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

Kód kurzu: GOC12

Na tomto špičkovom štvordennom kurze získajú účastníci vedomosti nevyhnutné na riešenie problémov s behom Win32, NET a NET core a UWP aplikácií a porozumenie fungovania malware a metódam jeho prenikania a skrývania sa. Zameriame sa predovšetkým na objasnenie funkcií OS, ktoré majú na beh aplikácií vplyv a na praktické postupy pri riešení problémov s ich prevádzkou. Nezabudneme sa tiež venovať technológiám, ktoré by mali obmedziť či zabrániť spusteniu aplikácií, ktoré sú pre beh OS nebezpečné.

Požadované vstupné znalosti

Znalosti v rozsahu kurzov uvedených v sekciách Predchádzajúce kurzy a Súvisiace kurzy

Dobrá znalosť technológií TCP/IP a DNS

Osnova kurzu

- Úvod do architektúry Windows
- Procesy a vlákna (thread)
- Memory management procesov
- Local Security Authority (LSASS)
- Bezpečnostný subsystém a identita, auditovanie
- Aplikačný monitoring
- Nástroje Sysinternals
- Nástroj process explorer (procexp)
- Nástroj process monitor (procmon)
- Nástroje z balíku PSTools
- Autoruns a ich obchádzanie
- Aplikačný troubleshooting
- User Account Control (UAC)
- Compatibility aplikácií
- 64-bit platforma, WOW (Windows on Windows)
- .NET a .NET core platforma, PowerShell
- Starší zabudovaný scriptovací jazyk VBScript
- Dnešný malware a jeho pronikanie
- Malware pod obyčajným užívateľom a jeho možnosti
- Software keyloggery, GUI click-jacking
- Škodlivé plug-in súčasti prehliadačov
- Rootkity a RootkitRevealer
- Možnosti ochrany proti malware
- Mandatory Access Control
- Data Execution Prevention
- Service Hardening
- Windows Firewall
- Software restriction policies a aplikačný whitelisting
- AppLocker a aplikačný WhiteListing
- Blokovanie PowerShellu
- Sledovanie behu aplikácií a auditovanie

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