

2024  
2025

# Atelier n°2 EBIOS RM & Microsoft Active Directory

SEC101 – CYBERSÉCURITÉ : RÉFÉRENTIEL, OBJECTIFS ET  
DÉPLOIEMENT  
STÉPHANE LARCHER

## Atelier EBIOS Risk Manager AD MegaCorp

# Atelier d'Analyse EBIOS Risk Manager Infrastructure Active Directory MegaCorp

## Table des matières

<b>Description Technique Complète .....</b>	<b>3</b>
<b>Profil Entreprise.....</b>	<b>3</b>
<b>Sites Français (Périmètre d'étude).....</b>	<b>3</b>
<b>Architecture Active Directory .....</b>	<b>3</b>
Structure de Forêt et Domaines .....	3
Topologie des Sites AD .....	4
Configuration de Réplication .....	4
<b>Structure Organisationnelle .....</b>	<b>6</b>
Hiérarchie des Unités Organisationnelles .....	6
Stratégies de Groupe (GPO) .....	8
<b>Population et Comptes .....</b>	<b>8</b>
Statistiques Générales .....	8
Types de Comptes.....	8
Groupes de Sécurité.....	9
<b>Infrastructure Serveurs.....</b>	<b>10</b>
Contrôleurs de Domaine .....	10
Serveurs Applicatifs .....	11
<b>Services et Applications.....</b>	<b>12</b>
Services Active Directory .....	12
Applications Métier .....	13
Infrastructure de Partage.....	14
<b>Configuration Réseau .....</b>	<b>15</b>
Architecture Réseau .....	15
Routage et Connectivité .....	16

<b>Sauvegarde et Haute Disponibilité .....</b>	<b>16</b>
Stratégie de Sauvegarde .....	16
Haute Disponibilité .....	17
<b>Monitoring et Administration.....</b>	<b>17</b>
Outils d'Administration .....	17
Surveillance et Alertes.....	18
<b>Conformité et Sécurité.....</b>	<b>19</b>
Politiques de Sécurité Appliquées .....	19
Rôles et Délégations .....	19
<b>Annexes Techniques .....</b>	<b>20</b>
Schéma de Réplication .....	20
Mapping des Services.....	20
<b><i>Atelier d'Analyse EBIOS Risk Manager.....</i></b>	<b>22</b>
<b>Contexte de la Mission.....</b>	<b>22</b>
Rappel : Présentation de MegaCorp International .....	22
<b>Méthodologie EBIOS Risk Manager .....</b>	<b>22</b>
Atelier 1 : Cadrage et Socle de Sécurité .....	22
Atelier 2 : Sources de Risque .....	24
Atelier 3 : Scénarios Stratégiques .....	24
Atelier 4 : Scénarios Opérationnels .....	25
Atelier 5 : Traitement du Risque .....	26
<b>Livrables Attendus .....</b>	<b>27</b>
1. Rapport d'Analyse EBIOS .....	27
2. Templates de Restitution.....	27
<b>Méthodes d'Investigation .....</b>	<b>27</b>
Outils d'Analyse Recommandés.....	27
Points d'Attention Spécifiques AD .....	28
<b>Contraintes et Considérations .....</b>	<b>28</b>
Contraintes Métier .....	28
Contraintes Techniques .....	29
<b>Questions Guides .....</b>	<b>29</b>

# Description Technique Complète

## Profil Entreprise

### MegaCorp International

- i. **Secteur d'activité** : Services technologiques et conseil
- ii. **Taille** : 10 000 employés dans le monde
- iii. **Chiffre d'affaires** : 2,5 milliards d'euros
- iv. **Implantation** : 15 sites internationaux, 3 sites principaux en France

## Sites Français (Périmètre d'étude)

### Paris-HQ (Siège Social)

- i. 3 500 employés
- ii. Fonctions : Direction, Finance, RH, IT Corporate
- iii. Bâtiments : Tour MegaCorp (32 étages)

### Lyon-Production

- i. 1 200 employés
- ii. Fonctions : Production, Qualité, Logistique
- iii. Site industriel de 50 000 m<sup>2</sup>

### Lille-RD (Recherche & Développement)

- i. 800 employés
- ii. Fonctions : R&D, Innovation, Laboratoires
- iii. Campus technologique de 25 000 m<sup>2</sup>

## Architecture Active Directory

### Structure de Forêt et Domaines

**Forêt principale** : megacorp.com

- i. **Niveau fonctionnel** : Windows Server 2016
- ii. **Schéma AD** : Version standard avec extensions Microsoft Exchange
- iii. **Mode de forêt** : Mode natif Windows Server 2016

**Domaine principal d'étude** : corp.megacorp.fr

- i. **Niveau fonctionnel domaine** : Windows Server 2016

- ii. **Mode domaine** : Mode natif Windows Server 2016
- iii. **FSMO Roles** : Centralisés sur le site Paris

## Topologie des Sites AD

### *Site Paris-HQ*

- i. **Réseaux associés :**
  - a. 192.168.1.0/24 (Réseau production principal)
  - b. 192.168.4.0/24 (Réseau développement et tests)
- ii. **Contrôleurs de domaine :**
  - a. DC-PARIS-01 (Windows Server 2019)
  - b. DC-PARIS-02 (Windows Server 2019)
  - c. DC-PARIS-03 (Windows Server 2016)
- iii. **Services hébergés :**
  - a. DNS intégré Active Directory
  - b. DHCP pour les réseaux locaux
  - c. Catalogue Global
  - d. Tous les rôles FSMO

### *Site Lyon-Production*

- i. **Réseau associé :**
  - a. 192.168.2.0/24
- ii. **Contrôleurs de domaine :**
  - a. DC-LYON-01 (Windows Server 2019)
  - b. DC-LYON-02 (Windows Server 2016)
- iii. **Services hébergés :**
  - a. DNS intégré (réplication)
  - b. DHCP local
  - c. Catalogue Global (DC-LYON-01)

### *Site Lille-RD*

- i. **Réseau associé :**
  - a. 192.168.3.0/24
- ii. **Contrôleurs de domaine :**
  - a. DC-LILLE-01 (Windows Server 2019)
- iii. **Services hébergés :**
  - a. DNS intégré (réplication)
  - b. DHCP local

## Configuration de Réplication

- i. **Liens de sites configurés :**

Liaison	Coût	Fréquence	Fenêtre	Protocole
Paris ↔ Lyon	10	15 minutes	24/7	IP
Paris ↔ Lille	20	30 minutes	24/7	IP
Lyon ↔ Lille	50	60 minutes	24/7	IP

**ii. Partitions de réplication :**

- a. Schema : Réplication forest-wide
- b. Configuration : Réplication forest-wide
- c. Domain : Réplication domain-wide
- d. Global Catalog : Réplication selective

## Structure Organisationnelle

### Hiérarchie des Unités Organisationnelles

DC=corp,DC=megacorp,DC=fr

- └─ OU=MegaCorp
  - └─ OU=Paris
    - └─ OU=Direction
      - └─ OU=Comite\_Direction
      - └─ OU=Direction\_Generale
      - └─ OU=Conseil\_Administration
    - └─ OU=Finance
      - └─ OU=Comptabilite
      - └─ OU=Controle\_Gestion
      - └─ OU=Tresorerie
    - └─ OU=RH
      - └─ OU=Recrutement
      - └─ OU=Formation
      - └─ OU=Paie
    - └─ OU=IT
      - └─ OU=Infrastructure
      - └─ OU=Developpement
      - └─ OU=Support
      - └─ OU=Securite
  - └─ OU=Lyon
    - └─ OU=Production
      - └─ OU=Chaine\_1
      - └─ OU=Chaine\_2
      - └─ OU=Maintenance
    - └─ OU=Qualite
      - └─ OU=Controle\_Qualite
      - └─ OU=Certification
      - └─ OU=Tests
    - └─ OU=Logistique
      - └─ OU=Approvisionnement
      - └─ OU=Stock
      - └─ OU=Expedition
  - └─ OU=Lille
    - └─ OU=RD
      - └─ OU=Recherche\_Fondamentale
      - └─ OU=Developpement\_Produit
      - └─ OU=Prototypage
    - └─ OU=Innovation
      - └─ OU=Projets\_Innovation
      - └─ OU=Partenariats
      - └─ OU=Veille\_Techno
    - └─ OU=Labs
      - └─ OU=Lab\_Materiaux
      - └─ OU=Lab\_Electronique
      - └─ OU=Lab\_Logiciel
  - └─ OU=Comptes\_Service
    - └─ OU=Services\_Infrastructure
    - └─ OU=Services\_Application
    - └─ OU=Services\_Metier
- └─ OU=Ressources
  - └─ OU=Groupes
    - └─ OU=Groupes\_Securite
    - └─ OU=Groupes\_Distribution
    - └─ OU=Groupes\_Application
  - └─ OU=Partages
    - └─ OU=Partages\_Publics
    - └─ OU=Partages\_Departement
    - └─ OU=Partages\_Projet



## Stratégies de Groupe (GPO)

### GPO organisationnelles principales :

Nom GPO	Scope d'application	Description
Default Domain Policy	Domaine entier	Politiques de base domaine
Default Domain Controllers Policy	DC OU	Politiques contrôleurs de domaine
Paris-Desktop-Settings	OU=Paris	Configuration postes Paris
Lyon-Production-Settings	OU=Lyon	Configuration postes Lyon
Lille-RD-Settings	OU=Lille	Configuration postes Lille
Server-Security-Baseline	Serveurs	Baseline sécurité serveurs
Workstation-Security-Baseline	Postes	Baseline sécurité postes
IT-Admin-Settings	OU=IT	Configuration équipes IT

## Population et Comptes

### Statistiques Générales

- i. **Comptes utilisateurs :**
  - a. **Total** : 8 542 comptes utilisateurs
  - b. **Actifs** : 8 495 comptes
  - c. **Désactivés** : 47 comptes
- ii. **Répartition géographique :**
  - a. Paris : 3 500 comptes
  - b. Lyon : 1 200 comptes
  - c. Lille : 800 comptes
  - d. Autres sites : 2 995 comptes

## Types de Comptes

### Comptes Utilisateurs Standards

- i. **Répartition par fonction :**

Département	Nombre de comptes	Description
Direction	25	Direction générale et comités
Finance	180	Comptabilité, contrôle, trésorerie
RH	85	Ressources humaines, paie
IT	120	Informatique et sécurité
Production	450	Opérateurs et techniciens
Qualité	95	Contrôle et certification
Logistique	140	Supply chain et expédition

<b>R&amp;D</b>	280	Recherche et innovation
<b>Labs</b>	125	Laboratoires spécialisés
<b>Support</b>	200	Support client et maintenance
<b>Autres</b>	6 990	Autres départements et sites

#### Comptes Administratifs

##### i. Hiérarchie administrative :

Niveau	Groupe AD	Nombre	Scope
Niveau 0	Domain Admins	5	Domaine complet
Niveau 0	Enterprise Admins	3	Forêt complète
Niveau 1	Server Operators	12	Serveurs
Niveau 1	IT_Site_Admins	8	Administration sites
Niveau 2	Helpdesk_Level1	15	Support niveau 1
Niveau 2	Helpdesk_Level2	8	Support niveau 2

#### Comptes de Service

##### i. Répartition par type :

Type de service	Nombre	Exemples d'utilisation
Services Infrastructure	45	DNS, DHCP, Backup, Monitoring
Services Base de Données	25	SQL Server, Oracle, MySQL
Services Web	30	IIS, Apache, Applications web
Services Applicatifs	80	ERP, CRM, Applications métier
Services Sécurité	15	Antivirus, SIEM, PKI
Services Réseau	20	Routeurs, Switches, Firewalls
<b>Total</b>	<b>215</b>	<b>Total comptes de service</b>

#### Groupes de Sécurité

##### Groupes Privilégiés par Défaut

Groupe	Type	Scope	Membres	Description
<b>Domain Admins</b>	Global	Domaine	5	Administration complète domaine
<b>Enterprise Admins</b>	Universal	Forêt	3	Administration complète forêt
<b>Schema Admins</b>	Universal	Forêt	2	Modification du schéma
<b>Backup Operators</b>	Builtin	Local	8	Opérations de sauvegarde
<b>Account Operators</b>	Builtin	Local	6	Gestion des comptes
<b>Server Operators</b>	Builtin	Local	12	Gestion des serveurs
<b>Print Operators</b>	Builtin	Local	4	Gestion des imprimantes

## Groupes Métier Personnalisés

Département	Groupes principaux	Membres approx.
Finance	GRP_Finance_RW, GRP_Finance_RO, GRP_Comptabilite	180
RH	GRP_RH_Full, GRP_RH_Paie, GRP_RH_Recrutement	85
Production	GRP_Production_Ops, GRP_Production_Maint	450
R&D	GRP_RD_Chercheurs, GRP_RD_Labs, GRP_RD_Projets	405
IT	GRP_IT_Infrastructure, GRP_IT_Dev, GRP_IT_Security	120

## Infrastructure Serveurs

### Contrôleurs de Domaine

#### Site Paris-HQ

##### i. DC-PARIS-01

- a. **OS** : Windows Server 2019 Datacenter
- b. **Rôles** : PDC Emulator, RID Master, Infrastructure Master
- c. **CPU** : 8 vCPU
- d. **RAM** : 16 GB
- e. **Stockage** : 500 GB SSD
- f. **IP** : 192.168.1.10

##### ii. DC-PARIS-02

- a. **OS** : Windows Server 2019 Standard
- b. **Rôles** : Global Catalog, DNS
- c. **CPU** : 6 vCPU
- d. **RAM** : 12 GB
- e. **Stockage** : 300 GB SSD
- f. **IP** : 192.168.1.11

##### iii. DC-PARIS-03

- a. **OS** : Windows Server 2016 Standard
- b. **Rôles** : DNS, Backup DC
- c. **CPU** : 4 vCPU
- d. **RAM** : 8 GB
- e. **Stockage** : 250 GB SSD
- f. **IP** : 192.168.1.12

#### Site Lyon-Production

##### i. DC-LYON-01

- a. **OS** : Windows Server 2019 Standard

- b. **Rôles** : Global Catalog, DNS, DHCP
  - c. **CPU** : 6 vCPU
  - d. **RAM** : 12 GB
  - e. **Stockage** : 300 GB SSD
  - f. **IP** : 192.168.2.10
- ii. **DC-LYON-02**
  - a. **OS** : Windows Server 2016 Standard
  - b. **Rôles** : DNS, Backup DC
  - c. **CPU** : 4 vCPU
  - d. **RAM** : 8 GB
  - e. **Stockage** : 250 GB SSD
  - f. **IP** : 192.168.2.11

#### *Site Lille-RD*

- i. **DC-LILLE-01**
  - a. **OS** : Windows Server 2019 Standard
  - b. **Rôles** : DNS, DHCP
  - c. **CPU** : 4 vCPU
  - d. **RAM** : 8 GB
  - e. **Stockage** : 250 GB SSD
  - f. **IP** : 192.168.3.10

### Serveurs Applicatifs

#### *Serveurs Base de Données*

- i. **SQL-PARIS-01**
  - a. **OS** : Windows Server 2019 Datacenter
  - b. **Application** : SQL Server 2019 Enterprise
  - c. **Bases** : ERP, CRM, RH
  - d. **CPU** : 16 vCPU
  - e. **RAM** : 64 GB
  - f. **Stockage** : 2 TB SSD
  - g. **IP** : 192.168.1.50
- ii. **SQL-LILLE-01**
  - a. **OS** : Windows Server 2019 Standard
  - b. **Application** : SQL Server 2019 Standard
  - c. **Bases** : R&D, Labs, Projets
  - d. **CPU** : 8 vCPU
  - e. **RAM** : 32 GB
  - f. **Stockage** : 1 TB SSD
  - g. **IP** : 192.168.3.50

## *Serveurs Web*

### **i. WEB-PARIS-01**

- a. **OS** : Windows Server 2019 Standard
- b. **Application** : IIS 10.0
- c. **Sites** : intranet.megacorp.fr
- d. **CPU** : 8 vCPU
- e. **RAM** : 16 GB
- f. **Stockage** : 500 GB SSD
- g. **IP** : 192.168.1.80

### **ii. WEB-PARIS-02**

- a. **OS** : Windows Server 2019 Standard
- b. **Application** : IIS 10.0
- c. **Sites** : reports.megacorp.fr
- d. **CPU** : 6 vCPU
- e. **RAM** : 12 GB
- f. **Stockage** : 300 GB SSD
- g. **IP** : 192.168.1.81

## *Serveurs Infrastructure*

### **i. BACKUP-PARIS-01**

- a. **OS** : Windows Server 2019 Datacenter
- b. **Application** : System Center DPM 2019
- c. **CPU** : 8 vCPU
- d. **RAM** : 32 GB
- e. **Stockage** : 10 TB HDD
- f. **IP** : 192.168.1.100

### **ii. MONITOR-PARIS-01**

- a. **OS** : Windows Server 2019 Standard
- b. **Application** : System Center SCOM 2019
- c. **CPU** : 6 vCPU
- d. **RAM** : 16 GB
- e. **Stockage** : 500 GB SSD
- f. **IP** : 192.168.1.110

## *Services et Applications*

### *Services Active Directory*

#### *Services DNS*

### **i. Configuration DNS intégrée AD :**

- a. **Zones principales** : corp.megacorp.fr, megacorp.fr

- b. **Zones de recherche inversée** : 192.168.1.x, 192.168.2.x, 192.168.3.x
  - c. **Forwarders** : 8.8.8.8, 8.8.4.4
  - d. **Scavenging** : Activé (7 jours)
  - e. **Réplication** : Tous les DNS dans la forêt
- ii. **Enregistrements critiques** :
  - a. \_ldap.\_tcp.corp.megacorp.fr
  - \_kerberos.\_tcp.corp.megacorp.fr
  - \_gc.\_tcp.corp.megacorp.fr
  - \_kpasswd.\_tcp.corp.megacorp.fr

## Services DHCP

- i. **Étendues configurées** :

Site	Étendue	Plage IP	Passerelle	DNS
Paris	Production	192.168.1.100-200	192.168.1.1	192.168.1.10,11
Paris	Dev	192.168.4.100-150	192.168.4.1	192.168.1.10,11
Lyon	Production	192.168.2.100-200	192.168.2.1	192.168.2.10,11
Lille	R&D	192.168.3.100-150	192.168.3.1	192.168.3.10

## Applications Métier

### ERP (Enterprise Resource Planning)

- i. **SAP ECC 6.0**
  - a. **Serveur** : SQL-PARIS-01
  - b. **Base de données** : SQL Server 2019
  - c. **Utilisateurs** : 2 500 comptes
  - d. **Modules** : Finance, Ventes, Achats, Production
  - e. **Authentification** : Intégrée Active Directory

### CRM (Customer Relationship Management)

- i. **Microsoft Dynamics 365**
- ii. **Déploiement** : Hybrid (Cloud + On-premise)
- iii. **Serveur local** : SQL-PARIS-01
- iv. **Utilisateurs** : 800 comptes
- v. **Authentification** : ADFS + Azure AD

### Système RH

- i. **SAP SuccessFactors**
- ii. **Déploiement** : Cloud avec connector AD
- iii. **Synchronisation** : Azure AD Connect

- iv. **Utilisateurs** : 1 200 comptes RH
- v. **Modules** : Paie, Recrutement, Formation

## Infrastructure de Partage

### *Partages Principaux*

- i. **\DC-PARIS-01\Public**
  - a. **Description** : Partage public pour documents généraux
  - b. **Taille** : 500 GB
  - c. **Utilisateurs** : Tous les employés
  - d. **Contenu** : Procédures, templates, communications
- ii. **\DC-PARIS-01\Finance**
  - a. **Description** : Partage département Finance
  - b. **Taille** : 2 TB
  - c. **Utilisateurs** : Groupe GRP\_Finance\_RW
  - d. **Contenu** : Documents financiers, budgets, reportings
- iii. **\DC-PARIS-01\IT**
  - a. **Description** : Partage département IT
  - b. **Taille** : 1 TB
  - c. **Utilisateurs** : Groupe GRP\_IT\_Infrastructure
  - d. **Contenu** : Scripts, outils, documentation technique
- iv. **\DC-PARIS-01\Backups**
  - a. **Description** : Partage pour sauvegardes
  - b. **Taille** : 5 TB
  - c. **Utilisateurs** : Groupe Backup Operators
  - d. **Contenu** : Sauvegardes système et applications

## Structure des Partages

```
\\DC-PARIS-01\  
├── Public\  
│   ├── Procedures\  
│   ├── Templates\  
│   └── Communications\  
├── Finance\  
│   ├── Budget\  
│   ├── Comptabilite\  
│   └── Reporting\  
├── IT\  
│   ├── Scripts\  
│   ├── Tools\  
│   └── Documentation\  
├── RH\  
│   ├── Recrutement\  
│   ├── Formation\  
│   └── Procedures\  
└── Backups\  
    ├── SystemState\  
    ├── Applications\  
    └── UserData
```

## Configuration Réseau

### Architecture Réseau

#### VLAN et Segmentation

VLAN ID	Nom	Réseau	Description
10	VLAN-Servers	192.168.1.0/25	Serveurs infrastructure
20	VLAN-Users-Paris	192.168.1.128/25	Postes utilisateurs Paris
30	VLAN-Dev	192.168.4.0/24	Environnement développement
40	VLAN-Lyon-Prod	192.168.2.0/24	Site Lyon
50	VLAN-Lille-RD	192.168.3.0/24	Site Lille
99	VLAN-Management	192.168.254.0/24	Management équipements

#### Ports et Protocoles

##### i. Ports Active Directory standard :

Service	Port	Protocole	Description
LDAP	389	TCP	Requêtes LDAP non chiffrées
LDAPS	636	TCP	LDAP over SSL



<b>Global Catalog</b>	3268	TCP	Catalogue global
<b>Global Catalog SSL</b>	3269	TCP	Catalogue global SSL
<b>Kerberos</b>	88	TCP/UDP	Authentification Kerberos
<b>DNS</b>	53	TCP/UDP	Résolution DNS
<b>RPC Endpoint Mapper</b>	135	TCP	RPC dynamique
<b>SMB</b>	445	TCP	Partages de fichiers
<b>NetBIOS</b>	139	TCP	Legacy NetBIOS

## Routage et Connectivité

### *Liens WAN entre Sites*

Liaison	Type	Bande passante	Latence	Provider
<b>Paris-Lyon</b>	MPLS	100 Mbps	5ms	Orange Business
<b>Paris-Lille</b>	MPLS	50 Mbps	8ms	Orange Business
<b>Lyon-Lille</b>	MPLS	20 Mbps	12ms	Orange Business

### *Accès Internet*

- i. **Paris** : Fibre dédiée 1 Gbps (Orange Pro)
- ii. **Lyon** : Fibre dédiée 500 Mbps (SFR Business)
- iii. **Lille** : Fibre dédiée 200 Mbps (Orange Pro)

## Sauvegarde et Haute Disponibilité

### Stratégie de Sauvegarde

#### *Active Directory*

- i. **System State Backup** :
  - a. **Fréquence** : Quotidienne
  - b. **Rétention** : 30 jours local, 1 an externalisé
  - c. **Stockage** : \BACKUP-PARIS-01\SystemState\
  - d. **Test de restauration** : Mensuel
- ii. **Sauvegarde NTDS.dit** :
  - a. **Méthode** : Snapshot VSS
  - b. **Fréquence** : 4 fois par jour
  - c. **Rétention** : 7 jours local
  - d. **Stockage** : Stockage SAN dédié

#### *Applications et Données*

- i. **Bases de données** :
  - a. **SQL Server** : Sauvegarde complète quotidienne + logs horaires
  - b. **ERP/CRM** : Sauvegarde applicative quotidienne
  - c. **Rétention** : 3 mois local, 2 ans externalisé

## Haute Disponibilité

### *Contrôleurs de Domaine*

- i. **Répartition des rôles FSMO :**
  - a. **PDC Emulator** : DC-PARIS-01
  - b. **RID Master** : DC-PARIS-01
  - c. **Infrastructure Master** : DC-PARIS-02
  - d. **Schema Master** : DC-PARIS-01
  - e. **Domain Naming Master** : DC-PARIS-01
  - f. **Redondance par site :**
  - g. **Paris** : 3 DC actifs
  - h. **Lyon** : 2 DC actifs
  - i. **Lille** : 1 DC actif

### *Services Critiques*

- i. **DNS :**
  - a. Redondance sur tous les DC
  - b. Cache DNS local sur chaque site
  - c. Forwarders multiples configurés
- ii. **DHCP :**
  - a. Redondance par site
  - b. Failover automatique 80/20

## Monitoring et Administration

### Outils d'Administration

#### *Consoles Centralisées*

- i. **Active Directory Administrative Center**
  - a. Installé sur : Postes d'administration IT
  - b. Utilisateurs : Groupe IT\_Admins
  - c. Fonctions : Gestion quotidienne AD
- ii. **Group Policy Management Console**
  - a. Installé sur : DC et postes IT
  - b. Utilisateurs : Groupe GPO\_Admins
  - c. Fonctions : Gestion des stratégies de groupe
- iii. **DNS Manager**
  - a. Installé sur : Tous les DC
  - b. Utilisateurs : Groupe DNS\_Admins
  - c. Fonctions : Gestion DNS intégrée

## *Scripts d'Administration*

- i. PowerShell DSC**
  - a. Configuration serveurs standardisée
  - b. Déploiement automatisé
  - c. Vérification de conformité
- ii. Scripts de maintenance**
  - a. Nettoyage des comptes inactifs
  - b. Rapports d'audit automatiques
  - c. Monitoring de la réplication

## *Surveillance et Alertes*

### *System Center Operations Manager*

- i. Serveur : MONITOR-PARIS-01 Packs de surveillance :**
  - a. Active Directory Management Pack
  - b. Windows Server Management Pack
  - c. SQL Server Management Pack
  - d. Network Device Management Pack
- ii. Alertes configurées :**
  - a. Échecs de réplication AD
  - b. Erreurs d'authentification
  - c. Espace disque DC critique
  - d. Services AD arrêtés

### *Logs et Audit*

- i. Event Log Forwarding :**
  - a. Centralisation sur MONITOR-PARIS-01
  - b. Rétention : 6 mois
  - c. Filtrage par criticité
- ii. Logs Active Directory :**
  - a. Directory Service
  - b. DNS Server
  - c. File Replication Service
  - d. DFS Replication

## Conformité et Sécurité

### Politiques de Sécurité Appliquées

#### *Politiques de Mots de Passe*

- i. Default Domain Policy :**
  - a. Longueur minimale : 8 caractères
  - b. Complexité : Requise
  - c. Âge maximum : 365 jours
  - d. Historique : 2 mots de passe
  - e. Âge minimum : 1 jour

#### *Politiques de Verrouillage*

- i. Account Lockout Policy :**
  - a. Seuil de verrouillage : 10 tentatives
  - b. Durée de verrouillage : 30 minutes
  - c. Remise à zéro : 30 minutes

#### *Audit Policy*

- i. Catégories auditées :**
  - a. Ouverture/fermeture de session
  - b. Gestion des comptes
  - c. Accès aux objets (limité)
  - d. Changements de politique
  - e. Utilisation des privilèges

## Rôles et Délégations

#### *Délégations Administratives*

- i. Délégation par OU :**

OU	Groupe délégué	Permissions
OU=Paris	GRP_IT_Paris_Admins	Full Control sauf modification OU
OU=Lyon	GRP_IT_Lyon_Admins	Full Control sauf modification OU
OU=Lille	GRP_IT_Lille_Admins	Full Control sauf modification OU
OU=Comptes_Service	GRP_Service_Account_Admins	Gestion comptes de service

#### *Séparation des Privilèges*

- i. Niveaux d'administration :**
  - a. **Tier 0** : Administration AD (Domain/Enterprise Admins)

- b. **Tier 1** : Administration serveurs (Server Operators)
- c. **Tier 2** : Support utilisateurs (Help Desk)

## Annexes Techniques

### Schéma de Réplication

- i. Réplication AD - Sites MegaCorp

#### Configuration DNS

- i. **Zones Active Directory Intégrées :**

```
corp.megacorp.fr (Zone principale)
├─ _msdcs.corp.megacorp.fr (Services AD)
├─ DomainDnsZones.corp.megacorp.fr
└─ ForestDnsZones.megacorp.fr
```

```
1.168.192.in-addr.arpa (Zone inverse Paris)
2.168.192.in-addr.arpa (Zone inverse Lyon)
3.168.192.in-addr.arpa (Zone inverse Lille)
```

### Mapping des Services

Service	Serveur Principal	Serveur Secondaire	Port
<b>DNS</b>	Tous DC	-	53
<b>LDAP</b>	Tous DC	-	389/636
<b>Kerberos</b>	Tous DC	-	88
<b>Global Catalog</b>	DC-PARIS-01, DC-LYON-01	-	3268/3269
<b>DHCP</b>	DC-PARIS-01	DC-PARIS-02	67/68
<b>DHCP Lyon</b>	DC-LYON-01	DC-LYON-02	67/68
<b>DHCP Lille</b>	DC-LILLE-01	-	67/68

*Cette documentation décrit l'infrastructure Active Directory de MegaCorp dans son état actuel. Elle sert de base pour l'analyse de sécurité et l'identification des axes d'amélioration.*

**Version** : 2.1

**Date** : Novembre 2024

**Classification** : Interne MegaCorp



# Atelier d'Analyse EBIOS Risk Manager

## Contexte de la Mission

### Rappel : Présentation de MegaCorp International

- i. **Profil de l'entreprise**
- ii. **Secteur** : Entreprise multinationale de services technologiques
- iii. **Taille** : 10 000 employés répartis sur 15 sites dans le monde
- iv. **Chiffre d'affaires** : 2,5 milliards d'euros
- v. **Sites principaux** : Paris (siège), Lyon (production), Lille (R&D)
- vi. **Contexte sécuritaire** Plusieurs incidents récents dans le secteur ont alerté la direction de MegaCorp :
  - vii. Ransomware ayant paralysé un concurrent pendant 3 semaines
  - viii. Vol de données sensibles chez un partenaire via exploitation de comptes privilégiés
  - ix. Attaque supply chain touchant plusieurs entreprises du secteur

**Votre mission** En tant qu'équipe de consultants en cybersécurité, vous devez réaliser une analyse de risques EBIOS Risk Manager sur l'infrastructure Active Directory de MegaCorp et proposer un plan de remédiation priorisé.

## Méthodologie EBIOS Risk Manager

### Atelier 1 : Cadrage et Socle de Sécurité

#### 1.1 Définition du Périmètre d'Étude

##### À réaliser :

1. Délimiter précisément le périmètre technique à analyser
2. Identifier les frontières organisationnelles
3. Définir les interfaces avec l'écosystème externe

##### Template de travail :

Dimension	Inclus dans le périmètre	Exclu du périmètre	Justification
Technique			
Géographique			
Organisationnelle			
Fonctionnel			

## 1.2 Identification des Biens Supports

### À identifier :

- Contrôleurs de domaine et leur criticité
- Services AD essentiels (DNS, DHCP, etc.)
- Base de données Active Directory
- Infrastructure réseau de réplication
- Comptes et groupes critiques

### Template de travail :

Bien Support	Type	Localisation	Criticité	Dépendances

## 1.3 Caractérisation des Valeurs Métier

### À analyser :

- Service d'authentification et d'autorisation
- Annuaire d'entreprise
- Gestion centralisée des configurations
- Continuité des opérations métier

### Critères de sécurité à évaluer :

- **Disponibilité** : Temps d'arrêt acceptable
- **Intégrité** : Niveau de confiance requis
- **Confidentialité** : Sensibilité des informations
- **Preuve** : Besoins de traçabilité

### Template de travail :

Valeur Métier	Description	D	I	C	P	Impact Business
		1-5	1-5	1-5	1-5	

## 1.4 Cartographie des Parties Prenantes

### Parties prenantes internes :

- Direction générale et COMEX
- DSI et équipes techniques
- Utilisateurs finaux par métier
- Responsables sécurité



### Parties prenantes externes :

- Clients et partenaires
- Prestataires informatiques
- Autorités de régulation
- Auditeurs externes

## Atelier 2 : Sources de Risque

### 2.1 Identification des Sources de Risque

#### Sources externes potentielles :

- Cybercriminels organisés
- Groupes APT (Advanced Persistent Threat)
- Concurrents déloyaux
- États nations
- Hacktivistes

#### Sources internes potentielles :

- Employés malveillants
- Personnel négligent
- Administrateurs compromis
- Prestataires externes

### 2.2 Analyse des Motivations et Capacités

#### Template d'analyse :

Source	Motivations	Ressources	Opportunités	Pertinence
				1-5

## Atelier 3 : Scénarios Stratégiques

### 3.1 Construction des Scénarios

#### Méthodologie :

1. Croiser sources de risque × objectifs visés
2. Identifier les chemins d'attaque de haut niveau
3. Évaluer les impacts sur les valeurs métier

#### Template de scénario :

Scénario	Sou	Objectif Visé	Chemin d'Attaque	Biens Pivots	Impact Valeurs

### 3.2 Évaluation Stratégique

#### Critères d'évaluation :

- Gravité des impacts
- Faisabilité pour la source
- Attractivité de la cible

## Atelier 4 : Scénarios Opérationnels

### 4.1 Déclinaison Technique

#### Pour chaque scénario stratégique :

1. Détailler les étapes techniques
2. Identifier les vulnérabilités exploitées
3. Préciser les événements redoutés

#### Template opérationnel :

Étape	Action Technique	Vulnérabilité	Événement Redouté	Détection
1				
2				
...				

### 4.2 Techniques d'Attaque AD à Considérer

#### Reconnaissance :

- Énumération LDAP
- Découverte de la topologie AD
- Cartographie des privilèges

#### Accès initial :

- Exploitation de comptes faibles
- Attaques par dictionnaire
- Ingénierie sociale

#### Élévation de privilèges :

- Exploitation de comptes de service

- Attaques sur les délégations
- Abus de groupes privilégiés

#### **Mouvement latéral :**

- Exploitation des trusts
- Propagation via partages
- Utilisation des credentials cachés

#### **Persistance :**

- Modification des groupes
- Implantation de backdoors
- Altération des GPO

## **Atelier 5 : Traitement du Risque**

### *5.1 Stratégies de Traitement*

#### **Options disponibles :**

- **Éviter** : Supprimer la source de risque
- **Réduire** : Diminuer probabilité ou impact
- **Transférer** : Assurance, externalisation
- **Accepter** : Risque résiduel assumé

### *5.2 Mesures de Sécurité*

#### **Catégories de mesures :**

- **Préventives** : Empêcher la réalisation du risque
- **Protectrices** : Limiter l'impact
- **Déetectrices** : Identifier les tentatives
- **Récupératrices** : Restaurer le service

#### **Template de plan de traitement :**

Mesure	Type	Priorité	Complexité	Délai	Coût	Efficacité
		1-5	1-5			1-5

## Livrables Attendus

### 1. Rapport d'Analyse EBIOS

#### Structure recommandée :

##### 1. Synthèse Exécutive

- 3 risques majeurs identifiés
- Impact métier potentiel
- Top 3 des recommandations prioritaires
- Niveau d'urgence des mesures

##### 2. Matrice de Risques Détaillée

- Scénarios de risque analysés
- Évaluation Impact × Vraisemblance
- Cartographie des menaces spécifiques AD

##### 3. Plan d'Action Technique

- Actions prioritaires avec justification
- Complexité d'implémentation
- Délais et ressources nécessaires

### 2. Templates de Restitution

#### Matrice EBIOS Spécialisée

Scénario	Source de Risque	Vraisemblance (1-5)	Impact (1-5)	Criticité	Mesures Existantes	Mesures Proposées

#### Plan d'Action Technique

Action	Priorité	Complexité	Délai Implémentation	Impact Sécurité	Quick Win
	Critique/Haute/Moyenne	Faible/Moyenne/Élevée	Court/Moyen/Long terme	Fort/Moyen/Faible	✓/X

## Méthodes d'Investigation

### Outils d'Analyse Recommandés

#### Reconnaissance Active Directory :

- Énumération des comptes et groupes
- Analyse des délégations et privilèges
- Cartographie des relations de confiance
- Audit des configurations de sécurité

### **Méthodes d'Analyse :**

- Entretiens avec les parties prenantes
- Analyse documentaire (politiques, procédures)
- Tests techniques non intrusifs
- Revue de configuration

### **Points d'Attention Spécifiques AD**

#### **Configuration des comptes :**

- Politique de mots de passe
- Gestion des comptes privilégiés
- Comptes de service et leurs SPN
- Comptes inactifs ou orphelins

#### **Architecture et topologie :**

- Relations d'approbation entre domaines
- Configuration de la réplication
- Délégations administratives
- Segmentation réseau

#### **Sécurité et audit :**

- Configuration des logs de sécurité
- Politiques de groupe appliquées
- Mesures de détection d'intrusion
- Procédures de sauvegarde et restauration

### **Contraintes et Considérations**

#### **Contraintes Métier**

##### **Disponibilité :**

- Infrastructure critique 24/7
- Fenêtres de maintenance limitées
- Impact sur la productivité

##### **Conformité :**

- Obligations réglementaires sectorielles
- Exigences clients et partenaires

- Standards internes de sécurité

## Contraintes Techniques

### Architecture existante :

- Applications legacy dépendantes
- Contraintes de compatibilité
- Limites budgétaires

### Ressources :

- Équipes IT limitées
- Compétences internes
- Planning de déploiement

## Questions Guides

- i. **Pour l'atelier 1 :**
  - a. Quelles sont les valeurs métier réellement critiques ?
  - b. Quel est le coût d'une indisponibilité AD ?
  - c. Quelles sont les exigences de conformité ?
- ii. **Pour l'atelier 2 :**
  - a. Quelles sources menacent spécifiquement ce secteur ?
  - b. Quels sont les vecteurs d'attaque les plus probables ?
  - c. Quelle est l'exposition externe de l'organisation ?
- iii. **Pour l'atelier 3 :**
  - a. Quels scénarios auraient l'impact le plus fort ?
  - b. Comment un attaquant peut-il progresser dans AD ?
  - c. Quels sont les chemins vers les données sensibles ?
- iv. **Pour l'atelier 4 :**
  - a. Quelles vulnérabilités techniques sont exploitables ?
  - b. Comment détecter ces types d'attaques ?
  - c. Quels indicateurs de compromission surveiller ?
- v. **Pour l'atelier 5 :**
  - a. Quelles mesures ont le meilleur ROI sécuritaire ?
  - b. Comment maintenir l'opérationnalité pendant les changements ?
  - c. Quel plan de déploiement adopter ?