

Masterclass: AI Agents for Attack Investigation

Duration: 3 Days Course Code: AIA Delivery Method: Virtual Classroom

Overview:

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.

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

Objectives:

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

Prerequisites:

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

Testing and Certification

- After finishing the course, you will be granted a CQURE Certificate of Completion. Please note that after completing the course you will also be eligible for CPE points!

Content:

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	

Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278

training@globalknowledge.com.sa

www.globalknowledge.com/en-sa/

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Worood, Riyadh 3140, Saudi Arabia