
# PROTECTION DES INFRASTRUCTURES ET IMPLÉMENTATION DE TIBER-EU

EIFR – Cybersécurité, quelles protections pour les établissements financiers ?

*Samuel Janin – Senior Manager – Technology & Digital Services – 5 juillet 2019*

# L'INFRASTRUCTURE IT AU CŒUR DE L'INFRASTRUCTURE DE MARCHE ET DU SECTEUR FINANCIER : UN RISQUE SYSTÉMIQUE ET UNE RESPONSABILITÉ PARTAGÉE

*« Nous devons traiter les cyberattaques comme un risque systémique »* car le secteur financier, *« est connecté à tous les secteurs de l'économie »*

*Bruno Le Maire*

### Legacy

Infrastructures hébergées (data centers)

Informatique de Caisses et d'Agences / Traitements Front, Middle et Back Office

DAB

### Digitalisation

Banques et services en ligne

Fintech / APIsation

Automatisation / IA

Data Lakes

Hébergements Cloud

### Opérateurs clés

Systèmes de paiement

Messagerie SWIFT

Chambres de compensation

Marchés régulés

Référentiels sectoriels

### Internet

Place publique

Media principal d'échange et de communication

# LES AXES DE PROTECTION DES INFRASTRUCTURES SONT MATURES, LA PRINCIPALE DIFFICULTÉ RÉSIDE DANS UNE FORME DE « VOLATILITÉ » DES SOLUTIONS FACE AUX RISQUES, AINSI QUE DANS LEUR DÉPLOIEMENT EFFECTIF

### Continuité de services

Complémenter les mécanismes de reprise et de continuité liés à une défaillance d'infrastructure (matérielle ou logicielle) à une continuité de services en cas d'invasion virale

### Détection et surveillance

Intégrer les mécanismes d'IA pour palier aux limites de la détection uniquement des « infractions » et bénéficier des outils de surveillance orientés « Threat Intelligence »

### Sécurité périmétrique

Au-delà de la mise en œuvre de SAS de firewalls et d'IDS, identifier comment les services maintenus ouverts peuvent ou non être exploités

### Cloisonnement

A mesure que l'ouverture des services et l'interconnectivité « de tout » s'accélère, repenser les architectures pour créer de réels espaces de confinement entres infrastructures, entre les données et entre métiers

### Défense en profondeur

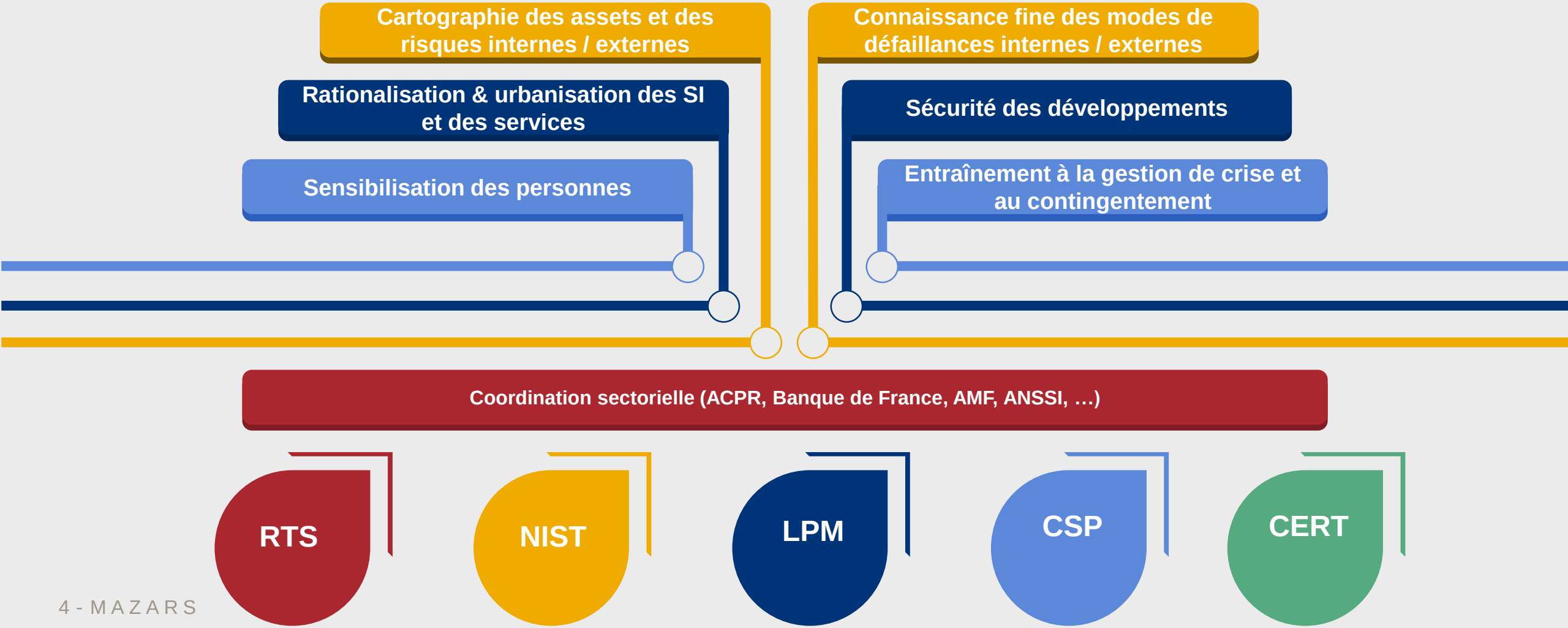
Combiner l'arsenal des défenses connues et éprouvées (protection endpoint & hardening système) avec un dispositif effectif de gestion des vulnérabilités

### Gestion des identités & des accès

Etendre l'interopérabilité des annuaires pour mieux gérer les contextes de sécurité en environnements ouverts, intégrer les contrôles d'accès aux données non structurées et gérer les accès avec privilèges

# DES BONNES PRATIQUES ESSENTIELLES POUR COMPLÉTER L'APPROCHE « INFRA »

*« La cybersécurité semble être une problématique technique. En réalité, elle est politique »*
*Bruno Le Maire*



# DES CAS CONCRETS…

Découvert en 2010 mais en développement **depuis 2006**, Stuxnet est un virus informatique ciblant les systèmes industriels ayant notamment causé de gros dégâts au programme nucléaire iranien.
Bien que non revendiqué, il a probablement été développé conjointement par les **Etats-Unis et Israel** (Unit 8200). Utilisant **4 failles zero-day**, son coût de développement est estimé à **plusieurs millions de dollars**.
Se transmettant par clef USB, il contourne les « air-gap », scanne le système à la recherche de Siemens Step7 contrôlant un PLC, et reste en sommeil si ce n'est pas le cas. Sinon, il renvoie en boucle à l'IHM les données issues des capteurs, et modifie le comportement du PLC.

STUXnet *SPECIFIQUE*

**2010**

En février 2016, 35 ordres de paiement sont envoyés par des hackers via le réseau SWIFT pour un montant de $951 millions depuis les comptes de la CBB à la Federal Reserve Bank of New York vers des comptes privés. $101 millions furent transférés dont **18 qui n'ont pas pu être récupérés**.

Le malware Dridex (spécialisé dans le vol d'informations bancaires, s'installant via une **macro Word**) aurait été utilisé dans cette attaque.
Les attaquants on pu s'infiltrer sur le réseau en janvier, et **observer pendant un mois** les procédures par lesquelles les virements sont faits. Un jour de clôture de la banque, ils émettent leurs propres ordres en **imitant ces procédures**.
Une faute d'orthographe dans un destinataire, « Fundation » au lieu de « Foundation » alertera les autorités qui arrêterons les virements non effectués.

BANGLADESH BANK *DISCOVERY*
Central Bank of Bangladesh

**2016**

**2015**

*UNIFIED KILL CHAIN* TV5MONDE

Les 8 et 9 avril 2015, une attaque **coupe la diffusion** des programmes, **détruit le serveur mail** et diffuse des messages de soutien à l'Etat Islamique sur les réseaux sociaux. Se faisant passer pour le groupe « Cybercaliphate », ce serait en fait le groupe de hackers russes **APT28** (ou Pawn Storm) soutenu par le gouvernement.

L'enquête menée par l'ANSSI démontrera que l'attaque, menée par **plusieurs dizaines de personnes**, a débuté par du **phishing fin janvier** auquel 3 employés ont répondu, permettant **l'installation d'un cheval de Troie**. 3 semaines avant l'attaque, un **malware se diffuse** sur les réseau profitant de lien entre réseau interne « métier » et le réseau « bureautique » ouvert sur l'extérieur. Les pirates ont ensuite **créé des comptes administrateurs** leur permettant de circuler et faire ce qu'ils voulaient sur le réseau.

**2018**

*SOCIAL ENGINEERING* PATHÉ

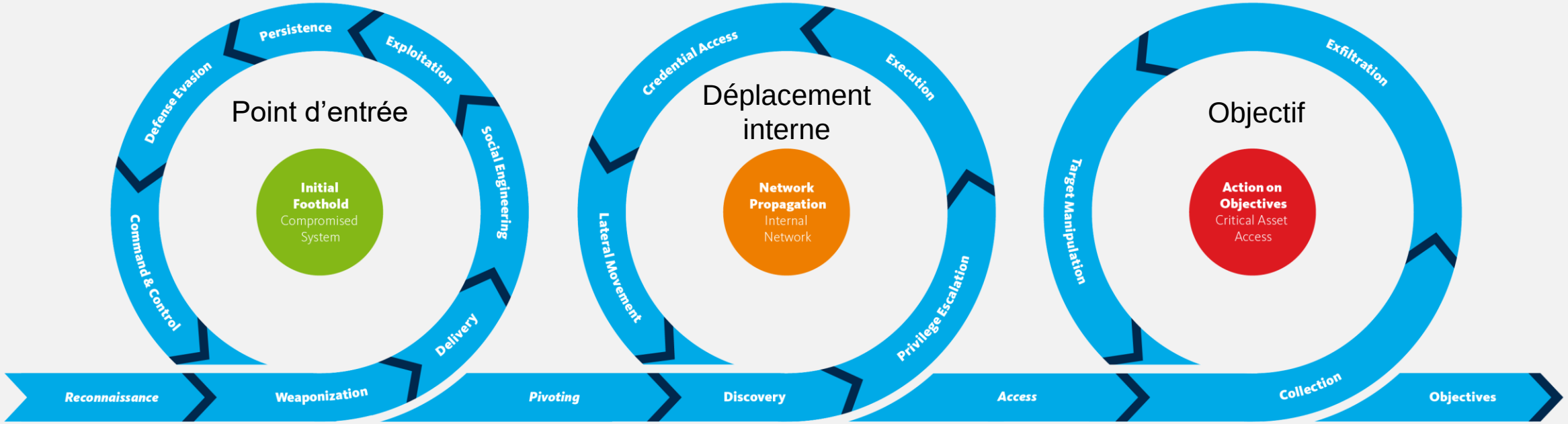
En mars 2018, il aura suffit d'une **bonne communication** bien préparée et d'une **fausse adresse mail** pour que deux dirigeants de la filiale néerlandaise du groupe Pathé opèrent des virements pour un montant de **19 millions d'euros** sur un compte possédé par les attaquants. Pour ce faire, les attaquants se sont fait passer pour des dirigeant groupe et ont prétexté une acquisition à Dubaï.
Ce type de **fraude au président** nécessité une connaissance très poussée de l'organisation de l'entreprise, de ses employés et de la communication interne pour réussir.
NB : On retrouve les phases de **reconnaissance** et **social engineering** de la Unified Kill Chain.



Cliquez sur les logos pour plus de détails

# LE MODÈLE « UNIFIED KILL-CHAIN » PERMET DE COMPRENDRE LES MODES DE DÉFAILLANCE D'UN SYSTÈME : EXPLOITÉ PAR UNE ÉQUIPE DE HACKERS ÉTHIQUES (RED TEAM) IL PERMET DE TESTER LE SYSTÈME

Déroulement d'une cyber-attaque : Vision combinant la Cyber Kill Chain de Lockheed Martin et l'ATT&CK Framework de MITRE




(1)

1 – **Reconnaissance** : découverte de la cible, points d'accès, vulnérabilités apparentes, …
2 – **Weaponization** : développement des outils d'attaque spécifiques aux vulnérabilités identifiées
3 – **Delivery** : Transmission du malware à la cible (spear phishing par exemple) en plusieurs étapes
4 – **Social Engineering** : Manipulation des employés
5 – **Exploitation** : Activation du malware et prise de contrôle de la machine cible
6 – **Persistence** : Mise en place d'accès à long terme (backdoor, création de compte,…)

7 – **Defense Evasion** : Contournement des mécanismes de détection et de défense (Antivirus, puis IPS, IDS, pare-feu,…)
8 – **Command & Control** : Mise en place des outils de communication et de contrôle de la machine compromise pour explorer et attaquer le réseau interne.
9 – **Pivoting** : Utilisation de la machine compromise comme nouvelle machine d'attaque du réseau interne.
10 – **Discovery** : Découverte du réseau accessible depuis la nouvelle machine, ciblage et attaque de nouvelles machines.
11 – **Privilege Escalation** : Augmentation de privilège sur le réseau.
12 – **Execution** : Attaque de la nouvelle machine ciblée

13 – **Credential Access** : Prise de contrôle d'identifiants, de mots de passe (lecture, modification, dump de hash)
14 – **Lateral Movement** : Prise de contrôle d'une autre machine sur le réseau.
15 – **Collection** : Identification et rassemblement des informations ciblées
16 – **Exfiltration** : Extraction des données collectées
17 – **Target Manipulation** : Manipulation du système cible pour atteindre les objectifs (crash, prise de contrôle, …)
18 – **Objectives** : Objectifs atteints

(1) Unified KC : La Kill Chain selon Paul Pols

# DÉFINITION / PRINCIPES

**Red Teaming :** simuler de manière **réaliste** une **attaque ciblée** contre une organisation afin d'évaluer son **niveau de sécurité global**.

Elle peut avoir pour objectif:

- L'évaluation de l'ensemble des **vulnérabilités** (humaines, procédurales, technologiques, informatiques, …)
  - ➢ Très **peu de personnes** au sein de l'organisation ciblée doivent être au courant de cette mission.
- L'évaluation des performances de la **Blue Team** (équipe en charge de protéger l'organisation contre les attaques cyber. Voir exercice OTAN Lock Shield)

Pour cela, un **cadre** est défini au sein duquel la Red Team est libre de ses actions pour atteindre un objectif de sécurité (ex: atteindre un disjoncteur dans un datacenter, récupérer un fichier sur un réseau interne, …)

## PENTEST

L'objectif des tests d'intrusion est de tester le niveau de sécurité du **système informatique** de l'entreprise uniquement, et se concentre donc sur les vulnérabilités informatiques « techniques ».

VS

## RED TEAMING

Il s'agit d'une **évaluation globale** du niveau de sécurité de l'entreprise, puisqu'elle inclut les vecteurs d'attaque, et donc l'évaluation des vulnérabilités suivants :

- **Social engineering** (OSINT, appels téléphoniques, rendez-vous,…)
- **Penetration testing** (Externes éventuellement mais surtout internes)
- **Physical intrusion**

*- Pentests et RedTeam ne s'opposent pas, **l'un ne remplace pas l'autre**.*
*- Il faut voir la RedTeam comme une **extension** des pentests à un périmètre plus large, permettant d'avoir une image plus fidèle du niveau de sécurité global de l'entreprise.*
*- La RedTeam s'adresse donc aux organisations ayant déjà une « **culture cybersécurité** » bien ancrée.*

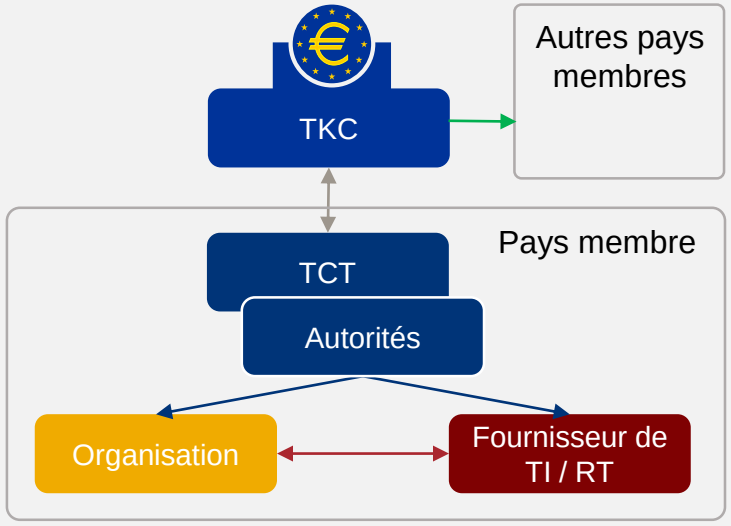
# FOCUS SUR TIBER-EU (THREAT INTELLIGENCE-BASED ETHICAL RED TEAMING)

**Framework** lancé par la Banque Centrale Européenne destiné à faciliter la mise en place de **programmes de tests Red Team** et promouvoir l'amélioration de la **résilience** des **institutions et infrastructures financières** en cas d'attaque cyber **sophistiquée**.

***OBJECTIFS***

- **Améliorer la résilience** des entités financières et du secteur en général
- Standardiser et **harmoniser les tests Red Team** en Europe avant que des frameworks incompatibles n'émergent
- **Fournir des orientations** sur la manière dont les entreprises peuvent planifier, exécuter et gérer ces test au niveau national ou européen
- **Centraliser et analyser** les résultats de tests pour **partager** les conclusions aux entreprises du secteur concernées (géré par TIBER-EU Knowledge Center : **TKC**)
- Permettre aux multinationales d'opérer des tests Red Team **au-delà des frontières** internes à l'UE
- permettre une **reconnaissance** des tests effectués via ce Framework au niveau européen

**NB :** - TIBER-EU se veut facilement adaptable à des entreprises **plus petites** ou **hors du secteur financier**
- TIBER-EU nécessite que les tests Red Team soient **conduits par des entités extérieures** à l'organisation ciblée



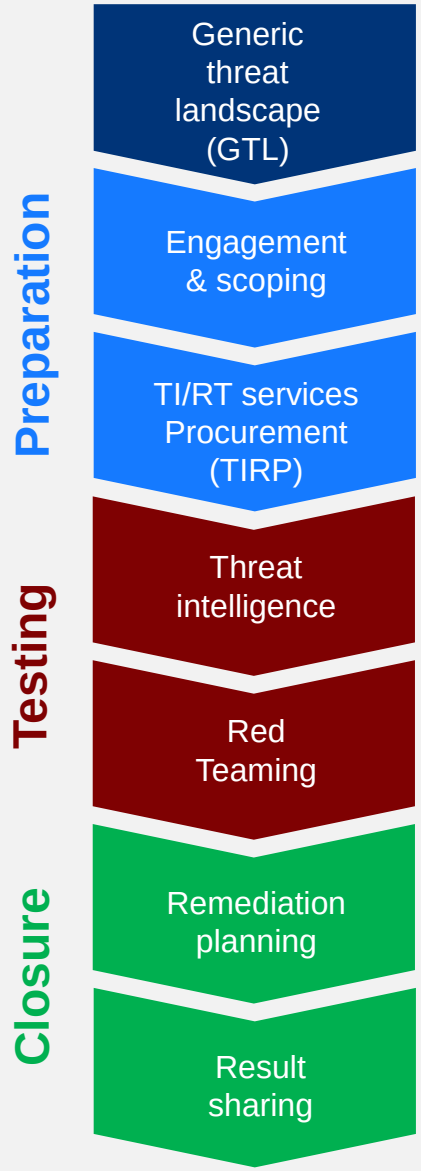

**Les acteurs :**

- L'**organisation** : responsable de la gestion des risques, du cadrage et de la préparation des tests du début à la fin pour faciliter leur déroulement
- Les **autorités nationales** : supervisent les tests et s'assurent qu'ils respectent bien le Framework TIBER-EU
- Le **fournisseur de TI/RT** : conduit les Tests d'Intrusion et Red Team

Il se décline dans chaque pays sous la forme de TIBER-XX (XX pour NL,BE,FR,…) lorsque les états membres décident de l'implémenter localement (**TIBER-NL** existe déjà, BE et DK sont en cours…).

➢ **L'initiative doit donc venir de chaque pays**, et passe par la création d'une TIBER Cyber Team (**TCT**) qui adapte TIBER-EU, fait l'interface entre l'Europe et les autorités nationales et leur apporte du support.

# LE FRAMEWORK EN DÉTAIL ….




## *LE PROCESS TIBER-EU*

Phase GTL (**facultative**) : évaluation des menaces et identification des acteurs menaçants du secteur en les liant à leurs TTPs (Tactics, Technics and Procedures) afin de les reproduire dans les phases suivantes.

**Phase de préparation** (**obligatoire**) : Lancement formel des tests TIBER-EU, établissement des rôles et responsabilités des équipes et des organisations (supervision, fournisseur de service, white team,…), définition du périmètre, etc.

**Phase de tests** (**obligatoire**) : Production d'un Targeted Threat Intelligence Report (scénarios de menaces utilisés lors du test, infos utiles,…) puis exécution des test Red Team sur les systèmes et les personnes pour cibler les Critical Functions (CFs) de l'organisation cible.

**Phase de clôture** (**obligatoire**) : Rapport sur les résultats des tests incluant des conseils techniques ou procéduraux, planning pour remédier aux vulnérabilités identifiées, partage des résultats avec les autorités compétentes et clôture du projet.

## *ROLES ET RESPONSABILITES*

**Parties prenantes :**

- **TCT** et Team Test Manager (**TTM**) : la TCT supervise et l'un de ses membres, le TTM, qui s'assure que les tests soient menés en accord avec le Framework TIBER-EU.
- **WT** et **WTL** (White Team Leader) : Les équipes de l'organisation cible qui ont connaissance des tests et qui les coordonnent en lien avec le TTM et les fournisseurs de TI / RT
- **Blue Team** (BT) : Exclue de la préparation des tests, n'intervient qu'en clôture éventuellement.
- Fournisseurs de services **TI / RT** : Réalisent les tests
- Agences de renseignement gouvernementales ou autorités nationales en cybersécurité éventuellement

## *RISK MANAGEMENT*

La conduite de tests Red Team implique nécessairement des risques de

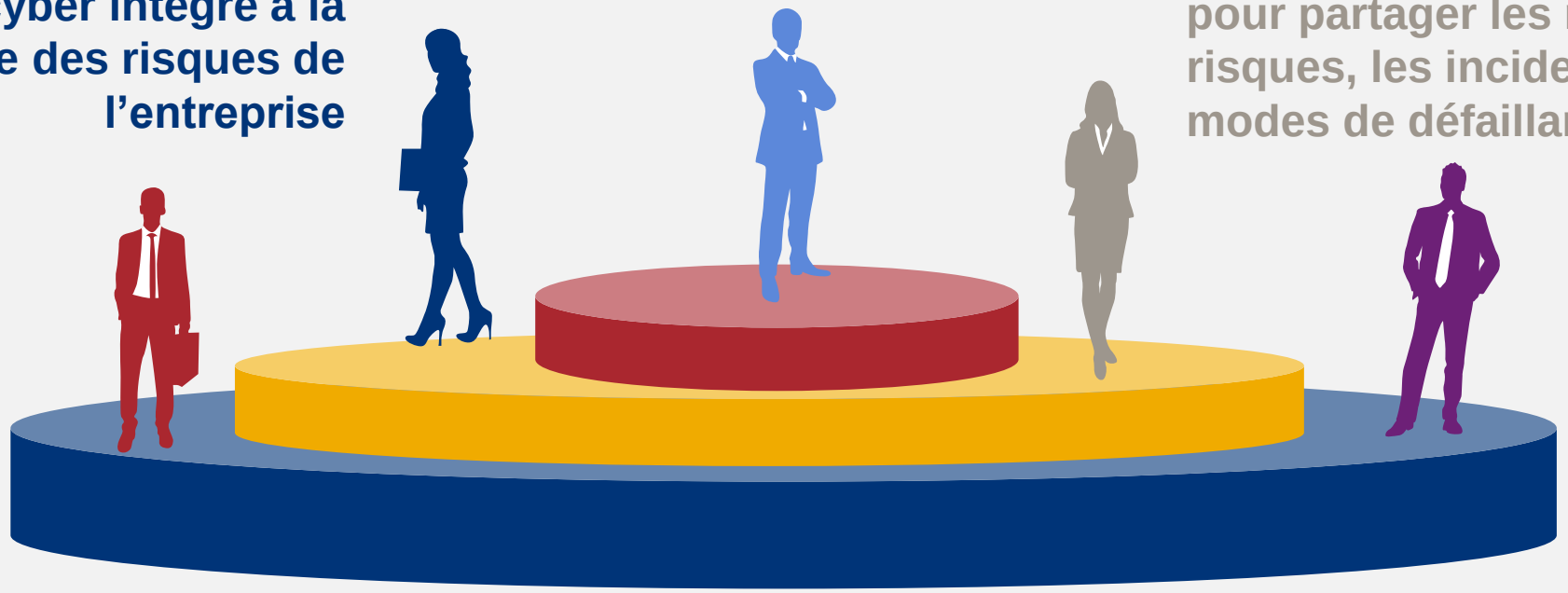
- déni-de-service
- crash système
- dommages sur des environnements de production
- perte ou modification de données…

Pour ces raisons, l'entreprise doit s'assurer d'identifier et évaluer ces risques pour permettre la conduite des tests de manière aussi sûre que possible.

# NOTRE VISION D'UNE CYBERSÉCURITÉ RÉUSSIE

**Un risque cyber intégré à la gouvernance des risques de l'entreprise**

**Une coopération sectorielle pour partager les modèles de risques, les incidents et les modes de défaillance connus**

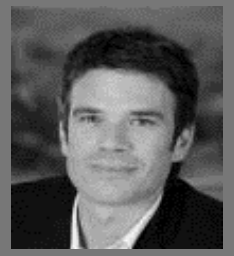


**Un SI maîtrisé et urbanisé et des ressources dédiées à une connaissance fine des modes de défaillance les plus complexes, à risque et/ou émergents**

**Des équipes régulièrement formées à la gestion de crise et sensibilisées aux gestes simples et essentiels d'hygiène informatique**

**Un système de surveillance efficace et complet du Build et du Run**

# CONTACT



**Samuel Janin**

Senior Manager

(P) +337.69.55.13.67

(E) samuel.janin@mazars.fr

Visit us at: www.mazars.fr

**Follow us on:**