

**Réalisation d’un exemple de matrice de rapport de sortie**

**Matrice de rapport de sortie**

|  |  |  |
| --- | --- | --- |
| **Date** | : | 19/01/2021 |
| **Statut** | : | en cours |
| **Confidentialité** | : | NON PROTEGE |
| **Nombre de pages** | : | 33 |
| **Réalisation** |  | Document réalisé par le club EBIOS |
| **Responsable des travaux** | : | GUILLOT Vincent – Armée de l’Air et de l’espace |
| **Contributeurs** |  | HANNA Georges – SERMA NES  HEDOUX Tony – ALL4TEC  OLIVE Jean – CGI  PAUL Stéphane – Thales  REY Sébastien – Armée de l’Air et de l’espace  VAN CAUTER Nicolas – Thales  VIE Anne Catherine – ALL4TEC |
| **Validation** | : | Groupe de travail |
| **Approbation** | : | Conseil d’administration |
| **Licence** | : |  |

**Historique des modifications**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Objet de la modification** | **Auteur(s)** | **Statut** |
| 19/01/2020 | Création initiale | GUILLOT Vincent | Document de travail |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Préface**

**Préambule :**

Le présent document est un modèle de rapport d’analyse des risques par application de la méthode EBIOS Risk Manager.

La méthode est une boîte à outils d’identification et de gestion des risques. En ce sens, toutes les étapes et techniques proposées dans les guides de l’ANSSI ne sont pas obligatoirement complètement utilisées dans une étude. De ce fait, le présent modèle est adaptable : les chapitres ou sous-chapitres peuvent être supprimés ou les tableaux peuvent être modifiés, en respect des règles précisées ci-dessous, afin de s’adapter aux pratiques de l’utilisateur et à la finalité de l’étude.

**Utilisation de la matrice :**

La matrice de rapport peut être utilisée :

* directement à l’aide d’une application de traitement de texte tel que WORD afin de compléter les différents tableaux et graphiques,
* et/ou à l’aide d’un script Python permettant d’insérer les données dans les tableaux WORD présentent dans des tableaux Excel.

Pour utiliser le script Python, le **titre** des tableaux et l’**agencement** des colonnes doivent être conservés.

L’interface graphique du script permet de choisir le ou les éléments (tableaux, graphiques) concernés par l’import de données. Une fois que les travaux d’import sont réalisés, les titres des tableaux peuvent être retirés.

Les tableaux EXCEL peuvent être réalisés manuellement ou à l’aide d’une application labellisée EBIOS Risk Manager par l’ANSSI.

Le script est actuellement utilisé par différents utilisateurs avec la matrice au format WORD présentée ci-après et des fichiers EXCEL produits par l’application Agile Risk Manager d’ALL4TEC.

La réalisation de ce script en langage Python et de sa documentation font l’objet d’une contribution distincte du club EBIOS.

Nota : la conception du script permet de l’adapter afin de changer l’ordre et le choix des colonnes retenues.

**Convention d’écriture :**

Les textes :

* surlignés en gris sont à personnaliser ou à compléter,
* *en italiques et surlignés en vert* sont des notes à l’attention du rédacteur,
* écrits en bleu sont des exemples à remplacer.



Nom Entreprise

Département

Service

**« Analyse de risques cybersécurité**

**du système Ω »**

|  |
| --- |
| **NIVEAU DE CONFIDENTIALITÉ[[1]](#footnote-2) À PRÉCISER**  Ce document ne doit être communiqué qu’aux personnes qualifiées pour le connaître. |

|  |  |  |
| --- | --- | --- |
| **Objet** | **Description** | |
| **Rédacteur(s)** |  |  |
| **Contributeur(s)** |  | |
| **Version** | du xx/xx/202x | Création initiale |
| **Confidentialité1** | non protégé | |
| **Licence** |  | |
| **Méthodologie** | Méthode EBIOS Risk Manager publiée en fin d’année 2018 par l’ANSSI | |
| **Métriques**  **-**  **Référentiels** | - [Appendice I : Échelle des besoins de sécurité](#APPENDICE_I)  - [Appendice II : Échelle de gravité](#Appendice_II)  - Appendice III : Catégories de [sources](#Appendice_III) de risques et d’objectifs visés  - [Appendice IV : Échelle d’évaluation des couples SR/OV](#Appendice_IV)  -- [Appendice V : Échelle d’évaluation des parties prenantes](#Appendice_V)  - [Appendice VI : Échelle de vraisemblance](#Appendice_VI)  - [Appendice VII : Glossaire méthode EBIOS Risk Manager](#Appendice_VII) | |

**SOMMAIRE**

[0. SYNTHESE 7](#_Toc62144122)

[1. CADRAGE ET SOCLE DE SECURITE 7](#_Toc62144123)

[1.1. Cadre de l’étude 7](#_Toc62144124)

[1.2. Périmètre métier et technique 7](#_Toc62144125)

[1.2.1. Présentation du système dans son environnement 7](#_Toc62144126)

[1.2.2. Analyse fonctionnelle 7](#_Toc62144127)

[1.2.3. Valeurs Métier 9](#_Toc62144128)

[1.2.4. Biens supports 9](#_Toc62144129)

[1.2.5. Synthèse du périmètre métier et technique 10](#_Toc62144130)

[1.3. Identification des événements redoutés 10](#_Toc62144131)

[1.4. Relation entre les besoins de sécurité des valeurs métier et la gravité des événements redoutés 11](#_Toc62144132)

[1.5. Socle de sécurité 11](#_Toc62144133)

[2. SOURCES DE RISQUE ET OBJECTIFS VISÉS 12](#_Toc62144134)

[2.1. Sources de risque 12](#_Toc62144135)

[2.2. Objectifs visés 12](#_Toc62144136)

[2.3. Évaluation des couples de sources de risques et objectifs visés 13](#_Toc62144137)

[3. SCENARIOS STRATEGIQUES 13](#_Toc62144138)

[3.1. Elaboration de la cartographie de la menace numérique et sélection des parties prenantes critiques 13](#_Toc62144139)

[3.1.1. Description des parties prenantes 14](#_Toc62144140)

[3.1.2. Évaluation des parties prenantes 14](#_Toc62144141)

[3.1.3. Représentation de la cartographie de la menace numérique initiale de l’écosystème 15](#_Toc62144142)

[3.2. Élaboration des scénarios stratégiques 15](#_Toc62144143)

[3.2.1. Représentations des scénarios stratégiques 16](#_Toc62144144)

[3.2.2. Scénarios stratégiques identifiés 17](#_Toc62144145)

[3.3. Mesures de sécurité sur l’écosystème 18](#_Toc62144146)

[3.4. Évaluation du niveau de menace résiduelle des parties prenantes 18](#_Toc62144147)

[3.5. Représentation de la cartographie de la menace numérique résiduelle de l’écosystème 19](#_Toc62144148)

[4. SCÉNARIOS OPÉRATIONNELS 19](#_Toc62144149)

[4.1. Élaboration des scénarios opérationnels 19](#_Toc62144150)

[4.1.1. Modélisation et évaluation des modes opératoires du chemin d’attaque Rxx 20](#_Toc62144151)

[5. TRAITEMENT DU RISQUE 21](#_Toc62144152)

[5.1. Stratégie et appétence au risque et objectifs de sécurité 21](#_Toc62144153)

[5.2. Synthèse des scénarios de risques 21](#_Toc62144154)

[5.3. Identification des mesures de sécurité de traitement du risque – Plan d’Amélioration Continue de la Sécurité (PACS) 23](#_Toc62144155)

[5.3.1. Couverture des risques par les mesures 23](#_Toc62144156)

[5.3.2. Suivi de la mise en œuvre des mesures de sécurité 23](#_Toc62144157)

[5.3.3. Tableau des risques résiduels 24](#_Toc62144158)

[5.3.4. Cartographie des risques résiduels 24](#_Toc62144159)

[Appendice I : Échelles des besoins de sécurité 25](#_Toc62144160)

[Appendice II : Échelle de gravité 26](#_Toc62144161)

[Appendice III : Catégories de sources de risque (SR) et d’objectifs visés (OV) 27](#_Toc62144162)

[Appendice IV : Échelle d’évaluation des couples SR/OV 28](#_Toc62144163)

[Appendice V : Échelle d’évaluation des parties prenantes 29](#_Toc62144164)

[Appendice VI : Échelles pour le calcul de la vraisemblance d’un scénario opérationnel 30](#_Toc62144165)

[Appendice VII : Glossaire méthode EBIOS Risk Manager 32](#_Toc62144166)

# SYNTHESE

L’objectif de ce paragraphe est de donner à titre indicatif une liste non exhaustive des thèmes pouvant être abordés lors de la synthèse de l’étude :

* sujet de l’étude,
* principales hypothèses et contraintes,
* risques inhérents / initiaux,
* principaux éléments du plan de traitement des risques,
* risques résiduels,
* PV d’acceptation des risques résiduels (s’il existe).

*Note pour le rédacteur : cette synthèse peut être formalisée au travers d’un paragraphe d’introduction du rapport d’analyse ou d’un document séparé accompagnant le rapport d’analyse.*

# 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 traiter les risques,

du système Ω au vu des différentes sources de risque auxquelles il peut être exposé dans son environnement de développement / de production / de déploiement / opérationnel.

Le périmètre de l’étude ne prend pas en compte les éléments suivants ………………….

Cette étude a été réalisée avec les hypothèses et contraintes « budgétaire, calendaire, technique, … » suivantes :

* ……

dont certaines d’entre elles sont détaillées au travers du socle de sécurité (§1.5).

## Périmètre métier et technique

Cette partie a pour objectifs de décrire les missions réalisées par le système dans son environnement de développement / de production / de déploiement / opérationnel en détaillant les valeurs métier (i.e. processus, informations) et biens supports mis en œuvre.

### Présentation du système dans son environnement

Les missions du système Ω sont :

* ………………….
* ………………….

### Analyse fonctionnelle

L’objectif de ce paragraphe est de représenter sous la forme d’un schéma fonctionnel les processus, informations et biens supports essentiels mis en œuvre par le système.

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

*Note pour le rédacteur : la convention de mise en forme du schéma fonctionnel présentée ci- après est donnée à titre d’exemple (inspirée en partie de celle utilisée par le logiciel CAPELLA).*

**Schéma fonctionnel du système** Ω



**Bien support 1**



**Bien support 2**



**Bien support 3**

**P.01 …………**



**Bien support 4**

**Bien support 5**



**P.04 ………**

**P.02 …………**

**P.03 …………**

**P.05 …………**

**Partie prenante 1**

**Partie prenante 1**

**Partie prenante 2**

**Périmètre**

**étudié**



**…….**

**…………**

**………..**



**……….**

**………..**



**I.01**

**I.02**

**I.05**

**I.05**

**I.03**

**I.04**

**I.06**



**…………**

Figure 1 : Architecture fonctionnelle

Tableau 1 - Informations du système

|  |  |  |
| --- | --- | --- |
| **Informations du système** | | |
| **I.01 …………………..** | **I.02 …………………** | **I.03 ……………………..** |
| **I.04 …………………..** | **I.05 …………………** | **I.06 ……………………..** |

### Valeurs Métier

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

Les descriptions des valeurs métier de type « processus » et « informations » ainsi que leurs besoins de sécurité sont listés dans le tableau donné ci-après.

L’[appendice I](#APPENDICE_I), présente les métriques utilisées pour la définition des besoins de sécurité

Tableau 2 - Liste des valeurs métier

| **Valeurs métier** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Abrév.** | **Nom** | **Description** | **Besoins de sécurité** | | |
| **D** | **I** | **C** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### Biens supports

Tableau 3 - Liste des biens supports

| **Biens supports** | | |
| --- | --- | --- |
| **Abrév.** | **Nom** | **Description** |
|  |  |  |
|  |  |  |
|  |  |  |

*Note pour le rédacteur : il est recommandé d’identifier de manière « unique » les éléments du système/écosystème (entités/personnes, …) soit en tant que bien support soit en tant que partie prenante (cf. § 3.1.2).*

### Synthèse du périmètre métier et technique

Tableau 4 - 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

Les événements redoutés sont associés aux valeurs métier et se rapportent à l’impact d’une atteinte à un des critères de sécurité de ces valeurs métier (ex : perte de disponibilité ou l’altération d’une fonction assurée par l’objet de l’étude).

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

Les événements redoutés peuvent être accidentels, environnementaux ou intentionnels. Seuls les événements redoutés intentionnels associés à des attaques « ciblées » seront exploités lors de l’élaboration des scénarios stratégiques (cf. § 3.2).

Tableau 5 - Caractérisation des événements redoutés

| **Evénements redoutés** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **☐[[2]](#footnote-3)** | **Valeur métier** | **Abrév.** | **Nom** | **Description[[3]](#footnote-4)** | **Impacts** | **Gravité** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Relation entre les besoins de sécurité des valeurs métier et la gravité des événements redoutés

Le tableau ci-après présente les relations entre les besoins de sécurité des valeurs métiers (VM) et la gravité des événements redoutés (ER).

Tableau 6 - Relation entre les besoins de sécurité des VM et la gravité des ER

| **Relation entre les besoins de sécurité des valeurs métiers et la gravité des événements redoutés** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Valeur métier** | **Abrév.** | **Besoins de sécurité** | **Nom de l’évènement redouté** | **Abrév.** | **Gravité** |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |

## Socle de sécurité

L’objectif de ce paragraphe est de lister les différents référentiels applicables au système, et d’identifier les éventuels **écarts d’application** des mesures de sécurité imposées/préconisées pour le système au cours de ses différentes phases de vie.

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

Tableau 7 - Liste des référentiels applicables et leurs états d’application global

|  |  |  |
| --- | --- | --- |
| **Liste des référentiel applicables** | | |
| **Réf.** | **Désignation** | **Ecarts d’applications** |
|  |  |  |
|  |  |  |

Tableau 8 - Etat d’application des exigences de sécurité des référentiels applicables

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Etat d’application des référentiels applicables** | | | | | |
| **Domaine** | **Réf.** | **Nom exigence** | **Description** | **Eléments[[4]](#footnote-5)** | **Ecarts d’application** |
|  |  |  |  |  |  |

*Note pour le rédacteur : selon les besoins de l’étude il peut également être réalisé un tableau d’application par référentiel applicable.*

# SOURCES DE RISQUE ET OBJECTIFS VISÉS

Ce chapitre a pour objectif d’identifier et d’évaluer la pertinence des sources de risque (SR) et de leurs objectifs visés (OV), en se plaçant côté attaquant.

## Sources de risque

Une source de risque peut être un élément, une personne, un groupe de personnes, ou une typologie de personnes (administrateurs techniques, administrateurs fonctionnels, attaquants externes, etc.) susceptible d’engendrer un risque. Les sources de risque peuvent collaborer de façon opportuniste ou organisée.

L’[appendice III](#Appendice_III), présente les catégories de sources de risques (tableau 30) utilisées dans le cadre de cette étude.

Tableau 9 - Liste des sources de risque

| **Sources de risque** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **☐[[5]](#footnote-6)** | **Source de risque** | **Abrév.** | **Catégorie** | **Description** | **Justification** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## 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 métier, atteindre ces objectifs implique en revanche l’occurrence d’un ou plusieurs évènements redoutés (cf. §.1.3).

L’[appendice III](#Appendice_III), présente les catégories d’objectifs visés (tableau 31) utilisées dans le cadre de cette étude.

Tableau 10 - Liste des objectifs visés

| **Objectifs visés** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Objectif Visé** | **Abrév.** | **Catégorie** | **Source de risque** | **Description** | **Evénement(s) redouté(s) associé(s)** |
|  |  |  |  |  |  |

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

Le tableau suivant présente les couples Sources de Risque / Objectifs Visés (SR/OV) envisagés.

Pour évaluer ces couples, les critères de motivation, de ressources et d’activité de la source de risque sont utilisés (cf. [appendice I](#Appendice_IV)V).

Tableau 11 - Liste des couples Sources de Risque / Objectifs Visés

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

# 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 pouvant constituer un vecteur d’attaque de par leurs accès[[6]](#footnote-7) numériques à l’objet de l’étude et à ses valeurs métier, de leur vulnérabilité ou de leur exposition aux sources de risque.

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

Cette cartographie permet de faire apparaître 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.

### Description des parties prenantes

Les parties prenantes sont listées dans le tableau donné ci-après.

Tableau 12 - Liste des parties prenantes

| **Description des parties prenantes** | | |
| --- | --- | --- |
| **Catégorie** | **Nom** | **Description** |
|  |  |  |
|  |  |  |
|  |  |  |

### Évaluation 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.

Tableau 13 - Evaluation des parties prenantes (avant application du socle)

| **Évaluation des parties prenantes** | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Catégorie** | **Nom** | Dépendance | Pénétration | **Exposition** | Maturité cyber | Confiance | **Fiabilité cyber** | **Menace** | **☐[[7]](#footnote-8)** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

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

Figure - Cartographie de la menace initiale de l’écosystème

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

## Élaboration 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 (cf. 3.1.1).

### Représentations des scénarios stratégiques

#### Scénario stratégique <SR1/OV1> -

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

#### Scénario stratégique <SR1/OV1> -

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

*Note pour le rédacteur : généré autant de fois que nécessaire*

**Tableau récapitulatif :**

Tableau 14 - Détails des chemins d’attaque du scénario stratégique associé au couple SRxx/OVxx

|  |  |
| --- | --- |
| **Chemins d’attaque du scénario stratégique associé au couple « SR1/OV1 »** | |
| **Réf.** | **Nom** |
|  |  |
|  |  |
|  |  |

### Scénarios stratégiques identifiés

Tableau 15 - Récapitulatif des chemins d’attaque des scénarios stratégiques

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Scénarios stratégiques identifiés** | | | | | | |
| **Couple SR/OV** | | | **Chemins d’attaques** | | **Gravité** | **Justification** |
| **☐[[8]](#footnote-9)** | **Source de risque** | **Objectif visé** | **Réf.** | **Nom** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Mesures de sécurité sur l’écosystème

Ce paragraphe a pour objectif d’identifier les mesures de sécurité pouvant réduire le niveau de menace induit par les parties prenantes. Ces mesures viennent en complément de celles décrites dans le socle de sécurité au §1.5.

Tableau 16 - Socle de sécurité applicable sur l’écosystème

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Etat d’application du socle sur les Parties Prenantes** | | | | | |
| **Domaine** | **Référence** | **Nom exigence** | **Description** | **Partie Prenante** | **Ecarts d’application** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Tableau 17 - Mesures de sécurité permettant de réduire la menace représentée par les parties prenantes (PP)

| **Mesures de sécurité permettant de réduire la menace représentée par les PP** | | | |
| --- | --- | --- | --- |
| **Nom** | **Description** | **Partie prenante** | **Chemin d’attaque** |
|  |  |  |  |
|  |  |  |  |

## Évaluation 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 ou de diminuer l’exposition du système aux parties prenantes. Les valeurs modifiées sont indiquées **en gras.**

Tableau 18 - Evaluation des parties prenantes (après application du socle)

| **Évaluation de la menace résiduelle des parties prenantes** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Partie Prenante** | **Mesure de sécurité** | Dépendance | Pénétration | **Exposition** | Maturité cyber | Confiance | **Fiabilité Cyber** | **Menace** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

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

Figure 5 : Cartographie de la menace résiduelle de l’écosystème

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

# SCÉNARIOS OPÉRATIONNELS

## Élaboration des scénarios opérationnels

A chaque chemin d’attaque stratégique retenu dans l’atelier 3 correspond un scénario opérationnel permettant à la source de risque d’atteindre son objectif visé. La finalité de cet atelier est de modéliser le séquencement des actions élémentaires mises en œuvre par les sources de risque pour réaliser les scénarios stratégiques.

Cette modélisation est réalisée pour chacun des chemins d’attaques (R1, R2, …) afin d’évaluer la vraisemblance des scénarios de risque.

*Nota : les types d’actions élémentaires utilisés sont ceux fournis par …….*

L’ANSSI propose trois approches pour coter la vraisemblance du scénario opérationnel : (i) méthode expresse; (ii) méthode standard; (iii) méthode avancée.

Il a été fait ici le choix de suivre la méthode ………..

L’[appendice VI](#Appendice_VI) présente les métriques utilisées.

### Modélisation et évaluation des modes opératoires du chemin d’attaque R1

|  |
| --- |
| Illustration du scénario opérationnel R1 |
|  |

### Modélisation et évaluation des modes opératoires du chemin d’attaque R2

|  |
| --- |
| Illustration du scénario opérationnel R2 |
|  |

### Modélisation et évaluation des modes opératoires du chemin d’attaque R3

|  |
| --- |
| Illustration du scénario opérationnel R3 |
|  |

### Modélisation et évaluation des modes opératoires du chemin d’attaque R4

|  |
| --- |
| Illustration du scénario opérationnel R4 |
|  |

### Modélisation et évaluation des modes opératoires du chemin d’attaque R5

|  |
| --- |
| Illustration du scénario opérationnel R5 |
|  |

# TRAITEMENT DU RISQUE

## Stratégie et appétence au risque et objectifs de sécurité

Pour chaque scénario de risque, des seuils d’acceptation du risque et un niveau de sécurité à atteindre en cas de non acceptation ont été déterminés. Ces décisions se formalisent dans la stratégie de traitement du risque présentée ci-dessous.

*Note pour le rédacteur : le tableau présenté ci-après est donné à titre d’exemple*

Tableau 19 - Niveaux de risques

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | **Acceptabilité du risque** | **Intitulé des décisions et des actions** |
| Faible | Acceptable en l’état | Aucune action n’est à entreprendre. |
| Moyen | Tolérable sous contrôle | Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d’une amélioration continue sur le moyen et long terme. |
| Elevé | Inacceptable | Des mesures de réduction du risque doivent impérativement être prises à court terme. Dans le cas contraire, toute ou une partie de l’activité sera refusée. |

Le tableau ci-après présente la matrice d’appétence aux risques utilisée pour cette analyse.

Tableau 20 - Matrice d’appétence aux risques

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

*Note pour le rédacteur : présenter ici la stratégie de réduction du risque à travers les objectifs de sécurité identifiés avec le commanditaire*

## Synthèse des scénarios de risques

La synthèse de l’ensemble des scénarios de risques identifiés lors de l’étude (cf. 3.2.1 et 4.1) est représentée dans la grille donnée ci-dessous. Cette représentation constitue la **cartographie du risque initial** avant application des mesures du PACS.

|  |
| --- |
| Cartographie du risque initial |
|  |

Tableau 21 - Liste des risques initiaux / inhérents

|  |  |
| --- | --- |
| **Liste des risques initiaux / inhérents** | |
| **Réf.** | **Nom** |
| R1 |  |
| R2 |  |
| R3 |  |
| R4 |  |
| R5 |  |
| R6 |  |

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

L’objectif de ce paragraphe est d’identifier les mesures de sécurité additionnelles (par rapport aux mesures issues des ateliers 1 et 3) permettant de réduire le risque.

### Couverture des risques par les mesures

Tableau 22 - Couverture des risques par les mesures

| **Couverture des risques par les mesures** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Mesure de sécurité** | | | **Eléments associés[[9]](#footnote-10)**  **(BS, PP, VM)** | **Scénarios de risques associés** | | **Retenue** | **Justification** |
| **N°** | **Nom** | **Domaine** | **Réf°** | **Nom** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

### Suivi de la mise en œuvre des mesures de sécurité

Tableau 23 - Plan de mise en œuvre des mesures de sécurité additionnelles

| **Plan de mise en œuvre des mesures de sécurité additionnelles** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Mesure de sécurité** | | **Eléments d’appréciation** | | | **Mise en œuvre** | | |
| **N°** | **Nom** | **Freins / difficulté** | **Coût / complexité** | **Priorité** | **Responsable** | **Echéance** | **Statut** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

*Note pour le rédacteur : le suivi de la mise en place des mesures de sécurité peut être effectué au travers d’un document spécifique.*

### Tableau des risques résiduels

Les risques résiduels listés ci-après sont les risques persistant après application des mesures de sécurité retenues.

Tableau 24 - Tableau des risques résiduels

|  |  |
| --- | --- |
| **Liste des risques résiduels** | |
| **Réf.** | **Nom** |
| R1 |  |
| R2 |  |
| R3 |  |
| R4 |  |
| R5 |  |
| R6 |  |

### Cartographie des risques résiduels

|  |
| --- |
| Cartographie du risque résiduel |
|  |

Nota : les valeurs modifiées sont indiquées en gras

Appendice I : Échelles des besoins de sécurité

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

Tableau 25 - Echelle de confidentialité

|  |  |
| --- | --- |
| **Niveau de l’échelle** | **Désignation détaillée** |
| ……….  (1/4) |  |
| ……….  (2/4) |  |
| ……….  (3/4) |  |
| ……….  (4/4) |  |

Tableau 26 - Echelle d’intégrité

|  |  |
| --- | --- |
| **Niveau de l’échelle** | **Désignation détaillée** |
| ……….  (1/4) |  |
| ……….  (2/4) |  |
| ……….  (3/4) |  |
| ……….  (4/4) |  |

Tableau 27 - Echelle de disponibilité

|  |  |
| --- | --- |
| **Niveau de l’échelle** | **Désignation détaillée** |
| ……….  (1/4) |  |
| ……….  (2/4) |  |
| ……….  (3/4) |  |
| ……….  (4/4) |  |

Appendice II : Échelle de gravité

*Note pour le rédacteur : cette échelle est à adapter à l’étude.*

Tableau 28 - Echelle de gravité

|  |  |
| --- | --- |
| **Gravité** | **Description détaillée de l’échelle** |
| **Mineure**  **(1/4)** |  |
| **Significative**  **(2/4)** |  |
| **Grave**  **(3/4)** |  |
| **Critique**  **(4/4)** |  |

Appendice III : Catégories de sources de risque (SR) et d’objectifs visés (OV)

*Note pour le rédacteur : à compléter.*

Tableau 29 - Catégories de sources de risques

|  |  |
| --- | --- |
| **Catégorie**  **(profils d’attaquants)** | **Description** |
|  |  |
|  |  |
|  |  |
|  |  |

Tableau 30 - Catégorie d’objectifs visés

|  |  |
| --- | --- |
| **Catégorie**  **(finalités poursuivies)** | **Description** |
|  |  |
|  |  |
|  |  |
|  |  |

Appendice IV : Échelle d’évaluation des couples SR/OV[[10]](#footnote-11)

*Note pour le rédacteur : cette échelle est à adapter à l’étude.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **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 motivée | Moyennement pertinent | Plutôt pertinent | Très pertinent | Très pertinent |
| Assez motivée | Moyennement pertinent | Plutôt pertinent | Plutôt pertinent | Très pertinent |
| Peu motivée | Peu pertinent | Moyennement pertinent | Plutôt pertinent | Plutôt pertinent |
| Très peu motivée | Peu pertinent | Peu pertinent | Moyennement pertinent | Moyennement pertinent |

Appendice V : Échelle d’évaluation des parties prenantes

*Note pour le rédacteur : cette échelle est à adapter à l’étude.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Niv.** | **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 peuvent être suspecte. |
| 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. |

Appendice VI : Échelles pour le calcul de la vraisemblance d’un scénario opérationnel

*Note pour le rédacteur : ces échelles sont à adapter à l’étude.*

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

1.1 Échelle de probabilité de succès d’une action élémentaire

|  |  |
| --- | --- |
| V5 – Quasi certaine | Probabilité de succès quasi-certaine *>90%* |
| V4 – Très élevée | Probabilité de succès très élevée *>60%* |
| V3 – Significative | Probabilité de succès significative *> 20%* |
| V2 – Faible | Probabilité de succès faible *< 20%* |
| V1 – Négligeable | Probabilité de succès très faible *<3%* |

1.2 Échelle de difficulté technique d’une action élémentaire

|  |  |
| --- | --- |
| D5 – Très élevée | Difficulté très élevée : l’attaquant engagera des ressources très importantes pour mener à bien son action. |
| D4 – Élevée | Difficulté élevée : l’attaquant engagera des ressources importantes pour mener à bien son action. |
| D3 – Modérée | Difficulté modérée : l’attaquant engagera des ressources significatives pour mener à bien son action. |
| D2 – Faible | Difficulté faible : les ressources engagées par l’attaquant seront faibles. |
| D1 – Négligeable | Difficulté négligeable, voire nulle : les ressources engagées par l’attaquant seront négligeables ou déjà disponibles. |

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

2.1 Matrice

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Difficulté technique du scénario opérationnel** | | | | |
|  |  | *1 - Négligeable* | *2 - Faible* | *3 - Modéré* | *4 - Elevée* | *5 – Très élevé* |
| **Probabilité de succès du scénario opérationnel** | *5 - Quasi Certaine* | 4 | 4 | 3 | 2 | 1 |
| *4 -Très élevée.* | 4 | 3 | 3 | 2 | 1 |
| *3 - Significative* | 3 | 3 | 2 | 2 | 1 |
| *2 – Faible* | 2 | 2 | 2 | 1 | 0 |
| *1 – Très faible* | 1 | 1 | 1 | 0 | 0 |

2.2 Échelle de vraisemblance d’un scénario opérationnel

|  |  |
| --- | --- |
| **Échelle** | **Description** |
| V5 - 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. |
| V4 - 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. |
| V3 - 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. |
| V2 - 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. |
| V1 - 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. |

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 sont considérés uniquement les scénarios de risque numérique intentionnel.

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

**Scénario stratégique :** 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 métier 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. Note pour le rédacteur : les terminologies « classification », « sensibilité » peuvent également être utilisées selon le contexte [↑](#footnote-ref-2)
2. ☑ Retenu ou ☐ Non retenu pour l’élaboration des scénarios stratégiques [↑](#footnote-ref-3)
3. Afin de pouvoir apprécier la gravité, la description de l’événement redouté doit permettre d’évaluer la nature et l’ampleur des impacts potentiels de celui-ci sur la ou les missions assurées par le système. [↑](#footnote-ref-4)
4. Eléments du système (biens supports voire parties prenantes dans certains cas) [↑](#footnote-ref-5)
5. ☑ Retenu - ☐ Non retenu [↑](#footnote-ref-6)
6. L’ensemble des phases de vie du système est à prendre en compte (cf. exploitation, maintenance, …) [↑](#footnote-ref-7)
7. ☑ Retenu - ☐ Non retenu au regard de la menace représentée par la partie prenante [↑](#footnote-ref-8)
8. ☑ Retenu - ☐ Non retenu [↑](#footnote-ref-9)
9. Bien support, partie prenante et/ou valeur métier [↑](#footnote-ref-10)
10. Sources de risque / Objectifs visés [↑](#footnote-ref-11)