THREAT-LED PENETRATION TESTING
Dalle esperienze TIBER-IT alle regole sui TLPT di DORA

TIBER-IT – Test volontari: esperienze, lezioni apprese e prospettive

TIBER-IT Cyber Team
Settore TIBER-IT
Divisione Continuità di servizio del settore finanziario
Servizio Supervisione Mercati e sistemi di pagamento
Dipartimento Pagamenti e infrastrutture di mercato

Agenda

- Il TIBER-IT e i TLPT: obiettivi, ruoli principali, processo
- Il TIBER-IT: esperienze e *lessons learned*
- Il TIBER-IT e i TLPT: prospettive

Il TIBER-IT e i TLPT: definizioni e obiettivi

Metodologie e strumenti per la conduzione di test avanzati di sicurezza: *Threat-led penetration testing* (TLPT) o *Red Teaming*

FSB FINANCIAL STABILITY BOARD

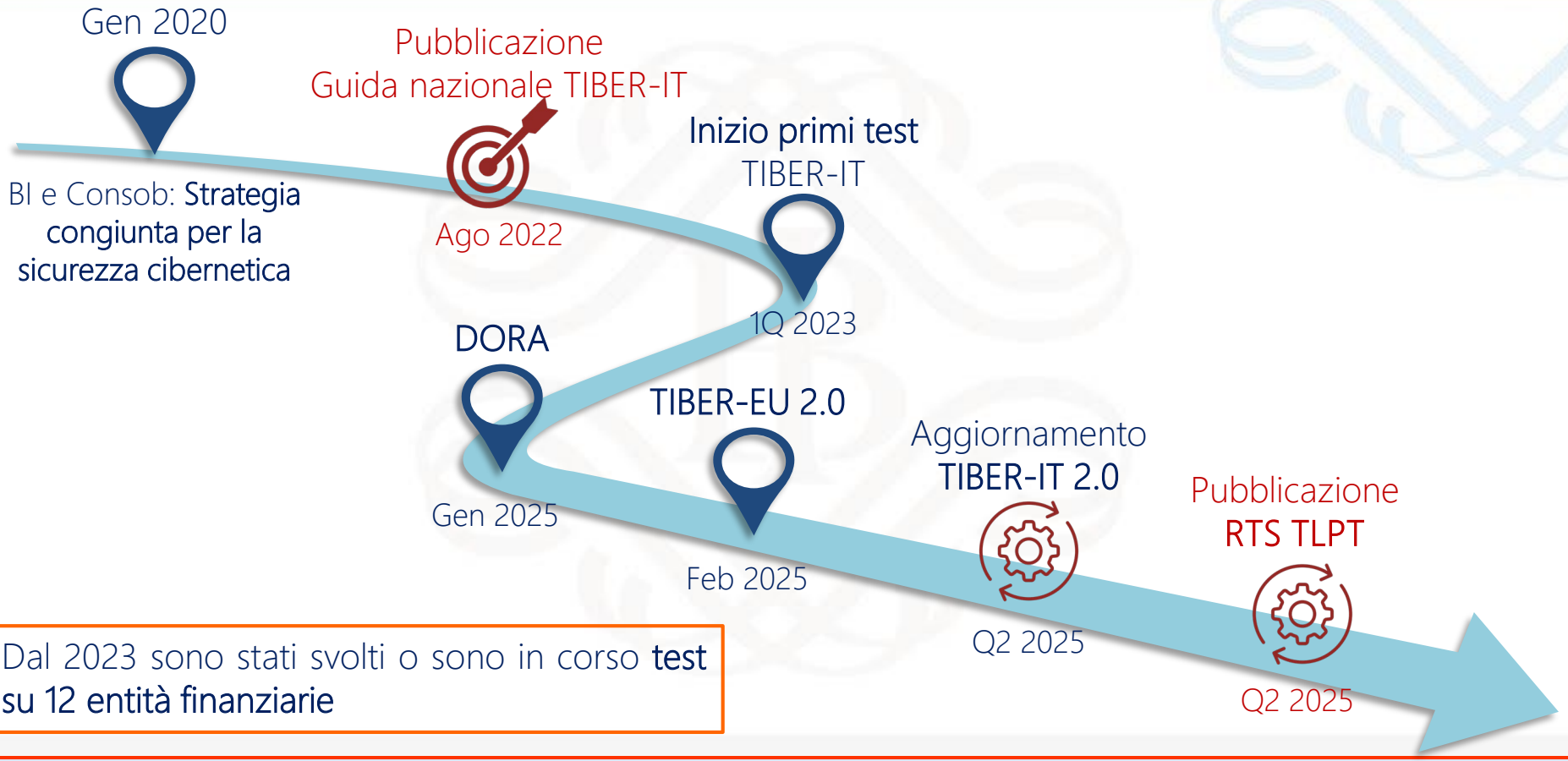
"TLPT is a **controlled attempt** to compromise the cyber resilience of an entity by **simulating the tactics, techniques and procedures of real-life threat actors**. It is based on **targeted threat intelligence** and focuses on an entity's people, processes and technology, with **minimal foreknowledge and impact on operations.**"

Fonti: G7 Fundamental Elements for TLPT (2018); FSB Cyber Lexicon (2018)

"test di penetrazione guidato dalla minaccia (TLPT): un quadro che **imita le tattiche, le tecniche e le procedure di attori reali** della minaccia che sono percepiti come minaccia informatica autentica che consente di eseguire un **test dei sistemi di produzione attivi e critici** dell'entità finanziaria in **maniera controllata, mirata e basata sull'analisi della minaccia** (red team)"

Fonte: Regolamento DORA, art. 3(17)

Il TIBER-IT e i TLPT: il percorso



Dal 2023 sono stati svolti o sono in corso **test** su 12 entità finanziarie

Il TIBER-IT e i TLPT: ruoli principali

BANCA D'ITALIA
EUROSISTEMA

ATTORI PRINCIPALI

TIBER-XX

Autorità che ha implementato il framework

Entità finanziaria soggetta a test

Fornitori di servizi esterni

TLPT DORA

Autorità TLPT*

Autorità di supervisione

Tester

RUOLI DEL PROCESSO

TIBER-XX

TIBER-IT Cyber Team (TCT)
Team Test Manager (TTM)

White Team (WT)
White Team Lead (WTL)

Red Team (RT) Provider

TLPT DORA

TLPT Cyber Team (TCT)
Test Manager (TM)

Control Team (CT)
Control Team Lead (CTL)

Blue Team (BT)

Threat Intelligence (TI) Provider

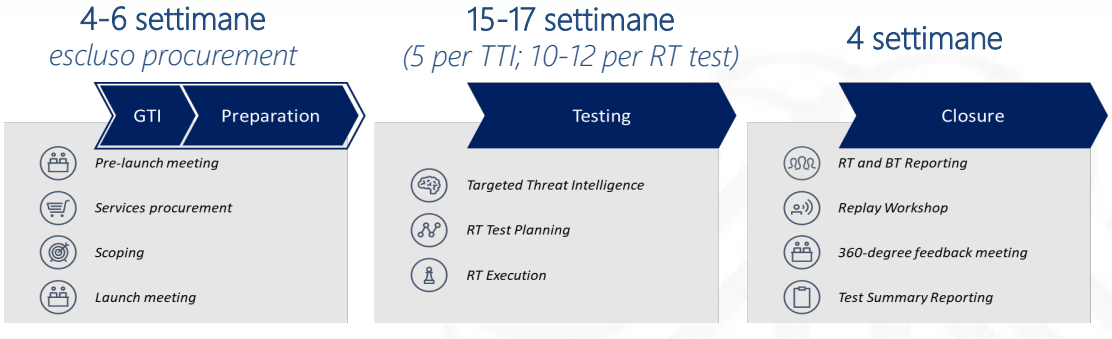
Testers (interni o esterni)

* Tipi di Autorità TLPT

- Single Public Authority – SPA (ex 26.9)
- Autorità delegata da Autorità competente (ex 26.10)
- Autorità competente (ex 46)

Attori e ruoli sostanzialmente uguali tra TIBER-XX e DORA TLPT

TLPT: il processo



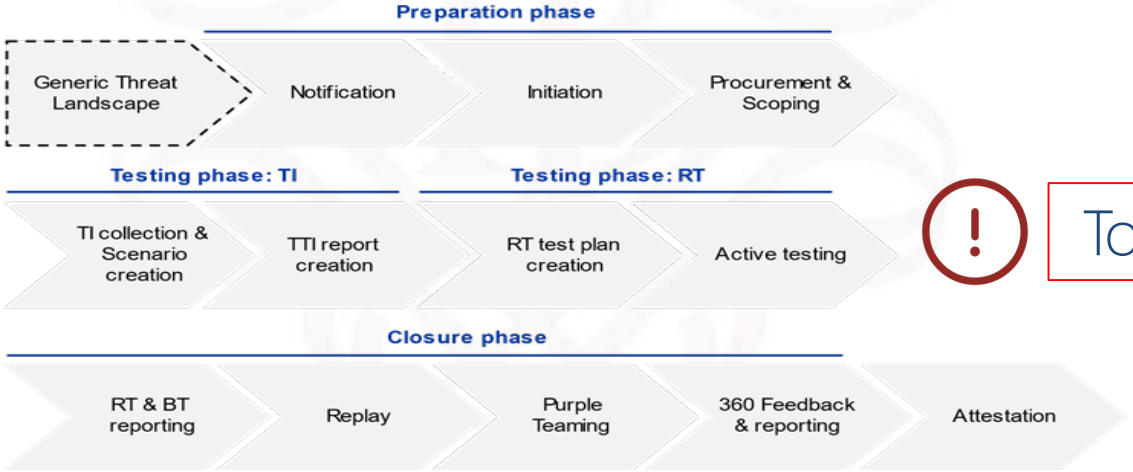
Da TIBER-IT 1.0

a TIBER-EU 2.0
e RTS TLPT

6 mesi
(di cui 3 per documenti di avvio)

Almeno 18 settimane
(4-6 per TTI; 14-15 per RT
*di cui **almeno 12 di active testing**)*

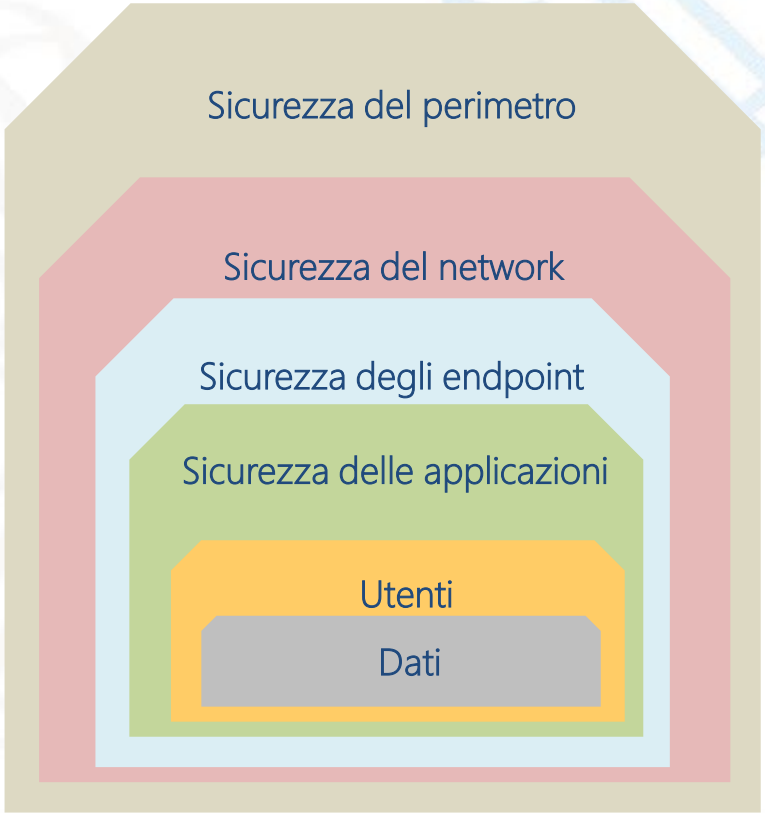
18 settimane
(10 per RTTR+BTTR+PT+replay;
8 per TSR+RP)



Totale **14 mesi**

Lezioni apprese in Europa

- La **resilienza cyber è alta**: in molti test gli attacchi vengono contenuti nel **perimetro di difesa esterno**
- In caso di **violazione del perimetro di difesa e degli endpoint**, le intrusioni sono **più difficili** da fermare
- Problemi comuni:
  - Identity & Access Management
  - Malware detection
  - Design & Architecture
  - Configuration management



Preparazione - Perimetro del test

Quante funzioni critiche inserire nel perimetro?

Trovare il **giusto compromesso** tra numero di funzioni critiche, tempistiche, risorse (economiche) ed evitare che il TLPT somigli troppo a un *penetration test*

Assenza di indicazioni precise nel framework*

Per ogni funzione critica → N sistemi a supporto

+ Funzioni = + sistemi = + lunghezza e + rischi, ma anche + opportunità di miglioramento

- Gestione del contante, ATM
- Gestione dei pagamenti
- Tesoreria e liquidità
- Infrastrutture IT condivise (es. IAM, AD, etc.)
- Digital corporate banking
- Polizze assicurative
- Internet banking
- Anagrafe Generale

** Nel TIBER-EU 2.0, per efficienza del test e in base alla granularità con cui si definiscono le funzioni critiche, se ne suggeriscono **massimo 10.** In DORA si fa riferimento a «**some or all critical functions**»*

Preparazione – Composizione del *Control Team*

Quanto grande? Chi deve essere il Control Team Lead (CTL)?

- Assenza di indicazioni precise nel framework rispetto alla numerosità
- Molto dipende dalla **struttura dell'entità finanziaria**: parcellizzata vs conoscenza di insieme
- In caso di CT molto ampi (+ di 10 persone) → ricorso a **CT core** e **CT esteso**
- CTL è «operativo» ma nel CT è presente anche un **C-level** (es. CISO, CRO, COO)
- Necessaria la presenza anche di funzioni con responsabilità nella procedura di **incident response e gestione terze parti/consulenti**
- Spesso CT è **affiancato da un PMO** nella gestione del progetto

Preparazione – Acquisizione dei fornitori

BANCA D'ITALIA
EUROSISTEMA

Lista di fornitori? Uno o più di uno? Accreditamento?

- Indicazioni precise nel framework*: rimando alla **TIBER-EU Guidance for Service Provider Procurement**
- Forte richiesta delle entità finanziarie di **schemi di certificazione e fornitori accreditati**
- Uso di **contratti quadro** già in essere per velocizzare il *procurement* e per «**fiducia**» nei fornitori
  - Attenzione del TM a evitare «conflitti di interesse» o pregressa conoscenza dell'infrastruttura
- Spesso uso di uno **stesso fornitore** per TI e RT
  - offerta economica più vantaggiosa, più semplice gestire i contratti

** Anche negli RTS sui TLPT di DORA sono presenti requisiti per i providers in termini di anni di esperienza, certificazioni, etc.*

BANCA D'ITALIA
EUROSISTEMA

Modalità di raccolta delle informazioni e definizione degli scenari

- Richiesta di un **Generic Threat Landscape** (GTL)
  - Oppure ricorso a documenti da fonti ritenute affidabili (TLS ENISA, CERTFin, ACN)
- **Almeno 5 macro scenari**, di cui 2 di backup, con un numero di flags variabile
  - Possibile aumento con più funzioni/sistemi inclusi nel perimetro
- Eventuali **scenari di backup**
  - Chiarire fin dall'inizio i criteri per la loro attivazione
  - Aumento dei costi e impatti sulla pianificazione
- Molte informazioni sulle entità sono reperibili da fonti aperte

Tipologia di scenari più frequenti

- ✓ Sfruttamento di vulnerabilità applicativa per la compromissione dei sistemi
- ✓ Compromissione dei sistemi tramite credenziali esfiltrate
- ✓ Deploy di ransomware tramite campagna di phishing
- ✓ Insider threat
- ✓ Esfiltrazione di dati sensibili
- ✓ Violazione della sicurezza fisica degli stabili e delle reti (attacco ibrido)

Nel *Targeted Threat Intelligence Report* la sezione generica è spesso **molto simile tra i vari test**.
PRO: possibilità di confronto tra test; **CONTRO**: scenari non pienamente *targeted*

Testing – Red Teaming

Gestione delle possibili *detection*

- Importanza della **valutazione dei rischi** del test e dei **processi di escalation**
  - Es. inclusione nel CT di personale che ha responsabilità sui fornitori
- **Account** del RT non facilmente riconducibili al CT
- Prevedere già nel RT Test Plan i criteri per l'eventuale passaggio al **Purple Teaming**

Gestione *leg-ups*

- Identificare i *leg-ups* **prima di iniziare** la fase di active testing e **pianificarne disponibilità e tempi di rilascio**
- **Stretta collaborazione** tra CT e RT
- **Non demonizzare** l'uso dei leg-ups

✓ *Ricezione e-mail di phishing e/o click su allegati*
✓ *Accesso VPN da esterno*
✓ *Accesso a VDI in segmenti interni della rete*
✓ *Rilascio di credenziali*
✓ *Informazioni su infrastruttura o sistema target*

Il TIBER-IT e i TLPT: prospettive (1/2)

BANCA D'ITALIA
EUROSISTEMA

DORA: requisiti relativi al testing

Basic Testing

- Il **programma di test** di resilienza operativa digitale è **parte integrante del framework dei gestione dei rischi**
- Test svolti da **soggetti indipendenti** (interni o esterni) e almeno **annualmente** su funzioni critiche
- Il programma deve prevedere **diverse tipologie di test** (ad es. *vulnerability assessments*, *code reviews*, *penetration test*)

TLPT

- **Ristretto numero di entità finanziarie** identificate dalle Autorità
- Almeno **un test ogni 3 anni**
- Mutuo riconoscimento
- Metodologia in accordo al **TIBER-EU**

Il TIBER-IT e i TLPT: prospettive (2/2)

BANCA D'ITALIA
EUROSISTEMA

EUROPEAN CENTRAL BANK
EUROSYSTEM

TIBER-EU 2.0: pubblicazione avvenuta lo scorso 11 febbraio
SSM - TLPT obbligatori: maggiori informazioni nei prossimi mesi

DORA RTS TLPT: approvazione Commissione europea avvenuta lo scorso 14 febbraio
In corso lo "scrutiny period" del Parlamento UE e Consiglio

BCE, settembre 2024: **"L'adozione del TIBER-EU contribuirà a soddisfare i requisiti di DORA"**

"*By adopting the TIBER-EU framework, competent authorities will equip themselves and financial entities to perform **sound TLPT and thereby meet the DORA requirements for such tests**.*"

"*There are **no differences** between the TIBER-EU **testing process** and the TLPT process set out in DORA.*"

"*The core requirements for DORA TLPT and the TIBER-EU framework are therefore **identical**. This means that financial entities completing a test under a national or European-level implementation of the TIBER-EU framework will, **assuming they fulfil the formal TLPT-related requirements** set by the competent authorities, be **DORA TLPT-compliant**.*"

IVASS
CONSOB

TIBER-IT 2.0 *(coming soon…)*
Identificazione entità per TLPT DORA
Prosecuzione **test volontari**

Contatti

Link alla pagina TIBER-IT

tiber-it@bancaditalia.it

Alcune icone in questa presentazione sono state reperite su Flaticon.com