AI+ Security Level 3™

AI CERTs

Com certificação

- **Nível:**
- **Duração:** 40h

Sobre o curso

A certificação **AI+ Security Level 3™** foi desenvolvida para capacitar profissionais a atuar ao mais alto nível na interseção entre Inteligência Artificial e cibersegurança, com foco na conceção, implementação e governação de sistemas de segurança avançados. Este programa posiciona-se como uma formação de nível especialista, orientada para arquitetar soluções de segurança inteligentes, resilientes e escaláveis em contextos empresariais complexos.

Ao longo do percurso, os participantes aprofundam a aplicação de machine learning e deep learning em cenários de cibersegurança, incluindo deteção avançada de ameaças, resposta automatizada e proteção de infraestruturas críticas. São abordados temas como adversarial AI, segurança de redes e endpoints, cloud e container security, blockchain, IAM e IoT security, proporcionando uma visão abrangente da engenharia de segurança orientada por IA.

A componente prática assume um papel central, com desenvolvimento de soluções completas de segurança com IA e um capstone project focado na conceção e implementação de sistemas de defesa inteligentes, permitindo consolidar competências técnicas e estratégicas em cenários reais.

Em parceria com a Rumos, Platinum Gold Partner.

Destinatários

- Profissionais séniores de cibersegurança;
- AI Security Engineers e arquitetos de segurança;
- Especialistas em cloud, DevSecOps e infraestruturas digitais;
- Ethical hackers e penetration testers com experiência avançada;
- Líderes tecnológicos e responsáveis por estratégia de segurança.

Objetivos

- Aplicar técnicas avançadas de IA e deep learning em cibersegurança;
- Desenvolver sistemas de deteção e resposta a ameaças em tempo real;
- Proteger infraestruturas cloud, redes e endpoints com IA;
- Implementar estratégias de defesa contra adversarial AI;
- Conceber arquiteturas seguras de sistemas de IA;
- Integrar IA em IAM, IoT e ambientes distribuídos;
- Liderar iniciativas avançadas de segurança orientadas por IA

Condições

Detalhes do exame

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

Pré-requisitos

- Conclusão recomendada das certificações AI+ Security Level 1™ e Level 2™;
- Conhecimentos avançados de cibersegurança (deteção de ameaças, incident response, network/endpoint security);
- Experiência em programação (Python) e frameworks de deep learning (ex.: TensorFlow, PyTorch);
- Conhecimentos sólidos de machine learning e deep learning;
- Familiaridade com ambientes cloud, containerização e ferramentas de segurança;
- Experiência com sistemas Linux e linha de comandos.

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
- Foundations of AI and Machine Learning for Security Engineering

- Machine Learning for Threat Detection and Response
- Deep Learning for Security Applications
- Adversarial AI in Security
- AI in Network Security
- AI in Endpoint Security
- Secure AI System Engineering
- AI for Cloud and Container Security
- AI and Blockchain for Security
- AI in Identity and Access Management (IAM)
- AI for Physical and IoT Security
- Capstone Project - Engineering AI Security Systems

Foundations of AI and Machine Learning for Security Engineering

- Core AI and ML Concepts for Security
- AI Use Cases in Cybersecurity
- Engineering AI Pipelines for Security
- Challenges in Applying AI to Security

Machine Learning for Threat Detection and Response

- Engineering Feature Extraction for Cybersecurity Datasets
- Supervised Learning for Threat Classification
- Unsupervised Learning for Anomaly Detection
- Engineering Real-Time Threat Detection Systems

Deep Learning for Security Applications

- Convolutional Neural Networks (CNNs) for Threat Detection
- Recurrent Neural Networks (RNNs) and LSTMs for Security
- Autoencoders for Anomaly Detection
- Adversarial Deep Learning in Security

Adversarial AI in Security

- Introduction to Adversarial AI Attacks
- Defense Mechanisms Against Adversarial Attacks
- Adversarial Testing and Red Teaming for AI Systems
- Engineering Robust AI Systems Against Adversarial AI

AI in Network Security

- AI-Powered Intrusion Detection Systems
- AI for Distributed Denial of Service (DDoS) Detection
- AI-Based Network Anomaly Detection
- Engineering Secure Network Architectures with AI

AI in Endpoint Security

- AI for Malware Detection and Classification
- AI for Endpoint Detection and Response (EDR)
- AI-Driven Threat Hunting
- Implementing Lightweight AI Models for Resource-Constrained Devices

Secure AI System Engineering

- Designing Secure AI Architectures
- Cryptography in AI for Security
- Ensuring Model Explainability and Transparency in Security
- Performance Optimization of AI Security Systems

AI for Cloud and Container Security

- AI for Securing Cloud Environments
- AI-Driven Container Security
- AI for Securing Serverless Architectures
- AI and DevSecOps

AI and Blockchain for Security

- Fundamentals of Blockchain and AI Integration
- AI for Fraud Detection in Blockchain
- Smart Contracts and AI Security
- AI-Enhanced Consensus Algorithms

AI in Identity and Access Management (IAM)

- AI for User Behavior Analytics in IAM
- AI for Multi-Factor Authentication (MFA)
- AI for Zero-Trust Architecture
- AI for Role-Based Access Control (RBAC)

AI for Physical and IoT Security

- AI for Securing Smart Cities
- AI for Industrial IoT Security
- AI for Autonomous Vehicle Security
- AI for Securing Smart Homes and Consumer IoT

Capstone Project – Engineering AI Security Systems

- Defining the Capstone Project Problem
- Engineering the AI Solution
- Deploying and Monitoring the AI System
- Final Capstone Presentation and Evaluation