AI+ Security Level 2™

AI CERTs

Com certificação

- **Nível:**
- **Duração:** 40h

Sobre o curso

A certificação **AI+ Security Level 2™** foi desenvolvida para capacitar profissionais a aplicar a Inteligência Artificial em contextos avançados de cibersegurança, de forma estruturada, prática e alinhada com a crescente sofisticação das ameaças digitais. O foco está na utilização de machine learning e técnicas avançadas de IA para deteção, prevenção e resposta a ciberataques em tempo real.

Ao longo do percurso, os participantes aprofundam a integração entre IA e cibersegurança, explorando áreas como deteção de ameaças (phishing, malware, anomalias de rede), autenticação inteligente e penetration testing automatizado. São também abordados temas como algoritmos avançados, incluindo Generative Adversarial Networks (GANs), permitindo uma abordagem mais sofisticada e proativa à defesa digital.

A componente prática assume um papel central, com exercícios aplicados, desenvolvimento de scripts em Python e um capstone project orientado para resolução de problemas reais de cibersegurança, consolidando competências técnicas e preparando os participantes para atuar em contextos exigentes e de elevado risco.

Em parceria com a Rumos, Platinum Gold Partner.

Destinatários

- Profissionais de cibersegurança que pretendam evoluir para níveis mais avançados com IA;
- Analistas de segurança, SOC analysts e especialistas em threat intelligence;
- Profissionais de IT e engenharia de sistemas com foco em segurança;
- Especialistas em dados e IA interessados em aplicações de cibersegurança;
- Profissionais que pretendam desenvolver competências avançadas em AI-driven security

Objetivos

- Aplicar técnicas avançadas de IA na deteção e mitigação de ciberameaças;
- Utilizar machine learning para identificar padrões anómalos e comportamentos suspeitos;
- Desenvolver scripts e ferramentas de segurança com Python;
- Implementar soluções de autenticação inteligente e proteção de acessos;
- Aplicar IA em análise de malware, phishing e ameaças de rede;
- Automatizar processos de penetration testing com apoio de IA;
- Desenvolver soluções práticas para cenários reais de cibersegurança

Condições

Detalhes do exame

- Duração: 90 minutos;
- Pontuação mínima de aprovação: 70% (35/50);
- Formato: 50 questões de escolha múltipla e múltipla resposta;
- Realização online, através de plataforma com proctoring por IA e agendamento flexível.

Pré-requisitos

- Conhecimentos básicos de cibersegurança (ex.: ameaças, CIA triad);
- Familiaridade com Python (variáveis, loops, funções);
- Noções de networking (endereços IP e funcionamento da internet);
- Conhecimentos introdutórios de machine learning;
- Experiência prévia com linha de comandos (Linux ou Windows) é recomendada;
- AI+ Security Level 1™ é recomendado, mas não obrigatório.

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 Artificial Intelligence (AI) and Cyber Security

- Python Programming for AI and Cybersecurity Professionals
- Application of Machine Learning in Cybersecurity
- Detection of Email Threats with AI
- AI Algorithm for Malware Threat Detection
- Network Anomaly Detection using AI
- User Authentication Security with AI
- Generative Adversarial Network (GAN) for Cyber Security
- Penetration Testing with Artificial Intelligence
- Capstone Project
- Optional Module: AI Agents for Security Level 2

Course Introduction

Introduction to Artificial Intelligence (AI) and Cyber Security

- Understanding the Cyber Security Artificial Intelligence (CSAI)
- An Introduction to AI and its Applications in Cybersecurity
- Overview of Cybersecurity Fundamentals
- Identifying and Mitigating Risks in Real-Life
- Building a Resilient and Adaptive Security Infrastructure
- Enhancing Digital Defenses using CSAI

Python Programming for AI and Cybersecurity Professionals

- Python Programming Language and its Relevance in Cybersecurity
- Python Programming Language and Cybersecurity Applications
- AI Scripting for Automation in Cybersecurity Tasks
- Data Analysis and Manipulation Using Python
- Developing Security Tools with Python

Application of Machine Learning in Cybersecurity

- Understanding the Application of Machine Learning in Cybersecurity
- Anomaly Detection to Behaviour Analysis
- Dynamic and Proactive Defense using Machine Learning
- Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats

Detection of Email Threats with AI

- Utilizing Machine Learning for Email Threat Detection
- Analyzing Patterns and Flagging Malicious Content
- Enhancing Phishing Detection with AI
- Autonomous Identification and Thwarting of Email Threats
- Tools and Technology for Implementing AI in Email Security

AI Algorithm for Malware Threat Detection

- Introduction to AI Algorithm for Malware Threat Detection

- Employing Advanced Algorithms and AI in Malware Threat Detection
- Identifying, Analyzing, and Mitigating Malicious Software
- Safeguarding Systems, Networks, and Data in Real-time
- Bolstering Cybersecurity Measures Against Malware Threats
- Tools and Technology: Python, Malware Analysis Tools

Network Anomaly Detection using AI

- Utilizing Machine Learning to Identify Unusual Patterns in Network Traffic
- Enhancing Cybersecurity and Fortifying Network Defenses with AI Techniques
- Implementing Network Anomaly Detection Techniques

User Authentication Security with AI

- Enhancing User Authentication with AI Techniques
- Introducing Biometric Recognition, Anomaly Detection, and Behavioural Analysis
- Providing a Robust Defence Against Unauthorized Access
- Ensuring a Seamless Yet Secure User Experience

Generative Adversarial Network (GAN) for Cyber Security

- Introduction to Generative Adversarial Networks (GANs) in Cybersecurity
- Creating Realistic Mock Threats to Fortify Systems
- Detecting Vulnerabilities and Refining Security Measures Using GANs
- Tools and Technology: Python and GAN Frameworks

Penetration Testing with Artificial Intelligence

- Enhancing Efficiency in Identifying Vulnerabilities Using AI
- Automating Threat Detection and Adapting to Evolving Attack Patterns
- Strengthening Organizations Against Cyber Threats Using AI-driven Penetration Testing

Capstone Project

- AI in Cybersecurity Use Cases
- Practical Implementation
- Outcome Presentation