpoint. ThreatHunt carries the same standard of proactive investigation across identity, network, cloud control planes, and SaaS — wherever your client's data sources reach.

Hypothesis-driven

A documented hypothesis, validated or refined against real telemetry.

TTP-based

Mapped to MITRE ATT&CK techniques — the behavior, not one known-bad indicator.

IOC-based

Targeted sweeps for indicators tied to new campaigns and advisories.

Anomaly-based

Deviations from normal endpoint, network, and identity behavior.

THE WHITE-LABEL HUNT REPORT

- **Executive summary** written for a non-technical business owner
- **Findings** with severity, exact process chain, host, and user
- **MITRE ATT&CK mapping** for every finding
- **Remediation steps** your helpdesk can action directly
- **Your brand, not ours** — present it as your own
- **No raw log dumps** — signal only, and negative results documented as valid findings

LOOKBACK

- Scheduled hunts: rolling **30–90 day** window
- CVE/campaign hunts: back to the **earliest confirmed exploitation date**

THREE WAYS TO RUN IT

TIER	CADENCE	WHAT'S INCLUDED
Essentials	Quarterly · 4 hunts/yr	One hypothesis/TTP-driven hunt per quarter, 30-day lookback, standard report
Standard	Monthly · 12 hunts/yr	Scheduled hunts rotating through the TTP library, 30–90 day lookback
Premium	Monthly + ad hoc	Everything in Standard, plus CVE/campaign-driven hunts kicked off within 24–48 hours of a major public disclosure

When nothing happens, *this is your proof.*

The hardest question in a QBR is the quiet one: what am I paying you for? A white-labeled hunt report answers it with documented, board-ready evidence that someone is actively hunting on your clients' behalf.

Start with a complimentary first hunt. We'll run one hunt on a client of your choosing, at no cost to you or them, and hand you the report. And our standing commitment: **we never compete with our partners for their clients.**

[Book a 15-minute walkthrough](#)