REPUBLIQUE DU CAMEROUN
Paix-Travail-Patrie

CAISSE DES DEPOTS ET CONSIGNATIONS

REPUBLIC OF CAMEROON
Peace-Work-Fatherland

DEPOSITS AND CONSIGNMENTS FUND

Rapport sur la conception d'une application de sécurité intelligente à la CDEC

Application de sécurité CDEC-Security

Onana Noah Faustin

Né le 02 mai 1997

Superviseur Général

Directeur Général de la CDEC
Monsieur Obam….

Encadreur Professionnel

Directeur du Système D'information à la CDEC
Monsieur Franco Atekwana

Encadreur Adjoint

Le Sous directeur Chargé Direction Qualité Etude Projet
Joel Obam

Encadreur Technique

Cadre à laDirectoin du Système D'information
Madame Yasmine Mairé

Dédicace

A ma petite famille.

A ma mère et à ma grand-mère bien-aimée, source de motivation et de volonté inépuisable.
A mon feu père Noah Abdon Cenang
A mon feu père spirituel Noah Manga Leon

Remerciements

A monsieur Le chargé de Mission Services du Premier Ministère Ekwa Dipanda Charle

A Monsieur le DAG CDEC

Sommaire

1. **Rapport de stage classique** (résumé, introduction, développement, avantages, difficultés/contraintes, conclusion).
2. **Conception technique détaillée** (Scrum, choix technologiques, cahier des fonctionnalités, diagrammes, plannings).

Résumé

Ce stage à la CDEC m’a permis d’identifier une faille dans le système de sécurité actuel et de proposer une solution innovante basée sur l’intelligence artificielle et la reconnaissance visuelle. L’application conçue vise à améliorer la traçabilité des objets personnels et renforcer la sécurité des employés et visiteurs.

Première partie : Contexte et Description du projet

Introduction générale

Dans le cadre de mon stage à la Caisse de Dépôt et Consignation (CDEC), j’ai observé une faille dans le système de sécurité : lors de la perte d’un sac à main, les caméras de surveillance n’ont pas permis de capturer le moment exact de la disparition. La recherche a nécessité de visionner des heures de vidéos sur différents angles, sans résultat probant.
Ce constat met en évidence la nécessité d’un outil plus performant, capable d’optimiser la surveillance et de faciliter la traçabilité des objets personnels des employés et visiteurs.

Développement

Au cours de mon stage à la CDEC, l’analyse du système de sécurité a révélé plusieurs limites qui entravent son efficacité. Ces failles ne sont pas liées à un manque de vigilance du personnel, mais plutôt à des contraintes techniques et organisationnelles. Le développement qui suit présente les principales problématiques observées, chacune accompagnée d’une explication détaillée et d’une conclusion mettant en évidence la nécessité d’une solution innovante.

La CDEC, en tant qu’institution moderne, doit garantir la sécurité des biens de ses collaborateurs et visiteurs. L’observation d’un cas de perte d’objet a révélé les limites des systèmes actuels, notamment l’absence de reconnaissance automatique et la difficulté des recherches manuelles. Ce contexte a motivé la conception d’une application de sécurité intelligente.

Problème identifié

Introduction générale

Les problématiques observées concernent principalement la **reconnaissance des objets par les caméras**, la **lenteur des recherches manuelles** et l'**absence d'un registre centralisé des biens personnels**. Chacune de ces limites sera présentée en détail afin de mieux comprendre leur impact sur le fonctionnement global du système de sécurité.

Problème 1 : Caméras incapables de reconnaître automatiquement les objets

Introduction

Lors de mes observations au sein du service de sécurité de la CDEC, j'ai constaté que les caméras installées remplissent uniquement une fonction de surveillance passive. Elles enregistrent les flux vidéo sans aucune capacité d'analyse ou de reconnaissance automatique des objets présents dans le champ de vision.

Développement

Cette limitation technique rend les vidéos difficilement exploitables pour des recherches ciblées. En cas de perte ou de vol, les agents doivent visionner manuellement des heures d'enregistrements pour tenter d'identifier un moment précis. L'absence de reconnaissance visuelle empêche toute automatisation du processus et mobilise inutilement les ressources humaines. Une caméra intelligente, couplée à un module d'intelligence artificielle, pourrait détecter et classifier les objets visibles (sacs, manteaux, ordinateurs, etc.) en temps réel. Cela permettrait de créer une base de données dynamique des objets présents dans les locaux et d'associer chaque objet à son propriétaire.

Conclusion

Le manque de reconnaissance automatique constitue une faille majeure dans le système actuel. L'intégration d'une IA de vision par ordinateur est donc essentielle pour transformer la surveillance passive en un outil actif de traçabilité et de sécurité.

Problème 2 : Recherche manuelle chronophage

Introduction

La procédure actuelle de recherche d'un objet perdu repose sur une méthode manuelle : les agents doivent parcourir les enregistrements vidéo de plusieurs caméras pour retrouver un indice. Ce processus est long, fastidieux et souvent infructueux.

Développement

Cette approche entraîne une perte de temps considérable et retarde la résolution des incidents. De plus, elle dépend fortement de la vigilance humaine, ce qui augmente le risque d'erreur ou d'omission. Une solution automatisée, basée sur l'analyse vidéo par IA, permettrait de retracer le

parcours d’un objet à partir de ses caractéristiques visuelles. L’algorithme pourrait identifier les séquences pertinentes et générer un rapport de déplacement, réduisant ainsi le temps d’enquête de plusieurs heures à quelques minutes.

Conclusion

La recherche manuelle est incompatible avec les exigences modernes de rapidité et d’efficacité. L’automatisation du processus par IA représente une évolution nécessaire pour optimiser la gestion des incidents et renforcer la réactivité du service de sécurité.

Problème 3 : Absence de base centralisée des biens personnels

Un autre point critique observé concerne l’absence d’un système centralisé permettant de répertorier les biens personnels des employés et visiteurs. Chaque individu gère ses objets de manière indépendante, sans enregistrement formel ni suivi numérique.

Développement

Cette lacune rend impossible toute traçabilité systématique. En cas de perte, il n’existe aucun moyen de vérifier rapidement la propriété ou la description exacte de l’objet concerné. La mise en place d’un répertoire numérique, lié aux profils utilisateurs, permettrait de stocker les informations sur les objets visibles et non visibles (comme les téléphones ou batteries externes). Ce registre servirait de référence pour l’IA lors des opérations de reconnaissance et de recherche automatisée.

L’absence de base centralisée limite la cohérence et la fiabilité du système de sécurité. La création d’un répertoire des biens personnels constitue une étape fondamentale pour garantir la traçabilité, la transparence et la rapidité des interventions.

Solutions proposées

Introduction générale

Face aux limites identifiées dans le système de sécurité de la CDEC, plusieurs pistes de solutions ont été envisagées. L'objectif n'est pas de remettre en cause les pratiques actuelles, mais de les renforcer grâce à des outils modernes et intelligents. Les solutions proposées reposent sur l'intégration de l'intelligence artificielle, la centralisation des données et l'automatisation des recherches. Elles visent à améliorer la traçabilité des objets personnels et à optimiser le travail des agents de sécurité.

Solution 1 : Application web/mobile intégrant IA et reconnaissance visuelle

Introduction

La première solution consiste à développer une application web et mobile capable d'exploiter les flux vidéo des caméras pour identifier automatiquement les objets visibles et les associer aux profils des utilisateurs.

Développement

Cette application, construite sur des technologies modernes comme Next.js et MongoDB, servirait d'interface entre les agents de sécurité et le système d'intelligence artificielle. L'IA analyserait en temps réel les images captées par les caméras, détecterait les objets et les classifierait selon leur type. L'application permettrait aux agents de consulter un tableau de bord centralisé, d'accéder aux alertes et de suivre les déplacements des objets. En parallèle, les utilisateurs (employés et visiteurs) pourraient interagir via une interface mobile pour enregistrer leurs biens et consulter leur état. L'intégration IA ↔ application garantit une surveillance active et une meilleure réactivité.

Cette solution transforme la surveillance passive en un système intelligent et interactif. Elle modernise la sécurité de la CDEC tout en offrant une expérience fluide aux agents et aux utilisateurs.

Solution 2 : Répertoire numérique des biens personnels liés aux profils utilisateurs

Introduction

La deuxième solution vise à créer une base de données centralisée où chaque employé ou visiteur peut enregistrer ses objets personnels, qu'ils soient visibles par les caméras ou non.

Développement

Ce répertoire numérique, hébergé sur MongoDB, serait lié directement aux profils utilisateurs. Les objets visibles (sacs, manteaux, ordinateurs) seraient automatiquement ajoutés par l'IA, tandis que

les objets non visibles (téléphones, batteries externes) seraient enregistrés manuellement par l'utilisateur. Cette centralisation permettrait de disposer d'un registre fiable et complet, facilitant la traçabilité et la vérification en cas de perte. Les agents de sécurité auraient accès à ce répertoire via leur tableau de bord, ce qui renforcerait la transparence et la rapidité des interventions.

La mise en place d'un répertoire numérique constitue une étape essentielle pour garantir la cohérence et la fiabilité du système. Elle offre une base solide sur laquelle l'IA peut s'appuyer pour effectuer ses analyses.

Solution 3 : Recherche automatisée en cas de perte

Introduction

La troisième solution consiste à automatiser le processus de recherche lorsqu'un objet est signalé comme manquant.

Développement

Au lieu de parcourir manuellement des heures de vidéos, l'IA analyserait directement les flux enregistrés pour retracer le parcours de l'objet. Grâce aux caractéristiques visuelles enregistrées dans le répertoire, l'algorithme pourrait identifier les séquences pertinentes et générer un rapport détaillé sur les déplacements de l'objet. Cette automatisation réduit considérablement le temps d'enquête et augmente la précision des résultats. Les agents de sécurité recevraient des alertes en temps réel et pourraient intervenir plus rapidement pour résoudre l'incident.

La recherche automatisée représente un gain de temps et d'efficacité majeur. Elle permet de passer d'une approche manuelle et chronophage à une méthode moderne, rapide et fiable, renforçant ainsi la sécurité globale de la CDEC.

Fonctionnement de la solution

Introduction générale

Le fonctionnement de l'application de sécurité intelligente repose sur une interaction fluide entre les caméras de surveillance, le module d'intelligence artificielle et la base de données centralisée. Chaque étape du processus contribue à assurer une traçabilité complète des objets personnels et à renforcer la réactivité du système en cas de perte ou de vol.

Étape 1 : En entrée —La caméra capture les objets visibles et IA les associe aux profils

Introduction

Lorsqu'un employé ou un visiteur entre dans les locaux de la CDEC, les caméras de surveillance capturent automatiquement les objets visibles.

Développement

Le module d’intelligence artificielle analyse en temps réel les flux vidéo pour identifier les objets présents (sacs, manteaux, ordinateurs, etc.). Ces objets sont ensuite associés au profil de l’utilisateur enregistré dans la base de données. Ce mécanisme permet de créer une correspondance fiable entre les individus et leurs biens, facilitant la traçabilité dès l’entrée dans l’établissement.

Conclusion

Cette étape garantit une première couche de sécurité en liant directement les objets visibles aux profils utilisateurs, réduisant ainsi les risques de confusion ou de perte non détectée.

Étape 2 : En procédure—Enregistrement manuel des objets non visibles

Introduction

Certains objets, comme les téléphones ou batteries externes, ne sont pas détectables par les caméras et nécessitent un enregistrement manuel.

Développement

L’application offre une interface permettant aux utilisateurs d’ajouter ces objets dans leur répertoire personnel. Chaque objet est lié au profil de l’utilisateur et stocké dans la base de données centrale. Cette fonctionnalité assure que même les biens invisibles aux caméras disposent d’une trace numérique, ce qui renforce la cohérence et la complétude du système.

Conclusion

L’enregistrement manuel compense les limites techniques de la reconnaissance visuelle et garantit une traçabilité exhaustive des biens personnels.

Étape 3 : Signalement de perte → traçage automatique par IA

Introduction

Lorsqu’un objet est déclaré manquant, le système déclenche automatiquement une recherche assistée par intelligence artificielle.

Développement

L’IA analyse les vidéos enregistrées pour retracer les déplacements de l’objet signalé. Grâce aux données stockées dans le répertoire numérique, elle peut identifier les séquences pertinentes et générer un rapport détaillé sur le parcours de l’objet. Les agents de sécurité reçoivent des alertes en temps réel et disposent d’outils d’investigation pour intervenir rapidement.

Conclusion

Cette automatisation transforme un processus chronophage en une opération rapide et efficace, renforçant la sécurité et la réactivité de la CDEC.

Avantages attendus

Introduction générale

La mise en place de l'application de sécurité intelligente à la CDEC ne se limite pas à combler les failles identifiées. Elle apporte également une série d'avantages stratégiques qui renforcent l'efficacité opérationnelle, la sécurité des biens et l'image moderne de l'organisation. Ces bénéfices se déclinent en plusieurs dimensions que nous détaillons ci-après.

Avantage 1 : Gain de temps — recherche automatisée

Introduction

L'un des principaux avantages de l'application est la réduction significative du temps consacré aux enquêtes sur les objets perdus ou volés.

Développement

Grâce à l'automatisation, l'IA analyse directement les vidéos et retrace le parcours des objets signalés. Les agents n'ont plus besoin de visionner manuellement des heures d'enregistrements. Cette optimisation libère du temps pour d'autres tâches essentielles et améliore la productivité globale du service de sécurité.

Conclusion

Le gain de temps est un atout majeur qui permet à la CDEC de gérer les incidents plus rapidement et avec une efficacité accrue.

Avantage 2 : Efficacité accrue — traçabilité en temps réel

Introduction

La traçabilité des objets constitue une avancée essentielle pour garantir la sécurité et la transparence.

Développement

L'IA suit en continu les déplacements des objets visibles et enregistre les informations dans la base de données centrale. Les agents disposent ainsi d'un tableau de bord en temps réel, leur permettant de localiser rapidement un objet et de vérifier son statut. Cette traçabilité réduit les risques de perte et facilite les investigations.

Conclusion

La traçabilité en temps réel renforce l'efficacité du système et offre une meilleure visibilité sur la gestion des biens personnels.

Avantage 3 : Sécurité renforcée — meilleure protection des biens

Introduction

La sécurité des biens des employés et visiteurs est au cœur des préoccupations de la CDEC.

Développement

En associant chaque objet à un profil utilisateur et en automatisant la surveillance, l'application réduit considérablement les risques de vol ou de disparition non détectée. Les alertes générées par l'IA permettent une intervention rapide et ciblée, augmentant ainsi le niveau de protection offert par le système.

Conclusion

La sécurité renforcée contribue à instaurer un climat de confiance et à protéger efficacement les biens des individus présents dans les locaux.

Avantage 4 : Innovation — valorisation de la CDEC

Introduction

Au-delà des aspects techniques, l'application représente une opportunité d'innovation pour la CDEC.

Développement

La mise en œuvre d'une solution basée sur l'intelligence artificielle positionne l'organisation comme un acteur moderne et proactif. Elle démontre sa capacité à adopter des technologies avancées pour répondre aux besoins de ses employés et visiteurs. Cette image innovante peut également renforcer la réputation de la CDEC auprès de ses partenaires et du grand public.

Conclusion

L'innovation apportée par cette application valorise la CDEC et confirme son engagement dans la modernisation de ses pratiques de sécurité.

Les plus de la solution proposé...

En plus des bénéfices directs liés à la sécurité et à la traçabilité, le projet d'application de sécurité intelligente génère des avantages indirects mais tout aussi stratégiques. Ces avantages concernent le développement des compétences, l'innovation technologique et l'ouverture vers de nouvelles opportunités pour la CDEC.

Avantage 5 : Développement des compétences et expériences en développement

Introduction

La conception de cette application constitue une opportunité unique pour les stagiaires et les équipes techniques de renforcer leurs compétences.

Développement

Le projet mobilise des technologies modernes telles que Next.js, MongoDB, JWT et l'intégration d'IA. Travailler sur un tel système permet aux développeurs d'acquérir une expérience pratique dans la création d'applications web sécurisées et dans l'implémentation de solutions d'intelligence artificielle. Cette montée en compétences contribue à la professionnalisation des équipes et à la valorisation du stage.

Conclusion

Le projet ne profite pas seulement à la CDEC, mais aussi aux stagiaires et développeurs qui enrichissent leur savoir-faire et leur expérience professionnelle.

Avantage 6 : Naissance et développement d'une IA

Introduction

La mise en place d'un module d'intelligence artificielle est une étape clé dans la modernisation des systèmes de sécurité.

Développement

Ce projet permet de concevoir, entraîner et déployer un réseau de neurones spécialisé dans la reconnaissance d'objets. Au-delà de son application immédiate, cette IA peut évoluer et être adaptée à d'autres besoins, comme la détection de comportements suspects ou la gestion automatisée des flux vidéo. La CDEC devient ainsi un acteur pionnier dans l'utilisation de l'IA pour la sécurité institutionnelle.

Conclusion

La naissance et l'évolution de cette IA représentent un investissement stratégique qui ouvre la voie à de futures innovations dans le domaine de la surveillance intelligente.

Avantage 7 : Solution exportable vers d’autres entreprises gouvernementales et privées

Introduction

L’application conçue pour la CDEC ne se limite pas à un usage interne. Elle possède un potentiel de diffusion vers d’autres organisations.

Développement

Grâce à son architecture modulaire et à ses fonctionnalités universelles (répertoire des biens, reconnaissance visuelle, recherche automatisée), la solution peut être proposée à d’autres institutions gouvernementales ou entreprises privées. Cela positionne la CDEC comme un innovateur capable de partager ses avancées technologiques et de contribuer à la modernisation des pratiques de sécurité dans divers secteurs.

Conclusion

La CDEC pourrait valoriser cette solution en la proposant à d’autres organisations, renforçant ainsi son image de leader en innovation et ouvrant la porte à de nouvelles collaborations.

Avantage 8 : Proposer des formations en développement d’applications web et industrielles

Introduction

La conception de l’application constitue une base solide pour développer des programmes de formation destinés à d’autres institutions.

Développement

En s’appuyant sur l’expérience acquise, la CDEC peut organiser des ateliers ou modules de formation en développement d’applications web (Next.js, MongoDB, Tailwind CSS) et industrielles. Ces formations permettraient de partager les compétences techniques acquises, de renforcer le savoir-faire local et de créer un réseau de développeurs capables de concevoir des solutions adaptées aux besoins des entreprises et administrations.

Conclusion

La CDEC devient ainsi un centre de compétences, valorisant son expertise et contribuant à la montée en puissance technologique d’autres institutions.

Avantage 9 : Formation en machine learning et deep learning

Introduction

Le projet intègre un réseau de neurones pour la reconnaissance visuelle, ce qui ouvre la voie à des formations spécialisées en intelligence artificielle.

Développement

La CDEC peut proposer des programmes de formation en machine learning et deep learning, basés sur des cas pratiques comme la détection d'objets et l'analyse vidéo. Ces formations permettraient aux stagiaires, étudiants et professionnels de se familiariser avec les frameworks modernes (TensorFlow, PyTorch) et d'acquérir une expertise dans la conception et l'entraînement de modèles IA. Cela renforcerait la capacité locale à développer des solutions intelligentes adaptées aux besoins nationaux.

Conclusion

La CDEC se positionne comme un acteur de référence dans la diffusion des connaissances en IA, contribuant à la formation de la prochaine génération de spécialistes.

Limites et précautions

Introduction générale

Bien que l'application de sécurité intelligente apporte de nombreux avantages, sa mise en œuvre doit être accompagnée de certaines précautions. Ces limites ne constituent pas des obstacles insurmontables, mais des points de vigilance à prendre en compte pour garantir un déploiement responsable et efficace.

Limite 1 : Respect de la vie privée

Introduction

L'utilisation d'un système basé sur l'intelligence artificielle et la reconnaissance visuelle soulève des questions sensibles liées à la protection des données personnelles.

Développement

Les caméras capturent en permanence des images des employés et visiteurs, ce qui peut être perçu comme une intrusion si aucune règle claire n'est définie. Il est donc nécessaire d'établir une politique de confidentialité stricte, précisant les conditions d'utilisation des données, leur durée de conservation et les droits des utilisateurs. La transparence et la conformité aux réglementations en vigueur (comme le RGPD ou ses équivalents locaux) sont essentielles pour instaurer la confiance.

Conclusion

Le respect de la vie privée doit être au cœur du projet. Une gouvernance claire des données garantit que l'innovation ne se fait pas au détriment des libertés individuelles.

Limite 2 : Besoin de formation du personnel

Introduction

La mise en place d'une nouvelle application nécessite une adaptation des pratiques des agents de sécurité et des utilisateurs.

Développement

Le personnel doit être formé à l'utilisation du tableau de bord, à l'interprétation des alertes générées par l'IA et à la gestion du répertoire des biens. Sans formation adéquate, le système risque d'être sous-utilisé ou mal exploité. Des sessions de formation régulières permettront de familiariser les agents avec les nouvelles fonctionnalités et d'assurer une transition fluide vers le nouveau modèle de surveillance.

Conclusion

La formation est une condition indispensable pour garantir l’efficacité du système et maximiser les bénéfices de l’innovation.

Deuxième partie : Conception technique

Introduction générale

La deuxième partie de ce rapport est consacrée à la **dimension technique** du projet. Elle décrit la méthodologie adoptée, les choix technologiques effectués, ainsi que les outils et ressources nécessaires à la réalisation de l’application de sécurité intelligente. Cette section ne se limite pas à une simple description des composants techniques : elle expose également la logique de conception, les diagrammes UML, les plannings de développement et l’identité visuelle de l’application. L’objectif est de fournir une vision claire et structurée du processus de création, depuis le prototype non fonctionnel jusqu’au déploiement dans un environnement opérationnel.

Méthodologie Scrum appliquée à la conception technique

Introduction

La méthodologie **Scrum** a été choisie comme cadre de conception pour organiser le développement de l’application de sécurité intelligente. Elle permet de diviser le projet en sprints successifs, chacun dédié à une étape technique précise : définition du cahier technique, conception des fonctionnalités, modélisation UML, planification du développement, identité visuelle, préparation du matériel et conclusion technique. Cette approche garantit une progression régulière et une adaptation continue aux besoins.

Sprint 1 : Cahier technique et technologies utilisées

Introduction

Le premier sprint de la méthodologie Scrum est consacré à la définition du **cahier technique**. Cette étape est essentielle car elle fixe les bases technologiques sur lesquelles repose l’ensemble du projet. Le choix des langages, frameworks et outils doit être cohérent avec les objectifs de performance, de sécurité et de scalabilité de l’application.

Développement

Le projet repose sur un ensemble de technologies modernes, sélectionnées pour leur efficacité et leur compatibilité avec les besoins identifiés :

- **JavaScript** Langage principal utilisé pour le développement web, garantissant flexibilité et compatibilité multiplateforme.
- **Next.js** Framework React optimisé pour la création d'applications web modulaires, avec rendu côté serveur (SSR) et génération statique (SSG). Il facilite la structuration des modules (Tontine, Entreprise, Marché).
- **MongoDB** Base de données NoSQL choisie pour sa capacité à gérer des données non structurées et évolutives, idéale pour stocker les profils utilisateurs et les objets associés.
- **JWT** Utilisé pour l'authentification sécurisée des utilisateurs, garantissant l'intégrité des sessions.
- **bcrypt** Outil de hachage des mots de passe, renforçant la sécurité des données sensibles.
- **Cookies** Employés pour la gestion des sessions et la persistance des connexions utilisateurs.

Chaque technologie est intégrée dans une architecture modulaire, permettant une évolution progressive du projet. Ce sprint se conclut par la validation du cahier technique, qui servira de référence pour les sprints suivants.

Conclusion

Le cahier technique constitue la fondation du projet. Les technologies retenues — JavaScript, Next.js, MongoDB, JWT, bcrypt et cookies — offrent un équilibre entre performance, sécurité et évolutivité. Ce premier sprint garantit que l'application repose sur des outils fiables et modernes, prêts à soutenir les fonctionnalités avancées prévues dans les étapes suivantes.

Sprint 2 : Cahier des fonctionnalités

Introduction

Après avoir défini le cahier technique et les technologies utilisées, le deuxième sprint est consacré à la rédaction du **cahier des fonctionnalités**. Cette étape consiste à identifier et décrire les principales fonctions que l'application doit offrir, afin de répondre aux besoins de traçabilité, de sécurité et d'efficacité identifiés dans la première partie du rapport.

Développement

Les fonctionnalités retenues sont organisées autour de trois axes : **gestion des objets**, **sécurité et traçabilité**, et **interfaces utilisateurs**.

Gestion des objets

- Enregistrement automatique des objets visibles par les caméras.
- Enregistrement manuel des objets non visibles (téléphones, batteries externes).
- Association des objets aux profils utilisateurs.
- Mise à jour et suppression des objets dans le répertoire numérique.

Sécurité et traçabilité

- Signalement de perte par l’utilisateur.
- Recherche automatisée par IA pour retracer le parcours de l’objet.
- Génération de rapports détaillés sur les déplacements des objets.
- Alertes en temps réel pour les agents de sécurité.

Interfaces utilisateurs

- Tableau de bord pour les agents (visualisation des objets, alertes, rapports).
- Application mobile pour les employés et visiteurs (enregistrement des biens, signalement de perte, suivi).
- Interface web pour la gestion centralisée des données.
- Authentification sécurisée via JWT et gestion des sessions par cookies.

Chaque fonctionnalité est conçue pour être modulaire, permettant une évolution progressive du système. Ce sprint se conclut par la validation du cahier des fonctionnalités, qui servira de base aux diagrammes UML et au planning de développement.

La plateforme contiendra une hiérarchie structurel de profils liés au objets. Les différents profiles sont.

SuperAdmin

Le SuperAdmin dispose de droits étendus pour gérer l’ensemble du système :

- S’authentifier et accéder au tableau de bord central.
- Consulter la liste des utilisateurs et nommer des administrateurs.
- Modifier, ajouter, supprimer et actualiser les informations de tous les utilisateurs.
- Consulter et gérer la liste des objets (ajout, suppression, mise à jour).
- Notifier les utilisateurs en cas d’alerte.
- Démarrer une recherche automatique par IA.
- Suivre les déplacements en temps réel.
- Détecter les objets dangereux, illégaux ou interdits.

Fonctionnalité clé : le SuperAdmin est le garant de la sécurité globale et du bon fonctionnement du système.

Personnels / Stagiaires

Les personnels et stagiaires disposent de fonctionnalités centrées sur leurs propres données :

- S’authentifier pour accéder à leur espace personnel.
- Modifier, ajouter, supprimer et actualiser leurs informations personnelles.
- Enregistrer et gérer leurs objets personnels.
- Suivre leurs déplacements en temps réel.
- Recevoir des alertes en cas de détection d’objets dangereux ou interdits.

Fonctionnalité clé : chaque utilisateur gère son propre répertoire numérique, garantissant une traçabilité individuelle.

Visiteurs

Les visiteurs bénéficient d’une identification automatisée par IA :

- Identification automatique via les caméras à l’entrée.
- Suivi des déplacements en temps réel.
- Détection d’objets dangereux, illégaux ou interdits.

Fonctionnalité clé : la reconnaissance visuelle permet une gestion simplifiée et sécurisée des visiteurs.

Conclusion

Le cahier des fonctionnalités définit clairement les services offerts par l’application en fonction des profils utilisateurs. Le **SuperAdmin** assure la gestion globale, les **personnels/stagiaires** gèrent leurs propres informations et objets, tandis que les **visiteurs** sont identifiés automatiquement par IA. Cette organisation garantit une traçabilité exhaustive et une sécurité renforcée, tout en restant évolutive et adaptable.

Liste des pages de l’application CDEC Security

La conception des interfaces visuelles de **CDEC Security** repose sur une organisation structurée des pages, chacune correspondant à un **profil utilisateur** et à ses **fonctionnalités spécifiques**. Cette approche garantit :

- Une **navigation intuitive** adaptée aux rôles (SuperAdmin, Personnel/Stagiaire, Visiteur).
- Une **séparation claire des responsabilités** et des droits d’accès.
- Une **cohérence visuelle et fonctionnelle** entre les modules (authentification, gestion, suivi, détection).

- Une **base solide pour le développement HTML/CSS/JavaScript/ReactJs/Nextjs/tailwindcss**, en permettant de progresser pas à pas dans la construction des interfaces.

La liste des pages sert donc de **plan directeur** pour la présentation de l'application : elle définit les écrans nécessaires, leur contenu et leur rôle dans l'expérience utilisateur. Chaque page est pensée comme une **porte d'entrée vers une fonctionnalité précise**, ce qui facilite la mise en œuvre technique et la démonstration du projet.

Pages générales

- **Page d'accueil** : introduction, logo, accès aux profils.
- **Page d'enregistrement** : formulaire pour créer un compte (nom, email, mot de passe, rôle).
- **Page de connexion** : authentification avec email + mot de passe.
- **Tableau de bord général** : redirection vers les fonctionnalités selon le rôle (SuperAdmin, Personnel, Visiteur).

🔹 SuperAdmin

- **Gestion des utilisateurs** : liste, ajout, modification, suppression.
- **Gestion des objets** : liste, ajout, modification, suppression.
- **Notifications** : envoi de messages aux utilisateurs.
- **Recherche automatique** : interface IA pour lancer une détection.
- **Suivi en temps réel** : carte ou tableau des déplacements.
- **Détection objets dangereux** : alertes automatiques.

🔹 Visiteur

- **Identification IA** : reconnaissance automatique par caméra.
- **Suivi en temps réel** : affichage des déplacements.
- **Détection objets dangereux** : alertes automatiques.

🔹 Pages complémentaires

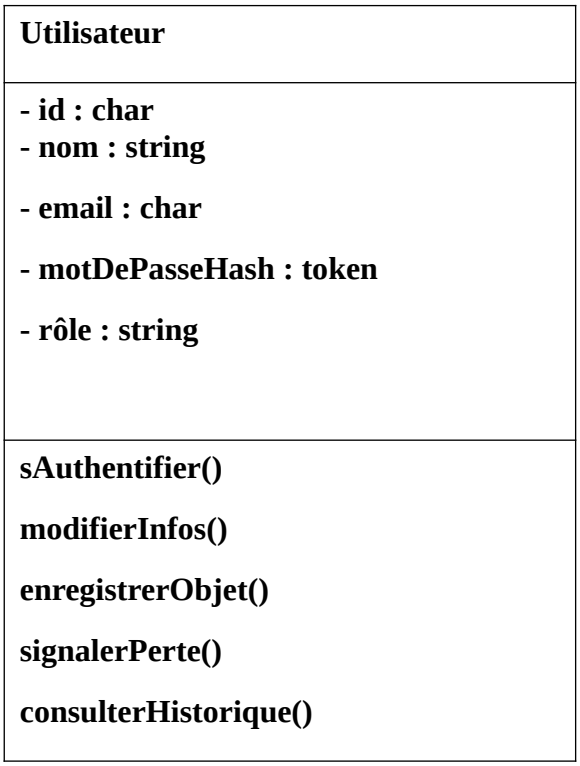
- **Historique** : mouvements des objets, traçabilité.
- **Signalements** : gestion des pertes et rapports IA.
- **Paramètres** : configuration du compte et préférences.

Sprint 3 : Diagrammes UML

Introduction

Les diagrammes UML permettent de représenter la structure et les interactions du système. Ils offrent une vision claire des classes, des relations et des cas d'utilisation. Dans ce projet, deux diagrammes principaux sont utilisés : le **diagramme de classes** et le **diagramme de cas d'utilisation**.

Diagramme de classes




```
+-------------------+
|    Utilisateur    |
+-------------------+
| - id              |
| - nom             |
| - email           |
| - motDePasseHash  |
| - rôle            |
+-------------------+
| + sAuthentifier() |
| + modifierInfos() |
| + enregistrerObjet() |
| + signalerPerte()    |
| + consulterHistorique() |
+-------------------+

      ^
      | Héritage
      |
+-------------------+       +-------------------+       +-------------------+
|   SuperAdmin      |       |   Personnel       |       |   Visiteur        |
+-------------------+       +-------------------+       +-------------------+
| + nommerAdmin()   |       | + gererObjetsPerso() |    | + identificationIA() |
```

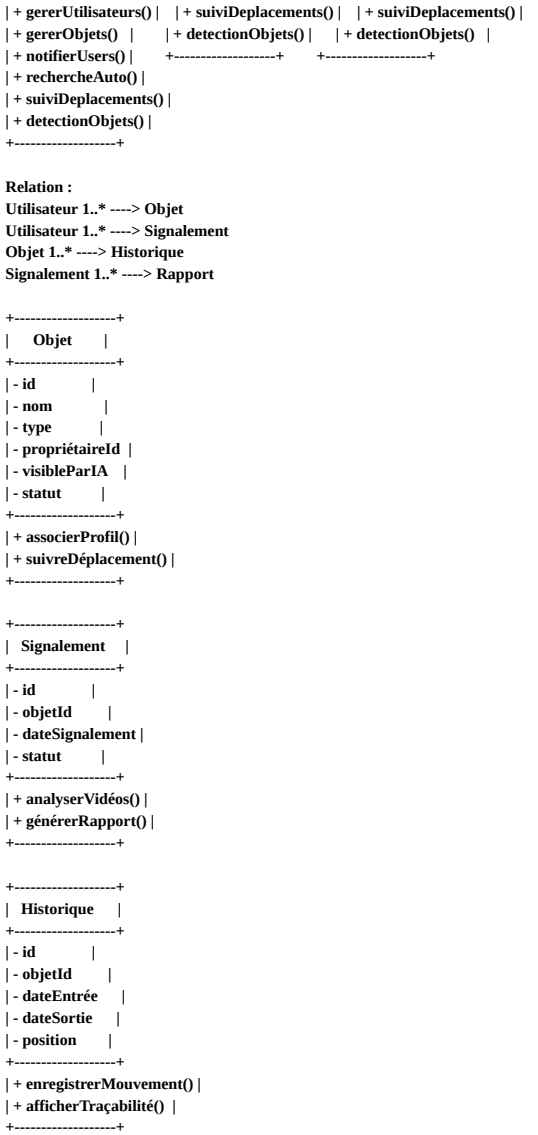

| + gererUtilisateurs() | | + suiviDeplacements() | | + suiviDeplacements() |
| + gererObjets() | | + detectionObjets() | | + detectionObjets() |
| + notifierUsers() | +----------+ +----------+
| + rechercheAuto() |
| + suiviDeplacements() |
| + detectionObjets() |
+----------+
Relation :
Utilisateur 1..* ----> Objet
Utilisateur 1..* ----> Signalement
Objet 1..* ----> Historique
Signalement 1..* ----> Rapport
+----------+
| Objet |
+----------+
| - id |
| - nom |
| - type |
| - propriétaireId |
| - visibleParIA |
| - statut |
+----------+
| + associerProfil() |
| + suivreDéplacement() |
+----------+
+----------+
| Signalement |
+----------+
| - id |
| - objetId |
| - dateSignalement |
| - statut |
+----------+
| + analyserVidéos() |
| + générerRapport() |
+----------+
+----------+
| Historique |
+----------+
| - id |
| - objetId |
| - dateEntrée |
| - dateSortie |
| - position |
+----------+
| + enregistrerMouvement() |
| + afficherTraçabilité() |
+----------+

Diagramme de cas d’utilisation (format texte brut)

Acteur : Agent de sécurité

Cas d’utilisation :

1. Enregistrer un objet
2. Associer objet ↔ profil utilisateur
3. Signaler une perte
4. Rechercher un objet
5. Consulter tableau de bord
6. Analyser vidéos IA
7. Générer rapport de traçabilité

Acteur : Employé / Visiteur

Cas d’utilisation :

1. Ajouter ses objets personnels
2. Signaler une perte
3. Consulter l’état de ses biens

Tableu des foctionalitées et Profils utlisateurs

Utilité du tableau des fonctionnalités

Le **tableau des fonctionnalités** est un élément fondamental dans le développement logiciel car :

- **Accord de base** : il représente un contrat implicite entre les parties prenantes (client, développeurs, encadrants). Il fixe les attentes et définit ce que le programmeur doit livrer.
- **Exhaustivité fonctionnelle** : il permet de lister toutes les fonctionnalités prévues, en évitant les oublis et en clarifiant les responsabilités par profil utilisateur.
- **Évolutivité** : les fonctionnalités d'une application sont appelées à évoluer. Ce tableau sert de base initiale, mais peut être enrichi au fil des besoins.
- **Checklist de codage** : il constitue une liste de contrôle pour le développeur, permettant de suivre l'avancement du projet et d'évaluer le niveau de progression de la plateforme.
- **Outil de suivi : il facilite la gestion de projet en reliant les fonctionnalités aux modules développés et aux tests réalisés.**

Tableau des fonctionnalités par profil utilisateur

Profil	Fonctionnalités
SuperAdmin	- S'authentifier - Consulter la liste des utilisateurs - Nommer les administrateurs - Modifier, ajouter, supprimer, actualiser les informations de tous les utilisateurs - Consulter la liste d'objets - Modifier, ajouter, supprimer, actualiser les objets de tous les utilisateurs - Notifier les utilisateurs - Démarrer une recherche automatique - Suivi des déplacements en temps réel - Détection d'objets dangereux, illégaux ou interdits
Personnels / Stagiaires	- S'authentifier - Modifier, ajouter, supprimer, actualiser les informations personnelles - Modifier, ajouter, supprimer, actualiser les objets personnels - Suivi des déplacements en temps réel - Détection d'objets dangereux, illégaux ou interdits

Visiteurs	- Identification automatique par IA avec les caméras - Suivi des déplacements en temps réel - Détection d’objets dangereux, illégaux ou interdits

Conclusion

Ce tableau est à la fois un **document de référence** et un **outil de pilotage**. Il fixe les attentes, sert de checklist pour le codage et permet de mesurer l’avancement du projet. Sa valeur réside dans sa clarté et son rôle de base commune entre les développeurs et les responsables du projet.

Sprint 4 : Planning de développement (liste des tâches par modules)

🔹 Application Web

- **Semaine 1-2 : Conception UI/UX Next.js + Tailwind**
    - Installation environnement de travail (2 jours)
    - Conception maquettes UI/UX (3 jours)
    - Configuration Next.js + Tailwind CSS (2 jours)
- **Semaine 3-4 : Développement API Node.js + MongoDB**
    - Mise en place base MongoDB (2 jours)
    - Développement API REST sécurisée (4 jours)
    - Connexion API ↔ Base de données (2 jours)
- **Semaine 5 : Authentification JWT + Cookies + Bcrypt**
    - Implémentation JWT (2 jours)
    - Gestion des sessions avec cookies (1 jour)
    - Hachage mots de passe avec bcrypt (1 jour)
- **Semaine 6 : Tests unitaires et intégration**
    - Tests unitaires (3 jours)
    - Tests d'intégration (4 jours)

Réseau de Neurones IA

- **Semaine 1-2 : Collecte et annotation des images**
    - Collecte dataset interne + externe (5 jours)
    - Annotation manuelle des images (5 jours)
- **Semaine 3-4 : Entraînement du modèle de reconnaissance**
    - Prétraitement des données (3 jours)
    - Conception CNN (5 jours)
    - Entraînement sur GPU (7 jours)
- **Semaine 5 : Validation et ajustement des performances**
    - Tests de précision et rappel (3 jours)
    - Ajustement hyperparamètres (3 jours)
- **Semaine 6 : Export du modèle pour intégration**
    - Conversion modèle (ONNX/TensorFlow Lite) (2 jours)

- Documentation technique IA (2 jours)

Intégration Web + IA

- **Semaine 1 : Connexion API IA ↔ Backend**
  - Développement endpoints IA (2 jours)
  - Liaison IA ↔ MongoDB (2 jours)
- **Semaine 2 : Synchronisation des données objets**
  - Synchronisation objets détectés ↔ base (3 jours)
  - Gestion signalements automatiques (2 jours)
- **Semaine 3 : Tests de traçabilité et alertes automatiques**
  - Tests traçabilité objets (3 jours)
  - Tests alertes en temps réel (2 jours)

Déploiement réseau local CDEC

- **Semaine 1 : Installation serveur et base MongoDB**
  - Déploiement Docker + Nginx (4 jours)
  - Configuration MongoDB serveur (2 jours)
- **Semaine 2 : Configuration des caméras et du flux vidéo**
  - Installation caméras IP (3 jours)
  - Configuration flux RTSP/ONVIF (2 jours)
- **Semaine 3 : Tests de charge et sécurité**
  - Tests de charge réseau (3 jours)
  - Tests sécurité (2 jours)
- **Semaine 4 : Formation du personnel**
  - Formation agents de sécurité (2 jours)
  - Formation administrateurs (2 jours)

Tableau de planification PERT des tâches de développement

Tâche	Durée (jours)	Prédécesseurs
Application Web		
Installation environnement de travail	2	-
Conception UI/UX (Next.js + Tailwind)	3	Installation environnement
Configuration Next.js + Tailwind CSS	2	Conception UI/UX
Mise en place base MongoDB	2	Installation environnement
Développement API Node.js	4	Base MongoDB
Connexion API ↔ Base de données	2	Développement API
Authentification JWT	2	API Node.js
Gestion sessions avec cookies	1	Authentification JWT
Hachage mots de passe (bcrypt)	1	Authentification JWT
Tests unitaires	3	Authentification + API
Tests d'intégration	4	Tests unitaires
Réseau de Neurones IA		
Collecte dataset images	5	-
Annotation manuelle des images	5	Collecte dataset
Prétraitement des données	3	Annotation images
Conception CNN	5	Prétraitement données
Entraînement sur GPU	7	Conception CNN
Validation performances	3	Entraînement
Ajustement hyperparamètres	3	Validation
Export modèle IA (ONNX/TFLite)	2	Ajustement hyperparamètres
Documentation technique IA	2	Export modèle
Intégration Web + IA		
Développement endpoints IA	2	Export modèle IA + API Node.js
Liaison IA ↔ MongoDB	2	Endpoints IA

Tâche	Durée (jours)	Prédécesseurs
Synchronisation objets détectés ↔ base	3	Liaison IA ↔ MongoDB
Gestion signalements automatiques	2	Synchronisation objets
Tests traçabilité objets	3	Signalements automatiques
Tests alertes en temps réel	2	Tests traçabilité
Déploiement réseau local CDEC		
Déploiement Docker + Nginx	4	Tests intégration
Configuration MongoDB serveur	2	Docker + Nginx
Installation caméras IP	3	MongoDB serveur
Configuration flux RTSP/ONVIF	2	Caméras IP
Tests de charge réseau	3	Flux vidéo
Tests sécurité	2	Tests de charge
Formation agents de sécurité	2	Tests sécurité
Formation administrateurs	2	Formation agents

Commentaires explicatifs

- Les **modules Application Web et IA** peuvent être développés en parallèle, mais l'**Intégration Web+IA** dépend de la finalisation des deux.
- Le **déploiement réseau local CDEC** ne peut commencer qu'après les tests d'intégration réussis.
- Les **formations** clôturent le projet, assurant la prise en main par les utilisateurs finaux.

Chemin critique PERT (séquence des tâches essentielles)

- **Installation environnement de travail** → 2 jours
- **Conception UI/UX (Next.js + Tailwind)** → +3 jours (cumul : 5)
- **Configuration Next.js + Tailwind CSS** → +2 jours (cumul : 7)
- **Mise en place base MongoDB** → +2 jours (cumul : 9)
- **Développement API Node.js** → +4 jours (cumul : 13)
- **Connexion API ↔ Base de données** → +2 jours (cumul : 15)
- **Auth. JWT + Cookies + Bcrypt** → +4 jours (cumul : 19)
- **Tests unitaires** → +3 jours (cumul : 22)
- **Tests d'intégration** → +4 jours (cumul : 26)
- **Collecte dataset images** → +5 jours (cumul : 31)
- **Annotation manuelle des images** → +5 jours (cumul : 36)
- **Prétraitement des données IA** → +3 jours (cumul : 39)
- **Conception CNN** → +5 jours (cumul : 44)
- **Entraînement sur GPU** → +7 jours (cumul : 51)
- **Validation performances IA** → +3 jours (cumul : 54)
- **Ajustement hyperparamètres** → +3 jours (cumul : 57)
- **Export modèle IA (ONNX/TFLite)** → +2 jours (cumul : 59)
- **Développement endpoints IA** → +2 jours (cumul : 61)
- **Liaison IA ↔ MongoDB** → +2 jours (cumul : 63)
- **Synchronisation objets détectés ↔ base** → +3 jours (cumul : 66)
- **Gestion signalements automatiques** → +2 jours (cumul : 68)
- **Tests traçabilité objets** → +3 jours (cumul : 71)
- **Tests alertes en temps réel** → +2 jours (cumul : 73)
- **Déploiement Docker + Nginx** → +4 jours (cumul : 77)
- **Configuration MongoDB serveur** → +2 jours (cumul : 79)
- **Installation caméras IP** → +3 jours (cumul : 82)
- **Configuration flux RTSP/ONVIF** → +2 jours (cumul : 84)
- **Tests de charge réseau** → +3 jours (cumul : 87)
- **Tests sécurité** → +2 jours (cumul : 89)
- **Formation agents de sécurité** → +2 jours (cumul : 91)

- **Formation administrateurs** → +2 jours (cumul : 93)

Durée totale du projet sur le chemin critique : 93 jours

Commentaires explicatifs

- Le chemin critique relie les tâches **Application Web** et **IA**, car l'intégration dépend de la finalisation des deux.
- Les tâches parallèles (comme identité visuelle ou documentation IA) ne rallongent pas la durée totale car elles ne sont pas sur le chemin critique.
- La durée totale du projet est estimée à **93 jours**, soit environ **19 semaines** (près de 5 mois).
- Toute modification ou retard sur une tâche du chemin critique rallonge directement la durée globale du projet.

Sprint 5 : Identité visuelle

Objectif

Définir l'image de l'application en cohérence avec l'identité de la CDEC, tout en intégrant des éléments visuels qui évoquent la **sécurité, la confiance et la traçabilité**.

Éléments de la charte graphique

Logo

- Inspiré du logo de la CDEC pour assurer une continuité institutionnelle.
- Intégration de formes géométriques simples (cercle, bouclier, cadenas stylisé) pour symboliser la **protection et la sécurité**.
- Utilisation de lignes épurées pour refléter la modernité et la fiabilité.



Palette de couleurs

- **Couleurs du logo CDEC** : Rouge (autorité, vigilance), Noir (rigueur, sérieux), Blanc (neutralité, transparence).
- **Couleurs complémentaires pour l'application** :
    - Bleu foncé → confiance et stabilité.
    - Vert → sécurité et validation (signal positif).
- Rapport visuel : le rouge/noir/blanc reste dominant pour rappeler l'identité CDEC, tandis que le bleu/vert est utilisé en accent pour renforcer la notion de sécurité et traçabilité.

Interfaces visuelles

- Tableaux et dashboards avec contrastes forts (fond sombre + accents colorés).
- Icônes simples et explicites (cadenas, œil, alerte, check).
- Navigation claire avec hiérarchie visuelle (rouge pour alertes, vert pour validation, bleu pour informations).

Description Des Interfaces

Description détaillée : Page de Connexion (Login)

Introduction

La page de connexion est la **porte d'entrée** de l'application **CDEC Security**. Elle est utilisée par tous les profils (SuperAdmin, Personnel/Stagiaire, Visiteur) pour accéder au système. Son rôle est de garantir que seuls les utilisateurs autorisés puissent entrer

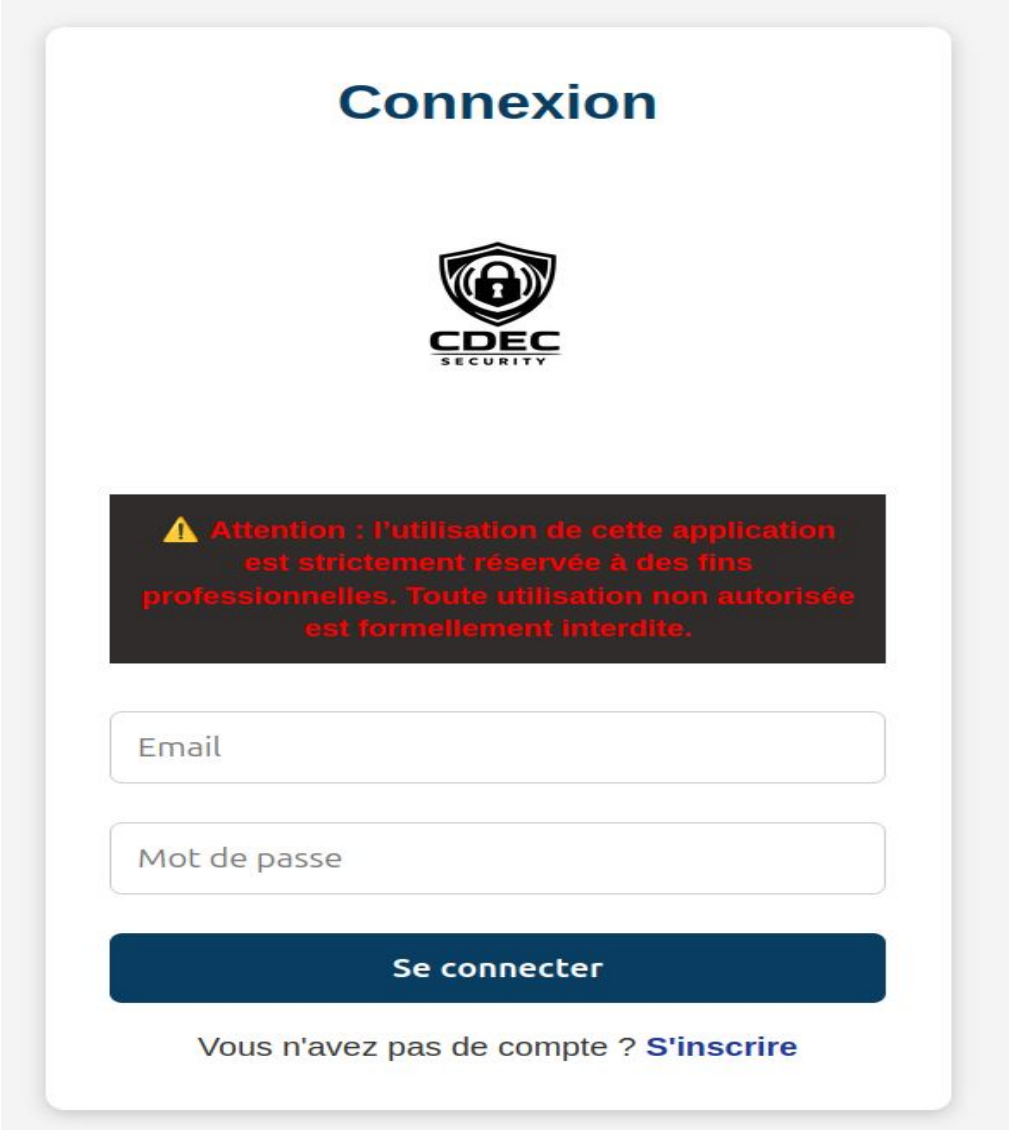
Développement

- **Rôle de l'utilisateur** : la personne qui utilise cette interface est un membre du système (administrateur, personnel ou visiteur). Elle doit s'authentifier pour accéder à ses droits spécifiques.
- **Droits et responsabilités** : l'utilisateur obtient un accès limité ou étendu selon son rôle. Le SuperAdmin peut gérer tout le système, tandis que le personnel ne gère que ses données personnelles et objets.
- **Utilité de la structure** : l'ergonomie simple (email + mot de passe) réduit les erreurs et facilite l'accès. Le message d'avertissement rappelle la dimension réglementaire et sécuritaire.
- **Relation avec la base de données** : lors de la connexion, les informations saisies sont vérifiées dans la table **Users** (email, mot de passe hashé, rôle). Cela garantit l'intégrité et la sécurité des données.
- **Relation avec l'utilisateur de l'application** : cette étape établit la confiance : l'utilisateur sait que ses données sont protégées et que l'accès est contrôlé.
- **Niveau hiérarchique** : la connexion est universelle, mais elle détermine ensuite le niveau hiérarchique (SuperAdmin, Personnel, Visiteur).
- **Avantages dans le réseau** : cette architecture permet un **contrôle centralisé des accès**, réduit les risques d'intrusion et assure une traçabilité des connexions.

Conclusion

La page de connexion est un **point stratégique** : elle filtre les utilisateurs, attribue les droits selon leur rôle et protège l’application contre les accès non autorisés. Elle incarne la première barrière de sécurité dans le réseau CDEC Security.

Image de L’interfaces.



Description de l’interface : Page de création de compte CDEC Security

Introduction

Cette interface illustre la **page de création de compte** de l’application **CDEC Security**. Elle s’inscrit dans la continuité de la logique sécuritaire et professionnelle du projet, en mettant en avant un design sobre et fonctionnel. L’objectif est de permettre aux utilisateurs autorisés de s’inscrire tout en rappelant les règles strictes d’utilisation.

Description détaillée : Page d’Enregistrement (Register)

Introduction

La page d’enregistrement permet à un nouvel utilisateur de **créer un compte** dans l’application. Elle est essentielle pour intégrer de nouveaux membres tout en respectant les règles de sécurité.

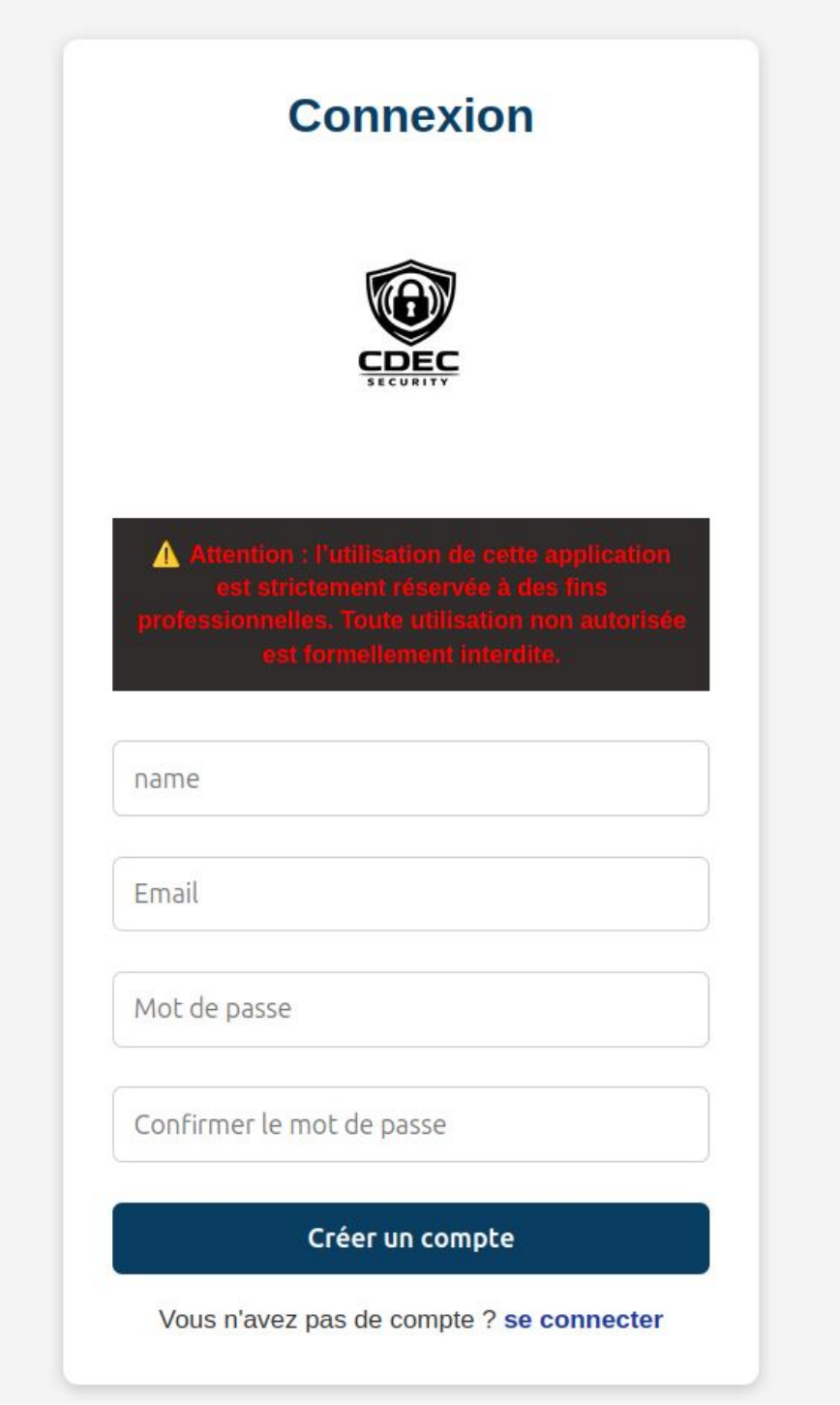
Développement

- **Rôle de l’utilisateur** : la personne qui utilise cette interface est un nouvel arrivant (stagiaire, personnel ou futur administrateur).
- **Droits et responsabilités** : après inscription, l’utilisateur obtient un rôle défini (stagiaire ou personnel). Le SuperAdmin peut ensuite promouvoir certains comptes en administrateurs.
- **Utilité de la structure** : le formulaire clair (nom, email, mot de passe, rôle) garantit une saisie simple et une gestion cohérente des profils.
- **Relation avec la base de données** : les informations sont enregistrées dans la table **Users**, avec un identifiant unique généré automatiquement. Les mots de passe sont stockés de manière sécurisée (hashés).
- **Relation avec l’utilisateur de l’application** : l’enregistrement donne à l’utilisateur une identité numérique dans le système, lui permettant d’interagir avec les autres modules.
- **Niveau hiérarchique** : l’inscription place l’utilisateur au niveau le plus bas (stagiaire ou personnel). Seul le SuperAdmin peut modifier ce statut.
- **Avantages dans le réseau** : cette architecture assure une **scalabilité** : de nouveaux utilisateurs peuvent être ajoutés facilement, tout en maintenant une hiérarchie claire et une sécurité renforcée.

Conclusion

La page d’enregistrement est la **porte d’intégration** des nouveaux utilisateurs. Elle structure la base de données, définit les rôles et garantit que chaque membre est identifié et authentifié. Elle contribue à la robustesse et à la sécurité du réseau CDEC Security.

Image de l’interface



Description détaillée : Tableau de bord SuperAdmin

Introduction

Le **Tableau de bord SuperAdmin** est l'interface centrale de l'application **CDEC Security**. Il est conçu pour l'utilisateur occupant le rôle le plus élevé dans la hiérarchie : le **Super Administrateur**. Cette page concentre toutes les fonctionnalités critiques de gestion et de supervision, constituant un véritable **centre de contrôle**.

Développement

- **Rôle de la personne qui utilise cette interface** : Le SuperAdmin est le **responsable global du système**. Il supervise la sécurité, gère les utilisateurs et les objets, envoie des notifications, déclenche des recherches IA, suit les déplacements en temps réel et reçoit les alertes de détection. Son rôle est stratégique : il assure la **cohérence et la sécurité** de l'ensemble du réseau.
- **Droits et responsabilités** : Le SuperAdmin possède les **droits les plus étendus** :
    - Créer, modifier ou supprimer des utilisateurs.
    - Administrer les objets enregistrés.
    - Envoyer des notifications à tous les profils.
    - Lancer des détections automatiques par IA.
    - Accéder aux données de suivi en temps réel.
    - Recevoir et traiter les alertes d'objets dangereux. Ces droits impliquent une **responsabilité élevée** : garantir la sécurité et la conformité du système.

Utilité de la structure et de l'ergonomie : L'interface est organisée en **sidebar** et **cards**. La sidebar regroupe les menus essentiels, tandis que les cards présentent chaque fonctionnalité avec un bouton d'accès rapide. Cette ergonomie permet une **navigation intuitive**, une **clarté visuelle** et une **réduction des erreurs**. Le SuperAdmin peut ainsi agir rapidement sans se perdre dans une interface complexe.

Relation avec la base de données : Chaque action du SuperAdmin est directement reliée à la base de données :

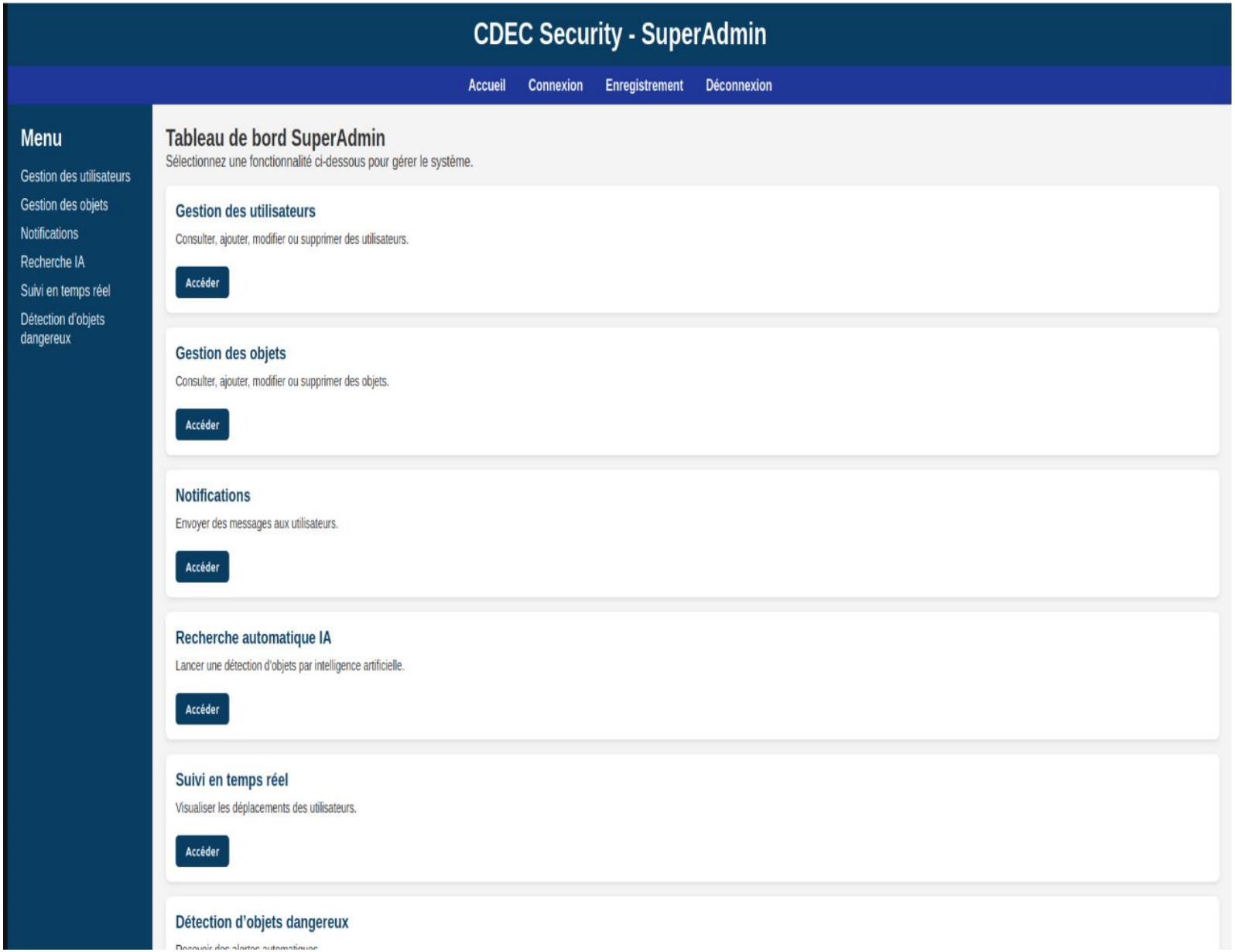
- La gestion des utilisateurs modifie la table **Users**.
- La gestion des objets agit sur la table **Objects**.
- Les notifications sont enregistrées dans la table **Messages**.
- Le suivi en temps réel exploite la table **Tracking**.
- La détection IA alimente la table **Alerts**. Cette relation garantit une **traçabilité complète** et une **cohérence des données**.

- **Relation avec l’utilisateur de l’application** : Le SuperAdmin est en interaction indirecte avec tous les autres utilisateurs. Ses décisions (ajout, suppression, notifications) influencent directement leur expérience. L’interface lui permet de **communiquer, contrôler et sécuriser** l’ensemble du système.
- **Niveau hiérarchique** : Le SuperAdmin occupe le **niveau le plus élevé** dans la hiérarchie. Il est au-dessus des personnels et des visiteurs. Son tableau de bord reflète cette position en lui donnant accès à toutes les fonctionnalités, contrairement aux autres profils qui disposent d’interfaces limitées.
- **Avantages de cette architecture dans le réseau** :
- **Centralisation** : toutes les actions passent par un point unique.
- **Sécurité renforcée** : les droits sont strictement hiérarchisés.
- **Traçabilité** : chaque action est enregistrée dans la base.
- **Efficacité** : l’ergonomie permet une gestion rapide et claire.
- **Scalabilité** : le SuperAdmin peut gérer un grand nombre d’utilisateurs et d’objets sans perte de performance.

Conclusion

Le **Tableau de bord SuperAdmin** est une **interface stratégique** qui incarne le rôle central de l’administrateur dans l’application **CDEC Security**. Il relie directement l’utilisateur à la base de données, définit son autorité hiérarchique et assure une gestion sécurisée et efficace du réseau. Grâce à sa structure claire et son ergonomie adaptée, il constitue le **pilier de la supervision globale**.

Image de l’interface



Description détaillée : Tableau de bord Visiteur

Introduction

Le **Tableau de bord Visiteur** est une interface conçue pour les personnes externes au système, qui doivent être identifiées et suivies lors de leur passage dans l'environnement sécurisé. Contrairement au SuperAdmin ou au Personnel, le Visiteur occupe un rôle limité mais essentiel : il est enregistré, authentifié et surveillé pour garantir la sécurité globale.

Développement

- **Rôle de la personne qui utilise cette interface** : Le Visiteur est un utilisateur ponctuel ou externe (collaborateur invité, fournisseur, consultant). Son rôle est de **s'identifier** et de permettre au système de **suivre ses déplacements** dans les zones autorisées.
- **Droits et responsabilités** : Le Visiteur dispose de droits restreints :
    - Accéder uniquement aux zones autorisées.
    - Être suivi en temps réel par le système.
    - Ne pas modifier les données du système ni gérer d'autres utilisateurs. Sa responsabilité est de respecter les règles d'accès et de sécurité.
- **Utilité de la structure et de l'ergonomie** : L'interface est simplifiée pour éviter toute confusion. Elle permet au Visiteur de voir ses informations de profil, ses autorisations et éventuellement ses mouvements. Cette ergonomie réduit les erreurs et assure une **expérience fluide** même pour un utilisateur non formé.
- **Relation avec la base de données** : Les informations du Visiteur sont enregistrées dans la table **Visitors** ou intégrées dans la table **Users** avec un rôle spécifique. Ses déplacements sont stockés dans la table **Tracking**, permettant une traçabilité complète.

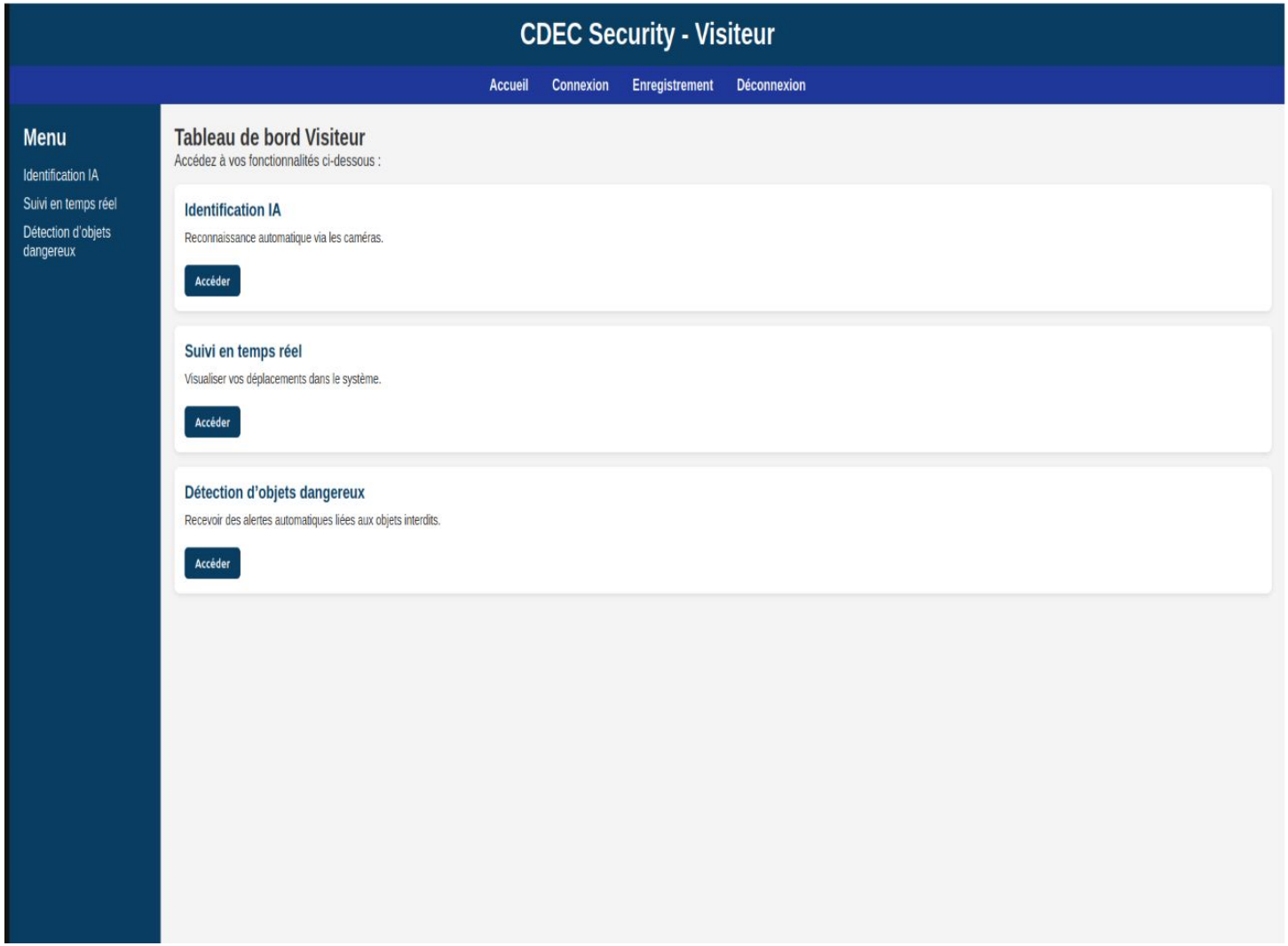
Relation avec l'utilisateur de l'application : Le Visiteur interagit avec le système de manière passive : il fournit ses informations et le système gère automatiquement son suivi. L'interface lui donne une transparence minimale sur ce qui est enregistré.

- **Niveau hiérarchique** : Le Visiteur est au **niveau le plus bas** de la hiérarchie. Il n'a aucun pouvoir décisionnel ni accès aux fonctionnalités critiques. Son rôle est uniquement de **se conformer** aux règles établies par le SuperAdmin et le Personnel.
- **Avantages de cette architecture dans le réseau** :
- **Sécurité renforcée** : chaque visiteur est identifié et suivi.
- **Traçabilité** : les déplacements sont enregistrés, ce qui permet de vérifier les accès en cas d'incident.
- **Clarté hiérarchique** : les droits sont strictement limités, évitant tout risque d'intrusion.
- **Interopérabilité** : l'architecture permet d'intégrer facilement des visiteurs dans le réseau sans perturber les autres niveaux.

Conclusion

Le **Tableau de bord Visiteur** est une interface simple mais stratégique. Il permet d’intégrer des personnes externes dans le système tout en maintenant un haut niveau de sécurité. Grâce à sa structure claire, sa relation directe avec la base de données et sa position hiérarchique limitée, il assure une **surveillance efficace** et une **protection renforcée du réseau**.

Image de l’interface



Description détaillée : Tableau de bord Personnel/Stagiaire

Introduction

Le **Tableau de bord Personnel/Stagiaire** est une interface dédiée aux membres internes de l'organisation (employés, stagiaires, collaborateurs). Contrairement au SuperAdmin, leur rôle est limité à la gestion de leurs propres informations et à l'utilisation des fonctionnalités qui leur sont attribuées. Cette page constitue leur **espace de travail numérique** au sein du système **CDEC Security**.

Développement

- **Rôle de la personne qui utilise cette interface** : Le Personnel ou Stagiaire est un utilisateur interne qui doit gérer son profil, ses objets personnels et interagir avec les modules de suivi et de détection. Son rôle est de **participer activement** au fonctionnement du système tout en respectant les règles de sécurité.
- **Droits et responsabilités** :
    - Modifier ses informations personnelles (nom, email, mot de passe).
    - Gérer ses objets enregistrés (ajout, suppression, mise à jour).
    - Consulter le suivi en temps réel de ses déplacements.
    - Recevoir des alertes de détection liées à ses activités. Contrairement au SuperAdmin, il ne peut pas gérer les autres utilisateurs ni administrer l'ensemble du système.
- **Utilité de la structure et de l'ergonomie** : L'interface est conçue pour être **simple et intuitive** : sidebar pour naviguer entre profil, objets, suivi et détection, et contenu central pour afficher les informations. Cette ergonomie permet au Personnel/Stagiaire de travailler efficacement sans se perdre dans des options complexes.

Utilité de la structure et de l'ergonomie : L'interface est conçue pour être simple et intuitive : sidebar pour naviguer entre profil, objets, suivi et détection, et contenu central pour afficher les informations. Cette ergonomie permet au Personnel/Stagiaire de travailler efficacement sans se perdre dans des options complexes.

- **Relation avec la base de données** :
- Les données personnelles sont stockées dans la table **Users** avec un rôle spécifique.
- Les objets sont liés à la table **Objects**, associés à l'identifiant de l'utilisateur.
- Les déplacements sont enregistrés dans la table **Tracking**.
- Les alertes sont stockées dans la table **Alerts**, filtrées par utilisateur. Cette relation assure une **cohérence entre l'interface et la base de données**.
- **Relation avec l'utilisateur de l'application** : Le Personnel/Stagiaire interagit directement avec l'application pour gérer ses informations et consulter ses données. L'interface lui donne

une **autonomie contrôlée**, tout en maintenant une dépendance vis-à-vis du SuperAdmin pour les décisions globales.

- **Niveau hiérarchique** : Le Personnel/Stagiaire occupe un **niveau intermédiaire** dans la hiérarchie. Il est au-dessus du Visiteur (qui n'a que des droits passifs), mais en dessous du SuperAdmin (qui contrôle tout le système).

Avantages de cette architecture dans le réseau :

- **Sécurité** : chaque utilisateur gère uniquement ses propres données.
- **Traçabilité** : toutes les actions sont enregistrées et liées à un identifiant unique.
- **Efficacité** : l'ergonomie permet une gestion rapide et autonome.
- **Hiérarchie claire** : les droits sont bien définis, évitant les conflits d'accès.
- **Scalabilité** : le système peut accueillir un grand nombre de personnels/stagiaires sans compromettre la sécurité.

Conclusion

Le **Tableau de bord Personnel/Stagiaire** est une interface essentielle pour les membres internes. Il leur offre un espace sécurisé et ergonomique pour gérer leurs informations et interagir avec le système. Grâce à sa relation directe avec la base de données et son positionnement hiérarchique intermédiaire, il garantit une **gestion efficace et sécurisée** dans le réseau **CDEC Security**.

Image de l’interface

Description détaillée : Page Gestion des objets personnels

Introduction

La page **Gestion des objets personnels** est une interface destinée aux **utilisateurs internes** (stagiaires et personnels). Elle leur permet de gérer les objets qu'ils utilisent ou possèdent dans le cadre de leur activité professionnelle. Cette fonctionnalité est essentielle pour assurer la **traçabilité**, la **sécurité** et la **responsabilité individuelle** au sein du système **CDEC Security**.

Rôle de la personne qui utilise cette interface : Le stagiaire ou le personnel utilise cette page pour enregistrer, modifier ou supprimer ses objets personnels (badge RFID, carte d'accès, etc.). Son rôle est de maintenir à jour son inventaire afin que le système puisse contrôler et surveiller l'usage de ces objets.

- **Droits et responsabilités** :
- Ajouter un nouvel objet à son profil.
- Modifier les informations d'un objet existant (nom, type, statut).
- Supprimer un objet qui n'est plus utilisé.
- Assurer que les objets enregistrés correspondent à la réalité. Ces droits impliquent la responsabilité de **déclarer correctement** ses possessions pour éviter les abus ou les failles de sécurité.
- **Utilité de la structure et de l'ergonomie** : L'interface est construite autour d'un **tableau clair** avec colonnes ID, Nom, Type, Statut et Actions. Les boutons « Modifier » et « Supprimer » rendent les interactions simples et rapides. Le bouton « Ajouter un nouvel objet » permet une extension facile de l'inventaire. Cette ergonomie garantit une **utilisation intuitive** même pour des utilisateurs peu expérimentés.

Relation avec la base de données : Chaque objet est lié à un utilisateur via un identifiant unique (userId). Les données sont stockées dans la table Objects, avec des champs tels que :

- `objectId` (identifiant de l'objet),
- `objectName` (nom de l'objet),
- `objectType` (type : accès, sécurité, etc.),
- `status` (actif, inactif),
- `userId` (propriétaire). Cette relation assure une **traçabilité complète** et permet au système de relier chaque objet à son propriétaire.
- **Relation avec l'utilisateur de l'application** : L'utilisateur interagit directement avec ses données. Il est autonome pour gérer ses objets, mais ses actions sont **contrôlées et enregistrées** dans la base. Cela crée une relation de confiance : l'utilisateur sait que ses objets sont reconnus par le système et que leur usage est sécurisé.

Niveau hiérarchique : Le stagiaire ou le personnel occupe un niveau intermédiaire. Il gère ses propres objets, mais n’a aucun droit sur ceux des autres. Le SuperAdmin, en revanche, peut consulter et superviser l’ensemble des objets enregistrés. Cette hiérarchie garantit une séparation claire des responsabilités.

- **Avantages de cette architecture dans le réseau** :
- **Sécurité renforcée** : chaque objet est identifié et lié à un utilisateur.
- **Traçabilité** : en cas d’incident, il est possible de savoir quel objet appartenait à qui.
- **Clarté hiérarchique** : les droits sont limités à l’utilisateur propriétaire.
- **Efficacité** : l’ergonomie du tableau permet une gestion rapide et intuitive.
- **Interopérabilité** : cette structure peut être reliée à d’autres modules (suivi en temps réel, détection d’objets dangereux).

Image de L’interface

Description détaillée : Page Suivi en temps réel

Introduction

La page **Suivi en temps réel** est une interface stratégique du système **CDEC Security**. Elle permet de visualiser les déplacements des utilisateurs dans l'environnement sécurisé. Cette fonctionnalité est essentielle pour assurer la **surveillance continue**, la **traçabilité des mouvements** et la **réactivité en cas d'incident**.

Développement

- **Rôle de la personne qui utilise cette interface** : Le SuperAdmin ou le personnel habilité utilise cette page pour **observer les déplacements des utilisateurs** (stagiaires, visiteurs, personnels). Son rôle est de garantir que les mouvements respectent les zones autorisées et de détecter toute anomalie.
- **Droits et responsabilités** :
    - Le **SuperAdmin** a accès à l'ensemble des données de suivi.
    - Le **Personnel/Stagiaire** peut consulter uniquement ses propres déplacements.
    - Le **Visiteur** est suivi automatiquement mais n'a pas accès à cette interface. La responsabilité de l'administrateur est de **contrôler et analyser** les données pour prévenir les risques.

Utilité de la structure et de l'ergonomie : L'interface est généralement composée d'un tableau ou d'une carte interactive affichant les positions en temps réel. Cette ergonomie permet une visualisation claire et immédiate des mouvements, facilitant la prise de décision rapide en cas d'incident.

- **Relation avec la base de données** : Les déplacements sont enregistrés dans la table **Tracking**, avec des champs tels que :
- `trackingId` (identifiant unique),
- `userId` (utilisateur suivi),
- `location` (position géographique ou zone),
- `timestamp` (date et heure). Cette relation assure une **traçabilité complète** et permet de reconstituer l'historique des déplacements.

- **Relation avec l'utilisateur de l'application** : L'utilisateur suivi n'interagit pas directement avec cette page, mais ses données sont affichées pour l'administrateur. Cela crée une relation de **surveillance passive** : l'utilisateur agit, le système enregistre, et l'administrateur observe.
- **Niveau hiérarchique** :

- Le **SuperAdmin** occupe le niveau le plus élevé et supervise tous les déplacements.
- Le **Personnel/Stagiaire** est à un niveau intermédiaire et peut consulter ses propres données.
- Le **Visiteur** est au niveau le plus bas et n’a aucun accès, mais ses mouvements sont enregistrés.

Avantages de cette architecture dans le réseau :

- **Sécurité renforcée** : chaque déplacement est suivi et enregistré.
- **Traçabilité** : possibilité de reconstituer les parcours en cas d’incident.
- **Réactivité** : détection immédiate des anomalies ou intrusions.
- **Clarté hiérarchique** : seuls les profils autorisés peuvent consulter les données.
- **Interopérabilité** : le suivi peut être relié à la détection d’objets dangereux pour une surveillance complète.

Conclusion

La page **Suivi en temps réel** est une **interface de surveillance essentielle**. Elle relie directement les utilisateurs à la base de données via leurs déplacements, définit les droits selon la hiérarchie et offre une vision claire et sécurisée du réseau. Grâce à sa structure ergonomique et sa traçabilité, elle constitue un **outil puissant de contrôle et de prévention** dans le système **CDEC Security**.

Image de l’interface

Description détaillée : Page Détection d’objets dangereux

Introduction

La page **Détection d’objets dangereux** est une interface cruciale du système **CDEC Security**. Elle permet de recevoir et visualiser des alertes automatiques générées par l’intelligence artificielle lorsqu’un objet suspect ou interdit est identifié. Cette fonctionnalité est au cœur de la mission de sécurité, car elle assure une **prévention proactive** des risques.

Développement

- **Rôle de la personne qui utilise cette interface** : Le **SuperAdmin** et le **Personnel/Stagiaire** utilisent cette page pour **surveiller les alertes**. Le SuperAdmin supervise l’ensemble du réseau, tandis que le Personnel/Stagiaire consulte les alertes liées à ses propres activités ou zones. Leur rôle est de **réagir rapidement** aux menaces détectées.
- **Droits et responsabilités** :
    - Le **SuperAdmin** peut consulter toutes les alertes, les classer par priorité et déclencher des actions correctives (blocage d’accès, notification générale).
    - Le **Personnel/Stagiaire** reçoit uniquement les alertes qui le concernent et doit signaler ou confirmer les incidents.
    - Le **Visiteur** n’a aucun accès à cette page, mais ses objets ou comportements peuvent être détectés et générer une alerte. Ces droits impliquent une responsabilité directe : **assurer la sécurité des personnes et des biens**.

Utilité de la structure et de l’ergonomie : L’interface est souvent composée d’un tableau de notifications ou d’une liste d’alertes avec détails (type d’objet, localisation, statut). Les alertes sont mises en évidence par des couleurs ou icônes (rouge pour danger, jaune pour suspicion). Cette ergonomie permet une lecture immédiate et une priorisation rapide des menaces.

- **Relation avec la base de données** : Les alertes sont enregistrées dans la table **Alerts**, avec des champs tels que :
- `alertId` (identifiant unique),
- `objectDetected` (nom ou type d’objet),
- `location` (zone où l’objet a été détecté),
- `timestamp` (date et heure),
- `status` (nouvelle, en cours, résolue). Cette relation garantit une **traçabilité complète** et permet d’analyser les incidents a posteriori.
- **Relation avec l’utilisateur de l’application** : L’utilisateur interagit directement avec les alertes : il peut les consulter, les confirmer ou les traiter. Cela crée une relation de **responsabilité active** : le système détecte, mais c’est l’utilisateur qui décide de l’action à entreprendre.

Niveau hiérarchique :

- Le **SuperAdmin** est au sommet et supervise toutes les alertes.
- Le **Personnel/Stagiaire** est à un niveau intermédiaire et gère uniquement ses propres alertes.
- Le **Visiteur** est au niveau le plus bas et n’a aucun accès, mais peut être sujet à une détection.
- **Avantages de cette architecture dans le réseau** :
- **Sécurité proactive** : les menaces sont détectées automatiquement.
- **Traçabilité** : chaque alerte est enregistrée et consultable.
- **Réactivité** : l’ergonomie permet une réponse rapide.
- **Clarté hiérarchique** : les droits sont adaptés au rôle de chaque utilisateur.
- **Interopérabilité** : la détection est reliée au suivi en temps réel et à la gestion des objets, créant un système intégré.

Conclusion

La page **Détection d’objets dangereux** est une **interface vitale** pour la sécurité du réseau **CDEC Security**. Elle relie l’intelligence artificielle à l’utilisateur, définit les responsabilités selon la hiérarchie et assure une surveillance proactive. Grâce à sa structure ergonomique et sa relation directe avec la base de données, elle constitue un **outil puissant de prévention et de protection**.

Description détaillée : Page Profil personnel

Introduction

La page **Profil personnel** est une interface individuelle qui permet à chaque utilisateur (stagiaire, personnel, voire SuperAdmin) de gérer ses informations personnelles. Elle constitue le **point de référence identitaire** dans le système **CDEC Security**, garantissant que chaque membre est correctement enregistré et reconnu.

Développement

- **Rôle de la personne qui utilise cette interface** : L'utilisateur (stagiaire ou personnel) utilise cette page pour **mettre à jour ses informations personnelles** : nom, email, mot de passe, rôle. Le SuperAdmin peut également consulter ou modifier les profils des autres, mais pour un utilisateur standard, cette page est son **espace personnel**.
- **Droits et responsabilités** :
    - Modifier ses propres informations (nom, email, mot de passe).
    - Mettre à jour son rôle si autorisé (souvent réservé au SuperAdmin).
    - Assurer l'exactitude des données saisies. La responsabilité de l'utilisateur est de maintenir ses informations à jour pour garantir la fiabilité du système.
- **Utilité de la structure et de l'ergonomie** : L'interface est organisée en **formulaire clair** avec champs et boutons. L'ergonomie simple permet une **navigation intuitive** et réduit les erreurs. La présence d'un espace pour la **photo de profil** renforce l'identification visuelle et la personnalisation.

Relation avec la base de données : Les données du profil sont stockées dans la table Users, avec des champs tels que :

- `userId` (identifiant unique),
- `name`, `email`, `password` (hashé),
- `role` (stagiaire, personnel, SuperAdmin),
- `profilePicture` (lien vers l'image). Cette relation assure une **cohérence entre l'interface et la base de données**, et permet au système de reconnaître chaque utilisateur.
- **Relation avec l'utilisateur de l'application** : L'utilisateur interagit directement avec ses données. Cette page lui donne une **autonomie contrôlée** : il peut gérer son identité numérique, mais reste soumis aux règles hiérarchiques (par exemple, il ne peut pas s'auto-promouvoir en SuperAdmin).
- **Niveau hiérarchique** :
- Le **SuperAdmin** peut consulter et modifier tous les profils.
- Le **Personnel/Stagiaire** ne peut modifier que son propre profil.

- Le **Visiteur** a un profil minimal, souvent créé automatiquement lors de son enregistrement. Cette hiérarchie garantit une séparation nette des responsabilités.

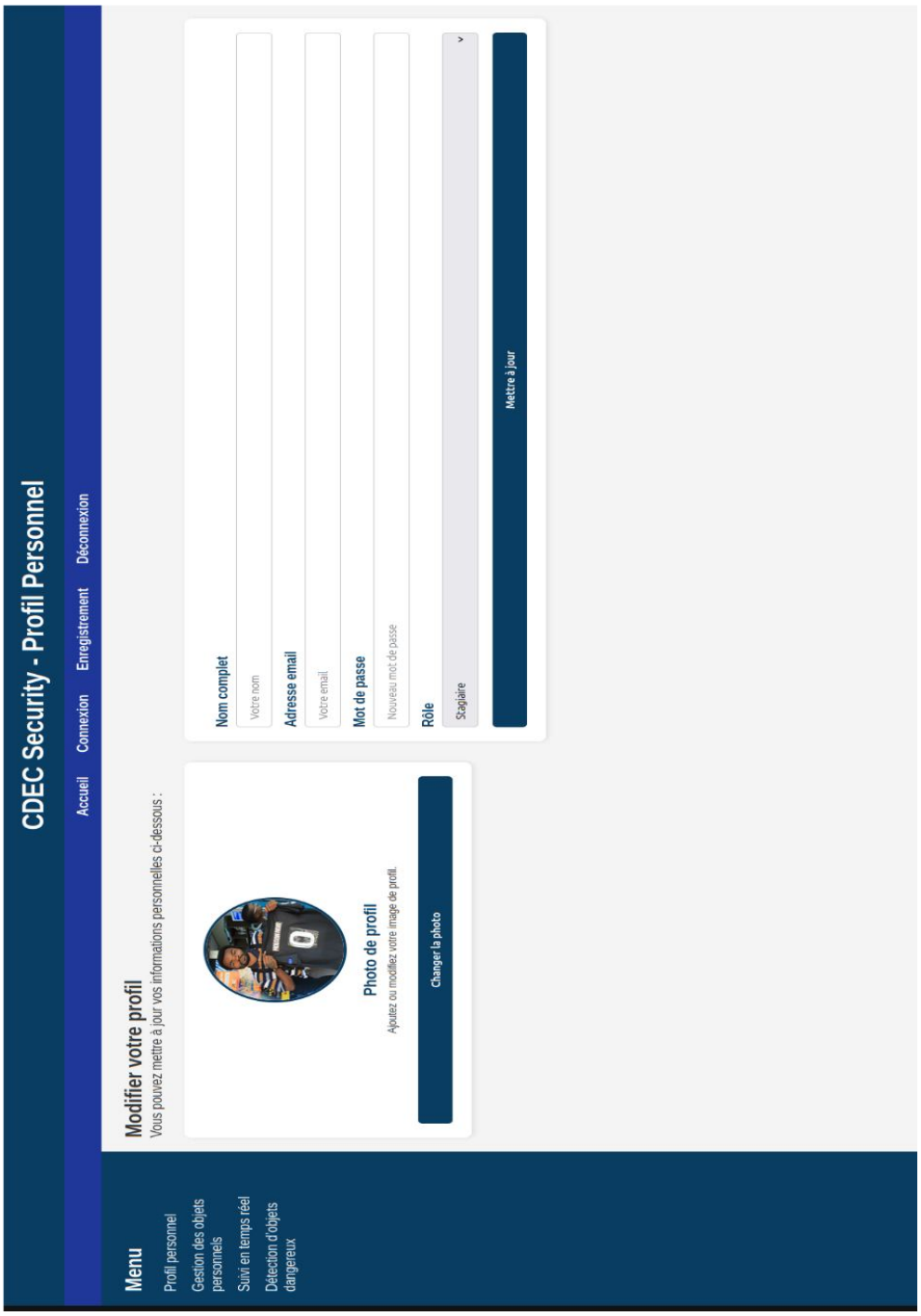
Avantages de cette architecture dans le réseau :

- **Sécurité** : chaque utilisateur est identifié de manière unique.
- **Traçabilité** : les modifications sont enregistrées et liées à un identifiant.
- **Clarté hiérarchique** : les droits sont adaptés au rôle.
- **Personnalisation** : la photo et les informations renforcent l'identification.
- **Interopérabilité** : le profil est lié à d'autres modules (objets, suivi, détection).

Conclusion

La page **Profil personnel** est une **interface fondamentale** qui relie l'utilisateur à la base de données et définit son identité numérique dans le système **CDEC Security**. Elle assure une gestion sécurisée et hiérarchisée des informations personnelles, tout en offrant une ergonomie simple et efficace. Elle constitue ainsi un **point d'ancrage essentiel** pour l'ensemble des fonctionnalités du réseau.

Image de l’interface



Sprint 6 : Matériel nécessaire et coût de production

Objectif

Recenser les ressources matérielles indispensables au bon fonctionnement du projet **CDEC Security**, en garantissant la performance, la fiabilité et la sécurité du système.

Le **Sprint 6** vise à établir une base solide pour la mise en œuvre technique du projet **CDEC Security**. Ce sprint se concentre sur la **planification matérielle** et la **prévision budgétaire**, deux éléments essentiels pour garantir la performance et la fiabilité du système. Les tableaux qui suivent permettent de visualiser, d'une part, les **ressources matérielles requises**, et d'autre part, le **coût global de production**.

Tableau des équipements requis

Ce tableau recense l'ensemble des **ressources matérielles nécessaires** au développement et au déploiement du système. Chaque catégorie d'équipement est associée à une description fonctionnelle précisant son rôle dans l'architecture du projet. L'objectif est de s'assurer que chaque composant — ordinateurs, serveurs, caméras intelligentes, routeurs, dispositifs de sauvegarde — contribue efficacement à la stabilité et à la sécurité du réseau. Ce tableau constitue donc une **base de référence technique**, permettant de planifier les achats, d'anticiper les besoins en maintenance et de garantir la compatibilité entre les différents modules (Web, IA, réseau local).

Équipement requis

Catégorie	Éléments matériels	Description / Rôle	Durée d'utilisation estimée
Ordinateurs performants	5 unités (Core i7/i9, 16 Go RAM, SSD 512 Go)	Développement, supervision et maintenance du système	6 mois
Serveurs dédiés	1 serveur principal + 1 serveur de sauvegarde	Hébergement de la base MongoDB, API Node.js et IA de reconnaissance	6 mois
Caméras intelligentes	10 caméras IP HD (vision nocturne, flux RTSP)	Surveillance et détection automatique des objets	6 mois
Connexion internet fiable	Routeur 4G illimité + fibre optique CDEC	Transmission des flux vidéo et synchronisation IA ↔ serveur	6 mois
Équipements réseau	Switch Gigabit, câblage RJ45 cat 6, onduleurs	Stabilité du réseau interne et protection électrique	6 mois
Matériel de sauvegarde	Disques externes SSD + NAS sécurisé	Sauvegarde des données sensibles et historiques	6 mois
Outils de développement	VS Code, Postman, Docker, GitHub, Trello	Environnement de travail collaboratif	6 mois

Tableau d’estimation du coût de production

Le second tableau traduit la planification matérielle en **valeurs économiques**. Il présente une estimation réaliste du **budget global** nécessaire à la mise en œuvre du projet, en détaillant les coûts unitaires et totaux par poste. Cette approche permet d’évaluer la **rentabilité du projet**, de justifier les investissements et de faciliter la prise de décision auprès des responsables techniques et financiers. Le tableau met en évidence les postes les plus coûteux (serveurs, ordinateurs performants, caméras intelligentes) et les éléments de support (connexion, outils logiciels, sauvegarde), afin d’obtenir une vision claire du **coût total de production**.

Estimation du coût

Poste	Quantité	Coût unitaire (FCFA)	Coût total (FCFA)
Ordinateurs portables	5	600 000	3 000 000
Serveurs dédiés	2	1 200 000	2 400 000
Caméras intelligentes	10	150 000	1 500 000
Routeur 4G + fibre	1	250 000	250 000
Équipements réseau	1 lot	300 000	300 000
Disques SSD + NAS	2	200 000	400 000
Licences et outils logiciels	-	150 000	150 000
Total estimé			**8 000 000 FCFA**

Synthèse

Ces deux tableaux forment un **ensemble cohérent** :

- Le premier définit **ce qu’il faut** pour construire et faire fonctionner le système.
- Le second indique **combien cela coûte** pour le réaliser.

Ensemble, ils constituent la **base logistique et financière** du projet **CDEC Security**, garantissant que la plateforme soit non seulement fonctionnelle et performante, mais aussi économiquement viable.

Sprint 7 : Conclusion technique

Objectif

Synthétiser les choix techniques effectués lors des sprints précédents et préparer le déploiement opérationnel de la plateforme **CDEC Security**. Cette conclusion sert de point de jonction entre la phase de conception et la phase de mise en œuvre, en validant la cohérence des décisions prises.

Description

Au terme des sprints de conception et de planification, plusieurs choix structurants ont été réalisés :

- Adoption de technologies modernes et robustes (**Next.js**, **MongoDB**, **JWT**, **bcrypt**, **cookies**) pour garantir la sécurité et la scalabilité de l'application web.
- Mise en place d'une architecture modulaire intégrant un **réseau de neurones IA** pour la reconnaissance et la traçabilité des objets.
- Définition d'une **charte graphique** alignée sur l'identité visuelle de la CDEC, renforçant la notion de sécurité et de confiance.
- Élaboration d'un **planning PERT** détaillé, permettant de suivre l'avancement du projet depuis l'installation de l'environnement jusqu'au déploiement final.
- Recensement des **ressources matérielles** et estimation des **coûts de production**, garantissant la faisabilité technique et financière du projet.

Ces choix assurent une cohérence entre les aspects **fonctionnels**, **techniques**, **visuels** et **logistiques**, tout en respectant les contraintes institutionnelles de la CDEC.

Livrable

Une **conclusion technique intégrée au rapport**, qui :

- Valide les décisions prises lors des sprints précédents.
- Prépare le terrain pour le **déploiement réseau local CDEC**.
- Sert de référence pour la phase de **maintenance et évolutivité** de la plateforme.

Conclusion

L'intégration des différentes sous-sections dans la méthodologie Scrum permet de transformer la conception technique en un processus structuré et progressif. Chaque sprint correspond à une étape clé, avec des livrables précis, garantissant une évolution régulière du projet vers un prototype fonctionnel puis un déploiement opérationnel.

Conclusion

Ce stage au sein de la CDEC m’a permis d’observer de près le fonctionnement du système de sécurité et d’identifier certaines limites techniques et organisationnelles. Loin de remettre en cause l’efficacité du personnel, ces constats ont mis en évidence la nécessité d’outils modernes capables de renforcer la traçabilité et la protection des biens personnels.

Les problématiques relevées — absence de reconnaissance automatique des objets, recherche manuelle chronophage et manque de base centralisée — ont été analysées en profondeur. Pour y répondre, une solution innovante a été proposée : une application web et mobile intégrant l’intelligence artificielle, un répertoire numérique des biens personnels et une recherche automatisée en cas de perte. Cette solution apporte de nombreux avantages : gain de temps, efficacité accrue, sécurité renforcée, valorisation de l’image de la CDEC, développement des compétences techniques, naissance d’une IA spécialisée et possibilité d’exporter la solution vers d’autres institutions. Toutefois, certaines limites doivent être prises en compte : respect de la vie privée, besoin de formation du personnel, complexité technique de l’intégration IA + base de données, dépendance à un réseau local fiable et contraintes matérielles au sein de la DSI (ordinateurs et connexion internet). Ces points de vigilance ne constituent pas des freins, mais des conditions à respecter pour assurer un déploiement réussi.

En définitive, ce projet représente une opportunité majeure pour la CDEC : il modernise ses pratiques de sécurité, valorise son image institutionnelle et ouvre la voie à de nouvelles perspectives de formation et de collaboration. Loin d’incriminer l’organisation, ce rapport met en lumière son choix d’innovation et son engagement à renforcer la sécurité de ses employés et visiteurs.