MASTER ROC

Réseau & Objets Connectés

Mémoire d'activité

Auteur : Saïfeddine Kilani
Alternant au sein d'**IP Twins**
Assistant **Rssi /** Administrateur **Réseau** et **Cybersécurité**
Tuteur : Éric DEWITTE | RSSI & Directeur Technique – IP Twins

PROBLÉMATIQUE : Performance et sécurité : Comment rester performant au sein d'une infrastructure traitant des données critiques, soumise à de fortes contraintes de disponibilité et à des interactions avec des acteurs à forts enjeux, tout en respectant ses engagements de cybersécurité, tel que l'ISO27001 ?

Ce mémoire s'inscrit dans un parcours de recherche, d'apprentissage et de réalisations techniques plus vaste. D'autres travaux, projets et publications sont à retrouver sur : saifeddine-kilani.fr

Table des matières

Remerciements

Comme le souligne un célèbre dicton espagnol, « Trois, s'aidant l'un l'autre, sont suffisants pour faire le travail de six », l'entraide est un acte des plus nobles. C'est donc tout naturellement qu'avant de débuter, je tenais à dédier une page de ce mémoire d'alternance pour toutes les personnes qui m'ont aidé et permis de pouvoir exercer ma passion à plein temps.

Sans surprise, c'est à mes parents que la première partie est consacrée. Je pourrais facilement disserter et ce durant des centaines de lignes mais pour faire simple, merci infiniment pour tout ce que vous m'avez donné, c'est grâce à vous que j'en suis là et que je peux vivre cette vie des plus désirables.

Si les mots confiance et bienveillance avaient une définition physique, ce serait sans doute IP Twins. Nombreux savent que recruter un alternant non majeur et sans aucune expérience concrète dans ce domaine est un pari des plus risqués. Cependant, j'ai été accepté là où nombreux ont été refusés, c'est donc naturellement que je remercie tous mes collègues d'entreprise et mon tuteur qui accepte de partager son savoir avec moi.

C'est avec mes ami(e)s et mes professeurs que je vais finir cette parenthèse des plus importantes. Comme je dis souvent, une personne est définie entre autres par son environnement. C'est donc en partie grâce à eux si je suis ici aujourd'hui.

C'est sur ces belles phrases que je vais commencer à vous rapporter le contenu de cette année d'alternance.

Introduction

''Comprendre'', j'ai toujours eu envie d'apprendre du monde qui m'entoure et des dynamiques profondes de ce dernier. Que ce soit le fonctionnement des ondes radio d'une simple voiture télécommandée que j'avais reçue à un anniversaire de ma jeunesse, ou, de nos jours, le fonctionnement des technologies d'alignement des IA pour mieux les contrôler, les réflexions sur la base de ce qui m'entoure ont été source d'apprentissage, toujours dirigées vers une même envie : ''comprendre''.

Après une scolarité en cursus général, j'ai vite perçu les limites techniques de cette formation.

J'ai alors pris une décision ambitieuse : me lancer en alternance dans l'informatique dès l'âge de 15 ans et poursuivre ce chemin jusqu'au doctorat, afin d'allier savoir-faire pratique de haute qualité et connaissances théoriques aiguisées.

Cette ambition s'est concrétisée avec la signature de mon contrat chez IP Twins, une entreprise qui m'a toujours accordé sa confiance et qui m'accompagne encore aujourd'hui. Elle m'a vu obtenir mon bac, décrocher mon BTS, valider ma troisième année d'étude en cybersécurité. Ce chemin continu de combler son caractère inattendu à cet instant ; celui d'une entrée en Master dans l'appréciable établissement qu'est le CNAM et qui je m'en réjouis d'avance, ne m'exonérera en rien quant à l'effort réclamé pour parachever mes études.

Ayant depuis peu cultivé l'idée selon laquelle ne peut naître un mouvement clair sans idée claire, le Master Roc paracheva ma volonté de continuer l'apprentissage des sciences et connaissances informatiques sans permettre aucun compromis sur le plan théorique. Ce Master me permet d'acquérir des connaissances précises sur, les liens fondamentaux et complexes que sont les réseaux qui lient les objets connectés, la clé de voute qu'est devenue la cybersécurité tant elle est devenue indispensable pour ne serait-ce qu'une simple présence sur internet et en fin, l'intelligence artificielle qui est subitement devenu sujet à tant de logorrhées intellectuelles.

Bien du chemin et du temps s'en est passé depuis que j'ai rejoint IP Twins. Arrivé fraîchement et naïvement au poste d'assistant technicien avec peu de connaissance informatique, j'ai multiplié les formations et lectures de documentations.

J'ai travaillé et exécuté sans relâche, dans un premier temps des tâches d'exécutant, jusqu'à acquérir un socle de connaissances et les compétences suffisantes pour évoluer au sein de cette entreprise. Technicien réseau, technicien supérieur, assistant administrateur, administrateur et aujourd'hui dans une fonction d'assistant RSSI.

Gestion et sécurisation de notre parc serveur, assistance technique pour mes collègues, déploiement de politiques de sécurité, campagne de sensibilisation, certification de notre infrastructure au normes nationales et internationales : j'ai acquis, traité et exécuté une masse de données et de connaissances qui m'ont permis de bâtir l'arborescence de mes connaissances.

C'est conscient de la chance que j'ai eue de faire les bonnes rencontres professionnelles et scolaires qu'aujourd'hui, je vous délivre ce travail avec toute la passion qui est la mienne, le tout dans la volonté que ce document ne soit qu'un pavé du chemin qui m'est destiné et qui ne fait que commencer.

Et rien de mieux pour débuter ce rapport qu'établir l'objectif de ce dernier à travers cette question, performance et sécurité : Comment rester performant au sein d'une infrastructure traitant des données critiques, soumise à de fortes contraintes de disponibilité et à des interactions avec des acteurs à forts enjeux, tout en respectant ses engagements de cybersécurité, tel que l'ISO27001?

Partie I/ Mon entreprise : IP Twins

1. Présentation d'IP Twins

Créée en 2002, IP Twins est un bureau d'enregistrement de noms de domaine dédié aux titulaires de marques et à leurs représentants, ainsi qu'une société de protection des marques en ligne. IP Twins a son siège à Paris et des filiales à Hong Kong et Singapour, ainsi que des antennes à Manille et en Espagne.

Depuis sa création, IP Twins n'a cessé d'évoluer avec un capital social de 41 050 € et un chiffre d'affaires en 2020 de 2 103 249 €. Elle peut aussi compter sur ses 13 employés qui sont répartis en 8 juristes, 3 IT et enfin 2 directeurs.

Mû par un sens relationnel aigu, IP Twins cultive une vision humaine du métier. IP Twins veut avant tout fournir à ses clients des conseils pertinents et des services sur mesure tout en conservant la qualité d'échanges que l'on est en droit d'attendre de juristes spécialisés. Les entreprises à la recherche d'un partenaire avec une expertise avérée de la gestion des noms de domaine et des solutions de protection de marque en ligne choisissent IP Twins pour les aider à sécuriser et défendre leur présence en ligne, à surveiller les contrefacteurs, et faire respecter leurs droits de propriété intellectuelle sur Internet.

IP Twins travaille constamment pour développer des technologies et des méthodes assurant la fiabilité et la précision dans l'administration des noms de domaine et la protection des marques des clients. C'est pourquoi IP Twins a développé différents outils spécifiques, dont Identitool, Similaritool, Domainarium et Detective :

- Identitool : Recherche gratuite de noms de domaine identiques à une marque dans toutes les extensions.
- Similaritool : Recherche de domaines similaires ou contenant une marque à l'échelle mondiale.
- Domainarium : Plateforme pour gérer facilement tous les noms de domaine via une interface unique.
- Detective : Outil de surveillance anti-contrefaçon détectant les domaines proches ou identiques à une marque, dans toutes les extensions.

Nous avons une certaine expertise de la propriété intellectuelle et du digital. Nous proposons des offres de service exhaustives, la disponibilité de notre équipe pour fournir des solutions sur mesure et de portée mondiale. Cela fait de nous un atout précieux dans le paysage numérique.

IP Twins est un membre actif de plusieurs associations professionnelles sur les sujets de PI et Internet.

Certains membres de notre équipe sont panélistes devant le Centre d'Arbitrage et de Médiation de l'Organisation Mondiale de la Propriété Intellectuelle, pour leur expérience substantielle dans les domaines du droit de la propriété intellectuelle, du commerce électronique et d'Internet.

La vocation d' IP Twins est restée la même : fournir des solutions et services de qualité aux experts juridiques, qu'ils soient en entreprise ou en cabinet. Nous accompagnons également les agences de branding.

2. Organisation et environnement de travail

Au sein d'un marché où la compétition fait rage, IP Twins a réussi à se forger une solide réputation. L'entreprise assure avec brio le pilotage des noms de domaine, la sécurisation digitale, la protection des marques sur internet et les services DNS les plus avancés. De grandes marques comme le PSG, Carrefour ou Veolia lui font entièrement confiance, signe que des sociétés importantes lui confient des enjeux majeurs liés à leur image numérique et à leur sûreté.

Installée à Paris, IP Twins évolue au cœur d'un environnement numérique pointu. Elle collabore avec des entreprises spécialisées en cybersécurité, des cabinets d'avocats, des bureaux d'enregistrement internationaux et des créateurs de solutions de surveillance et de détection.

Grâce à cette collaboration, ainsi qu'à sa participation active à des salons et événements professionnels, l'entreprise maintient un haut niveau d'innovation et d'expertise.

IP Twins s'organise autour de divers axes opérationnels, chacun étant pointu dans son domaine:

La Direction Générale : menée par le fondateur, qui se tient aussi au courant des dernières tendances technologiques et supervise la conception des produits.

Le Pôle Technique : dirigé par Éric Dewitte, notre Directeur Technique, et inclut l'équipe de développement interne, ainsi que moi-même en tant qu'administrateur réseau.

L'équipe des Affaires Juridiques est composée d'experts en droit de la propriété intellectuelle. Leur mission est la gestion des contentieux et la rédaction de rapports (actions en justice...).

La collaboration est fluide, avec des échanges constants entre les différents pôles, notamment pour harmoniser les interventions relatives aux dossiers clients ou face à des cas complexes, généralement au cours de réunions qui se tiennent tous les deux jours.

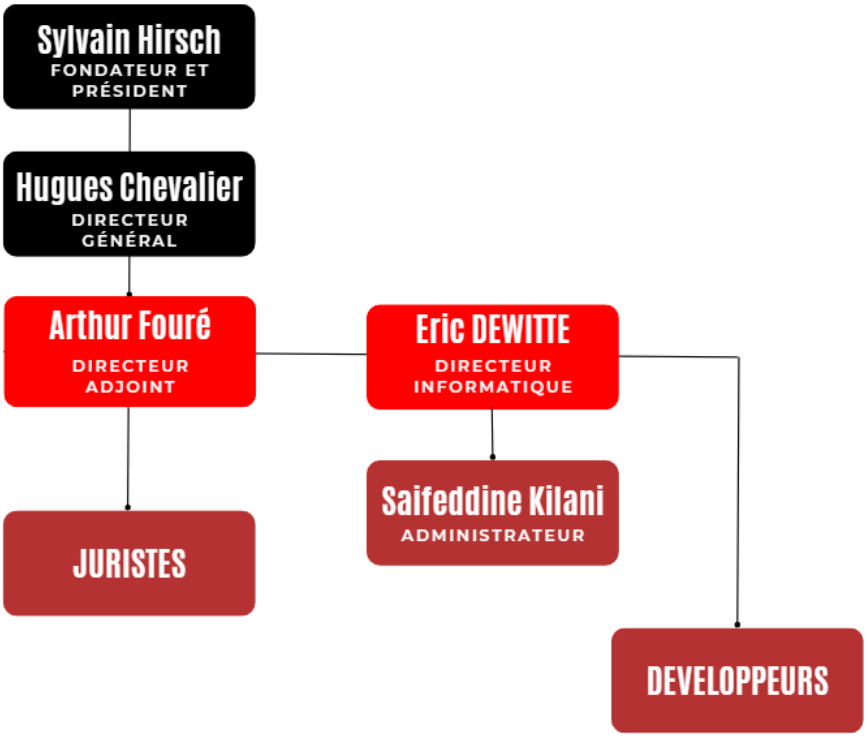


Figure 1 : *Organigramme simplifié d'IP Twins*

Chez IP Twins, le style de gestion repose sur une culture axée sur la responsabilisation, l'assurance et l'expertise technique. On incite chaque membre de l'équipe à s'impliquer activement dans son rôle, à suggérer des perfectionnements et à faire des choix judicieux dans son domaine de compétence. Cette indépendance s'allie à un environnement structuré et à un soutien continu, en particulier de la part des chefs de département et du Directeur Technique.

L'organisation demeure ouverte et interdisciplinaire, encourageant la communication entre les divers départements (technique, juridique, commercial), ce qui est crucial pour une entreprise engagée dans des questions aussi variées que la protection des marques ou la cybersécurité DNS.

Comme vous allez pouvoir le constater, mon travail à IP Twins a été divers. Sous la tutelle du directeur technique, j'ai exercé cette année des tâches d'administrateur et d'assistant RSSI.

J'ai été chargé d'assurer le bon fonctionnement, la sécurité et la performance des systèmes d'information d' IP Twins, j'ai notamment fait des tâches de type administration des systèmes ou j'ai installé, configurer et mis à jour les systèmes d'exploitation et les logiciels serveurs. J'ai aussi géré une quarantaine de serveurs, en assurant leur disponibilité, leur performance et leur mise à jour.

Il y a aussi eu de la gestion des réseaux : administration d'équipements réseau (switches, routeurs, firewalls). Assurer la sécurité et la supervision du réseau et participer à l'architecture réseau et à son évolution sont des missions que j'ai souvent effectuées.

Dans le cadre de la sécurisation de notre parc informatique, j'ai fait le suivi de mise en place des politiques de sécurité (antivirus, pare-feu, droits d'accès), de la gestion des sauvegardes, de la restauration des données et en fin de la sécurité des systèmes dans le cadre de la certification ISO 27001.

Il y a eu également quelques tâches de support technique et apports divers telles que : assurer un support aux utilisateurs et configurer des nouveaux postes et suivre des mises à jour sur les postes des collaborateurs.

Dans l'optique de l'amélioration continue de notre SI, j'ai proposé des améliorations pour optimiser les performances et la sécurité (type GLPI, IDS, chiffrages, …, lors de la certification ISO 27001 en 2024).

3. Présentation du tuteur et encadrement professionnel

Mon tuteur au sein d'IP Twins est Éric Dewitte, RSSI de l'entreprise et administrateur systèmes et réseaux depuis sa création en 2004. Il assure la gestion et le maintien en conditions opérationnelles et sécurisées du système d'information.

Ses missions couvrent notamment la cybersécurité, la gestion des risques cyber, le suivi des dispositifs de sécurité, le pilotage de la certification ISO 27001 ainsi que la préparation de l'entreprise aux futures exigences de la directive NIS2.

Depuis maintenant plusieurs années au sein d'IP Twins, j'ai l'opportunité de travailler à ses côtés sur des sujets variés liés à l'administration systèmes et réseaux, à la cybersécurité et à la gestion des infrastructures. Cet accompagnement me permet de développer progressivement mon autonomie, mes compétences techniques ainsi qu'une vision plus globale des enjeux opérationnels et de sécurité liés à l'activité de l'entreprise.

4. Analyse stratégique

IP Twins est une société spécialisée dans la gestion de noms de domaine (registrar) et la protection des marques sur Internet.

Fondée en 2002 par un ancien conseil en propriété industrielle, l'entreprise opère principalement en Europe, en Asie et en Afrique du Sud.

Quelques chiffres :

- Chiffre d'affaires : ~3 M€, en croissance constante.
- Effectif : 21 collaborateurs.
- Portefeuille clients : une centaine de comptes principaux.

IP Twins possède 3 objectifs stratégiques avec une croissance interne par développement de nouveaux services mais également, une volonté de diversification de la clientèle (corporate et cabinets d'avocats).et enfin la poursuite de l'internationalisation (Espagne en projet).

L'entreprise est reconnue pour sa participation active à des salons professionnels internationaux (INTA, ECTA), renforçant sa crédibilité.

4.1 Analyse du marché

Le marché est vaste, complexe et concurrentiel : toutes les entreprises ont des besoins en gestion de noms de domaine et protection des marques.

On remarque une fidélité élevée des clients, peu enclins à changer de prestataire, ce qui permet une forme de stabilité. On peut aussi apercevoir grâce à différents indicateurs un mouvement de consolidation du secteur. La segmentation limitée par produits ou zones géographiques est aussi à noter.

L'accent semble être mis sur une forme de prudence budgétaire des entreprises, que ce soit pour s'offrir une forme de stabilité ou préparer de futurs investissements. Comme pour tous les secteurs, il y a une inexorable montée des enjeux liés de près ou de loin à la cybersécurité.

Cela se traduit de différentes façons, dont la volonté des acteurs de ce marché de ne collaborer qu'avec des acteurs sécurisés donc certifiés. Il y a aussi un nouveau cycle de candidatures ouvert par l'ICANN (Internet Corporation for Assigned Names and Numbers) pour créer de nouveaux noms de domaine génériques de premier niveau (plus communément appelés extensions, tels que .app, .tech, .paris, etc.).
Les clients sont principalement de grands comptes internationaux et des cabinets d'avocats spécialisés en propriété intellectuelle.

Il y a aussi d'autres entreprises, plus ou moins grosses. Elles sont clientes d'IP Twins suite à des appels d'offres ou contact en commun.
Les Attentes clés sont divers:

- Expertise technique et juridique.
- Réactivité et accompagnement personnalisé.
- Haut niveau de sécurité et conformité.

4.2 Analyse concurrentielle, PESTEL et SWOT

Sur le marché français, IP Twins évolue dans un environnement concurrentiel composé d'acteurs bien établis, chacun avec des positionnements spécifiques. Parmi eux, Nameshield se distingue par un ancrage fort dans la cybersécurité, proposant des solutions de protection renforcées contre les menaces numériques. Gandi, quant à lui, adopte une approche plus résolument technique, en se concentrant principalement sur les services d'hébergement et de gestion de noms de domaine, avec une clientèle orientée vers les utilisateurs autonomes et les développeurs.

À l'échelle internationale, des entreprises comme CSC et ComLaude figurent parmi les principaux concurrents. Elles offrent des services de gestion de portefeuille de noms de domaine pour de grands groupes, en mettant l'accent sur la standardisation, la conformité et la gestion centralisée à grande échelle.

Dans ce paysage concurrentiel, IP Twins se distingue par plusieurs atouts majeurs :

Une double expertise juridique et technique : L'entreprise allie la maîtrise des aspects techniques liés à la gestion des noms de domaine avec une connaissance approfondie des enjeux juridiques en matière de propriété intellectuelle et de lutte contre la contrefaçon numérique.

Une organisation agile : Grâce à sa taille et à sa structure flexible, IP Twins est en mesure d'adapter rapidement ses solutions aux besoins spécifiques de ses clients, en offrant un accompagnement sur mesure.

Une réputation solide et reconnue, renforcée par l'obtention de certifications exigeantes telles que l'ISO 27001, qui attestent de son engagement en matière de sécurité de l'information et de protection des données.

Environnement macro (PESTEL)

Facteur PESTEL	Éléments clés
Politique / Réglementaire	- Mise en œuvre de la directive NIS2, renforçant les obligations de cybersécurité des entreprises.- Application continue du RGPD, encadrant la protection des données personnelles, y compris dans la gestion des noms de domaine.
Économique	- Contexte de rationalisation budgétaire dans les entreprises, poussant à optimiser les dépenses numériques.- Nouvelle opportunité commerciale avec l'ouverture d'un nouveau round ICANN (création de nouveaux gTLDs).
Technologique	- Renforcement permanent des mesures de cybersécurité, avec une demande croissante en solutions de protection de marques et noms de domaine.
Socioculturel / Environnemental	- Impact socioculturel et environnemental limité, du fait d'une clientèle exclusivement B2B et de services essentiellement numériques.

L'équipe IP Twins est organisée par métiers : développement, administrateurs systèmes, account management. L'ensemble de ces services travaillent en collaboration, le tout piloté par un Managing Director.

IP Twins possède des ressources matérielles et immatérielles, on peut citer les bureaux à Paris, Genève, Hong Kong, Singapour, les marques déposée dans plusieurs juridictions mais aussi une certification ISO 27001.

Les finances sont qualifiables de saines, ainsi elles permettent l'investissement.

Les compétences clés qui sont prisées chez IP Twins sont l'expertise unique technique et juridique, une maîtrise des process ICANN mais aussi une réputation internationale.

IP Twins se positionne de manière stratégique comme un acteur qui se dit intermédiaire, occupant une place des plus importantes entre deux types d'acteurs qu'on retrouve

traditionnellement sur ce marché : d'un côté, les pure players techniques spécialisés dans la gestion opérationnelle des noms de domaine et des infrastructures numériques ; de l'autre, les cabinets de conseil en propriété intellectuelle (PI), davantage orientés vers les aspects juridiques, réglementaires et stratégiques de la protection des marques.

Ce positionnement hybride et novateur permet à IP Twins d'offrir une proposition de valeur unique, en combinant une expertise technique avancée avec une compréhension fine des enjeux juridiques liés à la propriété intellectuelle. Cette double compétence renforce la capacité de l'entreprise à accompagner efficacement ses clients, aussi bien sur le plan technique que stratégique, et constitue un véritable facteur de différenciation sur un marché où les compétences sont souvent cloisonnées.

SWOT

Forces	Faiblesses
Expertise combinée juridique et technique	Taille plus modeste que les leaders mondiaux
Certification ISO27001	Visibilité limitée auprès du grand public
Bonne rentabilité	Dépendance relative à un nombre restreint de clients
Réputation solide	
Présence internationale	
Opportunités	**Menaces**
Nouveau round ICANN	Consolidation du marché et concentration accrue
Demande croissante de cybersécurité	Concurrence renforcée des acteurs anglo-saxons
Diversification de la clientèle	Pression budgétaire des entreprises
Sensibilité accrue au risque de Phishing	

4.3 Positionnement stratégique d'IP Twins

Notre feuille de route stratégique s'articule autour de cinq priorités. Premièrement, nous enrichissons notre offre pour les clients existants avec des services complémentaires (audit, veille, formation, cybersécurité) tout en consolidant notre position de partenaire global. Deuxièmement, nous diversifions notre clientèle en ciblant les cabinets d'avocats et les multinationales.

Troisièmement, nous valorisons notre différenciation unique : double expertise technique/juridique et certification ISO27001. Quatrièmement, nous anticipons les évolutions réglementaires comme la NIS2. Enfin, nous accélérons notre internationalisation avec l'Espagne et le renforcement de nos positions en Asie et Afrique du Sud.

Cette stratégie combine croissance, innovation et excellence opérationnelle pour consolider notre leadership dans la protection des marques en ligne.

PARTIE II — ACTIVITES PROFESSIONNELLES ET MISSIONS REALISEES

Mission 1 — Automatisation des mises à jour et intégration…

C'est avec passion que me vient la rédaction de cette partie. Ce projet, au-delà d'être très instructif, est la matérialisation même de mon engagement et du temps passé au sein de mon entreprise. C'est non seulement le premier projet que j'ai été amené à réaliser en autonomie, mais aussi celui que je n'ai cessé d'améliorer depuis mon arrivée. Il s'est autant nourri de moi que moi de lui, dans le sens où c'est à travers ce dernier que j'ai acquis certaines connaissances importantes quant à la gestion de ce genre de mission, et ce projet a été bien des fois amendé pour répondre aux problématiques et besoins qui n'ont cessé d'évoluer depuis sa création. J'ose espérer que la lecture des paragraphes suivants vous retransmettra non seulement l'évolution technique qui a été la mienne, mais bien l'évolution sur le fond comme sur la forme de mon socle de compétences et de connaissances.

1. Contexte de la mission

Peu de temps après le début des cours, on m'a chargé de la gestion d'un parc serveurs. En effet, mon tuteur a décidé que j'allais devenir responsable d'une partie des serveurs. Ainsi, je vais notamment être celui qui va s'occuper de tout ce qui touche, de près ou de loin, aux mises à jour.

Pour la petite explication, une partie des serveurs qui m'ont été attribués servent à prendre des captures d'écran sur demande de clients de leur produit de site dits marketplace comme Amazon, AliExpress, Le Bon Coin…, afin d'ensuite communiquer des informations aux juristes qui vérifieront avec ces clients si les produits en question sont réellement ceux des clients ou des contrefaçons vendues par une personne non autorisée. C'est ce qu'on appelle la surveillance de marketplace et la protection d'image de marque.

C'est donc à partir de ce gain de responsabilité que chaque début de semaine en entreprise, je passais une journée dans le meilleur des cas, voire plus, à faire la mise à jour des serveurs sous ma responsabilité.

Après plusieurs mois à faire ces tâches, notamment de mise à jour, le constat était le suivant : si je passe une semaine par mois à faire des mises à jour, en deux ans, je perds trois mois à faire des tâches peu intéressantes et très répétitives. Ce temps peut être qualifié de perdu quand je vois ce que je pourrais faire. C'est à partir de cela que m'est venue l'idée de rendre automatique les mises à jour de ce parc serveur afin de récupérer ce temps et de l'investir ailleurs.

2. Analyse des besoins et objectifs

Cette automatisation peut voir le jour car nous avons estimé que ces serveurs n'étaient pas critiques et simple à remettre en place en cas de problème dû à des mise à jours problématiques.

À partir de là, nombreuses furent les options et idées, mais avant d'aller plus loin, comme pour tout projet de cette importance, il me fallait établir le cahier des charges afin de clairement savoir ce qui m'est demandé. Ici, les demandes étaient relativement simples : mettre à jour les serveurs, s'assurer que cela s'est bien passé et tenir une liste des applications, services et autres choses qui ont été mis à jour. Cette dernière étape est importante car elle nous permet d'avoir un historique précis et un inventaire plus ou moins détaillé de ce qui a été mis à jour, quand cela a été mis à jour et par qui.

C'est ainsi qu'en cas d'éventuel problème, nous pourrons être en capacité de déterminer si cela a un lien avec une des mises à jour ou autre. À une époque, la liste se tenait sur un fichier Excel mais depuis que mon entreprise a passé la certification ISO 27001, nous avons revu nos process et la chose s'effectue maintenant sur GLPI, idée que j'ai amenée pour centraliser ce genre de tâches.

Pour résumer, les serveurs devront être mis correctement à jour, ensuite il faut mettre sur GLPI le contenu de ces mises à jour.

Il restait à ce stade une source de réflexion : comment s'assurer, sans avoir à se connecter sur GLPI et aller dans les bons tickets, que les mises à jour ont correctement eu lieu ? C'est ainsi que m'est venue l'idée aussi de mettre en place un envoi de mail, aussi automatisé, afin d'avoir un récapitulatif de chaque serveur pour savoir si tout a été correctement mis à jour. Après mûres réflexions avec mon tuteur, les mises à jour automatiques pourraient être faites le samedi soir car c'est le moment où les serveurs sont les moins utilisés. Une fois le lundi arrivé, je pourrais vérifier que tout est correctement fait à travers le récapitulatif par mail.

3. Développement de la solution automatisée

Maintenant que le contexte est clairement établi, que le projet a été présenté à mon tuteur et validé et qu'un environnement de test m'a été octroyé, quelque chose d'évident reste à résoudre : comment faire cela ? Non seulement au début de ce projet je n'avais pas les compétences techniques nécessaires, mais en plus bien des solutions différentes étaient possibles.

C'est ainsi que pendant plusieurs jours, majoritairement en autodidacte mais aussi avec l'aide de mon tuteur, j'ai entrepris le chemin de la formation.

J'ai lu des dizaines et des dizaines de documentations, consulté de nombreux sites, visionné toujours plus de vidéos pour enfin avoir une idée un peu plus claire de comment j'allais faire cette mission.

Les serveurs à ma disposition étant sur un système d'exploitation Debian, j'ai décidé d'utiliser le langage par défaut de ce système, le Bash. Cela tombe bien : la machine sur laquelle est hébergée GLPI est aussi sur Debian. Bash est l'interpréteur de commandes principal sous Linux. Il sert à exécuter des commandes système, automatiser des tâches avec des scripts, gérer les fichiers, processus et configurations, contrôler et administrer le système via la ligne de commande.

C'est ainsi un outil essentiel pour tout utilisateur Linux. Une fois le langage choisi pour mon programme d'automatisation, j'étais en capacité de mettre à jour avec ce programme les serveurs et de localiser et extraire les informations souhaitées, le contenu de ce qui a été mis à jour, et de tout mettre dans un même fichier.

Voici à quoi ressemblait le programme à ce moment :

```
#!/bin/sh
apt-get update > rep1
apt-get upgrade -y > rep2
more /var/log/dpkg.log | grep "status installed" > rep3
cat /etc/hostname /home/saif/rep1 /home/saif/rep2 /home/saif/rep3 >> /home/saif/rep4
```

Figure 2 : Un aperçu d'une partie du programme à ce stade.

Maintenant, il me fallait trouver un moyen de m'envoyer ces informations par email pour avoir mon récapitulatif et les envoyer aussi sur GLPI. J'ai donc poursuivi mes recherches pour trouver une solution d'envoi par mail. C'est ainsi que j'ai utilisé la commande mail.

Celle-ci permet d'envoyer des mails avec, si l'on souhaite, le contenu d'un fichier quelconque comme corps du mail. Ainsi, en utilisant cette méthode, je pourrais envoyer ces mails de récapitulatif en utilisant le fichier généré comme corps du mail. Cela me permet de répondre

directement à cette volonté d'avoir un rapport de ce qui se passe.

C'est donc décidé, j'ajoute cette commande à mon programme. La réalité est que l'utilisation de cette commande demande l'installation de certains paquets et autres, ainsi que leur configuration. Dans mon cas, les serveurs avaient déjà les installations et configurations nécessaires, ce qui m'a permis de ne pas avoir à les faire moi-même.

À ce stade, j'avais déjà résolu une grande partie des problématiques et demandes initiales. Il restait cependant deux problèmes majeurs, dont comment faire pour que le programme se lance automatiquement sans aucune intervention humaine à une intervalle régulière.

Si je n'arrive pas à trouver comment faire cela, le projet perd sa pierre angulaire, à savoir d'être automatique. Après d'autres recherches et l'intervention de mon tuteur pour m'accompagner et m'aider dans la conception de ce programme, j'ai appris qu'il était possible d'automatiser le lancement de programme grâce à un fichier qui s'appelle CRON. Il suffit simplement d'ajouter une ligne en indiquant la périodicité souhaitée et quel programme est concerné. Ainsi, je venais de trouver comment automatiser le lancement du programme de mise à jour. Comme vu auparavant, ce programme sera exécuté tous les samedis soir pour des raisons de charge de travail réduite des serveurs à ce moment.

Donc si l'on résume, à ce stade, je suis en capacité de générer des fichiers qui contiennent des informations concernant ce qui a été mis à jour, ensuite je suis en capacité de m'envoyer le contenu de ces fichiers par mail afin d'avoir un rapport de ce qui a été ou non mis à jour.

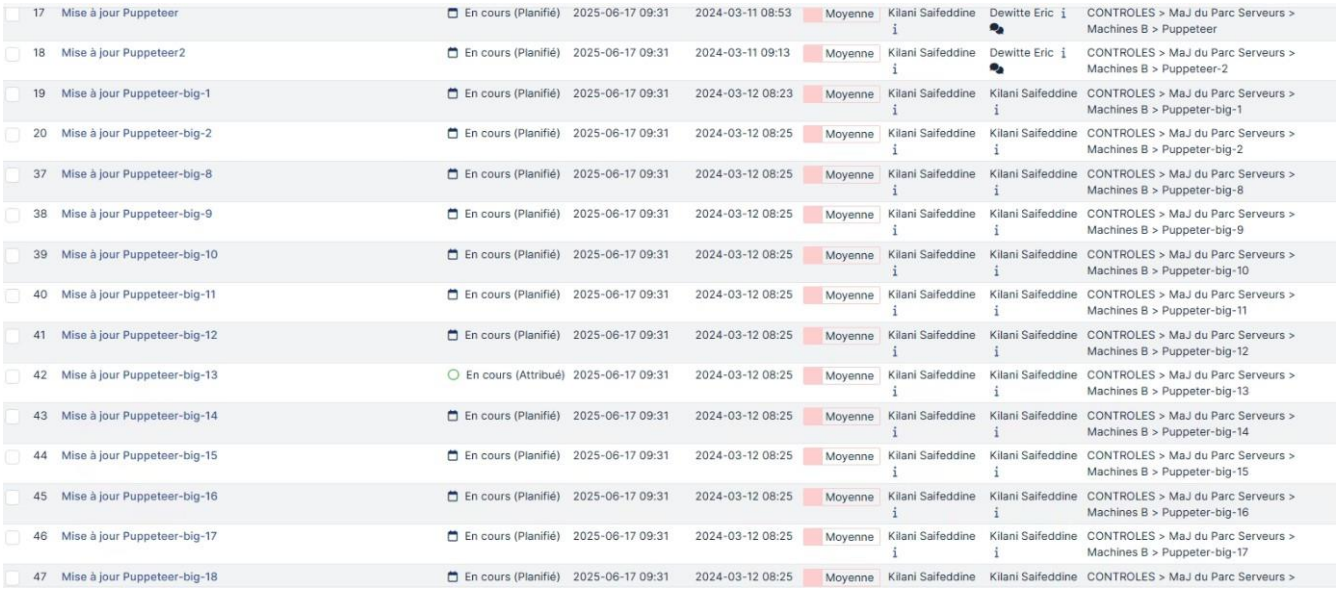
Le tout est automatique : le programme se lance tout seul le samedi soir à la même heure à chaque fois sans aucune intervention humaine. Il ne me reste plus qu'à ajouter la dernière demande du cahier des charges à savoir : ajouter les informations des mises à jour dans GLPI.

4. Intégration avec GLPI et système de supervision

Pour ajouter à ces explications un peu plus de contexte et de précision, chaque serveur a son propre ticket sur la plateforme GLPI. Ainsi, à chaque fois qu'un serveur est mis à jour, le contenu de ces mises à jour doit être renseigné dans le ticket GLPI du serveur en question. Cela permet d'avoir un suivi individuel et précis de chaque serveur sans avoir une masse d'informations qui serait difficilement utilisable.

L'idée est que nous n'avons besoin que d'ouvrir un ticket sur un serveur en particulier et nous pouvons de suite savoir depuis combien de temps il est mis à jour, quelle est la dernière mise à jour qui a été effectuée, quel est son contenu…

Il faut donc que le programme trouve un moyen de déposer les informations sur le bon ticket à chaque fois, qu'on sache à quelle date cela a été déposé et par qui.



17	Mise à jour Puppeteer	En cours (Planifié)	2025-06-17 09:31	2024-03-11 08:53	Moyenne	Kilani Saifeddine	Dewitte Eric	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeteer
18	Mise à jour Puppeteer2	En cours (Planifié)	2025-06-17 09:31	2024-03-11 09:13	Moyenne	Kilani Saifeddine	Dewitte Eric	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeteer-2
19	Mise à jour Puppeteer-big-1	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:23	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-1
20	Mise à jour Puppeteer-big-2	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-2
37	Mise à jour Puppeteer-big-8	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-8
38	Mise à jour Puppeteer-big-9	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-9
39	Mise à jour Puppeteer-big-10	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-10
40	Mise à jour Puppeteer-big-11	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-11
41	Mise à jour Puppeteer-big-12	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-12
42	Mise à jour Puppeteer-big-13	En cours (Attribué)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-13
43	Mise à jour Puppeteer-big-14	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-14
44	Mise à jour Puppeteer-big-15	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-15
45	Mise à jour Puppeteer-big-16	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-16
46	Mise à jour Puppeteer-big-17	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs > Machines B > Puppeter-big-17
47	Mise à jour Puppeteer-big-18	En cours (Planifié)	2025-06-17 09:31	2024-03-12 08:25	Moyenne	Kilani Saifeddine	Kilani Saifeddine	CONTROLES > MaJ du Parc Serveurs >

Figure 3 : *Capture d'écran des tickets de mise à jour de mes serveurs sur GLPI*

Ci-dessus, on peut y voir, sur les colonnes de gauche à droite, leur nom, leur statut, leur date de dernière modification, puis de création, leur importance, à qui est attribué le ticket et qui le supervise, puis où il se situe dans l'arborescence des tickets.

Pour ce faire, à chaque fois, le programme va se connecter au serveur GLPI, après quoi il déposera les informations voulues dans le bon fichier. Pour y parvenir, j'ai eu besoin de beaucoup de recherches, de nombreux échecs pour trouver comment la connexion se faisait, et une grande aide de mon tuteur.

Il s'est aussi rapidement posé la problématique d'avoir un programme correctement rédigé, qui permette à d'autres personnes de le comprendre et de le modifier simplement.

Le tout m'a demandé un grand travail de fond et de réflexion pour arriver au programme final :

```
#!/bin/bash CONFIG

#EMAIL="ton.email@domaine.com"

GLPI_URL="https://ton-glpi.exemple.com/apirest.php"

GLPI_USER_TOKEN="TON_USER_TOKEN"

GLPI_APP_TOKEN="TON_APP_TOKEN"

TICKET_ID=3

  GENERER LE RAPPORT

apt update -y > /tmp/rep1.txt 2>&1 apt
#
upgrade -y >> /tmp/rep1.txt 2>&1

grep "status installed" /var/log/dpkg.log > /tmp/rep2.txt 2>/dev/null cat

/tmp/rep1.txt /tmp/rep2.txt > /tmp/rapport.txt

   ENVOI MAIL

mail -s "Rapport MAJ $(hostname) - $(date +%F)" "$EMAIL" < /tmp/rapport.txt AJOUT
#
   GLPI

SESSION=$(curl -s -X GET "$GLPI_URL/initSession" \
#
  -H "App-Token: $GLPI_APP_TOKEN" \

  -H "Authorization: user_token $GLPI_USER_TOKEN" | jq -r '.session_token')

[[ -z "$SESSION" || "$SESSION" == "null" ]] && echo "Erreur session GLPI" && exit 1 curl

-s -X POST "$GLPI_URL/Ticket/$TICKET_ID/ITILFollowup" \

  -H "App-Token: $GLPI_APP_TOKEN" \

  -H "Session-Token: $SESSION" \

  -H "Content-Type: application/json" \

  -d "{\"input\": {\"content\": \"$(sed 's/"/\\"/g' /tmp/rapport.txt)\"}}" curl -s -X

GET "$GLPI_URL/killSession" \

  -H "App-Token: $GLPI_APP_TOKEN" \

  -H "Session-Token: $SESSION"
```

Figure 4 : *Aperçu d'une partie du programme final*

5. Tests, validation et mise en production

Avec ce travail, tout le cahier des charges est respecté, il ne me restait plus qu'à effectuer différents tests pour être sûr que le programme fonctionnait comme je le voulais.

Dans cette phase de test, il y a eu notamment la reproduction d'erreurs au moment de la mise à jour pour voir comment le programme se comportait. C'est ainsi que différents tests de cette nature ont eu lieu. Une fois que le programme a été validé par mon tuteur, il ne me restait plus qu'à le mettre sur chaque serveur, faire les modifications nécessaires sur le programme si besoin il y avait, et voir si dans des conditions réelles, il fonctionnait.

À ce stade, et après toutes les modifications que j'ai effectuées, le programme fonctionnait comme on le voulait. Dans chaque ticket, le contenu des mises à jour apparaissait.

Après plusieurs semaines à vérifier que le programme s'exécutait correctement, que l'envoi du mail de récapitulatif se faisait, que les informations étaient correctement saisies dans les bons tickets sur GLPI, on a pu officialiser l'utilisation du programme. Bien sûr, depuis sa mise en place, ce dernier n'a pas arrêté d'être vérifié, surveillé, amendé. Aujourd'hui encore, ce programme tourne et fonctionne comme on le souhaitait quand on l'a imaginé. Cette automatisation permet aujourd'hui de superviser automatiquement 30 serveurs et d'éviter plusieurs heures d'intervention manuelle chaque mois. Le temps auparavant consacré à ces opérations peut désormais être investi dans des missions à plus forte valeur ajoutée.

Au vu des changements qu'il a connus et qu'il va connaître, il devrait toujours répondre à cette volonté d'automatisation.

5. Compétences mobilisées et acquises, analyse critique & axes d'amélioration

Cette mission m'a permis de développer de nombreuses compétences techniques et méthodologiques. J'ai dû apprendre à utiliser plus en profondeur Linux et Bash afin de concevoir une solution répondant à un besoin concret de l'entreprise. Ce projet m'a également permis d'acquérir une meilleure compréhension de l'automatisation des tâches, de la planification de traitements récurrents à l'aide de CRON, ainsi que de l'utilisation de l'API GLPI pour assurer le suivi des opérations réalisées.

Au-delà des aspects purement techniques, cette mission m'a confronté à l'ensemble des étapes d'un projet : identification d'un besoin, définition d'un cahier des charges, phase de recherche, développement, tests, mise en production et amélioration continue. Elle m'a également appris l'importance de documenter son travail et de concevoir des solutions compréhensibles et

maintenables par d'autres personnes.

Mission 2 — Nom de domaine & Infrastructure DNS

Chez IP Twins, s'occuper des serveurs DNS est essentiel car c'est le cœur de ce que nous faisons : gérer les noms de domaine pour des sociétés et des marques partout dans le monde. En tant que registrar certifié, IP Twins sert de lien entre les organismes qui gèrent les noms (comme l'AFNIC pour le. fr, l'ICANN pour les domaines internationaux, ou d'autres registres nationaux) et nos clients. Cette certification nous permet d'enregistrer, de modifier, de transférer et de supprimer des noms de domaine pour nos clients, en veillant à ce que tout soit conforme administrativement et en gérant les aspects techniques des enregistrements DNS associés.

Pour les personnes non initiées, on peut comparer, dans un but explicatif, le DNS à Google Maps :

Chaque maison, bâtiment, rue, place à ses coordonnées GPS. Par exemple, la mairie du 5e arrondissement de Paris se situe à la latitude : 48,8462486267° N et la longitude : 2,34460401535° E.

Seulement, si nous autres usagers devions enregistrer ces séries de chiffres pour chaque lieu que l'on fréquente, la tâche serait extrêmement complexe. C'est ainsi qu'ont été créées les cartes, puis les applications comme Google Maps, pour pouvoir faire la traduction entre des coordonnées GPS et une adresse.

Pour le DNS, c'est exactement la même chose : chaque site a ses coordonnées IP. Seulement, si à chaque fois que l'on souhaite se rendre sur un site, on devait apprendre son IP par cœur, cela deviendrait rapidement infaisable. C'est ainsi que les serveurs DNS traduisent ces adresses IP en noms de domaine : au lieu d'apprendre l'IP 216.58.214.174, j'ai juste à taper google.com pour accéder au moteur de recherche.

Donc, dès qu'un client fait une demande concernant un domaine, que ce soit pour un nouvel enregistrement, un changement d'adresse IP, ou pour supprimer quelque chose, cette demande passe par notre système interne.

Ce système crée automatiquement les fichiers de zone nécessaires, actualise les serveurs DNS concernés, et informe les serveurs secondaires pour que l'information se répande. En tant qu'administrateur réseau et cybersécurité, mon travail comprend donc naturellement la maintenance de cette infrastructure, sa surveillance, et une intervention rapide en cas de problème. Ce travail demande une grande précision, car une petite erreur ou un problème de synchronisation peut affecter l'accès aux domaines de nos clients et, par conséquent, leur présence sur internet, leur boîte mail, et autres.

Voici à quoi ressemble une requête DNS :

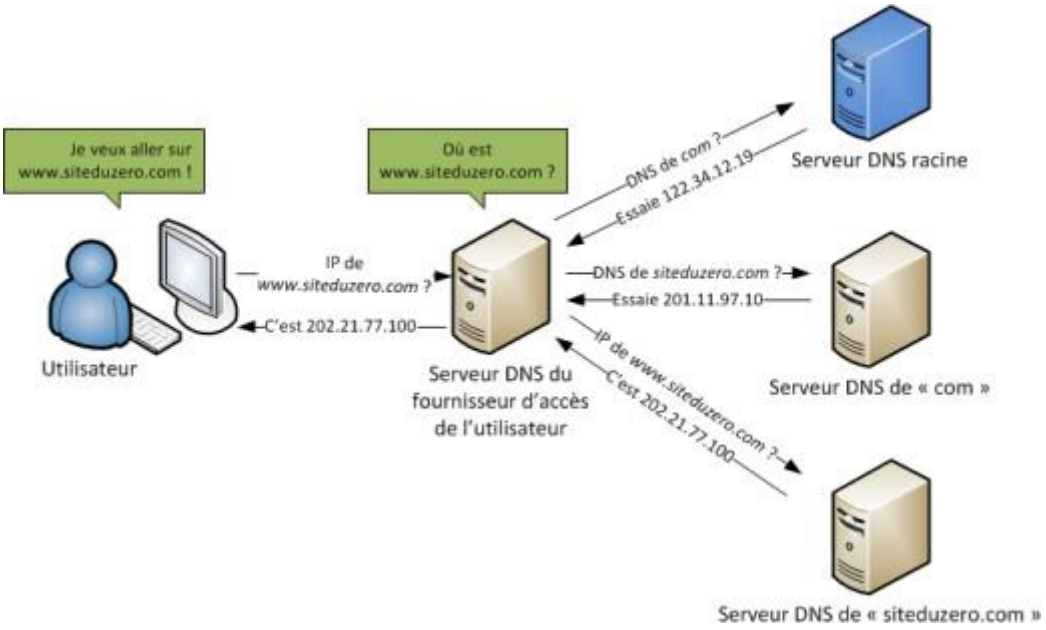


Figure 5 : *Schéma d'une résolution d'une requête DNS pour accéder à la page internet ''siteduzero.com''*

1. Présentation de l'infrastructure DNS d'IP Twins

IP Twins s'appuie sur une structure DNS qui semble conventionnelle, mais pensée pour offrir une disponibilité sans faille et une robustesse des services. Nous déployons un système sur 5 continents différents de 5 serveurs maître/secondaires : un serveur DNS central (maître) et quatre serveurs auxiliaires (secondaires).

Cette disposition aide à fractionner les demandes et à procurer une sauvegarde, pour que les demandes DNS restent traitées même si le serveur central est momentanément hors service. Le DNS, ou Système de Noms de Domaine, est une composante clé de la structure d'Internet.

Cette infrastructure assure la gestion de plusieurs milliers de noms de domaine appartenant à des entreprises évoluant dans des secteurs variés et parfois sensibles.

Après avoir présenté le fonctionnement général d'une résolution DNS, il est désormais possible d'observer l'architecture « réelle » utilisée au sein d'IP Twins pour assurer la gestion et la disponibilité des noms de domaine de ses clients :

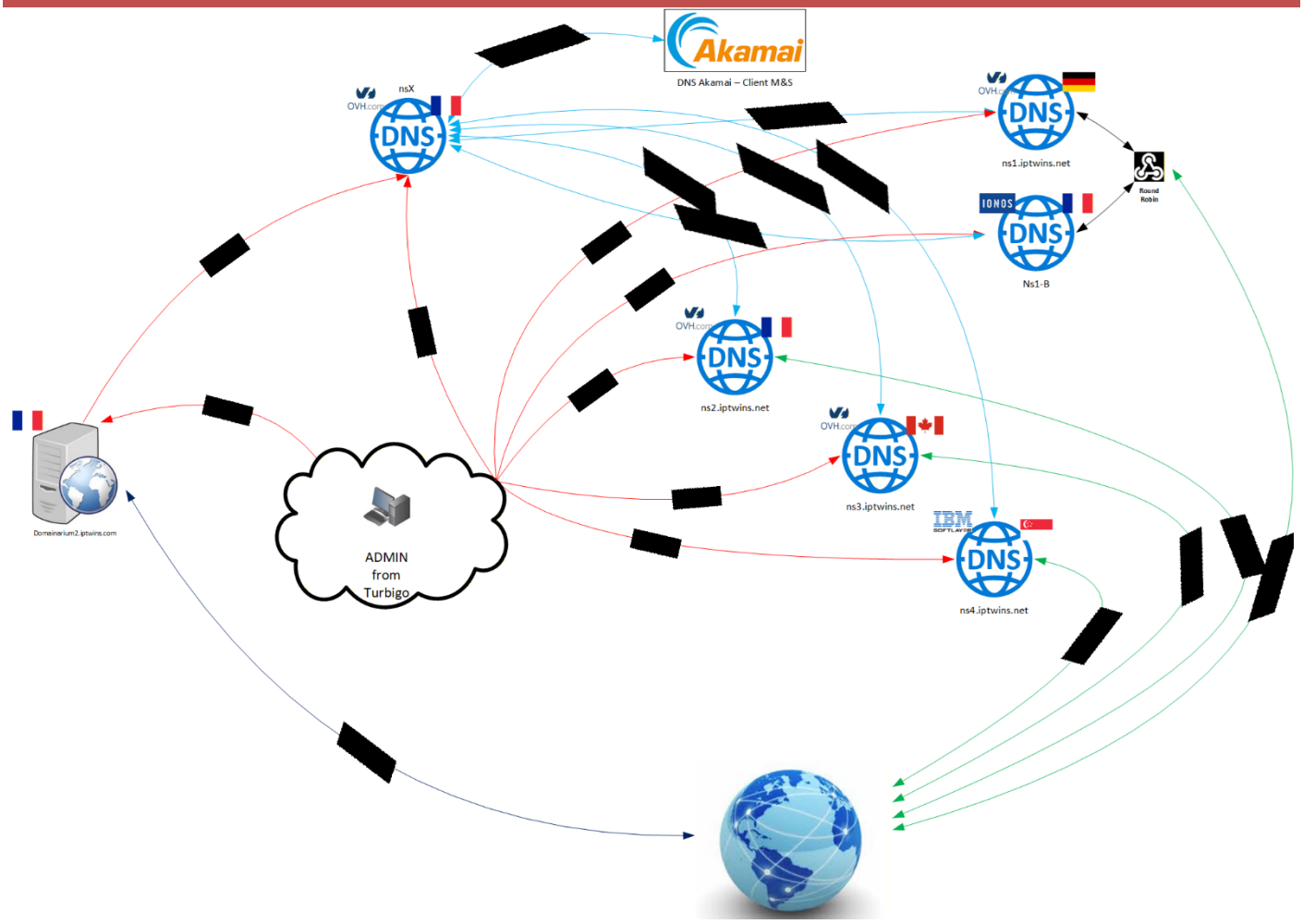


Figure 6 : *Architecture simplifiée de l'infrastructure DNS IP Twins.*

Pour des raisons de confidentialité, certaines informations ont volontairement été masquées sur ce schéma. Celui-ci reste néanmoins représentatif de l'architecture DNS sur laquelle j'interviens quotidiennement au sein d'IP Twins.

Cette infrastructure repose sur plusieurs serveurs DNS répartis dans différents pays. Cette répartition géographique n'est pas le fruit du hasard : elle permet d'assurer une forte résilience de l'infrastructure. Si un serveur ou un datacenter venait à être indisponible, les autres serveurs continueraient à répondre aux requêtes DNS, limitant ainsi l'impact pour les clients.

Au centre de cette architecture se trouve Domainarium, la plateforme développée par IP Twins. C'est par son intermédiaire que sont réalisées les opérations de gestion des noms de domaine et des zones DNS. Les modifications effectuées sont ensuite propagées vers les différents serveurs DNS afin de maintenir une cohérence globale de l'infrastructure.

On retrouve également sur ce schéma les postes d'administration situés à Turbigo, depuis lesquels nous réalisons avec Eric les opérations de gestion, de supervision et de maintenance de l'infrastructure. Certains clients disposent également de solutions complémentaires, comme

Akamai dans le cas présenté ici. L'ensemble forme un écosystème distribué où chaque composant joue un rôle précis dans la disponibilité, la résilience et la cohérence globale des données DNS.

Au cours de mon alternance, j'ai été amené à travailler avec Éric Dewitte sur plusieurs aspects de cette infrastructure, notamment la supervision des serveurs, le contrôle de la synchronisation des zones DNS, l'analyse d'incidents ainsi que l'automatisation de différents mécanismes de vérification visant à garantir la cohérence des données entre les différents nœuds.

2. Supervision et synchronisation des serveurs DNS

Avec l'aide de mon tuteur, j'ai créé des scripts automatiques pour vérifier que les données DNS restent identiques sur nos cinq serveurs. Ces programmes examinent périodiquement le nombre d'éléments enregistrés sur chacun. Si un serveur a des informations différentes (par exemple, si un serveur secondaire n'a pas reçu la mise à jour récente), un email d'alerte est envoyé immédiatement. Si les données des serveurs DNS ne correspondent pas, un autre programme se lance tout seul.

Il examine les informations supplémentaires des fichiers de zone (comme le numéro de série des fichiers qui évolue positivement à chaque modification) pour trouver la version la plus récente. Ensuite, il force tous les serveurs à se mettre à jour à partir de cette version correcte, ce qui remet tout en ordre sans qu'on ait besoin d'intervenir.

3. Automatisation des contrôles et gestion des incidents

Il m'est arrivé de voir une synchronisation échoue à cause d'une simple erreur de frappe dans un fichier (un point oublié, une valeur incorrecte ou un numéro de série mal incrémenté). Dans ce cas, nous avons des programmes qui regardent les journaux de la machine afin de nous trouver les problèmes.

Dans ce cas, je corrige le fichier avec l'erreur, je rafraîchis la configuration de ce nom de domaine, si besoin, je force manuellement la mise à jour des serveurs secondaires.

Par exemple, un client a demandé à nos chargés de comptes de supprimer rapidement un enregistrement mal configuré qui pointait vers une ancienne adresse IP. La modification a fonctionné sur le serveur principal, mais une erreur de réplication (à cause d'une valeur trop longue) a créé une différence temporaire.

Grâce aux alertes, j'ai été averti rapidement et j'ai forcé la mise à jour des fichiers de zone sur les serveurs secondaires concernés.

3. Sécurisation des échanges DNS

Pour sécuriser la communication entre le serveur principal et ses répliques, on s'appuie sur des clés TSIG (Signature de Transaction). Chaque serveur dispose d'une clé unique, créée via l'algorithme HMAC-SHA512. Ces clés, intégrées aux fichiers de configuration, assurent que les transferts de zone sont authentiques et non altérés. Si une clé est incorrecte ou obsolète, le transfert est bloqué, protégeant les serveurs d'écritures non désirées.

En plus de TSIG, nous avons renforcé la sécurité en limitant l'accès aux fichiers essentiels et en restreignant les adresses IP autorisées à faire des requêtes récursives. Sur nos serveurs de production, le DNS récursif est désactivé ; ils ne fonctionnent qu'en tant que serveurs faisant autorité pour nos zones. Ainsi, le DNS est vital pour l'image en ligne de nos clients et leur fonctionnement interne. Une panne, même courte, peut bloquer un site, perturber les e-mails, et nuire à la réputation.

4. Gestion des normes et continuité de service

Face aux enjeux de cybersécurité, notre DNS doit être robuste, rapide et respecter des normes comme l'ISO 27001 ou les directives de l'ANSSI. Notre mission dépasse la technique : il faut assurer un suivi précis des actions, justifier les accès, protéger les fichiers de zone, garantir les sauvegardes et pouvoir vérifier l'historique des changements à tout moment. Tous nos scripts d'administration sont expliqués, datés et exécutés selon des procédures approuvées par mon tuteur.

5. Compétences mobilisées et acquises, analyse critique & axes d'amélioration

Durant ce projet, j'ai développé une solide compétence dans le pilotage d'un ensemble de serveurs DNS.

J'ai appris à mettre en place des automatismes pour les opérations importantes, à créer des programmes fiables, à déceler les problèmes ardus et à respecter les règles établies.

J'ai aussi réalisé à quel point les détails, comme la durée de vie ou le numéro de série d'une zone, sont cruciaux et peuvent causer de gros soucis si on les oublie. Les différentes tâches que j'ai menées, de la création de programmes à la correction d'erreurs, en passant par la sécurisation avec TSIG, la surveillance constante, la gestion des alertes et l'examen des configurations, m'ont permis d'améliorer mes connaissances en réseau, sécurité et administration système.

J'ai aussi intégré l'importance du DNS dans une structure exigeante sur le plan technique. S'occuper d'un système DNS dans une société comme IP Twins va donc bien au-delà de la simple configuration des zones.

Cela demande une surveillance constante, des solutions de réparation efficaces, une protection des échanges de données et une automatisation bien gérée. Grâce à ma participation à ce projet, j'ai pu consolider mes capacités techniques tout en adoptant une approche de qualité et de conformité, ce qui est essentiel dans un contexte où la fiabilité du service DNS est cruciale pour le bon fonctionnement de l'entreprise.

Mission 3 — Amélioration continue du système d'information et conformité ISO 27001

1. Contexte de sécurisation du système d'information

La volonté générale des acteurs, qu'ils soient du domaine informatique ou d'autres secteurs, de se sécuriser afin de se protéger contre des pirates toujours plus ingénieux pousse aujourd'hui les entreprises à prendre, le plus rapidement possible, toutes les dispositions nécessaires pour se sécuriser et démontrer leur niveau de sécurisation. En effet, la menace ne cesse d'évoluer, les attaques sont de plus en plus sophistiquées, ciblées, rapides et destructrices, ce qui oblige les entreprises à ne plus simplement réagir, mais à anticiper.

Cette anticipation passe par la mise en place de politiques de sécurité solides, d'outils de défense adaptés, et surtout, par l'obtention de certifications reconnues qui viennent prouver, aux yeux des partenaires, des clients, des fournisseurs et parfois des autorités, qu'un certain niveau de sécurité est atteint et maintenu.

Pour permettre de démontrer qu'une entreprise respecte un niveau de sécurisation adéquat, des certifications et réglementations diverses ont été créées, encadrées, normalisées, puis largement répandues dans le monde professionnel. Certaines sont devenues incontournables dans leur domaine. Selon l'activité précise de l'entreprise, les types de données qu'elle traite, les secteurs qu'elle touche, sa localisation géographique ainsi que celle de ses clients, il existe un ensemble plus ou moins large de certifications à envisager.

Certaines sont obligatoires du point de vue légal, et le non-respect de ces obligations peut entraîner des sanctions importantes, des pertes de contrats voire l'impossibilité de poursuivre certaines activités. D'autres certifications ne sont pas imposées par la loi mais sont devenues extrêmement recommandées, à tel point que leur absence peut directement impacter le nombre de clients et de prestataires qui acceptent de travailler avec l'entreprise, par manque de garanties en matière de sécurité.

2. Participation à la démarche ISO 27001

C'est dans ce monde dynamique, exigeant, en perpétuelle évolution, qu'évoque IP Twins. C'est donc naturellement que s'est posée la question du passage à la certification ISO 27001. Reconnaissant l'importance capitale de cette norme en matière de sécurité de l'information, et conscient que l'avenir de la société passe par sa capacité à démontrer la rigueur de ses pratiques, il a été décidé que nous devions entamer le processus d'obtention de cette certification dans les plus brefs délais.

C'est ainsi que mon tuteur Éric Dewitte et moi-même, avec l'aide d'autres salariés, avons commencé à étudier comment réussir cette certification.

Pour se faire, IP Twins a appelé ORANGE CYBERDEFENSE pour nous aiguiller à travers des audits et différentes aides afin de réussir la certification.

Le point fondamental à saisir pour la certification ISO 27001, c'est qu'elle établit des exigences pour tout le SI de l'entreprise sans clairement définir comment y répondre. C'est ainsi à l'entreprise qui passe la certification de trouver comment y répondre selon ce qu'elle peut investir et ce dont elle a besoin. Après le premier audit d'ORANGE CYBERDEFENSE sur l'ensemble de notre SI, nous avions une liste de non-conformités majeures et mineures qu'il fallait corriger avant de passer notre certification.

Les corrections apportées ont notamment porté sur la formalisation de procédures existantes, le déploiement de GLPI pour assurer la traçabilité des actions, l'installation d'un pare-feu Pfsense, la mise en place d'un filtrage MAC ainsi que le renforcement du suivi des comptes et des droits d'accès.

3. Mise en place et structuration de GLPI

Certaines de ces non-conformités étaient simplement corrigibles en rédigeant des politiques et divers documents expliquant comment IP Twins gère telle ou telle donnée. Il fallait dans un grand nombre de cas juste avoir une trace écrite de processus que nous suivions déjà mais sans le noter. L'exemple qui me vient naturellement est la vérification que je faisais toutes les deux semaines sur les switchs pour vérifier qu'aucun compte n'a été créé, modifié et/ou supprimé par un tiers non autorisé. Je le faisais évidemment chaque semaine mais sans aucune preuve de mes passages. C'est en faisant l'inventaire de tout ce que l'on devait maintenant répertorier, noter, vérifier, que l'idée de mettre en place un serveur GLPI m'est venue.

En effet, GLPI permet notamment, grâce à son système de tickets, de créer un suivi de ce que l'on veut. IP Twins m'a demandé de gérer le déploiement de GLPI et de migrer toutes les données concernant l'inventaire du parc IP Twins, les différents suivis, fichiers qui recensent les mises à jour et autres mises à jour. J'ai donc passé un certain temps à mettre en place l'arborescence des tickets en fonction de ce dont on avait besoin.

Une fois les catégories créées, il me suffisait plus qu'à créer les bons tickets dans chaque catégorie, mes tickets de mise à jour dans la catégorie CONTROLES
> MaJ du Parc Serveurs, pour les vérifications de comptes ce sera dans COMPTES ET ACCES
> Revue périodique…

À terme, plusieurs dizaines de tickets ont été créés afin d'assurer le suivi des contrôles périodiques, des mises à jour serveurs et des différentes vérifications exigées dans le cadre de la certification ISO 27001.

4. Déploiement du pare-feu Pfsense

Comme on peut le constater à ce stade, la certification reste en grande partie bureaucratique dans le sens où elle demande la rédaction de documents ou la formalisation de tâches que l'entreprise fait déjà. Il y a cependant aussi une partie réellement technique que nous allons aborder ici.

Avant la certification, notre réseau informatique était le suivant : une box qui nous permettait d'avoir un accès internet, cette box était directement liée à notre switch général.

Ce dernier, via une baie de brassage, distribuait l'accès internet à toutes les salles de nos locaux. Il était aussi relié à deux routeurs qui donnaient sur des machines d'administration d'un côté pour mon tuteur et moi, et à des machines de développement pour l'équipe DEV.

L'un des audits passés avant la certification a mis en lumière le manque de sécurité d'une telle infrastructure. En effet, la box internet était directement reliée au switch général sans aucun filtrage de ce qui rentrait ou sortait du réseau d'IP Twins.

C'est ainsi que j'ai eu pour mission de trouver une solution pour filtrer l'entrée et la sortie des données. Solution que j'ai rapidement trouvée car à cette période-là, en cours, nous étions en train de travailler sur Pfsense.

C'est un outil logiciel qui est largement utilisé dans les environnements professionnels pour sécuriser et gérer les connexions réseau. C'est ce qu'on appelle communément un pare-feu.

C'est ainsi que j'ai présenté à mon tuteur un boîtier physique qui héberge ce logiciel. L'idée était de mettre ce boîtier entre la box internet et le switch général pour que tout le trafic passe par ce pare-feu. Voici à quoi cela ressemble :

Figure 7 : *Photo du routeur Pfsense. Le câble blanc vient de la box internet, le câble bleu va vers le switch général.*

Cette modification a permis d'introduire une couche de filtrage inexistante auparavant et d'obtenir une meilleure maîtrise des flux entrant et sortant du réseau de l'entreprise.

Nous avons aussi installé une serrure pour la porte de la baie. On peut l'ouvrir avec un badge ou une carte, ce qui, en plus de limiter l'accès et de le sécuriser, nous permet d'avoir les dates et heures d'entrée et de sortie dans la baie.

5. Sécurisation réseau et filtrage MAC

Il y a aussi d'autres tâches que j'ai effectuées dans cette optique de sécurisation du SI : le filtrage MAC.

Chaque appareil qui communique sur internet possède une carte réseau. Chacune de ces cartes possède une suite de chiffres et de nombres, comme un numéro de série, que l'on appelle adresse MAC.

Pour être sûr que seules les machines autorisées à accéder au réseau IP Twins puissent y accéder, il a été décidé de mettre en place un filtrage MAC. Une liste d'adresses MAC des appareils de confiance est donc montée et renseignée dans un switch qui est en capacité d'autoriser seulement ces appareils à communiquer. C'est tout le projet que j'ai également mené. Cela a commencé avec la sélection du bon switch, qui peut effectuer ces tâches de filtrage.

Une fois acheté, je l'ai mis à la place de l'ancien switch général dans notre baie serveur. J'ai au préalable établi la liste des appareils de confiance. Ce travail a nécessité l'inventaire de l'ensemble des équipements autorisés à accéder au réseau afin de constituer une liste de référence fiable.

Voici comment indiquer à ce switch les appareils de confiance :

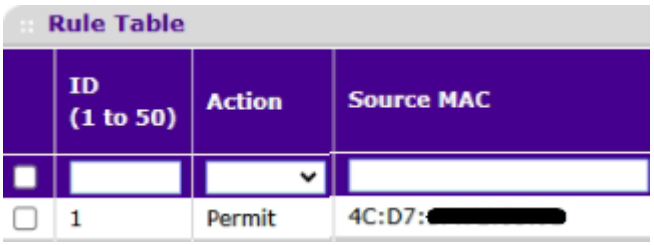


Figure 8 : *Capture d'écran du switch général. On y voit l'autorisation d'une adresse MAC, anonymisée pour des raisons de confidentialité.*

Une fois cette liste renseignée dans l'appareil, seuls les appareils autorisés pourront accéder au réseau. Une fois l'installation terminée, il ne me restait plus qu'à tester que mon poste pouvait encore aller sur internet. Et c'est là que cela ne fonctionnait pas.

C'est ainsi que j'ai découvert toute une partie du travail d'administrateur, à savoir comprendre et résoudre ce genre de problème.

Pour ce faire, j'ai fait un point sur ce que j'avais fait : j'ai remplacé l'ancien switch général par le nouveau qui peut faire des filtrages. Je lui ai indiqué quelles machines étaient autorisées à communiquer, mais cela ne fonctionnait pas. C'est ainsi que j'ai décidé de suivre le chemin que prenait mon ordinateur pour aller sur internet, et je me suis rendu compte qu'il passait par un autre boîtier que j'avais oublié.

En effet, étant donné que dans les locaux d'IP Twins, il y avait plus d'ordinateurs que de prises Ethernet disponibles sur les murs, il y avait des mini switchs dans chaque salle pour avoir plus de prises et distribuer l'accès à tous les postes.

Seulement, ces petits appareils possèdent aussi une carte réseau, donc une adresse MAC, donc nécessitent d'être autorisés à communiquer.

C'est ainsi que j'ai résolu ce problème et que mon filtrage a fonctionné. Les appareils non autorisés ne pouvant pas se connecter à internet ni communiquer avec qui que ce soit dans notre réseau, ma mission fut un succès.

9. Gestion des identités et sécurisation des accès Microsoft Azure

Il reste maintenant un dernier gros point dans cette partie concernant l'amélioration continue du SI, c'est le côté sécurisation des postes de travail de mes collègues. En effet, toujours dans cette optique de passage de certification, IP Twins a décidé d'utiliser une solution tout-en-un proposée par Microsoft qui s'appelle AZURE.

Microsoft Azure est une plateforme qui propose, entre autres, des outils avancés qui vont permettre l'administration réseau et la sécurisation des postes.

Grâce à des services intégrés divers et variés tels qu'Azure Active Directory, Microsoft Defender for Endpoint, Intune et Defender for Cloud, Azure permet de gérer, surveiller et protéger efficacement les postes utilisateurs et les appareils mobiles connectés à l'environnement.

C'est donc grâce à cet outil que j'allais superviser l'amélioration continue de la sécurisation des postes de travail. Concrètement, cette plateforme assure la surveillance en temps réel de l'état des postes de travail de l'entreprise : vérifier s'ils sont à jour, s'ils présentent des vulnérabilités, ou s'ils ont été exposés à des menaces.

On peut gérer à distance les configurations des postes, installer ou désinstaller des logiciels, déployer des correctifs de sécurité, et appliquer automatiquement des règles de conformité

(chiffrement, antivirus activé, mot de passe fort, etc.).

Un outil qui nous est paru pertinent, à mon tuteur et moi, est le Secure Score :

Le Secure Score est un indicateur fourni par Microsoft dans Azure qui permet de mesurer le niveau de sécurité du SI, soit de l'ensemble des comptes et postes rattachés à AZURE.

Quand nous avions commencé à utiliser cette solution, le Secure Score était très bas, autour de 27%. Cette note nous indiquait qu'il fallait faire des tâches recommandées pour améliorer la note. Elle nous indiquait aussi que les entreprises de taille similaire étaient autour de 47%. C'est comme cela que l'objectif d'atteindre ce pourcentage au minimum a été lancé.

Pour améliorer facilement le Secure Score sur Azure, voici les premières tâches que j'ai effectuées : activer l'authentification multifacteur (MFA) pour tous les comptes, surtout les administrateurs ; maintenir les postes à jour avec les derniers correctifs ; chiffrer systématiquement les données et disques ; activer Microsoft Defender sur tes ressources clés ; limiter l'ouverture des ports réseau en bloquant ceux inutiles via les groupes de sécurité ; appliquer le principe du moindre privilège pour les droits utilisateurs ; activer la journalisation pour surveiller les activités et alertes ; mettre en place des sauvegardes régulières ; utiliser Azure Policy pour automatiser des règles de sécurité ; et restreindre les accès publics aux ressources pour réduire la surface d'attaque.

Toutes ces tâches, je les ai effectuées durant un long moment pour toujours améliorer la note qui était la nôtre. De temps à autre, il y avait des vulnérabilités détectées sur nos postes, en raison d'un manque de mise à jour ou de logiciels qui auraient été compromis. À chaque fois que cela était critique, je me dépêchais d'effectuer les correctifs demandés.

Pour optimiser la chose, j'ai aussi automatisé un grand nombre de mises à jour des logiciels quand des versions plus récentes étaient disponibles.

Ces tâches ont porté leurs fruits car nous sommes aujourd'hui à un score de 53%
:

Figure 9 : *Capture d'écran de la note de sécurité d'IP Twins. On voit que les entreprises similaires sont autour de 46 %, ce qui fait qu'IP Twins est au-dessus de la moyenne.*

10. Passage certifications & Correction des vulnérabilités

C'est après tous ces efforts que nous avons passé la certification ISO 27001 avec un organisme nommé CertiTrust. Ce dernier est un organisme de certification indépendant, reconnu à l'international, spécialisé dans la délivrance de certifications de systèmes de management, notamment la norme ISO 27001.

La certification ISO 27001 suit un cycle de trois ans. Dans un premier temps, IP Twins subira un audit initial, qui permet d'obtenir la certification. Ensuite, deux audits de surveillance sont réalisés : le premier un an après l'obtention de la certification, et le second deux ans après.

Ces audits partiels permettent de vérifier que le système de gestion de la sécurité est toujours conforme et bien maintenu. Dans le cas où des non-conformités seraient détectées, les audits de surveillance ont pour but de vérifier si des correctifs ont été appliqués.

Enfin, à la fin du cycle de trois ans, un audit complet de recertification est effectué pour renouveler la certification et entamer un nouveau cycle. Il est important de noter que toute non-conformité majeure identifiée lors d'un audit de surveillance peut entraîner une suspension ou un retrait de la certification, bien que de manière générale, il faille plusieurs non-conformités pour réellement avoir ce genre de sanction.

IP Twins, à ce jour, a passé sa certification et son premier audit de surveillance. Pour l'audit de certification, nous avons, sur plusieurs jours, présenté le SI d'IP Twins et montré comment nous avons répondu aux exigences de la norme.

Les certificateurs, qui étaient deux, ont demandé de passer au peigne fin tous nos processus. Très souvent, il fallait simplement leur montrer le bon document. Parfois, ils insistaient pour voir les machines et programmes en production.

De manière générale, cet audit de certification s'est plutôt bien passé. Une fois terminé, nous avons été rapidement fixés : nous avions obtenu la certification, mais il y avait une dizaine de non-conformités.

C'est ainsi que les certificateurs nous ont indiqué qu'il fallait produire dans le mois qui suivait un plan de correction afin de rapidement régulariser la situation.

L'audit de surveillance, venu l'année d'après, a été plus léger. En effet, le certificateur était cette fois seul, et les points à auditer étaient bien moins nombreux. C'était essentiellement une vérification du respect de notre plan de réponse aux non-conformités défini par l'audit de certification.

Parmi les anomalies constatées, l'une d'elles portait sur la nécessité de contrôler la température ambiante du local serveur. En réalité, la supervision thermique des salles informatiques est un point clé concernant la sûreté des installations et de leur environnement.

Cette exigence est directement liée à des mesures de la norme, qui stipulent la protection du matériel contre les dangers physiques et environnementaux, ainsi que le suivi constant du milieu des infrastructures essentielles.

Le fait de maîtriser la température aide à maintenir la disponibilité et l'intégrité des systèmes en évitant les risques de surchauffe, qui pourraient causer des défaillances du matériel, des interruptions de service ou des pertes de données.

Bien que cette action ne soit pas clairement définie dans la norme comme une « surveillance de la température », elle est perçue comme une pratique essentielle pour tout système de gestion de la sécurité de l'information désireux d'assurer une haute résilience et une continuité des services.

Pour assurer une surveillance adéquate de l'environnement dans la baie informatique, suivant les préconisations de l'ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers), j'ai donc décidé de mettre en place des capteurs thermiques.

Me basant sur leurs recommandations, j'ai déterminé que 27 °C représentait une limite exigeant une intervention. J'ai donc programmé les capteurs pour qu'ils signalent tout dépassement de cette température via un email automatique, et qu'ils activent aussi le système de ventilation de la baie.

Figure 10 : *Photo du système de ventilation à gauche et de la sonde thermique à droite*

Suite à la mise en œuvre de toutes les mesures de protection conseillées, incluant l'activation de l'authentification à facteurs multiples, le cryptage des informations, la mise à niveau des appareils, la limitation des accès au réseau et l'établissement de règles de sécurité appropriées, sans oublier d'autres bonnes pratiques, le Score de Sécurité Azure a connu une amélioration notable.

Ces interventions ont solidité la sécurité générale du SI d'IP Twins. Forts de ces ajustements, les audits ont été approuvés avec succès, attestant que les systèmes respectent les impératifs de sécurité requis et marquant l'achèvement de cette certification.

6. Compétences mobilisées et acquises, analyse critique & perspectives d'évolution

Cette mission m'a permis de développer une vision plus globale de la cybersécurité et de la manière dont celle-ci s'intègre dans le fonctionnement quotidien d'une entreprise. Au-delà des aspects purement techniques, j'ai découvert l'importance de la conformité, de la traçabilité et de la formalisation des processus dans une démarche de sécurisation du système d'information.

La participation à la certification ISO 27001 m'a amené à comprendre que la sécurité ne repose pas uniquement sur des outils techniques, mais également sur des procédures, des contrôles réguliers, une documentation rigoureuse et une amélioration continue. J'ai ainsi participé à la mise en place de différents dispositifs de suivi, au déploiement de GLPI, à la sécurisation du réseau avec Pfsense ainsi qu'au renforcement du contrôle des accès.

Cette mission m'a également permis de développer ma capacité d'analyse face aux recommandations formulées lors des audits. Il a fallu comprendre les non-conformités relevées, identifier les solutions les plus adaptées à IP Twins puis participer à leur mise en œuvre en tenant compte des contraintes techniques, organisationnelles et financières de l'entreprise.

SYNTHÈSE PROFESSIONNELLE

1. Développement des compétences techniques

Fort des quelques projets que je viens de vous présenter, j'ai vu mon socle de compétences largement se nourrir de ces expériences et ainsi fleurir. Ces trois travaux m'ont chacun apporté, à travers leur complexité et leur singularité, des savoirs qui sont des plus importants lorsque l'on évolue dans un domaine qui se veut aussi exigeant.

L'automatisation que j'ai mise en place pour mon projet m'a permis, à partir d'un constat personnel, de créer un projet, de définir un cahier des charges, de définir l'investissement homme/jour et les matériaux/logiciels nécessaires. L'établissement d'un plan clair, net et précis a aussi été fait pour ce projet. Cela m'a éduqué quant à l'apprentissage/formation à de nouvelles méthodes et connaissances pour répondre aux besoins d'un projet en cours.

J'ai aussi été mis dans une position où je devais revoir à la hausse ou à la baisse les objectifs pour que le projet soit réalisable et/ou qu'il réponde correctement aux problématiques posées initialement.

J'ai, plus ou moins à mes dépens, appris à briser la glace qui se forme entre la théorisation d'un projet et sa mise en production. Plus concrètement, j'ai eu à acquérir des savoirs techniques quant à l'utilisation de ce système d'exploitation (Linux) et à la manière avec laquelle on peut lui indiquer quelles actions exécuter (Bash).

Pour ce qui est du cœur de métier d'IP Twins, je ne peux qu'être appréciatif d'avoir eu l'opportunité de manier des technologies aussi pointues, tant intellectuellement qu'en pratique. L'enfant, quelque peu méconnu du grand public et qui est pourtant des plus importants, qu'est le DNS m'a permis d'être au contact de ce qui se fait de plus profond en informatique. La gestion d'un tel service a été si formatrice.

Administrer une chose qui, si l'on commet la moindre erreur, pourrait littéralement paralyser toute l'activité d'une entreprise, d'un gouvernement ou autre, est une activité des plus stressantes et stimulantes. J'ai appris dans un tel cadre à respecter des procédures très strictes. De la même manière, j'ai appris une forme de rigueur aiguë quant à la manière avec laquelle je travaille sur ce projet.

2. Développement méthodologique et organisationnel

Un point fondamental qu'il me semble important de noter est l'importance, quand on est partie prenante dans un tel projet, de bien comprendre comment le tout fonctionne et s'emboîte.

Dans un monde aussi riche et hautement complexe que le DNS, il est extrêmement important d'avoir une vision éclairée et précise du fonctionnement de ce dernier pour éviter toute erreur qui n'aurait pas lieu d'être. Cela m'a forcé à développer ma curiosité pour comprendre le plus rapidement possible les aspects d'une telle technologie qui me seraient étrangers.

La constante amélioration que j'ai apportée au SI s'inscrit dans un large contexte mondial comme précédemment expliqué. Il se trouve que c'est une mission des plus importantes car elle impacte tout un chacun chez IP Twins, que ce soit salariés, direction, logiciels ou matériaux. Personne n'y a fait exception. Un tel projet se base sur des directives nationales voire internationales.

Cela amène les acteurs, comme mon tuteur et moi, à faire une veille des plus rigoureuse quant à l'évolution du monde dans lequel nous évoluons. S'inspirer des recommandations et conseils que nous ont apportés notamment nos prestataires afin d'apporter les solutions les plus adaptées à IP Twins s'est avéré être une mission des plus ardues.

Dans un tel contexte, en plus des connaissances théoriques et pratiques, s'est ajouté tout un logiciel de réflexion qui me pousse à constamment sourcer et documenter mes choix. Une remise en question sur la base de toutes les actions que je faisais a été nécessaire pour savoir si mes faits étaient conformes à ce que nous souhaitions. Le même travail a été produit sur tout le SI et le personnel d'IP Twins.

Il y a évidemment aussi des compétences de présentation et je dirais même de représentation de mon entreprise que j'ai dû développer pour participer aux audits de ces certifications.

3. Évolution professionnelle et posture technique

Que ce soit sur le plan humain, intellectuel, technique, pragmatique ou autre, j'ai été mis devant une réalité qui peut échapper à ceux qui n'entrechoquent pas leur connaissance à des situations concrètes. De ce brassage m'est venue une remise en question de mes acquis et une maturité nouvelle.

Cette aventure a façonné mon approche du travail, me rendant plus autonome, rigoureux et responsable. J'ai aussi appris à m'adapter facilement à un contexte en constante évolution, où la sécurité doit toujours être une priorité absolue, sans délai ni compromission.

Ce parcours a renforcé mon désir d'atteindre la perfection technique, tout en boostant ma confiance.

Le fait de gérer des tâches concrètes, importantes et parfois délicates, a révélé chez moi une grande soif d'apprendre, un esprit d'initiative plus développé, et une aptitude à rester précis même sous pression.

Conclusion

Avec toute l'émotion qui est la mienne à cet instant, je peux faire s'achever mon mémoire et, avec lui, toutes les questions et réflexions autour desquelles ce document s'est forgé.

Au terme de cette année supplémentaire d'alternance chez IP Twins, les faits sont là. Il est possible de concilier beaucoup d'exigences, à condition de mettre en place une stratégie adaptée, évolutive, et surtout fondée sur une volonté forte de rigueur et de clarté opérationnelle.

Globalement, les tâches que j'ai menées à bien ont produit des résultats concrets et mesurables. L'automatisation de la procédure de mise à jour des serveurs a grandement réduit le temps que les équipes passaient sur les tâches répétitives, tout en renforçant la traçabilité et la protection des données.

L'optimisation et l'administration de l'infrastructure DNS ainsi que l'instauration de systèmes de contrôle ont renforcé la disponibilité et la stabilité du système, tout en réduisant les risques d'erreurs humaines. Pour finir, ma participation directe à l'obtention de la certification ISO 27001 illustre que les actions de sécurisation et de mise en conformité peuvent être menées sans impacter la productivité de l'entreprise, bien au contraire, elles en sont le fondement.

Cette progression a été déterminante pour affiner mes aptitudes dans divers domaines. J'ai consolidé mes connaissances touchant aux standards actuels (ISO 27001), l'analyse des dangers, les configurations DNS, les instruments de contrôle comme GLPI, ainsi que les systèmes fondamentaux. J'ai écrit des procédures conformes aux exigences de certification ; jusqu'à la conception et la mise en production de scripts d'automatisation, j'ai appris à mener une analyse de bout en bout, à documenter rigoureusement mes choix et à rendre mes solutions précises et maintenables.

L'année qui vient n'est pas une simple étape : c'est appel à m'investir toujours plus.

Cette année a nourri ma volonté de poursuivre encore longtemps l'étude de l'informatique et ce jusqu'au doctorat. Loin d'une motivation qui serait celle d'acquérir un titre honorifique, mais bien pour l'ivresse de comprendre, la flamme d'apprendre, et la quête d'un savoir qui ne se satisfait jamais du superficiel.

A cet instant, ces quelques mots ne sonnent pas la fin d'un mémoire mais bien l'aurore d'un travail encore bien long. Et c'est sur cette promesse de continuer que je vous remercie d'avoir pris le temps de lire ce document, qui j'en suis sur ne sera pas le dernier.

ANNEXES

Figure 1 (Page 8) – Organigramme simplifié d'IP Twins
Cette figure présente l'organisation hiérarchique simplifiée d'IP Twins. Elle met en évidence les différents pôles de l'entreprise ainsi que les liens fonctionnels entre les équipes juridiques, techniques et de direction. Elle permet également de situer mon positionnement au sein du pôle technique sous la supervision du Directeur Technique.

Figure 2 (Page 17) – Aperçu d'une partie du programme à ce stade
Cette capture d'écran illustre une version intermédiaire du programme d'automatisation développé dans le cadre de la gestion des mises à jour serveurs. À ce stade du projet, les mécanismes principaux de récupération des mises à jour et de génération des rapports étaient déjà opérationnels.

Figure 3 (Page 19) – Tickets de mise à jour sur GLPI
Cette figure présente l'organisation des tickets GLPI utilisés pour assurer le suivi des mises à jour des serveurs. Chaque serveur dispose d'un ticket dédié permettant d'assurer la traçabilité des opérations réalisées conformément aux exigences de suivi et d'audit interne.

Figure 4 (Page 20) – Extrait du programme final
Cette figure présente un extrait du programme final développé en Bash. Celui-ci automatise les mises à jour des serveurs, génère des rapports détaillés, transmet les informations par courrier électronique et alimente automatiquement les tickets GLPI associés.

Figure 5 (Page 23) – Exemple de résolution DNS
Cette figure illustre le fonctionnement général d'une résolution DNS. Elle met en évidence les différentes étapes permettant de traduire un nom de domaine en adresse IP afin de permettre à un utilisateur d'accéder à une ressource sur Internet.

Figure 6 (Page 24) – Architecture simplifiée de l'infrastructure DNS IP Twins
Cette figure représente une version simplifiée et partiellement anonymisée de l'infrastructure DNS utilisée au sein d'IP Twins. Elle met en évidence la répartition géographique des serveurs DNS, les mécanismes de redondance ainsi que les différents composants participant à l'administration et à la diffusion des zones DNS.

Figure 7 (Page 30) – Photo du routeur PfSense
Cette figure présente le pare-feu PfSense déployé au sein de l'infrastructure d'IP Twins. On y distingue notamment les connexions réseau principales permettant d'assurer le routage, le

filtrage et la sécurisation des flux entre Internet et le réseau interne de l'entreprise.

Figure 8 (Page 31) – Capture d'écran du switch général
Cette figure illustre une partie de la configuration du switch principal de l'entreprise. Elle met en évidence l'autorisation d'une adresse MAC, anonymisée pour des raisons de confidentialité, dans le cadre des mécanismes de contrôle d'accès au réseau mis en œuvre chez IP Twins.

Figure 9 (Page 34) – Capture d'écran de la note de sécurité d'IP Twins
Cette figure présente le score de sécurité obtenu par IP Twins au travers des outils de supervision Microsoft Azure. Elle permet de comparer le niveau de sécurité de l'entreprise à celui d'organisations similaires et met en évidence les efforts réalisés dans le cadre de l'amélioration continue de la cybersécurité.

Figure 10 (Page 35) – Photo du système de ventilation et de la sonde thermique
Cette figure présente le système de ventilation ainsi que la sonde thermique utilisés pour surveiller les conditions environnementales de l'infrastructure. Ces équipements participent au maintien de conditions de fonctionnement optimales pour le matériel informatique et contribuent à la continuité de service.

Définitions des Termes Techniques :

- Bash : Langage de script utilisé sous Linux pour automatiser des tâches système.
- Cron : Outil Linux pour planifier l'exécution automatique de scripts à des intervalles définis.
- GLPI : Outil open-source de gestion des tickets IT et des actifs informatiques. Utilisé chez IP Twins pour le suivi des mises à jour et des incidents.
- TSIG (Transaction Signature) : Protocole de sécurité pour authentifier les transferts de zones DNS entre serveurs, évitant les modifications non autorisées.
- HMAC-SHA512 : Algorithme cryptographique utilisé pour générer des clés TSIG, garantissant l'intégrité des données DNS.
- PfSense : Pare-feu open-source, déployé chez IP Twins pour filtrer le trafic réseau.
- Microsoft Azure : Plateforme cloud de Microsoft utilisée pour sécuriser et gérer les postes de travail via des outils comme Defender et Intune.
- Secure Score : Indicateur Azure évaluant le niveau de sécurité d'un SI.
- MFA (Authentification Multifacteur) : Méthode de sécurité exigeant plusieurs preuves d'identité (ex : mot de passe + SMS). Déployée sur Azure pour IP Twins.
- ISO 27001 : Norme internationale pour la gestion de la sécurité de l'information. IP Twins l'a obtenue en 2024.
- NIS2 : Directive européenne renforçant les obligations de cybersécurité pour les entreprises critiques (ex : gestion de DNS).
- RGPD : Règlement européen sur la protection des données personnelles. Impacte la gestion des logs et accès chez IP Twins.
- ANSSI : Agence française de cybersécurité.
- ICANN : Organisme gérant les noms de domaine mondiaux (ex : .com, .fr). Partenaire clé d'IP Twins.
- AFNIC : Gestionnaire des noms de domaine .fr. Collabore avec IP Twins pour les enregistrements.
- gTLD (Generic Top-Level Domain) : Extensions génériques (.com, .org).
- DNS (Domain Name System) : Système traduisant les noms de domaine (google.com) en adresses IP (216.58.214.174).
- Serveur maître/secondaire : Architecture DNS où le maître héberge les données originales et les secondaires les répliquent pour la redondance.
- Filtrage MAC : Restriction d'accès réseau basée sur l'adresse physique (MAC) de la carte réseau.
- Microsoft Defender for Endpoint : Solution de sécurité pour détecter et bloquer les menaces sur les postes clients.
- Intune : Outil Microsoft pour gérer à distance les appareils (mises à jour, politiques de sécurité).
- Defender for Cloud : Service Azure supervisant la sécurité des infrastructures cloud et hybrides.
- API (Application Programming Interface) : Interface permettant à deux applications ou

services informatiques de communiquer et d'échanger des données automatiquement.

- Active Directory (AD) : Service d'annuaire Microsoft permettant la gestion centralisée des utilisateurs, groupes, ordinateurs et droits d'accès.
- Adresse IP : Identifiant numérique attribué à un équipement connecté à un réseau permettant sa localisation et sa communication.
- Akamai : Fournisseur mondial de services DNS, CDN et cybersécurité utilisé par certaines entreprises pour améliorer la disponibilité, les performances et la protection de leurs services Internet.
- CDN (Content Delivery Network) : Réseau de serveurs répartis géographiquement permettant d'accélérer la distribution de contenus sur Internet.
- Domainarium : Plateforme développée par IP Twins permettant la gestion centralisée des noms de domaine et des zones DNS.
- DNS Autoritaire : Serveur DNS détenant les informations officielles d'une zone DNS et chargé de répondre aux requêtes concernant cette dernière.
- DNS Récursif : Serveur DNS chargé d'effectuer les recherches nécessaires afin de trouver l'adresse IP correspondant à un nom de domaine demandé par un utilisateur.
- Firewall : Équipement ou logiciel permettant de filtrer les flux réseau entrants et sortants selon des règles de sécurité définies.
- Journalisation (Logging) : Enregistrement des événements et actions réalisés sur un système informatique afin de permettre le suivi, l'audit et l'analyse des incidents.
- Marketplace : Plateforme de vente en ligne permettant à différents vendeurs de commercialiser leurs produits ou services auprès d'utilisateurs.
- Réplication : Processus consistant à copier automatiquement des données d'un système vers un autre afin d'assurer leur cohérence et leur disponibilité.
- Registrar : Organisme accrédité permettant l'enregistrement, le renouvellement, le transfert et la gestion des noms de domaine.
- Sauvegarde (Backup) : Copie de sécurité de données ou de systèmes permettant leur restauration en cas d'incident ou de perte.
- Supervision : Ensemble des mécanismes permettant de surveiller l'état de fonctionnement d'un système, d'un réseau ou d'un service informatique.
- Ticket : Élément créé dans un outil de gestion comme GLPI afin de suivre une demande, une intervention ou un incident.
- Zone DNS : Fichier contenant l'ensemble des enregistrements DNS associés à un ou plusieurs noms de domaine.
- TSIG (Transaction Signature) : Mécanisme d'authentification permettant de sécuriser les transferts de zones DNS entre serveurs autorisés.
- VLAN (Virtual Local Area Network) : Technologie permettant de segmenter logiquement un réseau afin d'améliorer son organisation et sa sécurité.
- ASHRAE : Normes de gestion thermique des salles serveurs.
- Script : Programme informatique écrit dans un langage permettant d'automatiser des tâches sans compilation préalable.
- Système d'Information (SI) : Infrastructure organisée (matériel, logiciel, processus) permettant de collecter, traiter et sécuriser les données d'une entreprise.

BIBLIOGRAPHIE / WEBOGRAPHIE

Normes et Références Institutionnelles

- ISO/IEC 27001:2022 – Information Security Management Systems.
- Directive (UE) 2022/2555 dite NIS2.
- Règlement Général sur la Protection des Données (RGPD).
- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Guide d'Hygiène Informatique.
- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Recommandations relatives à l'administration sécurisée des systèmes d'information.
- Microsoft Security Benchmark.
- ICANN Policies and Procedures.

Documentations Techniques

- Documentation officielle Debian.
- Documentation officielle GLPI.
- Documentation officielle PfSense.
- Documentation officielle Microsoft Azure.
- Documentation officielle Microsoft Defender for Endpoint.
- Documentation officielle Microsoft Intune.
- Documentation officielle Defender for Cloud.
- Documentation officielle ISC BIND9.
- Documentation officielle ICANN.
- Documentation officielle AFNIC.
- Documentation officielle Akamai.
- Documentation officielle FreeBSD.

Sites Internet

- saifeddine-kilani.fr
- https://glpi-project.org
- https://www.pfsense.org
- https://learn.microsoft.com
- https://www.icann.org
- https://www.afnic.fr
- https://www.akamai.com
- https://www.bind9.readthedocs.io
- https://www.freebsd.org
- https://cyber.gouv.fr
- https://www.cnil.fr
- https://www.iso.org
- https://www.cloudflare.com/learning/dns/what-is-dns/
- https://owasp.org
- https://www.debian.org

Ressources internes IP Twins

- Documentation interne relative à l'administration des serveurs DNS.
- Documentation interne relative à la certification ISO 27001.
- Procédures internes de gestion des incidents et des changements.
- Documentation technique Domainarium.
- Documentation technique Turbigo.