



Attaquer son Active Directory **pour savoir le défendre.**

Vous administrez un Active Directory sans savoir par où quelqu'un entrerait ? Vous menez l'attaque vous-même, guidé pas à pas, pour voir exactement ce qui cède. Puis vous décidez quoi durcir en premier, et vous jouez la crise : qui décide quoi dans les six premières heures si ça arrive vraiment.

DURÉE	TARIF INTER	INTRA	NIVEAU
4 jours	3 000 € HT	dès 1 500 € HT/jour	Accessible – aucun prérequis offensif

À l'issue de la formation

- Lire une architecture Active Directory et repérer ce qu'il expose
- Comprendre les grandes familles d'attaque et ce qu'elles supposent côté attaquant
- Interpréter un rapport de pentest, un PingCastle ou un BloodHound sans traducteur
- Construire un plan de durcissement priorisé et défendable devant la direction
- Savoir quoi collecter, quoi surveiller et quoi décider dans les premières heures d'une crise

Pour qui

- RSSI, RSSI adjoints et responsables sécurité
- DSI et responsables infrastructure
- Administrateurs Active Directory et équipes système
- Auditeurs, consultants GRC et chefs de projet sécurité
- Membres désignés d'une cellule de crise cyber

Prérequis

Savoir ce qu'est un annuaire d'entreprise, un compte, un groupe et un droit. Aucune compétence en test d'intrusion n'est demandée : vous menez les attaques vous-même, guidé pas à pas par le formateur, puis vous décidez de ce qu'il faut corriger en premier.

Déroulé

Jour 1 Votre annuaire vu par un attaquant

- Architecture Active Directory typique : forêt, domaines, unités d'organisation, contrôleurs de domaine
- Authentification et autorisation : ce qui se passe vraiment quand un utilisateur ouvre sa session
- Tour d'horizon des protocoles : Kerberos, NTLM, LDAP, SMB, DNS - à quoi sert chacun, ce que chacun donne
- Les recommandations et bonnes pratiques ANSSI, Microsoft et CIS : ce qui compte, ce qui est du folklore
- Démonstration : la reconnaissance complète d'un domaine en vingt minutes, commentée pas à pas

Jour 2 Comment un domaine tombe

- Vue d'ensemble des méthodes de gestion du risque appliquées au système d'information
- Les étapes d'une attaque : point d'entrée, élévation, latéralisation, prise du domaine
- Démonstrations commentées : Kerberoasting, DCSync, délégations Kerberos, abus de certificats AD CS
- Ce que l'attaquant lit dans BloodHound, et ce que ça dit de votre annuaire
- Lire enfin un rapport : PingCastle, Purple Knight, rapport de pentest - trier le critique du cosmétique
- Analyser les contre-mesures : pour chaque attaque, ce qui l'arrête et ce qui ne change rien

Jour 3 Durcir et administrer proprement

- Concevoir un plan de durcissement priorisé, chiffré et défendable en comité de direction
- Déployer les directives : stratégies de groupe, LAPS, Protected Users, comptes de service
- Savoir auditer son infrastructure : quoi demander, à quelle fréquence, à qui
- Les modèles d'administration : EAM et modèle en tiers, intérêt réel et limites de terrain
- Forêt d'administration : quand l'investissement se justifie, quand il devient un gouffre
- Administration à privilèges à la demande : PAM, JIT et JEA

Jour 4 Identité cloud et gestion de crise

- Identité hybride : Entra Connect, fédération AD FS, et la surface que tout cela ouvre
- Panorama des outils Microsoft : Password Protection, Secure Score, Defender for Identity
- Infrastructure de clés internes : ce qu'elle permet de durcir, ce qu'elle expose si elle est mal posée
- Collecter les événements au niveau de l'entreprise : quels journaux, quels identifiants d'évènement, quelle rétention
- Exercice de crise : le domaine est compromis, qui décide quoi et dans quel ordre
- Reconstruire : plan de reprise Active Directory, ce qui se prépare avant et jamais pendant

Ce qui est compris

- Lab de démonstration Active Directory + Windows 11 24H2 avec EDR actif
- Grille de lecture d'un rapport PingCastle et d'un graphe BloodHound
- Modèle de plan de durcissement priorisé, réutilisable tel quel
- Fiche réflexe de crise Active Directory (les 48 premières heures)
- Slides formateur et supports stagiaires PDF

Prochaines sessions inter-entreprises

DATES	LIEU ET FORMAT	PLACES
11 - 14 janvier 2027	À distance · Distanciel	6 places
10 - 13 mai 2027	Paris · Présentiel ou distanciel	8 places
20 - 23 septembre 2027	Paris · Présentiel ou distanciel	8 places

Résistez aux hackers - organisme de formation certifié Qualiopi. Prise en charge OPCO possible, les pièces sont fournies.
Inscription et devis : <https://resistez-aux-hackers.com/contact.html> - formation@resistez-aux-hackers.com
Programme susceptible d'évoluer. Version du 08/10/2026. Accessibilité : nous contacter pour toute situation de handicap, nous étudions les adaptations possibles.