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

ID SADDD-L3 **Preis** CHF 3'890.– (exkl. MwSt.) **Dauer** 3 Tage

Voraussetzungen

- Abschluss von Master Class: Securing Active Directory Deep Dive (SADDD-L1) oder gleichwertige Kenntnisse
- Abschluss von Master Class: Securing Active Directory Deep Dive LEVEL 2 (SADDD-L2) oder gleichwertige Kenntnisse
- Praktische Erfahrung mit Active Directory Administration und Gruppenrichtlinien
- Grundkenntnisse in PowerShell-Scripting
- Verständnis von Kerberos, NTLM und grundlegenden AD-Angriffsvektoren (Pass-the-Hash, Golden Ticket)

Kursinhalt

ACL-basierte Angriffe

- Theorie: ACL-Abuse-Pfade im Überblick
- Live-Lab: ACL-Abuse-Kette vollständig durchführen
- Tooling

Kerberos Delegation – der vollständige Guide

- Unconstrained Delegation – Printer Bug & Coercion
- Resource-Based Constrained Delegation (RBCD) – Angriff via MachineAccountQuota

NTLM Relay – immer noch tödlich

- Angriffskette: Coercion + NTLM Relay gegen LDAP
- Vollständige Härtung – priorisierte Reihenfolge

Persistenz-Mechanismen im AD – der vollständige Katalog

- AdminSDHolder als Backdoor
- GPO-Hijacking als Persistenz

Detection Engineering für Active Directory

- Advanced Audit Policy – vollständige Konfiguration
- Sysmon-Konfiguration für Domänencontroller

Honey Tokens, Canary Accounts & Deception

- Honey Accounts – Attribute die Angreifer anlocken
- Canary-Objekte für BloodHound-Erkennung

Purple Teaming für Active Directory

- Assumed Breach Übung – Ablauf

Incident Response für Active Directory

- Die ersten 2 Stunden: Triage
- Persistenz-Suche – PowerShell-Befehle

Tiered Administration – Betrieb und Reifegradmodell

- Authentication Policies und Authentication Silos
- Break-Glass / Notfall-Admin-Zugriff

Netzwerksicherheit rund um AD

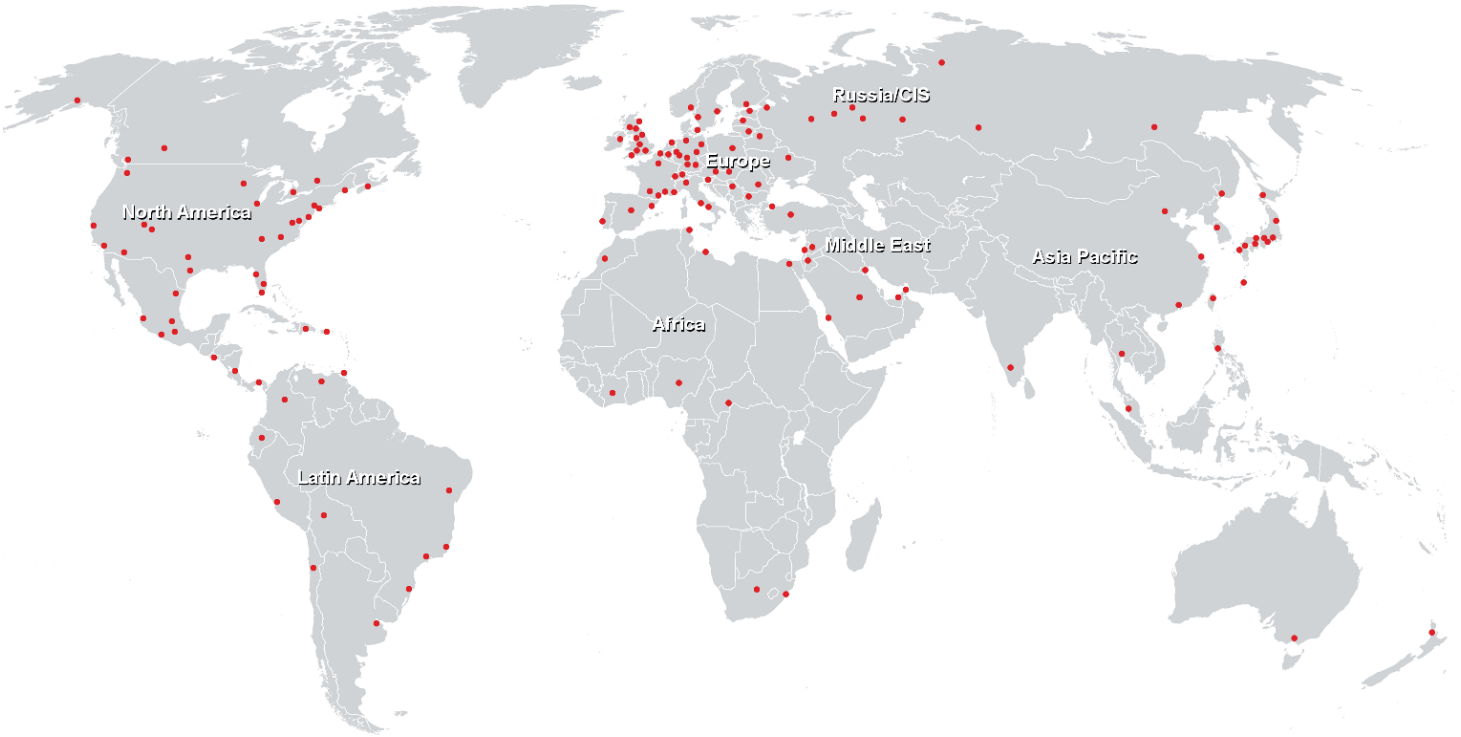
- DHCPv6 / IPv6 – das unterschätzte Risiko
- Null Sessions und anonyme LDAP-Abfragen

Notes from the field: Was als nächstes kommt

- Windows LAPS (neue Generation) – Migration von Legacy LAPS
- Kerberos AES-Only – RC4 vollständig deaktivieren

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

Weltweite Trainingscenter





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