Red Teaming (short)

Martin Stanek

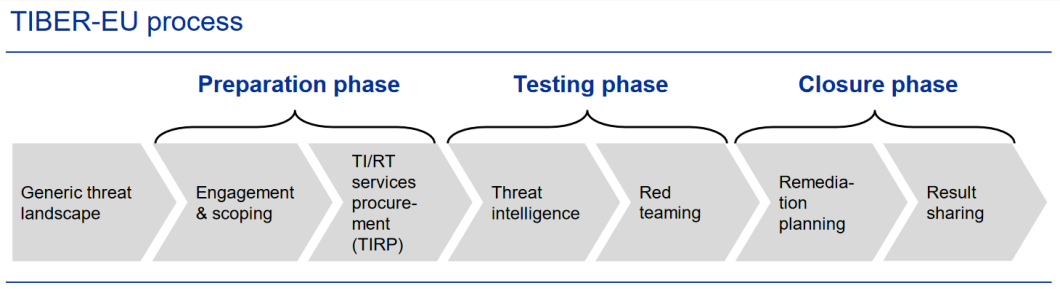
2025

Red Team vs. Blue Team

- Red team
  - *authorized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture*
- Blue team
  - *responsible for defending an enterprise's use of information systems by maintaining its security posture against real or simulated attacks*
- White team
  - *responsible for refereeing an engagement between a Red Team and a Blue Team*
- Purple team – a combination of red and blue teams
  - sharing information and insights
  - better identification of security weaknesses and vulnerabilities (speed, accuracy, coverage)

Red Teaming

- ethical hacking & goal-oriented & specific objectives
- variety of real-world TTP employed
- might be time-consuming and costly (when compared with a pentest)
- requires a careful planning and oversight



- TIBER-EU – European framework for threat intelligence-based ethical red-teaming
- ECB (TIBER-XX Implementation Guides, specific for a country/jurisdiction)

TIBER-EU (2)

- supporting guidance, templates, recommendations, e.g.
  - TIBER-EU Services Procurement Guidelines
  - TIBER-EU White Team Guidance
  - TIBER-EU Purple Teaming Best Practices
  - scoping
  - threat intelligence
  - planning
  - reporting

Variety of resources and tools

- Adversary Emulation Library (see Lecture 2)
- Atomic Red Team (`atomicredteam.io`)
  - library of tests mapped to the MITRE ATT&CK framework
  - granular verification of Blue team detection capabilities
- Automation of adversary emulation
  - Mitre CALDERA
  - Prelude Operator
- Other emulation tools, e.g.
  - Firedrill, The DumpsterFire Toolset
  - Stratus Red Team (cloud focused)

Exercises

1. TryHackMe: Boogeyman 1
   Send me a screenshot showing successfully completed all questions in Task 4.

Resources

1. ECB, *What is TIBER-EU?*
   `www.ecb.europa.eu/paym/cyber-resilience/tiber-eu`