



FORMATION

EBIOS

Risk Manager

V.2.04 • Mai 2024

Avant de commencer...



Présentations

- Qui êtes vous ?
- Qu'attendez vous de la formation ?



Objectif pédagogique

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



Horaires

- 9h15 – 12h00
- 13h45 – 17h00
(2 pauses)



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

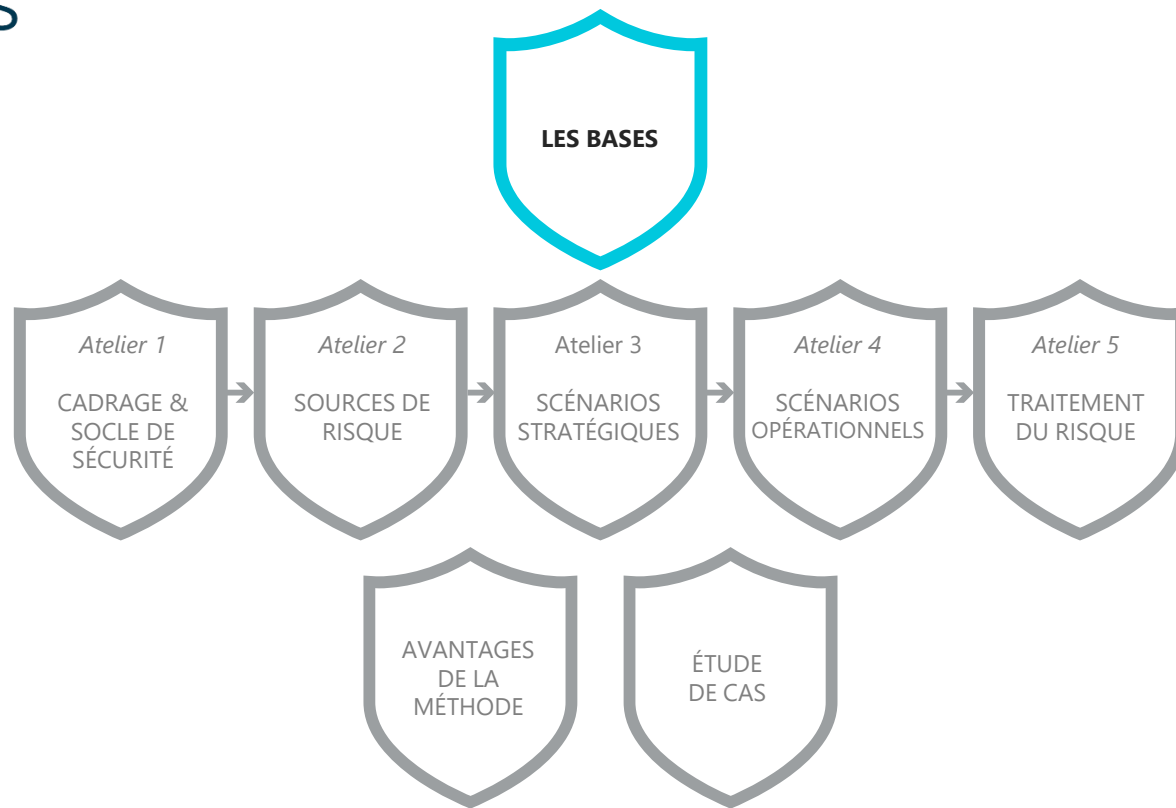


Sommaire





Les bases



Discussion de groupe

Quelle est votre définition
du risque ?



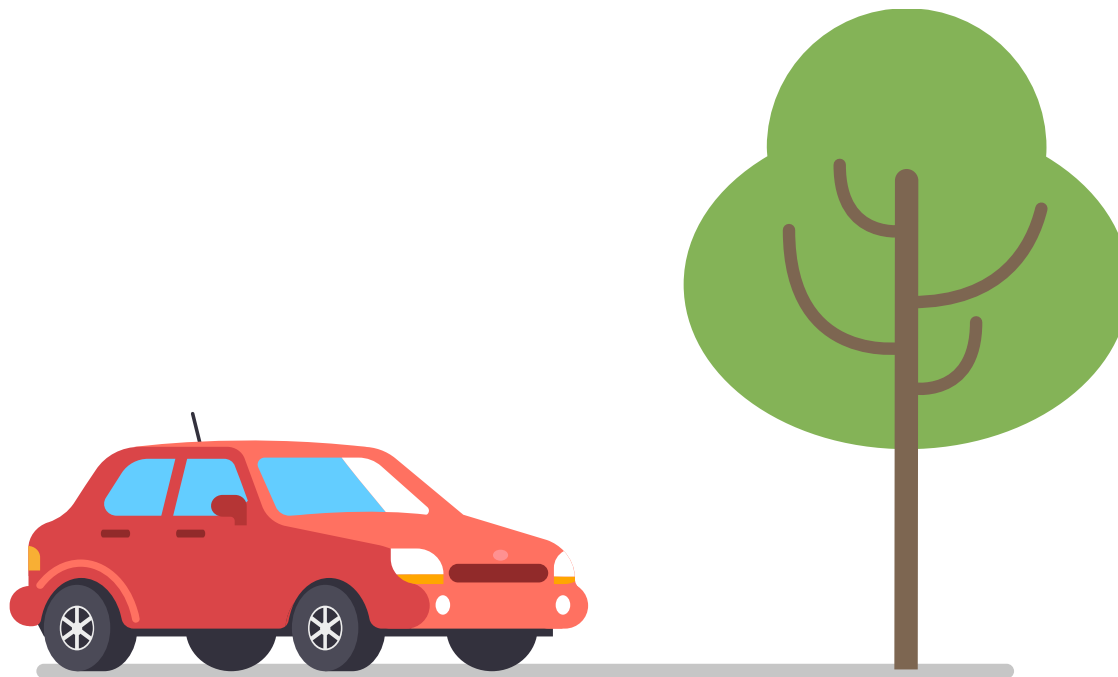
Les fondamentaux de la gestion des risques

Qu'est-ce qu'un risque ?

- **Risque (LAROUSSE)** : Danger, inconvénient plus ou moins probable auquel on est exposé.
- **Risque (ISO 31000:2010)** : Effet de l'incertitude sur l'atteinte des objectifs. Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement et de sa vraisemblance.
- **Risque (EBIOS Risk Manager)** : Possibilité qu'un événement redouté survienne et que ses effets perturbent les missions de l'objet de l'étude.



Qu'est-ce qu'un risque : exemple de la voiture



Qu'est-ce qu'un risque : exemple de la voiture

Risque

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

Événement redouté :
la voiture percute un arbre

Objet de l'étude :

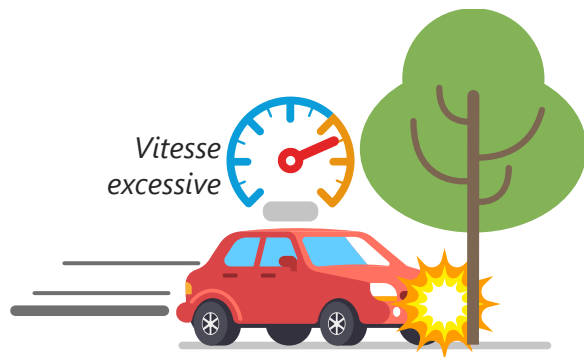
la voiture

Mission :

arriver à destination



Quelle est la gravité de ce risque ?



La gravité varie selon la vitesse de la voiture



La gravité varie selon la taille de l'arbre

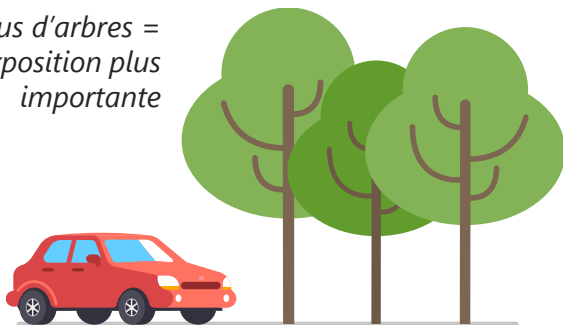


La gravité varie selon la valeur de la voiture (prix, robustesse...)

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

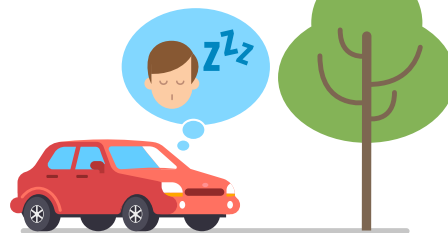
Quelle est la vraisemblance de ce risque ?

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**

Risque

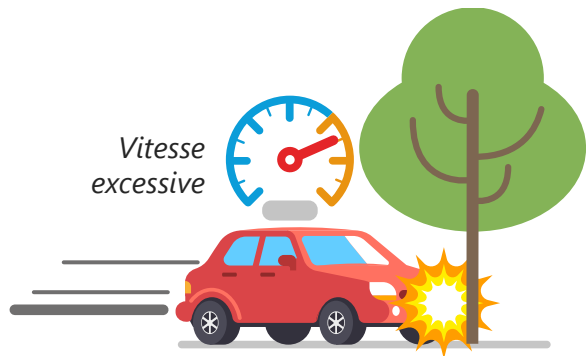
Possibilité qu'un événement redouté survienne et que ses effets perturbent les missions de l'objet de l'étude.

Événement redouté : le système embarqué se fait pirater et la voiture percute un arbre

Objet de l'étude :
la voiture

Mission :
arriver à destination





La gravité varie selon la vitesse de la voiture



La gravité varie selon la taille de l'arbre



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

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

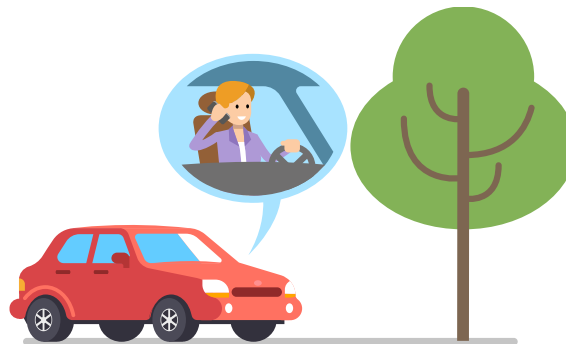


Menace : le hacker
Plus d'attaquants = plus de possibilités de se faire hacker



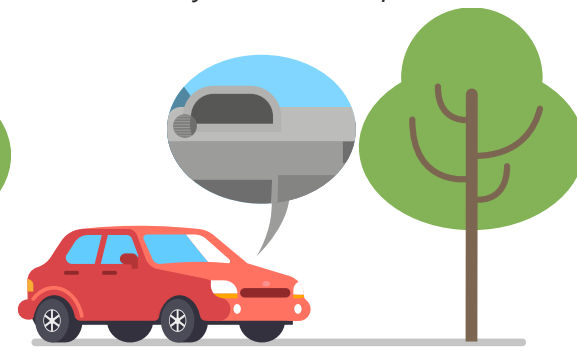
La vraisemblance varie selon le nombre d'attaquants

Vulnérabilité du conducteur



La vraisemblance varie selon le niveau d'attention du conducteur

Vulnérabilité du système embarqué



La vraisemblance varie selon le nombre de failles de sécurité dans le système embarqué

**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.

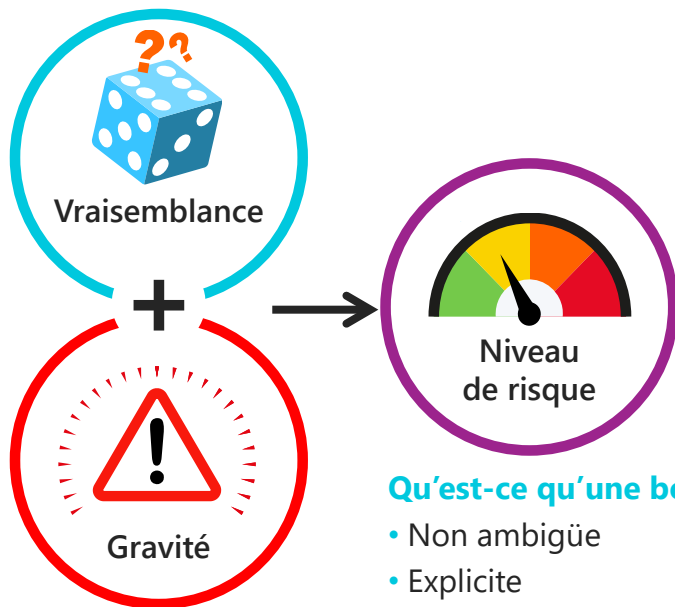
Vraisemblance

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



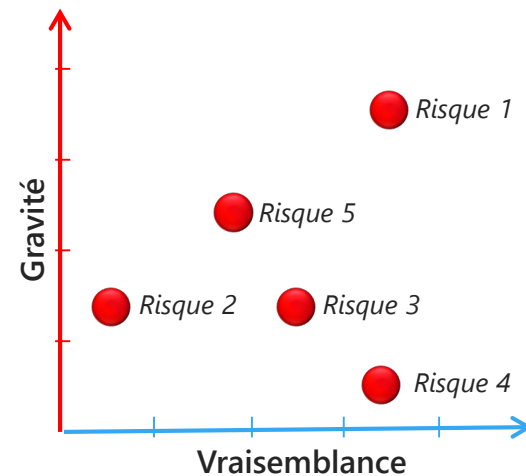
L'estimation de la gravité et de la vraisemblance sont réalisées grâce à des échelles définies par l'organisation si elles existent.

Comment évaluer le niveau d'un risque ?



Qu'est-ce qu'une bonne échelle ?

- Non ambiguë
- Explicite
- Comprise par tous (utilisateurs et lecteurs)
- Tous les niveaux sont susceptibles d'être utilisés
- Privilégie un nombre de niveaux pair.



Exercice : éléments utiles à l'estimation de la gravité et la vraisemblance

Éléments utiles à l'estimation...

... du niveau de risque

Importance de l'objet de l'étude considéré

Exposition aux menaces considérées

Existence de vulnérabilités

Facilité d'exploitation des vulnérabilités

Nombre de conséquences identifiées

Capacité et motivation des attaquants



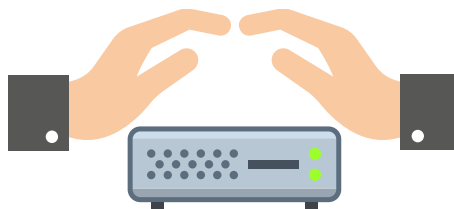
Rappel sur les fondamentaux de la sécurité numérique

Les besoins de sécurité : Disponibilité, Intégrité et Confidentialité



Disponibilité

Propriété d'être accessible et utilisable à la demande par une entité autorisée.



Intégrité

Propriété d'exactitude et de complétude.



Confidentialité

Propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés.

Rappel sur les fondamentaux de la sécurité numérique

Les actifs

Il est crucial de savoir ce qui a de la valeur dans son organisation...

Actifs d'information et de processus

Fichiers de données, processus, base de données, procédure et manuels d'utilisateurs, archives...

Actifs physiques

Serveurs informatiques, PC portables, matériels de communication, PABX, unité de climatisation...



... pour savoir quoi protéger !

Actifs applicatifs

Progiciels, logiciels spécifiques, systèmes d'exploitation, outils de développement, utilitaires...

Actifs humains

Personnels de direction, techniciens, développeurs, administrateurs...

Rappel sur les fondamentaux de la sécurité numérique

La menace

Menace

Terme générique utilisé pour désigner toute intention hostile de nuire dans le cyber espace. Une menace peut être ciblée ou non sur l'objet de l'étude.



Interne ou externe, cyber, humaine et délibérée

Exemple de menaces relatives aux actifs (délibérées ou humaines)



Menaces sur les actifs personnels :

- Vol ou usurpation d'identité en ligne
- Accès non autorisé aux informations financières d'une personnes – vol d'argent à une personne et fraude.

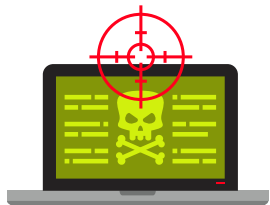


Menaces sur les actifs organisationnels :

- Défiguration de site web ou classifiées de défense
- Vol de nom de domaine par des cybersquatteurs
- Accès non autorisé à des rapports financiers
- Accès non autorisé à des informations sensibles.

Rappel sur les fondamentaux de la sécurité numérique

La vulnérabilité



Vulnérabilité

Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.

| Type | Exemples |
|-----------|---|
| Matériel | <ul style="list-style-type: none">• Maintenance insuffisante/ mauvaises installations des supports de stockage• Manque de prudence lors de la mise au rebut |
| Logiciel | <ul style="list-style-type: none">• Tests de logiciels absents ou insuffisants• Interface utilisateurs compliquée |
| Réseau | <ul style="list-style-type: none">• Voies de communication non protégées• Architecture réseau non sécurisée |
| Personnel | <ul style="list-style-type: none">• Formation insuffisante à la sécurité• Travail non surveillé d'une équipe extérieure ou d'une équipe d'entretien |
| Site | <ul style="list-style-type: none">• Utilisation inadaptée ou négligente du contrôle d'accès physique aux bâtiments et salles• Emplacement situé dans une zone sujette aux inondations |
| Organisme | <ul style="list-style-type: none">• Absence de politique relative à l'utilisation des courriels• Absence de responsabilités en sécurité de l'information dans les descriptions de postes |

Rappel sur les fondamentaux de la sécurité numérique

Relation entre vulnérabilité et menace



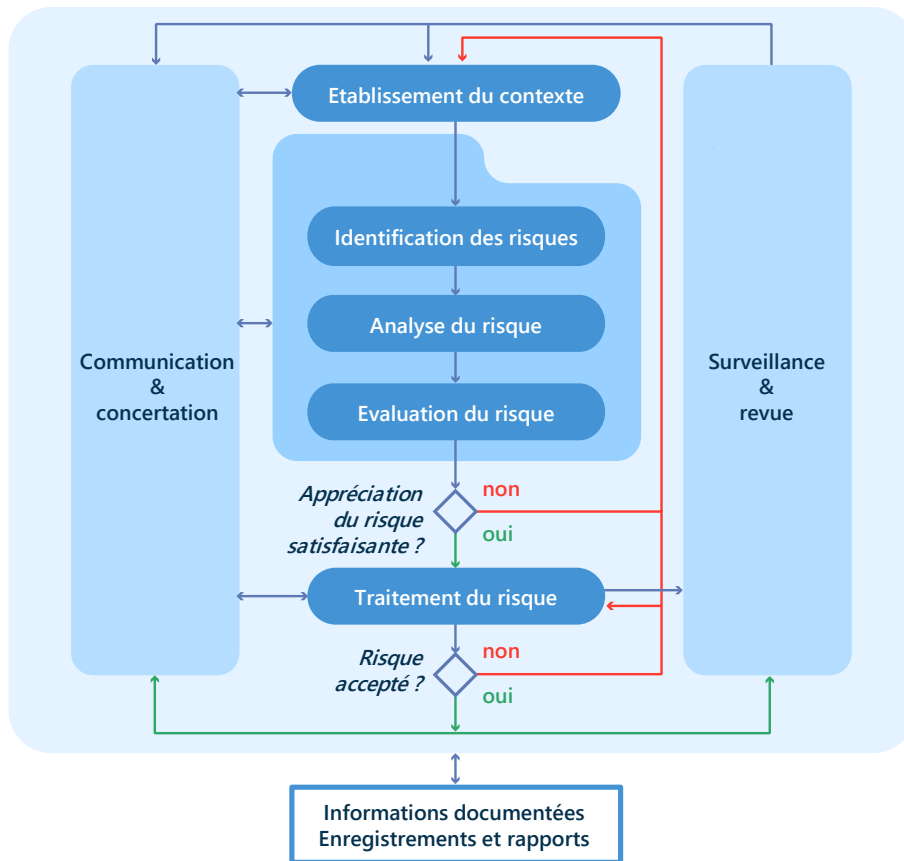
| Vulnérabilités | Menaces |
|---|--|
| Entrepôt non protégé et sans surveillance | > Vol |
| Procédures compliquées de traitement de données | > Erreur d'entrée de données par le personnel |
| Pas de séparation de tâches | > Fraude, utilisation non autorisés d'un système |
| Données non chiffrées | > Vol d'information |
| Utilisation de logiciels piratés | > Poursuite judiciaire, virus |
| Pas de revue des droits d'accès | > Accès non autorisé par des personnes qui ont quitté l'organisation |
| Pas de procédures de sauvegarde | > Perte d'information |



En soi, la présence d'une vulnérabilité ne produit pas de dommage ; une menace doit exister pour l'exploiter.

Corollaire : une menace qui n'est pas en lien avec une vulnérabilité ne représente pas un risque.

Processus de l'analyse de risque



L'analyse de risque



Si je ne sais pas ce que je dois protéger, comment le protéger ?

Une analyse de risque a pour but de :

- Identifier, évaluer et couvrir les principaux risques qui peuvent peser sur le SI
- Gérer durablement les risques dans le temps.



**Une analyse de risque ne vous protège pas des risques.
Elle vous permet d'en faire prendre conscience aux décideurs.**

Carte d'identité de la méthode EBIOS Risk Manager



Vision

Offrir une compréhension partagée des risques cyber entre les décideurs et les opérationnels.

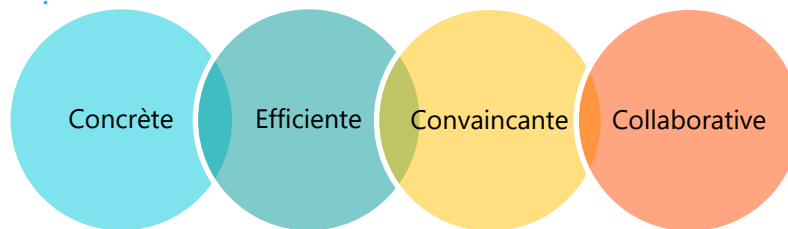
Utilisateurs de la méthode

Risk managers, RSSI, Chefs de projet, experts en cybersécurité et personnes souhaitant manager les risques sur un système.

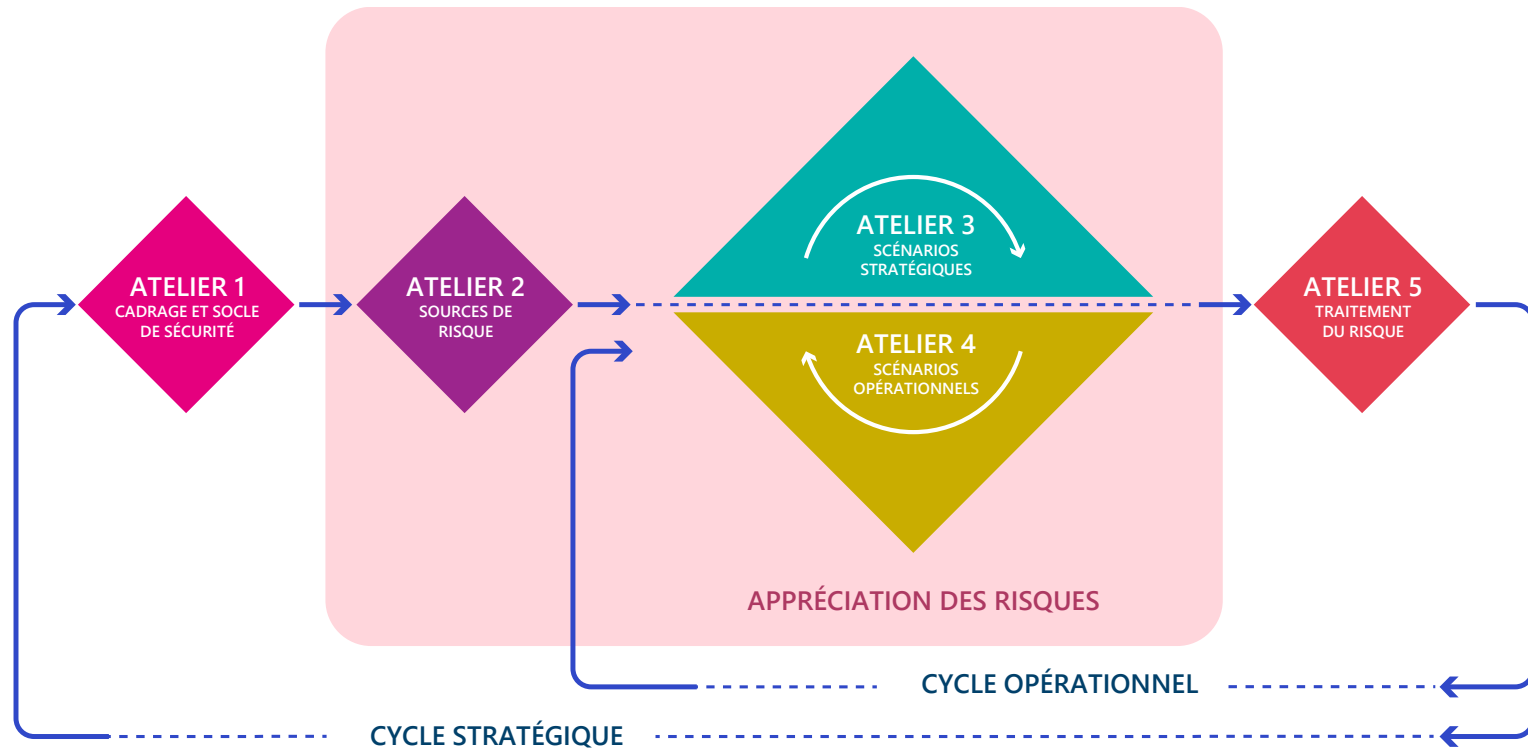
Fondamentaux

1. Une démarche structurée en ateliers, adaptable selon l'objectif de l'étude,
2. Une synthèse entre conformité et scénarios de risques,
3. Une alternance entre point de vue de l'organisation et celui de l'attaquant,
4. Une prise en compte de l'écosystème,
5. Une approche efficace plutôt qu'exhaustive.

Valeurs



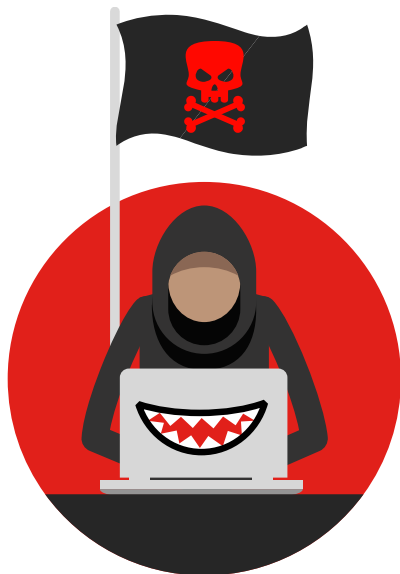
Fondement 1 : une démarche structurée en ateliers



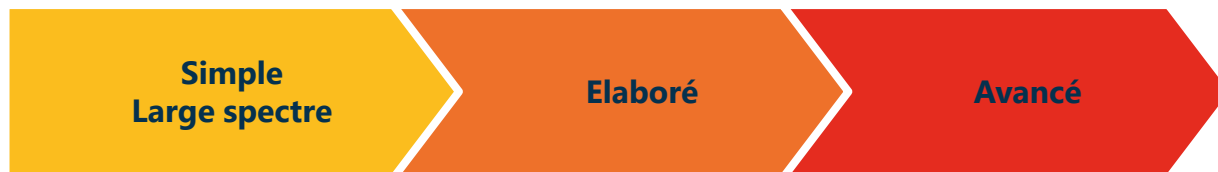


Fondement 2 : une synthèse entre conformité et scénarios de risques

La pyramide du management du risque



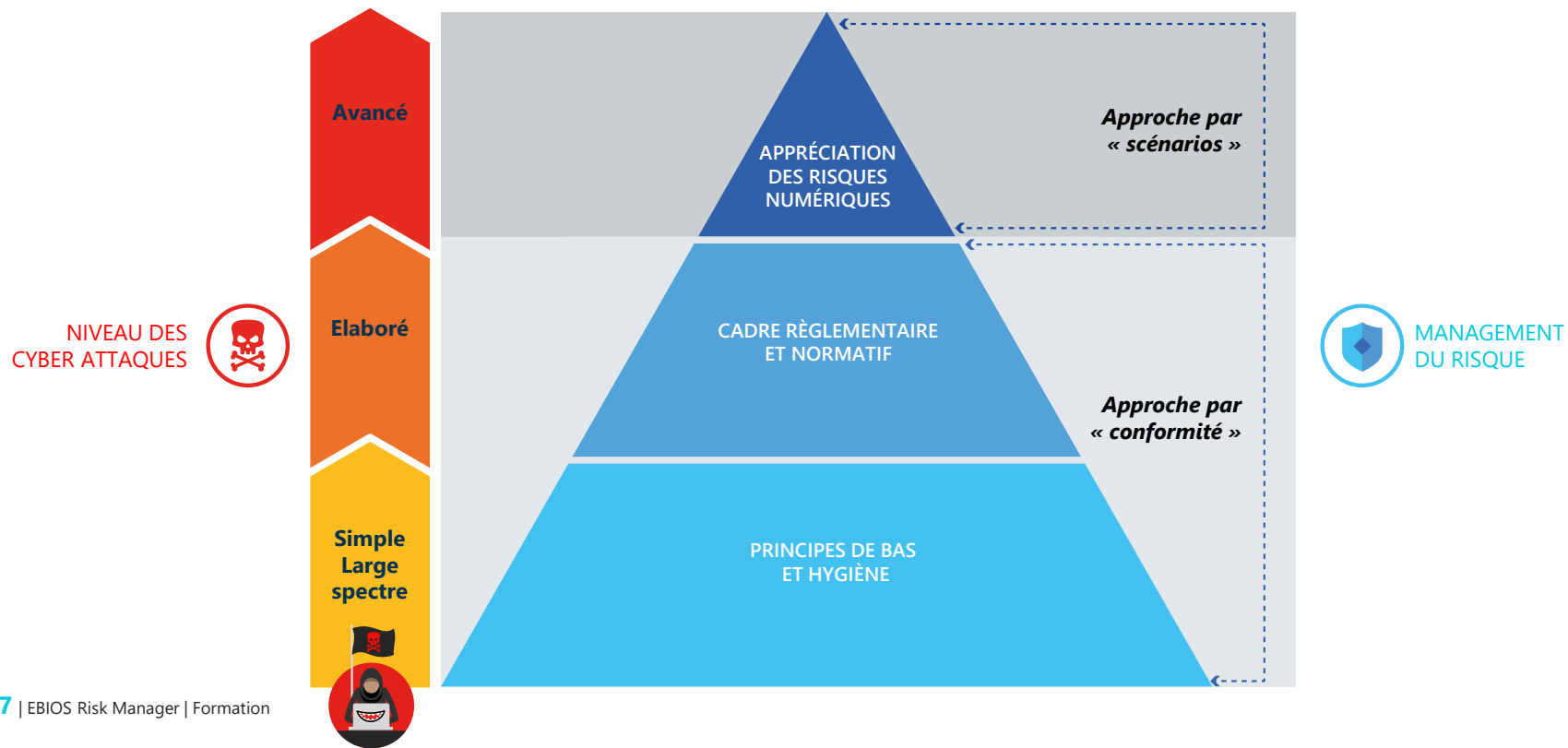
Niveaux des cyber attaques





Fondement 2 : une synthèse entre conformité et scénarios de risques

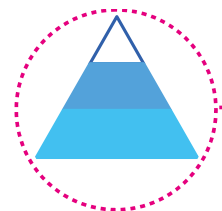
La pyramide du management du risque



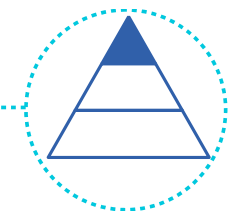
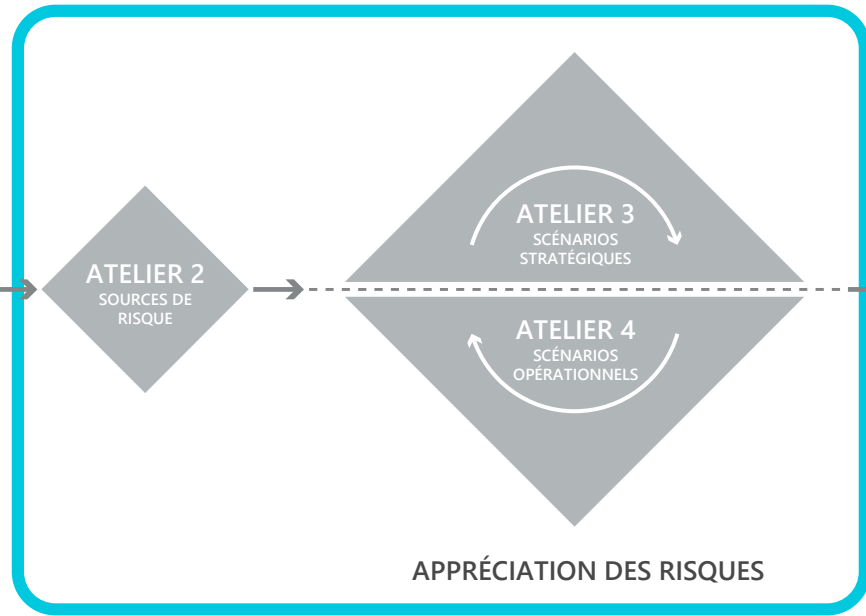


Fondement 2 : une synthèse entre conformité et scénarios de risques

La pyramide du management du risque



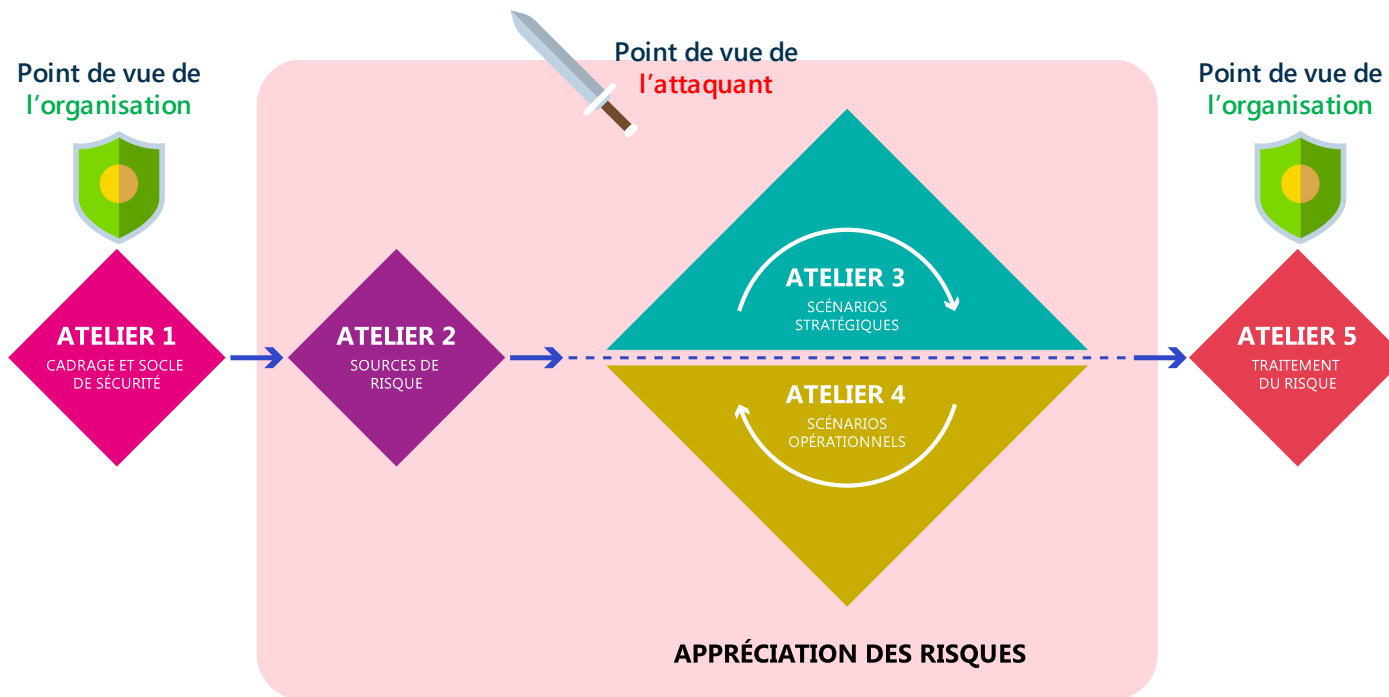
Approche par « conformité »



Approche par « scénarios »

Fondement 3 : une alternance entre points de vue

Organisation versus attaquant



Fondement 4 : une prise en compte de l'écosystème

Ensemble des parties prenantes en interaction avec l'objet de l'étude

Quelles parties prenantes de l'écosystème peuvent exposer le SI par leur faible fiabilité cyber et du fait de ma forte dépendance ?

Légende



Source de Risque



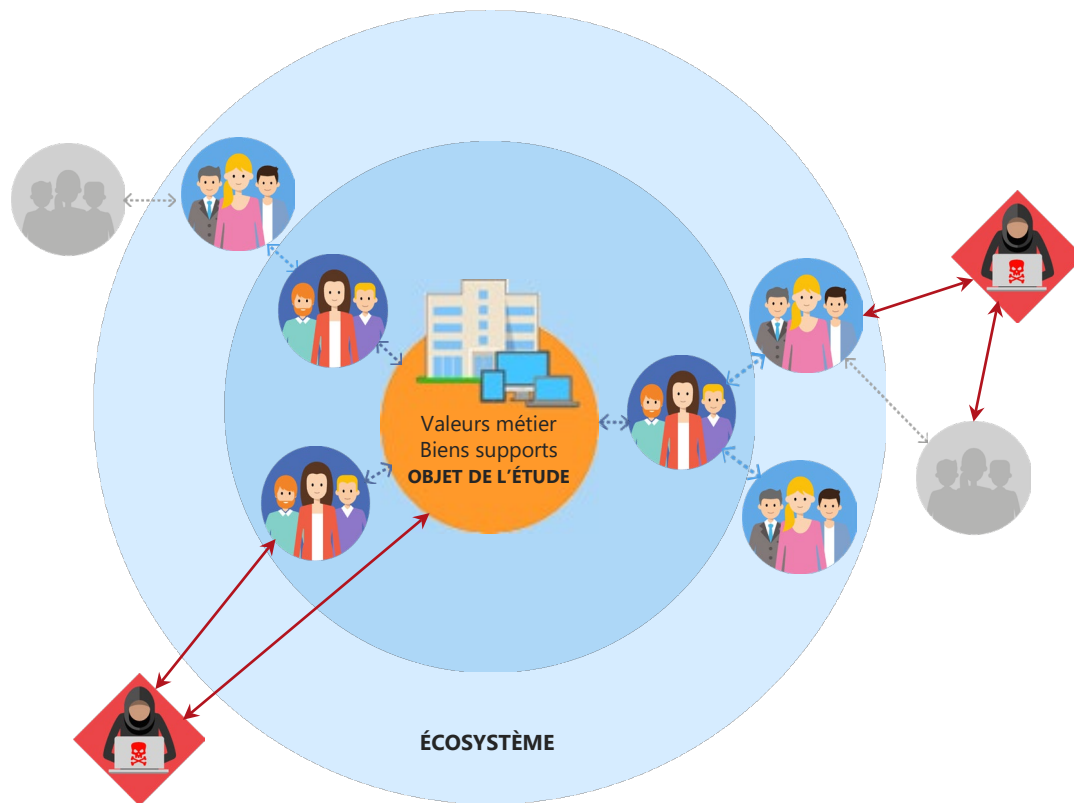
Partie prenante directement reliée au système (1^{er} niveau de relation)



Partie prenante reliée à une autre partie prenante (2^{ème} niveau de relation)



Partie prenante de 3^{ème} niveau



Fondamentaux 5 : une approche efficace plutôt qu'exhaustive

Un outil de gestion de risque

- Focalisation sur les éléments les plus importants / urgents / graves
 - Production d'un document efficace et accessible plutôt qu'exhaustif
- ⇒ EBIOS RM est un outil de gestion de risque efficace et utile.



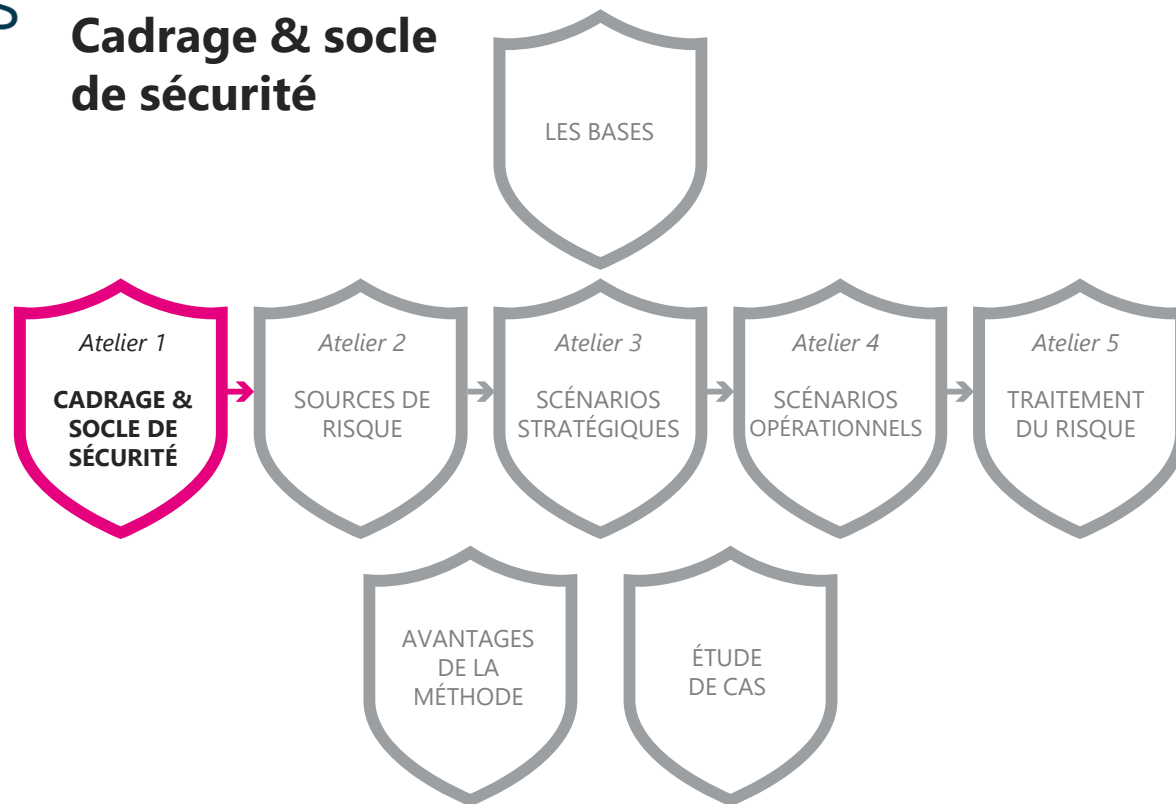
Ce que vous devez être capable de faire à ce stade



› Savoir définir un risque

› Lister les 5 fondamentaux
de la méthode EBIOS *Risk
Manager*

Atelier 1 Cadrage & socle de sécurité



Cadrage & socle de sécurité

Atelier 1



Objectif

Définir le cadre de l'étude et du projet, son périmètre métier et technique.



Participants

Direction, Métiers, RSSI, DSI.

Éléments en entrée

Si disponible, résultats d'une précédente analyse des risques

ATELIER 1 CADRAGE ET SOCLE DE SÉCURITÉ

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 et leurs justifications.



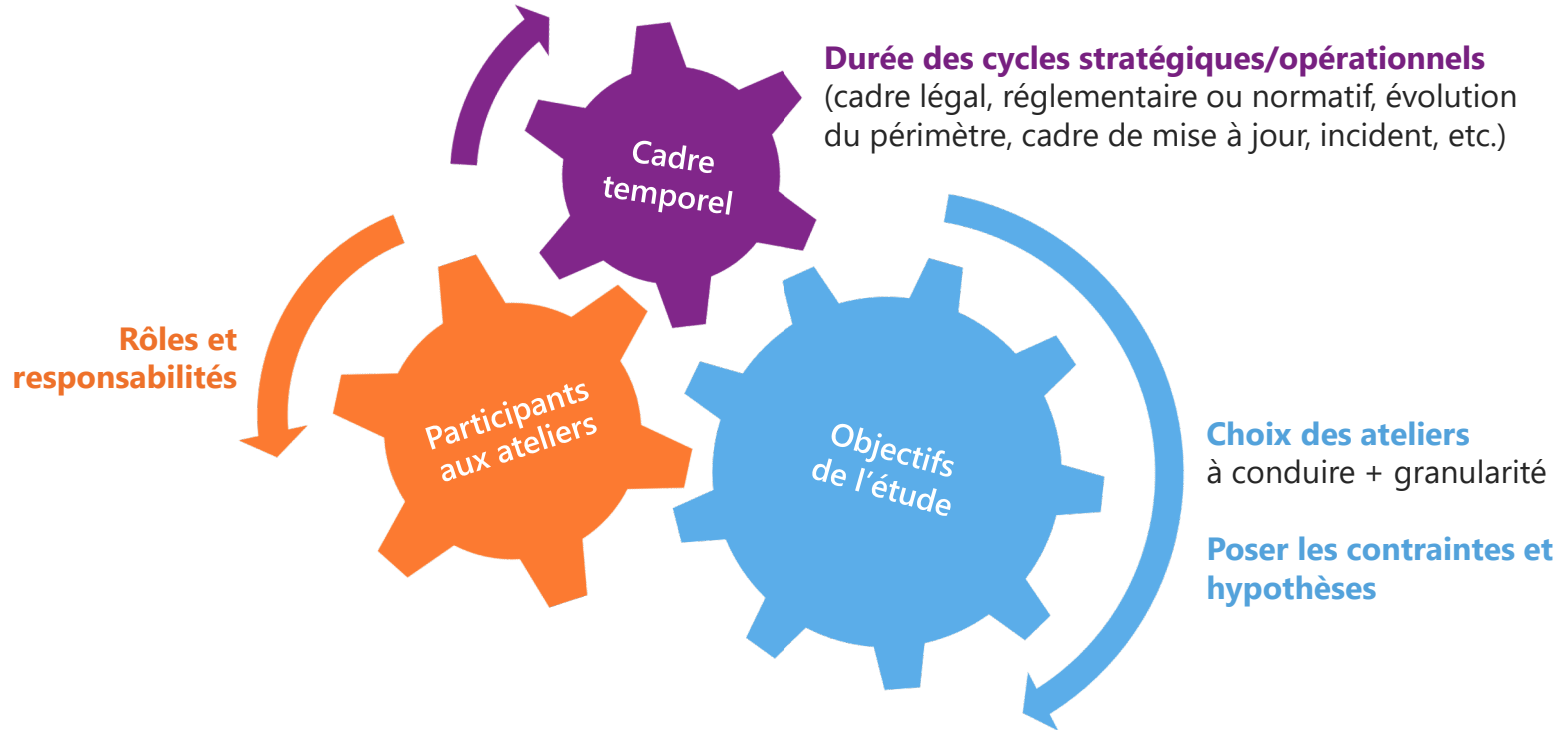
Cadrage & socle de sécurité

Atelier 1

- **Activité 1**
Définir le cadre de l'étude
- **Activité 2**
Définir le périmètre métier et technique
- **Activité 3**
Identifier les événements redoutés
- **Activité 4**
Déterminer le socle de sécurité



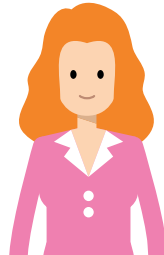

Définir le cadre de l'étude

Activité 1-1



Exemple d'un RACI

Activité 1-1

| |  Pierre – RSSI |  Paul – Direction |  Marjorie – Architecte |  Jacques – IT |
|---|--|--|---|--|
| Définition du périmètre de l'analyse de risques | R | A | I | C |
| Identification des exigences légales, réglementaires, et contractuelles | R | A | C | I |
| Évaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude | I | I | A R | C |
| Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème | C | R | C | A |

R = Responsable | A = Approbateur | C = Consulté | I = Informé

Définir le périmètre métier et technique

Activité 1-2 • Les questions à se poser

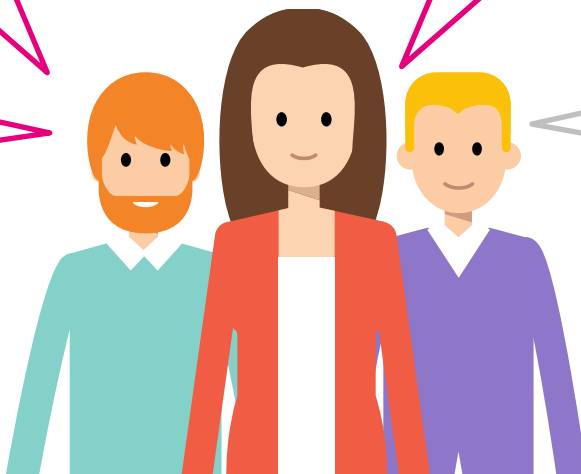
Quelles sont les **valeurs métier** (processus et informations majeures) permettant à l'objet étudié de réaliser ses missions ?

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

Quels sont les événements redoutés (atteintes aux valeurs métier préjudiciables pour l'organisation) ? Quelle est la gravité du préjudice ?

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

Quel est le socle de sécurité applicable ? (exigences contractuelles / réglementaires / PSSI)



Définir le périmètre métier et technique

Activité 1-2 • Quelques définitions



Missions

Fonction, finalité, raison d'être de l'objet de l'étude.

Valeurs métier

Composante importante pour l'organisation dans l'accomplissement de sa mission :

- un service,
- une fonction support,
- une étape dans un projet,
- information ou savoir-faire.

Biens supports

Composante du système d'information sur laquelle repose une ou plusieurs valeurs métier :

- numérique,
- physique, ou
- organisationnelle.

Définir le périmètre métier et technique

Activité 1-2 • Focus sur la mission

Mission

Fonction, finalité, raison d'être de l'objet de l'étude.

Pour vous aidez à identifier la mission de l'organisation, vous pouvez...

- Vous demander à quoi sert l'objet de l'étude ?
- Vous demander quelle est sa finalité pour le métier de l'organisation ?



Définir le périmètre métier et technique

Activité 1-2 • Focus sur les valeurs métiers

Valeur métier

Composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet et toute information ou savoir-faire associé.

Pour vous aider à identifier les valeurs métiers, vous pouvez commencer par regarder le fonctionnement de l'organisation, ses macro-processus.

Vous pouvez aussi identifier des **informations** qui seraient transverses à l'organisation.

Conseils !



- *Toujours se positionner dans l'objectif de la réussite de la mission.*
- *Cela doit être une valeur métier pour la maîtrise d'ouvrage / direction métier.*

Définir le périmètre métier et technique

Activité 1-2 • Focus sur les biens supports

Bien support

Composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Peut être de nature numérique, physique ou organisationnelle.

Pour vous aider à identifier les biens support de l'objet de l'étude, vous pouvez identifier ...

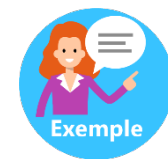
- les services numériques,
- les applications,
- les réseaux informatiques,
- les structures organisationnelles,
- les ressources humaines,
- les locaux,
- etc.

qui permettent de mener à bien les processus ou de traiter les informations, c'est-à-dire les valeurs métiers.



Définir le périmètre métier et technique

Activité 1-2 • Exemple



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. [...]

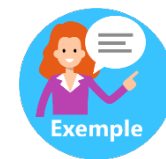
[Sources Internet : Le Point.fr et ZDNet]

| | |
|---|-------------|
| Commanditaire de l'analyse de risque | Le collègue |
| Mission | |
| Valeur métier | |
| Bien support | |



Définir le périmètre métier et technique

Activité 1-2 • Exemple



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. [...]

[Sources Internet : Le Point.fr et ZDNet]

| | |
|---|---|
| Commanditaire de l'analyse de risque | Le collègue |
| Mission | Gestion des résultats scolaires pour évaluer les élèves |
| Valeur métier | Notes des élèves (information) |
| Bien support | Système d'information du collègue |



Pourquoi et comment limiter le nombre de valeurs métier et de biens supports ?

Activité 1-2

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.

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



› 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 (les classer par exemple selon leurs besoins de sécurité).



Premières notions

Activité 1-2 • Synthèse

DAB
➤ **Bien support**

Processus "délivrer
les billets"
➤ **Valeur métier**

Mission
➤ **Distribuer des
billets de banque**



Faible au niveau du
terminal
➤ **Vulnérabilité**

Hacker
➤ **Attaquant
(Source de risques)**

Cas fictif • Société de biotechnologies

Activité 1-2



**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

Définir le périmètre métier et technique

Activité 1-2



Mission : ????

| | | | | |
|--|--|--|--|--|
| DÉNOMINATION DE LA VALEUR MÉTIER | | | | |
| Nature de la valeur métier (processus ou information) | | | | |
| Description | | | | |
| Propriétaire (interne/externe) | | | | |
| DÉNOMINATION DU/DES BIENS SUPPORTS ASSOCIÉS | | | | |
| Description | | | | |
| Propriétaire (interne/externe) | | | | |

Définir le périmètre métier et technique

Activité 1-2



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) | | | |
| Description | | | |
| Propriétaire (interne/externe) | | | |
| DÉNOMINATION DU/DES BIENS SUPPORTS ASSOCIÉS | | | |
| Description | | | |
| Propriétaire (interne/externe) | | | |

Définir le périmètre métier et technique

Activité 1-2



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"> • l'identification des antigènes • la production des antigènes (vaccin vivant atténué, inactivé, sous-unité) : fermentation (récolte), purification, inactivation, filtration, stockage • l'évaluation préclinique • le développement clinique | | | Activité consistant à réaliser : <ul style="list-style-type: none"> • le remplissage de seringues (stérilisation, remplissage) • le conditionnement (étiquetage et emballage) | Informations permettant d'assurer le contrôle qualité et la libération de lot (ex : antigène, répartition aseptique, conditionnement, libération finale...) |
| Propriétaire (interne/externe) | Pharmacien de biotechnologies | | | 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 pour produire des antigènes | Ensemble de machines et équipements informatiques permettant de fabriquer des vaccins à grande échelle | Serveurs bureautiques pour stocker les données relatives à la traçabilité et au contrôle des différents processus |
| Propriétaire (interne/externe) | DSI | Laboratoires | Laboratoires | DSI + Fournisseurs de matériel | DSI |

Identifier les événements redoutés

Activité 1-3 • Les questions à se poser

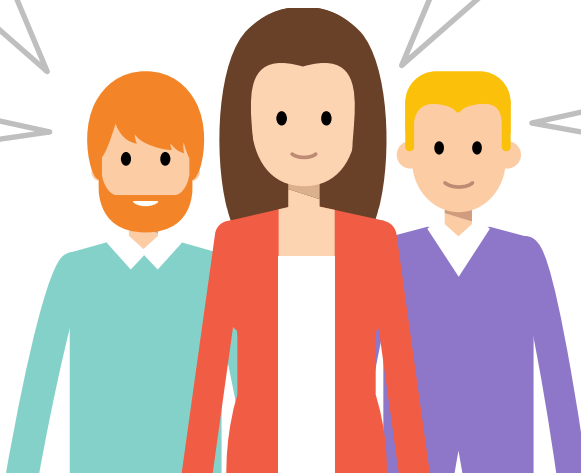
Quels sont les valeurs métier (processus et informations majeures) permettant à l'objet étudié de réaliser ses missions ?

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

Quels sont les événements redoutés (atteintes aux valeurs métier préjudiciables pour l'organisation) ? Quelle est la gravité du préjudice ?

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

Quel est le socle de sécurité applicable ? (exigences contractuelles / réglementaires / PSSI)



Identifier les événements redoutés

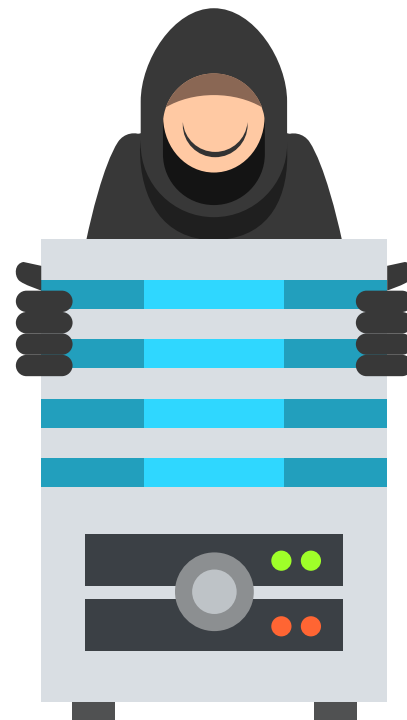
Activité 1-3

Événement Redouté (ER)

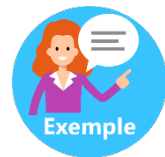
Un événement redouté est associé à une valeur métier et porte atteinte à un critère ou besoin de sécurité de la valeur métier. Chaque événement redouté est évalué selon le niveau de gravité des conséquences, à partir d'une métrique.

Conseils !

- *Se situer du point de vue de l'organisation*
- *Identifier les événements qui font « le plus peur »*
- *Les événements redoutés doivent formuler / traduire les craintes des métiers :*
 - *Un événement redouté est décrit sous la forme d'une expression courte ou d'un scénario permettant une compréhension facile du préjudice lié à l'atteinte de la valeur métier concernée.*
 - *Il n'est pas nécessaire d'être exhaustif.*
 - *Les événements redoutés doivent conserver du sens pour le métier.*



Comment estimer l'impact d'un événement redouté ?



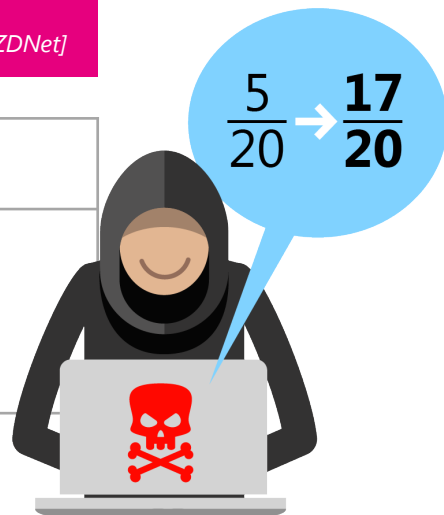
QUIZ

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

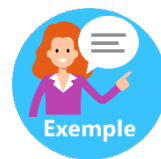
Un adolescent de quinze ans a été interpellé pour s'être introduit dans le système informatique de son collègue dans le but de modifier ses résultats scolaires. [...]

[Sources Internet : Le Point.fr et ZDNet]

| | |
|-----------------------------------|------------------------|
| Evènement redouté possible | Modification des notes |
| Impacts | |



Comment estimer l'impact d'un événement redouté ?



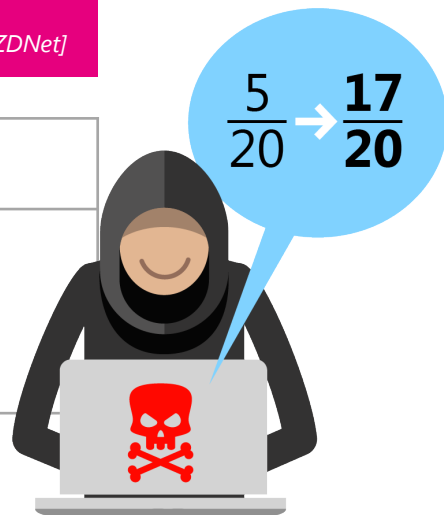
QUIZ

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. [...]

[Sources Internet : Le Point.fr et ZDNet]

| | |
|-----------------------------------|--|
| Evènement redouté possible | Modification des notes |
| Impacts | <ul style="list-style-type: none">• Impact opérationnel (la poursuite d'étude des collégiens)• Impact d'image (vis à vis des autres établissements scolaires) |



Catégories d'impacts possibles

Activité 1-3 • Vue globale

Impacts sur les missions et service de l'organisation

Impacts humains, matériels ou environnementaux

Impacts sur la gouvernance

Impacts financiers

Impacts juridiques

Impacts sur l'image et la confiance



Catégories d'impacts possibles

Activité 1-3

Impacts sur les missions et service de l'organisation

Conséquences directes ou indirectes
sur la réalisation des missions et services



Catégories d'impacts possibles

Activité 1-3

Impacts sur les missions et service de l'organisation

Conséquences directes ou indirectes sur l'intégrité physique de personnes

Impacts humains, matériels ou environnementaux

Dégâts matériels ou destruction de biens supports

Conséquences écologiques à court ou long terme, directes ou indirectes



Catégories d'impacts possibles

Activité 1-3

Impacts sur les missions et service de l'organisation

Impacts humains, matériels ou environnementaux

Impacts sur la gouvernance

Conséquences directes ou indirectes sur la qualité des liens sociaux au sein de l'organisation

Conséquences directes ou indirectes sur la liberté de décider, de diriger, de mettre en oeuvre la stratégie de développement

Conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisation, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes



Catégories d'impacts possibles

Activité 1-3

Impacts sur les missions et service de l'organisation

Impacts humains, matériels ou environnementaux

Impacts sur la gouvernance

Impacts financiers

Conséquences pécuniaires, directes
ou indirectes

Catégories d'impacts possibles

Activité 1-3

Impacts sur les missions et service de l'organisation

Impacts humains, matériels ou environnementaux

Impacts sur la gouvernance

Impacts financiers

Impacts juridiques

Conséquences suite à une non-conformité
légale, réglementaire, normative ou
contractuelle

Catégories d'impacts possibles

Activité 1-3

Impacts sur les missions et service de l'organisation

Impacts humains, matériels ou environnementaux

Impacts sur la gouvernance

Impacts financiers

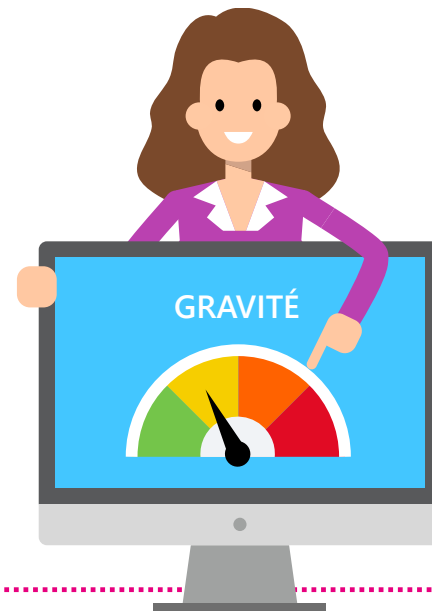
Impacts juridiques

Impacts sur l'image et la confiance

Conséquences directes ou indirectes
sur l'image de l'organisation, la notoriété,
la confiance des clients

Définir une échelle de gravité

Activité 1-3



Conseil !

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



| Echelle | Définition |
|--------------------------|---|
| G1 • Mineur | 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) |
| G2 • Significatif | 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) |
| G3 • Important | 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) |
| G4 • Critique | 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) |

Exemple d'échelle de gravité

| Niveaux | Impacts financiers | Impacts juridiques | Impacts opérationnels | Impacts sociaux | Impacts sur les biens et les personnes | Impacts sur l'image ou la réputation |
|-----------------------|--------------------|--------------------|-----------------------|-----------------|---|---|
| 1 Mineur | | | | | Ils sont négligeables | Ils sont négligeables |
| 2 Significatif | | | | | Ils sont perceptibles mais limités : <ul style="list-style-type: none"> • Vol et dégradation mineurs. • Risques psychosociaux mineurs : stress, anxiété... • Incapacité totale de travail (ITT) inférieure ou égale à 8 jours | Ils sont perceptibles mais limités : <ul style="list-style-type: none"> • Perturbations légères, limitées dans la durée |
| 3 Important | | | | | Ils sont importants : <ul style="list-style-type: none"> • Risques psychosociaux importants : mise en danger, dépression, harcèlement, absentéisme, ... • Vols et dégradations importantes. • ITT supérieure à 8 jours ou ITT impactant un mineur | Ils sont importants quel que soit le domaine concerné : <ul style="list-style-type: none"> • Conséquences perceptibles et durables. Un effort substantiel va devoir être consenti pour y remédier |
| 4 Critique | | | | | Ils sont critiques : <ul style="list-style-type: none"> • Nombreux blessés, décès et / ou invalidités ; • Application du droit de retrait ; • Atteinte directe à des éléments cruciaux aux biens ou personnes (appareil médical, eau potable, ...) | Ils sont critiques : <ul style="list-style-type: none"> • Conséquences durables pouvant nécessiter un traitement et une communication à haut niveau. • Une communication à l'échelle nationale, voire internationale est possible |

Exemple d'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">• Impacts sur la sécurité ou la santé des personnes• Impacts sur l'image et la confiance• Impacts juridiques | |
| | | | |
| | | | |
| | | | |
| Fabriquer des vaccins | | | |
| | | | |
| Traçabilité et contrôle | | | |

Exemple d'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"> • Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts juridiques | |
| | Fuite des informations d'études et recherches de l'entreprise | <ul style="list-style-type: none"> • Impacts sur le patrimoine intellectuel • Impacts financiers | |
| | Perte ou destruction des informations d'études et recherches | <ul style="list-style-type: none"> • Impacts sur les missions et services de l'organisme • Impacts sur les coûts de développement • Impacts sur le patrimoine intellectuel | |
| | Interruption des phases de tests des vaccins pendant plus d'une semaine | <ul style="list-style-type: none"> • Impacts sur les missions et services de l'organisme • Impacts financiers | |
| 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"> • Impacts financiers | |
| | 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"> • Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts financiers | |
| Traçabilité et contrôle | Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire | <ul style="list-style-type: none"> • Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts juridiques | |

Exemple d'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"> Impacts sur la sécurité ou la santé des personnes Impacts sur l'image et la confiance Impacts juridiques | 3 |
| | Fuite des informations d'études et recherches de l'entreprise | <ul style="list-style-type: none"> Impacts sur le patrimoine intellectuel Impacts financiers | 3 |
| | Perte ou destruction des informations d'études et recherches | <ul style="list-style-type: none"> Impacts sur les missions et services de l'organisme Impacts sur les coûts de développement Impacts sur le patrimoine intellectuel | 2 |
| | Interruption des phases de tests des vaccins pendant plus d'une semaine | <ul style="list-style-type: none"> Impacts sur les missions et services de l'organisme Impacts financiers | 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"> Impacts financiers | 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"> Impacts sur la sécurité ou la santé des personnes Impacts sur l'image et la confiance Impacts financiers | 4 |
| Traçabilité et contrôle | Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire | <ul style="list-style-type: none"> Impacts sur la sécurité ou la santé des personnes Impacts sur l'image et la confiance Impacts juridiques | 4 |

Déterminer le socle de sécurité

Activité 1-4 • Les questions à se poser

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 ?

Quels sont les événements redoutés (atteintes aux valeurs métier préjudiciables pour l'organisation) ? Quelle est la gravité du préjudice ?

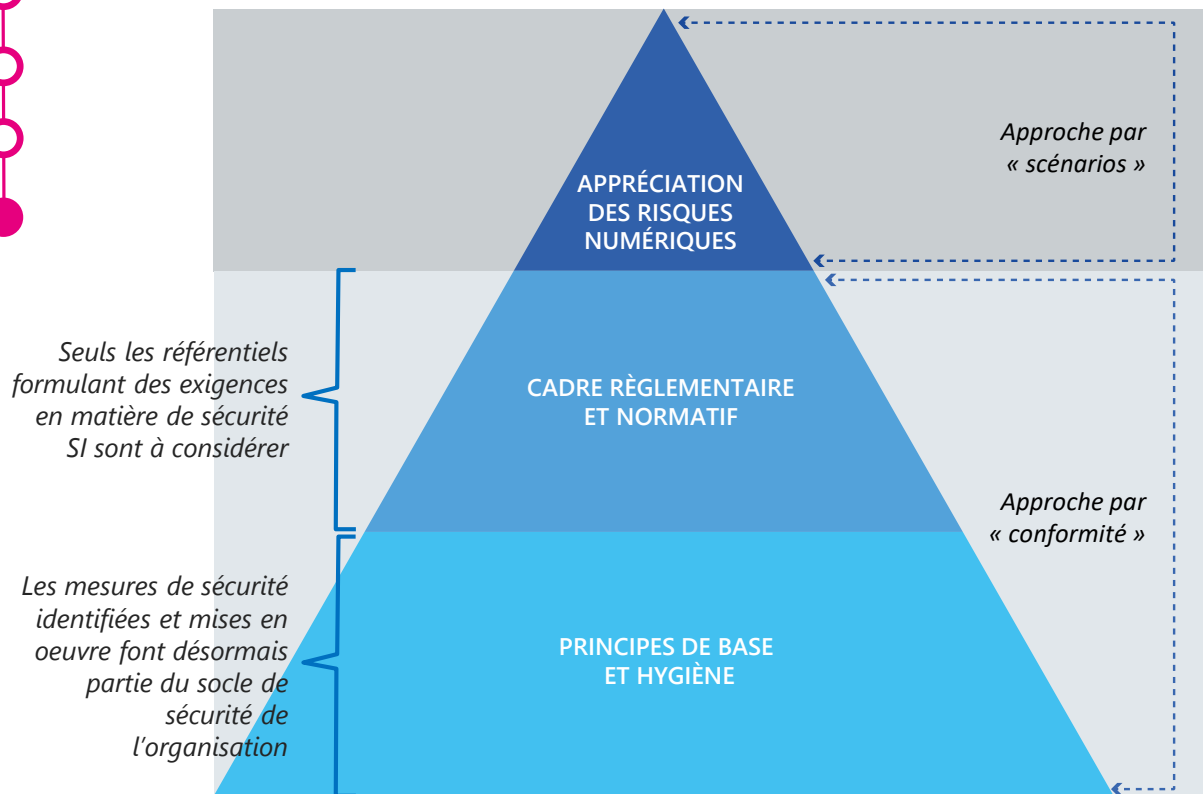
A quoi sert l'objet de l'étude ? Quelles sont ses missions principales, ses finalités ?

Quel est le socle de sécurité applicable ? (exigences contractuelles / réglementaires / PSSI)



Déterminer le socle de sécurité

Activité 1-4



Important !

Bien identifier les écarts et leurs causes.



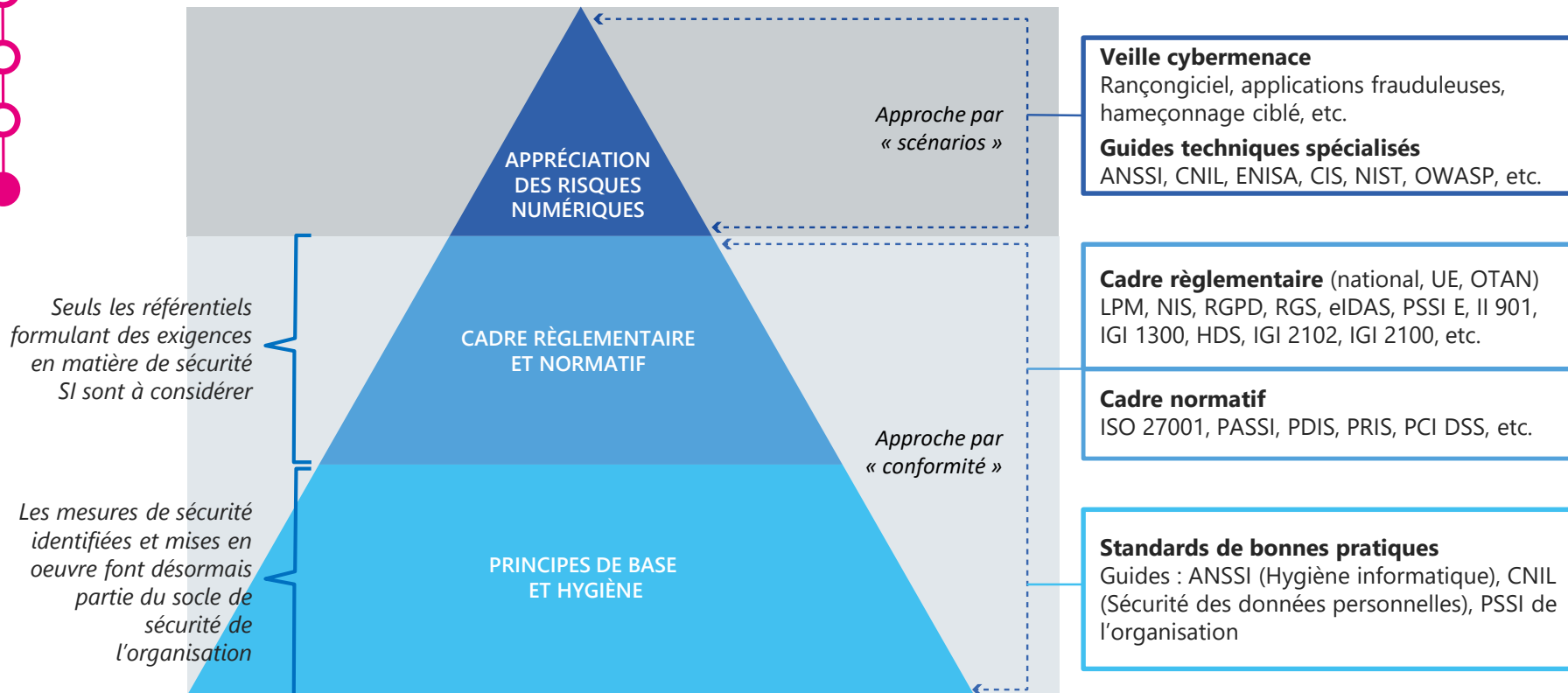
Socle de sécurité Approche par « conformité »

Identifier les règles applicables à l'objet de l'étude :

- **Référentiels externes**
Guides de recommandations de l'ANSSI, etc.
- **Référentiels internes**
Règles de sécurité internes à l'organisation (PSSI).
- **Normes**
Famille ISO 27000, etc.
- **Règlementations en vigueur**
IGI 1300, II 901, LPM, directive NIS, RGS, etc.

Déterminer le socle de sécurité

Activité 1-4



Exemple de socle de sécurité

Activité 1-4 • Exemple avec l'II 901

Revue de conformité à l'instruction interministérielle 901

| Titre | Article | Exigences de sécurité | Note | Détails de l'écart & Justifications |
|--|---|---|------|---|
| TITRE II Protection des systèmes d'information sensibles | ARTICLE 5 Détermination la sensibilité des informations | <p>Chaque entité mettant en oeuvre un système d'information sensible :</p> <ul style="list-style-type: none"> • Identifie l'information sensible qu'elle traite • Marque cette information par les moyens de son choix • Détermine , si besoin, une échelle de sensibilité correspondant à des niveaux en matière de disponibilité, d'intégrité et de confidentialité des informations de son système d'information sensible • Applique des mesures de protection adaptées. <p>Lorsque les informations sensibles transitent entre plusieurs entités, leur niveau de sensibilité est explicitement mentionné par l'entité émettrice afin qu'elles soient protégées en conséquence par l'entité destinataire en termes de disponibilité, d'intégrité et de confidentialité, pendant et après leur transit.</p> | 3 | |
| | ARTICLE 6 Gouvernance de la protection des systèmes d'information | <p>Chaque entité :</p> <ul style="list-style-type: none"> • Applique une politique de sécurité des systèmes d'information (PSSI), validée au plus haut niveau de l'entité et couvrant tous les aspects , techniques ou non, de la sécurité (communication, ressources humaines et financières, aspects juridiques, etc.); • Organise la gouvernance et attribue les responsabilités en matière de sécurité des systèmes d'information. | 2 | Responsabilités pas encore toutes définies |
| | ARTICLE 7 Maîtrise des risques | <p>La PSSI de l'entité résulte d'une analyse des risques menée :</p> <ul style="list-style-type: none"> • Pour tous les risques, pas seulement techniques, qu'ils soient d'origine humaine ou non • Pour chacun des systèmes d'information de l'entité • En appréciant l'impact qu'une menace sur un composant du système pourrait avoir sur les missions de l'entité, son image, son patrimoine ou la sécurité des biens et de personnes. | 0 | Analyse de risque pas encore menée |
| | ARTICLE 8 homologation de systèmes d'information sensibles | <p>Tout système d'information sensible doit faire l'objet d'une homologation de sécurité avant a mise en service. Dans le dossier d'homologation figurent notamment les risques résiduels, c'est-à-dire ceux qui ne sont pas couverts par des mesures de protection. L'autorité d'homologation doit être choisie au sein de l'entité, au niveau hiérarchique suffisant pour assumer la responsabilité afférente à la décision d'homologation. Elle accepte notamment les risques résiduels. Elle est en principe l'autorité qui emploie le système. En prononçant sa décision d'homologation, l'autorité d'homologation déclare que le système d'information est conforme aux règles prévues par la présente instruction.</p> | 1 | Le processus d'homologation vient d'être initié |

Exemple de socle de sécurité

Activité 1-4 • Exemple avec le RGS

Revue de conformité au référentiel général de sécurité (RGS) v2.0

| Domaine | Ref. | Exigences de sécurité (corps du RGS) | Note | Détails de l'écart & Justifications |
|------------|------|--|------|--|
| Conformité | R1 | Une analyse de risque a été menée sur le SI. | 1 | Analyse de risque initiée (atelier 1 en cours) |
| | R2 | Les objectifs de sécurité ont été établis. | 3 | |
| | R3 | Des mesures techniques et/ou organisationnelles ont été établies pour atteindre les objectifs de sécurité. | 0 | En attente résultat audit et AdR |
| | R4 | Le système d'information fait l'objet d'un processus d'homologation donnant lieu à une décision (attestation formelle) signée par l'autorité responsable. | 1 | Cadrage réalisé |
| | R5 | L'autorité administrative met en place un suivi opérationnel de la sécurité du SI notamment au travers de mesures de surveillance et de détection, permettant de réagir au plus vite aux incidents de sécurité et de les traiter au mieux. | 0 | Non commencé |
| | R6 | Pour les SI déjà en service, un audit de la sécurité du système d'information en interne ou externalisé auprès d'un prestataire doit être mené avec mise en œuvre des mesures correctives fixées dans le rapport d'audit. | 2 | Audit planifié |
| | R7 | Veiller aux clauses relatives à la sécurité des contrats que l'autorité administrative passe avec des prestataires chargés de les assister dans leur démarche de sécurisation de leurs systèmes. | 0 | Non commencé |
| | R8 | Sensibiliser le personnel aux questions de sécurité, ainsi que former ceux qui interviennent plus spécifiquement dans la mise en œuvre et le suivi opérationnel de la sécurité du système d'information (surveillance, détection, prévention). | 2 | Plan de sensibilisation en cours de validation DRH |

Exemple de socle de sécurité

Activité 1-4



Société de biotechnologies – Déterminer le socle de sécurité

| Quels sont les référentiels qui s'appliquent à la société de biotechnologies ? | Oui | Non |
|--|-----|-----|
| 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) | | |
| Référentiel Général de Sécurité (RGS) | | |

Exemple de socle de sécurité

Activité 1-4



Société de biotechnologies – Déterminer le socle de sécurité

| Quels sont les référentiels qui s'appliquent à la société de biotechnologies ? | Oui | Non |
|--|-------------------------------------|-------------------------------------|
| Politique de sécurité (PSSI) de l'organisation | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Règlement européen de protection des données (RGPD) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Guide d'hygiène informatique | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Annexe A de l'ISO 27001 | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Code de la santé publique | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Arrêté sectoriel « produits de santé » (Loi de programmation militaire) | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Instruction générale interministérielle 1300 (IGI 1300) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Référentiel Général de Sécurité (RGS) | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

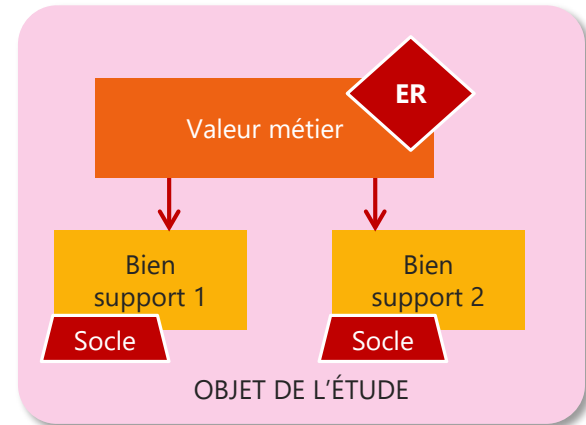
Comment constituer les scénarios de risques ?

Fin de l'atelier 1

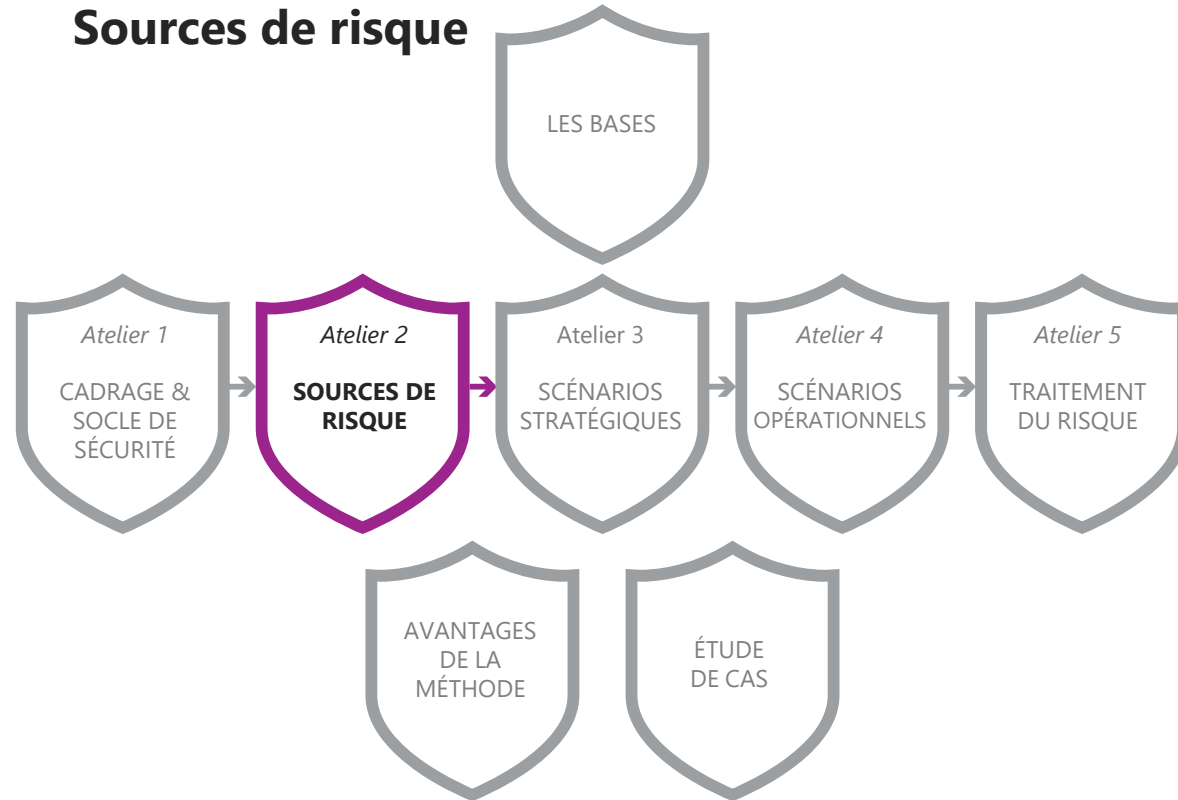
Légende

Socle = Socle de sécurité, liste des référentiels applicables, état d'application, identification des écarts et leurs justifications

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



Atelier 2 Sources de risque



Sources de risque

Atelier 2



Objectif

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



Participants

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

Éléments en entrée

- Valeurs métier atelier 1
- Événements redoutés atelier 1

ATELIER 2 SOURCES DE RISQUE

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.



Sources de risque

Atelier 2



Activité 1

**Identifier les sources
de risque et objectifs visés**



Activité 2

Évaluer les couples SR/OV



Activité 3

Sélectionner les couples SR/OV

Comment identifier des sources de risque et objectifs visés

Activité 2-1 • Les questions à se poser

Quels sont les objectifs visés (OV) par chaque source de risque en termes d'effets recherchés ?

Quelles sont les caractéristiques des couples SR/OV? (e.g. motivation, activité connue ressources...)

Quelles sont les sources de risque (SR) susceptibles de porter atteinte aux missions de l'organisation ou à des intérêts supérieurs?

Quels sont les couples SR/OV les plus pertinents ?



Etat de la menace, quelques tendances



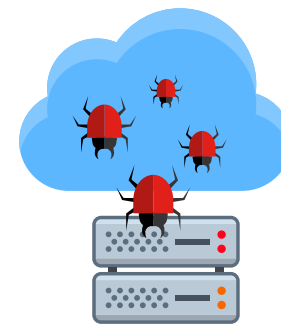
Des acteurs offensifs aux capacités en constante progression

- Cybercriminalité,
- Acteurs étatiques,
- Capacités privées.



Des intentions d'espionnage et de sabotage peu visibles, mais toujours préoccupantes

- Espionnage,
- Ciblage d'infrastructures critiques,
- Opérations d'influence et de déstabilisation.



De nombreuses faiblesses exploitées

- Exploitation massive de vulnérabilités ,
- Cloud,
- Chaîne d'approvisionnement,
- Faible sécurisation des données.

Comment identifier des sources de risque et objectifs visés

Activité 2-1

Sources de
risque (SR)



Etatique



Crime
organisé



Terroriste



Activiste



Amateur



Concurrent



Vengeur

Comment identifier des sources de risque et objectifs visés

Activité 2-1

Sources de risque (SR)



Etatique



Crime
organisé



Terroriste



Activiste



Amateur



Concurrent



Vengeur

Objectifs visés (OV)



Espionnage



Pré-
positionnement



Influence
déstabilisation



Entrave au
fonctionnement



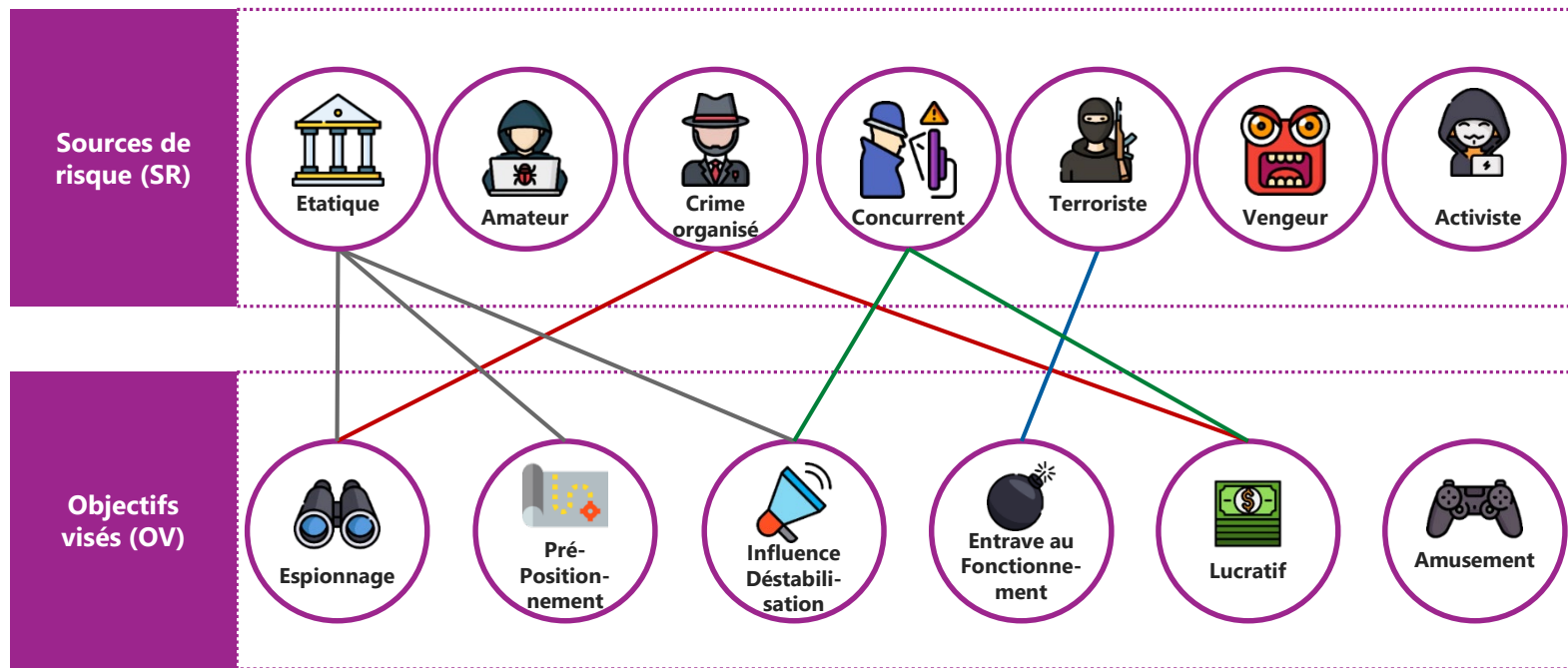
Lucratif



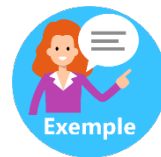
Amusement

Comment identifier des sources de risque et objectifs visés

Activité 2-1



Récapitulons le vocabulaire que nous avons vu



Activité 2-1

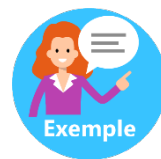
Un adolescent de 15 ans « pirate » le système de son collègue pour améliorer ses notes

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. [...]

[Sources Internet : Le Point.fr et ZDNet]

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

Récapitulons le vocabulaire que nous avons vu



Activité 2-1

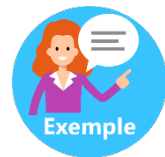
Un adolescent de 15 ans « pirate » le système de son collègue pour améliorer ses notes

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. [...]

[Sources Internet : Le Point.fr et ZDNet]

| | 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 | |
| Impacts | <ul style="list-style-type: none">• Impact sur la poursuite d'études des collégiens• Impact d'image vis-à-vis des autres établissements scolaires | |
| Source de risque | Adolescent | |
| Objectif visé | Modifier ses résultats scolaires | |

Récapitulons le vocabulaire que nous avons vu



Activité 2-1

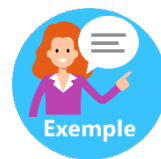
Un adolescent de 15 ans « pirate » le système de son collègue pour améliorer ses notes

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. 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 |
|--------------------------|--|-----------------|
| 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 | |
| Impacts | <ul style="list-style-type: none">• Impact sur la poursuite d'études des collégiens• Impact d'image vis-à-vis des autres établissements scolaires | |
| Source de risque | Adolescent | |
| Objectif visé | Modifier ses résultats scolaires | |

Récapitulons le vocabulaire que nous avons vu



Activité 2-1

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. 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 |
|--------------------------|---|---|
| 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 |
| Impacts | <ul style="list-style-type: none"> Impact sur la poursuite d'études des collégiens Impact d'image vis-à-vis des autres établissements scolaires | Impact d'image vis-à-vis des familles Impact sur les missions et services du collège |
| Source de risque | Adolescent | Adolescent |
| Objectif visé | Modifier ses résultats scolaires | Se venger du collègue |

Évaluer les couples SR/OV

Activité 2-2 • Les questions à se poser

Quels sont les objectifs visés (OV) par chaque source de risque en termes d'effets recherchés ?

Quelles sont les caractéristiques des couples SR/OV? (e.g. motivation, activité connue ressources...)

Quelles sont les sources de risque (SR) susceptibles de porter atteinte aux missions de l'organisation ou à des intérêts supérieurs?

Quels sont les couples SR/OV les plus pertinents ?



Évaluer les couples SR/OV

Activité 2-2

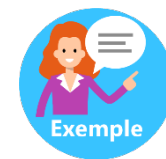
Comment caractériser les couples SR/OV ?

- Retours d'expérience des participants, jugement d'experts...
- Métriques de caractérisation
- Les métriques retenus :
 - Motivation
 - Ressources
 - Activité (optionnelle)



Évaluer les couples SR/OV

Activité 2-2 • Exemple du collégien



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. [...]

[Sources Internet : Le Point.fr et ZDNet]

| | 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 |
| Impacts | <ul style="list-style-type: none">• Impact sur la poursuite d'études des collégiens• Impact d'image vis-à-vis des autres établissements scolaires |
| Source de risque | Adolescent |
| Objectif visé | Modifier ses résultats scolaires |
| Motivation | |
| Ressources | |
| Activité | |

Évaluer les couples SR/OV

Activité 2-2 • Exemple du collégien



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. [...]

[Sources Internet : Le Point.fr et ZDNet]

| | 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 |
| Impacts | <ul style="list-style-type: none">• Impact sur la poursuite d'études des collégiens• Impact d'image vis-à-vis des autres établissements scolaires |
| Source de risque | Adolescent |
| Objectif visé | Modifier ses résultats scolaires |
| Motivation | Forte motivation pour permettre son passage |
| Ressources | Accès à un simple ordinateur |
| Activité | Non évaluée |

Sélectionner les couples SR/OV

Activité 2-3 • Les questions à se poser

Quels sont les objectifs visés (OV) par chaque source de risque en termes d'effets recherchés ?

Quelles sont les caractéristiques des couples SR/OV? (e.g. motivation, activité connue ressources...)

Quelles sont les sources de risque (SR) susceptibles de porter atteinte aux missions de l'organisation ou à des intérêts supérieurs?

Quels sont les couples SR/OV les plus pertinents ?



Évaluer les couples SR/OV

Activité 2-3

| | | RESSOURCES | | | | |
|---|---------------|---|---------------------------|------------------------|-----------------------|------------------|
| | | Incluant les ressources financières, le niveau de compétences cyber, l'outillage, le temps dont l'attaquant dispose pour réaliser l'attaque, etc. | | | | |
| MOTIVATION Intérêts, éléments qui poussent la source de risque à atteindre son objectif | | Ressources limitées | Ressources significatives | Ressources importantes | Ressources illimitées | |
| | | 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



Activité 2-3

| Sources de risque | Objectifs visés | Motivation | Ressources | Pertinence |
|-------------------|---|------------|---------------------------|------------------------------|
| Activiste | Divulguer des informations sur les tests animaliers | Peu motivé | Ressources significatives | Moyennement pertinent |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Sélectionner les couples SR/OV

Activité 2-3



| Sources de risque | Objectifs visés | Motivation | Ressources | Pertinence |
|----------------------|---|------------|---------------------------|------------------------------|
| Activiste | Divulguer des informations sur les tests animaliers | Peu motivé | Ressources significatives | Moyennement pertinent |
| Activiste | Saboter la campagne nationale de vaccination | | | |
| Concurrent | Voler des informations | | | |
| Cybercriminel | Menace d'altération de la composition des vaccins à des fins d'extorsion d'une rançon | | | |

Sélectionner les couples SR/OV

Activité 2-3



| Sources de risque | Objectifs visés | Motivation | Ressources | Pertinence |
|-----------------------|---|------------------|---------------------------|------------------------------|
| Activiste | Divulguer des informations sur les tests animaliers | Peu motivé | Ressources significatives | Moyennement pertinent |
| Activiste | Saboter la campagne nationale de vaccination | Assez motivé | Ressources significatives | |
| Concurrent | Voler des informations | Fortement motivé | Ressources importantes | |
| Cyber-criminel | Menace d'altération de la composition des vaccins à des fins d'extorsion d'une rançon | Peu motivé | Ressources limitées | |

Sélectionner les couples SR/OV

Activité 2-3



| Sources de risque | Objectifs visés | Motivation | Ressources | Pertinence |
|-----------------------|---|------------------|---------------------------|------------------------------|
| Activiste | Divulguer des informations sur les tests animaliers | Peu motivé | Ressources significatives | Moyennement pertinent |
| Activiste | Saboter la campagne nationale de vaccination | Assez motivé | Ressources significatives | Plutôt pertinent |
| Concurrent | Voler des informations | Fortement motivé | Ressources importantes | Très pertinent |
| Cyber-criminel | Menace d'altération de la composition des vaccins à des fins d'extorsion d'une rançon | 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.

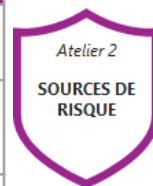
Confrontation des deux points de vue

Activité 2-3



| ER les plus graves | | |
|-------------------------|---|---------|
| Valeur métier | Événement redouté | Gravité |
| Fabriquer des vaccins | Interruption de la production ou de la distribution de vaccins pendant plus d'une semaine pendant un pic d'épidémie | 4 |
| Traçabilité et contrôle | Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire | 4 |
| R&D | Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée | 3 |
| R&D | Fuite des informations d'études et recherches de l'entreprise | 3 |

| SR/OV les plus pertinents | |
|---------------------------|--|
| Sources de risque | Objectif visé |
| Concurrent | Voler des informations |
| Activiste | Saboter la campagne nationale de vaccination |



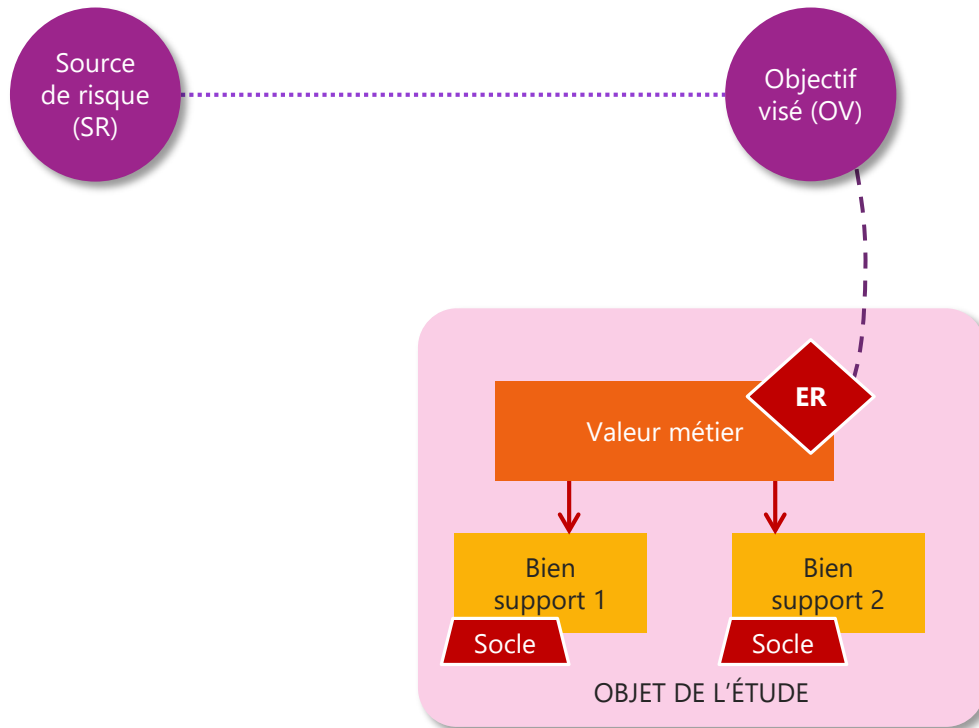
Quelle gravité pour mon scénario stratégique ?

Fin de l'atelier 2

Légende

Socle = Socle de sécurité, liste des référentiels applicables, état d'application, identification des écarts et leurs justifications

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



Quelques exemples pour mémoriser le vocabulaire EBIOS Risk Manager



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

[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 | |

Quelques exemples pour mémoriser le vocabulaire EBIOS Risk Manager



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

[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 chaine 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) |

Quelques exemples pour mémoriser le vocabulaire EBIOS Risk Manager



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

Source : Next impact – 12/11/2018

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

Quelques exemples pour mémoriser le vocabulaire EBIOS Risk Manager



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

Source : Next impact – 12/11/2018

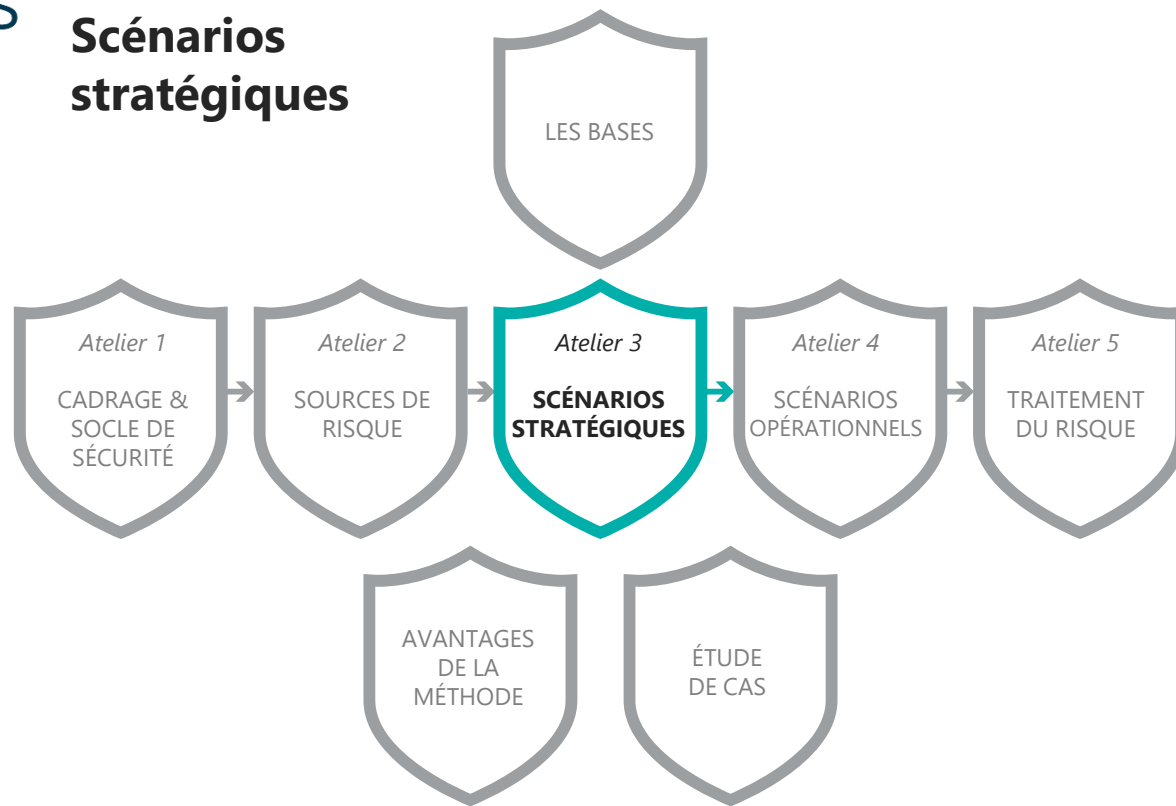
Des escrocs sont parvenus à convaincre l'ancien directeur financier de Pathé Pays-Bas que la direction de Pathé lui ordonnait de verser d'importantes sommes sur un compte tiers pour financer une acquisition à Dubaï.

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 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 |

Atelier 3 Scénarios stratégiques



Scénarios stratégiques

Atelier 3



Objectif

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



Participants

Métiers, Architectes fonctionnels, Juristes, RSSI, Spécialiste cybersécurité.

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)

ATELIER 3 SCÉNARIOS STRATÉGIQUES

Éléments en sortie

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



Scénarios stratégiques

Atelier 3

- **Activité 1**
Cartographier l'écosystème
- **Activité 2**
Élaborer les scénarios stratégiques
- **Activité 3**
Définir les mesures de sécurité sur l'écosystème

Cartographier l'écosystème

Atelier 3-1 • Les questions à se poser

Quelles sont les **parties prenantes critiques (PPC)** (i.e. les maillons faibles de l'écosystème disposant d'un accès privilégié aux valeurs métier) ?

Quels sont les scénarios stratégiques, i.e. ensembles de chemins d'attaque allant d'une source de risques à un objectif visé ?
L'attaquant est-il susceptible de passer par une PPC ?

Quelles sont les **parties prenantes** (i.e. acteurs humains ou informatiques en interaction avec l'objet de l'étude) qui forment l'écosystème ?

Quelles mesures de sécurité peut-on appliquer aux parties prenantes critiques ?



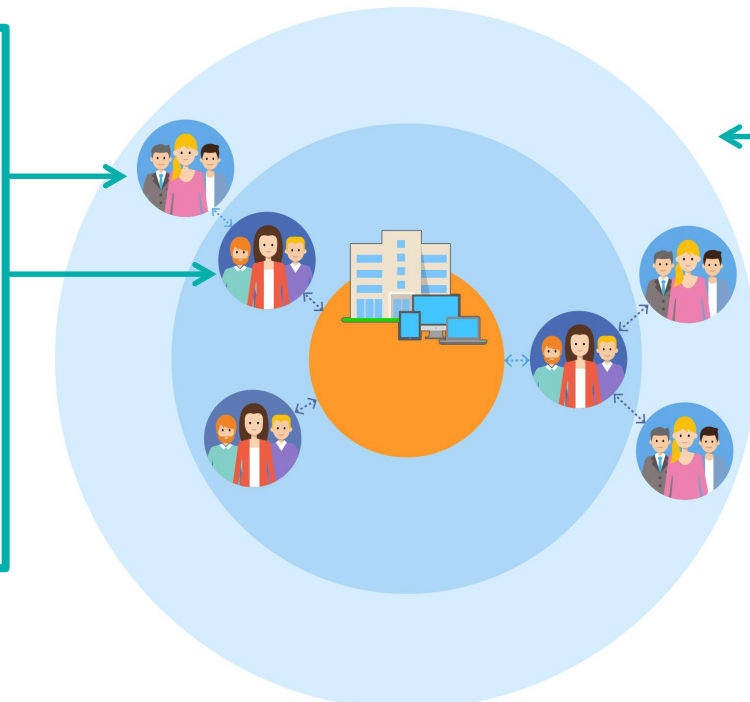
Définitions

Atelier 3-1

Qu'est-ce qu'une partie prenante ?

A ce stade, on considère l'objet de l'étude comme une boîte noire. Tout ce qui interagit avec cette boîte noire est une partie prenante.

Les parties prenantes sont les **éléments dont la sécurité ne dépend pas directement du commanditaire du système étudié.**

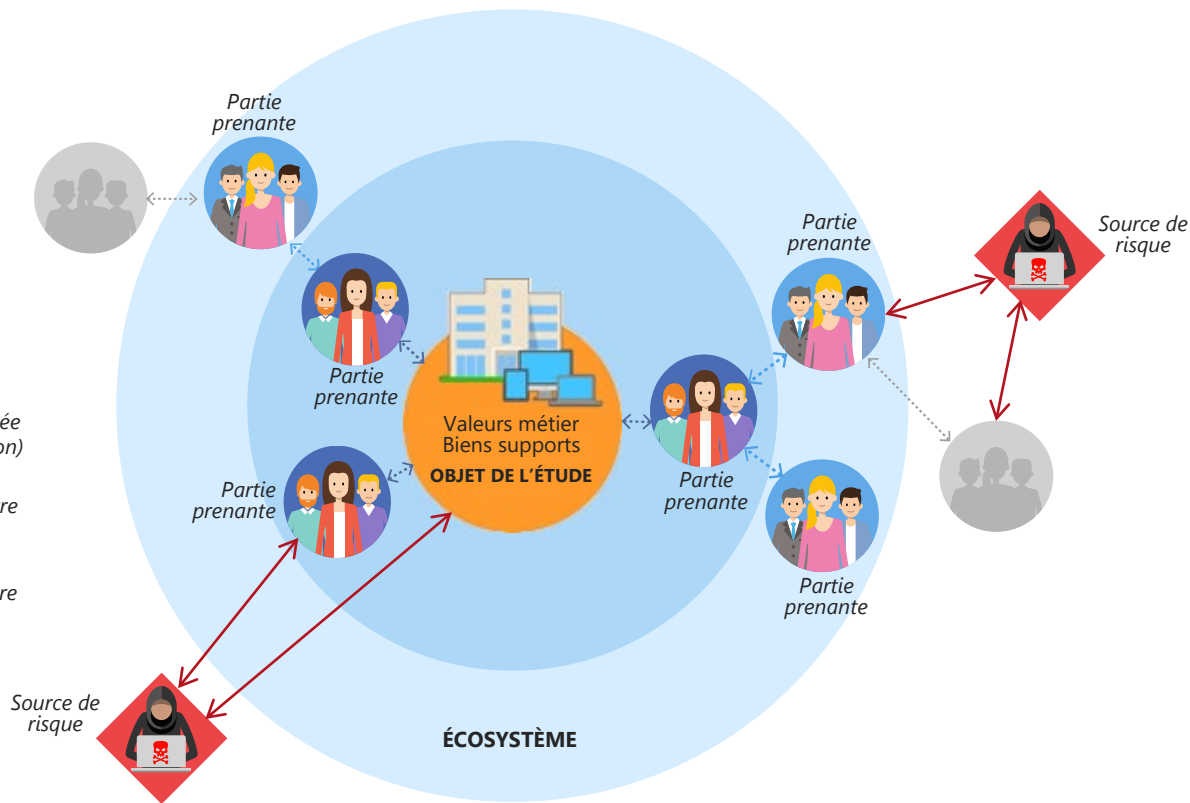


Qu'est-ce que l'écosystème ?

L'écosystème comprend l'ensemble des parties prenantes qui gravitent autour de l'objet de l'étude et concourent à la réalisation de ses missions (partenaires, sous-traitants, filiales, etc.).

Cartographier l'écosystème

Atelier 3-1 • Identifier les parties prenantes de l'écosystème



Légende



Partie prenante directement reliée au système (1^{er} niveau de relation)



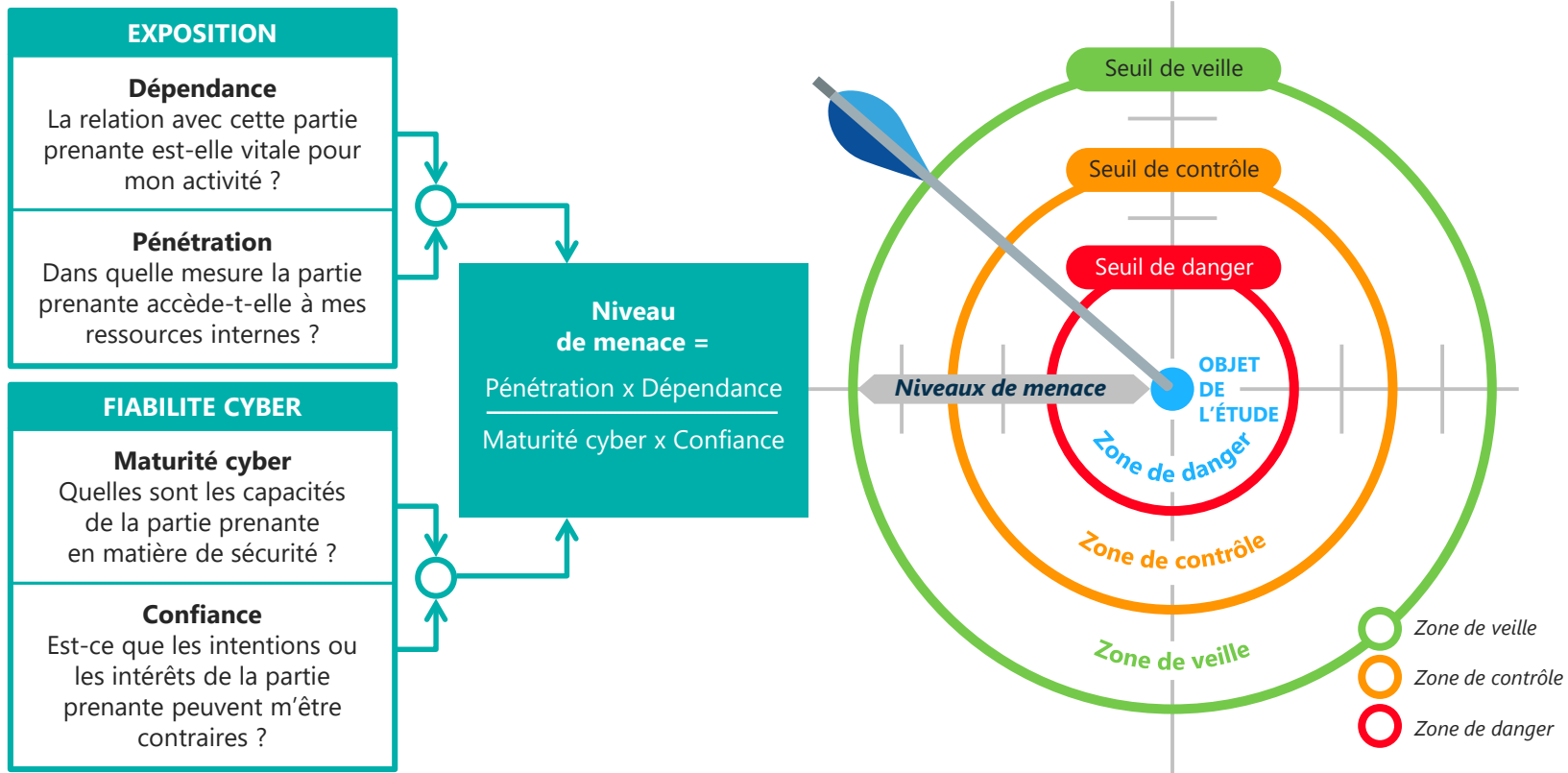
Partie prenante reliée à une autre partie prenante (2^{ème} niveau de relation)



Partie prenante reliée à une autre partie prenante (3^{ème} niveau de relation ou plus)

Cartographier l'écosystème

Atelier 3-1 • Evaluer et cartographier la criticité des parties prenantes



Cartographier l'écosystème

Atelier 3-1 • Critères de cotation des parties prenantes vis-à-vis du système

| | 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 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 | 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 | 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 | 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, switches, 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. |

Cartographier l'écosystème

Atelier 3-1 • Critères de cotation des parties prenantes vis-à-vis du système

| | DÉPENDANCE | PÉNÉTRATION | MATURITÉ CYBER | CONFIANCE |
|---|--|---|---|---|
| 1 | Pas de lien avec le SI de la partie prenante pour réaliser la mission. | Accès ou accès avec des privilèges de type administrateur à des terminaux utilisateurs (poste de travail, téléphone, 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 privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de téléphones, etc.) ou accès physique aux équipements. | Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité n'est assurée selon un mode réactif. | Les intentions de la partie prenante sont connues mais pas positives. |
| 3 | 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.). | La 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 privilèges de type administrateur à des équipements d'infrastructure (annuaire d'entreprise, DNS, DHCP, switches, 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 gestion 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. |

DÉPENDANCE

PÉNÉTRATION

MATURITÉ CYBER

CONFIANCE

EXPOSITION

FIABILITE CYBER

MENACE CYBER

Cartographier l'écosystème

Atelier 3-1 • Exemple du collégien

Description des Parties Prenantes



Professeurs

Fournissent des informations sur leur matières (sorties, devoirs à faire, livres à apporter...), renseignent les notes des élèves, etc.



Administration

Fournissent des informations générales, notifie les absences, compile les notes, etc.



Collégiens

Consultent les instructions de leurs professeurs, consultent leurs notes, échanges entre eux, etc.



Parents d'élèves

Consultent les informations générales, consultent les notes de leurs enfants, interagissent avec les professeurs ou l'administration, etc.

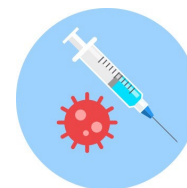
Cartographier l'écosystème

Atelier 3-1 • Exemple du collégien

| Parties- prenantes | Dépendance | Pénétration | Maturité Cyber | Confiance | Criticité |
|------------------------|---|--|--|---|-------------|
| Professeur (P1) | 3 Assure la saisie des notes | 1 Droits simples d'utilisateur, en écriture sur toutes les notes | 1 Aucune | 4 Membre de l'éducation nationale | 0,75 |
| Administration (P2) | 4 Compilation | 2 Accès privilégié pour gérer les informations de l'élève | 2 A suivi une formation et une sensibilisation obligatoire | 4 Membre de l'éducation nationale | 1 |
| Collégien (P3) | 1 | 1 Droits simples d'utilisateur | 1 Aucune | 1 Intention inconnue | 1 |
| Parents (P4) | 1 | 1 Droits simples d'utilisateur | 1 Aucune | 1 Intention inconnue | 1 |

Cas fictif • Société de biotechnologies

Atelier 3-1 • Evaluer la criticité des parties prenantes



Société de biotechnologie fabricant des vaccins

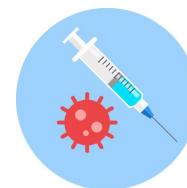
| Catégorie | Nom | Dépendance | Pénétration | Maturité cyber | Confiance | Niveau de menace |
|-------------|--|------------|-------------|----------------|-----------|------------------|
| Client | C1 - Établissements de santé | 1 | 1 | 1 | 3 | 0,3 |
| Client | C2 - Pharmacies | 1 | 1 | 2 | 3 | 0,2 |
| 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 | | | | | |
| Prestataire | F2 - Fournisseurs de matériel (chaîne de production) | | | | | |
| Prestataire | F3 - Prestataire informatique | | | | | |

EXPOSITION

FIABILITE CYBER

Cas fictif • Société de biotechnologies

Atelier 3-1 • Evaluer la criticité des parties prenantes



Société de biotechnologie fabricant des vaccins

| 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 |

EXPOSITION

FIABILITE CYBER

Construire la cartographie de menace de l'écosystème

Atelier 3-1



CLIENTS

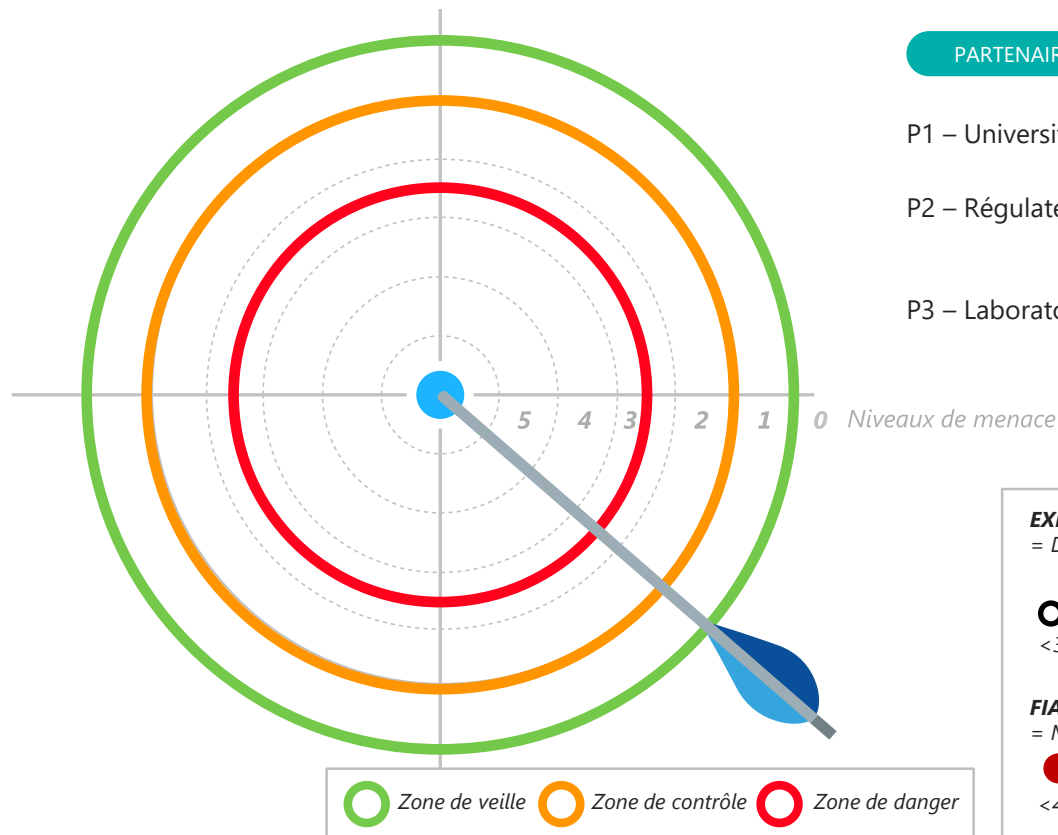
- C1 • Etablissements de santé
- C2 • Pharmacies
- C3 • Dépositaires & Grossistes répartiteurs

PRESTATAIRES

- F3 • Prestataire informatique
- F2 • Fournisseurs de matériel
- F1 • Fournisseurs industriels chimistes

PARTENAIRES

- P1 – Universités
- P2 – Régulateurs
- P3 – Laboratoires



EXPOSITION

= Dépendance x Pénétration



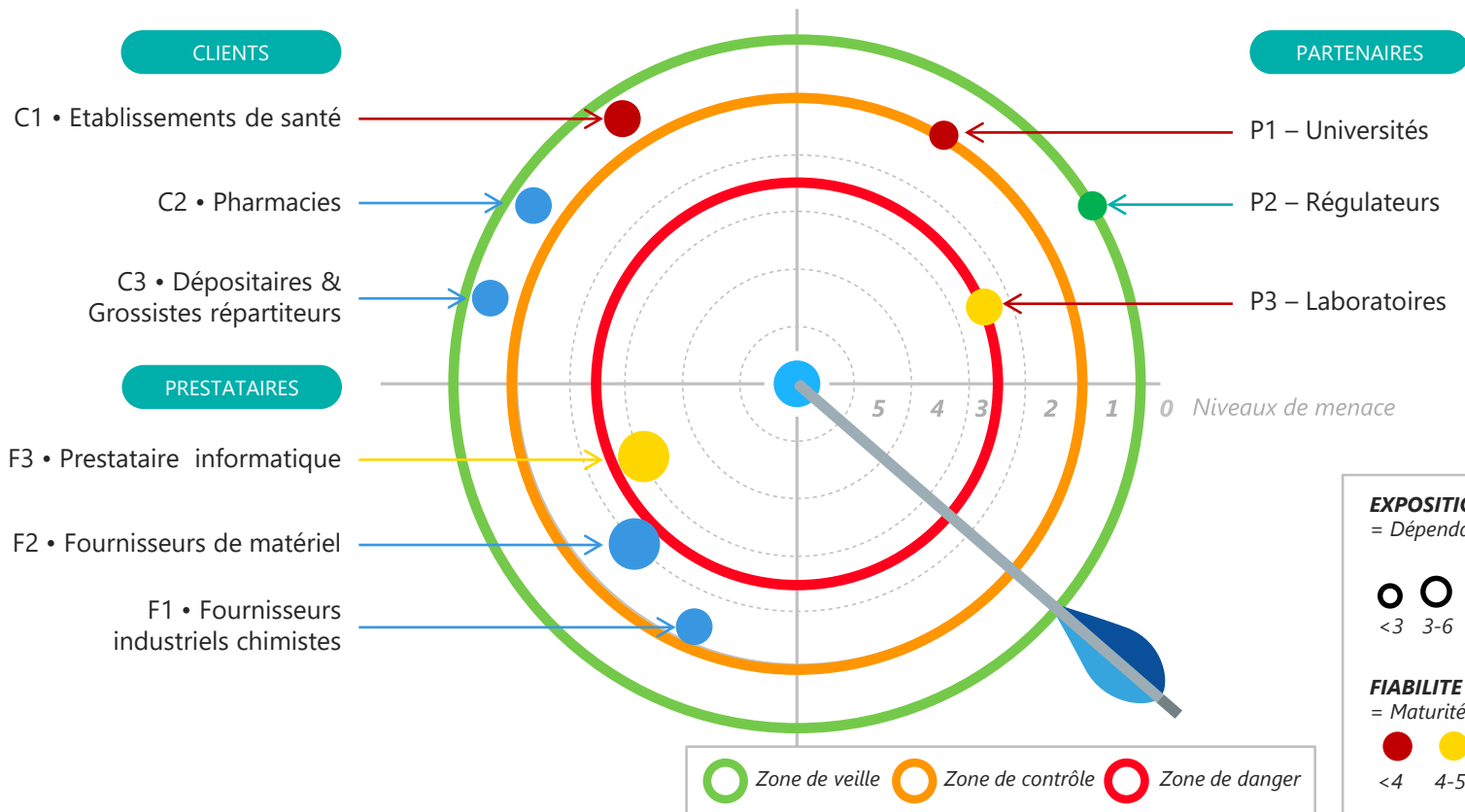
FIABILITE CYBER

= Maturité cyber x Confiance



Construire la cartographie de menace de l'écosystème

Atelier 3-1



Élaborer les scénarios stratégiques (point de vue de l'attaquant)

Atelier 3-2 • Les questions à se poser

Quelles sont les parties prenantes critiques (PPC) (i.e. les maillons faibles de l'écosystème disposant d'un accès privilégié aux valeurs métier) ?

Quels sont les **scénarios stratégiques**, i.e. ensembles de **chemins d'attaque** allant d'une **source de risques** à un **objectif visé** ? L'attaquant est-il susceptible de passer par une **PPC** ?

Quelles sont les parties prenantes (i.e. acteurs humains ou informatiques en interaction avec l'objet de l'étude) qui forment l'écosystème ?

Quelles mesures de sécurité peut-on appliquer aux parties prenantes critiques ?



Élaborer les scénarios stratégiques (point de vue de l'attaquant)

Atelier 3-2 • La démarche

Créer un **scénario stratégique** par couple SR/OV

Décrire les **chemins d'attaque** (i.e. séquencements possibles des événements, dont événements intermédiaires portant sur l'écosystème)

Mettre en exergue les atteintes aux valeurs métier (i.e. **événements redoutés**)

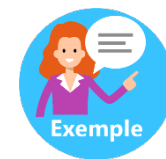
En déduire la **gravité** du scénario stratégique

Trucs et astuces

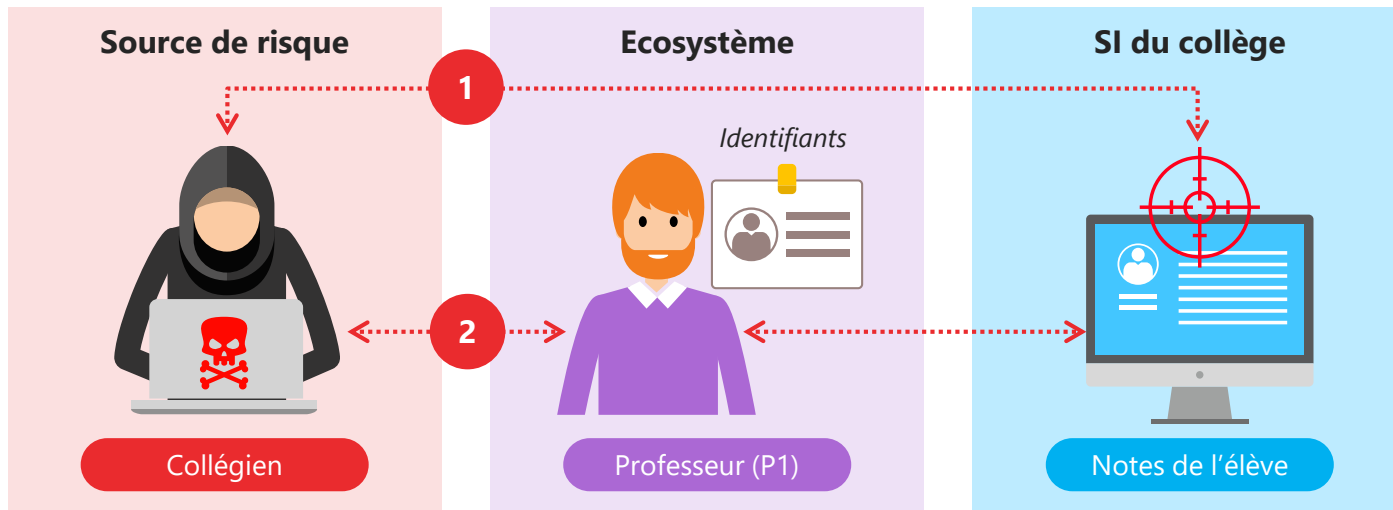
- Si un SR/OV mène à plusieurs ER, retenir la gravité la plus forte
- Il existe trois types de chemins d'attaque
 - Direct sur l'objet de l'étude
 - Par rebond, via l'écosystème
 - Visant exclusivement l'écosystème

Élaborer les scénarios stratégiques

Atelier 3-2 • Exemple du collégien



Source de risque : Collégien
Objectif visé : Modifier ses notes
Événement redouté : Les résultats scolaires
d'un ou plusieurs collégiens sont erronés



Élaborer les scénarios stratégiques

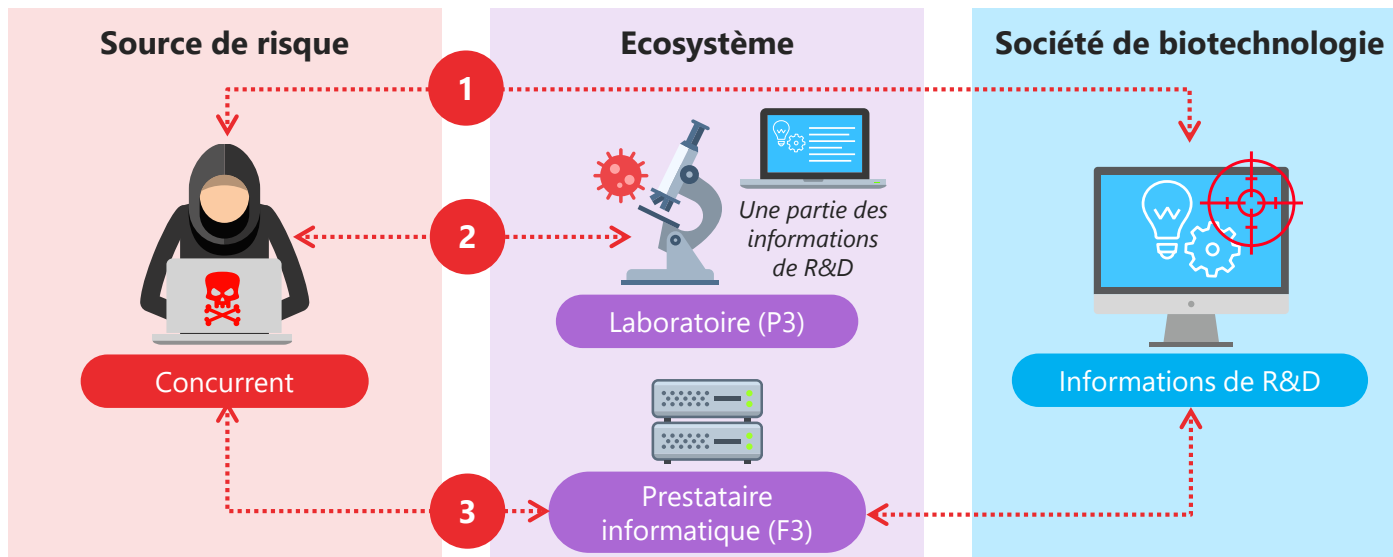
Atelier 3-2 • Exemple de la société de biotechnologies



Source de risque : Concurrent
Objectif visé : Voler des informations
Événement redouté : Fuite des informations
d'études et recherches de l'entreprise



Un scénario stratégique
constitué de 3 chemins
d'attaque



Élaborer les scénarios stratégiques

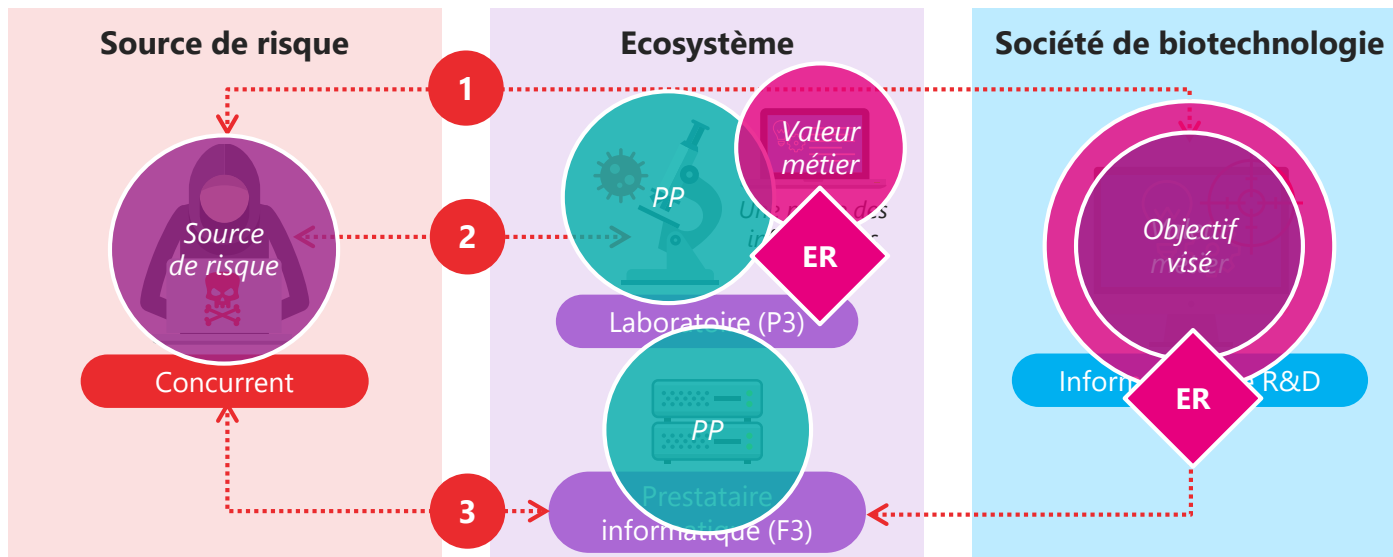
Atelier 3-2 • Exemple de la société de biotechnologies



Source de risque : Concurrent
Objectif visé : Voler des informations
Événement redouté : Fuite des informations d'études et recherches de l'entreprise



Un scénario stratégique
constitué de 3 chemins
d'attaque



Déterminer le socle de sécurité

Atelier 3-3 • Les questions à se poser

Quelles sont les parties prenantes critiques (PPC) (i.e. les maillons faibles de l'écosystème disposant d'un accès privilégié aux valeurs métier) ?

Quels sont les scénarios stratégiques, i.e. ensembles de chemins d'attaque allant d'une source de risques à un objectif visé ? L'attaquant est-il susceptible de passer par une PPC ?

Quelles sont les parties prenantes (i.e. acteurs humains ou informatiques en interaction avec l'objet de l'étude) qui forment l'écosystème ?

Quelles **mesures de sécurité** peut-on appliquer aux **parties prenantes critiques** ?

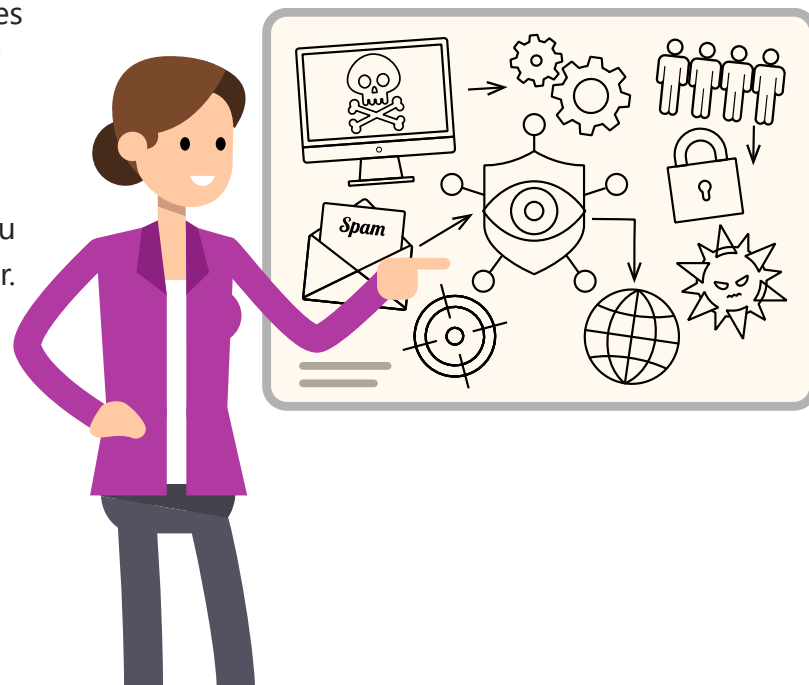


Définir les mesures de sécurité sur l'écosystème

Atelier 3-3

Réfléchir aux mesures de sécurité

- Importance de réfléchir **aux mesures de sécurité** que l'on peut proposer aux parties prenantes les plus à risque afin de réduire leur niveau de menace.
- Elles peuvent participer :
 - à la réduction de leur exposition, et/ou
 - à l'augmentation de leur fiabilité cyber.



Définir les mesures de sécurité sur l'écosystème

Atelier 3-3

Exemple du collégien (rappel)

| Partie prenante | Dépendance | Pénétration | Maturité Cyber | Confiance | Criticité |
|-----------------|--|--|--------------------|---|-------------|
| Professeur (P1) | 3 Assure la saisie des notes | 1 Droits simples d'utilisateur, en écriture sur toutes les notes | 1 Aucune | 4 Membre de l'éducation nationale | 0,75 |

Décision : Afin de limiter la criticité du professeur, il faut baisser son niveau d'exposition et d'augmenter son niveau de fiabilité cyber.

| Partie prenante | Chemin d'attaque stratégique | Mesure de sécurité | Criticité initiale | Criticité résiduelle |
|-----------------|------------------------------|---|--------------------|----------------------|
| Professeur (P1) | 3 | <p>Pénétration (1→1) Limiter les droits en édition aux seuls élèves du professeur et dans la matière qu'il enseigne</p> <p>Maturité Cyber (1→2) Sensibiliser régulièrement sur l'hygiène informatique et l'ingénierie sociale</p> | 1,5 | 0,375 |

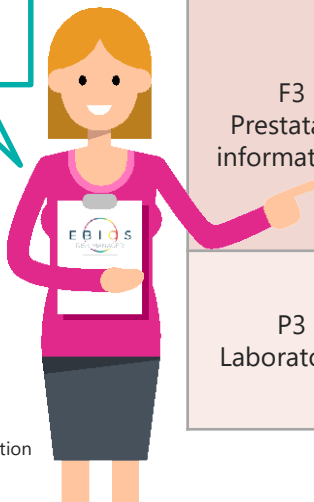
Cas fictif • Société de biotechnologies

Atelier 3-3 • Définir les mesures de sécurité sur l'écosystème



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 est l'efficacité de ces mesures ?



| Partie prenante | Chemin d'attaque stratégique | Mesures de sécurité | Menace initiale | Menace 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 | |

Comment constituer les scénarios de risques ?

Fin de l'atelier 3

Légende

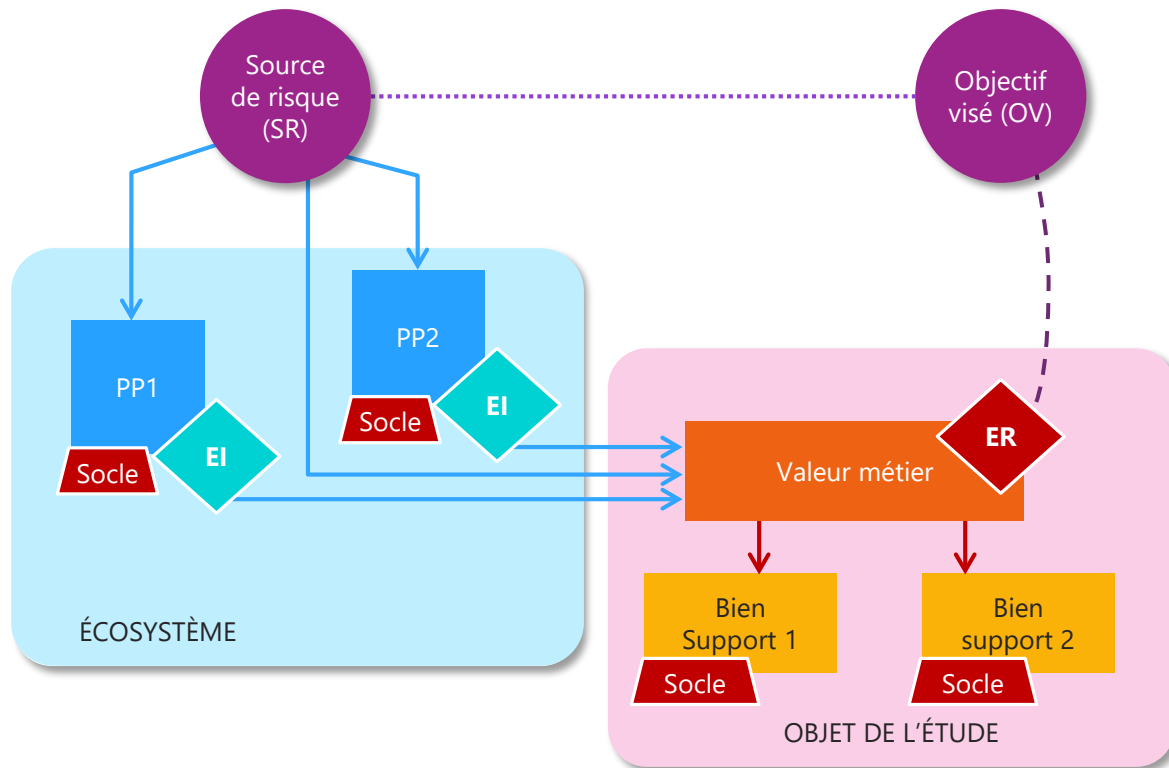
Socle = Socle de sécurité, liste des référentiels applicables, état d'application, identification des écarts et leurs justifications

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

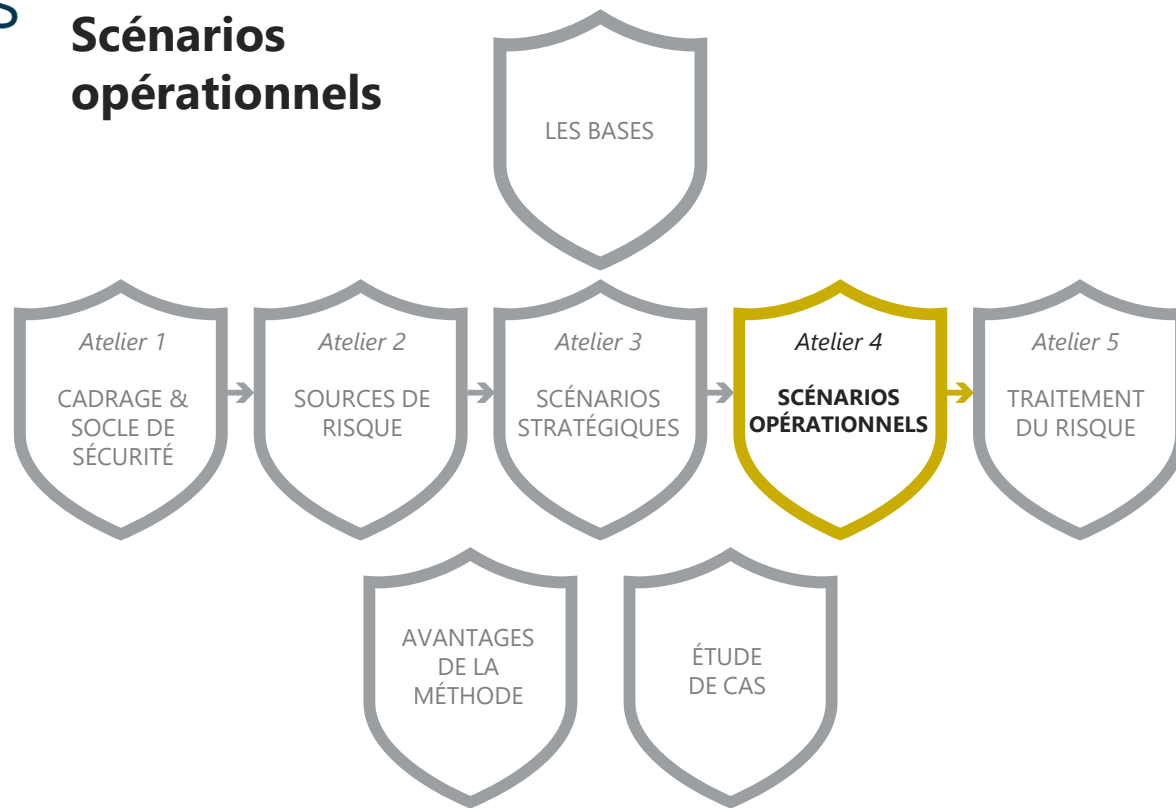
PP = Partie prenante de l'écosystème

→ Chemin d'attaque d'un scénario stratégique

EI = Événement intermédiaire associé à une valeur métier de l'écosystème



Atelier 4 Scénarios opérationnels





Scénarios opérationnels

Atelier 4



Objectif

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



Participants

RSSI, DSI, Architectes SI, (Spécialiste cybersécurité).

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)

ATELIER 4
SCÉNARIOS
OPÉRATIONNELS

Éléments en sortie

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



Scénarios opérationnels

Atelier 4



Activité 1

Elaborer les scénarios opérationnels



Activité 2

**Evaluer la vraisemblance des scénarios
opérationnel**

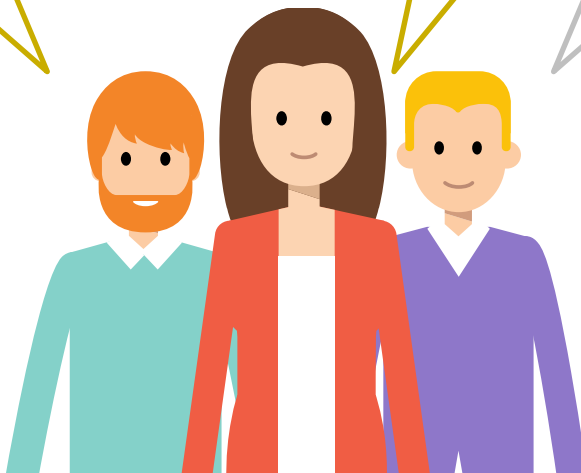
Elaborer les scénarios opérationnels

Activité 4-1 • Les questions à se poser

Quelles sont les **scénarios opérationnels** schématisant les **modes opératoires techniques** qui seront mis en œuvre lors de l'attaque ?

Quelles sont les **biens supports critiques** susceptibles de servir de vecteur d'entrée ?

Quelle est la vraisemblance du scénario opérationnel ?



Des scénarios structurés selon une séquence d'attaque type

Activité 4-1



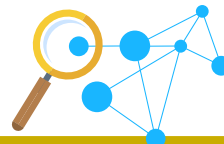
Connaître

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.

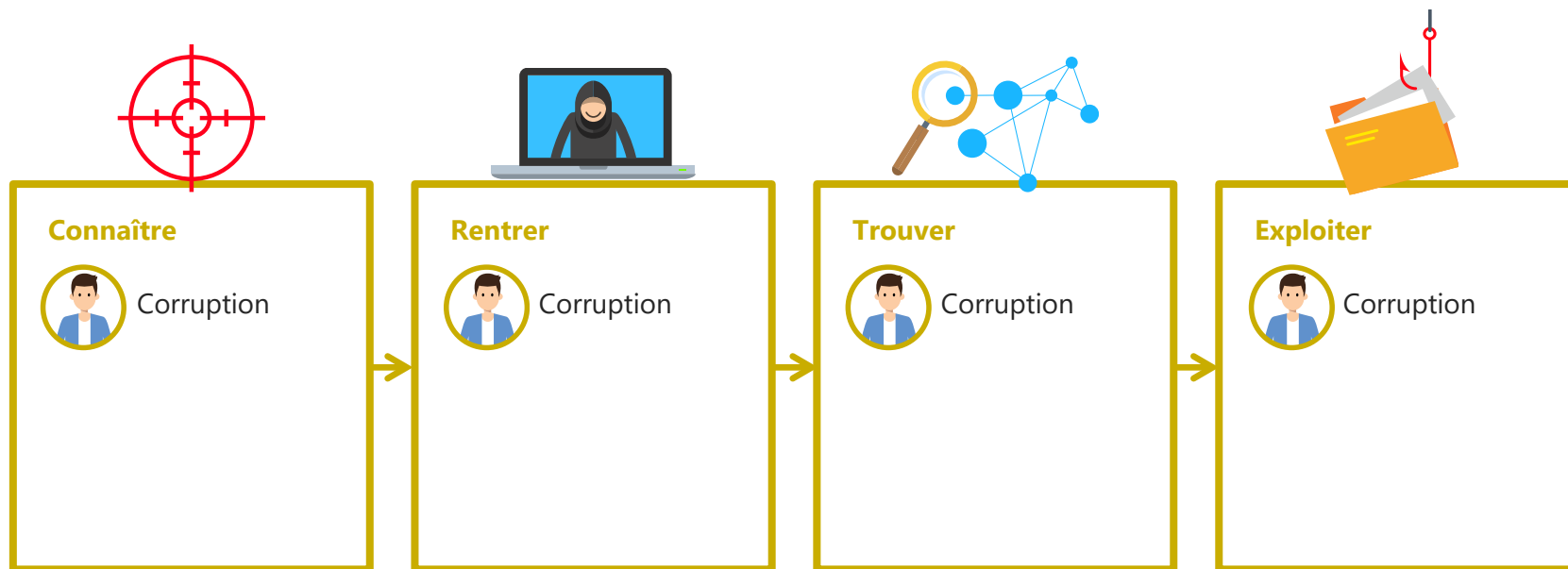


Exploiter

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

Des scénarios structurés selon une séquence d'attaque type

Activité 4-1

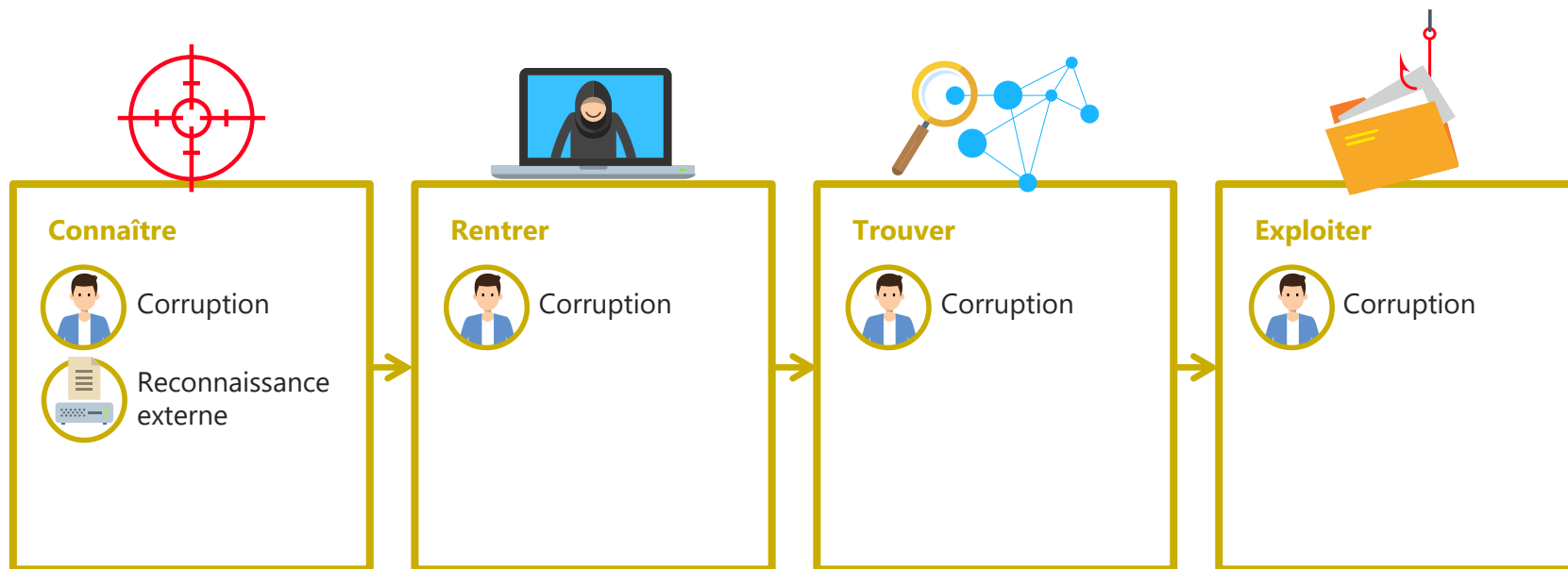


Recrutement d'une source, corruption de personnel.

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).

Des scénarios structurés selon une séquence d'attaque type

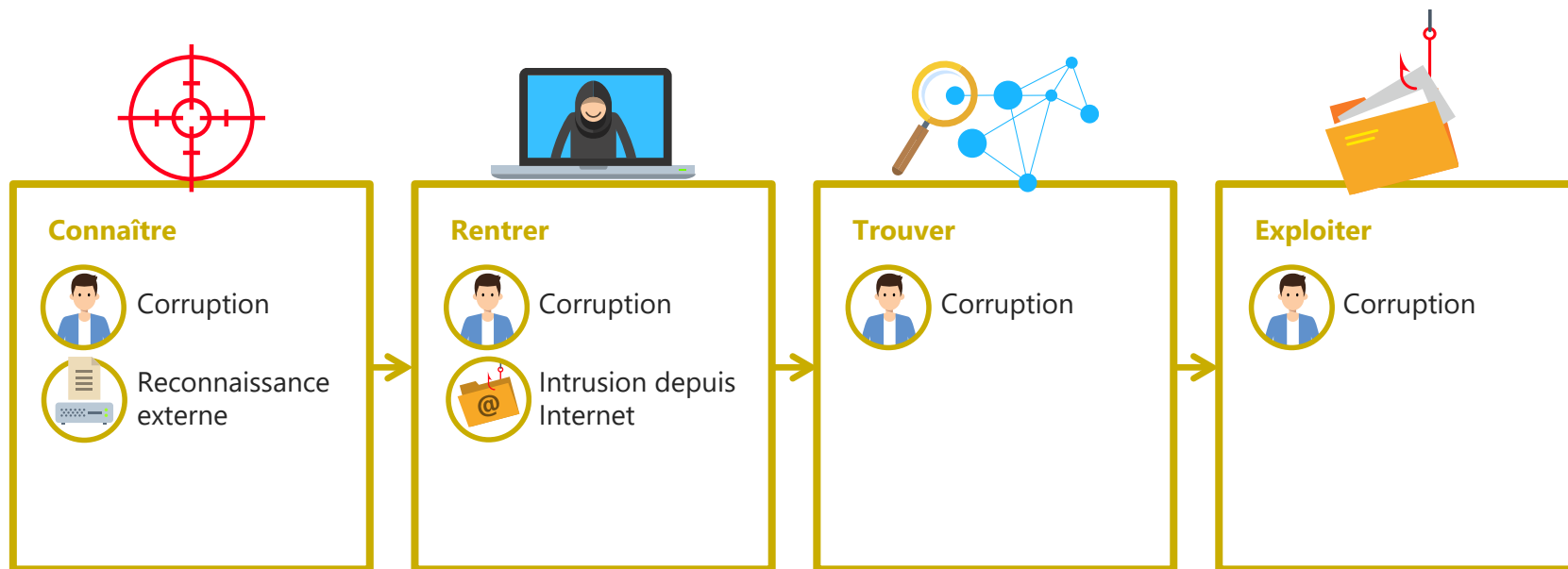
Activité 4-1



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.

Des scénarios structurés selon une séquence d'attaque type

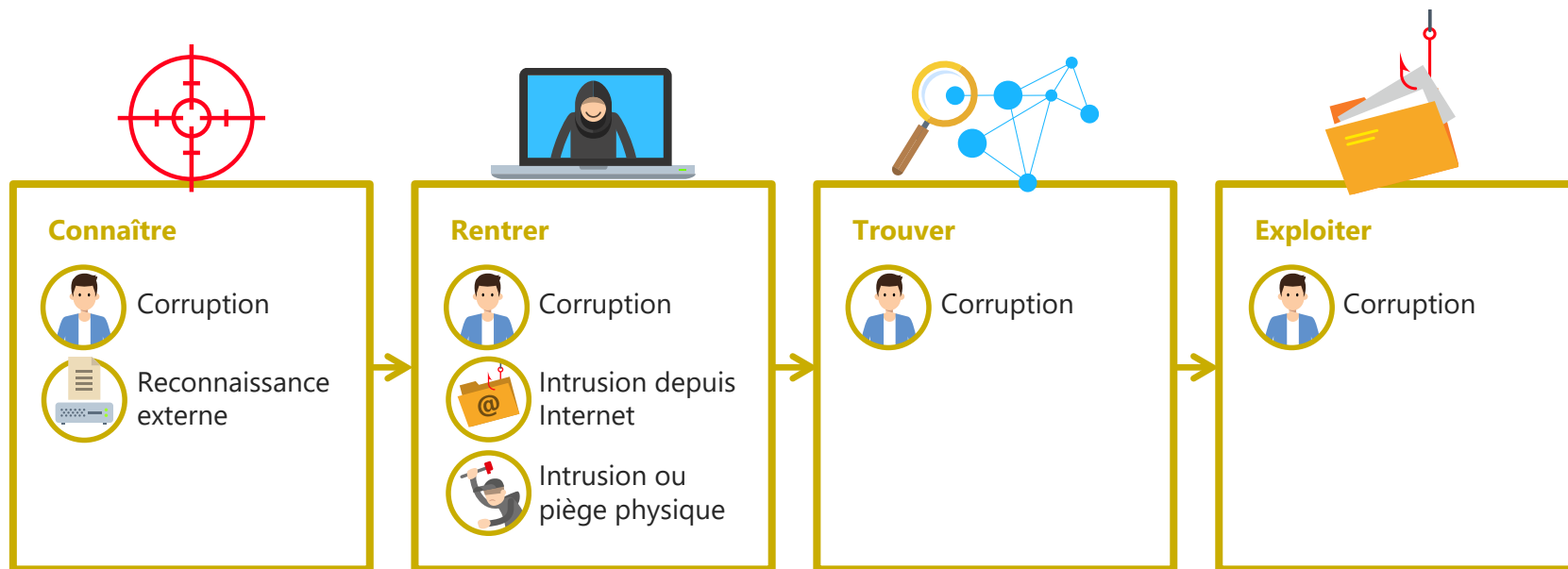
Activité 4-1



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.

Des scénarios structurés selon une séquence d'attaque type

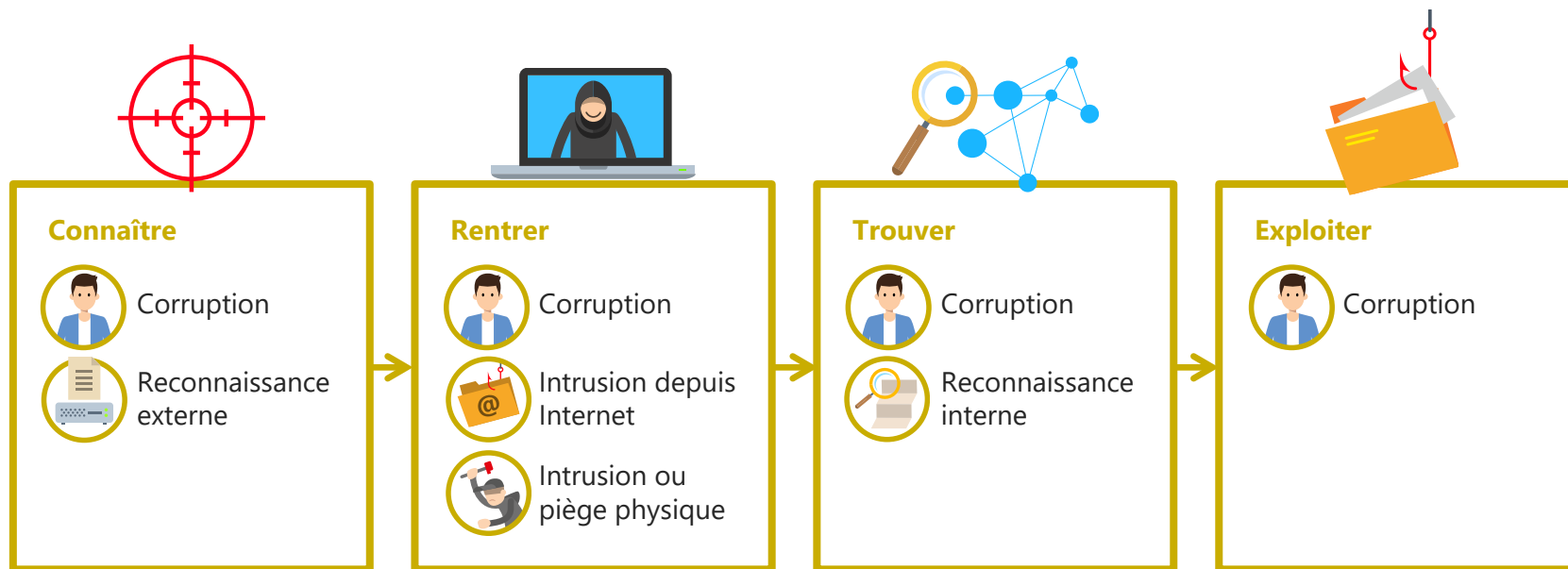
Activité 4-1



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.).

Des scénarios structurés selon une séquence d'attaque type

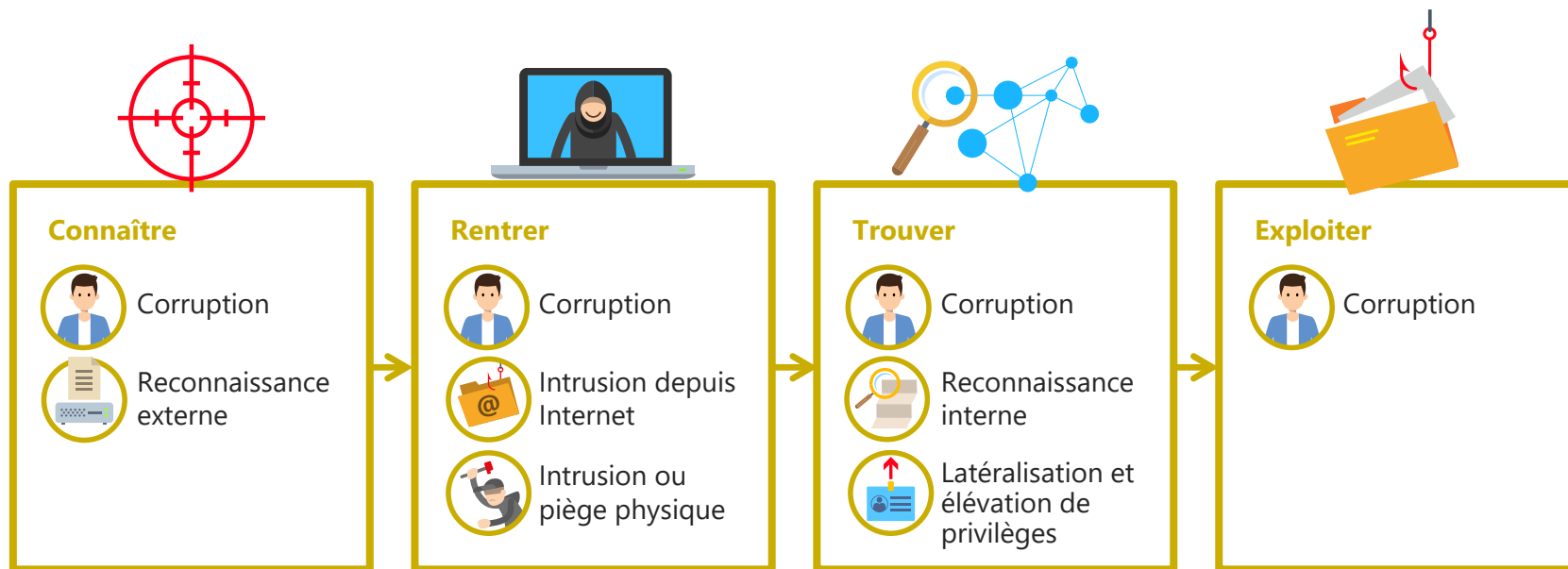
Activité 4-1



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.

Des scénarios structurés selon une séquence d'attaque type

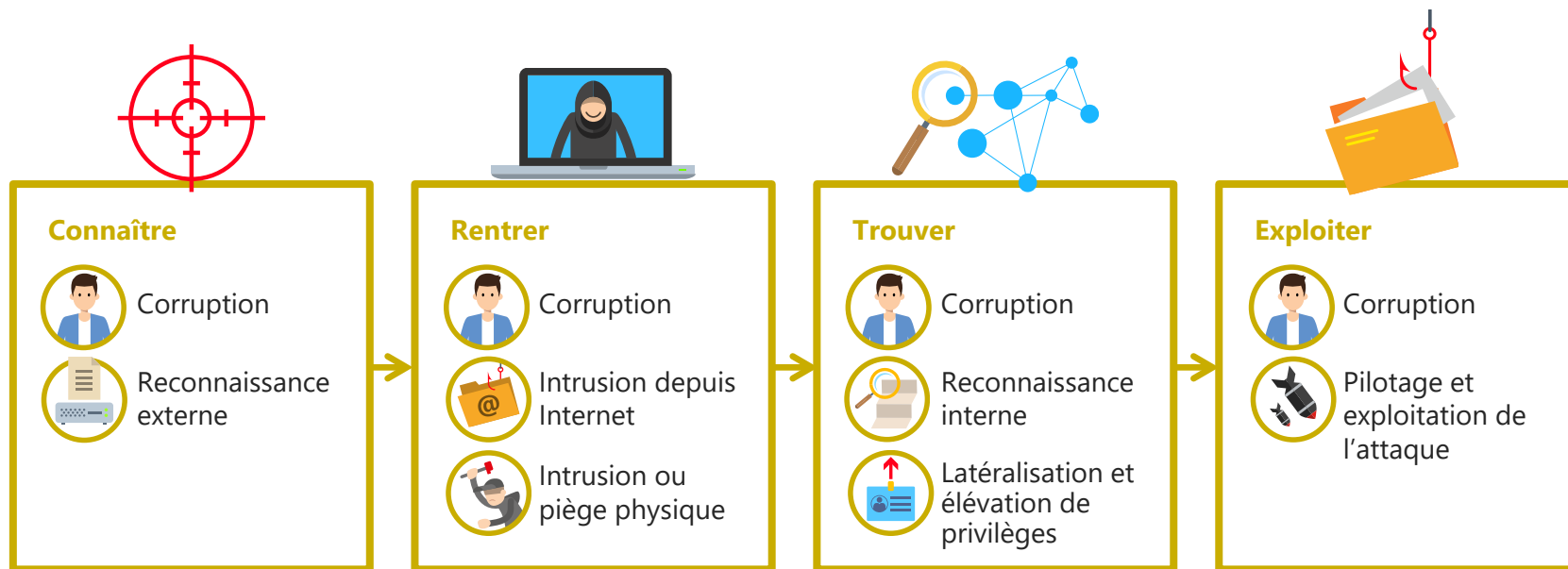
Activité 4-1



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.).

Des scénarios structurés selon une séquence d'attaque type

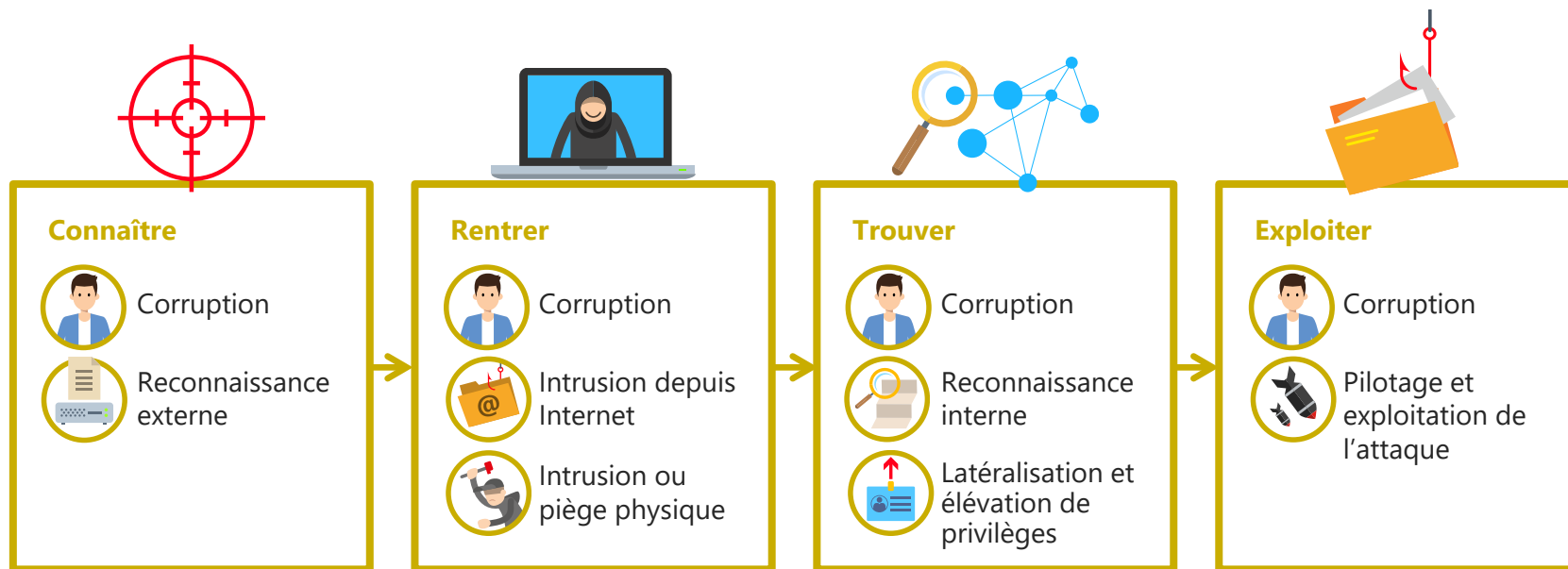
Activité 4-1



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 (par ex. opération de sabotage) ou durable et se réaliser en toute discrétion (par ex. opération d'espionnage visant à régulièrement exfiltrer des informations).

Des scénarios structurés selon une séquence d'attaque type

Activité 4-1



Important !

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



Définition

Activité 4-1



Bien support critique

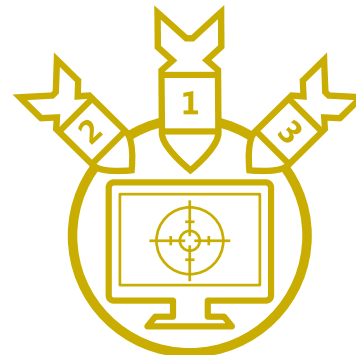
Bien support jugé très susceptible d'être ciblé par une source de risque pour atteindre son objectif.

Les biens supports critiques sont ceux qui apparaissent dans les scénarios opérationnels.



Action élémentaire

Action unitaire exécutée par une source de risque sur un bien support critique dans le cadre d'un scénario opérationnel.



Mode opératoire

Suite d'actions élémentaires que la source de risque devra probablement réaliser pour atteindre son objectif.

Elaborer les scénarios opérationnels

Activité 4-1

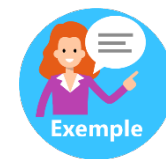
Comment construire un scénario opérationnel ?

- Partir des chemins d'attaque identifiés lors de l'atelier 3.
- Construire, pour chaque chemin d'attaque retenu un scénario opérationnel permettant à la source de risque d'atteindre son objectif.
- Enrichir les chemins d'attaques de quelques précisions sur la manière dont l'attaquant va procéder.



Elaborer les scénarios opérationnels

Activité 4-1 • Exemple du collégien



Rappel

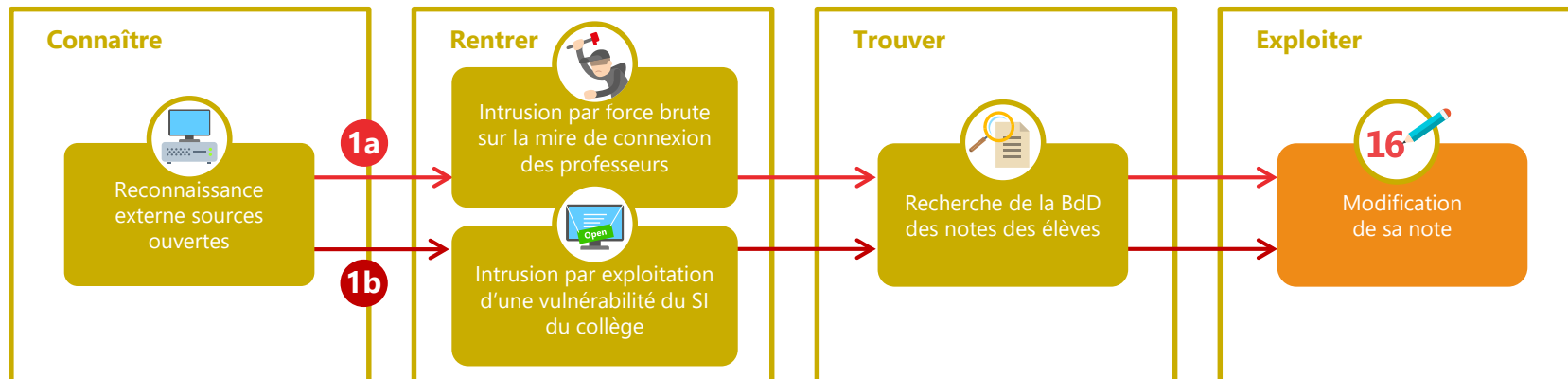
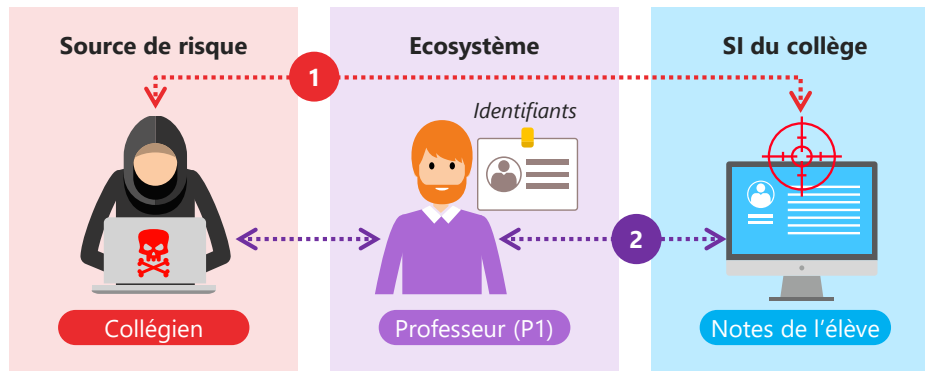
2 chemins d'attaque identifiés sur la modification de notes :

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

A3

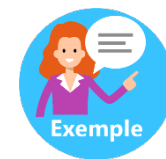
Scénario stratégique : Modification de la base de données par attaque directe.

Chemin d'attaque : n°1 • **Gravité :** 3



Elaborer les scénarios opérationnels

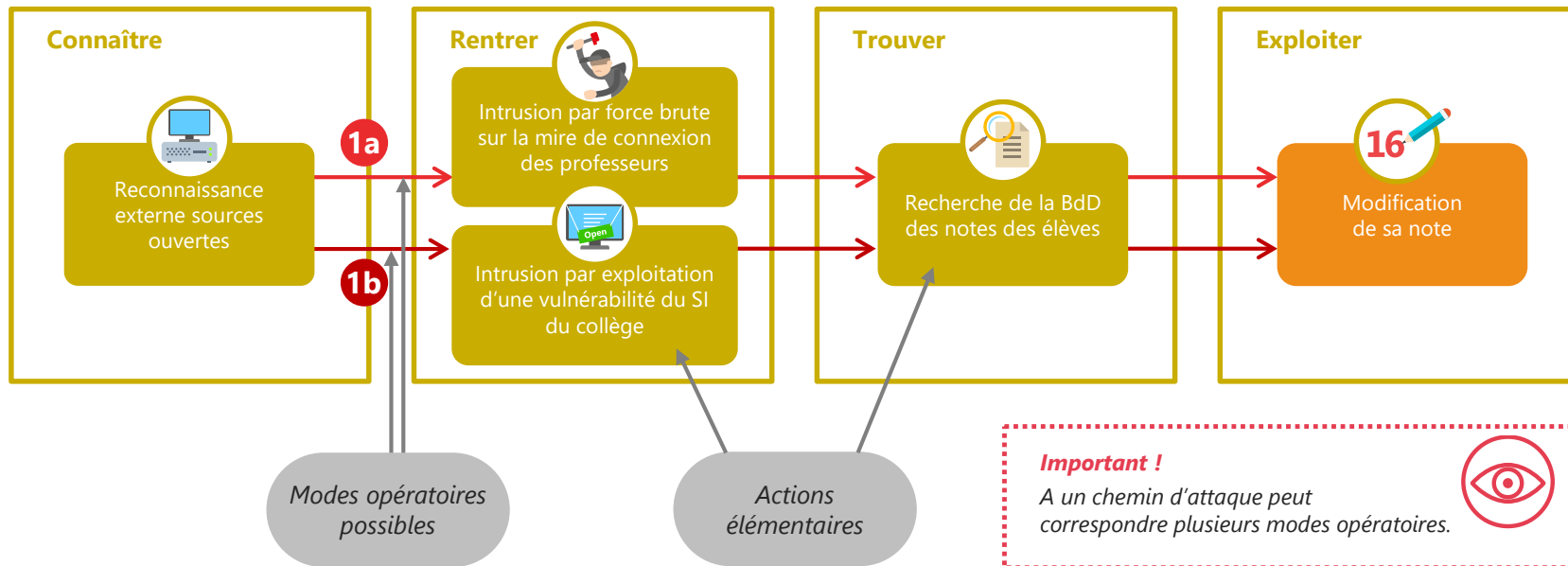
Activité 4-1 • Exemple du collégien



A3

Scénario stratégique : Modification de la base de données par attaque directe.

Chemin d'attaque : n°1 • **Gravité :** 3



Elaborer les scénarios opérationnels

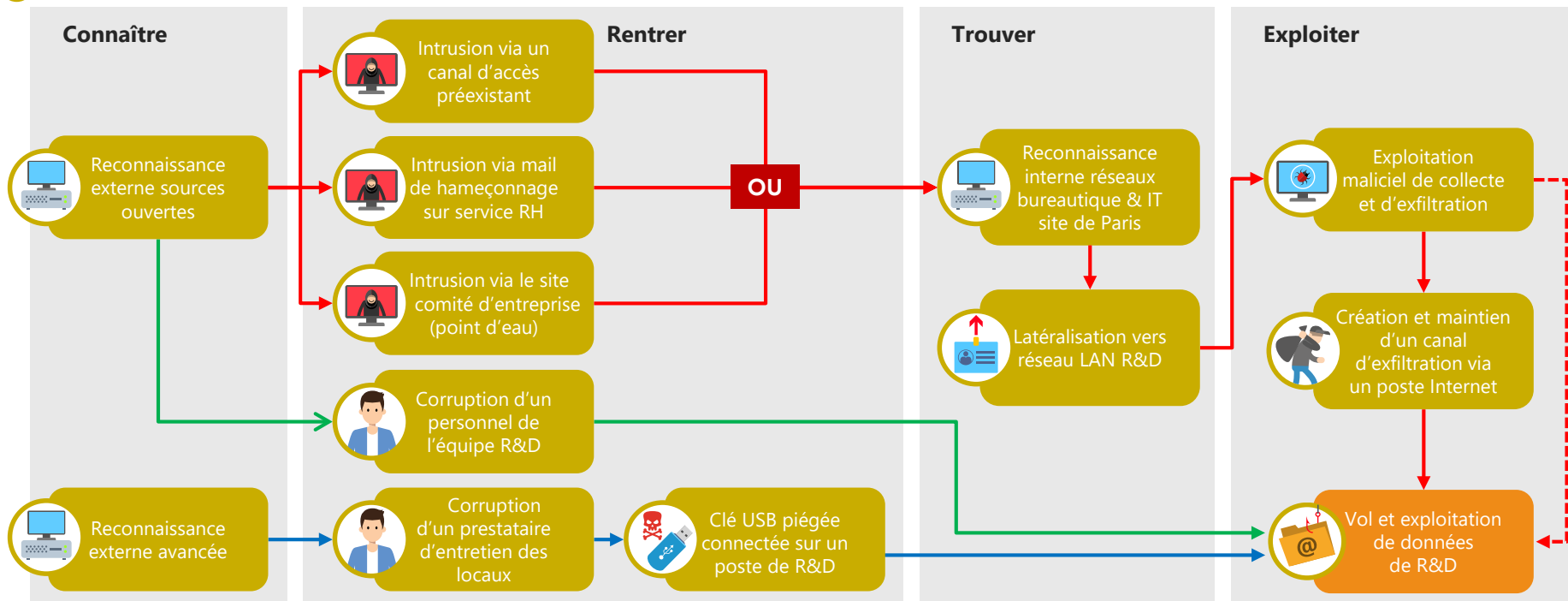


Activité 4-1

A3

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

Chemin d'attaque : n°1
Gravité : 3



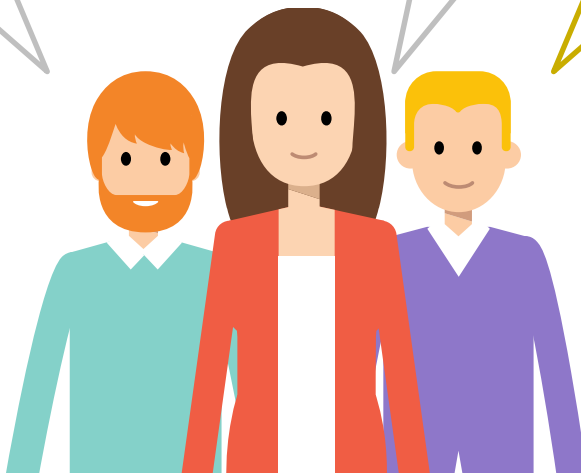
Evaluer la vraisemblance des scénarios opérationnels

Activité 4-2 • Les questions à se poser

Quelles sont les scénarios opérationnels schématisant les modes opératoires techniques qui seront mis en œuvre lors de l'attaque ?

Quelles sont les biens supports critiques susceptibles de servir de vecteur d'entrée ?

Quelle est la **vraisemblance** du scénario opérationnel ?



Définir une échelle de vraisemblance

Activité 4-2



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

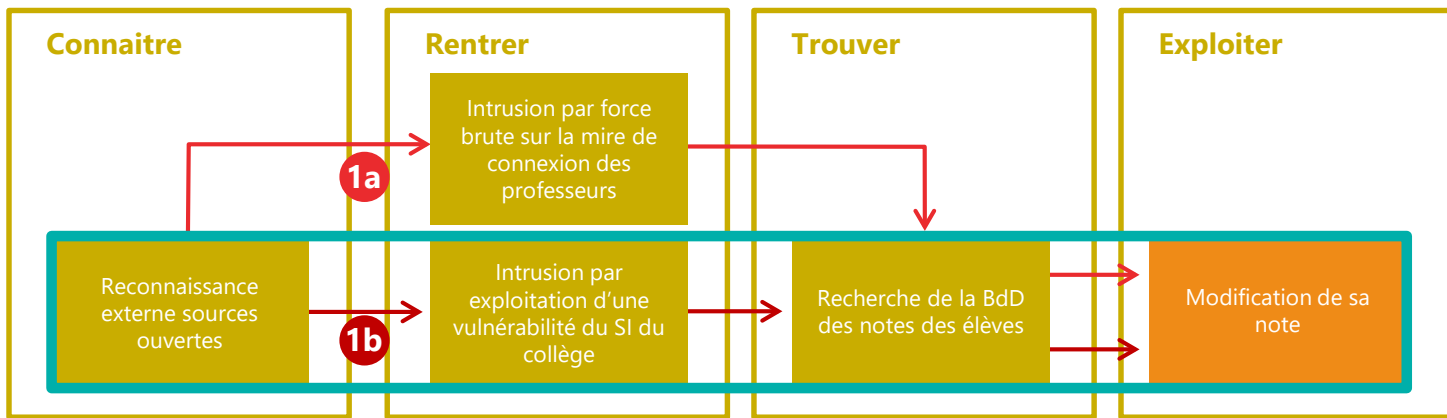
Conseil !

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



Les différents mode de calcul de la vraisemblance

Activité 4-2

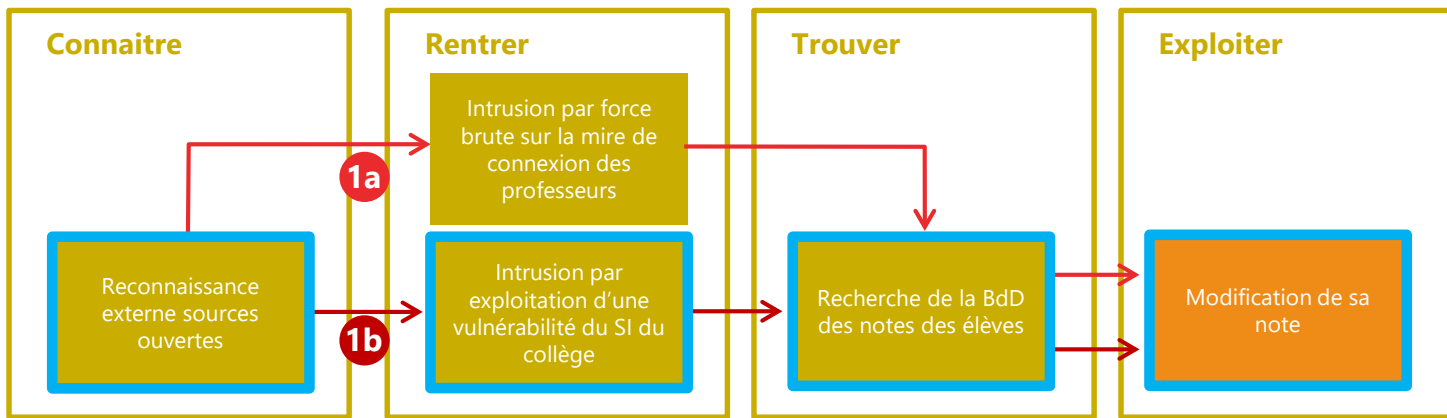


Méthode expresse

Estimer la vraisemblance globale du mode opératoire qui semble le plus probable.

Les différents mode de calcul de la vraisemblance

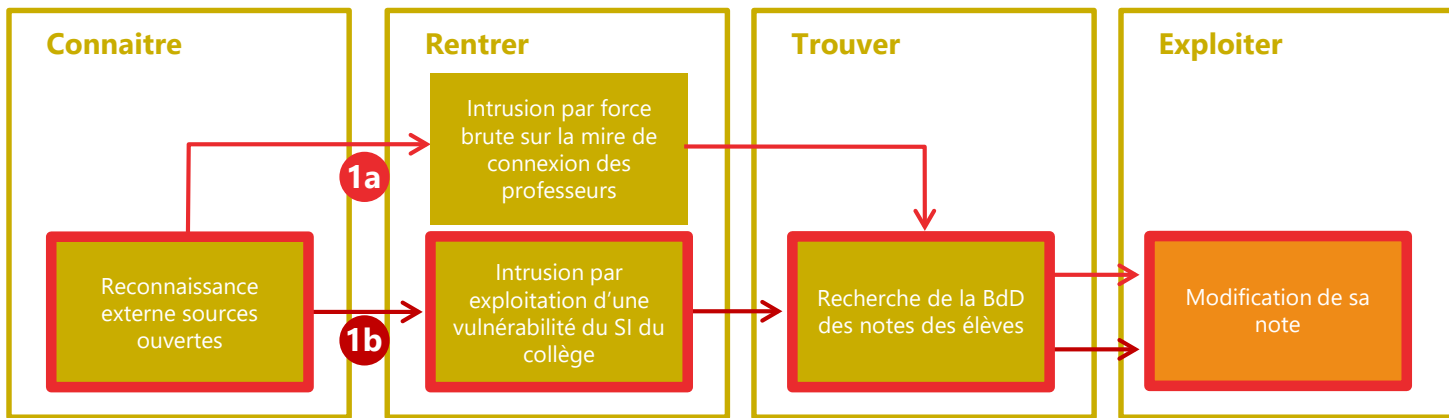
Activité 4-2



Méthode standard
Estimer la vraisemblance de chaque action élémentaire du mode opératoire du point de vue de l'attaquant.

Les différents mode de calcul de la vraisemblance

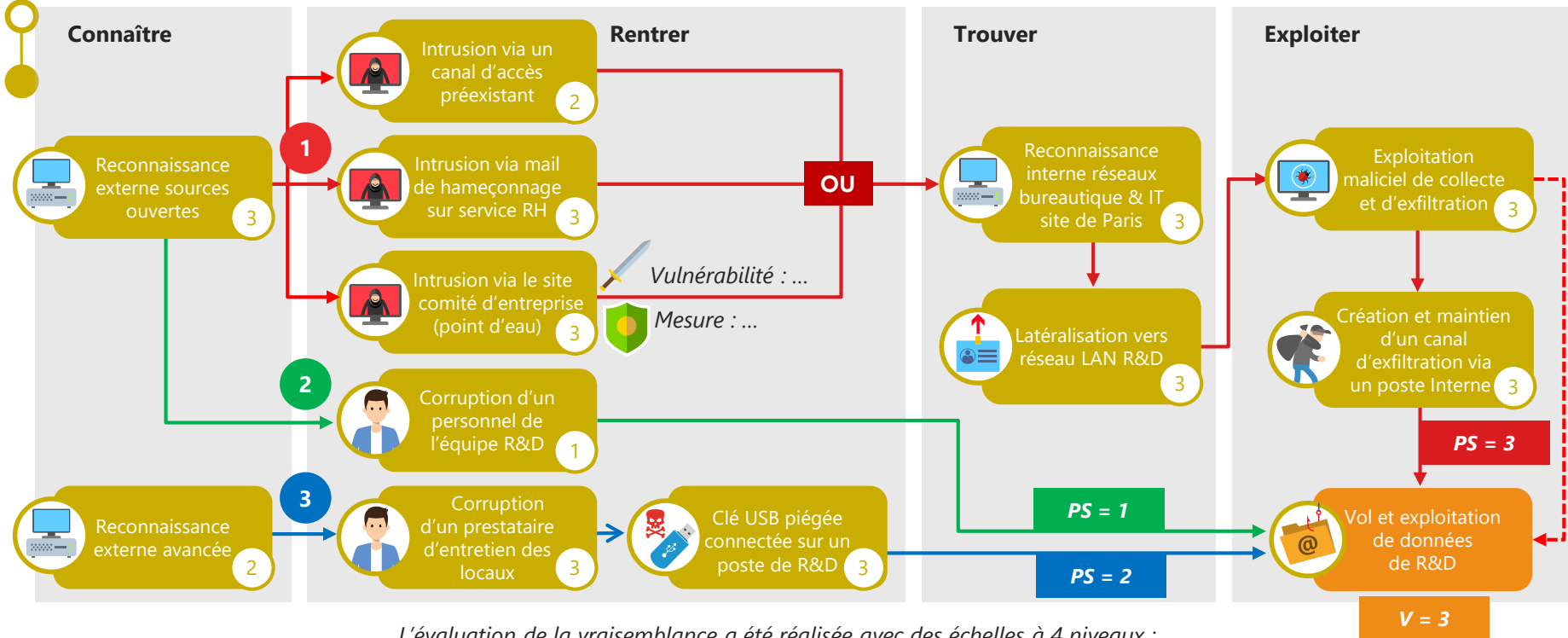
Activité 4-2



Méthode avancée
En plus de l'évaluation de la vraisemblance, j'effectue la cotation de la « difficulté technique » de chaque action élémentaire du mode opératoire du point de vue de l'attaquant.

Elaborer les scénarios opérationnels

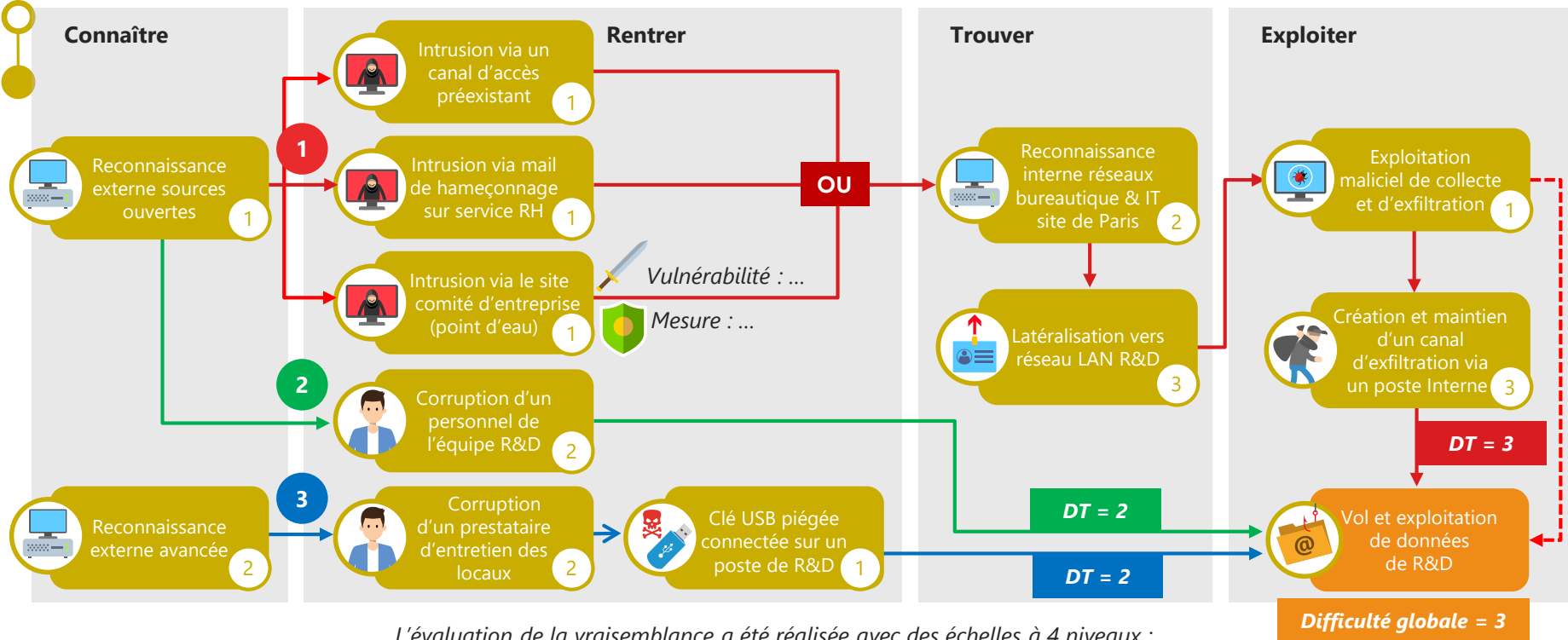
Activité 4-2 • Cotation en mode standard



L'évaluation de la vraisemblance a été réalisée avec des échelles à 4 niveaux :
• Pour la probabilité de succès (PS) : 1 – probabilité faible à 4 – quasi-certaine.
• Pour la vraisemblance (V) : V1 – peu vraisemblable à V4 – quasi-certain.

Elaborer les scénarios opérationnels

Activité 4-2 • Cotation en mode avancé



L'évaluation de la vraisemblance a été réalisée avec des échelles à 4 niveaux :
 • Pour la difficulté technique (DT) : 1 – Difficulté faible à 4 – Difficulté très élevée.

Elaborer les scénarios opérationnels

Activité 4-2 • Cotation en mode avancé

| | | DIFFICULTÉ TECHNIQUE | | | |
|--------------------------|---|------------------------------|------------------------------|---------------------------------|---------------------------------|
| | | 4 | 3 | 2 | 1 |
| PROBABILITE DE SUCCES | 4 | Vraisemblance moyenne (2) | Vraisemblance élevé (3) | Vraisemblance très élevé (4) | Vraisemblance très élevé (4) |
| | 3 | Vraisemblance moyenne (2) | Vraisemblance élevé (3) | Vraisemblance élevé (3) | Vraisemblance très élevé (4) |
| | 2 | Vraisemblance faible (1) | Vraisemblance moyenne (2) | Vraisemblance élevé (3) | Vraisemblance élevé (3) |
| | 1 | Vraisemblance faible (1) | Vraisemblance faible (1) | Vraisemblance moyenne (2) | Vraisemblance moyenne (2) |

Elaborer les scénarios opérationnels

Activité 4-2 • Cotation en mode avancé

Calcul de la vraisemblance globale en mode avancé

Les valeurs de probabilité des modes opératoires ont été calculées selon la méthode standard vue précédemment

Valeur de difficulté calculée

Vraisemblance Globale

| Mode opératoire | Probabilité de succès | Difficulté technique | Vraisemblance |
|-----------------|-----------------------|----------------------|---------------|
| MO1 | 3- Très élevée | 3- Élevée | 3- Élevée |
| MO2 | 1- Faible | 2- Modérée | 2- Moyenne |
| MO3 | 2- Significative | 2- Modérée | 3- Élevée |

Comment constituer les scénarios de risques ?

Fin de l'atelier 4

Légende

Socle = Socle de sécurité, liste des référentiels applicables, état d'application, identification des écarts et leurs justifications

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

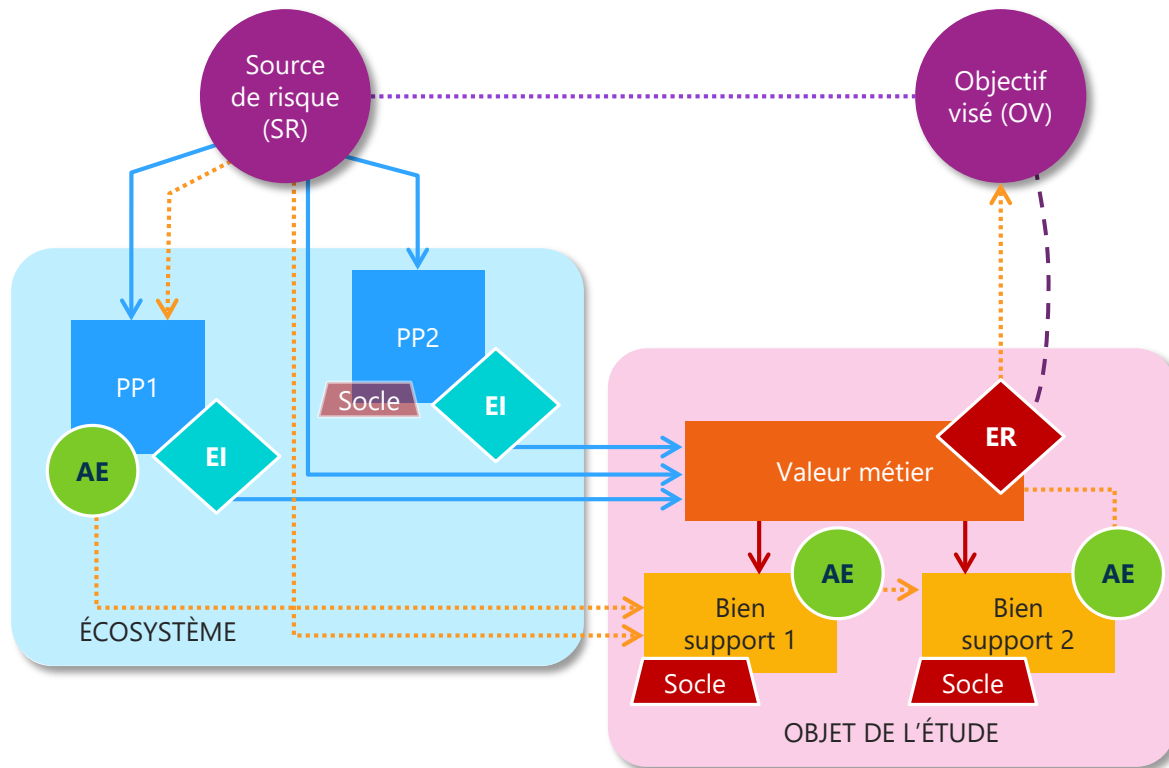
PP = Partie prenante de l'écosystème

→ Chemin d'attaque d'un scénario stratégique

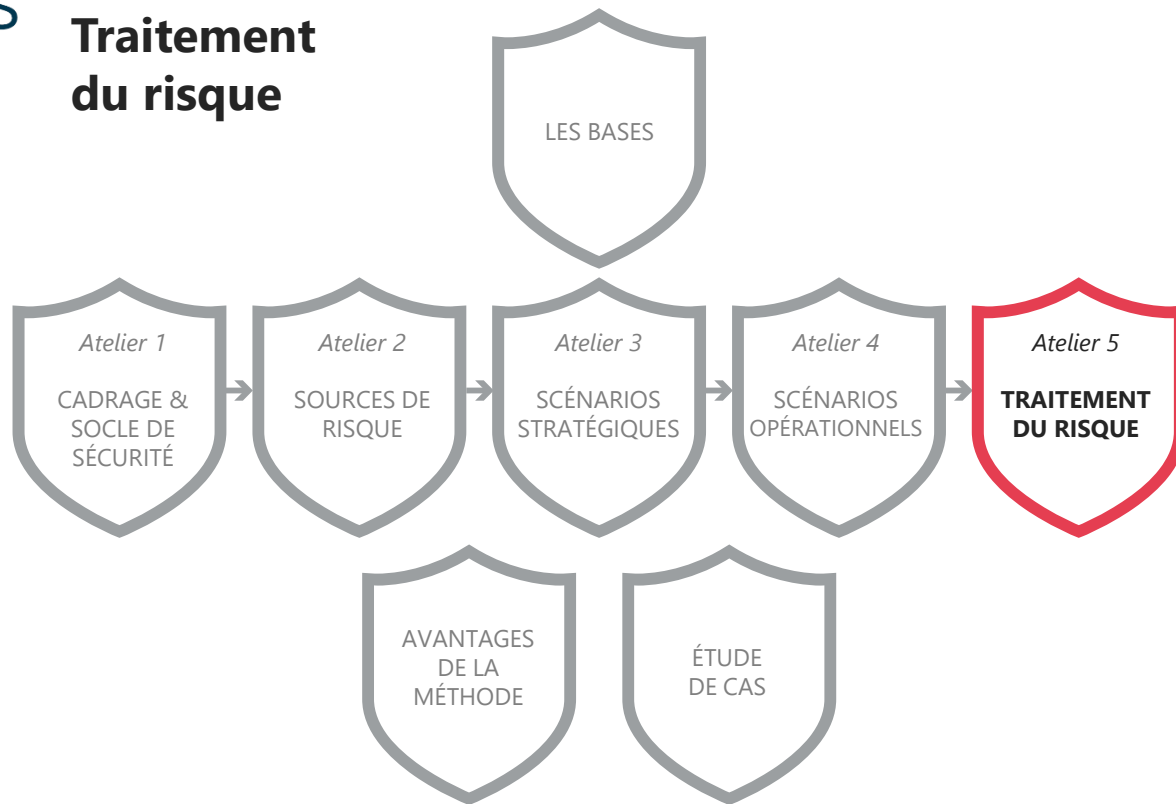
EI = Événement intermédiaire associé à une valeur métier de l'écosystème

→ Mode opératoire d'un scénario opérationnel

AE = Action élémentaire sur un bien support



Atelier 5 Traitement du risque



Traitement du risque

Atelier 5



Objectif

Définir une stratégie de traitement du risque et identifier les risques résiduels.



Participants

Direction, Métiers, RSSI, DSI.

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)


ATELIER 5 TRAITEMENT DU RISQUE

Éléments en sortie

- Synthèse des risques initiaux
- Stratégie de traitement du risque
- Plan de traitement du risque
- Synthèse des risques résiduels
- Cadre du suivi des risques

Traitement du risque

Atelier 5

- 
- Activité 1
Réaliser une évaluation des risques
 - Activité 2
Décider de la stratégie de traitement du risque
 - Activité 3
Définir les mesures de sécurité
 - Activité 4
Évaluer et documenter les risques résiduels
 - Activité 5
Mettre en place le cadre de suivi des risques



Réaliser une évaluation des risques

Atelier 5-1 • Les questions à se poser

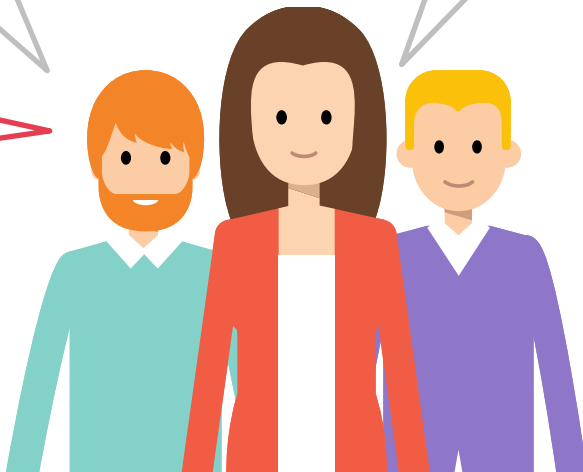
Quelle stratégie de traitement des risques faut-il adopter ?

Sur quelles actions élémentaires faudrait-il agir pour rendre la vie de l'attaquant plus difficile ?
Quelles mesures de sécurité faut-il mettre en place sur les biens supports critiques pour traiter les risques ?

Quelle est la cartographie des risques résiduels ?

Quels sont les **niveaux** des risques initiaux ?
Comment représenter les risques ?

Comment maintenir l'objet de l'étude en conditions de sécurité dans la durée ?



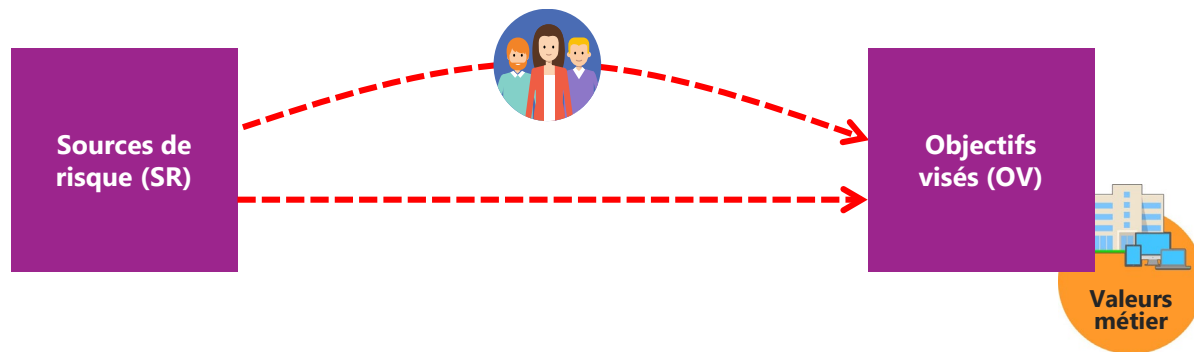
Scénario de risque

- **Séquence ou combinaison d'événements** qui conduisent de la cause initiale à la conséquence indésirable (ISO 27005:2022).
- **Scénario complet**, allant de la source de risque à l'objectif visé par elle, décrivant un chemin d'attaque et le scénario opérationnel associé (EBIOS RM).



Construction de la formulation du risque

Atelier 5-1 • Vision globale



Construction de la formulation du risque

Atelier 5-1 • Vision détaillée

Lors de l'atelier 1, le métier exprime des événements redoutés (ER) et évalue leur gravité. Les ER les plus graves serviront de base pour le reste de la construction du risque.

Lors de l'atelier 2, le métier valide des couples de sources de risque et d'objectifs visés. Les plus pertinents, à mettre en relation avec les ER précédemment retenus, seront (re)formulés et contextualisés.

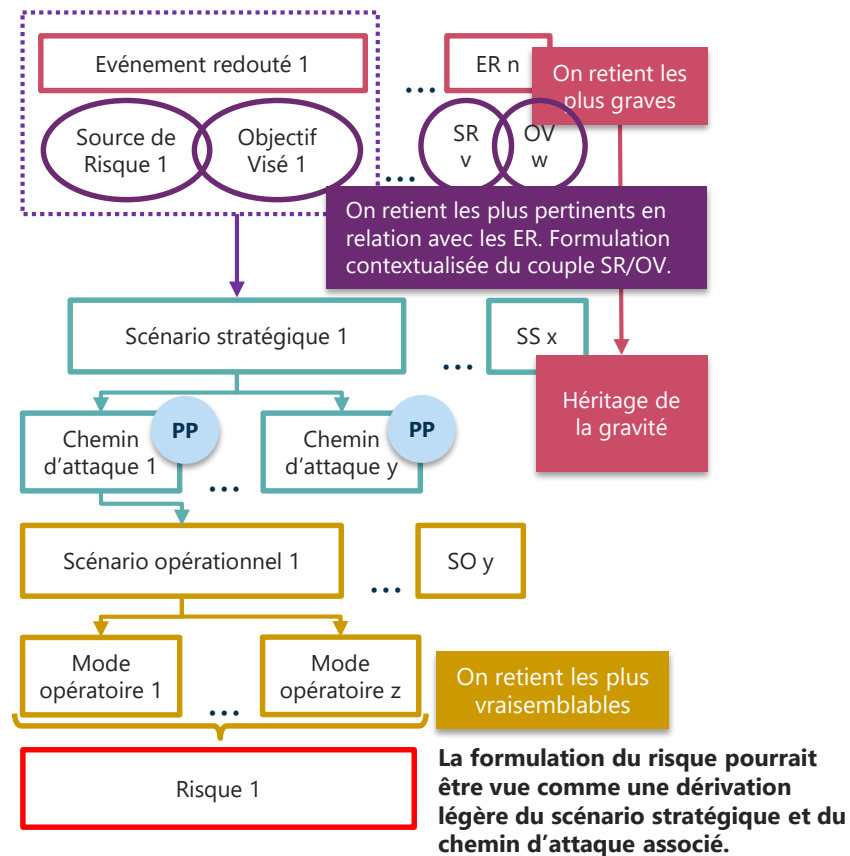
Sur la base des couples SR/OV retenus et contextualisés, création de scénarios stratégiques (SS).

Puis raffinement des SS en chemins d'attaque, avec reformulation, en y intégrant pour certains des parties prenantes.

Reprise du SS + chemin d'attaque retenu.

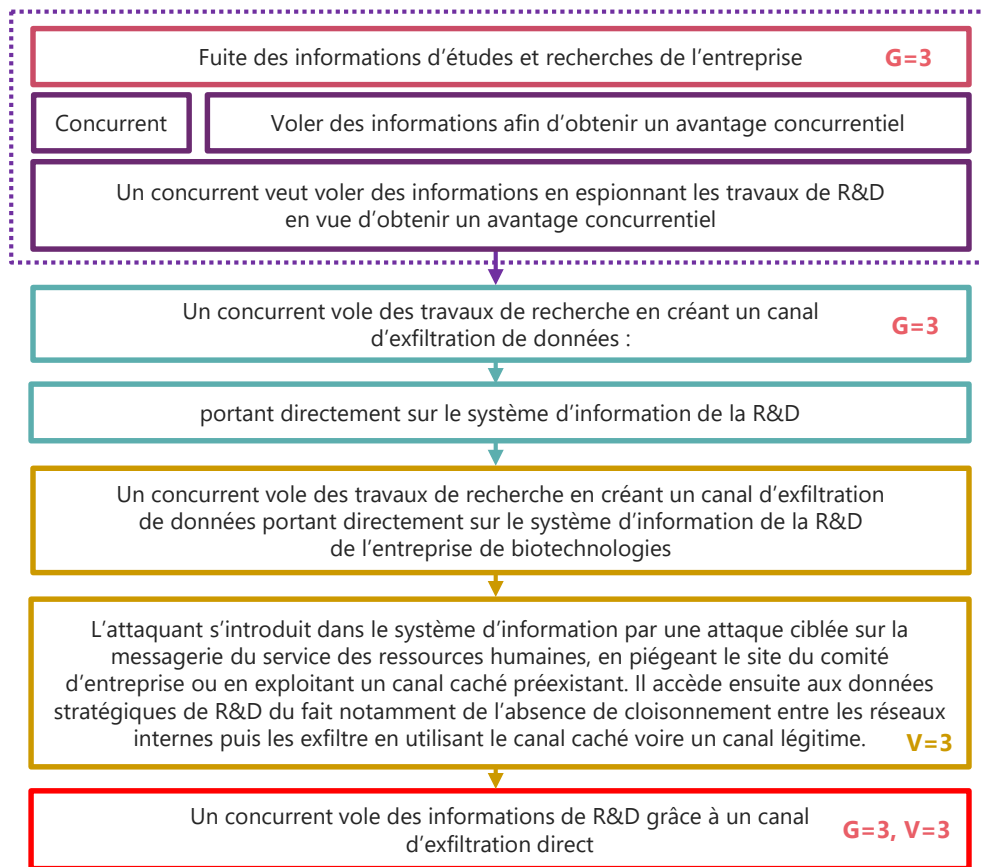
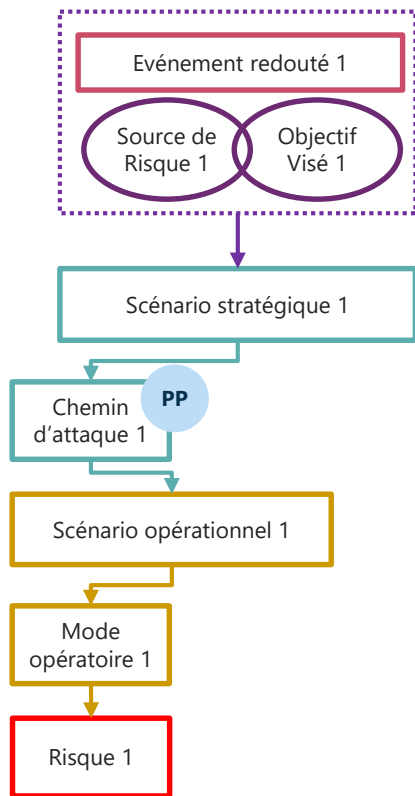
Description synthétique de chaque mode opératoire

Synthèse du scénario stratégique et du mode opératoire ayant permis d'obtenir ce risque.



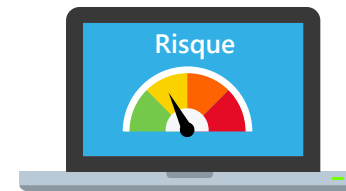
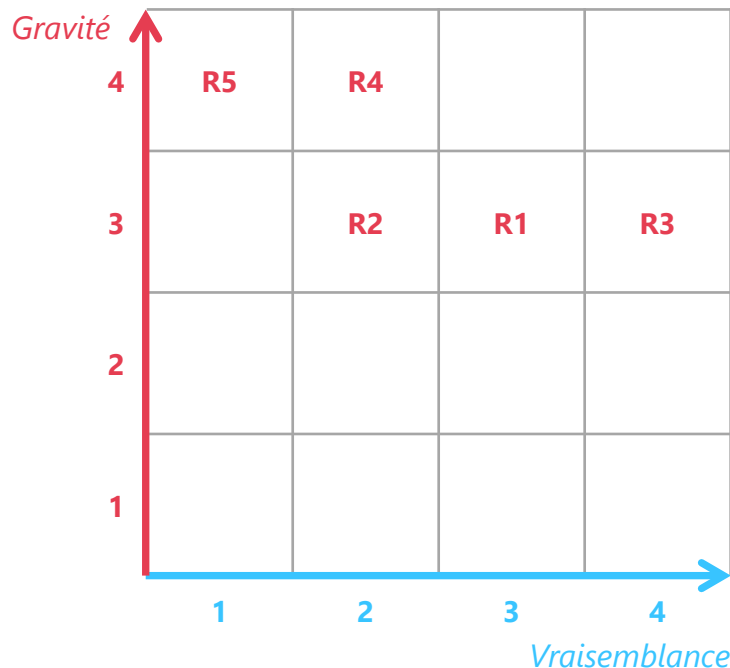
Construction de la formulation du risque

Atelier 5-1 • Exemple avec R1



Représentation du risque

Atelier 5-1 • Exemple avec R1



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.

Décider de la stratégie de traitement du risque

Atelier 5-2 • Les questions à se poser

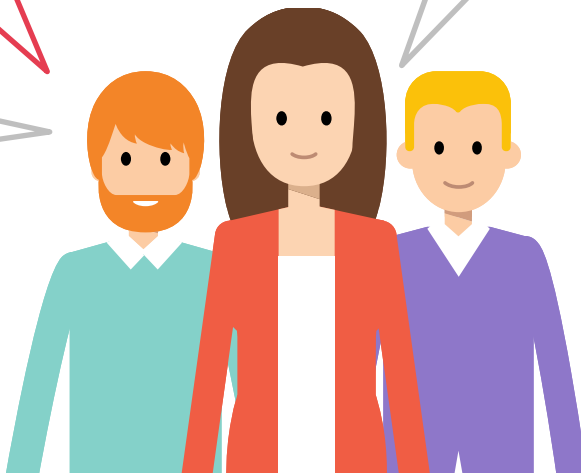
Quelle **stratégie de traitement** des risques faut-il adopter ?

Sur quelles actions élémentaires faudrait-il agir pour rendre la vie de l'attaquant plus difficile ?
Quelles mesures de sécurité faut-il mettre en place sur les biens supports critiques pour traiter les risques ?

Quelle est la cartographie des risques résiduels ?

Quels sont les niveaux des risques initiaux ?
Comment représenter les risques ?

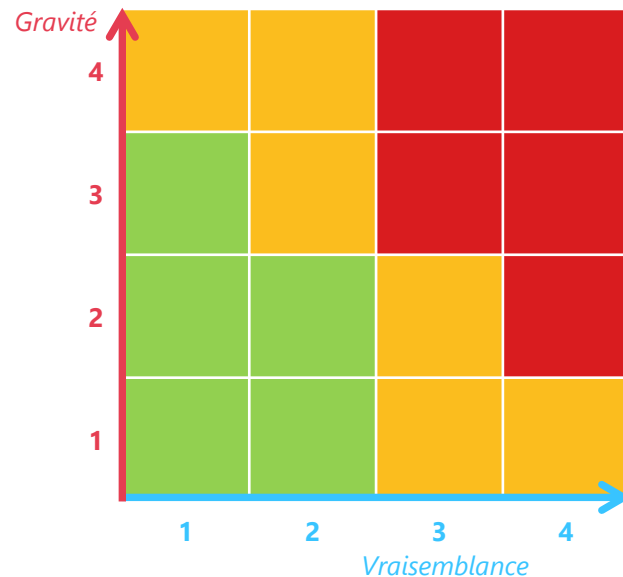
Comment maintenir l'objet de l'étude en conditions de sécurité dans la durée ?



Définir l'échelle d'acceptabilité du risque

Atelier 5-2

| Niveau de risque | Acceptabilité du risque | Intitulé des décisions et des actions |
|------------------|--------------------------------|--|
| 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 |
| Elevé | 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 |



Important !

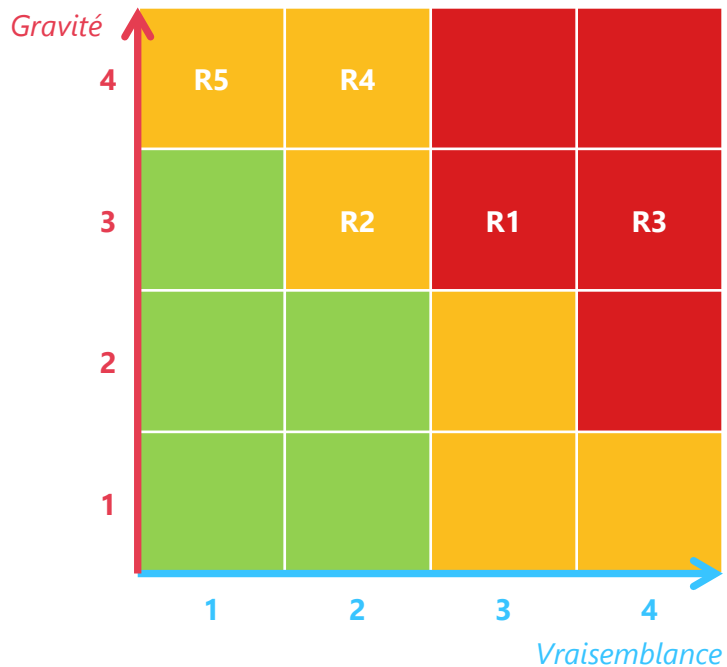
La représentation de l'échelle d'acceptabilité doit permettre de comparer les risques les uns par rapport aux autres et être compréhensible par l'ensemble des participants.



Application de l'échelle d'acceptabilité du risque à la matrice des risques

Atelier 5-2

Atelier 5
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.

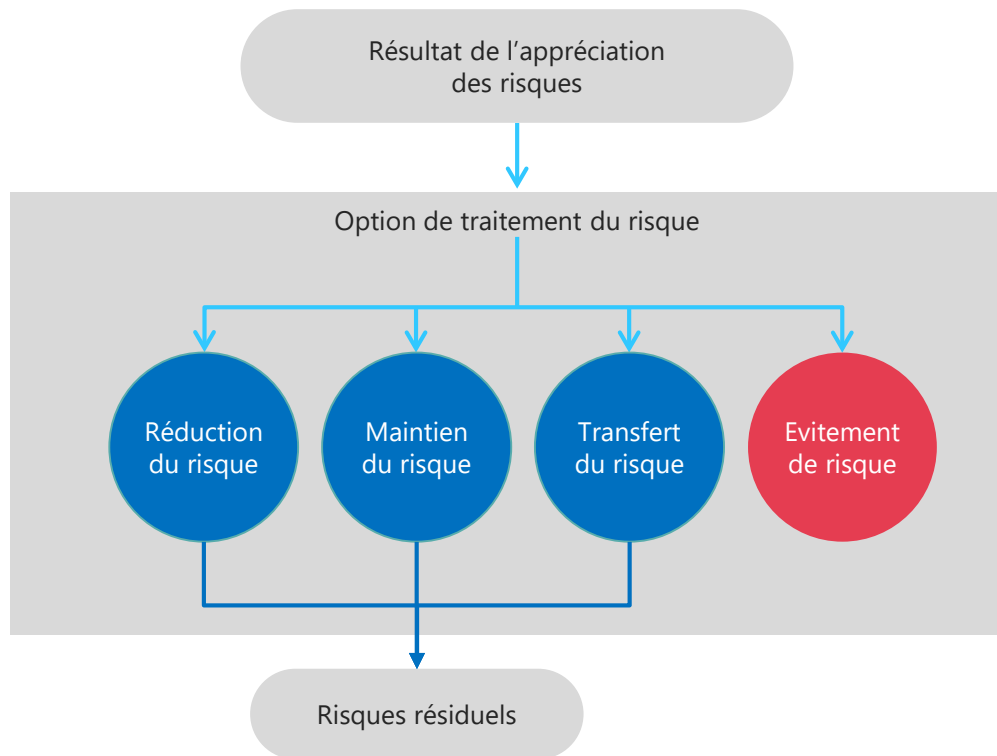
Important !

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

Atelier 5-2 : Options de traitement du risque (selon ISO 27005:2022)



Définir les mesures de sécurité

Atelier 5-3 • Les questions à se poser

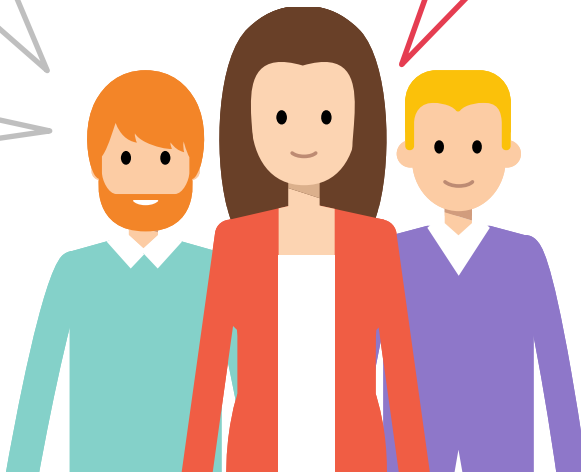
Quelle stratégie de traitement des risques faut-il adopter ?

Quels sont les niveaux des risques initiaux ?
Comment représenter les risques ?

Sur quelles **actions élémentaires** faudrait-il agir pour rendre la vie de l'attaquant plus difficile ?
Quelles **mesures de sécurité** faut-il mettre en place sur les **biens supports critiques** pour traiter les risques ?

Quelle est la cartographie des risques résiduels ?

Comment maintenir l'objet de l'étude en conditions de sécurité dans la durée ?



Définir les mesures de sécurité

Atelier 5-3 • Dans un plan de traitement du risque

Selon les stratégies de traitement retenues pour chaque risque :

- Définir des mesures de sécurité.
- Répartir ces mesures de sécurité dans un plan de traitement du risque, selon 4 groupes de mesures :
 - Gouvernance
 - Protection
 - Défense
 - Résilience
- Placer dans le plan de traitement du risque les mesures identifiées lors des différents ateliers.





Structuration du plan de traitement du risque

Atelier 5-3 • Exemples de thématique

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.



Cas fictif – société de biotechnologies

Atelier 5-3 • Définir les mesures de sécurité dans un plan de traitement du risque



| Mesure de sécurité | Risques associés | Responsable | Freins et difficultés de mise en œuvre | Coût / Complexité | Charge estimée | Échéance | Priorité | Statut |
|--------------------|------------------|-------------|--|-------------------|----------------|----------|----------|--------|
| GOVERNANCE | | | | | | | | |
| | | | | | | | | |
| PROTECTION | | | | | | | | |
| | | | | | | | | |
| DEFENSE | | | | | | | | |
| | | | | | | | | |
| RESILIENCE | | | | | | | | |
| | | | | | | | | |

Cas fictif – société de biotechnologies

Atelier 5-3 • Définir les mesures de sécurité dans un plan de traitement du risque

| Mesure de sécurité | Risques associés | Responsable | Freins et difficultés de mise en œuvre | Coût / Complexité | Charge estimée | Échéance | Priorité | Statut |
|---|------------------|-------------------------|---|-------------------|----------------|----------|----------|----------|
| GOUVERNANCE | | | | | | | | |
| Sensibilisation renforcée au hameçonnage par un prestataire spécialisé | R1 | RSSI | Validation de la hiérarchie obligatoire | + | | 6 mois | | En cours |
| Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI | R1, R5 | RSSI | | ++ | 10 j / h | | P1 | 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 | | ++ | 5 j / h | | P2 | 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 | ++ | | 12 mois | | A lancer |
| Limitation des données transmises au laboratoire au juste besoin | R2 | Équipe R&D | | + | | 3 mois | | Terminé |
| PROTECTION | | | | | | | | |
| Protection renforcée des données de R&D sur le SI (pistes : 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 | | ++ | 20 j / h | | P3 | A lancer |

Cas fictif – société de biotechnologies

Atelier 5-3 • Définir les mesures de sécurité dans un plan de traitement du risque

| Mesure de sécurité | Risques associés | Responsable | Freins et difficultés de mise en œuvre | Coût / Complexité | Charge estimée | Échéance | Priorité | Statut |
|---|------------------|------------------------------|---|-------------------|----------------|----------|----------|----------|
| DEFENSE | | | | | | | | |
| 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 |
| | | | | | | | | |
| | | | | | | | | |
| RESILIENCE | | | | | | | | |
| Renforcement du plan de continuité d'activité | R4, R5 | Équipe continuité d'activité | | ++ | | 12 mois | | En cours |
| | | | | | | | | |
| | | | | | | | | |

Évaluer et documenter les risques résiduels

Atelier 5-4 • Les questions à se poser

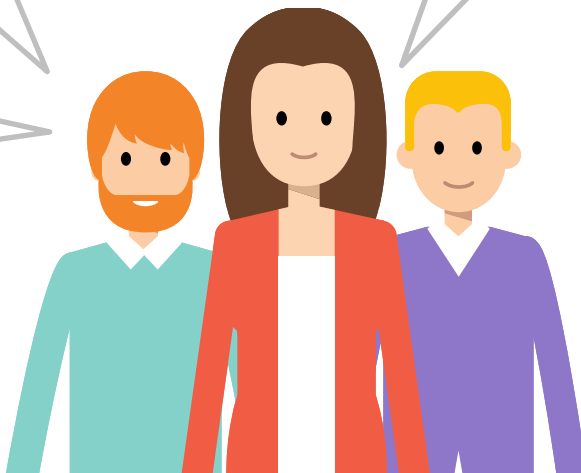
Quelle stratégie de traitement des risques faut-il adopter ?

Sur quelles actions élémentaires faudrait-il agir pour rendre la vie de l'attaquant plus difficile ?
Quelles mesures de sécurité faut-il mettre en place sur les biens supports critiques pour traiter les risques ?

Quelle est la cartographie des **risques résiduels** ?

Quels sont les niveaux des risques initiaux ?
Comment représenter les risques ?

Comment maintenir l'objet de l'étude en conditions de sécurité dans la durée ?



Définition

Atelier 5-4

Risque résiduel

Scénario de risque subsistant après application de la stratégie de traitement du risque. Cette évaluation repose sur la gravité et la vraisemblance du risque après l'application du plan de traitement du risque.



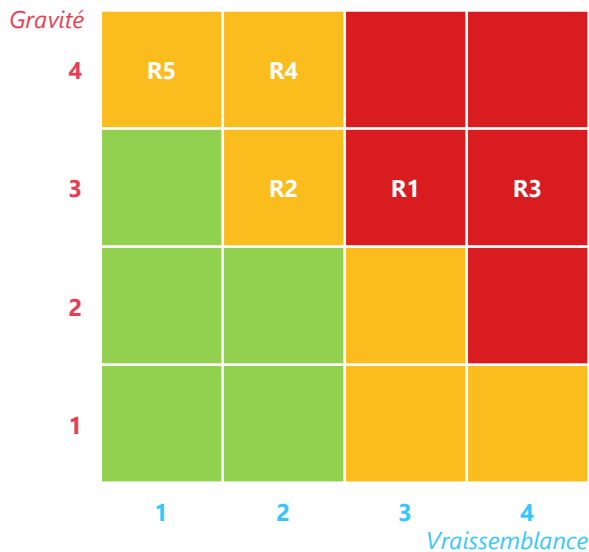
Cas fictif – société de biotechnologies

Atelier 5-4 • Évaluer et documenter les risques résiduels

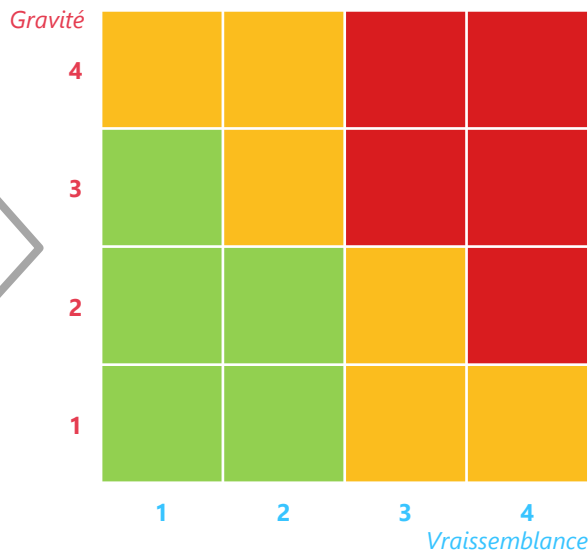


Utilisez le plan de traitement du risque pour évaluer et documenter les risques résiduels

Cartographie du risque actuel
(avant traitement)



Cartographie du risque résiduel
(après application du PLAN)



Pour un jalon majeur



Important !

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



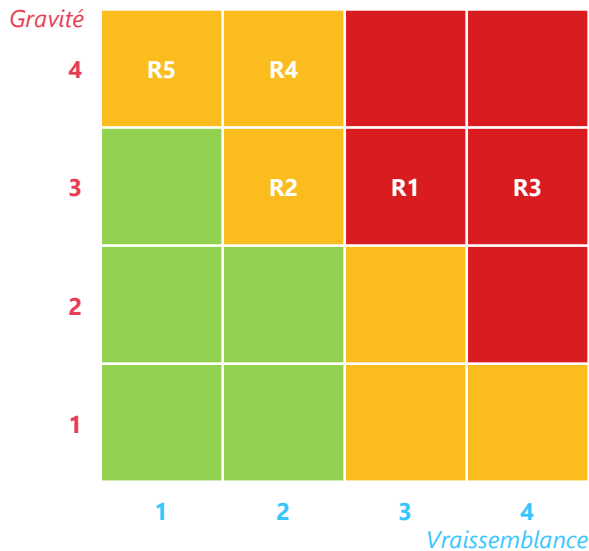
Cas fictif – société de biotechnologies

Atelier 5-4 • Évaluer et documenter les risques résiduels

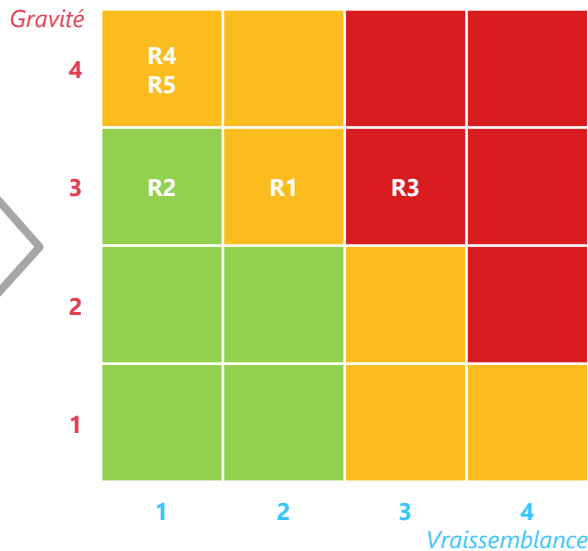


Utilisez le plan de traitement du risque pour évaluer et documenter les risques résiduels

Cartographie du risque actuel
(avant traitement)



Cartographie du risque résiduel
(après application du PLAN)



Pour un jalon majeur



Important !

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



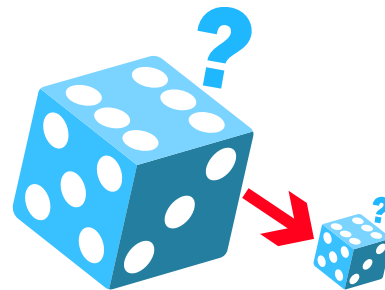
Recalcul du risque

Atelier 5-4



Plan de traitement du risque

Rappel : la cartographie du risque résiduel s'effectue APRES application du plan de traitement du risque.



Vraisemblance

Les mesures de sécurité ne font baisser (le cas échéant) que la vraisemblance.

Mettre en place le cadre de suivi des risques

Atelier 5-5 • Les questions à se poser

Quelle stratégie de traitement des risques faut-il adopter ?

Sur quelles actions élémentaires faudrait-il agir pour rendre la vie de l'attaquant plus difficile ?
Quelles mesures de sécurité faut-il mettre en place sur les biens supports critiques pour traiter les risques ?

Quelle est la cartographie des risques résiduels ?

Quels sont les niveaux des risques initiaux ?
Comment représenter les risques ?

Comment **maintenir** l'objet de l'étude en **conditions de sécurité** dans la durée ?



Recalcul du risque

Fin de l'atelier 5



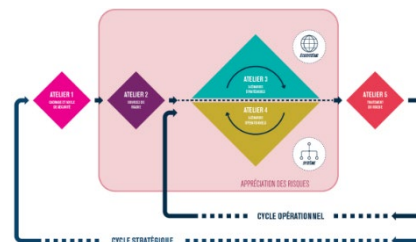
Mettre en place un comité de pilotage pour assurer le suivi des risques.

| MEASURE DE SECURITE | RESANANS DE RISQUES ASSOCIES | RESPONSABLE | INDICATEURS DE NIVEAU EN BOURSE | COÛT / COMPLEXITE | ESPERANCE | STATUT |
|--|------------------------------|-------------------------|---|-------------------|-----------|----------|
| SECURITE | | | | | | |
| Sensibilisation renforcée au hame langage par un prestataire spécialiste | R1 | RISD | Validation de CHACU individuel | -- | 4 mois | En cours |
| Audit de sécurité technique et organisationnel de l'ensemble de la plateforme par un PASSI | R1, R5 | RISD | | -- | 3 mois | A lancer |
| Intégration d'une clause de garantie d'un niveau de sécurité adéquate dans les contrats avec les prestataires et laboratoires | R3, R5, R4 | Forque juridique | Efficacité au fil de l'eau à la négociation des contrats | -- | 10 mois | En cours |
| Mise en place d'une procédure de remplacement de tous les matériels de sécurité pour lesquels un prestataire ou un laboratoire | R3, R5, R4 | RISD / Forque juridique | | -- | 4 mois | A lancer |
| Audit de sécurité organisationnel des prestataires et laboratoires de Mise en place et suivi des plans d'action consécutifs | R2, R5, R4 | RISD | Acceptation de la démarche par les prestataires et laboratoires | -- | 4 mois | A lancer |
| Limitation des données transmises aux Laboratoires au juste besoin | R3 | Forque R&D | | - | 1 mois | Terminé |

Suivi de l'avancement des mesures

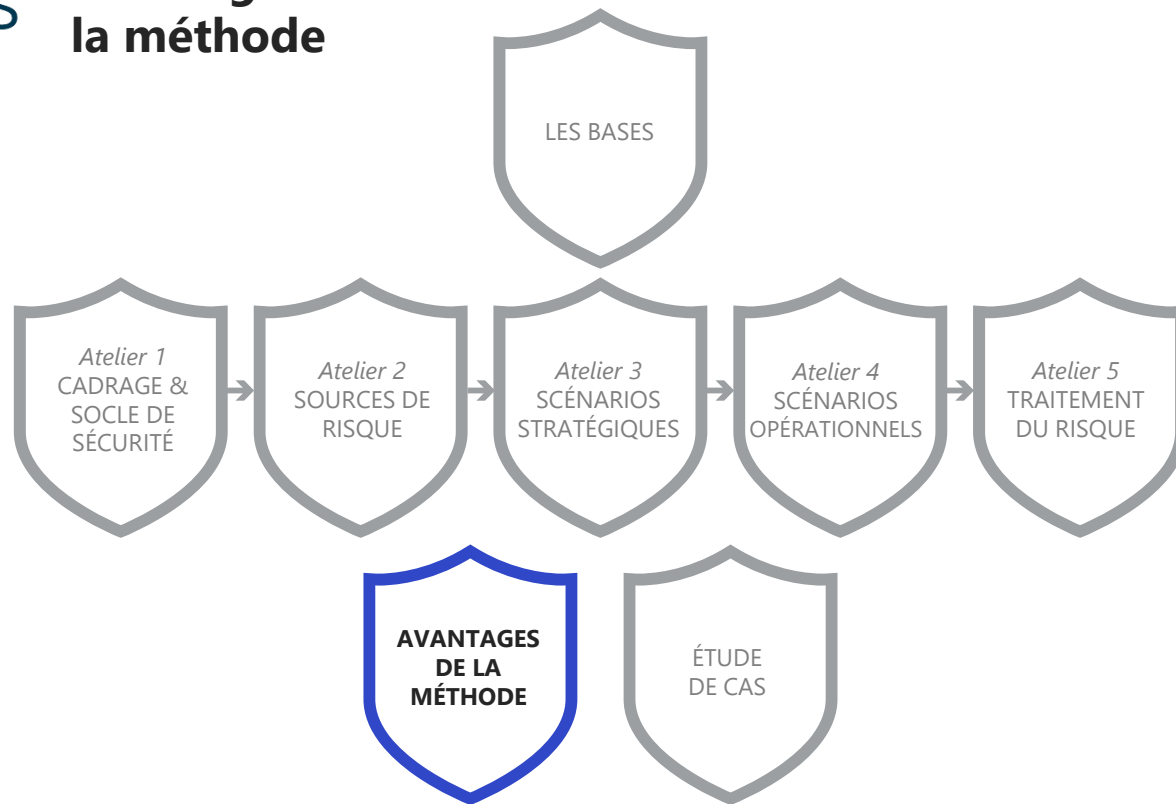


Suivi des indicateurs de maintien en condition de sécurité

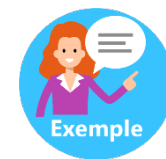


Suivi des mises à jour de l'étude des risques selon les cycles stratégique et opérationnel

Avantages de la méthode

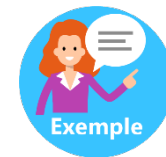


Une démarche adaptable selon l'objectif de l'étude



| Objectif de l'étude | Ateliers a conduire | | | | |
|--|---------------------|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Identifier le socle de sécurité adapté à l'objet de l'étude | | | | | |
| 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 de l'homologation d'un système | | | | | |

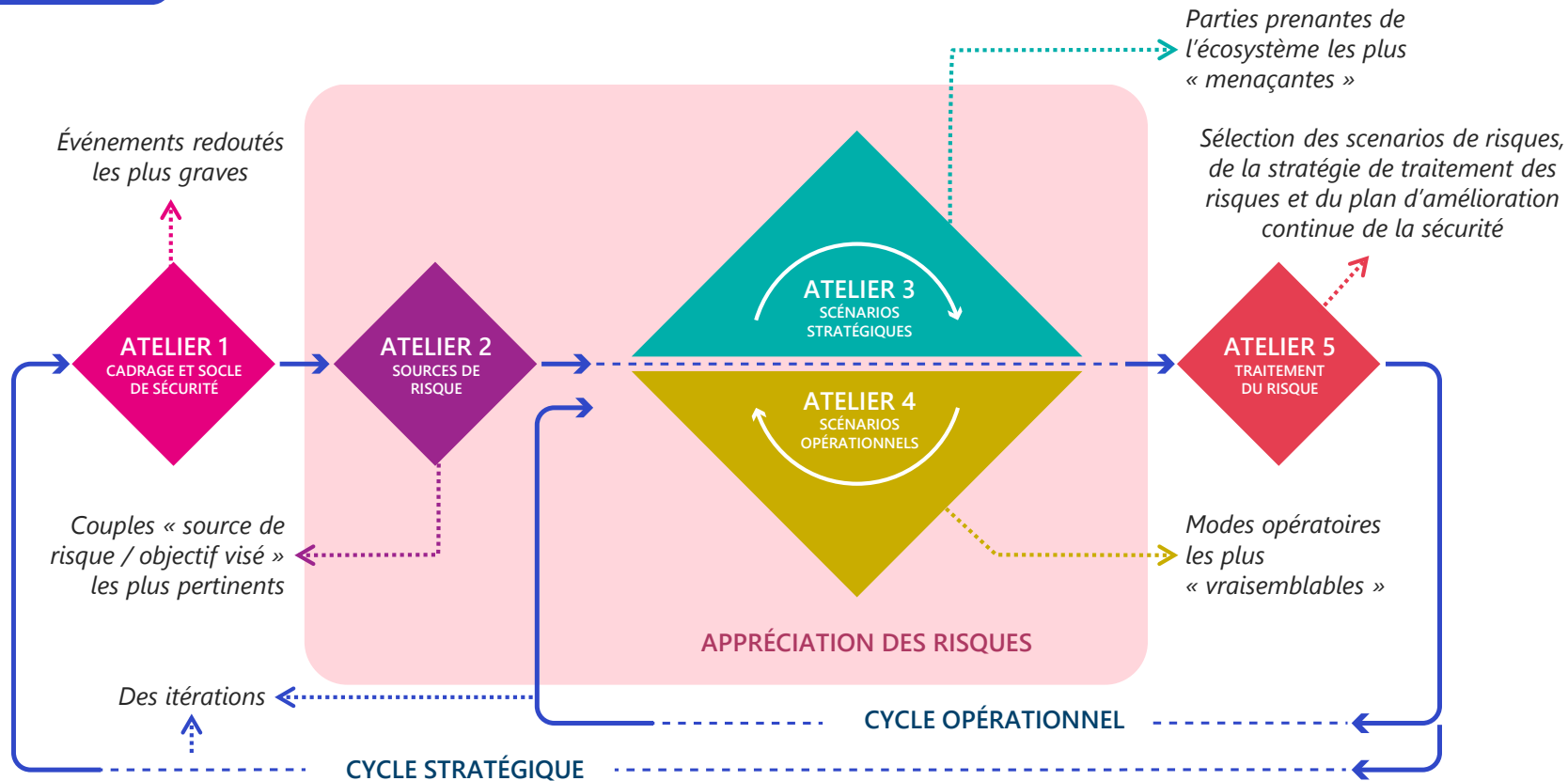
Une démarche adaptable selon l'objectif de l'étude



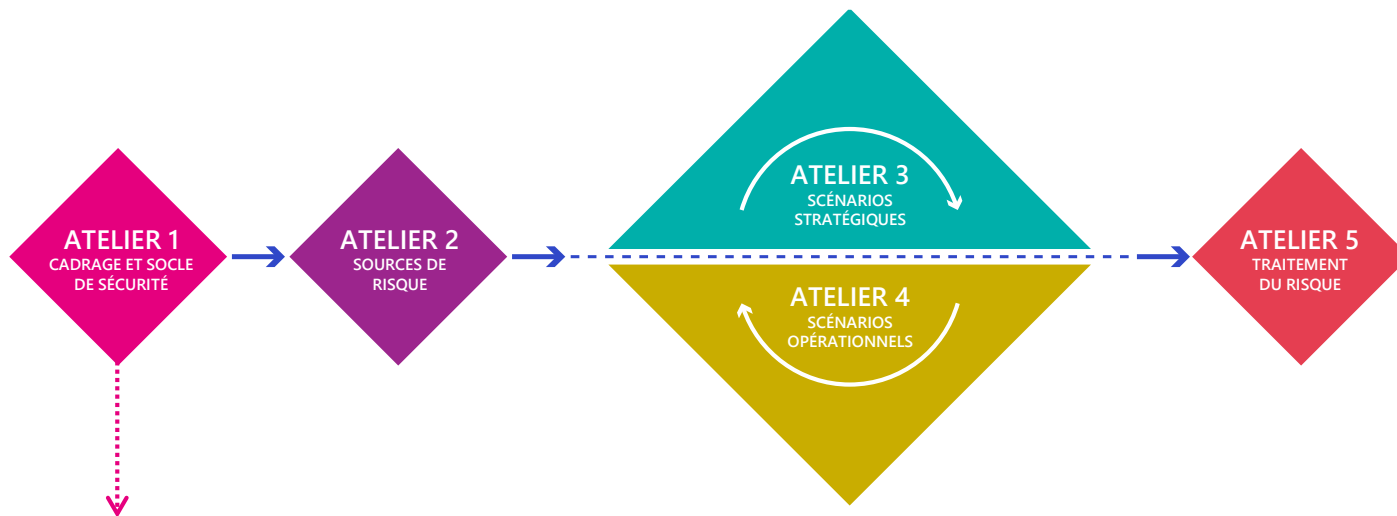
| Objectif de l'étude | Ateliers a conduire | | | | |
|--|---------------------|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Identifier le socle de sécurité adapté à l'objet de l'étude | X | | | | |
| Etre en conformité avec les référentiels de sécurité numérique | | | | | |
| Evaluer le niveau de menace 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 de l'homologation d'un système | | | | | |



Une approche efficace plutôt qu'exhaustive

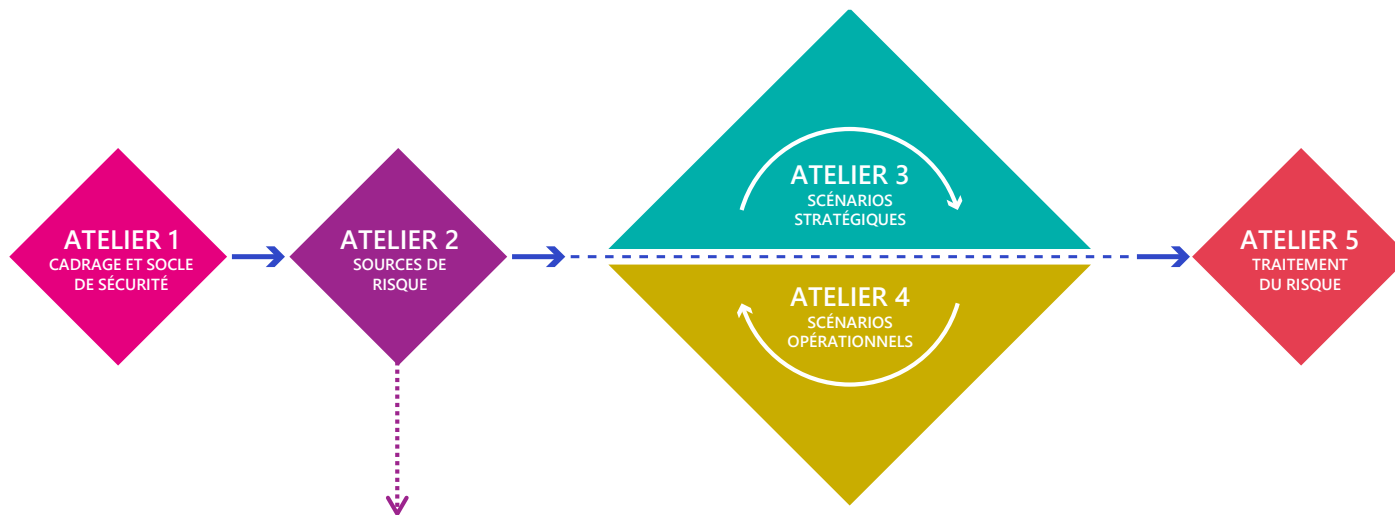


Chaque atelier va permettre de produire des éléments directement exploitables



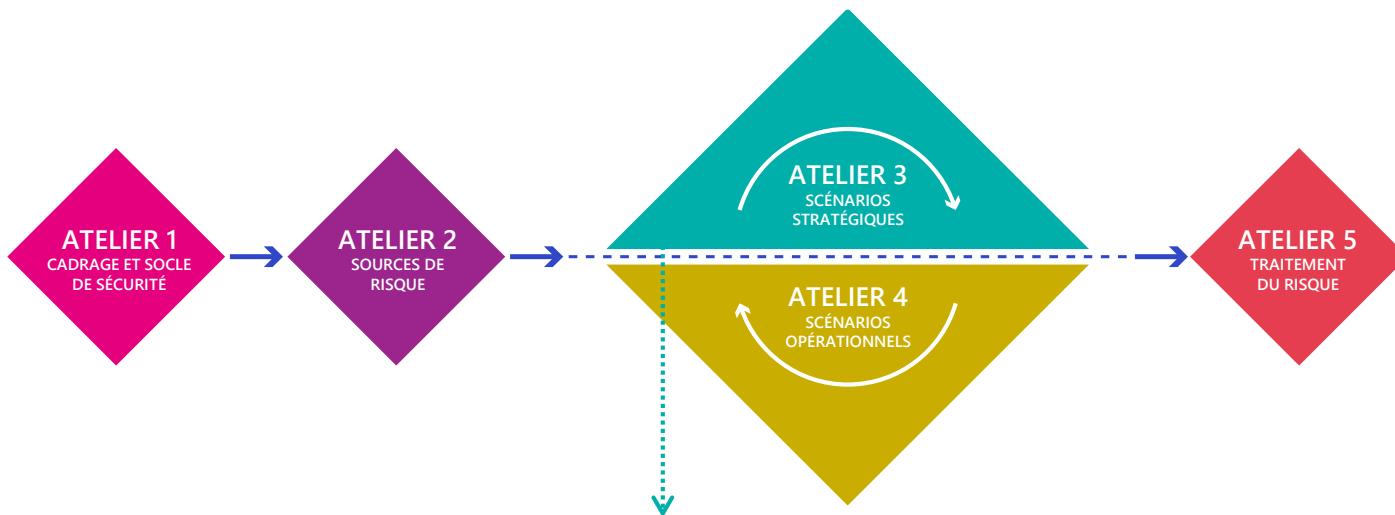
- La liste des actifs les plus importants
- La liste des événements redoutés
- Un socle de sécurité permettant d'identifier des mesures à mettre à place

Chaque atelier va permettre de produire des éléments directement exploitables



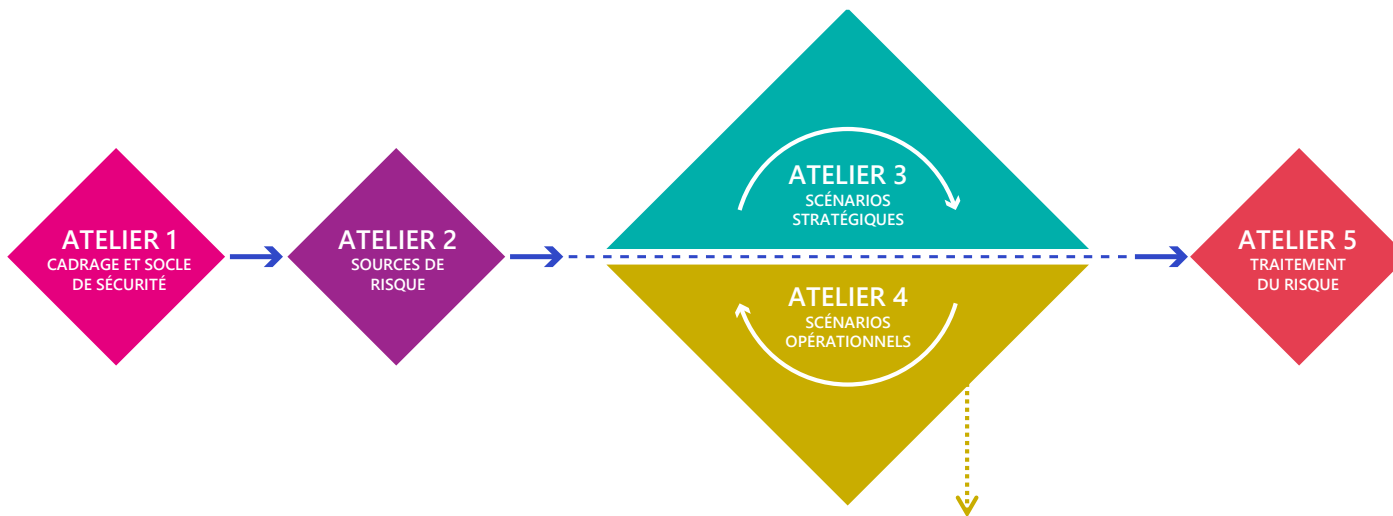
- La liste des attaquants susceptibles de vouloir nous attaquer
- La liste des cibles que les attaquants cherchent à atteindre

Chaque atelier va permettre de produire des éléments directement exploitables



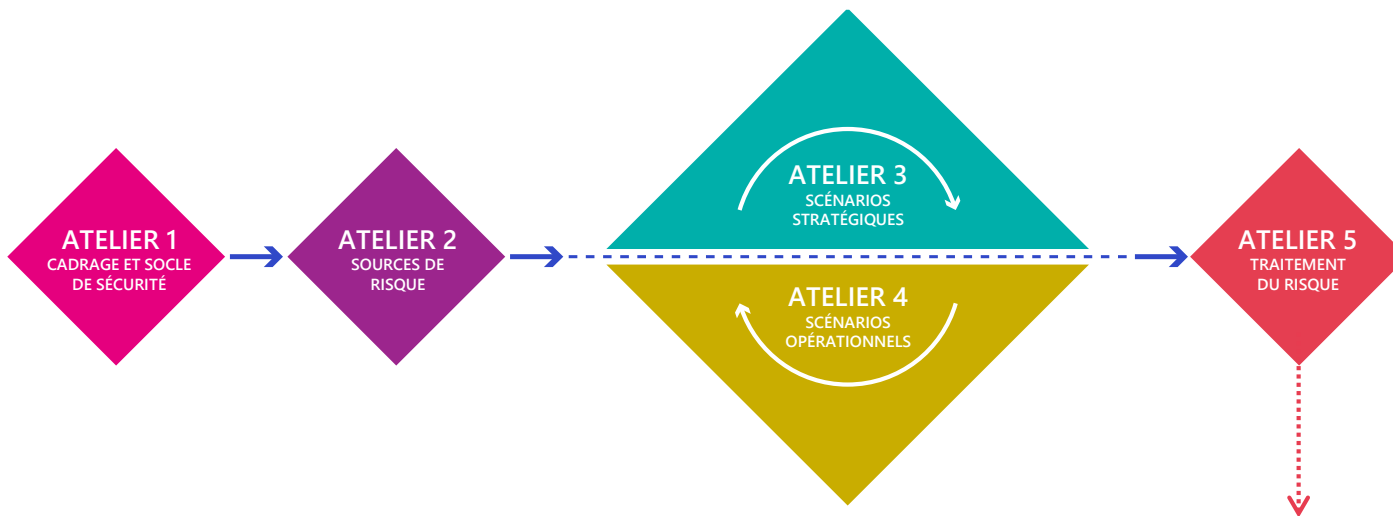
- La liste des parties prenantes les plus menaçantes
- Une liste de mesures à appliquer sur ces parties prenantes
- Des scénarios stratégiques d'attaque

Chaque atelier va permettre de produire des éléments directement exploitables



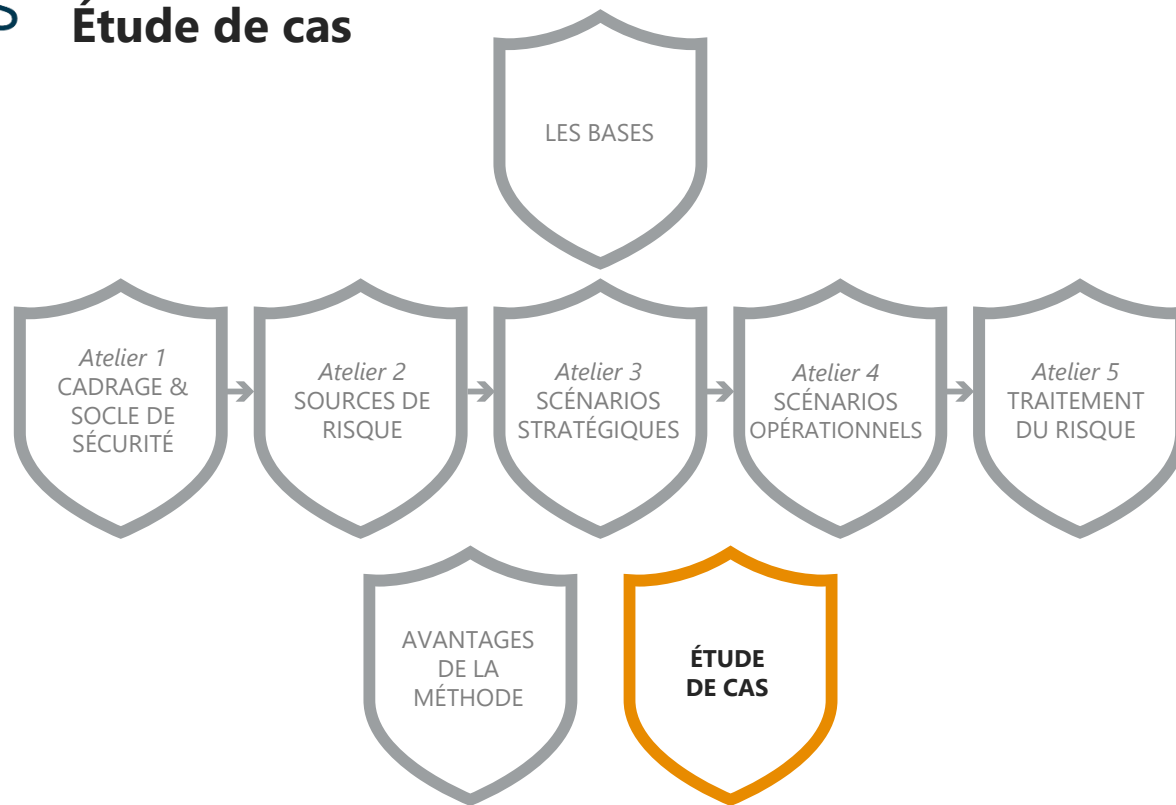
- La liste des modes opératoires les plus vraisemblables que pourraient suivre les attaquants pour atteindre leurs objectifs

Chaque atelier va permettre de produire des éléments directement exploitables



- La liste des risques résiduels
- La liste des mesures à appliquer

Étude de cas

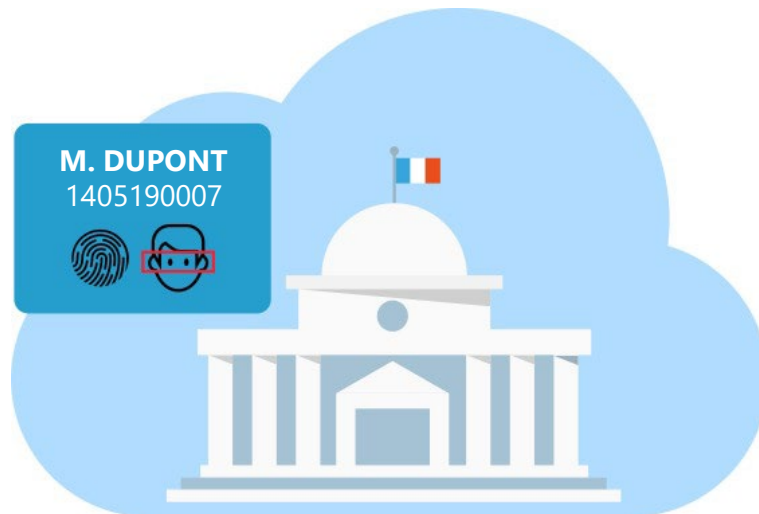


Présentation de l'étude de cas

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.



Présentation de l'étude de cas



Directeur de la SGTIN



Responsable métier



Responsable
des achats



RSSI



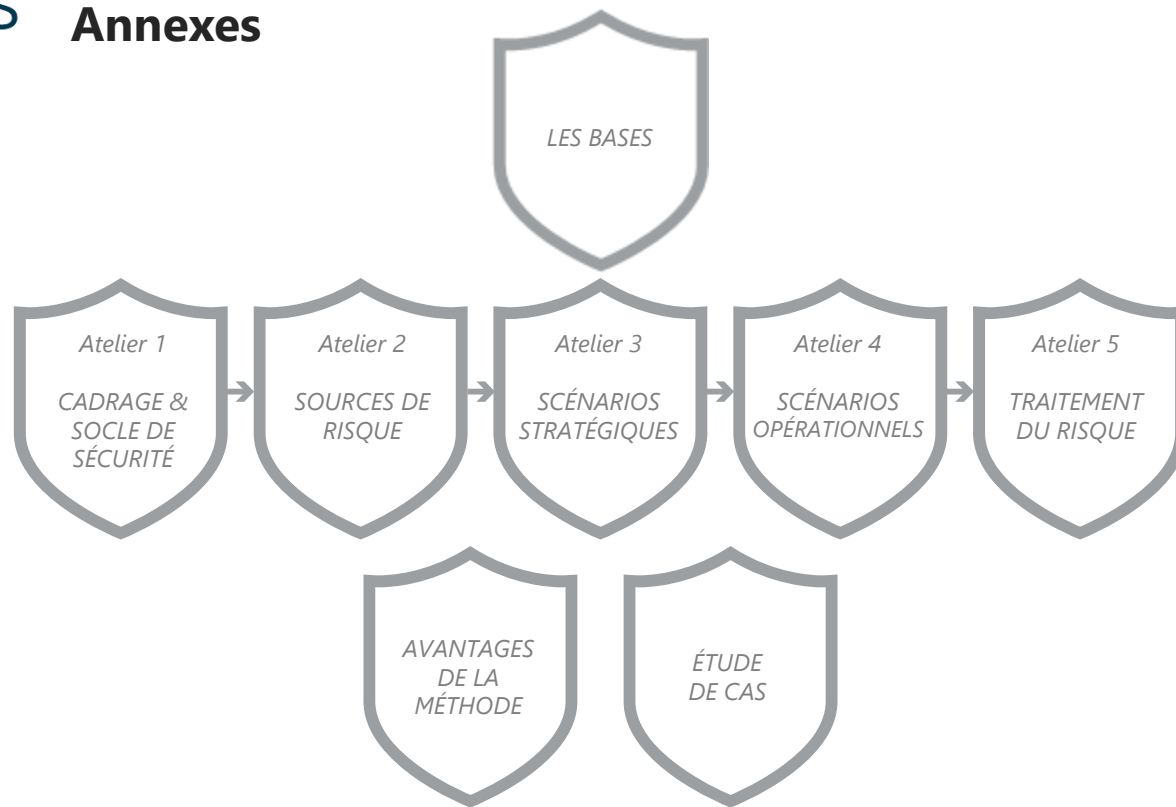
DSI

Répartition des rôles dans chaque équipe

- › Nombre d'équipes : 3
- › Nombre de personnes par
équipe 5



Annexes



F.A.Q.

Comment migrer d'une analyse de risque réalisée en EBIOS 2010 vers de l'EBIOS RM ?

- Des éléments ré-exploitable
- Quelques différences conceptuelles
- Éléments ré-exploitable partiellement
- Changement de vision

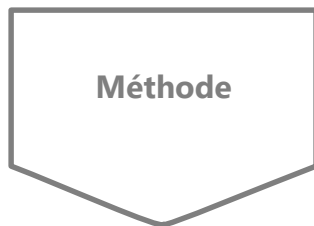




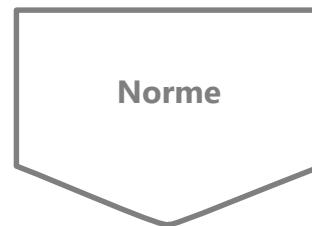
Compatibilité avec la norme ISO 27005:2022



EBIOS RM comme l'ISO 27005 présente une structuration de la notion de risque sécurité



Méthode



Norme





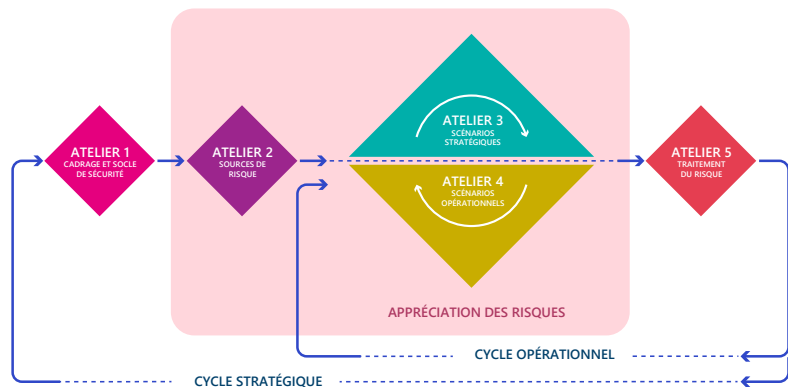
EBIOS RM vs ISO 27005:2022

Principes de bases



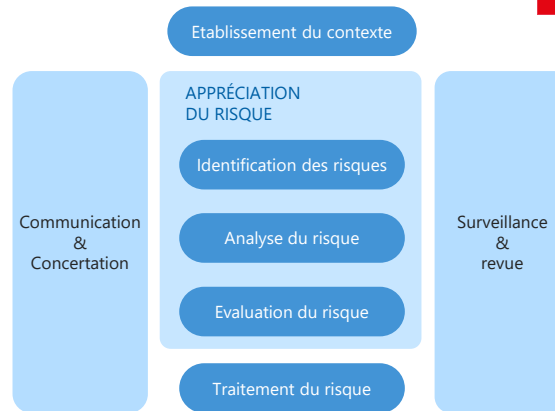
EBIOS RM vs ISO 27005:2022

Principes de bases



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 ?



5 Étapes

1. L'établissement du contexte
 2. L'identification des risques
 3. L'analyse du risque
 4. L'évaluation du risque
 5. Le traitement du risque
- Et 2 autres activités : la communication et la surveillance & revue.

Compatibilité d'EBIOS RM avec l'étape 1

Etablissement du contexte ISO 27005:2022

1. L'établissement du contexte

Identification des exigences de base des parties intéressées

⇒ ISO 27005 = EBIOS RM (Socle de sécurité)

Non-conformité

L'ensemble des non-conformités permettront d'avoir une vision claire de la maturité du périmètre

⇒ ISO 27005 = EBIOS RM

Conséquence

L'évaluation de la gravité se fait à travers les critères de conséquences et leurs criticités avec le niveau de magnitude

⇒ ISO 27005 (Conséquences) = EBIOS RM (Impacts)

Vraisemblance

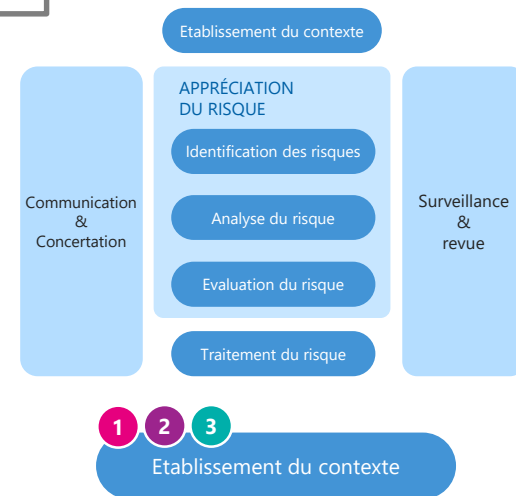
Utilisation d'échelles reposant sur des probabilités ou des fréquences

⇒ ISO 27005 = EBIOS RM (avec éventuellement une adaptation conformément aux recommandations de l'ISO)

Politique d'acceptation des risques

Evaluation de l'appétence au risque rarement spécifique à la sphère cyber

⇒ ISO 27005 = EBIOS RM



Compatibilité d'EBIOS RM avec l'étape 2

Identification des risques ISO 27005:2022



2. Identification des risques

Processus consistant à rechercher, reconnaître et décrire les risques



Atelier 1 : identification des événements redoutés

Atelier 2 : sélection des couples SR/OV les plus pertinents

Atelier 3 : création du lien entre ER, SR et VM

Résultat : la combinaison de ces éléments permet de faire apparaître des scénarios de risque → atteinte de l'objectif fixé par l'ISO 27005.

But : détermination des sources et de ce qui peut se produire

Résultat : une liste de risques.

Il est à noter une différence majeure de sémantique

Ebios RM ne s'intéresse qu'aux sources intentionnelles (le socle de sécurité couvre le reste).

ISO 27005 intègre explicitement les sources non intentionnelles.

Ainsi que la distinction suivante :

Ebios RM **ne dissocie pas** l'objectif à court terme de l'attaquant et son objectif à long terme (EFR).

ISO 27005 **distingue** l'objectif à court terme de l'attaquant et son objectif à long terme (EFR).

Compatibilité d'EBIOS RM avec l'étape 2

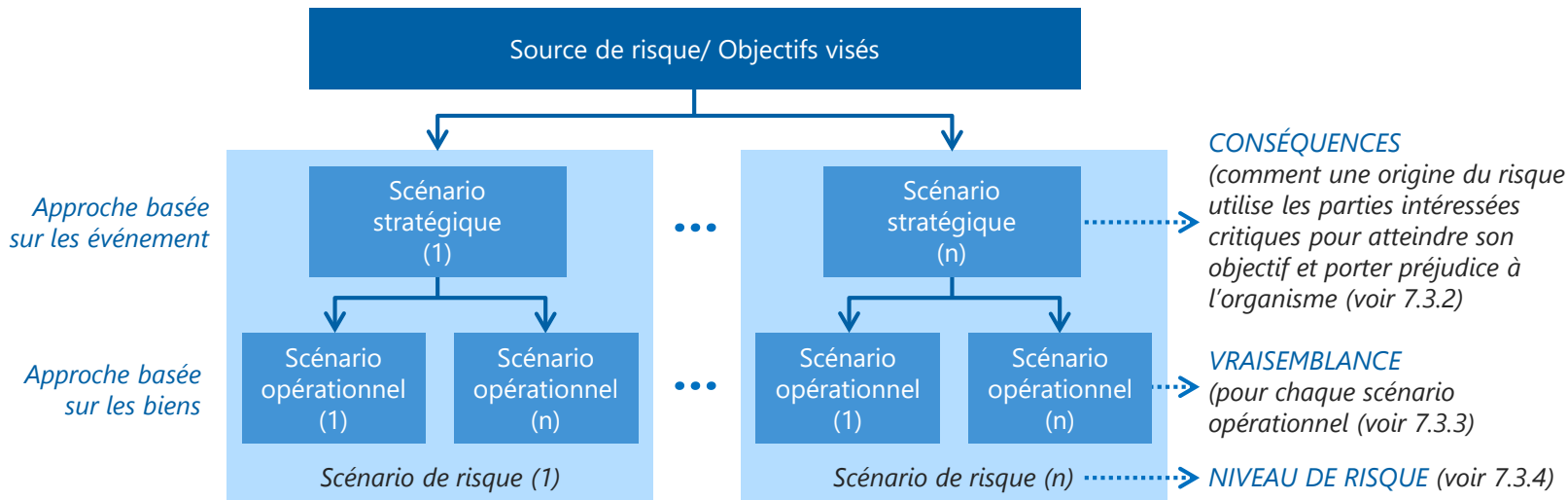
Identification des risques ISO 27005:2022

2. Identification des risques



L'ISO 27005 identifie deux approches possibles pour l'identification des risques basée sur :

- Les événements et intégrant l'écosystème
- Les biens supports

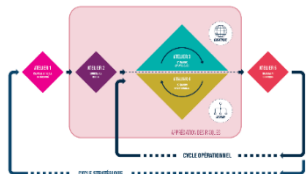
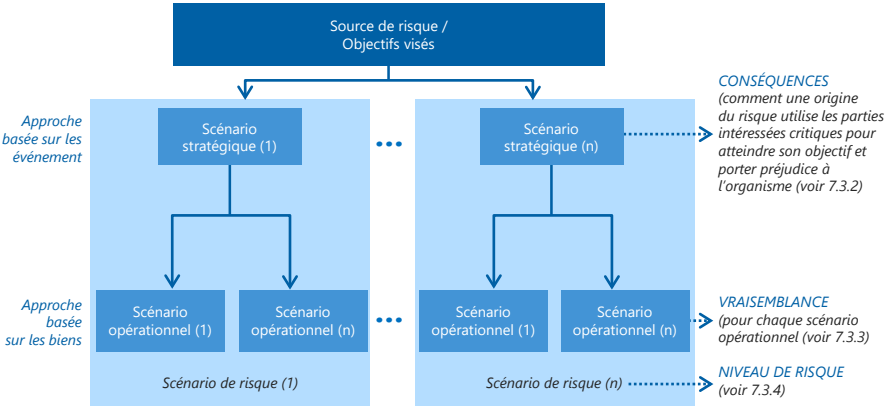
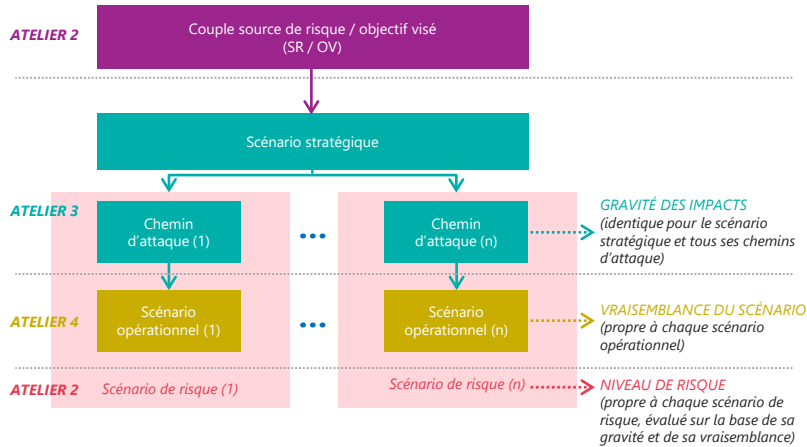


Compatibilité d'E BIOS RM avec l'étape 2

Identification des risques ISO 27005:2022



2. Identification des risques



Compatibilité d'EBIOS RM avec les étapes 3 et 4

Analyse et évaluation du risque ISO 27005:2022

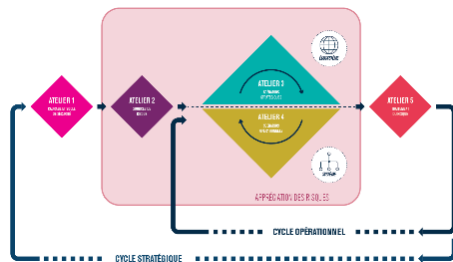


3. Analyse du risque
4. Évaluation du risque



- Atelier 2 : volonté de passage à l'acte (pertinence)
- Atelier 1 (3) : gravité
- Atelier 4 : vraisemblance
- Atelier 5 : placement de chaque risque sur une matrice d'acceptation du risque, où chaque cellule reflète ces critères.

- Évaluation, à travers un ensemble de critères déterminés en amont, des risques identifiés.
- Ces valeurs permettront ensuite de classer le risque, en le confrontant aux critères d'acceptation du risque, définis par l'organisme



Compatibilité d'EBIOS RM avec l'étape 5

Traitement du risque ISO 27005:2022



5. Traitement du risque

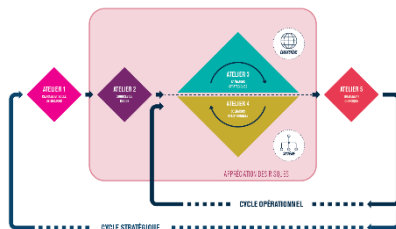


Propose un traitement général du risque lors de la dernière étape :

1. Simplifie le choix de l'option de traitement, en priorisant en fonction des niveaux de risque la réduction ou l'acceptation.
2. Production documentaire qui peut être faite à partir des résultats obtenus dans chaque atelier.
3. Formaliser un plan de traitement du risque
4. Accepter les risques

Propose un traitement général du risque décomposé en plusieurs étapes :

1. Choisir l'option de traitement, en partant du principe que la réduction est l'option prioritaire
2. Préparer une déclaration d'acceptabilité (DdA), en lien avec l'annexe A de l'ISO 27001
3. Formaliser un plan de traitement du risque
4. Accepter les risques résiduels



Compatibilité d'EBIOS RM avec les process transverses

Communication & Surveillance ISO 27005:2022



Process transverses : communication et surveillance

Communication

La communication est bien présente, mais n'est pas identifiée comme une activité spécifique, c'est un travail de fond, intégré à chaque atelier.

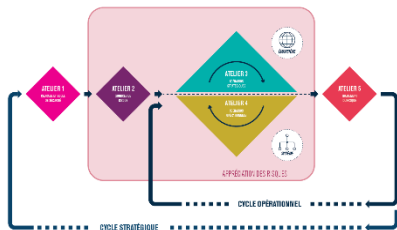
Informations sur les risques, leurs causes, leurs conséquences, leurs vraisemblances et les moyens de maîtrise mis en œuvre pour les traiter sont communiqués [...] aux parties intéressées ».



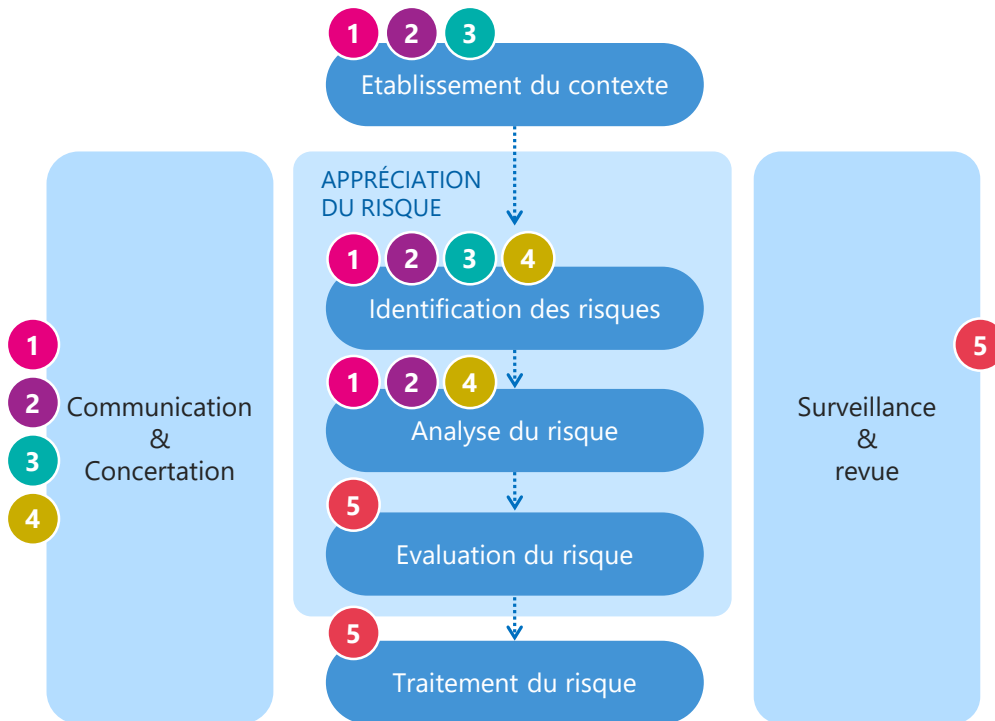
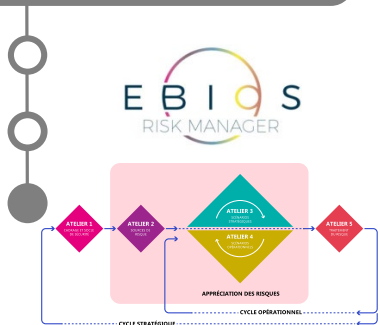
Surveillance

Le process de surveillance est directement implémenté dans EBIOS RM.

Les déclencheurs (ISO 27005) ont leur équivalents avec l'initiation des cycles opérationnels et stratégiques.



Compatibilité d'EBIOS RM avec ISO 27005:2022



EBIOS RM vs ISO 27005:2022

Pierre de Rosette



| EBIOS RM | ISO 27005 |
|------------------------------|--------------------------------|
| Partie prenante | Partie intéressée |
| Cadrage et socle de sécurité | Etablissement du contexte |
| Scénario stratégique | Approche par événements |
| Scénario opérationnel | Approche par les biens support |
| Évènement redouté | Conséquence |
| Évènement intermédiaire | Conséquence intermédiaire |
| Valeur métier | Bien primaire |
| Bien support | Bien support |
| Source de risque | Source de risque |
| Niveau de Menace | Niveau de danger |
| Impact | Critères de conséquences |
| Besoin de sécurité | Objectif de sécurité |
| Gravité | Gravité |
| N/A | Déclencheur |