Royaume du Maroc
Université Sultan MoulaySlimane
Ecole Supérieure de Technologie – Béni Mellal
DépartementInformatique et Techniques de Gestion

Rapport Du Stage D'initiation

Sous le thème :
Conception et développement d'une application web de gestion des incidents de sécurité

Période de stage : du 14/07/2025 au 15/08/2025
Présenté et souten le ....., devant un Jury composé de :

Président :

Président :

Effectué par :
FOULI Mohamed
Lieu du stage : TACHFIR SARL-Rabat
Année universitaire : 2025 - 2026

Encadré par :
Encadrant industriel : Ms Anas Idrissi
Encadrantepédagogique : Pr Siham Bakkouri
Co-Encadrante pédagogique : Pr Loubna El- liazidi

Dédicace

Je tiens tout d'abord à dédier ce travail à mes chers parents, dont le soutien inconditionnel, les sacrifices et l'amour constant ont été pour moi une source précieuse de motivation et d'inspiration tout au long de ce parcours.

À mon frère bien-aimé, je souhaite exprimer ma profonde gratitude pour son soutien moral constant et ses conseils avisés. Ses recommandations ont été un véritable guide, m'aidant à surmonter les obstacles et à tirer le meilleur parti de cette expérience professionnelle.

Je remercie également ma famille élargie pour leur appui continu et leurs encouragements, qui ont toujours été un moteur dans ma progression.

À l'équipe de l'entreprise TACHFIR Sarl IT Services et Consulting, je rends hommage pour leur générosité, leur assistance précieuse et leur expertise, qui ont grandement contribué à l'élaboration de ce rapport. Je leur suis également reconnaissant pour l'opportunité offerte de découvrir le monde professionnel.

À toutes les personnes qui ont partagé avec moi mes moments de joie et mes réussites, et qui ont été présentes à chaque étape de ce parcours, je vous adresse mes sincères remerciements.

À mes amis et collègues, merci pour leur amitié, leur soutien constant et les échanges enrichissants qui ont marqué cette belle aventure.

Enfin, je dédie ce travail à toutes les personnes qui m'ont accompagné durant cette année de formation à l'École Supérieure de Technologie de Beni Mellal (ESTBM), en particulier à nos professeurs distingués, dont les enseignements ont fortement contribué à mon développement académique et professionnel.

Je dédie ce travail avec enthousiasme, gratitude et joie.

Remerciment

Ce travail n'est pas uniquement le fruit de mes efforts personnels, mais également le résultat d'une collaboration et d'un soutien de plusieurs personnes à qui je souhaite exprimer ma profonde reconnaissance.

Je tiens tout particulièrement à remercier mes parents pour leur soutien constant et leurs encouragements indéfectibles, sans lesquels cette réussite n'aurait pas été possible.

Je souhaite également exprimer ma gratitude à mon superviseur, M. Anas Idrissi, pour son accompagnement tout au long de mon stage. Sa disponibilité, ses conseils avisés et son expertise ont été essentiels à mon apprentissage et à mon développement professionnel.

Je remercie aussi chaleureusement l'ensemble des professeurs du département d'informatique de l'École Supérieure de Technologie de Beni Mellal (ESTBM) pour leur soutien académique et leurs encouragements continus.

Enfin, j'adresse mes remerciements à tous les membres de l'administration de l'ESTBM ainsi qu'au personnel de la société TACHFIR Rabat pour leur aide précieuse et leur soutien tout au long de cette année académique et professionnelle.

Je vous suis infiniment reconnaissant à tous pour votre contribution à ma réussite et pour l'accompagnement inestimable que vous m'avez offert.

Merci à vous tous.

Sommaire

Sommaire

Résumée

Ce rapport présente le déroulement d'un projet de conception et de développement d'une application web de gestion des incidents de sécurité. Il décrit l'analyse des besoins, la conception du système, ainsi que les différentes étapes de réalisation et de tests effectuées pour assurer un suivi efficace des incidents.

Ce projet a permis de mettre en pratique et de renforcer des compétences techniques et organisationnelles, tout en développant une compréhension concrète du processus de gestion des incidents de sécurité au sein d'un environnement professionnel.

Introduction Générale

L'informatique occupe aujourd'hui une place prépondérante dans le fonctionnement des entreprises modernes. Elle constitue un pilier essentiel pour la gestion des activités, la communication interne et la sécurisation des données. Dans ce contexte, les menaces informatiques deviennent de plus en plus nombreuses et sophistiquées, obligeant les entreprises à adopter des solutions innovantes pour garantir la sécurité de leurs systèmes d'information.

C'est dans cette optique que s'inscrit mon stage au sein de l'entreprise **TACHFIR SARL** – Rabat, une société spécialisée dans la cybersécurité, la transformation digitale et le conseil en technologies de l'information.

L'objectif de ce stage était de concevoir et développer une application web de gestion des incidents de sécurité, permettant d'automatiser le suivi des incidents signalés, d'en faciliter l'analyse et d'assurer une meilleure réactivité dans la résolution des problèmes.

Ce rapport décrit en détail le déroulement de cette expérience. Il est structuré en plusieurs parties :

- une présentation de l'entreprise d'accueil,
- la description du contexte général du projet,
- l'analyse et la conception du système,
- la phase de réalisation,
- et enfin une conclusion récapitulative des acquis et perspectives.

Chapitre 1 :
Présentation De L’entreprise

1. Présentation générale de TACHFIR SARL:

TACHFIR SARL est une entreprise marocaine basée à Rabat, spécialisée dans les domaines de la cybersécurité, de la transformation digitale, de l'intégration des systèmes informatiques et du conseil en technologies.

Fondée par des experts passionnés du numérique, **TACHFIR** accompagne les entreprises dans la mise en place de solutions sécurisées, performantes et adaptées à leurs besoins spécifiques. Sa mission principale est de renforcer la sécurité informatique des organisations tout en optimisant leurs infrastructures technologiques.

Domaines d'expertise :

- Cybersécurité et audit des systèmes d'information
- Développement et intégration d'applications web et mobiles
- Cloud computing et virtualisation
- Solutions de réseau et infrastructure IT
- Conseil et accompagnement en transformation digitale

L'entreprise se distingue par une approche centrée sur la qualité, l'innovation et la satisfaction du client. Elle combine expertise technique, veille technologique et méthodologie agile pour répondre efficacement aux défis du numérique.

2. Organisation et structure interne

L'entreprise est structurée autour de plusieurs départements complémentaires, chacun jouant un rôle clé dans la réussite des projets et la satisfaction des clients. Cette organisation favorise la collaboration, la réactivité et l'innovation au sein des équipes.

- Département Développement et Intégration
  - Conçoit, développe et intègre des solutions logicielles sur mesure. Assure la qualité, la performance et la conformité des applications livrées.

- Département Cybersécurité et Audit
  - Protège les systèmes d'information grâce à des audits, tests d'intrusion et politiques de sécurité. Veille à la conformité et à la gestion des risques.

- Département Support et Maintenance
  - Assure le suivi post-déploiement des solutions et la résolution des incidents. Garantit la disponibilité, la performance et la satisfaction client.

- Département Réseau et Infrastructure
  - Gère la conception et la maintenance des réseaux et serveurs. Optimise la stabilité, la sécurité et la performance des infrastructures informatiques.

- Département Administration et Gestion
  - Supervise les activités administratives, financières et RH. Veille au bon fonctionnement interne et à la conformité réglementaire de l'entreprise.

L'ensemble de ces départements collabore de manière transversale et coordonnée afin d'assurer la qualité des projets livrés, la conformité aux exigences des clients et la croissance durable de l'entreprise. Cette structure favorise la synergie entre les équipes et une approche globale orientée performance et innovation.

3. Objectifs principaux :

- **Élever les entreprises par la technologie**
  - Tachfir se donne pour mission d'aider ses clients à « élever leur business », en fournissant des solutions technologiques innovantes et sécurisées.

- **Allier innovation et sécurité**
  - L'entreprise affirme que ses services se situent « là où l'innovation rencontre une sécurité impénétrable ».

- **Fournir des services IT complets et sécurisés**
  - Dans leurs services, ils mentionnent l'audit et les tests de pénétration pour évaluer les systèmes, ainsi que le développement web et mobile avec un accent fort sur la sécurité.

- **Mettre à disposition des experts certifiés**
  - Pour atteindre ces objectifs, Tachfir met en avant un « équipe d'experts » disposant de nombreuses certifications (ex. Java, Kubernetes, CyberOps, etc.) pour garantir la qualité et la fiabilité.

- **Garantir la confiance et la tranquillité d'esprit pour les clients**
  - Une part essentielle de leur objectif est de donner aux clients « la liberté de prospérer sans souci », en étant « vos gardiens d'une technologie sans faille et d'une paix d'esprit inégalée ».

Chapitre 2 :
Contexte général du projet

1. Problématique :

Dans un contexte numérique en perpétuelle évolution, les cybermenaces deviennent de plus en plus sophistiquées, fréquentes et difficiles à anticiper. Les entreprises, quelle que soit leur taille, sont désormais confrontées à des risques accrus de failles, d'attaques et d'incidents de sécurité susceptibles d'affecter leurs systèmes d'information, leurs données sensibles et leur réputation.

Face à ces menaces, il est essentiel de mettre en place un système de gestion des incidents de sécurité permettant de détecter rapidement les anomalies, d'enregistrer les événements, de suivre leur évolution et d'y apporter des solutions efficaces. Ce dispositif doit également offrir une traçabilité complète des actions menées et faciliter la communication entre les équipes techniques, les responsables sécurité et la direction.

Cependant, dans de nombreuses organisations, la gestion des incidents reste encore manuelle et non centralisée, souvent réalisée à l'aide de simples fichiers Excel, e-mails ou outils non spécialisés. Cette approche entraîne plusieurs inconvénients majeurs :

- Une perte de temps dans la collecte et le traitement des informations,
- Un manque de cohérence et de traçabilité dans le suivi des incidents,
- Des risques d'erreurs humaines ou d'oubli dans la résolution,
- Une difficulté à générer des rapports fiables pour le pilotage et la conformité réglementaire,
- Une communication fragmentée entre les différents départements concernés.

Pour pallier ces limites, il devient indispensable de développer une application web centralisée dédiée à la gestion automatisée des incidents de sécurité. Cette solution permettra à la société TACHFIR et à ses clients de disposer d'un outil performant, intuitif et sécurisé pour :

- Enregistrer et classifier les incidents en temps réel,
- Attribuer les tâches aux responsables concernés,
- Suivre l'évolution du traitement jusqu'à la résolution complète,
- Analyser et documenter les causes et les impacts,
- Générer des rapports statistiques pour l'amélioration continue du dispositif de sécurité.

Un tel système contribuera non seulement à renforcer la posture de cybersécurité de TACHFIR et de ses partenaires, mais aussi à améliorer la réactivité, la transparence et l'efficacité opérationnelle face aux menaces numériques actuelles et futures.

1. Problématique :

Dans un contexte numérique en perpétuelle évolution, les cybermenaces deviennent de plus en plus sophistiquées, fréquentes et difficiles à anticiper. Les entreprises, quelle que soit leur taille, sont désormais confrontées à des risques accrus de failles, d'attaques et d'incidents de sécurité susceptibles d'affecter leurs systèmes d'information, leurs données sensibles et leur réputation.

Face à ces menaces, il est essentiel de mettre en place un système de gestion des incidents de sécurité permettant de détecter rapidement les anomalies, d'enregistrer les événements, de suivre leur évolution et d'y apporter des solutions efficaces. Ce dispositif doit également offrir une traçabilité complète des actions menées et faciliter la communication entre les équipes techniques, les responsables sécurité et la direction.

Cependant, dans de nombreuses organisations, la gestion des incidents reste encore manuelle et non centralisée, souvent réalisée à l'aide de simples fichiers Excel, e-mails ou outils non spécialisés. Cette approche entraîne plusieurs inconvénients majeurs :

- Une perte de temps dans la collecte et le traitement des informations,
- Un manque de cohérence et de traçabilité dans le suivi des incidents,
- Des risques d'erreurs humaines ou d'oubli dans la résolution,
- Une difficulté à générer des rapports fiables pour le pilotage et la conformité réglementaire,
- Une communication fragmentée entre les différents départements concernés.

Pour pallier ces limites, il devient indispensable de développer une application web centralisée dédiée à la gestion automatisée des incidents de sécurité. Cette solution permettra à la société TACHFIR et à ses clients de disposer d'un outil performant, intuitif et sécurisé pour :

- Enregistrer et classifier les incidents en temps réel,
- Attribuer les tâches aux responsables concernés,
- Suivre l'évolution du traitement jusqu'à la résolution complète,
- Analyser et documenter les causes et les impacts,
- Générer des rapports statistiques pour l'amélioration continue du dispositif de sécurité.

Un tel système contribuera non seulement à renforcer la posture de cybersécurité de TACHFIR et de ses partenaires, mais aussi à améliorer la réactivité, la transparence et l'efficacité opérationnelle face aux menaces numériques actuelles et futures.

2. Objectifs du projet :

Le présent projet a pour objectif principal de concevoir et développer une application web centralisée dédiée à la gestion des incidents de sécurité informatique au sein de TACHFIR et de ses clients. Cette solution vise à automatiser et à optimiser le processus de traitement des incidents, tout en garantissant la traçabilité, la réactivité et la sécurité des données.

- Objectif général :

Mettre en place une plateforme web intégrée permettant de détecter, enregistrer, suivre et résoudre efficacement les incidents de sécurité, tout en assurant une centralisation des informations et une meilleure coordination entre les équipes techniques et décisionnelles.

- Objectifs spécifiques :
- Automatiser la gestion des incidents afin de réduire les interventions manuelles et les risques d'erreur.
- Assurer la traçabilité complète des actions effectuées sur chaque incident, depuis la détection jusqu'à la clôture.
- Faciliter la communication et la collaboration entre les différents départements impliqués (cybersécurité, support, réseau, etc.).
- Mettre en place un système de notifications et d'alertes en temps réel pour améliorer la réactivité face aux incidents.
- Fournir des tableaux de bord et rapports statistiques permettant une analyse approfondie et un suivi des performances en matière de sécurité.
- Garantir la confidentialité, l'intégrité et la disponibilité des données traitées au sein de la plateforme.
- Améliorer la qualité du service offert par TACHFIR à ses clients en renforçant la fiabilité et la transparence du suivi des incidents.
- Offrir une interface ergonomique et intuitive facilitant la prise en main et l'utilisation quotidienne de l'outil par les utilisateurs.

3. Méthodologie de travail :

La réalisation de ce projet a suivi une approche méthodologique rigoureuse permettant d'assurer la qualité, la cohérence et la réussite de l'application développée. La démarche adoptée s'articule autour de plusieurs étapes clés, allant de l'analyse des besoins à la mise en œuvre finale de la solution.

- *Étude préliminaire et analyse des besoins :*

Cette première phase a consisté à comprendre le contexte du projet et à identifier précisément les besoins de l'entreprise TACHFIR et de ses clients en matière de gestion des incidents de sécurité.
Les principales actions menées à cette étape sont :

  - L'analyse du fonctionnement actuel de la gestion des incidents (processus manuel, outils utilisés, limites constatées).
  - La collecte des besoins auprès des responsables techniques et de la direction sécurité.
  - La définition des objectifs fonctionnels et techniques du futur système.

- *Conception fonctionnelle et technique :*

Après l'analyse, une modélisation du système a été réalisée afin de définir la structure et le fonctionnement de l'application.
Cette étape a permis de :

  - Élaborer les diagrammes UML (cas d'utilisation, séquences, classes).
  - Définir l'architecture logicielle de la solution (front-end, back-end, base de données).
  - Choisir les technologies adaptées (frameworks, langages, outils de sécurité, etc.).

- *Développement et intégration :*

Le développement a été mené de manière itérative et agile, permettant d'avancer par étapes et de valider progressivement les fonctionnalités.
Les tâches principales ont été :

  - La création de la base de données et des modèles de données.
  - Le développement des modules (gestion des incidents, utilisateurs, notifications, rapports).
  - L'intégration entre les différentes couches de l'application.
  - La mise en place des mécanismes de sécurité (authentification, gestion des rôles, protection des données).

- *Tests et validation :*

Une série de tests unitaires, fonctionnels et de performance a été effectuée afin de garantir la fiabilité et la conformité du système.
Ces tests ont permis de :

  - Vérifier le bon fonctionnement de chaque module.
  - Détecter et corriger les anomalies.
  - Évaluer la stabilité, la sécurité et la convivialité de l'application.

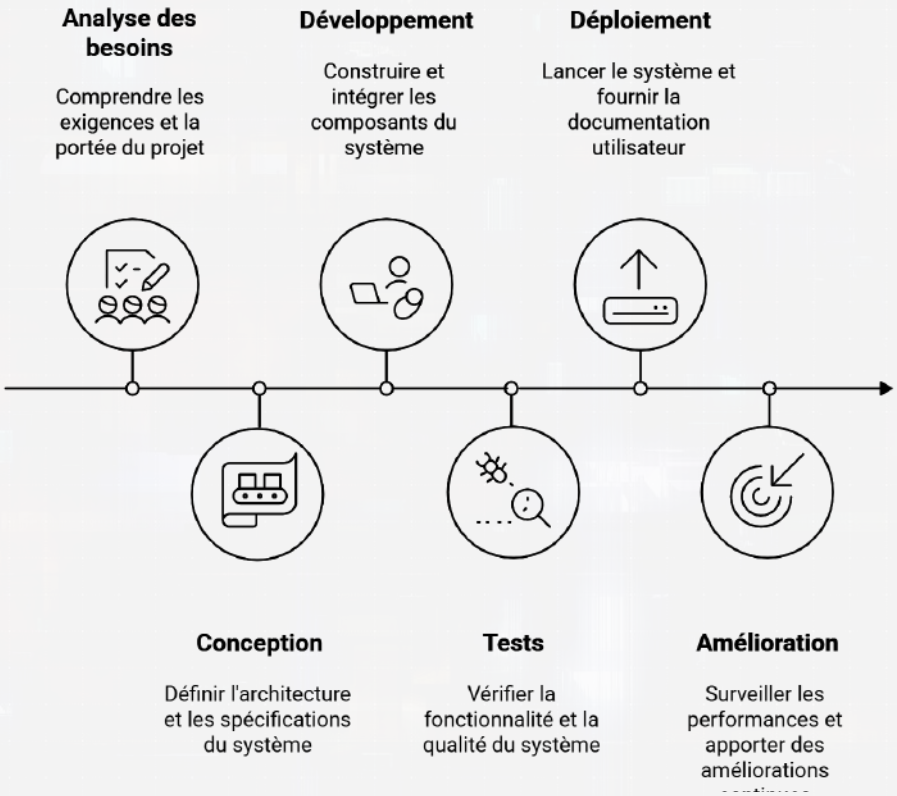
- *Déploiement et documentation :*

Une fois validée, l'application a été déployée dans un environnement contrôlé.
Les actions principales de cette phase incluent :

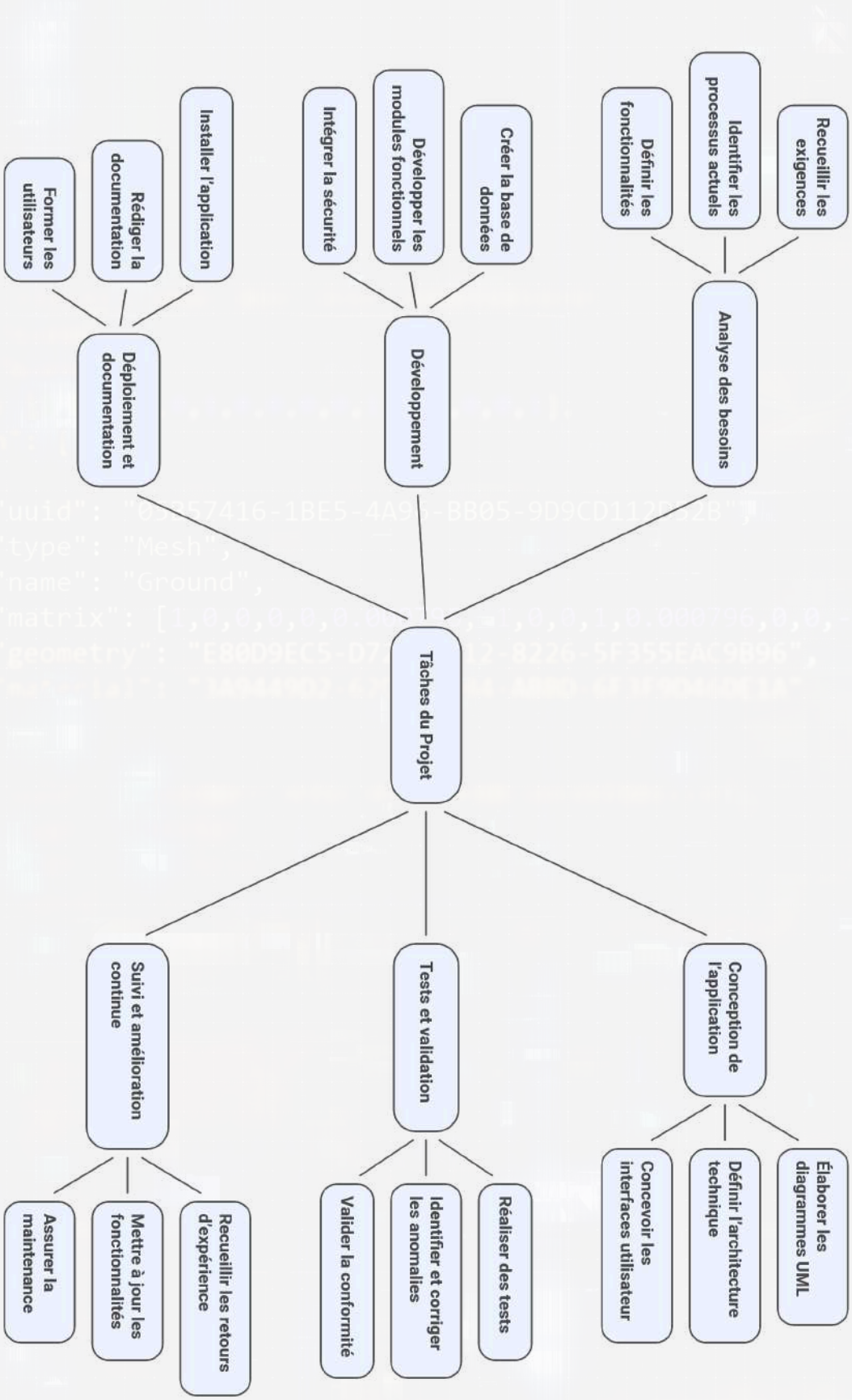
  - Le déploiement sur un serveur web interne ou cloud.
  - La rédaction de la documentation technique et utilisateur.
  - La formation des utilisateurs pour une prise en main rapide et efficace.

- *Suivi et amélioration continue :*

Après la mise en production, un suivi régulier est assuré afin de recueillir les retours d'expérience et d'apporter les améliorations nécessaires.
Cette phase permet d'optimiser les performances, d'ajouter de nouvelles fonctionnalités et de maintenir la sécurité du système à jour.



5. Tâches du projet



Chapitre 3 :
Analyse et Conception

1. Analyse du système :

1.1 Objectif général :

- Mettre en place une application web centralisée permettant :
- D'enregistrer les incidents de sécurité détectés,
- De suivre leur traitement et résolution,
- D'assurer la traçabilité des actions,
- Et de fournir des rapports statistiques pour le pilotage de la sécurité.

2.1 Acteurs du système :

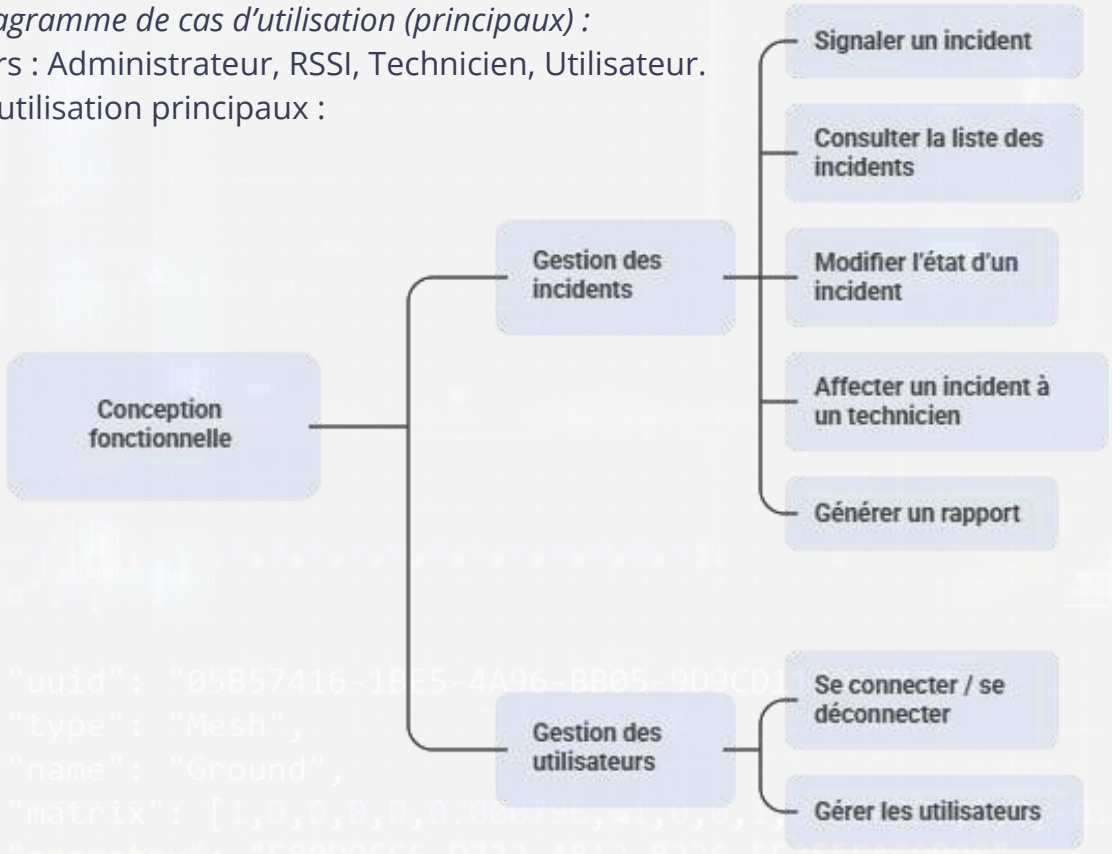
Acteur	Rôle
Administrateur	Gère les utilisateurs, les rôles, et supervise l'ensemble des incidents.
Responsable Sécurité (RSSI)	Analyse les incidents, attribue les tâches, valide la résolution.
Technicien	Traite les incidents qui lui sont attribués.
Utilisateur / Client	Signale un incident et consulte son état d'avancement.

3.1 Fonctionnalités principales :

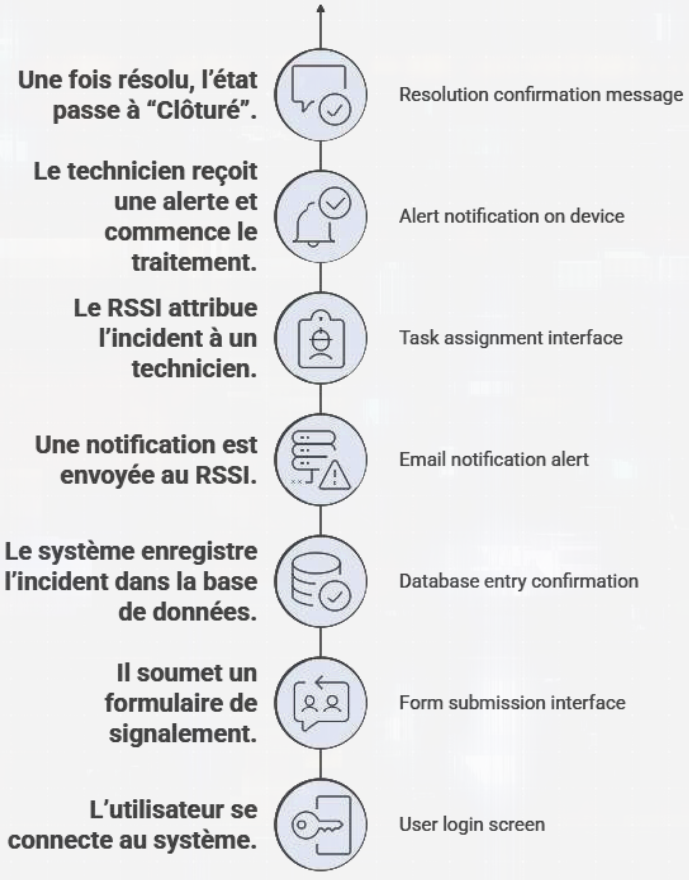
- *Gestion des incidents : création, classification, suivi, mise à jour, clôture.*
- *Affectation automatique ou manuelle des incidents aux techniciens.*
- *Système de notifications (email ou interne) lors de nouvelles affectations ou mises à jour.*
- *Tableaux de bord et statistiques : nombre d'incidents ouverts, temps moyen de résolution, type d'incidents les plus fréquents, etc.*
- *Gestion des utilisateurs et rôles : création, suppression, droits d'accès.*
- *Authentification sécurisée et gestion de session.*

2. Conception fonctionnelle (UML) :

1.2 Diagramme de cas d'utilisation (principaux) :
Acteurs : Administrateur, RSSI, Technicien, Utilisateur.
Cas d'utilisation principaux :

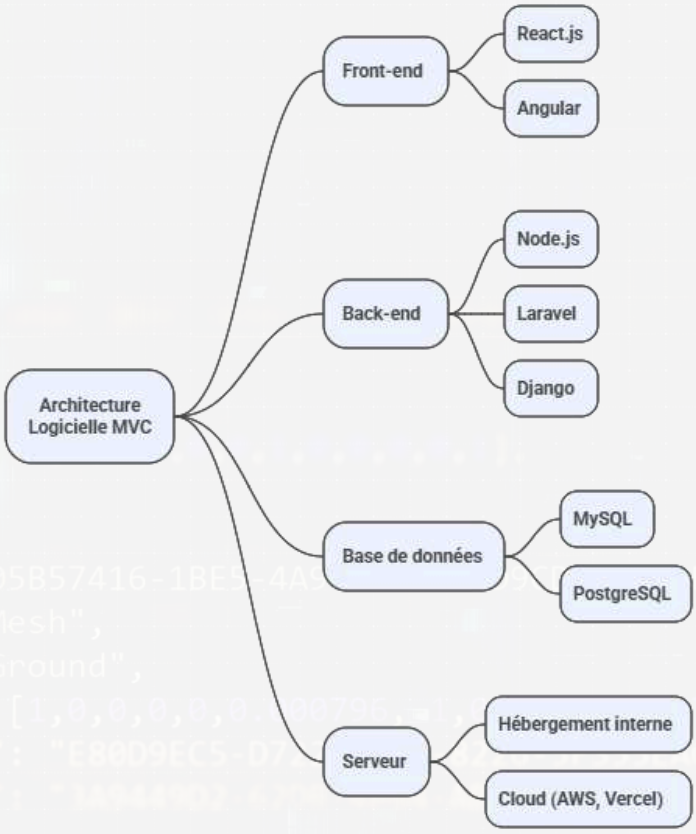


2.2 Diagramme de séquence (exemple : signalement d'un incident)



3. Conception technique :

3.1 *Architecture logicielle :*
Architecture MVC (Modèle – Vue – Contrôleur) :



3.2 Modèle conceptuel de données (MCD) :
Entités principales :

Entité	Attributs	Relations
Utilisateur	id, nom, email, mot_de_passe, rôle	1–N avec Incident
Incident	id, titre, description, priorité, statut, date_ouverture, date_clôture	N–1 avec Utilisateur, N–1 avec Technicien
Technicien	id, nom, spécialité, email	1–N avec Incident
Notification	id, message, date, type	N–1 avec Utilisateur
Rapport	id, période, contenu, auteur	N–1 avec RSSI

3.3 Contraintes et sécurité :

- Authentification JWT / Session sécurisée
- Hashage des mots de passe (bcrypt)
- Validation des formulaires côté client et serveur
- Gestion des rôles et autorisations
- Sauvegarde automatique de la base de données

3.4 Interface utilisateur (maquette fonctionnelle) :

- Page d'accueil : tableau de bord des incidents
- Page signalement : formulaire d'ajout d'incident
- Page de gestion : liste filtrable des incidents
- Page statistiques : graphiques et rapports
- Page d'administration : gestion des comptes utilisateurs

4. Résultat attendu :

Une application :

- Sécurisée et ergonomique
- Assurant la traçabilité complète des incidents
- Facilitant la collaboration entre les départements techniques
- Permettant une analyse statistique claire de la sécurité

Chapitre 4 :
Réalisation du Projet

1. Introduction :

Après l'étape d'analyse et de conception, la phase de réalisation a consisté à mettre en œuvre l'ensemble des fonctionnalités définies lors de la conception fonctionnelle et technique.

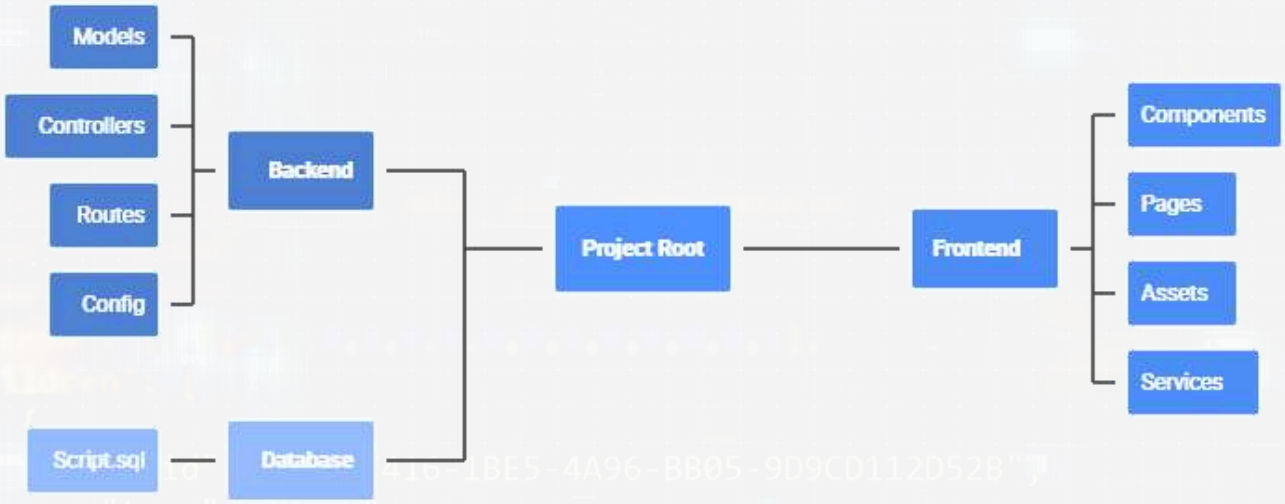
L'objectif principal de cette phase était de développer une application web complète, sécurisée et intuitive, permettant la gestion centralisée des incidents de sécurité au sein de l'entreprise TACHFIR SARL.

2. Environnement de développement

Composant	Outil / Technologie utilisée	Rôle
Langage côté client (Front-end)	HTML5, CSS3, JavaScript / React.js	Conception de l'interface utilisateur dynamique et réactive
Langage côté serveur (Back-end)	PHP / Laravel *(ou Node.js selon le choix)*	Gestion de la logique métier et de la communication avec la base de données
Base de données	MySQL	Stockage des incidents, utilisateurs et notifications
Serveur web	Apache / Nginx	Hébergement de l'application
Outil de versionnement	Git & GitHub	Suivi des versions et travail collaboratif
IDE / Éditeur	Visual Studio Code	Écriture et débogage du code
Outils de sécurité	JWT, bcrypt, HTTPS	Authentification et chiffrement des données

3. Structure générale du projet :

L'application repose sur une architecture MVC (Modèle - Vue - Contrôleur), garantissant une séparation claire entre la logique métier, les données et la présentation.



4. Principales interfaces développées :

a. Page de connexion :

- Authentifie les utilisateurs selon leur rôle (Administrateur, Technicien, RSSI, Client).
- Vérifie les identifiants via la base de données.
- Redirige vers le tableau de bord correspondant.

b. Tableau de bord :

- Présente une vue globale du nombre d'incidents : ouverts, en cours, résolus.
- Affiche des graphiques statistiques sur les incidents par type, priorité ou responsable.

c. Gestion des incidents :

- Formulaire d'ajout d'un nouvel incident (titre, description, priorité, pièce jointe, etc.).
- Liste dynamique avec filtres (par statut, date ou technicien).
- Boutons d'actions : modifier, clôturer, supprimer.
- Historique des actions effectuées sur chaque incident.

d. Gestion des utilisateurs :

- Permet à l'administrateur d'ajouter, modifier ou supprimer un compte.
- Attribution de rôles et gestion des permissions.
- Réinitialisation de mot de passe sécurisée.

e. Système de notifications :

- Alertes automatiques lors d'un nouvel incident ou changement d'état.
- Envoi d'e-mails ou notifications internes.

f. Rapports et statistiques :

- Génération de rapports PDF sur les incidents traités.
- Visualisation graphique via chart.js (barres, camemberts, etc.).
- Exportation des données pour l'analyse.

5. Mécanismes de sécurité intégrés :

- Authentification par JSON Web Token (JWT).
- Hashage des mots de passe avec bcrypt.
- Validation des formulaires côté serveur et client.
- Accès restreint selon le rôle de l'utilisateur.
- Sauvegardes automatiques de la base de données.
- Utilisation du protocole HTTPS pour le chiffrement des communications.

6. Tests et validation :

Des tests unitaires et fonctionnels ont été réalisés afin d'assurer :

- Le bon fonctionnement de chaque module.
- L'intégrité des données échangées entre client et serveur.
- La sécurité de l'accès et la gestion correcte des rôles.
- La rapidité de chargement et la compatibilité avec plusieurs navigateurs.

Résultat :
Les tests se sont révélés concluants. L'application répond aux besoins fonctionnels exprimés et garantit une gestion fluide, rapide et sécurisée des incidents.

7. Déploiement :

L'application a été déployée sur un serveur de test interne de TACHFIR.
Le déploiement comprend :

- Configuration du serveur Apache / Nginx.
- Importation de la base de données MySQL.
- Définition des variables d'environnement (clé JWT, mot de passe DB).
- Test du fonctionnement global sur le réseau interne.

8. **Conclusion de la réalisation :**

Cette phase a permis de concrétiser la solution proposée lors de l'analyse et de la conception.

L'application développée permet désormais :

- Un suivi centralisé et automatisé des incidents,
- Une communication fluide entre les équipes techniques,
- Et une meilleure visibilité sur la performance du service de sécurité.

Le projet a ainsi contribué à renforcer la posture de cybersécurité de **TACHFIR** tout en apportant une valeur ajoutée opérationnelle à son service technique.

Conclusion Générale

Au terme de ce stage au sein de l'entreprise TACHFIR SARL IT Services & Consulting, cette expérience a représenté une étape essentielle dans mon parcours de formation et dans mon développement professionnel. Elle m'a permis de confronter mes connaissances théoriques acquises à l'École Supérieure de Technologie de Béni Mellal à la réalité du monde professionnel, et d'enrichir mes compétences techniques, méthodologiques et relationnelles.

L'objectif principal de ce projet était la conception et le développement d'une application web de gestion des incidents de sécurité, un outil visant à automatiser le processus de traitement, de suivi et de résolution des incidents informatiques.

Grâce à une démarche rigoureuse d'analyse, de conception et de réalisation, cette solution a permis de répondre efficacement aux besoins identifiés, tout en assurant la traçabilité, la fiabilité et la sécurité des informations traitées.

Sur le plan technique, ce stage m'a offert l'opportunité de manipuler différentes technologies du développement web, d'approfondir mes connaissances en programmation orientée objet, en modélisation UML, en base de données relationnelle, et d'appliquer des principes de sécurité informatique indispensables dans le contexte actuel de la cybersécurité.

Sur le plan humain, il m'a permis de m'intégrer dans une équipe professionnelle, d'apprendre à collaborer efficacement, à gérer le temps et à m'adapter aux contraintes réelles d'un projet informatique.

L'application développée constitue ainsi une valeur ajoutée tangible pour l'entreprise TACHFIR, en contribuant à améliorer la réactivité et la qualité du suivi des incidents. Elle représente également un aboutissement concret des compétences acquises durant ma formation.

Enfin, ce stage m'a conforté dans mon choix d'orientation vers le domaine de l'ingénierie logicielle et de la cybersécurité, un secteur à fort potentiel d'évolution et d'innovation.

Il marque pour moi le point de départ d'une carrière que je souhaite poursuivre avec passion, rigueur et curiosité, tout en continuant à développer mes compétences techniques et professionnelles.