|  |
| --- |
| [Catégorie ] |

[Adresse société]

[Société]

Tél : [Téléphone société]

[Télécopie société]

[Titre ]

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

Ce rapport est généré à partir de la version [État ] du projet le [Date de publication].

|  |  |  |  |
| --- | --- | --- | --- |
| **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 : Projet Coffre fort : Joyston, Lucas, Mustapha, Anthony
* Objectif à atteindre : Mettre en place un coffre fort sécurisé de mot de passe
* Cadre Temporel :
* Atelier 1 : 24-09-2020
* Atelier 2 : 24-09-2020
* Atelier 3 : 25-09-2020
* Atelier 4 : 25-09-2020
* Atelier 5 : 25-09-2020
* Durée des cycles stratégiques et opérationnels :
* Durée des cycles stratégiques : 3 ans
* Durée des cycles opérationnels : 1 an
* Niveau de confidentialité : Sensible
* Personne responsable d'accepter les risques résiduels au terme de l'étude :
* ANTON RAVEENDRAN Joyston

### Acteurs

| **Nom** | **Prénom** | **Poste** |
| --- | --- | --- |
| ANTON RAVEENDRAN | Joyston | Ingénieur Cybersécurité |
| AHMED MOHAMED ALI | Mustapha | Etudiant |
| OWCZAREK | Lucas | Etudiant |
| PEREIRA | Anthony | Etudiant |

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** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ANTON RAVEENDRAN Joyston** | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R |
| **AHMED MOHAMED ALI Mustapha** | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R |
| **OWCZAREK Lucas** | R | R | R | R | R | R | R | R | R | R | R | R | R | R | R |

Tableau 2: RACI

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

### Valeur métier

| **Valeur Métier** | **Nature** | **Description** |
| --- | --- | --- |
| Stockage | Processus | Stocker des identifiants et mots de passe |
| Génération | Processus | Générer des mots de passe aléatoire |
| Authentification | Processus | Permet de s'authentifier au logiciel |
| Mots de passe et identifiants stockés | Information | Contient les identifants et mot de passe stockés |
| Clé de chiffrement | Information | Contient la clé de chiffrement |
| Mot de passe maitre | Information | Contient le mot de passe maitre |
| Chiffrement | Processus | Système de chiffrement asymétrique |

Tableau 3 : Tableau des valeurs métiers

### Bien support

| **Bien support** | **Description** |
| --- | --- |
| Ordinateur | Il s agit d une application qui permet de lancer l application |
| Executable | Logiciel de gestionnaire de mot de passe |

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** |
| --- | --- | --- | --- | --- | --- | --- |
| Stocker des mots de passe | Service de stockage sécurisé de mot de passe | Carlos | Mot de passe maitre | User1 | Ordinateur | User1 |

Tableau 5 : Tableau des missions

## Activité 1.c (Événement redoutés)

### Echelles

#### Liste des échelles

| **Nom de l'échelle** | **Nombre d’échelons de l’échelle** |
| --- | --- |
| fgdfgdf | 4 |
| EchelleProjet | 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 | Faible : moins de 1 min de dispo |
| 2 | Moyen faible : moins de 5 minutes |
| 3 | Moyen : moins 30 minutes |
| 4 | Grave : moins de 1h |
| 5 | Critique : Au dela de 1h |

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** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Clé de chiffrement | Clé de chiffrement volée | Vol de la clé de chiffrement qui permet de sécuriser les mots de passe | Permet de déchiffrer les mots de passe stockés dans le cas où le mot de passe maitre est divulgué | 3 | 3 | 3 | 1 | 5 |
| Mot de passe maitre | Vol du mot de passe maitre | Vol du mot de passe du coffre fort | Permet d accéder à l intégralité des mots de passe | 3 | 3 | 3 | 1 | 5 |
| Mots de passe et identifiants stockés | Vol des mots de passe du portefeuille | Vol des logins présent dans le portefeuille | Accès aux comptes de l'utilisateur | 3 | 3 | 3 | 2 | 5 |
| Stockage | Modification de la fonction de stockage des mots de passe | Désactiver le chiffrement des mots de passe stockés | Permet d accéder à l intégralité des mots de passe | 1 | 3 | 1 | 1 | 4 |
| Génération | Modification de la fonction de génération de mot de passe | La fonction de génération de mot de passe n est plus aléatoire | Permet d accéder à l intégralité des mots de passe | 1 | 3 | 1 | 1 | 3 |
| Authentification | Authentification | Modification de la fonction d'authentification rendant toutes les entrées légitimes | Accès aux mots de passes de l'utilisateur | 2 | 3 | 2 | 1 | 5 |
| Chiffrement | Chiffrement | Modification de la fonction fonction de chiffrement la rendant obsolète voir indisponible | Accès aux mots de passe en clair | 2 | 3 | 2 | 1 | 4 |

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** |
| --- | --- | --- | --- |
| Guide | Guide de cloisonement ANSSI | Appliqué avec restriction | ou sans restriction a voir |

Tableau 10 : Liste des socles de sécurité

### Règles

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

| **ID de la règle** | **Titre de la règle** | **Description de la règle** | **État de la règle** | **Justification des écarts** | **Responsable** | **Date limite de la mise en application** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Ceci est un titre de règle | Ceci est une description de règle | Partiellement conforme | d | zd | 0000-00-00 |

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 | Amateur | Membre de l'entourage, envieux, jaloux, rancunier | Lucratif | Récupération de donnés sensibles |
| Organisation structurée | Officine spécialisée | Concurrent | Espionnage | Récupérer des informations sur l entreprise à laquelle est rattaché l utilisateur |
| Individu isolé | Hacker | Pirate attaquant | Lucratif | Vol de données utilisateurs, revente |

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** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Amateur | Membre de l'entourage, envieux, jaloux, rancunier | Lucratif | Récupération de donnés sensibles | 3 | 1 | 1 |  |  |  |  | Moyenne |
| Officine spécialisée | Concurrent | Espionnage | Récupérer des informations sur l entreprise à laquelle est rattaché l utilisateur | 3 | 3 | 3 |  |  |  |  | Élevée |
| Hacker | Pirate attaquant | Lucratif | Vol de données utilisateurs, revente | 3 | 3 | 3 |  |  |  |  | Élevée |

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** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Amateur | Membre de l'entourage, envieux, jaloux, rancunier | Lucratif | Récupération de donnés sensibles | 3 | 1 | 1 |  |  |  |  | Moyenne | P2 |
| Officine spécialisée | Concurrent | Espionnage | Récupérer des informations sur l entreprise à laquelle est rattaché l utilisateur | 3 | 3 | 3 |  |  |  |  | Élevée | P1 |
| Hacker | Pirate attaquant | Lucratif | Vol de données utilisateurs, revente | 3 | 3 | 3 |  |  |  |  | Élevée | 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 : 6

Seuil de contrôle : 4

Seuil de veille : 2

### 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** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Informatique | Exécutable | Interne | 4 | 1 | 4 | 1 | 1 | 1 | 1 | 1 | 16 | Critique |
| Informatique | Ordinateur | Externe | 4 | 1 | 4 | 1 | 2 | 1 | 1 | 1 | 8 | Critique |
| Clients | Utilisateur | Externe | 4 | 1 | 4 | 1 | 1 | 1 | 1 | 1 | 16 | Critique |

Tableau 15 : Détails des parties prenantes et leurs caractéristiques

#### Parties prenantes internes

${cartographie2}

Figure : Schéma des parties prenantes internes

#### Parties prenantes externes

${cartographie3}

Figure : 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** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Clé de chiffrement | Clé de chiffrement volée | Vol de la clé de chiffrement qui permet de sécuriser les mots de passe | Permet de déchiffrer les mots de passe stockés dans le cas où le mot de passe maitre est divulgué | 3 | 3 | 3 | 1 | 5 |
| Mot de passe maitre | Vol du mot de passe maitre | Vol du mot de passe du coffre fort | Permet d accéder à l intégralité des mots de passe | 3 | 3 | 3 | 1 | 5 |
| Mots de passe et identifiants stockés | Vol des mots de passe du portefeuille | Vol des logins présent dans le portefeuille | Accès aux comptes de l'utilisateur | 3 | 3 | 3 | 2 | 5 |
| Stockage | Modification de la fonction de stockage des mots de passe | Désactiver le chiffrement des mots de passe stockés | Permet d accéder à l intégralité des mots de passe | 1 | 3 | 1 | 1 | 4 |
| Génération | Modification de la fonction de génération de mot de passe | La fonction de génération de mot de passe n est plus aléatoire | Permet d accéder à l intégralité des mots de passe | 1 | 3 | 1 | 1 | 3 |
| Authentification | Authentification | Modification de la fonction d'authentification rendant toutes les entrées légitimes | Accès aux mots de passes de l'utilisateur | 2 | 3 | 2 | 1 | 5 |
| Chiffrement | Chiffrement | Modification de la fonction fonction de chiffrement la rendant obsolète voir indisponible | Accès aux mots de passe en clair | 2 | 3 | 2 | 1 | 4 |

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** |
| --- | --- | --- | --- | --- |
| Organisation structurée | Officine spécialisée | Concurrent | Espionnage | Récupérer des informations sur l entreprise à laquelle est rattaché l utilisateur |
| Individu isolé | Hacker | Pirate attaquant | Lucratif | Vol de données utilisateurs, revente |

Tableau 17 : Source de risques et objectifs visés

### Scénarios stratégiques

| **Nom du Scénario stratégique** | **Source de risque / Objectif visé** |
| --- | --- |
| Vol de données | Pirate attaquant / Lucratif |
| DDOS | Concurrent / Espionnage |

Tableau : 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 | Vol de données | TEST 2 | TEST 2 | 5 |
| R2 | C4 | Vol de données | TEST | TEST | 4 |
| R3 | C5 | Vol de données | TEST | TEST | 5 |
| R4 | C6 | Vol de données | TEST | TEST | 5 |
| R5 | C8 | Vol de données | TEST | TEST | 3 |
| R6 | C1 | DDOS | TEST | TEST | 5 |
| R7 | C4 | DDOS | TEST | TEST | 4 |
| R8 | C5 | DDOS | TEST | TEST | 5 |
| R9 | C6 | DDOS | TEST | TEST | 5 |
| R10 | C7 | DDOS |  |  | 5 |

Tableau : 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** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Informatique | Exécutable | Interne | 4 | 4 | 1 | 1 | 16 | Critique |
| Informatique | Ordinateur | Externe | 4 | 4 | 2 | 1 | 8 | Critique |
| Clients | Utilisateur | Externe | 4 | 4 | 1 | 1 | 16 | Critique |

Tableau : Détails des parties prenantes et leurs caractéristiques

### Mesure de sécurité

${mesure\_de\_securite}

Tableau : Tableau des mesures de sécurité

### Évaluation

${evaluation}

Tableau : Tableau des évaluations

### Parties prenantes

${cartographie4}

Figure : 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** |
| --- | --- | --- | --- | --- | --- | --- |
| Vol de données | Pirate attaquant | Lucratif | Clé de chiffrement volée | R1 | TEST 2 | 5 |
| Vol de données | Pirate attaquant | Lucratif | Chiffrement | R2 | TEST | 4 |
| Vol de données | Pirate attaquant | Lucratif | Authentification | R3 | TEST | 5 |
| Vol de données | Pirate attaquant | Lucratif | Vol des mots de passe du portefeuille | R4 | TEST | 5 |
| Vol de données | Pirate attaquant | Lucratif | Modification de la fonction de génération de mot de passe | R5 | TEST | 3 |
| DDOS | Concurrent | Espionnage | Clé de chiffrement volée | R6 | TEST | 5 |
| DDOS | Concurrent | Espionnage | Chiffrement | R7 | TEST | 4 |
| DDOS | Concurrent | Espionnage | Authentification | R8 | TEST | 5 |
| DDOS | Concurrent | Espionnage | Vol des mots de passe du portefeuille | R9 | TEST | 5 |
| DDOS | Concurrent | Espionnage | Clé de chiffrement volée | R10 |  | 5 |

Tableau : Tableau des scénarios stratégiques

### Scénario opérationnel

| **N° du risque** | **Chemin d'attaque stratégique** | **Scénario opérationnel** |
| --- | --- | --- |
| R1 | TEST 2 | Description |
| R4 | TEST | Description |
| R3 | TEST | Description |
| R2 | TEST | Description |
| R5 | TEST | Description |
| R6 | TEST | Description |
| R9 | TEST | Description |
| R8 | TEST | Description |
| R10 |  | Description |
| R7 | TEST | Description |

Tableau : Détails des scénario opérationnel

### Liste des modes opératoires

| **Scénario opérationnel** | **Mode opératoire** |
| --- | --- |
| Scenario opérationnel pour : TEST 2 | Description |
| Scenario opérationnel pour : TEST | Description |
| Scenario opérationnel pour : TEST | Description |
| Scenario opérationnel pour : TEST | Description |
| Scenario opérationnel pour : TEST | Description |
| Scenario opérationnel pour : TEST | Description |
| Scenario opérationnel pour : TEST | Description |
| Scenario opérationnel pour : TEST | Description |
| Scenario opérationnel pour : | Description |
| Scenario opérationnel pour : TEST | Description |

Tableau : Détails des modes opératoires

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

### Liste des échelles

| **nom\_echelle** | **nb\_niveau\_echelle** |
| --- | --- |
| Perso Joyston | 5 |
| ajout | 4 |

Tableau : Tableau des échelles de gravité

### Niveaux des échelles de vraisemblance

|  |
| --- |
| nom echelle |
| Perso Joyston |
| Valeur du niveau | Description du niveau |
| Perso Joyston | 1 | Faible : moins de 1 min de dispo |
| Perso Joyston | 2 | Moyen faible : moins de 5 minutes |
| Perso Joyston | 3 | Moyen : moins 30 minutes |
| Perso Joyston | 4 | Grave : moins de 1h |
| Perso Joyston | 5 | Critique : Au dela de 1h |
| ajout | 1 | Faible : moins de 1 min de dispo |
| ajout | 2 | Moyen faible : moins de 5 minutes |
| ajout | 3 | Moyen : moins 30 minutes |
| ajout | 4 | Grave : moins de 1h |
| ajout | 5 | Critique : Au dela de 1h |

Tableau : Détails des niveaux des échelles de vraisemblance

### Évaluer la vraisemblance des scénarios opérationnels

|  |
| --- |
| fgdfgdf |
| R1 | TEST 2 | Scenario opérationnel pour : TEST 2 | 5 |
| R4 | TEST | Scenario opérationnel pour : TEST | 5 |
| R3 | TEST | Scenario opérationnel pour : TEST | 5 |
| R2 | TEST | Scenario opérationnel pour : TEST | 5 |
| R5 | TEST | Scenario opérationnel pour : TEST | 5 |
| R6 | TEST | Scenario opérationnel pour : TEST | 5 |
| R9 | TEST | Scenario opérationnel pour : TEST | 5 |
| R8 | TEST | Scenario opérationnel pour : TEST | 5 |
| R10 |  | Scenario opérationnel pour : | 5 |
| R7 | TEST | Scenario opérationnel pour : TEST | 5 |
| EchelleProjet |
| R1 | TEST 2 | Scenario opérationnel pour : TEST 2 | 5 |
| R4 | TEST | Scenario opérationnel pour : TEST | 5 |
| R3 | TEST | Scenario opérationnel pour : TEST | 5 |
| R2 | TEST | Scenario opérationnel pour : TEST | 5 |
| R5 | TEST | Scenario opérationnel pour : TEST | 5 |
| R6 | TEST | Scenario opérationnel pour : TEST | 5 |
| R9 | TEST | Scenario opérationnel pour : TEST | 5 |
| R8 | TEST | Scenario opérationnel pour : TEST | 5 |
| R10 |  | Scenario opérationnel pour : | 5 |
| R7 | TEST | Scenario opérationnel pour : TEST | 5 |

Tableau : 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 | R1 R4 | R6 R9 | R8 | R10 | R3 |  |
| 4 |  |  |  |  | R2 R7 |  |
| 3 |  |  | R5 |  |  |  |
| 2 |  |  |  |  |  |  |
| 1 |  |  |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | Vraisemblance |

Figure : 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 | R1 R4 | R6 R9 | R8 | R10 | R3 |  |
| 4 |  |  |  |  | R2 R7 |  |
| 3 |  |  | R5 |  |  |  |
| 2 |  |  |  |  |  |  |
| 1 |  |  |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | Vraisemblance |

Figure : 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** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| dssdss | dsdsds | 5.b | R4 | Defense |  |  | + | 0000-00-00 | A lancer |
| Mesure 2tyytr | Mesure 2trtrt | 5.b | R9 |  |  |  |  |  |  |
| Joyston | Joyston | 5.b | R10 | Gouvernance |  |  | + | 0000-00-00 | A lancer |
| dssdss | dssdss | 5.b | R6 | Gouvernance | Joyston | Faible | + | 2022-02-01 | A lancer |
| dssdss | dssdss | 5.b | R7 | Gouvernance | Joyston | Faible | + | 2022-02-01 | A lancer |
| fdsd | dsdsds | 5.b | R1 |  |  |  |  |  |  |
| sddss | dsdds | 5.b | R2 |  |  |  |  |  |  |
| sddss | dsdsds | 5.b | R3 |  |  |  |  |  |  |
| zeeze | ezeze | 5.b | R5 |  |  |  |  |  |  |
| ezez | ezezez | 5.b | R7 |  |  |  |  |  |  |
| dssdss | dssdss | 5.b | R6 |  |  |  |  |  |  |
| dssdss | dssdss | 5.b | R7 |  |  |  |  |  |  |

Tableau : 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** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TEST 2 | Clé de chiffrement volée | fdsd | 5 | 1 | 5 | TEST10 | TEST10 | 1 | 0 | Joyston |
| TEST | Vol des mots de passe du portefeuille | dssdss | 5 | 1 | 5 | dfdf | fdfs | 1 | 0 | Jean |
| TEST | Authentification | sddss | 5 | 5 | 25 | fggf | fgg | 3 | 0 | gf |
| TEST | Chiffrement | sddss | 4 | 5 | 20 | fgf | gfgf | 3 | 0 | gff |
| TEST | Modification de la fonction de génération de mot de passe | zeeze | 3 | 3 | 9 | eefdf | fsdf | 1 | 0 | Pierre |
| TEST | Clé de chiffrement volée | dssdss | 5 | 2 | 10 | rtrtr | rtrtrt | 1 | 0 | trtr |
| TEST | Vol des mots de passe du portefeuille | Mesure 2tyytr | 5 | 2 | 10 | rtrt | trtr | 1 | 0 | rtrtr |
|  | Clé de chiffrement volée | Joyston | 5 | 4 | 20 | rttr | rtr | 1 | 0 | rttr |
| TEST | Chiffrement | dssdss | 4 | 5 | 20 | fgfg | fgff | 5 | 0 | fgf |
| TEST | Chiffrement | ezez | 4 | 5 | 20 | fgfg | fgff | 5 | 0 | fgf |

Tableau : Évaluation et documentation des risques résiduels

### Cartographie du risque initial

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gravité |  |  |  |  |  |  |
| 5 | R1 R4 | R6 R9 | R8 | R10 | R3 |  |
| 4 |  |  |  |  | R2 R7 |  |
| 3 |  |  | R5 |  |  |  |
| 2 |  |  |  |  |  |  |
| 1 |  |  |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | Vraisemblance |

Figure : Cartographie du risque initial

### Cartographie du risque résiduel

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gravité |  |  |  |  |  |  |
| 5 | R1 R4 R6 R9 R10 |  | R3 R8 |  |  |  |
| 4 |  |  | R2 |  | R7 |  |
| 3 | R5 |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 1 |  |  |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | Vraisemblance |

Figure : Cartographie du risque résiduel

# Annexes