Rapport de stage

Technicienne informatique

Aliya MAATIT

Stage réalisé du 14 avril au 20 juin 2025

Tuteur de stage : Romain OGER
Tuteur pédagogique : Fayssal BENKHALDOUN

Etablissement : IUT de Villetaneuse – Sorbonne Paris Nord
Formation : BUT2 Réseaux et Télécommunications
Entreprise d'accueil : MOMA GROUP

Remerciements

Je tiens à remercier l'ensemble des enseignants de l'IUT, qui m'ont accompagnée tout au long de ma formation. Grâce à eux, j'ai pu acquérir de solides bases et développer mes compétences. Ils ont toujours su se montrer disponibles pour répondre à mes questions et me soutenir quand j'en avais besoin.

Je remercie aussi Monsieur Benkhaldoun, mon tuteur pédagogique, pour ses conseils et son aide tout au long de ce stage. Il a su répondre à mes questions concernant les démarches avec l'IUT, m'a orientée dans la rédaction de ce rapport, et m'a toujours encouragée à donner le meilleur de moi-même. Je le remercie également pour la qualité de ses cours de mathématiques pendant ces deux années, et pour l'attention qu'il porte à la réussite de ses étudiants.

Je souhaite également remercier Romain Oger, mon tuteur de stage, de m'avoir offert cette première expérience professionnelle. Merci pour sa disponibilité, sa patience et sa bienveillance tout au long de ces semaines. Il a su me former, répondre à mes questions et me faire découvrir le monde de l'entreprise dans de très bonnes conditions.

Je remercie aussi Aymen Abid, technicien chez Xefi et prestataire chez Moma Group, pour sa gentillesse, sa disponibilité et tous les conseils qu'il a pu me donner. Il a toujours pris le temps de m'aider à progresser et à comprendre ce que je faisais.

Enfin, je remercie toute l'équipe de MOMA GROUP pour leur accueil et leur confiance, ainsi que ma famille pour son soutien constant, que ce soit dans mes recherches de stage ou pendant toute cette expérience.

Sommaire

Abstract

This report is about my first work experience during an internship in IT support and network security. During this time, I learned how to use different tools and how to explain technical problems to people who don't know much about computers. I faced some challenges like managing passwords safely, improving how the company handles staff arrival and departure, and helping users with their problems. These experiences helped me improve my technical skills and my way of communicating. I also realized the importance of teaching users and making security better step by step, for example by using two-factor authentication. I think I could have asked my tutor less and been more confident when talking with users. For the company, I suggest to improve cybersecurity, add better backup systems, and move more data to the cloud. Overall, this internship confirmed my interest in networks and security and gave me useful experience for my future career.

Introduction

Aujourd'hui, la transformation numérique touche toutes les entreprises, quelle que soit leur taille ou leur secteur. Cette évolution entraîne une complexification des systèmes informatiques, ainsi qu'une augmentation des risques liés à la sécurité des données et à la gestion des accès. Dans ce contexte, assurer un support informatique efficace et garantir la sécurité des infrastructures sont devenus des défis majeurs.

Mon stage s'est déroulé dans une entreprise où ces enjeux étaient bien présents, mais où j'ai rapidement constaté que les pratiques sur le terrain pouvaient différer des recommandations théoriques, notamment en matière de sécurité informatique et d'organisation des processus internes. Cela m'a amenée à me poser plusieurs questions : comment concilier les exigences techniques et les contraintes humaines ? Comment sensibiliser des utilisateurs souvent peu familiers avec les outils numériques à adopter de bonnes pratiques ? Et comment organiser un service informatique pour qu'il soit à la fois réactif et sécurisé ?

Cette expérience m'a donc offert l'opportunité d'aborder ces problématiques, en intervenant sur des missions variées : gestion des accès et mots de passe, mise en place de l'authentification multifacteur, assistance aux utilisateurs avec un souci de pédagogie, et gestion du parc informatique via GLPI. Par ailleurs, j'ai participé à la formalisation de procédures, à la communication avec différents services, et à l'accompagnement des utilisateurs dans leur montée en compétences.

Ce stage représentait pour moi une étape essentielle dans mon parcours, me permettant de confronter les savoirs acquis en formation à la réalité du terrain, et de confirmer mon intérêt pour les métiers des réseaux et de la sécurité informatique.

Le rapport qui suit présente d'abord l'entreprise et son organisation, avant de décrire les missions réalisées. J'y analyse ensuite les principaux problèmes rencontrés, les solutions mises en place, ainsi que les enseignements que j'en ai tirés, tant sur le plan technique que relationnel. Enfin, je propose des pistes d'amélioration pour l'entreprise et fais le bilan de cette première immersion professionnelle.

1. Présentation de l'entreprise

1.1. Historique de l'entreprise

Fondé en 1997 par Benjamin Patou, MOMA GROUP est un groupe français reconnu dans les secteurs de la restauration haut de gamme et de l'événementiel de prestige. Le groupe s'est développé autour de trois entités principales, incarnant chacune une expertise spécifique :

- MOMA GROUP : branche historique, dédiée aux activités de restauration et de vie nocturne (restaurants, clubs).
- MOMA EVENT : agence spécialisée en conseil en communication et production événementielle.
- MOMA SELECTION : entité chargée de la gestion et de la privatisation de lieux d'exception pour l'organisation d'événements privés ou professionnels.

Le siège social est situé dans le 16ème arrondissement de Paris et regroupe notamment les équipes de MOMA GROUP et de MOMA SELECTION. MOMA EVENT est, quant à elle, implantée à Saint-Ouen. Le reste des collaborateurs exerce directement sur le terrain, au sein des différents établissements du groupe.

1.2. Activité principale

La réputation de MOMA GROUP repose en grande partie sur ses établissements emblématiques, tels que *Victoria, Andia, Manko* ou encore *Noto*. Cette notoriété dépasse les frontières françaises avec des implantations dans des destinations prestigieuses, notamment Saint-Tropez, Megève, Marrakech, Dubaï ou encore l'Arabie Saoudite.

Les activités de MOMA GROUP s'articulent principalement autour de trois pôles complémentaires : la restauration haut de gamme, les établissements festifs (clubs) et l'événementiel de prestige. En 2023, le groupe comptait environ 800 collaborateurs pour un chiffre d'affaires avoisinant 130 millions d'euros.

Figure 1 : Restaurant Andia Paris

1.3. Organisation interne

En janvier 2025, le groupe a connu une réorganisation majeure à la suite du départ de Benjamin Patou, fondateur historique. Ce départ est intervenu dans le cadre du rachat du groupe par l'investisseur Walter Butler, devenu actionnaire majoritaire. À cette occasion, Benjamin Patou a conservé deux établissements emblématiques : Lapérouse et Lafayette.

Cette réorganisation marque un tournant pour le groupe, avec une volonté affirmée de structurer davantage ses fonctions support, et notamment le pôle informatique.

Le siège est organisé autour des services suivants :

- Comité Exécutif
- Comité de Direction
- Opérations
- Finance et Comptabilité
- Juridique
- Communication
- Ressources Humaines
- Informatique
- Développement et Projets

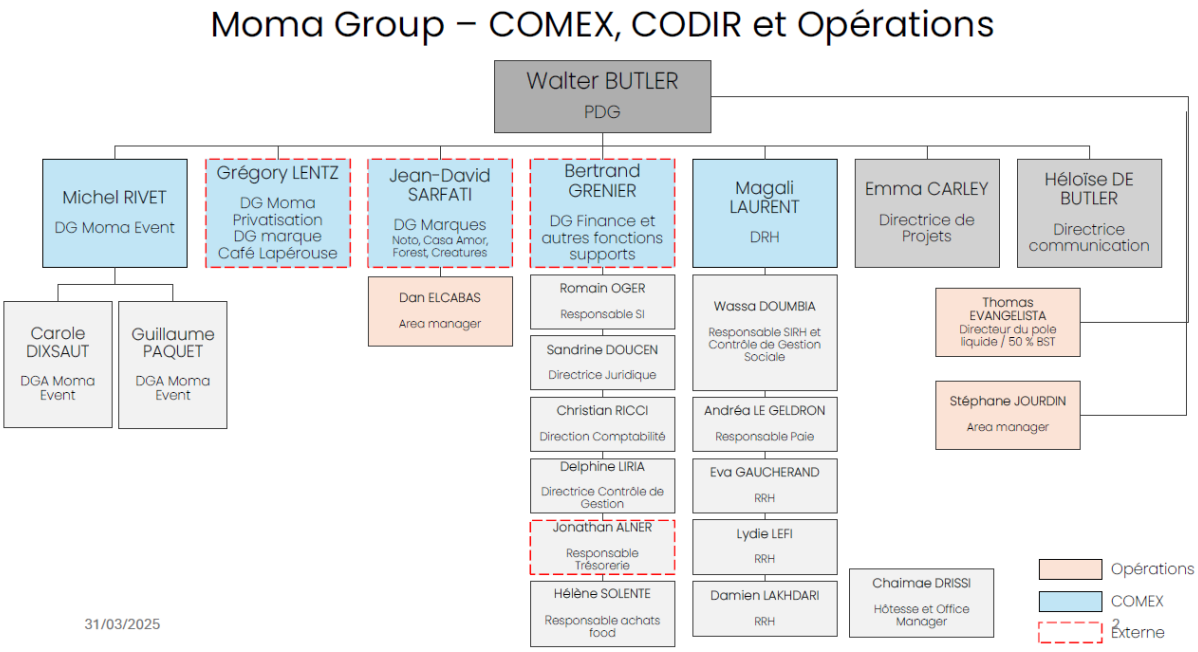


Figure 2 : Organigramme de Moma Group

1.4. Le service informatique et ses missions

Le service informatique repose aujourd'hui sur un modèle hybride, associant compétences internes pour les aspects stratégiques et prestataires externes pour le support technique.

Le service est placé sous la responsabilité de Romain Oger, Directeur des Systèmes d'Information (DSI). Il pilote l'ensemble des projets liés aux systèmes d'information, gère les relations avec les prestataires, et veille à la cohérence des choix technologiques du groupe.

Le DSI s'appuie sur plusieurs partenaires externes et interne pour l'exécution opérationnelle :

- François Vergnet : Responsable des systèmes de caisse (POS), basé à Orléans, en charge du suivi des installations dans les restaurants et leurs administrations.

- Aymen Abid : Technicien informatique de la société XEFI, présent 2 demi-journées par semaine au siège pour les interventions techniques courantes.

- Clément Farron : Consultant indépendant spécialisé en cybersécurité, agissant en tant que RSSI externalisé.

- Société XEFI : En charge de l'infogérance globale, assurant une continuité de service et un accompagnement technique approfondi.

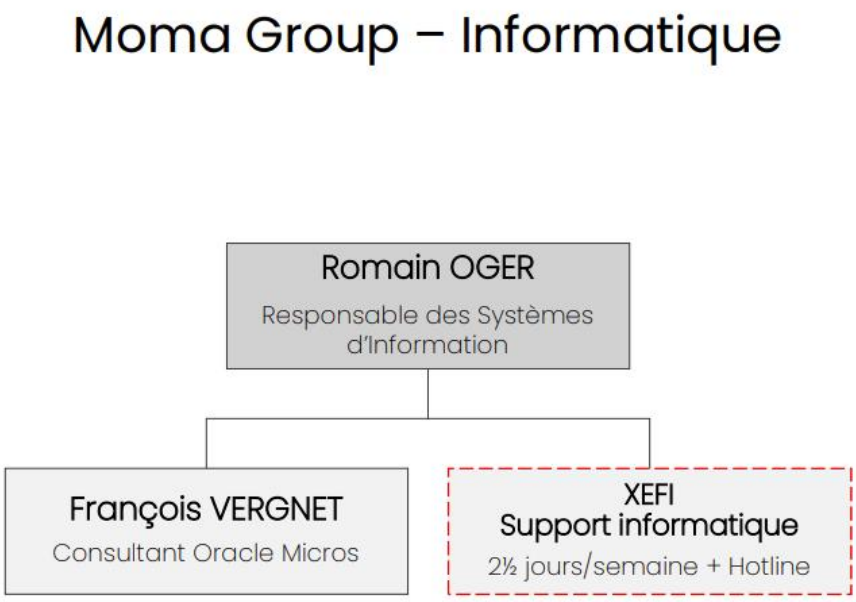


Figure 3 : Organigramme du service IT

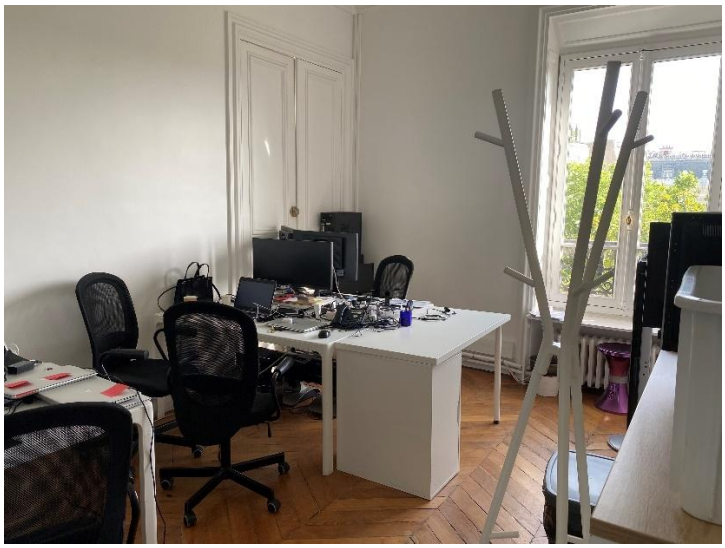


Figure 4 : Bureau du service IT

Missions principales du service informatique :

- Gestion et supervision de l'infrastructure réseau et des systèmes au siège
- Gestion des comptes utilisateurs (création, modification, suppression)
- Suivi des procédures de sauvegarde et de sécurisation des données
- Assistance technique et coordination entre les services internes et les prestataires externes

Le choix d'une organisation externalisée pour l'informatique permet à MOMA GROUP de disposer de compétences pointues tout en gardant la maîtrise stratégique de son système d'information.

1.5. Enjeux numériques et cybersécurité de l'entreprise

Mon stage s'est déroulé dans un contexte de mutation organisationnelle profonde, avec pour objectif principal la structuration du service informatique. Plusieurs défis ont été identifiés par le DSI. Parmi eux, le renforcement de la sécurité des accès utilisateurs, face à des pratiques jusqu'alors peu sécurisées, comme le stockage de mots de passe dans des fichiers non protégés. De plus, l'absence de procédures claires pour la gestion des comptes, notamment lors des départs de collaborateurs, représentait un risque important.

L'hétérogénéité des pratiques informatiques entre les différents établissements compliquait par ailleurs la supervision globale des systèmes. Face à ces constats, le groupe s'est fixé comme objectif une centralisation progressive des ressources informatiques vers le siège, afin d'harmoniser les pratiques et de renforcer la sécurité.

Dans ce contexte, mes missions ont porté sur plusieurs axes. J'ai contribué à la rédaction et à l'amélioration des procédures internes de gestion des comptes utilisateurs. J'ai également participé à l'analyse des vulnérabilités existantes et formulé des recommandations pour améliorer la gestion des mots de passe. Parmi ces recommandations figuraient l'intégration d'un gestionnaire de mots de passe, la définition d'une politique de mots de passe robustes, ainsi que des actions de sensibilisation auprès des collaborateurs.

J'ai également participé aux projets techniques supervisés par le DSI, portant notamment sur l'amélioration de l'infrastructure réseau et le déploiement progressif de bonnes pratiques en cybersécurité.

Ce stage m'a offert une immersion concrète dans les enjeux liés à la cybersécurité dans un environnement multisite exigeant, marqué par des activités sensibles et une transformation organisationnelle en cours.

2. Description du projet(s) et/ou travaux effectués

Au cours de mon stage de 10 semaines au sein du service informatique de MOMA GROUP, j'ai été pleinement intégrée à l'équipe en place et ai contribué activement à diverses missions techniques et organisationnelles. Ce stage s'est déroulé dans un contexte particulier, marqué par une restructuration du service informatique et une nécessité accrue de formaliser et sécuriser les processus internes, en réponse à des enjeux techniques, économiques et humains.

2.1. Objectifs des travaux

L'objectif principal de mon stage était de contribuer au bon fonctionnement du système d'information (SI), à travers des missions variées, alliant assistance, analyse, gestion documentaire et cybersécurité. Plus précisément, il s'agissait de :

- Assurer un support technique de niveau 1 et 2 aux utilisateurs, en local ou à distance via BeyondTrust.

- Participer activement à l'amélioration de la sécurité informatique en interne, notamment par la mise en place de l'authentification multifacteur (MFA) et par la sensibilisation des utilisateurs.

- Participer aux projets stratégiques, en particulier dans le cadre de la sécurisation de l'environnement Microsoft 365 et de la préparation de migrations techniques.

- Accompagner et former les stagiaires pour garantir la continuité et la pérennité des actions menées

2.2. Contexte technique

Le service informatique de MOMA GROUP a connu plusieurs bouleversements ces dernières années, notamment liés aux changements d'effectifs et à la crise sanitaire.
Avant la pandémie de 2020, l'équipe informatique comptait quatre personnes : un Directeur des Systèmes d'Information (DSI), un gestionnaire de bases de données, un consultant Oracle et un technicien support. Cependant, la crise sanitaire a brutalement stoppé l'activité principale du groupe, entraînant une forte baisse des revenus. Pour faire face à cette situation, l'entreprise a dû contracter un prêt garanti par l'État, sans pour autant parvenir, après la reprise, à retrouver un équilibre financier suffisant pour rembourser cet emprunt. Cela a conduit à des réductions budgétaires, touchant directement le service informatique.

Après la crise, le service est passé de quatre à trois personnes. Peu de temps après, le DSI est parti en arrêt maladie longue durée. Pour assurer la continuité, mon tuteur — initialement gestionnaire de données — a été nommé DSI par nécessité, réduisant encore les effectifs à seulement deux personnes : le nouveau DSI et le consultant Oracle.

Face à cette situation critique et à une charge de travail croissante (accumulation de tickets, difficultés à maintenir les systèmes et procédures), le DSI a obtenu l'accord de la direction pour faire appel à un prestataire externe, la société XEFI, qui a mis à disposition un technicien informatique deux journée et demie par semaine (mercredi après-midi et vendredi). Bien que ce renfort ait permis d'alléger temporairement la charge liée au support, cela restait insuffisant pour répondre aux besoins opérationnels et stratégiques du groupe. C'est dans ce contexte que j'ai été recrutée en tant que stagiaire, avec un autre stagiaire, afin de renforcer le support informatique, participer à la réorganisation du service et contribuer à des projets plus structurels, notamment en matière de sécurisation des systèmes et de formalisation des procédures internes.

En parallèle, l'infrastructure serveurs de MOMA GROUP est entièrement externalisée auprès de *XEFI Ingénierie*, une filiale du groupe *XEFI*, qui assure l'hébergement et l'administration des serveurs critiques, situés à Lyon. Cela concerne notamment les serveurs Active Directory (AD), le VPN, ainsi que d'autres services essentiels à l'activité.

L'environnement technique reposait sur plusieurs outils essentiels pour assurer le bon fonctionnement du système d'information et du support informatique. Le logiciel *GLPI* (Gestion Libre de Parc Informatique), une solution open source, était utilisé pour la gestion des tickets, le suivi de ceux-ci et l'inventaire du parc informatique.

Pour les prises en main à distance des postes de travail, le service avait recours à *BeyondTrust Remote Support*, facilitant le dépannage même à distance.

La messagerie professionnelle et les outils collaboratifs reposaient sur *Microsoft 365*, avec *Admin 365* utilisé par les administrateurs pour gérer les comptes, les groupes de sécurité, les boîtes partagées et les licences.

Les postes de travail étaient protégés par *Malwarebytes*, un antivirus installé localement sur chaque machine. La gestion des accès physiques au siège était assurée via *Optimabox*, un système de contrôle par badge. Enfin, l'infrastructure réseau et certains services externes, notamment l'hébergement de sites Internet ou de services annexes, étaient gérés via *OVH*.

Cette diversité d'outils permettait de couvrir les besoins essentiels de l'entreprise, tout en laissant apparaître certaines limites liées à l'absence de formalisation, au manque d'automatisation et aux ressources humaines restreintes.

2.3. Mes missions

Au cours de ce stage, j'ai eu l'opportunité de participer à plusieurs missions variées, qui m'ont offert une expérience concrète du fonctionnement d'un service informatique en entreprise. Ces activités m'ont permis de développer mes compétences techniques tout en contribuant activement à des projets stratégiques visant à renforcer l'efficacité et la sécurité du système d'information.

2.3.1. Support informatique aux utilisateurs

L'une de mes principales responsabilités a été d'assurer le support informatique de premier niveau aux utilisateurs. Le contexte était particulier : ce support était habituellement assuré par un technicien externe, salarié de XEFI, qui n'intervenait que deux demi-journée epar semaine. En dehors de ces créneaux, les appels à la hotline informatique étaient redirigés vers notre bureau, me conduisant à prendre en charge la majorité des demandes quotidiennes.

Les sollicitations étaient diverses : problèmes d'accès aux messageries professionnelles, dysfonctionnements matériels, difficultés d'impression, incidents liés aux applications métiers ou encore configuration de nouveaux équipements. Ce contact régulier avec les utilisateurs m'a permis d'affiner mes capacités d'écoute et d'adaptation, notamment face à des interlocuteurs

peu familiers avec les outils numériques. J'ai appris à poser des questions précises et à reformuler les problèmes afin d'en cerner la cause réelle. J'ai aussi su adapter mon discours pour vulgariser les notions techniques quand cela s'avérait nécessaire.

Parmi ces interventions, j'étais également chargée de la gestion des incidents techniques dans la salle de réunion, utilisée pour des réunions internes ou des rendez-vous clients. Cette salle était équipée de l'outil ClickShare, un système de partage d'écran sans fil permettant la projection depuis un ordinateur portable.

Figure 5 : Salle de réunion

Mon rôle consistait à intervenir dès qu'un problème technique se présentait lors de l'utilisation de la salle (absence d'image ou de son, déconnexion de l'outil, micro ou caméra défectueux, etc.). Dans ces cas-là, je procédais à une remise à défaut complète des équipements : déconnexion et reconnexion des périphériques, vérification de l'alimentation, redémarrage du système ClickShare si nécessaire, contrôle des câblages.

Au-delà de ces interventions correctives, j'accompagnais également les collaborateurs dans l'utilisation de l'outil, notamment ceux qui n'avaient jamais utilisé ClickShare. Je leur expliquais de manière simple comment connecter leur appareil, utiliser le bouton de partage ou passer en mode présentation. Cette pédagogie permettait de prévenir de futurs incidents liés à une mauvaise utilisation et contribuait à l'autonomie des équipes.

Pour les interventions à distance, j'utilisais BeyondTrust, facilitant la prise en main rapide des postes concernés. En collaboration avec le technicien externe, je gérais également la boîte mail

dédiée au support, assurant le suivi des tickets et sollicitant l'équipe pour les demandes nécessitant validation ou expertise particulière.

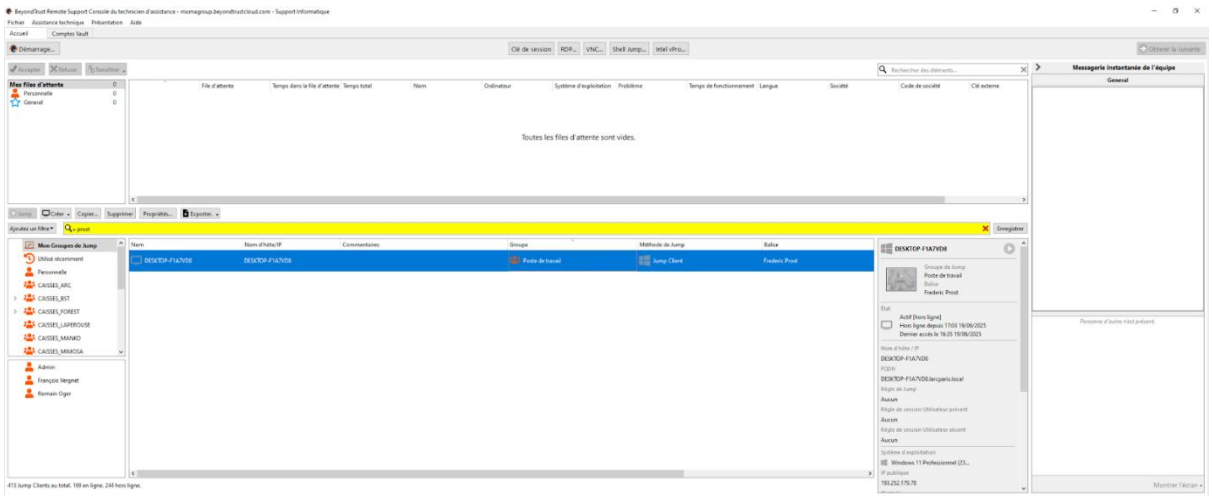


Figure 6 : Interface de Beyond Trust

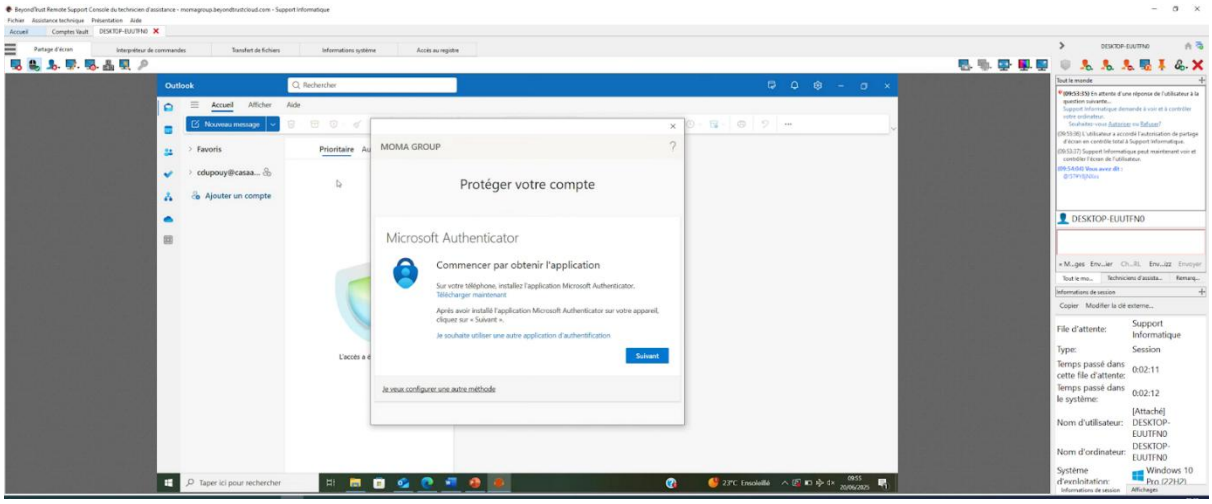


Figure 7 : Partage d'écran avec Beyond Trust

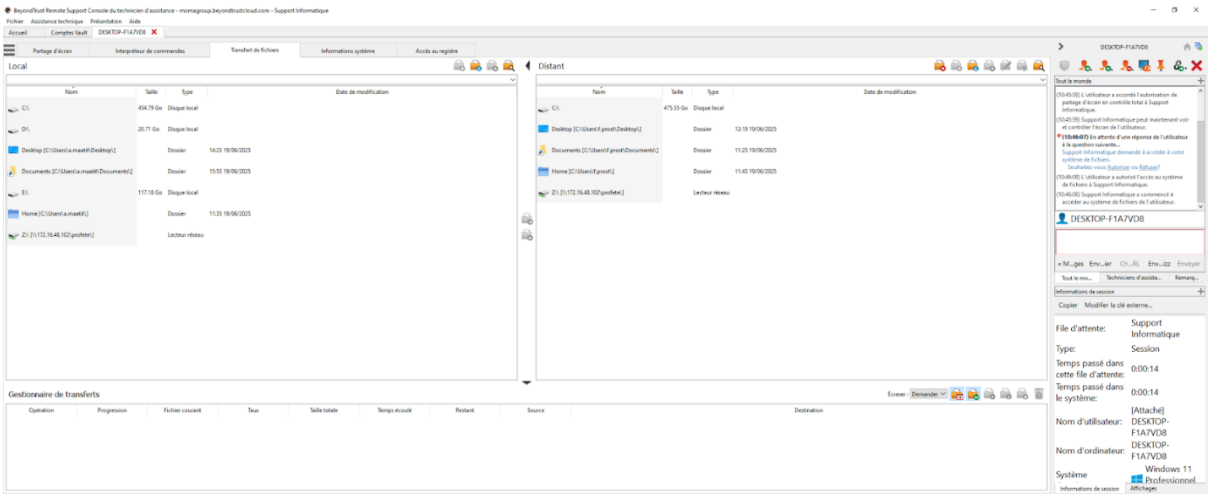


Figure 8 : Transfert de fichiers avec Beyond Trust

Progressivement, les collaborateurs ont pris l'habitude de me solliciter directement, ce qui a renforcé la relation de confiance et instauré une réelle proximité. Cette dimension humaine, combinée aux enjeux techniques, a été pour moi une expérience particulièrement enrichissante.

2.3.2. Formation des stagiaires

Durant mon stage, j'ai également eu l'opportunité de former deux stagiaires aux profils différents.

- Léa, étudiante en RH et gestion, qui a effectué un tour des différents services avant de rester deux semaines en informatique. Malgré sa méconnaissance initiale de l'informatique, je l'ai accompagnée et formée en vulgarisant les concepts techniques pour la rendre autonome sur certaines tâches telles que la création d'adresses mail, la préparation de badges, ou encore la communication auprès des collaborateurs pour l'information sur la mise en place du MFA.

- Azzedine, étudiant en informatique et réseaux, que j'ai formé sur des aspects plus techniques : explications des procédures internes, présentation de la structure de l'entreprise, identification des problèmes récurrents, préparation des postes informatiques pour les collaborateurs, et utilisation des outils de gestion et support. Cette expérience a renforcé mes capacités pédagogiques et d'adaptation à différents niveaux de connaissances.

2.3.3. Mise en place de l'authentification multi-facteur (MFA)

Dès mon arrivée, j'ai identifié plusieurs faiblesses dans la gestion de la sécurité des accès informatiques. Certaines pratiques héritées d'anciennes organisations du service informatique, comme l'usage de fichiers Excel contenant des identifiants sensibles (comptes Office 365, Active Directory), ne correspondaient plus aux standards actuels de cybersécurité.

J'ai proposé à mon tuteur la mise en place progressive de l'authentification multi-facteur (MFA) sur l'ensemble des comptes Office 365. Le déploiement s'est organisé par vagues successives, en commençant par les collaborateurs occupant des fonctions stratégiques (direction, responsables de services), puis en l'étendant progressivement à l'ensemble des effectifs, y compris le personnel opérationnel.

Cette démarche a nécessité un accompagnement attentif. L'activation du MFA entraînait en effet une déconnexion automatique des sessions Office, parfois perçue comme contraignante par les utilisateurs. Pour faciliter cette transition, j'ai rédigé une procédure détaillée que j'ai améliorée au fil des retours et des difficultés rencontrées.

La mise en œuvre de cette mesure a permis de renforcer significativement la sécurité globale des accès aux ressources informatiques de l'entreprise.

2.3.4. Préparation de la migration des comptes Office 365

Dans le cadre de l'évolution du système d'information, j'ai également participé à la préparation de la migration des comptes Office 365. Ma première mission a été de réaliser, avec mon tuteur, un état des lieux complet des domaines rattachés à l'infrastructure via l'interface OVH. Cette analyse a permis d'identifier et de supprimer les domaines obsolètes, notamment ceux d'anciens établissements, dans une logique de simplification et de rationalisation.

Durant cette phase, j'ai assuré un rôle d'interface entre le service informatique et les utilisateurs, afin d'expliquer les démarches à suivre et de répondre aux interrogations. La migration technique des comptes a ensuite été confiée au technicien externe.

2.3.5. Renforcement de la sécurité des mots de passe

Toujours dans une logique d'amélioration de la sécurité, j'ai également contribué à la refonte des pratiques liées à la gestion des mots de passe. Avant mon arrivée, ceux-ci étaient souvent faibles, parfois identiques pour plusieurs comptes, et conservés en clair dans les fichiers mentionnés précédemment.

J'ai donc généralisé l'utilisation de mots de passe robustes et aléatoires lors de la création de comptes ou de la préparation de nouveaux postes. Par mesure de sécurité, ces mots de passe n'étaient plus consignés dans des fichiers, d'autant plus qu'ils pouvaient être réinitialisés si besoin. J'activais systématiquement l'option « changer le mot de passe à la première connexion » afin que l'utilisateur soit le seul à connaître ses identifiants définitifs.

Ces actions, combinées à l'instauration de l'authentification multi-facteur, ont contribué à renforcer la sécurité globale du système d'information.

2.3.6. Gestion et mise à jour du parc informatique via GLPI

J'ai également participé activement à la remise à jour de l'inventaire informatique à l'aide de l'outil GLPI, qui avait été partiellement délaissé par manque d'effectifs. La base comportait de nombreuses incohérences : matériels volés ou détruits encore référencés, doublons, erreurs d'affectation…

À chaque intervention technique, je procédais à une mise à jour rigoureuse, en ajoutant des commentaires détaillés permettant de conserver un historique précis (ancien utilisateur, usage particulier, spécificités du matériel).

J'ai aussi contribué à organiser, avec la société Confia (spécialisée dans la destruction sécurisée de matériel informatique), le traitement des équipements devenus obsolètes ou hors d'usage (ordinateurs, téléphones, caisses, tablettes…).

Figure 9 : Matériels détruits par Confia

2.3.7. Sensibilisation au phishing avec Mantra

La sensibilisation des utilisateurs joue un rôle essentiel dans la sécurisation du système d'information. Au cours de mon stage, j'ai participé à la mise en place de la solution Mantra, un outil permettant d'organiser des campagnes régulières de faux emails de phishing. Ces messages sont conçus pour ressembler à de vrais courriels internes (avec logos, signatures, noms de responsables), afin d'évaluer la vigilance des collaborateurs.

Selon leurs réactions (clics, saisies d'informations, signalement), Mantra fournit un retour immédiat à l'utilisateur, accompagné d'explications pédagogiques. L'outil intègre également des

modules de formation interactifs accessibles via Teams, avec l'assistance d'un chatbot dédié. Un tableau de bord permet ensuite de suivre les résultats et les progrès individuels.

Cette démarche a permis de renforcer la vigilance collective, notamment après plusieurs cas d'attaques réelles subies par l'entreprise par le passé.

2.3.8. Interventions sur sites

Durant mon stage, j'ai eu l'occasion de participer à deux interventions sur sites :

- Intervention au *Manko* : À la suite d'un incendie dans les cuisines, de la suie s'était répandue dans tout le restaurant, qui ne disposait pas de fenêtres. Des travaux complets étaient en cours pour la remise en état. Notre mission principale était de déplacer une baie informatique vers un nouvel emplacement. Nous avons rencontré les prestataires informatiques pour vérifier la pertinence du devis, clarifier les contrats à résilier (notamment 2-3 contrats de téléphonie inutiles) et valider la configuration du nouvel emplacement. L'ancienne baie était très désorganisée, avec un câblage enchevêtré et une sécurité insuffisante (baie non verrouillée).

Figure 10 : Restaurant Manko avant l'incendie

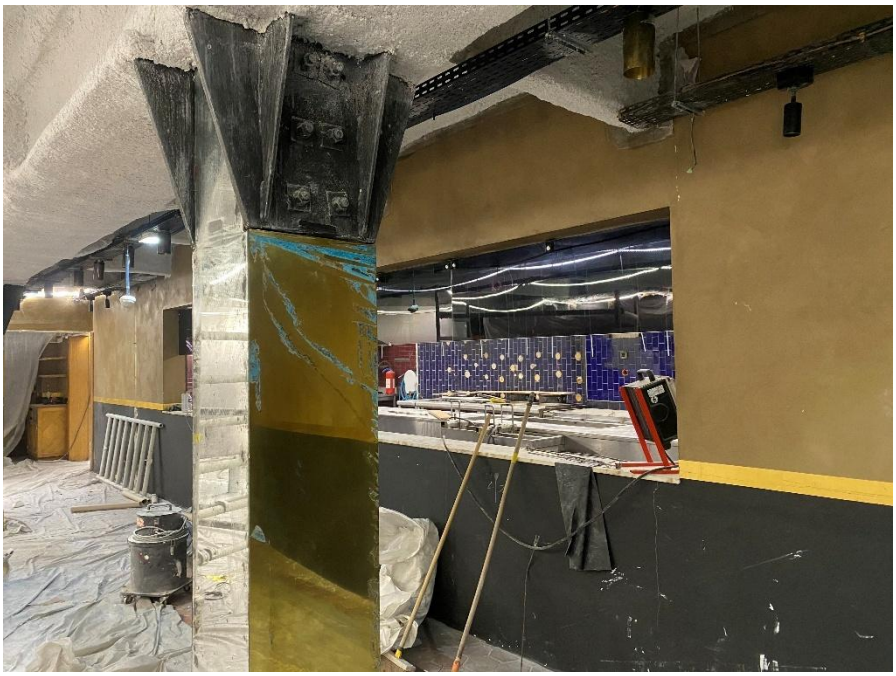


Figure 11: Restaurant Manko après l'incendie

Figure 12 : Ancienne baie à déplacer

- Intervention pour Moma Group chez *Lapérouse* : Nous avons récupéré des caisses Oracle Micros appartenant à Moma Group. Le matériel a été transporté avec un véhicule

de fonction et entreposé dans le bureau informatique de l'entreprise. Cette intervention a permis d'assurer une bonne traçabilité et une gestion sécurisée du matériel récupéré.

2.3.9. Conclusion

Ces différentes missions m'ont permis d'acquérir une solide expérience dans la gestion du parc informatique, la sécurisation des systèmes d'information, et l'accompagnement des utilisateurs. Ce stage a été particulièrement formateur, tant sur le plan technique que relationnel, et m'a offert une vision globale et concrète des enjeux liés au métier.

2.4. Compétences mobilisées

Au cours de ce stage, j'ai mobilisé plusieurs compétences techniques que j'ai acquises dans le cadre de ma formation en BUT Réseaux et Télécommunications, notamment en systèmes, en réseaux, en cybersécurité et en gestion de parc informatique.

En tant qu'étudiante en deuxième année de BUT Réseaux et Télécommunications, j'ai pu m'appuyer sur les bases solides que j'ai acquises dans les différents enseignements. Même si l'administration du réseau de l'entreprise était principalement déléguée à XEFI, mon rôle de technicienne informatique m'a permis d'utiliser, directement ou indirectement, certaines notions vues en cours.

2.4.1. Compétences en réseau et systèmes

Les connaissances acquises lors des modules de réseaux (adressage IP, DNS, routage…) m'ont permis de mieux comprendre l'architecture du système d'information de l'entreprise. Cela m'a également été utile pour diagnostiquer certains incidents, notamment lorsqu'ils étaient liés à des problèmes de connexion aux serveurs ou à des ports bloqués.

Bien que je n'aie pas été directement chargée de l'administration des équipements réseau (switchs, routeurs, etc.), ma capacité à comprendre rapidement les schémas d'infrastructure réseau et à échanger avec le prestataire externe s'est révélée précieuse.

Sur la partie système, mes bases en Linux et en commandes Bash m'ont facilité la prise en main de l'environnement Windows Server et des scripts PowerShell. Même si je n'avais jamais utilisé PowerShell auparavant, la logique de ligne de commande et de scripting vue en cours m'a permis de monter rapidement en compétences pour comprendre et adapter les procédures.

2.4.2. Compétences en cybersécurité

Le domaine de la cybersécurité a été au cœur de mes missions, et c'est sans doute l'aspect où j'ai le plus mis en pratique mes apprentissages. Les enseignements théoriques et pratiques suivis à l'IUT, notamment en matière de sécurité des systèmes d'information, m'ont permis de :

- Proposer et mettre en œuvre l'authentification multi-facteur (MFA), que j'ai su présenter comme une solution efficace et prioritaire pour sécuriser les accès des utilisateurs.

- Renforcer les pratiques de gestion des mots de passe, en générant des mots de passe robustes et en mettant en place des procédures sécurisées pour leur transmission et leur renouvellement.

- Comprendre et participer à la sensibilisation au phishing, en utilisant notamment l'outil *Mantra MS*, que nous avons intégré pour former les collaborateurs aux risques liés aux emails malveillants. Grâce aux cours de cybersécurité, j'ai parfaitement saisi les enjeux et pu expliquer les risques aux collaborateurs de manière claire et adaptée à leurs usages.

Les bonnes pratiques abordées lors des travaux pratiques de cybersécurité ont été un véritable socle pour mener ces actions avec pertinence.

2.4.3. Compétences en communication technique

Enfin, un autre aspect important de mes compétences mobilisées a été la communication. Grâce aux projets réalisés à l'IUT et aux exposés techniques que nous avons régulièrement présentés, j'ai pu adapter mon discours face aux utilisateurs, vulgariser les concepts techniques, et assurer un accompagnement personnalisé. Cela a été particulièrement utile lors du déploiement de la MFA et de la gestion quotidienne du support.

3. Organisation de l'étude (planning)

L'organisation de mes missions durant ce stage a été pensée pour allier apprentissage progressif, montée en compétences, et autonomie dans l'exécution. Cette structuration m'a permis non seulement de développer mes capacités techniques mais également de renforcer mes compétences transversales telles que la communication, la gestion du temps, et le travail d'équipe.

Mon organisation s'est naturellement construite autour de plusieurs grandes phases : une phase d'intégration, une phase d'action avec la prise en main de projets spécifiques (comme le déploiement de la MFA), et enfin une phase de transmission et de pérennisation des compétences acquises. La répartition de ces étapes dans le temps s'est appuyée sur un dialogue constant avec mon tuteur et l'équipe informatique, ainsi que sur les priorités organisationnelles de l'entreprise.

3.1. Phase initiale (semaines 1 et 2)

Les deux premières semaines ont constitué une période d'adaptation et de découverte indispensable à la réussite de mon stage. Durant cette phase, j'ai été formé aux outils spécifiques utilisés dans l'entreprise, notamment :

- Admin Microsoft 365 : gestion des utilisateurs, création/modification des boîtes mail, activation et gestion de licences, activation de fonctionnalités avancées.
- BeyondTrust (anciennement Bomgar) : outil sécurisé de prise en main à distance indispensable pour le support technique.
- GLPI : gestionnaire de tickets et base de connaissances interne.
- Optima Box : logiciel métier utilisé pour la gestion commerciale et administrative par les collaborateurs.

En parallèle de l'apprentissage de ces outils techniques, j'ai aussi cherché à comprendre l'organisation fonctionnelle de l'entreprise : comment étaient structurés les différents services, qui étaient mes interlocuteurs réguliers, comment fonctionnaient les relations avec les prestataires, et quelle était la politique de sécurité informatique en place.

Cette phase a aussi été l'occasion de mettre en pratique mes compétences acquises à l'IUT. Chaque ticket de support représentait une nouvelle opportunité d'apprentissage. Par exemple, pour chaque demande utilisateur :

- J'établissais un diagnostic en fonction des symptômes décrits.
- Je faisais des recherches dans la base de connaissance ou via des ressources externes si nécessaire. 2 jours et demi
- Je proposais une solution adaptée et je m'assurais du retour utilisateur pour valider sa satisfaction.

Mon tuteur m'a confié très tôt une autonomie progressive dans le traitement des tickets afin que je puisse monter en compétences rapidement. Cette immersion a constitué une base solide pour aborder les phases suivantes.

3.2. Déploiement de la MFA (à partir de la semaine 3)

Dès la troisième semaine, j'ai pris l'initiative de proposer la mise en place de l'authentification multi-facteur (MFA) pour renforcer la sécurité des comptes Office 365. Après validation par mon tuteur, j'ai élaboré une procédure claire et détaillée pour accompagner les utilisateurs dans l'activation de la MFA. Le déploiement s'est fait progressivement, par lots hebdomadaires, afin de faciliter le suivi et la gestion des retours. Chaque mercredi, un lot de collaborateurs sélectionnés selon leur responsabilité (ceux avec les accès les plus sensibles étant priorisés) recevait un mail personnalisé, généré via publipostage, expliquant la procédure. Les utilisateurs disposaient d'une semaine pour procéder à l'activation, après quoi j'activais la MFA via l'Admin 365, provoquant une déconnexion automatique de toutes les sessions Office 365 sur tous leurs appareils.

Ce processus demandait un suivi rigoureux, notamment pour identifier les personnes injoignables ou absentes, en contactant leurs supérieurs, collègues ou les ressources humaines pour vérifier leur statut. Ce déploiement, bien que progressif, reste un projet majeur avec encore plusieurs centaines de comptes à sécuriser, ce qui laisse place à une continuation et un suivi post-stage.

3.3. Gestion quotidienne des demandes

En parallèle du projet MFA, j'étais chargé de traiter l'ensemble des demandes quotidiennes transmises via le système de tickets GLPI. Ces demandes recouvraient un large spectre d'actions :

- Création et configuration de postes de travail pour les nouveaux arrivants : installation de Windows 10/11, paramétrage des accès réseau, configuration des imprimantes, ajout aux groupes AD.
- Gestion des droits d'accès aux fichiers partagés ou aux équipes Teams.
- Attribution de badges d'accès physiques en collaboration avec le service RH.
- Dépannages divers : problèmes d'impression, lenteurs réseau, configuration de boîtes mails Outlook, récupération de fichiers supprimés.

J'ai rapidement appris à hiérarchiser ces demandes en fonction de leur impact métier, afin de ne pas bloquer les collaborateurs dans leurs tâches essentielles.

Cette gestion quotidienne m'a permis de développer des compétences en communication technique, car il était nécessaire d'adapter mon discours selon le niveau informatique de l'utilisateur concerné.

3.4. Réunions hebdomadaires

Chaque vendredi, je participais à une réunion hebdomadaire avec l'ensemble de l'équipe informatique, composée de François (expert Oracle), Aymen (technicien XEFI) et Romain (DSI). Ces points réguliers permettaient de faire le bilan des tickets en cours, d'échanger sur les projets en développement et de partager idées ou propositions d'amélioration. Ces réunions étaient essentielles pour garder une vision d'ensemble et ajuster les priorités en fonction des urgences remontées.

3.5. Formation des stagiaires

À mi-parcours, une nouvelle stagiaire est arrivée dans le service sans que cela soit initialement prévu. J'ai dû assurer sa formation rapidement, en lui transmettant les bases techniques et les

bonnes pratiques du service. Plus tard, durant ma dernière semaine, j'ai également formé Azzedine, le nouveau stagiaire informatique, afin de lui transférer mes missions et assurer une continuité efficace des tâches.

3.6. Suivi mensuel des campagnes Mantra

Une fois par mois, un point était organisé avec l'équipe Mantra pour suivre l'avancement des campagnes de sensibilisation au phishing. Cette étape permettait d'évaluer l'efficacité des campagnes, de détecter les difficultés rencontrées par les collaborateurs, et d'adapter les supports ou les méthodes de sensibilisation en conséquence.

3.7. Gestion autonome du temps

Enfin, j'ai appris à gérer mon emploi du temps de façon autonome, en conciliant les contraintes des collaborateurs (horaires, réunions, pauses déjeuner) avec mes propres disponibilités. Cette flexibilité m'a permis d'intervenir rapidement sur des problèmes complexes nécessitant un contact direct avec les utilisateurs ou une prise en main à distance des postes de travail.

4. Analyse des problèmes rencontrés et justification des solutions proposées

Cette première expérience en entreprise a été particulièrement formatrice, car elle m'a permis de confronter les notions théoriques apprises en formation à la réalité du terrain. Très rapidement, j'ai pu constater que les pratiques en entreprise ne sont pas toujours alignées avec les bonnes pratiques recommandées, notamment en matière de sécurité informatique et d'organisation des processus internes. Plusieurs dysfonctionnements sont ainsi apparus, que j'ai analysés et pour lesquels j'ai proposé des solutions adaptées, aussi bien sur le plan technique qu'organisationnel.

4.1. Gestion des mots de passe et risques associés

Le premier point critique concernait la gestion des mots de passe. J'ai constaté que certains identifiants sensibles étaient stockés en clair dans des fichiers Excel. Cette pratique présente un risque majeur en cas d'accès non autorisé au fichier. Plutôt que d'imposer un outil tiers dans l'immédiat, j'ai d'abord sensibilisé mes collègues à ces risques, en rappelant les bases de la protection des informations confidentielles. J'ai recommandé par la suite l'utilisation d'un

gestionnaire de mots de passe chiffré, mieux adapté à un environnement professionnel et permettant une gestion sécurisée et centralisée des accès.

Cette démarche s'inscrit dans une logique de montée progressive en sécurité, en commençant par corriger les pratiques à risque avant d'introduire des outils supplémentaires.

4.2. Absence de procédure claire pour les entrées et sorties des collaborateurs

Un autre problème récurrent concernait l'absence de procédure claire lors de l'arrivée ou du départ d'un collaborateur. Dans certains cas, j'apprenais le départ d'un salarié simplement en découvrant du matériel inutilisé dans l'armoire informatique, ou en discutant avec des collègues. Ce manque de communication interne générait des risques importants : matériel non récupéré, comptes toujours actifs et donc exploitables par d'anciens employés, ou encore envoi potentiel de messages malveillants par vengeance.

Pour pallier ce problème, nous avons organisé une réunion avec le service des ressources humaines afin de formaliser une procédure claire. Chaque départ devait désormais donner lieu à l'ouverture d'un ticket dans GLPI, accompagné d'une feuille de restitution du matériel. Cette nouvelle organisation permet d'assurer un suivi rigoureux de chaque collaborateur sortant et renforce la sécurité globale de l'entreprise.

4.3. Communication avec les utilisateurs et diagnostic des pannes

Dans le cadre du support informatique, j'ai aussi constaté que de nombreux utilisateurs avaient des difficultés à exprimer précisément leurs problèmes, souvent par méconnaissance des termes techniques. Cela compliquait considérablement l'établissement d'un diagnostic fiable et rallongeait inutilement le temps de résolution.

Face à cette situation, j'ai adopté une démarche pédagogique : poser des questions simples, éviter le jargon technique, reformuler si nécessaire et accompagner l'utilisateur pas à pas. En parallèle, j'ai rédigé des guides simplifiés avec des captures d'écran pour faciliter la compréhension, ce qui a permis de fluidifier les échanges et d'améliorer l'efficacité globale du support.

4.4. Mise en place complexe de l'authentification multifacteur (MFA)

L'activation progressive de l'authentification multifacteur a également généré de nombreuses difficultés. Plusieurs utilisateurs n'avaient pas anticipé cette obligation et nous sollicitaient en

urgence au moment de l'activation, souvent paniqués à l'idée de perdre l'accès à leurs mails professionnels.

Pour répondre à ces problématiques, nous avons ajusté le processus : envoi de rappels réguliers avant l'activation, simplification des guides explicatifs, accompagnement par téléphone, et prise en main à distance via BeyondTrust. Certaines catégories de personnel, comme ceux travaillant en cuisine ou en salle, étaient plus difficiles à joindre par e-mail. Dans ces cas, le téléphone ou l'intermédiaire de leurs responsables hiérarchiques était privilégié.

Enfin, pour les utilisateurs refusant d'installer l'application sur leur téléphone personnel, une alternative leur a été proposée sous forme d'extension navigateur. Cette solution a permis de concilier exigences de sécurité et respect de la vie privée.

4.5. Autonomisation des utilisateurs et gestion du temps du support

Un autre point clé a été la gestion de la dépendance excessive de certains utilisateurs vis-à-vis du support. Certains demandaient de l'aide même pour des tâches simples réalisables en suivant les guides. Afin de gagner en efficacité, nous avons opté pour une posture plus formatrice : accompagner une première fois, puis encourager l'utilisateur à utiliser les ressources mises à sa disposition.

Cette approche permet de responsabiliser les utilisateurs et d'alléger la charge de travail du support, tout en développant l'autonomie numérique de chacun.

4.6. Transition nécessaire vers Windows 11

Enfin, la fin de support annoncée pour Windows 10 a soulevé un nouveau défi : identifier quels ordinateurs étaient compatibles avec Windows 11. Pour cela, j'ai mis en place un fichier récapitulatif listant chaque poste et ses composants techniques, associé à un utilitaire de vérification de compatibilité. Les utilisateurs ont été sollicités par e-mail pour exécuter cette vérification sur leur poste.

Cette démarche permet de planifier sereinement la migration, d'éviter les mauvaises surprises techniques, et de préparer progressivement l'entreprise à cette transition.

4.7. Gestion des accès VPN

L'accès distant via VPN a également été un sujet sensible. Entre erreurs d'identifiants de la part des utilisateurs, mauvaise compréhension du fonctionnement de l'outil et dysfonctionnements techniques côté serveur, les incidents étaient fréquents.

La solution a été multiple : accompagnement individuel des utilisateurs, simplification des guides, et création de tickets auprès de notre prestataire (XEFI) pour résoudre les problèmes côté infrastructure. Cela a permis de maintenir la continuité d'accès, notamment pour les collaborateurs en télétravail.

4.8. Conclusion

Dans l'ensemble, cette expérience m'a appris à concilier les impératifs techniques avec les réalités humaines. Chaque solution mise en place reposait sur trois principes essentiels : sécuriser les accès, simplifier les démarches pour les utilisateurs, et responsabiliser ces derniers afin d'éviter une dépendance totale au service informatique. Cette approche équilibrée a permis d'améliorer à la fois la sécurité, l'efficacité du support et l'autonomie des collaborateurs.

5. Mise en évidence des résultats

Au cours de cette expérience, plusieurs changements concrets ont été mis en place afin de corriger les dysfonctionnements identifiés. Ces améliorations ont eu un impact direct sur la qualité du support, la sécurité des systèmes et l'organisation interne de l'entreprise. Les résultats suivants illustrent ces évolutions.

5.1. Gestion des mots de passe : amélioration de la sécurité

Avant mon intervention, les mots de passe utilisés étaient généralement simples et peu sécurisés. Certains mots de passe critiques ressemblaient par exemple à *Zur29382*, ce qui les rendait vulnérables aux attaques par force brute ou par dictionnaire. Après avoir sensibilisé les utilisateurs et recommandé l'utilisation de générateurs de mots de passe complexes, nous sommes progressivement passés à des mots de passe bien plus robustes, tels que *5#Hd2@d6Ni!M*. Cette évolution a renforcé la sécurité globale des comptes internes.

Pour accompagner ce changement, j'ai également présenté des solutions d'outils de gestion de mots de passe chiffrés, adaptés à un usage professionnel. Cette approche progressive permet d'installer durablement de bonnes pratiques tout en évitant de brusquer les utilisateurs.

5.2. Procédure d'arrivée et de départ : sécurisation des accès

La question de la gestion des départs a connu une nette amélioration. Auparavant, il arrivait que du matériel informatique reste stocké sans explication claire, ou que des comptes utilisateurs ne soient pas désactivés immédiatement après le départ d'un collaborateur.

Suite à mes préconisations, un formulaire de ticket spécifique a été mis en place sur GLPI pour centraliser les demandes liées aux départs. Ce formulaire comprend désormais plusieurs options essentielles, telles que la suppression ou la conservation de l'espace OneDrive, la mise en place d'une éventuelle délégation de boîte mail ou encore le transfert des courriers professionnels vers un autre responsable. Un nouveau modèle de fiche de remise du matériel a également été rédigé (voir annexe), permettant un suivi précis du matériel restitué.

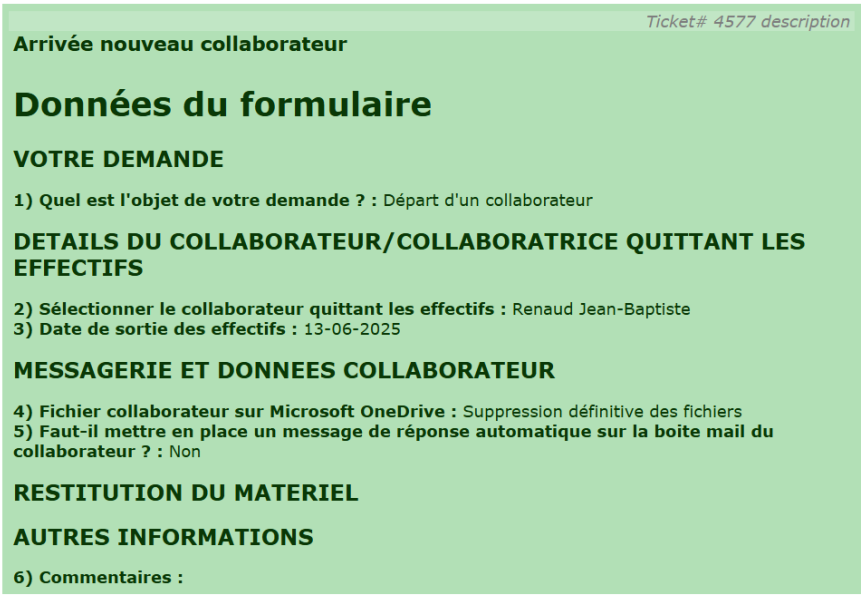


Figure 13 : Tickets GLPI pour le départ d'un collaborateur

Ces nouvelles procédures ont permis d'éviter les oublis, d'assurer un meilleur contrôle du parc matériel et d'améliorer la sécurité des accès.

5.3. Mise en place de l'authentification multifacteur (MFA)

La généralisation de l'authentification multifacteur a nécessité une organisation rigoureuse. Pour anticiper les blocages et rassurer les utilisateurs, une procédure complète a été rédigée et mise à disposition, avec captures d'écran et explications pas à pas (voir annexe). En cas de difficulté, les utilisateurs avaient également la possibilité de contacter le support par téléphone.

Le choix d'alternatives pour ceux qui refusaient l'installation sur téléphone personnel, notamment l'utilisation d'une extension navigateur, a contribué à lever certains freins. Grâce à ces actions, l'acceptation de la MFA s'est améliorée progressivement, même auprès des collaborateurs les plus réticents.

5.4. Transition vers Windows 11

Afin de préparer efficacement la transition vers Windows 11, j'ai mis en place un suivi précis de l'ensemble du parc informatique. Un fichier Excel, généré à partir d'un export de notre outil Malwarebytes (voir capture d'écran), regroupe toutes les informations essentielles sur chaque poste : nom du PC, type de processeur, compatibilité avec Windows 11, dernière connexion utilisateur, etc.

Cette démarche proactive permet de planifier la migration sans précipitation, d'éviter les mauvaises surprises et d'assurer une transition fluide dans les mois à venir.

5.5. Utilisation de BeyondTrust

L'outil BeyondTrust s'est révélé indispensable pour améliorer la prise en main à distance et accompagner efficacement les utilisateurs. Grâce à cet outil, il est possible de visualiser l'écran de l'utilisateur, transférer des fichiers, consulter les propriétés système ou encore prendre directement la main pour effectuer certaines manipulations (voir capture d'écran ci-dessous).

Cela a permis d'améliorer considérablement le temps de résolution des incidents, tout en offrant un accompagnement pédagogique et personnalisé à distance.

5.6. Bilan global

Dans l'ensemble, les résultats obtenus traduisent une amélioration significative de la sécurité informatique, une meilleure organisation des procédures internes, et une plus grande autonomie des utilisateurs dans la gestion de leurs outils numériques. Ces changements ont contribué à alléger la charge du support informatique tout en responsabilisant les collaborateurs. L'objectif de concilier efficacité, pédagogie et sécurité a été atteint, et ces bases solides permettront à l'entreprise de continuer à améliorer ses pratiques informatiques à l'avenir.

6. Conclusion technique : perspective du travail réalisé

Ce stage m'a permis de consolider et d'enrichir mes compétences techniques, tout en développant une approche plus globale de la gestion informatique en entreprise. J'ai acquis une bonne maîtrise des outils de support tels que GLPI, BeyondTrust pour la prise en main à distance, ainsi que les solutions Microsoft 365 pour la gestion des comptes et de la messagerie. Mais au-delà des aspects purement techniques, cette expérience m'a appris à vulgariser mes explications pour des utilisateurs peu sensibilisés à l'informatique, et à adapter ma communication en fonction de leurs profils.

Avec le recul, j'aurais pu améliorer certains aspects de mon comportement professionnel. Par exemple, j'ai parfois sollicité mon tuteur plus que nécessaire, par crainte de faire des erreurs. Cette prudence m'a permis d'éviter des maladresses, mais j'aurais pu gagner en autonomie en prenant davantage confiance en mes capacités. J'ai aussi appris à mieux gérer certaines situations conflictuelles, notamment avec des utilisateurs exagérant l'urgence de leurs problèmes. Avec l'expérience, j'ai compris l'importance de débriefer ces cas plus rapidement avec mon tuteur pour ajuster nos priorités et notre posture.

Enfin, ce stage m'a permis d'identifier plusieurs axes d'amélioration pour renforcer la sécurité et l'efficacité de l'entreprise :

- Renforcer la cybersécurité avec la mise en place d'un Plan de Reprise d'Activité (PRA) et la souscription à une assurance cyber.

- Optimiser la gestion des données en migrer l'ensemble de l'infrastructure locale vers un environnement cloud unifié, notamment OneDrive, pour mettre fin à l'hybridation actuelle (disques partagés + SharePoint).

- Améliorer la protection réseau par l'ajout de systèmes de détection et de prévention d'intrusion (IDS/IPS).

- Mettre en place des sauvegardes externes dédiées aux données critiques (backups indépendants du stockage courant).

Ces propositions s'inscrivent dans une logique de continuité et d'amélioration progressive, afin de sécuriser davantage les systèmes, simplifier le quotidien des utilisateurs et garantir la pérennité de l'activité en cas d'incident.

7. Conclusion: expérience professionnelle et relations humaines

Mon intégration au sein de l'entreprise a été un peu complexe au départ, principalement en raison de l'organisation interne. Le siège ne dispose pas de véritable salle de pause, seulement deux petites salles avec un lavabo, un frigo et un micro-ondes. Chacun ayant l'habitude de manger seul à son bureau, il était difficile de créer du lien avec les autres employés. Cela a eu un impact sur ma légitimité au début, car les collaborateurs ne me connaissaient pas vraiment et hésitaient parfois à me faire confiance, notamment lors des échanges par mail.

Pour remédier à cela, j'ai pris l'habitude de mettre mon tuteur en copie des échanges importants et j'ai configuré une signature professionnelle sur ma messagerie, ce qui a renforcé mon positionnement. Avec le temps, et surtout lorsque j'ai commencé à résoudre les problèmes des utilisateurs, les relations se sont améliorées naturellement. Mes interventions m'ont permis de rencontrer davantage de personnes et de développer de bonnes relations avec l'équipe.

Cette immersion dans le monde professionnel m'a permis de comprendre les réalités du travail en entreprise, avec la cohabitation de plusieurs services, des rôles variés, des personnalités

différentes, et surtout l'obligation de travailler ensemble malgré des objectifs parfois divergents. Travailler dans le milieu de la restauration et du club m'a également montré un environnement particulier : les interlocuteurs ne sont pas toujours disponibles en journée à cause des horaires décalés et des rendez-vous professionnels fréquents. De plus, il s'agissait souvent de personnes issues de milieux sociaux différents du mien, ce qui a enrichi mon expérience humaine.

Ce stage a renforcé mon choix de m'orienter vers les réseaux et la cybersécurité. Ce sont les domaines qui m'ont le plus intéressé durant cette période, que ce soit dans la pratique technique ou la réflexion stratégique sur les besoins de l'entreprise.

Enfin, j'ai compris que le métier de technicien support peut être parfois ingrat. En tant que premier interlocuteur face aux problèmes informatiques, il est courant de subir la frustration ou le stress des utilisateurs. J'ai appris à prendre du recul, à rester calme et à ne pas prendre ces réactions personnellement, même si cela a été difficile au début.

Cette expérience m'a donc apporté beaucoup sur le plan technique, mais également sur le plan humain, en me préparant aux exigences et aux réalités du monde professionnel.

8. Annexes obligatoires

8.1. Table de figures/illustrations

8.2. Bibliographie

BeyondTrust Corporation. (s.d.). Récupéré sur BeyondTrust Remote Support: https://www.beyondtrust.com/fr/remote-support

Outil professionnel de prise en main à distance sécurisé, utilisé par les équipes de support informatique. Permet d'assister les utilisateurs où qu'ils soient.

Dashlane Inc. (s.d.). Récupéré sur Dashlane Password Generator: https://www.dashlane.com/fr/features/password-generator

Générateur de mots de passe forts, intégré dans le gestionnaire Dashlane, pour renforcer la sécurité des comptes utilisateurs.

GLPI . (s.d.). *Gestion Libre de Parc Informatique*. Récupéré sur GLPI : https://glpi-project.org/fr/

GLPI est un logiciel libre de gestion de parc informatique et de helpdesk, utilisé pour gérer les équipements informatiques et suivre les tickets d'incidents.

Inc., H. (s.d.). *HP (Hewlett-Packard) – Support Drivers & Documentation*. Récupéré sur Support HP: https://support.hp.com/fr-fr

Portail officiel de support HP pour le téléchargement de pilotes, BIOS et documentation matériel pour ordinateurs et imprimantes HP.

Microsoft Corporation. (s.d.). *Comment utiliser l'application Contrôle d'intégrité du PC*. Récupéré sur Microsoft: https://support.microsoft.com/fr-fr/windows/comment-utiliser-l-application-contr%C3%B4le-d-int%C3%A9grit%C3%A9-du-pc-9c8abd9b-03ba-4e67-81ef-36f37caa7844

Documentation officielle Microsoft détaillant les prérequis matériels et logiciels pour la compatibilité avec Windows 11.

Microsoft Corporation. (s.d.). *Vue d'ensemble des services de domaine Active Directory*. Récupéré sur Microsoft Corporation: https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Service d'annuaire Microsoft permettant de centraliser l'authentification et la gestion des ressources réseau (utilisateurs, groupes, ordinateurs).

Optimabox. (s.d.). *Notices*. Récupéré sur Optimabox: https://optimabox.fr/fr/Docs/

Solution de contrôle d'accès physique (badges) utilisée pour la gestion sécurisée des entrées et sorties dans les bâtiments.

8.3. Lexique

Active Directory (AD) : Service Microsoft permettant de gérer les utilisateurs, ordinateurs et ressources réseau dans une entreprise.

Backup (sauvegarde) : Copie des données informatiques pour éviter leur perte en cas de problème.

GLPI : Logiciel libre utilisé pour la gestion des tickets d'incidents et des ressources informatiques.

IDS/IPS : Systèmes de détection (IDS) et prévention (IPS) des intrusions dans un réseau informatique.

Infrastructure hybride : Architecture informatique combinant des services sur site (local) et dans le cloud.

OneDrive : Service de stockage en ligne proposé par Microsoft, utilisé pour centraliser les fichiers d'entreprise.

PRA (Plan de Reprise d'Activité) : Plan permettant de rétablir rapidement les services informatiques après un incident majeur.

Support informatique : Assistance apportée aux utilisateurs pour résoudre leurs problèmes

Ticket : Demande ou signalement d'un problème technique enregistré dans un logiciel de gestion (ex : GLPI).

Utilisateur : Personne utilisant un service informatique ou un équipement dans l'entreprise.

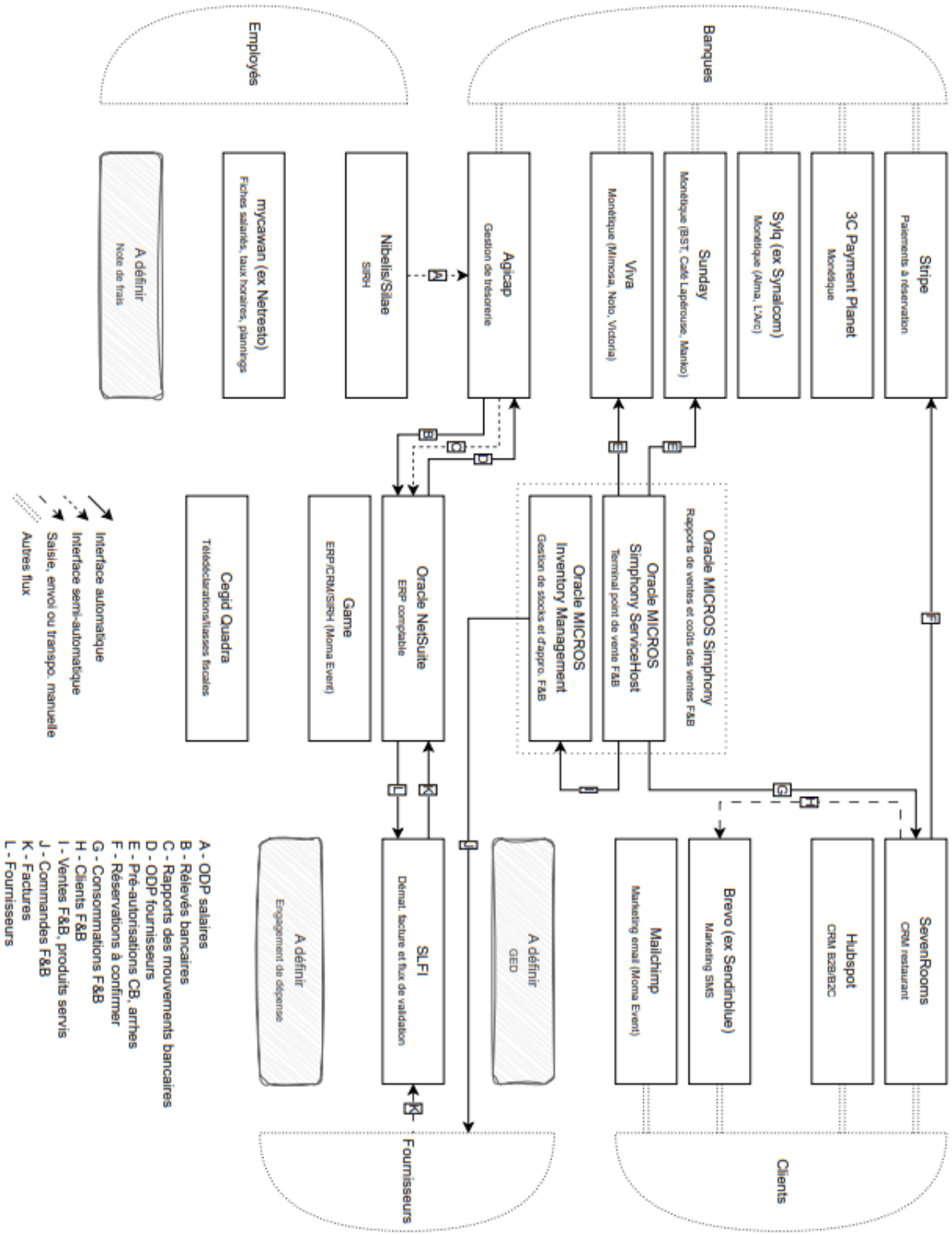
VPN : Réseau privé virtuel permettant une connexion sécurisée à distance au réseau de l'entreprise.

SharePoint : Plateforme collaborative de Microsoft permettant le partage et la gestion de documents.

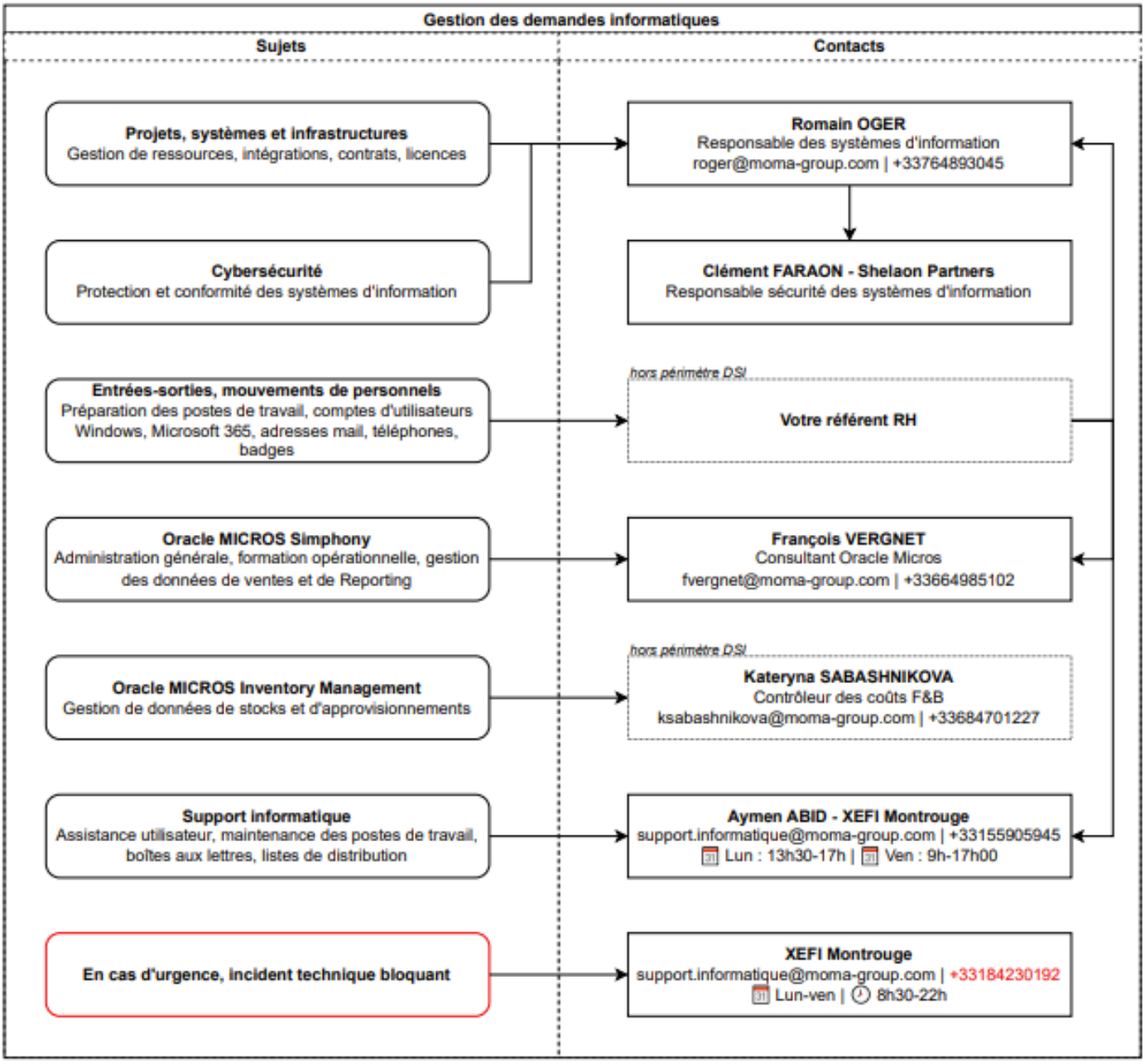
8.4. Index

8.5. Annexes supplémentaires

8.5.1. Cartographie du SI


Moma Group | Cartographie SI 2025
Employés
Banques
Clients
Fournisseurs
Stripe
Paiements à réservation
3C Payment Planet
Monétique
Sylq (ex Synalcom)
Monétique (Alma, L'Arc)
Sunday
Monétique (BST, Café Lapérouse, Manko)
Viva
Monétique (Mimosa, Noto, Victoria)
Agicap
Gestion de trésorerie
Nibelis/Silae
SIRH
mycawan (ex Netresto)
Fiches salariés, taux horaires, plannings
A définir
Note de frais
Oracle MICROS Simphony
Rapports de ventes et coûts des ventes F&B
Oracle MICROS Simphony ServiceHost
Terminal point de vente F&B
Oracle MICROS Inventory Management
Gestion de stocks et d'appro. F&B
Oracle NetSuite
ERP comptable
Game
ERP/CRM/SIRH (Moma Event)
Cegid Quadra
Télédéclarations/liasses fiscales
SevenRooms
CRM restaurant
Hubspot
CRM B2B/B2C
Brevo (ex Sendinblue)
Marketing SMS
Mailchimp
Marketing email (Moma Event)
A définir
GED
SLFI
Dématt. facture et flux de validation
A définir
Engagement de dépense
Interface automatique
Interface semi-automatique
Saisie, envoi ou transpo. manuelle
Autres flux
A - ODP salaires
B - Relevés bancaires
C - Rapports des mouvements bancaires
D - ODP fournisseurs
E - Pré-autorisations CB, arrhes
F - Réservations à confirmer
G - Consommations F&B
H - Clients F&B
I - Ventes F&B, produits servis
J - Commandes F&B
K - Factures
L - Fournisseurs

8.5.2. Organisation IT



8.5.3. Procédure « Mise en place de la MFA »

Mise en place de la MFA.docx

8.5.4. Organigramme complet de MOMA GROUP

MOMA Organigramme Avril 2025.pdf