AttackVector

METHODOLOGY OVERVIEW

How AttackVector tests

The phases, standards, severity model, evidence rules, and report structure behind every AttackVector engagement, so you know what to expect before testing begins.

AttackVector Inc. · Tampa Bay, Florida · attackvector.com
Version 1.0 · September 2026

Every AttackVector engagement follows the same methodology, whether the target is an external perimeter, an internal network, a web application, a cloud tenant, or the people who work at your company. The details change with the scope. The structure does not. This overview describes that structure.

1. Engagement phases

Phase 1 Scoping	Before any testing starts, we agree in writing on what is in scope, what is out of scope, the testing window, emergency contacts on both sides, and the objectives that matter to your business. Written authorization from someone entitled to give it is a hard requirement.
Phase 2 Reconnaissance	We map the attack surface from the outside using open sources and active enumeration. For external work this means domains, subdomains, IP ranges, exposed services, certificates, leaked credentials, and cloud assets tied to your organization. For internal work it means hosts, shares, identity relationships, and trust boundaries.
Phase 3 Exploitation	Confirmed weaknesses are exploited by hand. Automated scanners are used for coverage, never as the finding itself. Where individual weaknesses chain together, we chain them, because the chain is usually the real story.
Phase 4 Proof and impact	For every exploited issue we go far enough to demonstrate the consequence, and no further. Destructive actions, denial of service, and anything that changes production data are off the table unless explicitly agreed in scoping.
Phase 5 Reporting	Findings are written up with evidence, severity, affected assets, and remediation while testing is still fresh. Draft reports are reviewed by a second tester before delivery. We walk through the report live with your team.
Phase 6 Retest	After you remediate, we test the fixed items again and update the report and attestation letter to reflect the closed state. Retest is part of the engagement, not an upsell.

2. Standards we reference

Our methodology is our own, but it is built on and mapped to public standards so that auditors and customers can see what was covered:

- PTES (Penetration Testing Execution Standard) for the overall engagement lifecycle.
- OWASP Web Security Testing Guide for web application and API coverage, with the checklist delivered alongside the report.
- OWASP Top 10 for LLM Applications for AI and language model features, agents, and retrieval pipelines.
- MITRE ATT&CK for describing adversary techniques in red team and internal reports, so that your detection team can map findings to their coverage.

- NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) for planning, execution, and post-testing activities.

Referencing a standard does not make the engagement a checklist. The standard tells us what to look at; the tester decides how hard to push.

3. Severity model

Each finding receives a CVSS v4.0 base score, then a severity rating that takes your business context into account. The two can differ. When we adjust, the report says so and explains why.

Severity	Definition	Recommended fix window
Critical	Exploitable now, from the position agreed in scope, with direct access to sensitive data, administrative control, or the ability to move into the internal network.	Begin immediately; aim to remediate or mitigate within days.
High	Exploitable with modest effort or a common precondition, leading to significant data exposure, privilege escalation, or account takeover.	Within two to four weeks.
Medium	Exploitable only with unusual conditions, or exploitable but with limited impact. Often a link in a chain rather than the end of one.	Within the next scheduled release or quarter.
Low	Weaknesses that reduce defense in depth, leak minor information, or deviate from good practice without a demonstrated path to impact.	As part of routine maintenance.

Informational observations, such as version disclosures with no known exploit, are listed separately so they do not inflate the findings count.

4. Evidence standards

A finding without evidence is an opinion. Every finding in an AttackVector report includes:

- The exact request, command, or action used, redacted where it would expose a credential.
- The response or observation that proves the outcome.
- The affected assets by hostname, URL, or identifier, so the owner can find them.
- Reproduction steps that your own engineer can follow to confirm the issue and later confirm the fix.

Where a finding relies on credentials or data belonging to your users, we use test accounts created for the engagement, and we say so.

5. Report structure

Reports follow a fixed structure so that readers know where to look:

1. Executive summary. Written for leadership and auditors. What we tested, what we found, what it means for the business, and what to do first.
2. Technical findings. One entry per finding: severity, score, affected assets, description, impact, evidence, remediation, and references. Ordered by severity.
3. Remediation roadmap. Findings grouped by priority and by the team that owns the fix.
4. Appendices. Scope and rules of engagement as agreed, methodology and coverage checklist, severity definitions, and the asset inventory discovered during reconnaissance.

> An attestation letter suitable for customers, auditors, and insurers is delivered alongside the report and updated after retest.

6. Retest policy

One retest of remediated findings is included in every engagement. You tell us when fixes are ready; we test the affected items using the same method and evidence standard as the original test. Fixed items are marked closed with the date and evidence of the retest; anything else stays open with a note on what was observed. Retest is intended for the items in the original report; new scope is a new engagement.

7. Rules of engagement

We test only what is authorized, from where we are authorized to test, during the agreed window. Specifically:

- Written authorization is obtained before any active testing.
- Denial of service and destructive techniques are excluded by default.
- Production data is not exfiltrated beyond the minimum needed to prove access.
- Sensitive steps are coordinated in real time with your named contact.
- Any credentials, sessions, or artifacts obtained during testing are handled as confidential and destroyed after the engagement closes.
- If we find evidence of a real intrusion by someone else, we stop and tell you immediately.

> See it in practice. An illustrative penetration test report for a fictional client, written in exactly this structure, is available at attackvector.com/sample-report. To talk through an engagement, visit attackvector.com/contact or call +1 813-344-2355.