New

Compromission et sécurisation de l'Active Directory

Détecter, analyser et sécuriser les attaques Active Directory

Présentiel ou en classe à distance

4 jours (28 h)

Prix inter : 3.150,00 € HT
Forfait intra : 7.490,00 € HT

Réf.: SR388

La formation **Compromission et sécurisation de l'Active Directory** apporte une vision complète et opérationnelle des mécanismes d'attaque, des vulnérabilités et des stratégies de défense propres aux environnements Active Directory. Les participants acquièrent une **maîtrise approfondie des mécanismes d'authentification (Kerberos, NTLM), des protocoles critiques (LDAP, SMB, DNS) et des failles** les plus couramment exploitées dans les infrastructures Windows.
Au-delà de l'analyse des attaques, la formation met l'accent sur le **durcissement de l'Active Directory** et la **gestion des incidents de sécurité**. Les apprenants apprennent à **concevoir une architecture AD robuste**, à déployer des contre-mesures efficaces (PAM, JIT, JEA, segmentation, GPO de sécurité) et à mettre en place une stratégie de surveillance et de détection adaptée aux menaces modernes. Les travaux pratiques permettent de simuler des attaques réelles, d'appliquer des mesures de protection concrètes et de maîtriser les étapes clés de la réponse à incident : confinement, éradication, reconstruction et restauration d'un environnement sain.

A qui s'adresse cette formation ?

Pour qui

- Administrateurs Windows, support informatique, RSSI

Prérequis

- Connaissances de base sur Windows, l'Active Directory, les réseaux et la sécurité informatique. Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Les fondamentaux en sécurité de l'Active Directory

- Décomposer l'architecture d'un Active Directory typique : domaines, forêts, rôles FSMO, services critiques
- Comprendre la méthodologie générale de compromission d'un AD : du poste utilisateur au contrôle du domaine
- Identifier les principaux vecteurs d'attaque : Kerberoasting, Pass-the-Hash/Pass-the-Ticket, NTLM Relay, attaques LDAP, exploitation des GPO
- Revoir les mécanismes d'authentification et d'autorisation : Kerberos, NTLM, tickets, tokens et délégation
- Passer en revue les protocoles et services associés (LDAP, SMB, RPC, DNS, WebDAV...) et leurs zones de faiblesse
- Intégrer les bonnes pratiques fondamentales : segmentation, moindre privilège, hygiène des comptes, gestion des accès et durcissement de base
  Atelier

  Exploration d'un environnement AD, identification des points d'exposition, analyse des flux d'authentification et des rôles essentiels

2 - Comprendre les risques et les attaques

- Situer l'AD dans les frameworks de gestion des risques SI : exposition, surface d'attaque, scénarios de menace
- Analyser en détail la méthodologie de compromission d'un AD on-premise : reconnaissance, mouvement latéral, élévation de privilèges, domination du

domaine
- Décomposer chaque étape d'une attaque réelle : collecte d'informations, exploitation, persistance, exfiltration
- Simuler différentes attaques et étudier les contre-mesures : détection, contention, réponse rapide
- Identifier et détecter les failles de sécurité les plus courantes dans un AD
- Présenter les outils d'attaque et de diagnostic : BloodHound, Mimikatz, Rubeus, SharpHound, PowerView...

Atelier

Simulation d'attaques sur un environnement contrôlé : exploitation de comptes, mouvements latéraux, extraction de secrets, analyse des logs et premiers réflexes défensifs

3 - Durcissement de l'infrastructure AD

- Construire un plan de durcissement structuré : priorisation, isolation des comptes à privilèges, réduction des surfaces d'attaque
- Déployer les directives de sécurité associées (GPO, configuration des services, filtrage des comptes, durcissement Kerberos/NTLM)
- Auditer une infrastructure AD : évaluation des paramètres critiques, revue des comptes sensibles, analyse de la configuration des contrôleurs de domaine
- Organiser la collecte des événements au niveau de l'entreprise : centralisation, corrélation, indicateurs de compromission spécifiques à AD
- Implémenter les mécanismes avancés de durcissement : PAM (Privileged Access Management), JIT (Just-In-Time), JEA (Just-Enough-Administration), ESAE ("bastion forest")

Atelier

Application concrète du durcissement : création et déploiement d'un ensemble de règles, configuration des comptes privilégiés, mise en place des services PAM/JIT/JEA

4 - Gérer une compromission de son Active Directory

- Suivre les étapes clés de la gestion d'un incident touchant l'AD : identification, confinement, éradication, surveillance renforcée
- Organiser la communication et la gestion de crise : coordination avec la DSI, le SOC, les métiers, les autorités selon le contexte
- Reconstruire un Active Directory compromis : remise à plat, restauration maîtrisée, vérification de la chaîne de confiance, réintégration progressive des services

Atelier

Mise en oeuvre des contre-mesures : confinement, révocation de tickets, nettoyage des artefacts d'attaque, rétablissement d'un environnement sain

Les objectifs de la formation

- Décrire les mécanismes internes Active Directory
- Identifier les fonctionnalités de sécurité
- Concevoir une architecture robuste
- Connaître et mettre en oeuvre les attaques et principales exploitations d'un réseau Active Directory
- Mettre en oeuvre les contre-mesures
- Reconstruire son Active Directory en cas de compromission

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une approche complète de la sécurité Active Directory
- Une formation orientée pratique et opérationnelle
- Une préparation à la gestion de crise cyber

Dates et villes 2026 - Référence SR388

Dernières places disponibles Session garantie

A distance

du 16 mars au 19 mars	du 6 juil. au 9 juil.	du 5 oct. au 8 oct.
du 26 mai au 29 mai	du 24 août au 27 août	du 30 nov. au 3 déc.

Strasbourg

du 16 mars au 19 mars	du 6 juil. au 9 juil.	du 5 oct. au 8 oct.

Sophia Antipolis

du 16 mars au 19 mars	du 6 juil. au 9 juil.	du 5 oct. au 8 oct.

Rouen

du 16 mars au 19 mars	du 6 juil. au 9 juil.	du 5 oct. au 8 oct.

Aix-en-Provence

du 16 mars au 19 mars	du 6 juil. au 9 juil.	du 5 oct. au 8 oct.

Lille

du 16 mars au 19 mars	du 6 juil. au 9 juil.	du 5 oct. au 8 oct.

Paris

du 16 mars au 19 mars	du 6 juil. au 9 juil.	du 5 oct. au 8 oct.
du 26 mai au 29 mai	du 24 août au 27 août	du 30 nov. au 3 déc.

Lyon

du 16 mars au 19 mars	du 6 juil. au 9 juil.	du 5 oct. au 8 oct.

Toulouse

du 26 mai au 29 mai	du 24 août au 27 août	du 30 nov. au 3 déc.

Rennes

du 26 mai au 29 mai	du 24 août au 27 août	du 30 nov. au 3 déc.

Nantes

du 26 mai au 29 mai	du 24 août au 27 août	du 30 nov. au 3 déc.