Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Installation de postes sécurisés, rackage de serveurs, accès URL et veille technologique chez Synexie

Dorian SAINT-MARTIN

Synexie

Responsable entreprise : Basile LHEUREUX

Responsable académique : Jean-Luc DAMOISEAUX

2023

Table des matières

1 Introduction 5
2 Installation complète d'un poste sécurisé 6
2.1 Contexte client 6
2.2 Mise en place de l'installation 6
2.2.1 Vérifier la conformité de l'équipement 6
2.2.2 Récupération de la procédure dans la base de connaissance interne à Synexie 6
2.3 Ajout de l'utilisateur sur l'AD, Active Directory 6
2.3.1 Création de l'utilisateur 6
2.3.2 Les actions des GPOs ,Group Object Policy 8
2.3.3 Assignation des licences 10
2.4 Mise en place des utilisateurs sur le poste 11
2.4.1 Création du premier compte temporaire 11
2.4.2 Jonction au domaine 11
2.4.3 Activation du compte "Administrateur" 11
2.4.4 Ouverture de la session de l'utilisateur final 11
2.5 Mise à jour des composants principaux 11
2.5.1 Mise à jour de l'OS et du BIOS via Dell Update 11
2.6 Installation des logiciels professionnels 12
2.6.1 Installation du client VPN SSL par Stormshield 12
2.6.2 Configuration d'Office 365 12
2.7 Installation des logiciels sécurisants 12
2.7.1 Installation de Cryhod par Prim'X 12
2.7.2 Installation de ZoneCentral par Prim'x 14
2.7.3 Installation de l'anti-virus Trend Micro Apex One 15
2.7.4 Installation de l'agent de supervision N-Able pour Synexie 15
2.7.5 Configuration de l'outil de sauvegarde cloud OneDrive 16
2.7.6 Filtrage Vade for Office 365 16
2.8 Finalisation de la commande 16
2.8.1 Contrôle qualité 16
2.8.2 Réemballage 16
2.9 Problème rencontré 16
3 Rackage de serveur 17
3.1 Contexte client 17
3.2 Mission 17
3.3 Résultats 18
4 Support : Rétablir l'accès à une URL 19
4.1 Problématique 19
4.2 Cause 19
4.3 Solution 19
5 Veille technologique : comparaison de logiciels de supervision 20
5.1 Problématique et objectif 20
5.2 Etude préliminaire 20
5.2.1 Prise d'information 20
5.2.2 Mise en forme des recherches et présentation 21
5.3 Définitions des objectifs 22
5.3.1 Mise en forme 22
5.4 Décision 23
6 Conclusion 25
7 Remerciements 27
8 Glossaire 29

1 Introduction

Ce rapport de stage témoigne de mon expérience au sein de Synexie où j'ai eu l'opportunité d'acquérir de nouvelles compétences dans les domaines de l'IT, Information Technology, et de la Cybersécurité. Créé en 2003 par Serge Nicod, Synexie est aujourd'hui un acteur reconnu à l'échelle régionale pour son rapport client chaleureux et son service de qualité. Celle-ci est principalement une entreprise d'intégrateur. Ses missions sont la mise en place de SI, Système d'Information, le maintien en condition opérationnel, le développement et occasionnellement l'audit. Elle est aussi fournisseur de matériel informatique.

La société s'organise en 3 pôles : tout d'abord, le pôle commercial, qui, comme son nom l'indique, est dédié à toute la partie vente et relation client. Ce sont eux qui prospectent et proposent des solutions aux futurs clients. Pour une solution d'infrastructure, le deuxième pôle entre en jeu, c'est la partie ITCC, Information Technology Certification Council. C'est celui-ci que j'ai intégré, ce sont tous les techniciens et ingénieurs qui vont mettre en place et maintenir la partie technique du réseau. Enfin, si le client a besoin d'une solution de développement, Synexie possède un pôle dédié aux développeurs.

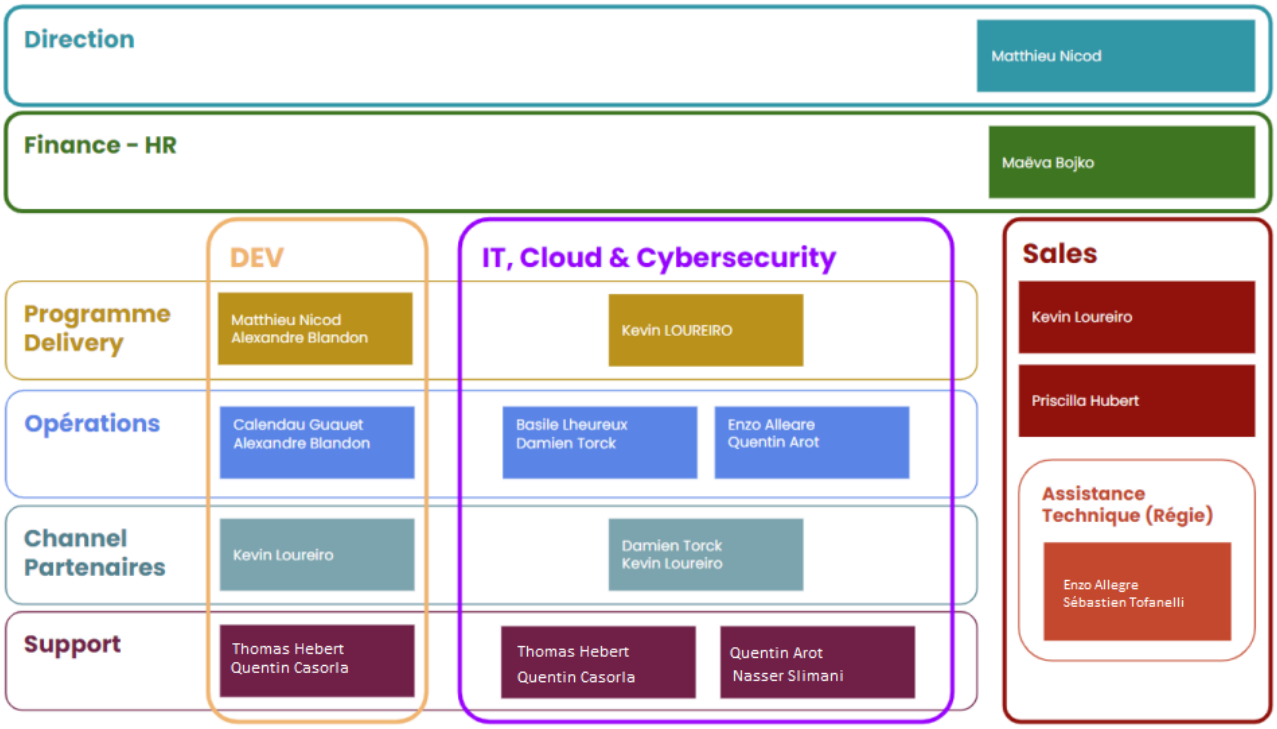

Figure 1 : Organigramme de Synexie

Avant mon arrivée chez Synexie, mes objectifs principaux étaient de découvrir le monde professionnel tout en élargissant mes qualifications. Pour atteindre cet objectif, j'ai notamment eu la chance d'observer et de participer à chaque étape de la vie du SI d'une entreprise. Cela inclut : la mise en place, la modification, la migration ainsi que l'élargissement. Et tout cela sur l'environnement le plus repandu : Windows.

J'ai structuré mon rapport de la manière suivante : dans une première partie, qui sera la plus longue, je décrirais comment j'ai pu configurer de nouveaux postes pour une entreprise nécessitant le plus haut niveau de sécurité. Ensuite, j'exposerais d'autres tâches plus spécifiques : rackage de serveur, rétablissement d'une URL ainsi que de la veille technologique portant sur de la supervision.

2 Installation complète d'un poste sécurisé

2.1 Contexte client

Notre client est une startup française innovant dans le domaine de l'aérospatiale. Fêtant tout juste sa première année, l'entreprise compte déjà entre 20 et 30 salariés. L'entreprise opère donc dans un milieu à haute plus-value militaire, et travaille déjà en collaboration avec l'industrie de haute technologie militaire française. Pour ces raisons à la fois économique, stratégique et militaire, le SI doit être le plus robuste possible tout en permettant une utilisation simple pour les salariés.

Pour répondre aux impératifs de sécurités et aux potentielles mauvaises pratiques des utilisateurs, chaque maillon de la chaine de sécurité se doit d'être absolument fiable. Pour la sécurisation de l'entreprise, nous utilisons les solutions suivantes : Cryhod, Zone Centrale, Trend Micro Apex One et Vade Secure. Aussi, il faut retenir que cette liste ne couvre pas toutes les mesures de sécurité du SI, ici n'apparaissent que celles relatives aux postes utilisateur.

La sélection de ces solutions a été établie en prenant en compte les certifications de l'ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information. En effet, celle-ci émet régulièrement des avis et des tests sur les nouvelles solutions dans le but d'améliorer au maximum la sureté des entreprises françaises face aux attaques pirates et gouvernementales.

Cette volonté de sécurisation doit nécessairement se prolonger durant la phase d'installation des postes.

2.2 Mise en place de l'installation

2.2.1 Vérifier la conformité de l'équipement

Avant toute manipulation, il est primordial de vérifier si l'équipement livré par notre fournisseur est en parfait état de marche et complet, si ce n'est pas le cas, nous devons faire un retour constructeur. La réputation de Synexie peut vite être ternie si le client reçoit un équipement détérioré. Cette vérification élémentaire est donc nécessaire.

2.2.2 Récupération de la procédure dans la base de connaissance interne à Synexie

Chez Synexie, il y a principalement deux bases de connaissance, tout d'abord, il y a le Notion. Cette première base de connaissance est générale et est basée sur différentes thématiques par exemple, on peut y retrouver un dossier "Stormshield" dans lequel il y a la procédure permettant de mettre en place un VPN SSL, Virtual Private Network with Secure Sockets Layer. La deuxième base s'appuie sur le client. C'est celle-ci qui va nous intéresser. Nous avons en effet un dossier client, chiffré, contenant les procédures permettant de maintenir ou de réparer le SI en cas de panne. Le client a lui aussi accès à ces procédures. Ce partage peut permettre au client de facilement s'autodiagnostiquer, en particulier s'il dispose d'un administrateur système.

Cette documentation est rédigée par la première personne effectuant la manipulation. Cela permet de capitaliser pleinement sur les nouvelles compétences d'un membre de l'équipe. Pour cette manipulation, je vais suivre la procédure "PROC-PC-001 - Mise en service nouveau PC".

2.3 Ajout de l'utilisateur sur l'AD, Active Directory

2.3.1 Création de l'utilisateur

Avant de commencer l'installation, nous allons devoir créer notre nouvel utilisateur sur l'AD, Active Directory. Pour cela, nous devons nous connecter sur la machine virtuelle dédiée.

Une fois connecté, nous ouvrons l'application "Utilisateurs et ordinateurs de l'Active Directory". Cette application va nous permettre de créer notre utilisateur et de lui assigner des politiques.

Pour créer l'utilisateur, nous cliquons sur "Nouvel utilisateur". Puis nous entrons ses informations. Cela inclut : son Nom, prénom, adresse mail et mot de passe.

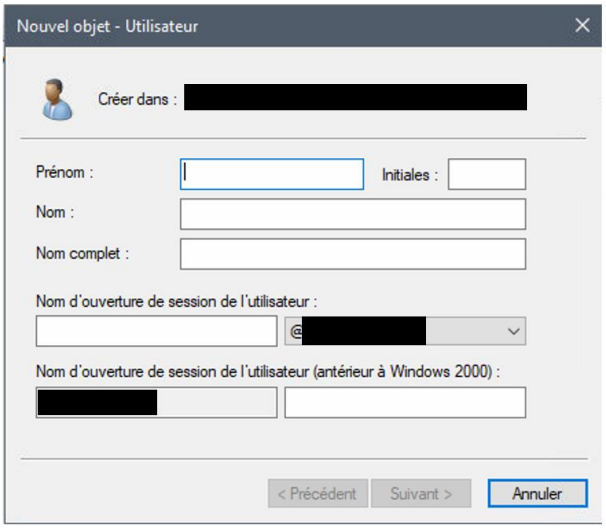

Figure 2 : Menu de création d'un utilisateur sur l'AD

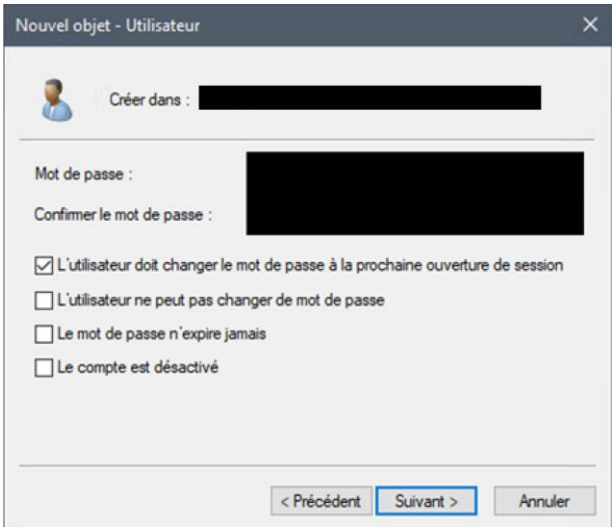

Figure 3 : Création et configuration du mot de passe par défaut

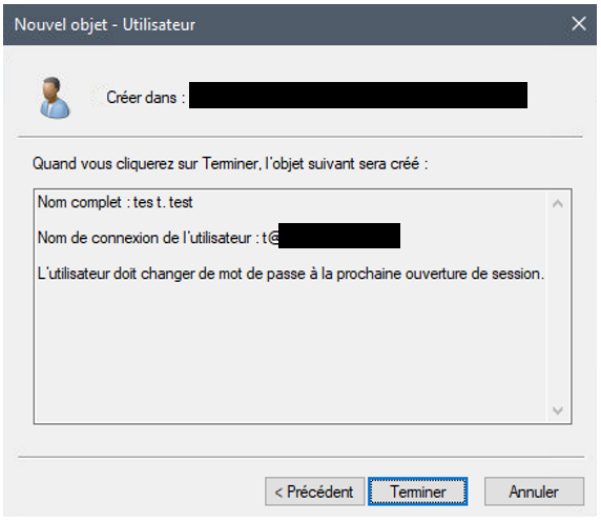

Figure 4 : Panneau récapitulatif du nouvel utilisateur

Une fois l'utilisateur créé, nous devons mettre son ordinateur dans les groupes Cryhod et Zone Central, qui permettront le paramétrage automatique de ses logiciels. En plus de cela, la création de l'utilisateur va faire remonter le profil sur le LDAP, Lightweight Directory Access Protocol, qui créera automatiquement un compte Microsoft 365 avec les informations fournies. De plus, les firewalls étant synchronisés avec le LDAP, le profil VPN sera lui aussi automatiquement créé.

2.3.2 Les actions des GPOs ,Group Object Policy

En plus de cette synchronisation, l'AD va avoir de réelles conséquences sur les utilisateurs et leurs postes. En effet, l'active directory est enfaite un serveur dédié à la configuration des postes, il peut donc avoir émettre des changements applicatifs, matériels ou du système d'exploitation.

Dans notre cas, les GPOs permettent de préconfigurer les logiciels Cryhod et Prim'x avec l'objectif d'atteindre une "cible" de sécurité. Ceci a pour but de sécuriser de manière uniforme tout un parc informatique le plus simplement et fiablement possible.

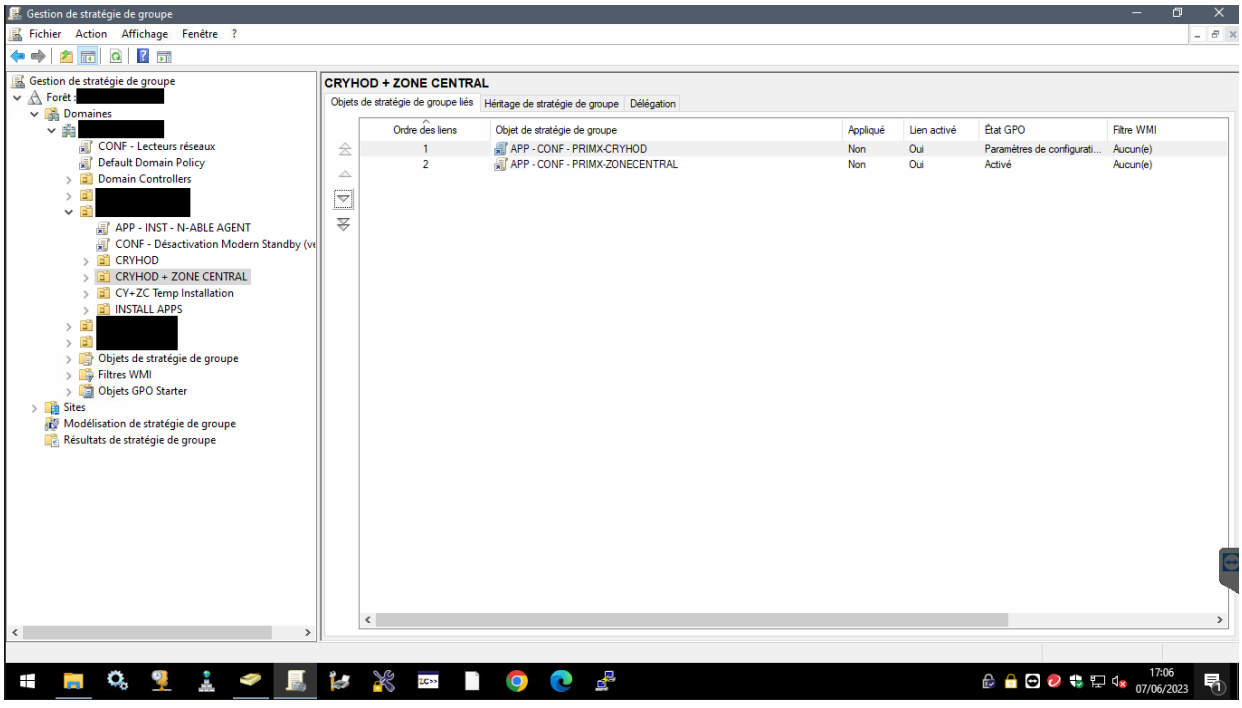

Figure 5 : Affichage des actions réalisées par la GPO "CRYHOD+ZONE CENTRAL"

Aussi, les GPOs permettent de modifier des paramètres système, dans notre cas, elles permettent d'ajouter les différentes imprimantes de l'entreprise et d'ajouter les lecteurs réseau permettant d'accéder aux données partagées.

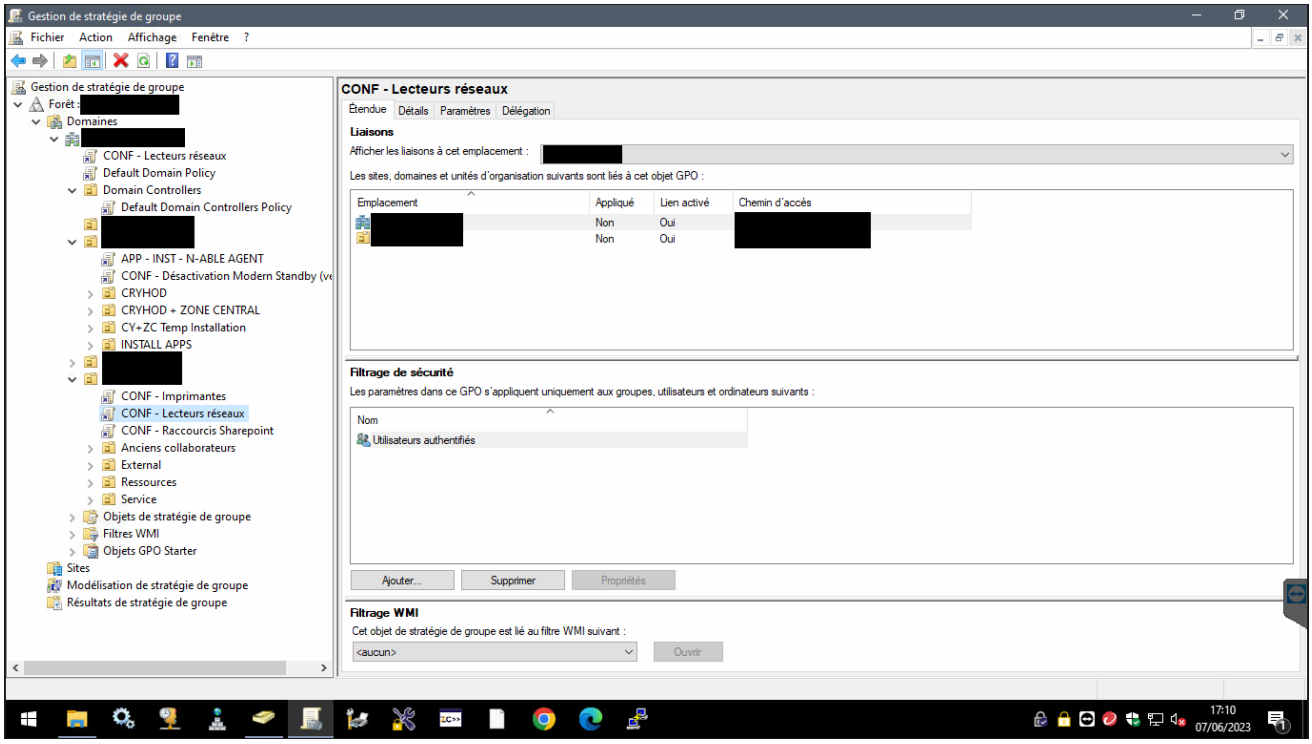

Figure 6 : Affichage de l'étendue de la GPO "Lecteurs réseaux"

Pour finir, les GPOs peuvent aussi avoir un impact sur l'environnement de l'utilisateur. On peut par exemple imaginer un changement visuel comme un fond d'écran d'entreprise. Ici, elles permettent d'ajouter les Sharepoints en raccourci pour faciliter le travail des utilisateurs.

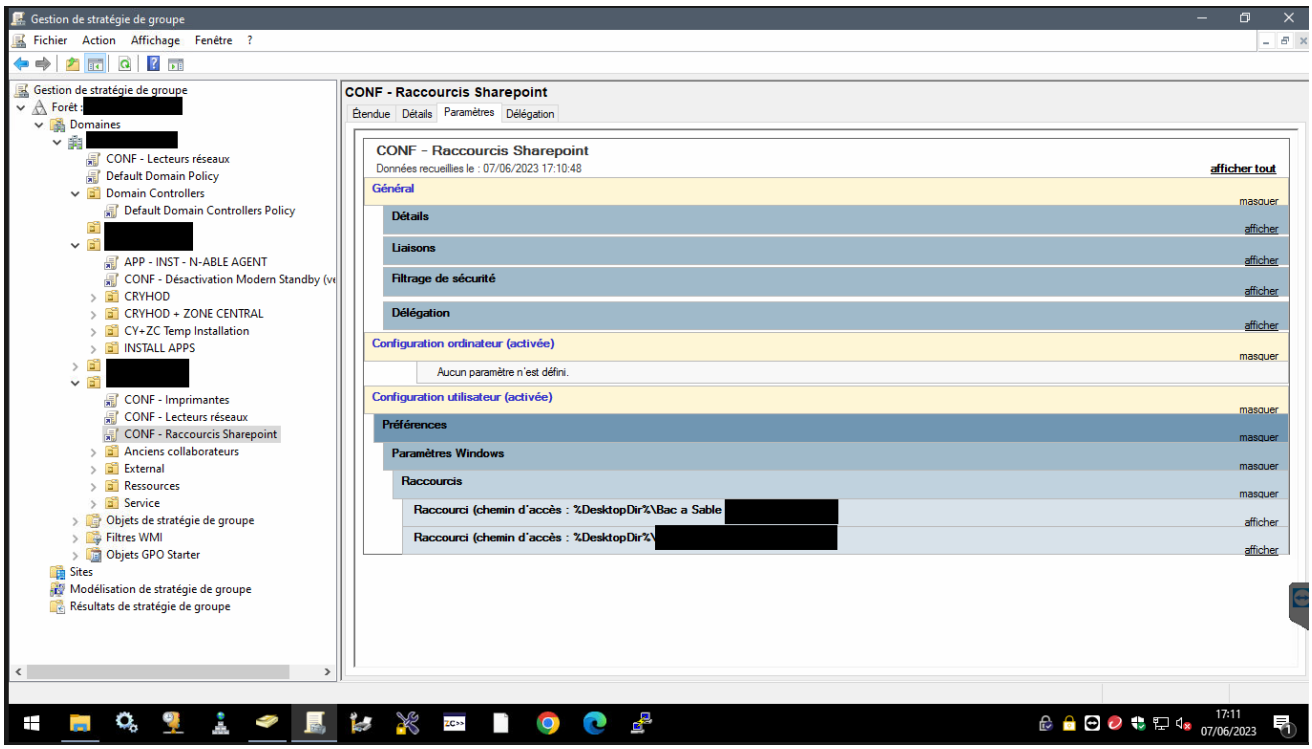

Figure 7 : Affichage des actions de la GPO "Raccourcis SharePoint"

2.3.3 Assignation des licences

Après avoir créé notre utilisateur et avoir patienté le temps que tout se synchronise, nous devons assigner la licence Microsoft pour permettre à l'utilisateur d'utiliser les produits Microsoft.
Pour cela, nous devons nous connecter à la console administrateur via le portail de Microsoft.

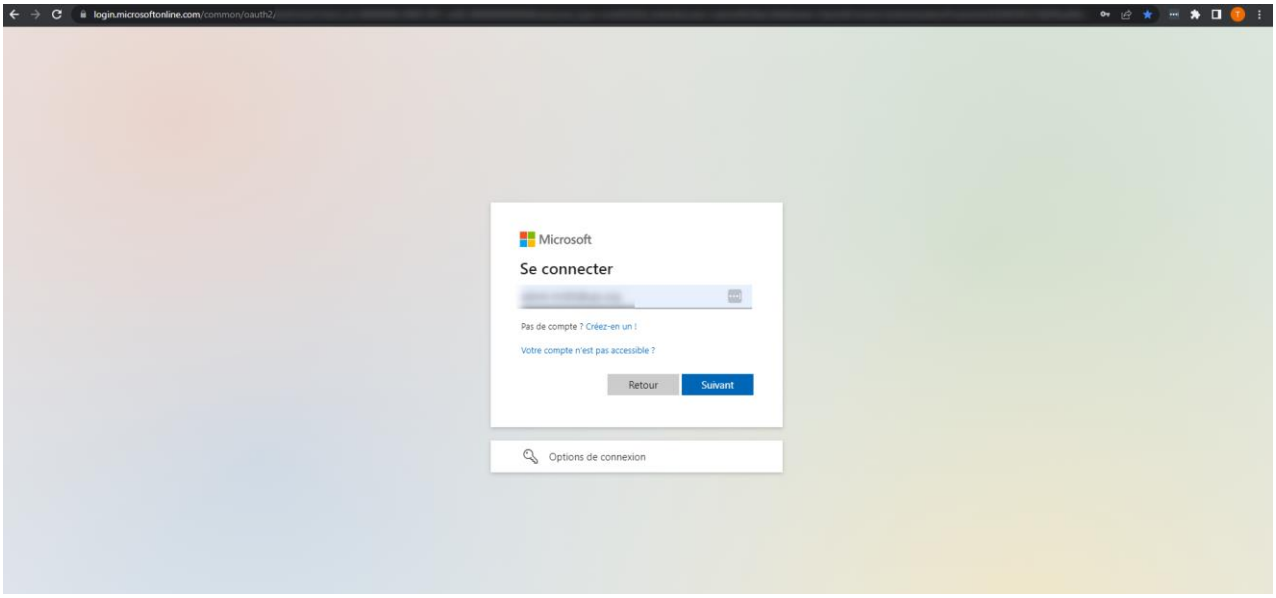

Figure 8 : Page de connexion au tenant Azure

Ensuite, nous nous rendons dans la catégorie 'Utilisateurs actifs', nous cherchons notre sujet puis nous lui assignons la licence adéquate.

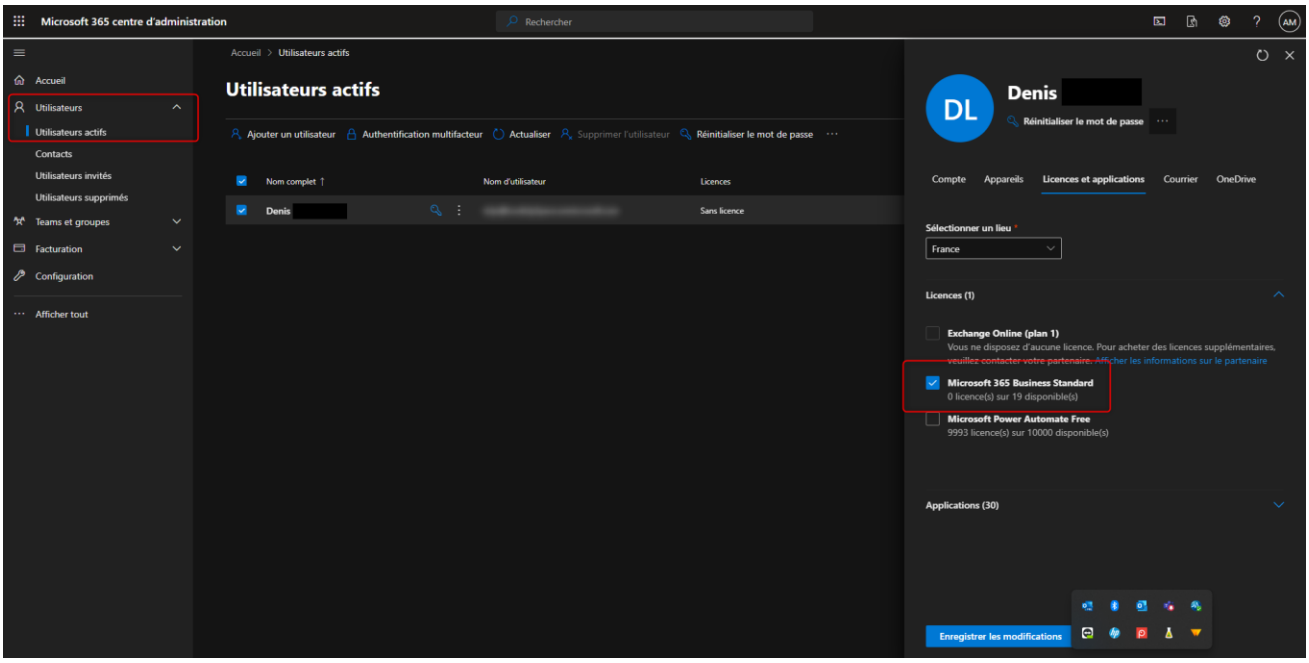

Figure 9 : Interface permettant d'affecter les licences aux utilisateurs

Notre utilisateur a maintenant accès aux logiciels Microsoft inclus dans la licence.

2.4 Mise en place des utilisateurs sur le poste

2.4.1 Création du premier compte temporaire

Pour débuter l'installation du poste, nous allons initier une installation classique de Windows. Un premier point important est de définir ce PC en tant que poste professionnel. Cela va nous donner la possibilité de joindre le PC à un domaine. Une autre étape importante est lors du nommage du PC. Pour garder un suivi du parc, il est vital d'être capable de nommer et différencier chaque poste. Pour cela, une nomenclature est définie par l'inventaire et doit être suivie à la lettre. Lorsqu'arrive l'étape de la création de l'utilisateur, on crée un utilisateur qui sera supprimé par la suite. Malgré cela, il est important de conserver l'identifiant et le mot de passe pour la suite de l'installation.

2.4.2 Jonction au domaine

Une étape primordiale consiste à joindre le PC au domaine. Pour cela, on va se rendre dans la catégorie "A propos" dans les paramètres, puis on clique sur "Renommer ce PC (avancé)". Là, on va cliquer sur "Modifier" dans la catégorie nom du poste et domaine. Ensuite, on entre le DNS, Domain Name Service, de l'AD et on se connecte à un compte. Après un redémarrage, on peut se connecter à un compte administrateur du domaine.

2.4.3 Activation du compte "Administrateur"

Une fois le PC lié au domaine, lorsque l'on va essayer de s'identifier sur l'écran d'accueil Windows, le PC va systématiquement tenter de s'y connecter via l'AD. Donc il est impossible de se connecter à un compte local. Pour lutter contre cela, deux options s'offrent à nous. La première est d'ajouter ".\" avant notre login. Cela force l'authentification en local. La seconde option, est celle que nous allons mettre en place consiste à utiliser le compte prédéfini "Administrateur". Ce compte est préétabli dans toutes les machines Windows. Ce compte a la particularité de posséder les droits administrateur d'office. En plus de cela, lorsque l'on tape "Administrateur". Sur la page d'accueil, Windows comprend automatiquement que l'on souhaite se connecter à l'administrateur local, autrement dit, "Administrateur" revient à ".\Administrateur". Pour des raisons évidentes de sécurité, cet utilisateur, bien que présent, est par défaut désactivé, nous allons donc procéder à son activation.

Pour activer le profile administrateur, il faut d'abord ouvrir le menu d'exécution en utilisant le raccourci Windows+R, ensuite entrer "lusrmgr.msc". Cette action va nous permettre d'ouvrir le panneau de configuration des utilisateurs locaux. Une fois celui-ci ouvert, ouvrir la catégorie "Utilisateurs", cliquer sur "Administrateur", mettre le mot de passe prédéfini, puis décocher "Le compte est désactivé".

2.4.4 Ouverture de la session de l'utilisateur final

Enfin, ouvrir la session de l'utilisateur final. Une pratique qui nous facilitera l'installation consiste à mettre cet utilisateur en administrateur sur la machine. Bien sûr, pour éviter tout problème ultérieur, il faut repasser le profil en tant qu'utilisateur standard à la fin de l'installation.

2.5 Mise à jour des composants principaux

2.5.1 Mise à jour de l'OS et du BIOS via Dell Update

Aujourd'hui nous le savons, utiliser du matériel à jour est absolument vital. C'est pourquoi, une étape consiste simplement à mettre à jour les composants bas du PC. Cela inclue l'OS, Operating System, ainsi que le BIOS, Basic Input/Output System. Dans le cas présent, les postes tournent sur Windows. Nous allons donc nous rendre dans les paramètres, puis mettre à jour rechercher les mises à jour. Ensuite, nous nous rendons sur Dell Update. Ce logiciel est livré avec le poste, il est donc propriétaire au matériel Dell. Ce logiciel permet de mettre facilement à jour le BIOS ainsi que tous les

drivers du poste. Durant le téléchargement et l'installation des mises à jour, nous pouvons procéder aux étapes suivantes. Puis, nous ferons un redémarrage.

2.6 Installation des logiciels professionnels

2.6.1 Installation du client VPN SSL par Stormshield

Pour permettre au client de télétravailler, nous avons choisi d'utiliser le client VPN SSL Stormshield. Nous avons opté pour ce logiciel, car il permet une intégration simple et totalement sécurisée. Le client utilisant des firewalls Stormshield, ce VPN se trouve être la meilleure option, autant à l'installation qu'à l'utilisation.

Pour l'installation, nous n'avons qu'à télécharger les fichiers d'installation du logiciel disponible sur le site de Stormshield, puis à l'installer. Après cela, le client peut se connecter à son site de travail en entrant ses identifiants et l'URL, Uniform Resource Locator, du VPN. Le compte de l'utilisateur doit donc être présent sur le firewall. Celui-ci a été créé en toute transparence grâce à l'AD.

2.6.2 Configuration d'Office 365

De nos jours, la suite Office est l'outil de base de beaucoup de personnel. C'est pourquoi, les clients demandent systématiquement que la suite Office soit configurée. La suite 365 étant installée nativement, nous n'avons qu'à connecter l'utilisateur grâce au compte généré par l'AD. La clef de licence étant déjà assignée sur le Tenant 365, aucune clef n'est à renseigner.

2.7 Installation des logiciels sécurisants

2.7.1 Installation de Cryhod par Prim'X

Cryhod est un logiciel permettant un déchiffrement pré-boot. C'est-à-dire que les disques du poste sont chiffrés lors de l'extinction puis déchiffrés lors de l'allumage (boot). Cette sécurité supplémentaire permet de sécuriser les données de l'entreprise en cas de vol du poste.

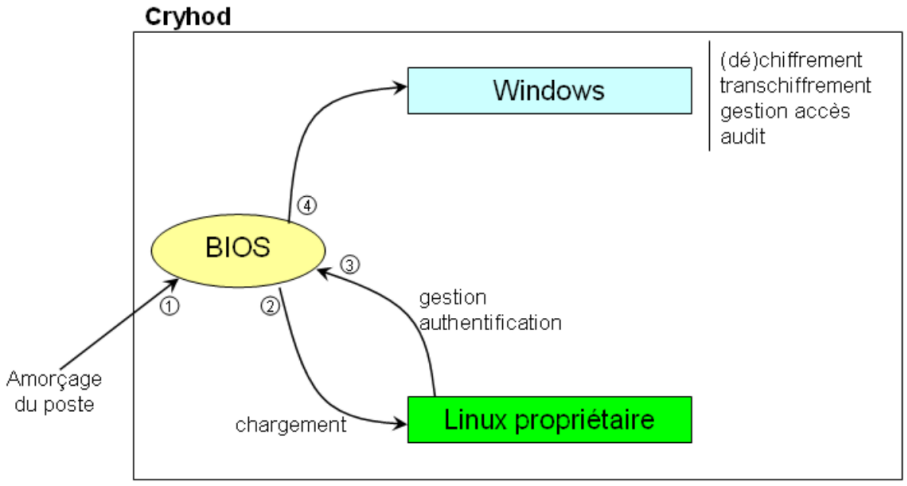

Figure 10 : Architecture du fonctionnement de Cryhod

Pour l'installation, nous devons mettre les fichiers d'installation sur le poste. Ses fichiers sont émis de manière restreinte et ciblée par l'éditeur du logiciel, Prim'X. Une fois les fichiers sur le poste nous allons pouvoir installer le logiciel. Une étape notable, consiste à créer une liste d'accès. Autrement dit, on va entrer un identifiant et un mot de passe permettant le déchiffrement du poste.

Figure 11 : Menu Cryhod permettant de créer la première liste d'accès du poste

Pour finaliser l'installation, nous allons pouvoir choisir le type de chiffrement, pour un souci de performance, nous allons sélectionner le chiffrement rapide. Le logiciel ne chiffre donc que les secteurs utilisés du disque. Si des données se trouvent en dehors de ces secteurs, elles resteront donc telles quelles. Etant donné que les PC installés sont totalement neufs, les secteurs inutilisés sont totalement vierges, une fuite de donnée n'est donc pas à craindre. Pour finaliser l'installation, nous devons laisser Cryhod désactiver Bitlocker, la solution de chiffrement de Microsoft, nous comparerons ensuite ces deux logiciels.

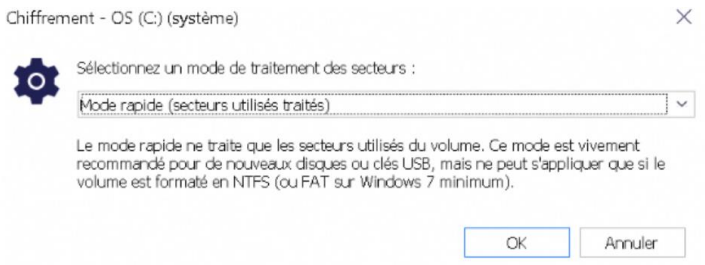

Figure 12 : Menu déroulant permettant de définir le type de chiffrement

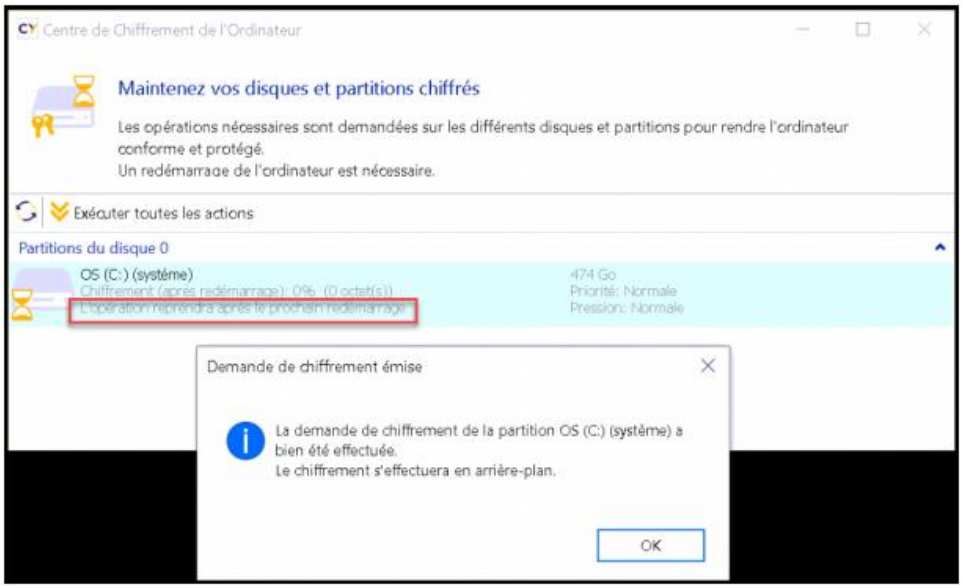

Figure 13 : Interface attestant de l'état d'avancement du chiffrement

Comme dit précédemment, le logiciel Cryhod fait l'objet d'une distribution restreinte. La distribution doit se limiter à l'OTAN, Organisation du Traité de l'Atlantique Nord, et à l'UE, Union Européenne, restreinte. Autrement dit, il est considéré que le partage de ce logiciel en dehors de l'OTAN et de l'UE pourrait nuire à la sécurité informatique de ceux-ci. Cela démontre une sécurité de très haut niveau. De plus, Cryhod est certifié CC AEL 3+, Common Criteria Evaluation Assurance Letter, cela veut dire que le logiciel a été testé et vérifié de manière méthodique. Il est apte à une utilisation civile sécurisée mais non apte à une utilisation militaire, milieu dans lequel une habilitation minimale CC AEL 5 est nécessaire. Aussi, Cryhod est certifié par l'ANSSI, cette certification permet aux fonctionnaires (mairies, administrations...) d'utiliser le logiciel dans un cadre étatique et cela apporte encore davantage de crédit à Prim'X.

Avec l'objectif de trouver la meilleure solution d'un point de vue de l'utilisation et de la sécurisation, je vais maintenant comparer BitLocker de Microsoft et Cryhod.

En ce qui concerne leur utilisation, Cryhod se distingue par sa portabilité multi-OS. Compatible avec Windows et Linux, il offre une flexibilité aux utilisateurs qui peuvent bénéficier de ses fonctionnalités de chiffrement sur différentes plateformes. Cette portabilité permet aux utilisateurs d'utiliser Cryhod sur leurs différents appareils, indépendamment du système d'exploitation utilisé.

D'un autre côté, Bitlocker, intégré dans les systèmes d'exploitation Windows, offre une implémentation transparente pour les utilisateurs qui utilisent déjà cette plateforme. Bitlocker tire pleinement parti des fonctionnalités de sécurité et des paramètres de gestion de Windows, simplifiant ainsi l'utilisation pour les utilisateurs de cet écosystème.

En ce qui concerne le niveau de sécurité, Cryhod et Bitlocker offrent tous deux des mécanismes de chiffrement robustes. Cryhod utilise l'algorithme de chiffrement AES, Advanced Encryption Standard, avec des clés de 256 bits, garantissant un haut niveau de sécurité. Il intègre également des fonctions de hachage pour renforcer l'intégrité des données. Bitlocker, utilise également l'algorithme AES, mais offrant aussi la possibilité d'utiliser le mode de chiffrement XTS-AES, XEX-based Tweaked Stealing, pour davantage de sécurité. De plus, Bitlocker est compatible avec les modules de plateforme sécurisée TPM, Trusted Plateform Module, renforçant ainsi la sécurité au niveau matériel.

En résumé, Cryhod se distingue par sa portabilité multi-OS, permettant aux utilisateurs de bénéficier de ses fonctionnalités de chiffrement sur différents OS. Bitlocker, quant à lui, offre une intégration transparente avec les systèmes d'exploitation Windows et tire parti des fonctionnalités de sécurité de Windows. En termes de sécurité, les deux logiciels utilisent l'algorithme AES, mais Bitlocker offre une flexibilité supplémentaire avec le mode de chiffrement XTS et la prise en charge du TPM. Enfin, l'argument faisant pencher la balance pour Cryhod est plutôt d'ordre géopolitique. En effet, l'éditeur, Prim'X étant français, la France et ses alliés européens ont une plus grande souveraineté sur leurs données, et l'utilisation de cette solution permet de s'émanciper malgré tout de l'hégémonie américaine et de Microsoft.

2.7.2 Installation de ZoneCentral par Prim'x

ZoneCentral est un logiciel permettant la création et l'accès à des répertoires chiffrés sur le poste ou partagé. Cette protection permet d'éviter le vol de donnée, du moins de données lisibles. Mais le logiciel de s'arrête pas là, il rend aussi les keyloggers inopérants en changeant le driver par une solution sécurisée, il permet le chiffrement de boite mail, de support amovible et de cache application.

Zone Central s'inscrivant parfaitement dans l'environnement Prim'X, celui-ci peut ou non utiliser la même liste d'accès que Cryhod évoqué précédemment. Par ailleurs, les authentifications via carte à puce et via Token sont toutes deux supportées par ces solutions.

Utilisant les mêmes algorithmes de chiffrement que Cryhod et reposant sur des technologies éprouvées, ZoneCentral est lui aussi certifié EAL3+, il est donc parfaitement adapté aux entreprises situées dans l'UE ou pays faisant partie de l'OTAN.

Etant donné que nous avons déjà créé la liste d'accès dans le cadre de notre mise en place, l'installation du logiciel est particulièrement sommaire. Toutefois, celle-ci nécessite un redémarrage permettant au poste d'atteindre la cible définie par les GPOs.

2.7.3 Installation de l'anti-virus Trend Micro Apex One

Pour la protection applicative, Synexie a décidé de proposer l'outil Trend Micro Apex One. Ce choix a notamment été fait car Trend Micro permet une sécurité à tous les niveaux. En effet, celui-ci permet évidemment de protéger efficacement le poste contre les attaques classiques de fishing, de vers et de chevaux de trois, mais il propose aussi des fonctionnalités de protection de vie privée très intéressantes. Il permet par exemple de monitorer facilement nos données exposées sur les réseaux sociaux, comme Linkedin ou Facebook, renforçant encore la sécurité du personnel.

En plus de ses fonctionnalités utilisateurs attrayantes, Trend Micro permet de monitorer le déploiement antiviral sur tout le parc via une console administrateur. Cette console permet de suivre les agents et envoie des alertes en cas de détection, mais elle permet aussi de modifier le comportement du logiciel, permettant par exemple de modifier le type de scan, ou d'activer ou non certains outils aux utilisateurs.

A titre de comparaison, Trend Micro-Apex One excelle particulièrement en la détection de faille zero day d'après l'Institut d'analyse IT AVTEST. Cette faculté permet une protection constante. Cette aptitude est permise par une détection via machine learning, qui va "prédire" le comportement d'un programme, bloquant l'attaque avant qu'elle ne s'exécute, et ce même si le malware est inédit.

L'installation du logiciel est relativement simple. Pour celle-ci, nous utilisons une version spécifique qui va permettre aux postes de directement apparaître sur la console administrateur sans faire aucune action supplémentaire. Une fois le fichier d'installation récupéré sur la console administrateur, on procède à l'installation. Les paramètres étant fixés par l'administrateur, on fait "suivant", "autoriser" et enfin "installer".

2.7.4 Installation de l'agent de supervision N-Able pour Synexie

Dans le cadre d'un dépannage, il est nécessaire que Synexie puisse facilement prendre la main sur le poste. Pour cela, plusieurs bonnes solutions existent comme AnyDesk ou TeamViewer. Malgré leurs efficacités, N-Able a rapidement été adopté car il ne nécessite aucune intervention de l'utilisateur du poste cible. Un technicien peut prendre à tout moment la main sur le poste. N-able permet aussi de lancer des scripts en toute transparence ce qui peut être utile pour administrer un ou plusieurs postes sans importuner les utilisateurs. Contrairement à ses concurrents, N-able permet aussi de changer de session utilisateur comme si nous étions sur site. Un grand pouvoir impliquant de grandes responsabilités, il est crucial que l'accès à la console d'administration soit sécurisé. C'est pourquoi un mot de passe complexe et la double authentification sont requis pour se connecter à celle-ci.

En plus d'une grande simplicité à l'utilisation, N-able est extrêmement simple à l'installation. En effet, Synexie utilise une version dédiée à chaque entreprise qui pointe vers la console d'administration de Synexie. Cela veut donc dire que le fichier d'installation est différentié pour chaque client. Lorsque l'installation est exécutée, tout se fait en transparence sur le poste. Quelques minutes après, on peut retrouver le nouveau PC dans le dossier correspondant au nom du client, nous pouvons alors prendre la main sur le poste.

2.7.5 Configuration de l'outil de sauvegarde cloud OneDrive

Malgré ses apparences de logiciel simplet et gratuit, OneDrive est aujourd'hui une des meilleures options lorsqu'il s'agit de stockage cloud, en particulier lorsqu'on parle de la version professionnelle. En effet, ce client ayant principalement des licences Microsoft 365 Business Standard, chaque utilisateur peut jouir de 1 Téraoctet dématérialiser sans coûts supplémentaires. En plus de cet avantage, OneDrive propose une utilisation parfaitement intégrée à l'environnement Windows. Aussi, un programme open source appelé OneDrived permet d'accéder à votre espace sur Linux. Le choix de OneDrive était donc sans appel.

Le logiciel étant sur le poste nativement, son installation est quasi-inexistante. Il ne nous reste qu'à lancer OneDrive, sélectionner les fichiers à sauvegarder et le tour est joué.

2.7.6 Filtrage Vade for Office 365

Le fishing est encore aujourd'hui un moyen simple et peu risqué d'arnaquer des particuliers et des entreprises sur internet. C'est pourquoi, une solution permettant le filtrage dynamique du flux de mail est vitale. Vade permet cela, en se connectant directement à l'Office 365. Mais c'est aussi bien plus que ça. Vade permet en effet de détecter, bloquer et supprimer les messages de fishing grâce à l'IA, Intelligence Artificielle, et ce même rétroactivement. Mais il permet aussi une sécurisation totale des utilisateurs en analysant les pièces jointes et URLs, permettant même de détecter les virus polymorphes.

En plus de cette fonction, Vade permet aussi la formation du personnel grâce à différents programmes de sensibilisation permettant aux salariés d'en apprendre davantage sur les stratagèmes des pirates ; car nous le savons, des utilisateurs avertis restent le meilleur moyen de défendre son SI.

L'installation est totalement transparente, aucune action n'est nécessaire tant que le nombre de licences est suffisant.

2.8 Finalisation de la commande

2.8.1 Contrôle qualité

Pour finir, avant de réemballer le matériel, nous nous assurons que toutes les étapes ont correctement été suivies. Pour cela, nous avons établi un formulaire faisant l'état des lieux d'un poste totalement configuré. Puis, nous vérifions chaque objet et constatons s'il est bien présent et configuré sur le poste.

2.8.2 Réemballage

Pour cette finale étape, nous remballons consciencieusement le matériel dans leurs cartons respectifs. Il faut alors être très soigné car il ne faut pas oublier que le client réceptionne du matériel totalement neuf et que, lui aussi, procèdera à l'étape de vérification de la marchandise.

2.9 Problème rencontré

Dans cette partie, je vais m'attarder sur un problème que j'ai rencontré lors de la mise en place de ces postes.

Tout d'abord, je dois remettre les choses dans leurs contextes. Aussi, il faut noter que la description que vous venez de consulter n'est pas séquentielle, chaque étape n'est pas décrite dans un ordre chronologique précis. J'ai décidé d'omettre certains détails pour en parler dans cette partie et éviter les répétitions.

La problématique provient du client VPN et du fait que ces installations ont été faites chez Synexie, donc à distance. Donc pour lier le poste au domaine, je devais d'abord installer le client VPN sur la session administrateur local. Une fois cela fait, je pouvais lier le poste au domaine. Cependant, depuis la dernière mise à jour du client, il est impossible d'installer le client VPN sur plusieurs comptes d'un même poste. Cela nécessite donc d'abord de désinstaller le VPN de la session locale, se reconnecter au compte de l'AD et réinstaller le client VPN. En résumé, il faut : installer le VPN sur une session locale, lier le pc au domaine, redémarrer le poste, relancer le VPN, se connecter sur la session de l'utilisateur, désinstaller le VPN de la session administrateur local, se reconnecter à la session utilisateur pour enfin réinstaller le client VPN : quelle acrobatie !

Une fois cette manipulation appréhendée, on peut s'en sortir. Cependant, j'ai une fois fait l'erreur d'installer le client VPN sur la session temporaire, sauf que même après avoir supprimé l'utilisateur, le client VPN était toujours considéré comme étant installé sur un utilisateur du poste. Je devais donc désinstaller le logiciel d'une session supprimée. Après avoir cherché une solution, je suis arrivé à la conclusion que c'était impossible. J'ai donc réinitialisé le poste et repris toute l'installation.

3 Rackage de serveur

3.1 Contexte client

Le client est un centre hospitalier spécialisé en traitement radiothérapique. Le centre permet en effet la détection et le traitement de maladies telles que le cancer ou certaines tumeurs. Cela est possible grâce aux scanneurs IRM, Imagerie par Résonnance Magnétique, et à ce que l'on appelle des canons à électron permettant d'affecter la partie malade sans ouvrir le patient. Cette prouesse est rendue possible grâce à des grandes machines coutant plusieurs millions d'euros. Ces machines sont toutes interconnectées grâce à une infrastructure permettant l'échange de radio, d'ordonnance, de données médicales et le pilotage des machines de traitement. Autrement dit, l'indisponibilité des services peut avoir des conséquences dramatiques sur la vie des patients.

Les serveurs étant vieillissants et commençant à montrer des faiblesses en termes de performance et n'étant plus sous garantit, une intervention était nécessaire ; toujours en étant le plus prévoyant possible.

3.2 Mission

Pour la réalisation de cette mission, nous étions trois à intervenir. Cela peut paraître excessif, mais il ne faut pas oublier qu'un serveur comme cela pèse environ 30 Kg. De plus élever ce genre de matériel à 2 mètres de hauteur, même en étant 3, n'est pas chose facile.

Cette mission s'est déroulée en plusieurs étapes. Tout d'abord, nous avons mis en place les deux commutateurs se trouvant tout en haut. Le rackage de ce type d'équipement est simple car il dispose d'attache basique ; une fois vissé, l'équipement ne peut plus être déplacé. Ensuite, nous avons monté les serveurs. Cela dispose d'une attache sur rail permettant de faire sortir le serveur du rac très simplement. Bien que simple à l'utilisation, ce système se trouve être relativement délicat lors de l'installation. En effet, la première étape consiste à mettre en place tous les rails qui accueilleront ensuite les serveurs. Ensuite, il faut clipser les serveurs dans les rails. Pour cela, il faut déplier les rails puis faire correspondre 6 vis qui doivent chacune être parfaitement alignées au risque de ne maintenir le serveur correctement. Une fois ceci effectué, la dernière étape consiste à mettre tous les câbles dans les passes câbles. Là aussi, ils sont particuliers, ceux-ci doivent permettre aux câbles de parfaitement se déplier lors du coulissement des serveurs. Cette étape est très importante, car vous l'aurez compris, un arrachement de câble pourrait avoir de graves conséquences il faut donc être très consciencieux.

3.3 Résultats

Figure 14 : Face avant des serveurs installés

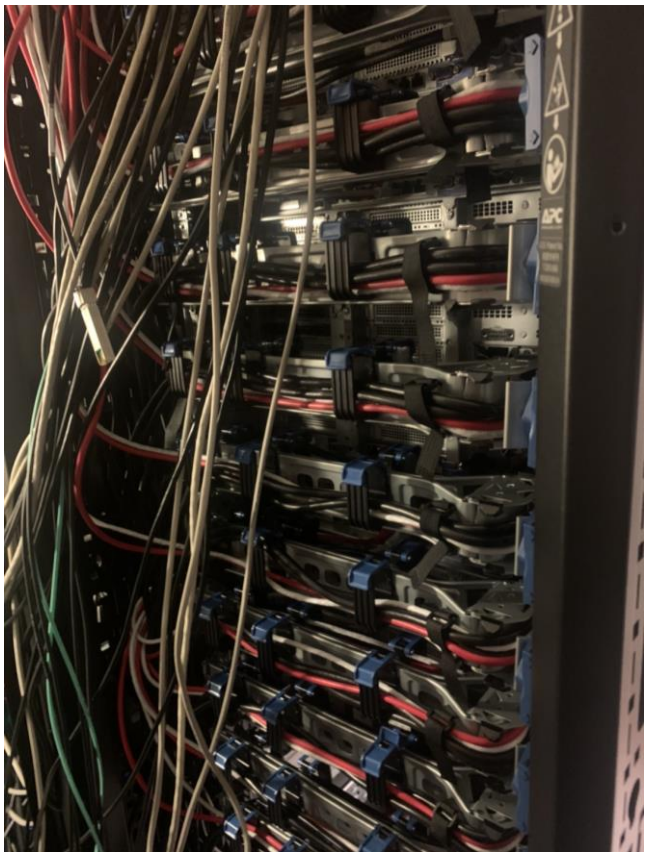

Figure 15 : Câble management à l'arrière des serveurs

4 Support : Rétablir l'accès à une URL

4.1 Problématique

Lors d'une journée d'observation support, le technicien et moi avions été confrontés à une utilisatrice pour qui il était impossible d'accéder à un site en particulier. Ce problème était critique car le site concernait l'activité professionnelle de la cliente.

4.2 Cause

Dans un premier temps, nous avons essayé nous-mêmes de nous connecter au site web : test réussi. Le problème ne vient donc pas du site web. Ensuite, nous avons fait différents tests sur le poste de l'utilisatrice. Dans un premier temps, nous avons essayé les classiques manipulations de navigateur : changer de navigateur, décharger le navigateur, mode incognito. Aucune des techniques n'a fonctionné. Nous avons donc déduit que le problème provenait de plus bas : le poste ne peut aller sur internet lorsqu'il cherche à accéder à cette URL.

Alors, j'ai pensé aux règles du pare-feu. Celle-ci bloquent en effet les requêtes depuis et vers les régions ayant un cyberespace dangereux comme l'Afrique ou l'Europe de l'Est. Comme nous le savons, toute URL représente enfaite une adresse IP pouvant être identifiée dans l'une de ces régions black-listées.

Nous avons donc ensuite utilisé le site web : https://www.infowebmaster.fr/ qui nous a permis de facilement trouver le pays d'hébergement du site. Le résultat était alors sans appel : le site est hébergé en Côte D'Ivoire.

Figure 16 : Page du site infowebmaster.fr

4.3 Solution

Pour résoudre ce problème, nous nous sommes alors connectés sur l'interface d'administration du Firewall. Le technicien que je suivais sachant que je possède le CSNA, Certified Stormshield Network Admin, me propose alors de faire la règle permettant de laisser passer les requêtes vers et

depuis cette URL. Je fais donc une première règle autorisant le trafic vers l'URL depuis le réseau interne utilisant les protocoles HTTP, Hyper Text Transfer Protocol ou HTTPS, Hyper Text Transfer Protocol Secure. Aussi, il ne faut pas oublier de placer ces règles au-dessus des règles de réputation bloquant le site. Après avoir fait cela, nous avons demandé à la cliente de réessayer de se connecter au site posant problème : cela a fonctionné.

5 Veille technologique : comparaison de logiciels de supervision

5.1 Problématique et objectif

Nous le savons, le monde de l'IT et plus généralement de l'informatique est en constante évolution. C'est pourquoi, un temps doit impérativement être alloué aux techniciens et aux ingénieurs dans le but de toujours rechercher des meilleurs outils. Cette concurrence peut permettre d'une part de trouver un outil permettant une meilleure rentabilité de l'employé, mais cela permet aussi de constamment former les équipes à propos des nouvelles technologies.

Aujourd'hui, Synexie utilise l'outil N-Able. Cet outil nous permet avant tout de prendre le contrôle des PC à distance. Aussi, N-Able nous permet de monitorer très basiquement les infrastructures et VMs, Virtual Machine, de nos clients. Il permet aussi une supervision applicative, nous facilitant grandement la surveillance de Windows. En plus de cela, N-Able possède une fonction de sauvegarde externalisée. Cette fonction se déclenche chaque jour sur les postes prédéfinis permettant une protection des données maximale.

Vous l'aurez compris, N-Able est, sur le papier, extrêmement complet et pourrais à lui seul permettre une supervision et un dépannage des utilisateurs. Malheureusement, la réalité est toute autre. Pour commencer, la fonction de supervision réseau est bien maigre. A vrai dire, les visuelles sont peu claires et peu personnalisables. La fonction de supervision se retrouve donc gravement affectée par ce manque d'évolutivité. Aussi, de notre expérience, N-Able souffre de problème de fiabilité. Plus précisément, lorsqu'on lançait le fichier MSI, Microsoft System Installer, la machine ne remontait pas sur la console admin rendant impossible toute administration ou prise de contrôle.

L'objectif de cette mission est donc de trouver un ou plusieurs outils permettant de remplacer N-Able dans le but de croître la capacité du support. Aussi, une meilleure vision des réseaux existants pourrait aider lors de projet d'évolutivité.

Vous pouvez le constater, la mise en place d'un nouvel outil est essentielle pour la croissance de Synexie. C'est en gardant ces objectifs en tête que je vais confronter les outils suivants : N-Able, Zabbix, Service Nav et Azure Monitor.

Pour mettre en valeur la confrontation et permettre aux ingénieurs et décisionnaires d'avoir la meilleure vision possible. Je vais tout d'abord devoir livrer une présentation lors d'une réunion réunissant les décisionnaires, les techniciens ainsi que les ingénieurs pour dégrossir les différents outils un maximum. Ensuite, je vais recueillir les différents prérequis auprès des ingénieurs à fin d'établir un tableau récapitulatif des fonctions spécifiques demandées qui permettra de prendre une décision finale.

5.2 Etude préliminaire

5.2.1 Prise d'information

Dans un premier temps, l'objectif est de dégrossir le plus possible pour étayer un maximum la première présentation qui abordera les logiciels de manière globale. Durant cette première prise d'information, je cherche à mettre en concurrence les points les plus généraux afin de déterminer l'inspiration générale des outils.

Pour comparer les outils, j'ai utilisé un document Excel dans lequel j'entre différents items. De la tarification, au type de logiciel en passant par le protocole de communication utilisé, on essaye ici de réunir un maximum d'information que l'on peut définir surfacique.

	Priorité	ZABBIX	SERVICENAV	N-ABLE	Azure Monitor	Commentaires
Support éditeur	1	*24h/5-2h/7*	*sous 24h/7*	NT	*24h/5-1h/7*	
Application Mobile	2	OUI	OUI	OUI	OUI	
On premises	3	OUI	OUI	NON	OUI	
Cloud	3	OUI	OUI	OUI	OUI	Azure Monitor et ServiceNav peuvent être full cloud ou on premises.
Emplacement géographique des SRV						
Remote control	1	OUI*	OUI*	OUI	OUI*	Zabbix permet uniquement d'exécuter des commandes/scripts à distance.
Macro	2	OUI	OUI	OUI	NON	
Gestion des utilisateurs	3	OUI	OUI	OUI	OUI	
Génération de rapport	3	OUI	OUI	OUI	OUI	N-able nécessite l'utilisation de Report Builder pour pouvoir les personnaliser.
Type de logiciel	2	*Opensource*	*Propriétaire*	*Propriétaire*	*Propriétaire*	

Figure 17 : Extrait du 1er tableau comparatif

Pour chercher les informations, j'ai généralement utilisé les documentations officielles ou le site internet g2.com qui permet de mettre en concurrence des outils dans le domaine de l'informatique. Il compare les outils souhaités à partir d'avis utilisateur. C'est donc une véritable mine d'or qui permet d'avoir une vision transversale et qui permet parfois de remettre en perspective les spécifications annoncées par les éditeurs.

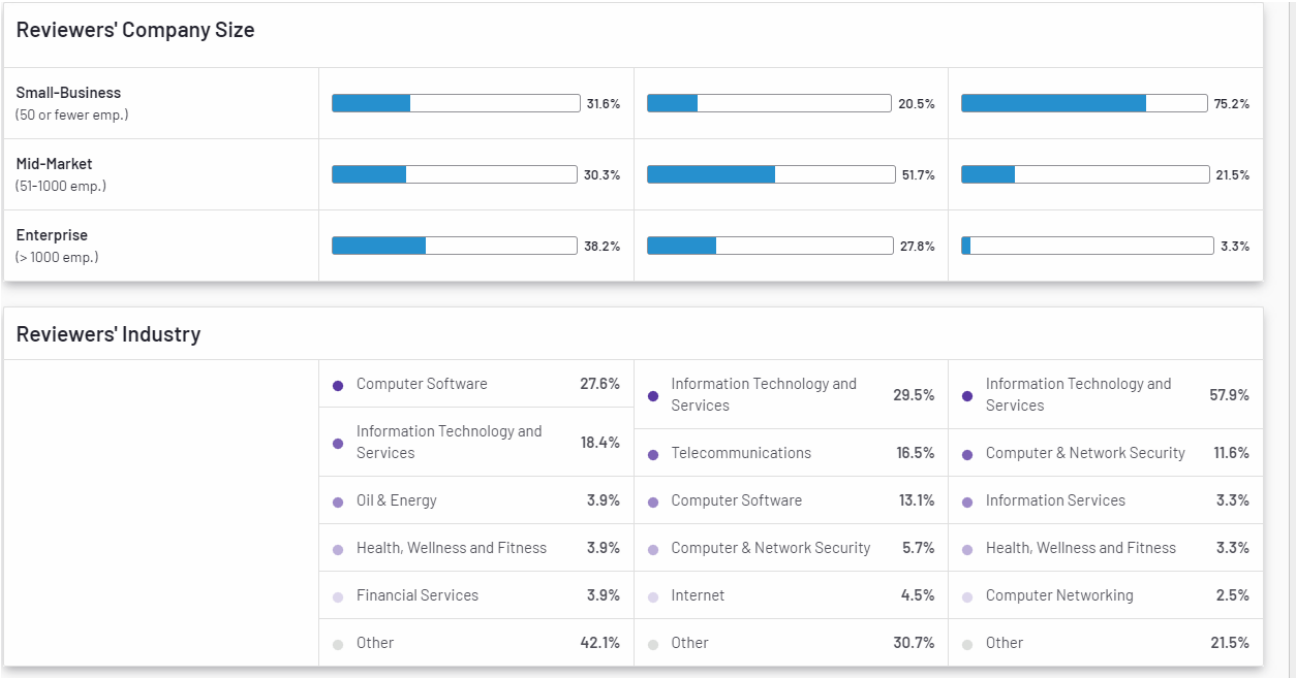

Figure 18 : Tableau comparatif donné par g2.com

5.2.2 Mise en forme des recherches et présentation

Afin de présenter ces premières recherches, je vais faire une présentation PowerPoint. Ayant étudié ce logiciel en cours, je maîtrise parfaitement celui-ci.

Vous l'aurez compris, lors de cette présentation, je vais rester fonctionnel sans aller trop dans le domaine technique de ces solutions. Je dois proposer quelque chose de clair et manifeste pour tous mes interlocuteurs.

Avec l'objectif de capter le plus possible l'attention de tout le monde et de permettre une session FAQ, Foire Aux Questions, constructive, j'ai décidé d'articuler la présentation de la manière suivante: dans un premier temps, je décris les objectifs de la réunion et les points abordés, et je rappelle les outils. Ensuite, je décris une à une les solutions en mettant en avant leurs points forts et négatifs. Enfin, je fais une page de conclusion permettant de rappeler à chacun les différences majeures entre chaque solution dans le but de démarrer facilement la session questions-réponses.

Figure 19 : Extrait de la présentation PowerPoint

5.3 Définitions des objectifs

Durant la session questions-réponses, nous avons tous pu grossièrement analyser les différentes possibilités et limitations de chaque solution. C'est pour cela que la phase suivante est primordiale.
A partir de la présentation, les ingénieurs seniors m'ont remis une liste de fonctions spécifiques à mettre en concurrence.

5.3.1 Mise en forme

Pour mettre en forme ces recherches approfondies, j'utilise le même tableau Excel précédemment cité. Je vais ensuite drastiquement étoffer celui-ci. Ici, les recherches prennent plus de temps que pour le livrable précédent. En effet, chaque solution étant différente et plus ou moins rependue, la prise d'information précise et fiable peut se retrouver être un véritable casse-tête ; mais là encore, la documentation officielle se retrouve bien souvent être notre meilleure alliée.

Supervision des ressources hardware
Supervision des stockages
Surveillance services Windows
Surveillance des ports/protocoles
Surveillance applicative
Outil de backup intégré
Surveillence service de backup
Notifications multi-supports
Facturation sur l'application

Figure 20 : Exemple de fonctionnalités spécifiques recherchées

5.4 Décision

La décision finale ne sera malheureusement prise que plus tard, après la fin du stage à partir de la deuxième version, plus complète, du tableau. Alors, les ingénieurs et les décisionnaires auront la lourde tâche de peser le pour et le contre de chaque solution.

Ils devront en effet choisir entre Zabbix et ses fonctionnalités très nombreuse, gratuit mais long à mettre en place, ServiceNav, complet, léger, mais soumis à licence, N-Able, qui permet de prendre le contrôle de PC à distance tout en proposant d'intéressantes fonctions annexes, mais qui souffre de lourds problèmes de fiabilité ou Azure Monitor qui à la fois bénéficie et pâtie de l'environnement Microsoft.

6 Conclusion

Pour finir, mon stage aura été d'une manière générale extrêmement enrichissant. Durant celui-ci, j'ai pu grandement améliorer mes compétences en réseau grâce aux nombreuses mises en conditions réelles et grâce aux enseignements dispensés en cours qui m'ont permis de bâtir mes compétences sur un solide socle. Mes nouvelles compétences en cybersécurités, plus particulièrement l'installation des logiciels sécurisants, me permettent d'avoir une vraie plus-value opérationnelle. Au-delà des compétences acquises, cette expérience m'a permis de réellement appréhender la vie en entreprise. J'ai notamment pu expérimenter les aléas clients et la gestion de crise directe. Dans de telles conditions, la formation et une bonne gestion émotionnelle sont primordiales. De plus, ce type de situation permet une montée en compétence évidente et rapide.

Après avoir acquis de précieuses compétences à l'IUT, je souhaite maintenant approfondir mon parcours universitaire en intégrant une école d'ingénieurs. Sachant que Synexie a déjà formé plusieurs ingénieurs qui sont aujourd'hui reconnus, poursuivre ma carrière au sein de cette entreprise est en parfaite adéquation avec mes objectifs.

Enfin je ne peux qu'être satisfait après d'avoir pu travailler dans de bonnes conditions matérielles et un bon environnement de travail : des locaux modernes, une ambiance agréable et un personnel amical établissant ainsi une atmosphère de confiance solide.

7 Remerciements

Je tiens avant tout à remercier mon maître de stage Basile LHEUREUX pour son accompagnement, sa disponibilité et ses conseils précieux durant mon stage.

Je tiens également à remercier Matthieu NICOD pour m'avoir accepté et intégré au sein de l'équipe de Synexie.

Aussi, je veux remercier Jean-Luc DAMOISEAUX pour son aide lors de la rédaction de mon rapport de stage et pour ses qualités de professeurs réseau.

En fin, de manière plus générale, je remercie toute l'équipe ITCC pour leur contribution à l'amélioration de mes compétences et pour leur accueil dans le monde professionnel.

8 Glossaire

Notion, plateforme regroupant des tutoriels et procédures mises à disposition par une entreprise pour cette même entreprise.

VPN SSL, réseau privé virtuel utilisant le protocole SSL/TLS pour sécuriser les communications.

AD, Active Directory, service de gestion des utilisateurs et des ressources dans un environnement Windows.

LDAP, Lightweight Directory Access Protocol, protocole utilisé pour accéder et gérer des services d'annuaire.

Driver, logiciel permettant à un système d'exploitation de communiquer avec un périphérique matériel.

Transparence, caractéristique d'un système ou d'un processus s’effectuant sans aucune présence visuelle.

Keylogger, logiciel ou dispositif matériel espion qui enregistre les frappes effectuées sur un clavier à des fins frauduleuses.

Support amovible, dispositif de stockage externe, comme une clé USB ou un disque dur externe, qui peut être connecté ou déconnecté d'un système.

Monitorer, surveiller ou suivre l'activité, le comportement ou les performances d'un système, d'un réseau ou d'un utilisateur.

Machine learning, technique d'intelligence artificielle permettant aux ordinateurs d'apprendre et de s'améliorer à partir de données sans être explicitement programmés.

Faille zero day, vulnérabilité de sécurité logicielle encore inconnue et non corrigée par les développeurs.

Stockage cloud, service de stockage en ligne permettant aux utilisateurs de sauvegarder, de partager et d'accéder à leurs données via Internet.

Open source, logiciel dont le code source est librement disponible, permettant aux utilisateurs de le modifier, de le distribuer et de l'utiliser librement.

Phishing, technique d'escroquerie en ligne visant à tromper les utilisateurs pour obtenir des informations personnelles ou financières en usurpant une organisation légitime.

Virus polymorphes, logiciels malveillants capables de se modifier et de changer de forme pour échapper à la détection antivirale.

Cyberespace, environnement virtuel créé par les systèmes informatiques interconnectés à travers Internet.

Règle de réputation, critère ou ensemble de critères utilisés pour évaluer la confiance ou la fiabilité d'une entité en ligne à partir de critères généraux.