LOGO ENTREPRISE

Nom Entreprise

Département

Service

**Analyse de risques cyber**

**du système ……**

**ANNEXE I** à la note d’envoi

N° …/……………… du …/xx/2020

**CONFIDENTIALITÉ**

**MENTION**

Ce document ne doit être communiqué qu’aux personnes qualifiées pour le connaitre

|  |  |  |
| --- | --- | --- |
| **Objet** | **Grade – Nom** | **Organisme – Fonction** |
| **Rédacteur** |  |  |
| **Participants** |  |  |
| **Vérification** |  |  |
| **Validation** |  |  |
| **Méthodologie**  **et outil** | - Méthode EBIOS Risk Manager publiée en fin d’année 2018 par l’ANSSI  - Logiciel Agile Risk Manager de la société All4TEC labelisé par l’ANSSI | |
| **Métriques**  **-**  **Référentiels** | - [Appendice I : Echelle de gravité](#APPENDICE_I)  - [Appendice II : Echelle des besoins de sécurité](#APPENDICE_II)  - [Appendice III : Echelle d’évaluation des couples SR/OV](#APPENDICE_III)  - [Appendice IV : Composition du socle de sécurité](#APPENDICE_IV)  - [Appendice V : Echelle d’évaluation des parties prenantes](#APPENDICE_V)  - [Appendice VI : Echelle de vraissemblance](#APPENDICE_VI)  - [Appendice VII : Glossaire méthode EBIOS Risk Manager](#APPENDICE_VII) | |

**SOMMAIRE**

[1. CADRAGE ET SOCLE DE SECURITE 4](#_Toc53000225)

[1.1. Cadre de l’étude 4](#_Toc53000226)

[1.2. Périmètre métier et technique 4](#_Toc53000227)

[1.2.1. Présentation du système dans son environnement 4](#_Toc53000228)

[1.2.2. Analyse Fonctionnelle 4](#_Toc53000229)

[1.2.3. Valeurs Métiers 6](#_Toc53000230)

[1.2.4. Biens supports 6](#_Toc53000231)

[1.2.5. Synthèse du périmètre métier et technique 7](#_Toc53000232)

[1.3. Identification des événements redoutés 8](#_Toc53000233)

[1.4. Besoins de sécurité 9](#_Toc53000234)

[1.5. Socle de sécurité 10](#_Toc53000235)

[2. SOURCES DE RISQUES ET OBJECTIFS VISES 11](#_Toc53000236)

[2.1. Sources de risques 11](#_Toc53000237)

[2.2. Objectifs visés 12](#_Toc53000238)

[2.3. Evaluation des sources des couples de risques et objectifs visés 13](#_Toc53000239)

[3. SCENARIOS STRATEGIQUES 14](#_Toc53000240)

[3.1. Elaboration de la cartographie de la menace numérique et sélection des parties prenantes critiques 14](#_Toc53000241)

[3.1.1. Phases de vies du SI 14](#_Toc53000242)

[3.1.2. Description des parties prenantes 14](#_Toc53000243)

[3.1.3. Evaluation des parties prenantes 15](#_Toc53000244)

[3.1.4. Représentation de la cartographie de la menace numérique de l’écosystème 16](#_Toc53000245)

[3.2. Elaboration des scénarios stratégiques 17](#_Toc53000246)

[3.2.1. Scénarios stratégiques retenus 17](#_Toc53000247)

[3.2.2. Représentations des scénarios stratégiques retenus 18](#_Toc53000248)

[3.3. Mesures de sécurité sur l’écosystème 22](#_Toc53000249)

[3.4. Evaluation du niveau de menace résiduelle des parties prenantes 23](#_Toc53000250)

[3.5. Représentation de la cartographie de la menace numérique résiduelle de l’écosystème 24](#_Toc53000251)

[4. SCENARIOS OPERATIONNELS 25](#_Toc53000252)

[4.1. Elaboration des scénarios opérationnels 25](#_Toc53000253)

[4.2. Evaluation de la vraisemblance 25](#_Toc53000254)

[5. TRAITEMENT DU RISQUE 26](#_Toc53000255)

[5.1. Synthèse des scénarios de risques 26](#_Toc53000256)

[5.2. Identification des mesures de sécurité de traitement du risque – Plan d’Amélioration Continue de la Sécurité (PACS) 26](#_Toc53000257)

[Appendice I : Echelle de gravité 27](#_Toc53000258)

[Appendice II : Echelle des besoins de sécurité 28](#_Toc53000259)

[Appendice III : Echelle d’évaluation des couples SR/OV 29](#_Toc53000260)

[Appendice IV : Composition du socle de sécurité 30](#_Toc53000261)

[Appendice V : Echelle d’évaluation des parties prenantes 31](#_Toc53000262)

[Appendice VI : Echelle de vraissemblance 32](#_Toc53000263)

[Appendice VII : Glossaire méthode EBIOS Risk Manager 34](#_Toc53000264)

# CADRAGE ET SOCLE DE SECURITE

## Cadre de l’étude

La présente étude a pour objectifs :

* d’identifier et d’apprécier les risques opérationnels d’origine cyber,
* d’identifier les mesures de sécurité permettant de réduire les risques,

du NOM du SI au vu des différentes sources de risques auxquels il peut être exposé dans son environnement opérationnel.

## Périmètre métier et technique

Cette partie a pour objectifs de décrire les missions métiers réalisées par le système dans son environnement opérationnel en détaillant les fonctions, données et biens supports mis en œuvre.

### Présentation du système dans son environnement

La mission du NOM du SI est de ……….

Le périmètre de l’étude en lien avec le système ……. est constitué de :

…….

A ce jour, il est mis en œuvre par ……. depuis :

* ……..

### Analyse Fonctionnelle

L’objectif de ce paragraphe est de représenter sous la forme d’un schéma fonctionnel les processus, informations et bien supports essentiels mise en œuvre par le système dans le cadre de leurs recensements.

SMQ-CEAM/F-010 v1.7 du 19/11/2014

F.01 …………

F.02 …………

F.03 …………

F.04 …………

D.02

D.01

D.03

**Données du système**

**Schéma Fonctionnel …….**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **D.01** | **D.02** | **D.03** |
| **D.04** | **D.05** | **D.06** |

### Valeurs Métiers

Une valeur métier est un processus ou une information nécessaire au système pour accomplir sa mission.

Les descriptions des valeurs métiers de type « processus » et « données » sont listées dans tableau donné ci-après.

| **Valeurs Métiers** | | |
| --- | --- | --- |
| **Abrév.** | **Nom des fonctions/processus** | **Description des fonctions/processus** |
|  |  |  |

### Biens supports

| **Biens supports** | | |
| --- | --- | --- |
| **Abréviation** | **Bien support** | **Description des biens supports** |
|  |  |  |

Nota : les biens supports de types « personnes » du système et de l’écosystème sont considérés comme des parties prenantes (cf. [§ 3.1.2 Description des parties prenantes](#_Description_des_parties))

### Synthèse du périmètre métier et technique

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Synthèse du périmètre métier et technique** | | | | | | |
| **Mission** | **Valeurs métier** | | | **Biens supports** | | |
| **Nom** | **Nature** | **Responsables** | **Nom** | **Type** | **Responsables** |
|  |  |  |  |  |  |  |

## Identification des événements redoutés

Un événement redouté est associé à une valeur métier et se rapporte à l’impact d’une attaque sur un des critères de sécurité d’une valeur métier (ex : perte de disponibilité ou l’altération d’une fonction/service assurée par le SI objet de l’étude).

L’appréciation du degré de préjudice/impact des événements redoutés est réalisée selon l’échelle de gravité donnée en [appendice I](#APPENDICE_I), elle doit permettre de comparer objectivement l’importance des missions et des valeurs métiers.

Les événements redoutés **à exploiter** sont ceux des **scénarios stratégiques** (cf. [§ 3](#_SCENARIOS_STRATEGIQUES)) qui permettent à une source de risque d’atteindre son **objectif visé** (cf. [§ 2.2](#_Objectifs_visés)).

**Nota :**

Il n’y a pas d’événements redoutés relatifs à la confidentialité :

* des logiciels ….. (F03) ;
* des firmwares …… (F04);
* ………  ;

ceux-ci-ci ne représentant pas d’intérêt pour les sources de risques identifiées dans le cadre de cette analyse de risques cyber.

| **Evénements redoutés** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **☐[[1]](#footnote-1)** | **Valeur métier** | **Evénement redoutés** | **Description** | **Impacts opérationnel** | **Gravité** |
|  |  |  |  |  |  |

## Besoins de sécurité

Les tableaux ci-après définissent les besoins de sécurité auxquels doivent répondent les valeurs métiers (fonction, donnée) au regard de l’impact/gravité des événements redoutés auxquels ils sont « liés ».

| **Besoins de sécurité** | | | |
| --- | --- | --- | --- |
| **Valeur métier** | **Besoins de sécurité** | **Description évènement redouté** | **Gravité** |
|  |  |  |  |

## Socle de sécurité

L’objectif de ce paragraphe est d’identifier les éventuels **écarts** d’application des mesures de sécurité imposées/préconisées par les différents référentiels applicables au système et à son écosystème au cours de ses différentes phases de vies (cf. § [3.1.1](#_Phases_de_vie))

Les référentiels applicables au système et son écosystème sont listés en [appendice II](#APPENDICE_II).

Ces écarts d’applications seront repris dans l’élaboration des scénarios comme vulnérabilités potentiellement exploitables par les sources de risques.

|  |  |  |  |
| --- | --- | --- | --- |
| **Domaine** | **Référence** | **Description – Biens supports et/ou partie prenante** | **Etat d’application** |
|  |  |  |  |

# SOURCES DE RISQUES ET OBJECTIFS VISES

Ce paragraphe a pour objectif d’identifier les sources de risques (SR) et leurs objectifs visés (OV) en lien avec l’objet de l’étude, qui permettront en se plaçant du côté de l’attaquant dans les paragraphes suivants afin d’élaborer les scénarios stratégiques et opérationnels.

## Sources de risques

Une source de risque est un élément, une personne, un groupe de personnes susceptible d’engendrer un risque. Les sources de risques peuvent collaborer de façon opportuniste ou organisée.

| **Sources de risques** | | | |
| --- | --- | --- | --- |
| **Source de risque** | **Abrév.** | **Catégorie** | **Description** |
|  |  |  |  |

## Objectifs visés

L’objectif visé est la finalité visée par une source de risque, selon ses motivations.

Si les objectifs visés ne portent pas toujours directement sur les valeurs métiers, atteindre ces objectifs implique en revanche l’occurrence d’un ou plusieurs évènements redoutés (cf. § [1.3](#_Identification_des_événements)).

| **Objectifs visés** | | | |
| --- | --- | --- | --- |
| **Objectif Visé** | **Abrév.** | **Catégorie** | **Description** |
|  |  |  |  |

## Evaluation des sources des couples de risques et objectifs visés

Le tableau suivant présente des couples Source de risque / Objectifs visés (SR/OV) envisagés.

Pour évaluer ces couples, les critères de motivation et de ressources de la source de risque ont été utilisés (cf. [appendice III](#APPENDICE_III)).

| **Couples sources et objectifs visés** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Identification** | | **Cotation** | | **Evaluation** | **Retenu** | **Observations** |
| **Source de risque** | **Objectif Visé** | **Motivation** | **Ressources** | **Pertinence** |
|  |  |  |  |  |  |  |

# SCENARIOS STRATEGIQUES

Après avoir identifié les objectifs des sources de risque, l’étude s’intéresse ici à l’environnement du système qui pourrait être utilisé pour mener une attaque informatique ciblée.

## Elaboration de la cartographie de la menace numérique et sélection des parties prenantes critiques

Ce paragraphe a pour objectif d’identifier les organismes ou systèmes d’information de l’écosystème pouvant constituer un vecteur d’attaque de par leurs accès numériques à l’objet de l’étude et à ses valeurs métiers, de leur vulnérabilité ou de leur exposition aux risques.

Ces parties prenantes, **internes** ou **externes** à l’organisation sont identifiées dans ce qui est appelée la **cartographie de la menace numérique de l’écosystème**.

Cette cartographie permet de faire apparaitre les parties prenantes d’intérêts au regard de leur niveau de menace vis-à-vis de l’objet de l’étude. Ces parties sont dites parties prenantes critiques.

### Phases de vies du SI

L’objectif de cette partie est de décrire les différentes phases de vies du système afin d’identifier les différents intervenants et « SI connexes » pouvant être connectés au SI objet de l’étude dans le cadre du recensement des parties prenantes de l’écosystème.

| **Phase** | **Description** | **SI en interface** | **Intervenants** |
| --- | --- | --- | --- |
| 0 | Production / Fabrication (chargement des logiciels, ….) | SI de production |  |
| 1 | Transport / supply chain |  |  |
| 2 | En service | Médias usagers |  |
| 3 | Maintien condition opérationnel ou de sécurité | PC maintenance  Médias MCO/MCS |  |

### 

### Description des parties prenantes

Les différentes parties prenantes listées ci-après ont été établies à partir des différents acteurs et « SI connexes » identifiés lors de la description des différents phases de vies du système (cf. § [3.1.1](#_Phases_de_vie)).

| **Description des parties prenantes** | | | |
| --- | --- | --- | --- |
| **☐[[2]](#footnote-2)** | **Catégorie** | **Nom** | **Définition** |
|  |  |  |  |

### Evaluation des parties prenantes

L’évaluation du niveau de menace des parties prenantes a été réalisée via la formule proposée par la méthode, sans aucune pondération, à savoir :

Niveau de menace = (dépendance x pénétration) / (maturité cyber x confiance).

L’[appendice V](#APPENDICE_V), présente les métriques de cotation de chacun de ces quatre critères.

| **Evaluation des parties prenantes** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Catégorie** | **Nom** | **Dépendance**  **Fonctionnelle** | **Degré de pénétration** | **Exposition** | **Maturité Cyber** | **Confiance** | **Fiabilité Cyber** | **Menace** |
|  |  |  |  |  |  |  |  |  |

### Représentation de la cartographie de la menace numérique de l’écosystème

|  |
| --- |
| **Cartographie de la menace numérique de l’écosystème** |
|  |

*L’*[*appendice V*](#APPENDICE_V)*, présente la définition du niveau des seuils des zones de menace.*

## Elaboration des scénarios stratégiques

L’élaboration des scénarios stratégiques a pour objectif d’identifier les points d’entrée, relais de propagation et vecteurs d’exploitation les plus pertinents dans une logique de moindre effort pour un attaquant. Ils découlent des couples (SR/OV) retenus au paragraphe [2.3](#_Evaluation_des_sources) et de l’identification des parties prenantes.

### Scénarios stratégiques retenus

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scénarios stratégiques retenus** | | | | | |
| **Couple SR/OV** | | | **Rx. Scénarios de risques stratégiques** | | **Gravité** |
| **☐[[3]](#footnote-3)** | **Source de risque** | **Objectif visé** | **Ref.** | **Nom** |
|  |  |  |  |  |  |

### Représentations des scénarios stratégiques retenus

#### Scénario stratégique 1.

**Illustration :**

|  |
| --- |
| **Illustration du scénario stratégique 1** |
|  |

**Tableau récapitulatif :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scénario stratégique 1** | | | | | |
| **Ref.** | **EI** | **Partie prenante** | **ER** | **Valeur métier** | **Bien support** |
|  |  |  |  |  |  |

#### Scénario stratégique 2.

**Illustration :**

|  |
| --- |
| **Illustration du scénario stratégique 2** |
|  |

**Tableau récapitulatif :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scénario stratégique 2** | | | | | |
| **Ref.** | **EI** | **Partie prenante** | **ER** | **Valeur métier** | **Bien support** |
|  |  |  |  |  |  |

## Mesures de sécurité sur l’écosystème

Après avoir identifié les parties prenantes critiques au travers de l’élaboration des scénarios stratégiques par lesquels les sources de risques pourraient réaliser leurs objectifs, ce paragraphe a pour objectif d’identifier les mesures de sécurité pouvant réduire le niveau de menace induit par celles-ci. Ces mesures viennent en complément de celles décrites dans le socle de sécurité au § [1.4](#_Socle_de_sécurité).

| **Mesures de sécurité de l’écosystème** | | | |
| --- | --- | --- | --- |
| **Nom** | **Description** | **Partie prenante** | **Scénarios**  **(EI+ER)** |
|  |  |  |  |

## Evaluation du niveau de menace résiduelle des parties prenantes

Les mesures de sécurité proposées précédemment ont principalement pour objectif d’augmenter la fiabilité cyber des parties prenantes. Certaines servent également à diminuer ou contenir le degré de pénétration de ces parties prenantes.

Les valeurs modifiées sont indiquées en gras.

| **Evaluation de la menace résiduelle des parties prenantes** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Mesure de sécurité** | **Partie Prenante** | **Dépendance**  **fonctionnelle** | **Degré de pénétration** | **Exposition** | **Maturité Cyber** | **Confiance** | **Fiabilité Cyber** | **Menace** |
|  |  |  |  |  |  |  |  |  |

## Représentation de la cartographie de la menace numérique résiduelle de l’écosystème

|  |
| --- |
| **Cartographie de la menace numérique résiduelle de l’écosystème** |
|  |

# SCENARIOS OPERATIONNELS

## Elaboration des scénarios opérationnels

#### Scénario opérationnel.

**Illustration :**

|  |
| --- |
| **Illustration du scénario opérationnel 1** |
|  |

## Evaluation de la vraisemblance

# TRAITEMENT DU RISQUE

## Synthèse des scénarios de risques

La synthèse de l’ensemble des scénarios de risques identifiés lors de l’étude (cf.3.2.1) est représentée dans la grille donnée ci-dessous. Cette représentation constitue la cartographie du risque initial avant traitement. Les risques identifiés peuvent être « accepté » ou « traité » en appliquant les mesures de sécurité listés dans le plan d’amélioration continue de la sécurité (cf. §5 .2).

## Identification des mesures de sécurité de traitement du risque – Plan d’Amélioration Continue de la Sécurité (PACS)

Appendice I : Echelle de gravité

La gravité représente une estimation de la hauteur des effets (impact) d'un événement redouté ou d'un risque. Elle représente ses conséquences.

|  |  |
| --- | --- |
| **Gravité** | **Description détaillée de l’échelle** |
| **1. Mineure** |  |
| **2. Significative** |  |
| **3. Grave** |  |
| **4. Critique** |  |
| **5.Catastrophique** |  |

Appendice II : Echelle des besoins de sécurité

Les échelles suivantes sont utilisées pour exprimer les besoins de sécurité en terme de confidentialité, intégrité et de disponibilité.

**1. Confidentialité**

|  |  |
| --- | --- |
| **Niveau de l’échelle** | **Désignation détaillée** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**2. Intégrité**

|  |  |
| --- | --- |
| **Niveau de l’échelle** | **Désignation détaillée** |
|  |  |
|  |  |
|  |  |
|  |  |

**3. Disponibilité**

|  |  |
| --- | --- |
| **Niveau de l’échelle** | **Désignation détaillée** |
|  |  |
|  |  |
|  |  |
|  |  |

Appendice III : Echelle d’évaluation des couples SR/OV[[4]](#footnote-4)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Ressources** | | | |
|  |  |  | Incluant les ressources financières, le niveau de compétences cyber, l’outillage, le temps dont l’attaquant dispose pour réaliser l’attaque, etc. | | | |
|  |  |  | Ressources limitées | Ressources significatives | Ressources importantes | Ressources illimitées |
| **Motivation** | Intérêts, éléments qui poussent la source de risque à atteindre son objectif | Fortement motivé | Moyennement pertinent | Plutôt pertinent | Très pertinent | Très pertinent |
| Assez motivé | Moyennement pertinent | Plutôt pertinent | Plutôt pertinent | Très pertinent |
| Peu motivé | Peu pertinent | Moyennement pertinent | Plutôt pertinent | Plutôt pertinent |
| Très peu motivé | Peu pertinent | Peu pertinent | Moyennement pertinent | Moyennement pertinent |

Appendice IV : Composition du socle de sécurité

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Appendice V : Echelle d’évaluation des parties prenantes

|  |  |  |  |
| --- | --- | --- | --- |
| **DÉPENDANCE** | **DEGRÉ DE PÉNÉTRATION** | **MATURITÉ CYBER** | **CONFIANCE** |
| 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. |
| 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. |
| 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. |
| 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. |

L’échelle de niveau de menace retenue pour l’évaluation des parties prenantes est donnée ci.

|  |  |  |
| --- | --- | --- |
| **Nom** | **Seuil** | **Couleur** |
| Zone de veille | 0.6 |  |
| Zone de contrôle | 1.4 |  |
| Zone de danger | 2.1 |  |

Appendice VI : Echelle de vraissemblance

**1. Cotation des actions élémentaires d’un scénarios opérationnel**

*1.1 Echelle de probabilité de succès d’une action élémentaire*

|  |  |
| --- | --- |
| V4 – Quasi certaine | Probabilité de succès quasi-certaine *>90%* |
| V3 – Très élevée | Probabilité de succès très élevée *>60%* |
| V2 – Significative | Probabilité de succès significative *> 20%* |
| V1 – Faible | Probabilité de succès faible *< 20%* |
| V0 – Très faible | Probabilité de succès très faible *<3%* |

*1.2 Echelle de difficulté technique d’une action élémentaire*

|  |  |
| --- | --- |
| D4 – Très élevée | Difficulté très élevée : l’attaquant engagera des ressources très importantes pour mener à bien son action. |
| D3 – Elevée | Difficulté élevée : l’attaquant engagera des ressources importantes pour mener à bien son action. |
| D2 – Modérée | Difficulté modérée : l’attaquant engagera des ressources significatives pour mener à bien son action. |
| D1 – Faible | Difficulté faible : les ressources engagées par l’attaquant seront faibles. |
| D0 – Négligeable | Difficulté négligeable, voire nulle : les ressources engagées par l’attaquant seront négligeables ou déjà disponibles. |

**2. Cotation des actions élémentaires d’un scénarios opérationnel**

*2.1 Matrice*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Difficulté technique du scénario opérationnel** | | | | |
|  |  | *0 - Négligeable* | *1 - Faible* | *2 - Modéré* | *3 - Elevée* | *4 – Très élevé* |
| **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 |

*2.2 Echelle de vraisemblance d’un scénario opérationnel*

|  |  |
| --- | --- |
| **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. |

*2.3 Echelle de vraisemblance d’un scénario opérationnel*

Dans les différents tableaux des risques, le niveau de vraisemblance associé à chaque risque correspond au niveau de vraisemblance maximal associé à chaque scénario de menaces associé au risque. Les sources de menaces sont communes pour les scénarios de menaces et les évènements redoutés.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Gravité** | 5. Catastrophique | Risque moyen | Risque moyen | Risque élevé | Risque élevé | Risque élevé |
| 4. Critique | Risque moyen | Risque moyen | Risque moyen | Risque élevé | Risque élevé |
| 3. Grave | Risque faible | Risque moyen | Risque moyen | Risque moyen | Risque élevé |
| 2. Significative | Risque faible | Risque faible | Risque moyen | Risque moyen | Risque moyen |
| 1. Mineure | Risque faible | Risque faible | Risque faible | Risque moyen | Risque moyen |
|  |  | 0. Invraisemblable | 1. Peu vraisemblable | 2. Vraisemblable | 3. Très vraisemblable | 4. Quasi-certain |
|  |  | **Vraisemblance** | | | | |

Appendice VII : Glossaire méthode EBIOS Risk Manager

**ANSSI :** Agence Nationale de la Sécurité et des Systèmes d’Information

**Action élémentaire :** action unitaire exécutée par une source de risque sur un bien support dans le cadre d’un scénario opérationnel.

*Exemples : exploiter une vulnérabilité, envoyer un mail piégé, effacer des traces, augmenter des privilèges.*

**Besoins de sécurité :** propriété de sécurité à garantir pour une valeur métier. Elle traduit un enjeu de sécurité pour la valeur métier.

*Exemples : disponibilité, intégrité, confidentialité, traçabilité.*

**Biens support :** composante du système d’information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle.

*Exemples : serveur, local technique, dispositif de vidéo protection, administrateurs.*

**Biens support critique :** bien support susceptible d’être ciblé par une source de risque pour atteindre son objectif. Les biens supports critiques sont ceux qui apparaissent dans les scénarios opérationnels.

**Cartographie de menace numérique de l’écosystème :** représentation visuelle du niveau de menace numérique des parties prenantes de l’écosystème vis-à-vis de l’objet étudié.

**Cartographie du risque :** représentation visuelle des risques issus des activités d’appréciation du risque.

**Chemin d’attaque :** suite d’événements distincts que la source de risque devra probablement générer pour atteindre son objectif. Cette terminologie concerne les scénarios stratégiques.

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

**Evènement redouté :** un événement redouté est associé à une valeur métier et porte atteinte à un critère ou besoin de sécurité de la valeur métier (exemple : indisponibilité d’un service, modification illégitime de données, divulgations de données classifiées). Les événements redoutés à exploiter sont ceux des scénarios stratégiques et se rapportent à l’impact d’une attaque sur une valeur métier. Chaque événement redouté est évalué selon le niveau de gravité des conséquences, à partir d’une métrique.

**Gravité :** estimation du niveau et de l’intensité des effets d’un risque. La gravité fournit une mesure des impacts préjudiciables perçus, qu’ils soient directs ou indirects.

**Menace :** terme générique utilisée pour désigner toute intention hostile de nuire dans le cyber espace. Une menace peut être ciblée ou non sur l’objet de l’étude.

**Mesures de sécurité :** moyen de traiter un risque prenant les formes de solutions ou d’exigences pouvant être inscrite dans un contrat.

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

**Mission :** fonction, finalité, raison d’être de l’objet de l’étude

**Mode opératoire :** suite d’actions élémentaires que la source de risque devra probablement réaliser pour atteindre son objectif. Cette terminologie concerne les scénarios opérationnels.

**Niveau de menace d’une partie prenante :** donne une mesure du potentiel de risque que fait peser une partie prenante de l’écosystème sur l’objet de l’étude, compte tenu de son interaction avec lui, de sa vulnérabilité, de son exposition au risque, de sa fiabilité, etc.

**Objectif visé (OV) :** finalité visée par une source de risque, selon ses motivations.

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

**Partie prenante :** élément de l’écosystème (personne, système d’information ou organisation) qui peut être interne ou externe à l’organisation de l’objet de l’étude.

*Exemples : partenaire, prestataire, client, fournisseur, filiale, service connexe support.*

**Partie prenante critique :** partie prenante de l’écosystème susceptible de constituer un vecteur d’attaque privilégié, du fait par exemple de son accès numérique privilégié à l’objet de l’étude, de sa vulnérabilité ou de son exposition au risque. Les parties prenantes critiques sont identifiées dans la cartographie de menace numérique de l’écosystème.

**Risque initial :** scénario de risque évalué avant application de la stratégie de traitement du risque. Cette évaluation repose sur la gravité et la vraisemblance du risque.

**Risque résiduel :** scénario de risque subsistant après application de la stratégie de traitement du risque. Cette évaluation repose sur la gravité et la vraisemblance du risque.

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

*Nota : dans la méthode EBIOS Risk Manager est considéré uniquement les scénarios de risque numérique intentionnel.*

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

**Scénarios stratégique:** chemins d’attaque allant d’une source de risque à un objectif visé en passant par l’écosystème et les valeurs métier de l’objet étudié. Les scénarios stratégiques sont évalués en termes de gravité.

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

*Exemples : services étatiques, hacktivistes, concurrents, employés vengeurs.*

**Stratégie de traitement du risque :** la stratégie de traitement du risque formalise les seuils d’acceptation du risque et un niveau de sécurité à atteindre en cas de non acceptation. Elle se réalise à partir de la cartographie du risque initial : pour chaque risque issu des activités d’appréciation du risque, la stratégie de traitement doit définir l’acceptabilité du risque (ex : inacceptable, tolérable, acceptable). Habituellement l’acceptabilité est directement déduite du niveau de risque et la stratégie en est la simple formalisation. Le rôle de la stratégie de traitement du risque est de décider de l’acceptation de chaque risque à la lumière des activités d’appréciations.

**Surface d’attaque :** concept utilisé pour évaluer le caractère avéré d’une vulnérabilité et la probabilité qu’elle soit exploitée par un attaquant.

**Valeur métier :** dans le cadre de l’étude composante importante pour l’organisation dans l’accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet ou toute information ou savoir-faire associé.

*Nota : les valeurs métiers représentent le patrimoine informationnel qu’une source de risque aurait intérêt à attaquer pour porter atteinte à l’objet de l’étude.*

**Vraisemblance :** estimation de la faisabilité ou de la probabilité qu’un risque se réalise, selon l’échelle adoptée (très faible, peu vraisemblable, ..).

**Vraisemblance élémentaire :** vraisemblance d’une action élémentaire identifiée dans un scénario opérationnel. Elle peut être jugement d’un expert ou à l’aide d’échelles. L’évaluation confronte d’une part les ressources et la motivation présumée des sources de risque et d’autre part le socle de sécurité de l’objet étudié et le niveau de vulnérabilité de l’écosystème (surface d’attaque exposée, vulnérabilités structurelles et organisationnelles, capacité de détection et de réaction, …).

**Vulnérabilité :** faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l’installation ou la configuration d’un système, ou dans la façon de l’utiliser. Une vulnérabilité peut être utilisée par un code d’exploitation et conduire à une intrusion dans le système.

1. ☑Evénement retenu - ☐ Evènement non retenu [↑](#footnote-ref-1)
2. ☑Evénement retenu - ☐ Evènement non retenu [↑](#footnote-ref-2)
3. ☑Evénement retenu - ☐ Evènement non retenu [↑](#footnote-ref-3)
4. Sources de risques / Objectifs visés [↑](#footnote-ref-4)