Mission 2

Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel

Mme Azri souhaite maintenant identifier les risques liés au traitement des données à caractère personnel dans le cadre du processus d'études de marché.
Pour réaliser ce travail, vous devez prendre appui sur la méthode PIA (*Privacy Impact Assessment*, en français « analyse d'impact relative à la protection des données ») proposée par la CNIL et présentée dans le document 1.

Travail à faire

La première phase de la méthode PIA repose sur la compréhension du contexte.

1. Identifiez, dans la description du contexte, les éléments permettant d'identifier les vulnérabilités liées au traitement des données à caractère personnel.
   > Documents 1 et 2

L'identification des menaces et des événements redoutés est un préalable à la cartographie des risques.

2. Complétez le tableau d'analyse des scénarios de menaces présenté dans le document 4. Justifiez les niveaux de vraisemblance retenus pour chaque menace.
   > Fiches savoirs technologiques 1 et 2
   > Documents 3 et 4
3. Retrouvez, pour chaque risque mentionné, l'événement redouté et son niveau de gravité estimé, en complétant le document 5.
   > Fiche savoirs technologiques 1
   > Documents 3, 4 et 5
4. Cartographiez les risques liés au traitement des données à caractère personnel par un schéma croisant les niveaux de vraisemblance et de gravité déterminés précédemment.
   > Fiche savoirs technologiques 1
5. Rédigez une note de synthèse à l'intention de Mme Azri pour l'informer des risques identifiés et de leur hiérarchisation. Cette note doit énumérer des propositions pour garantir la confidentialité et l'intégrité des données à caractère personnel dans le cadre du processus d'études de marché.
   > Fiche savoirs technologiques 2

> Voir lexique BTS SIO, p. 221

CHAPITRE 1

Missions professionnelles

Document 3 Risques identifiés sur les données à caractère personnel

Scénario 1

Usurpation d'un compte d'authentification d'un opérateur par un intervenant extérieur lors d'une opération de maintenance sur un ordinateur, pour récupérer des données confidentielles.

Les données se situent sur le serveur de base de données et non sur le poste de l'opérateur ; la menace reste peu probable. Par contre, les données confidentielles peuvent bénéficier à une entité malveillante avec des conséquences importantes pour CentreCall.

Scénario 2

Suppression ou vol de données dans la base de données par un salarié mécontent, dans l'objectif de nuire à CentreCall, voire de les communiquer à un concurrent.

L'action est facile à mener avec des conséquences importantes.

Scénario 3

Consultation de données par un employé non-habilité due à une erreur de manipulation.

La consultation de données sans habilitation est peu probable, parce qu'une politique de sécurité rigoureuse dans ce domaine est mise en place par M^me^ Azri. Cependant, dans le cas d'une faiblesse temporaire dans ce domaine, les risques sont limités car le périmètre d'habilitation de chaque utilisateur est restreint.

Scénario 4

Altération de données sur le serveur de base de données par un attaquant extérieur à l'organisation afin de déstabiliser les campagnes d'études de marché.

Les serveurs de base de données sont actuellement peu protégés des menaces qui viendraient de l'extérieur de l'organisation. Une attaque de ce type provoquerait d'importantes conséquences, notamment sur la qualité et la crédibilité des futures synthèses d'études de marché.

Scénario 5

Arrêt du serveur de base de données par une attaque extérieure due à une multitude de requêtes.

Actuellement, le serveur de base de données pourrait être arrêté pour cette raison. Le risque serait alors maximal, car le travail de tous les opérateurs et des Call managers *dépend de l'accès aux données hébergées sur le serveur.*

Document 4 Analyse des scénarios de menaces

Source de menace	Type de menace	Bien support	Niveau de vraisemblance	Critères de sécurité		
				Confidentialité	Disponibilité	Intégrité
Scénario de menace lié au risque 1 : attaquant extérieur	Espionnage	Ordinateur de l'opérateur	**2** : limité (les données ne sont présentes que sur le serveur de base de données)	L'authentification n'est plus assurée aux seules personnes habilitées.		
…	…	…				

Mesure de la vraisemblance : **1** négligeable – **2** limité – **3** important – **4** maximal.

Document 5 Événements redoutés

Exemple : scénario 1	Usurpation d'identité	Niveau de gravité : **3** (important). Les données confidentielles peuvent être exploitées par une entité malveillante.
…	…	

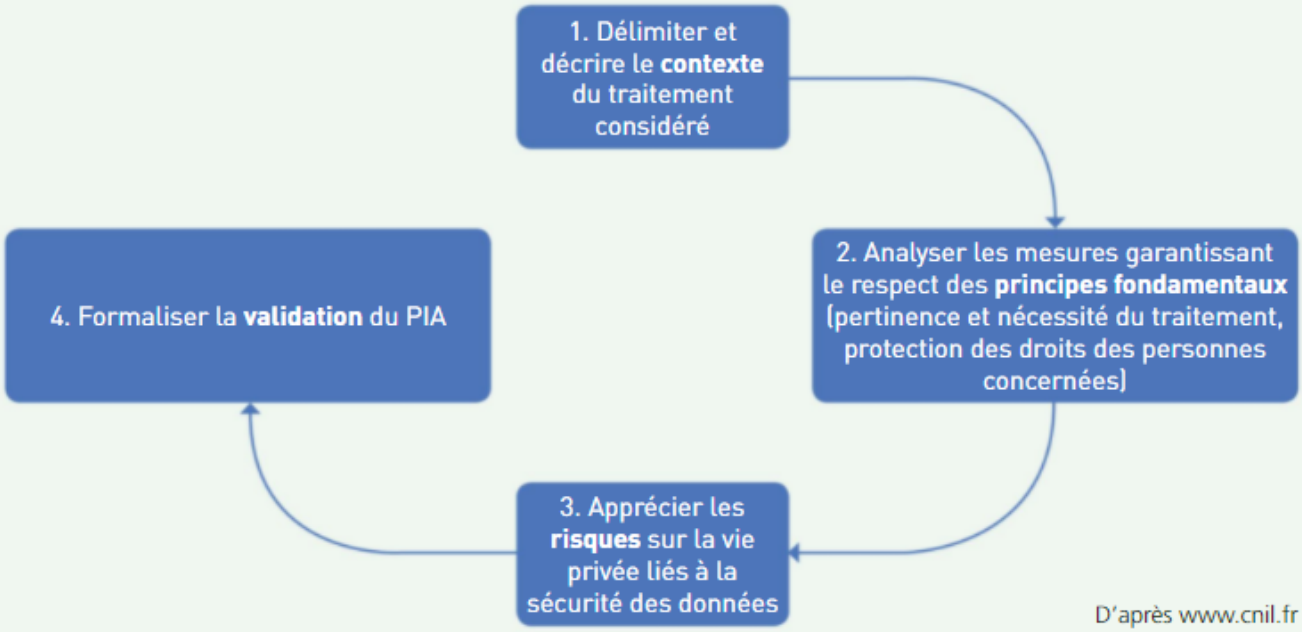
Mesure de la gravité : **1** négligeable – **2** limité – **3** important – **4** maximal.

› Voir lexique BTS SIO, p. 221

Dossier documentaire

Document 1 Démarche PIA (*Privacy Impact Assessment*)

Une «analyse d'impact relative à la protection des données» (voir article 35 du RGPD), plus communément appelée *Privacy Impact Assessment* (PIA) décrit la manière d'employer la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité) préconisée par l'ANSSI. Quatre phases permettent de mener un PIA :



D'après www.cnil.fr

Document 2 Contexte du PIA relatif au traitement d'une étude de marché chez CentreCall

Le PIA porte sur le processus d'étude de marché mis en œuvre par CentreCall. M^me^ Azri est responsable du traitement des données manipulées dans le cadre de ce processus. L'objectif des études de marché est de collecter et d'analyser des informations qui identifient les caractéristiques d'un marché. Les données traitées sont ensuite mises à disposition des différents clients.

Données traitées
Informations personnelles, réponses au questionnaire, enregistrement audio de l'entretien, analyse des résultats de l'étude de marché.
Destinataires
• CentreCall. • Clients de l'étude de marché.
Durée de conservation
Les données sont conservées 1 an.

Cycle de vie des données

– Demande d'enregistrement de l'appel : la personne contactée notifie son acceptation ou non de l'enregistrement de l'entretien, et elle est informée des conditions de traitements de ses données à caractère personnel.

– Collecte des réponses aux questionnaires : les données sont collectées par l'opérateur par saisie sur son ordinateur de bureau, puis enregistrées sur un serveur de base de données hébergé par CentreCall.

– Vérification de l'enregistrement audio de l'entretien : l'enregistrement audio est vérifié puis sauvegardé sur un serveur de fichiers hébergé par CentreCall.

– Analyse des résultats de l'étude de marché.

Supports des données

– Un téléphone IP (*Internet Protocol*) est utilisé pour la conversation.

– Un ordinateur de bureau est mobilisé lors de l'enregistrement des réponses et de l'entretien.

– Plusieurs serveurs de base de données redondants stockent les réponses aux questionnaires, et un serveur de fichiers stocke l'enregistrement audio de l'entretien.

> Voir lexique BTS SIO, p. 221

Fiche savoirs technologiques 1

La typologie des risques et leurs impacts

I Définitions de vulnérabilité, menace et risque

Vulnérabilité	Menace	Risque
En informatique, une vulnérabilité est une faiblesse de la sécurité du système d'information (SI) qui peut affecter son fonctionnement normal.	Une menace est une cause intentionnelle ou non-intentionnelle qui peut entraîner des dommages sur le SI.	Un risque de sécurité du SI est la probabilité de l'exploitation d'une vulnérabilité du SI par une menace. Le niveau d'un risque est estimé en fonction de sa gravité et de la vraisemblance de son apparition.

Les objectifs de la sécurité informatique consistent à limiter les vulnérabilités du SI.

II La typologie des risques informatiques

1. La méthode EBIOS

> EBIOS Risk Manager : www.lienmini.fr/6988-104
> Fiche méthode 5, p. 211

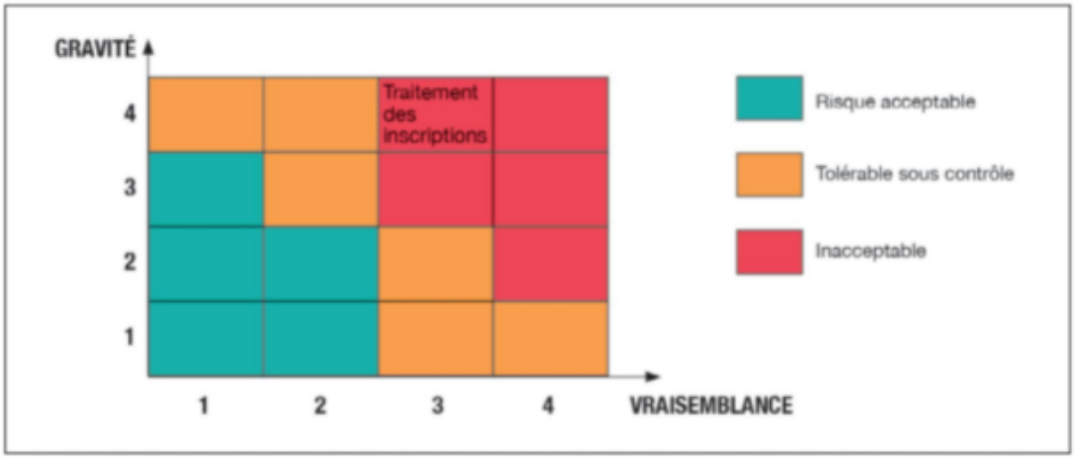
La méthode EBIOS Risk Manager (Expression des besoins et identification des objectifs de sécurité) développée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et retenue par la CNIL (Commission nationale de l'informatique et des libertés) permet d'identifier et de hiérarchiser les différents risques dans un contexte clairement défini.

Un risque est défini par l'ANSSI comme « un scénario qui combine un événement redouté et un ou plusieurs scénarios de menaces ». Un événement redouté désigne par exemple la possibilité d'atteindre des données avec des conséquences probables sur la vie privée des personnes concernées.

2. L'évaluation des risques

L'évaluation des impacts des risques informatiques est réalisée par le croisement de son niveau de vraisemblance et de gravité.

Exemple de cartographie des risques



La vraisemblance reflète la probabilité ou la possibilité que l'un des modes opératoires de l'attaquant aboutisse à l'objectif visé. Elle dépend des vulnérabilités des supports face aux menaces et des capacités des sources de risque à les exploiter.

La gravité évalue l'enjeu d'un événement redouté sur des « valeurs métier », c'est-à-dire stratégiques pour l'organisation (informations confidentielles, processus métier, matériels, logiciels, etc.).

Exemple de mesure de la gravité

Valeur métier	Évènement redouté	Impacts	Gravité
Facturation	Altération des informations sur les factures	• Impossibilité de recevoir un paiement • Perte de crédibilité • Impossibilité de remplir les obligations légales	G3 - Grave

III Les impacts des risques informatiques

L'ANSSI, au travers de sa méthode EBIOS, identifie différentes catégories d'impacts.

Impacts sur les missions et les services de l'organisation	Conséquences directes ou indirectes sur la réalisation des missions et services.
Impacts humains, matériels ou environnementaux	• **Impacts sur la sécurité ou sur la santé des personnes :** conséquences sur l'intégrité physique de personnes. • **Impacts matériels :** dégâts matériels ou destruction de biens supports. • **Impacts sur l'environnement :** conséquences écologiques à court ou long terme.
Impacts sur la gouvernance	• **mpacts sur la capacité de développement ou de décision :** conséquences sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement. • **Impacts sur le lien social interne :** conséquences sur la qualité des liens sociaux au sein de l'organisation. • **Impacts sur le patrimoine intellectuel ou culturel :** conséquences sur les connaissances non-explicites accumulées par l'organisation sur le savoir-faire, les capacités d'innovation, les références culturelles communes.
Impacts financiers	Conséquences pécuniaires.
Impacts juridiques	Conséquences suite à une non-conformité légale, réglementaire, normative ou contractuelle.
Impacts sur l'image et la confiance	Conséquences sur l'image de l'organisation, la notoriété, la confiance des clients.

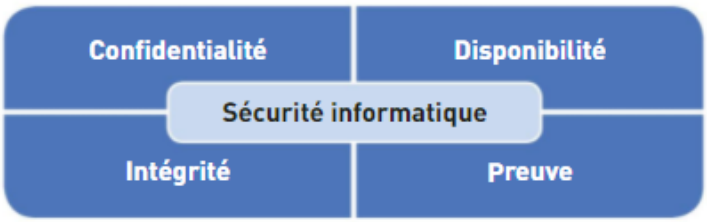
› Voir lexique BTS SIO, p. 221

CHAPITRE 1

Fiche savoirs technologiques 2

Les principes de la sécurité

La sécurité des systèmes d'information repose sur quatre principes fondamentaux :



I La confidentialité

La **confidentialité** vise à assurer que les données ne sont accessibles qu'aux seules personnes autorisées.

> **Exemple :** la connexion d'un utilisateur au réseau de l'organisation par son identifiant et son mot de passe personnel ne donne accès qu'aux données qu'il est autorisé à consulter ou à modifier.

II La disponibilité

La **disponibilité** doit rendre les données accessibles et utilisables par les personnes autorisées sans interruption.

> **Exemple :** la redondance des connexions réseaux permet d'accéder aux données de manière continue, même si une connexion est rompue.

III L'intégrité

Le principe d'**intégrité** s'assure que les données ne peuvent pas être modifiées pendant leur transfert, leur traitement ou leur stockage.

> **Exemple :** des protocoles de cryptage, comme le protocole SSL, permettent de s'assurer que les données ne sont pas modifiées pendant leur transfert sur le réseau.

IV La preuve

Le principe de non-répudiation consiste à apporter la preuve non réfutable d'un acte malveillant. La non-répudiation est assurée par la combinaison de trois éléments : l'authentification, l'imputabilité et la traçabilité.

Authentification	Imputabilité	Traçabilité
L'authentification permet de s'assurer de la légitimité de la demande d'accès, et d'accorder les droits associés à celle-ci. La saisie d'un identifiant et d'un mot de passe peut être une solution d'authentification.	L'imputabilité désigne la possibilité d'attribuer la responsabilité d'un acte à une personne clairement identifiée.	La traçabilité permet de fournir un historique de l'utilisation d'un système d'information pour disposer d'une preuve des actions menées sur des données.

> **Exemple :** en cas d'action malveillante sur un service informatique de l'organisation, le fichier de journalisation (*log*) doit permettre de prouver qui est intervenu et sur quel service, afin d'apporter la preuve de l'acte.

La méthode EBIOS Risk Manager

I Présentation de la méthode EBIOS Risk Manager

> Guide de la méthode EBIOS Risk Manager : www.lienmini.fr/6988-002

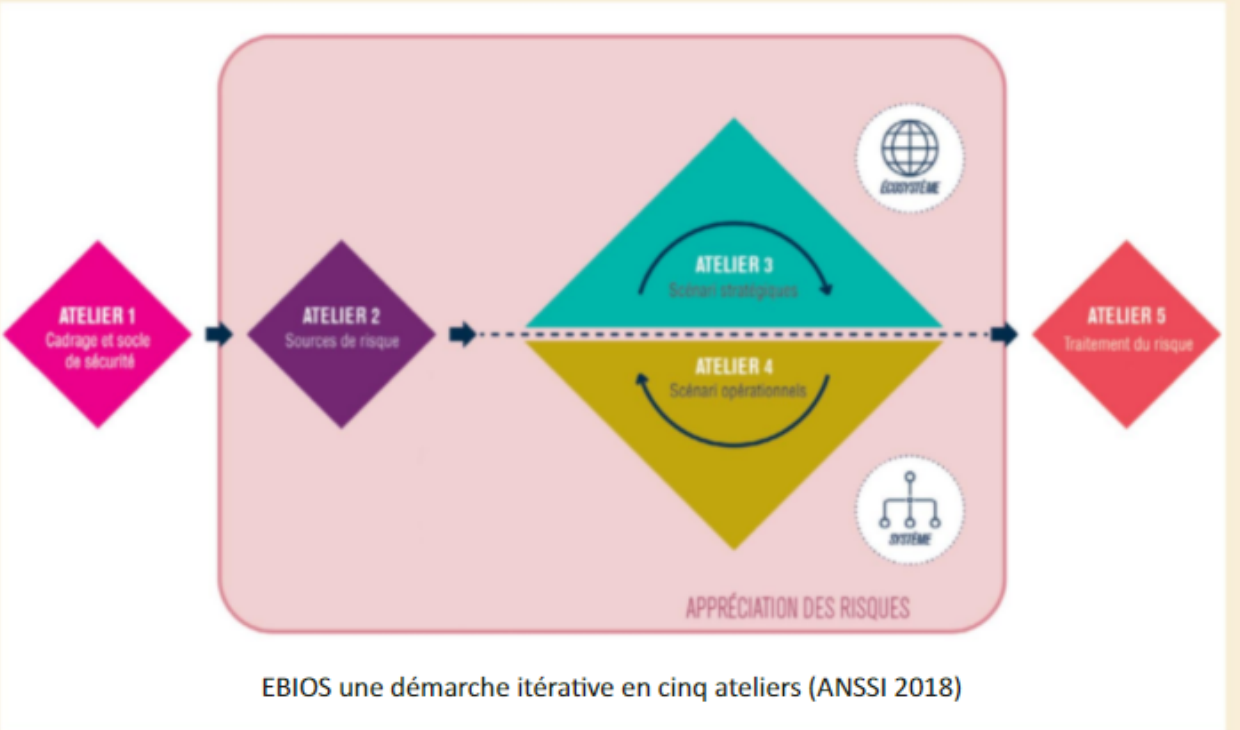
La méthode EBIOS (expression des besoins et identification des objectifs de sécurité) Risk Manager (RM) est présentée par l'ANSSI comme une « boîte à outils ». Elle donne les lignes directrices pour identifier, analyser et traiter les risques en sécurité de l'information. Il s'agit d'un outil de gestion de risques complet, régulièrement mis à jour et conforme aux référentiels normatifs internationaux.

EBIOS RM repose sur une approche d'appréciation de risques allant du plus global au plus précis. Ainsi, cette approche va du plus simple en termes de scénarios d'attaques, au plus élaboré. Elle vise à obtenir une synthèse entre l'approche par conformité et celle par scénarios.

Ainsi, en plus de permettre de conduire une analyse de risque complète et fine sur un processus ou une activité spécifique de l'organisation, elle permet :
– d'identifier le socle de sécurité de l'organisation ;
– d'être en conformité avec les référentiels de sécurité numérique de la CNIL et de l'ANSSI ;
– d'évaluer le niveau de menace de l'écosystème de l'objet de l'analyse ;
– d'identifier les axes prioritaires d'amélioration de la sécurité par la réalisation d'une étude préliminaire du risque.

II Les étapes de la méthode EBIOS Risk Manager

EBIOS RM consiste en une approche en cinq ateliers. L'approche par conformité est utilisée pour déterminer le socle de sécurité sur lequel s'appuie l'approche par scénarios pour élaborer ceux de risque particulièrement ciblés ou sophistiqués.



EBIOS une démarche itérative en cinq ateliers (ANSSI 2018)

> Voir lexique BTS SIO, p. 221

1. Atelier 1 : Cadrage et socle de sécurité

ÉCHELLE	CONSÉQUENCES
G4 CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 SIGNIFICATIVE	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

EBIOS, niveaux de gravité (ANSSI 2018)

L'atelier 1 suit une approche par conformité, ce qui permet d'aborder l'étude du point de vue de la défense. L'objectif de cet atelier, est de recenser les missions, valeurs métier (ou biens essentiels comme un identifiant, un mot de passe, voire les données des utilisateurs) et biens supports relatifs à l'objet étudié (comme un serveur, un poste, un logiciel ou un commutateur). L'atelier vise donc à identifier l'objet de l'étude. Ensuite, il faut identifier les événements redoutés associés aux valeurs métier et évaluer la gravité de leur impact.

2. Atelier 2 : Sources de risque

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

Le but de l'atelier 2 est d'identifier les sources de risque (SR) et leurs objectifs visés (OV). L'objectif est de répondre à la question suivante : qui ou quoi pourrait porter atteinte aux missions et valeurs métier identifiés dans l'atelier 1, et dans quel but ? Les sources de risque et les objectifs visés sont ensuite évalués. Au final, les couples SR/OV jugés les plus pertinents sont retenus à la fin de cet atelier. Ils seront utiles à la construction des scénarios des ateliers 3 et 4.

3. Atelier 3 : Scénarios stratégiques

• **Compréhension de l'écosystème**

L'atelier 3 permet d'avoir une vision claire de l'écosystème et des menaces. L'écosystème comprend l'ensemble des parties qui gravitent autour de l'objet de l'étude et concourent à la réalisation de ses missions comme des partenaires, des sous-traitants. De plus en plus de modes opératoires d'attaque exploitent les maillons les plus vulnérables de cet écosystème pour atteindre leur objectif, comme par exemple le fait de viser la disponibilité d'un service en attaquant le fournisseur de cloud.

› Voir lexique BTS SIO, p. 221

• **Élaboration de scénarios stratégiques**

L'objectif de l'atelier 3 est d'avoir une vision claire de l'écosystème, afin d'identifier les parties les plus vulnérables. Il s'agit ensuite de bâtir des scénarios de haut niveau, appelés scénarios stratégiques. Ces derniers sont autant de chemins d'attaque que pourrait emprunter une source de risque pour atteindre son objectif. Ils sont évalués en termes de gravité. À l'issue de cet atelier, il est déjà possible de définir des mesures de sécurité sur l'écosystème. Les scénarios stratégiques retenus dans l'atelier 3 constituent la base des scénarios opérationnels de l'atelier 4.

SOURCES DE RISQUE	OBJECTIFS VISÉS	CHEMINS D'ATTAQUE STRATÉGIQUES	GRAVITÉ
Concurrent	Voler des informations en espionnant les travaux de R&D en vue d'obtenir un avantage concurrentiel	Trois chemins d'attaque à investiguer. Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données : 1. portant directement sur le système d'information de la R&D ; 2. sur le système d'information du laboratoire (P3), qui détient une partie des travaux ; 3. passant par le prestataire informatique F3.	**3 Grave**

4. Atelier 4 : Scénarios opérationnels

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

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

5. Atelier 5 : Traitement du risque

Le dernier atelier consiste à réaliser une synthèse de l'ensemble des risques étudiés pour définir une stratégie de traitement du risque. Lors de cet atelier, on établit la synthèse des risques résiduels et le cadre de suivi des risques est défini.

Le processus de la méthode EBIOS (RM)

> Voir lexique BTS SIO, p. 221