VIVALTEK | ACTIVE DIRECTORY COMPLIANCE

INTRODUCTION

L'Active Directory (AD[1]) constitue un **point d'entrée central** vers l'ensemble de vos accès et données critiques. **S'il est compromis, c'est toute votre organisation qui peut être paralysée,** avec des conséquences directes sur votre chiffre d'affaires et vos engagements contractuels. Un AD compromis peut entraîner plusieurs jours à plusieurs semaines d'interruption avec des équipes à l'arrêt et des contrats clients compromis. Il est donc essentiel de **contrôler votre AD et prouver qu'il est sécurisé par des audits réguliers.** C'est également un atout stratégique pour développer votre activité et gagner de nouveaux marchés.

OBJECTIFS

Evaluer la sécurité de votre Active Directory, détecter les points faibles et les mauvaises configurations qui le rendent vulnérable.

- **Analyser la configuration des comptes utilisateurs**
- **Evaluer la sécurité de l'AD**
- **Identifier les vulnérabilités et risques exploitables, détecter les anomalies et configurations obsolètes**
- **Renforcer la posture de sécurité de l'AD**

LES CHIFFRES CLÉS*

80 %
des failles de sécurité sont liées aux vulnérabilités de l'Active Directory.

42 %
d'augmentation des attaques ciblant Active Directory en 2025.

90 %
des cyberincidents impliquent une compromission du système d'identité.

72 %
des entreprises ont subi une attaque par ransomware en 2023, les cybercriminels visant de plus en plus Active Directory.

**Toutes les sources sont disponibles sur notre site internet, dans la fiche produit correspondante.*

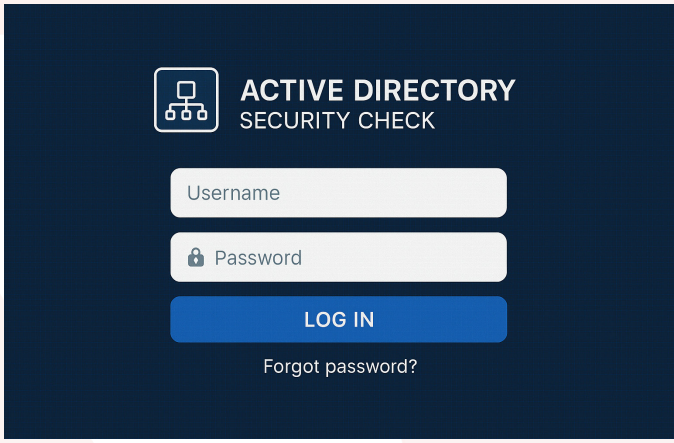
CONTACTEZ NOTRE EXPERT 02 52 61 46 75 | contact@vivaltek.com

Comment fonctionne l'Active Directory Compliance ?

Le module Active Directory Compliance commence par **définir le périmètre et collecter toutes les configurations** des comptes, groupes, GPO[2] et droits via des exports et analyses LDAP[3] ou PowerShell. Il **identifie ensuite les vulnérabilités et mauvaises pratiques,** comme les mots de passe faibles, les comptes inactifs ou les délégations excessives.

2 techniques possibles :

- L'utilisation d'un compte Administrateur pour **tester l'ensemble de l'Active Directory et vérifier les bonnes pratiques.**
- L'utilisation d'un compte utilisateur pour **déterminer le périmètre et les accès qu'il peut avoir ou s'octroyer.**



Sur quoi s'appuie l'Active Directory Compliance ?

- Des tests d'attaques simulées pour **mesurer la résistance du système** à l'escalade de privilèges et aux techniques comme le Pass-the-Hash.
- Une **évaluation du niveau de risque** pour renforcer la sécurité de l'AD et garantir la continuité des services.
- Les informations administrateurs ou utilisateurs qui permettent une connexion à l'AD.

Pourquoi effectuer une simulation avec l'Active Directory Compliance ?

1. **Protéger l'Active Directory,** cœur du système d'authentification et d'autorisation, qui donne accès à tous les services critiques et aux données sensibles de l'entreprise.

2. **Permettre de détecter les mauvaises pratiques, les comptes à risque et configurations trop permissives,** souvent exploitées lors d'attaques de type ransomware.

3. **Eviter les interruptions d'activité,** bloquer les accès non autorisés coûteux, et répondre aux exigences des normes ainsi qu'aux attentes des partenaires.

4. **Renforcer la confiance globale des clients et partenaires** en démontrant que l'entreprise maîtrise ses accès et sa sécurité interne, réduisant ainsi les risques financiers et réputationnels majeurs.

Simulation avec l'Active Directory Compliance :

Vise à **sécuriser le cœur du système d'accès de l'entreprise** en identifiant les pratiques à risque et les failles d'autorisation. Elle permet de **prévenir les attaques, d'éviter les interruptions coûteuses et de répondre aux exigences de conformité.** C'est un gage de maîtrise et de confiance pour les partenaires.

Sur quelle fréquence effectuer une analyse Active Directory ?

L'Active Directory constitue un élément central de l'infrastructure informatique dans de nombreuses entreprises. Il assure la gestion des identités, des accès et des droits de l'ensemble des utilisateurs. Cependant, **en raison de son rôle stratégique, il représente également une cible privilégiée pour les cyberattaquants.** En effet, une simple faille de configuration peut suffire à compromettre l'ensemble du Système d'Information.

C'est pourquoi il est vivement conseillé de réaliser une **évaluation régulière de l'Active Directory,** ou à l'occasion d'événements sensibles tels qu'un changement de prestataire, une restructuration des services IT ou un incident de sécurité. Cette démarche permet d'identifier à temps les dérives potentielles : comptes inactifs, privilèges excessifs, failles techniques non corrigées ou encore mauvaises attributions de droits d'accès.

Pour l'entreprise, cela contribue à **renforcer la sécurité de l'environnement Windows**, à **améliorer la résilience globale du système** et à limiter les risques d'escalade de privilèges.

Evaluer la sécurité de votre Active Directory, détecter les points faibles et les mauvaises configurations qui le rendent vulnérable.

Lexique

[1]**AD :** L'Active Directory est un système de Microsoft qui permet de gérer les utilisateurs, les mots de passe, les accès et les droits au sein d'un réseau d'entreprise.

[2]**GPO (Group Policy Object) :** C'est une règle utilisée dans un réseau Windows pour contrôler et automatiser les paramètres des ordinateurs et des utilisateurs.

[3]**LDAP :** C'est un protocole qui permet d'accéder à un annuaire d'informations (Active Directory), comme les noms d'utilisateurs, les mots de passe ou les adresses e-mail.

Consultez notre lexique complet à l'adresse suivante : https://vivaltek.com/lexique-complet

VIVALTEK
2, Impasse Johannes Gutenberg, Z.A Les Acacias III 85430 La Boissière des Landes
02 52 61 46 75 | contact@vivaltek.com