Formation BTS CIEL A

La méthode EBIOS Risk Manager

Expression des Besoins et Identification des Objectifs de Sécurité

C04	ANALYSER UN SYSTÈME INFORMATIQUE	U4
S4.4	Méthodologies d'analyse de risque (EBIOS , ISO27005)	Niveau 2 expression

Ressources :

- Formation EBIOS-RM proposée par l'ENSIBS
  Présentation effectuée par Julien BREYAULT, enseignant en cyberdéfense à l'ENSIBS – Membre du club EBIOS
- Support de formation (2019), guide et méthode ANSSI (cyber.gouv)
- Support de formation V.2.04 (mai 2024), guide et méthode ANSSI (cyber.gouv)
- Livret stagiaire Formation EBIOS RM
- Livre BTS SIO bloc 3 Cybersécurité des systèmes informatiques –
- La norme ISO 27005 – Gestion des risques liés à la sécurité de l'information - Jean-Charles Pons ENI – magistère
- Cyber-résilience en entreprise – Sébastien DEON – chapitre 5 EBIOS 210

Sitographie

- https://www-ensibs.univ-ubs.fr/fr/formations/formations/formation-courte-non-diplomante-ZO/sciences-technologies-sante-STS/ebios-rm-mise-en-pratique-de-la-methode-et-des-outils-KN02TEHL.html
- https://cyber.gouv.fr/la-methode-ebios-risk-manager
- https://club-ebios.org/site/productions/
- https://club-ebios.org/site/faq/
- https://www.all4tec.com/logiciel-ebios-risk-manager-labellise-agile-risk-manager/

1. Définition :

Elle permet de déterminer les mesures de sécurité adaptées à la menace et de mettre en place le cadre de suivi et d'amélioration continue à l'issue d'une analyse de risque partagée au plus haut niveau.

Historique :

1995 Développée par la DCSSI Direction centrale de la sécurité des systèmes d'information

2009 DCSSI -> ANSSI

2010 EBIOS v3 ou EBIOS 2010

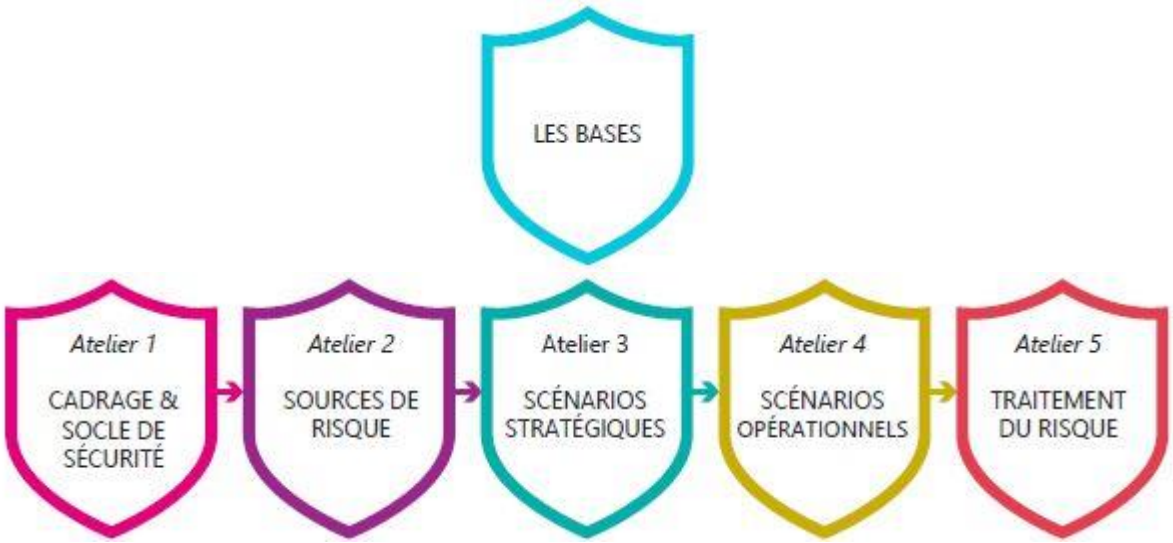
2018 Mise à jour

2019 Publication

2022 passage de EBIOS 2010 à EBIOS Risk Manager est conforme à la norme ISO 27005 (grandes lignes d'une gestion des risques autour des métiers , de la cybersécurité et de la protection de la vie privée)

2. Présentation du support fourni par Julien Breyault – ENSIBS

Objectif métier : réaliser une analyse de risque avec la méthode EBIOS-RM de l'ANSSI



- Les bases
  - Qu'est-ce qu'un risque ?
  - Quelle est la gravité de ce risque ?
  - Quelle est la vraisemblance de ce risque ?
  - Comment évaluer le niveau d'un risque ?
  - Carte d'identité de la méthode EBIOS RM
  - La pyramide du management du risque
  - EBIOS RM : une méthode basée sur 5 ateliers

- Les 5 ateliers
  - Le vocabulaire
  - Atelier 1 : cadrage et socle de sécurité
  - Atelier 2 : sources de risque
  - Atelier 3 : scénarios stratégiques
  - Atelier 4 : scénarios opérationnels
  - Atelier 5 : traitement du risque

3. Déroulement de la présentation (Prise de notes) :

Sensibiliser les étudiants

Possibilité qu'un événement redouté survienne et que ses effets perturbent les missions de l'objet de l'étude ?

Exemple : La voiture percute l'arbre (page 4 …)
Objet de l'étude : la voiture
Mission : arriver à destination (cela dépend de la mission , notion **de valeur**)
Gravité : vitesse de la voiture – taille de l'arbre - prix robustesse

La gravité varie selon le nombre d'impacts.

Notions de :
- Mesure de sécurité
- Menaces , vulnérabilité, mesure de sécurité
- Gravité, vraisemblance

Les échelles sont définies par l'organisation

Exemple : Société de biotechnologies fabriquant des vaccins

Scénarios de risques

R1 :Un concurrent vole des informations de R&D grâce à un canal d'exfiltration direct
R2 :Un concurrent vole des informations de R&D en exfiltrant celles détenues par le laboratoire
R3 :Un concurrent vole des informations de R&D grâce à un canal d'exfiltration via le prestataire informatique
R4 :Un activiste provoque un arrêt de la production des vaccins en compromettant l'équipement de maintenance du fournisseur de matériel
R5 :Un activiste perturbe la distribution de vaccins en modifiant leur étiquetage

R : Risque

Éléments utiles :

Valeur métier	gravité
Menaces considérées	vraisemblances
Existences de vulnérabilités	vraisemblances
Exploitation de vulnérabilité	vraisemblances
Sources de risques	vraisemblances
impacts	gravité

Questions à se poser :

- Risques qui pèsent sur mon SI
- Exposition à ces risques
- Maîtrise des risques
- Risques dans le temps

Qui a la charge de l'application de la méthode ?

Risk manager , RSSI , chef de projet

Vision : compréhension partagée des risques

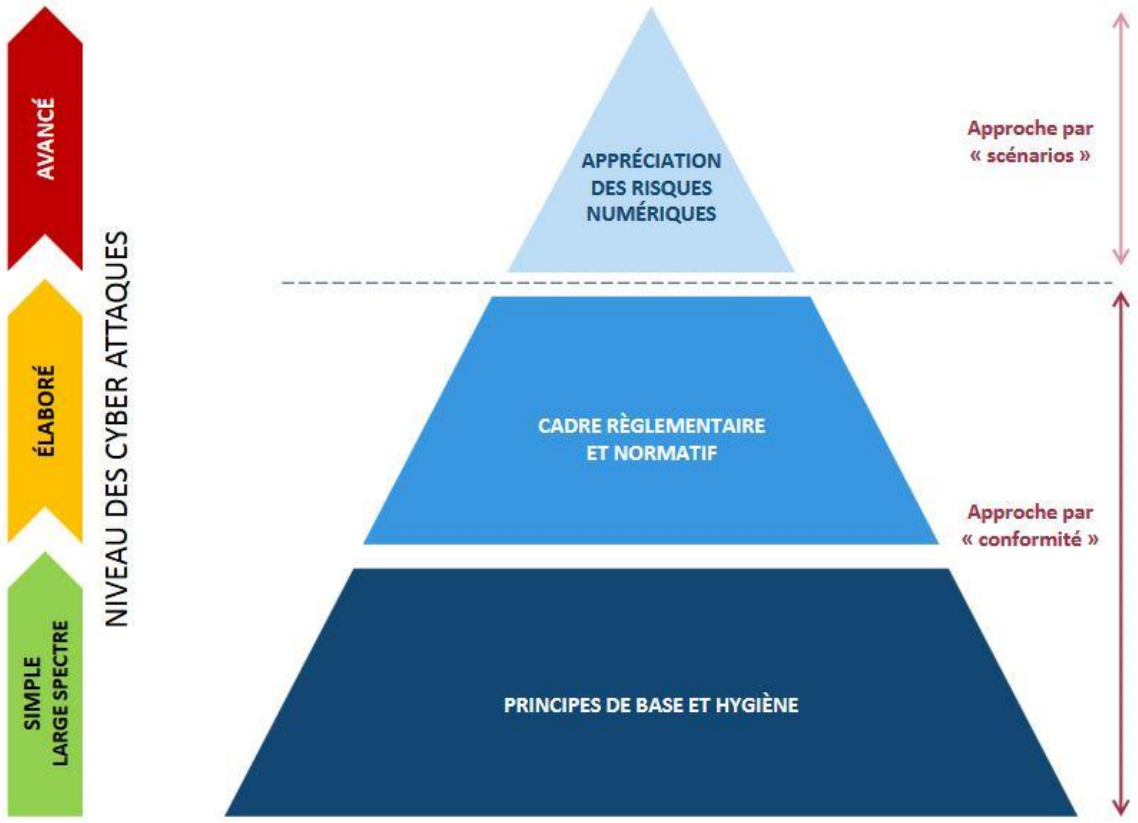
Fondamentaux : (p 24 – support de formation)

Conformité – scénarios

Point de vue SI / attaque

Ateliers / efficacité

Valeurs : concrète , efficace convaincante et collaborative



(guide ANSSI Page 5)
En premier , les 42 règles du guide ANSSI PME (standards)
En second , les normes entreprises bancaires contexte métiers (normatif et réglementaire)
En troisième , les scénarios -> qui ? comment ? (veille cybermenace – guides techniques)

<u>Les ateliers</u>
1 : normes (standards) et sociétés (le + long)
2 : sources
3 : stratégiques
4 : comment (pentest interne externe)
5 : traitement du risque

On trouve 2 cycles : stratégique et opérationnel
Périodicité : 1 an ou changement (dans la société , référentiel , de sources)
L'ensemble du cycle doit être rejoué.

<u>Méthode en 5 ateliers :</u>

1 – ce qu'on redoute , le + grave , métier
2- source de risque / objectif visé
3 – parties prenantes , écosystème , intégrateur prestataire

Exemple de l'adolescent

Introduction dans le SI du collège – Modifier les résultats scolaires

	ATTAQUE
Source de risque	Adolescent
Objectif visé	Ses résultats scolaires
Évènement redouté	Modification - les résultats d'un ou plusieurs ne sont plus justifiables.
Valeur métier	résultats scolaires
Bien support	SI du collège / Gestion des résultats
Impacts	Poursuite d'étude des collégiens – image établissement

en page 14 formation

Principes de base :

- Les normes
- Les scénarios (confidentialité – intégrité – disponibilité)

L'atelier 1 page 17

Métiers et techniques

Projet s'effectue sur une partie ou sur tout le SI

Valeurs métiers fonctionnelles (processus , informations (données))

Supports : réseaux , logiciels , scripts , humains, locaux

Exemple : : Société de biotechnologies fabriquant des vaccins (page 19)

Etat :

- Niveau de maturité faible en sécurité numérique
- Sensibilisation basique à la sécurité (prise de poste)
- Charte informatique

Définition du périmètre métier et technique

Mission : Identifier et fabriquer des vaccins

MISSION	IDENTIFIER ET FABRIQUER DES VACCINS				
DÉNOMINATION DE LA VALEUR MÉTIER				Fabriquer des vaccins	
NATURE DE LA VALEUR MÉTIER *(PROCESSUS OU INFORMATION)*				Processus	
DESCRIPTION				Activité consistant à réaliser : • le remplissage de seringues (stérilisation, remplissage) ; • le conditionnement (étiquetage et emballage).	
ENTITÉ OU PERSONNE RESPONSABLE *(INTERNE/EXTERNE)*				Responsable production	
DÉNOMINATION DU/DES BIENS SUPPORTS ASSOCIÉS					
DESCRIPTION					
ENTITÉ OU PERSONNE RESPONSABLE *(INTERNE/EXTERNE)*					

MISSION	IDENTIFIER ET FABRIQUER DES VACCINS				
DÉNOMINATION DE LA VALEUR MÉTIER	Recherche & développement (R&D)			Fabriquer des vaccins	Traçabilité et contrôle
NATURE DE LA VALEUR MÉTIER *(PROCESSUS OU INFORMATION)*	Processus			Processus	Information
DESCRIPTION	Activité de recherche et développement des vaccins nécessitant : • l'identification des antigènes ; • la production des antigènes (vaccin vivant atténué, inactivé, sous-unité) : fermentation (récolte), purification, inactivation, filtration, stockage ; • l'évaluation préclinique ; • le développement clinique.			Activité consistant à réaliser : • le remplissage de seringues (stérilisation, remplissage) ; • le conditionnement (étiquetage et emballage).	Informations permettant d'assurer le contrôle qualité et la libération de lot (exemples : antigène, répartition aseptique, conditionnement, libération finale…)
ENTITÉ OU PERSONNE RESPONSABLE *(INTERNE/EXTERNE)*	Pharmacien			Responsable production	Responsable qualité
DÉNOMINATION DU/DES BIENS SUPPORTS ASSOCIÉS	Serveurs bureautiques (internes)	Serveurs bureautiques (externes)	Systèmes de production des antigènes	Systèmes de production	Serveurs bureautiques (internes)
DESCRIPTION	Serveurs bureautiques permettant de stocker l'ensemble des données de R&D	Serveurs bureautiques permettant de stocker une partie des données de R&D	Ensemble de machines et équipements informatiques permettant de produire des antigènes	Ensemble de machines et équipements informatiques permettant de fabriquer des vaccins à grande échelle	Serveurs bureautiques permettant de stocker l'ensemble des données relatives à la traçabilité et au contrôle, pour les différents processus
ENTITÉ OU PERSONNE RESPONSABLE *(INTERNE/EXTERNE)*	DSI	Laboratoires	Laboratoires	DSI + Fournisseurs de matériel	DSI

Lorsque le tableau est établi, on ne le rectifie plus.

On étudie entre 5 et 10 valeurs métiers.

Il faut considérer l'ensemble des infos en tenant compte de l'héritage des fonctions sur les autres valeurs métiers.

L'échelle de gravité est définie par l' ANSSI dans le cadre d'EBIOS. (page 23)

Mineure – significative (dégradation) – grave (forte) – critique (incapacité)

<u>Les évènements redoutés</u>

Tableau selon la valeur métier R&D , Traçabilité Données

Exemple : Fuite de données , serveur en panne , machine obsolète , hacking , perte de disque , FAI

Vol de données – pas grave

Vol de données et utilisation - gravité

Ransomware – arrêt de production (durée ? reprise ? impossibilité de produire)

⇒ On s'attache au niveau les + hauts de gravité 3 et 4

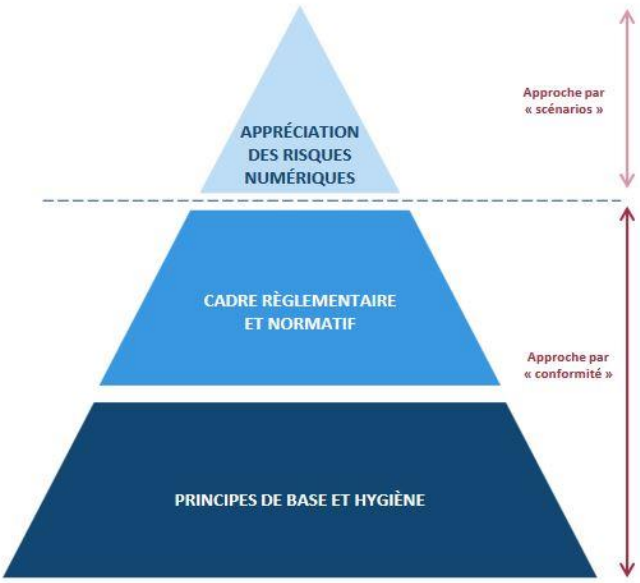
Puis le niveau 2, il se peut qu'il hérite des niveaux 3 et 4

Identifier les d'événements redoutés **ER**

<u>Déterminer le socle de sécurité (</u>page 25)

Approche par conformité (ANSSI , normes et réglementation)

Approche par scénario



ATELIER 2
SOURCES DE RISQUE

Sources de risque par rapport à l'objectif visé

Tableau croisé motivation et ressources

			RESSOURCES			
			Incluant les ressources financières, le niveau de compétences cyber, l'ouillage, le temps dont l'attaquant dispose pour réaliser l'attaque, etc.			
			Ressources limitées	Ressources significatives	Ressources importantes	Ressources illimitées
MOTIVATION	Intérêts, éléments qui poussent la source de risque à atteindre son objectif	Fortement motivé	Moyennement pertinent	Plutôt pertinent	Très pertinent	Très pertinent
		Assez motivé	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent	Très pertinent
		Peu motivé	Peu pertinent	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent
		Très peu motivé	Peu pertinent	Peu pertinent	Moyennement pertinent	Moyennement pertinent

Reprise de l'exemple de la société de biotechnologies fabriquant des vaccins

Réponses de la salle pour les sources de risques : hacktiviste , employé vengeur, pays, Anti VAC ,

Quelle gravité pour mon scénario stratégique ? (fabriquer des vaccins / traçabilité et contrôle)

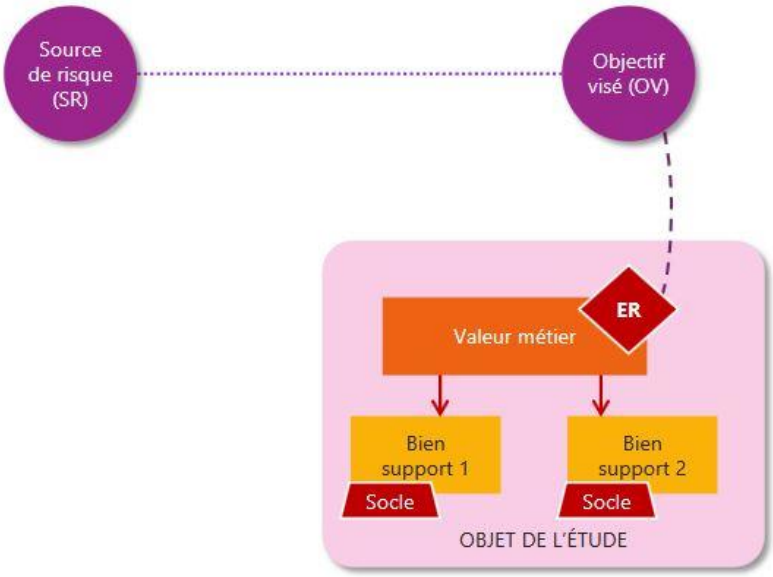
Page 32

ER les plus graves

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ	GRAVITÉ
Fabriquer des vaccins	Interruption de la production ou de la distribution de vaccins pendant plus d'une semaine pendant un pic d'épidémie	4
Traçabilité et contrôle	Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire	4
R&D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée	3
R&D	Fuite des informations d'études et recherches de l'entreprise	3

SR/OV les plus pertinents

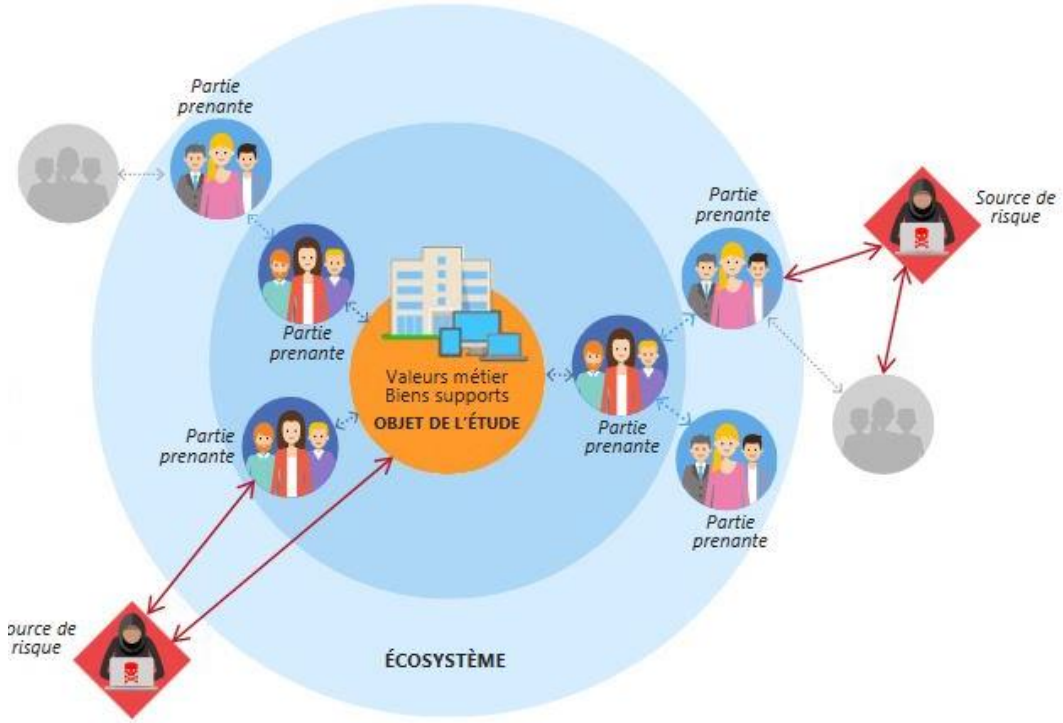
SOURCES DE RISQUE	OBJECTIF VISÉ
Concurrent	Voler des informations
Hacktiviste	Saboter la campagne nationale de vaccination



Page 98 support formation mai 2024

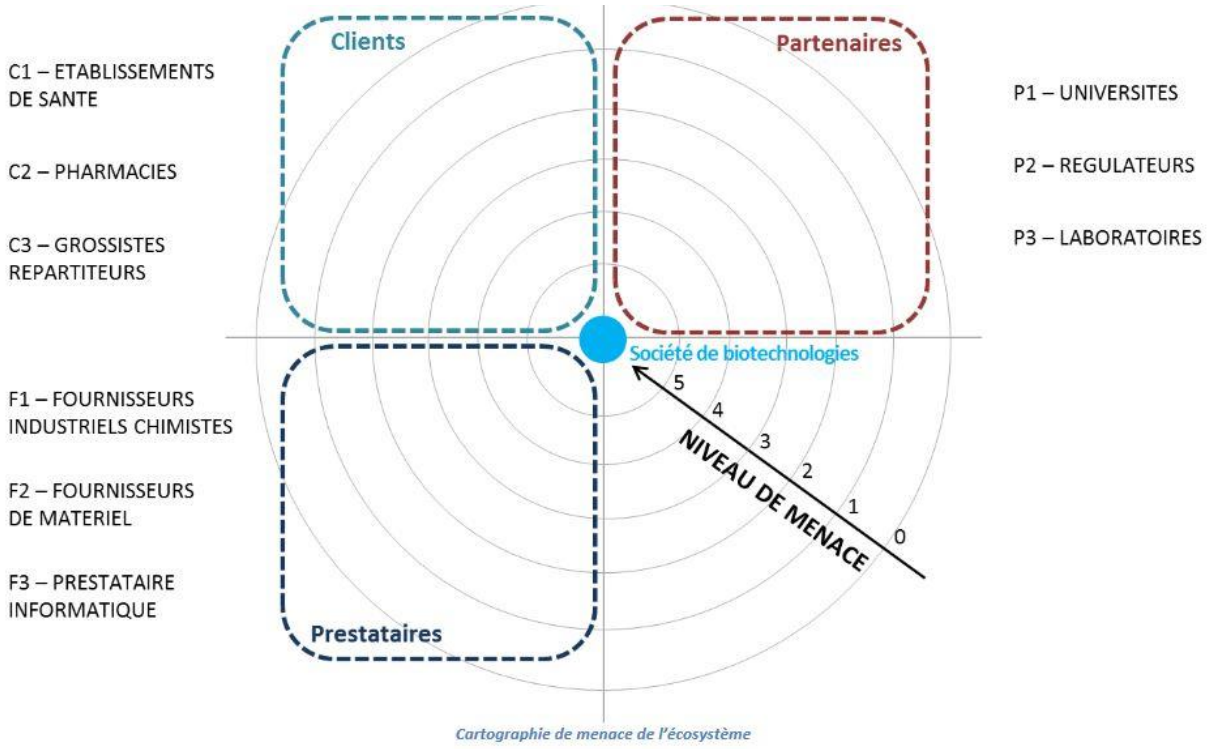
ATELIER 3
SCÉNARIOS STRATÉGIQUES

cartographie des menaces - écosystème



Support p 108 et Livret stagiaire p 11 13

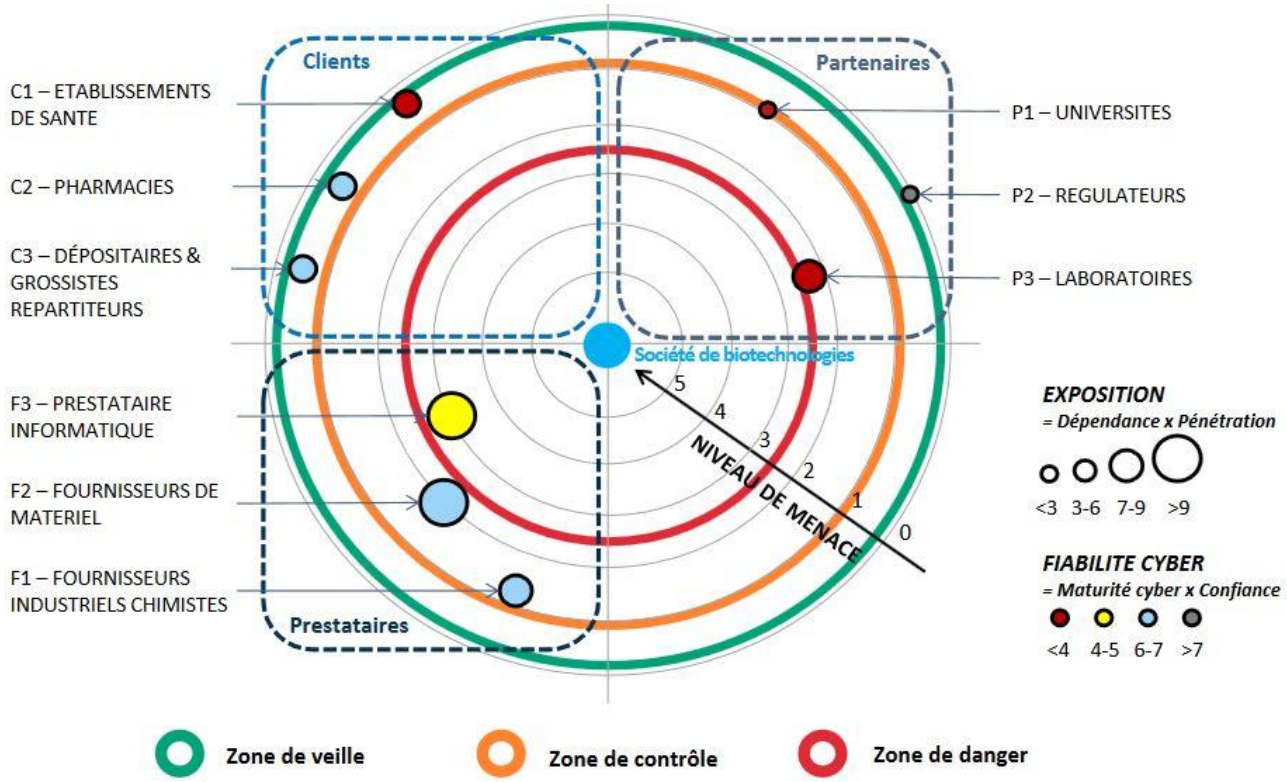
Exemple société de biotechnologies



Cartographie de menace de l'écosystème

Notion de fiabilité Cyber qui est le produit de la maturité Cyber par la confiance

Exposition / Fiabilité dépendance par Pénétration



Notion de zone de danger : Prestataires / laboratoires

Solutions : Il faut demander les labellisations (ISO) , ANSSI, cyber malveillance

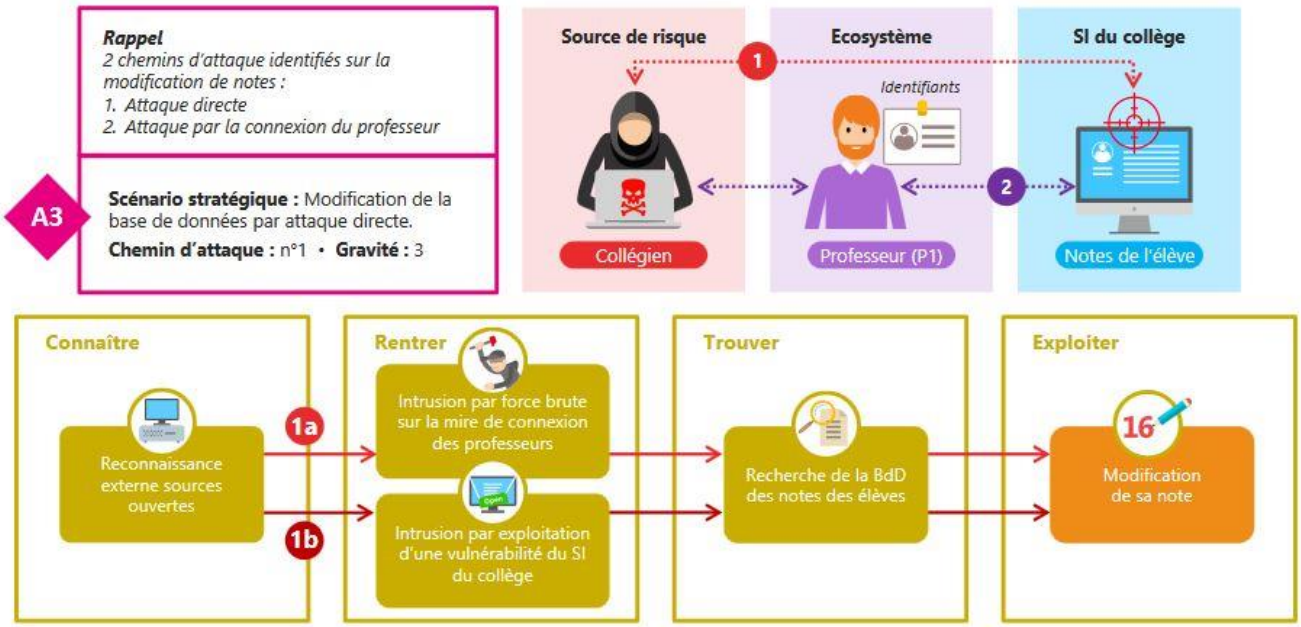
Scénarios pour définir une échelle de vraisemblance

Partir des chemins d'attaque identifiés lors de l'atelier 3.

• Construire, pour chaque chemin d'attaque retenu un scénario opérationnel permettant à la source de risque d'atteindre son objectif.

• Enrichir les chemins d'attaques de quelques précisions sur la manière dont l'attaquant va procéder.

<u>Des scénarios structurés selon une séquence d'attaque type</u>



Support de formation mai 2024

Source d'informations (atelier 4)

MITRE ATT&CK® est une base de connaissances, accessible au monde entier, sur les tactiques et techniques des cyberattaquants, basée sur des observations du monde réel.

Echelle	Définition
V4 Certain OU déjà produit	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés OU un tel scénario s'est déjà produit au sein de l'organisation (historique d'incidents)
V3 Très vraisemblable	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée
V2 Vraisemblable	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative
V1 Peu vraisemblable	La source de risque a peu de chances d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible

Source d'informations (atelier 4)

MITRE ATT&CK® est une base de connaissances, accessible au monde entier, sur les tactiques et techniques des cyberattaquants, basée sur des observations du monde réel.

Stratégie et traitement des risques

<u>Stratégies possibles :</u>

- Réduction du risque
- Maintien du risque
- Partage du risque (transfert)
- Refus du risque (exemple la plaque d'égout rouillée) - évitement

Cet atelier peut servir à rédiger le PACS (Plan d'Amélioration Continue de la Sécurité).

La vraisemblance du scénario est modifiée par le risque encouru

Mise en place d'un comité de pilotage pour assurer le suivi des risques

4. **Etude de cas « démarche administrative de renouvellement d'un titre d'identité numérique (TIN) »**
   - Livret du stagiaire p24
   - Support de formation 2019 p 89
   - Support de formation mai 2024 page 191
5. **Exemple de traitement dans le livre BTS SIO 1ère année BLOC 3**
   Fiche savoirs technologiques 1 p23 , Fiche méthode 5 p211
   Contexte : Protéger les données à caractère personnel
   L' entreprise se nomme Centrecall
   Une DSI
   3 pôles :
   - infrastructures et serveurs
   - applications
   - données

Missions :

- Identifier les risques liés aux données à caractère personnel
- Recenser les traitements sur les données à caractère personnel
- Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractères personnel

Utilisation de la méthode PIA

https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-1-fr-methode.pdf

1) Identifier les **vulnérabilités** dans le traitement des données
2) Compléter le tableau d'analyse des menaces.. Justifier les niveaux de **vraisemblance**
3) Retrouver pour chaque risque mentionné, **l'événement redouté** et son niveau de **gravité** estimé.
4) Cartographiez les risques liés au traitement des données à caractère personnel par un schéma croisant les niveaux de vraisemblance et de gravité. Fiche savoirs technologiques 1
5) Rédigez une note de synthèse