RAPPORT DE STAGE

STAGE INGENIEURIE RESEAU ET INFRASTRUCTURE

NADIM KIFOUCHE

Stage de Licence – 2 Avril 2024 à 26 Juillet 2024 (4 mois)

Tuteur de stage : Wilfried Darragon
Enseignant Référent : Khalil Djelloul

Etablissement : Université d'Orléans
Entreprise d'accueil : EY France – La Défense

SOMMAIRE

REMERCIEMENTS

Je tiens tout d'abord à exprimer ma profonde gratitude envers Wilfried Darragon, mon superviseur de stage, pour son soutien constant, ses conseils éclairés et sa confiance en mes capacités tout au long de cette période de stage. Sa disponibilité, son expertise et sa bienveillance ont grandement enrichi mon expérience professionnelle et m'ont permis de progresser dans mes compétences.

Mes remerciements vont également à toute l'équipe Infra EY France, avec laquelle j'ai eu le privilège de travailler. J'aimerais aussi remercier Riadh Zid, Fabrice Arditti, Cedrik Kety, Lourderadge Covindarassou qui m'ont aiguillé tout au long du stage sur l'aspect technique, sur l'aspect administratif et aussi sur l'aspect humain. Mes remerciements vont également à l'équipe Cybersécurité, notamment Belhassen El Mekki, Oussem Zid et Youcef Boukhris.

Leur accueil chaleureux, leur esprit d'équipe et leur collaboration ont rendu mon intégration au sein de l'entreprise fluide et agréable. Je suis reconnaissant envers chacun des membres de l'équipe pour leur patience, leur encouragement et les précieux échanges que nous avons partagés.

Je souhaite exprimer ma reconnaissance envers mon professeur référent Monsieur Khalil Djelloul, pour sa disponibilité et sa réactivité. Ma profonde reconnaissance également à Madame Sophie Robert.

Je tenais également à remercier toute l'équipe pédagogique qui m'a permis d'acquérir toutes les connaissances nécessaires depuis ma première année de licence.

Mes remerciements vont également à l'ensemble du personnel de EY France ainsi qu'à toutes les personnes rencontrées au sein de l'entreprise, pour leur accueil bienveillant et leur contribution à mon expérience professionnelle.

INTRODUCTION

Au cours de ma formation universitaire à l'Université d'Orléans, j'ai eu l'opportunité d'effectuer un stage au sein de EY (anciennement Ernst & Young) dans le cadre de la validation de ma Licence Informatique parcours Ingénierie. Ce stage, d'une durée de 4 mois s'est déroulé du 2 Avril 2024 au 26 Juillet 2024 et a constitué une étape intéressante dans mon parcours académique et professionnel.

L'objectif principal de ce stage était de mettre en pratique les connaissances théoriques acquises au cours de mes études et de découvrir le fonctionnement concret d'une entreprise dans le domaine de l'IT. J'ai ainsi eu l'occasion d'observer de près les différentes facettes du métier d'Ingénieur Infrastructure et Réseau et les différents aspects qui tournent autour tels que la Sécurité ou encore le côté Administratif. J'ai pu ainsi contribuer activement aux missions qui m'ont été confiées telles que la mise en place d'un SIEM open-source, du scripting, du rackage de serveur et de switch ou encore de participer à l'élaboration de documents internes et externes.

Dans ce rapport, je vais tout d'abord présenter l'entreprise qui m'a accueilli en stage, en mettant en lumière son historique, son domaine d'activité et sa structure organisationnelle. Ensuite, je détaillerai les missions qui m'ont été assignées et les différentes tâches que j'ai accomplies au cours de cette période. Par la suite, j'analyserai les enseignements que j'ai tirés de cette expérience professionnelle, en mettant en avant les compétences développées et les défis rencontrés. Enfin, je conclurai ce rapport en dressant un bilan personnel et professionnel du stage, ainsi qu'en formulant si besoin quelques recommandations pour l'entreprise.

Ce stage a été pour moi une occasion précieuse de mettre en pratique mes connaissances, de développer de nouvelles compétences et d'explorer le monde professionnel dans le domaine qui m'intéresse. Je suis reconnaissant envers toutes les personnes qui m'ont accompagné et soutenu tout au long de cette aventure.

PRESENTATION DU STAGE

1. Présentation de EY France

1. Général

EY (aussi connu sous son ancien nom Ernst & Young) est un cabinet d'audit financier et de conseil. Membre du Big Four, il est le troisième réseau mondial au niveau de son chiffre d'affaires (après Deloitte et PwC) en 2020.

EY a été fondée en 1989. Les entreprises Ernst & Whinney et Arthur Young fusionnent pour créer Ernst & Young (EY) avec pour objectif de développer le secteur de l'Audit Comptable. Depuis sa création, elle s'est développée dans plusieurs autres domaines. Au fil des années, elle a su diversifier ses activités et s'adapter aux évolutions du marché pour devenir l'un des acteurs majeurs de son secteur.

Au travers de son réseau d'audit mondial, le cabinet EY propose une large palette de services aux entreprises à tout stade de leur développement : jeune entreprise innovante ou entreprise de taille intermédiaire (ETI), société familiale ou société cotée en Bourse. EY fournit des prestations d'audit financier, de conseil (systèmes d'information, ressources humaines, organisation, finance, stratégie…), de cabinets d'avocats (notamment sur les questions fiscales).

2. Une activité pluridisciplinaire de conseil développée

Spécialisée dans la certification des comptes, EY propose également des services de conseil fiscal, de conseil juridique, de conseil en stratégie et de maîtrise des risques. Ses équipes de spécialistes interviennent dans de multiples domaines d'expertise : droit social, droit des affaires, fiscalité, marketing, transaction, comptabilité, technologie, développement durable, etc. Le cabinet couvre l'ensemble des activités de management et aide ses clients à optimiser leur performance opérationnelle. Par ailleurs, la Fondation Ernst & Young soutient divers projets de mécénats en lien avec de grandes institutions culturelles.

3. Les métiers d'EY et leurs objectifs

L'expertise et la qualité des services offerts par EY ont pour objectif de créer les conditions de la confiance dans l'économie et les marchés financiers. La coordination de ces métiers représente un enjeu essentiel pour répondre aux demandes de ses clients, nécessitant d'allier des compétences multiples et complémentaires.

Afin de favoriser la transversalité, un Comité Exécutif veille à la coordination de l'ensemble des activités, permettant d'adopter une logique de marché dépassant la simple logique de métier.

Cette démarche est essentielle, pour deux raisons. D'une part elle permet de faire émerger des offres pluridisciplinaires en réponse aux besoins de leurs clients et, d'autre part elle permet de contrôler la bonne application de la législation et des règles propres à EY.

Le nombre important de métiers exercés et d'expertises présentes au sein du cabinet nécessite la mise en place d'outils pour identifier les collaborateurs disposant de compétences spécifiques et de partager les connaissances au sein de l'entreprise.

1. *Audit et Conseil Comptable*

- Aider les clients à répondre aux besoins de transparence et de fiabilité des informations.

2. *Financières et extra-financières*

- Valider à l'usage des tiers la qualité et la sincérité de l'information chiffrée.
- Accompagner les clients dans leurs problématiques comptables (normes, processus, opérations).
- Évaluer les dispositifs antifraude et anticorruption, enquêter sur les allégations et analyser les données.

3. *Conseil*

Aider les organisations à :

- Devancer un environnement en constante évolution.
- Capter et déployer l'ensemble des opportunités digitales.
- Transformer l'organisation pour améliorer sa performance.
- Maîtriser les risques pour créer de la valeur.

EY s'appuie sur une combinaison unique d'expertises sectorielles et de compétences pour faire face aux enjeux de nos clients.

4. *Fiscalité et Droit*

- Créer de la valeur de manière durable et responsable grâce à la conception et la mise en place de solutions juridiques et fiscales innovantes.
- Défendre les intérêts des clients dans un univers juridique et fiscal de plus en plus complexe.
- Identifier des solutions qui permettent aux clients d'atteindre leurs objectifs opérationnels tout en minimisant leurs risques.

5. *Transactions*

Aider les entreprises à :

- Optimiser et sécuriser le processus de vente ou d'acquisition.
- Évaluer des actifs corporels ou incorporels et valider les décisions stratégiques par la construction de modèles financiers.
- S'adapter à la compétition accrue et à des processus plus complexes et tendus en matière de croissance externe.
- Assurer la réussite opérationnelle post-acquisition des transactions.

6. *Les métiers de l'interne (Core Business Services (CBS))*

Les métiers de l'interne sont composés des directions Knowledge, Markets & Business Development, Marketing et Communication, Risque et Qualité, Ressources Humaines, Achats, Finance, Immobilier, Informatique, Juridique et Support administratif.

Elles contribuent au bon fonctionnement et au développement de l'activité (soutien dans la réponse aux appels d'offres et dans la réalisation des missions), au rayonnement de la marque EY, à l'information délivrée aux clients (conférences, petits déjeuners techniques) et au partage des connaissances.

Parmi ces 768 collaborateurs, une centaine travaille pour EY au niveau Europe ou Monde.

4. Activités par métier

Voici ci-dessous listées les activités par métier :

- Audit et conseil financier : certification des comptes, accompagnement des directions financières, lutte contre la fraude, audits environnementaux et sociaux…
- Conseil : Conseil en stratégie et data sciences, marketing et innovation, Conseil en management, Conseil en technologie…
- Transactions : évaluation des risques et opportunités et accompagnement des entreprises dans le cadre d'opérations telles que fusion, acquisition, reprise, cession ou restructuration.
- Fiscalité et Droit (EY Société d'Avocats) : fiscalité des entreprises, domestique et internationale, droit social, droit des affaires…
- Banque et marchés de capitaux (FSO) : un département transversal qui permet de répondre aux enjeux particuliers du secteur de la finance grâce à l'ensemble de nos compétences en audit, conseil, transactions, fiscalité et droit

5. Effectifs et autres chiffres (FY2018)

Avec une présence dans plus de 150 pays, EY est de nos jours une organisation mondiale considérable, qui emploie plus de 260 000 personnes, et dispose d'une quinzaine de bureaux en France. Le cabinet est l'auditeur de référence de plus de la moitié des entreprises du CAC40, ainsi que d'une multitude d'ETI et de PME françaises.

EY repose sur une gouvernance globale qui regroupe les 28 régions dans quatre grandes zones opérationnelles : Amériques, EMEIA (Europe, Moyen-Orient, Inde et Afrique), Asie-Pacifique, Japon.

Afin de garantir toujours plus de flexibilité, les équipes dirigeantes travaillent étroitement avec les responsables de leur zone opérationnelle ainsi que l'équipe de direction mondiale. Cette organisation transverse nous permet de prendre rapidement les décisions et d'assurer la cohérence dans le déploiement de notre stratégie, tout en garantissant à nos clients le même niveau d'excellence et la même constance dans la qualité de nos prestations partout dans le monde.

6. EY au sein des « Big Four »

EY, Deloitte, KPMG et PriceWaterhouseCoopers (PwC), britanniques ou américains, sont surnommés les "Big Four" (traduction littérale, les « quatre grands ») puisque ces quatre cabinets d'audit, présents dans le monde entier, sont des incontournables dans le monde des multinationales et de la finance et dominent le marché.

EY est le 1er en termes de gros mandats (contrat pour garantir que le service sera dans l'intérêt de l'entreprise), avec 22 mandats dans le CAC40 et le troisième réseau mondial en termes de chiffre d'affaires.

7. Exécutif Western Europe & Maghreb (WEM) et France

La région WEM, créée en 2017, comprend la France, les Pays-Bas, la Belgique, le Luxembourg, le Maghreb et l'Afrique Francophone. Elle compte 17 pays au total. Avec 2,4 milliards d'euros de chiffre d'affaires, dont 800 millions d'euros exportés dans le reste du réseau EY, 600 associés dont 300 en France et 12 000 collaborateurs, c'est actuellement la 3ème région d'EY dans le monde.

EY poursuit son mouvement d'intégration par un poids renforcé des régions pour accroître sa capacité d'investissement vers de nouvelles compétences et de nouvelles technologies et ainsi étendre l'offre de solutions à forte valeur ajoutée pour ses clients et la diversité des opportunités professionnelles pour ses collaborateurs.

2. Objectifs et sujet du stage

Au cours de mon stage au sein du pôle CBS (Core Business Services, pôle essentiel au bon fonctionnement de l'entreprise, intégrant par exemple les ressources humaines, l'IT..) de l'entreprise EY FRANCE, j'ai eu l'opportunité de participer activement à diverses missions, chacune visant à assurer le bon fonctionnement de l'infrastructure informatique d'EY France. Chaque tâche réalisée a contribué à la stabilité et à l'efficacité des environnements technologiques de l'entreprise. Par exemple, j'ai travaillé sur la maintenance et le décommissionnement de serveurs, ce qui impliquait la surveillance continue des performances, l'application de mises à jour critiques et la résolution de problèmes techniques complexes. J'ai également observé le projet de migration de données, garantissant ainsi une transition fluide et sécurisée entre différentes plateformes technologiques. En outre, j'ai appris quelles sont les stratégies lors de l'élaboration d'une infrastructure pour garantir par exemple la sauvegarde et la récupération des données (serveurs de back-up, réplication...) pour prévenir toute perte d'information cruciale. Ces missions m'ont permis de développer des compétences techniques approfondies, tout en me familiarisant avec les pratiques et les protocoles essentiels à la gestion des infrastructures IT dans un contexte professionnel de grande envergure. L'ensemble des missions réalisées a été documenté avec précision pour partager mes différents travaux au lecteur.

TRAVAIL REALISE

1. Détails des missions réalisées

Mission 1 – Décommissionnement des serveurs

Objectif : Formater de manière sécurisée les serveurs des sites de Strasbourg, Lille, Paris, Nice, Montpellier, Lyon, Marseille, Bordeaux, Tours et Nantes, en suivant une procédure standardisée pour garantir la sécurité des données et la conformité aux normes.

Outils utilisés :

1. Remote Desktop Connection Manager : Pour accéder aux serveurs à distance et effectuer les opérations nécessaires.

2. Fichier ISO fourni par Blancco (entreprise qui fournit l'ISO) : Utilisé pour le formatage sécurisé des disques durs des serveurs.

Étapes :

1. Connexion au Server Manager :
    - Utilisation d'un compte secondaire (pratique de sécurité) de l'Active Directory pour accéder à un Server Manager.
2. Accès aux machines via le navigateur :
    - Chaque machine possédait deux adresses IP : une pour la machine principale et une pour manager le hardware. Connexion effectuée via l'adresse de management (FRxxxxxxxxx-R).
3. Formatage des serveurs :
    - Utilisation de l'interface utilisateur de DELL pour monter l'ISO et redémarrer les serveurs sur celui-ci. L'interface est très simple d'utilisation.
    - Répétition de cette procédure pour chaque serveur à décommissionner.
4. Mise à jour du Change :
    - Un Change a été soumis pour chaque site concerné (bonnes pratiques fournies par ITIL, un ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information. Un Change est une demande importante d'action sur l'infrastructure, nécessitant

une validation par toutes les parties impliquées directement ou indirectement via ServiceNow (Interface de ticketing) pour garantir la sécurité et la synchronisation des équipes impliquées.

Améliorations apportées :

- Standardisation des procédures : Utilisation d'une méthodologie uniforme pour garantir la cohérence et la qualité du processus de décommissionnement.
- Respect des protocoles de sécurité : Utilisation de l'ISO fourni par Blancco pour assurer un formatage sécurisé des disques durs et la protection des données sensibles.
- Communication proactive : Informer les équipes concernées via le processus de Change afin de minimiser les perturbations et de garantir la collaboration entre les différentes parties impliquées.

Mission 2 – Patch des vulnérabilités sur certains serveurs

Objectif : Résoudre un incident signalé via ServiceNow, indiquant des vulnérabilités sur une liste de serveurs Microsoft en raison de mises à jour manquantes. Les informations sur les vulnérabilités ont été fournies par le GVM (outils remontant les vulnérabilités).

Outils utilisés :

1. Remote Desktop Connection Manager : Pour accéder aux serveurs à distance et effectuer les opérations nécessaires.

2. Le récapitulatif Excel associant les vulnérabilités aux serveurs.

Étapes :

1. Connexion au serveur Manager :
    - Utilisation d'un compte secondaire (pratique de sécurité, mot de passe généré par l'application TheVault) de l'Active Directory pour accéder à un chaque serveur.
2. Vérifications des mises à jour installées pour chaque serveur :
    - Accès à ***Control Panel -> Program and Features -> View Installed Update***.
    - Comparaison des mises à jour installées avec les informations fournies par le document récapitulant les vulnérabilités.

3. Ajout des mises à jour nécessaires :
    - Téléchargement des fichiers de mises à jour à partir du site de Microsoft.
    - Copie à distance des fichiers sur les serveurs et exécution des mises à jour.
4. Mise à jour de l'incident :
    - Mise à jour de l'incident pour indiquer que la vulnérabilité a été résolue et fermeture de l'incident.

Améliorations apportées :

- Patch des serveurs effectué, réduisant ainsi les vulnérabilités.
- Communication proactive : Notification de la résolution de l'incident pour informer les parties prenantes de la situation.

Mission 3 – Script PowerShell pour la détection d'antivirus

Objectif : Implémenter une solution pour EY Global qui permet de détecter si les serveurs français ne sont plus protégés par Symantec (Suppression du service réalisé par une autre équipe) mais protégé par Windows Defender (Changement Global pour l'antivirus des serveurs).

Outils utilisés :


1. Visual Studio, outil classique de développeur.
2. PowerShell_ISE présente toutes les commandes de l'Active Directory et une CLI où ont pu être fait les différents tests.
3. Documentation Windows Powershell.

Étapes :

1. Consultation des documentations nécessaires :
    - Apprentissage de commande de base pour manipuler l'Active Directory.
    - Consultation de la documentation Microsoft pour comprendre les meilleures pratiques et les procédures recommandées.

2. Implémentation :
    - Implémentation de la solution pour automatiser la vérification des serveurs.
    - Test d'utilisation pour s'assurer du bon fonctionnement de l'automatisation.
3. Test :
    - Test de fonctionnement avec la vérification sur une sélection de serveurs représentatifs pour valider l'efficacité de l'automatisation.
4. Communication :
    - Communication de la réponse à l'équipe ayant formulé la demande, en leur fournissant un rapport détaillé sur les serveurs concernés.

Améliorations apportées :

- Automatisation d'une tâche longue et fastidieuse, réduisant ainsi le temps et les efforts nécessaires pour effectuer la vérification manuellement.
- Communication proactive : Informer l'équipe des serveurs qui ont toujours le service Symantec installé ou qui n'ont pas le service Microsoft Defender activé, leur permettant ainsi de prendre des mesures correctives si nécessaire.
- Ajout d'une étape de consultation de la documentation Microsoft pour garantir la conformité aux meilleures pratiques et aux recommandations de sécurité.
- Inclusion d'une phase de test pour vérifier le bon fonctionnement de l'automatisation avant la communication des résultats à l'équipe demandeuse.

Mission 4 – Rédaction d'un Accord Interne de Service

Objectif : Établir des règles claires concernant le support technique entre les parties EY Local (le support Audio-Visuel et les Ingénieurs) et Business pour les conférences (et autres événements) organisées pour les clients.

Outil utilisé :

1. Word, éditeur de texte. 

Étapes :

1. Discussion avec les équipes concernées :
    - Prendre des notes sur les remarques et les exigences de chaque équipe afin de les intégrer dans l'accord.
2. Mise en place d'un plan logique :
    - Elaboration d'un plan logique détaillé pour la rédaction de l'accord, en tenant compte des besoins et des préoccupations de toutes les parties concernées.
3. Rédaction :
    - Rédaction précise de l'accord, en veillant à protéger l'équipe de support interne en spécifiant clairement les responsabilités et les processus à suivre en cas de problème. Éviter les zones d'ombres et clarifier les termes et les conditions.
    - Vérification régulière avec les responsables pour corriger et affiner les détails tout au long du processus d'écriture.
4. Communication :
    - Présentation de l'accord aux différentes parties concernées pour examen et validation.
    - Signature par les différentes parties une fois que toutes les modifications ont été convenues et intégrées.

Améliorations apportées :

- Clarification des responsabilités : Détailler clairement les responsabilités de chaque partie pour éviter les malentendus et les conflits futur.

Mission 5 – Renforcement des règles de filtrage du Firewall de l'environnement de l'équipe Infra (Palo Alto et FortiGate).

Objectif : Après une analyse de la part de l'équipe Cybersécurité, l'équipe Infra a renforcé le filtrage afin d'être moins vulnérable.

Outils utilisés :

1. Interface Palo Alto (Firewall entrées).
2. Interface FortiGate (Firewall sorties).

3. Utilisation de Whois.

Étapes :

1. Analyse des intrusions :
    - Analyse des différentes intrusions ou tentatives.
    - Prise en note des différentes failles.
2. Mise en place de nouvelles règles :
    - Mise en place de nouvelles règles de sécurité afin de renforcer le filtrage.
3. Mise en place d'alerte :
    - Mise en place d'alerte par mail aux équipes dédiées.
    - Envoi de logs au serveur SIEM. Le serveur SIEM permettra le rapport et l'analyse des différents logs (MISSION 7).
4. Communication :
    - Communication des changements aux équipes Cyber et Infra.

Améliorations apportées :

- Renforcement de la sécurité de nos Firewalls.
- Mise en place d'alertes.

Mission 6 – Mise en place d'un SIEM pour l'environnement de l'Infrastructure.

Objectif : Mise en place d'un puits de logs et analyse de ses données pour pouvoir surveiller le Palo Alto, le FortiGate ainsi que la mise en place d'agents EDR (surveiller et bloquer l'accès pour des serveurs qui n'ont pas de Syslog) sur l'Active Directory et d'autres serveurs pour l'environnement de l'Infra.

Outils utilisés :

1. vSphere afin de créer une Virtual Machine Linux qui hébergera le SIEM.
2. Serveur de rebond Windows, car le serveur Linux n'a pas d'interface.
3. Putty, pour se connecter (SSH).

4. Wazuh qui est un logiciel de substitution de Splunk, gratuit et open-source contrairement à ce dernier (préféré car moins cher, rapport besoin/prix avantageux).

Étapes :

1. Collecte des logs :
    - Mise en place d'envoi de Syslog (Push) pour le Palo Alto et le FortiGate. Mise en place d'un agent sur le serveur Active Directory.
    - Création de la connexion entre le SIEM et les différents équipements.
    - Mise en place d'agent sur certains servers sensibles de l'environnement.
2. Décodage des informations :
    - Traduction entre les différents formats de logs afin de pouvoir corréler les informations.
3. Mise en place de visualisation :
    - Utilisation des différentes fonctionnalités de Wazuh afin de créer des visualisations intégrant toutes les différentes machines monitorées.
    - Création des visualisations selon les besoins.
4. Mise en place de Dashboard :
    - Création de Dashboard en fonction de différents aspects à surveiller.
5. Définition des groupes :
    - Création des différents groupes Users, Administrateurs et Créateurs. Gestion des droits de ses différents groupes afin de gérer la sécurité du serveur.
6. Mise en place de l'alerte :
    - Mise en place d'alertes par le biais d'un serveur SMTP.

Améliorations apportées :

- Mise en place d'un moyen de surveillance des différents éléments vulnérables de l'infrastructure.
- Economie avec l'utilisation d'une solution gratuite contrairement à Splunk (10k€ les 10 Go de log).
- Analyse efficace des besoins car Wazuh est très intéressant d'un point de vue rapport qualité/prix pour un petit environnement.

Mission 7 – Inventaire des salles VDI (Switch internet à chaque étage).

Objectif : Vérification des conformités et de l'état des différents racks dans les salles VDI du 12ème au 28ème et du RDC.

Outil utilisé :

1. Command Prompt afin de tester la connexion des différents UPS (onduleurs) au réseau. 

Étapes :

1. Vérification des normes :
    - Vérification de la conformité des différents branchements entre les fibres, les commutateurs et les onduleurs.
2. Vérification de l'onduleur :
    - Vérification de son état en consultant les logs, du fonctionnement des alertes.
3. Documentation :
    - Prise en note de l'état des différents racks.
    - Mise en place d'un tableau récapitulatif.
4. Communication :
    - Communication du responsable de l'Infrastructure de la tour.

Améliorations apportées :

- Suivi des différentes salles VDI et mise à jour de leurs états.
- Communication aux responsables.

Mission 8 – Automatisation de la création des groupes d'accès pour l'équipe d'Analyse.

Objectif : Automatisation de la création des groupes et de dossiers, automatisation de l'accès à ces dossiers, maintien automatique des groupes, suppression automatique des dossiers.

Outils utilisés :

1. OneAccess est la manière standard de créer des groupes d'accès (pour n'importe quelle équipe).
2. Un langage de développement (indéfini).

Étapes :

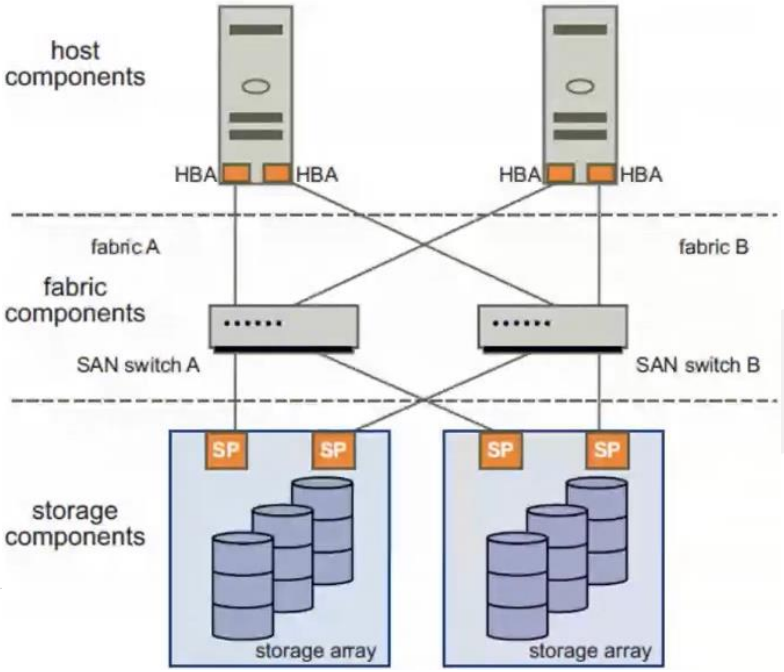
1. Réunion :
    - Réunion pour comprendre les besoins et les attentes de l'équipe GDS
    - En attente d'informations au niveau supérieur hiérarchique.

2. Outils techniques

1. L'Hyperconvergence remplace le SAN.

a. Le SAN : une solution qui tend à disparaître.

Le SAN (Storage Area Network) est un réseau spécialisé qui permet de regrouper et de gérer les ressources de stockage à l'échelle d'un datacenter, offrant un accès rapide et fiable aux données pour les serveurs.



Il utilise des protocoles comme Fibre Channel ou iSCSI pour des transferts de données à haute vitesse. Les principaux inconvénients du SAN sont son coût élevé, sa complexité d'installation et de gestion, ainsi que la nécessité de compétences spécialisées pour le maintenir. De plus, les SAN peuvent être moins flexibles et évolutifs par rapport à d'autres solutions de stockage modernes comme les infrastructures hyperconvergées telles que celles proposées par Nutanix.

Coût élevé de gestion :

- Nécessite la gestion de tous les SLA (Service Level Agreements) des fabricants.
- Obligation de maintenir des contrats de maintenance avec chaque fabricant.
- Frais administratifs et de suivi supplémentaires pour assurer la conformité et les performances des contrats.

Complexité d'installation :

- Gestion de multiples interfaces de différents fabricants.

- Problèmes potentiels d'intégration et de compatibilité entre les systèmes (ESXI).
- Besoin de connaissances spécialisées pour chaque technologie utilisée.

Moins de flexibilité :

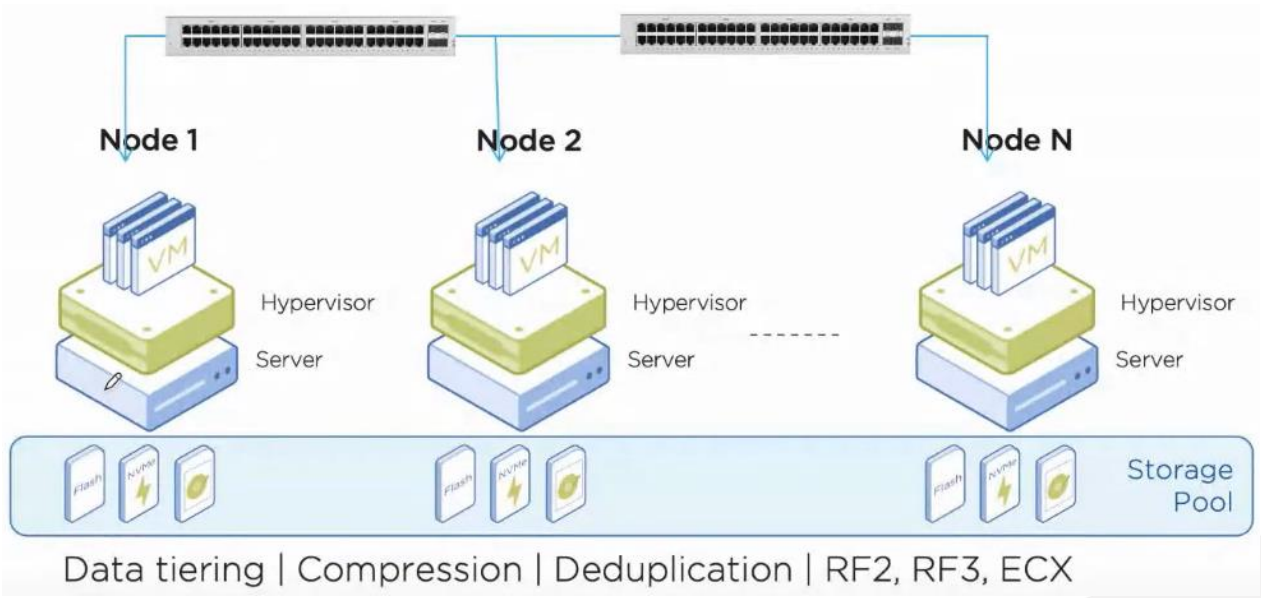
- Capacités ressources limitées pouvant entraîner une extension impossible.
- Difficulté à adapter rapidement les systèmes aux nouvelles exigences ou aux changements du marché.
- Restrictions imposées par les différents fabricants sur les mises à jour et les extensions.

Ces points montrent pourquoi le SAN, autrefois la solution privilégiée, tend à être remplacé par des infrastructures hyperconvergées comme celles de Nutanix, offrant plus de simplicité, de flexibilité et de rentabilité.

b. Hyperconvergence.

L'hyperconvergence est une approche moderne de l'infrastructure informatique qui intègre de manière étroite le calcul, le stockage et la mise en réseau dans une seule solution logicielle, souvent hébergée sur du matériel standardisé. Cette architecture unifiée simplifie considérablement la gestion des centres de données en éliminant le besoin de systèmes de stockage et de réseaux distincts, tout en offrant une plus grande flexibilité et une évolutivité aisée. Les infrastructures hyperconvergées permettent une gestion centralisée via une interface unique, réduisant ainsi les coûts opérationnels et les efforts de maintenance.

En utilisant des technologies avancées de virtualisation, l'hyperconvergence permet aux entreprises de déployer et de gérer facilement des ressources informatiques selon leurs besoins, en optimisant l'utilisation des ressources et en garantissant une haute disponibilité des applications. De plus, elle facilite l'adaptation rapide aux exigences changeantes du marché, rendant les entreprises plus agiles et réactives.



c. Performance et redondance : RAID

Le RAID (Redundant Array of Independent Disks) est une technologie de stockage qui combine plusieurs disques durs en une seule unité logique afin d'améliorer la performance, la redondance des données, ou les deux. En répartissant les données sur plusieurs disques, le RAID permet de renforcer la tolérance aux pannes et d'optimiser les vitesses de lecture et d'écriture.

Il existe plusieurs niveaux de RAID, chacun offrant un équilibre différent entre performance, capacité et protection des données :

- RAID 0 (Striping) : Améliore la performance en répartissant les données sur plusieurs disques, mais sans redondance, donc aucune protection contre les pannes.
- RAID 1 (Mirroring) : Duplique les données sur deux disques ou plus, offrant une haute disponibilité et une tolérance aux pannes au détriment de la capacité de stockage totale.
- RAID 5 (Striping with Parity) : Combine la performance et la redondance en répartissant les données et les informations de parité sur trois disques ou plus. En cas de panne d'un disque, les données peuvent être reconstruites.
- RAID 6 (Striping with Double Parity) : Similaire au RAID 5, mais avec une double parité, permettant de tolérer la panne de deux disques simultanément.

Les principales limitations du RAID incluent la complexité de configuration et de gestion, ainsi que les coûts potentiels liés à l'acquisition de plusieurs disques. De

plus, malgré la redondance, le RAID n'est pas une solution de sauvegarde en soi, car il ne protège pas contre la corruption des données ou les attaques malveillantes. Toutefois, le RAID reste une technologie clé pour améliorer la fiabilité et la performance des systèmes de stockage.

d. Nutanix : une solution.

Nutanix est une entreprise technologique spécialisée dans les infrastructures hyperconvergées, fournissant des solutions de cloud hybride et multicloud. Fondée en 2009, Nutanix propose une plateforme logicielle qui intègre le calcul, le stockage et la virtualisation dans une solution unique et simplifiée, permettant aux entreprises de moderniser leurs centres de données et de faciliter la gestion de leurs environnements informatiques. Les clients peuvent ainsi déployer et gérer des applications à grande échelle avec une flexibilité accrue, qu'elles soient hébergées sur site, dans un cloud public ou dans une configuration hybride. En somme, Nutanix permet aux entreprises de gagner en agilité et en réactivité, tout en optimisant les coûts et en améliorant la performance globale de leur infrastructure informatique.

2. Active Directory

a. Qu'est-ce que Active Directory ?

Active Directory (AD) est une technologie de service de répertoire développée par Microsoft pour les environnements Windows. Il joue un rôle central dans la gestion des réseaux d'entreprise, offrant une manière centralisée et sécurisée de gérer les utilisateurs, les ordinateurs, les groupes, et bien d'autres objets réseau.

Active Directory est une base de données et un ensemble de services conçus pour permettre aux administrateurs de gérer les permissions et l'accès aux ressources réseau de manière efficace. Les services AD offrent une infrastructure hiérarchique pour stocker des informations sur les objets du réseau, facilitant la gestion de ces objets de manière centralisée.

b. Les domaines

Un domaine est un groupe logique d'objets au sein d'Active Directory, partageant une base de données commune. Les domaines sont les principales unités organisationnelles dans AD, offrant une frontière de sécurité et de gestion. Chaque domaine possède son propre ensemble de règles et de politiques, ainsi qu'un contrôleur de domaine (DC) responsable de l'authentification et de la gestion des objets.

- **Contrôleurs de domaine (DC)** : Serveurs qui répondent aux demandes d'authentification et appliquent les politiques de sécurité du domaine.
- **Relations d'approbation** : Permettent aux utilisateurs de différents domaines d'accéder aux ressources des autres domaines, facilitant la collaboration et l'interopérabilité au sein d'une entreprise.

c. La réplication

La réplication est un processus clé dans Active Directory, garantissant que toutes les modifications apportées à la base de données AD sur un contrôleur de domaine sont répliquées sur les autres contrôleurs de domaine dans le même domaine ou dans d'autres domaines de la forêt.

- **Réplication intra-site** : Se produit entre les contrôleurs de domaine au sein d'un même site, optimisée pour la vitesse.
- **Réplication inter-site** : Se produit entre les contrôleurs de domaine situés dans des sites différents, optimisée pour minimiser la bande passante du réseau.

d. L'authentification

L'authentification dans Active Directory est le processus de vérification de l'identité des utilisateurs et des ordinateurs qui tentent d'accéder au réseau. AD utilise plusieurs protocoles d'authentification pour garantir la sécurité :

- **Kerberos** : Protocole d'authentification par défaut, offrant une authentification mutuelle et des tickets pour accéder aux services réseau.
- **NTLM** : Protocole de secours utilisé pour la compatibilité avec les anciens systèmes.
- **LDAP (Lightweight Directory Access Protocol)** : Utilisé pour interroger et modifier les objets dans AD, essentiel pour les opérations de recherche et de gestion des objets.

e. Group Policy Objects (GPO)

Les Group Policy Objects (GPO) sont des ensembles de configurations définies par les administrateurs pour gérer les environnements des utilisateurs et des ordinateurs au sein d'un domaine Active Directory. Les GPO permettent d'appliquer des politiques de sécurité, de déployer des logiciels, de configurer les paramètres système, et bien plus encore.

- **Application des GPO** : Les GPO sont appliqués aux utilisateurs et aux ordinateurs via des liens vers des unités organisationnelles (OU), des sites ou des domaines.

- **Hiérarchie des GPO** : Les GPO sont appliqués dans un ordre spécifique (Local, Site, Domaine, OU), et les paramètres peuvent être hérités ou remplacés en fonction de la configuration des GPO.
- **Éditeur de GPO** : Outil utilisé par les administrateurs pour créer et gérer les GPO, offrant une interface centralisée pour définir les politiques.

En conclusion, l'Active Directory (AD) est un service de répertoire développé par Microsoft qui centralise et simplifie la gestion des ressources réseau. Il permet aux administrateurs de contrôler les utilisateurs, les groupes, les ordinateurs et les permissions depuis un emplacement unique. AD améliore la sécurité grâce à des mécanismes d'authentification robustes comme Kerberos, et permet l'application cohérente de politiques de sécurité via les Group Policy Objects (GPO). De plus, l'Active Directory est hautement évolutif.

ANALYSE - PERSPECTIVES

Avoir pu travailler avec des personnes expérimentées et compétentes m'a permis de progresser, de comprendre et d'apprivoiser le métier. C'est-à-dire que tout au long du stage, certains aspects, certains termes qu'ils soient techniques ou non m'ont paru moins obscurs. En tant que junior, ce stage m'a permis de démystifier le fonctionnement d'une grosse entreprise, le fonctionnement des hiérarchies et l'application des compétences techniques.

Le stage réalisé au sein d'EY m'a ouvert les yeux sur l'étendue des outils et du jargon informatique. J'ai découvert que l'informatique est un domaine très vaste et parfois complexe. Cet aspect est particulièrement intéressant car il offre de nombreuses opportunités d'apprentissage, suggérant que la "routine" pourrait potentiellement ne pas exister à l'avenir, si on le souhaite.

J'ai éprouvé beaucoup de plaisir à travailler avec deux équipes différentes durant mon stage. J'ai d'abord collaboré avec l'équipe Cybersécurité, puis avec l'équipe Infrastructure. J'aime tous les domaines de l'informatique, c'est pourquoi j'imagine me diriger vers la cybersécurité à l'avenir. Pour cela, il est nécessaire d'être un informaticien complet. Les discussions et les interactions que j'ai eues m'ont beaucoup enrichi. Le domaine de la cybersécurité est vaste, passionnant et très sensible. Il implique beaucoup de responsabilités, ce qui me plaît car j'aimerais avoir une vie professionnelle dynamique, notamment grâce à la gestion des risques.

La polyvalence requise pour une carrière en cybersécurité me motive également. Se former comme Pentester pour devenir ensuite Risk Manager est une carrière qui m'intéresse, tant pour son évolution que pour le panel de compétences que j'acquerrais avec le temps. L'aspect sensible de ce domaine me plaît énormément. La gestion critique des données, la sécurisation des serveurs et le consulting me passionnent.

Le domaine de l'intelligence artificielle est un domaine qui m'intéresse fortement aussi. Après plusieurs discussions au sein de l'équipe Infra mais aussi à l'extérieur (Cybersécurité, DevOps), j'ai appris que le Python devenait fondamental. Mon idéal serait de travailler dans la sécurité au sein d'une entreprise d'intelligence artificielle. Ce stage a été bénéfique à ce niveau car mon le chemin s'est dégagé.

J'ai compris qu'il est essentiel de posséder des compétences en management, car se limiter uniquement à l'aspect technique peut être insuffisant. Dans le domaine de l'informatique, être techniquement compétent est crucial, mais savoir gérer des équipes, communiquer efficacement et prendre des décisions stratégiques l'est tout autant. Par exemple, le rôle d'un professionnel en cybersécurité ne se limite pas à identifier et résoudre des problèmes techniques. Il implique également de coordonner des équipes, de gérer des projets, et de communiquer clairement avec différents acteurs, y compris ceux qui ne sont pas spécialisés en informatique. Développer ces compétences managériales est indispensable pour progresser dans une carrière en cybersécurité et assumer des responsabilités plus importantes, telles que celles d'un Risk Manager. La mondialisation et par la même occasion la compétitivité des étrangers sur le marché du travail augmente significativement la concurrence, ce qui nous oblige à développer à terme des qualités managériales.

Le stage m'a également permis d'ajouter des contacts à mon annuaire personnel. Des membres de l'Infra et du Cyber qui ont été satisfaits de mon passage, m'ont gardé en contact, ce qui me sera utile à l'avenir notamment pour mon stage de deuxième année dans mon futur master.

Le stage et le domaine d'étude universitaire est cohérent. Cependant, la licence Informatique parcours ingénierie est très théorique. Par exemple en réseau, j'ai acquis beaucoup de compétences applicatives durant le stage comme l'utilisation de Firewall (mise en place de policies Palo Alto par exemple), la connaissance de nouveaux protocoles ou encore le fonctionnement de l'hyperconvergence. Cette licence m'a permis d'acquérir des bases solides, que j'ai pu mettre à contribution pendant mon stage.

CONCLUSION

Récapitulation des tâches et des responsabilités :

Lors de mon stage chez EY, j'ai participé à plusieurs missions cruciales. J'ai sécurisé et décommissionné des serveurs sur plusieurs sites en utilisant des outils comme Remote Desktop Connection Manager et des fichiers ISO sécurisés de Blancco. J'ai résolu des vulnérabilités sur des serveurs Microsoft en appliquant des patchs manquants. J'ai implémenté un script PowerShell pour détecter la protection antivirus sur les serveurs français. J'ai rédigé un Accord Interne de Service pour clarifier les responsabilités entre les équipes techniques et business. J'ai renforcé les règles de filtrage des firewalls Palo Alto et mis en place un SIEM pour surveiller l'infrastructure, notamment avec Wazuh pour l'analyse des logs. Enfin, j'ai effectué un inventaire des salles VDI, vérifiant la conformité et l'état des équipements réseau et UPS, en communiquant régulièrement les mises à jour aux responsables. J'ai eu la chance d'effectuer des missions diverses qui ont renforcé ma compréhension des aspects techniques et managériaux.

Acquisitions de compétences et connaissances :

Au cours de mon stage chez EY, j'ai acquis et renforcé plusieurs compétences et connaissances clés :

1. Compétences Techniques :

Gestion de serveurs : Maîtrise des outils comme Remote Desktop Connection Manager pour accéder à distance et gérer les serveurs, ainsi que l'utilisation de fichiers ISO pour le formatage sécurisé. Manipulation de l'Active Directory et de tout l'environnement Windows en général.

Sécurité informatique : Application de pratiques de sécurité strictes pour le décommissionnement des serveurs, patching des vulnérabilités, et renforcement des règles de filtrage des firewalls Palo Alto.

Automatisation : Développement de script PowerShell pour la détection des antivirus sur les serveurs, automatisant ainsi des tâches répétitives et fastidieuses.

Mise en place de SIEM : Installation et configuration de Wazuh pour la collecte et l'analyse des logs, permettant une surveillance proactive de l'infrastructure.

2. Compétences en Gestion de Projet :

Rédaction de documents officiels : Création d'un Accord Interne de Service, nécessitant des compétences en communication et en rédaction pour clarifier les responsabilités entre différentes équipes. Création de documentation pour les futurs utilisateurs de mes différents projets.

Standardisation des processus : Mise en place de méthodologies uniformes pour garantir la cohérence et la qualité des procédures de décommissionnement et de mise à jour des serveurs.

3. Compétences en Communication :

Communication proactive : Information régulière des parties prenantes sur les changements et les résolutions de problèmes, assurant ainsi la transparence et la collaboration entre les équipes.

Documentation et reporting : Maintien de documents détaillés sur l'état des équipements et les interventions réalisées, facilitant le suivi et la gestion des infrastructures.

4. Compétences Managériales :

Gestion des incidents : Coordination de la résolution des incidents signalés via ServiceNow, incluant la mise à jour des statuts et la fermeture des incidents après résolution.

Évaluation des risques : Analyse des intrusions et mise en place de nouvelles règles de sécurité, démontrant une capacité à anticiper et à atténuer les risques.

Expérience significative :

La mise en place du SIEM a été l'expérience la plus significative car j'avais la responsabilité de surveiller un environnement sensible. De plus, cela m'a permis d'explorer une grande variété de domaine de l'informatique et de comprendre le fonctionnement d'un environnement. Techniquement, j'ai dû décoder les logs pour pouvoir les mutualiser (log parser au préalable). J'ai aussi placé des agents sur des serveurs, j'ai programmé des rapports et aussi analyse les alertes. J'ai aussi mis en place des Dashboard et gérer les différents groupes d'utilisateurs, qui peuvent être de simples utilisateurs (read only) mais aussi des administrateurs.

Future carrière :

Pour mon futur, ce stage m'a persuadé de continuer avec le Master ARIAS (Application répartie, Intelligence Artificielle et Sécurité) à l'Université d'Orléans. Après avoir présenté la maquette aux collègues de travail et après avoir réfléchi et analysé, j'ai décidé de poursuivre avec ce Master car il permet de se former et d'acquérir beaucoup de compétences techniques. J'ai aussi remarqué pendant le stage que l'Intelligence Artificielle était une question majeure dans le pôle innovation (question autour de COPILOT, prix des licences, question autour de la sécurité des informations...). Les discussions avec le responsable de la cybersécurité étaient aussi intéressantes car on a parlé des métiers de ce domaine. Le Développement est en général un point fort des Pentesters. Il faudra redoubler d'efforts pour acquérir le plus de compétences et de capacités pour être le plus opérationnel possible à la sortie du master. A propos de l'anglais, c'est un axe sur lequel je dois fournir des efforts car j'ambitionne bien plus loin que les frontières nationales.

Expérience enrichissante :

D'un point de vue général, ce stage a été enrichissant pour moi sur bien des aspects. J'ai pu travailler avec une équipe très sympathique avec laquelle j'ai noué des liens amicaux. J'ai beaucoup appris au niveau relationnel comme le comportement à tenir avec les différentes personnes selon leurs hiérarchies. J'ai appris à prendre des initiatives et cela m'a été permis grâce à mon équipe et à mon responsable qui étaient très ouverts d'esprit. J'ai compris aussi à quel point la cohésion d'équipe est importante. Mon responsable était très soucieux à ce niveau. De plus, j'ai remarqué qu'il y avait des conflits d'intérêts entre les différentes équipes ce qui m'a fait comprendre le caractère intransigeant du travail.

En conclusion, ce stage m'a non seulement permis de développer des compétences techniques et managériales, mais aussi de grandir personnellement en améliorant ma capacité à collaborer et à communiquer efficacement. Les leçons apprises ici resteront gravées dans ma mémoire et guideront mes futures expériences professionnelles. Je suis reconnaissant pour cette opportunité et pour l'accueil chaleureux et le soutien constant de mes collègues et de mon responsable. Cette expérience m'a conforté dans mon choix de carrière et m'a donné la motivation nécessaire pour poursuivre mes études et mes aspirations professionnelles avec confiance et détermination.

ANNEXE

La liste des documents (également cliquable) :