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 1™

CODE:	LENGTH:	PRICE:
AIC_AT-2101	40 Hours	kr4,950.00

Description

Empowering Cybersecurity with AI

Start your AI security journey with our all-in-one bundle. Explore core concepts in AI-driven protection, vulnerability management, and intelligent threat response.

Why This Certification Matters

- **Comprehensive** Learning: Explore AI and cybersecurity integration through Python, machine learning, and threat mitigation to build a strong technical foundation.
- **Hands-on Approach:** Apply concepts in a Capstone Project, solving real-world cybersecurity challenges by leveraging AI tools and practical problem-solving skills.
- **Cutting-Edge Knowledge:** Dive into advanced topics like AI-based authentication and GANs to understand next-gen cybersecurity strategies and innovations.
- **Boost Strategic Decision-Making with AI Analytics:** Master AI models to analyze business data, predict outcomes, and enable more informed, real-time decisions that enhance competitive advantage.
- **AI-Driven Threat Detection:** Learn to detect malware, phishing, and anomalies using machine learning, enhancing your ability to predict and prevent attacks.
- **Industry Relevance:** Stay ahead in cybersecurity by mastering AI applications, making you a valuable asset for future-focused security roles and organizations.

The following tools will be explored in this course:

- CrowdStrike
- Flair.ai
- ChatGPT
- Pluralsight

Objectives

Exam Objectives

- **Automation of Security Processes:** Learners will develop the ability to automate routine security tasks such as monitoring, logging, and incident response using AI technologies, improving efficiency and accuracy.
- **Data Privacy and Compliance in AI Security:** Learners will understand the importance of data privacy and regulatory compliance when using AI in security, enabling them to develop and implement secure, legally compliant systems.
- **Threat Detection and Response Using AI:** Learners will develop the skills to use AI-powered tools and techniques to detect, analyze, and respond to security threats in real-time
- **Real-Time Cyberattack Prevention with AI:** Learners will acquire the ability to leverage AI to anticipate and prevent cyberattacks before they occur, using predictive models and behavioral analysis.

Prerequisites

- Basic Python Programming: Familiarity with loops, functions, and variables.
- Basic Cybersecurity Knowledge: Understanding of CIA triad and common threats (e.g., malware, phishing).

- Basic Machine Learning Concepts: Awareness of fundamental machine learning concepts, not mandatory.
- Basic Networking: Understanding of IP addressing and TCP/IP protocols.
- Linux/Command Line Skills: Ability to navigate and use the CLI effectively.

Programme

Module 1: Introduction to Cybersecurity

1. 1.1 Definition and Scope of Cybersecurity
2. 1.2 Key Cybersecurity Concepts
3. 1.3 CIA Triad (Confidentiality, Integrity, Availability)
4. 1.4 Cybersecurity Frameworks and Standards (NIST, ISO/IEC27001)
5. 1.5 Cyber Security Laws and Regulations (e.g., GDPR, HIPAA)
6. 1.6 Importance of Cybersecurity in Modern Enterprises
7. 1.7 Careers in Cyber Security

Module 2: Operating System Fundamentals

1. 2.1 Core OS Functions (Memory Management, Process Management)
2. 2.2 User Accounts and Privileges
3. 2.3 Access Control Mechanisms (ACLs, DAC, MAC)
4. 2.4 OS Security Features and Configurations
5. 2.5 Hardening OS Security (Patching, Disabling Unnecessary Services)
6. 2.6 Virtualization and Containerization Security Considerations
7. 2.7 Secure Boot and Secure Remote Access
8. 2.8 OS Vulnerabilities and Mitigations

Module 3: Networking Fundamentals

1. 3.1 Network Topologies and Protocols (TCP/IP, OSI Model)
2. 3.2 Network Devices and Their Roles (Routers, Switches, Firewalls)
3. 3.3 Network Security Devices (Firewalls, IDS/IPS)
4. 3.4 Network Segmentation and Zoning
5. 3.5 Wireless Network Security (WPA2, Open WEP vulnerabilities)
6. 3.6 VPN Technologies and Use Cases
7. 3.7 Network Address Translation (NAT)
8. 3.8 Basic Network Troubleshooting

Module 4: Threats, Vulnerabilities, and Exploits

1. 4.1 Types of Threat Actors (Script Kiddies, Hacktivists, Nation-States)
2. 4.2 Threat Hunting Methodologies using AI
3. 4.3 AI Tools for Threat Hunting (SIEM, IDS/IPS)
4. 4.4 Open-Source Intelligence (OSINT) Techniques
5. 4.5 Introduction to Vulnerabilities
6. 4.6 Software Development Life Cycle (SDLC) and Security Integration with AI
7. 4.7 Zero-Day Attacks and Patch Management Strategies
8. 4.8 Vulnerability Scanning Tools and Techniques using AI
9. 4.9 Exploiting Vulnerabilities (Hands-on Labs)

Module 5: Understanding of AI and ML

1. 5.1 An Introduction to AI
2. 5.2 Types and Applications of AI
3. 5.3 Identifying and Mitigating Risks in Real-Life

4. 5.4 Building a Resilient and Adaptive Security Infrastructure with AI
5. 5.5 Enhancing Digital Defenses using CSAI
6. 5.6 Application of Machine Learning in Cybersecurity
7. 5.7 Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats
8. 5.8 Threat Intelligence and Threat Hunting Concepts

Module 6: Python Programming Fundamentals

1. 6.1 Introduction to Python Programming
2. 6.2 Understanding of Python Libraries
3. 6.3 Python Programming Language for Cybersecurity Applications
4. 6.4 AI Scripting for Automation in Cybersecurity Tasks
5. 6.5 Data Analysis and Manipulation Using Python
6. 6.6 Developing Security Tools with Python

Module 7: Applications of AI in Cybersecurity

1. 7.1 Understanding the Application of Machine Learning in Cybersecurity
2. 7.2 Anomaly Detection to Behavior Analysis
3. 7.3 Dynamic and Proactive Defense using Machine Learning
4. 7.4 Utilizing Machine Learning for Email Threat Detection
5. 7.5 Enhancing Phishing Detection with AI
6. 7.6 Autonomous Identification and Thwarting of Email Threats
7. 7.7 Employing Advanced Algorithms and AI in Malware Threat Detection
8. 7.8 Identifying, Analyzing, and Mitigating Malicious Software
9. 7.9 Enhancing User Authentication with AI Techniques
10. 7.10 Penetration Testing with AI

Module 8: Incident Response and Disaster Recovery

1. 8.1 Incident Response Process (Identification, Containment, Eradication, Recovery)
2. 8.2 Incident Response Lifecycle
3. 8.3 Preparing an Incident Response Plan
4. 8.4 Detecting and Analyzing Incidents
5. 8.5 Containment, Eradication, and Recovery
6. 8.6 Post-Incident Activities
7. 8.7 Digital Forensics and Evidence Collection
8. 8.8 Disaster Recovery Planning (Backups, Business Continuity)
9. 8.9 Penetration Testing and Vulnerability Assessments
10. 8.10 Legal and Regulatory Considerations of Security Incidents

Module 9: Open Source Security Tools

1. 9.1 Introduction to Open-Source Security Tools
2. 9.2 Popular Open Source Security Tools
3. 9.3 Benefits and Challenges of Using Open-Source Tools
4. 9.4 Implementing Open Source Solutions in Organizations
5. 9.5 Community Support and Resources
6. 9.6 Network Security Scanning and Vulnerability Detection
7. 9.7 Security Information and Event Management (SIEM) Tools (Open-Source options)
8. 9.8 Open-Source Packet Filtering Firewalls
9. 9.9 Password Hashing and Cracking Tools (Ethical Use)
10. 9.10 Open-Source Forensics Tools

Module 10: Securing the Future

1. 10.1 Emerging Cyber Threats and Trends
2. 10.2 Artificial Intelligence and Machine Learning in Cybersecurity
3. 10.3 Blockchain for Security
4. 10.4 Internet of Things (IoT) Security
5. 10.5 Cloud Security
6. 10.6 Quantum Computing and its Impact on Security
7. 10.7 Cybersecurity in Critical Infrastructure
8. 10.8 Cryptography and Secure Hashing
9. 10.9 Cyber Security Awareness and Training for Users
10. 10.10 Continuous Security Monitoring and Improvement

Module 11: Capstone Project

1. 11.1 Introduction
2. 11.2 Use Cases: AI in Cybersecurity
3. 11.3 Outcome Presentation

Optional Module: AI Agents for Security Level 1

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

Follow on courses

- AI+ Ethical Hacker™
- AI+ Security Level 2™
- 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

- **Automation of Security Processes:** Learners will develop the ability to automate routine security tasks such as monitoring, logging, and incident response using AI technologies, improving efficiency and accuracy.
- **Data Privacy and Compliance in AI Security:** Learners will understand the importance of data privacy and regulatory compliance when using AI in security, enabling them to develop and implement secure, legally compliant systems.
- **Threat Detection and Response Using AI:** Learners will develop the skills to use AI-powered tools and techniques to detect, analyze, and respond to security threats in real-time
- **Real-Time Cyberattack Prevention with AI:** Learners will acquire the ability to leverage AI to anticipate and prevent cyberattacks before they occur, using predictive models and behavioral analysis.

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.