



RAPPORT DE CONDUITE DE PROJETS

Présenté par :

Louis Dufour, Paul Squizzato, Eloan André et Darius Bertrand



2023 | FEVRIER

La présentation générale du projet :

Description succincte de votre idée du projet

Le but de cette SAE sera de développer une solution de détection d'intrusion pour les systèmes industriels.

Les systèmes industriels sont la cible de plus en plus d'attaques informatiques, dues à leur récente connexion via des réseaux vulnérables tels qu'Internet, malgré la criticité de leur utilisation (production et distribution d'énergie, assainissement des eaux, etc).

Dans le cadre de travaux internes, le CEA-Leti a développé une méthode d'analyse de risques spécifique à ce type de systèmes.

Cette méthode est capable de générer des scénarios d'attaques (suites d'actions réalisées par un attaquant) permettant de causer des dommages au système.

L'attaquant se situe sur le réseau et pourra donc envoyer, recevoir, bloquer des messages entre les dispositifs du système.

Dans le cadre de ce projet, nous cherchons à transformer cette méthode d'analyse de risques en sonde de détection d'intrusion, afin de détecter en temps réel si ces scénarios d'attaques se produisent dans le réseau (i.e., si les messages dangereux sont envoyés au bon moment par l'attaquant).

Pour ce faire, nous devons programmer des automates d'état fini afin de pouvoir suivre l'état et transformation en temps réel de ces systèmes industriels. Cela nous permettra de prévoir les attaques et de réagir en conséquence.

Genèse de l'idée du projet

L'idée à l'origine du projet provient principalement à cause d'attaques cyber qui sont des actions malveillantes menées par un individu ou une organisation pour accéder sans autorisation à des systèmes informatiques, des réseaux et des données, en causant potentiellement des dommages ou des interruptions de service volontaires. Il ne manque pas d'exemples d'attaques.

Un exemple classique d'attaque est Stuxnet, un ver informatique utilisé pour nuire aux centrales d'enrichissement d'uranium Iraniennes en 2010. L'attaque a visé les centrifugeuses, ce qui les a ralenties, causant des explosions.

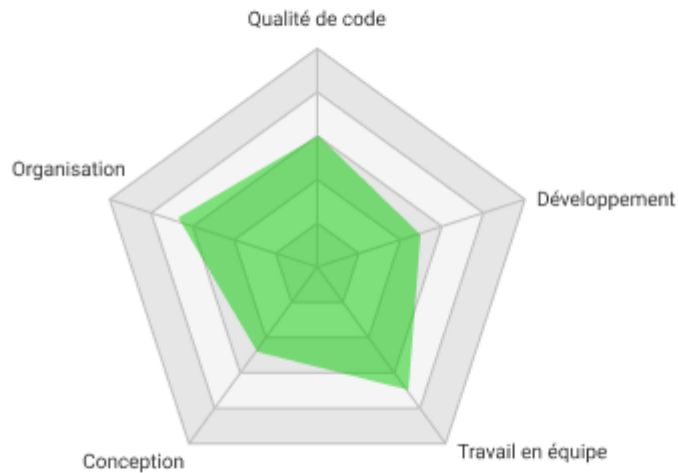
Mr. Puys, un de nos tuteurs chercheur à l'organisme CEA-Leti nous a donné une mission dans un contexte professionnel qui consiste à développer une solution de détection d'intrusion dans des systèmes industriels, leur sécurité étant une priorité.

Equipe de projet et son organisation du travail

Présentation des membres de l'équipe :



Louis Dufour



Engagement

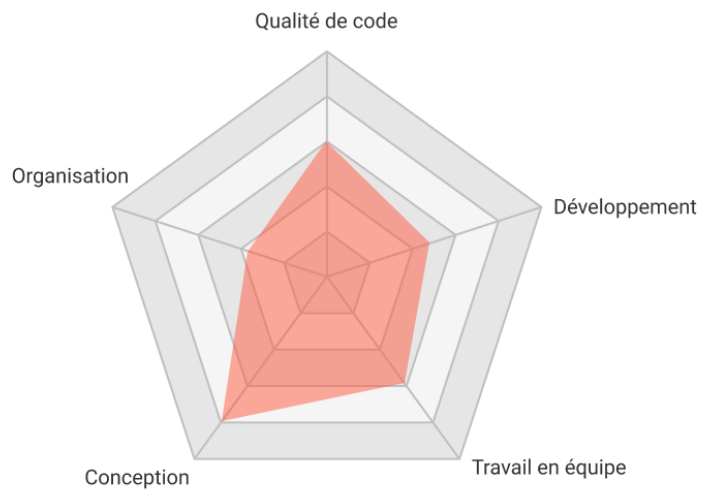


- Je m'engage à bien communiquer avec mes collègues de travail, car lors de l'ancienne SAE3.01, un gros manque de communication entre les membres, s'était fait ressentir.
- Je m'engage à mieux faire respecter l'utilisation de la méthode KanBan au sein de mon groupe.
- Je m'engage à d'avantages à communiquer avec mes tuteurs afin de leur offrir un réel suivi du projet.





Paul

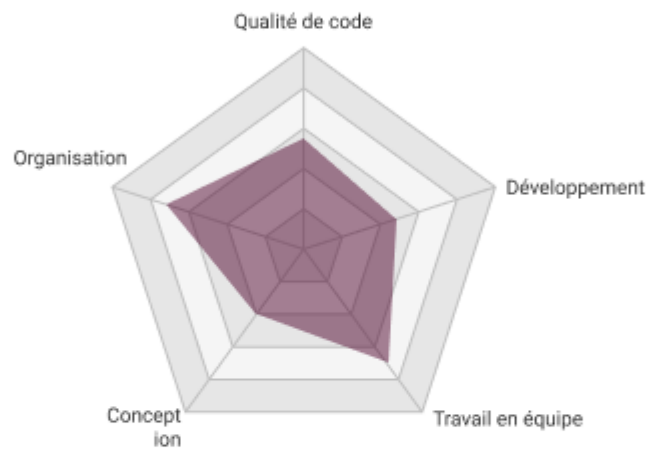


Engagement

- Je m'engage à davantage participer aux différentes parties de l'implémentation de notre projet, et de ne pas me limiter aux tâches où je suis à l'aise avec les technologies.
- Étant donné que le sujet du projet suggère un sérieux plus important que les autres applications proposées, je m'engage à ce que j'améliore mon implication personnelle en dehors des séances prévues sur l'emploi du temps.
- Je m'engage bien sûr à venir en aide à mes camarades dès qu'ils en ont le besoin, afin de faire en sorte que personne ne soit délaissé, et que le groupe reste entier jusqu'à la fin du projet.



Darius



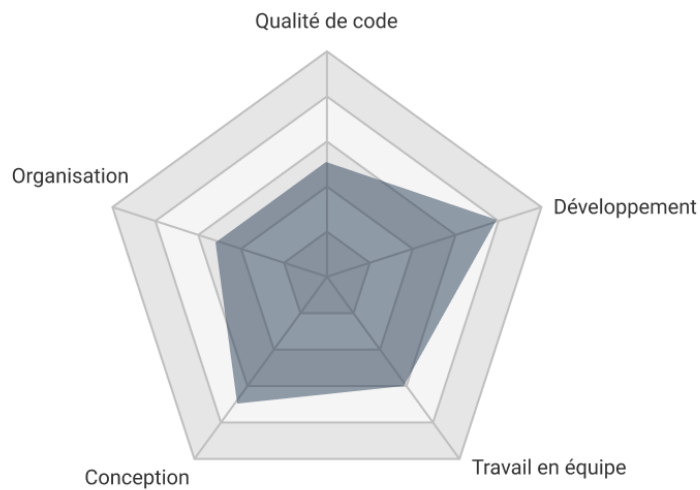
Engagement



- Je m'engage à bien me documenter dès le début du projet et en dehors des heures de celui-ci sur les différents langages que l'on utilise.
- Je m'engage à mieux gérer mon temps sur chaque tâche et à utiliser le kaban.
- Je m'engage à mieux communiquer avec notre tuteur pour pouvoir lui poser le plus de questions possible.

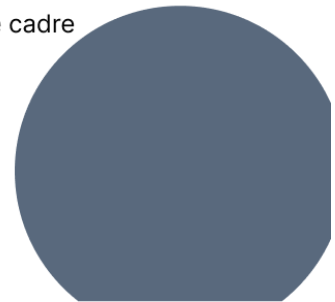


Eloan



Engagement

- Je m'engage à travailler plus souvent de chez moi car lors de ma précédente SAE, il s'agissait d'un points que je n'arrivais pas à mettre en place
- Je m'engage à aider mes collègues sur les sections de code ou de documentation que j'ai faites
- Je m'engage à faire beaucoup de recherche sur la sécurité dans le cadre de ce projet



Notre organisation de travail pour ce projet :

Pour ce projet, nous avons choisi de partir sur une **méthode agile**, car c'est un projet tout nouveau pour nous et il n'est pas exclu que certaines prévisions soient amenées à changer. Suite à la nature du projet qui a la possibilité d'être extensible.



Figure 1 : Scrum

Dans notre contexte le **scrum master** n'est pas réellement présent, c'est-à-dire que personne n'est derrière nous afin de bien vérifier à la bonne pratique de la méthode Scrum ou encore une personne qui assistera le product owner.

Le **product owner** pour ce projet sera notre tuteur **Maxime Puys**. Son rôle est de représenter les besoins client. Son but va être de créer une vision produit. Sa grande charge est de créer le document backlog. Il priorise les tâches et explique le contenu. Il va gérer les dates butoir et les RELEASE(les versions) c'est un ensemble de sprint. S'il n'est pas assez présent, il peut déléguer à un **Proxy Product Owner (PPO)**. Dans notre cas, cette responsabilité sera déléguée à Louis, mais une fois le sprint commencé, il ne peut pas et ne doit pas changer ce que va faire l'équipe. Nos dates butoir seront fortement appuyées par l'outil PERT qu'on verra plus tard.

Notre équipe scrum : comme vous l'aurez compris dans la présentation des membres. Ce n'est pas toujours la même personne qui s'occupe de la même tâche, car nous sommes multi compétences.

Notre équipe s'organise elle-même pour les tâches. C'est-à-dire qu'on discute entre nous afin de s'entraider ou d'encore se répartir les tâches afin que tout le monde puisse avoir une vision globale du projet et qui puisse en ressortir une expérience.

Notre but n'est pas de viser la production, mais plutôt la mise à niveau de chacun pour qu'on puisse monter en compétences sur nos futurs projets. Notre organisation de l'espace dédié à l'équipe est aussi réfléchi.

Les outils utilisés par notre équipe



Discord : qui nous permet de communiquer entre nous et de s'échanger des informations (*Image, liens de documentation, ...*)



Figma : permet la réalisation de certains composants pour le rapport (*pour ce rapport, les cartes des membres ont été réalisées sous cet outil*)



Diagrams.net : permet la réalisation des schémas conceptuels de notre projet.



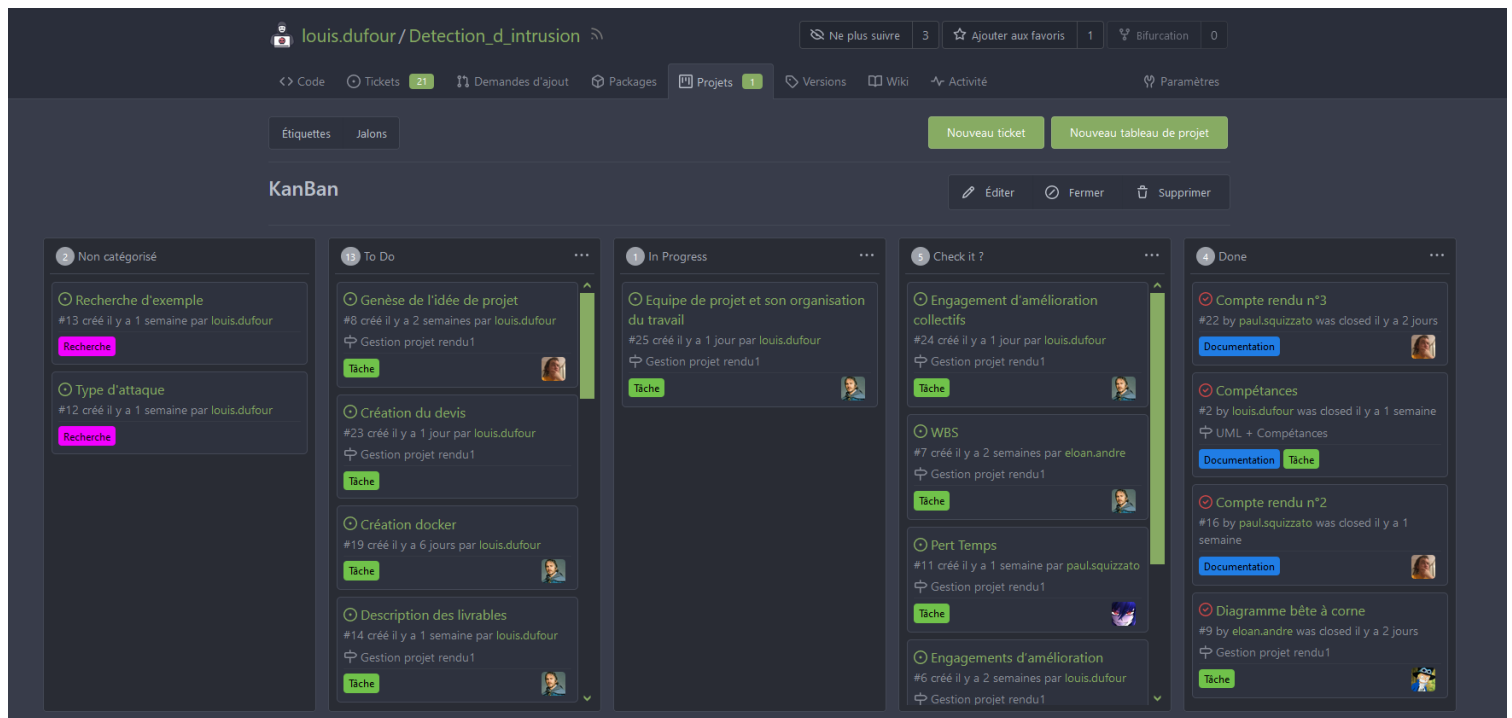
Drive Google : très utile pour réaliser des documents en équipe (*gdocs, gsheets, ...*)

Comme l'implique la méthode agile, nous réalisons des **daily meeting** avec Maxime afin d'avoir un suivi continue sur le sprint en cours de réalisation. Ces réunions ont des durées plus ou moins variables, mais actuellement nous nous rencontrons chaque semaine pendant moins d'une heure pour faire le point. (problèmes rencontrés, ce qu'on a fait et ce qu'on compte faire)

Actuellement, nous n'avons pas encore réalisé de **sprint planning meeting** ou encore de **sprint review** et **sprint retrospective**. Nous sommes actuellement au début du projet et nous venons tout juste de finir la planification de notre projet.

Nous n'utilisons pas encore d'outils d'artefacts comme burn down charts. Par contre nous avons mis en place un KanBan. Le **KanBan** est un système permettant de partager l'information et de maîtriser visuellement le flux de travail. Il est fortement favorisé dans notre projet, car cela nous permet de pouvoir voir ce que chacun fait au moment T. Cela évite des erreurs de communications ou encore que certaines personnes se retrouvent à faire la même chose et par conséquent d'avoir une perte de ressource.

Voici un exemple de notre KanBan actuel



Il s'organise en 5 colonnes :

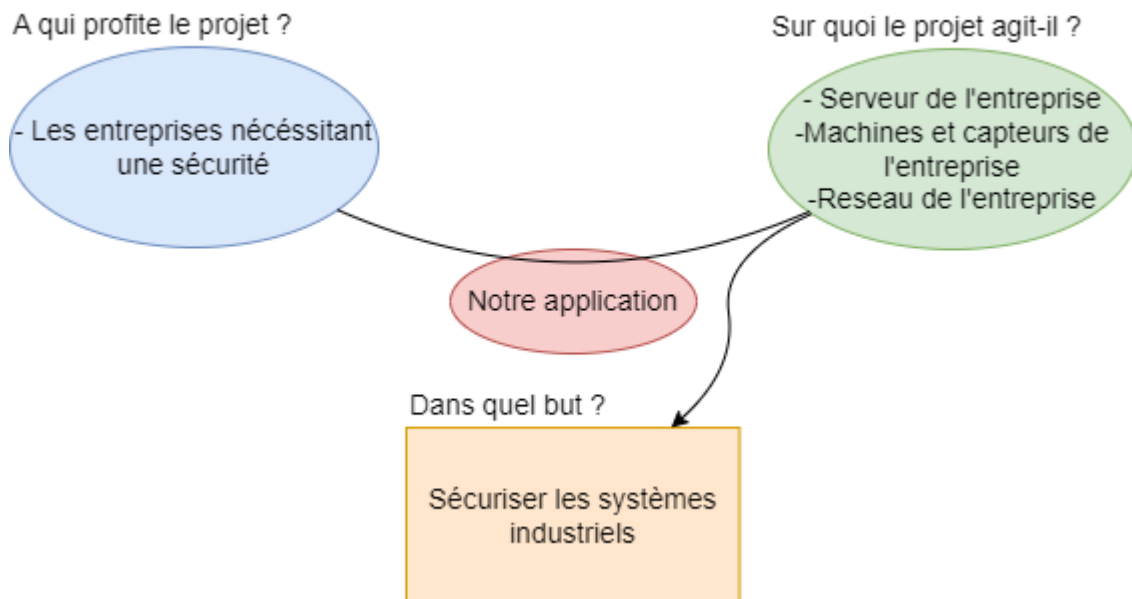
- Non catégorisé = pour les tâches qui sont destinées à la recherche principalement
- To Do = Ceux qui doit être fait
- In Progress = Ceux qui est entrain de se réaliser
- Check it ? = Ceux qu'il faudra vérifier
- Done = Ce qui est fini

Engagement d'amélioration collectifs concrets par rapport à la SAE3.01

Notre groupe s'engage à :

- Faire preuve de rigueur quant à notre gestion de projet, avec une utilisation régulière et poussée de notre KanBan, ainsi que des tickets sur Codefirst.
- Répondre au besoin client demandé : qui est dans notre cas, la création d'une solution pour notre tuteur qui travaille en tant que chercheur dans l'organisme CEA-Leti.
- Nous nous engageons à livrer une application un minimum fonctionnelle

Transcription des besoins



Nous avons fait le choix de présenter uniquement un diagramme de bête à corne pour le moment. Comme vous l'aurez compris nous travaillons en méthodes agiles et notre projet est extensible en fonction de son avancée.

Description des livrables

Pour ce projet, nous aurons plusieurs livrables. Parmi eux, il y aura un récapitulatif au format PDF contenant le budget final, l'avancée du projet et un rappel des contraintes ainsi que des éléments montrant que nous les aurons respectées.

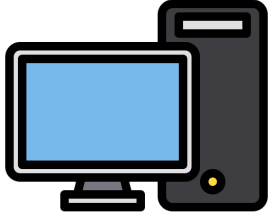



Nous devons rendre une application fonctionnelle, en plusieurs versions, avec le code jusqu'à atteindre la version finale.

Également, nous mettrons en ligne plusieurs versions de la documentation du code de l'application, pour la version finale bien sûr, mais aussi des versions antérieures puisque nous avons choisi de nous orienter vers une intégration et un développement continu.

L'application devra donc répondre aux attentes et aux fonctionnalités prévues en proposant une surveillance adaptée en fonction de la machine industrielle et en fonction de son environnement. Elle doit être en mesure de contrôler et notifier si un problème d'intrusion est détecté.

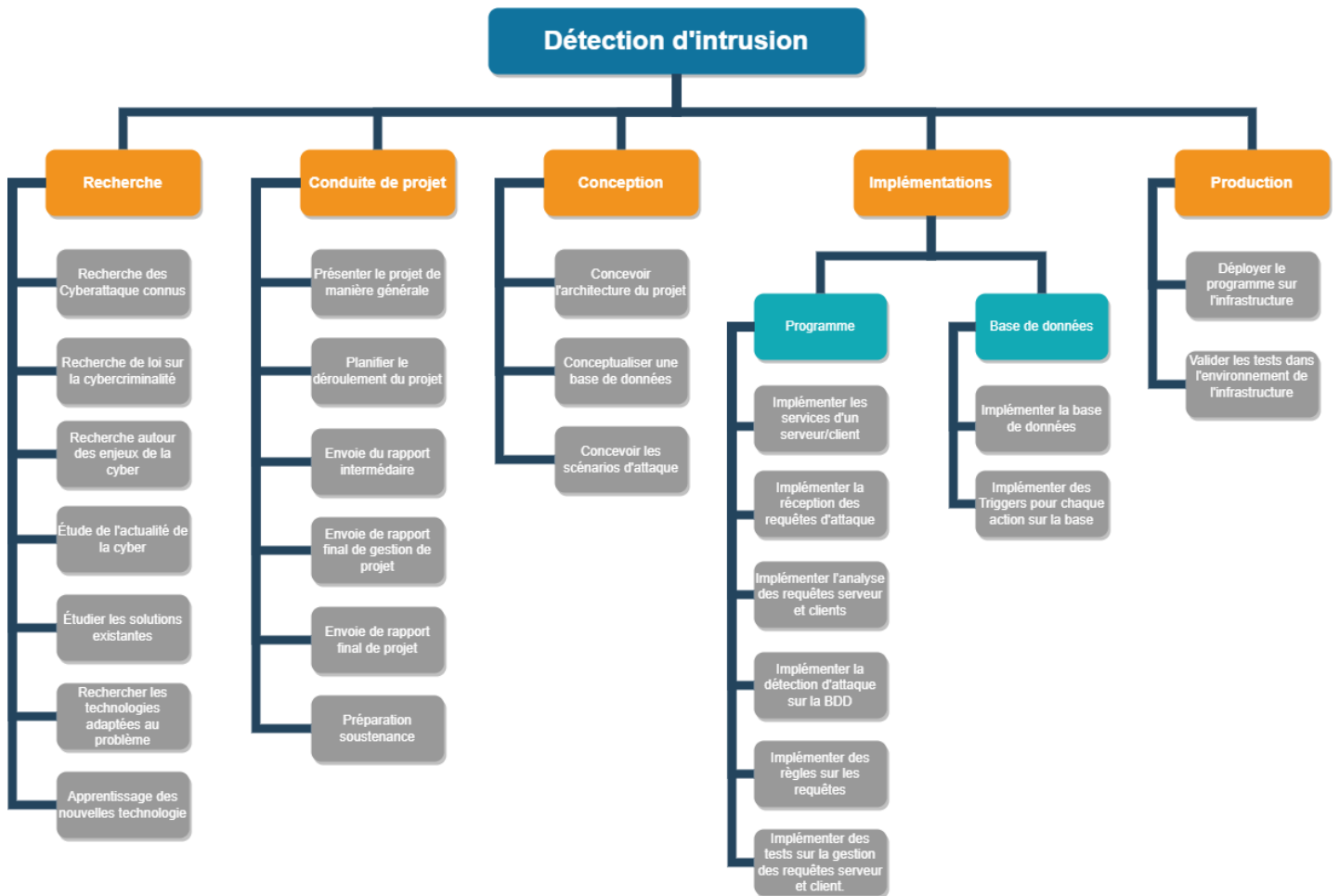
Contraintes

Lors du déroulement de ce projet nous devons nous adapter à différentes contraintes t'elle que:

Type de Contraintes	Description
Matériel 	Nous avons une contrainte de sécurité qui nous empêche d'être administrateur sur nos postes de travail. Par conséquent, nous utilisons des machines virtuelles afin de réaliser notre développement.
Humaine 	Notre tuteur n'étant pas professeur sur le site de l'IUT, il sera plus difficile de le voir pour lui montrer notre avancement.
Coût 	<p>Nos coûts sont une énorme contrainte, car le projet peut demander très rapidement un gros investissement financier en fonction de sa nature.</p> <p>La raison principale provient des tests, car nous devons peser le facteur de coût et d'effort par rapport au résultat venant de nos tests pour limiter le nombre de bug.</p> <p>Si l'investissement financier est léger par rapport au sujet. Nous serions dans l'obligation de refuser pour ne pas avoir la responsabilité des risques de bugs potentiels.</p>
Juridique 	<p>La plus grosse contrainte du projet repose principalement sur des lois juridiques qui nous forcent à sécuriser efficacement notre programme.</p> <p>Ou encore de garantir la maintenabilité du produit.</p>


La planification du projet :

WBS - La décomposition du projet en tâches élémentaire



PERT Temps

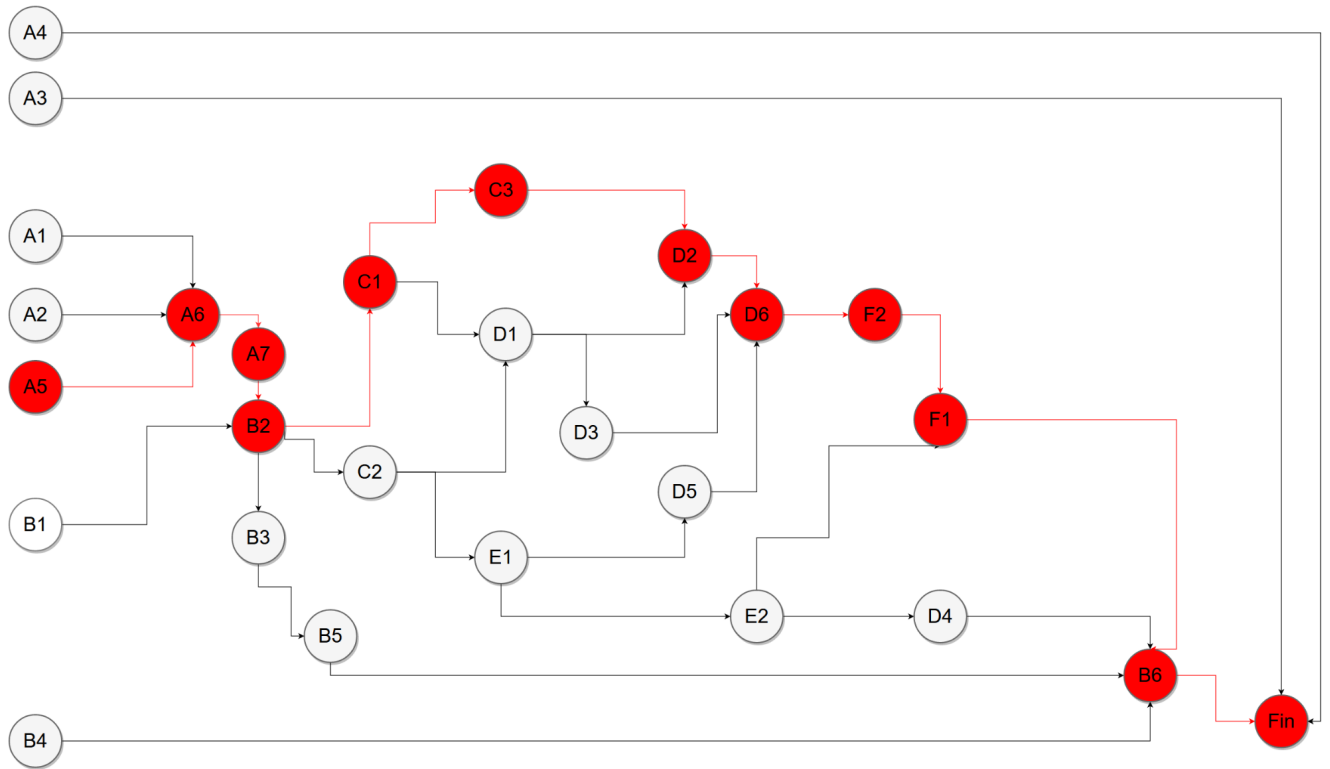
 : Tâches critiques

 : Tâches potentiellement modifiables

Tâches	Tâches	Estimation temps en heures	Date début	Date limites	Antériorités	Début de la tâche au plus tôt	Fin de la tâche au plus tôt	Début de la tâche au plus tard	Fin de la tâche au plus tard	Marge	Remarque
Recherche des Cyberattaques connus	A1	3	25-01-2023	28-01-2023	-	0	3	3	6	3	
Recherche de loi sur la cybercriminalité	A2	3	25-01-2023	28-01-2023	-	0	3	3	6	3	
Recherche autour des enjeux de la cyber	A3	2	25-01-2023	03-04-2023	-	0	2	73	75	73	
Etude de l'actualité de la cyber	A4	2	25-01-2023	03-04-2023	-	0	2	73	75	73	
Etudier les solutions existantes	A5	6	25-01-2023	28-01-2023	-	0	6	0	6	0	
Rechercher les technologies adaptées au problème	A6	5	28-01-2023	30-01-2023	A1/A2/A5	6	11	6	11	0	
Apprentissage des nouvelles technologies	A7	6	30-01-2023	04-02-2023	A6	11	17	11	17	0	
Présenter le projet de manière générale	B1	4	25-01-2023	01-02-2023	-	0	4	13	17	13	
Planifier le déroulement du projet	B2	4	04-02-2023	08-02-2023	A7/B1	17	21	17	21	0	
Envoi du rapport intermédiaire	B3	6	08-02-2023	09-02-2023	B2	21	27	58	64	37	
Envoi de rapport final de projet	B4	8	25-01-2023	27-03-2023	-	0	8	62	70	62	
Envoi de rapport final de gestion de projet	B5	6	09-02-2023	30 mars	B3	0	6	64	70	64	
Soutenance final	B6	5	31-03-2023	03-04-2023	F1/B4/B5/D4	70	75	70	75	0	
Concevoir l'architecture du projet	C1	5	08-02-2023	16-02-2023	B2	21	26	21	26	0	

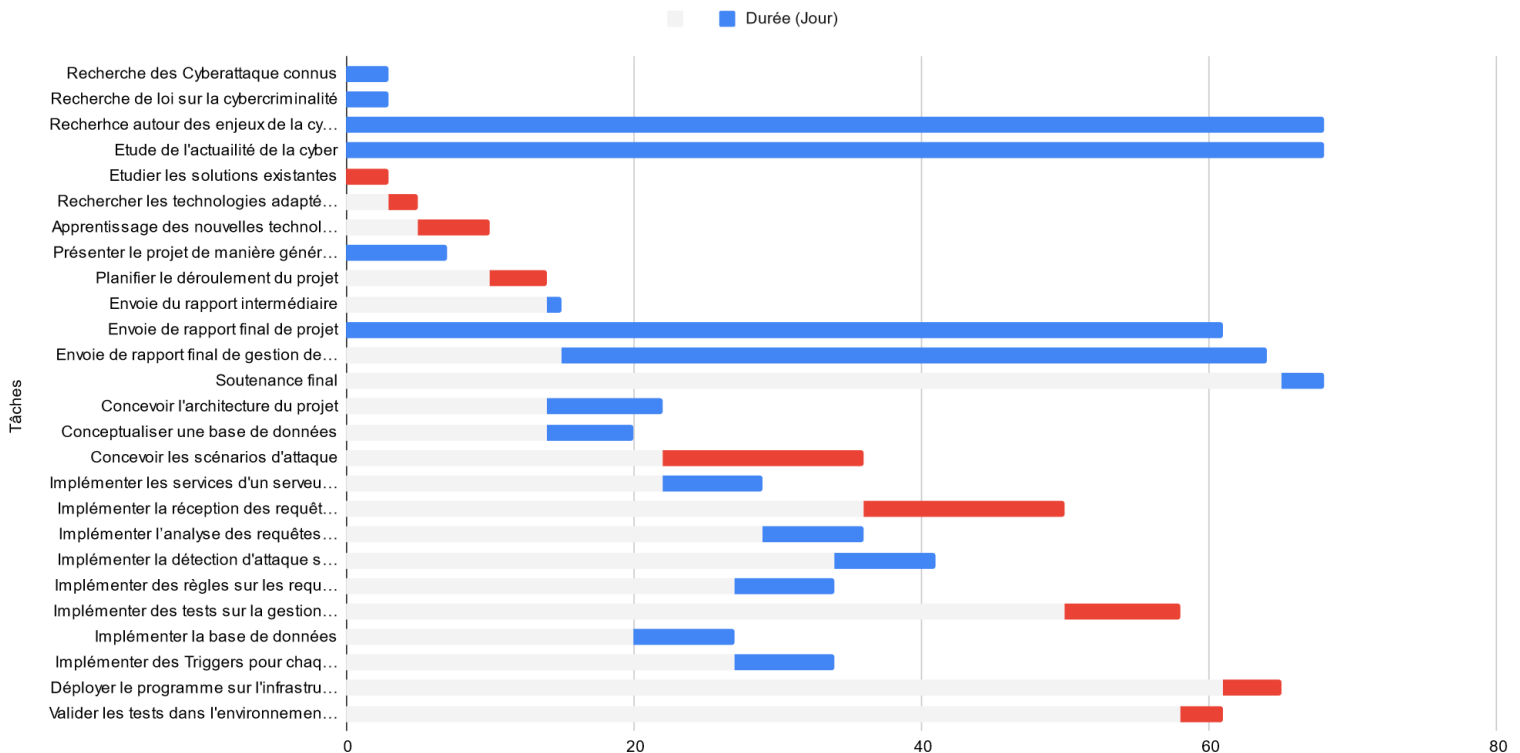
Conceptualiser une base de données	C2	4	08-02-2023	14-02-2023	B2	21	25	23	27	2	Le projet évoluera ensuite au CEA pour l'adapter à toutes les bases de données
Concevoir les scénarios d'attaque	C3	7	16-02-2023	02-03-2023	C1	26	33	26	33	0	
Implémenter les services d'un serveur/client	D1	5	16-02-2023	23-02-2023	C1/C2	26	31	30	35	4	
Implémenter la réception des requêtes d'attaque	D2	12	02-03-2023	16-03-2023	C3/D1	33	45	33	45	0	Cette estimation de temps pourrait être modifiée
Implémenter l'analyse des requêtes serveur et clients	D3	10	23-02-2023	02-03-2023	D1	31	41	35	45	4	
Implémenter la détection d'attaque sur la BDD	D4	13	28-02-2023	07-03-2023	E2	35	48	57	70	22	Cette estimation de temps pourrait être modifiée
Implémenter des règles sur les requêtes	D5	8	21-02-2023	28-02-2023	E1	27	35	37	45	10	
Implémenter des tests sur la gestion des requêtes serveur et client.	D6	15	16-03-2023	24-03-2023	D2/D3/D5	45	60	45	60	0	
Implémenter la base de données	E1	2	14-02-2023	21-02-2023	C2	25	27	35	37	10	Le projet évoluera ensuite au CEA pour l'adapter à toutes les bases de données
Implémenter des Triggers pour chaque action sur la base	E2	6	21-02-2023	28-02-2023	E1	27	33	51	57	24	Nous ne sommes pas certains de comment va se dérouler cette tâche et si sa désignation devrait changer
Déployer le programme sur l'infrastructure	F1	4	27-03-2023	31-03-2023	E2/F2	66	70	66	70	0	
Valider les tests dans l'environnement de l'infrastructure	F2	6	24-03-2023	27-03-2023	D6	60	66	60	66	0	
total:		157							Tâches potentiellement modifiables		

PERT



GANTT Prévisionnel

GANTT prévisionnel



Rouge : Chemin critique

Date jalon (chemin critique)

1. **08-02-2023** : Planifier le déroulement du projet
2. **16-02-2023** : Concevoir l'architecture du projet
3. **02-03-2023** : Concevoir les scénarios d'attaque
4. **16-03-2023** : Implémenter la réception des requêtes d'attaque
5. **24-03-2023** : Implémenter des tests sur la gestion des requêtes serveur et client.
6. **27-03-2023** : Valider les tests dans l'environnement de l'infrastructure
7. **31-03-2023** : Déployer le programme sur l'infrastructure
8. **03-04-2023** : Soutenance

ESTIMATIONS DES COÛTS



Délivré à :

Aubière
5 Av. Blaise Pascal 63170

Date de délivrance

9 Février 2023

Description	Quantité	Prix unité	Total
Machine	2	\$2500	\$5000
Développeur	4	\$2750	\$11000
Abonnement Internet	1	\$300	\$300
Total			\$16300

INFORMATION DE GROUPE

Groupe SAE
Nom des membres :
ANDRE Eloan
BERTRAND Darius
DUFOUR Louis
SQUIZZATO Paul
Intitulé de projet : Détection d'intrusion
Payez avant le : 30 novembre 2023

A handwritten signature in black ink, appearing to be 'A. Eloan', written over a light blue horizontal line.

Directeur financier autoproclamé

Indicateurs de suivi de projet et de qualité. Justification du choix des indicateurs

Notre indicateur clé le plus important est le temps, le coût n'étant pas une réelle contrainte dans notre cadre d'étudiant.

Efficacité

- Temps d'avance ou de retard = Temps prévisionnel - Temps accordé à la tâche en tout
- Nombre de merge
- Nombre de commit

Réactivité

- Temps moyen nécessaire pour résoudre un problème critique (ex: Problème pour charger les tables)
- Temps moyen nécessaire pour résoudre un problème mineur (ex: Requête ne fonctionne pas)
- Temps de réponse à un problème de conception

Qualité

Du code :

- Taux d'erreurs = Nombre de bugs/ Lignes de code (à l'aide de sonarQube intégré à Code#0)
- Nous compterons aussi à l'aide de Code#0 le nombre de vulnérabilités qui devra être de 0 si l'on travaille sur une application de sécurité

De l'application :

- Nombre de retours d'utilisateurs positifs / Nombre de retours d'utilisateurs

Facteurs évitables

- Perte de temps : Temps d'attente d'une réponse - Temps de résolution si utilisation optimale des ressources à disposition
- Taux : Perte de temps totale / Temps du projet