République Algérienne Démocratique et Populaire
الجمهورية الجزائرية الديمقراطية الشعبية
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
وزارة التعليم العالي والبحث العلمي
Université de SAAD DAHLEB BLIDA 1
جامعة سعد دحلب البليدة1

Mémoire de fin d'études

En vue de l'obtention du diplôme de Master en informatique

Option :

Sécurité des systèmes d'information

Par

Rabah AROUDJ et Abdelghani BELAIDI

Implémentation d'une plateforme de sensibilisation sur la cybersécurité

Soutenu le jj/06/2023, devant la commission d'examen :

Mme. Leila OUAHRANI	Présidente
Mme. Imane CHIKHI	Examinatrice
Mme. Imane CHERFA	Promotrice
M. Abdeldjallil HANNOUN	Encadrant

Promotion : 2022/2023

Dédicaces

À Allah

Tout puissant qui m'a inspiré, qui m'a guidé dans le bon chemin, je vous dois ce que je suis devenu. Louanges et remerciements pour votre clémence et miséricorde.

À Mes très chers parents

Aucune phrase, nul remerciement ne saurait être suffisant pour exprimer l'amour que j'ai pour vous. Vous m'avez entouré d'une grande affection, Sans vos prières, votre générosité et votre dévouement, je n'aurais pu surmonter le stress de ces longues années d'étude. Merci d'avoir toujours cru en moi, ce travail est le fruit de vos sacrifices et soutien tout au long de ces années, que dieu vous protège et vous garde en bonne santé.

À Ma sœur et mon frère adorés

Yasmine et Abderahmene pour leurs encouragements et leur soutien moral. Merci d'être toujours là pour moi, que dieu vous protège.

À Mon cher binôme

Rabah pour tous ce qu'on a vécu et passé ensemble tout au long de ces années.

À Mes très chers amis et collègues

Sofyane, Khalil, Mohamed, Abdelhak pour leurs soutiens et leurs encouragements.

À tous ceux qui me sont très chers et que j'ai omis de citer.

Merci !.

Abdelghani

À Allah

Tout puissant qui m'a inspiré, qui m'a guidé dans le bon chemin, je vous dois ce que je suis devenue. Louanges et remerciements pour votre clémence et miséricorde.

À Mes très chers parents

Aucune phrase, aucun mot ne saurait exprimer à sa juste valeur le respect et l'amour que je vous porte. Vous m'avez entouré d'une grande affection, Sans vos prières, votre générosité et votre dévouement, je n'aurais pu surmonter le stress de ces longues années d'étude. .A travers ce modeste travail, je vous remercie et prie Dieu le tout puissant qu'il vous garde en bonne santé.

À Ma grand mère

Ces quelques lignes ne sauraient exprimer toute l'affection et tout l'amour que je vous dois. Que dieu vous préserve et vous accorde santé et prospérité.

À mes frères et mes sœurs

Omar, Mustapha, Hamza, Hamida, Nora, Kheira, Hakima J'ai beaucoup de chance de vous avoir à mes côtés, et je vous souhaite beaucoup de bonheur et de réussite.

À tous les membres de ma grande famille

ls n'ont épargné aucun effort pour m'aider et me soutenir.

À Mon cher binôme

Abdelghani avec qui j'ai passé les plus beaux jours de ma vie. . .des jours inoubliables pleins de couleurs et de rires.

À Mes très chers amis et collègues

Abdelhak, Nadir, Hicham, Billel pour leurs soutiens et leurs encouragements.

À tous ceux qui me sont très chers et que j'ai omis de citer.

Merci !.

Rabah

REMERCIEMENT

Nous aimerions prendre un moment pour exprimer nos sincères remerciements à toutes les personnes qui ont joué un rôle important dans la réalisation de ce travail.

Tout d'abord, nous tenons à remercier du fond du cœur Dieu le tout puissant, qui nous a accordé la force, le courage et la patience nécessaires pour surmonter toutes les difficultés rencontrées lors de notre parcours. Sa grâce et sa bénédiction ont été essentielles pour mener à bien ce modeste travail.

Ensuite, nous souhaitons exprimer notre profonde reconnaissance envers notre promotrice, le Dr CHERFA Imène. Sa disponibilité inépuisable, sa tolérance, ses orientations précieuses et ses conseils éclairés ont été d'une valeur inestimable tout au long de ce processus. Sa bienveillance et son soutien constant nous ont permis de progresser et d'atteindre nos objectifs.

Nous exprimons nos chaleureux remerciements à toute l'équipe de l'entreprise MNA Algérie, en particulier au directeur BELARBI Mohamed Abdou, ainsi qu'à NABAOUI Fayçal et à tous les autres intervenants professionnels qui ont généreusement contribué à la partie pratique de ce mémoire. Leur expertise, leur collaboration et leur assistance ont enrichi notre travail et nous ont permis d'acquérir des connaissances précieuses dans notre domaine d'étude.

À notre Maître et Présidente de Jury, le Dr AYACHI Nabila, ainsi qu'à notre examinatrice, le Dr OUCIF Ghania, nous exprimons une gratitude sincère pour avoir accepté d'évaluer notre travail. Votre expertise, votre engagement et votre disponibilité ont été d'une importance capitale pour nous. Votre évaluation approfondie et vos commentaires constructifs nous ont permis de parfaire notre travail et de le présenter de la meilleure façon possible.

Enfin, nous aimerions témoigner notre profonde reconnaissance à toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de cette thèse. Que ce soit par leur soutien moral, leurs conseils, leurs encouragements ou leur collaboration, leur contribution a été précieuse et nous leur en sommes infiniment reconnaissants.

Nous sommes conscients que ce travail n'aurait pas été possible sans l'aide et le soutien inestimables de toutes ces personnes, et nous tenons à leur exprimer notre profond respect, notre gratitude sincère et notre reconnaissance éternelle.

Résumé :

Aujourd'hui, les organisations exploitent de plus en plus les technologies de sécurité avancées et offrent une formation continue à leurs professionnels de la sécurité. Cependant, très peu d'efforts sont déployés pour sensibiliser les utilisateurs ordinaires à la sécurité de l'information, ce qui les rend vulnérables et constitue le maillon le plus faible de toute organisation. Par conséquent, les cybercriminels organisés concentrent leurs efforts sur l'exploitation des erreurs humaines afin de réussir leurs missions.

Ce travail s'intéresse justement à la sensibilisation, et répond à des besoins exprimés par l'équipe de MNA Groupe. Nous proposons une solution qui a pour objectif de sensibiliser le personnel en proposant des formations et des simulations d'attaques automatisées de phishing. Il permet aux entreprises de gérer ces attaques et formations de manière complète, en incluant la possibilité d'ajouter, d'affecter et de modifier les scénarios. De plus, il offre aux employés la possibilité de suivre ces formations et de les valider. Notre solution est utilisable par les entreprises et leurs employés, et offre un volet de suivi qui permet la visualisation, le suivi et l'exploitation des données grâce à un tableau de bord affichant les statistiques. Cette fonctionnalité aide les entreprises à évaluer leur niveau de maturité en matière de sécurité.

Mots clés : Formation, Sensibilisation, attaque automatisée, phishing, sécurité.

ملخص :

اليوم، تستغل المؤسسات التقنيات المتقدمة في مجال الأمان بشكل متزايد وتوفر تدريبًا مستمرًا لمحترفي الأمان الخاصة بها. لكن، يتم بذل جهود قليلة جدًا لتوعية المستخدمين العاديين بأمن المعلومات، مما يجعلهم عرضة للتهديدات ويشكلون أضعف حلقة في أي منظمة. وبالتالي، يركز المجرمون السيبرانيون المنظمون .جهودهم على استغلال الأخطاء البشرية لتحقيق مهماتهم

النسخة الأولى من النظام تهدف إلى توعية الموظفين من خلال تقديم التدريب ومحاكاة هجمات الصيد الاحتيالية المتواجدة بشكل آلي. يتيح للشركات إدارة هذه الهجمات والتدريب بشكل شامل، بما في ذلك إمكانية إضافة وتعيين وتعديل السيناريوهات. بالإضافة إلى ذلك، يوفر للموظفين إمكانية متابعة هذه التدريبات. تسمح حلولنا أيضًا باستخدام النظام بواسطة عدة مستخدمين من الشركات وموظفيها، مع توفير جانب للمتابعة يمكن من خلاله عرض وتتبع واستخدام البيانات من خلال لوحة إحصائية. تساعد هذه الميزة الشركات في تقييم مستوى نضجها في مجال الأمان. سيتم تصميم النظام القائم حاليًا للتكيف مع التغيرات لمواجهة التهديدات الجديدة التي .تستغل العامل البشري

هدفنا الرئيسي من خلال هذا المشروع التخرج هو تقديم الحل المناسب لتوعية موظفي الشركات وتلبية الاحتياجات المعبر عنها من قبل فريق MNAGroupe.

الكلمات المفتاحية: التدريب، هجمات الصيد الاحتيالية، أمن المعلومات، لوحة إحصائية، التهديدات

Abstract :

Today, organizations are increasingly leveraging advanced security technologies and providing ongoing training to their security professionals. However, very little effort is being made to raise awareness among ordinary users about information security, making them vulnerable and constituting the weakest link in any

organization. As a result, organized cybercriminals focus their efforts on exploiting human errors to accomplish their missions. The first version of the system aims to raise awareness among staff by offering training and automated phishing attack simulations. It enables companies to manage these attacks and training comprehensively, including the ability to add, assign, and modify scenarios. Additionally, it provides employees with the opportunity to undergo these training sessions. Our solution also allows for multi-user usage of the system by companies and their employees, while offering a tracking feature that allows for visualization, monitoring, and data exploitation through a statistical dashboard. This functionality helps companies assess their level of security maturity. The ongoing design of the system will be adaptable to changes in order to address new threats that exploit the human factor. Our main objective through this final year project is to provide the appropriate solution to raise awareness among company personnel and meet the expressed needs of the MNA Group team.

Key-words : Awareness, information security, training, phishing attacks, dashboard.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

AOL	*America Online*
APT	*Menaces Persistantes Avancées*
ASAP	*Automated Security Awareness Platform*
FBI	*Federal Bureau of Investigation*
IC3	*The Internet Crime Complaint Center*
ICS	*Industrial Control Systems*
IDS	*les systèmes de détection d'intrusion*
ISO	*International Organization for Standardization*
LID	*Lutte Informatique Défensive*
MNA	*Mare Nostrum Advising*
OVH	On Vous Héberge
PECB	*Professional Evaluation and Certification Board*
RGPD	*Règlement Général sur la Protection des Données*
SIEM	*Security Information and Event Management*
SMSI	*Système de Management de la Sécurité de l'Information*
TI	*Technologie de l'Information*
UML	*Unified Modeling Language*

Glossaire

Actifs : Tout système d'information, matériel informatique et de télécommunications, logiciels, progiciels, listes, banques de données et informations (textuelle, sonore, symbolique ou visuelle) placées dans un matériel informatique ou sur un média informatique et/ou électronique [10].

Confidentialité : Confidentialité. Garantit que les données sont uniquement consultées par des utilisateurs autorisés disposant des informations d'identification appropriées [4].

Chevaux de Troie : sont des programmes informatiques cachés dans d'autres programmes. Le but d'un cheval de Troie est de créer une porte dérobée (backdoor) pour qu'un pirate informatique puisse ensuite accéder facilement l'ordinateur ou le réseau informatique. Il peut aussi voler des mots de passe, copier des données, exécuter des actions nuisibles [19].

Disponibilité : Garantit que les données peuvent être consultées à tout moment et de manière sécurisée pour répondre aux besoins continus de l'entreprise [4].

Intégrité : Garantit que toutes les données stockées sont fiables, exactes et exemptes de modifications non justifiées [4].

Les IDS (Intrusion Detection Systems) : analysent et surveillent le trafic réseau pour détecter des signes indiquant que des hackers utilisent un cyber menace connue afin de s'infiltrer dans votre réseau ou y voler des données. Les systèmes d'IDS comparent l'activité réseau en cours avec une base de données d'attaques connues afin de détecter divers types de comportements tels que les violations de la politique de sécurité, les malwares et les scanners de port [16].

Menace : peut-être tout ce qui peut profiter d'une vulnérabilité pour violer la sécurité et altérer, effacé, nuire à un ou plusieurs objets d'intérêt [11].

OVH :est une entreprise française spécialisée dans les services d'hébergement et de cloud computing. Fondée en 1999 par Octave Klaba, OVH est devenue l'un des principaux acteurs mondiaux dans le domaine de l'hébergement web.

Ransomware (le malware de rançonnage) : est un type de malware qui empêche les utilisateurs d'accéder à leur système ou à leurs fichiers personnels et exige le paiement d'une rançon en échange du rétablissement de l'accès [24].

SIEM (Security Information and Events Management) : est une solution logicielle qui regroupe et analyse l'activité de nombreuses ressources différentes sur l'ensemble de votre infrastructure informatique [17].

Scam : Le scam est un message e-mail non sollicité qui contient une proposition alléchante cachant une escroquerie [20].

Vulnérabilité : Une vulnérabilité est une faille de sécurité. Elle provient dans la majorité des cas d'une faiblesse dans la conception d'un système d'information (SI), d'un composant matériel ou d'un logiciel [9].

Virus : On peut cependant définir un virus comme un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs [19].

Zero-day : sont des cybermenaces sur une vulnérabilité publiquement inconnue d'un système d'exploitation ou d'une application [26].

INTRODUCTION GÉNÉRALE

La cybersécurité vise à protéger les ordinateurs, serveurs, appareils mobiles, systèmes techniques et réseaux contre les attaques malveillantes. Elle est également connue sous les termes de sécurité des systèmes d'information ou sécurité informatique. Les risques liés à la sécurité des informations sont présents dans différents contextes, allant de l'informatique d'entreprise aux terminaux mobiles. Les utilisateurs des systèmes d'information peuvent être inconscients des dangers et des attaques perpétrées par des hackers. Afin de remédier à cela, il est essentiel de sensibiliser les utilisateurs des systèmes d'information au sein des entreprises aux dangers et aux attaques.

Avant d'expliquer la mise en œuvre d'une plateforme de sensibilisation à la cybersécurité, plusieurs questions se posent et il serait idéal de les exprimer. Nous cherchons à avoir une vision claire du travail futur. Notre principale préoccupation est de savoir comment sensibiliser efficacement les utilisateurs des systèmes d'information au sein des entreprises aux dangers en général, et plus spécifiquement au phishing. Les employés sont-ils capables de reconnaître les courriels infectés par le phishing ? Quelles méthodes devrions-nous utiliser pour assurer une sensibilisation fiable ?

Notre projet de fin d'études consiste à mettre en place une plateforme de sensibilisation sur la cybersécurité., pour l'entreprise MNA (Mare Nostrum Advising) Groupe. L'objectif principal de ce travail consiste à sensibiliser les fonctionnaires des entreprises à l'importance de la cybersécurité de manière générale, en mettant un accent particulier sur la lutte contre les dangers et les attaques, en particulier le phishing. Nous visons également à tester et à renforcer le niveau de sécurité au sein des entreprises, afin de garantir une protection adéquate contre les menaces informatiques. Dans cette optique, nous prévoyons de mettre en place une plateforme dédiée à la sensibilisation, qui permettra également d'automatiser une attaque de phishing afin de la rendre plus facilement utilisable et efficace. L'objectif final est de fournir aux fonctionnaires des entreprises un outil pratique et interactif qui leur permettra de mieux comprendre les risques liés à la cybersécurité et de renforcer leurs connaissances en matière de prévention et de lutte contre le phishing, tout en améliorant le niveau global de sécurité dans les organisations.

Notre mémoire est structuré en quatre chapitres, organisés de la manière suivante :
Le premier chapitre se compose de deux parties. Dans la première partie, nous présenterons l'organisme d'accueil, le MNA Groupe. La deuxième partie sera consacrée aux notions de base de la cyber sécurité sur lesquelles repose notre projet.

Le deuxième chapitre sera consacré à un état de l'art sur la sensibilisation à la cyber sécurité. Nous présenterons également des outils similaires et les comparerons entre eux.

Le troisième chapitre donnera une vision globale de l'architecture et des fonctionnalités de notre solution. Nous aborderons la conception globale et détaillée qui illustrera notre approche et notre raisonnement.

Dans le dernier chapitre de notre mémoire, nous aborderons l'implémentation de notre application, les outils utilisés, ses fonctionnalités, la gestion des mesures de sécurité, son dé- ploiement et des scénarios de test illustrant les résultats obtenus.

Enfin, notre mémoire se conclura par une synthèse générale qui résume les principales fonctionnalités et objectifs de notre solution, ainsi que des perspectives d'amélioration.

Chapitre

1

Chapitre 1 : Organisme d'accueil et concepts fondamentaux

1.1 Introduction

Au cours de la dernière décennie, les cyberattaques ont connu une évolution très cruciale, les cybercriminels sont devenus plus novateurs dans leurs attaques et les réponses en matière de cybersécurité ont dû évoluer en conséquence. Selon les statistiques sur la cybersécurité, 43 % des cyberattaques ciblent les petites entreprises, 64 % des entreprises ont subi des attaques sur le Web et 62% ont subi des attaques de phishing et d'ingénierie sociale [1].

Dans ce chapitre, nous allons dans un premier lieu présenter très brièvement le MNA Groupe, notre organisme d'accueil. Ensuite, nous allons explorer différentes notions liées à la sécurité de l'information, en examinant les aspects et les mesures qui lui sont associées. Nous nous intéresserons également à l'ingénierie sociale, en étudiant les types d'attaques généralement utilisées, puis nous nous concentrons sur le phishing plus spécifiquement, tout en abordant les mesures de prévention correspondantes.

1.2 MNA Groupe

MNA Groupe est une entreprise renommée dans le domaine de la sécurité de l'information. Dotée d'une équipe de professionnels hautement qualifiés et expérimentés, elle se distingue par sa spécialisation en audit, conseil et accompagnement en cybersécurité. Implantée dans plusieurs régions stratégiques, notamment en France (Paris et Marseille), en Afrique du Nord (Algérie) et en Afrique de l'Ouest (Sénégal), l'entreprise est en mesure de répondre aux besoins de sa clientèle dans ces différentes zones géographiques. MNA Groupe dispose également d'une structure dédiée et certifiée QUALIOPI, connue sous le nom de « MN Advising Cert », qui offre des programmes de formation de haut niveau. Grâce à leur expertise et à l'utilisation d'outils adaptés, les consultants de l'entreprise sont en mesure de former efficacement les collaborateurs des organisations clientes, en améliorant leurs compétences en matière de sécurité de l'information.

1.3 Services offerts par MNA Groupe

Plusieurs services sont offerts par MNA Groupe, chacun a ses propres fonctionnalités. Les services sont décrits dans ce qui suit :

1.3.1 Stratégie Cybersécurité :

Ce service assure les fonctionnalités suivantes :

— Fournir une expertise aux Directions Générales.

— Évaluer le niveau de maturité en matière de cybersécurité ou de confidentialité de l'entreprise.

— Élaborer des schémas directeurs et des feuilles de route pour la cybersécurité et la confidentialité.

— Encadrer et suivre des programmes de cybersécurité ou de confidentialité.

1.3.2 La supervision et la surveillance de la fonction Cyber :

Les fonctionnalités prises en charges par ce service sont les suivantes :

— Établissement et définition de la supervision et la surveillance de la fonction cyber.

— Définition et adaptation du cadre documentaire de référence.

— Mise en place d'un SMSI (Système de Management de la Sécurité de l'Information) conforme à la norme ISO(International Organization of Standardization) 27001.

— Amélioration de la supervision et du reporting en matière de cybersécurité (indicateurs clés de performance, tableau de bord).

1.3.3 Accompagnement de la fonction Cyber :

L'accompagnement de la fonction Cyber inclus les fonctionnalités suivantes :

— Élaboration de rôles et fonctions d'excellence en matière de cybersécurité.

— Implémentation de programmes de cybersécurité.

— Assistance dans le choix et le déploiement d'outils, de services et de solutions en matière de cybersécurité.

— Accompagnement pour la mise en place d'une assurance cyber.

— Sécurisation des projets.

— Sensibilisation à la cybersécurité.

1.4 La sécurité de l'information

Dans cette partie, nous aborderons le concept de sécurité de l'information, ses différents aspects, ainsi que les risques et les menaces avancés auxquels elles sont exposées.

1.4.1 Définition

La sécurité de l'information est l'ensemble des moyens, techniques, outils et ressources mis en œuvre pour minimiser la vulnérabilité d'un système ou, si cela est possible, de le protéger contre des menaces accidentelles ou intentionnelles [2].

La sécurité de l'information assure la protection de la confidentialité, l'intégrité et la disponibilité de l'information, qui sont aussi connues sous le nom de la triade CID [3] comme décrit dans la figure ci-dessous (voir la figure 1.1), la sécurité de l'information se définit principalement en trois axes mais un quatrième s'ajoute, il s'agit de la traçabilité.

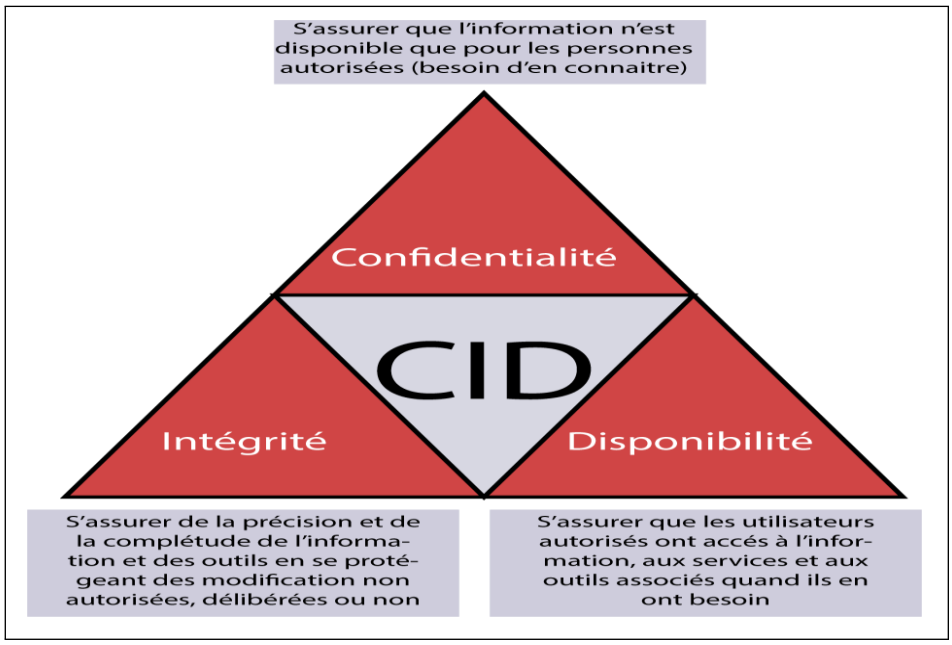

FIGURE 1.1 – Les critères de la sécurité de l'information

1.4.2 Les aspects de la sécurité

La sécurité des centres de données implique le maintien de l'information et de la stabilité du système dans son ensemble, ce qui nécessite une référence à deux niveaux de sécurité : l'un physique et l'autre logique.

1.4.2.1 Sécurité physique

La sécurité physique des ordinateurs consiste en l'application de barrières physiques et de procédures de contrôle en tant que mesures préventives contre les menaces qui pèsent sur les ressources et les informations confidentielles ; elle fait référence aux contrôles et aux mécanismes de sécurité autour des équipements de traitement des données et des dispositifs de stockage, tels que les contrôles d'accès aux bâtiments et bureaux, les caméras de sécurité, les capteurs et les systèmes biométriques

d'identité, entre autres mesures. La sécurité physique englobe également les moyens d'accès à distance mis en œuvre pour protéger le matériel [5].

1.4.2.2 Sécurité logique(Cybersécurité)

La sécurité logique complète la sécurité physique. Sa fonction est de protéger les systèmes, processus et programmes de protection des logiciels et des données, ainsi que l'accès ordonné et autorisé des utilisateurs aux informations. La sécurité logique comprend toutes les mesures établies par la direction pour minimiser les risques de sécurité associés aux opérations quotidiennes effectuées à l'aide des technologies de l'information, comme le vol d'information, la perte de données, l'entrée de virus, la modification non autorisée de données, les attaques de réseaux, etc. La sécurité logique vise à préserver la confidentialité, l'intégrité, l'authenticité et la disponibilité des données [5].

1.4.3 Les risque liés à la sécurité de l'information

Les risques liées à la sécurité de l'information sont la probabilité de pertes pour l'organisation est-elle élevée, moyenne, faible ou nulle ? Trois facteurs entrent en ligne de compte dans la détermination du risque : la nature de la menace, la vulnérabilité du système et l'importance de l'actif qui pourrait être endommagé ou rendu indisponible. Le risque peut donc être défini de la manière suivante : Risque = Menace x Vulnérabilité x Actif [6].

Une cyberattaque est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore des ordinateurs personnels, en s'appuyant sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques [7].

1.4.4 Les APT

Largement reconnu comme la classe de menaces de sécurité la plus sophistiquée et la plus puissante. APT(Advanced Persistantes Threats) fait référence à des attaquants humains bien informés qui sont organisés, hautement sophistiqués et motivés pour atteindre leurs objectifs contre une ou plusieurs organisations ciblées sur une période prolongée [8]. Parmi ces objectifs :

- Accéder à la défense, aux finances et à d'autres cibles des informations provenant de gouvernements, d'entreprises et personnes
- Maintenir un pied dans ces environnements pour permettre utilisation et contrôle futurs.
- Modifier les données pour perturber les performances de leurs cibles.

En général, une APT présente les caractéristiques suivantes :

- Acteurs : les attaques sont menées par des acteurs ayant une mission spécifique souvent soutenus par des États-nations.
- Objectifs : le but de l'attaque qui peut être stratégique ou politique.

- Délais : la durée de l'attaque sur un système infiltré.
- Ressources : cela comprend le temps et l'expertise en matière de sécurité et de développement.
- Méthodes : les techniques sophistiquées utilisées par les APT.
- Origine de l'attaque : les attaquants prennent souvent le temps de dresser une carte complète des faiblesses d'un système avant de choisir un (des) point(s) d'entrée(s).
- Valeur de l'attaque : la valeur de l'attaque peut faire référence à la taille de la cible ou à la taille des opérations d'attaque. Les grandes organisations ont tendance à être la cible des APT.

1.5 Les mesures de la sécurité de l'information

Voici les mesures de la sécurité de l'information :

1.5.1 Le cyber défense

Le cyber défense ou LID(Lutte Informatique Défensive), qui correspond aux aspects dynamiques et temps réel de la sécurité informatique pour pouvoir détecter les attaques et se défendre, est basée sur de nombreux outils et produits de sécurité comme les IDS(Intrusion Detection Systems), les outils de scan de vulnérabilités, les antivirus ainsi que les systèmes de gestion et corrélation d'événements sécurité SIEM (Security Information and Events Management)[12].

1.5.2 Le concept des équipes dans la cybersécurité

En cybersécurité, il existe trois grandes équipes opérationnelles, qui lorsqu'elles travaillent ensemble, créent trois autres équipes. Elles sont toutes gérées par une équipe principale.

1.5.2.1 Les équipes opérationnelles

Ces équipes peuvent être internes ou externes à une entreprise. Une grande compagnie aura généralement l'ensemble de ces équipes en interne alors que de plus petites entreprises pourraient n'en avoir qu'une ou deux seulement et faire appel à des firmes de consultants pour combler le manque [13].

- **Équipe Rouge - Red Team :** L'équipe rouge, ou équipe offensive, est une équipe composée d'employés ou de consultants externes à l'entreprise et dont le mandat est d'attaquer celle-ci à la manière d'un pirate, afin de détecter les vulnérabilités existantes qu'un acteur malveillant pourrait exploiter. Ses mandats sont variés et ont différentes portées, ils peuvent aller du simple test d'une application ou d'un site web à une simulation d'attaque complète, visant à tester les

équipes de sécurité physique et cyber ainsi que les mesures défensives en place [13].

- **Équipe bleue - Blue Team :** L'équipe bleue est l'équipe défensive. C'est elle qui est responsable, à l'aide d'outils, de protéger l'organisation des menaces externes, mais aussi internes. L'équipe bleue ne fait pas que surveiller le réseau. C'est une équipe pluridisciplinaire, elle est aussi constituée de chercheurs de menaces (Threat Hunter), d'employés en réponse aux incidents (Incident Response), en recherche d'information (Cyber Threat Intel) et aussi en enquêtes numériques (Digital Forensic). D'autres professions non citées ici font aussi partie de l'équipe défensive. [13]
- **Équipe jaune - Yellow Team :** C'est une équipe qui a toute sa place ici, bien que récemment arrivée dans le paysage de la cybersécurité. Dans cette équipe qu'on surnomme les bâtisseurs, on trouve entre autres les développeurs d'applications et de logiciels ainsi que des architectes système. Il est bien important d'inclure ces personnes dans les équipes de la cybersécurité, car ce sont elles qui créent les systèmes, logiciels et intégrations permettant à l'organisation d'être productive. Intégrer les principes de la cybersécurité dès le début du développement peut fortifier considérablement un logiciel et aider à la protection de l'organisation [13].

1.5.2.2 Les équipes mixtes

Nous savons déjà qu'il est important pour les équipes offensives et défensives de travailler ensemble afin de mettre de en lumière et corriger les faiblesses de l'organisation. Mais il est tout aussi important que ces deux équipes travaillent aussi avec celle des bâtisseurs afin que les solutions apportées par cette équipe soient développées et implémentées de façon sécuritaire [13].

- **Équipe mauve – Purple team :** L'équipe mauve, probablement la plus connue des équipes mixtes, est la collaboration des équipes rouge (offensive) et bleue (défensive). Le but de cette collaboration est de parfaire la posture de sécurité d'une organisation en améliorant les détections et les systèmes de défense. Un autre objectif est de bonifier les compétences des employés des deux équipes grâce au partage de connaissance [13].
- **Équipe verte – Green team :** Mélangez l'équipe bleue (défensive) et l'équipe jaune (bâtisseurs) et vous obtenez l'équipe verte. Une équipe dont le but est d'améliorer les défenses en place grâce à la standardisation et la priorisation des journaux et des événements de sécurité, l'obtention de meilleurs journaux et de données nécessaires aux équipes défensives. Grâce aux bâtisseurs de l'équipe jaune, l'équipe verte permettra aussi de bonifier la surveillance avec la mise en place d'antivirus nouvelle génération ou de systèmes de protection des terminaux [13].
- **Equipe orange – Orange team :** L'équipe orange, c'est l'association des attaquants (rouge) et des bâtisseurs (jaune). L'objectif de cette équipe est d'amener les bâtisseurs à être plus conscients de la cybersécurité, de ses enjeux et des défis qu'elle représente. En les sensibilisant à la façon dont les cybercriminels pensent et exploitent les réseaux ou logiciels, les bâtisseurs seront amenés à développer en ayant cette pensée en tête, ce qui finalement leur permettra de produire un code plus robuste [13].

1.5.2.3 L'équipe blanche – White team

Au-dessus de toutes ces équipes se trouve l'équipe blanche. Les membres de cette équipe proviennent de nombreux autres métiers comme la gouvernance, la conformité, la logistique et la gestion, par exemple. Le but de cette équipe n'est pas d'interagir avec une autre comme le font l'équipe rouge et l'équipe jaune, mais plutôt de gérer toutes ces équipes. L'équipe blanche va s'assurer que les politiques et procédures sont bien mises en place. Elle va aussi demander à ce que des tests de sécurité et de pénétration soient effectués sur des applications développées à l'interne ou afin de tester certains systèmes, et dans certains cas, même, de tester des équipes pour déterminer si leurs procédures sont bien suivies et suffisantes. Elle assure le suivi des ajustements apportés à la suite de ces tests et de l'application des politiques de sécurité [13]. On peut résumer les concepts des équipes dans la figure ci-dessous (voir la figure 1.2).

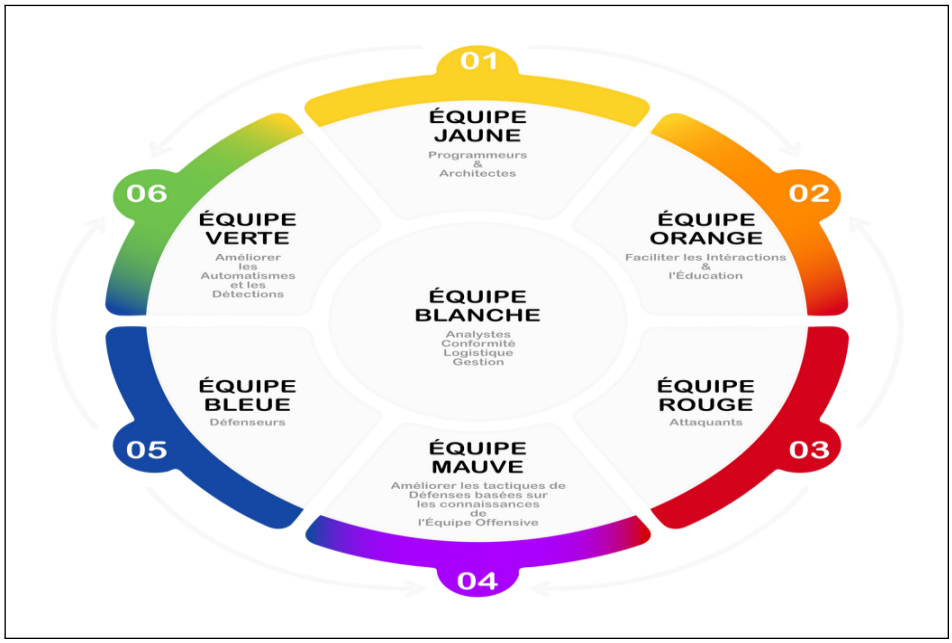

FIGURE 1.2 – Les concepts des équipes dans la cybersécurité

1.6 Ingénierie sociale

Dans cette section, nous allons discuter de l'ingénierie sociale et les différents types d'attaques, y compris les attaques de phishing. Nous examinerons les méthodes utilisées par les pirates informatiques pour mener ces attaques et les mesures de sécurité qui peuvent être mises en place pour prévenir leur succès.

1.6.1 Définition

L'ingénierie sociale regroupe des techniques utilisées par les cybercriminels pour inciter des utilisateurs peu méfiants à leur envoyer leurs données confidentielles, infectant ainsi leurs ordinateurs avec des programmes malveillants ou ouvrant des liens vers des sites infectés [18].

Elle peut prendre plusieurs formes, comme la manipulation, la persuasion, l'intimidation ou la séduction. En général, les attaquants d'ingénierie sociale ont un des deux objectifs suivants :

- Le sabotage : Perturber ou corrompre des données pour causer des dommages ou des désagréments.
- Le vol : Obtenir des objets de valeur comme des informations, des accès ou de l'argent.

La plupart des attaques d'ingénierie sociale reposent sur une communication réelle entre les attaquants et les victimes. L'attaquant a tendance à inciter l'utilisateur à se compromettre, plutôt que d'utiliser des méthodes de force brute pour accéder aux données des victimes.
Le cycle d'attaque donne à ces criminels un processus fiable pour tromper les victimes. Les étapes du cycle d'attaque de l'ingénierie sociale sont généralement les suivantes :

- Se préparer en recueillant des informations générales sur la victime ou sur un groupe plus large dont elle fait partie.
- S'infiltrer en établissant une relation ou en initiant une interaction, en commençant par établir la confiance.
- Exploiter la victime une fois que la confiance et une faiblesse sont établies pour faire progresser l'attaque.
- Se désengager une fois que l'utilisateur a effectué l'action souhaitée.

Ce processus peut se dérouler dans un seul courriel ou sur plusieurs mois dans une série de conversations sur les médias sociaux. Il peut même s'agir d'une interaction en face à face. Mais il se conclut finalement par une action que la victime entreprend, comme partager ces informations ou elle expose à un logiciel malveillant.

1.6.2 Types d'attaques d'ingénierie sociale

Presque tous les types d'attaques de cybersécurité contiennent une forme d'ingénierie sociale. Par exemple, les arnaques classiques par courrier électronique et par virus sont chargées de connotations sociales.

L'ingénierie sociale peut être faite numériquement par des attaques mobiles en plus des appareils de bureau. Cependant, elles peuvent tout même aussi bien être confrontées à une menace en personne. Ces attaques peuvent se chevaucher et se superposer pour créer un scam. Voici quelques méthodes courantes utilisées par les attaquants en ingénierie sociale :

1.6.2.1 Le phishing (l'hameçonnage)

a) Définition : Une attaque de phishing est une cyberattaque dans laquelle un attaquant crée un e-mail frauduleux mais d'apparence authentique pour tromper les destinataires afin qu'ils exécutent des instructions nuisibles. Il peut s'agir de cliquer sur un lien, d'ouvrir une pièce jointe, de fournir des informations sensibles ou de transférer de l'argent [21].

b) L'origine : L'expression « phishing » est initialement apparue dans le milieu informatique des années 1990, chez les hackers qui avaient pour objectif de tromper les utilisateurs d'AOL (America Online) en leur faisant totalement laisser tomber et abandonner leurs données de connexion.

Pour l'anecdote, le « ph » est associé à une tradition de piratage fantaisiste, et a probablement été influencé par le terme « phreaking », abréviation de « phreaking téléphonique », une forme de piratage qui consistait à jouer des sons dans les combinés téléphoniques pour obtenir des appels gratuits. Pour les particuliers, cela inclut les achats non autorisés, le vol de fonds ou le vol d'identité.

En outre, le phishing est une pratique particulièrement utilisée afin de s'incruster au sein de réseaux d'entreprises ou de gouvernements. Dans la situation d'une entreprise, les employés sont utilisés et notamment compromis dans l'objectif final de passer outre les différents périmètres de sécurité mise en place, de faire une distribution massive de logiciels malveillants au sein d'un système, un réseau ou un environnement fermé, ou bien d'obtenir un accès privilégié à des données sécurisées [22].

c) Le fonctionnent des attaques de phishing Le cœur d'une attaque de phishing est de faire croire le message de phishing au destinataire du courriel. Pour ce faire, les attaquants doivent créer du contenu de courriel qui est pertinent ou intéressant pour le destinataire. De plus, elle doit être conforme au ton, au langage et au style de l'organisation ou de la personne qu'elle prétend être. Un attaquant consciencieux passe beaucoup de temps à la recherche. Pour certaines organisations, les attaquants ont tendance à faire des recherches approfondies. Ils recherchent ensuite les adresses courriel des employés sur le site Web de l'entreprise ou les médias sociaux pour envoyer des courriels de phishing. Une fois que la victime est piégée, l'attaquant peut passer à l'étape suivante de l'atteinte de ses objectifs [23].

d) Les objectifs Voici les trois objectifs de phishing :

- **Objectif 1 : Vol d'information**
  Certains courriels d'hameçonnage sont conçus pour voler des renseignements personnels. Ces courriels prétendent provenir de sources fiables comme des entreprises bien connues et des ministères. Ils créent une excuse pour obliger le destinataire à fournir leurs données personnelles. Les fraudeurs peuvent vendre ces informations ou les utiliser pour leur propre profit. Cela comprend la demande de carte de crédit au nom de la victime, la demande de remboursement d'impôt et les demandes de règlement d'assurance [24].

- **Objectif 2 : Fraude financière**

  Certains courriels d'hameçonnage demandent aux destinataires de transférer des fonds vers un compte. Ces courriels prétendent souvent provenir d'un expéditeur de confiance, comme un patron ou une organisation bien connue. Ils présentent une situation qui nécessite une attention immédiate pour créer un sentiment d'urgence. Les victimes peuvent être trop impatientes de vérifier la crédibilité du courriel et finir par effectuer le transfert. Dans un nouveau message d'intérêt public, l'IC3 (Internet Crime Complaint Center) du FBI (Federal Bureau of Investigation) a signalé que les fraudes par courriel commercial (EAC) ont coûté aux entreprises du monde entier 43 milliards de dollars entre juin 2016 et décembre 2021[24].

- **Objectif 3 : Intrusion dans le réseau**

  Une attaque de phishing peut être utilisée pour violer les réseaux d'entreprise afin d'atteindre des objectifs plus importants, comme l'infection par ransomware et le vol de données. En fait, les attaques de phishing sont l'un des moyens les plus courants par lesquels les auteurs de menaces obtiennent un accès initial aux réseaux d'entreprise. Selon le rapport Cisco 2021 Cybersecurity Threat Trends, 90 % des atteintes à la sécurité des données sont liées à le phishing. Les attaques de phishing permettent d'infiltrer le réseau de deux façons principales [23].

  Phishing links : La plupart des courriels de phishing contiennent un lien qui mène le destinataire à une page Web contrôlée par l'attaquant. Cette page Web peut télécharger directement des logiciels malveillants sur la machine de la victime. La page Web peut être un faux portail d'ouverture de session pour un service commercial couramment utilisé.

  Phishing attachements : Certains courriels d'hameçonnage sont joints à des fichiers malveillants. Ces fichiers peuvent être déguisés à l'aide de noms de fichiers non épicés. Il peut également s'agir de types de fichiers légitimes comme les fichiers Word et Excel qui ont été falsifiés.

e) Les types de Phishing Bulk Phishing : est l'attaque classique de phishing employant un large filet pour piéger autant de victimes que possible - pensez au chalutage de fond dans le cyberespace. Le Bulk phisher en vrac peut avoir un faible taux de succès global, mais repose sur le fait que sur des milliers ou même des millions de victimes potentielles, quelques-uns seront toujours mordre à l'hameçon. Les bulk phishing campaigns en vrac sont souvent peu complexes et peuvent être menées à l'aide d'une « trousse d'hameçonnage » facilement accessible [23].

Le Spear Phishing et Le Whaling : comme les attaques générales de Phishing, le harponnage et la chasse à la baleine utilisent des courriels provenant de sources qui semblent dignes de confiance pour tromper leurs victimes. Plutôt que de ratisser large, le harponnage cible des individus ou des personnages particuliers. Les administrateurs de la TI (Technologie de l'Information) et les professionnels des RH(Ressources humaine) sont des cibles fréquentes en raison du niveau d'accès qu'ils peuvent avoir au sein de l'organisation. Comme le Spear Phishing, le whaling créer des campagnes autour d'une cible spécifique, mais avec un plus grospoisson à l'esprit [23].

Clone Phishing Attack : Les Clone Phishing attacks sont moins créatives que la pêche au spear et à phishing, mais tout de même très efficaces. Ce style d'attaque à tous les locataires de base d'une arnaque de phishing. Cependant, la différence ici est que plutôt que de se faire passer pour un utili-

sateur ou une organisation avec une demande spécifique, les attaquants copient un courriel légitime qui a déjà été envoyé par une organisation de confiance. Les pirates utilisent alors la manipulation de lien pour remplacer le lien réel inclus dans le courriel original pour rediriger la victime vers un site frauduleux afin de tromper les utilisateurs en entrant les identifiants qu'ils utiliseraient sur le site réel [23].

Le Smishing et Le Vishing : la plupart des attaques de phishing ont toujours lieu par courriel, mais un certain nombre d'attaques dérivées utilisant d'autres médiums ont également été observées. Le smishing fait référence aux attaques de phishing envoyées par message texte (SMS). Le phishing vocal ou le « vishing » remplace le faux texte par une arnaque audio, en direct ou enregistrée. La prise de contrôle de dizaines de comptes Twitter très médiatisés en juillet 2020 a été possible grâce à une campagne de consultation sophistiquée ciblant les employés de Twitter [23].

f) Les attaques les plus connues de Phishing Le Phishing a été à l'origine de certains des incidents de cybersécurité les plus notables de l'histoire. La fuite de courriels de 2016 de la campagne présidentielle d'Hilary Clinton a commencé par une attaque de phishing contre le président de campagne « John Podesta ». L'incident de prise de contrôle de compte de Twitter en 2020 a commencé par plusieurs attaques vishing sur les employés. Et selon certaines mesures, le phishing est la première action dans un quart de toutes les campagnes de ransomware [23].

1.6.2.2 Scareware

Scareware est une tactique malveillante utilisée pour inciter les victimes à télécharger ou à acheter des logiciels et des mises à jour infectés par des logiciels malveillants. Le plus souvent, les attaques de scareware font croire aux utilisateurs qu'ils doivent acheter ou installer un logiciel déguisé en solution de cybersécurité.

Le but des scarewares est de menacer les utilisateurs d'ordinateurs d'acheter de faux logiciels ou d'infecter davantage leur appareil. Les scarewares montrent aux utilisateurs des alertes de sécurité contextuelles qui semblent être des avertissements de véritables sociétés antivirus, affirmant généralement que les fichiers sont infectés ou que l'appareil est en danger [25].

1.6.2.3 Watering hole

Une attaque par trou d'eau consiste à lancer ou à télécharger un code malveillant à partir d'un site Web légitime, qui est couramment visité par les cibles de l'attaque. Par exemple, des attaquants pourraient compromettre un site d'information sur le secteur financier, sachant que des personnes qui travaillent dans la finance et représentent donc une cible attrayante, sont susceptibles de visiter ce site. Le site compromis installe généralement un cheval de Troie de porte dérobée qui permet à l'attaquant de compromettre et de contrôler à distance l'appareil de la victime. L'attaquant recherche des vulnérabilités existantes qui ne sont pas connues et qui n'ont pas été corrigées - ces faiblesses sont considérées comme des exploits de type "zero-day" [25].

1.6.2.4 Pretexting (usurpation d'identité)

Est défini comme l'acte de créer un scénario inventé pour persuader une victime ciblée de divulguer des informations ou d'effectuer une action. C'est plus que créer un mensonge ; dans certains cas, il peut s'agir de créer une toute nouvelle identité, puis d'utiliser cette identité pour manipuler la réception d'informations. Les ingénieurs sociaux peuvent utiliser des prétextes pour se faire passer pour des personnes dans certains emplois et rôles qu'ils n'ont jamais eux-mêmes occupés. Le faux-semblant n'est pas une solution unique. Un ingénieur social doit développer de nombreux prétextes différents au cours de sa carrière. Tous auront un point commun : la recherche. De bonnes techniques de collecte d'informations peuvent faire ou défaire un bon prétexte. Par exemple, imiter le parfait représentant du support technique est inutile si votre cible n'utilise pas de support extérieur. Le faux-semblant est également utilisé dans des domaines de la vie autres que l'ingénierie sociale [28].

1.6.2.5 Le Baiting

Est similaire à une attaque de phishing, mais attire une victime par des stratégies de séduction. Les pirates utilisent le baiting des biens promis si un utilisateur se rend identifiants de connexion à un site spécifique. Les systèmes de baiting ne se limitent pas aux systèmes numériques en ligne et peuvent également être lancés par l'utilisation de supports physiques [29].

1.6.2.6 Le Whaling

Est une autre variante courante du phishing qui cible spécifiquement les cadres supérieurs des entreprises et les chefs des agences gouvernementales. Les attaques de whaling usurpent généralement les adresses e-mail d'autres personnes de haut rang dans l'entreprise ou l'agence et contiennent des messages urgents sur une fausse urgence ou une opportunité urgente. Les attaques de whaling réussies peuvent exposer de nombreuses informations confidentielles et sensibles en raison de l'accès réseau de haut niveau dont disposent ces cadres et directeurs [30].

1.7 Conclusion

Dans ce chapitre, nous avons abordé divers concepts liés à notre projet, tels que la sécurité de l'information, l'ingénierie sociale et l'attaque de phishing, qui joue un rôle crucial dans notre projet. Nous nous intéressons dans le chapitre qui suit à la littérature dédiée à la sensibilisation, qui y sera le sujet principal.

Chapitre

2

Chapitre 2 : Etat de l'art sur la sensibilisation à la cybersécurité

2.1 Introduction

Dans le monde réel, la sensibilisation à la cybersécurité revêt une importance cruciale, elle est devenue une préoccupation majeure dans notre société de plus en plus connectée et dépendante de la technologie. Avec la prolifération des cyberattaques et des violations de données, il est essentiel de former et d'informer les individus sur les risques et les bonnes pratiques en matière de sécurité en ligne. Au cours de ce chapitre, nous aborderons la notion de sensibilisation à la cybersécurité, et soulignerons importance. Nous explorerons les différentes étapes nécessaires pour mettre en place un programme de sensibilisation efficace. De plus, nous examinerons les objectifs visés par la sensibilisation à la cybersécurité et présenterons les différentes plateformes pouvant être utilisées dans ce contexte.

2.2 La sensibilisation à la cybersécurité

La sensibilisation à la cybersécurité est un processus continu d'éducation et de formation des utilisateurs aux menaces qui se cachent dans le cyberespace ; à la manière de les prévenir et à ce qu'ils doivent faire en cas d'incident de sécurité informatique. Elle contribue également à leur inculquer un sens de la responsabilité proactive pour assurer la sécurité de l'entreprise et de ses actifs [15].

2.3 Les étapes pour mettre en place un programme de sensibili-sation à la cybersécurité

Pour mettre en place un programme de sensibilisation efficace, des étapes à suivre ont été proposées par [14], elles sont décrites dans ce qui suit :

2.3.1 Identifier les risques

Cette première étape consiste à avoir une vision actualisée des principales menaces auxquelles l'organisation est exposée en termes de cybersécurité. La connaissance des risques et de leurs implications permet d'élaborer correctement votre campagne de sensibilisation ainsi que de cibler la formation adéquate qui doit être dispensée à toutes les personnes concernées.

2.3.2 Modifier les comportements

La pandémie de Covid 19 a imposé beaucoup de changement aux organisations notamment le télétravail et ses nombreux risques. En effet, le travailleur à distance reste une cible des cybercriminels.

Les connaissances et les comportements antérieurs ne sont peut-être plus solides pour couvrir toutes les vulnérabilités. Le moyen efficace pour transformer les comportements et rester en phase avec les nouveaux défis est de veiller à ce que la sensibilisation à la cybersécurité soit dispensée de manière personnalisée, ciblée ainsi que succincte.
Pour y arriver, les organisations doivent se servir d'une variété d'outils et de techniques comme :

- Des vidéos captivantes
- Des scénarios réalistes
- Des quiz
- Des politiques
- Des tests de simulation de phishing dans le monde réel
- Des affiches de sensibilisation
- Des études de cas réels pour renforcer les messages clés.

2.3.3 Planifier des formations durant toute l'année

Les organisations doivent planifier l'organisation des formations de sensibilisation à intervalles réguliers sur toute l'année à mesure que le paysage des risques évolue et que de nouvelles technologies sont mises en ligne.
Les cybercriminels lancent également des attaques généralement au cours des événements mondiaux ou saisonniers. C'est le cas avec COVID-19 où le nombre de cyber attaques par phishing sur le thème est astronomique.
Les employés ne seront pas capables d'identifier les attaques ou de réagir de manière appropriée lorsqu'elles ne reçoivent pas une formation de sensibilisation tout au long de l'année.

2.3.4 Tester l'efficacité de la formation de sensibilisation

Il s'agit de procéder à des simulations de phishing et de divers tests de sécurité afin de déterminer la réaction des employés. Ces tests aident les employés à identifier, éviter et signaler les menaces qui pourraient mettre en péril la sécurité de l'organisation.

2.3.5 Suivre des mesures

Les organisations doivent établir des mesures de réussite afin de déterminer si la campagne de sensibilisation est efficace. Il s'agit des indicateurs de succès qui permettront d'identifier les domaines dans lesquels les employés ont des difficultés et qui nécessitent des formations avancées.

2.4 Objectif de la sensibilisation

La sensibilisation de la cybersécurité a comme but de :

2.4.1 Amélioration du SMSI

Le premier avantage de la sensibilisation provient des améliorations qui peuvent résulter de l'assimilation de la politique de sécurité par le personnel et la prise de conscience sur leurs responsabilités.

2.4.2 Amélioration de la réputation grâce à la fiabilité

La confiance est cruciale à la réputation et aux marques d'une organisation. Lorsque la plupart des employés sont sensibilisés à la sécurité de l'information, les visiteurs estiment que l'organisation prend clairement au sérieux la sécurité et la confidentialité.

2.4.3 Responsabilité des personnels

La sensibilisation des employés à leurs responsabilités est essentielle pour qu'ils mettent en pratique les meilleures approches et se conforment aux exigences en termes de sécurité. Par ailleurs, investir dans une technologie coûteuse ne servira pas à grand-chose lorsque le personnel ne connaît pas ou ne comprend pas ses responsabilités.

2.4.4 Mise à jour de la connaissance

La sensibilisation rafraîchit la connaissance des employés et des parties impliquées dans le SMSI. Les organisations peuvent donc adopter un programme de sensibilisation continu.

2.4.5 Démontrer la conformité

La sensibilisation du personnel entre dans le cadre de la conformité à la norme ISO 27001 d'autant que le personnel reçoive une formation de sensibilisation appropriée et que tout le monde ait le même niveau ainsi que la même qualité de formation.

2.4.6 Réduction de la résistance à la cybersécurité

La sensibilisation signifie que le personnel comprend le bien-fondé de la sécurité de l'information. Lorsqu'elle est satisfaisante, le personnel utilise efficacement les contrôles de sécurité. À titre

d'exemple, comprendre la nécessité d'avoir un mot de passe et comment choisir un bon mot de passe facilite la sécurité.

2.4.7 Réduction des incidents de sécurité de l'information

Les employés des organisations qui savent à quoi s'en tenir sont moins susceptibles d'exposer les actifs informationnels à l'insécurité ou d'ignorer les premiers signes de problèmes. Les personnes sensibilisées et guidées par des professionnels de la sécurité hautement qualifiés font preuve de compétence et de prudence lorsque cela est nécessaire.

2.5 Outils similaires

Dans le monde réel il existe plusieurs plateformes qui font la sensibilisation des fonctionnaires dans les entreprises contre les cybermenaces, parmi ces plateformes nous trouvons :

2.5.1 TERRANOVA SECURITY

Terranova Security fournit des produits et services innovants pour la formation de sensibilisation à la sécurité mondiale (voir la figure 2.1) [44], les simulations d'hameçonnage et la conformité au RGPD (Règlement Générale sur la Protection des Données). Leur plateforme de sensibilisation à la sécurité permet aux organisations de gérer et de diffuser du contenu de formation, d'évaluer la rétention des connaissances, de suivre la participation et les progrès.

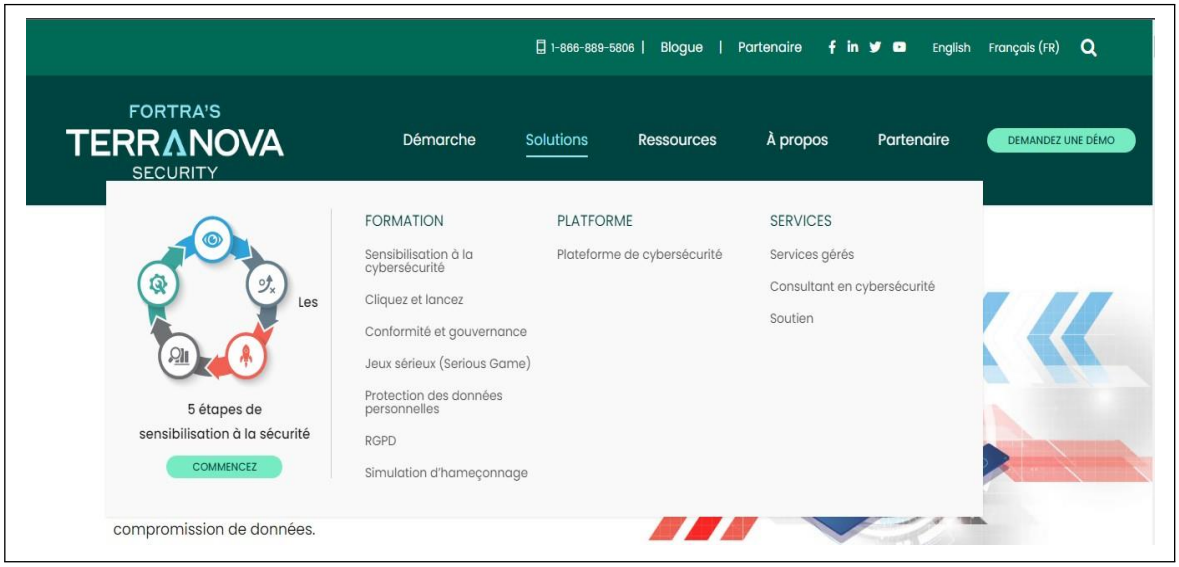

FIGURE 2.1 – L'interface web de la plateforme de sensibilisation du Terranova

2.5.2 Kaspersky ASAP

Kaspersky offre des programmes de formation à la sensibilisation à la sécurité pour aider à empêcher les employés de causer des cybers incidents par erreur. Kaspersky ASAP (Automated Security Awareness Platform) est une plateforme d'apprentissage en ligne qui sensibilise les employés à la cybersécurité et leur enseigne les bonnes pratiques de cybersécurité. Kaspersky propose également des formations et des cours de sensibilisation à la cybersécurité industrielle pour les utilisateurs de tous les jours, les experts en sécurité IT/OT,les opérateurs ICS (Industrial Control System) et plus encore, voici l'interface web de la plateforme de Kaspersky, illustrée dans la figure ci-dessous (voir la figure 2.2) [45].

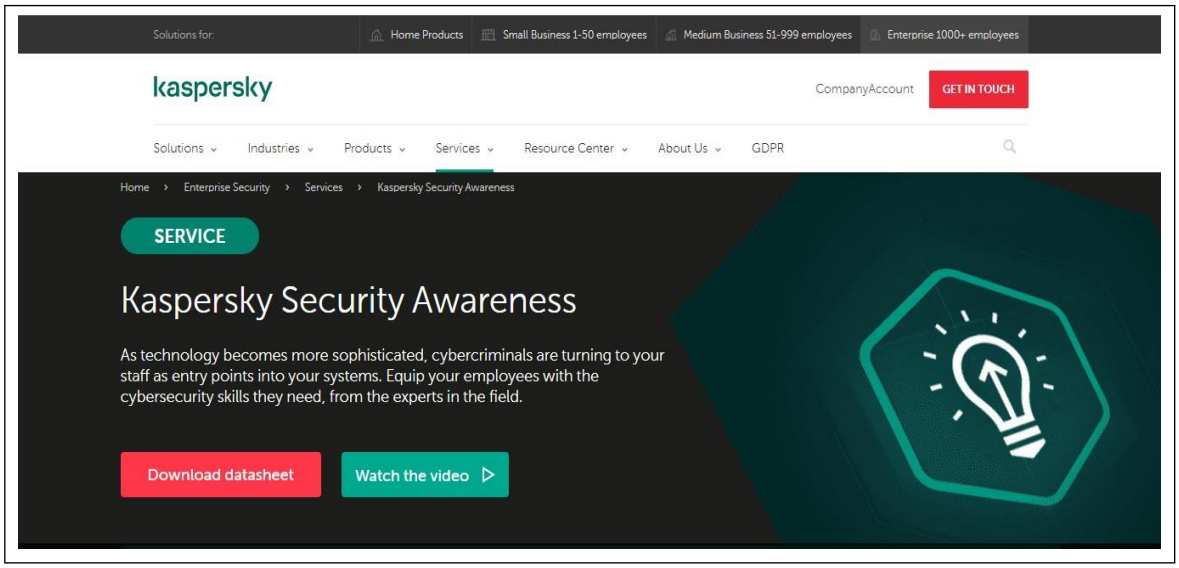

FIGURE 2.2 – L'interface web de la plateforme de sensibilisation du Kaspersky

2.6 Comparaison entre Terranova et Kaspersky

Terranova et Kaspersky sont deux plates-formes qui offrent des services de sécurité informatique, mais se distinguent par leurs caractéristiques et leurs domaines d'expertise. Voici une comparaison entre les deux :

2.6.1 Domaine d'expertise

Terranova : Terranova est une plateforme de cybersécurité spécialisée dans la détection et la prévention des APTs. Elle se concentre principalement sur la sur- veillance en temps réel des activités malveillantes et sur la prévention des cyberat- taques sophistiquées.

Kaspersky : Kaspersky est une société de sécurité informatique bien établie qui propose une gamme complète de produits et de services de cybersécurité, allant de la protection antivirus de base à la sécurité des réseaux d'entreprise. Kaspersky couvre un large éventail de menaces, y compris les logiciels malveillants, les ransomwares, les attaques de phishing, etc.

2.6.2 Fonctionnalités et solutions

Terranova : La plateforme Terranova offre des fonctionnalités avancées de détec- tion des menaces, d'analyse comportementale, de gestion des vulnérabilités et de réponse aux incidents. Elle se concentre principalement sur la détection proactive des attaques sophistiquées et sur l'analyse approfondie des comportements suspects.

Kaspersky : Kaspersky propose une gamme de solutions de sécurité informatique pour les particuliers, les petites et moyennes entreprises, ainsi que pour les grandes entreprises. Leurs produits comprennent des solutions antivirus, des pare-feu, des outils de protection de la vie privée, des systèmes de détection des intrusions, etc. Ils offrent également des services de sécurité gérés pour les entreprises.

2.6.3 Portée et présence

Terranova : Terranova est une plateforme relativement nouvelle sur le marché de la cybersécurité. Sa présence peut varier en fonction des régions et des secteurs d'activité spécifiques. Elle se concentre principalement sur les entreprises et les organisations qui nécessitent une protection avancée contre les menaces ciblées.

Kaspersky : Kaspersky est une entreprise mondiale de sécurité informatique pré- sente dans de nombreux pays. Elle bénéficie d'une présence étendue et propose ses produits et services à un large éventail de clients, allant des particuliers aux grandes entreprises.

2.6.4 Réputation et historique

Terranova : Étant donné que Terranova est relativement nouveau, sa réputation et son historique peuvent être moins établis par rapport à des sociétés plus anciennes et bien connues dans le domaine de la cybersécurité.

Kaspersky : Kaspersky jouit d'une réputation solide et a une longue histoire dans l'industrie de la sécurité informatique. Ils sont bien connus pour leurs technologies de détection des menaces et leurs recherches approfondies sur les cyberattaques.

2.7 Discussion

Les deux plateformes de sensibilisation permettent une détection de menaces et de vulnérabilités. Le MNA Groupe n'a pas opté pour ces solutions car il voulait opter pour une solution qui répond à ses besoins spécifiques, comme la personnalisation du contenu pour répondre à ses besoins, la flexibilité et l'adaptation à la culture et aux valeurs de MNA Groupe, une interface conviviale facilement manipulable par ses utilisateurs, des simulations de cyberattaques, et un soutien continu en termes de ressources de formation et d'assistance technique pour accompagner MNA Groupe.

2.8 Conclusion

L'étude réalisée dans ce chapitre nous a permis de bien identifier le contexte de la sensibilisation à la cybersécurité, ses objectifs, ainsi que les outils similaires et les étapes nécessaires pour mettre en place un programme de sensibilisation. Maintenant que nous avons délimité le périmètre de notre travail, nous allons nous concentrer sur la partie conception, qui sera le sujet du prochain chapitre.

Chapitre

3

Chapitre 3 : Conception

3.1 Introduction

Après avoir terminé l'étude bibliographique, nous entamons la construction de notre système. Une des étapes clé de la réussite d'un nouveau projet logicielle est la conception. Pour la réussite de cette dernière, il est crucial d'identifier et d'exprimer les besoins de l'entreprise.

Dans ce chapitre, nous commencerons par définir une cartographie du système à développer pour donner un aperçu sur l'idée véhiculée par notre système. Puis, nous présenterons le cycle de vie suivi qui implique les différentes activités d'ingénierie que nous avons menées et leur ordonnancement. Ensuite nous définissons les objectifs du nouveau système et les fonctionnalités qui doivent être prises en considération tout au long du projet, en tenant compte des différents acteurs impliqués dans le système. Nous terminerons ce chapitre par la conception de notre système.

3.2 Cycle de vie et langage de modélisation

Pour développer notre projet, nous avons utilisés le cycle de vie en cascade. Le cycle de vie (voir Figure 3.2) en cascade est un modèle de développement de logiciels qui suit une approche linéaire et séquentielle, avec des phases distinctes, où chaque phase dépend de la réussite de la phase précédente.

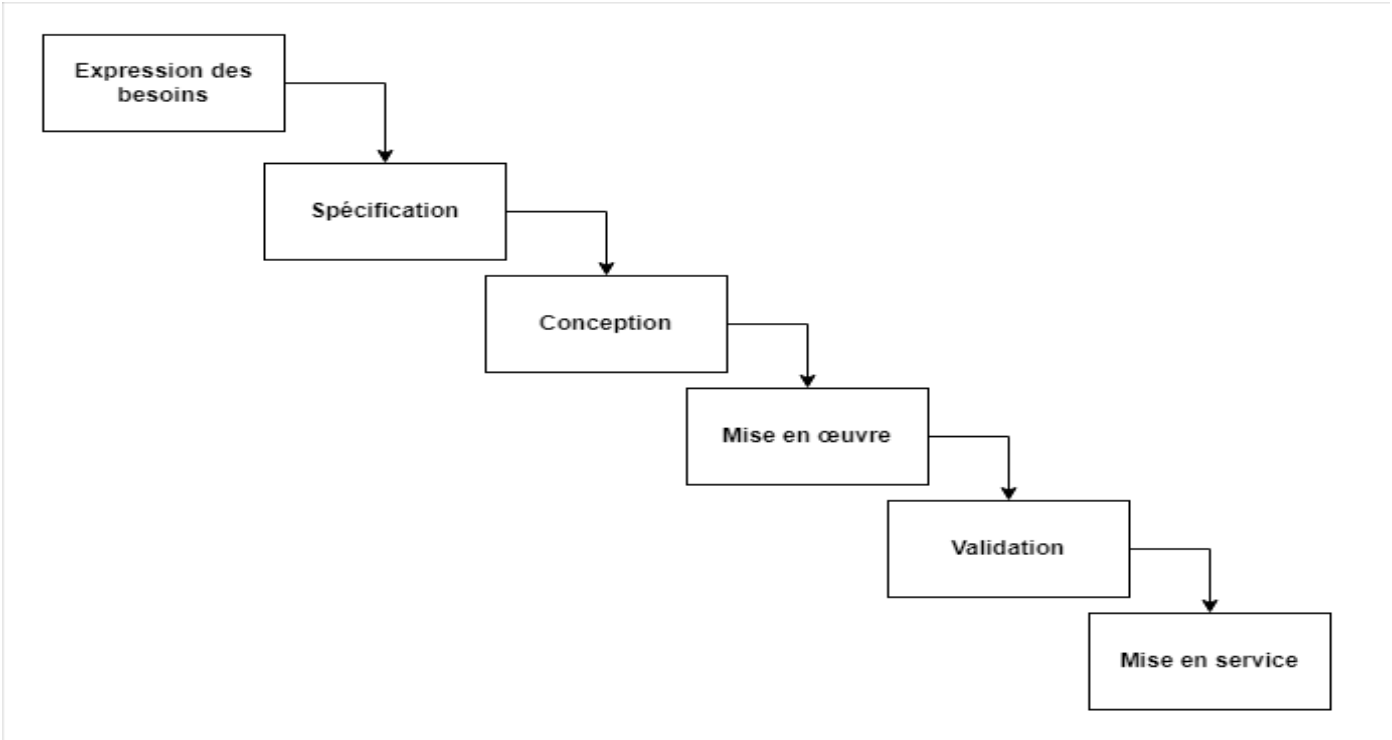

FIGURE 3.1 – Cycle de vie

Quant au langage de modélisation, nous avons utilisé le langage de modélisation unifié (UML) comme support de modélisation [46].

3.2.1 Expression et spécification des besoins

La spécification des besoins est une étape clé dans le processus de développement du projet. Elle vise à comprendre les attentes et les exigences des parties prenantes afin de définir les objectifs du projet et de créer une feuille de route pour son développement. Cela permet d'assurer que les résultats finaux répondent aux besoins réels des utilisateurs et apportent une valeur ajoutée significative.

3.2.1.1 Expression des objectifs du système

En utilisant des réunions, des documents et des entretiens périodiques avec les acteurs de l'entreprise, nous avons réussi à sélectionner les objectifs à atteindre et à satisfaire grâce à la mise en œuvre du nouveau système. Ces objectifs peuvent être regroupés de la manière suivante :

- Faciliter la sensibilisation des employés de l'entreprise à la sécurité de l'information.
- Assurer le suivi des performances des employés en termes de formation.
- Surveiller les résultats des employés en matière de détection et de prévention des attaques de phishing.
- Permettre l'utilisation du système par plusieurs entreprises.
- Automatiser la réalisation des tests des attaques de phishing sur les employées d'entreprise.

3.2.1.2 Identification des acteurs

Un acteur dans un système d'information représente l'abstraction d'un rôle joué par des entités externes telles qu'un utilisateur humain, un dispositif matériel ou un autre système, qui interagissent directement avec le système étudié. Bien que les utilisateurs humains soient les principaux acteurs, un acteur peut également être un autre système d'information ou un logiciel qui interagit avec le système d'information concerné. Les acteurs ont la capacité de consulter et/ou de modifier directement l'état du système en émettant et/ou en recevant des messages, pouvant contenir des données.

Il est possible qu'une personne physique soit représentée par plusieurs acteurs dans le système si elle joue plusieurs rôles distincts. De même, plusieurs personnes physiques peuvent avoir le même rôle dans le système, et elles seront représentées par un seul acteur.

Pour notre système, les acteurs sont les suivants :

- Administrateur
- Auditeur système
- Entreprise
- Auditeur entreprise
- Employé

Acteur	Description	Principales tâches
Administrateur	Ce rôle est celui de la gestion des entreprises, des cours, des auditeurs et de l'affectation des cours aux entreprises.	- Ajouter, supprimer, modifier une entreprise - Ajouter, supprimer, modifier un auditeur - Ajouter, supprimer, modifier un cours - Ajouter, supprimer une affectation
Auditeur système	Ce rôle est chargé de surveiller l'ensemble des activités qui se déroulent dans l'application.	Superviser toutes les activités qui se déroulent au sein de l'application.
Entreprise	Ce rôle est celui de la gestion des employés, de l'affectation des cours aux employés, ainsi que de lancement des attaques de phishing.	- Ajouter, supprimer, modifier une employée - Visualiser les statistiques des attaques de phishing - Visualiser les statistiques des formations des employées
Auditeur entreprise	Ce rôle est chargé de surveiller l'ensemble des activités qui se déroulent dans l'application par l'entreprise.	Superviser de toutes les activités qui se déroulent au sein de l'application par l'entreprise.
Employé	Tout employé de l'entreprise	- Suivre des formations - Passer les tests finaux et Quiz - Consulter l'ensemble de ses formations - Consulter son notes

TABLE 3.1 – Acteur du système

3.2.1.3 Identification des cas d'utilisations

Les diagrammes des cas d'utilisations sont des représentations UML qui permettent de visualiser les diverses fonctionnalités qu'un système doit fournir pour différents utilisateurs. Ils offrent une meilleure compréhension des fonctionnalités du système ainsi que des rôles des différents acteurs.

Voici le diagramme de cas d'utilisation globale (voir Figure 3.3) :

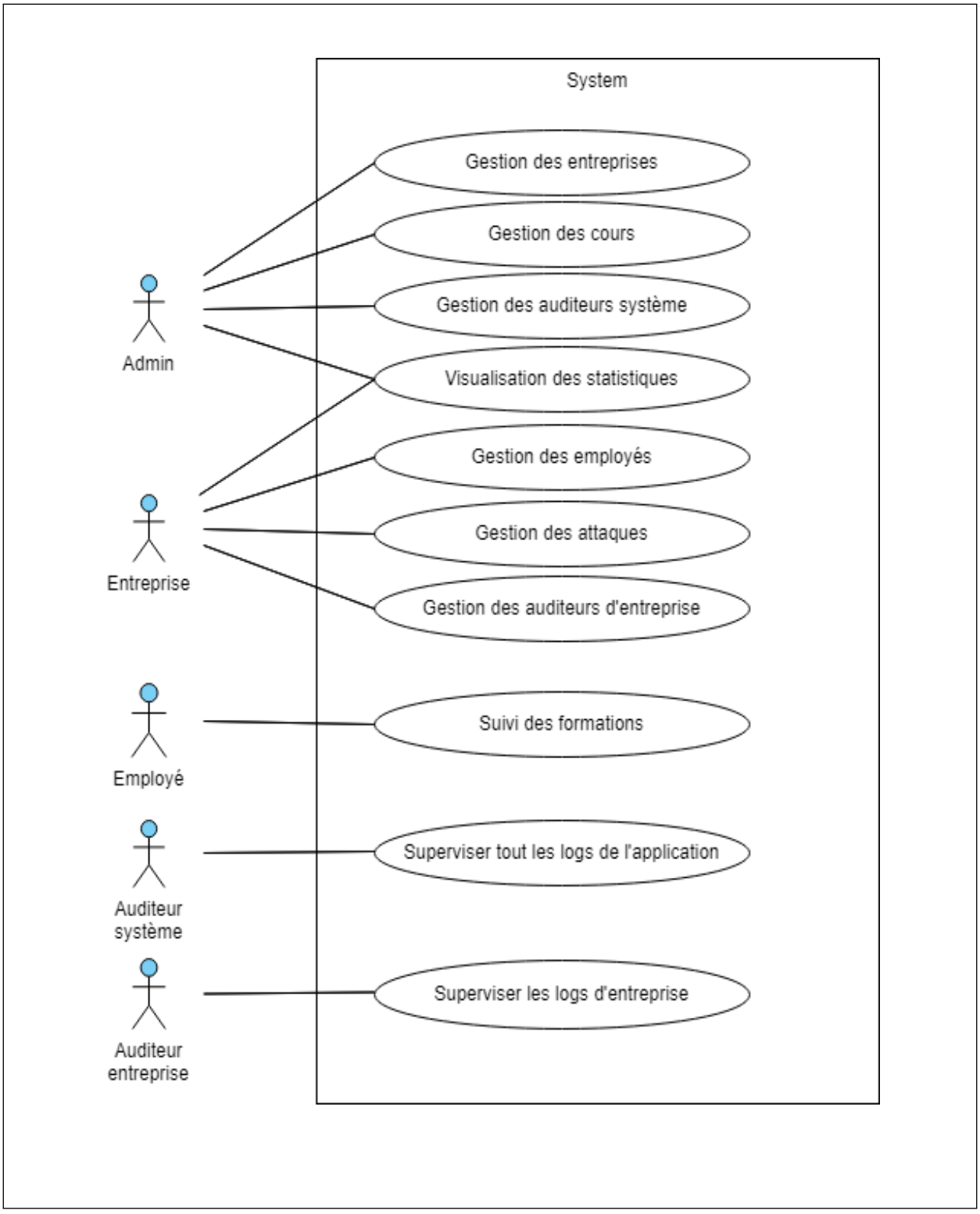

FIGURE 3.2 – Diagramme de cas d'utilisation globale

3.2.1.4 Scénarios et diagrammes de séquence

Afin de clarifier les besoins des utilisateurs et pour aider les concepteurs à comprendre comment le système doit fonctionner, nous avons utilisé les scénarios et le diagramme de séquence d'UML.

Dans ce qui suit, nous présentons les scénarios et les diagrammes de séquence des cas d'utilisation les plus importants de l'application.

a) Authentification : L'acteur est : utilisateur.

Etape principales :

Les étapes principales de l'authentification sont les suivantes :

1. L'utilisateur ouvre l'application.
2. L'application affiche l'interface de connexion.
3. L'utilisateur remplit son email et mot de passe et envoyer les informations.

Conditions : Si l'utilisateur entre des informations d'email et de mot de passe valides, il pourra accéder à la plateforme. Dans le cas contraire, il sera redirigé vers la page de connexion et n'aura pas accès.

Le diagramme de séquences de la figure ci-dessous (voir Figure 3.4) illustre les étapes de scénario précédent.

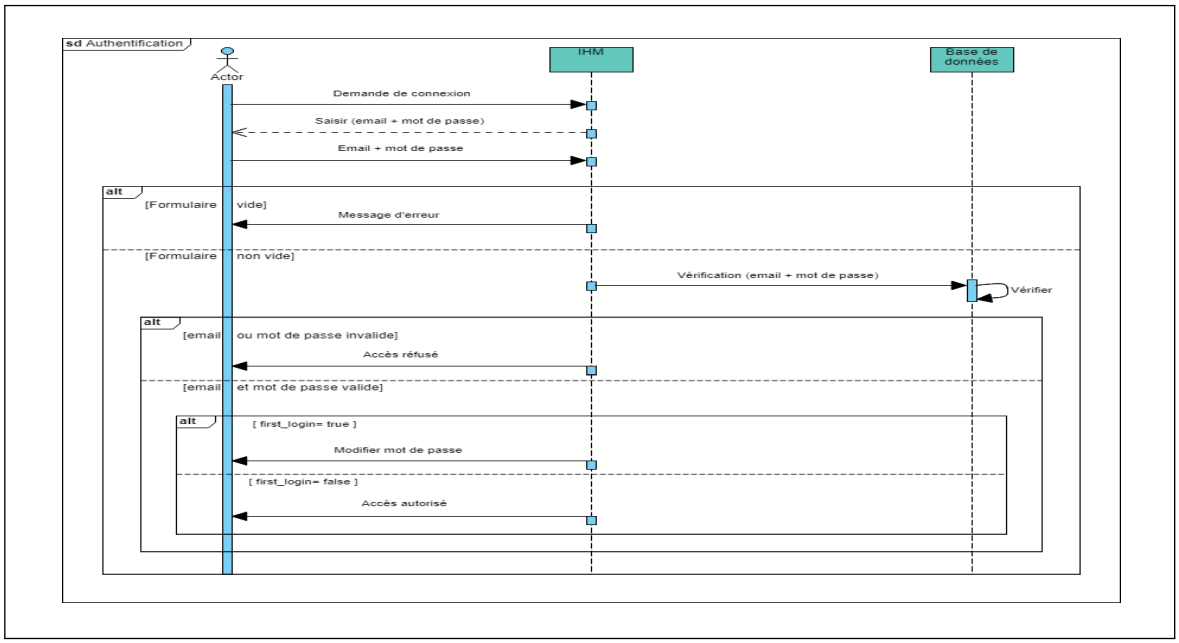

FIGURE 3.3 – Diagramme de séquence : Authentification

b) Gestion des attaques de phishing : L'acteur est : entreprise.

Etape principales :

Les étapes principales de gestion des attaques de phishing sont les suivantes :

1. L'entreprise ouvre l'application et s'authentifie.
2. L'application affiche l'interface de l'entreprise
3. L'entreprise choisie le phishing.

4. L’application affiche une interface qui contient un tableau répertoriant les attaques de phishing déjà effectuées.

5. L’entreprise effectue l’action d’ajouter une attaque

6. L’application affiche une interface qui contient un formulaire d’attaque.

7. L’entreprise remplit le nom et sélectionne : le profil d’envoie, le groupe, le modèle de l’email et la page de destination, puis lance l’attaque.

Conditions : si le formulaire de l’attaque est vide et le nom d’attaque existe déjà, l’entreprise recevra un message d’erreur sinon l’attaque sera effectuée avec succès.

Ces étapes décrivent le processus général que l’entreprise suit pour ajouter une nouvelle attaque de phishing, Le diagramme de séquences illustré dans la figure ci- dessous (voir Figure 3.4) montre les étapes de scénario précédent.

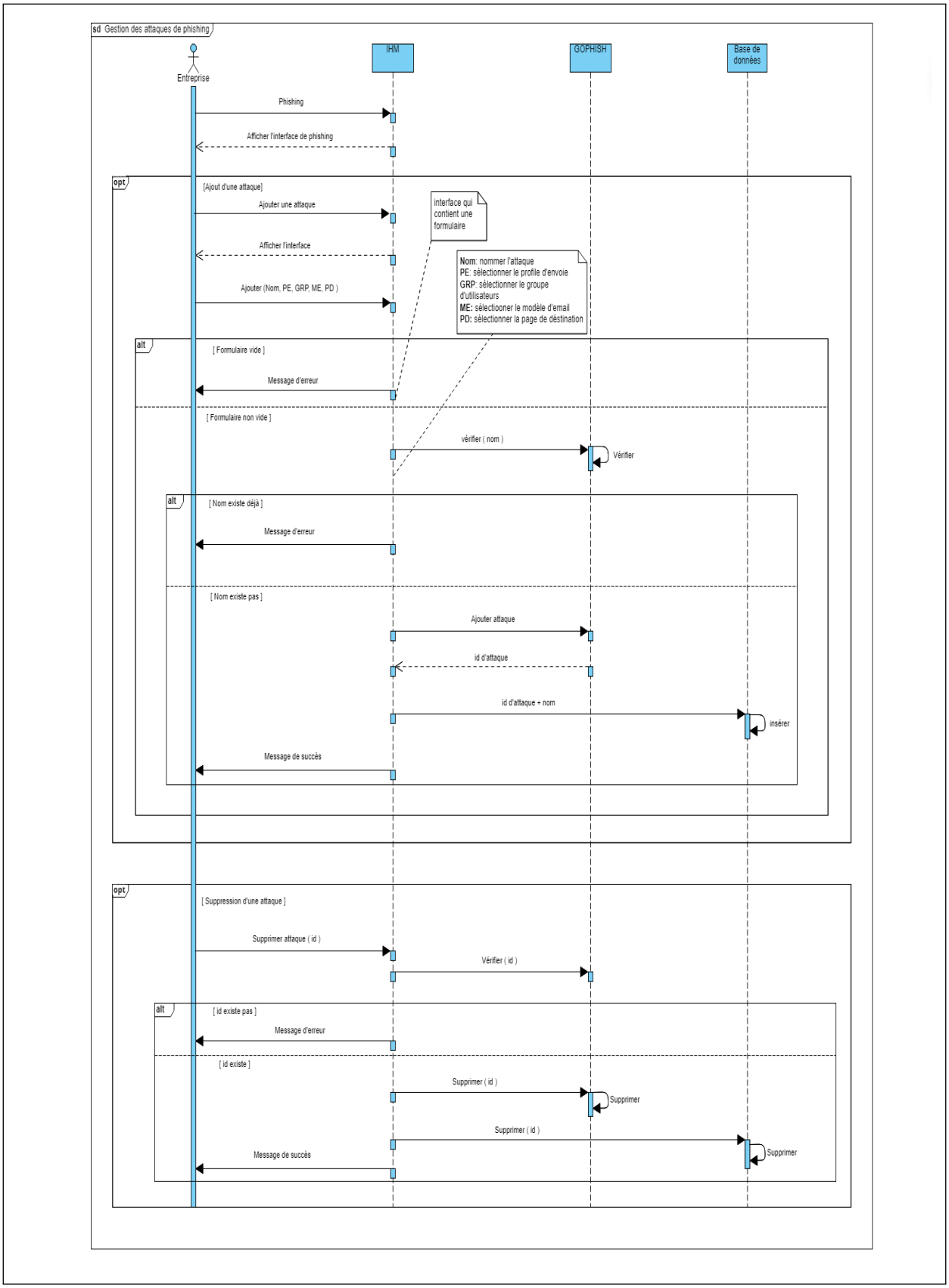

FIGURE 3.4 – Diagramme de séquence : Gestion d'une attaque de phishing

c) Affectation des cours aux employés : L'acteur est : entreprise.

les principales étapes de l'effectation des cours aux employés sont les suivantes :

Etape principales :

1. L'entreprise ouvre l'application et s'authentifie.
2. L'application affiche l'interface de l'entreprise
3. L'entreprise choisie l'affectation.
4. L'application affiche une interface qui contient un tableau des affectations déjà effectuées.
5. L'entreprise choisie d'affecter un cours.
6. L'application affiche une interface de l'affectation.
7. L'entreprise sélectionne les employés et leur envoie les cours.

Le diagramme de séquences illustré dans la figure ci-dessous (voir Figure 3.6) montre les étapes du scénario précédent.

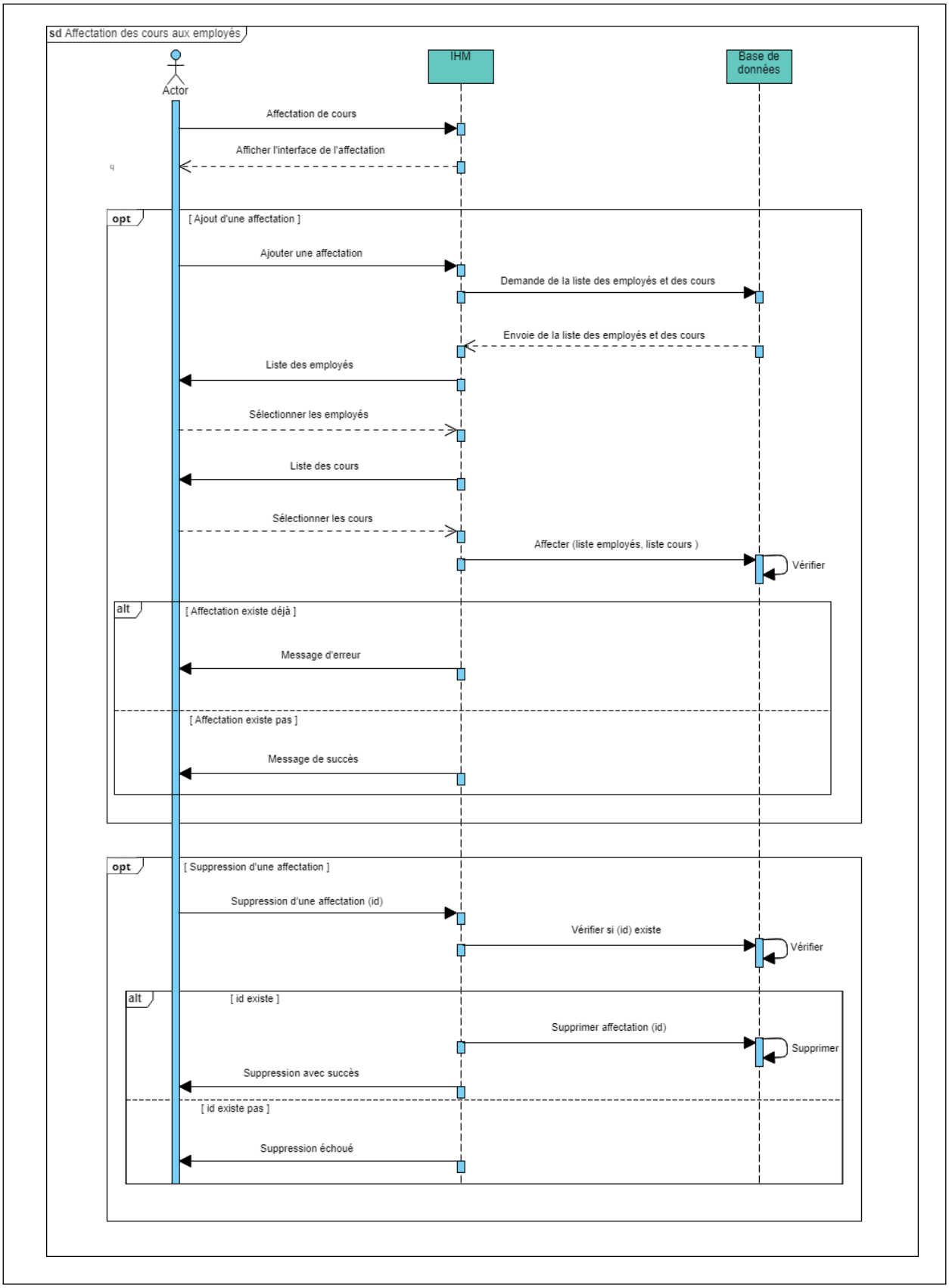

FIGURE 3.5 – Diagramme de séquence : Affectation des cours aux employés

3.2.2 Conception

La conception est une étape clé dans le cycle de vie d'un logiciel. Elle consiste à transformer les spécifications fonctionnelles et techniques en une architecture logicielle détaillée qui peut être implémentée. Cette étape de conception permet de définir les différents composants du système, leurs interactions, et leurs comportements.

Dans cette phase, différents diagrammes UML peuvent être utilisés pour représenter les différents aspects de l'architecture logicielle. Nous allons utiliser le diagramme d'activité pour décrire les différentes activités et processus du système, en montrant les actions à effectuer et les décisions à prendre. Puis nous utilisons le diagramme de classes pour définir les différentes classes du système, leurs attributs, leurs méthodes, et leurs relations. Enfin, nous utilisons le diagramme de déploiement pour représenter l'architecture matérielle du système, en montrant les différents nœuds et les connexions.

3.2.2.1 Définition du processus global

Le processus global de notre système (illustré dans la figure 3.7) consiste à effectuer un suivi pour les employés d'une entreprise. Cela implique trois autres processus que nous allons définir dans ce qui suit : lancement d'une formation, lancement d'une attaque et évalution de cours. Après chaque formation ou attaque, l'action d'affichage de statistique est effectuée pour décider si les cours doivent être évalués ou pas.

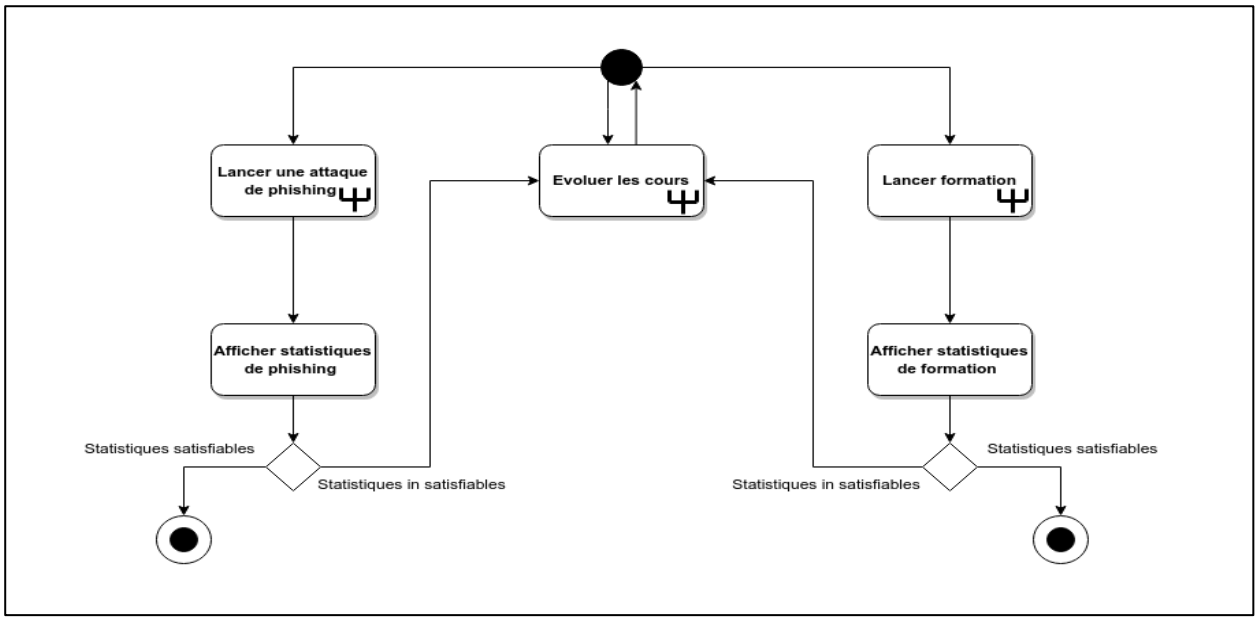

FIGURE 3.6 – Diagramme d'activité : Processus global

a) Lancement de l'attaque de phishing : Notre solution propose des attaques de phishing automatisées pour tester les employés et lutter contre cette menace. Cette fonctionnalité permet aux entreprises de simuler des attaques de phishing réalistes afin d'évaluer la vulnérabilité de leurs employés et de renforcer leur sensibilisation à ce type d'attaque. Grâce à des tests réguliers et ciblés, les entreprises peuvent identifier les lacunes en matière de cybersécurité, mettre en place des programmes

de sensibilisation et offrir une formation supplémentaire aux employés les plus vulnérables. Cela contribue à renforcer la résilience globale de l'entreprise face aux attaques de phishing. Le processus de lancement d'attaque est décrit dans le diagramme suivants (Figure 3.8) :

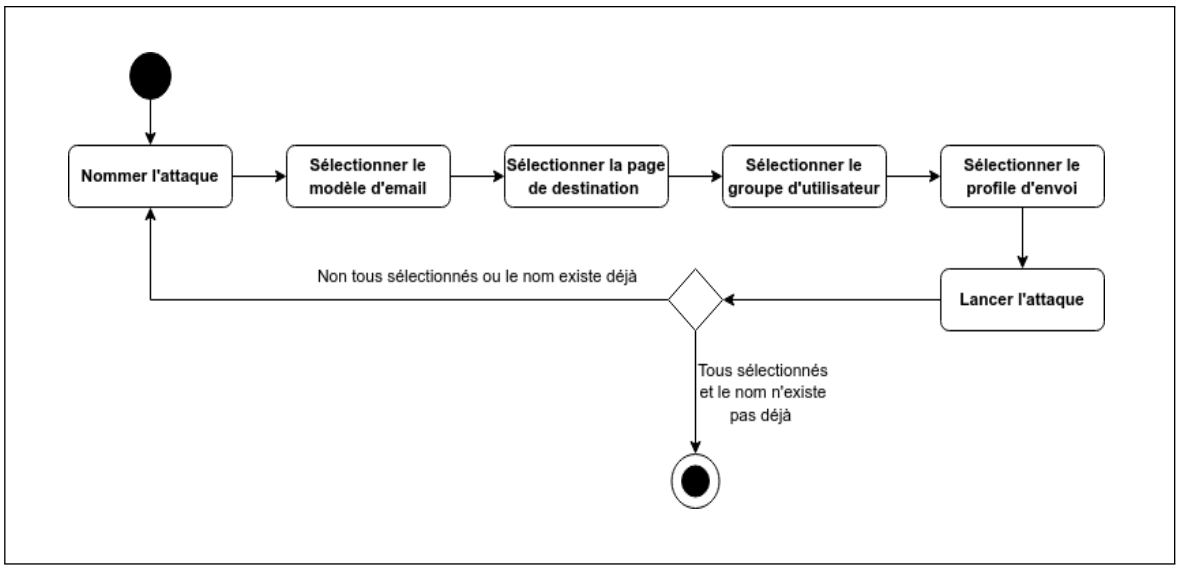

FIGURE 3.7 – Diagramme d'activité : Lancement d'une attaque

- **Le profil d'envoi (Sending profile)** : Un "Profil d'envoi" est la configuration SMTP qui indique à Gophish comment envoyer des e-mails [30].
- **Modèle d'email (Email template)** : Un "Modèle" est le contenu des e-mails qui sont envoyés aux destinataires. Ils peuvent être importés à partir d'un e-mail existant ou créés à partir de zéro [31].
- **Page de destination (Landing page)** : Une page de destination est le contenu HTML renvoyé lorsque les destinataires cliquent sur les liens dans les e-mails de Gophish [32].
- **Groupe d'utilisateur (Users and groups)** : Gophish gère les destinataires des campagnes par groupes. Chaque groupe peut contenir un ou plusieurs destinataires [33].

b) Évolution des cours : L'évolution de cours est une étape clé de notre solution de sensibilisation en cybersécurité. Nous avons donc mis en place une démarche pour accompagner l'équipe de cybersécurité dans cette étape. Le processus est décrit dans un diagramme qui permet de garantir l'évolution de formations adaptées et efficaces pour les employés.

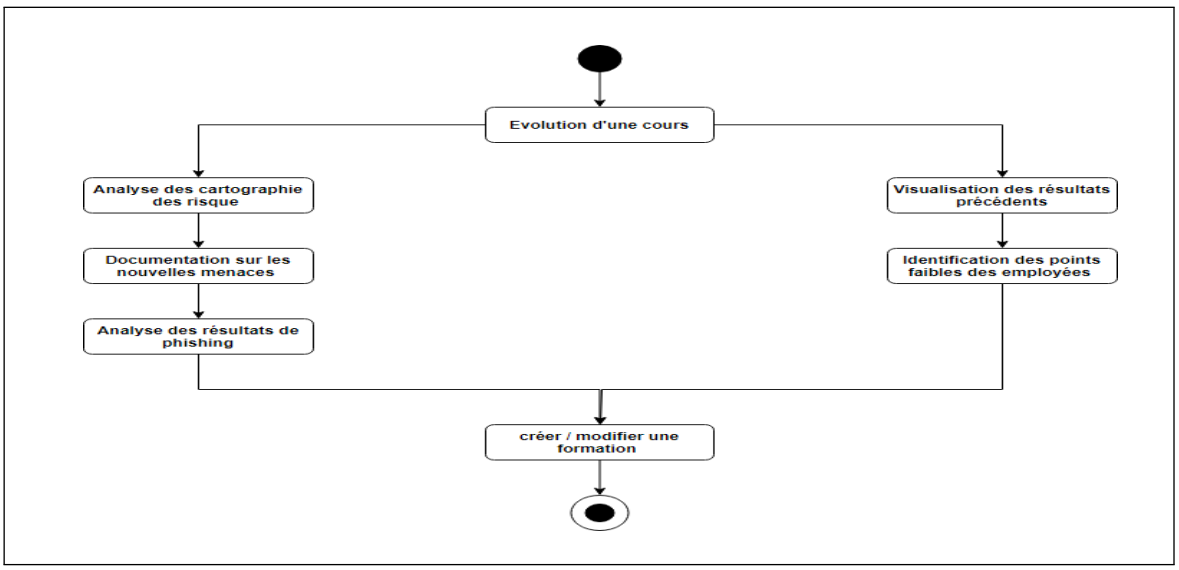

FIGURE 3.8 – Diagramme d'activité : Evolution d'un cours

c) Lancement de la formation : Nous utilisons des formations créées par nous avec l'assistance de l'équipe de cybersécurité de MNA GROUPE certifiée PECB (Professional Evaluation and Certification Board) pour sensibiliser les utilisateurs. La plateforme gère l'ensemble du processus de formation, de la création à l'affectation des formations.

Les employés peuvent suivre les formations et passer des quiz. Voici le processus de lancement de formation :

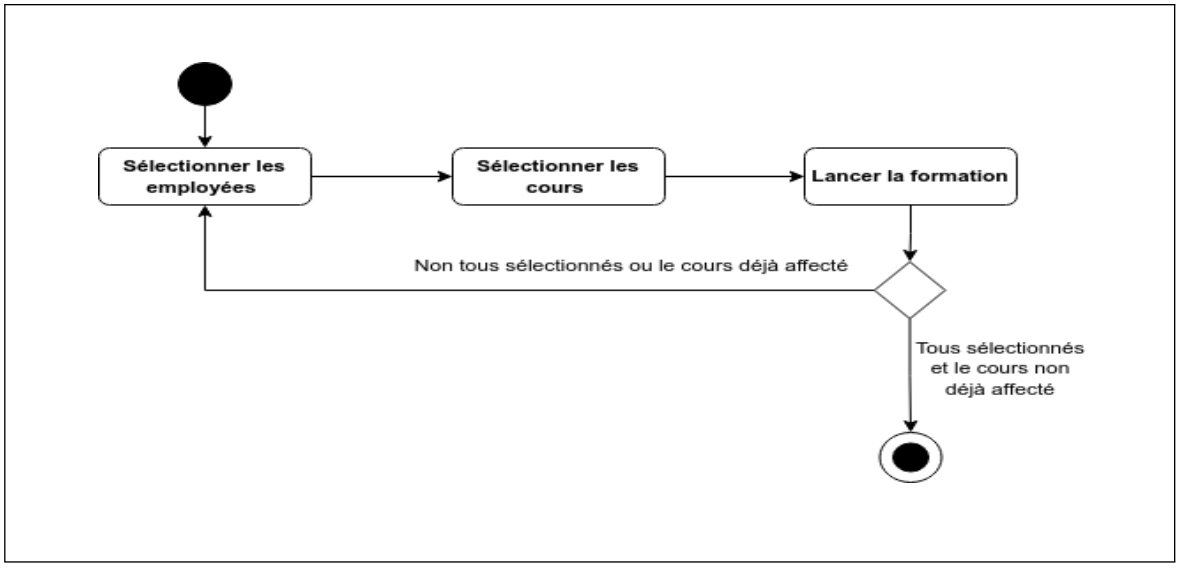

FIGURE 3.9 – Diagramme d'activité : Lancement d'une formation

3.3 Conception détaillée

Après avoir défini la vue comportementale de notre système, nous examinerons maintenant de plus près le système en abordant la conception détaillée des modules.

Dans ce qui suit, nous présentons le diagramme de classes de conception pour identifier les différentes classes de notre système.

3.3.1 Diagramme de classes de conception

Nous présentons le diagramme de classe de conception de notre solution (Voir Figure 3.11) :

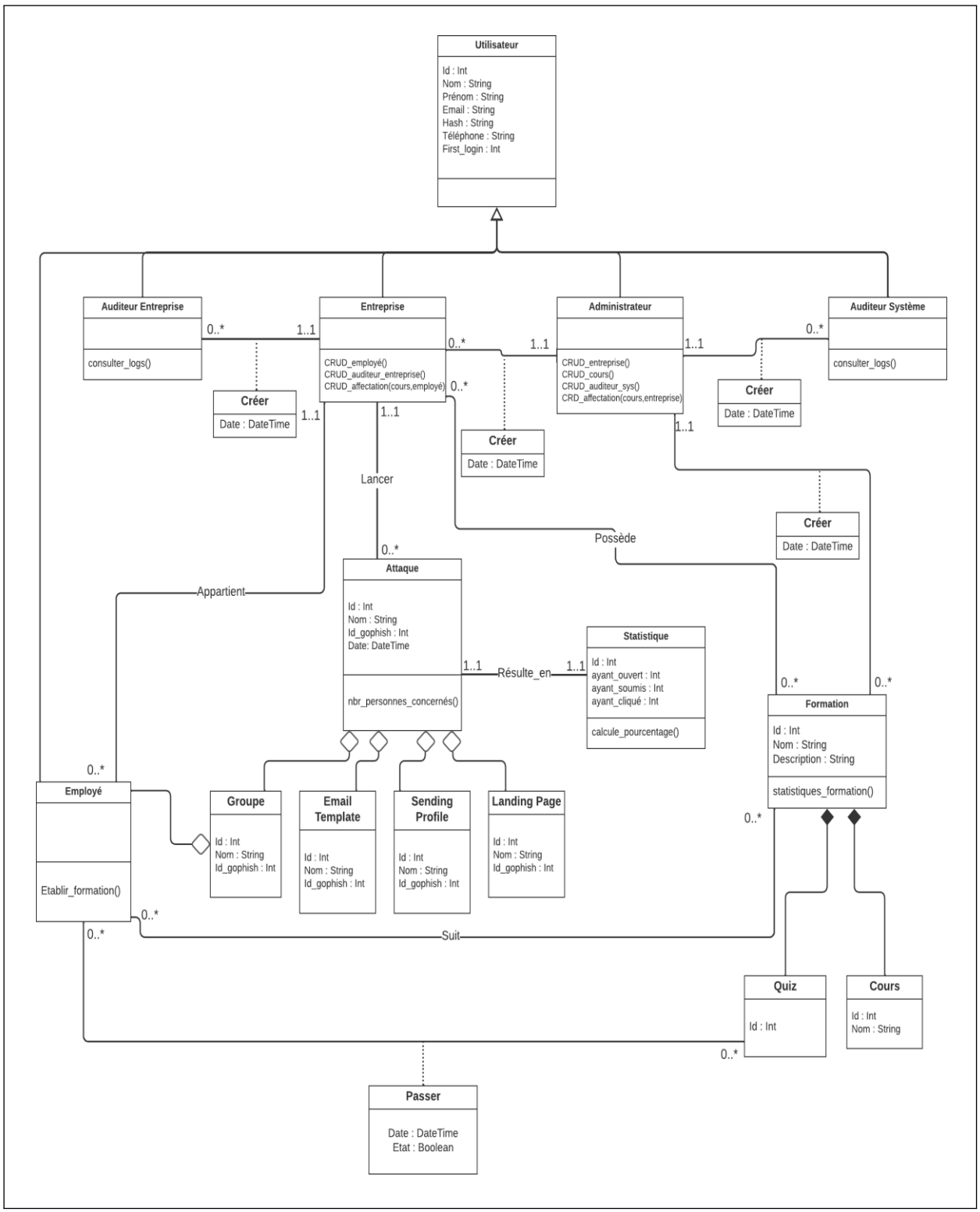

FIGURE 3.10 – Diagramme de classes de conception

Dans le tableau ci-dessous, nous présenterons en détail les classes importantes de notre diagramme :

Classe	Id	Attributs et méthodes	Désignation
Utilisateur	id	- Id - Nom - Prénom - Email - Mot de passe - First_login	- Identificateur de l'utilisateur - Nom de l'utilisateur - Prénom de l'utilisateur - Email de l'utilisateur - Mot de passe de l'utilisateur - Identifier la première connexion
Admin	id	- CRUD_entreprise() - CRUD_cours() - CRUD_auditeu_sys() - CRD_affectation(cours, entreprise)	- Ajouter, rechercher, mettre à jour, supprimer une entreprise - Ajouter, rechercher, mettre à jour, supprimer un cours - Ajouter, rechercher, mettre à jour, supprimer un auditeur - Ajouter, rechercher, supprimer une affectation
Entreprise	id	- CRUD_employé() - CRUD_auditeur_ entreprise() - CRD_affectation(cours, employé)	- Ajouter, rechercher, mettre à jour, supprimer un employé - Ajouter, rechercher, mettre à jour, supprimer un auditeur de l'entreprise - Ajouter, rechercher, supprimer une affectation
Employé	id	Etablir_formation()	Suit le cours et passer les quiz
Auditeur de système	id	Consulter_logs()	Consulter les logs de l'application
Auditeur d'entreprise	id	Consulter_logs()	Consulter les logs de l'entreprise
Attaque	id	- id - nom - id_gophish - nbr_personnes_concernés()	- Identificateur de l'attaque - Nom de l'attaque - Identificateur de l'attaque dans gophish - Nombre de personnes concernés par cette attaque

Statitique	id	- id - ayant_ouvert() - ayant_soumis() - ayant_cliqué()	- Identificateur de statistique - Le nombre de personnes ayant ouvert l'email de phishing - Le nombre de personnes ayant soumis leur données - Le nombre de personnes ayant cliqué sur le lien de phishing
Formation	id	- Id - Nom - Description	- Identificateur de formation - Titre de formation - La description de formation

TABLE 3.2 – Tableau descriptif des classes, attributs et méthodes

3.4 Conclusion

Dans ce chapitre, nous avons présenté notre conception en terme de vue statique et de vue dynamique de notre système. C'est une étape cruciale dans le développement de tout projet, qui implique de traduire les exigences et les spécifications en une conception tangible pouvant être mise en œuvre.

Cela nous permettra de passer à l'étape de l'implémentation puis le déploiement et les tests qui feront l'objet du chapitre suivant.

Chapitre

4

Chapitre 4 : Implémentation et résultats

4.1 Introduction

Cette dernière partie se concentre sur la présentation de la phase de réalisation et de déploiement de notre solution. Ces étapes revêtent une importance équivalente à la phase de conception, car elles permettent de concrétiser le travail effectué précédemment en mettant en œuvre et en déployant la solution.

Nous commençons par fournir une brève description des principales technologies et des outils qui nous ont aidés à réaliser notre solution. Nous les regroupons en catégories, telles que les langages de programmation, les frameworks, la base de données et les outils utilisés. Ensuite, nous présentons la solution développée en illustrant les principales fonctionnalités par le biais de captures d'écran des interfaces. Enfin, nous expliquons les mesures de sécurité mises en place et décrivons le processus de déploiement du système.

4.2 Présentation de l'environnement technologique

Dans cette section, nous allons présenter l'environnement technologique dans lequel s'inscrit notre application. Nous décrirons les langages, les frameworks et le système de gestion de base de données que nous avons utilisés pour l'implémentation.

4.2.1 Langages utilisés

Python : Le langage Python est un langage de programmation open source multi-plateformes et orienté objet. Grâce à des bibliothèques spécialisées, Python s'utilise pour de nombreuses situations comme le développement logiciel, l'analyse de données, ou la gestion d'infrastructures. Python aussi un langage de programmation interprété, et permet l'exécution du code sur n'importe quel ordinateur. Utilisable aussi bien par des programmeurs débutants qu'experts, Python permet de créer des programmes de manière simple et rapide [34] (voir la figure 4.1).

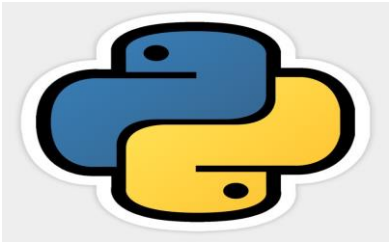

FIGURE 4.1 – Logo Python

HTML 5 : Le langage HTML (de l'anglais Hypertext Markup Language) est, depuis les toutes premières heures de l'Internet, le programme de base en matière de structuration, de mise en réseau et de contenu sur le World Wide Web. Cependant, le langage de balisage n'a cessé de se développer suite à la sortie de la version HTML 4.01 en décembre 1999 [35] (voir la figure 4.2).

FIGURE 4.2 – Logo HTML 5

CSS 3 : Une feuille de style CSS (de l'anglais Cascading Style Sheets) est un langage informatique (langage CSS) qui décrit la présentation des documents HTML, XHTML et XML. Les standards définissant le code CSS sont publiés par le World Wide Web Consortium (W3C). L'utilisation du CSS est indispensable pour le développement web (front end) afin de rendre le site esthétique et responsive design [36] (voir la figure 4.3).

FIGURE 4.3 – Logo CSS 3

JavaScript : Le JavaScript est un langage de programmation créé en 1995. Le JavaScript est aujourd'hui l'un des langages de programmation les plus populaires et il fait partie des langages web dits « standards » avec le HTML et le CSS. Le JavaScript est un langage dynamique, c'est-à-dire un langage qui va nous permettre de générer du contenu dynamique pour nos pages web. Un contenu « dynamique » est un contenu qui va se mettre à jour dynamiquement, c'est-à-dire changer sans qu'on ait besoin de modifier le code manuellement mais plutôt en fonction de différents facteurs externes [37] (voir la figure 4.4).

FIGURE 4.4 – Logo JavaScript

4.2.2 Frameworks utilisés

Un framework est une plate-forme de développement de logiciels. Il crée une base sur laquelle les développeurs peuvent créer des applications pour une plate-forme donnée. Par exemple, un framework peut contenir des classes et des fonctions prédéfinies qui peuvent être utilisées pour traiter les entrées, gérer le matériel et interagir avec le logiciel système. Cela simplifie le processus de développement car les développeurs n'ont pas à réinventer la roue à chaque fois qu'ils développent une nouvelle application.

Dans cette section, nous mentionnons tous les frameworks et bibliothèques que nous utilisons :

Flask : Flask est un petit framework web Python léger, qui fournit des outils et des fonctionnalités utiles qui facilitent la création d'applications web en Python. Il offre aux développeurs une certaine flexibilité et constitue un cadre plus accessible pour les nouveaux développeurs, puisque vous pouvez construire rapidement une application web en utilisant un seul fichier Python. Flask est également extensible et ne force pas une structure de répertoire particulière ou ne nécessite pas de code standard compliqué avant de commencer [38] (voir la figure 4.5).

FIGURE 4.5 – Logo Flask

Bootstrap : Bootstrap est un framework développé par l'équipe du réseau social Twitter. Proposé en open source (sous licence MIT), ce framework utilisant les langages HTML, CSS et JavaScript fournit aux développeurs des outils pour créer un site facilement. Ce framework est pensé pour développer des sites avec un design responsive, qui s'adapte à tout type d'écran, et en priorité pour les smartphones. Il fournit des outils avec des styles déjà en place pour des typographies, des boutons, des interfaces de navigation et bien d'autres encore. On appelle ce type de framework un "Front-End Framework" [39] (voir la figure 4.6).

FIGURE 4.6 – Logo Bootstrap

Vue.js : Vue.js est un framework javascript open-source destiné au développement d'interfaces web interactives (côté Frontend). Il fournit un cadre de développement épuré et simple à utiliser, par le biais de son organisation et sa structuration du code en composants. L'objectif de Vue.js est de fournir les avantages de la liaison de données réactive et des composants de vue composables avec une API aussi simple que possible [40] (voir la figure 4.7).

FIGURE 4.7 – Logo Vue.js

4.2.3 Système de gestion de base de données

La gestion des données est un élément important dans toute application manipulant des données. Nous allons présenter dans ce qui suit le système de gestion de base de données que nous avons utilisé, qui est le SGBD MySQL.

MySQL : MySQL a été lancé à l'origine en 1995. Depuis, il a connu quelques changements de propriétaire et de gestion, avant de se retrouver chez Oracle Corporation en 2010. Alors qu'Oracle est en charge maintenant, MySQL est toujours un logiciel open source, ce qui signifie que vous pouvez l'utiliser et le modifier librement. Le nom vient de l'association de « My » – le nom de la fille du co-fondateur – avec SQL (de anglais Structured Query Language) qui est un langage de programmation qui vous aide à accéder et gérer les données dans une base de données relationnelle [41] (voir la figure 4.8).

FIGURE 4.8 – Logo MySQL

4.2.4 Outils utilisés

En plus des langages, frameworks et SGBD, nous avons utilisé quelques outils qui nous ont facilité le développement de notre système. Nous les présentons dans ce qui suit et abordons l'intérêt de chacun d'eux.

Visual studio code : Vscode est un éditeur de code source multi-plateforme crée par Microsoft. Il supporte des dizaines de langages de programmation. Il intègre plusieurs fonctionnalités facilitant la saisie et la correction du code aux développeurs comme la coloration syntaxique ou encore le système d'auto-complétions IntelliSense [42] (voir la figure 4.9).

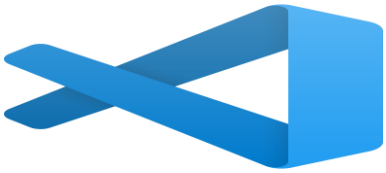

FIGURE 4.9 – Logo Vscode

API GoPhish : Gophish a été construit à partir de zéro avec une API (interface de programmation d'application) JSON qui permet aux développeurs et aux administrateurs système d'automatiser facilement les campagnes de phishing simulées [43] (voir la figure 4.10).

FIGURE 4.10 – Logo GoPhish

4.3 Sécurité du système

Il est essentiel d'intégrer des mesures de sécurité à tous les niveaux lors du développement d'un système d'information, afin de garantir une protection maximale et de maintenir son fonctionnement, sa continuité et sa disponibilité sur le long terme. Pour assurer une sécurité optimale de notre système, nous avons mis en place des mesures de sécurité à la fois au niveau physique et au niveau applicatif.

4.3.1 Sécurité au niveau physique

La sécurité physique des VPS est prise en charge par OVH [47]. Ils sont responsables de la gestion et de la mise en place des mesures de sécurité physique pour assurer la protection des serveurs. L'objectif est d'assurer la protection et la disponibilité continue des données hébergées sur les VPS OVH.

- OVH accorde une grande importance à la sécurité physique des VPS.
- Des centres de données hautement sécurisés sont utilisés pour héberger les serveurs VPS.
- Des systèmes de surveillance vidéo et des contrôles d'accès stricts sont en place 24h/24.
- Des équipes de sécurité qualifiées surveillent en permanence les installations.

- Des mesures d'authentification avancées, telles que des clés d'accès et des cartes à puce, sont utilisées pour limiter l'accès physique aux serveurs.
- Des politiques de gestion des câbles, de maintenance préventive et de sauvegarde régulière des données sont mises en œuvre.

4.3.2 Sécurité au niveau logique

Pour assurer la sécurité au niveau applicatif nous avons mis en place les contrôles suivants :

- **Authentification :** L'authentification consiste à vérifier les informations d'identification de l'utilisateur. Dans les applications Web, ce processus est géré par des sessions qui utilisent des paramètres tels que l'email, le nom d'utilisateur et le mot de passe pour identifier l'utilisateur. Si ces paramètres correspondent, l'utilisateur est considéré comme authentifié. Dans Flask, les sessions sont utilisées pour stocker et maintenir les informations spécifiques à chaque utilisateur entre les requêtes HTTP. Elles permettent de gérer l'authentification et l'état de l'application de manière persistante.
- **Gestion des privilèges et des droits d'accès :** Dans le contexte de sécurisation d'une application web, il est essentiel de vérifier si un utilisateur a les droits nécessaires pour accéder à la ressource demandée. Dans notre application, nous avons mis en place une classification des utilisateurs en différents profils tels que l'Administrateur, l'Auditeur système, l'Entreprise, l'Auditeur d'entreprise, et l'employé. Les privilèges et les droits d'accès sont gérés lors de la création des comptes. Chaque utilisateur est associé à un profil qui détermine ses droits d'accès aux fonctionnalités des différents modules de l'application.
- **Contrôle de saisie :** Dans notre système, nous mettons en place un contrôle strict des champs saisis par l'utilisateur afin de garantir l'intégrité des données et d'éliminer les risques d'injections SQL. Le système effectue des vérifications sur les champs obligatoires pour s'assurer qu'ils sont correctement renseignés par l'utilisateur. De plus, il vérifie également les valeurs et les types de données des champs pour assurer leur conformité.
- **Journalisation (logging) :** Dans notre système, nous utilisons des fichiers journaux (logs) pour enregistrer les exceptions survenues pendant l'exécution ainsi que pour tracer les opérations effectuées par les utilisateurs. Ces fichiers permettent de garder une trace des événements et de faciliter la surveillance et le débogage du système.

4.4 Présentation du prototype

Dans ce qui suit nous allons présenter le prototype de notre système à travers les interfaces suivantes :

Interface de connexion : voici l'interface de connexion qui l'illustre (la figure 4.11) ci-dessous.

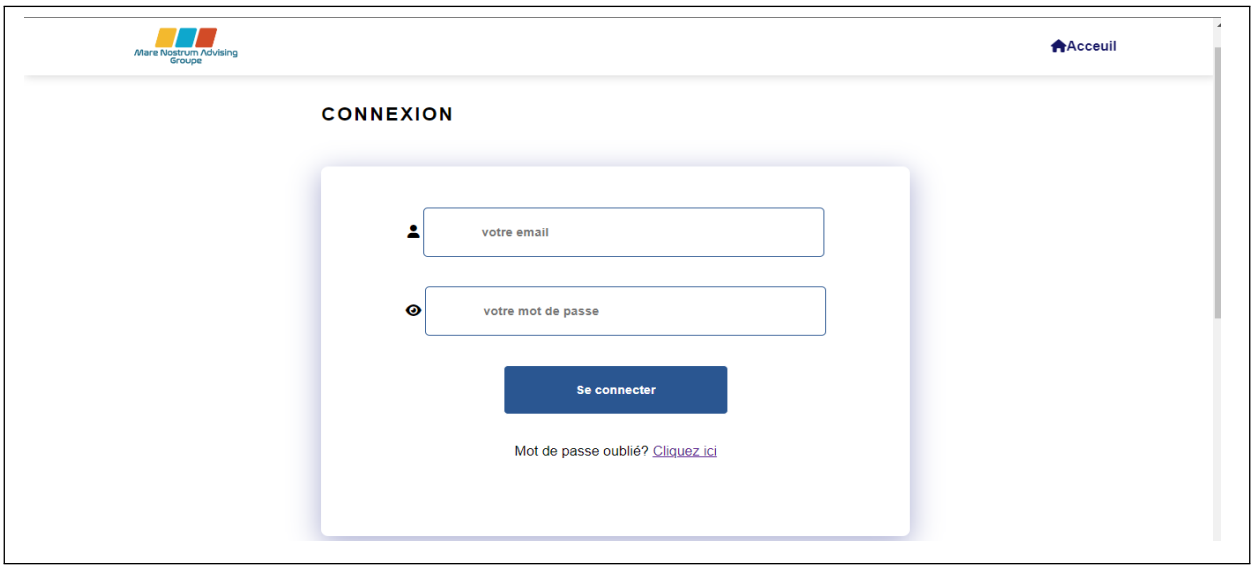

FIGURE 4.11 – Interface de connexion

Interface de l'administrateur : (la figure 4.12) suivante représente l'interface d'un administrateur.

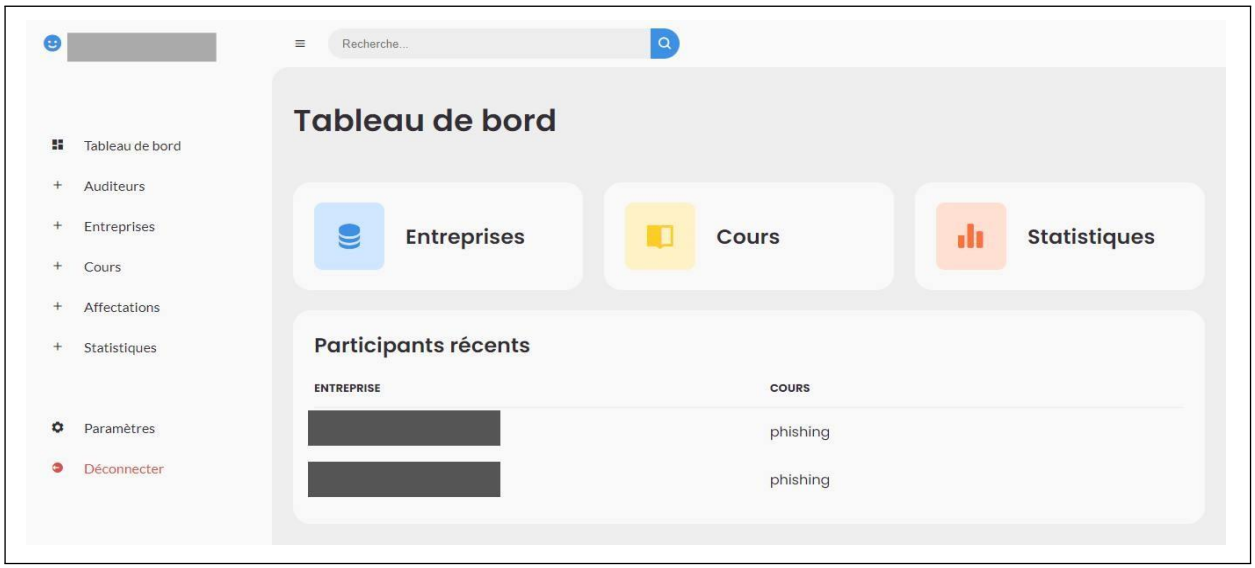

FIGURE 4.12 – Interface de l'administrateur

Interface de l'affectation des cours aux entreprises : (La figure 4.13) ci-dessous représente une interface de l'affectation des cours aux entreprises.

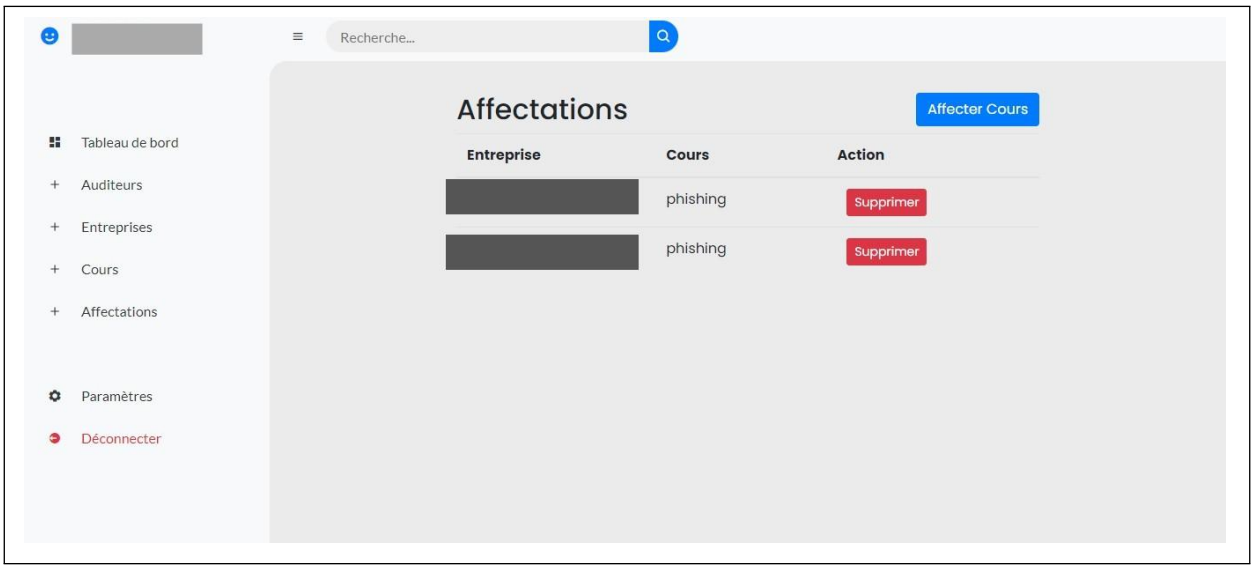

FIGURE 4.13 – Interface de l'affectation des cours aux entreprises

Interface de l'entreprise : (La figure 4.14) ci-dessous représente l'interface de l'entreprise.

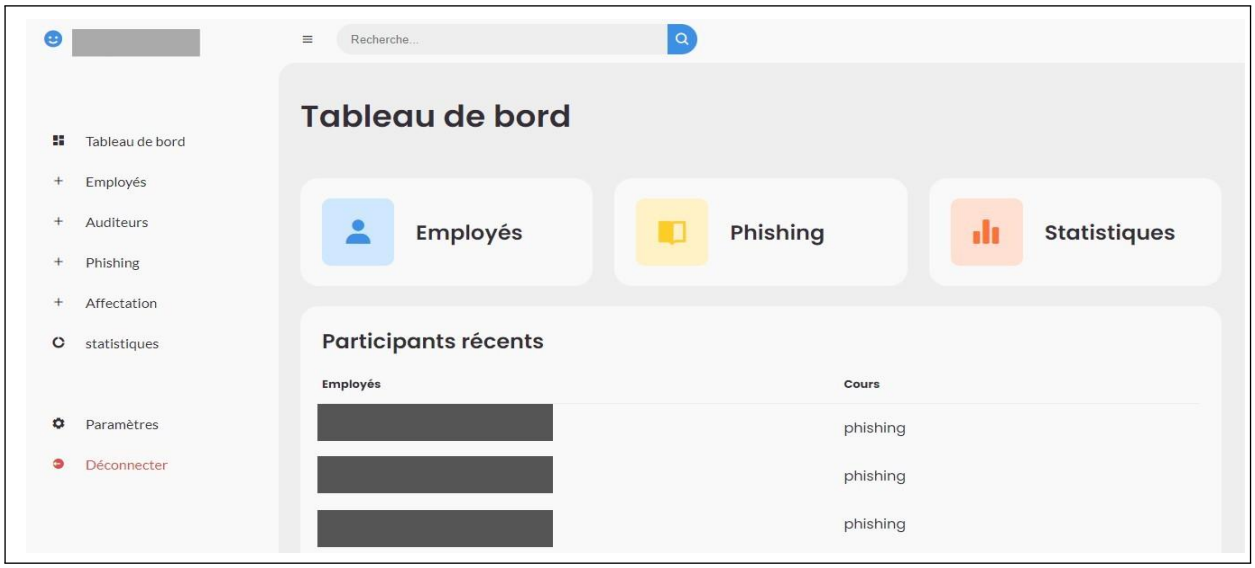

FIGURE 4.14 – Interface de l'entreprise

Interface de l'employé : (La figure 4.15) suivante représente une interface de l'employé.

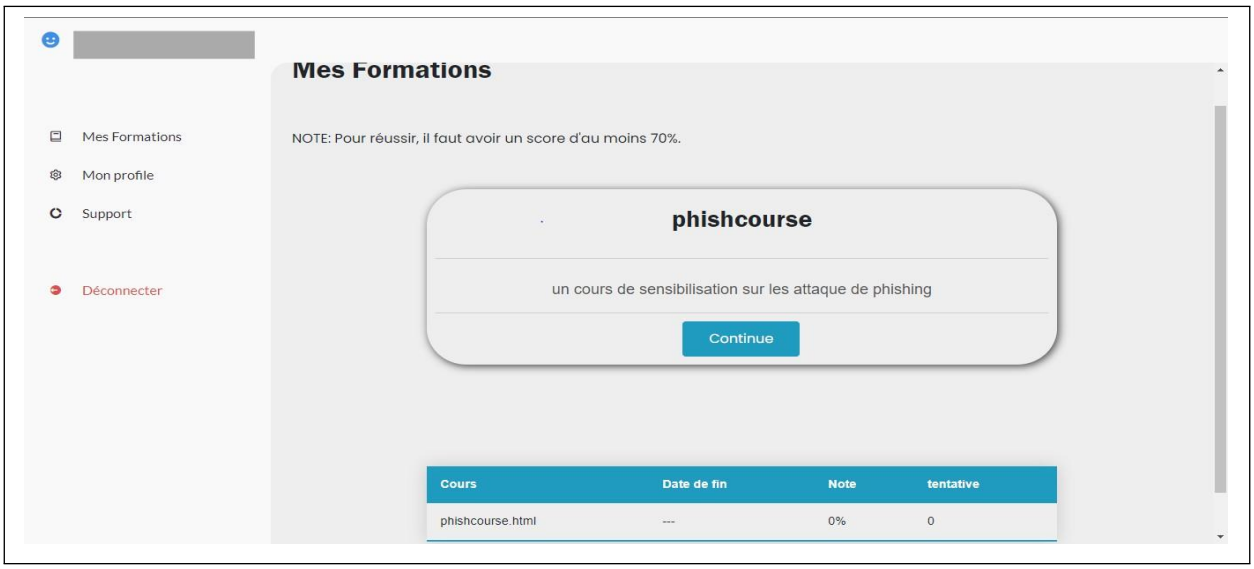

FIGURE 4.15 – Interface de l'employé

Interface de l'auditeur de système : (La figure 4.16) ci-dessous représente une interface de l'auditeur de système.

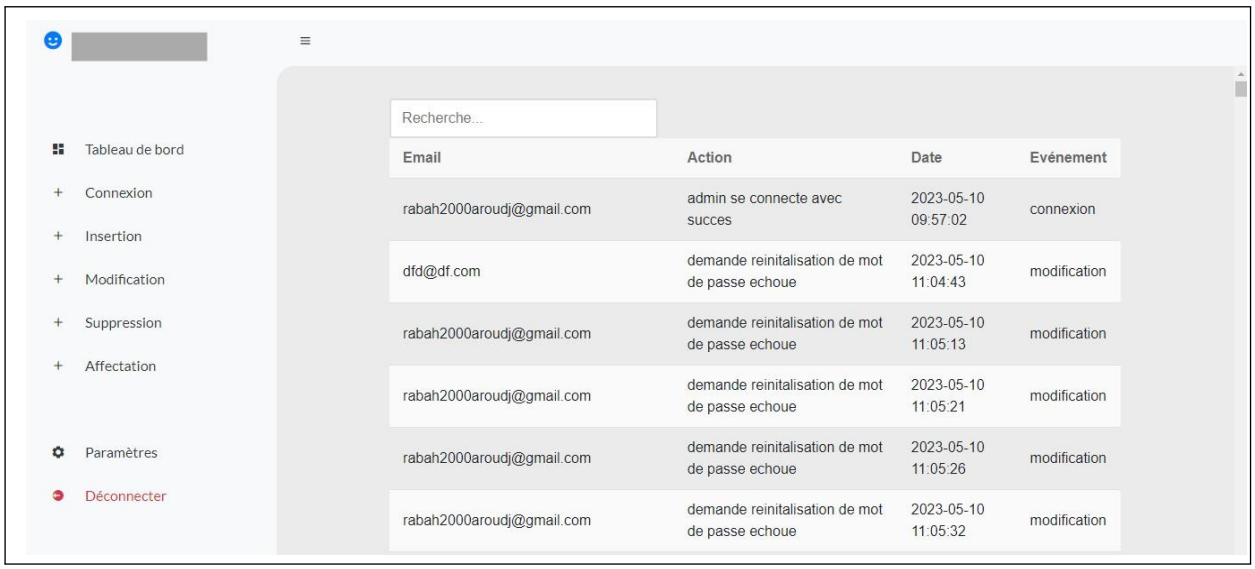

FIGURE 4.16 – Interface de l'auditeur de système

Interface de l'attaque de phishing : (La figure 4.17) ci-dessous représente une interface de l'attaque de phishing.

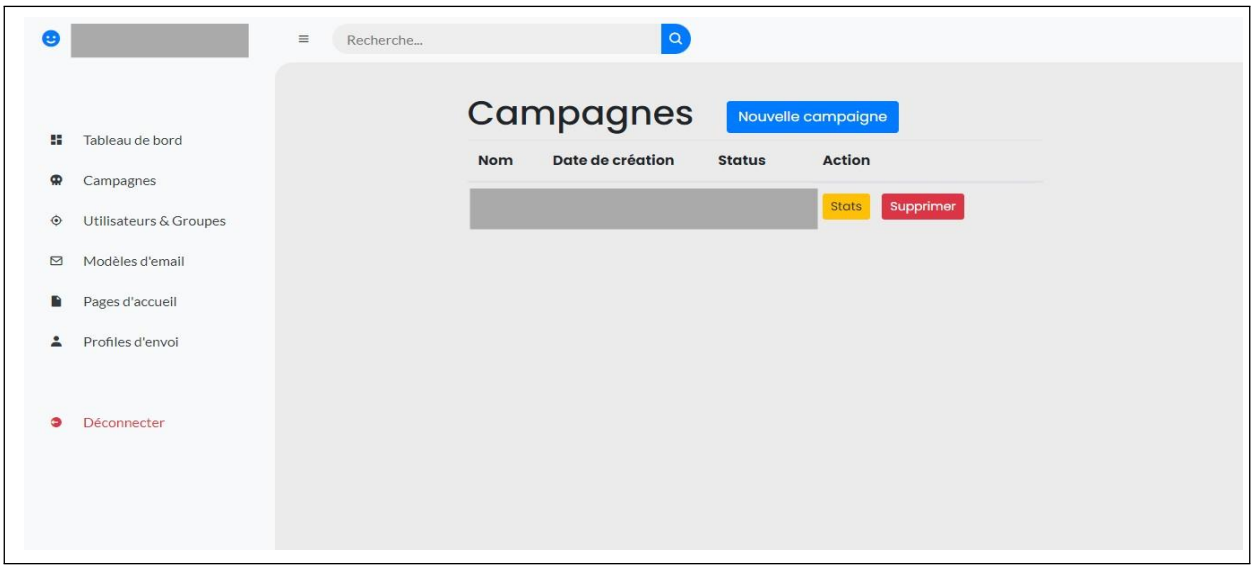

FIGURE 4.17 – Interface de l'attaque de phishing

4.5 Déploiement

Pour déployer notre application Web développée avec Flask en utilisant Python sur un VPS OVH (On Vous Héberge),voici les étapes principales :

- Configurer le code source Flask en mode de production conformément à la documentation officielle de Flask.
- Créer une base de données MySQL vide et récupérer les informations de connexion nécessaires.
- Modifier le fichier de configuration « .cfg » dans le code source Flask avec les informations de la base de données.
- Configurer le serveur Web sur notre VPS OVH en suivant les recommandations fournies par OVH.
- Transférer les fichiers de l'application Flask sur le VPS OVH en utilisant un protocole de transfert de fichiers.
- Exécuter les commandes de configuration nécessaires pour démarrer l'application Flask sur le VPS.
- Surveiller l'application après le déploiement pour s'assurer de son bon fonctionnement.

Ces étapes permettent de déployer notre application Flask sur un VPS OVH et de la rendre accessible en production. On peut résumer ces étapes dans le diagramme de déploiement ci-dessous :

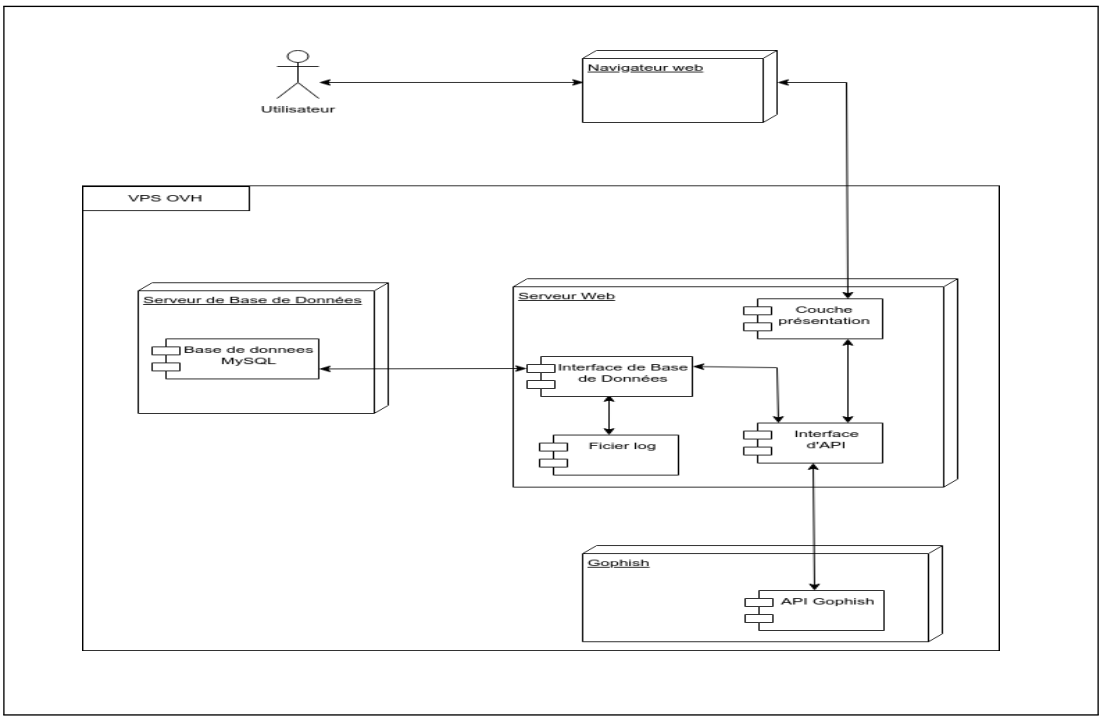

FIGURE 4.18 – Diagramme de déploiement

4.6 Tests

L'étape de test consiste à vérifier si le logiciel développé répond aux exigences et aux spécifications définies et s'il fonctionne correctement. Pour la réaliser, nous avons défini un scénario de test réel. Il est décrit dans ce quit suit.

Une compagnie d'assurance basée en Côte d'Ivoire, qui compte 120 employés, souhaite sensibiliser ses employés sur les dangers de phishing (l'hameçonnage), dont la plupart n'ont aucune expérience dans le domaine informatique. La première étape de ce processus consiste à organiser une première session de simulation d'attaque de phishing afin de recueillir des données. Parmi ces données, on souhaite connaître le nombre d'employés ayant été ciblés par l'attaque, combien ont ouvert l'email de phishing, combien ont cliqué sur le lien et combien ont soumis leurs informations personnelles.

La deuxième étape consiste à former les employés qui ont été victimes de l'attaque précédante sur les dangers du phishing, puis à recueillir des statistiques sur la formation. Par exemple, on souhaite savoir combien d'employés ont participé à cette formation, le taux de réussite et le taux d'échec.

La dernière étape consiste à organiser une deuxième session de simulation d'attaque de phishing et à collecter les mêmes données que lors de la première session, afin de les comparer pour mieux comprendre l'impact de la formation et des attaques de phishing sur les employés de la compagnie.

Il est important de noter que les différentes étapes de ce processus sont réalisées avec les mêmes 120 employés, et ce scénario a été approuvé par le directeur de la compagnie.

4.7 Résultat et discussion

Après avoir exécuté les plans de test, nous avons enregistré les résultats de chaque étape. Nous allons dans ce qui suit présenter les résultats obtenus, et nous allons à la fin les discuter.

Etape 1 (attaque pré-sensibilisation) : les résultats de l'attaque pré-sensibilisation sont les suivants :

- Nombre de cibles (nombre d'employés ont été ciblés par l'attaque) : 120
- Nombre d'employés ayant ouvert l'e-mail de phishing : 98
- Nombre d'employés ayant cliqué sur le lien de phishing : 86
- Nombre d'employés ayant soumis leurs données : 80

Le graphique ci-dessous présente de manière visuelle les résultats obtenus (voir la figure 4.19) :

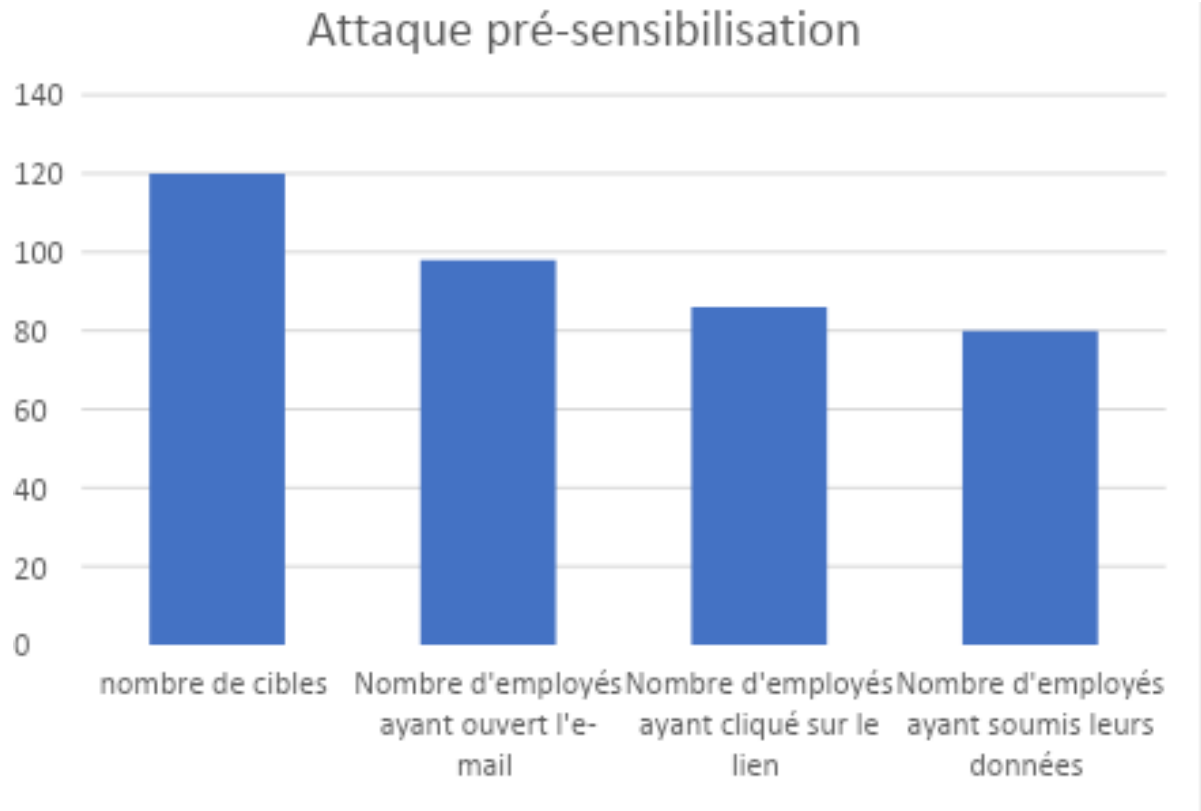

FIGURE 4.19 – Graphe des résultats pré-sensibilisation

Etape 2 (sensibilisation) : les résultats de l'étape de la sensibilisation sont les suivants :

- Nombre de cibles (nombre d'employé à former) : 120
- Nombre d'employés ayant réussi : 108
- Nombre de succès dès la première tentative : 87
- Nombre d'employés ayant échoué : 12

Le graphique ci-dessous présente de manière visuelle les résultats obtenus (voir la figure 4.20) :

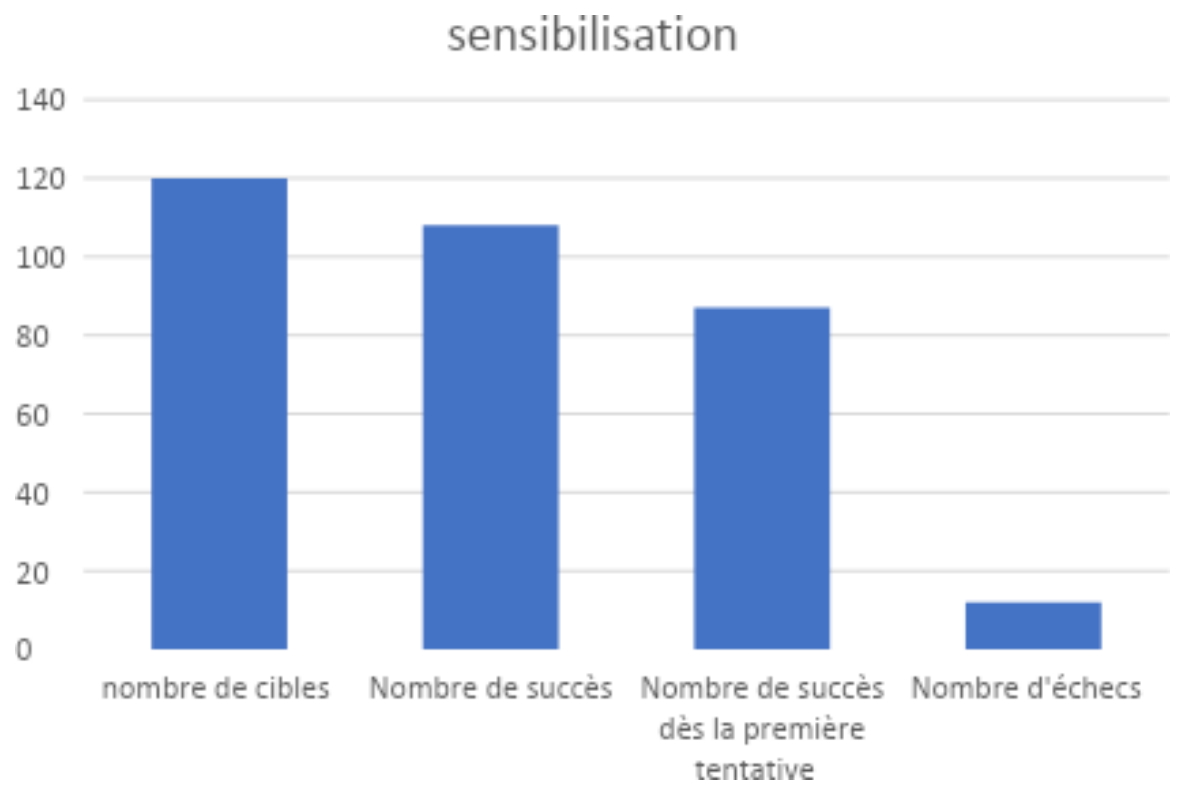

FIGURE 4.20 – Graphe des résultats de sensibilisation

Etape 3 (attaque post-sensibilisation) : les résultats de l'attaque post-sensibilisation sont les suivants :

- Nombre de cibles (nombre d'employés ont été ciblés par l'attaque) : 120
- Nombre d'employés ayant ouvert l'e-mail de phishing : 19
- Nombre d'employés ayant cliqué sur le lien de phishing : 8
- Nombre d'employés ayant soumis leurs données : 2

Le graphique ci-dessous présente de manière visuelle les résultats obtenus (voir la figure 4.21) :

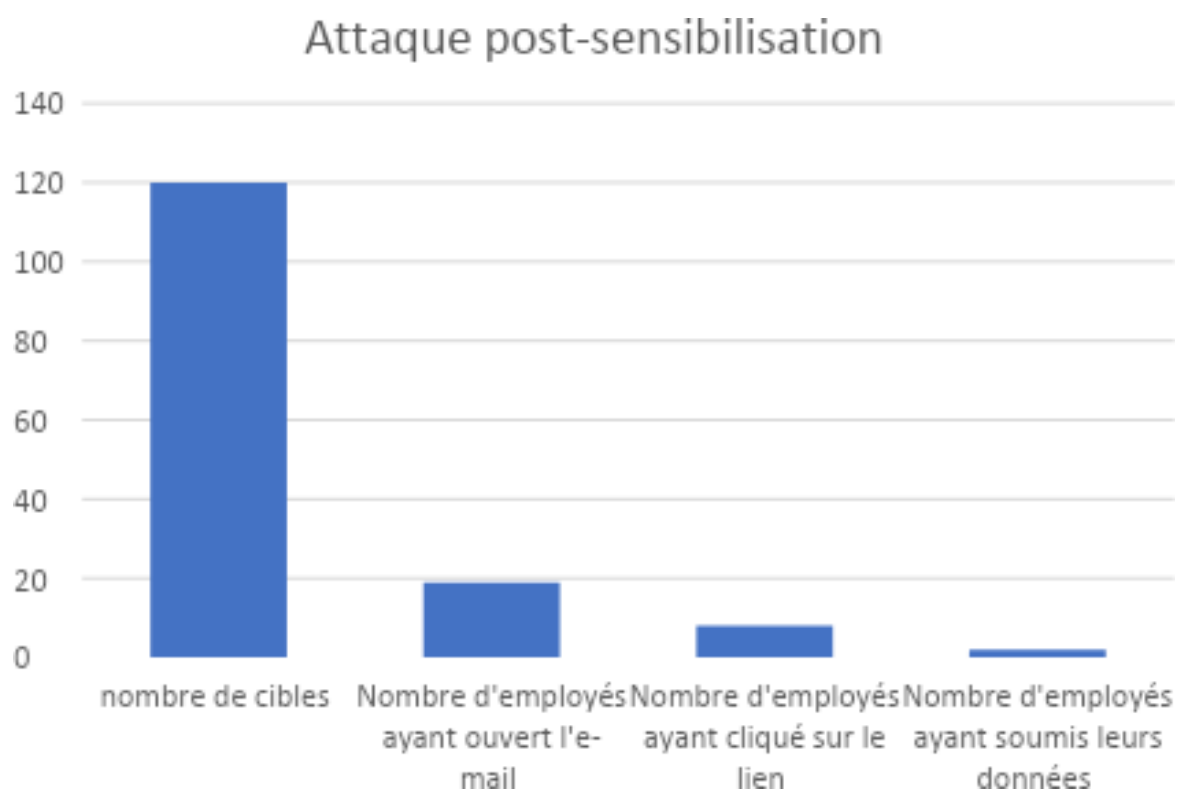

FIGURE 4.21 – Graphe des résultats post-sensibilisation

Le tableau ci-dessous résume les résultats obtenus de des attaques effectuées avant et après la sensibilisation.

Attaques	Nombre de cibles	Nombre qui ouvre l'e-mail	Nombre qui clique sur le lien	Nombre qui soumet leurs données
Pré-sensibilisation	120	98	86	80
Post-sensibilisation	120	19	8	2

TABLE 4.1 – Tableau comparatif des résultats avant et après la sensibilisation

Les données du tableau sont présentées de manière visuelle dans le graphe suivant (voir Figure 4.22) :

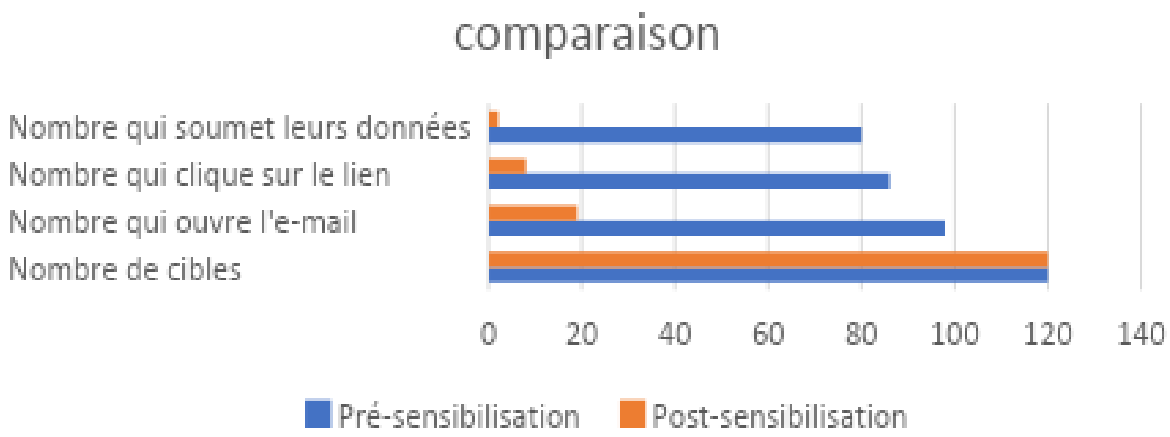

FIGURE 4.22 – Graphe comparatif des résultats avant et après la sensibilisation

En comparant les résultats de l'attaque pré-sensibilisation et de l'attaque post-sensibilisation, nous pouvons observer des différences significatives dans les comportements des employés face aux tentatives de phishing. Voici une analyse comparative des deux attaques :

Nombre de cibles : Lors de l'attaque pré-sensibilisation, nous avons ciblé l'ensemble de nos 100 employés, ce qui a été maintenu pour l'attaque post-sensibilisation. Ainsi, le nombre de cibles reste constant dans les deux cas. Il est important de noter que les cibles pré et post représentent les mêmes personnes.

Ouverture de l'e-mail : Dans l'attaque pré-sensibilisation, 90 employés ont ouvert l'e-mail de phishing, soit un taux d'ouverture de 90%. En revanche, lors de l'attaque post-sensibilisation, seuls 20 employés ont ouvert l'e-mail, ce qui représente un taux d'ouverture nettement inférieur de 20%. Cela indique une amélioration significative de la prudence des employés après avoir bénéficié d'une sensibilisation.

Clic sur le lien : Lors de l'attaque pré-sensibilisation, 75 employés ont cliqué sur le lien inséré dans l'e-mail, soit un taux de clic de 83.3%. En comparaison, lors de l'attaque post-sensibilisation, seulement 10 employés ont cliqué sur le lien, soit un taux de clic considérablement réduit de 50%. Cette diminution démontre clairement l'efficacité de la sensibilisation dans la réduction des comportements à risque.

Soumission des données : Dans l'attaque pré-sensibilisation, 70 employés ont soumis leurs données, représentant une vulnérabilité potentielle de 70%. En revanche, lors de l'attaque post sensibilisation,seuls 2 employés ont soumis leurs données, indiquant une amélioration drastique de la sécurité, avec un taux de soumission réduit à 2%.

En analysant ces résultats, nous remarquons que la sensibilisation a joué un rôle essentiel dans la réduction des comportements risqués face aux attaques de phishing. Les employés ont montré une plus grande prudence en matière d'ouverture d'e-mails suspects, de clics sur des liens inconnus et de soumission de leurs données personnelles.

Bien que les résultats obtenus soient intéressants en termes de prévention contre le phishing, des tests complémentaires doivent être effectués. En effet, la période qui sépare la sensibilisation et l'attaque est courte, donc il est normal que les employés fassent attention à leurs comportements dans la période qui suit la formation. Il serait intéressant de refaire l'attaque après un certain temps pour avoir des retours concernant la fréquence des rappels.

Une première conclusion de ces tests est que dans le domaine de la cybersécurité, il est essentiel de prendre en compte le facteur humain, qui est souvent négligé mais revêt d'une grande importance. D'autres scénarios impliquant d'autres compagnies et d'autres profils sont nécessaires pour pouvoir tirer plus de conclusions.

4.8 Conclusion

Dans cette section, nous avons présenté les technologies utilisées lors de la phase de développement du projet, discuté de l'aspect sécurité de la solution, et présenté le prototype à travers des captures d'écran des interfaces. Enfin, nous avons énuméré les étapes à suivre pour le déploiement du système.

Cependant, il est important de noter que la réalisation du projet et de ce scénario de test ne marque pas la fin du processus de développement de notre système. En effet, d'autres scénarios impliquant d'autres compagnies et d'autres profils sont nécessaires pour pouvoir tirer des conclusions.

CONCLUSION GÉNÉRALE

Dans le cadre de notre projet, nous avons développé un outil qui permet aux entreprises de mettre à l'épreuve leurs employés en matière de cybersécurité et de renforcer leur sensibilisation, en particulier face aux attaques de phishing. Notre solution offre une gamme complète de fonctionnalités, offrant ainsi de nombreux avantages pour les entreprises et leurs employés.

Grâce à notre solution, les entreprises peuvent évaluer de manière précise le niveau de conscience de leurs employés en matière de cyberattaques, en se concentrant spécifiquement sur les attaques de phishing. Nous avons mis en place une automatisation efficace des attaques de phishing, permettant aux entreprises de simuler des scénarios réalistes et de mesurer la réaction de leurs employés. En fonction des résultats obtenus, notre solution facilite également l'affectation de formations ciblées pour améliorer les compétences de sensibilisation des employés.

Un aspect clé de notre application réside dans son caractère automatisé, qui permet aux entreprises de gagner du temps et d'économiser des efforts considérables. Les tests de maturité des employés, qui étaient auparavant chronophages, peuvent désormais être effectués de manière plus efficace grâce à notre outil. Les entreprises peuvent ainsi consacrer davantage de temps à d'autres activités essentielles, tout en renforçant la sécurité de leurs employés face aux menaces cybernétiques.

Une autre fonctionnalité importante de notre solution est la génération automatique de statistiques sur les attaques et les formations. Ces statistiques fournissent aux entreprises une vision claire de l'efficacité de leurs mesures de sensibilisation à la cybersécurité. Elles facilitent également le processus d'affectation des formations en identifiant les employés qui nécessitent une attention particulière et en mettant en évidence les domaines spécifiques où des améliorations sont nécessaires.

Dans une perspective d'amélioration, il serait souhaitable d'envisager les élé- ments suivants pour notre application :

- L'intégration d'un système de messagerie directement au sein de notre application, permettant aux utilisateurs de communiquer et de partager des informations de manière plus fluide et sécurisée.
- La mise en place d'une application Mobile côté client (FrontEnd) qui exploite les API Backend déjà implémentées.
- L'ajout d'un système de notification intégré dans notre application, afin d'informer les utilisateurs des événements importants ou des mises à jour.
- Amélioration du design de l'application pour offrir une meilleure expérience utilisateur.
- Amélioration du contenu du cours.
- Intégrer de nouveaux modules permettant de faire face à d'autres types d'attaques.

Ces fonctionnalités supplémentaires contribueront à améliorer l'expérience utilisateur de notre application en renforçant la communication interne et en facilitant la gestion des informations importantes. Elles offriraient également une meilleure interaction avec les utilisateurs et une plus grande efficacité dans la gestion des mesures de sécurité.

Enfin, il est aussi souhaitable d'effectuer d'autres scénarios de tests avec d'autres compagnies et d'autres profils d'employés, pour tester l'efficacité du système face à d'autres profil, et pour pouvoir tirer de nouvelles conclusions, sur la durée nécessaire pour effectuer un rappel de sensibilisation par exemple, la fréquence des rappel, .etc.

BIBLIOGRAPHIE

[1] **Tremblay, J. (2020)**. Cyber-sécurité : Les 15 faits et statistiques les plus alarmants. Tophebergeur Blog. https ://www.tophebergeur.com/blog/faits-statistiques-cybersecurite/

[2] **BOUADJEMI, A., &amp ; RAHMOUNI, M. K**. Modélisation formelle pour la sécurité d'un système d'information.

[3] PECB, ISO 27001 Lead Implementer, 2013.

[4] **Harrington, D. (s. d.).** . Sécurité des données : importance, types et solutions | Varonis. Consulté le 17 janvier 2023, à l'adresse https ://www.varonis.com/fr/blog/securite-donnees.

[5] Les aspects de sécurité d'un centre de données. (2022, 20 décembre). Département TI. Consulté le 17 janvier 2023, à l'adresse https ://www.departement-ti.com/2019/11/18/les-aspects-de-securite-dun-centre-de-donnees/

[6] Comment réaliser une évaluation des risques informatiques. (2019, 3 avril). Blog de Netwrix. Consulté le 18 janvier 2023, à l'adresse https ://blog.netwrix.fr/2019/04/03/comment-realiser-une-evaluation-des-risques-informatiques/

[7] Les 10 types de cyberattaques les plus courants. (2018, 4 juillet). Blog de Netwrix. Consulté le 18 janvier 2023, à l'adresse https ://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants/

[8] **Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019)**. Strategically-motivated advanced persistent threat : Definition, process, tactics and a disinformation model of counterattack. Computers & Security,86, 402-418.

[9] Vulnérabilités : de quoi parle-t-on ?(2019, 14 mars). Consulté le 18 janvier 2023, à l'adresse https ://www.orangecyberdefense.com/fr/insights/blog/gestion-des-vulnerabilites/vulnerabilites-de-quoi-parle-t-on

[10] **Dubois, J. (2022, 9 décembre**. Les actifs informationnels. Monsieur TI. Consulté le 18 janvier 2023, à l'adresse https ://monsieurti.ca/les-actifs-informationnels/

[11] **GeeksforGeeks. (2022, 28 juin)**. Threats to Information Security. Consulté le 18 janvier 2023,à l'adresse https ://www.geeksforgeeks.org/threats-to-information-security/

[12] **Daniel, V. E. N. T. R. E. (2011)**. Cyberattaque et cyberdéfense. Lavoisier.

[13] **Triaud, E. (2022, 29 décembre)**. Les équipes en cybersécurité. secwyse.io. Consulté le 20 janvier 2023, à l'adresse https ://secwyse.io/articles/les-equipes-en-cybersecurite/

[14] Clause 7.3 : Sensibilisation à la cybersécurité – Norme ISO 27001. (2021, 16 septembre). Protectam. Consulté le 20 janvier 2023, à l'adresse https ://protectam.fr/iso-27001/clause-7-3-sensibilisation-a-la-cybersecurite/

[15]Sensibilisation à la cybersécurité : définition, importance, objectif et défis. (2023b, janvier 3). Exter. Consulté le 20 janvier 2023, à l'adresse https ://www.exter.fr/sensibilisation-a-la-cybersecurite/

[16]**Buckbee, M. (2019, 25 janvier)**. IDS et IPS : en quoi sont-ils différents ? Consulté le 22 janvier 2023, à l'adresse https ://www.varonis.com/fr/blog/ids-et-ips-en-quoi-sont-ils-differents

[17]**Buckbee, M. (2022, 6 juin)**. What is SIEM ? A Beginner's Guide. Consulté le 22 janvier 2023,à l'adresse https ://www.varonis.com/blog/what-is-siem

[18]**Kaspersky. (2021, 13 janvier)**. Ingénierie sociale - Définition. www.kaspersky.fr. Consulté le 20 janvier 2023, à l'adresse https ://www.kaspersky.fr/resource-center/definitions/what-is-social-engineering

[19]**Gill, S. (2003)**. Type d'attaques. Document soumis à la licence GNU FDL. http ://sgill. ep. profweb. qc. ca/spip/IMG/pdf/02_TypeAttaque. pdf, 37.

[20]**Royer, J. M. (2004)**. Sécuriser l'informatique de l'entreprise : enjeux, menaces, prévention et parades. Editions ENI.

[21]What is Phishing ? - Definition, Examples, and Protection. (2022, 7 novembre). SANGFOR. Consulté le 22 janvier 2023, à l'adresse https ://www.sangfor.com/blog/cybersecurity/what-is-phishing-attack

[22]Phishing : définition simple et détaillée. (2022, août 24). JobPhoning. Consulté le 22 janvier 2023, à l'adresse https ://jobphoning.com/dictionnaire/phishing

[23]**Grimmick, R. (2022, 3 juin)**. Phishing Attacks : Types, Prevention, and Examples. Consulté le 22 janvier 2023, à l'adresse https ://www.varonis.com/blog/phishing-attacks

[24]**Malwarebytes. (2019, 19 novembre)**. Ransomwares : de quoi s'agit-il et comment s'en débarrasser. Consulté le 22 janvier 2023, à l'adresse https ://fr.malwarebytes.com/ransomware/

[25]**Gonzalez, C. (2022, 3 mai)**. Top 8 Social Engineering Techniques and Howto Prevent Them [2022]. Exabeam. Consulté le 20 janvier 2023, à l'adresse https ://www.exabeam.com/information-security/top-8-social-engineering-techniques-and- how-to-prevent-them-2022/

[26]**Tounsi, W. (2019)**. Cybervigilance et confiance numérique : La cybersécurité à l'ère du Cloud et des objets connectés. ISTE Group.

[27]**Emungu, A. (2022, 23 avril)**. Social-Engineering -The-Art-of-Human-Hacking-Christopher-Hadnagy-www.indianpdf.com -Book-Novel-PDF-Download. . . studylib.net. Consulté le 20 janvier 2023, à l'adresse https ://studylib.net/doc/25798327/social-engineering–the-art-of-human-hacking-christopher-. . .

[28]**Conteh, N. Y., & Schmick, P. J. (2016)**. Cybersecurity : risks, vulnerabilities and counter-measures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31.

[29]**Copado, T. (2022, 12 décembre)**. 12 Types of Social Engineering Attacks to Look Out For. Consulté le 22 janvier 2023, à l'adresse https ://www.copado.com/devops-hub/blog/12-types-of-social-engineering-attacks-to-look-out-for

[30]Sending Profiles - API Documentation. (s. d.). Consulté le 22 février 2023, à l'adresse https ://docs.getgophish.com/api-documentation/sending-profiles

[31]Templates - API Documentation. (s. d.). Consulté le 22 février 2023, à l'adressehttps ://docs.getgophish.com/api-documentation/templates

[32]Landing Pages - API Documentation. (s. d.). Consulté le 22 février 2023, à l'adresse https ://docs.getgophish.com/api-documentation/landing-pages

[33]Users & Groups - API Documentation. (s. d.). Consulté le 22 février 2023, à l'adressehttps ://docs.getgophish.com/api-documentation/users-and-groups

[34]**De Futura, L. R. (s. d.).**Python : qu'est-ce que c'est ? Futura. Consulté le 25 avril 2023, à l'adresse https ://www.futura-sciences.com/tech/definitions/informatique-python-19349/

[35]Introduction à HTML5. (2020, 2 juillet). IONOS Digital Guide. Consulté le 25 avril 2023, à l'adresse https ://www.ionos.fr/digitalguide/sites-internet/developpement-web/html5-cest-quoi/

[36]CSS Faciles : Introduction aux feuilles de style CSS. (s. d.). Consulté le 25 avril 2023, à l'adresse http ://www.css-faciles.com/

[37]**Pierre Giraud. (2019, août 28).**Introduction au JavaScript - Pierre Giraud. Consulté le 25 avril 2023, à l'adresse https ://www.pierre-giraud.com/javascript-apprendre-coder-cours/introduction/

[38]**Dyouri, A. (s. d.).**Créer une application Web avec Flask Python. Developpez.com. Consulté le 25 avril 2023, à l'adresse https ://python.developpez.com/tutoriel/intro-flask-python3/

[39]Rédaction, L. (2019b). Bootstrap ; définition, tutoriels, astuces,pratiques.www.journaldunet.com.https ://www.journaldunet.com/web-tech/developpeur/1159810-bootstrap-definition-tutoriels-astuces-pratiques/

[40]Introduction | Vue.js. (s. d.). Consulté le 25 avril 2023, à l'adresse https ://vuejs.org/guide/introduction.html

[41]Kinsta. (2022, 26 mai). Qu'est-ce que MySQL ? Une explication simple pour les débutants. Kinsta®.Consulté le 25 avril 2023, à l'adresse https ://kinsta.com/fr/base-de-connaissances/qu-est-ce-que-mysql/

[42]Why Visual Studio Code ? (2021, 3 novembre). Consulté le 25 avril 2023, à l'adressehttps ://code.visualstudio.com/docs/editor/whyvscode

[43]Introduction - API Documentation. (s. d.). Consulté le 25 avril 2023, à l'adressehttps ://docs.getgophish.com/api-documentation/

[44]Partner of Choice in Security Awareness | Terranova Security. (2023, March 3). https ://terranovasecurity.com/

[45]Automated Security Awareness Platform | Kaspersky. (n.d.). https ://www.kaspersky.com/small-to-medium-business-security/security-awareness-platform

[46]About the Unified Modeling Language Specification Version 2.5.1. (n.d.). https ://www.omg.org/spec/UML/

[47] OVHcloud. (n.d.). OVHcloud. https ://www.ovhcloud.com/en/