AI+ Security: Level 2

Category: AI, Data & Analytics | **Vendor:** AI Certs

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	AI+ Security: Level 2
Related Exam:	AI+ Security: Level 2

Course Overview

AI+ Security Level 2 offers professionals a thorough exploration of the integration of AI and Cybersecurity. Beginning with fundamental Python programming tailored for AI and Cybersecurity applications, participants delve into essential AI principles before applying machine learning techniques to detect and mitigate cyber threats, including email threats, malware, and network anomalies. Advanced topics such as user authentication using AI algorithms and the application of Generative Adversarial Networks (GANs) for Cybersecurity purposes are also covered, ensuring participants are equipped with cutting-edge knowledge. Practical application is emphasized throughout, culminating in a Capstone Project where attendees synthesize their skills to address real-world cybersecurity challenges, leaving them adept in leveraging AI to safeguard digital assets effectively.

About This Course

AI+ Security Level 2 offers professionals a thorough exploration of the integration of AI and Cybersecurity. Beginning with fundamental Python programming tailored for AI and Cybersecurity applications, participants delve into essential AI principles before applying machine learning techniques to detect and mitigate cyber threats, including email threats, malware, and network anomalies. Advanced topics such as user authentication using AI algorithms and the application of Generative Adversarial Networks (GANs) for Cybersecurity purposes are also covered, ensuring participants are equipped with cutting-edge knowledge. Practical application is emphasized throughout, culminating in a Capstone Project where attendees synthesize their skills to address real-world cybersecurity challenges, leaving them adept in leveraging AI to safeguard digital assets effectively.

Who Should Attend

Security Analyst

Prerequisites & Entry Requirements

General Prerequisites:

Basic Python Skills: Familiarity with Python basics, including variables, loops, and functions, Basic Cybersecurity: Basic understanding of cybersecurity principles, such as the CIA triad and common cyber threats, Basic Machine Learning Awareness: General awareness about machine learning, no technical skills required, Basic Networking Knowledge: Understanding of IP addresses and how the internet works, Basic command line Skills: Comfort using the command line like Linux or Windows termil for basic tasks, Interest in AI for Security: Willingness to explore how AI can be applied to detect and mitigate security threats

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Course Objectives

- AI-Driven Threat Detection
- Application of Machine Learning in Cybersecurity
- Enhanced User Authentication Methods
- AI-Enhanced Penetration Testing

Detailed Course Outline

- Introduction to Artificial Intelligence (AI) and Cyber Security

  Understanding the Cyber Security Artificial Intelligence (CSAI) An Introduction to AI and its Applications in Cybersecurity Overview of Cybersecurity Fundamentals Identifying and Mitigating Risks in Real-Life Building a Resilient and Adaptive Security Infrastructure Enhancing Digital Defenses using CSAI

- Python Programming for AI and Cybersecurity Professionals

  Python Programming Language and its Relevance in Cybersecurity Python Programming Language and Cybersecurity Applications AI Scripting for Automation in Cybersecurity Tasks Data Analysis and Manipulation Using Python Developing Security Tools with Python

- Application of Machine Learning in Cybersecurity

  Understanding the Application of Machine Learning in Cybersecurity Anomaly Detection to Behaviour Analysis Dynamic and Proactive Defense using Machine Learning Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats

- Detection of Email Threats with AI

  Utilizing Machine Learning for Email Threat Detection Analyzing Patterns and Flagging Malicious Content Enhancing Phishing Detection with AI Autonomous Identification and Thwarting of Email Threats Tools and Technology for Implementing AI in Email Security

- AI Algorithm for Malware Threat Detection

Introduction to AI Algorithm for Malware Threat Detection Employing Advanced Algorithms and AI in Malware Threat Detection Identifying, Analyzing, and Mitigating Malicious Software Safeguarding Systems, Networks, and Data in Real-time Bolstering Cybersecurity Measures Against Malware Threats Tools and Technology: Python, Malware Analysis Tools

- Network Anomaly Detection using AI

Utilizing Machine Learning to Identify Unusual Patterns in Network Traffic Enhancing Cybersecurity and Fortifying Network Defenses with AI Techniques Implementing Network Anomaly Detection Techniques

- User Authentication Security with AI

Introduction Enhancing User Authentication with AI Techniques Introducing Biometric Recognition, Anomaly Detection, and Behavioural Analysis Providing a Robust Defence Against Unauthorized Access Ensuring a Seamless Yet Secure User Experience Tools and Technology: AI-based Authentication Platforms Conclusion

- Generative Adversarial Network (GAN) for Cyber Security

Introduction to Generative Adversarial Networks (GANs) in Cybersecurity Creating Realistic Mock Threats to Fortify Systems Detecting Vulnerabilities and Refining Security Measures Using GANs Tools and Technology: Python and GAN Frameworks

- Penetration Testing with Artificial Intelligence

Enhancing Efficiency in Identifying Vulnerabilities Using AI Automating Threat Detection and Adapting to Evolving Attack Patterns Strengthening Organizations Against Cyber Threats Using AI-driven Penetration Testing Tools and Technology: Penetration Testing Tools, AI-based Vulnerability Scanners

- Capstone Project

Introduction Use Cases: AI in Cybersecurity Outcome Presentation

- Introduction to Artificial Intelligence (AI) and Cyber Security

Understanding the Cyber Security Artificial Intelligence (CSAI) An Introduction to AI and its Applications in Cybersecurity Overview of Cybersecurity Fundamentals Identifying and Mitigating Risks in Real-Life Building a Resilient and Adaptive Security Infrastructure Enhancing Digital Defenses using CSAI

- Introduction to Artificial Intelligence (AI) and Cyber Security

  Understanding the Cyber Security Artificial Intelligence (CSAI) An Introduction to AI and its Applications in Cybersecurity Overview of Cybersecurity Fundamentals Identifying and Mitigating Risks in Real-Life Building a Resilient and Adaptive Security Infrastructure Enhancing Digital Defenses using CSAI

- Python Programming for AI and Cybersecurity Professionals

  Python Programming Language and its Relevance in Cybersecurity Python Programming Language and Cybersecurity Applications AI Scripting for Automation in Cybersecurity Tasks Data Analysis and Manipulation Using Python Developing Security Tools with Python

- Application of Machine Learning in Cybersecurity

  Understanding the Application of Machine Learning in Cybersecurity Anomaly Detection to Behaviour Analysis Dynamic and Proactive Defense using Machine Learning Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats

- Detection of Email Threats with AI

  Utilizing Machine Learning for Email Threat Detection Analyzing Patterns and Flagging Malicious Content Enhancing Phishing Detection with AI Autonomous Identification and Thwarting of Email Threats Tools and Technology for Implementing AI in Email Security

- AI Algorithm for Malware Threat Detection

  Introduction to AI Algorithm for Malware Threat Detection Employing Advanced Algorithms and AI in Malware Threat Detection Identifying, Malware Analysis Tools

- Network Anomaly Detection using AI

  Utilizing Machine Learning to Identify Unusual Patterns in Network Traffic Enhancing Cybersecurity and Fortifying Network Defenses with AI Techniques Implementing Network Anomaly Detection Techniques

- Network Anomaly Detection using AI

  Utilizing Machine Learning to Identify Unusual Patterns in Network Traffic Enhancing Cybersecurity and Fortifying Network Defenses with AI Techniques Implementing Network Anomaly Detection Techniques

- User Authentication Security with AI

Introduction Enhancing User Authentication with AI Techniques Introducing Biometric Recognition, AI-based Vulnerability Scanners

- Capstone Project

Introduction Use Cases: AI in Cybersecurity Outcome Presentation

, Introduction to Artificial Intelligence (AI) and Cyber Security, Python Programming for AI and Cybersecurity Professionals, Application of Machine Learning in Cybersecurity, Detection of Email Threats with AI, AI Algorithm for Malware Threat Detection, Network Anomaly Detection using AI, User Authentication Security with AI, Generative Adversarial Network (GAN) for Cyber Security, Penetration Testing with Artificial Intelligence, Capstone Project, Optional Module: AI Agents for Security Level 2

□□ Certification Path

AI+ Security: Level 2

Exam: AI+ Security: Level 2

Additional Course Details

Nexus Humans AI+ Security: Level 2 training program is a workshop that presents an invigorating mix of sessions, lessons, and masterclasses meticulously crafted to propel your learning expedition forward.

This immersive bootcamp-style experience boasts interactive lectures, hands-on labs, and collaborative hackathons, all strategically designed to fortify fundamental concepts.

Guided by seasoned coaches, each session offers priceless insights and practical skills crucial for honing your expertise. Whether you're stepping into the realm of professional skills or a seasoned professional, this comprehensive course ensures you're equipped with the knowledge and prowess necessary for success.

While we feel this is the best course for the AI+ Security: Level 2 course and one of our Top 10 we encourage you to read the course outline to make sure it is the right content for you.

Additionally, private sessions, closed classes or dedicated events are available both live online and at our training centres in Dublin and London, as well as at your offices anywhere in the UK, Ireland or across EMEA.

Frequently Asked Questions

Q: What delivery options are available for AI+ Security: Level 2?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The AI+ Security: Level 2 course helps prepare you for the AI+ Security: Level 2 certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the AI+ Security: Level 2 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 5-day AI+ Security: Level 2 course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the AI+ Security: Level 2 training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for AI+ Security: Level 2?

Yes, we provide corporate training, dedicated training, and closed classes for AI+ Security: Level 2. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: AI+ Security: Level 2, AI Certs, vILT, AI+ Security

---

Q: Why choose Nexus Human for AI+ Security: Level 2?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your AI+ Security: Level 2 training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 14/11/2026.