MasterCamp : Solution Factory



*KEGREISZ Clément  
JUGET Ulysse  
CALMON Audrey  
MAISL Elliot  
DUFFOURG Esteban* [*Ivaylo.ganchev@intervenants.efrei.net*](mailto:Ivaylo.ganchev@intervenants.efrei.net)

Table des matières

[Introduction 2](#_Toc139389889)

[Role-based access control (RBAC) 3](#_Toc139389890)

[Use case *(Scénario Support du projet)* : 3](#_Toc139389891)

[Limites, contraintes, parties prenantes, exigences particulières : 4](#_Toc139389892)

[Besoins et caractéristiques du projet 5](#_Toc139389893)

[Problématique et objet du projet 6](#_Toc139389894)

[Données existantes, formes et description 6](#_Toc139389895)

[Contraintes humaines et matérielles 6](#_Toc139389896)

[Objectifs premiers et finaux du projet 6](#_Toc139389897)

[Répartition des tâches au sein de l’équipe 7](#_Toc139389898)

[Diagrammes 8](#_Toc139389899)

[Organisation 10](#_Toc139389900)

[Planning Prévisionnel et Répartition des taches 10](#_Toc139389901)

[Github 11](#_Toc139389902)

[Notre solution : 11](#_Toc139389903)

[a. Guide d’installation 11](#_Toc139389904)

[b. Prérequis matériels et logiciels 12](#_Toc139389905)

[c. Log Admin 13](#_Toc139389906)

[d. Démonstration et guide 13](#_Toc139389907)

[Conclusion 17](#_Toc139389908)

# Introduction

La cybersécurité englobe divers domaines d'intérêt captivants. Dans le cadre du programme de troisième année de l'EFREI Paris, une école d'ingénieurs en informatique, les étudiants ont été invités à répondre à un appel d'offres de leur choix, afin d'explorer l'un de ces domaines. Dans le cadre du Mastercamp, un mois intensif dédié à l'apprentissage approfondi de la sécurité informatique, nous avons eu l'opportunité de renforcer nos compétences techniques et de mener à bien un projet. Parmi les trois sujets proposés, notre groupe 333 "Intranet", composé d'Audrey Calmon, Elliot Maisl, Ulysse Juget, Clément Kegreisz et Esteban Duffourg, a opté pour la réponse relative au "rôle-based access control" (RBAC). Étant donné le caractère très vaste du sujet proposé par notre cours, Solution Factory, nous avons élaboré notre propre appel d'offres. Ce rapport présente une définition du RBAC, notre appel d'offres, une analyse approfondie de notre problématique, ainsi que notre solution technique.

# Role-based access control (RBAC)

Dans le contexte de la sécurité et du réseau, RBAC fait référence à Role-Based Access Control, ce qui signifie le Contrôle d'Accès Basé sur les Rôles en français. Le projet RBAC vise à mettre en place un système de contrôle d'accès pour gérer les autorisations d'accès aux ressources dans un système informatique ou un réseau.

Le contrôle d'accès basé sur les rôles repose sur l'idée que les utilisateurs se voient attribuer des rôles spécifiques au sein d'une organisation et que ces rôles déterminent les autorisations dont ils disposent. Au lieu d'attribuer des autorisations individuelles à chaque utilisateur, le RBAC attribue des autorisations aux rôles et chaque utilisateur se voit attribuer un ou plusieurs rôles. Cela permet une gestion plus centralisée des autorisations et une simplification de la gestion des utilisateurs.

# Use case *(Scénario Support du projet)* :

**Objet** : Appel d'offre pour la conception et la mise en place d'un système de contrôle d'accès basé sur les rôles pour l'intranet de SecureCorp

Cher Intranet,  
SecureCorp, une entreprise leader dans le domaine de la sécurité informatique, vous contacte aujourd'hui afin de solliciter votre expertise pour le redéveloppement de notre intranet d'entreprise. Nous sommes convaincus de votre capacité à répondre à nos besoins et à concevoir un système de contrôle d'accès basé sur les rôles (RBAC) robuste et évolutif.

Contexte:  
SecureCorp est une entreprise mondiale spécialisée dans les solutions de sécurité informatique et le développement de logiciels. Notre intranet actuel est obsolète et ne répond plus efficacement à nos besoins en matière de collaboration et de gestion des ressources internes. Nous souhaitons donc mettre en place un intranet modernisé, doté d'un système de contrôle d'accès basé sur les rôles, qui nous permettra de réguler l'accès aux différentes fonctionnalités et informations disponibles.

Objectifs du projet :

* Redesign de l'interface utilisateur de notre intranet pour améliorer l'expérience utilisateur et favoriser la productivité des employés.
* Mise en place d'un système RBAC flexible et modifiable pour gérer les autorisations d'accès en fonction des rôles attribués aux utilisateurs.
* Création de différents rôles prédéfinis (administrateur, gestionnaire de projet, membre de l'équipe, etc.) avec des permissions spécifiques correspondant à leurs responsabilités.
* Possibilité de personnaliser les rôles et les permissions en fonction des besoins spécifiques de chaque département ou projet.
* Implémentation d'un mécanisme de gestion des utilisateurs pour faciliter l'attribution des rôles et l'ajout/suppression des utilisateurs du système.
* Garantie de la sécurité des données et des informations sensibles stockées sur l'intranet.

Livraison attendue :  
Nous attendons de votre part une proposition détaillée comprenant les éléments suivants :

* Une analyse des besoins fonctionnels et techniques pour la mise en place du système RBAC.
* Une proposition de conception de l'interface utilisateur pour le nouvel intranet.
* Une description complète des différents rôles prédéfinis et de leurs permissions associées.
* Une méthodologie de mise en œuvre du système RBAC, incluant les étapes de développement, de test et de déploiement.
* Un plan de formation pour sensibiliser et former nos employés à l'utilisation du nouvel intranet.

Calendrier prévisionnel :  
Date limite de réception des offres : 29/06/2023  
Évaluation des propositions et sélection du prestataire : 30/06/2023  
Début du projet : 01/07/2023  
Livraison finale du système RBAC et du nouvel intranet : 07/07/2023

Contraintes et exigences :

* Le système RBAC doit être développé en utilisant des technologies sécurisées et robustes, en conformité avec les meilleures pratiques de l'industrie.
* L'interface utilisateur doit être intuitive, ergonomique et adaptée à tous les types d'appareils (ordinateurs de bureau, tablettes, smartphones).
* Le système doit être évolutif afin de prendre en compte la croissance future de notre entreprise et de permettre des modifications rapides des rôles et des permissions.
* Toutes les données et les informations stockées sur l'intranet doivent être protégées et sécurisées conformément aux normes de sécurité en vigueur.

Nous vous invitons à soumettre votre proposition détaillée en réponse à cet appel d'offre avant la date limite indiquée ci-dessus. N'hésitez pas à nous contacter si vous avez des questions ou besoin de clarifications supplémentaires.

Nous sommes impatients de collaborer avec votre équipe et de mettre en place un système RBAC efficace pour notre intranet d'entreprise.

Cordialement,  
Samantha Johns  
DSI  
SecureCorp

# Limites, contraintes, parties prenantes, exigences particulières :

Limites :

Le projet se limite à la conception et à la mise en place d'un système de contrôle d'accès basé sur les rôles pour l'intranet de SecureCorp.

Contraintes :

* Le système RBAC doit être développé en utilisant des technologies sécurisées et robustes, conformément aux meilleures pratiques de l'industrie.
* L'interface utilisateur doit être intuitive, ergonomique et adaptée à tous les types d'appareils (ordinateurs de bureau, tablettes, smartphones).
* Le système doit être évolutif pour prendre en compte la croissance future de l'entreprise et permettre des modifications rapides des rôles et des permissions.
* Toutes les données et les informations stockées sur l'intranet doivent être protégées et sécurisées conformément aux normes de sécurité en vigueur.

Parties prenantes :

* **SecureCorp** : L'entreprise qui sollicite l'expertise du prestataire pour le redéveloppement de son intranet et la mise en place du système RBAC.
* **Prestataire (nous)** : L'entreprise à qui l'appel d'offre est adressé et qui sera responsable de la conception et de la mise en place du système RBAC.
* **Employés de SecureCorp** : Les utilisateurs finaux du nouvel intranet, qui bénéficieront d'une meilleure expérience utilisateur et d'un contrôle d'accès basé sur les rôles.
* **Départements et projets de SecureCorp** : Les entités internes qui auront des besoins spécifiques en termes de rôles et de permissions, et qui devront être pris en compte lors de la personnalisation du système RBAC.

Exigences particulières :

* Le système RBAC doit permettre la création de rôles prédéfinis avec des permissions spécifiques correspondant aux responsabilités de chaque rôle.
* Il doit être possible de personnaliser les rôles et les permissions en fonction des besoins spécifiques de chaque département ou projet.
* Un mécanisme de gestion des utilisateurs doit être mis en place pour faciliter l'attribution des rôles et l'ajout/suppression des utilisateurs du système.
* Le prestataire doit garantir la sécurité des données et des informations sensibles stockées sur l'intranet, en respectant les normes de sécurité en vigueur.
* Le calendrier prévisionnel du projet doit être respecté, avec une livraison finale du système RBAC et du nouvel intranet à la date spécifiée.

# Besoins et caractéristiques du projet

Le projet de conception et de mise en place d'un système de contrôle d'accès basé sur les rôles pour l'intranet de SecureCorp vise à répondre aux besoins suivants :

**Amélioration de l'expérience utilisateur** : L'intranet actuel ne satisfait plus efficacement les besoins de collaboration et de gestion des ressources internes. Le nouveau système doit permettre un redesign de l'interface utilisateur, en le rendant plus convivial, intuitif et ergonomique. L'objectif est de favoriser la productivité des employés en facilitant l'accès aux fonctionnalités et aux informations pertinentes.

**Gestion des autorisations d'accès** : Le système RBAC doit permettre une gestion flexible des autorisations en fonction des rôles attribués aux utilisateurs. Il doit être modifiable pour permettre des ajustements rapides des permissions en fonction des besoins évolutifs de l'entreprise. Des rôles prédéfinis (administrateur, gestionnaire de projet, membre de l'équipe, etc.) doivent être créés, chacun ayant des permissions spécifiques correspondant à leurs responsabilités.

**Personnalisation des rôles et des permissions** : Il est nécessaire de pouvoir personnaliser les rôles et les permissions en fonction des besoins spécifiques de chaque département ou projet au sein de SecureCorp. Cela permettra d'adapter le système aux différentes structures organisationnelles et aux exigences particulières de chaque équipe.

**Mécanisme de gestion des utilisateurs** : Le système doit être doté d'un mécanisme de gestion des utilisateurs permettant de faciliter l'attribution des rôles et l'ajout/suppression des utilisateurs du système. Il doit offrir une interface conviviale pour gérer les utilisateurs de manière efficace, tout en garantissant la sécurité des données personnelles.

**Sécurité des données et des informations** : Toutes les données et les informations stockées sur l'intranet doivent être protégées et sécurisées conformément aux normes de sécurité en vigueur. Le système RBAC doit mettre en place des mesures de sécurité robustes pour prévenir les accès non autorisés et assurer la confidentialité des données sensibles.

# Problématique et objet du projet

## Données existantes, formes et description

Le design et la structure de notre application pourront s’inspirer des sites internet et des applications déjà existants dans le milieu professionnel administratif. Notre but est d’appliqué sur un site et une infrastructure donnée une solution RBAC pertinente.

## Contraintes humaines et matérielles

Il est clair que ce projet est ambitieux et encore plus pour une équipe de 5 sur une fenêtre de temps aussi courte. Nous avons eu recours à l’utilisation de méthode de management afin que le suivie et la production du projet suivent leur cours de façon optimale. Techniquement nous avons été limités par un produit performant sur machine locale et non déployé sur l’internet car cela entrainerait des couts financiers que nous ne pouvons assumer. Nous avons donc utilisé les technologies ReactJS, Vite, PostgreSQL, Express.js et Prisma.

## Objectifs premiers et finaux du projet

Objectifs premiers :

**Redesign de l'interface utilisateur** : L'objectif principal est d'améliorer l'expérience utilisateur en repensant l'interface de l'intranet de SecureCorp. Cela comprend une conception conviviale, intuitive et ergonomique qui favorise la productivité des employés et facilite l'accès aux fonctionnalités pertinentes.

**Mise en place d'un système RBAC robuste** : Le déploiement d'un système de contrôle d'accès basé sur les rôles est un élément clé du projet. L'objectif est de créer un système RBAC flexible, modifiable et évolutif qui permettra une gestion efficace des autorisations d'accès en fonction des rôles attribués aux utilisateurs.

**Création de rôles prédéfinis et personnalisation** : Le projet vise à établir différents rôles prédéfinis tels que l'administrateur, le gestionnaire de projet et le membre de l'équipe, avec des permissions spécifiques adaptées à leurs responsabilités. De plus, le système doit permettre la personnalisation des rôles et des permissions pour répondre aux besoins spécifiques de chaque département ou projet au sein de SecureCorp.

Objectifs finaux :

**Amélioration de la collaboration et de la gestion des ressources** : En mettant en place un système RBAC efficace, l'intranet de SecureCorp deviendra un outil central pour la collaboration et la gestion des ressources internes. Les utilisateurs auront accès aux fonctionnalités et aux informations appropriées en fonction de leurs rôles, ce qui facilitera la coordination et la productivité au sein de l'entreprise.

**Sécurité renforcée des données et des informations** : L'objectif final est de garantir la sécurité des données et des informations stockées sur l'intranet de SecureCorp. Le système RBAC doit mettre en place des mesures de sécurité robustes pour prévenir les accès non autorisés et assurer la confidentialité des données sensibles, conformément aux normes de sécurité en vigueur.

**Adaptabilité aux besoins futurs** : Le système RBAC doit être évolutif, permettant ainsi de prendre en compte la croissance future de l'entreprise et de faciliter les modifications rapides des rôles et des permissions. Cela permettra à SecureCorp de s'adapter aux changements organisationnels et de maintenir l'efficacité de son intranet sur le long terme.

# Répartition des tâches au sein de l’équipe

Chaque semaine nous nous sommes imposés les taches suivantes et nous les avons accompagné de « Daily » qui maintenait un flux de productivité continue :

**Brainstorming et planification** : L'équipe se réunit pour discuter des objectifs du projet, des fonctionnalités souhaitées et des contraintes. Ensemble, ils élaborent un plan détaillé pour le projet, identifient les principales étapes et définissent les livrables attendus.

**Recherche et analyse des besoins** : L'équipe effectue une recherche approfondie sur les systèmes de contrôle d'accès basés sur les rôles, analyse les besoins des utilisateurs et étudie les meilleures pratiques en matière de conception d'interfaces utilisateur conviviales. Ils partagent leurs résultats et conclusions lors de réunions de groupe pour prendre des décisions éclairées.

De cela s’est majoritairement dessiné plusieurs tâches majeures :

**Conception de l'interface utilisateur** : Les membres de l'équipe travaillent ensemble pour concevoir une interface utilisateur intuitive et attrayante. Ils utilisent des outils de conception collaboratifs et partagent régulièrement leurs idées et prototypes pour recueillir les commentaires de l'équipe et s'assurer que l'interface répond aux besoins des utilisateurs.

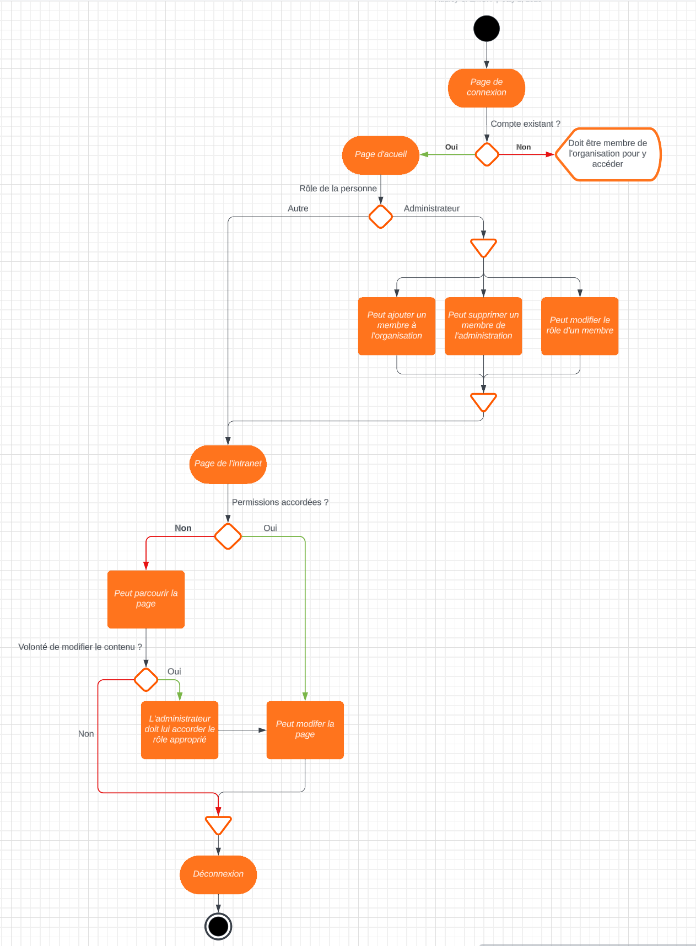
**Développement collaboratif** : L'équipe se divise en sous-groupes pour développer différentes fonctionnalités du système RBAC. Chaque sous-groupe est responsable d'une partie spécifique du projet et collabore étroitement pour assurer l'interopérabilité et l'intégration harmonieuse des différentes fonctionnalités. Les membres de l'équipe partagent régulièrement leurs progrès, résolvent les problèmes ensemble et se soutiennent mutuellement dans leurs tâches de développement.

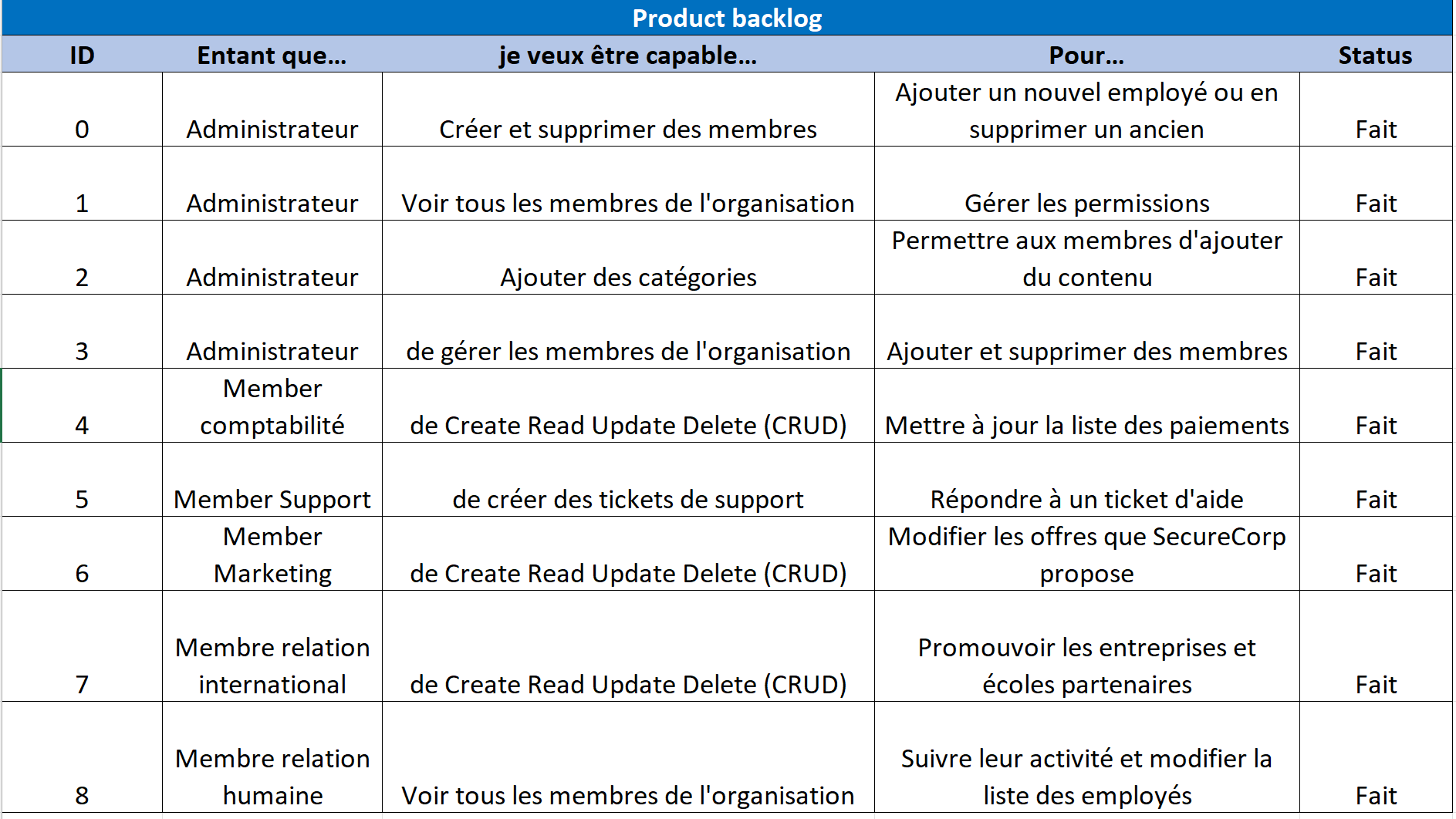
**Tests et validation** : Les membres de l'équipe travaillent en collaboration pour tester le système RBAC à différents niveaux (fonctionnalités, performances, sécurité) et détecter les éventuels problèmes ou bogues. Ils partagent les résultats des tests, discutent des solutions possibles et effectuent les corrections nécessaires de manière collaborative.

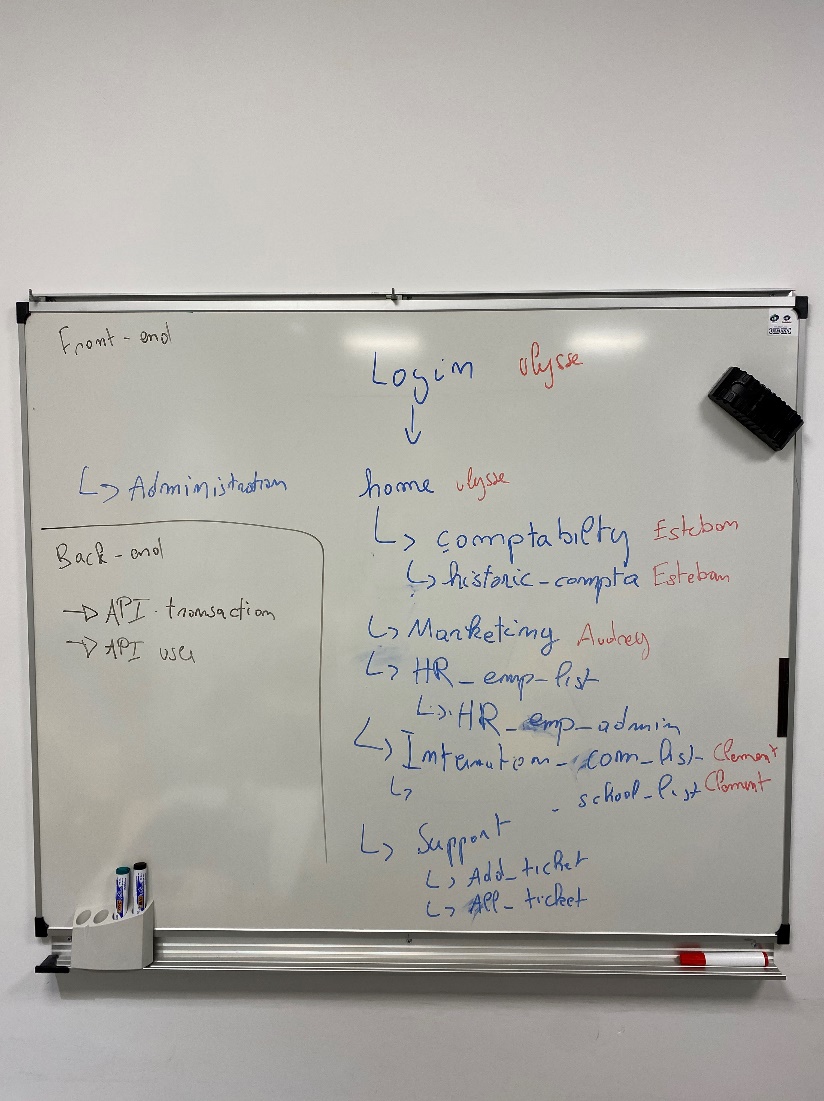
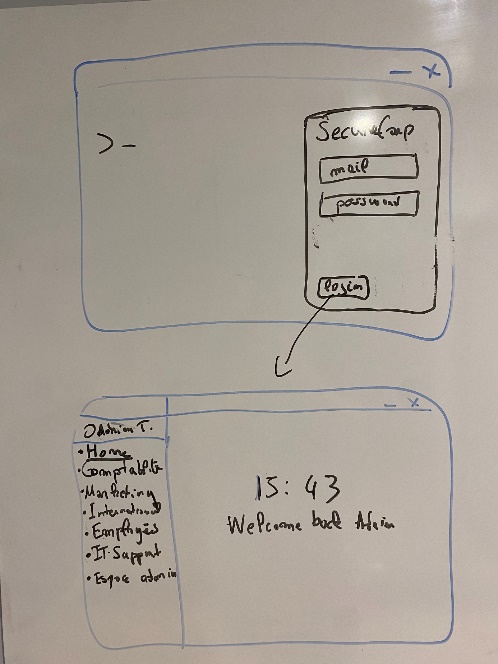
**Formation et support** : L'équipe collabore pour créer des supports de formation, organiser des sessions de formation et fournir un support post-formation aux utilisateurs du système RBAC. Ils partagent leurs connaissances et compétences pour garantir que tous les membres de l'équipe sont bien informés et capables de répondre aux questions et aux besoins des utilisateurs.

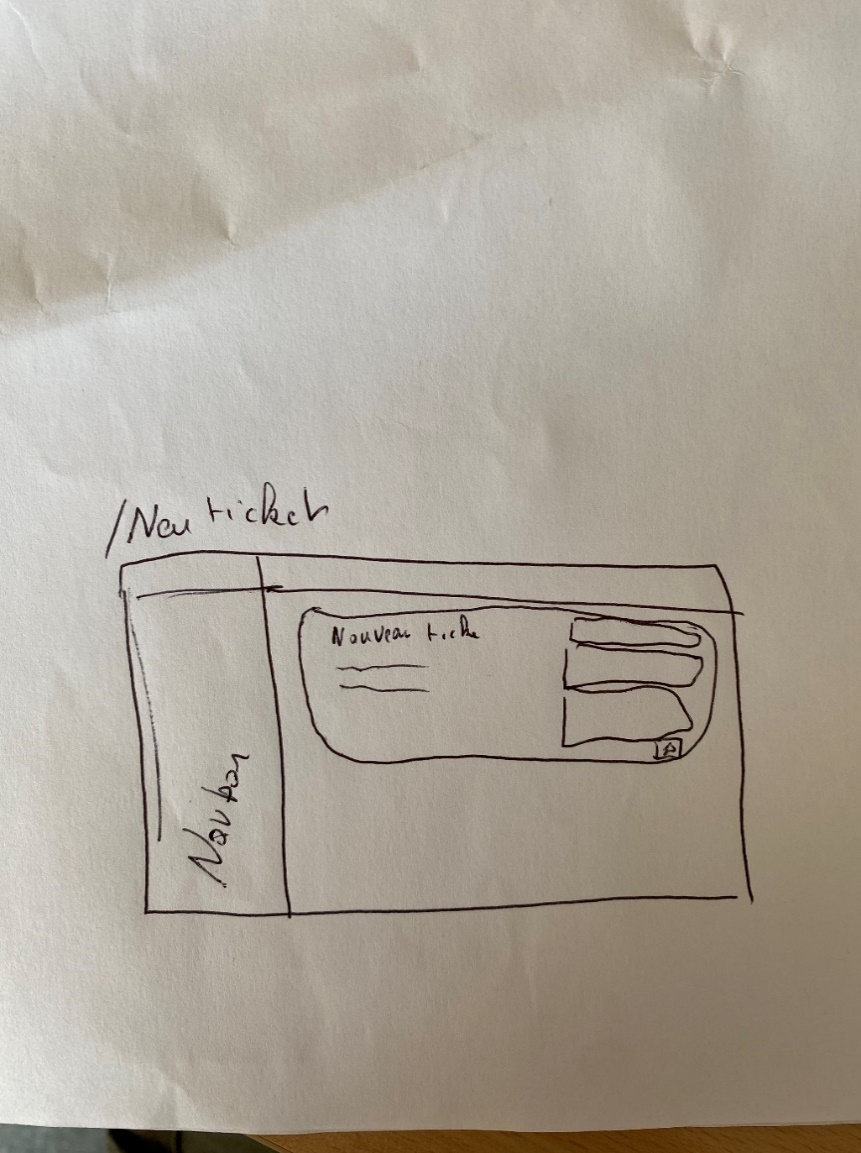
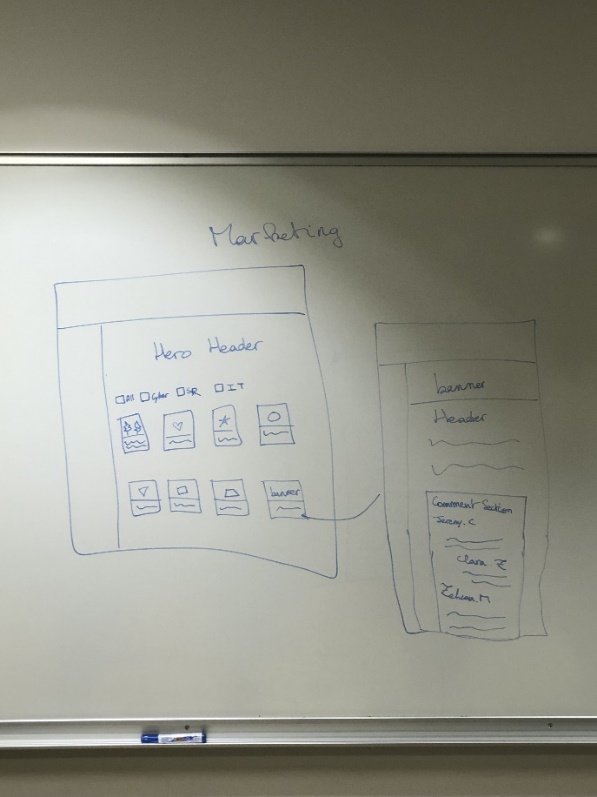
Cette répartition collaborative encourage la communication, la créativité et la collaboration entre les membres de l'équipe, permettant ainsi de tirer parti des forces et des idées de chacun. Il est essentiel de maintenir des canaux de communication ouverts, d'organiser des réunions régulières pour partager les progrès et de favoriser l'échange d'idées et de connaissances tout au long du projet.

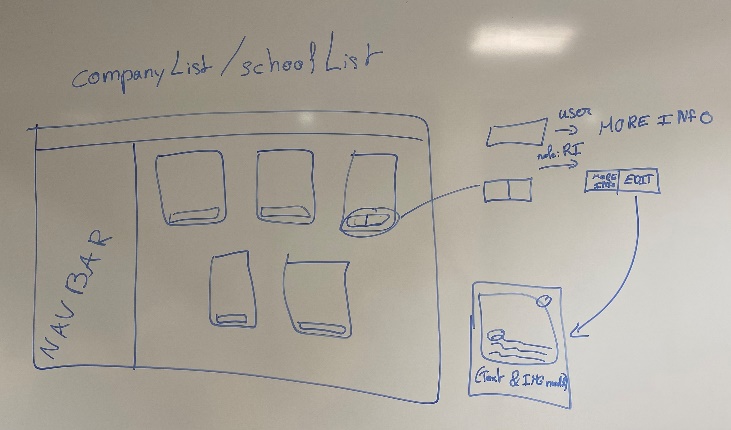
# Diagrammes

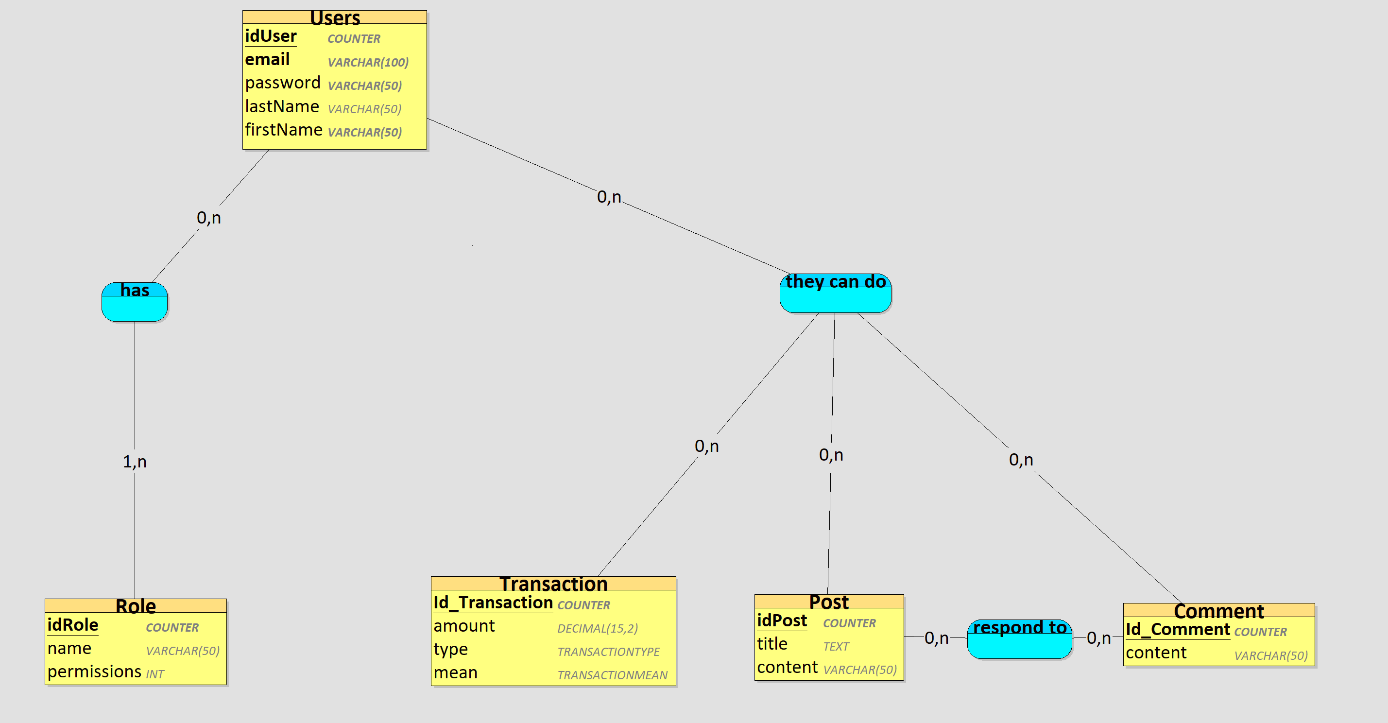
  
*Diagramme FlowChart*

  
*Diagramme Product Backlog*

  
*/home, 12 Juin, Esquisse Vue d’ensemble, 13 Juin, Esquisse*

  
*/Marketing, 13 Juin, Esquisse /Newticket, 14 Juin, Esquisse*

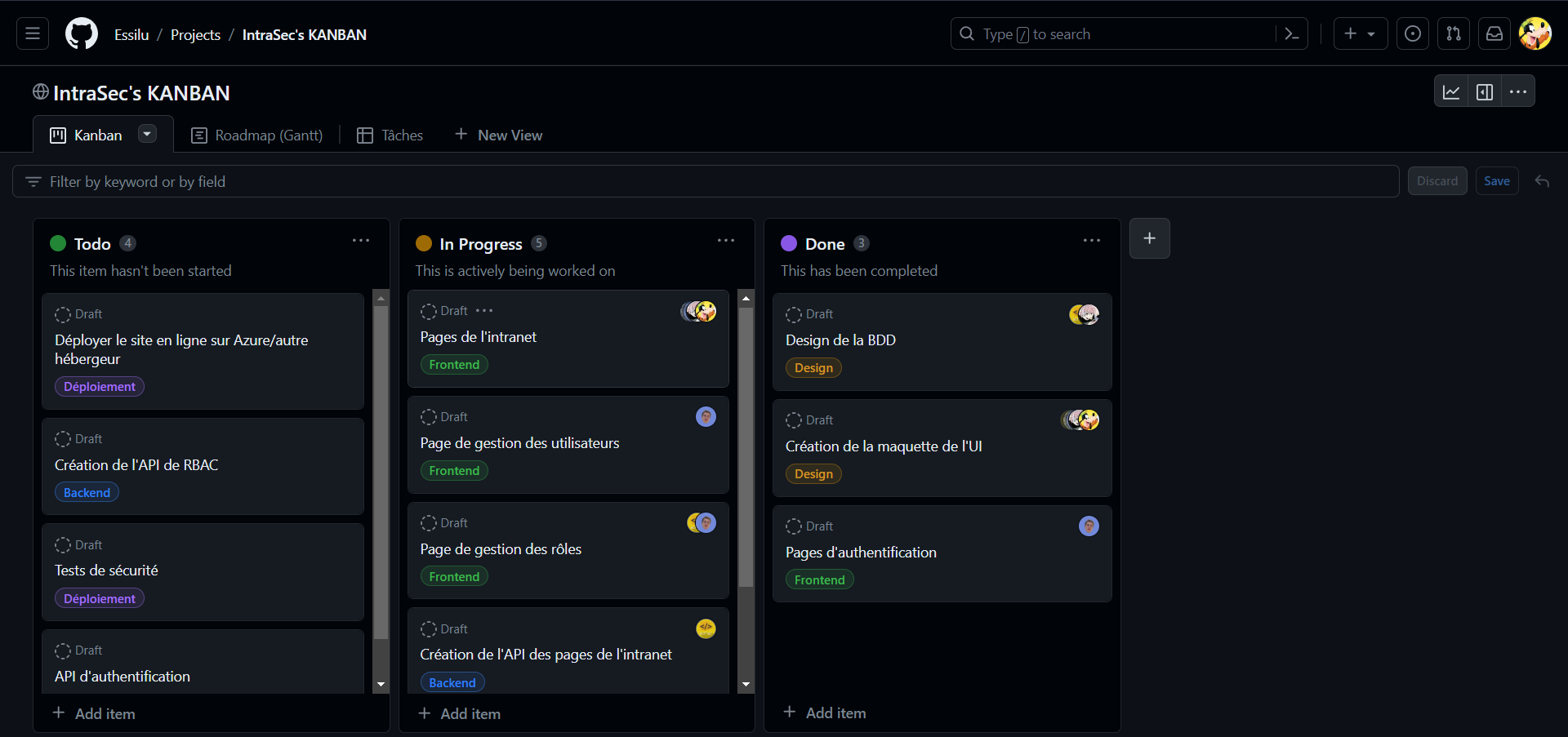
  
*/companyList & /schoolList, 14 Juin, Esquisse*

  
*Diagramme de conception de base de données, 13 Juin, Looping*

# Organisation

## Planning Prévisionnel et Répartition des taches

<https://github.com/users/Essilu/projects/1>  
*Lien du suivie de projet (équivalent Trello)*

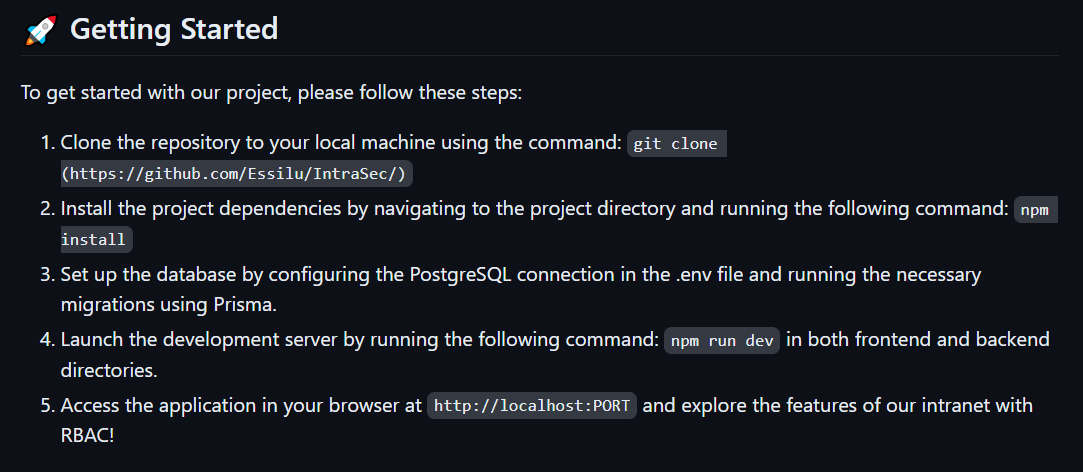


## Github

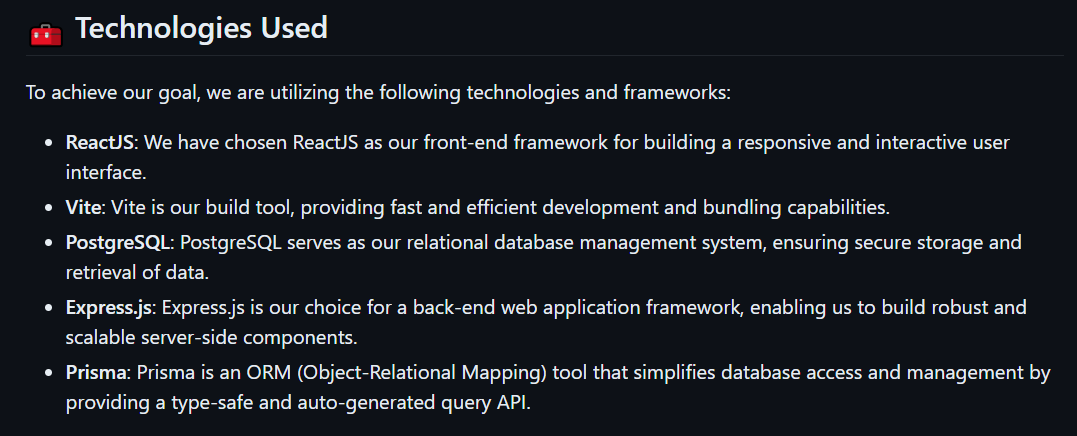
<https://github.com/Essilu/IntraSec>  
*Lien du repository du projet*

# Notre solution :

## Guide d’installation



## Prérequis matériels et logiciels



Pour la création de notre solution, nous nous sommes tout d’abord concentrés sur le frontend avec la création des pages pour savoir quelles fonctionnalités implémenter et pour qui. Nous avions déjà une idée des rôles à créer mais pas tout à fait en ce qui concernait leurs droits. Une fois que nous avions bien avancer sur le frontend et que le backend était prêt, nous avons travaillés sur les permissions et leurs implémentations.

Pour notre système de rôles, nous avons besoin de savoir si chaque rôle a, ou non, une certaine permission. Il existe une petite cinquantaine de permissions, par exemple "Voir les transactions bancaires" (la comptabilité), Créer un ticket de Support, Modifier n'importe quel article du blog marketing, Supprimer uniquement ses propres articles du blog marketing, Créer un rôle, etc.

Ainsi, nous avons dressé la liste de toutes les permissions possibles, il faut maintenant les ajouter dans les rôles.

La solution la plus simple aurait été d'ajouter dans notre base de données des rôles un champ par permission, avec une valeur booléenne (oui/non). Seulement cela prend beaucoup d'espace (disque, mémoire, etc), n'est pas très pratique à coder car il y a beaucoup de permissions, et n'est pas très adaptable si nous voulons ajouter ou modifier/enlever des permissions à l'avenir (il faudra ajouter/modifier/enlever beaucoup de champs, sur potentiellement beaucoup de rôles).

Ainsi, nous avons utilisé une technique appelée les "flags bitwise", qui utilise des propriétés beaucoup plus bas niveau d'informatique. Pour faire simple, en informatique un nombre est représenté par une série de 0 et de 1. Ainsi, en binaire, le nombre "0000001100101100" représente le nombre 812. Il est intéressant de remarquer que nous pouvons uniquement mettre des 0 ou des 1 pour chaque chiffre composant le nombre, appelés "bit". Nous avons utilisé cette propriété à notre avantage : nos permisssions sont donc stockées dans un seul nombre, où chaque chiffre du nombre correspond à une permission, et en fonction de si le bit est à 0 ou 1, la permission est respectivement désactivée ou activée.

Par exemple, si nous disons que pour les transactions de comptabilité, la nomenclature est : 1er bit : Créer, 2nd bit: Voir, 3ème bit: Modifier, 4ème bit: Supprimer, et que nous voyons qu'un rôle à les permissions "7", alors nous savons qu'il a les permissions "0111", c'est-à-dire Créer, Voir, Modifier, mais pas Supprimer.

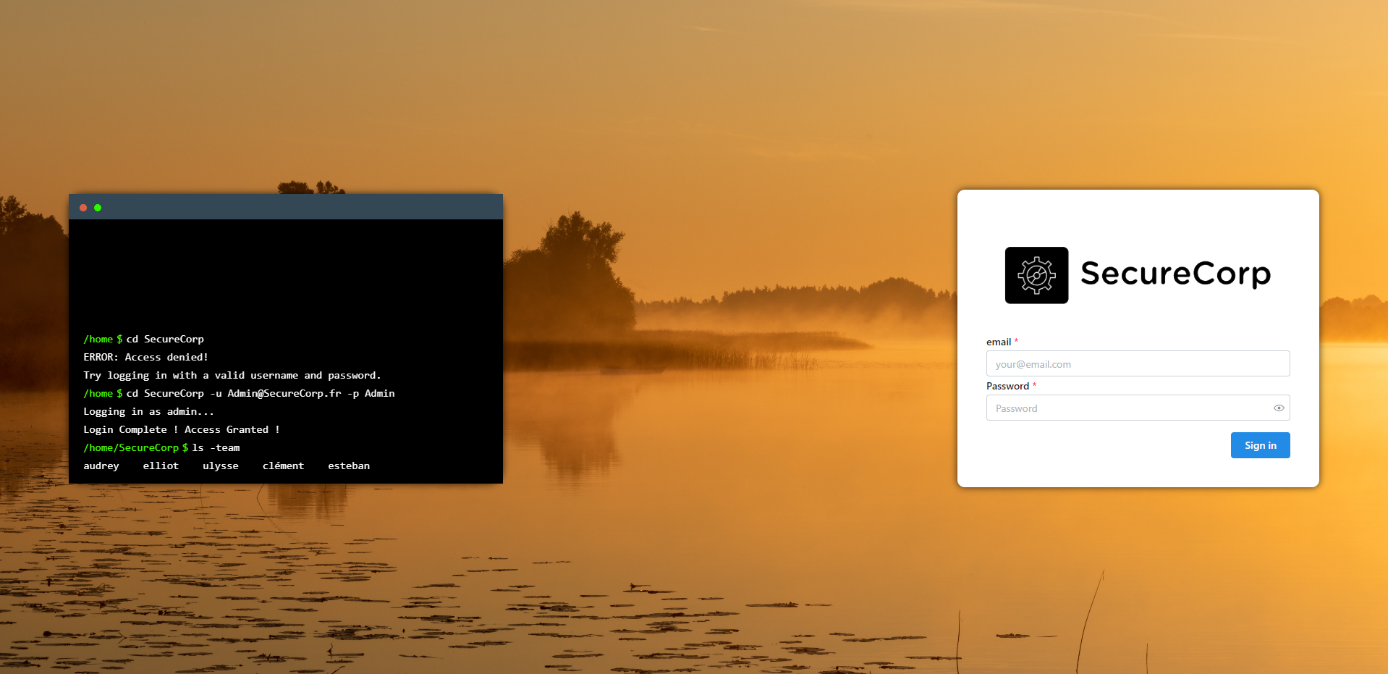
Ceci nous permet de stocker les permissions de manière très optimisée et de faire des calculs très rapides, avec une empreinte quasi-nulle sur les mémoires disque et vive des machines. C'est aussi très facilement scalable, si nous voulons ajouter des permissions il faut juste s'assurer qu'elles ne dépassent pas les 64 bits (taille maximale des nombres sur la majorité des ordinateurs d'aujourd'hui), et pour cela, nous avons séparé les nombres par catégories. Ainsi, nous avons un nombre pour les transactions, un nombre pour les posts (article de blog, ticket de support…), un nombre pour les commentaires (de blog, de support…), un nombre pour les utilisateurs (créer un nouvel utilisateur, supprimer un utilisateur…), et un dernier pour les rôles.

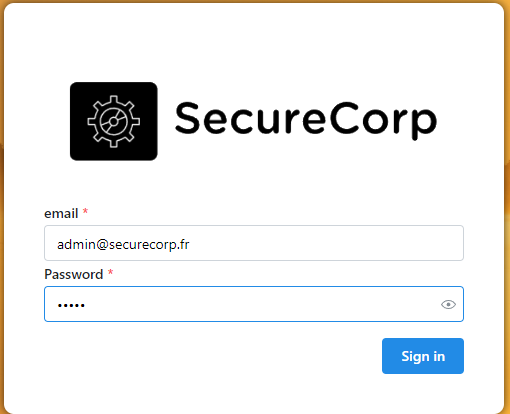
Ajouter une catégorie sera alors aussi simple que d'ajouter un champ aux rôles avec la valeur "0" (tout de désactivé par défaut).

## Log Admin

Email : [*admin@securecorp.fr*](mailto:admin@securecorp.fr)  
password : admin

## Démonstration et guide

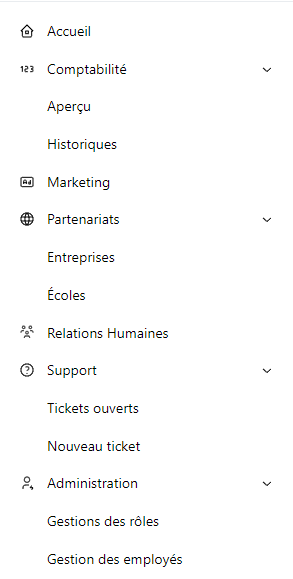
  
*/login/*

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

*/home/*

Une image contenant texte, logiciel, nombre, Icône d’ordinateur

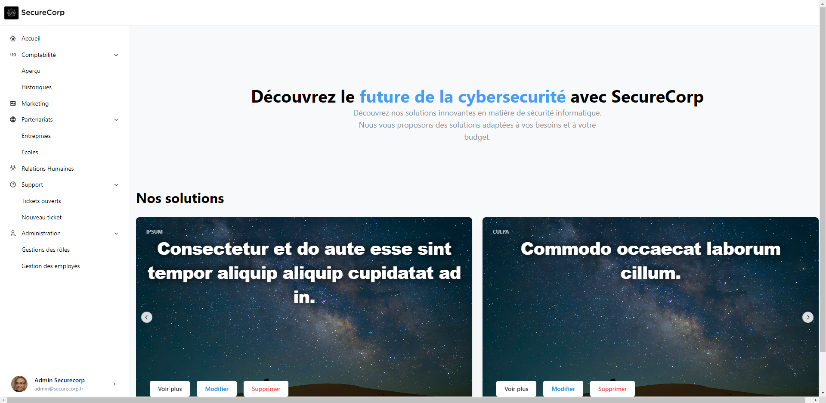
Description générée automatiquement

/comptabilité 1 1

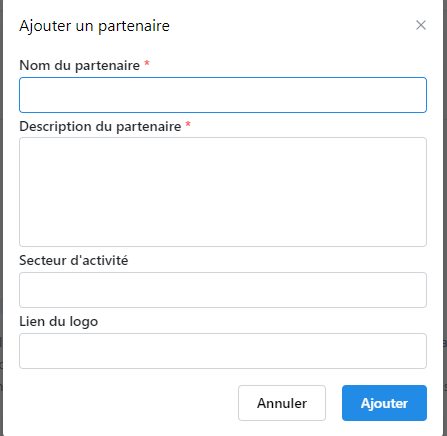
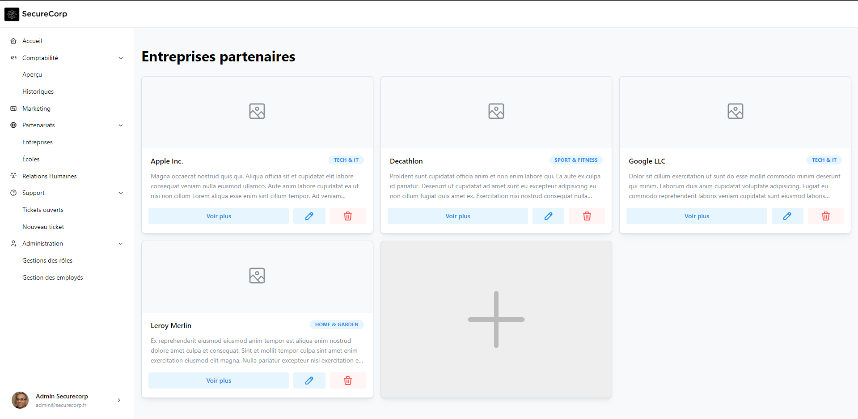
/Navbar 1

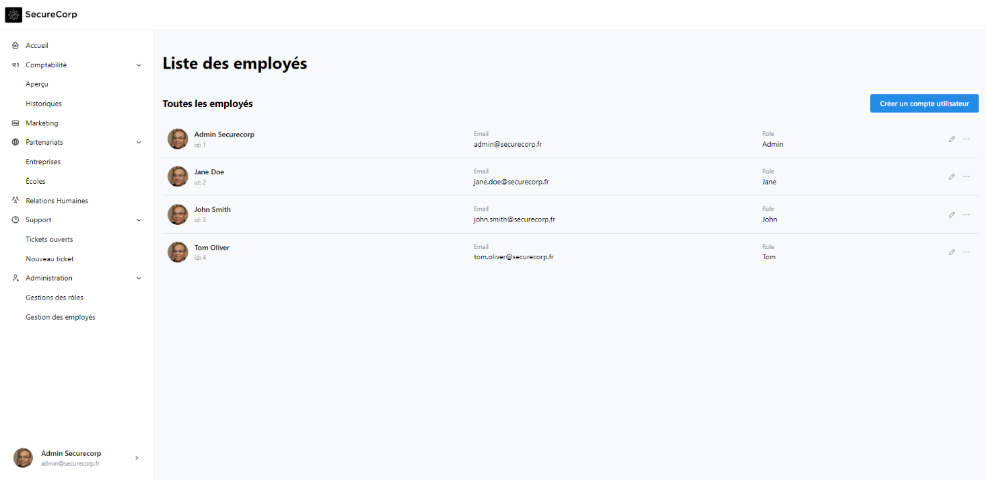
Une image contenant texte, capture d’écran, nombre, Police

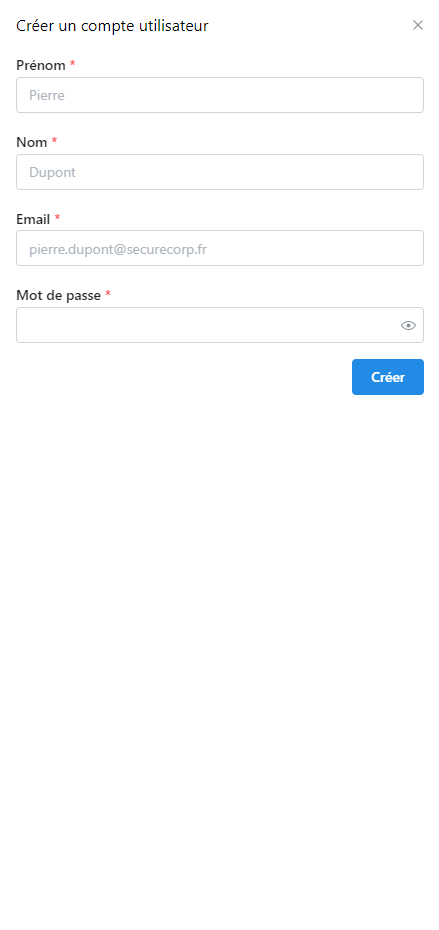
Description générée automatiquement

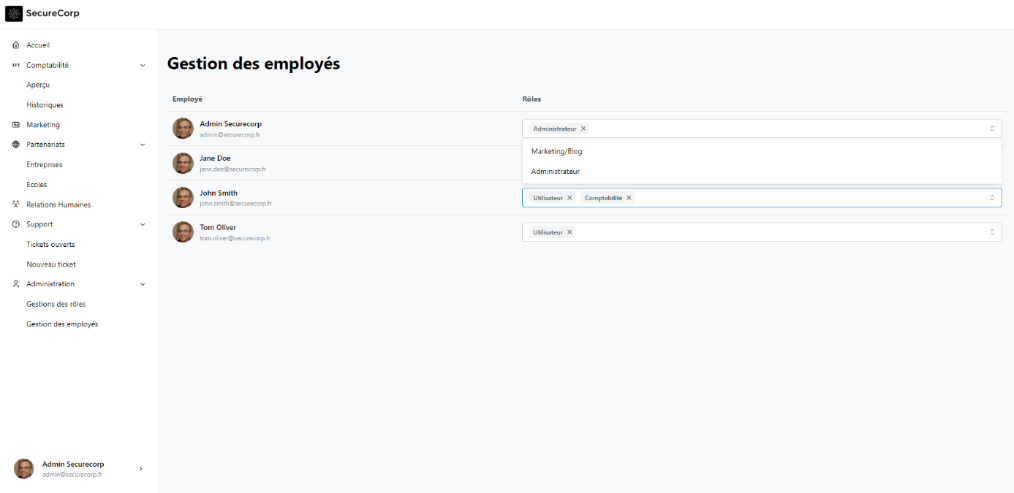


Log en tant qu’admin les cartes sont modifiables

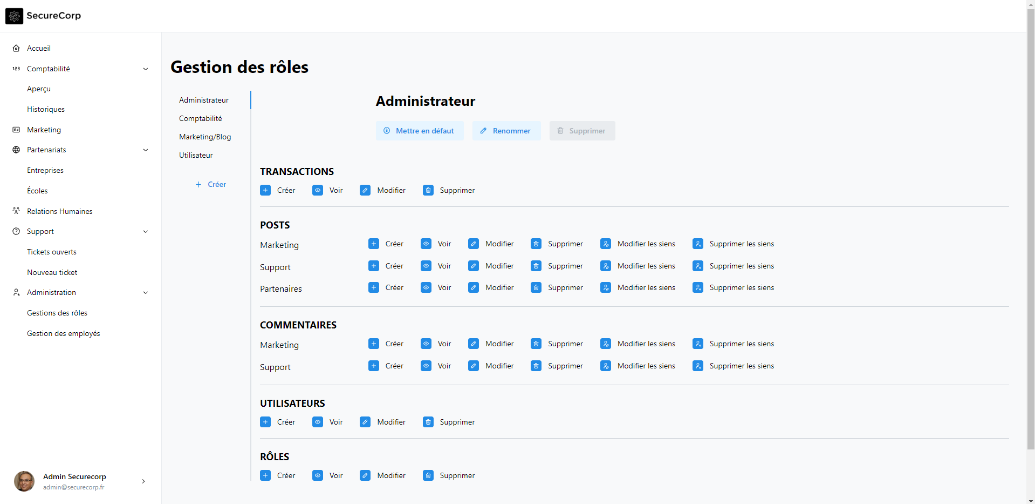




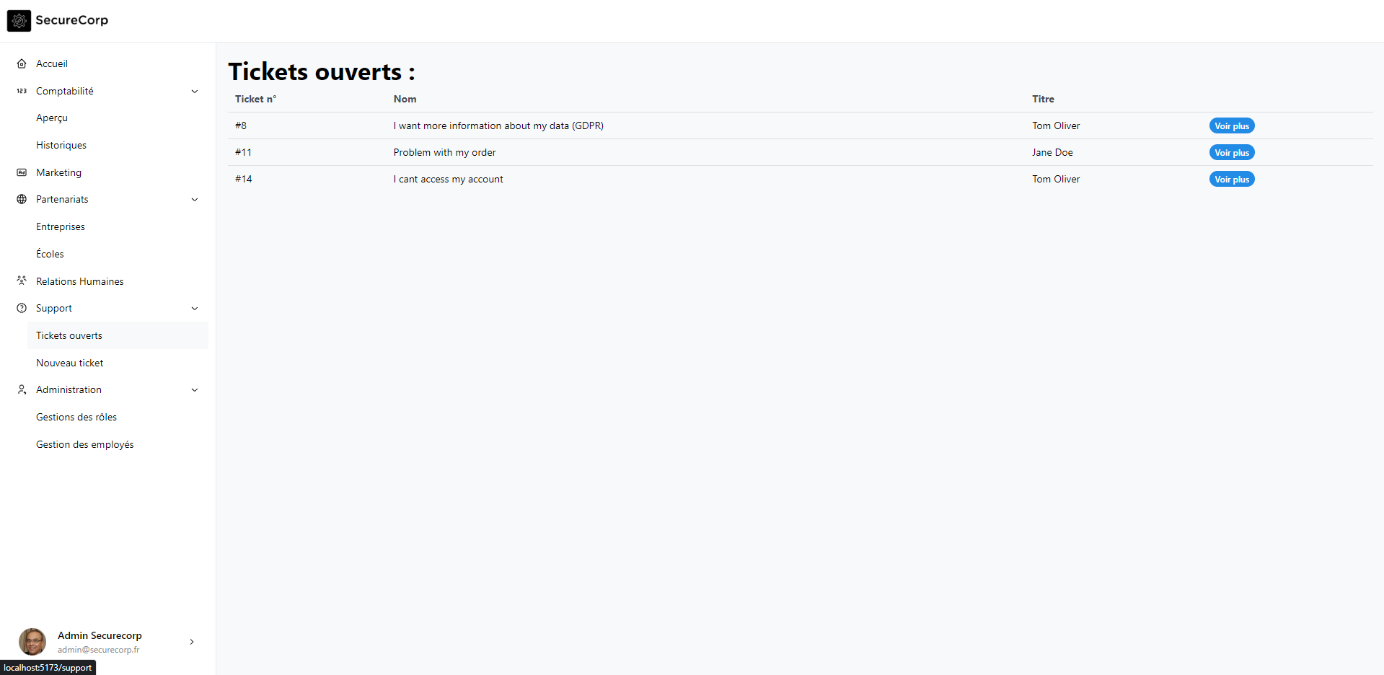
 *Toujours en tant qu’admin la gestion des employés est modifiable*



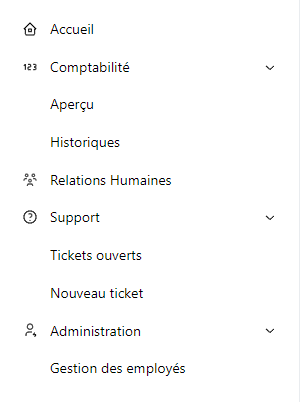
*Le plus important, la Gestion des Rôles*

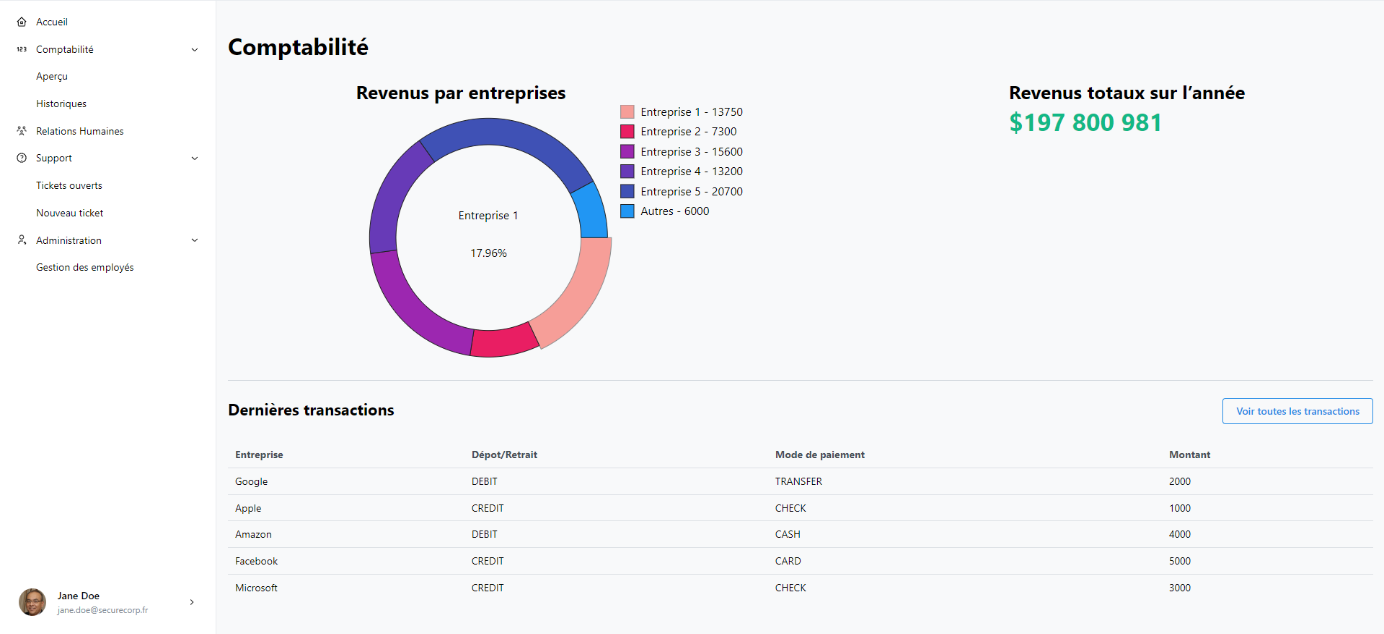






*Pour l’équipe technique nous avons mis en place un system de tickets*





*Maintenant que nous sommes log en tant qu’un utilisateur n’ayant pas les permissions d’édition  
de la page comptabilité nous voyons qu’en effet il ne peut pas modifier la page*

# Conclusion

Finalement, notre projet de conception et de mise en place d'un système de contrôle d'accès basé sur les rôles pour l'intranet de SecureCorp a pour objectif d'améliorer l'expérience utilisateur et de renforcer la sécurité des données et des informations. Grâce à la mise en œuvre du RBAC, nous permettons une gestion plus centralisée des autorisations d'accès en attribuant des permissions aux rôles plutôt qu'aux utilisateurs individuels.

Notre solution propose un redesign de l'interface utilisateur de l'intranet, offrant une expérience conviviale, intuitive et ergonomique pour les employés. Nous avons développé un système RBAC flexible, modifiable et évolutif, qui permet de créer des rôles prédéfinis et de personnaliser les permissions en fonction des besoins spécifiques de chaque département ou projet.

De plus, nous avons mis en place un mécanisme de gestion des utilisateurs facilitant l'attribution des rôles et l'ajout/suppression des utilisateurs du système. La sécurité des données et des informations sensibles est garantie grâce à des mesures de sécurité robustes conformes aux normes en vigueur.

Malgré les contraintes temporelles et les ressources limitées, notre équipe a utilisé des méthodes de gestion efficaces pour assurer le suivi et la production du projet. Les différentes méthodes de travail en groupe vus en cours de méthodologie nous ont été très utiles. Nous avons utilisé des technologies telles que ReactJS, Vite, PostgreSQL, Express.js et Prisma pour développer notre solution. Nous avons donc tous pu améliorer nos compétences techniques et en apprendre plus sur le RBAC. C’était un projet très intéressant qui nous apporté énormément car nous avons pu améliorer notre esprit d’équipe.

En somme, notre projet répond aux besoins de SecureCorp en fournissant une solution RBAC complète et adaptée à leur intranet d'entreprise. Nous espérons que notre proposition sera retenue et que notre solution contribuera à renforcer la sécurité et la productivité au sein de SecureCorp. Nous aimerions remercier