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+ Ethical Hacker™

CODE:	LENGTH:	PRICE:
AIC_AT-220	40 Hours	kr4,950.00

Description

Protect Digital Landscapes: Harness AI-Enhanced Technologies
The AI+ Ethical Hacker™ certification delves into the intersection of cybersecurity and artificial intelligence, a pivotal juncture in our era of rapid technological progress. Tailored for budding ethical hackers and cybersecurity experts, it offers comprehensive insights into AI's transformative impact on digital offense and defense strategies. Unlike conventional ethical hacking courses, this program harnesses AI's power to enhance cybersecurity approaches. It caters to tech enthusiasts eager to master the fusion of cutting-edge AI methods with ethical hacking practices amidst the swiftly evolving digital landscape. The curriculum encompasses four key areas, from course objectives and prerequisites to anticipated job roles and the latest AI technologies in Ethical Hacking.
The following tools will be explored in this course:

- Acunetix
- Wazuh
- Shodan
- OWASP ZAP

Objectives

- AI-Integrated Cybersecurity Techniques
  Learners will develop the ability to integrate AI tools and technologies into cybersecurity practices. This includes using AI for ethical hacking tasks such as reconnaissance, vulnerability assessments, penetration testing, and incident response.
- Threat Analysis and Anomaly Detection
  Students will develop skills in applying machine learning algorithms to detect unusual patterns and behaviors that may indicate potential security threats. This capability is essential for proactively identifying and mitigating risks before they escalate.
- AI for Identity and Access Management (IAM)
  Learners will understand how to apply AI to enhance IAM systems, crucial for maintaining secure access to resources within an organization. This involves using AI to improve authentication processes and manage user permissions more dynamically and securely.
- Automated Security Protocol Optimization
  Students will be equipped to utilize AI to dynamically adjust and optimize security protocols based on real-time data analysis and threat assessment. Learners will explore how AI algorithms can predict and respond to potential security breaches by automatically tweaking firewall rules, security configurations, and other protective measures.

Audience

This certification is ideal for aspiring ethical hackers and cybersecurity professionals who want to integrate AI technologies into their skill set. It caters to tech enthusiasts looking to stay ahead in the rapidly evolving digital landscape.

Prerequisites

- Programming Proficiency: Knowledge of Python, Java, C++, etc for automation and scripting.
- Networking Fundamentals: Understanding of networking protocols, subnetting, firewalls, and routing.
- Operating Systems Knowledge: Proficiency in using Windows and Linux operating systems.
- Cybersecurity Basics: Familiarity with fundamental cybersecurity concepts, including encryption, authentication, access controls, and security protocols.
- Machine Learning Basics: Understanding of machine learning concepts, algorithms, and basic implementation.
- Web Technologies: Understanding of web technologies, including HTTP/HTTPS protocols, and web servers.

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

Certification Overview
Course Introduction

Module 1: Foundation of Ethical Hacking Using Artificial Intelligence (AI)
1.1 Introduction to Ethical Hacking
1.2 Ethical Hacking Methodology
1.3 Legal and Regulatory Framework
1.4 Hacker Types and Motivations
1.5 Information Gathering Techniques
1.6 Footprinting and Reconnaissance
1.7 Scanning Networks
1.8 Enumeration Techniques

Module 2: Introduction to AI in Ethical Hacking
2.1 AI in Ethical Hacking
2.2 Fundamentals of AI
2.3 AI Technologies Overview
2.4 Machine Learning in Cybersecurity
2.5 Natural Language Processing (NLP) for Cybersecurity
2.6 Deep Learning for Threat Detection
2.7 Adversarial Machine Learning in Cybersecurity
2.8 AI-Driven Threat Intelligence Platforms
2.9 Cybersecurity Automation with AI

Module 3: AI Tools and Technologies in Ethical Hacking
3.1 AI-Based Threat Detection Tools
3.2 Machine Learning Frameworks for Ethical Hacking
3.3 AI-Enhanced Penetration Testing Tools
3.4 Behavioral Analysis Tools for Anomaly Detection
3.5 AI-Driven Network Security Solutions
3.6 Automated Vulnerability Scanners
3.7 AI in Web Application
3.8 AI for Malware Detection and Analysis
3.9 Cognitive Security Tools

Module 4: AI-Driven Reconnaissance Techniques
4.1 Introduction to Reconnaissance in Ethical Hacking
4.2 Traditional vs. AI-Driven Reconnaissance
4.3 Automated OS Fingerprinting with AI
4.4 AI-Enhanced Port Scanning Techniques
4.5 Machine Learning for Network Mapping
4.6 AI-Driven Social Engineering Reconnaissance
4.7 Machine Learning in OSINT
4.8 AI-Enhanced DNS Enumeration & AI-Driven Target Profiling

Module 5: AI in Vulnerability Assessment and Penetration Testing
5.1 Automated Vulnerability Scanning with AI
5.2 AI-Enhanced Penetration Testing Tools
5.3 Machine Learning for Exploitation Techniques
5.4 Dynamic Application Security Testing (DAST) with AI
5.5 AI-Driven Fuzz Testing
5.6 Adversarial Machine Learning in Penetration Testing
5.7 Automated Report Generation using AI
5.8 AI-Based Threat Modeling
5.9 Challenges and Ethical Considerations in AI-Driven Penetration Testing

Module 6: Machine Learning for Threat Analysis
6.1 Supervised Learning for Threat Detection
6.2 Unsupervised Learning for Anomaly Detection
6.3 Reinforcement Learning for Adaptive Security Measures

6.4 Natural Language Processing (NLP) for Threat Intelligence
6.5 Behavioral Analysis using Machine Learning
6.6 Ensemble Learning for Improved Threat Prediction
6.7 Feature Engineering in Threat Analysis
6.8 Machine Learning in Endpoint Security
6.9 Explainable AI in Threat Analysis

Module 7: Behavioral Analysis and Anomaly Detection for System Hacking
7.1 Behavioral Biometrics for User Authentication
7.2 Machine Learning Models for User Behavior Analysis
7.3 Network Traffic Behavioral Analysis
7.4 Endpoint Behavioral Monitoring
7.5 Time Series Analysis for Anomaly Detection
7.6 Heuristic Approaches to Anomaly Detection
7.7 AI-Driven Threat Hunting
7.8 User and Entity Behavior Analytics (UEBA)
7.9 Challenges and Considerations in Behavioral Analysis

Module 8: AI Enabled Incident Response Systems
8.1 Automated Threat Triage using AI
8.2 Machine Learning for Threat Classification
8.3 Real-time Threat Intelligence Integration
8.4 Predictive Analytics in Incident Response
8.5 AI-Driven Incident Forensics
8.6 Automated Containment and Eradication Strategies
8.7 Behavioral Analysis in Incident Response
8.8 Continuous Improvement through Machine Learning Feedback
8.9 Human-AI Collaboration in Incident Handling

Module 9: AI for Identity and Access Management (IAM)
9.1 AI-Driven User Authentication Techniques
9.2 Behavioral Biometrics for Access Control
9.3 AI-Based Anomaly Detection in IAM
9.4 Dynamic Access Policies with Machine Learning
9.5 AI-Enhanced Privileged Access Management (PAM)
9.6 Continuous Authentication using Machine Learning
9.7 Automated User Provisioning and De-provisioning
9.8 Risk-Based Authentication with AI
9.9 AI in Identity Governance and Administration (IGA)

Module 10: Securing AI Systems
10.1 Adversarial Attacks on AI Models
10.2 Secure Model Training Practices
10.3 Data Privacy in AI Systems
10.4 Secure Deployment of AI Applications
10.5 AI Model Explainability and Interpretability
10.6 Robustness and Resilience in AI
10.7 Secure Transfer and Sharing of AI Models
10.8 Continuous Monitoring and Threat Detection for AI

Module 11: Ethics in AI and Cybersecurity
11.1 Ethical Decision-Making in Cybersecurity
11.2 Bias and Fairness in AI Algorithms
11.3 Transparency and Explainability in AI Systems
11.4 Privacy Concerns in AI-Driven Cybersecurity
11.5 Accountability and Responsibility in AI Security
11.6 Ethics of Threat Intelligence Sharing
11.7 Human Rights and AI in Cybersecurity
11.8 Regulatory Compliance and Ethical Standards
11.9 Ethical Hacking and Responsible Disclosure

Module 12: Capstone Project
12.1 Case Study 1: AI-Enhanced Threat Detection and Response
12.2 Case Study 2: Ethical Hacking with AI Integration
12.3 Case Study 3: AI in Identity and Access Management (IAM)
12.4 Case Study 4: Secure Deployment of AI Systems

Optional Module: AI Agents for Ethical Hacking

1. Understanding AI Agents
2. Case Studies
3. Hands-On Practice with AI Agents

Follow on courses

Recommended Certifications:

- AI+ Security Level 1™
- AI+ Security Level 2™
- AI+ Security Compliance™
- AI+ Network™
- AI+ Security Level 3™

Test and Certification

- AI-Integrated Cybersecurity Techniques
  Learners will develop the ability to integrate AI tools and technologies into cybersecurity practices. This includes using AI for ethical hacking tasks such as reconnaissance, vulnerability assessments, penetration testing, and incident response.
- Threat Analysis and Anomaly Detection
  Students will develop skills in applying machine learning algorithms to detect unusual patterns and behaviors that may indicate potential security threats. This capability is essential for proactively identifying and mitigating risks before they escalate.
- AI for Identity and Access Management (IAM)
  Learners will understand how to apply AI to enhance IAM systems, crucial for maintaining secure access to resources within an organization. This involves using AI to improve authentication processes and manage user permissions more dynamically and securely.
- Automated Security Protocol Optimization
  Students will be equipped to utilize AI to dynamically adjust and optimize security protocols based on real-time data analysis and threat assessment. Learners will explore how AI algorithms can predict and respond to potential security breaches by automatically tweaking firewall rules, security configurations, and other protective measures.

Exam Details

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

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.

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.