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

Kód kurzu: GOC12

V tomto špičkovém čtyřdenním kurzu získají účastníci znalosti nezbytné pro řešení problémů s během Win32, NET a NET core i UWP aplikací a porozumnění fungování malware a metodám jeho pronikání a skrývání se. Zaměříme se především na objasnění funkcí OS, které mají na běh aplikací vliv, a na praktické postupy při řešení problému s jejich provozem. Nezapomeneme se take věnovat technologiím, které by měly omezit či zabránit spuštění aplikací, jež jsou pro běh OS nebezpečné.

Předpokládané vstupní znalosti

Znalosti v rozsahu kurzů uvedených v sekcích Předchozí kurzy a Související kurzy

Dobrá znalost technologií TCP/IP a DNS

Osnova kurzu

Úvod do architektury Windows

Procesy a vlákna (thread)

Memory management procesů

Local Security Authority (LSASS)

Bezpečnostní subsystém a identita, auditování

Aplikační monitoring

Nástroje Sysinternals

Nástroj process explorer (procexp)

Nástroj process monitor (procmon)

Nástroje z balíku PSTools

Autoruns a jejich obcházení

Aplikační troubleshooting

User Account Control (UAC)

Compatibility aplikací

64-bit platforma, WOW (Windows on Windows)

.NET a .NET core platforma, PowerShell

Starší zabudovaný scriptovací jazyk VBScript

Dnešní malware a jeho pronikání

Malware pod obyčejným uživatelem a jeho možnosti

Software keyloggery, GUI click-jacking

Škodlivé plug-in součásti prohlížečů

Rootkity a RootkitRevealer

Možnosti ochrany proti malware

Mandatory Access Control

Data Execution Prevention

Service Hardening

Windows Firewall

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

Software restriction policies a aplikační whitelisting

AppLocker a aplikační WhiteListing

Blokování PowerShellu

Sledování běhu aplikací a auditování

Příprava k certifikačním zkouškám

U certifikačních zkoušek Microsoft platí, že kromě certifikací MCM, není účast na oficiálním MOC kurzu nutnou podmínkou pro složení zkoušky

Oficiální kurzy MOC firmy Microsoft i naše vlastní kurzy GOC jsou vhodnou součástí přípravy na certifikační zkoušky firmy Microsoft, jako jsou MTA, MCP, MCSA, MCSE, nebo MCM

Primárním cílem kurzu ovšem není přímo příprava na certifikační zkoušky, ale zvládnutí teoretických principů a osvojení si praktických dovedností nutných k efektivní práci s daným produktem

MOC kurzy obvykle pokrývají téměř všechny oblasti, požadované u odpovídajících certifikačních zkoušek. Jejich probrání na kurzu ale nebývá dán vždy přesně stejný čas a důraz, jako vyžaduje certifikační zkouška

Jako další přípravu k certifikačním zkouškám lze využít například knihy od MS Press (tzv. Self-paced Training Kit) i elektronický self-test software

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