Préparation à la certification EBIOS RM

Slides de démonstration

ERM
v1.0 (07/2025)

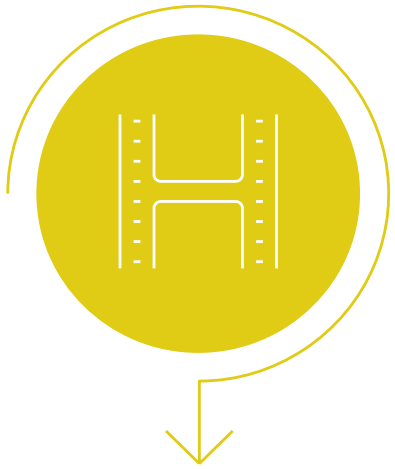
EBIOS RISK MANAGER

A0

Introduction à EBIOS RM

VERISAFE
L'EXPERTISE CYBERSÉCURITÉ

Comment se déroule la formation ?



Module de formation
Format vidéo

Podcast audio
Synthèse du module en format audio

Généré par IA

QCM
Test de connaissances pour chaque module

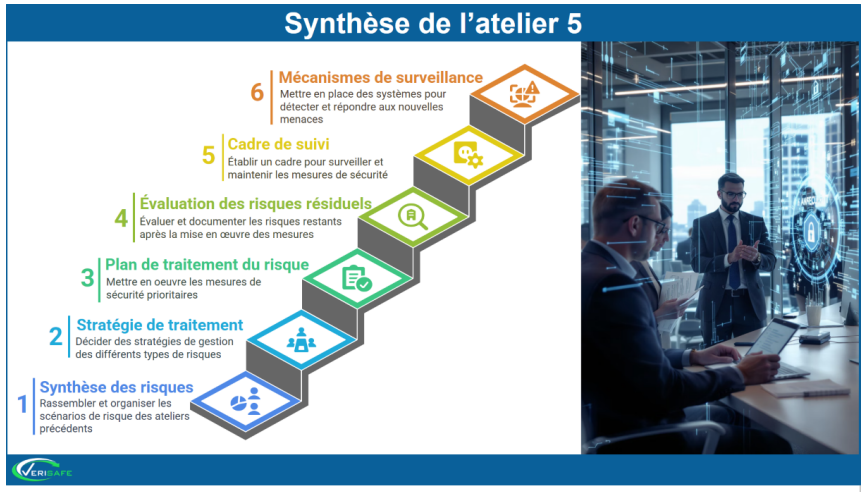
Examen blanc
Étude de cas à réaliser (SAMBOT)

Questions d'examen
QCM et questions ouvertes

Module A0 à A5

Module A6

Support de formation



Diapositive projetée en vidéo

Cet atelier 5 constitue l'aboutissement concret de la démarche EBIOS RM, celui du passage à l'action. Il s'appuie sur une série d'étapes essentielles permettant de transformer l'analyse en décisions opérationnelles et stratégiques.

On démarre par la **synthèse des scénarios de risque** identifiés dans les ateliers précédents, offrant une vision consolidée des risques avec une cartographie claire selon gravité et vraisemblance. Cette cartographie est un outil fondamental pour prioriser et orienter les efforts.

Vient ensuite la définition de la **stratégie de traitement du risque**, étape clé où la direction doit être pleinement impliquée. Il s'agit de décider, pour chaque risque, s'il est accepté, réduit, partagé, ou s'il conduit à un refus d'activité. Ces décisions stratégiques conditionnent la suite.

Sur cette base, on élabore un **plan de traitement du risque (PTR),** regroupant les mesures concrètes — organisationnelles, techniques, contractuelles — qui seront mises en œuvre. Ce plan précise responsabilités, ressources, délais et priorités, garantissant ainsi un pilotage structuré et réaliste.

Une fois les mesures en place, **on évalue les risques résiduels**, ceux qui persistent malgré les actions. Ils sont eux aussi cartographiés pour suivre l'évolution du niveau de risque et éclairer les décisions d'acceptation ou d'ajustement.

Enfin, pour assurer la pérennité et l'efficacité de la démarche, l'atelier se conclut par la mise en place d'un **cadre de suivi et de mécanismes de surveillance**. Ces dispositifs permettent d'adapter en continu l'analyse de risque à un environnement dynamique et évolutif, garantissant ainsi la réactivité face aux nouvelles menaces et aux transformations de l'organisation.

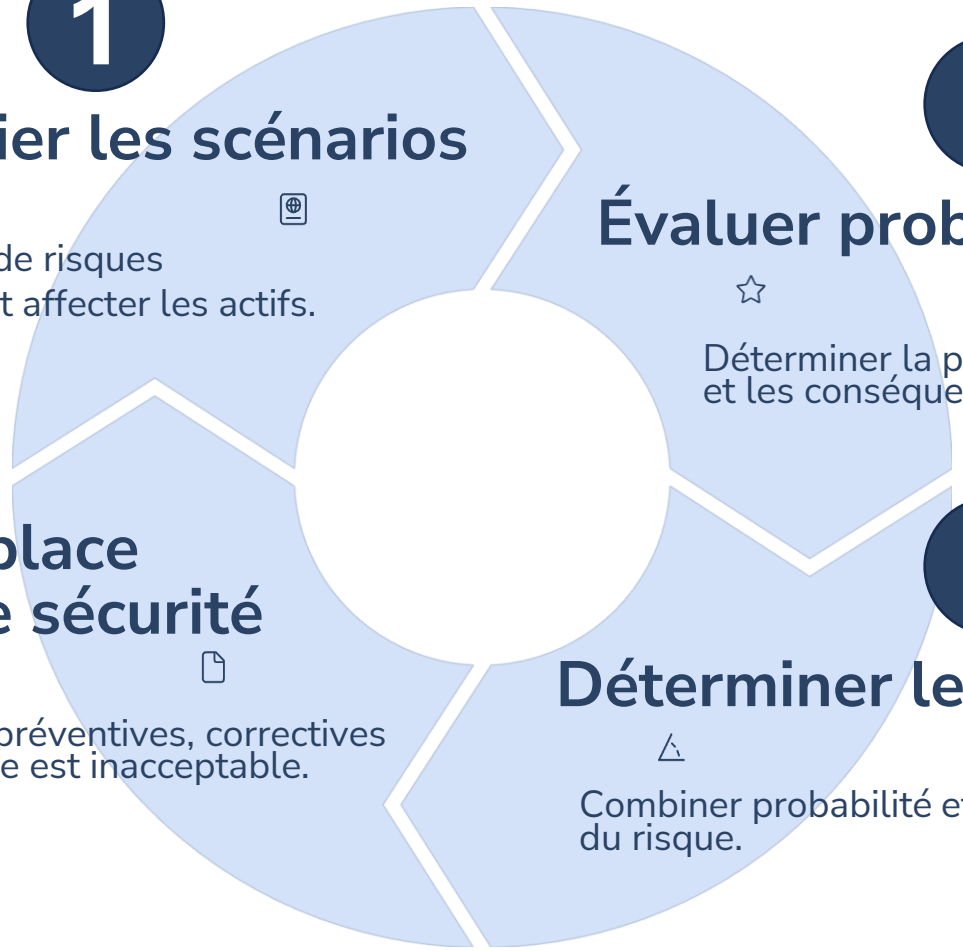
En résumé, l'atelier 5 est un véritable chantier de pilotage de la sécurité, ancrant la gestion des risques dans la durée et la réalité opérationnelle.

Résumé de la transcription du discours du formateur

Généré par IA

Notes prises par le participant

La sécurité par une approche risque



1 Identifier les scénarios

Recenser les scénarios de risques potentiels qui pourraient affecter les actifs.

2 Évaluer probabilité et impact

Déterminer la probabilité d'occurrence et les conséquences potentielles.

3 Déterminer le niveau de risque

Combiner probabilité et impact pour établir la criticité du risque.

4 Mettre en place des mesures de sécurité

Déployer des mesures préventives, correctives ou détectives si le risque est inacceptable.

La sécurité par une approche risque

Groupe cybercriminel
(threat agent / threat actor)

motivations, moyens

Probabilité d'occurrence
(vraisemblance)

niveau d'exposition

Chiffrement & exfiltration de données

Menace

Cible

Actif(s)
données du SI

Exploite

Possède

Vulnérabilité(s)

Incident de sécurité

Dans EBIOS RM, on parle d'évènement redouté (ER)

C I D

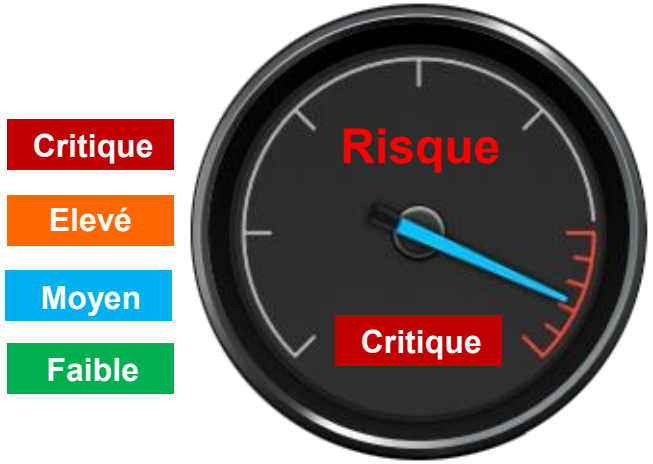
Impact sur les actifs

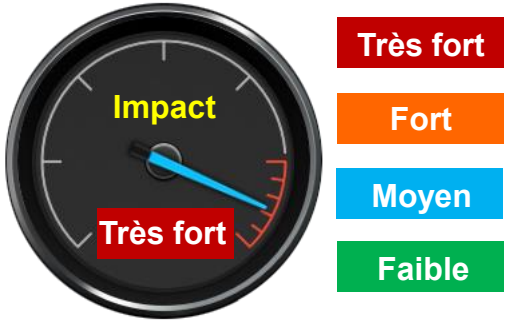
F I J

Conséquences pour l'organisme

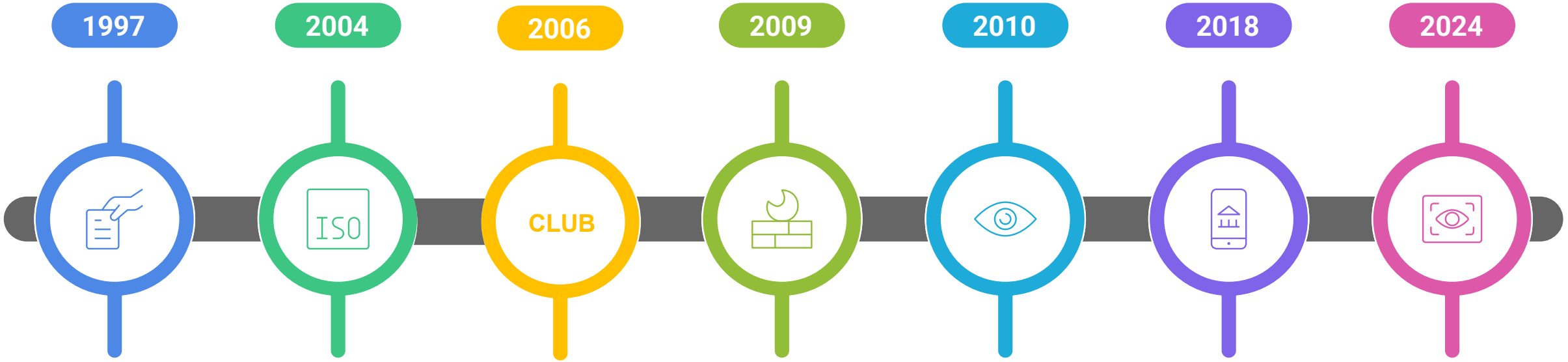
aggravation

Conséquences pour les tiers
(clients, partenaires,…)





Historique d'EBIOS Risk Manager



EBIOS RM → Expression des Besoins et Identification des Objectifs de Sécurité - Risk Manager

APPRÉCIATION DES RISQUES (Risk assessment)

Ensemble du processus d'identification, d'analyse et d'estimation des risques (ISO 31000:2018).

Dans la démarche EBIOS RM, cela correspond aux ateliers 2 (sources de risque), 3 (scénarios stratégiques) et 4 (scénarios opérationnels).

3 Élaborer des scénarios opérationnels

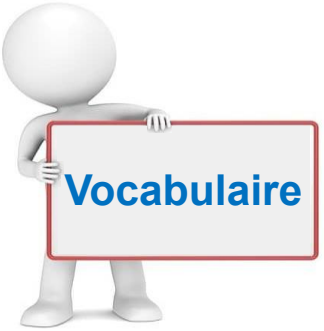
Définir des scénarios détaillés pour évaluer les risques spécifiques

2 Développer des scénarios stratégiques

Créer des scénarios de haut niveau pour comprendre les impacts potentiels

1 Identifier les sources de risque

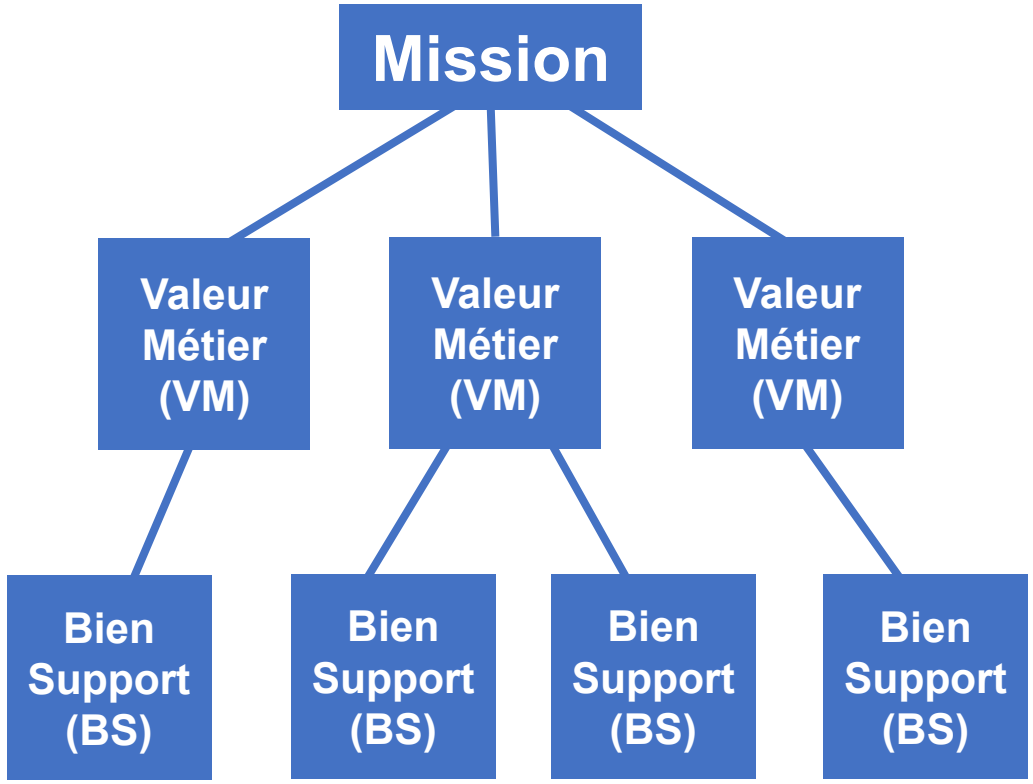
Déterminer les menaces potentielles et leurs origines



Pour toutes les définitions données dans ce chapitre, nous indiquons tout d'abord la définition donnée par l'ANSSI dans le guide EBIOS RM.

MISSION (Mission)

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



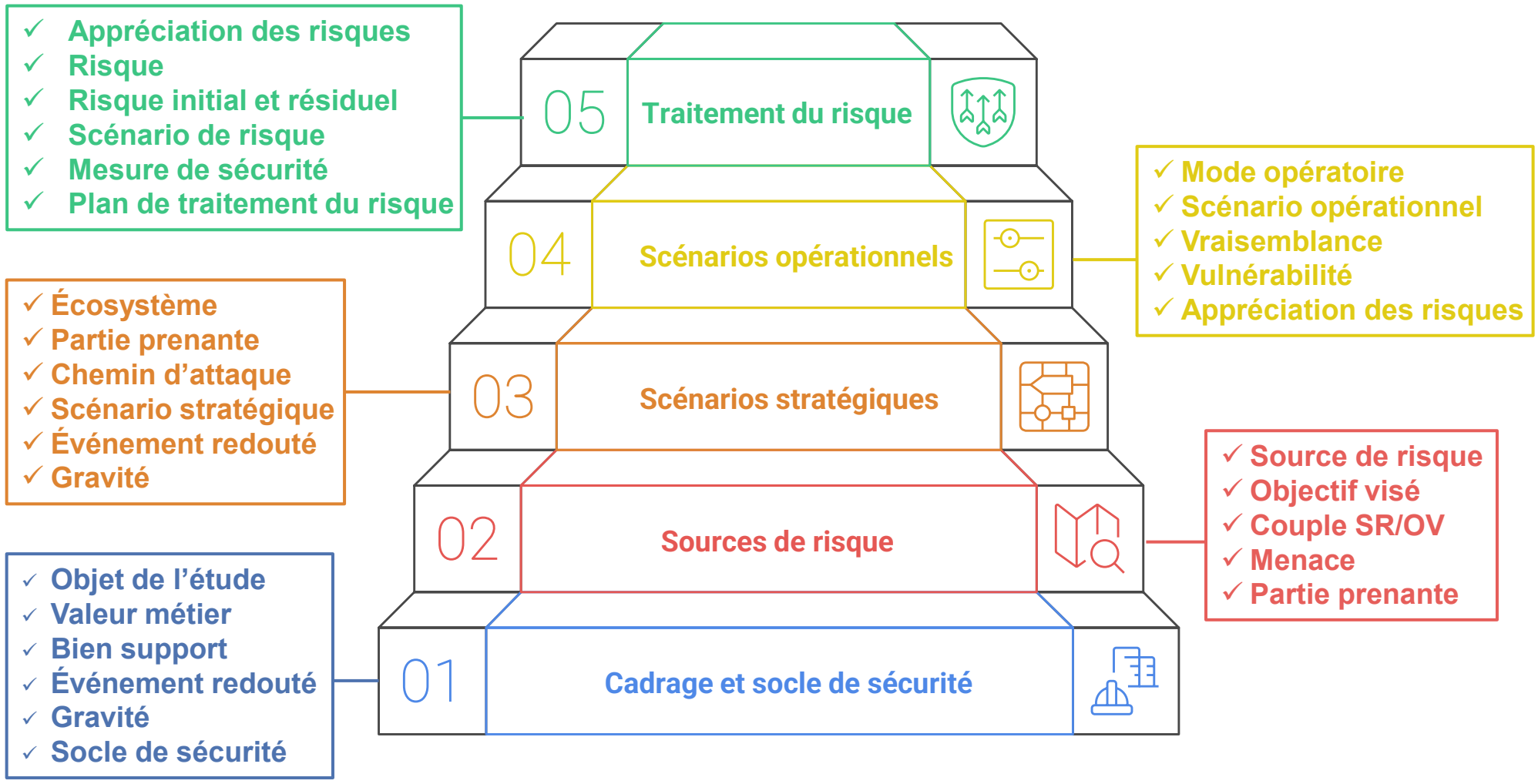
MISSION

Raison d'être
Justification de l'existence de l'objet d'étude

Finalité
Objectif ou résultat souhaité de l'étude

Fonction
Rôle ou tâche de l'objet d'étude

Tour d’horizon des 5 ateliers de la méthode



ERM
v1.0 (07/2025)

EBIOS RISK MANAGER

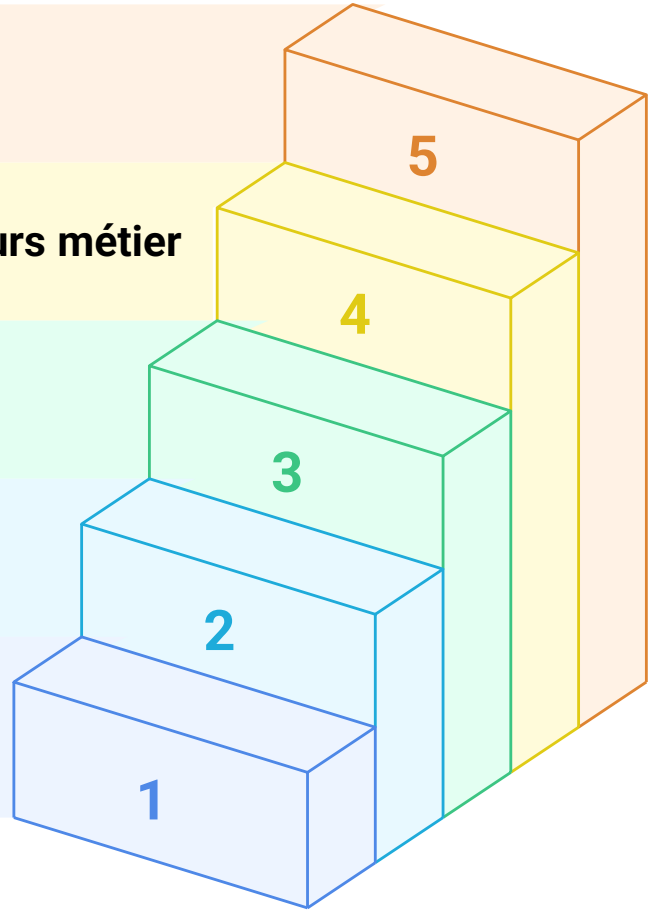
A1

Atelier 1 : Cadrage et socle de sécurité

VERISAFE
L'EXPERTISE CYBERSÉCURITÉ

Les objectifs de l’atelier

- Examiner les mesures de sécurité existantes et les écarts avec les référentiels
- Identifier les risques potentiels pour les valeurs métier
- Reconnaître les actifs et processus critiques
- Définir les limites de l'étude des risques
- Établir clairement les objectifs de l'analyse de risques



Quels sont les participants ?

🎯 Objectif de la réunion de lancement (kick-off)

Aligner les parties prenantes sur :

- Les objectifs du projet
- La méthode utilisée
- Le périmètre étudié
- Les rôles et responsabilités

👥 Participants incontournables

- **Direction / Décideur**
  Valide les orientations stratégiques et garantit l'alignement de l'étude avec les priorités organisationnelles
- **Métiers**
  Identifient les processus critiques, les valeurs métier et expriment les événements redoutés
- **RSSI / Responsable cybersécurité**
  Apporte sa connaissance des exigences de sécurité et évalue le socle de sécurité existant
- **DSI / Responsable IT**
  Identifie les biens supports, l'infrastructure technique et les dépendances critiques

👤 Autres acteurs possibles (selon contexte)

- **Responsable conformité**
- **Juriste**
- **Chef de projet**
- **Prestataire externe**

🛠️ Outil recommandé : Matrice RACI

- **Permet de clarifier les rôles**

Les livrables de l’atelier

4 Socle de sécurité
Évaluer les mesures de sécurité existantes et les lacunes.

3 Événements redoutés
Évaluer les risques potentiels et leur impact.

2 Définition du périmètre
Identifier les missions et les valeurs métier.

1 Éléments de cadrage
Établir la gouvernance et les objectifs de l'étude.

ERM
v1.0 (07/2025)

EBIOS RISK MANAGER

A2

Atelier 2 : Sources de risque (SR)

VERISAFE
L'EXPERTISE CYBERSÉCURITÉ

Évaluer la pertinence des couples SR/OV

Processus d'Évaluation

- Attendre l'épuisement des idées lors de la phase de brainstorming
- Effectuer un premier tri intuitif basé sur l'expertise collective
- Appliquer les trois critères d'évaluation formels (motivation, ressources, activité)
- Coter chaque couple SR/OV selon ces critères
- Sélectionner les couples les plus pertinents pour les ateliers suivants

Motivation

Évaluer si la source de risque a un véritable intérêt à atteindre cet objectif. L'action correspond-elle à ses intentions habituelles ? Par exemple, un groupe activiste ciblant une campagne de vaccination est cohérent avec ses motivations idéologiques.

Ressources

Analyser les moyens dont dispose la source de risque : compétences techniques, outils, personnel, temps, financement et infrastructures. Un cybercriminel disposant d'infrastructures sophistiquées présente un niveau de menace plus élevé qu'un prestataire mécontent avec un simple accès VPN.

Activité

Déterminer si cette source de risque est ou a été active dans votre secteur ou environnement. Les antécédents d'attaques contre des organisations similaires augmentent la crédibilité de la menace. Utilisez des rapports publics et une veille sectorielle pour votre évaluation.

Sélectionner les couples SR / OV pertinents

❑ Pertinence évaluée

- ➢ Prioriser les couples ayant une forte motivation, des ressources disponibles et une activité confirmée

❑ Complémentarité

- ➢ Diversifier les types de menaces pour éviter la redondance et obtenir une vision globale

❑ Quantité optimale

- ➢ Généralement 3 à 6 couples SR-OV bien choisis suffisent (adaptable selon la complexité du système)

Tableau d'évaluation (exemple)

IDENTIFICATION		COTATION			CARACTÉRISATION				ÉVALUATION	
Source de risque (SR)	Objectif visé (OV)	Motivation	Ressources	*Activité*	*Modes opératoires*	*Secteurs d'activités*	*Arsenal d'attaque*	*Faits d'armes*	Pertinence du couple SR/OV	Choix P1/P2
				Colonnes facultatives						

		Motivation		
		+	+ +	+ + +
Ressources	+ + +	MOYEN	ÉLEVÉ	ÉLEVÉ
	+ +	FAIBLE	MOYEN	ÉLEVÉ
	+	FAIBLE	FAIBLE	MOYEN

Source : ANSSI - Fiche méthode 4

ERM
v1.0 (07/2025)

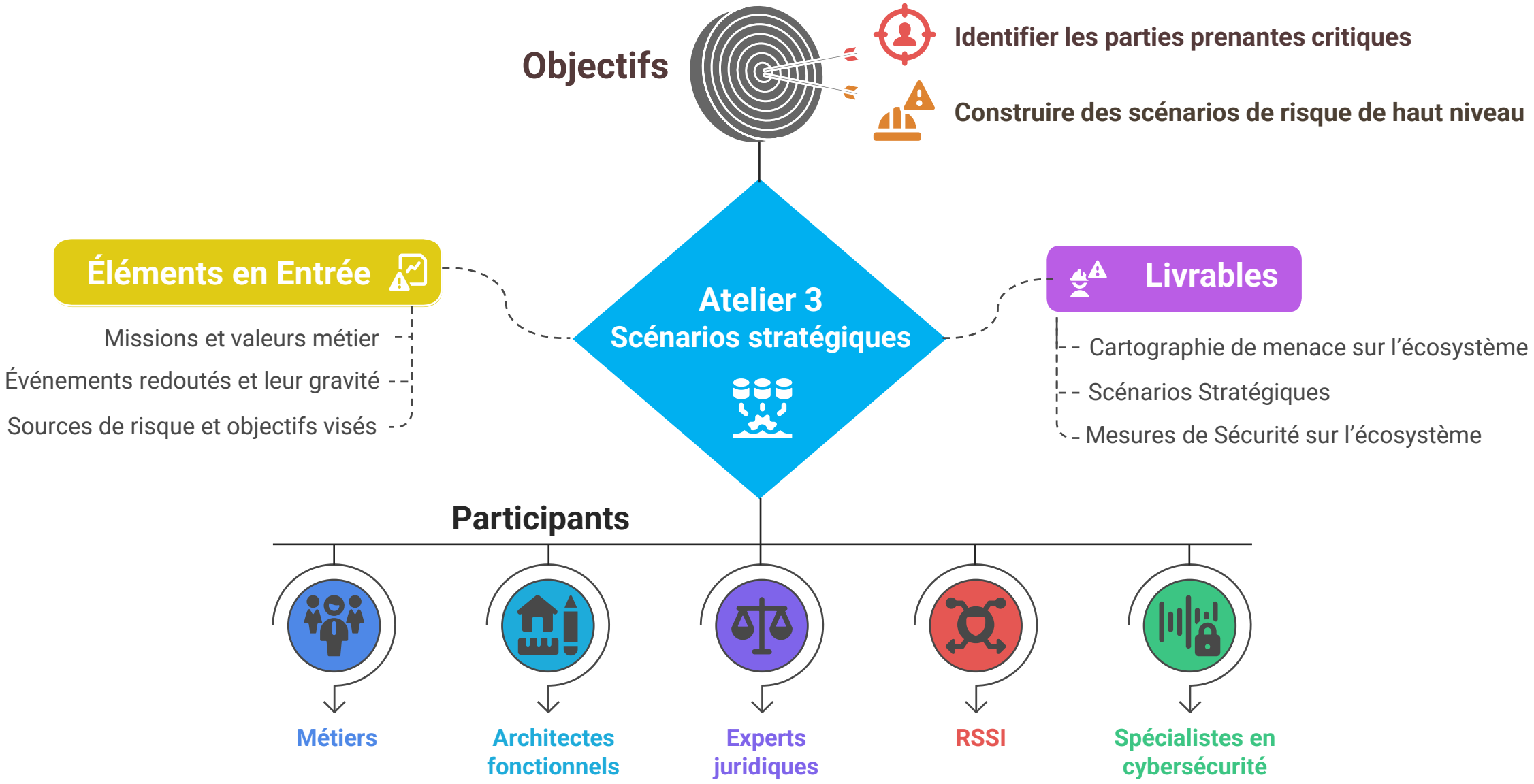
EBIOS RISK MANAGER

A3

Atelier 3 : Scénarios stratégiques

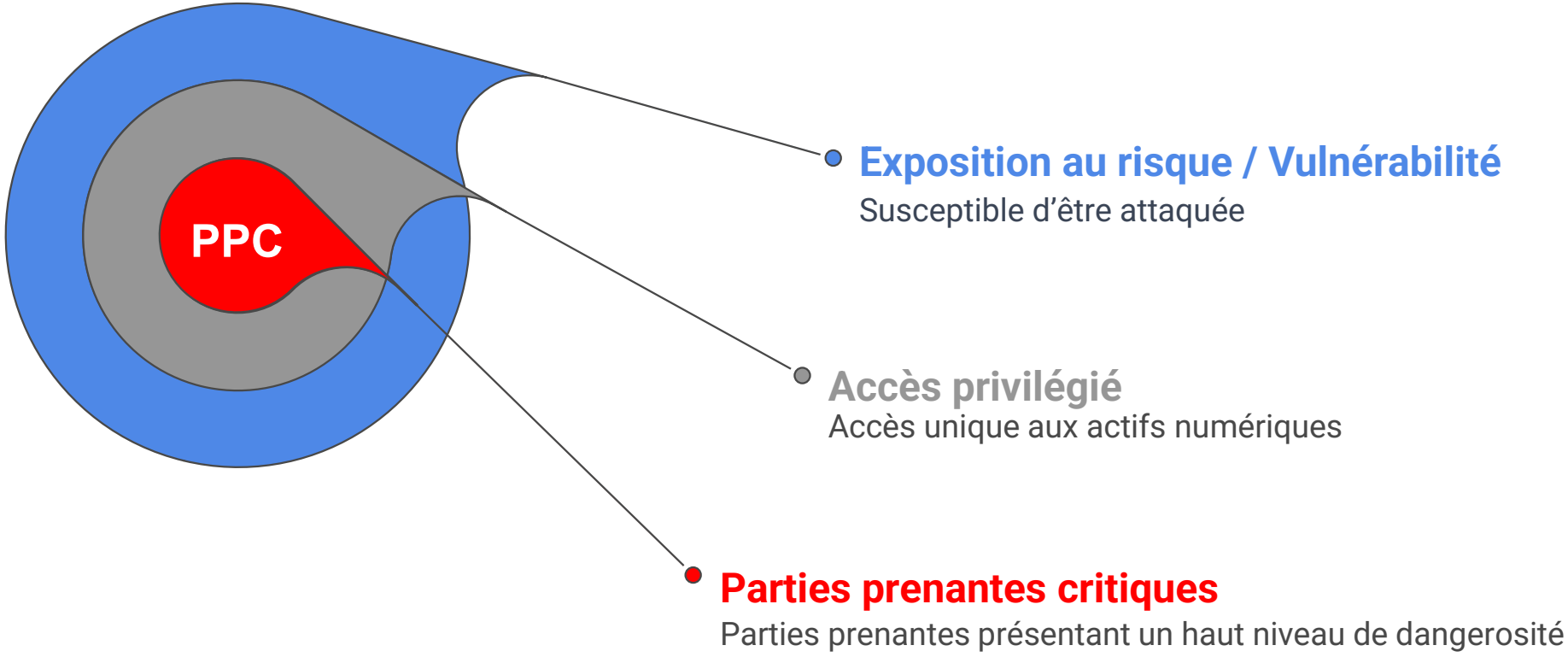
VERISAFE
L'EXPERTISE CYBERSÉCURITÉ

Objectifs, participants et livrables



PARTIE PRENANTE CRITIQUE (PPC) (Critical stakeholder)

Partie prenante de l'écosystème susceptible de constituer un vecteur d'attaque privilégié, du fait par exemple de son accès numérique privilégié à l'objet de l'étude, de sa vulnérabilité ou de son exposition au risque.
Les parties prenantes critiques sont identifiées dans l'estimation de la dangerosité des parties prenantes de l'écosystème.



NIVEAU DE DANGEROSITE D'UNE PARTIE PRENANTE

Donne une mesure du potentiel de risque que fait peser une partie prenante de l'écosystème sur l'objet de l'étude, compte tenu de son interaction avec lui, de sa vulnérabilité, de son exposition au risque, de sa fiabilité, etc.

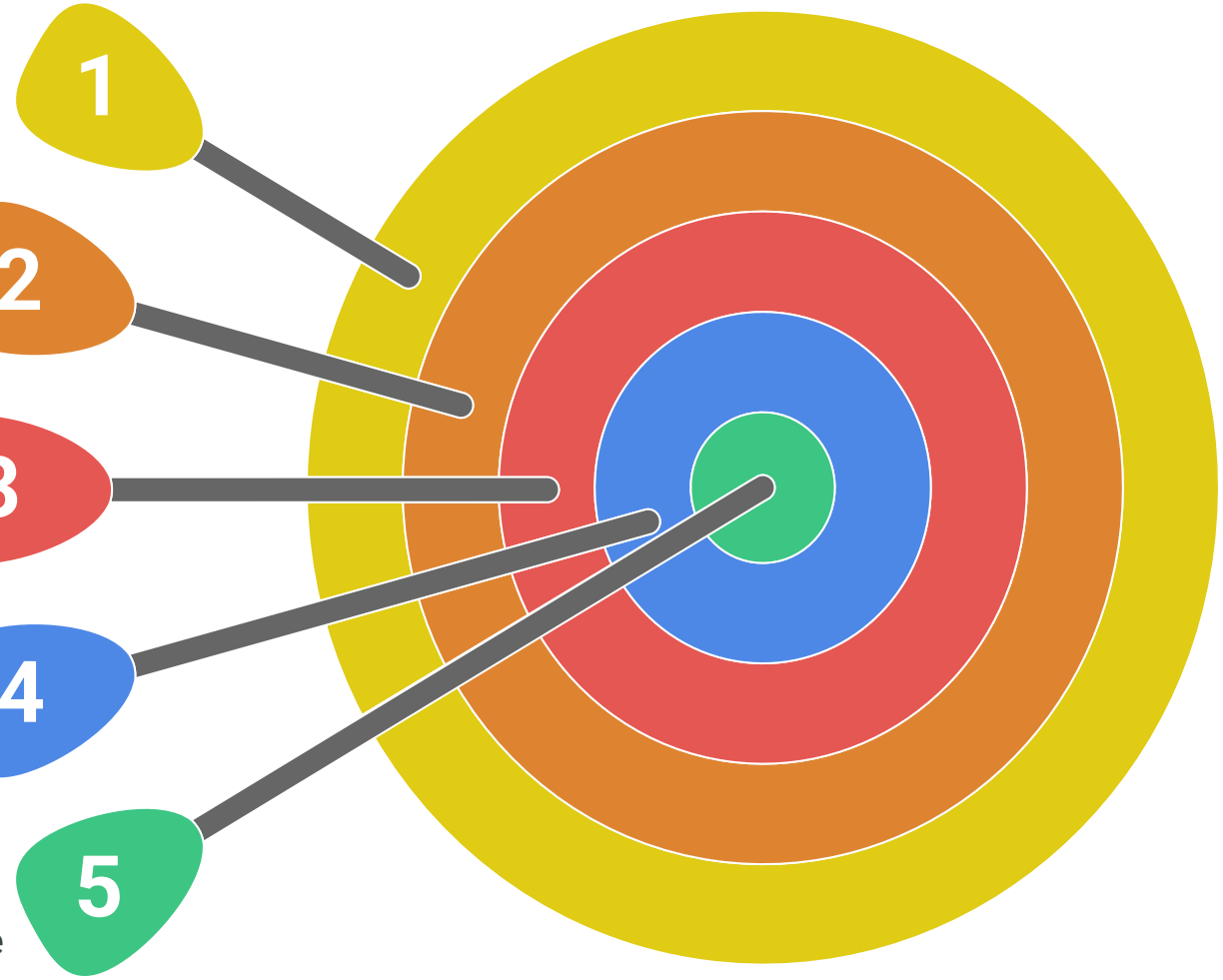
Menace potentielle
Risque global posé par la partie prenante

Fiabilité en matière de Cybersécurité
Fiabilité de la partie prenante dans la sécurité

Exposition aux menaces
Vulnérabilité aux menaces externes

Vulnérabilité
Faiblesses internes de la partie prenante

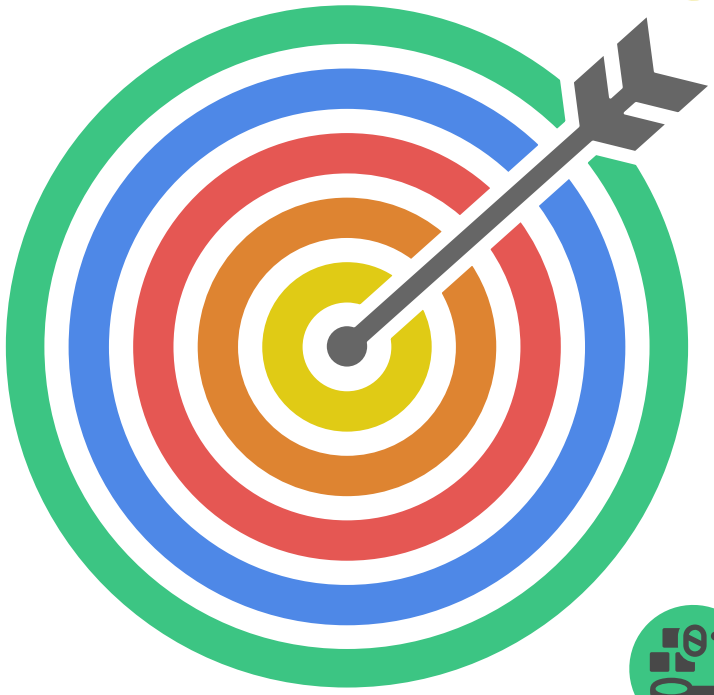
Interaction avec le système
Nature de l'engagement de la partie prenante



SCÉNARIO STRATÉGIQUE (Strategic scenario)

Chemins d'attaque allant d'une source de risque à un objectif visé en passant par l'écosystème et les valeurs métier de l'objet étudié.

Les scénarios stratégiques sont estimés en termes de gravité.



Objectif visé
Résultat final souhaité par une source de risque

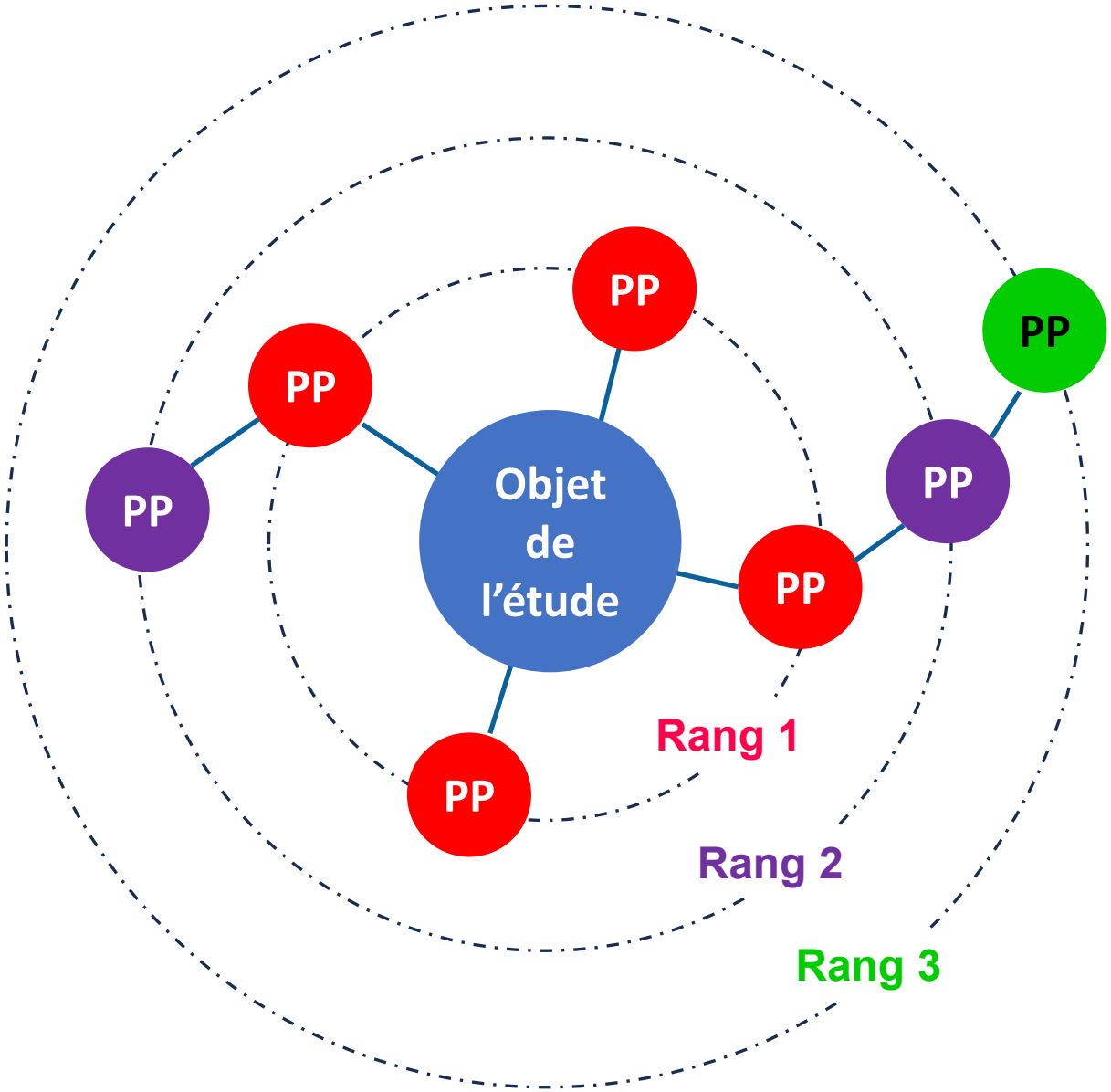
Valeur métier
Composante importante pour l'organisation dans l'accomplissement de sa mission

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

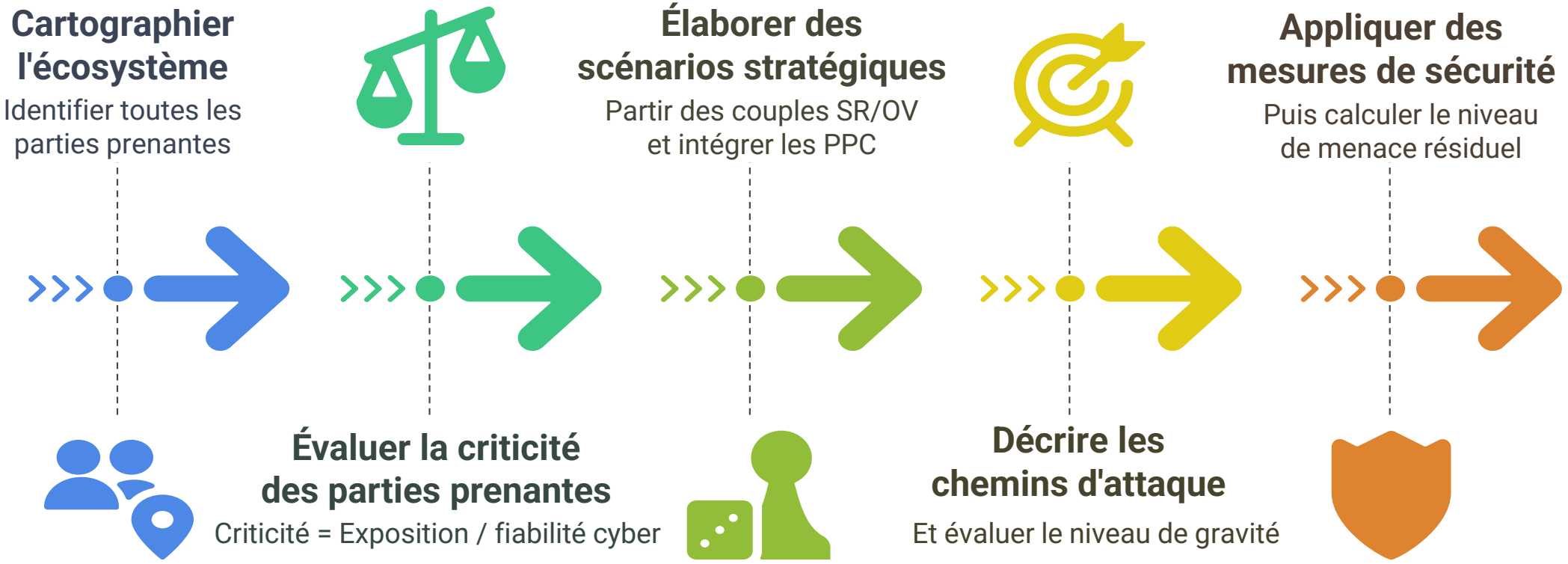
Source de Risque
Élément, personne, groupe de personnes ou organisation susceptible d'engendrer un risque

Gravité
Mesure de l'impact préjudiciable en cas de réussite du scénario

Parties prenantes en cascade



Synthèse de l’atelier



ERM
v1.0 (07/2025)

EBIOS RISK MANAGER

A4

Atelier 4 : Scénarios opérationnels

VERISAFE
L'EXPERTISE CYBERSÉCURITÉ

Elaboration des scénarios opérationnels

Une approche réaliste des cyberattaques

Une attaque réussie repose rarement sur une seule vulnérabilité, mais plutôt sur une succession d'actions coordonnées exploitant plusieurs failles :

- Failles techniques (ex: configurations réseau)
- Failles organisationnelles (ex: processus défaillants)
- Failles humaines (ex: mots de passe faibles)
- Failles physiques (ex: accès non sécurisés)

Des vulnérabilités, anodines individuellement, peuvent devenir critiques lorsqu'elles sont combinées dans un enchaînement logique et structuré.

Méthodologie de construction des scénarios

Identification

Utiliser les scénarios stratégiques de l'atelier 3 et la cartographie du système d'information

Modélisation

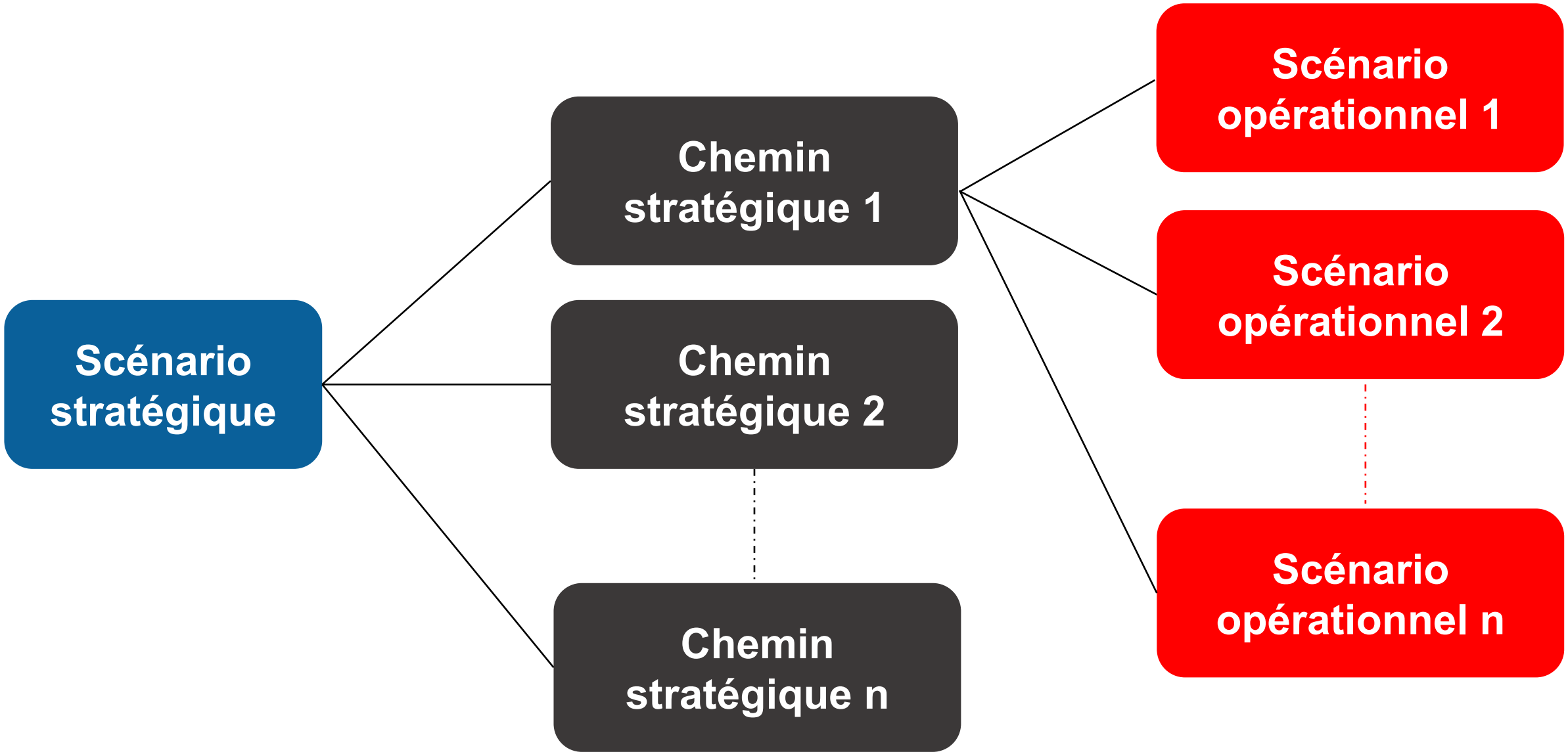
S'appuyer sur des référentiels comme la Cyber Kill Chain ou le framework MITRE ATT&CK

Représentation

Élaborer des schémas d'attaque ou des graphes visuels comme recommandé par l'ANSSI

Un scénario opérationnel efficace décrit un enchaînement cohérent et réaliste montrant comment une source de risque pourrait atteindre un objectif stratégique en exploitant plusieurs failles à travers des biens supports clairement identifiés.

Chemin d’attaque stratégique & Scénario opérationnel

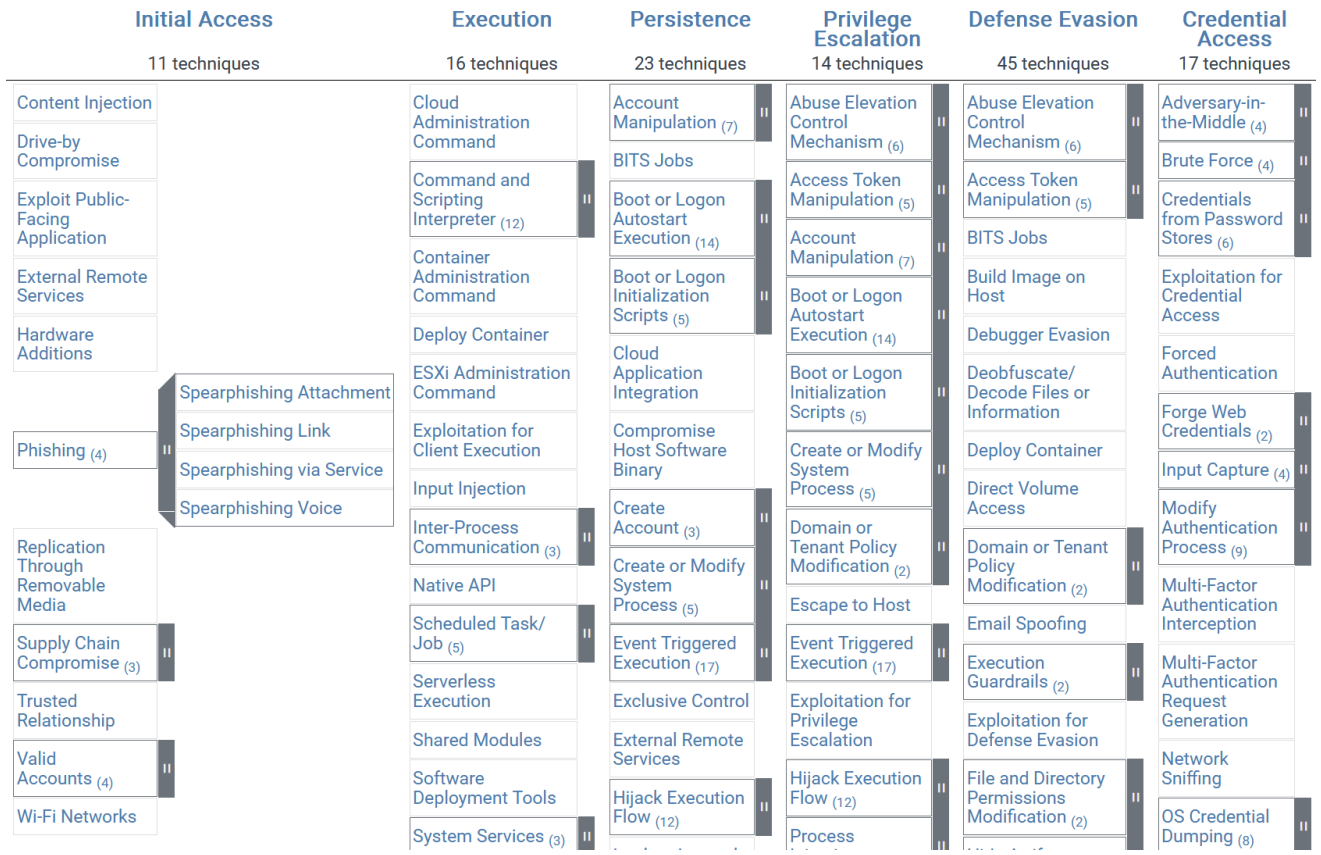


ACTION ÉLÉMENTAIRE (Elementary action)

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

EXEMPLES : exploiter une vulnérabilité, envoyer un email piégé, effacer des traces, augmenter des privilèges.

Les actions élémentaires correspondent aux techniques et sous-techniques du framework MITRE ATT&CK



Évaluation de la vraisemblance avec la méthode avancée

ÉCHELLE DE PROBABILITÉ DE SUCCÈS D'UNE AE	
NIVEAU	**DESCRIPTION**
4 - QUASI-CERTAINE	Probabilité de succès quasi-certaine > 90%
3 - TRÈS ÉLEVÉE	Probabilité de succès très élevée > 60%
2 - SIGNIFICATIVE	Probabilité de succès significative > 20%
1 - FAIBLE	Probabilité de succès faible < 20%
0 - TRÈS FAIBLE	Probabilité de succès très faible < 3%

$$\text{Indice\_Pr}(AE_n) = \text{Min}\left\{\text{Indice\_Pr}(AE_n), \text{Max}(\text{Indices\_Pr}(AE_{n-1}))\right\}$$

cumulé intermédiaire — *cumulés intermédiaires*

Plus le niveau est élevé, plus c'est dangereux !

ÉCHELLE DE DIFFICULTÉ TECHNIQUE D'UNE AE	
NIVEAU	**DESCRIPTION**
4 – TRÈS ÉLEVÉE	Difficulté très élevée : Ressources très importantes nécessaires
3 – ÉLEVÉE	Difficulté élevée : Ressources importantes nécessaires
2 – MODÉRÉE	Difficulté modérée : Ressources significatives nécessaires
1 – FAIBLE	Difficulté faible : Ressources faibles nécessaires
0 – NÉGLIGEABLE	Difficulté négligeable, voire nulle : Ressources négligeables ou déjà disponibles

$$\text{Indice\_Diff}(AE_n) = \text{Max}\left\{\text{Indice\_Diff}(AE_n), \text{Min}(\text{Indices\_Diff}(AE_n\_1))\right\}$$

cumulé intermédiaire — *cumulés intermédiaires*

Plus le niveau est élevé, moins c'est dangereux !

Calcul de la vraisemblance : méthode avancée (1/2)

Indice_Diff (*AEn*) = Max {Indice_Diff(*AEn*), ~~Min (Indices_Diff(*AEn*_1))~~}

cumulé intermédiaire — ~~*cumulés intermédiaires*~~

	CONNAITRE			RENTRER			TROUVER			EXPLOITER			MODE OPÉRATOIRE	SCÉNARIO OP.
Mode Opératoire	Action Elémentaire	Difficulté	Difficulté cumulée	Action Elémentaire	Difficulté	Difficulté cumulée	Action Elémentaire	Difficulté	Difficulté cumulée	Action Elémentaire	Difficulté	Difficulté cumulée	Difficulté globale	**Difficulté**
MO1	AE_1	3	3	AE_2	2	3	AE_3	4	4	AE_4	3	4	4	
MO2	AE_5	3	3	AE_6	4	4				AE_7	4	4	4	**3**
MO3	AE_8	3	3	AE_9	2	3	AE_{10}	3	3	AE_{11}	3	3	3	

Max des Diff(*AEn*)

Min des Diff(*MOn*)

Calcul de la vraisemblance : méthode avancée (2/2)

Indice_Diff (*AEn*) = Max {Indice_Diff(*AEn*), Min (Indices_Diff(*AEn*_1))}

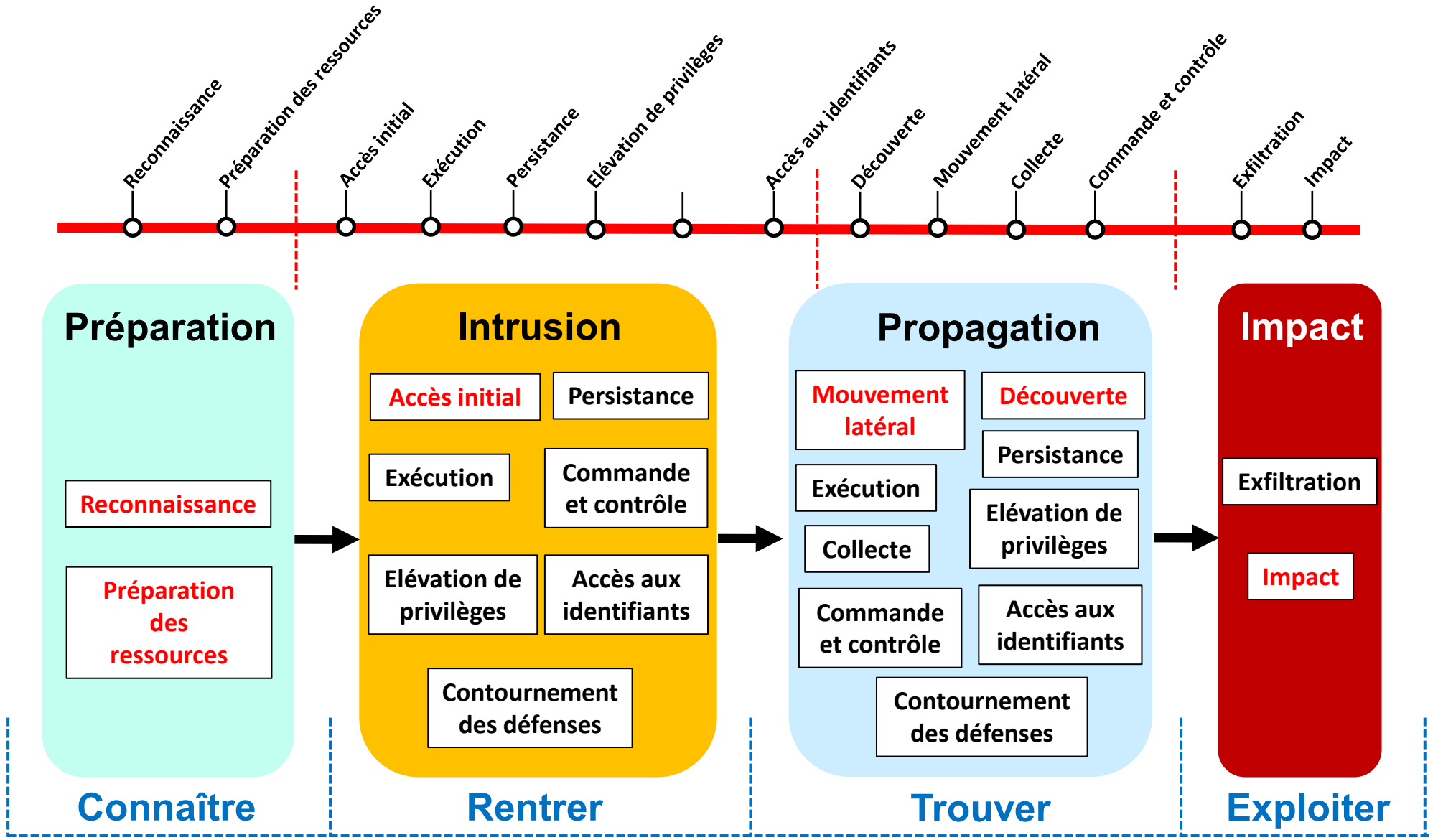
cumulé intermédiaire — *cumulés intermédiaires*

	CONNAITRE			RENTRER				TROUVER						EXPLOITER			MODE OPÉRATOIRE	SCÉNARIO OP.
Mode Opératoire	Action Elémentaire	Difficulté	Difficulté cumulée	Action Elémentaire	Difficulté	Difficulté retenue	Difficulté cumulée	Action Elémentaire	Difficulté	Difficulté cumulée	Action Elémentaire	Difficulté	Difficulté cumulée	Action Elémentaire	Difficulté	Difficulté cumulée	Difficulté globale	**Difficulté**
MO1	AE_1	3	3	AE_3	2	2	3	AE_7	4	4				AE_{10}	3	4	4	**3**
				AE_4	4													
				AE_5	3													
MO2	AE_2	3	3	AE_6	2		3	AE_8	2	3	AE_9	1	3	AE_{11}	3	3	3	

Si dans MO1, on peut « rentrer » par AE_3 OU AE_4 OU AE_5 alors on retient MIN (AE_3, AE_4, AE_5)

Si pour « trouver » dans MO2, il faut effectuer AE_8 ET AE_9 alors on retient MAX (AE_8, AE_9)

MITRE ATT&CK & Kill chain de l'ANSSI



ERM
v1.0 (07/2025)

EBIOS RISK MANAGER

A5

Atelier 5 : Traitement du risque

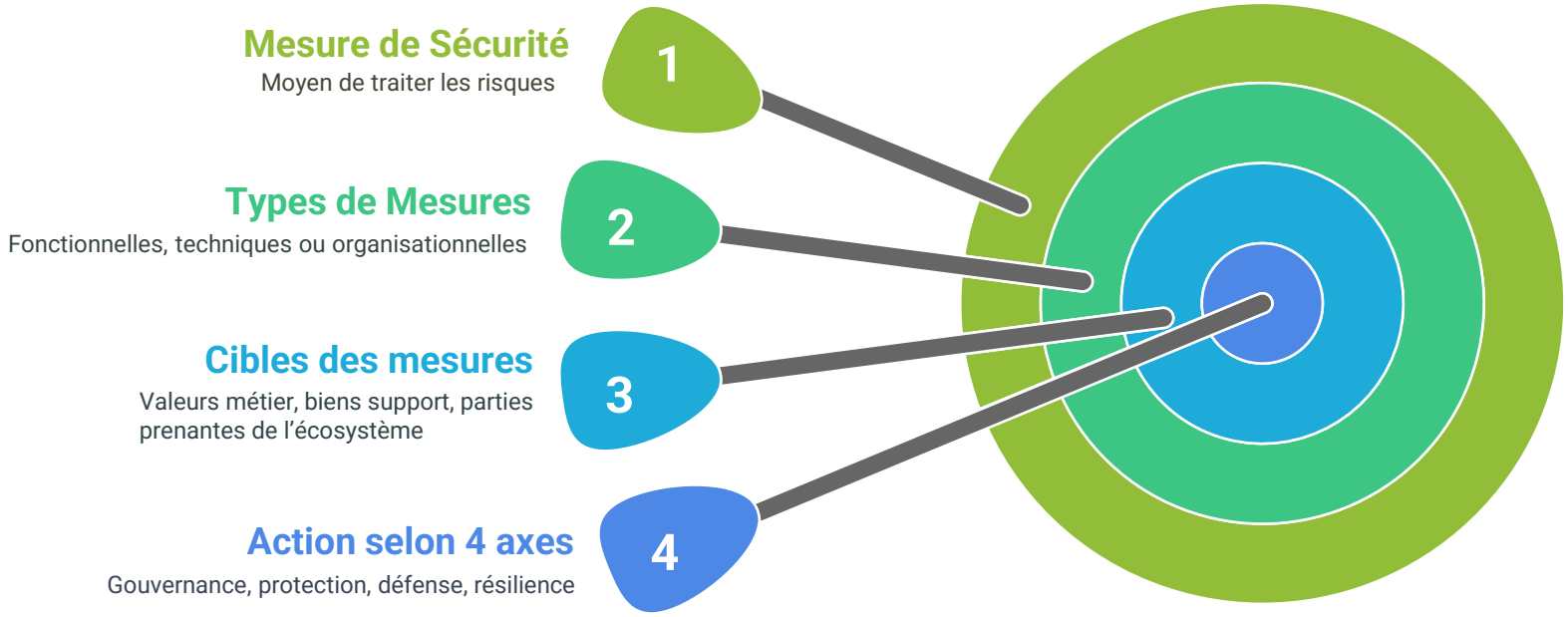
VERISAFE
L'EXPERTISE CYBERSÉCURITÉ

MESURE DE SÉCURITÉ (Security control)

Moyen de traiter un risque prenant la forme de solutions ou d'exigences pouvant être inscrites dans un contrat.

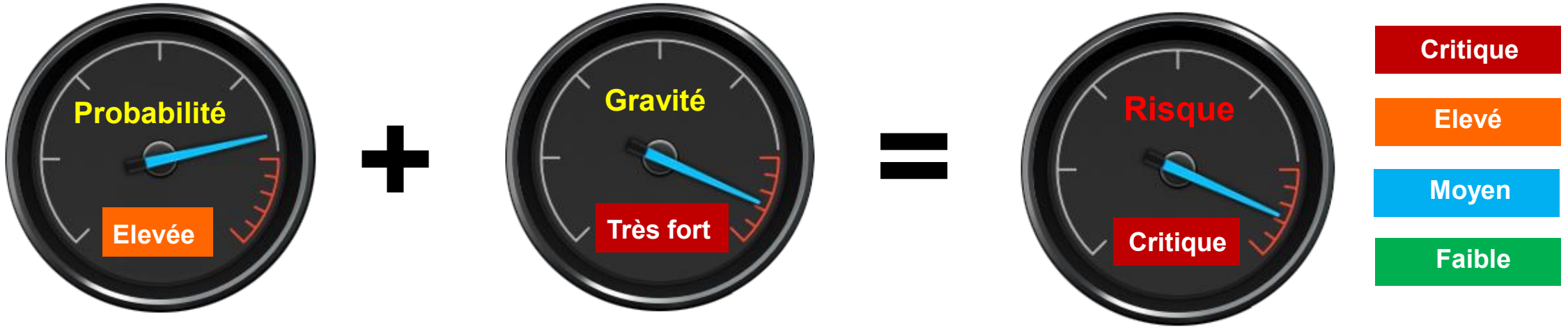
NOTES :

- **une mesure peut être d'ordre fonctionnel, technique ou organisationnel ;**
- **elle peut agir sur une valeur métier, un bien support, une partie prenante de l'écosystème ;**
- **certaines mesures peuvent se renforcer mutuellement en agissant selon des axes complémentaires (gouvernance, protection, défense, résilience).**



NIVEAU DE RISQUE (Risk level)

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



PLAN DE TRAITEMENT DU RISQUE (Risk management plan)

Le plan de traitement du risque (parfois juste noté plan de traitement) formalise l'ensemble des mesures de traitement du risque à mettre en oeuvre.

Il favorise l'élévation du niveau de maturité SSI de l'organisation et permet une gestion progressive des risques résiduels.

Les mesures définies dans le plan de traitement du risque concernent à la fois l'objet étudié et son écosystème.

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

Risque initial, résiduel et stratégie de traitement du risque

RISQUE (Risk)

Possibilité qu'un événement redouté survienne et que ses effets impactent les missions de l'objet de l'étude. Dans le contexte cyber où s'inscrit EBIOS *Risk Manager*, un risque est décrit sous la forme d'un scénario de risque.

RISQUE INITIAL (Initial risk)

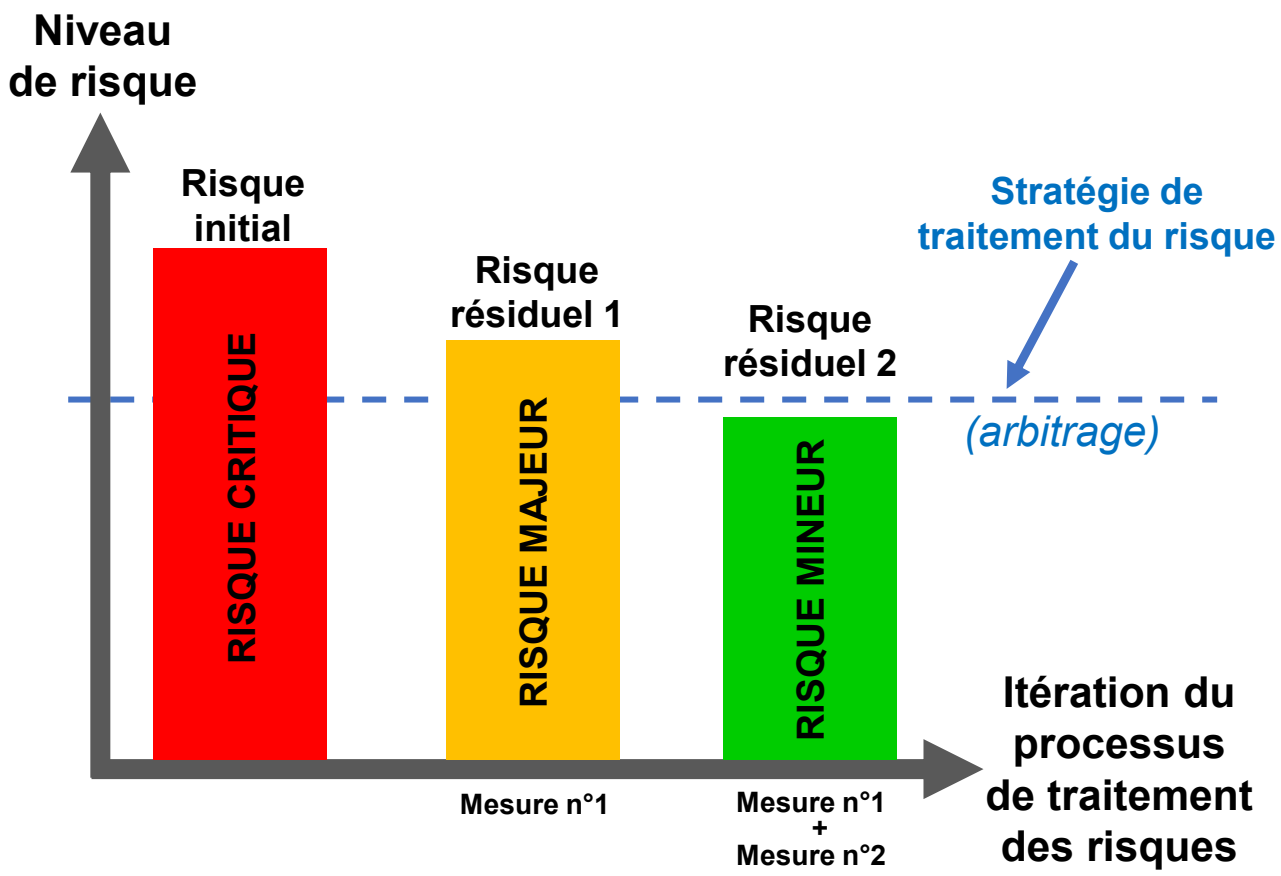
Scénario de risque évalué avant application de la stratégie de traitement du risque. Cette évaluation repose sur la gravité et la vraisemblance du risque.

RISQUE RÉSIDUEL (Residual risk)

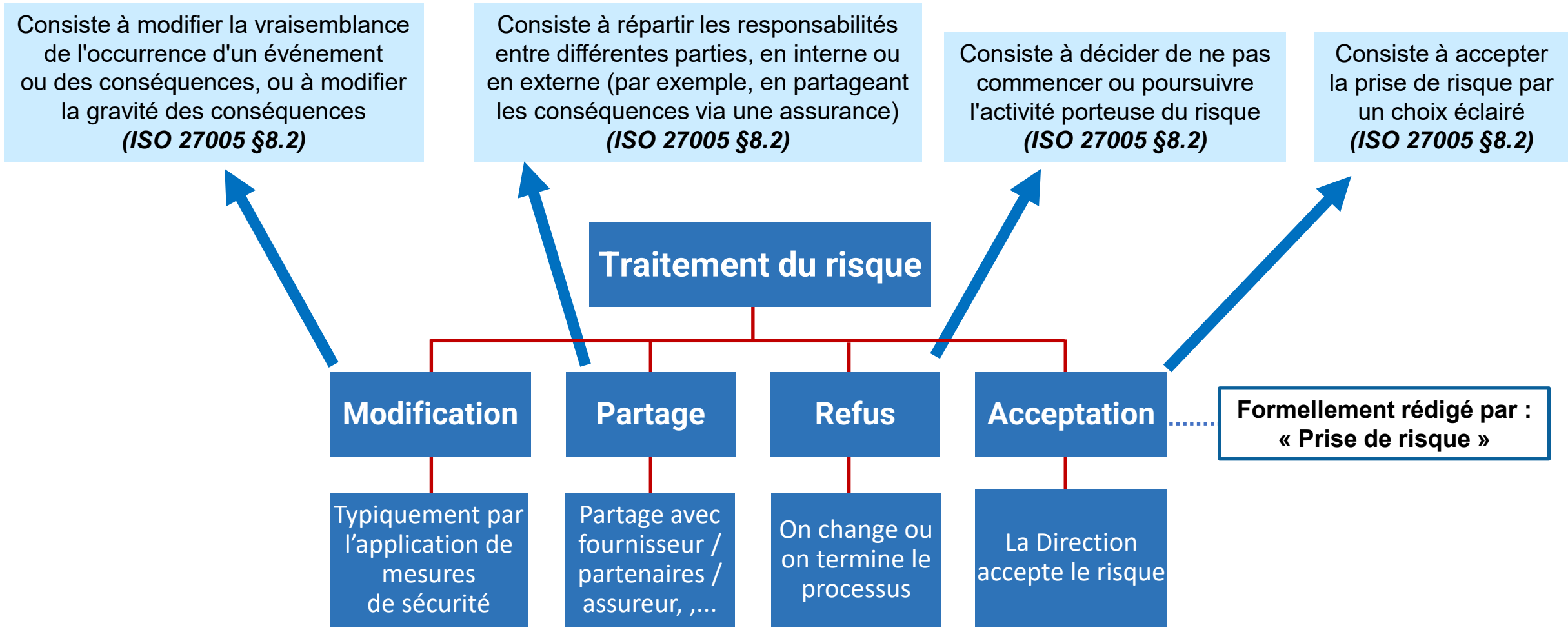
Scénario de risque subsistant après application de la stratégie de traitement du risque. Cette évaluation repose sur la gravité et la vraisemblance du risque.

STRATÉGIE DE TRAITEMENT DU RISQUE

La stratégie de traitement du risque formalise les seuils d'acceptation du risque et un niveau de sécurité à atteindre en cas de non acceptation.



Les 4 options de traitement du risque selon l'ISO 27005:2022



Source : Options appropriées de traitement du risque selon l'ISO 27005:2022 (*§8.2*)

Synthèse de l’atelier

6 Mécanismes de surveillance
Mettre en place des systèmes pour détecter et répondre aux nouvelles menaces

5 Cadre de suivi
Établir un cadre pour surveiller et maintenir les mesures de sécurité

4 Évaluation des risques résiduels
Évaluer et documenter les risques restants après la mise en œuvre des mesures

3 Plan de traitement du risque
Mettre en oeuvre les mesures de sécurité prioritaires

2 Stratégie de traitement
Décider des stratégies de gestion des différents types de risques

1 Synthèse des risques
Rassembler et organiser les scénarios de risque des ateliers précédents