ECE ÉCOLE D'INGÉNIEURS ENGINEERING SCHOOL	**Note de cadrage PPE : Prototype d'outil d'émulation d'un adversaire IoT**	**Septembre 2025 / Avril 2026**

Auteurs :

Angel	VELASCO
Grégoire	MARCHAL
Michael	ADDA
Clément	D'ALBERTO
Jérémy	POPULAIRE

Coach Référent:

H. SOUBRA

1. Présentation de l'équipe

Nous sommes une équipe de cinq étudiants répartis sur deux majeures complémentaires qui sont Data & IA, et Cybersécurité. Jérémy Populaire, en majeure Data & IA, aura pour rôle principal d'intégrer des solutions d'intelligence artificielle au sein du prototype (analyse de logs, détection d'anomalies, automatisation de scénarios, etc.). Les quatre autres membres, Michaël Adda, Clément D'Alberto, Grégoire Marchal et Angel Velasco sont quant à eux en majeure Cybersécurité. Ils seront responsables de la conception, de l'implémentation et de la reproduction des scénarios d'attaque (intrusions, dénis de service, manipulation de données, compromission de capteurs, etc.), ainsi que des analyses de vulnérabilité et des protocoles de test.

Cette répartition va permettre d'allier expertise offensive et capacités d'analyse avancée puisque les compétences en cybersécurité serviront à construire et exécuter des scénarios réalistes, tandis que la spécialisation Data & IA apportera des approches d'automatisation et d'analyse pour évaluer et améliorer la résilience des systèmes IoT.

2. Contexte et problématique

2.1 Contexte général (IoT et enjeux de sécurité)

L'Internet des Objets (IoT) s'impose aujourd'hui comme un pilier de la transformation numérique. On estime qu'il y a plus de 20 milliards d'objets connectés en 2025, et ce nombre pourrait dépasser 40 milliards à l'horizon 2034 (source : How many devices are connected to the IoT?). Les entreprises et organisations intègrent de plus en plus l'IoT dans leurs opérations, que ce soit pour l'industrie, la santé, la domotique ou encore dans les transports.

Cependant, cette massification engendre de nouveaux défis. Les appareils IoT disposent souvent de ressources limitées (mémoire, puissance de calcul, autonomie) et sont rarement conçus avec des mécanismes de sécurité robustes. Ils deviennent alors des points d'entrée privilégiés pour les cyber attaquants.

2.2 Problématique centrale du projet

Face à ces menaces croissantes, les chercheurs et les professionnels de la cybersécurité ont besoin d'outils permettant de simuler le comportement d'un adversaire IoT dans un environnement maîtrisé. Ces outils offrent la possibilité de :

- reproduire différents scénarios d'attaque (intrusion, falsification de données, déni de service, etc.),
- évaluer la résilience et la robustesse des systèmes connectés,
- générer des données utiles pour entraîner ou tester des mécanismes de détection,
- anticiper et mitiger de futures menaces.

Problématique centrale : Comment développer un prototype d'outil capable d'émuler de manière réaliste divers scénarios d'attaques IoT, afin de soutenir la recherche et renforcer la sécurité des infrastructures connectées ?

3. Objectifs SMART

L'objectif est de développer un prototype opérationnel d'émulation d'adversaire IoT capable d'exécuter différents scénarios d'attaque (intrusion réseau, déni de service, manipulation de données, compromission de capteurs, et/ou attaque sur protocole IoT) intégrés dans un environnement virtualisé reproductible (**Spécifique**). Concrètement, le projet portera sur la mise en place d'un environnement IoT réel (Raspberry Pi, microcontrôleurs type Arduino et capteurs simples) et d'une application permettant de lancer et d'orchestrer des attaques de niveau réseau, applicatif et, dans certains cas, physiques, tout en conservant un cadre sécurisé et éthique (**Mesurable**). Pour garantir l'atteignabilité, nous utiliserons du matériel abordable et des bibliothèques open-source éprouvées (MQTT, Docker, Nmap, Scapy, etc.), en mobilisant les compétences disponibles dans l'équipe et en privilégiant des outils et composants accessibles (**Atteignable**). Afin de rester réalistes, nous limiterons volontairement la portée aux attaques basiques et contrôlées, adaptées à un contexte académique et encadrées sur les plans éthique et légal (**Réaliste**). Le projet sera structuré en jalons temporels clairs (conception, implémentation, tests et validation) avec des échéances intermédiaires et l'objectif de livrer un prototype fonctionnel et une documentation complète d'ici avril (**Temporellement défini**).

4. Méthodologie et organisation interne

4.1 Approche et méthode de travail

Méthodologie : approche incrémentale (cycle en V simplifié) :

- Recherches et état de l'art,
- Mise en place de l'environnement IoT,
- Développement des scénarios d'attaque,
- Développement de l'application,
- Tests, documentation et rapport final.

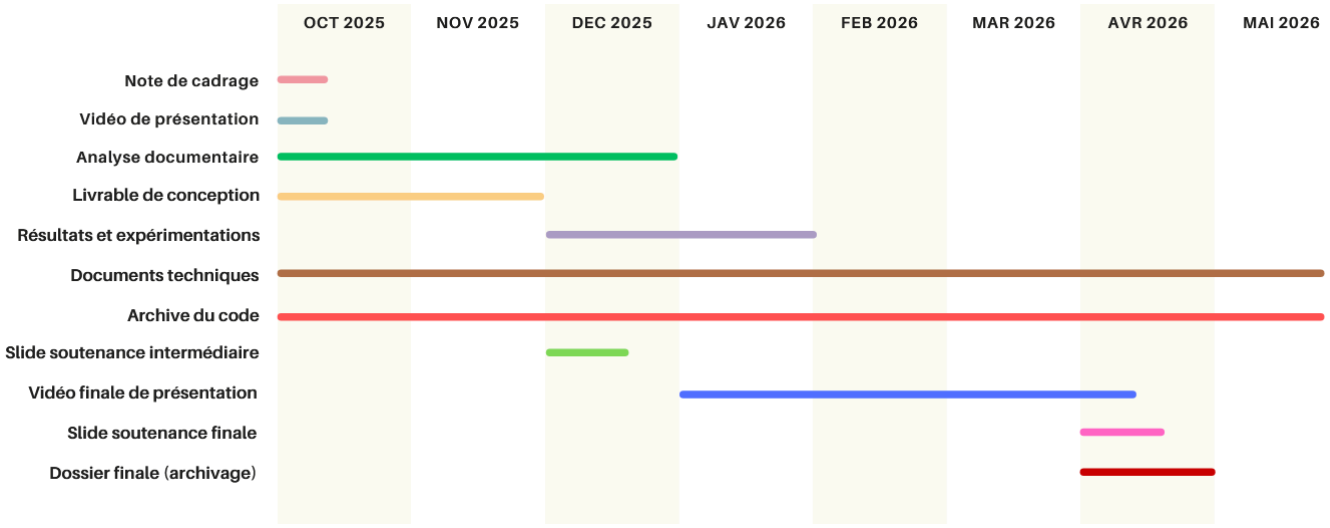
4.2 Outils de gestion et de collaboration

- GitHub pour le code et la documentation,
- Trello / Notion pour la gestion des tâches,
- Google Drive / Slack pour la communication et le partage.
- Discord pour les réunions et partage de documentations

4.3 Organisation des réunions

- 1 réunion hebdomadaire d'équipe,
- 1 point intermédiaire tous les mois avec le référent.

5. Planning prévisionnel (Gantt)



6. Anticipation des risques

6.1 Identification des risques

Risque n°1 – Panne matérielle (Raspberry Pi, capteurs)

Le matériel utilisé (Raspberry Pi, capteurs) peut tomber en panne ou être endommagé lors des manipulations. Ce type d'incident entraînerait un blocage partiel ou total des expérimentations, car notre projet repose sur un petit nombre de composants physiques.

Risque n°2 – Incompatibilités logicielles et dépendances

L'utilisation de différentes bibliothèques, outils (Python, Docker, Node-RED, MQTT) et systèmes d'exploitation peut générer des incompatibilités. Une mise à jour imprévue ou un conflit de versions pourrait compromettre le déploiement ou empêcher le bon fonctionnement de certains modules.

Risque n°3 – Non-respect des règles éthiques ou fuite d'outils exploitables

Comme le projet porte sur l'émulation d'attaques, il existe un risque que les outils développés soient utilisés de manière malveillante ou sortent du cadre académique. Une mauvaise gestion pourrait également mener à l'exécution involontaire de tests sur des réseaux extérieurs, exposant ainsi des tiers.

Risque n°4 – Retard de planning et indisponibilité des membres

Des retards dans l'avancement du projet peuvent survenir en raison de la charge académique parallèle ou de l'indisponibilité ponctuelle de certains membres. Cela peut entraîner une surcharge de travail en fin de projet et compromettre la livraison dans les délais.

6.2 Mesures d'atténuation / plan de contingence

Risque n°1 – Panne matérielle (Raspberry Pi, capteurs)

- Tester l'ensemble du matériel en début de projet pour vérifier son bon fonctionnement.
- Documenter précisément les branchements et montages pour faciliter un remplacement rapide.
- Prévoir quelques composants de rechange si le budget le permet.

Risque n°2 – Incompatibilités logicielles et dépendances

- Figer les versions des bibliothèques et outils utilisés dans des fichiers de configuration.
- Créer des scripts d'installation reproductibles et documentés pour l'ensemble de l'équipe.
- En cas de problème, revenir rapidement à une version antérieure stable.

Risque n°3 – Non-respect des règles éthiques ou fuite d'outils exploitables

- Travailler uniquement dans un environnement réseau isolé et contrôlé.
- Maintenir le code dans un dépôt privé, accompagné d'avertissements clairs sur son usage.
- Rappeler explicitement dans la documentation la finalité pédagogique et éthique du projet.

Risque n°4 – Retard de planning et indisponibilité des membres

- Répartir les tâches de manière claire et équitable dès le début.
- Organiser des réunions hebdomadaires pour suivre l'avancement et réajuster si nécessaire.
- Documenter régulièrement les progrès afin de permettre la reprise par un autre membre.