

Sommaire

Table des matières

Sommaire	1
Outils Utilisés	3
Acronymes	3
Introduction	3
Présentation de l'entreprise	4
Domaine de recherche et d'innovation.....	5
Relations extérieures	5
Relations internes	5
Implantation	6
Activité du service NTIC	7
Historique de l'entreprise Sites.....	7
Organigramme de l'équipe NTIC chez Sites	8
Campagne de phishing (novembre – décembre 2023)	9
Objectifs	9
Élaboration d'un contexte	9
Mise en place du mail de phishing	10
Technologies utilisées	10
Contexte.....	10
Réalisation de l'objectif	10
Création du modèle du mail.....	10
Création de la home page.....	11
Création de la Landing Page :	11
Indices à la detection d'une fraude.....	12
Courriel suspect.....	12
Lien frauduleux	12
Mauvais logo	13
Bilan de la campagne de phishing.....	13
Envoi des mails.....	13

Statistique de la campagne	14
Bilan personnel sur la mission	14
Difficultés rencontrées	14
Compétences acquises	15
Ce que j'ai le plus aimé	16
Ce que j'ai le moins aimé	17
Mission 2 : Support technique	17
Contexte	17
Objectifs	17
Technologies utilisées :	17
Descriptif de la mission	17
Interface de GLPI	17
Gestion des tickets sur GLPI	18
Environnement AD	18
Active Directory : définition	18
Interface Active Directory	19
Mode de prise en main à distance	19
Commande pour utiliser MSRA	19
Difficultés rencontrées	20
Compétences acquises	20
Ce que j'ai le plus aimé au support	20
Ce que j'ai moins aimé au support	21
Bilan d'alternance	21
Bilan professionnel	21
Bilan technique	22
Bilan humain	22

Outils Utilisés

GLPI, Centreon, Outils Microsoft (Word, Excel, Outlook, OneDrive, etc.) 3CX, Trend Micro, Akuitéo, Gestionnaire de serveur Windows.

Acronymes

LP : Licence Professionnelle

AD : Active Directory

IP : Internet Protocol

RDP : Remote Desktop Protocol

MSRA : Microsoft Remote Assistance est l'outil de prise en main à distance développé par Microsoft

NTIC : Nouvelle Technologie de l'Information et de la Communication

ERP : Enterprise Resource Planning

CSE : Comité sociale et entreprise.

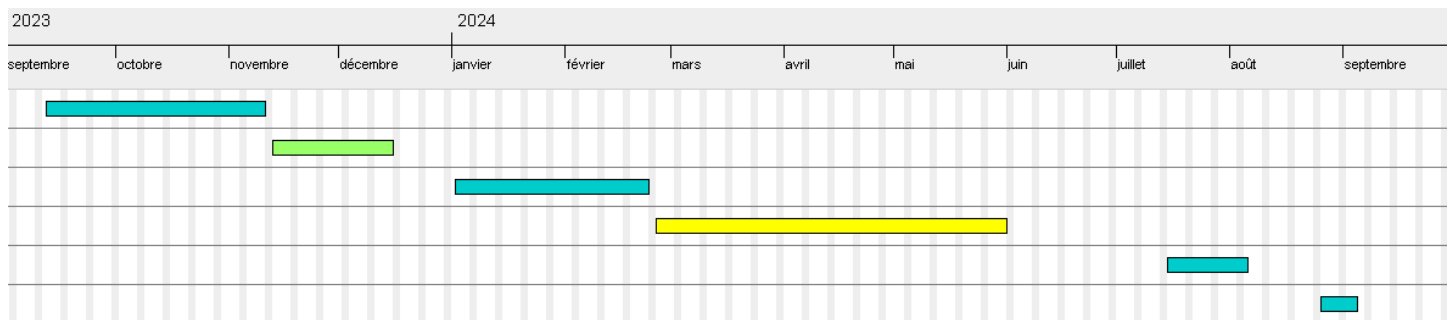
Introduction

Dans le cadre de la formation en alternance (LP Exploitation et Sécurité des Systèmes d'Informations et des Réseaux) j'ai eu la chance d'intégrer l'équipe NTIC de la société Sites en tant que technicien support et réseau. Cette intégration au sein de cette équipe m'a permis de gagner en compétence dans de nombreux domaines :

- Gestion de parc informatique (matériels, logiciels, etc.)
- Gestion des tickets d'incidents techniques
- Gestion de la communication avec les différents collaborateurs et les membres de mon équipe
- Méthode de travail en entreprise ainsi que le fonctionnement
- Rédaction de rapport

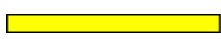
- Savoir expliquer un problème technique et mettre en place des solutions

Le diagramme de Gantt ci-dessous illustre les tâches réalisées cette année avec la répartition d'un projet, de l'activité support ainsi que la réalisation du projet tuteuré.



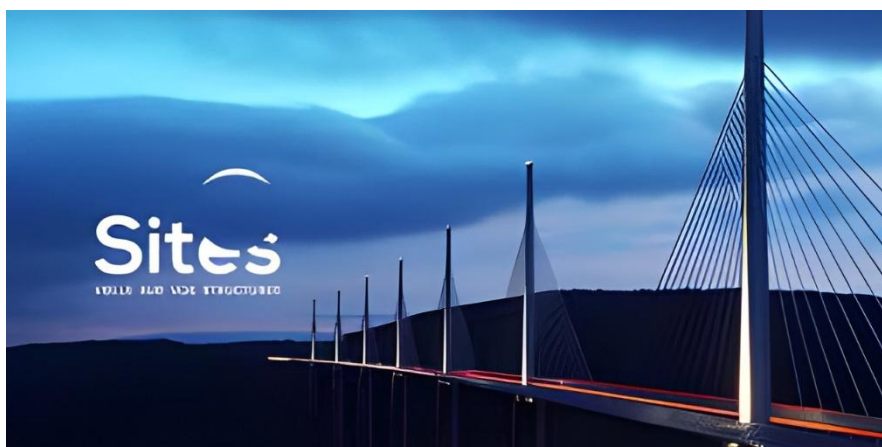
 : Support aux collaborateurs

 : Campagne de phishing

 : Projet tuteuré

Présentation de l'entreprise

Sites se spécialise dans la surveillance de santé structurelle, c'est une société d'ingénierie qui se spécialise dans plusieurs domaines comme l'instrumentation, le monitoring, l'inspection, expertise, relevés et mesures, assistance technique aux maîtres d'ouvrage.



Sites a pu se positionner comme un leader dans son domaine de diagnostic et l'auscultation des structures. Elle agit notamment dans de nombreux secteurs comme l'industrie, l'énergie nucléaire, les infrastructures et les ouvrages d'art, tout cela grâce à ses aptitudes en matière d'ingénierie.

Raison sociale	Sites
Date de création	1984
Chiffre d'affaires	48M (en 2023)
Siège social	1 Av. Edouard Belin, 92500 Rueil-Malmaison
Site internet	https://www.sites.fr/

Domaine de recherche et d'innovation

L'Entreprise Sites investit dans le développement afin d'améliorer ses méthodes de fonctionnement et les technologies utilisées, elle se démarque dans 3 domaines plus important : Instrumentation et le Monitoring (développement d'outil interne de surveillance), inspections par drones souvent utilisées pour des zones difficiles d'accès comme des barrages ou des ponts et les relevés 3D avec l'utilisation de scanner laser. En termes d'innovation côté service informatique, on cherche à rendre automatiques et plus faciles certaines tâches comme le déploiement d'application ou l'exécution des scripts

Relations extérieures

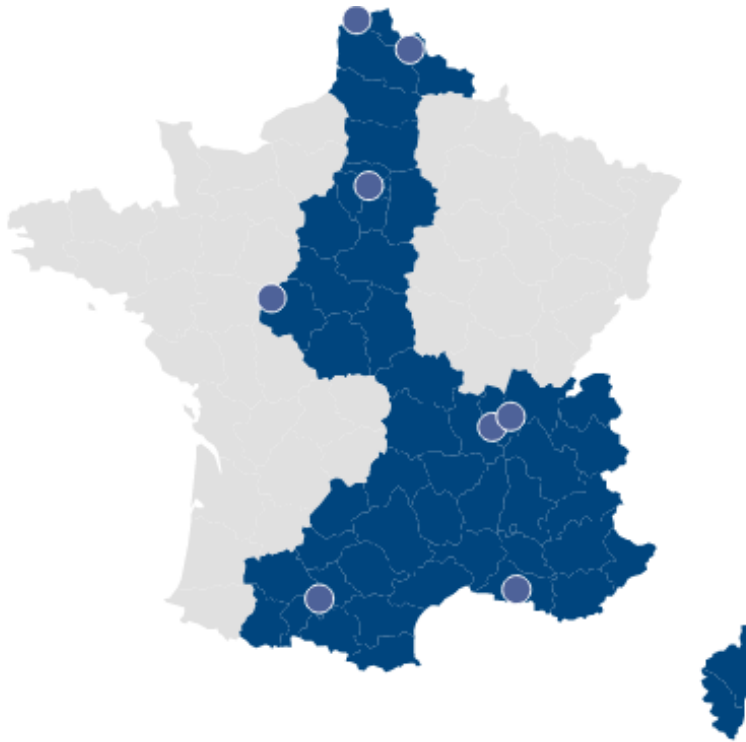
Sites collabore avec plusieurs acteurs (publics et privés) et dans de nombreux domaines. Parmi eux on retrouve : EDF, Eiffage, Grand Lyon, Viaduc de Millau, SNCF Total, Cofiroute, Le Louvre, Alstom, etc.

Relations internes

L'Entreprise est basée sur une structure collaborative et interne où plusieurs groupes différents travaillent ensemble afin d'apporter des meilleures solutions et d'améliorer l'innovation. En termes de filiales, Sites possède désormais le groupe Cornis dont le siège

social se trouve à Paris mais également Vibrattec qui est une société experte des phénomènes mécaniques, acoustiques et vibratoires.

Implantation



Sites possède un réseau d'agence sur toute la France, notamment à : Écully, Dardilly, Rueil-Malmaison (siège), Aix-en-Provence, Coquelles et Marcq-en-Barœul. Sites possède également des filiales à l'étranger notamment en Chine et en Afrique du Sud :



Activité du service NTIC

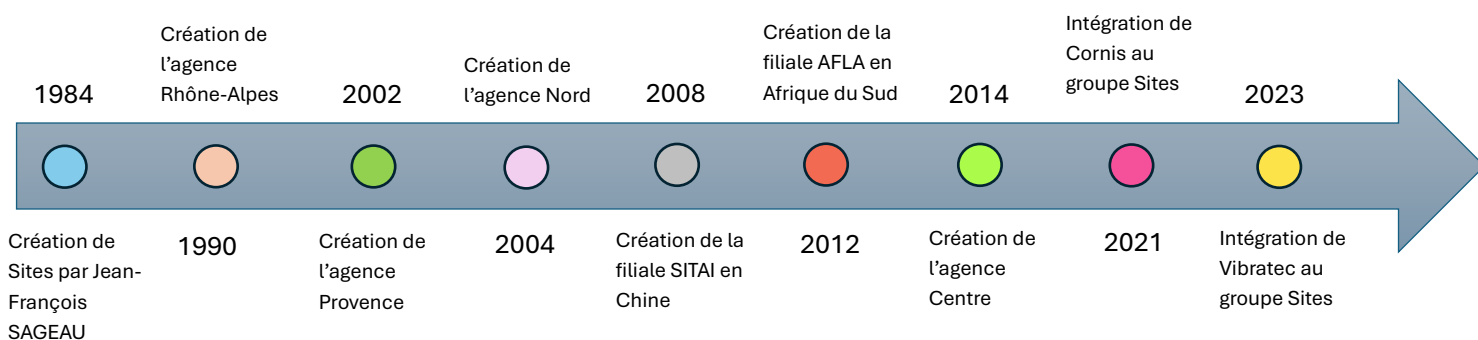
Lors de cette année d'alternance au sein de l'équipe support NTIC j'ai été amené à gérer :

- Le support et l'assistance (50%)
- La gestion du patrimoine informatique (25%)
- La maintenance et la supervision (20%)
- L'Administration (5%)

En termes de responsabilités on peut retrouver l'aspect sécurité avec la protection des données et le respect de la charte informatique, la maintenance des systèmes ; s'assurer du fonctionnement des différents systèmes que ce soient des ordinateurs, des serveurs ou d'autres équipement réseaux.

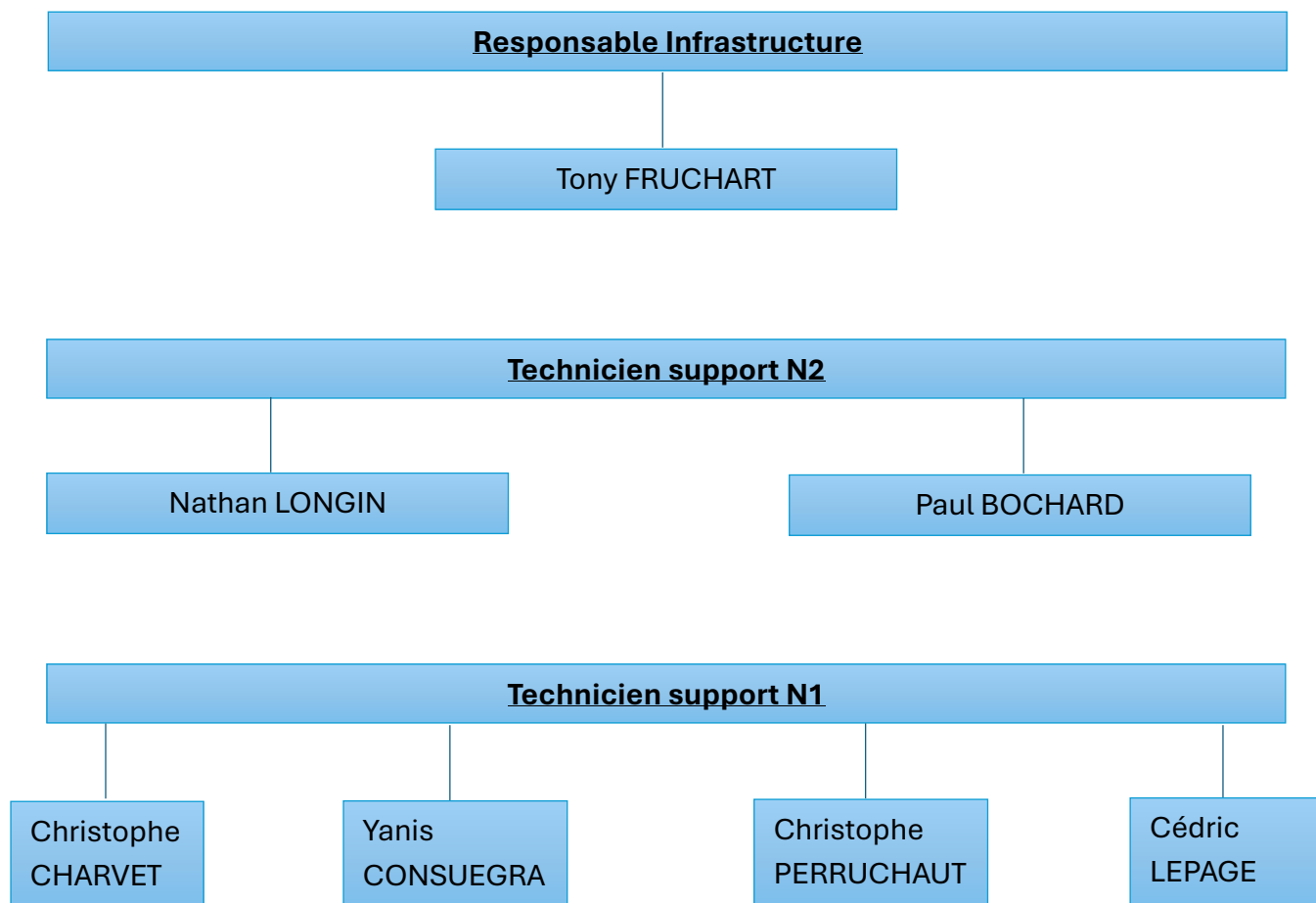
Historique de l'entreprise Sites

Cette frise chronologique met en évidence les grandes étapes liées au développement du groupe Sites depuis sa création :



Organigramme de l'équipe NTIC chez Sites

Voici un organigramme mettant en exergue les différentes personnes qui travaillent au Support NTIC :



Campagne de phishing (novembre – décembre 2023)

Objectifs

Le but de ce projet est de réaliser une campagne de phishing afin de sensibiliser le personnel de l'entreprise Sites et Vibratec en mettant en place un courriel trompeur et ainsi de récupérer les statistiques des collaborateurs en fonction de leurs actions face à cette tentative de fraude et de vérifier le niveau de maturité du personnel.

Élaboration d'un contexte

Avant de réaliser une quelconque mise en place de la campagne de phishing il faut trouver un thème qui va dépendre de plusieurs critères :

- Date à laquelle est réalisé cette campagne de phishing : dans mon cas cela peut jouer sur le contexte des fêtes de fin d'années.
- Des précédentes campagnes : l'objectif n'est pas de réaliser une campagne similaire aux précédentes afin de monter toutes les possibilités et les menaces des tentatives de phishing.
- Représentation des menaces réelles : le scénario doit être réaliste et représenter les dangers actuels.

Le thème qui sera finalement retenu est la distribution de boîtes de chocolats par le CSE pour les collaborateurs sur les périodes de fin d'années, les salariés seront donc amenés à entrer leurs informations personnelles dans l'objectif de recevoir le gain.

Mise en place du mail de phishing

Technologies utilisées



⇒ Afin de mettre en place cette campagne je vais utiliser l'outil open source qui Gophish, il est parfait pour ce projet et permet de répondre à plusieurs critères intéressants. De plus, je suis amené à utiliser du langage PowerShell afin d'importer la liste des utilisateurs depuis l'AD

Contexte

Plusieurs fois durant l'année, des campagnes de phishing internes sont réalisées sur des thèmes assez différents, l'objectif recherché est de sensibiliser les collaborateurs aux risques des attaques de phishing et donc d'analyser et de tester leurs comportements face à cette situation.

Réalisation de l'objectif

Création du modèle du mail

Maintenant que j'ai choisis et pris connaissance du sujet sur lequel va porter ma campagne il me reste plus qu'à coder un modèle de mail en langage HTML5 depuis le

logiciel Gophish, cette page sera le premier affichage vu par l'utilisateur quand il recevra le courriel dans sa boîte mail Outlook.

Au fil de cette campagne de phishing, j'ai volontairement introduit des « indices » qui permettent aux différents collaborateurs de déduire qu'il s'agit d'un courriel trompeur.

Création de la home page

Voici à quoi ressemble la page d'accueil du mail :

Le CSE vous offre une boîte de chocolats !

Bonjour à tous,

À l'occasion des fêtes de fin d'année, le CSE a le plaisir de vous offrir une boîte de chocolats à recevoir directement chez vous !

150 boîtes de la marque Lindt sont disponibles, seulement les 150 premiers formulaires seront donc pris en compte.

Vous trouverez les informations à nous retourner sur le formulaire ci-dessous **avant le 25/12/2023 à 14h00** date à laquelle les commandes seront effectuées.

ACCÉDER AU FORMULAIRE

La livraison des boîtes aura lieu entre le 28-30 décembre directement à votre domicile.



Bonne fête à tous !

[Votre CSE](#)

L'objectif recherché et la stratégie mise en place est l'urgence, le fait d'indiquer qu'il y a un nombre de boîtes de chocolats limitées peut inciter l'utilisateur à entrer ses informations rapidement.

En règle générale il s'agit d'une stratégie régulièrement mise en place par les attaquants pour inciter les utilisateurs à cliquer sur les courriels et les liens malveillants.

Création de la Landing Page :

La landing Page est la page qui s'affiche juste après avoir cliqué sur le lien permettant d'accéder au formulaire que l'on voit sur le courriel malveillant :

ACCÉDER AU FORMULAIRE

Une fois que l'utilisateur aura cliqué sur le lien, il sera amené sur une page qui va lui demander ses informations personnelles afin de recevoir la boîte de chocolat.



Nom* :

Prénom* :

Adresse postale* :

Ville* :

Téléphone* :

Email :

Pour inciter une nouvelle fois l'utilisateur, des petites étoiles rouges ont été placées volontairement afin de rendre la saisie des informations obligatoires

Indices à la detection d'une fraude

Jusqu'à la page où les utilisateurs peuvent entrer leurs informations personnelles, de nombreux indices ont été introduits volontairement afin d'affirmer qu'il pourrait s'agir d'une tentative de Phishing.

Courriel suspect

L'adresse électronique n'est pas affichée par défaut pour les mails internes, de plus celle-ci ne semble pas correspondre à l'adresse du CSE Sites.

CSE <csesites@sitesapps.fr>

Lien frauduleux

En passant sa souris sur le lien du bouton pour accéder au formulaire on peut voir qu'il semble suspect et qu'il ne redirige pas vers une adresse connue :



Le domaine « sitesapps.fr » est utilisé uniquement pour réaliser les campagnes de phishing.

Mauvais logo

Lorsque l'utilisateur se rend sur la page du formulaire, on peut voir que le logo ne correspond pas à celui du CSE Sites :



Faux logo
récupéré
sur internet



Vrai logo CSE Sites

Bilan de la campagne de phishing

Envoi des mails

Comme énoncé précédemment, Gophish permet de suivre en temps réel plusieurs informations et notamment les mails envoyés au fil du temps, cela permet de vérifier qu'il n'y a pas d'erreur dans l'envoi et de contrôler que tous collaborateurs ont bien reçu le courriel.

Campaign Timeline



Statistique de la campagne

Gophish permet évidemment d'afficher les résultats de la campagne et donc d'analyser le niveau de maturité de la société concernant les attaques de Phishing. Il va retenir les personnes ayant ouvert le mail, les collaborateurs qui ont cliqués sur le lien et ceux qui ont transmis des données. Il s'agit ici du résultat final de cette mission qui nous permet d'affirmer ou non notre niveau de maturité dans le domaine des attaques phishing



Bilan personnel sur la mission

Difficultés rencontrées

- Dans un premier temps il fallait trouver un thème qui correspond et qui n'a pas déjà été réalisé, le choix été assez difficile car l'objectif été de demandé des données personnelles à l'utilisateur, il fallait donc faire le lien entre le thème et l'objectif.

- La première difficulté a été de reprendre la programmation orientée web, en effet j'ai été amené à coder certaines parties de la campagne de phishing en HTML5. C'est un élément que je redoutais dès le départ car je n'avais pas utilisé ce langage depuis plusieurs années, cela a été un léger frein dès la partie conception du courriel, cependant les ressources sur le web m'ont bien aidé sur plusieurs éléments.
- L'objectif était également de mettre en évidence des indices qui pourraient laisser penser à une attaque de phishing, cela a été assez difficile dans un premier temps car certains indices sont à mon sens assez évidents. Il fallait donc trouver une sorte d'équilibre car tous le monde ne possède pas la même approche sur le sujet
- Le respect des délais est une contrainte assez forte surtout avec le thème choisi pour cette campagne car cela devait être réalisé avant la semaine de vacances d'hiver et donc avant les fêtes de fin d'années.
- Côté technique et utilisation du logiciel, l'outil Gophish ne présente pas de solutions automatiques en ce qui concerne les mails signalés comme du phishing par les utilisateurs, cela nécessite une intervention manuelle sur l'interface des utilisateurs. Cela peut s'avérer problématique dans le cas où une campagne touche un plus grand nombre d'utilisateurs et par conséquent un taux de reporting plus élevé.

Compétences acquises

Lors de la réalisation de ce projet, j'ai acquis de nombreuses compétences utiles :

- La réalisation de ce type de projet développe la créativité dans le sens où il faut trouver un thème à mettre en place selon plusieurs critères. Ce projet m'a poussé

à chercher des idées à introduire dans cette campagne pour la rendre plus crédible aux yeux des utilisateurs.

- J'ai pu notamment développer des compétences en matière de sécurité informatique en apprenant toutes les méthodes liées aux attaques et aux détections de phishing. De plus, j'ai révisé le langage HTML5 dont je n'avais pas spécialement de grande compétence sur ce sujet, cela m'a permis de m'améliorer en développement et sécurité web
- Ce projet m'a également appris le respect des délais, en effet dans ce type de mission, il n'est pas envisageable de retarder l'instant où la campagne de phishing est censé être envoyée aux différents utilisateurs. Cela montre l'importance des délais et de la gestion du temps dans un projet.

Ce que j'ai le plus aimé

- J'ai beaucoup aimé le mélange entre les domaines du développement web et de la sécurité informatique, cela m'a permis de m'améliorer dans plusieurs disciplines et de démontrer que le développement est lié à la cybersécurité.
- Durant la formation en licence, nous avons été amenés à suivre des cours en sécurité informatique et nous avons abordé certaines notions concernant le thème du phishing, j'ai donc pu m'inspirer des éléments vus durant ma formation pour ma mission.
- Enfin, j'ai apprécié le côté documentation et explication de la campagne pour les utilisateurs, c'est-à-dire synthétiser dans un document tous les éléments qui permettent d'identifier qu'il s'agit, les bonnes actions à mettre en œuvre, etc.

Ce que j'ai le moins aimé

- Cette mission a plus d'aspects positif que négatif, malgré cela j'ai moins apprécié le fait que le rendu final est une date précise car cela pouvait parfois m'amener à aller plus vite sur certaines parties de la mission et me limiter dans les fonctionnalités à ajouter pour éviter d'accumuler du retard.

Mission 2 : Support technique

Contexte

- Le support technique représente la grande partie de mon activité durant mon année d'alternance chez Sites. En effet, tous au long de l'année j'ai répondu à des demandes et des incidents très variés pour les collaborateurs.

Objectifs

- L'objectif du support informatique est de résoudre les incidents utilisateurs et de traiter les demandes.

Technologies utilisées :

GLPI : Outils de ticketing qui me permet de traiter les tickets utilisateurs

Environnement Active Directory : Outil de gestion qui me permet principalement de gérer les utilisateurs, les ordinateurs et les groupes de sécurité.

MSRA : système de prise en main à distance développé par Microsoft qui aide à la résolution des incidents et à la réponse des demandes utilisateurs.

Descriptif de la mission

Interface de GLPI

[AJOUTER SCREEN GLPI]

Gestion des tickets sur GLPI

L'outil de gestion de ticket GLPI m'aide à traiter les incidents et les demandes des différents collaborateurs, la plupart du temps, les tickets concernent :

- Préparation d'un poste informatique
- Demande d'installation de logiciel
- Demande de droits d'accès et récupération de mot de passe
- Incident divers sur les logiciels internes et externes

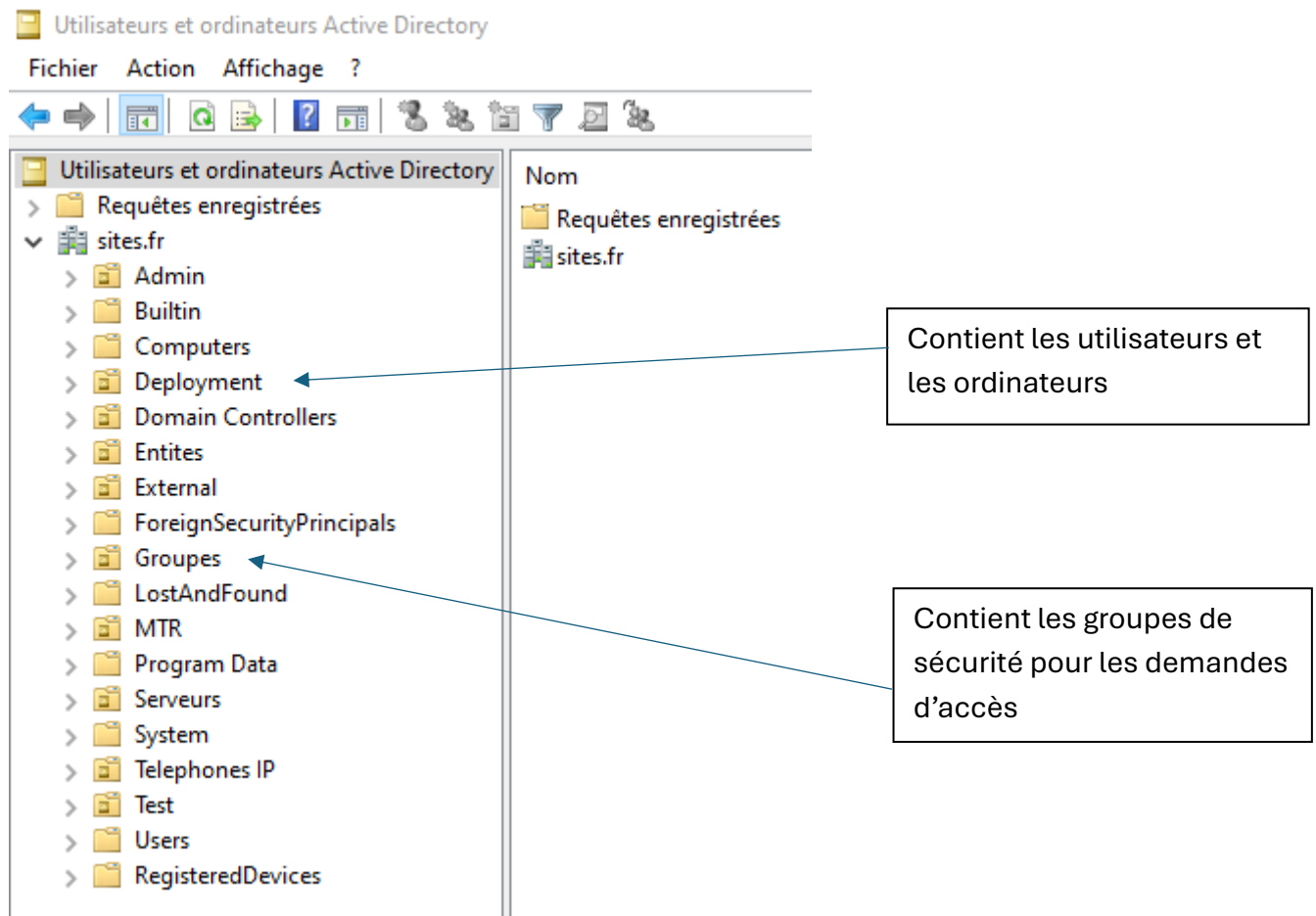
Pour cela GLPI assure le suivi et les démarches que les techniciens utilisent pour répondre aux demandes et aux incidents. Par ailleurs, GLPI contient toutes les informations des postes informatiques, des téléphones, des logiciels et des utilisateurs du système.

Environnement AD

Active Directory : définition

L'environnement Active Directory me permet de gérer les utilisateurs, les ordinateurs et les groupes. Il est utilisé pour la résolution d'un grand nombre de ticket comme les changements de mot de passe, la préparation d'ordinateur, les demandes d'accès, etc.

Interface Active Directory



Mode de prise en main à distance

J'utilise l'outil Microsoft MSRA afin de prendre le contrôle sur les postes utilisateurs pour la résolution de problème et les demandes d'installations, parfois certaines actions peuvent demander plus de privilèges, dans ce cas l'outil RDP (Remote Desktop Protocol) est utilisé pour avoir les droits administrateurs sur la machine.

Commande pour utiliser MSRA

[SCREEN DE MSRA]

Difficultés rencontrées

- La difficulté la plus importante que j'ai rencontrée la priorisation de certains tickets par rapport à d'autre, il était parfois difficile de choisir quelle demande est la plus importante par rapport à une autre.
- Lors du début de l'alternance j'étais assez hésitant lors des appels car je n'avais pas vraiment cette habitude, au fil du temps tout cela s'est amélioré.
- Au départ, j'avais beaucoup de difficultés à retenir le nom des groupes et le nom des collaborateurs mais aussi certaines règles concernant les validations avant d'agir sur un ticket.

Compétences acquises

- Dans un premier temps, l'activité au support m'a permis de développer mes compétences en informatique de manière générale et d'élargir mes capacités. De plus cela m'aide à résoudre certains problèmes informatiques bien plus rapidement.
- Certains tickets nécessitent parfois une réflexion profonde et des recherches plus poussées avant la réalisation, cela a donc amélioré mon niveau en recherche de solution et d'analyse de problématique.
- Le support m'a également permis d'interagir avec de nombreux collaborateurs et par conséquent cela amélioré mon expression orale, ma façon de m'exprimer.

Ce que j'ai le plus aimé au support

- Lors du traitement d'incident technique, j'ai beaucoup aimé faire de la recherche afin de parvenir à résoudre le problème.

- J'ai aimé le côté pédagogique lorsqu'il fallait expliquer aux différents collaborateurs comment le problème a pu être résolu et qu'elles sont les démarches à suivre si l'incident se reproduit.
- Enfin, j'ai apprécié l'aspect évolutif du travail, c'est-à-dire utiliser des nouvelles méthodes pour répondre aux demandes et aux incidents. Cela m'a obligé à m'adapter à de nouvelles technologies et à changer ma manière de travailler sur certaines demandes.

Ce que j'ai moins aimé au support

- Je ne retiens pas spécialement d'aspect négatif au support informatique chez Sites, cependant j'ai un peu moins pris de plaisir à résoudre des incidents sur des logiciels assez anciens avec très peu de documentation.

Bilan d'alternance

Bilan professionnel

Cette année d'alternance au sein de l'entreprise Sites restera une très belle expérience professionnelle et un très bon souvenir, j'ai pu acquérir beaucoup d'expériences dans plusieurs domaines que ce soit humain, professionnel et technique. J'ai eu la possibilité de mettre en œuvre mes différentes compétences en informatique et à participer à la réalisation des tâches d'un véritable salarié. J'ai par ailleurs aimé l'importance qui m'a été accordée pendant cette année d'alternance car cela a joué un rôle important dans l'apprentissage et l'enrichissement de mes compétences.

Le fait d'avoir suivi une formation en alternance durant une année complète m'a permis de m'investir sur un projet à long terme car jusqu'à présent je n'avais effectué que des stages de plusieurs mois. C'est pour cette raison que je recommande fortement l'année d'alternance afin d'acquérir plus d'expérience et de consolider ses différentes compétences.

Bilan technique

L'année d'alternance aura été très enrichissante sur le plan technique que se soit dans le domaine du réseau, en sécurité informatique ou d'informatique en général. Tous cela m'a permis d'enrichir mes connaissances et de les mettre en pratique lors des traitements des demandes et des incidents pour les collaborateurs. Lorsque j'ai postulé chez Sites, j'ai su directement que le poste correspond à mes attentes et qu'il est lié au domaine dans lequel je souhaite poursuivre.

Grâce à cette année d'alternance, j'ai pu approfondir mes capacités sur les nombreux outils informatiques qui sont mis en place sur le système comme la supervision, le logiciel de ticketing, les différents services Windows (MDT, WSUS, etc.) et tous les autres logiciels utiles.

J'ai pu améliorer mes capacités dans tous ce qui est lié à la recherche et à la résolution de problèmes et des incidents pour les utilisateurs. De plus, j'ai également eu la chance d'avoir plusieurs projets enrichissants ou j'ai pu m'inspirer des enseignements pour mettre en œuvre certaines notions.

Bilan humain

Cette année d'alternance m'a également apporté de l'expérience dans le domaine de la communication et du relationnel avec les autres salariés. J'ai rapidement trouvé ma place au sein de l'équipe NTIC et même avec les autres membres de l'agence. Ce côté relationnel m'a permis d'en savoir plus sur les autres collaborateurs et sur le fonctionnement de l'entreprise de manière général. Enfin, j'ai également pu travailler sur certains points qu'il me reste encore à améliorer.