SEC411: **AI Security Principles and Practices: GenAI and LLM Defense**

2 Day Course | 14 CPEs | Laptop Required

You Will Be Able To

- Build essential GenAI and LLM security skills, from tokenization and attack surface analysis to the OWASP Top 10 for LLMs—no AI background required
- Identify, exploit, and defend against AI-specific threats like prompt injection, jailbreaking, and RAG manipulation in hands-on labs
- Implement practical defenses for training pipelines, inference environments, and RAG systems across enterprise settings
- Secure advanced AI architectures, including agentic systems and reasoning models.
- Apply frameworks such as MITRE ATLAS, OWASP Top 10 for LLMs, and NIST AI RMF in real-world security operations
- Integrate AI security into existing SOC workflows and incident response

Who Should Attend

SEC411 is ideal for cybersecurity professionals seeking to understand and defend against threats introduced by generative AI and large language models. This includes:

- Security analysts
- Engineers
- SOC operators
- Incident Responders
- Red Teamers
- IT professionals who want to expand their skill set to include AI system security

No prior AI or data science experience is required—only a foundation in general cybersecurity principles.

SEC411 is a living, practitioner-focused AI security course for cybersecurity professionals entering GenAI and large language models (LLM) defense. No prior AI experience required.

The initial release features 14+ hours of expert-led content and three progressive hands-on labs. The curriculum continuously expands during your four-month access window, with new modules, lab challenges, and recordings added so your training keeps pace with the rapidly evolving AI threat landscape.

Through Docker-based labs and an integrated learning assistant, you will build skills from AI fundamentals and tokenization security to advanced prompt attacks, RAG vulnerabilities, and autonomous system defense.

SEC411 emphasizes practical, immediately applicable skills. You will exploit AI-specific vulnerabilities in hands-on labs and then implement production-ready defenses that actually work.

Business Takeaways

This course will help your organization:

- Rapidly upskill cybersecurity teams to address GenAI and LLM security without prior AI experience
- Continuous learning: new labs, modules, and recordings expand automatically during the four-month access window
- Gain deployable, real-world skills through Docker-based, hands-on labs
- Improve engagement and retention with gamified learning and an integrated learning assistant
- Reduce AI deployment risk and meet compliance requirements with NIST AI RMF, EU AI Act, and other standards
- Stay current on emerging threats through ongoing curriculum updates

Section Descriptions

SECTION 1: KNOW – Understanding the AI Threat Landscape

Build essential AI literacy for security professionals. Learn how LLMs operate, identify AI-specific attack surfaces, and apply the OWASP Top 10 for LLMs. This foundation bridges traditional security experience to AI threats with hands-on exploration of tokenization security.

TOPICS:

- Security implications of LLM architecture, training processes, and inference mechanisms
- AI system attack surface mapping and threat modeling using MITRE ATLAS
- OWASP Top 10 for LLM Applications, from prompt injection to model theft
- Tokenization vulnerabilities and exploitation techniques across different model families
- AI supply chain security, training data poisoning, and model manipulation tactics

SECTION 2: DEFEND – Securing the AI Lifecycle

Secure AI systems from training to runtime. Implement practical defenses for training pipelines, inference environments, and RAG systems. Master input and output filtering, guardrail implementation, and RAG-specific security controls through progressive attack and defense challenges.

TOPICS:

- Security implications of LLM architecture, training processes, and inference mechanisms
- AI system attack surface mapping and threat modeling using MITRE ATLAS
- OWASP Top 10 for LLM Applications, from prompt injection to model theft
- Tokenization vulnerabilities and exploitation techniques across different model families
- AI supply chain security, training data poisoning, and model manipulation tactics

SECTION 3: DEFEND – Securing the AI Lifecycle

Integrate AI security into enterprise architecture and protect autonomous systems. Deploy secure LLM applications, implement robust API security, connect AI monitoring with SOC operations, and address new threats in agentic systems and reasoning models using production-ready strategies.

TOPICS:

- Secure AI deployment architectures and API protections for LLM services
- Authentication, authorization, and monitoring integrated with existing security operations
- Security for agentic systems, including permission models, tool validation, and agent control
- Reasoning model security, focusing on chain-of-thought protection and defending against reasoning manipulation
- Incident response for AI security events and development of enterprise AI security programs