What is Threat-Led Penetration Testing?

Threat-Led Penetration Testing (TLPT) is intelligence-led red teaming against an organisation's live, critical systems. A threat intelligence team profiles the real adversaries most likely to target you and builds scenarios from them, then an independent red team executes those attacks against production under tight rules, while only a small control group knows it is a test. It is the core of regulatory schemes like the EU's DORA, the ECB's TIBER-EU, and the Bank of England's CBEST. Unlike a standard penetration test, TLPT measures your detection and response, not just whether a vulnerability exists.

HOW IT WORKS

01 How a TLPT engagement works

The model, set out in frameworks like TIBER-EU, runs in phases:

- Threat intelligence: a provider builds a picture of the threat actors most relevant to your sector and business, and turns it into concrete attack scenarios and target objectives, often called flags.
- Red teaming: an independent red team runs those scenarios against your live systems, chaining initial access, escalation, and movement toward the flags, inside agreed rules of engagement.
- Control and oversight: a small control team on your side, and in regulated schemes a supervisor, manages scope, safety, and a kill switch. Only they know the test is live.
- Closure: findings, the detection timeline, and remediation are worked through with the blue team in a replay.

Named frameworks that define or require this include DORA, TIBER-EU, CBEST, and CREST STAR-FS.

02 How TLPT differs from a standard pentest

A standard penetration test and TLPT answer different questions:

- Scope: a pentest targets an agreed system or application; TLPT targets the organisation and its critical live functions.

SOURCES

[1] TIBER-EU framework

[2] Digital Operational Resilience Act (Regulation (EU) 2022/2554)

[3] CBEST intelligence-led testing

- Intelligence-led: scenarios come from the real threat actors relevant to you, not a generic checklist.
- Live and covert: it runs against production and the blue team is not told, so it measures genuine detection and response.
- Oversight and depth: regulated TLPT involves a supervisor and strict control, and runs longer and deeper than a typical pentest.

TLPT complements a pentest rather than replacing it. You still need regular pentests for coverage, and TLPT to test whether your defences hold against a targeted adversary.

03 Who needs TLPT and what you get

TLPT is now a regulatory requirement for many financial entities in the EU under DORA, which makes advanced testing mandatory for significant firms, and it has long been established for the sector under the Bank of England's CBEST and the ECB's TIBER-EU. Beyond regulation, any organisation that wants a realistic measure of its detection and response, not just its vulnerability list, benefits.

What you get is a tested picture of how far a real attacker gets, where detection worked and where it failed, the specific gaps in prevention and response, and a remediation plan validated with your own defenders.

See how a real adversary would fare against your defences.
securelayer7.net/learn/pentest/what-is-threat-led-penetration-testing

Open online