# AI+ Security: Level 1

**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 1 |
| **Related Exam:** | AI+ Security: Level 1 |

## Course Overview

AI+ Security level 1 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 1 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

## Learning Outcomes

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

**Course Objectives**

- Automation of Security Processes
- Data Privacy and Compliance in AI Security
- Threat Detection and Response Using AI
- Real-Time Cyberattack Prevention with AI

## Detailed Course Outline

- Introduction to Cyber Security

  Definition and Scope of Cyber Security Key Cybersecurity Concepts CIA Triad (Confidentiality, Integrity, Availability) Cybersecurity Frameworks and Standards (NIST, ISO/IEC27001) Cyber Security Laws and Regulations (e.g., GDPR, HIPAA) Importance of Cybersecurity in Modern Enterprises Careers in Cyber Security

- Python Programming Fundamentals

  Introduction to Python Programming Understanding of Python Libraries Python Programming Language for Cybersecurity Applications AI Scripting for Automation in Cybersecurity Tasks Data Analysis and Manipulation Using Python Developing Security Tools with Python®

- Applications of AI in Cybersecurity

  Understanding the Application of Machine Learning in Cybersecurity Anomaly Detection to Behavior Analysis Dynamic and Proactive Defense using Machine Learning Utilizing Machine Learning for Email Threat Detection Enhancing Phishing Detection with A Autonomous Identification and Thwarting of Email Threats Employing Advanced Algorithms and AI in Malware Threat Detection Identifying, Analyzing, and Mitigating Malicious Software Enhancing User Authentication with AI Techniques Penetration Testing with AI®

- Incident Response and Disaster Recovery

Incident Response Process (Identification, Containment, Eradication, Recovery) Incident Response Lifecycle Preparing an Incident Response Plan Detecting and Analyzing Incidents Containment, and Recovery Post-Incident Activities Digital Forensics and Evidence Collection Disaster Recovery Planning (Backups, Business Continuity) Penetration Testing and Vulnerability Assessments Legal and Regulatory Considerations of Security Incidents®

- Open Source Security Tools

Introduction to Open-Source Security Tools Popular Open Source Security Tools Benefits and Challenges of Using Open-Source Tools Implementing Open Source Solutions in Organizations Community Support and Resources Network Security Scanning and Vulnerability Detection Security Information and Event Management (SIEM) Tools (Open-Source options) Open-Source Packet Filtering Firewalls Password Hashing and Cracking Tools (Ethical Use) Open-Source Forensics Tools®

- Securing the Future

Emerging Cyber Threats and Trends Artificial Intelligence and Machine Learning in Cybersecurity Blockchain for Security Internet of Things (IoT) Security Cloud Security Quantum Computing and its Impact on Security Cybersecurity in Critical Infrastructure Cryptography and Secure Hashing Cyber Security Awareness and Training for Users Continuous Security Monitoring and Improvement®

- Capstone Project

Introduction Use Cases: AI in Cybersecurity Outcome Presentation®

- Operating System Fundamentals

Core OS Functions (Memory Management, Process Management) User Accounts and Privileges Access Control Mechanisms (ACLs, DAC, MAC) OS Security Features and Configurations Hardening OS Security (Patching, Disabling Unnecessary Services) Virtualization and Containerization Security Considerations Secure Boot and Secure Remote Access OS Vulnerabilities and Mitigations®

- Networking Fundamentals

Network Topologies and Protocols (TCP/IP, OSI Model) Network Devices and Their Roles (Routers, Switches, Firewalls) Network Security Devices (Firewalls, IDS/IPS) Network Segmentation and Zoning Wireless Network Security (WPA2, Open WEP vulnerabilities) VPN Technologies and Use Cases Network Address Translation (NAT) Basic Network Troubleshooting®

- Threats, Vulnerabilities, and Exploits

Types of Threat Actors (Script Kiddies, Hacktivists, Nation-States) Threat Hunting Methodologies using AI AI Tools for Threat Hunting (SIEM, IDS/IPS Open-Source Intelligence (OSINT) Techniques Introduction to Vulnerabilities Software Development Life Cycle (SDLC) and Security Integration with AI Zero-Day Attacks and Patch Management Strategies Vulnerability Scanning Tools and Techniques using AI Exploiting Vulnerabilities (Hands-on Labs)®

- Understanding of AI and ML

An Introduction to AI Types and Applications of AI Identifying and Mitigating Risks in Real-Life Building a Resilient and Adaptive Security Infrastructure with AI Enhancing Digital Defenses using CSAI Application of Machine Learning in Cybersecurity Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats Threat Intelligence and Threat Hunting Concepts®

- Introduction to Cyber Security

Definition and Scope of Cyber Security Key Cybersecurity Concepts CIA Triad (Confidentiality, HIPAA) Importance of Cybersecurity in Modern Enterprises Careers in Cyber Security®

- Operating System Fundamentals

Core OS Functions (Memory Management, IDS/IPS Network Segmentation and Zoning Wireless Network Security (WPA2, IDS/IPS Open-Source Intelligence (OSINT) Techniques Introduction to Vulnerabilities Software Development Life Cycle (SDLC) and Security Integration with AI Zero-Day Attacks and Patch Management Strategies Vulnerability Scanning Tools and Techniques using AI Exploiting Vulnerabilities (Hands-on Labs)®

- Understanding of AI and ML

An Introduction to AI Types and Applications of AI Identifying and Mitigating Risks in Real-Life Building a Resilient and Adaptive Security Infrastructure with AI Enhancing Digital Defenses using CSAI Application of Machine Learning in Cybersecurity Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats Threat Intelligence and Threat Hunting Concepts®

- Python Programming Fundamentals

  Introduction to Python Programming Understanding of Python Libraries Python Programming Language for Cybersecurity Applications AI Scripting for Automation in Cybersecurity Tasks Data Analysis and Manipulation Using Python Developing Security Tools with Python®

- Applications of AI in Cybersecurity

  Understanding the Application of Machine Learning in Cybersecurity Anomaly Detection to Behavior Analysis Dynamic and Proactive Defense using Machine Learning Utilizing Machine Learning for Email Threat Detection Enhancing Phishing Detection with A Autonomous Identification and Thwarting of Email Threats Employing Advanced Algorithms and AI in Malware Threat Detection Identifying, Business Continuity) Penetration Testing and Vulnerability Assessments Legal and Regulatory Considerations of Security Incidents®

- Open Source Security Tools

  Introduction to Open-Source Security Tools Popular Open Source Security Tools Benefits and Challenges of Using Open-Source Tools Implementing Open Source Solutions in Organizations Community Support and Resources Network Security Scanning and Vulnerability Detection Security Information and Event Management (SIEM) Tools (Open-Source options) Open-Source Packet Filtering Firewalls Password Hashing and Cracking Tools (Ethical Use) Open-Source Forensics Tools®

- Securing the Future

  Emerging Cyber Threats and Trends Artificial Intelligence and Machine Learning in Cybersecurity Blockchain for Security Internet of Things (IoT) Security Cloud Security Quantum Computing and its Impact on Security Cybersecurity in Critical Infrastructure Cryptography and Secure Hashing Cyber Security Awareness and Training for Users Continuous Security Monitoring and Improvement®

- Capstone Project

  Introduction Use Cases: AI in Cybersecurity Outcome Presentation®

- Introduction to Cyber Security

  Definition and Scope of Cyber Security Key Cybersecurity Concepts CIA Triad (Confidentiality, HIPAA) Importance of Cybersecurity in Modern Enterprises Careers in Cyber Security

- Operating System Fundamentals

  Core OS Functions (Memory Management, Business Continuity) Penetration Testing and Vulnerability Assessments Legal and Regulatory Considerations of Security Incidents®

- Open Source Security Tools

  Introduction to Open-Source Security Tools Popular Open Source Security Tools Benefits and Challenges of Using Open-Source Tools Implementing Open Source Solutions in Organizations Community Support and Resources Network Security Scanning and Vulnerability Detection Security Information and Event Management (SIEM) Tools (Open-Source options) Open-Source Packet Filtering Firewalls Password Hashing and Cracking Tools (Ethical Use) Open-Source Forensics Tools®

- Securing the Future

  Emerging Cyber Threats and Trends Artificial Intelligence and Machine Learning in Cybersecurity Blockchain for Security Internet of Things (IoT) Security Cloud Security Quantum Computing and its Impact on Security Cybersecurity in Critical Infrastructure Cryptography and Secure Hashing Cyber Security Awareness and Training for Users Continuous Security Monitoring and Improvement®

- Capstone Project

  Introduction Use Cases: AI in Cybersecurity Outcome Presentation®

, Introduction to Cyber Security, Operating System Fundamentals, Networking Fundamentals, Threats, and Exploits, Understanding of AI and ML, Python Programming Fundamentals, Applications of AI in Cybersecurity, Incident Response and Disaster Recovery, Open Source Security Tools, Securing the Future, Capstone Project, Optional Module: AI Agents for Security Level 1

## □□ Certification Path

AI+ Security: Level 1

Exam: AI+ Security: Level 1

# Additional Course Details

Nexus Humans AI+ Security: Level 1 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 1 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 1?

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 1 course helps prepare you for the AI+ Security: Level 1 certification path.

---

### Q: Which exam does this course prepare me for?

This course prepares you for the AI+ Security: Level 1 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 1 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 1 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 1?

Yes, we provide corporate training, dedicated training, and closed classes for AI+ Security: Level 1. 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 1, AI Certs, vILT, AI+ Security

---

## Q: Why choose Nexus Human for AI+ Security: Level 1?

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 1 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 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)