// tier-3 human-led hunting

ThreatHunt™

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

OVERVIEW

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. This is not automated triage. It is forensic work, and it surfaces the quiet footholds that never generate an alert: native-tool execution, dormant persistence, and identity abuse that standard platforms stay silent on.

HOW IT WORKS

Monthly hypothesis-driven sprints

Each cycle targets a specific advanced evasion tactic across your enrolled clients. Analysts pursue the hypothesis, validate every lead, and discard the noise. Findings are categorized by MITRE technique, never by transient campaign name, so a report holds its meaning long after a threat's nickname has changed.

TELEMETRY IN SCOPE

Endpoint
Process, script, and execution telemetry

Network
Egress, beaconing, and lateral movement

Identity
Sign-in, privilege, and token abuse

REPRESENTATIVE MITRE ATT&CK COVERAGE

TACTIC	HUNTED BEHAVIOR	TECHNIQUE
Initial Access	Social-engineering-driven execution via lure pages	T1204
Execution	Paste-and-run and fake-update command execution	T1059
Persistence	Registry, scheduled task, and startup persistence	T1547 / T1053
Defense Evasion	Living-off-the-land use of native Windows tooling	T1218
Credential Access	Credential theft and token manipulation	T1003 / T1556
Command & Control	Anomalous outbound channels and beaconing	T1071

When nothing happens, this is your proof.

The hardest question in the channel 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.

WHAT YOU RECEIVE

The white-label hunt report

01 Executive summary written for a non-technical business owner

02 Findings with severity, exact process chain, host, and user

03 MITRE ATT&CK mapping for every finding

04 Clear remediation steps your helpdesk can action directly

05 Your brand, not ours: put your logo on it and present it as your own

06 No raw log dumps. Signal only, with context and next steps

ENGAGEMENT MODEL

Simple to enroll, yours to deliver

01 Channel-exclusive. Delivered through you, never around you

02 Complimentary first hunt on a client of your choosing

03 Ongoing premium service once you have seen the depth

04 Same SOC that protects your paying clients, every hunt

WHY VIJILAN

SOC
A global 24/7 SOC staffed by senior, human Tier-3 analysts

CS
CrowdStrike Powered Service Provider and Services Partner

ISO
ISO 27001 certified

SOC2
SOC 2 Type 2 certified

BUILT FOR

Partners serving clients in regulated industries, healthcare, finance, and DoD or CMMC environments, and any MSP ready to move a client's security posture from reactive to proactive. ThreatHunt is the deliverable that makes the difference visible.

Proactive is a position, not a promise.

Any provider can say they hunt. ThreatHunt lets you prove it, in writing, with your name on the cover, at every QBR.

// START HERE

Start with a complimentary hunt

We will run one hunt on a client of your choosing, at no cost to you or them, and hand you the report.

Book a 15-minute walkthrough

// or reply "I want to learn more"

SOC 2 TYPE 2 · ISO 27001 · CROWDSTRIKE POWERED SERVICE PROVIDER · CHANNEL-EXCLUSIVE