

Masterclass: AI Agents for Attack Investigation

Cursusduur: 3 Dagen Cursuscode: AIA Trainingsmethode: Virtual Learning

Beschrijving:

In this course, Participant will gain crucial cybersecurity knowledge and skills in terms of AI Agents for Attack Investigation. They 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.

This course is based on practical knowledge from tons of successful projects, many years of real-world experience and no mercy for misconfigurations or insecure solutions! All exercises are based on Windows Server, Windows 10, Kali Linux, and Ubuntu.

During this course, you will have the opportunity to go through CQURE's custom lab exercises, interact with our world-renowned Expert and receive a lifelong certification after completing the course.

Doelgroep:

This course is designed for security professionals across offensive, defensive, and hybrid roles. Analysts, hunters, SOC teams, and incident responders

Doelstelling:

- How-to build custom AI agents to support security investigations
- Implement Retrieval-Augmented Generation (RAG) systems for effective knowledge management
- Development and deployment of multi-agent systems using CrewAI
- Creation of n8n workflows
- How to implement security controls for AI systems
- Address AI-specific vulnerabilities with practical mitigation strategies

Vereiste kennis en vaardigheden:

Participants are recommended to have the following:

Basic understanding of security concepts such as networks, endpoints, threats, and vulnerabilities

Basic Knowledge of Programming/Scripting

General awareness of concepts such as machine learning, automation, or data analysis

Examens en certificering

■

Cursusinhoud:

Module 1: APT Attacks ; MITRE ATT;CK	Module 6: Introduction to RAG	Module 11: CrewAI and Multi-Agent Models
Module 2: Introduction to AI	Module 7: Advanced RAG Methodologies	Module 12: Introduction to n8n
Module 3: Python Fundamentals for Security	Module 8: Tool Calling ; Memory Management	Module 13: Multimodal AI Agents
Module 4: Log Analysis with Sysmon	Module 9: Domain Investigation Agent	■ Module 14: AI Red Teaming ; Security
Module 5: Building Your First AI Model with LangChain	Module 10: LangChain ; ReAct Model	

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