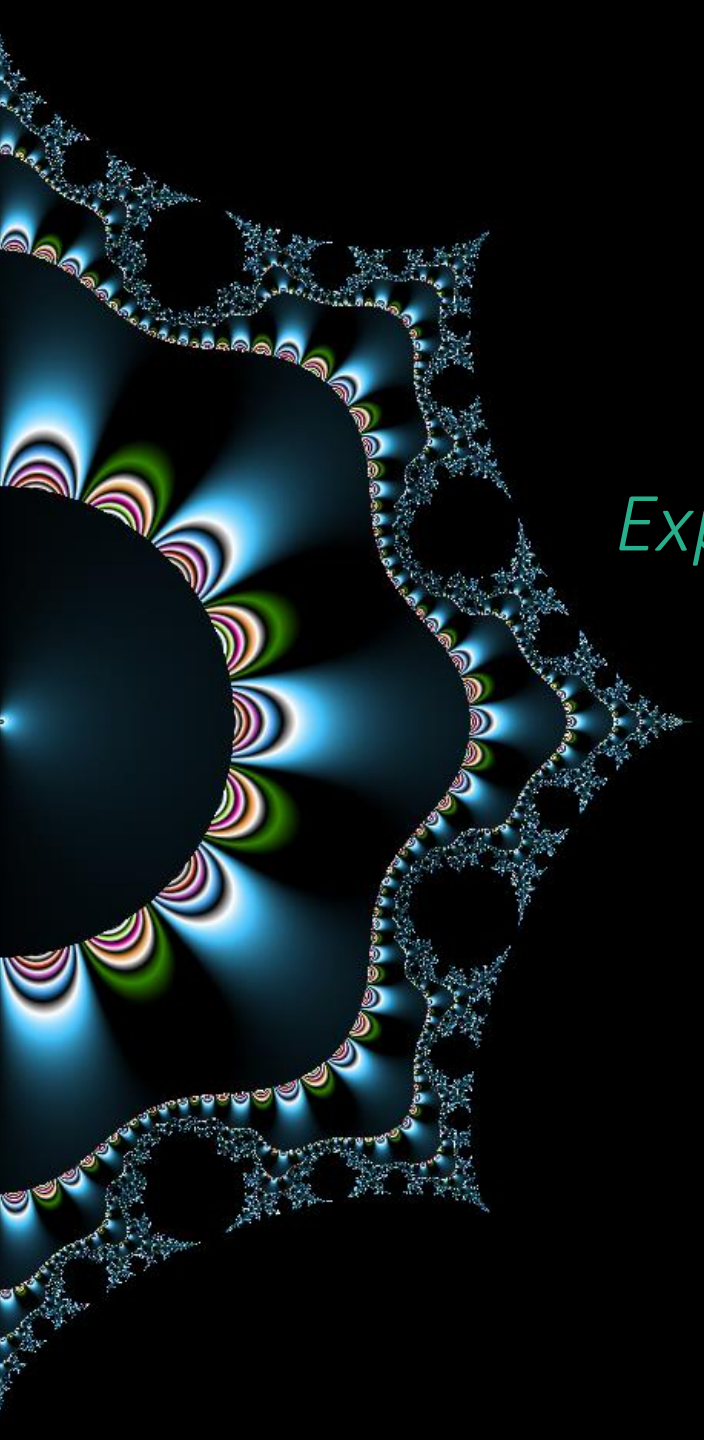


EBIOS RM

Expression des Besoins et Identification des Objectifs de Sécurité

Thibaut HENIN

tbowan@arsouyes.org

Evolution d’Ebios

1995

EBIOS

Par la DCSSI

Logiciel (tableaux)

2010

EBIOS

Par l’ANSSI

Ateliers (tableaux)

2018

EBIOS-RM

Par l’ANSSI

Relooking

Ressources

https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/

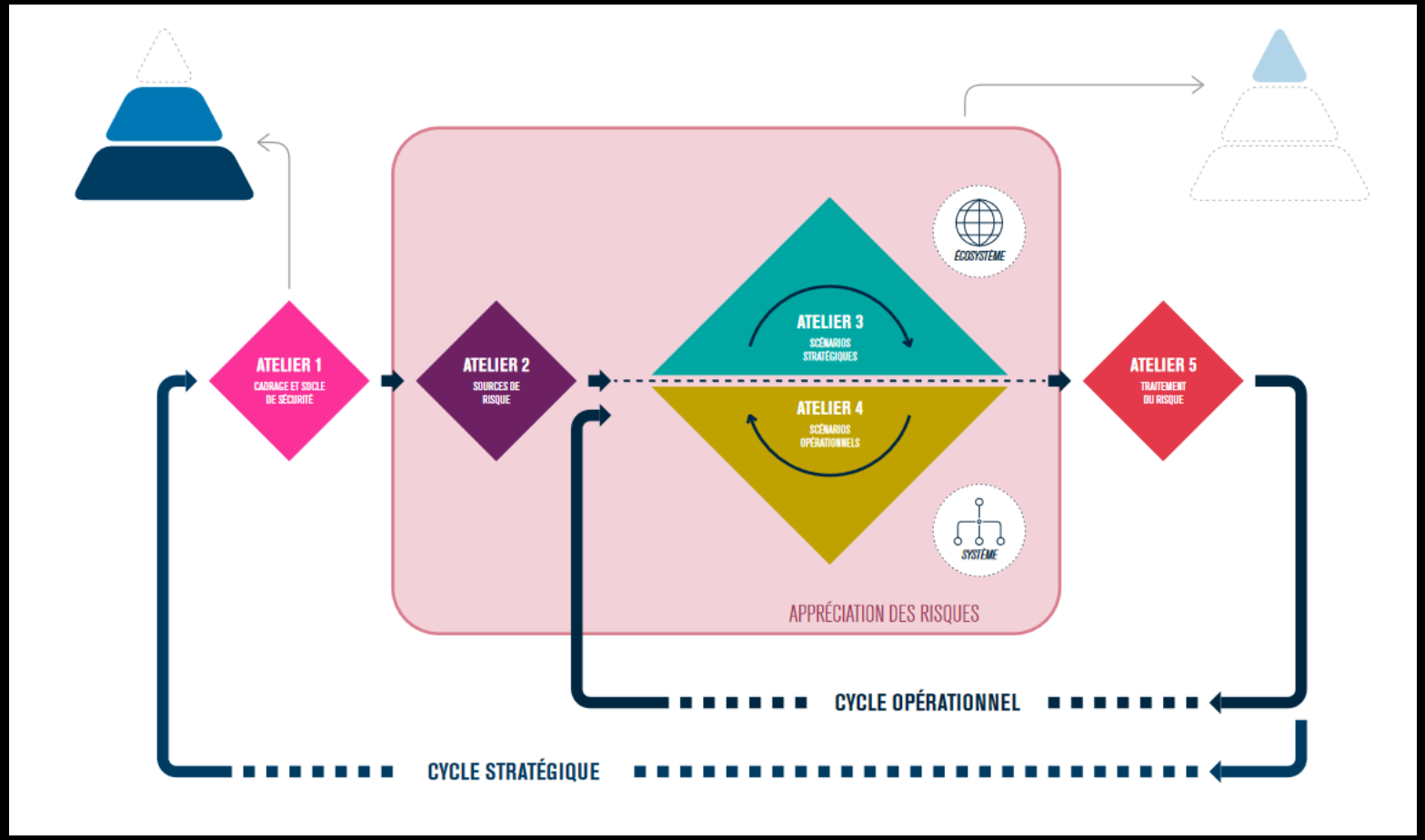
Le guide

(PDF de 49 pages)

9 Fiches

(PDF de 84 pages)

Déroulement : 5 Ateliers



Atelier 1

Cadrage et socle de sécurité

Objectif

Périmètre

(métier et technique)

Etat des lieux

(événements et mesures en place)

1 - Cadrage

Objectif de l’étude

(pourquoi faire Ebios)

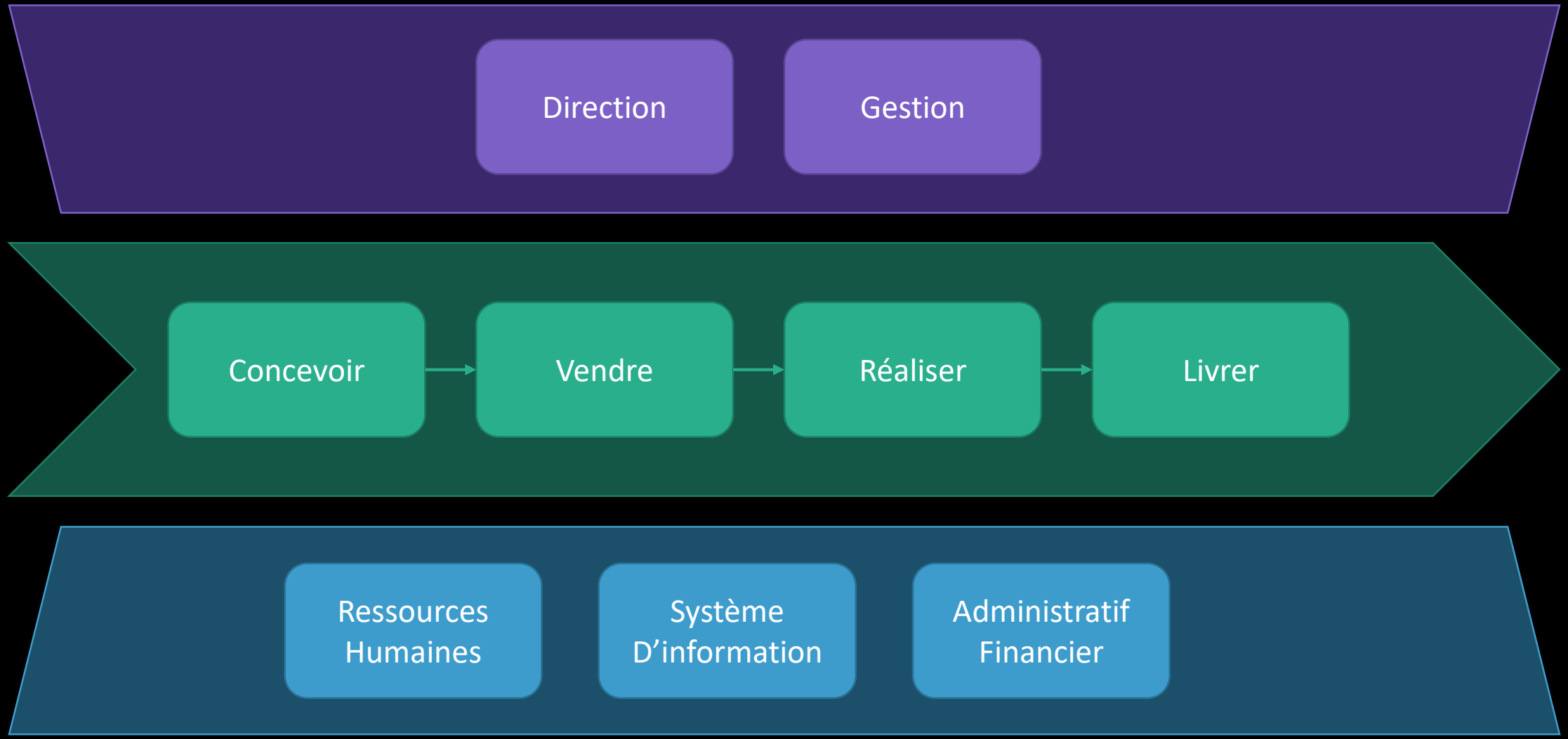
Participants

(matrice raci)

Durée

(calendrier et charge)

2 - Périmètre métier



2 - Périmètre métier

Fiche Méthode n°1 & 2

Valeurs métier

(processus / informations)

Valeurs support

(Biens à protéger)

MISSIONS	MISSION 1	MISSION…		
DÉNOMINATION DE LA VALEUR MÉTIER	Valeur métier 1	Valeur métier 2		Valeur métier…
NATURE DE LA VALEUR MÉTIER (PROCESSES OU INFORMATION)				
DESCRIPTION				
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE / EXTERNE)				
DÉNOMINATION DU / DES BIEN(S) SUPPORT(S) ASSOCIÉ(S)	Bien support 1	Bien support 2	Bien sup-port 3	Bien support…
DESCRIPTION				
ENTITÉ OU PERSONNE RESPONSABLE (INTERNE / EXTERNE)				

3 – Événements redoutés

Fiche Méthode n°3

Impacts de l'événement

(liste des conséquences)

Gravité

(score de 1 à 4)

VALEUR MÉTIER	EVÈNEMENT REDOUTÉ	IMPACTS	GRAVITÉ
R&D	Perte ou destruction des informations d'études et recherches conduisant à un fort impact, notamment sur les futures autorisations de mises sur le marché de l'entreprise	■ Impacts sur les missions et services de l'organisme ■ Impacts sur les coûts de développement ■ Impacts sur la gouvernance de l'organisme	3
	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 la gouvernance de l'organisme ■ Impacts financiers	3
	Interruption des phases de tests des vaccins pendant plus d'une semaine	■ Impacts sur les missions et services de l'organisme ■ Impacts financiers	2

4 – Socle

Fiche Méthode n°3

Norme applicables

(i.e. guides de l'ANSSI, CNIL, …)

Ecarts

(et justification)

TYPE DE RÉFÉRENTIEL	NOM DU RÉFÉRENTIEL	ÉTAT D'APPLICATION	ÉCARTS	JUSTIFICATION DES ÉCARTS
Règles d'hygiène informatique et bonnes pratiques	Guide d'hygiène informatique de l'ANSSI	Appliqué avec restrictions	Règle 8 : identifier nommément chaque personne accédant au système et distinguer les rôles	Existence d'un compte *admin* non nominatif pour l'administration de l'ERP (solution propriétaire ne permettant pas l'administration par un autre compte)
			Règle 37 : définir et appliquer une politique de sauvegarde des composants critiques	Politique de sauvegarde en cours de rédaction par un groupe de travail

Atelier 2

Sources de risques

Objectif

Quel adversaire ?

1/2 – Identification

Fiche Méthode n°4

Qui ?

(Source de Risque)

Pourquoi ?

(Objectif Visé)

SOURCES DE RISQUE	OBJECTIFS VISÉS
Hacktiviste	Saboter la prochaine campagne nationale de vaccination en perturbant la production ou la distribution des vaccins, pour générer un choc psychologique sur la population et discréditer les pouvoirs publics.
Concurrent	Voler des informations en espionnant les travaux de R&D en vue d'obtenir un avantage concurrentiel.
Hacktiviste	Divulguer au grand public des informations sur la façon dont les vaccins sont conçus en collectant des photos et vidéos des tests animaliers afin de rallier l'opinion publique à sa cause.
Cyber-terroriste	Altérer la composition de vaccins distribués lors d'une campagne nationale de vaccination à des fins de bioterrorisme.

2/2 – Évaluation / Sélection

Fiche Méthode n°4

Motivation

(Veulent-ils le faire ?)

Ressources

(Peuvent-ils le faire ?)

Activité

(Le font ils souvent ?)

SOURCES DE RISQUE	OBJECTIFS VISÉS	MOTIVATION	RESSOURCES	ACTIVITÉ	PERTINENCE
Hacktiviste	Saboter la campagne nationale de vaccination	++	+	++	**Moyenne**
Concurrent	Voler des informations	+++	+++	+++	**Élevée**
Hacktiviste	Divulguer des informations sur les tests animaliers	++	+	+	**Faible**
Cyber-terroriste	Altérer la composition de vaccins à des fins bioterroristes	+	++	+	**Faible**

Atelier 3

Scénarios stratégiques

Objectif

Identifier les menaces

(globalement)

1.1 – Parties prenantes

Fiche Méthode n°5

Externes

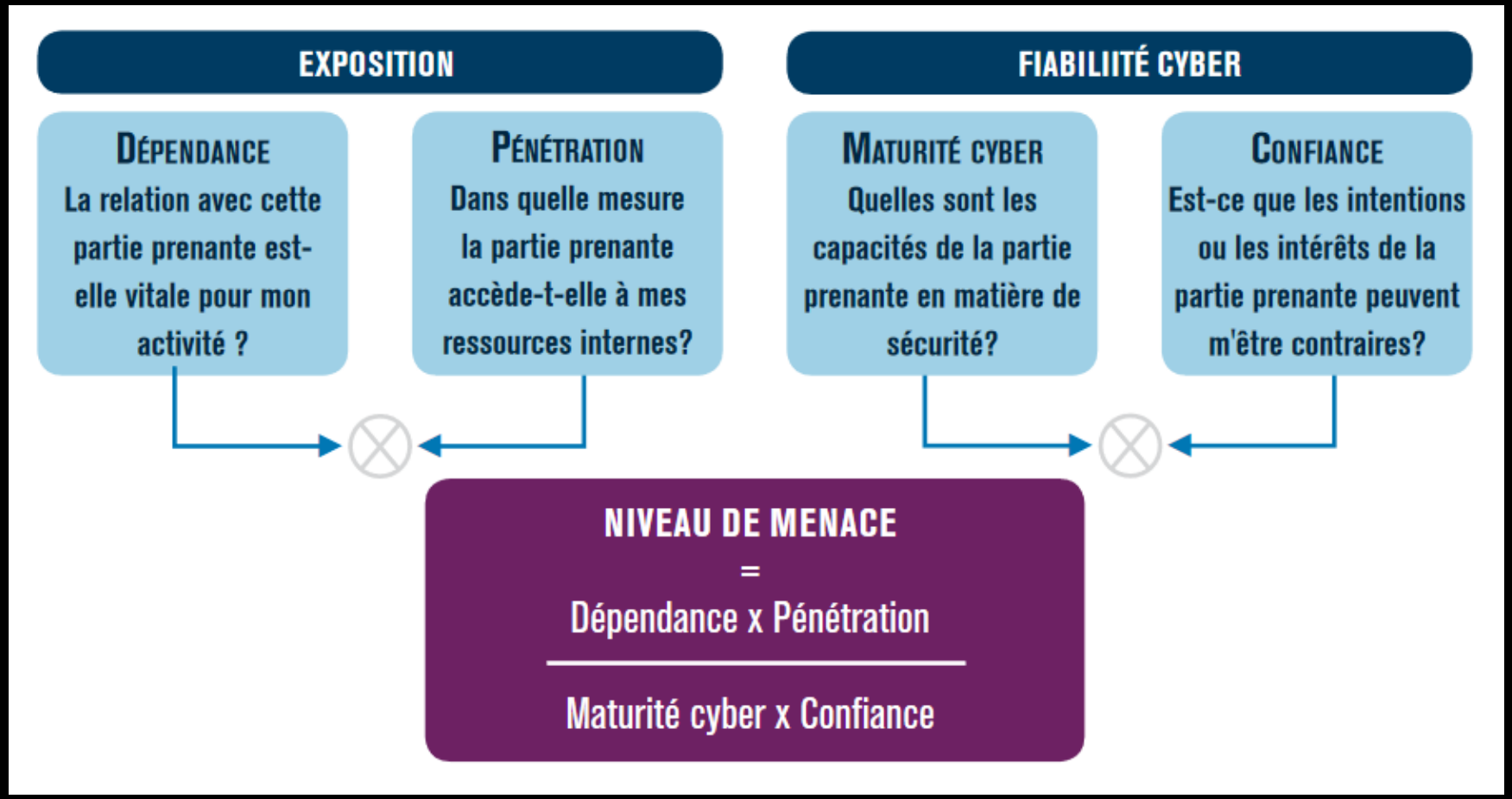
(clients, partenaires, prestataires)

Interne

(services, filiales)

1.2 – Niveau de menace

Fiche Méthode n°5



1.3 – Cartographie des menaces

Fiche Méthode n°5

CATÉGORIE	PARTIE PRENANTE	DÉPENDANCE	PÉNÉTRATION	MATURITÉ	CONFIANCE	NIVEAU DE MENACE
CLIENTS	C1 – Établissements de santé	1	1	1	3	0,3
	C2 – Pharmacies	1	1	2	3	0,2
	C3 – Dépositaires / Grossistes répartiteurs	1	2	2	3	0,3
PARTENAIRES	P1 – Universités	2	1	1	2	1
	P2 – Régulateurs	2	1	2	4	0,3
	P3 – Laboratoires	3	3	2	2	2,25
PRESTATAIRES	F1 – Fournisseurs industriels chimistes	4	2	2	3	1,3
	F2 – Fournisseurs de matériel de production	4	3	2	3	2
	F3 – Prestataire informatique	3	4	2	2	3

1.4 – Sélection (4 zones)

Fiche Méthode n°5

Danger

(non acceptable, à traiter)

Veille

(acceptable, non prioritaire)

Contrôle

(tolérable, rester vigilant)

Hors périmètre

(négligeable)

2 – Scénarios

Qui

(SR/OV)

Comment

(globalement, parties prenantes)

Gravité

SOURCES DE RISQUE	OBJECTIFS VISÉS	CHEMINS D'ATTAQUE STRATÉGIQUES	GRAVITÉ
Concurrent	Voler des informations en espionnant les travaux de R&D en vue d'obtenir un avantage concurrentiel	Trois chemins d'attaque à investiguer. Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données : 1. portant directement sur le système d'information de la R&D ; 2. sur le système d'information du laboratoire (P3), qui détient une partie des travaux ; 3. passant par le prestataire informatique F3.	**3 Grave**
Hacktiviste	Saboter la prochaine campagne nationale de vaccination pour générer un choc psychologique sur la population et discréditer les pouvoirs publics	Deux chemins d'attaque à investiguer. Un hacktiviste perturbe la production ou la distribution de vaccins : 1. en provoquant un arrêt de la production industrielle par compromission de l'équipement de maintenance du fournisseur de matériel F2 ; 2. en modifiant l'étiquetage des vaccins.	**4 Critique**

3 – Mesures de sécurité

Fiche Méthode n°6

Réduire la menace

(zones de danger et contrôle)

Parties prenantes

(dépendance et/ou sécurité)

PARTIE PRENANTE	CHEMINS D'ATTAQUE STRATÉGIQUES	MESURES DE SÉCURITÉ	MENACE INITIALE	MENACE RÉSIDUELLE
F2 Fournisseurs de matériel	Arrêt de production par compromission de l'équipement de maintenance	**Réduire le risque de piégeage des équipements de maintenance utilisés sur le système industriel.** Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site (permet de réduire la pénétration des fournisseurs de 3 à 2).	2	1,3
F3 Prestataire informatique	Vol d'informations en passant par le prestataire informatique	**Accroitre la maturité cyber du prestataire (2 → 3) :** ■ audit de sécurité (à inclure dans le contrat) ; ■ suivi du plan d'action interne. **Renforcer la protection des données de R&D.** Solutions à investiguer : chiffrement, cloisonnement du réseau R&D.	3	2
P3 Laboratoires	Vol d'informations sur le système d'information du laboratoire	**Diminuer la pénétration des laboratoires (3 → 2) :** limitation des données transmises au laboratoire au juste besoin (mauvaise habitude actuelle de « tout » diffuser).	2,25	1,5

Atelier 4

Scénarios opérationnels

Objectif

Identifier les menaces

(concrètes et techniques)

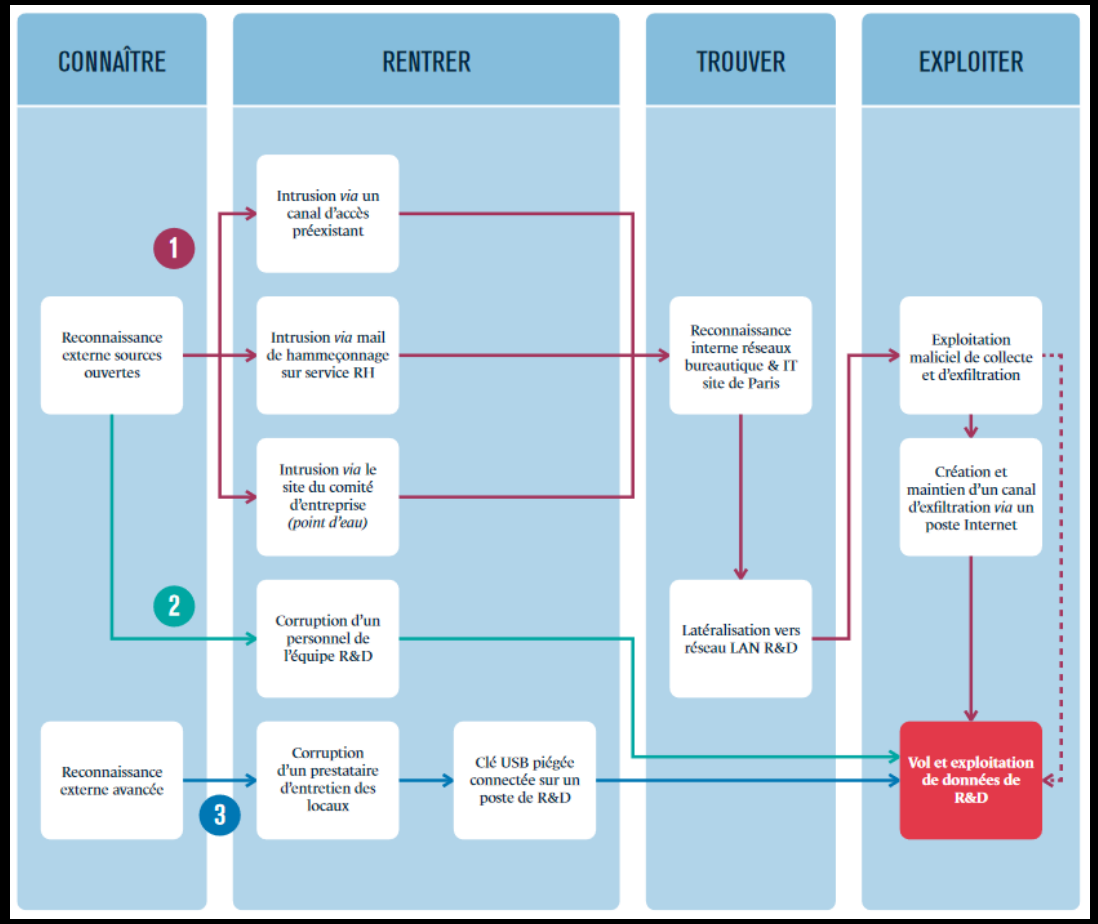
1 – Élaboration de Scénarios

Fiche Méthode n°7

Chemins d'attaques

(ou graphes)

Concrétisation des scénarios stratégiques



2 – Évaluer la vraisemblance

Fiche Méthode n°8

		DIFFICULTÉ TECHNIQUE DU SCÉNARIO OPÉRATIONNEL				
		0 – NÉGLIGEABLE	1 – FAIBLE	2 – MODÉRÉE	3 – ÉLEVÉE	4 – TRÈS ÉLEVÉE
PROBABILITÉ DE SUCCÈS DU SCÉNARIO OPÉRATIONNEL	4 – QUASI CERTAINE	4	4	3	2	1
	3 – TRÈS ÉLEVÉE	4	3	3	2	1
	2 – SIGNIFICATIVE	3	3	2	2	1
	1 – FAIBLE	2	2	2	1	0
	0 – TRÈS FAIBLE	1	1	1	0	0

Atelier 5

Traitement du risque

Objectif

Plan d’action d’amélioration de la sécurité

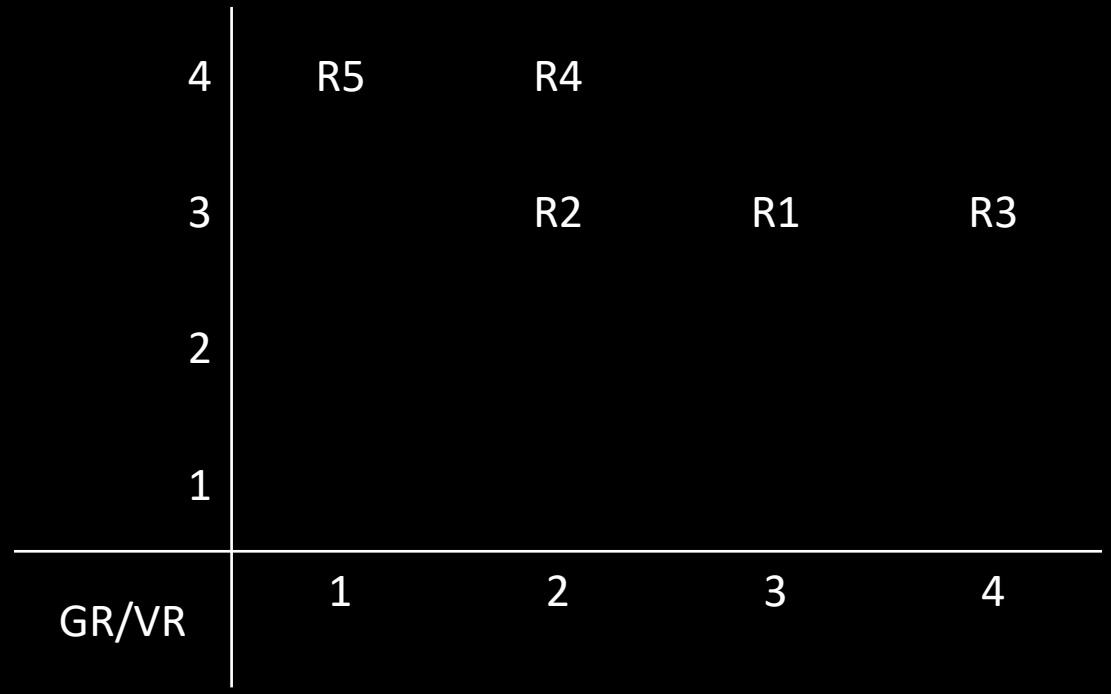
(Politique de Sécurité du Système d’Information)

1 – Synthèse des scénarios

Scénario = Menace

Diagrame de Farmer

(gravité vs Vraisemblance)



2.1 – Stratégie de traitement

Faible

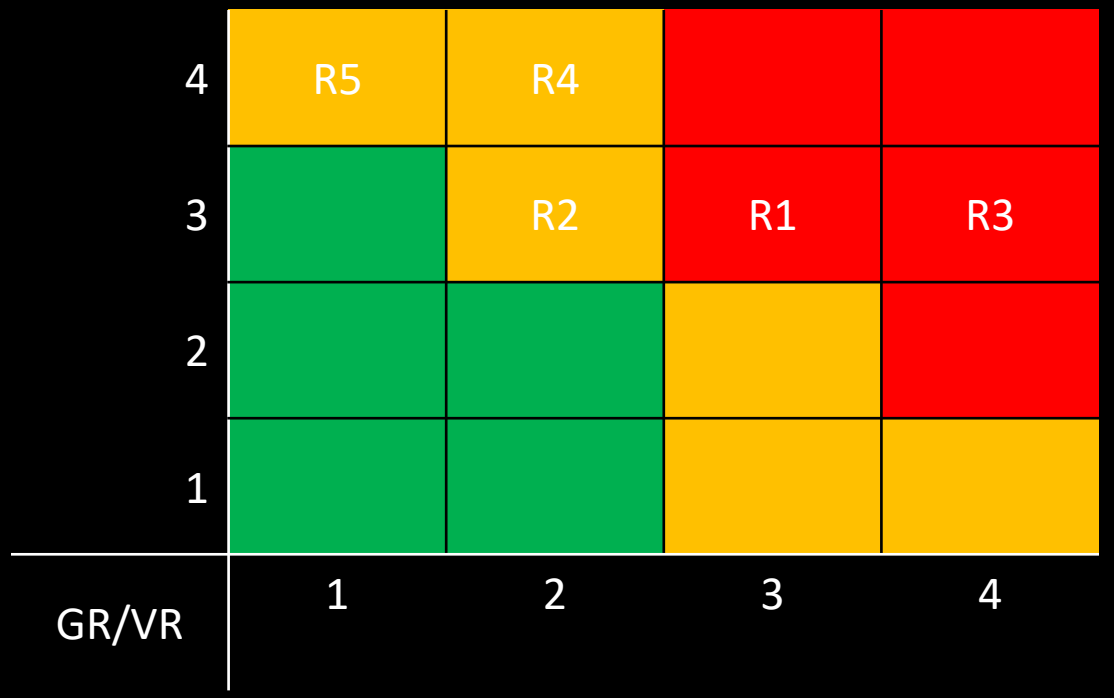
(acceptable en l'état)

Moyen

(Tolérable sous contrôle)

Élevé

(Inacceptable)



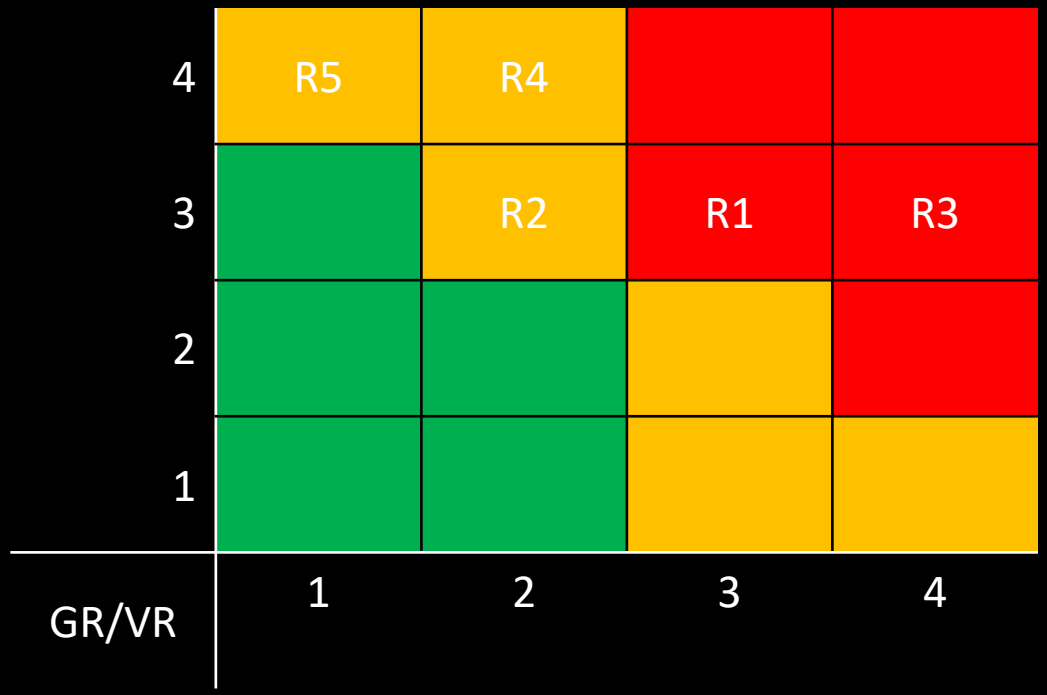
2.2 – Mesures de sécurité

Fiche Méthode n°9

MESURE DE SÉCURITÉ	SCÉNARIOS DE RISQUES ASSOCIÉS	RESPONSABLE	FREINS ET DIFFICULTÉS DE MISE EN ŒUVRE	COÛT / COMPLEXITÉ	ECHÉANCE	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

3 – Risques résiduels

Avant



Après