



EBIOS

Risk Manager

Fiches méthodes

Note à l'attention des lecteurs :

Ces « fiches méthodes » ont été créées pour aider les utilisateurs de la méthode EBIOS *RISK MANAGER* à réaliser chaque atelier.

Disponibles en version « projet », elles peuvent être utilisées en l'état et appuyer efficacement le déroulement des ateliers décrits dans le guide.

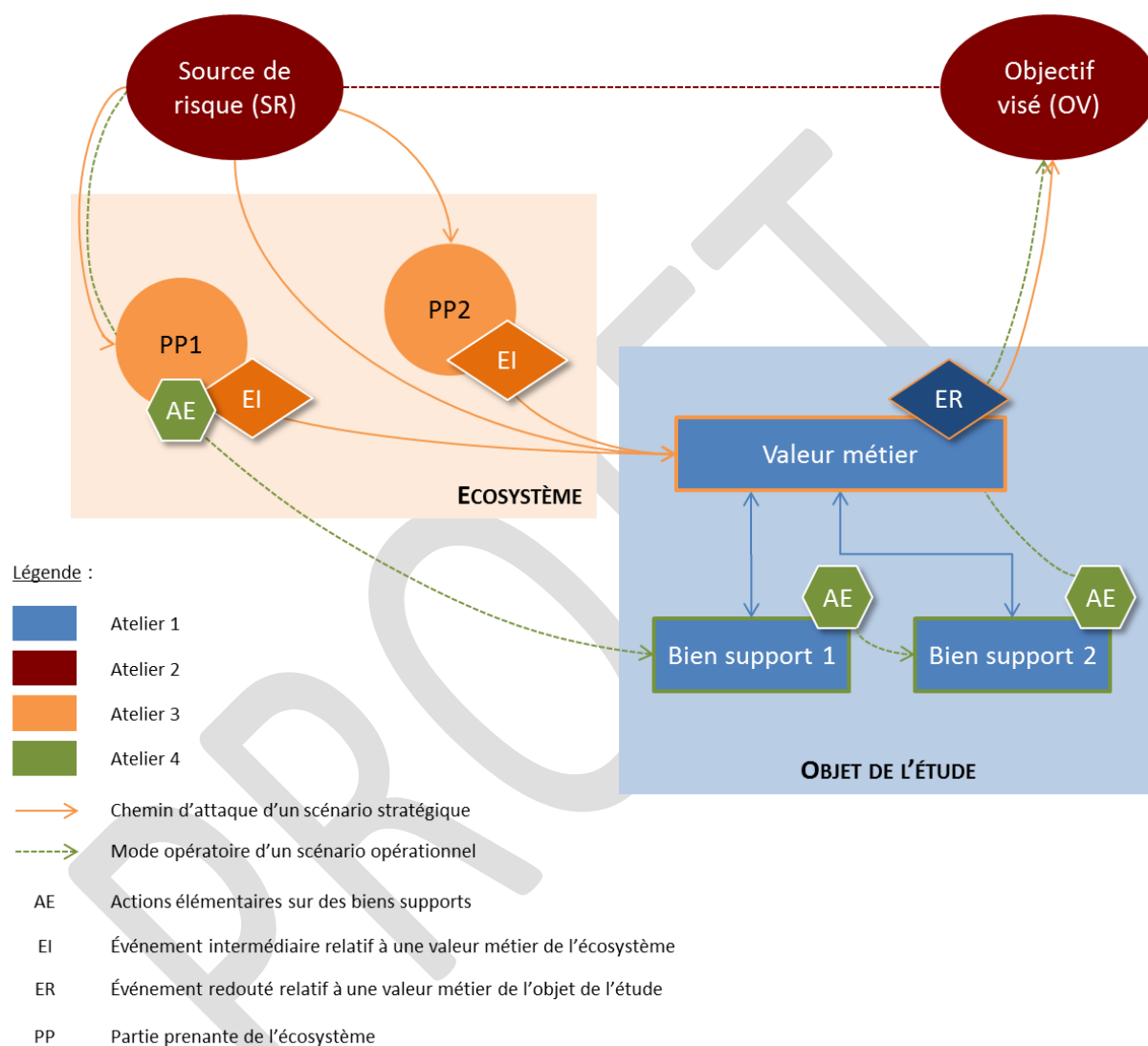
Une version 1.0 en français et en anglais sera prochainement disponible.

Table des matières

Introduction : positionnement des ateliers dans la démarche d'appréciation des risques	3
Fiche méthode n°1 : Définir le périmètre métier et technique (Atelier 1)	5
Fiche méthode n°2 : Identifier les biens supports (Ateliers 1, 4 et 5)	6
Fiche méthode n°3 : Évaluer la gravité des impacts des événements redoutés (Ateliers 1 et 3)	8
Fiche méthode n°4 : Identifier et caractériser les sources de risque (Atelier 2)	12
Fiche méthode n°5 : Construire la cartographie de menace numérique de l'écosystème (Atelier 3)	16
Fiche méthode n°6 : Définir des mesures de sécurité pour l'écosystème (Atelier 3)	21
Fiche méthode n°7 : Construire des graphes d'attaque (Atelier 4)	22
Fiche méthode n°8 : Évaluer la vraisemblance des scénarios opérationnels (Atelier 4)	28
Fiche méthode n°9 : Structurer les mesures de traitement du risque (Atelier 5)	40
Termes et définitions	41

Introduction : positionnement des ateliers dans la démarche d'appréciation des risques

Le schéma ci-dessous présente les différents termes utilisés dans EBIOS *Risk Manager* pour l'appréciation des risques.



Lors de l'atelier 1, les participants identifient le périmètre métier et technique de l'objet de l'étude, correspondant aux **valeurs métier** et **biens supports**. Ils définissent également les **événements redoutés** associés aux valeurs métiers et leur niveau de gravité.

L'atelier 2 permet d'identifier les couples **source de risque/objectif visé** (SR/OV) les plus pertinents pour la suite de l'étude. Certains objectifs visés (du point de vue de l'attaquant) se rapprocheront de certains événements redoutés (du point de vue de l'organisation). Par exemple on peut rapprocher l'objectif visé « exfiltrer des informations pour obtenir un avantage concurrentiel » de l'événement redouté « fuite des informations de R&D de l'entreprise ». Ce rapprochement est une première étape vers la construction des scénarios stratégiques.

Au début de l'atelier 3, les participants identifient les **parties prenantes** de l'écosystème de l'objet étudié et évaluent leur niveau de menace. Suite à cette évaluation, les participants définissent des

scénarios stratégiques partant de la source de risque vers son objectif visé. Ces scénarios mettent en œuvre des **chemins d'attaque** au cours desquels la source de risque génère un ou des événements redoutés sur les valeurs métier de l'objet étudié. Dans une logique de moindre effort du point de vue de la source de risque, certains chemins d'attaque sont susceptibles de passer par des parties prenantes de l'écosystème en générant des **événements dits intermédiaires**.

Dans l'atelier 4, les participants établissent des **scénarios opérationnels** qui décrivent les **modes opératoires** techniques susceptibles d'être utilisés par la source de risque pour réaliser les scénarios stratégiques identifiés dans l'atelier 3. Un scénario opérationnel est un enchaînement **d'actions élémentaires** portant sur les biens supports de l'objet étudié ou de son écosystème. Chaque chemin d'attaque d'un scénario stratégique donne lieu à un scénario opérationnel, lequel est évalué en termes de vraisemblance.

PROJET

Fiche méthode n°1 : Définir le périmètre métier et technique (Atelier 1)

Le travail de recensement des missions, valeurs métier et biens supports relatifs à l'objet de l'étude, peut être formalisé dans une table, telle que celle proposée ci-dessous :

Missions	Mission 1		Mission ...
Dénomination de la valeur métier	<i>Valeur métier 1</i>	<i>Valeur métier 2</i>	<i>Valeur métier ...</i>
Nature de la valeur métier (processus ou information)			
Description			
Entité ou personne responsable (interne/externe)			
Dénomination du/des bien(s) support(s) associé(s)	<i>Bien support 1</i>	<i>Bien support 2</i>	<i>Bien support 3</i>
Description			
Entité ou personne responsable (interne/externe)			

À chaque valeur métier et bien support correspond une entité ou une personne responsable. Cette entité ou personne peut être interne à l'organisation ou une partie prenante externe de l'écosystème. Les éléments relatifs à l'écosystème seront repris dans le cadre de l'atelier 3.

Fiche méthode n°2 : Identifier les biens supports (Ateliers 1, 4 et 5)

Les types de biens supports représentent les grandes catégories de composants d'un système d'information sur lesquels reposent les valeurs métier ou les mesures de sécurité.

Cette fiche méthode pourra vous être utile lors de la définition du périmètre métier et technique (Atelier 1), de la construction des scénarios opérationnels (Atelier 4) ou de la définition des mesures de sécurité (Atelier 5).

Les biens supports peuvent être regroupés selon les catégories suivantes :

Bien support	Exemples (listes non exhaustives)
Systèmes informatiques et de téléphonie	
Matériels ¹	
Terminal utilisateur	Ordinateur fixe, ordinateur portable, tablette, ordiphone
Périphérique	Imprimante, scanner, clavier, souris, caméra, microphone, objet connecté
Téléphone	Téléphone fixe ou mobile, analogique ou IP
Équipement de stockage	Clé USB, disque dur, CD-ROM, carte mémoire
Serveur	Mainframe, serveur lame, serveur rack
Moyen d'administration	Poste d'administration, serveur outils d'administration, bastion
Équipement réseau	Commutateur, routeur, passerelles d'entrée depuis l'extérieur, borne wifi
Équipement de sécurité	Pare-feu, sonde (IDS/IPS), passerelle VPN
Équipement industriel	Automate programmable industriel, capteur, actionneur, système SCADA, système instrumenté de sécurité
Logiciels	
Service d'infrastructure	Service d'annuaire, service de gestion d'adresses IP (DHCP), service de nom de domaine (DNS), contrôleur de domaine, serveur d'impression
Application/Service applicatif	Serveur web, service web, serveur d'application, serveur de courrier électronique, serveur de bases de données, progiciels (RH, relation client, ERP)
Intergiciel (<i>middleware</i>)	EAI (<i>Enterprise Application Integration</i>), ETL (<i>Extract-Transform-Load</i>), ODBC (<i>Open DataBase Connectivity</i>)
Système d'exploitation, hyperviseur	Windows, Linux, MacOS, Xen

¹ Les matériels embarquent la plupart du temps des logiciels permettant leur fonctionnement.

Micrologiciel (<i>firmware</i>)	BIOS (Basic Input Output System), UEFI (<i>Unified Extensible Firmware Interface</i>), gestionnaire de composants d'un téléphone mobile, programme stocké dans une clé USB équipée d'un microprocesseur
Logiciel de sécurité	Outil de gestion d'événements SIEM (<i>Security Information and Event Management</i>)
Réseaux/Canaux informatiques et de téléphonie	
Réseau/Canal informatique	Câble réseau, fibre optique, liaison radio (wifi, Bluetooth, etc.)
Réseau/Canal téléphonique	Ligne téléphonique
Organisations	
Personne	Employé, stagiaire, prestataire, personnel d'entretien
Support papier	Document manuscrit ou imprimé
Échange verbal	Réunion, discussion de couloir
Élément d'ingénierie sociale	Information partagée sur les réseaux sociaux
Locaux	
Site/Bâtiment/Salle	Site du siège social, site d'usine, enceinte, bâtiment de stockage, bâtiment industriel, salle de réunion, salle serveur
Système de sécurité physique	Système d'accès par badge, système de détection d'intrusion, système de vidéo-protection
Système de sûreté de fonctionnement	Climatisation, sécurité incendie, alimentation électrique

Pour aller plus loin et notamment avoir des définitions plus précises des biens supports mentionnés, vous pouvez vous reporter au guide « Cartographie du système d'information » de l'ANSSI.

Fiche méthode n°3 : Évaluer la gravité des impacts des événements redoutés (Ateliers 1 et 3)

1 / Quelles catégories d'impacts faut-il prendre en compte ?

Les catégories ci-après peuvent servir de base pour identifier les impacts liés aux événements redoutés et faciliter l'évaluation de la gravité :

- impacts sur les missions et services de l'organisation ;
- impacts humains, matériels ou environnementaux ;
- impacts sur la gouvernance ;
- impacts financiers ;
- impacts juridiques ;
- impacts sur l'image et la confiance.

Note : selon le contexte, certaines catégories peuvent correspondre à des facteurs aggravants ou à des impacts indirects.

Impact	Exemples (listes non exhaustives)
Impacts sur les missions et services de l'organisation	
Conséquences directes ou indirectes sur la réalisation des missions et services	<i>Incapacité à fournir un service, dégradation de performances opérationnelles, retards, impacts sur la production ou la distribution de biens ou de services, impossibilité de mettre en œuvre un processus clé</i>
Impacts humains, matériels ou environnementaux	
<u>Impacts sur la sécurité ou sur la santé des personnes</u> Conséquences directes ou indirectes sur l'intégrité physique de personnes	<i>Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire</i>
<u>Impacts matériels</u> Dégâts matériels ou destruction de biens supports	<i>Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématurée de matériels</i>
<u>Impacts sur l'environnement</u> Conséquences écologiques à court ou long terme, directes ou indirectes	<i>Contamination radiologique ou chimique des nappes phréatiques ou des sols, rejet de polluants dans l'atmosphère</i>
Impacts sur la gouvernance	
<u>Impacts sur la capacité de développement ou de décision</u> Conséquences directes ou indirectes sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement	<i>Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisation, changement contraint de stratégie, perte de fournisseurs ou de sous-traitants clés</i>

<u>Impacts sur le lien social interne</u> Conséquences directes ou indirectes sur la qualité des liens sociaux au sein de l'organisation.	<i>Perte de confiance des employés dans la pérennité de l'organisation, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, perte de sens des valeurs communes</i>
<u>Impacts sur le patrimoine intellectuel ou culturel</u> Conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisation, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes.	<i>Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés</i>
Impacts financiers	
Conséquences pécuniaires, directes ou indirectes.	<i>Perte de chiffre d'affaires, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées</i>
Impacts juridiques	
Conséquences suite à une non-conformité légale, réglementaire, normative ou contractuelle.	<i>Procès, amende, condamnation d'un dirigeant, amendement de contrat</i>
Impacts sur l'image et la confiance	
Conséquences directes ou indirectes sur l'image de l'organisation, la notoriété, la confiance des clients.	<i>Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte de notoriété, perte de confiance d'utilisateurs</i>

2 / Quelle échelle de gravité utiliser ?

Lorsque l'on évalue une échelle de niveaux d'impacts, le principal enjeu réside dans le fait qu'elle soit comprise et utilisable par les personnes amenées à évaluer l'importance des conséquences d'un événement redouté. Idéalement, son élaboration est réalisée en collaboration avec les personnes qui vont estimer ces niveaux – particulièrement les métiers – afin de faciliter son appropriation et la cohérence de la cotation. La « meilleure » échelle de gravité à utiliser reste celle déjà mise en place, si elle existe, pour l'appréciation des risques de l'organisation dans le cadre de son management du risque global (qui inclut le risque financier, juridique, etc.). En effet, le risque numérique doit au final s'intégrer dans la cartographie globale du risque. D'autre part, un certain nombre de réglementations sectorielles disposent d'échelles de niveaux d'impacts qu'il convient donc d'utiliser, ou avec lesquelles il convient au moins d'être compatible.

Si vous ne disposez pas d'une telle échelle, établissez-en une avec les métiers au début de l'atelier dédié aux événements redoutés. Pour ce faire, vous pouvez utiliser et adapter l'échelle générique ci-après, qui prend en compte les impacts internes à l'organisation et les éventuelles conséquences externes sur les écosystèmes.

Niveau de l'échelle	Conséquences
G5 – Catastrophique	<p>Conséquences sectorielles ou régaliennes au-delà de l'organisation</p> <p><i>Ecosystème(s) sectoriel(s) impacté(s) de façon importante, avec des conséquences éventuellement durables</i></p> <p><i>Et/ou : difficulté pour l'Etat, voire incapacité, d'assurer une fonction régalienne ou une de ses missions d'importance vitale</i></p> <p><i>Et/ou : impacts critiques sur la sécurité des personnes et des biens (crise sanitaire, pollution environnementale majeure, destruction d'infrastructures essentielles, etc.)</i></p>
G4 – Critique	<p>Conséquences désastreuses pour l'organisation, avec d'éventuels impacts sur l'écosystème</p> <p><i>Incapacité pour l'organisation d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens : l'organisation ne surmontera vraisemblablement pas la situation (sa survie est menacée), les secteurs d'activité ou étatiques dans lesquels il opère seront susceptibles d'être légèrement impactés sans conséquence durable</i></p>
G3 – Grave	<p>Conséquences importantes pour l'organisation</p> <p><i>Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens : l'organisation surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé), sans impact sectoriel ou étatique</i></p>
G2 – Significative	<p>Conséquences significatives mais limitées pour l'organisation</p> <p><i>Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens : l'organisation surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé)</i></p>
G1 – Mineure	<p>Conséquences négligeables pour l'organisation</p> <p><i>Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens : l'organisation surmontera la situation sans trop de difficultés (consommation des marges)</i></p>

L'usage d'une échelle à 4 ou 5 niveaux est guidé par les considérations suivantes :

- la nécessité de mesurer des impacts très élevés qui correspondent à des crises majeures, voire une déstabilisation et une perte de résilience allant au-delà de la seule organisation concernée (exemples : paralysie ou forte dégradation de l'ensemble d'un secteur industriel, incapacité pour l'État d'assurer une fonction régalienne, crise sanitaire ou pollution majeure touchant une zone importante, compromission d'information hautement classifiée) : dans ce cas, une échelle à 5 niveaux est recommandée. Dans le cas contraire, une échelle à 4 niveaux suffit ;
- la cohérence du nombre de niveaux entre les échelles de gravité et de vraisemblance pour l'appréciation des risques lors de l'atelier 4 (si vous utilisez une échelle de vraisemblance à 5 niveaux, utilisez de préférence une échelle de gravité à 5 niveaux).

Note : l'estimation de l'importance des impacts doit être contextualisée, de telle sorte que les acteurs soient capables de bien distinguer les niveaux d'impacts de l'échelle. Une façon usuelle de procéder est de fournir des exemples pour appuyer la description de chaque niveau.

Exemple d'échelle de gravité pour une activité de production industrielle :

Niveau de l'échelle	Conséquences sur l'exploitation
G4 – Critique	Arrêt durable de l'exploitation nécessitant une intervention de maintenance
G3 – Grave	Arrêt temporaire de l'exploitation puis reprise avec une procédure particulière (ex. : opérateur supplémentaire)
G2 – Significative	Poursuite de l'exploitation avec une action opérateur
G1 – Mineure	Poursuite de l'exploitation avec une alarme signalant le défaut

Fiche méthode n°4 : Identifier et caractériser les sources de risque (Atelier 2)

1 / Catégories de sources de risque (SR) et d'objectifs visés (OV)

La grille suivante présente des catégories génériques de sources de risque intentionnelles et d'objectifs visés, que vous pouvez utiliser pour identifier les couples SR/OV.

Catégories de sources de risque

Les profils d'attaquants peuvent être regroupés selon trois grandes catégories :

- les organisations structurées guidées par une logique d'efficacité et de gain, qui ont des moyens sophistiqués et conséquents, voire quasi-illimités (états, crime organisé) ;
- les organisations ou groupes guidés par une motivation idéologique, qui disposent de moyens significatifs mis en œuvre de façon relativement coordonnée (terroristes, activistes) ;
- les attaquants individuels, gangs isolés ou officines, qui disposent de moyens limités mais spécialisés.

Ces catégories peuvent collaborer entre-elles de façon opportuniste ou organisée (ex : organisation terroriste faisant appel à une officine spécialisée).

Profils d'attaquants	Exemples et modes opératoires habituels
Étatique	États, agences de renseignement. <i>Attaques généralement conduites par des professionnels, respectant un calendrier et un mode opératoire défini. Les caractéristiques de ce profil d'attaquant sont sa capacité à réaliser une opération offensive sur le long terme (ressources stables, procédures), et à adapter ses outils et méthodes à la topologie de la cible. Par extension, ces acteurs ont les moyens d'acheter ou de découvrir des vulnérabilités jour zéro (0-Day), certains sont en mesure d'infiltrer des réseaux isolés et de réaliser des attaques successives pour atteindre une ou des cibles finales (par exemple via une attaque sur la chaîne d'approvisionnement).</i>
Crime organisé	Organisations cybercriminelles (mafias, gangs, officines organisées). <i>Arnaque en ligne, arnaque au président, demande de rançon/attaque par rançongiciel, exploitation de réseaux de robots (botnet), etc. Du fait notamment de la prolifération des kits d'attaques facilement accessibles en ligne, les cybercriminels mènent des opérations de plus en plus sophistiquées et organisées, à des fins lucratives ou de fraude. Certains ont les moyens d'acheter ou de découvrir des vulnérabilités jour zéro (0-Day).</i>
Terroriste	Cyber-terroristes, cyber-milices. <i>Attaques habituellement peu sophistiquées mais menées avec une forte détermination de déstabilisation et de destruction : déni de service (visant par exemple à rendre indisponible les services d'urgence d'un centre hospitalier, arrêts intempestifs d'un système industriel de production d'énergie), exploitation de vulnérabilités de sites Internet et défigurations.</i>
Activiste idéologique	Cyber-hacktivistes, groupements d'intérêt, sectes. <i>Modes opératoires et sophistication des attaques relativement similaires à ceux des cyber-terroristes, mais avec des motivations moins destructrices. Certains acteurs sont à même de mener des attaques pour véhiculer une idéologie, un message (exemple : utilisation massive des réseaux sociaux comme caisse de résonance).</i>

Officine spécialisée	<p>Profil de « cyber-mercenaire » doté de capacités informatiques généralement élevées sur le plan technique. Il est de ce fait à distinguer des <i>script-kiddies</i> avec qui il partage toutefois l'esprit de défi et de recherche de reconnaissance, mais avec un objectif de gain financier. De tels groupes peuvent s'organiser en officines spécialisées proposant de véritables services de piratage.</p> <p><i>Ce type de hacker chevronné est souvent à l'origine de la conception et la création d'outils et kits d'attaques² accessibles en ligne (éventuellement monnayés), qui sont ensuite utilisés « clés en main » par d'autres groupes d'attaquants. Il n'a pas de motivations particulières autres que le gain financier.</i></p>
Amateur	<p>Profil du hacker « <i>script-kiddies</i> » ou doté de bonnes connaissances informatiques, et motivé par une quête de reconnaissance sociale, d'amusement, de défi.</p> <p><i>Attaques basiques, mais capacité à utiliser des kits d'attaques proposés en ligne.</i></p>
Vengeur	<p>Les motivations de ce profil d'attaquant sont guidées par un esprit de vengeance aigu ou un sentiment d'injustice (exemples : ancien salarié licencié pour faute grave, prestataire mécontent suite au non renouvellement d'un marché, etc.).</p> <p><i>Les caractéristiques de ce profil d'attaquant sont sa détermination et sa connaissance interne des systèmes et processus organisationnels. Cela peut le rendre redoutable et lui conférer un pouvoir de nuisance important.</i></p>
Malveillant pathologique	<p>Les motivations de ce profil d'attaquant sont d'ordre pathologique ou opportuniste et sont parfois guidées par l'appât du gain (exemples : concurrent déloyal, client malhonnête, escroc, fraudeur).</p> <p><i>Ici, soit l'attaquant dispose d'un socle de connaissances en informatique qui l'amène à tenter de compromettre le SI de sa cible, soit il exploite par lui-même des kits d'attaques disponibles en ligne, soit il décide de sous-traiter l'attaque informatique en faisant appel à une officine spécialisée. Dans certains cas, l'attaquant peut faire appel à une source interne (salarié mécontent, prestataire peu scrupuleux) et la corrompre.</i></p>

Catégories d'objectifs visés

Finalités poursuivies	Description
Espionnage	<p>Opération de renseignement (étatique, économique). Dans de nombreux cas, l'attaquant s'installe durablement dans le système d'information et en toute discrétion.</p> <p>L'armement, le spatial, l'aéronautique, le secteur pharmaceutique, l'énergie ou encore certaines activités de l'État (économie, finances, affaires étrangères) constituent des cibles privilégiées.</p>
Pré-positionnement stratégique	<p>Pré-positionnement visant généralement une attaque sur le long terme, sans que la finalité poursuivie soit clairement établie (exemples : compromission de réseaux d'opérateurs de télécommunication, infiltration de sites Internet d'information de masse pour lancer une opération d'influence politique ou économique à fort écho). La compromission soudaine et massive d'ordinateurs afin de constituer un réseau de robots peut être affiliée à cette catégorie.</p>

² Citons les services de type CaaS (*Crimeware as a Service*).

Influence	Opération visant à diffuser de fausses informations ou à les altérer, mobiliser les leaders d'opinion sur les réseaux sociaux, détruire des réputations personnelles et/ou professionnelles, divulguer des informations confidentielles, dégrader l'image d'une organisation ou d'un l'État. La finalité est généralement la déstabilisation ou la modification des perceptions.
Entrave au fonctionnement	Opération de sabotage visant par exemple à rendre indisponible un site Internet, à provoquer une saturation informationnelle, à empêcher l'usage d'une ressource numérique, à rendre indisponible une installation physique. Les systèmes industriels peuvent être particulièrement exposés et vulnérables au travers des réseaux informatiques auxquels ils sont interconnectés (exemple : envoi de commandes afin de générer un dommage matériel ou une panne nécessitant une maintenance lourde). Les attaques en déni de service distribué (DDoS) sont des techniques largement utilisées pour neutraliser des ressources numériques
Lucratif	Opération visant un gain financier, de façon directe ou indirecte. Généralement liée au crime organisé, on peut citer : escroquerie sur Internet, blanchiment d'argent, extorsion ou détournement d'argent, manipulation de marchés financiers, falsification de documents administratifs, usurpation d'identité, etc. Il est à noter que certaines opérations à but lucratif peuvent recourir à un mode opératoire relevant des catégories ci-dessus (exemple : espionnage et vol de données, rançongiciel pour neutraliser une activité), mais l'objectif final reste financier.
Défi, amusement	Opération visant à réaliser un exploit à des fins de reconnaissance sociale, de défi ou de simple amusement. Même si l'objectif est essentiellement ludique et sans volonté particulière de nuire, ce type d'opération peut conduire à des conséquences importantes pour la victime.

2 / Formalisation des couples SR/OV

L'analyse des couples SR/OV peut être documentée dans un tableau, tel que celui proposé ci-après (P1 : couple SR/OV prioritaire, P2 : couple secondaire) :

IDENTIFICATION		COTATION			CARACTERISATION				EVALUATION	
Source de risque (SR)	Objectif visé (OV)	Motivation	Ressources	<i>Activité</i>	<i>Modes opératoires</i>	<i>Secteurs d'activités</i>	<i>Arsenal d'attaque</i>	<i>Faits d'armes</i>	Pertinence du couple SR/OV	Choix P1/P2

Les ressources incluent à la fois les capacités financières et matérielles de la source de risque, et son niveau de compétence en matière de cyber-attaques. Cette compétence peut être également recherchée auprès d'offices spécialisées (sophistication des modes opératoires, arsenal d'attaque, etc.).

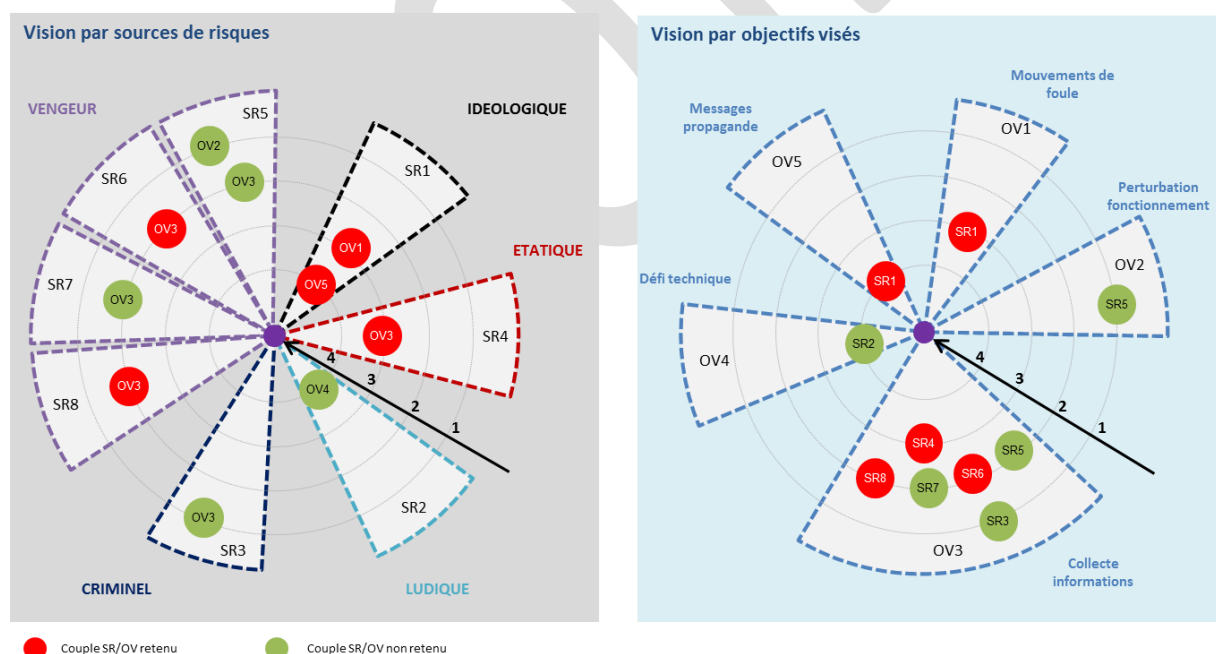
Les informations en italique sont optionnelles. Elles permettent de caractériser plus finement les sources de risque et nécessitent généralement le support d'une expertise avancée ou de bases de connaissances en analyse de la menace.

Le niveau de pertinence d'un couple SR/OV peut être évalué à partir des cotations de

motivation, ressources et activité. En l'absence d'information suffisante sur l'activité de la source de risque dans votre secteur, vous pouvez évaluer chaque couple SR/OV sur la seule base de sa motivation et de ses ressources, en utilisant par exemple la métrique ci-après :

		Motivation		
		+	++	+++
Ressources	+++	MOYEN	ELEVE	ELEVE
	++	FAIBLE	MOYEN	ELEVE
	+	FAIBLE	FAIBLE	MOYEN

Une représentation sur des cartographies visuelles de type radar est également recommandée pour faciliter la sélection des couples SR/OV prioritaires et valoriser les résultats de l'atelier. Dans l'illustration ci-après, deux angles de vue sont représentés (par sources de risque et par objectifs visés), ce qui permet d'affiner l'exploitation des résultats de l'atelier. La distance radiale correspond au niveau de pertinence évalué pour l'élément (plus les cercles sont proches du centre, plus ils sont estimés dangereux pour l'organisation). La sélection des couples SR/OV est réalisée en privilégiant des couples situés près du centre et suffisamment éloignés les uns des autres, afin de disposer d'un panel de sources de risque et d'objectifs visés varié.



Fiche méthode n°5 : Construire la cartographie de menace numérique de l'écosystème (Atelier 3)

1 / Quelles sont les parties prenantes (PP) à prendre en compte ?

Les parties prenantes à prendre en considération peuvent être de deux natures :

- parties prenantes externes :
 - clients ;
 - partenaires, cotraitants ;
 - prestataires (sous-traitants, fournisseurs).
- parties prenantes internes :
 - services connexes techniques (exemple : services supports proposés par une DSI) ;
 - services connexes métiers (exemple : entité commerciale utilisatrice des données métiers) ;
 - filiales (notamment implantées dans d'autres pays).

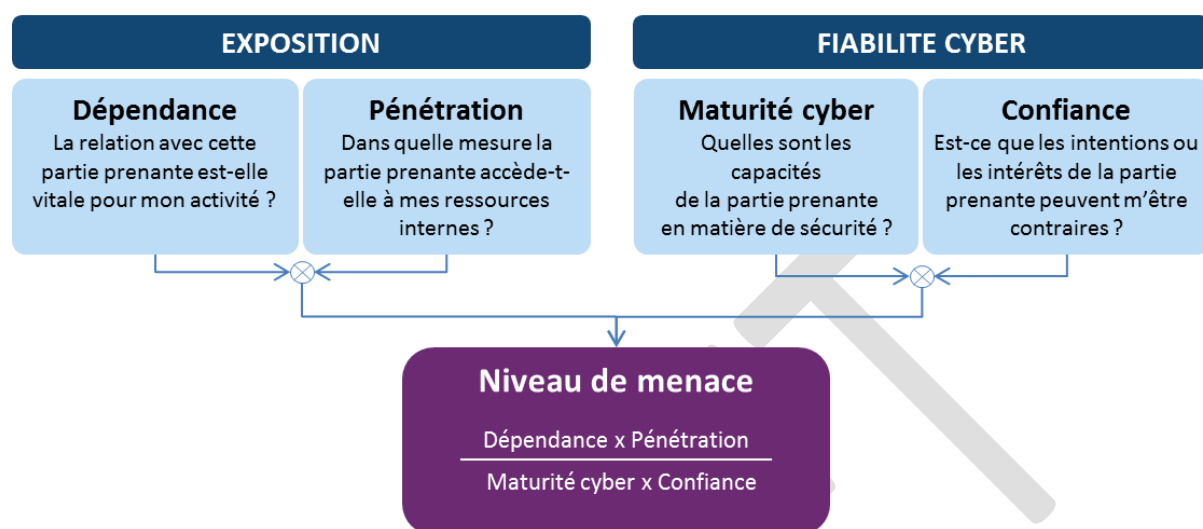
Le nombre de parties prenantes au sein de l'écosystème peut s'avérer très élevé et donc difficile à gérer. Il revient au responsable projet, avec l'aide du RSSI, de définir les catégories de parties prenantes à évaluer en priorité et ainsi effectuer une première sélection. Par exemple, le responsable projet peut choisir d'inclure dans le périmètre d'analyse uniquement certaines parties prenantes internes à l'organisation (exemple : services support, services métiers). Nous vous recommandons alors d'établir des cartographies distinctes pour les parties prenantes internes à votre organisation et celles qui lui sont externes, car les mesures de sécurité seront certainement contractualisées différemment.

Nous vous recommandons également, si cela se révèle pertinent, d'établir une cartographie des parties prenantes par phase de vie ou de mission (exemple : exploitation, maintenance), ce qui permettra d'une part de segmenter l'effort d'évaluation, et d'autre part d'identifier les parties prenantes induisant en permanence une menace vis-à-vis de l'objet de l'étude et celles qui ne représentent une menace qu'à certaines phases.

Note : les sources de risque identifiées dans l'atelier 2 ne sont pas à prendre en compte en tant que telles lors de la réalisation de cette étape. Les parties prenantes qui pourront également être considérées comme des sources de risque sont ici étudiées uniquement en tant que parties prenantes (exemple : entreprise partenaire dans le contexte étudié mais concurrente par ailleurs).

2 / Comment évaluer le niveau de menace que représentent les parties prenantes vis-à-vis de l'objet de l'étude ?

Nous proposons les critères d'évaluation ci-après. Les critères d'exposition tendent à accroître la menace alors que ceux relatifs à la fiabilité cyber l'atténuent.



Note : la formule de calcul ci-dessus est générique et vous permettra de réaliser une première évaluation. Si vous souhaitez l'affiner en fonction du contexte, vous pouvez la calibrer afin de valoriser certains critères qui vous paraissent prépondérants par rapport aux autres. Par exemple, pour exprimer une plus grande sensibilité au niveau de maturité cyber, vous pouvez pondérer le critère Maturité dans l'expression précédente. Dans le même ordre d'idée, si vous considérez qu'une partie prenante sera utilisée à ses dépens comme simple intermédiaire par un attaquant, alors le critère Confiance ne sera pas prépondérant et pourra être retiré de la formule pour cette partie prenante.

Une métrique de cotation de chaque critère est proposée ci-après. Là encore, n'hésitez pas à l'adapter au contexte de votre activité et à l'objet de l'étude.

Dépendance	Pénétration	Maturité cyber	Confiance
1 : Relation non nécessaire aux fonctions stratégiques	1 : Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, ordiphone, etc.).	1 : Des règles d'hygiène sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	1 : Les intentions de la partie prenante ne peuvent être évaluées.
2 : Relation utile aux fonctions stratégiques	2 : Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	2 : Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	2 : Les intentions de la partie prenante sont considérées comme neutres.

3 : Relation indispensable mais non exclusive	3 : Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	3 : Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	3 : Les intentions de la partie prenante sont connues et probablement positives.
4 : Relation indispensable et unique (pas de substitution possible à court terme)	4 : Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs de l'organisation.	4 : La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et prend pleinement en compte une dimension proactive.	4 : Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

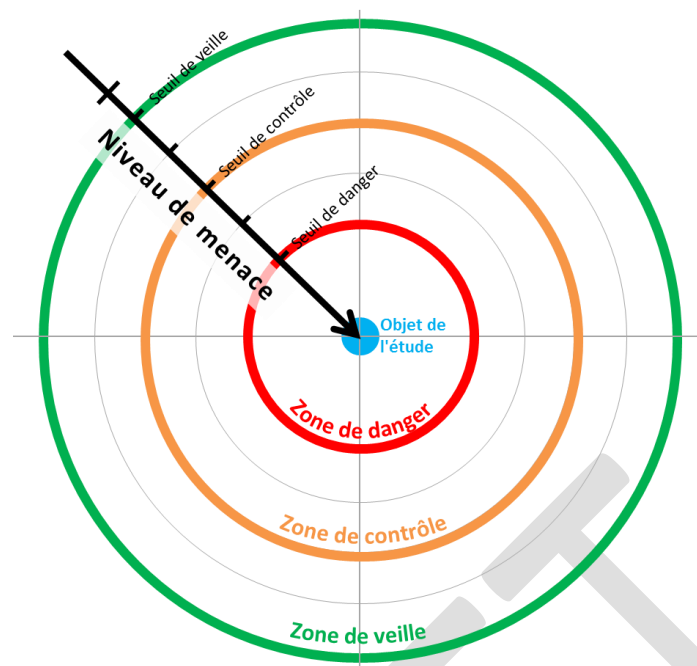
Exemple : société de biotechnologie fabriquant des vaccins.

Les parties prenantes de l'écosystème ont été évaluées selon la métrique précitée :

Catégorie	Partie prenante	Dépendance	Pénétration	Maturité	Confiance	Niveau de menace
Clients	C1 – Établissements de santé	1	1	1	3	0,3
	C2 – Pharmacies	1	1	2	3	0,2
	C3 – Dépositaires / Grossistes répartiteurs	1	2	2	3	0,3
Partenaires	P1 – Universités	2	1	1	3	0,6
	P2 – Régulateurs	2	1	2	4	0,25
	P3 – Laboratoires	3	3	2	2	2,25
Prestataires	F1 – Fournisseurs industriels chimistes	4	2	2	3	1,3
	F2 – Fournisseurs de matériel de production	4	2	2	3	1,3
	F3 – Prestataire informatique	3	4	2	2	3

3 / Quelle représentation adopter ?

La représentation radar suivante est proposée. La distance radiale correspond au niveau de menace selon l'échelle d'évaluation utilisée. Plus une partie prenante fait peser une menace numérique importante pour l'objet de l'étude, plus elle se situe près du centre.



Les parties prenantes situées dans les zones de danger et de contrôle doivent être incluses dans le périmètre d'appréciation des risques car elles risquent d'être exploitées par un attaquant. Concrètement, ces parties prenantes (dites critiques) doivent être prises en compte dans l'élaboration des scénarios stratégiques.

Zone de danger : zone pour laquelle le niveau de menace est considéré comme très élevé et difficilement acceptable. Par conséquent, aucune partie prenante ne devrait se situer dans cette zone. Les mesures de sécurité prises par la suite devraient faire sortir de cette zone les parties prenantes qui viendraient à s'y trouver.

Zone de contrôle : zone pour laquelle le niveau de menace est considéré comme élevé mais tolérable sous contrôle. Les parties prenantes qui s'y trouvent doivent faire l'objet d'une vigilance particulière (par exemple, enrôlement dans l'organisation de management du risque) et ont vocation, à moyen terme, à rejoindre une position moins menaçante au travers de mesures de réduction du risque.

Zone de veille : zone pour laquelle le niveau de menace est considéré comme faible et acceptable en l'état. Les parties prenantes qui s'y trouvent peuvent faire l'objet d'une veille sans être prises en compte dans l'élaboration des scénarios stratégiques.

Hors périmètre : les parties prenantes situées à l'extérieur de la zone de veille représentent un niveau de menace jugé négligeable. Elles ne font l'objet d'aucun traitement du risque.

4 / Comment fixer les valeurs seuil des zones de menace ?

Le choix des valeurs seuil – veille, contrôle, danger – est de la responsabilité de la gouvernance projet selon le retour d'expérience disponible, la sensibilité au risque et les ambitions visées. Le chef de projet ou le RSSI aura pour rôle d'apporter son expertise pour définir des valeurs pertinentes. Dans la pratique²², ces valeurs sont souvent définies après évaluation de l'ensemble des parties prenantes, de façon à obtenir un juste équilibre dans l'acceptation du risque lié à

l'écosystème. Il est en général plus facile d'ajuster les valeurs par différence au regard des seuils fixés de manière plus ou moins approximative, dans un premier temps. Deux méthodes sont ainsi proposées.

Seuil de danger : il pourra être fixé en référence à une partie prenante considérée comme à la limite de l'admissibilité, soit pour l'exclure, soit pour l'inclure. La détermination de ce seuil entraînera des conséquences importantes sur la politique de sécurité : celle-ci devra permettre de diminuer en-deçà du seuil de danger le risque associé ou de refuser d'établir ou maintenir l'interaction correspondante.

Seuil de contrôle : il pourra être fixé en utilisant comme référence des attaques antérieures, survenues dans un contexte comparable. La valeur de ce seuil est déterminante pour la suite de l'analyse car elle entraîne la prise en compte des parties prenantes dans l'élaboration des scénarios stratégiques.

Seuil de veille : il est moins déterminant mais définit la sensibilité relative à la prise en compte ou non de parties prenantes dans le suivi des risques résiduels.

Si vous considérez manquer de retour d'expérience et en l'absence d'arbitrage de la gouvernance projet, vous pouvez fixer vos valeurs seuil comme suit, une fois l'évaluation de l'ensemble des parties prenantes effectuée :

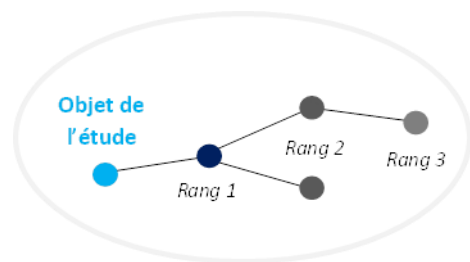
- Périètre de danger : 10% des parties prenantes de niveaux de menace les plus élevés.
- Périètre de contrôle : 40% des parties prenantes suivantes.
- Périètre de veille : 40% des parties prenantes suivantes.
- Hors périètre : les 10% restantes.

5 / Quel degré de profondeur choisir ?

En première approche et en l'absence de toute autre analyse, vous pouvez commencer par établir votre cartographie de menace en ne considérant que les parties prenantes qui interagissent directement avec l'objet étudié (partie prenante de rang 1).

Pour affiner cette analyse, considérez ensuite de façon itérative les parties prenantes de rang 2 voire de rang 3, en particulier si elles sont liées à une partie prenante de rang 1 jugée critique. Les règles suivantes peuvent vous aider à ajuster ce degré de profondeur :

- partie prenante située dans le périètre de danger : évaluation des PP connexes jusqu'au rang 3 ;
- PP située dans le périètre de contrôle : évaluation des PP connexes de rang 2 ;
- PP non critique (à l'extérieur du périètre de contrôle) : pas d'analyse plus approfondie des PP connexes.



Pour garantir une bonne lisibilité, les parties prenantes de rang 1 seront représentées en priorité sur la cartographie radar. Les parties prenantes de rangs 2 et 3 pourront éventuellement apparaître selon leur niveau de menace.

Fiche méthode n°6 : Définir des mesures de sécurité pour l'écosystème (Atelier 3)

Selon le niveau de menace d'une partie prenante vis-à-vis de l'objet de l'étude, des mesures de sécurité pourront être mises en place. Le jeu de règles suivant peut ainsi être adopté, le critère d'entrée étant le niveau de menace évalué pour la partie prenante :

Niveau de menace	Acceptabilité	Recommandations d'actions
Très élevé – Zone de danger	Inacceptable	Aucune partie prenante dans cette zone : réduction du risque, ou refus d'établir l'interaction.
Elevé – Zone de contrôle	Tolérable sous contrôle	Enrôlement de la partie prenante dans le processus de management du risque : <ul style="list-style-type: none">- surveillance particulière, voire accrue, en termes de cyberdéfense ;- audit de sécurité technique et organisationnel ;- réduction/transfert du risque dans le cadre d'un plan d'amélioration continue de la sécurité.
Faible – Zone de veille	Acceptable en l'état	Sans objet (menace résiduelle)

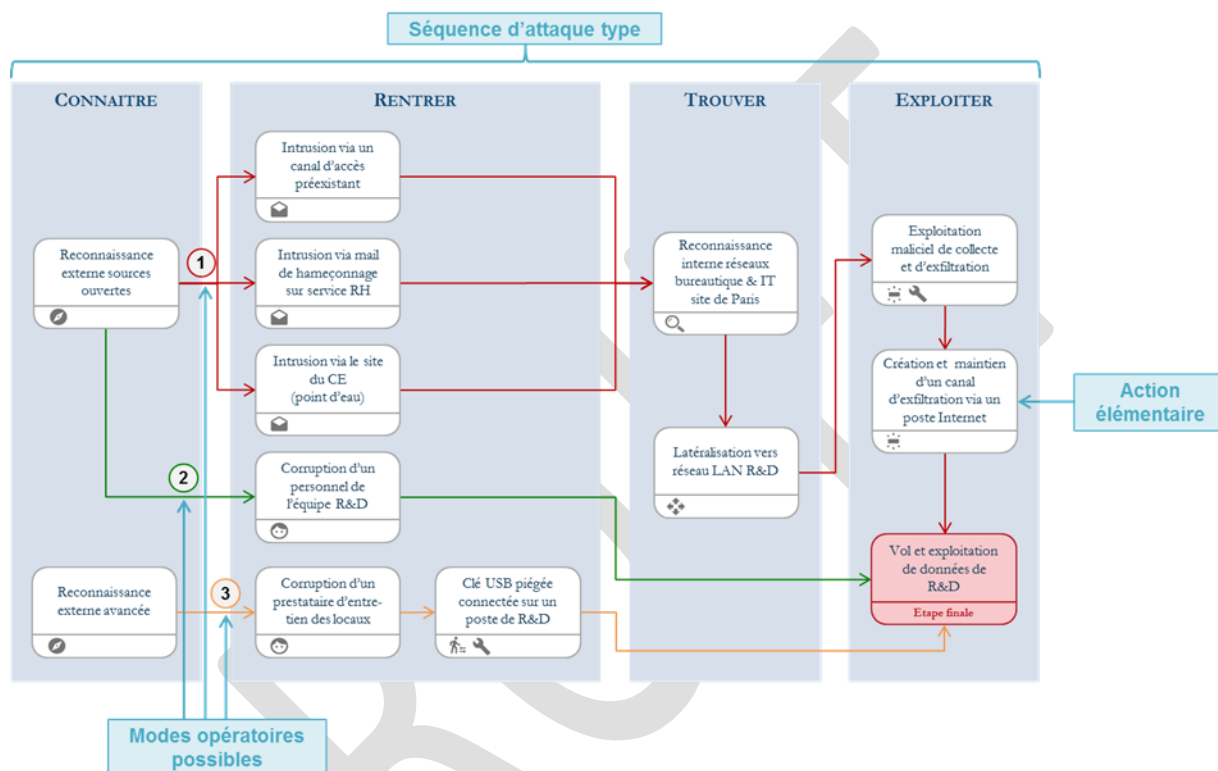
Vous pouvez définir une première orientation en proposant un critère sur lequel agir en priorité (par exemple : augmenter la confiance ou la maturité, diminuer la pénétration ou la dépendance). Ces orientations sont guidées notamment par les considérations suivantes :

- choix du critère le plus pénalisant dans la situation initiale ;
- choix du critère pour lequel une amélioration sera obtenue à moindre coût ;
- choix du critère le plus efficace *a priori* au vu des scénarios stratégiques identifiés.

Vous pouvez nuancer le jeu de règles ci-dessus pour les parties prenantes qui se trouvent dans la zone de danger, particulièrement s'il apparaît très difficile de les faire sortir de cette zone compte tenu de contraintes opérationnelles (par exemple : *une partie prenante pourra être tolérée dans la zone de danger seulement si ses niveaux de maturité et de confiance sont au moins de 3*).

Fiche méthode n°7 : Construire des graphes d'attaque (Atelier 4)

Un scénario opérationnel peut être représenté sous la forme d'un graphe d'attaque permettant de visualiser les modes opératoires planifiés par l'attaquant pour atteindre son objectif. Le graphe d'attaque se présente sous la forme d'un **enchaînement d'actions élémentaires sur des biens supports**. Plusieurs modes opératoires peuvent être réalisés par la source de risque pour atteindre son objectif visé : ils sont représentés par des chaînes séquentielles différentes avant d'atteindre l'étape finale. Un exemple de scénario opérationnel est donné ci-après.



1 / Modèle de séquence d'attaque type

Les scénarios opérationnels peuvent être structurés selon une séquence d'attaque type. Le modèle proposé s'articule autour de 4 phases :

- **CONNAITRE** : ensemble des activités de ciblage, de reconnaissance et de découverte *externes* menées par l'attaquant pour préparer son attaque et accroître ses chances de succès (cartographie de l'écosystème, recherche d'information sur les personnes et les systèmes clés, recherche et évaluation de vulnérabilités, etc.). Ces informations sont collectées par tous les moyens possibles selon la détermination et les ressources de l'attaquant : renseignement, intelligence économique, exploitation des réseaux socio-professionnels, approches directes, officines spécialisées pour obtenir de l'information inaccessible en source ouverte, etc.
- **RENTRER** : ensemble des activités menées par l'attaquant pour s'introduire numériquement ou physiquement, soit directement et frontalement dans le système d'information de la cible, soit dans son écosystème en vue d'une attaque par rebond. L'intrusion se fait généralement via des biens supports « de frontière » qui servent de

points d'entrée du fait de leur exposition (exemple : poste utilisateur connecté à Internet, tablette de maintenance d'un prestataire, imprimante télé-maintenue, etc.).

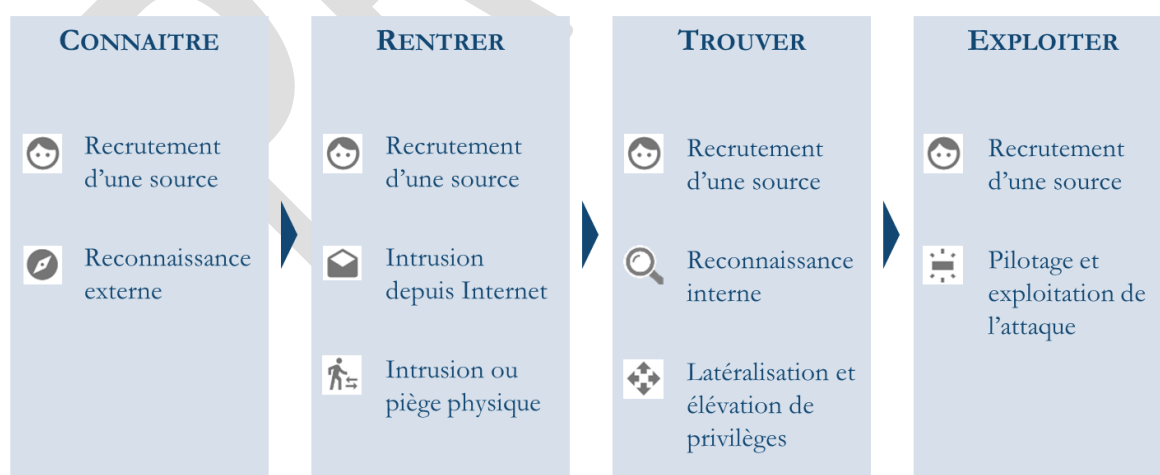
- **TROUVER** : ensemble des activités de reconnaissance *interne* des réseaux et systèmes, de latéralisation, d'élévation de privilèges, et de persistance, qui permettent à l'attaquant de localiser les données et biens supports recherchés. Lors de cette phase, l'attaquant cherche généralement à rester discret et à effacer ses traces.
- **EXPLOITER** : ensemble des activités d'exploitation des données et biens supports trouvés dans l'étape précédente. Par exemple, dans le cas d'une opération de sabotage, cette phase inclut le déclenchement de la charge active (exemple : rançongiciel), dans le cas d'une opération d'espionnage visant à exfiltrer des mails, il peut s'agir de mettre en place et maintenir la capacité discrète de recueil et d'exfiltration des données.

Vous pouvez adopter des modèles de séquences d'attaque plus sophistiqués et les décliner en variantes selon la technique d'attaque de la source de risque pour atteindre son objectif (exfiltration d'information, écoute passive, déni de service, rançongiciel, etc.).

Note : pour la phase « Rentrer », nous vous recommandons de distinguer dans le séquençement les actions élémentaires pour s'introduire dans les systèmes d'information de l'écosystème, et celles portant sur les biens supports de l'objet de l'étude. S'agissant de l'écosystème, vous ne pourrez pas toujours décrire avec précision quels seront les biens supports ciblés chez la partie prenante concernée. Dans ce cas, restez à un niveau de description macroscopique et fonctionnel (exemple : SI bureautique, chaîne de production).

2 / Catégories d'actions élémentaires et moyens usuellement mis en œuvre

L'illustration ci-après propose une catégorisation d'actions élémentaires en lien avec le modèle de séquence d'attaque proposé précédemment. Les moyens et techniques couramment observés sont précisés pour chaque catégorie d'actions élémentaires (en italique). N'hésitez pas à adapter cette base à votre contexte et à l'enrichir de toute information issue de vos activités de veille (exemple : exploitation des bulletins du CERT-FR et des bulletins de veille des cyberattaques).



Note : Dans certains cas, lorsqu'un canal d'exfiltration est nécessaire et diffère du canal d'infiltration, une intrusion depuis Internet ou par piège physique peut être réalisée dans la phase « Exploiter ». L'intrusion initiale peut par exemple être réalisée via Internet, mais l'exfiltration via un canal physique ad hoc mis en place (cas des systèmes isolés).



Recrutement d'une source, corruption de personnel

Une opération de « recrutement » d'une source à l'intérieur de l'organisation ou y ayant accès peut être longue et complexe, mais très utile pour mettre en place un piège matériel ou fournir de l'information sur le système d'information ciblé. Les raisons poussant une cible à trahir son entité d'origine – potentiellement à son insu – sont couvertes par quatre grandes catégories, dites « MICE » (*Money, Ideology, Compromission, Ego*). Des officines spécialisées en matière de recrutement de sources existent.



Reconnaissance externe de la cible

Lors de la phase de reconnaissance, la source de risque va rechercher dans l'ensemble de ses bases disponibles les informations nécessaires à la planification de son attaque. Les données collectées peuvent être de nature technique ou concerner l'organisation de la cible et de son écosystème. Les moyens employés peuvent être très variés :

- *Réseaux sociaux (social engineering) ;*
- *Internet (poubelles numériques, sites) ;*
- *Forums de discussion sur Internet ;*
- *Forums et salons professionnels ;*
- *Faux client, faux journaliste, etc. ;*
- *Prise de contact directe (anciens salariés, etc.) ;*
- *Officines ou agences spécialisées (sources non ouvertes) ;*
- *Renseignement d'origine électromagnétique (interceptions).*



Intrusion depuis Internet ou des réseaux informatiques tiers

L'intrusion initiale a pour objectif d'introduire un outil malveillant dans le système d'information ciblé ou dans un autre appartenant à l'écosystème (par exemple la chaîne d'approvisionnement – *supply chain*), en général au niveau d'un bien support d'entrée plus particulièrement exposé. Idéalement pour l'attaquant, l'intrusion initiale de l'outil malveillant est réalisée depuis Internet. Les techniques et vecteurs d'intrusion les plus couramment utilisés sont :

- *les attaques directes à l'encontre des services exposés sur Internet ;*
- *les mails d'hameçonnage (phishing) ou de harponnage (spearfishing) ;*
- *les attaques via des serveurs spécifiquement administrés à cet effet ou compromis (attaques dites par point d'eau ou waterhole) ;*
- *le piège d'une mise à jour légitime d'un logiciel ou d'un firmware.*



Intrusion ou piège physique

Cette méthode d'intrusion est utilisée pour accéder physiquement à des ressources du système d'information afin de le compromettre. Elle peut être réalisée par une personne externe ou simplifiée par le recrutement d'une source interne à l'organisation ciblée. L'intrusion physique est notamment utile à l'attaquant qui souhaite accéder à un système isolé d'Internet, ce qui nécessite de franchir un ou plusieurs *air gaps*. Des techniques d'intrusion physique couramment utilisées sont données ci-après.

- *Connaissance des identifiants de connexion ;*
- *Compromission de la machine (ex : clé USB piégée) ;*
- *Connexion au réseau d'un matériel externe au système d'information ;*
- *Intrusion via un réseau sans fil mal sécurisé ;*
- *Piège d'un matériel en amont via la chaîne d'approvisionnement (attaque dite de la supply chain) ;*
- *Utilisation abusive de moyens d'accès légitimes au système d'information (ex : vol et utilisation du téléphone portable professionnel d'un personnel).*



Reconnaissance interne

En général, à l'issue de l'intrusion initiale, l'attaquant se retrouve dans un environnement de type réseaux locaux dont les accès peuvent être contrôlés par des mécanismes d'annuaires (*Active Directory*, *OpenLDAP*, etc.). De fait, il doit mener des activités de reconnaissance interne lui permettant de cartographier l'architecture réseau, identifier les mécanismes de protection et de défense mis en place, recenser les vulnérabilités exploitables, etc. Lors de cette étape, l'attaquant cherche à localiser les services, informations et biens supports, objets de l'attaque. Les techniques de reconnaissance interne ci-après sont largement utilisées.

- *Cartographie des réseaux et systèmes pour mener la propagation (scan réseau) ;*
- *Cartographie avancée (exemple : dump mémoire) ;*
- *Recherche de vulnérabilités (par exemple pour faciliter la propagation) ;*
- *Accès à des données système critiques (plan d'adressage, coffres forts, mots de passe, etc.) ;*
- *Cartographie des services, bases de données et biens supports d'intérêt pour l'attaque ;*
- *Dissimulation des traces ;*
- *Utilisation de maliciel générique ou à façon permettant d'automatiser la reconnaissance interne.*



Latéralisation et élévation de privilèges

À partir de son point d'accès initial, l'attaquant va mettre en œuvre des techniques de latéralisation et d'élévation de privilèges afin de progresser et de se maintenir dans le système d'information. Il s'agit généralement pour l'attaquant d'exploiter les vulnérabilités structurelles internes du système (manque de cloisonnement des réseaux, contrôle d'accès insuffisant, politique d'authentification peu robuste, négligences relatives à l'administration et à la maintenance du système d'information, absence de supervision, etc.).

- *Exploitation de vulnérabilités logicielles ou protocolaires (notamment identifiées lors de la reconnaissance) ;*

- *Modification ou abus de droits sur des comptes clés utilisateurs, administrateurs, machines ;*
- *Autres techniques spécifiques : attaque par force brute, dump mémoire, attaque « pass-the-hash ».*

Note : les phases de reconnaissance interne et de latéralisation / élévation de privilèges sont en pratique itératives et interviennent au fur et à mesure que l'attaquant progresse dans le système d'information.



Pilotage et exploitation de l'attaque

Cette étape finale correspond à la réalisation de l'objectif visé par la source de risque. Selon cet objectif, il peut par exemple s'agir de déclencher la charge malveillante destructrice, d'exfiltrer ou de modifier de l'information. L'attaque peut être ponctuelle (par exemple dans le cas d'une opération de sabotage), ou durable et se réaliser en toute discrétion (par exemple dans le cas d'une opération d'espionnage visant à régulièrement exfiltrer des informations). Les moyens et techniques d'exploitation d'une attaque vont dépendre de l'objectif visé. Dans le cas où celui-ci perdure dans le temps et nécessite d'être orienté, l'attaquant devra mettre en place un canal de pilotage, qu'il soit synchrone ou asynchrone, voire même physique dans le cas d'un *air gap*.

Ci-après quelques exemples de techniques d'exploitation utilisées selon l'objectif visé :

Espionnage

- *Exfiltration de données ;*
- *Observation ou écoute passive à distance (drone, matériel d'écoute, etc.) ;*
- *Interception et exploitation de signaux parasites compromettants (menace TEMPEST)³.*

Entrave au fonctionnement (sabotage, neutralisation)

- *Attaque par déni de service distribué ;*
- *Atteinte à l'intégrité d'un bien support ou d'une donnée (effacement, chiffrement, altération) ;*
- *Brouillage d'un bien support (pour rendre aveugle ou neutraliser) ;*
- *Leurre d'un bien support (pour tromper ou falsifier)⁴ ;*
- *Systèmes industriels : envoi de commandes à risque pour la sûreté de fonctionnement⁵ ;*
- *Agression électromagnétique intentionnelle (AGREMI).*

Lucratif (fraude, détournement d'usage, falsification)

- *Modification d'une base de données (par exemple pour dissimuler une activité frauduleuse) ;*
- *Altération ou détournement d'usage d'une application métier ou support ;*
- *Usurpation d'identité (dans une logique d'abus de droits) ;*
- *Détournement ou extorsion d'argent (exemple : rançongiciel, mineur de crypto monnaie) ;*

³ La menace TEMPEST peut être également exploitée de façon active en piégeant préalablement, par exemple via la *supply chain*, un périphérique (câble, clavier, souris, vidéoprojecteur) qui devient alors une source de SPC activable et désactivable à distance par des émetteurs suffisamment puissants, ce qui permet de créer un canal de fuite.

⁴ Inclut les techniques de leurre cognitif en vue d'induire en erreur ou dissimuler une activité aux yeux d'un utilisateur (ex : fausse mire d'authentification pour tromper un utilisateur, masquage d'un message d'alerte).

⁵ Par exemple pour entraîner une usure prématurée d'un équipement ou modifier des seuils d'alerte sur des paramètres de fonctionnement clés. L'évaluation fine des modes d'exploitation d'une attaque sur un système industriel est indissociable des analyses de sûreté de fonctionnement.

- *Pourriel à des fins commerciales.*

Influence (agitation, propagande, déstabilisation)

- *Défiguration de sites Internet ;*
- *Diffusion de messages idéologiques via la prise de contrôle d'un canal d'information ;*
- *Usurpation d'identité (dans une logique d'atteinte à la réputation).*

PROJET

Fiche méthode n°8 : Évaluer la vraisemblance des scénarios opérationnels (Atelier 4)

La vraisemblance d'un scénario opérationnel reflète le degré de faisabilité ou de possibilité que l'un des modes opératoires de l'attaquant aboutisse à l'objectif visé. La vraisemblance est un indicateur d'aide à la décision. Combinée à la gravité, elle permet d'estimer le niveau de risque et de déduire la stratégie de traitement du risque.

1 / Quelle échelle de vraisemblance utiliser ?

Une échelle de niveaux de vraisemblance doit être comprise et utilisable par les personnes chargées d'évaluer la possibilité qu'un risque se concrétise. Son élaboration peut utilement être réalisée en collaboration avec les personnes qui vont estimer ces niveaux : ainsi les valeurs auront une signification concrète et seront cohérentes.

Si vous ne disposez pas d'échelle de vraisemblance, établissez-en une au début de l'atelier 4. Pour ce faire, vous pouvez **utiliser et adapter l'échelle générique** ci-après.

Échelle de vraisemblance d'un scénario opérationnel	
Niveau de l'échelle	Description
V4 – Quasi-certain	La source de risque va très certainement atteindre son objectif visé empruntant un des modes opératoires envisagés. La vraisemblance du scénario de risque est très élevée.
V3 – Très vraisemblable	La source de risque va probablement atteindre son objectif visé en empruntant un des modes opératoires envisagés. La vraisemblance du scénario de risque est élevée.
V2 – Vraisemblable	La source de risque est susceptible d'atteindre son objectif visé en empruntant un des modes opératoires envisagés. La vraisemblance du scénario de risque est significative.
V1 – Peu vraisemblable	La source de risque a relativement peu de chances d'atteindre son objectif visé en empruntant un des modes opératoires envisagés. La vraisemblance du scénario de risque est faible.
V0 – Invraisemblable	La source de risque a très peu de chances d'atteindre son objectif visé en empruntant un des modes opératoires envisagés. La vraisemblance du scénario de risque est très faible.

Note : l'estimation de la vraisemblance d'un scénario opérationnel n'a pas vocation à être prédictive

(elle ne traduit pas la probabilité que la source de risque réalisera son attaque selon ce scénario⁶). Par contre, si l'attaquant décide de mener son attaque via le mode opératoire concerné, alors sa vraisemblance de réussite sera celle estimée.

Le recours à une échelle à 4 ou 5 niveaux est guidé par les considérations suivantes :

- la cohérence du nombre de niveaux entre les échelles de gravité et de vraisemblance (si vous utilisez une échelle de gravité à 4 niveaux, utilisez une échelle de vraisemblance à 4 niveaux) ;
- la nécessité d'estimer des vraisemblances plus ou moins finement.

2 / Quelle approche choisir pour coter la vraisemblance du scénario opérationnel ?

Vous pouvez envisager trois approches pour coter la vraisemblance du scénario opérationnel :

- Méthode expresse : cotation directe de la vraisemblance du scénario ;
- Méthode standard : cotation de la « probabilité de succès » de chaque action élémentaire du scénario, du point de vue de l'attaquant.
- Méthode avancée : en plus de la « probabilité de succès », cotation de la « difficulté technique » de chaque action élémentaire du scénario, du point de vue de l'attaquant.

Note : ici la « probabilité » ne doit pas être entendue au sens mathématique du terme.

a) Méthode expresse : cotation directe de la vraisemblance globale du scénario

Dans les méthodes présentées ci-après (standard et avancée), on évalue la vraisemblance globale du scénario à partir de la cotation des actions élémentaires. La méthode expresse consiste à évaluer directement la vraisemblance globale du scénario, sur la base de considérations générales relatives à la source de risque (motivations, ressources) et à la sécurité des biens supports ciblés dans le scénario (exposition, vulnérabilités). La section « *Comment coter les actions élémentaires ?* » sera une aide précieuse pour l'appréciation. Il est possible de considérer séparément les modes opératoires envisagés dans le scénario opérationnel et d'identifier celui qui semble être le plus vraisemblable.

Dans cette approche, vous pouvez :

- soit estimer directement le niveau de vraisemblance du scénario ;
- soit coter sa probabilité de succès et sa difficulté technique, et en déduire par croisement la vraisemblance du scénario selon la matrice type présentée ci-dessous.

⁶ A contrario, si ce scénario a été sélectionné après les ateliers 2 et 3, c'est qu'il est considéré comme pertinent.

		Difficulté technique du scénario opérationnel				
		0 – Négligeable	1 – Faible	2 – Modérée	3 – Élevée	4 – Très élevée
Probabilité de succès du scénario opérationnel	4 – Quasi-certaine	4	4	3	2	1
	3 – Très élevée	4	3	3	2	1
	2 – Significative	3	3	2	2	1
	1 – Faible	2	2	2	1	0
	0 – Très faible	1	1	1	0	0

b) Méthode standard : probabilité de succès des actions élémentaires

Dans la méthode standard, vous allez coter chaque action élémentaire selon un indice de probabilité de succès vu de l'attaquant. L'échelle suivante peut être adoptée, les pourcentages de chance sont mentionnés à titre indicatif pour faciliter la cotation :

Échelle de probabilité de succès d'une action élémentaire		
Niveau de l'échelle	Description	
4 – Quasi-certaine	Probabilité de succès quasi-certaine	> 90%
3 – Très élevée	Probabilité de succès très élevée	> 60%
2 – Significative	Probabilité de succès significative	> 20%
1 – Faible	Probabilité de succès faible	< 20%
0 – Très faible	Probabilité de succès très faible	< 3%

Par exemple, un indice de « 3 – Très élevée » pour une action élémentaire d'intrusion par mail piégé (*spearfishing*) signifiera que vous estimez que l'attaquant a de très fortes chances de réussir son action, c'est-à-dire que l'un des utilisateurs ciblés par la campagne de *spearfishing* clique sur la pièce jointe piégée.

Note : les échelles de cotation des actions élémentaires doivent avoir autant de niveaux que l'échelle de vraisemblance.

c) Méthode avancée : probabilité de succès et difficulté technique des actions élémentaires

Dans la méthode avancée, vous allez également coter la difficulté technique de réalisation de l'action élémentaire, du point de vue de l'attaquant. Elle permet d'estimer les ressources que l'attaquant devra engager pour mener son action et accroître ses chances de réussite. L'échelle suivante peut être adoptée :

Échelle de difficulté technique d'une action élémentaire	
Niveau de l'échelle	Description
4 – Très élevée	Difficulté très élevée : l'attaquant engagera des ressources très importantes pour mener à bien son action.
3 – Élevée	Difficulté élevée : l'attaquant engagera des ressources importantes pour mener à bien son action.
2 – Modérée	Difficulté modérée : l'attaquant engagera des ressources significatives pour mener à bien son action.
1 – Faible	Difficulté faible : les ressources engagées par l'attaquant seront faibles.
0 – Négligeable	Difficulté négligeable, voire nulle : les ressources engagées par l'attaquant seront négligeables ou déjà disponibles.

Notes :

- *La méthode avancée permet une appréciation plus fine de la vraisemblance : elle prend en compte le niveau d'expertise et de ressources dont l'attaquant aura besoin pour mener son attaque, compte-tenu de la sécurité du système cible. De fait, cette méthode permet de considérer le retour sur investissement pour l'attaquant et donc de bâtir une stratégie de traitement du risque pilotée par une logique de découragement.*
- *Les critères de cotation « difficulté technique » et « probabilité de succès » ne sont pas rigoureusement indépendants. Néanmoins, la « difficulté technique » est plus particulièrement liée au niveau de protection de la cible (son exposition et ses vulnérabilités), alors que la « probabilité de succès » est davantage influencée par son niveau de défense et de résilience (capacités de supervision, de réaction en cas d'incident et de continuité d'activité).*

3 / Méthodes standard et avancée : comment coter les actions élémentaires ?

La cotation des actions élémentaires n'est pas forcément aisée. En effet, elle doit prendre en compte et confronter :

- d'une part la motivation/détermination et les ressources/capacités de la source de risque ;
- d'autre part la sécurité du système ciblé au sein de son écosystème.

La cotation peut être effectuée par jugement d'expert, ce qui implique de disposer dans le groupe de travail d'une expertise suffisante en cyber-attaques et d'une connaissance fine du niveau de sécurité de l'objet de l'étude au sein de son écosystème. Pour vous aider dans ce travail de cotation et le rendre plus objectif et reproductible, vous trouverez en fin de fiche les principaux critères pour déterminer la probabilité de succès ou la difficulté technique d'une action élémentaire.

4 / Méthodes standard et avancée : comment calculer la vraisemblance du scénario opérationnel ?

a) Méthode standard

Vous avez coté dans l'étape précédente chaque action élémentaire selon un indice de probabilité de succès. Vous pouvez évaluer l'indice global de probabilité de succès du scénario en appliquant la règle suivante. Le principe est de progresser dans un mode opératoire en évaluant de proche en proche à chaque action élémentaire « AE_n » d'un nœud « n », un indice de probabilité cumulé intermédiaire à partir de l'indice élémentaire de « AE_n » et des indices cumulés intermédiaires du nœud précédent « n-1 » :

$$\text{Indice_Pr}_{\text{cumulé intermédiaire}}(AE_n) = \text{Min} \left\{ \text{Indice_Pr}(AE_n), \text{Max}_{\text{cumulés intermédiaires}}(\text{Indices_Pr}(AE_{n-1})) \right\}$$

L'indice global de probabilité de succès (étape finale) est obtenu en prenant l'indice de probabilité cumulé intermédiaire le plus élevé parmi les modes opératoires qui aboutissent à l'étape finale. Il correspond au(x) mode(s) opératoire(s) dont la chance de succès paraît la plus élevée.

Note : la règle de calcul ci-dessus permet une évaluation relativement simple et rapide de l'indice global de probabilité de succès. Elle trouve toutefois ses limites lorsqu'une séquence d'un mode opératoire comporte une longue chaîne d'étapes en série (environ une dizaine à titre indicatif)⁷ : l'évaluation aura alors tendance à surestimer la probabilité de succès du mode opératoire correspondant, aboutissant à une vraisemblance surestimée du scénario opérationnel. Pour les séquences de mode opératoire concernées, vous pouvez compenser cette limite en diminuant d'un niveau l'indice de probabilité cumulé intermédiaire obtenu en bout de séquence.

La **vraisemblance du scénario opérationnel** obtenue à l'issue de ces opérations correspond à l'indice global de probabilité de succès.

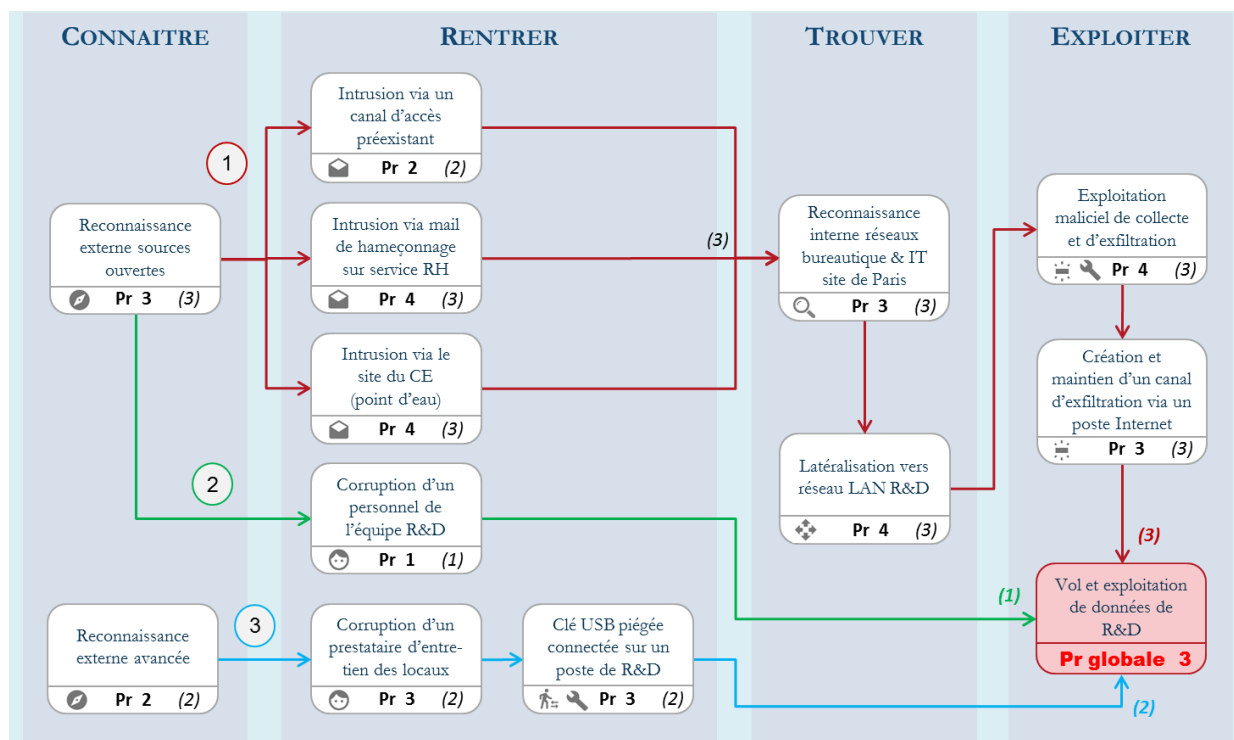
Exemple : société de biotechnologie fabriquant des vaccins.

L'évaluation de la vraisemblance a été réalisée avec des échelles à 4 niveaux :

- Pour la probabilité de succès : « Pr 1 » – probabilité faible à « Pr 4 » – quasi-certaine.
- Pour la vraisemblance : « V1 » – peu vraisemblable à « V4 » – quasi-certain.

Les indices de probabilité cumulés intermédiaires sont indiqués entre parenthèses et en *italique*.

⁷ Particulièrement si les actions élémentaires correspondantes ont des indices de probabilité de succès identiques.



L'indice global de probabilité de succès du scénario est estimé à « 3 – Très élevé » : l'atteinte de l'objectif visé par la source de risque selon l'un ou l'autre des modes opératoires du scénario opérationnel est considérée comme **très vraisemblable (V3)**. Le mode opératoire le plus facile ou faisable étant le rouge numéroté ①.

b) Méthode avancée

Commencez par calculer l'indice global de probabilité de succès de *chaque mode opératoire* du scénario opérationnel selon la démarche exposée précédemment.

Calculez ensuite l'indice de difficulté technique de chaque mode opératoire selon les modalités ci-après. Le principe est de progresser sur une séquence d'un mode opératoire en évaluant de proche en proche à chaque action élémentaire « AE_n » d'un nœud « n », un indice de difficulté cumulé intermédiaire à partir de la difficulté élémentaire de « AE_n » et des difficultés cumulées intermédiaires du nœud précédent « n-1 » :

$$\text{Indice_Diff}_{\text{cumulé intermédiaire}}(AE_n) = \text{Max} \left\{ \text{Indice_Diff}(AE_n), \text{Min}(\text{Indices_Diff}_{\text{cumulés intermédiaires}}(AE_{n-1})) \right\}$$

Note : la règle de calcul ci-dessus permet une évaluation relativement simple et rapide de l'indice global de difficulté technique. Elle trouve toutefois sa limite lorsqu'une séquence d'un mode opératoire comporte une longue chaîne d'étapes en série (environ une dizaine)⁸ : l'évaluation aura alors tendance à sous-estimer la difficulté du mode opératoire correspondant, aboutissant à une vraisemblance sous-estimée du scénario opérationnel. Pour les séquences de mode opératoire concernées, vous pouvez compenser cette limite en augmentant d'un niveau l'indice de difficulté cumulé intermédiaire obtenu en bout de séquence.

⁸ Particulièrement si les actions élémentaires correspondantes ont des indices de difficulté identiques.

Enfin, déduisez la vraisemblance globale du scénario opérationnel en procédant comme suit⁹ :

- évaluez le niveau de vraisemblance de chaque mode opératoire aboutissant à l'étape finale, en utilisant la grille croisée ci-après (qui peut être adaptée) ;
- le niveau de vraisemblance pour le scénario opérationnel est celui du mode opératoire le plus vraisemblable ;
- ce niveau de vraisemblance peut être ensuite pondéré selon la nature de la source de risque (motivation et ressources). Si vous estimez que celle-ci sera particulièrement déterminée à atteindre son objectif – et donc prête à solliciter des moyens conséquents et à persévérer en cas d'échecs successifs, alors vous pouvez décider d'augmenter d'un niveau la vraisemblance obtenue.

		Difficulté technique du mode opératoire				
		0 – Négligeable	1 – Faible	2 – Modérée	3 – Élevée	4 – Très élevée
Probabilité de succès du mode opératoire	4 – Quasi-certaine	4	4	3	2	1
	3 – Très élevée	4	3	3	2	1
	2 – Significative	3	3	2	2	1
	1 – Faible	2	2	2	1	0
	0 – Très faible	1	1	1	0	0

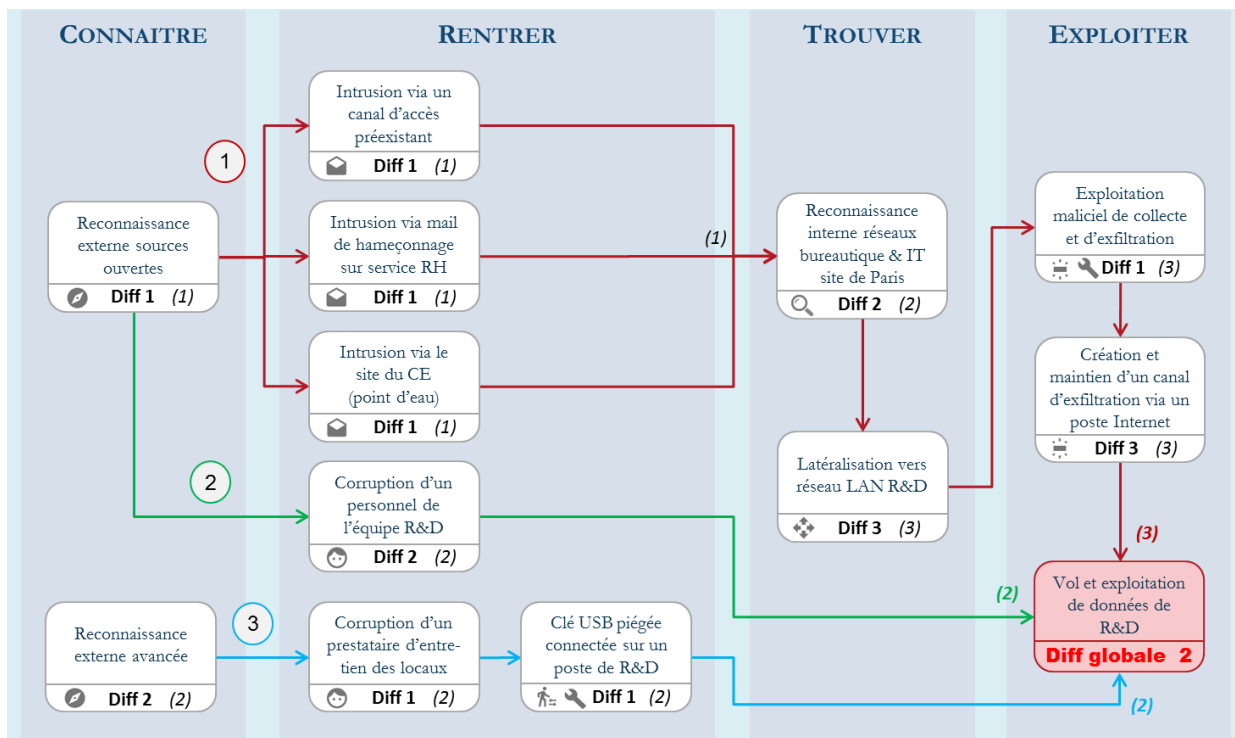
Notes :

- Le modèle suppose les probabilités de succès indépendantes entre-elles, ce qui n'est pas nécessairement vrai. La même remarque s'applique pour les difficultés techniques. D'autre part, pour certaines catégories d'actions (telle que la corruption d'un membre du personnel), la probabilité de succès peut être dépendante de la difficulté, ce qui n'est pas capturé par défaut dans le modèle.
- L'utilisation d'un logiciel de construction et de cotation de graphes d'attaque est fortement recommandée.

Exemple : société de biotechnologie fabriquant des vaccins.

Les indices de difficulté cumulés intermédiaires sont indiqués entre parenthèses et en *italique*.

⁹ Vous pourriez également retenir comme vraisemblance celle obtenue en croisant l'indice global de probabilité de succès et l'indice global de difficulté technique obtenus. Mais votre résultat pourrait être faussé en cas de croisement des indices de probabilité et de difficulté relatifs à des modes opératoires différents. Dans ce cas la vraisemblance du scénario opérationnel serait surestimée.










La difficulté technique du scénario est estimée globalement à « 2 – Modéré », les modes opératoires les moins difficiles techniquement étant ceux numérotés ② et ③. Compte-tenu des probabilités de succès évaluées précédemment, il est possible d'établir la synthèse suivante :


	Probabilité succès	Difficulté technique	Vraisemblance
Chemin ①	3 – Très élevée	3 – Élevée	V2 – Vraisemblable
Chemin ②	1 – Faible	2 – Modérée	V2 – Vraisemblable
Chemin ③	2 – Significative	2 – Modérée	V2 – Vraisemblable
Scénario global			V2 – Vraisemblable

Les trois modes opératoires envisagés dans le graphe d'attaque ont le même niveau de vraisemblance. On aboutit à une vraisemblance « **V2 – Vraisemblable** » pour le scénario. Par rapport à l'évaluation réalisée avec la méthode standard (V3), la vraisemblance estimée est moindre : la prise en compte du critère de difficulté technique apporte une pondération sur l'estimation du niveau de vraisemblance. En effet, si le mode opératoire ① apparaît comme ayant la probabilité de succès la plus élevée, il présente également une difficulté technique relativement élevée.

5 / Éléments d'aide pour la cotation des actions élémentaires

Catégories d'actions élémentaires	Éléments majeurs déterminant la probabilité de succès ou la difficulté technique des actions
 <p>Recrutement d'une source</p>	<ul style="list-style-type: none"> - Nombre de cibles potentielles ayant accès aux informations visées, aux biens supports critiques ou à leur environnement physique (Note 1) - Personnels, prestataires, fournisseurs susceptibles d'être animés par un esprit de vengeance (exemple : salarié mécontent licencié récemment) - Personnels ayant fait l'objet d'un processus d'habilitation de sécurité et/ou d'une enquête, lequel apporte un certain niveau d'assurance sur leur intégrité - Satisfaction des cibles au sujet de leur salaire ou de leur considération au sein de l'organisation - Adhésion des cibles potentielles aux valeurs de l'entreprise (Note 2)
 <p>Reconnaissance externe</p>	<ul style="list-style-type: none"> - Informations sur l'entité et son écosystème facilement accessibles sur Internet (sites web, forums de discussions en ligne, réseaux socio-professionnels, etc.) - Participation régulière de l'entité, de ses partenaires (fournisseurs, sous-traitants, clients) ou d'anciens salariés à des salons professionnels ou forums en ligne (Note 3) - Usage du chiffrement dans les relations de l'entité avec l'extérieur, dans les services offerts par l'entité à l'extérieur (Note 4) - Compétences particulières nécessaires pour la recherche des informations, compte-tenu du domaine d'activité de l'entité (Note 5)
 <p>Intrusion depuis Internet</p>	<p>Les critères diffèrent selon la technique d'intrusion utilisée par l'attaquant.</p> <p><u>Attaque frontale de services</u></p> <ul style="list-style-type: none"> - Nombre de services et/ou d'applicatifs exposés sur Internet - Services exposés ayant fait l'objet d'une homologation ou d'un processus de développement intégrant la sécurité - Technologie de filtrage mise en place (exemple : reverse proxy, waf...) (Note 6) - Utilisation de biens supports « de frontière » certifiés ou qualifiés (Note 7) <p><u>Hameçonnage / Point d'eau</u></p> <ul style="list-style-type: none"> - Nombre d'utilisateurs pouvant être visés (Note 8) - Utilisateurs régulièrement sensibilisés et formés à réagir aux attaques par hameçonnage et point d'eau - Filtre anti-spam performant mis en place (Note 9) - Capacité de filtrage de la navigation Internet des utilisateurs mise en place (exemple : proxy, IPS) (Note 10) - Filtrage des sites Internet reposant sur une liste blanche (liste de sites autorisés) (Note 11) <p><u>Intrusion via un réseau sans fil</u></p> <ul style="list-style-type: none"> - Existence de réseaux sans fil (Wi-Fi) dans l'environnement bureautique ou industriel de l'entité - Accès Wi-Fi sécurisés, par exemple selon le guide de recommandations de l'ANSSI <p><u>Intrusion via un logiciel ou un correctif légitime</u></p> <ul style="list-style-type: none"> - Existence d'une politique de sécurité relative aux mises à jour des logiciels, applications métier et <i>firmware</i> (Note 12) - Sources et canaux de confiance (voire certifiés ou qualifiés), vérification de l'identité des signataires pour les mises à jour

 <p>Intrusion ou piège physique</p>	<ul style="list-style-type: none"> - Maîtrise des interventions des prestataires : gestion des accès aux locaux, supervision, journalisation, etc. (Note 13) - Processus d'habilitation de sécurité ou enquête préliminaire réalisés pour les prestataires qui interviennent sur site - Utilisation de matériels informatiques gérés par l'organisation pour que les prestataires effectuent les interventions sur les biens supports de l'entité (exemple : valise de maintenance, clé USB de <i>firmware</i>) (Note 14) - Nombre et facilité d'accès des points de connexion physique et logique aux réseaux informatiques de l'entité - Existence de liens de télémaintenance ou de de connexions avec des réseaux tiers sécurisés - Existence d'une politique de sécurité pour la <i>supply chain</i> industrielle (exemple : exigences contractuelles, audits de sécurité des fournisseurs, etc.) - Existence de mesures de sécurité pour la maintenance des biens supports (Note 15) - Existence de mesures de sécurité physique et type de technologie utilisée : contrôle d'accès (exemple : portique, badge, digicode, biométrie), vidéo protection, etc. - Supervision de la sécurité physique et réactivité des équipes d'intervention en cas d'une détection d'intrusion (sur place, à distance, 24/7, seulement heures ouvrées) - Nombre de barrières à franchir pour accéder physiquement aux biens supports critiques (Note 16) - Personnels de sécurité formés au risque d'introduction physique de matériels d'écoute - Utilisateurs sensibilisés, voire entraînés, à la vigilance vis-à-vis des intrusions physiques - Connaissance mutuelle des personnes pouvant avoir un accès légitime - Existence d'une politique de sécurité pour les déplacements professionnels, sensibilisation des salariés aux risques lors de leurs missions
 <p>Reconnaissance interne</p>  <p>Latéralisation, élévation de privilèges</p>	<p>Les éléments majeurs qui influent sur la probabilité de succès ou la difficulté technique d'une reconnaissance interne, d'une latéralisation ou d'une élévation de privilèges sont relativement similaires et regroupés.</p> <ul style="list-style-type: none"> - Utilisateurs ayant des droits d'administrateur sur leur poste (Note 17) - Existence d'une politique de gestion des profils d'utilisateurs et de leurs droits d'accès, application du principe du moindre privilège - Connexions à distance sur les systèmes limitées à des machines dédiées à l'administration, sans accès à Internet - Existence d'un centre de supervision de la sécurité (SOC) - Existence d'une politique d'authentification sur les réseaux (Note 18) - Cloisonnement des réseaux informatiques de l'entité par domaines de confiance ou de sensibilité des données (par exemple selon les guides de recommandations de l'ANSSI) - Administration sécurisée des réseaux et services (par exemple selon les guides de recommandations de l'ANSSI) - Niveau d'hétérogénéité du parc informatique (Note 19) - Nombre et spécificité des services offerts par le système d'information (Note 20) - Facilité d'accès des données critiques (Note 21)
 <p>Pilotage, exploitation de l'attaque</p>	<p>Les éléments à considérer peuvent dépendre de l'objectif visé par l'attaquant et du mode d'attaque employé.</p> <ul style="list-style-type: none"> - Nature du canal qu'il faudrait mettre en place pour piloter ou exploiter une attaque sur les biens supports visés (Note 22) - Contraintes de temps présumées pour l'exploitation de l'attaque (Note 23) - Existence d'un centre de supervision de la sécurité (SOC) - Existence d'un dispositif anti-DDOS - Prise en compte de la menace TEMPEST, liée à l'interception de signaux parasites compromettants, notamment si les locaux de l'entité sont situés dans une zone urbaine de forte densité

 <p>Outils malveillants</p>	<p>Comme mentionné plus haut, la plupart des attaques demande la mise en place de logiciels malveillants (<i>malwares</i>) dans les systèmes ciblés, parfois à différentes étapes. Cette section, complémentaire aux précédentes, regroupe les éléments majeurs qui déterminent la réussite et le coût d'un outil malveillant. Elle peut vous aider à affiner l'estimation de la vraisemblance d'une action élémentaire qui nécessiterait un <i>malware</i>.</p> <ul style="list-style-type: none"> - Type de technologie des biens supports ciblés par l'outil malveillant (Note 24) - Délai d'application des correctifs de sécurité après leur publication. Mise en œuvre des recommandations de l'ANSSI relatives au MCS (Note 25) - Degré d'ancienneté de la technologie des biens supports ciblés
---	--

Note 1 : plus les cibles potentielles sont nombreuses, plus il sera facile pour l'attaquant de trouver une cible corruptible.

Note 2 : des personnes mal considérées et mal payées seront naturellement plus faciles à corrompre. Il ne faut pas sous-estimer ces leviers qui s'avèrent puissants.

Note 3 : beaucoup d'informations sont aisément obtenues au travers d'approches informelles dans les milieux professionnels. Lors de démarches commerciales notamment, de nombreuses informations sensibles sont souvent échangées (exemple : faux client, réponse à un appel d'offre).

Note 4 : les protocoles de chiffrement permettent de limiter l'impact des fuites de données, en particulier vis-à-vis des interceptions ou des détournements de trafic.

Note 5 : des attaques nécessitant de fortes compétences dans un ou plusieurs domaines d'expertise en lien avec l'activité de la cible (exemple : contrôle aérien, risque NRBC – nucléaire, radiologique, bactériologique, chimique, signalisation ferroviaire) sont naturellement plus chères et difficiles à trouver que des attaques ne nécessitant que des compétences en sécurité informatique.

Note 6 : ces outils fonctionnent sur la base de signatures et sont assez efficaces pour détecter les attaques les plus grossières.

Note 7 : une technologie qualifiée ou certifiée est plus robuste vis à vis des exploits, car elle a fait l'objet d'une qualité de développement accrue, avec une attention importante donnée à la sécurité, et a subi des tests d'intrusion (exemple : certification de sécurité de premier niveau, critères communs, agrément, référentiel général de sécurité).

Note 8 : plus il y a d'utilisateurs, plus il est facile de tester plusieurs cibles jusqu'à ce que l'une d'elle réalise l'opération attendue.

Note 9 : ce type d'outil est assez efficace pour détecter les attaques les plus grossières (hameçonnage de masse, par exemple envoi d'un courriel piégé contenant un rançongiciel non ciblé).

Note 10 : les solutions de filtrage de la navigation permettent à la fois de filtrer ce qui est connu comme hébergeant une activité malveillante et d'enregistrer le trafic à des fins d'investigation poussée dans le cadre d'une supervision de sécurité.

Note 11 : les navigations autorisées par listes blanches sont relativement complexes à contourner par un attaquant qui souhaite mener une attaque par point d'eau.

Note 12 : la mise en place de mesures de sécurisation des mises à jour logicielles et *firmware* peut rendre beaucoup plus difficile une attaque de type cheval de Troie. Exemples de mesures : sas antivirus (certifié) avant application des mises à jour, procédures de contrôle d'intégrité des patches et correctifs.

Note 13 : des interventions réalisées en dehors des heures ouvrées ou en l'absence de toute surveillance humaine facilitent une activité frauduleuse ou illégitime. Il en est de même si un prestataire dispose d'un badge d'accès lui permettant de circuler librement dans toutes les zones.

Note 14 : le fait qu'un prestataire utilise ses propres moyens d'intervention pour, par exemple, effectuer la maintenance d'un automate ou la mise à jour d'un réseau informatique, accroît le risque d'introduction d'un éventuel code malveillant ciblé ou non, éventuellement à l'insu du prestataire.

Note 15 : exemples de mesures : retrait des supports de stockage à mémoire non volatile, scellement physique, application du référentiel d'exigences de l'ANSSI relatif à l'intégration et à la maintenance des systèmes industriels.

Note 16 : il est recommandé de disposer d'au moins 3 barrières physiques pour accéder aux biens supports critiques.

Note 17 : le fait qu'un utilisateur ait des droits d'administrateur sur son poste facilite grandement les opérations de reconnaissance interne, latéralisation et élévation de privilèges.

Note 18 : exemples de moyens d'authentification du plus sécurisé au moins sécurisé : authentification forte (exemple : carte à puce), mot de passe avec politique contraignante, mot de passe sans politique, pas d'authentification.

Note 19 : plus le niveau d'hétérogénéité est élevé, plus la surface d'attaque est importante et plus il est facile de trouver une vulnérabilité exploitable. A titre indicatif : hétérogénéité élevée (évolutions externes, BYOD, services disparates, etc.), hétérogénéité moyenne (rationalisation progressive, convergence des applicatifs, etc.), hétérogénéité faible et maîtrisée (applicatifs standards, etc.).

Note 20 : plus les services métiers offerts par le système d'information sont nombreux et spécifiques, plus la surface d'attaque est importante et plus il est facile de trouver une vulnérabilité exploitable.

Note 21 : la recherche des informations techniques (plans d'adressage, mots de passe, etc.) ou métiers peut être largement complexifiée pour l'attaquant. Exemples du plus facile au plus difficile : données stockées en clair dans une zone centralisée et facilement identifiable (par leur nommage, etc.), données stockées à de multiples endroits, données chiffrées (pour l'attaquant, il sera alors nécessaire d'obtenir la clé de déchiffrement).

Note 22 : exemples de canaux de *command & control* : canal préexistant déjà en place (*backdoor*), canal synchrone mis en place pour l'attaque (exemples : direct, reverse tcp/http), canal asynchrone (exemples : mail, réseaux sociaux), canal physique (exemple : *air gap* via des supports de stockage amovibles).

Note 23 : le temps d'exploitation va dépendre de l'objectif visé. Il peut être très court par exemple (quelques minutes à quelques heures) dans le cas d'un sabotage ou d'une attaque en déni de service non persistante, ou relativement long (plusieurs mois, voire années) pour une opération d'espionnage. D'autre part, certaines contraintes de temps peuvent rendre la tâche plus difficile pour l'attaquant. A titre indicatif, par ordre croissant de difficulté : aucune contrainte, l'attaque peut être portée n'importe quand ; le timing doit être précis, mais le préavis est important ; le timing doit être précis et l'attaquant aura peu de préavis ; l'attaque doit être coordonnée sur plusieurs machines, sans connexion à Internet.

Note 24 : il est rare qu'un logiciel malveillant soit développé spécifiquement pour une attaque. Toutefois, selon la technologie des biens supports visés, l'attaquant pourra être amené à adapter ou redévelopper un *malware*. Dans certains cas, si la technologie ciblée est très spécifique, il devra même acquérir le bien support (exemple : calculateur aéronautique, automate programmable industriel). Le type de technologie ciblé influe donc énormément sur la difficulté technique.

Note 25 : un bien support à jour en termes de correctifs de sécurité oblige pour l'attaquant le développement d'un exploit dit « *0-day* », donc inconnu du public. Dans le cas contraire, l'attaquant n'a qu'à exploiter une vulnérabilité publique (difficulté nulle et probabilité de succès quasi-certaine). Plus le délai d'application d'un correctif de sécurité sur une vulnérabilité connue est long, plus la fenêtre d'opportunité pour obtenir un exploit sans difficulté est importante.

Fiche méthode n°9 : Structurer les mesures de traitement du risque (Atelier 5)

Les mesures de traitement du risque peuvent être structurées selon les lignes de sécurité en profondeur ci-après :

- gouvernance et anticipation ;
- protection ;
- défense ;
- résilience.

Elles peuvent être organisées comme suit :

Gouvernance et anticipation	<ul style="list-style-type: none">• Gouvernance :<ul style="list-style-type: none">- organisation de management du risque et de l'amélioration continue- processus d'homologation- maîtrise de l'écosystème- gestion du facteur humain (sensibilisation, entraînement)- indicateurs de pilotage de la performance numérique• Connaissance des vulnérabilités : audits de sécurité, veille• Connaissance de la menace : veille (renseignement, intelligence économique)
Protection	<ul style="list-style-type: none">• Cloisonnement des biens supports par domaines de confiance• Gestion de l'authentification et du contrôle d'accès• Gestion de l'administration/supervision• Gestion des entrées/sorties de données et des supports amovibles• Protection des données (intégrité, confidentialité, gestion des clés cryptographiques)• Sécurité des passerelles d'interconnexion et des biens supports « de frontière »• Sécurité physique et organisationnelle• Maintien en condition de sécurité et gestion d'obsolescence• Sécurité des processus de développement, d'acquisition (chaîne d'approvisionnement), et de maintien en condition opérationnelle• Sécurité vis-à-vis des signaux parasites compromettants
Défense	<ul style="list-style-type: none">• Surveillance d'évènements• Détection et classification d'incidents• Réponse à un incident cyber
Résilience	<ul style="list-style-type: none">• Continuité d'activité (sauvegarde et restauration, gestion des modes dégradés)• Reprise d'activité• Gestion de crise cyber

Termes et définitions

Action élémentaire (<i>Elementary action</i>)	Action unitaire exécutée par une source de risque sur un bien support dans un scénario opérationnel. <u>Exemples</u> : exploiter une vulnérabilité, envoyer un email piégé, effacer des traces, augmenter des privilèges.
Air gap	Mesure de sécurité consistant à isoler physiquement un système de tout réseau informatique. Les différents moyens de contournement sont les transferts par support amovibles, la mise en place de connexion pirate, etc.
Appréciation des risques (<i>Risk assessment</i>)	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 (<i>Security need</i>)	Propriété de sécurité à garantir pour une valeur métier. Elle traduit un enjeu de sécurité pour la valeur métier. <u>Exemples</u> : disponibilité, intégrité, confidentialité, traçabilité.
Bien support (<i>Supporting asset</i>)	Composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle. <u>Exemples</u> : 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 (<i>Critical supporting asset</i>)	Bien support jugé très susceptible d'être ciblé par une source de risque pour atteindre son objectif. Les biens supports critiques sont les biens supports qui apparaissent dans les scénarios opérationnels.
Brute force (<i>Brute force attack</i>)	Méthode qui consiste à essayer toutes les combinaisons possibles pour accéder à la ressource.
Cartographie de menace numérique de l'écosystème (<i>Ecosystem digital threat mapping</i>)	Représentation visuelle (exemple : radar) du niveau de menace des parties prenantes de l'écosystème vis-à-vis de l'objet étudié.
Cartographie du risque (<i>Risk mapping</i>)	Représentation visuelle (exemple : radar, diagramme de Farmer) des risques issus des activités d'appréciation du risque.
Chemin d'attaque (<i>Attack path</i>)	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 (<i>Security patch</i>)	Section de code que l'on ajoute à un logiciel, pour corriger une vulnérabilité identifiée.
Déni de service (<i>Denial of service</i>)	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 <i>Distributed denial of service</i> 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 (<i>Ecosystem</i>)	Ensemble des parties prenantes 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. 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.
Effaceur de trace (<i>Rootkit</i>)	Ensemble de techniques mises en œuvre par un ou plusieurs codes malveillants pour dissimuler les traces de leur activité, sur les systèmes ou le réseau.
Evènement intermédiaire (<i>Intermediate event</i>)	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. <u>Exemples</u> : 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.
Evènement redouté (<i>Feared event</i>)	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.
Exploit (<i>Exploit</i>)	Elément de programme permettant à un individu ou à un logiciel malveillant d'exploiter une vulnérabilité dans un logiciel, un firmware, un matériel, un protocole, que ce soit à distance ou sur la machine sur laquelle cet exploit est exécuté. L'objectif peut être de s'emparer d'un ordinateur ou d'un réseau, d'accroître le privilège d'un logiciel ou d'un utilisateur, etc.
Gravité (<i>Severity</i>)	Estimation de la hauteur et de l'intensité des effets d'un risque. La gravité donne une mesure des impacts préjudiciables perçus, qu'ils soient directs ou indirects. <u>Exemples</u> : négligeable, mineure, majeure, critique, maximale.
Hameçonnage (<i>Phishing</i>)	Technique d'envoi massif de mails utilisée pour obtenir des renseignements personnels. Consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration, etc.) afin de lui soutirer les renseignements personnels.
Harponnage (<i>Spearfishing</i>)	Variante de l'hameçonnage (<i>phishing</i>) épaulée par des techniques d'ingénierie sociale. Contrairement à l'hameçonnage traditionnel basé sur l'envoi d'un message générique à un grand nombre de destinataires, le <i>spearfishing</i> se focalise sur un nombre limité d'utilisateurs à qui il est envoyé un message fortement personnalisé.
Homologation de sécurité (<i>Security accreditation</i>)	Validation par une autorité dite d'homologation, que le niveau de sécurité est conforme aux attentes et que les risques résiduels sont acceptables dans le cadre de l'étude.

Ingénierie sociale (<i>Social engineering</i>)	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 cible, à laquelle est lié le système d'information visé. Utilisant ses connaissances, son charisme, l'imposture ou le culot, l'attaquant abuse de la confiance, de l'ignorance ou de la crédulité des personnes ciblées.
Maliciel ou logiciel malveillant (<i>Malware</i>)	Programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté. On peut les catégoriser en 3 types : les « exploits », nécessaires pour obtenir des droits sur les machines dont ne dispose pas l'attaquant avant l'attaque, les « portes dérobées » (<i>backdoors</i>), servant à rajouter des fonctionnalités en vue de faciliter un exploit, et les « effaceurs de traces » (<i>rootkits</i>), servant à dissimuler l'activité.
Menace (<i>Threat</i>)	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 (<i>Security control</i>)	Moyen de traiter un risque prenant la forme de solutions ou d'exigences pouvant être inscrites dans un contrat. <u>Note</u> : <ul style="list-style-type: none"> • 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 (<i>Mission</i>)	Fonction, finalité, raison d'être de l'objet de l'étude.
Prestataire qualifié (<i>Service provider</i>)	La qualification d'un prestataire de service atteste de sa conformité aux exigences de l'ANSSI. Citons : <ul style="list-style-type: none"> • PASSI (prestataire d'audit de la sécurité des systèmes d'information) • PDIS (prestataire de détection des incidents de sécurité) • PRIS (prestataire de réponse aux incidents de sécurité) • PSCE (prestataire de services de certification électronique) • PSHE (prestataire de service d'horodatage électronique) • SecNumCloud (prestataire de service d'informatique en nuage)
Niveau de menace d'une partie prenante (<i>Threat level of a stakeholder</i>)	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 (<i>Risk level</i>)	Mesure de l'importance du risque, exprimée par la combinaison de la gravité et de la vraisemblance.
Objectif visé (OV) (<i>Target objective</i>)	Finalité visée par une source de risque, selon ses motivations. <u>Exemples</u> : 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 <i>(Studied object)</i>	Organisation, système d'information ou produit faisant l'objet de l'analyse de risque.
Partie prenante <i>(Stakeholder)</i>	Élément de l'écosystème (personne, système d'information ou organisation) qui peut être interne ou externe à l'organisation de l'objet de l'étude. <u>Exemples</u> : partenaire, prestataire, client, fournisseur, filiale, service connexe support.
Partie prenante critique (PPC) <i>(Critical stakeholder)</i>	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) <i>(Security continuous improvement plan)</i>	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 <i>(Waterhole)</i>	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.
Porte dérobée <i>(Backdoor)</i>	Fonctionnalité inconnue de l'utilisateur légitime donnant un accès secret au système et permettant à l'attaquant d'en prendre le contrôle.
Rançongiciel <i>(Ransomware)</i>	Malware qui chiffre les documents ou l'ensemble de l'ordinateur infecté et qui demande de l'argent (une rançon) à son propriétaire en échange de la clé permettant le déchiffrement.
Risque initial <i>(Initial risk)</i>	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 <i>(Residual risk)</i>	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 <i>(Risk scenario)</i>	Scénario complet, allant de la source de risque à l'objectif visé par elle, décrivant un chemin d'attaque et le scénario opérationnel associé. <u>Note</u> : dans le cadre de ce guide, on considère uniquement les scénarios de risque numérique de nature intentionnelle.
Scénario opérationnel <i>(Operational scenario)</i>	Enchaînement 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 <i>(Strategic scenario)</i>	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) <i>(Risk origin)</i>	<p>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).</p> <p><u>Exemples</u> : services étatiques, hacktivistes, concurrents, employés vengeurs.</p>
Stratégie de traitement du risque <i>(Risk treatment strategy)</i>	<p>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.</p>
Surface d'attaque <i>(Attack surface)</i>	<p>Concept utilisé pour évaluer le caractère avéré d'une vulnérabilité et la probabilité qu'elle soit exploitée par un attaquant.</p>
Technique d'accès ou d'intrusion <i>(Access or intrusion mode of attack)</i>	<p>Toute méthode, technique, moyen permettant à l'attaquant de prendre pied et de compromettre un système d'information, ou d'accéder aux informations qu'il contient.</p>
Technique d'exploitation d'une attaque <i>(Exploitation mode of attack)</i>	<p>Toute méthode, technique, moyen permettant à l'attaquant de réaliser son objectif sur le système ciblé.</p>
Test ou audit d'intrusion <i>(Penetration test, pentest)</i>	<p>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 de 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).</p>
Valeur métier <i>(Business asset)</i>	<p>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.</p> <p><u>Exemples</u> : 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.</p> <p><u>Notes</u> :</p> <ul style="list-style-type: none"> • 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 (<i>Likelihood</i>)	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 (<i>Elementary likelihood</i>)	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 (<i>Vulnerability</i>)	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.
Zéro-jour (<i>0-Day</i>)	Exploit visant une vulnérabilité dont le patch n'a pas encore été publié par l'éditeur, soit parce que cette vulnérabilité n'est pas connue de celui-ci, soit parce que l'éditeur est en cours d'analyse.