Windows 11/10 - application troubleshooting, whitelisting and fighting malware

Course code: GOC12

This four-days instructor-led course gives students understanding of Win32, .NET and .NET core and UWP applications and understanding of how malware spreads, how it infects systems and how it hides inside. The training covers methods of application troubleshooting and also protection methods that can minimize malware spreading or its gains.

Prerequisities

Knowledge in extent of the courses which are listed in the bellow sections Previous Courses and Related Courses

Good understanding of TCP/IP and DNS technologies

Course outline

Introduction to Windows architecture

Processes and threads

Process and kernel memory management

Local Security Authority (LSASS)

Security subsystem, user identity and auditing

Application monitoring

SysInternals tools

Process Explorer (procexp)

Process Monitor (procmon)

Toolkit PSTools

Autoruns tool and its avoidance

User Account Control (UAC)

Application compatibility

64-bit platform and WOW (Windows on Windows)

.NET and .NET core platform and PowerShell

Older built-in scripting language VBScript

Today's malware and its spreading

Malware under limited accounts and its abilities

Software keyloggers and GUI click-jacking

Malware as web browser plug-ins

Rootkits and RootkitRevealer

Antimalware technology options

Mandatory Access Control

Data Execution Prevention

Service Hardening

Windows Firewall

Software Restriction Policies and application whitelisting

AppLocker and application whitelisting

Powershell auditing and blocking

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Windows 11/10 - application troubleshooting, whitelisting and fighting malware

Monitoring application usage and auditing

Preparation for Microsoft certification

Most Microsoft certification exams do not require students to attend an official MOC course in order to pass the exam.

This applies to all certifications except for MCM

Official Microsoft MOC courses as well as our own GOC courses are good ways of preparation for Microsoft certifications such as MCP, MTA, MCSA, MCSE or MCM

This does not mean that official MOC courses would serve as the only necessary praparation. The primary goal of an MOC course is to provide for sufficient theoretical knowledge and practical experience to effectively work with the related product

MOC courses usually cover most of the topics required by their respective certification exams, but often do not give every topic the same amount of time and emphassis as may be required to completelly pass the exam

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk