GRAND ENOV+
AGENCE D'INNOVATION & DE PROSPECTION INTERNATIONALE

mewo
CAMPUS MÉTIERS

# Rapport d'alternance

## Titre RNCP34022 d'Administrateur des Systèmes d'Information en alternance

Rapport présenté au jury du campus MEWO à Metz dans le cadre d'une formation par apprentissage.

Présenté par : Mahmut-Selim AKALAN

Rapport confidentiel.

Tutrice : Aurélie VUILLAUME
GRAND ENOV+
DU 18 SEPTEMBRE 2023 AU 19 JUILLET 2024

## Message de Remerciement :

Je tiens à exprimer ma profonde gratitude envers toutes les personnes qui ont contribué à rendre mon expérience d'alternance aussi enrichissante et mémorable.

Tout d'abord, je souhaite remercier Madame Aurélie VUILLAUME pour son précieux encadrement, ses conseils avisés et sa confiance tout au long de cette période d'alternance. Ses compétences professionnelles et son dévouement m'ont permis d'acquérir une perspective approfondie du monde du travail et d'atteindre mes objectifs avec succès.

Je suis également reconnaissant envers toute l'équipe de GRAND E-NOV+ pour son accueil chaleureux, sa collaboration exemplaire et son soutien constant. Chaque membre de l'équipe a contribué à ma croissance professionnelle et personnelle, et je suis reconnaissant pour les précieuses leçons que j'ai apprises à leurs côtés.

Je tiens à exprimer ma gratitude envers Monsieur Julien ROVIRA et l'équipe pédagogique du CAMPUS MEWO pour leur suivi attentif et leurs conseils pertinents tout au long de mon parcours d'alternance. Leur expertise et leur soutien m'ont permis de mettre en pratique les connaissances théoriques acquises en classe et d'évoluer professionnellement.

Enfin, je remercie ma famille et mes amis pour leur soutien indéfectible et leur encouragement constant tout au long de cette aventure. Leur soutien moral a été une source d'inspiration et de motivation tout au long de mon parcours.

Cette expérience d'alternance a été une étape décisive dans mon développement professionnel et personnel, et je suis reconnaissant envers chacune des personnes mentionnées ci-dessus pour avoir rendu cette expérience possible. Je reste profondément reconnaissant pour les leçons apprises et les souvenirs précieux que je garderai toujours.

Merci infiniment.

Cordialement,

Mahmut-Selim AKALAN.

mewo CAMPUS MÉTIERS

# VALIDATION ENTREPRISE

Je soussigné

VUILLAUME Aurélie

Tuteur du stagiaire

Selim AKALAN

Certifie avoir lu le rapport d'activité professionnelle du stagiaire cité ci-dessus, valide son contenu et autorise la diffusion de son rapport au Campus MEWO de Metz.

Si certaines pages contiennent des contenus confidentiels à ne pas diffuser à d'autres personnes que celles composant le jury, veuillez les indiquer ci-dessous

Le rapport complet doit rester confidentiel.

Date, signature du tuteur et cachet de l'entreprise

13/06/2024

mewo - 7, rue Édouard Belin - 57070 METZ - Mettis ligne B - Grahamm Bell
tél. : 03 87 78 08 08 - fax : 03 87 78 69 69 - contact@mewo.fr - www.mewo.fr
NDA 44570372857 - UAI 0573778X - RCS 820 472 918 00011
APE 8542 Z - S.A.S. au capital de 20 000 €

# Table des matières

## Introduction :

Lors de mon expérience en alternance au sein de l'entreprise GRAND E-NOV+ où j'ai effectué deux années d'alternance, ma deuxième année de BTS et ma licence d'Administrateur des Systèmes d'Information, j'ai eu l'opportunité de travailler au sein du service informatique, où j'étais en charge avec diverses responsabilités cruciales dans la gestion et le support des infrastructures informatiques de l'entreprise. J'ai eu la chance de plonger en profondeur dans les défis et les besoins réels de la gestion des systèmes informatiques dans une entreprise multi-sites en évolution rapide.

Mes principales tâches consistaient à gérer les tickets à différents niveaux, de la résolution de problèmes internes à la coordination de l'aide des prestataires de services. Je suis intervenu pour réparer le système et le réseau afin que tout continue de fonctionner correctement et que tout problème puisse être résolu rapidement.

J'avais également la responsabilité de mettre en place le matériel informatique des nouveaux collaborateurs, comme créer leurs comptes et leur procurer leurs postes de travail. Notre travail était de veiller à ce que tout se passe bien lorsque de nouvelles personnes rejoignaient l'entreprise, depuis l'organisation de leurs affaires jusqu'à leur installation.

Ce qui est différent dans mon métier, c'est que je dois beaucoup voyager, notamment dans la région Grand-Est où notre entreprise dispose de huit lieux de travail différents. Cette mobilité m'a permis de développer des compétences organisationnelles et de communication essentielle, tout en me permettant de mieux comprendre les besoins spécifiques de chaque site et de chaque équipe.

Dans ce rapport, je vais détailler mes différentes responsabilités et les défis rencontrés lors de mon travail au sein du service informatique. Je vais également mettre en évidence les compétences que j'ai développées et les leçons que j'ai apprises tout au long de cette expérience d'alternance enrichissante.

Je suis convaincu que cette expérience m'a fourni des bases solides pour mon développement professionnel futur dans le domaine de l'informatique, tout en renforçant ma capacité à m'adapter à un environnement de travail diversifié et en constante évolution.

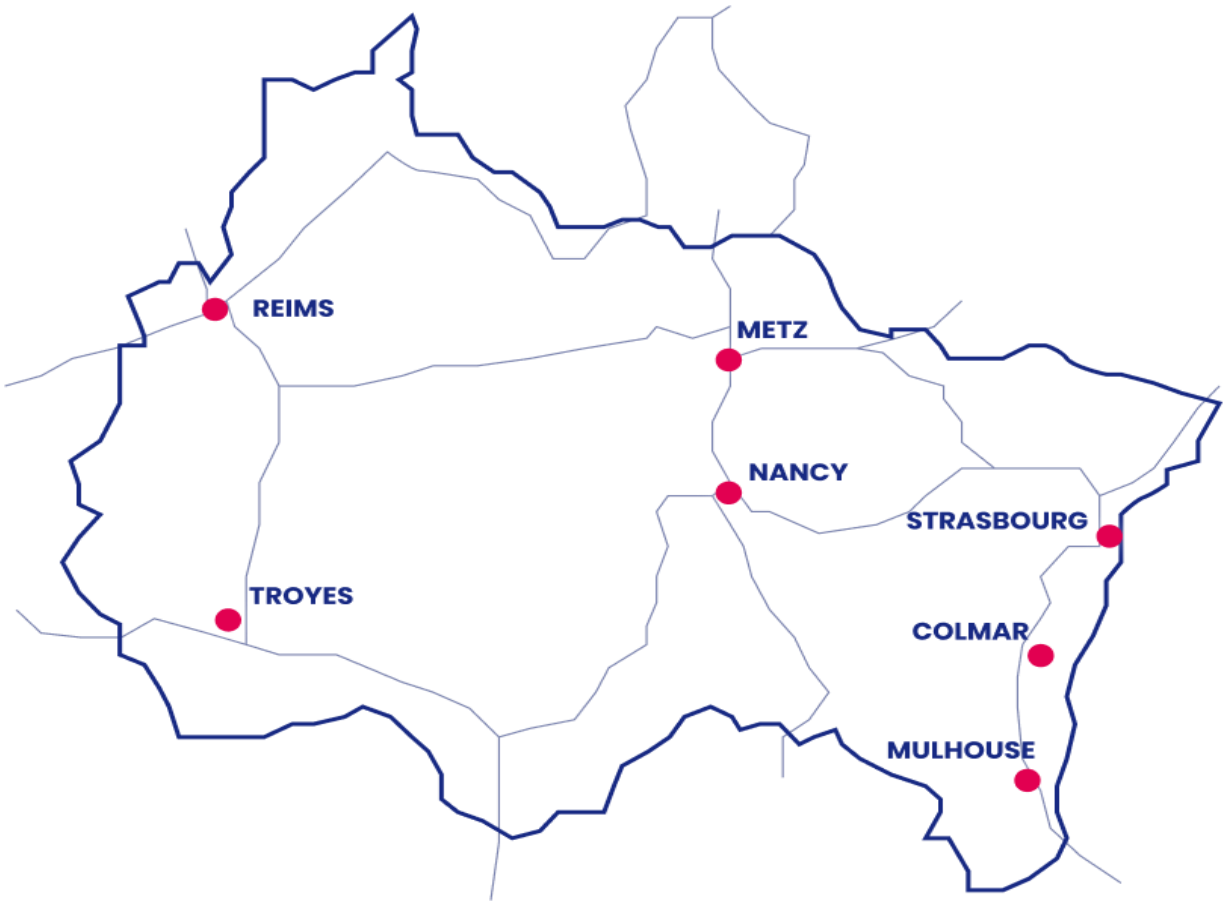
## Présentation de l'entreprise :

Présentation générale :

Grand E-NOV+ est une agence d'innovation et de prospection internationale de la région Grand Est, qui a été fondée en 2018 sous l'impulsion et avec le soutien de la Région Grand Est et de la Chambre de Commerce et d'Industrie du Grand Est. L'agence contribue au développement et au rayonnement du Grand Est en France comme à l'international en guidant les entreprises et les territoires dans leurs projets de transformation et d'innovation ainsi que d'implantation d'entreprises.

Grand-Enov+ est présente sur sept sites dans le Grand Est, incluant Troyes, Reims, Nancy, Metz, Strasbourg, Colmar et Mulhouse.

Chez Grand E-NOV+, nos équipes compte plus de 80 employés et met à profit son expertise dans divers domaines, tels que le conseil en stratégie digitale, le développement logiciel et applications, l'intelligence artificielle et l'analyse de données, le design et l'expérience utilisateur, ainsi que la cybersécurité et la protection des données.




*Plan de l'Agence Grand E-nov+*

## Historique de Grand Enov+ :

- **2018 : Fondation de Grand Enov+**
  Grand E-NOV+ est fondée en 2018 sous l'impulsion et avec le soutien de la Région Grand Est et de la Chambre de Commerce et d'Industrie du Grand Est. L'agence naît de la volonté commune de stimuler l'innovation et la croissance économique dans la région.

- **2019 : Lancement des Premiers Programmes**
  En 2019, Grand E-NOV+ lance ses premiers programmes d'accompagnement et de soutien aux entreprises du Grand Est dans leur transition vers l'économie numérique. L'agence organise également ses premiers événements et rencontres pour favoriser les échanges et la collaboration entre les acteurs de l'innovation.

- **2020 : Expansion et Diversification**
  En 2020, Grand E-NOV+ connaît une expansion rapide de son réseau, avec l'ouverture de nouveaux bureaux à travers le Grand Est. L'agence diversifie également ses domaines d'intervention, en proposant de nouveaux services de conseil et d'accompagnement aux entreprises dans les domaines de la transformation digitale, de l'innovation et de la prospection internationale.

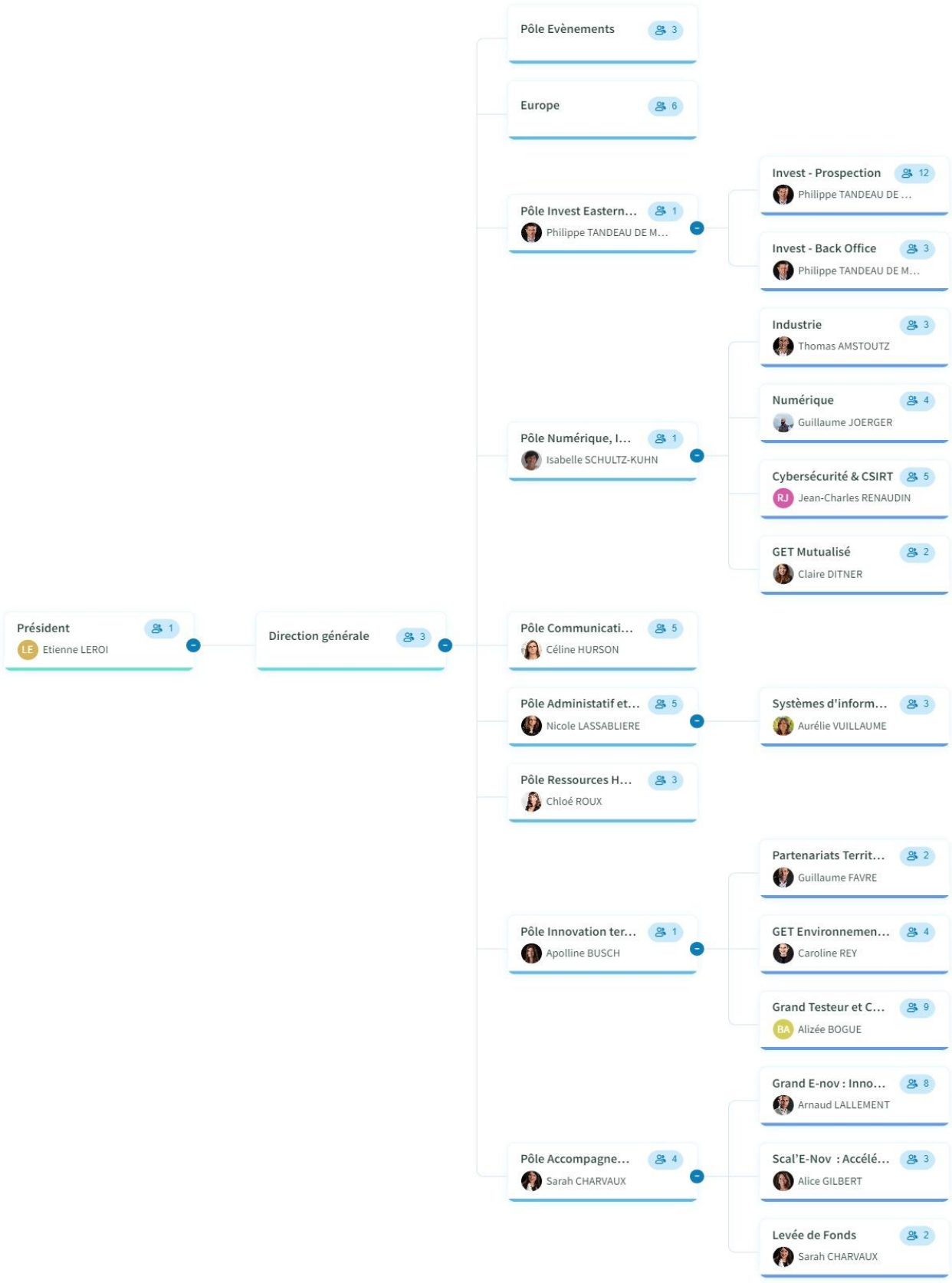
- **2021 : Renforcement de la Présence Internationale**
  En 2021, Grand E-NOV+ intensifie ses efforts pour renforcer sa présence et son rayonnement à l'international. L'agence établit des partenariats stratégiques avec des acteurs clés dans différents pays, afin d'accompagner les entreprises du Grand Est dans leur développement à l'étranger.

- **2022 : Consolidation des Réalisations**
  En 2022, Grand E-NOV+ consolide ses réalisations et ses succès passés, en mettant l'accent sur la qualité de ses services et la satisfaction de ses clients. L'agence poursuit son engagement envers l'innovation et l'excellence, et renforce ses liens avec l'écosystème de l'innovation dans le Grand Est et au-delà.

- **2023 : Nouvelles Initiatives et Projets**
  En 2023, Grand E-NOV+ lance de nouvelles initiatives et projets ambitieux pour soutenir l'innovation et la croissance économique dans la région. L'agence continue à jouer un rôle actif dans la promotion de l'entrepreneuriat et de l'innovation, en encourageant l'émergence de nouvelles entreprises et de nouveaux projets à fort potentiel.

- **2024 : Vision pour l'Avenir**
  En 2024, Grand E-NOV+ poursuit sa mission avec détermination et ambition. L'agence reste résolument tournée vers l'avenir, prête à relever les défis qui se présentent et à saisir les opportunités qui se dessinent. Avec un engagement indéfectible envers l'innovation et l'excellence, Grand E-NOV+ s'affirme comme un partenaire de confiance pour les entreprises du Grand Est et au-delà.

## Organigramme :




*Organigramme GEN+ 1*

## Principale mission de l'Agence :

- Guider les entreprises et les territoires dans leurs projets de transformation et d'innovation
- Contribuer à l'attractivité de la région Grand Est en France comme à l'international
- Sous l'impulsion et avec le soutien de la Région Grand Est et de la CCI Grand Est, Grand E-NOV+ déploie de nombreuses actions pour le territoire. Accompagnée de son réseau de partenaires, Grand E-NOV+ **contribue au développement et au rayonnement de la région Grand Est**.
- L'agence Grand E-NOV+ guide les entreprises du Grand Est dans la **recherche de partenaires internationaux** et l'**identification de sources de financements** européens, en sa qualité de membre du réseau « Enterprise Europe Network ».
- Grand E-NOV+ contribue également à des actions concrètes avec les entreprises et les territoires, pour changer l'avenir dans le Grand Est
- Promouvoir la **commande publique** auprès des entreprises et favoriser l'évolution des pratiques des acheteurs,
- Renforcer le niveau de **cyber-résilience** des entreprises et du territoire,
- Contribuer à l'**attractivité** de la région en attirant les investissements internationaux,
- Soutenir les **projets structurants** des territoires et la **structuration de filières**,
- Animer une dynamique autour des **zones d'activité du futur**,
- Soutenir le déploiement des **projets structurants des collectivités territoriales**.
- Grand E-NOV+ mène de nombreuses actions pour animer l'écosystème d'innovation et les acteurs du Grand Est
- Événements : 360 Grand Est, Prix Grand Est Transformation, ...,
- Clubs de décideurs : entreprises innovantes et territoires.

## Les dispositifs opérés par Grand E-Nov+ pour structurer et renforcer les offreurs de solutions du Grand Est :


### GRAND E-NOV, l'expertise métier dédiée à l'innovation

- Aide les entreprises à intégrer les **meilleures pratiques en matière d'innovation**
- Accompagne la **structuration des filières régionales** en lien avec l'écosystème
- Guide les entreprises **vers la transformation numérique et l'industrie du futur**
- Identifie les **opportunités de financement publics et privés** de la recherche et de l'innovation

### INVEST EASTERN FRANCE, l'expertise métier dédiée à la prospection internationale

- Définit et met en œuvre la **stratégie** et **le plan d'action régional de prospection des Investissements Directs Etrangers**
- **Accompagne** les porteurs de projets **jusqu'à leur décision d'implantation** en Grand Est
- **Membre du réseau des partenaires INVEST** du Grand Est


## GRANDTESTEUR, programme d'expérimentations territoriales du Grand Est

- **Un catalogue** de solutions made in Grand Est à destination des territoires
- Une **communauté d'acteurs** pour favoriser l'entraide et la montée en compétence
- Un **réseau de territoires partenaires** pour expérimenter dans le Grand Est

## COMMANDE PUBLIQUE GRAND EST

- Déploie un **réseau d'appui aux entreprises** sur tout le territoire
- **Informe, forme et accompagne les entreprises**
- **Met en place des outils** à destination des entreprises et des acheteurs publics du Grand Est
- Contribue au **rayonnement international des entreprises du Grand Est** via les marchés publics


## L'ACCÉLÉRATEUR SCAL'E-NOV

- Propose **un parcours post-incubation**
- Met à disposition des **outils de financement dédiés**
- Crée des **synergies entre startups et grands groupes**
- Établit un **maillage fort** sur tout le territoire Grand Est

## GRAND EST TRANSFORMATION

- Fédère et soutient les offreurs de solutions innovantes du Grand Est dans les secteurs du **numérique, de l'industrie et de l'environnement**
- Dispose d'un réseau **dynamique**, composé d'experts et de partenaires,
- Contribue à la **transformation des entreprises du territoire**
- Fait rayonner et attire de **nouveaux offreurs de solutions et de talents**

## Le dispositif opéré par Grand E-Nov+ pour accompagner les entreprises du Grand Est dans la cybersécurité :

Grand Est Cybersécurité, centre régional d'assistance aux victimes d'attaques informatiques.

Service gratuit d'assistance aux PME, ETI (Entreprises de taille intermédiaire), collectivités, établissements publics et associations du territoire.

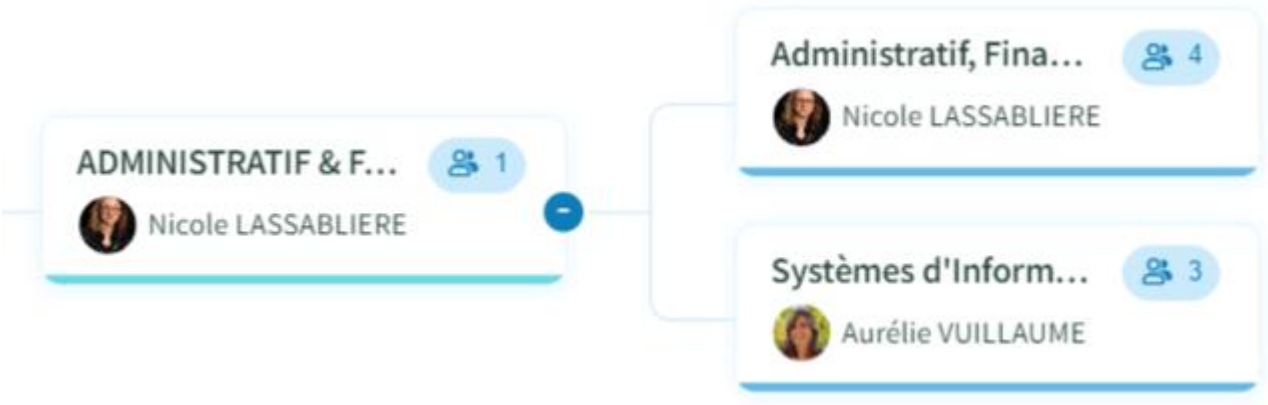
Le site internet du centre d'assistance dans la cybersécurité qui pourrait servir à toutes nos entreprises de la région : https://www.cybersecurite.grandest.fr .
Ce service a été créé dans le but d'accompagner les entreprises qui se retrouvent en difficulté lors d'une attaque informatique. De nos jours il y a énormément d'entreprises qui ne suivent pas correctement les procédures lorsqu'elles subissent une attaque sur leur réseau. Grand Est Cybersécurité autrement dit le CSIRT s'occupe d'accompagner du début à la fin les entreprises qui subissent des attaques et qui se font hacker. Ce service est totalement gratuit et financé par la région.

Lors d'une attaque informatique il faut commencer par avoir les bons réflexes comme : Alertez le service informatique, isolez les systèmes attaqués, constituez une équipe de gestion de crise, tenez un registre des évènements et actions réalisées et préservez les preuves. Ensuite piloter la crise comme : la mise en place des solutions de secours, la déclaration du sinistre auprès de notre assureur, déposez plainte, identifiez l'origine de l'attaque et son étendue, notifiez l'incident à la CNIL et gérez votre communication. Et dernièrement sortir de la crise comme : faire une remise en service progressive et contrôlée et tirez les enseignements de l'attaque.

Grand Est Cybersécurité vous accompagne correctement afin que vos déclarations, vos réflexes et votre crise soient gérés correctement. Sur leur site internet, vous pourrez retrouver ces trois différentes rubriques pour avoir toutes les informations concernant le CSIRT et les conseils qu'il vous donnent aussi en cas d'attaque informatique.

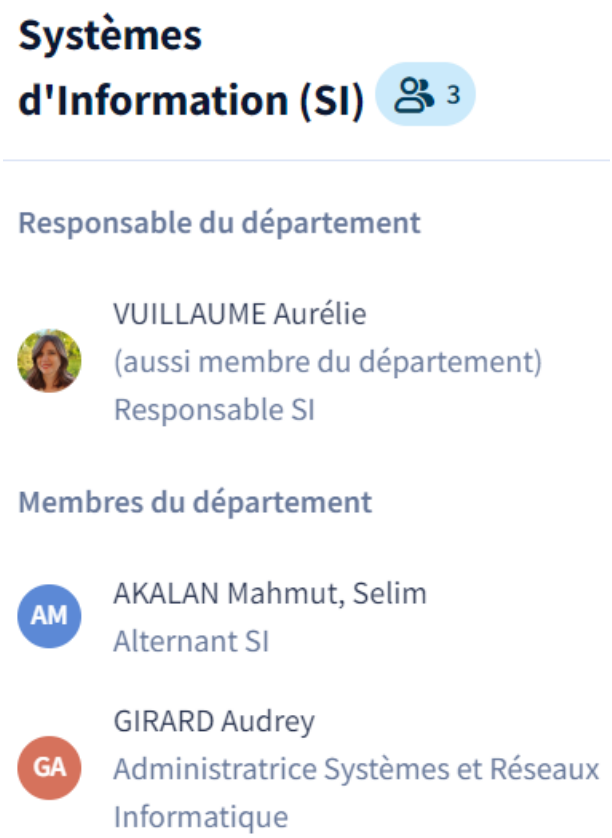
## Service Informatique de Grand Enov :

### A) Présentation du service informatique




*Pôle service informatique*

Le service SI fait partie du pôle Administratif & Finances, dirigé par Nicole LASSABLIERE. Le service SI composé de 3 collaborateurs est dirigé par Aurélie VUILLAUME.




*Service SI*

## B) Présentation de l'infrastructure

En 2018 l'infrastructure de chez Grand Enov+ a complétement changé. Tous les serveurs physiques sont passé en Cloud reposant principalement sur une infrastructure Microsoft. Grand Enov+ a décidé de révolutionner sont infrastructure avec le Cloud dans l'objectif de :

- Simplifier le managemennt
- Diminuer les coûts

J'ai donc travaillé dans un environnement en full Cloud, ce qui m'a permis de me familiariser avec M365, Azure AD et toutes les fonctionnalités tierces de Microsoft comme Microsoft Defender, Microsoft Purview (Sécurité et conformité), Microsoft Intune (Endpoint Manager), Microsoft Entra et Exchange.

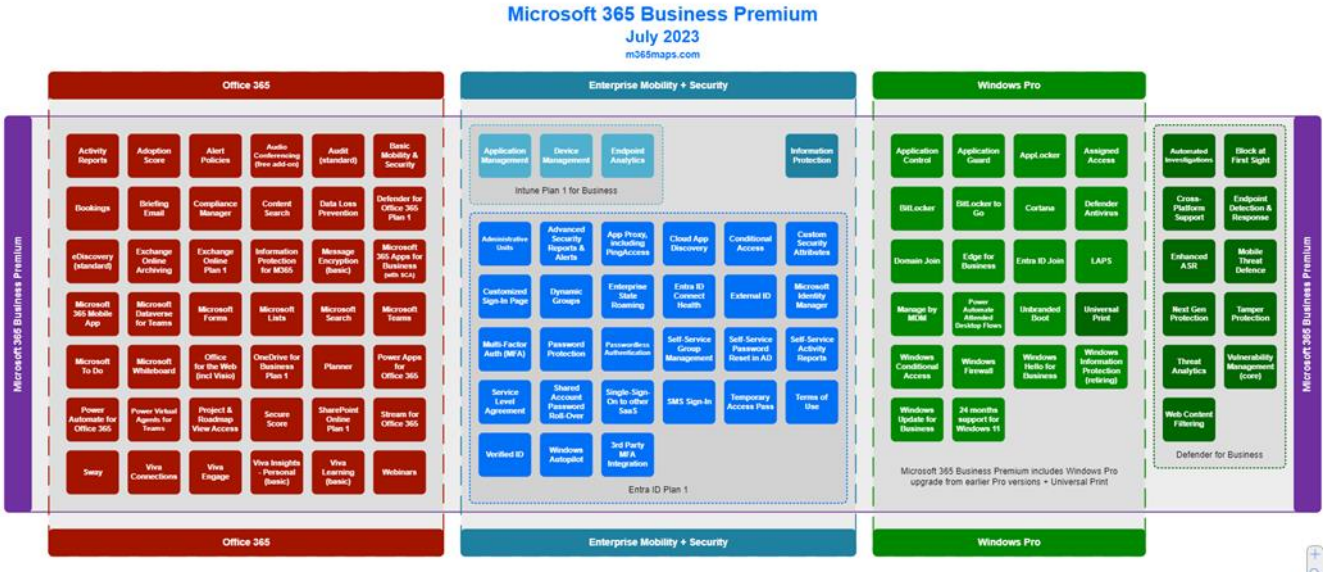



*Schéma M365 Business Premium*

- Microsoft Defender : On utilise Microsoft 365 Defender pour une visibilité sans égal des menaces sur notre réseau. Cela nous a permis de répondre aux incidents, recherchez proactivement des menaces, suivre nos ressources et déployez des stratégies pour sécuriser nos identités, appareils, espaces de travail Office 365, applications, etc.
- Microsoft Purview : On utilise le Portail de conformité Microsoft Purview pour atteindre nos objectifs en matière de conformité et de confidentialité. On trouve des solutions intégrées qui permettent de protéger nos informations sensibles, de gérer les cycles de vie des données, de réduire les risques internes, de protéger les données personnelles…
- Microsoft Intune : On utilise Micrsoft Intune pour une gestion unique de l'équipe gestion des accès qui permet de renforcer la sécurité des appareils et applications Microsoft 365 des employés, de les gérer et de les actualiser, …
- Microsoft Entra : On utilise le centre d'administration Microsoft Entra pour gérer les identités, les autorisations et l'accès réseau.

- Exchange : On gère les paramètres de courrier avancés tels que la mise en quarantaine, le chiffrement et les règles de flux de courrier, ...

L'environnement Office 365 interconnecte nos 7 sites grâce au Cloud en ligne. L'utilisation des outils permettent aux utilisateurs de collaborer à distance en toute simplicité avec de nombreuses fonctionnalités telles que :

- Travailler simultanément sur un fichier
- Créer, animer, gérer des réunions internes ou externes avec Teams
- Communiquer facilement par Teams
- ...

Le schéma qui résume parfaitement notre infrastructure se trouve ci-dessous. Notre réseau est hébergé entièrement en Cloud.

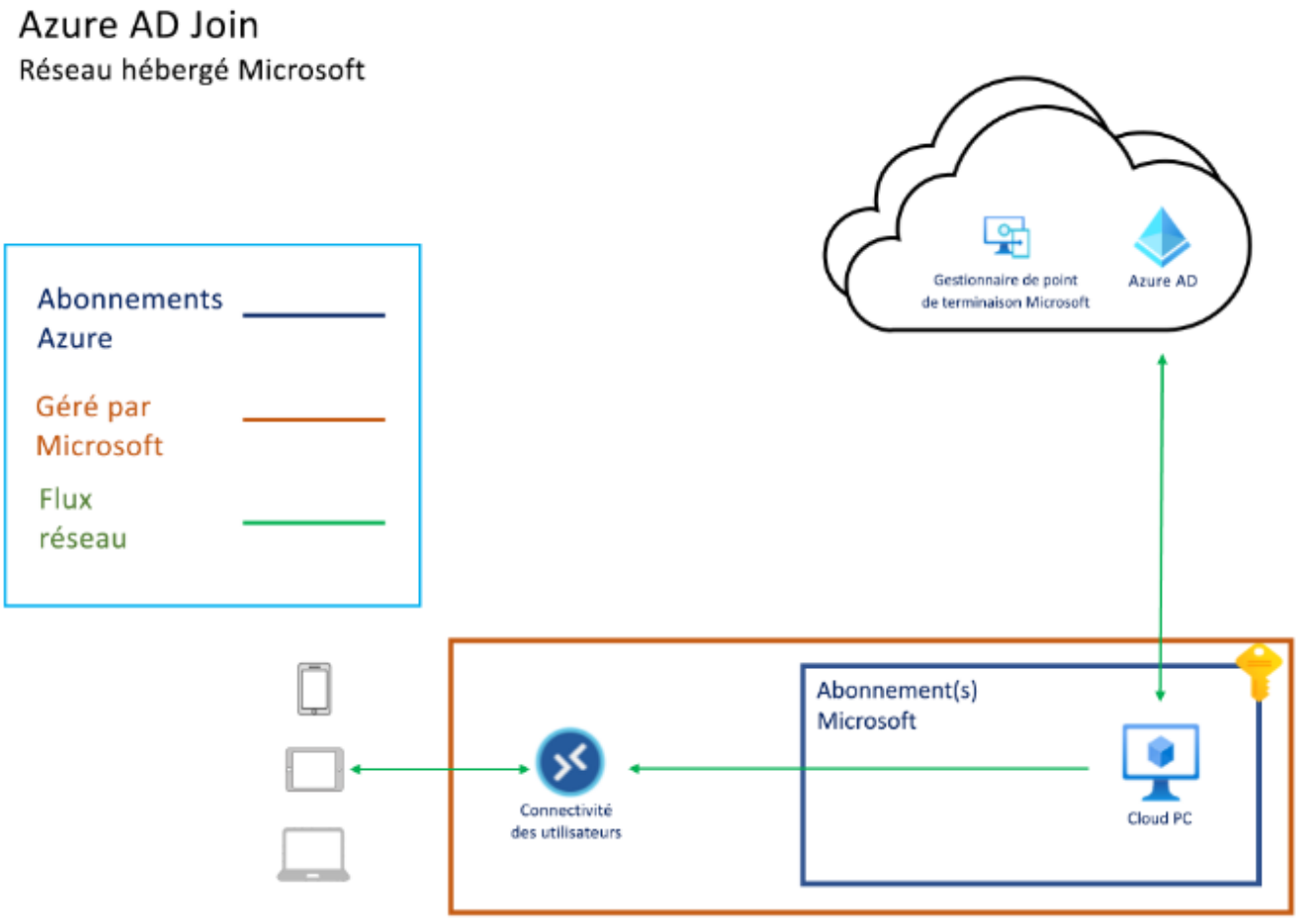



*Schéma de l'infrastructure de Grand E-NOV+*

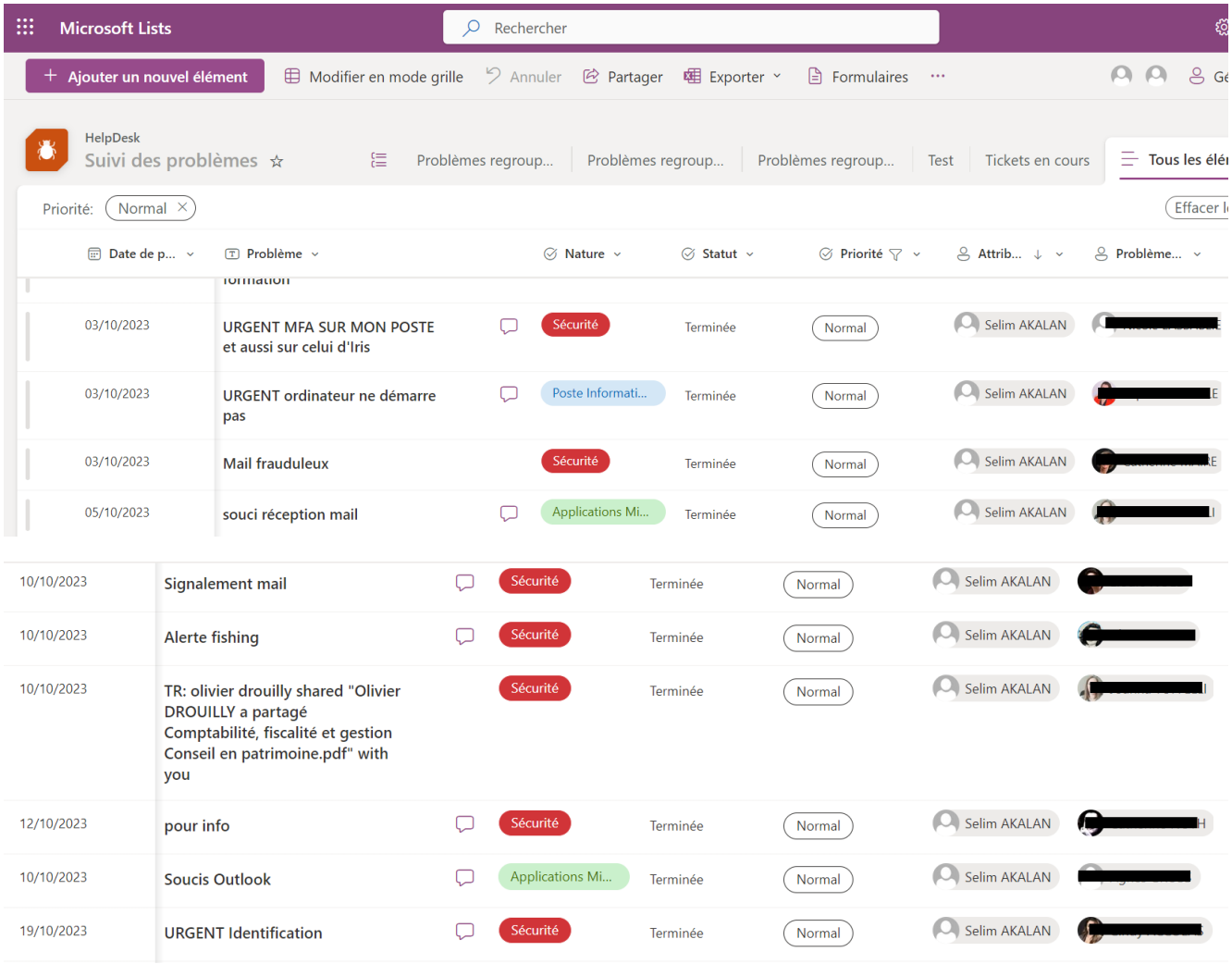
La plupart des sites de notre entreprise dispose de son propre réseau, comprenant routeur, pare-feu et switch dédiés. Les fournisseurs de services réseau varient d'un site à l'autre, de sorte que nous n'avons pas le même fournisseur pour tous les sites. Par exemple, sur le site de Metz, nous utilisons le réseau de notre propriétaire (voir annexe 1, 2, 3, 4).

## Les tâches effectuées en entreprise :

### A) Support aux utilisateurs

Pour la première tâche, je suis chargé du support aux utilisateurs avec l'appuie de ma responsable et de notre administratrice Système et Réseau. Je ne suis pas seulement responsable des tickets N1, mais je peux également gérer tous types de demandes. En cas de demandes de niveau trop élevé, nous faisions appel à un prestataire externe avec lequel nous avons un contrat de même pour les interventions sur les switchs et Firewall qui sont sous contrat. Ce prestataire prend en charge notre service SI lorsque le service SI interne est en vacances ou pour la commande et la mise en place de matériel informatique de type réseau.

Je suis souvent amené à effectuer différents déplacements sur nos sites situés dans le Grand Est. La plupart du temps, je suis accompagné, mais il m'est arrivé d'intervenir seul.




*Outil de ticketing : Microsft Lists*

### B) Accueil d'un nouveau collaborateur

Je suis chargé de préparer le matériel pour nos nouveaux collaborateurs, en 2 ans, l'effectif des collaborateurs a augmenté de 15 environ avec en moyenne 8 stagiaires/apprentis par an. Le responsable du nouveau collaborateur remonte via Microsoft Forms les informations et besoins relatifs au nouveau collaborateur. Ce formulaire contient : nom, prénom, date d'arrivé, matériel à livrer (pc, téléphone professionnel, chargeur, dock, écran…), le lieu de livraison les droits spécifiques à lui octroyer, le type d'abonnement téléphonique mobile, téléphone fixe, les logiciels métier à installer, service dans lequel la nouvelle personne va travailler, et les listes de diffusions dont lequel il doit faire partie.

Les informations nécessaires à la préparation du poste sont transmises par ma responsable via nos réunions internes de services. Une fois les informations en ma possession, je peux alors commencer à préparer le matériel.

Je commence par attribuer le matériel dans Salesforce, notre gestionnaire de parc informatique. En général, les écrans, docks, claviers sont attribués au numéro de bureau du site où la personne sera présente. Par exemple, si la personne travaille à Strasbourg, dans le bureau 5, le matériel est attribué à ce bureau, de sorte que lors de son départ, elle ne doit rendre que le PC, le téléphone professionnel le cas échéant, et la souris.

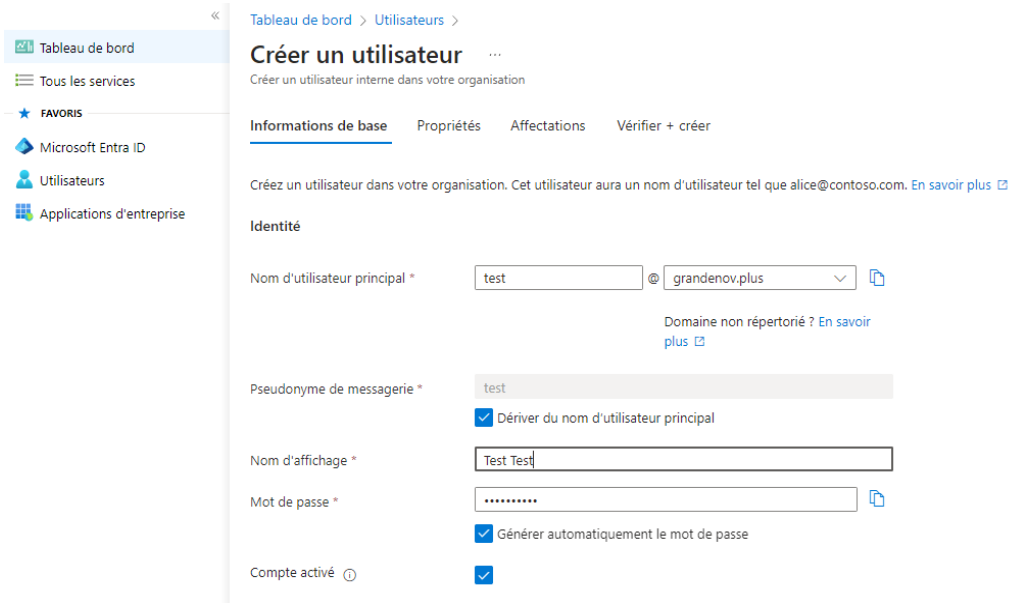
Une fois que son profil est créé et que le matériel est attribué sur Salesforce, je créé également son compte Microsoft avec toutes les informations nécessaires : lieu de travail, numéro professionnel attribué, licences demandées, et les différents groupes de travail auxquels elle devait appartenir, ainsi que les groupes de sécurité comme MFA et BitLocker. Ensuite, je commence à configurer le PC.

L'avantage de travailler dans un environnement Microsoft 365 est que, lors du démarrage du PC, il suffit de le connecter à un compte administrateur M365, et le PC se configure directement sur notre tenant. Une fois le PC configuré avec l'installation de différents logiciels tels que TeamViewer pour la prise en main à distance, Adobe Reader et Google Chrome.

Nous configurions ensuite le téléphone professionnel, l'intégrions dans le domaine et toutes les ressources de l'entreprise sont disponibles lors de l'installation du téléphone.

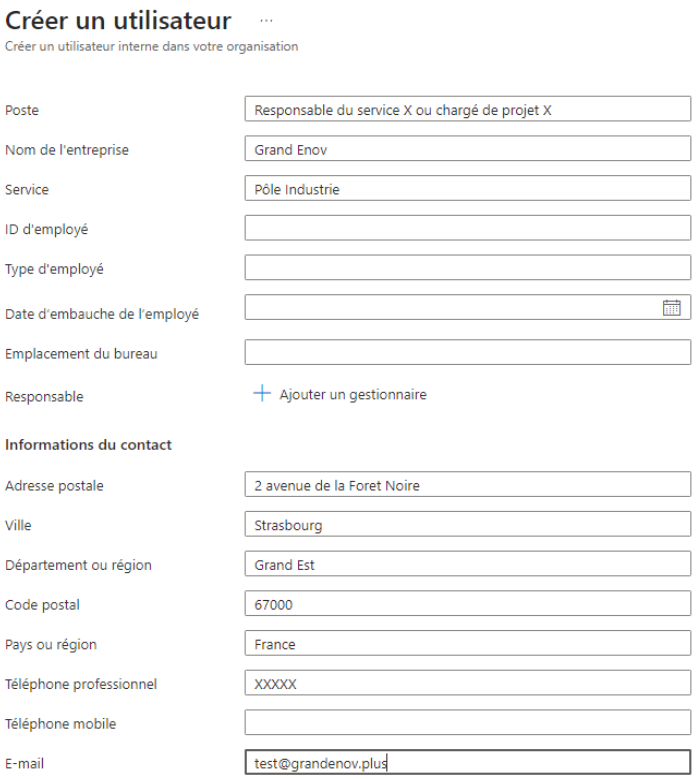
Pour la création d'un compte utilisateur :

- Je lance Microsoft Entra ID.
- Dans l'onglet Utilisateur à gauche, je sélectionne Nouvel utilisateur.
- Je créé l'adresse mail.



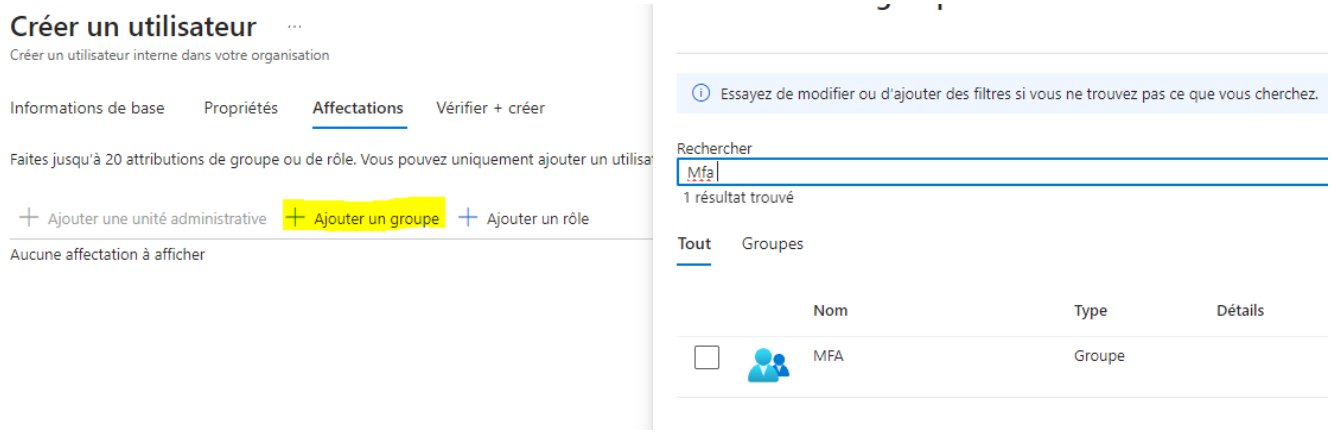

*Azure AD --> Microsoft Entra ID*

- Je renseigne les informations du nouveau collaborateur.




*Création d'un utilisateur*

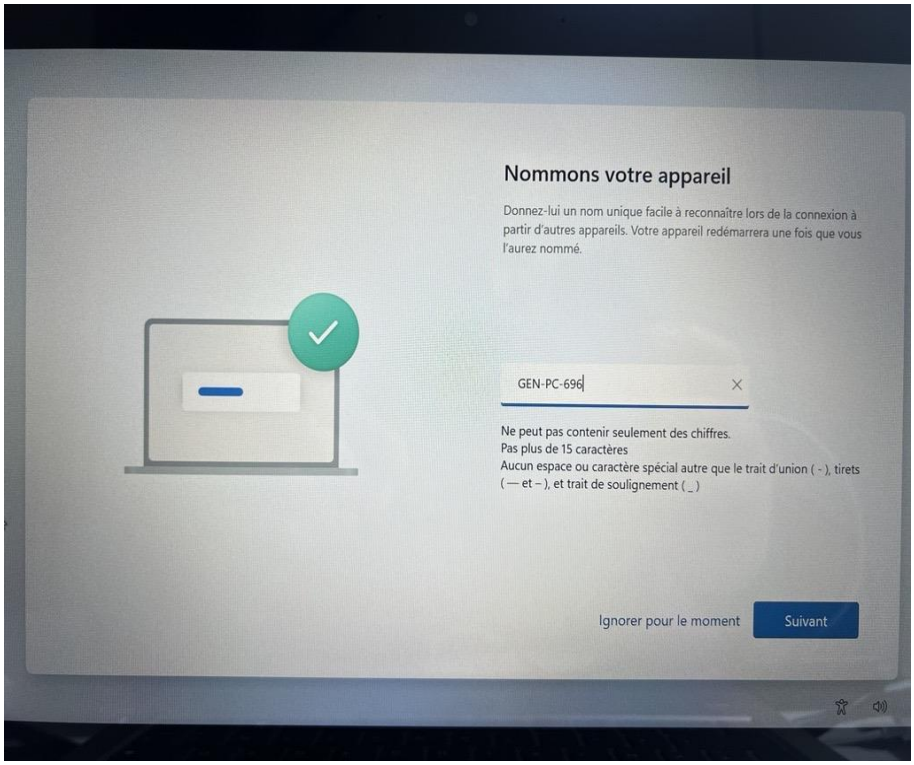
- Je l'ajoute aux différents groupes du pôle auquel il appartient, et dans notre service SI, je l'ajoute aux groupes de sécurité comme la double authentification et Bitlocker.




*Intégration d'un utilisateur dans un groupe de sécurité*

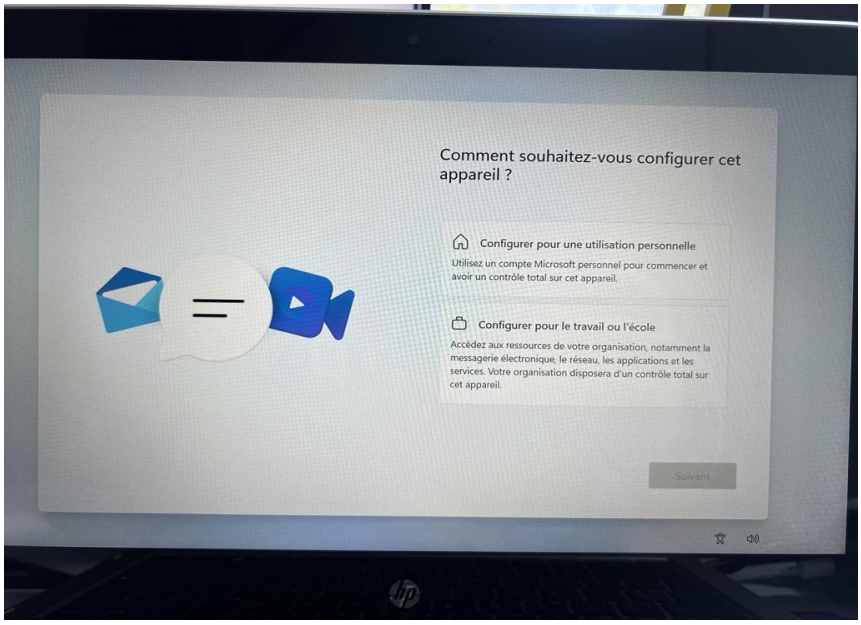
Pour la préparation du pc :

- Je commence par nommer le PC par GEN-PC-XXX (en utilisant le numéro du matériel attribué dans Salesforce, par exemple GEN-MAT-200).

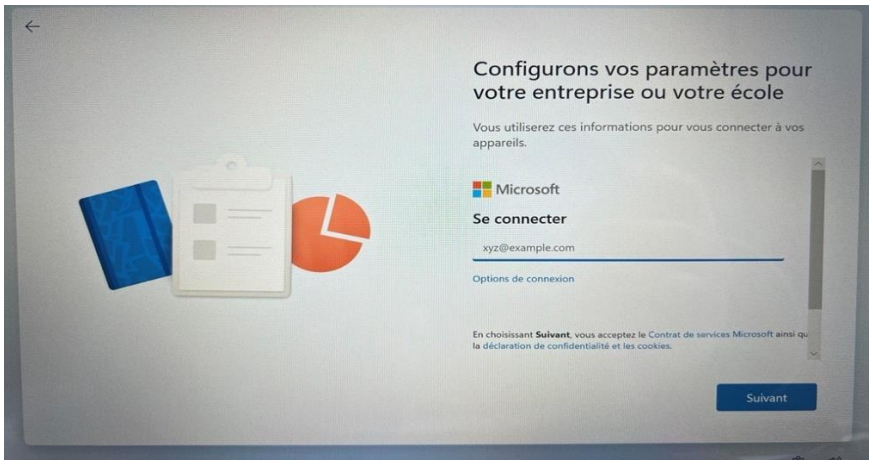



*Nomination d'un PC*

- J'entame ensuite la configuration de l'appareil pour le travail.
- Je connecte le compte du domaine Grand Enov.




*Configuration d'un nouveau PC*




*Connexion à un domaine avec un compte Microsoft*

- Je passe toutes les étapes de configuration.
- Je définis un code confidentiel.
- Le bureau Windows apparait.
- Je supprime les logiciels inutiles/ pré installé sur le poste (anti-virus, M365 ou office, OneNote). Ensuite, j'installe les logiciels comme TeamViewer, Adobe Reader et Google Chrome.
- J'installe la suite Office 365.
- Je me déconnecte ensuite du compte admin et je me connecte sur le compte du nouveau collaborateur.
- Une fois connecté, je mets en place son OneDrive et synchronise les dossiers de partage de l'agence. Selon les groupes auxquels il a accès, il pourra accéder aux ressources de l'entreprise dans le dossier partagé que j'ai synchronisé dans son OneDrive.
- Mise en place de la MFA avec le téléphone professionnel.

- J'établis ensuite la fiche de remise qui est à signer par le collaborateur ainsi qu'un livret d'accueil SI avec les informations de connexion et le fonctionnement du SI au sein de l'Agence.

### C) Chargé de l'intégration des téléphones dans le MDM (mobile device management)

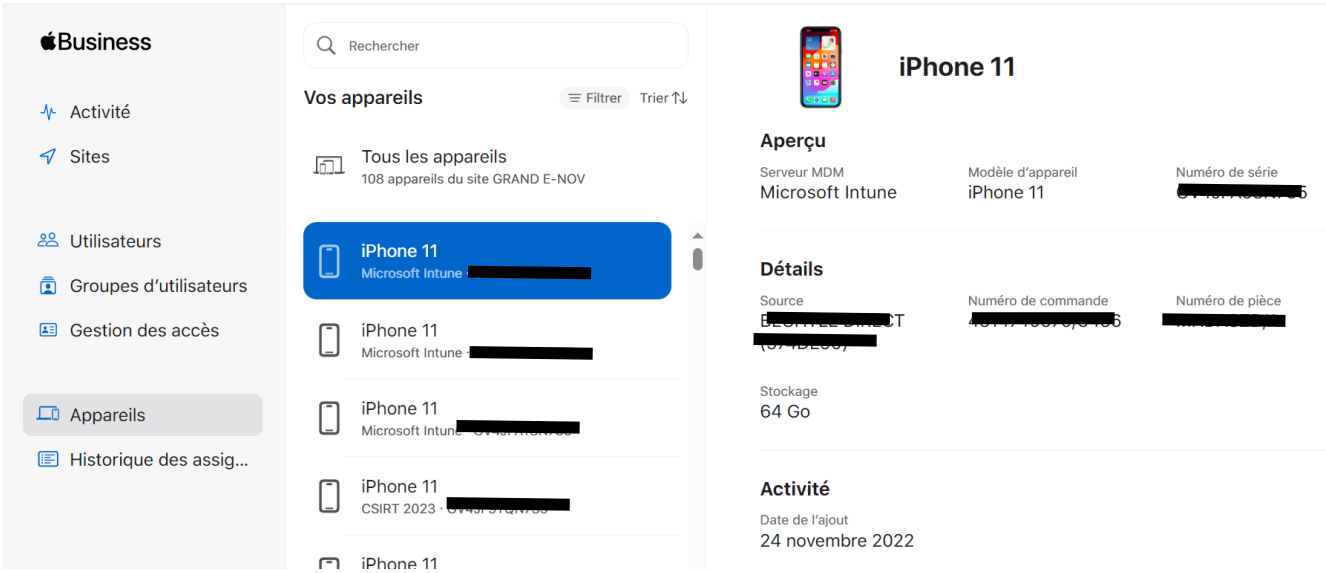
Lors de mon alternance, j'ai eu la chance d'avoir l'opportunité de faire partie du projet pour l'intégration des tous les téléphones professionnels fournit à nos collaborateurs, dans notre Tenant Microsoft.

Pourquoi ce projet ?

Lors de la mise en place de notre infrastructure, avant mon arrivée dans la société, les téléphones sous IPhone n'étaient pas enrôlés correctement, c'est-à-dire que les téléphones ne remontaient pas sur l'Entra ID. Donc j'ai eu pour mission, de prévoir des déplacements sur nos différents sites afin d'enrôler les téléphones sur le tenant afin d'y améliorer la sécurité de ceux-ci (configuration de Defender, mise en place d'un store d'applications approuvées par le SI, ...). Les nouveaux collaborateurs sont eux intégrés dès le départ sur le tenant M365.

Pour l'intégration des téléphones par Apple Business Manager (pour le service SI) :

- On se connecte sur ABM
- Dans Appareils, avec le numéro de série du téléphone, on recherche le numéro à intégrer dans le Tenant.
- On sélectionne le serveur MDM auquel on veut l'intégrer et on valide.

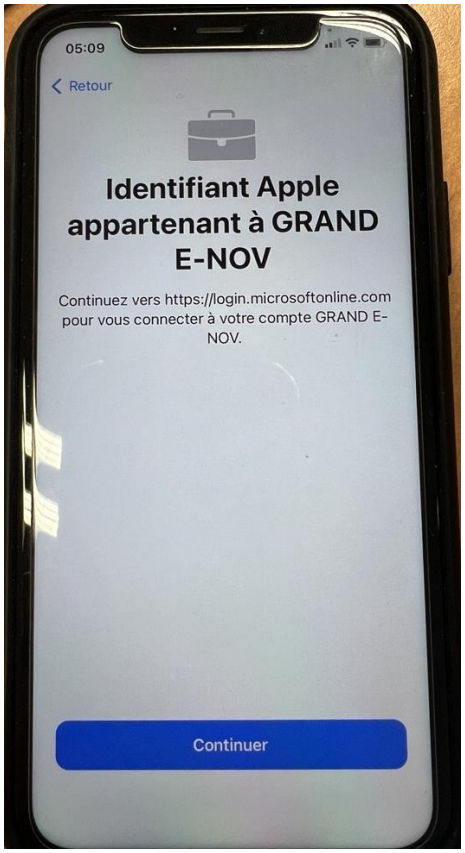


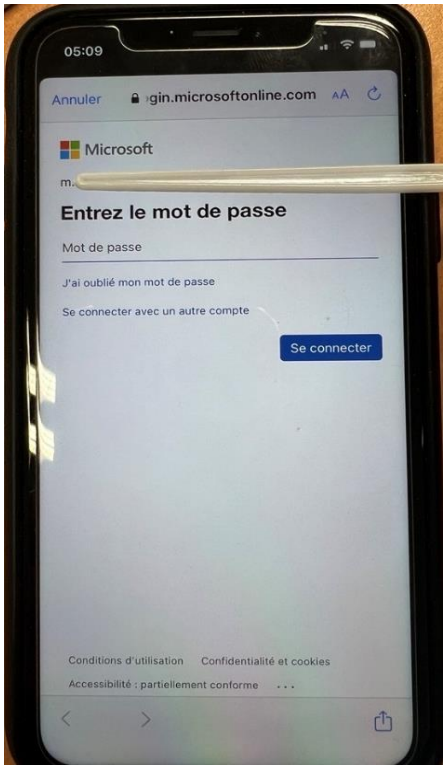

- Il faut attendre quelques minutes et ensuite allumer le nouveau téléphone.
- On passe toutes les étapes de configuration (langue, ...)
- On lui sélectionne un réseau Wifi afin qu'il n'y ait pas de coupure.

- Une fois sur la page « Apps et Données », on sélectionne « Ne pas transférer les apps et les données ».


- L'identifiant Apple correspond à l'identifiant Microsoft. Une fois qu'on connecte le compte Microsoft le téléphone va remonter dans le Tenant de notre domaine.

-Une fois correctement connecté, il faudra attendre quelques minutes. L'appareil passera par une étape de récupération des données (ressources de l'entreprise, applications, logiciels, etc.).




-Ensuite il demandera le mot de passe afin d'approuver la connexion au domaine.

-Une fois que toutes les applications sont remontées, il faudra configurer **: MSdefender** (image 1), le Portail **d'entreprise** (image2) **et Microsoft Authenticator**(image3).

1 2 3

Procédure pour l'intégration à Apple Business Manager d'un iPhone non intégré par le revendeur (pour le service SI) :

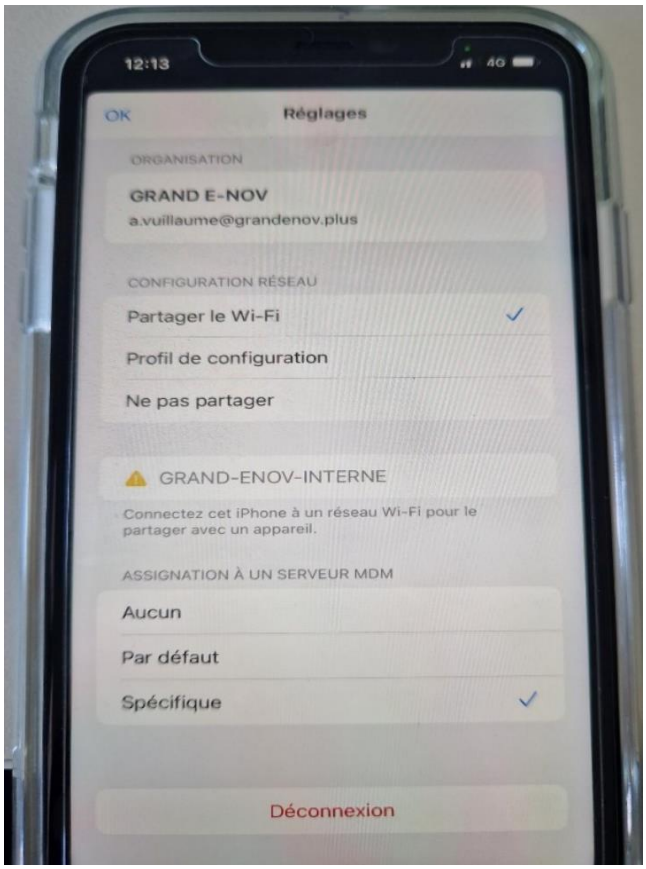
Prérequis

- Compte administrateur Apple avec le droit « Gestionnaire d'inscription d'appareil »
- Un iPhone avec Apple Configurator lié au compte administrateur + l'iPhone non enregistré
- Les DEUX téléphones doivent être sous IOS 17 minimum
- L'iPhone administrateur doit avoir une connexion Wi-Fi stable (donc on oublie le réseau wifi du bâtiment, privilégier un accès en partage de connexion)

Sur l'iPhone administrateur :

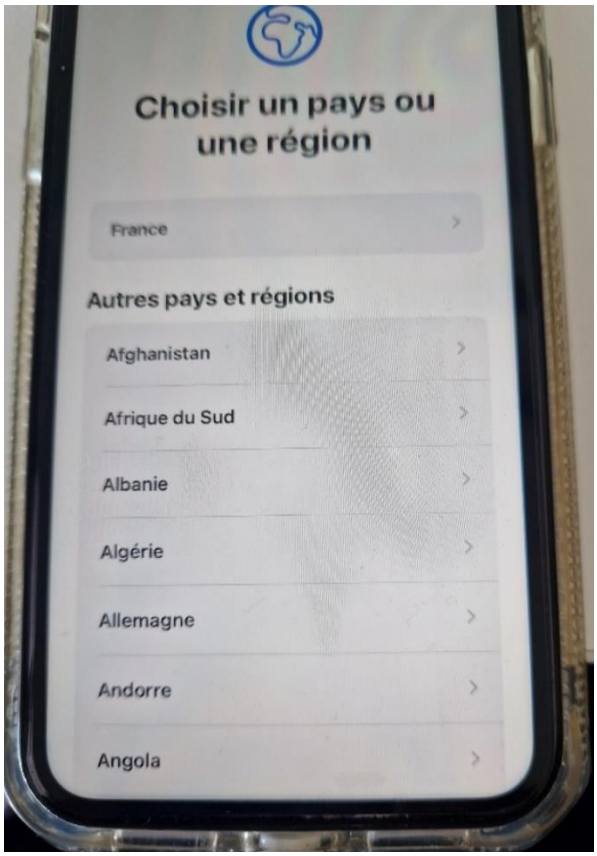
1. Ouvrir Apple Configurator
2. Dans les réglages (engrenage en bas à gauche) :

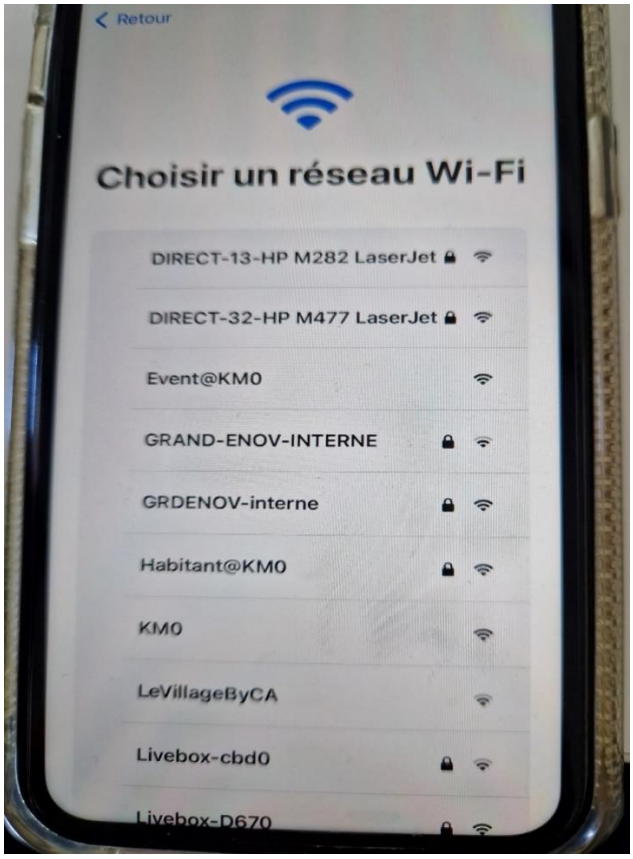
- On vérifie que l'organisation est bien « GRAND E-NOV »
- Pour la configuration Réseau, on choisit « Partager le Wi-Fi »
- Pour « Assignation à un serveur MDM », on choisit « Spécifique et sélectionner le serveur MDM souhaité »




Sur l'iPhone à intégrer :

- Continuer la configuration jusqu'à voir apparaître l'écran de sélection du réseau Wi-Fi
Attention : ignorer la page de démarrage rapide (sélectionner « Configurer sans un autre appareil »)



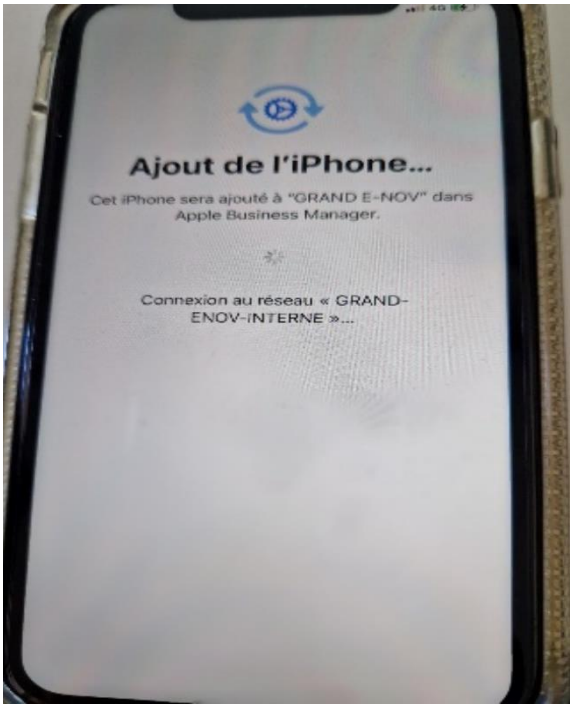




Lors de l'allumage de l'iPhone à intégrer, on va voir apparaître une notification « Nouvel iPhone » sur l'iPhone administrateur ignorez-là.

Sur l'iPhone administrateur :

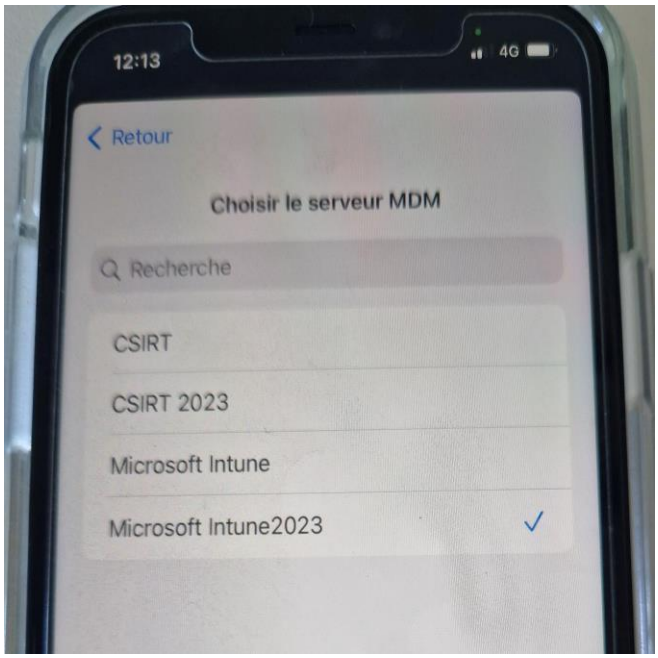
- Quitter le menu Réglages et approcher l'iPhone de celui à configurer.

- On choisit le motif apparu sur l'écran de l'iPhone à intégrer dans le cercle sur Apple Configurator ou procéder à un jumelage manuel.

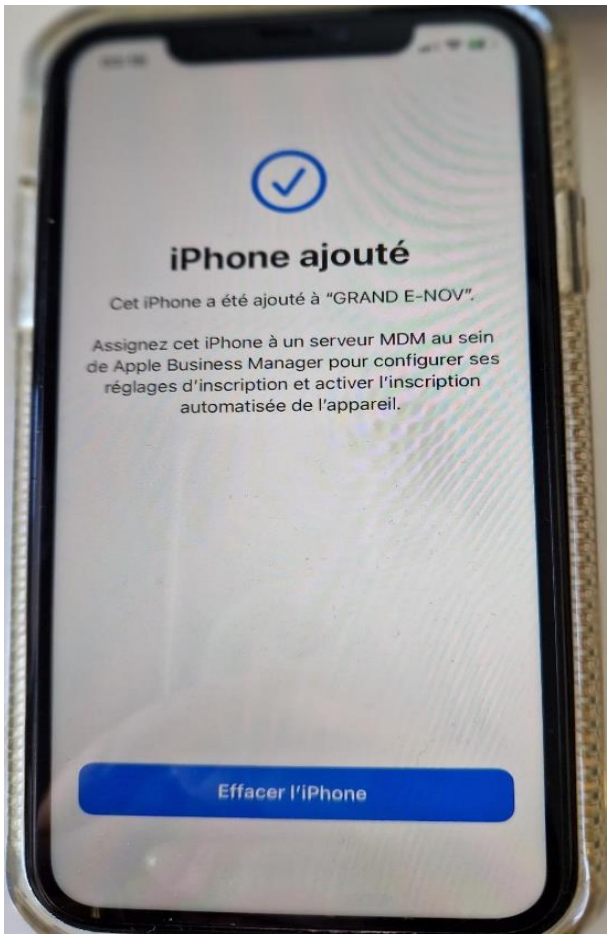




Sur l'iPhone à intégrer :

- L'iPhone est ajouté au domaine GRAND E-NOV et assigné au serveur MDM choisi précédemment.



- Sélectionne « Effacer l'iPhone »



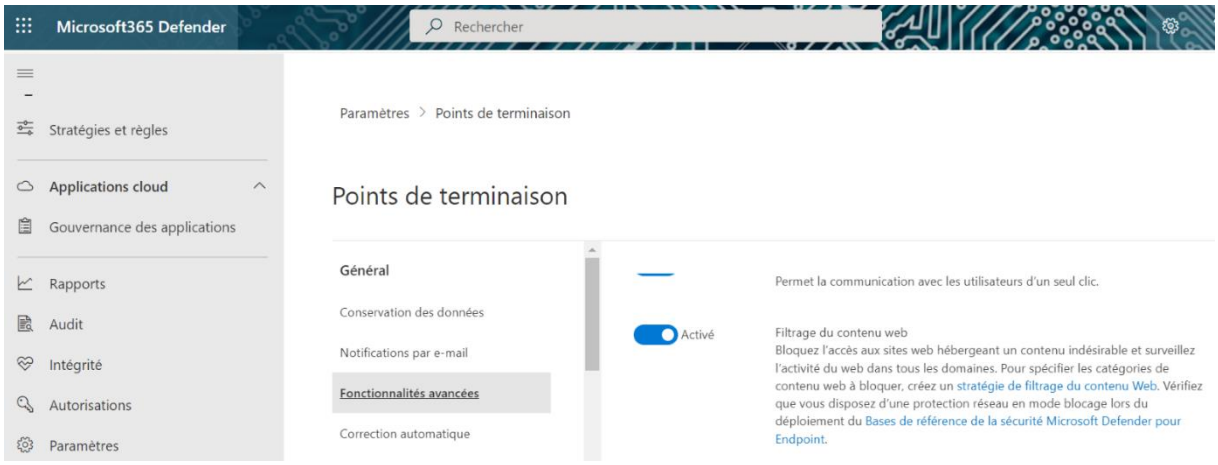

Vérifier que le téléphone soit bien remonté sur Intune, sinon force la synchronisation dans « Appareils » -> « iOS/iPadOS » -> « Inscription iOS/iPadOS » -> « Inscription du programme d'application » et sélectionne le bon jeton puis « synchroniser »

### D) Filtrage Web

Le service SI gère le filtrage de la navigation Web de nos utilisateurs avec Microsoft Defender.

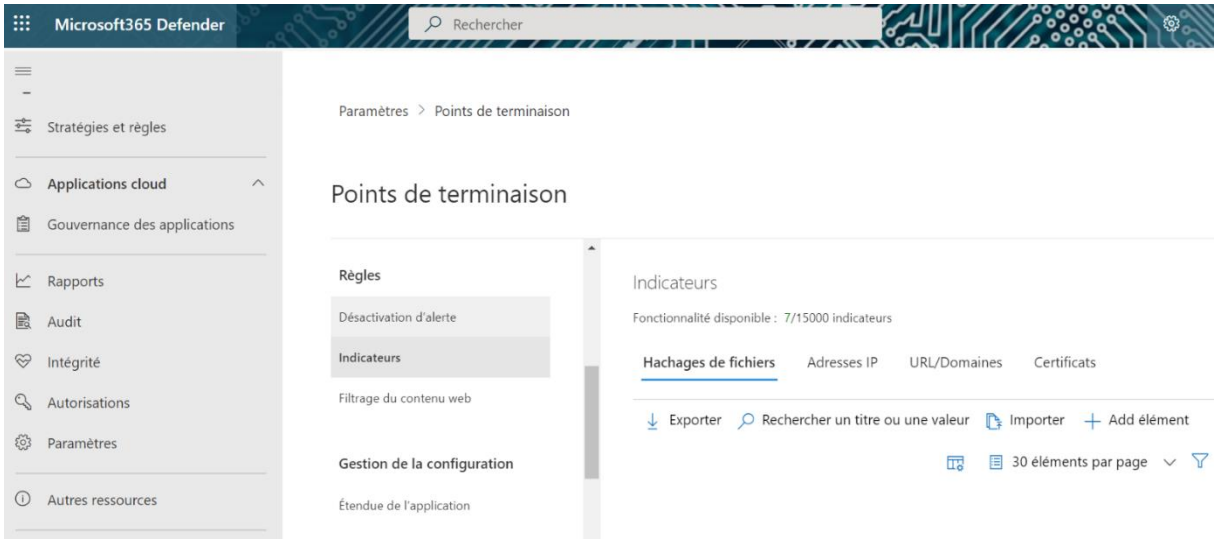
Préambule : L'EDR Microsoft Defender offre une solution complète de protection pour les utilisateurs et les Endpoint. Ce document a pour objectif de décrire la gestion du filtrage Web des postes et mobiles de l'Agence quelques soit le lieu de connexion. Connexion au panel Microsoft Defender : https://security.microsoft.com/

Le filtrage Web est une fonctionnalité avancée de Microsoft Defender, il faut veiller à ce qu'elle soit active dans Paramètres – Points de terminaisons – Fonctionnalités avancées :



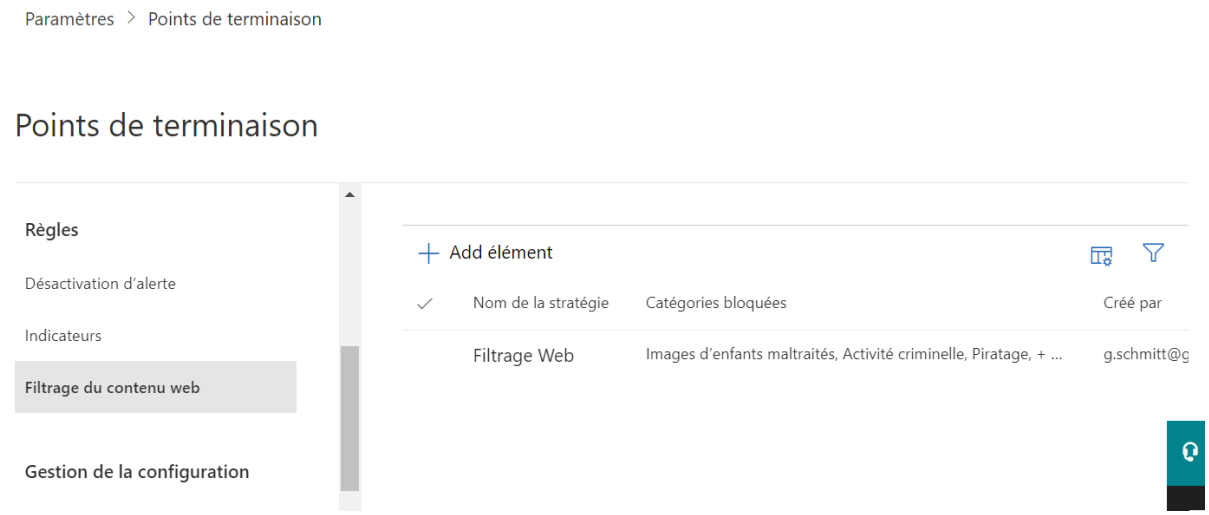

*Point de terminaison dans Defender.*

Une fois la fonctionnalité activée, pour gérer le filtrage, on se rend dans l'onglet Règles, Paramètres – Points de terminaisons – Règles.



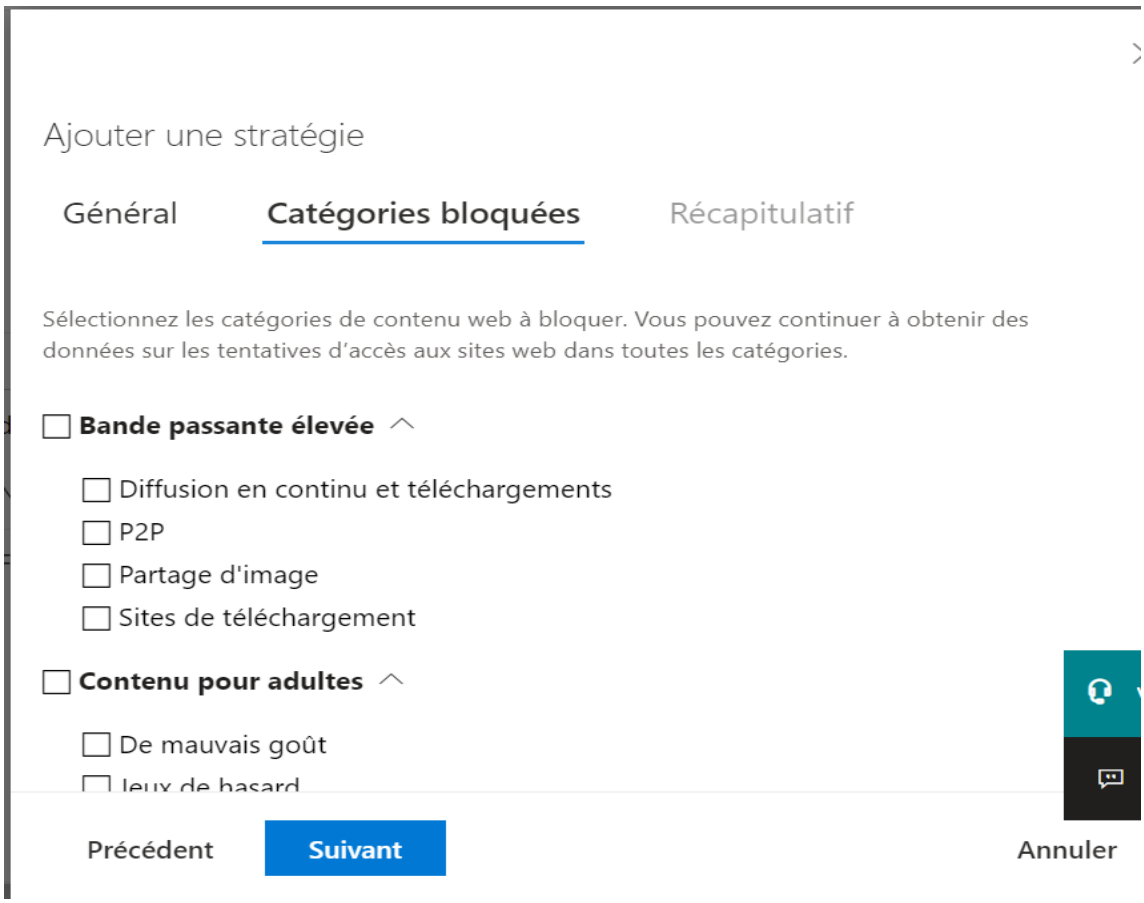

*Mettre une règle en place dans Defender*

Pour que ce dernier soit fonctionnel, il s'agira de mettre en place une stratégie de filtrage Web. Pour ce faire, il faut aller dans la partie Filtrage du contenu Web.




*Mettre une règle en place pour le filtrage web*

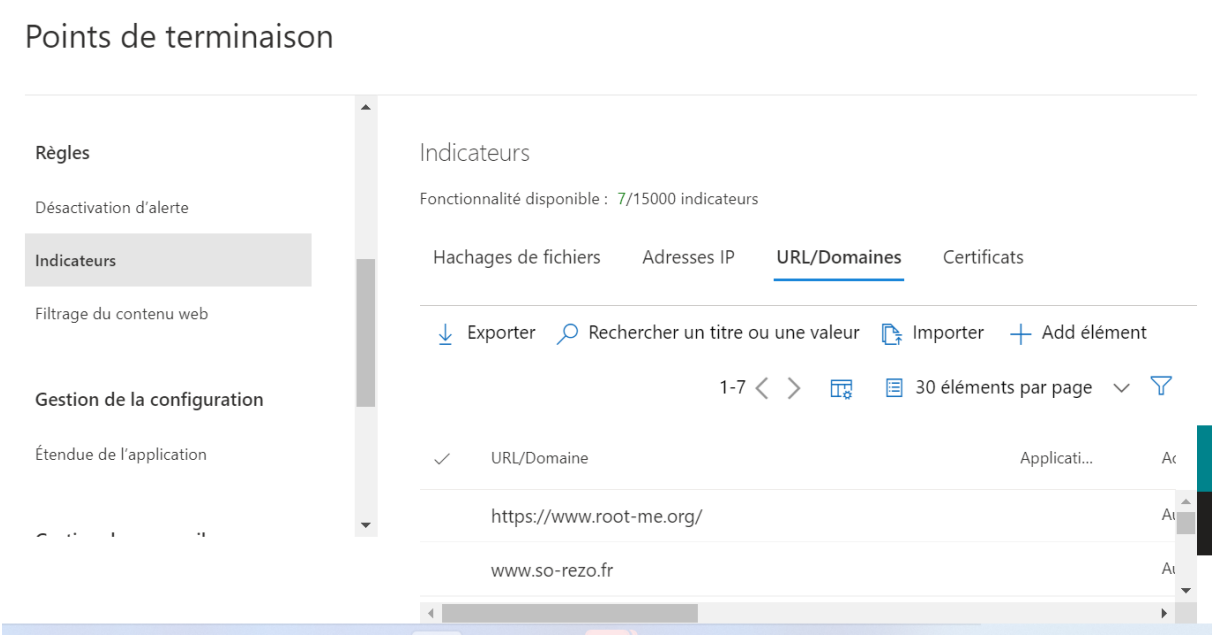
La fonction « *Add Element* » permet de créer une règle, il suffit de sélectionner les catégories de site à filtrer.




*Sélection d'une catégorie à filtrer*

Microsoft s'appuie sur une base de données interne constamment mise à jour. Il est bien sûr possible de bloquer des sites manuellement.

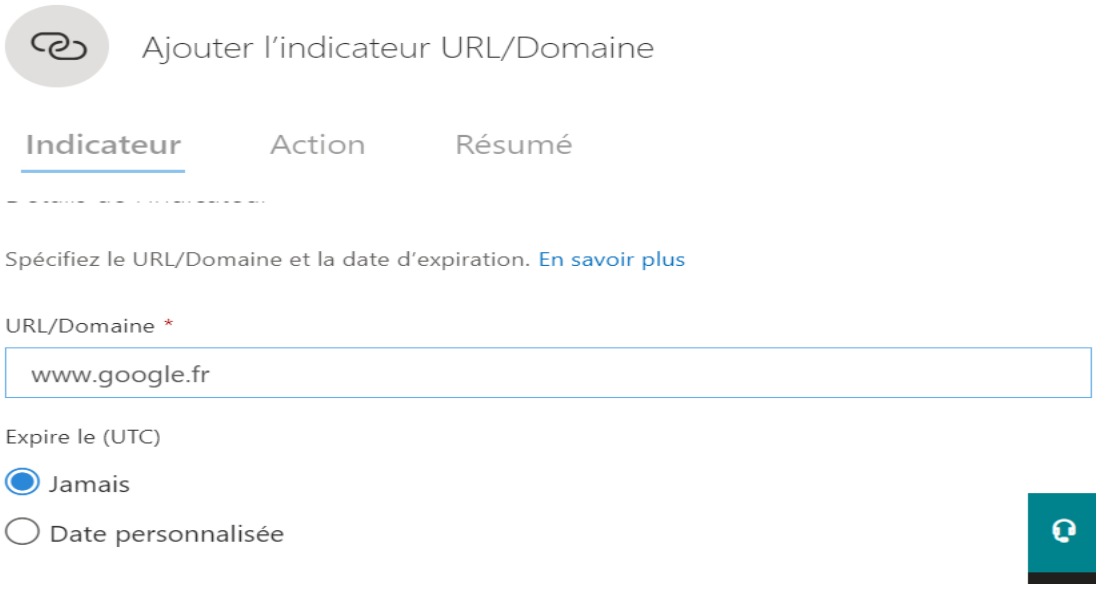
Pour autoriser ou bloquer un site internet, il faut se rendre dans Paramètres - Points de terminaisons – Indicateurs.




*Autorisation d'un accès web*

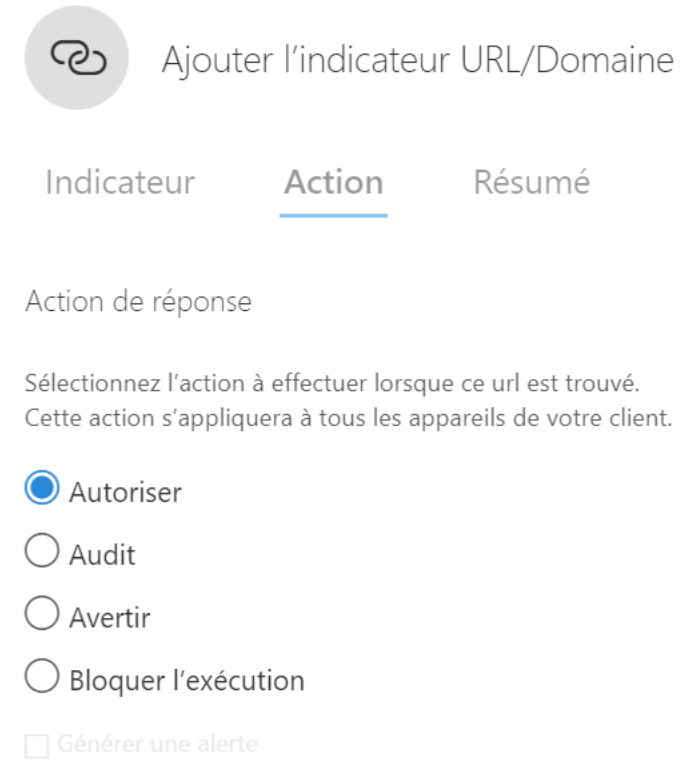
Il existe plusieurs types de filtrages, les deux cas qui nous intéressent sont URL/Domaines et les Adresses IP.

Cliquer sur un des types de filtrages, dans ce cas-ci URL/Domaines, puis sur Add Element :




*Insérer l'URL du site à débloquer*

Indiquer l'URL, puis la périodicité. Il est possible de choisir une échéance, puis cliquer sur *Suivant* :




*Autorisation de l'accès à l'URL indiquer*

Choisir l'action à effectuer : il est possible d'auditer le site (combien de connexion à ce site au sein de notre domaine etc), d'avertir l'utilisateur d'une potentielle faille, de bloquer le site ou de l'autoriser dans le cas d'un faux positif.

Passer les différentes étapes et enregistrer la règle.

A savoir :
Le temps de propagation des règles de filtrage annoncé par Microsoft peut prendre jusqu'à 120 minutes.

## E) La gestion et mise en place des accès conditionnels

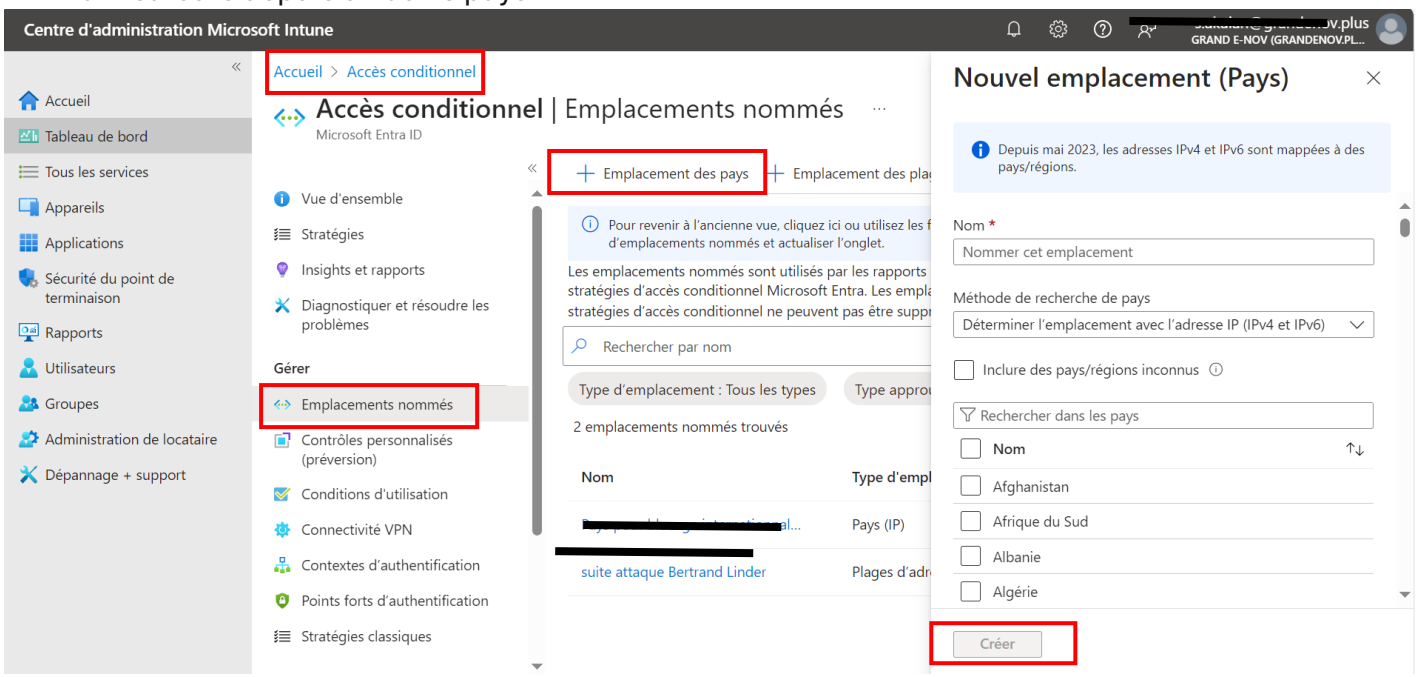
Le périmètre de sécurité moderne s'étend au-delà du périmètre réseau d'une organisation pour inclure l'identité de l'utilisateur et de l'appareil. Les organisations utilisent désormais des signaux basés sur l'identité dans le cadre de leurs décisions de contrôle d'accès. L'accès conditionnel Microsoft Entra regroupe des signaux pour prendre des décisions et appliquer des stratégies organisationnelles. L'accès conditionnel est le moteur de stratégie Confiance Zéro de Microsoft, qui prend en compte des signaux provenant de différentes sources lors de l'application des décisions de stratégie.
Les stratégies d'accès conditionnel, dans leur forme la plus simple, sont des instructions if-then : **si** un utilisateur souhaite accéder à une ressource, **alors** il doit effectuer une action. Par exemple : si un utilisateur souhaite accéder à une application ou à un service comme Microsoft 365, il doit effectuer une authentification multifacteurs pour pouvoir y accéder.
Les administrateurs sont confrontés à deux objectifs principaux :

- Permettre aux utilisateurs d'être productifs où et quand ils le veulent
- Protéger les ressources de l'entreprise

Utilisez des stratégies d'accès conditionnel pour appliquer les contrôles d'accès appropriés pour garantir la sécurité de votre organisation.

En tant que responsable, ma responsabilité est de mettre en place des accès conditionnels afin d'ajouter une couche de sécurité supplémentaire sur l'ensemble de notre infrastructure.

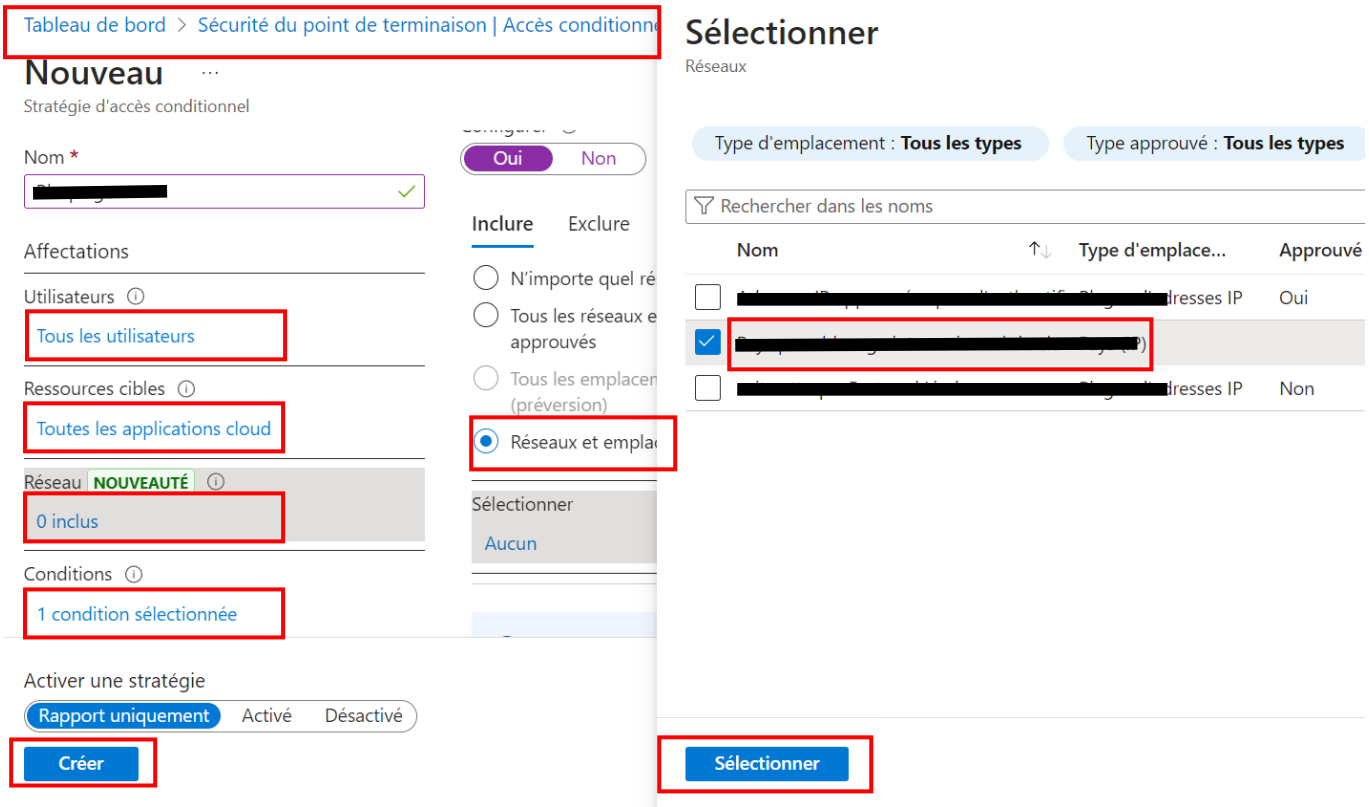
Voici un exemple d'un accès conditionnel mise en place pour bloquer les accès de nos utilisateurs depuis un autre pays.




*Création d'un accès conditionnel*

Pour créer une nouvelle stratégie afin de bloquer les connexions depuis d'autres pays, suivez ces étapes :

1. J'accède aux stratégies d'accès conditionnel dans le portail d'administration Microsoft Entra.
2. Je créé une nouvelle stratégie :
    - Je nomme la stratégie.
    - J'ajoute les utilisateurs ou les groupes que je souhaite inclure dans cette stratégie.
    - Je cible les ressources auxquelles je veux appliquer cette stratégie.
    - J'ajoute la règle créée précédemment dans la partie réseau et je spécifie les conditions.
3. Je clique sur "Créer" pour finaliser la stratégie.

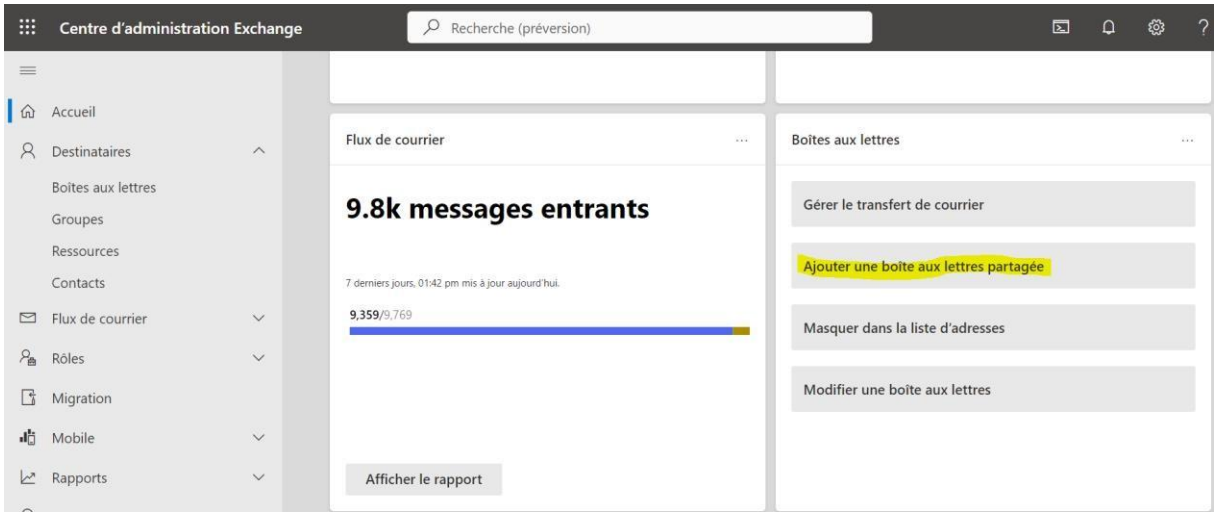



*Créé la stratégie*

### F) Création d'une boîte aux lettres partagée

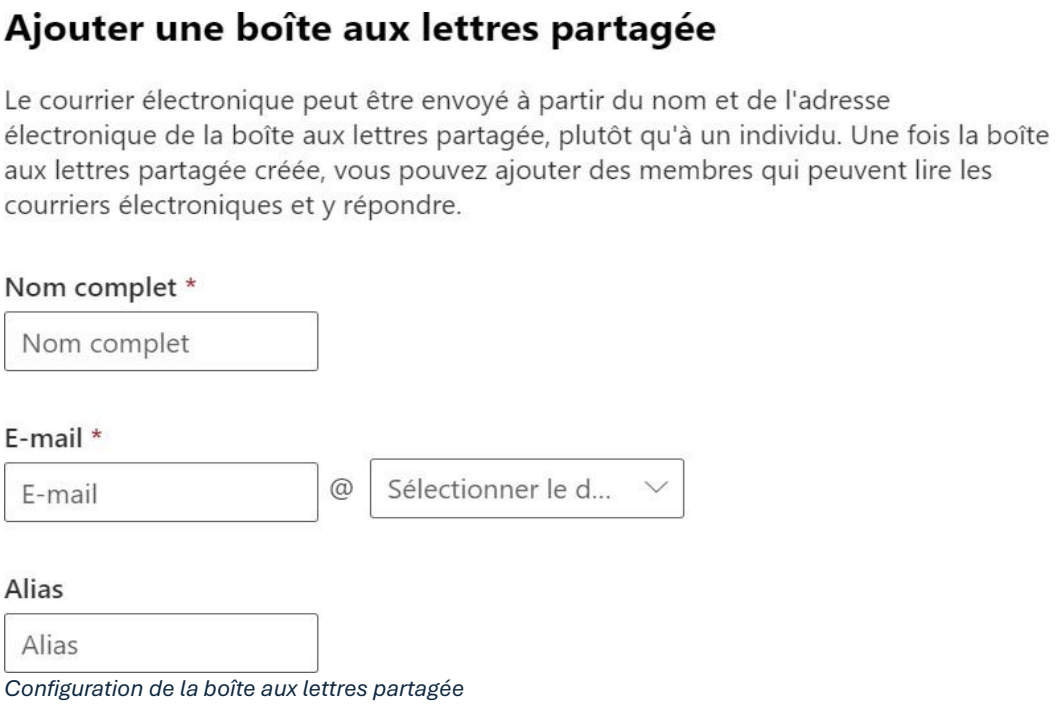
Chez Grand Enov+, les équipes utilisent fréquemment des boîtes aux lettres partagées pour améliorer la collaboration et la gestion des communications. Une boîte aux lettres partagée permet à plusieurs utilisateurs d'accéder à une même adresse électronique, facilitant ainsi le suivi des conversations, le partage des informations et la répartition des tâches. Ce système est particulièrement utile pour les départements qui reçoivent un grand nombre de courriels, comme le service client, le support technique ou les ventes. En utilisant une boîte aux lettres partagée, chaque membre de l'équipe peut voir les messages envoyés et reçus, répondre aux courriels en utilisant l'adresse partagée, et garantir ainsi une communication fluide et coordonnée. Cette approche optimise l'efficacité et assure que les demandes des clients ou des partenaires ne passent pas inaperçues.

1. Accès au centre d'administration d'Exchange :
    - J'ouvre un navigateur web.
    - J'accède à l'URL du centre d'administration d'Exchange.
2. Ajout d'une boîte aux lettres partagée :
    - Dans le centre d'administration d'Exchange, je clique sur l'option « Boîtes aux lettres partagées » dans le volet de navigation.
3. Création d'une nouvelle boîte aux lettres partagée :
    - Je clique sur le bouton « + Ajouter une boîte aux lettres partagée ».



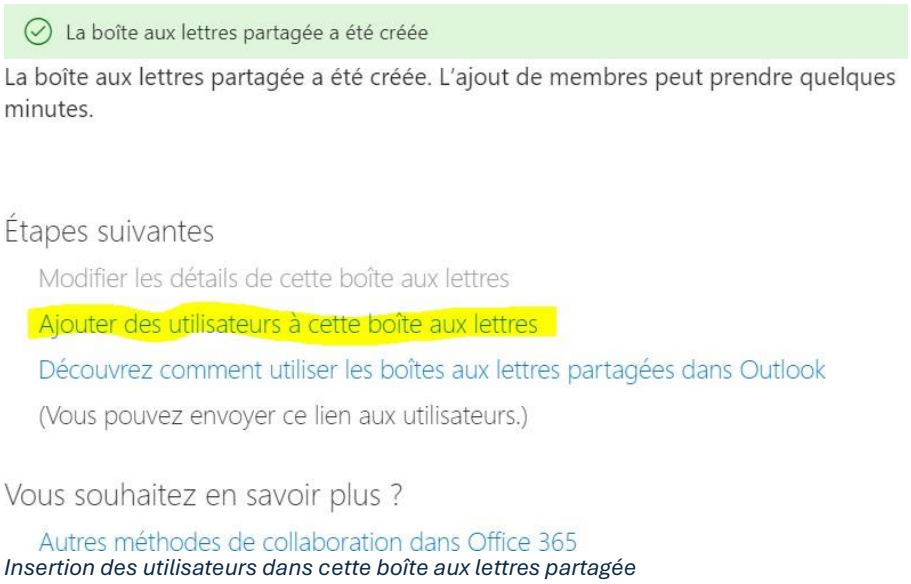

*Création d'une boîte aux lettres partagée*

- Je donne un nom à la boîte aux lettres partagée.
- Je sélectionne le nom de domaine approprié pour cette boîte aux lettres.




*Configuration de la boîte aux lettres partagée*

- J'ajoute les utilisateurs qui veulent partager cette boîte aux lettres.
- Je clique sur « Ajouter des utilisateurs à cette boîte aux lettres ».




*Insertion des utilisateurs dans cette boîte aux lettres partagée*

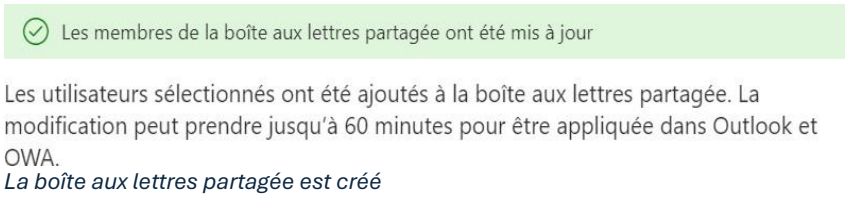
- Je clique sur « Add members » pour ajouter des membres.


*Insertion des utilisateurs dans cette boîte aux lettres partagée*

- Je cherche les utilisateurs via la barre de recherche.


*Rechercher les utilisateurs à mettre dans votre boîte aux lettres partagée*

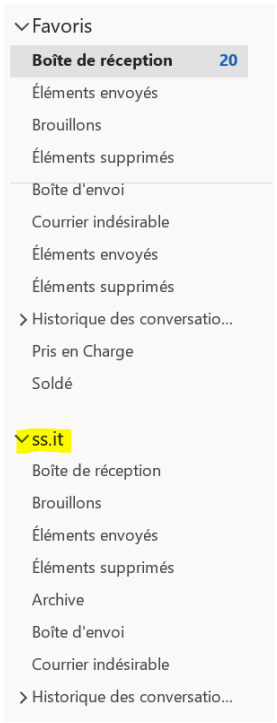
- Je paramètre l'envoi des mails, la lecture et la gestion de cette boîte aux lettres partagée.




*La boîte aux lettres partagée est créé*


*Gestion d'autorisation et d'envoyer de la boîte aux lettres*

- J'attends quelques minutes et la boîte aux lettres partagée apparaîtra sous la boîte mail principale dans l'application Outlook.




*Vérification dans Outlook*

- Un test est effectué, et la boîte aux lettres partagée reçoit et peut envoyer des courriels.


Test

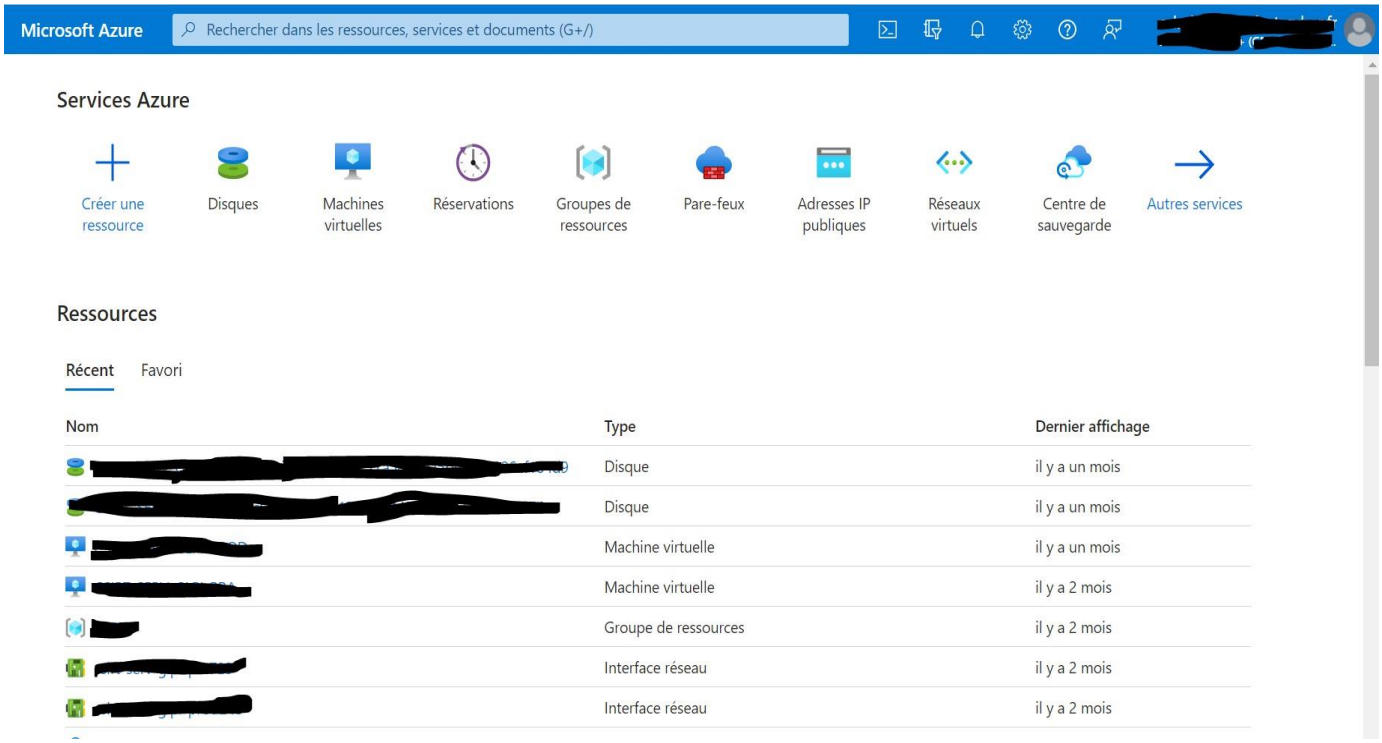
*Test d'envoi et réception*

### G) Ouverture de port pour un serveur

L'ouverture de ports sur un serveur est une opération cruciale pour permettre la communication entre le serveur et les clients ou autres serveurs sur le réseau. Les ports sont des points de connexion spécifiques qui permettent aux données de circuler entre les appareils. Chaque application ou service utilise un port spécifique pour envoyer et recevoir des informations. Par exemple, le port 80 est utilisé pour le trafic HTTP, tandis que le port 443 est utilisé pour le trafic HTTPS sécurisé.

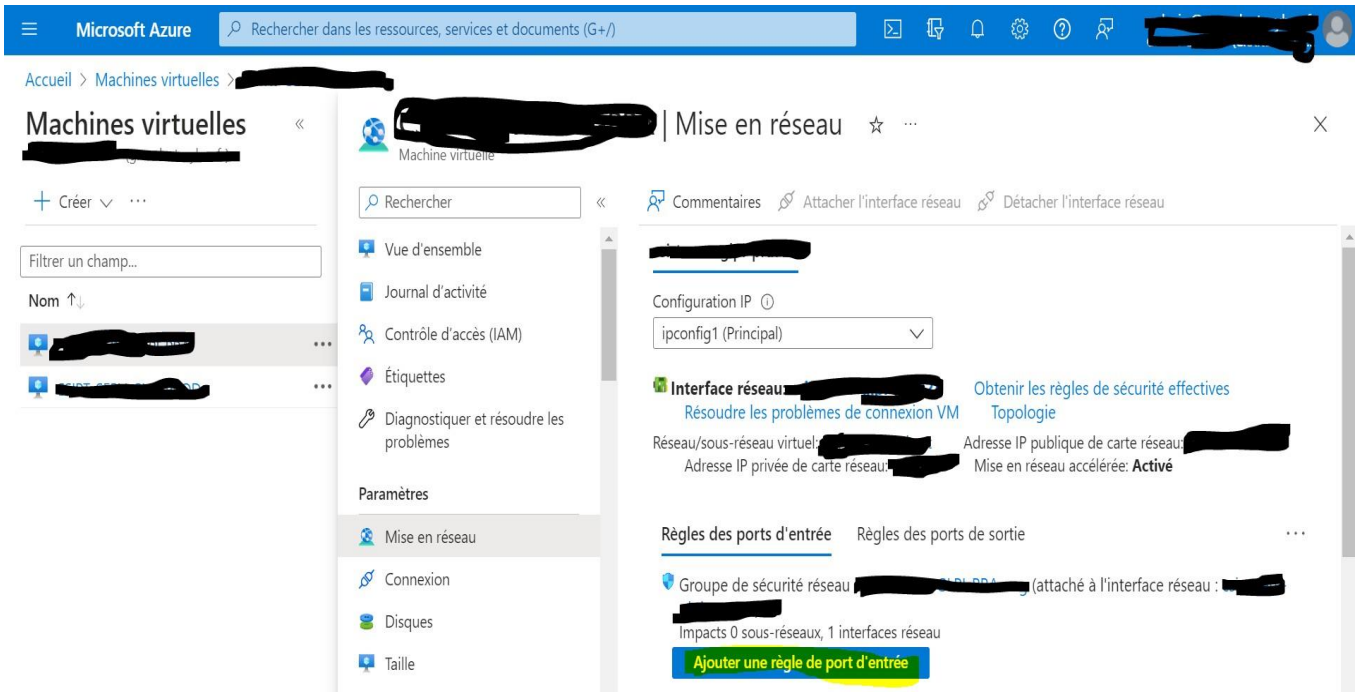
Chez Grand Enov+, il est essentiel de bien gérer l'ouverture des ports pour assurer la sécurité et la performance des systèmes. Une configuration adéquate permet de garantir que seuls les services nécessaires sont accessibles, réduisant ainsi les risques de sécurité tout en optimisant les ressources réseau. Avant d'ouvrir un port, il est important de comprendre quel service en a besoin et de vérifier les politiques de sécurité en place. Une gestion rigoureuse des ports ouverts contribue à maintenir un environnement informatique sûr et efficace, tout en permettant aux équipes de travailler de manière fluide et coordonnée.

- Je vais sur le portail Microsoft Portal Azure.
- Je sélectionne la machine virtuelle concernée.




*Ouverture de port dans le portail Azure*

- Je clique sur « Mise en réseau ».
- Je sélectionne « Ajouter une règle de port d'entrée ».




*Sélection du serveur et de l'ajout du port*

Ici je peux définir toute la configuration sur le port que l'on veut ajouter sur notre serveur.

- Source : Le filtre source peut correspondre à n'importe lequel, une plage d'adresses IP, mon adresse IP, un groupe de sécurité d'application ou une étiquette par défaut. Il spécifie le trafic entrant autorisé ou refusé par la règle à partir d'une plage d'adresses IP source spécifique.

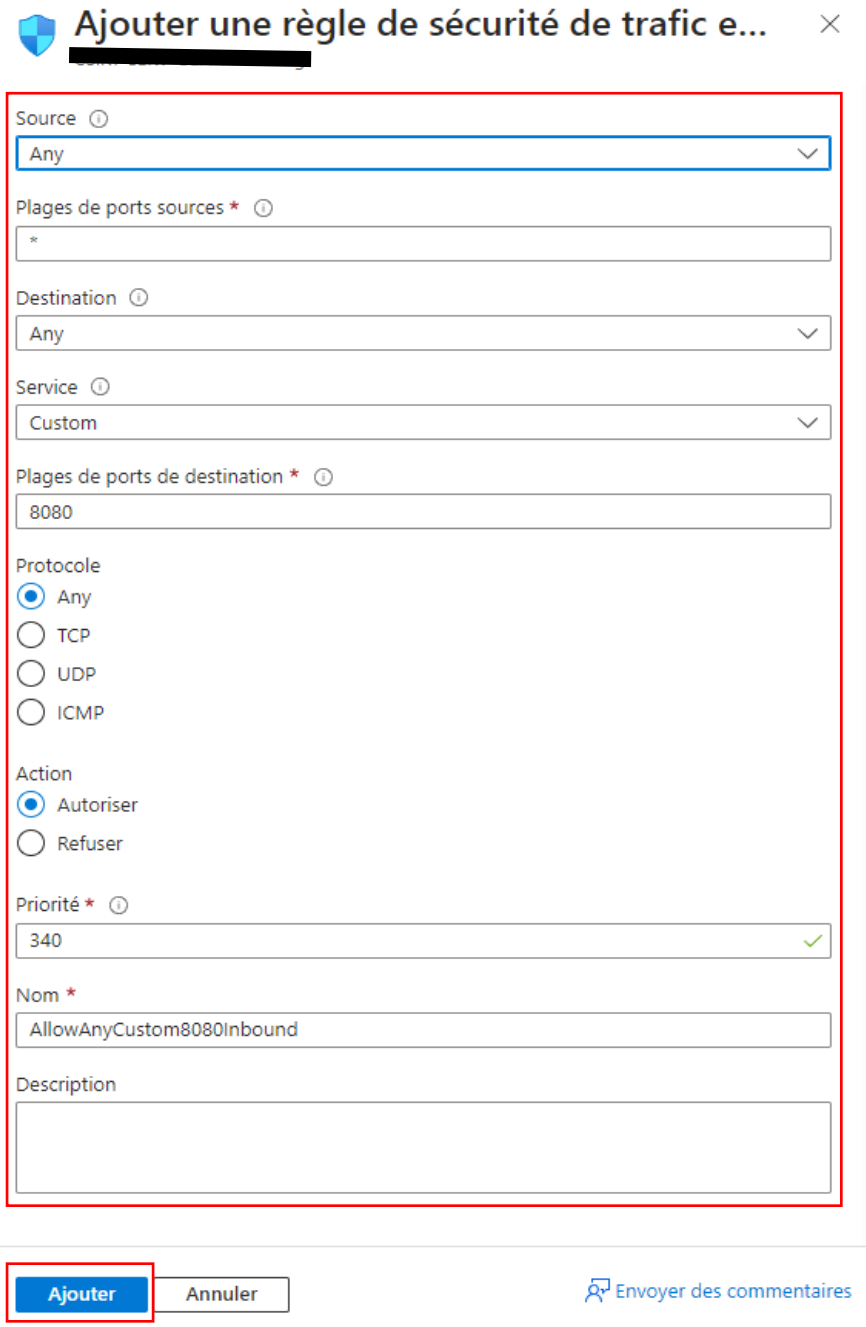
- Plages de ports sources : Fournissez un port unique (comme 80), une plage de ports (comme 1024-65535) ou une liste de ports uniques et/ou de plages de ports séparés par des virgules (comme 80,1024-65535). Ce paramètre spécifie les ports sur lesquels le trafic est autorisé ou refusé par cette règle. Indiquez un astérisque (*) pour autoriser le trafic sur n'importe quel port.

- Destination : Le filtre de destination peut être N'importe lequel, une plage d'adresses IP, un groupe de sécurité d'application ou une étiquette par défaut. Il spécifie le trafic sortant autorisé ou refusé par la règle vers une plage d'adresses IP de destination déterminée.

- Service : Le service spécifie le protocole de destination et la plage de ports pour cette règle. Vous pouvez choisir un service prédéfini, comme RDP ou SSH, ou fournir une plage de ports personnalisée.

- Plages de ports de destination : Fournissez un port unique (comme 80), une plage de ports (comme 1024-65535) ou une liste de ports uniques et/ou de plages de ports séparés par des virgules (comme 80,1024-65535). Ce paramètre spécifie les ports sur lesquels le trafic est autorisé ou refusé par cette règle. Indiquez un astérisque (*) pour autoriser le trafic sur n'importe quel port.

- Protocole : je choisis un protocole dans la liste.
- Action : Autoriser ou Refuser.
- Priorité : Les règles sont traitées par ordre de priorité : plus le nombre est faible, plus la priorité est élevée. Nous vous recommandons de laisser des intervalles entre les règles, par exemple, 100, 200, 300, etc. Vous pourrez ainsi ajouter facilement de nouvelles règles sans avoir à modifier les règles existantes.
- Nom : Je donne un nom au port.
- Description : Des indications que je ne veux pas oublier, etc.



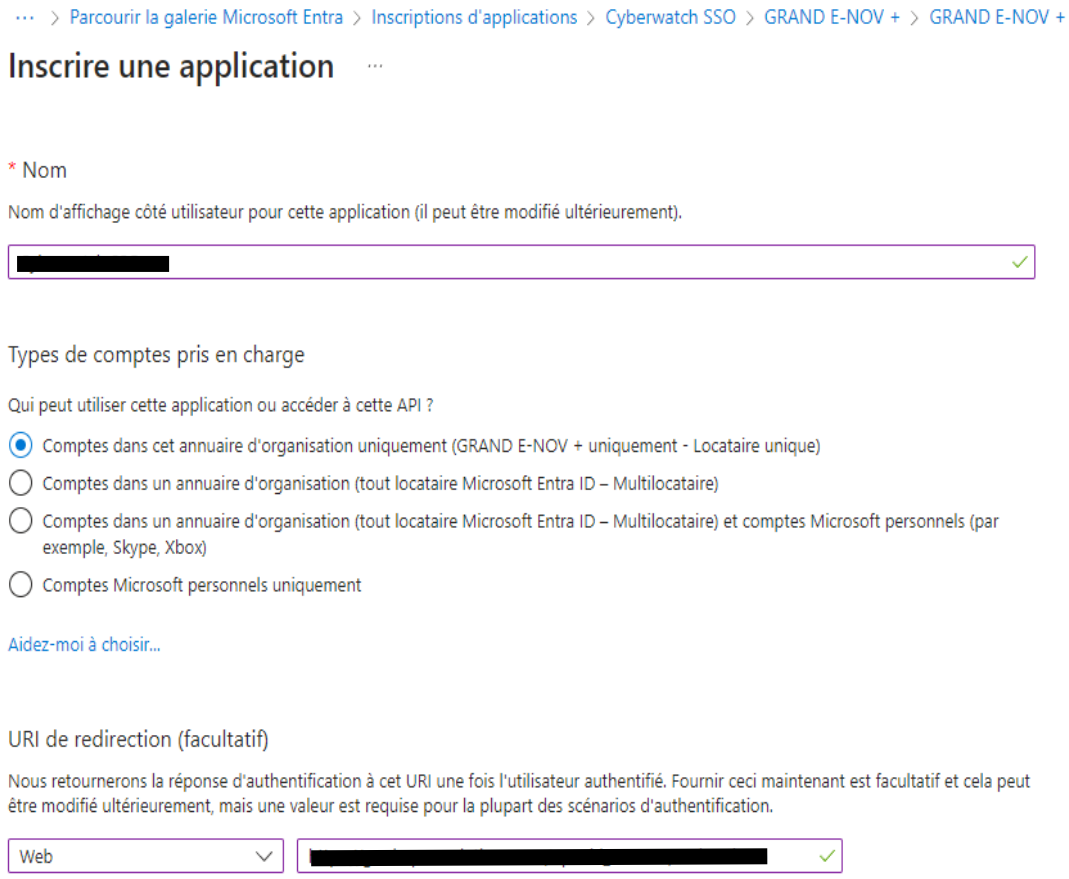

*Configuration du port*

### H) Mise en place SSO sur une application

La mise en place du Single Sign-On (SSO) sur une application permet aux utilisateurs d'accéder à plusieurs applications avec un seul jeu d'identifiants. Cela simplifie le processus de connexion, améliore l'expérience utilisateur et renforce la sécurité en centralisant la gestion des accès. Chez Grand Enov+, l'intégration du SSO vise à offrir une expérience fluide et sécurisée, en utilisant des protocoles standards comme SAML, OAuth ou OpenID Connect.

Étape 1 : À partir de Microsoft Entra ID

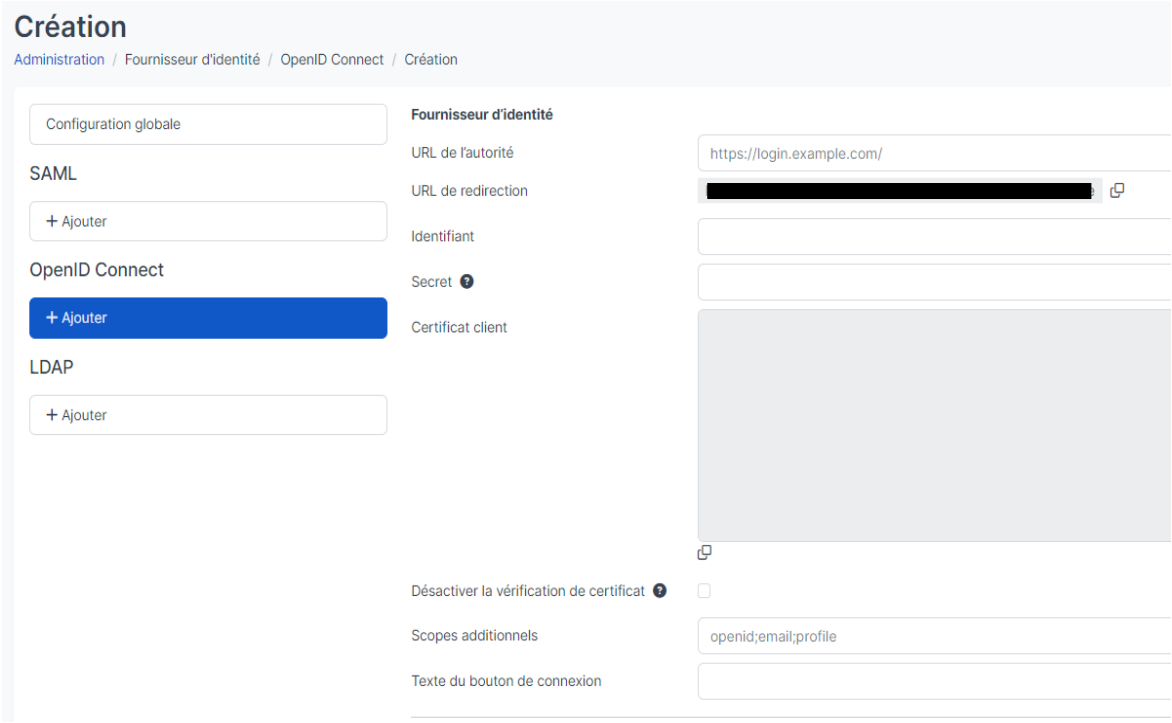
1. Créez une nouvelle application :
    - Je donne un nom à l'application.
    - L'URI de redirection est fourni par l'application à intégrer.
2. Une fois l'application créée dans Entra, je saisie dans l'application à intégrer l'ID d'application (champ Identifiant dans « le nom de l'application »)




*Page de configuration d'une SSO pour une application*

3. Retournez dans l'application :
    - Dans l'URL de l'autorité, je saisie https://login.microsoftonline.com/ 'l'ID de l'annuaire (locataire)'/v2.0.
    - J'enregistre les modifications.

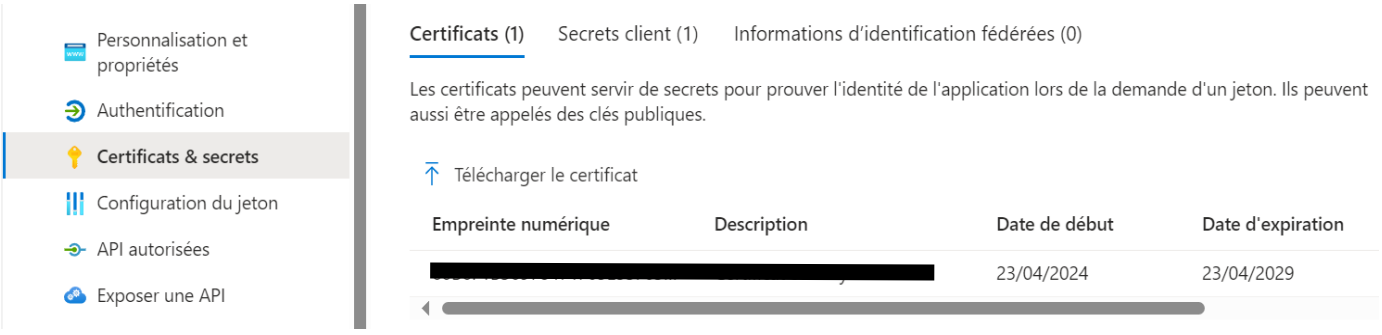
4. L'application fournit un certificat sous forme de texte qui commence par ===== BEGIN CERTIFICATE ======.




*Création de la SSO dans l'application avec*

- Je renomme le fichier .txt en .cer.
- Je l'importe dans Entra : dans API => Certificats et secrets.
- Dans le secret client : J'ajoute un nouveau client.

Je m'assure de sauvegarder correctement les configurations après chaque étape.




*Insertion du certificat*

## I) Participation à un AUDIT cybersécurité

Pendant mon alternance, j'ai eu l'opportunité de participer à un audit de cybersécurité visant à évaluer la santé de notre infrastructure en termes de sécurité. Cette expérience m'a permis de comprendre en profondeur ce qu'implique un audit, les actions principales réalisées sur une infrastructure, ainsi que les points stratégiques vérifiés.

Au cours des réunions d'audit, j'ai pu observer les discussions et les exigences détaillées tout au long du processus, depuis le début jusqu'à la fin. À la clôture de l'audit, le prestataire a envoyé un document comprenant les observations, les évaluations et les recommandations pour l'audit organisationnel, ainsi que l'audit de Microsoft 365.

Les recommandations fournies visent à améliorer la sécurité de notre infrastructure et à obtenir de meilleurs résultats lors des prochains audits, en sécurisant les points de vulnérabilité identifiés.

almond

*Prestaire qui a réalisé l'audit*

## J) Participation à une campagne de sensibilisation

Pendant mon alternance, j'ai participé avec la société "Avant de cliquer" pour la mise en place d'un outil campagne de sensibilisation à la sécurité informatique en entreprise. Cette expérience m'a permis de contribuer à l'éducation des employés sur les risques de sécurité informatique, comme le phishing et les malwares, ainsi que sur les bonnes pratiques à adopter. Voici un exemple de faux mail :

Activité suspecte sur votre compte de messagerie

RI Responsable Informatique <s.i@portailinform
À Selim AKALAN 27/05/2024

En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur web.
Cliquez ici pour télécharger des images. Pour protéger la confidentialité, Outlook a empêché le téléchargement automatique de certaines images dans ce message.

Selim,

Un tiers a récemment utilisé votre mot de passe pour se connecter à votre compte de messagerie électronique.

Nous avons bloqué la tentative de connexion dans le cas où il s'agirait d'un piratage essayant d'accéder à votre compte.

Veuillez examiner les détails de la tentative de connexion :

- Adresse IP : 46.228.82.222
- Position : Pologne

Si vous n'avez pas effectué cette tentative de connexion, cela signifie peut-être qu'un tiers essaie d'accéder à votre compte. Nous vous conseillons de vous connecter à votre compte et de réinitialiser votre mot de passe immédiatement.

**Réinitialiser le mot de passe**

Cordialement,

Votre équipe support

*Exemple de mail reçu*

### Objectifs de la Campagne :

- Éduquer les employés sur les menaces de sécurité courantes.
- Promouvoir les bonnes pratiques de sécurité informatique.
- Réduire les risques d'erreurs humaines en matière de sécurité.

### Activités Réalisées :

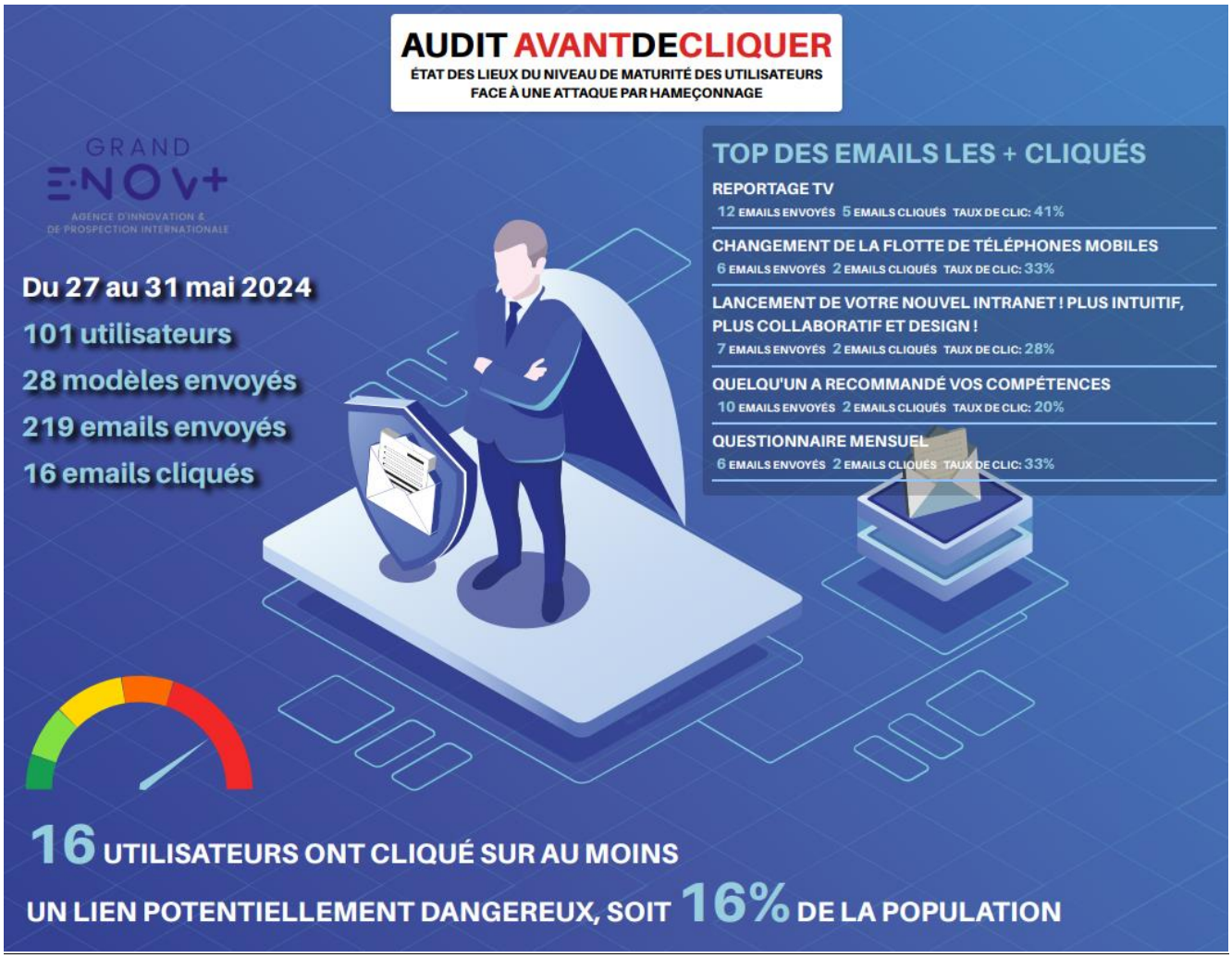
- Développement de supports pédagogiques (présentations, vidéos, quiz).
- Organisation de sessions de formation en présentiel et en ligne.
- Mise en place de simulations d'attaques de phishing pour tester la vigilance des employés.

### Résultats Observés :

- Amélioration de la compréhension des employés sur les menaces de sécurité.
- Diminution des incidents de sécurité après la campagne.
- Identification d'axes d'amélioration pour les futures campagnes.

Cette expérience m'a permis de renforcer mes compétences en sensibilisation à la sécurité informatique et en gestion de projet.

Résultat de l'Agence sur le premier audit AvantdeCliquer :




*Résultat de l'Agence sur l'Audit de sensibilisation*

## Conclusion :

Mon alternance chez Grand E-NOV+ en tant qu'administrateur système, réseau et sécurité a été une expérience particulièrement enrichissante et formatrice. Cette période a été marquée par l'acquisition de compétences techniques et par un profond développement professionnel.

Durant cette alternance, j'ai été impliqué dans de nombreux projets critiques, notamment la mise en place de solutions de sécurité avancées avec Microsoft Defender, ainsi que la gestion des accès conditionnels et l'intégration des téléphones dans le Mobile Device Management (MDM). Ces responsabilités m'ont permis de développer des compétences essentielles en gestion d'infrastructures IT modernes et en sécurité des systèmes d'information.

Les différentes missions qui m'ont été confiées, telles que le support aux utilisateurs, la préparation du matériel pour les nouveaux collaborateurs, et la participation à des audits de cybersécurité, m'ont permis de comprendre les enjeux réels de la sécurité informatique et de la gestion des réseaux dans un environnement professionnel.

Les défis rencontrés, notamment lors de l'audit de sécurité et de la mise en place de nouvelles politiques de sécurité, m'ont appris à adopter une approche rigoureuse et proactive. J'ai appris à analyser les problèmes, à proposer des solutions efficaces et à collaborer avec différentes équipes pour assurer le bon fonctionnement et la sécurité de notre infrastructure.

Je tiens à exprimer ma gratitude envers mes superviseurs et collègues pour leur soutien et leur confiance. Leur encadrement et leurs conseils m'ont permis de progresser rapidement et de m'intégrer pleinement à l'équipe. Leur expertise et leur disponibilité ont été des atouts précieux pour ma formation.

Cette alternance a confirmé mon intérêt pour le domaine de l'administration système, réseau et sécurité, et a renforcé ma détermination à poursuivre une carrière dans ce secteur. Les compétences techniques et professionnelles acquises au cours de cette expérience seront des bases solides pour mes futurs projets professionnels.

Mon alternance chez Grand E-NOV+ a été une étape déterminante dans mon parcours. Elle m'a offert une expérience concrète et significative dans un environnement professionnel exigeant, tout en me permettant de contribuer activement à des projets d'importance pour l'entreprise. Je suis reconnaissant pour cette opportunité et enthousiaste à l'idée de mettre à profit ces compétences dans ma future carrière.

## Glossaire :

**CRM** : Le CRM ou gestion de la relation client (Customer Relationship Management) est une stratégie de gestion des relations et interactions d'une entreprise avec ses clients ou clients potentiels. Un système CRM aide les entreprises à interagir en permanence avec les clients, à rationaliser leurs processus et à améliorer leur rentabilité.

**Salesforce** : Salesforce est une entreprise technologique américaine spécialisée dans la fourniture de solutions de gestion de la relation client (CRM, Customer Relationship Management). Fondée en 1999 par Marc Benioff et Parker Harris, Salesforce propose une plateforme de services basée sur le cloud qui aide les entreprises à gérer leurs interactions avec les clients et les prospects. Salesforce est une solution complète pour les entreprises cherchant à améliorer leurs relations avec les clients, augmenter leurs ventes, fournir un service client exceptionnel et optimiser leurs campagnes marketing, le tout via une plateforme intégrée et accessible en ligne.

**MFA :** L'authentification multifacteur (MFA) est une méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN.

**BitLocker** : BitLocker est la technologie de chiffrement Windows qui protège vos données contre les accès non autorisés en chiffrant votre lecteur et en exigeant un ou plusieurs facteurs d'authentification avant qu'il ne le déverrouille.

**Tenant** : Le mot Tenant peut se traduire par : locataire, résident, occupant. Dans l'univers du Cloud, le terme Tenant désigne un nuage privé dans lequel les données du locataire vont être stockées.

**Azure AD** : Azure Active Directory (Azure AD) est un service cloud de gestion des identités et des accès proposés par Microsoft. Il permet aux organisations de gérer de manière centralisée les utilisateurs, les groupes, les appareils, et l'accès aux applications SaaS et aux ressources cloud. Azure AD offre des fonctionnalités telles que l'authentification unique (SSO), l'authentification multifacteur (MFA), le contrôle d'accès basé sur les rôles (RBAC), et la gestion des appareils, facilitant ainsi la sécurisation et la gestion des environnements informatiques modernes, aussi bien dans le cloud que sur site via une intégration avec Active Directory.

**SaaS** : "Software as a Service", est un modèle de distribution de logiciels dans lequel les applications sont hébergées par un fournisseur de services et mises à disposition des utilisateurs via Internet. Les utilisateurs accèdent aux applications via un navigateur web, sans nécessiter de téléchargement ni d'installation locale. Ce modèle permet aux entreprises de souscrire à des logiciels, de les utiliser à la demande, et de payer généralement par abonnement, évitant ainsi les coûts d'achat de licences et de maintenance des infrastructures sous-jacentes.

**OneDrive** : OneDrive est un service de stockage en ligne de Microsoft, intégré à Office 365, qui permet aux utilisateurs de stocker, synchroniser, partager et collaborer sur des fichiers et documents via le cloud, tout en offrant des fonctionnalités avancées de sécurité et de gestion des données, disponibles dans des versions gratuites et payantes.
**MDM** : MDM (Mobile Device Management) est une solution de gestion permettant de sécuriser, de surveiller et de gérer les appareils mobiles tels que les smartphones et les tablettes utilisés par les employés au sein d'une organisation, assurant ainsi une conformité et une sécurité optimales.
**EDR** : EDR (Endpoint Detection and Response) est une technologie de sécurité qui surveille et répond aux menaces potentielles sur les périphériques (endpoints) tels que les ordinateurs portables, les ordinateurs de bureau et les serveurs. Elle permet de détecter, d'analyser et de répondre aux activités suspectes ou malveillantes afin de renforcer la sécurité des systèmes informatiques d'une organisation.
**Endpoint** : Un "endpoint" (ou périphérique de point de terminaison en français) est un appareil individuel, comme un ordinateur portable, un ordinateur de bureau, un smartphone, une tablette, ou tout autre dispositif connecté à un réseau informatique. En informatique et en sécurité, les endpoints sont des points d'entrée potentiels pour les attaques, ce qui rend la sécurité des endpoints (Endpoint Security) cruciale pour la protection des données et des systèmes de l'entreprise. La gestion des endpoints (Endpoint Management) inclut la configuration, la surveillance, la mise à jour et la sécurisation de ces périphériques pour assurer la conformité et minimiser les risques de sécurité.
**Filtrage web** : Le filtrage web est une technique utilisée pour contrôler et limiter l'accès des utilisateurs à des sites web spécifiques en fonction de règles prédéfinies. Il permet de bloquer l'accès à des contenus inappropriés, malveillants ou non autorisés, renforçant ainsi la sécurité du réseau et améliorant la productivité des utilisateurs en limitant l'accès à des sites non pertinents.
**Accès conditionnel** : L'accès conditionnel est une stratégie de sécurité qui contrôle l'accès aux ressources informatiques en fonction de certaines conditions prédéfinies. L'accès conditionnel permet de définir des règles d'accès basées sur différents critères tels que l'emplacement de l'utilisateur, le type d'appareil utilisé, l'état de sécurité de l'appareil, et d'autres facteurs de risque. Cela permet de renforcer la sécurité en limitant l'accès aux ressources sensibles uniquement aux utilisateurs et appareils qui respectent les critères de sécurité définis.

**SSO** : SSO (Single Sign-On) est une méthode d'authentification qui permet à un utilisateur de se connecter une seule fois pour accéder à plusieurs applications et services, sans avoir à se reconnecter à chaque fois. En d'autres termes : SSO simplifie l'expérience utilisateur en permettant une connexion unique à plusieurs applications avec un seul ensemble d'identifiants. Il améliore la sécurité en réduisant le nombre de mots de passe que les utilisateurs doivent gérer et potentiellement exposer. Il est largement utilisé dans les environnements d'entreprise et cloud pour améliorer l'efficacité, la sécurité et l'expérience utilisateur globale.

**URI** : URI (Uniform Resource Identifier) est une chaîne de caractères utilisée pour identifier une ressource sur un réseau, que ce soit sur Internet ou dans d'autres systèmes informatiques. Un URI est une séquence de caractères qui identifie de manière unique une ressource sur un réseau, telle qu'une page web, un fichier, un service, ou tout autre objet. Il peut être utilisé pour localiser la ressource en spécifiant le protocole d'accès (comme HTTP, FTP, etc.) et l'adresse de la ressource.

**URL** : Une URL (Uniform Resource Locator) est une forme particulière d'URI (Uniform Resource Identifier) qui permet d'identifier de manière unique une ressource sur Internet et de spécifier l'endroit où elle se trouve. Une URL est une adresse web spécifique qui indique comment accéder à une ressource sur Internet, en précisant le protocole d'accès (comme HTTP, HTTPS, FTP), le nom de domaine ou l'adresse IP du serveur, et le chemin vers la ressource. Par exemple, https://www.example.com/index.html est une URL qui spécifie le protocole HTTPS, le nom de domaine "www.example.com" et le chemin "/index.html" pour accéder à une page web spécifique.

**API** : Une API (Application Programming Interface) est un ensemble de règles et de protocoles qui permet à différentes applications logicielles de communiquer entre elles. Une API définit les méthodes standardisées par lesquelles des logiciels peuvent interagir entre eux pour échanger des données et des services. Elle spécifie les types de requêtes que l'on peut faire, comment formater les données, et les types de retour attendus. Les API sont largement utilisées pour permettre l'intégration entre différentes applications et services, facilitant ainsi le développement de logiciels complexes et la création d'écosystèmes numériques.

**SAML** : L'acronyme *SAML* signifie Security Assertion Markup Language. Son rôle principal en matière de sécurité en ligne est de vous permettre d'accéder à plusieurs applications Web à l'aide d'une seule paire d'identifiants. Ce standard transfère les informations d'authentification dans un format spécifique entre deux parties : en général un fournisseur d'identité et une application Web.

**OAuth** : L'OAuth est une norme technique permettant de donner des autorisations aux utilisateurs. Il s'agit d'un protocole permettant de transmettre une autorisation d'un service à un autre sans partager les informations d'identification de l'utilisateur, telles qu'un nom d'utilisateur et un mot de passe.

**OpenID Connect** : Est un protocole d'authentification basé sur le protocole OAuth 2.0, qui permet de vérifier l'identité des utilisateurs et d'obtenir des informations de base sur leur profil de manière sécurisée. Il simplifie le processus de connexion en permettant aux utilisateurs de s'authentifier une seule fois pour accéder à plusieurs applications ou services. OpenID Connect est largement utilisé pour l'authentification unique (SSO) et offre des fonctionnalités robustes pour gérer les sessions utilisateur, tout en garantissant la confidentialité et la sécurité des données d'authentification.

## Annexes :

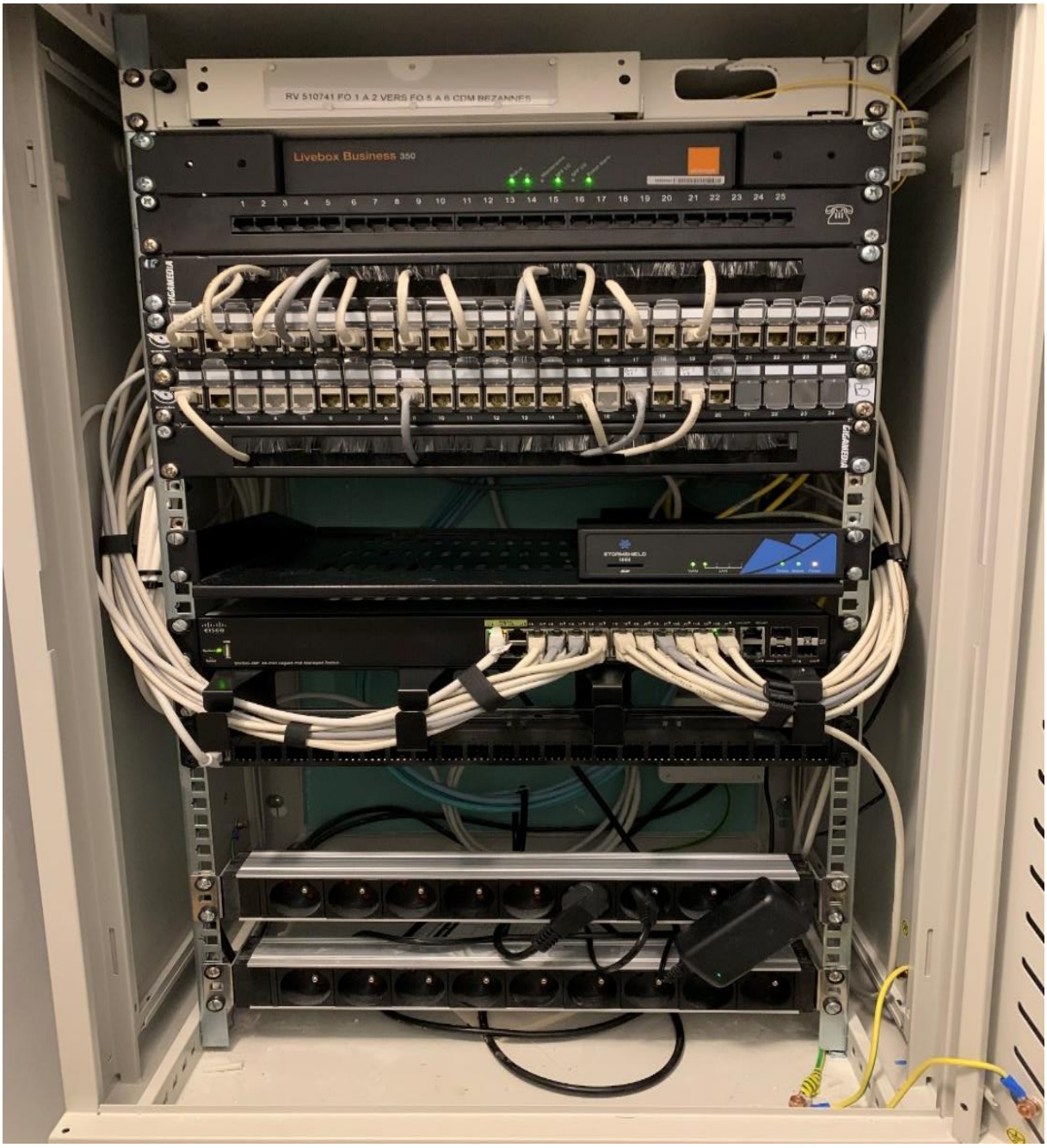
## Annexe 1 : Site de Strasbourg


*Site de Strasbourg*

## Annexe 2 : Site de Nancy

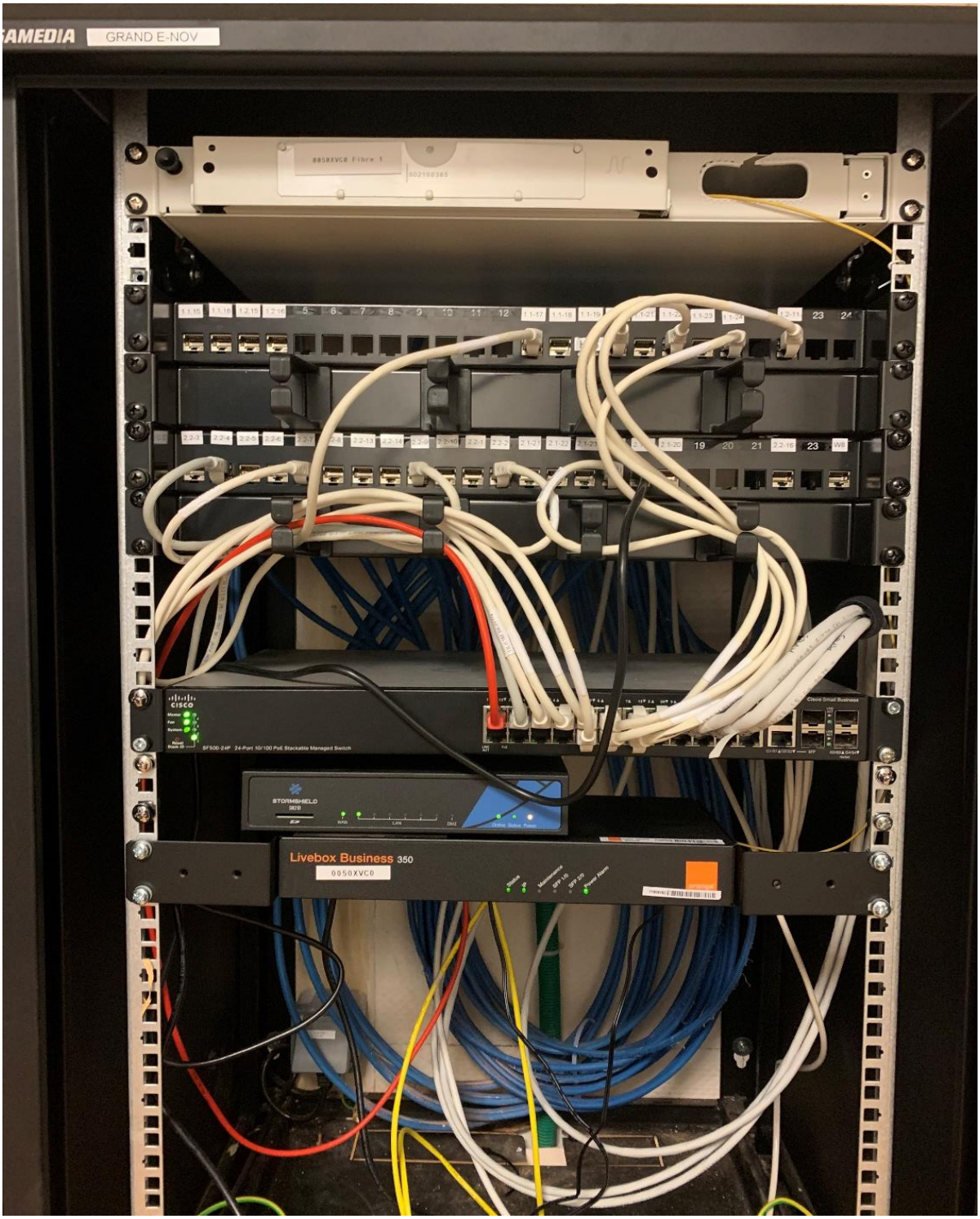

*Site de Nancy*

## Annexe 3 : Site de Bezannes




*Site de Bezannes*

## Annexe 4 : Site de Colmar




*Site de Colmar*