GRC+ SERVICE SHEET · NOVEMBER 2026

Red Teaming

A penetration test asks what can be broken. A red team asks whether you would notice. We play a realistic attacker with an agreed goal, and only a few of your people know it is happening.

SERVICE
Advisory service

USUALLY TAKES
Weeks, typically, from scoping to the final report

What It Is

Red team tests that simulate real threat actors against your people, processes and technology, to show whether attacks are detected and stopped.

WHY IT MATTERS
Tools are not the same as detection
Security tools can be in place without anyone noticing a real attack, or knowing what to do.
- Alerts nobody follows up
- Gaps between teams
- Plans never tried under pressure

THE OUTCOME
Proof of what works
You see where the attack was caught and where it was not, and your defenders learn from it.
- A timeline of the attack and your response
- A joint replay
- A plan for detection and response

What We Test

Intelligence	Who would target you and how, and what is publicly known about your organisation.
Initial access	Phishing, exposed systems or physical access, as you agree in advance.
Moving towards the goal	From the first foothold to the systems or data named in the scenario.
Detection and response	What your team saw and did, and when.
Threat Detection	Attacker techniques run openly with your security team, to see which are logged, detected or blocked, and how to close the gaps in your monitoring.

What You Receive

The red team report PDF	Each finding with its evidence, risk, the steps to reproduce it and a fix.
A management summary In the report	What was tested, the main risks and the decisions needed, without the technical detail.
A walkthrough Video call	A session with your team to go through the findings and answer questions.
A retest on request Updated report	We check your fixes and update the report, so you can show the result to auditors and customers.

From Scope to Verified Fixes

1	**Scoping** Targets, people, test windows and exclusions, with written authorisation and rules of engagement.
2	**Intelligence** Threat scenarios and public information about your organisation.
3	**Attack simulation** A realistic attack towards the agreed goal, with a small group informed.
4	**Report** Findings with evidence, risk and a fix, a management summary and a walkthrough with your team.
5	**Retest** We check your fixes and update the report.

A guide, not a fixed promise: the length of each phase depends on your scope.

Regulations That Ask for It

DORA TLPT RTS	**DORA Threat-Led Penetration Testing (TLPT)** Threat intelligence and red team testing for the threat-led penetration test DORA requires of identified financial entities at least every three years.
MITRE ATT&CK	Red team tests that simulate real threat actors against your people, processes and technology, to show whether attacks are detected and stopped.
AIUC-1	
TIBER-NL	Red team tests that show whether a real attack would be detected and stopped.
TIBER-BE	
TIBER-ES	
TIBER-IT	
TIBER-DK	
TIBER-SE	
TIBER-FI	
TIBER-CZ	
TIBER-SK	

Why Organisations Choose GRC+

Independent of your suppliers	We test what you have. We take no margin on a product we assess or recommend.
Findings tied to your requirements	Our team also works on NIS2, DORA, ISO 27001, PCI DSS and Swift CSP, so results can serve your audits too.
Risk rated for your business	We rate each finding by what it could cost you, not only by a scanner's score.
Written rules of engagement first	Scope, limits and contacts are agreed in writing before any test starts.

Questions Buyers Ask

What is the difference between red teaming and penetration testing?

A penetration test looks for as many vulnerabilities as possible in a defined scope. A red team test pursues specific objectives, such as reaching a critical system, the way a real attacker would, and tests whether your organisation detects and responds.

Is a red team test safe for our production systems?

Tests run under agreed rules of engagement, with a control team on your side that can pause or stop the test at any time. Actions that carry risk are agreed in advance.

Can a red team test meet TIBER, DNB ART or DORA TLPT?

We run red team tests that follow TLPT methods, and work alongside the TLPT provider your authority accepts. The same holds for TIBER and DNB ART, which set their own roles, phases and documents.

Are we ready for a red team?

If basic penetration test findings are still open, fix those first, because a red team would simply find them again. An ATT&CK detection assessment can be a good step before it.

Talk to Us

Thirty minutes with a principal consultant on what applies to you and what to do first.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/red-teaming