Synthèse des Labs EBIOS MegaCorp

# Lab 1 : Analyse EBIOS Express

Réaliser une analyse EBIOS simplifiée de l’Active Directory (AD)

## Étapes

* - Identifier 5 valeurs métier critiques
* - Lister 10 biens supports essentiels
* - Définir 3 scénarios de risque majeurs
* - Évaluer vraisemblance et impact
* - Proposer 5 mesures prioritaires

## Valeurs Métier

* - Authentification des utilisateurs (SSO, accès ERP/CRM)
* - Annuaire d’entreprise (gestion des identités)
* - Continuité des opérations (accès réseau, services)
* - Intégrité des configurations systèmes (GPO, DNS)
* - Traçabilité & conformité (logs, audits AD)

## Biens Supports

* - DC-PARIS-01 (contrôleur principal + FSMO)
* - DC-PARIS-02 (Global Catalog + DNS)
* - DC-LYON-01 (DHCP + AD)
* - DC-LILLE-01 (R&D + DNS)
* - DNS intégré à l’AD
* - Base NTDS.dit
* - GPO « Server-Security-Baseline »
* - Comptes Domain Admins
* - SQL-PARIS-01 (ERP, CRM)
* - MONITOR-PARIS-01 (monitoring)

## Scénarios de Risque

* - Compromission d’un compte « Domain Admin »
* - Attaque de ransomware via GPO modifiée
* - Altération de la réplication AD

## Mesures Prioritaires

* - Mise en œuvre de l’authentification MFA
* - Revue des délégations AD
* - Surveillance active via SCOM
* - Segmentation réseau des DC
* - Test mensuel de restauration AD

# Lab 2 : Matrice de Risque AD

Construire votre matrice de risque spécifique

## Étapes

* - Utiliser le template fourni
* - Placer vos scénarios identifiés
* - Ajuster selon votre contexte
* - Identifier zones rouges
* - Prioriser les actions

## Zones Critiques

* - Compromission Admin → Zone critique (rouge)
* - GPO détournée → Zone haute (orange)
* - Réplication AD dégradée → Zone moyenne (jaune)

## Contexte

* - Fonctionnement 24/7
* - Maintenance limitée
* - Services externalisés

## Actions Prioritaires

* - MFA
* - SIEM avancé
* - Segmentation réseau
* - Suppression comptes inactifs
* - Révision mots de passe

# Lab 3 : Plan d'Action

Créer une roadmap de sécurisation AD

## Étapes

* - Partir des risques identifiés
* - Définir mesures court terme
* - Planifier actions long terme
* - Estimer efforts et coûts
* - Créer planning projet

## Mesures Court Terme

* - Revue des droits Domain Admins
* - Application GPO de baseline
* - Activation logs avancés

## Actions Long Terme

* - Mise en place d’un PAM
* - Migration partielle vers Azure AD
* - Réécriture des scripts de maintenance

## Planning Projet

* - Phase 1 (1 mois) : quick wins
* - Phase 2 (3 mois) : durcissement GPO
* - Phase 3 (6 mois) : PAM + refonte AD