Sommaire

I) L’environnement économique du stage chez *INFOTECH*

A – Le secteur : FAAA

1. Présentation

Faaa est une commune mitoyenne de Papeete. C’est la ville la plus peuplée de toute la Polynésie française, avec une population de 29 506 habitants (selon les statistiques du recensement 2017, la ville étant ainsi plus peuplée que sa voisine Papeete).

2. Le secteur économique

Faaa joue un rôle central dans l'économie locale grâce à plusieurs éléments clés :

Transport et Logistique

L'aéroport international de Tahiti-Faaa, situé sur son littoral, est un élément crucial pour l'économie de la commune et de la Polynésie française en général.

Il sert de porte d'entrée principale pour les voyageurs venant de l'étranger et constitue un centre logistique important pour les importations et exportations (Contrat de Ville) (TAHITI INFOS, les informations de Tahiti).

Initiatives Locales et Services Publics

La commune se distingue également par son innovation dans les services publics.

Elle est la première en Polynésie française à avoir mis en place le paiement en ligne des redevances, facilitant ainsi les démarches administratives pour ses habitants (Outremers 360).

Développement Social et Éducation

Sur le plan social, Faaa soutient ses résidents à travers diverses propositions, comme le renouvellement des bourses communales pour les étudiants.

Ces bourses aident à couvrir les frais de cantine scolaire, soulageant ainsi les familles à faible revenu (TAHITI INFOS, les informations de Tahiti).

Ces actions montrent l'engagement de Faaa envers un développement durable et inclusif, tout en renforçant ses infrastructures et en améliorant la qualité de vie de sa population.

B – L'entreprise par rapport au secteur

1. L'histoire de la Société INFOTECH.

INFOTECH est une société de services locale spécialisée, depuis plus de neuf ans, dans l'équipement informatique et la maintenance des établissements publics et privés (mairie, école, collège et lycée), grandes surfaces, sociétés et particuliers dans un esprit de confiance, de performance, et de compétence.
Afin de répondre au mieux aux attentes de ses clients, INFOTECH développe toute une gamme de services sur mesure à un tarif abordable qui couvre l'essentiel des besoins potentiels. Il est possible d'intervenir à tout moment et anticiper les dysfonctionnements matériels ou logiciels dans le cadre d'un contrat de maintenance informatique et de télémaintenance.

Infotech assure la maintenance complète du parc informatique et garantit un suivi et des révisions adaptées. Infotech est composée d'une équipe expérimentée qui peut concevoir, mettre en place et gérer l'ensemble des systèmes d'information, en veillant à ce qu'il réponde aux exigences des différents établissements publics ou privés.
Cela inclut la gestion des serveurs, des réseaux, des bases de données, des logiciels, ainsi que la sécurisation des données sensibles.

2. *INFOTECH* aujourd'hui et demain

Activité principale : fournir une solution globale répondant aux besoins de ses clients.
INFOTECH propose 3 grands pôles d'activitées complémentaires:

Logiciels

- Conception, réalisation et diffusion
- Adaptation permanente aux besoins de ses clients
- Développements spécifiques
- Évolution technologique
- Solutions antivirales, Anti Spam, Filtrage de contenu web
- EDR sauvegarde restauration
- Virtualisation
- Cloud Computing

Matériels

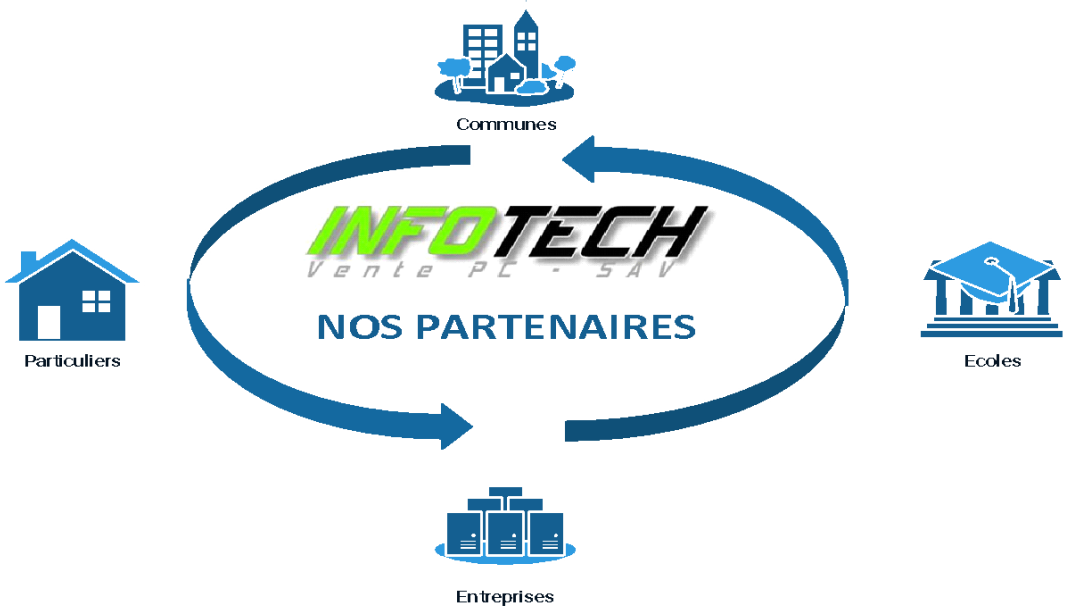
- Ordinateurs, imprimantes, douchette,
- Câblage, accessoires, consommables
- Spécialiste de l'équipement réseau, client-serveur et multiposte
- pointeuse
- Système de stockage NAS/SAN

Services

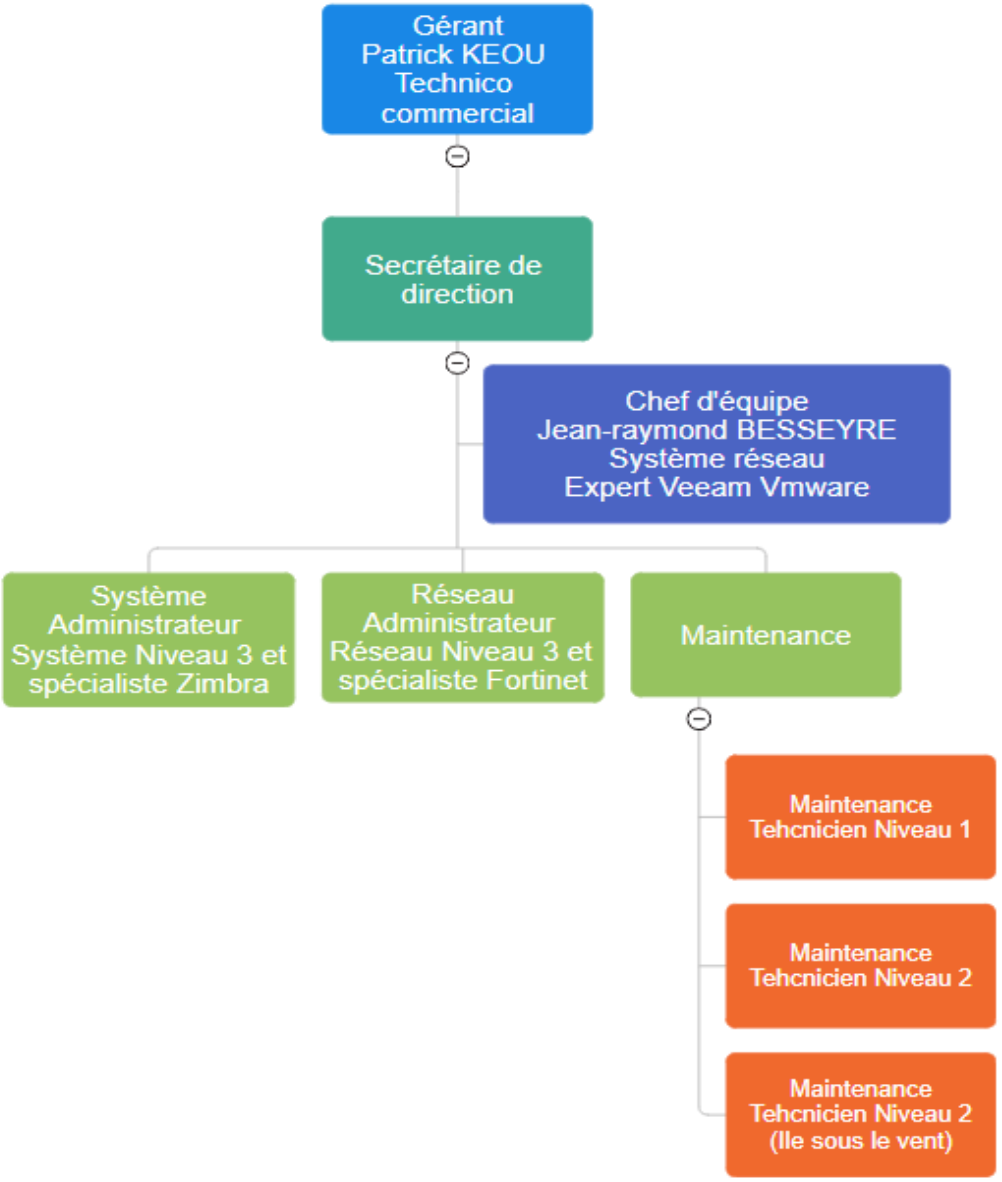
- Gestion de parc
- Sécurité réseaux : Protection des données
- Câblage réseau et fibre optique
- Installation de salle serveur
- Études et conseils
- Configuration et paramétrage avant mise en place
- Supervision (cartographie, monitoring, télémétrie)
- Installation sur site
- Assistance téléphonique
- Télémaintenance : connexion à distance
- Mise à jour des logiciels
- Location de matériels
- Hotspot : connexion wifi
- SAV

Nos partenaires

Forts de nos différentes expériences, nos clients sont de secteurs très variés.



C – Mieux comprendre l'organisation de la société *INFOTECH*



1. Descriptif de la structure sociale

L'équipe est composée pour la partie technique de :

- 3 Techniciens informatique qualifiés (2 sur Tahiti et 1 basé à Raiatea) ;
- 1 Administrateur réseaux ;
- 1 Administrateur systèmes ;
- 1 Chef d'équipe ;

Et au niveau administratif :

- 1 secrétaire de direction ;
- 1 secrétaire comptable ;
- 1 technico-commercial.

II) Consolidation des compétences

A – Les missions

➢ Installation de mon poste informatique

Le 13/05/2024 à 8h on m'a confié comme première mission, d'installer mon poste informatique. Je devais contrôler un écran d'ordinateur, un clavier, et une souris afin de valider leur fonctionnement.

Résultat :

À 8h30, fin du contrôle et mise en place des périphériques sur une unité centrale.
À 9h30, création de mon identifiant et d'un mot de passe par un administrateur afin de pouvoir accéder à une session Windows.

➢ Intervention chez un client sur Papeete

Mise en place :

Le 14/05/2024 à 8h30, nous intervenons sur place avec le maître de stage chez Gondrand Voyages Tahiti, un des clients potentiels de la société.

Situation:

Le problème est lors de l'envoi des mails, le logiciel utilisé est Outlook qui est exploité sur MacOS. Nous intervenons sur place car les ordinateurs Mac sont plus difficiles à gérer à distance.

Solution :

Pour résoudre le problème temporairement, le tuteur a basculé les données stockées sur Outlook, le logiciel e-mail d'origine du système d'exploitation MacOS.
L'intervention a duré 1h, nous sommes retournés ensuite au siège qui se situe à Faaa.

➢ Transfert de données

Situation :

Le client voulait changer de licence windows, cela pourrait impacter les données tels que les image stockées sur Onedrive.

Besoin : Vider les images stockées sur Onedrive afin de les transférer dans un dossier local.

Mise en place :

Le 14/05/2024 à 13h, ma mission est de déplacer 11 000 images stockées dans la galerie OneDrive vers un dossier “IMAGE” stocké en local, il s'agit de libérer l'espace OneDrive du client. Le temps a été estimé de 5 min à 10 min pour 500 photos transférées, donc environ 3h30 de transfert en utilisant la méthode pour 500 photos transférées en 10 min maximum.

Résultat :

Toutes les photos ont bien été transmises, cela à pris 1 journée.

➢ Intervention chez deux clients

Situation :

Si aucune intervention au niveau des postes informatiques n'est effectuée, les postes risquent d'être attaqués par des virus et risque aussi d'être saturé au niveau des disques durs ou des composants du pc.

Besoin :

Faire des maintenances régulières, mensuelles afin d'analyser, de diagnostiquer et de réparer si besoin les postes informatiques saturés, endommagés ou attaqués.

Mise en service :

Le 14/05/2024 à 14h, je suis allé en intervention avec une technicienne dans deux entreprises situées à Papeete. Clients qui ont un contrat avec INFOTECH.
Nous nous y rendons afin de procéder à une maintenance des postes informatiques des deux entreprises, une avait 4 postes et l’autre en avait 1. Nous avons tout d'abord lancé les logiciels permettant d'effectuer des analyses et de nettoyer les PC, puis nous avons effectué un test d’impression afin de valider le bon fonctionnement des postes informatiques. Le temps a été estimé à 1h maximum.

Logiciels utilisées :

Nous avons utilisé plusieurs logiciels pour effectuer les analyses et le nettoyage des postes informatiques. Les logiciels utilisés sont CCleaner pour le nettoyage, ADWcleaner pour l’anti-malware, Crystal Disk pour l'état du disque dur, GLPIagent pour faire un état des lieux de tous les postes.

Résultat :

Tous les postes ont été sauvegardés, il n’y avait aucun virus, aucune saturation du disque.

➢ Intervention sur Taiarapu-Ouest

Besoin :

Se rendre sur place afin de régler les soucis que rencontrent le client, réaffectation des imprimante dans leurs vlan respectif et contrôle des switch.

Mise en place :

Le 15/05/2024, nous intervenons à Taiarapu-ouest, plus précisément à la mairie de Vairao. Nous y passons toute la journée car il y avait plusieurs tâches à réaliser, notamment avec le contrôle des switchs, la mise en place des imprimantes dans leurs réseaux correspondants (Vlan), et l'installation d'une solution Windows LAPS.

Problème :

Il y avait un switch et nous ne parvenions pas à accéder et à réinitialiser.
En effet, nous ne pouvions pas entrer dans le switch avec le mot de passe utilisé et par câble console car le mot de passe était soit incorrect ou perdu.
Pour le câble console, le switch n'avait pas de port console, il était non réinitialisable car nous n'avons pas réussi à le "RESET".

Solution :

Nous avons procédé d'une autre manière en interceptant les câbles passant par ce switch afin de les muter sur un autre switch (accessible).
Cette intervention a permis de remettre les imprimantes dans leur bon réseau (Vlan).
Cela nous a pris 8h, car il y avait plusieurs postes informatiques à configurer et il y avait 3 secteurs à la mairie de Vairao, dont l'annexe et l'entrepôt.
Par contre, nous ne sommes pas parvenus à mettre en place la solution Windows LAPS par faute de temps, car nous arrivions à la fin de la journée.

Résultat :

Les imprimantes ont été réassignées dans leurs vlan respectif et les switchs ont été contrôlés et configurés avec succès.

➢ Annonce des projets

Le 16/05/2024, un technicien de INFOTECH m'annonce les projets que je vais devoir faire durant les 6 semaines.

- Le premier est la mise en place d’un réseau DMZ, c'est-à-dire qu’il y aura 1 serveur qui réceptionnera le réseau internet afin de pouvoir le distribuer aux autres serveurs. Cela permet d’avoir une sécurité accrue afin de protéger les serveurs d’une attaque web.
- Le second projet est de créer un serveur permettant de centraliser les log (erreurs).

➢ Mise en place de la solution Windows LAPS

Situation :

INFOTECH n'a pas de solution permettant la centralisation, la gestion et la création de mot de passe administrateur local pour les postes de la mairie de Vairao.

Besoin :

Mettre en place une solution permettant la centralisation, la gestion et la création de mot de passe administrateur locale pour les postes de la mairie de Vairao.

Mise en place :

Le 16/05/2024 à 10h, on m’assigne pour mission de mettre en place la solution Windows LAPS pour les postes de la mairie de Vairao. Mon tuteur m’envoi un mail pour que je puisse suivre un tuto en ligne. Il s'agit d’une solution permettant de créer des mots de passe de comptes administrateurs locaux aléatoirement sur une durée donnée, afin de les centraliser sur l’Active directory dont seulement une poignée d'utilisateurs ont accès.
Cette tâche m'a pris 1 journée et demi car il y a plusieurs étapes pour mettre en place cette solution.
La première étape est d’installer le logiciels qui pèse 1 Mo, la seconde étape est de configurer ce logiciels en ligne de commande et la troisième étape est de créer une GPO pour pouvoir déployer ce logiciel sur tous les postes de la mairie afin d’obtenir des mot de passe administrateur local aléatoire et centralisé.

Résultat :

La solution Windows LAPS à bien été mise en place, cependant il y avait quelques postes ou le logiciel ne s'est pas installé via la GPO.

Solutions :

Pour remédier au problème il fallait installer le logiciel manuellement sur chaque poste informatique ou le logiciel ne s’est pas effectué via la GPO.

➢ Vérification et dépannage de la solution Windows LAPS

Le 21/05/2024, j'ai procédé à la vérification de Windows Laps afin de résoudre quelques soucis concernant le déploiement du logiciel via la GPO.
N'ayant pas trouvé la solution sur le moment, j'ai rédigé un mail au technicien de la mairie de Vairao pour qu'il puisse installer Windows LAPS manuellement sur les postes informatiques ou le logiciel ne s'est pas installé via la GPO.
Je lui ai envoyé la procédure à suivre pour mener à bien cette tâche.

➢ Configuration du serveur BASTION

Définition d'un "serveur bastion" :

Le serveur bastion est celui qui va permettre au client de pouvoir accéder aux autres serveurs, qu'il s'agisse du serveur Active directory, du serveur de messagerie.
Il dispose d'une interface graphique et d'une authentification "user & password".

Situation :

Le bastion de la mairie de Tumaraa n'est plus accessible car le serveur à plusieurs problèmes au niveau de sa configuration.

Besoin :

Les clients ont besoin d'accéder aux autres serveurs, pour cela il faut réinstaller un nouveau serveur bastion.

Mise en place :

Le 22/05/2024, on m'assigne pour mission de configurer le nouveau serveur bastion de la mairie de Tumaraa car leur ancien serveur bastion n'étant plus disponible.
Le tuteur me montre les étapes à suivre, à ajouter l'entrée DNS sur le serveur ONATI, à vérifier le DDNS et autoriser sur le pare-feu le DNAT vers le nouveau serveur bastion pour y accéder via le web. Une fois les étapes exécutées et vérifiées, il fallait créer le serveur en se basant sur "OVF". Une solution permettant de sauvegarder un serveur et le tuteur a fait la sauvegarde d'un serveur bastion avec les configurations par défaut au format "OVF" afin de ne pas re-créer et re-configurer le serveur en cas où il le faudrait.

Configuration :

Une fois le serveur créé il fallait adapter la configuration selon une procédure écrite par le tuteur.

La configuration comprend le changement des adresses IP, le changement des informations Active Directory, la configuration Guacamole et SSH.
Une partie de la procédure était à faire en ligne de commande sous linux et le reste sur l'interface graphique du serveur bastion.
La dernière étape était de supprimer les anciennes connexions par défaut et créer de nouvelles pour les serveurs utilisés actuellement. C'est-à-dire configurer les nouvelles connexions en se basant sur leurs adresses IP et leurs systèmes d'exploitation.
Si un serveur utilise linux il fallait mettre le bon port soit "22" et pour Windows "3389".

Résultat :

Une fois les connexions créées, le serveur bastion était opérationnel.

➢ Configuration Crontab et Logrotate

Le tuteur m'a transmis une feuille avec une configuration "crontab" et "logrotate" pour que je puisse créer une tâche automatisé avec Crontab, et organiser les fichiers avec la bonne date et l'heure avec Logrotate pour les logs du serveur bastion.

➢ Intervention chez un client

Situation :

Si les postes informatiques ne sont pas soufflés, pas diagnostiqués, les postes risquent de ne pas bien fonctionner à cause de l'accumulation de poussière au niveau des composants et ils risquent d'être attaqués et saturés.

Besoin :

Souffler les postes informatiques, faire une analyse ainsi que le diagnostic des 14 postes de la société afin d'éviter tous types d'attaques et de saturation du disque dur.

Mise en place :

Le 23/05/2024 à 13h, je suis allé en intervention avec un technicien à YINKET, une entreprise située à Titioro. La mission a été de souffler 14 postes informatiques et de faire la maintenance Windows, notamment avec le lancement de plusieurs logiciels pour vérifier, nettoyer et protéger les postes informatiques. L'intervention a pris toute l'après-midi.

Résultat :

Tous les postes ont bien été soufflés et ont bien été vérifiés et diagnostiqués.

Il n'y avait aucune menace concernant les virus ni aucune saturation au niveau des disques durs et du NAS.

➢ Mise en place d'une GPO

Situation :

Les agents de INFOTECH ont tendance à sauvegarder les mot de passe sur les navigateurs web, cela est risqué car les gestionnaires de mot de passe des navigateurs ne sont pas à l'abri d'attaque provenant du web.

Besoin :

Les membres de la société ont besoin d'une solution permettant la désactivation du gestionnaire de mot de passe des navigateurs afin de ne pas les sauvegarder quand on les propose.

Mise en place :

Le 28/05/2024, on m'assigne pour mission de mettre en place une GPO permettant de désactiver le gestionnaire de mots de passe des navigateurs Google Chrome, Microsoft Edge et Firefox.
La première étape étant de créer la GPO au niveau du gestionnaire de stratégie de groupe du serveur Active Directory du client concerné.
Une fois la GPO créée, il faut télécharger les fichiers ADMX et ADML de chaque navigateur.
Ce sont des fichiers configurés à des fins de stratégie de groupe, ils permettent la configuration des paramètres logiciels pour pouvoir les appliquer via une GPO sur les postes ou utilisateurs concernés.
La GPO va permettre de déployer le paramètre ou le logiciel sur l'ensemble du réseau concerné.
Dans le cas de cette mission j'ai copié et collé les fichiers "ADMX et ADML" de chaque navigateur dans les bons dossiers afin de pouvoir configurer les paramètres logiciels sur la GPO.
Par la suite, j'ai configuré les paramètres logiciels de manière à désactiver le gestionnaire de mots de passe des trois navigateurs.
Une fois la configuration terminée il suffit d'appliquer la GPO pour qu'elle prenne effet, un redémarrage des postes informatiques peut être nécessaire pour mettre à jour la stratégie de groupe.

Résultat :

Une fois la GPO déployée, les postes ont bien pris en compte les paramètres logiciels de la GPO, c'est-à-dire que nous n'avons plus accès et ne pouvons plus activer le gestionnaire de mots de passe des trois navigateurs concernés.

➢ Export et import d'une GPO

Problématique :

La configuration d'une GPO peut prendre beaucoup de temps à mettre en place.

Besoin :

INFOTECH à besoin d'une solution permettant l'installation instantané des configuration d'une GPO sur un autre domaine.

Mise en place :

Le 29/05/2024, j'ai pour mission d'exporter la GPO sur un autre domaine, c'est-à-dire qu'il faut faire une sauvegarde de la GPO permettant la désactivation du gestionnaire de mots de passe des trois navigateurs dans un dossier, puis de rendre accessible ce dossier sur les autres serveurs Active Directory des autres clients.

Solution :

La méthode utilisée afin de rendre accessible le dossier de sauvegarde de la GPO est l'utilisation de "ZIMBRA" pour envoyer par mail le dossier de sauvegarde.
Une fois le dossier envoyé, il fallait se rendre sur un autre serveur Active Directory pour permettre l'importation des paramètres logiciels de la GPO configurée précédemment.
Dans le cas de cette mission, le tuteur a choisi le serveur Active Directory de INFOTECH afin de tester l'importation des paramètres de la GPO d'un domaine à un autre.
La GPO est configurée sur le domaine "taiarapu-ouest.pf" et doit être exportée vers le domaine "infotech.pf". Il s'agit de mettre en place une méthode d'exportation et d'importation des paramètres de la GPO sur un autre domaine afin de ne pas re-créer et de re-configurer la GPO sur chaque domaine.
Une fois sur le serveur Active Directory de INFOTECH, il fallait télécharger le dossier de sauvegarde afin d'importer les paramètres contenus dans cette sauvegarde sur une nouvelle GPO créée sur le domaine "infotech.pf".
Pour permettre l'importation il fallait d'abord créer une nouvelle GPO sur le domaine "infotech.pf"

, ensuite faire un clic droit sur cette GPO et cliquer sur importer des paramètres.
Une fois terminé, les paramètres sauvegardés précédemment vont être assignés à cette nouvelle GPO qui par la suite sera déployée sur le domaine “infotech.pf”.

Résultat :

Une fois que les paramètres ont été importés, il fallait vérifier si les paramètres attribués à cette nouvelle GPO ont pris effet. Pour cela il fallait que je lance une commande sur mon poste pour pouvoir mettre à jour ma stratégie de groupe.
Après avoir exécuté la commande, les paramètres se sont bien appliqués et je ne pouvais plus activer le gestionnaire de mots de passe sur les trois navigateurs web.

➢ Maquette CISCO-PACKET-TRACER

Durant la deuxième semaine, j’ai fait une maquette sur cisco-packet-tracer afin de simuler et de configurer un réseau contenant un pare-feu, un réseau utilisateur, une DMZ et internet. J’ai pu regarder des tutos sur youtube et google afin de connaître les différentes commandes pour paramétrer les différents matériels du réseau.
Le but étant de configurer les routeurs, le pare-feu et les différents serveurs. Une fois la configuration faite, il fallait ajouter des règles au pare-feu afin de filtrer les différentes requêtes, réseau et protocole (port).
Il y avait du “icmp” pour les PING, “tcp” et “udp” sur le port “53” pour le DNS, “udp” sur le port “67” et “68” pour le DHCP, “tcp” sur le port “80” et “443” pour le HTTP et HTTPS.
Tous ces protocoles ont été utilisés dans le cas de cette maquette, il fallait taper des commandes pour autoriser ou pas certains protocoles et ports.
Pour obtenir un réseau plus sécurisé et plus particulièrement pour le réseau internet, il fallait faire très attention aux niveaux des autorisations et des permissions configurées au sein du pare-feu, car le réseau externe est la zone de non confiance.

➢ Mise en place d’un server syslog avec ELK

Problématique :

La recherche d'erreurs ou l’utilisation des logs est difficile à cerner car les logs sont constitués uniquement de ligne, cela rend les recherches plus difficile en cas de problème.

Besoin :

INFOTECH à besoin d'une solution permettant la centralisation des logs sur un serveurs, afin d'analyser, visualiser, et agir plus vite par rapport aux erreurs.

Mise en place :

Du premier juin au sept juin j'ai eu pour mission de mettre en place un serveur syslog avec ELK afin de centraliser les logs des pare-feu et switchs de l'entreprise INFOTECH et de ses clients.

-ELK permet d'agréer les journaux de tous les systèmes et applications, de les analyser, et de créer des visualisation pour la surveillance des applications et de l'infrastructure, un dépannage plus rapide, l'analytique de la sécurité, etc.

Il est composé de trois applications dont:

- "Elasticsearch" qui est un moteur de recherche et d'analyse distribué utilisant le format JSON.

-"Logstash" qui ingère, transforme et transfert les données vers Elasticsearch.

-"Kibana" qui permet de donner forme aux données et est l'interface utilisateur extensible.

La première étape était de créer le serveur avec les bons composants afin qu'il puisse supporter les trois applications et ses données.

Le tuteur s'est chargé de la création du serveur et m'a confié les commandes par la suite.

Une fois le serveur créé il fallait suivre les différentes étapes pour l'installation des trois applications, l'installation des trois application doit se faire dans un ordre précis, c'est à dire qu'il faut télécharger Elasticsearch en premier, Kibana en deuxième puis Logstash en dernier, cela permet d'avoir une organisation des données et des configurations plus claires et ordonnées.

Configuration :

Une fois les trois applications installées je les ai configuré en modifiant leurs fichier soit "elasticsearch.yml & kibana.yml & filebeat.yml". Dans la mise en place de ce serveur je n'ai pas utilisé logstash pour la récupération des données mais plutôt

filebeat, filebeat à les mêmes fonctionnalités que logstash et à en plus plusieurs modules permettant le stockage de plusieurs systèmes et applications.

La seconde étape étant de modifier le fichier de configuration d'elasticsearch pour attribuer une adresse ip. Une fois l'adresse ip ajouter et laisser avec le port par défaut soit 9200, il fallait sauvegarder les modifications puis faire un restart du service elasticsearch pour mettre à jour les configurations.

Par la suite, j'ai configuré kibana afin d'avoir accès au site web, une fois à l'intérieur du fichier de configuration de kibana je lui ai attribué la même adresse ip que elasticsearch mais sur un port différents soit 5601.
J'ai par la suite ajouter l'adresse ip et le port pointant vers elasticsearch afin de récupérer les données stockées par celui-ci.
J'ai ensuite configuré filebeat afin de récupérer les logs des pare-feu client et entreprises.
Une fois à l'intérieur du fichier de configuration j'ai ajouté les adresses ip et port de elasticsearch et kibana pour que filebeat puisse communiquer et transférer des données avec ces deux applications.
Une fois les adresses ip configurées j'ai activé le module "fortinet.yml" afin de configurer ce fichier pour pouvoir récupérer les données des pare-feu, la configuration étant d'ajouter l'adresse ip du serveur et le port par défaut du module soit 9004.
Une fois les éléments ajoutés, filebeat écoutera sur l'adresse ip et le port spécifié dans le modules fortinet.yml, afin de récupérer les données des pare-feu configurés de manière à envoyer ces logs vers le module fortinet.yml.

Résultat :

Une fois toutes les applications et les modules configurés, il fallait accéder à kibana via le web en indiquant le protocole http ou https, l'adresse ip et le port spécifié pour kibana.
Une fois sur le site de kibana, j'ai vérifié que les logs était bien transmis, pour cela, je me suis rendu dans un onglet se nommant "découvrir" et de cette façon on pouvait visualiser, trier et observer les logs transférer.
Plusieurs manipulations étaient possibles et des tests ont été effectués afin de créer des graphiques et des visualisations des logs transmis.

➢ Chiffrement SSL / TLS des données transitant

Problématique :

Les données sont transmises en clair entre kibana et le navigateur web, cela est une faille de sécurité car des pirates du web peuvent s'interposer pour pouvoir récupérer les données.

Besoin :

Mettre en place des certificats TLS pour chiffrer les données transitant.

Mise en place :

Du trois juin au cinq juin, une seconde mission m'a été confiée ainsi qu'à mon tuteur par un autre informaticien, qui est de sécuriser les données transitant entre chaque applications et infrastructures.
C'est-à-dire chiffrer et déchiffrer le flux de données transitant des pare-feux à filebeat et de kibana au navigateur.

Configuration :

Pour la partie certificat TLS de kibana, j'ai pu créer un certificat TLS auto-signé via une commande openssl. J'ai créé le certificat et je l'ai assigné dans le fichier de configuration de kibana vers la partie configuration TLS.

Résultat :

Suite à cela, le certificat ssl auto-signé a bien été intégré et on a pu accéder au site kibana de façon sécurisée (https).

➢ Chiffrement TLS entre un pare-feu et logstash

Du 10 juin au 11 juin en à eu pour mission de chiffrer et déchiffrer les données envoyées des pare-feu clients et entreprises vers logstash. Pour des fins de flexibilité nous avons changé de stratégie pour l'application recevant les données.
L'ancienne application été filebeat, après plusieurs modifications, ajout et configuration nous ne sommes pas parvenu à déchiffrer les données chiffrées envoyé par les pare-feu sur filebeat, pour ce faire nous avons décidé de changer de tactique en optant pour la solution logstash qui offre plus de flexibilité au niveau des configuration.

Résultat :

Le tuteur n'a pas eu le temps de chiffrer les données transitant entre les pare-feu et filebeat.

➢ Dépannage d'un pc client

Problématique :

Le mode avion s'active sans cesse et le touchpad ne fonctionne plus.

Besoin :

Régler le problème du mode avion et du touchpad.

Solution :

Pour remédier au problème j'ai fait plusieurs recherches afin de connaître la source du problème et après vérification il s'agissait des fonctions de la touche "FN".

Il fallait maintenir cette touche et choisir des fonctions bien précises, situées sur les touches du clavier.

En appuyant sur la touche FN puis en choisissant une fonction, cela permettait de désactiver ou d'activer le mode avion et le touchpad.

Résultat :

Le problème était donc une mauvaise manipulation de la touche FN et de ses fonctions.

Une fois les vérifications et manipulations terminées, le pc était opérationnel avec le touchpad qui fonctionne à nouveau et le mode avion qui ne s'active plus.

➢ Mise en place des configuration d'un disjoncteur wifi

Problématique :

Les disjoncteurs habituels n'ont pas de fonction wifi, il faut les désactiver manuellement et ne disposent pas d'automatisation ON/OFF.

Besoin :

Configurer un disjoncteur wifi avec plusieurs fonctions afin d'automatiser l'activation ON et la désactivation OFF sur une plage spécifiée en heure et en minute.

Mise en place :

Le 12 juin à 9h Patrick (chef de l'entreprise) me confie pour mission, de paramétrer un disjoncteur avec des fonctions wifi, je lis la notice et il est marqué qu'il faut télécharger une application "**Smart Life**", il s'agit de l'application permettant de se connecter au matériel concerné et de le configurer à sa guise.

Configuration :

Les configurations demandés par Patrick est de mettre en place un compte à rebours, une connexion à distance via le wifi, un monitoring de la consommation d'électricité en jours mois et années, et le temps de mise sous tension du disjoncteur avec une plage spécifié, comme par exemple: (le disjoncteur doit s'allumer à 6h du matin et s'éteindre à 18h).

Résultat :

Une fois avoir pris connaissance des fonctionnalités de l'application, j'ai mis en place les configurations demandées par Patrick et j'ai pu effectuer plusieurs tests afin de valider le bon fonctionnement des configurations appliquées.
Le test à durer plusieurs minutes pour configurer au mieux la mise en place d'une plage ON/OFF spécifié, pour la partie compte à rebours il était situé dans les paramètres et permettait de configurer une durée pour mettre en marche ou en arrêt le disjoncteur.
Pour la partie électricité, il a fallu faire un test de plusieurs heures car l'application prend en "kWh". Une fois les tests effectués, le disjoncteur était opérationnel par rapport à la configuration demandée.

➢ Rédiger des procédures

Problématique :

Les projets mis en place tels que windows laps, configuration du disjoncteur wifi, déploiement d'une GPO ou mise en service du serveur ELK, peuvent prendre énormément de temps à reproduire si aucune procédure n'a été faite.

Besoin :

Une fois les projets mis en place, il faut rédiger des procédures afin de pouvoir reproduire la solution / serveur chez d'autres clients. La procédure devra être rédigée de sorte à ce que tout lecteur parviennent à mettre en place la solution / serveur.

Mise en place :

Du 16 mai au 5 juin j'ai pu rédiger les procédures de la solution windows laps et celle du déploiement, export / import d'une GPO.
Le 17 juin, j'ai pris le temps de rédiger deux procédures, celle pour la configuration du disjoncteur wifi et celle pour l'installation et la configuration du serveur ELK.

Résultat :

Les deux procédures ont été finalisées à temps, c'est-à-dire que j'ai pu les terminées en 5h. Pour les procédures windows laps et GPO, je les ai terminées en 5h également.
Une fois les procédures terminées je les ai transmises à mon tuteur pour qu'il puisse examiner et vérifier le contenu pour que par la suite, elles puissent être validées et archivées dans un dossier procédure dédié.

➢ Configuration de GLPI

Problématique :

INFOTECH ne reçoit aucune notification quand les licences ou certificats expirent.
Cela peut causer des problèmes au niveau des clients qui se retrouvent sans licence pendant un moment et donc ne peuvent plus accéder à la fonctionnalité (ex : mail pro) jusqu'à renouvellement de la licence.

Besoin :

INFOTECH à besoin d'être prévenu 4 mois avant l'expiration des licences, ceci permettrait à INFOTECH de pouvoir intervenir avant l'expiration des licences et de ce fait, éviter aux clients des problèmes.

Mise en place :

Du 20 au 21 juin j'ai eu pour mission de mettre en place une solution de notification permettant d'être averti en cas d'expiration des licences.
Pour ce faire, un administrateur a créé une session GLPI avec le profil super-admin afin de pouvoir configurer GLPI. Une fois à l'intérieur de GLPI j'ai fait plusieurs recherches et j'ai pu trouver la solution.
Il suffisait de configurer l'envoie des mail se situant dans la rubrique: configuration > notification > config mail.
Il fallait mettre l'adresse mail de l'expéditeur et du destinataire, le nom, ip, et port du serveur SMTP, ensuite il fallait enregistrer cette configuration afin que les notifications soient envoyées dans le mail professionnel d'infotech.
Pour que GLPI envoi des mail, il y avait une extension à installer sur le serveur GLPI, j'ai donc accéder en ligne de commande au serveur et j'ai installé l'extension MSMTP avec un sudo apt-get, une fois l'extension installée, j'ai configuré le fichier afin qu'il envoi les notifications sur l'email professionnel. J'ai pu faire des tests d'envoie avec succès.
Ensuite, je me suis rendu dans la partie configuration > notification > software licence, pour configurer une notification dédiée à la licence.
La seconde étape est de se rendre dans configuration > actions automatiques, afin de configurer une action automatique pour l'envoie d'alerte d'expiration des licences.

Une fois dans la rubrique j'ai configuré l'option "software" pour une fréquence d'exécution à 4 jours , un statut à "programmer", le mode d'exécution en CLI, une plage horaire d'exécution de 0 à 24h, et un temps de conservation des journaux pour 30 jours.
J'ai ensuite sauvegardé la configuration et je me suis rendu dans administration > entité > infotech > notification, et j'ai configuré l'adresse mail de l'expéditeur et du destinataire puis j'ai activé au niveau des licence l'options "alert sur l'expiration des licence" , "envoyer les alerts sur les licences avant" " 99 jours".
De ce fait, les notification d'expiration des licences seront envoyés sur l'email pro 99 jours avant l'expiration des licences, soit 3 mois et demi comme demandé.

TEST :

Pour mettre en place cette solution j'ai du faire plusieurs test, notamment en configurant la date d'expiration d'une licence au 01/08/2024 et en configurant la partie action automatique avec une fréquence d'exécution à 1 min en mode CLI afin d'exécuter toute les 1 min la tâche d'envoyer des alertes d'expirations au mail pro.
Pour avoir un aperçu du processus, il fallait configurer la durée sur 31 jours dans administration > entité > infotech > notification > licence, et envoyer les alertes sur les licences avant 31 jours, soit deux mois.
Puisqu'il y a un certificat expirant en août et que nous somme en juin et que l'on a spécifié qu'il fallait que les notifications soient envoyées deux mois avant l'expiration, lorsque l'action automatique va s'exécuter, il va envoyer la notification au mail pro deux mois avant l'expiration car nous l'avons spécifié dans administration > entité > infotech > notification > licence.
Si l'exécution de l'action automatique se lance et qu'il n'y pas de licence qui expire dans une plage deux deux mois, à compter de ce jour, alors aucune notification ne sera envoyée. Exemple: une licence expirant le 10/10/2024 et que nous sommes en juin, il y un écart de 4 mois, il n'y aura aucune notification envoyée au mail pro.
Dans le cas où la date d'expiration est le 01/08/2024 il y aura une notification envoyée dans le mail pro car il y a un écart de 2 mois. On peut spécifier la durée à laquelle on veut que la notification soit envoyée avant la date d'expiration, pour le test j'ai utilisé 2 mois et une licence expirant le 01/08/2024 afin de voir si une notification est bien envoyée deux mois avant l'expiration.

Résultat :

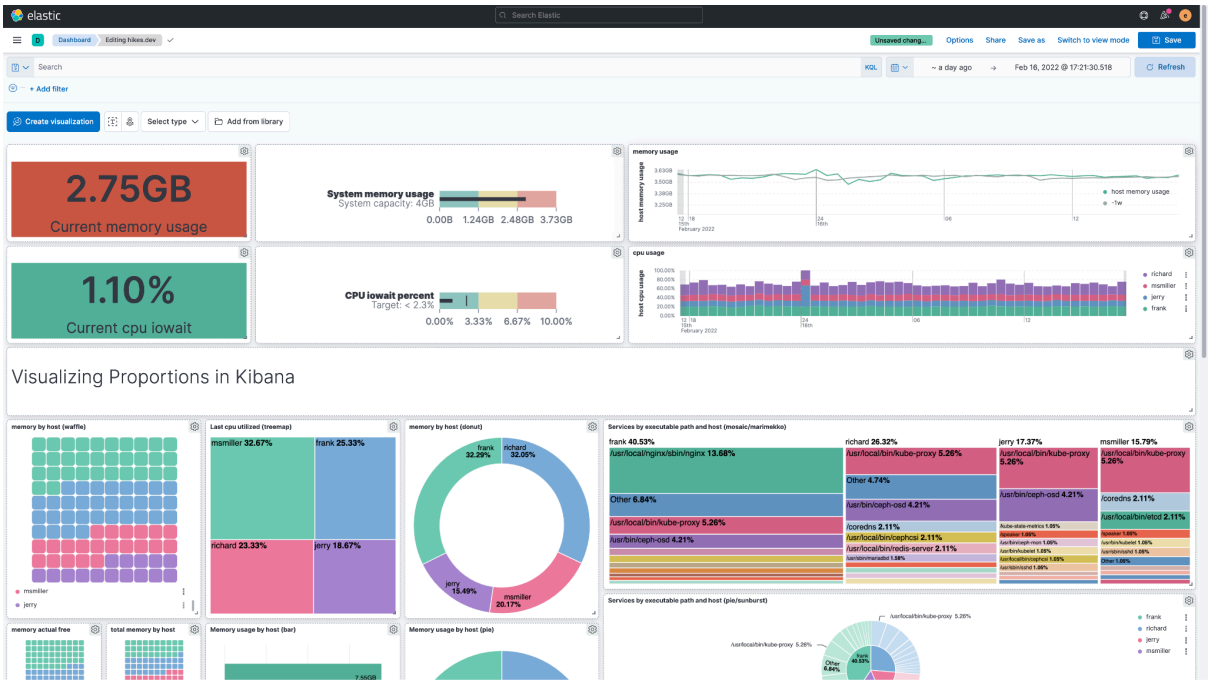
Les notifications ont bien été configurées, j'ai bien reçu les notifications X mois avant la date d'expiration des licences.

➢ Conclusion :

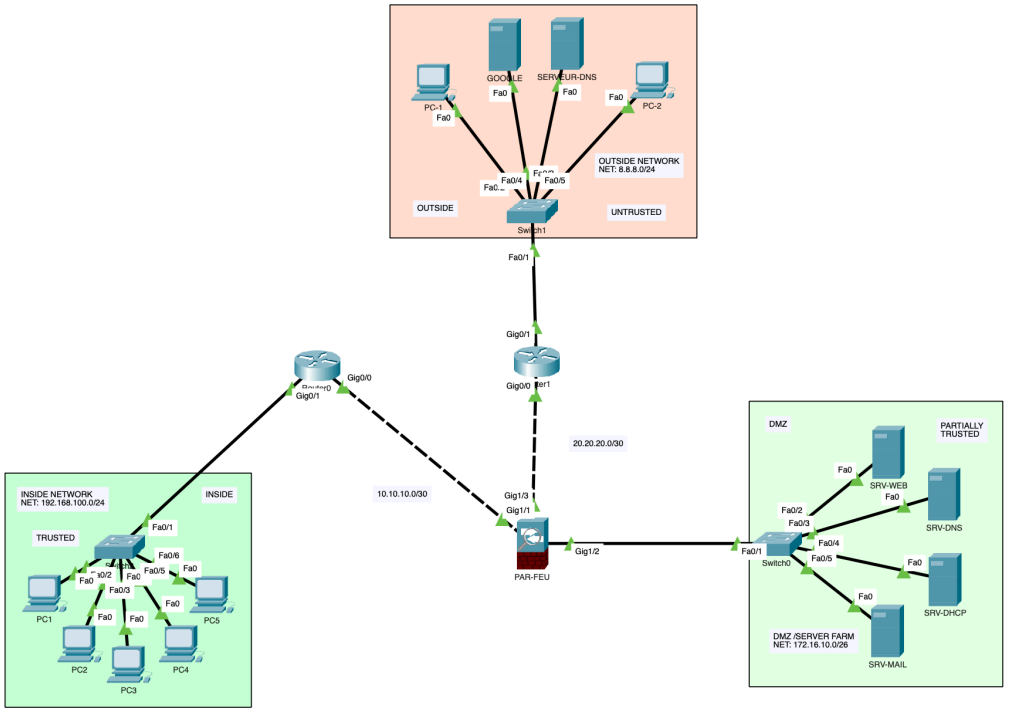
Durant toute la période de stage j'ai pus apprendre énormément de chose qu'il s'agisse de la mise en place d'un serveur de centralisation de logs avec ELK, le déploiement d'une GPO pour installer un logiciels sur des postes informatique, la compréhension des serveurs DHCP, DNS, MAIL et BASTION, les commande linux, la compréhension des différents port utilisées par le web, le NAT et DNAT au niveau du routeur, les différentes règles dites ACL au niveau du pare feu afin de sécuriser les entrées et sorties, les chiffrement TLS, la configuration et la gestion de GLPI, et les intervention chez les client et les logiciels utilisées.

➢ Annexes :

I/ Exemple de graphique ELK



II/ Maquette CISCO-PACKET-TRACER



III/ Interface de l'apps SMART-LIFE