Azure AD

SÉCURISATION DE L'INFRASTRUCTURE DE L'USS ENTERPRISE AVEC ENTRAID AD

Sécurité Avancée et Politiques de Sécurité

1. Politiques de Détection et de Blocage des Attaques
   - Surveillance des Identités : Implémenter un système de détection des anomalies pour surveiller les connexions aux comptes des membres d'équipage. Utiliser des outils d'intelligence artificielle pour analyser les comportements et identifier les accès non autorisés.
   - Alertes en Temps Réel : Configurer des alertes instantanées pour les tentatives de connexion suspectes. Cela inclut les échecs répétitifs de connexion et les connexions à partir d'emplacements géographiques atypiques.
   - Bloquer les Adresses IP Suspectes : Établir des listes noires d’adresses IP connues pour être associées à des activités malveillantes. Bloquer automatiquement ces adresses pour protéger les identités.

2. Activation de l'Authentification Multi-Facteurs (MFA)
   - Mise en Œuvre de MFA : Exiger que tous les officiers supérieurs utilisent l'authentification multi-facteurs pour accéder aux systèmes contenant des données sensibles. Cela peut inclure des méthodes comme des codes envoyés par message, des applications d'authentification ou des dispositifs biométriques.
   - Formation à la Sécurité : Organiser des sessions de formation pour sensibiliser les officiers sur l'importance de la MFA et des meilleures pratiques pour gérer leurs identifiants.

3. Politiques d'Accès Restreint

- Définition des Zones de Sécurité : Créer des zones de sécurité géographiques et numériques en fonction des niveaux de risque. Par exemple, restreindre l'accès aux systèmes critiques depuis des planètes non sécurisées ou des vaisseaux inconnus.
- Contrôle d'Accès Basé sur les Rôles (RBAC) : Mettre en place un système de contrôle d'accès basé sur les rôles, où les membres d'équipage n'ont accès qu'aux données et systèmes nécessaires à leur fonction.

4. Tests de Sécurité

- Simulations de Connexions : Effectuer des tests de pénétration réguliers en simulant des connexions depuis divers secteurs de la galaxie, y compris des emplacements connus pour être vulnérables.
- Rapports et Améliorations : Après chaque simulation, générer des rapports détaillés sur les failles de sécurité identifiées et mettre à jour les politiques en conséquence pour corriger les vulnérabilités.

Automatisation avec PowerShell

1. Ajouter une nouvelle recrue à Starfleet

   Pour ajouter un nouvel utilisateur, on peut utiliser le cmdlet New-ADUse :

```
# Paramètres de la nouvelle recrue
$nom = "Jean-Luc Picard"
$prenom = "Jean-Luc"
$username = "jpicard"
$password = "P@ssw0rd"   #respecter les exigences de complexité
$ou = "OU=Starfleet,DC=example,DC=com"   #Remplacer par l'unité d'organisation

# Créer le nouvel utilisateur
New-ADUser -Name $nom -GivenName $prenom -Surname "Picard" `
           -SamAccountName $username -UserPrincipalName "$username@example.com" `
           -Path $ou -AccountPassword (ConvertTo-SecureString $password -AsPlainText -Force) `
           -Enabled $true

Write-Host "Utilisateur $nom ajouté avec succès!"
```

2. Gérer les groupes

Pour ajouter ou supprimer des membres d'un groupe, on peut utiliser les cmdlets Add-ADGroupMember et Remove-ADGroupMember :

Ajouter un membre à un groupe :

```
# Paramètres
$groupe = "EquipesExploration"
$membre = "jpicard"

# Ajouter le membre au groupe
Add-ADGroupMember -Identity $groupe -Members $membre

Write-Host "Membre $membre ajouté au groupe $groupe."
```

Supprimer un membre d'un groupe :

```
# Paramètres
$groupe = "EquipesMedicales"
$membre = "jdoe"

# Supprimer le membre du groupe
Remove-ADGroupMember -Identity $groupe -Members $membre -Confirm:$false

Write-Host "Membre $membre supprimé du groupe $groupe."
```

3. Appliquer des politiques de sécurité

Lier une GPO à une Unité d'Organisation :

Pour appliquer des politiques de sécurité, vous pouvez utiliser des stratégies de groupe (GPO).

```
# Paramètres
$gpoName = "SécuritéMissionSensibles"
$ou = "OU=Starfleet,DC=example,DC=com"

# Lier la GPO à l'unité d'organisation
New-GPLink -Name $gpoName -Target $ou

Write-Host "GPO $gpoName liée à l'OU $ou."
```

Intégration et Sécurisation des Applications

1. Intégration des applications SaaS avec Azure AD

a. Intégration des applications essentielles :

- Accéder au portail Azure :
  - Se connecter au portail Azure avec un compte ayant les droits d’administrateur.
- Créer une nouvelle application d’entreprise :
  - Aller dans "Azure Active Directory" > "Applications d'entreprise" > "Nouvelle application".
  - Rechercher et sélectionner "Journal de Bord" (Captain's Log) et "Centre de Commandement" (Command Center).
- Configurer l’authentification SSO :
  - Dans la section SSO de l’application, choisir le type de SSO (par exemple, SAML ou OIDC selon ce que l'application supporte).
  - Remplir les informations requises comme l'URL de réponse, l'ID d'entité, etc., en fonction de la documentation de l'application.
  - Télécharger le certificat nécessaire si l'application l'exige.
- Ajouter les utilisateurs et groupes :
  - Dans la section "Utilisateurs et groupes", ajouter les membres d'équipage qui auront accès à ces applications.
  - S’assurer de donner accès aux groupes appropriés, par exemple "Équipage - Journal de Bord".

b. Tester l’accès SSO

- Demander à quelques membres d’équipage de se connecter aux applications via le portail d'accès et vérifier que l’authentification SSO fonctionne correctement.

2. Intégration des applications SaaS avec Azure ADAjouter une application personnalisée : Gestion des Réparations

a. Créer l'application personnalisée dans Azure AD :

- Dans "Applications d'entreprise", cliquer sur "Nouvelle application" puis sur "Créer votre propre application".
- Nommer l'application "Gestion des Réparations" et sélectionner "Ajouter une application à partir de zéro".

b. Configurer l'authentification SSO pour l'application :

- Comme pour les applications SaaS, configurer le SSO (SAML, OIDC, etc.) en suivant les étapes nécessaires.

c. Configurer les rôles et permissions :

- Dans la section "Sécurité", on peut définir des rôles personnalisés.
- Créer un rôle "Ingénieur" qui aura la permission de modifier les données de l'application.
- S’assurer que d’autres rôles (comme "Membre d'équipage") n'ont que des permissions de lecture si nécessaire.

d. Attribution des rôles :

- Dans la section "Utilisateurs et groupes", assigner le rôle "Ingénieur" aux utilisateurs appropriés qui sont responsables de la gestion des réparations.

3. Tester les accès et les permissions

a. Valider les connexions :

- Demander à chaque membre d’équipage (ingénieurs et autres) de se connecter à l'application "Gestion des Réparations" et vérifier :
  - Que les ingénieurs peuvent modifier les données.
  - Que les autres utilisateurs peuvent uniquement visualiser les informations sans possibilité de modification.

b. Vérification des journaux d'accès :

- Allez dans "Azure Active Directory" > "Journaux" pour consulter les tentatives de connexion et vérifier que les accès sont conformes aux permissions définies.

Surveillance et Réponse aux Incidents

1. Surveillance des Tentatives d'Accès
   - Objectif : Protéger les données confidentielles des missions de Starfleet.
   - Actions :
     - Déployer des systèmes de surveillance des accès aux bases de données critiques.
     - Utiliser des outils d'analyse de données pour suivre les tentatives d'accès et détecter les patterns anormaux.

2. Analyse des Logs
   - Objectif : Identifier les activités suspectes.
   - Actions :
     - Examiner les logs des systèmes pour repérer des accès non autorisés, en particulier aux plans des moteurs à distorsion.
     - Mettre en place des analyses régulières pour détecter des anomalies, telles que des accès en dehors des heures normales ou depuis des adresses IP suspectes.

3. Configuration des Alertes
   - Objectif : Être informé en temps réel des activités anormales.
   - Actions :
     - Configurer des alertes pour toute connexion suspecte provenant de zones de l'espace non reconnues ou de systèmes étrangers.
     - Utiliser des tableaux de bord en temps réel pour visualiser l'activité réseau et recevoir des notifications instantanées en cas d'incidents.

4. Simulation d'Incidents de Sécurité
   - Objectif : Tester les procédures de réponse aux incidents.
   - Actions :
     - Concevoir des scénarios de simulation tels que des tentatives de piratage des systèmes du vaisseau.
     - Mettre en œuvre des exercices qui incluent :
       - La réinitialisation des accès compromis.
       - La mise en quarantaine des systèmes affectés pour limiter la propagation de l'incident.
       - L'analyse post-incident pour améliorer les procédures et la formation.