SolutionLab

Untangling tech for humans

Threat-Led Penetration Testing (TLPT)

Version 1.0

January 2025

SolutionLab +370 526 20370 info@solutionlab.net

1 Contents

1 Contents 2
2 Threat-Led Penetration Testing (TLPT) Methodology 3
3 Qualifications 4
3.1 Preparation Phase 5
3.2 Testing Phase: Threat Intelligence (External Provider) 6
3.3 Testing Phase: Read Team Tests (SolutionLab) 6
3.4 Closure Phase 8
4 References and Sources 9
5 About this document 10

2 Threat-Led Penetration Testing (TLPT) Methodology

Threat-Led Penetration Testing (TLPT) is a crucial component of the Digital Operational Resilience Act (DORA), providing a rigorous assessment of a financial entity's resilience against sophisticated cyberattacks. This methodology outlines a DORA-compliant approach to TLPT, emphasizing alignment with regulatory requirements and industry best practices. DORA emphasizes advanced testing, especially for significant financial entities (as assessed by competent authorities based on factors like criticality, importance of functions, and ICT risk profile), thus elevating the importance of comprehensive TLPT methodologies.

This methodology is structured around the following phases, reflecting the lifecycle of a robust TLPT engagement:

- **2.1 Preparation Phase:** Scoping, planning, and stakeholder engagement.
- **2.2 Testing Phase:** Threat intelligence gathering and red team operations.
- **2.3 Closure Phase:** Reporting, remediation, and follow-up.

SolutionLab's team of experts possesses extensive experience in penetration testing, red teaming, and attack simulation. We support financial entities in navigating the TLPT journey, offering pragmatic and cost-effective solutions that address the specific requirements of DORA. We fulfil DORA requirements related to tester suitability, technical capabilities, adherence to codes of conduct, risk management practices, and professional indemnity insurance.

3 Qualifications

As SolutionLab, we possess the necessary qualifications to conduct penetration testing in accordance with DORA Article 27. Our team's capabilities directly address the key requirements:

- **Highest Suitability and Reputability:** Our team possesses the skills and expertise required for penetration testing, aligning with Article 27(1)(a). We maintain a proven track record and adhere to professional standards, demonstrating the competence DORA requires.
- **Technical and Organizational Capabilities:** We fulfill Article 27(1)(b) with our appropriate policies and procedures, including documented methodologies and quality assurance arrangements. Our advanced expertise in penetration testing and red team operations signifies our technical skills, while established processes ensure strong organizational capabilities.
- **Adherence to Formal Codes of Conduct:** We adhere to relevant professional standards, meeting the requirements of Article 27(1)(c). Following ethical frameworks and industry standards guarantees responsible testing within established guidelines.
- **Independent Assurance of Risk Management:** We support Article 27(1)(d) by having appropriate risk management policies and controls. Independent assurance reports demonstrate our robust approach to risk management during testing engagements, protecting client information and operations.
- **Professional Indemnity Insurance:** Our professional indemnity insurance further reinforces our suitability, even though it's not a direct requirement of Article 27(1)(a-d). It supports sound risk management and mitigates potential damages for tested entities, likely fulfilling criteria in Article 27(2) regarding legal and regulatory compliance.

3.1 Preparation Phase

Scoping and Planning:

- **Identify Critical Functions (CIFs):** Align with DORA's emphasis on identifying CIFs (as per Article 3) as these drive the scope and focus of the TLPT. This includes assessing interdependencies with third parties.
- **Define Scope and Objectives:** Clearly define the scope, objectives, and rules of engagement in collaboration with the financial entity. Ensure alignment with regulatory requirements outlined in DORA and associated policy instruments (e.g., RTS on TLPT). Address aspects such as target environment (production/test/both), permitted attack vectors and timelines.
- **Develop Risk Assessment:** Conduct a tailored risk assessment specific to the planned TLPT, as required by DORA, considering potential impacts and mitigation strategies. This includes addressing data protection and business risk considerations (as per Article 27 of DORA).
- **Ensure Regulatory Compliance:** Verify adherence to DORA, relevant RTS, ITS and guidance, and the NIS2 directive. Include the proportionality principle regarding the complexity of the test and the cyber maturity of the financial entity.

Stakeholder Engagement:

- **Establish Control Team (White Team):** Form a control team within the financial entity to oversee the TLPT, ensuring secrecy and appropriate communication channels.
- **Coordinate with Service Providers:** Select qualified and accredited threat intelligence and red team service providers, ensuring they meet DORA's stipulations for independence and expertise and address potential conflicts of interest (as stressed in the DORA Paper regarding testing resources and DORA's article 27). Emphasize adherence to professional indemnity insurance requirements as highlighted by DORA.
- **Draft Initiation Document:** Prepare a comprehensive initiation document outlining all aspects of the TLPT, including roles, responsibilities, communication protocols, and confidentiality agreements.

3.2 Testing Phase: Threat Intelligence (External Provider)

- **Threat Landscape Analysis:** Leverage up-to-date and sector-specific threat intelligence (as also discussed in the DORA paper regarding cyber scenarios). Focus on threat actors, their tactics, techniques, and procedures (TTPs) most relevant to the financial sector and the entity's specific CIFs. Prioritize realistic attack scenarios that reflect actual threats.
- **Scenario Development:** Design attack scenarios that simulate real-world attacks, including advanced persistent threats (APTs), phishing campaigns, supply chain attacks, and exploits targeting vulnerabilities relevant to the identified CIFs. Focus on realistic attack vectors and attack origin, which have been addressed in the source document, as also DDoS attacks, malware infection, zero day exploits, multi factor authentication fatigue attacks, insider threat and advanced persistent threat (APT), and attack targets as supply chain attack, cloud security breach, web application attack and mobile device attack. Finally, focus also on attack consequences as maximum credible events and data breach.

3.3 Testing Phase: Read Team Tests (SolutionLab)

Red Team Operations:

- **Execution of Attack Scenarios:** Execute pre-agreed attack scenarios within the defined scope and timeline, obtaining prior approval from the control team. Emphasize non-disruptive testing methodologies to ensure minimal impact on business operations.
- **Adherence to Timelines:** Conduct testing within agreed timelines, maintaining regular communication with the control team.
- **Secrecy and Confidentiality:** Uphold strict confidentiality to maintain test integrity.
- **Nemesis Integration:** Integrate Nemesis as Breach & Attack Simulation tool to enhance efficiency, automation, remediation, and reporting capabilities. This addresses the DORA relevant continuous validation and automated reporting functionalities.

Purple Teaming [1](Optional):

- **Purple Teaming (Optional):** Conduct limited purple teaming exercises where appropriate, ensuring adherence to strict secrecy protocols to maintain test integrity.

- **Collaboration:**
  - Engage in limited purple teaming exercises under exceptional circumstances to continue TLPT while ensuring secrecy.
  - Methods include "catch-and-release," "war gaming," or "collaborative proof-of-concept."
  - **Nemesis Facilitation:**
    - Offers customizable scenarios that allow for targeted assessments, facilitating collaboration between Red and Blue Teams[2].

Real-Time Monitoring and Safety Checks:

- **Safeguards Implementation:**
  - Implement measures to prevent operational disruptions during testing.
  - Suspend TLPT under exceptional circumstances to prevent risks to data, assets, or critical functions.
  - **Nemesis Safeguards:**
    - Simulates controlled cyberattacks, ensuring tests are non-disruptive and maintain operational stability.
- **Communication:**
  - Maintain regular communication with the control team to address risks dynamically.
  - Consult with the threat intelligence provider and test managers as needed.
  - **Nemesis Reporting:**
    - With one click, Nemesis provides a detailed and professional automated report that can be presented to executives to make informed decisions to strengthen their security posture.

[1] Purple Teaming - A collaborative effort between the Red Team and Blue Team to enhance security by sharing insights, testing defenses, and improving detection and response strategies during or after simulated attacks.

[2] Blue Team - Staff defending a financial entity's systems against attacks, including third-party providers, unaware of the ongoing TLPT.

3.4 Closure Phase

- **Notification:** Notify the blue team (and relevant stakeholders) post-testing, as per pre-agreed communication protocols.
- **Reporting:**
  - **Red Team Report:** Deliver a detailed red team report outlining the testing process, findings, and recommendations within a specified timeframe.
  - **Blue Team Report:** The blue team should provide a response report within a pre-agreed timeframe, detailing their observations, detection mechanisms, and response actions during the TLPT.
- **Remediation and Verification:** Assist the financial entity in implementing remediation measures and conduct follow-up testing to verify their effectiveness.
- **Feedback:** Gather feedback from all involved parties to continuously improve the TLPT process.
- **Replay and Purple Teaming Exercises:**
  - Within ten weeks post-testing, the blue team and testers conduct a replay of the offensive and defensive actions.
  - The control team leads a purple teaming exercise to address identified vulnerabilities and unresolved issues.
- **Summary Report:**
  - After the TLPT authority confirms the adequacy of the red and blue team reports, the financial entity submits a summary report of the TLPT findings within eight weeks for approval.
  - Sensitive information is omitted upon request.

4 References and Sources

- **DORA-info.eu**:
  "TLPT Regulation" - https://www.dora-info.eu/rts-tlpt/
  "TLPT Recitals" - https://www.dora-info.eu/rts-tlpt/recitals/
  "Art. 7 Specificities for pooled and joint TLPTs" - https://www.dora-info.eu/rts-tlpt/article-7/
- **GFMA**:
  "A Framework for Threat-Led Penetration Testing in the Financial Sector" - https://www.gfma.org/wp-content/uploads/2020/12/gfma-penetration-testing-guidance-for-regulators-and-financial-firms-version-2-december-2020.pdf
- **European Securities and Markets Authority (ESMA)**:
  "Final report on DORA RTS on TLPT" - https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-29_-_Final_report_DORA_RTS_on_TLPT.pdf
- **European Banking Authority (EBA)**:
  "Joint Regulatory Technical Standards specifying elements related to threat led penetration tests" - https://eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/joint-regulatory-technical-standards-specifying-elements-related-threat-led-penetration-tests

5 About this document

Document Versions			
Draft	0.1	17/11/2024	George Ziakas
Updated with SL and Nemesis information	0.2	07/01/2025	George Ziakas
DORA relevant approaches	0.3	23/01/2025	Markus Vervier
Review	0.4	23/01/2025	Zoja Antuchevič
Final version	1.0	27/01/2025	Zoja Antuchevič

Authors	
George Ziakas	gziakas@solutionlab.net
Markus Vervier	markus.vervier@persistent-security.net

https://solutionlab.net

Address
Kareivių str. 11B LT-09109, Vilnius, Lithuania

Phone
+370 652 55 795
Email
sec@SolutionLab.net