Masterclass: Threat Hunting with AI

Duration: 3 Days **Course Code: TAI** **Delivery Method: Virtual Learning**

Overview:

Our Threat Hunting with AI Support course is designed for Security Analysts, IT Administrators, Incident Responders and Threat Hunters. During the course participants will learn modern attack techniques, local privilege escalation methods, and identity infrastructure attacks, as well as ways these attacks can be detected and mitigated. This knowledge is enhanced with case studies demonstrating how real-world attacks occur using the methods learned. Additionally, participants will be introduced to solutions that, with AI support, can enhance the threat hunting process. The course concludes by showcasing how threat hunting and threat detection design can be performed using both manual and automated methods.

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.

Target Audience:

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.

Objectives:

- Understand modern attack techniques and how they are executed and detected
- Identify and investigate privilege escalation and identity-based attacks
- Understand Windows authentication architecture and common exploitation paths
- Apply structured investigation methods using real-world case studies
- Use Microsoft Defender for Endpoint (EDR) for threat detection and hunting
- Detect and analyze attacks on identity infrastructure
- Perform basic network, memory, and disk forensic analysis
- Leverage Microsoft Sentinel and Security Copilot in threat detection and investigation
- Combine manual and AI-assisted methods to improve threat hunting and response

Prerequisites:

- Familiarity with cybersecurity concepts and attack/defense basics
- Basic understanding of Windows environments, identity systems, and enterprise IT
- Comfort with tools like PowerShell, logging, and security monitoring (implied from content like EDR, AD, forensics)

Testing and Certification

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

Content:

- Module 1: Modern Attack Techniques and Tracing Them
- Module 2: Local Privilege Escalation Techniques and Tracing Them
- Module 3: Case Study – Investigating In-Place Attacks
- Module 4: Windows Authentication Architecture ; Cryptography
- Module 5: Case Study – Investigating Identity Theft
- Module 6: Attacks on Identity Infrastructure and Tracing Them
- Module 7: Microsoft 365 Defender for Endpoint (EDR)
- Module 8: Security Operations with Microsoft EDR (Defender for Endpoint) – Advanced Threat Hunting with Defender
- Module 9: Microsoft Security Copilot
- Module 10: Case Study – Detecting a Complex Threat with Microsoft Sentinel and Microsoft Copilot for Security
- Module 11: Network Forensics and Monitoring
- Module 12: Memory Dumping and Analysis
- Module 13: Disk Dumping and Analysis

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/