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 3™

CODE:	LENGTH:	PRICE:
AIC_AT-2103	40 Hours	kr4,950.00

Description

Master the Future of Cybersecurity with AI-Driven Solutions
The AI+ Security Level 3™ course provides a comprehensive exploration of the intersection between AI and cybersecurity, focusing on advanced topics critical to modern security engineering. It covers foundational concepts in AI and machine learning for security, delving into areas like threat detection, response mechanisms, and the use of deep learning for security applications. The course addresses the challenges of adversarial AI, network and endpoint security, and secure AI system engineering, along with emerging topics such as AI for cloud, container security, and blockchain integration. Key subjects also include AI in identity and access management (IAM), IoT security, and physical security systems, culminating in a hands-on capstone project that tasks learners with designing and engineering AI-driven security solutions.
The following tools will be explored in this course:

- Splunk User Behavior Analytics (UBA)
- Microsoft Defender for Endpoint
- Microsoft Azure AD Conditional Access
- Adversarial Robustness Toolbox (ART)

Objectives

- **Apply Deep Learning for Cyber Defense**
  Acquire expertise in using deep learning algorithms for advanced applications like malware analysis, phishing detection, and predictive threat modeling.
- **Integrate AI with Cloud and Container Security**
  Understand the use of AI for securing cloud-based platforms and containerized applications, focusing on scalability and automation in threat mitigation.
- **Enhance Identity and Access Management with AI**
  Learn to apply AI techniques to streamline identity verification, manage access control systems, and secure authentication processes.
- **Secure IoT Devices Using AI**
  Explore how AI can be used to address unique IoT security challenges, including detecting compromised devices and protecting communication protocols.

Prerequisites

- Completion of AI+ Security Level 1™ and 2™
- Intermediate/Advanced Python Programming: Proficiency or expert in Python, including deep learning frameworks (TensorFlow, PyTorch).
- Intermediate Machine Learning Knowledge: Proficiency in understanding of deep learning, adversarial AI, and model training.
- Advanced Cybersecurity Knowledge: Proficiency in threat detection, incident response, and network/endpoint security.
- AI in Security Engineering: Knowledge of AI's role in identity and access management (IAM), IoT security, and physical security.
- Cloud and Container Expertise: Understanding of cloud security, containerization, and blockchain technologies.
- Linux/CLI Mastery: Advanced command-line skills and experience with security tools in Linux environments

There are no mandatory prerequisites for certification. Certification is based solely on performance in the examination. However, candidates may choose to prepare through self-study or optional training offered by AI CERTs® Authorized Training Partners (ATPs).

Programme

Module 1: Foundations of AI and Machine Learning for Security Engineering
1.1 Core AI and ML Concepts for Security
1.2 AI Use Cases in Cybersecurity
1.3 Engineering AI Pipelines for Security
1.4 Challenges in Applying AI to Security

Module 2: Machine Learning for Threat Detection and Response
2.1 Engineering Feature Extraction for Cybersecurity Datasets
2.2 Supervised Learning for Threat Classification
2.3 Unsupervised Learning for Anomaly Detection
2.4 Engineering Real-Time Threat Detection Systems

Module 3: Deep Learning for Security Applications
3.1 Convolutional Neural Networks (CNNs) for Threat Detection
3.2 Recurrent Neural Networks (RNNs) and LSTMs for Security
3.3 Autoencoders for Anomaly Detection
3.4 Adversarial Deep Learning in Security

Module 4: Adversarial AI in Security
4.1 Introduction to Adversarial AI Attacks
4.2 Defense Mechanisms Against Adversarial Attacks
4.3 Adversarial Testing and Red Teaming for AI Systems
4.4 Engineering Robust AI Systems Against Adversarial AI

Module 5: AI in Network Security
5.1 AI-Powered Intrusion Detection Systems
5.2 AI for Distributed Denial of Service (DDoS) Detection
5.3 AI-Based Network Anomaly Detection
5.4 Engineering Secure Network Architectures with AI

Module 6: AI in Endpoint Security
6.1 AI for Malware Detection and Classification
6.2 AI for Endpoint Detection and Response (EDR)
6.3 AI-Driven Threat Hunting
6.4 Implementing Lightweight AI Models for Resource-Constrained Devices

Module 7: Secure AI System Engineering
7.1 Designing Secure AI Architectures
7.2 Cryptography in AI for Security
7.3 Ensuring Model Explainability and Transparency in Security
7.4 Performance Optimization of AI Security Systems

Module 8: AI for Cloud and Container Security
8.1 AI for Securing Cloud Environments
8.2 AI-Driven Container Security
8.3 AI for Securing Serverless Architectures
8.4 AI and DevSecOps

Module 9: AI and Blockchain for Security
9.1 Fundamentals of Blockchain and AI Integration
9.2 AI for Fraud Detection in Blockchain
9.3 Smart Contracts and AI Security
9.4 AI-Enhanced Consensus Algorithms

Module 10: AI in Identity and Access Management (IAM)
10.1 AI for User Behavior Analytics in IAM
10.2 AI for Multi-Factor Authentication (MFA)
10.3 AI for Zero-Trust Architecture
10.4 AI for Role-Based Access Control (RBAC)

Module 11: AI for Physical and IoT Security
11.1 AI for Securing Smart Cities
11.2 AI for Industrial IoT Security
11.3 AI for Autonomous Vehicle Security
11.4 AI for Securing Smart Homes and Consumer IoT

Module 12: Capstone Project - Engineering AI Security Systems
12.1 Defining the Capstone Project Problem
12.2 Engineering the AI Solution
12.3 Deploying and Monitoring the AI System
12.4 Final Capstone Presentation and Evaluation

Optional Module: AI Agents for Security level 3
Understanding AI Agents
Case Studies
Hands-On Practice with AI Agents

Follow on courses

- AI+ Ethical Hacker™
- AI+ Security Level 1™
- AI+ Security Compliance™
- AI+ Network™
- AI+ Security Level 2™

Test and Certification

- **Apply Deep Learning for Cyber Defense**
  Acquire expertise in using deep learning algorithms for advanced applications like malware analysis, phishing detection, and predictive threat modeling.
- **Integrate AI with Cloud and Container Security**
  Understand the use of AI for securing cloud-based platforms and containerized applications, focusing on scalability and automation in threat mitigation.
- **Enhance Identity and Access Management with AI**
  Learn to apply AI techniques to streamline identity verification, manage access control systems, and secure authentication processes.
- **Secure IoT Devices Using AI**
  Explore how AI can be used to address unique IoT security challenges, including detecting compromised devices and protecting communication protocols.

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.

- **Duration**: 90 minutes
- **Passing Score**: 70% (35/50)
- **Format:** 50 multiple-choice/multiple-response questions
- **Delivery Method:** Online via proctored exam platform (flexible scheduling)

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.