

ENDPOINT DETECTION & RESPONSE

Avalon deploys, configures, tunes, and validates your EDR platform, then proves the result with controlled attack-simulation testing — so the EDR you already own delivers real protection, not just a checkbox.

THE PROBLEM WE ADDRESS

Endpoints remain the most common initial-access point into federal networks, and an untuned or partial EDR deployment means the agency learns about an intrusion from CISA, an IG, or the adversary — not its own console.

Default vendor policies in a federal environment generate alert volumes that overwhelm understaffed SOC's — alert fatigue is how real detections get missed inside tools that technically "saw" the attack.

WHAT WE DO

- Authoritative inventory reconciliation against the EDR console
- Agent-health audit: stale check-ins, broken sensors, audit-only mode
- Policy configuration review against vendor baselines and CIS Benchmarks
- Controlled detection-efficacy test using safe adversary emulation
- Pilot-ring deployment with performance baselining
- Staged audit-to-blocking progression with soak periods and rollback criteria
- SIEM ingestion, dashboards, and analytic rules for EDR telemetry
- SOC runbook set covering triage through containment

HOW WE DO IT

1 KICKOFF & BASELINE

Console access provisioned, inventory reconciled, and a controlled efficacy baseline test run.

DELIVERABLE

Coverage + efficacy baseline

3 DEPLOYMENT & TUNING

Waves rolled out on the change-board calendar; progression from audit to blocking mode with SIEM integration.

DELIVERABLE

Fleet deployed + tuned

2 DESIGN & PILOT

Remediation and wave plan designed; a pilot ring deployed and performance-validated.

DELIVERABLE

Validated pilot ring

4 TRANSFER & CLOSEOUT

Runbooks handed off, a tabletop exercise run, and a closing ATT&CK retest confirms the improvement.

HANDOVER

Runbooks + retest results

VALUE DELIVERED

- › **A coverage number, not a guess.** Inventory reconciliation and agent-health audits turn an unknown fleet into a defensible coverage percentage.
- › **Proof, not a vendor's word.** Controlled ATT&CK-mapped emulation shows what the platform would actually catch, before and after tuning.
- › **Alert fatigue engineered out.** A staged audit-to-blocking progression and custom detections cut false-positive volume per analyst, measured.
- › **Runbooks built for a real incident.** The same team writes containment procedures and delivers incident response, so they hold up if one follows.

THE ONE THING TO REMEMBER

Four measured numbers, not adjectives.

COMMONLY PROCURED AS

EDR deployment, tuning & validation services

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	12–20 wks for a mid-size deployment; 3–6 wks for a standalone assessment
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-53, OMB M-22-01, MITRE ATT&CK, CIS Benchmarks

WHO WE WORK WITH

- CISO / SOC lead needing a defensible EDR coverage number
- ISSO evidencing SI-4/IR-4 controls for an authorization package
- IT operations lead migrating or hardening an existing EDR platform

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

NIST SP 800-53

OMB M-22-01

MITRE ATT&CK

CIS BENCHMARKS