TIBER

Threat Intelligence-based Ethical Red Teaming

Deadline for verification (Version2.0):
March 2025

What is TIBER?

The objective of the TIBER framework is to put in place a programme to test and improve resilience of financial infrastructure and institutions, at national and European level, against sophisticated cyber-attacks.

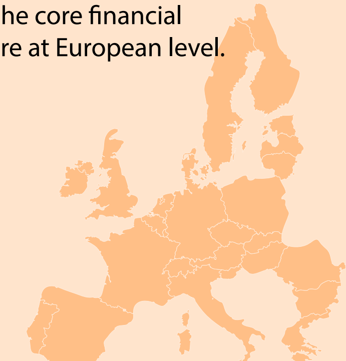
The TIBER framework has been designed for use at entities which are part of the core financial infrastructure at European level.

Here's why it matters

TIBER helps identify and address vulnerabilities in cybersecurity defences. By simulating real-world attacks, TIBER enhances resilience and ensures better protection against cyber threats.

Who it impacts?

The TIBER framework has been designed for use at entities which are part of the core financial infrastructure at European level.



What it means for your business

You will be able to bolster resilience through controlled cyber threat simulations.

Actions required:

- Make use of threat intelligence to simulate realistic cyber-attacks and test the effectiveness of your defenses.
- Enact red team tests tailored to the critical functions specific to your organization.
- Enhance my cybersecurity posture based on insights gained from testing
- Implement measures to strengthen security.

Compliance is not mandatory; hence it is up to the relevant authorities to determine whether and when TIBER tests are to be performed.

Cyberdefense

What does TIBER entail?

Assessment Preparation:

Identify critical assets and infrastructure for testing.

Establish communication channels with relevant authorities.

Engage with Red Teamers:

Select experienced red teaming professionals or third-party service providers.

Provide necessary access and permissions for testing.

Simulation Execution:

Conduct realistic cyber-attack simulations based on threat intelligence.

Evaluate detection and response capabilities against simulated attacks.

Report and Remediation:

Document findings, including vulnerabilities and weaknesses identified.

Develop and implement remediation plans based on red teaming exercise outcomes.

Engage with Regulators:

Share findings and remediation efforts with national authorities and regulators.

Collaborate on improving cybersecurity resilience based on test results