AIX ynov CAMPUS

Rapport de stage

FIN D'ANNÉE 2019-2020

MASSEGLIA, Léo | Stagiaire cyber-sécurité
SOGETI ESEC | PARC DU GOLF 350 RUE JEAN RENÉ GUILLIBERT GAUTHIER DE LA LAUZIÈRE, 13300 AIX–EN-PROVENCE

Maitre de Stage : Léo SURET – [Project Manager]

Durée du stage : 22/06/2020 à 31/07/2020

Table des matières

1.Remerciements

Je tiens à remercier l'équipe ESEC pour mon accueil au sein de la structure, je me suis tout de suite senti à l'aise et intégré à l'équipe et ai pu remarquer la forte cohésion qui les anime.

Par exemple grâce aux « Cyber-cafés » du matin permettant de faire un point avec l'équipe de prendre des nouvelles et parler de tout et de rien avant de commencer sa journée de travail, mais aussi grâce à l'organisation d'*Afterworks* dans des bars et restaurants.

Je tiens aussi à adresser des remerciements particuliers mon maitre de stage Léo SURET qui a su m'aider à m'intégrer dans la structure et me présenter aux équipes, me faire visiter les bâtiments et répondre à toutes mes questions.

Toute l'équipe a travaillé et partagé des moments avec moi comme avec un « vrai » membre de l'ESEC, cette expérience a été une belle découverte de plusieurs corps de métiers que je ne connaissais pas, et du fonctionnement de la vie en entreprise.

2. Introduction

2.1. Présentation du stage

Le stage de fin d'année Ynov est effectué pendant les deux premières années de Bachelor et a pour but d'acquérir de l'expérience professionnelle en fin de cursus, il permet non-seulement de travailler en entreprise et de sortir du cadre de l'école mais aussi de pouvoir renforcer les compétences acquises pendant le cursus ou même en acquérir de nouvelles qui auraient pu ne pas être traitées à l'école.

Pour ce stage de fin d'année de Bachelor 1, j'ai réalisé mon stage chez Sogeti ESEC Méditerranée à l'agence d'Aix en Provence.

Ce rapport de stage permettra tout d'abord de comprendre le fonctionnement de Capgemini, et de sa filiale ESEC, leur mode de travail et les missions qui leur sont attribuées.
Ensuite j'aborderai la mission que j'ai pu réaliser au côté de l'équipe ESEC, le fonctionnement de SWIFT, des différents audits planifiés

Pour finir cette introduction j'aimerais aborder une courte définition des points clefs du rôle de consultant cyber sécurité :

Le consultant cyber sécurité réalise avant tout des missions de conseil pour accompagner ses clients et renforcer leur sécurité, pour être armé face aux cyberattaques, pour cela il va devoir étudier le degré de sécurité d'un système d'information pour mieux connaitre ses faiblesses et corriger ses failles.
Il devra aussi former le personnel de sécurité de la société sur l'importance de sécuriser le système informatique et de connaitre les règlementations en matière de sécurité informatique

Le consultant peut aussi établir un manuel d'utilisation pour les employés de l'entreprise, pour les former sur les démarches à entreprendre pour mettre en sureté son ordinateur.

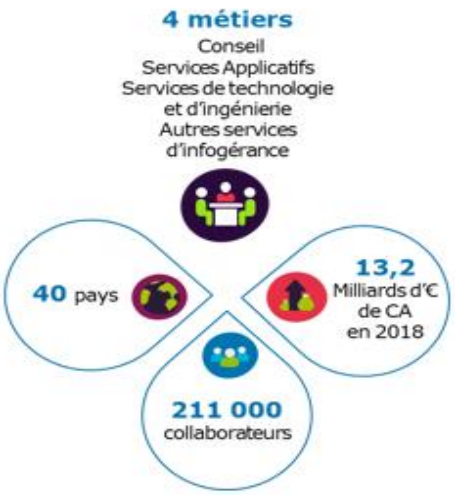
Les enjeux de ma mission en tant que consultant cyber ont été de :

- Comprendre le besoin du client (Echange autour de la Propale, étude du CSP CSCF SWIFT)
- Détenir des compétences dans l'architecture réseau,
- Être en capacité de monter ne compétences rapidement sur des nouveaux sujets (Cloisonnement réseau, gestion de privilège (Bastion), SOC, MFA) compréhension des audits

2.2. Capgemini, Sogeti et ESEC

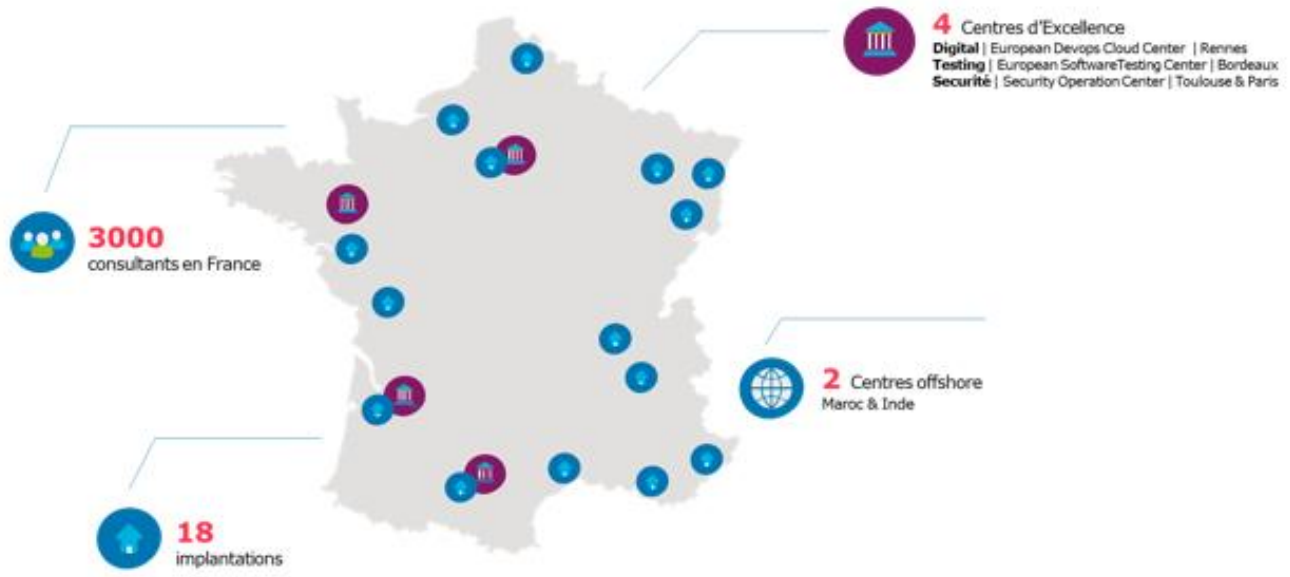
2.2.1. Capgemini dans le monde

Capgemini est un des leaders mondiaux du conseil, des services informatiques et de la transition numérique, créé par Serge Kampf en 1976 d'abord sous le nom de Sogeti, deviendra Capgemini suite à plusieurs rachats, Capgemini deviendra une entreprise à part entière et Sogeti une filiale de du groupe. L'entreprise est désormais cotée au CAC 40 à la bourse de Paris et est l'ESN (Entreprise de Services Numériques) au plus gros chiffre d'affaires en France, dans le top 10 mondial. Présent sur tous les continents, ci-dessous une carte de la répartition du groupe dans le monde, ses secteurs d'activité et quelques chiffres supplémentaires (source 2019).



2.2.2. Capgemini France

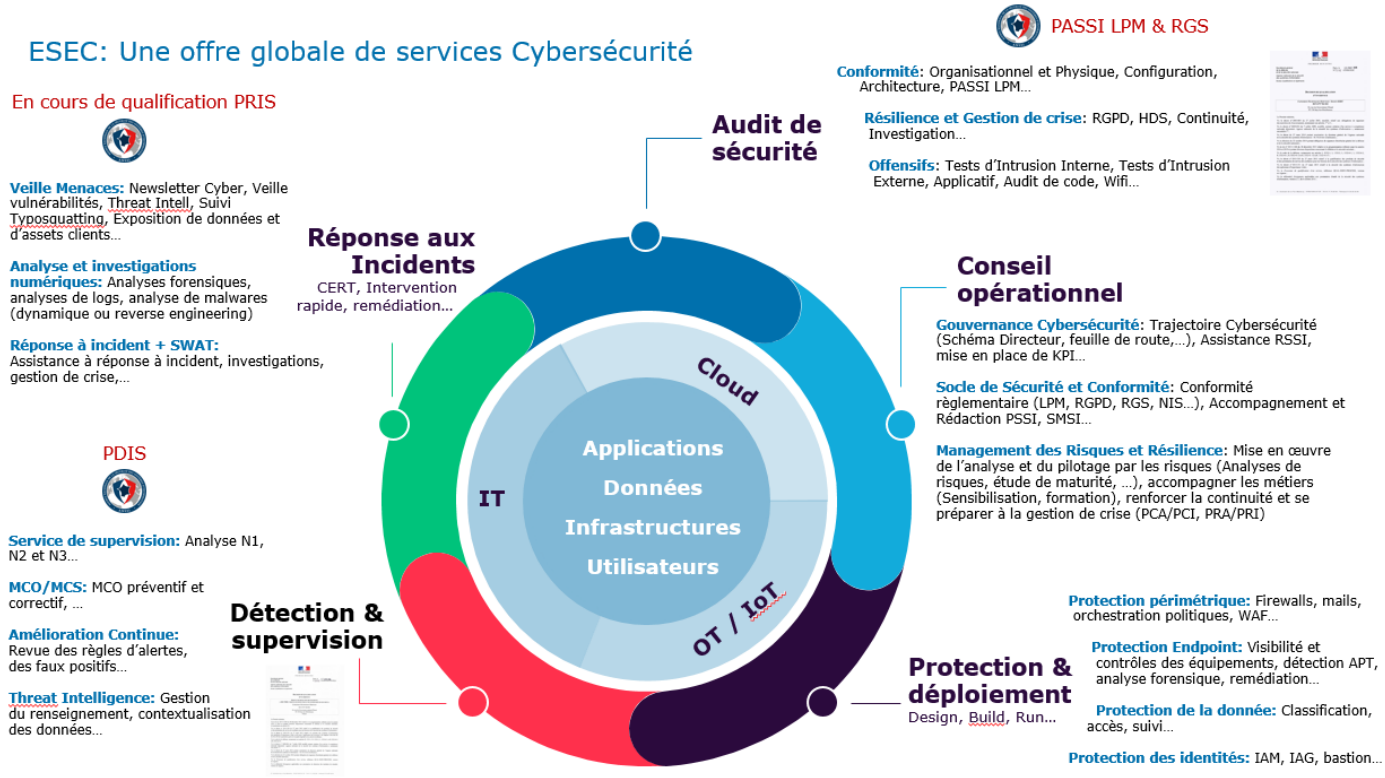
En France, pays de naissance de la société, Capgemini est situé dans 18 grandes villes et possède deux centres dits « *offshore* » situés au Maroc et en Inde.



2.2.3. ESEC

L'ESEC est la division cyber sécurité de Capgemini, c'est aussi ici que j'ai réalisé mon stage, dans l'agence d'Aix en Provence, voici quelques chiffres à propos de la structure.

L'ESEC agit sur 5 pôles de sécurité allant du consulting / Audit à des domaines de gestion de crise et de protection, dans des centres de surveillance globale (SOC) ou des équipes d'intervention d'urgence *pre/post* attaque informatique. Voici un graphique représentant tous ces pôles. Pendant mon stage j'ai par exemple travaillé avec des collaborateurs du pôle *Audit de sécurité*, pour sécuriser et mettre aux normes une infrastructure.



2.2.4. Déroulement d'un contrat

Chez l'ESEC et comme dans beaucoup d'entreprises, un contrat se déroule dans un certain ordre et doit respecter certaines procédures (voir ci-dessous)

- Premièrement l'approche commerciale va consister en plusieurs étapes permettant de trouver un client, comprendre ses insatisfactions par rapport à son produit actuel, ses besoins futurs, et lui confirmer que l'on est en mesure de lui apporter ce dont il a besoin.

- Ensuite, l'avant-vente, cette démarche permet de conseiller les ingénieurs pour s'accorder sur une solution ainsi que la proposition commerciale finale qui sera présentée au client, le consultant avant-vente est donc celui qui fait le lien entre la partie technique et commerciale.

- La proposition commerciale est une offre formalisée et écrite. Elle est spécifique à chaque prospect : y sont résumés les besoins et contexte du client. ... Concevoir une proposition commerciale va vous permettre : De donner un cadre précis à votre relation commerciale, notamment sur le plan juridique.

- Les audits (présentés plus tard) sont la partie pratique du contrat.

- La réunion de clôture fait partie des rites du projet. Même si elle n'est pas systématiquement jouée dans les organisations, elle permet de :
    - Tirer les leçons de l'expérience du projet et les capitaliser pour les projets suivants ;
    - Proposer des améliorations dans les référentiels de management de projet, et ainsi faire vivre le progrès permanent ;
    - Donner l'opportunité aux membres de l'équipe projet de s'exprimer sur leur vécu personnel du projet et sur le plaisir ou les difficultés qu'ils y ont trouvés ;
    - Reconnaître les contributions de chacun, pour les valoriser ;

3. Les travaux effectués

En raison des clauses de confidentialité (projet en pre-production, informations sensibles) et en tant que stagiaire sécurité soucieux de bien faire, je ne pourrai pas parler du contrat de l'entreprise pour laquelle j'ai travaillé mais je vais le décrire de manière « anonymisée ».

3.1. Outils mis à ma disposition

Je disposais pour mener à bien mes missions d'un ordinateur portable configuré pour travailler sur des projets sensibles, doté d'un BitLocker (Chiffrement du disque au verrouillage de l'ordinateur), d'une licence office 365, d'un gestionnaire de connexion Cisco AnyConnect me permettant de vérifier la sécurité d'un réseau qui, si elle n'était pas respectée, m'empêchait de me connecter et de travailler dessus, et d'un accès VPN obligatoire avec authentification par token temporaires. Autant dire que la sécurité était de mise.

J'ai travaillé la majeure partie du temps en télétravail depuis chez moi du au dé-confinement progressif,

Néanmoins, je suis allé tous les Lundis à l'agence à Aix pour y travailler toute une journée

3.2. Mes missions

En tant que stagiaire sécurité j'ai secondé mon maitre de stage qui travaillait dans le pôle Protection & Déploiement sur sa mission, le but : Mettre à jour toute une infrastructure obsolète pour une multinationale en vue de respecter les nouvelles normes de sécurité 2019 de Swift.

3.2.1. Qu'est-ce que SWIFT

Swift est une société fondée à Bruxelles en 1973, dans le but d'établir des protocoles et normes pour les transactions financières.

Les banques dans le monde avaient besoin d'un moyen sécurisé et rapide de transférer de l'argent d'un pays vers un autre, et c'est là que Swift s'est imposé pour répondre à la demande.

Swift procure un réseau sécurisé permettant plus de 10 000 transactions financières dans 212 pays différents. Les clients de la société sont bien souvent des banques, des sociétés de courtage, des bourses d'échange...

3.2.1.1. Comment marche une transaction via SWIFT

SWIFT est un réseau de messagerie que les institutions financières utilisent pour transmettre en toute sécurité des informations et des instructions par le biais d'un système de codes.

SWIFT attribue à chaque organisation financière un code unique qui a 8 caractères ou 11 caractères. Le code est appelé code d'identification bancaire (BIC), code SWIFT, SWIFT ID, ou code ISO 9362.3.

Pour comprendre comment le code est attribué, regardons la banque italienne *UniCredit Banca*, dont le siège est à Milan. Elle est dotée du code SWIFT de 8 caractères UNCRITMM.

- Les quatre premiers caractères correspondent au code de l'institut (UNCR pour *UniCredit Banca*)
- Les deux caractères suivants correspondent au code pays (IT pour Italie)
- Les deux caractères suivants correspondent à la location/code de ville (MM pour Milan)
- Les trois derniers caractères sont optionnels, mais les organisations les utilisent pour assigner des codes a des branches individuelles (La branche de la banque *UniCredit Banca* à Venise pourrait utiliser le code UNCRITMMZZZ)

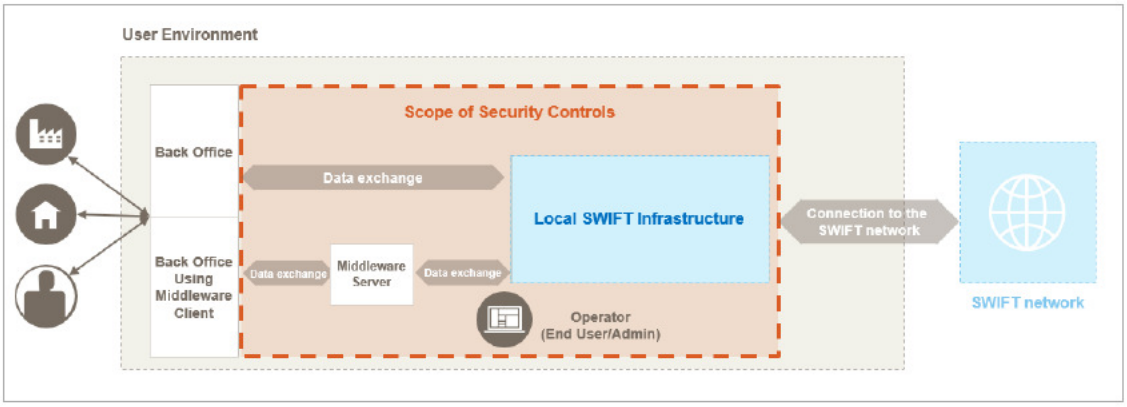
Supposons qu'un client d'une branche de la *Bank of America* à New York veut envoyer de l'argent à son ami qui est client à la branche UniCredit Banca de Venise. Le client new-yorkais peut entrer dans sa branche de la *Bank of America* avec le numéro de compte de son ami et le code SWIFT unique d'*UniCredit Banca* pour sa branche de Venise. *Bank of America* enverra un message SWIFT de transfert de paiement à *UniCredit Banca* sur le réseau SWIFT sécurisé. Une fois qu'*Unicredit Banca* reçoit le message SWIFT concernant le paiement entrant, il l'effacera et créditera l'argent sur le compte de l'ami italien.

Aussi puissant que soit SWIFT, gardez en tête que ce n'est qu'un système de messagerie. SWIFT ne détient aucun fond et ne gère aucune sécurité, ni de comptes clients.

3.2.2. La sécurité chez Swift

Swift met à jour chaque année un programme contenant des normes que chaque client devra mettre en place pour continuer à travailler avec SWIFT.

Ce programme est nommé **CSP** Swift (Customer Security Program) et contient une liste de normes nommée **CSCF** (Customer Security Control Framework) dont voici le périmètre de sécurité.



Par exemple, il faudra monter un Bastion CyberArk (Gestion des accès à privilèges comme les administrateurs), un SOC (Security Operations Center) pour faire de la surveillance globale sur le réseau. Actuellement, l'infrastructure de la société possède des failles réseau qu'il faut corriger, pour devenir compatible avec Swift.

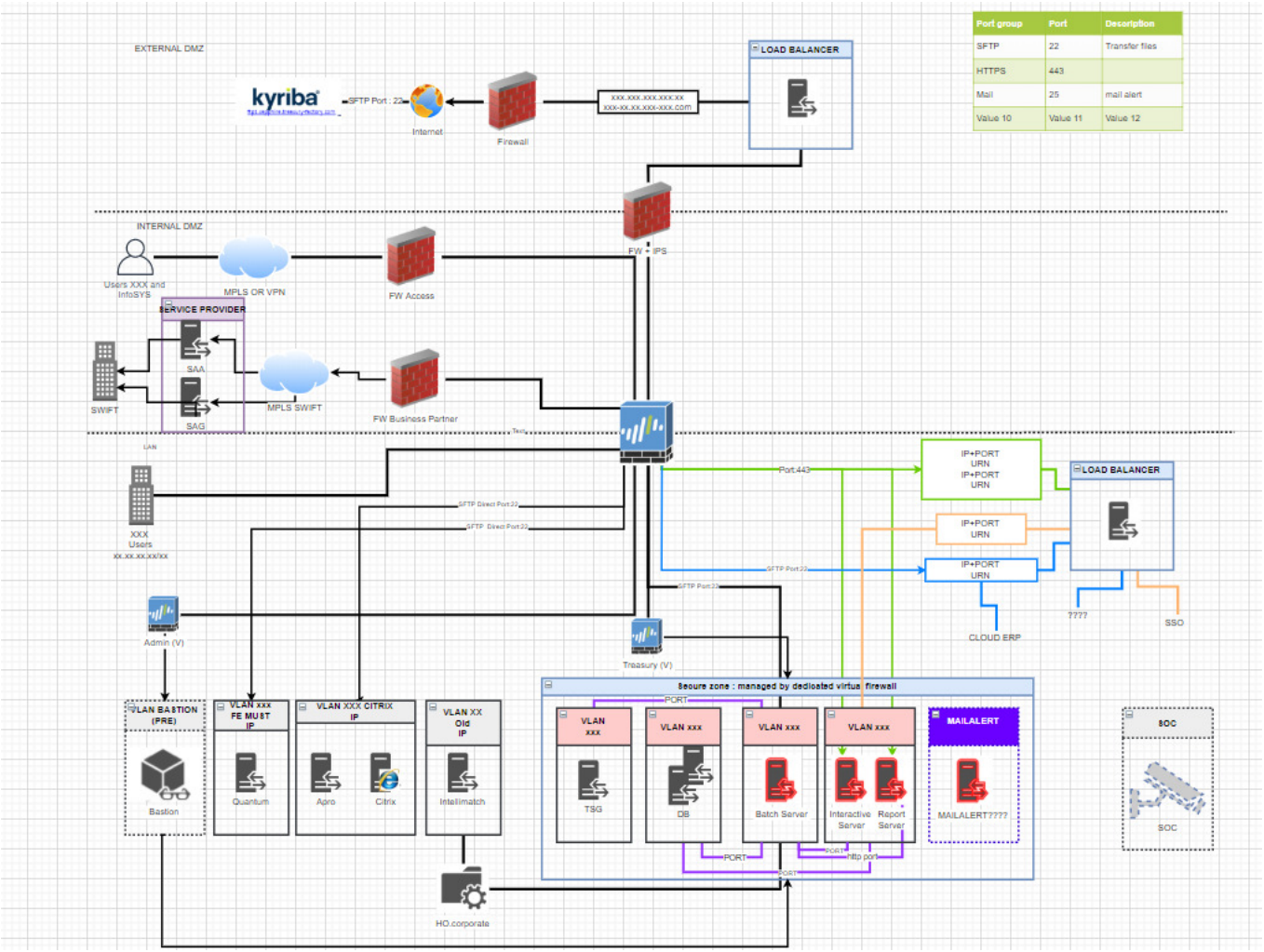
Pendant ma mission j'ai donc été chargé de faire des prototypes d'infrastructures correspondant aux nouvelles normes pour que mon maitre de stage puisse les proposer pendant ses réunions avec la pôle sécurité de l'entreprise cliente, corriger les éventuelles erreurs et discuter des nouvelles failles de sécurités dans le système actuel que nous aurions repéré. Je n'étais pas seul sur cette mission, j'ai travaillé avec Léo mon maitre de stage et Pierre, un collaborateur fraichement arrivé dans l'entreprise, en apprentissage « pentest » (repérage de failles par la simulation d'une cyber-attaque).

3.3. Architecture proposée pour répondre aux normes

Durant ce stage j'ai donc été chargé de conceptualiser la nouvelle architecture de l'entreprise pour répondre aux normes de SWIFT.

J'ai pour ça fusionné plusieurs documents comportant les architectures actuelles ainsi que les améliorations prévues pour 2020, et ai pu repenser une nouvelle architecture grâce à la liste de normes CSCF 2020

Voici le schéma final anonymisé (pas d'IP, pas de port, pas de VLAN aucun nom d'entreprise) pour ne pas dévoiler d'informations confidentielles, le schéma est donc moins explicite que dans sa version originale…



Ce schéma nous a permis d'avoir une base d'architecture sur laquelle se baser pour les audits, nous avons pu le proposer à l'équipe technique de notre client pour qu'elle le valide et y apporte des informations.

Dans les améliorations de sécurité nous pouvons noter l'ajout d'un centre de monitoring (surveillance réseau) externe : le ***SOC***, ainsi que d'un firewall particulier permettant la gestion des accès privilégiés (Admins) : ***Bastion***.

3.4. Les audits

Il m'a été donnée l'opportunité de participer à la planification et la réalisation d'audits lors de mon stage.

L'audit (informatique dans ce cas) a pour objectif d'identifier les différentes failles de sécurité dans une infrastructure et évaluer les risques liés aux activités de l'entreprise ou de l'administration sur ce réseau.

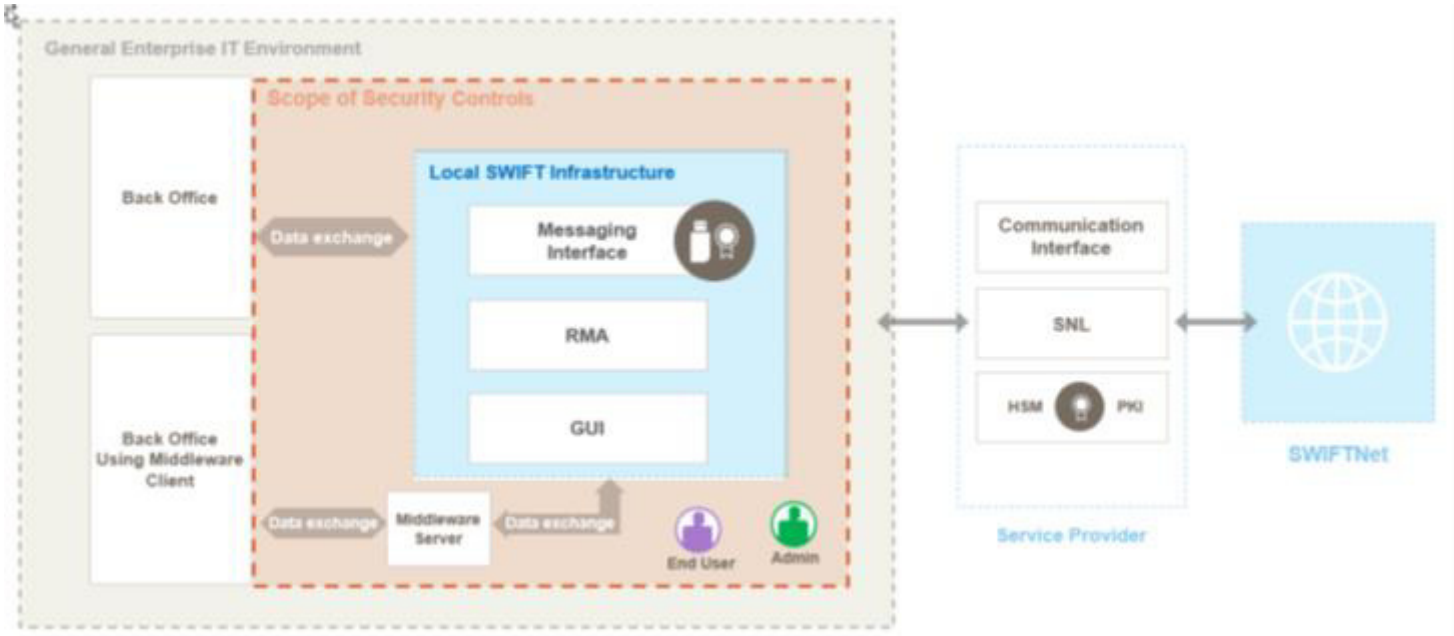
3.4.1. Le périmètre d'audit

L'audit réalisé par mon équipe encadre un certain périmètre, ici c'est une architecture A2 –

Architecture A2 :

L'utilisateur possède une interface de messagerie mais pas d'interface de communication, l'interface de communication est détenue par le fournisseur du service.

Le schéma ci-dessous explique le cas où l'utilisateur détient l'interface de messagerie mais pas celle de communication



De manière plus détaillée, voici les éléments composant le périmètre client à auditer :

Couche client

- 200 utilisateurs avec possibilité d'accès en remote et depuis les locaux
- Poste client sous Windows 7
- Serveur Windows 2008 R2 avec Citrix XenApp
- Mode dégradé avec poste dédié disposant d'un mode d'authentification avec token

Couche applicative

- Serveur TRAX payment virtuel sous Windows 2012 R2
- Serveur TRAX SWIFT Gateway sous Windows 2008 R2
- Interfaces d'échange interne et avec le Service Provider

Couche base de données

- Serveur AIX hébergeant une base de données ORACLE

Volet supervision et administration

- SOC
- Citrix / Cyberark

3.4.2 Les différentes portées d'audit

Voici la liste des portées d'audit préconisées par rapport au CSCF v2020 et au périmètre concerné par l'audit.

	Audit d'architecture	Audit de configuration	Audit organisationnel et physique	Tests d'intrusion
	Vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans le système d'information vis-à-vis de l'état de l'art et des exigences et règles internes de l'audité.	Vérifier la mise en œuvre de pratiques de sécurité conformes à l'état de l'art et aux exigences et règles internes de l'audité en matière de **configuration des dispositifs matériels et logiciels déployés dans le système d'information**.	S'assurer que **les politiques et procédures de sécurité définies par l'audité pour assurer le maintien en conditions opérationnelles et de sécurité du système concerné sont conformes** au besoin de sécurité de l'organisme audité, à l'état de l'art ou aux normes en vigueur.	**Découvrir les vulnérabilités** sur le système d'information audité et **vérifier leur exploitabilité et leur impact**, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un attaquant potentiel.
Restrict Internet access & Protect critical systems	✓	✓	✓	✓
Reduce attack surface and vulnérabilities	✓	✓	✓	✓
Physically secure the environment			✓	✓
Prevent compromise of credential		✓	✓	✓
Manage identities and segregate privileges	✓	✓	✓	✓
Detect anomalous activity	✓	✓	✓	✓
Plan for incident response			✓	✓

3.4.3 La planification des audits

Avec mon équipe, nous avons organisé diverses réunions pour planifier les audits, le but était simple, pour chaque point du CSCF 2020 (Voir définition plus haut) nous avons assigné un type d'audit et donc une équipe spéciale, ce tri nous permet d'avoir une organisation claire et une répartition des tâches.

Par exemple ici :

Priority 20	Priority 201	Security Cont	Chapi tr	Title	Control Objective		Équipe	Périmètre de l'audit	Responsable	Date de début	Date de livrable	Effort
Mand	Mandato	1. Restrict Internet Access & Protect Critical Systems from General IT Environ	1.1	SWIFT Environment Protection	A segregated secure zone safeguards the user's SWIFT infrastructure from compromises and attacks on the broader enterprise and external environments.	[redacted] é : Bruno Saerens comme contact a Emmanuel qui fera les tests pour les BT Finance. CyberArk. Tests sont pending rera la nouvelle plateforme -07 -07 prod mi septembre	CyberArk	orga + archi	[redacted]	1/16/2020	6/30/2020	

Pour le tout premier point les équipes « Audit de configuration » et « Audit organisationnel » seront en charge.

Une fois cette planification faite, nous avons donné rendez-vous au client pour une réunion « kick-off » permettant de vérifier que tous les points du contrat étaient respectés, et que l'audit allait se dérouler dans les règles de l'art.

4. Conclusion

Pour conclure, j'ai fait mon stage de fin d'études de Bachelor 1 en tant que stagiaire cyber sécurité au sein de l'entreprise Capgemini , lors de ce stage de 6 semaines j'ai pu apprendre de nouvelles compétences que je n'avais pas forcément développé pendant mon année scolaire ainsi que les appliquer dans diverses missions d'architecture ainsi que de planification d'audit.

Ce stage a été enrichissant pour moi car il m'a permis de découvrir une partie du grand domaine de la cyber sécurité, assez différente de la vision que l'on s'en fait habituellement, j'ai pu découvrir le domaine du consulting et de l'audit sécurité. Il m'a aussi permis de me rendre compte que les missions de consulting chez le client n'étaient pas les plus adaptées à mon profil, mais que la partie de sécurisation pourrait plus me correspondre.

A la fin de ma période de stage je me rends compte que si je devais m'orienter vers un poste ce serait probablement plus dans le domaine de la surveillance & détection d'intrusion ou dans la réponse aux incidents (voir pie chart dans le point 2.2.3)

Ce stage a été particulièrement constructif car il m'a permis d'avoir une représentation claire de la cyber sécurité, et de pouvoir me rendre compte de comment ce domaine fonctionne en entreprise, chose qui était assez floue pour moi jusque-là.

De plus, l'entreprise qui m'a accueilli à ce moment la traversait une période importante et travaillait sur un contrat intéressant, et je suis fier d'avoir pu y contribuer