Master Class: Windows Security and Infrastructure Management with Windows Internals (WSI)

ID WSI **Price** 3,000.— €(excl. tax) **Duration** 4 days

Course Overview

This is a 4-day deep dive course on Windows Security and Infrastructure Management with Windows Internals, ideal for Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants, and other people responsible for implementing network and perimeter security.

It is delivered by one of the best people in the market in the security field and what is more, this is an international Live Virtual Class so you will be able to share the learning experience with a group of IT pros from around the world without leaving your home or office!

Who should attend

The course is perfect for enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants.

Prerequisites

To attend this training, you should have a good hands-on experience in administering Windows infrastructure. At least 5 years in the field is recommended.

Course Objectives

During this 4-day course in 28 hours of super intensive training you will gain crucial cybersecurity knowledge and skills in Windows Security and Infrastructure Management with Windows Internals. Moreover, you will be able to:

- Get the highest quality and unique learning experience – the class is limited to 12 participants by default.
- Get the opportunity to interact with our world-renowned Experts.
- Go through CQURE's custom lab exercises and practice them after the course.
- Receive a lifelong certification after completing the course!

Course Content

- Windows Internals & System Architecture
- Process and Thread Management
- System Security Mechanisms
- Debugging & Auditing
- Memory Analysis
- Storage Management
- Startup and Shutdown
- Infrastructure Security Solutions
- Layered Network Services
- Monitoring and Event Tracing
- Points of Entry Analysis

Detailed Course Outline

Module 1:Windows Internals & System Architecture

- Introduction to the Windows 10 and Windows Server 2019 security concepts
- Architecture overview and terms
- Key System Components
- Advanced Local Procedure Call
- Information gathering techniques

Module 2: Process and Thread Management

- Process and thread internals
- Protected processes
- Process priority management
- Examining Thread Activity
- Process and thread monitoring and troubleshooting techniques (advanced usage of Process Explorer, Process Monitor, and other tools)

Module 3: System Security Mechanisms

- Integrity Levels
- Session Zero

- Privileges, permissions and rights
- Passwords security (techniques for getting and cracking passwords)
- Registry Internals
- Monitoring Registry Activity
- Driver signing (Windows Driver Foundation)
- User Account Control Virtualization
- System Accounts and their functions
- Boot configuration
- Services architecture
- Access tokens
- Biometric framework for user authentication

Module 4: Debugging & Auditing

- Available debuggers
- Working with symbols
- Windows Global Flags
- Process debugging
- Kernel-mode debugging
- User-mode debugging
- Setting up kernel debugging with a virtual machine as the target
- Debugging the boot process
- Crash dump analysis
- Direct Kernel Object Manipulation
- Finding hidden processes
- Rootkit Detection

Module 5: Memory Analysis

- Memory acquisition techniques
- Finding data and activities in memory
- Step-by-step memory analysis techniques
- Tools and techniques to perform memory forensic

Module 6: Storage Management

- Securing and monitoring Files and Folders
- Protecting Shared Files and Folders by Using Shadow Copies
- Implementing Storage Spaces
- Implementing iSCSI
- Implementing FSRM, managing Quotas, File Screens, and Storage Reports
- Implementing Classification and File Management Tasks, Dynamic Access Control
- Configuring and troubleshooting Distributed File System

Module 7: Startup and Shutdown

- Boot Process overview
- BIOS Boot Sector and Bootmgr vs. the UEFI Boot Process
- Booting from iSCSI
- Smss, Csrss, and Wininit
- Last Known Good configuration
- Safe Mode capabilities
- Windows Recovery Environment (WinRE)
- Troubleshooting Boot and Startup Problems

Module 8: Infrastructure Security Solutions

- Windows Server Core Improvements in Windows Server 2019
- AppLocker implementation scenarios
- Advanced BitLocker implementation techniques (provisioning, Standard User Rights and Network Unlock?
- Advanced Security Configuration Wizard
- IPSec
- Advanced GPO Management
- Practicing Diagnostic and Recovery Toolkit
- Tools

Module 9: Layered Network Services

- Network sniffing techniques
- Fingerprinting techniques
- Enumeration techniques
- Networking Services Security (DNS, DHCP, SNMP, SMTP and other)
- Direct Access
- High Availability features: cluster improvements and SMB ?Scale – Out File Server)
- Network Load Balancing

Module 10: Monitoring and Event Tracing

- Windows Diagnostic Infrastructure
- Building auditing
- Expression?based audit policies
- Logging Activity for Accounts and processes
- Auditing tools, techniques and improvements
- Auditing removable storage devices

Module 11: Points of Entry Analysis

- Offline access
- Kali Linux /other tools vs. Windows Security
- Unpatched Windows and assigned attacks
- Domain Controller attacks
- Man?in?the Middle attacks
- Services security

About Fast Lane

Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services

- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Worldwide Presence

with high-end training centers around the globe

Multiple Awards

from vendors such as AWS, Microsoft, Cisco, Google, NetApp, VMware

Experienced SMEs

with over 19.000 combined certifications

Germany
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610

info@flane.de / www.flane.de

Austria
ITLS GmbH
(Partner of Fast Lane)
Tel. +43 1 6000 8800

info@itls.at / www.itls.at

Switzerland
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080

info@flane.ch / www.flane.ch