

# Soutenance de Stage

**Technicienne informatique**

**Stage réalisé du 14 avril au 20 juin 2025**

---

**Tuteur de stage : Romain OGER**

**Tuteur pédagogique : Fayssal BENKHALDOUN**

**Aliya MAATIT**



# SOMMAIRE

Introduction et remerciements

---

L'entreprise et son équipe

---

Les missions

---

Organisation du travail

---

Problèmes rencontrés & solutions

---

Conclusion techniques et humaines

---

Conclusion en anglais

---

# I - Introduction et remerciements

## Contexte du stage :

- Transformation numérique de l'entreprise
- Enjeux de sécurité et de gestion des accès
- Besoin d'un support informatique réactif et structuré

## Objectifs du stage :

- Assurer le support informatique
- Participer au renforcement de la sécurité informatique (MFA, mot de passe)
- Formalisation des procédures

## Questionnement :

- Equilibre entre contraintes techniques, humaines et organisationnelles.

- M. Benkhaldoun – Tuteur pédagogique
- Romain Oger – Tuteur de stage
- Aymen Abid – Technicien référent
- Équipe MOMA GROUP

## II - Présentation de l'entreprise

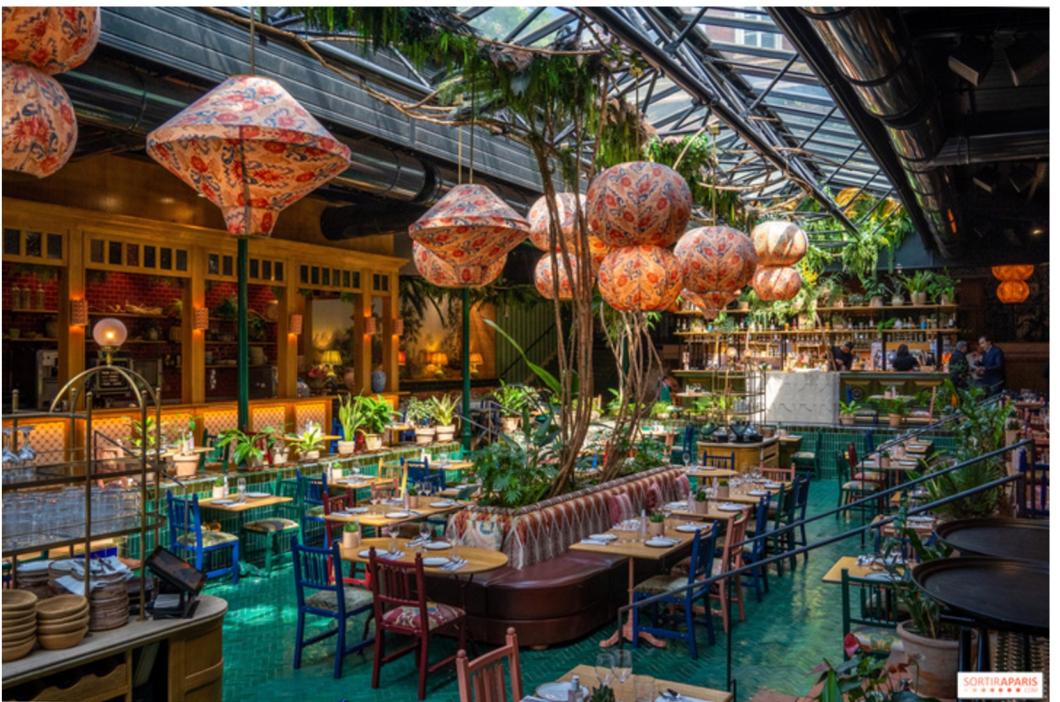
---

- Fondé en 1997 par Benjamin Patou
- Siège à Paris 16<sup>e</sup>
- Groupe de restauration haut de gamme et événementiel
- 3 entités principales :
  - MOMA GROUP (restaurants, clubs)
  - MOMA EVENT (événementiel & communication)
  - MOMA SELECTION (lieux privatisables)



# Activité et rayonnement du groupe

- Établissements emblématiques : Victoria, Manko, Andia, Noto
- Présence en France et à l'international : Saint-Tropez, Megève, Marrakech, Dubaï, Arabie Saoudite
- En 2023 : 800 collaborateurs et un CA d'environ 130 millions d'euros



Restaurant Andia



Restaurant Noto

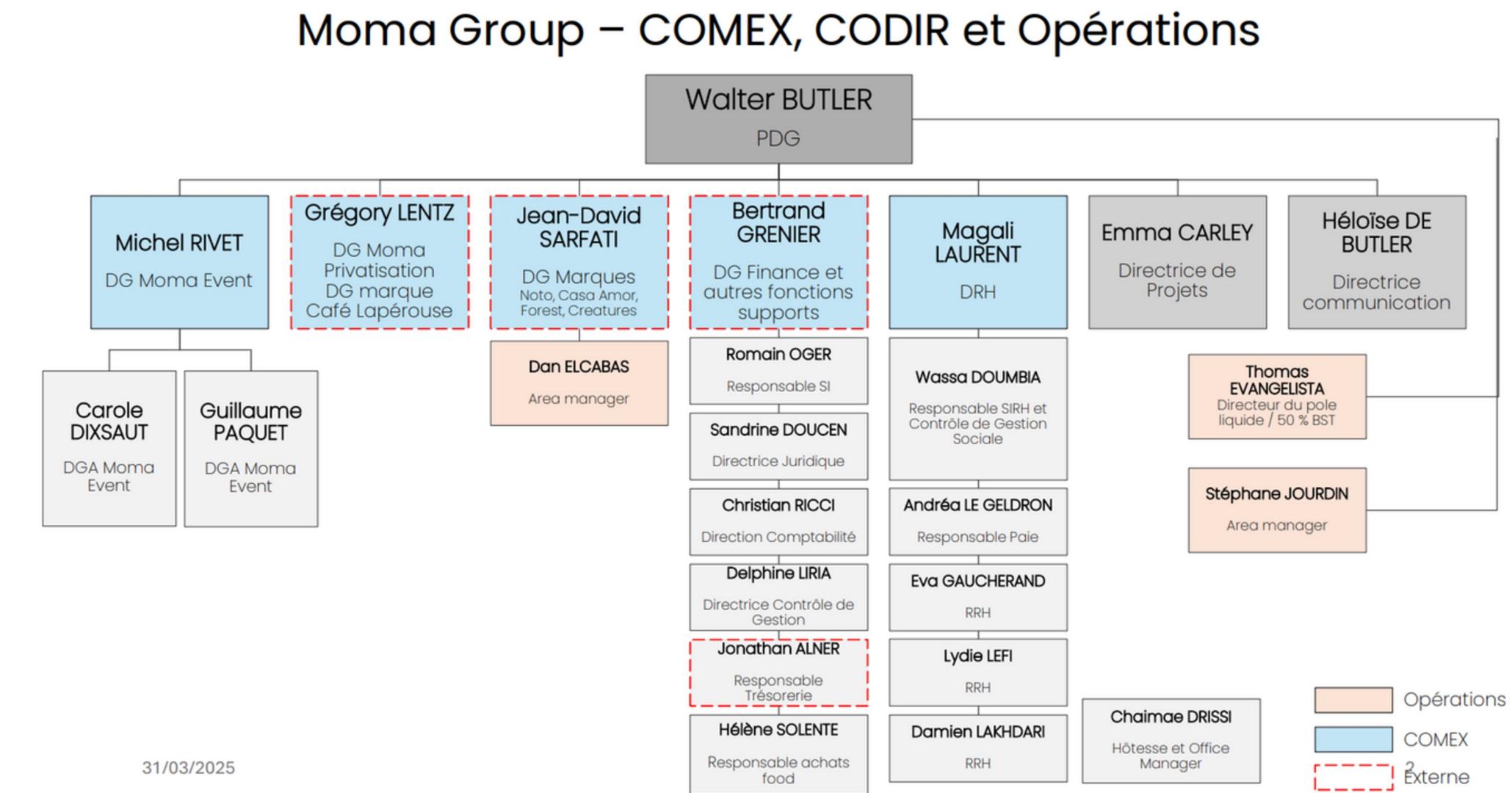
# Organisation interne

## Réorganisation :

- Départ du fondateur Benjamin Patou
- Rachat par Walter Butler (investisseur)
- Nouvel objectif : professionnalisation et structuration

## Renforcement des fonctions support :

- Mise en avant du service informatique
- Centralisation des processus
- Meilleure coordination entre services



WALTER  
BUTLER



BENJAMIN  
PATOU

31/03/2025

# Le service informatique et ses enjeux numériques

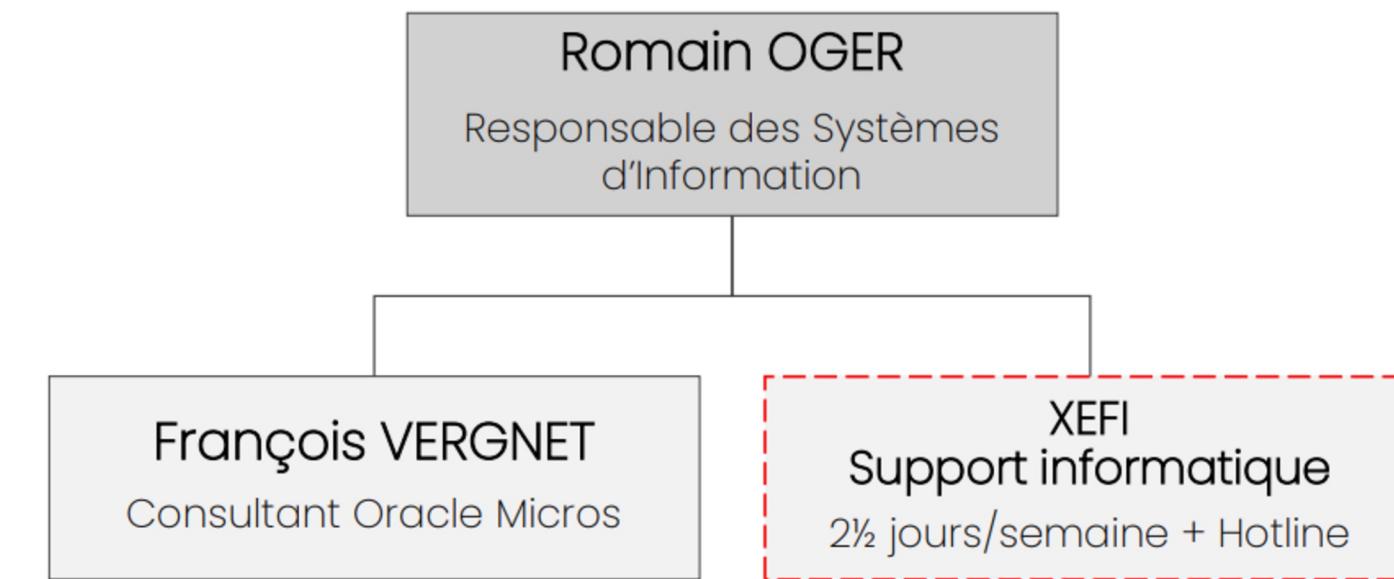
## Équipe IT :

- François Vergnet (systèmes de caisse)
- Aymen Abid (technicien XEFI)
- Clément Farron (RSSI externe)
- Société XEFI (infogérance globale)

## Missions principales :

- Gestion des accès et du réseau
- Support technique (local + distant)
- Sécurisation des données
- Gestion des systèmes de caisses
- Dotation matérielles / Gestion du parc

## Moma Group – Informatique



## Enjeux numériques :

- Sécurité des accès et des mots de passe
- Formalisation des procédures IT
- Harmonisation des pratiques multisites

## III - Les missions

### Contexte du stage

- Réduction d'effectifs après crise sanitaire
- Forte charge liée au support utilisateur
- Procédures internes peu formalisées
- Enjeux croissants de cybersécurité



### Objectifs principaux

- Assurer le support technique (N1/N2 - local et distant)
- Renforcer la sécurité : déploiement MFA, mots de passe
- Participer à la gestion des comptes M365
- Accompagner les stagiaires & rédaction des procédures



# Environnement technique

## Outils utilisés :

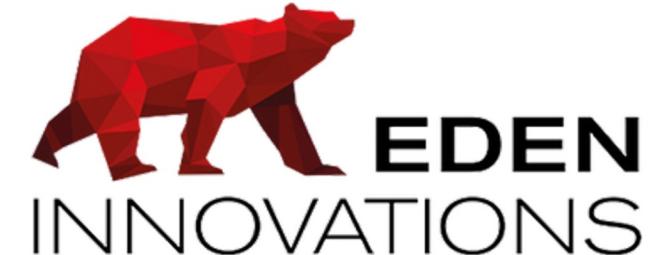
- GLPI : gestion du parc, tickets
- BeyondTrust : prise en main à distance
- Admin365 : gestion des comptes M365
- Active Directory (hébergé chez XEFI)
- Optimabox : contrôle d'accès au siège
- Malwarebytes : antivirus installé sur chaque poste

## Infrastructure externalisée :

- Hébergement serveurs (VPN, AD) chez XEFI Lyon
- Administration par XEFI Ingénierie



Malwarebytes®



# Missions principales réalisées

---

1

## Support et accompagnement

- Assistance utilisateurs local & distant (BeyondTrust)
- Formation de stagiaires (RH & IT)
- Interventions terrain (Manko, Lapérouse)

2

## Sécurité & cybersécurité

- Déploiement MFA + procédure utilisateur
- Renforcement politique de mots de passe

3

## Sensibilisation & pédagogie

- Simulation de phishing avec Mantra
- Modules e-learning + accompagnement

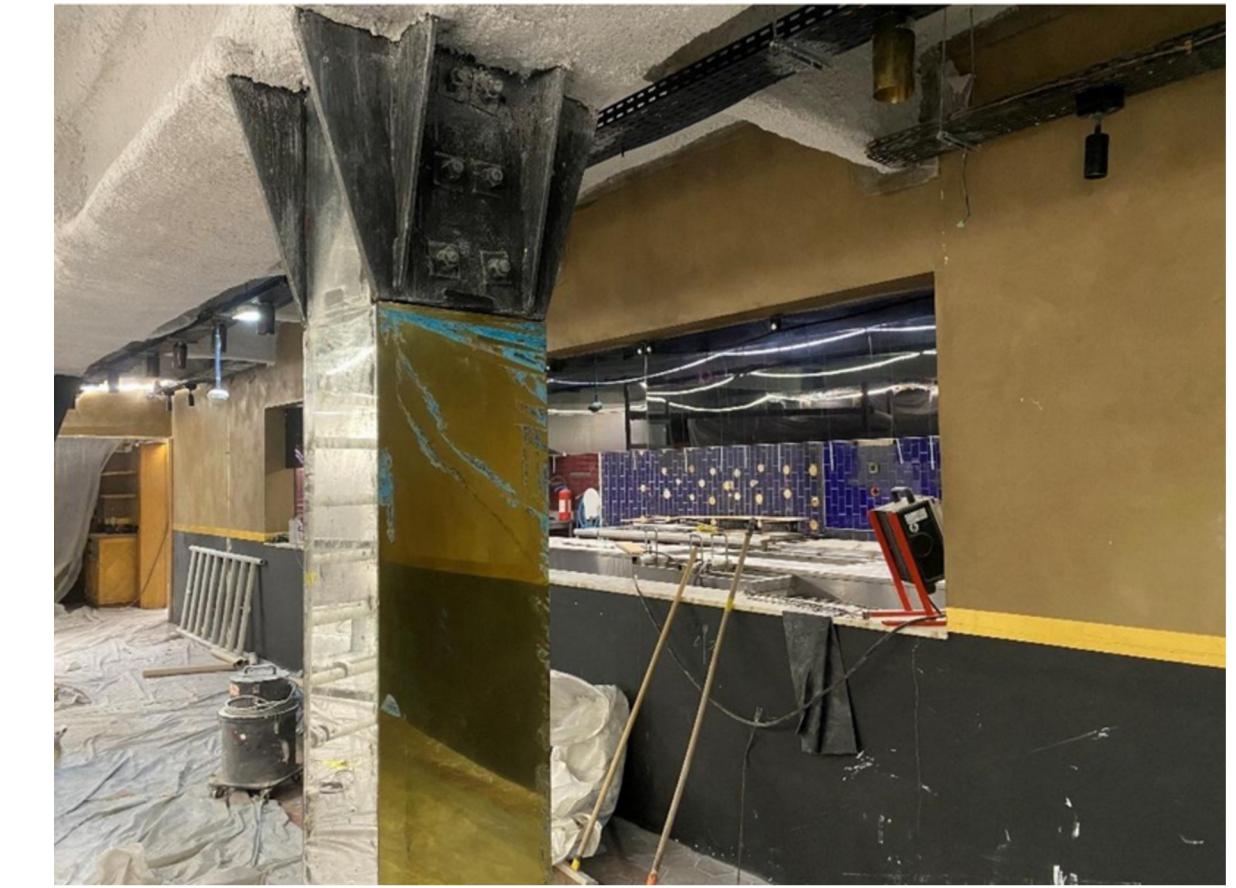
4

## Gestion technique & parc

- Mise à jour de GLPI (matériel, affectations, historiques)
- Tri et destruction des équipements obsolètes (Confia)
- Préparation à la migration vers Windows 11



Restaurant Manko avant



Restaurant Manko après

A screenshot of the Beyond Trust Remote Support interface. On the left, a Microsoft Authenticator setup window is displayed, prompting the user to download the app and set up two-factor authentication. On the right, a log of a support session titled "DESKTOP-EUUTFNO" is shown. The log includes a timestamp of "09:53:30", a message from "Support informatique" asking for a response, and a note that the user has granted full control to the support team. The session details show a "File d'attente" time of 0:02:11 and a "Temps passé dans le système" of 0:02:12. The session is running on a Windows 10 Pro (22H2) system.

Interface Beyond Trust



Baie du Manko a déplacer

## Mise en place de la MFA :

La Direction des Systèmes d'Information renforce la sécurité des comptes Office 365 en activant la fonctionnalité MFA (Authentification Multi-Facteur) qui permet d'ajouter une méthode d'identification supplémentaire lors de la connexion aux comptes Office 365.

Nous vous rappelons ci-dessous vos identifiants Office 365, ainsi que votre mot de passe.  
**Attention le lien pour le mot de passe n'est valide qu'une seule fois, veillez à bien le noter.**

Votre adresse mail :

Votre mot de passe :

Nous activerons la MFA le **mercredi 11 juin**, après ce délai nous l'activerons manuellement (**entrant la déconnexion de vos comptes Office 365**).

- 1) Installation de l'application Microsoft Authenticator

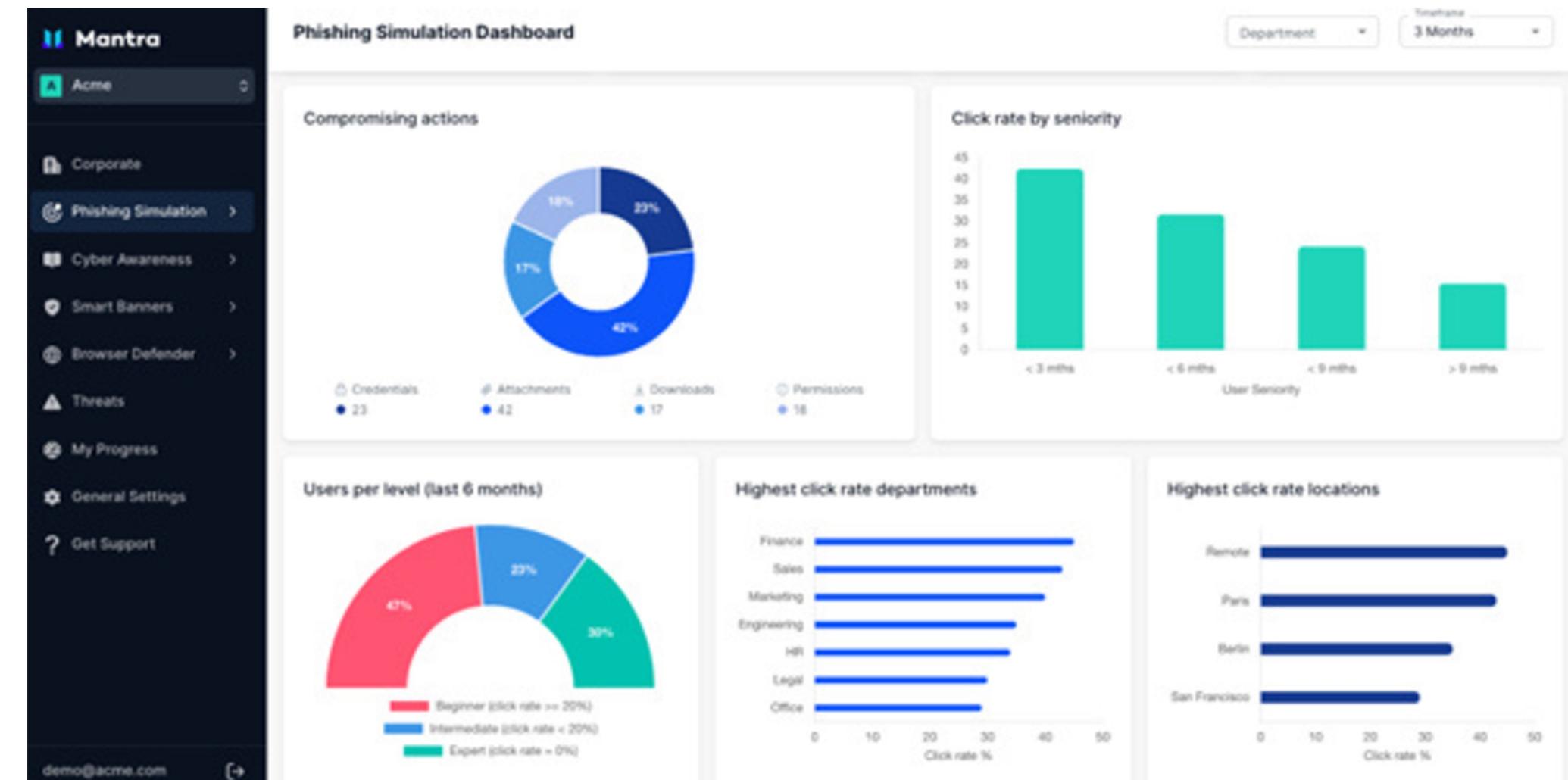
Avant de commencer, téléchargez l'application **Microsoft Authenticator** sur votre smartphone :

- iPhone : [App Store](#)
- Android : Google Play

Installez l'application, mais **n'ouvrez pas de session pour l'instant**.

- 2) Configuration de la MFA

1. Rendez-vous sur le site suivant depuis votre ordinateur : <https://aka.ms/mfasetup>
2. Connectez-vous avec vos identifiants Office 365 (adresse e-mail professionnelle + mot de passe).
3. Cliquez sur « Ajouter une méthode de connexion ».



Interface Mantra MS



Salle de réunion avec ClickShare



Matériels détruits par Confia

# Compétences mobilisées

---

## Réseaux & systèmes

- Lecture d'architecture réseau (AD, DNS, VPN)
- Scripts PowerShell (initiation)

## Cybersécurité

- Déploiement de la MFA
- Renforcement des mots de passe
- Sensibilisation phishing (outil Mantra)

## Communication technique

- Vulgarisation & accompagnement
- Formation stagiaires
- Rédaction de procédures

## IV - Organisation du travail & planning

---

### Organisation par phases

- **Sem. 1-2** : Découverte, outils, prise en main (GLPI, BeyondTrust, M365...)
- **Sem. 3-9** : Projets (MFA, support, phishing, parc...)
- **Fin de stage** : Formation des nouveaux stagiaires, passation

### Rythme hebdomadaire

- Traitement des tickets GLPI
- Réunion IT tous les vendredis
- Déploiement MFA le mercredi
- Campagnes Mantra : 1/mois

# V - Problèmes rencontrés & solutions proposées

## Problèmes identifiés

- Mots de passe stockés en clair (Excel)
- Absence de procédure pour départ des employés
- MFA mal perçue / refusée
- Utilisateurs trop dépendants du support
- Migration Windows 11 à préparer
- Accès VPN : erreurs & dysfonctionnement

## Solutions mises en place

- Sensibilisation + renforcement
- Processus formalisé avec RH + ticket GLPI + feuille de sortie matériel
- Guides simplifiés + rappels + MFA via navigateur (alternative à l'app mobile)
- Accompagnement personnalisé + posture pédagogique pour autonomie
- Outil de vérification compatibilité Win11 + suivi PC
- Support VPN renforcé + tickets prestataire XEFI

# VI - Conclusion

---

## Bilan technique :

- Bonne maîtrise : GLPI, BeyondTrust, Microsoft 365
- Cybersécurité renforcée : MFA, mots de passe, phishing
- Progression en autonomie et diagnostic
- Propositions d'amélioration réalisistes (PRA, cloud, IDS/IPS...)

## Perspectives

- Intérêt confirmé pour la cybersécurité
- Envie de projets plus techniques (réseaux/sécurité)
- Expérience utile pour mon avenir professionnel
- Objectif personnel : passage de la certification CCNA 200-301

## Évolutions personnelles :

- Meilleure gestion du stress & des urgences
- Communication adaptée aux utilisateurs
- Meilleure confiance en moi



# VII - Conclusion en anglais

## Key Learnings :

- Applied technical knowledge in real-world situations
- Strengthened skills in IT support, cybersecurity & internal processes

## Major Contributions :

- Improved password policies
- Deployed multi-factor authentication (MFA)
- Supported users (local & remote)
- Helped formalize IT procedures

## Looking Ahead :

- Strong interest in cybersecurity & network infrastructure
- Preparing for the Cisco CCNA 200-301 certification



Merci pour votre attention !

---

