



## Formation – CFSSI

1<sup>er</sup> semestre 2019

# Avant de commencer...



Présentations : Qui êtes vous ? Qu'attendez vous de la formation ?



Horaires : 9h15 – 12h00 ; 13h45 – 17h00 (2 pauses)



Objectif pédagogique :

**Être capable de réaliser une étude des risques selon la méthode EBIOS Risk Manager**



Approche pédagogique :

- Acquisition des prérequis nécessaires à la conduite d'une étude EBIOS Risk Manager
- Application successive des 5 ateliers pour comprendre les mécanismes
- Cas pratique traitant une étude EBIOS Risk Manager de bout en bout

# Programme

- ◆ EBIOS *Risk Manager* : les bases
  - ◆ 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
  - ◆ Étude de cas
- 

# Programme

- ◆ **E BIOS Risk Manager : les bases**
  - ◆ 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
  - ◆ Étude de cas
- 

## Qu'est-ce qu'un risque ?



# Qu'est-ce qu'un risque ?

## RISQUE

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

Objet de l'étude : la voiture

Mission : arriver à destination



Événement redouté : la voiture percute un arbre

## Quelle est la gravité de ce risque ?

Vitesse excessive



La gravité varie selon la vitesse de la voiture



La gravité varie également selon la taille de l'arbre



La gravité varie selon la valeur (prix, robustesse) de la voiture

**La gravité varie selon le nombre d'impacts et leur niveau mais aussi selon la valeur de l'objet étudié**

# Quelle est la vraisemblance de ce risque ?

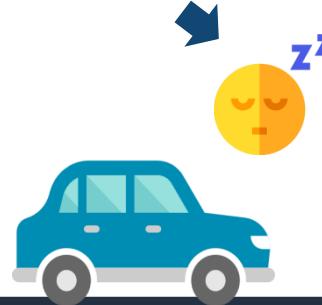
Menace : l'arbre

Plus d'arbres = exposition plus importante



La vraisemblance varie selon le nombre d'arbres

Vulnérabilité du conducteur



La vraisemblance varie selon le niveau d'attention du conducteur

Mesure de sécurité



La vraisemblance varie selon les panneaux de signalisation en place

**La vraisemblance varie selon l'exposition aux menaces, le niveau de vulnérabilité et les mesures de sécurité**

# Comment évaluer le niveau d'un risque ?

## NIVEAU DE RISQUE (EBIOS RISK MANAGER)

Mesure de l'importance du risque, exprimée par la combinaison de la gravité et de la vraisemblance



### GRAVITÉ

Estimation du niveau et de l'intensité des effets d'un risque



### VRAISEMBLANCE

Estimation de la faisabilité ou de la probabilité qu'un risque se réalise



L'estimation de la gravité et de la vraisemblance sont réalisées grâce à des échelles définies par l'organisation



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

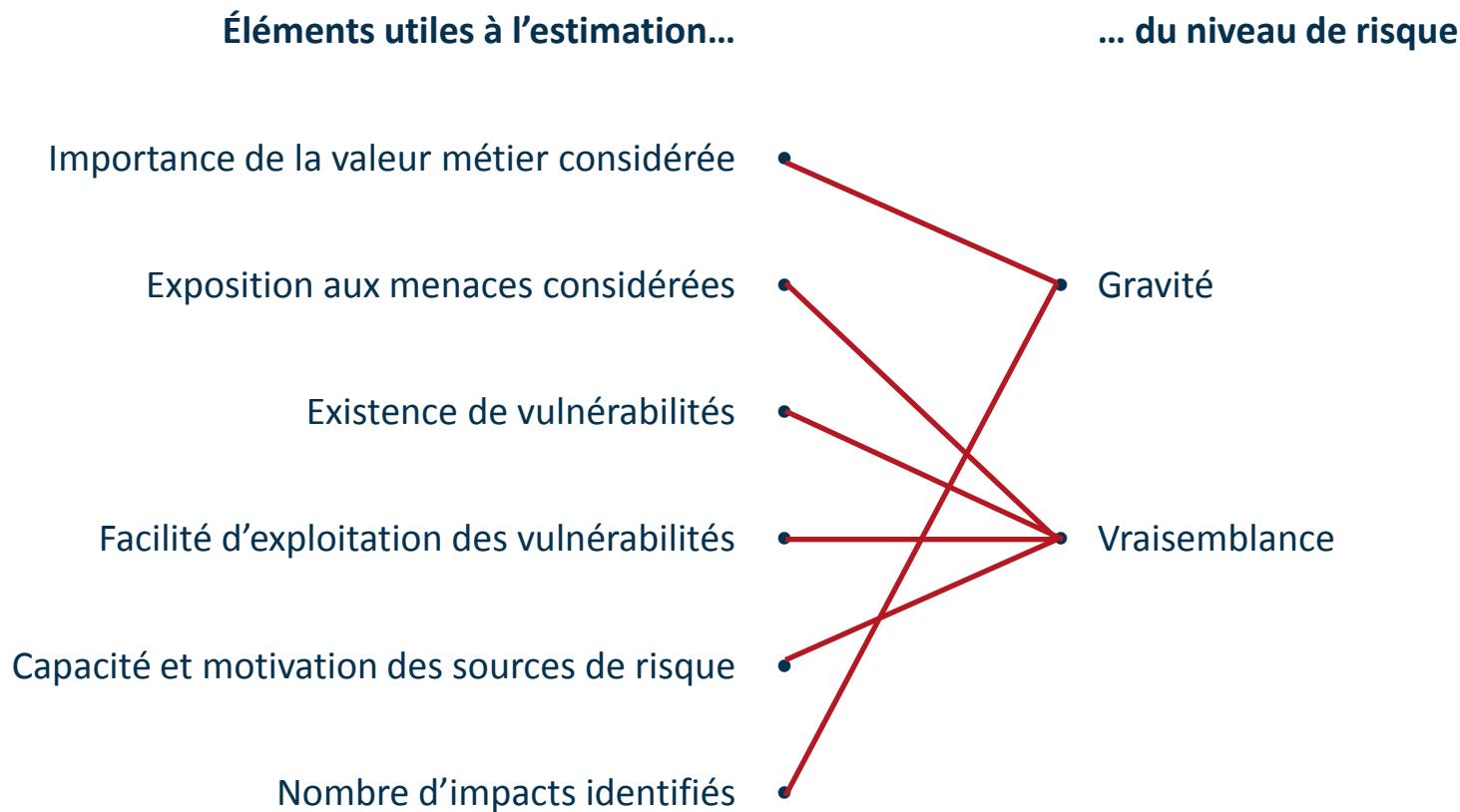
## Éléments utiles à l'estimation...

## ... du niveau de risque

- |  |   |                 |
|--|---|-----------------|
| Importance de la valeur métier considérée    | • |                 |
| Exposition aux menaces considérées           | • | • Gravité       |
| Existence de vulnérabilités                  | • |                 |
| Facilité d'exploitation des vulnérabilités   | • | • Vraisemblance |
| Capacité et motivation des sources de risque | • |                 |
| Nombre d'impacts identifiés                  | • |                 |



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



## Quelques questions à se poser

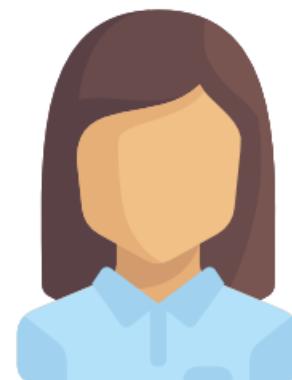


Quel est mon degré d'exposition à ces risques ?

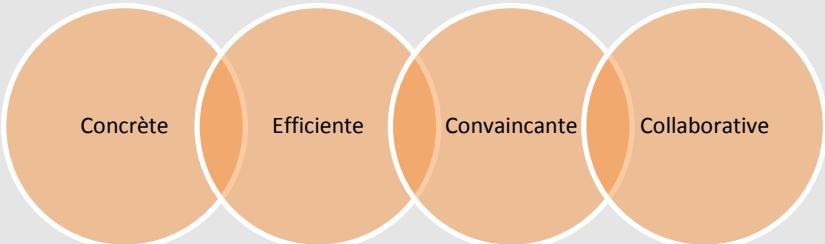
Comment maîtriser ces risques pour les rendre tolérables ou acceptables ?

Quels sont les risques qui pèsent sur mon SI ou mon projet ?

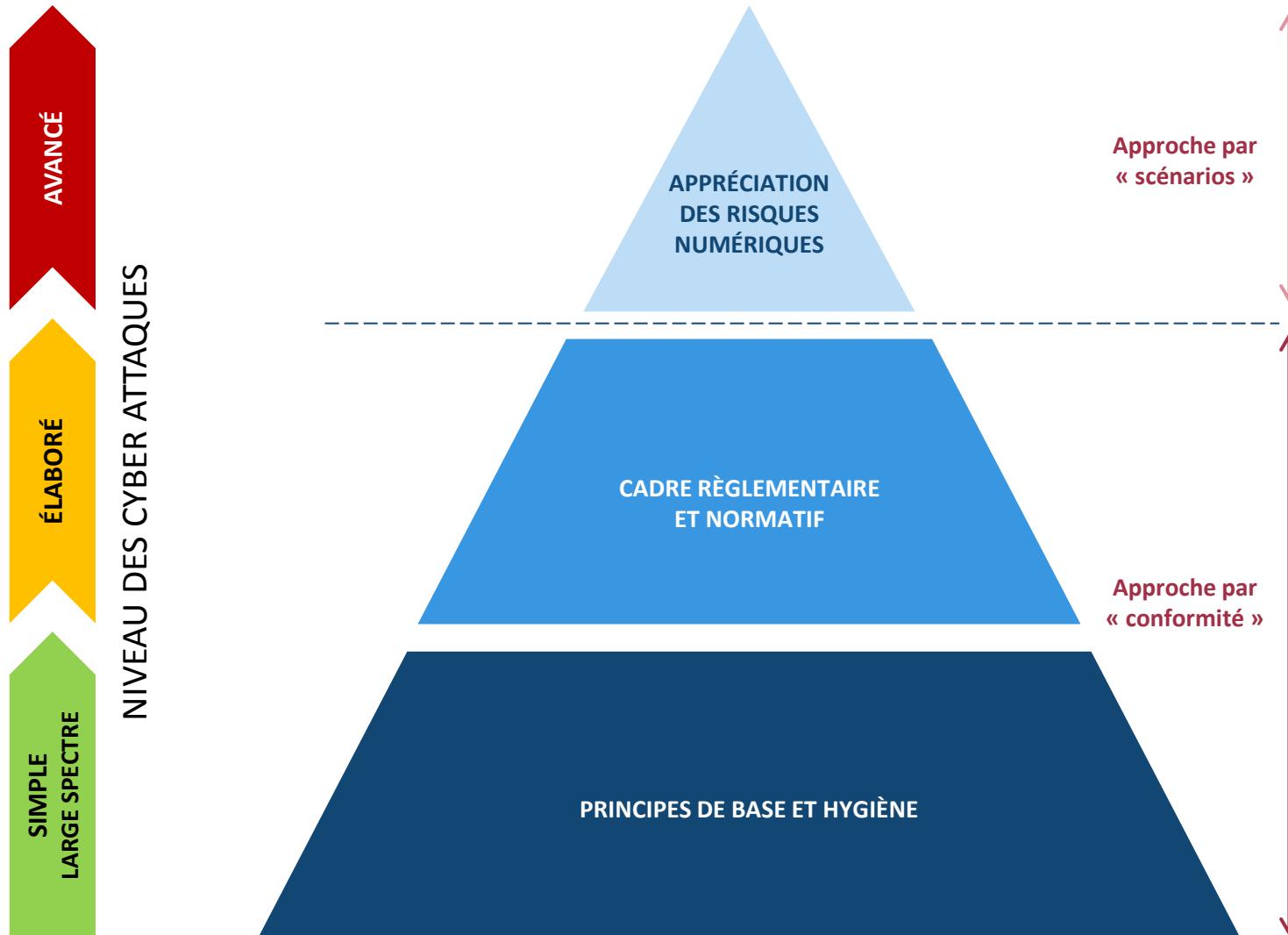
Comment gérer les risques dans le temps ?



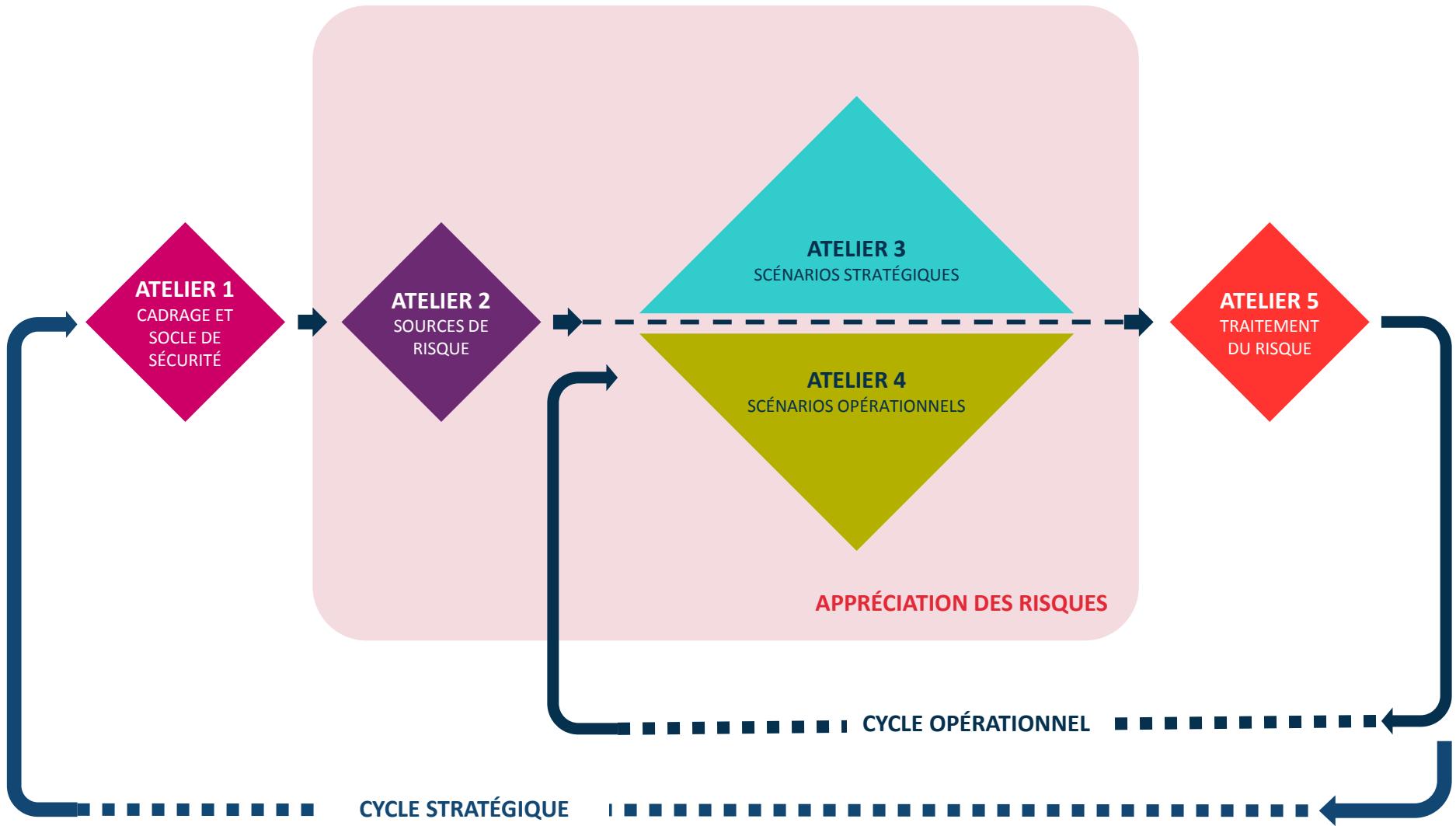
# Carte d'identité de la méthode EBIOS Risk Manager

UTILISATEURS	VISION
 <p><i>Risk managers</i> RSSI Chefs de projet</p>	<p><i>Offrir une compréhension partagée des risques cyber entre les décideurs et les opérationnels</i></p>
FONDAMENTAUX	VALEURS
<ul style="list-style-type: none"><li>• Une synthèse entre conformité et scénarios de risques</li><li>• Une alternance entre point de vue de l'organisation et celui de l'attaquant</li><li>• Une démarche structurée en ateliers, adaptable selon l'objectif de l'étude</li><li>• Une approche efficace plutôt qu'exhaustive</li><li>• Une prise en compte de l'écosystème</li></ul>	 <p>Concrète      Efficiente      Convaincante      Collaborative</p>

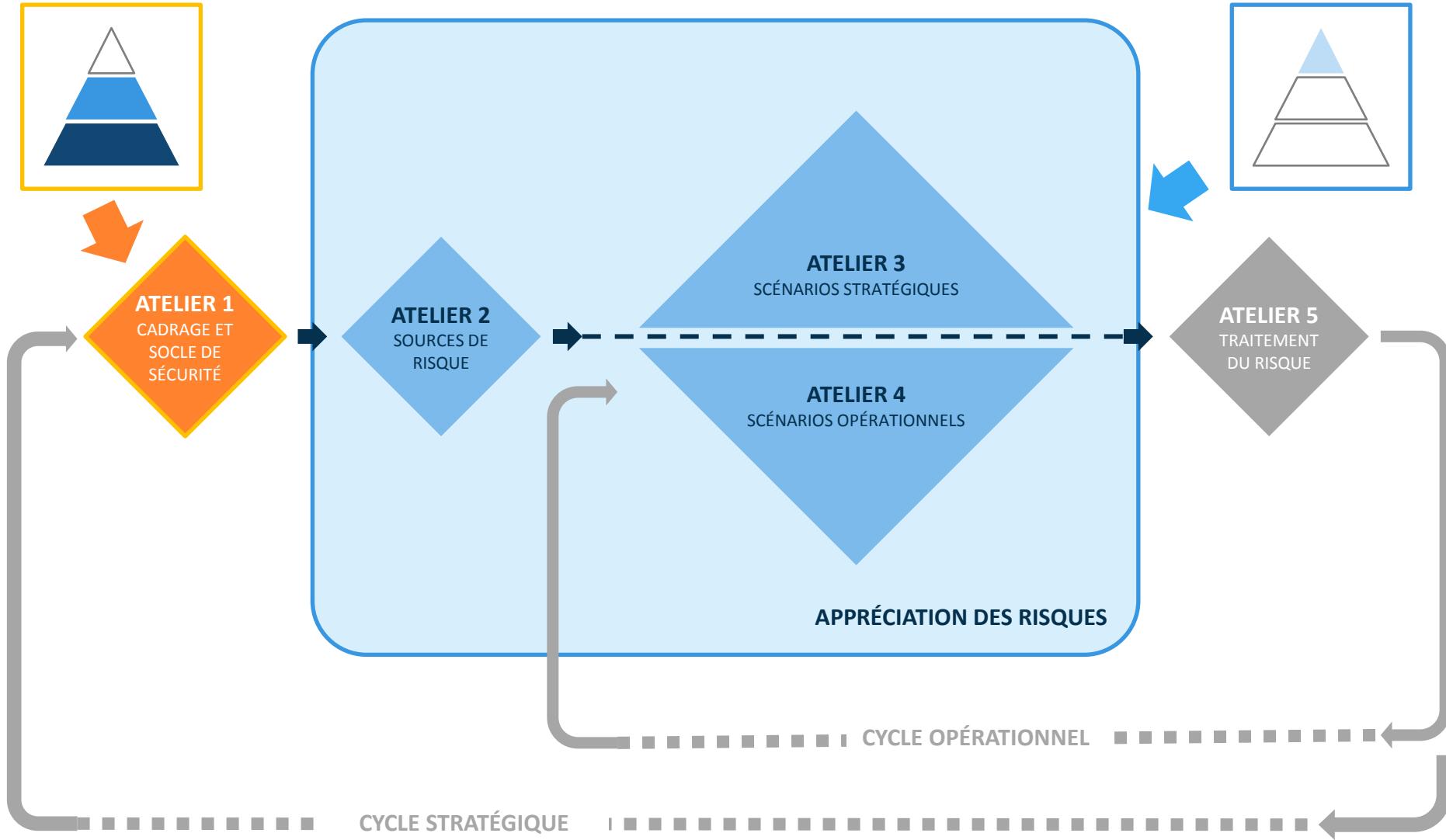
# La pyramide du management du risque : le concept phare de EBIOS Risk Manager



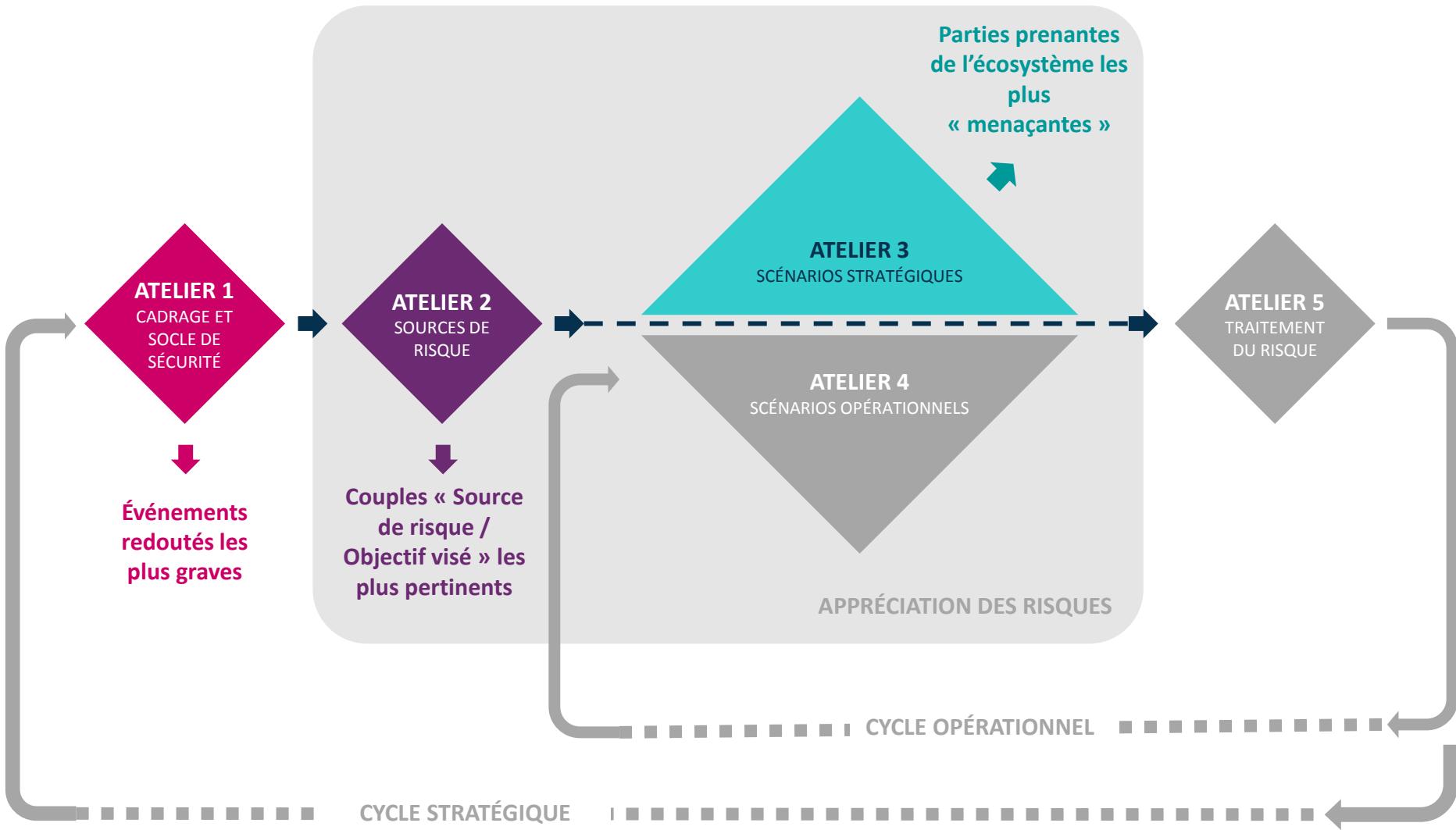
# EBIOS Risk Manager : une méthode basée sur 5 ateliers



# E BIOS Risk Manager - Pyramide de management du risque



# E BIOS Risk Manager : des choix à chaque étape



# Programme

- ◆ EBIOS Risk Manager : les bases
- ◆ **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
- ◆ Étude de cas





# Un peu de vocabulaire pour commencer

**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. [...]*

[Sources Internet : Le Point.fr et ZDNet]

ATTAQUE	
Source de risque	
Objectif visé	
Évènement redouté	
Valeur métier	
Bien support	
Impacts	



# Un peu de vocabulaire pour commencer

**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. [...]*

[Sources Internet : Le Point.fr et ZDNet]

ATTAQUE	
<b>Source de risque</b>	Adolescent
<b>Objectif visé</b>	Modifier ses résultats scolaires
<b>Évènement redouté</b>	Les résultats scolaires d'un ou plusieurs collégiens sont erronés
<b>Valeur métier</b>	Résultats scolaires
<b>Bien support</b>	Système informatique de gestion des résultats scolaires
<b>Impacts</b>	<ul style="list-style-type: none"><li>Impact sur la poursuite d'études des collégiens</li><li>Impact d'image vis-à-vis des autres établissements scolaires</li></ul>

# Atelier 1 : cadrage et socle de sécurité



**OBJECTIF :** Définir le cadre de l'étude et du projet, son périmètre métier et technique



## ÉLÉMENTS EN SORTIE :

- Éléments de cadrage de l'étude : participants, planning...
- Périmètre métier et technique : missions, valeurs métier, biens supports
- Événements redoutés et leur niveau de gravité
- Socle de sécurité : liste des référentiels applicables, état d'application, identification des écarts



**PARTICIPANTS :** Direction, Métiers, RSSI, DSi

## Définir le périmètre métier et technique : les questions à se poser

A quoi sert l'objet de l'étude ?  
Quelles sont ses **missions** principales, ses finalités ?

Quels sont les **valeurs métier** (processus et informations majeures) permettant à l'objet étudié de réaliser ses missions ?

Quels sont les **biens supports** (services numériques, réseaux informatiques, **ressources humaines, locaux**) qui permettent de mener à bien ces processus ou traiter ces informations ?



## Cas fictif – société de biotechnologies



### SOCIÉTÉ DE BIOTECHNOLOGIE FABRIQUANT DES VACCINS



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



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



Existence d'une charte informatique

# Définir le périmètre métier et technique

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 : <ul style="list-style-type: none"> <li>• le remplissage de seringues (stérilisation, remplissage) ;</li> <li>• le conditionnement (étiquetage et emballage).</li> </ul>	
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE)		Responsable production	
DÉNOMINATION DU/DES BIENS SUPPORTS ASSOCIÉS			
DESCRIPTION			
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE)			

# Définir le périmètre métier et technique

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 : <ul style="list-style-type: none"> <li>l'identification des antigènes ;</li> <li>la production des antigènes (vaccin vivant atténué, inactivé, sous-unité) : fermentation (récolte), purification, inactivation, filtration, stockage ;</li> <li>l'évaluation préclinique ;</li> <li>le développement clinique.</li> </ul>	Activité consistant à réaliser : <ul style="list-style-type: none"> <li>le remplissage de seringues (stérilisation, remplissage) ;</li> <li>le conditionnement (étiquetage et emballage).</li> </ul>	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			
DESCRIPTION			
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE)			

# Définir le périmètre métier et technique

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	<p>Activité de recherche et développement des vaccins nécessitant :</p> <ul style="list-style-type: none"> <li>l'identification des antigènes ;</li> <li>la production des antigènes (vaccin vivant atténué, inactivé, sous-unité) : fermentation (récolte), purification, inactivation, filtration, stockage ;</li> <li>l'évaluation préclinique ;</li> <li>le développement clinique.</li> </ul>	<p>Activité consistant à réaliser :</p> <ul style="list-style-type: none"> <li>le remplissage de seringues (stérilisation, remplissage) ;</li> <li>le conditionnement (étiquetage et emballage).</li> </ul>	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		Systèmes de production	
DESCRIPTION		Ensemble de machines et équipements informatiques permettant de fabriquer des vaccins à grande échelle	
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE/EXTERNE)		DSI + Fournisseurs de matériel	

# Définir le périmètre métier et technique

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 : <ul style="list-style-type: none"> <li>l'identification des antigènes ;</li> <li>la production des antigènes (vaccin vivant atténué, inactivé, sous-unité) : fermentation (récolte), purification, inactivation, filtration, stockage ;</li> <li>l'évaluation préclinique ;</li> <li>le développement clinique.</li> </ul>		Activité consistant à réaliser : <ul style="list-style-type: none"> <li>le remplissage de seringues (stérilisation, remplissage) ;</li> <li>le conditionnement (étiquetage et emballage).</li> </ul>	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

# Comment limiter le nombre de valeurs métier et de biens supports ?

Il ne s'agit pas dans cette étape de lister l'intégralité des valeurs métier et biens supports de l'organisation

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



**Ne conserver que les valeurs métiers identifiées comme les plus pertinentes ou sensibles**  
(les classer par exemple selon leurs besoins de sécurité)

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

**5 à 10 valeurs métiers constituent généralement une base suffisante**

Les valeurs métier qui n'auront pas été retenues pourront hériter des mesures prises pour protéger les autres valeurs métier

# Identifier les événements redoutés

## ÉVÉNEMENT REDOUTÉ

Un événement redouté est associé à une valeur métier et porte atteinte à l'un de ses besoins de sécurité

Objet de l'étude : la voiture

Mission : arriver à destination

Valeur métier : se déplacer (processus)



- Impacts sur la réalisation de la mission
- Impacts matériels
- Impacts sur la sécurité des personnes
- Impacts sur l'environnement
- Impacts financiers

Événement redouté : la voiture percute un arbre (la rendant ainsi inutilisable)

## Définir une échelle de gravité

ÉCHELLE	DÉFINITION
<b>G4 – CRITIQUE</b>	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée)
<b>G3 – GRAVE</b>	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé)
<b>G2 – SIGNIFICATIVE</b>	Dégradation des performances de l'activité sans impacts sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé)
<b>G1 – MINEURE</b>	Aucun impact opérationnel 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)



Il est recommandé de reprendre une échelle de gravité déjà définie dans l'organisation ou lors de l'étude des risques précédente



## Quelles sont les qualités d'une bonne échelle ?

Elle n'est pas ambiguë

Elle permet de faire du bricolage

Elle est explicite

Elle est comprise de ceux qui vont l'utiliser

Tous les niveaux sont susceptibles d'être utilisés

Elle privilégie un nombre de niveaux pair



## Quelles sont les qualités d'une bonne échelle ?

Elle n'est pas ambiguë



Elle permet de faire du bricolage



Elle est explicite



Elle est comprise de ceux qui vont l'utiliser



Tous les niveaux sont susceptibles d'être utilisés



Elle privilégie un nombre de niveaux pair





# Identifier les événements redoutés

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIES D'IMPACT	GRAVITÉ
R&D	Perte ou destruction des informations d'études et recherches	<ul style="list-style-type: none"><li>Impacts sur les missions et services de l'organisme</li><li>Impacts sur les coûts de développement</li><li>Impacts sur le patrimoine intellectuel</li></ul>	2

## Catégories d'impact (1/2)

Catégorie d'impact	Exemples (listes non exhaustives)
<b>Impacts sur les missions et services de l'organisme</b>	
Conséquences directes ou indirectes sur la réalisation des missions et services.	Incapacité à fournir un service, dégradation de performances opérationnelles, retards, impacts sur la production ou la distribution de biens ou de services, impossibilité de mettre en œuvre un processus clé.
<b>Impacts sur la gouvernance de l'organisme</b>	
<u>Impacts sur la capacité de développement ou de décision</u>  Conséquences directes ou indirectes sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement.	Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisme, changement contraint de stratégie, perte de fournisseurs ou de sous-traitants clés.
<u>Impacts sur le lien social interne</u>  Conséquences directes ou indirectes sur la qualité des liens sociaux au sein de l'organisation.	Perte de confiance des employés dans la pérennité de l'organisme, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, affaiblissement/perte de sens des valeurs communes.
<u>Impacts sur le patrimoine intellectuel ou culturel</u>  Conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes.	Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés.

## Catégories d'impact (2/2)

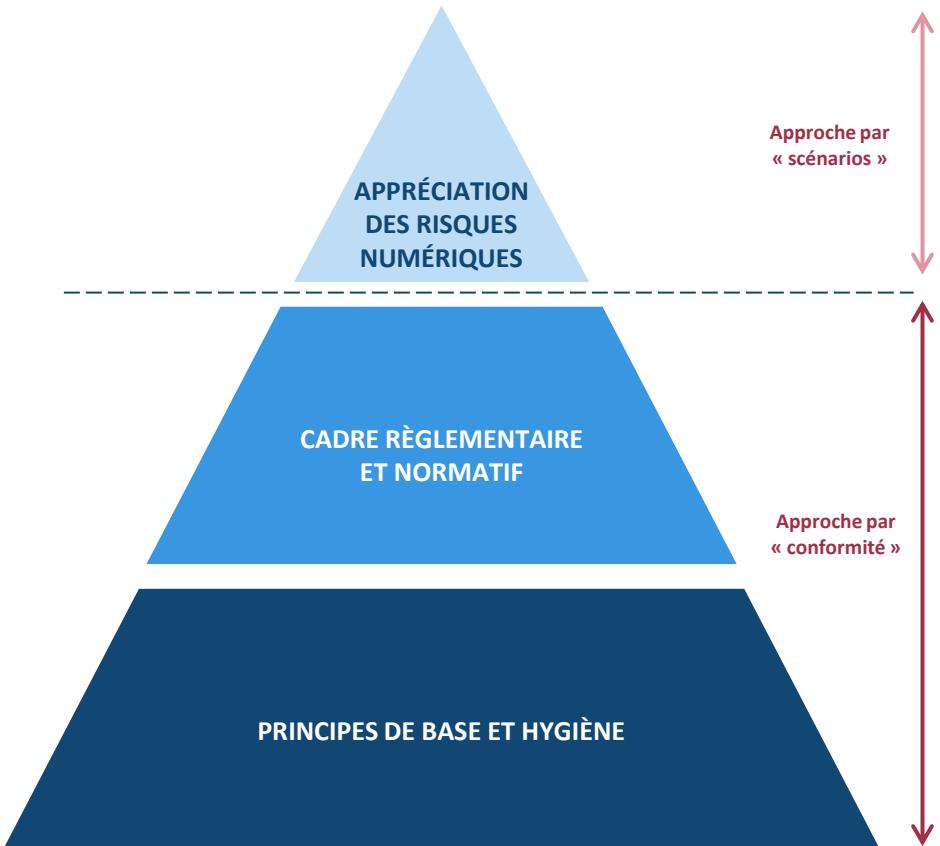
Catégorie d'impact	Exemples (listes non exhaustives)
<b>Impacts humains, matériels ou environnementaux</b>	
<u>Impacts sur la sécurité ou sur la santé des personnes</u>  Conséquences directes ou indirectes sur l'intégrité physique de personnes.	Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire.
<u>Impacts matériels</u>  Dégâts matériels ou destruction de biens supports.	Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématurée de matériels.
<u>Impacts sur l'environnement</u>  Conséquences écologiques à court ou long terme, directes ou indirectes.	Contamination radiologique ou chimique des nappes phréatiques ou des sols, rejet de polluants dans l'atmosphère.
<b>Impacts financiers</b>	
Conséquences pécuniaires, directes ou indirectes.	Perte de chiffre d'affaire, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées.
<b>Impacts juridiques</b>	
Conséquences suite à une non-conformité légale, réglementaire, normative ou contractuelle.	Procès, amende, condamnation d'un dirigeant, amendement de contrat.
<b>Impacts sur l'image et la confiance</b>	
Conséquences directes ou indirectes sur l'image de l'organisation, la notoriété, la confiance des clients.	Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte d'avance concurrentielle, perte de notoriété, perte de confiance d'usagers.



# Identifier les événements redoutés

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIES D'IMPACT	GRAVITÉ
R&D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée	<ul style="list-style-type: none"> <li>Impacts sur la sécurité ou la santé des personnes</li> <li>Impacts sur l'image et la confiance</li> <li>Impacts juridiques</li> </ul>	3
	Fuite des informations d'études et recherches de l'entreprise	<ul style="list-style-type: none"> <li>Impacts sur le patrimoine intellectuel</li> <li>Impacts financiers</li> </ul>	3
	Perte ou destruction des informations d'études et recherches	<ul style="list-style-type: none"> <li>Impacts sur les missions et services de l'organisme</li> <li>Impacts sur les coûts de développement</li> <li>Impacts 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>Impacts sur les missions et services de l'organisme</li> <li>Impacts financiers</li> </ul>	2
Fabriquer des vaccins	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>Impacts sur la sécurité ou la santé des personnes</li> <li>Impacts sur l'image et la confiance</li> <li>Impacts financiers</li> </ul>	4
	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>Impacts financiers</li> </ul>	2
Traçabilité et contrôle	Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire	<ul style="list-style-type: none"> <li>Impacts sur la sécurité ou la santé des personnes</li> <li>Impacts sur l'image et la confiance</li> <li>Impacts juridiques</li> </ul>	4

# Déterminer le socle de sécurité



## SOCLE DE SÉCURITÉ APPROCHE PAR « CONFORMITÉ »

Identifier l'ensemble des **référentiels de sécurité** (liste de mesures) qui s'appliquent à l'objet de l'étude :

- **Bonnes pratiques de sécurité** : guides de recommandations de l'ANSSI, règles de sécurité internes à l'organisation (PSSI), etc.
- **Normes** : famille ISO 27000, etc.
- **Règlementations en vigueur** : IGI 1300, II 901, LPM, directive NIS, RGS, etc.

→ Seuls les référentiels formulant des exigences en matière de sécurité sont à considérer

→ Intégration des résultats de précédentes études de risques à cette étape : les mesures de sécurité identifiées et mises en œuvre font désormais partie du socle de sécurité de l'organisation



# Déterminer le socle de sécurité

Politique de sécurité (PSSI) de l'organisation

Règlement européen de protection des données (RGPD)

Guide d'hygiène informatique

Annexe A de l'ISO 27001

Code de la santé publique

Arrêté sectoriel « produits de santé » (Loi de programmation militaire)

Instruction Générale Interministérielle 1300 (IGI 1300)



## Déterminer le socle de sécurité

Politique de sécurité (PSSI) de l'organisation



Règlement européen de protection des données (RGPD)



Guide d'hygiène informatique



Annexe A de l'ISO 27001



Code de la santé publique



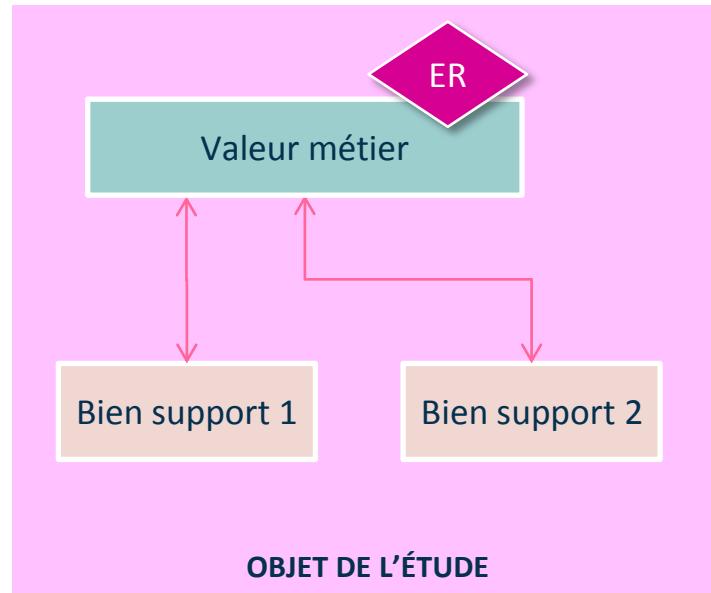
Arrêté sectoriel « produits de santé » (Loi de programmation militaire)



Instruction Générale Interministérielle 1300 (IGI 1300)



# Comment constituer les scénarios de risques ? (fin de l'atelier 1)

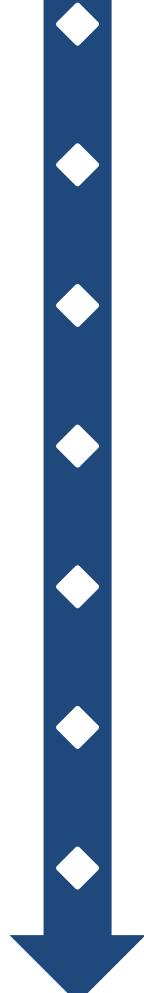


Légende :

ER Événement redouté relatif à une valeur métier de l'objet de l'étude

# Programme

- ◆ EBIOS Risk Manager : les bases
- ◆ 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
- ◆ Étude de cas



## Atelier 2 : sources de risque



**OBJECTIF :** Identifier les Sources de Risque (SR) et leurs Objectifs Visés (OV) en lien avec l'objet de l'étude

### ÉLÉMENTS EN ENTRÉE :

- Valeurs métier (**atelier 1**)
- Événements redoutés (**atelier 1**)



### ÉLÉMENTS EN SORTIE :

- Liste des couples SR/OV retenus pour la suite de l'étude
- Liste des couples SR/OV secondaires, qui seront si possible mis sous surveillance
- Représentation des SR/OV sous la forme d'une cartographie



**PARTICIPANTS :** Métiers, RSSI, (Spécialiste analyse de la menace cyber), Direction (validation des résultats de l'atelier)

# Etat de la menace, quelques tendances

**Allemagne : des centaines de données personnelles de politiques, militants, journalistes et artistes piratées**

Source : Libération – 04/01/2019

Le ransomware (rançongiciel) SamSam a déjà permis de mettre la main sur quelque 5,9 millions de dollars depuis qu'il s'est manifesté pour la première fois fin 2015 et qu'il a fait pas mal de victimes belges.

Source : Datanews – 01/08/2018

ACCUEIL > HIGH-TECH

**Piratage massif du groupe hôtelier Marriott, 500 millions de clients touchés**

CYBERSECURITE C'est le second plus gros vol de données après celui dont avait été victime Yahoo en 2013...

Source : 20 minutes – 30/11/2018

**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 impact – 12/11/2018

## Comment évaluer la pertinence des couples SR/OV ?

		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 <small>Intérêts, éléments qui poussent la source de risque à atteindre son objectif</small>	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



DEGRÉ DE PERTINENCE D'UN COUPLE SR/OV



# Évaluer les couples SR/OV et sélectionner les plus pertinents

SOURCES DE RISQUE	OBJECTIFS VISÉS	MOTIVATION	RESSOURCES	PERTINENCE
Hacktiviste	Divulguer des informations sur les tests animaliers	Peu motivé	Ressources significatives	Moyennement pertinent

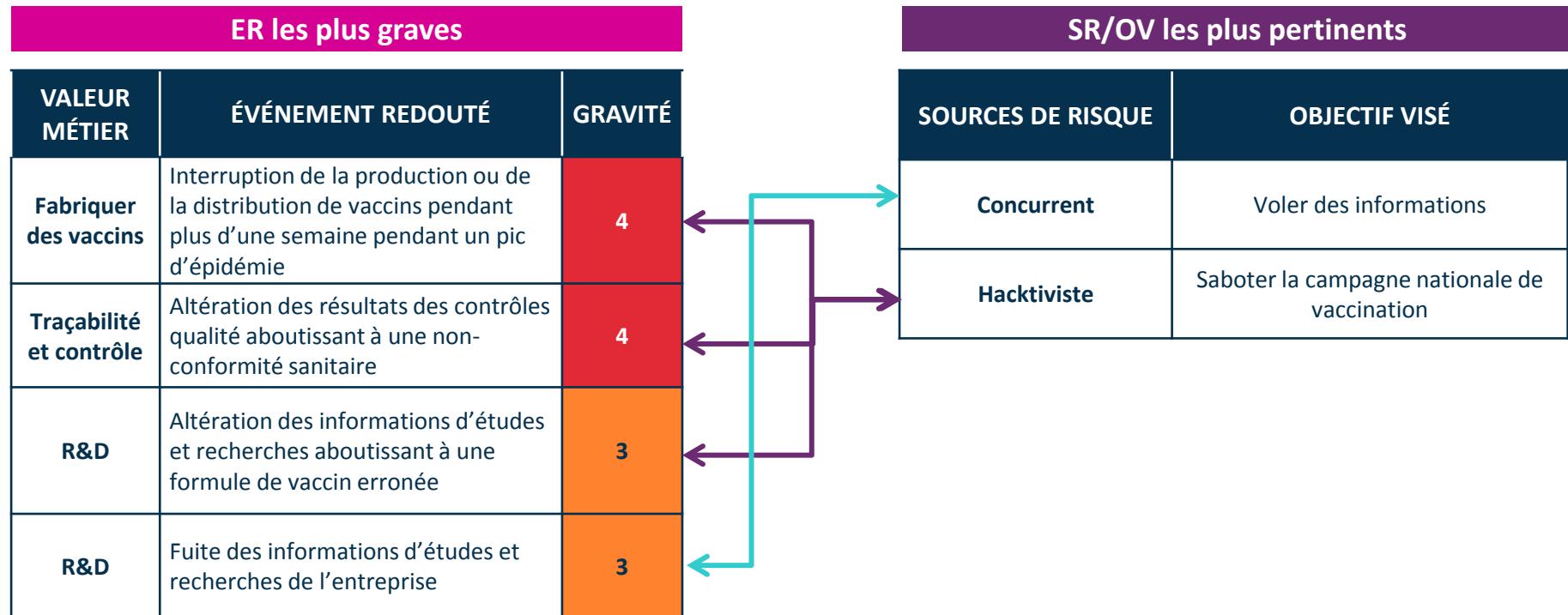


# Évaluer les couples SR/OV et sélectionner les plus pertinents

SOURCES DE RISQUE	OBJECTIFS VISÉS	MOTIVATION	RESSOURCES	PERTINENCE
Concurrent	Voler des informations	Fortement motivé	Ressources importantes	Très pertinent
Hacktiviste	Saboter la campagne nationale de vaccination	Assez motivé	Ressources significatives	Plutôt pertinent
Hacktiviste	Divulguer des informations sur les tests animaliers	Peu motivé	Ressources significatives	Moyennement pertinent
Cyber-terroriste	Altérer la composition des vaccins à des fins de bioterrorisme	Peu motivé	Ressources limitées	Peu pertinent

Dans ce contexte, les couples SR/OV très pertinents ou plutôt pertinents seront retenus pour la suite de l'étude

## Quelle gravité pour mon scénario stratégique ?





## Récapitulons le vocabulaire que nous avons vu

**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.*

[Sources Internet : Le Point.fr et ZDNet]

	PREMIÈRE ATTAQUE	SECONDE ATTAQUE
<b>Source de risque</b>	Adolescent	
<b>Objectif visé</b>	Modifier ses résultats scolaires	
<b>Évènement redouté</b>	Les résultats scolaires d'un ou plusieurs collégiens sont erronées	
<b>Valeur métier</b>	Résultats scolaires (information)	
<b>Bien support</b>	Système informatique de gestion des résultats scolaires	
<b>Impacts</b>	<ul style="list-style-type: none"><li>Impact sur la poursuite d'études des collégiens</li><li>Impact d'image vis-à-vis des autres établissements scolaires</li></ul>	



## Récapitulons le vocabulaire que nous avons vu

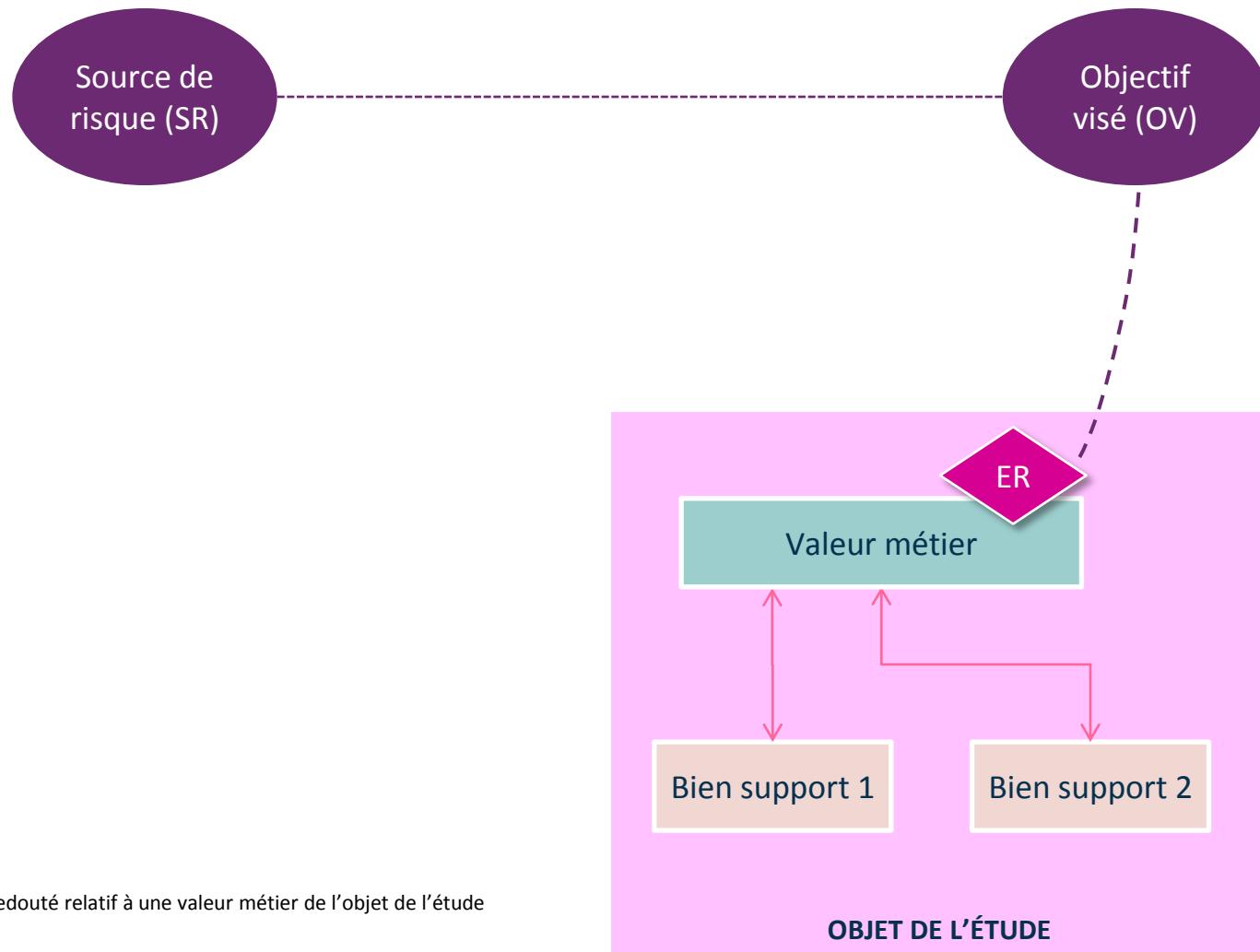
**Un adolescent de 15 ans « pirate » le système de son collège pour améliorer ses notes.**

*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.*

[Sources Internet : Le Point.fr et ZDNet]

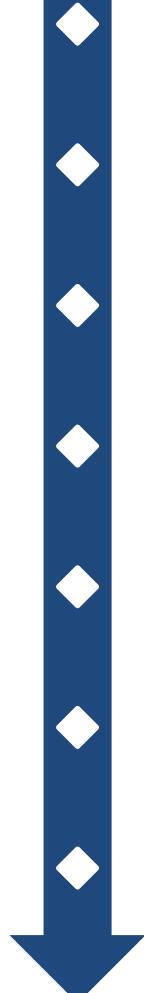
	PREMIÈRE ATTAQUE	SECONDE ATTAQUE
<b>Source de risque</b>	Adolescent	Adolescent
<b>Objectif visé</b>	Modifier ses résultats scolaires	Se venger du collège
<b>Évènement redouté</b>	Les résultats scolaires d'un ou plusieurs collégiens sont erronées	Les échanges avec les collégiens ou leurs familles sont impossibles pendant plusieurs jours
<b>Valeur métier</b>	Résultats scolaires	Échanger des informations
<b>Bien support</b>	Système informatique de gestion des résultats scolaires	Service informatique d'échange de courriels
<b>Impacts</b>	<ul style="list-style-type: none"> <li>• Impact sur la poursuite d'études des collégiens</li> <li>• Impact d'image vis-à-vis des autres établissements scolaires</li> </ul>	<ul style="list-style-type: none"> <li>• Impact d'image vis-à-vis des familles</li> <li>• Impact sur les missions et services du collège</li> </ul>

# Comment constituer les scénarios de risques ? (fin de l'atelier 2)



# Programme

- ◆ EBIOS Risk Manager : les bases
- ◆ 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
- ◆ Étude de cas



## Atelier 3 : scénarios stratégiques



**OBJECTIF :** Identifier les parties prenantes critiques de l'écosystème et construire des scénarios de risque de haut niveau (scénarios stratégiques)

### ÉLÉMENTS EN ENTRÉE :

- Missions et valeurs métier (**atelier 1**)
- Événements redoutés et leur gravité (**atelier 1**)
- Sources de risque et objectifs visés retenus (**atelier 2**)



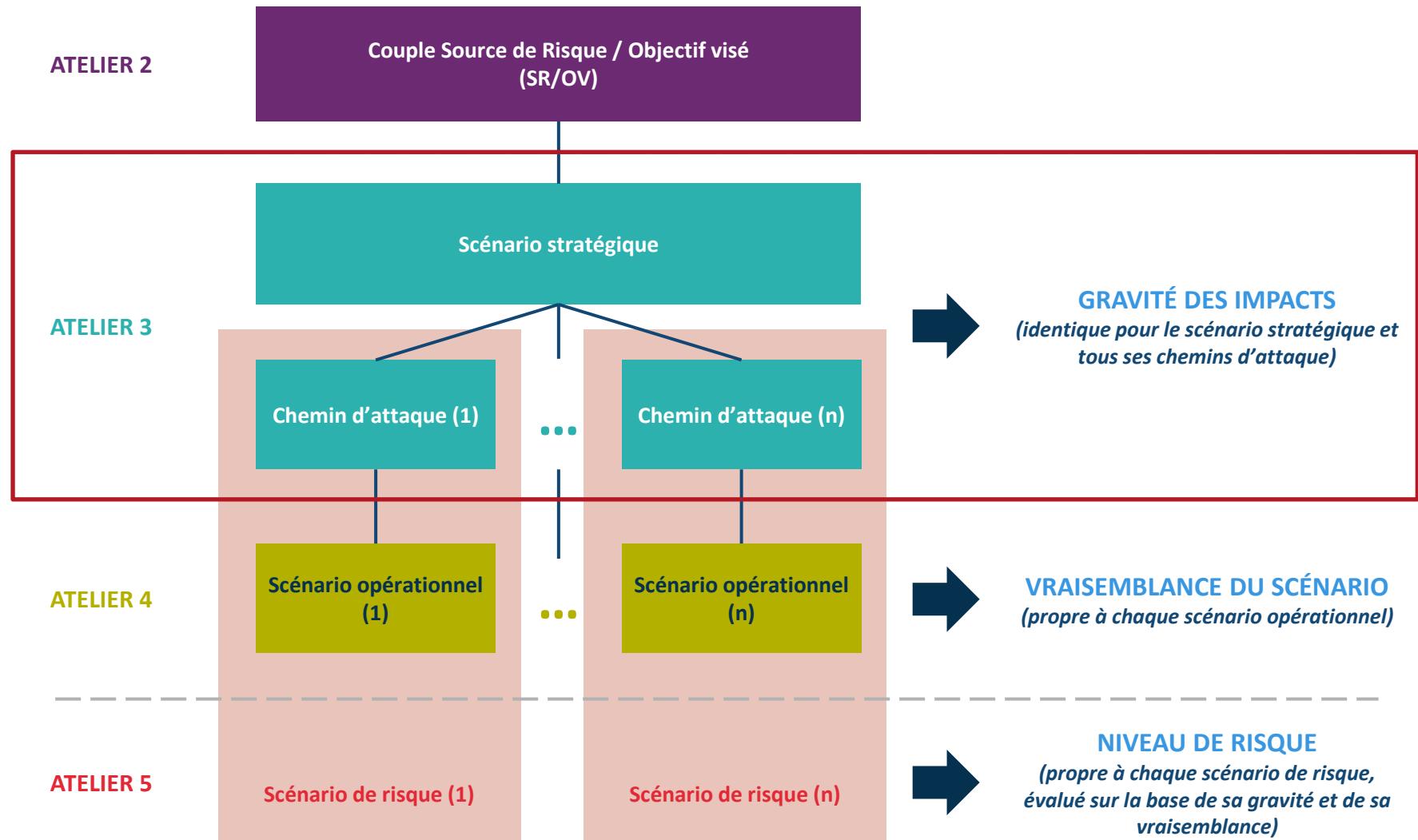
### ÉLÉMENTS EN SORTIE :

- Cartographie de menace de l'écosystème
- Scénarios stratégiques
- Mesures de sécurité retenues pour l'écosystème

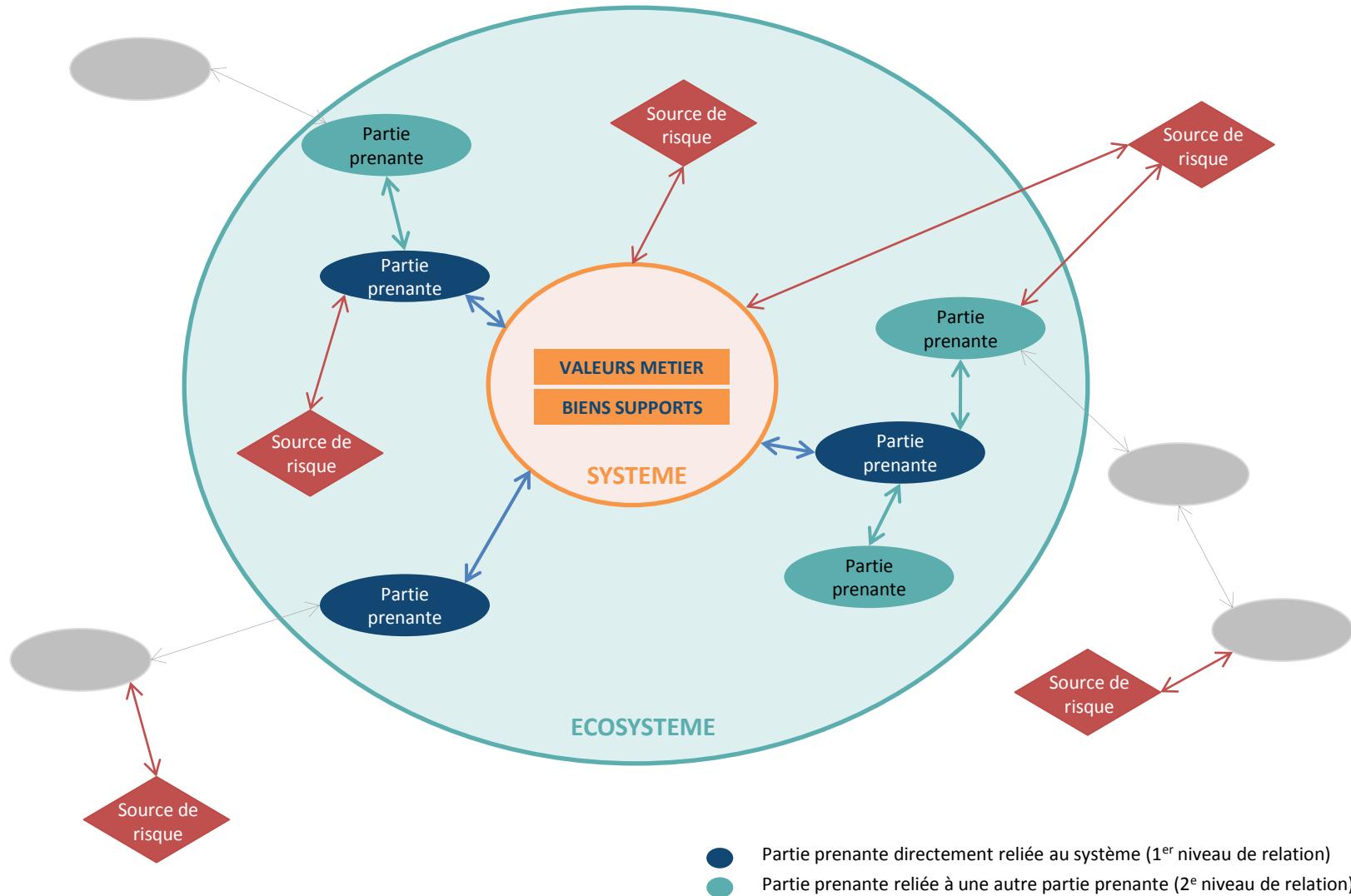


**PARTICIPANTS :** Métiers, Architectes fonctionnels, Juristes, RSSI, (Spécialiste cybersécurité)

# Articulation des différents ateliers

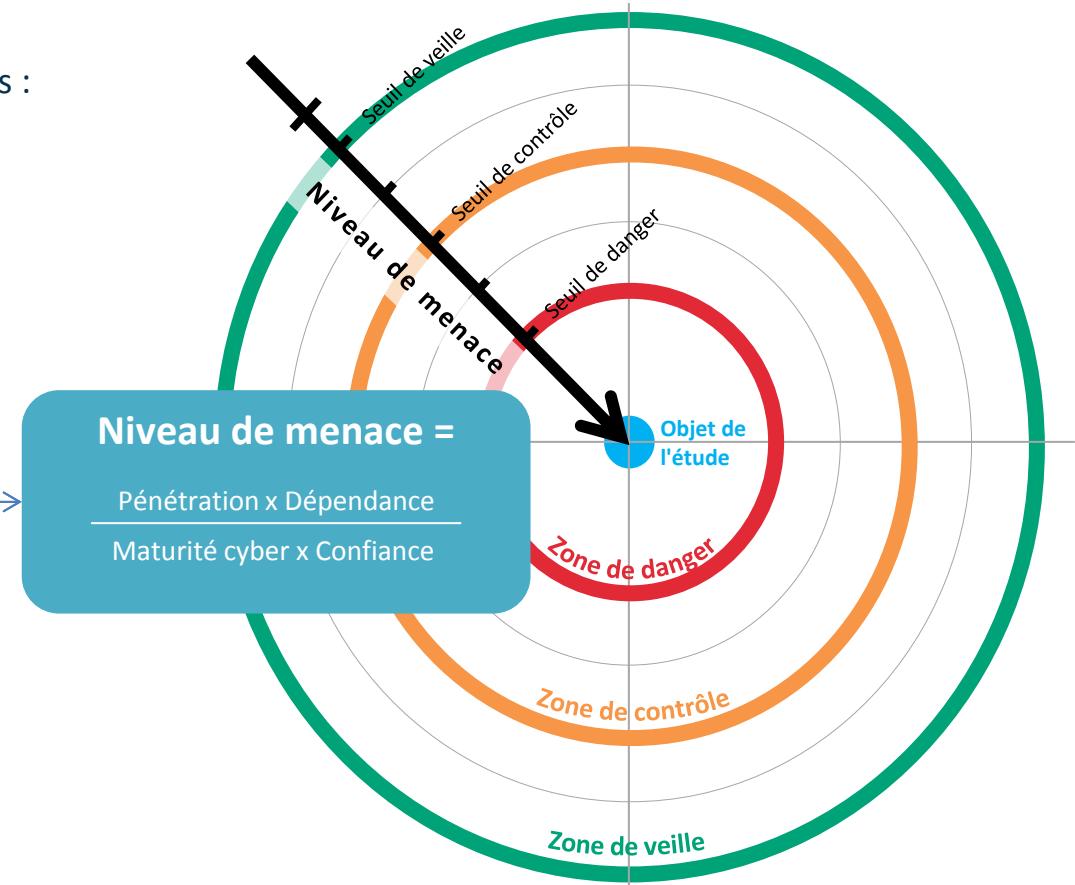
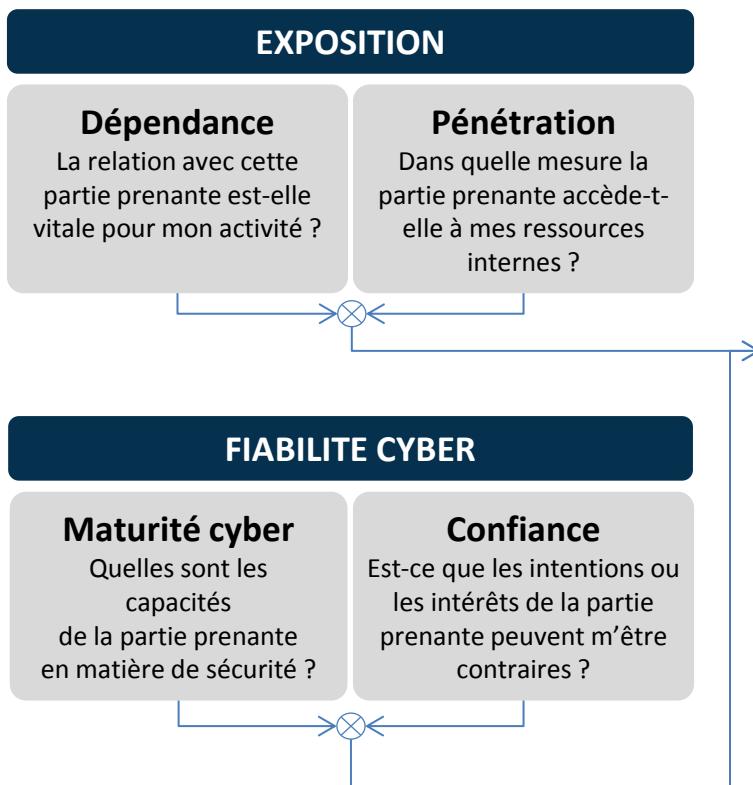


# Identifier les parties prenantes de l'écosystème



# Construire la cartographie de menace de l'écosystème

Pour chaque partie prenante, évaluer 4 critères :





# Évaluer le niveau de menace de chaque partie prenante

CATÉGORIE	NOM	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFiance	NIVEAU DE MENACE
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					



# Construire la cartographie de menace de l'écosystème

C1 – ETABLISSEMENTS DE SANTE

C2 – PHARMACIES

C3 – GROSSISTES REPARTITEURS

F1 – FOURNISSEURS INDUSTRIELS CHIMISTES

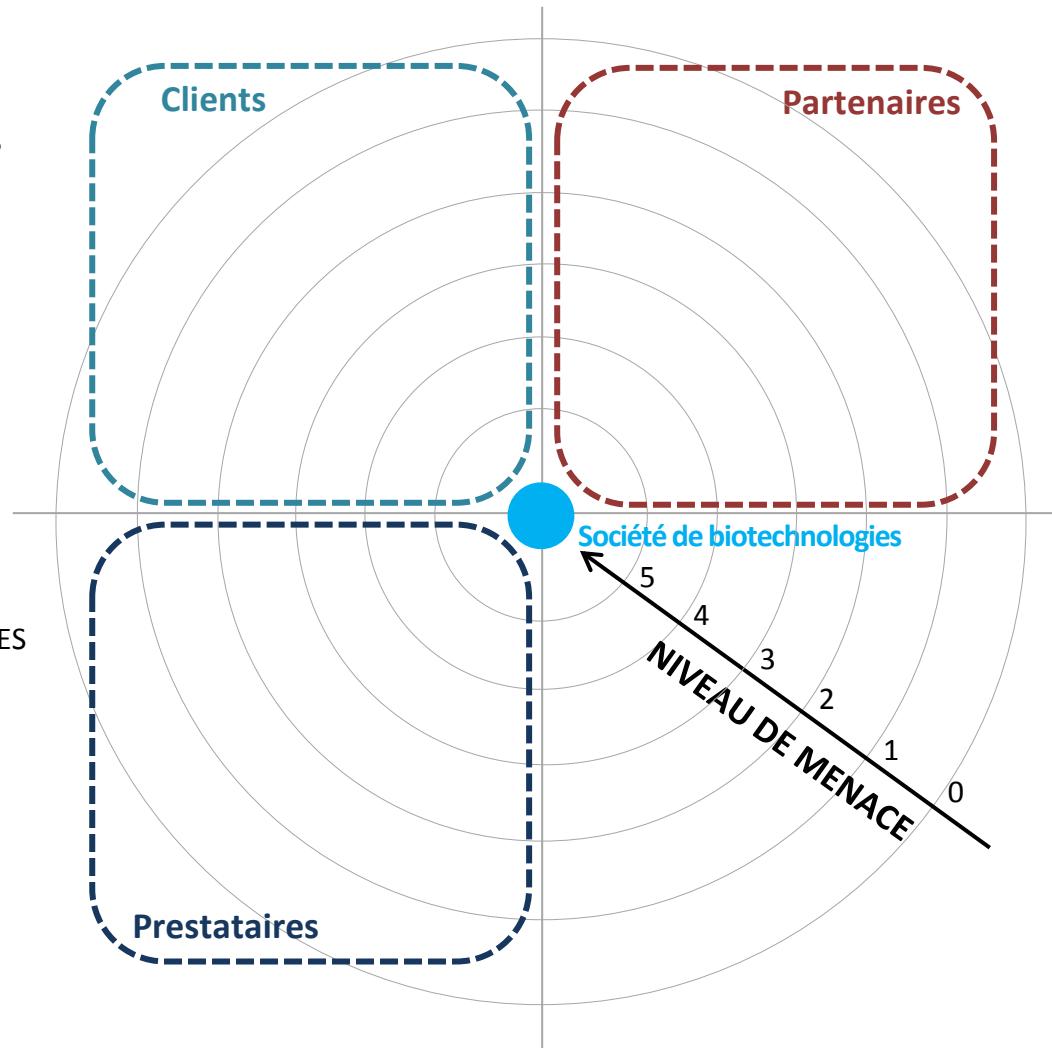
F2 – FOURNISSEURS DE MATERIEL

F3 – PRESTATAIRE INFORMATIQUE

P1 – UNIVERSITES

P2 – REGULATEURS

P3 – LABORATOIRES

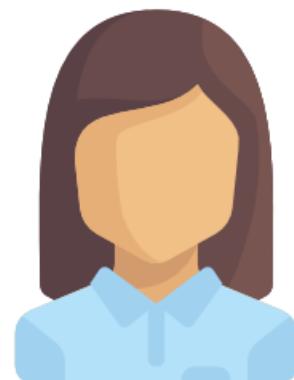




## Cartographie de menace de l'écosystème

Quelles sont les 3 parties prenantes les plus menaçantes (parties prenantes critiques) ?

Quelle est la partie prenante la moins menaçante ?





## Critères de cotation de la menace proposés

	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFiance
1	Pas de lien avec le SI de la partie prenante pour réaliser la mission	Pas d'accès ou accès avec des priviléges 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	Lien avec le SI de la partie prenante utile à la réalisation de la mission	Accès avec priviléges 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	Lien avec le SI de la partie prenante indispensable mais non exclusif (possible substitution)	Accès avec priviléges 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	Lien avec le SI de la partie prenante indispensable et unique (pas de substitution possible)	Accès avec priviléges de type administrateur à des équipements d'infrastructure (annuaires d'entreprise, DNS, DHCP, switchs, 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.



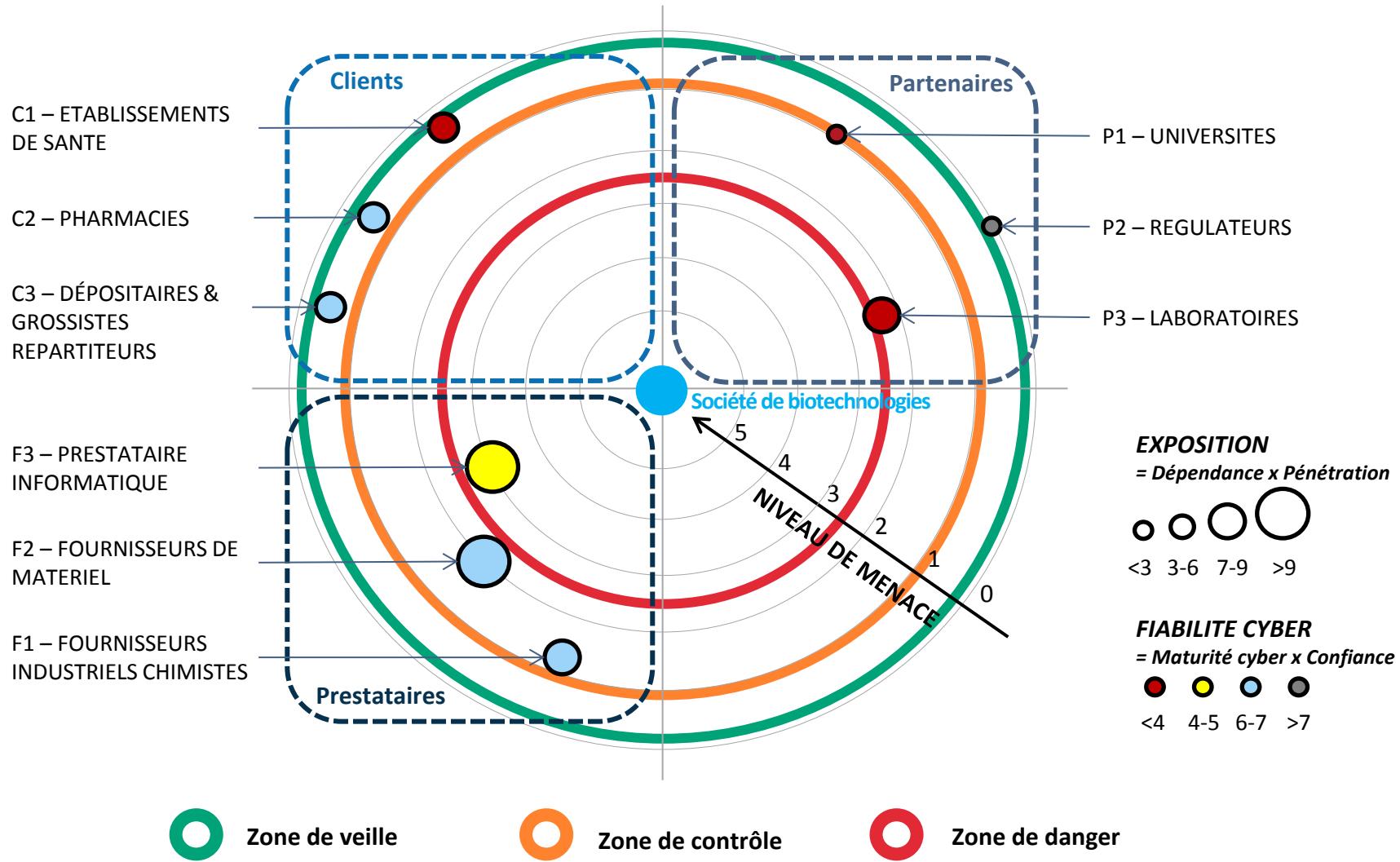
## Évaluer le niveau de menace de chaque partie prenante

CATÉGORIE	NOM	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFiance	NIVEAU DE MENACE
Client	C1 - Établissements de santé	1	1	1	3	0,3
Client	C2 - Pharmacies	1	1	2	3	0,2
Client	C3 - Grossistes répartiteurs	1	2	2	3	0,3
Partenaire	P1 - Universités	2	1	1	2	1
Partenaire	P2 - Régulateurs (ANSM, EMA...)	2	1	2	4	0,25
Partenaire	P3 - Laboratoires	3	3	2	2	2,25
Prestataire	F1 - Fournisseurs industriels chimistes	4	2	2	3	1,3
Prestataire	F2 - Fournisseurs de matériel (chaîne de production)	4	3	2	3	2
Prestataire	F3 - Prestataire informatique	3	4	2	2	3



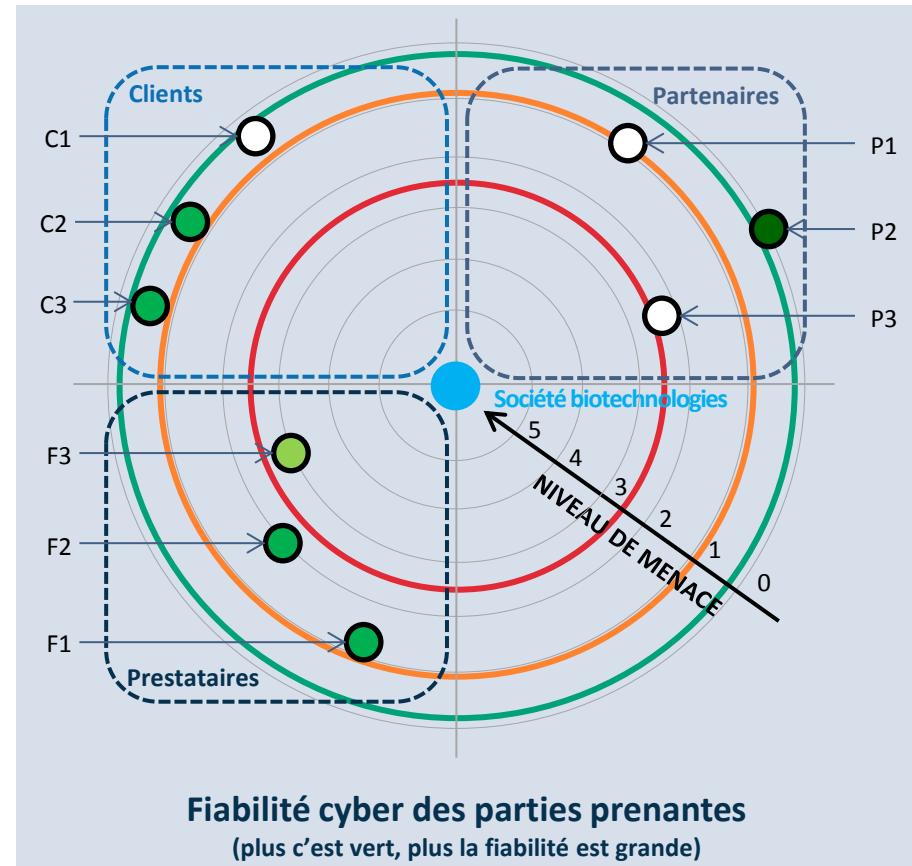
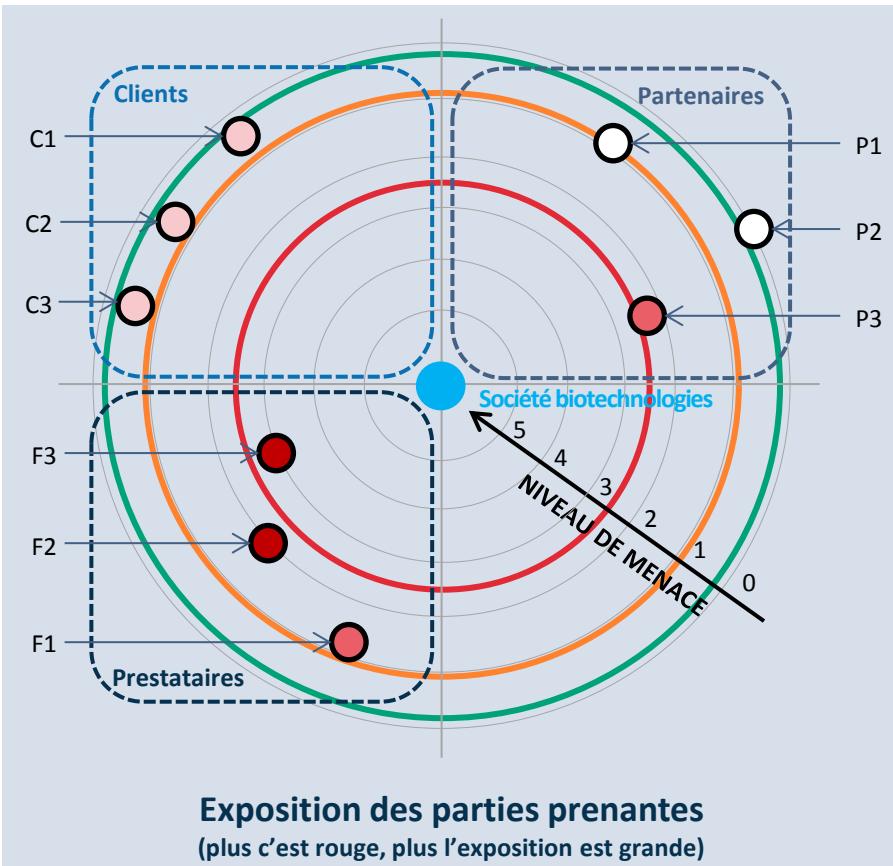


# Construire la cartographie de menace de l'écosystème





# Construire la cartographie de menace de l'écosystème (autre proposition de représentation)



Plus on est proche du centre, plus la partie prenante est menaçante

**Légende :**

C1 – ÉTABLISSEMENTS DE SANTÉ

C2 – PHARMACIES

C3 – DÉPOSITAIRES & GROSSISTES RÉPARTITEURS

P1 – UNIVERSITÉS

P2 – RÉGULATEURS

P3 – LABORATOIRES

F1 – FOURNISSEURS INDUSTRIELS CHIMISTES

F2 – FOURNISSEURS DE MATERIEL

F3 – PRESTATAIRE INFORMATIQUE

ZONE DE VEILLE

ZONE DE CONTRÔLE

ZONE DE DANGER

# Élaborer des scénarios stratégiques (du point de vue de l'attaquant)

Quelles sont les **valeurs métier** de l'organisation que je dois viser pour atteindre mon objectif ?

Pour permettre ou faciliter mon attaque, suis-je susceptible d'**attaquer les parties prenantes critiques de l'écosystème** disposant d'un accès privilégié aux valeurs métier ?





# Élaborer des scénarios stratégiques

A2

Source de risque : Concurrent

Objectif visé : Voler des informations

SOURCE DE  
RISQUE



CONCURRENT

ECOSYSTÈME

SOCIÉTÉ DE BIOTECHNOLOGIE

Informations  
de R&D





# Élaborer des scénarios stratégiques

A2

Source de risque : Concurrent

Objectif visé : Voler des informations

**SOURCE DE RISQUE**



**CONCURRENT**

**ECOSYSTÈME**

1

2

3



**LABORATOIRE (P3)**



Une partie des  
informations de  
R&D



**PRESTATAIRE INFORMATIQUE  
(F3)**

**SOCIÉTÉ DE BIOTECHNOLOGIE**

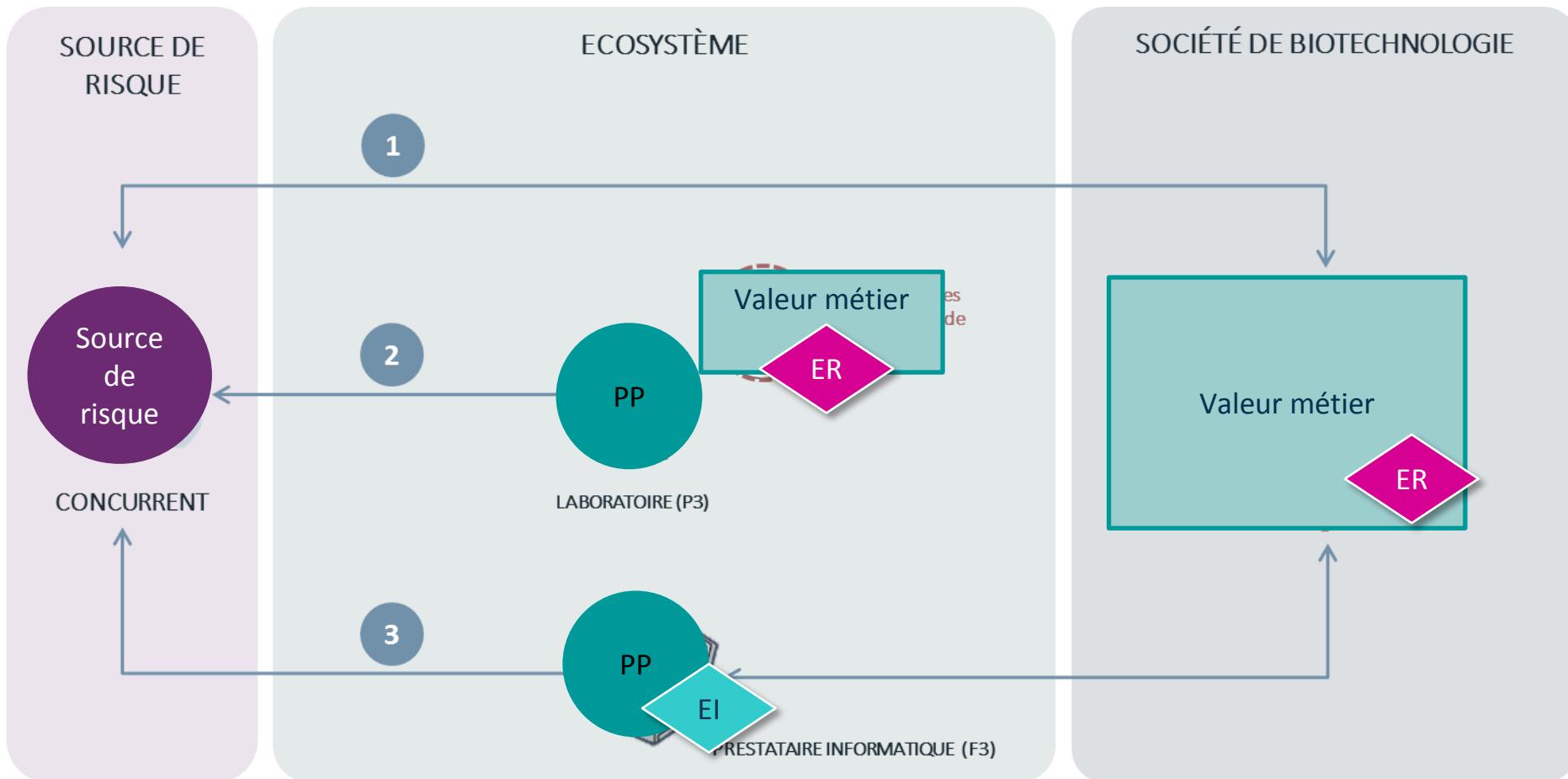
Informations  
de R&D



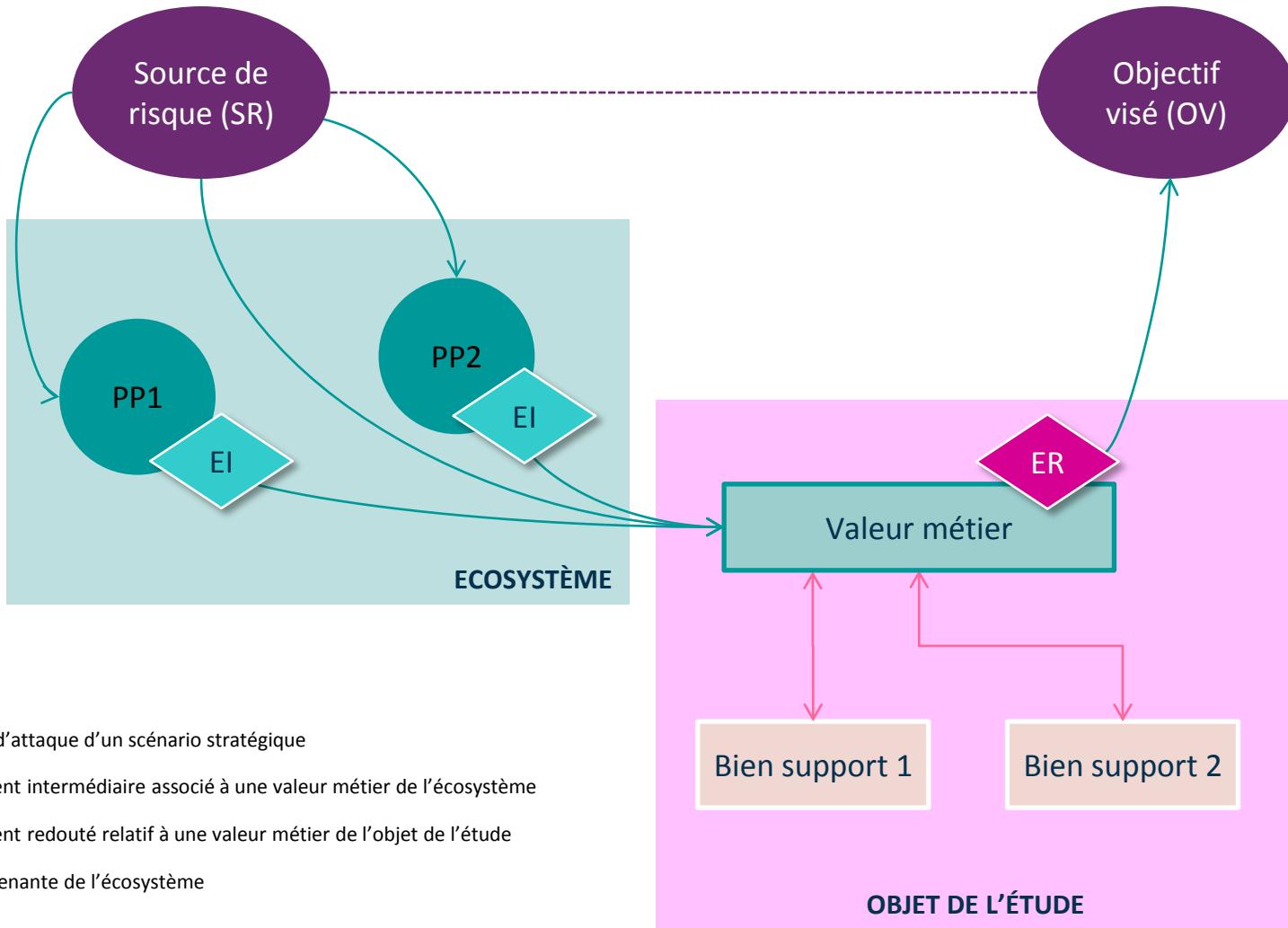
**Gravité : 3**

Un scénario stratégique constitué de 3 chemins d'attaque

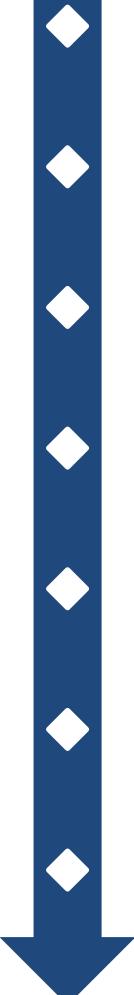
## Rappel du vocabulaire observé



# Comment constituer les scénarios de risques ? (fin de l'atelier 3)



# Programme

- ◆ EBIOS Risk Manager : les bases
  - ◆ 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
  - ◆ Étude de cas
- 

## Atelier 4 : scénarios opérationnels



**OBJECTIF :** Construire les scénarios opérationnels schématisant les modes opératoires techniques qui seront mis en œuvre par les sources de risque

### ÉLÉMENTS EN ENTRÉE :

- Missions, valeurs métier et biens supports (**atelier 1**)
- Socle de sécurité (**atelier 1**)
- Sources de risque et objectifs visés retenus (**atelier 2**)
- Scénarios stratégiques retenus (**atelier 3**)



### ÉLÉMENTS EN SORTIE :

- Scénarios opérationnels
- Évaluation des scénarios opérationnels en termes de vraisemblance



**PARTICIPANTS :** RSSI, DSI, Architectes SI, (Spécialiste cybersécurité)

## Rappel : articulation des ateliers

ATELIER 2

Couple Source de Risque / Objectif visé  
(SR/OV)

ATELIER 3

Scénario stratégique

Chemin d'attaque (1)

Chemin d'attaque (n)

ATELIER 4

Scénario opérationnel  
(1)

Scénario opérationnel  
(n)

ATELIER 5

Scénario de risque (1)

Scénario de risque (n)

**GRAVITÉ DES IMPACTS**

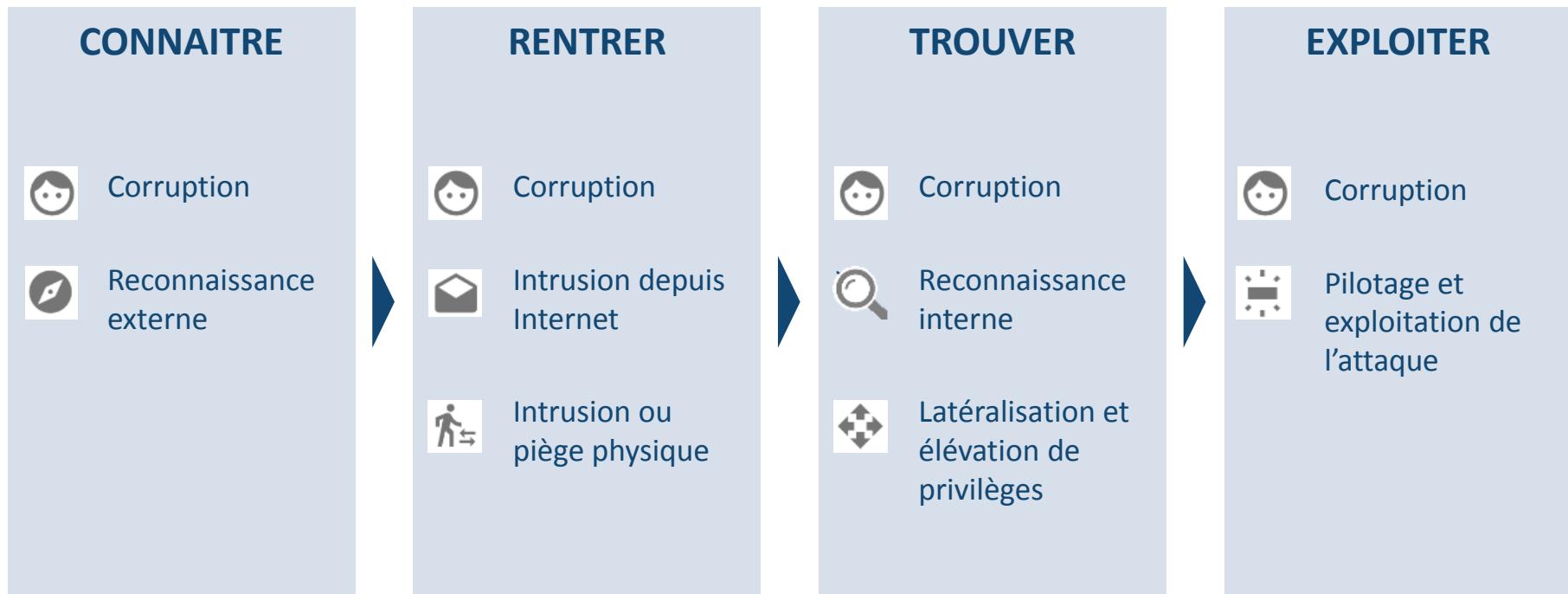
*(identique pour le scénario stratégique et tous ses chemins d'attaque)*

**VRAISEMBLANCE DU SCÉNARIO**  
*(propre à chaque scénario opérationnel)*

**NIVEAU DE RISQUE**

*(propre à chaque scénario de risque, évalué sur la base de sa gravité et de sa vraisemblance)*

# Des scénarios structurés selon une séquence d'attaque type



→ Il est important de noter que ces étapes sont modulaires (par exemple selon si l'attaquant attaque directement ou par rebond via une partie prenante de l'écosystème)



# Élaborer les scénarios opérationnels

A3

Scénario stratégique : Un concurrent vole des informations de R&D

Chemin d'attaque : n°1 – attaque directe

Gravité : 3

CONNAITRE

RENTRER

TROUVER

EXPLOITER

Vol et exploitation  
de données de  
R&D



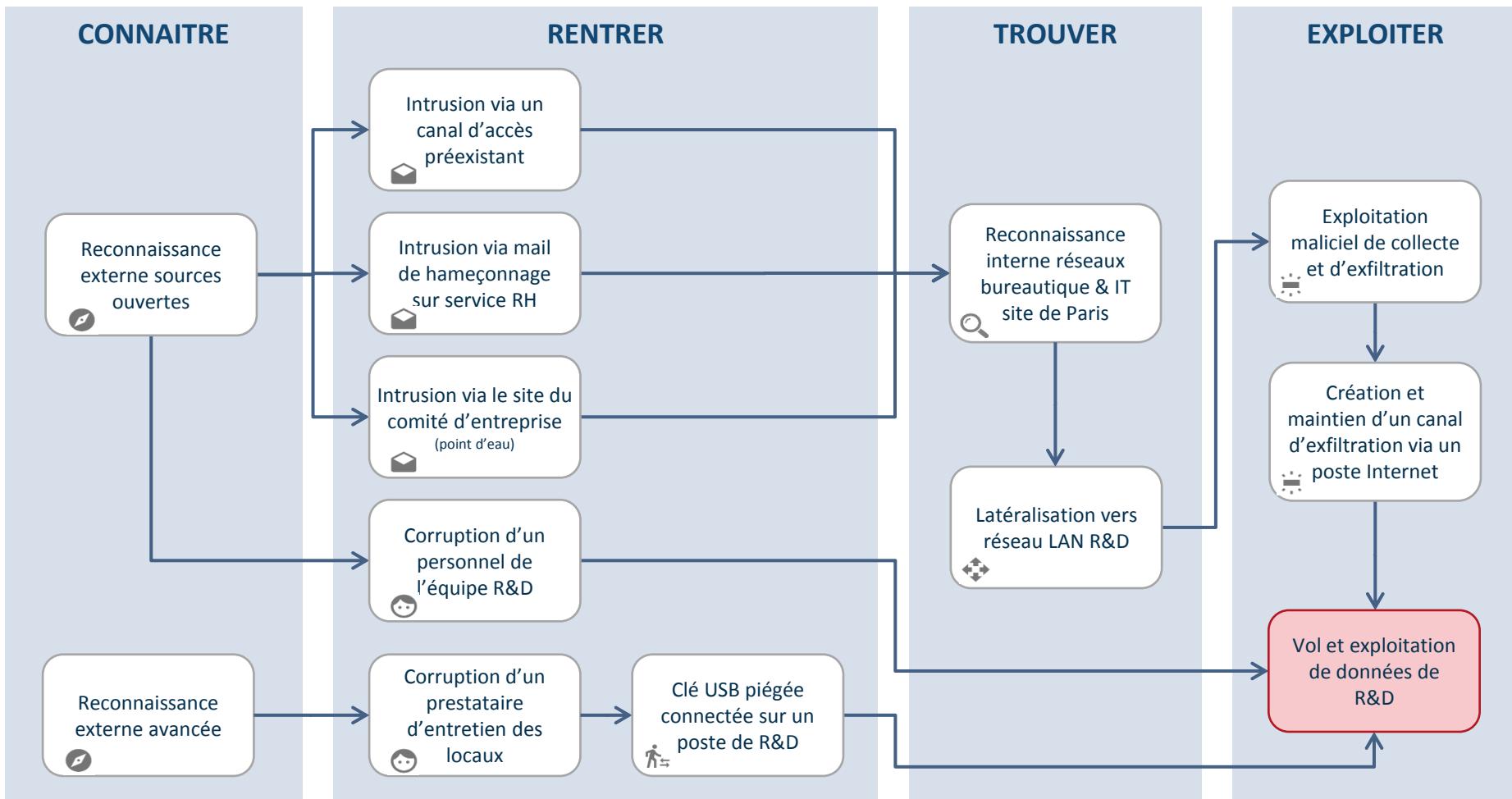
# Élaborer les scénarios opérationnels

A3

Scénario stratégique : Un concurrent vole des informations de R&D

Chemin d'attaque : n°1 – attaque directe

Gravité : 3



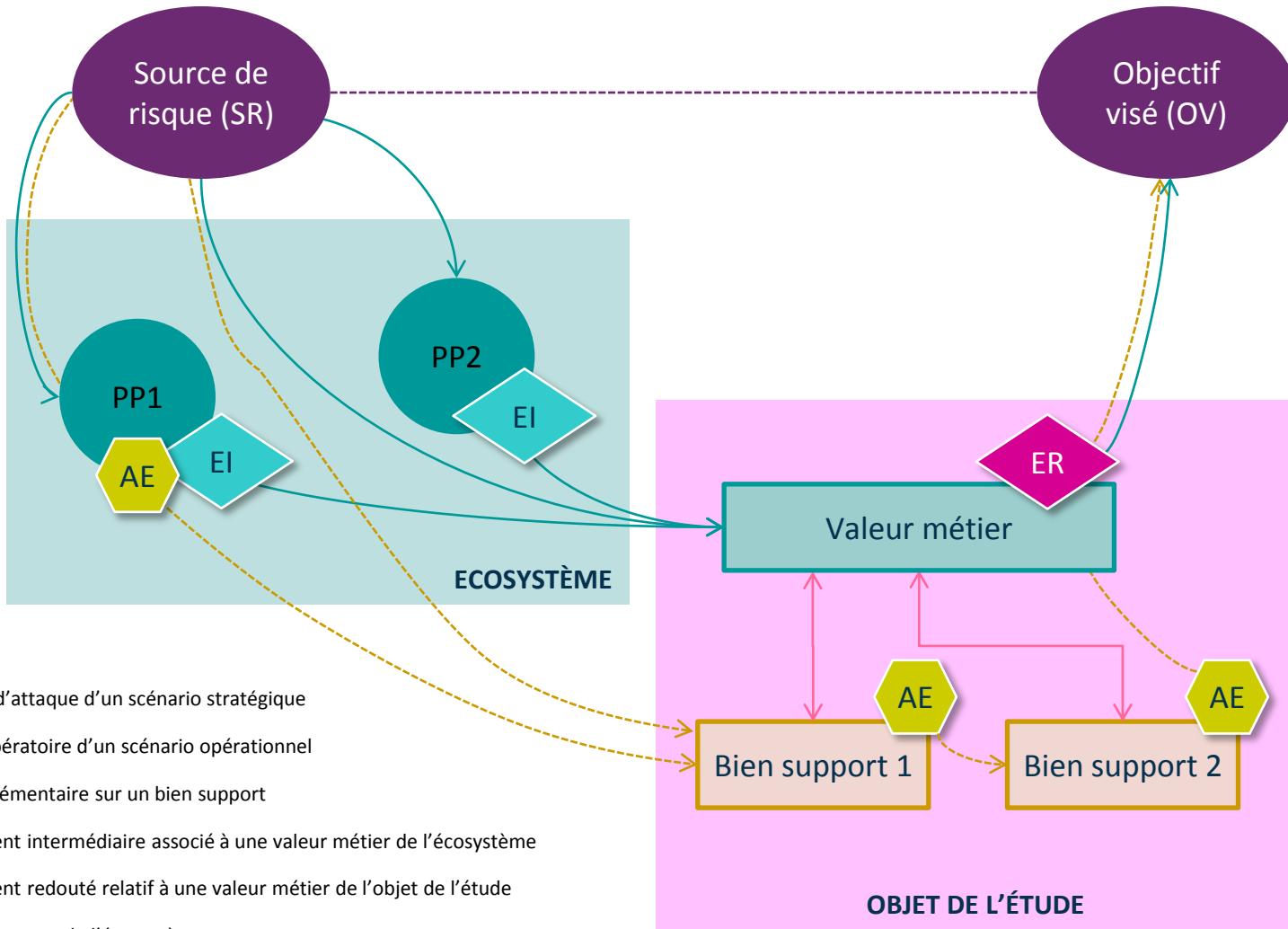
# Définir une échelle de vraisemblance

ÉCHELLE	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



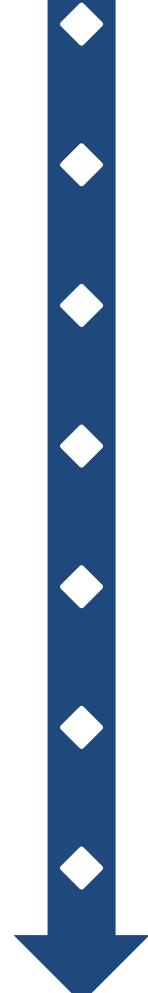
Il est recommandé de reprendre une échelle de vraisemblance déjà définie dans l'organisation ou lors de l'étude des risques précédente

# Comment constituer les scénarios de risques ? (fin de l'atelier 4)



# Programme

- ◆ EBIOS Risk Manager : les bases
- ◆ 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**
- ◆ Étude de cas



## Atelier 5 : traitement du risque



**OBJECTIF :** Définir une stratégie de traitement du risque et identifier les risques résiduels

### ÉLÉMENTS EN ENTRÉE :

- Socle de sécurité (**atelier 1**)
- Mesures de sécurité portant sur l'écosystème (**atelier 3**)
- Scénarios stratégiques (**atelier 3**)
- Scénarios opérationnels (**atelier 4**)



### ÉLÉMENS EN SORTIE :

- Stratégie de traitement du risque
- Plan d'amélioration continue de la sécurité (PACS)
- Synthèse des risques résiduels
- Cadre du suivi des risques



**PARTICIPANTS :** Direction, Métiers, RSSI, DSi

## Rappel : articulation des ateliers

ATELIER 2

Couple Source de Risque / Objectif visé  
(SR/OV)

ATELIER 3

Scénario stratégique

Chemin d'attaque (1)

Chemin d'attaque (n)

GRAVITÉ DES IMPACTS

*(identique pour le scénario stratégique et tous ses chemins d'attaque)*

ATELIER 4

Scénario opérationnel  
(1)

Scénario opérationnel  
(n)

VRAISEMBLANCE DU SCÉNARIO  
*(propre à chaque scénario opérationnel)*

ATELIER 5

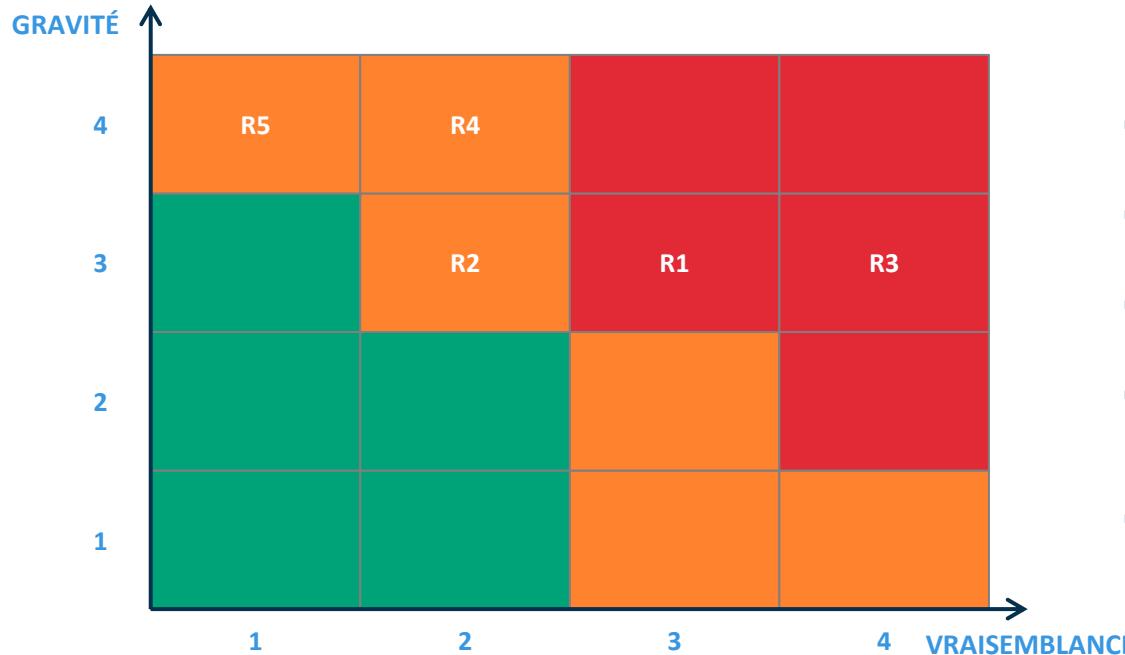
Scénario de risque (1)

Scénario de risque (n)

NIVEAU DE RISQUE

*(propre à chaque scénario de risque, évalué sur la base de sa gravité et de sa vraisemblance)*

# Décider de la stratégie de traitement du risque



## *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 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

→ La représentation de la stratégie de traitement doit permettre de comparer les risques les uns par rapport aux autres et être compréhensible par l'ensemble des participants

# Décider de la stratégie de traitement du risque

## OPTIONS DE TRAITEMENT DU RISQUE (ISO 27005 : 2018)

### RÉDUCTION DU RISQUE



La ceinture de sécurité est une réduction de risque : elle n'empêche pas l'accident, mais amoindrit généralement son effet

### MAINTIEN DU RISQUE



Rouler sans casque revient à accepter un risque de traumatisme crânien jugé faible par le conducteur par rapport à l'inconfort qu'il apporte

### REFUS DU RISQUE



Par conception, les plaques d'égout sont rondes, de manière à ce que la plaque ne puisse pas tomber à travers son propre trou

### PARTAGE DU RISQUE



Le producteur transfère généralement le risque d'accident sur un cascadeur professionnel

# Définir les mesures de sécurité dans un plan d'amélioration continue de la sécurité (PACS)

Mesure de sécurité	Scénarios de risques associés	Responsable	Freins et difficultés de mise en œuvre	...	Coût / Complexité	Échéance	Statut
<b>GOUVERNANCE</b>							
Sensibilisation renforcée au hameçonnage par un prestataire spécialisé	R1	RSSI	Validation de la hiérarchie obligatoire		+	Juin 2019	En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI	R1, R5	RSSI			++	Mars 2019	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 2020	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 2019	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 2019	A lancer
Limitation des données transmises au laboratoire au juste besoin	R2	Équipe R&D			+	Mars 2019	Terminé
<b>PROTECTION</b>							
Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonnement)	R1, R3	DSI			+++	Septembre 2019	En cours
Renforcement du contrôle d'accès physique au bureau R&D	R1	Équipe sûreté			++	Mars 2019	Terminé
Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site	R4	DSI			++	Septembre 2019	A lancer

## Gérer les risques résiduels

Cartographie du risque initial (avant traitement)



Cartographie du risque résiduel (après application du PACS)



→ Au terme de l'analyse, les risques résiduels sont acceptés formellement par la direction

# Mettre en place le cadre de suivi des risques



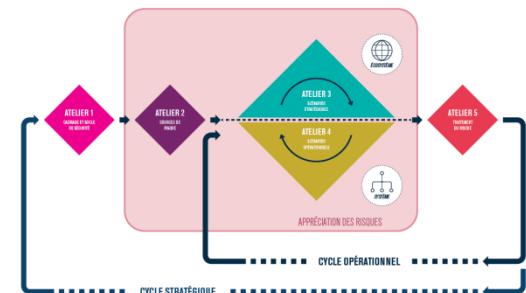
Mettre en place un comité de pilotage pour assurer le suivi des risques

MEURE DE SÉCURITÉ	SCÉNARIOS DE RISQUES ASSOCIÉS	RESPONSABLE	FREINS ET DIFFICULTÉS DE MISE EN ŒUVRE	COÛT / COMPLEXITÉ	ECHÉANCE	STATUT
<b>GOUVERNANCE</b>						
Sensibilisation renforcée au hanse-coupage par un prestataire spécialisé	R1	RSSI	Validation du CHSCT indispensable	+	6 mois	En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI	R1, R5	RSSI		++	3 mois	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	++	18 mois	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		++	6 mois	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	++	6 mois	A lancer
Limitation des données transmises aux laboratoires au juste besoin	R2	Équipe R&D		+	3 mois	Terminé
<b>PROTECTION</b>						
Protection renforcée des données de R&D sur le SI (piste : chiffrement, cloisonnement)	R1, R3	DSI		+++	9 mois	En cours
Renforcement du contrôle d'accès physique au bureau R&D	R1	Équipe sûreté		++	3 mois	Terminé
Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site	R4	DSI		++	9 mois	A lancer



## Suivi de l'avancement du PACS

Suivi des indicateurs de maintien en condition de sécurité



Suivi des mises à jour de l'étude des risques selon les cycles stratégique et opérationnel



# Vous vous souvenez des articles évoqués ce matin ?

ACCUEIL &gt; HIGH-TECH

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

CYBERSECURITE C'est le second plus gros vol de données après celui dont avait été victime Yahoo en 2013...

Source : 20 minutes – 30/11/2018

« 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 chaîne n'exclut pas que les éléments nécessaires au déchiffrement des données aient été compromis. »

Source de risque	
Objectif visé	
Évènement redouté	
Valeur métier	
Bien support	
Impacts	



# Vous vous souvenez des articles évoqués ce matin ?

ACCUEIL > HIGH-TECH

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

CYBERSECURITE C'est le second plus gros vol de données après celui dont avait été victime Yahoo en 2013...

Source : 20 minutes – 30/11/2018

« 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 chaîne n'exclut pas que les éléments nécessaires au déchiffrement des données aient été compromis. »

Source de risque	?
Objectif visé	Lucratif ?
Évènement redouté	Vol des informations des clients du groupe hôtelier
Valeur métier	Informations des clients du groupe
Bien support	Base de données de sa filiale Starwood
Impacts	Image, juridique (RGPD)



# Vous vous souvenez des articles évoqués ce matin ?

## 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 impact – 12/11/2018

Source de risque	
Objectif visé	
Évènement redouté	
Valeur métier	
Bien support	
Impacts	



# Vous vous souvenez des articles évoqués ce matin ?

## 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 impact – 12/11/2018

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

# Programme

- ◆ EBIOS Risk Manager : les bases
- ◆ 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
- ◆ **Étude de cas**



## Présentation de l'étude de cas



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.



## Définir le périmètre métier et technique

MISSION	RENOUVELER DES TITRES D'IDENTITÉ NUMÉRIQUE						
NOM DE LA VALEUR MÉTIER							
NATURE DE LA VALEUR MÉTIER							
ENTITÉ RESPONSABLE							
NOM DU/DES BIENS SUPPORTS ASSOCIÉS							
ENTITÉ OU PERSONNE RESPONSABLE							



# Définir le périmètre métier et technique

MISSION		RENOUVELER DES TITRES D'IDENTITÉ NUMÉRIQUE								
NOM DE LA VALEUR MÉTIER	Gestion des pré-demandes	Gestion des demandes de renouvellement de TIN		Impression des TIN		Distribution des TIN		Informations des citoyens et TIN		
NATURE DE LA VALEUR MÉTIER	Processus	Processus		Processus		Processus		Processus		
ENTITÉ RESPONSABLE	SGTIN (responsable de la valeur métier même si elle peut déléguer l'exécution des processus à un prestataire)									
NOM DU/DES BIENS SUPPORTS ASSOCIÉS	SI de pré-demande	Locaux	SI de renouvellement de TIN	Locaux	SI d'impression des TIN	Locaux	Courrier	SI de la mairie	SI d'impression des TIN	
ENTITÉ OU PERSONNE RESPONSABLE	SGTIN	SGTIN et Mairie	SGTIN	Mairie et Hébergeur	SGTIN	SGTIN	Société d'acheminement des TIN	Mairie	SGTIN	



## Identifier les événements redoutés

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIES D'IMPACT	GRAVITÉ	COMMENTAIRES / JUSTIFICATION
Informations des citoyens	Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.)	<ul style="list-style-type: none"> <li>Impact juridique (RGPD)</li> <li>Impact d'image</li> </ul>	4	<ul style="list-style-type: none"> <li>• Usurpation d'identité</li> </ul>

# Échelle de gravité validée pour le projet

ÉCHELLE	DÉFINITION
G4 – CRITIQUE	Les impacts découlant de la réalisation de l'événement redouté peuvent conduire à la création d'identités erronées ou à l'usurpation d'identité
G3 – GRAVE	Les impacts découlant de la réalisation de l'événement redouté ne permettent pas à l'organisation de réaliser tout ou partie de son activité
G2 – SIGNIFICATIVE	Les impacts découlant de la réalisation de l'événement redouté sont significatifs sur les performances de l'activité (dégradation des performances)
G1 – MINEURE	Les impacts découlant de la réalisation de l'événement redouté sont négligeables (des solutions de contournement existent et sont efficaces)

## Catégories d'impact (1/2)

Catégorie d'impact	Exemples (listes non exhaustives)
<b>Impacts sur les missions et services de l'organisme</b>	
Conséquences directes ou indirectes sur la réalisation des missions et services.	Incapacité à fournir un service, dégradation de performances opérationnelles, retards, impacts sur la production ou la distribution de biens ou de services, impossibilité de mettre en œuvre un processus clé.
<b>Impacts sur la gouvernance de l'organisme</b>	
<u>Impacts sur la capacité de développement ou de décision</u>  Conséquences directes ou indirectes sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement.	Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisme, changement contraint de stratégie, perte de fournisseurs ou de sous-traitants clés.
<u>Impacts sur le lien social interne</u>  Conséquences directes ou indirectes sur la qualité des liens sociaux au sein de l'organisation.	Perte de confiance des employés dans la pérennité de l'organisme, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, affaiblissement/perte de sens des valeurs communes.
<u>Impacts sur le patrimoine intellectuel ou culturel</u>  Conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisme, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes.	Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés.

## Catégories d'impact (2/2)

Catégorie d'impact	Exemples (listes non exhaustives)
<b>Impacts humains, matériels ou environnementaux</b>	
<u>Impacts sur la sécurité ou sur la santé des personnes</u> Conséquences directes ou indirectes sur l'intégrité physique de personnes.	Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire.
<u>Impacts matériels</u> Dégâts matériels ou destruction de biens supports.	Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématuée de matériels.
<u>Impacts sur l'environnement</u> Conséquences écologiques à court ou long terme, directes ou indirectes.	
<u>Impacts financiers</u> Conséquences pécuniaires, directes ou indirectes.	Perte de chiffre d'affaire, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées.
<u>Impacts juridiques</u> Conséquences suite à une non-conformité légale, réglementaire, normative ou contractuelle.	
<u>Impacts sur l'image et la confiance</u> Conséquences directes ou indirectes sur l'image de l'organisation, la notoriété, la confiance des clients.	
	Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte d'avance concurrentielle, perte de notoriété, perte de confiance d'usagers.



# Identifier les événements redoutés

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIES D'IMPACT	GRAVITÉ	COMMENTAIRES / JUSTIFICATION
<b>Impression des TIN</b>	Certains TIN imprimés ne correspondent pas à des demandes légitimes	<ul style="list-style-type: none"> <li>Impact financier lié au coût de réimpression du TIN</li> <li>Impact juridique lié à l'implication de la SGTIN dans les procès pour création de fausses identités</li> </ul>	4	<ul style="list-style-type: none"> <li>Usurpation d'identité</li> <li>Fraude (création de faux TIN)</li> </ul>
<b>Distribution des TIN / TIN</b>	Vol de TIN légitimes durant leur acheminement à la mairie	<ul style="list-style-type: none"> <li>Impact juridique (RGPD)</li> <li>Impact financier lié au coût de renouvellement de TIN</li> </ul>	4	<ul style="list-style-type: none"> <li>Usurpation d'identité</li> </ul>
<b>Informations des citoyens</b>	Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.)	<ul style="list-style-type: none"> <li>Impact juridique (RGPD)</li> <li>Impact d'image</li> </ul>	4	<ul style="list-style-type: none"> <li>Usurpation d'identité</li> </ul>
<b>Gestion des demandes de renouvellement de TIN</b>	Le service permettant à un agent de mairie de faire une demande de renouvellement de TIN est indisponible	<ul style="list-style-type: none"> <li>Impact d'image</li> <li>Impact financier lié au coût d'investigation et de retour à la normale</li> </ul>	3	Pas d'existence de solution de contournement, impossibilité de réaliser la mission pendant la durée d'indisponibilité
<b>Gestion des demandes de renouvellement de TIN</b>	Le service de notification de renouvellement de TIN n'est pas accessible aux utilisateurs	<ul style="list-style-type: none"> <li>Impact d'image lié au délai d'obtention du TIN</li> <li>Impact financier lié au coût d'investigation et de retour à la normale</li> </ul>	2	Existence d'une solution de contournement avec une dégradation des performances (la mairie peut contacter par téléphone ou mail le citoyen pour le notifier)
<b>Gestion des pré-demandes</b>	Le service permettant de réaliser une pré-demande par internet auprès de la SGTIN est indisponible	<ul style="list-style-type: none"> <li>Impact d'image</li> <li>Impact financier lié au coût d'investigation et de retour à la normale</li> </ul>	1	Existence d'une solution de contournement (possibilité de renseigner les informations directement à la mairie)

# Méthode d'évaluation de la pertinence des couples SR/OV

		RESSOURCES			
		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



# Évaluer les couples SR/OV et sélectionner les plus pertinents

SOURCES DE RISQUE	OBJECTIF VISÉ	MOTIVATION	RESSOURCES	PERTINENCE
Agent malveillant SGTIN	Discréder ou saboter le service de renouvellement de TIN	Assez motivé	Ressources significatives	Plutôt pertinent



# Évaluer les couples SR/OV et sélectionner les plus pertinents

SOURCES DE RISQUE	OBJECTIF VISÉ	MOTIVATION	RESSOURCES	PERTINENCE
Organisation de malfaiteurs	Gagner de l'argent en collectant des informations ou en revendant des TIN	Fortement motivé	Ressources importantes	Très pertinent
Hacktiviste	Perturber la fabrication de TIN	Fortement motivé	Ressources importantes	Très pertinent
État	Faire fabriquer des faux TIN pour faire circuler des espions sur le territoire	Fortement motivé	Ressources illimitées	Très pertinent
Agent malveillant SGTIN	Discréder ou saboter le service de renouvellement de TIN	Assez motivé	Ressources significatives	Plutôt pertinent
Terroriste	Créer un faux TIN pour entrer sur le territoire	Assez motivé	Ressources limitées	Moyennement pertinent
Citoyen malhonnête	Créer une fausse identité	Très peu motivé	Ressources limitées	Peu pertinent
Hacker amateur	Tester ses compétences sur un système « grandeur nature »	Peu motivé	Ressources limitées	Peu pertinent



# Lien entre les ER (atelier 1) et les couples SR/OV retenus (atelier 2)

## SR/OV les plus pertinents

SOURCES DE RISQUE	OBJECTIF VISÉ
Organisation de malfaiteurs	Gagner de l'argent en collectant des informations ou en revendant des TIN
Hacktiviste	Perturber la fabrication des TIN
État	Faire fabriquer des faux TIN pour faire circuler des espions sur le territoire

## ER les plus graves

ÉVÉNEMENT REDOUTÉ	VALEUR MÉTIER
Certains TIN imprimés ne correspondent pas à des demandes légitimes	Impression des TIN
Vol de TIN légitimes durant leur acheminement à la mairie	Distribution des TIN
Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.)	Informations des citoyens



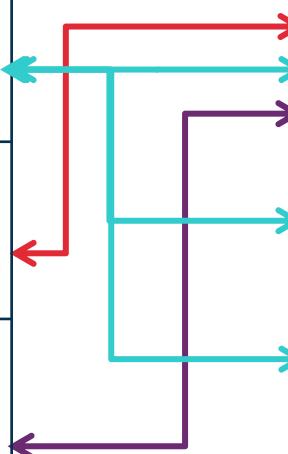
# Lien entre les ER (atelier 1) et les couples SR/OV retenus (atelier 2)

## SR/OV les plus pertinents

SOURCES DE RISQUE	OBJECTIF VISÉ
Organisation de malfaiteurs	Gagner de l'argent en collectant des informations ou en revendant des TIN
Hacktiviste	Perturber la fabrication des TIN
État	Faire fabriquer des faux TIN pour faire circuler des espions sur le territoire

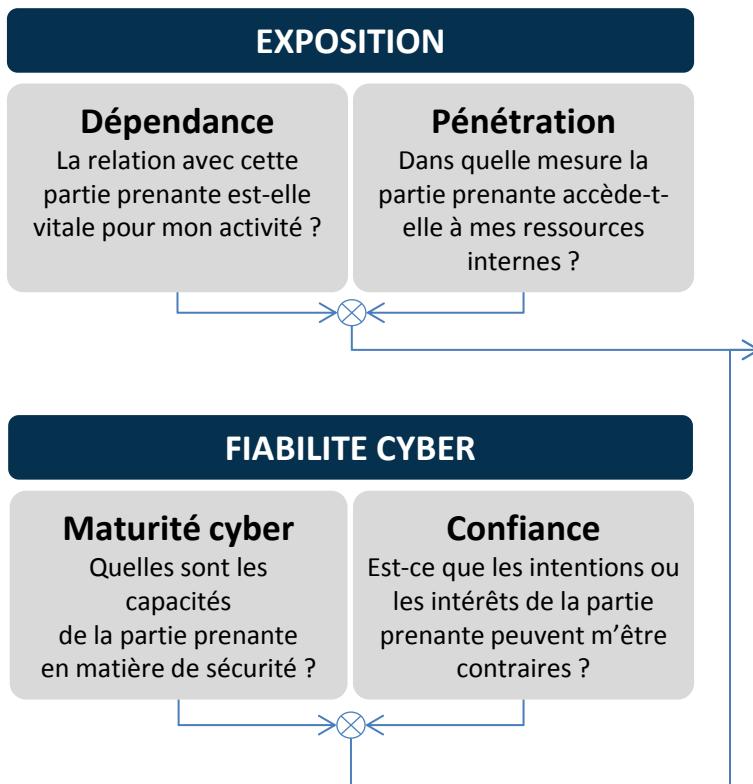
## ER les plus graves

ÉVÉNEMENT REDOUTÉ	VALEUR MÉTIER
Certains TIN imprimés ne correspondent pas à des demandes légitimes	Impression des TIN
Vol de TIN légitimes durant leur acheminement à la mairie	Distribution des TIN
Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.)	Informations des citoyens

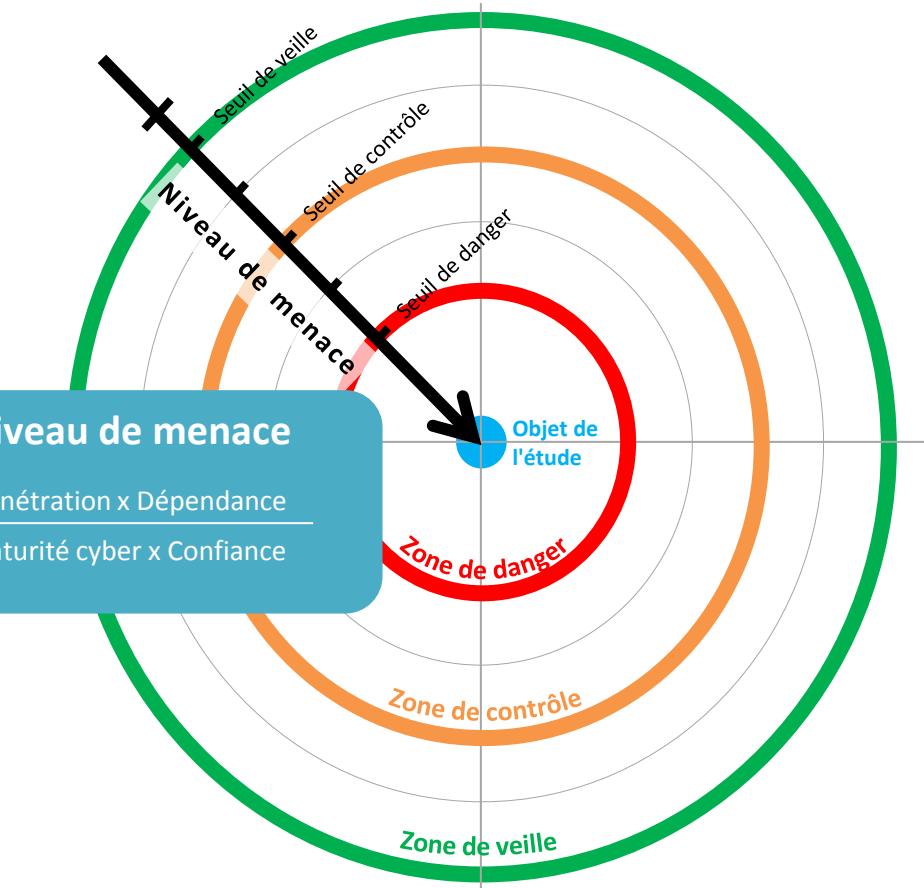


# Construire la cartographie de menace numérique de l'écosystème

Pour chaque partie prenante, évaluer 4 critères :



**Niveau de menace**  
 $\frac{\text{Pénétration} \times \text{Dépendance}}{\text{Maturité cyber} \times \text{Confiance}}$



# Critères de cotation de la menace proposés

	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFiance
1	Pas de lien avec le SI de la partie prenante pour réaliser la mission	Pas d'accès au système d'information de la SGTIN ni aux TIN.	<ul style="list-style-type: none"> <li>Pas d'information sur le niveau de maturité</li> <li><b>OU</b> des règles d'hygiène sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.</li> </ul>	Les intentions de la partie prenante ne sont pas connues.
2	Lien avec le SI de la partie prenante utile à la réalisation de la mission	Accès à des postes de travail de la SGTIN en mode utilisateur ou accès physique aux bureaux de la SGTIN	<p>Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale.</p> <p>La sécurité numérique est assurée selon un mode réactif.</p>	Les intentions de la partie prenante sont considérées comme neutres.
3	Lien avec le SI de la partie prenante indispensable mais non exclusif (possible substitution)	<ul style="list-style-type: none"> <li>Accès avec priviléges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.)</li> <li><b>OU</b> accès aux TIN</li> <li><b>OU</b> accès étendu au SI ponctuellement à des fins d'audit et de contrôle</li> </ul>	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	Lien avec le SI de la partie prenante indispensable et unique (pas de substitution possible)	<ul style="list-style-type: none"> <li>Accès avec priviléges de type administrateur à des équipements d'infrastructure (annuaires d'entreprise, DNS, baies de stockage, etc.)</li> <li><b>OU</b> accès physique aux salles serveurs où sont stockées les informations des citoyens</li> </ul>	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.

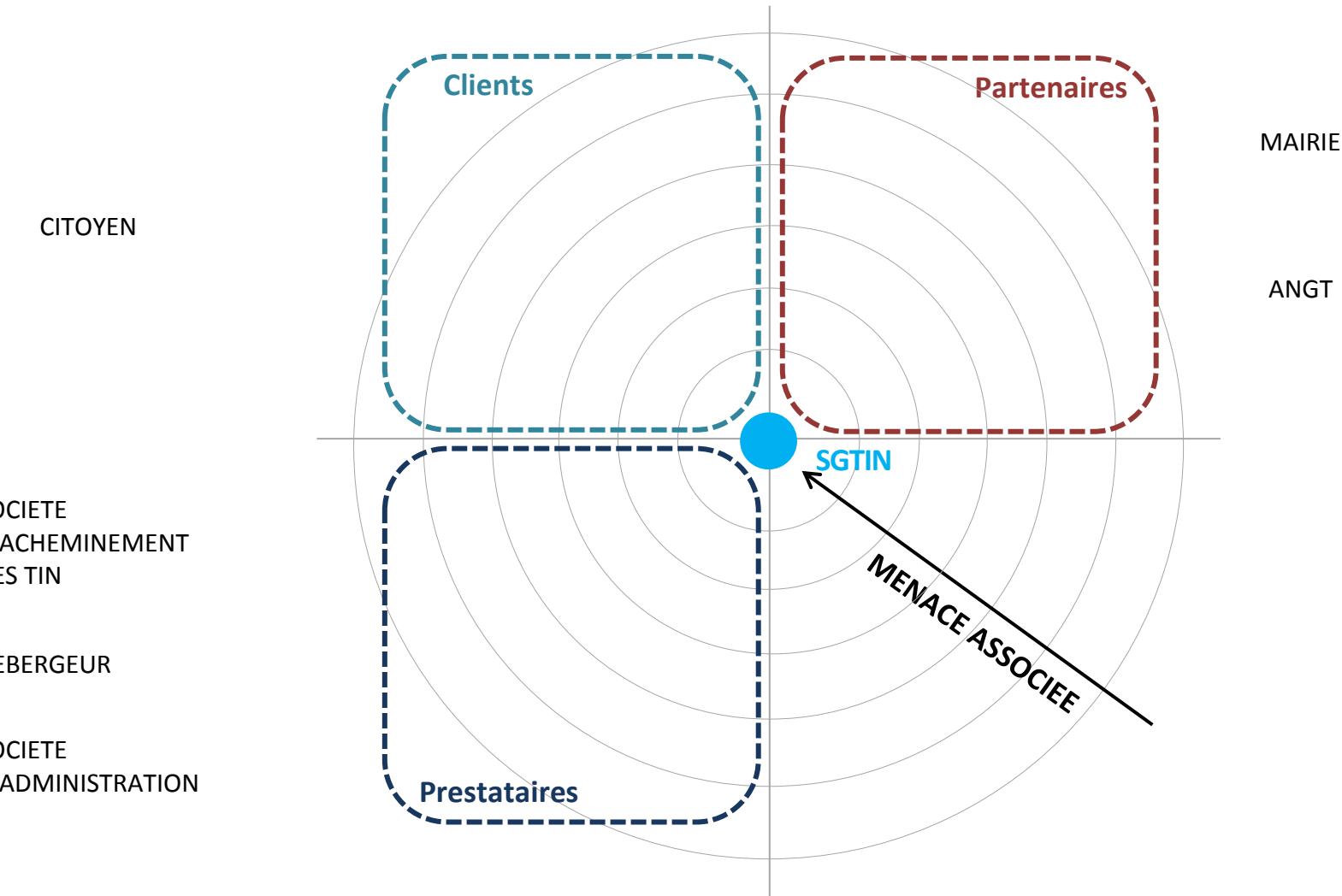


# Evaluer le niveau de menace associé aux parties prenantes de l'écosystème

CATÉGORIE	NOM	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFiance	NIVEAU DE MENACE
Utilisateur	Citoyen					
Partenaire	Mairie					
Partenaire	Autorité Nationale de Gestion des Titres (ANGT)					
Prestataire	Société d'administration					
Prestataire	Hébergeur (Héberweb)					
Prestataire	Société d'acheminement des TIN					



# Construire la cartographie de menace numérique de l'écosystème





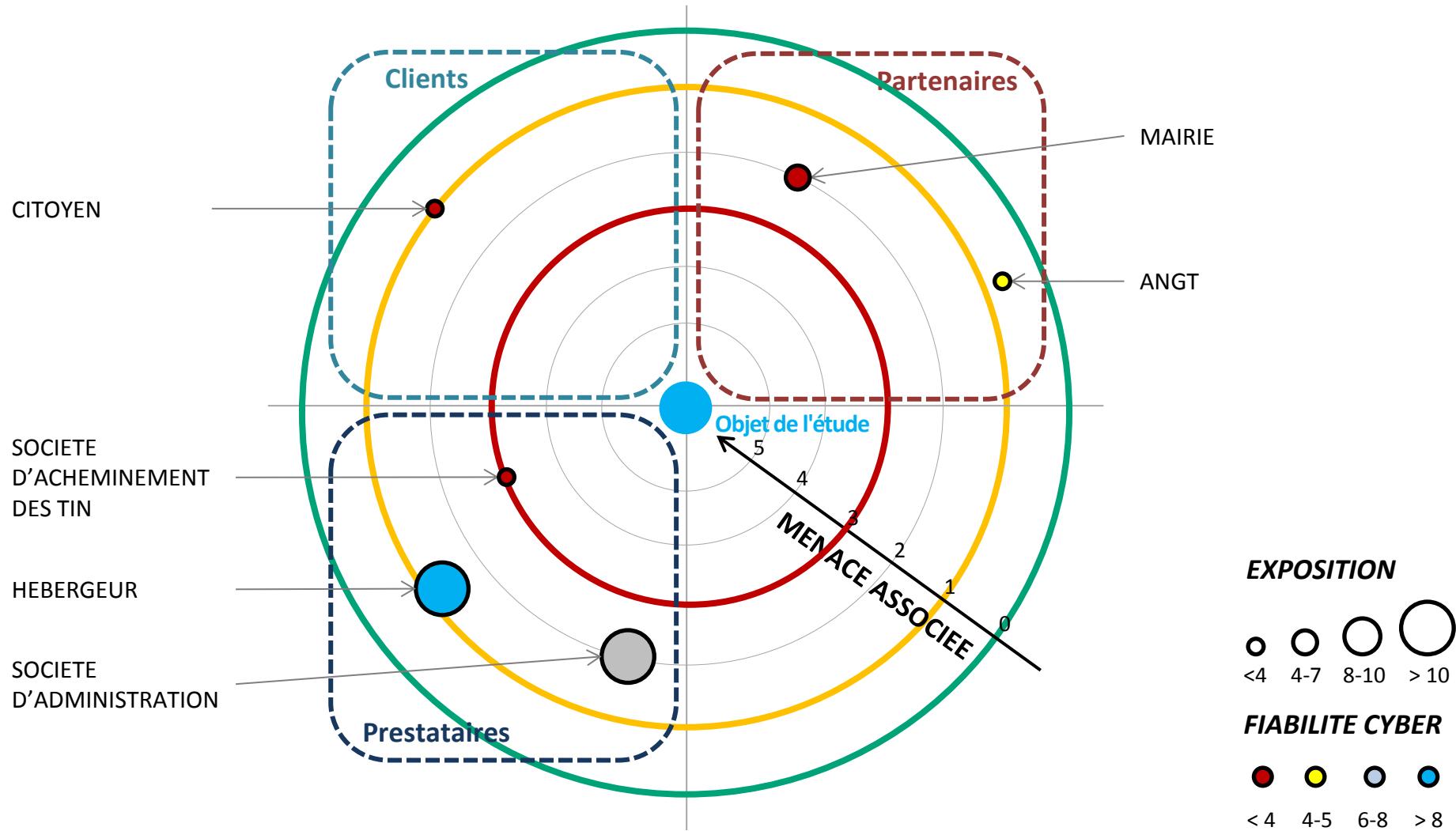
## Evaluer le niveau de menace associé aux parties prenantes de l'écosystème

CATÉGORIE	NOM	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFiance	NIVEAU DE MENACE
Utilisateur	Citoyen	1	1	1	1	1
Partenaire	Mairie	2	3	1	3	2
Partenaire	Autorité Nationale de Gestion des Titres (ANGT)	1	3	1	4	0,75
Prestataire	Société d'administration	3	4	2	3	2
Prestataire	Hébergeur (Héberweb)	3	4	3	3	1,3
Prestataire	Société d'acheminement des TIN	1	3	1	1	3





# Construire la cartographie de menace numérique de l'écosystème





# Élaborer des scénarios stratégiques

A2

Source de risque :

Objectif visé :

SOURCE DE RISQUE

ÉCOSYSTÈME

SGTIN

Gravité :

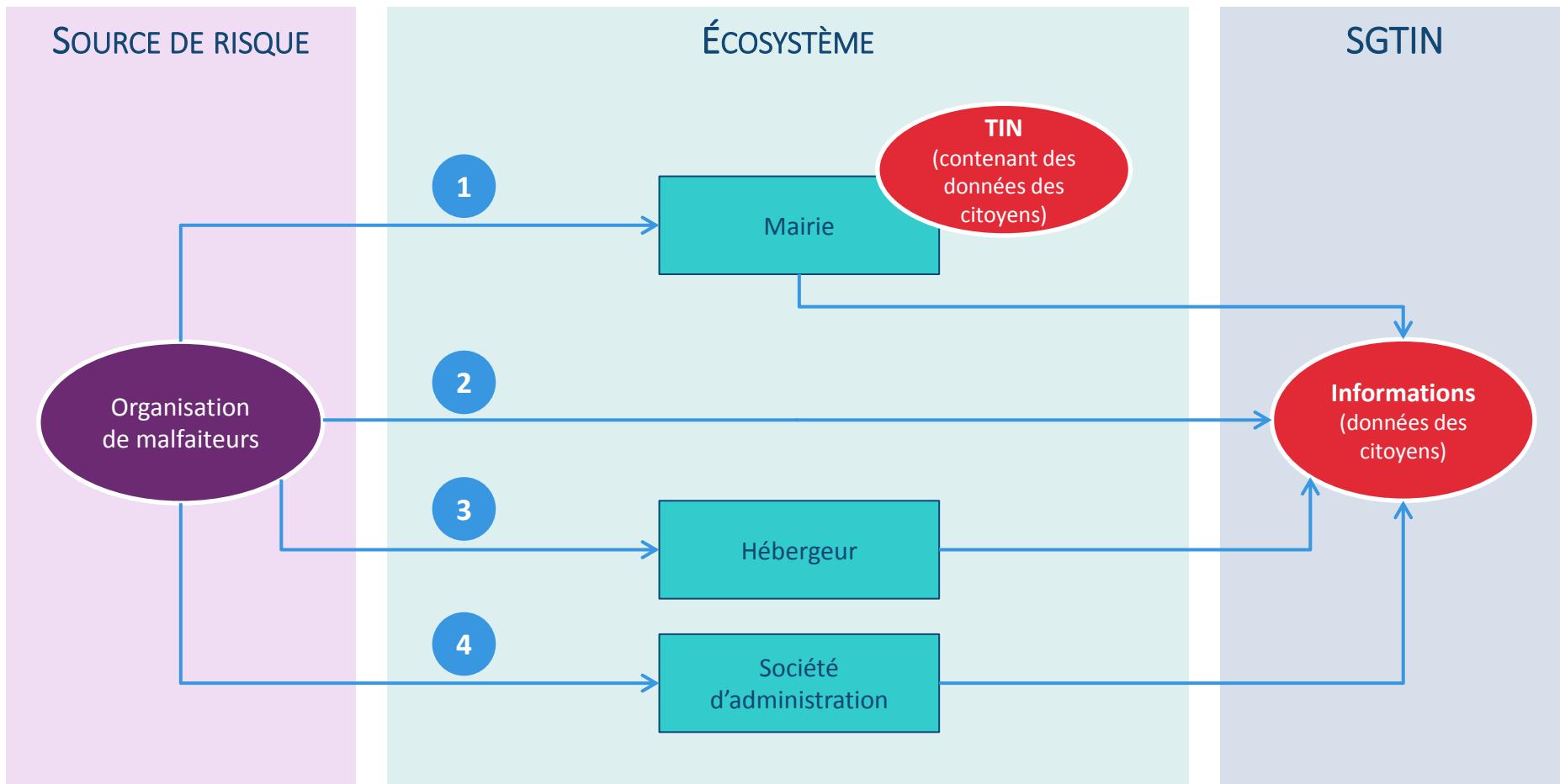


# Élaborer des scénarios stratégiques

A2

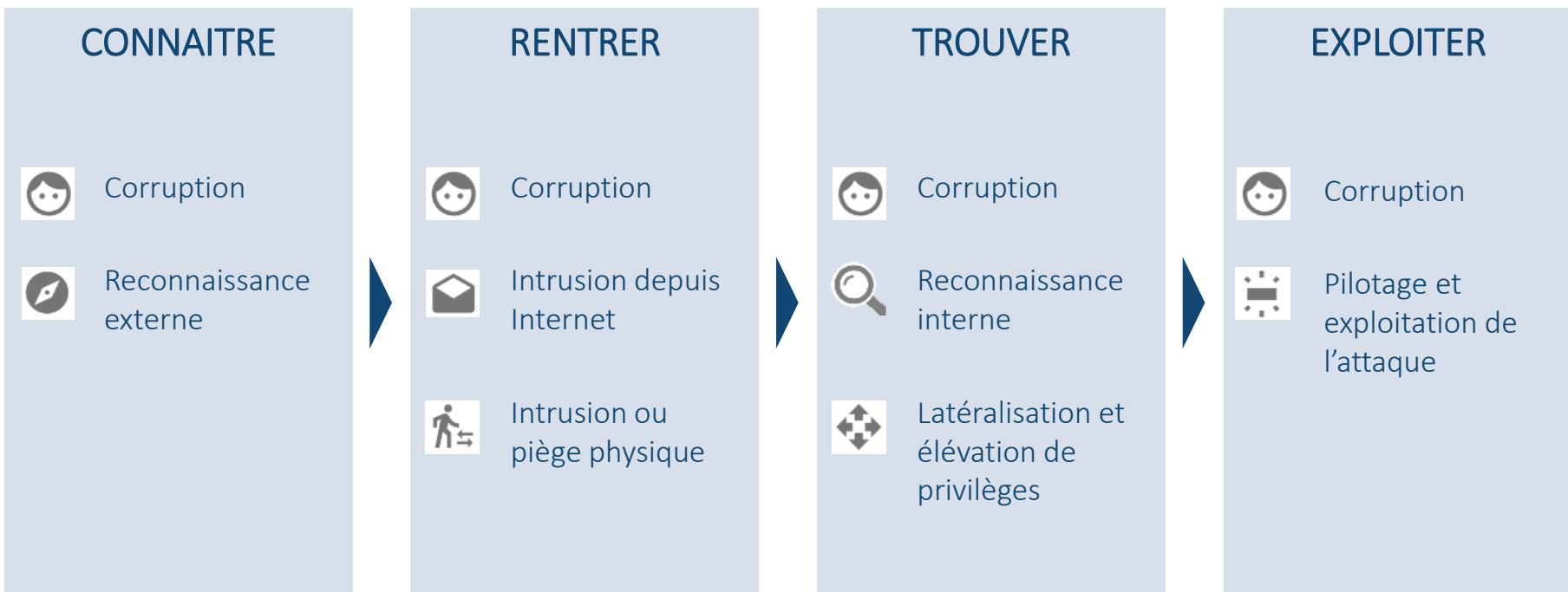
**Source de risque :** Organisation de malfaiteurs

**Objectif visé :** Collecter des données à caractère personnel



**Gravité : 4**

# Des scénarios structurés selon une séquence d'attaque type





# Élaborer les scénarios opérationnels

A3

Scénario stratégique :

Chemin d'attaque :

Gravité :

CONNAITRE

RENTRER

TROUVER

EXPLOITER



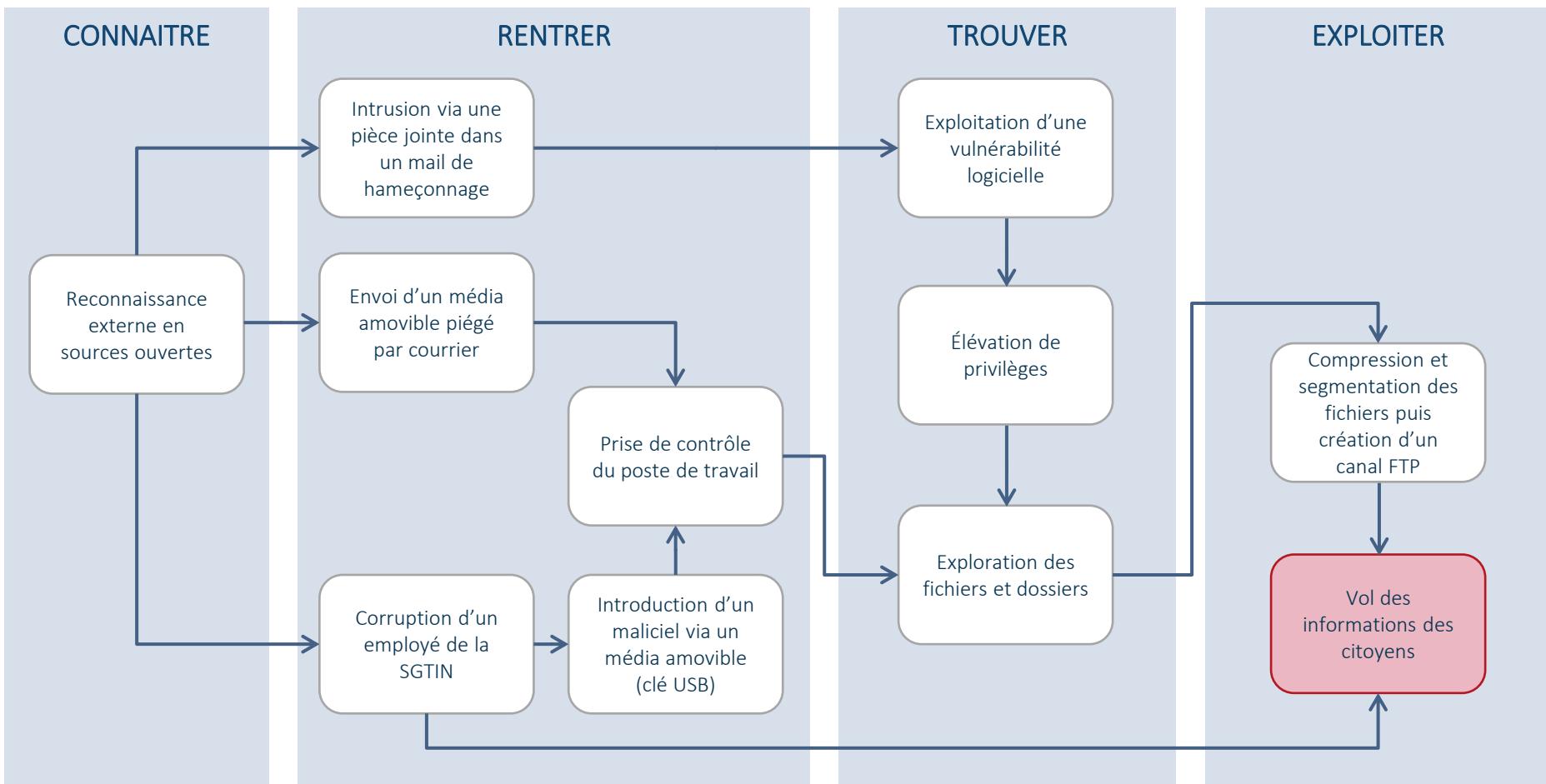
# Élaborer les scénarios opérationnels

A3

**Scénario stratégique :** Organisation de malfaiteurs qui veut voler des données personnelles

**Chemin d'attaque : n°2 – « attaque directe »**

**Gravité : 4**

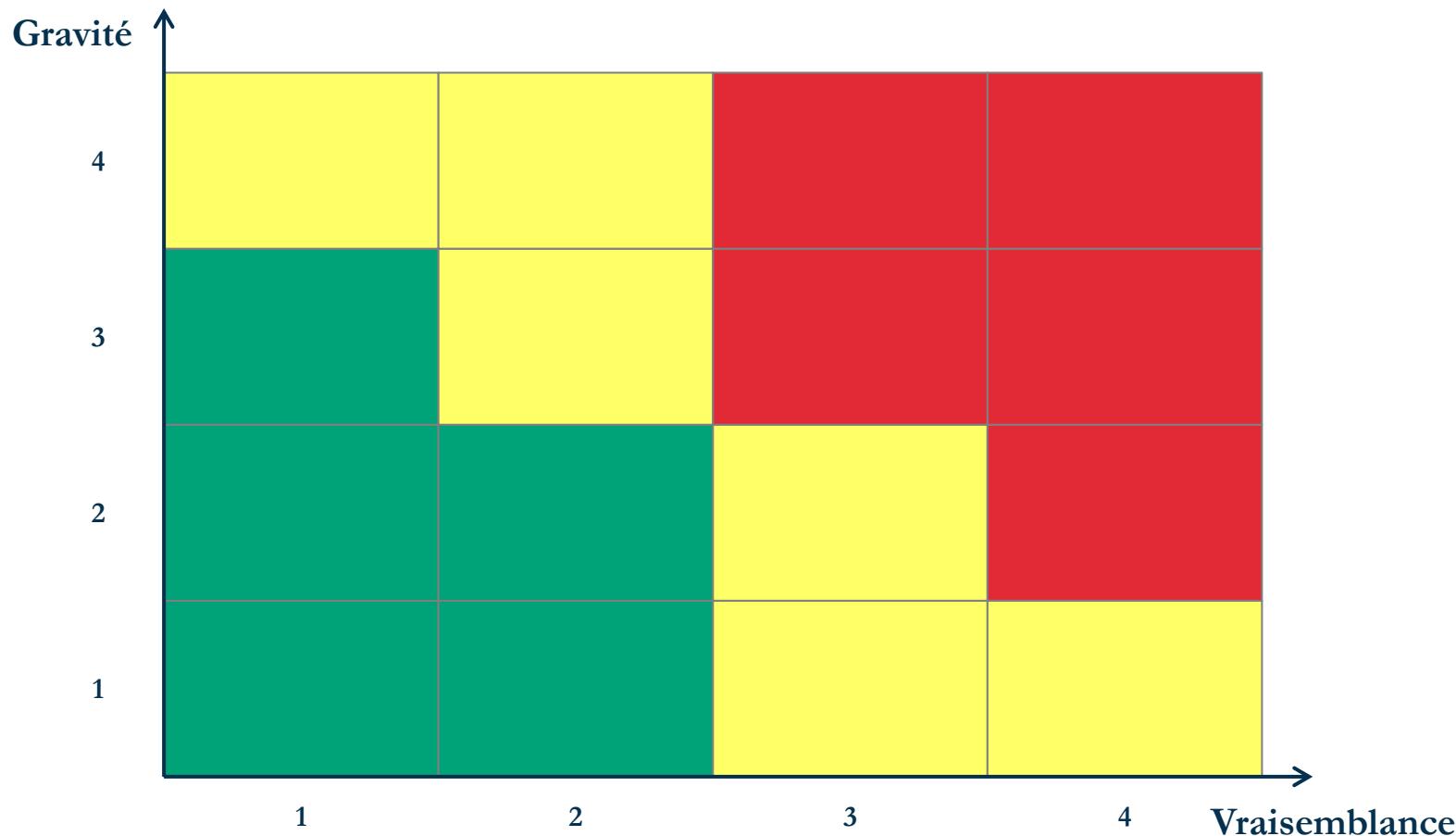


# Échelle de vraisemblance validée pour le projet

ÉCHELLE	DÉFINITION
V4 – QUASI CERTAIN	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée
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



## Réaliser une synthèse des scénarios de risque





# Définir les mesures de sécurité dans un plan d'amélioration continue de la sécurité (PACS)

MESURE DE SÉCURITÉ	SCÉNARIOS DE RISQUES ASSOCIÉS	RESPONSABLE	FREINS ET DIFFICULTÉ DE MISE EN ŒUVRE	COÛT / COMPLEXITÉ	ÉCHÉANCE	STATUT