Master Class: Workshop Microsoft PowerShell Advanced Security

ID MSPSAS **Price** CHF 4,390.—(excl. VAT) **Duration** 3 days

Who should attend

Administrators, IT decision-makers

Prerequisites

Workshop Microsoft PowerShell Fundamentals & Advanced Bundle (MSPSFA) or equivalent knowledge

Course Objectives

Workshop Microsoft PowerShell Fundamentals & Advanced Bundle (MSPSFA) or equivalent knowledge

Course Content

IT security – comprehensive analysis of potential security risks

- IT security is not an end in itself
- Classification of potential threats
- Risk management, cost-benefit analyses, and ROI assessment of security measures
- Implementation of the "defense in depth" concept
- The Pareto principle in IT security
- Security as a process
- Attack Tactics and Privilege Escalation
- Security by obscurity vs. KISS

The architecture of PowerShell and its potential vulnerability

- The role and development of command line tools in the Microsoft context
- Comparison of the management approach in MS Windows and the MS Exchange Manage Shell
- Modular approach of PowerShell and object orientation
- Risk assessment compared to .cmd and .exe
- authentication

Clean Code vs. Obfuscation

- Clean code principles
- Code obfuscation techniques
- Aliases – Obfuscation with on-board tools
- Das Tool Invoke-Obfuscation
- Detecting obfuscation using statistical methods
- Code Encoding

Code-Injection und Execution in Memory

- Invoke-Expression
- Executing code from the on-board help
- Functions with untested parameters
- In-Memory-Execution durch Remote-Code

Credentials

- Handling secure strings and PSCredential objects
- Secure credentials with certificates
    - Fundamentals of Public Key Infrastructure
    - Store credentials in encrypted form (certificate)
    - Use encrypted credentials for remote sessions
- Credentials für Remote Scripts
- Credentials für Scheduled Jobs

Elevation

- Running script code in the LocalSystem context
- Self-Elevator

Is co-signed

- Management of the PowerShell code signature
- PKI requirements
- Code signing

AppLocker

- The design of Applocker implementation guidelines
- Bypass Applocker script rules
- Managing Applocker through Powershell

Powershell Logging

- Types and application scenarios of logging
- Transcript
- Over-the-shoulder-Transcription via GPO
- Powershell Output-Streams
- Deep script block logging in the event log

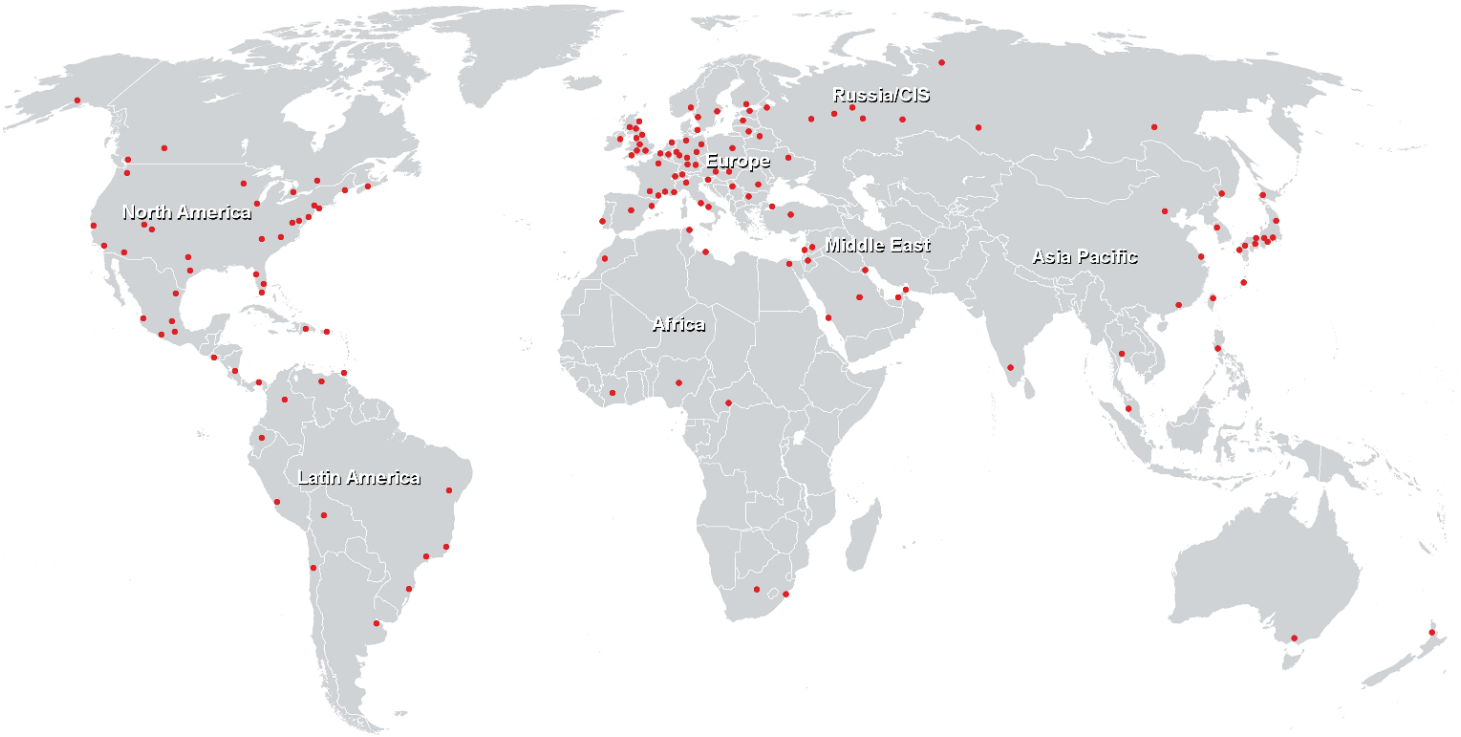
Master Class: Workshop Microsoft PowerShell Advanced Security (MSPSAS)

Just-Enough-Administration

- The principle of least privilege
- PowerShell Constrained Language Mode
- What is JEA?
- PS Session Config und Role Capabilities
- Setting up and testing the JEA configuration

Master Class: Workshop Microsoft PowerShell Advanced Security (MSPSAS)

Training Centres worldwide





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