Implémentation

Sécurisation de l'identité Microsoft Entra (ex Azure AD)

Bénéfices

Améliorer la sécurité de l'identité et renforcer la productivité et l'expérience utilisateur; construire les bases du **modèle Zéro-Trust** dans l'environnement Microsoft.

- Renforcer l'accès aux applications cloud en fonction du contexte de connexion des utilisateurs.
- Fournir une protection en temps réel contre les attaques sur l'identité (phishing, spear phishing, password spray, malicious consent grant).
- Simplifier la gouvernance de l'identité, durcir la sécurité des comptes à privilèges
- Fournir un point d'entrée unique aux utilisateurs pour l'accès aux applications et simplifier l'administration de la plateforme.
- Renforcer la sécurité des accès invités

Comment

- **Définition des usages et contraintes** de connexion des utilisateurs (réseaux de confiance, télétravail, appareils)
- **Design et mise en œuvre des accès conditionnels** (MFA, protocoles hérités, conformité des appareils, périmètre des applications, gestion des connexions et des utilisateurs à risque)
- Implémentation de la **gouvernance des identités** (Privileged Identity Management, mise en œuvre des revues d'accès et des affectations de rôle à privilège)
- **Accompagnement** des **équipes IT** à l'adoption et la maitrise de la solution mise en place
- **Pilote de déploiement** pour 10% de la population d'utilisateur jusqu'à 500 utilisateurs

Livrables

- Document d'architecture général de la plateforme Microsoft Entra
- Référentiel de la configuration technique de la plateforme Microsoft Entra
- Document d'exploitation de la plateforme Microsoft Entra
- Guides utilisateurs