|  |
| --- |
| Confidentiel |

Tél :

|  |
| --- |
| Draft / Final |

Ce rapport est généré à partir de la version 01.01 du projet le 15/06/21.

|  |  |  |  |
| --- | --- | --- | --- |
| **SUIVI DES EVOLUTIONS** | | | |
| **Révision** | **Date** | **Auteur** | **Modification** |
| **--** |  |  | Première version |
| **-A** |  |  |  |
| **-B** |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **APPROBATION** | | | | |
|  | **Nom** | **Rôle** | **Date** | **Signature** |
| **Créé ou modifié par** |  |  |  |  |
| **Vérifié par** |  |  |  |  |
| **Approuvé par** |  |  |  |  |
| **Approuvé par le client si nécessaire** |  |  |  |  |

**Sommaire**

[1 Activité 1 - Cadrage et socle de sécurité 6](#_Toc73371629)

[1.1 Activité 1.a - Cadrer l’étude 6](#_Toc73371630)

[1.1.1 Données principales 6](#_Toc73371631)

[1.1.2 Acteurs 7](#_Toc73371632)

[1.1.3 RACI 8](#_Toc73371633)

[1.2 Activité 1.b (Biens primordiaux/support) 9](#_Toc73371634)

[1.2.1 Valeur métier 9](#_Toc73371635)

[1.2.2 Bien support 10](#_Toc73371636)

[1.2.3 Mission 11](#_Toc73371637)

[1.3 Activité 1.c (Événement redoutés) 12](#_Toc73371638)

[1.3.1 Echelles 12](#_Toc73371639)

[1.3.1.1 Liste des échelles 12](#_Toc73371640)

[1.3.1.2 Détails des Niveaux d’échelles 13](#_Toc73371641)

[1.3.1.2.1 Détails des niveaux de l’échelle ${echelle\_X} 13](#_Toc73371642)

[1.3.1.2.2 Détails des niveaux de l’échelle ${echelle\_Y} 14](#_Toc73371643)

[1.3.2 Événements redoutés 15](#_Toc73371644)

[1.4 Activité 1.d - Les socles de sécurité 16](#_Toc73371645)

[1.4.1 Socle de sécurité 16](#_Toc73371646)

[1.4.2 Règles 17](#_Toc73371647)

[1.4.2.1 Etat de prise en compte du socle XXX 17](#_Toc73371648)

[2 Activité 2 - Sources de risque 18](#_Toc73371649)

[2.1 Activité 2.a - Identifier les sources de risques et les objectifs 18](#_Toc73371650)

[2.1.1 Sources de risque et objectifs visés 18](#_Toc73371651)

[2.2 Activité 2.b - Évaluer les couples sources de risque/objectifs visés 19](#_Toc73371652)

[2.2.1 Évaluation des sources de risques 19](#_Toc73371653)

[2.3 Activité 2.c - Sélectionner les couples SR/OV retenus pour la suite de l’analyse 20](#_Toc73371654)

[2.3.1 Choix des sources de risque 20](#_Toc73371655)

[2.3.2 Cartographie des "Source de risque / Objectif visé" 21](#_Toc73371656)

[3 Activité 3 - Scénarios stratégiques 22](#_Toc73371657)

[3.1 Activité 3.a -Construire la cartographie des menaces numériques de l'écosystème et sélectionner les parties prenantes critiques 22](#_Toc73371658)

[3.1.1 Création des seuils 22](#_Toc73371659)

[3.1.2 Parties prenantes 23](#_Toc73371660)

[3.1.2.1 Parties prenantes internes 24](#_Toc73371661)

[3.1.2.2 Parties prenantes externes 25](#_Toc73371662)

[3.2 Activité 3.b - Élaborer des scénarios stratégiques 26](#_Toc73371663)

[3.2.1 Liste des évènements redoutés établis à l'atelier 1.c 26](#_Toc73371664)

[3.2.2 Liste des couples sources de risques / objectifs visés retenus établis à l'atelier 2 27](#_Toc73371665)

[3.2.3 Scénarios stratégiques 28](#_Toc73371666)

[3.2.4 Chemins d'attaque 29](#_Toc73371667)

[3.3 Activité 3.c - Définir des mesures de sécurité sur l'écosystème 30](#_Toc73371668)

[3.3.1 Liste des parties prenantes établis à l'atelier 3.a 30](#_Toc73371669)

[3.3.2 Mesure de sécurité 31](#_Toc73371670)

[3.3.3 Évaluation 32](#_Toc73371671)

[3.3.4 Parties prenantes 33](#_Toc73371672)

[4 Activité 4 - Scénarios opérationnels 34](#_Toc73371673)

[4.1 Activité 4.a (Élaborer les scénarios opérationnels) 34](#_Toc73371674)

[4.1.1 Liste des scénarios stratégiques établis lors de l'atelier 3.b 34](#_Toc73371675)

[4.1.2 Scénario opérationel 35](#_Toc73371676)

[4.1.3 Liste des modes opératoires 36](#_Toc73371677)

[4.2 Activité 4.b - Évaluer la vraisemblance des scénarios opérationnels 37](#_Toc73371678)

[4.2.1 Liste des échelles 37](#_Toc73371679)

[4.2.2 Niveaux des échelles de vraisemblance 38](#_Toc73371680)

[4.2.3 Évaluer la vraisemblance des scénarios opérationnels 39](#_Toc73371681)

[5 Activité 5 - Traitement du risque 40](#_Toc73371682)

[5.1 Activité 5.a - Réaliser une synthèse des scénarios de risque 40](#_Toc73371683)

[5.1.1 Cartographie du risque initial 40](#_Toc73371684)

[5.2 Activité 5.b - Décider de la stratégie de traitement du risque et définir les mesures de sécurité 41](#_Toc73371685)

[5.2.1 Cartographie du risque initial 41](#_Toc73371686)

[5.2.2 Plan d’amélioration continue de la sécurité 42](#_Toc73371687)

[5.3 Activité 5.c - Évaluer et documenter les risques résiduels 43](#_Toc73371688)

[5.3.1 Évaluation et documentation des risques résiduels 43](#_Toc73371689)

[Cartographie du risque initial 44](#_Toc73371690)

[5.3.2 Cartographie du risque résiduel 45](#_Toc73371691)

[6 Annexes 46](#_Toc73371692)

**Liste des tableaux**

[Tableau 1 : Liste des acteurs 8](#_Toc73371693)

[Tableau 2: RACI 9](#_Toc73371694)

[Tableau 3 : Tableau des valeurs métiers 10](#_Toc73371695)

[Tableau 4 : Liste des biens supports 11](#_Toc73371696)

[Tableau 5 : Tableau des missions 12](#_Toc73371697)

[Tableau 6 : Tableau des échelles de gravité 13](#_Toc73371698)

[Tableau 7 : Détails des niveaux de l'échelle ${echelle\_X} 14](#_Toc73371699)

[Tableau 8 : Détails des niveaux de l'échelle ${echelle\_Y} 15](#_Toc73371700)

[Tableau 9 : Détails des événements redoutés 16](#_Toc73371701)

[Tableau 10 : Liste des socles de sécurité 17](#_Toc73371702)

[Tableau 11 : socle de sécurité XXX 18](#_Toc73371703)

[Tableau 12 : Source de risques et objectifs visés 19](#_Toc73371704)

[Tableau 13 : Evaluations des sources de risque 20](#_Toc73371705)

[Tableau 14 : Synthèse des sources de risque retenues 21](#_Toc73371706)

[Tableau 15 : Détails des parties prenantes et leurs caractéristiques 24](#_Toc73371707)

[Tableau 16 : Détails des événements redoutés 27](#_Toc73371708)

[Tableau 17 : Source de risques et objectifs visés 28](#_Toc73371709)

[Tableau 18 : Tableau des scénarios stratégiques 29](#_Toc73371710)

[Tableau 19 : Tableau des chemins d'attaque 30](#_Toc73371711)

[Tableau 20 : Détails des parties prenantes et leurs caractéristiques 31](#_Toc73371712)

[Tableau 21 : Tableau des mesures de sécurité 32](#_Toc73371713)

[Tableau 22 : Tableau des évaluations 33](#_Toc73371714)

[Tableau 23 : Tableau des scénarios stratégiques 35](#_Toc73371715)

[Tableau 24 : Détails des scénario opérationnel 36](#_Toc73371716)

[Tableau 25 : Détails des modes opératoires 37](#_Toc73371717)

[Tableau 26 : Tableau des échelles de gravité 38](#_Toc73371718)

[Tableau 27 : Détails des niveaux des échelles de vraisemblance 39](#_Toc73371719)

[Tableau 28 : Évaluation de la vraisemblance 40](#_Toc73371720)

[Tableau 29 : Tableau des plans d'amélioration continue de la sécurité 43](#_Toc73371721)

[Tableau 30 : Évaluation et documentation des risques résiduels 44](#_Toc73371722)

**Liste des illustrations**

Figure 1 : Schéma des sources de risque / Objectif visé 23

Figure 2 : Schéma des parties prenantes internes 26

Figure 3 : Schéma des parties prenantes externes 27

Figure 4 : Schéma des parties prenantes internes/externes - initiales/résiduelles 35

Figure 5 : Cartographie du risque initial 42

Figure 6 : Cartographie du risque initial 43

Figure 7 : Cartographie du risque initial 46

Figure 8 : Cartographie du risque résiduel 47

# Activité 1 - Cadrage et socle de sécurité

## Activité 1.a - Cadrer l’étude

### Données principales

* Nom du projet : CarlosCoffreFort
* Objectif à atteindre : Réussir à développer un coffre-fort de sécurité visant une évalaution EAL3
* Cadre Temporel :
* Atelier 1 : 18-05-2021
* Atelier 2 : 19-05-2021
* Atelier 3 : 20-05-2021
* Atelier 4 : 21-05-2021
* Atelier 5 : 22-05-2021
* Durée des cycles stratégiques et opérationnels :
* Durée des cycles stratégiques : 2 ans
* Durée des cycles opérationnels : 1an
* Niveau de confidentialité : Confidentiel
* Personne responsable d'accepter les risques résiduels au terme de l'étude :
* PINTO Carlos

### Acteurs

| **Nom** | **Prénom** | **Poste** |
| --- | --- | --- |
| PINTO | Carlos | Ingénieur sécurité |
| GHAZLI | INEL | Ingénieur sécurité |
| DREUILHET | Romain | Ingénieur sécurité |
| LEBON | Michael | Ingénieur sécurité |
| BOURGAIN | Maxime | Ingénieur sécurité |

Tableau 1 : Liste des acteurs

### RACI

| # | **1.a** | **1.b** | **1.c** | **1.d** | **2.a** | **2.b** | **2.c** | **3.a** | **3.b** | **3.c** | **4.a** | **4.b** | **5.a** | **5.b** | **5.c** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PINTO Carlos** | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R |
| **GHAZLI INEL** | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I |
| **DREUILHET Romain** | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I |
| **LEBON Michael** | I | I | I | I | I | I | I | I | I | I | I | I | I | I | I |

Tableau 2: RACI

## Activité 1.b (Biens primordiaux/support)

### Valeur métier

| **Valeur Métier** | **Nature** | **Description** |
| --- | --- | --- |
| Mot de passe à stocker | Information | Mot de passe que le coffre fort doit stocker |
| Mot de passe du coffre fort | Information | Mot de passe permettant de déverouiller le coffre fort de mot de passe. |
| Clé de vérification de signature | Information | La mise à jour est sécuritée et impose de disposer d'une clé publique de vérification de signature |

Tableau 3 : Tableau des valeurs métiers

### Bien support

| **Bien support** | **Description** |
| --- | --- |
| Memoire Flash | Mémoire Flash permettant de stocker les données non confidentielles |
| Mémoire RAM | Mémoire RAM de travail du processeur |

Tableau 4 : Liste des biens supports

### Mission

| **Nom de la mission** | **Description de la mission** | **Responsable** | **Valeur Métier** | **Responsable de la valeur métier** | **Bien Support** | **Responsable du bien support** |
| --- | --- | --- | --- | --- | --- | --- |
| Enregistrer des comptes | La mission rendue est de pouvoir stocker des mots de passe | Carlos | Mot de passe à stocker | Carlos | Memoire Flash | Carlos |
| Enregistrer des comptes | La mission rendue est de pouvoir stocker des mots de passe | Carlos | Mot de passe à stocker | Carlos | Mémoire RAM | Carlos |
| Limiter l'accès au coffre fort | L'accès au coffre-fort de mot de passe doit être limité aux personnes habilités | Carlos | Mot de passe du coffre fort | Carlos | Memoire Flash | Carlos |
| Limiter l'accès au coffre fort | L'accès au coffre-fort de mot de passe doit être limité aux personnes habilités | Carlos | Mot de passe du coffre fort | Carlos | Mémoire RAM | Carlos |
| Mise à jour sécurisé | Le coffre fort doit pouvoir être mis à jourde façon sécurisé | Carlos | Clé de vérification de signature | Carlos | Memoire Flash | Carlos |
| Démarrage sécurisé | Le coffre fort vérifie que son logiciel est authentique avant de s'executer | Carlos | Clé de vérification de signature | Carlos | Memoire Flash | Carlos |
| Mise à jour sécurisé | Le coffre fort doit pouvoir être mis à jourde façon sécurisé | Carlos | Clé de vérification de signature | Carlos | Mémoire RAM | Carlos |

Tableau 5 : Tableau des missions

## Activité 1.c (Événement redoutés)

### Echelles

#### Liste des échelles

| **Nom de l'échelle** | **Nombre d’échelons de l’échelle** |
| --- | --- |
| EchelleDeGravité | 5 |

Tableau 6 : Tableau des échelles de gravité

#### Détails des Niveaux d’échelles

##### Détails des niveaux de l’échelle ${echelle\_X}

| **Valeur du niveau** | **Description du niveau** |
| --- | --- |
| 1 | Nulle |
| 2 | Très faible |
| 3 | Faible |
| 4 | Moyen |
| 5 | Elevée |

Tableau 7 : Détails des niveaux de l'échelle ${echelle\_X}

##### Détails des niveaux de l’échelle ${echelle\_Y}

${da\_niveau2}

Tableau 8 : Détails des niveaux de l'échelle ${echelle\_Y}

### Événements redoutés

| **Valeur métier** | **Nom de l'événement redouté** | **Description de l'événement redouté** | **Impacts** | **Confidentialité** | **Intégrité** | **Disponibilité** | **Traçabilité** | **Gravité** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Mot de passe à stocker | ER1-Publication des mots passe enregistrés | Les mots de passe ne sont plus confidentiels | Accès aux services par un tiers non autorisé | 3 | 0 | 0 | 0 | 1 |
| Mot de passe du coffre fort | ER2-MotDePasseDuCoffreFort | Les mots de passe ne sont plus confidentiels | Un utilisateur non autorisé a accès à l'ensemble des comptes enregistrés | 3 | 0 | 0 | 0 | 4 |
| Clé de vérification de signature | ER3-ModificationCléSignature | La clé de signature publique officielle est remplacée par une clé non officielle. | Récupération par un attaquant des mots de passe enregistrés | 0 | 0 | 0 | 3 | 5 |

Tableau 9 : Détails des événements redoutés

## Activité 1.d - Les socles de sécurité

### Socle de sécurité

| **Type de référentiel** | **Nom du référentiel** | **État d'application** | **Commentaire** |
| --- | --- | --- | --- |
| Référentiel de sécurité | Règles de codage | Non appliqué |  |

Tableau 10 : Liste des socles de sécurité

### Règles

#### Etat de prise en compte du socle XXX

Tableau 11 : socle de sécurité XXX

# Activité 2 - Sources de risque

## Activité 2.a - Identifier les sources de risques et les objectifs

### Sources de risque et objectifs visés

| **Type d'attaquant** | **Profil d'attaquant** | **Description source de risque** | **Objectif visé** | **Description de l'objectif** |
| --- | --- | --- | --- | --- |
| Individu isolé | Hacker | Hacker isolé | Vol d'argent | Gagner de l'argent en vendant des comptes utilisateurs sur le dark web. |
| Individu isolé | Connaissance | Connaissance de la victime qui à accès physiquement aux locaux. | Espionnage | Une connaissance par curiosité veut accéder aux comptes de la victime par curiosité. |

Tableau 12 : Source de risques et objectifs visés

## Activité 2.b - Évaluer les couples sources de risque/objectifs visés

### Évaluation des sources de risques

| **Profil d'attaquant** | **Description source du risque** | **Objectif visé** | **Description de l'objectif** | **Motivation** | **Ressources** | **Activité** | **Mode opératoire** | **Secteur d'activité** | **Arsenal d'attaque** | **Fait d'armes** | **Pertinence** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hacker | Hacker isolé | Vol d'argent | Gagner de l'argent en vendant des comptes utilisateurs sur le dark web. | 3 | 2 | 2 |  |  |  |  | Élevée |
| Connaissance | Connaissance de la victime qui à accès physiquement aux locaux. | Espionnage | Une connaissance par curiosité veut accéder aux comptes de la victime par curiosité. | 1 | 1 | 1 |  |  |  |  | Faible |

Tableau 13 : Evaluations des sources de risque

## Activité 2.c - Sélectionner les couples SR/OV retenus pour la suite de l’analyse

### Choix des sources de risque

| **Profil d'attaquant** | **Description source du risque** | **Objectif visé** | **Description de l'objectif** | **Motivation** | **Ressources** | **Activité** | **Mode opératoire** | **Secteur d'activité** | **Arsenal d'attaque** | **Fait d'armes** | **Pertinence** | **Choix P1/P2** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hacker | Hacker isolé | Vol d'argent | Gagner de l'argent en vendant des comptes utilisateurs sur le dark web. | 3 | 2 | 2 |  |  |  |  | Élevée | P1 |
| Connaissance | Connaissance de la victime qui à accès physiquement aux locaux. | Espionnage | Une connaissance par curiosité veut accéder aux comptes de la victime par curiosité. | 1 | 1 | 1 |  |  |  |  | Faible | P1 |

Tableau 14 : Synthèse des sources de risque retenues

### Cartographie des "Source de risque / Objectif visé"

${cartographie1}

Figure 1 : Schéma des sources de risque / Objectif visé

# Activité 3 - Scénarios stratégiques

## Activité 3.a -Construire la cartographie des menaces numériques de l'écosystème et sélectionner les parties prenantes critiques

### Création des seuils

Seuil de danger : 4

Seuil de contrôle : 2

Seuil de veille : 1

### Parties prenantes

| **Catégorie** | **Partie prenante** | **Type** | **Dépendance** | **Facteur de pondération dépendance** | **Pénétration** | **Facteur de pondération pénétration** | **Maturité** | **Facteur de pondération maturité** | **Confiance** | **Facteur de pondération confiance** | **Niveau de Menace** | **Criticité** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Producteur | ChinaUsine | Externe | 4 | 1 | 4 | 1 | 1 | 1 | 1 | 1 | 16 | Critique |
| Développeur | IndiaDev | Externe | 4 | 1 | 4 | 1 | 1 | 1 | 1 | 1 | 16 | Critique |
| Utilisateur | Utilisateur | Externe | 4 | 1 | 4 | 1 | 1 | 1 | 1 | 1 | 16 | Critique |
| Logiciel | Logiciel | Interne | 4 | 1 | 4 | 1 | 3 | 1 | 3 | 1 | 1.78 | Critique |
| Matériel | Matériel | Interne | 4 | 1 | 4 | 1 | 3 | 1 | 3 | 1 | 1.78 | Critique |

Tableau 15 : Détails des parties prenantes et leurs caractéristiques

#### Parties prenantes internes

${cartographie2}

Figure 2 : Schéma des parties prenantes internes

#### Parties prenantes externes

${cartographie3}

Figure 3 : Schéma des parties prenantes externes

## Activité 3.b - Élaborer des scénarios stratégiques

### Liste des évènements redoutés établis à l'atelier 1.c

| **Valeur métier** | **Nom de l'événement redouté** | **Description de l'événement redouté** | **Impacts** | **C** | **I** | **D** | **T** | **Gravité** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Mot de passe à stocker | ER1-Publication des mots passe enregistrés | Les mots de passe ne sont plus confidentiels | Accès aux services par un tiers non autorisé | 3 | 0 | 0 | 0 | 1 |
| Mot de passe du coffre fort | ER2-MotDePasseDuCoffreFort | Les mots de passe ne sont plus confidentiels | Un utilisateur non autorisé a accès à l'ensemble des comptes enregistrés | 3 | 0 | 0 | 0 | 4 |
| Clé de vérification de signature | ER3-ModificationCléSignature | La clé de signature publique officielle est remplacée par une clé non officielle. | Récupération par un attaquant des mots de passe enregistrés | 0 | 0 | 0 | 3 | 5 |

Tableau 16 : Détails des événements redoutés

### Liste des couples sources de risques / objectifs visés retenus établis à l'atelier 2

| **Type d'attaquant** | **Profile de l'attaquant** | **Description source de risque** | **Objectifs visés** | **Description de l'objectif** |
| --- | --- | --- | --- | --- |
| Individu isolé | Hacker | Hacker isolé | Vol d'argent | Gagner de l'argent en vendant des comptes utilisateurs sur le dark web. |
| Individu isolé | Connaissance | Connaissance de la victime qui à accès physiquement aux locaux. | Espionnage | Une connaissance par curiosité veut accéder aux comptes de la victime par curiosité. |

Tableau 17 : Source de risques et objectifs visés

### Scénarios stratégiques

| **Nom du Scénario stratégique** | **Source de risque / Objectif visé** |
| --- | --- |
| ST-1-VolMotPasseStocké | Hacker isolé / Vol d'argent |
| ST-2-Connaissance-Espionnage | Connaissance de la victime qui à accès physiquement aux locaux. / Espionnage |

Tableau 18 : Tableau des scénarios stratégiques

### Chemins d'attaque

| **ID du risque** | **ID du chemin** | **Nom du scénario stratégique** | **Chemin d'attaque stratégique** | **Description** | **Gravité** |
| --- | --- | --- | --- | --- | --- |
| R1 | C1 | ST-1-VolMotPasseStocké | Chemin logique |  | 1 |
| R2 | C2 | ST-1-VolMotPasseStocké | Chemin physique |  | 1 |
| R3 | C1 | ST-2-Connaissance-Espionnage | Brute force mot de passe |  | 4 |

Tableau 19 : Tableau des chemins d'attaque

## Activité 3.c - Définir des mesures de sécurité sur l'écosystème

### Liste des parties prenantes établis à l'atelier 3.a

| **Catégorie** | **Partie prenante** | **Type** | **Dépendance** | **Pénétration** | **Maturité** | **Confiance** | **Niveau de menace** | **Criticité** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Producteur | ChinaUsine | Externe | 4 | 4 | 1 | 1 | 16 | Critique |
| Développeur | IndiaDev | Externe | 4 | 4 | 1 | 1 | 16 | Critique |
| Utilisateur | Utilisateur | Externe | 4 | 4 | 1 | 1 | 16 | Critique |
| Logiciel | Logiciel | Interne | 4 | 4 | 3 | 3 | 1.78 | Critique |
| Matériel | Matériel | Interne | 4 | 4 | 3 | 3 | 1.78 | Critique |

Tableau 20 : Détails des parties prenantes et leurs caractéristiques

### Mesure de sécurité

${mesure\_de\_securite}

Tableau 21 : Tableau des mesures de sécurité

### Évaluation

${evaluation}

Tableau 22 : Tableau des évaluations

### Parties prenantes

${cartographie4}

Figure 4 : Schéma des parties prenantes internes/externes - initiales/résiduelles

# Activité 4 - Scénarios opérationnels

## Activité 4.a (Élaborer les scénarios opérationnels)

### Liste des scénarios stratégiques établis lors de l'atelier 3.b

| **Nom du scénario Stratégique** | **Description source de risque** | **Objectifs visé** | **Événements redoutés** | **N° risque** | **Chemin d'attaque stratégique** | **Gravité** |
| --- | --- | --- | --- | --- | --- | --- |
| ST-1-VolMotPasseStocké | Hacker isolé | Vol d'argent | ER1-Publication des mots passe enregistrés | R1 | Chemin logique | 1 |
| ST-1-VolMotPasseStocké | Hacker isolé | Vol d'argent | ER1-Publication des mots passe enregistrés | R2 | Chemin physique | 1 |
| ST-2-Connaissance-Espionnage | Connaissance de la victime qui à accès physiquement aux locaux. | Espionnage | ER2-MotDePasseDuCoffreFort | R3 | Brute force mot de passe | 4 |

Tableau 23 : Tableau des scénarios stratégiques

### Scénario opérationnel

| **N° du risque** | **Chemin d'attaque stratégique** | **Scénario opérationnel** |
| --- | --- | --- |
| R1 | Chemin logique | reza |
| R2 | Chemin physique | azer |
| R3 | Brute force mot de passe | rrrr |

Tableau 24 : Détails des scénario opérationnel

### Liste des modes opératoires

| **Scénario opérationnel** | **Mode opératoire** |
| --- | --- |
| Scenario opérationnel pour : Chemin logique | reza |
| Scenario opérationnel pour : Chemin physique | azer |
| Scenario opérationnel pour : Brute force mot de passe | rrrr |

Tableau 25 : Détails des modes opératoires

## Activité 4.b - Évaluer la vraisemblance des scénarios opérationnels

### Liste des échelles

Tableau 26 : Tableau des échelles de gravité

### Niveaux des échelles de vraisemblance

Tableau 27 : Détails des niveaux des échelles de vraisemblance

### Évaluer la vraisemblance des scénarios opérationnels

Tableau 28 : Évaluation de la vraisemblance

# Activité 5 - Traitement du risque

## Activité 5.a - Réaliser une synthèse des scénarios de risque

### Cartographie du risque initial

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gravité |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 4 |  |  | R3 |  |  |  |
| 3 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 1 | R1 | R2 |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | Vraisemblance |

Figure 5 : Cartographie du risque initial

## Activité 5.b - Décider de la stratégie de traitement du risque et définir les mesures de sécurité

### Cartographie du risque initial

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gravité |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 4 |  |  | R3 |  |  |  |
| 3 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 1 | R1 | R2 |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | Vraisemblance |

Figure 6 : Cartographie du risque initial

### Plan d’amélioration continue de la sécurité

| **Mesure de sécurité** | **Description mesure de sécurité** | **Atelier** | **Scénario des risques associés** | **Principe de sécurité** | **Responsable** | **Frein et difficultés de mise en oeuvre** | **Cout** | **Échéance** | **statut** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Imposer la complexité du mot de passe | Les mots de passe font au minimum 12 caractères | 5.b | R3 |  |  |  |  |  |  |
| Capot | Capot de protection | 5.b | R2 |  |  |  |  |  |  |

Tableau 29 : Tableau des plans d'amélioration continue de la sécurité

## Activité 5.c - Évaluer et documenter les risques résiduels

### Évaluation et documentation des risques résiduels

| **Nom du risque** | **Événement redouté** | **Mesure de sécurité** | **Gravité initiale** | **Vraisemblance initiale** | **Risque initial** | **Nom du risque résiduel** | **Description du risque résiduel** | **Vraisemblance résiduelle** | **Risque résiduelle** | **Gestion du risque résiduel** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Chemin physique | ER1-Publication des mots passe enregistrés | Capot | 1 | 2 | 2 |  |  | 2 | 0 |  |
| Brute force mot de passe | ER2-MotDePasseDuCoffreFort | Imposer la complexité du mot de passe | 4 | 3 | 12 |  |  | 1 | 0 |  |

Tableau 30 : Évaluation et documentation des risques résiduels

### Cartographie du risque initial

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gravité |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 4 |  |  | R3 |  |  |  |
| 3 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 1 | R1 | R2 |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | Vraisemblance |

Figure 7 : Cartographie du risque initial

### Cartographie du risque résiduel

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gravité |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 4 | R3 |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 1 | R1 | R2 |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | Vraisemblance |

Figure 8 : Cartographie du risque résiduel

# Annexes