



# EBIOS *Risk Manager*

## Formation

10/06/2025

TLP: CLEAR

PAP: CLEAR





# Introduction

Les données sont notre pétrole ! Les moyens sont contraints. Nos systèmes et la réglementation ne sont pas parfaitement maîtrisés et évoluent en permanence. Les attaques se multiplient. Les attaquants s'organisent et leurs capacités s'accroissent.

Dans ce contexte, il est plus que jamais indispensable de « penser risques » pour **décider de ce qui est nécessaire et suffisant pour se protéger**, de manière efficace.



# Plan de la formation

1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. Apprécier les risques
  - a. Approche par conformité
  - b. Approche par scénarios
5. Traiter les risques
6. Étude de cas complète
7. Conclusion

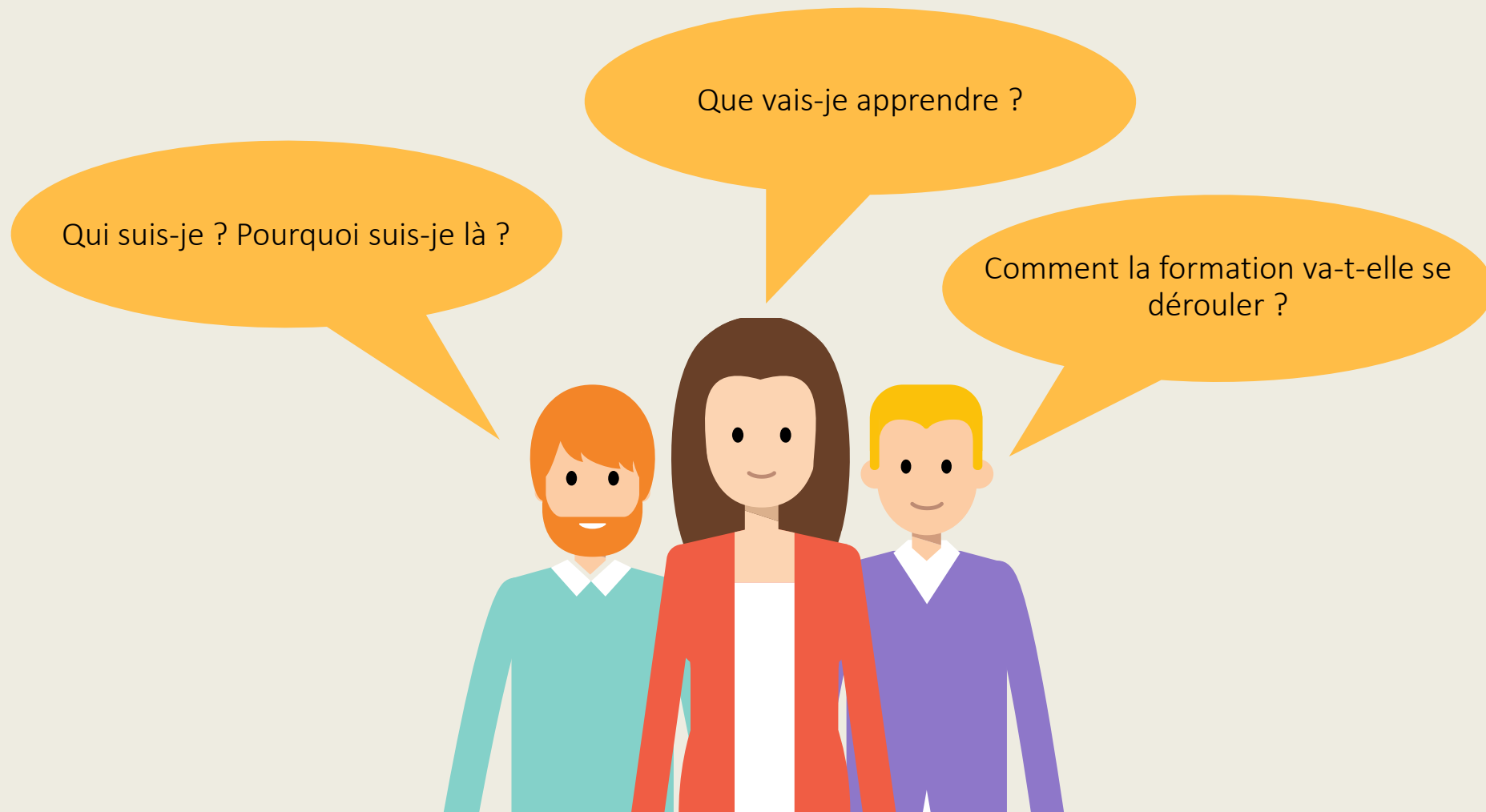


# Plan de la formation

1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. Apprécier les risques
  - a. Approche par conformité
  - b. Approche par scénarios
5. Traiter les risques
6. Étude de cas complète
7. Conclusion



# De quoi va-t-on parler ?





# Présentations



- Qui êtes-vous ?
- Quels sont vos besoins ?

Nous allons nous adapter dans la mesure du possible !



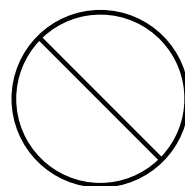
# Qu'allez-vous apprendre ? Comment ?



## Objectif pédagogique

Être capable de mener une étude des risques avec la méthode EBIOS *Risk Manager*

(il faudra mener votre première étude pour véritablement savoir faire)



## Hors de notre objectif

- Bases de la sécurité de l'information  
→ [voir le MOOC de l'ANSSI](#)
- Grands principes d'EBIOS *Risk Manager*  
→ [voir les mini-séquences du Club EBIOS](#)
- Vous apprendre les guides : il suffit de les ouvrir !  
→ [voir les guides](#)



## Horaires

- Formation sur 2 jours
  - 9h00 – 12h00
  - 14h00 – 17h00
- (2 pauses)

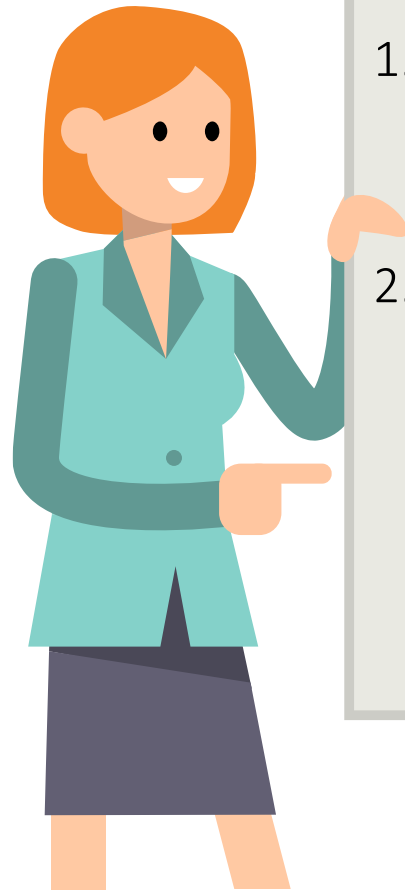


## Approche pédagogique

- Formation réellement active : vous allez travailler !
- Appropriation des concepts nécessaires à la conduite d'une étude EBIOS *Risk Manager*
- Application des outils indispensables (et non de toutes les techniques possibles)
- Cas pratique : une étude de bout en bout



# Qu'avons-nous appris ?



1. On n'est pas là pour se reposer !
2. On va pouvoir mener des études **EBIOS Risk Manager** à l'issue de la formation

→ En avant !





# Plan de la formation

1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. Apprécier les risques
  - a. Approche par conformité
  - b. Approche par scénarios
5. Traiter les risques
6. Étude de cas complète
7. Conclusion



# De quoi va-t-on parler ?





# Qu'est-ce qu'un risque ?

Exemple de la  
voiture



**Risque** : scénario menant à un événement redouté qui engendre des conséquences indésirables

**Événement redouté** (qu'est-ce qu'on craint ?)  
Un accident

**Conséquences** (quels sont les impacts ?)  
Conducteur blessé, casse et réparations, destination non atteinte, nature affectée, image de soi, etc.

**Scénario** (comment cela peut-il arriver ?)  
Vitesse excessive, inattention, dangers sur la route, piratage de la voiture, etc.

Le risque est un ensemble, ex : vitesse excessive → accident → voiture cassée et blessures.  
Il est estimé en termes de gravité et de vraisemblance.



# Analyse des risques

Décomposons un peu !

- Un pirate...
- qui veut montrer les dangers des véhicules connectés...
- détourne...
- les fonctionnalités de déplacement...
- du système embarqué d'un véhicule...
- en profitant d'une nouvelle faille découverte...
- et provoque un accident...
- qui détruit le véhicule et blesse le conducteur.

- Source de risque
- Objectif visé
- Mode opératoire
- Valeur métier
- Bien support
- Vulnérabilité
- Événement redouté
- Conséquences





# Exercice collégial

Identifiez ou imaginez les éléments d'un risque à partir de l'article



Un adolescent de 15 ans « pirate »  
le système de son collègue pour  
améliorer ses notes

*Un adolescent de quinze ans a été  
interpellé pour s'être introduit  
dans le système informatique de  
son collègue dans le but de modifier  
ses résultats scolaires. [...]*

[Source : Le Point.fr et ZDNet]

Concepts d'un risque	Éléments du risque de l'article
Source de risque	
Bien support	
Valeur métier	
Évènement redouté	
Conséquences	
Objectif visé	



# Correction

Identifiez ou imaginez les éléments d'un risque à partir de l'article



Un adolescent de 15 ans « pirate »  
le système de son collège pour  
améliorer ses notes

*Un adolescent de quinze ans a été  
interpellé pour s'être introduit  
dans le système informatique de  
son collège dans le but de modifier  
ses résultats scolaires. [...]*

[Source : Le Point.fr et ZDNet]

Concepts d'un risque	Éléments du risque de l'article
Source de risque	Adolescent de quinze ans
Bien support	Système informatique du collège
Valeur métier	Notes des élèves
Évènement redouté	Les notes des élèves sont modifiées
Conséquences	Poursuite d'études des collégiens impactée Image vis-à-vis des autres établissements scolaires
Objectif visé	Modifier ses résultats scolaires



# Exercice collégial

Identifiez ou imaginez les éléments d'un risque à partir de l'article



## Piratage massif du groupe hôtelier Marriott. 500 millions de clients touchés

*C'est une méga-fuite de données. Le groupe hôtelier américain Marriott a révélé qu'il avait été victime d'un piratage massif, avec des accès non-autorisés à la base de données de sa filiale Starwood.*

*Noms, adresses postale et électronique, dates de réservation, numéros de téléphone et de passeport...*

*Les informations d'environ 500 millions de clients ont été dérobées. [...] Les accès non autorisés, avec une duplication de la base de données ont commencé en 2014. Marriott assure que les numéros de cartes de crédit étaient chiffrés [...]*

*Mais la chaine n'exclut pas que les éléments nécessaires au déchiffrement des données aient été compromis.*

[Source : 20 minutes – 30/11/2018]

Concepts d'un risque	Éléments du risque de l'article
Source de risque	
Bien support	
Valeur métier	
Évènement redouté	
Conséquences	
Objectif visé	



# Correction

Identifiez ou imaginez les éléments d'un risque à partir de l'article



## Piratage massif du groupe hôtelier Marriott. 500 millions de clients touchés

*C'est une méga-fuite de données. Le groupe hôtelier américain Marriott a révélé qu'il avait été victime d'un piratage massif, avec des accès non-autorisés à la base de données de sa filiale Starwood.*

*Noms, adresses postale et électronique, dates de réservation, numéros de téléphone et de passeport...*

*Les informations d'environ 500 millions de clients ont été dérobées. [...] Les accès non autorisés, avec une duplication de la base de données ont commencé en 2014. Marriott assure que les numéros de cartes de crédit étaient chiffrés [...]*

*Mais la chaine n'exclut pas que les éléments nécessaires au déchiffrement des données aient été compromis.*

[Source : 20 minutes – 30/11/2018]

Concepts d'un risque	Éléments du risque de l'article
Source de risque	?
Bien support	Vol des informations des clients du groupe hôtelier
Valeur métier	Informations des clients du groupe
Évènement redouté	Base de données de sa filiale Starwood
Conséquences	Image, juridique (RGPD)
Objectif visé	Lucratif ?





# Exercice collégial

Identifiez ou imaginez les éléments d'un risque à partir de l'article



## Pathé victime d'une arnaque au président à 19 millions d'euros

*Des escrocs sont parvenus à convaincre l'ancien directeur financier de Pathé Pays-Bas que la direction de Pathé lui ordonnait de verser d'importantes sommes sur un compte tiers pour financer une acquisition à Dubaï.*

*Au total, plus de 19,2 millions d'euros auraient ainsi été dérobés à l'entreprise en mars 2018.*

*Les faits n'ont été révélés publiquement que lors du procès opposant l'ex-employé incriminé à son entreprise dans le cadre de son licenciement. Selon Pathé, il aurait « négligé des signaux » qui auraient dû l'alerter du caractère frauduleux des opérations.*

Source : Next inact – 12/11/2018

Concepts d'un risque	Éléments du risque de l'article
Source de risque	
Bien support	
Valeur métier	
Évènement redouté	
Conséquences	
Objectif visé	



# Correction

Identifiez ou imaginez les éléments d'un risque à partir de l'article



## Pathé victime d'une arnaque au président à 19 millions d'euros

*Des escrocs sont parvenus à convaincre l'ancien directeur financier de Pathé Pays-Bas que la direction de Pathé lui ordonnait de verser d'importantes sommes sur un compte tiers pour financer une acquisition à Dubaï.*

*Au total, plus de 19,2 millions d'euros auraient ainsi été dérobés à l'entreprise en mars 2018.*

*Les faits n'ont été révélés publiquement que lors du procès opposant l'ex-employé incriminé à son entreprise dans le cadre de son licenciement. Selon Pathé, il aurait « négligé des signaux » qui auraient dû l'alerter du caractère frauduleux des opérations.*

Source : Next inact – 12/11/2018

Concepts d'un risque	Éléments du risque de l'article
Source de risque	Escrocs
Bien support	Usurpation de l'identité d'un directeur de l'organisation
Valeur métier	Identité des directeurs (information)
Évènement redouté	Directeurs (personnes)
Conséquences	Financier, image
Objectif visé	Lucratif, fraude



# Estimation des risques

Qu'est-ce que la gravité ?



**Gravité** : estimation du niveau des conséquences potentielles.

**Conséquences sur l'objectif** (quels effets sur la mission ?)

Aucun | Retard | Destination non atteinte

**Conséquences sur la santé**

Aucuns | Blessure légère | Blessure grave | Décès

**Autres conséquences** (financières, sur l'environnement, etc.)

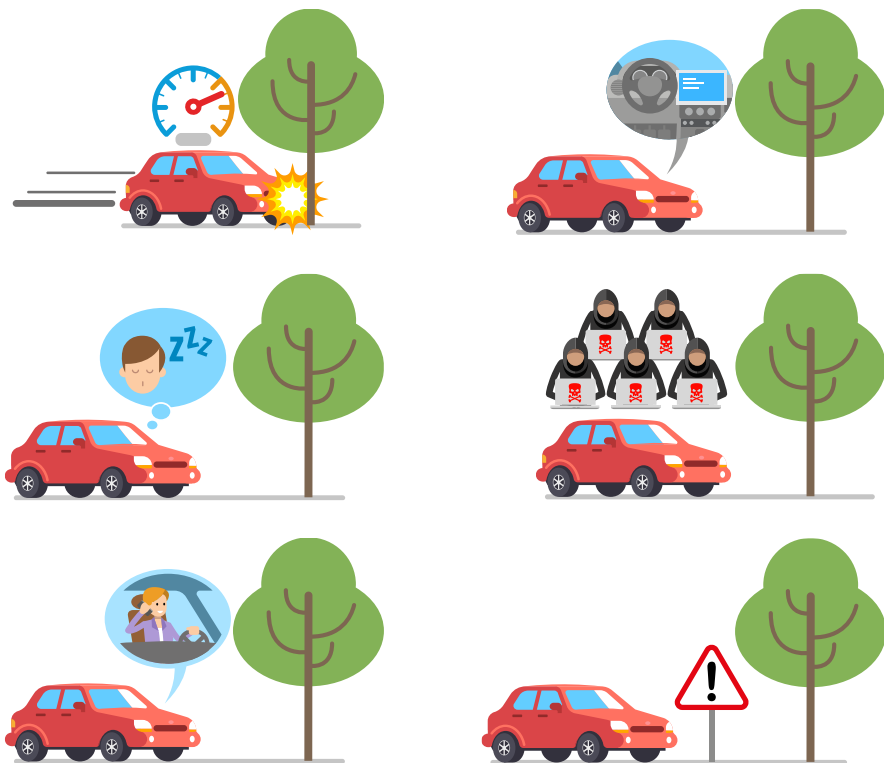
La gravité dépend des conséquences potentielles.

Elle est estimée selon des échelles qui hiérarchisent les conséquences par types.  
On retient généralement le maximum (la conséquence potentielle la plus grave).



# Estimation des risques

Qu'est-ce que la vraisemblance ?



**Vraisemblance** : estimation de la possibilité de réalisation des scénarios.

**Sources de risques** (qui peut nous attaquer ?)  
Peu | Moyennement | Plutôt | Très pertinent

**Vulnérabilités** (quels sont nos points faibles ?)  
Minimale | Faible | Importante | Maximale (avérée)

**Parties prenantes** (de qui dépend-on ?)

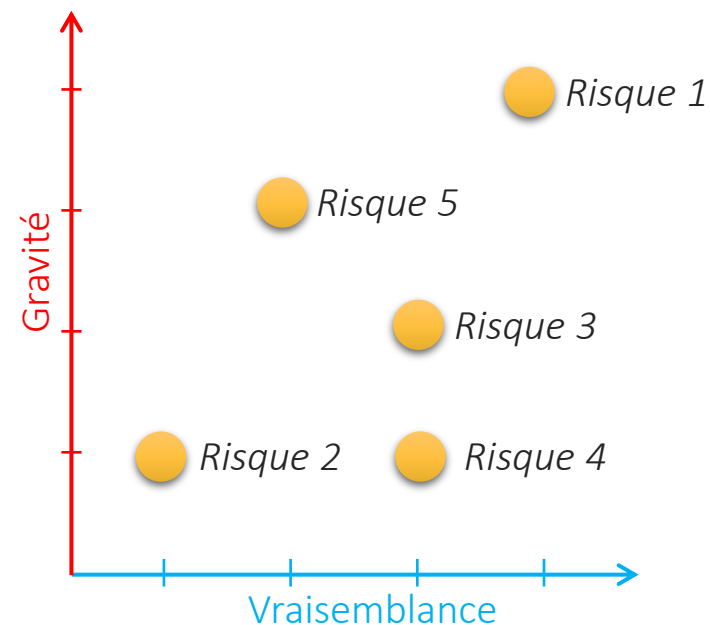
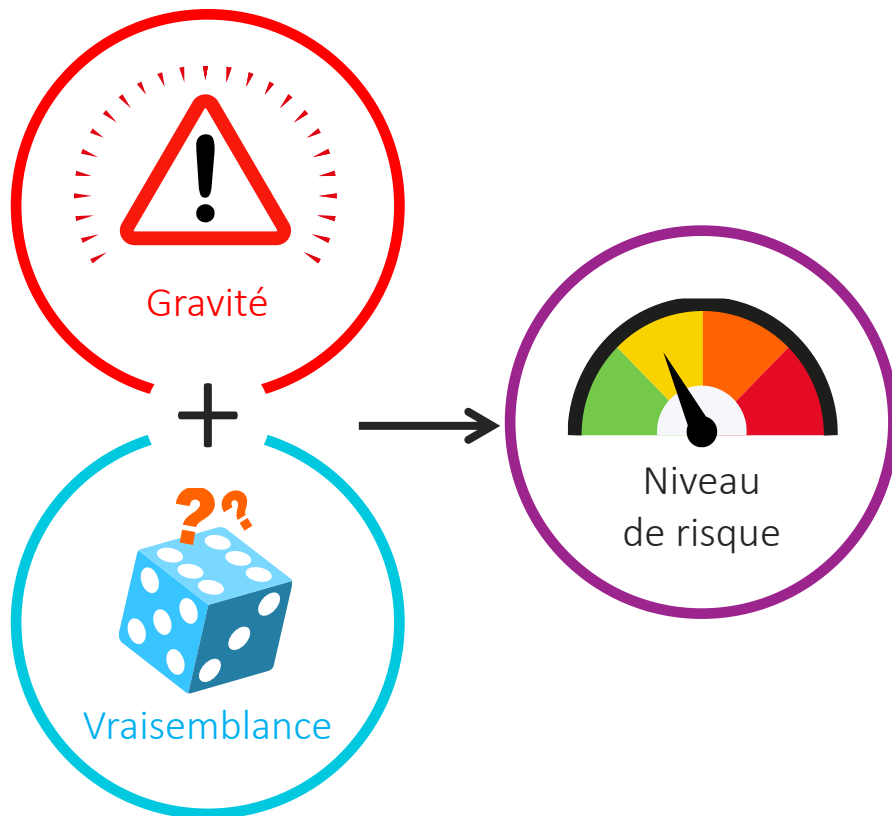
**Mesures en place** (quelles solutions d'atténuation ?)

La vraisemblance dépend de plusieurs facteurs : pertinence des sources de risques, niveau des vulnérabilités, dangerosité des parties prenantes et mesures en place.  
On décompose les scénarios pour estimer progressivement ces différents facteurs.



# Estimation des risques

Qu'est-ce que le niveau de risque ?



Le niveau d'un risque est composé de sa gravité et de sa vraisemblance.  
On ne fait pas d'opération « mathématique » !  
On peut ainsi positionner les risques sur une matrice comparer (évaluation des risques).



# Exercice collégial

Éléments utiles à l'estimation de la gravité et de la vraisemblance

Éléments utiles à l'estimation...

... du niveau de risque

Niveau d'un impact

Exposition aux sources de risques considérées

Existence de vulnérabilités

Facilité d'exploitation des vulnérabilités

Nombre de conséquences identifiées

Capacité et motivation des sources de risques



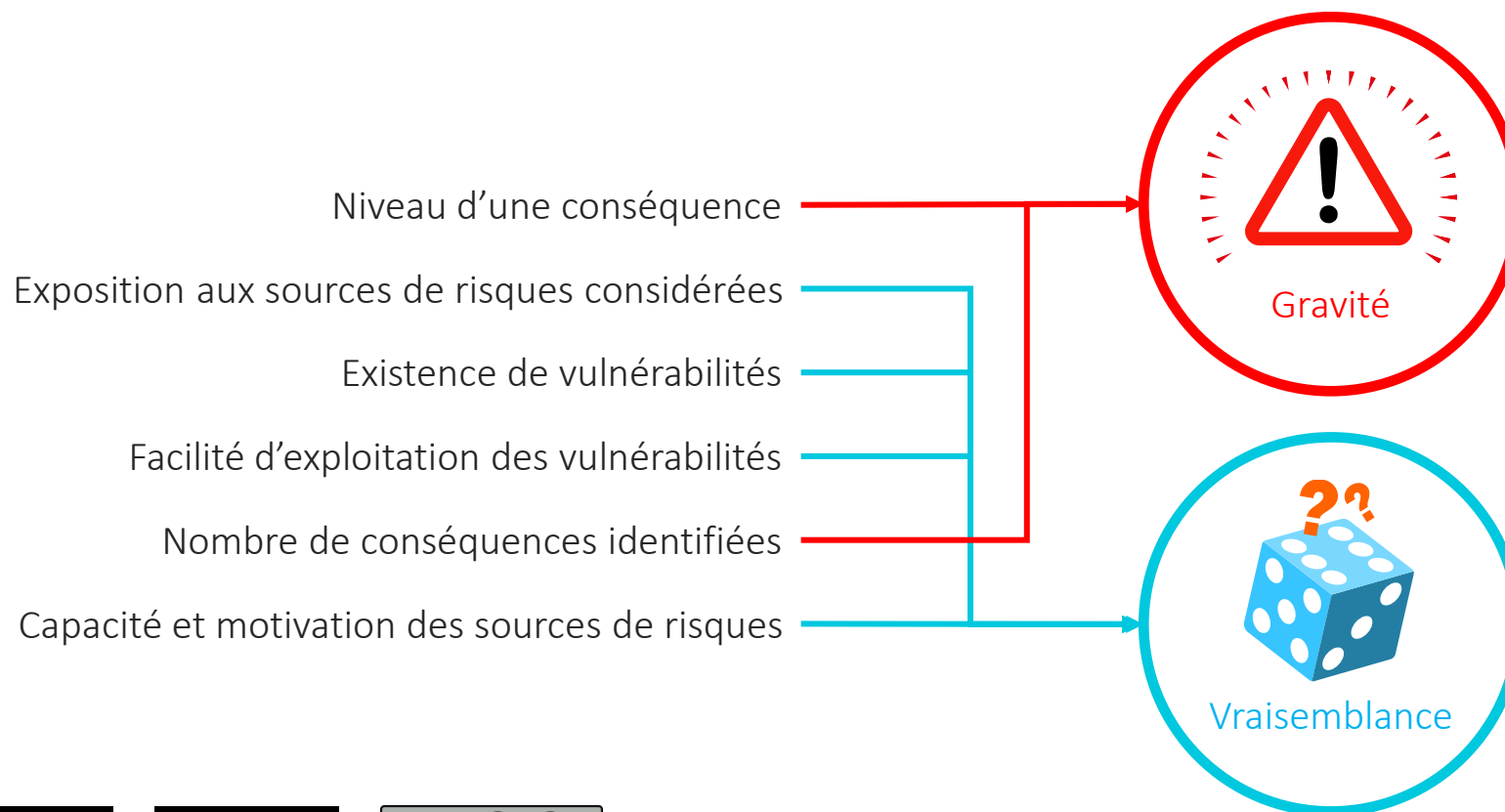


# Correction

Éléments utiles à l'estimation de la gravité et de la vraisemblance

Éléments utiles à l'estimation...

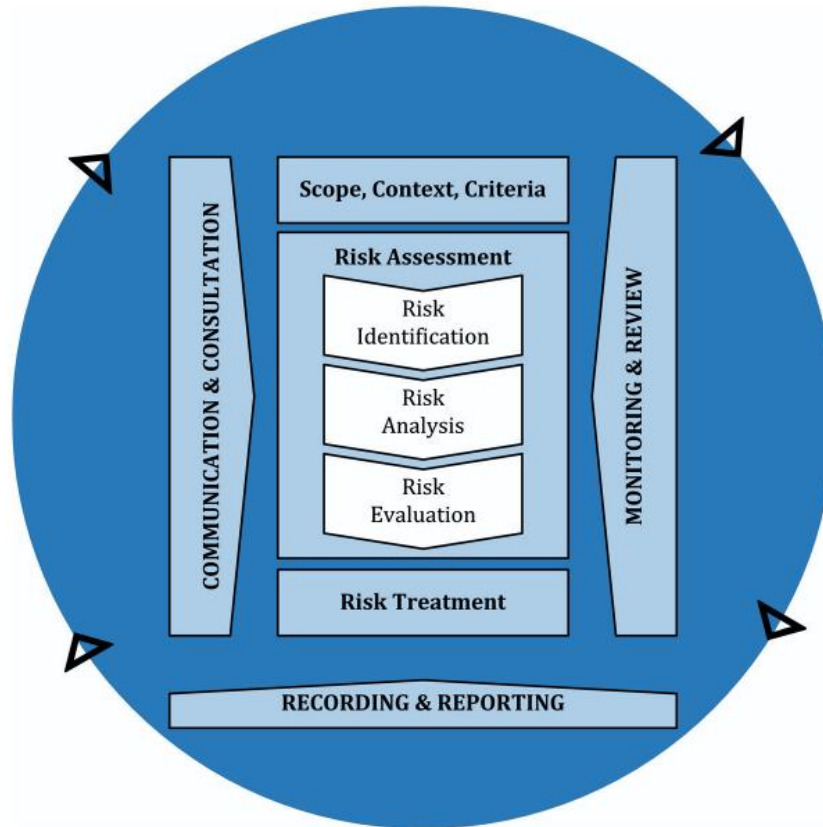
... du niveau de risque



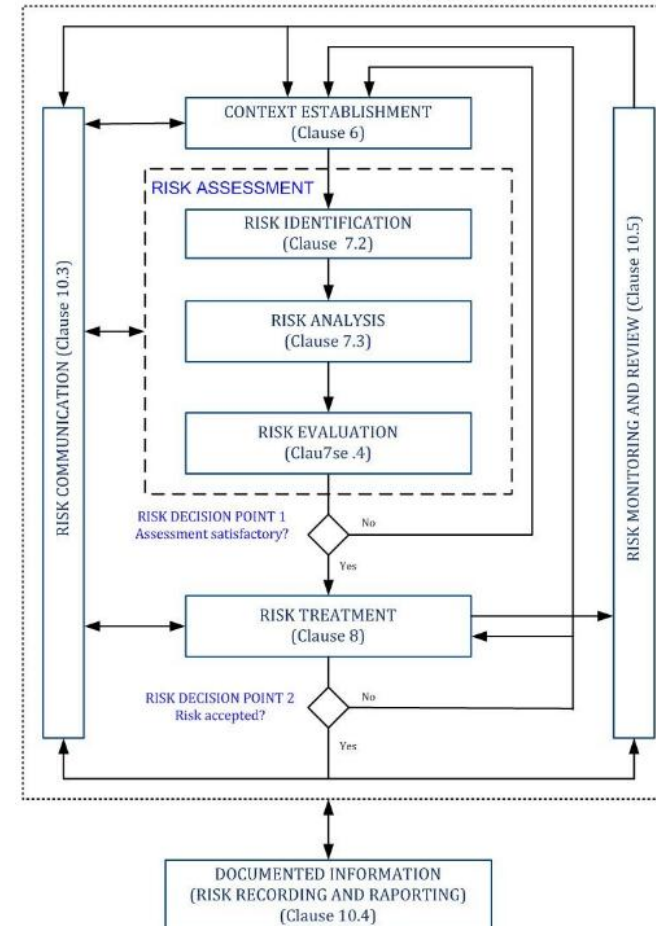


# Le processus de gestion des risques

ISO 31000 et ISO/IEC 27005 définissent les concepts et principes



ISO 31000



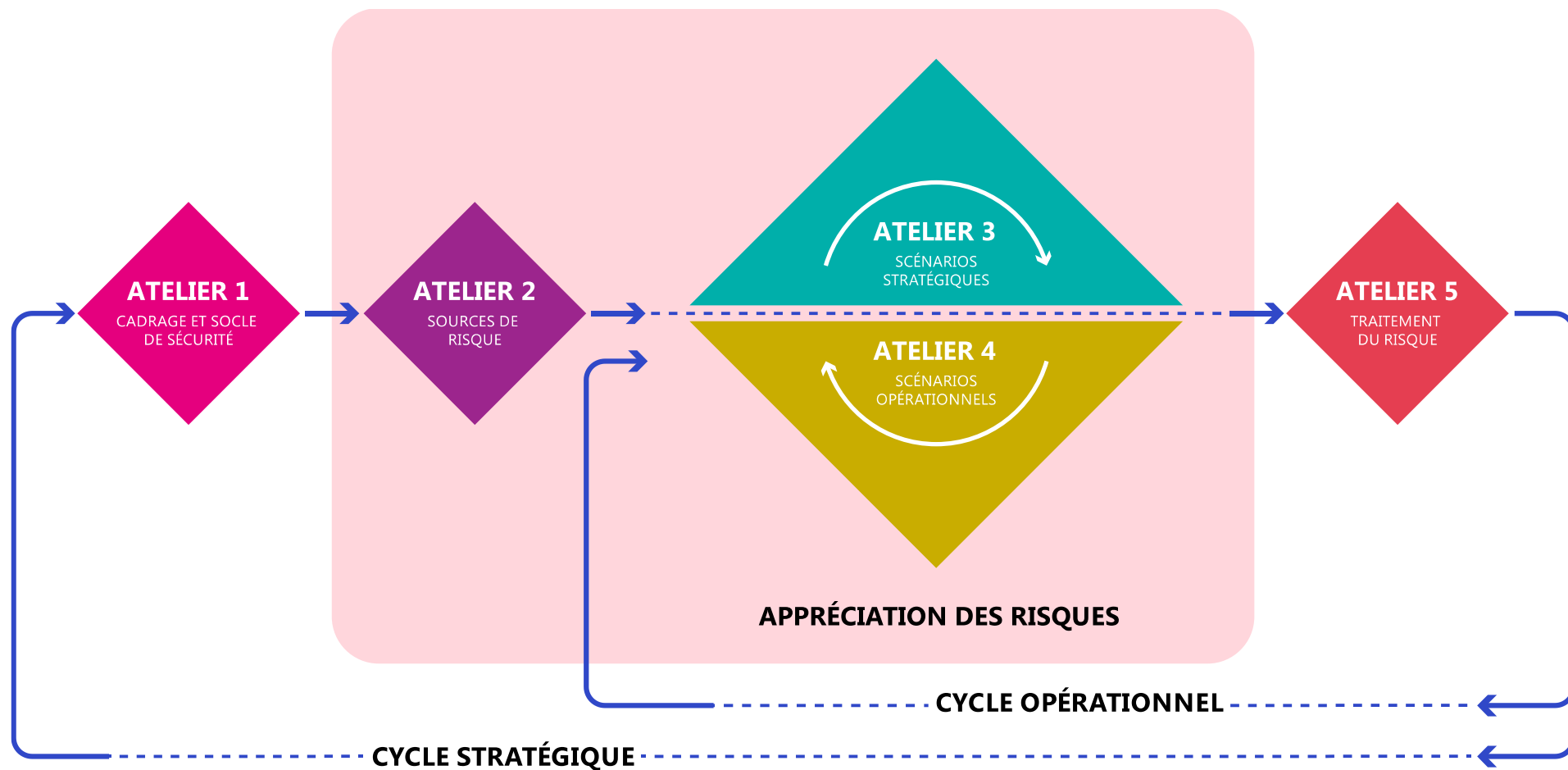
ISO/IEC 27005





# La méthode EBIOS *Risk Manager*

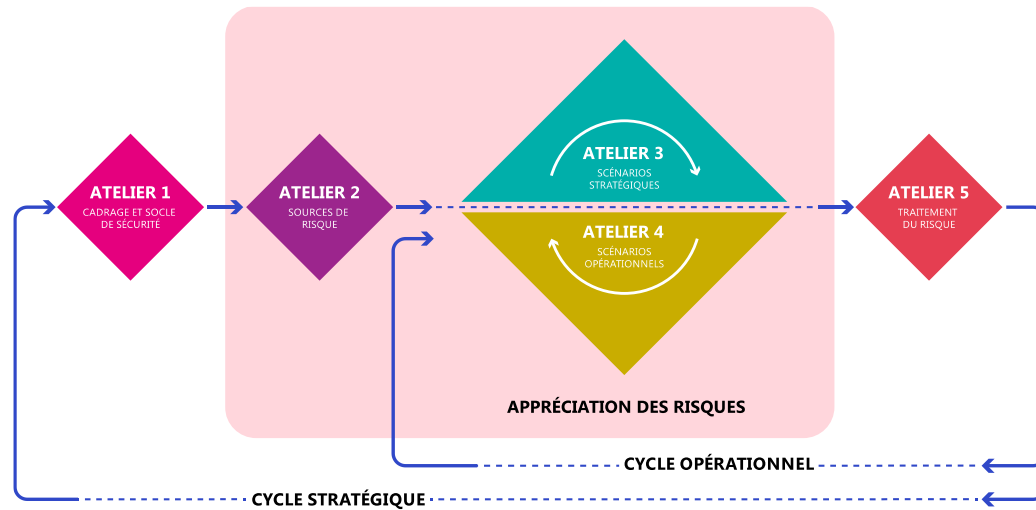
La démarche de l'ANSSI met en œuvre ISO 31000 et ISO/IEC 27005





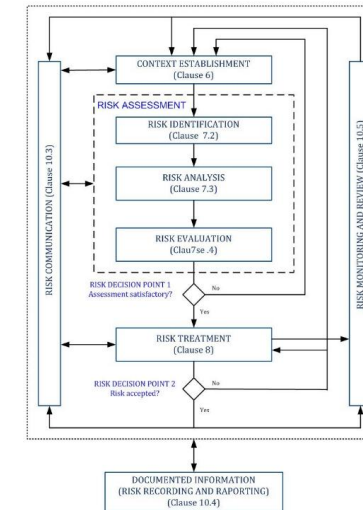
# EBIOS Risk Manager vs. ISO/IEC 27005

Mêmes idées, organisation différente



## EBIOS Risk Manager : 5 ateliers

1. Le point de vue du défenseur : Qu'est ce qui doit être protégé, et pourquoi ?
2. Qui est l'agresseur et pourquoi passe-t-il à l'acte ?
3. Par où l'attaquant va-t-il agir ?
4. Comment l'attaquant va-t-il agir ?
5. Quelle stratégie de sécurité au regard des risques identifiés ?



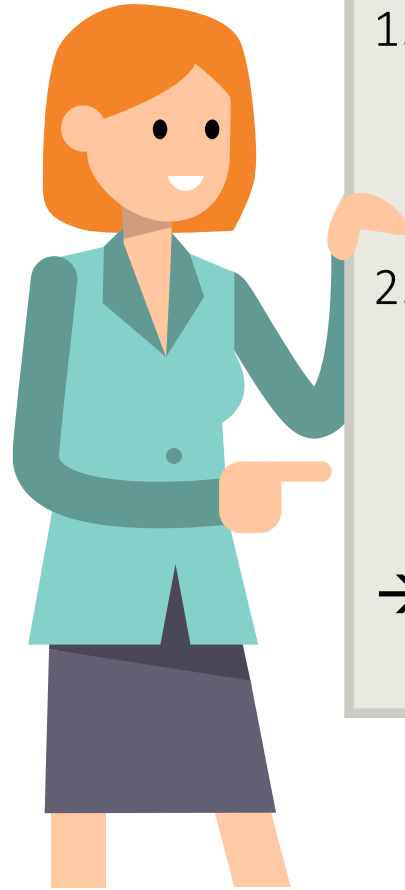
## ISO/IEC 27005 : 7 sous-processus

1. L'établissement du contexte
2. L'identification des risques
3. L'analyse des risques
4. L'évaluation des risques
5. Le traitement des risques

Et 2 sous-processus transverses : communication & concertation et Surveillance & revue



# Qu'avons-nous appris ?



1. Comprendre ce qu'est un **risque** dans EBIOS *Risk Manager*
  2. Comprendre que le **niveau d'un risque** est composé de sa **gravité** et de sa **vraisemblance**
- Rentrons maintenant dans le vif du sujet !



# Plan de la formation

1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. Apprécier les risques
  - a. Approche par conformité
  - b. Approche par scénarios
5. Traiter les risques
6. Étude de cas complète
7. Conclusion



# De quoi va-t-on parler ?

Établir le contexte





# Outil 01 – Cadrer une étude

Du besoin de se poser les bonnes questions !

Établir le contexte

## L'objectif

Pourquoi me demande-t-on de mener une étude ?

- Se conformer à l'ISO/IEC27001
- Élaborer le dossier d'homologation d'un système
- Élaborer les règles de la politique de l'organisme
- Rédiger des exigences pour un cahier des charges
- Fournir des pistes à creuser par un test d'intrusion
- Préparer une revue des partenaires

Ceci permet notamment de :

1. choisir les **outils** d'EBIOS ;
2. choisir le **socle de règles** ;
3. cadrer les **types de conséquences** ;
4. définir la **forme des mesures**.

## Le sujet

Sur quel objet l'étude porte-t-elle ?

- L'organisme entier
- Une activité organisationnelle
- Un système en particulier
- Un composant précis
- Un produit qu'on achète
- Un produit qu'on vend
- Un outil de sécurité

Ceci permet notamment de :

1. choisir les **outils** d'EBIOS ;
2. définir le **niveau de détail** ;
3. déterminer les **interlocuteurs à impliquer**.

## Les destinataires

À qui l'étude est-elle destinée ?

- La Direction d'un organisme
- Un responsable métier
- Une autorité d'homologation
- Le responsable de la sécurité des systèmes d'information
- Le délégué à la protection des données
- Une autorité tierce
- Des auditeurs techniques
- Des auditeurs organisationnels

Ceci permet notamment de :

1. définir la **forme de l'étude** (compréhension par le destinataire) ;
2. cadrer les **types de conséquences** ;
3. choisir le **socle de règles**.

## Le temps

Quel est les contraintes temporelles de l'étude ?

- Étude *one shot*
- Étude récurrente
- Étude permanente (mise à jour et enrichissement en continu)
- Fortes contraintes temporelles
- Conditions de mise à jour

Ceci permet notamment de :

1. définir les **cycles de révision** ;
2. choisir la manière d'utiliser les **outils** d'EBIOS ;
3. organiser les **interactions** ;
4. adapter l'**exhaustivité**.



# Exercice collégial

Pour chaque cas, quelles sont les principales spécificités de l'étude ?

Étude d'un système pour son homologation

Étude d'un produit à vendre

Première étude !

Établir le contexte



# Correction

Pour chaque cas, quelles sont les principales spécificités de l'étude ?

## Étude d'un système pour son homologation

Spécificité : production d'éléments pour la prise de décision d'une autorité

- Les éléments doivent pouvoir s'intégrer au dossier d'homologation
- Les données doivent être cohérentes avec les autres études et outils
- Accent sur l'intelligibilité des risques, mesures et risques résiduels

## Étude d'un produit à vendre

Spécificité : méconnaissance du contexte précis des clients

- N'utiliser que les éléments maîtrisés : référentiels connus applicables, biens supports, scénarios opérationnels, mesures
- Tenir à jour et valoriser ces éléments

## Première étude !

Spécificité : un risque de se noyer et de ne jamais voir le bout de l'étude

- 1 élément par outil : 1 valeur métier, 1 bien support, 1 source de risque, 1 scénario stratégique, 1 scénario opérationnel...
- Développer ensuite d'autres cas





# Outil 02 – Choisir et affecter les outils

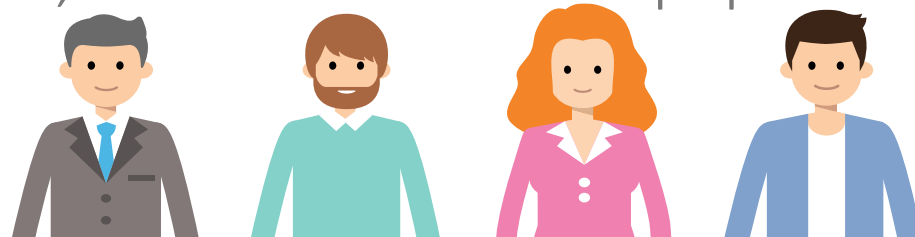
Exemple issu des guides de l'ANSSI

Objectif de l'étude	Ateliers a conduire				
	1	2	3	4	5
Identifier le socle de sécurité adapté à l'objet de l'étude	X				
Etre en conformité avec les référentiels de sécurité numérique					
Evaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude					
Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème					
Réaliser une étude préliminaire de risque pour identifier les axes prioritaires d'amélioration de la sécurité					
Conduire une étude de risque complète et fine, par exemple sur un produit de sécurité ou en vue d'homologuer un système					



# Qui va faire quoi ?

Mener une étude, c'est un travail d'équipe



Principaux éléments d'étude

	Autorité	Métier	Technique	Expert SSI
Valeurs métier	I	R A	I	I
Biens supports	I	C	R A	I
Socle de règles	I	R	C	C A
Événements redoutés	I	R A	I	C
Sources de risques	I	C	I	R A
Parties prenantes	I	R A	I	C
Scénarios stratégiques	I	C A	I	R
Scénarios opérationnels	I	I	R A	C
Risques	A	R	I	R
Mesures	A	C	C	R

Différents profils sont nécessaires pour mener l'étude : obtenir les informations pertinentes, comprendre et traiter des risques, prendre des décisions, etc.

Selon les outils choisis, il convient donc de déterminer les personnes appropriées et leur rôle pour les mettre en œuvre.

R Responsable

A Approbateur

C Consulté

I Informé



# Outil 03 – Identifier le périmètre

## Une vision du SI dans les strates du cyberspace

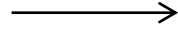
Établir le contexte

Le périmètre est décrit par les missions, valeurs métier et biens support.

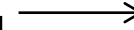
Le niveau de détail dépend notamment de l'objet de l'étude et de ses destinataires.

Pour les sujets complexes, il peut être utile de décrire également les liens entre composants.

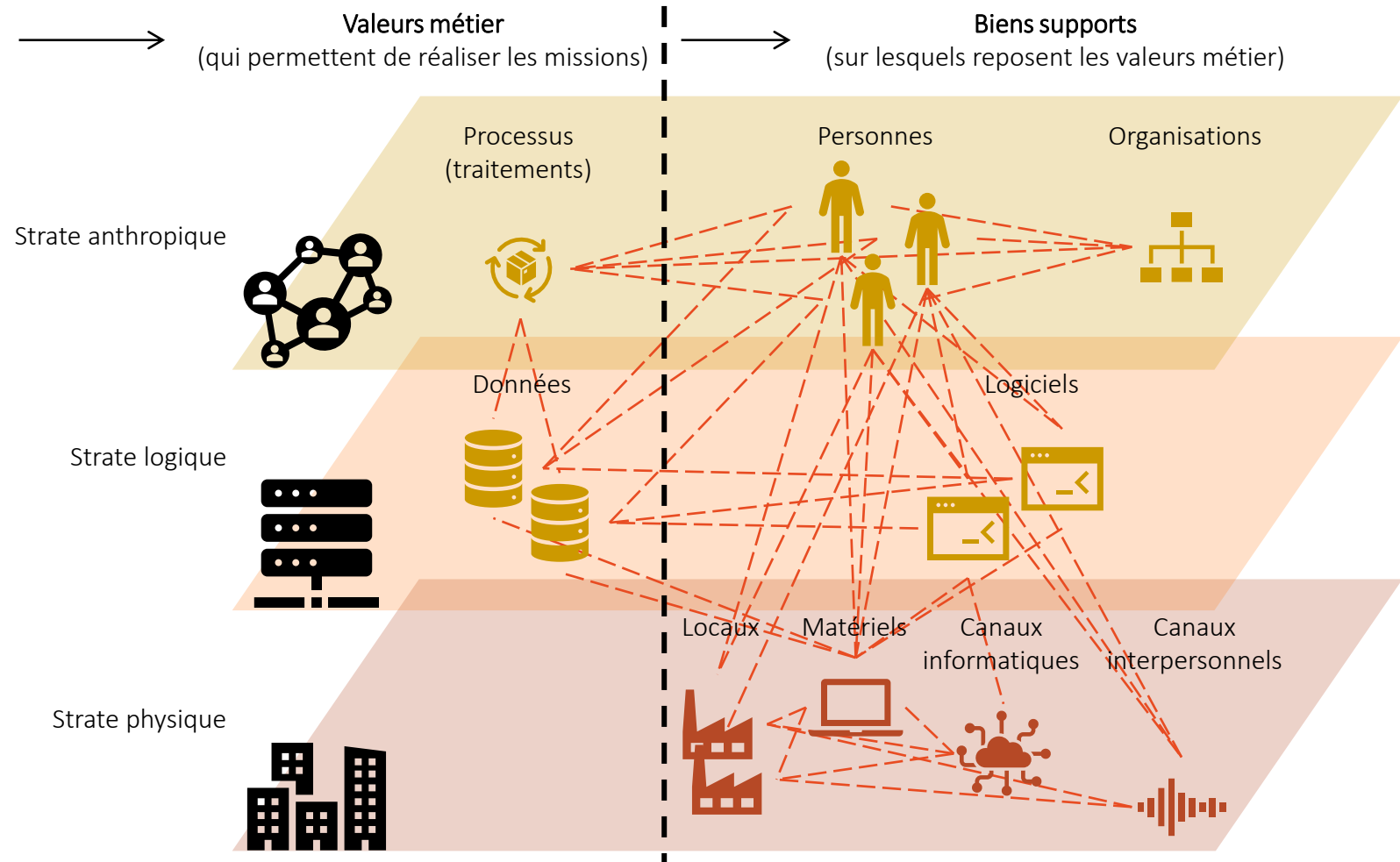
Missions  
(les finalités)



Valeurs métier  
(qui permettent de réaliser les missions)



Biens supports  
(sur lesquels reposent les valeurs métier)





# Exercice collégial

Identifiez ou imaginez les éléments d'un risque à partir de l'article



Un adolescent de 15 ans « pirate »  
le système de son collègue pour  
améliorer ses notes

*Un adolescent de quinze ans a été  
interpellé pour s'être introduit  
dans le système informatique de  
son collègue dans le but de modifier  
ses résultats scolaires. [...]*

[Source : Le Point.fr et ZDNet]

Composants	Composants de l'article
Mission	
Valeur métier	
Bien support	

Établir le contexte



# Correction

Identifiez ou imaginez les éléments d'un risque à partir de l'article



Un adolescent de 15 ans « pirate »  
le système de son collège pour  
améliorer ses notes

*Un adolescent de quinze ans a été  
interpellé pour s'être introduit  
dans le système informatique de  
son collège dans le but de modifier  
ses résultats scolaires. [...]*

[Source : Le Point.fr et ZDNet]

Composants	Composants de l'article
Mission	Gérer les résultats scolaires
Valeur métier	Notes des élèves
Bien support	Système informatique du collège



# Outil 04 – Identifier les parties prenantes

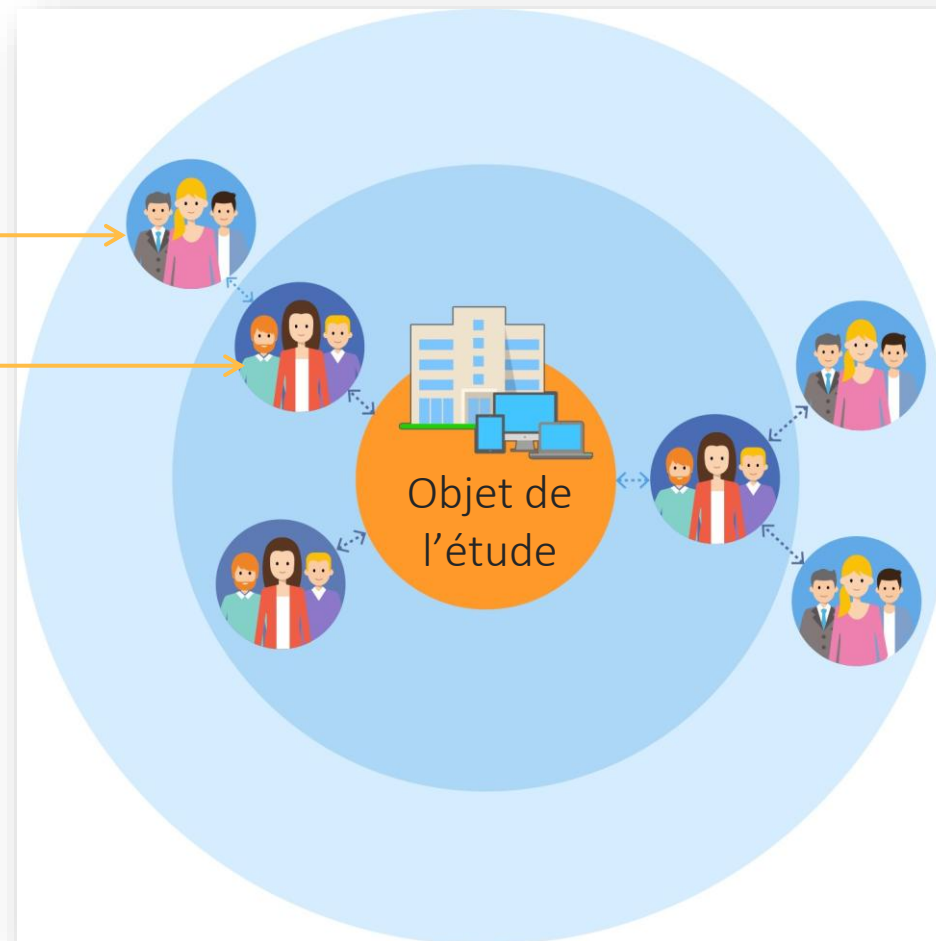
Comment décrire l'écosystème ?

## Qu'est-ce qu'une partie prenante ?

Tout acteur qui interagit avec l'objet de l'étude est une partie prenante.

Il peut s'agir de partenaires, « clients », « fournisseurs », sous-traitants directs ou indirects, etc.

L'ensemble des parties prenantes compose l'écosystème.





# Exercice collégial



Pensez-vous que les acteurs suivants sont des parties prenantes ?

Professeurs

Administration

Fournisseurs de matériels

Éditeurs de logiciel

Collégiens

Parents d'élèves

Établir le contexte



# Correction



Pensez-vous que les acteurs suivants sont des parties prenantes ?

Professeurs	✗	Non, ils font partie du collège (ce sont des biens supports)
Administration	✗	Non, toujours pas ! (encore une fois, c'est un bien support)
Fournisseurs de matériels	✓	Là, oui !
Éditeurs de logiciel	✓	Oui
Collégiens	✓	Oui, ils vont au collège mais n'en font pas partie
Parents d'élèves	✓	Oui, ils accèdent aussi au système du collège

Les biens supports font partie du périmètre de l'objet de l'étude. On les « maîtrise ».  
Les parties prenantes font partie de l'écosystème. On ne les maîtrise pas.





# Contexte des exercices à venir

Établir le contexte



Société de biotechnologie fabriquant des vaccins

Estimation d'un niveau de maturité faible en matière de sécurité numérique

Sensibilisation basique à la sécurité du numérique à la prise de poste des salariés

Existence d'une charte informatique



# Exercice en groupes



Décrivez l'objet de l'étude : valeurs métier et biens supports

Recherche & développement (R&D)

Fabriquer des vaccins

Traçabilité et contrôle

Établir le contexte

--	--	--	--	--	--	--	--



# Correction



Décrivez l'objet de l'étude : valeurs métier et biens supports

## Recherche & développement (R&D)

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

## Fabriquer des vaccins

Activité consistant à réaliser :

- le remplissage de seringues (stérilisation, remplissage)
- le conditionnement (étiquetage et emballage)

## Traçabilité et contrôle

Informations permettant d'assurer le contrôle qualité et la libération de lot (ex : antigène, répartition aseptique, conditionnement, libération finale...)

### Serveurs bureautiques (internes)

Serveurs bureautiques permettant de stocker l'ensemble des données de R&D

### Systèmes de production des antigènes

Ensemble de machines et équipements informatiques pour produire des antigènes

Pharmacien de biotechnologies

DSI

### Systèmes de production

Ensemble de machines et équipements informatiques permettant de fabriquer des vaccins à grande échelle

DSI

### Serveurs bureautiques (internes)

Serveurs de stockage des données relatives à la traçabilité et au contrôle des processus

DSI

Établir le contexte



# Exercice en groupes



Décrivez l'écosystème de l'objet de l'étude : parties prenantes

Clients

Partenaires

Sous-traitants

Fournisseurs

Établir le contexte

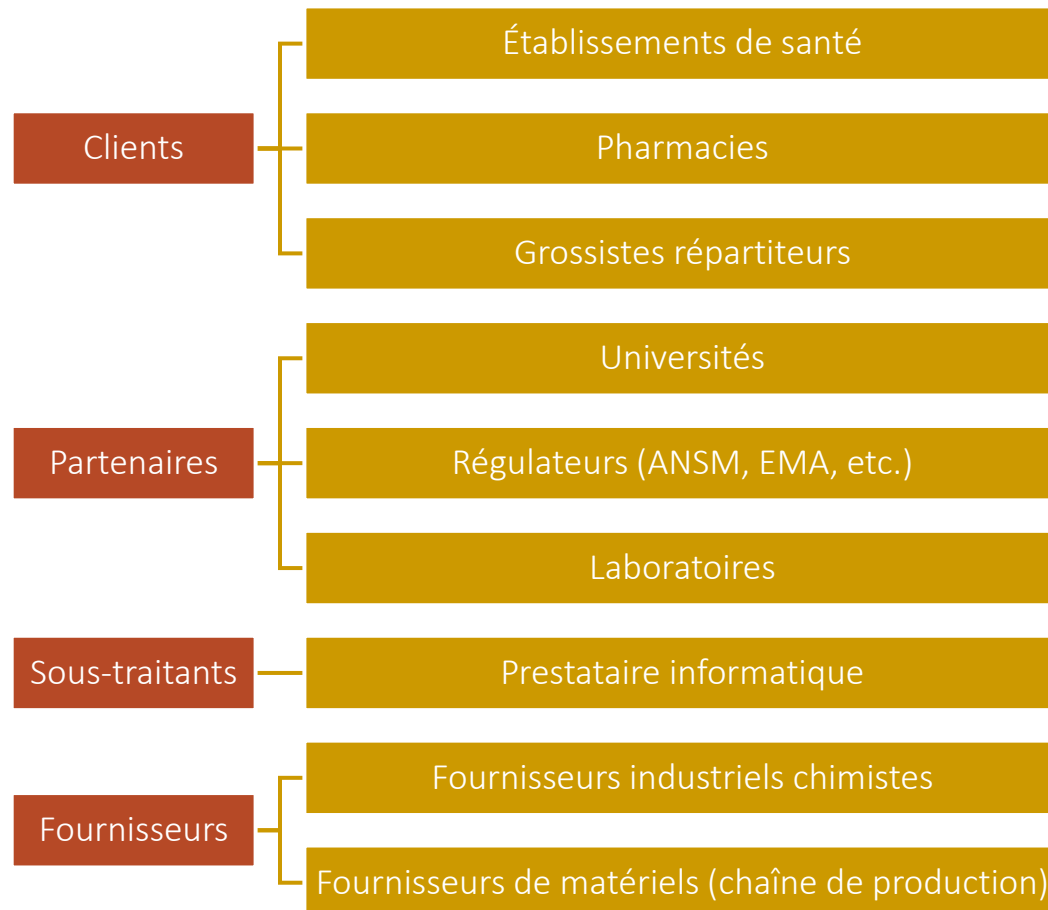


# Correction



Décrivez l'écosystème de l'objet de l'étude : parties prenantes

Établir le contexte





# Conseil pour ne pas se noyer

Limiter le nombre de valeurs métier et de biens supports

Établir le contexte

Il ne s'agit PAS de lister l'intégralité des valeurs métier et biens supports de l'organisme.

Nous ne sommes pas dans une démarche de cartographie du système d'information.

Les valeurs métier qui ne sont pas retenues hériteront des mesures prises pour protéger les autres.



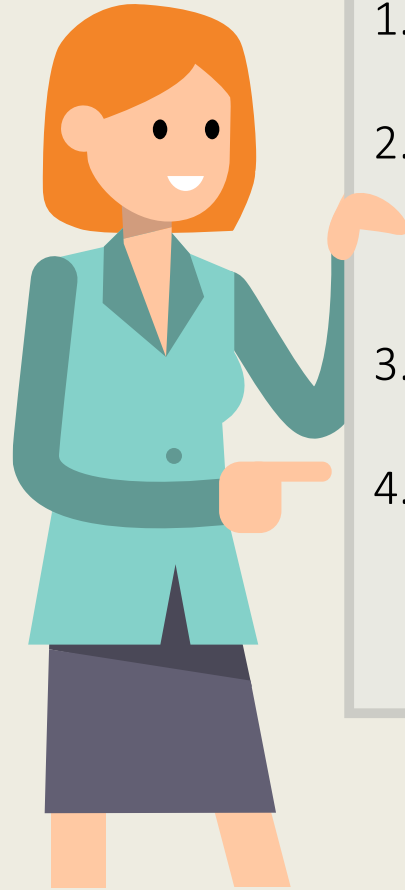
➤ Considérer des ensembles d'informations plutôt que des informations isolées

➤ 5 à 10 valeurs métiers constituent généralement une base suffisante

➤ Ne conserver que les valeurs métiers identifiées comme les plus pertinentes ou sensibles



# Qu'avons-nous appris ?



1. Savoir **cadrer une étude** selon son objectif, son sujet, ses destinataires et le temps
  2. Comprendre qu'il est nécessaire d'impliquer des **profils appropriés** pour mettre en œuvre chaque **outil** d'EBIOS *Risk Manager*
  3. Savoir délimiter et décrire l'objet de l'étude (**missions, valeurs métier** et **biens supports**)
  4. Savoir décrire l'écosystème (**parties prenantes**)
- Maintenant que nous savons de quoi on parle, passons à l'appréciation des risques !



# Plan de la formation

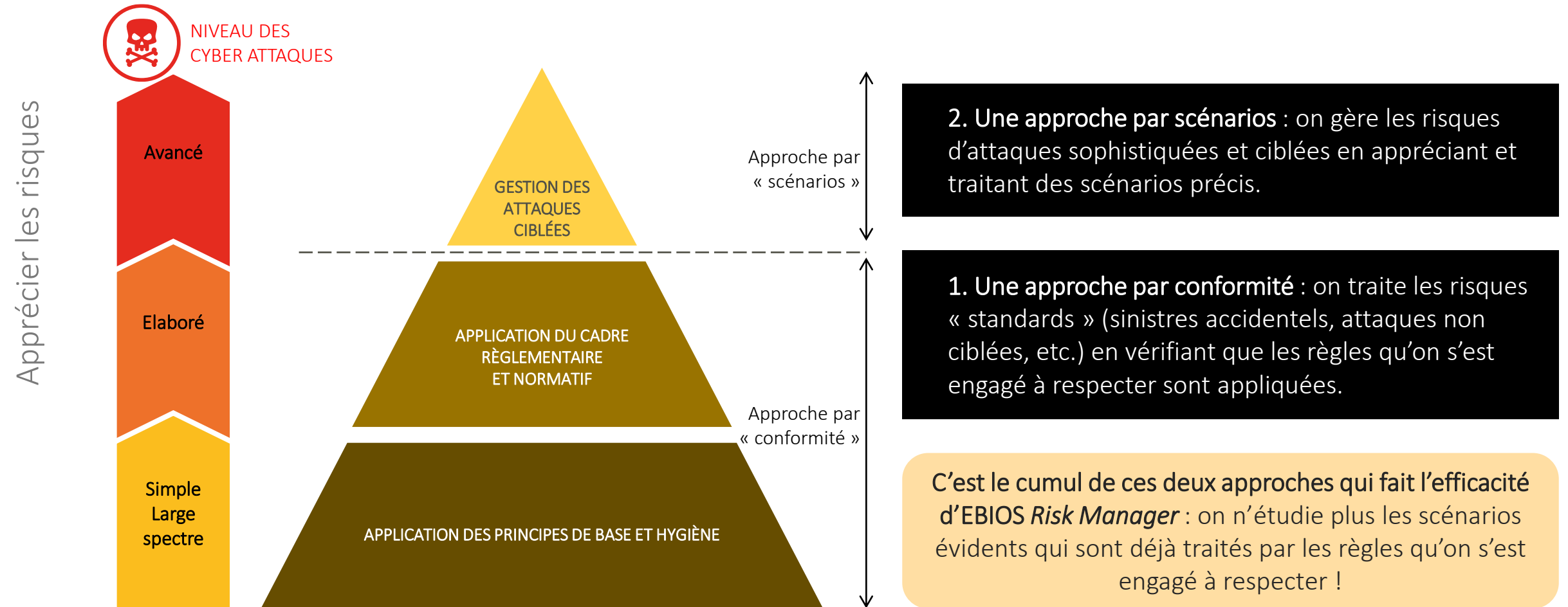
1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. **Apprécier les risques**
  - a. Approche par conformité
  - b. Approche par scénarios
5. Traiter les risques
6. Étude de cas complète
7. Conclusion





# L'efficacité d'EBIOS *Risk Manager*

Deux approches cumulatives pour gérer les risques





# Plan de la formation

1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. Apprécier les risques
  - a. Approche par conformité
  - b. Approche par scénarios
5. Traiter les risques
6. Étude de cas complète
7. Conclusion



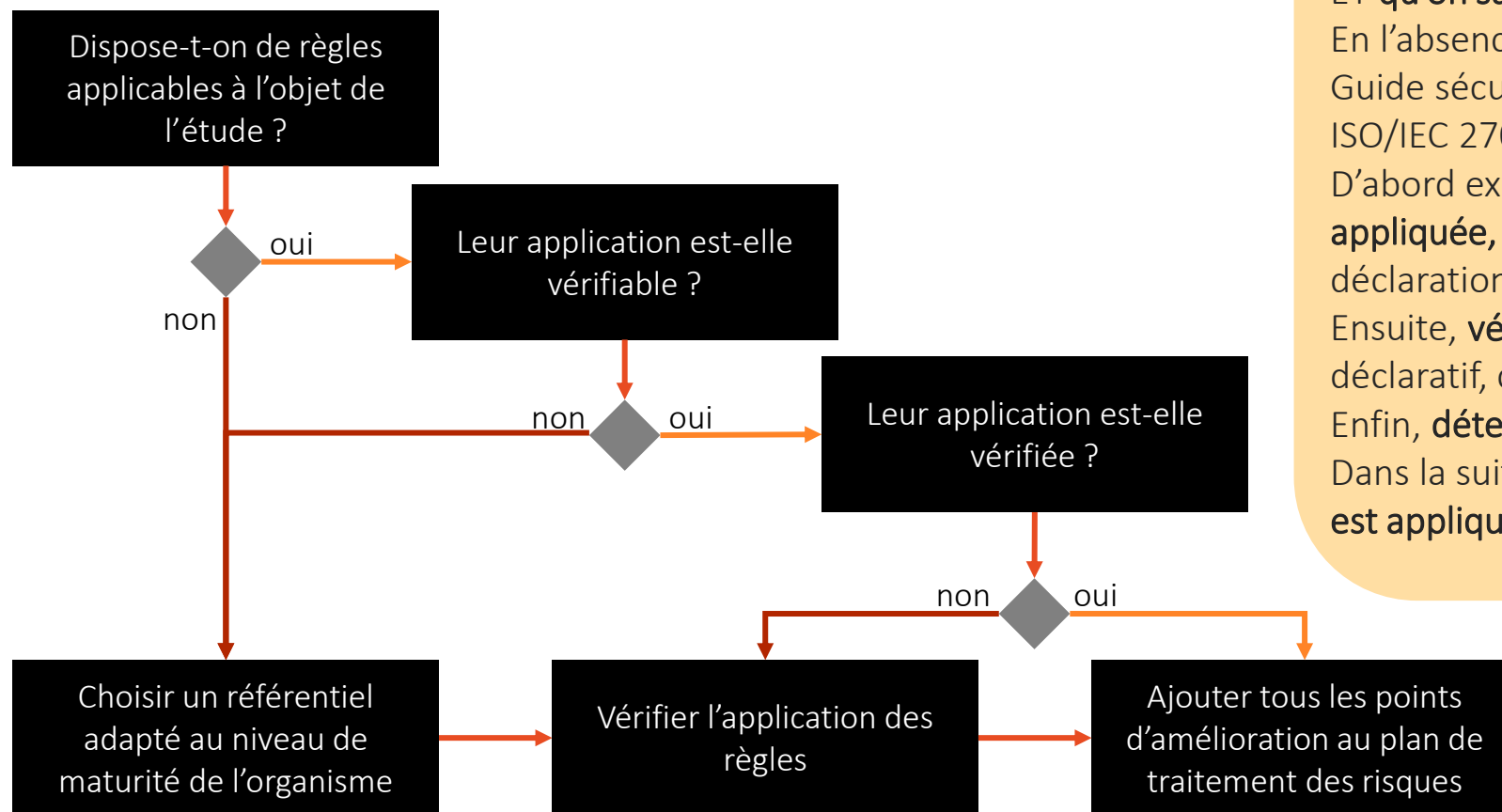
# De quoi va-t-on parler ?





# Outil 05 – Identifier et évaluer le socle de règles

## La mécanique générale



Le socle : règles reconnues comme **applicables** ET **qu'on sait évaluer** (ex : politique SSI).

En l'absence de socle, choisir un « **simple** » (ex : Guide sécurité de la CNIL) ou **générique** (ex : ISO/IEC 27002).

D'abord expliquer **comment chaque règle est appliquée, ou pourquoi elle ne l'est pas** (cf. déclaration d'applicabilité de l'ISO/IEC 27001).

Ensuite, **vérifier l'application** des règles : déclaratif, contrôle interne, audit, etc.

Enfin, **déterminer les actions** pour rectifier.

Dans la suite de l'étude, considérer que **le socle est appliqué**.



# Exercice collégial



Au vu du cas étudié, quels seraient les référentiels à considérer ?

Politique de sécurité (PSSI) de l'organisation

Règlement général sur la protection des données  
(RGPD)

Guide d'hygiène informatique de l'ANSSI

Annexe A de l'ISO/IEC 27001 (bonnes pratiques)

Code de la santé publique

Arrêté sectoriel « produits de santé »

Instruction générale interministérielle 1300 (IGI 1300)



# Correction



Au vu du cas étudié, quels seraient les référentiels à considérer ?

Politique de sécurité (PSSI) de l'organisation



Non, il n'y en a pas...

Règlement général sur la protection des données (RGPD)



Ben non ! Trop large ou applicable à UN traitement

Guide d'hygiène informatique de l'ANSSI



Oui, si l'organisme sait comment l'appliquer

Annexe A de l'ISO/IEC 27001 (bonnes pratiques)



Oui, sauf s'il y a une politique

Code de la santé publique



Non plus, trop large, pas assez directement applicable

Arrêté sectoriel « produits de santé »



Oui, une bonne idée si pas de politique

Instruction générale interministérielle 1300 (IGI 1300)

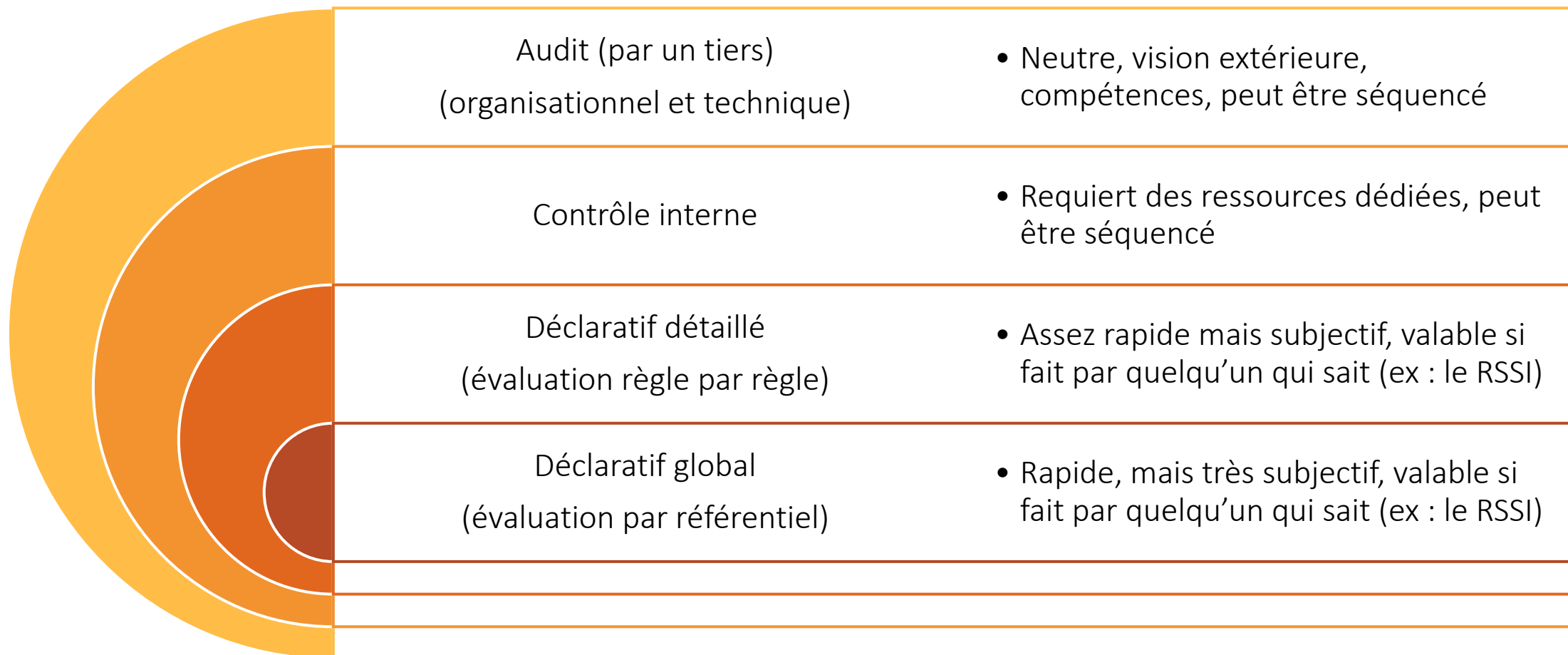


Non, pas applicable aux données non classifiées



# Comment évaluer la conformité au socle ?

Plusieurs solutions cumulables





# Les bonnes pratiques traitent les risques standards et non ciblés

## ISO 27002 Updated Controls List



- Les règles qu'on s'est engagé à respecter suffisent à traiter la plupart des risques
  - Les bonnes pratiques sont reconnues comme efficaces
  - Elles protègent disponibilité, intégrité et confidentialité des données
  - Les causes accidentelles
  - Les causes délibérées
- Des vérifications doivent toutefois être faites
  - Sont-elles réellement appliquées ?
  - Ne peuvent-elles pas être améliorées ?





# Mesures



Peut-on déterminer des mesures sur le socle de règles ?

- Oui ! On peut d'ores-et-déjà déterminer des mesures complémentaires au socle
  - Corriger les écarts
  - Améliorer les règles, notamment dans 3 cas
    - Si elles sont mal comprises
    - Si elles sont difficilement appliquées
    - Si elles divergent trop des bonnes pratiques (ISO/IEC 27002, recommandations de l'ANSSI, etc.)

**Quid des éventuelles mesures déterminées à ce stade ?**

Elles sont ajoutées au plan de traitement des risques

Elles peuvent être considérées comme mises en œuvre dans la suite de l'étude



# Qu'avons-nous appris ?



1. Comprendre qu'un socle **inapplicable ou invérifiable** n'est pas un socle
  2. Savoir **choisir son socle**
  3. Bien comprendre qu'on **vient de traiter les risques standards**, et que maintenant, on ne va étudier sous forme de scénarios que les risques spécifiques et ciblés
- Maintenant, l'approche par scénarios !



# Plan de la formation

1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. **Apprécier les risques**
  - a. Approche par conformité
  - b. **Approche par scénarios**
5. Traiter les risques
6. Étude de cas complète
7. Conclusion



# De quoi va-t-on parler ?





# Des scénarios par raffinements successifs

Une appréciation progressive des risques





# Outil 06 – Identifier et analyser les événements redoutés

## Que doit-on craindre ?



### Quels cas va-t-on étudier ?

- La perte de **disponibilité** : quels seraient les conséquences si chaque valeur métier disparaissait ?
- La perte d'**intégrité** : quels seraient les conséquences si chaque valeur métier était modifiée de manière non désirée ?
- La perte de **confidentialité** : quels seraient les conséquences si chaque valeur métier était connue de personnes non autorisées ?



### Quelles conséquences va-t-on analyser ?

- Conséquences **sur l'organisation**
  - Conséquence sur le fonctionnement
  - Conséquence financière
  - Conséquences sur l'image
  - Conséquence juridique
  - etc.
- Conséquences **au-delà de l'organisation**
  - Conséquence sur les droits et libertés des personnes
  - Conséquence sur l'environnement
  - Conséquence sur les parties prenantes
  - etc.

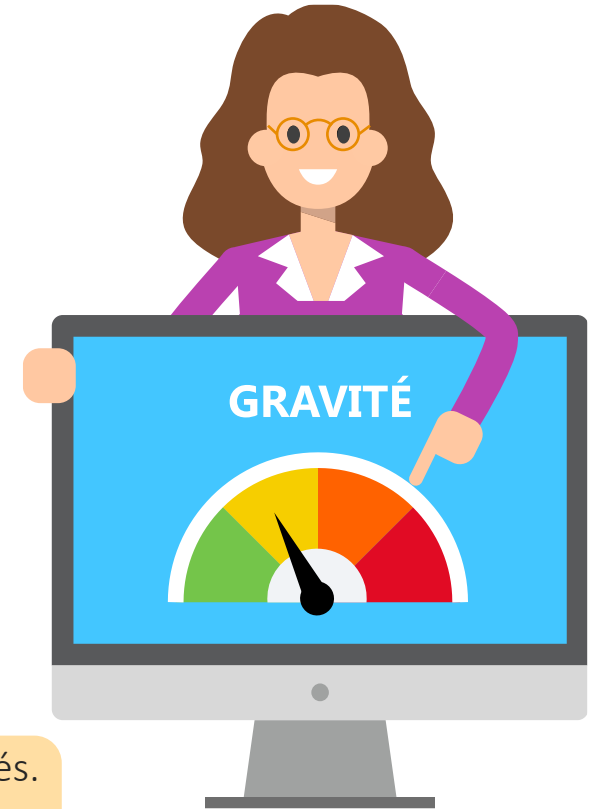


# Comment estimer la gravité ?

Une échelle pour toutes les conséquences – Exemple issu des guides

Gravité	Description
1. Mineure	Aucune conséquence opérationnelle ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges)
2. Significative	Dégradation des performances de l'activité sans conséquence sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé)
3. Importante	Forte dégradation des performances de l'activité, avec d'éventuelles conséquences significatives sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé)
4. Critique	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuelles conséquences graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée)

Dans ce cas, il conviendra de décrire les conséquences potentielles des événements redoutés. Il est recommandé de reprendre la même échelle de gravité définie dans la politique de l'organisme ou utilisée dans les autres études de risques.





# Comment estimer la gravité ?

Une échelle explicite par type de conséquences – Exemple d'une PME

Établissement du contexte

Gravité	Conséquences financières	Conséquences fonctionnelles	Conséquences sur l'image	Conséquences juridiques	Conséquences business	Conséquences sur la vie privée
1. Minimale	Aucun ou seulement quelques dizaines ou centaines d'euros annuels	Aucun ou seulement dégradation fonctionnelle avec peu de conséquence sur un processus	Aucun ou conséquence négligeable sur l'image	Aucun ou seulement sanction interne	Aucun ou seulement perte de petits prospects	Aucun ou seulement désagrément matériel, moral ou physique négligeable (ex : <i>spam</i> )
2. Limitée	Milliers d'euros annuels	Dégradation fonctionnelle limité sur un processus	Image impactée, mais de manière circonscrite et temporaire	Pénalités contractuelles avec des petits clients	Perte de petits clients	Désagrément matériel, moral ou physique significatif, qui pourra être surmonté après quelques difficultés
3. Importante	Dizaines de milliers d'euros annuels	Dégradation fonctionnelle limité sur plusieurs processus	Image atteinte de manière publique, mais limitée dans le temps	Pénalités contractuelles fortes (avec des grands comptes), mention dans une affaire civile ou pénale, non-respect de la loi et de la réglementation (protection de la vie privée notamment), enquête administrative, condamnation ou amende	Perte de grands comptes (clients ou prospects)	Conséquence matérielle, morale ou physique qui ne sera surmontée qu'avec difficultés
4. Maximale	Centaines de milliers d'euros annuels	Arrêt fonctionnel sur l'ensemble des processus	Image dégradée de manière profonde et durable	Non-respect majeur de la loi et de la réglementation (protection de la vie privée notamment), condamnation pénale, pénalités contractuelles avec plusieurs acteurs	Perte massive de clients	Conséquence matérielle, morale ou physique qui pourrait ne pas être surmontée

La meilleure échelle, c'est celle qui est comprise par tous ! Elle est explicite (non ambiguë), non recouvrante (les niveaux ne se chevauchent pas), et elle permet d'étaler largement les événements redoutés (ils n'ont pas tous la même valeur)





# Exercice

Analysez et estimez les principaux événements redoutés



Valeur métier	Événement redouté	Types de conséquences	Gravité
R&D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée	<ul style="list-style-type: none"><li>• Conséquences sur la sécurité ou la santé des personnes</li><li>• Conséquences sur l'image et la confiance</li><li>• Conséquences juridiques</li></ul>	
Fabriquer des vaccins			
Traçabilité et contrôle			



# Correction



À l'issue, on a une liste hiérarchisée des événements redoutés

Valeur métier	Événement redouté	Types de conséquences	Gravité
R&D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée	<ul style="list-style-type: none"><li>• Conséquences sur la sécurité ou la santé des personnes</li><li>• Conséquences sur l'image et la confiance</li><li>• Conséquences juridiques</li></ul>	3
	Fuite des informations d'études et recherches de l'entreprise	<ul style="list-style-type: none"><li>• Conséquences sur le patrimoine intellectuel</li><li>• Conséquences financières</li></ul>	3
	Perte ou destruction des informations d'études et recherches	<ul style="list-style-type: none"><li>• Conséquences sur les missions et services de l'organisme</li><li>• Conséquences sur les coûts de développement</li><li>• Conséquences sur le patrimoine intellectuel</li></ul>	2
	Interruption des phases de tests des vaccins pendant plus d'une semaine	<ul style="list-style-type: none"><li>• Conséquences sur les missions et services de l'organisme</li><li>• Conséquences financières</li></ul>	2
Fabriquer des vaccins	Fuite du savoir-faire de l'entreprise concernant le processus de fabrication des vaccins et de leurs tests qualité	<ul style="list-style-type: none"><li>• Conséquences financières</li></ul>	2
	Interruption de la production ou de la distribution de vaccins pendant plus d'une semaine pendant un pic d'épidémie	<ul style="list-style-type: none"><li>• Conséquences sur la sécurité ou la santé des personnes</li><li>• Conséquences sur l'image et la confiance</li><li>• Conséquences financières</li></ul>	4
Traçabilité et contrôle	Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire	<ul style="list-style-type: none"><li>• Conséquences sur la sécurité ou la santé des personnes</li><li>• Conséquences sur l'image et la confiance</li><li>• Conséquences juridiques</li></ul>	4



# Mesures



Peut-on déterminer des mesures sur les événements redoutés ?

- Oui ! On peut d'ores-et-déjà déterminer des mesures complémentaires au socle
  - Agir sur les valeurs métier
    - Leur existence : écarter des données ou des activités qui engendrent les risques trop élevés
    - Leur disponibilité : haute disponibilité, sauvegardes, etc.
    - Leur intégrité : empreintes, signature, etc.
    - Leur confidentialité : classification, chiffrement, pseudonymisation, anonymisation, etc.
  - Agir sur les conséquences
    - Limiter leur ampleur : exercices, préparation de crise, etc.
    - Compenser de manière proactive : provisionner, assurance, etc.

**Quid des éventuelles mesures déterminées à ce stade ?**

Elles sont ajoutées au plan de traitement des risques

Elles peuvent être considérées comme mises en œuvre dans la suite de l'étude



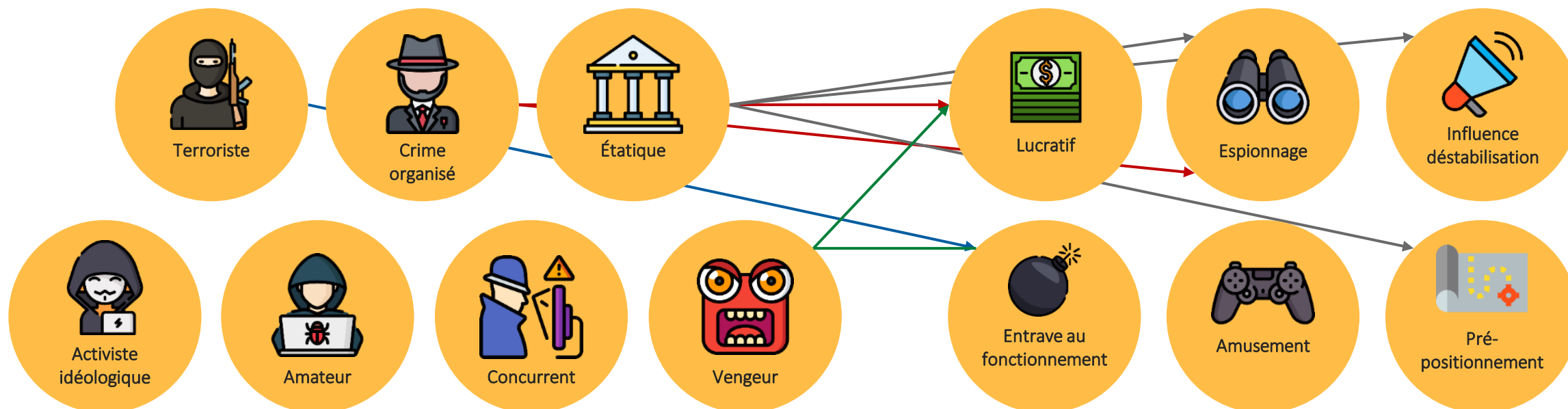
# Outil 07 – Analyser les sources de risques

À quels attaquants est-on exposé ?



Quelles sources de risques  
considérer ?

Quels sont leurs objectifs ?





# Exercice collégial

Identifiez les composants de risques depuis l'article



**Un adolescent de 15 ans « pirate » le système de son collège pour améliorer ses notes**

*Un adolescent de quinze ans a été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires.*

*Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité pendant quatre jours.*

[Source : Le Point.fr et ZDNet]

Composants	Première attaque	Seconde attaque
Valeur métier		
Bien support		
Évènement redouté		
Conséquences		
Source de risque		
Objectif visé		



# Exercice collégial

Identifiez les composants de risques depuis l'article



**Un adolescent de 15 ans « pirate » le système de son collège pour améliorer ses notes**

*Un adolescent de quinze ans a été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires.*

*Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité pendant quatre jours.*

[Source : Le Point.fr et ZDNet]

Composants	Première attaque	Seconde attaque
Valeur métier	Résultats scolaires (information)	
Bien support	Système informatique de gestion des résultats scolaires	
Évènement redouté	Les résultats scolaires d'un ou plusieurs collégiens sont erronées	
Conséquences	<ul style="list-style-type: none"><li>• Conséquence sur la poursuite d'études des collégiens</li><li>• Conséquence sur l'image vis-à-vis des autres établissements scolaires</li></ul>	
Source de risque	Un élève	
Objectif visé	Modifier ses résultats scolaires	



# Exercice collégial

Identifiez les composants de risques depuis l'article



## Un adolescent de 15 ans « pirate » le système de son collège pour améliorer ses notes

*Un adolescent de quinze ans a été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires.*

*Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité pendant quatre jours.*

[Source : Le Point.fr et ZDNet]

Composants	Première attaque	Seconde attaque
Valeur métier	Résultats scolaires (information)	Échanger des informations
Bien support	Système informatique de gestion des résultats scolaires	Service informatique d'échange de courriels
Évènement redouté	Les résultats scolaires d'un ou plusieurs collégiens sont erronées	Les échanges avec les collégiens ou leurs familles sont impossibles pendant plusieurs jours
Conséquences	<ul style="list-style-type: none"><li>• Conséquence sur la poursuite d'études des collégiens</li><li>• Conséquence sur l'image vis-à-vis des autres établissements scolaires</li></ul>	<ul style="list-style-type: none"><li>• Conséquence sur l'image vis-à-vis des familles</li><li>• Conséquence sur les missions et services du collège</li></ul>
Source de risque	Un élève	Un élève
Objectif visé	Modifier ses résultats scolaires	Se venger du collège



# Comment estimer la pertinence des sources de risques / objectifs visés ?

Établissement du contexte

		RESSOURCES			
		Incluant les ressources financières, le niveau de compétences cyber, l'outillage, 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





# Exercice

Analysez et estimez les principales sources de risques



Sources de risque	Objectifs visés	Motivation	Ressources	Pertinence
Hacktiviste	Divulguer des informations sur les tests animaliers			

Dans ce contexte, les couples sources de risques / objectifs visés « très pertinents » et « plutôt pertinents » seront retenus pour la suite de l'étude.



# Correction



À l'issue, on a une liste hiérarchisée des sources de risques

Sources de risque	Objectifs visés	Motivation	Ressources	Pertinence
Hacktiviste	Divulguer des informations sur les tests animaliers	Peu motivé	Ressources significatives	Moyennement pertinent
Hacktiviste	Saboter la campagne nationale de vaccination	Assez motivé	Ressources significatives	Plutôt pertinent
Concurrent	Voler des informations	Fortement motivé	Ressources importantes	Très pertinent
Cyber-terroriste	Altérer la composition des vaccins à des fins de bioterrorisme	Peu motivé	Ressources limitées	Peu pertinent

Dans ce contexte, les couples sources de risques / objectifs visés « très pertinents » et « plutôt pertinents » seront retenus pour la suite de l'étude.

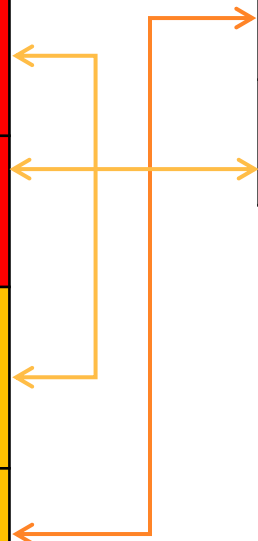


# Il faut ensuite « raccrocher » les composants...



Événements redoutés 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

Sources de risques / objectifs visés les plus pertinents	
Sources de risque	Objectif visé
Concurrent	Voler des informations
Hacktiviste	Saboter la campagne nationale de vaccination





# Autre technique

## Analyse directe par événement redouté



Valeur métier	Événement redouté	Gravité	Source de risques	Objectifs visés
Fabriquer des vaccins	Interruption de la production ou de la distribution de vaccins pendant plus d'une semaine pendant un pic d'épidémie	4	Hacktiviste	Saboter la campagne nationale de vaccination
Traçabilité et contrôle	Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire	4	Hacktiviste	Saboter la campagne nationale de vaccination
R&D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée	3	Hacktiviste	Saboter la campagne nationale de vaccination
R&D	Fuite des informations d'études et recherches de l'entreprise	3	Concurrent	Voler des informations



# Mesures



Peut-on déterminer des mesures sur les sources de risques ?

- Oui ! On peut d'ores-et-déjà déterminer des mesures complémentaires au socle
  - Agir sur les mesures en place
    - Vérifier qu'elles sont au niveau des sources de risques, les renforcer sinon
    - Détection et protection face aux attaques connues de sources de risques retenues
  - Agir sur les sources de risques / objectifs visés
    - Communiquer pour tenter de dissuader

Quid des éventuelles mesures déterminées à ce stade ?

Elles sont ajoutées au plan de traitement des risques

Elles peuvent être considérées comme mises en œuvre dans la suite de l'étude



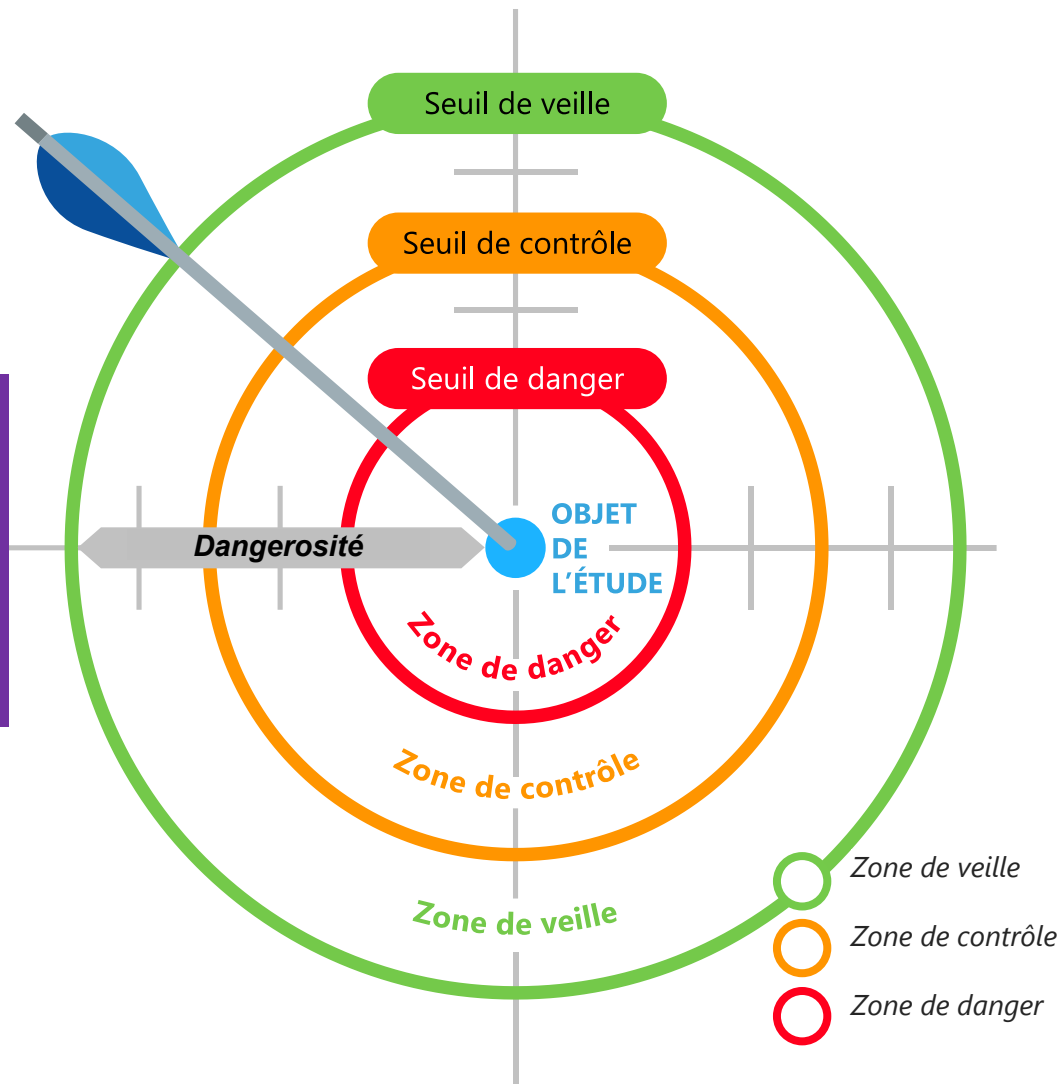
# Outil 08 – Analyser les parties prenantes

EXPOSITION
<b>Dépendance</b> La relation avec cette partie prenante est-elle vitale pour mon activité ?
<b>Pénétration</b> Dans quelle mesure la partie prenante accède-t-elle à mes ressources internes ?

FIABILITÉ CYBER
<b>Maturité cyber</b> Quelles sont les capacités de la partie prenante en matière de sécurité ?
<b>Confiance</b> Est-ce que les intentions ou les intérêts de la partie prenante peuvent m'être contraires ?



$$\text{Dangerosité} = \frac{\text{Pénétration} \times \text{Dépendance}}{\text{Maturité cyber} \times \text{Confiance}}$$





# Comment estimer la dangerosité des parties prenantes ?

## Exemple d'échelle

Établissement du contexte

Niveau	Dépendance	Pénétration	Maturité cyber	Confiance
1. Minimale	Pas de lien avec le SI de la partie prenante pour réaliser la mission.	Pas d'accès ou accès avec des privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, ordiphone, etc.).	Des règles d'hygiène sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne sont pas connues.
2. Faible	Lien avec le SI de la partie prenante utile à la réalisation de la mission.	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux bureaux de l'organisme.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est assurée selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
3. Importante	Lien avec le SI de la partie prenante indispensable mais non exclusif (possible substitution).	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4. Maximale	Lien avec le SI de la partie prenante indispensable et unique (pas de substitution possible).	Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires d'entreprise, DNS, DHCP, <i>switchs</i> , pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs de l'organisme.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et prend pleinement en compte une dimension proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.



# Exemple



Parties prenantes	Dépendance	Pénétration	Maturité cyber	Confiance	Dangerosité
Professeur	<b>3. Importante</b> → Assure la saisie des notes	<b>1. Minimale</b> → Droits simples d'utilisateur, en écriture sur toutes les notes	<b>1. Minimale</b> → Aucune	<b>4. Maximale</b> → Membre de l'éducation nationale	$(3 \times 1) / (1 \times 4) = 0,75$
Administration	<b>4. Maximale</b> → Compilation	<b>2. Faible</b> → Accès privilégié pour gérer les informations de l'élève	<b>2. Faible</b> → A suivi une formation et une sensibilisation obligatoire	<b>4. Maximale</b> → Membre de l'éducation nationale	$(4 \times 2) / (2 \times 4) = 1$
Élève	<b>1. Minimale</b>	<b>1. Minimale</b> → Droits simples d'utilisateur	<b>1. Minimale</b> → Aucune	<b>1. Minimale</b> → Intention inconnue	$(1 \times 1) / (1 \times 1) = 1$
Parents	<b>1. Minimale</b>	<b>1. Minimale</b> → Droits simples d'utilisateur	<b>1. Minimale</b> → Aucune	<b>1. Minimale</b> → Intention inconnue	$(1 \times 1) / (1 \times 1) = 1$





# Exercice en groupes

Estimez les critères et calculez la dangerosité des parties prenantes



Catégorie	Nom	Dépendance	Pénétration	Maturité cyber	Confiance	Dangerosité
Client	C1 - Établissements de santé					
Client	C2 - Pharmacies					
Client	C3 - Grossistes répartiteurs					
Partenaire	P1 - Universités					
Partenaire	P2 - Régulateurs (ANSM, EMA...)					
Partenaire	P3 - Laboratoires					
Prestataire	F1 - Fournisseurs industriels chimistes					
Prestataire	F2 - Fournisseurs de matériel (chaîne de production)					
Prestataire	F3 - Prestataire informatique					



# Exercice en groupes

Représentez les parties prenantes sur la cible



## CLIENTS

C1 • Etablissements de santé

C2 • Pharmacies

C3 • Dépositaires &  
Grossistes répartiteurs

## PRESTATAIRES

F3 • Prestataire informatique

F2 • Fournisseurs de matériel

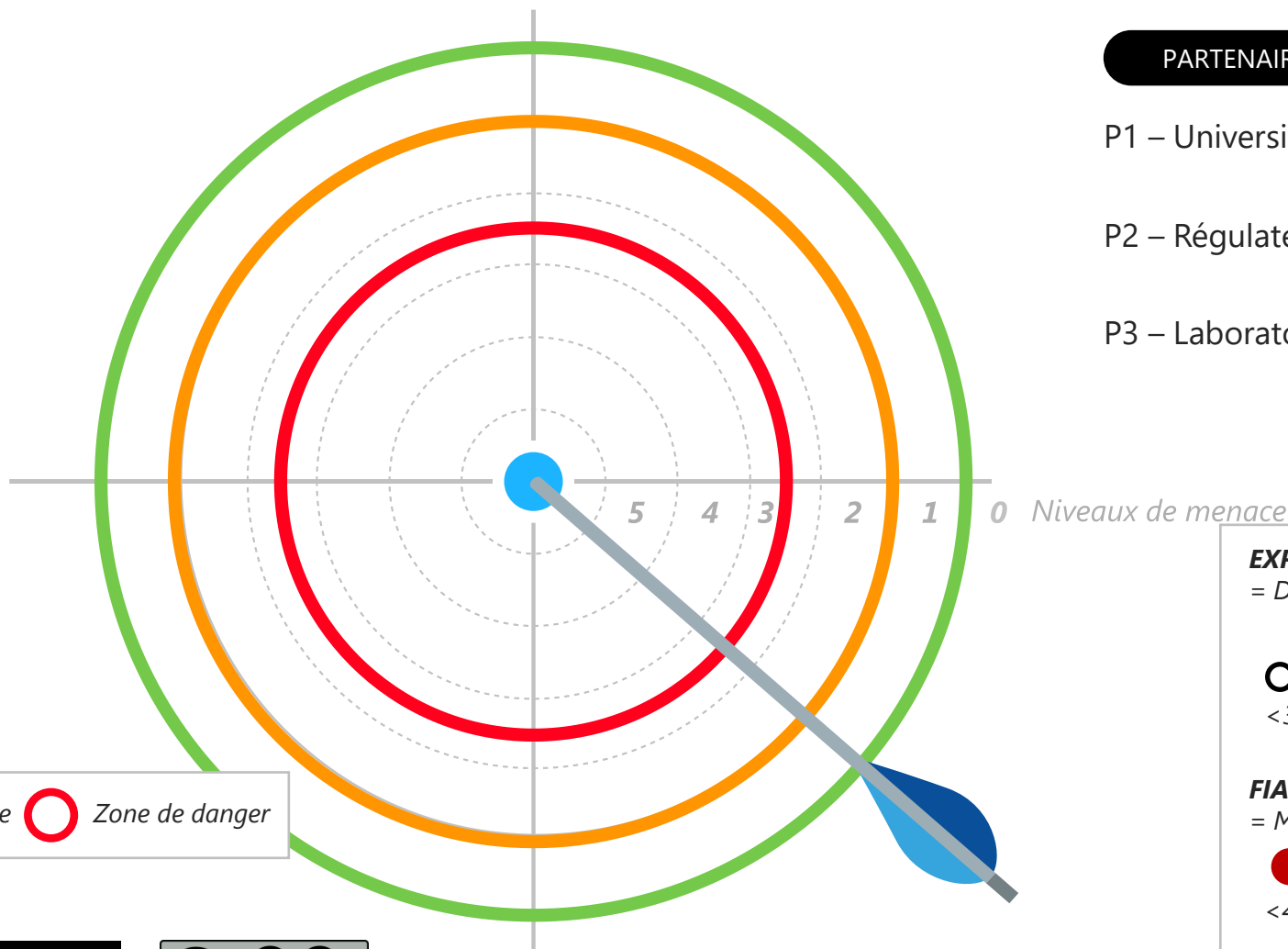
F1 • Fournisseurs  
industriels chimistes

## PARTENAIRES

P1 – Universités

P2 – Régulateurs

P3 – Laboratoires



Zone de veille Zone de contrôle Zone de danger

### EXPOSITION

= Dépendance x Pénétration



### FIABILITE CYBER

= Maturité cyber x Confiance





# Correction

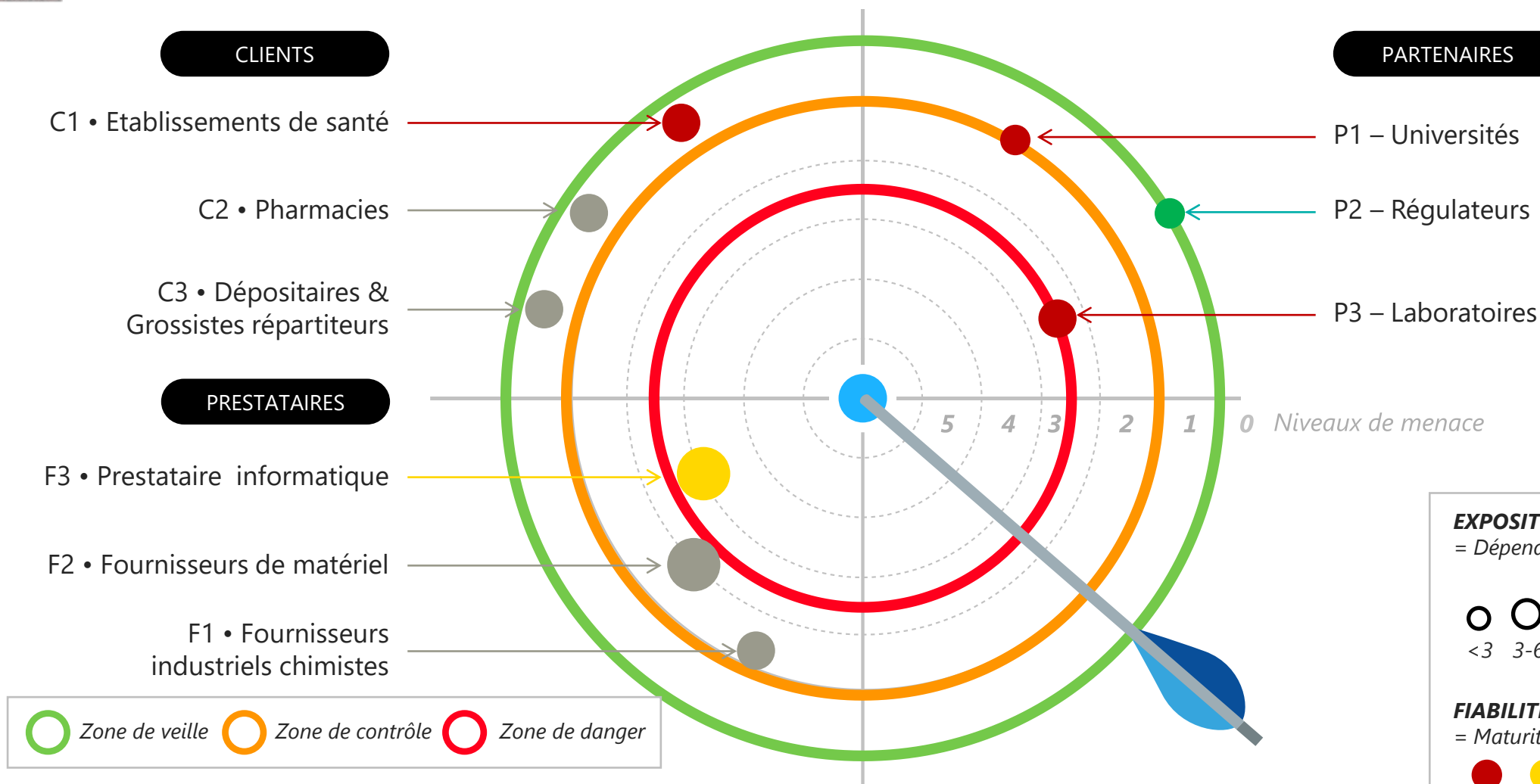


À l'issue, on a une liste hiérarchisée de parties prenantes

Catégorie	Nom	Dépendance	Pénétration	Maturité cyber	Confiance	Dangerosité
Client	C1 - Établissements de santé	1. Minimale	1. Minimale	1. Minimale	3. Importante	0,3
Client	C2 - Pharmacies	1. Minimale	1. Minimale	2. Faible	3. Importante	0,2
Client	C3 - Grossistes répartiteurs	1. Minimale	2. Faible	2. Faible	3. Importante	0,3
Partenaire	P1 - Universités	2. Faible	1. Minimale	1. Minimale	2. Faible	1
Partenaire	P2 - Régulateurs (ANSM, EMA...)	2. Faible	1. Minimale	2. Faible	4. Maximale	0,25
Partenaire	P3 - Laboratoires	3. Importante	3. Importante	2. Faible	2. Faible	2,25
Prestataire	F1 - Fournisseurs industriels chimistes	4. Maximale	2. Faible	2. Faible	3. Importante	1,3
Prestataire	F2 - Fournisseurs de matériel (chaîne de production)	4. Maximale	3. Importante	2. Faible	3. Importante	2
Prestataire	F3 - Prestataire informatique	3. Importante	4. Maximale	2. Faible	2. Faible	3



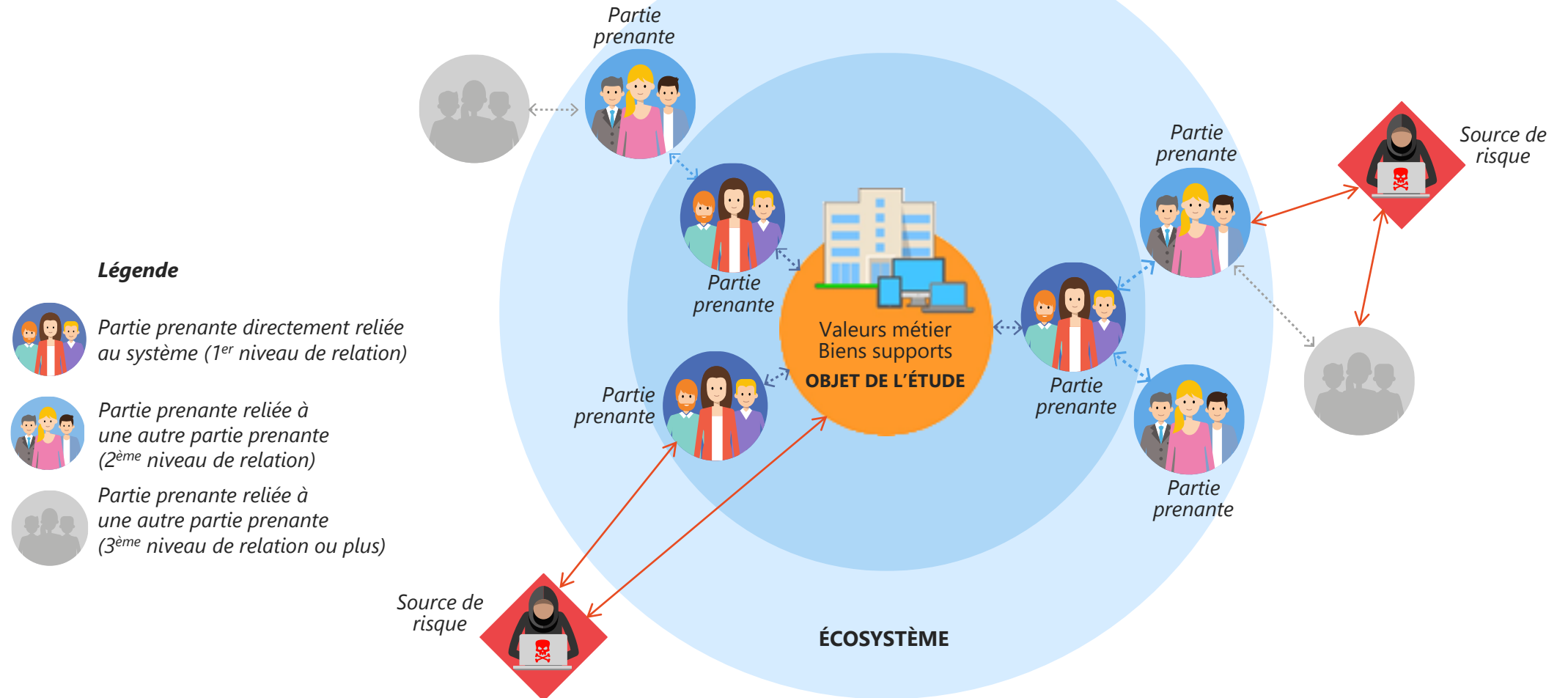
# Correction (suite)





# Outil 09 – Analyser les scénarios stratégiques

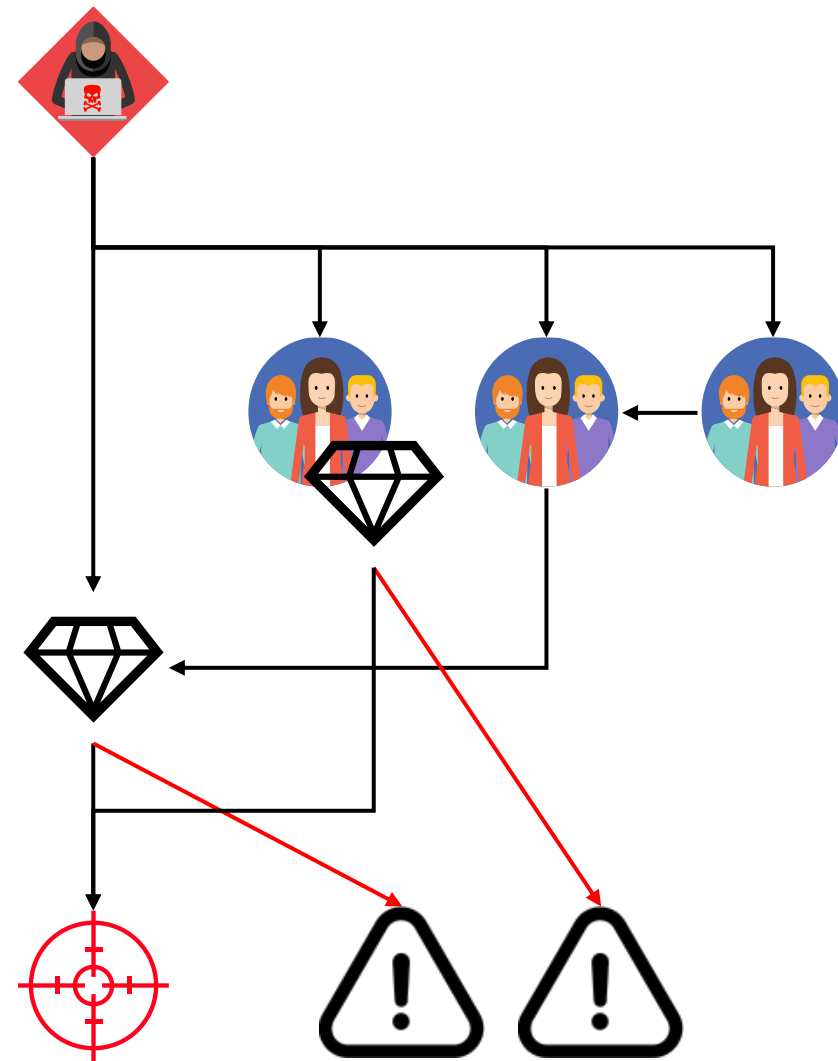
Quels chemins dans l'écosystème ?





# La démarche

- Pour chaque source de risques, on crée un scénario stratégique :
  - Quel est son objectif visé ?
  - Pour l'atteindre, la source de risque peut-elle :
    - s'attaquer directement à l'objet de l'étude ?
    - s'attaquer à une partie prenante qui détient une partie des valeurs métier ?
    - passer par une ou plusieurs parties prenantes pour s'attaquer à l'objet de l'étude ?
  - On ajoute autant de chemins d'attaques que de cas envisagés
  - Quels sont les événements redoutés concernés ?
- On peut utilement scinder ou fusionner ou regrouper des scénarios stratégiques





# Exemple



Source de risque : Élève

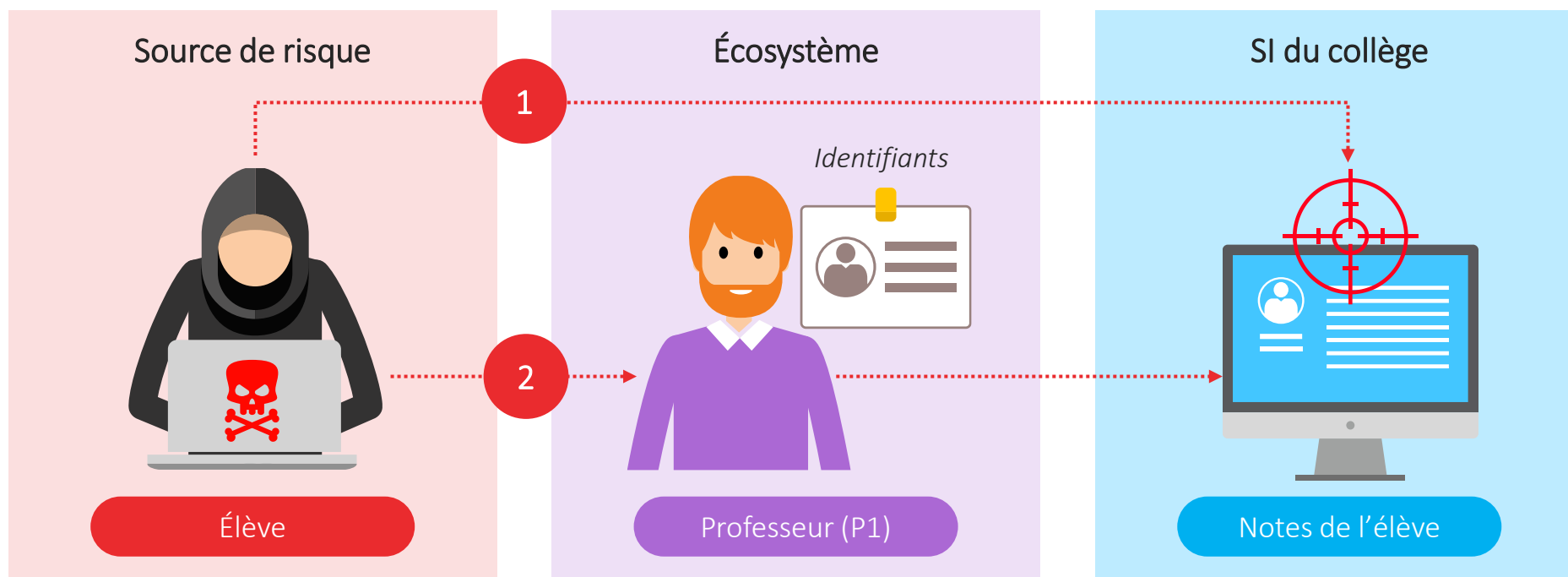
Objectif visé : Modifier ses notes

Événement redouté : Les résultats scolaires d'un ou plusieurs collégiens sont erronés



Gravité  
3

Ce scénario stratégique est composé de 2 chemins d'attaque





# Exercice collégial

Analysez les chemins d'attaques de la source de risques



Source de risque : Concurrent

Objectif visé : Voler des informations

Événement redouté : Fuite des informations  
d'études et recherches de l'entreprise



Gravité

3

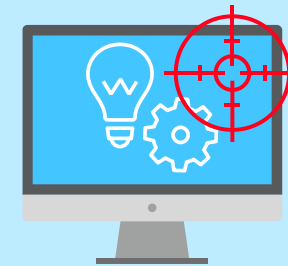
Source de risque



Concurrent

Écosystème

Société de biotechnologie



Informations de R&D





# Correction



Source de risque : Concurrent

Objectif visé : Voler des informations

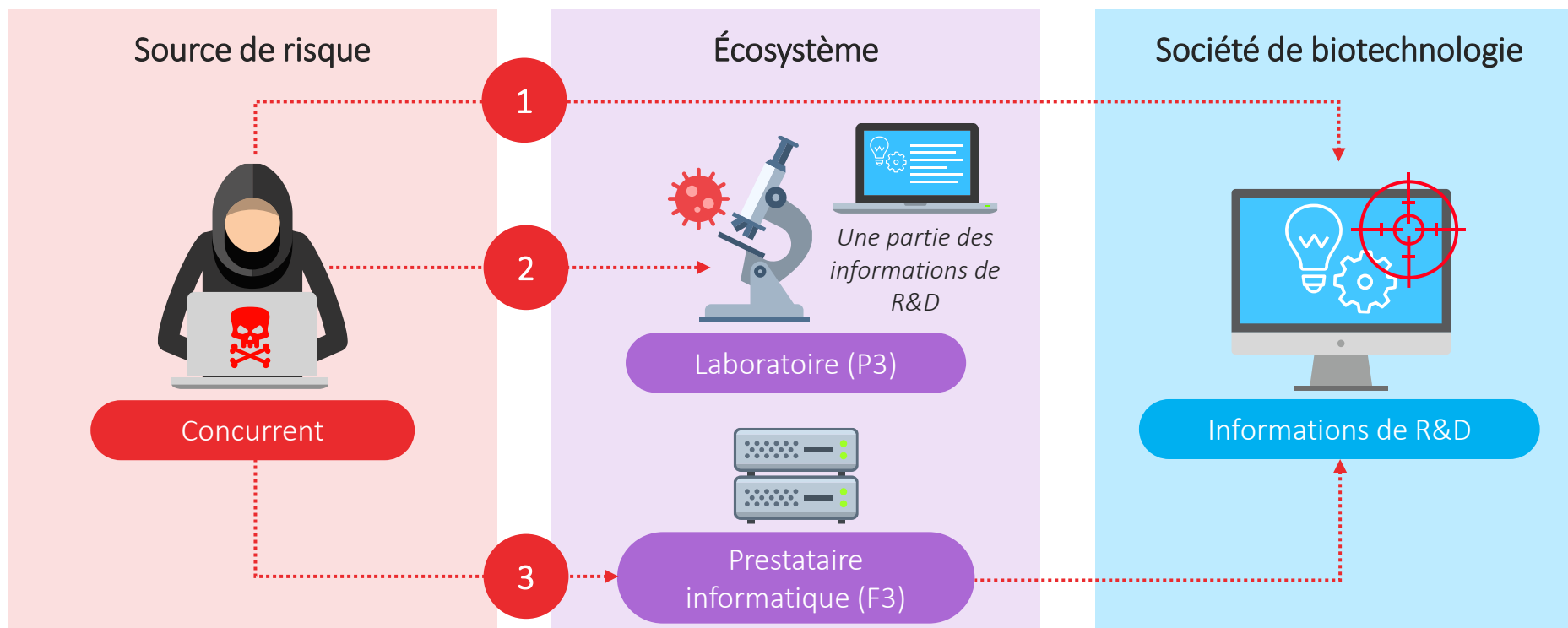
Événement redouté : Fuite des informations d'études et recherches de l'entreprise



Gravité

3

Ce scénario stratégique est composé de 3 chemins d'attaque





# Mesures



Peut-on déterminer des mesures sur les parties prenantes ?

- Oui ! On peut d'ores-et-déjà déterminer des mesures complémentaires au socle
  - Agir sur l'exposition
    - Réduire la dépendance : interroger les choix de partenaires, identifier des substitutions
    - Réduire la pénétration : réduire les droits, réduire les données traitées, internaliser, etc.
  - Agir sur la fiabilité cyber
    - Améliorer la maturité cyber : imposer des règles (ex : clauses types dans les contrats), aider à progresser / vérifier la sécurité (ex : questionnaire, audit, sensibilisation), etc.
    - Améliorer la confiance : demander des garanties (ex : certification), changer de partenaire

Quid des éventuelles mesures déterminées à ce stade ?

Elles sont ajoutées au plan de traitement des risques

Elles peuvent être considérées comme mises en œuvre dans la suite de l'étude



# Exemple



Partie prenante	Dépendance	Pénétration	Maturité cyber	Confiance	Dangerosité
Professeur (P1)	3. Importante → Assure la saisie des notes	1. Minimale → Droits simples d'utilisateur, en écriture sur toutes les notes	1. Minimale → Aucune	4. Maximale → Membre de l'éducation nationale	0,75

Afin de limiter la criticité du professeur, il conviendrait de baisser son niveau d'exposition (dépendance et/ou pénétration) et/ou d'augmenter son niveau de fiabilité cyber (maturité cyber et/ou confiance).

Partie prenante	Chemin(s) d'attaque	Mesure de sécurité	Dangerosité initiale	Dangerosité résiduelle
Professeur (P1)	N°2	<b>Pénétration (1→1)</b> Limiter les droits en édition aux seuls élèves du professeur et dans la matière qu'il enseigne <b>Maturité cyber (1→2)</b> Sensibiliser régulièrement sur l'hygiène informatique et l'ingénierie sociale	0,75	0,375



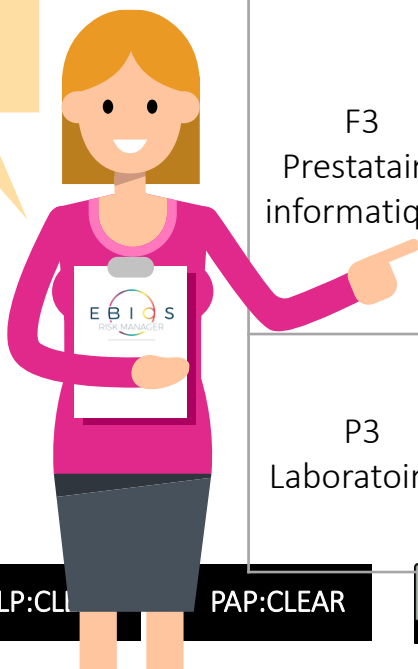
# Exercice collégial



Déterminez des mesures et estimez la dangerosité résiduelle

Pour le scénario stratégique  
« le concurrent vole les  
travaux de recherche »,  
quelles mesures  
proposez-vous pour le  
prestataire informatique et  
les laboratoires (F3 et P3) ?

Quelle serait  
l'efficacité  
de ces mesures ?



Partie prenante	Chemin d'attaque	Mesures	Dangerosité initiale	Dangerosité résiduelle
F2 Fournisseur de matériel	Arrêt de production par compromission de l'équipement de maintenance	Réduire le risque de piègeage des équipements de maintenance utilisés sur le système industriel. Dotation de matériels de maintenance administrés par la DSI et qui seront mis à disposition du prestataire sur site.	2	1,3
F3 Prestataire informatique	Vol d'informations en passant par le prestataire informatique		3	
P3 Laboratoires	Vol d'informations sur le système d'information du laboratoire		2,25	



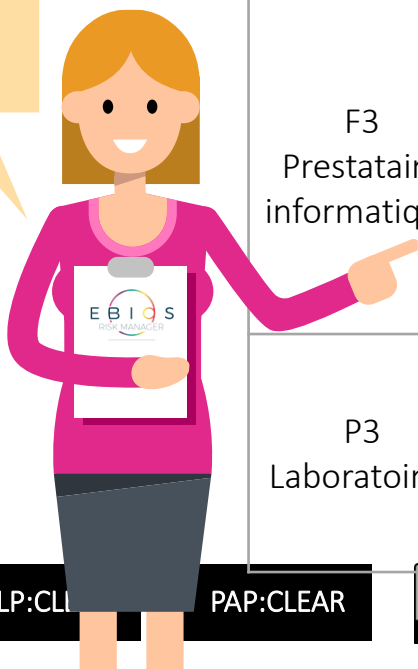
# Correction



Traiter les risques

*Pour le scénario stratégique  
« le concurrent vole les  
travaux de recherche »,  
quelles mesures  
proposez-vous pour le  
prestataire informatique et  
les laboratoires (F3 et P3) ?*

*Quelle serait  
l'efficacité  
de ces mesures ?*



Partie prenante	Chemin d'attaque	Mesures	Dangerosité initiale	Dangerosité résiduelle
F2 Fournisseur de matériel	Arrêt de production par compromission de l'équipement de maintenance	Réduire le risque de piègeage des équipements de maintenance utilisés sur le système industriel. Dotation de matériels de maintenance administrés par la DSI et qui seront mis à disposition du prestataire sur site.	2	1,3
F3 Prestataire informatique	Vol d'informations en passant par le prestataire informatique	Accroître la maturité cyber du prestataire (2 → 3) • Audit de sécurité (à inclure dans le contrat) • Suivi du plan d'action interne Renforcer la protection des données de R&D Solutions à investiguer : chiffrement, cloisonnement du réseau R&D.	3	2
P3 Laboratoires	Vol d'informations sur le système d'information du laboratoire	Diminuer la pénétration des laboratoires (3 → 2) Limitation des données transmises au laboratoire au juste besoin (mauvaise habitude actuelle de « tout » diffuser).	2,25	1,5



# Outil 10 – Analyser les scénarios opérationnels

Comment les scénarios stratégiques peuvent-ils se réaliser ?

## Comment construire un scénario opérationnel ?

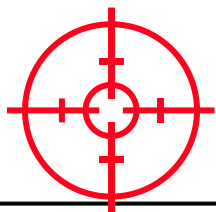
- Partir de chaque chemin d'attaque de chaque scénario stratégique
- Construire un scénario opérationnel qui permet à la **source de risque** d'atteindre son **objectif**, en analysant les **modes opératoires** possibles et leur séquençement d'**actions élémentaires**
- Enrichir les scénarios opérationnels d'explications sur la manière dont la source de risque va procéder
- Estimer la **vraisemblance** du scénario opérationnel





# Le séquençement type d'une attaque

La notion de chaîne d'attaque (*kill chain*)



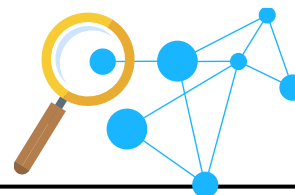
## Connaître

Ensemble des activités de ciblage, de reconnaissance et de découverte externe menées par l'attaquant pour préparer son attaque.



## Rentrer

Ensemble des activités menées par l'attaquant pour s'introduire dans le système d'information.



## Trouver

Ensemble des activités de reconnaissance interne des réseaux et systèmes.

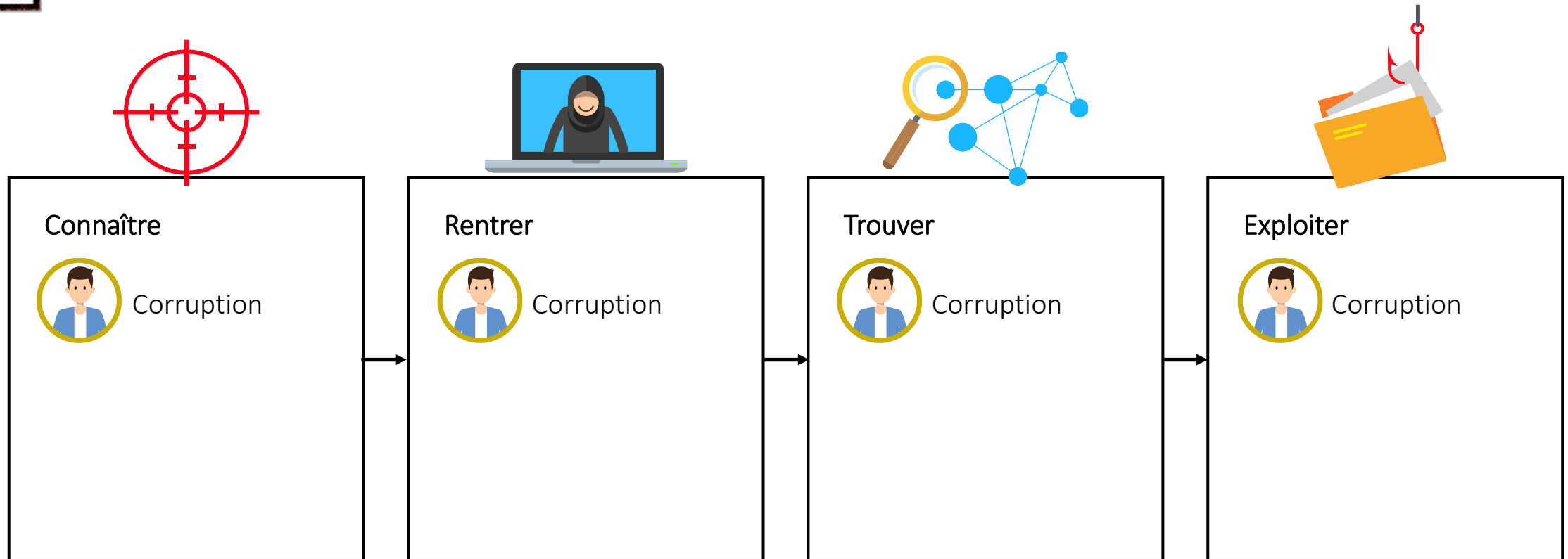


## Exploiter

Ensemble des activités d'exploitation des données et biens supports trouvés dans l'étape précédente.



# Exemple



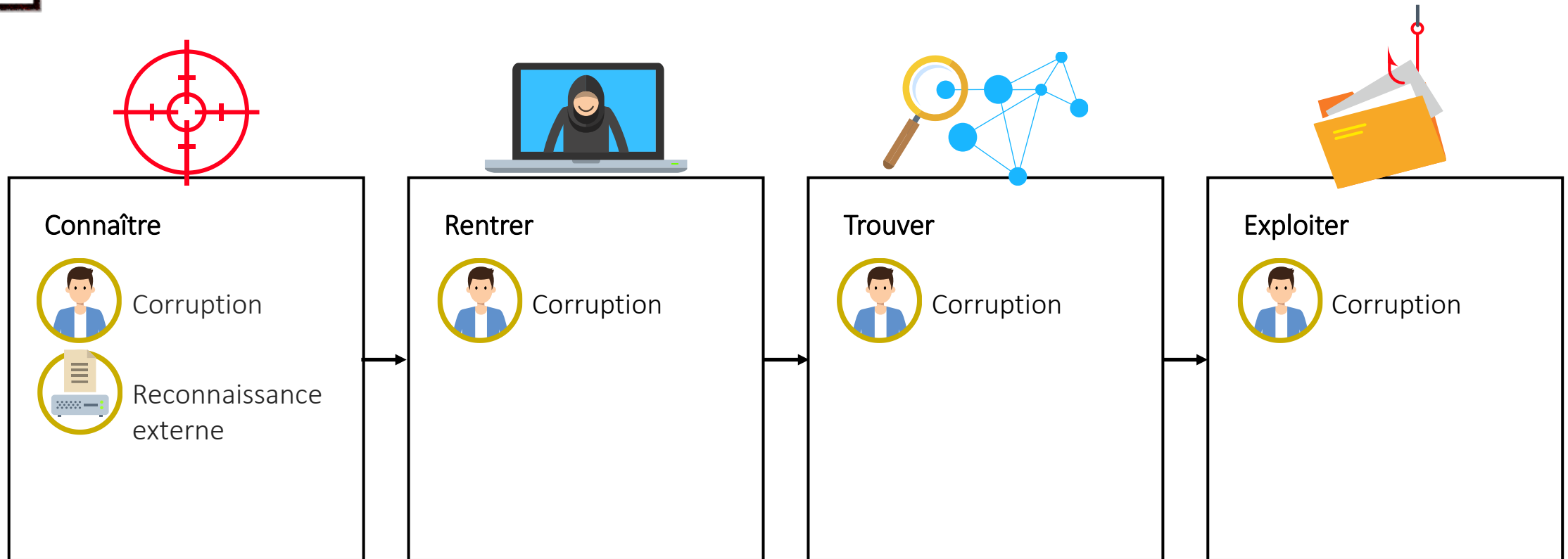
Recrutement d'une source, corruption de personnel.

Les raisons poussant une cible à trahir son entité d'origine – potentiellement à son insu – sont couvertes par quatre grandes catégories, dites « MICE » (*Money, Ideology, Compromission, Ego*).





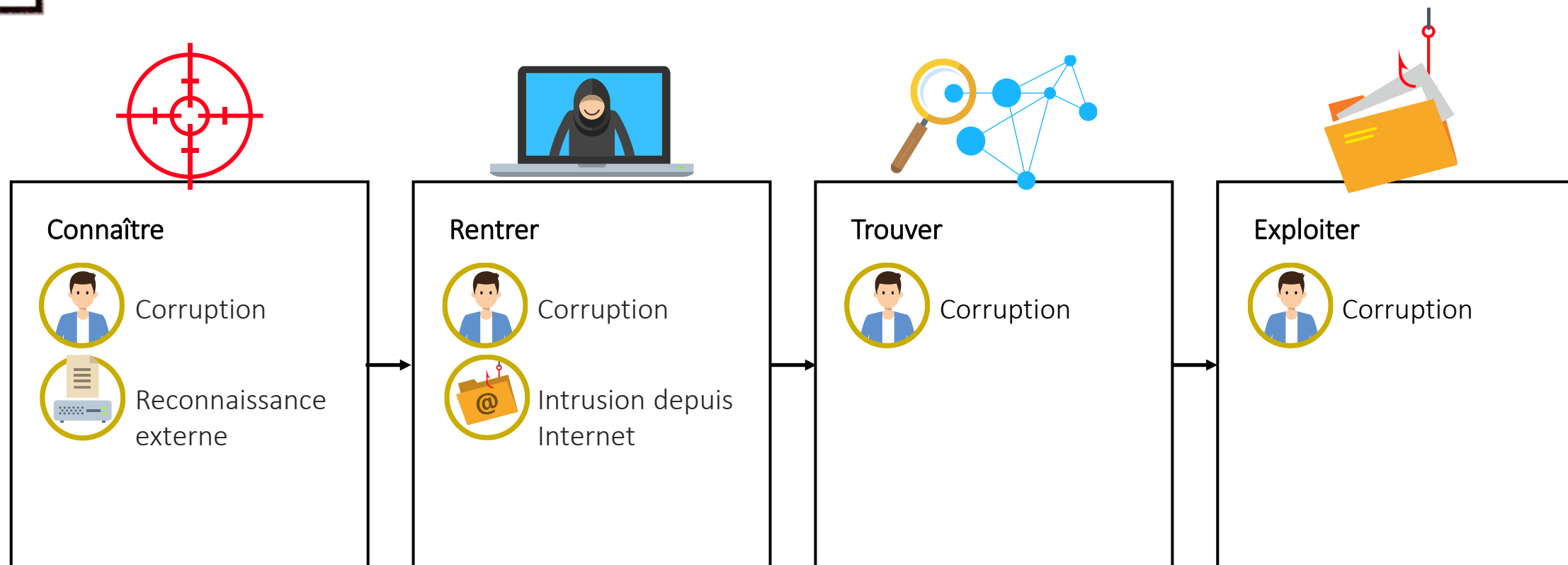
# Exemple



Les données collectées peuvent être de nature technique ou concerner l'organisation de la cible et de son écosystème : *social engineering*, Internet (scans de sites, forums de discussion), salons professionnels, faux client, faux journaliste, officines ou agences spécialisées (sources non ouvertes), renseignement (interceptions), etc.



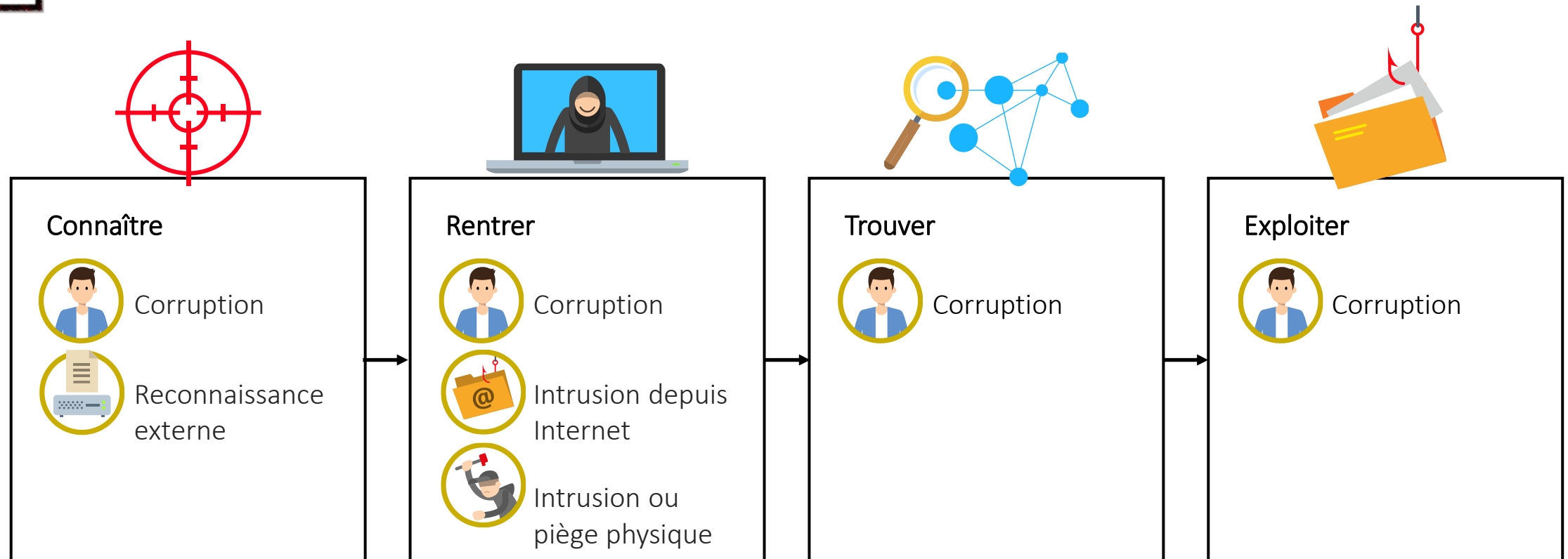
# Exemple



Idéalement pour l'attaquant, l'intrusion initiale de l'outil malveillant est réalisée depuis Internet. Les techniques et vecteurs d'intrusion les plus couramment utilisés sont : les attaques directes à l'encontre des services exposés sur Internet, les mails d'hameçonnage, les attaques par point d'eau, le piège d'une mise à jour a priori légitime, etc.



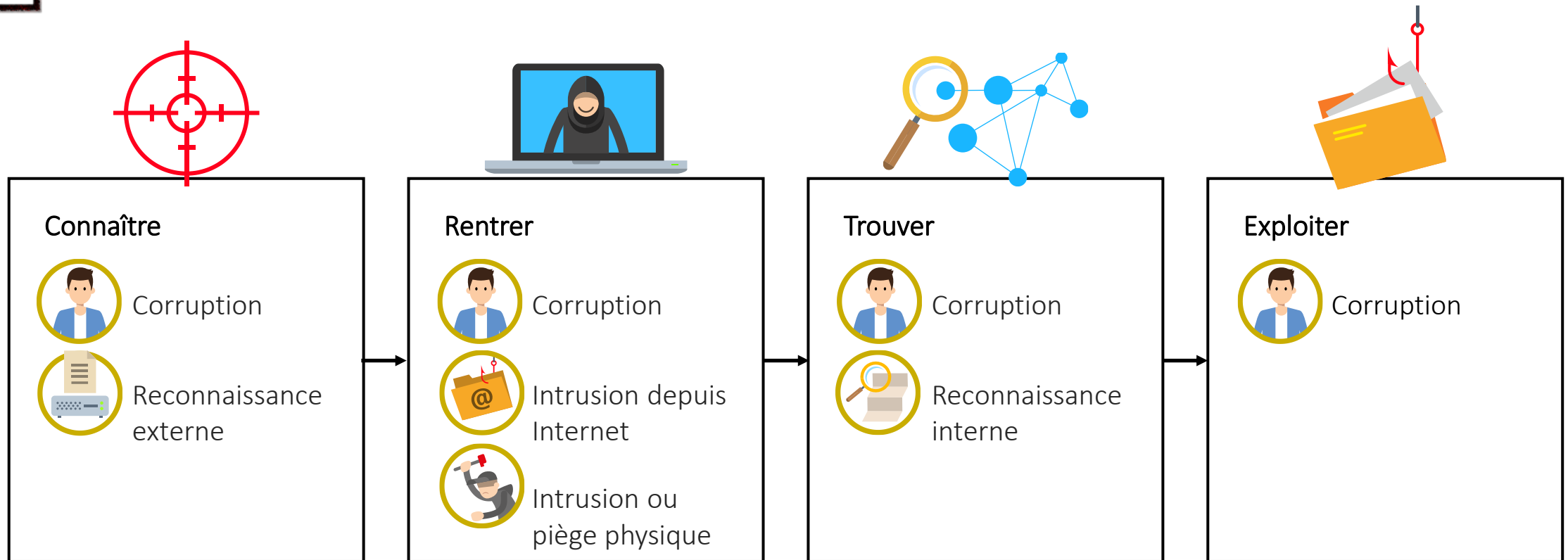
# Exemple



Cette méthode d'intrusion est utilisée pour accéder physiquement à des ressources du système d'information afin de le compromettre. L'intrusion physique est notamment utile à l'attaquant qui souhaite accéder à un système isolé d'Internet (compromission de la machine (exemple : clé USB piégée), intrusion via un réseau sans fil mal sécurisé, etc.).



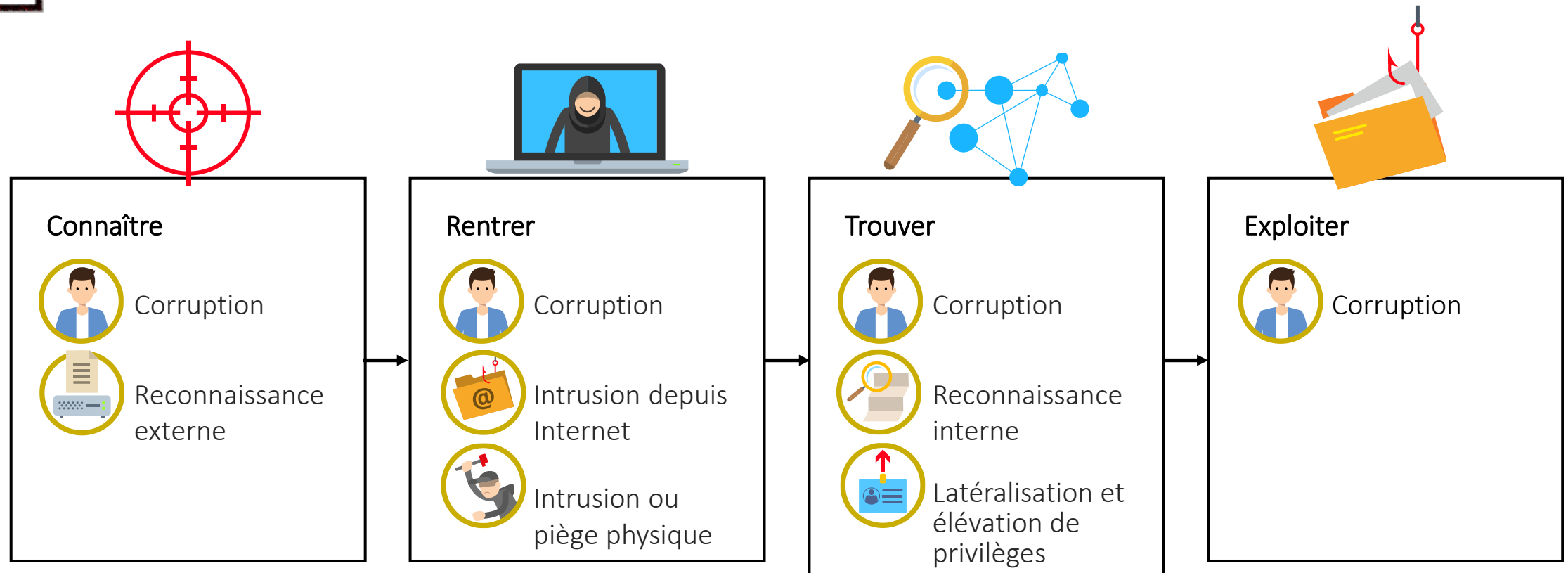
# Exemple



Activités permettant de cartographier l'architecture réseau, identifier les mécanismes de protection et de défense mis en place, recenser les vulnérabilités exploitables, etc. Lors de cette étape, l'attaquant cherche à localiser les services, informations et biens supports, objets de l'attaque.



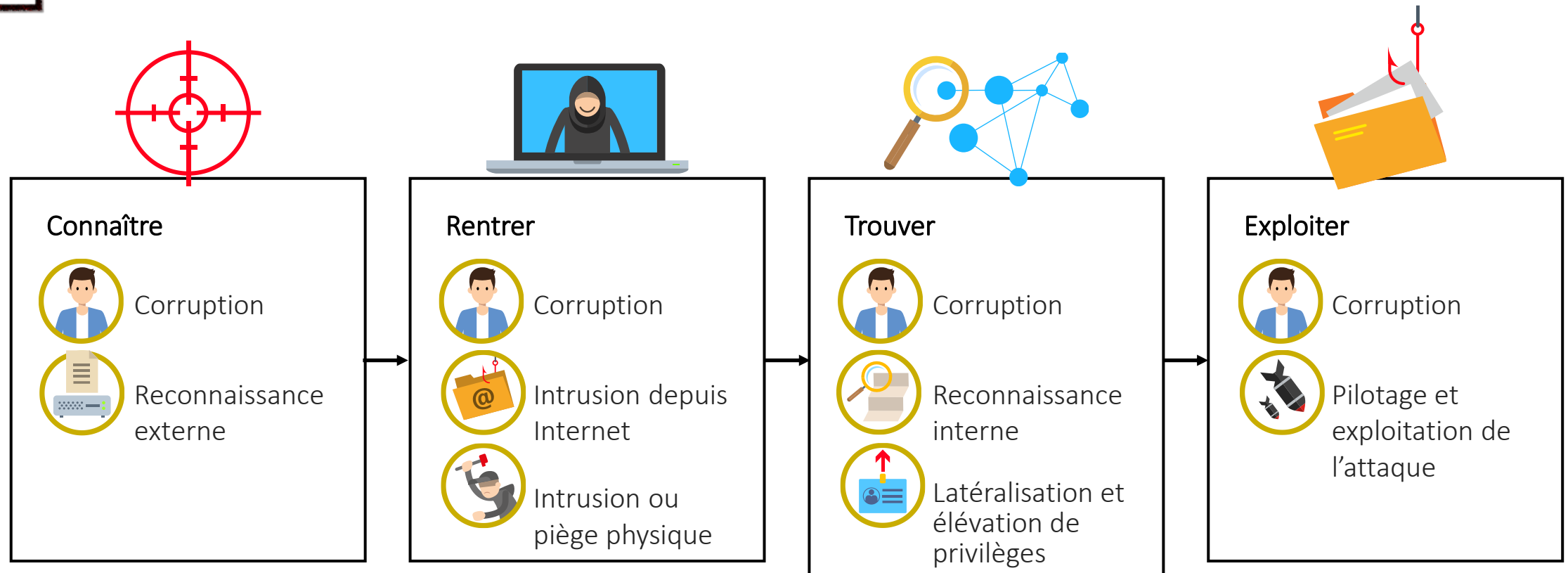
# Exemple



Mise en œuvre des techniques de latéralisation et d'élévation de privilèges afin de progresser et de se maintenir dans le système d'information, via l'exploitation des vulnérabilités structurelles internes du système (manque de cloisonnement des réseaux, contrôle d'accès insuffisant, politique d'authentification peu robuste, etc.).



# Exemple



Réalisation de l'objectif visé par la source de risque, par exemple : déclencher la charge malveillante destructrice, exfiltrer ou modifier de l'information. L'attaque peut être ponctuelle (ex : opération de sabotage) ou durable et se réaliser en toute discrétion (ex : opération d'espionnage visant à régulièrement exfiltrer des informations).



# Autre exemple



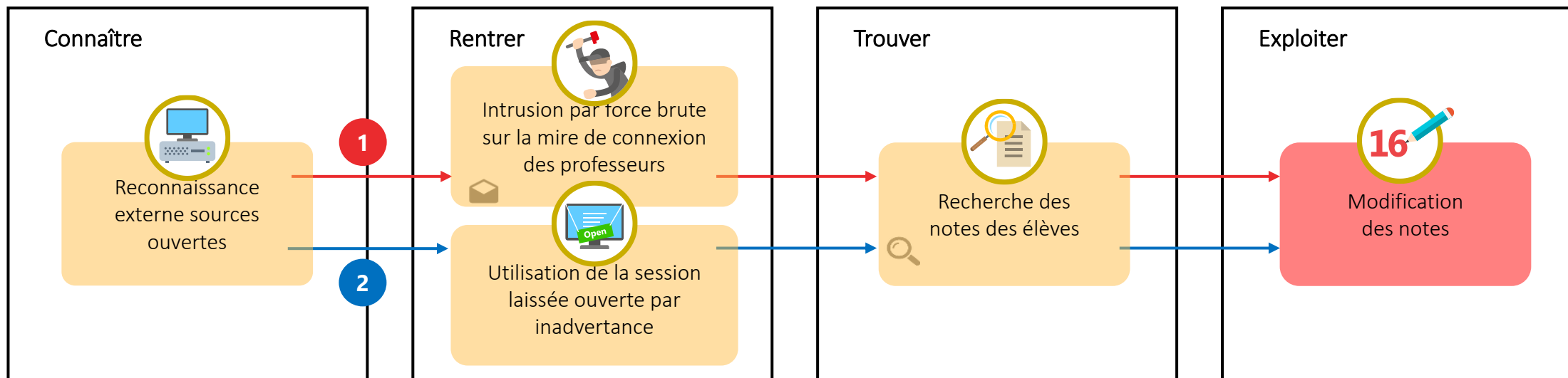
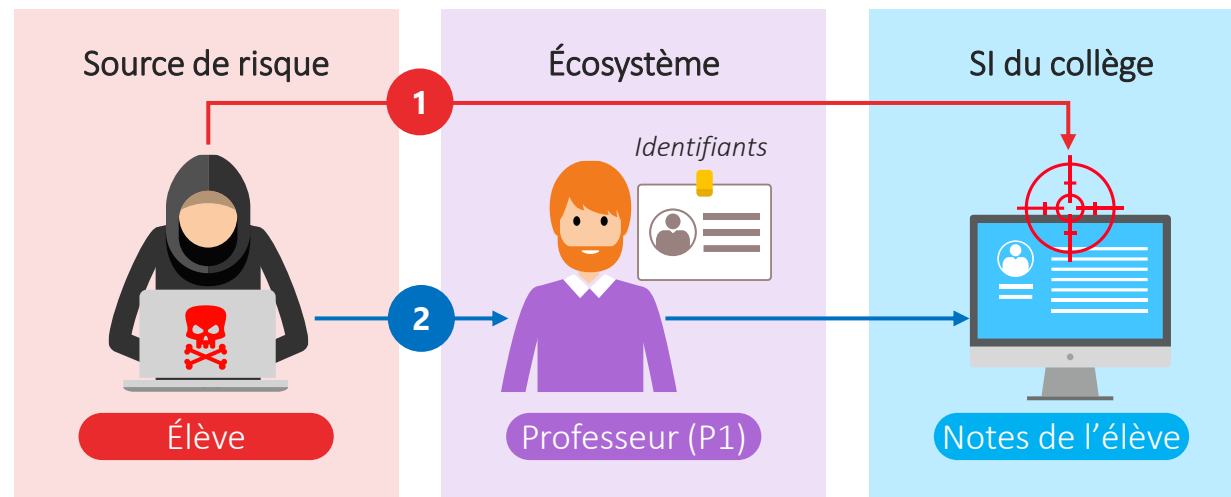
## Rappel

2 chemins d'attaque identifiés sur la modification de notes :

1. Attaque directe
2. Attaque par la connexion du professeur

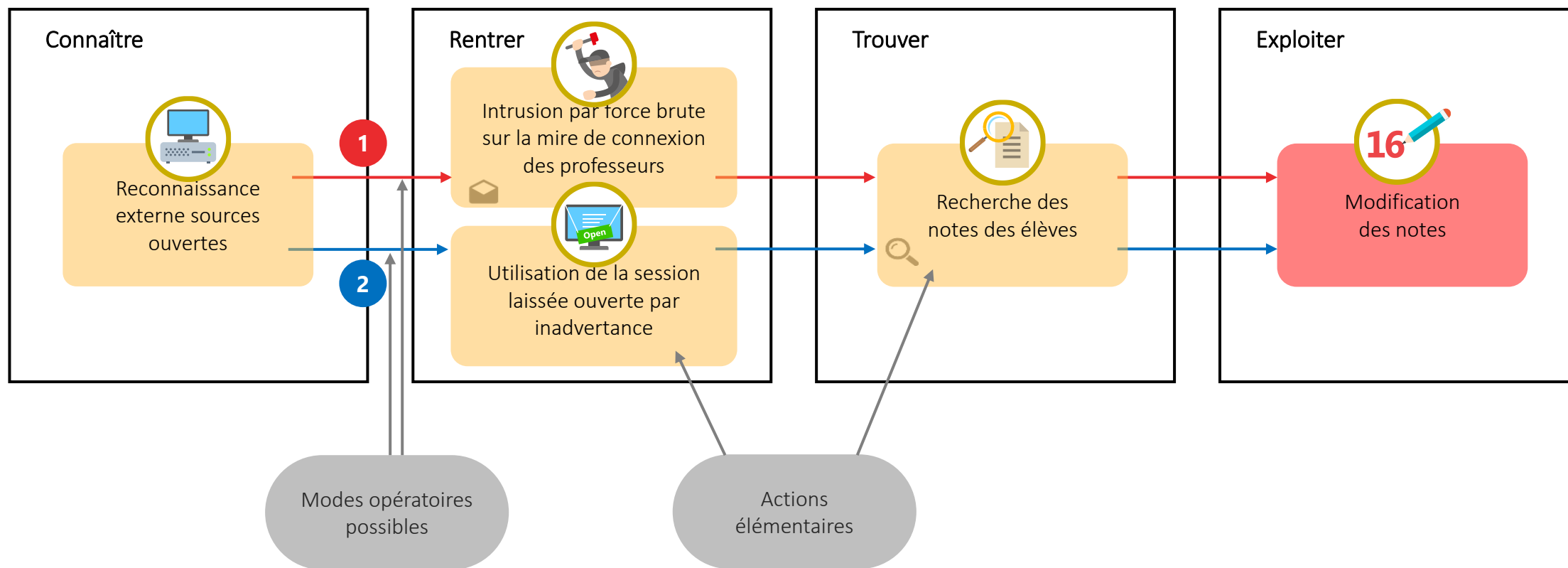
**Scénario stratégique :** Modification de la base de données par utilisation frauduleuse de la session du professeur.

**Chemin d'attaque :** n°2 • **Gravité :** 3





# Autre exemple



À un chemin d'attaque peuvent correspondre plusieurs modes opératoires, chacun composé d'un séquençement d'actions élémentaires





# Comment estimer la vraisemblance ?

Une échelle appliquée plus ou moins finement

Établissement du contexte

Vraisemblance	Description
4. Maximale	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'organisme (historique d'incidents)
3. Importante	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée
2. Faible	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative
1. Minimale	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



On peut l'appliquer aux scénarios stratégiques (très grossièrement), chemins d'attaques, modes opératoires, ou actions élémentaires (très finement). On calcule ensuite la vraisemblance des macro-éléments en fonction de la vraisemblance des micro-éléments.



# Exercice en groupes

Appréciez le chemin d'attaque



Scénario stratégique :

Un concurrent vole des informations de R&D

Chemin d'attaque : n°1

Gravité : 3

Connaître

Rentrer

Trouver

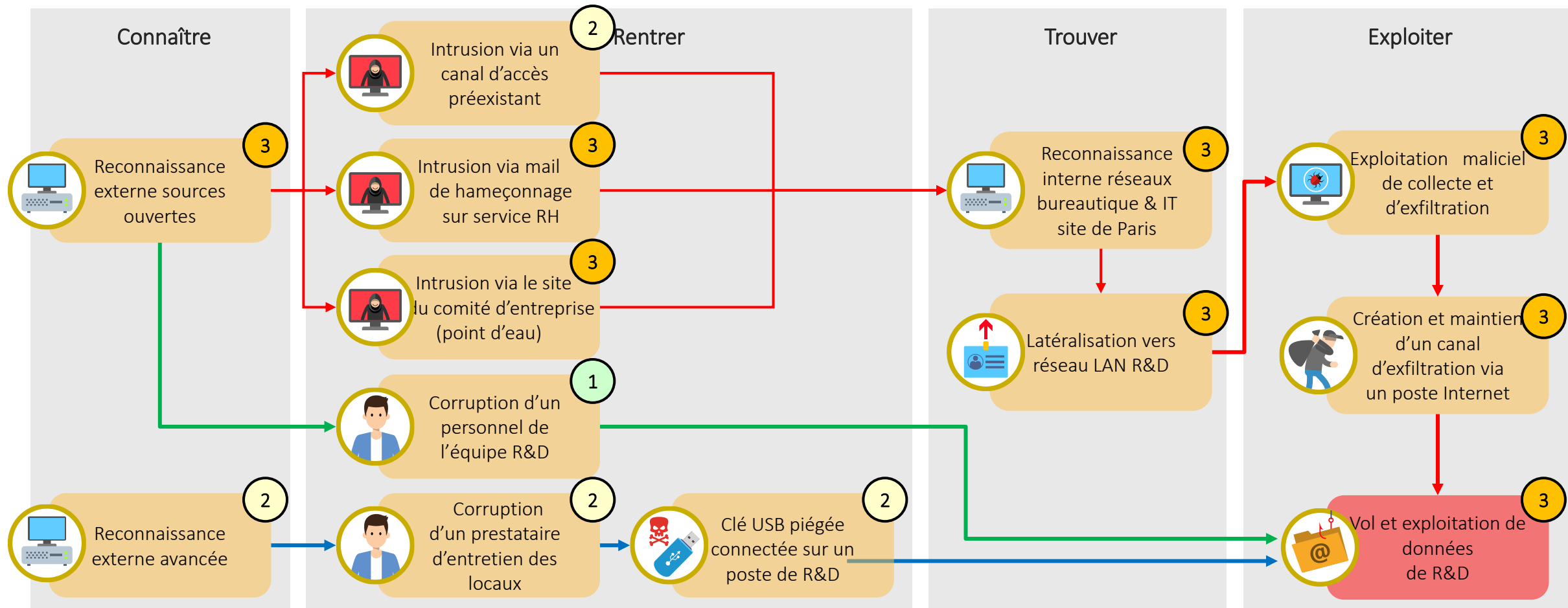
Exploiter



# Correction



Scénario stratégique : Un concurrent vole des informations de R&D	Chemin d'attaque : n°1 Gravité : 3
--	---------------------------------------





# Mesures



Peut-on déterminer des mesures sur les scénarios opérationnels ?

- Oui ! On peut d'ores-et-déjà déterminer des mesures complémentaires au socle
  - Agir sur l'exposition
    - Réduire la dépendance : interroger les choix de partenaires, identifier des substitutions
    - Réduire la pénétration : réduire les droits, réduire les données traitées, internaliser, etc.
  - Agir sur la fiabilité cyber
    - Améliorer la maturité cyber : imposer des règles (ex : clauses types dans les contrats), aider à progresser / vérifier la sécurité (ex : questionnaire, audit, sensibilisation), etc.
    - Améliorer la confiance : demander des garanties (ex : certification), changer de partenaire

Quid des éventuelles mesures déterminées à ce stade ?

Elles sont ajoutées au plan de traitement des risques

Elles peuvent être considérées comme mises en œuvre dans la suite de l'étude



# Outil 11 – Évaluer les risques

Comment comparer les risques ?

- 1. Formuler les risques** selon les destinataires de l'étude et les outils employés
  - Un risque est un scénario, qui doit raconter comment une source de risque, avec son objectif visé, va employer un scénario stratégique, et plus précisément un scénario opérationnel, et engendrer un ou plusieurs événements redoutés
  - On peut décider de créer les risques en partant de chaque élément étudié : par événement redouté, par source de risques, par scénario stratégique, par scénario opérationnel, par mode opératoire, voire autre (généralement, on crée un risque par scénario opérationnel)
  - On va devoir choisir le niveau de détail et de formulation le plus approprié aux destinataires de l'étude, et on peut également les regrouper, les scinder, etc.
- 2. Déterminer leur gravité et leur vraisemblance**
  - La gravité est héritée du/des événements redoutés considérés
  - La vraisemblance est héritée des chemins d'attaques ou modes opératoires ou actions élémentaires
- 3. Les représenter sur un graphique**, avec la vraisemblance en abscisse et la gravité en ordonnée, pour pouvoir juger de leur acceptabilité



# Formuler les risques en détail...

On exprime des événements redoutés et estime leur gravité.  
Les plus graves serviront de base pour le reste de la construction du risque.

On valide des couples de sources de risque et d'objectifs visés.  
Les plus pertinents, mis en relation avec les événements redoutés, seront (re)formulés et contextualisés.

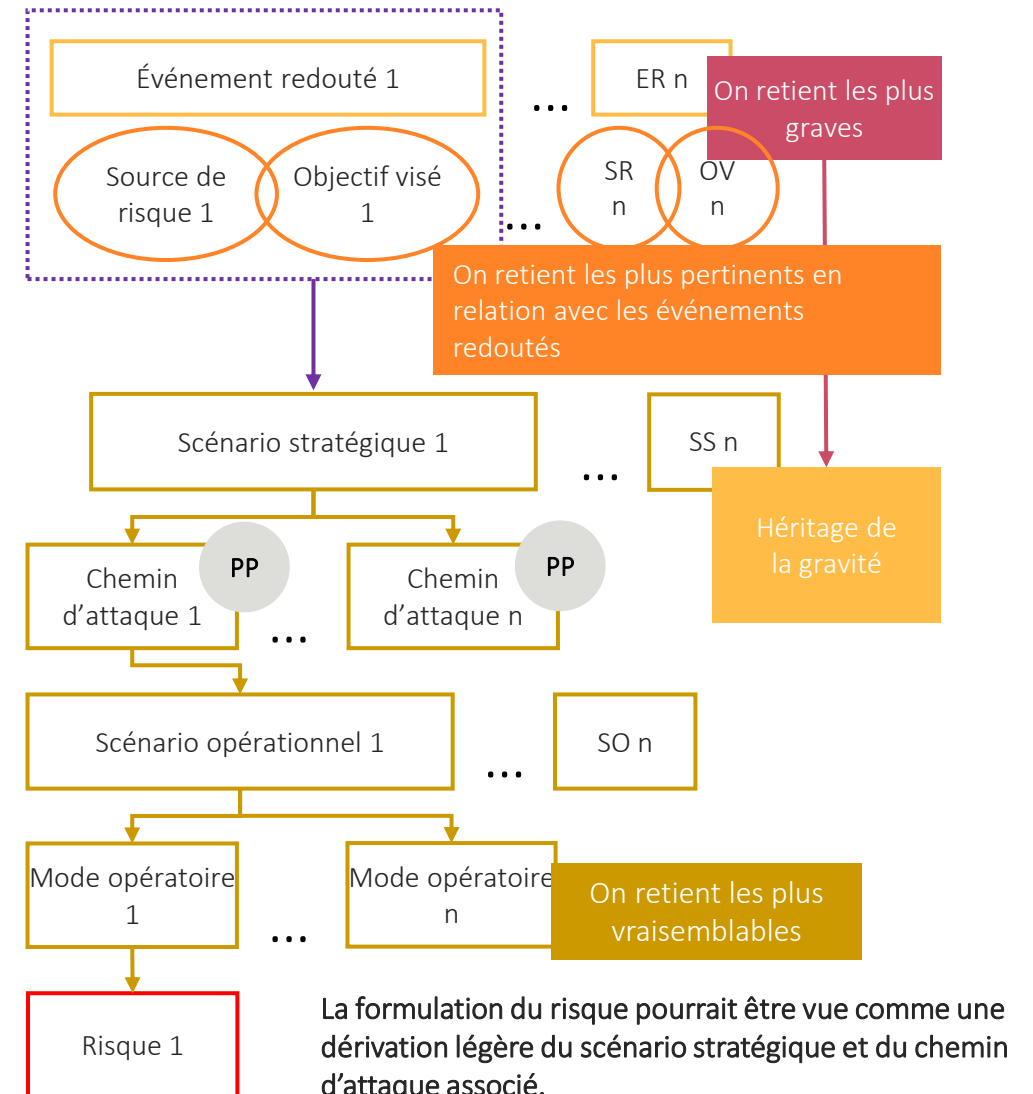
On crée les scénarios stratégiques.

On raffine les scénarios stratégiques en chemins d'attaques, avec reformulation, en y intégrant pour certains des parties prenantes.

On décline les différents chemins d'attaques des scénarios stratégiques en scénarios opérationnels.

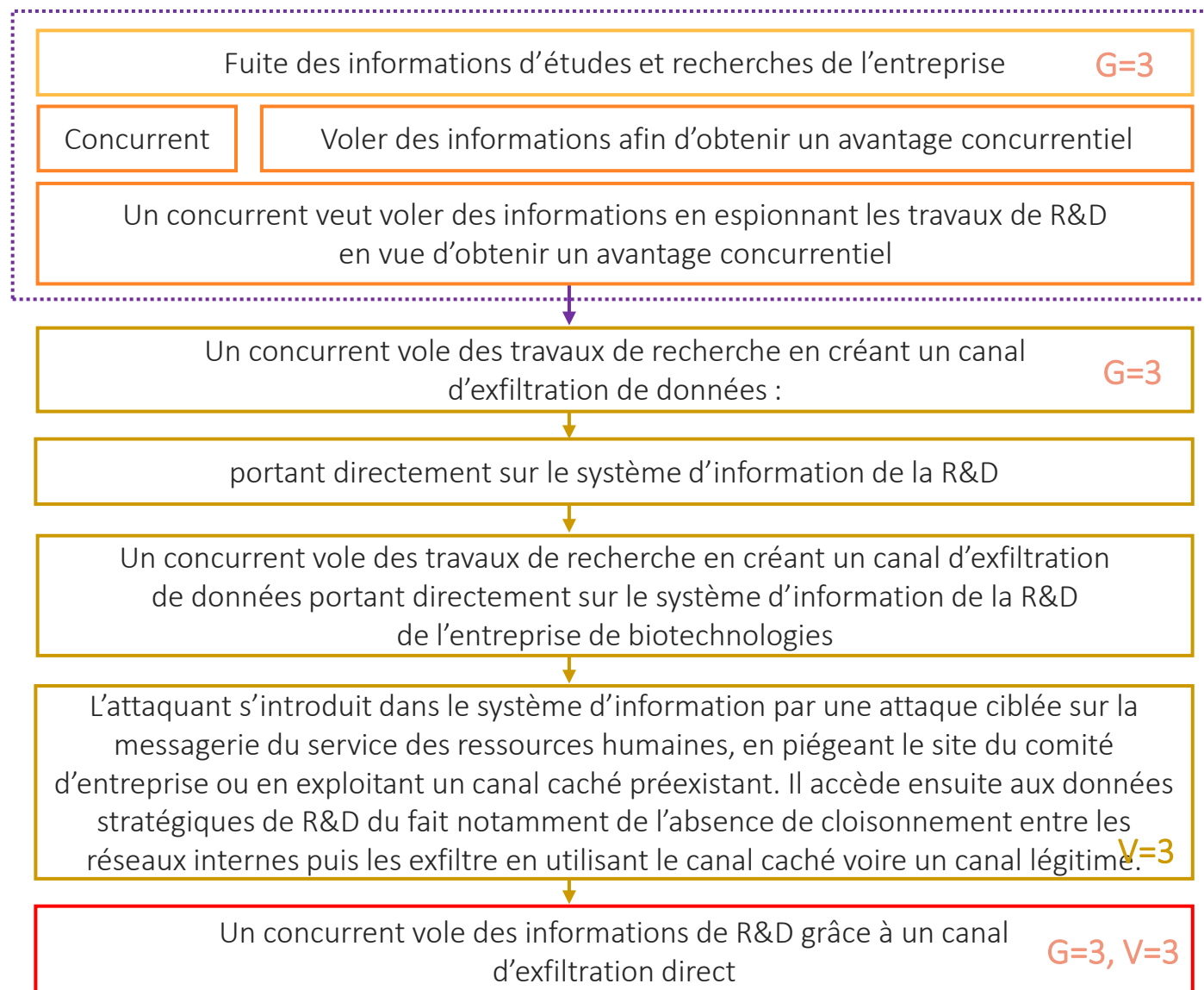
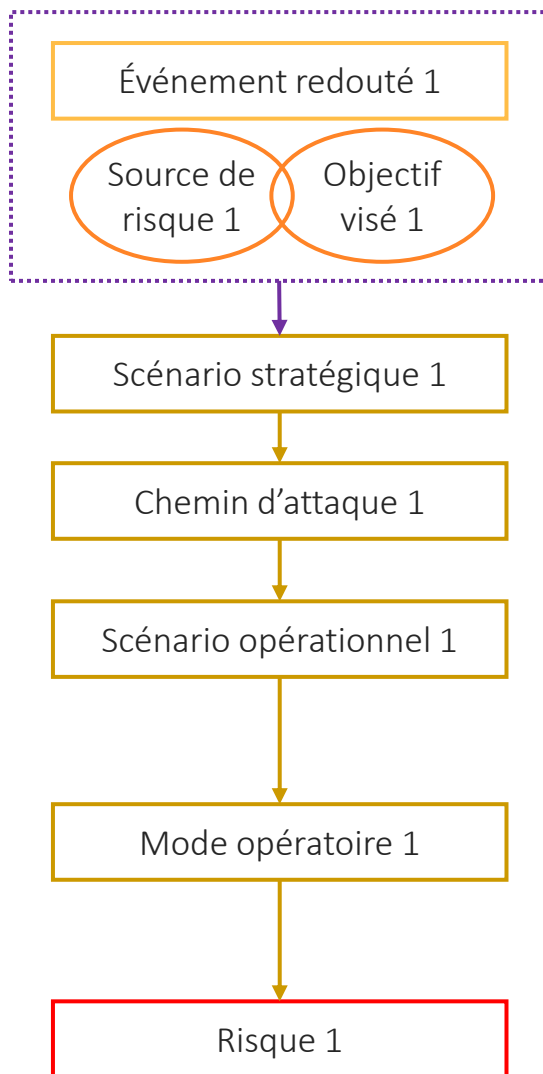
On décrit synthétiquement chaque mode opératoire de chaque scénario opérationnel.

On formule le risque comme une synthèse du scénario stratégique et du mode opératoire.





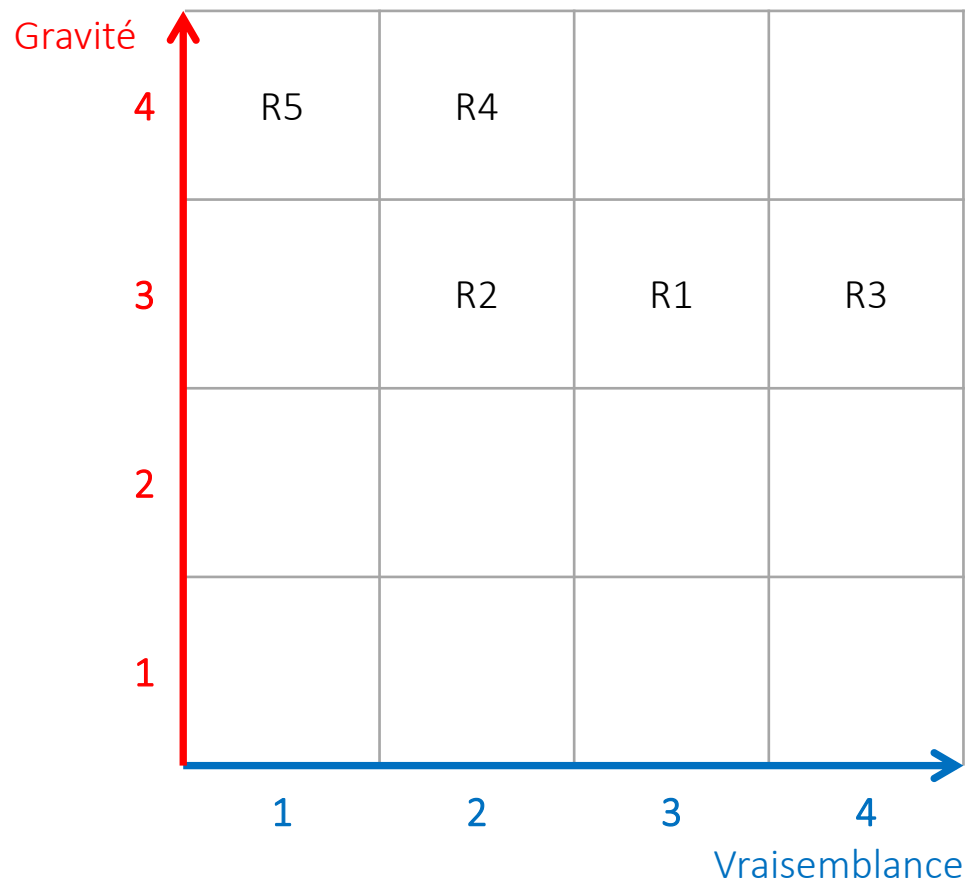
# Exemple





# Comment représenter les risques ?

## Exemple



### Risques

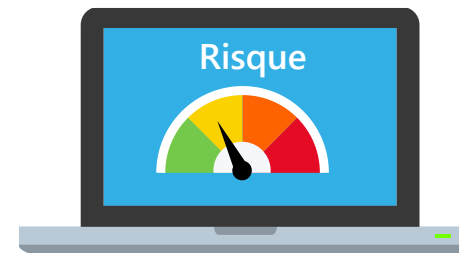
**R1** > Un concurrent vole des informations de R&D grâce à un canal d'exfiltration direct

**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 hacktiviste provoque un arrêt de la production des vaccins en compromettant l'équipement de maintenance du fournisseur de matériel

**R5** > Un hacktiviste perturbe la distribution de vaccins en modifiant leur étiquetage.



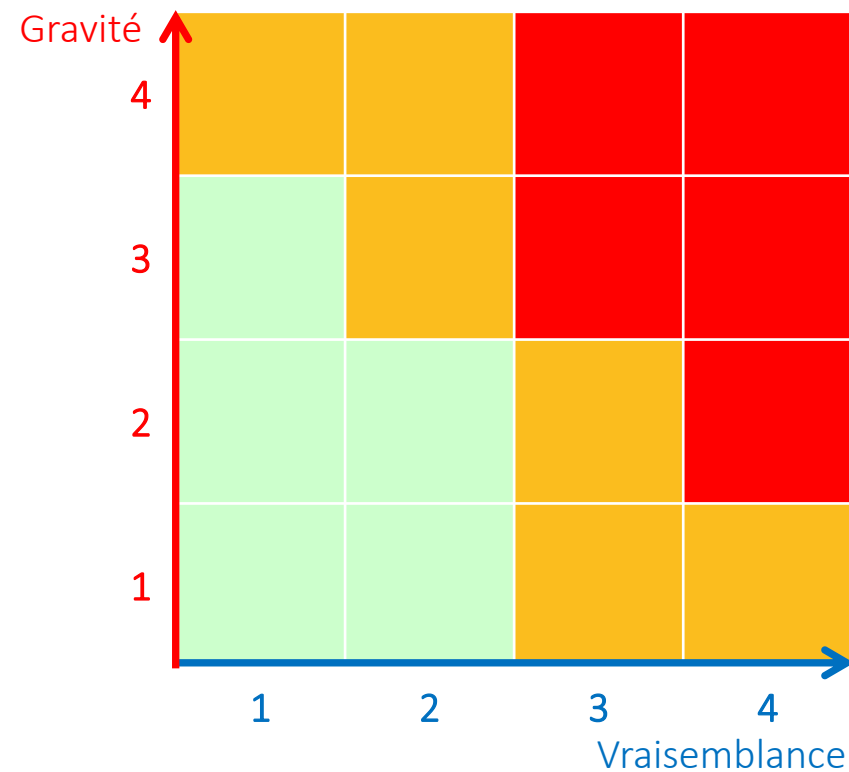




# Comment juger de l'acceptabilité des risques ?

## L'échelle d'acceptation des risques

Niveau	Acceptabilité	Orientations
Faible	Acceptable en l'état	Aucune action n'est à entreprendre
Moyen	Tolérable sous contrôle	Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme
Élevé	Inacceptable	Des mesures de réduction du risque doivent impérativement être prises à court terme. Dans le cas contraire, tout ou partie de l'activité sera refusé

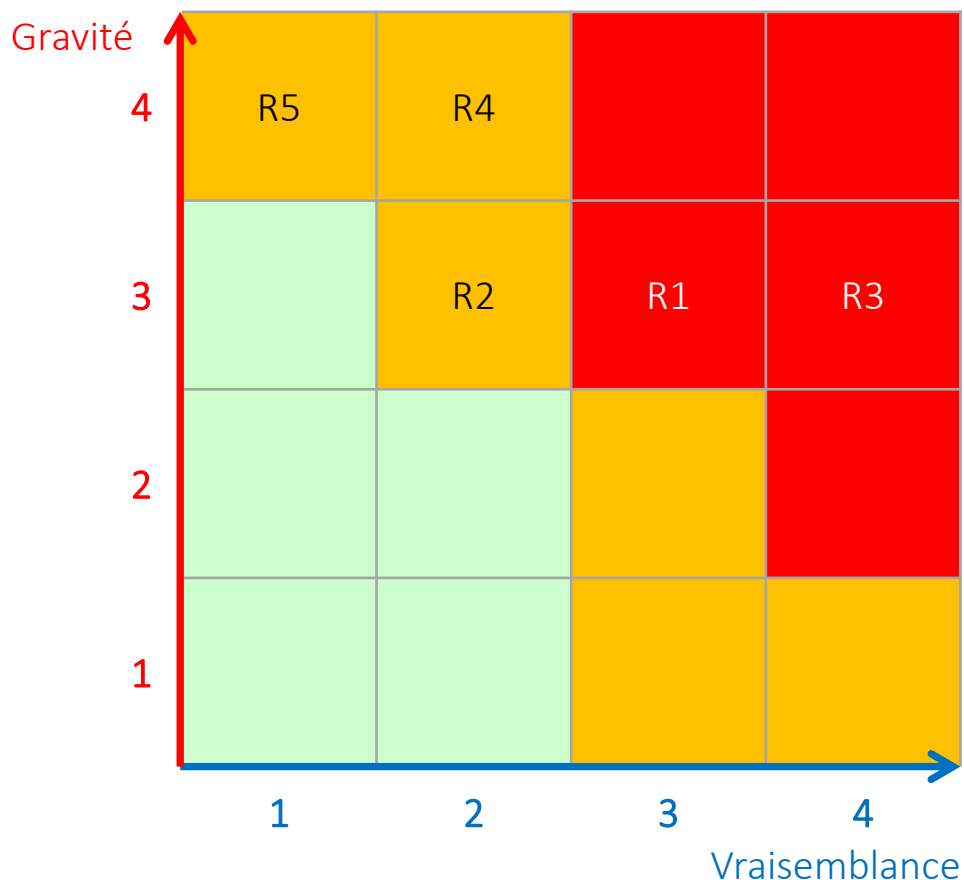


La représentation de l'échelle d'acceptation des risques doit permettre de comparer les risques les uns par rapport aux autres et être compréhensible par l'ensemble des participants.



# Application de l'échelle d'acceptation

## Exemple



### 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

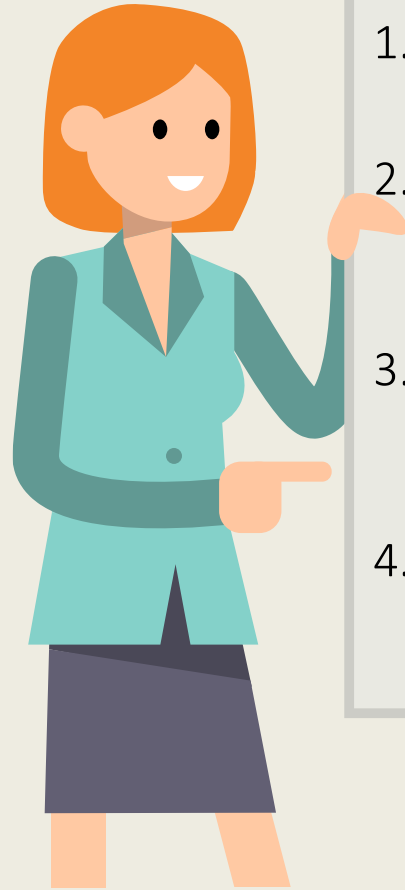
**R3** > Un concurrent vole des informations de R&D grâce à un canal d'exfiltration via le prestataire informatique

**R4** > Un hacktiviste provoque un arrêt de la production des vaccins en compromettant l'équipement de maintenance du fournisseur de matériel

**R5** > Un hacktiviste perturbe la distribution de vaccins en modifiant leur étiquetage.



# Qu'avons-nous appris ?



1. Savoir identifier et analyser les **événements redoutés** (conséquences et gravité)
  2. Savoir analyser les **scénarios stratégiques** (sources de risques et pertinence, parties prenantes et dangerosité)
  3. Savoir analyser les **scénarios opérationnels** (chemins d'attaques, chaînes d'actions unitaires et vraisemblance)
  4. Savoir évaluer les **risques**
- On peut maintenant traiter les risques !



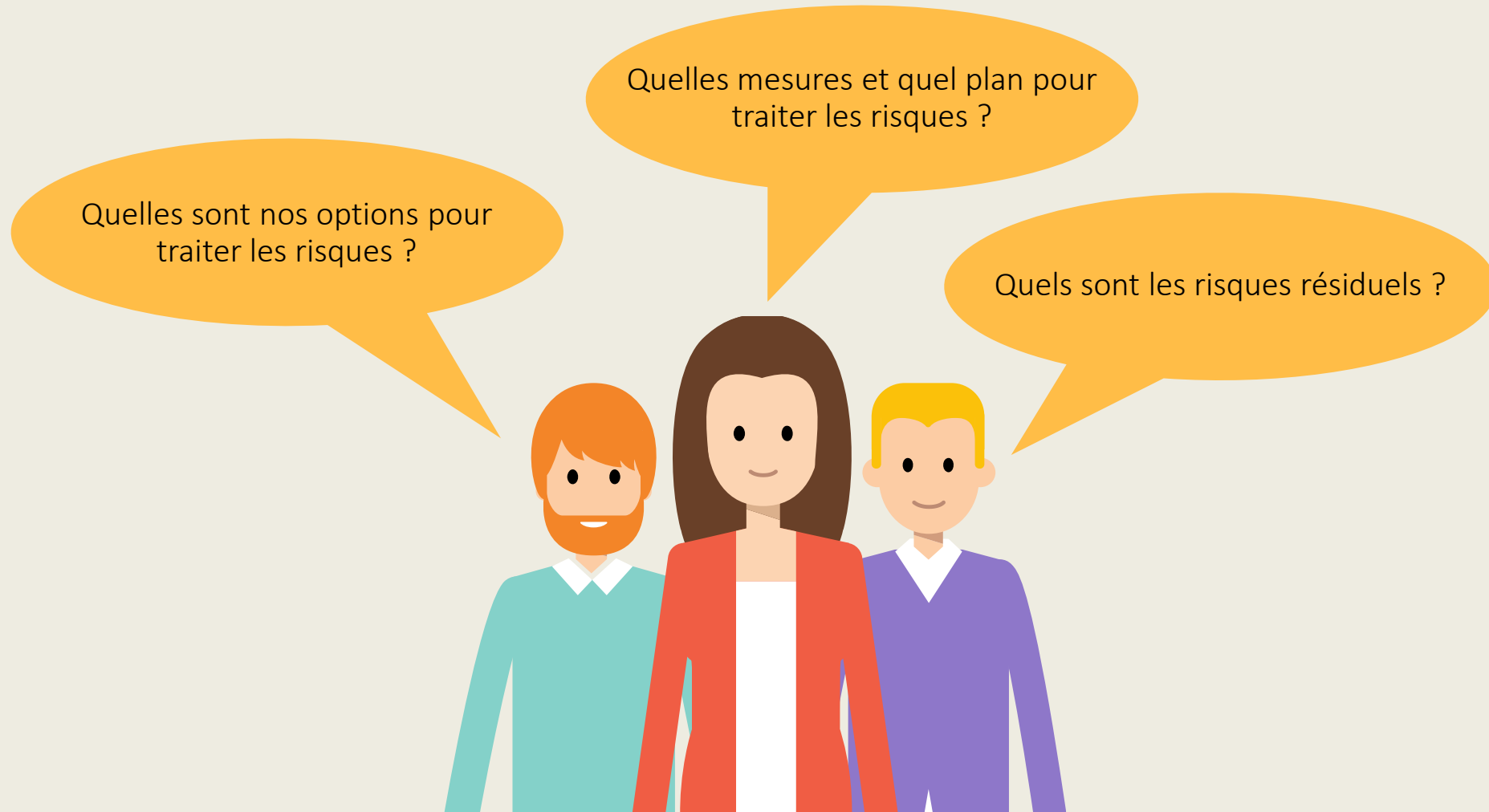
# Plan de la formation

1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. Apprécier les risques
  - a. Approche par conformité
  - b. Approche par scénarios
5. Traiter les risques
6. Étude de cas complète
7. Conclusion



# De quoi va-t-on parler ?

Traiter les risques





# Outil 12 – Choisir les options de traitement

Quelle stratégie pour traiter chaque risque ?

Pour chaque risque, notamment au vu des critères d'acceptation des risques, il convient de décider d'une ou plusieurs options pour le traiter

## Réduire le risque

- Appliquer des mesures pour réduire la vraisemblance, ou éventuellement la gravité (pas simple !) du risque

## Refuser le risque

- Appliquer des mesures pour réduire, arrêter ou ne pas démarrer, l'activité porteuse du risque

## Partager le risque

- Appliquer des mesures pour transférer tout ou partie du risque à un tiers (ex : partager des conséquences via une assurance)

## Prendre le risque

- Maintenir le risque à son niveau

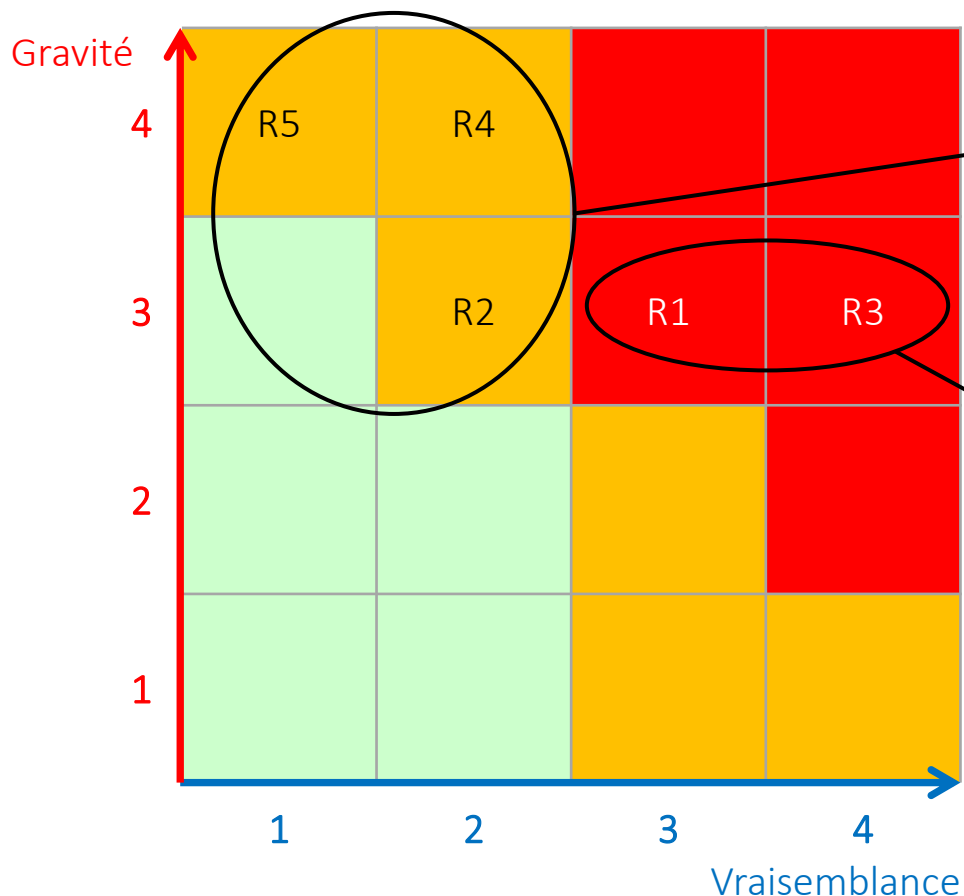


# Choix des options de traitement

## Exemple



Traiter les risques



### Risques

**R1** > Un concurrent vole des informations de R&D gr ce   un canal d'exfiltration direct

**R2** > Un concurrent vole des informations de R&D en exfiltrant celles d tenues par le laboratoire

**R3** > Un concurrent vole des informations de R&D gr ce   un canal d'exfiltration via le prestataire informatique

**R4** > Un hacktiviste provoque un arr t de la production des vaccins en compromettant l' quipement de maintenance du fournisseur de mat riel

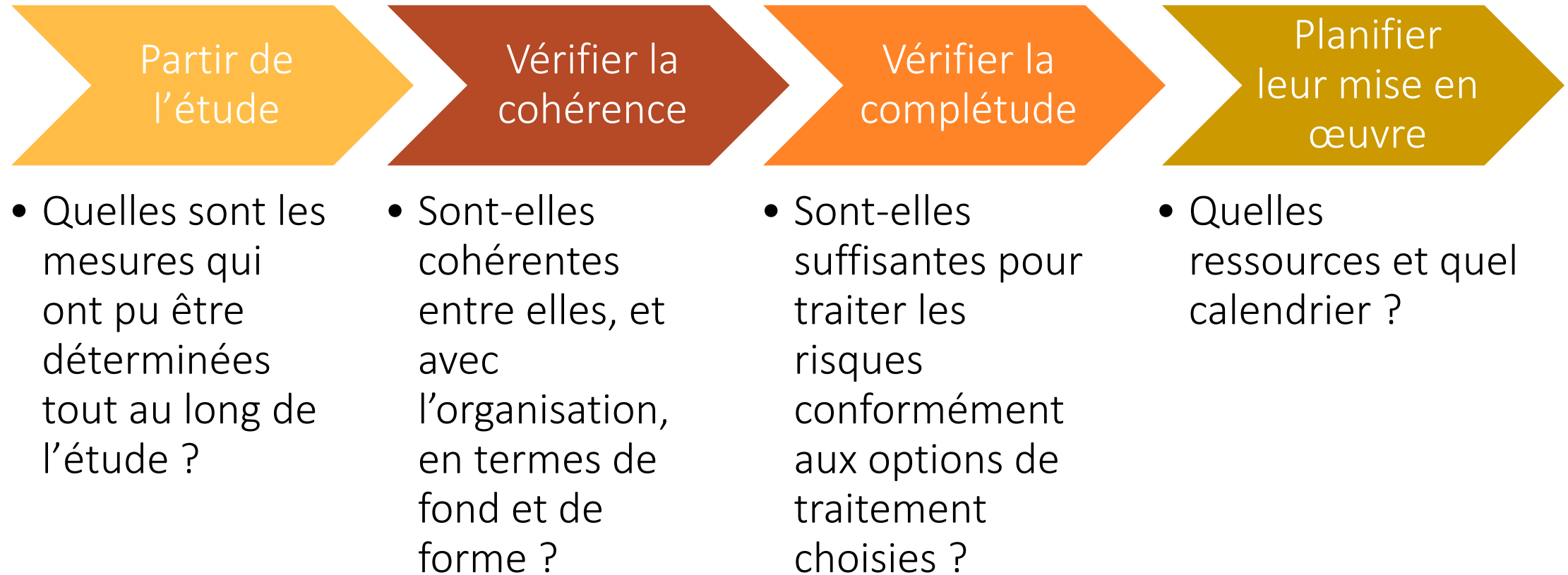
**R5** > Un hacktiviste perturbe la distribution de vaccins en modifiant leur  tiquetage.



# Outil 13 – Déterminer les mesures

Quelles mesures pour traiter les risques ?

Traiter les risques







# Bâtir son plan de traitement des risques

Exemples de catégories pour classer les mesures

## Gouvernance et anticipation

- Organisation de management du risque et d'amélioration continue
- Processus d'homologation
- Maîtrise de l'écosystème

## Protection

- Gestion de l'authentification et du contrôle d'accès
- Sécurité physique et organisationnelle
- Maintien en condition de sécurité et gestion d'obsolescence

## Résilience

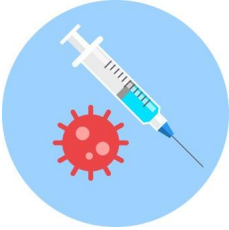
- Continuité d'activité (sauvegarde et restauration, gestion des modes dégradés)
- Reprise d'activité
- Gestion de crise cyber

## Défense

- Surveillance d'événements
- Détection et classification d'incidents
- Réponse à un incident cyber



# Bâtir son plan de traitement des risques



## Exemple (1/2)

Mesure	Risques traités	Responsable	Freins et difficultés de mise en œuvre	Coût / Complexité	Échéance	Statut
Gouvernance						
Sensibilisation renforcée au hameçonnage par un prestataire spécialisé	R1	RSSI	Validation de la hiérarchie obligatoire	+	Juin 2023	En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI	R1, R5	RSSI		++	Mars 2023	A lancer
Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contrats avec les prestataires et laboratoires	R2, R3, R4	Équipe juridique	Effectué au fil de l'eau à la renégociation des contrats	++	Juin 2024	En cours
Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire ou un laboratoire	R2, R3, R4	RSSI / Équipe juridique		++	Juin 2023	A lancer
Audit de sécurité organisationnel des prestataires et laboratoires clés. Mise en place et suivi des plans d'action consécutifs	R2, R3, R4	RSSI	Acceptation de la démarche par les prestataires et laboratoires	++	Juin 2024	A lancer
Limitation des données transmises au laboratoire au juste besoin	R2	Équipe R&D		+	Mars 2023	Terminé
Protection						
Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonnement)	R1, R3	DSI		+++	Septembre 2023	En cours
Renforcement du contrôle d'accès physique au bureau R&D	R1	Équipe sûreté		++	Mars 2023	Terminé
Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site	R4	DSI		++	Septembre 2024	A lancer



# Bâtir son plan de traitement des risques



## Exemple (2/2)

Mesure	Risques traités	Responsable	Freins et difficultés de mise en œuvre	Coût / Complexité	Échéance	Statut
Gouvernance						
Sensibilisation Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil	R1	RSSI	Achat d'un outil, budget à provisionner	++	9 mois	A lancer
Protection						
Renforcement du plan de continuité d'activité	R4, R5	Équipe continuité d'activité			++	En cours



# Outil 14 – Gérer les risques résiduels

Que faire des risques qui subsistent après application des mesures ?

La logique est la suivante :

1. **Ré-estimer les gravités et vraisemblances**, compte tenu des nouvelles mesures déterminées
  - La plupart des mesures peuvent diminuer la vraisemblance (sensibilisation, authentification forte, chiffrement, sauvegardes, etc.)
  - Certaines mesures peuvent également diminuer la gravité (minimisation des données, recours à une assurance, plan de communication, etc.)
  - Mais l'application de mesures ne modifie pas forcément gravité ou vraisemblance (voir les niveaux définis dans les échelles)
2. **Faire décider de leur acceptation** : notion d'homologation de sécurité (dans le cadre de systèmes)

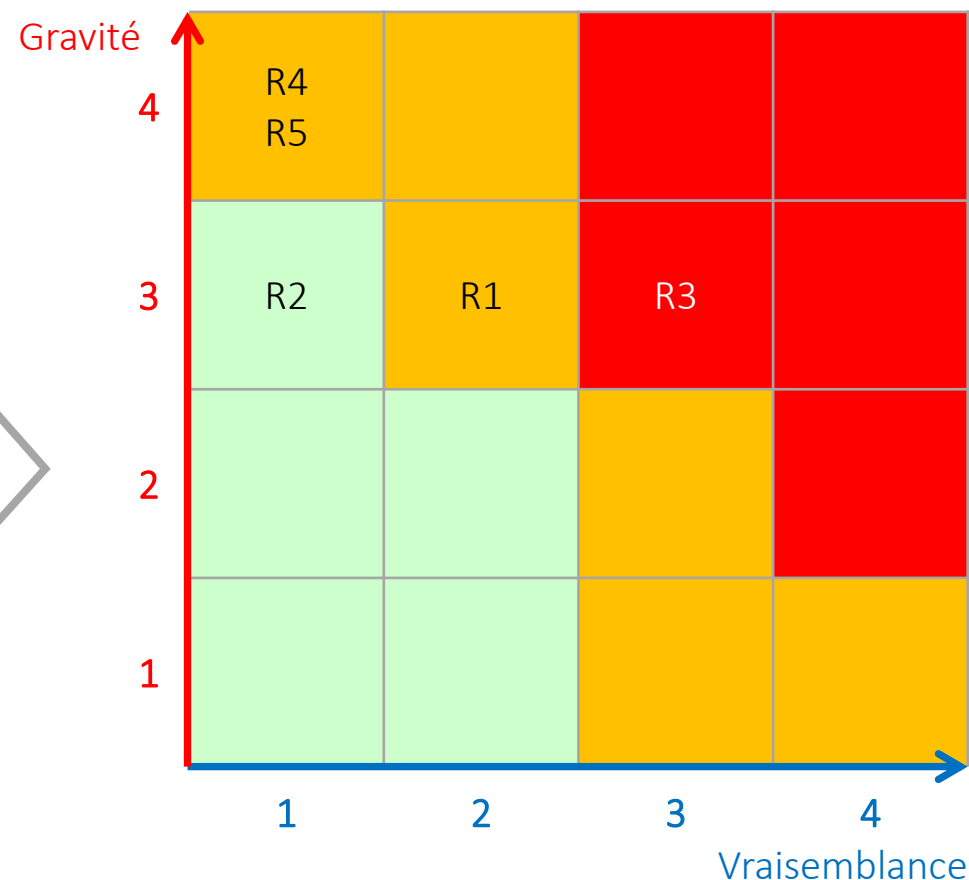
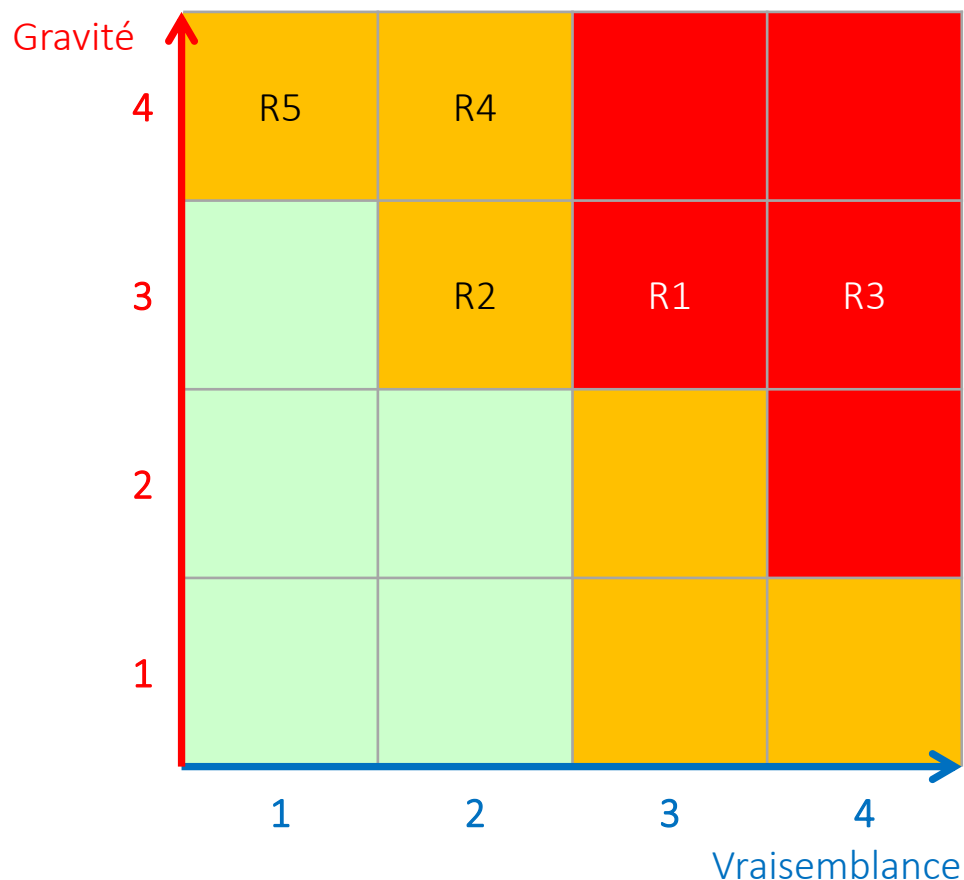


# Évaluer les risques résiduels

Comment la cartographie des risques va-t-elle évoluer ?

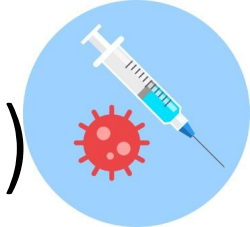


Traiter les risques

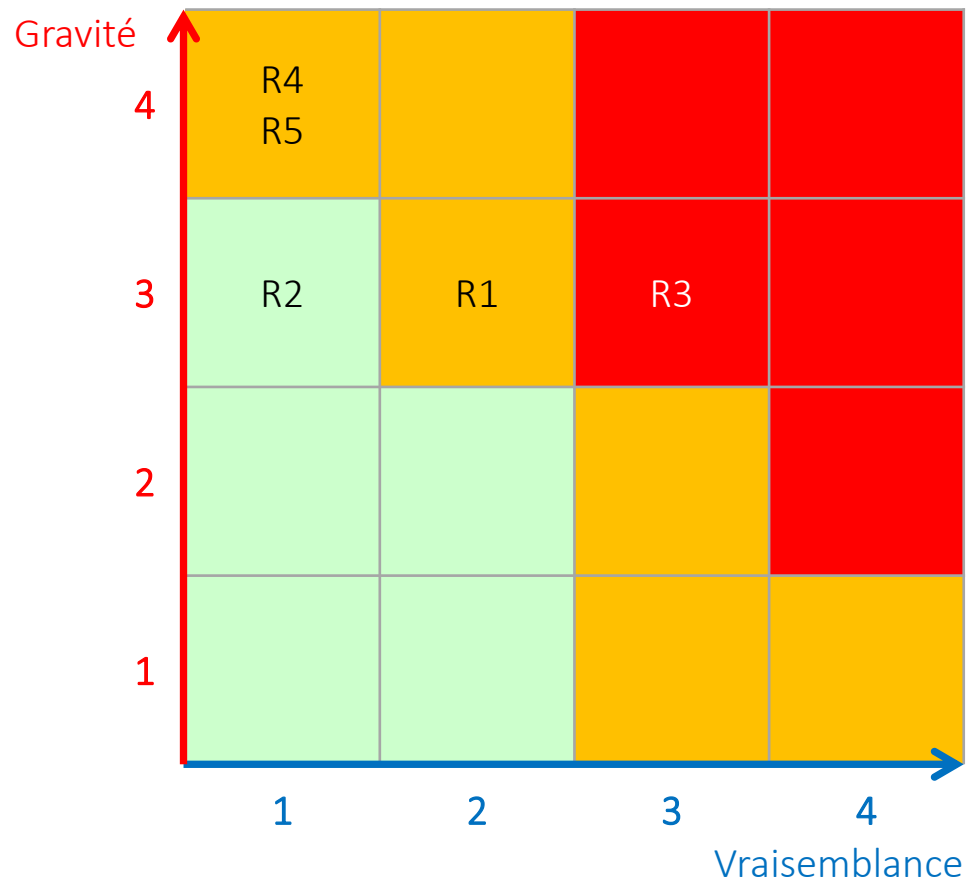




# Accepter les risques résiduels (cf. homologation)



Une décision éclairée, une prise de responsabilité



Niveau	Acceptabilit�	Orientations
Faible	Acceptable en l�tat	Aucune action n�est � entreprendre
Moyen	Tol�rable sous contr�le	Un suivi en termes de gestion du risque est � mener et des actions sont � mettre en place dans le cadre d�une am�lioration continue sur le moyen et long terme
�lev�	Inacceptable	Des mesures de r�duction du risque doivent imp�rativement �tre prises � court terme. Dans le cas contraire, tout ou partie de l�activit� sera refus�

Ici, plusieurs risques r siduels sont encore moyens, voire  lev s. Un responsable (ex : l autorit  d homologation) va devoir d cider de les accepter ou de les refuser !  
On voit aussi que les orientations de l  chelle devraient  tre am lior es, sinon ce serait un refus automatique...



# Outil 15 – Surveiller et revoir les risques

Comment maintenir l'objet de l'étude en conditions de sécurité ?

La logique est la suivante :

1. Suivre l'avancement de la mise en œuvre des mesures prévues dans le plan de traitement des risques (ex : comité de pilotage)
2. Éventuellement, estimer la performance des mesures (cf. ISO/IEC 27001) : pertinence (objectifs/moyens), efficacité (objectifs/résultats), efficience (résultats/moyens)
3. Surveiller les risques (outils et indicateurs), notamment les plus élevés, afin de détecter leur survenance au plus tôt
4. Revoir l'étude des risques
  - En cas de changement significatif dans les composants des risques (valeurs métier, biens supports, parties prenantes, etc.)
  - Au moins une fois par an (bonne pratique)



# Qu'avons-nous appris ?



1. Savoir déterminer des **mesures** pour traiter les risques
  2. Comprendre comment estimer et faire accepter les **risques résiduels**
  3. Comprendre comment **surveiller et suivre** les risques dans le temps
- Mettons tout cela en pratique !





# Plan de la formation

1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. Apprécier les risques
  - a. Approche par conformité
  - b. Approche par scénarios
5. Traiter les risques
6. Étude de cas complète
7. Conclusion



# Étude de cas

## Présentation

Vous êtes amené à réfléchir sur un cas d'étude se basant sur la **démarche administrative de renouvellement d'un titre d'identité numérique (TIN)**.

L'objectif de l'étude est de **conduire une étude complète des risques sur le SI de renouvellement de TIN et ses interconnexions avec l'extérieur**. Le commanditaire de l'étude est la Société de Gestion des Titres d'Identité Numérique (SGTIN).

Vous pouvez désormais prendre connaissance du dossier d'étude de cas fourni.





# Étude de cas

Constituez des équipes et attribuez les rôles



Directeur de la SGTIN



Responsable métier



Responsable  
des achats



RSSI



DSI

## Répartition des rôles dans chaque équipe

- Nombre d'équipes : 1 à 4
- Nombre de personnes par équipe : 2 à 5





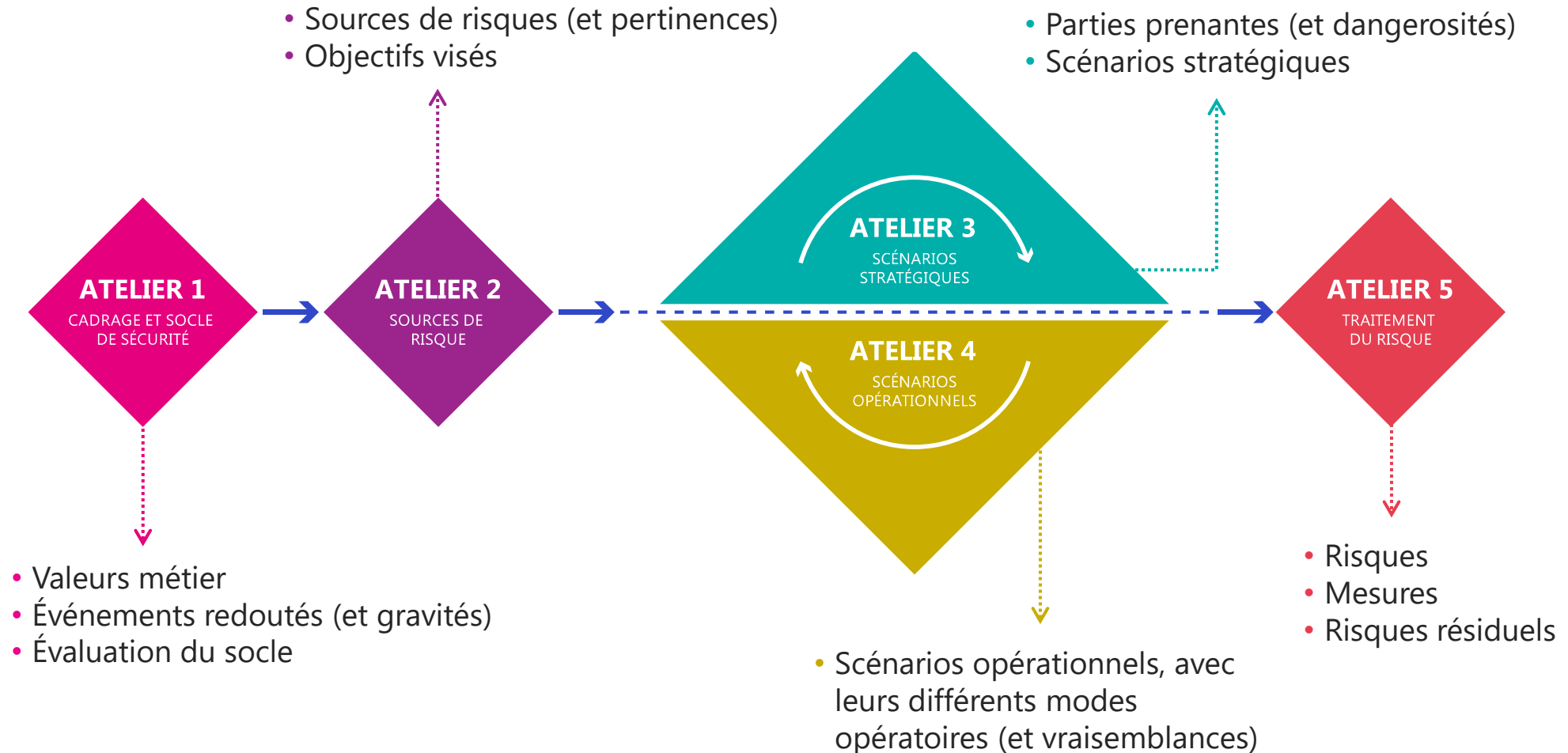
# Plan de la formation

1. Objectifs de la formation
2. Concepts indispensables
3. Établir le contexte
4. Apprécier les risques
  - a. Approche par conformité
  - b. Approche par scénarios
5. Traiter les risques
6. Étude de cas complète
7. Conclusion



# Ateliers d'EBIOS Risk Manager

## Résultats de la démarche complète





## Et maintenant ?

- Vous êtes maintenant capables de mener des études de risques, notamment avec la méthode EBIOS *Risk Manager*
- Vous trouverez d'autres informations dans les guides de l'ANSSI
  - Des informations plus détaillées
  - Des termes parfois différents (notamment ceux qui ne respectent pas les normes et cultures d'entreprises)
- Pour être compétent, l'idéal est de mener une étude de risques réelle



*La meilleure manière  
de commencer, c'est  
d'arrêter de parler et  
de s'y mettre.*

Walt Disney





# Allez, un dernier exercice !

Qu'est-ce qu'EBIOS ?



Une méthode  
d'analyse de risque ?



**Non**, c'est une méthode  
de gestion des risques :  
contexte, appréciation  
(identification, analyse,  
évaluation), traitement,  
communication, revue



Une usine à gaz ?



**Non**, c'est une boîte à  
outils, qu'il faut  
employer de manière  
appropriée (au  
commanditaire, à  
l'objectif, au niveau de  
maturité, etc.)



Des comprimés  
pour l'indigestion ?



Hé **Oui** ;)



EBIOS c'est la vie ?



**Évidemment !**  
On peut l'employer dans  
tous les domaines  
(sécurité, vie privée, etc.)  
et sur tous les objets  
(organisation, système,  
composant, etc.)





## Pour finir...

- Vous sentez-vous prêts à mener une étude de risques ?
- Vos objectifs pour cette formation sont-ils atteints ?
- Avez-vous des questions ?



**Matthieu GRALL**

Expert en management des données,  
sécurité de l'information, protection de  
la vie privée et nouvelles technologies

matthieu.grall [at] expert-conseil.pro

10/06/2025

TLP:CLEAR

PAP:CLEAR








# Ressources utilisées

- Référentiels
  - ISO 31000:2018
  - ISO/IEC 27005:2002
  - EBIOS *Risk Manager* de 2024
  - Kit de formation EBIOS *Risk Manager* de 2024
- Images
  - Page de garde : Grid, par Magic Creative, de PIXABAY
  - Logo et illustrations liées à EBIOS *Risk Manager* : kit de formation de l'ANSSI



# Informations de versions

Date	Actions réalisées	
2018-2019	Création de la présentation Julie DUCLOS et Maricela PELEGRIN-BOMEL (ANSSI)	
08/04/2020	Améliorations (mise en cohérence avec le Livret formateur et le Livret stagiaire) Matthieu GRALL (SODIFRANCE)	
2024	Publication d'un nouveau kit de formation ANSSI	
10/06/2025	Exploitation du nouveau kit de formation de l'ANSSI (récupération d'illustrations, non reprise des éléments marketing, obsolètes, de culture générale, trop détaillés ou inutiles dans le cadre d'une formation à EBIOS <i>Risk Manager</i> , corrections des erreurs méthodologiques et des incohérences), amélioration de la cohérence avec les normes, ajout d'explications, mise en évidence des outils, améliorations mineures diverses (changement de modèle, mises en forme, animations, harmonisation de termes, etc.)  Matthieu GRALL	