Enterprise Computing Solutions - Education Services

OFERTA FORMATIVA

Detalles de contacto

Avda Europa 21, 28108 Alcobendas

Email: formacion.ecs.es@arrow.com
Phone: +34 91 761 21 51

AI+ Security Compliance™

CÓDIGO:	DURACIÓN:	Precio:
AIC_AT-230	40 Hours	€495.00

Description

Empowering Compliance Through AI
The AI+ Security Compliance™ is an advanced course that merges the fundamental principles of cybersecurity compliance with the transformative power of artificial intelligence (AI). Building on the CISSP framework, this course focuses on how AI can enhance compliance processes, improve risk management, and ensure robust security measures in alignment with regulatory standards. This course introduces you to the core principles of cyber security compliances, while exploring the potential of AI to enhance your security posture. This course structure integrates comprehensive cybersecurity compliance principles with advanced AI applications, providing learners with the necessary skills to ensure compliance and enhance security through AI technologies.
The following tools will be explored in this course:

- Secureframe
- LeewayHertz
- Securiti
- Scytale

Objetivos

- **AI-Enhanced Compliance Management**
  Students will be able to integrate AI tools and techniques to streamline and automate compliance processes, ensuring adherence to international cybersecurity standards and regulations.
- **AI-Driven Security Solutions**
  Students will gain hands-on experience with AI applications in security, learning how to implement AI-powered tools for incident response, threat detection, and asset security.
- **Risk Management with AI**
  Students will develop the ability to use AI for conducting comprehensive risk assessments, identifying potential vulnerabilities, and implementing proactive risk mitigation strategies.
- **Understanding of Future AI Trends in Cybersecurity**
  Students will be equipped with knowledge of emerging AI technologies, such as quantum computing, and their implications for cybersecurity, allowing them to stay ahead of evolving threats and innovations.

Público

Ideal for security professionals, compliance officers, and AI developers working on security-critical AI projects.

Requisitos Previos

- Basic understanding of cybersecurity principles.
- Knowledge of networking fundamentals.
- Familiarity with programming concepts and languages (Python recommended)
- An introductory course on AI or machine learning is beneficial but not required

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).

Programa

Module 1: Introduction to Cybersecurity Compliance and AI
1.1 Overview of Cybersecurity Compliance
1.2 International Compliance Standards
1.3 Developing Compliance Programs
1.4 Implementing Compliance Programs
1.5 AI in Cybersecurity Compliance
1.6 Case Studies and Applications
Module 2: Security and Risk Management with AI
2.1 Risk Management Frameworks
2.2 Conducting Risk Assessments
2.3 AI in Risk Assessment
2.4 Compliance and AI
2.5 Incident Response and AI
Module 3: Asset Security and AI for Compliance
3.1 Data Classification and Protection
3.2 AI in Privacy Protection
3.3 Asset Management with AI
3.4 Case Studies and Best Practices
Module 4: Security Architecture and Engineering with AI
4.1 Secure Design Principles
4.2 AI in Cryptography
4.3 AI in Vulnerability Assessment
4.4 Security Models and AI

Module 5: Communication and Network Security with AI
5.1 Network Security Fundamentals
5.2 AI in Network Monitoring
5.3 AI-driven Network Defense
5.4 Compliance in Network Security
Module 6: Identity and Access Management (IAM) with AI
6.1 IAM Fundamentals
6.2 AI in Identity Verification
6.3 Access Control and AI
6.4 Threats to IAM and AI Solutions

Module 7: Security Assessment and Incident Response with AI
7.1 Security Testing Techniques
7.2 AI in Security Testing
7.3 Continuous Monitoring and AI
7.4 Incident Response Planning
7.5 Managing Cybersecurity Incidents
7.6 Legal and Regulatory Considerations

Module 8: Security Operations with AI
8.1 Security Operations Center (SOC)
8.2 Data Classification and Protection
8.3 Privacy Compliance
8.4 Disaster Recovery and AI
8.5 AI in Security Orchestration

Module 9: Software Development Security and Audit with AI
9.1 Secure Software Development Life Cycle (SDLC)
9.2 AI in Application Security Testing
9.3 AI in Secure DevOps
9.4 Threat Modeling and AI
9.5 Internal and External Audits
9.6 Continuous Monitoring

Module 10: Future Trends in AI and Cybersecurity Compliance
10.1 Emerging AI Technologies
10.2 AI in Cyber Threat Intelligence
10.3 Quantum Computing and AI
10.4 Ethical Considerations and AI Governance
10.5 Practical Applications

Optional Module: AI Agents for Security Compliance

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

Follow on courses

- AI+ Ethical Hacker™
- AI+ Security Level 1™
- AI+ Security Level 2™
- AI+ Security Level 3™
- AI+ Network™

Examen y certificación

- **AI-Enhanced Compliance Management**

Students will be able to integrate AI tools and techniques to streamline and automate compliance processes, ensuring adherence to international cybersecurity standards and regulations.

- **AI-Driven Security Solutions**

Students will gain hands-on experience with AI applications in security, learning how to implement AI-powered tools for incident response, threat detection, and asset security.

- **Risk Management with AI**

Students will develop the ability to use AI for conducting comprehensive risk assessments, identifying potential vulnerabilities, and implementing proactive risk mitigation strategies.

- **Understanding of Future AI Trends in Cybersecurity**

Students will be equipped with knowledge of emerging AI technologies, such as quantum computing, and their implications for cybersecurity, allowing them to stay ahead of evolving threats and innovations.

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)

Fechas Programadas

Fecha	Localización	Zona horaria	Idioma	Modalidad de impartición	Impartición garantizada	Precio
01 Jan 0001			English	Self Paced Training		€495.00

Información Adicional

Esta formación también está disponible en modalidad presencial. Por favor contáctenos para más información.