REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie
Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Filière : Télécommunications
***Spécialité : R**éseaux et **T**élécommunications*

Thème :

Conception d'un système de protection des données sensibles

Soutenu le
04 / 07 /2023

Réalisé par :

GHARNAOUT Riham

KADER Imène

Devant le jury composé de :

Président : M^me^ HAROUN
Examinateur: Mr AKLIOUT
Encadreur: M^me^ MECHID Samira

Année Universitaire : 2022/2023

REMERCIEMENTS

Nous remercions en premier lieu Dieu tout puissant qui nous a dotés d'une grande volonté et d'un savoir adéquat pour mener à terme notre projet.

Avant de commencer la présentation de ce rapport, nous profitons de l'occasion pour remercier du fond du cœur toute personne qui a contribué de près ou de loin à la réalisation de ce travail.

Notre profonde gratitude et nos sincères remerciements à notre encadreur, en l'occurrence **Mme MECHID Samira**, pour avoir accepté de nous encadrer et pour l'intérêt qu'elle a porté à notre travail, son suivi, sa disponibilité et ses conseils et orientations.

Nos remerciements à **Mr. Hichem BENZAOUI** qui nous a insisté de faire ce choix de recherche, a été plus qu'un maître de stage, il nous a guidés, critiqués, fait des suggestions. Son encouragement permanent et son dynamisme organisateur nous ont énormément facilité la tâche. Nous lui remercions vivement pour tout.

Nous tenons à remercier **Mr. Khaled KHENOUF**, il nous a guidés, conseillés tout au long de notre stage, pour l'intérêt qu'il a porté à notre travail, son suivi, sa disponibilité et ses conseils et orientations.

Chers parents. Nous tenons à exprimer notre profonde gratitude et nos sincères remerciements pour tout ce que vous avez fait pour nous.

À tous nos enseignants et membres du département informatique de l'université **M'HAMED BOUGARA-BOUMERDES**.

DÉDICACES

Du profond de mon cœur, je dédie ce travail à tous ceux qui me sont chers,

À l'âme de ma chère grand-mère,

À toi, à qui il est impossible de t'oublier,

A MA CHERE MERE

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être.

Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours, mon adorable mère **Saida** .

A MON CHEER PÉRE,

Qui n'ont jamais cessé, de formuler des prières à mon égard, de me soutenir et de m'épauler pour que je puisse atteindre mes objectifs, mon cher père **Said**.

Que ce modeste travail soit l'exaucement de vos vœux tant formulés.

A mes chères sœurs (Maissa, Maria, Youssra) qui n'ont pas cessé de me conseiller, encourager et soutenir tout au long de mes études. Que Dieu les protège et leur offre la chance et le bonheur.

Ma chère tante Hassiba, merci pour votre amour et votre soutien continu. Merci d'être toujours à mes côtés, vous, votre mari et vos enfants (Aya, Khouloud, Adem).

Imad, je tiens à exprimer toute ma gratitude envers vous pour votre patience, votre assistance morale et vos précieux conseils. Merci du fond du cœur pour tout ce que vous avez fait pour moi. Votre présence et votre soutien sont d'une valeur inestimable.

A tous les cousins, les voisins et les amis(Sally, Lynda ,Yamina , Thanina, Ilham, Rym) que j'ai connu jusqu'à maintenant.

Merci pour leurs amours et leurs encouragements.

Sans oublier mon binôme Riham pour son soutien moral, sa patience et sa compréhension tout au long de ce projet.

A tous ceux que j'aime, Merci !

IMENE KADER

DÉDICACES

Je dédie ce travail :

A la femme qui a souffert sans me laisser souffrir, qui n'a jamais dit non à mes exigences et qui n'a épargné aucun effort pour me rendre heureuse tu es l'essence même de l'amour maternel, une source infinie de tendresse et de compassion. Je suis bénie de t'avoir comme mère, et je te remercie du fond du cœur pour tout ce que tu as fait et continues de faire pour moi. Avec tout mon amour, ma reconnaissance éternelle mon adorable mère Nora .

A l'homme mon précieux offre du dieu qui doit ma vie ma réussite et tout mon respect je t'exprime encore une fois toute ma reconnaissance pour tout ce que tu as fait pour moi. Ton amour, ton soutien inconditionnel et ta foi en moi sont des trésors inestimables. Je suis profondément reconnaissant de t'avoir comme père et mentor. : mon cher père Rezki .

À mes chères sœurs Aya, Amina, Rahma, ainsi qu'à mes cousines Maroua, Lilia, Menel, Hadjer, Ikram et Azhar, qui n'ont jamais cessé de me conseiller, d'encourager et de soutenir tout au long de mes études. Que Dieu les protège et leur offre la chance et le bonheur qu'elles méritent.

À mes grand- père, mes oncles Boubaker Mohamed et mes tantes que dieu leur donne une longue et joueuse vie.

À ma tante Zohra, merci infiniment pour tes encouragements constants. Ta présence bienveillante et tes paroles encourageantes ont été une source de motivation tout au long de ce projet.

À tous les voisins Meriem Zahra Kahina et mes amis Lynda Bouchra Ilham Thanina Rym Yamina ainsi les amis que j'ai connu jusqu'à maintenant. Merci pour leur amour et leurs encouragements.

Sans oublier mon binôme, Kader Imène, pour leur soutien moral, leur patience et leur compréhension tout au long de ce projet. Votre collaboration précieuse a été essentielle pour surmonter les défis et atteindre nos objectifs communs. Votre engagement et votre dévouement ont contribué à la réussite de notre travail. Cette dédicace est une reconnaissance sincère de notre partenariat et de notre amitié.

Gharnaout Riham

RÉSUMÉ

Ce mémoire se concentre sur la conception d'un système de protection des données sensibles au sein de Sonatrach, l'une des principales entreprises du secteur de l'énergie. Avec la prolifération croissante des attaques informatiques sophistiquées et les risques associés à la sécurité des systèmes d'information, il est devenu essentiel pour les organisations de renforcer leurs mesures de sécurité et de protéger leurs données sensibles.

La recherche effectuée repose sur une méthodologie rigoureuse qui comprend une analyse approfondie de Sonatrach, ainsi qu'une revue de la littérature sur la sécurité informatique et la protection des données sensibles. L'objectif principal est de concevoir un système de protection adapté aux besoins spécifiques de Sonatrach, tout en tenant compte des défis actuels en matière de sécurité.

Ce travail vise à contribuer à l'amélioration de la sécurité informatique et à la protection des données sensibles au sein de Sonatrach. Les résultats et les recommandations de cette étude fournissent des bases solides pour la mise en place d'un système de protection efficace, permettant à Sonatrach de faire face aux menaces émergentes et d'assurer la sécurité de ses données sensibles.

Mots clés : Attaque, Protection , Donnée sensible ,conception , sécurité informatique .

ABSTRACT

This dissertation focuses on the design of a sensitive data protection system within Sonatrach, one of the leading companies in the energy sector. With the increasing proliferation of sophisticated cyber attacks and the associated risks to information security, it has become essential for organizations to strengthen their security measures and protect their sensitive data.

The research conducted is based on a rigorous methodology that includes an in-depth analysis of Sonatrach, as well as a review of the literature on computer security and the protection of sensitive data. The main objective is to design a protection system that is tailored to the specific needs of Sonatrach, while taking into account current security challenges.

This work aims to contribute to the improvement of computer security and the protection of sensitive data within Sonatrach. The findings and recommendations of this study provide a solid foundation for the implementation of an effective protection system, enabling Sonatrach to address emerging threats and ensure the security of its sensitive data.

Keywords: Attack, Protection, Sensitive Data, Design, Cybersecurity .

ملخص

هذه المذكرة تركز على تصميم نظام لحماية البيانات الحساسة داخل سوناطراك، واحدة من الشركات الرائدة في قطاع الطاقة .مع تزايد انتشار الهجمات الإلكترونية المتطورة والمخاطر المرتبطة بأمن أنظمة المعلومات، أصبح من الضروري على المؤسسات تعزيز تدابير الأمان وحماية بياناتها الحساسة.

تعتمد البحث المجرى على منهجية صارمة تتضمن تحليلًا معمقًا لسوناطراك، بالإضافة إلى مراجعة الأدبيات المتعلقة بأمن الحواسيب وحماية البيانات الحساسة .الهدف الرئيسي هو تصميم نظام حماية يتناسب مع الاحتياجات الخاصة لسوناطراك، مع مراعاة التحديات الحالية في مجال الأمن.

يهدف هذا العمل إلى المساهمة في تحسين أمان الحواسيب وحماية البيانات الحساسة داخل سوناطراك .توفر نتائج وتوصيات هذه الدراسة أساسًا قويًا لتنفيذ نظام حماية فعال، مما يمكّن سوناطراك من مواجهة التهديدات الناشئة وضمان أمان بياناتها الحساسة.

الكلمات الرئيسية: الهجوم، الحماية، البيانات الحساسة، التصميم، أمن تكنولوجيا المعلومات.

Table de matières

CHAPITRE II : Généralité sur la sécurité d'un système d'information

CHAPITRE III : Analyse et Conception

CHAPITRE IV: Réalisations.

Liste des figures

Liste des tableaux

Liste des abréviations

A:

AD: Active Directory.

ARP: Address Resolution Protocol.

B:

BDD: Base de Données.

C:

CPU: Central Processing Unit.

CSS: Cascading Style Sheets.

D:

DDoS: Distributed Denial of Service.

DHCP: Dynamic Host Configuration Protocol.

DNS: Domain Name System.

G :

GRH : Gestion des Ressources Humaines.

H:

HTTP: Hypertext Transfer Protocol.

HTML: Hypertext Markup Language.

I:

IDS: Intrusion Detection System.

IP: Internet Protocol.

IPsec: Internet Protocol Security.

L:

LAN: Local Area Network.

M:

MYSQL: My Structured Query Language.

P:

PKI : Public Key Infrastructure.

PHP: Hypertext Preprocessor.

R :

RGPD : Règlement Général sur la Protection des Données.

S:

SCP: Secure Copy.

SFTP: Secure File Transfer Protocol.

SI : Système d'Information.

SQL : Structured Query Language.

SSH : Secure Shell (coquille sécurisée).

SSI: Server Side Includes.

SSL: Secure Sockets Layer.

T:

TCP: Transmission Control Protocol.

TCP/IP: Transmission Control Protocol/Internet Protocol.

TI: Traitement de l'Information.

TLS: Transport Layer Security.

U:

UDP: User Datagram Protocol.

URL: Uniform Resource Locator.

W:

WLAN: Wireless Local Area Network.

X:

XSS: Cross-Site Scripting.

INTRODUCTION GÉNÉRALE

De nos jours, les attaques contre les systèmes d'information se multiplient, avec une sophistication croissante, une puissance accrue et une intelligence plus développée, engendrant des dommages considérables. Malheureusement, la majorité de ces attaques sont nouvelles et échappent au radar des systèmes de protection, nécessitant souvent des interventions complexes et coûteuses pour la remise en état et la maintenance après l'attaque. Les organisations sont confrontées à un défi constant pour faire face à ces menaces émergentes et s'adapter rapidement aux tactiques changeantes des attaquants. La sécurité des systèmes d'information est devenue une priorité absolue pour les entreprises et les gouvernements, nécessitant une vigilance constante et des investissements significatifs dans des solutions de cybersécurité efficaces.

La nécessité de mener cette recherche découle de l'importance croissante de la sécurité informatique dans les entreprises et les particuliers connectés à Internet. De nos jours, la protection des données sensibles est devenue une préoccupation majeure, notamment pour les organisations qui gèrent des informations sensibles et confidentielles. Cette évolution rapide a suscité l'intérêt des chercheurs et des professionnels pour comprendre les concepts de base de la sécurité informatique, les mécanismes de sécurité, ainsi que les méthodes et les outils de protection des données sensibles.

Notre objectif principal dans ce mémoire est donc de concevoir un système de protection des données sensibles adapté aux besoins spécifiques de Sonatrach. Pour atteindre cet objectif, nous avons adopté une approche méthodologique rigoureuse, basée sur l'analyse approfondie de l'organisme d'accueil, la revue de littérature sur la sécurité informatique et la protection des données sensibles, ainsi que la modélisation et la conception à l'aide d'UML.

Au terme de notre recherche approfondie sur la sécurité informatique et la protection des données sensibles dans un environnement organisationnel complexe, nous avons développé une application dédiée à la protection des données sensibles au sein du Département Technologie de l'Information de Sonatrach.

Cette application a été conçue dans le but de renforcer les mesures de sécurité et de confidentialité des données sensibles au sein de l'entreprise (D-LAB)

Dans le premier chapitre intitulé « Présentation de l'organisme d'accueil et étude de l'existant », nous présenterons en détail l'organisme d'accueil, le Département Technologie de l'Information de la division LAB (D-LAB) de Sonatrach, en mettant en lumière tous les éléments et entités qui concourent à son fonctionnement.

Le deuxième chapitre, « Généralités sur la sécurité d'un système d'information », sera consacré à la revue de littérature sur la sécurité informatique. Nous aborderons les concepts de base de

la sécurité, la protection des données sensibles et les objectifs de la sécurité, tout en explorant les mécanismes de sécurité, les services de sécurité et les types d'attaques les plus courantes.
Dans le troisième chapitre intitulé « Analyse et Conception », nous analyserons les objectifs du projet et les exigences fonctionnelles spécifiques à la conception du système de protection des données sensibles. Nous utiliserons également UML pour modéliser et concevoir différentes perspectives du système.
Enfin, dans le quatrième chapitre, nous décrirons la réalisation du système, en mettant en évidence les choix techniques, tels que les langages de programmation, les outils et les logiciels utilisés, ainsi que le diagramme de déploiement et les interfaces de l'application Web.
En conclusion, ce mémoire vise à contribuer à la conception d'un système de protection des données sensibles au sein de l'organisme d'accueil Sonatrach. Nous espérons que les résultats et les recommandations de cette étude seront bénéfiques pour l'amélioration de la sécurité informatique et la protection des données sensibles au sein de Sonatrach, ainsi que pour les chercheurs et les professionnels travaillant dans ce domaine passionnant et en constante évolution.

CHAPITRE I

Présentation de l'organisme d'accueil et étude de l'existant

1 Introduction :

Au sein du Département Technologie de L'information de la division LAB (D-LAB) de Sonatrach, notre mémoire a été mis en œuvre. Ce chapitre propose une étude approfondie de la présentation de l'organisme d'accueil d'un système informatique, et de tous les éléments et entités qui concourent à son fonctionnement.

2 Présentation de l'organisme d'accueil :

2.1 Sonatrach :

Sonatrach (acronyme de Société nationale pour la recherche, la production, le transport, la transformation, et la commercialisation des hydrocarbures), est une entreprise pétrolière et gazière algérienne. Créée le 31 décembre 1963. C'est un acteur majeur de l'industrie pétrolière surnommé la major africaine. Sonatrach est classée la première entreprise d'Afrique. [1]

2.2 Identité visuelle (logo) :

En mars 1967, Sineinventa le logo et proposa les couleurs (orange, rouge et noir) de la jeune entreprise ; le logo de Sonatrach est simple, moderne et professionnel, tout en faisant référence aux activités principales de l'entreprise dans l'industrie pétrolière et gazière.

Figure I-1: logo de Sonatrach

3 Présentation de la direction d'accueil (D-LAB) :

Au sein du Division LAB (D-LAB) de Sonatrach, il y a un département qui supervise l'infrastructure technologique de l'organisation (Département Technologie de L'information). Cette équipe chargée de la mise en œuvre, de l'amélioration et de la sauvegarde des réseaux informatiques, de la gestion des données et d'autres systèmes informatiques. Il est possible que ce département spécifique porte le nom de Département des technologies de l'information.

De nouvelles technologies sont évaluées et mises en œuvre par le département technologie de l'information pour soutenir les efforts de recherche et développement du D-LAB Sonatrach. Celles-ci incluent la modélisation de processus, la simulation, la gestion de données massives et d'autres technologies récentes. Le service informatique travaille avec les autres services de

Sonatrach pour s'assurer que les besoins de l'entreprise sont satisfaits par la mise en place de solutions adaptées.

4 Le département Technologies de L'information :

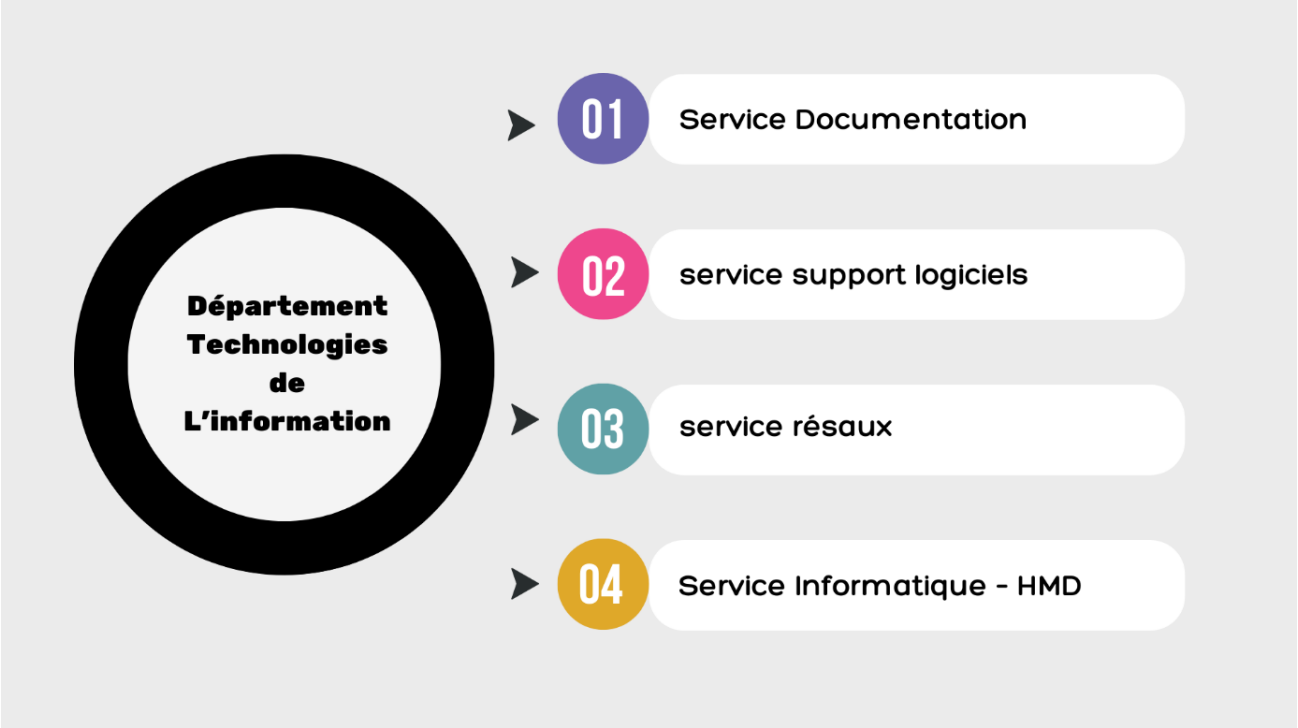


Figure I- 2 : Architecteur du département Technologies de L'information.

Missions du Département Technologies de l'Information :

- La promotion et le développement des activités informatiques.

- Le développement du réseau informatique de la Division.

- Le Data management.

- La prise en charge des systèmes informatiques en exploitation.

- L'acquisition, l'adaptation, le développement et la mise en œuvre de nouvelles solutions informatiques pour les besoins des utilisateurs.

- La standardisation, l'actualisation et la disponibilité du parc informatique.

- La mise en œuvre de la politique de sécurité informatique de l'entreprise.

Le Département Technologies de l'Information est composé de :

- Un Service Développement et Maintenance Logiciels

- Un Service Système, sécurité et Réseaux

- Un Service Documentation Technique

- Un Service Informatique – HMD

5 Description du système informatique :

Dans cette section, nous allons recenser tous les éléments et entités qui contribuent au fonctionnement du système informatique. En nous appuyant sur les visites effectuées et les documents fournis, nous allons organiser l'inventaire des équipements informatiques de la manière suivante :

5.1 Inventaire des serveurs :

5.1.1 Serveur AD (active directory) :

Est un service d'annuaire (bibliothèque) de la famille Windows.

Le rôle d'Active Directory est de stocker de manière centralisée les informations relatives aux objets du réseau et de faciliter l'accès, la recherche et la modification.

Les objets peuvent être des comptes utilisateurs, des groupes, des ordinateurs, des imprimantes, des dossiers, des applications...

Les cinq rôles Active Directory sont :

- Services de domaine AD (AD DS) : Annuaire
- AD Certificate Services (AD CS) : gestion des certificats numériques
- Services de fédération AD (AD FS) : ressources partagées
- Services de gestion des droits AD (AD RMS) : protection des données
- AD Lightweight Directory Services (AD LDS): Une version allégée d'Active Directory

5.1.2 Serveur DNS :

Un serveur DNS fournit une résolution de noms pour les réseaux TCP/IP. En d'autres termes, il permet aux utilisateurs d'ordinateurs clients d'identifier les hôtes distants par leur nom plutôt que par leur adresse IP numérique. L'ordinateur client envoie le nom de l'hôte distant au serveur DNS, qui répond avec l'adresse IP appropriée. L'ordinateur client peut alors envoyer le message directement à l'adresse IP de l'hôte distant. Si le serveur DNS n'a pas d'entrée pour l'hôte distant

dans sa base de données, il peut répondre au client avec l'adresse d'un serveur DNS qui est plus susceptible d'avoir des informations pour cet hôte distant, ou il peut interroger d'autres serveurs DNS [2]

5.1.3 Serveur DHCP :

Un serveur DHCP (Dynamic Host Configuration Protocol) attribue dynamiquement des adresses IP aux clients dans un délai spécifié.

Au lieu d'attribuer manuellement à chaque hôte une adresse statique avec tous les paramètres (par exemple, serveur de noms, adresse de passerelle par défaut, réseau @ IP), le serveur DHCP attribue au client un bail d'accès au réseau pour une durée fixe (terme). Toutes les informations dont le serveur a besoin pour passer des paramètres au client. [3]

5.1.4 Serveur de contrôle d'accès :

Le contrôle d'accès désigne différentes solutions techniques qui sécurisent et gèrent l'accès physique à un bâtiment ou à un site, ou l'accès logique aux systèmes d'information. On distingue ainsi le contrôle d'accès physique et le contrôle d'accès logique. [4]

5.1.5 Serveur de fichiers :

Un serveur de fichiers est une instance de serveur central dans un réseau informatique qui permet aux clients connectés d'accéder aux ressources qui y sont stockées. Le terme comprend à la fois le matériel et les logiciels requis pour configurer de tels serveurs. Les utilisateurs accédant au serveur peuvent ouvrir et, si nécessaire, lire, modifier et supprimer des dossiers et des fichiers sur le serveur de fichiers, ainsi que télécharger leurs propres fichiers sur le serveur, s'ils disposent des autorisations appropriées. Pour qu'un serveur de fichiers fonctionne de manière fiable, il a besoin du bon matériel. Bien sûr, cela commence par le disque dur, qui doit fournir suffisamment d'espace pour les fichiers et programmes requis, y compris le système d'exploitation correspondant et les logiciels requis pour servir les clients. Le serveur doit également disposer de suffisamment de RAM et de performances de processeur pour gérer l'accès aux fichiers et aux programmes par différents utilisateurs aussi rapidement et efficacement que possible. [5]

5.1.6 Serveur d'application BBD :

Un serveur d'application est un serveur Web qui reçoit des données textuelles d'un client, les envoie à un serveur de base de données sous la forme d'une requête SQL, puis met à jour la page Web du client pour incorporer la réponse du serveur. [6]

5.1.7 Serveur d'application weblogic :

Oracle WebLogic Server est une plate-forme unifiée et évolutive pour le développement, le déploiement et l'exécution d'applications d'entreprise, telles que Java, sur site et dans le cloud. WebLogic Server fournit une implémentation fiable, mature et extensible de Java Enterprise Edition (EE) et Jakarta EE.

WebLogic est l'une des solutions de référence parmi les produits de serveur d'application Java EE. Vous maîtriserez la mise en œuvre, la configuration, le déploiement et le réglage des applications WebLogic Server pour JEE. Vous apprendrez également comment sécuriser des serveurs et déployer des applications en cluster. [7]

5.1.8 Serveur de base de données(oracle) :

Le serveur base de données et fonctionne de manière client-serveur le serveur gère la base de données et clients communiquent avec le serveur. [8]

5.1.9 Serveur management de baie de stockage (Symantec backup) :

Il s'agit d'un serveur de fichiers autonome, connecté au réseau via un protocole de communication (tel que TCP/IP), dont la fonction principale est de stocker des données dans un volume centralisé pour des clients réseau hétérogènes.

5.1.10 Robot de sauvegarde :

Le serveur est également sauvegardé par l'application de sauvegarde, il est donc également client de cette application. Les clients sont également des serveurs et représentent l'environnement à sauvegarder. Un client comprend un ensemble de données à sauvegarder sur une machine déterminée (serveur de fichiers, serveur d'application, etc.), et plusieurs clients peuvent coexister sur la même machine physique, et chaque client a ses propres attributs.

Son rôle principal est de réaliser les phases de sauvegarde, d'archivage et de récupération des données (système d'exploitation, fichiers, bases de données, etc.)

5.2 Inventaire des logiciels et système d'exploitation :

5.2.1 Les logiciels :

Dans cette section, nous allons lister tous les logiciels qui sont mis en place au sein de l'entreprise, notamment ceux qui contribuent à la protection des données sensibles de l'entreprise comme suit :

5.2.1.1 Active Directory :

Microsoft a développé Active Directory en 1996 dans le but d'établir un service d'annuaire pour les systèmes d'exploitation sous Windows. La base de données est conçue pour consolider les informations importantes sur l'utilisateur telles que le titre, le numéro de téléphone et le nom ainsi que l'identité de l'ordinateur et de l'équipement informatique. Le service fusionne également les mots de passe et les droits d'accès pour une authentification simplifiée. [9]

- Pourquoi mettre en place un Active Directory ?

En construisant un système centralisé pour les données des utilisateurs et l'équipement informatique, la mise en œuvre d'Active Directory peut offrir de nombreux avantages. Cette innovation améliore notamment la sécurité du réseau grâce aux autorisations d'accès définies par les administrateurs pour les utilisateurs ou groupes d'utilisateurs aux différentes ressources et logiciels. De plus, Active Directory introduit des fonctionnalités capables de simplifier la gestion des installations et des mises à jour de logiciels sur le réseau. [9]

- Que contient l'Active Directory ?

1. Les dossiers partagés, le poste de travail, l'imprimante, le scanner et d'autres ressources sont disponibles.
2. Les services et droits autorisés pour les groupes d'utilisateurs et les listes d'utilisateurs sont disponibles.
3. Le courrier électronique et d'autres services.

- L'entreprise peut améliorer la sécurité de ses données et respecter les normes de conformité réglementaire en intégrant des solutions de gestion des identités et des accès à Active Directory. Cela facilite l'application de protocoles pour la rotation des mots de passe, la gestion des certificats et la surveillance des activités de connexion et de déconnexion.

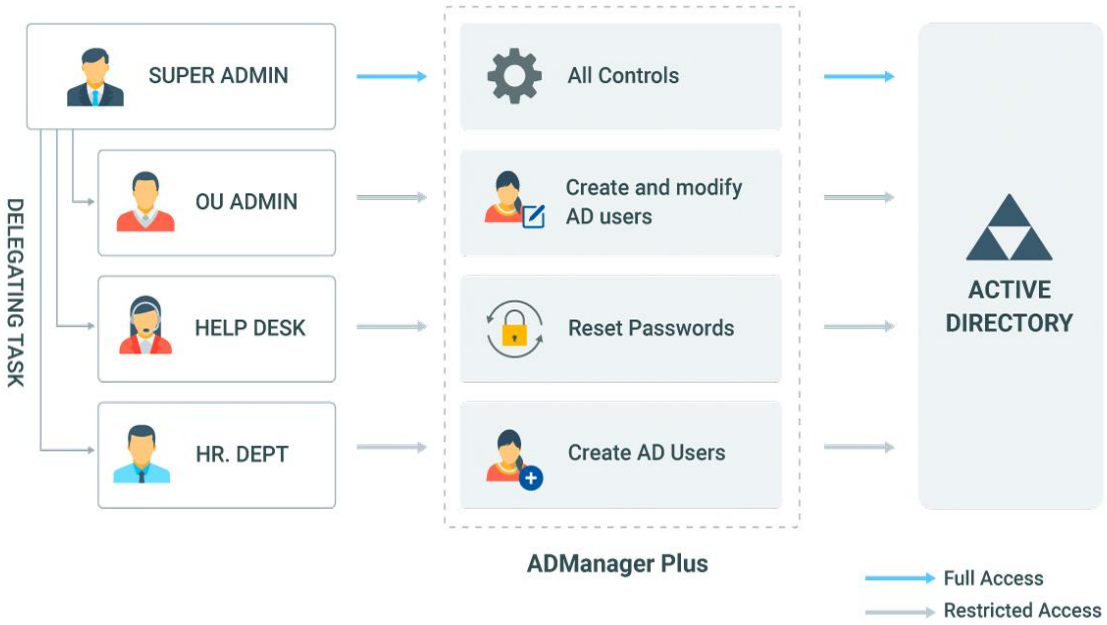


Figure I-3: La gestion des droits d'accès et des permissions.

5.2.2 Symantec antivirus :

Votre PC est protégé contre un large éventail de logiciels malveillants tels que les virus, les logiciels espions, les bots et les vers par Norton Anti-virus. Le logiciel garantit que les performances de votre PC ne sont pas affectées et qu'il n'interfère en aucune façon avec votre travail. Le système de protection supérieur Norton comprend de nombreuses technologies de protection. Ces technologies fonctionnent en tandem pour prévenir les attaques de manière proactive et identifier et éliminer les menaces potentielles avant qu'elles ne puissent endommager votre ordinateur.

Avec Intrusion Protection protégeant votre ordinateur contre les attaques Web, votre navigation peut se faire en toute sécurité. De plus, la protection contre les vulnérabilités récemment introduite comble les failles de sécurité potentielles dans votre système d'exploitation, vos applications, vos navigateurs et vos modules complémentaires, en veillant à ce que les pirates ne puissent pas en profiter. [10]

Les systèmes informatiques peuvent être protégés contre les logiciels malveillants et les virus nuisibles grâce à l'utilisation du logiciel antivirus Symantec. Ce logiciel utilise deux techniques différentes pour détecter et supprimer les menaces : la détection basée sur les signatures pour identifier et supprimer les virus connus, et la détection heuristique, qui empêche les nouveaux dangers non identifiés d'affecter le système.

- Pourquoi mettre en place Symantec antivirus ?

Il est important d'installer un logiciel antivirus tel que Symantec Antivirus pour protéger votre système informatique contre les virus, les logiciels malveillants, les chevaux de Troie et autres menaces de sécurité. Voici une liste des principaux avantages de ce forfait :

a. Antivirus de nouvelle génération
b. Prévention des logiciels malveillants sans fichier
c. Gestion et reporting centralisés
d. Détection et réponse aux points finaux
e. Renseignements sur les menaces
f. Chasse aux menaces
g. Contrôle des ports et des périphériques
h. Accessibilité 24h/24 et 7j/7 [11]

- Quelle est les fonctions de protection par Symantec antivirus :

1. Analyse du comportement des utilisateurs pour identifier les comportements à haut risque de certains utilisateurs sur tous leurs appareils.
2. La technologie Symantec éprouvée offre une protection permanente des appareils en couches.
3. Les technologies de pare-feu intelligent et de prévention des intrusions bloquent les menaces avant qu'elles n'atteignent les appareils.
4. Techniques d'exclusion et d'atténuation de l'utilisation de la mémoire pour se protéger contre les applications à risque.

5. Gestion du chiffrement pour stocker en toute sécurité les clés de récupération pour les appareils Windows, Mac et Android. [12]

Figure I-4: Les fonctions de protection par Symantec antivirus.

5.2.3 Les système d'exploitation :

Dans cette partie, nous énumérerons tous les systèmes d'exploitation actuellement utilisés au sein de l'entreprise, de la manière suivante :

5.2.3.1 Windows Server 2008:

Robuste et fiable, Windows Server 2008 a été dévoilé au monde le 27 février 2008 par Microsoft en tant que système d'exploitation serveur. Son esthétique est la plus similaire à celle de Windows Vista. Doté de fonctionnalités recherchées, ce système d'exploitation est idéal pour les serveurs qui ont besoin d'une disponibilité optimale à tout moment. Au lieu d'arrêter un disque pour corriger l'erreur, un sous-processus peut désormais traiter toute erreur de disque détectée grâce à la mise en œuvre de la fonctionnalité "NTFS à réparation automatique". De plus, avec ce système d'exploitation amélioré, certains correctifs peuvent être installés par l'administrateur système sans qu'il soit nécessaire de redémarrer le système.

Windows Server 2008 peut également être utilisé comme plusieurs types de serveurs. Il peut être utilisé comme serveur de fichiers pour stocker les fichiers et les données de l'entreprise. Il peut également être utilisé comme serveur Web, hébergeant des sites Web pour un ou plusieurs particuliers (ou entreprises). Les serveurs sont également utiles pour partager des imprimantes et des applications au sein d'une entreprise ou d'un domaine. La concentration des ressources apporte une plus grande efficacité à l'entreprise. [13]

5.2.3.2 Windows Server 2016:

Windows Server 2016 est le système d'exploitation de serveur x64 de Microsoft, qui fait partie de la famille Windows NT pour les serveurs d'entreprise. Il est également connu sous le nom de "Windows Server vNext"

Le premier aperçu technique a été publié le 1er octobre 2014, en même temps que System Center 2016. La cinquième version de prévisualisation a été publiée fin avril 2016. Windows Server 2016 est sorti le 5 octobre 2016.

Les nouvelles fonctionnalités incluent l'utilisation de conteneurs (avec isolation), de microservices et de clouds hybrides. [14]

Dans l'ensemble, Windows Server 2016 est un système d'exploitation serveur puissant et riche en fonctionnalités qui offre des capacités de sécurité, de virtualisation, de stockage et de gestion améliorées.

5.2.3.3 Windows Server 2019:

Le système d'exploitation Windows Server 2019 est fourni par Microsoft, prend en charge les postes de travail Windows 10 et fournit des services de base tels que les services d'hébergement et le stockage de fichiers dans les réseaux informatiques. Windows Server 2019 est le successeur de Windows Server 2016. Le système d'exploitation Windows Server 2019 comprend plusieurs améliorations par rapport aux versions précédentes, mais les plus importantes sont sans aucun doute la gestion des conteneurs Linux et Kubernetes. L'amélioration la plus évidente est qu'il s'agit d'un serveur Windows très ouvert au monde open source et à ses efforts. Ainsi, par exemple, en utilisant Web PI (Web Platform Installer), il est très facile d'installer Python, PHP et MySQL qui sont parfaitement compatibles avec IIS. Si nous commençons avec la version Windows NT 4 Server, il s'agit de la 7e version majeure de Windows Server. [15]

5.2.3.4 Windows 7; 10; 11:

Windows 7, 10 et 11 sont des versions différentes du système d'exploitation Windows publiées par Microsoft.

Windows 7 : Sorti en 2009, est un système d'exploitation populaire et largement utilisé. Il introduit de nombreuses fonctionnalités telles que des aperçus améliorés de la barre des tâches, des listes de raccourcis et Aero Snap, permettant aux utilisateurs d'organiser et de gérer facilement leurs fenêtres ouvertes. [16]

Windows 10 : Sorti en 2015, est la version actuelle du système d'exploitation Windows. Il introduit de nombreuses nouvelles fonctionnalités et améliorations, telles que la fonctionnalité de bureau virtuel, l'assistant vocal Cortana et le navigateur Edge. [17]

Windows 11 : Est la dernière version de Windows, sortie en octobre 2021. Il introduit un nouveau design, de nouvelles fonctionnalités telles que Snap Layouts et Snap Groups pour un meilleur multitâche et des performances améliorées. Windows 11 inclut également des versions mises à jour des fonctionnalités de Windows 10 telles que le menu Démarrer, le Centre d'action et l'Explorateur de fichiers. [18]

5.3 Inventaire des application métiers :

Dans cette section, nous mentionnerons toutes les applications en place dans l'entreprise sans explication détaillée, car la plupart des applications mentionnées sont produites et développées par l'entreprise pour servir ses besoins, et nous les mentionnons comme suit :

a. Gestion de ressources humaines « Sous oracle »

b. Facturations « Sous oracle »
c. Applicatifs de Gestion des passations de marché (BDD MY SQL)
d. Gestion Immobilier
e. Gestion des contrats (Sous oracle)
f. Applicatifs Techrap pour la réalisation des rapports techniques
g. Portail Intranet (BDD MY SQL)

5.4 Inventaire des équipements réseaux:

5.4.1 Switch distribution en redondance :

Le commutateur de couche de distribution joue un rôle important dans le réseau d'entreprise. Il reçoit le trafic de la couche d'accès et le transmet à la couche centrale, détermine l'accès des groupes de travail et fournit une connectivité basée sur des règles. [19]

La redondance assure une disponibilité continue du réseau. Cependant, lorsque des commutateurs sont utilisés pour la redondance dans un réseau, des boucles peuvent se produire. [20]

5.4.2 Contrôleur Wifi :

Un contrôleur LAN sans fil, ou contrôleur WLAN, surveille et gère de manière centralisée les points d'accès sans fil et permet aux périphériques sans fil de se connecter à un WLAN. En tant qu'appareil centralisé, le contrôleur WLAN est généralement situé dans le centre de données auquel tous les points d'accès sans fil du réseau sont directement ou indirectement connectés. [21]

5.4.3 Switch serveur :

Un commutateur de serveur est un appareil qui transfère le trafic (trames) en fonction des informations de la couche 3 (principalement via des adresses mac). Le commutateur serveur prend en charge toutes les fonctions de commutation et dispose également de fonctions de routage inter-VLAN. Ces commutateurs sont conçus pour améliorer les performances de routage sur les grands réseaux locaux (LAN). [22]

5.4.4 Switchs 48 ports et 24 ports.

6 Topologie du réseau :

La topologie du réseau décrit la disposition des ordinateurs, des câbles et des autres composants du réseau. C'est une représentation graphique du réseau physique. Le type de topologie utilisé affecte le type et les capacités du matériel réseau, sa gérabilité et son évolutivité, est la topologie qui existe dans la société est la topologie en étoile. Dans une topologie en étoile, chaque ordinateur du réseau possède un segment de câble connecté à un composant central ou concentrateur. Un concentrateur est un périphérique qui connecte plusieurs ordinateurs. Dans une topologie en étoile, le signal se déplace de l'ordinateur au concentrateur, puis du concentrateur à tous les ordinateurs du réseau. À grande échelle, plusieurs réseaux locaux peuvent être interconnectés dans une topologie en étoile. [23]

7 Conclusion:

Ce chapitre a présenté en détail l'organisme d'accueil au sein du Département Technologie de l'Information de la division LAB (D-LAB) de Sonatrach et le rôle du Département Technologies de l'Information. Nous avons également effectué un inventaire approfondi du système informatique, en identifiant les serveurs, les logiciels, les systèmes d'exploitation, les applications métiers et les équipements réseau utilisés au sein de cet organisme.

Cette analyse approfondie nous a fourni une compréhension claire de la structure et des composants du système informatique de Sonatrach, ainsi que de la topologie de son réseau. Le chapitre suivant sera sur les généralités de la sécurité informatique.

CHAPITRE II

Généralités sur la sécurité d'un système d'information

1 Introduction :

La sécurité informatique est devenue une préoccupation majeure pour les entreprises et les particuliers connectés à Internet. Ce chapitre vise à présenter les concepts de base de la sécurité informatique, qui constituent la base essentielle pour notre étude. Ces principes jouent un rôle crucial dans la protection des systèmes d'information. Nous discuterons les notions de base de la sécurité, la protection des données sensibles et des objectifs de la sécurité.

Enfin, nous examinerons brièvement les mécanismes de sécurité, les services de sécurité et les types d'attaques les plus courantes.

2 Système d'information :

Les systèmes d'information sont une partie essentielle du fonctionnement d'une entreprise moderne. Il permet de gérer et de traiter efficacement l'information, de faciliter la prise de décision et d'augmenter la productivité. Et Il vous permet de collecter des données pertinentes, de les organiser et de les analyser pour en extraire des informations exploitables. Il peut également aider à automatiser les processus et à accélérer les flux de travail.

Un système d'information est un groupe de composants qui fonctionnent ensemble pour collecter, stocker, traiter et distribuer des informations. Cela comprend la technologie, les processus, les politiques et les personnes qui travaillent ensemble pour fournir des informations utiles et pertinentes à tous les niveaux de l'organisation. [24]

Les systèmes d'information peuvent être classés en différents types tels que les systèmes de gestion de base de données, les systèmes de gestion de contenu, les systèmes de gestion de la chaîne d'approvisionnement, les systèmes de gestion de la relation client, les systèmes de gestion des ressources humaines, etc.

3 La sécurité de système d'information :

L'information est la pierre angulaire de l'entreprise d'aujourd'hui. C'est sa force et sa raison d'être documents, bases de données, méthodes de travail, méthodes de production, dossiers des employés, informations sectorielles sont autant d'informations qui constituent la structure et le

fondement de l'entreprise, c'est le capital intellectuel de l'entreprise, plus précisément le capital informationnel. Toute perte d'information peut porter un coup fatal à l'entreprise et même au pays. Si ces informations sont perdues, volées ou tombent entre les mains d'une autre entreprise, les données n'ont plus de raison d'être car elles ne sont plus exclusives.

Aujourd'hui, l'information est précieuse parce qu'elle est unique à une entreprise. Par conséquent, il est dans l'intérêt de l'entreprise de protéger ses actifs informationnels. [25]

De manière générale, un système de sécurité est « l'ensemble des moyens techniques, organisationnels et humains nécessaires à la maintenance et à la sécurisation des systèmes

D'information d'une entreprise ». C'est d'abord un moyen de réduire la vulnérabilité des systèmes d'information en procédant à une analyse détaillée des intrusions possibles, puis de protéger l'environnement informatique interne et externe de l'entreprise d'éventuelles intrusions ou surveillances malveillantes. Cela se fait généralement avec un logiciel de sécurité puissant. [26]

4 Les notions de base de la sécurité :

La sécurité des systèmes d'information est une préoccupation majeure pour toutes les entreprises. Les systèmes d'information sont des éléments essentiels de l'entreprise car ils stockent et traitent des informations sensibles telles que des états financiers, des informations client et des données confidentielles.

C'est un terme très large, est destiné à guider les organisations avec des politiques de cybersécurité dans le domaine de la sécurité de l'information. Voici quelques concepts de base de la sécurité des systèmes d'information :

4.1 La Confidentialité

La confidentialité est l'une des choses les plus importantes que la sécurité du réseau doit maintenir en établissant des conditions et des normes spéciales pour que les utilisateurs accèdent aux informations et en définissant des droits pour garantir que les informations qui doivent être protégées ne soient accessibles que par les parties autorisées à sa disposition. [27]

Pour protéger la confidentialité, les organisations doivent prendre des mesures de sécurité adéquates, notamment des listes de contrôle d'accès (ACL), le chiffrement, l'authentification à

deux facteurs et des mots de passe forts, un logiciel de gestion de la configuration, la surveillance et l'alerte.

4.2 L'intégrité :

L'intégrité implique la protection des informations contre toute modification non autorisée. Il s'agit de protéger les données contre toute suppression ou modification inappropriée. Les entreprises doivent mettre en place des contrôles d'accès pour s'assurer que seul le personnel autorisé peut modifier les données. Une façon d'assurer l'intégrité consiste à utiliser des signatures numériques pour vérifier l'authenticité du contenu ou sécuriser les transactions. [27]

4.3 La disponibilité :

La sécurité des données nécessite l'inclusion d'afin d'être efficace. Lorsqu'il s'agit de rendre les informations et les systèmes accessibles uniquement aux utilisateurs autorisés, la disponibilité est essentielle. Le bon fonctionnement des systèmes informatiques, des contrôles de sécurité et des logiciels est indispensable pour garantir que ces services sont disponibles aux moments appropriés. Par exemple, Une base de données financière hors ligne peut entraîner de graves interruptions des processus commerciaux, comme des paiements de factures manqués et des retards pour vos comptables. [27]

4.4 L'authentification :

L'accès aux informations et aux systèmes ne devrait être accordé qu'aux personnes autorisées, ce qui est obtenu par l'authentification. Des politiques de mot de passe robustes, une authentification à deux facteurs et des contrôles d'accès doivent être mis en place par les entreprises pour garantir des mesures de sécurité appropriées. En mettant en œuvre un code d'accès, l'identité d'un utilisateur peut être vérifiée, maintenant la sécurité informatique en confirmant l'utilisateur réel. Pour autoriser l'accès uniquement aux personnes autorisées et maintenir la confiance dans la communication, le contrôle d'accès, comme la protection par mot de passe, est nécessaire pour limiter l'accès à des ressources spécifiques. [28]

Il convient de mentionner qu'il existe une distinction entre l'identification et l'authentification. Le premier fait référence à l'identifiant public, tandis que le second se rapporte à un composant secret qui n'est familier qu'à l'utilisateur. Par conséquent, le système de sécurité corrèle l'identifiant public avec le composant d'authentification pour s'assurer que l'identifiant est authentique.

4.5 La non-répudiation :

La non-répudiation des informations vise à garantir qu'aucune partie à la communication ne pourra refuser la transaction. Le but est de s'assurer que l'éditeur de l'information (quelle qu'elle soit) ne puisse pas nier qu'il est bien la source de l'information. Pour atteindre cet objectif de sécurité informatique et pour y parvenir, nous utilisons des signatures d'emails, de documents ou de certificats. Par conséquent, seul l'utilisateur qui possède la clé privée peut signer l'e-mail. Par conséquent, cette personne ne peut nier être l'émetteur. [29]

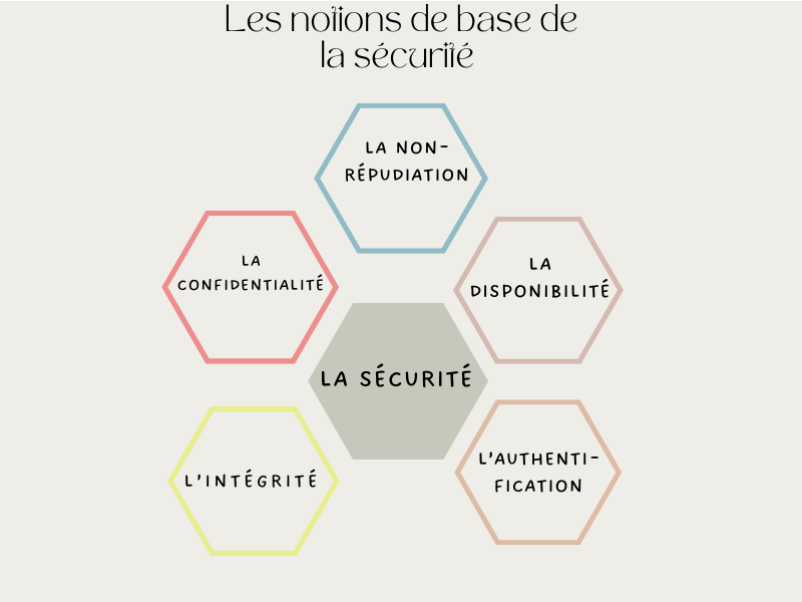


Figure II-5: Les notions de base de la sécurité.

5 La protection des données sensibles :

Les données sensibles représentent une catégorie de données personnelles qui, en raison de leur contenu, doivent être protégées dans une plus grande mesure. Ils sont la propriété de la personne physique à laquelle se rapporte leur contenu.

5.1 Définition :

Les données sensibles sont des données spécifiques concernant la vie privée des personnes physiques. Les règles concernant sa protection figurent dans le Règlement général sur la protection des données, également connu sous le nom de RGPD.

Les structures qui collectent des données sensibles ont la responsabilité de les sécuriser et de les sécuriser. Par exemple, les entreprises accordent une attention particulière aux activités de recrutement. En effet, durant ces périodes, ils reçoivent de grandes quantités de données qu'il faut ensuite traiter en toute sécurité.

5.2 Type de données sensibles :

Les données considérées comme sensibles comprennent des informations personnelles sur leurs propriétaires qui relèvent de la sphère privée. On y retrouve notamment des informations sures:

1. L'origine raciale et ethnique
2. Les opinions politiques
3. Les croyances et religions
4. Les opinions philosophiques
5. L'appartenance syndicale
6. Les données génétiques et biométriques
7. Les caractéristiques physiques
8. Les informations relatives au dossier médical

9.Les informations sur la vie sexuelle comprenant l'orientation sexuelle [30]

- Les données sensibles existants dans l'entreprise sont :

a. Les rapports clients

b. Les rapports techniques

c. Les contrats, et dossier juridique, GRH et les Base de données

6 Objectifs de la sécurité :

Toutes les entreprises utilisent des outils numériques et des systèmes d'information avancés dans leurs activités professionnelles quotidiennes, utilisant leurs données internes ainsi que les données de leurs clients. [24] Différents objectifs de sécurité informatique ont pour mission de protéger ces données, nous mentionnons les suivants :

6.1 La prévention

Prendre des mesures pour prévenir les attaques Une fois la phase d'analyse terminée, [31] il est nécessaire de vérifier l'efficacité de la protection afin de protéger au maximum le système (tests opérationnels, tests de récupération de données, tests d'attaques malveillantes, etc.). [27]

6.2 Détection

Prenez des mesures pour savoir quand, comment, par qui et quels biens ou biens ont été endommagés par l'attaque. Choisissez quoi protéger, quand et comment. Parfois, avec des ressources limitées, il suffit de choisir la solution la plus pertinente. [29]

6.3 Réaction

Prendre des mesures après une attaque de sécurité afin de pouvoir restaurer les biens et les actifs, ou réduire l'impact de l'attaque. [28]

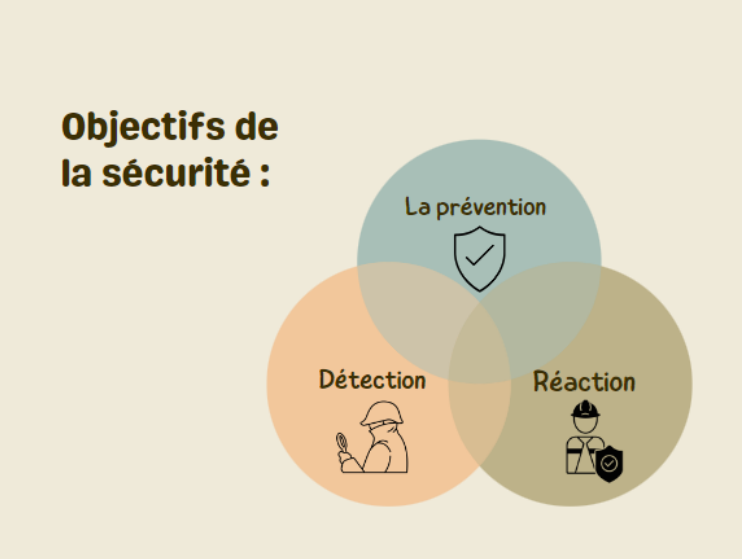


Figure II-6: Objectifs de la sécurité.

7 Mécanismes de sécurité :

Les mécanismes sont divisés en ceux mis en œuvre dans une couche de protocole spécifique et ceux qui ne sont pas spécifiques à une couche de protocole ou à un service de sécurité spécifique.

- Mécanismes de sécurité spécifiques : peuvent être intégrés dans les couches de sécurité

Protocoles appropriés pour fournir certains services de sécurité OSI. [32]

7.1 Mécanismes de sécurité spécifiques :

Mécanisme	Définition
Le chiffrement	Transformation à l'aide d'algorithmes mathématiques donné sous une forme non intelligible. La Conversion et récupération ultérieure des données Dépend de l'algorithme et de la clé de cryptage.
Signature Numérique	Une transformation se produit ou des données sont ajoutées de manière sporadique. Unité de données soumise à la cryptographie.
Contrôle d'accès	Divers mécanismes d'application des droits d'accès Ressource.
Intégrité des Données	Divers mécanismes utilisés pour assurer l'intégrité cellulaire Un flux de données ou d'unités de données.
Echange D'authentification	Mécanismes pour garantir l'identité de l'entité moyen d'échange d'informations
Remplissage du Trafic	Insérer des bits dans les lacunes du flux de données pour éviter les tentatives d'analyse du trafic.
Contrôle de Routage	Vous permet de choisir un itinéraire physiquement sécurisé Ciblant spécifiquement certaines données et permettant changements de routage, en particulier en cas de violation Doute sur la sécurité.
Notarisation	Faites appel à un tiers de confiance pour vous assurer Propriétés de l'échange de données

Tableau II-1: Mécanismes de sécurité spécifiques.

Autres mécanismes :

- Traffic Padding : Mécanisme qui génère de fausses informations sur le réseau pour rendre l'analyse de trafic plus difficile.
- Détection d'intrusions : Repérer les activités suspectes ou anormales sur le réseau

Pare-feu (filtrage): autoriser et interdire certains types de messages à circuler dans le réseau.

- Antivirus : empêcher les codes malveillants de s'exécuter.

8 Les protocoles de la sécurité :

- **IPsec :** Le protocole Internet Protocol Security (IPsec) authentifie et crypte les paquets IP, ce qui sécurise les communications entre les ordinateurs et les périphériques qui utilisent ce protocole. IPsec fonctionne sur la couche réseau du modèle OSI. Il diffère de SSH, SSL et TLS en ce sens que c'est le seul protocole qui ne fonctionne pas aux couches supérieures du modèle OSI. Il est possible de négocier des clés cryptographiques et d'établir une authentification mutuelle.

- **SSH :** Secure Shell (SSH) est un protocole qui permet de contrôler à distance un ordinateur ou un appareil en établissant un canal sécurisé entre eux. Il remplace efficacement Telnet et est largement utilisé sur les systèmes Linux, Unix et Windows. L'authentification des ordinateurs distants s'effectue par cryptographie à clé publique. En obtenant et validant un certificat, le client SSH établit des connexions sécurisées avec le serveur SSH. Les connexions SSH sont effectuées sur le port 22. Lorsqu'une connexion SSH est établie, les fichiers peuvent être transférés en toute sécurité via les protocoles SFTP ou SCP. En outre, SSH gère la création de tunnels sécurisés pour l'accès à distance aux ressources réseau.

- **Protocole PKI :** PKI est une architecture de sécurité qui offre un niveau de confiance plus élevé pour l'échange d'informations sur les réseaux non sécurisés. L'ICP repose sur la cryptographie à clé publique, une technologie développée pour chiffrer et déchiffrer les données à l'aide de deux types de clés différents : une clé publique et une clé privée. Un utilisateur conserve sa clé privée tout en donnant une clé publique à un autre utilisateur. Les données chiffrées avec une clé publique ne peuvent pas être déchiffrées sans la clé privée correspondante.

- **SSL/TLS :** Les protocoles de cryptage SSL (Secure Sockets Layer) et TLS (Transport Layer Security) assurent la sécurité des connexions Internet. Ils sont utilisés pour le surf en ligne, la messagerie instantanée, le courrier électronique et la communication vocale IP. Ces protocoles reposent sur un ICP pour l'acquisition et la validation des certificats. Les connexions SSL sont considérées comme des connexions sécurisées. Afin de chiffrer les données, SSL et TLS utilisent des clés publiques et de session. Le partage des clés de session se fait par cryptage asymétrique, tandis que les données de session sont chiffrées par cryptage symétrique. Une clé de récupération est nécessaire en cas de perte de données car les clés de session sont spécifiques à chaque connexion. SSL et

TLS cryptent les segments de connexion réseau à partir de la couche de transport OSI. Ils sont reconnus comme des protocoles de la couche d'application. [33]

9 Services de sécurité :

Les services destinés à préserver les systèmes d'information d'une organisation des menaces externes et internes sont appelés services de sécurité des systèmes d'information (SSI). La confidentialité, la sécurité, l'intégrité et la disponibilité du système de données sont garanties par un éventail d'étapes techniques, juridiques et organisationnelles qui améliorent le traitement des données et la sécurité de la transmission des informations. Ces services sont utilisés pour maximiser la protection des données et des informations d'une organisation sur une base cohérente, Voici quelques exemples de services de sécurité des systèmes d'information :

9.1 Gestion des identités et des accès :

La gestion des identités et de l'accès assure un accès sécurisé à l'information. Elle s'assure que chaque personne a les droits d'accès appropriés. L'accès non autorisé à des renseignements sensibles comporte des risques. Pour assurer un accès adéquat, un système avec des politiques intégrées d'autorisation, d'authentification et de mot de passe sécurisé est nécessaire. De plus, la conservation précise des enregistrements est essentielle à la sécurité du système. [34]

Grâce à ce service, il est possible de restreindre et de surveiller l'accès des utilisateurs aux systèmes et aux données en fonction de leurs rôles et responsabilités. La gestion des identités à l'intérieur d'un domaine se fait aujourd'hui en utilisant une variété de méthodes. La gestion des identités et de la sécurité relève habituellement des administrateurs des TI.

La vérification des utilisateurs, qu'ils soient internes ou externes, est un élément nécessaire d'un système efficace de gestion de l'identité. Il pourrait être nécessaire de rencontrer physiquement l'entité pour recevoir une confirmation visuelle afin de l'identifier. Les identifiants et identifiants uniques, ainsi que les caractéristiques correspondantes, sont attribués à l'entité.

L'accès aux services protégés n'est accordé qu'après une authentification appropriée. Cela signifie que chaque fois qu'un utilisateur tente d'accéder au service, le processus d'authentification doit être suivi.

.

9.2 Gestion des incidents de sécurité :

La gestion des incidents de sécurité est une préoccupation majeure. Elle a besoin d'un plan d'intervention bien organisé et d'une affectation ciblée des ressources. Les incidents de sécurité peuvent être causés par diverses vulnérabilités ou menaces, y compris des logiciels malveillants, des erreurs humaines et des catastrophes naturelles. L'identification, le confinement, l'éradication et le rétablissement doivent tous faire partie d'un programme réussi de gestion des incidents. L'identification permet de limiter la propagation de la menace. Le but du confinement est d'isoler les systèmes ou les données endommagés. Le but de l'éradication est d'éliminer la menace, et le rétablissement implique de restaurer les données et de reprendre le contrôle sur les actifs. [35]

Les incidents de sécurité sont des violations des politiques de sécurité de l'organisation. Il s'agit de violations de données et de cyberattaques. Ils sont gérés par un certain ministère au sein de l'organisation. Les responsabilités de gestion sont réparties entre de nombreux acteurs organisationnels, y compris le service des technologies de l'information et le service des ressources humaines.

Il est possible de contacter des experts externes pour aider à résoudre le problème en cas d'incident grave ou de divulgation de données. Il est essentiel d'avoir une stratégie pour faire face à ces deux scénarios.

Pour les événements mineurs, il est facile de les gérer à l'interne en prenant des mesures correctives comme changer les mots de passe où mettre en place de nouvelles mesures de sécurité.

9.3 Gestion de la conformité :

Pour assurer une exploitation éthique et sécuritaire, les entreprises sont tenues de suivre des règles précises. Les réglementations exigent la conformité pour protéger l'infrastructure informatique et les données tout en offrant un accès équitable à toutes les parties concernées. En particulier, ce service garantit le respect des lois et des meilleures pratiques définies par l'industrie, assurant le niveau maximal de protection des consommateurs.

La réduction des violations de la réglementation est au cœur de la gestion de la conformité, ce qui équivaut à une diminution des risques et à l'évitement de sanctions financières sévères. Plus précisément, la gestion de la conformité réglementaire tente d'atténuer les risques réglementaires numériques, qui pourraient finalement nuire aux employés et aux clients. Une

part importante des réglementations relatives aux données est directement liée à la protection de la vie privée des clients, ce qui leur assure que leurs données restent hors de portée de pratiques contraires à l'éthique. [36]

Une cybersécurité et une gestion des données médiocres peuvent entraîner des pénalités et des effets résiduels pour une organisation. Ainsi, des contrôles d'autorisation sont nécessaires pour enquêter sur les violations de données et respecter la gestion de la conformité. Un audit rigoureux est impératif dans ce processus.

9.4 Surveillance de la sécurité :

Les informations sont recueillies et analysées par la surveillance de sécurité pour identifier les comportements réseau suspects ou interdits. Cela nécessite de définir les comportements qui devraient déclencher des alertes et, si nécessaire, de prendre les mesures appropriées.

Pourquoi la surveillance de la sécurité ?

Des pirates aux programmes malveillants en passant par les employés mécontents ou négligents, les appareils et systèmes d'exploitation dépassés ou vulnérables, l'informatique mobile, le cloud computing public et les prestataires de service tiers, la plupart des entreprises sont fréquemment exposées à des menaces de gravité variable dans le déroulement normal de leurs activités. Compte tenu de l'omniprésence et de l'inévitabilité des risques de sécurité, un temps de réponse rapide est nécessaire pour assurer la sécurité du système, et une surveillance continue est essentielle pour assurer une détection des menaces et une réponse rapide. [37]

10 La gestion des risques dans les entreprises :

Pour permettre la gestion des risques, la norme ISO 27005 propose un processus qui commence par l'identification des risques au sein d'une entreprise. Ce processus se fait en identifiant les actifs, les menaces ou attaques, les contre-mesures, les vulnérabilités et les conséquences.

10.1 Les actifs :

Un actif est défini comme tout élément qui représente la valeur d'une organisation. (Tout élément qui a de la valeur pour l'organisation et qui doit être protégé). Il existe deux types d'actifs au niveau de l'entreprise : les actifs primaires et les actifs secondaires.

Actifs primaires : il s'agit de la raison d'être de l'entreprise, et ces actifs comprennent les processus commerciaux et les informations de l'entreprise.

Actifs secondaires : spécifie les éléments de support de l'actif principal. Cela englobe notamment les matériels, les logiciels, les réseaux, le personnel ou encore les locaux de l'organisation. [38]

10.2 Les Vulnérabilité :

Une vulnérabilité est une faille de sécurité. Dans la plupart des cas, elle provient de faiblesses des systèmes d'information (SI), des composants matériels ou de la conception logicielle et constitue un point d'application potentiel de la menace. Exemples : Absence de politiques de sécurité, utilisation de mots de passe en clair, etc. [39]

10.3 Les menaces :

Une menace est tout ce qui peut utiliser une vulnérabilité pour accéder, modifier, bloquer ou même détruire complètement un système. Elle est liée à une vulnérabilité, et chaque vulnérabilité peut être vulnérable à de multiples menaces. La compréhension des diverses menaces aide à déterminer leur danger et les mesures de contrôle appropriées pour réduire leur impact potentiel.

Une menace est une source crédible d'incidents qui peuvent avoir des effets négatifs et graves sur une personne ou un groupe de personnes actives peuvent être classés selon leur origine ou leur source, leur type, leur motif ou leur action.

Les principales menaces effectives auxquelles les systèmes d'information peuvent être confrontés face à:

- **Un utilisateur du système :** la grande majorité des problèmes liés à la sécurité, les utilisateurs des systèmes d'information sont souvent des utilisateurs négligents.
- **Une personne malveillante (hacker et crackers) :** Une personne qui copie avec succès un système, que ce soit légalement ou illégalement, peut alors accéder à de l'information ou utiliser des programmes qu'elle ne devrait pas pouvoir utiliser. Un exemple de ceci est l'utilisation des défauts de logiciel qui sont connus au sujet mais ne sont pas corrigés.
- **Programmes malveillants :** conçus pour nuire ou abuser des ressources système sont installées sur le système de manière involontaire ou malveillante, Ouvre la porte à l'intrusion ou à la modification des données.

10.4 Les contre-mesures :

Ce sont des procédures ou des techniques pour résoudre des vulnérabilités ou réponses à des attaques spécifiques (auquel cas il peut y avoir d'autres attaques ciblant la même vulnérabilité) et mis en œuvre dans la prévention des menaces.

10.5 Les conséquences :

Est le résultat de la réalisation du risque, il peut être Dégradé, détruit, corrompu, violé l'un des objectifs de sécurité ou perdu actifs.

10.6 Les Attaques :

Une attaque est un acte malveillant visant à contourner les mesures de sécurité d'un système d'information et utiliser les failles du système informatique pour atteindre le but que la personne en charge du système ne connaît pas.

Une attaque est également un ensemble d'un ou plusieurs événements pouvant avoir une ou plusieurs conséquences en termes de sécurité. Il peut être passif (pour la confidentialité uniquement) ou actif (pour l'intégrité, l'authentification, la non-répudiation et/ou le contrôle d'accès)

11 Famille d'attaques :

11.1 Les attaques applicatives :

11.1.1 Injection de code :

Consiste à injecter du code supplémentaire dans un programme afin d'exécuter des taches supplémentaires, exemples : l'injection SQL et la faille XSS.

Une attaque de type injection SQL consiste à envoyer une valeur à une application web à utiliser dans une requête SQL, écrite de manière à exécuter une requête SQL différente de celle initialement écrite dans l'application. Une attaque Permettre aux visiteurs du site Web d'exécuter une partie du code en dehors de l'application via des scripts intersites ou XSS. [40]

11.1.2 Le dépassement de tampon (Buffer Overflow) :

Le débordement de tampon ou (buffer overflow) est une attaque très efficace et assez complexe à exécuter. Il est conçu pour exploiter les failles, les faiblesses des applications (types de navigateurs, logiciels de messagerie, etc.) pour exécuter du code arbitraire, compromettant ainsi la cible (obtention de privilèges d'administrateur, etc.). Un débordement

de tampon est ce qui se produit lorsque, dans un programme, plus de données sont placées dans l'espace mémoire qu'il ne peut en contenir.

Dans ce cas, les données sont toujours insérées dans la mémoire même si elles écrasent d'autres données qui n'auraient pas dû être écrasées. En fait, l'écrasement des données critiques du programme entraîne souvent des plantages du programme. [41]

11.2 Les attaques par programme malveillant :

11.2.1 Virus :

Un virus informatique est un programme malveillant qui se réplique automatiquement en se copiant dans un autre programme. Il se propage dans d'autres codes ou documents exécutables dans le but d'infecter les systèmes vulnérables, de prendre le contrôle des administrateurs et de voler les données des utilisateurs. (Ils sont conçus pour piéger) Il peut avoir des effets néfastes en perturbant le fonctionnement de l'ordinateur infecté en effectuant des modifications indésirables. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, etc. [42]

11.2.2 Vers (Worm) :

Les vers sont des logiciels malveillants qui se répliquent sur plusieurs ordinateurs à l'aide d'un réseau informatique, tel qu'Internet.

- **Mode opératoire :**

Contrairement aux virus informatiques, les vers n'ont pas besoin d'un programme hôte pour se reproduire. Il utilise les différentes ressources de l'ordinateur qui l'héberge pour assurer sa réplication. [43]

Le but des vers n'est pas seulement de se reproduire. Le ver a également souvent des objectifs malveillants, tels que :

- Surveiller l'ordinateur sur lequel il se trouve ;
- Fournir des portes dérobées aux pirates ;
- Détruire ou autrement endommager les données sur l'ordinateur sur lequel elles se trouvent ;
- Envoi de requêtes multiples à un serveur Internet pour le saturer (déni de service)

- **Les classes de vers :**

  - Vers de réseau (Vers de réseaux de partage de fichiers.) ;
  - Vers de courrier électronique ;
  - Vers de messagerie instantanée ;
  - Vers Internet ; [44]

11.2.3 Cheval de Troie :

- **Définition** :

Un cheval de Troie est un type de logiciel malveillant et ne doit pas être confondu avec un virus ou un autre parasite [49], est un logiciel malveillant qui se présente comme un programme légitime, mais qui permet vraiment le contrôle à distance ou modifie son fonctionnement. Il pourrait être caché dans des fichiers téléchargés, des courriels qui ont été assemblés, ou des logiciels illégaux. Une fois installé, il recueille des données, supprime des fichiers, met en place d'autres logiciels malveillants, et vole des mots de passe. En outre, il ouvre des portes brisées pour permettre aux pirates de prendre le contrôle secret de l'ordinateur infecté. [45]

Un cheval de Troie est un type spécifique de logiciel malveillant. Contrairement aux virus, les chevaux Troie ne sont pas auto-répliqués et doivent être installés volontairement par l'utilisateur. [46]

- **Fonctionnement :**

Pour attaquer les victimes, les chevaux Troie se posent souvent comme des documents légitimes. Une fois ouverts, ils installent des logiciels malveillants, espionnent les utilisateurs ou causent des dommages. Par exemple, les chevaux de Troie utilisent l'ingénierie sociale pour imiter les articulations des pièces de puzzle régulières. Ils attaquent l'appareil lorsqu'ils sont exposés. Un cheval Troie a besoin de dissimulation pour bien fonctionner. [46]

- **Types de chevaux de Troie :**

Il existe différents types de chevaux de Troie, chacun ayant ses propres caractéristiques et objectifs malveillants. Voici quelques exemples de types de chevaux de Troie :

  - Cheval de Troie « à porte dérobée »
  - Cheval de Troie bancaire

- Cheval de Troie par déni de service distribué (DDoS)
- Cheval de Troie par exploit
- Cheval de Troie voleur de données
- Cheval de Troie sur messagerie instantanée. [46]

11.2.4 Porte dérobée(backdoor) :

Une porte dérobée est un logiciel malveillant permettant à un attaquant de prendre le contrôle d'un système infecté. Les portes dérobées ont évolué en botnets, des groupes de machines infectées reliées à un serveur central de commande et contrôle (C&C). Les RATs (Remote Administration Tools) sont des frameworks facilitant la gestion des machines infectées, offrant diverses fonctionnalités telles que la capture d'écran et le transfert de fichiers. Ces frameworks sont parfois appelés chevaux de Troie. [47]

11.2.5 Bombe logique :

Les bombes logiques sont des codes malveillants qui sont programmés pour exploser à un moment précis ou en réponse à un événement spécifique. Elles sont généralement utilisées dans le but de causer des dommages ou une interruption après un certain temps ou lorsque certaines conditions sont remplies.

Ces programmes peuvent avoir plusieurs objectifs malveillants, tels que la destruction de données, le vol d'informations sensibles, l'endommagement de systèmes informatiques, etc. Ils peuvent être intégrés dans des programmes ou des scripts légitimes, ou cachés dans des fichiers ou des documents apparemment inoffensifs.

Lorsqu'une bombe logique est activée, elle peut causer des dommages importants, tels que la suppression de fichiers ou de données, le blocage de l'accès à un système, ou la propagation de codes malveillants sur d'autres systèmes. Les conséquences peuvent être graves, notamment en cas d'utilisation de ces programmes pour des actes criminels ou terroristes. [47]

11.2.6 Logiciel espion :

Le spyware, également appelé logiciel espion, est un programme malveillant conçu pour collecter secrètement des informations sur l'utilisateur d'un ordinateur ou d'un appareil mobile. Ces informations peuvent inclure les sites web visités, les mots de passe saisis, les conversations en ligne, les courriels envoyés et reçus, les fichiers téléchargés, les photos et vidéos, ainsi que d'autres données personnelles sensibles.

Les logiciels espions s'installent souvent à l'insu des utilisateurs, se faisant passer pour des programmes légitimes ou étant inclus dans des téléchargements gratuits ou des pièces jointes d'e-mails. Ils opèrent en arrière-plan, collectant des informations sans que l'utilisateur ne le remarque. [48]

11.2.7 Ransomware :

Un ransomware est un logiciel malveillant qui obtient l'accès à l'information sensible contenue dans un système, le chiffre de sorte que l'utilisateur ne peut y accéder, puis demande le paiement avant de permettre aux données d'être rendues publiques. Typiquement, les rançongiciels font partie d'une escroquerie par hameçonnage. L'utilisateur télécharge le ransomware en cliquant sur un lien caché. L'agresseur calcule des renseignements précis qui ne peuvent être consultés que par une formule mathématique qui lui est familière. Les données sont détruites lorsque l'attaquant reçoit le paiement. [49]

11.3 Les attaques par message électronique :

11.3.1 Les spam :

Le spam fait référence aux communications électroniques non sollicitées reçues. Les spammer envoient du spam à de nombreuses personnes. Le spam peut prendre la forme de publicités, d'annonces commerciales, de tentatives d'arnaque, etc. Le terme "spam" est utilisé pour décrire les e-mails non sollicités, mais il peut également s'appliquer à d'autres formes de communication non désirées, telles que les SMS, les appels téléphoniques, les messages instantanés, les commentaires sur les réseaux sociaux, etc.

Le spam peut contenir de la publicité, des escroqueries, des virus ou d'autres types de contenu malveillant. Les expéditeurs de SPAM utilisent souvent des techniques de marketing trompeuses ou illégales pour tenter de convaincre les destinataires de cliquer sur des liens, d'acheter des produits ou de fournir des informations personnelles.

11.3.2 Phishing :

L'hameçonnage est une forme de fraude en ligne conçue pour amener les gens à fournir des informations personnelles, financières ou confidentielles.

Cette méthode consiste à former les internautes à divulguer des informations confidentielles grâce à l'utilisation d'un crochet constitué de mensonges et de faux électroniques. La méthode la plus courante consiste à usurper l'identité de la structure par e-mail et à inclure un lien vers un faux site Web où il vous sera demandé de confirmer un compte sous un prétexte plus ou

moins probable. Ces e-mails contiennent souvent des liens vers des sites Web malveillants qui ressemblent à des sites Web légitimes, ou ils peuvent contenir des pièces jointes chargées de logiciels malveillants. Les phishers visent à obtenir des informations confidentielles telles que des numéros de carte de crédit, des informations bancaires, des mots de passe ou d'autres données sensibles.

11.3.3 Un Hoax (canular) :

Hoax est un mot Anglais qui signifie " canular ". En informatique, cela fait référence à des informations inexactes ou invérifiables qui utilisent la puissance d'Internet pour se propager largement.

Un faux rapport ou une fausse rumeur qui est propagée négligemment, souvent par l'utilisation des médias sociaux ou d'Internet, est qualifié de "canular". L'utilisation de canulars peut être utilisée pour tromper ou manipuler les gens en les avenant à croire de fausses informations.

Avant de partager ou de diffuser une information, il est essentiel de vérifier son authenticité. Pour ce faire, vous pouvez soit effectuer une recherche en ligne pour voir si d'autres sources conviennent à l'information, soit entrer directement en contact avec la source originale du matériel pour obtenir des applications.

Quelques sites conçus afin d'aider les internautes à identifier les canulars informatiques :

- HoaxBuster (site francophone) http://www.hoaxbuster.com
- HoaxKiller (site francophone) http://www.hoaxkiller.fr
- Snopes (site américain) http://www.snopes.com [50]

11.4 Les attaques sur les réseaux :

11.4.1 Reconnaissance :

La reconnaissance est le processus de collecte de données sur un système afin de cerner ses vulnérabilités.

Le terme "attaque de reconnaissance" désigne les attaques informatiques visant à recueillir des connaissances sur un système informatique ou un réseau. Ces détails pourraient être utilisés par les voleurs d'ordinateurs pour découvrir des failles de sécurité et accéder à des données ou des systèmes sensibles. Les méthodes d'enquête de service de réseau, les contrôles de port, les tests

de pénétration, les analyses de protocole et les analyses de trafic de réseau sont quelques exemples d'attaques de reconnaissance. [51]

- **Les type de reconnaissance :**

Reconnaissance active : le pirate interagit avec la victime pour obtenir des informations.

Reconnaissance passive : le pirate peut obtenir des informations à propos de la victime sans la solliciter.

11.4.2 Accès :

Une attaque d'accès est une tentative non autorisée d'accéder à un compte ou à un réseau en utilisant des méthodes incorrectes. Les attaques par mot de passe, la redirection de port et l'homme au milieu peuvent être des exemples. Les attaques d'accès peuvent exploiter des failles de sécurité et nécessitent des compétences sophistiquées. Ils peuvent être comparés aux attaques logiques et physiques, qui utilisent respectivement l'ingénierie sociale en ligne ou ciblent des individus ou l'infrastructure. Les attaques d'ingénierie sociale, telles que les e-mails malveillants, sont particulièrement difficiles à protéger car elles utilisent la tromperie et la confiance. [52]

- **Attaques par mot de passe :** Un type de cybercriminalité appelé piratage de mots de passe implique des criminels qui tentent d'accéder à des ordinateurs, des comptes ou des fichiers qui sont protégés par mot de passe. Ils utilisent fréquemment des logiciels pour accélérer le processus de déchiffrement ou de génération de mots de passe. Lors de la création de mots de passe, il est essentiel de suivre de bonnes procédures de sécurité en s'abstenant d'utiliser des noms de famille, des adresses personnelles, etc. Surtout pour quelqu'un que vous connaissez bien, les phrases de passe sont généralement simples à comprendre et à décomposer. Pour deviner ou chercher les mots de passe couramment utilisés, les pirates ont besoin de techniques et d'équipement spécialisés. Environ 75% des internautes utilisent les 500 premiers mots de passe les plus courants, ce qui les rend vulnérables. [53]

- **Redirection de port :** La redirection de port est une attaque "d'exploitation de confiance" qui utilise un hôte infecté pour faire passer le trafic à travers un pare-feu qui serait normalement bloqué. Ce type d'attaque est principalement limité par l'utilisation d'un modèle de confiance approprié. Les logiciels antivirus et les systèmes IDS peuvent détecter et empêcher les attaquants d'installer des utilitaires de redirection de port sur cet hôte. [54]

- **Attaque de l'homme du milieu :** Connue en français sous le nom de « man-in-the-middle », une attaque de type man-in-the-middle est une cyberattaque qui interfère avec deux entités communicantes pour intercepter ou altérer les communications et voler des données. Ces entités peuvent être des particuliers, des entreprises et des serveurs. Un attaquant peut se faire passer pour l'une des cibles, se faire passer pour les deux ou rester passif. Ce type d'attaque, également connu sous le nom de MITM, existe depuis longtemps, mais n'est pas aussi répandu que le phishing car il doit cibler la victime ou au moins le réseau.

  Les pirates utiliseront des attaques man-in-the-middle (ou MITM) pour essayer de récupérer les données. Il peut alors les utiliser, les modifier ou les supprimer. Par exemple, ces données pourraient être celles des comptes de messagerie, des comptes bancaires ou des systèmes de messagerie. [55]

11.4.3 Déni de service :

Le déni de service (DoS) se produit lorsqu'un attaquant désactive ou modifie un réseau, un système ou un service dans le but de refuser le service attendu aux utilisateurs ordinaires. Une attaque par déni de service peut désactiver ou ralentir un système au point de le rendre inutilisable. Le déni de service peut inclure aussi simplement la suppression ou la modification d'informations. Dans la plupart des cas, l'attaque se résume à l'exécution d'un programme ou d'un script piraté. C'est pour cette raison que les attaques par déni de service sont les plus redoutées. [56]. Il existe plusieurs types d'attaques de DoS, on peut citer :

- **Déni de service distribué (DDoS) :** Attaquer une ressource en utilisant un botnet, ou un groupe d'ordinateurs contrôlés par une personne, est connu comme le déni de service distribué. [38]

  Ces types d'attaques visent à saturer le réseau avec des données illégitimes, submergeant les liens Internet au point que tout trafic légitime est bloqué.

  Les attaques DDoS utilisent des méthodes similaires aux deux autres attaques Dos, mais elles sont déployées à plus grande échelle. En règle générale, des centaines ou des milliers de points d'attaque tentent de submerger une seule cible. Pour saturer un réseau victime, le principe est d'utiliser plusieurs vecteurs d'attaque et un maître les contrôlant. Les attaquants utilisent des maîtres pour contrôler plus facilement la source. En effet, il nécessite une connexion (en TCP) Laissez le maître configurer et préparer l'attaque. Le maître envoie uniquement des commandes aux sources en UDP. [54]

11.4.4 Le Sniffing :

Le sniffer est un dispositif qui permet d'écouter le trafic réseau et de collecter les informations qui y circulent. Sur un réseau non commuté, les données sont envoyées à toutes les machines du réseau. Cependant, lors d'une utilisation normale, les machines ignorent les paquets qui ne leur sont pas destinés. En utilisant un mode spécifique sur l'interface réseau, il devient possible d'écouter l'intégralité du trafic transitant par l'adaptateur réseau, que ce soit une carte Ethernet ou sans fil. Il est donc essentiel de comprendre les différentes formes d'attaques de reniflement afin de les identifier correctement. [38] Les deux types d'attaques de reniflement les plus courants sont :

- **Sniffing actif :** Dans le sniffing actif, un attaquant manipule un réseau basé sur un commutateur pour obtenir des paquets. La plupart des réseaux utilisent aujourd'hui un commutateur, un appareil qui connecte deux points de terminaison du réseau. Ils utilisent un commutateur pour transférer les données vers un port désigné à l'aide de l'adresse MAC du port (Media Access Control). Un attaquant pourrait exploiter cette vulnérabilité en injectant du trafic dans LAN (réseau local) pour activer le sniffing.

- **Sniffing passif** : Le sniffing passif se produit via un concentrateur ou un réseau sans fil, où l'attaquant utilise l'adresse MAC pour lire le port de destination des données. Contrairement aux renifleurs actifs, ils n'établissent aucune communication directe avec la cible. La plupart des renifleurs de paquets sont difficiles à détecter car ils sont passifs. [57]

11.4.5 L'usurpation d'identité :

C'est une méthode qui implique de mentir sur son adresse IP afin de passer pour quelqu'un d'autre. Il existe différentes méthodes pour y parvenir ; parmi celles-ci, on peut citer :

- **ARP Spoofing :** Le trafic réseau de plusieurs ordinateurs est redirigé par cette attaque vers la machine du pirate. Elle utilise les réseaux physiques des victimes et corrompt la mémoire de la machine Victime. Le pirate aura accès à tout le trafic allant à l'interrupteur de son ordinateur, lui permettant de l'écouter, de le changer, puis d'acheminer les paquets vers leur destination réelle.

- **DNS Spoofing :** Afin d'orienter les internautes vers de faux sites web, le pirate profite des lacunes du système DNS et de sa mise en œuvre sur les serveurs de noms de domaine. Son but est de faire correspondre l'adresse IP d'une machine sous son contrôle à l'URL réelle d'une machine publique. [38]

11.5 Les attaques sur les mots de passe :

11.5.1 Attaque par dictionnaire :

Une attaque de dictionnaire est une méthode utilisée pour accéder à un ordinateur, à un réseau ou à une ressource informatique protégée par mot de passe en utilisant une liste de mots couramment utilisés comme tentatives de mots de passe. Cette technique peut également être employée pour tenter de déchiffrer des communications ou des documents cryptés. Les attaquants exploitent des listes de mots qui incluent souvent des termes largement connus tels que des noms d'animaux, des noms de personnages célèbres ou des informations disponibles publiquement comme les dates de naissance. Les attaques de dictionnaire réussissent souvent en raison de l'utilisation répandue de mots de passe communs. Toutefois, ces attaques échouent généralement lorsque les systèmes utilisent des mots de passe complexes, combinant majuscules, minuscules et chiffres. [58]

11.5.2 Force brute :

Les attaques par force brute sont parmi les moyens les plus fréquents et les plus simples pour les pirates d'accéder aux comptes, ce qui explique pourquoi ils sont si populaires. En vérité, ces types d'attaques par mot de passe seraient impliqués dans 80% des violations de piratage. Afin d'accéder au compte d'un utilisateur, un pirate informatique utilisera un logiciel pour tester chaque lettre, numéro, et symbole combinaison caractère par caractère jusqu'à ce qu'ils trouvent le bon. Ceci est fait méthodiquement, en commençant souvent par les mots de passe les plus populaires, ce qui explique pourquoi "123456" et "mot de passe" prennent moins d'une seconde à déchiffrer. Le programme est généralement automatisé, a la capacité de contourner les restrictions et de prendre en considération les exigences de mot de passe comme un nombre minimum de caractères et l'inclusion d'un nombre ou d'un symbole. [59]

12 Les types d ' attaques :

12.1 Attaque directe :

C'est l'attaque la plus facile à exécuter. Le pirate attaque sa victime directement depuis son ordinateur. La plupart des "script kiddies" utilisent cette technique. En fait, les hacks qu'ils utilisent ne peuvent être que légèrement configurés. De nombreux programmes envoient des paquets directement à la victime. Si vous êtes attaqué de cette manière, vous pourrez très probablement retracer l'attaque jusqu'à sa source et identifier l'attaquant.

Figure II-7: attaque direct.

12.2 Attaque indirect :

- **Attaque par rebond indirect :** C'est la tactique la plus populaire du hacker. Le rebond a en fait deux avantages : masquer l'identité du hacker (adresse IP). Enfin, utilisez les ressources de l'ordinateur intermédiaire pour attaquer puisqu'elles sont plus puissantes (CPU, bande passante, etc.).

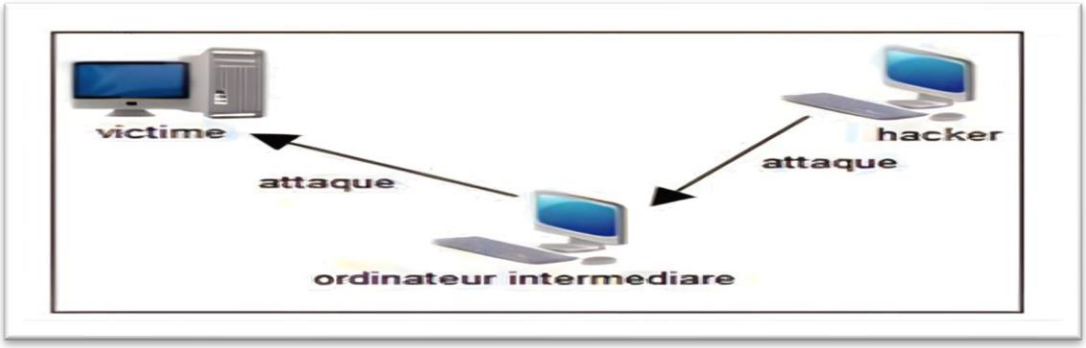


Figure II-8: attaque par rebond indirect.

- **Les attaques indirectes par réponses :** Attaques faites indirectement par des réponses : Cette attaque est une variation de l'attaque par rebond. Du point de vue d'un hacker, elle offre les mêmes avantages. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire

pour qu'il l'exécute, l'attaquant lui enverra une demande. Et l'ordinateur cible recevra cette réponse à la requête. Il est difficile de localiser la cause dans ce cas aussi bien. [60]

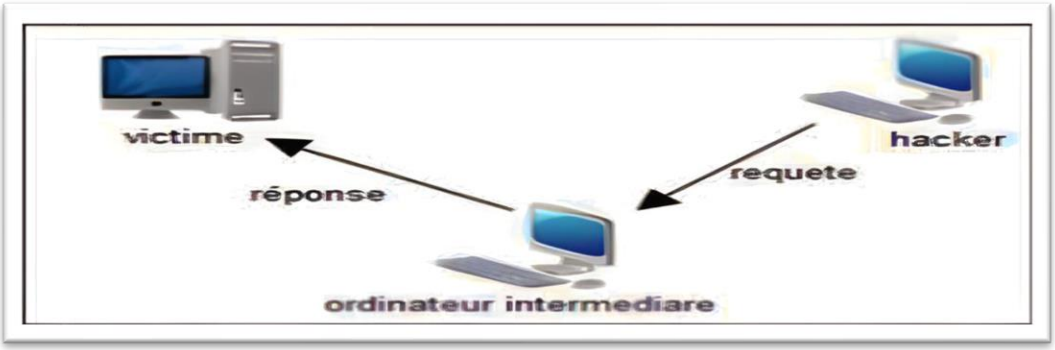


Figure II-9: attaque indirectes par réponses.[61]

13 Les dispositifs de la protection :

Les dispositifs de sécurité se caractérisent par la résolution d'autant de problèmes que possible. Il ne peut pas fournir une protection complète contre toutes les attaques, comme tous les autres systèmes de sécurité, car cela s'est avéré être une tâche difficile jusqu'à présent.

Il existe plusieurs dispositifs de sécurité disponibles qui permettent de protéger à la fois les systèmes et les services qu'ils fournissent. Dans la section qui suit, nous abordons les principaux outils utilisés :

13.1 Norme ISO :

Les normes sont des documents de référence établis volontairement pour couvrir des intérêts industriels ou économiques importants. Elles fournissent des recommandations sur la conception, l'utilisation et l'efficacité des biens, des processus, des services, des systèmes ou des personnes.

L'ISO (Organisation internationale de normalisation) est une organisation mondiale composée de représentants d'organismes nationaux de normalisation de 167 pays. Fondée en 1947, elle produit des normes mondiales dans divers domaines industriels et commerciaux, connues sous le nom de normes ISO. Ces normes sont utiles aux gouvernements, aux organismes de réglementation, aux professionnels, aux fournisseurs, aux clients et aux organisations de tous secteurs. Elles servent également les intérêts du grand public.

Dans le domaine de la sécurité de l'information, l'ISO a créé la famille ISO/IEC 27000 pour les systèmes de gestion de la sécurité de l'information et la sécurité des systèmes d'information. Ces normes internationales comprennent des techniques, des précautions et des bonnes

pratiques reconnues mondialement. Elles sont applicables à toutes les entreprises, indépendamment de leur taille, de leur secteur d'activité ou de leur pays d'origine. [38]

13.2 Formation des utilisateurs :

On considère généralement que la majorité des problèmes de sécurité sont situés entre la chaise et le clavier !

Charte: l'intérêt principal d'une charte d'entreprise a pour objet de définir les règles et les modalités d'utilisation des ressources du système d'information de SONATRACH mises à la disposition des utilisateurs dans le cadre de l'exercice de leurs fonctions. Elle met en évidence leurs droits et obligations ainsi que leurs responsabilités en cas de manquement au respect de la présente charte, tout en les informant des mesures de contrôle et de supervision mises en place, dans le souci de préserver la sécurité, l'intégrité et la performance du système d'information de la Société. La présente charte vise à préserver le système d'information, règlementer l'usage de ses ressources et sensibiliser les utilisateurs pour une utilisation conforme aux bonnes pratiques à même de pérenniser son intégrité face aux abus et aux cyberattaques.

13.3 Audit de sécurité :

L'audit de sécurité du réseau fournit une image complète du réseau sous la forme d'un rapport détaillé qui fournit un instantané en temps réel de l'état du réseau. En utilisant des filtres dans les rapports, il est possible d'analyser les résultats du balayage et de prendre des mesures de sécurité proactives pour sécuriser le réseau, comme la fermeture des ports ouverts, la suppression des comptes d'utilisateurs inutilisés ou la désactivation des points d'accès sans fil.

Journalisation :

Le but de la journalisation est de suivre les connexions et les activités en ligne de chaque acteur. En fait, la journalisation d'événements (journaux) est un outil crucial pour gérer la sécurité du système plus généralement ainsi que la sécurité des réseaux. Les revues sont une riche source d'information qui peut être utilisée pour déterminer si des attaques ont eu lieu, les analyser et peut-être prendre des mesures pour en prévenir d'autres.

13.4 Les antivirus :

Un programme antivirus est un logiciel dont le but principal est de protéger un ordinateur contre diverses infections informatiques comme les virus. Les logiciels antivirus peuvent à la fois détecter la présence de virus sur un ordinateur et les supprimer aussi complètement que possible s'ils sont découverts. [62]

13.5 Pare feu :

Un programme logiciel ou un système physique qui régule les connexions réseau est connu comme un pare-feu. Il protège un réseau privé contre les incursions provenant d'un réseau externe, comme Internet, en filtrant les communications de logiciels malveillants. Conformément aux règles établies, le pare-feu est également chargé d'appliquer la politique de sécurité du réseau en autorisant ou bloquant des communications spécifiques.

Une interface externe spécifique au réseau est utilisée par un pare-feu pour filtrer les paquets de données entrant et sortant d'un réseau protégé. Il ne peut toutefois pas assurer la protection contre les erreurs internes ou les attaques externes, qui constituent la majorité des problèmes de sécurité. [54]

14 Conclusion :

Ce chapitre a mis en évidence les notions fondamentales de sécurité dans les réseaux informatiques et souligné l'importance des stratégies de sécurité pour faire face aux attaques. La sécurité informatique est essentielle pour assurer la survie et la fiabilité d'un réseau informatique.

Le prochain chapitre portera sur le contexte métier et l'articulation de notre solution.

CHAPITRE III

Analyse et Conception

1 Introduction :

Dans le troisième chapitre d'analyse et de conception, nous donnerons la description et les objectifs du projet et toutes les exigences fonctionnelles à suivre.

Dans la deuxième partie, nous nous concentrons davantage sur la modélisation, l'analyse et la conception à l'aide d'UP.

UML (Unified Modeling Language) est un langage graphique de modélisation des systèmes d'information. Il fournit une notation standardisée pour représenter visuellement différents aspects d'un système, tels que les classes, les objets, les relations et les activités. UML permet de communiquer et de documenter les informations relatives à ces éléments à l'aide d'un texte explicatif.

La conception est la phase de description de la structure, du comportement et de l'architecture d'un système, et elle est utilisée pour présenter différentes perspectives du système.

Dans la dernière section, nous avons élaboré quelques diagrammes d'activités et des diagrammes de classes.

2 Etude de l’existent :

Les cyberattaques étant de plus en plus fréquentes et sophistiquées, la sécurité de l’information est devenue une préoccupation majeure pour les entreprises. Diverses solutions de sécurité et de protection ont été élaborées par les entreprises pour contrer cette menace. Ces solutions vont de la mise en place de politiques de sécurité informatique à l’utilisation de logiciels de sécurité en passant par la formation des membres du personnel et la sensibilisation aux risques pour la sécurité.

Toute entreprise qui veut protéger ses données et ses renseignements confidentiels contre les cyberattaques doit accorder la priorité à la sécurité des technologies de l’information. Dans cette situation, D-LAB fournit à ses utilisateurs une variété de solutions de sécurité, y compris SEPM (Symantec Endpoint Protection Manager), un programme de sécurité intégré dans la direction générale(DG) de SONATRACH, et Symantec Antivirus. Pour assurer la meilleure défense possible contre les attaques informatiques, il y a encore quelques vulnérabilités à fermer malgré ces outils de sécurité. Dans cette partie, nous examinerons les solutions de sécurité actuellement disponibles et les mesures qui peuvent être prises pour améliorer la protection.

2.1 Solutions existantes:

Il existe de nombreuses solutions de sécurité informatique dans D-LAB pour répondre aux différents besoins et menaces, voici quelques-unes des principales :

- **Antivirus(Symantec) :** Les menaces avancées et les attaques intelligentes obligent aujourd'hui les entreprises à sécuriser leurs infrastructures informatiques. Pour protéger les données de l'entreprise contre les cybermenaces, Symantec propose des solutions de sécurité avec des fonctionnalités de surveillance et de protection intégrées. La protection des données sensibles contre les menaces de sécurité peut être massivement assistée par Symantec Antivirus.

- **SEPM (Symantec Endpoint Protection Manager) :** Symantec Endpoint Protection Manager (SEPM) est une solution de sécurité informatique proposée par Symantec pour les entreprises de toutes tailles. Un programme de sécurité intégré dans la direction générale(DG) de SONATRACH Il s'agit d'une plateforme de gestion de la sécurité qui permet de protéger les ordinateurs, les serveurs et les appareils mobiles contre les menaces informatiques telles que les virus, les logiciels malveillants, les ransomwares et les attaques de phishing.

  SEPM fonctionne en utilisant un agent de sécurité qui est installé sur les appareils protégés. L'agent collecte les informations de sécurité et les envoie à la console d'administration centrale, où les administrateurs peuvent gérer les politiques de sécurité, les mises à jour et les rapports de sécurité. La console permet également de configurer des alertes de sécurité pour informer les administrateurs en cas d'activité suspecte.

  Les poste client sont gérés par l'antivirus Symantec Endpoint Protection Manager (SEPM).

- **SCCM (System Center Configuration Manager) :** est un outil de gestion de la configuration et des mises à jour pour les systèmes d'exploitation Windows et les applications Microsoft intégré dans la direction générale(DG) de SONATRACH. Il permet une gestion centralisée des mises à jour de sécurité, des correctifs logiciels, des configurations système et de la distribution des logiciels. SCCM permet aux administrateurs informatiques de déployer et de gérer efficacement les mises à jour de sécurité sur un grand nombre de machines en même temps, réduisant ainsi le temps et les ressources nécessaires pour effectuer ces tâches manuellement. En outre, SCCM permet de gérer de manière

centralisée les configurations système, les paramètres de sécurité et les applications installées sur les machines, ce qui facilite la maintenance des systèmes informatiques dans les entreprises.

- **Systèmes de gestion des identités et des accès (Active directory) :** La gestion des droits d'accès et des permissions sur les données sensibles de l'entreprise est un rôle important joué par Active Directory en matière de protection des données. Il peut spécifiquement limiter l'accès aux données confidentielles uniquement par les utilisateurs autorisés, ainsi que restreindre l'accès à partir de certaines régions géographiques ou appareils. Les dossiers partagés, Authentification, l'accès aux réseaux sont contrôles et sécurises par l'active directory.

- **Symantec backup :** L'existence de Symantec Backup au niveau de D-LAB protège les données. Symantec Backup enregistre et récupère les données en cas de panne du système, de perte de données ou de destruction de données. Le logiciel peut effectuer automatiquement des sauvegardes complètes, incrémentielles.

  Symantec Backup protège les données en les stockant sur des supports de stockage externes comme des disques durs ou des bandes de sauvegarde. Si le système plante, le logiciel peut rapidement restaurer les données.

  Symantec Backup à D-LAB assure la disponibilité des données et la protection contre les pertes et les dommages. La combinaison de cette technologie avec d'autres mesures de sécurité comme des mises à jour régulières et la surveillance des activités suspectes réduit les risques d'atteinte à la protection des données et d'interruption des activités.

- L'internet est contrôlé par le pare-feu au niveau de la direction générale (DG).

2.2 Les critiques des solutions existantes:

Malgré les améliorations constantes des solutions de sécurité, il existe toujours quelques vulnérabilités qui peuvent inaperçues, laissant ainsi les systèmes et les données vulnérables aux attaques tel que :

- **Optimisation des ressources :** La direction générale de l'entreprise utilise un pare-feu pour protéger l'ensemble du réseau, y compris plusieurs divisions telles que D-LAB

(division laboratoire). La direction générale propose une solution pour optimiser les ressources de l'entreprise, mais cette solution présente des difficultés et peut exposer la division D-LAB aux risques de cyberattaques. Il est donc essentiel de tenir compte des besoins de sécurité de chaque division et de mettre en place les outils appropriés. La stratégie de la direction générale consiste à minimiser les accès à Internet en utilisant un pare-feu au niveau de sortie pour filtrer le trafic entrant. Cependant, il est important de noter que le pare-feu du DG ne protège pas contre les menaces internes causées par des employés malveillants ou des erreurs humaines. Ainsi, la division D-LAB doit mettre en œuvre des mesures de sécurité interne telles que la formation en sécurité informatique, l'utilisation de mots de passe forts et la surveillance des activités des utilisateurs. Le pare-feu est une mesure cruciale, mais d'autres mesures de protection doivent être mises en place pour assurer une protection complète contre les menaces.

- **Les mise à jour manuelle :** Il est important de garder son système à jour avec les dernières mises à jour de sécurité et de stabilité pour éviter les vulnérabilités et les bugs qui pourraient nuire à la performance de votre ordinateur ou compromettre la sécurité de vos données. C'est pourquoi il est recommandé de vérifier régulièrement les mises à jour disponibles pour le système d'exploitation et les installer dès que possible. Il est impossible de gérer les mises à jour manuelles lorsque plusieurs postes de travail sont utilisés dans une organisation. Dans cette situation, il est conseillé d'utiliser des outils de gestion des mises à jour pour simplifier la procédure.

- **Manque de la visibilité sur le réseau :** Le manque de visibilité sur le réseau peut être un problème pour les entreprises car il peut rendre la surveillance et le contrôle de l'activité du réseau plus difficile. Sans une bonne visibilité, il peut être difficile d'identifier les menaces potentielles, les failles de sécurité, les erreurs et les problèmes de rendement**.**

- **La disponibilité:** La disponibilité des systèmes informatiques est un facteur essentiel pour assurer leur sécurité. Afin d'optimiser les ressources, les entreprises réduisent fréquemment le nombre d'équipes dédiées à la sécurité de l'information. Cela peut être représenté par une seule équipe qui gère la sécurité au niveau de l'entreprise et doit inclure toutes les divisions de l'entreprise, y compris les laboratoires tels que D-LAB.

Bien que cette approche puisse sembler efficace d'un point de vue financier, elle peut avoir des conséquences négatives sur la sécurité du système. En effet, la sécurité de l'information est un domaine complexe et en constante évolution qui exige des connaissances spécialisées et une surveillance continue. Une seule équipe peut avoir de la difficulté à suivre les progrès technologiques, les nouvelles menaces et les vulnérabilités, ainsi qu'à assurer une surveillance continue des systèmes informatiques de l'entreprise. De plus, si cette équipe devait faire faillite ou s'absenter, l'entreprise pourrait devenir vulnérable aux attaques de sécurité**.**

2.3 Solutions proposées :

La cyberattaque est un enjeu majeur pour l'entreprise, en particulier dans l'environnement informatique actuel. Les systèmes informatiques modernes sont pleins de bogues, donc si l'une des vulnérabilités cachées est exploitée, cela peut entraîner de graves conséquences. L'attaquant peut accéder au système en exploitant une faille dans le système d'exploitation ou le logiciel d'application. Malheureusement les entreprises sont piratées chaque année, ce qui est très dommageable pour les entreprises. Les moyennes de Protections existantes assurer un pourcentage % de protection contre les cyberattaques et c'est pourquoi nous avons créé ce système pour augmenter la protection, réduire les menaces et limiter le risque environnemental dans l'entreprise.

Afin de faire face aux attaques informatiques de plus en plus sophistiquées, il est crucial de mettre en place des mesures de sécurité efficaces. Une solution prometteuse consisterait à développer une plateforme capable de gérer les alertes et les mises à jour automatiques en temps réel. Cette plateforme pourrait détecter les attaques et envoyer des alertes au pare-feu qui assure la protection contre ces attaques

Une amélioration de la gestion des alertes et des mises à jour peut être réalisée en intégrant des outils tels que Symantec Endpoint Protection Manager (SEPM) et System Center Configuration Manager (SCCM). SEPM permet de gérer les politiques de sécurité et de surveiller en temps réel les événements liés à la sécurité, tandis que SCCM permet de gérer les mises à jour et les configurations des ordinateurs et des serveurs de manière centralisée. De plus, l'utilisation d'un outil de scan de vulnérabilité comme ScanPod peut être ajoutée pour identifier les éventuelles failles de sécurité dans les systèmes et les applications.

Pour renforcer la sécurité des systèmes informatiques, il est également possible d'ajouter Symantec Backup Exec pour la sauvegarde distante et la restauration des données, les fichiers

vitaux et sensibles doivent être sauvegardés à distance. Les sauvegardes régulières peuvent réduire la perte de données à la suite d'une défaillance du disque dur, du piratage ou de catastrophes naturelles. Le stockage à distance des fichiers de sauvegarde les protège contre les dommages physiques comme les incendies ou les inondations qui pourraient endommager les fichiers locaux. Ainsi que d'implémenter un pare-feu robuste. Le pare-feu peut bloquer les tentatives d'intrusion et protéger les réseaux contre les attaques malveillantes.

Il est crucial d'informer les utilisateurs sur l'importance de protéger les informations de l'entreprise en suivant les directives de la charte informatique. La création de mots de passe uniques et solides pour chaque compte, ainsi que la responsabilité de les protéger, est un aspect clé de cette charte. Les utilisateurs doivent être conscients de l'importance de ne jamais partager leurs mots de passe avec quiconque et d'éviter de les stocker sur des documents ou des appareils non sécurisés. La protection des mots de passe est essentielle pour éviter les violations de données. En suivant les meilleures pratiques de la charte informatique, les utilisateurs peuvent aider à garantir la sécurité des données de l'entreprise et protéger leur propre information personnelle.

Il est important de contrôler et de surveiller les dossiers de partage afin de protéger les données sensibles. Les audits réguliers permettent d'identifier les risques potentiels et de mettre en place des mesures de sécurité appropriées pour prévenir l'accès non autorisé. Il est également essentiel de suivre l'historique des dossiers partagés pour détecter toute activité suspecte ou non autorisée. Le balayage régulier des dossiers partagés peut aider à identifier les logiciels malveillants ou les virus qui pourraient compromettre la sécurité des données sensibles. Ces mesures de contrôle et de surveillance permettent aux entreprises de protéger efficacement leurs données sensibles et de réduire les risques de violation de sécurité.

Les autorisations et les droits d'accès sont des éléments clés pour assurer la sécurité des données d'entreprise. Les autorisations déterminent quels utilisateurs et groupes ont accès à des ressources spécifiques, telles que des fichiers, des dossiers et des applications. Les droits d'accès définissent le niveau d'accès pour chaque utilisateur ou groupe, tel que lecture, écriture ou suppression. Il est important de définir et de gérer correctement les autorisations et les droits d'accès pour s'assurer que seuls les utilisateurs autorisés peuvent accéder aux données sensibles. Les autorisations et les droits d'accès doivent être accordés en fonction des besoins de chaque utilisateur ou groupe et revus périodiquement pour s'assurer qu'ils restent appropriés. Les

employés qui quittent l'entreprise doivent immédiatement voir leurs privilèges et leur accès révoqués pour éviter les failles de sécurité.

Le cryptage des données est une mesure de sécurité essentielle pour protéger les données sensibles contre les failles de sécurité. Les données doivent être cryptées à la fois en stockage et en transit. Le chiffrement consiste à convertir les données dans un format illisible sans la clé de déchiffrement appropriée. Les algorithmes de chiffrement doivent être choisis avec soin pour assurer la sécurité des données. Il est recommandé d'utiliser un algorithme de cryptage fort tel que AES (Advanced Encryption Standard) qui est largement utilisé pour protéger les données sensibles. Le chiffrement des données aide à empêcher les cybercriminels d'accéder à des informations sensibles, même s'ils sont capables de contourner d'autres mesures de sécurité. Par conséquent, le cryptage doit être utilisé comme mesure de sécurité de base pour protéger les données sensibles dans les entreprises.

3 Description du projet :

Le projet vise à concevoir et développer un système de protection des données sensibles de l'entreprise. L'objectif principal de ce projet, intitulé "conception d'un système de protection des données sensibles", est de réaliser une application web.
Notre application est conçue pour protéger les données sensibles et les précieuses ressources numériques contre les accès non autorisés et les utilisations inappropriées. Pour assurer la confidentialité, l'intégrité et la disponibilité des données sensibles, ces programmes offrent des mesures de sécurité avancées.

3.1 Objectifs :

Notre projet est axé sur la réalisation d'une application Web sécurisée et fiable. L'objectif principal de ce projet est de mettre en place des mesures de sécurité avancées afin de protéger les données sensibles de l'entreprise contre les accès non autorisés et les utilisations inappropriées.

Les objectifs clés du projet sont les suivants :

- **Protection des dossiers :** L'un des objectifs principaux est de mettre en œuvre des mécanismes de protection robustes pour garantir la sécurité des dossiers contenant des données sensibles. Cela implique de mettre en place des stratégies de contrôle d'accès, de chiffrement des données et de détection des intrusions.

- **Sauvegardes régulières :** Un aspect essentiel de la protection des données sensibles est d'établir des processus de sauvegarde réguliers. Cela permet de créer des copies de sauvegarde des données sensibles afin de les restaurer en cas de perte ou de dommage. Les sauvegardes régulières garantissent la disponibilité des données en cas de besoin.

- **Gestion des autorisations :** Un autre objectif important est de mettre en place un système de gestion des autorisations afin de contrôler l'accès aux données sensibles. Cela comprend l'attribution de droits d'accès appropriés aux utilisateurs et la limitation des privilèges en fonction des rôles et des responsabilités.

- **Mises à jour des applications :** Il est essentiel de maintenir les applications utilisées pour traiter les données sensibles à jour. Cela inclut l'installation régulière de correctifs de sécurité et de mises à jour logicielles pour combler les vulnérabilités connues et renforcer la résistance aux attaques.

- **Mises à jour des hôtes :** Outre les mises à jour des applications, il est tout aussi important de maintenir les systèmes d'hébergement à jour. Cela comprend l'application régulière des mises à jour fournies par les fournisseurs de systèmes d'exploitation et de matériel pour garantir la stabilité et la sécurité du système.

- **Surveillance des attaques et des vulnérabilités :** Une autre priorité est de mettre en place des mécanismes de surveillance pour détecter les attaques potentielles et les vulnérabilités du système. Cela permet une réponse proactive aux incidents de sécurité et une mitigation rapide des risques.

En atteignant ces objectifs, notre projet visera à fournir un système de protection des données sensibles solide et fiable, renforçant ainsi la confiance des utilisateurs et la sécurité de l'entreprise.

4 Démarche de développement :

Un projet informatique, quelle que soit sa taille et la portée de ses objectifs, nécessite la mise en place d'un planning organisationnel tout au long de son cycle de vie.

Afin de réaliser notre travail, nous avons utilisé UML comme un langage de modélisation et UP(Unified Process) comme une démarche d'Analyse des besoins et de conception de notre application.

4.1 UML :

UML (Unifier Modeling Language) est un langage graphique standardisé qui nous permet de représenter visuellement les différents composants d'un système tels que les entités, les interactions et les flux de données. En utilisant UML, nous pouvons communiquer efficacement des concepts et des idées entre les membres de l'équipe et les parties prenantes, favorisant ainsi la compréhension et la collaboration.

4.2 Le Processus Unifié :

UP (Unified Process), est une méthodologie de développement logiciel itérative et incrémentale qui guide le processus d'analyse des besoins, de conception et de développement de notre application. UP se divise en phases clés, notamment l'élaboration, la construction, la transition et la production, qui nous permettent de planifier, de concevoir, de développer et de mettre en œuvre notre application de manière itérative.

5 Expression des besoins :

5.1 Exigences fonctionnelles :

- **Login :** permet aux utilisateurs et administrateurs d'accéder à leurs profils en fournissant leurs informations personnelles (nom utilisateur, nom administrateur, mot de passe) L'utilisateur ou l'administrateur peut vérifier son identité et accéder à des fonctionnalités spécifiques à sa position en saisissant des informations de connexion telles que l'état (utilisateur ou administrateur) et le mot de passe. Cette procédure de connexion offre une protection supplémentaire en décourageant l'accès non autorisé aux données sensibles et aux informations de profil.

- **Authentification :** L'authentification permet aux utilisateurs d'accéder aux application web et de bénéficier de leurs fonctionnalités, jouant un rôle essentiel dans la protection de la confidentialité des données.

- **Demande dossier :** Après l'authentification, les utilisateurs ont la possibilité de soumettre des demandes de dossier en fonction de leurs besoins individuels en matière de protection

des données et de sauvegarde. Grâce à cette possibilité de demander des protections des dossiers, les utilisateurs peuvent garantir une élégante protection et sauvegarde de leurs informations ce qui renforce la confiance et la satisfaction des utilisateurs dans le système.

- **Demande applicative :** Après l'authentification les utilisateurs a la possibilité de soumettre des demandes d'application, en fonction des différents types d'applications disponibles. Ces demandes peuvent inclure l'installation de nouvelles applications, ainsi que des mises à jour régulières des applications existantes et des logiciels. Cette fonctionnalité permet aux utilisateurs de maintenir à jour leurs environnements applicatifs, garantissant ainsi un fonctionnement optimal et sécurisé de leurs systèmes.

- **Suivre demande :** En tant qu'utilisateur authentifié, je peux consulter mes demandes (dossier, applicative) à tout moment, même avant de recevoir la demande par l'administrateur. Cette fonctionnalité me permet d'avoir un aperçu des demandes en attente et de suivre activement leur progression.

- **Traiter la demande :**

  - **Dossier** : Les demandes sont traitées pour assurer la protection des dossiers, ce qui implique d'autorisations appropriées pour limiter l'accès au personnel autorisé uniquement. De plus, des procédures de sauvegarde régulières doivent être établies pour garantir la préservation des données en cas de problème ou de perte.

  - **Applicative** : Les demandes sont traitées pour assure efficacement les demandes liées à l'installation des applications, ainsi que les mises à jour régulières des applications et des correctifs. Afin d'assurer la réception des demandes des utilisateurs, nous évaluons leur pertinence et leur faisabilité avant de procéder à l'installation des applications nécessaires. De plus, la gestion des patchs garantit qu'ils sont appliqués de manière appropriée pour assurer la stabilité du système.

- **Vérification :**

  - **Attaque :** Une autre équipe est chargée de la détection des attaques sur le système, en surveillant en permanence l'activité du réseau et les journaux de sécurité afin d'identifier toute activité suspecte ou tentative d'intrusion. Lorsqu'une attaque est détectée, cette équipe prend des contre-mesures immédiates pour contrer l'attaque et protéger le

système. Ainsi saisir toutes les informations de la détection et contre mesure sue l'application tel que le numéro de port.

- **Vulnérabilité :** Une autre équipe est chargée de détecter les vulnérabilités des hôtes. Il effectue régulièrement des analyses et des tests de sécurité pour identifier les éventuelles faiblesses des systèmes et des applications qu'il gère. Une fois qu'une violation est détectée, des mesures de protection sont mises en place pour réduire le risque. Saisissant ainsi toutes les informations de la vulnérabilité sur l'application

➢ **Modification mot de passe :** Les utilisateurs et administrateurs disposent de droits sur leurs informations personnelles, ce qui leur permet de les modifier à tout moment, leur mot de passe.

5.2 Identification des acteurs (les cas d'utilisations) :

Nous répondrons aux questions suivantes : Quels sont les utilisateurs et les administrateurs utilisent le système ? Il est essentiel d'identifier les acteurs impliqués dans le système ainsi que les cas d'utilisation correspondants, qui représentent les différentes fonctionnalités du système :

- **L'utilisateur :** personne qui possède un compte, qui peut demander, traiter ses demande (dossier, applicative) ainsi que modifier son mot de passe.
- **Admin dossier :** est une personne qui possède un compte et a accès à des dossier pour la protection et la sauvegarde.
- **Admin applicative :** est une personne qui possède un compte et a accès d'un applicative pour l'installation et les mise à jour des applications et des patchs.
- **Admin monitoring :** L'équipe responsable du compte est spécialisée dans la détection des attaques, la contre-attaque et la détection des vulnérabilités de l'hôte, tout en assurant une protection adéquate.

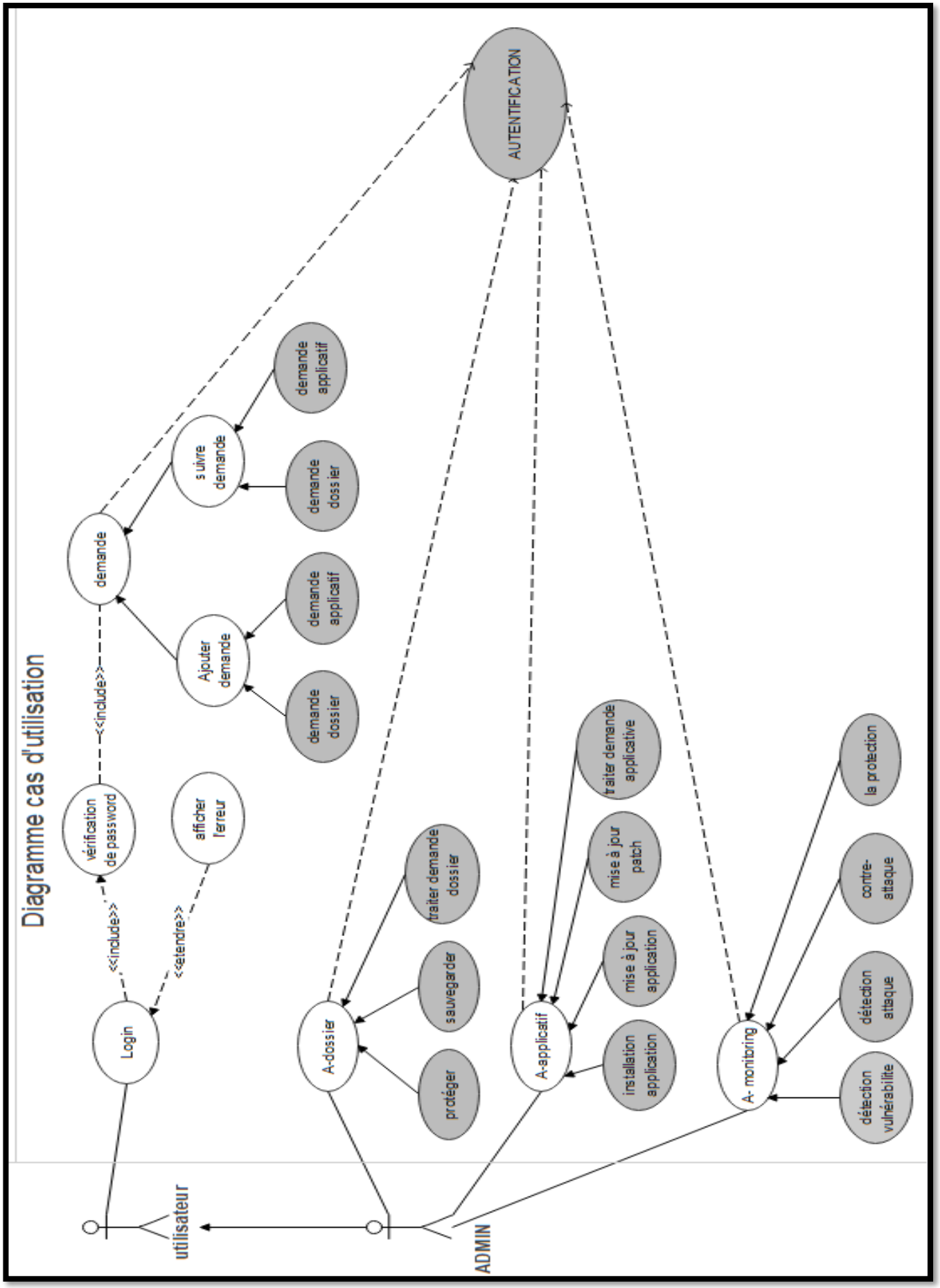


Figure III-10: Le diagramme des cas d'utilisation.

6 Analyse et conception :

Passons maintenant à l'analyse et à la conception du projet. Nous débuterons par la modélisation dynamique, qui comprendra plusieurs diagrammes d'activités. Ensuite, nous aborderons la modélisation statique, qui inclura le dictionnaire de données, le diagramme de classes et le modèle logique de données. Cette approche nous permettra d'avoir une vision complète et détaillée de la structure et du fonctionnement de notre système.

6.1 Modélisation dynamique :

Pour modéliser la partie dynamique de notre système, nous devrions représenter graphiquement les étapes séquentielles du processus, en mettant l'accent sur les activités, les actions et les décisions qui composent le système, qui est généralement illustrée dans les diagrammes d'activités.

6.1.1 Diagrammes d’activités :

Nous allons présenter le diagramme d’activité générale et quelques cas d’utilisation :

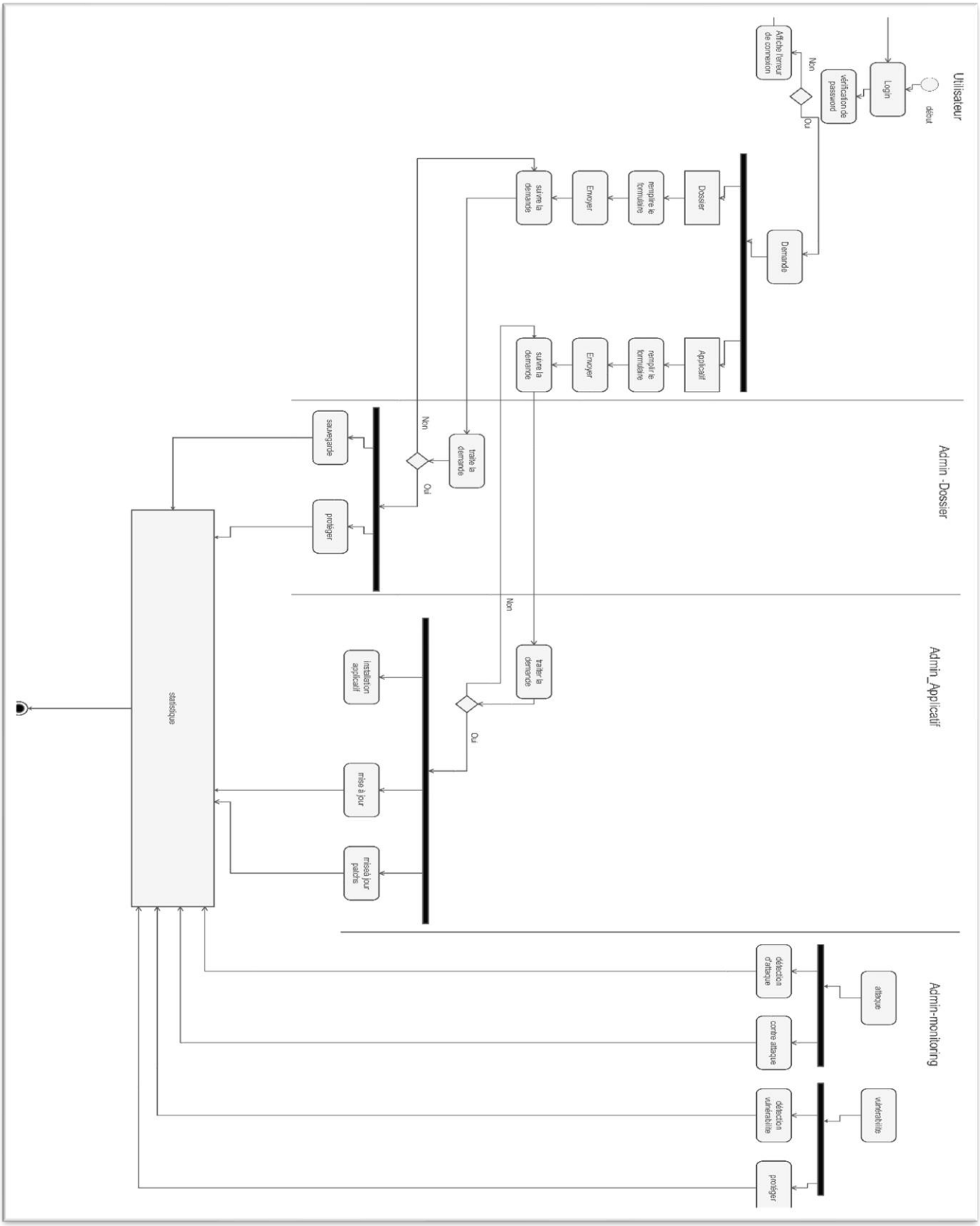


Figure III-11: Diagramme d'activité générale.

- **Authentification :**

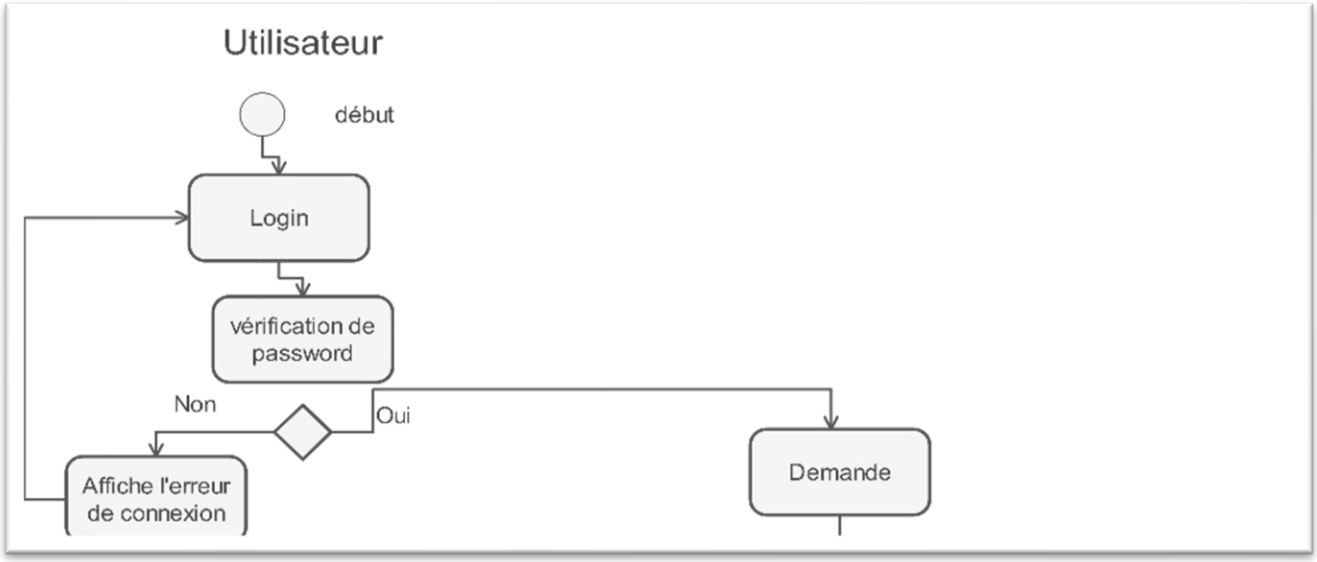


Figure III-12 : Diagramme d'activité de cas s'authentifier.

- **Ajouter et suivre nouvelle demande de protection (dossier, applicatif)**

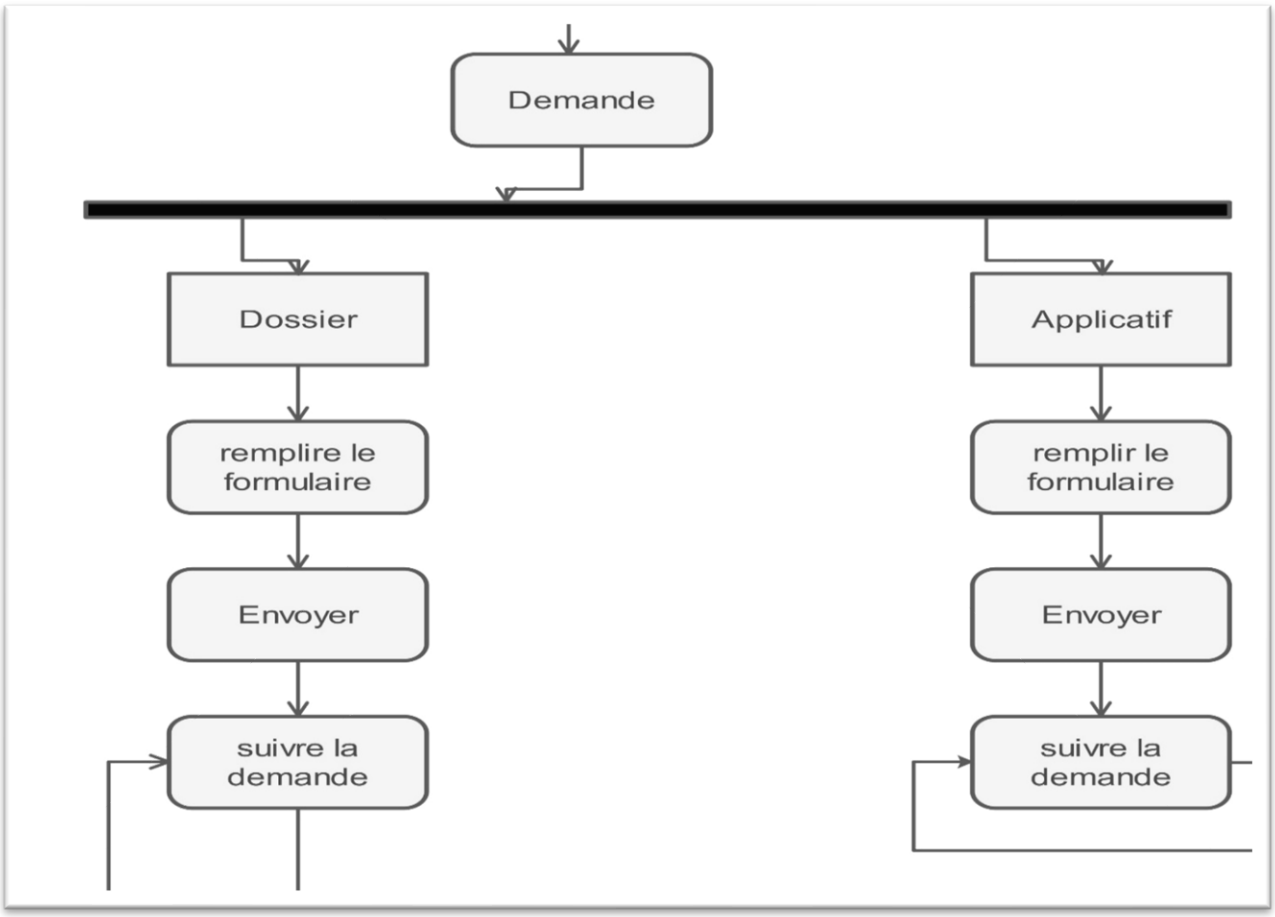
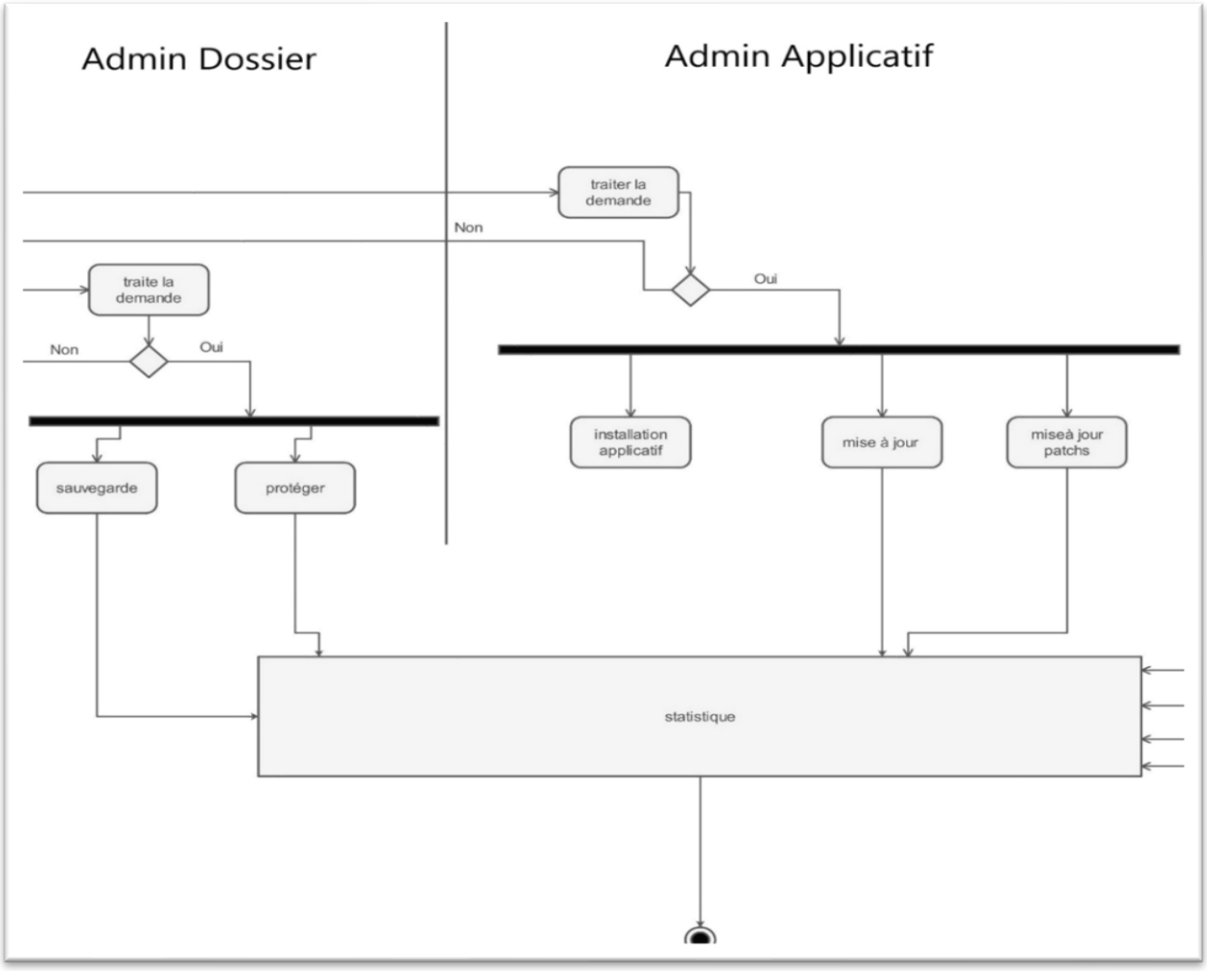
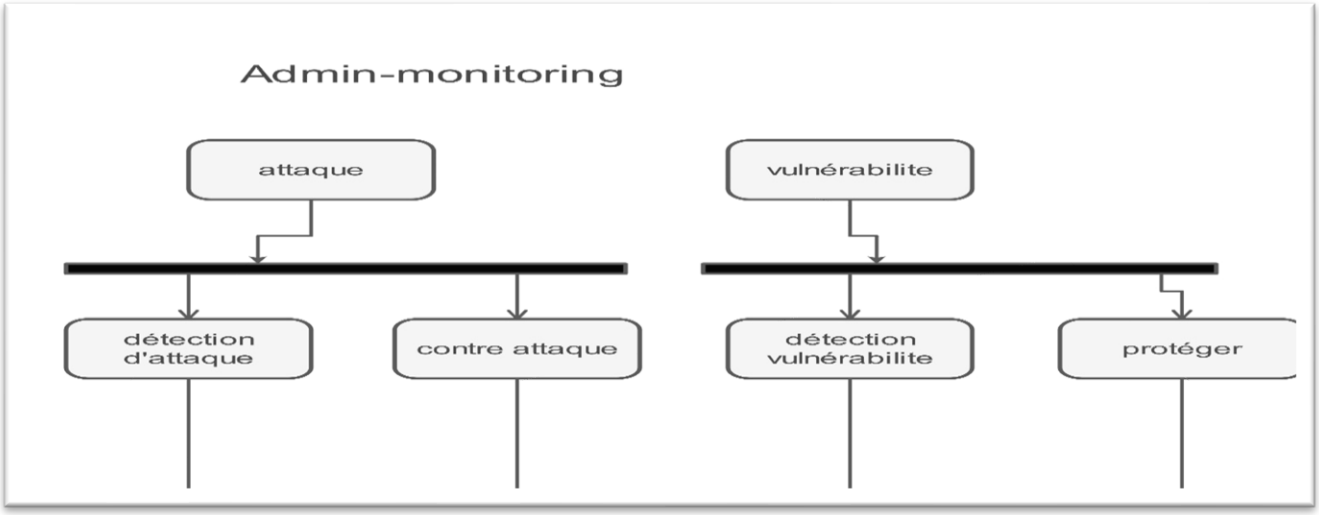


Figure III-13 :Diagramme d'activité de cas ajouter et suivre un nouvel demande.



- **Traiter les demandes (dossier, applicatif) :**

Figure III-14: Diagramme d'activité de cas traiter les demandes .



- **Surveillance et protection (attaque, vulnérabilités) :**

Figure III-15 : Diagramme d'activité de cas surveillance et protection.

6.2 Modélisation statique :

Pour modéliser la partie statique du système, la première étape consiste à implémenter le dictionnaire de données présenté ci-dessous et le modèle de données logiques dérivé du diagramme de classes conçu.

6.2.1 Dictionnaire de données :

Avant de pouvoir réaliser le diagramme de classe, on doit d'abord définir le dictionnaire de données illustré ci-dessous :

Classe	Définition de l'attribut	Attribut	Type
Admin	Identifiant d'admin	id	Numérique
	Le rôle d'administrateur	rôle	Texte
	Nom de la personne	nom	Texte
	Matricule de la personne	MLE	Texte
Applicatif	Identifiant d'applicatif	id	Numérique
	Nom applicatif	nom_app	Texte
	Groupe d'applicative	gr_host	Texte
	Identifiant d'admin	Admin_id	Numérique
	Identifiant de host	host_id	Numérique
	Mise à jour	majr	Texte
Attaque	Identifiant d'attaque	Id	Numérique
	Nom d'attaque	nom	Texte
	Identifiant de host	host_id	Numérique
	Date d'intervention	date_intervention	Date
	Identifiant d'admin	admin_id	Numérique
	login	login	Texte
	Etat d'attaque	etat	Texte
	Port d'attaque	port	Texte
Demande	Identifiant de la demande	id	Numérique
	Identifiant d'utilisateur	utilisateur_id	Numérique

	Nature de la demande	Nature	Texte
	Nom de répertoire	nom_rep	Texte
	Nom d'applicatif	nom_app	Texte
	Identifiant de répertoire	Rep_id	Numérique
	Identifiant d'applicatif	App_id	Numérique
	Autorisation de la demande	Autorisation	Texte
	Date de demande	date_dem	Date
	Heurs de demande	time	Texte
	Traitement de la demande	traiter	Texte
	Login	login	Texte
	Date d'intervention	date_intervention	Date
	Tache de réalisation de la demande	Tache_realiser	Texte
Dossier	Identifiant de répertoire	id	Numérique
	Nom de répertoire	nom_rep	Texte
	Identifiant demande	demande id	Numérique
	Identifiant d'administrateur	Admin_id	Numérique
	Identifiant de sauvegarde	Sauv_id	Numérique
	Les droit de demandeur	Droits	Texte
	Chemin de dossier	Chemin	Texte
	Protection de dossier	Protection	Texte
	Chiffrement de dossier	Chiffrement	Texte
	Date de lancement de la demande	Date de lancement	Date
	Date d'intervention	Date d'intervention	Date
Hosts	Identifiant de host	id	Numérique
	Nom de host	nom_host	Texte
	Groupe des hosts	Gr_host	Texte
	Type de vulnérabilités	Type_vul	Texte
	Identifiant d'administrateur	Admin_id	Numérique
	Identifiant d'attaque	Attaque_id	Numérique
	Mise à jour	maj	Texte
Login	Nom de la personne	username	Texte

	Mot de passe d'authentification	password	Texte
	Rôle d'authentificateur	role	Texte
	Identifiant d'utilisateur	utilisateur_id	Numérique
Patchs	Identifiant de patch	id	Numérique
	Nom de patch	nom_patch	Texte
	Type de système	type_systeme	Texte
	Date d'intervention	date_ intervention	Date
	Identifiant de host	host_id	Numérique
	Identifiant d'applicatif	app_id	Numérique
	Mise à jour	majr	Texte
	Identifiant d'administrateur	admin_id	Numérique
Sauvegarde	Identifiant de sauvegarde	id	Numérique
	Identifiant de dossier	dossier _id	Numérique
	Type de sauvegarde	type_sauvegarde	Texte
	Etat	etat	Texte
	1ère Chemin de sauvegarde	chemin 1	Texte
	2éme Chemin de sauvegarde	chemin 2	Texte
	Identifiant d'administrateur	admin_id	Numérique
	Heure de sauvegarde	time	Texte
	Login	login	Texte
	Date d'intervention	date_intervention	Date
Utilisateur	Identifiant d'utilisateur	id	Numérique
	Login	login	Texte
	Mot de passe	pw	Texte
	Rôle de l'utilisateur	rôle	Texte
	MLE de l'utilisateur	MLE	Texte
	Nom de compte	nom_compte	Texte
	Nom de l'utilisateur	Nom	Texte
	Prénom de l'utilisateur	prenom	Texte
	Nom de service de l'utilisateur	nom_service	Texte
	Profil de l'utilisateur	profil	Texte
	Adresse email de l'utilisateur	E_mail	Texte

	Responsable de l'utilisateur	responsable	Texte
Vulnérabilités	Identifiant de vulnérabilités	id	Numérique
	Type de vulnérabilités	type	Texte
	Système	systeme	Texte
	Etat de vulnérabilités	etat	Texte
	Identifiant de host	host_id	Numérique
	Date d'intervention	date_intervention	Date
	Identifiant d'administrateur	admin_id	Numérique
	Login	login	Texte
	Heure de vulnérabilité	time	Texte
	Chemin de vulnérabilités	chemin	Texte

Tableau III-2 : Dictionnaire de données.

6.2.2 Diagramme de classe :

Dans cette partie, nous étudierons les entités statiques du système. Ceci est illustré par le diagramme de classes suivant :

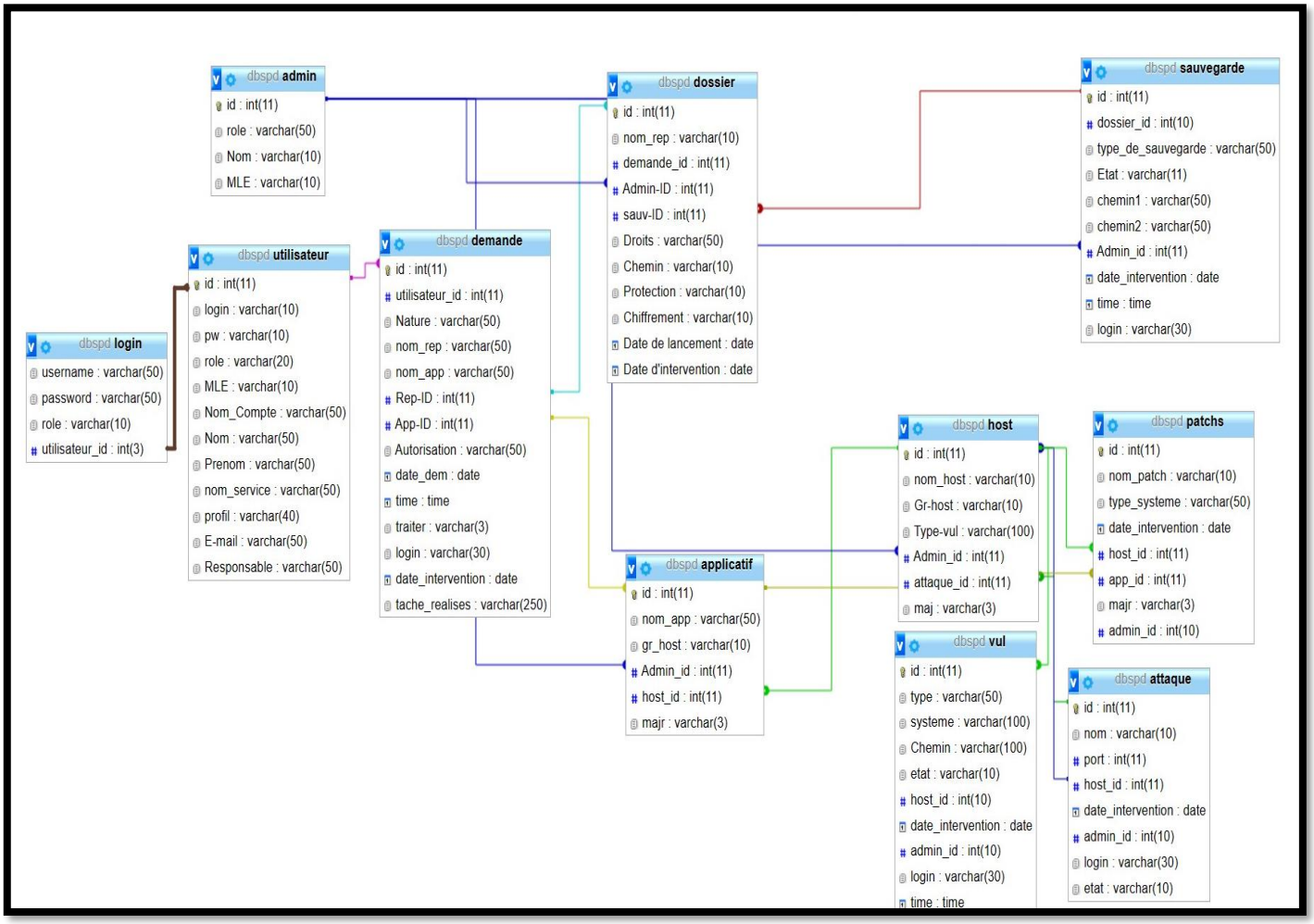
Figure III-16: Le Diagramme de classe.

6.2.3 Modèle logique des données :

Le modèle logique de données est une représentation de la structure des données indépendamment du langage de programmation utilisé. Son objectif est de définir les types de données manipulés lors des opérations de traitement. Par conséquent, le modèle logique est influencé par le type de base de données spécifique utilisé.

Le modèle logique de données qui est lié au diagramme de classes de l'application web à développer.

- Admin (id, rôle, Nom, MLE) ;



- Applicatif (id, nom_app#, gr_hoste, Admin_id #, host_id #, majr) ;

- Attaque (id, nom, port, host_id#, date intervention, admin_id ,login , etat) ;
- Demande(id,utilisateur_id#,Nature,nom_rep#,nom_app#,Rep_ID#,App_ID#, Autorisation , date_dem ,time ,traiter,login,date_intervention,tache_ralises) ;
- Dossier (id, nom_rep#, demande_id#, Admin_id#, sauv_ID#, Droits, chemin, protection, chiffrement, Date de lancement, Date d'intervention) ;
- host(id,nom_host,Gr_host,type_vul,Admin_id#,Attaque_id#,maj);
- login(username, password, role, utilisateur_id#) ;
- patchs(id, nom_patch, type_systeme, date_intervention, host_id#, app_id#, majr, admin_id);
- sauvegarde(id, dossier_id, type_de_sauvegarde, etat, chemin1, chemin2, Admin_id#, date_intervention , time, login) ;
- utilisateur (id, login, pw, role, MLE#, nom_compte, Nom, prenom, nom_service, profil, E_mail, Responsable) ;
- vul(id, type, système, chemin, etat, host_id, date_intervention, admin_id #, login, time);

7 Conclusion :

Dans ce chapitre, nous avons examiné en détail l'analyse et la conception de notre application web. Nous avons spécifié les différents administrateurs et utilisateurs de notre système, et nous les avons représentés en utilisant UML.

La partie conception est terminée, dans le chapitre qui suit, nous allons nous intéresser à la réalisation de notre application web.

CHAPITRE IV

Réalisation

1 Introduction :

Dans ce chapitre consacré à la réalisation, nous aborderons les éléments clés tels que les langages de programmation, les outils et logiciels utilisés, le diagramme de déploiement, les navigateurs web et les interfaces de notre application web seront présentés de manière organisée en commençant par une brève description du diagramme de déploiement, suivi de la figure qui le caractérise. Les langages utilisés pour la réalisation de l'application seront brièvement définis dans le point suivant ; et puisqu'un langage de programmation ne peut se détacher des outils et des logiciels de programmation, chacun de ces derniers se verra attribué. Ces éléments sont essentiels pour la mise en œuvre d'un projet réussi. Nous explorerons les différentes options disponibles et présenterons les bonnes pratiques pour assurer une expérience utilisateur optimale.

2 Le Diagramme de déploiement :

Le diagramme de déploiement du système que nous avons réalisé, est illustré par la figure suivante :

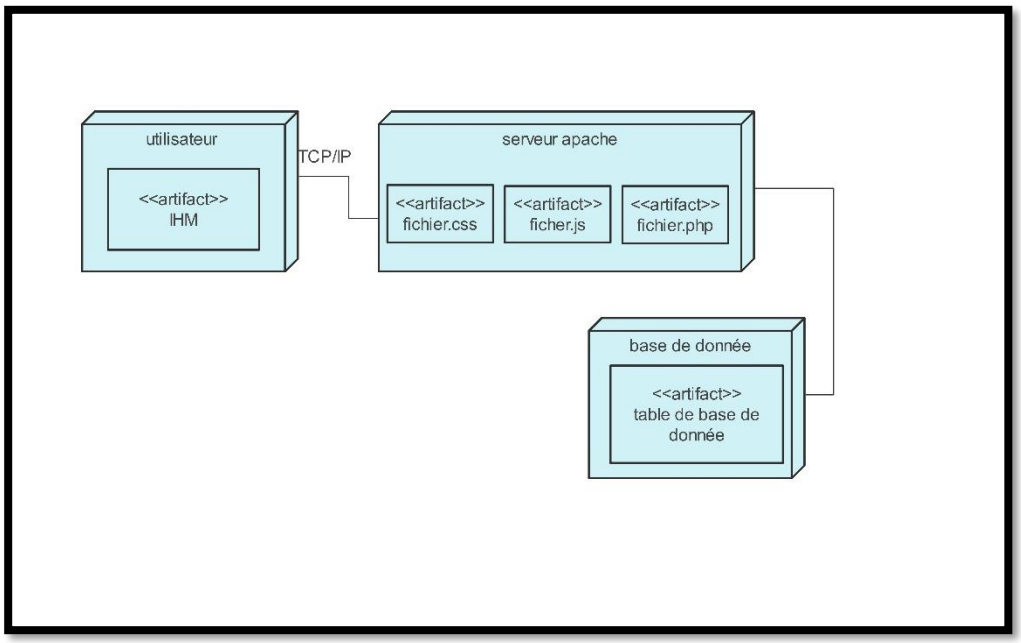


Figure IV-17:Diagramme de déploiement .

Chaque utilisateur dispose de son propre "poste client", qui est un "PC" connecté au serveur Web Apache, qui fonctionne comme son propre serveur d'application et où se déploie notamment l'application d'authentification. Chacun de ces utilisateurs utilise la même interface

utilisateur et le mécanisme d'authentification fourni par le serveur Apache. Toutes les tables sont conservées dans une base de données spécifique hébergée par le serveur de base de données « MySQL ».

3 Langages utilisés :

Lors de la réalisation de l'application Web, un ensemble diversifié de langages de programmation a été utilisé pour mettre en œuvre la vision décrite lors de la phase de conception. Voici une brève description de chaque langage utilisé :

3.1 HTML (HyperText Markup Language) :

HTML, qui signifie HyperText Markup Language, est un langage informatique utilisé pour écrire des pages Web. Avec lui, il est possible d'écrire de l'hypertexte, de formater du contenu, de créer des formulaires de saisie, d'ajouter des images, des vidéos ou des graphiques aux pages, ou encore de faire la sémantique des pages Web. Ce langage fonctionne avec un système de balisage qui sert à mettre en évidence différents éléments à travers des titres, des sous-titres, etc. [63]

3.2 CSS :

Le CSS joue un rôle crucial dans la préparation visuelle du contenu, offrant une présentation attrayante lorsque le document est ouvert dans un navigateur web. Grâce au CSS, on peut spécifier les couleurs, les polices, les marges, les bordures, les animations et d'autres propriétés visuelles pour personnaliser l'apparence de chaque élément HTML. Cela permet aux développeurs de créer des mises en page esthétiques et cohérentes, améliorant ainsi l'expérience utilisateur lors de la navigation sur un site Web. [64]

3.3 JavaScript :

JavaScript spécifie un langage de développement informatique, plus précisément un langage de script orienté objet côté client . Il apparaît principalement sur les pages Internet. Il permet entre autres d'introduire de petites animations ou effets sur des pages Web ou des pages HTML. Le langage JavaScript est principalement utilisé pour améliorer l'ergonomie des sites Web et/ou des interfaces utilisateurs des applications. Il est également utilisé pour incorporer des effets esthétiques, mais est rarement indispensable. Son principal intérêt réside dans son mode de fonctionnement : le langage JavaScript offre bien la possibilité d'exécuter du code sans recharger la page web. En cela, il joue un rôle dans l'amélioration de la vitesse de chargement des pages, un critère ergonomique et SEO de plus en plus important. [65]

3.4 PHP :

PHP est un langage de script côté serveur qui est principalement utilisé pour générer des pages web dynamiques. Il permet d'interagir avec des bases de données, de traiter les formulaires et d'exécuter d'autres tâches du côté serveur pour créer des fonctionnalités avancées. [66]

3.5 MySQL :

MySQL est un serveur de bases de données relationnelles Open Source. Un serveur de bases de données stocke les données dans des tables séparées plutôt que de tout rassembler dans une seule table. Cela améliore la rapidité et la souplesse de l'ensemble. Les tables sont reliées par des relations définies, qui rendent possible la combinaison de données entre plusieurs tables durant une requête. Le SQL dans "MySQL" signifie "Structured Query Language" : le langage standard pour les traitements de bases de données. [67]

4 Outils et logiciels utilisés :

4.1 Notepad++ :

Est un éditeur de texte gratuit et open source qui offre plus que la simple saisie de texte au format txt. Particulièrement appréciée est sa capacité à créer des lignes de code et prend en charge la coloration des étiquettes en fonction du langage de programmation utilisé. Cela rend le code plus facile à lire et à comprendre, met en évidence les éléments clés et améliore la lisibilité. En tant qu'outil polyvalent, Notepad++ est largement utilisé par les programmeurs et les développeurs pour écrire, modifier et organiser efficacement leur code source. Il utilise des composants Scintilla et est conçu pour fonctionner dans un environnement Microsoft Windows. Notepad++ est un outil gratuit et open-source largement utilisé par les développeurs débutants et expérimentés.

Le "++" dans le nom fait référence à l'opérateur d'auto-incrémentation dans les langages de programmation tels que C, C++, Java et JavaScript.[68]

4.2 Environnement Apache/MySQL/PHP (WampServer) :

Apache est le serveur Web le plus utilisé sur Internet. Il est conçu pour écouter les requêtes des programmes clients qui lui sont envoyées sur le réseau. Apache est un logiciel libre et open source, ce qui lui confère une grande stabilité et flexibilité, notamment en raison de sa structure.

MySQL est un système de gestion de base de données (SGBD) largement utilisé, tandis que PHP est un langage de programmation impératif et orienté objet.

WampServer, anciennement connu sous le nom de WAMP5, est une plateforme de développement Web qui permet d'exécuter des scripts PHP localement sans se connecter à un serveur externe. Il ne s'agit pas d'un logiciel à proprement parler, mais d'un environnement composé de deux serveurs (Apache et MySQL), d'un interpréteur de scripts (PHP) et de PHPMyAdmin pour l'administration web des bases de données MySQL.

WampServer dispose d'une interface d'administration qui permet de gérer et d'administrer ces serveurs via une icône (icône de barre d'état) près de l'horloge Windows.

4.3 EdrawMax :

Est un logiciel de création de diagrammes polyvalent qui peut facilement effectuer diverses tâches telles que la création d'organigrammes, d'organigrammes, de diagrammes de réseau, de présentations commerciales, de plans architecturaux, de cartes mentales, d'illustrations scientifiques, de design de mode, de diagrammes UML, de flux de travail, de structure de programme, etc. sur. C'est un outil tout-en-un qui offre un large éventail de fonctions pour répondre aux besoins des différents secteurs d'activité.[69]

4.4 Les Navigateurs Web :

- **Internet Explorer :**

Internet Explorer, également appelé IE, MIE ou MSIE en abrégé, est un navigateur Web créé par Microsoft et préinstallé avec le système d'exploitation Windows. Il a succédé à Netscape Navigator à la fin des années 1990 et a été le navigateur le plus utilisé au monde jusqu'en 2012 environ. Ses principaux concurrents sont Mozilla Firefox (depuis 2004) et Google Chrome (depuis 2008). À partir de la version 7, le nom officiel est Windows Internet Explorer**.**

- **Opera :**

Opera est un navigateur Web gratuit et compatible multiplateforme développé par la société norvégienne Opera, qui fournit également divers autres logiciels liés à Internet. Opera est moins utilisé que les autres navigateurs Web, n'ayant qu'une part de marché de 1,30 % en janvier 2013. Cependant, c'est le troisième navigateur mobile le plus populaire au monde avec une part de marché de 13,65 % en février 2014.[70]

5 Présentation des interfaces:

Notre application contient des utilisateurs et des administrateurs Chaque administrateur a un rôle spécifique dans l'application. Dans ce qui suit, nous décrivons les différentes responsabilités et fonctions attribuées à chaque administrateur.

5.1 Page login :

C’est l’interface qui s’affiche à tout utilisateur voulant visiter le site de "PROTECTION DONNES", Chaque utilisateur doit passer par un système d'authentification sécurisé qui saisit son identifiant et son mot de passe pour accéder à son espace utilisateur ou administrateur. Si ses informations existent dans la base de données et qu'elles sont S'ils correspondent, le système affichera la page convenue, sinon il affichera un message d'erreur.

- **Page inscription utilisateur :**

Lorsque l'utilisateur souhaite accéder à son profil utilisateur, cette interface s'affiche, lui permettant de remplir le formulaire correspondant. Il lui suffit de saisir son identifiant et son mot de passe dans les champs prévus à cet effet. Une fois les informations renseignées, l'utilisateur peut confirmer en cliquant sur le bouton "Connexion". Cette action déclenchera le processus de vérification de l'authenticité des informations fournies, assurant ainsi une connexion sécurisée à son espace personnel.

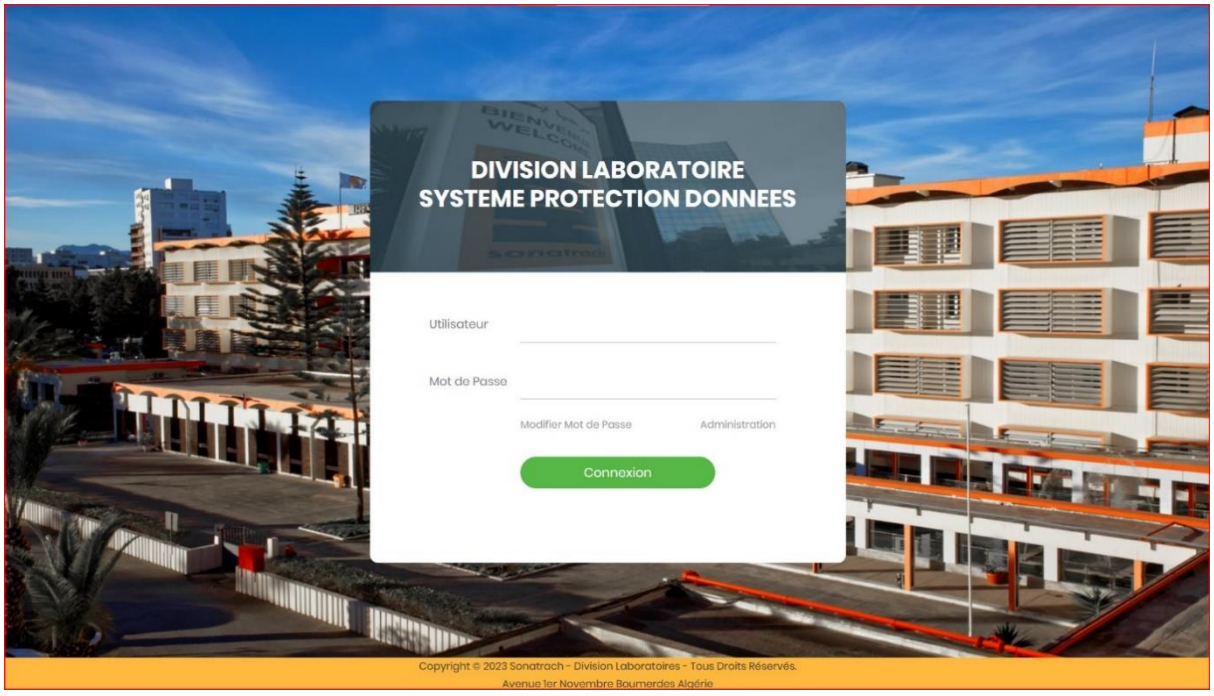


Figure IV-18 : Fenêtre d’inscription utilisateur.

- **Page inscription administrateur :**

Lorsque l'administrateur voudra accéder à son espace, cette interface s'affichera et il lui sera demandé de remplir le formulaire correspondant. L'administrateur doit renseigner son identifiant et son mot de passe dans les champs prévus à cet effet. Après avoir rempli les informations requises, l'administrateur peut confirmer en cliquant sur le bouton "Connexion". Cette action déclenchera le processus de vérification des informations fournies pour garantir l'authenticité de l'administrateur. Une fois identifié, l'administrateur pourra accéder à son espace réservé et bénéficier de fonctionnalités avancées pour gérer et superviser les données et les utilisateurs de manière sécurisée.

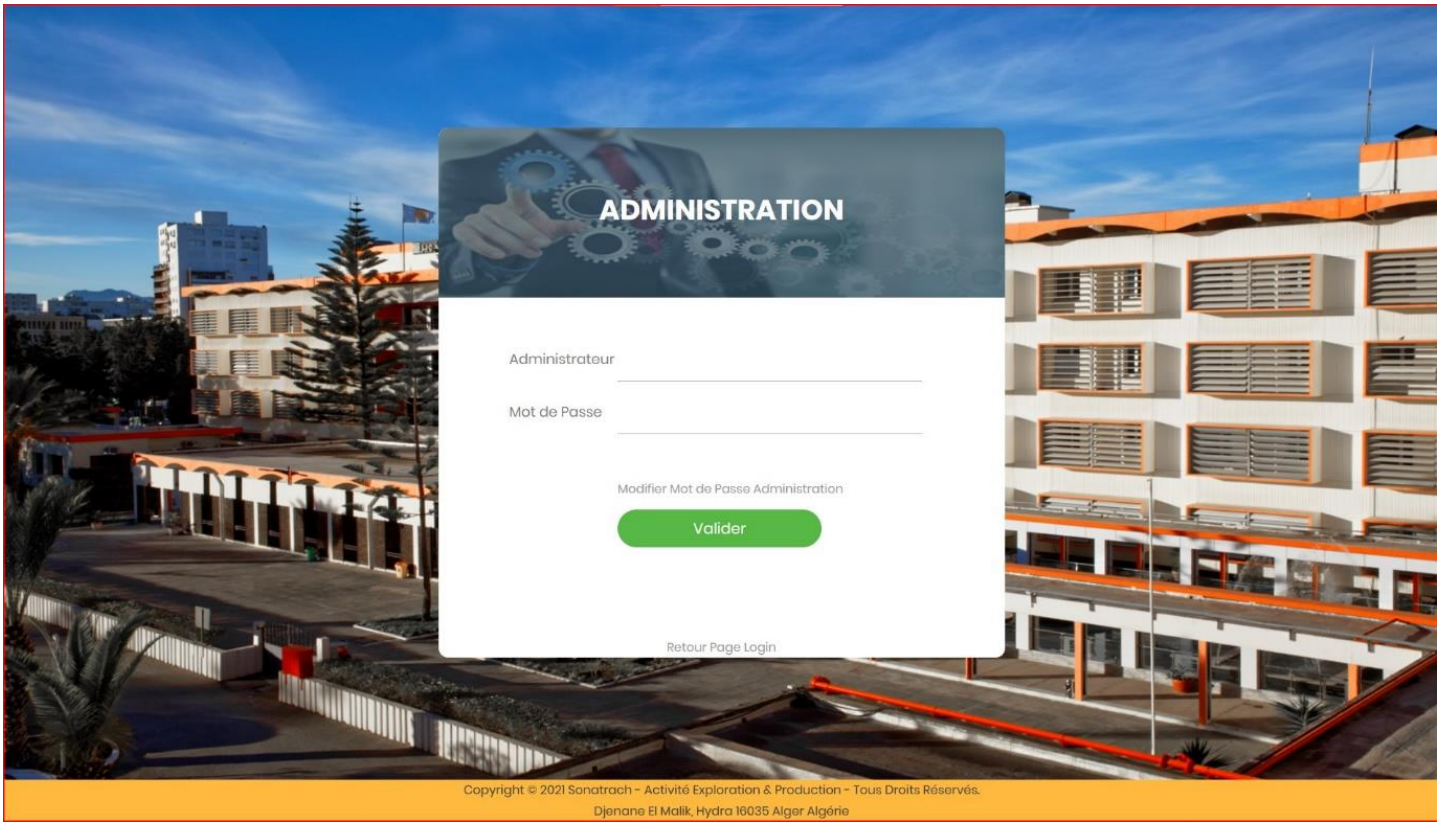


Figure IV-19 : Fenêtre d'inscription administrateur.

- **MODIFICATION - MOT DE PASSE :**

Les utilisateurs et les administrateurs peuvent modifier leurs mots de passe en cliquant sur le bouton "Modifier le mot de passe" dans la page login. Il doit renseigner son identifiant, son ancien mot de passe et son nouveau mot de passe sur un formulaire dédié. En authentifiant le formulaire, leur mot de passe sera mis à jour. Cette fonctionnalité protège les comptes et

empêche tout accès non autorisé. Des mots de passe forts sont recommandés, y compris des caractères alphanumériques et des symboles, pour une sécurité accrue du compte.

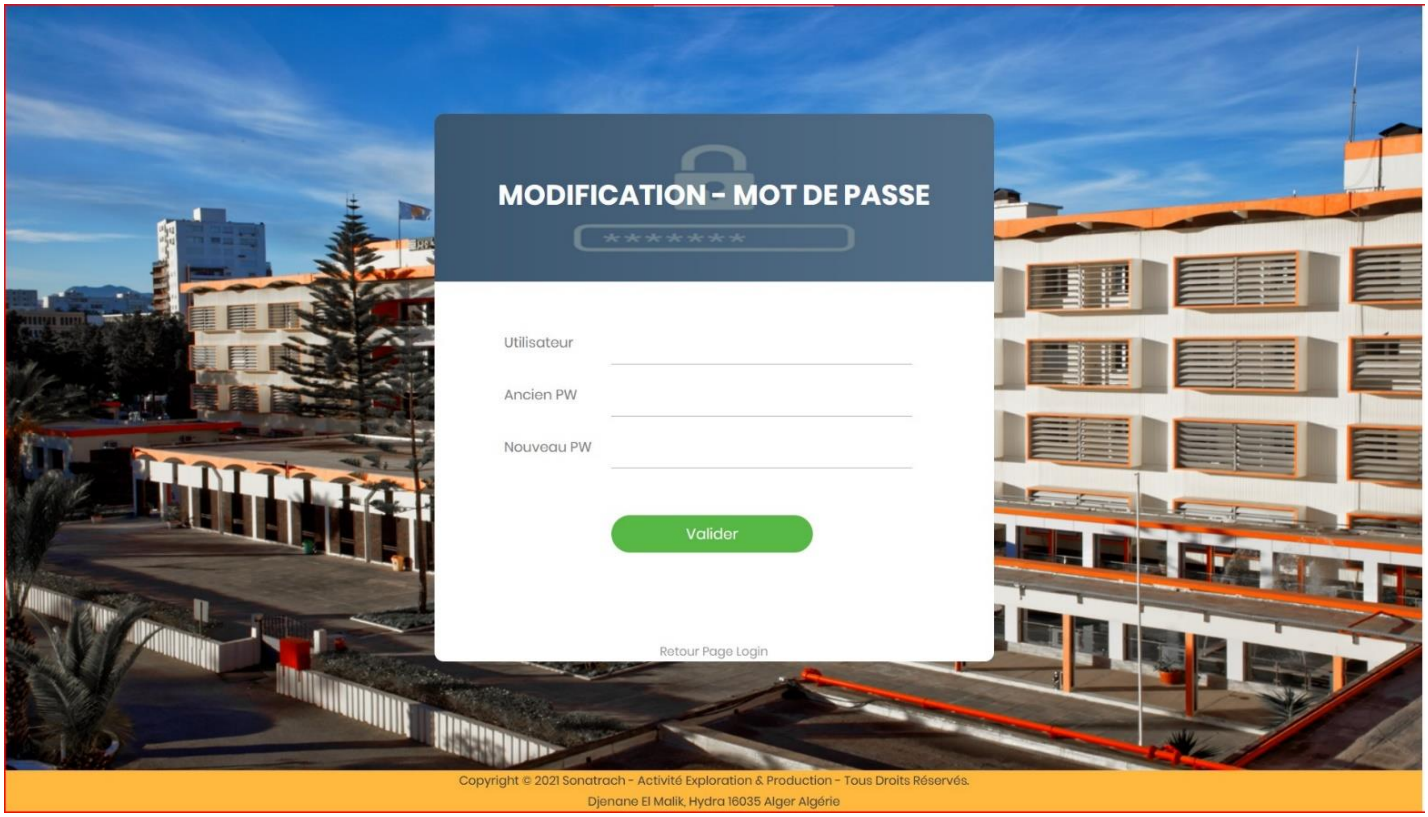


Figure IV-20 : Fenêtre de modification mot de passe.

5.2 Page utilisateur :

Cette interface inclut la page utilisateur où vous pouvez trouver l'accueil et lancer des demandes. Lorsque vous sélectionnez "Demande dossier", vous avez la possibilité de soumettre une demande de protection de dossier pour préserver la confidentialité de vos informations personnelles qui y sont contenues. De plus, si vous choisissez "Demande d'application", vous pouvez demander l'installation de nouvelles applications ou des mises à jour d'applications existantes. À partir de cette page, vous pouvez également accéder aux options des dossiers non traités et des applicative non traitées. Ces options vous permettent de suivre l'état de traitement des demandes et de vérifier si elles ont été traitées.

Figure IV- 21 : Page d'accueil utilisateur.

Figure IV- 22: profil utilisateur.

- **Demande dossier :**

Dans cette interface, lorsque vous sélectionnez une demande de dossier, vous serez invité(e) à fournir plusieurs informations. Une fois que vous avez décidé de faire une demande de dossier pour la protection, vous devrez remplir un formulaire en fournissant les détails nécessaires tel que le nom du répertoire, sélectionner les autorisations souhaitées, telles que l'écriture, la lecture ou l'écriture/lecture. Indiquer l'heure de la demande et l'agent responsable. En fournissant des informations précises et complètes, vous facilitez la gestion de votre demande de protection de dossier. Une fois enregistrée, votre demande sera affichée dans un tableau avec des détails tels que le nom d'utilisateur, le service responsable, la nature de la demande, le nom du répertoire, les autorisations demandées, la date et l'heure de la demande, ainsi que l'état de la demande. Cela permet une gestion efficace et transparente de toutes les demandes de dossier enregistrées, et vous pouvez suivre l'évolution et le statut de votre demande sur le tableau.

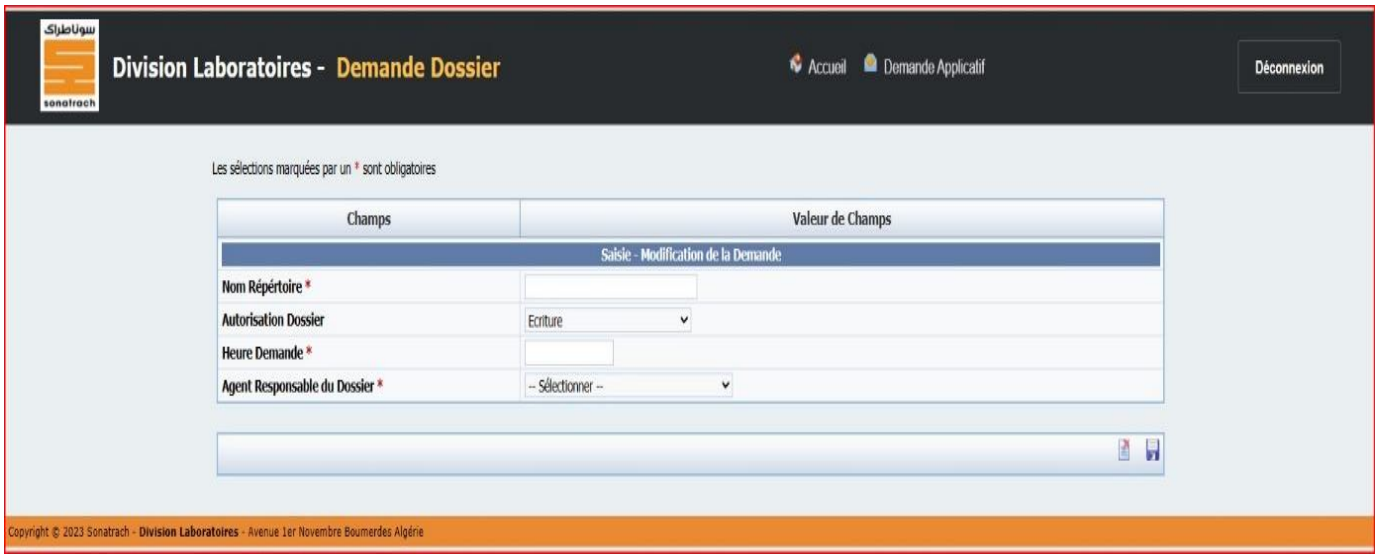


Figure IV-23:Ajouter demande dossier.

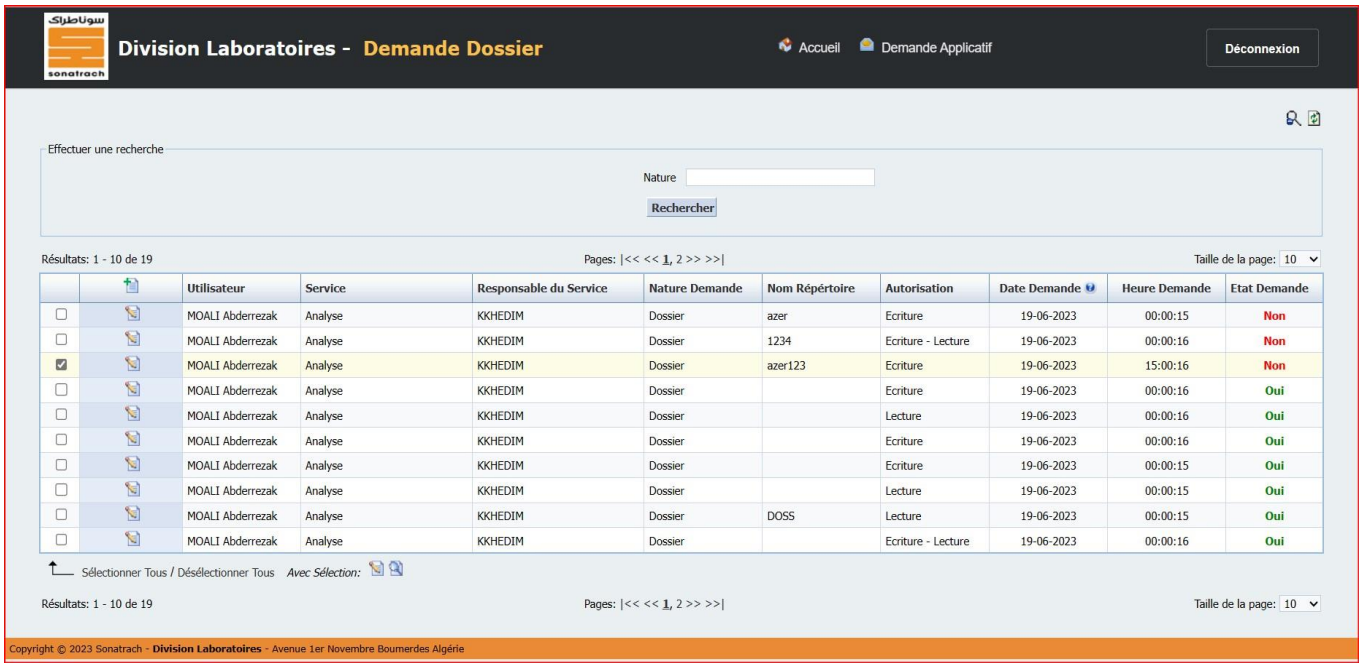


Figure IV- 24: page demande dossier.

- **Demande applicative :**

Depuis cette interface, lorsque vous sélectionnez une demande applicative, il vous sera demandé de fournir plusieurs informations. Une fois que vous avez choisi de faire une demande applicative vous devrez remplir un formulaire en fournissant les détails nécessaires tel que le nom applicatif et sélectionner les autorisations souhaitées, telles que l'installation, mise à jour ou installation /mise à jour , indiquer l'heure de la demande et l'agent responsable. En fournissant des informations précises au lieu et complètes, vous facilitez la gestion de votre demande d'applicative. Une fois enregistrée, votre demande sera affichée dans un tableau avec des détails tels que le nom d'utilisateur, le service responsable, la nature de la demande, le nom du l'applicative, les autorisations demandées, la date et l'heure de la demande, ainsi que l'état de la demande. Cela permet une gestion efficace et transparente de toutes les demandes d'installation et de mise à jour d'applications.

Figure IV- 25:Ajouter demande applicative.

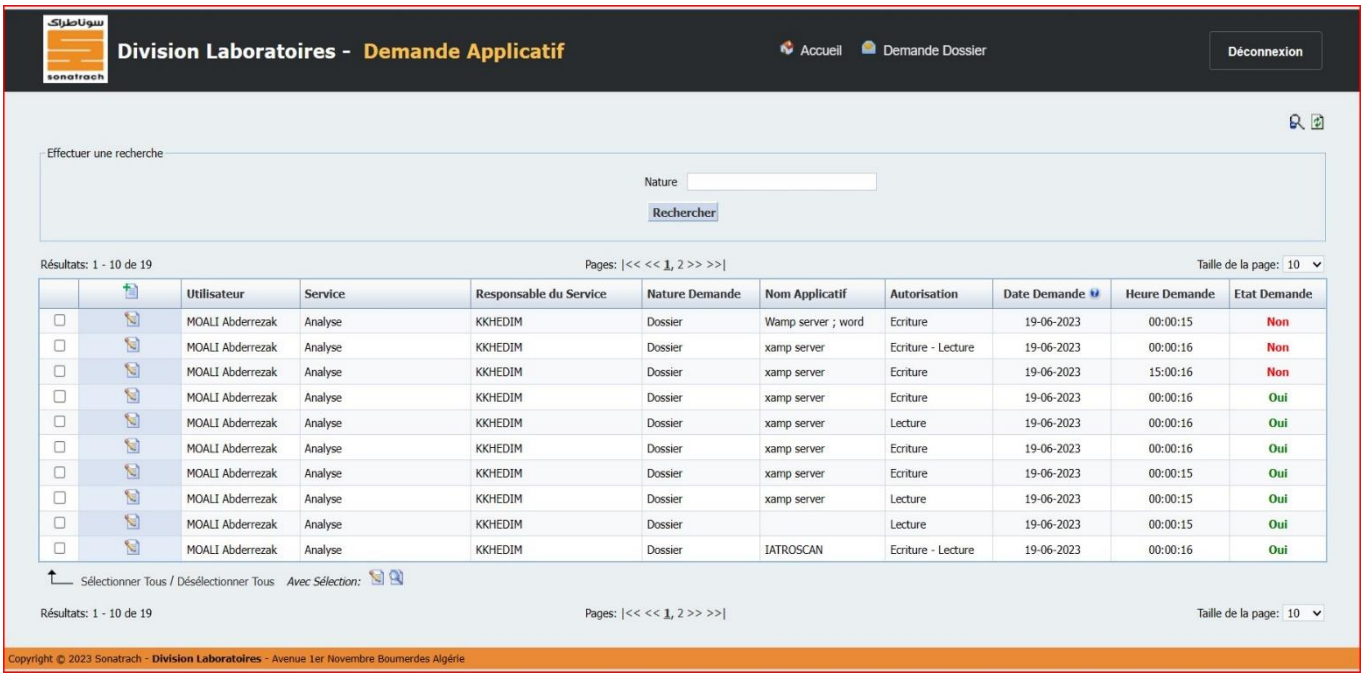


Figure IV- 26: page demande applicative.

5.3 Demande Dossier non trait (Les alertes) :

Dans cette interface, nous avons une alerte pour demandes dossier non traitées. Si l'administrateur saisit une date d'intervention, l'état est "Oui", indiquant que le dossier est traité. Si aucune date d'intervention n'est saisie, l'état reste "Non traité", signifiant que le dossier n'a pas encore été traité. Cette fonctionnalité permet de suivre et de gérer facilement les demandes de protection de dossiers, en assurant leur traitement en temps opportun.

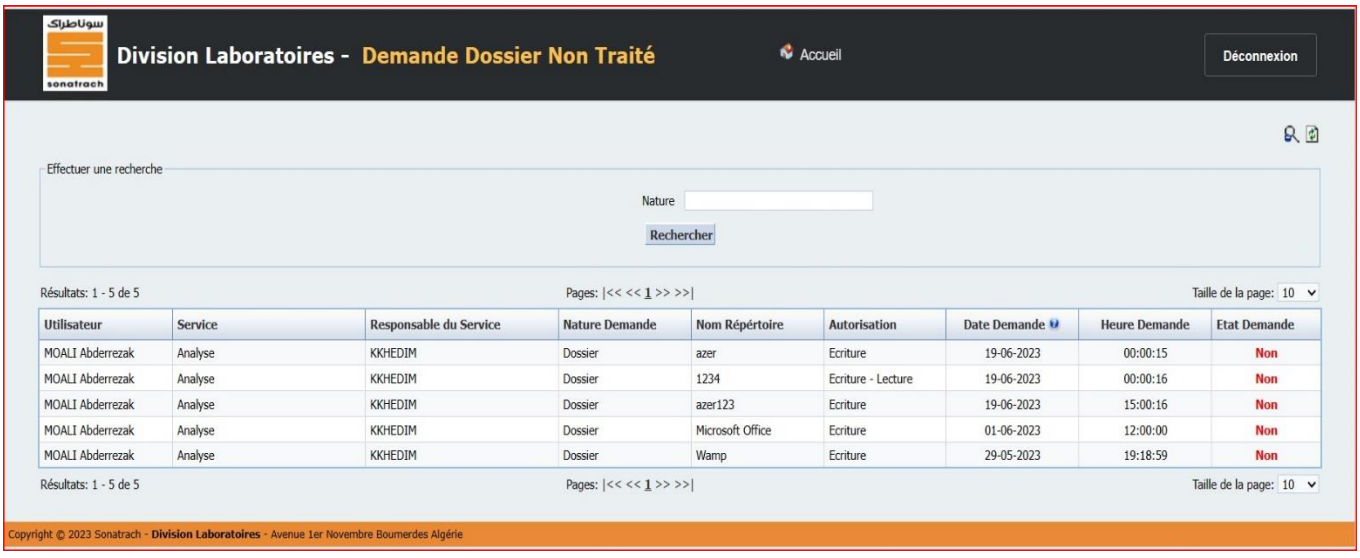


Figure IV- 27: page demande dossier non trait.

- **Demande applicative non traite (Les alertes) :**

Dans cette interface, nous avons une alerte pour demandes applicative non traitées. Si l'administrateur saisit une date d'intervention, l'état est "Oui", indiquant que le dossier est traité. Si aucune date d'intervention n'est saisie, l'état reste "Non traité", signifiant que l'applicative n'a pas encore été traité. Cette fonctionnalité permet de suivre et de gérer facilement les demandes applicatives, en assurant leur traitement en temps opportun.

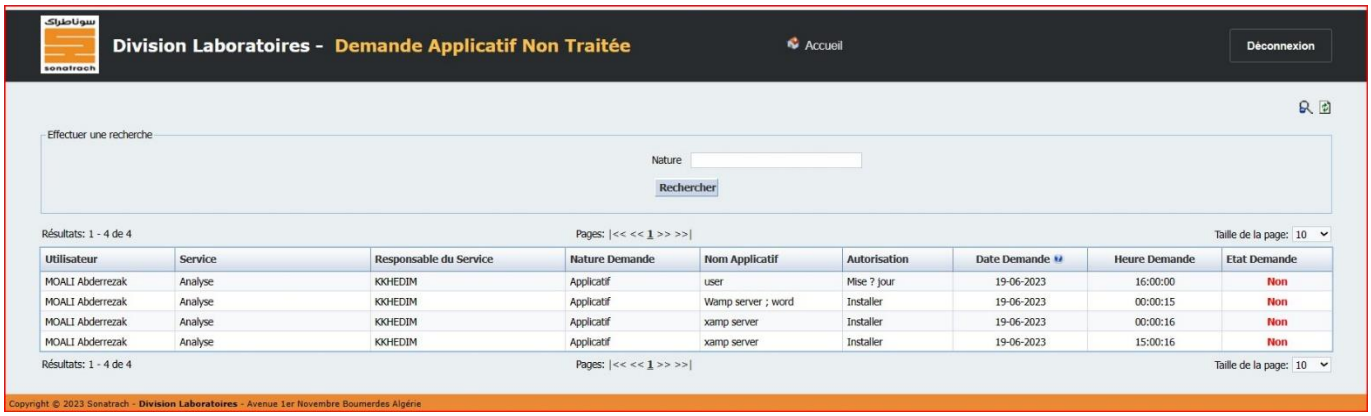


Figure IV- 28:demande applicative non traite .

5.4 Page admin dossier :

Cette interface donne aux administrateurs un contrôle total sur le site. Il leur permet de consulter les demandes de protection des dossiers reçues et de répondre aux besoins des utilisateurs en accordant des autorisations et en mettant en place des mécanismes de chiffrement. L'administrateur peut ainsi sauvegarder et exercer un contrôle précis et assurer la satisfaction des utilisateurs tout en préservant la sécurité des données.

Figure IV- 29: Page d'accueil d'administrateur dossier.

Figure IV- 30: Profil Administrateur(dossier).

- **Les alertes (Anomalies Signalées):**

Cette interface vous permet de recevoir des alertes sur les anomalies signalées. Il affiche les demandes de protection en attente qui nécessitent une intervention de l'administrateur. Lorsque l'administrateur a terminé de protéger les dossiers, il peut renseigner les champs obligatoires tels que l'heure d'intervention et les tâches effectuées en cliquant sur le bouton "Modifier l'enregistrement". Les actions de l'administrateur sont alors journalisées et affichées dans le dossier correspondant. Cela permet de suivre l'intervention de l'administrateur et de garantir la protection des fichiers de manière efficace.

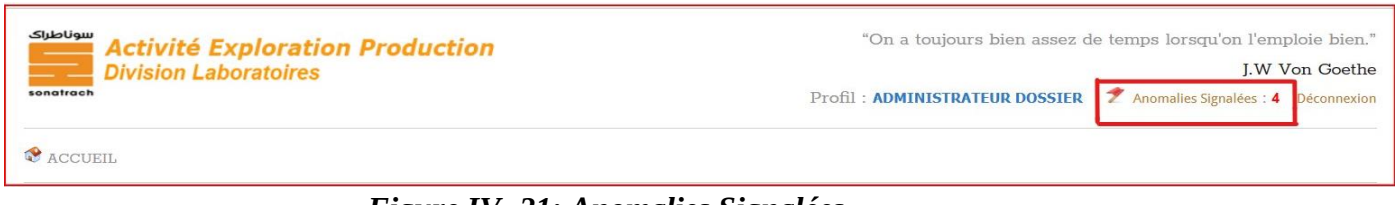


Figure IV- 31: Anomalies Signalées.

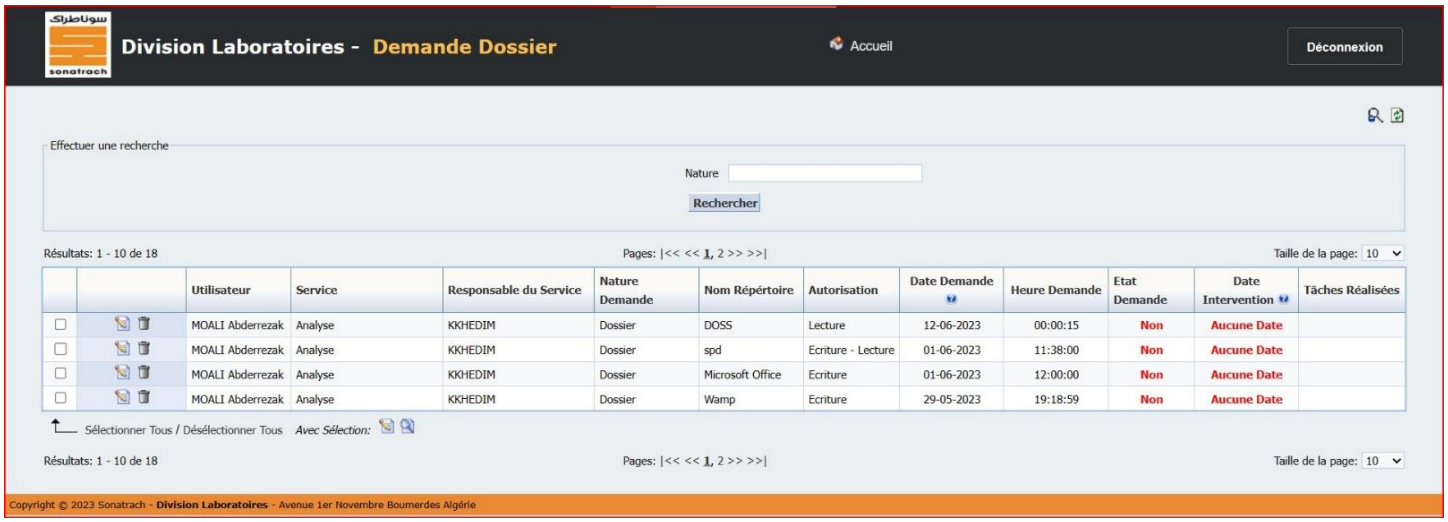


Figure IV- 32: Les demandes de protection en attente(dossiers) .

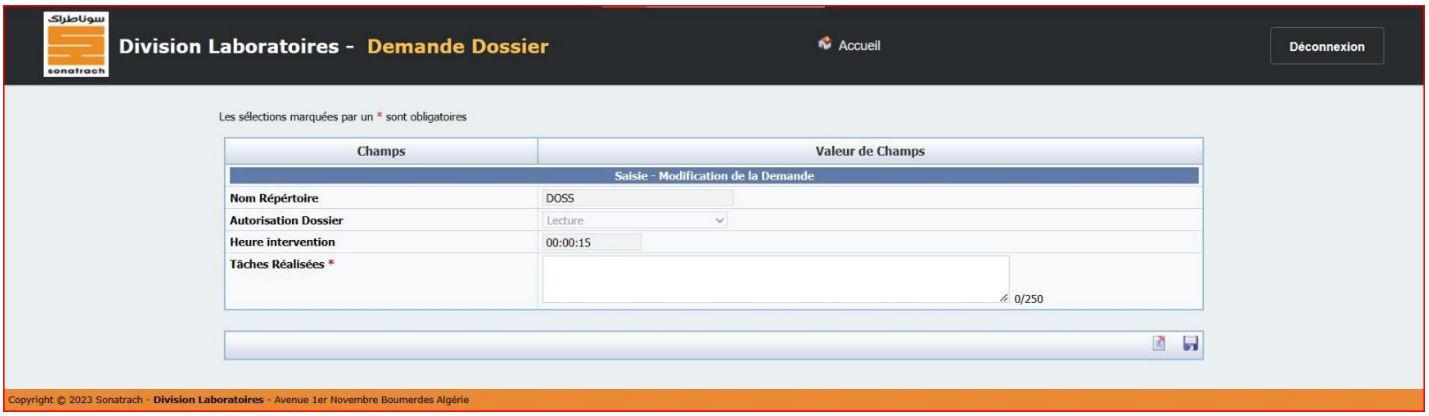


Figure IV- 33 : L'intervention d'administrateur(dossiers).

- **Dossier (trait et non trait) :**

L'interface administrateur de dossiers propose deux options pratiques : "Dossiers traités" et "Dossiers non traités". En cliquant sur "Dossiers traités", vous accédez rapidement aux dossiers déjà traités, vous offrant ainsi une vue d'ensemble de leur statut. Si vous souhaitez consulter les dossiers en attente de traitement, il vous suffit de cliquer sur "Dossiers non traités". Ces fonctionnalités vous permettent de suivre facilement l'état des demandes de dossiers, que ce soit pour ceux déjà traités ou en attente d'action. Cela facilite la gestion efficace des dossiers et vous permet de répondre rapidement aux besoins des utilisateurs.

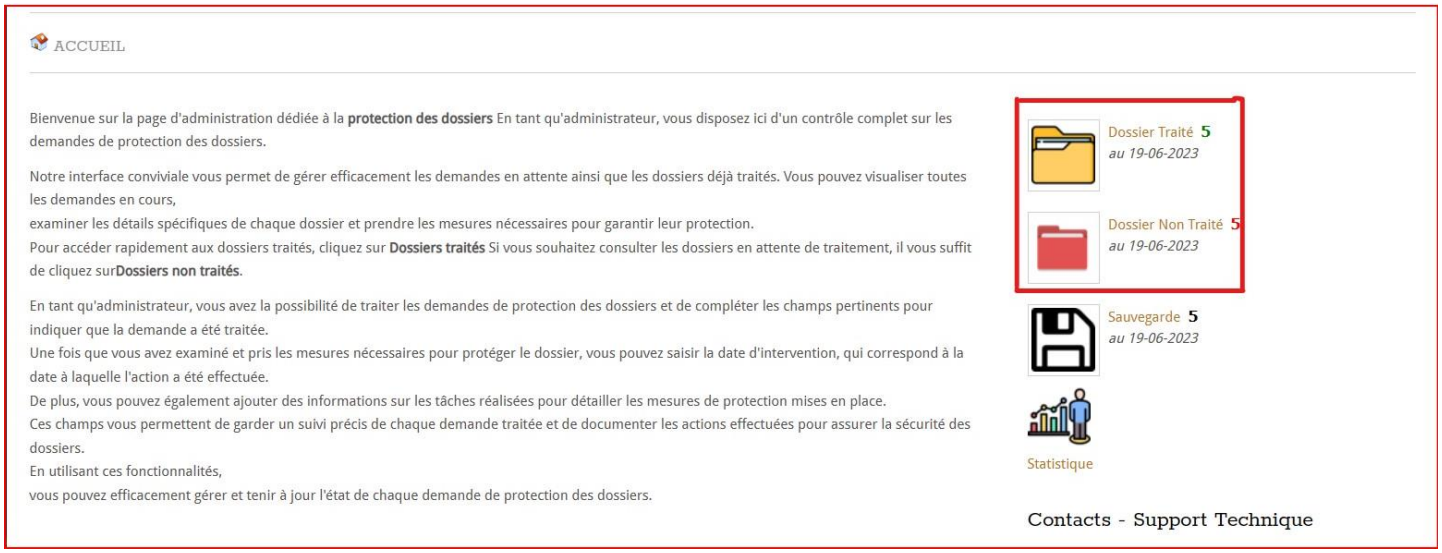


Figure IV- 34 : Dossier (traiter et non traiter).

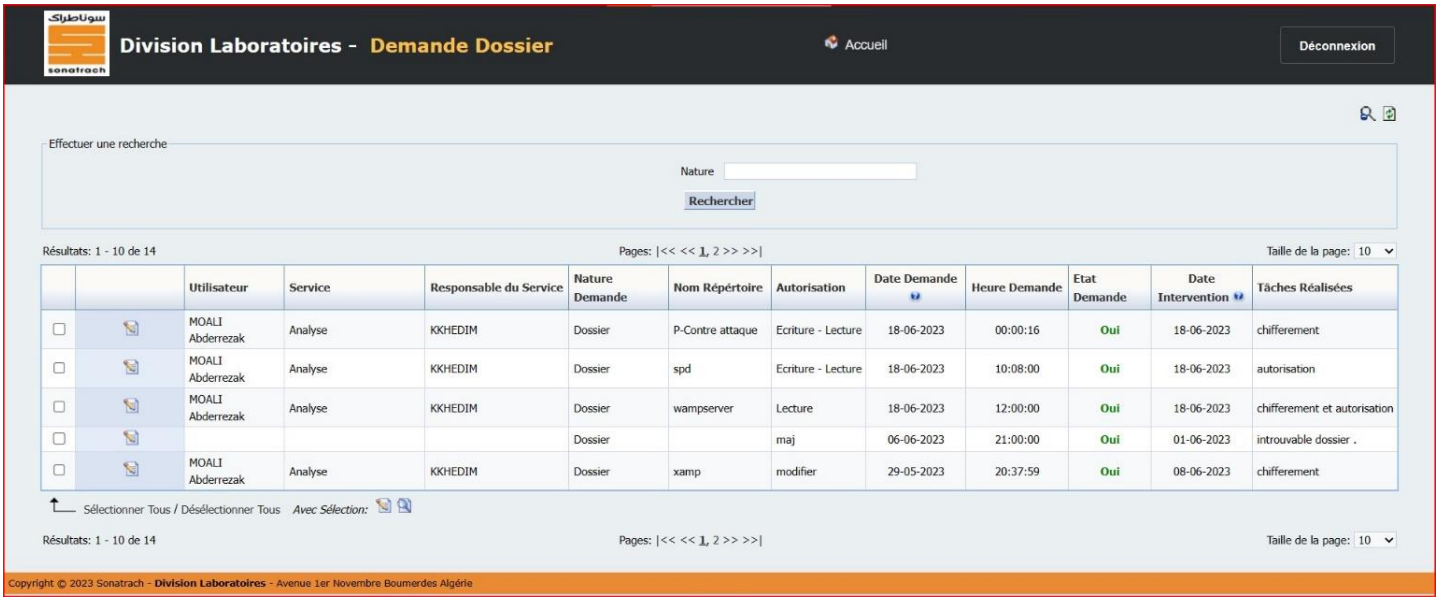


Figure IV- 35: Dossier trait .

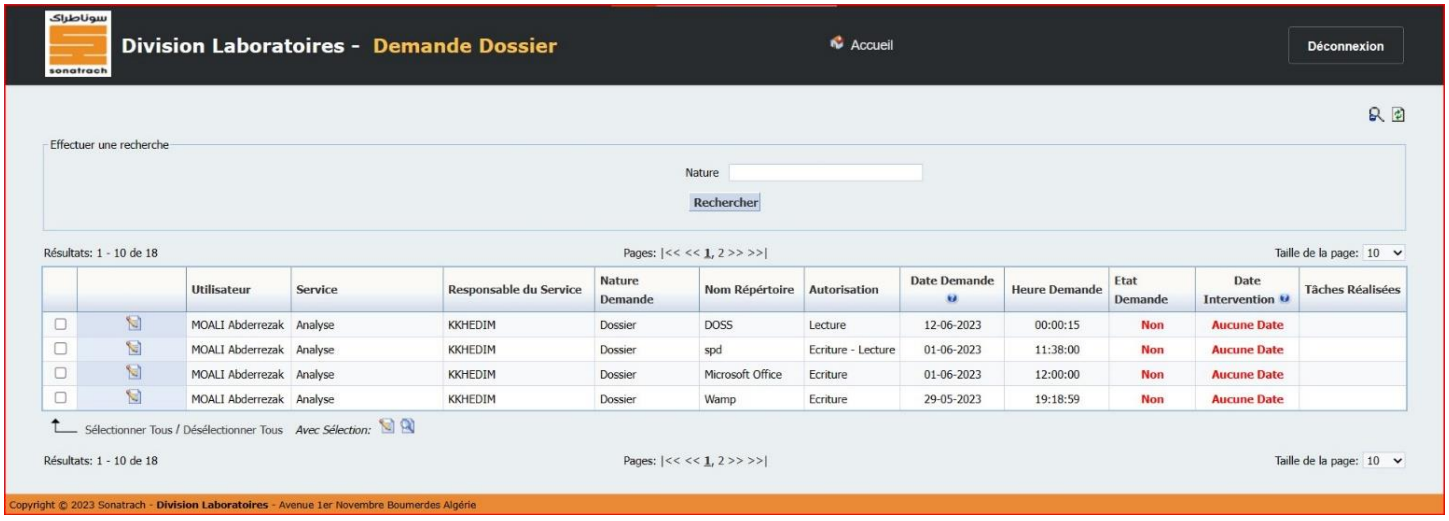


Figure IV- 36: Dossier non trait.

- **Sauvegarde :**

Une fois les fichiers traités, l'administrateur effectuera des sauvegardes régulières pour assurer la sécurité et la disponibilité des données. Ces sauvegardes utilisent deux chemins différents, ce qui augmente la sécurité des données. Pour chaque sauvegarde, l'administrateur renseigne les champs suivants : sélectionnez le dossier approprié et entrez le chemin de sauvegarde (1er et 2ème), l'heure de la sauvegarde et le nom de l'administrateur responsable. Après avoir saisi les informations, l'administrateur confirme l'enregistrement en cliquant sur le bouton Enregistrer. Ces sauvegardes régulières garantissent la protection des données sensibles et leur disponibilité en cas de besoin. Ils permettent également aux administrateurs de suivre et de consigner les opérations de sauvegarde, garantissant ainsi la responsabilité de leur exécution. Ainsi, la sécurité et la disponibilité des données sont maintenues de manière fiable dans le système.

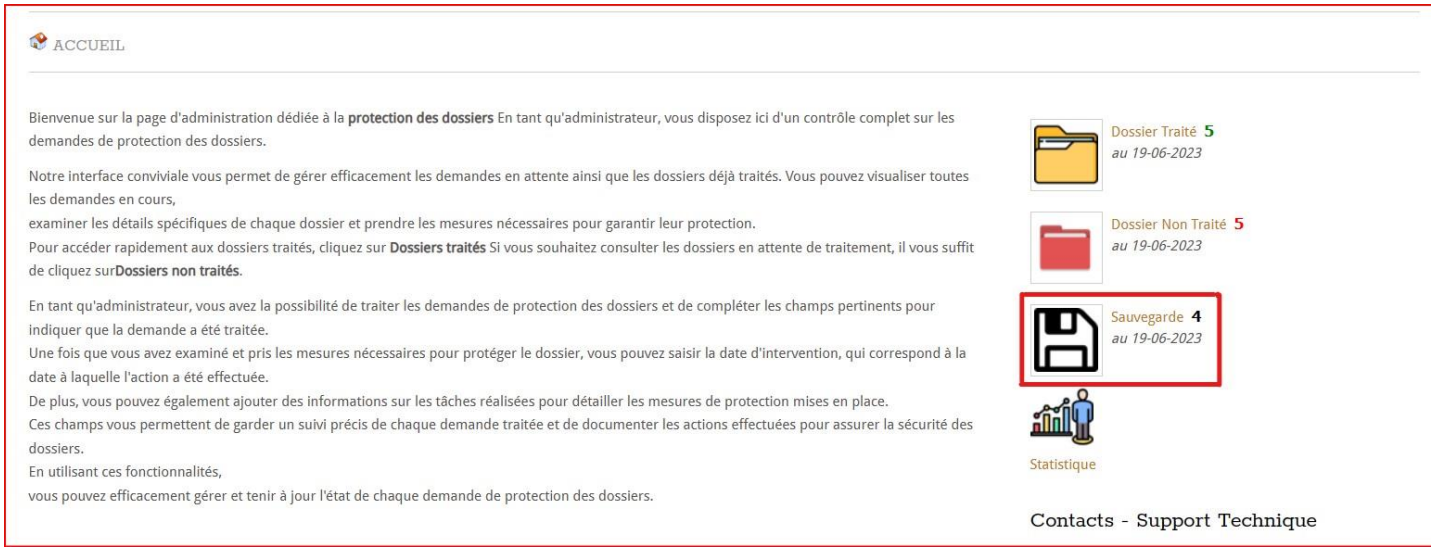


Figure IV- 37: Sauvegarde .

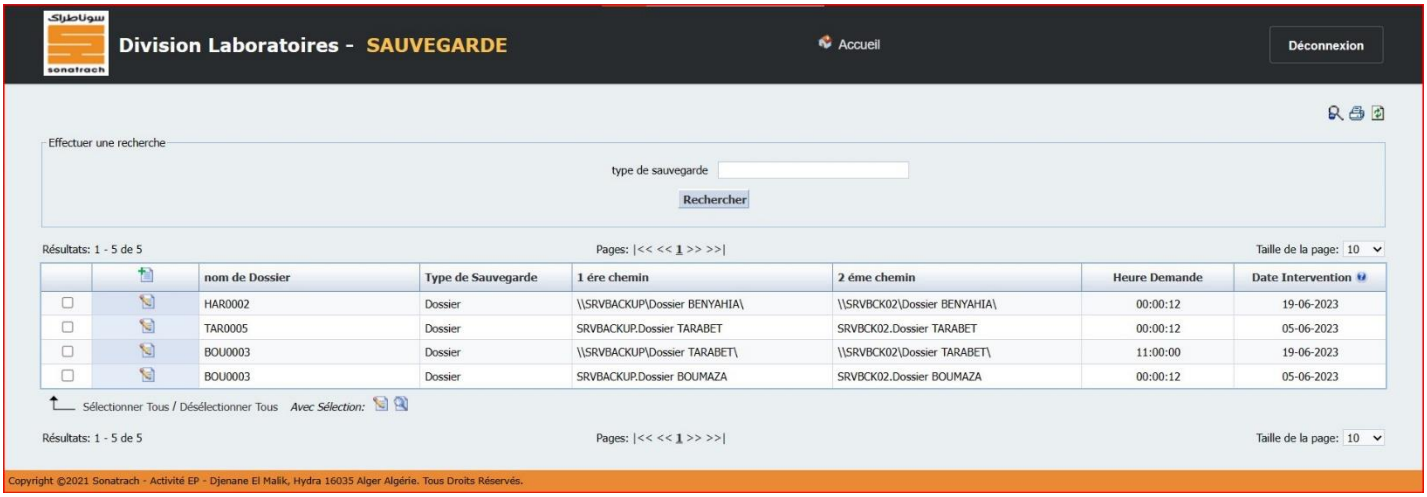


Figure IV- 38 : Dossier sauvegarde .

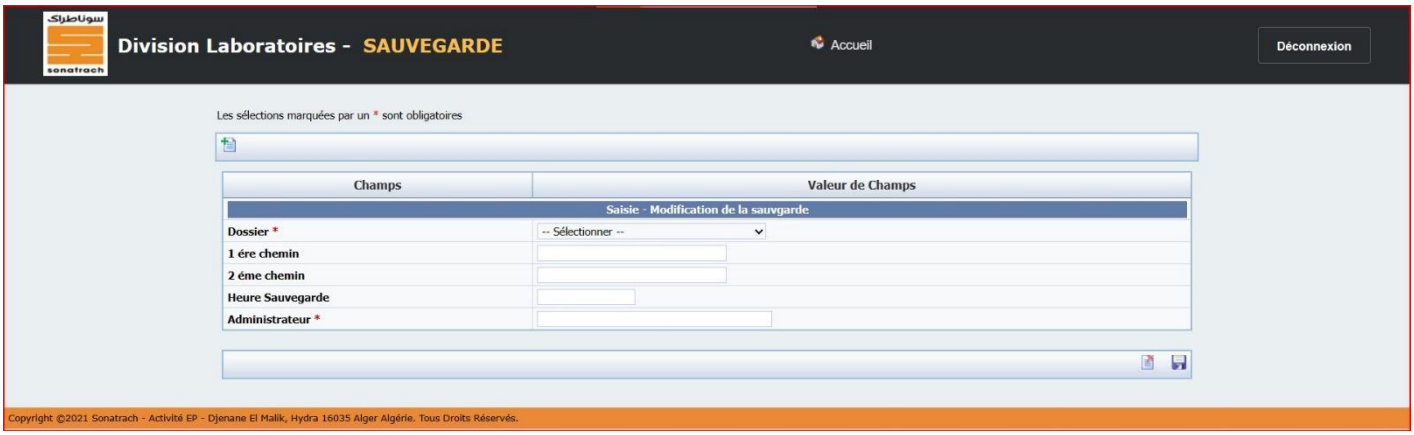


Figure IV- 39 : Ajouter une sauvegarde.

5.5 Admin applicative :

Cette interface donne aux administrateurs un contrôle total sur le site. Il leur permet d'examiner les demandes d'applications entrantes et de répondre aux besoins des utilisateurs en accordant des mises à jour et en installant des applications. Cela permet aux administrateurs de surveiller les correctifs et les hôtes en effectuant des mises à jour et de confirmer que le logiciel antivirus est mis à jour pour empêcher les attaques et les vulnérabilités. Cela lui donne un contrôle précis et assure la satisfaction de l'utilisateur.

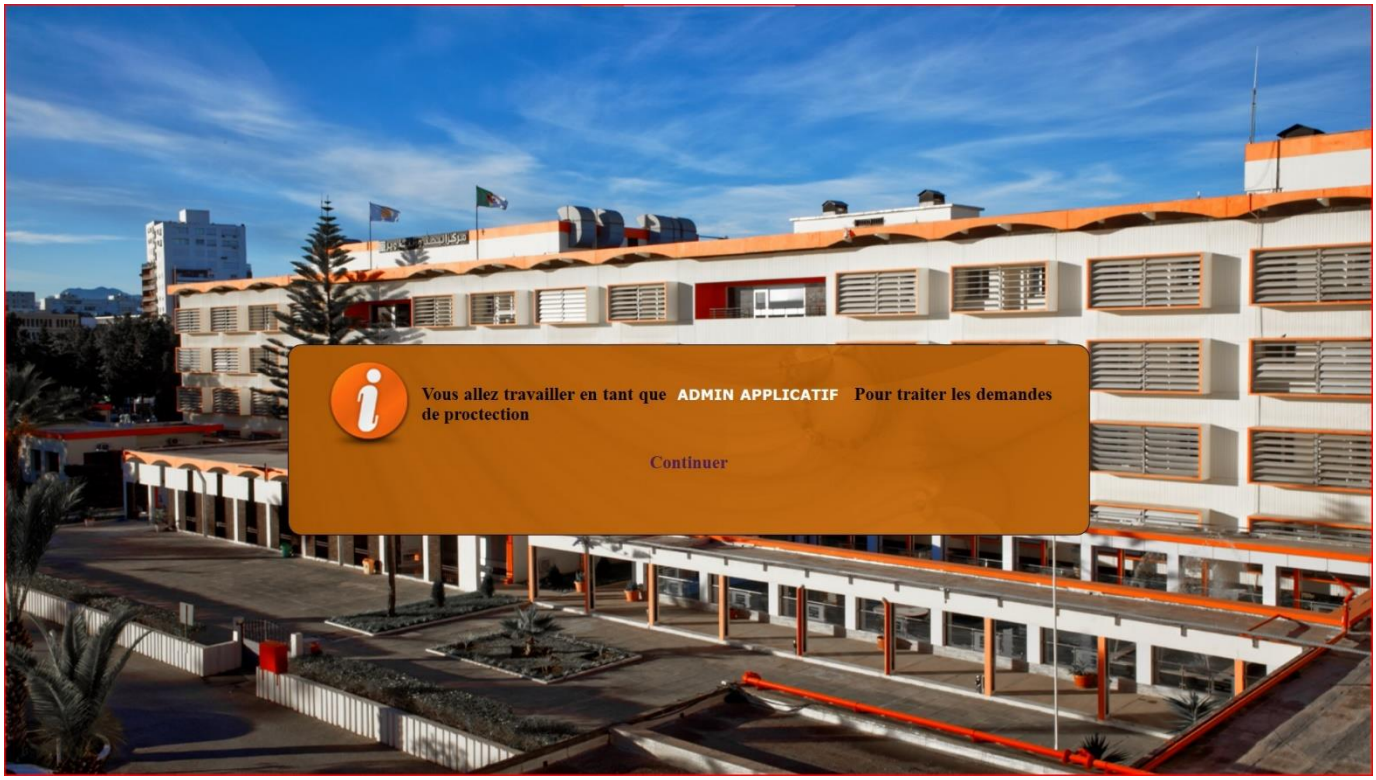


Figure IV- 40 : Page d'accueil d'administrateur applicatif.

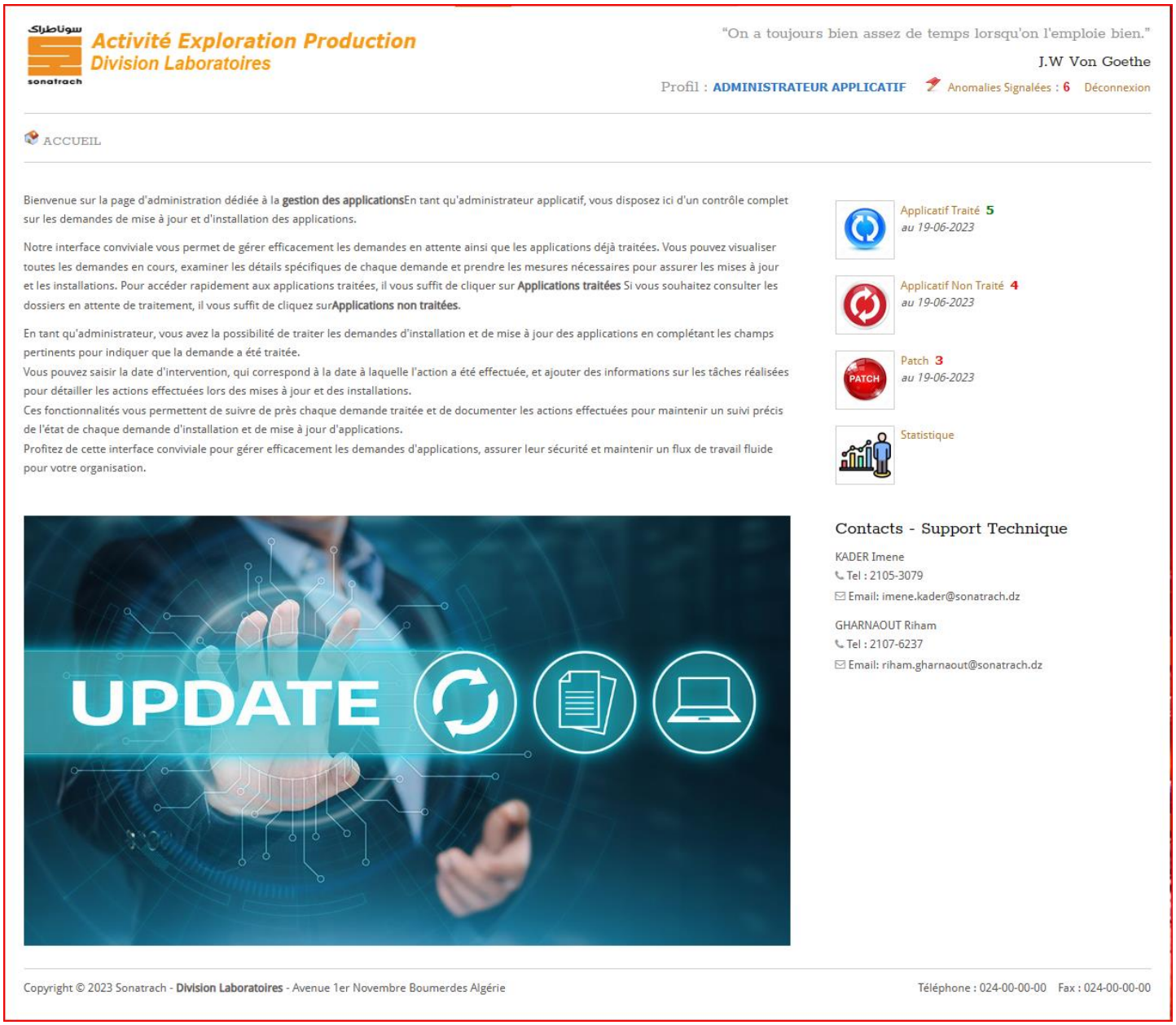


Figure IV- 41: Profil Administrateur(applicatif).

- **Les alertes (Anomalies Signalées):**

Cette interface vous permet de recevoir des alertes sur les anomalies signalées. Il affiche les demandes de protection en attente qui nécessitent une intervention de l'administrateur. Une fois que l'administrateur a mis à jour ou installé l'application selon les besoins de l'utilisateur, il peut renseigner les champs obligatoires tels que l'heure d'intervention et les tâches effectuées en cliquant sur le bouton "Modifier l'enregistrement". Ces actions de l'administrateur sont enregistrées et affichées dans l'interface d'utilisateur (demande applicative), assurant ainsi un suivi efficace des interventions et une gestion optimale des mises à jour et des installations de l'application.

Figure IV- 42: Anomalies Signalées(applicatif).

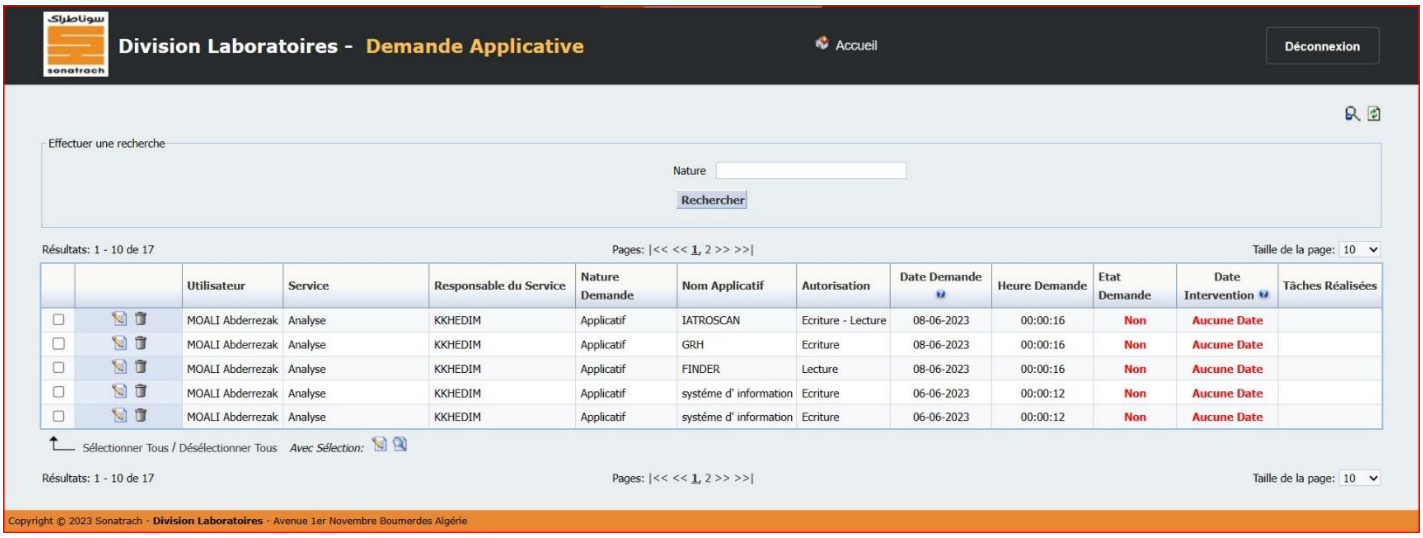


Figure IV- 43: Les demandes de protection en attente(applicative).

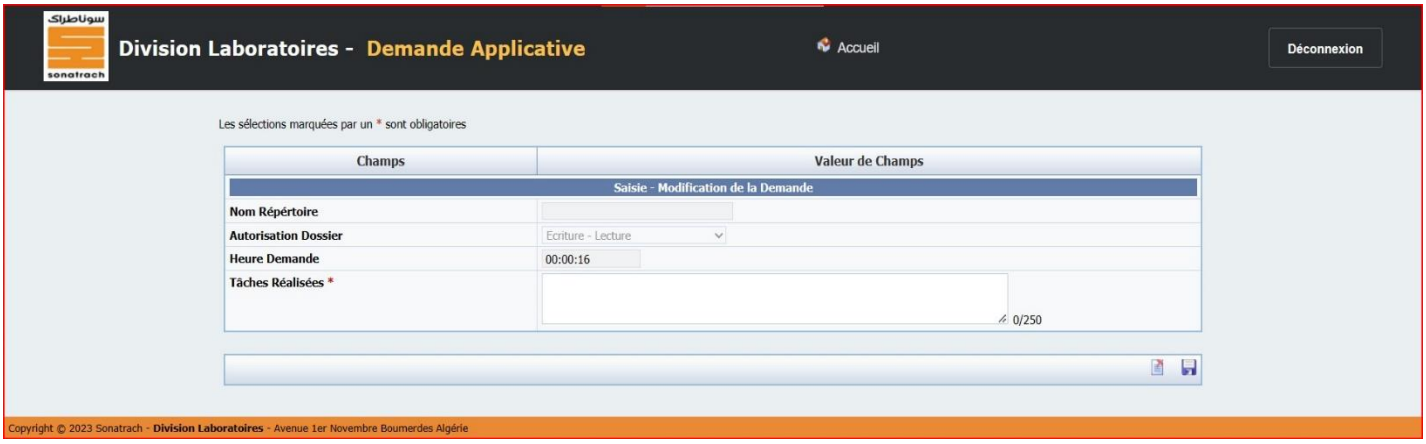


Figure IV- 44: L'intervention d'administrateur(applicative).

- **Applicative (traiter et non traiter) :**

L'interface administrateur d'applicatif propose deux options pratiques : "Applicatif traités" et "Applicatif non traités". En cliquant sur "Applicatif traités", vous accédez rapidement aux applicative déjà traités, vous offrant ainsi une vue d'ensemble de leur statut. Si vous souhaitez consulter les applicatives en attente de traitement, il vous suffit de cliquer sur "Applicatif non traités". Ces fonctionnalités vous permettent de suivre facilement l'état des demandes, que ce soit pour ceux déjà traités ou en attente d'action.

Cela facilite la gestion efficace des applications et vous permet de répondre rapidement aux besoins des utilisateurs.

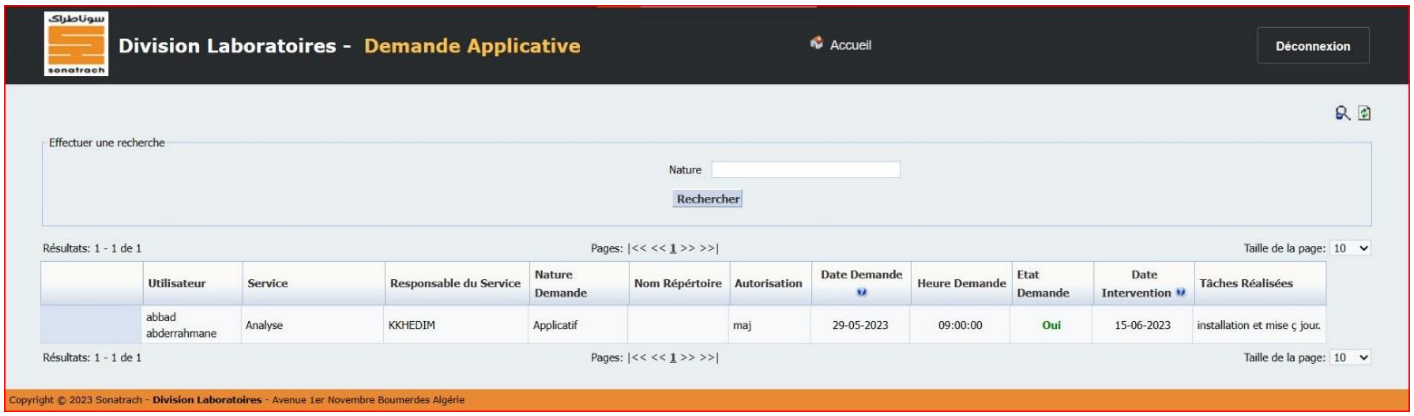


Figure IV- 45: Applicative traite .

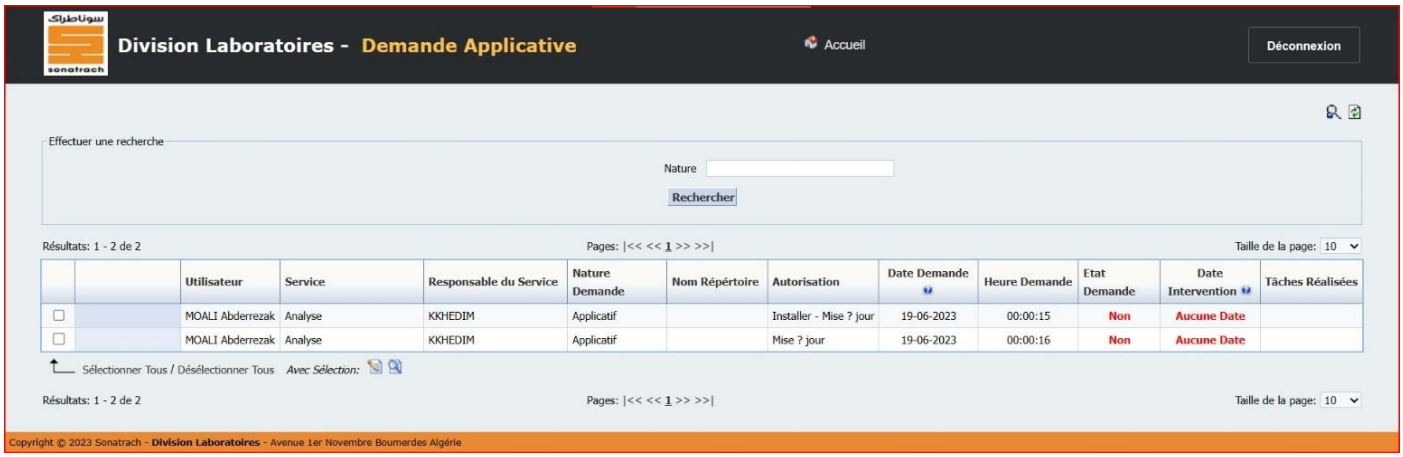


Figure IV- 46: Applicative non traite .

- **Patchs :**

Grâce à cette interface, les hôtes, les systèmes et les applications peuvent être visualisés en détail, ainsi que leur état de mise à jour respectif. Cette fonctionnalité permet une gestion efficace des hôtes en s'assurant que les applications de l'hôte sont à jour. L'administrateur joue un rôle clé dans ce processus, remplissant les champs obligatoires pour chaque opération de mise à jour. Ces champs incluent le nom du correctif, le type de système, le nom d'hôte, l'application affectée, la date d'intervention et l'identité de l'administrateur. Avec ces informations, il est possible de vérifier et de confirmer qu'une application particulière dans cet hôte, dans ce système, est bien à jour. Ainsi, l'interface assure un contrôle précis et une traçabilité des opérations de mise à jour, facilitant ainsi la gestion et le suivi des mises à jour applicatives.

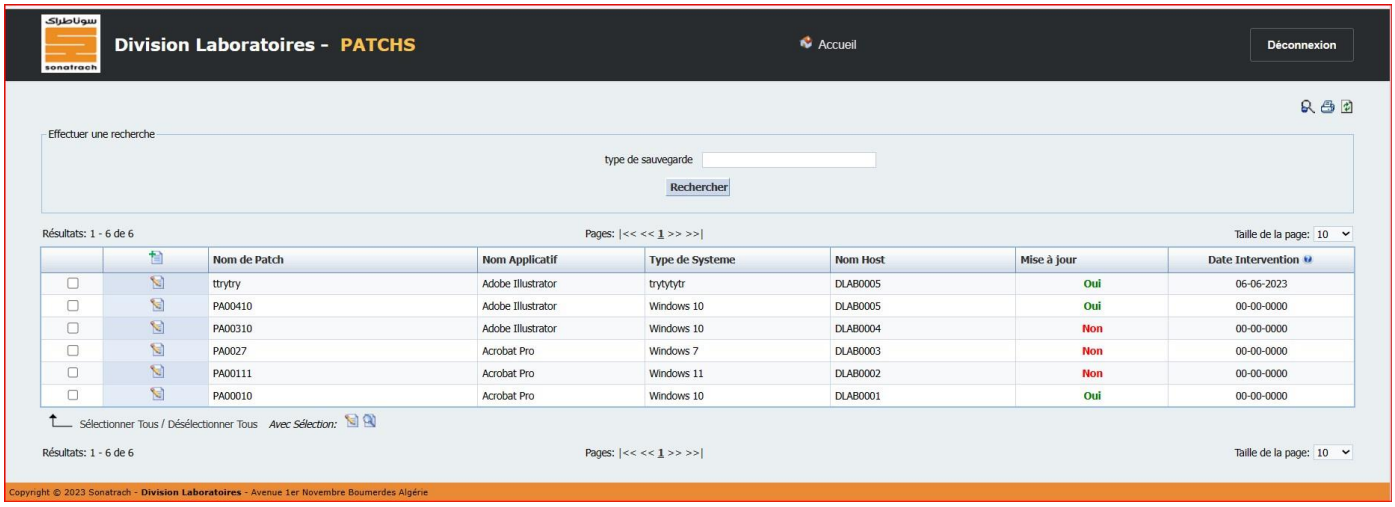


Figure IV- 47: Patchs.

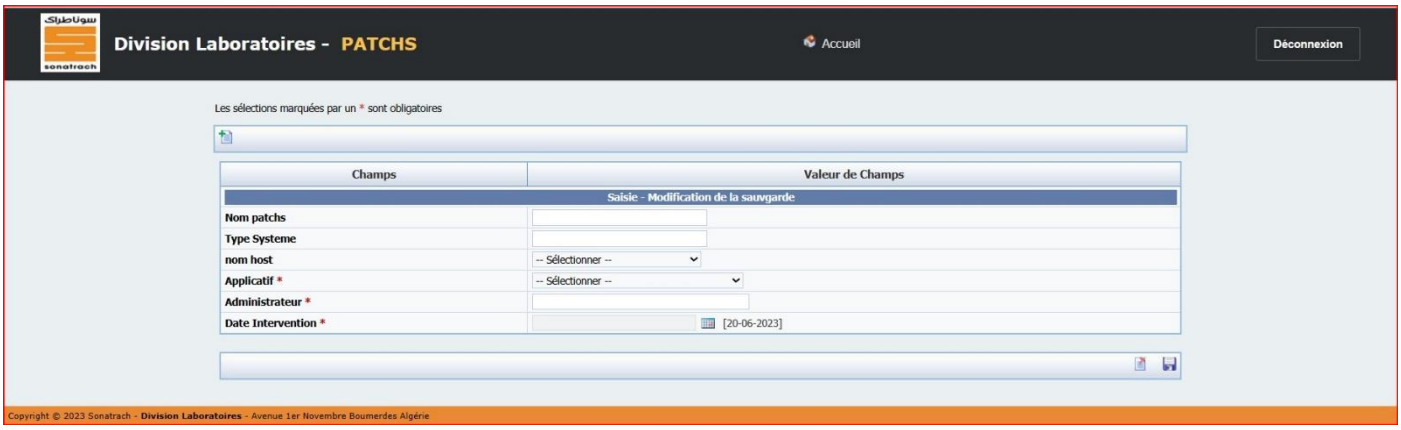


Figure IV- 48 : l'intervention d'administrateur (mise à jour d'applicatif).

5.6 Page Admin monitoring :

Cette interface fournit aux administrateurs un contrôle total sur le site, leur permettant de surveiller les attaques et les vulnérabilités sur les hôtes du réseau, tout en offrant une flexibilité pour adapter la protection en fonction de leurs besoins spécifiques. Les administrateurs peuvent utiliser cette interface pour visualiser et analyser les attaques en cours, les activités suspectes et les vulnérabilités détectées sur chaque hôte**.**

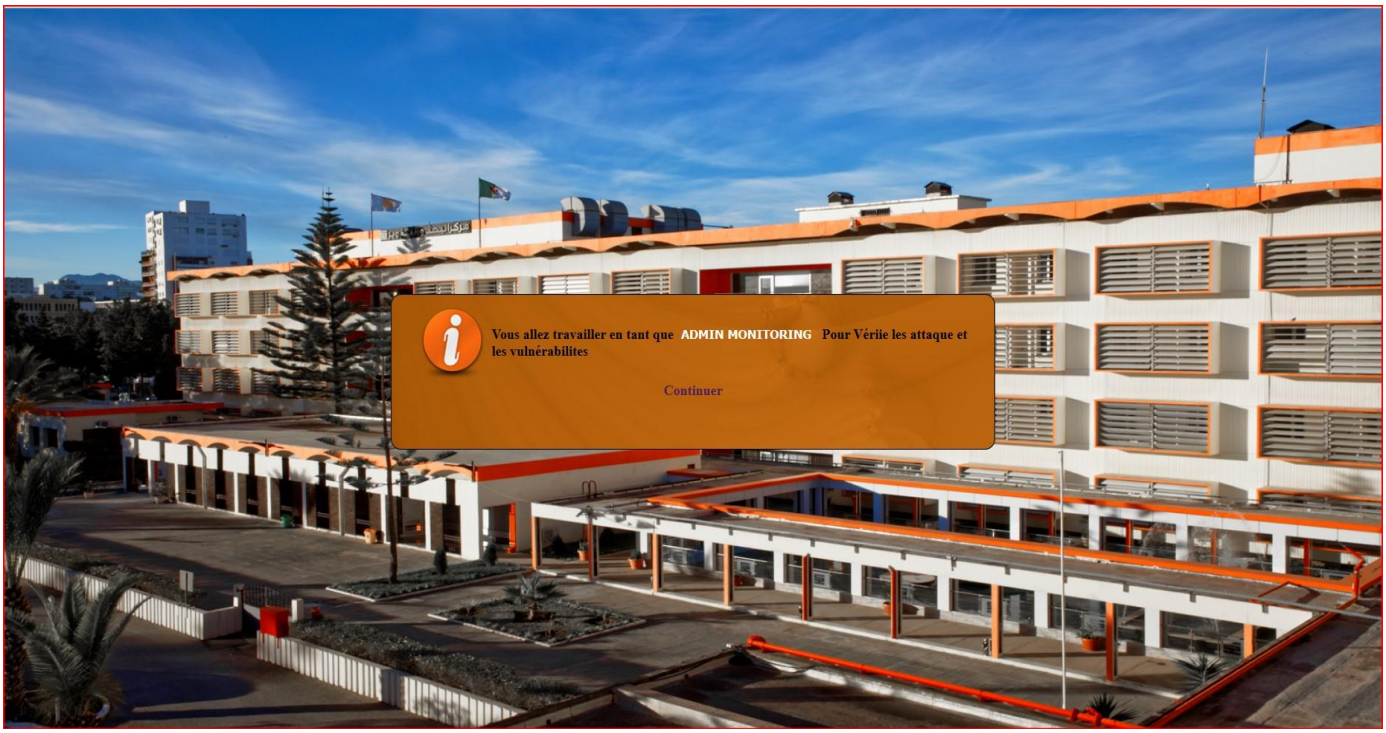


Figure IV- 49: page d'accueil d'administrateur monitoring.

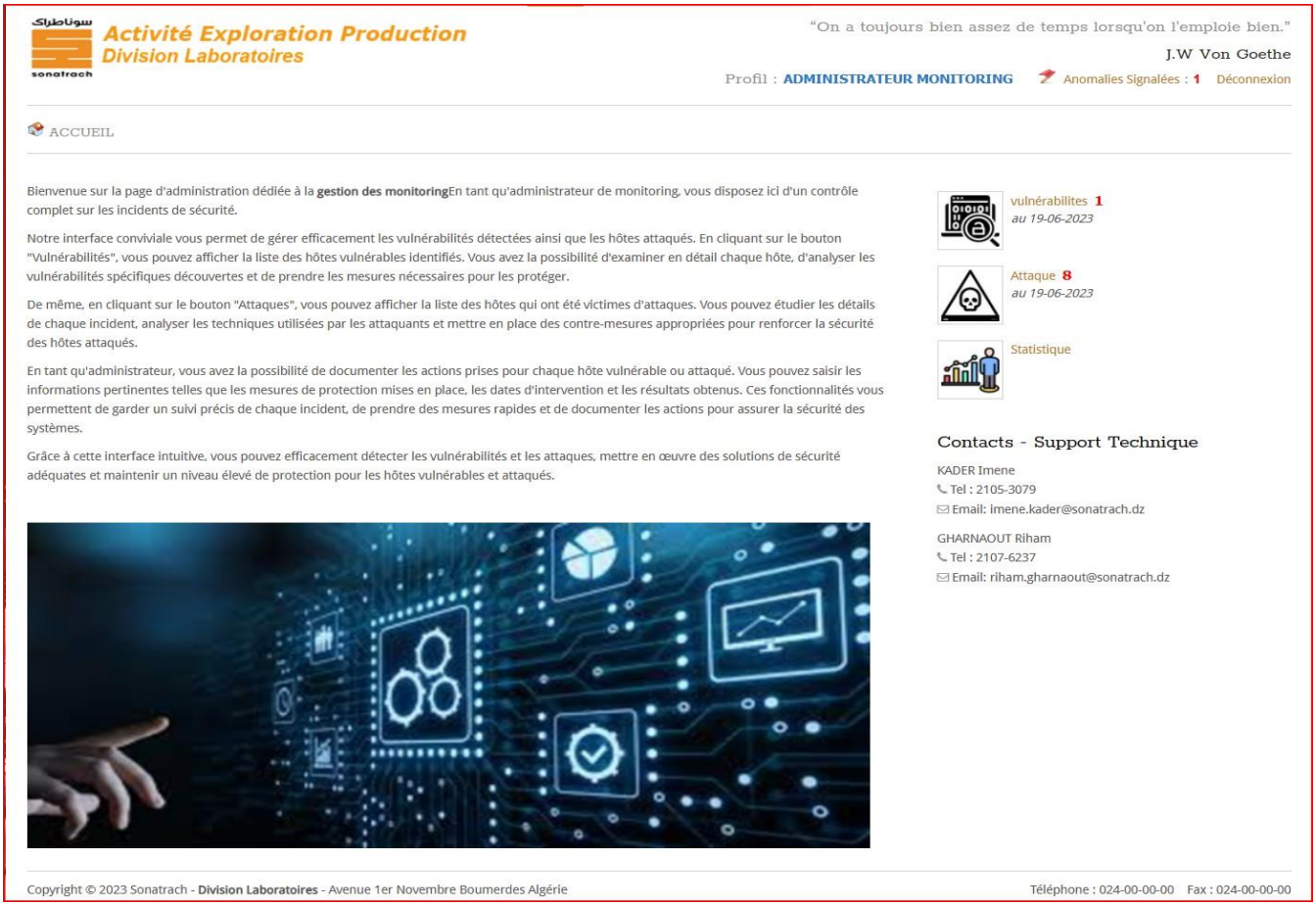


Figure IV- 50: Page profil d'administrateur monitoring.

- **Page vulnérabilité :**

Cette interface offre une fonctionnalité où, lorsqu'un administrateur détecte une Vulnérabilité, il peut remplir les informations suivantes pour documenter l'incident : le nom de l'hôte concerné par Vulnérabilité, le type de vulnérabilité exploitée, le type de système informatique concerné, le chemin par lequel la vulnérabilité a été exploitée et l'administrateur.

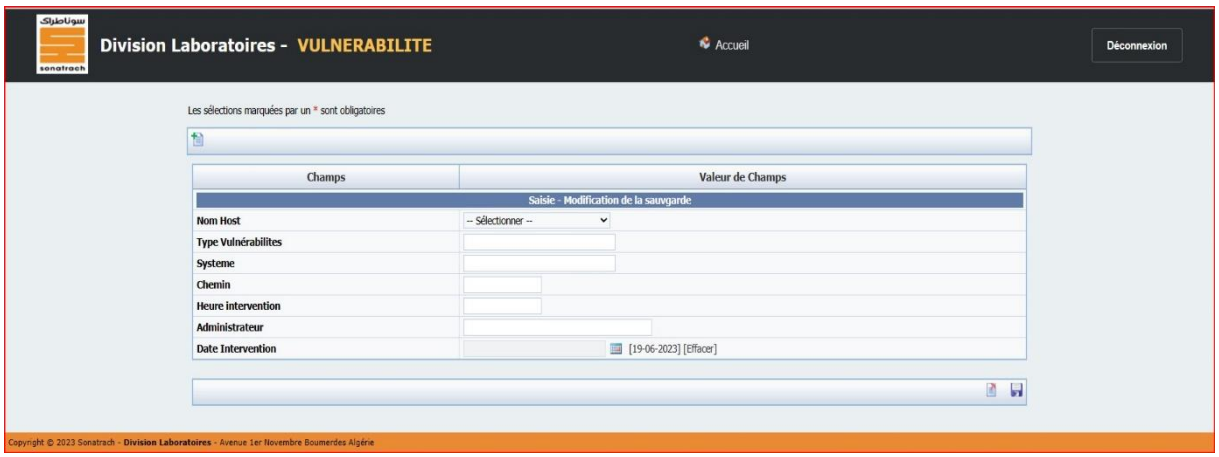


Figure IV- 51 : page administrateur détection de Vulnérabilité.

- Lorsque l'administrateur clique sur le bouton "Enregistrer", les informations sont saisies dans un tableau dédié. Ce tableau permet de consigner de manière organisée les détails de Vulnérabilité détectée. Ces informations sont cruciales pour une analyse plus approfondie de Vulnérabilité permettant ainsi de mieux comprendre les faiblesses du système qui ont été exploitées.

Ensuite, l'administrateur chargé de la protection revient sur l'interface et a la possibilité de saisir la date d'intervention spécifique liée aux mesures de protection prises. La date d'intervention fait référence à la période durant laquelle des actions ont été entreprises pour renforcer la sécurité du système. L'administrateur peut saisir cette date dans un champ dédié de l'interface. De plus, il est possible de spécifier l'état de la protection en

utilisant un choix binaire, soit "oui" si des mesures de protection ont été mises en place, soit "non" si aucune action n'a été entreprise.

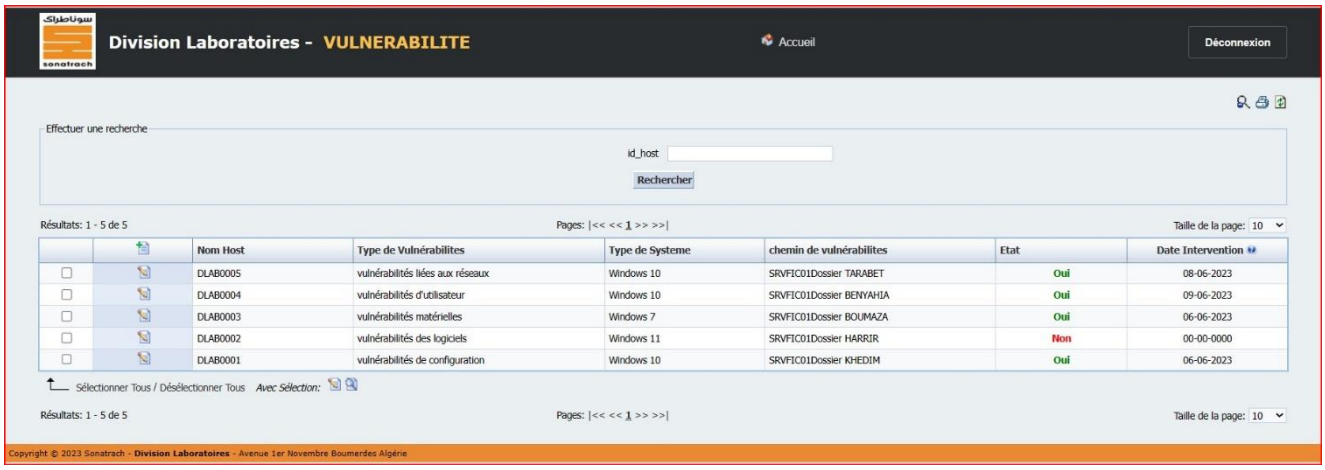


Figure IV- 52 :page administrateur de protection.

- **Attaque :**

Cette interface propose une fonctionnalité permettant à un administrateur de documenter les incidents liés à la détection d'attaques. Lorsqu'une attaque est identifiée, l'administrateur peut saisir les informations suivantes dans l'interface : le nom d'attaque concerné par l'attaque, le numéro de port d'attaque détectée, le nom d'host, et l'administrateur responsable de la détection. Ces informations servent à consigner de manière organisée les détails de l'attaque détectée.

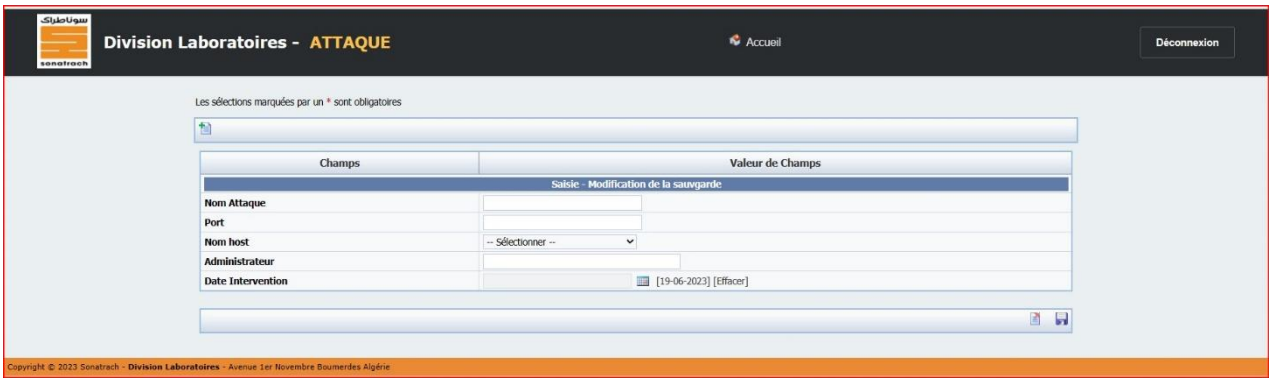


Figure IV- 53 :page administrateur détection d'attaque.

- Lorsque l'administrateur clique sur le bouton "Enregistrer", les informations sont saisies dans un tableau dédié. Ce tableau permet de consigner de manière organisée les détails de l'attaque détectée. Ces informations sont cruciales pour une analyse plus approfondie des attaques, permettant ainsi de mieux comprendre les méthodes utilisées par l'attaquant et les faiblesses du système qui ont été exploitées.

L'administrateur responsable de la contre-attaque peut ensuite accéder à l'interface et enregistrer la date d'intervention spécifique liée aux mesures de protection prises contre les attaques. Cette date d'intervention fait référence à la période durant laquelle des actions ont été mises en œuvre pour renforcer la sécurité du système. L'administrateur a la possibilité de saisir cette date dans un champ dédié de l'interface. De plus, il peut spécifier l'état de la protection en utilisant un choix binaire : "oui" pour indiquer que des mesures de protection ont été effectivement mises en place, ou "non" si aucune action n'a été entreprise jusqu'à présent. Cette fonctionnalité permet à l'administrateur de garder une trace des interventions réalisées, de mesurer l'efficacité des mesures de protection et de prendre les mesures nécessaires pour maintenir un niveau de sécurité adéquat face aux attaques.

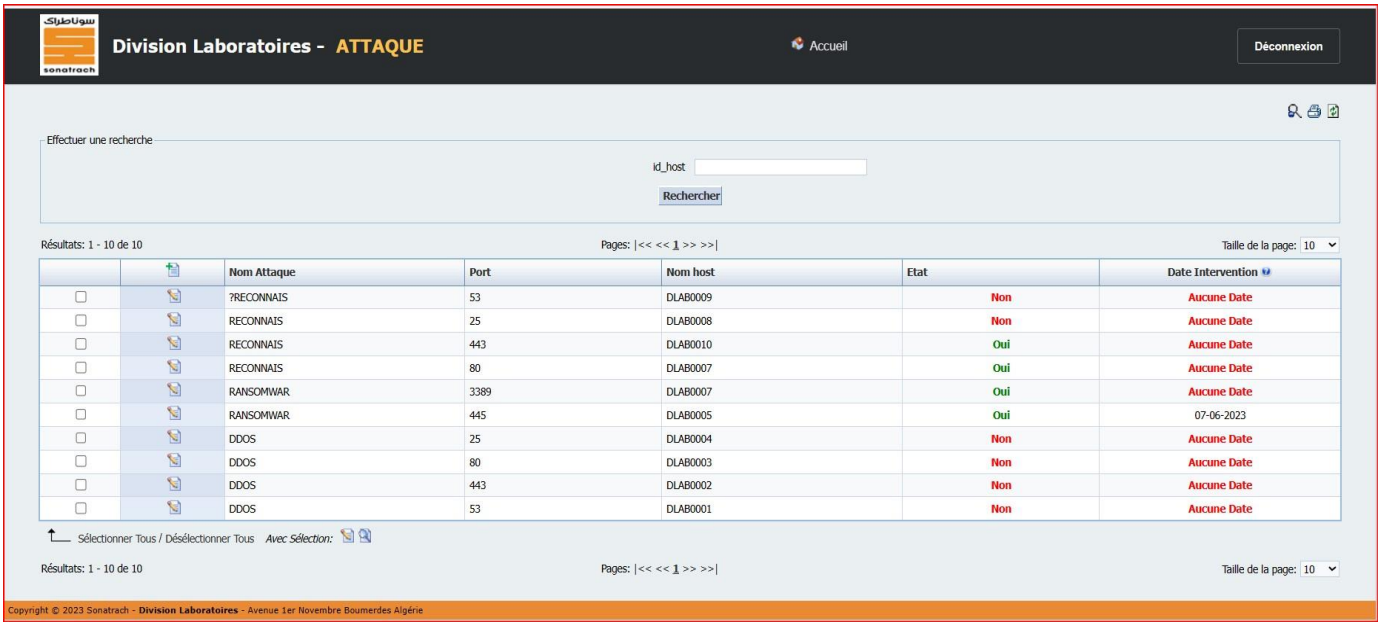


Figure IV- 54: page administrateur contre – attaque.

5.7 Statistique :

L'interface statistique est une fonctionnalité présente dans toutes les interfaces, notamment l'interface administrateur des dossiers, l'interface administrateur des applicatifs et l'interface de monitoring. Elle offre une vue globale et synthétique des informations liées à la gestion et à la sécurité du système. Cette interface statistique permet aux administrateurs de visualiser les statistiques importantes telles que le nombre total de dossiers, le nombre d'applicatifs, les sauvegardes effectuées, les patchs, les vulnérabilités détectées et les attaques enregistrées.

Les cercles représentent deux aspects clés de la gestion de la sécurité : la répartition globale de la protection en pourcentage et le pourcentage de protection réussie. Ces mesures jouent un rôle essentiel dans la gestion de la sécurité.

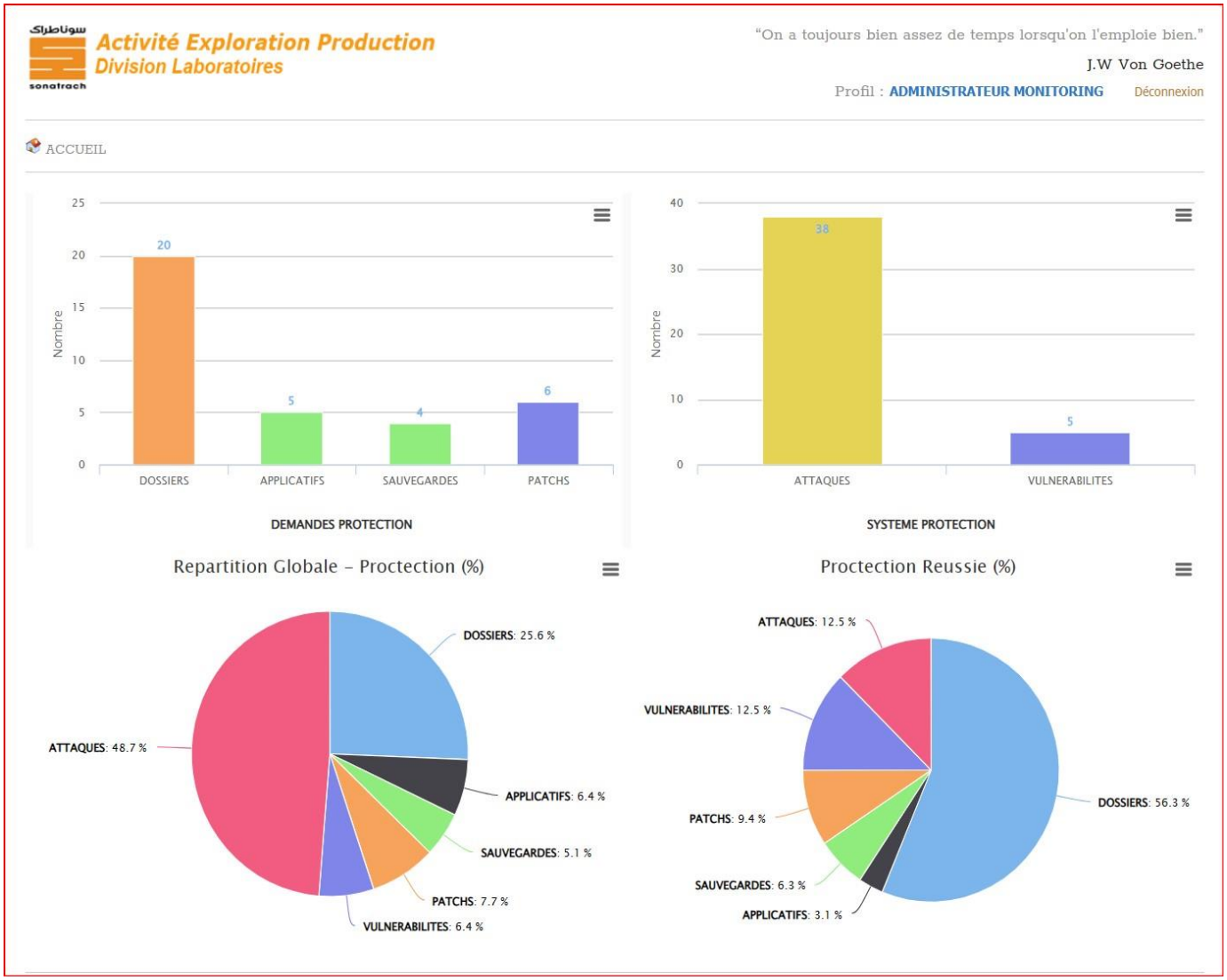


Figure IV- 55: Page statistique globale.

- Lorsque l'administrateur clique sur un dossier dans les statistiques de demande de Protection, le système affiche le nombre de dossiers traités et non traités.

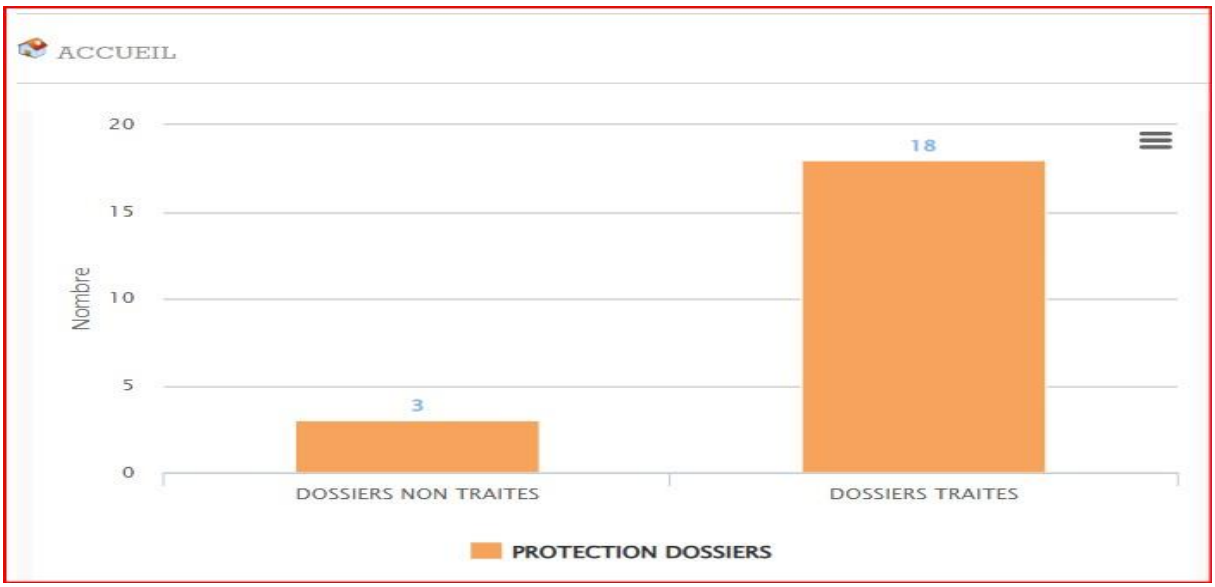


Figure IV- 56:Page statistique dossier.

- Lorsque l'administrateur clique sur applicative dans les statistiques de demande de protection, le système affiche le nombre d'applicative traités et non traités.

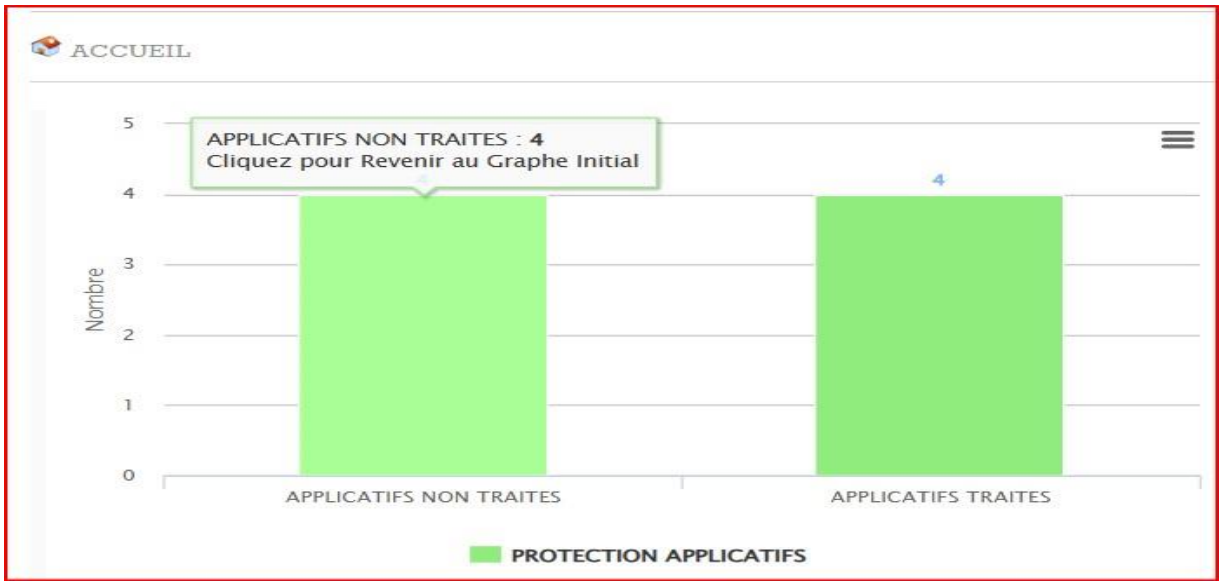


Figure IV- 57:Page statistique applicative.

- Lorsque l'administrateur clique sur sauvegarde dans les statistiques de demande de protection, le système affiche le nombre de dossiers, le nombre incrémental et complet.

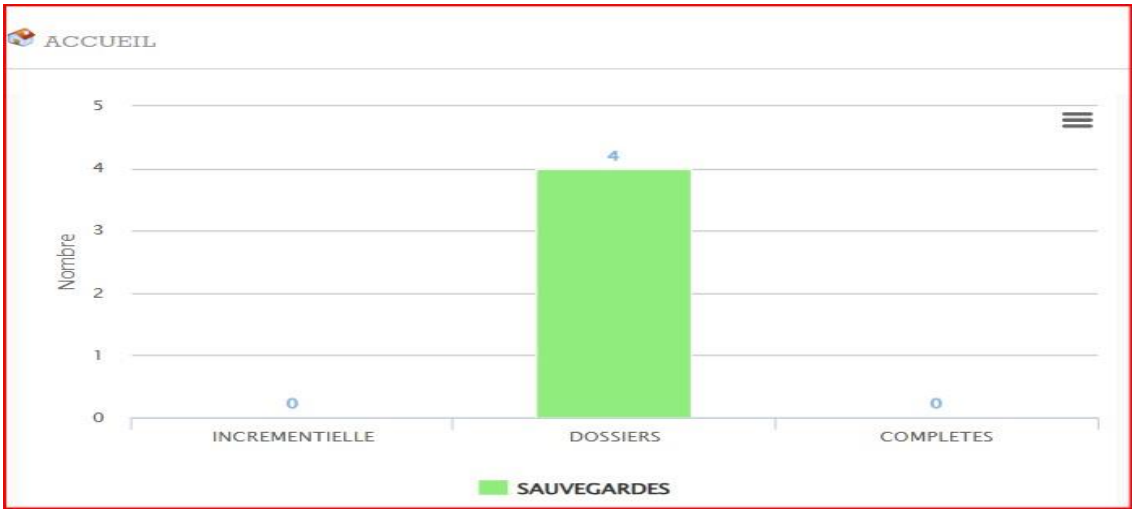


Figure IV- 58:Page statistique sauvegarde.

- Lorsque l'administrateur clique sur patchs dans les statistiques de demande de protection, le système affiche le nombre des patchs mise à jour et non mise à jour.

Figure IV- 59:page statistique patchs.

- Lorsque l'administrateur clique sur attaque dans les statistiques de système de protection, le système affiche le nombre d'attaque traités et non traités.

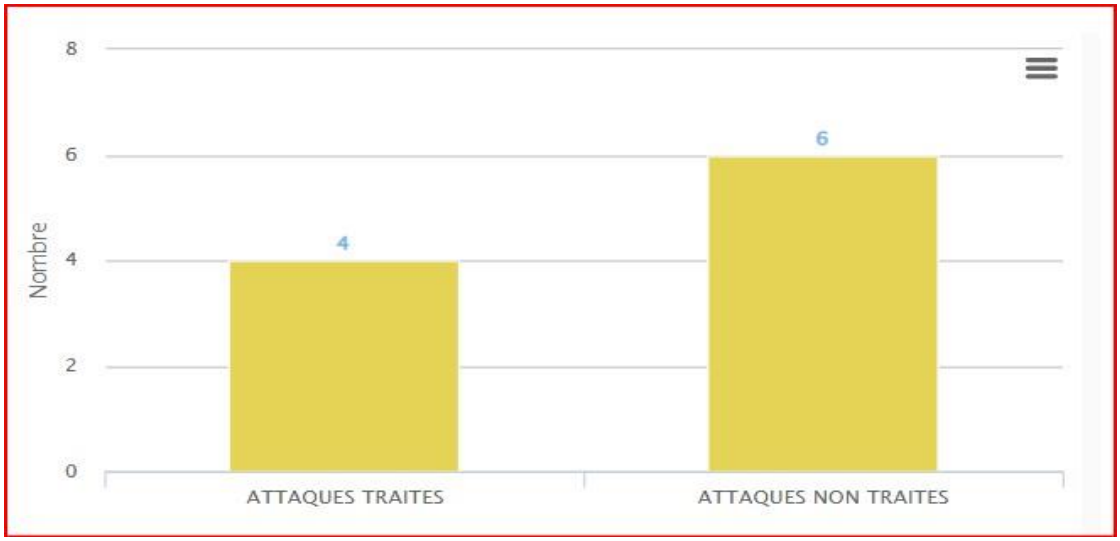


Figure IV- 60:page statistique attaque.

- Lorsque l'administrateur clique vulnérabilité dans les statistiques de système de protection, le système affiche le nombre vulnérabilité traités et non traités.

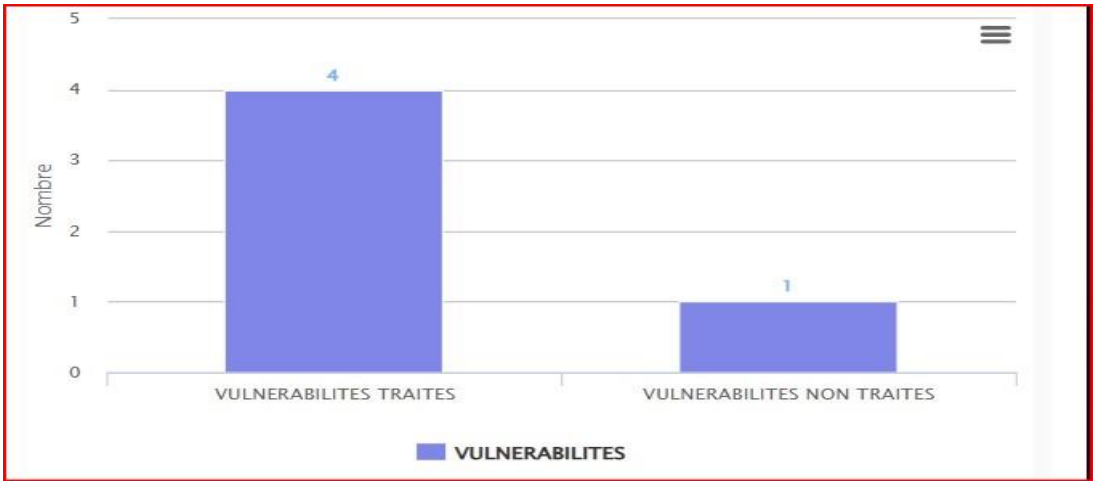


Figure IV- 61:page statistique vulnérabilité.

- **Répartition globale de la protection :**

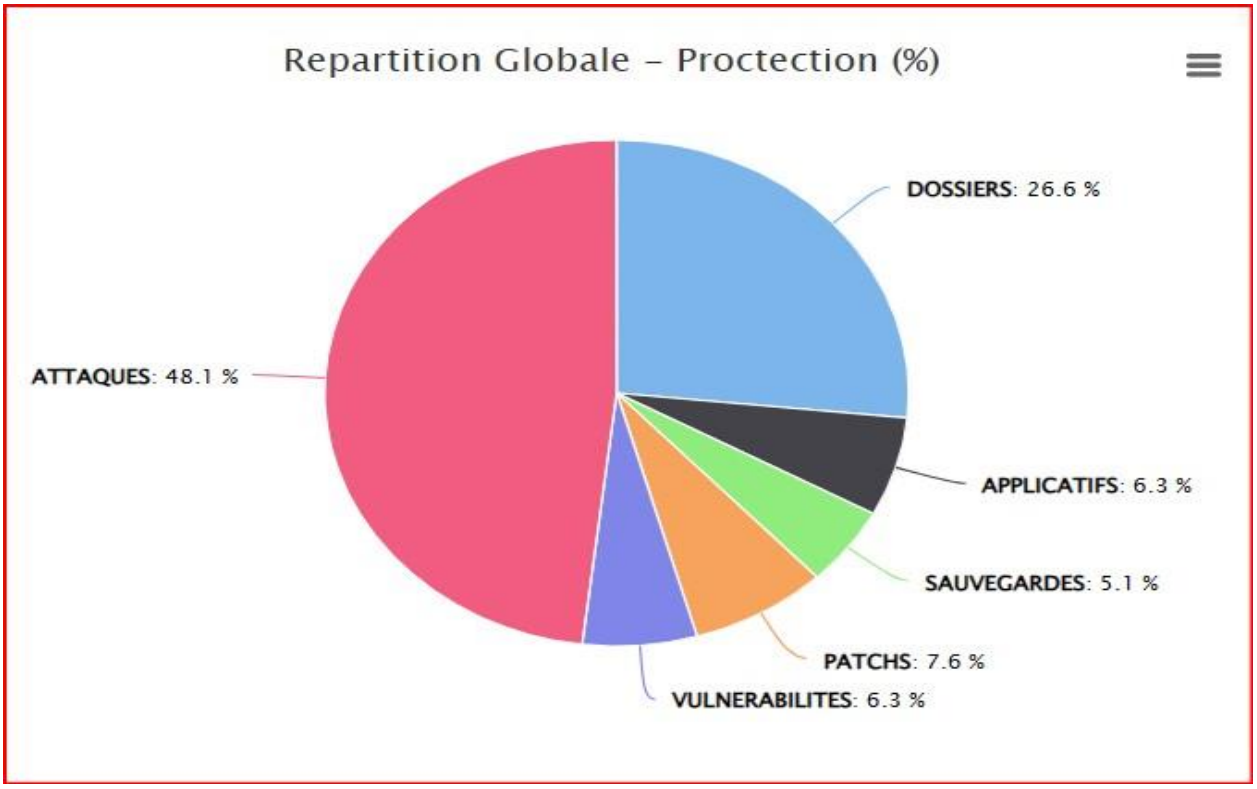


Figure IV- 62:Page répartition globale de la protection .

- **Protection réussie :**

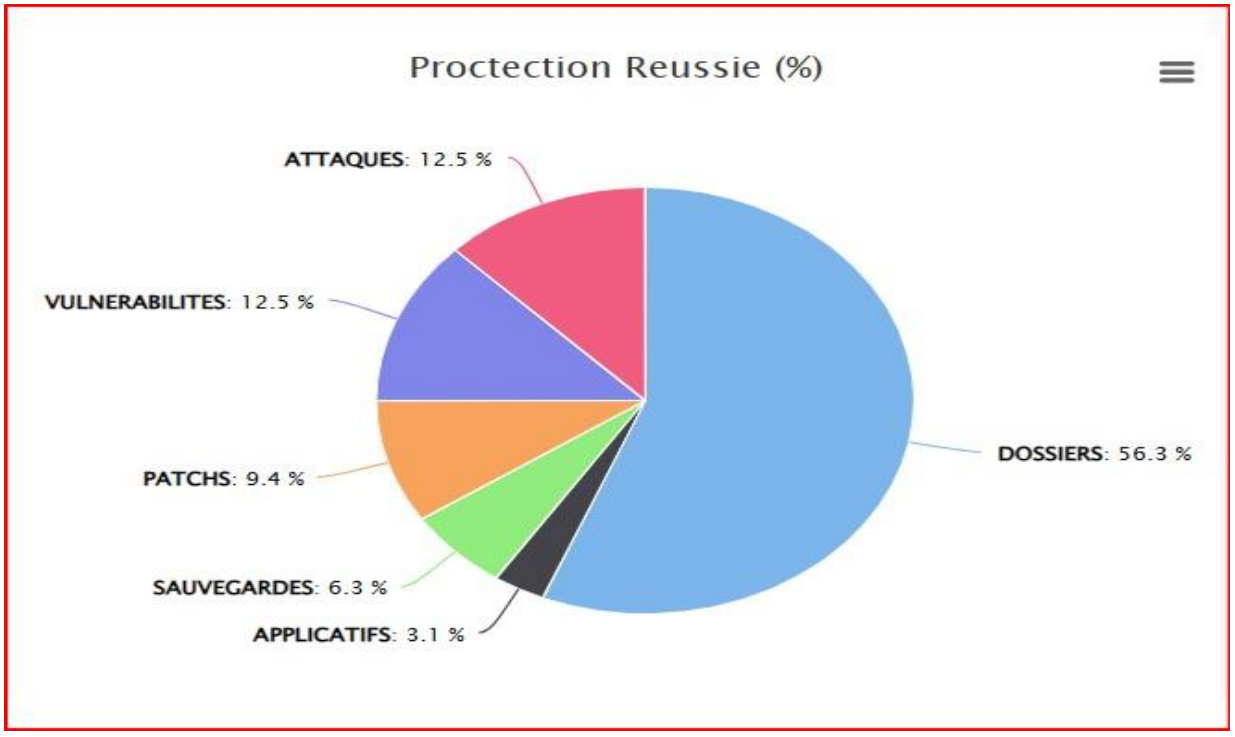


Figure IV- 63:Page protection réussie .

6 Conclusion :

La phase de réalisation est l'étape la plus importante dans le cycle de vie d'une application. Dans ce chapitre, nous avons présenté les aspects pratiques liés à l'application, tels que le diagramme de déploiement associé à notre système, suivi des langages, outils et logiciels de développement nécessaires. Enfin, nous avons illustré les principales interfaces incluses dans notre application et les outils garantissant la sécurité de notre système de protection.

CONCLUSION GÉNÉRALE

Aujourd'hui, les attaques ciblant les données sensibles sont de plus en plus puissantes et sophistiquées, ce qui compromet la sécurité des informations confidentielles. Notre intérêt pour la sécurité des systèmes d'information nous a motivés à adopter une solution dans la résolution des problèmes liés à la protection des données sensibles. Nous avons réalisé une étude approfondie sur la sécurité des systèmes d'information et la cryptographie pour acquérir une compréhension approfondie des enjeux et des risques associés à ces données dans un monde numérique en constante évolution.

Notre projet vise à fournir des solutions adaptées qui garantissent la confidentialité, l'intégrité et la disponibilité des informations sensibles. Nous cherchons à aider les entreprises à renforcer leurs infrastructures de sécurité, à établir des politiques et des procédures solides, ainsi qu'à former leur personnel pour réduire les risques de cyberattaques et de violations de données. Notre application web répond aux défis croissants de sécurité des données sensibles et aux attaques informatiques de plus en plus sophistiquées. Elle offre une solution complète pour la protection des dossiers sensibles, Grâce à des mesures de sécurité avancées, telles que le chiffrement des données et la gestion fine des autorisations d'accès les mises à jour régulières. Notre application vise à réduire les risques d'accès non autorisé en assurant que seules les personnes autorisées peuvent accéder aux informations confidentielles. En établissant ces objectifs, nous nous assurons que nos mesures de sécurité sont alignées sur les besoins réels de nos utilisateurs, ce qui garantit une protection efficace et adaptée de leurs données sensibles. Tout d'abord, nous avons identifié les différents utilisateurs et administrateurs qui interagiront avec notre application. Cela comprend les utilisateurs finaux, tels que les employés d'une entreprise, ainsi que les administrateurs chargés de gérer les autorisations et les paramètres de sécurité.

Ensuite, nous avons spécifié les besoins fonctionnels à travers des diagrammes de cas d'utilisation. Ces diagrammes décrivent les actions et les interactions entre les utilisateurs et les administrateurs et le système. En parallèle, nous avons utilisé des diagrammes d'activité pour modéliser les flux de travail et les processus internes de l'application.

La phase de conception a étendu la représentation effectuée lors de l'analyse en y intégrant les aspects techniques les plus proches des besoins spécifiques. Les livrables de cette phase comprenaient le diagramme de classe et le schéma relationnel.

La réalisation a été effectuée en utilisant les outils d'implémentation appropriés, en intégrant le contenu et le style, ainsi qu'en gérant la base de données avec des technologies telles que PHP/MySQL.

Notre projet joue un rôle essentiel dans la réalisation de nos objectifs et dans la résolution de notre problématique. Cependant, nous sommes conscients qu'il existe encore des possibilités d'amélioration de notre application, en prenant en compte les besoins de notre entreprise à savoir :

- Les mises à jour automatiques et les récupérer à partir des fichiers log de SCCM (System Center Configuration Manager)
- installer, configurer et intégrer Symantec Endpoint Protection Manager (SEPM) pour gérer les alertes.
- ajouter Symantec Backup Exec à notre système afin de bénéficier de la sauvegarde automatique.

Bibliographie& Webographie :

[1] https://sonatrach.com/ (Consulté le 12/03/2023)

[2]https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203373-serveur-dns-domain-name-system-definition/ (Consulté le 13/03/2023)

[3] ACHTA SOULEYMANE MOIDI, MAHAMAT MODOU ADAM MAINA, Jul 02, 2020 '' *SERVEUR DHCP SOUS LINUX*'' , polycopie de cours , Ecole Nationale Supérieure des TIC.

[4] Mr landoulsi Mohamed, 2019 ;'' *contrôle d'Access* '' , polycopie de cours ,institut supérieur des études technologique de radés .

[5] Hm Dh, Déc. 22, 2019,''*Projet Serveur de Fichiers"*, polycopie de cours .

[6] David Konan, Sep 22, 2020 '*'12.bdd.pdf",* polycopie de cours .

[7] https://www.oracle.com/dz/java/weblogic/ (Consulté le 14/03/2023)

[8] Majed Jallouli ; *''Introduction aux bases de données.pdf''* polycopie de cours.

[9] Ingrid Pilard, 05/01/23, ''*Active Directory : définition, avantages et différence avec le LDAP'' article* .

[10]https://www.techspot.com/downloads/150-symantec-norton-antivirus-definition-update.html (Consulté le 04/04/2023)

[11]https://www.logiciels.pro/logiciel-saas/symantec-endpoint-protection/ (Consulté le 11/04/2023)

[12] https://officemaker.fr/la-securisation-dans-le-cloud-de-vos-donnees- naura-jamais-ete-aussi-simple-symantec-endpoint-protection-cloude/ (consulté le 12/04/2023)

[13] https://www.computerhope.com/jargon/w/windows-2008.html (Consulté le13/04/2023)

[14] https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-server-2016 (Consulté le 17/04/2023)

[15]https://www.gladir.com/OS/WINDOWS2019SERVER/intro.htm (Consulté le 20/04/2023)

[16] https://www.microsoft.com/fr-fr/windows/end-of-support (Consulté le 22/04/2023)
[17]https://learn.microsoft.com/fr-fr/windows/release-health/status-windows-10-22h2 (Consulté le 25/04/2023)
[18]https://www.pocket-lint.com/fr-fr/ordinateurs/actualites/microsoft/157297-fonctionnalites-de-windows-11/ (Consulté le 27/04/2023)
[19] Howard, juin 10, 2021,'' *Comment choisir le switch de distribution idéal ?* '', article .
[20] Damien Soulages, 31 août 2018,'' *Redondance des Switchs et Problèmes liés à la redondance", article* .
[21] Worton, juil. 29, 2021,'' *Présentation du contrôleur de réseau local sans fil et questions fréquentes", article* .
[22] Sheldon, juil. 28, 2021,'' *Switch de niveau 3 ou routeur : Quelle est la meilleure option ?" , article.*
[23] dualcorefree, Oct. 07, 2009,'' *Topologies Des Réseaux' ',*article .

[24] Joelle Mumley (15/11/2021), "*What is Cybersecurity? – Definition & Principles",* study, Retrieve, article .

[25] Yakout Fet, May 29, 2021,*'' Cours Sécurité de L'information''*, polycopie de cours .

[26]http://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information(Consulté le 05/05/2023)

[27] Cyberjobs Médias, 31 OCTOBRE 2021, '' *Zoom sur les 5 objectifs de la sécurité informatique*'', article .

[28] intrapole, 18 mars 2009, ' *'Confidentialité / Intégrité / Disponibilité''*, article.

[29] DAHMANE Mourad ; Juin 2014 ; ' *'Sécurité des Systèmes d'Information (SSI)*'', Mémoire de Fin d'études En vue de l'obtention du diplôme de Master en Informatique Spécialité : Conduite de Projets Informatiques(CPI),2014.

[30] https://infonet.fr/lexique/definitions/donnees-sensibles/(Consulté le 07/05/2023)

[31] . Pierre-Louis Lussan, 17 octobre 2022, Country Manager South-West Europe," *Les bases de la sécurité et de la protection des données*" , article .

[32] Dr. Mohamed Amine FERRAG, 2018,' *'Sécurité Informatique*'' ,Polycopie de cour .

[33] SALEM OUSSAMA YACINE , BRAIK AZOUAOU ,BAFFOU AHMED , ''les honeypots/ IDS'', Mémoire de Fin d'études , M'Hamed bougara , Boumerdes , 2021/2022 .

[34] Ghislain Danny BATOMEN YANGA, Gisèle MEKUATE DEFO ;; Janvier 2012 – '*'LES SYSTEMES DE GESTION DES IDENTITES ET DES ACCES : MISE EN ŒUVRE ET APPORT POUR LA SECURITE D'UNE ORGANISATION*'' , Mémoire de Fin d'études.

[35] Patrick Boucher, Déc. 21,2021 ; '*'Les 6 étapes d'une gestion des incidents de sécurité de l'information* '', article .

[36]https://www.proofpoint.com/fr/threat-reference/compliance-management (Consulté le 10/06/2023)

[37]https://www.hpe.com/be/fr/what-is/security-monitoring.html(consulté le 11/06/2023)

[38] HAFSI Meriem, GBOBIA Arnaud Koudou ; 2012 / 2013 ''*Développement d'une ontologie pour la Sécurité Informatique''* , Mémoire de Fin d'études.

[39]https://www.orangecyberdefense.com/fr/insights/blog/gestion-des-vulnerabilites/vulnerabilites-de-quoi-parle-t-on (Consult le 11/06/2023)

[40] Julien Iguchi-Cartigny ; 04 Mars au 30 Août 2013 ;'' *Scenarios d'Attaques et Détection d'Intrusions ''*, Mémoire de Fin d'études.

[41] Amine Abdeljaoued; *" Etude technique de l'attaque de Buffer Overflow" , Projet de Fin d'Etudes* .

[42] https://www.formatio.info/files/Les-Virus.pdf(Consulté le 15/06/2023)

[43] François Paget, '*'Vers & Virus - Classification, lutte anti-virale et perspectives, DUNOD''*, 2005, livre.

[44] ONDAPHE CHRISTIAN ARTHUR; '*'COURS DE SECURITE INFORMATIQUE''*, polycopie de cour .

[45]https://learn.microsoft.com/fr-fr/security-updates/security/20200343 (Consulté le 16/06/2023)

[46]https://www.avast.com/fr-fr/c-trojan#:~:text=ou%20Windows%2011.-,Comment%20fonctionnent%20les%20chevaux%20de%20Troie%20%3F,d'autres%20types%20de%20dommages(Consulté le 17/06/2023)

[47] Paul RASCAGNERES,*''analyse des menaces et mise oeuvre des contre-mesures'' ;* édition : avril 2016 , livre .

[48] Cyber Albert,*'' Les guides de la cyber sécurité''* Décembre 6, 2022, article .

[49] *Darril hall and Erin watson :computer Security testing, Penetration and basic security*, 2016, polycopie de cour .

[50] Aida Soufi ; 23 octobre 2011 ; '' *Le canular informatique (hoax)* '', article .

[51] Sandrine Cestpafo '*'Que sont les attaques de reconnaissance et comment fonctionnent-elles* ?'' - 22 mars 2023, article .

[52] Jeremy Cioara, David Minutella, Heather Stevenson; Dec 19, 2007;'' CCENT Exam Prep (Exam 640-822)'', livre.

[53] EasyDmarc;'' *What is a Password Attack in Cyber Security*?'' May 29, 2022 , article .

[54] Dr Radja Boukharrou, '*'Sécurité des réseaux''*, 20192020 , polycopie de cour .

[55]https://www.futura-sciences.com/tech/definitions/cybersecurite-attaque-man-in-middle-10048/(Consulté le 20 /06/2023)

[56] Mr. Ahmed ZEBOUDJ, Mr. Nassim KHOBZI'' *CONCEPTION D'UN SYSTEME DE DETECTION D'INTRUSION BASE SUR UN ARBRE DE DECISION''* 2014/2015 , mémoire fin d'étude .

[57]https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-are-sniffing-attacks/ (Consulté le 20/06/2023)

[58]https://www.techtarget.com/searchsecurity/definition/dictionary-attack (Consulté le 21/06/2023)

[59] Megan Rees Updated Nov 25, 2022 ‘’ *the 8 Most Common Types of Password Attacks ‘’*, article .

[60] ADDA Imane, DAOU Silia ;2021 ; *Mise en œuvre d’une solution de sécurité basée sur le pare-feu PfSense pour l’Entreprise Portuaire de Béjaïa*, mémoire fin d’étude .

[61] https://pdfbib.com/193-cours-formationhacking-piratage.pdf.(Consulté le 22/06/2023)

[62] Yasmine chihab , ‘’10 anti virus’’ , polycopie de cour .

[63] https://habefast.ch/glossaire/html/ (Consulté le 22/06/2023)

[64]https://www.websiterating.com/fr/website-builders/glossary/what-is-css/ (Consulté le 23/06/2023)

[65]https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203585- javascript/ (Consulté le 23/06/2023)

[66] https://www.w3schools.com/php/php_intro.asp (Consulté le 23/06/2023)

[67] https://www.mysql.com/what-is-mysql/ (Consulté le 23/06/2023)

[68] https://www.blogdumoderateur.com/tools/notepad/ (Consulté le 24/06/2023)

[69]https://www.capterra.fr/software/82970/edrawmax#:~:text=Edraw%20Max%20est%20un%20logiciel,de%20travail%2C%20structures%20de%20programmes%2C(Consulté le 26/06/2023)

[70] Badja riad,Djabali nacer yacine ,Messoudene Khaled .*mémoire de fin de cycle Conception et réalisation d’un site web dynamique dédié aux boutiques en ligne. Université de Bejaïa. 2013*.