# Master Class: Workshop Microsoft PowerShell Advanced Security

**ID** MSPSAS **Preis** auf Anfrage **Dauer** 3 Tage

## Zielgruppe

Administratoren, IT-Entscheider

## Voraussetzungen

Workshop Microsoft PowerShell Grundlagen & Aufbau Bundle (MSPSFA) oder äquivalentes Wissen

## Kursinhalt

### IT-Sicherheit – ganzheitliche Analyse potenzieller Sicherheitsrisiken

- IT-Sicherheit ist kein Selbstzweck
- Klassifizierung der möglichen Bedrohungen
- Risiko-Management, Cost-Benefit-Analysen und ROI-Bewertung von Sicherheitsmassnahmen
- Umsetzung des „Defense in depth“-Konzepts
- Das Pareto-Prinzip in der IT-Sicherheit
- Security als Prozess
- Angriffstaktiken und Privilege Escalation
- Security by obscurity vs. KISS

### Die Architektur der Powershell und ihre mögliche Vulnerabilität

- Die Rolle und Entwicklung der Kommandozeilen-Werkzeuge im Microsoft-Kontext
- Vergleich des Management-Ansatzes bei MS-Windows und der MS-Exchange-Manage-Shell
- Modularer Ansatz der Powershell und Objektorientierung
- Risikobewertung im Vergleich zu .cmd und .exe
- Authentifizierung

### Clean Code vs. Obfuscation

- Clean-Code Prinzipien
- Techniken der Code-Verschleierung
- Aliases – Obfuscation mit Bordmitteln
- Das Tool Invoke-Obfuscation
- Obfuscation mit statistischen Mitteln erkennen
- Code Encoding

### Code-Injection und Execution in Memory

- Invoke-Expression
- Ausführen von Code aus der Bordhilfe
- Functions mit ungeprüften Parametern
- In-Memory-Execution durch Remote-Code

### Credentials

- Handling von Secure Strings und PSCredential-Objekten
- Credentials mit Zertifikaten sichern
    - Grundlagen der Public Key Infrastructure
    - Credentials verschlüsselt speichern (Zertifikat)
    - Verschschlüsselte Credentials für Remote Sessions einsetzen
- Credentials für Remote Scripts
- Credentials für Scheduled Jobs

### Elevation

- Running Script-Code im LocalSystem-Kontext
- Self-Elevator

### Codesignatur

- Management der Powershell Codesignatur
- Anforderungen an die PKI
- Signieren von Code

### Applocker

- Das Design von Applocker-Ausführungsrichtlinien
- Applocker Script-Regeln umgehen
- Managing Applocker durch Powershell

### Powershell Logging

- Arten und Einsatzszenarien des Logging
- Transcript
- Over-the-shoulder-Transcription via GPO
- Powershell Output-Streams
- Deep Scriptblock Logging im Eventlog

### Just-Enough-Administration

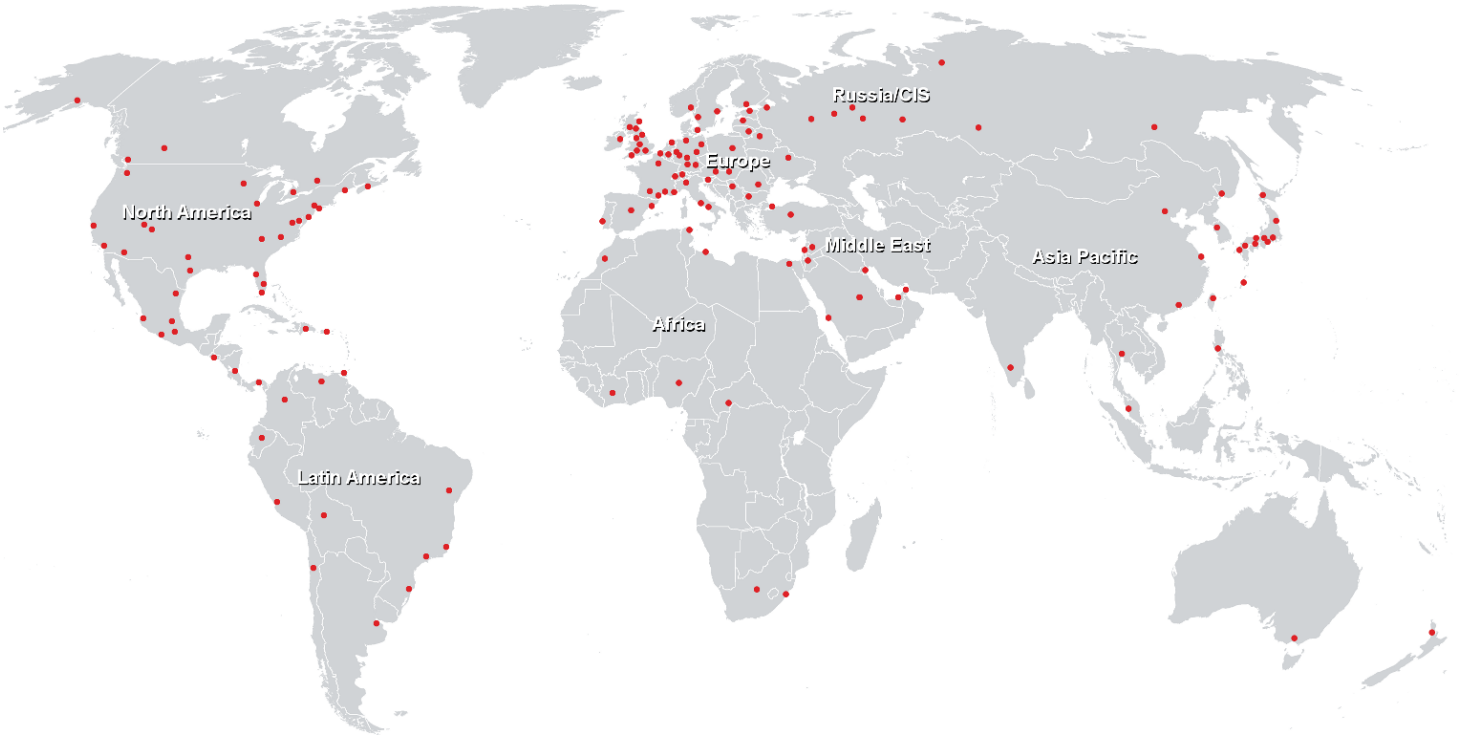
- Das Prinzip der geringsten Privilegien
- PowerShell Constrained Language Mode

# Master Class: Workshop Microsoft PowerShell Advanced Security (MSPSAS)

- Was ist JEA?
- PS Session Config und Role Capabilities
- Einrichten und Testen der JEA-Konfiguration

# Master Class: Workshop Microsoft PowerShell Advanced Security (MSPSAS)

**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**