

SECURITY INCIDENT RESPONSE & FORENSIC ANALYSIS

When a federal system is compromised, Avalon finds the intruder, scopes what was touched, removes the adversary, and documents it to a standard counsel, leadership, the IG, and CISA will accept.

THE PROBLEM WE ADDRESS

A mishandled incident takes mission systems offline and leaves data integrity in question while the agency guesses at the blast radius — most program offices have no full-time forensic examiners.

Evidence handled without chain of custody can be rendered unusable for prosecution, counterintelligence referral, or personnel action — spoliation exposes the agency and its leadership.

WHAT WE DO

- IR plan development or overhaul, aligned to NIST SP 800-61 Rev. 3
- Scenario-specific playbooks: ransomware, BEC, credential theft, exfiltration
- Facilitated tabletop exercises with documented after-action reports
- Triage and incident confirmation with an evidence-preservation order
- Write-blocked disk imaging, live memory capture, cloud audit-log preservation
- Timeline reconstruction, lateral-movement mapping, persistence identification
- Isolation strategy balancing evidence preservation against mission continuity
- Daily situation reports and a final report with indicator package

HOW WE DO IT

1 ACTIVATION & TRIAGE

Evidence-preservation order issued, initial telemetry review, and isolation recommendations (hours 0–72).

DELIVERABLE

Preservation order + isolation plan

3 ANALYSIS & CONTAINMENT

Timeline reconstruction, data-impact assessment, and containment sequencing with agency ops staff.

DELIVERABLE

Timeline + impact assessment

2 SCOPING & ACQUISITION

Targeted collection, forensic imaging, and log preservation before retention windows lapse.

DELIVERABLE

Preserved forensic evidence

4 ERADICATION & REPORTING

Coordinated eviction, clean-state validation, final report, and reporting-obligation support.

HANDOVER

Final report + indicator package

VALUE DELIVERED

- › **A qualified team fast.** Retainer clients activate within hours; the examiner in the pitch is the examiner on the incident.
- › **Independent when it matters.** A firm that runs your SOC has a conflict investigating what the SOC missed — Avalon is structurally independent.
- › **Chain-of-custody rigor by default.** Every acquisition is hashed and logged whether or not litigation is anticipated.
- › **Cloud-identity depth built in.** M365/Entra ID and cloud-tenant investigation is native, not an add-on to a legacy-endpoint practice.

THE ONE THING TO REMEMBER

Independent, compliance-fluent forensics.

COMMONLY PROCURED AS

Incident response & digital forensics services

AT A GLANCE

Model	Retainer or emergency activation, fixed or T&M
Typical	30–60 days end to end; retainer activation within hours
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-61 Rev. 3, NIST SP 800-86, CISA Federal IR/Vuln Playbooks, DFARS 252.204-7012

WHO WE WORK WITH

- › CISO / agency leadership responding to a confirmed or suspected compromise
- › ISSM standing up a retainer ahead of an incident
- › Program office needing IR readiness plans and tabletop exercises

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 800-61 REV. 3

NIST SP 800-86

CISA IR/VULN PLAYBOOKS

DFARS 252.204-7012