

THREAT HUNTING & APT DETECTION

Avalon's hunters build agency-specific hypotheses from current threat intelligence, then test them against your own telemetry to find adversaries automated tools were never going to catch.

THE PROBLEM WE ADDRESS

Nation-state actors have proven they can sit inside federal networks for months or years without tripping a single alert, because nothing they do looks abnormal to signature-based tools.

Most federal SOC's are alert-centric, built around tool alerts and ticket queues, with nobody funded to go looking for what the tools missed.

WHAT WE DO

- Agency-specific threat model built from current intelligence and sector targeting
- Hypotheses translated into testable statements mapped to MITRE ATT&CK
- Inventory of EDR coverage, log sources, retention, and cloud audit configuration
- Endpoint hunting for persistence mechanisms and living-off-the-land tradecraft
- Active Directory and cloud-identity attack-path analysis
- M365/Entra, AWS GovCloud, and Azure Government control-plane hunting
- Executive and technical findings reports with ATT&CK-mapped evidence
- Detection content pack (Sigma rules, SIEM queries, watchlists) transferred to the SOC

HOW WE DO IT

1 PRE-ENGAGEMENT & KICKOFF

ROE signed, account provisioning, and scope confirmed against telemetry reality.

DELIVERABLE

Confirmed scope + access

2 HYPOTHESIS DEVELOPMENT

Threat profile built, hunt plan signed off, and collectors deployed where approved.

DELIVERABLE

Signed hunt plan

3 ACTIVE HUNT SPRINTS

Iterative hunting across endpoint, identity, network, and cloud lanes, with a weekly rolling findings brief.

DELIVERABLE

Validated findings, weekly

4 REPORTING & HANDOFF

Evidence validation, detection-content packaging, and a SOC handoff session.

HANDOVER

Detection content pack + handoff

VALUE DELIVERED

- › **An answer, not a guess.** Every hunt returns validated findings or a documented, defensible negative for the scope examined.
- › **Your monitoring gets better either way.** Hunt logic that produced value converts into Sigma rules and SIEM content the SOC keeps.
- › **No appliance, no data leaves your boundary.** Hunts run on your existing telemetry stack, supplemented by agency-approved tooling only.
- › **Independence that graded homework can't provide.** A hunt performed by the firm that built your defenses is grading its own work — Avalon isn't.

THE ONE THING TO REMEMBER

No appliance to buy. No data leaves your boundary.

COMMONLY PROCURED AS

Threat hunting / compromise assessment services

AT A GLANCE

Model	Fixed-price, scoped per engagement
Typical	4–8 wks for a single-enclave hunt; 8–12+ wks at enterprise scope
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	MITRE ATT&CK, NIST SP 800-53 RA-10, NIST SP 800-172 (3.11.2e), GSA HACS Cyber Hunt

WHO WE WORK WITH

- › CISO / SOC lead needing an answer to "are we compromised right now?"
- › ISSO evidencing RA-10/CA-7 continuous-monitoring controls
- › Agency that can no longer rely on CISA's reduced proactive hunt capacity

COMMITMENT TO QUALITY

Avalon is led directly by a PMP-certified founder with a decade of enterprise engineering experience where every engagement gets senior-level attention, never a subcontracted bench. Delivery follows NIST SP 800-53, RMF, and FISMA, evidence-backed and control-mapped by design. ISO 9001/27001 is on the roadmap as the pipeline scales.

Status: Small business federal contractor based in Los Angeles, CA

MITRE ATT&CK

NIST SP 800-53 RA-10

NIST SP 800-172 (3.11.2E)

GSA HACS CYBER HUNT