**Déroulement du projet Cybersécurité**

Rudy Krauffel

Louis Hans

Corentin Lente



MOTUC

Table des matières

[Choix de la méthode de gestion de projet 3](#_Toc36824706)

[La méthode Agile 3](#_Toc36824707)

[1. Scrum 3](#_Toc36824708)

[2. Notre méthode 4](#_Toc36824709)

[Décryptage des fichiers 5](#_Toc36824710)

[Réalisation des diagrammes de processus métiers 7](#_Toc36824711)

[Analyses des risques et rédaction des recommandations 8](#_Toc36824712)

[Conclusion 10](#_Toc36824713)

## Choix de la méthode de gestion de projet

Les contraintes de ce projet étaient les suivantes :

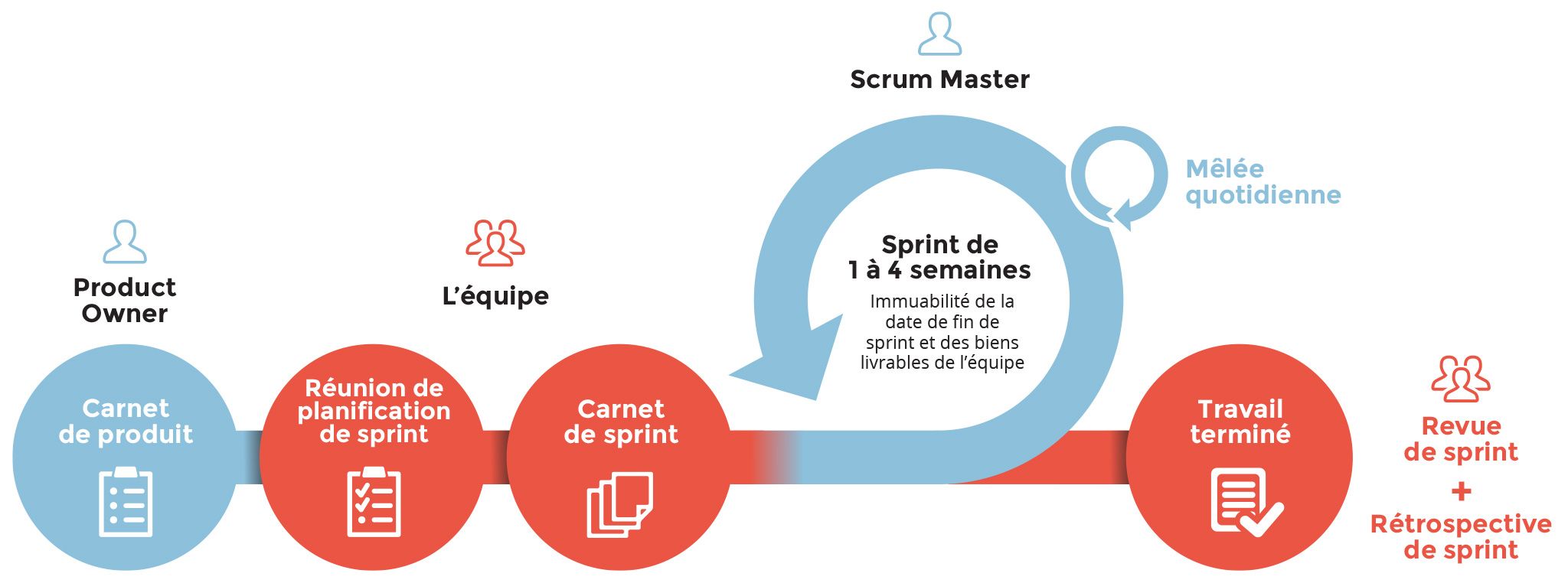
* Deadline : une semaine
* Ressources : 3 informaticiens
* Livrables : 50 pages de documentation
* Confinement : interactions limitées

Au vu de la quantité de travail requise, nous devions adopter une méthodologie de gestion de projet flexible, qui confère une grande autonomie à chacune des ressources disponibles tout en maintenant une certaine synchronisation entre les différents acteurs du projet.

Les méthodes dites classiques de gestion de projets présentent des avantages et des garanties, mais c’est la flexibilité qui pour nous primait. La situation actuelle de confinement nous a poussé à choisir la méthode Agile pour ce projet, car nos expériences professionnelles passées nous prouvent qu’elle s’adapte parfaitement au travail en équipe, même en télétravail.

## La méthode Agile

### Scrum



La méthode agile valorise les points suivants :

* Planning adaptatif, réponse rapide aux changements et aux problèmes
* Motivation des effectifs
* Retour sur le produit
* Intégration continue / Déploiement continu
* Incrémentation progressive de la valeur ajoutée
* Priorisation
* Investissement personnel des acteurs phares

Scrum, la variante la plus populaire de la méthode Agile, est basée sur des cycles itératifs de planification :

* Journalière : Le Daily Scrum est une réunion quotidienne qui rassemble l'ensemble de l'équipe de réalisation qui ne doit pas durer plus de 15 minutes.
* Par cycle (aussi appelé Sprint) d’une durée typique de 2 semaines.
* Par release (trimestrielle, bisannuelle, etc…)

Les acteurs principaux de la méthode agile en milieu professionnel sont :

* Product Owner : il est au centre de la communication dans le projet. Il va synthétiser les retours de l’équipe et en faire des stories et des taches, qui sont des unités de travail sur lesquelles un développeur peut travailler seul. Ces taches s’accumulent dans un backlog. Le product owner va ensuite fixer les ordres de priorité des items du backlog.
* Le Scrum Master s’assure du respect de la méthode pendant les Sprints, dirige la conduite des daily scrums, et échange continuellement avec les stakeholders pour faire état du travail réalisé et la suite possible des opérations.

### Notre méthode

Pour ce projet, il est évident que nous n’avons pu mettre en place une gestion de projet avec Scrum dans les règles de l’art. Nous n’avons ni les ressources, ni le temps, le contexte professionnel complet nécessaire. Toutefois, nous pouvons apprendre de la méthode et l’adapter à nos problématiques.

L’analyse du problème posé par le projet à mis en exergue trois grands axes de travail distincts :

* Décryptage des fichiers de l’entreprise
* Réalisation de diagrammes des processus métiers de l’entreprise
* Analyse des risques et recommandations

Ces trois items peuvent être interprétés comme des stories, et constituent donc notre sprint backlog rudimentaire.

Ils constituent l’ensemble du travail à réaliser. Par conséquent, la priorisation n’est pas nécessaire et chacun d’entre nous peut se mettre au travail sur une de ces stories. Là où un Product Owner les aurait divisées en tâches surement plus courtes, nous avons décidé de les laisser telles quelles, jugeant qu’une granularité plus fine des taches serait contre-productive avec une deadline si proche.

Ici, chacun d’entre nous prend la responsabilité de réaliser une large tache, et gagne en vitesse et en efficacité au fur et à mesure de l’avancée du travail. Dans une équipe Scrum professionnelle, tous les membres de l’équipe ont des compétences égales sur les diverses taches qu’ils ont à réaliser, et peuvent donc s’atteler à des items de petite taille sans temps d’acclimatation. Comme le sujet est nouveau pour nous, il était plus sûr pour chacun de nous de rester concentré sur un seul aspect du projet.

La répartition s’est faite ainsi :

* Rudy Krauffel : Décryptage des fichiers
* Corentin Lente : Réalisation des diagrammes de processus métiers
* Louis Hans : analyse des risques et rédactions des recommandations

Tous les jours, nous nous appelions pour faire un point sur l’avancée de nos taches respectives, comme cela se fait en Daily Scrum. Nous nous sommes rendu compte que malgré les fortes différences entre nos stories, notre approche était très similaire. En effet, nous avons pris l’initiative de diviser nos items de travail en sous-tâches permettant une avancée itérative et une production de valeur continue dans le cadre de ce projet.

Cette méthode, couplée avec la mise en place d’un git pour notre projet, nous permet de vérifier l’un des points les plus importants de la méthode agile : l’intégration continue.

## Décryptage des fichiers

La problématique posée par le décryptage de ces fichiers était multiple. Il a fallu découper le décryptage en taches réalisables en moins d’une journée.

La première était de déchiffrer le rébus contenu dans le mail du hacker. La très faible résolution de l’image a rendu la tache difficile mais, nous avons réussi à obtenir ce message:

Je viens d'appliquer un algorithme de cryptage XOR tous vos fichiers. Je vous laisse une semaine pour trouver la clé de six caractères alpha minuscules, maxi. Le texte, écarté lettre par lettre avec la clé, caractère par caractère.

Le message connu, il fallu mettre en place une stratégie pour produire un programme de décryptage dans le temps imparti.

Les étapes identifiées étaient les suivantes :

* Programmer un décrypteur
* Programmer un générateur de clé
* Programmer un vérificateur de phrase décryptées
* Combiner les différentes parties du code en un Brute Force
* Tester le Brute Force sur un message crypté avec une clé de petite taille
* Lancer le Brute Force sur un fichier du projet
* Décrypter tous les fichiers avec la clé obtenue

Cette analyse a été réalisée lundi matin et le travail sur le décrypteur à commencé lundi après-midi. Le cryptage XOR étant relativement simple à mettre en œuvre, nous avons rapidement pu commencer la programmation du générateur de clés.

L’approche initiale était de générer toutes les clés possibles, de les stocker, puis de les tester une par une.

La vérification quant à elle se base sur une analyse du début du texte à décrypter, pour déceler la présence de mots français. Le programme s’est donc articulé autour de ces trois pôles : génération préliminaire des clés, décryptage, vérification.

Nous avons collaboré avec le groupe de Gérald Gatouillat pour tester en aveugle nos programmes. Un message court a été encrypté à l’aide d’une clé de 3 caractères puis échangé afin que chaque groupe puisse tester son Brute Force. Nous avons réussi à trouver la clé du message de Gérald mardi matin.

Mardi après-midi, nous avons donc tenté de lancer le programme sur les fichiers de l’entreprise MOTUC. Rapidement, nous avons réalisé que le nombre de clés de 6 caractères rendait totalement impossible leur génération et stockage préalable au décryptage. La liste de clés prenait plusieurs giga-octets d’espace mémoire et le programme était d’une lenteur inacceptable.

Un changement de stratégie a donc dû être opéré pour la génération des clés. Une création des clés à la volée à été mise en place pour optimiser le through-put du programme et réduire la charge sur la mémoire. Avec cette méthode et sans vérification du décryptage, le programme passe par toutes les clés en environ 90 minutes et n’utilisait que 15 Mo de mémoire vive.

Restait à vérifier ces possibilités générées, là aussi à la volée pour éviter le stockage. Ici aussi, un problème survenait à cause du changement d’échelle du nombre de clés. Là où le brute force du message de Gérald prenait 20 secondes, une extrapolation rapide de la vitesse d’exécution de notre programme portait la durée totale du décryptage à 300 heures. Il a donc fallu repenser la façon dont nous vérifions les phrases décryptées.

La source de la lenteur d’exécution à été identifiée comme étant le nombre élevé de comparaison avec le dictionnaire de mots français. En réduisant ces comparaisons, il devait être possible de diminuer largement le temps de complétion du brute force.

Le test de vérification a donc été modifié pour ne vérifier que les phrases portant des signes d’intelligibilité : espaces récurrents et groupements de lettres de taille raisonnable pouvant être des mots. Si cette condition n’était pas rencontrée, aucun appel au dictionnaire n’est fait, et donc pas de temps perdu. Parmi les phrases qui valident cette condition, on accepte comme solutions probables celles qui contiennent au moins trois mots reconnus comme français.

Cette méthode s’est avérée assez efficace et a trouvé la clé en 50 min. Dès lors, nous avons pu décrypter tous les fichiers, et trouvé dans l’un d’eux les instructions nécessaires à l’annulation de la rançon.

Des pistes d’amélioration n’ont pas été explorées, telles que l’utilisation du multi-threading, la gestion des caractères en Bytes plutôt qu’en tableaux de booléens, etc… Autant de solutions qui aurait surement permis d’effectuer le Brute Force en quelques minutes maximum, mais qui n’étaient plus nécessaires dès lors que nous avions décrypté les fichiers avec succès, dans la journée de mercredi.

Nous avons préféré nous concentrer sur la rédaction des documents restants.

## Réalisation des diagrammes de processus métier

Afin de répondre à la situation de crise il était demandé d’exploiter les schémas/workflow des processus métiers de l’entreprise, dans le but d’organiser au mieux la reprise de son activité. Cependant ces fichiers ne sont pas exploitables car ils ont été crypté pendant l’attaque.

Pour palier à la situation délicate dans laquelle se trouve l’entreprise et lui permettre une reprise des plus rapide de son activité, il a été demandé de réaliser de nouveaux schémas BPMN représentant les différents processus métiers de l’entreprise, et ce à partir des données que nous avons pu récupérer dans les archives.

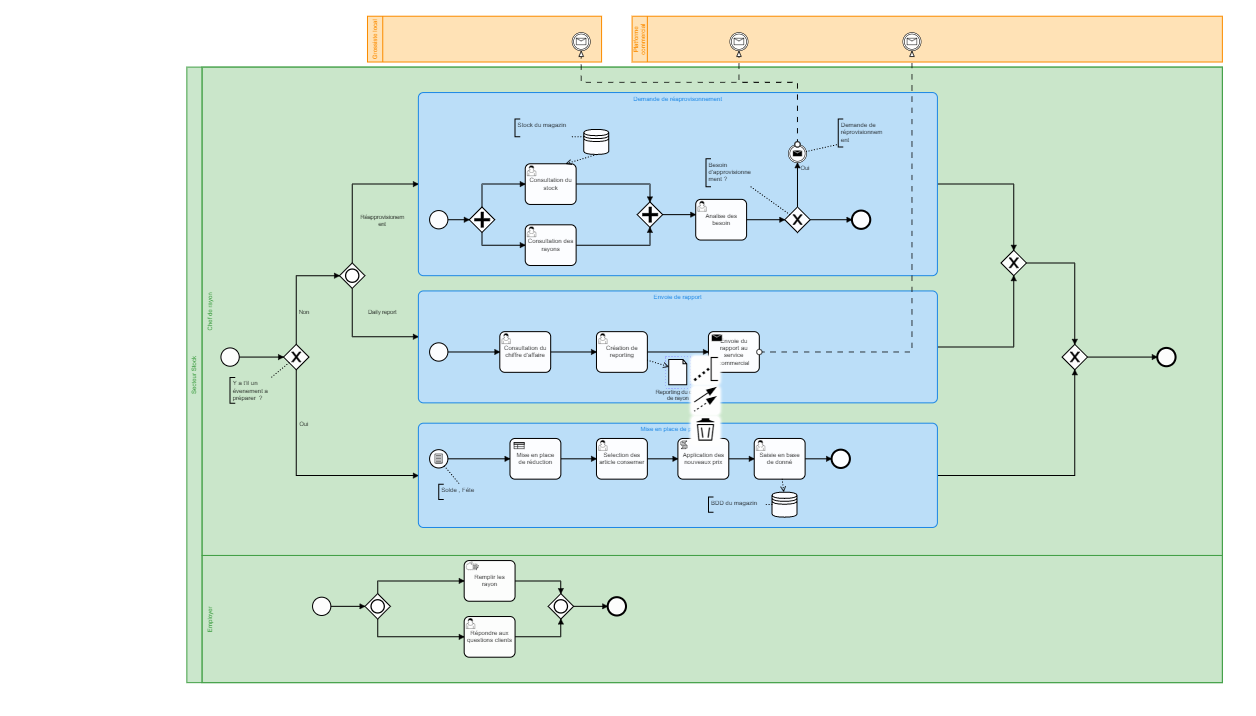
Les étapes de notre démarche :

* Identification des différents secteurs de l’entreprise
* Identification des interactions entre les différents secteurs de l’entreprise
* Identification des différents processus propre à chaque métier.
* Recherche d’informations concernant ces différents processus métier.
* Apprentissage approfondi des différentes méthodes et techniques de conception de Diagramme BPMN
* Représentation de ces processus sous forme de schémas.
* Réalisation des différents diagrammes BPMN.

Au tout début du projet, nous avons commencé par lister les différents processus métier de l’entreprise et les différentes personnes pouvant intervenir au sein de ses processus.

Une fois ces processus identifiés nous nous sommes renseignés sur les meilleurs pratiques de réalisation d’un diagramme BPMN. Nous avons mis en place une légende simple commune à tous nos diagrammes.

* En vert le secteur étudié
* En bleu les différents processus métier
* En orange les différents services avec lesquels les processus étudiés interagissent

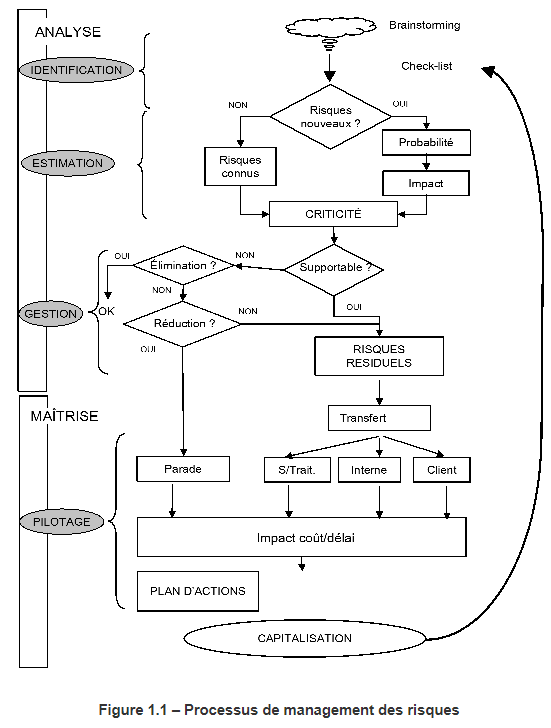


Nous avons par la suite approfondi nos recherches sur la représentation des différents processus métier chez la concurrence, dans le but de s’en inspirer pour la réalisation de nos schémas tout en les réadaptant à notre cas d’étude. Une fois ce travail réalisé nous avons débuté la réalisation de nos diagrammes BPMN.

Nous avons donc pu commencé à faire la représentation de nos différents processus métier pour les douze secteurs de l’entreprise. Certains de ces secteurs ne comportant qu’un seul processus métier il fut assez facile de les schématiser. Ce travail fut bien plus complexe pour certains secteurs de l’entreprise ou des ressources pouvaient être utilisées par différents processus simultanément. Nous retrouvâmes également cette difficulté lors de la représentation d’interaction inter-processus avec la mise en place d’événement.

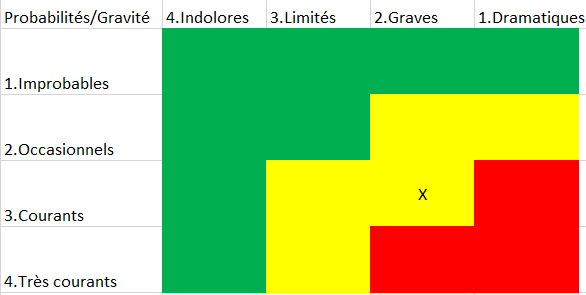
## Analyses des risques et rédaction des recommandations

Les différentes tâches qui m’ont été attribuées étaient essentiellement rédactionnelle. C’est pour cela qu’il fallait une lecture approfondie des différents documents qui nous ont été fourni. Dans cette lecture, nous devions analyser les nombreux facteurs de risque possibles. Pour cela, l’enseignement acquis lors des années scolaires a CESI a permis une rédaction d’un dossier d’analyse de risque détaillé.



Dans ce dossier, il y a des matrices pour évaluer la criticité des différents risques sur l’entreprise.

Comme cette matrice qui est simple à comprendre et facile à mettre en place.



Ici nous avons un risque qui sera donc grave et courant, il faudra donc le traiter en priorité. Voici un exemple de matrice que nous avons utilisé tout au long du dossier du management des risques pour mettre en évidence les ordres de priorités de l’entreprise concernant la gestion des risques.

Ces risques sont tous différents, il y a des risques liés à l’informatique et la sécurité comme les serveurs, la sécurisation des bâtiments et la formation du personnel. Puis il y en a d’autres plus communs à tout type d’entreprise comme les risques environnementaux, politique, de marché et bien d’autres encore.

L’élaboration de ce dossier à permis à l’entreprise d’avoir un retour global sur la gestion des risques. Par conséquent ils vont pouvoir adopter de nouvelle méthode de gestion de projet en intégrant cette gestion des risques.

## Conclusion

Ce projet s’est dans son ensemble déroulé dans de bonnes conditions.

Notre volonté d’adopter une méthode de gestion de projet favorisant la flexibilité et l’autonomie s’est avérée payante au vu des aléas rencontrés à différentes étapes de notre projet, ainsi que de la nature insolite des conditions de travail à distance pour la totalité de la durée du projet.

C’était une situation inédite pour nous et la méthode agile a inspiré un cadre de travail dans lequel nous avons pu malgré tout coordonner nos efforts et atteindre les résultats attendus.