THREAT-LED PENETRATION TESTING (TLPT) IN COMPLIANCE WITH THE DORA

Regulation: Advanced Red-Teaming Tests for Regulated Financial Institutions

The European DORA regulation (Digital Operational Resilience Act) introduces a new standard for ICT risk management. It requires significant financial entities to regularly conduct **Threat-Led Penetration Testing** (TLPT)—intelligence-driven tests based on threats, simulating the capabilities of advanced organized cyber attackers (APT). The goal is not only to find vulnerabilities but also to **verify the organization's ability to detect, respond to, and recover from an attack** that matches a real and coordinated scenario.

What is Threat-Led Penetration Testing and why are standard tests insufficient?

Unlike standard penetration testing, TLPT:

- **Simulates an attack in its full complexity**, including intrusion, lateral movement, privilege escalation, persistence, and data exfiltration,
- Is guided by **current threat intelligence** and specific sector scenarios,
- Includes a **coordination phase** with a defined scope, engagement rules, identification of critical systems, and setting of test objectives.

From a technical perspective, TLPT requires detailed knowledge of attack vectors and the ability to mimic methods of real attackers who exploit zero-day vulnerabilities, social engineering, code obfuscation, or supply chain attacks.

What requirements does DORA set regarding TLPT?

01
Testing must be conducted based on the **current threat profile**, not as a universal scenario.

02
The test must address **critical functions and systems** whose failure could threaten service stability.

03
Organizations must **involve external, independent, and qualified testers.**

04
Results must lead to the **implementation of remedial measures** and possible retesting.

Institutions subject to DORA regulation will have to meet requirements for both the **frequency of testing** and its **documentation and reporting** to the relevant supervisory authority (e.g., ECB). The active **red-team testing phase must last at least 12 weeks**. This duration is necessary to mimic hidden threat actors.

What are the requirements for testing teams?

DORA also emphasizes the **quality and qualification** of entities conducting advanced tests. Testers must meet strict criteria, e.g.:

- They must be **reputable experts** with proven technical and organizational skills and specific knowledge,
- Testers must be **certified** and undergo independent audits or confirmation of proper risk management during testing,
- They must have adequate **liability insurance** in case of caused damages.

If an institution wishes to use its own **internal red team**, it must obtain regulator approval and ensure the organizational independence of the internal team (to prevent conflicts of interest). *Operational threat intelligence* for the scenario must be provided by an **external** provider.

How does testing work in practice?

Reconnaissance – Identification of the target application and connection to the internal network. Gathering information about the target system, such as IP addresses, DNS records, and other metadata.

Footprinting – Analysis of available information about the application and associated systems. Determining available services, versions, and other information.

Sniffing – Eavesdropping and collection of transmitted data to identify vulnerabilities leading to data leakage.

Scanning – Network scanning to identify active hosts and ports. Scanning specific application services, such as APIs, GUIs.

Enumeration – Identification of user accounts and groups in the system. Determining available functions and permissions in the application.

Vulnerability scanning and analysis – Security assessment of the operating system, database and other components. Use of standard automated and manual tools to identify vulnerabilities in the application.

Exploitation – Attempting to exploit identified vulnerabilities to gain unauthorized access or leak information. Simulating attacks on the application environment.

Post-exploitation – Continuing exploration of the environment after gaining access. Gathering additional information and attempting privilege escalation.

Reporting – Compiling a detailed report containing identified weaknesses, recommendations for improvement, and evidence of tests conducted. Delivering the results to responsible persons in the organization.

Cleanup – In case of successful access, taking measures to minimize possible consequences. Deleting traces of testing and restoring the system to its original state.

Why BDO?

BDO provides TLPT services in compliance with specific requirements of European regulators (e.g., ECB, EBA, ESMA) and proven methodologies such as TIBER-EU, CBEST, or iCAST. Our methodology combines a red teaming approach, knowledge of the regulatory framework, and deep technical know-how—including scenarios reflecting sector threats and digital attacks in the European financial space.

Certified red team with expert experience

Our specialists hold certifications such as OSCP, CRTP, eCPPT, BSCP, CEH, CRT, CPSA, CISSP, CCISO, and others. They have experience testing large banks, insurers, and ICT providers.

Knowledge of DORA, NIS2, and TIBER-EU

We understand regulatory frameworks and can tailor TLPT tests to legislative and sector oversight requirements. We assist with overall cyber resilience strategy.

Independence and credibility

As an independent consulting firm, we do not own any technologies and offer truly objective assessments. Cooperation with BDO is a clear signal of quality and trust for both regulators and clients.

Benoît Wtterwulghe
Partner
benoit.wtterwulghe@bdo.lu
+352 45 123 795

Veronika Macháčková-Koch
Director
veronika.machakova@bdo.lu
+352 45 123 776

Othmane Mouline
Senior Manager
othmane.mouline@bdo.lu
+352 45 123 863