Formation – CFSSI

1er semestre 2019

Avant de commencer…

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

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

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

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

Programme

EBIOS *Risk Manager* : les bases

Atelier 1 : cadrage et socle de sécurité

Atelier 2 : sources de risque

Atelier 3 : scénarios stratégiques

Atelier 4 : scénarios opérationnels

Atelier 5 : traitement du risque

Étude de cas

Qu’est-ce qu’un risque ?

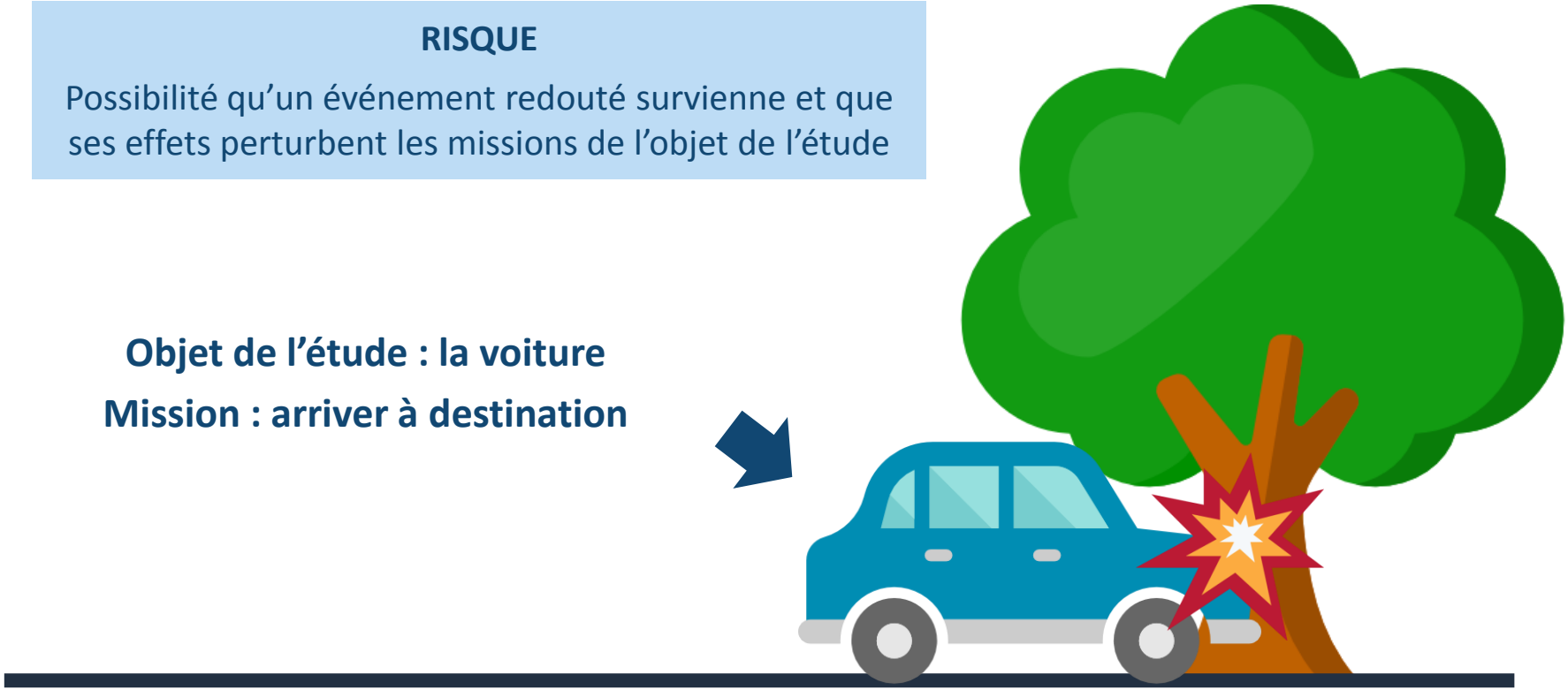
Qu’est-ce qu’un risque ?

RISQUE

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

Objet de l’étude : la voiture

Mission : arriver à destination



Événement redouté : la voiture percute un arbre

Quelle est la gravité de ce risque ?

La gravité varie selon la vitesse de la voiture

La gravité varie également selon la taille de l'arbre

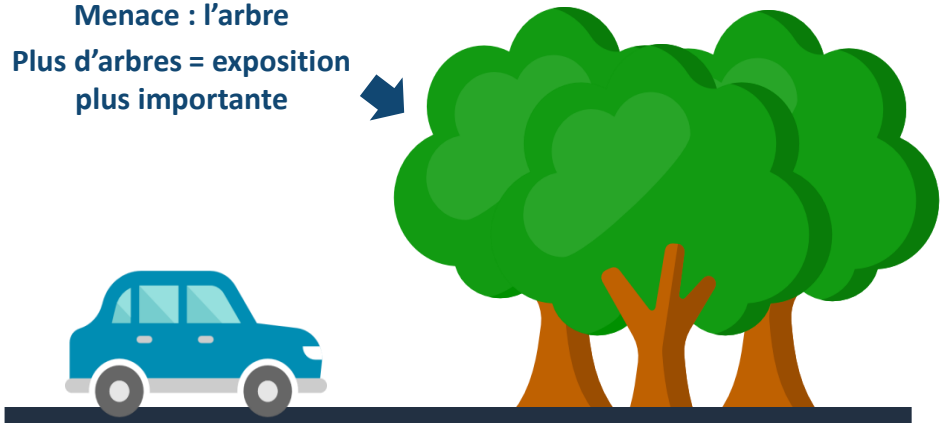
La gravité varie selon la valeur (prix, robustesse) de la voiture

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

Quelle est la vraisemblance de ce risque ?

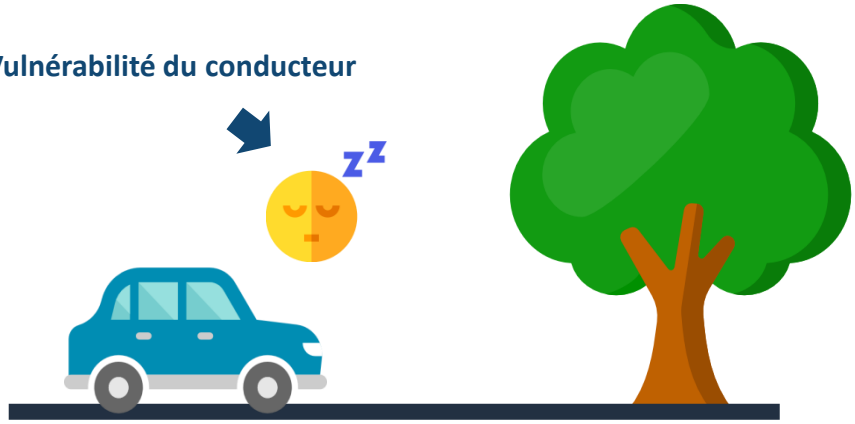
Menace : l'arbre

Plus d'arbres = exposition plus importante



La vraisemblance varie selon le nombre d'arbres

Vulnérabilité du conducteur



La vraisemblance varie selon le niveau d'attention du conducteur

Mesure de sécurité

La vraisemblance varie selon les panneaux de signalisation en place

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

Comment évaluer le niveau d'un risque ?

NIVEAU DE RISQUE (EBIOS *RISK MANAGER*)

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

GRAVITÉ

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

VRAISEMBLANCE

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

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

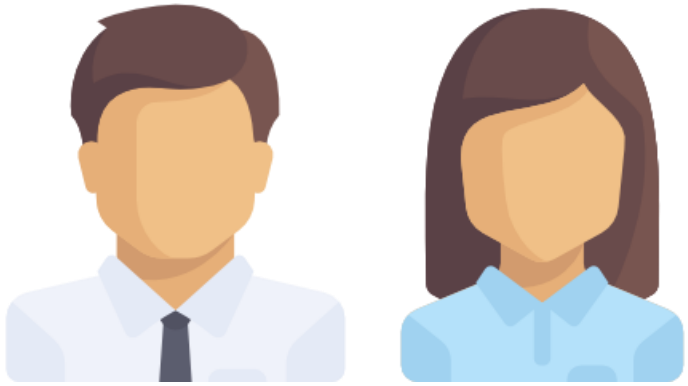
Quelques questions à se poser

Quel est mon degré d'exposition à ces risques ?

Comment maitriser ces risques pour les rendre tolérables ou acceptables ?

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

Comment gérer les risques dans le temps ?



Carte d'identité de la méthode EBIOS *Risk Manager*

UTILISATEURS

Risk managers

RSSI

Chefs de projet

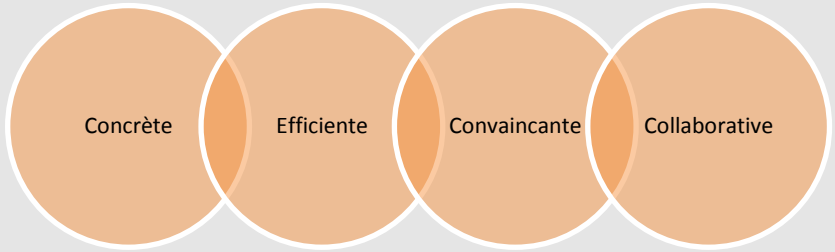
VISION

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

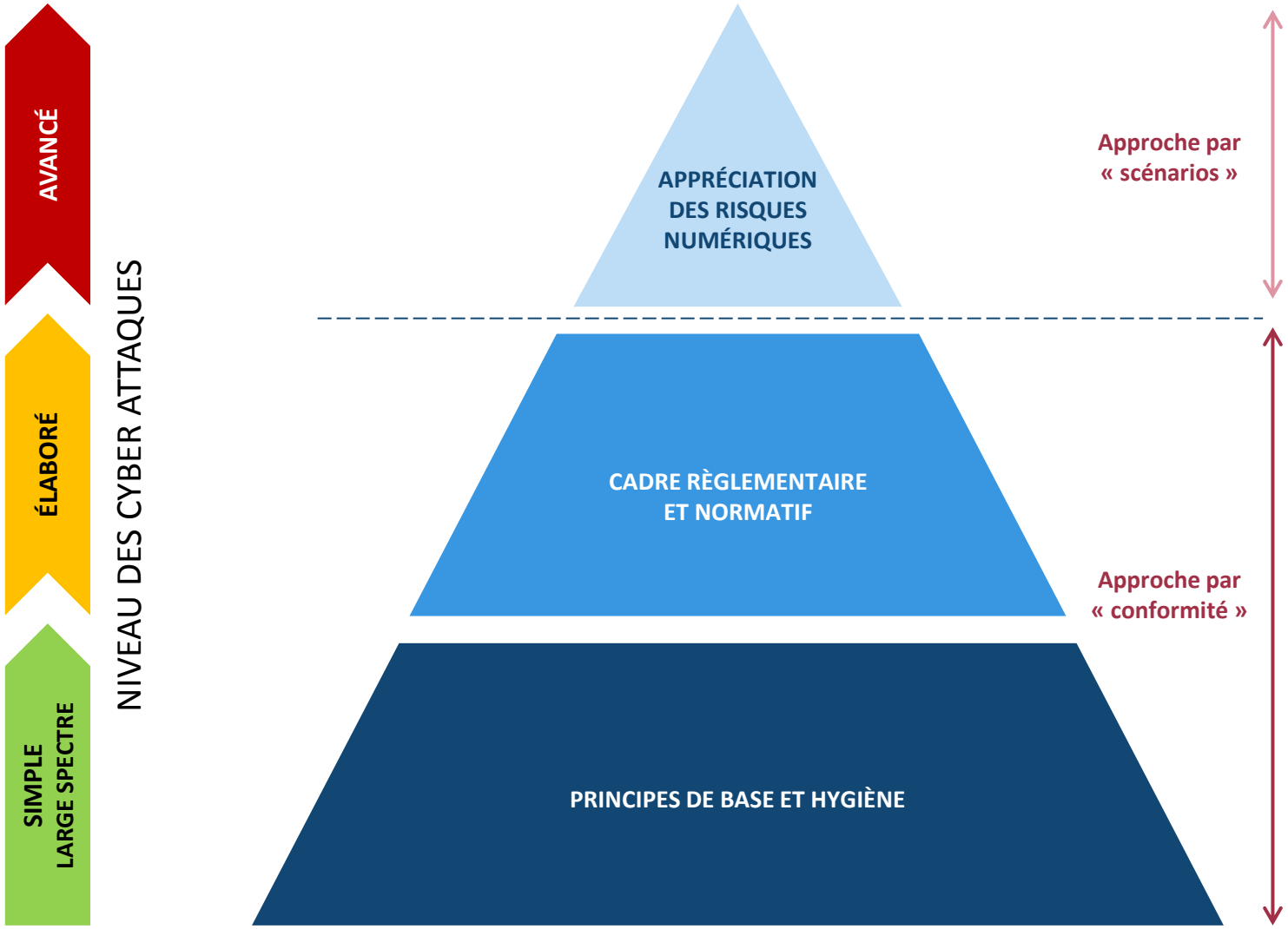
FONDAMENTAUX

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

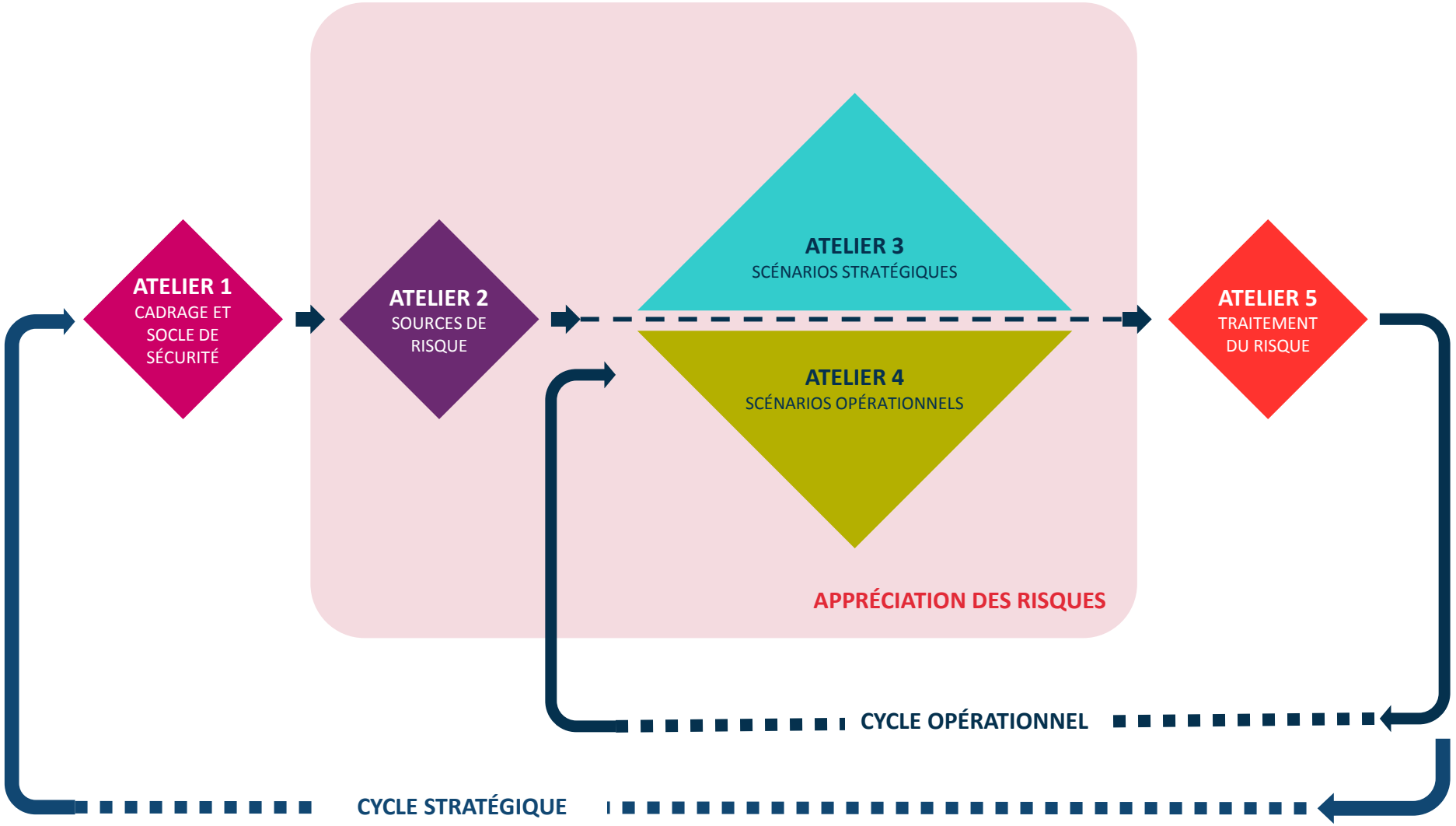
VALEURS



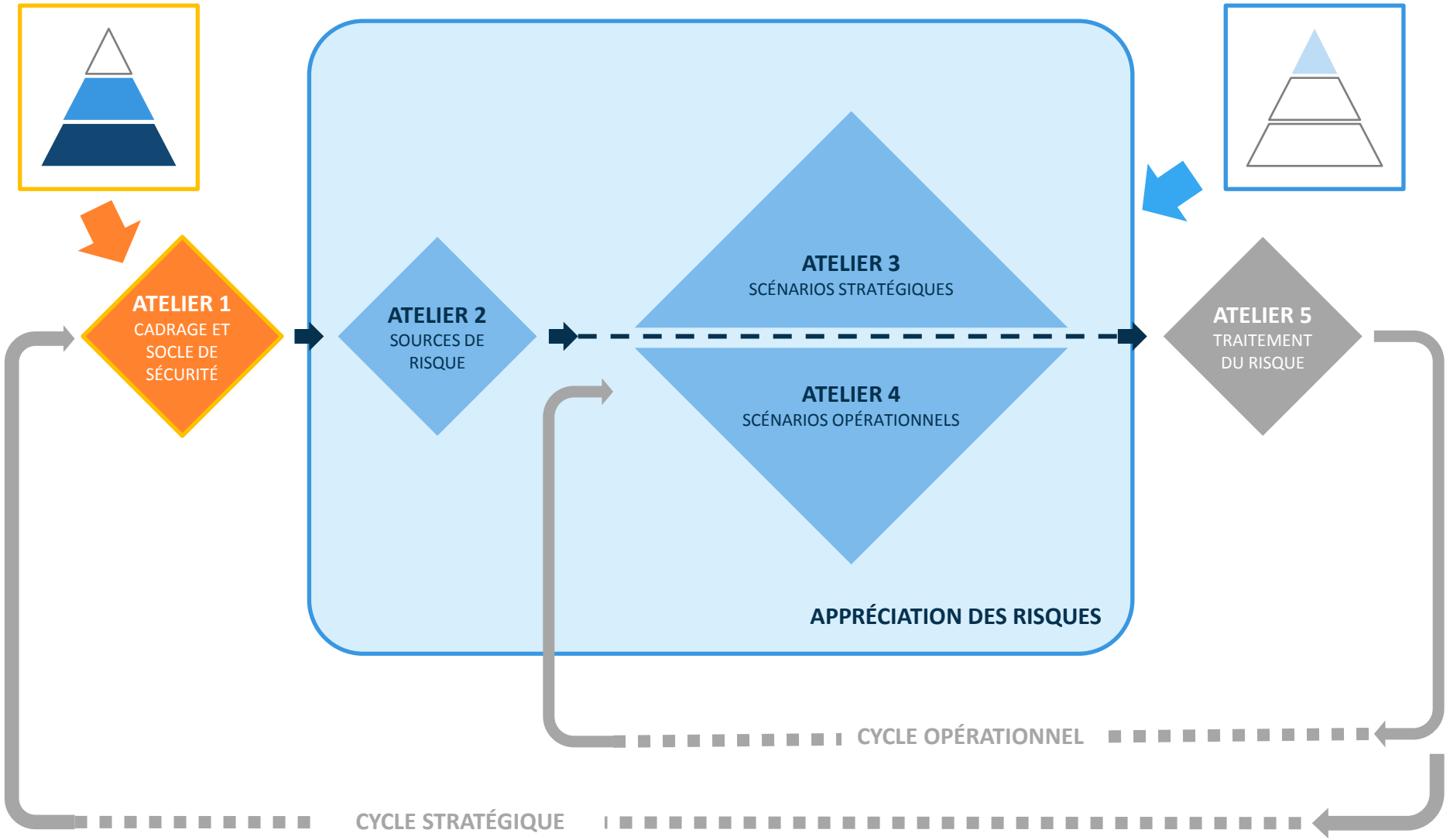
La pyramide du management du risque : le concept phare de EBIOS *Risk Manager*



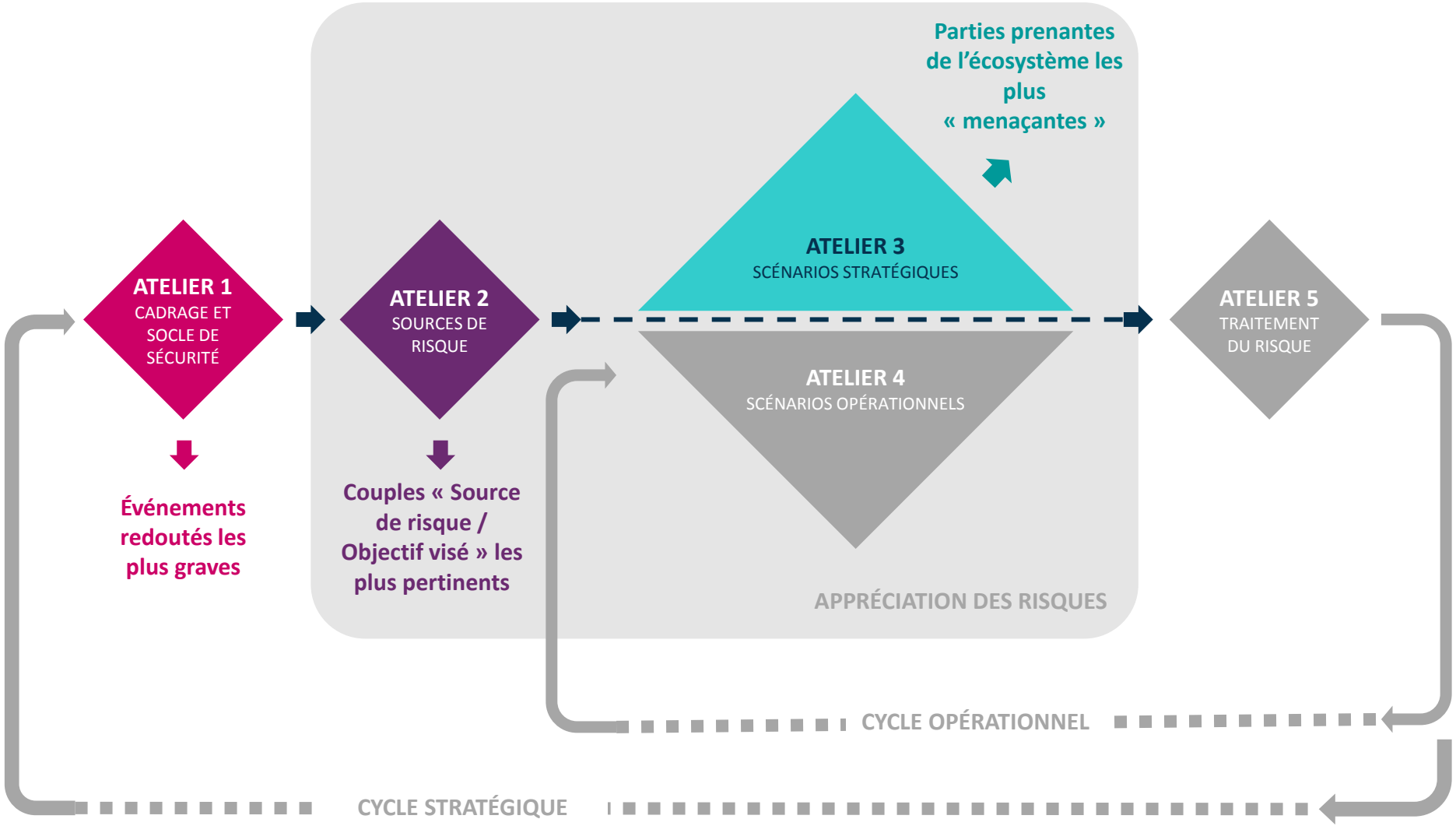
EBIOS *Risk Manager* : une méthode basée sur 5 ateliers



EBIOS *Risk Manager* - Pyramide de management du risque



EBIOS *Risk Manager* : des choix à chaque étape



Programme

- EBIOS Risk Manager : les bases
- **Atelier 1 : cadrage et socle de sécurité**
- Atelier 2 : sources de risque
- Atelier 3 : scénarios stratégiques
- Atelier 4 : scénarios opérationnels
- Atelier 5 : traitement du risque
- Étude de cas

Un peu de vocabulaire pour commencer

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

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

[Sources Internet : Le Point.fr et ZDNet]

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

A1

Atelier 1 : cadrage et socle de sécurité

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

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

PARTICIPANTS : Direction, Métiers, RSSI, DSI

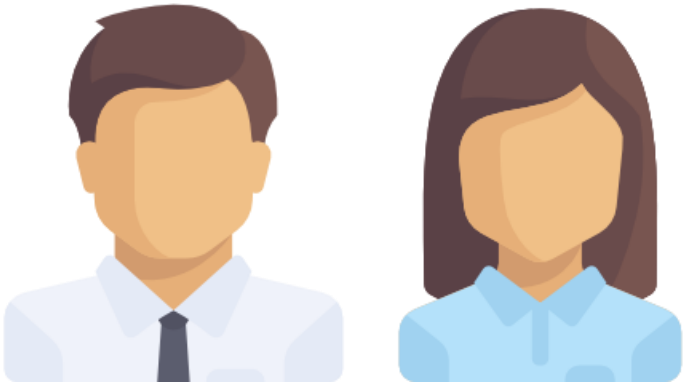
A1

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

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

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

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



A1

Cas fictif – société de biotechnologies

SOCIÉTÉ DE BIOTECHNOLOGIE FABRIQUANT DES VACCINS

- Estimation d'un niveau de maturité faible en matière de sécurité du numérique
- Sensibilisation basique à la sécurité du numérique à la prise de poste des salariés
- Existence d'une charte informatique

A1

Définir le périmètre métier et technique

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

A1

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

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

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

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

Considérer des ensembles d'informations plutôt que des informations isolées

5 à 10 valeurs métiers constituent généralement une base suffisante

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

A1

Identifier les événements redoutés

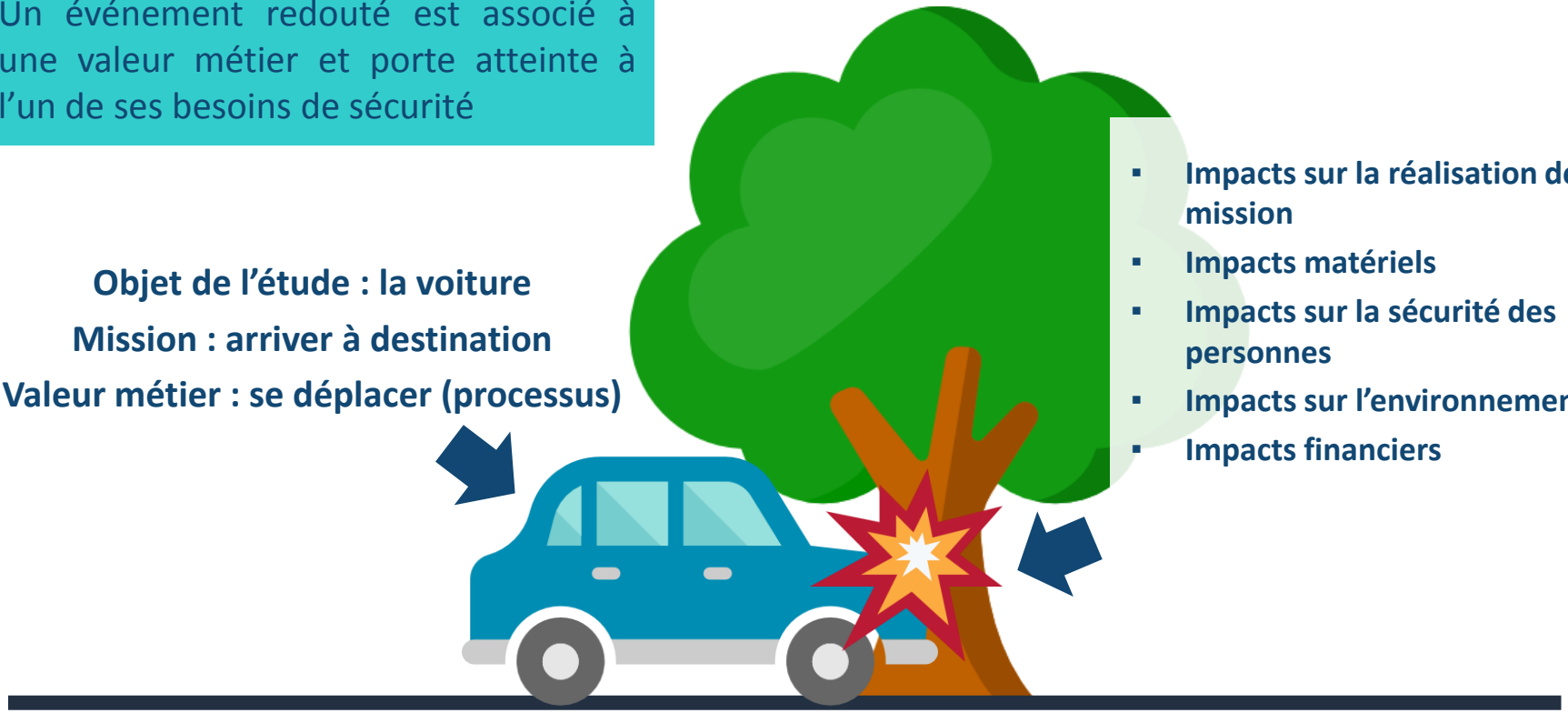
ÉVÉNEMENT REDOUTÉ

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

Objet de l'étude : la voiture

Mission : arriver à destination

Valeur métier : se déplacer (processus)



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

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

A1

Définir une échelle de gravité

ÉCHELLE	DÉFINITION
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)
G3 – GRAVE	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)
G2 – SIGNIFICATIVE	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)
G1 – MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges)

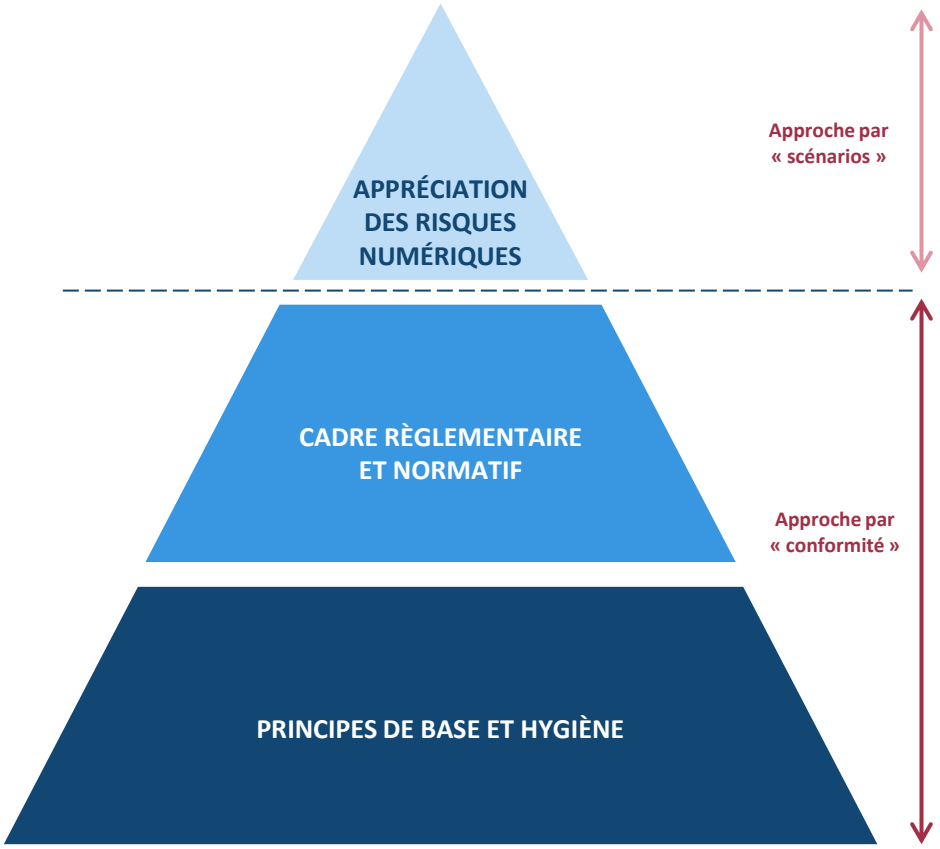
Il est recommandé de reprendre une échelle de gravité déjà définie dans l'organisation ou lors de l'étude des risques précédente

Identifier les événements redoutés

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIES D'IMPACT	GRAVITÉ
R&D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée	• 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	• Impacts sur le patrimoine intellectuel • Impacts financiers	3
	Perte ou destruction des informations d'études et recherches	• 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	• Impacts sur les missions et services de l'organisme • Impacts financiers	2
Fabriquer des vaccins	Interruption de la production ou de la distribution de vaccins pendant plus d'une semaine pendant un pic d'épidémie	• Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts financiers	4
	Fuite du savoir-faire de l'entreprise concernant le processus de fabrication des vaccins et de leurs tests qualité	• Impacts financiers	2
Traçabilité et contrôle	Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire	• Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts juridiques	4

A1

Déterminer le socle de sécurité



SOCLE DE SÉCURITÉ
APPROCHE PAR « CONFORMITÉ »

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

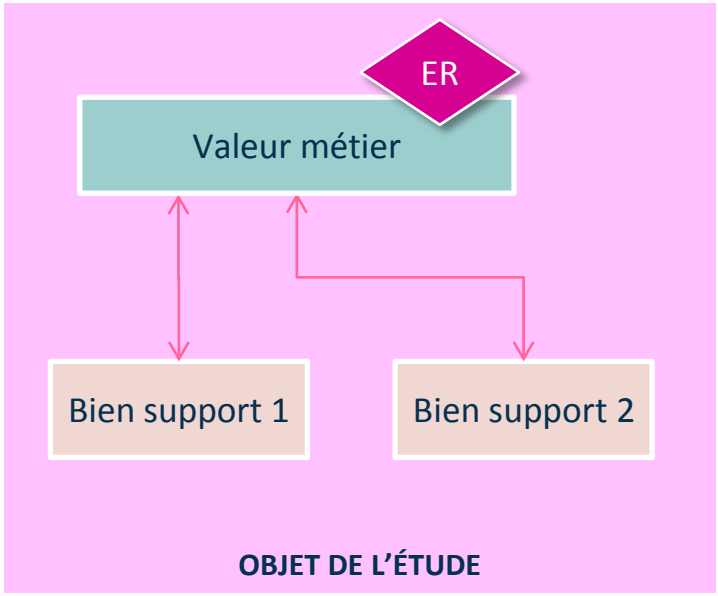
- **Bonnes pratiques de sécurité** : guides de recommandations de l'ANSSI, règles de sécurité internes à l'organisation (PSSI), etc.
- **Normes** : famille ISO 27000, etc.
- **Règlementations en vigueur** : IGI 1300, II 901, LPM, directive NIS, RGS, etc.

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

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

A1

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



Légende :

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

Programme

- EBIOS Risk Manager : les bases
- Atelier 1 : cadrage et socle de sécurité
- **Atelier 2 : sources de risque**
- Atelier 3 : scénarios stratégiques
- Atelier 4 : scénarios opérationnels
- Atelier 5 : traitement du risque
- Étude de cas

A2

Atelier 2 : sources de risque

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

ÉLÉMENTS EN ENTRÉE :

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

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

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

Petit point sur l'actualité

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

Source : Libération – 04/01/2019

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

Source : Datanews – 01/08/2018

ACCUEIL › HIGH-TECH

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

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

Source : 20 minutes – 30/11/2018

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

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

Au total, plus de 19,2 millions d'euros auraient ainsi été dérobés à l'entreprise en mars 2018. Les faits n'ont été révélés publiquement que lors du procès opposant l'ex-employé incriminé à son entreprise dans le cadre de son licenciement. Selon Pathé, il aurait « *négligé des signaux* » qui auraient dû l'alerter du caractère frauduleux des opérations.

Source : Next inpact – 12/11/2018

A2

Comment évaluer la pertinence des couples SR/OV ?

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

DEGRÉ DE PERTINENCE D'UN COUPLE SR/OV

Évaluer les couples SR/OV et sélectionner les plus pertinents

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

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

A2

Quelle gravité pour mon scénario stratégique ?

ER les plus graves

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

SR/OV les plus pertinents

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

A2

Récapitulons le vocabulaire que nous avons vu

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

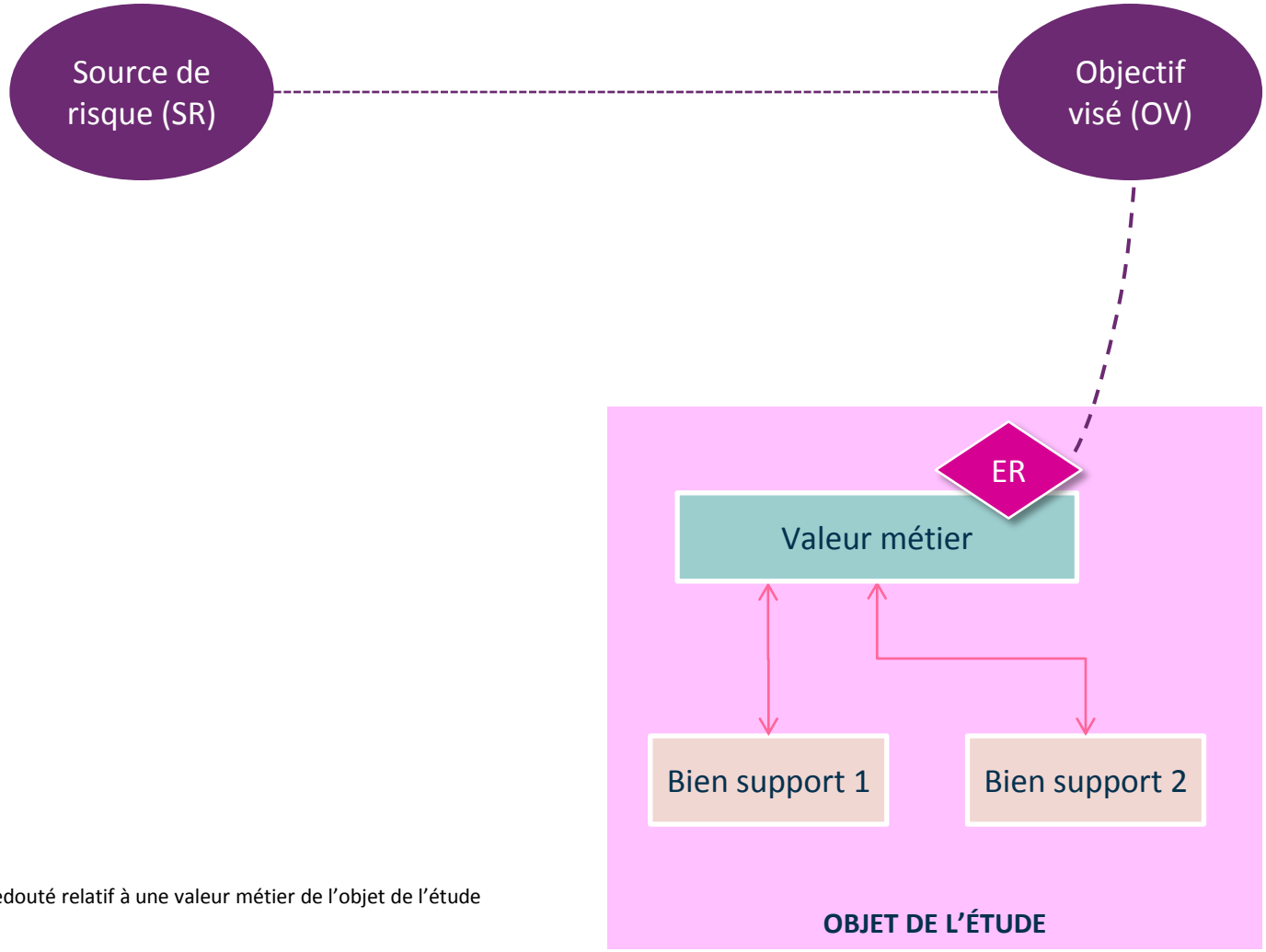
Un adolescent de quinze ans a été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires. Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité pendant quatre jours.

[Sources Internet : Le Point.fr et ZDNet]

	PREMIÈRE ATTAQUE	SECONDE ATTAQUE
Source de risque	Adolescent	Adolescent
Objectif visé	Modifier ses résultats scolaires	Se venger du collège
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
Valeur métier	Résultats scolaires	Échanger des informations
Bien support	Système informatique de gestion des résultats scolaires	Service informatique d'échange de courriels
Impacts	• 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

A2

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



Légende :

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

Programme

- EBIOS Risk Manager : les bases
- Atelier 1 : cadrage et socle de sécurité
- Atelier 2 : sources de risque
- **Atelier 3 : scénarios stratégiques**
- Atelier 4 : scénarios opérationnels
- Atelier 5 : traitement du risque
- Étude de cas

A3

Atelier 3 : scénarios stratégiques

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

ÉLÉMENTS EN ENTRÉE :

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

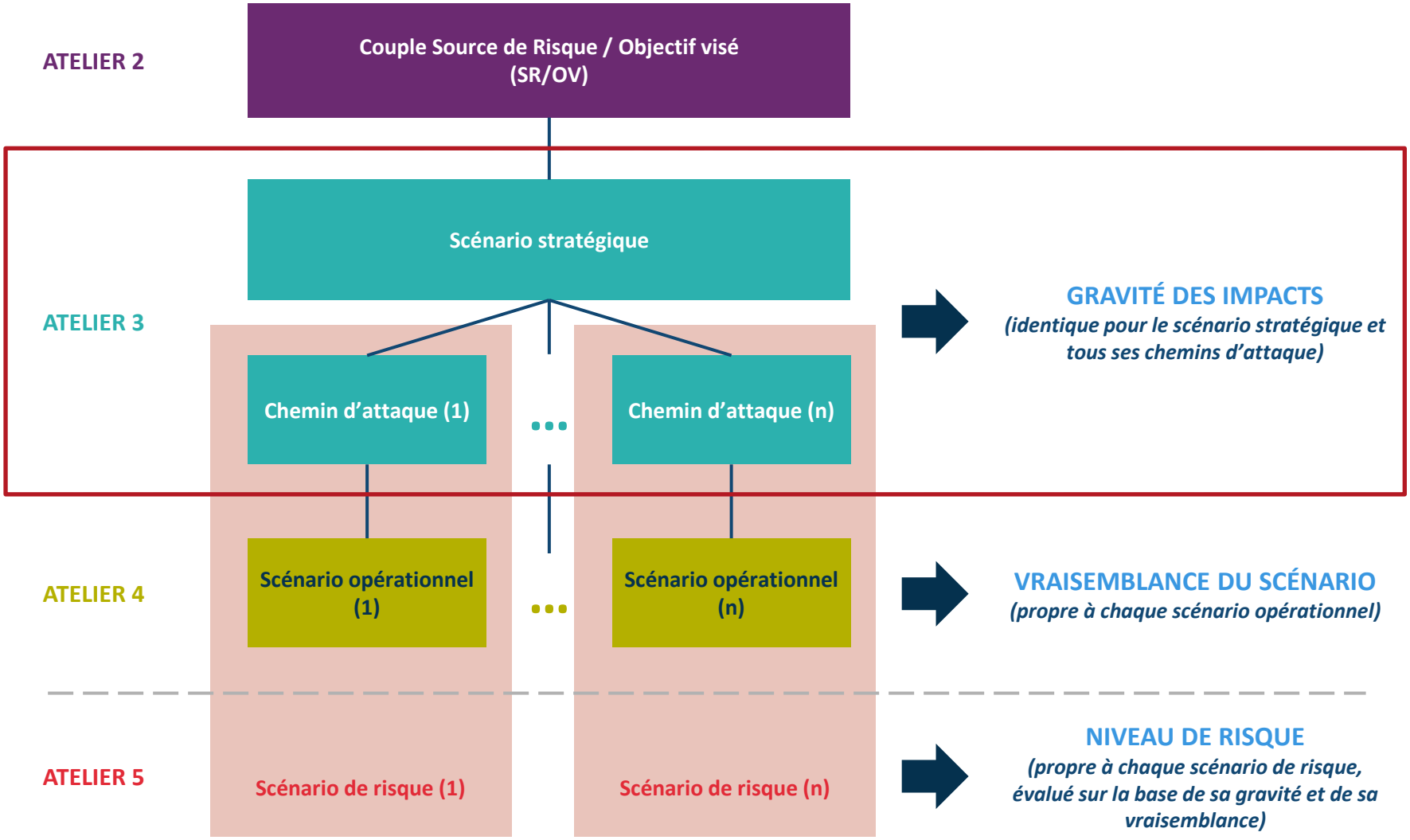
ÉLÉMENTS EN SORTIE :

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

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

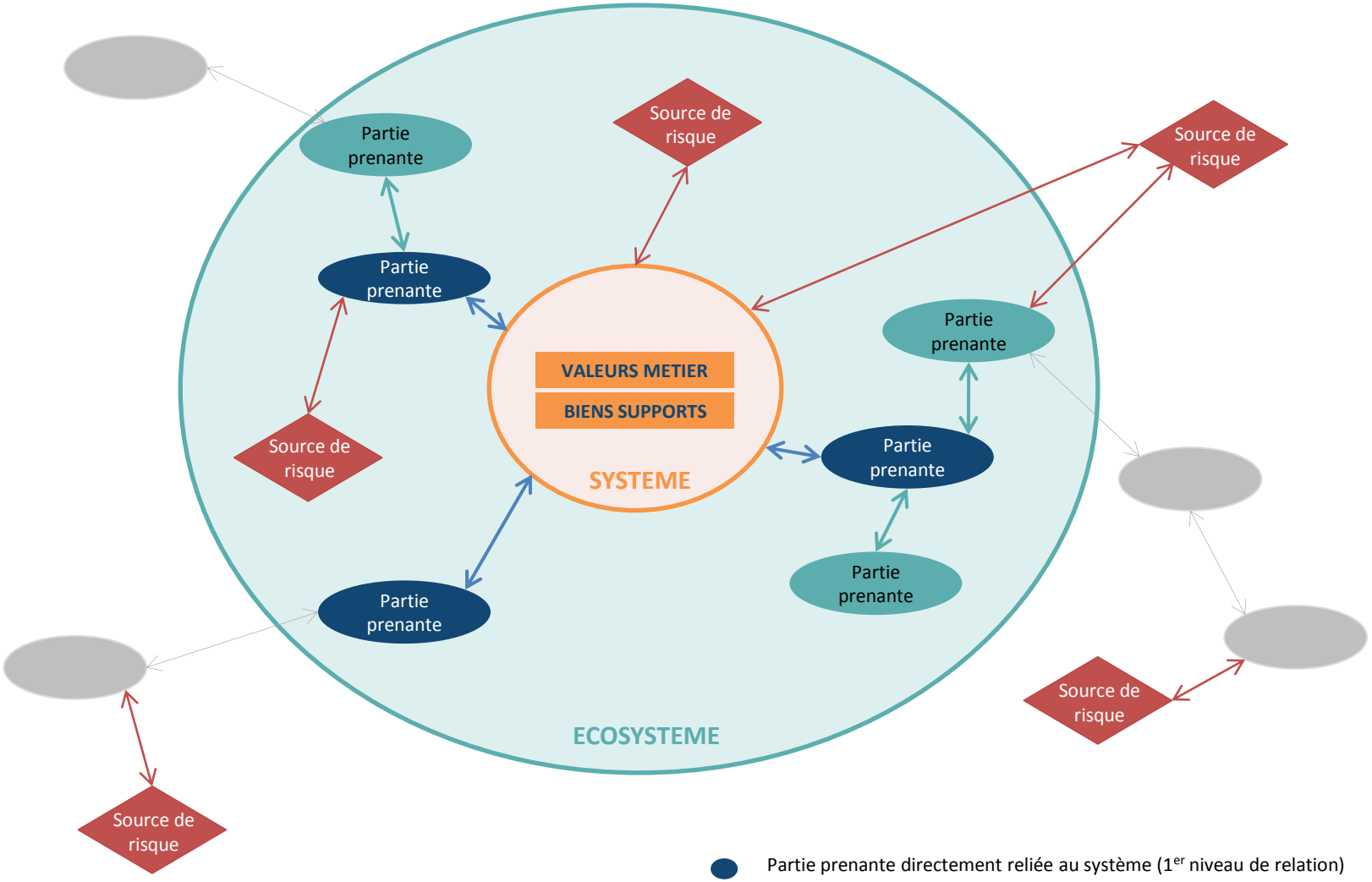
A3

Articulation des différents ateliers



A3

Identifier les parties prenantes de l'écosystème



Construire la cartographie de menace de l'écosystème

Pour chaque partie prenante, évaluer 4 critères :

EXPOSITION

Dépendance
La relation avec cette partie prenante est-elle vitale pour mon activité ?

Pénétration
Dans quelle mesure la partie prenante accède-t-elle à mes ressources internes ?

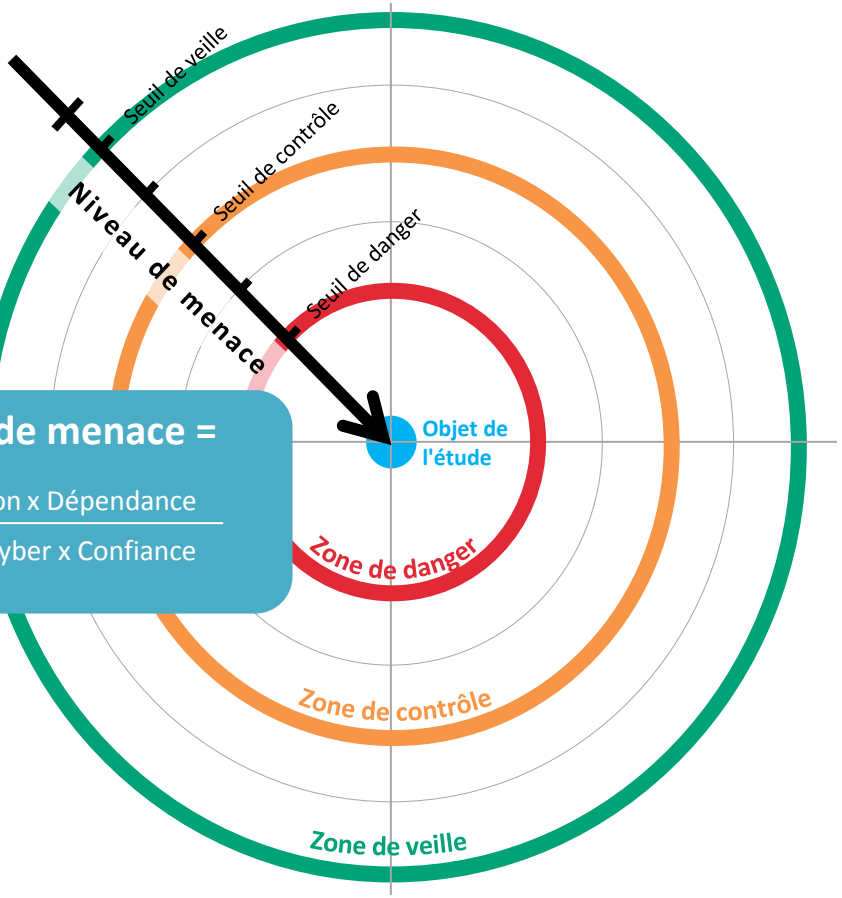
FIABILITE CYBER

Maturité cyber
Quelles sont les capacités de la partie prenante en matière de sécurité ?

Confiance
Est-ce que les intentions ou les intérêts de la partie prenante peuvent m'être contraires ?

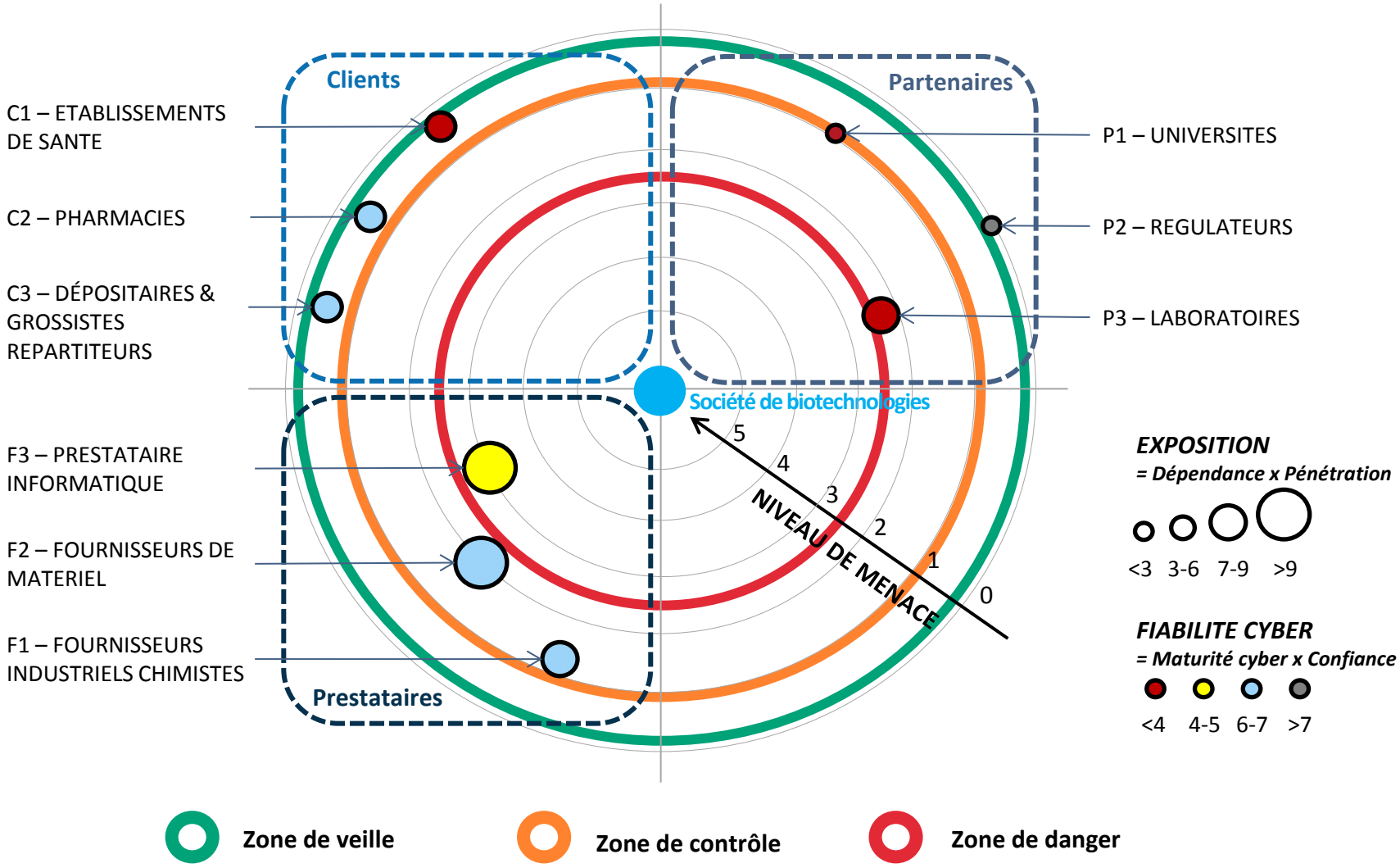
Niveau de menace =

$$\frac{\text{Pénétration x Dépendance}}{\text{Maturité cyber x Confiance}}$$



A3

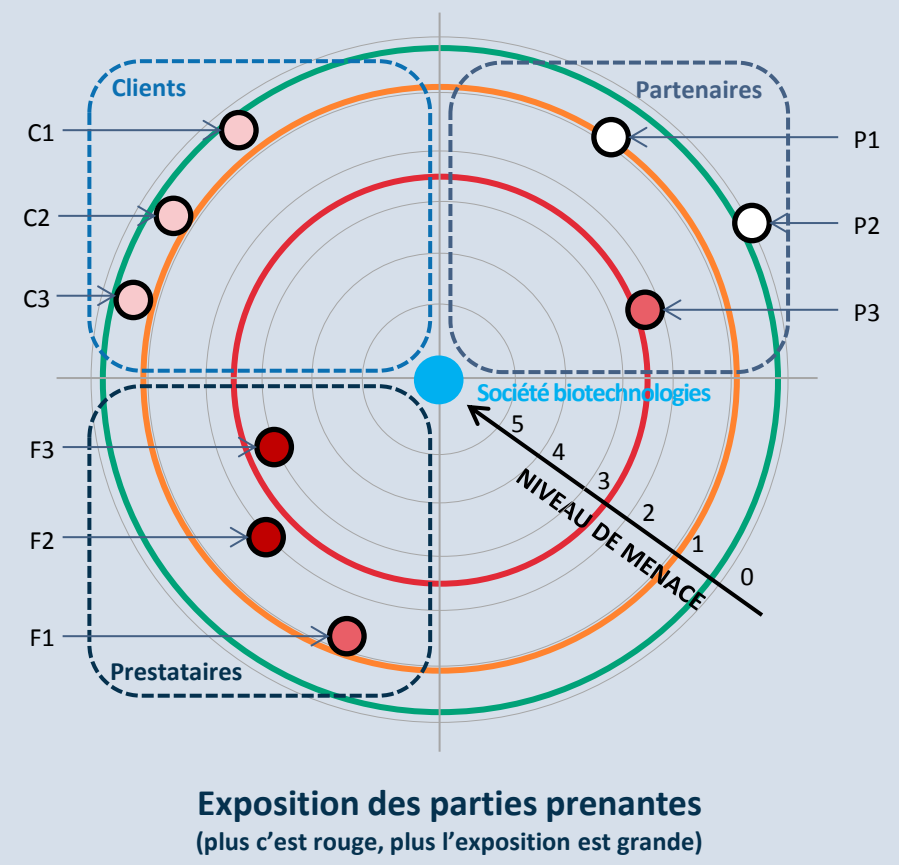
Construire la cartographie de menace de l'écosystème



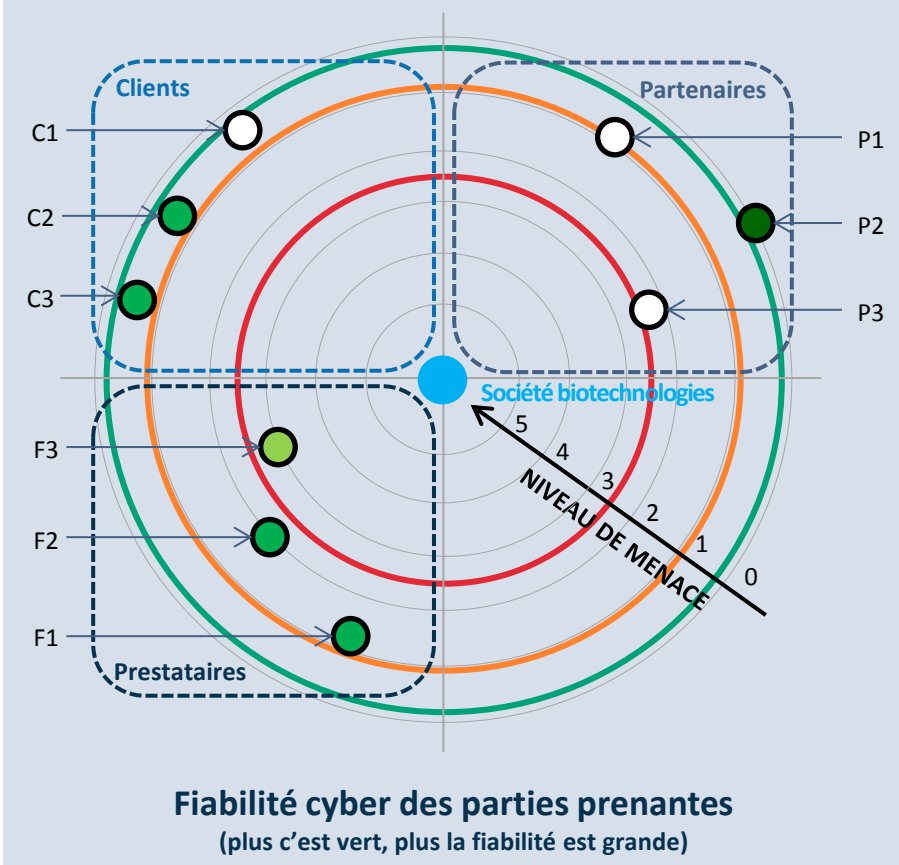
A3

Construire la cartographie de menace de l'écosystème

(autre proposition de représentation)



Exposition des parties prenantes
(plus c'est rouge, plus l'exposition est grande)



Fiabilité cyber des parties prenantes
(plus c'est vert, plus la fiabilité est grande)

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

Légende :

C1 – ÉTABLISSEMENTS DE SANTÉ
C2 – PHARMACIES
C3 – DÉPOSITAIRES & GROSSISTES RÉPARTITEURS

P1 – UNIVERSITÉS
P2 – RÉGULATEURS
P3 – LABORATOIRES

F1 – FOURNISSEURS INDUSTRIELS CHIMISTES
F2 – FOURNISSEURS DE MATÉRIEL
F3 – PRESTATAIRE INFORMATIQUE

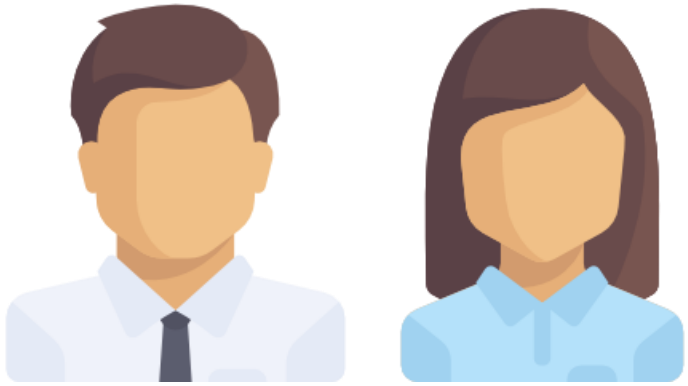
ZONE DE VEILLE
ZONE DE CONTRÔLE
ZONE DE DANGER

A3

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

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

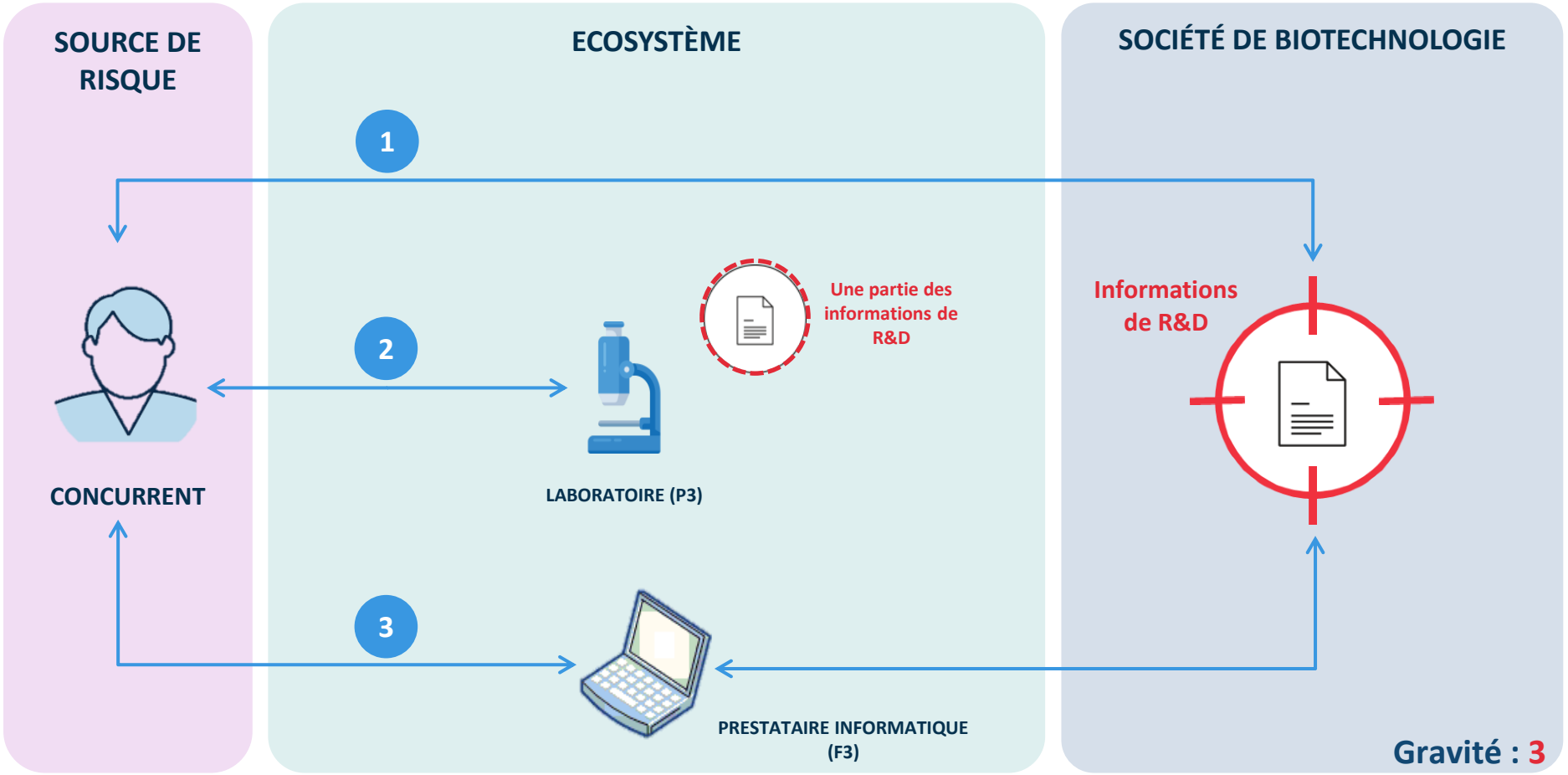
Pour permettre ou faciliter mon attaque, suis-je susceptible d'**attaquer les parties prenantes critiques de l'écosystème** disposant d'un accès privilégié aux valeurs métier ?



A3

Élaborer des scénarios stratégiques

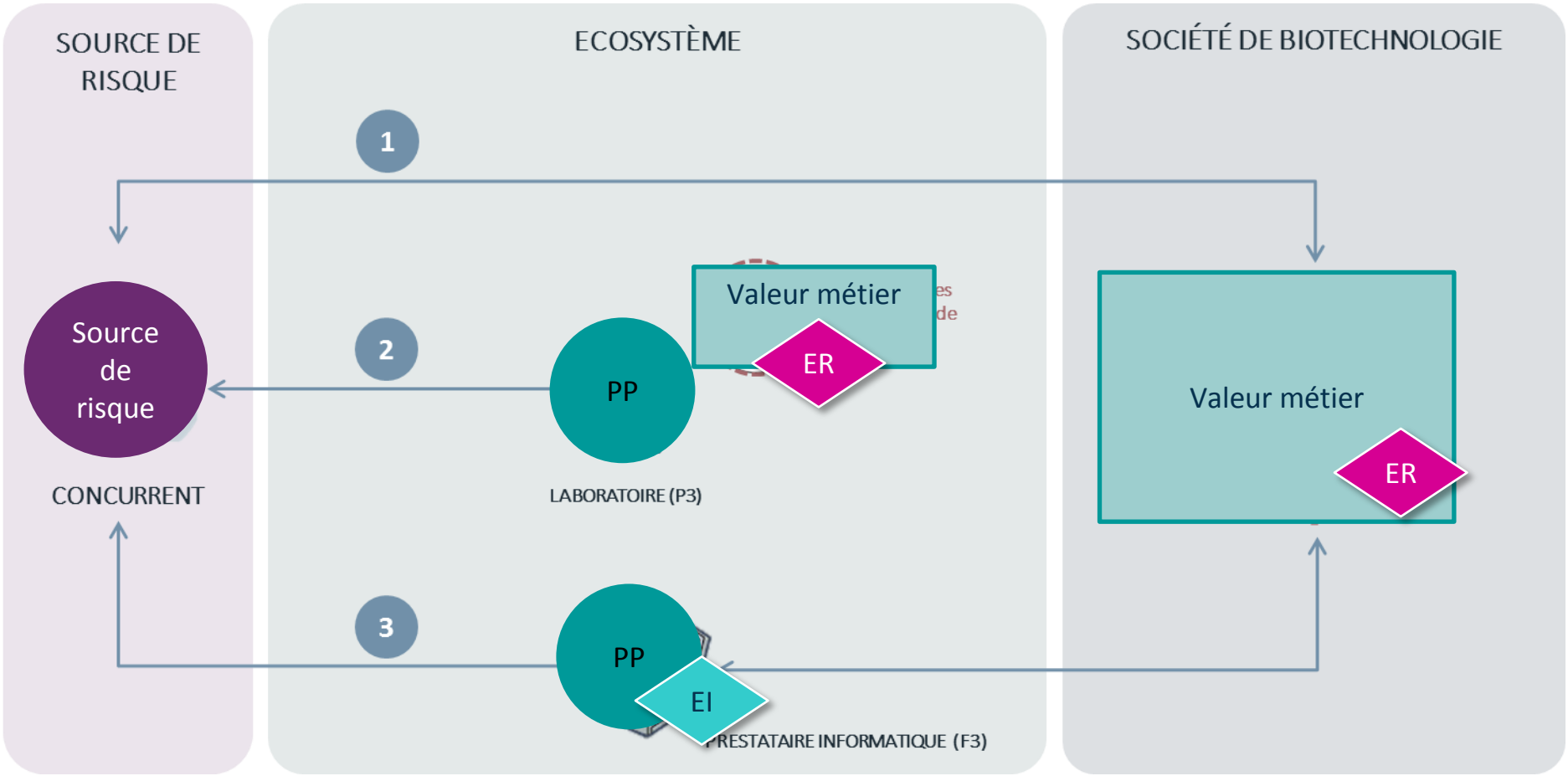
A2 **Source de risque :** Concurrent **Objectif visé :** Voler des informations



Un scénario stratégique constitué de 3 chemins d'attaque

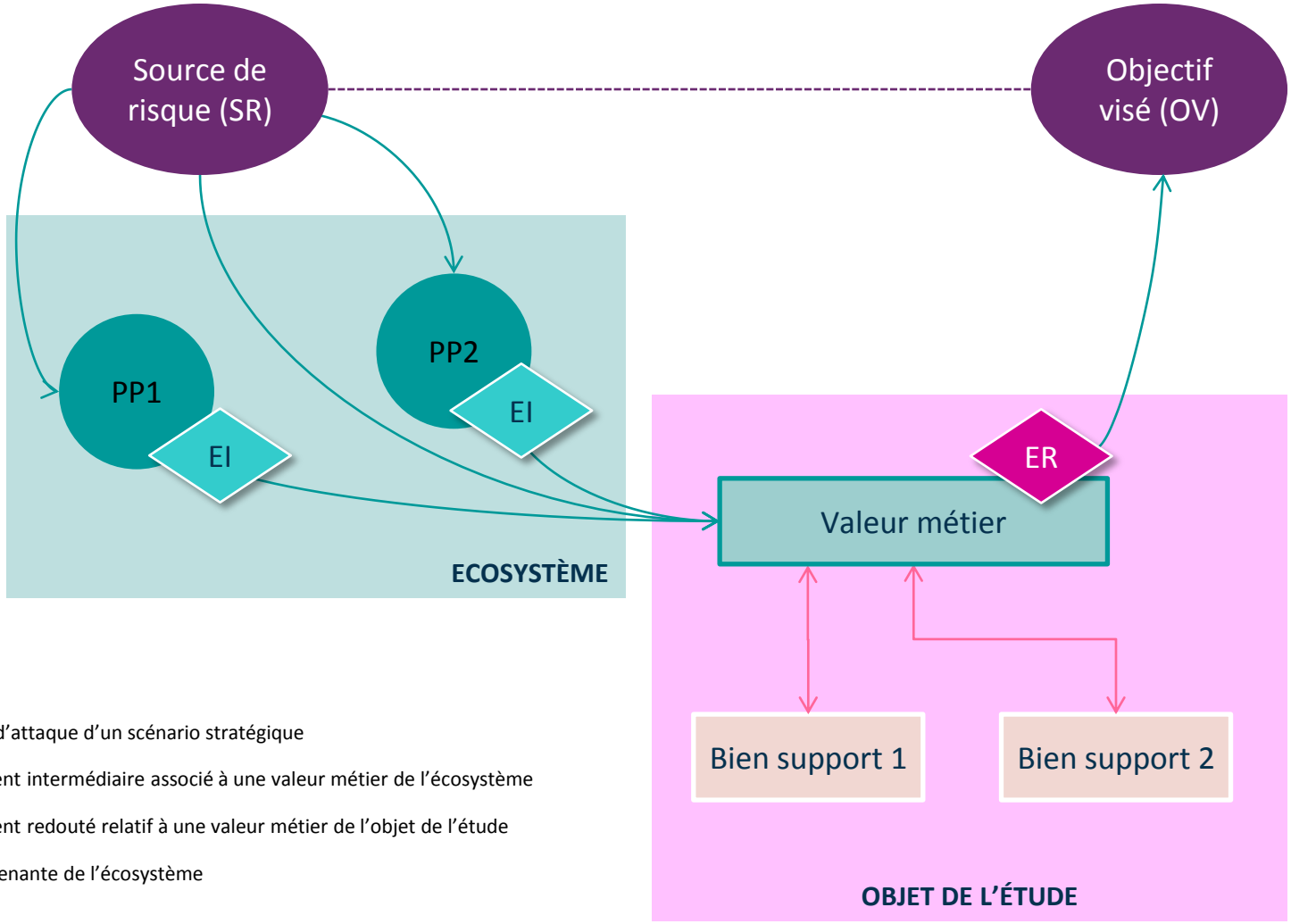
A3

Rappel du vocabulaire observé



A3

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



Légende :

→	Chemin d'attaque d'un scénario stratégique
EI	Événement intermédiaire associé à une valeur métier de l'écosystème
ER	Événement redouté relatif à une valeur métier de l'objet de l'étude
PP	Partie prenante de l'écosystème

Programme

- EBIOS Risk Manager : les bases
- Atelier 1 : cadrage et socle de sécurité
- Atelier 2 : sources de risque
- Atelier 3 : scénarios stratégiques
- **Atelier 4 : scénarios opérationnels**
- Atelier 5 : traitement du risque
- Étude de cas

A4

Atelier 4 : scénarios opérationnels

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

ÉLÉMENTS EN ENTRÉE :

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

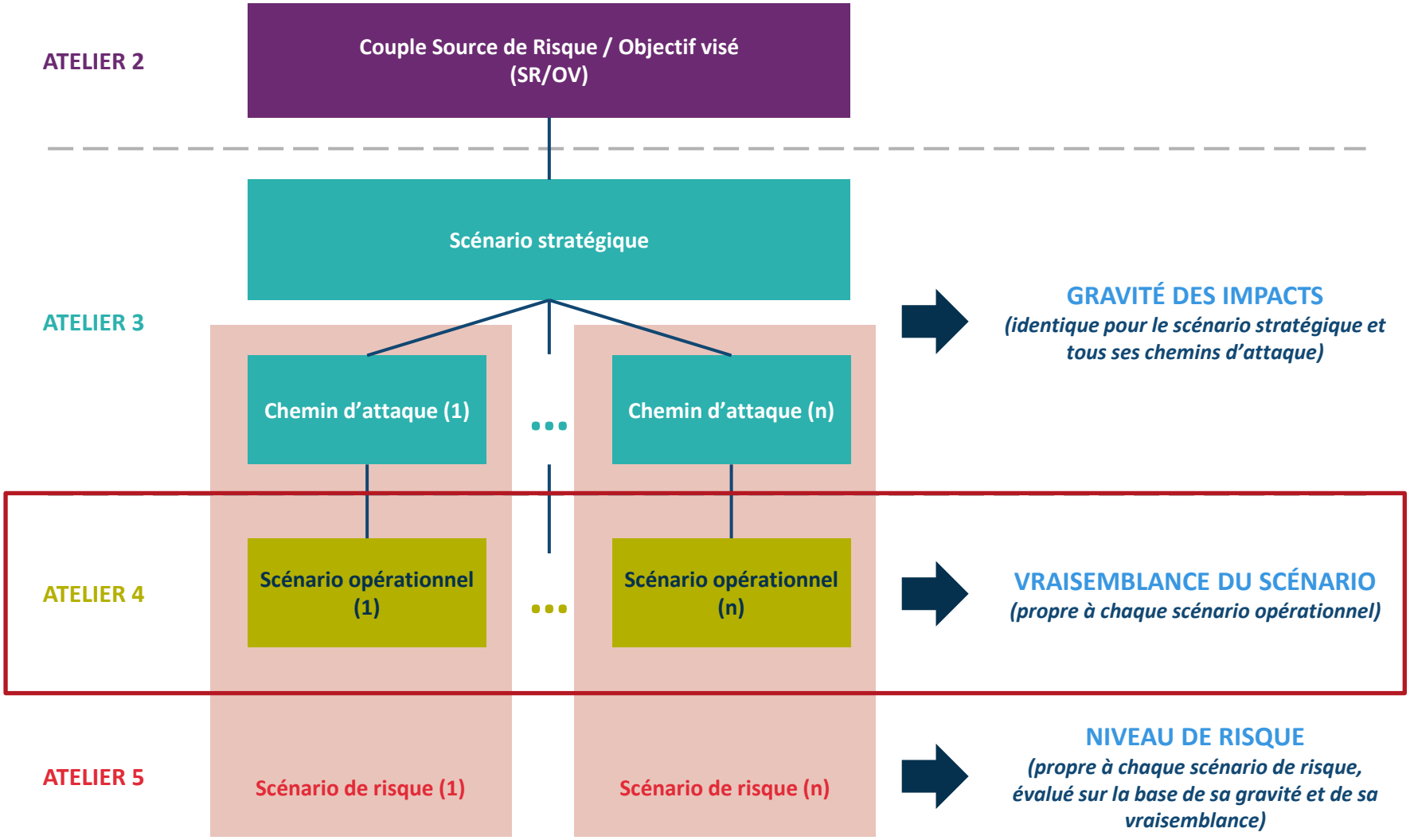
ÉLÉMENTS EN SORTIE :

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

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

A4

Rappel : articulation des ateliers



Des scénarios structurés selon une séquence d'attaque type

CONNAITRE

- Corruption
- Reconnaissance externe

RENTRER

- Corruption
- Intrusion depuis Internet
- Intrusion ou piège physique

TROUVER

- Corruption
- Reconnaissance interne
- Latéralisation et élévation de privilèges

EXPLOITER

- Corruption
- Pilotage et exploitation de l'attaque

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

A4

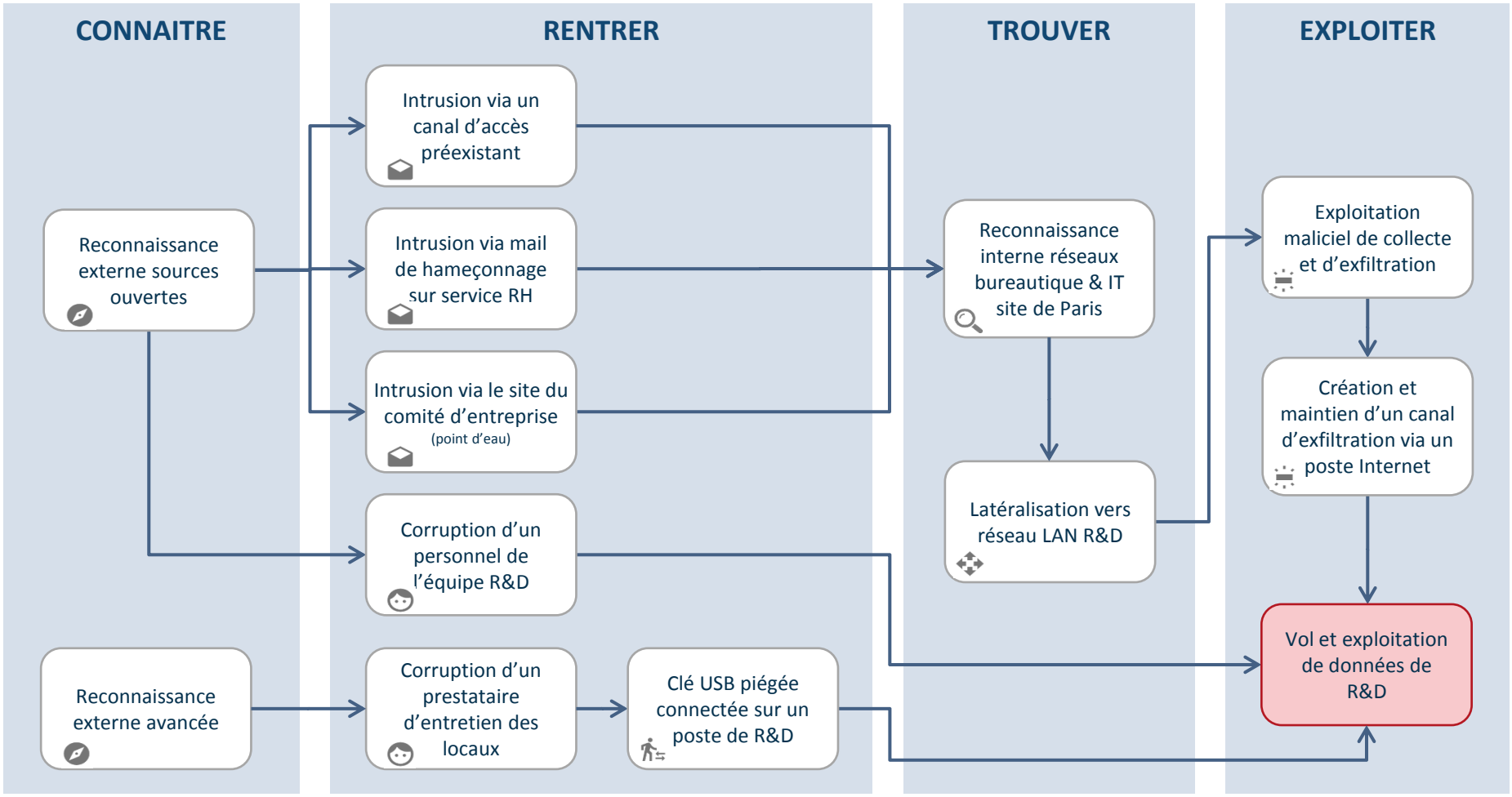
Élaborer les scénarios opérationnels

A3

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

Chemin d'attaque : n°1 – attaque directe

Gravité : 3



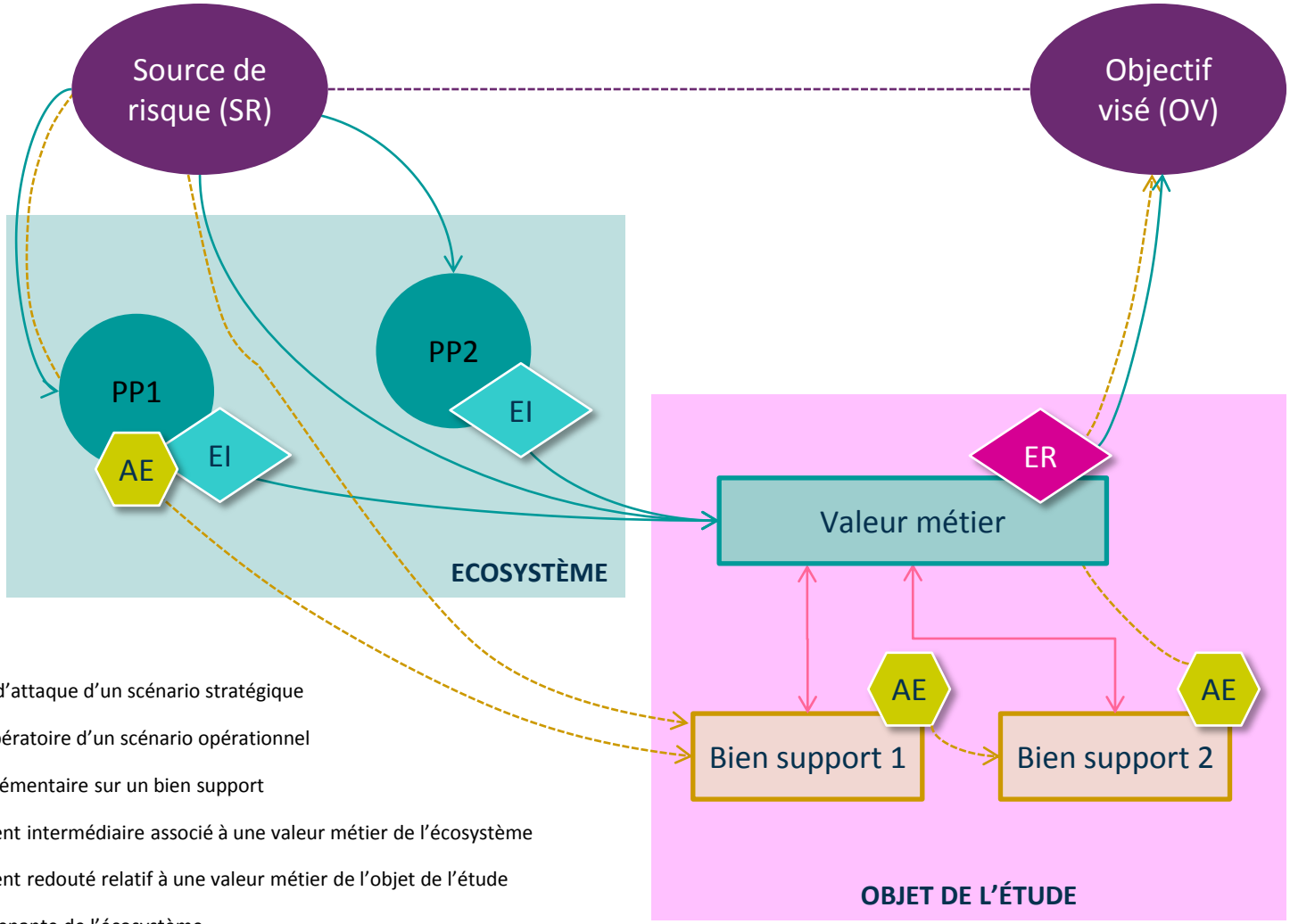
Définir une échelle de vraisemblance

ÉCHELLE	DÉFINITION
V4 – CERTAIN OU DÉJÀ PRODUIT	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés OU un tel scénario s'est déjà produit au sein de l'organisation (historique d'incidents)
V3 – TRÈS VRAISEMBLABLE	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée
V2 – VRAISEMBLABLE	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative
V1 – PEU VRAISEMBLABLE	La source de risque a peu de chances d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible

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

A4

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



Légende :

→	Chemin d'attaque d'un scénario stratégique
⇢	Mode opératoire d'un scénario opérationnel
AE	Action élémentaire sur un bien support
EI	Événement intermédiaire associé à une valeur métier de l'écosystème
ER	Événement redouté relatif à une valeur métier de l'objet de l'étude
PP	Partie prenante de l'écosystème

Programme

- EBIOS Risk Manager : les bases
- Atelier 1 : cadrage et socle de sécurité
- Atelier 2 : sources de risque
- Atelier 3 : scénarios stratégiques
- Atelier 4 : scénarios opérationnels
- **Atelier 5 : traitement du risque**
- Étude de cas

A5

Atelier 5 : traitement du risque

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

ÉLÉMENTS EN ENTRÉE :

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

ATELIER 5
TRAITEMENT DU RISQUE

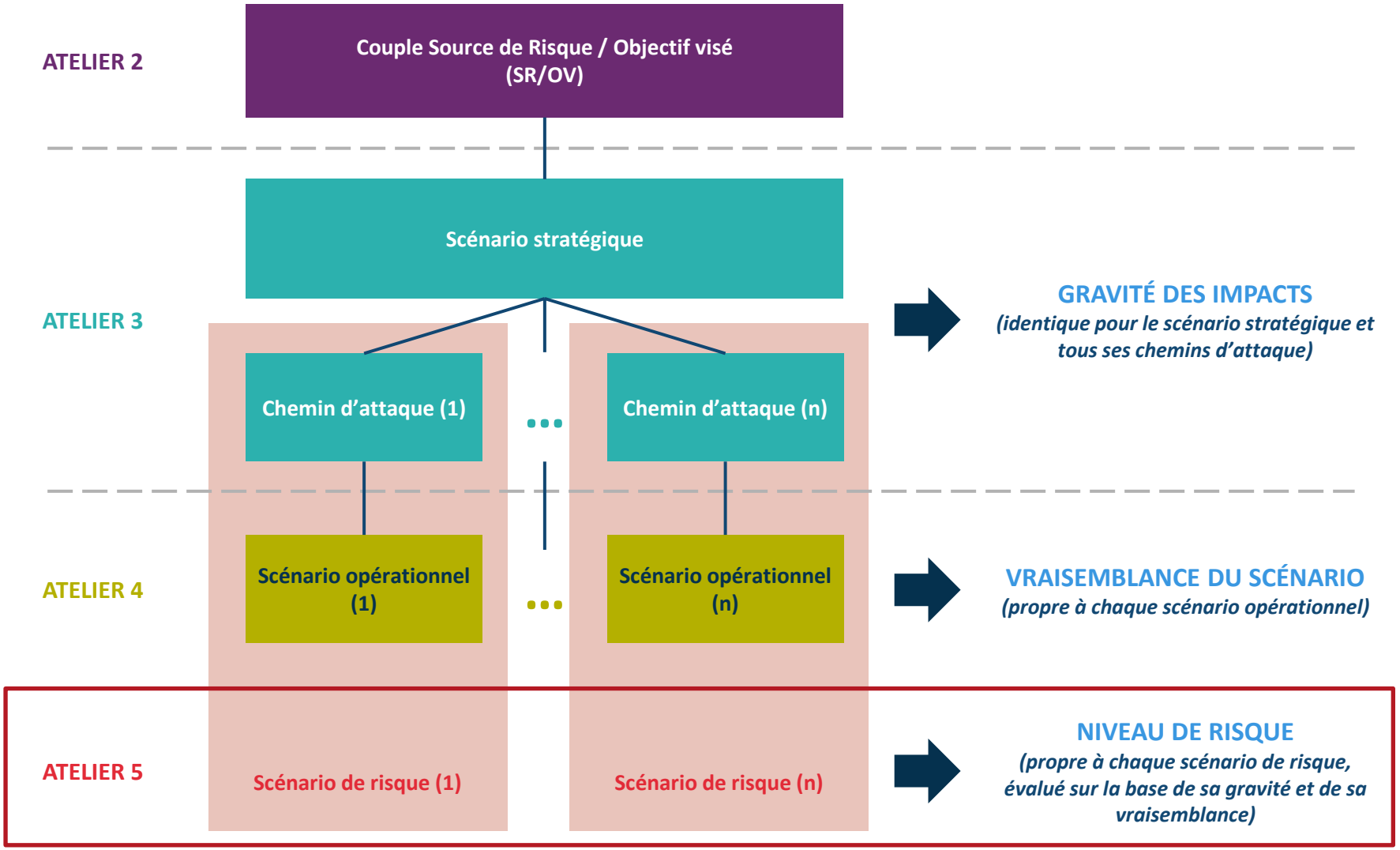
ÉLÉMENTS EN SORTIE :

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

PARTICIPANTS : Direction, Métiers, RSSI, DSI

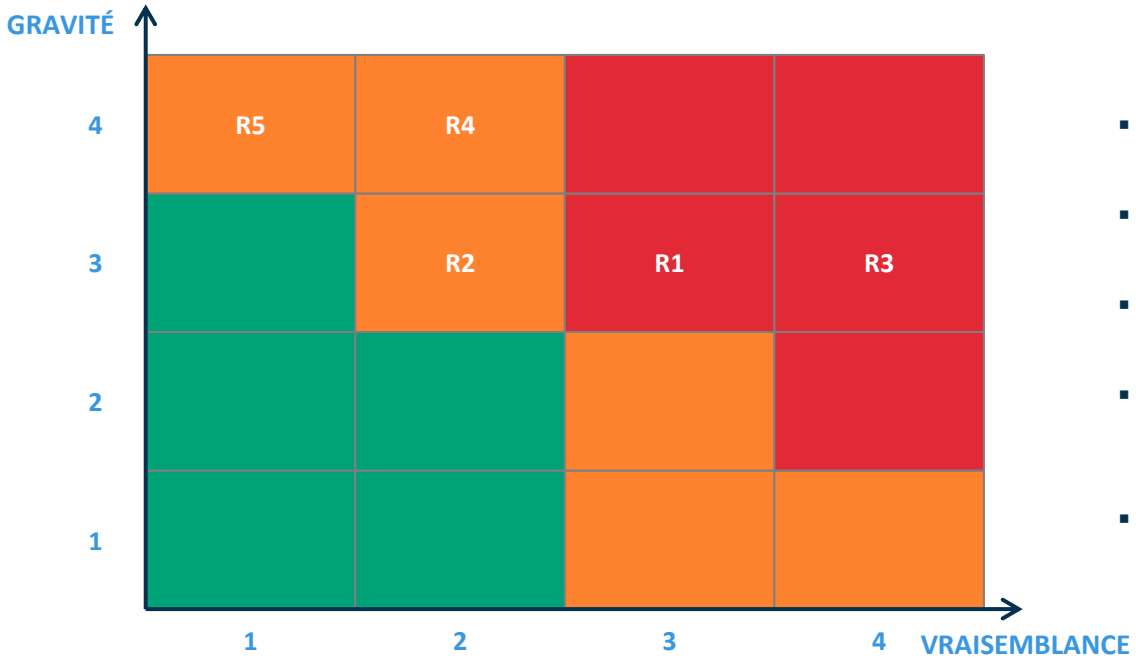
A5

Rappel : articulation des ateliers



A5

Décider de la stratégie de traitement du risque



Scénarios de risques :

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

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

A5

Décider de la stratégie de traitement du risque

OPTIONS DE TRAITEMENT DU RISQUE (ISO 27005 : 2018)

RÉDUCTION DU RISQUE

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

MAINTIEN DU RISQUE

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

REFUS DU RISQUE

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

PARTAGE DU RISQUE

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

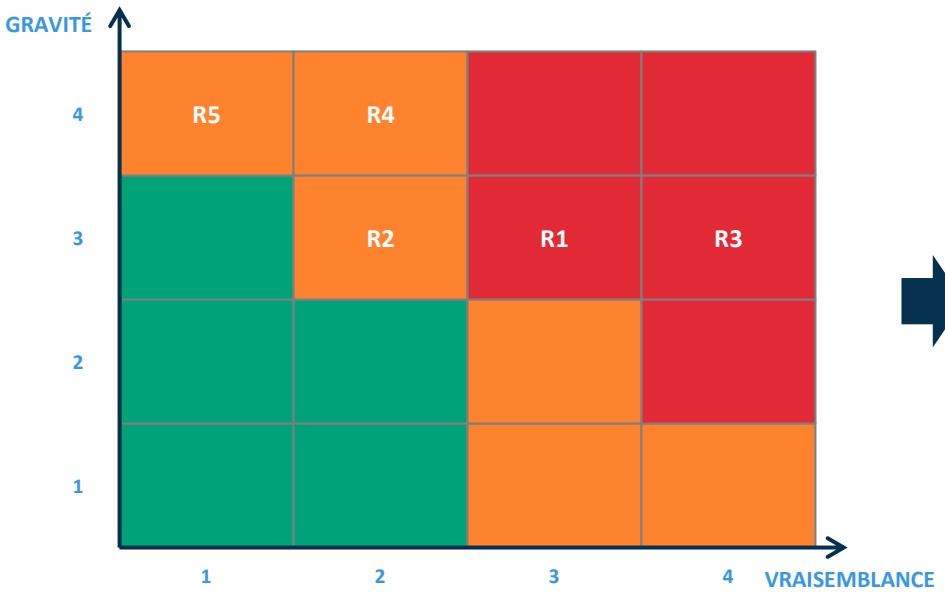
Définir les mesures de sécurité dans un plan d'amélioration continue de la sécurité (PACS)

Mesure de sécurité	Scénarios de risques associés	Responsable	Freins et difficultés de mise en œuvre	...	Coût / Complexité	Échéance	Statut
GOUVERNANCE							
Sensibilisation renforcée au hameçonnage par un prestataire spécialisé	R1	RSSI	Validation de la hiérarchie obligatoire		+	Juin 2019	En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI	R1, R5	RSSI			++	Mars 2019	A lancer
Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contrats avec les prestataires et laboratoires	R2, R3, R4	Équipe juridique	Effectué au fil de l'eau à la renégociation des contrats		++	Juin 2020	En cours
Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire ou un laboratoire	R2, R3, R4	RSSI / Équipe juridique			++	Juin 2019	A lancer
Audit de sécurité organisationnel des prestataires et laboratoires clés. Mise en place et suivi des plans d'action consécutifs	R2, R3, R4	RSSI	Acceptation de la démarche par les prestataires et laboratoires		++	Juin 2019	A lancer
Limitation des données transmises au laboratoire au juste besoin	R2	Équipe R&D			+	Mars 2019	Terminé
PROTECTION							
Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonnement)	R1, R3	DSI			+++	Septembre 2019	En cours
Renforcement du contrôle d'accès physique au bureau R&D	R1	Équipe sûreté			++	Mars 2019	Terminé
Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site	R4	DSI			++	Septembre 2019	A lancer

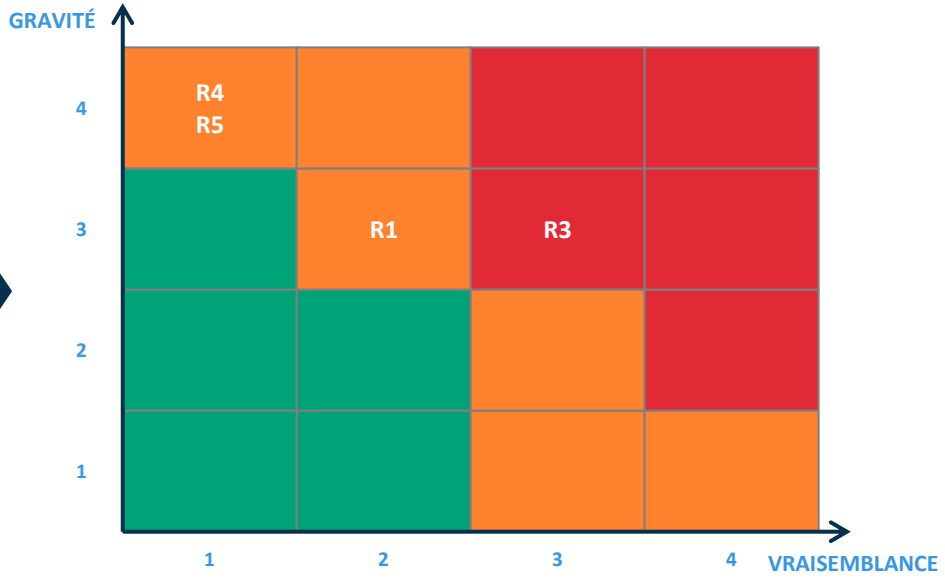
A5

Gérer les risques résiduels

Cartographie du risque initial (avant traitement)



Cartographie du risque résiduel (après application du PACS)



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

A5

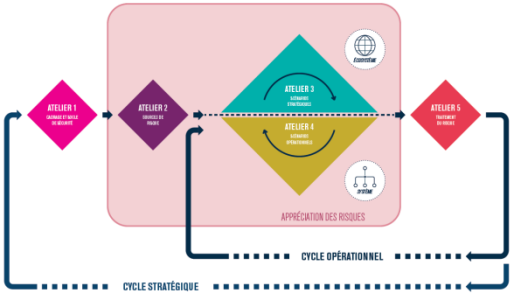
Mettre en place le cadre de suivi des risques

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

MESURE DE SÉCURITÉ	SCÉNARIOS DE RISQUES ASSOCIÉS	RESPONSABLE	FREINS ET DIFFICULTÉS DE MISE EN ŒUVRE	COÛT / COMPLEXITÉ	ÉCHÉANCE	STATUT
GOUVERNANCE						
Sensibilisation renforcée au hameçonnage par un prestataire spécialisé	R1	RSSI	Validation du CHSCT indispensable	+	6 mois	En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI	R1, R5	RSSI		++	3 mois	À lancer
Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contrats avec les prestataires et laboratoires	R2, R3, R4	équipe juridique	Effectué au fil de l'eau à la renégociation des contrats	++	18 mois	En cours
Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire ou un laboratoire	R2, R3, R4	RSSI / équipe juridique		++	6 mois	À lancer
Audit de sécurité organisationnel des prestataires et laboratoires clés. Mise en place et suivi des plans d'action consécutifs	R2, R3, R4	RSSI	Acceptation de la démarche par les prestataires et laboratoires	++	6 mois	À lancer
Limitation des données transmises aux laboratoires 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		++	9 mois	À lancer

Suivi de l'avancement du PACS

Suivi des indicateurs de maintien en condition de sécurité



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

Programme

- EBIOS Risk Manager : les bases
- Atelier 1 : cadrage et socle de sécurité
- Atelier 2 : sources de risque
- Atelier 3 : scénarios stratégiques
- Atelier 4 : scénarios opérationnels
- Atelier 5 : traitement du risque
- **Étude de cas**

Livret stagiaire
p.24 à 28

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.