

Masterclass: PowerShell for Digital Investigation & Threat Hunting

Cursusduur: 4 Dagen Cursuscode: PST Trainingsmethode: Virtual Learning

Beschrijving:

This advanced course equips cybersecurity professionals with the skills to detect, investigate, and respond to modern threats using native Windows tools and PowerShell. With a strong focus on real-world attacker behaviors, participants will learn to identify Advanced Persistent Threats (APTs), analyze attack timelines, and uncover hidden or deleted artifacts using forensic techniques. PowerShell is used throughout the course as both a defensive and investigative tool, supporting artifact collection, process and network analysis, registry inspection, and script-based detection. Participants will explore common attacker techniques such as living-off-the-land binaries (LOLBins), scheduled tasks, and encoded payloads, and learn how to detect and counter them through logging, event analysis, and behavioral detection rules.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Doelgroep:

This course is designed for security professionals across offensive, defensive, and hybrid roles. Analysts, hunters, SOC teams, and incident responders will learn to enhance investigations with AI-driven workflows. Red and purple teamers will strengthen adversary emulation and detection validation, while engineers and developers gain hands-on experience building AI-powered tools, pipelines, and multi-agent systems. Security leaders and architects will benefit from practical insights into securing AI systems and addressing emerging vulnerabilities.

Doelstelling:

- Investigate advanced persistent threats (APTs) using PowerShell and native Windows tools.
- Perform digital forensics and artifact collection for incident investigations.
- Analyze process, network, and registry artifacts to identify malicious activity.
- Implement PowerShell logging, detection, and threat hunting techniques.
- Conduct Active Directory enumeration and investigate fileless attacks.
- Apply real-world threat hunting and incident response techniques through hands-on exercises.

Vereiste kennis en vaardigheden:

- Basic understanding of Windows systems and cybersecurity fundamentals
- Familiarity with PowerShell, networking, and Active Directory is recommended
- Prior experience in system or security administration is an advantage

Examens en certificering

- After completing the course, participants will receive a CQURE Certificate of Completion and will also be eligible for CPE points.

Cursusinhoud:

Module 1: APT Attacks ; Investigation	Module 5: Process ; Network Artifact Collection	Module 9: Hands-On Threat Hunting Case Study
Module 2: PowerShell 101 for Blue Teams	Module 6: PowerShell Logging ; Detection	Module 10: Active Directory Enumeration with PowerShell
Module 3: Understanding Information Gathering and Timelining	Module 7: Threat Hunting with WMI ; Scheduled Tasks	Module 11: Red Teaming Tactics with PowerShell
Module 4: PowerShell for Digital Forensics ; Artifact Collection	Module 8: PowerShell for Enterprise	Module 12: Complete Fileless Attack Analysis Walkthrough

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein