

VULNERABILITY ASSESSMENT & EXPLOITATION

Avalon finds the weaknesses in your systems, networks, and applications, then safely proves which ones a real attacker could use — so remediation dollars go where the risk is.

THE PROBLEM WE ADDRESS

Vulnerability scanners flag thousands of findings by a generic severity score blind to your network, your compensating controls, or what an attacker could actually reach.

FISMA requires an annual independent assessment, RMF requires the Assess step before an ATO, and FedRAMP requires an annual test for Moderate/High systems — a gap here blocks the authorization, not just the network.

WHAT WE DO

- Scoping and a signed Rules of Engagement before testing begins
- Authenticated and unauthenticated scanning across network, host, and app layers
- Configuration review against recognized security benchmarks
- Manual validation of every finding — eliminating scanner false positives
- Controlled exploitation under signed authorization, no data destruction
- Post-exploitation and business-impact mapping
- Findings report with severity, evidence, and remediation roadmap
- Executive readout and optional retest / verification pass

HOW WE DO IT

1 KICKOFF & SCOPING

ROE and authorization-to-test letter signed; testing windows and credentials confirmed.

DELIVERABLE
Signed ROE

3 VALIDATION & EXPLOITATION

False positives eliminated; exploitable findings confirmed and safely demonstrated.

DELIVERABLE
Validated findings

2 RECON & IDENTIFICATION

Attack-surface mapping, scanning, and configuration review build the candidate findings list.

DELIVERABLE
Candidate findings list

4 REPORTING & RETEST

Findings mapped to mission impact, prioritized report delivered, stakeholders briefed; optional retest verifies fixes.

HANDOVER
Prioritized report + retest option

VALUE DELIVERED

- Real risk, not scanner noise.** Only findings manually validated as genuinely exploitable make the report — effort stops chasing false positives.
- Mission-impact prioritization.** Post-exploitation analysis translates findings into what actually matters, not just a CVSS score.
- Assessment-ready evidence.** Methodology aligns to NIST SP 800-115, PTES, and FedRAMP Pen Test Guidance, feeding your authorization package.
- Senior hands the whole way.** The person who scopes the engagement is the person who runs it.

THE ONE THING TO REMEMBER

The senior tester who scopes the work is the one who does it.

COMMONLY PROCURED AS

Vulnerability assessment / penetration testing services

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	4–8 wks per engagement
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-115, PTES, MITRE ATT&CK, FedRAMP Pen Test Guidance

WHO WE WORK WITH

- Capture manager scoping a security-testing subcontract line
- ISSO / system owner preparing for an RMF Assess or annual FISMA cycle
- CISO / IT security lead prioritizing a remediation budget

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 800-115 PTES MITRE ATT&CK

FEDRAMP PEN TEST GUIDANCE