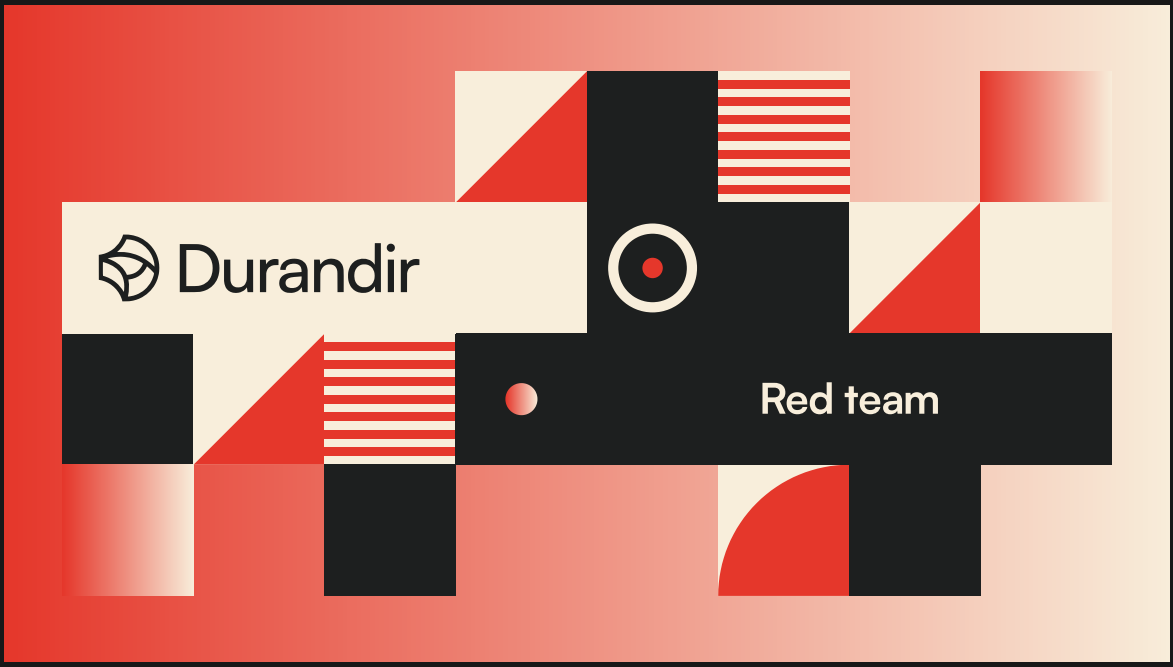
Red team



Published	Nov 10, 2026
Last updated	Nov 16, 2026
Category	Services

We test your websites, APIs and networks the way an attacker would, and tell you what to fix first.

A red team engagement answers a plain question: if someone set out to break into your systems today, how far would they get? We answer it by trying, under your authorisation, against the systems you choose.

The work is done by the Durandir team with tools we build ourselves: Durandir Cybersecurity to run and verify the tests, and Durandir Harness to keep the case and its evidence. It is the same software we publish for security teams. You do not need to install or operate anything.

Depending on what you need, the engagement can be a penetration test of a defined set of systems, a full red team exercise aimed at an objective you set, or a review of a system against a recognised standard.

Black, grey or white box

How much we know before we start changes what the test tells you, so it is the first thing we decide together.

- Black box: we start with nothing but the name of the target, as an outside attacker would. It shows what a stranger can find and reach.
- Grey box: we start with what a customer, an employee or a partner would have, such as a user account or basic documentation. It shows what someone with a foot inside can do.
- White box: we work with full information, including architecture, configuration and source code where you want it reviewed. It is the most thorough and finds weaknesses the other two cannot reach in the same time.

Many organisations combine them: a black box phase to see the outside view, followed by a grey or white box phase to go deeper. We will recommend what fits your situation and your budget, and explain why.

How an engagement runs

It starts with scope. Together we write down which systems will be tested, on which dates, with which methods, and who in your organisation authorises it. Nothing is tested before that document is signed.

The scope is loaded into the tooling, which checks every target against it while the test runs, so nothing outside the agreement is touched.

Then we map what is exposed and look for weaknesses. Durandir Agent takes on the repetitive part of that mapping under a tester's supervision, and a person verifies each result. A weakness counts as a finding only when we have confirmed it and can show the steps that reproduce it.

We work to OWASP WSTG, NIST SP 800-115 and PTES, and classify findings with MITRE ATT&CK, CWE and CVSS.

If something puts you at immediate risk, you hear about it the day we find it.

What you receive

A report your team can act on. For each finding: what it is, how we confirmed it, how to reproduce it, how severe it is and how to fix it. It is built from the evidence recorded during the test, so every finding leads back to the request and the response that prove it.

A summary in plain language for the people who decide on priorities and budget.

A retest after you have applied the fixes can be included in the scope.

We stay with you

The result is not a document that arrives by email and ends there. You have one person at Durandir to talk to from the first call to the last fix, and you know at each stage what we are doing and what comes next.

Before the test we help you prepare: who needs to know, what to back up, which hours are safest. During it you get regular updates, and you can reach us at any moment if something looks wrong on your side.

When the report is ready we go through it with you and with your technical team, finding by finding, until it is clear what each one means and how to fix it. We remain available for questions while you work on the fixes.

Confidentiality

What we find in your systems is yours. Engagement data is handled on our own equipment, shared only with the people you name, and deleted or returned at the end of the engagement as agreed in the scope.