Master Class: Securing Active Directory Deep Dive (SADDD-L1)

ID SADDD-L1 **Preis** 5.900,– € (exkl. MwSt.) **Dauer** 5 Tage

*„Ich war sehr beeindruckt von der Qualität des **Securing Active Directory Deep Dive** Kurses. Der Kurs war sehr umfangreich und hat mir ein tiefes Verständnis für Active Directory und dessen Sicherheitsaspekte vermittelt. Der Dozent war extrem kompetent und konnte komplexe Konzepte klar und verständlich vermitteln. Darüber hinaus war die Hilfestellung während des Kurses ausgezeichnet. Ich hatte jederzeit Zugang zu qualitativ hochwertigen Materialien und Ressourcen, die mir geholfen haben, das Gelernte zu vertiefen. Insgesamt würde ich den Kurs jedem empfehlen, der sein Wissen über Active Directory und Sicherheit vertiefen möchte.“* Christian Peters, Leiter IT & Organisation | Zentrale Dienste, Industrie- und Handelskammer zu Lübeck

Zielgruppe

Dieser Kurs wendet sich an erfahrene System-Administratoren, Consultants und Active Directory-Designer. Nach diesem Seminar werden Sie in der Lage sein, Active Directory hochsicher zu designen, zu implementieren und zu beraten.

Voraussetzungen

Mindestens 5 Jahre Erfahrung mit Active Directory und Client-Systemen

Kursziele

In diesem Master-Class-Kurs wird das Thema Active Directory-Security ganz zentral in den Focus genommen - Mittlerweile sind diverse Angriffs-Szenarien bekannt, die beispielsweise bei dem Bundestag-Hack zum Einsatz gekommen sind (mimikatz et.al.).

Diese validen Angriffs-Szenarien zielen auf Credential-Thefting oder auf Ransomeware-Implementierung ab (bspw. Bei dem Logistiker Maersk mit einem geschätzten Schaden von 300 Millionen Euro).

Das Ziel dieses Workshops ist es, diese Szenarien zu verstehen, um diese dann verhindern zu können und eine Active Directory-Implementierung umzusetzen, die diesen Angriffen widersteht und auch gegen zukünftige Angriffe durchgehärtet ist.

Das Active Directory sind Ihre „Kronjuwelen“ – ohne Active Directory sind die meisten Firmen-Umgebungen produktiv komplett lahmgelegt.

Deswegen: Verstehe, härten und monitoring, damit Sie besser schlafen können.

Kursinhalt

In diesem DeepDive Workshop erfahren Sie, wie Sie Active-Directory-Umgebungen hochsicher implementieren, konfigurieren und betreiben.

Das Active Directory ist „in die Jahre“ gekommen. Besonders sicherheits-technisch sollte ein Active Directory NIEMALS im Standard betrieben werden. Angriffs-Szenarien wie Pass-the-Hash, Silver-Ticket, Golden-Ticket oder sogar Skeleton-Key sind gängige Wege von Angreifern, die das Active Directory und somit die User und die Administratoren angreifen können und die Identitäten übernehmen können. Nicht zuletzt hat der Hack des Bundestages mit Hilfe von u.a. mimikatz die Angreifbarkeit des Active Directorys gezeigt.

In diesem Master-Class-Kurs werden zuerst die Angriffsszenarien auf das Active Directory tief durchleuchtet und auch durchgeführt. Mit dem daraus gewonnen Wissen wird das Active Directory nun grundlegend gehärtet. Dies betrifft vorhandene Installationen, die zuerst tiefgehend analysiert werden sollten, sowie neue Implementierungen, die dann komplett durchgehärtet werden, um somit auch in der Zukunft als angriffssicher zu gelten. Das Wissen für diesen Kurs wurde in über 20 Jahren Active Directory-Erfahrung erworben, sowie in jahrelangen Trainings durch Paula Januszkiewicz und Sami Laiho, beide weltweit führend im Thema Security.

In diesen Kurs fließen weiter die Erfahrungen von über 50+ Active Directory-Konzepten ein, die der Trainer während seiner letzten 15

Jahren geschrieben hat – vom KMU bis zum Enterprise-Level mit 375.000 Benutzern. Das Thema Security wird ebenfalls in Richtung der General Data Protection Regulation (GDPR) betrachtet, die am 25. Mai 2018 in Kraft trat.

Wir versprechen: Unser Bestes KnowHow für Sie und Ihre tagtägliche Arbeit von unseren erfahrensten Trainern und Consultants

Schulungsumgebung:

In der Schulungsumgebung wird komplett mit Hyper-V gearbeitet. Für den proaktiven Aufbau der Schulungsumgebung nutzen wir ein Powershell-Skript, mit dem Sie in Sekunden neue virtuelle Maschinen erstellen können. Das Skript wurde von Ihrem Trainer selber entwickelt und ermöglicht den Schulungsaufbau nach Wunsch des Kunden in extremer Schnelligkeit mit geringem Aufwand.

Hardware:

Jedem Teilnehmer steht ein dedizierter Server in einem Rechenzentrum mit insgesamt 1 Gbit-Anschluss ins Internet zur Verfügung. Jeder Teilnehmer-Server ist folgendermaßen ausgestattet:

- 128 GB RAM
- mind. 20 vCores
- 2 NVME-SSDs mit mind. 3.000 MB/s schreibend und mind. 2.000 MB/s lesend
- 1 Gbit ins Internet Gesamt-Bandbreite

Über die Master Class:

Die Advanced Master Class wurde von Andy Wendel entwickelt. Sie wird von ihm selbst oder von erfahrenen, von ihm autorisierten Trainer*innen durchgeführt.

Andy Wendel ist Senior Datacenter- und Cloud-Architekt sowie Certified Security Master Specialization Advanced Windows Security. Ausgebildet wurde und wird er von den international renommierten Sicherheitsexpert*innen Paula Januszkiewicz und Sami Laiho. Diese Zertifizierung wird jedes Jahr erneuert. Andy Wendel arbeitet seit Ende der 1990er Jahre als IT-Trainer und -Consultant und ist zudem zertifizierter Microsoft Learning Consultant (MCLC). Weltweit hat Microsoft nur 56 Certified Learning Consultants ausgezeichnet.

Detaillierter Kursinhalt

- Wiederholung der Best-Practices zur Installation von Domänen-Controllern aus 20 Jahren Erfahrung als ADDS-Senior-Consultant
- Hausgemachte Sicherheitsprobleme im Active Directory
  - Kerberos verstehen
  - NTLM vs. Kerberos
  - SMB
    - SMB-Versionen
    - Angriffs-Szenarien
    - Sicherer Einsatz von SMB
  - PAC_Validation und die Probleme mit der Microsoft-Implementierung von Kerberos – en detail
  - PTH – Pass the Hash – inklusive Live-Attacke mit allen Teilnehmern
  - Silver Ticket
  - Golden Ticket
  - Skeleton Key
- Kerberos Ticket Service
  - Kerberos verstehen
  - Kerberos-Passwörter ändern: Warum und wie…
  - Kerberos-Passwörter ändern: Der Königsweg ohne Ausfälle
- Credential-Thefting verhindern – Ein DeepDive:
  - Angriffs-Szenarie
    - Pass-the-Hash
    - Silver-Ticket
    - GoldenTicket
    - Skeleton-Key
  - Credential-Thefting verhindern
    - Windows Defender Credential Guard konfigurieren
    - Windows Defender Remote Credential Guard Bitlocker
    - Windows Defender Device Guard einsetzen
    - AppLocker einsetzen
    - Windows Defender Application Guard einsetzen
- Konzepte verstehen:
  - Tier.Modelle betreiben
  - Von Red-Forest, Golden-Forest und Bastion Forests
  - Single-Domain-Modell hochsicher
- Clean-Installation-Source
  - Hash-Werte der *.iso-Dateien verifizieren
  - Fciv.exe, Powershell, 7zip und IgorHasher
- Aufsetzen des ersten Domänencontrollers
  - ms-ds-machineaccountquota verstehen
  - redircmp einsetzen für neue Computer-Systeme
  - redirusr einsetzen für neue User
  - Bitlocker
  - Bitlocker und TPM 1.2 vs. 2.0
  - Bitlocker und PreBoot-Authentifizierung

- AppLocker
- Monitoring
  - AD-Audit-Plus
  - CyberArk
- Sicheres Backup und Recovery von Bitlocker-geschützen Backup-Volumes
- Firewalling auf Domänencontrollern
- IPSEC mit RDP konfigurieren
- Härten der Domänencontroller nach
  - Center of Internet Security
  - gpPack& PaT
  - SIM
  - LDA
  - Microsoft-Tools

- Aufsetzen weitere Domänencontroller
- Secure Deployment von Domänencontrollern, Memberservern und Clients via MDT
  - Installation und Konfiguration von MDT hochsicher
  - Härtung von MDT-Servern
  - Ausrollen hochsicherer Memberserver und Clients
- Domänen-Controller sicher via IPSEC betreiben
  - IPSEC konfigurieren und einsetzen
  - IPSEC Monitoring via MMC
- PKI-Server aufsetzen als interne Trusted-ROOT-CA
  - PKI konfigurieren
  - Automatisches Zertifikats-Deployment aktivieren via Gruppenrichtlinien
  - Enrollement von Nicht-Standard-Zertifikaten
  - Härten der PKI nach
    - Center of Internet Security
    - gpPack& PaT
    - SIM
    - LDA
    - Microsoft-Tools
- Jump-Server und Priviliged Acccess-Workstation (PAW) – Konzepte verstehen und umsetzen
  - Jump-Server aufsetzen und konfigurieren
    - RSAT-Installation
    - ADMIN-Center installieren mit gültigem Zertifikat einer Trusted-Root-PKI
    - Bitlocker
    - Bitlocker und TPM 1.2 vs. 2.0
    - Bitlocker und PreBoot-Authentifizierung
    - AppLocker
    - IPSEC mit RDP konfigurieren
    - Backup von Jump-Server auf bitlocker-geschützte Volumes
    - Firewalling auf JUMP-Servern
  - Härten der Jump-Server nach
    - Center of Internet Security
    - gpPack& PaT
    - SIM
    - LDA
    - Microsoft-Tools
  - PAW aufsetzen und konfigurieren
    - Bitlocker
    - Bitlocker und TPM 1.2 vs. 2.0
    - Bitlocker und PreBoot-Authentifizierung
    - AppLocker
    - IPSEC und RDP konfigurieren
    - Backup von PAWs auf bitlocker-geschützte Volumes
    - Firewalling auf PAWs
  - Härten der Domänencontroller nach
    - Center of Internet Security
    - gpPack& PaT
    - SIM
    - LDA
    - Microsoft-Tools
- Sicherheit in Domänen-Netzwerken
  - 802.1X mit
    - MAC-Adressen
    - Zertifikateni
  - MAC-Flooding auf Switchen
    - Hubbing-Mode ausschalten
  - IPSEC mit Kerberos und Zertifikaten
- Windows Defender Advanced Threat Protection (WDATP)
  - Konzept von WDATP verstehen
  - WDATP ausrollen und monitoren
  - WDATP auf Domänencontrollern…
  - WDATP auf Jump-Servern und PAWs
  - WDATP auf Windows 10 Clients
- Fragen der Teilnehmer

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch