

${N°rue} rue ${RueAvenue}

${Zip code} ${Ville}

${Pays}

Tél : ${N°tel}

${LienSite}

${Titre}

*Table des matières* :

[Activité 1 (Cadrage et socle de sécurité) 1](#_Toc71626256)

[Activité 1.a (Cadrer l’étude) 1](#_Toc71626257)

[Activité 1.b (Biens primordiaux/support) 4](#_Toc71626258)

[Activité 1.c (Événement redoutés) 7](#_Toc71626259)

[Activité 1.d (Les socles de sécurité) 10](#_Toc71626260)

[Activité 2 (Source de risque) 12](#_Toc71626261)

[Activité 2.a (Identifier les sources de risques et les objectifs) 12](#_Toc71626262)

[Activité 2.b (Évaluer les couples sources de risque/objectifs visés) 13](#_Toc71626263)

[Activité 2.c (Sélectionner les couples SR/OV retenus pour la suite de l’analyse) 14](#_Toc71626264)

[Activité 3 (Scénarios stratégiques) 16](#_Toc71626265)

[Activité 3.a (Construire la cartographie des menaces numériques de l'écosystème et sélectionner les parties prenantes critiques) 16](#_Toc71626266)

[Activité 3.b (Élaborer des scénarios stratégiques) 18](#_Toc71626267)

[Activité 3.c (Définir des mesures de sécurité sur l'écosystème) 22](#_Toc71626268)

[Activité 4 (Scénarios opérationnels) 24](#_Toc71626269)

[Activité 4.a (Élaborer les scénarios opérationnels) 24](#_Toc71626270)

[Activité 4.b (Évaluer la vraisemblance des scénarios opérationnels) 25](#_Toc71626271)

[Activité 5 (Traitement du risque) 27](#_Toc71626272)

[Activité 5.a (Réaliser une synthèse des scénarios de risque) 27](#_Toc71626273)

[Activité 5.b (Décider de la stratégie de traitement du risque et définir les mesures de sécurité) 28](#_Toc71626274)

[Activité 5.c (Évaluer et documenter les risques résiduels) 29](#_Toc71626275)

# Activité 1 (Cadrage et socle de sécurité)

## Activité 1.a (Cadrer l’étude)

Données principales ( f\_projet)

Nom du projet : ${nomProjet}

Objectif à atteindre : ${Objectif}

Cadre Temporel :

Atelier 1 : ${jj/mm/aaaa1}

Atelier 2 : ${jj/mm/aaaa2}

Atelier 3 : ${jj/mm/aaaa3}

Atelier 4 : ${jj/mm/aaaa4}

Atelier 5 : ${jj/mm/aaaa5}

Durée des cycles stratégiques et opérationnels

Durée des cycles stratégiques : ${dure1}

Durée des cycles opérationnels : ${dure2}

Niveau de confidentialité : ${niveauConfidentialite}

Personne responsable d'accepter les risques résiduels au terme de l'étude : ${responsable}

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.a (Cadrer l’étude)

Acteurs

| **nom** | **prenom** | **poste** |
| --- | --- | --- |
| ANTON RAVEENDRAN | Joyston | Ingénieur Cybersécurité |
| AHMED MOHAMED ALI | Mustapha | Etudiant |
| OWCZAREK | Lucas | Etudiant |
| PEREIRA | Anthony | Etudiant |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.a (Cadrer l’étude)

RACI

| **nom** | **prenom** | **id\_atelier** | **ecriture** |
| --- | --- | --- | --- |
| ANTON RAVEENDRAN | Joyston | 1.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 1.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 1.c | Réalisation |
| ANTON RAVEENDRAN | Joyston | 1.d | Réalisation |
| ANTON RAVEENDRAN | Joyston | 2.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 2.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 2.c | Réalisation |
| ANTON RAVEENDRAN | Joyston | 3.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 3.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 3.c | Réalisation |
| ANTON RAVEENDRAN | Joyston | 4.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 4.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 5.a | Réalisation |
| ANTON RAVEENDRAN | Joyston | 5.b | Réalisation |
| ANTON RAVEENDRAN | Joyston | 5.c | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 1.a | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 1.b | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 1.c | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 1.d | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 2.a | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 2.b | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 2.c | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 3.a | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 3.b | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 3.c | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 4.a | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 4.b | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 5.a | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 5.b | Réalisation |
| AHMED MOHAMED ALI | Mustapha | 5.c | Réalisation |
| OWCZAREK | Lucas | 1.a | Réalisation |
| OWCZAREK | Lucas | 1.b | Réalisation |
| OWCZAREK | Lucas | 1.c | Réalisation |
| OWCZAREK | Lucas | 1.d | Réalisation |
| OWCZAREK | Lucas | 2.a | Réalisation |
| OWCZAREK | Lucas | 2.b | Réalisation |
| OWCZAREK | Lucas | 2.c | Réalisation |
| OWCZAREK | Lucas | 3.a | Réalisation |
| OWCZAREK | Lucas | 3.b | Réalisation |
| OWCZAREK | Lucas | 3.c | Réalisation |
| OWCZAREK | Lucas | 4.a | Réalisation |
| OWCZAREK | Lucas | 4.b | Réalisation |
| OWCZAREK | Lucas | 5.a | Réalisation |
| OWCZAREK | Lucas | 5.b | Réalisation |
| OWCZAREK | Lucas | 5.c | Réalisation |
| PEREIRA | Anthony | 1.a | Réalisation |
| PEREIRA | Anthony | 1.b | Réalisation |
| PEREIRA | Anthony | 1.c | Réalisation |
| PEREIRA | Anthony | 1.d | Réalisation |
| PEREIRA | Anthony | 2.a | Réalisation |
| PEREIRA | Anthony | 2.b | Réalisation |
| PEREIRA | Anthony | 2.c | Réalisation |
| PEREIRA | Anthony | 3.a | Réalisation |
| PEREIRA | Anthony | 3.b | Réalisation |
| PEREIRA | Anthony | 3.c | Réalisation |
| PEREIRA | Anthony | 4.a | Réalisation |
| PEREIRA | Anthony | 4.b | Réalisation |
| PEREIRA | Anthony | 5.a | Réalisation |
| PEREIRA | Anthony | 5.b | Réalisation |
| PEREIRA | Anthony | 5.c | Réalisation |

**Activité 1 (Cadrage et socle de sécurité)**

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

Valeur métier

| **nom\_valeur\_metier** | **nature\_valeur\_metier** | **description\_valeur\_metier** |
| --- | --- | --- |
| 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 |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.b (Biens primordiaux/support)

Bien support

| **nom\_bien\_support** | **description\_bien\_support** |
| --- | --- |
| Ordinateur | Il s agit d une application qui permet de lancer l application |
| Executable | Logiciel de gestionnaire de mot de passe |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.b (Biens primordiaux/support)

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 |

**Activité 1 (Cadrage et socle de sécurité)**

## Activité 1.c (Événement redoutés)

Echelle

| **Nom de l'échelle** | **Échelle de gravité** |
| --- | --- |
| fgdfgdf | 4 |
| EchelleProjet | 5 |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.c (Événement redoutés)

Niveau

| **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 |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.c (Événement redoutés)

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 |

**Activité 1 (Cadrage et socle de sécurité)**

## Activité 1.d (Les socles de sécurité)

Socle de sécurité

| **Type de référentiel** | **Nom du référentiel** | **État d'application** |
| --- | --- | --- |
| Guide | Guide de cloisonement ANSSI | Appliqué avec restriction |

**Activité 1 (Cadrage et socle de sécurité)**

Activité 1.d (Les socles de sécurité)

Règles

| **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** |
| --- | --- | --- | --- | --- | --- | --- |

# Activité 2 (Source de risque)

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

Sources de risque et objectifs visés

| **Type d'ttaquant** | **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 |

**Activité 2 (Source de risque)**

## 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 |

**Activité 2 (Source 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 |  |
| 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 |

**Activité 2 (Source de risque)**

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

Cartographie des "Source de risque / Objectif visé"

${Cartographie1}

# **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 (q\_seuil)

Seuil de danger : ${danger}

Seuil de contrôle : ${contrôle}

Seuil de veille : ${veille}

**Activité 3 (Scénarios stratégiques)**

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

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 |

Parties prenantes internes

${Cartographie2}

Parties prenantes externes

${Cartographie3}

**Activité 3 (Scénarios stratégiques)**

## 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 |

**Activité 3 (Scénarios stratégiques)**

Activité 3.b (Élaborer des scénarios stratégiques)

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

${p\_srov4}

**Activité 3 (Scénarios stratégiques)**

Activité 3.b (Élaborer des scénarios stratégiques)

Scénarios stratégiques

${s\_scenario\_strategique1}

**Activité 3 (Scénarios stratégiques)**

Activité 3.b (Élaborer des scénarios stratégiques)

Chemins d'attaque

${t\_chemin\_d\_attaque\_strategique}

**Activité 3 (Scénarios stratégiques)**

## 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 |

**Activité 3 (Scénarios stratégiques)**

Activité 3.c (Définir des mesures de sécurité sur l'écosystème)

Liste des scénarios stratégiques établis à l'atelier 3.b

${s\_scenario\_strategique2}

# Activité 4 (Scénarios opérationnels)

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

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

${s\_scenario\_strategique3}

**Activité 4 (Scénarios opérationnels)**

## Activité 4.b (Évaluer la vraisemblance des scénarios opérationnels)

Niveaux des échelles de vraisemblance

${da\_echelle}

**Activité 4 (Scénarios opérationnels)**

Activité 4.b (Évaluer la vraisemblance des scénarios opérationnels)

Niveaux des échelles de vraisemblance

${u\_scenario\_operationnel}

**Activité 4 (Scénarios opérationnels)**

Activité 4.b (Évaluer la vraisemblance des scénarios opérationnels)

Niveaux des échelles de vraisemblance

| **Numéro du risque** | **Chemin d'attaque stratégique** | **Scénario opérationnel** | **Vraisemblance** |
| --- | --- | --- | --- |
| R1 | TEST 2 | Description | 1 |
| R4 | TEST | Description | 1 |
| R3 | TEST | Description | 5 |
| R2 | TEST | Description | 5 |
| R5 | TEST | Description | 3 |
| R6 | TEST | Description | 2 |
| R9 | TEST | Description | 2 |
| R8 | TEST | Description | 3 |
| R10 |  | Description | 4 |
| R7 | TEST | Description | 5 |

# Activité 5 (Traitement du risque)

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

Cartographie du risque initial

${Cartographie4}

**Activité 5 (Traitement du risque)**

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

Plan d'amélioration continue de la sécurité

${za\_traitement\_de\_securite}

**Activité 5 (Traitement du risque)**

## Activité 5.c (Évaluer et documenter les risques résiduels)

Évaluation et documentation des risques résiduels

$ {x\_revaluation\_du\_risque}