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

ID SADDD-L1 **Prix** CHF 5 900,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

This course is designed for experienced system administrators, consultants and Active Directory designers. After this seminar, you will be able to design, implement and consult on highly secure Active Directory.

Pré-requis

At least 5 years of experience with Active Directory and client systems.

Objectifs

In this master class course, the topic of Active Directory security is taken centrally into focus - in the meantime, various attack scenarios are known, which were used, for example, in the Bundestag hack (mimikatz et.al.).

These valid attack scenarios are aimed at credential theft or ransomware implementation (e.g. at the logistics company Maersk with an estimated damage of 300 million euros).

The goal of this workshop is to understand these scenarios so that you can prevent them and implement an Active Directory implementation that resists these attacks and is hardened against future attacks.

The Active Directory are your "crown jewels" - without Active Directory, most corporate environments are completely crippled productively.

That's why: Understand, harden and monitor so you can sleep better.

Contenu

In this DeepDive workshop, you will learn how to implement, configure and operate Active Directory environments in a highly secure manner.

The Active Directory is "getting on in years". Especially from a security point of view, an Active Directory should NEVER be operated in the standard. Attack scenarios such as Pass-the-Hash, Silver-Ticket, Golden-Ticket or even Skeleton-Key are common ways of attackers who can attack the Active Directory and thus the users and administrators and take over the identities. Last but not least, the hack of the Bundestag with the help of mimikatz and others has shown the vulnerability of the Active Directory.

In this Master Class course, the attack scenarios on the Active Directory are first deeply examined and also carried out. With the knowledge gained from this, the Active Directory is now fundamentally hardened. This applies to existing installations, which should first be analyzed in depth, as well as new implementations, which are then completely hardened in order to be considered attack-proof in the future. The knowledge for this course was acquired in over 20 years of Active Directory experience, as well as in years of training by Paula Januszkiewicz and Sami Laiho, both world leaders in the field of security.

This course further incorporates the experience of over 50+ Active Directory concepts written by the instructor over his last 15 years - from SMB to enterprise level with 375,000 users. The topic of security is also being looked at in the direction of the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018.

We promise: Our best know-how for you and your daily work from our most experienced trainers and consultants.

Training Environment:

In the training environment, we work entirely with Hyper-V. For the proactive setup of the training environment, we use a Powershell script with which you can create new virtual machines in seconds. The script was developed by your trainer himself and enables the training setup according to the customer's wishes in extreme speed with little effort.

Hardware:

Each participant has a dedicated server in a data center with a total of 1 Gbit connection to the Internet. Each participant server is equipped as follows:

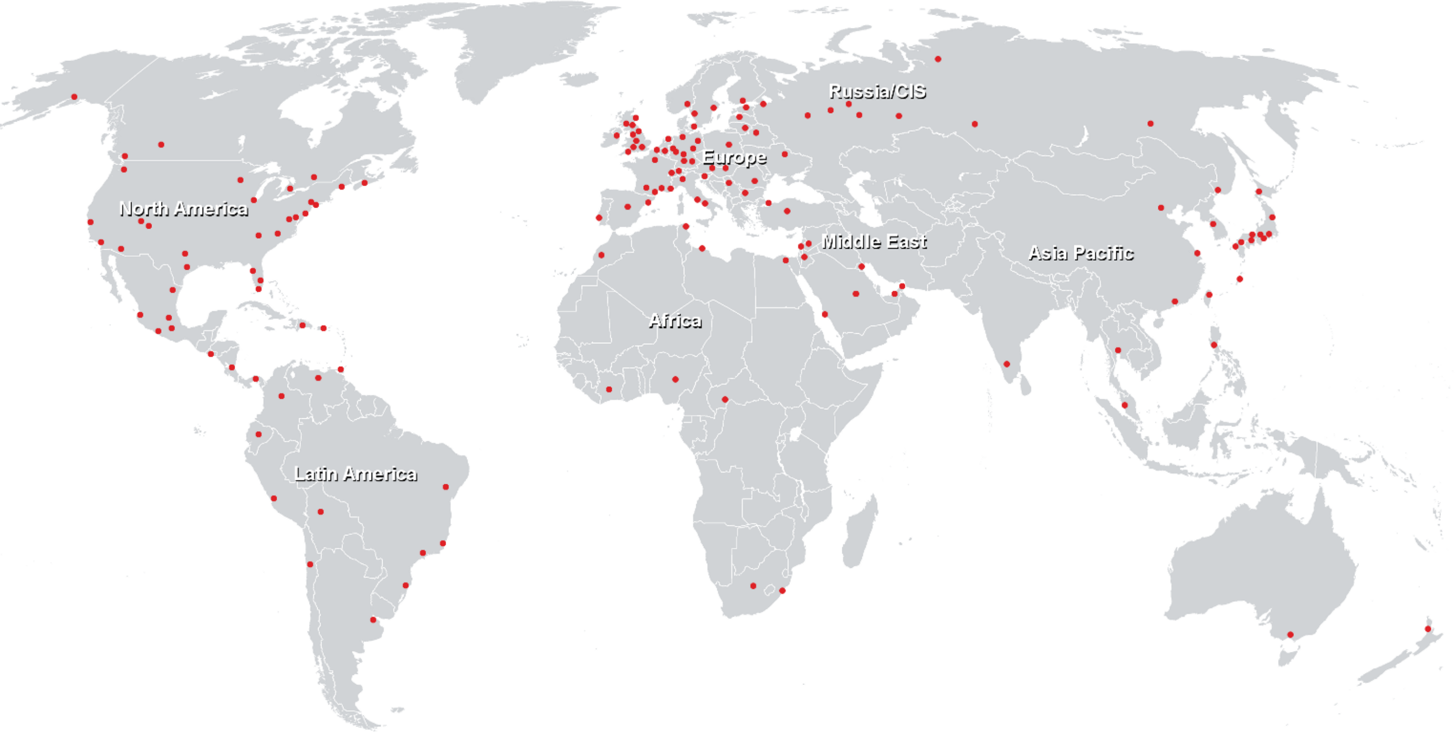
- 128 GB RAM
- at least 20 vCores
- 2 NVME-SSDs with at least 3,000 MB/s writing and at least 2,000 MB/s reading
- 1 Gbit to the Internet Total bandwidth

Content Outline

- Review of best practices for installing domain controllers from 20 years of experience as an ADDS senior consultant
- Homegrown security issues in Active Directory
    - Understanding Kerberos
    - NTLM vs. Kerberos
- SMB
    - SMB versions
    - Attack scenarios
    - Secure use of SMB
- PAC_Validation and the problems with the Microsoft implementation of Kerberos – in detail
- PTH – Pass the Hash – including live attack with all participants
- Silver Ticket
- Golden Ticket
- Skeleton Key
- Kerberos Ticket Service
    - Understanding Kerberos
    - Change Kerberos passwords: Why and how…
    - Changing Kerberos passwords: The silver bullet without failures
- Preventing credential theft – A DeepDive:
    - Attack Scenario
        - Pass-the-Hash
        - Silver ticket
        - GoldenTicket
        - Skeleton-Key
    - Prevent credential theft
        - Configure Windows Defender Credential Guard
        - Windows Defender Remote Credential Guard Bitlocker
        - Deploy Windows Defender Device Guard
        - Deploy AppLocker
        - Deploy Windows Defender Application Guard
- Understanding concepts:
    - Operating Tier.models
    - From Red-Forest, Golden-Forest and Bastion Forests
    - Highly secure single-domain model
- Clean installation source
    - Verify hash values of *.iso files
    - Fciv.exe, Powershell, 7zip and IgorHasher
- Set up the first domain controller
    - Understanding ms-ds-machineaccountquota
    - Use redircmp for new computer systems
    - Using redirusr for new users
    - Bitlocker
    - Bitlocker and TPM 1.2 vs. 2.0
    - Bitlocker and PreBoot authentication
    - AppLocker
    - Monitoring
        - AD-Audit-Plus
        - CyberArk
    - Secure backup and recovery of Bitlocker-protected backup volumes
    - Firewalling on domain controllers
    - Configuring IPSEC with RDP
    - Hardening domain controllers according to
        - Center of Internet Security
        - gpPack& PaT
        - SIM
        - LDA
        - Microsoft tools
- Setting up additional domain controllers
- Secure deployment of domain controllers, member servers and clients via MDT
    - Highly secure installation and configuration of MDT
    - Hardening of MDT servers
    - Rolling out highly secure member servers and clients
- Operating domain controllers securely via IPSEC
    - Configuring and using IPSEC
    - IPSEC monitoring via MMC
- Set up PKI server as internal Trusted ROOT CA
    - Configure PKI
    - Enable automatic certificate deployment via group policies
    - Enrolment of non-standard certificates
    - Hardening the PKI according to
        - Center of Internet Security
        - gpPack& PaT
        - SIM
        - LDA
        - Microsoft tools
- Jump Server and Privileged Access Workstation (PAW) – Understanding and implementing concepts
    - Setting up and configuring jump servers
        - RSAT installation
        - Install ADMIN Center with valid certificate of a Trusted Root PKI
        - Bitlocker

    - Bitlocker and TPM 1.2 vs. 2.0
    - Bitlocker and PreBoot authentication
    - AppLocker
    - Configuring IPSEC with RDP
    - Backup of Jump servers to bitlocker-protected volumes
    - Firewalling on JUMP servers
  - Hardening the Jump server according to
    - Center of Internet Security
    - gpPack& PaT
    - SIM
    - LDA
    - Microsoft tools
  - Set up and configure PAW
    - Bitlocker
    - Bitlocker and TPM 1.2 vs. 2.0
    - Bitlocker and PreBoot authentication
    - AppLocker
    - Configuring IPSEC and RDP
    - Backup of PAWs to bitlocker-protected volumes
    - Firewalling on PAWs
  - Hardening the domain controllers according to
    - Center of Internet Security
    - gpPack& PaT
    - SIM
    - LDA
    - Microsoft tools
- Security in domain networks
  - 802.1X with
    - MAC addresses
    - Certificates
  - MAC flooding on switches
    - Switch off hubbing mode
  - IPSEC with Kerberos and certificates
- Windows Defender Advanced Threat Protection (WDATP)
  - Understanding the concept of WDATP
  - Roll out and monitor WDATP
  - WDATP on domain controllers…
  - WDATP on Jump Servers and PAWs
  - WDATP on Windows 10 clients

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