

Threat-Led Penetration Testing

SERVICE BENEFITS

- ✓ Ensures full alignment with DORA's threat-led testing requirements
- ✓ Works across CBEST, TIBER-EU and iCAST to meet varied regulatory needs
- ✓ Uses live threat data to create realistic financial sector attack scenarios
- ✓ Access to highly certified professionals with leading industry credentials
- ✓ Detailed reports with actionable remediation guidance for DORA compliance

OVERVIEW

Razorthorn delivers comprehensive red team assessments tailored for financial institutions seeking DORA compliance through advanced intelligence led penetration testing. Our service evaluates operational resilience across critical services including technology, personnel and processes that support IBSs. Working within established frameworks including CBEST, TIBER-EU and iCAST, our approach ensures financial institutions meet regulatory requirements while strengthening their security posture.

Through our partnership with iSanctuary, we deliver targeted assessments that reflect current financial sector threats and attack methods, providing genuine insight into an organisation's readiness for DORA compliance.

Our methodology combines sophisticated threat intelligence with authentic attack simulations to validate defence capabilities, while our experienced team of security professionals ensures comprehensive coverage of both technical vulnerabilities and regulatory compliance requirements, delivering actionable insights for continuous security improvement.

THE RAZORTHORN APPROACH

1. Scoping and Planning

Begins with close stakeholder collaboration to define critical assets and align testing scope with DORA requirements. During this phase, we establish clear objectives and offer additional consultancy support where needed.

2. Threat Intelligence Gathering

Leverages our partnership with iSanctuary to collect and analyse sector specific threat intelligence. This intelligence is adapted to address regional risks and informs our testing strategy.

3. Attack Scenario Design

We develop realistic attack paths based on gathered intelligence. Each scenario is crafted to ensure compliance with framework standards while targeting specific organisational vulnerabilities.

4. Red Team Execution

Involves conducting unannounced simulations that test various attack vectors including social engineering, network intrusion and data exfiltration. Our team provides real time monitoring throughout the engagement.

5. Comprehensive Reporting

Delivers detailed findings through separate TI and Red Team reports, including thorough vulnerability analysis and prioritised remediation steps. These reports serve as valuable documentation for regulatory compliance.

6. Purple Teaming (Optional)

Enables collaboration with your Blue Team to close detection gaps and implement continuous improvements. This final phase helps establish long term resilience through knowledge sharing and practical defence enhancement.

