A purple arrow with black background

Description automatically generated

**Version 1.0**

METSYS : S.A.S au capital de 944 444€, SIRET 538 663 683 00091, 538 663683 R.C.S. Nanterre, APE 6202A

Siège social : 121 rue d’Aguesseau, 92 100 Boulogne-Billancourt, France.

Téléphone : +33 (0)1 81 89 19 70

<www.metsys.fr>

RAPPORT D’AUDIT D’ARCHITECTURE ET DE SECURITE ACTIVE DIRECTORY

[company\_address]

**[company\_name]**

28 juin 2024

**Rapport d’audit**

**Active Directory**

Table des matières

[ Table des illustrations 3](#_Toc168649104)

[ Résumé 4](#_Toc168649105)

[ Introduction 5](#_Toc168649106)

[ Chaine de cyberattaques 6](#_Toc168649107)

[L'Importance de la chaine de cyberattaques 6](#_Toc168649108)

[ Tableau raci 7](#_Toc168649109)

# Table des illustrations

[Illustration 1 - Chaine de cyberattaques 7](#_Toc163833098)

# Introduction

L'audit Active Directory constitue une pratique essentielle pour toute entreprise souhaitant maintenir la sécurité et l'efficacité de son infrastructure informatique. En tant que répertoire centralisé des ressources informatiques, Active Directory joue un rôle fondamental dans la gestion des utilisateurs, des groupes, des politiques de sécurité et des ressources réseau au sein d'une organisation. Cependant, au fil du temps, la complexité croissante des infrastructures informatiques et la diversité des opérations effectuées dans Active Directory peuvent entraîner des incohérences, des vulnérabilités de sécurité et des risques de conformité.

Un audit Active Directory permet de procéder à une évaluation approfondie de la santé et de la sécurité de l'environnement Active Directory d'une entreprise. Il implique l'analyse des paramètres de sécurité, des stratégies d'accès, des journaux d'activité et des configurations pour identifier les éventuelles failles de sécurité, les problèmes de conformité et les inefficacités opérationnelles. Grâce à cet examen approfondi, les équipes informatiques peuvent prendre des mesures correctives proactives pour renforcer la sécurité, améliorer les performances et garantir la conformité aux réglementations en vigueur.

Pour une entreprise, un audit Active Directory revêt une importance cruciale pour plusieurs raisons. Tout d'abord, il permet de détecter et de corriger rapidement les failles de sécurité potentielles, réduisant ainsi les risques de violations de données et les attaques informatiques. De plus, en assurant la conformité aux normes de sécurité et aux réglementations, telles que le RGPD, HIPAA ou SOX, un audit Active Directory aide à éviter les amendes financières et les conséquences juridiques néfastes. Enfin, en optimisant les performances et la gestion d'Active Directory, les audits réguliers contribuent à maintenir la productivité des utilisateurs et la disponibilité des services informatiques essentiels pour l'entreprise.

# Chaine de cyberattaques

La chaine de cyberattaques, ou *cyber kill chain* en anglais, est un modèle conceptuel développé par Lockheed Martin pour décrire les étapes d'une attaque cybernétique, du stade initial de la planification à l'objectif final de l'attaquant. Cette méthodologie permet de comprendre le processus suivi par les attaquants et aide les organisations à concevoir des stratégies de défense efficaces.

Une image contenant texte, capture d’écran, cercle, conception

Description générée automatiquement

Illustration 1: Chaine de cyberattaques

## L'Importance de la chaine de cyberattaques

* **Compréhension des Menaces** : La Cyber Kill Chain fournit un cadre pour comprendre les tactiques, techniques et procédures (TTP) utilisées par les attaquants tout au long du processus d'attaque.
* **Détection Précoce** : En identifiant les différentes étapes de l'attaque, les organisations peuvent mettre en place des mesures de détection et de prévention pour arrêter les attaquants à différentes phases de la chaîne.
* **Réponse Rapide** : La connaissance des étapes de la Cyber Kill Chain permet aux équipes de sécurité de répondre plus rapidement et plus efficacement aux incidents en cours, en limitant les dommages potentiels.
* **Prévention Future** : En comprenant les tactiques utilisées par les attaquants, les organisations peuvent renforcer leur posture de sécurité pour prévenir les attaques futures.

# Tableau raci

Un tableau RACI est un outil de gestion de projet et de responsabilité qui aide à définir les rôles et les responsabilités des membres d'une équipe dans le cadre d'un projet ou d'un processus. Le terme "RACI" est un acronyme basé sur les quatre types de responsabilités généralement attribuées dans un projet ou une activité :

* **Responsable (*Responsible* - R) :** La personne ou l'équipe qui est chargée d'effectuer la tâche. Il peut y avoir plusieurs personnes responsables d'une tâche, mais une personne doit être principalement responsable.
* **Approuve (*Accountable* - A) :** La personne ou l'entité qui a l'autorité finale et la responsabilité globale de la tâche. Il s'agit souvent du "décideur" qui doit donner l'approbation finale.
* **Consulté (*Consulted* - C) :** Les personnes ou les parties prenantes qui doivent être consultées ou dont l'expertise est nécessaire avant de prendre une décision ou d'effectuer une tâche. Ce sont généralement des personnes dont la contribution est importante pour le succès de la tâche.
* **Informé (*Informed* - I) :** Les personnes ou les parties prenantes qui doivent être tenues informées du progrès de la tâche ou de la décision, mais qui n'ont pas nécessairement besoin de participer activement.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Support N1 | Support N2 | Support N3 | Projet | DSI | RSSI | Réseaux | Utilisateurs |
| Evolution du niveau fonctionnel de la Forêt |  | I | R | AR |  | C |  |  |
| Extension du Schéma |  | I | R | AR |  | C |  |  |
| Ajout/Suppression Utilisateur dans les groupes "Administrateurs de l'Entreprise", "Administrateurs du Schéma" |  |  | R | AR | I | C |  |  |
| Gestion des relations d'approbation Forêt |  |  | R | AR | I | C |  |  |
| Gestion des contrôleurs de domaine FSMO (transfert de rôle / seize) |  |  | R | AR |  | I |  |  |
| Gestion (création/suppression) d'un nouveau domaine au sein de la Forêt |  | I | R | AR | I | C |  |  |
| ****Sites et sous-réseaux**** | | | | | | | | | |
| Gestion d'un site (création/modification/suppression) |  |  | R | AR |  | I |  |  |
| Gestion d'un lien de site (création/modification/suppression) |  |  | R | AR |  | I | C |  |
| ****Domaine**** | | | | | | | | | |
| Ajout/Suppression Utilisateur dans les groupes "Administrateurs ", "Administrateurs du Domaine" |  |  | R | AR | I | C |  |  |
| Gestion des relations d'approbation |  |  | R | AR |  | C |  |  |
| Gestion des contrôleurs de domaine FSMO (transfert de rôle / seize) |  |  | R | AR |  | I |  |  |
| Déploiement du socle master (futur Contrôleur de Domaine) |  |  | R | AR |  | I |  |  |
| Promotion d'un Contrôleur de domaine |  |  | R | AR |  | I |  |  |
| Décommissions d'un Contrôleur de domaine |  |  | R | AR |  | I |  |  |
| Maintenance (socle master) d'un Contrôleur de domaine |  |  | R | AR |  | I |  |  |
| Déploiement SP/Hotfix sur un contrôleur de domaine |  |  | R | AR |  | I |  |  |
| Activation d'un contrôleur de domaine en tant que Global Catalog |  |  | R | AR |  | I |  |  |
| Sauvegarde d'un contrôleur de domaine |  |  | R | AR |  |  |  |  |
| Restauration d'un contrôleur de domaine |  |  | R | AR |  |  |  |  |
| Restauration Autoritaire de l'annuaire |  |  | R | AR | I | I |  |  |
| Restauration NON-Autoritaire de l'annuaire |  |  | R | AR | I | I |  |  |
| Restauration d'un objet unitaire depuis la Corbeille |  |  | R | AR |  |  |  |  |
| Gestion de la synchronisation de temps (Windows Time) |  |  | R | AR |  |  |  |  |
| Gestion des délégations d'administration |  |  | R | AR | I | C |  |  |
| Provisionning et modification de comptes utilisateurs/groupes utilisateurs |  | AR |  |  |  |  |  |  |
| Réinitialisation d'un mot de passe compte utilisateur |  | AR |  |  |  |  |  |  |
| Provisionning et modification de comptes Administrateur/Groupes d'administration/Délégation |  |  | R | AR | I | I |  |  |
| Réinitialisation d'un mot de passe compte Administrateur |  |  | R | AR | I | I |  |  |
| Provisionning et modification de comptes de services |  |  | R | AR | I | I |  |  |
| Réinitialisation d'un mot de passe compte de services |  |  | R | AR | I | I |  |  |
| Intégration de serveurs membres au datacenter |  |  | R | AR |  |  |  |  |
| Intégration de postes de travail |  | AR |  |  |  |  |  |  |
| ****GPO**** | | | | | | | | | |
| Assignation des GPO (Sites, Domaine, OU, filtres WMI, filtres par groupes de sécurité) |  |  | AR | R |  |  |  |  |
| Sauvegarde/Restauration des GPO (avec la console GPMC) |  |  | AR |  |  |  |  |  |
| Définition des politiques de sécurité, de mot de passe, d'audit |  |  | AR | R | C | C |  | I |
| ****DNS**** | | | | | | | | | |
| Gestion d'enregistrements statiques DNS |  |  | AR | R |  |  |  |  |
| Configuration des paramètres du serveur DNS (contrôleurs de domaine) |  |  | AR | R |  |  |  |  |
| Configuration des paramètres IP client DNS (contrôleurs de domaine) |  |  | AR | R |  |  |  |  |
| Configuration des paramètres IP client DNS (serveurs membres) |  |  | AR | R |  |  |  |  |
| Configuration des paramètres IP client DNS (postes de travail et serveurs membres) (DHCP ou statique) |  | AR | I | I |  |  |  |  |
| ****Opérations de maintenance**** | | | | | | | | | |
| Vérification de la haute disponibilité |  |  | AR | R |  |  |  |  |
| Analyse des journaux d'évènements |  |  | AR | R |  |  |  |  |
| Vérification des opérations de backup |  |  | AR | R |  |  |  |  |
| Audit de la sécurité |  |  | AR | R |  | I |  |  |
| Réalisation des statistiques d'utilisation |  |  | AR | R |  |  |  |  |
| Vérification des réplications |  |  | AR | R |  |  |  |  |
| Identification des comptes à supprimer |  | R | AR | R |  |  |  |  |
| Redémarrage de services / serveurs |  |  | AR | R |  |  |  |  |
| Gestion du produit antivirus (MAJ signature) |  |  | AR | R |  | I |  |  |
| ****Supervision de l'infrastructure d'annuaire**** | | | | | | | | | |
| Monitoring des services |  |  | AR | R |  |  |  |  |
| Monitoring des services antivirus |  |  | AR | R |  | I |  |  |
| ****Gestion des incidents et problèmes - continuité de service**** | | | | | | | | | |
| Diagnostic gestion des incidents niveau 2 |  | AR |  |  |  |  |  |  |
| Support N3 (par ex. Vérification de l'intégrité d'une base AD) |  |  | AR | R |  |  |  |  |