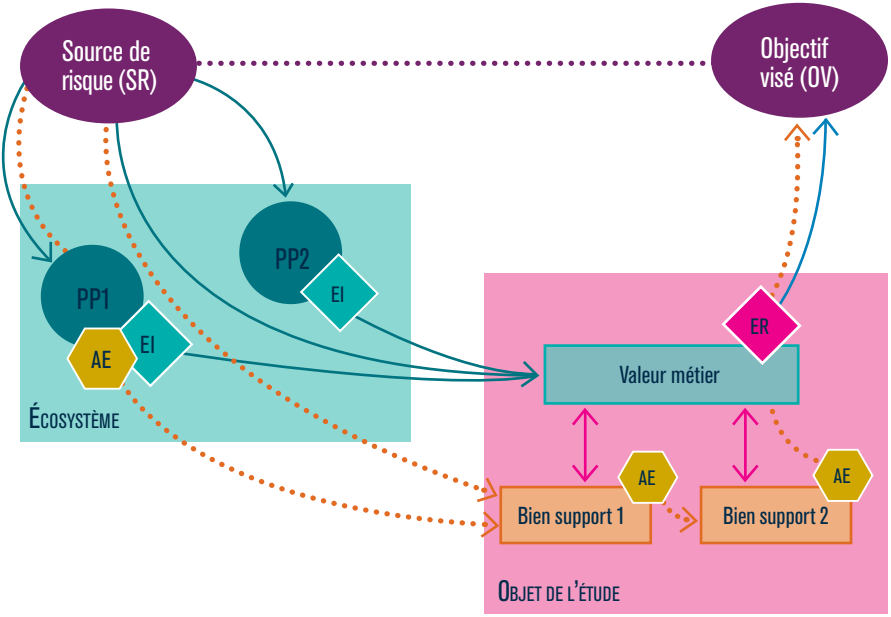
EBIOS
RISK MANAGER

LE SUPPLÉMENT

FICHES MÉTHODES

INTRODUCTION :
COMMENT CONSTITUER LES SCÉNARIOS DE RISQUES ?
(FIN DE L'ATELIER 4)

Le schéma ci-dessous présente les différentes notions abordées par EBIOS *Risk Manager* dans le cadre d'une démarche d'appréciation des risques.



Légende :

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

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 métier 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 pour aller vers l'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.

FICHE MÉTHODE

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

NOTE : il est possible d'associer un ou plusieurs biens supports à une valeur métier.

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 représenter une partie prenante externe de l'écosystème. Les éléments relatifs à l'écosystème seront repris dans le cadre de **l'atelier 3**.

FICHE MÉTHODE

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 (LISTE NON EXHAUSTIVE)
SYSTÈMES INFORMATIQUES ET DE TÉLÉPHONIE	
MATÉRIELS[1]	
TERMINAL UTILISATEUR	Ordinateur fixe, ordinateur portable, tablette, téléphone mobile.
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 WI-FI.
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'adresse 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 (*MIDDLEWARE*)	*Entreprise Application Integration* (EAI), *Extract-Transform-Load* (ETL), *Open DataBase Connectivity* (ODBC).

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

SYSTÈME D'EXPLOITATION, HYPERVISEUR	Windows, Linux, MacOS, Xen.
MICROGICIEL (*FIRMWARE*)	*Basic Input Output System* (BIOS), *Unified Extensible Firmware Interface* (UEFI), gestionnaire de composants d'un téléphone mobile, programme stocké dans une clé USB équipée d'un microprocesseur.
LOGICIEL DE SÉCURITÉ	Outil de gestion d'évènements *Security Information and Event Management* (SIEM).
RÉSEAUX/CANAUX INFORMATIQUES ET DE TÉLÉPHONIE	
RÉSEAU/CANAL INFORMATIQUE	Câble réseau, fibre optique, liaison radio (Wi-Fi, Bluetooth, etc.).
RÉSEAU/CANAL TÉLÉPHONIQUE	Ligne téléphonique.
ORGANISATIONS	
PERSONNE	Employé, stagiaire, prestataire, personnel d'entretien.
SUPPORT PAPIER	Document manuscrit ou imprimé.
ÉCHANGE VERBAL	Réunion, échange informel.
ÉLÉMENT D'INGÉNIERIE SOCIALE	Information partagée sur les réseaux sociaux.
LOCAUX ET INSTALLATIONS PHYSIQUES	
SITE/BÂTIMENT/SALLE	Siège social, usine, site 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 disposer de définitions plus précises des biens supports mentionnés, vous pouvez vous reporter au guide cartographie de l'ANSSI[2] .

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

FICHE MÉTHODE

3

Évaluer la gravité 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 (LISTE NON EXHAUSTIVE)
IMPACTS SUR LES MISSIONS ET SERVICE DE L'ORGANISATION	
CONSÉQUENCES DIRECTES OU INDIRECTES SUR LA RÉALISATION DES MISSIONS ET SERVICES	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.
IMPACTS HUMAINS, MATÉRIELS OU ENVIRONNEMENTAUX	
IMPACTS SUR LA SÉCURITÉ OU SUR LA SANTÉ DES PERSONNES **CONSÉQUENCES DIRECTES OU INDIRECTES SUR L'INTÉGRITÉ PHYSIQUE DE PERSONNES**	Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire.
IMPACTS MATÉRIELS **DÉGÂTS MATÉRIELS OU DESTRUCTION DE BIENS SUPPORTS**	Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématurée de matériels.
IMPACTS SUR L'ENVIRONNEMENT **CONSÉQUENCES ÉCOLOGIQUES À COURT OU LONG TERME, DIRECTES OU INDIRECTES**	Contamination radiologique ou chimique des nappes phréatiques ou des sols, rejet de polluants dans l'atmosphère.

IMPACTS SUR LA GOUVERNANCE	
IMPACTS SUR LA CAPACITÉ DE DÉVELOPPEMENT OU DE DÉCISION **CONSÉQUENCES DIRECTES OU INDIRECTES SUR LA LIBERTÉ DE DÉCIDER, DE DIRIGER, DE METTRE EN ŒUVRE LA STRATÉGIE DE DÉVELOPPEMENT**	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.
IMPACTS SUR LE LIEN SOCIAL INTERNE **CONSÉQUENCES DIRECTES OU INDIRECTES SUR LA QUALITÉ DES LIENS SOCIAUX AU SEIN DE L'ORGANISATION**	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.
IMPACTS SUR LE PATRIMOINE INTELLECTUEL OU CULTUREL **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**	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.
IMPACTS FINANCIERS	
CONSÉQUENCES PÉCUNIAIRES, DIRECTES OU INDIRECTES	Perte de chiffre d'affaires, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées.
IMPACTS JURIDIQUES	
CONSÉQUENCES SUITE À UNE NON-CONFORMITÉ LÉGALE, RÉGLEMENTAIRE, NORMATIVE OU CONTRACTUELLE	Procès, amende, condamnation d'un dirigeant, amendement de contrat.
IMPACTS SUR L'IMAGE ET LA CONFIANCE	
CONSÉQUENCES DIRECTES OU INDIRECTES SUR L'IMAGE DE L'ORGANISATION, LA NOTORIÉTÉ, LA CONFIANCE DES CLIENTS	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'usagers.

2 / Quelle échelle de gravité utiliser ?

Lorsque l'on crée 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. Il est conseillé de l'élaborer en concertation avec les personnes qui vont estimer ces niveaux – particulièrement les métiers – afin de faciliter son appropriation et la cohérence de la cotation. L'échelle de gravité à privilégier reste celle déjà mise en place (si elle existe) pour apprécier les risques de l'organisation dans le cadre d'une démarche globale de management du risque (incluant les risques financier, juridique, etc.). Le risque numérique doit en effet s'insérer 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 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 dès le début de l'atelier dédié aux événements redoutés. Pour ce faire, vous pouvez utiliser et adapter l'échelle générique ci-après. Elle tient compte des impacts internes à l'organisation et d'éventuelles conséquences externes sur les écosystèmes.

NIVEAU DE L'ÉCHELLE	DÉFINITION
G5 – CATASTROPHIQUE	**Conséquences sectorielles ou régaliennes au-delà de l'organisation.** Écosystème(s) sectoriel(s) impacté(s) de façon importante, avec des conséquences éventuellement durables. Et/ou : difficulté pour l'État, voire incapacité, d'assurer une fonction régalienne ou une de ses missions d'importance vitale. Et/ou : impacts critiques sur la sécurité des personnes et des biens (crise sanitaire, pollution environnementale majeure, destruction d'infrastructures essentielles, etc.).
G4 – CRITIQUE	**Conséquences désastreuses pour l'organisation avec d'éventuels impacts sur l'écosystème.** Incapacité pour l'organisation d'assurer la totalité ou une 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 elle opère seront susceptibles d'être légèrement impactés, sans conséquences durables.
G3 – GRAVE	**Conséquences importantes pour l'organisation.** 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.
G2 – SIGNIFICATIVE	**Conséquences significatives mais limitées pour l'organisation.** 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).
G1 – MINEURE	**Conséquences négligeables pour l'organisation.** 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).

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, 4 niveaux suffiront ;
- la cohérence du nombre de niveaux entre les échelles de gravité et de vraisemblance pour l'appréciation des risques réalisée 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 distinguer les niveaux d'impacts de l'échelle. Une façon usuelle de procéder est d'appuyer d'exemples 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 sous une procédure particulière (exemple : 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

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 disposant de moyens sophistiqués et conséquents, voire quasi illimités (États, crime organisé) ;
- les organisations ou groupes guidés par une motivation idéologique disposant de moyens significatifs mis en œuvre de façon relativement coordonnée (terroristes, activistes) ;
- les attaquants disposant de moyens limités mais spécialisés (individus isolés, groupes d'individus ou officines).

Ces catégories peuvent collaborer de façon opportuniste ou organisée
EXEMPLE : organisation terroriste faisant appel à une officine spécialisée.

◆

PROFILS D'ATTAQUANTS	EXEMPLES ET MODES OPÉRATOIRES HABITUELS
ÉTATIQUE	États, agences de renseignement. *Attaques généralement conduites par des professionnels, respectant un calendrier et un mode opératoire prédéfinis. Ce profil d'attaquant se caractérise par sa capacité à réaliser une opération offensive sur un temps long (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) et certains sont capables d'infiltrer des réseaux isolés et de réaliser des attaques successives pour atteindre une ou des cibles (par exemple au moyen d'une attaque visant la chaîne d'approvisionnement).*

CRIME ORGANISÉ	Organisations cybercriminelles (mafias, gangs, officines). *Arnaque en ligne ou au président, demande de rançon ou attaque par rançongiciel, exploitation de réseaux de « machines robots » (botnet), etc. En raison notamment de la prolifération de 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).*
TERRORISTE	Cyberterroristes, cybermilices. *Attaques habituellement peu sophistiquées mais menées avec détermination à des fins de déstabilisation et de destruction : déni de service (visant par exemple à rendre indisponibles 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.*
ACTIVISTE IDÉOLOGIQUE	Cyber-hacktivistes, groupements d'intérêt, sectes. *Modes opératoires et sophistication des attaques relativement similaires à ceux des cyberterroristes mais motivés par des intentions moins destructrices. Certains acteurs vont mener ces attaques pour véhiculer une idéologie, un message (exemple : utilisation massive des réseaux sociaux comme caisse de résonnance).*
OFFICINE SPÉCIALISÉE	Profil de « cybermercenaire » doté de capacités informatiques généralement élevées sur le plan technique. Il est de ce fait à distinguer des *script-kiddies* avec qui il partage toutefois l'esprit de défi et la quête de reconnaissance mais avec un objectif lucratif. De tels groupes peuvent s'organiser en officines spécialisées proposant de véritables services de piratage. *Ce type de hacker chevronné est souvent à l'origine de la conception et de la création d'outils et kits d'attaques [3] accessibles en ligne (éventuellement monnayés) qui sont ensuite utilisables « clés en main » par d'autres groupes d'attaquants. Il n'a pas de motivations particulières autres que le gain financier.*
AMATEUR	Profil du hacker « *script-kiddies* » ou doté de bonnes connaissances informatiques, et motivé par une quête de reconnaissance sociale, d'amusement, de défi. *Attaques basiques mais capacité à utiliser les kits d'attaques accessibles en ligne.*
VENGEUR	Les motivations de ce profil d'attaquant sont guidées par un esprit de vengeance aigüe ou un sentiment d'injustice ***(exemples : salarié licencié pour faute grave, prestataire mécontent suite au non-renouvellement d'un marché, etc.).*** *Ce profil d'attaquant se caractérise par sa détermination et sa connaissance interne des systèmes et processus organisationnels. Cela peut le rendre redoutable et lui conférer un pouvoir de nuisance important.*
MALVEILLANT PATHOLOGIQUE	Les motivations de ce profil d'attaquant sont d'ordre pathologique ou opportuniste et parfois guidées par l'appât du gain (***exemples : concurrent déloyal, client malhonnête, escroc, fraudeur).*** *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 porter son attention sur une source interne (salarié mécontent, prestataire peu scrupuleux) et tenter de la corrompre.*

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

CATÉGORIES D'OBJECTIFS VISÉS

INALITÉS POURSUIVIES	DESCRIPTION
ESPIONNAGE	Opération de renseignement (étatique, économique). Dans de nombreux cas, l'attaquant s'installe durablement dans le système d'information et en toute discrétion. 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.
PRÉPOSITIONNEMENT STRATÉGIQUE	Prépositionnement 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.
INFLUENCE	Opération visant à diffuser de fausses informations ou à les altérer, mobiliser les leaders d'opinion sur les réseaux sociaux, détruire des réputations, divulguer des informations confidentielles, dégrader l'image d'une organisation ou d'un 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 avoir de lourdes conséquences 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) :

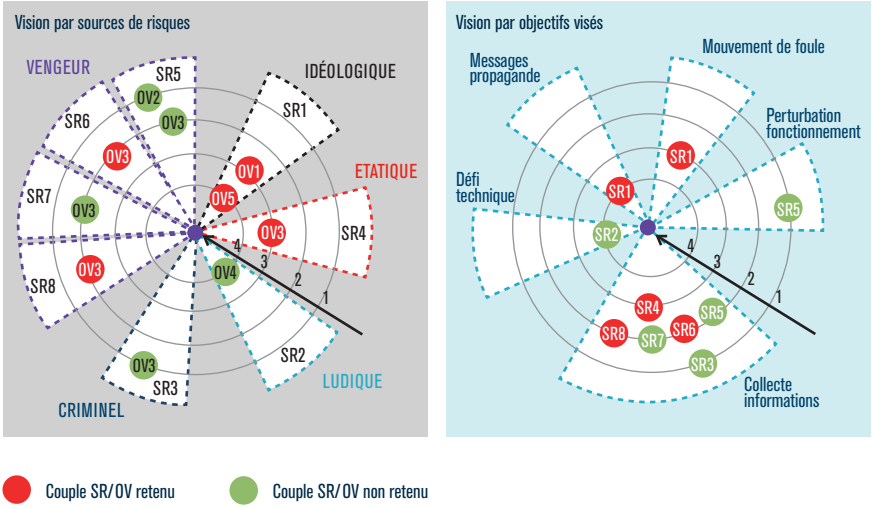
IDENTIFICATION		COTATION			CARACTÉRISATION				ÉVALUATION	
Source de risque (SR)	Objectif visé (OV)	Motivation	Ressources	*Activité*	*Modes opératoires*	*Secteurs d'activités*	*Arsenal d'attaque*	*Faits d'armes*	Pertinence du couple SR/OV	Choix P1/P2

Les ressources incluent à la fois les capacités financières et matérielles de la source de risque, et son niveau de compétence en matière de cyberattaques. Cette compétence peut être également recherchée auprès d'officines spécialisées **(sophistication des modes opératoires, arsenal d'outils 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 solides en analyse de la menace. Le niveau de pertinence d'un couple SR/OV peut être évalué à partir du niveau de motivation, des ressources et de l'activité. En l'absence d'informations suffisantes 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 : Une représentation sur des cartographies visuelles de type radar est également

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

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'objet de l'étude). 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

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 métier **(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. 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.

EXEMPLE : services support, services métier.

Nous vous recommandons également, si cela se révèle pertinent, d'établir une cartographie des parties prenantes par phase de vie ou de mission, 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 étapes.

EXEMPLE : exploitation, maintenance.

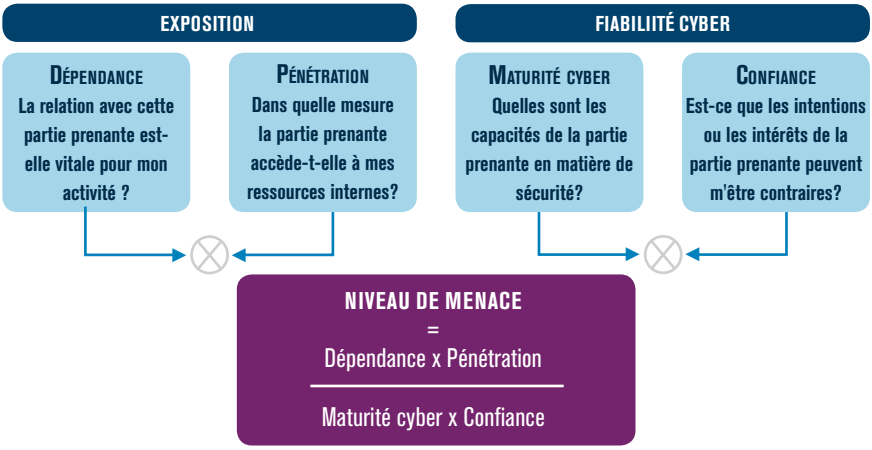
NOTE : les sources de risque identifiées dans l'atelier 2 ne sont pas à prendre en compte en tant que telles lors de la réalisation de cette étape. Les parties prenantes qui pourront également être considérées comme des sources de risque sont ici étudiées uniquement en tant que parties prenantes.

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 de maturité cyber 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 de confiance ne sera pas prépondérant et pourra être retiré de la formule.

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.	Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile, etc.).	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
2	Relation utile aux fonctions stratégiques	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.	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.	Les intentions de la partie prenante sont considérées comme neutres.
3	Relation indispensable mais non exclusive.	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	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.	Les intentions de la partie prenante sont connues et probablement positives.
4	Relation indispensable et unique (pas de substitution possible à court terme).	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.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et se réalise de manière proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

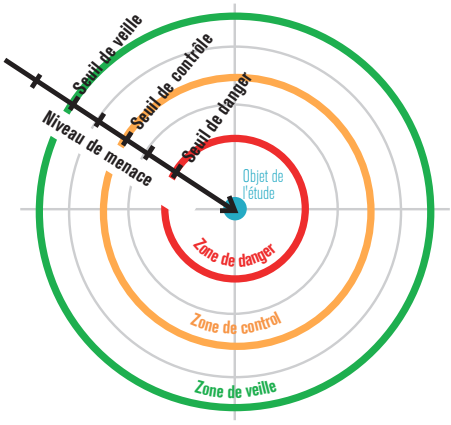
EXEMPLE : société de biotechnologie fabriquant des vaccins.

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	2	1
	P2 – Régulateurs	2	1	2	4	0,3
	P3 – Laboratoires	3	3	2	2	2,25
PRESTATAIRES	F1 – Fournisseurs industriels chimistes	4	2	2	3	1,3
	F2 – Fournisseurs de matériel de production	4	3	2	3	2
	F3 – Prestataire informatique	3	4	2	2	3

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 tolérable sous contrôle. Les parties prenantes qui s'y trouvent doivent faire l'objet d'une vigilance particulière et ont vocation, à moyen terme, à rejoindre une position moins menaçante au travers de mesures de réduction du risque.
EXEMPLE : enrôlement dans l'organisation de management 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.

4 / Comment fixer les valeurs délimitant les 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 pratique, 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 :

- Périmètre de danger : 10 % des parties prenantes de niveaux de menace les plus élevés.
- Périmètre de contrôle : 40 % des parties prenantes suivantes.
- Périmètre de veille : 40 % des parties prenantes suivantes.
- Hors périmètre : les 10 % restants.

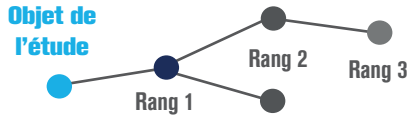
◆

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 périmètre de danger : évaluation des PP connexes jusqu'au rang 3 ;
- PP située dans le périmètre de contrôle : évaluation des PP connexes de rang 2 ;
- PP non critique (à l'extérieur du périmètre 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

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.
ÉLEVÉ – ZONE DE CONTRÔLE	Tolérable sous contrôle	Enrôlement de la partie prenante dans le processus de management du risque : -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.

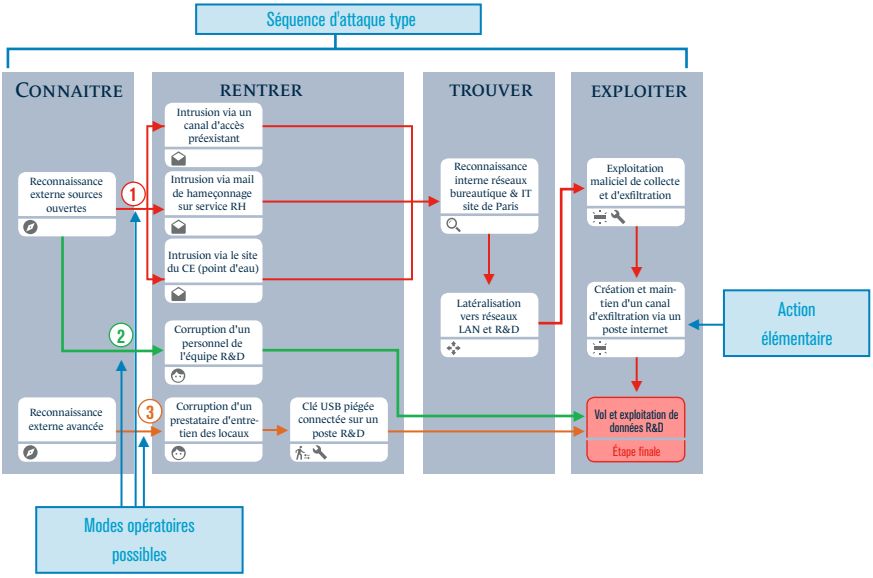
EXEMPLE : une partie prenante pourra être tolérée dans la zone de danger seulement si ses niveaux de maturité et de confiance sont au moins de 3.

FICHE MÉTHODE

7

Élaborer 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 e**nchaînement 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

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 socioprofessionnels, 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 celui de son écosystème en vue d'une attaque par rebond. L'intrusion se fait généralement via des biens supports périmétriques 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 ne pas laisser de 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, 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.
EXEMPLE : rançongiciel.

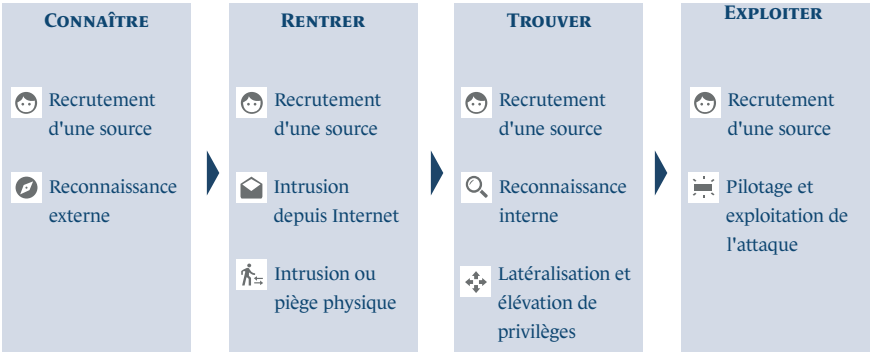
Vous pouvez adopter des modèles de séquences d'attaque plus sophistiqués et les décliner en variantes selon la technique d'attaque de la source de risque pour atteindre son objectif (exfiltration d'information, écoute passive, déni de service, rançongiciel, etc.).

NOTE : pour la phase « Rentrer », nous vous recommandons de distinguer dans le séquencement 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 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 (puces ♦). 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 obtenir des informations sur le système 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 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 a priori légitime.

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 (exemple : 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.

EXEMPLE : 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 lui 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.). Les techniques ci-après sont largement utilisées :

- 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 ultime étape 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[4]).

4 La menace TEMPEST peut également être exploitée de façon active en piégeant préalablement, par exemple via la supply chain, un périphérique (câble, clavier, souris, vidéoprojecteur). Il devient alors une source de signaux parasites compromettants activable et désactivable à distance à condition de disposer d'émetteurs suffisamment puissants pour créer un canal de fuite.

ENTRAVE AU FONCTIONNEMENT (SABOTAGE, NEUTRALISATION)

- Attaque par déni de service distribué (DDoS) ;
- 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[5] d'un bien support (pour tromper ou falsifier) ;
- Systèmes industriels : envoi de commandes à risque pour la sûreté de fonctionnement[6] ;
- 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.

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).

---

5 Inclut les techniques de leurre cognitif en vue d'induire en erreur ou dissimuler une activité aux yeux d'un utilisateur (exemple : demande d'authentification illégitime, message d'alerte masqué).

6 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.

FICHE MÉTHODE

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 cela, 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 en empruntant l'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 en empruntant l'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 en empruntant l'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 en empruntant l'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 l'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 scénario [7]). 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 de 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 plus ou moins finement ces vraisemblances.

◆

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.

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

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 d'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 :

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

		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 ciblé. 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 cyberattaques 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 » :

$$\underset{\textit{cumulé intermédiaire}}{\text{Indice\_Pr}(AE_n)} = \text{Min}\left\{\text{Indice\_Pr}(AE_n), \underset{\textit{cumulés intermédiaires}}{\text{Max}(\text{Indices\_Pr}(AE_{n-1}))}\right\}$$

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 parait 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**[8]**)**. 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.

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

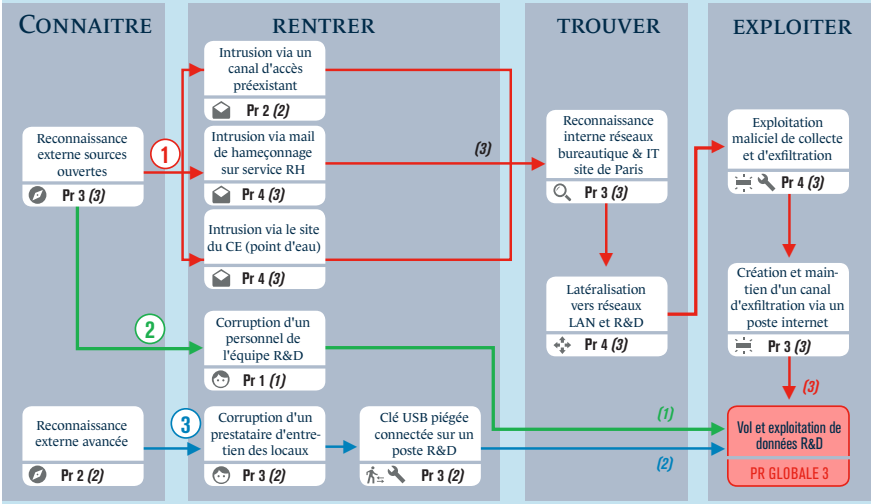
La **vraisemblance du scénario opérationnel** obtenue à l'issue de ces opérations correspond à l'indice global de probabilité de succès.

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*.



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.

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* » :

$$(AE_n) = \text{Max} \left\{ \text{Indice\_Diff}(AE_n), \underbrace{\text{Min (Indices\_Diff}(AE_{n-1}))}_{\textit{cumulés intermédiaires}} \right\}$$

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[9]). 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.

Enfin, déduisez la vraisemblance globale du scénario opérationnel en procédant comme suit[10] :

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

10 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.

- 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 ensuite être pondéré selon la nature de la source de risque (motivation et ressources). Si vous estimez celle-ci comme 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 OPÉRATIONNEL				
		0 – NÉGLIGEABLE	1 – FAIBLE	2 – MODÉRÉE	3 – ÉLEVÉE	4 – TRÈS ÉLEVÉE
PROBABILITÉ DE SUCCÈS DU MODE 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

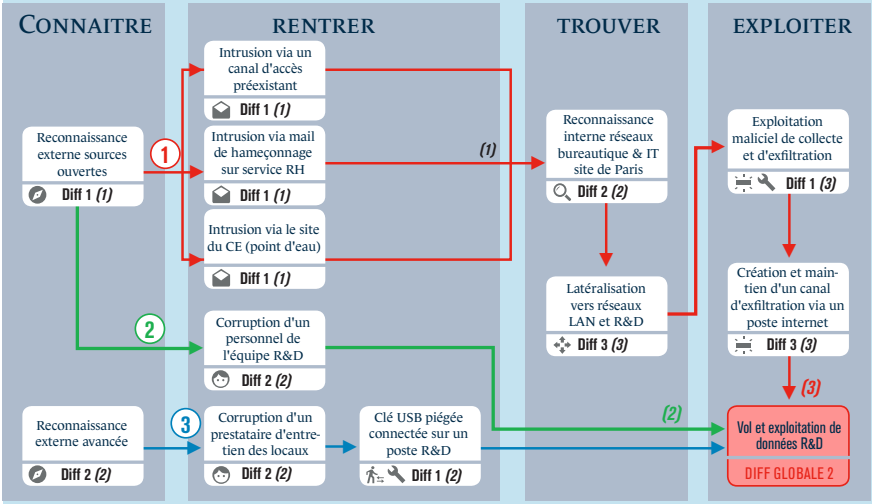
NOTES :

■ 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.



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

Cette section présente pour chaque catégorie d'action élémentaire **(voir fiche méthode 7)** les éléments majeurs qui déterminent sa probabilité de succès ou sa difficulté technique.

RECRUTEMENT D'UNE SOURCE, CORRUPTION DE PERSONNEL

- 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, qui apporte un certain niveau d'assurance sur leur intégrité.
- Satisfaction des cibles à l'égard de leur salaire ou de leur considération au sein de l'organisation.
- Adhésion des cibles potentielles aux valeurs de l'entreprise **(Note 2)**.

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.

RECONNAISSANCE EXTERNE DE LA CIBLE

- 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)**.

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'offres.
Note 4 : les protocoles de chiffrement permettent de limiter l'impact des fuites de données, en particulier vis-à-vis des interceptions ou 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 coûteuses et difficiles à identifier et traiter que des attaques mettant en œuvre des procédés essentiellement techniques.

INTRUSION DEPUIS INTERNET OU DES RÉSEAUX INFORMATIQUES TIERS

Les critères diffèrent selon la technique d'intrusion utilisée par l'attaquant.

ATTAQUE FRONTALE DE SERVICES

- 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, etc. (Note 6)**.

- Utilisation de biens supports « de frontière » certifiés ou qualifiés **(Note 7)**.

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 fait l'objet de tests d'intrusion

EXEMPLE : certification de sécurité de premier niveau, critères communs, agrément, référentiel général de sécurité.

HAMEÇONNAGE / POINT D'EAU

Nombre d'utilisateurs susceptibles d'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)**.

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

INTRUSION VIA UN RÉSEAU SANS FIL

- 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 technique de l'ANSSI[11].

11 Note technique – Recommandations de sécurité relatives aux réseaux Wi-Fi, ANSSI, 2013.

INTRUSION VIA UN LOGICIEL OU UN CORRECTIF LÉGITIME

- Existence d'une politique de sécurité relative aux mises à jour des logiciels, applications métier et firmware **(Note 12)**.
- Sources et canaux de confiance (voire certifiés ou qualifiés), vérifica tion de l'identité des signataires pour les mises à jour.

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 patchs et correctifs.

INTRUSION OU PIÈGE PHYSIQUE

- 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 *firmware* **(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 connexions avec des réseaux tiers sécurisés.
- Existence d'une politique de sécurité pour la chaîne d'approvisionnement 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 de 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.

Note 13 : des interventions réalisées en dehors des heures ouvrées ou en l'absence de toute vigilance/présence 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 trois barrières physiques pour accéder aux biens supports critiques.

RECONNAISSANCE INTERNE

LATÉRALISATION ET ÉLÉVATION DE PRIVILÈGES

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.

- 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)**.

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, mot de passe avec politique contraignante, mot de passe sans politique, pas d'authentification.

EXEMPLE : carte à puce.

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. À 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 métier offerts par le système d'information sont nombreux et spécifiques, plus la surface d'attaque est importante et plus il est facile d'identifier 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 par ordre croissant de difficulté : 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).

PILOTAGE ET EXPLOITATION DE L'ATTAQUE

Les éléments à considérer peuvent dépendre de l'objectif visé par l'attaquant et du mode d'attaque employé.

- 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.

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 (quelques minutes à quelques heures), par exemple 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. À 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.

OUTILS MALVEILLANTS

La plupart des attaques demande l'installation de logiciels malveillants dans les systèmes ciblés, parfois en plusieurs étapes. Cette section, complémentaire des précédentes, regroupe les éléments majeurs qui déterminent la réussite et le coût d'un projet malveillant (mode opératoire, outil(s), etc.). Elle peut vous aider à affiner l'estimation de la vraisemblance d'une action élémentaire qui nécessiterait l'installation d'un logiciel malveillant.

- 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 24 : il est rare qu'un logiciel soit développé spécifiquement pour être malveillant et servir un dessein d'attaque.

Toutefois, selon la technologie des biens supports visés, l'attaquant pourra être amené à adapter ou redévelopper un logiciel malveillant. 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

9

Structurer les mesures de traitement du risque (atelier 5)

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

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

Elles peuvent être organisées comme suit :

GOUVERNANCE ET ANTICIPATION	**Gouvernance** ♦organisation de management du risque et d'amélioration continue ; ♦processus d'homologation ; ♦maîtrise de l'écosystème ; ♦gestion du facteur humain (sensibilisation, entrainement) ; ♦indicateurs de pilotage de la performance numérique. **Connaissance des vulnérabilités** ♦audits de sécurité, veille. **Connaissance de la menace** ♦veille (renseignement, intelligence économique).
PROTECTION	♦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 périmétriques (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	♦Surveillance d'événements ; ♦Détection et classification d'incidents ; ♦Réponse à un incident cyber.
RÉSILIENCE	♦Continuité d'activité (sauvegarde et restauration, gestion des modes dégradés) ; ♦Reprise d'activité ; ♦Gestion de crise cyber.

Termes et définitions

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 amovible, la mise en place de connexion pirate, etc.

◆

EFFACEUR DE TRACE *(Rootkit)*

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.

◆

EXPLOIT *(Exploit)*

Élément 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 est exécuté cet exploit. 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.

◆

FORCE BRUTE *(Brute force attack)*

Méthode qui consiste à essayer toutes les combinaisons possibles pour accéder à la ressource.

HAMEÇONNAGE *(Phishing)*

L'hameçonnage consiste en l'extorsion d'informations confidentielles (codes d'accès, coordonnées bancaires, etc.) par subterfuge. En se faisant passer pour une personne ou un tiers de confiance (banque, Impôts, fournisseur d'accès à Internet, etc.), l'attaquant tente de soutirer des informations à ses victimes en ayant recours à différentes méthodes : courriel porteur de demandes incongrues et indiscrètes, téléchargement de pièces jointes piégées, suivi de liens redirigeant vers des sites frauduleux, etc.

◆

HARPONNAGE *(Spearfishing)*

Variante du hameçonnage (*phishing*) à laquelle s'ajoutent des techniques d'ingénierie sociale. Contrairement au hameçonnage traditionnel basé sur l'envoi d'un message générique à un grand nombre de destinataires, le spearfishing se focalise sur un nombre limité d'utilisateurs auxquels est envoyé un message fortement personnalisé.

◆

LOGICIEL MALVEILLANT *(Malware)*

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 classer en trois catégories : les « exploits », nécessaires pour obtenir des droits sur les machines dont ne dispose pas l'attaquant avant l'attaque, les « portes dérobées » (*backdoors*), servant à rajouter des fonctionnalités en vue de faciliter un exploit et les « effaceurs de traces » (*rootkits*), servant à dissimuler l'activité.

PORTE DÉROBÉE *(Backdoor)*

Fonctionnalité inconnue de l'utilisateur légitime donnant un accès secret au système et permettant à l'attaquant d'en prendre le contrôle.

◆

PRESTATAIRE QUALIFIÉ *(Service provider)*

La qualification d'un prestataire de service atteste de sa conformité aux exigences de l'ANSSI. Citons :

- 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).

◆

RANÇONGICIEL *(Ransomware)*

Contraction des mots « rançon » et « logiciel », un rançongiciel est par définition un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Pour y parvenir, le rançongiciel va empêcher l'utilisateur d'accéder à ses données, par exemple en les chiffrant, puis lui indiquer les instructions utiles au paiement de la rançon en échange de la restitution de ses données.

TECHNIQUE D'ACCÈS OU D'INTRUSION *(Access or intrusion mode of attack)*

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.

◆

TECHNIQUE D'EXPLOITATION D'UNE ATTAQUE *(Exploitation mode of attack)*

Toute méthode, technique, moyen permettant à l'attaquant de réaliser son objectif sur le système ciblé.

◆

ZÉRO-JOUR *(0-Day)*

Exploit visant une vulnérabilité dont le correctif 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 poursuit son analyse.

NOTES

Version 1.1 – Janvier 2019
ANSSI-PA-058

Licence Ouverte/Open Licence (Etalab – V1)

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