Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

AI+ Security Level 2™

CODE:	LENGTH:	PRICE:
AIC_AT-2102	40 Hours	kr4,950.00

Description

Protect and Secure: Leverage Intelligent AI Solutions

Transform your security knowledge with our AI+ Security Level 2™ course and exam bundle. Learn essential AI-driven security strategies and safeguard next-gen technologies.

Why This Certification Matters

- **Comprehensive AI-Cybersecurity Integration:** Understand how AI and Cybersecurity merge, enhancing your capability to combat evolving digital threats effectively.
- **Practical Python Programming Skills:** Learn Python tailored for AI and Cybersecurity applications, gaining hands-on coding skills to address real-world security issues.
- **Advanced Threat Detection Techniques:** Master ML techniques to identify and mitigate email threats, malware, and network anomalies, improving cybersecurity defense.
- **Cutting-Edge AI Algorithms:** Utilize AI algorithms for advanced user authentication and explore Generative Adversarial Networks (GANs) to strengthen cybersecurity systems.
- **Real-World Application Focus:** Apply your skills in a Capstone Project, solving real-world cybersecurity problems and preparing for advanced industry challenges.

The following tools will be explored in this course:

- CrowdStrike
- Microsoft Cognitive Toolkit (CNTK)
- Flair.ai

Objectives

Exam Objectives

- **AI-Driven Threat Detection:** Learners will gain expertise in using AI algorithms for detecting various cybersecurity threats, including email threats, malware, and network anomalies, enhancing security monitoring capabilities.
- **Application of Machine Learning in Cybersecurity:** Students who will go through this course will have the ability to apply machine learning techniques to predict, detect, and respond to cyber threats effectively, using data-driven insights.
- **Enhanced User Authentication Methods:** Learners will develop skills in implementing advanced AI-based user authentication systems, improving security protocols to verify user identities more accurately and resist fraudulent attempts.
- **AI-Enhanced Penetration Testing:** Students will learn how to use AI tools to automate and enhance penetration testing processes, identifying vulnerabilities more efficiently and comprehensively than traditional methods.

Prerequisites

- Completion of AI+ Security Level 1™, but not mandatory
- 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 terminal for basic tasks
- Interest in AI for Security: Willingness to explore how AI can be applied to detect and mitigate security threats.

Programme

Module 1: Introduction to Artificial Intelligence (AI) and Cyber Security

1. 1.1 Understanding the Cyber Security Artificial Intelligence (CSAI)
2. 1.2 An Introduction to AI and its Applications in Cybersecurity
3. 1.3 Overview of Cybersecurity Fundamentals
4. 1.4 Identifying and Mitigating Risks in Real-Life
5. 1.5 Building a Resilient and Adaptive Security Infrastructure
6. 1.6 Enhancing Digital Defenses using CSAI

Module 2: Python Programming for AI and Cybersecurity Professionals

1. 2.1 Python Programming Language and its Relevance in Cybersecurity
2. 2.2 Python Programming Language and Cybersecurity Applications
3. 2.3 AI Scripting for Automation in Cybersecurity Tasks
4. 2.4 Data Analysis and Manipulation Using Python
5. 2.5 Developing Security Tools with Python

Module 3: Application of Machine Learning in Cybersecurity

1. 3.1 Understanding the Application of Machine Learning in Cybersecurity
2. 3.2 Anomaly Detection to Behaviour Analysis
3. 3.3 Dynamic and Proactive Defense using Machine Learning
4. 3.4 Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats

Module 4: Detection of Email Threats with AI

1. 4.1 Utilizing Machine Learning for Email Threat Detection
2. 4.2 Analyzing Patterns and Flagging Malicious Content
3. 4.3 Enhancing Phishing Detection with AI
4. 4.4 Autonomous Identification and Thwarting of Email Threats
5. 4.5 Tools and Technology for Implementing AI in Email Security

Module 5: AI Algorithm for Malware Threat Detection

1. 5.1 Introduction to AI Algorithm for Malware Threat Detection
2. 5.2 Employing Advanced Algorithms and AI in Malware Threat Detection
3. 5.3 Identifying, Analyzing, and Mitigating Malicious Software
4. 5.4 Safeguarding Systems, Networks, and Data in Real-time
5. 5.5 Bolstering Cybersecurity Measures Against Malware Threats
6. 5.6 Tools and Technology: Python, Malware Analysis Tools

Module 6: Network Anomaly Detection using AI

1. 6.1 Utilizing Machine Learning to Identify Unusual Patterns in Network Traffic
2. 6.2 Enhancing Cybersecurity and Fortifying Network Defenses with AI Techniques

3. 6.3 Implementing Network Anomaly Detection Techniques

Module 7: User Authentication Security with AI

1. 7.1 Introduction
2. 7.2 Enhancing User Authentication with AI Techniques
3. 7.3 Introducing Biometric Recognition, Anomaly Detection, and Behavioural Analysis
4. 7.4 Providing a Robust Defence Against Unauthorized Access
5. 7.5 Ensuring a Seamless Yet Secure User Experience
6. 7.6 Tools and Technology: AI-based Authentication Platforms
7. 7.7 Conclusion

Module 8: Generative Adversarial Network (GAN) for Cyber Security

1. 8.1 Introduction to Generative Adversarial Networks (GANs) in Cybersecurity
2. 8.2 Creating Realistic Mock Threats to Fortify Systems
3. 8.3 Detecting Vulnerabilities and Refining Security Measures Using GANs
4. 8.4 Tools and Technology: Python and GAN Frameworks

Module 9: Penetration Testing with Artificial Intelligence

1. 9.1 Enhancing Efficiency in Identifying Vulnerabilities Using AI
2. 9.2 Automating Threat Detection and Adapting to Evolving Attack Patterns
3. 9.3 Strengthening Organizations Against Cyber Threats Using AI-driven Penetration Testing
4. 9.4 Tools and Technology: Penetration Testing Tools, AI-based Vulnerability Scanners

Module 10: Capstone Project

1. 10.1 Introduction
2. 10.2 Use Cases: AI in Cybersecurity
3. 10.3 Outcome Presentation

Optional Module: AI Agents for Security Level 2

1. 1. What Are AI Agents
2. 2. Key Capabilities of AI Agents in Advanced Cybersecurity
3. 3. Applications and Trends for AI Agents in Advanced Cybersecurity
4. 4. How Does an AI Agent Work
5. 5. Core Characteristics of AI Agents
6. 6. Types of AI Agents

Follow on courses

- AI+ Ethical Hacker™
- AI+ Security Level 1™
- AI+ Security Compliance™
- AI+ Network™
- AI+ Security Level 3™

Test and Certification

Exam Policies & Integrity

Before your exam, you must accept the AI CERTs® Candidate Agreement. It ensures fairness, transparency, and unbiased certification for all candidates.

Recertification Requirements

AI CERTs requires recertification every year to keep your certification valid. Notifications will be sent three months before the due date, and candidates must follow the steps in the candidate handbook to complete the process.

Exam Objectives

- **AI-Driven Threat Detection:** Learners will gain expertise in using AI algorithms for detecting various cybersecurity threats, including email threats, malware, and network anomalies, enhancing security monitoring capabilities.
- **Application of Machine Learning in Cybersecurity:** Students who will go through this course will have the ability to apply machine learning techniques to predict, detect, and respond to cyber threats effectively, using data-driven insights.
- **Enhanced User Authentication Methods:** Learners will develop skills in implementing advanced AI-based user authentication systems, improving security protocols to verify user identities more accurately and resist fraudulent attempts.
- **AI-Enhanced Penetration Testing:** Students will learn how to use AI tools to automate and enhance penetration testing processes, identifying vulnerabilities more efficiently and comprehensively than traditional methods.

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
01 Jan 0001			English	Self Paced Training		kr4,950.00

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.