Threat intelligence-based ethical red teaming

Minds made for transforming financial services

What's involved in a TIBER-EU exercise?

The TIBER-EU framework sets out a mandatory three-phase process for an end-to-end test. The preparation phase (which includes engagement, scoping and procurement) represents the formal launch of the test. The teams responsible for managing the test are established, the scope of the test is determined, attested by the entity's board and validated by the authority (e.g., overseers or supervisors). The threat intelligence (TI) and red team (RT) providers are then procured by the entity to carry out the test.

In the testing phase (which includes TI and RT), the TI provider prepares a targeted threat intelligence report on the entity, setting out attack scenarios for the test and useful information on the entity. The report will be used by the RT provider to prepare a RT test plan and carry out an intelligence-led RT test of specified critical live production systems, people and processes that underpin the entity's critical functions.

Finally, the closure phase (which includes remediation planning and result sharing) requires the RT provider to draft a red team test report, which will include details of the approach taken to the testing, along with the findings and observations from the test.

Where necessary, the report will include advice on areas for improvement in terms of technical controls, policies and procedures, and education and awareness. The main stakeholders will now be aware of the test and should replay the executed scenarios, and discuss the issues uncovered during the test. The entity will take on board the findings, and agree and finalize a remediation plan, in close consultation with the supervisor or overseer. The process of the test will be reviewed and the key findings from it will be shared with other relevant stakeholders.

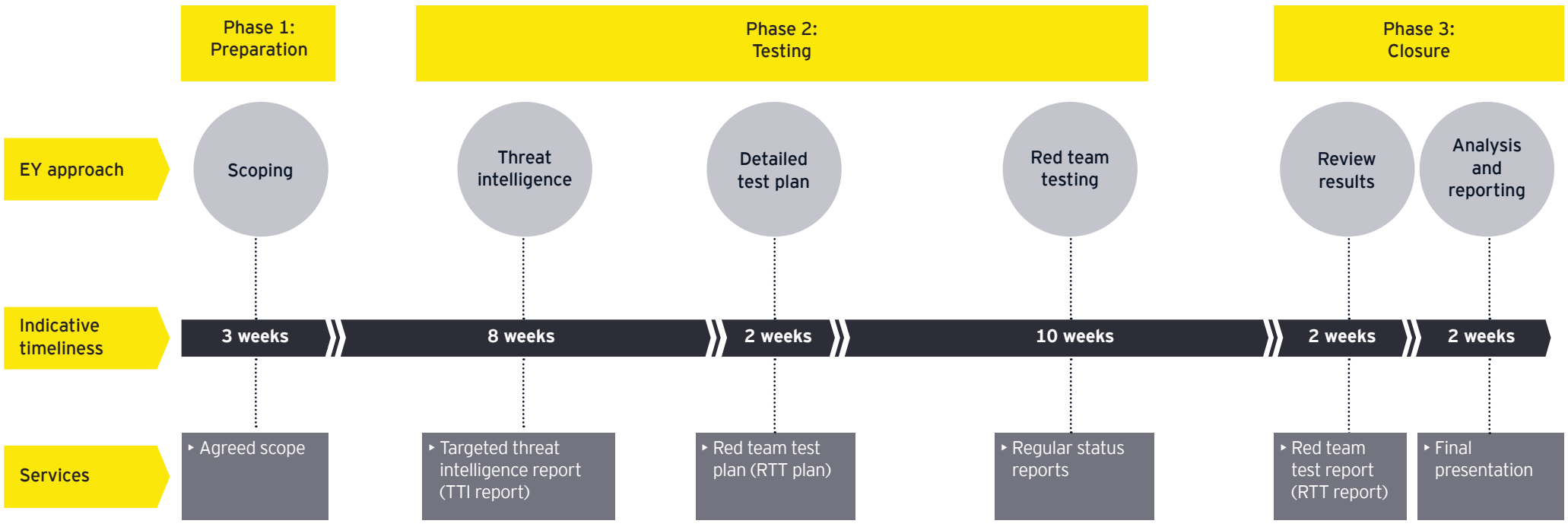
Background and context

In May 2018, the European Central Bank (ECB) published new guidance promoting increased cybersecurity resilience across financial systems through simulations of cyber-attacks that closely resemble those in the real world. That guidance is now being adopted by national authorities and local regulators across Europe.

The ECB's threat intelligence-based ethical red teaming (TIBER-EU) guidelines support European and national authorities in conducting tests, which should be applied to investment and commercial banks, payment systems, central counter-parties, exchanges and others (collectively referred to as entities). The test is designed to be based on threat intelligence specific to individual entities and to mimic the tactics, techniques and procedures of real-life threat actors.

How can organizations prepare?

- Entities should be proactive and invest in preparation and readiness activities well in advance of regulatory involvement.
- Keep in mind that delivering a test in a production environment, while aligning with regulatory frameworks, is effort-intensive, time-consuming and carries significant risk.
- Organizations should factor sufficient time to engage relevant senior management stakeholders from across the business, including board, audit and risk committees, and senior executives while keeping in mind the confidentiality of the exercise.



The time is now – get ready before regulatory engagement

Regulators see significant cyber threats to the financial system, and those that depend upon it, and are therefore strengthening their policies and guidelines to promote better overall resilience. TIBER-EU is an important part of that effort, and it is prudent for organizations to engage proactively. The framework was initially advisory, but it is being made law in some countries.

EY view point

The traditional approach to attack and penetration testing has proven effective in helping organizations identify common vulnerabilities in systems and business applications. However, financial regulators are now demanding a more holistic approach to testing an entity's ability to anticipate, prevent, detect and respond to sophisticated attacks by advanced threat actors on people, processes and technology. Regulatory-driven testing expectations combine threat intelligence, targeted testing and knowledge transfer.

How EY teams can help

EY teams have experience and capability to help guide you through some of the major challenges that are faced by organizations in completing TIBER-EU exercises. This includes:

- Our robust planning, project governance, and careful stakeholder management reduce risk and provide additional control. There is a heightened need for this when the regulator is involved in the testing exercise.
- Where actionable threat intelligence does not form part of your strategic cybersecurity program, we can help you enhance your own capability in this area, and provide guidance in order to meet regulatory demands in this regard.
- We know how organizations that do not perform them regularly can underestimate the effort involved in safely performing advanced testing in their environment.

Who to contact

Leanne Salisbury
Cybersecurity Manager
Ernst & Young S.L
T: +34 649 738 990
E: leanne.salisbury@es.ey.com

Lorenzo Bernardi
Cybersecurity Senior Manager
Special Business Services EY Consulting BV
T: +32 471 343 697
E: lorenzo.bernardi@be.ey.com

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities. EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

EY is a leader in shaping the financial services industry
Over 30,000 of our people are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. At EY Financial Services, we share a single focus – to build a better financial services industry, not just for now, but for the future.

EYG No. 005237-20Gbl
ED None

ey.com/fsminds