



160-4-72

PROJETS TRANSVERSAUX APPLIQUÉS AU DÉVELOPPEMENT DURABLE

les membres du groupe :

- Ilhan Gokmen
- Mohamed Ilias Hamlaoui
- Louisa Ould Bouali
- Oussama Yassine
- Melissa Yessad

les rôles :

Louisa Ould Bouali	DEVELOPER
Ilhan Gokmen	CHEF DE PROJET
Mohamed Ilias Hamlaou	SCRUM MASTER
Oussama Yassine	LEAD DEVELOPER
Melissa Yessad	DEVELOPER

Choix du sujet :

Cybersécurité : cartographie des attaques et prévisions des menaces

Ce sujet nous a intéressés car il allie analyse de données, prévention des risques et enjeux réels de sécurité. Il permet aussi de se familiariser avec des outils utilisés dans le monde professionnel.



Description du sujet :

Source : [Kaggle](#)

Le projet consiste à créer un site web interactif présentant une carte du monde des cyberattaques. L'objectif est de visualiser les attaques avec des filtres dynamiques (par type, pays et date), **si les données nécessaires sont disponibles**. Des graphes récapitulatifs et des pop-ups informatifs détailleront chaque attaque. Une section dédiée expliquera les types d'attaques, avec éventuellement un chatbot NLP. Les données seront analysées, transformées, testées, puis affichées de manière claire. Le projet inclut aussi un suivi rigoureux du code, des tests, de la documentation et de l'organisation.

Description des données :

Les données utilisées regroupent différentes cyberattaques survenues dans plusieurs pays, entre autres la **Chine**, **l'Inde**, le **Royaume-Uni**, ou encore **l'Allemagne**.

kaggle_data									
Country	Year	Attack Type	Target Industry	Financial Loss (in Million \$)	Number of Affected Users	Attack Source	Security Vulnerability Type	Defense Mechanism Used	Incident Resolution Time (in Hours)
China	2019	Phishing	Education	80.53	773169	Hacker Group	Unpatched Software	VPN	63
China	2019	Ransomware	Retail	62.19	295961	Hacker Group	Unpatched Software	Firewall	71
India	2017	Man-in-the-Middle	IT	38.65	605895	Hacker Group	Weak Passwords	VPN	20
UK	2024	Ransomware	Telecommunications	41.44	659320	Nation-state	Social Engineering	AI-based Detection	7
Germany	2018	Man-in-the-Middle	IT	74.41	810682	Insider	Social Engineering	VPN	68
Germany	2017	Man-in-the-Middle	Retail	98.24	285201	Unknown	Social Engineering	Antivirus	25
Germany	2016	DDoS	Telecommunications	33.26	431262	Insider	Unpatched Software	VPN	34
France	2018	SQL Injection	Government	59.23	909991	Unknown	Social Engineering	Antivirus	66
India	2016	Man-in-the-Middle	Banking	16.88	698249	Unknown	Social Engineering	VPN	47
UK	2023	DDoS	Healthcare	69.14	685927	Hacker Group	Unpatched Software	Firewall	58
China	2019	Phishing	Telecommunications	88.67	493675	Unknown	Zero-day	VPN	29
China	2016	SQL Injection	Healthcare	38.81	920768	Hacker Group	Unpatched Software	AI-based Detection	27
India	2019	Ransomware	Education	30.56	583204	Insider	Zero-day	Firewall	37
France	2023	DDoS	Healthcare	58.37	599797	Nation-state	Unpatched Software	AI-based Detection	35
France	2024	DDoS	IT	48.01	922258	Unknown	Social Engineering	Encryption	64
Australia	2022	Phishing	Banking	64.31	120789	Nation-state	Zero-day	Encryption	36
Russia	2017	Man-in-the-Middle	Healthcare	13.04	850158	Hacker Group	Unpatched Software	AI-based Detection	67
India	2015	DDoS	IT	93.14	805278	Insider	Social Engineering	Encryption	56
UK	2019	Malware	Telecommunications	14.01	578443	Insider	Social Engineering	Firewall	28
India	2016	DDoS	IT	36.45	261808	Nation-state	Social Engineering	AI-based Detection	6
Brazil	2015	Ransomware	Retail	49.55	920172	Hacker Group	Weak Passwords	Antivirus	43
France	2023	Ransomware	Education	17.72	261661	Insider	Social Engineering	VPN	11
India	2017	DDoS	Government	76.71	246205	Nation-state	Unpatched Software	Firewall	30
Japan	2022	Phishing	Telecommunications	20.42	186148	Nation-state	Weak Passwords	Antivirus	32
Brazil	2023	DDoS	Telecommunications	51.84	699007	Hacker Group	Social Engineering	VPN	30
China	2021	Phishing	Retail	51.06	628562	Insider	Zero-day	AI-based Detection	52
Japan	2022	Malware	Education	53.04	570494	Nation-state	Unpatched Software	VPN	53
Japan	2022	Ransomware	Banking	26.17	937653	Insider	Unpatched Software	Encryption	24
France	2020	Malware	IT	87.32	599757	Unknown	Social Engineering	Antivirus	9
Australia	2015	DDoS	Government	82.7	904805	Hacker Group	Zero-day	Encryption	61
UK	2022	SQL Injection	Education	66.24	678876	Hacker Group	Social Engineering	AI-based Detection	11
France	2020	Malware	Telecommunications	18.38	246900	Hacker Group	Zero-day	AI-based Detection	34
India	2015	SQL Injection	IT	42.99	85255	Unknown	Unpatched Software	Encryption	61
Japan	2022	Phishing	Banking	98.47	972469	Nation-state	Zero-day	Antivirus	21
Brazil	2023	Phishing	Healthcare	14.51	113777	Nation-state	Weak Passwords	VPN	27
Brazil	2020	Phishing	Banking	17.75	739540	Hacker Group	Zero-day	Encryption	31
China	2020	Man-in-the-Middle	Education	19.81	722788	Nation-state	Zero-day	Firewall	70
Japan	2021	SQL Injection	Retail	82.52	214372	Insider	Unpatched Software	Encryption	12
USA	2022	DDoS	Retail	32.53	235314	Insider	Weak Passwords	AI-based Detection	62
Brazil	2016	DDoS	Education	96.98	140812	Nation-state	Unpatched Software	VPN	71

Chaque ligne représente une attaque, avec des informations comme :

- le type d'attaque (phishing, ransomware, etc.),
- l'industrie ciblée (éducation, IT, télécoms...),
- le nombre d'utilisateurs affectés,
- les pertes financières estimées,
- l'origine de l'attaque (groupe de hackers, États, etc.),
- la faille de sécurité exploitée (mot de passe faible, logiciel non mis à jour...),
- le mécanisme de défense utilisé,
- et le temps de résolution de l'incident.

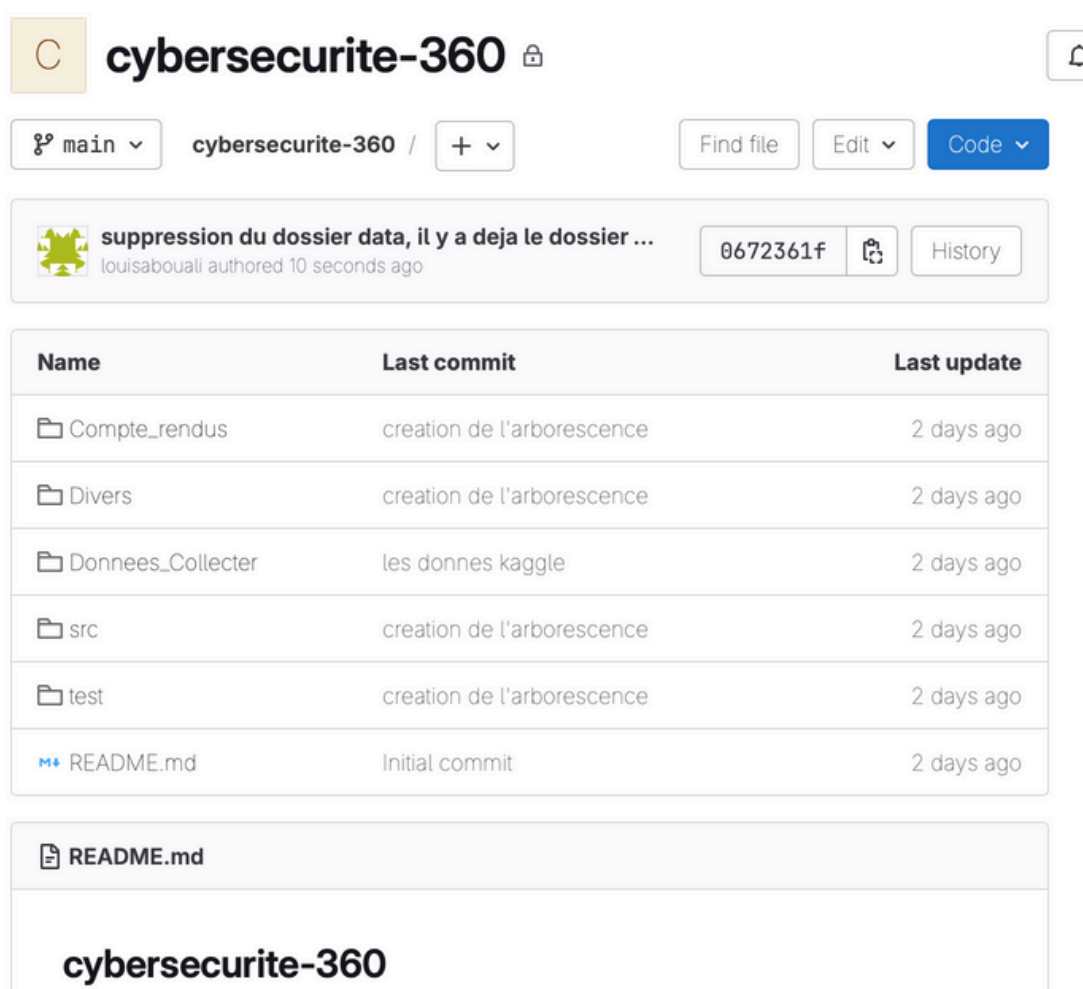
outil de gestion de versions et d'accès concurrents au code : **Git**

Le lien : <https://gitlab.univ-lr.fr/cybersecurite-360/cybersecurite-360>

Nous avons choisi **GitLab** comme outil de gestion de versions et d'accès au code, car tous les membres du groupe le maîtrisent déjà.

Concernant l'organisation du projet, nous nous sommes mis d'accord sur la structure suivante :

- **Compte_rendus**
- **Divers**
- **Donnees_Collecter**
- **src**
- **test**
- **README.md**



The screenshot shows the GitLab interface for the repository 'cybersecurite-360'. At the top, there's a navigation bar with 'main' selected, the repository name 'cybersecurite-360', and buttons for 'Find file', 'Edit', and 'Code'. Below this, a commit message 'suppression du dossier data, il y a deja le dossier ...' by 'louisabouali' is shown. The main content is a table listing the repository's structure:

Name	Last commit	Last update
Compte_rendus	creation de l'arborescence	2 days ago
Divers	creation de l'arborescence	2 days ago
Donnees_Collecter	les donnes kaggle	2 days ago
src	creation de l'arborescence	2 days ago
test	creation de l'arborescence	2 days ago
README.md	Initial commit	2 days ago

Below the table, there's a section for 'README.md' with the repository name 'cybersecurite-360' displayed.

Le dossier **Compte_rendus** contient tous les comptes rendus hebdomadaires.

Dans **Donnees_Collecter**, on trouve les données à utiliser ainsi qu'un fichier .md qui explique leur utilisation : à quoi elles servent, pourquoi et comment elles ont été collectées.

Le code source est placé dans **src**, les tests dans **test**, et les fichiers divers dans **Divers**.

Enfin, le **README** sera complété progressivement, au fur et à mesure de l'avancement du groupe et du projet.

Gestion de projet : Trello

Le lien : <https://trello.com/b/HxLaeJRG/lu2in013-projet>

Nous avons de nouveau choisi d'utiliser **Trello**, car la plupart des membres du groupe l'ont déjà utilisé.

Notre organisation repose sur plusieurs listes :

- **Tâches** : pour toutes les tâches à faire
- **En cours** : pour les tâches en cours de réalisation
- **Test** : pour les tâches terminées mais qui doivent encore être testées
- **Done** : pour les tâches entièrement terminées
- **Validé** : une liste où l'on déplace chaque semaine les tâches validées par l'ensemble du groupe (utile pour rédiger les comptes rendus)
- **Backlog** : une liste qui regroupe les grandes tâches du projet, classées par catégories (organisation, développement, administration), et qui sert à partager les idées du groupe.

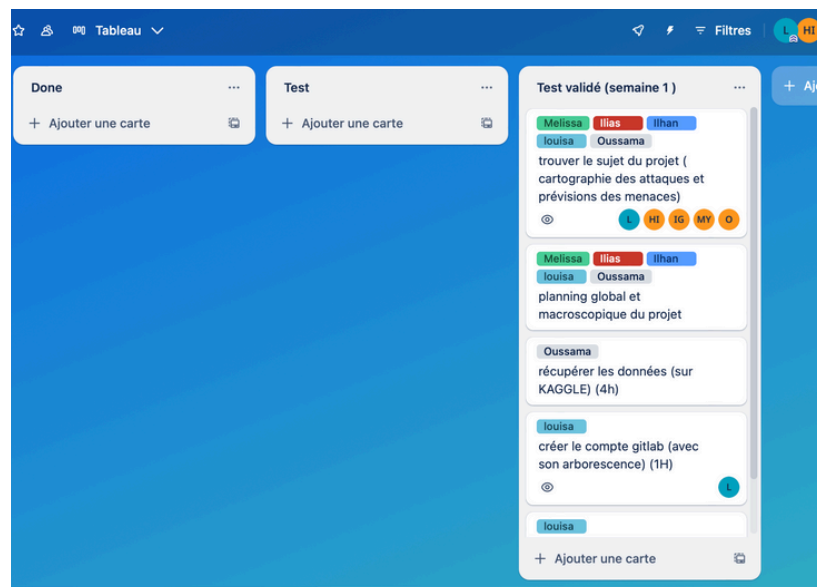
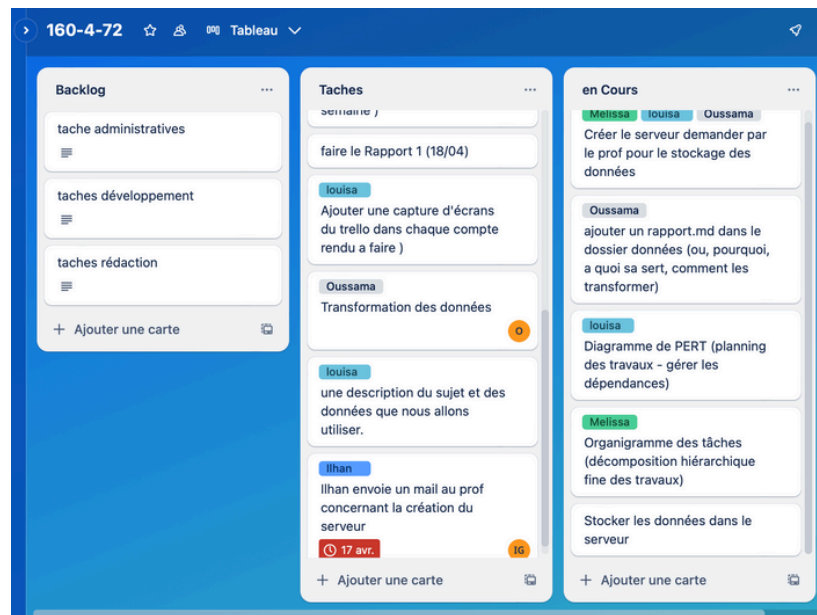
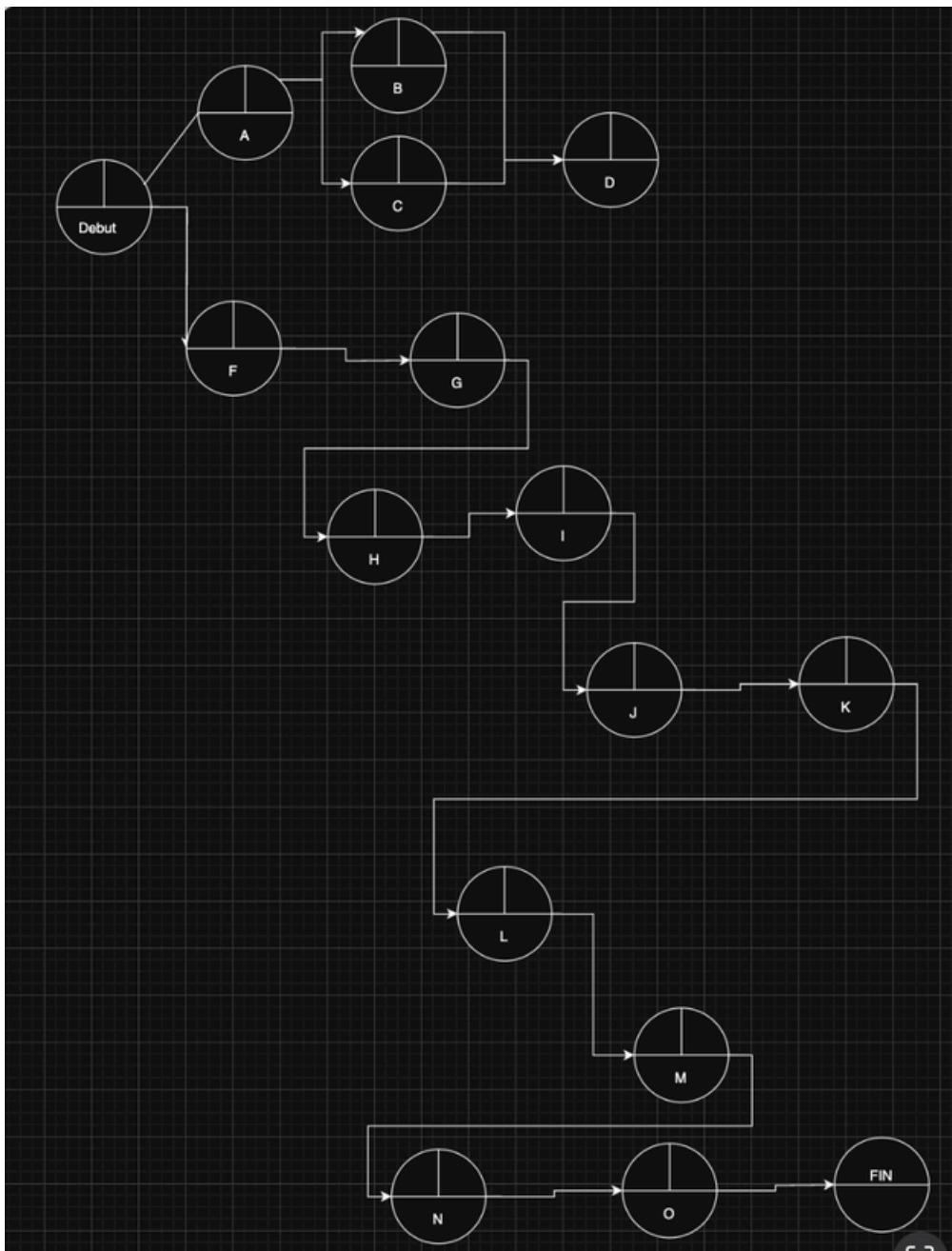


Diagramme de PERT:

ID	Tâche	Durée (jours)	Dépend de
A	Conception <u>Figma</u>	3	-
B	Développement <u>Front-End</u>	1	A
C	Développement <u>Back-End</u>	6	A
D	Intégration & Tests	6	B, C
E	Déploiement	4	D
F	Collecte des données	3	-
G	Compréhension des données	3	F
H	Traitement des données	3	G
I	Nettoyage des données	2	H
J	Gestion des données manquantes	2	I
K	Visualisation des données	3	J
L	Identification des KPis	2	K
M	Sélection des <u>short-cuts</u>	2	L
N	Inspection des données	2	M
O	Rapport final d'analyse	2	N

Diagramme de PERET :

Ce diagramme permet de mieux comprendre les relations entre les tâches et d'identifier les chemins critiques qui pourraient affecter l'avancement du projet.
Organigramme non complet!!



Organigramme Fonctionnel des taches:

Il aide à clarifier l'ensemble des tâches nécessaires à la réalisation du projet et à attribuer des responsabilités spécifiques à chaque membre de l'équipe, tout en permettant une gestion détaillée des ressources.

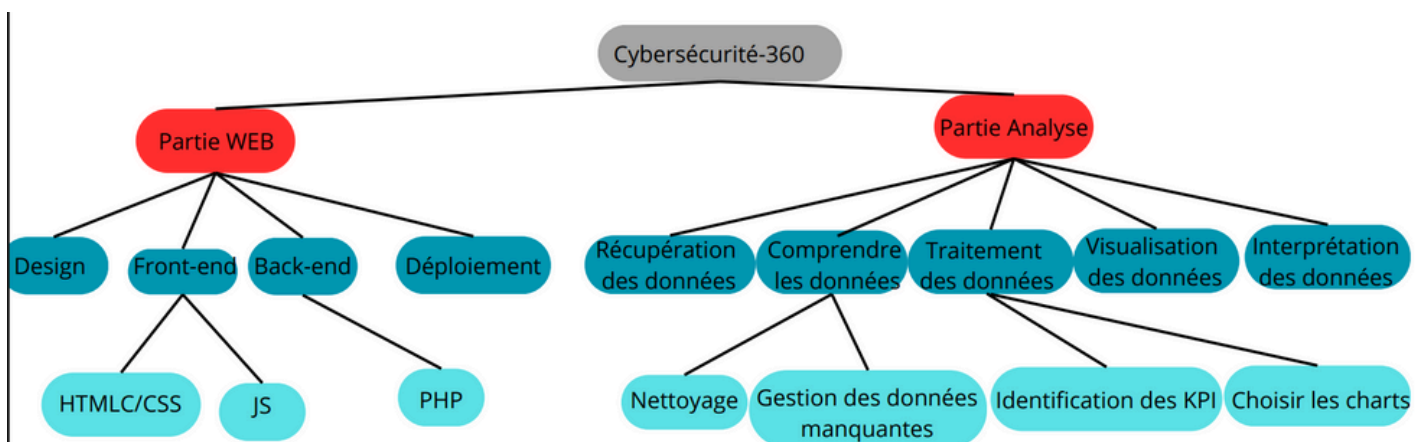


Diagramme de GANT:

Ce diagramme fournit une vue d'ensemble claire des différentes étapes du projet et aide à organiser le travail sur la durée, tout en identifiant les périodes de chevauchement et les dépendances entre les tâches.

[illegible]