

Etude de cas EBIOS AD

Par Anthony Mvakanga, Tom Bazire et Guillaume Sanchez.

Nous avons réalisé cette étude en nous basant sur la mise en application de la méthode, présente dans le document “2025 06 13 - partie III - SEC101 - Ebios et AD.pdf”.

Cette méthode se décompose en 3 point principaux : L’analyse EBIOS Express, la matrice de risque AD et le plan d’action.

Analyse EBIOS Express

L’Objectif de cette analyse est de réaliser une analyse EBIOS simplifiée de l’Active Directory. On commence par identifier 5 valeurs métiers critiques :

- 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).

Ensuite, nous avons recensé 10 biens supports essentiels présent dans cette AD :

- DC-PARIS-01 qui sont le contrôleur principal et le FSMO.
- DC-PARIS-02 qui ont le catalogue global et les serveur DNS.
- DC-LYON-01 qui ont les serveurs DHCP et d’Active Directory
- DC-LILLE-01 car ils ont pour mission la recherche et développement et les serveur DNS.
- Les DNS intégré à l’AD.
- Base “NTDS.dit” qui est contenu dans l’annuaire.
- GPO « Server-Security-Baseline »
- Les comptes “Domain Admins”
- SQL-PARIS-01 (ERP, CRM)
- MONITOR-PARIS-01 pour les outils de monitoring

À partir de toutes ces informations, nous avons défini 3 scénarios de risque majeurs.

- Le premier scénario serait la compromission d’un compte du “Domain Admin”. Il aurait comme impacte 5 et comme vraisemblance 4.
- Le second scénario, une attaque de ransomware depuis la GPO qui serait modifié. Il aurait comme impacte 4 et comme vraisemblance 3.

- Le troisième pourrait-être une altération de la réplication de l'AD donc un problème de communication entre différents sites. Il aurait comme impacte 3 et comme vraisemblance 2.

Pour prévenir c'est éventuelle scénario, nous avons retenu c'est 5 mesures prioritaires:

- Mise en œuvre de l'authentification MFA pour les comptes privilégiés
- Revue des délégations AD et durcissement des GPO
- Surveillance active via SCOM (alertes critiques AD)
- Segmentation réseau des DC (VLAN Management)
- Test mensuel de restauration AD (System State)

Matrice de Risque AD

L'objectif est de construire une matrice de risque spécifique au scénario que nous avons répertorier.

Pour rappel, les scénarios possibles sont la compromission Admin qui est une zone critique (rouge), le GPO détournée qui est une zone haute (orange) et la réplication de l'AD dégradée qui est une zone moyenne (jaune).

Nous avons pris en compte plusieurs contraintes dans cette AD. Son fonctionnement 24/7 sur les sites critiques, une maintenance limitée qui impacte les mesures applicables et les services externalisés.

Les zones rouges sont la compromission de comptes à privilèges et l'absence de logs fiables sur événements critiques.

Les actions à réaliser dans ce cas-là, mettre en place l'authentification multifacteur une surveillance avancée avec SIEM, cloisonnement de l'AD. Il faut également supprimer les comptes inactifs et faire régulièrement une révision de mots de passe.

Plan d'Action

L'objectif de ce plan d'action est de créer une roadmap de sécurisation AD.

Si on part des risques comme la compromission comptes, la propagation via GPO et les attaque persistante (APT), on peut définir les mesures à court terme et à long terme suivante :

- Mesures court terme :
 - o Revue immédiate des droits Domain Admins
 - o Application GPO de baseline sur tous les DC
 - o Activation logs avancés sur MONITOR-PARIS-01
- Mesure long terme :
 - o Mise en place d'un PAM (Privileged Access Management)
 - o Migration partielle vers Azure AD + segmentation

- Réécriture des scripts de maintenance et surveillance

Voici une estimation des efforts et des coûts :

- Pour la mise en place d'une MFA (l'authentification multi facteur) : faible coût / impact fort
- PAM : effort élevé / **ROI** sécurité important
- Surveillance : moyen coût / gain visibilité élevé

Pour mettre en place ces mesures, j'ai pensé qu'on pourrait procéder ainsi :

- Phase 1 (1 mois) : mesures urgentes / quick wins
- Phase 2 (3 mois) : surveillance et durcissement GPO
- Phase 3 (6 mois) : PAM + restructuration AD