EBIOS RISK MANAGER

TABLE DES MATIÈRES

QU'EST-CE QUE LA MÉTHODE EBIOS RISK MANAGER ?

EBIOS Risk Manager [1] (EBIOS RM) est la méthode d'appréciation et de traitement des risques numériques publiée par l'Agence nationale de la sécurité et des systèmes d'information (ANSSI) avec le soutien du Club EBIOS [2]. Elle propose une boite à outils adaptable, dont l'utilisation varie selon l'objectif du projet et est compatible avec les référentiels normatifs en vigueur, en matière de gestion des risques [3] comme en matière de sécurité du numérique [4].

EBIOS RM permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maitriser. Elle permet aussi de valider le niveau de risque acceptable et de s'inscrire à plus long terme dans une démarche d'amélioration continue. Enfin, cette méthode permet de faire émerger les ressources et arguments utiles à la communication et à la prise de décision au sein de l'organisation et vis-à-vis de ses partenaires.

La méthode EBIOS RM peut être utilisée à plusieurs fins :

- mettre en place ou renforcer un processus de management du risque numérique au sein d'une organisation ;
- apprécier et traiter les risques relatifs à un projet numérique, notamment dans l'objectif d'une homologation de sécurité ;
- définir le niveau de sécurité à atteindre pour un produit ou un service selon ses cas d'usage envisagés et les risques à contrer, dans la perspective d'une certification ou d'un agrément par exemple.

Elle s'applique aussi bien aux organisations publiques ou privées, quels que soient leur taille, leur secteur d'activité et que leurs systèmes d'information soient en cours d'élaboration ou déjà existants.

---

1 EBIOS est une marque déposée par le Secrétariat général de la défense et de la sécurité nationale.
2 Le Club EBIOS est une association de loi 1901 regroupant des experts individuels et organismes, issus des secteurs public ou privé. Il supporte et enrichit le référentiel français de gestion des risques depuis 2003.
3 En particulier la norme ISO 31000:2018.
4 En particulier les normes de la série ISO/IEC 27000.

Une démarche itérative en 5 ateliers

La méthode EBIOS Risk Manager adopte une approche de management du risque numérique partant du plus haut niveau (grandes missions de l'objet étudié) pour atteindre progressivement les fonctions métier et techniques, par l'étude des scénarios de risque possibles. Elle vise à obtenir une synthèse entre « conformité » et « scénarios », en positionnant ces deux approches complémentaires là où elles apportent la plus forte valeur ajoutée. Cette démarche est symbolisée par la pyramide du management du risque numérique (*cf.* figure 1).

L'approche par conformité est utilisée pour déterminer le socle de sécurité sur lequel s'appuie l'approche par scénarios pour élaborer des scénarios de risque particulièrement ciblés ou sophistiqués. Cela suppose que les risques accidentels et environnementaux sont traités *a priori via* une approche par conformité au sein du socle de sécurité. L'appréciation des risques par scénarios, telle que la décrit la méthode EBIOS RM, se concentre donc sur les menaces intentionnelles.

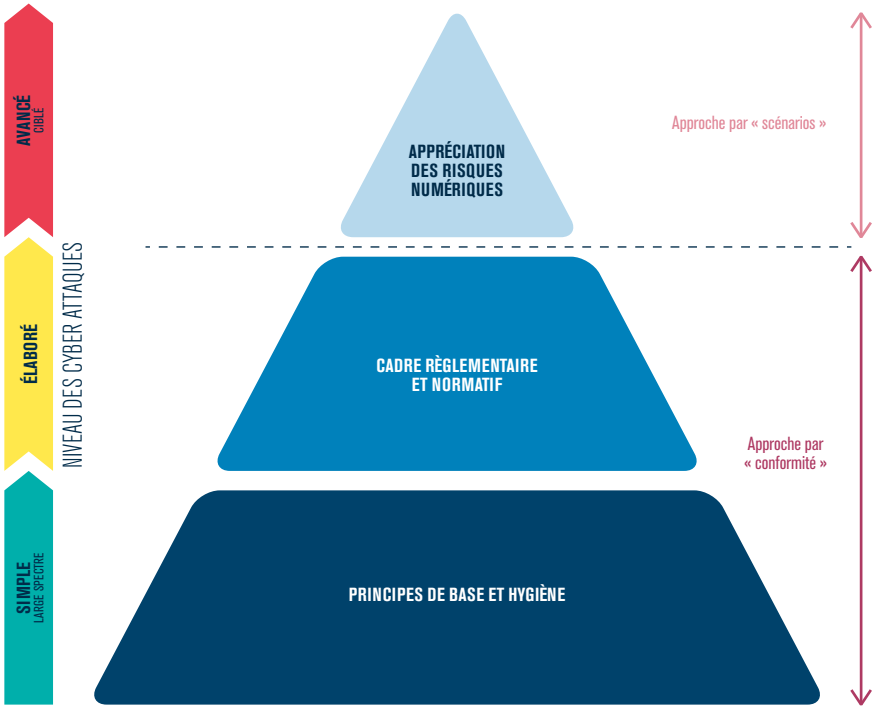
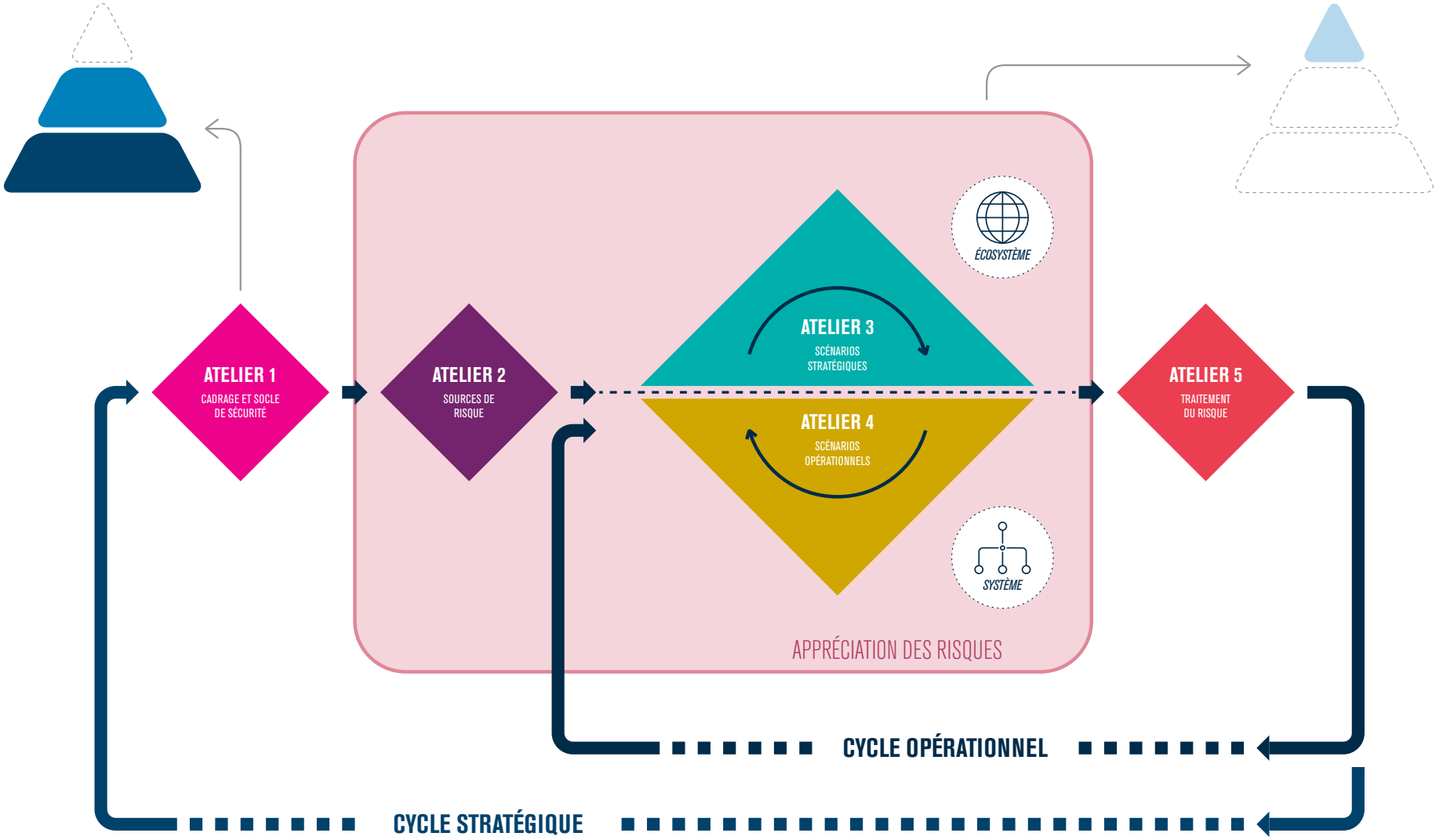


*Figure 1 — **Pyramide du management du risque numérique***

LA MÉTHODE EBIOS RM ADOPTE UNE DÉMARCHE ITÉRATIVE QUI S'ARTICULE AUTOUR DE CINQ ATELIERS.

*Figure 2 — **Une démarche itérative en 5 ateliers***



ATELIER 1

Cadrage et socle de sécurité

Le premier atelier vise à identifier l'objet de l'étude, les participants aux ateliers et le cadre temporel. Au cours de cet atelier, vous recensez les missions, valeurs métier [5] et biens supports relatifs à l'objet étudié. Vous identifiez les événements redoutés associés aux valeurs métier et évaluez la gravité de leurs impacts. Vous définissez également le socle de sécurité et les écarts.

NOTE : l'atelier 1 permet de suivre une approche par « conformité », correspondant aux deux premiers étages de la pyramide du management du risque numérique et d'aborder l'étude du point de vue de la « défense ».

◆

ATELIER 2

Sources de risque

Dans le deuxième atelier, vous identifiez et caractérisez les sources de risque (SR) et leurs objectifs de haut niveau, appelés objectifs visés (OV). Les couples SR/OV jugés les plus pertinents sont retenus au terme de cet atelier. Les résultats sont formalisés dans une cartographie des sources de risque.

5 Les « valeurs métier » correspondent aux « biens essentiels » de la méthode EBIOS 2010.

ATELIER 3

Scénarios stratégiques

Dans l'atelier 3, vous allez acquérir une vision claire de l'écosystème et établir une cartographie de menace numérique de celui-ci vis-à-vis de l'objet étudié. Ceci va vous permettre de bâtir des scénarios de haut niveau, appelés scénarios stratégiques. Ils représentent les chemins d'attaque qu'une source de risque est susceptible d'emprunter pour atteindre son objectif. Ces scénarios se conçoivent à l'échelle de l'écosystème et des valeurs métier de l'objet étudié. Ils sont évalués en termes de gravité. À l'issue de cet atelier, vous pouvez déjà définir des mesures de sécurité sur l'écosystème.

◆

ATELIER 4

Scénarios opérationnels

Le but de l'atelier 4 est de construire des scénarios techniques reprenant les modes opératoires susceptibles d'être utilisés par les sources de risque pour réaliser les scénarios stratégiques. Cet atelier adopte une démarche similaire à celle de l'atelier précédent mais se concentre sur les biens supports critiques. Vous évaluez ensuite le niveau de vraisemblance des scénarios opérationnels obtenus.

NOTES

- Les ateliers 3 et 4 s'alimentent naturellement au cours d'itérations successives.
- Les ateliers 2, 3 et 4 permettent d'apprécier les risques, ce qui constitue le dernier étage de la pyramide du management du risque numérique. Ils sollicitent le socle de sécurité selon des axes d'attaque différents, pertinents au regard des menaces considérées et en nombre limité pour en faciliter l'analyse.

ATELIER 5

Traitement du risque

Le dernier atelier consiste à réaliser une synthèse de l'ensemble des risques étudiés en vue de définir une stratégie de traitement du risque. Cette dernière est ensuite déclinée en mesures de sécurité inscrites dans un plan d'amélioration continue. Lors de cet atelier, vous établissez la synthèse des risques résiduels et définissez le cadre de suivi des risques.

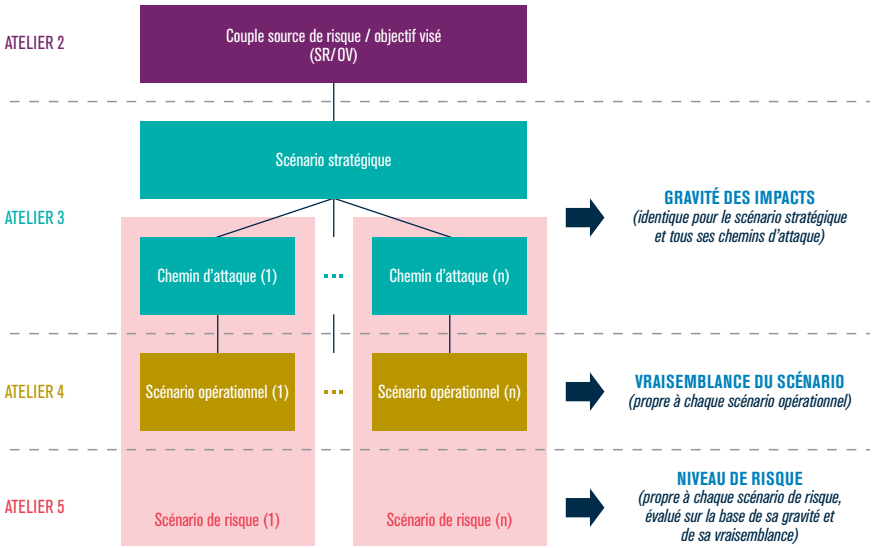


*Figure 3 — **Lien entre les différents ateliers***

NOTE : chaque chemin d'attaque d'un scénario stratégique donne lieu à un scénario opérationnel. Un scénario de risque correspond à l'association d'un chemin d'attaque et de son scénario opérationnel.

LES CYCLES

La démarche prévoit deux cycles, dont les durées sont définies lors du premier atelier :

- un cycle stratégique revisitant l'ensemble de l'étude et en particulier les scénarios stratégiques ;
- un cycle opérationnel revenant sur les scénarios opérationnels à la lumière des incidents de sécurité survenus, de l'apparition de nouvelles vulnérabilités et de l'évolution des modes opératoires.

◆

UN EXEMPLE SUIVI PAS À PAS

La méthode est illustrée à l'aide d'un exemple mettant en scène une entreprise fictive, à savoir une société de biotechnologie fabriquant des vaccins. Cet exemple se veut réaliste dans l'objectif de fournir au lecteur une illustration concrète et pédagogique de la méthode.

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

Différents usages d'EBIOS Risk Manager

EBIOS RM est une méthode adaptable. Elle constitue une véritable boîte à outils, dont les activités à réaliser, leur niveau de détail et leur séquencement, seront adaptés à l'usage désiré. En effet, la manière dont s'applique la méthode diffère selon le sujet étudié, les livrables attendus, le degré de connaissance du périmètre de l'étude ou encore le secteur auquel on l'applique. La grille ci-après propose des cas d'usage selon l'objectif visé.

	ATELIERS PRINCIPAUX À CONDUIRE OU EXPLOITER				
OBJECTIF DE L'ÉTUDE	1	2	3	4	5
Identifier le socle de sécurité adapté à l'objet de l'étude	X				
Être en conformité avec les référentiels de sécurité numérique	X				X
Évaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude			X *(note 1)*		
Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème		X	X		
Réaliser une étude préliminaire de risque pour identifier les axes prioritaires d'amélioration de la sécurité	X *(note 2)*	X	X		X *(note 3)*
Conduire une étude de risque complète et fine, par exemple sur un produit de sécurité ou en vue de l'homologation d'un système	X	X	X	X	X
Orienter un audit de sécurité et notamment un test d'intrusion			X	X	
Orienter les dispositifs de détection et de réaction, par exemple au niveau d'un centre opérationnel de la sécurité (SOC)			X	X	

NOTE 1 : étape a) de l'atelier uniquement ; cela ne nécessite pas d'avoir conduit au préalable les ateliers 1 et 2.
NOTE 2 : dans le cadre d'une étude préliminaire, le degré de profondeur de l'atelier 1 est à adapter (exemple : ne recenser que les principales valeurs métiers, réaliser une analyse sommaire du socle de sécurité).
NOTE 3 : étape b) de l'atelier uniquement.

ATELIER

1

Cadrage et socle de sécurité

1/ Les objectifs de l'atelier

Le but de ce premier atelier est de définir le cadre de l'étude, son périmètre métier et technique, les événements redoutés associés et le socle de sécurité. Cet atelier est un prérequis à la réalisation d'une appréciation des risques. La période à considérer pour cet atelier est celle du cycle stratégique.

◆

2/ Les participants à l'atelier [6]

- Direction ;
- Métiers ;
- Responsable de la sécurité des systèmes d'information (RSSI) ;
- Direction des systèmes d'information (DSI).

◆

3/ Les données de sortie

À l'issue de l'atelier, vous devez avoir identifié :

- les éléments de cadrage : objectifs visés, rôles et responsabilités, cadre temporel ;
- le périmètre métier et technique : missions, valeurs métier, biens supports ;
- les événements redoutés et leur niveau de gravité ;
- le socle de sécurité : liste des référentiels applicables, état d'application, identification et justification des écarts.

6 L'équipe pourra être complétée par toutes personnes jugées utiles.

4/ Les étapes de l'atelier

Cet atelier peut par exemple se dérouler sur une à trois séances d'une demi-journée [7]. L'objectif sera de :

a. définir le cadre de l'étude ;
b. définir le périmètre métier et technique de l'objet étudié ;
c. identifier les événements redoutés et évaluer leur niveau de gravité ;
d. déterminer le socle de sécurité.

◆

5/ Comment procéder ?

a DÉFINIR LE CADRE DE L'ÉTUDE

Pour initier l'atelier, commencez par exposer l'objet et les attendus de la réunion aux participants. Accordez-vous sur les **objectifs** de l'étude. Ceux-ci peuvent être par exemple la mise en place d'un processus de management du risque cyber dans l'organisme, l'homologation d'un système d'information ou encore l'identification du niveau de sécurité à atteindre pour obtenir une certification produit. Selon l'objectif défini, il en est déduit le niveau de granularité de l'étude et les ateliers à conduire.

Identifiez ensuite les **participants** aux différents ateliers, leurs rôles et leurs responsabilités dans le cadre de l'étude (animateur de l'atelier, contributeur, décideur, etc.). Pour cela, vous pouvez par exemple réaliser une matrice

7 La durée de l'atelier est proposée à titre indicatif. Elle n'inclut pas le travail de préparation et de formalisation à réaliser en amont et en aval.

de type RACI [8]. À cette étape, il est indispensable d'identifier quelle est la personne responsable d'accepter les risques résiduels au terme de l'étude.

Définissez ensuite le **cadre temporel** de l'étude (durées des cycles opérationnel et stratégique). Ces durées doivent être adaptées aux contraintes projet et cohérentes avec le cadre légal, règlementaire et normatif en vigueur. Communément, pour une homologation de système d'information, les durées génériques sont de trois ans pour le cycle stratégique et d'un an pour le cycle opérationnel.

Des aspects relatifs à la gestion de projet comme le planning des ateliers à mener ou les contraintes de ressources pourront également être abordés.

b DÉFINIR LE PÉRIMÈTRE MÉTIER ET TECHNIQUE

Dans un deuxième temps, vous allez recenser les missions, valeurs métier et biens supports relatifs à l'objet de l'étude [9]. Les questions qui pourront être posées sont :

- *À quoi sert l'objet de l'étude ? Quelles sont ses missions principales, ses finalités, ses raisons d'être ?*
- *Quels sont les processus et les informations majeures permettant à l'objet étudié de réaliser ses missions ?*
- *Quels sont les services numériques, applications, réseaux informatiques, structures organisationnelles, ressources humaines, locaux, etc. qui permettent de mener à bien ces processus ou de traiter ces informations ?*

Commencez par lister l'ensemble des **missions** de l'objet étudié, c'est-à-dire les finalités et raisons d'être majeures de ce dernier (la manière dont il participe à la création de valeur, par exemple). Selon le niveau de granularité de l'étude, les missions à identifier peuvent parfois être intrinsèques à l'objet étudié mais sont généralement celles de l'organisme dans lesquelles l'objet s'inscrit.

De la même manière, recensez ensuite l'ensemble des **valeurs métier** associées à l'objet de l'étude, à savoir les informations ou processus jugés importants, dans le cadre de l'étude, et qu'il convient de protéger. Les valeurs métier représentent le patrimoine informationnel qu'une source de risque aurait intérêt à attaquer pour atteindre ses objectifs (exemple : service d'annulation de réservations en ligne, informations clients, résultats de travaux de R&D, phase de déploiement d'un projet, savoir-faire en conception de pièces aéronautiques, etc.).

À ce stade, l'objectif n'est pas de rechercher l'exhaustivité mais bien de veiller à limiter le nombre de valeurs métier pour ne garder que celles identifiées comme essentielles ou sensibles. Procéder ainsi permet de conserver une certaine agilité dans l'étude et de réduire le travail au niveau utile et acceptable. Pour parvenir à cette fin, vous pouvez par exemple :

- considérer des ensembles d'informations plutôt que des informations isolées ;
- classer les valeurs métier selon leurs besoins de sécurité (disponibilité, intégrité, confidentialité, etc.) [10].

En termes de volumétrie, 5 à 10 valeurs métier constituent généralement une base suffisante pour orienter la suite de l'étude. Les valeurs métier qui n'auront pas été retenues pourront cependant hériter des mesures prises pour protéger les autres valeurs métier.

8 **RACI** : Responsable de la mise en œuvre de l'activité, Autorité légitime pour approuver l'activité, Consulté pour obtenir des informations nécessaires à l'activité, Informé des résultats de l'activité.

9 Pour réaliser cette activité, vous pouvez vous appuyer sur le modèle proposé dans la fiche méthode n°1.

10 Pour classer les valeurs métier, il est possible de juger si leurs besoins de sécurité sont « très importants », « notables » ou « négligeables ». Il est également possible pour l'évaluation des besoins de sécurité d'une valeur métier d'utiliser des échelles de cotation, par exemple celles à 3 ou 4 niveaux utilisées dans les exemples de la méthode EBIOS 2010. Toutefois, l'objectif n'est pas la recherche d'une valeur absolue mais plutôt d'une position relative des valeurs métier les unes par rapport aux autres.

Listez ensuite les **biens supports** relatifs à chaque valeur métier. Il s'agit des éléments du système d'information sur lesquels les valeurs métier reposent. Pour cela, appuyez-vous sur la cartographie du système d'information de l'organisme [11]. Vous pouvez structurer votre recensement selon les grandes catégories proposées dans la fiche méthode n°2.

NOTE : à ce stade, vous pouvez limiter l'identification des biens supports aux plus importants, par exemple un à trois biens supports pour chaque valeur métier. Ils seront ensuite complétés lors de l'élaboration des scénarios opérationnels.

11 Pour la construire, il est possible de s'appuyer sur le guide de l'**ANSSI,** *Cartographie du système d'information – guide d'élaboration en 5 étapes.* Guide, 2018.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

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 ; étiquetage) ; ■ 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

NOTE : au cours de cette étape, vous pouvez être amené à identifier des valeurs métier ou biens supports placés sous la responsabilité d'entités extérieures à votre organisation. Ces éléments pourront être repris dans l'atelier 3, lors de la réalisation de la cartographie de menace numérique de l'écosystème.

c IDENTIFIER LES ÉVÉNEMENTS REDOUTÉS

Identifier et caractériser les **événements redoutés** (ER) permet aux acteurs de comparer objectivement l'importance des missions et valeurs métier tout en prenant conscience des enjeux de sécurité. Dans EBIOS RM, les événements redoutés sont associés aux valeurs métiers et traduisent une atteinte préjudiciable pour l'organisation. Le degré de préjudice ou d'impact est évalué selon une échelle de gravité permettant la hiérarchisation des événements redoutés.

Afin de faire émerger les ER, vous pouvez pour chaque valeur métier recensée dans l'étape précédente, mener des recherches sur les effets néfastes consécutifs par exemple à une atteinte :

- à la disponibilité de la valeur métier (exemple : information inaccessible, interruption totale ou partielle de service, impossibilité de réaliser une phase d'un processus) ;
- à son intégrité (exemple : falsification ou modification d'une information, détournement d'usage d'un service, altération d'un processus) ;
- à sa confidentialité (exemple : divulgation d'information, accès non autorisé à un service, compromission d'un secret) ;
- à la traçabilité (exemple : perte de traçabilité d'une action ou d'une modification d'information, impossibilité de tracer l'enchaînement d'un processus) ;
- et plus globalement à la qualité de service et aux performances auxquelles la valeur métier doit répondre.

L'estimation de la gravité de chaque ER est fonction de la criticité de la valeur métier vis-à-vis :

- des missions de l'organisation ;
- de la réglementation ;
- de la nature et de l'intensité des impacts directs, voire indirects.

La fiche méthode n°3 est proposée pour vous aider à réaliser cette activité.

NOTES

- 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. L'évaluation préalable des besoins de sécurité peut aider à l'estimation de la gravité.
- Pour les ER portant atteinte à la disponibilité, nous vous recommandons de préciser au-delà de quelle perte de service le niveau de gravité mentionné est atteint (exemple : indisponibilité du service pendant une durée supérieure à 2 heures, impossibilité de diffuser des flux de données supérieurs à 1 Mbps). Cette approche vous permettra notamment d'ancrer dans votre appréciation du risque la notion de mode de fonctionnement dégradé.
- Pour estimer la gravité, considérez tous les types d'impacts envisageables – internes, externes, directs, indirects – afin de pousser les acteurs à envisager des impacts auxquels ils n'auraient peut-être pas songé de prime abord.
- À ce stade, les ER sont identifiés du point de vue de l'organisation, en dehors de tout scénario d'attaque. Ils seront ensuite utiles à l'élaboration des scénarios stratégiques (atelier 3), du point de vue de l'attaquant et pourront être actualisés dans ce cadre.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

La cotation de la gravité des impacts est effectuée sur la base de la grille suivante :

ÉCHELLE	CONSÉQUENCES
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 impact 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).

La société a recensé une partie des événements redoutés dans le tableau suivant :

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**
Fabriquer des vaccins	Fuite du savoir-faire de l'entreprise concernant le processus de fabrication des vaccins et de leurs tests qualité	Impacts financiers	**2**
	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**
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**

d DÉTERMINER LE SOCLE DE SÉCURITÉ

Déterminer le socle de sécurité et les écarts suppose d'adopter une approche par conformité, correspondant aux deux premiers étages de la pyramide de management du risque. Pour cela, vous devrez identifier l'ensemble des **référentiels de sécurité** qui s'appliquent à l'objet de l'étude. Ces référentiels peuvent être :

- des règles d'hygiène informatique et bonnes pratiques de sécurité : guides de recommandations de l'ANSSI [12], règles de sécurité internes à l'organisation, etc. ;
- des normes : famille ISO 27000, etc. ;
- des règlementations en vigueur : vous pouvez vous reporter au site de l'ANSSI [13] qui dresse un panorama des textes règlementaires en matière de sécurité numérique.

Si l'objet de l'étude est un système ou un produit déjà existant, évaluez ensuite **l'état d'application** des différents référentiels listés, par exemple au moyen d'un indicateur de couleur (vert pour « appliqué sans restriction », orange pour « appliqué avec restrictions », rouge pour « non appliqué », etc.) et identifiez clairement les **écarts**, ainsi que les causes de ces derniers.

12 www.ssi.gouv.fr/administration/bonnes-pratiques
13 www.ssi.gouv.fr/administration/reglementation

Le socle de sécurité peut être formalisé dans une table, telle que celle proposée ci-dessous à titre d'illustration :

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

Les écarts observés vis-à-vis du socle de sécurité seront repris dans l'appréciation des risques, conduite dans les ateliers suivants afin d'identifier les risques qu'ils font peser sur l'organisation. Des mesures de sécurité pourront alors être définies au cours de l'atelier 5 pour les limiter.

NOTE : les résultats des études de risques précédemment réalisées seront intégrés à cette étape. En effet, ces études vous ont permis d'identifier et de mettre en œuvre des mesures de sécurité. Celles-ci font donc désormais partie du socle de sécurité de votre organisation et pourront être éprouvées dans les ateliers suivants d'appréciation des risques.

ATELIER

2

Sources de risque

1 / Les objectifs de l'atelier

Le but de l'atelier 2 est d'identifier les **sources de risque** (SR) et leurs **objectifs visés** (OV), en lien avec le contexte particulier de l'étude. L'atelier vise à répondre à la question suivante : *qui ou quoi pourrait porter atteinte aux missions et valeurs métier identifiées dans l'atelier 1, et dans quels buts ?*

Les sources de risque et les objectifs visés sont ensuite caractérisés et évalués en vue de retenir les plus pertinents. Ils seront utiles à la construction des scénarios des ateliers 3 et 4.

◆

2 / Les participants à l'atelier [14]

- Direction (au minimum lors de la dernière étape de l'atelier) ;
- Métiers ;
- RSSI ;
- Un spécialiste en analyse de la menace numérique complètera éventuellement votre groupe de travail, selon le niveau de connaissance de l'équipe et le niveau de précision souhaité.

◆

3 / Les données de sortie

À l'issue de l'atelier, vous devez avoir établi les éléments suivants :

- la liste de couples SR/OV prioritaires retenus pour la suite de l'étude ;
- la liste des couples SR/OV secondaires susceptibles d'être étudié dans un second temps et qui feront, si possible, l'objet d'une surveillance attentive ;
- une cartographie des sources de risque.

◆

4 / Les étapes de l'atelier

Cet atelier, d'une durée variable, peut nécessiter 2 heures à une journée de travail [15] en vue de :

a. identifier les sources de risque et les objectifs visés ;
b. évaluer les couples SR/OV ;
c. sélectionner les couples SR/OV jugés prioritaires pour poursuivre l'analyse.

◆

5 / Comment procéder ?

Pour mener cet atelier, vous avez besoin de connaitre les missions et les valeurs métier de l'objet étudié, issus de l'atelier 1.

La caractérisation fine des sources de risque et de leurs objectifs visés nécessite de disposer d'informations précises sur l'état de la menace et doit idéalement se tourner vers le secteur concerné : attaquants ou groupes d'attaquants, ressources et motivations supposées, modes opératoires, activités les plus exposées, etc. Les bulletins quotidiens de veille sur les cyberattaques et les actualités relatives à la cybersécurité sont également de précieuses sources d'information permettant de compléter et préciser la connaissance de la menace et de la contextualiser.

14 L'équipe pourra être complétée par toutes personnes jugées utiles.

15 La durée de l'atelier est proposée à titre indicatif. Elle n'inclut pas le travail de préparation et de formalisation à réaliser en amont et en aval.

La fiche méthode n°4 vous oriente sur la façon d'organiser ces informations afin de la rendre actionnable pour l'appréciation des risques dans le cadre de l'atelier 2.

a IDENTIFIER LES SOURCES DE RISQUE ET LES OBJECTIFS VISÉS

Pour mener l'atelier, vous devez vous poser les questions suivantes :

- *quelles sont les sources de risque susceptibles de porter atteinte aux missions de l'organisation ou à des intérêts supérieurs (sectoriels, étatiques, etc.) ?*
- *quels peuvent être les objectifs visés par chaque source de risque en termes d'effets recherchés ?*

Une façon de procéder est de passer en revue les catégories de sources de risque et d'objectifs visés proposées dans la fiche méthode n°4 : pour chaque catégorie de source de risque, déterminez quel est le profil de l'attaquant et quels types d'objectifs il cherche à atteindre. Une même source de risque peut le cas échéant générer plusieurs couples SR/OV, avec des objectifs visés de natures différentes.

NOTES

- Une des clés de succès consiste à rechercher des catégories de couples SR/OV variées afin de disposer d'un panel différencié de profils d'attaquant et d'objectifs visés à partir desquels seront établis les scénarios stratégiques de l'atelier 3. Il est également important de ne pas laisser d'angle mort : assurez-vous de couvrir le plus largement possible les valeurs métier de l'organisation.
- L'objectif visé par une source de risque peut aller au-delà du seul périmètre de l'objet de l'étude. Dans ce cas, ce dernier est susceptible de servir d'intermédiaire pour atteindre l'OV ou de subir des impacts collatéraux du fait de son exposition au risque.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

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.

b ÉVALUER LES COUPLES SR/OV

Lorsque l'équipe aura cessé de produire de nouveaux couples SR/OV, vous pourrez évaluer la pertinence de chaque couple. L'objectif est d'identifier, dans le vivier de sources de risque et objectifs visés recensés, ceux qui vous semblent les plus pertinents. Si le retour d'expérience des participants peut constituer une première base d'évaluation, nous vous recommandons également d'utiliser des critères et métriques de caractérisation qui apporteront une certaine objectivité. Les critères d'évaluation habituellement utilisés sont :

- la motivation de la source de risque à atteindre son objectif ;
- ses ressources (financières, compétences, infrastructures d'attaque) ;
- son activité (est-elle active dans le périmètre de l'objet de l'étude, dans l'écosystème, dans l'industrie concernée, dans une industrie similaire, etc.).

c SÉLECTIONNER LES COUPLES SR/OV RETENUS POUR LA SUITE DE L'ANALYSE

Sur la base des travaux précédents, vous pouvez alors finaliser l'atelier en sélectionnant les couples SR/OV retenus pour la suite de l'étude. L'un des critères de choix est évidemment le niveau de pertinence évalué dans l'étape précédente. Privilégiez des couples SR/OV suffisamment distincts les uns des autres et qui impacteront vraisemblablement différentes valeurs métier et biens supports. En termes de volumétrie, 3 à 6 couples SR/OV constituent généralement une base suffisante pour élaborer des scénarios stratégiques.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

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**

Le groupe de travail retiendra en priorité les couples de pertinence élevée et moyenne, laissant de côté dans un premier temps la menace cyber-terroriste et celle liée aux hacktivistes souhaitant divulguer des informations sur les tests animaliers, qui sont jugées moins prégnantes.

ATELIER

3

Scénarios stratégiques

1 / Les objectifs de l'atelier

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.). De plus en plus de modes opératoires d'attaque exploitent les maillons les plus vulnérables de cet écosystème pour atteindre leur objectif (exemple : atteinte à la disponibilité d'un service en attaquant le fournisseur de service en nuage, piège de la chaîne logistique d'approvisionnement de serveurs facilitant l'exfiltration de données sensibles).

L'objectif de l'atelier 3 est de disposer d'une vision claire de l'écosystème, afin d'en identifier les parties prenantes les plus vulnérables. Il s'agit ensuite de bâtir des scénarios de haut niveau, appelés **scénarios stratégiques**. Ces derniers sont autant de chemins d'attaque que pourrait emprunter une source de risque pour atteindre son objectif (*i.e.* un des couples SR/OV sélectionnés lors de l'atelier 2).

L'atelier 3 est à aborder comme une étude préliminaire de risque. Il peut conduire à identifier les mesures de sécurité à appliquer vis-à-vis de l'écosystème. Les scénarios stratégiques retenus dans l'atelier 3 constituent la base des scénarios opérationnels de l'atelier 4.

◆

2 / Les participants à l'atelier [16]

- Métiers ;
- Architectes fonctionnels ;
- RSSI ;
- Un spécialiste en cybersécurité complètera éventuellement votre groupe de travail, selon le niveau de connaissance de l'équipe et le degré d'affinement visé.

16 L'équipe pourra être complétée par toutes personnes jugées utiles.

◆

3 / Les données de sortie

À l'issue de l'atelier, vous devez avoir établi et identifié les éléments suivants :

- la cartographie de menace numérique de l'écosystème et les parties prenantes critiques ;
- les scénarios stratégiques et événements redoutés ;
- les mesures de sécurité retenues pour l'écosystème.

◆

4 / Les étapes de l'atelier

Cet atelier, d'une durée variable, peut nécessiter une à trois demi-journées de travail [17] en vue de :

a. construire la cartographie de menace numérique de l'écosystème et sélectionner les parties prenantes critiques ;
b. élaborer des scénarios stratégiques ;
c. définir des mesures de sécurité sur l'écosystème.

17 La durée de l'atelier est proposée à titre indicatif. Elle n'inclut pas le travail de préparation et de formalisation à réaliser en amont et en aval.

5 / Comment procéder ?

Pour mener cet atelier, vous avez besoin de connaître :

- *les missions et valeurs métier de l'objet étudié (atelier 1) ;*
- *les événements redoutés et leur gravité (atelier 1) ;*
- *les sources de risque et objectifs visés retenus (atelier 2) ;*
- *la cartographie du SI et en particulier sa vue écosystème (voir note).*

NOTE : la vue écosystème présente les différentes parties prenantes avec lesquelles l'objet étudié interagit directement ou indirectement pour réaliser ses missions et services. Dans un souci d'efficacité, elle peut se limiter aux interactions associées aux valeurs métier. Lorsque c'est possible, vous avez tout intérêt à utiliser une cartographie existante et à la compléter au besoin. Pour plus de précisions, vous pouvez vous reporter avec profit au guide de cartographie proposé par l'ANSSI.

a CONSTRUIRE LA CARTOGRAPHIE DE MENACE NUMÉRIQUE DE L'ÉCOSYSTÈME ET SÉLECTIONNER LES PARTIES PRENANTES CRITIQUES

Une partie prenante est dite critique (PPC) dès lors qu'elle est susceptible de constituer un vecteur d'attaque pertinent, du fait par exemple de son accès numérique privilégié à l'objet étudié, de sa vulnérabilité ou de son exposition. Une source de risque bien renseignée (c'est-à-dire connaissant l'écosystème de la cible) tentera, dans une logique de moindre effort, d'attaquer la partie prenante qui apparait comme le « maillon faible ». L'objectif est donc d'identifier ces parties prenantes critiques pour les inclure dans l'élaboration des scénarios stratégiques.

Vous allez d'abord évaluer le niveau de menace induit par chaque partie prenante de l'écosystème sur l'objet étudié. Il est préférable de faire reposer l'évaluation des parties prenantes sur des critères plutôt que sur le seul jugement d'experts ou le retour d'expérience.

Vous établirez ensuite la **cartographie de menace numérique de l'écosystème** [18] sur laquelle doit apparaître l'ensemble des parties prenantes d'intérêt au regard de leur niveau de menace vis-à-vis de l'objet de l'étude.

Vous serez alors en mesure de sélectionner les parties prenantes critiques. L'utilisation de seuils d'acceptation du risque facilitera ce travail de sélection. Une démarche simple de réalisation de la cartographie de menace numérique et de sélection des parties prenantes critiques est proposée dans la fiche méthode n°5. Les parties prenantes y sont évaluées sur la base de critères d'exposition (dépendance, pénétration) et de fiabilité cyber (maturité, confiance).

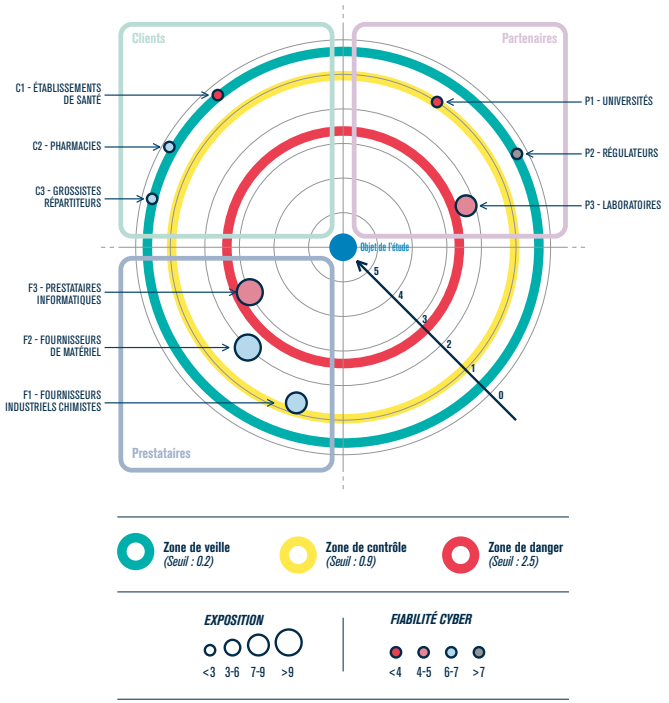
18 Cet outil vous permettra de faciliter d'une part la sélection des parties prenantes critiques (PPC) et d'autre part l'identification des mesures de sécurité à mettre en œuvre et contractualiser. La cartographie de menace numérique est une déclinaison, sous l'angle de la gestion du risque numérique, de la cartographie du SI. Elle est utile à la conduite de nombreux projets et reflète votre gouvernance en matière de management du risque numérique de l'écosystème.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

L'équipe a décidé de se concentrer dans un premier temps sur les parties prenantes externes de l'écosystème de la société. Elle a identifié les acteurs suivants :

CATÉGORIE	PARTIE PRENANTE
Clients	**C1** – Établissements de santé
	C2 – Pharmacies
	C3 – Dépositaires et grossistes répartiteurs
Partenaires	**P1** – Universités
	P2 – Régulateurs
	P3 – Laboratoires
Prestataires	**F1** – Fournisseurs industriels chimistes
	F2 – Fournisseurs de matériel de production
	F3 – Prestataire informatique

L'évaluation de chaque partie prenante a permis d'établir la cartographie de menace numérique ci-après :



L'équipe a retenu F3 – Prestataire informatique comme partie prenante critique.
Les parties prenantes P3 et F2 sont également retenues comme parties prenantes critiques.
Les autres parties prenantes n'ont pas été retenues comme critiques.
Après discussion avec le RSSI, P1 et F1 bien que situées dans la zone de contrôle, n'ont pas été retenues par le responsable projet, compte tenu du contexte et de la nature des sources de risque en jeu [19].

19 Comme indiqué en préambule, il s'agit ici de montrer que l'analyse et l'évaluation effectuées sont une aide à la décision, mais que cette dernière revient à la gouvernance projet qui peut décider d'écarter tel ou tel élément de menace pour des raisons contextuelles ou politiques.

b ÉLABORER DES SCÉNARIOS STRATÉGIQUES

Dans l'étape précédente, vous avez construit la cartographie de menace numérique de l'écosystème et sélectionné les parties prenantes critiques. L'objectif est maintenant d'imaginer des scénarios réalistes de haut niveau, indiquant de quelle façon un attaquant pourrait procéder pour atteindre son objectif. Il peut par exemple choisir d'exploiter l'écosystème ou de dévoyer certains processus métiers.

Ces scénarios dits stratégiques sont identifiés par déduction. Dans cette démarche, les éléments d'analyse des étapes précédentes vous seront précieux. Pour animer cet atelier, prenez comme point de départ les couples SR/OV sélectionnés dans l'atelier 2. Puis, pour chaque couple SR/OV, lancez les discussions en (vous) posant les questions suivantes du point de vue de l'attaquant :

- *quelles sont la ou 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 ?*

Une fois les éléments les plus exposés identifiés, vous pouvez élaborer le scénario stratégique issu du couple SR/OV en décrivant le séquencement des événements générés par la source de risque pour atteindre son objectif. Les atteintes aux valeurs métier correspondent à des **événements redoutés** pour l'objet étudié tandis que les événements portant sur l'écosystème sont des événements intermédiaires.

***Exemples d'événements (intermédiaires ou redoutés) d'un scénario stratégique** : création d'un canal d'exfiltration depuis l'infrastructure du prestataire, modification d'un paramètre critique de processus industriel (seuil de température haute), attaque en déni de service du fournisseur d'informatique en nuage, suppression ou altération d'une base de données, usurpation d'identité d'un service support.*

NOTE : les événements redoutés qui interviennent dans les scénarios stratégiques sont à rechercher dans la liste des ER établie lors de l'atelier 1. Toutefois, contrairement à l'exercice de l'atelier 1, les ER sont ici exploités sous l'angle de l'attaquant. Le point de vue étant différent, la liste des ER est susceptible d'être mise à jour.

Vous pouvez représenter vos scénarios sous la forme de **graphes d'attaque** ou directement sur la vue écosystème de la cartographie du SI en y superposant le ou les chemins d'attaque.

Vous évaluerez alors le niveau de **gravité** de chaque scénario, au regard des impacts potentiels associés aux événements redoutés sur les valeurs métier.

NOTES

- Gardez à l'esprit que la finalité est d'identifier les points d'entrée, relais de propagation et vecteurs d'exploitation les plus pertinents, dans une logique de moindre effort, et de les décrire sous la forme d'événements correspondant à des objectifs intermédiaires pour l'attaquant pour atteindre son objectif. Attention toutefois à ne pas élaborer des scénarios stratégiques trop détaillés.
- Généralement, un à trois chemins d'attaque pour chaque couple SR/OV sont suffisants pour explorer un champ de risque pertinent. Prenez soin de privilégier une variété de scénarios où interviennent différentes parties prenantes critiques et catégories de valeurs métier.

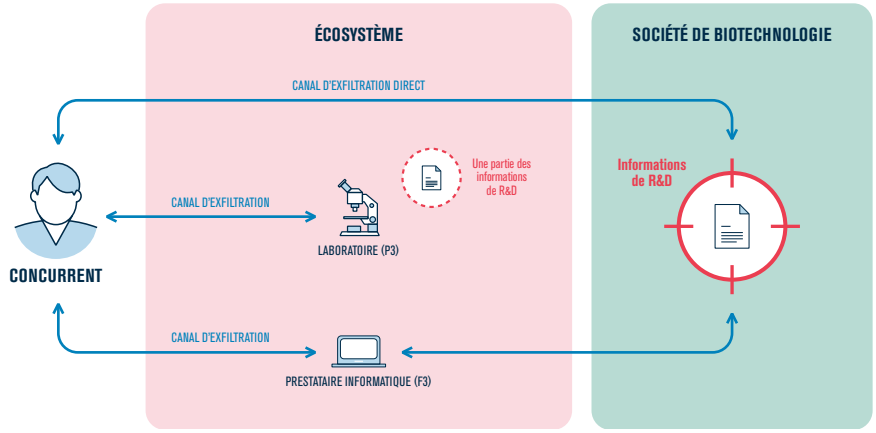
EXEMPLE : société de biotechnologie fabriquant des vaccins.

Le groupe de travail s'est d'abord intéressé au couple SR/OV « Un concurrent veut voler des informations en espionnant les travaux de R&D en vue d'obtenir un avantage concurrentiel » (voir atelier 2). Les trois chemins d'attaque ci-après ont été jugés pertinents.

Le concurrent vole les travaux de recherche :

1. en créant un canal d'exfiltration de données portant directement sur le système d'information de la R&D ;
2. en créant un canal d'exfiltration de données sur le système d'information du laboratoire, qui détient une partie des travaux (partie prenante P3 identifiée comme critique dans l'étape précédente) ;
3. en créant un canal d'exfiltration de données passant par le prestataire informatique (partie prenante critique F3).

Le scénario stratégique associé est représenté ci-après. Il est de **gravité 3 (grave)** selon la cotation effectuée lors de l'atelier 1 sur les valeurs métier.

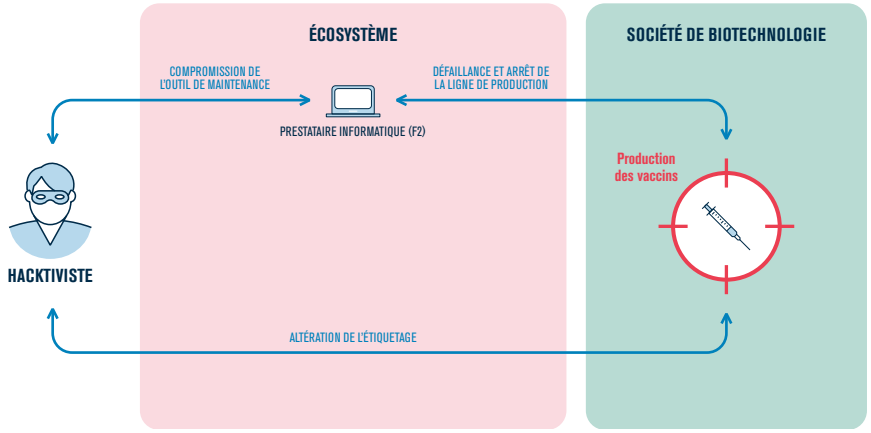


Puis le groupe de travail s'est penché sur le couple SR/OV : « Une organisation hacktiviste veut saboter la prochaine campagne nationale de vaccination, en perturbant la production ou la distribution des vaccins, pour générer un choc psychologique sur la population et discréditer les pouvoirs publics ». Deux chemins d'attaque ont été identifiés comme pertinents.

Le 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 (conséquence : la fabrication des vaccins est fortement perturbée) ;
2. en modifiant l'étiquetage des vaccins (conséquence : les vaccins ne sont pas livrés au bon endroit).

Le scénario stratégique associé est représenté ci-après. Il est de **gravité 4 (critique)** selon la cotation effectuée dans l'atelier 1, car est ici considéré le cas le plus défavorable puisque l'incident survient lors d'un pic d'épidémie et dure au-delà d'une semaine.



En synthèse, deux scénarios stratégiques ont été retenus :

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**

C DÉFINIR DES MESURES DE SÉCURITÉ SUR L'ÉCOSYSTÈME

Les travaux précédemment menés auront éventuellement mis en lumière des vulnérabilités structurelles liées à vos parties prenantes internes et externes, que des attaquants tenteront d'exploiter pour arriver à leurs fins. Vous aurez également peut-être identifié un scénario dans lequel votre organisation serait impactée de façon collatérale par une attaque informatique ciblant l'un de vos partenaires. La dernière étape de l'atelier 3 porte sur la recherche de pistes de réduction de ces risques et leur traduction en **mesures de sécurité**.

Les mesures de sécurité auront pour vocation de réduire le niveau de menace intrinsèque induit par les parties prenantes critiques (exemple : réduire la dépendance à un sous-traitant) [20]. Elles pourront également agir sur le déroulement des scénarios stratégiques.

NOTE : les mesures de sécurité seront susceptibles d'impacter la gouvernance de votre organisation, voire celle de vos parties prenantes externes. Par conséquent, des arbitrages du ressort de la direction seront à prévoir.

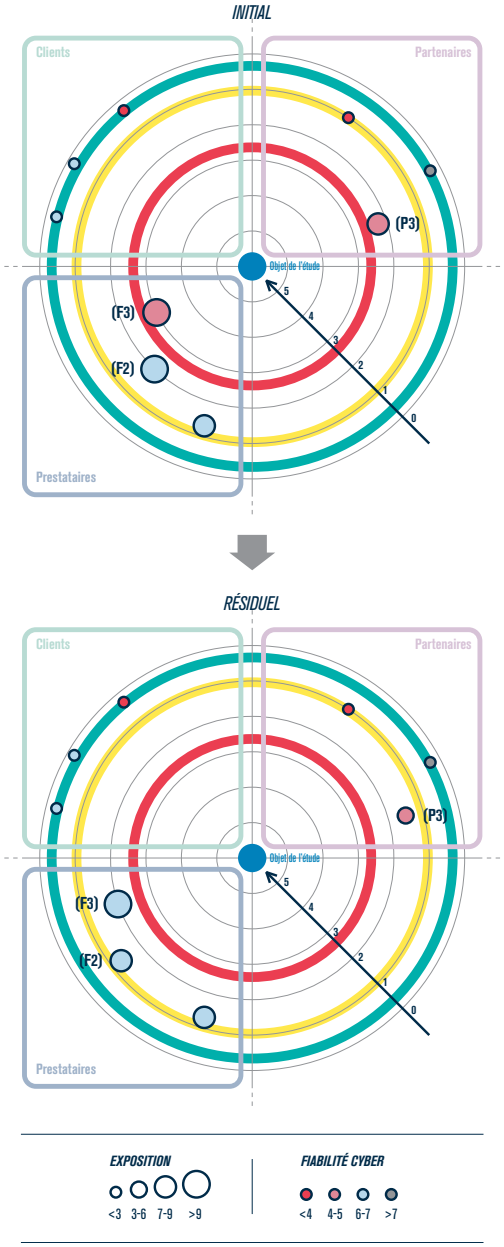
20 Des règles simples sont proposées dans la fiche méthode n°6.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

Des mesures de sécurité ont été définies en priorité pour les prestataires F2, F3 et P3. Ces derniers sont en effet impliqués dans des scénarios stratégiques particulièrement problématiques.

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

L'application des objectifs ci-dessus devrait permettre sous 9 à 12 mois de réduire le risque, avec une cartographie de menace numérique résiduelle comme suit :



ATELIER

4

Scénarios opérationnels

1 / Les objectifs de l'atelier

L'objectif de l'atelier 4 est de construire des scénarios opérationnels. Ils schématisent les modes opératoires que pourraient mettre en œuvre les sources de risque pour réaliser les scénarios stratégiques. Cet atelier adopte une démarche similaire à celle de l'atelier précédent mais se concentre sur les biens supports. Les scénarios opérationnels obtenus sont évalués en termes de vraisemblance. À l'issue de cet atelier, vous allez réaliser une synthèse de l'ensemble des risques de l'étude.

La période à considérer pour cet atelier est celle du cycle opérationnel.

◆

2 / Les participants à l'atelier[21]

- RSSI ;
- DSI ;
- Un spécialiste en cybersécurité complètera éventuellement le groupe de travail, selon le niveau de connaissance de l'équipe et le degré de précision souhaité.

◆

3 / Les données de sortie

À l'issue de cet atelier, vous devez avoir établi :

- la liste des scénarios opérationnels et leur vraisemblance.

21 L'équipe pourra être complétée par toutes personnes jugées utiles.

4 / Les étapes de l'atelier

Cet atelier, d'une durée variable, peut nécessiter une à trois demi-journées de travail [22] en vue de :

a. élaborer les scénarios opérationnels ;
b. évaluer leur vraisemblance.

◆

5 / Comment procéder ?

Pour mener cet atelier, vous avez besoin de connaitre :

- *les missions, valeurs métier et biens supports relatifs à l'objet de l'étude (atelier 1) ;*
- *le socle de sécurité (atelier 1) ;*
- *les sources de risque et objectifs visés retenus (atelier 2) ;*
- *les scénarios stratégiques retenus (atelier 3) ;*
- *les vues applications et infrastructures logiques de la cartographie du système d'information.*

a ÉLABORER LES SCÉNARIOS OPÉRATIONNELS

Une attaque réussie relève le plus souvent de l'exploitation de plusieurs failles. Les attaques intentionnelles suivent généralement une démarche séquencée. Celle-ci exploite de façon coordonnée plusieurs vulnérabilités de nature informatique, organisationnelle ou encore physique. Une telle approche fondée sur l'exploitation simultanée de failles distinctes peut avoir des

22 La durée de l'atelier est proposée à titre indicatif. Elle n'inclut pas le travail de préparation et de formalisation à réaliser en amont et en aval.

conséquences lourdes alors même que les vulnérabilités exploitées peuvent sembler anodines lorsqu'on les considère individuellement.

Les scénarios opérationnels définis dans cet atelier pourront être structurés selon une séquence d'attaque type. Plusieurs modèles [23] existent et peuvent être utilisés (exemple : modèle de *cyber kill chain* de Lockheed Martin). La démarche doit vous permettre d'identifier les **biens supports critiques** susceptibles de servir de vecteurs d'entrée ou d'exploitation ou de relais de propagation pour l'attaque modélisée. Lors de l'atelier 5, les mesures de sécurité porteront naturellement sur ces biens supports plus particulièrement ciblés. Toutefois, les autres biens supports pourront hériter de ces mesures.

Construisez les scénarios opérationnels en vous basant sur les scénarios stratégiques retenus dans l'atelier 3 et en vous appuyant sur la cartographie du système d'information. Une bonne approche consiste à représenter vos scénarios sous la forme **de graphes ou de schémas d'attaque**, utiles à la représentation des modes opératoires de l'attaquant. Vous pouvez vous appuyer sur la fiche méthode n°7 pour réaliser cette étape.

NOTE : à chaque chemin d'attaque stratégique retenu dans l'atelier 3 correspond un scénario opérationnel permettant à la source de risque d'atteindre son objectif.

Le schéma ci-après présente le mode opératoire type d'une attaque dite par « point d'eau » dont l'objectif est de permettre à une source de risque d'établir un canal d'exfiltration de données.

23 Un modèle type est proposé dans la fiche méthode n°7.

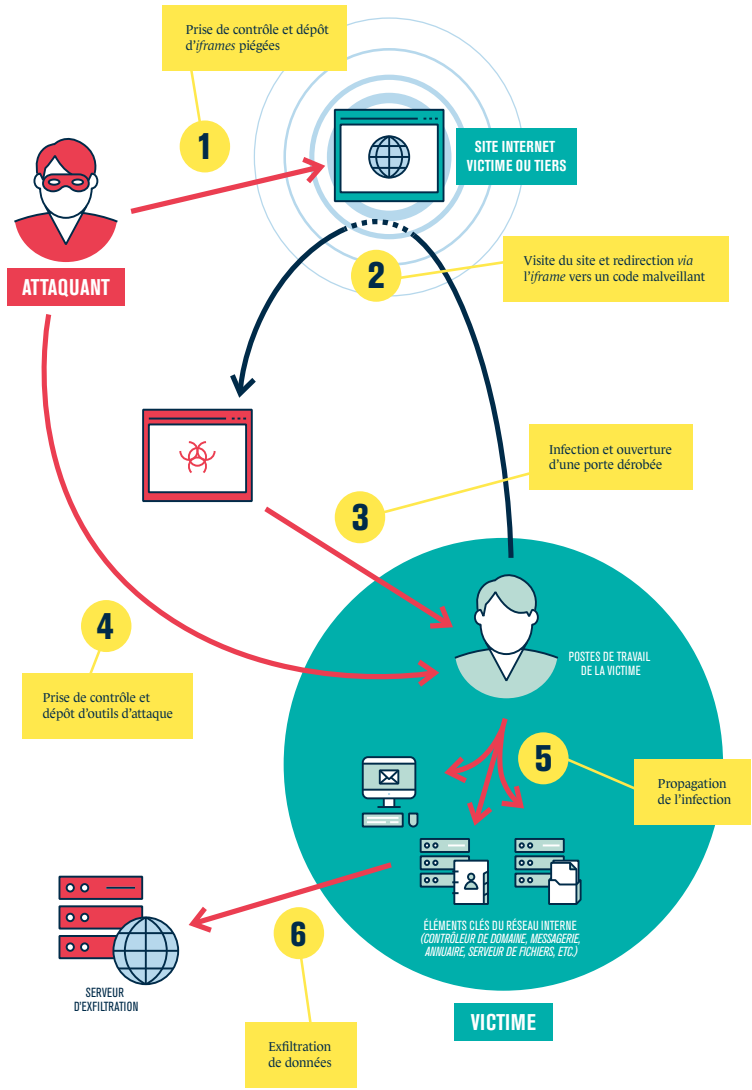


*Figure 4 — **Illustration d'un schéma d'attaque dit par « point d'eau »***

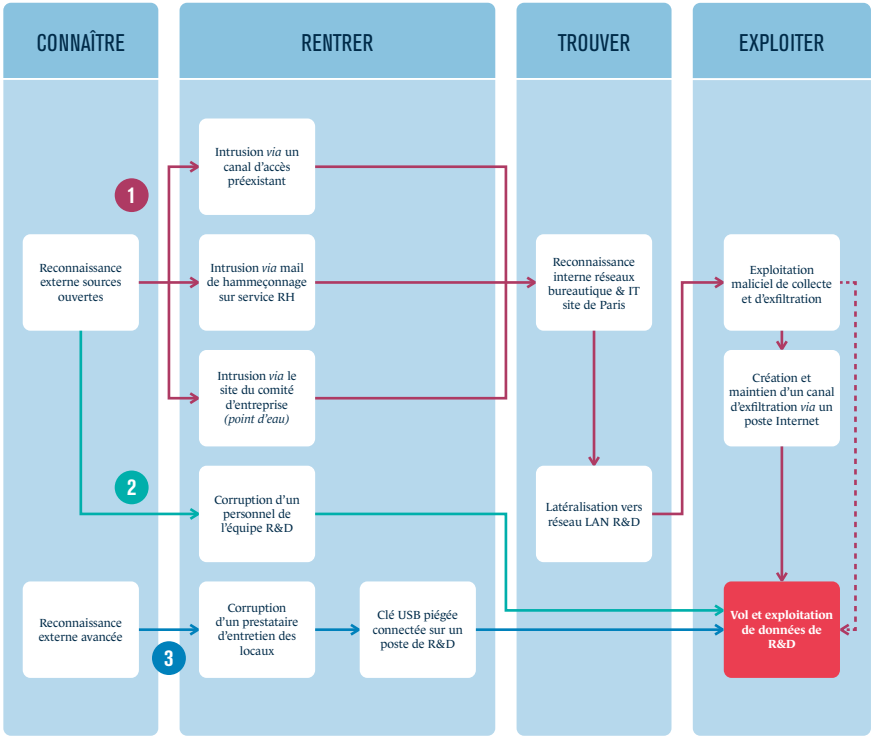
NOTE : dans vos scénarios opérationnels, ajustez la granularité du mode opératoire au niveau de maturité de l'organisation et de profondeur d'analyse visée. Cette approche à géométrie variable permet d'inclure des actions élémentaires macroscopiques (exemple : attaque de type « WannaCry ») ou plus affinées selon le niveau de détail souhaité pour la séquence du scénario étudié ou la sensibilité du groupe de biens supports considéré.

Afin d'éviter une quantité excessive de combinaisons de modes opératoires, privilégiez ceux de moindre effort pour la source de risque et sollicitant un panel représentatif de biens supports présents dans l'organisation.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

L'équipe projet a décidé de représenter les scénarios opérationnels sous la forme de graphes d'attaque. Elle a choisi de se concentrer sur la réalisation d'un premier scénario opérationnel correspondant à un chemin d'attaque stratégique identifié dans l'atelier 3.

Scénario opérationnel relatif au chemin d'attaque « Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données portant directement sur le système d'information de la R&D (de l'entreprise de biotechnologies) » :



L'équipe projet a étudié plusieurs techniques d'accès, parmi lesquelles des actions de collusion, permettant à l'attaquant de rentrer dans le système d'information. L'exploitation d'un éventuel canal préexistant a été considérée à la suite du retour d'expérience du RSSI, mais reste à approfondir. Si un tel canal caché existe, alors il pourrait également servir de canal d'exfiltration (flèche en pointillé). 3 modes opératoires ont été jugés pertinents.

1. L'attaquant s'introduit dans le système d'information par une attaque ciblée sur la messagerie du service des ressources humaines en piégeant le site du comité d'entreprise ou en exploitant un canal caché préexistant. Il accède ensuite aux données stratégiques de R&D du fait notamment de l'absence de cloisonnement entre les réseaux internes puis les exfiltre en utilisant le canal caché voire un canal légitime.

2. L'attaquant corrompt un salarié de l'équipe R&D qui récupère ensuite facilement les informations depuis son poste de travail, dans la mesure où aucune action de supervision n'est réalisée.

3. L'attaquant corrompt un personnel d'entretien des locaux et lui demande de brancher une clé USB préalablement piégée sur un poste de travail de R&D. Cette opération est facilitée par le fait que l'entretien des locaux est réalisé en dehors des heures ouvrées, que le personnel d'entretien a accès librement au bureau d'études et que les ports USB ne sont soumis à aucune restriction.

Lors de l'atelier, il a été noté à maintes reprises que le manque de rigueur actuel dans l'application des correctifs de sécurité facilitait considérablement l'exploitation de vulnérabilités.

b ÉVALUER LA VRAISEMBLANCE DES SCÉNARIOS OPÉRATIONNELS

Pour chaque scénario opérationnel, vous allez évaluer sa vraisemblance globale, qui reflète sa probabilité de réussite ou sa faisabilité.

NOTE : pour rappel, la gravité du scénario opérationnel correspond à la gravité du scénario stratégique associé, évaluée lors de l'atelier 3.

Commencez par évaluer la **vraisemblance élémentaire** de chaque action élémentaire de votre scénario. Celle-ci peut être estimée par le jugement d'un expert ou à l'aide de métriques. L'évaluation confronte d'une part les ressources et la motivation présumées de la source de risque et d'autre part le socle de sécurité de l'objet étudié et le niveau de vulnérabilité de l'écosystème (surface d'attaque exposée, vulnérabilités structurelles et organisationnelles, capacités de détection et de réaction, etc.).

Évaluez ensuite la **vraisemblance globale** du scénario à partir des vraisemblances élémentaires. L'évaluation peut par exemple porter sur le mode opératoire de moindre effort pour la source de risque. Vous pouvez vous reporter à la fiche méthode n° 8 pour réaliser cette évaluation.

NOTE : vous pouvez également effectuer une évaluation directe de la vraisemblance globale du scénario, sans passer par une cotation détaillée des actions élémentaires. Considérez par exemple la vraisemblance des différents modes opératoires dans leur ensemble. Cette méthode expresse perd toutefois en précision par rapport à l'évaluation des vraisemblances élémentaires.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

Les cinq scénarios opérationnels ont été élaborés au cours de l'étape précédente par l'équipe projet (ils ne seront pas représentés ici). Ils ont été évalués selon leur niveau de vraisemblance, sur la base de la grille de cotation suivante :

ÉCHELLE DE VRAISEMBLANCE GLOBALE D'UN SCÉNARIO OPÉRATIONNEL

ÉCHELLE	DESCRIPTION
V4 quasi certain	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée.
V3 Très vraisemblable	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée.
V2 Vraisemblable	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative.
V1 Peu vraisemblable	La source de risque a peu de chance d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible.

CHEMINS D'ATTAQUE STRATÉGIQUES (ASSOCIÉS AUX SCÉNARIOS OPÉRATIONNELS)	VRAISEMBLANCE GLOBALE
Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données portant directement sur le système d'information de la R&D	**V3** Très vraisemblable
Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données sur le système d'information du laboratoire, qui détient une partie des travaux	**V2** Vraisemblable
Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données passant par le prestataire informatique	**V4** Quasi-certain
Un hacktiviste perturbe la production de vaccins en provoquant un arrêt de la production industrielle par compromission de l'équipement de maintenance du fournisseur de matériel	**V2** Vraisemblable
Un hacktiviste perturbe la distribution de vaccins en modifiant leur étiquetage	**V1** Peu vraisemblable

Le vol des données d'études R&D par l'intermédiaire du prestataire informatique est considéré comme quasi certain. D'une part, le prestataire en question dispose de droits d'accès élevés sur le système d'information de la société de biotechnologie et d'autre part la sécurité de son système d'information est faible. La combinaison de ces facteurs aggravants rend une opération d'intrusion et exfiltration très facile pour un attaquant avec un minimum de ressources engagées.

Le vol de données par exfiltration directe est considéré comme très vraisemblable compte tenu des nombreuses vulnérabilités techniques et organisationnelles observées dans l'organisation : utilisateurs peu informés sur les risques numériques (exemple : hameçonnage), site du comité d'entreprise facilement accessible depuis Internet, maintien en condition de sécurité quasi inexistant, réseaux non cloisonnés et administrés depuis des postes connectés à Internet, flux sortants non supervisés, données R&D non protégées et centralisées sur un serveur facilement identifiable.

NOTE : lors de l'élaboration des scénarios opérationnels dans cet atelier, vous pouvez être amené à mettre à jour ou compléter les scénarios stratégiques de l'atelier 3, par exemple si vous identifiez une vulnérabilité impactant une partie prenante non considérée ou un mode opératoire alternatif auquel vous n'aviez pas pensé. Les participants à l'atelier 3 pourront alors choisir de retenir ou non les propositions formulées. Les ateliers 3 et 4 s'alimentent ainsi au cours d'itérations successives. Veillez toutefois à ne pas dépasser deux itérations pour ne pas trop complexifier l'analyse.

ATELIER

5

Traitement du risque

1 / Les objectifs de l'atelier

Le but de cet atelier est de réaliser une synthèse des scénarios de risque identifiés et de définir une stratégie de traitement du risque. Cette stratégie aboutit à la définition de mesures de sécurité, recensées dans un plan d'amélioration continue de la sécurité (PACS). Les risques résiduels sont ensuite identifiés ainsi que le cadre de suivi de ces risques.

2 / Les participants à l'atelier [24]

Les participants sont les mêmes que ceux de l'atelier 1 :

- Direction ;
- Métiers ;
- RSSI ;
- DSI.

3 / Les données de sortie

À l'issue de l'atelier, vous devez avoir défini les éléments suivants :

- la stratégie de traitement du risque ;
- la synthèse des risques résiduels ;
- le plan d'amélioration continue de la sécurité ;
- le cadre du suivi des risques.

24 L'équipe pourra être complétée par toutes personnes jugées utiles.

4 / Les étapes de l'atelier

Cet atelier, d'une durée variable, peut nécessiter deux à quatre demi-journées de travail [25] en vue de :

a. réaliser la synthèse des scénarios de risque ;
b. définir la stratégie de traitement du risque et les mesures de sécurité ;
c. évaluer et documenter les risques résiduels ;
d. mettre en place le cadre de suivi des risques.

5 / Comment procéder ?

Pour mener cet atelier, vous avez besoin de connaitre :

- *le socle de sécurité (atelier 1) ;*
- *les scénarios stratégiques (atelier 3) ;*
- *les mesures de sécurité portant sur l'écosystème (issues de l'atelier 3) ;*
- *les scénarios opérationnels (atelier 4).*

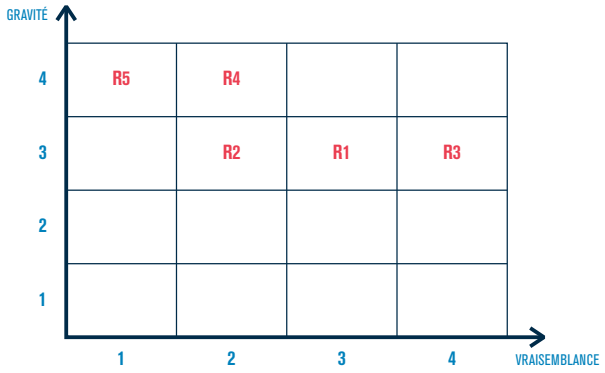
a RÉALISER UNE SYNTHÈSE DES SCÉNARIOS DE RISQUE

Réalisez d'abord une synthèse des scénarios de risque identifiés. Une représentation simple de ces scénarios facilitera leur exploitation par la suite.

Ces scénarios sont le plus souvent positionnés sur une grille, un radar [26] ou un diagramme de Farmer selon leurs niveaux de gravité et de vraisemblance. L'ensemble des représentations adoptées constituera votre **cartographie du risque initial**, c'est-à-dire avant traitement.

25 La durée de l'atelier est proposée à titre indicatif. Elle n'inclut pas le travail de préparation et de formalisation à réaliser en amont et en aval.
26 Diagramme de Kiviat.

EXEMPLE : société de biotechnologie fabriquant des vaccins.



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

Nous vous invitons à affiner ce travail de synthèse en représentant vos scénarios de risque par source de risque et objectif visé (ou selon tout autre critère qui vous semble pertinent). L'objectif est de fournir des éclairages et angles d'analyse différenciés capables d'aider à la compréhension et à l'identification des zones de risque les plus critiques.

NOTE : la couverture des événements redoutés identifiés dans l'atelier 1 est un aspect à considérer dans le travail de synthèse que vous effectuez. Il s'agit d'identifier si des ER de gravité importante – et les valeurs métier sous-jacentes – n'ont pas été laissés de côté, occasionnant un angle mort dans l'appréciation des risques. Passez en revue l'ensemble des ER de l'atelier 1 et identifiez ceux qui n'ont pas été abordés dans un scénario de risque : selon leur gravité et les valeurs métier concernées, vous pourrez alors décider de faire une itération des ateliers 2, 3 et 4 afin de compléter la liste des scénarios de risque. Établissez au besoin une matrice de couverture entre les événements redoutés de l'atelier 1 et les scénarios de risque traités dans l'appréciation des risques.

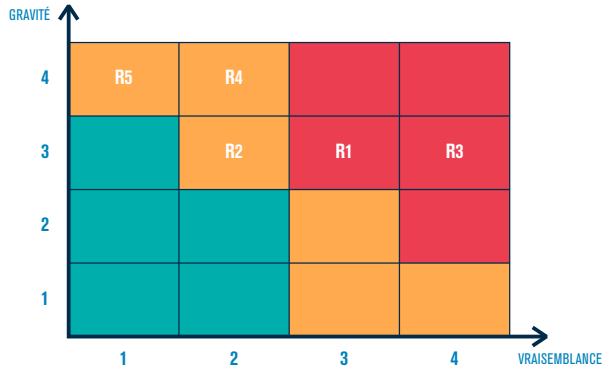
b DÉCIDER DE LA STRATÉGIE DE TRAITEMENT DU RISQUE ET DÉFINIR LES MESURES DE SÉCURITÉ

Pour chaque scénario de risque, accordez-vous sur des seuils d'acceptation du risque et un niveau de sécurité à atteindre en cas de non acceptation. Cette décision se formalise dans la **stratégie de traitement du risque**. Nous vous recommandons les classes d'acceptation suivantes, couramment utilisées en management du risque.

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
Élevé	**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

On pourra par exemple représenter la stratégie de traitement du risque selon le schéma ci-après :

EXEMPLE : société de biotechnologie fabriquant des vaccins.



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

Une fois la stratégie de traitement validée pour chaque scénario, définissez les **mesures de sécurité** associées pour le traiter. Il peut s'agir de mesures *ad hoc* liées au contexte d'emploi et de menace, ou du renforcement de mesures comprises dans le socle de sécurité. Elles viennent compléter les mesures sur l'écosystème identifiées dans l'atelier 3.

L'identification des mesures de traitement du risque doit faire écho aux scénarios stratégiques et opérationnels. Parcourez chaque scénario et posez-vous la question suivante : *quelles sont les phases ou actions élémentaires pour lesquelles il serait pertinent de renforcer la sécurité, afin de rendre la tâche plus difficile pour l'attaquant et diminuer sa probabilité de réussite ?* Dans le cadre d'une démarche d'analyse de la valeur, sécurisez en priorité les actions élémentaires dont la vraisemblance est la plus forte ainsi que les nœuds stratégiques ou opérationnels par lesquels la source de risque pourrait passer. Il s'agit alors de sécuriser en priorité les biens supports critiques concernés.

Documentez l'ensemble de ces mesures de traitement dans un **plan d'amélioration continue de la sécurité (PACS)**, échelonné dans le temps et structuré [27]. À chaque mesure sont associés le responsable, les principaux freins et difficultés de mise en œuvre, le coût et l'échéance. Le PACS favorise l'élévation du niveau de maturité SSI de l'organisation et permet une gestion progressive des risques résiduels.

27 La fiche méthode n°9 propose une structure type des mesures de sécurité.

EXEMPLE : société de biotechnologie fabriquant des vaccins.

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
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
Renforcement de la sécurité du système industriel selon les recommandations ANSSI	R4, R5	RSSI / DSI / Sûreté	Stratégie et plan d'action à définir et valider	+++	12 mois	À lancer
Chiffrement des échanges de données avec les laboratoires	R2	DSI	Identifier le produit de chiffrement et le faire accepter par les laboratoires	++	9 mois	À lancer
DÉFENSE						
Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil.	R1	DSI	Achat d'un outil, budget à provisionner	++	9 mois	À lancer
RÉSILIENCE						
Renforcement du plan de continuité d'activité	R4, R5	Équipe continuité d'activité		++	6 mois	En cours

C ÉVALUER ET DOCUMENTER LES RISQUES RÉSIDUELS

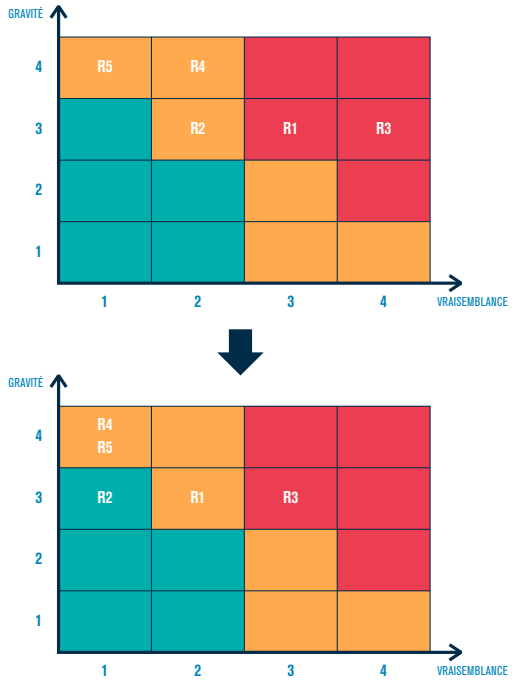
L'évaluation des **risques résiduels (RR)** intervient après l'application des mesures de traitement définies dans l'étape précédente. Vous pouvez par exemple documenter les risques résiduels selon le modèle suivant :

RR01 – *LIBELLÉ DU RISQUE RÉSIDUEL : […]*		
Description et analyse du risque résiduel : ■ *Description sommaire (dont impacts à craindre)* ■ *Vulnérabilités résiduelles susceptibles d'être exploitées par la source de risque* ■ *Autres causes ou facteurs aggravants (négligence, erreur, concours de circonstance, etc.)*		
Événements redoutés concernés : ■ *Événement redouté 1* ■ *Événement redouté 2* ■ *[…]*		
Mesures de traitement du risque existantes et complémentaires : ■ *Mesure 1* ■ *Mesure 2* ■ *[…]*		
Évaluation du risque résiduel :		
Gravité initiale :	Vraisemblance initiale :	Niveau de risque initial :
Gravité résiduelle :	Vraisemblance résiduelle :	Niveau de risque résiduel :
Gestion du risque résiduel : ■ *Mesures particulières de suivi et de contrôle du risque résiduel.*		

Nous vous recommandons de représenter les risques résiduels de la même manière que la cartographie du risque initial. La cartographie du risque résiduel ainsi obtenue pourra alors servir de référence lorsque doit être réalisée la revue formelle des risques (à l'occasion d'une commission d'homologation par exemple). Elle constitue un outil d'aide à la décision pour l'acceptation des risques résiduels.

NOTE : n'hésitez pas à associer à chaque grand jalon du plan d'amélioration de la sécurité (T0+3 mois, T0+6 mois, etc.) une cartographie des risques résiduels. Vous pourrez ainsi présenter à votre hiérarchie ou en commission d'homologation, l'évolution des risques résiduels dans le temps, au regard des actions mises en œuvre.

EXEMPLE : société de biotechnologie fabriquant des vaccins.



La direction a décidé de maintenir le risque R3 à un niveau résiduel élevé, malgré l'application des mesures de remédiation prévues. Ce risque est en effet considéré comme particulièrement problématique, le prestataire informatique étant relativement opposé à la mise en place des mesures de sécurité. Celles-ci impliquent en effet un changement assez profond dans ses méthodes de travail. La piste envisagée pour maîtriser ce risque consisterait donc à entrer dans le capital de ce prestataire afin de modifier la gouvernance en matière de sécurité numérique ou de changer de prestataire.

D'autre part, la direction souhaite mettre sous surveillance la menace bioterroriste jugée actuellement peu pertinente (voir atelier 2), mais qui représente pour elle une préoccupation forte.

d METTRE EN PLACE LE CADRE DE SUIVI DES RISQUES

Le management du risque, notamment le suivi des risques, doit s'appuyer sur des **indicateurs de pilotage** pour assurer par exemple le maintien en condition de sécurité. Ces indicateurs permettent de vérifier l'efficacité des mesures prises et leur adaptation à l'état de la menace.

Une fois ces indicateurs listés, définissez ou affinez le processus d'amélioration continue de la sécurité et la gouvernance afférente (organisation, rôles et responsabilités, comités associés). Il est recommandé de constituer un **comité de pilotage** se réunissant tous les six mois pour aborder cette montée en puissance ou tous les douze mois en rythme de croisière afin d'assurer un suivi des indicateurs, de l'avancement du PACS et de l'évolution des risques.

La mise à jour de l'étude des risques se réalise dans le respect des cycles stratégique et opérationnel prévus. En cas d'événements importants susceptibles de remettre en cause la pertinence des scénarios (émergence d'une nouvelle menace, évolution significative de l'écosystème ou de l'objet de l'étude, etc.), ceux-ci feront l'objet d'une mise à jour au juste niveau.

Bibliographie

ORGANISATION INTERNATIONALE DE NORMALISATION, *ISO 31000 : 2018 – Management du risque – Principes et lignes directrices.* ISO, février 2018.

◆

ORGANISATION INTERNATIONALE DE NORMALISATION, *ISO 27001 : 2013 corr.2 (2015) – Systèmes de management de la sécurité de l'information – Exigences.* ISO, 2015.

◆

ORGANISATION INTERNATIONALE DE NORMALISATION, *ISO 27002 : 2013 corr.2 (2015) – Code de bonnes pratiques pour le management de la sécurité de l'information.* ISO, 2015.

◆

ORGANISATION INTERNATIONALE DE NORMALISATION, *ISO 27005 : 2011 – Gestion des risques liés à la sécurité de l'information.* ISO, juin 2011.

◆

ANSSI, *Guide d'hygiène informatique – Renforcer la sécurité de son système d'information en 42 mesures.* Guide, septembre 2017.

◆

ANSSI, *Cartographie du système d'information – guide d'élaboration en 5 étapes.* Guide, 2018.

◆

ANSSI, *Guides sur la cybersécurité des systèmes industriels. Guides, janvier 2014 et octobre 2016 pour l'étude de cas.*

Termes et définitions

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.

◆

APPRÉCIATION DES RISQUES *(Risk assessment)*

Ensemble du processus d'identification, d'analyse et d'évaluation 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).

◆

BESOIN DE SÉCURITÉ *(Security need)*

Propriété de sécurité à garantir pour une valeur métier. Elle traduit un enjeu de sécurité pour la valeur métier.

EXEMPLES : disponibilité, intégrité, confidentialité, traçabilité.

◆

BIEN SUPPORT *(Supporting asset)*

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

EXEMPLES : serveur, réseau de téléphonie, passerelle d'interconnexion, local technique, dispositif de vidéo protection, équipe en charge du projet, administrateurs, département de R&D.

◆

BIEN SUPPORT CRITIQUE *(Critical supporting asset)*

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.

CARTOGRAPHIE DE MENACE NUMÉRIQUE DE L'ÉCOSYSTÈME *(Ecosystem digital threat mapping)*

Représentation visuelle (exemple : radar) du niveau de menace numérique des parties prenantes de l'écosystème vis-à-vis de l'objet étudié.

◆

CARTOGRAPHIE DU RISQUE *(Risk mapping)*

Représentation visuelle (exemple : radar, diagramme de Farmer) des risques issus des activités d'appréciation du risque.

◆

CHEMIN D'ATTAQUE *(Attack path)*

Suite d'événements distincts que la source de risque devra probablement générer pour atteindre son objectif. Cette terminologie concerne les scénarios stratégiques.

◆

CORRECTIF DE SÉCURITÉ *(Security patch)*

Section de code ajoutée à un logiciel dans le but de corriger une vulnérabilité identifiée.

◆

DÉNI DE SERVICE *(Denial of service)*

Une attaque par déni de service vise à rendre indisponible un ou plusieurs services par l'exploitation, par exemple, d'une vulnérabilité logicielle ou matérielle. On parle de déni de service distribué (de l'anglais Distributed denial of service ou DDoS) lorsque l'attaque fait intervenir un réseau de machines – la plupart du temps compromises – afin d'interrompre le ou les services visés.

ECOSYSTÈME *(Ecosystem)*

Ensemble des parties prenantes en interaction avec l'objet de l'étude. On entend par interaction toute relation intervenant dans le fonctionnement normal de l'objet de l'étude. Les sources de risque ne sont pas considérées a priori comme des parties prenantes, sauf si elles peuvent avoir un effet sur le fonctionnement de l'objet de l'étude.

◆

EVÈNEMENT INTERMÉDIAIRE *(Intermediate event)*

Dans la séquence d'un scénario stratégique, un événement intermédiaire peut être généré par la source de risque à l'égard d'une partie prenante de l'écosystème en vue de faciliter l'atteinte de son objectif.

EXEMPLES : création d'un canal d'exfiltration depuis l'infrastructure du prestataire, attaque en déni de service du fournisseur d'informatique en nuage de la cible.

◆

ÉVÉNEMENT REDOUTÉ *(Feared event)*

Un événement redouté est associé à une valeur métier et porte atteinte à un critère ou besoin de sécurité de la valeur métier (exemples : indisponibilité d'un service, modification illégitime du seuil de température haute d'un processus industriel, divulgation de données classifiées, modification d'une base de données). Les événements redoutés à exploiter sont ceux des scénarios stratégiques et se rapportent à l'impact d'une attaque sur une valeur métier. Chaque événement redouté est évalué selon le niveau de gravité des conséquences, à partir d'une métrique.

◆

GRAVITÉ *(Severity)*

Estimation du niveau et de l'intensité des effets d'un risque. La gravité fournit une mesure des impacts préjudiciables perçus, qu'ils soient directs ou indirects.

EXEMPLES : négligeable, mineure, majeure, critique, maximale.

HOMOLOGATION DE SÉCURITÉ *(Security accreditation)*

Validation par une autorité dite d'homologation, que le niveau de sécurité atteint par l'organisation est conforme aux attentes et que les risques résiduels sont acceptés dans le cadre de l'étude.

◆

INGÉNIERIE SOCIALE *(Social engineering)*

Acquisition déloyale d'information, utilisée pour obtenir d'autrui, un bien, un service ou des informations clés. Cette pratique exploite les failles humaines et sociales de la structure ciblée, à laquelle est lié le système d'information visé. En ayant recours à ses connaissances, au charisme, à l'audace, l'attaquant abuse de la confiance, de l'ignorance ou de la crédulité des personnes ciblées.

◆

MENACE *(Threat)*

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.

◆

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).

MISSION *(Mission)*

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

◆

MODE OPÉRATOIRE *(Operating mode)*

Suite d'actions élémentaires que la source de risque devra probablement réaliser pour atteindre son objectif. Cette terminologie concerne les scénarios opérationnels.

◆

NIVEAU DE MENACE D'UNE PARTIE PRENANTE (VIS-À-VIS DE L'OBJET DE L'ÉTUDE) *(Threat level of a stakeholder)*

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.

◆

NIVEAU DE RISQUE *(Risk level)*

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

◆

OBJECTIF VISÉ (OV) *(Target objective)*

Finalité visée par une source de risque, selon ses motivations.

EXEMPLES : voler des informations à des fins lucratives ou d'espionnage industriel, diffuser un message idéologique, se venger d'un organisme, générer une crise sanitaire.

OBJET DE L'ÉTUDE / OBJET ÉTUDIÉ *(Studied object)*

Organisation, système d'information ou produit faisant l'objet de l'appréciation des risques.

◆

PARTIE PRENANTE *(Stakeholder)*

Élément (personne, système d'information, organisation, ou source de risque) en interaction directe ou indirecte avec l'objet de l'étude. On entend par interaction toute relation intervenant dans le fonctionnement normal de l'objet de l'étude. Une partie prenante peut être interne ou externe à l'organisation à laquelle appartient l'objet de l'étude.

EXEMPLES : partenaire, prestataire, client, fournisseur, filiale, service connexe support.

◆

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 la cartographie de menace numérique de l'écosystème.

◆

PLAN D'AMÉLIORATION CONTINUE DE LA SÉCURITÉ (PACS) *(Security continuous improvement plan)*

Le PACS formalise l'ensemble des mesures de traitement du risque à mettre en œuvre. 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 PACS concernent à la fois l'objet étudié et son écosystème.

POINT D'EAU *(Waterhole)*

Piège mis en place sur un serveur d'un site Internet régulièrement visité par les utilisateurs ciblés. L'attaquant attend une connexion de sa victime sur le serveur pour la compromettre. Le site Internet piégé peut être un site légitime ou un faux site.

◆

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.

◆

SCÉNARIO DE RISQUE *(Risk scenario)*

Scénario complet, allant de la source de risque à l'objectif visé par elle, décrivant un chemin d'attaque et le scénario opérationnel associé.

NOTE : dans le cadre de ce guide, on considère uniquement les scénarios de risque numérique de nature intentionnelle.

SCÉNARIO OPÉRATIONNEL *(Operational scenario)*

Enchainement d'actions élémentaires portées sur les biens supports de l'objet étudié ou de son écosystème. Planifiés par la source de risque en vue d'atteindre un objectif déterminé, les scénarios opérationnels sont évalués en termes de vraisemblance.

◆

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 évalués en termes de gravité.

◆

SOURCE DE RISQUE (SR) *(Risk origin)*

Élément, personne, groupe de personnes ou organisation susceptible d'engendrer un risque. Une source de risque peut être caractérisée par sa motivation, ses ressources, ses compétences, ses modes opératoires (de prédilection).

EXEMPLES : services étatiques, hacktivistes, concurrents, employés vengeurs.

◆

STRATÉGIE DE TRAITEMENT DU RISQUE *(Risk treatment strategy)*

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. Elle se réalise à partir de la cartographie du risque initial : pour chaque risque issu des activités d'appréciation du risque, la stratégie de traitement doit définir l'acceptabilité du risque (exemple : inacceptable, tolérable, acceptable). Habituellement l'acceptabilité est directement déduite du niveau de risque et la stratégie en est la simple formalisation. Le rôle de la stratégie de traitement du risque est de décider de l'acceptation de chaque risque à la lumière des activités d'appréciation.

SURFACE D'ATTAQUE *(Attack surface)*

Ensemble des biens supports sur lesquels repose l'objet de l'étude ou qui sont en interaction avec celui-ci, qui pourraient être utilisés pour réaliser une attaque. Une surface d'attaque est d'autant plus large que le nombre de biens supports est grand ou que ces derniers disposent de vulnérabilités exploitables par un attaquant.

◆

TEST OU AUDIT D'INTRUSION *(Penetration test, pentest)*

Méthode consistant généralement à simuler une attaque d'un utilisateur mal intentionné, en essayant plusieurs codes d'exploitation afin de déterminer ceux qui donnent des résultats positifs. Il s'agit à la fois d'une intention défensive (mieux se protéger) et d'une action offensive (agresser son propre système d'information). On analyse alors les risques potentiels dus à une mauvaise configuration (audit d'infrastructure) ou à un défaut de programmation (audit de produit).

◆

VALEUR MÉTIER *(Business asset)*

Dans le cadre de l'étude, 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.

EXEMPLES : service d'annulation de réservations en ligne ou de sauvegarde, informations clients, service de supervision, résultats de travaux de R&D, données à caractère personnel, phase de déploiement d'un projet, savoir-faire en conception de pièces aéronautiques.

NOTES :

- les valeurs métier représentent le patrimoine informationnel qu'une source de risque aurait intérêt à attaquer pour porter atteinte à l'objet de l'étude ;
- dans EBIOS 2010, cela correspond aux biens essentiels.

VRAISEMBLANCE *(Likelihood)*

Estimation de la faisabilité ou de la probabilité qu'un risque se réalise, selon l'échelle adoptée (très faible, peu vraisemblable, quasi certain, etc.)

◆

VRAISEMBLANCE ÉLÉMENTAIRE *(Elementary likelihood)*

Vraisemblance d'une action élémentaire identifiée dans un scénario opérationnel. Elle peut être jugement d'un expert ou à l'aide d'échelles. L'évaluation confronte d'une part les ressources et la motivation présumées de la source de risque et d'autre part le socle de sécurité de l'objet étudié et le niveau de vulnérabilité de l'écosystème (surface d'attaque exposée, vulnérabilités structurelles et organisationnelles, capacités de détection et de réaction, etc.).

◆

VULNÉRABILITÉ *(Vulnerability)*

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.

Version 1.1 – Décembre 2018
ANSSI-PA-048

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI – 51, boulevard de la Tour-Maubourg – 75 700 PARIS 07 SP
www.ssi.gouv.fr – communication@ssi.gouv.fr – ebios@ssi.gouv.fr