REDFin

Co-financed by the European Union
Connecting Europe Facility

ABI Lab

Be (Cyber) Prepared

Framework per verificare la capacità di risposta

Workshop
7 novembre 2019

IL SALONE DEI PAGAMENTI
PAYVOLUTION

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Perché un CERT Finanziario? - Obiettivi

Il CERT Finanziario Italiano:

- risponde all'esigenza di **innalzare** la **capacità** del settore di **gestione dei rischi cyber** e di **coordinamento** in caso di attacchi
- è un'opportunità di **coordinamento** centrale delle attività di contrasto e prevenzione per una strategia di cybersecurity di settore sempre più efficace

DIFFONDERE LE COMPETENZE CYBER E FARE AWARENESS

- Approfondire **contenuti e impatti** delle **normative** di riferimento sul tema della **cybersecurity**
- Sviluppare **campagne di sensibilizzazione** sulla cybersecurity
- Svolgere **esercitazioni** e **simulazioni su scenari cyber**

SVILUPPARE UNA LOGICA DI ISAC ITALIANO

- **Incrementare l'info-sharing** su minacce/ vulnerabilità/ incidenti
- Svolgere **analisi evolutive** delle **minacce cyber**
- Monitorare l'evoluzione dei **rischi** emergenti e gli **impatti** per il settore finanziario

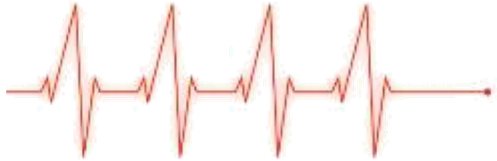
COORDINARE LE EMERGENZE E GLI INCIDENTI INFORMATICI

- **Svolgere attività di coordinamento** centrale in caso di **incidente**
- **Supportare operativamente** le strutture di presidio delle **singole realtà**
- **Definire e aggiornare** a livello di settore lessons learned e strategie di risposta

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

CERTFin – Activities Overview

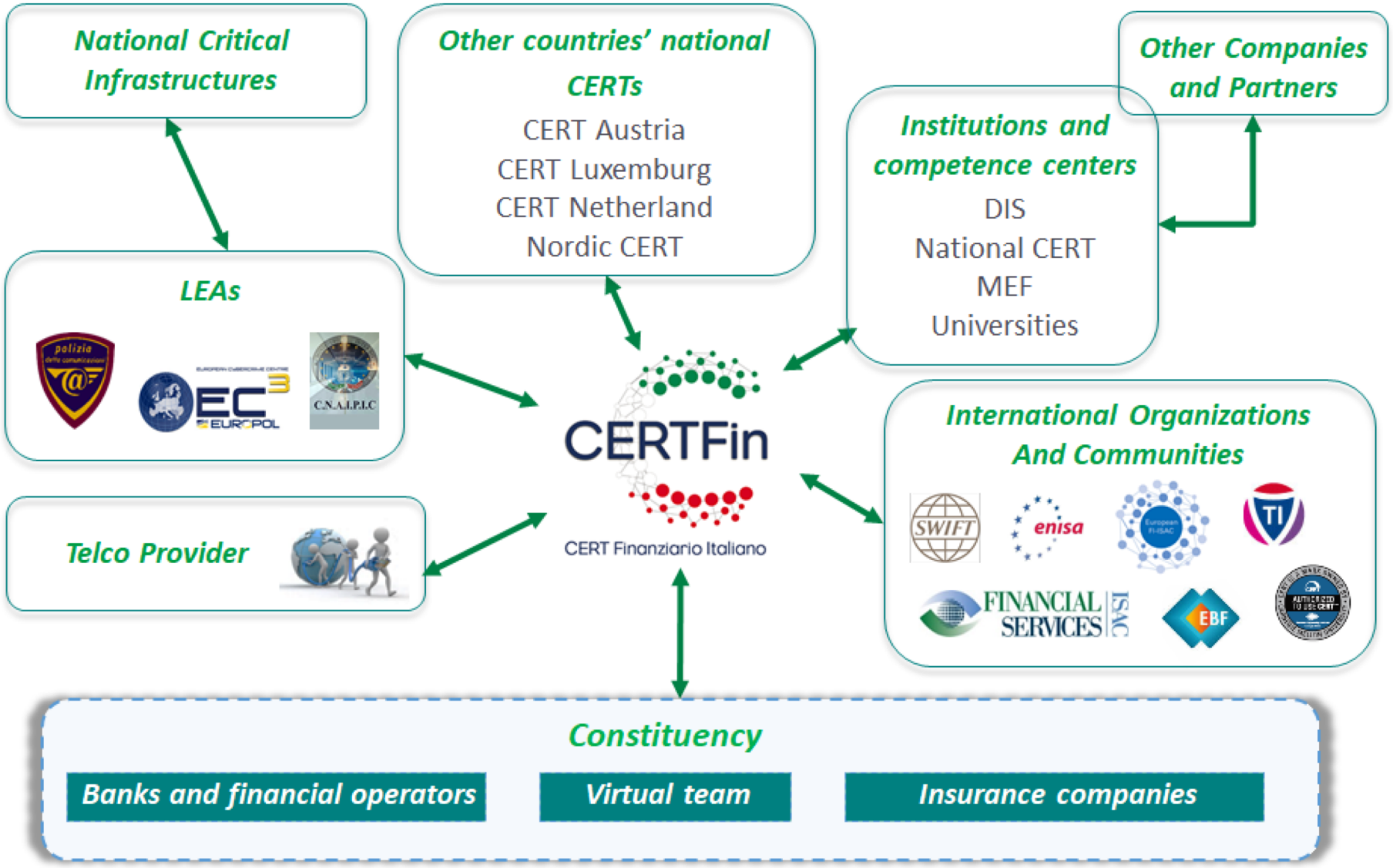
CERTFIN ACTIVITIES

FINANCIAL INFO SHARING AND ANALYSIS CENTER (FinISAC) 	CYBER KNOWLEDGE AND SECURITY AWARENESS 	CYBER EMERGENCY RESPONSE TEAM 
THREAT INTELLIGENCE AND LANDSCAPE SCENARIO 	AWARENESS 	EUROPEAN PROJECTS 

49 Participants (including Banks, Insurance companies, Market infrastructures)

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Il CERT Finanziario Italiano come network di collaborazioni per rafforzare la sicurezza

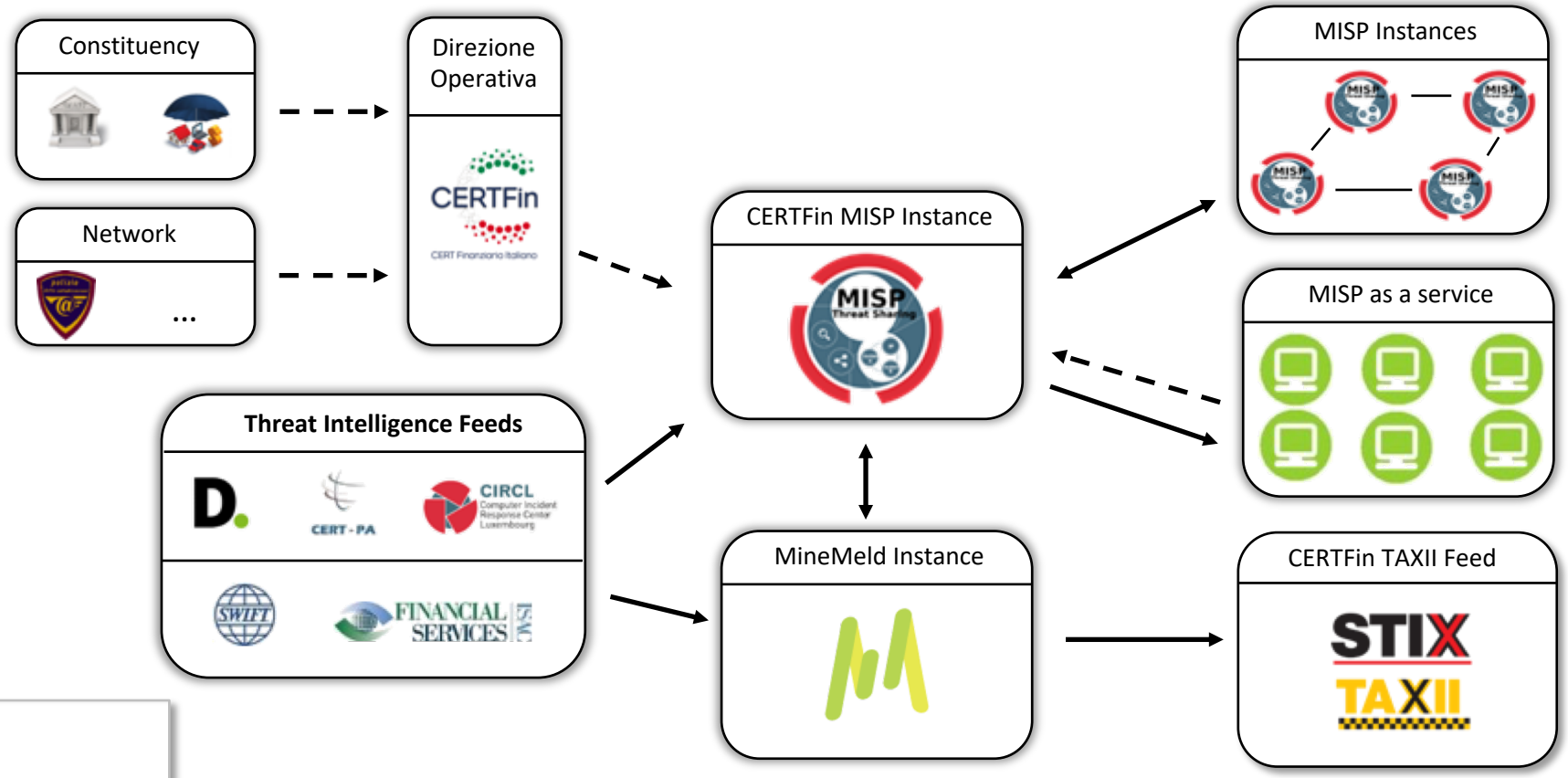


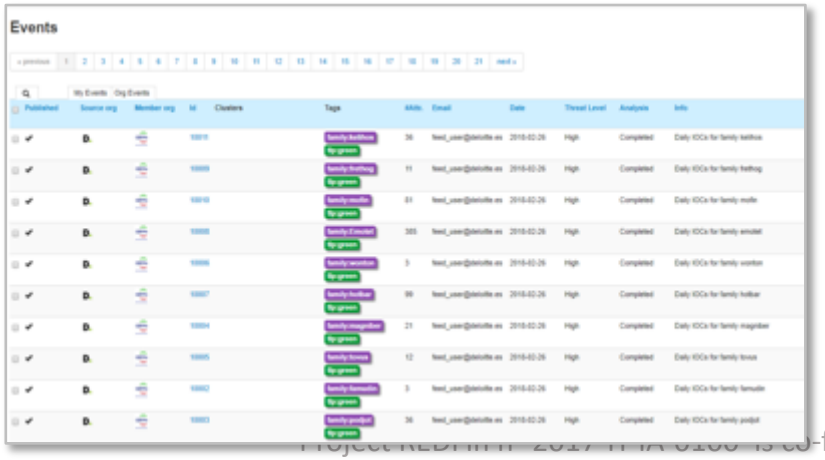
Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

L'architettura per l'information sharing tramite MISP

FULLY OPERATIONAL

- La **MISP (Malware Information Sharing Platform)** consente di ricevere **informazioni** su **attacchi** ed altri fenomeni fraudolenti **in forma strutturata** ed in un formato machine readable (**STIX**)
- Aumenta il **costante e tempestivo scambio di informazioni** utili a scoprire, prevenire e constastare eventi che possano impattare **l'integrità**, la **disponibilità** e la **riservatzza** delle





Eventi ed IoC totali gestiti tramite MISP*

Eventi	IoC	Media IoC / Evento
>106.000	6.655.932	62

Project REDFin IT-2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Resoconto attività CERTFin nel 2019

Information Sharing – FinISAC

SINTESI OPERATIVITÀ

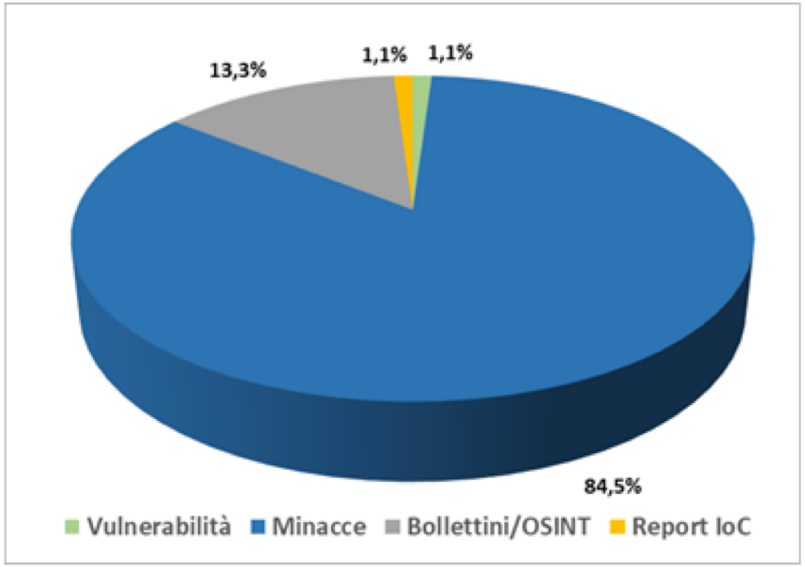
Inviati alert relativi a **570 differenti fenomeni,** che considerando anche eventuali approfondimenti/update sono pari a oltre **790 segnalazioni**

Inviate **63 segnalazioni a singole banche su minacce, possibili compromissioni o specifiche vulnerabilità sulla rete**

Monitorate **44 segnalazioni a singole organizzazioni su specifiche vulnerabilità sulla rete**

Interessati oltre **63.452 destinatari**

TIPOLOGIE SEGNALAZIONI



RELAZIONI CON LA CONSTITUENCY E CON GLI STAKEHOLDER

10 sessioni di approfondimento con il Team Virtuale

Confronto e **condivisione principali fenomeni** con CNAIPIC, Telco Provider e CERT Nazionale

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

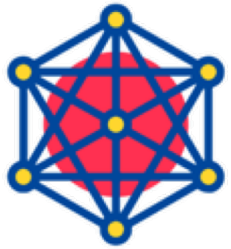
REDFin – Come è nato

Readiness **E**nhancement to **D**efend **Fin**ancial Sector

Risponde ad una call europea (**CEF-TC-2017-2: Cyber Security**) rivolta a migliorare I livelli di preparazione dei CERT

Si propone di incrementare il grado consapevolezza e di resilienza nel settore finanziaria italiano

Fornendo strumenti per prevenire e rispondere ad attacchi cyber



Tramite un approccio innovativo basato su **Cyber Threat Intelligence** e **Metodologie di Test** mirate alla

- **Uniformazione** dei processi
- **Ottimizzazione** delle risorse
- **Confrontabilità** dei risultati

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Le Fasi del Progetto

1. Project Management

- Project Plan
- Data Management Plan
- Kick-off meeting
- Business sustainability model
- Final technical report

Completed

2. Analysis of cyber tabletop and red teaming exercises

- Report describing the current context of cyber exercises of the Banking sector in Europe

Completed

3. Developing of Methodologies and operating models for

- Threat Intelligence and Scenario Identification
- Cyber Tabletop
- Red Teaming

Completed

4. Identification of cyber threat scenarios

- at **least 2 threat scenarios one for cyber tabletop and one for red teaming** will be identified leveraging on Cyber Threat intelligence capabilities
- The output will be used for the exercises foreseen in Activity 5
- summary of potential key **threats scenarios targeting the financial sector**
- **potential attack surfaces** (people, processes and infrastructure)

Completed

5. Execution of cyber tabletop and red teaming exercises

- Development of **educational material** for the cyber exercises and **educational sessions**
- **2 cyber tabletop exercises** with **20 participants** interested into the exercise
- **3-5 Red-Teaming exercises** will be conducted,. **Each** exercise will **involve only one bank**, responding to a dedicated call of interest and applying on a voluntary' base

6. Dissemination

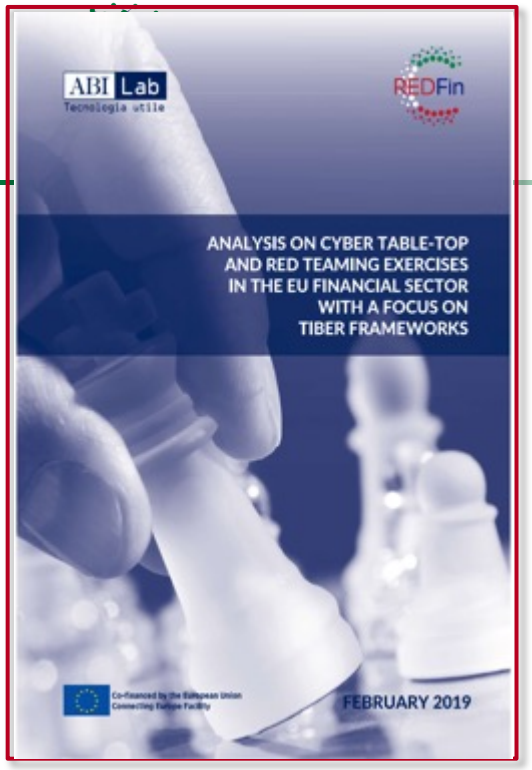
- Continuous representations of the project achievement to CERTFin constituency and European W.G.. e.g. ENISA FI-1SAC; EC3 Europol EBF.
- Events & workshop
- Final presentation of project result, and brochure and publications

Ongoing

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

La prima pubblicazione

ABI Lab



Report on cyber exercises in the EU banking sector

REDFin — Co-financed by the European Union, Connecting Europe Facility — ABI Lab Tecnologia utile

Feature/Attribute: Supporting Documentation

CBEST	TIBER-NL	TIBER-EU	TIBER-BE	TIBER-DK
• CBEST Implementation Guide • CBEST Scope Specification • CBEST Services Assessment Guide • CBEST Understanding Cyber Threat Intelligence Operations • CBEST An introduction to Cyber Threat Modelling • CBEST Targeting Report Specification Document • CBEST Threat Intelligence Report Specification • CBEST Intelligence Assessment • CREST Penetration Testing Servic • CBEST Asses • CBEST and R • Intelli Respo • Intelli - Th of - Qu int - Th	• TIBER-NL Guide: How to conduct the TIBER-NL test • Ideal White Team Lead • White Team Guidance • Services Assessment Guide • Format Scope Specification • Format Test Plan • Format Red Team Test • Format 360 Feedback Report • Format TIBER-NL Test Summary	• TIBER- EU Framework: - How to implement the TIBER-EU framework - Services Procurement Guidelines - White Team Guidance	• TIBER-BE framework National Implementation Guidance • Format Scope Specification • Format Test Plan • Generic Threat intelligence document • Format RT Test Report • Format TIBER-BE Test Summary • Format 360° feedback Report • TIBER- EU Framework - White Team guidance - Services Procurement guidelines	• TIBER-DK General Implementation Guide • TIBER-DK Generic TL report • TIBER-DK Operational Guide • TIBER- EU Framework - White Team guidance - Services Procurement guidelines - Scoping Template - Input for TTI template - 360 feedback templates

Definition - Official definition of the Framework
Framework Promoter - Subject(s) that promote the adoption of the framework
Framework Target - Recipient(s) of the Framework
Parties Involved - (Authorities – Entities - Service Providers)
Service Provider – Conditions for the test service providers
Supervision - Subject(s) in charge of the Framework implementation
Test - Typology of tests to be conducted according to the Framework
Threat Intelligence Sources - suggested in the Framework
Test targets - Target(s) involved in the test
Phases - Phases envisaged by the Framework
Phases Output - Documents/Reports produced as outputs of the Framework's phases
Supporting Documentation - for the implementation of the Framework

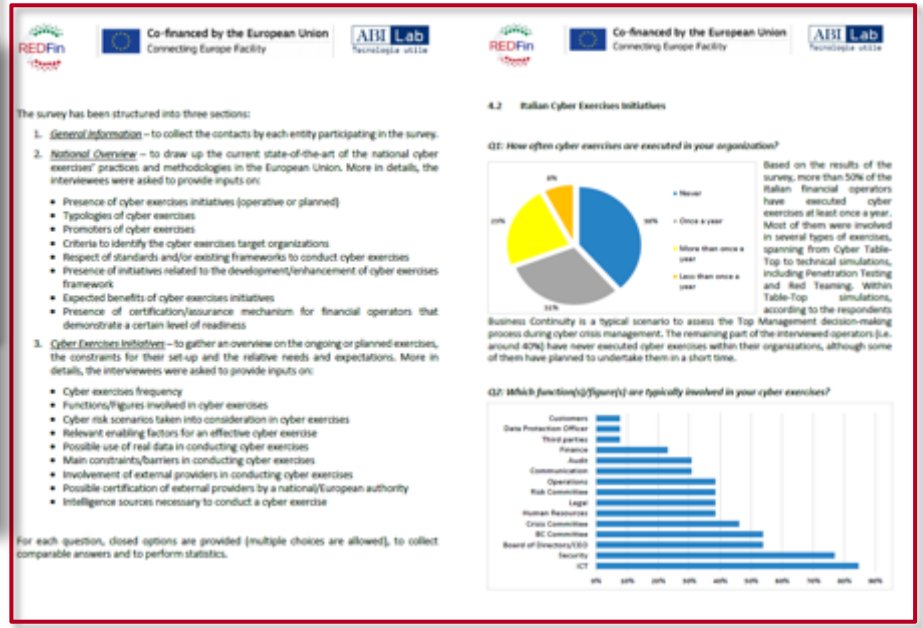
REDFin — Co-financed by the European Union, Connecting Europe Facility — ABI Lab Tecnologia utile

Feature/Attribute: Threat Intelligence Sources

CBEST	TIBER-NL	TIBER-EU	TIBER-BE	TIBER-DK
• OSINT • Internal sources • Governmental sources • CLOSINT	• OSINT • Internal sources • TECHINT • HUMINT	• OSINT • Internal sources • Governmental sources • Dark web	• OSINT • TECHINT • HUMINT • Intelligence-based intial targeting	• Internal sources • OSINT • HUMINT

Feature/Attribute: Test targets

CBEST	TIBER-NL	TIBER-EU	TIBER-BE	TIBER-DK
Critical functions: the people, processes and technologies required to deliver a core service which, if disrupted, could have a detrimental impact on UK financial stability, the firm's safety and soundness, the firm's customer base or the firm's market conduct.	**Critical Economic Functions:** the people, processes and technologies required to deliver a core service, which, if disrupted, could have a detrimental impact on the Dutch financial stability, the firm's safety and soundness, the firm's customer base or the firm's market conduct.	**Critical functions:** a function that can be considered critical or essential to the financial services sector and/or a financial services sector organization. They encompass critical technological systems, processes, and people.	**Critical functions:** the people, processes and technologies required to deliver a core service which, if disrupted, could have a detrimental impact on the financial stability, the concerned institution's safety and soundness or the institution's customer base.	**Critical functions:** the people, processes and technologies required by the tested institution to deliver a core service which, if disrupted, could have a detrimental impact on financial stability, the institution's safety and soundness, the institution's customer base or the institution's market conduct.



In Italia si pensa che…

Gli **scenari critici** si compongono con **logical threats** (malware, hackers o attacchi DOS) verso **servizi on-line**

Le **funzioni aziendali** da coinvolgere nelle esercitazioni sono ICT e Sicurezza, Alta Direzione e Continuità Operativa

OSINT (fonti aperte) e **deep/dark web** sono considerate fonti di informazioni valide

Circa il 60% dei rispondenti desidererebbe che I **fornitori** di threat Intelligence e di servizi di test siano **qualificati**

E inportante poter disporre di **risorse esterne** a support delle esercitazioni cyber

I principali fattori abilitanti sono:
Impegno del Top Management
E **disponibilità di risorse qualificate**

I maggiori vincoli per l'esecuzioni di esercitazioni cyber sono

1. **Scarsità di know-how**
2. Costi
3. Consenso interno

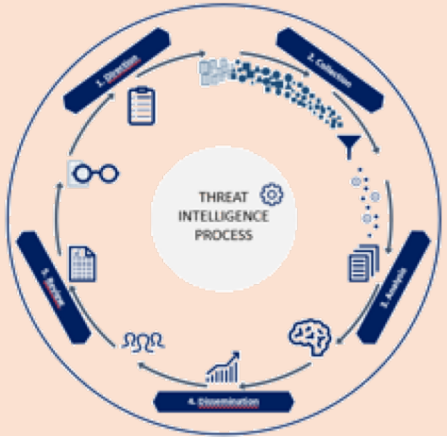
Esercitazioni cyber vengono eseguite almeno una volta l'anno da più del 50% degli intervistati

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Le Metodologie

Cyber Threat Intelligence (CTI)

- Definizioni
- Due livelli: GTI & TTI
- Fasi della Metodologia
- Gli Output



Red Teaming (RT)

- Introduction
- Phases Overview
- Roles & Responsabilities
- Preparation & Testing Phases
- Closure Phase
- Gant chart

Table-Top (TT)

- Introduction
- Phases Overview
- Roles & Responsabilities
- Planning
- Design
- Execution
- Evaluation
- Gant chart

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Intelligence

Intelligence : un tipo particolare di informazione

- ***Dato***: un dato elementare (nome, età, cap, telefono, etc).

- ***informazione***: dati inseriti in un contesto, o considerati ad un livello superiore di astrazione (contatto della rubrica del cellulare)

- ***Conoscenza***: interpretazione ed utilizzo delle informazioni per risolvere problemi o prendere decisioni. (a quali contatti invio pubblicità sul nuovo gusto di gelato)

BANK OF ENGLAND, CBEST Intelligence-Led Testing – 2016
https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf

Threat Intelligence è il processo strategico di raccolta ed analisi delle **informazioni utili a creare conoscenza per ridurre I rischi**.

Queste informazioni riguardano **identità**, **obiettivi**, **motivazioni**, **tattiche** e **strumenti** delle minacce

rivolte **verso** determinati **bersagli** , organizzazioni, funzioni e processi aziendali , **o** le **informazioni** in essi contenute

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Cyber Threat Intelligence

Definition

Cyber Threat Intelligence *consiste in una serie di* ***informazioni*** *analizzate* ***sull'intenzione, l'opportunità e la capacità di agire di attori malintenzionati.*** *Può essere considerato un sottoinsieme di attività di intelligence su un'organizzazione, poiché* ***si concentra sulle minacce informatiche*** *e affronta gli obiettivi aziendali al fine di determinare se l'intelligenza creata è utile*

Objective

L'obiettivo principale di Cyber Threat Intelligence è **ridurre l'incertezza** sviluppando rapporti, chiamati anche **scenari di minaccia**, che sono **attuabili, tempestivi e pertinenti**, e tali da consentire **decisioni** più informate per la **riduzione del rischio**

Methodology

La **Generic Threat Intelligence** (GTI) ha lo scopo di produrre uno **scenario minacce per il settore finanziario italiano**, concentrandosi sull'identificazione delle cyber-threat nazionali e settoriali. Si basa su scoperte del settore, eventi raccolti, vulnerabilità finanziarie rilevate e tendenze di attacco.

La **Targeted Threat Intelligence (TTI)** ha lo scopo di produrre uno **scenario minacce specifico per un attore finanziario**, (Targeted Threat Scenario), concentrandosi sull'identificazione di cyber-threats caratteristici, relativi alle funzioni aiservizi critici, alle vulnerabilità che colpiscono beni tecnologici in uso,.

Benefits

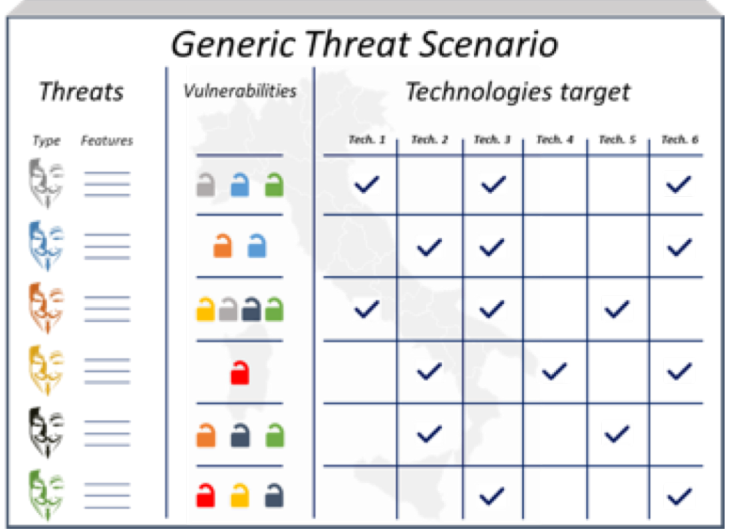
Il vantaggio principale di Cyber Threat Intelligence è la produzione di un output contestualizzato che **crea conoscenza volta a mitigare** una circostanza o un evento cyber che abbia il potenziale per sfruttare intenzionalmente o involontariamente una o più vulnerabilità, con conseguente **perdita di riservatezza, integrità o disponibilità** di informazioni e servizi.

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic e Targeted Threat Intelligence

Identifica le **minacce informatiche a livello nazionale e settoriale**, sulla base di informazioni di settore (eventi di minaccia, vulnerabilità finanziarie e tendenze di attacco).

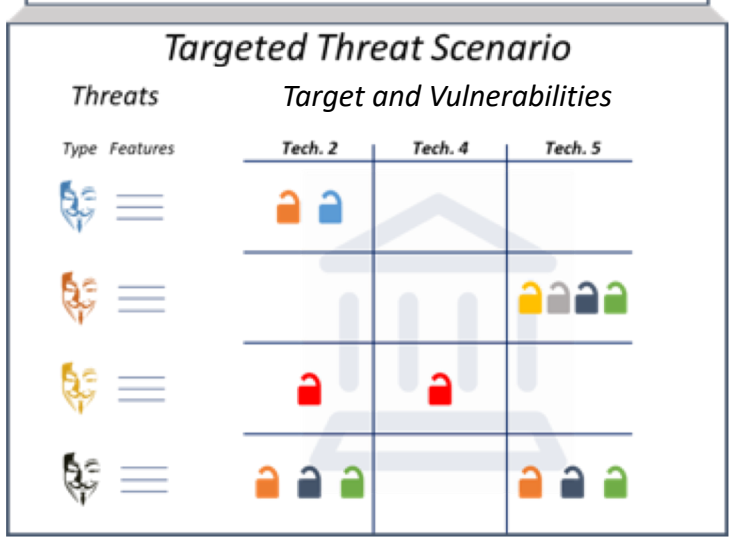
Identifica le **minacce informatiche specifiche del contesto** relative a funzioni e servizi critici, vulnerabilità che incidono sulle risorse tecnologiche. Parte dalla la GTI.



Documentazione interna

logs

informazioni



Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

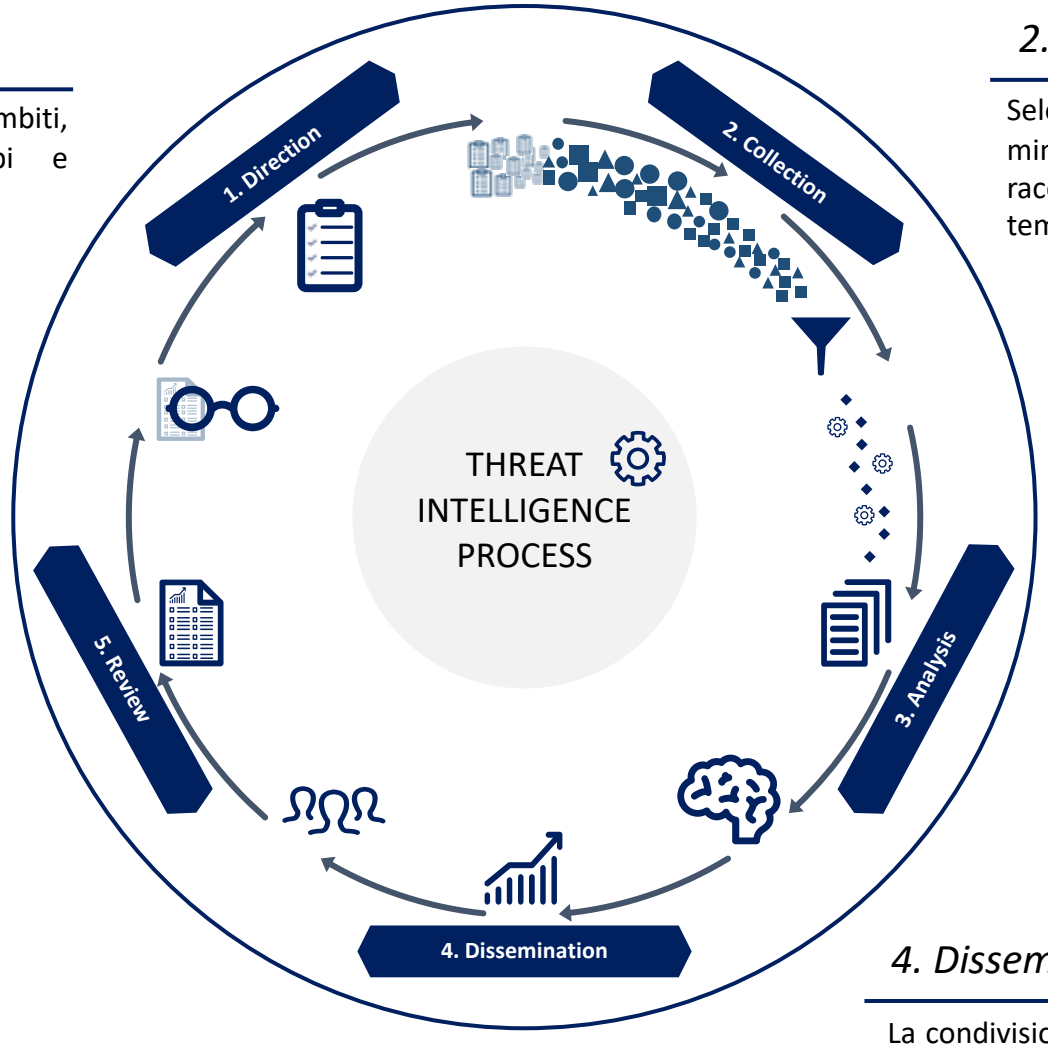
Threat Intelligence - Fasi della metodologia

1. Direction

Individua obiettivi finalità, ambiti, sorgenti informative, tempi e risorse.

2. Collection

Selezione di informazioni specifiche sulle minacce e informazioni relative mediante raccolta e normalizzazione di dati in tempo reale e passati.



3. Analysis

Trasformazione dei dati grezzi e loro combinazione per formare un quadro generale di intelligence delle minacce, colmando eventuali lacune in cui le informazioni disponibili sono insufficienti.

5. Review

Implementa la logica di miglioramento continuo della metodologia di intelligence sulle minacce informatiche : questa attività deve evidenziare:
Deviazioni dai risultati previsti;
Esecuzione di modifiche al piano di produzione TI

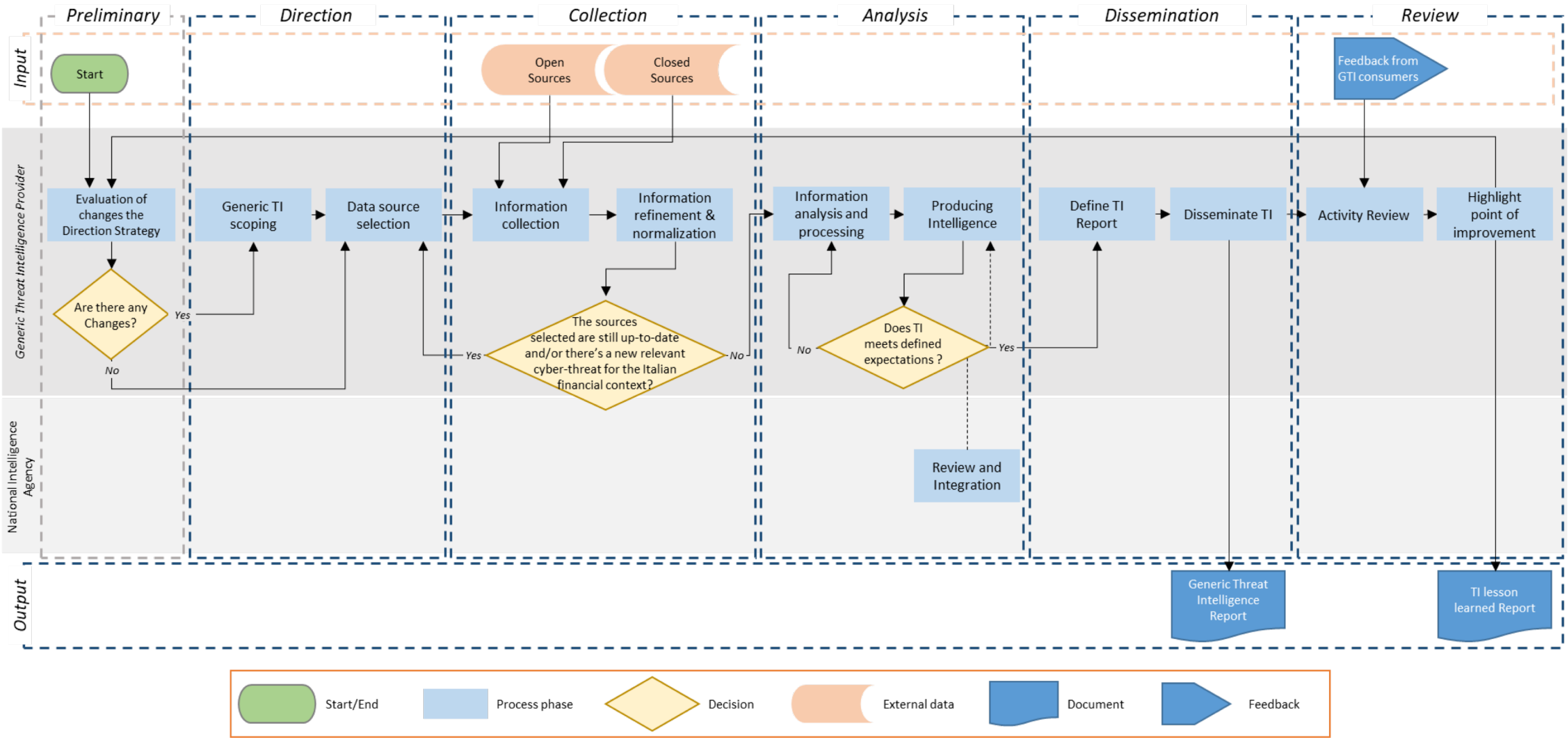
- .

4. Dissemination

La condivisione è una fase fondamentale di TI volta a diffondere la conoscenza ai livelli strategici, operativi e tattici all'interno delle organizzazioni.

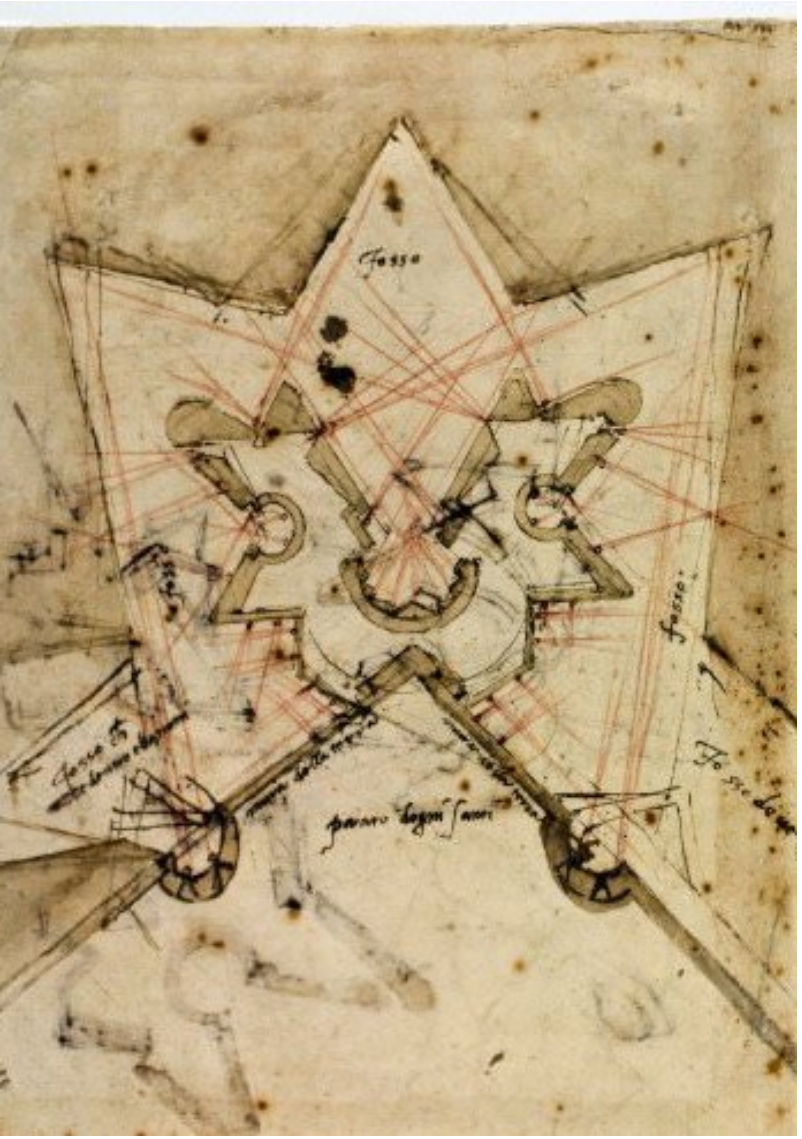
Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Threat Intelligence – Fasi della metodologia



Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Threat Intelligence – Perché?



- Con gli spagnoli in Italia, i fiorentini decisero di deporre Alessandro de' Medici e costituire un governo repubblicano.
- Temendo un assedio **dopo il sacco di Roma** nel 1529 nominarono "Governatore generale sopra le fortificazioni" un famoso artista, uno dei primi ad appoggiare la repubblica, incaricandolo di **programmare** i bastioni per **la difesa** della città in **previsione dell'assedio** che sarebbe stato operato dalle forze imperiali.

1. Direction

- Egli visita **Pisa**, **Livorno** e **Ferrara** per studiarne le fortificazioni.

2. Collection

- Capisce che le difese di Firenze, realizzate per altri tipi di attacchi, **non** sarebbero state **in grado di resistere ai nuovi bombardamenti**

3. Analisys

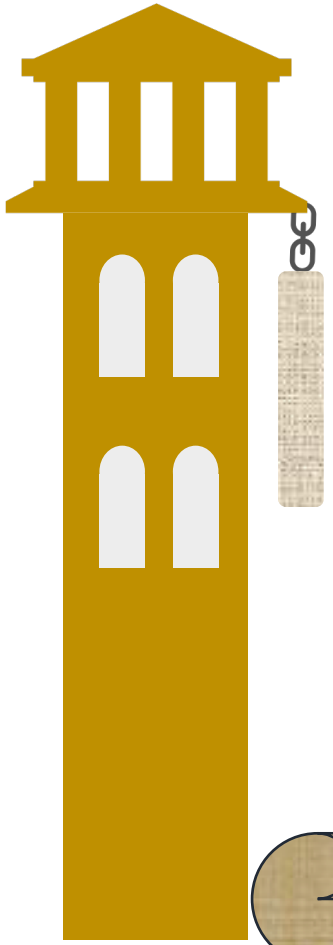
- Realizza quindi dei disegni di opere complesse dalle forme concave e convesse che consentissero sia la **difesa dalle nuove artiglierie** che il contrattacco.

3. Dissemination

- Ma non cera tempo per realizzarle

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Threat Intelligence – Perché !

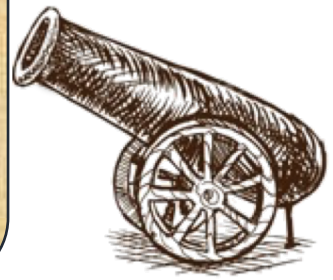


Da Ascanio Condivi nella sua vita ediz. Fior del 1746

Giunto in Firenze la prima cosa, che facesse, fu di fare armare il Campanile di San Miniato, il quale era per le continue percosse dell'Artiglieria nemica, tutto lacerato, e portava pericolo, che a lungo andare non rovinasse con gran disvantaggio di quei di dentro.

Il modo di armarlo fu questo: che pigliando un gran numero di materassi ben pieni di lana con gagliarde corde giù gli calava dalla sommità fin a piè , coprendo quella parte , che poteva esser battuta.

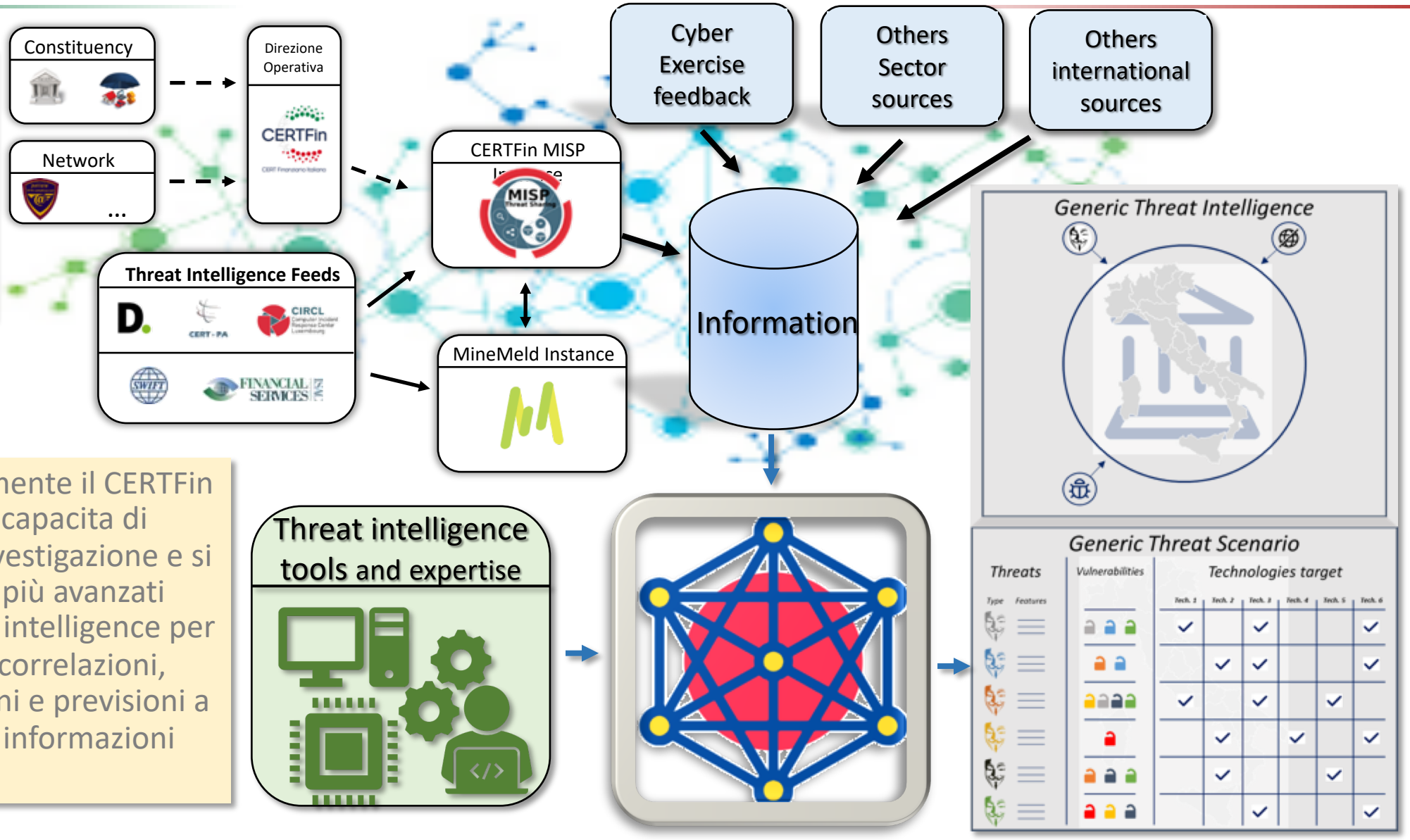
E perciocchè i Cornicioni della Torre sporgevano in fuori, venivano i Materassi ad esser lontani dal muro principale del Campanile, meglio di sei palmi, di manierachè le palle dell'Artiglieria venendo, parte per la lontananza d'onde eran tratte, parte per lo objetto di que materassi, facean nessuno, o poco danno non offendendo nè anco i materassi medesimi, perciocchè cedevano.
Così si mantenne quella Torre tutto il tempo della guerra, che durò un'anno senza che mai fosse offesa, e giovando grandemente per salvar la terra, ed offendere i nemici.



Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Threat Intelligence nel CERTFin

A partire dal FinISAC e dal complesso delle sue altre attività di studio e monitoraggi il CERTFin ha accesso a numerose sorgenti informative



Più recentemente il CERTFin ha acquisito capacita di analisi ed investigazione e si è dotato dei più avanzati strumenti di intelligence per consentono correlazioni, estrapolazioni e previsioni a partire dalle informazioni raccolte

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Developing of Methodologies and Operating Models

Cyber Threat Intelligence (CTI)

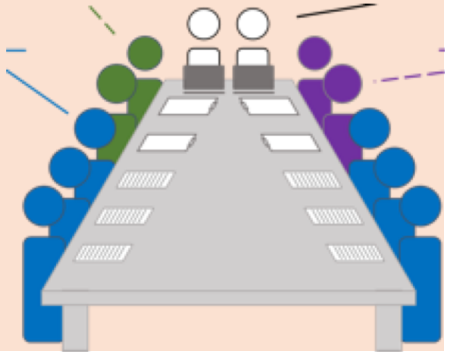
- Definizioni
- Due livelli: GTI & TTI
- Fasi della Metodologia
- Gli Output

Red Teaming (RT)

- Introduction
- Phases Overview
- Roles & Responsabilities
- Preparation & Testing Phases
- Closure Phase
- Gant chart

Table-Top (TT)

- Introduction
- Phases Overview
- Roles & Responsabilities
- Planning
- Design
- Execution
- Evaluation
- Gant chart



Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Table-Top

Definition

Cyber Table-top sono **esercizi informatici basati sulla discussione** volti a testare, in modo simulato, la risposta agli incidenti informatici e i piani di continuità aziendale.

Coinvolge un pubblico specifico limitato composto dalle **principali parti interessate** per la gestione di eventi di cyber crisi o emergenza; le parti interessate sono in genere **quadri** e **top manager** e personale del **team interno per la sicurezza** delle informazioni.

Objective

Valuta la **capacità** dei partecipanti **di** implementare i processi di **risposta agli incidenti informatici** dell'organizzazione e le capacità per affrontare un attacco informatico complesso.

Fare pratica con gli strumenti di **comunicazione aziendale** e le **procedure di crisi/emergenza**, verificando anche la capacità di definire comunicazioni chiare per i dipendenti e le parti interessate esterne e di convocare il comitato di crisi **in modo tempestivo**.

Benefits

Far **toccare con mano i potenziali impatti** di un evento cyber, le implicazioni, le complicazioni gestionali e organizzative.

Simulare il **coinvolgimento** di diverse parti interessate:

- Nel **processo di gestione di crisi** / incidenti;
- Nei **processi decisionali**;
- Nella **risposta del gruppo** durante questi tipi di eventi.

Consentire ai partecipanti di acquisire **familiarità con i ruoli e le attività nello scenario di crisi** / incidente, aumentando il livello generale di **conoscenza** e **consapevolezza**.

Migliorare le capacità di **comunicazione e coordinamento** durante la fase di risposta alle crisi.

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Le fasi del Table-Top

Planning

- *Pre-launch meeting*
- *Service Procurement*
- *Scoping*
- *Launch Meeting*

GTI Design

- *TT Test planning*

Execution

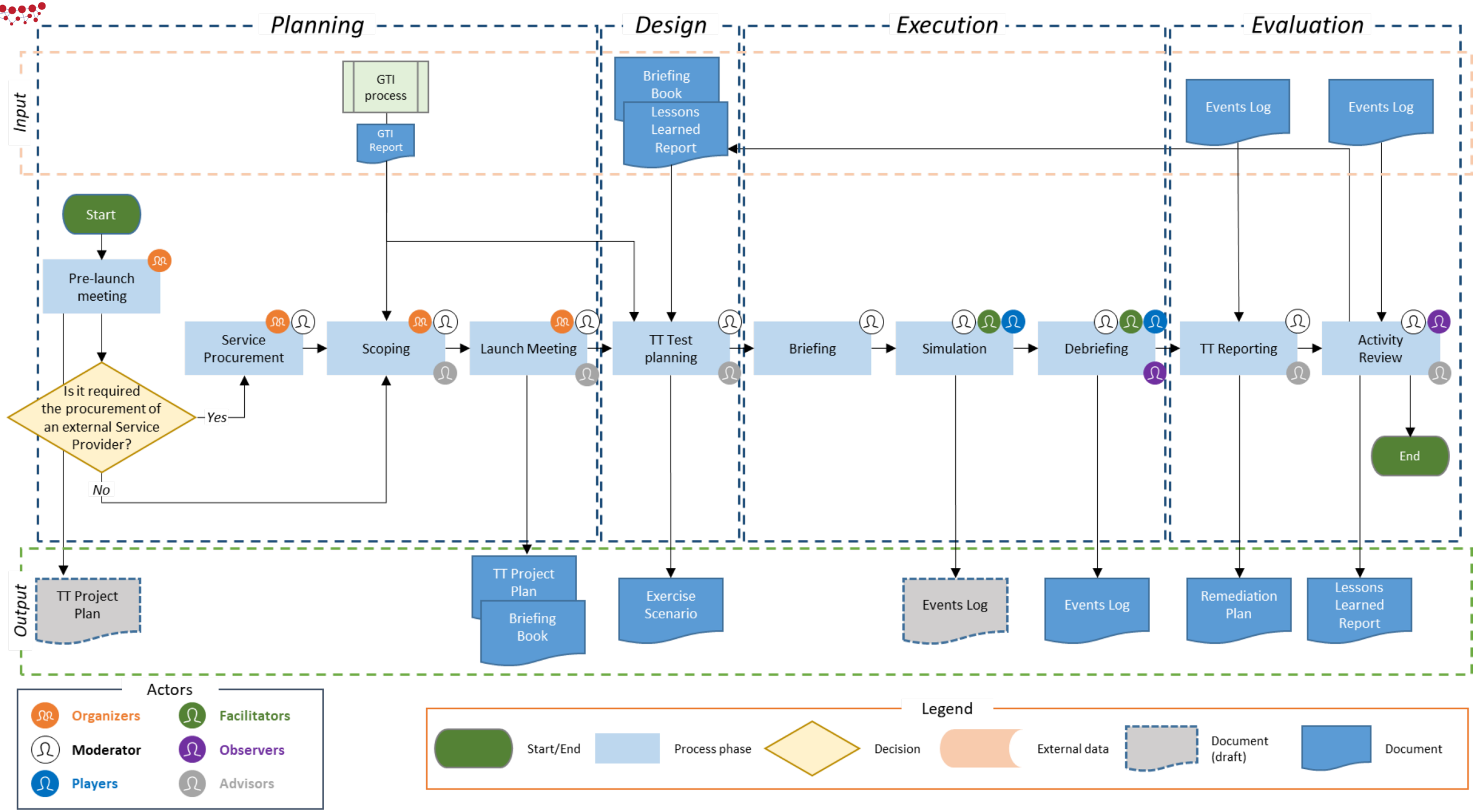
- *Briefing*
- *Simulation*
- *Debriefing*

Evaluation

- *TT Reporting*
- *Activity Review*

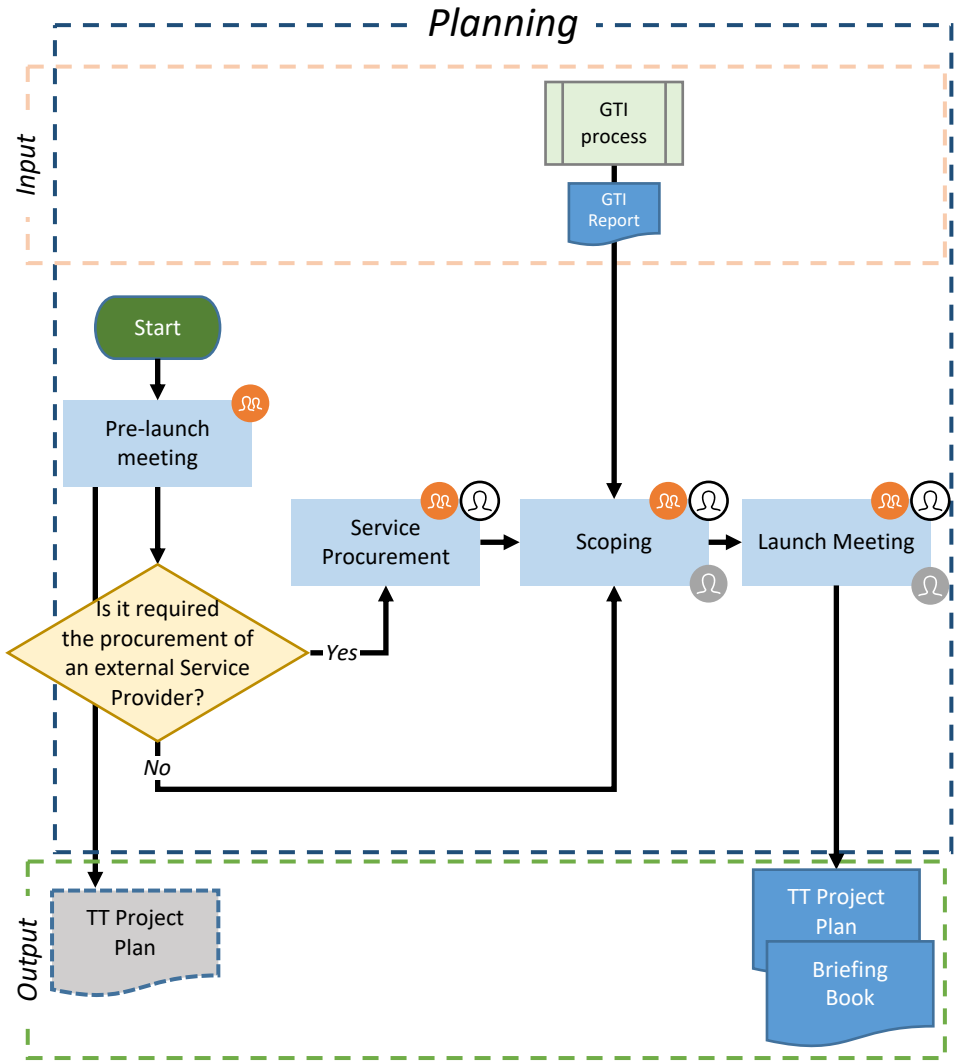
Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Il Workflow del Table-Top



Le fasi del Table Top: Planning

Planning | GTI | Design | Execution | Evaluation



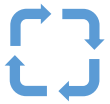
Pre-Launch meeting

- Definition of goals and objectives
- Identification of areas and processes that need to be tested
- Identification of Stakeholders
- Definition of roles and responsibilities of exercise players
- Preparation of an high-level Table-Top Project plan

Service Procurement

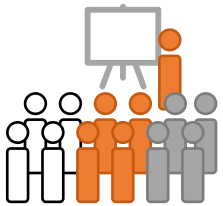
- Service Provider selection
- Setting contractual details
- Setting roles and responsibilities of the Service Provider within the exercise scope

Scoping



- Definition of the scope of the Table-Top

Launch meeting

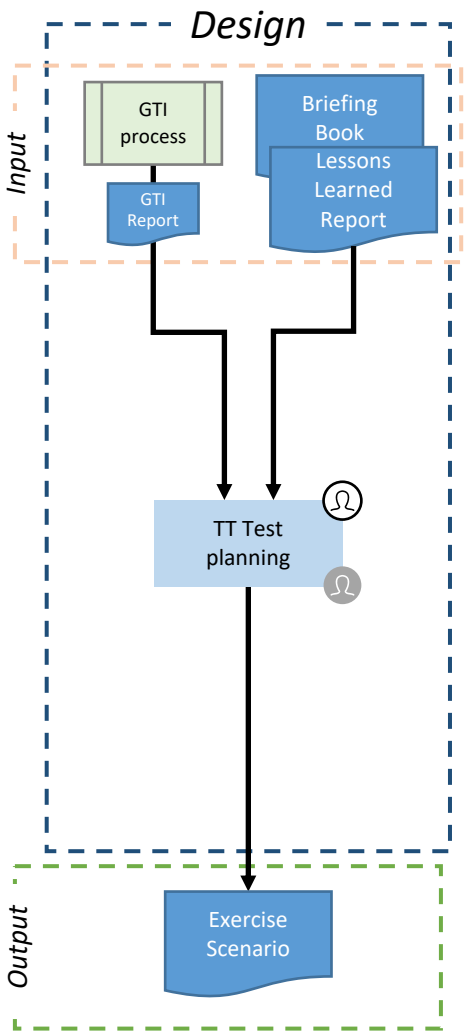


- Share the exercise operational project steps
- Share the organizational structure of the exercise (players, timing, etc.)
- Share the exercise outputs and expectations

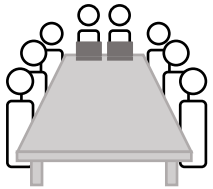
Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Le fasi del Table Top: Design

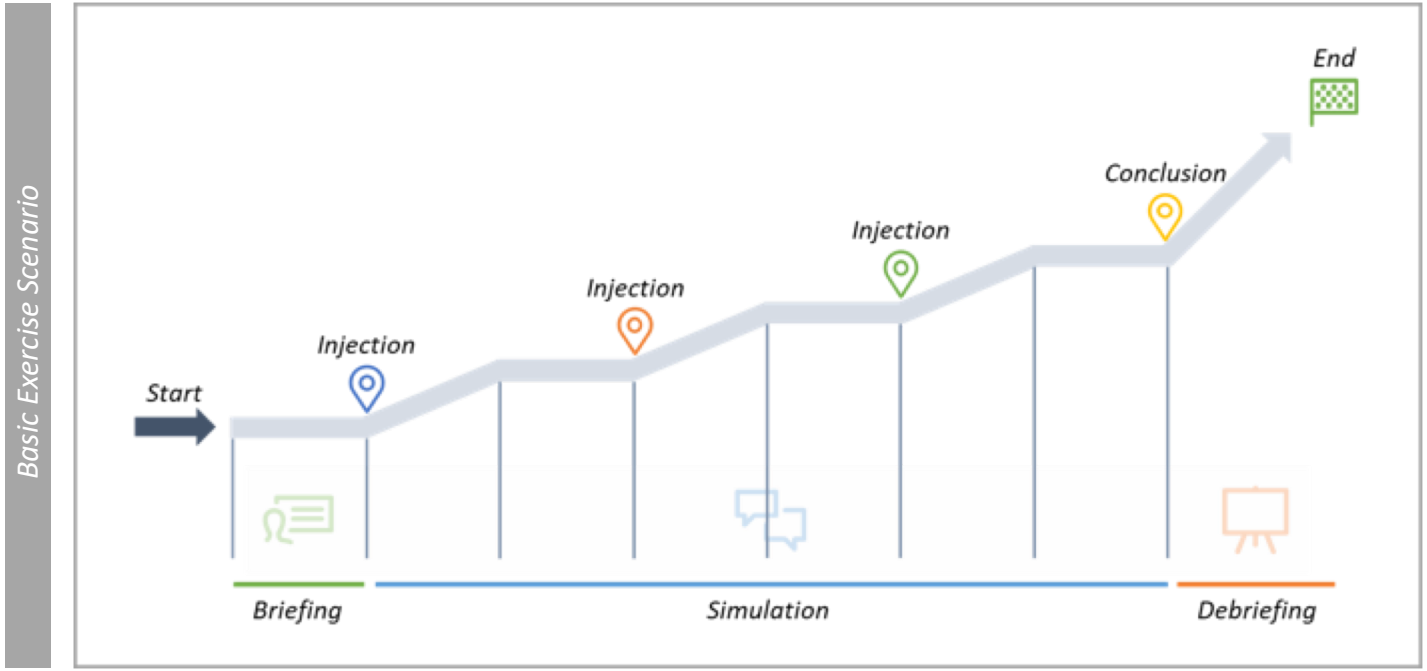
Planning | GTI | Design | Execution | Evaluation



TT Test Planning

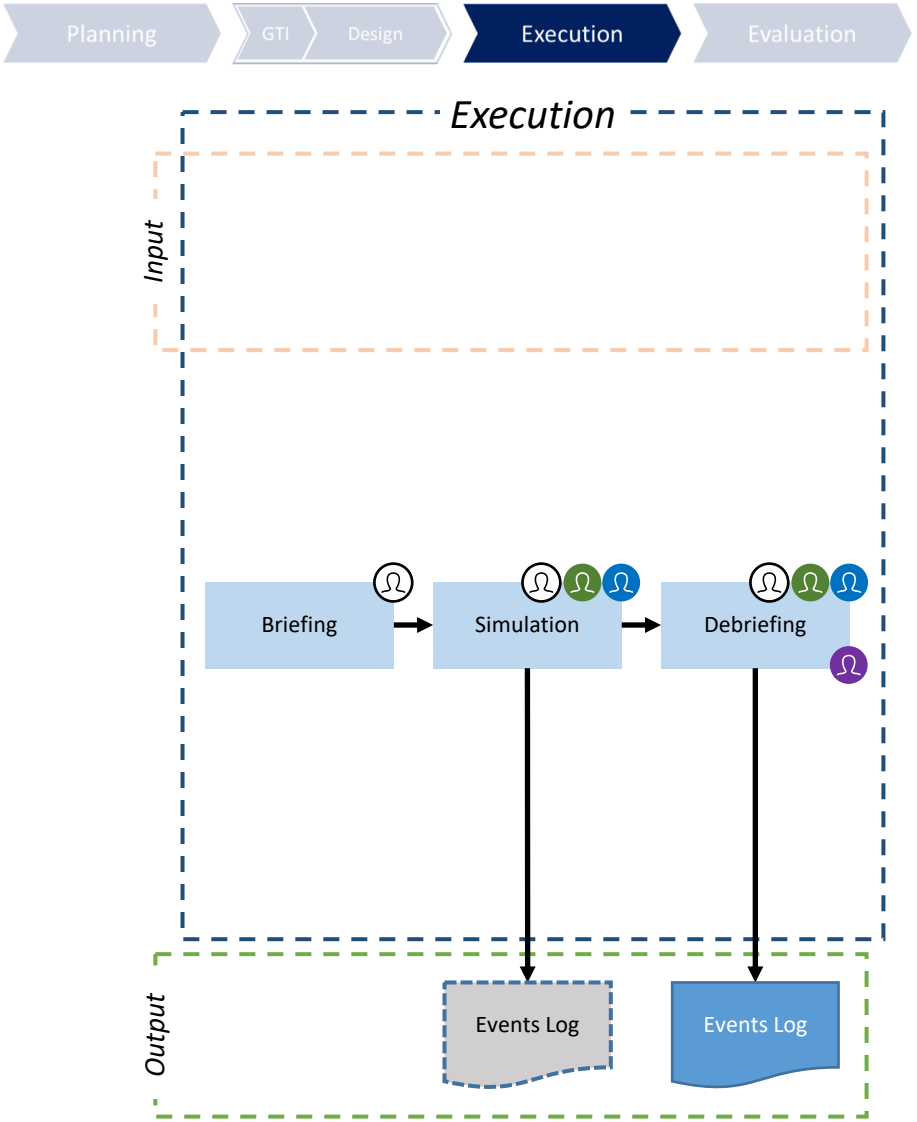


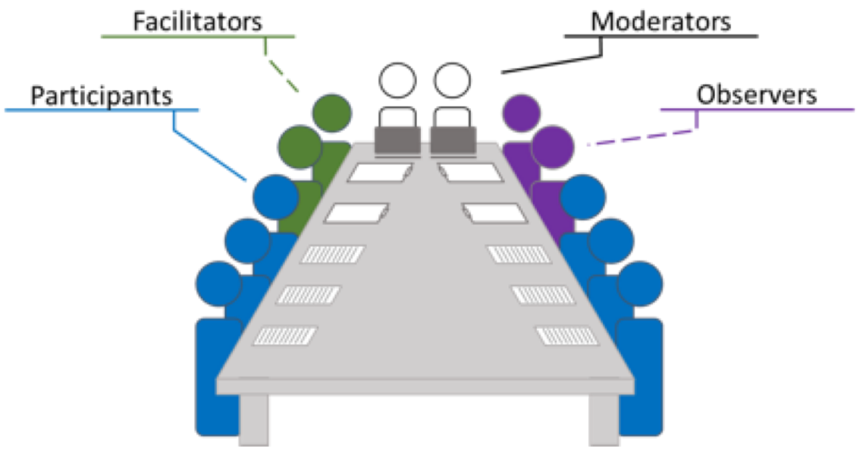
- Evaluate a relevant Threat Intelligence Scenario in order to contextualize exercise scenario to financial sector cyber-threats
- Set the rules of the exercise (e.g. execution methods, teams involved and related roles, communication methods, usable tools, etc.)
- Design the Exercise Scenario: **basic** and parametric



Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Le fasi del Table Top: Execution





a. Briefing

- Moderators present Table-Top scenario context, guidelines and rules to Participants

b. Simulation

- Moderators provide the injection plan (e.g. SOC alerts, news articles, etc.), monitor participants discussion and support the decision making process
- Participants respond to injections by practicing incident response processes

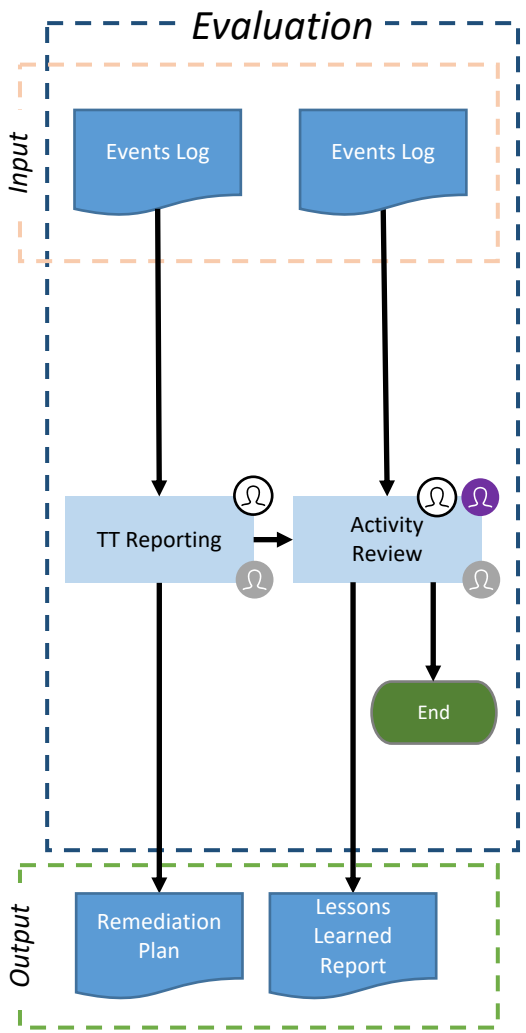
c. Debriefing

- Moderators review exercise, collect participant feedback
- Moderators draw-up the Events Log

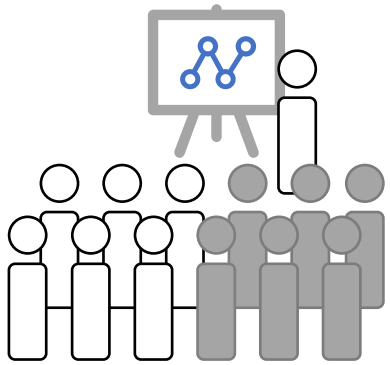
Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Le fasi del Table Top: Evaluation

Planning | GTI | Design | Execution | Evaluation

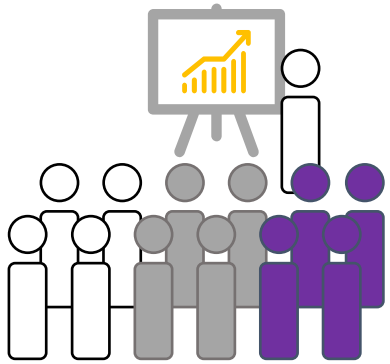


TT Reporting



- The Table-Top reporting activity is aimed at drawing up the Remediation Plan.

Activity Review



- The Activity Review is aimed at drawing up the Lessons Learned Report in order to evaluate specific areas of improvement of the Table-Top exercise, in term of the effectiveness of the organization of the teams and of the deisgned exercise scenario.

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

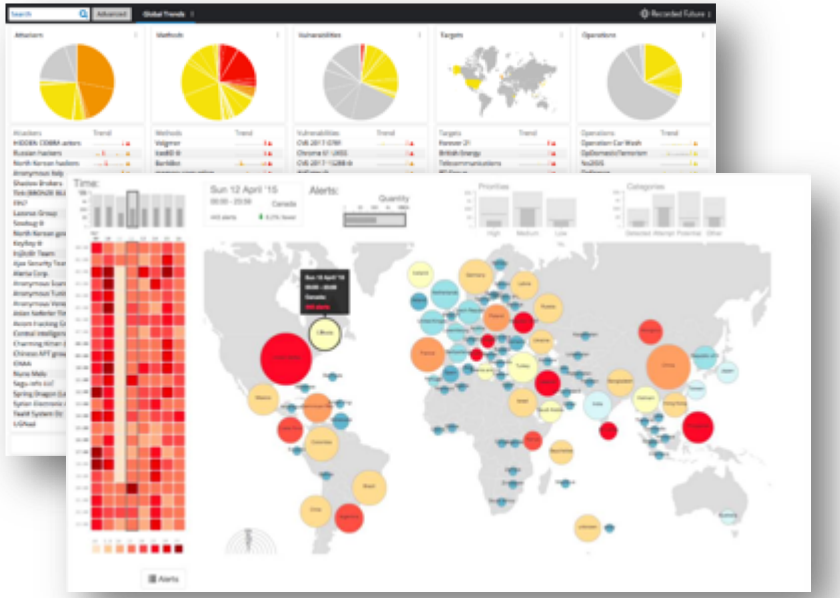
Generic Threat Intelligence – *an example*

1. Direction Planning

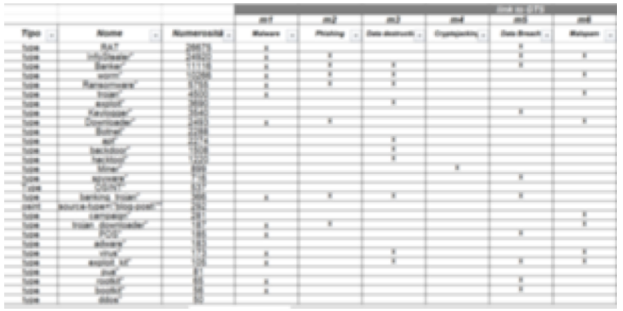
GTI Strategy

- **Obiettivi:**
  - ✓ Creare uno scenario per l'esercitazione di Table-Top;
  - ✓ Aumentare il livello di awareness del personale interno.
- **Strategia di raccolta:**
  - o *Fonti*:
  - ✓ Utilizzo fonti esterne (OSINT);
  - ✓ Utilizzo fonti interne (Report prodotti nell'ambito del progetto REDFin).
  - o *Modalità di raccolta:*
  - ✓ Manuale
- **Strategia di diffusione:**
  - ✓ CERTFin Costituency

2. Collection



3. Analysis & Processing

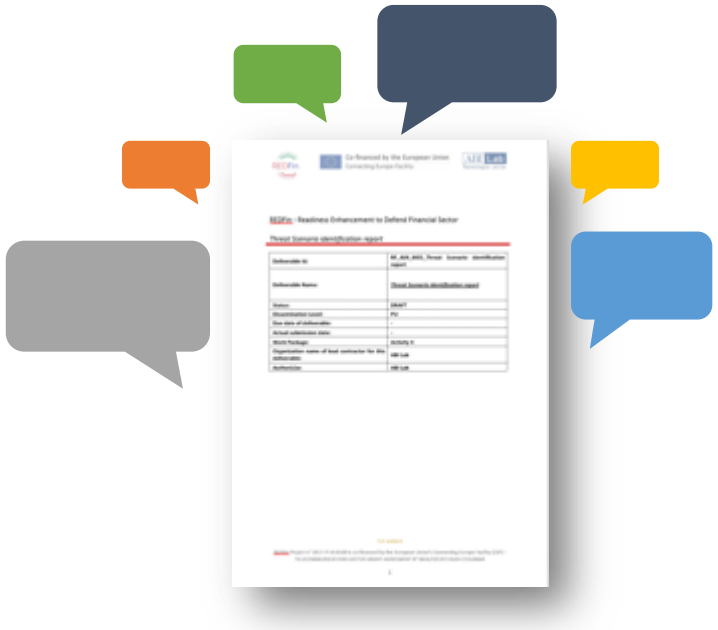


Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *an example*

4. Dissemination

5. Review



Generic Threat Scenario

Rappresentazione delle **principali minacce informatiche del settore finanziario a livello nazionale**, frutto dell'analisi condotta sugli eventi di minaccia, vulnerabilità finanziarie e dei principali trend di attacco.

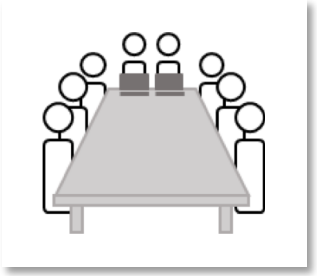
Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber exercise planning*

Generic Threat Scenario

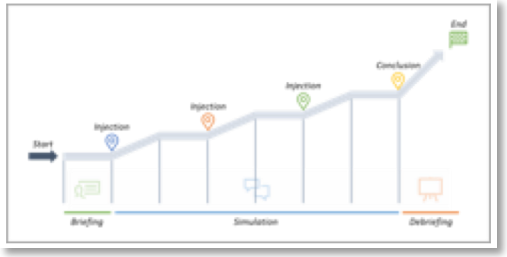
Generic Threat Scenario del settore finanziario nazionale

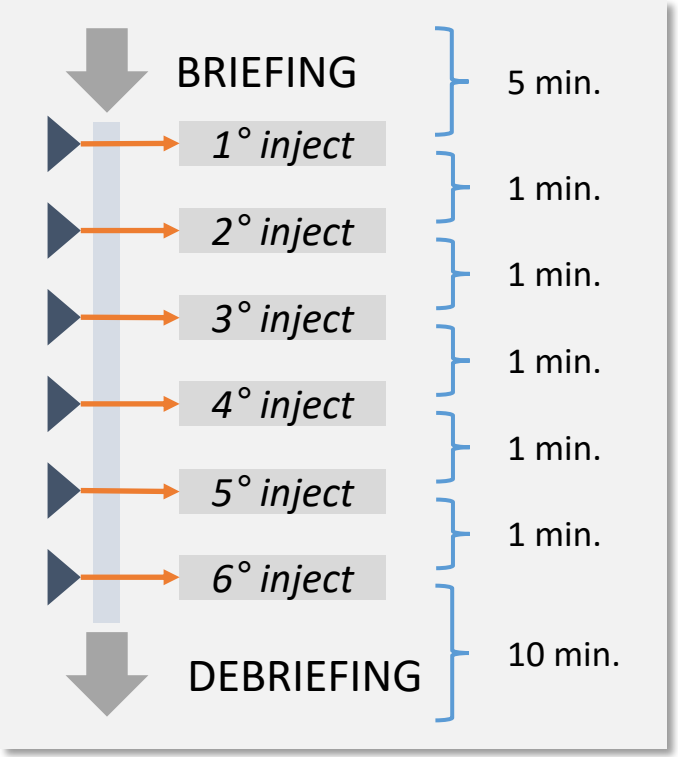
Design Phase



Scenario	Phishing
Strumenti Partecipazione	Piattaforma digitale utilizzabile dal proprio smartphone
Regole	• Saranno poste 6 domande a risposta chiusa • È possibile rispondere solo una volta a ciascuna domanda • Il tempo di risposta a ciascuna domanda è di 60 secondi • È possibile richiedere al moderatore delucidazioni in merito ai quesiti posti
Durata	• Briefing (5 min.) • Execution (5 min.) • Debriefing (10 min.)

Exercise Scenario





Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber simulation game*

OBIETTIVO

L'obiettivo del **Cyber Simulation Game** è quello di simulare l'occorrenza di uno **scenario di incidente informatico** per un **contesto finanziario** fittizio al fine di **valutare il livello di cyber awareness** nella gestione dell'incidente.

MODALITA' DI PARTECIPAZIONE

Il Cyber Simulation Game sarà effettuato in modalità **interattiva**, fornendo ai partecipanti un link ad una pagina web alla quale i partecipanti potranno collegarsi via laptop, smartphone o tablet e registrare un proprio pseudonimo da utilizzare per la partecipazione (n.b. **non sarà effettuata alcuna profilazione dei partecipanti**).

RISULTATI

Al termine della simulazione saranno forniti i **risultati in forma aggregata** dei principali **trend** di **risposta** dei partecipanti e discusse le **lessons learned.**

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber simulation game*

Per partecipare al **Cyber Simulation Game** accedere al link sottostante:

https://www.pollev.com/lrusso806

LET'S PLAY!

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Test Inject 0

Chi era l'artista incaricato di dirigere le fortificazioni di Firenze ?

(scegliere uno fra le tartarughe ninja)

- Michelangelo
- Donatello
- Leonardo
- Raffaello

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber simulation game*

Inject 1

Inject 2

Inject 3

Inject 4

Inject 5

Inject 6

Si riceve informazione che l'istituto ha ricevuto un’email sospetta contenente un link che rimanda ad una pagina web. Tale pagina contiene un disclaimer di un Gruppo denominato "BeenHacked" che dichiara di essere in possesso di diverse informazioni riservate sottratte, ed avanza una richiesta di riscatto per evitarne la pubblicazione sotto forma di pagamento in Bitcoin (10 bitcoin, pari a circa 85K€) entro 24 ore. Quali fra le azioni indicate si ritene opportuno effettuare ?

(scegliere una o più risposte)

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber simulation game*

Inject 1

Inject 2

Inject 3

Inject 4

Inject 5

Inject 6

A seguito di alcune analisi effettuate internamente è emerso che le informazioni sottratte sono relative ai nominativi dei clienti, e i numeri delle loro carte di pagamento. Quali fra le azioni indicate si ritiene opportuno effettuare?

(scegliere una o più risposte)

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber simulation game*

Inject 1

Inject 2

Inject 3

Inject 4

Inject 5

Inject 6

Nelle ore successive, la funzione "Pagamenti" notifica numerose transazioni di denaro in uscita, superiori ai € 10K ciascuno. Viene, inoltre, appurato che alcuni dei conti colpiti dal data breach sono oggetto di tali movimenti. Parte di questi conti risultano essere di proprietà di importanti top-clients (clienti corporate). Quale delle seguenti azioni si intende porre in essere ?

(scegliere una o più risposte)

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber simulation game*

Inject 1

Inject 2

Inject 3

Inject 4

Inject 5

Inject 6

Al seguito del breach occorso l'istituto rileva dei sensibili rallentamenti nel sistema dei pagamenti. In aggiunta si iniziano a ricevere comunicazioni di carattere urgente da altri istituti con cui collabora, nonchè da clienti e fornitori, in cui si evidenziano problematiche nell'esecuzione dei pagamenti.

Quale delle seguenti azioni l'istituto dovrebbe porre in essere al fine di gestire al meglio gli eventi descritti?

(scegliere una o più risposte)

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber simulation game*

Inject 1

Inject 2

Inject 3

Inject 4

Inject 5

Inject 6

Viene rilevata una notizia su un sito web di un quotidiano nazionale che riporta una violazione di dati personali e finanziari che avrebbe coinvolto la clientela dell'istituto. Contestualmente, i media pubblicano sulle proprie pagine web numerosi post provenienti da diversi social network in cui i clienti amplificano la notizia della violazione lamentando inoltre problemi di accesso ai servizi online e presenza di movimentazione sospetta sui propri conti correnti. Quali delle seguenti azioni l'istituto dovrebbe porre in essere al fine di gestire al meglio gli eventi descritti?

(scegliere una o più risposte)

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber simulation game*

Inject 1

Inject 2

Inject 3

Inject 4

Inject 5

Inject 6

Al seguito della gestione degli eventi descritti il Direttore dell'Ufficio Legale interno richiede di fornire evidenza della tipologia e numerosità di dati oggetto della violazione al fine di definirne la gestione da un punto di vista di Compliance. Quali delle seguenti azioni si ritiene opportuno porre in essere al fine di gestire al meglio le richieste pervenute?

(scegliere una o più risposte)

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Debriefing (1/6)

Inject 1	***A.*** Analisi di intelligence per verificare l'attendibilità del gruppo BeenHacked e delle informazioni pubblicate ***B.*** Indirizzo delle analisi tecniche di sicurezza sui sistemi potenzialmente coinvolti nell'evento al fine di determinarne la root cause e contenerla/mitigarla

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Debriefing (2/6)

Inject 2	**B**. Classificazione dell'evento **C**. Reporting verso l'Autorità Garante della Privacy

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Debriefing (3/6)

Inject 3	**C.** Nessun blocco sui pagamenti **F.** Monitoraggio dei destinatari delle transazioni e comunicazione alle forze dell'ordine ed autorità competenti

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Debriefing (4/6)

Inject 4

A. Comunicazione alla clientela del disservizio
B. Indirizzo delle analisi tecniche di sicurezza sui sistemi

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Debriefing (5/6)

Inject 5	**B.** Effettuazione di un comunicato stampa in cui si rassicura la clientela circa la gestione dell'evento e delle singole problematiche occorse. **C.** Comunicazione dell'evento all'ufficio Legale interno **D.** Comunicazione dell'evento all'ufficio Media & Communication interno

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Debriefing (6/6)

Inject 6	**A.** Invio del Registro dei Trattamenti (privacy) **D.** Invio del report dell'incidente di sicurezza occorso, redatto al termine della gestione degli eventi di sicurezza

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

Generic Threat Intelligence – *Cyber Game simulation*

LESSON LEARNED

Benefici di una simulazione Cyber:

- **Aumentare** la **capacità di risposta** agli attacchi cyber;
- **Aumentare** il livello complessivo di **cyber awareness**;
- **Migliorare le capacità di comunicazione** e coordinazione.

Saper correttamente **identificare gli scenari** e, per ciascuno di questi, **conoscere le azioni da intraprendere** (segnalazioni alle autorità, segnalazioni alla clientela, strategie di risposta, ecc.)

Saper correttamente **commisurare le azioni di risposta** agli **incidenti** in modo da consentire un bilanciamento tra:

- La sicurezza dei sistemi;
- L'erogazione continua dei servizi.

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669

REDFin

Co-financed by the European Union
Connecting Europe Facility

ABI Lab

IL SALONE DEI PAGAMENTI
PAYVOLUTION

The sole responsibility of this publication lies with the author. The European Union and the Agency (INEA) are not responsible for any use that may be made of the information contained therein.

Project REDFin n° 2017-IT-IA-0100 is co-financed by the European Union's Connecting Europe Facility. GA N° INEA/CEF/ICT/A2017/1528669