Master Class: Securing Active Directory Deep Dive LEVEL 3 (SADDD-L3)

ID SADDD-L3 **Prix** CHF 3 890,– (Hors Taxe) **Durée** 3 jours

A qui s'adresse cette formation

- Administrateurs Active Directory et administrateurs systèmes Windows souhaitant approfondir leurs compétences en sécurisation des environnements AD.
- Ingénieurs cybersécurité responsables du durcissement et de la défense des infrastructures d'identité.
- Analystes SOC, Blue Teamers et Detection Engineers chargés de détecter et d'investiguer les attaques ciblant Active Directory.
- Consultants sécurité, auditeurs techniques et pentesters souhaitant comprendre les techniques d'attaque les plus avancées utilisées contre Active Directory.
- Membres d'équipes Red Team et Purple Team désireux d'améliorer leurs capacités offensives et défensives.
- Responsables de la réponse à incident amenés à gérer des compromissions d'Active Directory et à piloter des opérations de remédiation et de restauration.
- Architectes infrastructures et experts Microsoft souhaitant renforcer la résilience et la gouvernance des services d'identité critiques.

Pré-requis

- Avoir suivi Master Class: Securing Active Directory Deep Dive (SADDD-L1) ou disposer de connaissances équivalentes
- Avoir suivi Master Class: Securing Active Directory Deep Dive LEVEL 2 (SADDD-L2) ou disposer de connaissances équivalentes
- Posséder une expérience pratique de l'administration Active Directory et des stratégies de groupe (GPO)
- Disposer de connaissances de base en scripting PowerShell
- Comprendre Kerberos, NTLM et les principaux vecteurs d'attaque Active Directory (Pass-the-Hash, Golden Ticket, etc.)

Objectifs

À l'issue de cette masterclass, vous devrez être en mesure de :

- Identifier et exploiter les vecteurs d'attaque avancés ciblant Active Directory, notamment les abus d'ACL, la délégation Kerberos et les attaques NTLM Relay.
- Détecter les activités malveillantes au sein d'un environnement Active Directory grâce aux techniques de Detection Engineering et aux mécanismes de déception.
- Identifier, analyser et éliminer les mécanismes de persistance utilisés par les attaquants après une compromission.
- Mettre en œuvre des mesures de durcissement avancées afin de réduire la surface d'attaque d'Active Directory.
- Réaliser des exercices de Purple Teaming pour améliorer conjointement les capacités de détection et de défense.
- Gérer efficacement un incident de sécurité affectant Active Directory, de la phase de triage jusqu'à la restauration complète de la forêt.
- Concevoir une stratégie de sécurisation pérenne intégrant les évolutions récentes des technologies d'authentification et d'administration Active Directory.

Contenu

Attaques basées sur les ACL

- Théorie : panorama des chemins d'exploitation des ACL
- Atelier pratique : exécution complète d'une chaîne d'attaque par abus d'ACL
- Outils et méthodologies associés

Délégation Kerberos – guide complet

- Unconstrained Delegation – Printer Bug et techniques de coercition
- Resource-Based Constrained Delegation (RBCD) – exploitation via MachineAccountQuota

NTLM Relay – toujours une menace majeure

- Chaîne d'attaque : Coercion + NTLM Relay contre LDAP
- Stratégie complète de durcissement avec priorisation des actions

Mécanismes de persistance dans Active Directory – catalogue complet

- Utilisation d'AdminSDHolder comme porte dérobée
- Détournement de GPO comme mécanisme de persistance

Detection Engineering pour Active Directory

- Configuration complète des stratégies d'audit avancées
- Configuration de Sysmon pour les contrôleurs de domaine

Honey Tokens, comptes Canary et techniques de déception

- Honey Accounts – attributs destinés à attirer les attaquants
- Objets Canary pour la détection dans BloodHound

Purple Teaming appliqué à Active Directory

- Exercice « Assumed Breach » – déroulement et méthodologie

Réponse à incident dans Active Directory

- Les deux premières heures : triage et priorisation
- Recherche de mécanismes de persistance avec PowerShell

Administration par niveaux de privilèges (Tiered Administration)

- Modèle opérationnel et niveaux de maturité
- Authentication Policies et Authentication Silos
- Comptes d'administration d'urgence (Break-Glass)

Sécurité réseau autour d'Active Directory

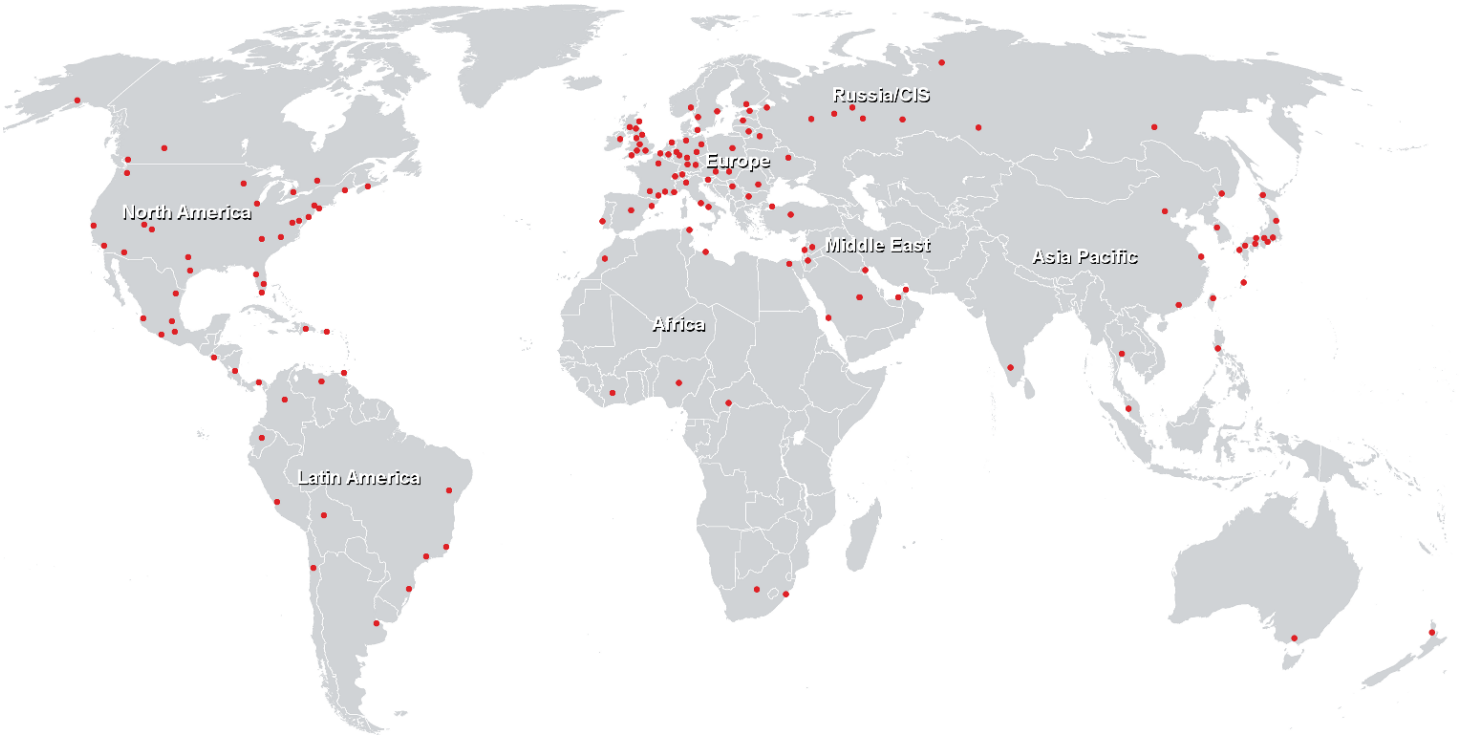
- DHCPv6 / IPv6 – un risque souvent sous-estimé
- Null Sessions et requêtes LDAP anonymes

Retours d'expérience : les prochaines évolutions

- Windows LAPS (nouvelle génération) – migration depuis Legacy LAPS
- Kerberos en mode AES uniquement – suppression complète de RC4

Master Class: Securing Active Directory Deep Dive LEVEL 3 (SADDD-L3)

Centres de formation dans le monde entier





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch