EUROPEAN CENTRAL BANK

EUROSYSTEM

DIRECTORATE GENERAL MARKET INFRASTRUCTURE AND PAYMENTS

Key takeaways from the ECRB roundtable on red teaming (TIBER-EU)

On 30 June 2022, the ECRB hosted its first roundtable that focused on red teaming[1], facilitated by the ECRB Secretariat and the Chair of the TIBER-EU Knowledge Centre (TKC). The roundtable was attended by 60 participants nominated by the ECRB member institutions.

The main goal of the roundtable was to enable an open discussion on the value of red teaming and the lessons learned from such exercises. Speakers from a TIBER-EU authority, the ECRB member institutions, and a red-team and threat-Intelligence provider presented their perspective on red teaming.

Several high-level themes emerged from the roundtable; below are the key takeaways:

- **Red teaming is about realistic testing of an entity's critical functions using technics, tactics, and procedures (TTP) used by real threat actors -** Being aware of the threat actors and their TTPs should be part of the cyber risk management process of all financial entities. Red teaming is the most comprehensive way for an entity to understand its strengths and weaknesses in defending its critical functions from real life cyber-attacks.

- **Red teaming provides a fresh perspective -** Frameworks like TIBER-EU allow for a fresh perspective on the cyber posture of an entity's critical functions and underlying systems. The generated insights can lead the entity to make more informed decisions on protection control improvements. For this, it is important that the threat scenarios are actionable, concise, and applicable to the entity being tested.

- **Red teaming is about communication -** this takes the form of working collaboratively at every phase of red teaming, especially between threat intelligence and red team providers, and other main stakeholders. The content, method of reporting and communicating must be tailored to the specific audience and, importantly, the outcome of the exercise must reach the highest level of the financial

[1] Within the TIBER-EU context, red teaming is the practice of simulating an attack (by ethical hackers) on the critical functions of an entity and its underlying systems, by mimicking the technics, tactics and procedures used by real hackers.

entity. What makes red teaming a unique testing tool is that it enables stakeholders to work together and learn from each other and for this, communication is vital.

- **Evolution of red teaming -** Red teaming has its own unique set of challenges e.g. the increasing need to include third parties that financial entities depend upon and to be able to simulate the TTPs of very sophisticated threat actors. In addition, greater flexibility may be needed to be able to conduct red teaming for less cyber-mature entities or across global entities.

The roundtable was received positively, and feedback indicates participants welcome future ECRB roundtables on cyber topics.