



13 cursos

Secure AI Code & Libraries with Static Analysis

Secure AI: Threat Model & Test Endpoints

Optimize AI Inference Speed & Accuracy

Harden AI: Secure Your ML Pipelines

Secure AI Model Deployments & Lifecycles

Secure AI Interpret and Protect Models

Secure AI with Privacy and Access Controls

Secure AI: Red-Teaming & Safety Filters

Secure AI Systems Across Lifecycle Stages

Automate AI Anomaly Detection & Response

Harden AI: Patch and Recover Incidents Fast

Secure Mobile AI Models Against Attacks

Detect & Respond to Mobile AI Threats

**coursera**

Jul 12, 2026

**DYLAN ALEXANDER OYARZUN**

completó con éxito el programa especializado en línea

# AI Security: Security in the Age of Artificial Intelligence

Congratulations on completing the AI Security: Security in the Age of Artificial Intelligence Specialization! You now possess critical expertise in securing AI systems across their lifecycle. Through hands-on projects, you gained proficiency in threat modeling with MITRE ATLAS, vulnerability assessment, static analysis, and red-teaming. You learned to implement ML pipeline security controls, design resilient deployments, automate anomaly detection, and respond to AI-specific incidents. Your skills include protecting training environments, securing inference endpoints, and defending against adversarial attacks like prompt injection and data poisoning.

**coursera**

Experts in the field

Este certificado acredita que el estudiante completó un programa en línea impartido a través de Coursera. No constituye una inscripción formal en ninguna universidad o entidad, ni otorga por sí mismo créditos académicos, calificaciones o un título. Las instituciones u organizaciones pueden, a su discreción, reconocer este aprendizaje para sus propios programas o credenciales.

Verifica este certificado en:

<https://coursera.org/verify/specialization/SQIF7VRNK066>