# Projet analyse de risque

## Sécurité des systèmes d'information

31/10/2020

---

*Joel ASSOGO KOUNGOU*

*Melissa HADJ SAID*

*William CLOEDT*

*Alexandre WOETS*

---

Hicham BEN-YOUSSEF

# Avant-propos

L'entreprise *« Maca Tennis Pro »* est PME qui s'occupe de déployer sa technologie dans des cours de tennis de club professionnel afin d'analyser le jeu des joueurs et leur permettre d'améliorer leur jeu. Elle assure l'installation, ainsi que le suivi du matériel.

La tâche principale de notre société est de fournir aux joueurs de tennis professionnels des informations statistiques détaillées et complètes. En déployant notre technologie de pointe auprès de nos clients, nous sommes en mesure de collecter les données nécessaires à l'analyse. Notre tâche est de concevoir des algorithmes capables d'analyser automatiquement les données et de préparer l'analyse. L'objectif est d'automatiser notre système pour fournir autant d'informations statistiques cohérentes que possible sans aucune intervention manuelle.

L'entreprise est constituée d'une cinquantaine d'employés, répartis en trois équipes. La première équipe est celle qui sera en contact avec les clients, démarchages, négociations, service suivi de client, cette équipe est le visage de l'entreprise. La deuxième équipe se déplace dans les locaux des clients et installe l'équipements. Quatre caméras positionnées aux quatre coins du court de tennis, déployable en intérieur et en extérieur. Ces caméras sont reliées à un mini-ordinateur qui collecte les images et les renvoie sur le cloud privé de l'entreprise. La troisième est l'équipe de recherche et développement, ils développent, conçoivent et améliorent les algorithmes afin d'analyser les images captées par les caméras. Les algorithmes ont pour objectif de visionner les matchs de tennis et analyser tous les éléments nécessaires au joueur, comme la posture, vitesse de la balle, repérer ses points faibles et de nombreux autres facteurs.

Chaque employé a son propre poste de travail et a accès au serveur de l'entreprise. La société est située à Paris et elle travaille avec des clients exclusivement en Europe. Les locaux de l'entreprise sont constitués d'un grand espace open-room, de deux salles de réunions, d'une salle informatique pour les serveurs et d'un bureau pour le président de l'entreprise.

Notre système d'information stocke et traite toutes les données clients. Ces données comprennent les caractéristiques techniques des courts de tennis et des données sur les joueurs de tennis. Ces données résument les statistiques des joueurs de tennis et leur style de jeu, ce qui peut révéler les faiblesses des joueurs de tennis. Par conséquent, les données ont une valeur très importante pour la survie de l'entreprise. Il est important que les données ne fuitent pas si l'on veut conserver nos clients. Les données collectées dans les courts de tennis sont un atout précieux pour nous, il est primordial de protéger les données des clients à tout prix.

Dans ce cas, notre direction estime que la garantie des processus de notre système d'information doit toujours se concentrer sur la protection de nos équipements techniques et des données d'informations. La direction s'engage également à mobiliser les ressources nécessaires à la mise en place et au fonctionnement de l'organisation de l'ISS.

L'élément principal à protéger en premier est le serveur contenant les données clients. Et il y a des algorithmes que les concurrents ne devraient pas connaître.

Enfin, la direction a rappelé que chaque membre de la structure est impliqué dans la sécurité du SI, il est donc nécessaire que chaque utilisateur contribue à sa sécurité en gardant sa vigilance et en respectant les PSSI.

# ATELIER 1 – CADRAGE ET SOCLE DE SÉCURITÉ

## 1. Définir le cadre de l'étude

Nous allons d'abord commencer par exposer l'objet et les attendus du projet aux membre de l'équipe. L'objectif de notre étude est l'identification du niveau de la sécurité de notre organisation. Nous devons d'abord procéder par définir les risques, ensuite les analyser et enfin essayer de trouver des solutions. Nous allons définir les tâches de chacun des membres de l'équipe, pour cela nous avons conçu une matrice RACI.

La réussite d'un projet repose sur une définition claire et précise des rôles et des responsabilités de chacun des acteurs. C'est pour cela que nous avons décidé de répartir les différentes responsabilités grâce à la Matrice RACI. Cet outil apporte une réponse très opérationnelle pour visualiser d'un coup d'œil la répartition des rôles. La matrice RACI permet de répondre à des questions telles que « Qui fait quoi ? » ou encore « Qui est responsable de cette partie ».

R : Réalise ; en charge d'effectuer l'action
A : Approuve ; en charge de superviser l'action et de référer à la hiérarchie
C : Consulter ; en charge de contribuer, d'apporter des conseils
I : Informer ; doit être informé

| Tâches | Joel | Melissa | William | Alexandre |
|---|---|---|---|---|
| **Atelier 1** | | | | |
| Définir le cadre de l'étude | R | R | I | I |
| Périmètre métier | C, A | I | I | R |
| Événements redoutés | C, A | R | I | I |
| **Atelier 2** | | | | |
| Couples SR/OV | R | C, A | I | I |
| **Atelier 3** | | | | |
| Cartographie | R | C, A | I | I |
| Scénarios stratégiques | C, A | R | I | I |
| Mesures de sécurité sur l'écosystème | R | C, A | I | I |
| **Atelier 4** | | | | |
| Élaborer les scénarios opérationnels | C, A | R | I | I |
| Évaluer leur vraisemblance | R | C, A | I | I |
| **Atelier 5** | | | | |
| Synthèse des scénarios de risque | R | C, A | I | I |
| Stratégie de traitement du risque | R | C, A | I | I |
| Les risques résiduels | C, A | R | I | I |
| Cadre de suivi des risques | C, A | R | I | I |

*Tableau de répartition des tâches*

Afin de nous organiser au mieux et avoir une vision précise de l'avancement de notre projet, nous avons réalisé un planning nous permettant d'organiser les tâches en fonction du temps imparti. Au vu de la quantité de travail à fournir en un temps assez limité, le chemin critique ne laisse pas de marge à un retard de tâche.

| Jalons / Tâches | 14/10/2020 | Du 14/10 au 22/10 | Du 23/10 au 29/10 | 30/10/2020 | 31/10/2020 |
|---|---|---|---|---|---|
| Choix de la méthode | | | | | |
| Atelier 1 | | | | | |
| Atelier 2 | | | | | |
| Atelier 3 | | | | | |
| Atelier 4 | | | | | |
| Atelier 5 | | | | | |
| Mise en page rapport | | | | | |
| | | | | | |
| **Légende** | **Tâche non commencée** | **Tâche terminé** | **Date au plus tôt** | **Date prévue pour la réalisation** | **Date au plus tard (chemin critique)** |

*Planning des tâches à réaliser*

## 2. Définir le périmètre métier et technique

Dans un premier temps, nous avons recensé les missions et les valeurs métiers relatifs à l'objet d'étude, à la suite de cela nous avons pu réaliser un tableau récapitulatif du périmètre métier.

**Missions**

1. Calculs mathématiques des statistiques du joueur pour l'aider à s'améliorer
2. Offrir un service aux joueurs via une application pour faciliter l'utilisation de ses données
3. Support pour les joueurs en cas de problèmes

**Valeurs Métiers**

1. Application (disponibilité)
2. Données des joueurs (confidentiel)
3. Support (disponibilité)
4. Algorithmes (confidentiel)

| Mission | | | Utilisation des données utilisateurs |
|---|---|---|---|

| Dénomination de la valeur métier | Développement des algorithmes d'analyse | Service application | Suivi client |
|---|---|---|---|
| Nature de la valeur métier | Processus | Disponibilité | Processus |
| Description | Création de nouveaux algorithmes pour améliorer l'analyse des données utilisateurs | Disponibilité de l'application à tout moment pour l'utilisateur | Mise en place d'un support pour répondre aux demandes des clients en cas de problèmes |
| Entité ou personne responsable | Equipe de Développement | Equipe de Développement | Equipe Contact Clients |

| Dénomination du/des biens supports associés | Serveurs bureautiques (intérieurs) | Serveurs bureautiques (externes) | Réseau bureautique (internes) |
|---|---|---|---|
| Description | Serveurs ou sont stockées l'ensemble des données de développement | Serveurs ou sont stockées les données utilisateurs | Réseau et matériel nécessaire pour répondre aux besoins des clients |
| Entité ou personne responsable | Chef d'équipe de Développement | DSI | Chef d'équipe Contact Clients |

*Tableau du périmètre métier*

## 3. Identifiés les évènements redoutés

La cotation de la gravité des impacts est effectuée sur la base de la grille suivante:

| Echelles | Conséquence |
|---|---|
| G4 Critique | Incapacité pour la société d'assurer tout ou une partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée). |
| G3 Grave | Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé). |
| G2 Significative | Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé). |
| G1 Mineur | Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges) |

*Tableau explicatif de l'échelle de gravité*

La société a recensé une partie des événements redoutés dans le tableau suivant:

| VALEUR MÉTIER | EVÈNEMENT REDOUTÉ | IMPACTS | GRAVITÉ |
|---|---|---|---|
| Menaces générales pesant sur les systèmes d'informations et les données | Panne matérielle et logicielle | Logiciels informatiques | G3 |
| | Erreur humaine : traitement incorrect des données | Données | G2 |
| | Fuite de données | - Confidentialité des données et des algorithmes d'analyses<br>- Logiciels informatiques et les systèmes d'information | G3 |
| | Spam et hameçonnage | - confidentialité des données et des algorithmes d'analyses<br>- logiciels informatiques et les systèmes d'info<br>- image et confiance<br>- sécurité des personnes | G4 |
| | Failles de sécurité | - Impact sur l'image et la confiance<br>-Impacts sur la sécurité des personnes | G3 |
| | Fuite des données des clients | - confidentialité des données<br>-image et la confiance<br>- sécurité des personnes | G4 |
| | Fuite ou corruption des algorithmes | - gouvernance de l'organisme | G4 |
| | Crise économique, inflation | Financiers | G2 |

| | | | |
|---|---|---|---|
| Situation de crise | Guerre, confinement | Financiers | G2 |
| Concurrence | Existence de brevets, marques et modèles antérieurs | Financiers<br>Image de l'entreprise | G2 |
| | Apparition d'un produit concurrent | | G2 |
| Marketing | Perception erronée du besoin (approche qualitative) | Financiers<br>Image de l'entreprise | G2 |
| | Marché surestimé en volume | | G2 |
| | Surestimation des prix du marché | | G2 |
| Risque fournisseurs | Défaillance d'un produit du fournisseur-clé | Financiers | G3 |
| | Augmentation des prix du matériels | | G2 |
| Catastrophes naturelles | Les incendies, les cyclones et les inondations | Matériaux de l'entreprise<br>Financier | G3 |

*Tableau des évènements redoutés*

# ATELIER 2 – SOURCES DE RISQUE

Dans cet atelier, nous avons identifié les sources de risque (SR) et leurs objectifs visés (OV), en lien avec notre contexte particulier de l'étude. Les sources de risque et les objectifs visés ont ensuite caractérisés et évalués en vue de retenir les plus pertinents.

| Sources de risque | Objectifs visés | Motivation | Ressources | Activité | Pertinence |
|---|---|---|---|---|---|
| **Concurrent** | Voler des algorithmes | +++ | +++ | +++ | Élevé |
| **Concurrent** | Voler des informations clients | +++ | +++ | +++ | Élevé |
| **Pirate informatique** | Voler les données de l'entreprise | ++ | +++ | + | Modéré |
| **Pirate informatique** | Paralysé l'entreprise | + | ++ | + | Faible |
| **Cyber terroriste** | Modifier les algorithmes | + | ++ | + | Faible |

*Tableau des couples SR/OV jugés prioritaires*

La source la plus pertinente retenue par l'entreprise est un risque venant d'une entreprise concurrente voulant nuire à l'entreprise à volant ou corrompant des données. Le groupe de travail retiendra en priorité les couples de pertinence élevée et moyenne, laissant de côté dans un premier temps la menace cyber-terroriste et celle liée aux hacktivistes souhaitant divulguer des informations sur les tests animaliers, qui sont jugées moins prégnantes.

## 4. Cartographie de menace numérique de l'écosystème et les parties prenantes critiques

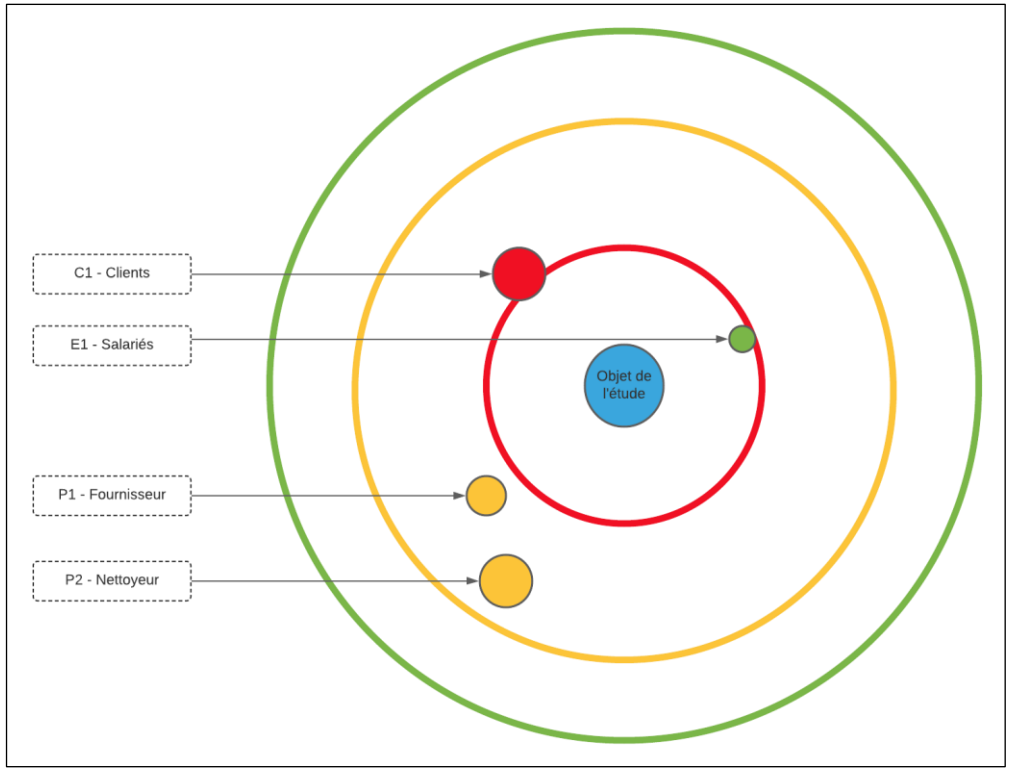
L'équipe a décidé de se concentrer dans un premier temps sur les parties prenantes internes et externes de l'écosystème de la société. Elle a identifié les acteurs suivants :

| Catégorie | Partie prenante |
|---|---|
| Client | C1 - Etablissement tennis |
| Entreprise | S1 - Salarié |
| Prestataire | P1 - Fournisseur de matériel électronique |
| | P2 - Service de nettoyage |

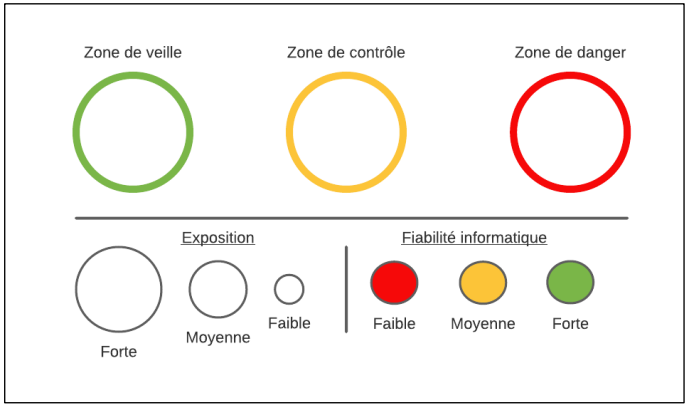
L'évaluation de chaque partie prenante a permis d'établir la cartographie de menace numérique présente à droite.

L'équipe a retenu les parties prenantes C1 – clients et E1 – salariés, comme parties prenantes critiques. La partie prenante P1 – Fournisseur a aussi été jugée comme partie prenante critique.

Les autres parties prenantes n'ont pas été retenues comme critiques. Après discussion, P2 bien que situées dans la zone de contrôle, n'a pas été retenue par l'équipe, compte tenu du contexte et de la nature des sources de risque en jeu.




*Cartographie de menace numérique*



## 5. Scénarios stratégiques

On s'est d'abord intéressé au couple de travail SR/OV « un concurrent veut voler les algorithmes d'analyses » les chemins d'attaques qui ont été jugé pertinents.

**Le concurrent vole les algorithmes recherche :**

- En créant un canal d'exfiltration de données portant directement sur le système d'information
- En créant un canal d'exfiltration de données sur les machines des employées qui s'occupe de l'analyse des données obtenu par l'algorithme.

Le scénario stratégique associé est représenté ci-après. Il est de gravité 4 (grave) selon la cotation effectuée lors de l'atelier 1 sur les valeurs métiers.

Puis le groupe de travail s'est penché sur le couple SR/OV : « Une pirate informatique veut voler les données de l'entreprise, en piratant l'un des employés de l'entreprise ». Trois chemins d'attaques ont été identifiés comme pertinents.

- **Par envoi de mails piégés**
  L'envoi de mails piégés aux utilisateurs de l'entreprise, soit de manière très ciblée avec des contenus de messages qui collent au travail de l'employé concerné. Le piégeage peut se faire soit avec une pièce jointe malveillante, soit en redirigeant vers un site Web qui présente des codes d'exploitation pour compromettre le navigateur Web.
- **En compromettant un site Web externe**
  La compromission d'un site Web sur lequel il est prévisible que des employés de l'entreprise vont se connecter. Il peut s'agir du site du CE, un consortium d'entreprises, un site d'actualités spécialisé dans le domaine d'activité, etc.
- **En piégeant un produit fournisseur**
  La compromission par le piégeage d'un produit chez le fournisseur. Ou les fournisseurs d'équipements pour l'entreprise ont été piraté, l'attaquant dépose un cheval de Troie dans leur produit. Il attendra ensuite que le produit soit installé pour le compromettre à son tour.

Le scénario stratégique associé est représenté ci-après. Il est de gravité 4 (critique) selon la cotation effectuée lors de l'atelier 1 sur les valeurs métier.

En synthèse, deux scénarios stratégiques ont été retenus :

| Source de risque | Objets visés | Chemins d'attaque stratégique | Gravité |
|---|---|---|---|
| Concurrent | Voler les algorithmes d'analyse | Canal d'exfiltration de données portant directement sur le système d'information<br><br>Canal d'exfiltration de données sur les machines des employées qui s'occupe de l'analyse des données obtenu par l'algorithme | 4 Critique |
| Pirate informatique | Voler les données de l'entreprise | Envoi de mails piégés<br><br>En compromettant un site Web externe<br><br>En piégeant un produit fournisseur | 4 Critique |

*Tableau des scénarios stratégiques*

## 6. Mesures de sécurité sur l'écosystème

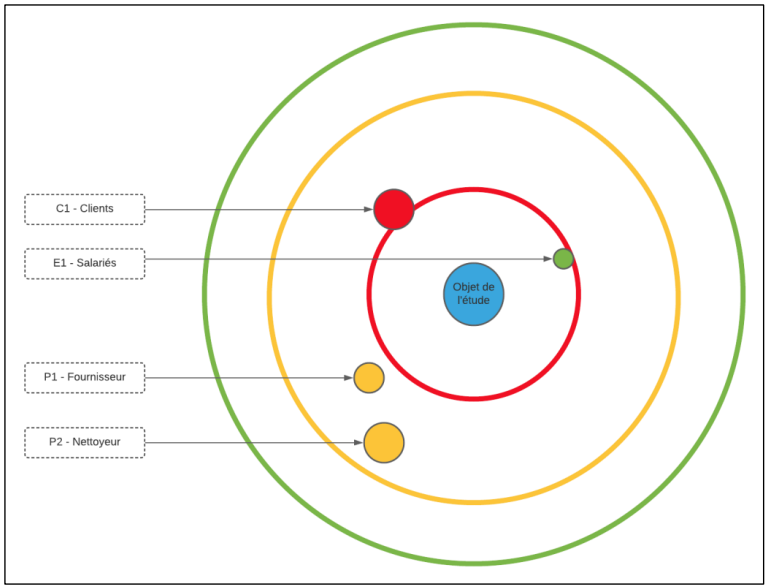
Des mesures de sécurité ont été définies en priorité pour les prestataires F2, F3 et P3. Ces derniers sont en effet impliqués dans des scénarios stratégiques particulièrement problématiques.

| Partie prenante | Chemin d'attaque stratégiques | Mesure de sécurité |
|---|---|---|
| C1 - Etablissement tennis | En compromettant un site Web externe | Accroitre la maturité cyber des établissements de client :<br>■ audit de sécurité<br>■ procédure de signalement d'incident de sécurité |
| S1 - Salarié | En créant un canal d'exfiltration de données sur les machines des employées qui s'occupent de l'analyse des données obtenu par l'algorithme | Stockage des données sur les serveurs pas sur les machines.<br>Renforcer la sécurité des serveurs et cryptage des données. |
| P1 - Fournisseur de matériel électronique | En piégeant un produit fournisseur | Réduire le risque de piégeage des équipements de maintenance utilisés sur le système industriel.<br>Vérification de l'intégrité du matériel par un expert avant utilisation |

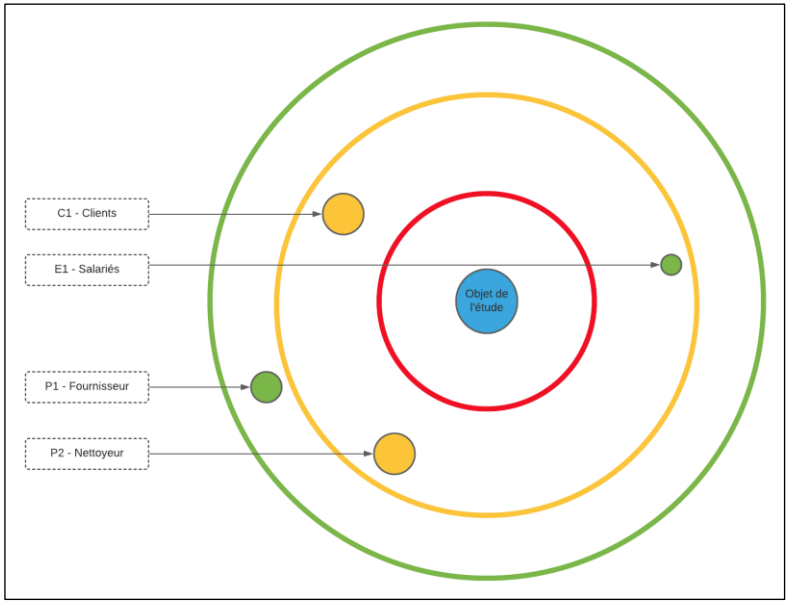
*Tableau des mesures de sécurité*

L'application des objectifs ci-dessus devrait permettre sous 9 à 12 mois de réduire le risque, avec une cartographie de menace numérique résiduelle comme il suit.

Initiale :




Résiduel :



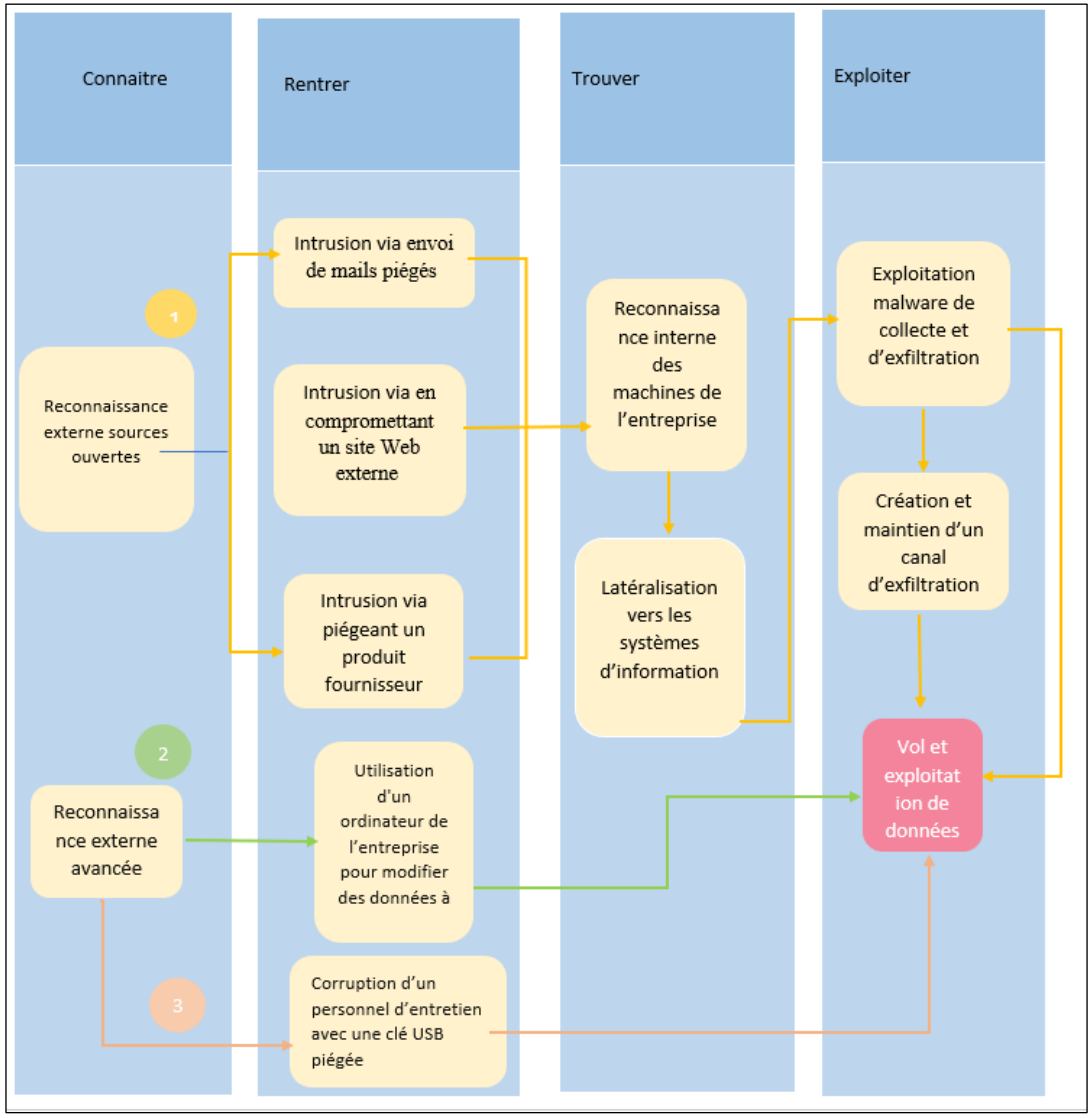
## 7. Scénarios opérationnels

Notre équipe a décidé de représenter les scénarios opérationnels sous la forme de graphes d'attaques. Nous avons choisi de se concentrer sur la réalisation d'un premier scénario opérationnel correspondant à un chemin d'attaque stratégique identifié dans l'atelier 3.

Scénario opérationnel relatif au chemin d'attaque : « Une pirate informatique veut voler les données de l'entreprise, en piratant l'un des employés de l'entreprise ».

Nous avons étudié plusieurs techniques d'accès, parmi lesquelles des actions de collusion, permettant à l'attaquant de rentrer dans le système d'information et 3 modes opératoires ont été jugés pertinents.

- L'attaquant s'introduit dans le système d'information par une attaque ciblée sur la messagerie d'un des employés par l'envoi de mails piégés ou en piégeant des site Web externe, Il accède ensuite aux données stratégiques de l'entreprise
- L'attaquant utilise un ordinateur de l'entreprise ensuite facilement les informations depuis son poste de travail, dans la mesure où aucune action de supervision n'est réalisée.
- L'attaquant corrompt un personnel d'entretien des locaux et lui demande de brancher une clé USB préalablement piégée sur un poste de travail. Cette opération est facilitée par le fait que l'entretien des locaux est réalisé en dehors des heures ouvrées, que le personnel d'entretien a accès librement au bureau d'études et que les ports USB ne sont soumis à aucune restriction




*Graphique des scénarios d'attaques*

## 8. Evaluation des vraisemblances des scénarios opérationnelles

Les cinq scénarios opérationnels ont été élaborés au cours de l'étape précédente par l'équipe projet. La vraisemblance est calculée selon la difficulté à réaliser le scénario d'attaque ainsi qu'à la probabilité de réussite. Ils ont été évalués selon leur niveau de vraisemblance, sur la base de la grille de cotation suivante :

| échelle | description |
|---|---|
| V4<br>Quasi certain | La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée. |
| V3<br>Très vraisemblable | La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée |
| V2<br>Vraisemblable | La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative |
| V1<br>Peu vraisemblable | La source de risque a peu de chance d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible. |

*Echelle de vraisemblance globale d'un scénario opérationnel*

*Tableau de calcul de la vraisemblance*

| | | Difficulté technique de scénario opérationnel | | | |
|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 |
| Probabilité de succès du scénario opérationnel | 4 | | | | |
| | 3 | | | | |
| | 2 | | | | |
| | 1 | | | | |

**1 : Faible, 2 : Modérée, 3 : élevée, 4 : très élevée**

| Chemins d'attaques stratégiques (associés aux scénarios opérationnelles) | Vraisemblance globale |
|---|---|
| Un concurrent modifie les algorithmes de l'entreprise, en s'introduisant dans les locaux, et en exploitant un ordinateur de l'entreprise | V1<br>Peu vraisemblable |
| Un concurrent détruit des données de l'entreprise en corrompant un personnel d'entretien, pour qu'il introduise une clé USB piégée | V2<br>Vraisemblable |
| Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données sur le système d'information de l'entreprise | V3<br>Très vraisemblable |
| Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données passant par les fournisseurs de l'entreprise | V3<br>Très Vraisemblable |
| Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données passant par les clients | V4<br>Quasi certain |

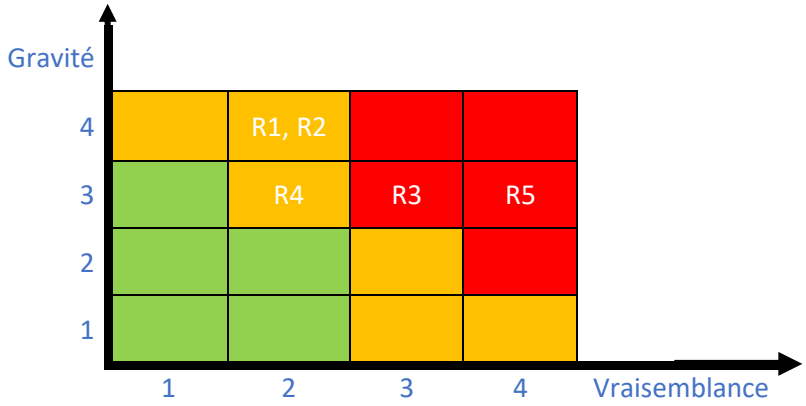
*Tableau des vraisemblances globales des scénarios opérationnelles*

Le vol des données d'études R&D par l'intermédiaire d'un des clients est considéré comme quasi certain. D'une part, les clients en question sont connectés au cloud de l'entreprise et d'autre part la sécurité de son système d'information est faible. La combinaison de ces facteurs aggravants rend une opération d'intrusion et exfiltration très facile pour un attaquant avec un minimum de ressources engagées.

Le vol de données par exfiltration directe est considéré comme très vraisemblable compte tenu des nombreuses vulnérabilités techniques et organisationnelles observées dans l'organisation et chez les fournisseurs : utilisateurs peu informés sur les risques numériques (exemple : hameçonnage), Non contrôle du nouveau matériel entrant, facilitée à entrer dans les locaux de l'entreprise etc.

# ATELIER 5 – TRAITEMENT DU RISQUE

## 9. Synthèse des scénarios de risque




**Scénarios de risques**

R1 : Un concurrent altère les algorithmes de l'entreprise, en s'introduisant dans les locaux, et en exploitant un ordinateur de l'entreprise.

R2 : Un concurrent altère les données de l'entreprise en corrompant un personnel d'entretien, pour qu'il introduise une clé USB piégée

R3 : Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données sur le système d'information de l'entreprise.

R4 : Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données passant par les fournisseurs de l'entreprise.

R5 : Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données passant par les clients.

## 10. Stratégie de traitement du risque et définir les mesures de sécurité

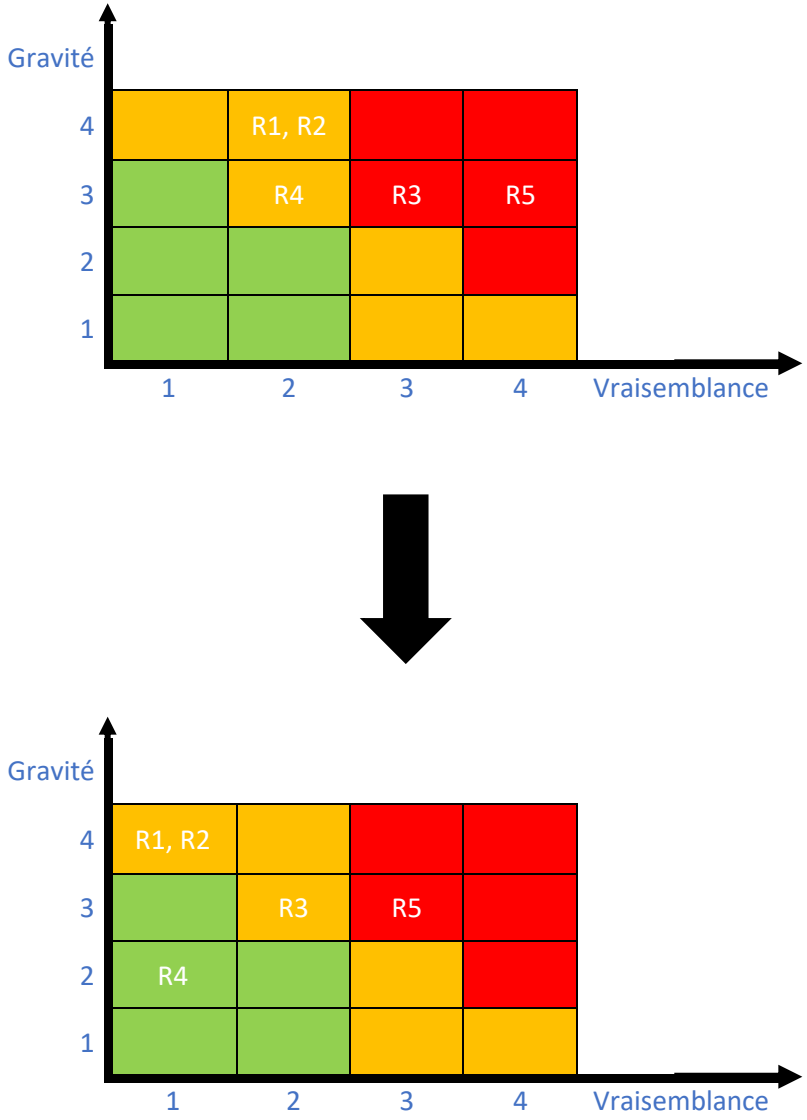
| Mesure de sécurité | Scénarios de risques associés | Responsable | Difficultés de mise en œuvre | Coût / complexité | Échéance | Statut |
|---|---|---|---|---|---|---|
| Gouvernance | | | | | | |
| Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contrats avec les clients et les fournisseurs | R4, R5 | Equipe juridique | Effectué au fil de l'eau à la renégociation des contrats | ++ | 12 mois | En cours |
| Sensibilisation renforcée à l'hameçonnage par un prestataire spécialisé | R3 | RSSI | Validation du CHSCT indispensable | + | 6 mois | En cours |
| Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un client ou fournisseur | R4, R5 | RSSI / Equipe juridique | | ++ | 9 mois | A lancé |
| Protection | | | | | | |
| Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonnement) | R1, R2, R3 | DSI | | +++ | 12 mois | A lancé |
| Renforcement du contrôle d'accès physique au bureau R&D | R1, R2 | Equipe de sureté | | ++ | 3 mois | Terminé |
| Chiffrement des échanges de données avec les clients | R5 | DSI | | ++ | 6 mois | En cours |
| Vérification de l'intégrité du matériel par un expert avant utilisation | R4 | DSI | | ++ | 3 mois | En cours |
| Défense | | | | | | |
| Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil. | R3 | DSI | Achat d'un outil, budget à provisionner | ++ | 9 mois | A lancé |

*Tableau de définition de mesure de sécurité*

## 11. Risques résiduels

Après application des mesures de traitements définies dans l'étape précédente nous sommes désormais en mesure d'évaluer les risques résiduels.

| RR01 – Vol ou altération de données |
|---|
| **Description et analyse du risque résiduel** |
| ■ Vol des données de l'entreprise<br>■ Vol des analyses fait par l'algorithme<br>■ Vol des données des clients<br>■ impact sur la confidentialité des données<br>■ impact sur la sécurité des personnes |
| **Événements redoutés concernés** |
| ■ Attaque par un pirate informatique<br>■ Corruption d'un membre personnel |
| **Mesures de traitement du risque existantes et complémentaires** |
| ■ Sensibilisation renforcée à l'hameçonnage par un prestataire spécialisé<br>■ Vérification de l'intégrité du matériel par un expert avant utilisation<br>■ Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un client ou fournisseur<br>■ Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant<br>■ Surveillance renforcée des flux entrants et sortants<br>■ Chiffrement des échanges<br>■ Protection renforcée des données<br>■ Renforcement du contrôle d'accès physique |




Les mesures prises afin d'atténuer les risques contre le SI de l'entreprise ont permis de dresser les résultats suivants. Après application des mesures de sécurités, les scénarios de risques ont significativement été diminués donnant les graphiques suivants :

## 12. Cadre de suivi des risques

Dans notre projet d'analyse de risque nous avons mis en œuvre des indicateurs de pilotage afin de mener à bien notre projet.

Nous avons défini les risques qui s'illustrent sur :

- Les menaces générales pesant sur les systèmes d'informations et les données qui comprennent par exemple la panne matérielle et logicielle telle qu'une panne de courant ou une corruption de données ou des erreurs humaines tel que traitement incorrect des données, élimination imprudente des données ou ouverture accidentelle de pièces jointes infectées mais aussi Spam, escroqueries et hameçonnage : e-mails non sollicités qui cherchent à inciter les gens à révéler des informations personnelles ou à acheter des produits frauduleux.
- Les menaces informatiques criminelles tel que le déni de service ou les Failles de sécurité ainsi que la malhonnêteté du personnel : vol de données ou d'informations sensibles, tels que les détails des clients ou la corruption de l'algorithme.
- Nous avons également les risques politiques, risques fournisseurs, risques marché, risques marketing.

Ensuite nous avons défini également les mesures afin de faire face à ces risques par l'intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contrats avec les clients et les fournisseurs, la mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un client ou fournisseur, le renforcement du contrôle d'accès physique au bureau R&D, le chiffrement des échanges de données avec les clients, la vérification de l'intégrité du matériel par un expert avant utilisation

Enfin nous avons établi un processus d'amélioration afin de renforcer la sécurité dont la surveillance renforcée des flux entrants et sortants (sonde IDS) et l'analyse des journaux d'évènements à l'aide d'un outil.

Nous avons constitué un comité de pilotage qui se réunit tous les six mois pour aborder cette montée en puissance ou tous les douze mois en rythme de croisière afin d'assurer un suivi des indicateurs, de l'avancement du plan d'amélioration continue de la sécurité et de l'évolution des risques.