Sécurisation de l'Infrastructure de l'USS Enterprise avec EntraID AD :

Les membres d'équipage, y compris le capitaine, officiers, et ingénieurs, doivent être gérés efficacement et en toute sécurité.

Objectifs :

Renforcer la sécurité avec des politiques avancées.
Automatiser la gestion des utilisateurs et des groupes via PowerShell.
Intégrer et sécuriser des applications.
Détecter et répondre aux incidents de sécurité.

Sécurité Avancée et Politiques de Sécurité

- Mettez en place des politiques pour détecter et bloquer les attaques contre les identités des membres d'équipage.
- Activez MFA pour tous les officiers supérieurs afin de sécuriser l'accès aux données sensibles de Starfleet.
- Créez des politiques d'accès pour restreindre les connexions depuis des emplacements non autorisés comme des planètes non sécurisées ou des vaisseaux inconnus.
- Testez les politiques en simulant des connexions depuis divers secteurs de la galaxie.

Automatisation avec PowerShell

- Créez des scripts pour automatiser la gestion des utilisateurs, , ajouter des nouvelles recrues de Starfleet ou des transferts d'autres vaisseaux.
- Gérez les groupes, comme les équipes d'exploration et les équipes médicales, en automatisant l'ajout et la suppression des membres.
- Appliquez automatiquement les politiques de sécurité pour les missions sensibles.

Intégration et Sécurisation des Applications

- **Intégrer une application SaaS avec Entra ID :**
    - Intégrez des applications essentielles de Starfleet, comme le Journal de Bord (Captain's Log) et le Centre de Commandement (Command Center), avec Azure AD pour un accès sécurisé.
    - Configurez le Single Sign-On (SSO) pour ces applications afin que les membres d'équipage puissent y accéder avec leurs identifiants Starfleet .

- **Ajouter une application personnalisée :**
    - Ajoutez l'application de Gestion des Réparations (Repair Management) utilisée par l'ingénierie.
    - Configurez les rôles et permissions pour l'application, permettant par exemple seulement aux ingénieurs de modifier les données.
    - Testez les accès pour vérifier que les permissions sont correctement appliquées.

Surveillance et Réponse aux Incidents

- Surveillez les tentatives d'accès aux données confidentielles des missions de Starfleet.
- Analysez les logs pour identifier les activités suspectes, comme des accès non autorisés aux plans des moteurs à distorsion.
- Configurez des alertes pour être informé en temps réel des activités anormales, comme des connexions depuis des zones de l'espace non reconnues.
- Simulez des incidents de sécurité, par exemple une tentative de piratage des systèmes du vaisseau, et testez vos procédures de réponse, incluant la réinitialisation des accès et la mise en quarantaine des systèmes compromis.

Rendu

Le projet est à rendre sur : **https://github.com/prenom-nom/ad-enterprise**, pensez à mettre votre repository en **public**.

Vous devez documenter toutes les configurations et scripts, les procédures de tests de fonctionnement, simulation.

L'évaluation se fera sous forme de présentation avec support à l'équipe pédagogique.

Base de connaissances

- Microsoft PowerShell pour Azure AD
- Microsoft Learn - Azure AD
- Microsoft Azure Security Center

Compétences visées

- PowerShell
- Administration système
- Sécurité