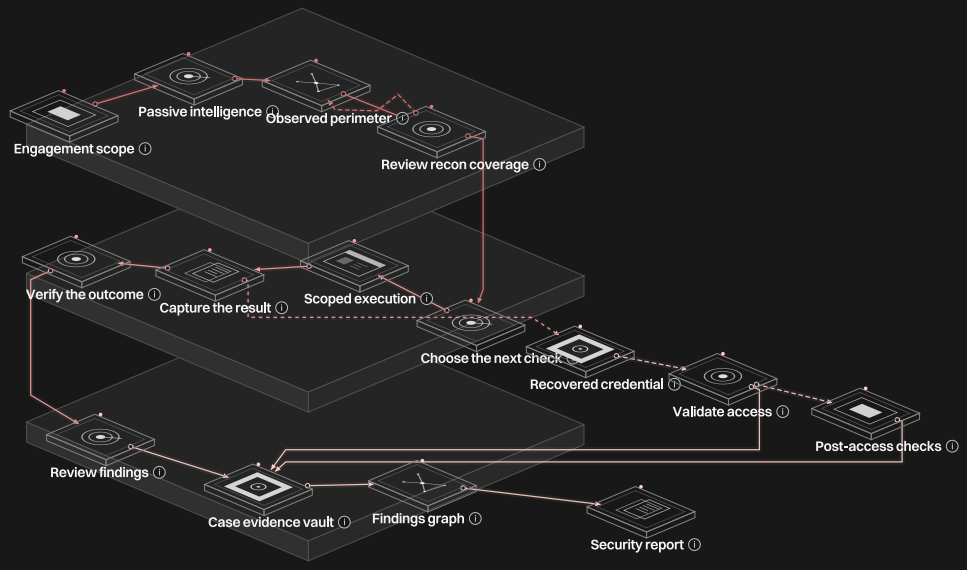
Durandir Cybersecurity



Published	Nov 10, 2026
Category	Products

We test the security of websites, APIs and networks, and we build the software our own testers use to do it.

Durandir Cybersecurity is two things. It is a service: our team runs security assessments for organisations that want to know how an attacker would get in and what to fix first. And it is software: one of the tools we publish, for security teams that run their own tests.

Both work the same way. Every finding is verified before it is reported, every step can be reproduced, and nothing is tested without written authorisation.

Security assessments

We carry out three kinds of engagement.

- Penetration tests of web applications, APIs and networks, against a defined scope.
- Red team exercises, where the goal is an objective you set, such as reaching a specific system or dataset, and the test measures how far a realistic attacker gets and whether your defences notice.
- Security audits and configuration reviews of a system or service against a recognised standard.

We work to OWASP WSTG, NIST SP 800-115 and PTES, and we map what we find to MITRE ATT&CK, CWE and CVSS so that your team can read the results in the terms it already uses.

Scope comes first

An engagement starts with a signed document that says which systems are in scope, on which dates, by which methods and who authorised it. Testing does not begin until that exists.

The scope is enforced during the test, not only agreed before it. The tooling checks each target against the authorised list and refuses to act on anything outside it.

If we find something that puts you at immediate risk, we tell you when we find it and do not wait for the report.

What you receive

A report written to be acted on. Each finding states what the weakness is, how it was confirmed, the exact steps to reproduce it, how severe it is and how to fix it. Unverified scanner output is left out.

An executive summary explains the overall position in plain language for the people who decide on budget and priorities.

A retest after you have applied the fixes can be included in the scope, to confirm which findings are closed.

The software

Security teams and bug bounty researchers can run the same workflow themselves with Durandir Cybersecurity. It keeps the scope, the requests sent, the responses received and the evidence for each finding in one case, and it produces the report from them.

It runs on your own hardware. Engagement data, including anything sensitive found during a test, stays with you.

The software is for authorised testing only: systems you own or have written permission to assess.