AI+ Security Level 1™

AI CERTs

Com certificação

- **Nível:**
- **Duração:** 40h

Sobre o curso

A certificação **AI+ Security Level 1™** foi desenvolvida para capacitar profissionais a integrar a Inteligência Artificial em práticas de cibersegurança, de forma estruturada, prática e alinhada com os desafios atuais das organizações. O foco está na utilização da IA para reforçar mecanismos de defesa, automatizar processos de segurança e responder de forma mais eficaz a ameaças digitais cada vez mais sofisticadas.

Ao longo do percurso, os participantes exploram a interseção entre cibersegurança e IA, incluindo fundamentos de redes, sistemas operativos, ameaças e vulnerabilidades, bem como aplicações de machine learning para deteção de anomalias, análise de ameaças e resposta a incidentes. São também abordados temas como automação com Python, compliance e proteção de dados, proporcionando uma base sólida para atuar em contextos de segurança orientados por IA.

A componente prática assume um papel central, com laboratórios, exercícios e um capstone project que permitem aplicar técnicas de IA a cenários reais de cibersegurança, reforçando competências na prevenção, deteção e mitigação de riscos.

Em parceria com a Rumos, Platinum Gold Partner.

Destinatários

- Profissionais de cibersegurança e segurança da informação;
- Administradores de sistemas e redes;
- Profissionais de IT interessados em segurança com apoio de IA;
- Analistas de segurança e threat intelligence;
- Profissionais que pretendam iniciar ou evoluir na área de AI security

Objetivos

- Compreender os fundamentos da cibersegurança e da sua integração com IA;
- Aplicar técnicas de machine learning para deteção de ameaças e anomalias;
- Utilizar Python para automação de processos de segurança;
- Identificar vulnerabilidades e aplicar estratégias de mitigação;
- Implementar processos de resposta a incidentes com apoio de IA;
- Utilizar ferramentas open source para análise e monitorização de segurança;
- Reforçar a proteção de sistemas, redes e dados em ambientes digitais

Condições

Detalhes do exame

- Duração: 90 minutos;
- Pontuação mínima de aprovação: 70% (35/50);
- Formato: 50 questões de escolha múltipla;
- Realização online, através de plataforma com proctoring e possibilidade de nova tentativa.

Pré-requisitos

- Conhecimentos básicos de cibersegurança (ex.: CIA triad, ameaças comuns);
- Familiaridade com conceitos de redes e sistemas operativos;
- Noções básicas de programação (preferencialmente Python) são recomendadas;
- Conhecimentos introdutórios de machine learning são benéficos, mas não obrigatórios.

Metodologia

A formação decorre em formato e-learning, com aproximadamente 40 horas de conteúdos on-demand, incluindo vídeos, e-book, podcasts e atividades práticas interativas. A aprendizagem pode ser realizada em qualquer momento e a partir de qualquer lugar, com quizzes modulares para acompanhar o progresso.

Programa

- Course Introduction
- Introduction to Cybersecurity
- Operating System Fundamentals
- Networking Fundamentals
- Threats, Vulnerabilities, and Exploits

- Understanding of AI and ML
- Python Programming Fundamentals
- Applications of AI in Cybersecurity
- Incident Response and Disaster Recovery
- Open Source Security Tools
- Securing the Future
- Capstone Project
- Optional Module: AI Agents for Security Level 1

Course Introduction

Introduction to Cybersecurity

- Definition and Scope of Cybersecurity
- Key Cybersecurity Concepts
- CIA Triad (Confidentiality, Integrity, Availability)
- Cybersecurity Frameworks and Standards
- Cyber Security Laws and Regulations
- Importance of Cybersecurity in Modern Enterprises

Operating System Fundamentals

- Core OS Functions
- User Accounts and Privileges
- Access Control Mechanisms
- OS Security Features and Configurations
- Hardening OS Security
- Virtualization and Containerization Security
- Secure Boot and Remote Access
- OS Vulnerabilities and Mitigations

Networking Fundamentals

- Network Topologies and Protocols
- Network Devices and Roles
- Network Security Devices
- Network Segmentation and Zoning
- Wireless Network Security
- VPN Technologies
- Network Address Translation
- Network Troubleshooting

Threats, Vulnerabilities, and Exploits

- Types of Threat Actors
- Threat Hunting Methodologies using AI
- AI Tools for Threat Hunting

- Open-Source Intelligence Techniques
- Vulnerability Identification
- SDLC and Security Integration
- Zero-Day Attacks and Patch Management
- Vulnerability Scanning Techniques
- Exploiting Vulnerabilities

Understanding of AI and ML

- Introduction to AI
- Types and Applications of AI
- Risk Identification and Mitigation
- Building Resilient Security Systems
- Machine Learning in Cybersecurity
- Threat Intelligence Concepts

Python Programming Fundamentals

- Introduction to Python
- Python Libraries
- Python for Cybersecurity
- Automation Scripts
- Data Analysis and Manipulation
- Developing Security Tools

Applications of AI in Cybersecurity

- Machine Learning Applications
- Anomaly Detection and Behaviour Analysis
- Email Threat Detection
- Phishing Detection
- Malware Detection
- User Authentication with AI
- Penetration Testing with AI

Incident Response and Disaster Recovery

- Incident Response Lifecycle
- Detection and Analysis
- Containment and Recovery
- Digital Forensics
- Disaster Recovery Planning
- Legal and Regulatory Considerations

Open Source Security Tools

- Overview of Open Source Tools
- Implementation in Organizations

- SIEM Tools
- Network Security Scanning
- Forensics Tools

Securing the Future

- Emerging Threats and Trends
- AI and ML in Cybersecurity
- IoT and Cloud Security
- Cryptography
- Security Awareness and Training
- Continuous Monitoring

Capstone Project

- AI in Cybersecurity Use Cases
- Practical Implementation
- Presentation of Results