CENTER FOR CYBERSECURITY
AT THE UNIVERSITY OF WEST FLORIDA

EC-Council Generative AI for Cybersecurity

UWF Florida Cybersecurity Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course Dates: June 1 – June 12, 2026

Duration: 14 days

Instructional Hours: 16 contact hours

Delivery Format: Asynchronous online (courses)

Target Audience: Courses: IT and Cybersecurity practitioners or staff;
Required Prerequisites / Background: Students from any background is welcome, some prior knowledge of Cyber Security and coding useful but not essential;

CEUs: 1.5, **CPEs:** 18

Course Instructor(s):

Instructor	Email
Dr. Hossain Shahriar	hshahriar@uwf.edu

Course Description

The Generative AI for Cybersecurity provides the participants the knowledge to leverage Generative AI, including LLMs, in cybersecurity. By mastering Generative AI, the participants enable their respective organization's resilience against cyber threats. Learners will earn a certificate of completion after completing all required assessment items from EC-Council.

Student Learning Outcomes: At the end of this course, students will be able to:

- Describe how LLM works with architecture
- Explain how LLM can be used for solving cybersecurity related tasks
- How to choose LLM technology based on open or closed source
- Apply prompt engineering and fine tuning to address problem solving

NIST NICE Cybersecurity Workforce Framework Mapping

The course addresses cybersecurity work roles as identified in NIST's Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

NICE Cyber Security Framework (CSF) Work Roles

- Data Analysis (IO-WRL-001)
- Knowledge Management (IO-WRL-003)
- System Security Analysis (IO-WRL-006)

DoD Cybersecurity Workforce Framework (DCWF) Work Roles

- Data Analyst (DCWF Code: 422
- AI/ML Specialist (DCWF Code: 623)
- AI Adoption Specialist (DCWF Code: 753)

Knowledge and Skills required to fulfill the above work roles mapped to the NICE Cybersecurity Workforce Framework:

- Knowledge of machine learning principles and practices (K0904)
- Knowledge of data mining tools and technologies (K0953)
- Knowledge of analytics (K1101)
- Skill in creating mathematical models (S0562)
- Skill in creating statistical models (S0563)
- Skill in performing regression analysis (S0640)
- Skill in conducting trend analysis (S0169)
- Determine data requirements (T1063)

Knowledge and Skills required to fulfill the above work roles mapped to the DoD Cybersecurity Workforce Framework:

- Design and develop machine learning models to achieve organizational
- objectives. (KSAT ID: 5871)
- Design, develop, and implement AI tools and techniques to achieve
- organizational objectives. (KSAT ID: 5872)
- Research the latest machine learning and AI tools, techniques, and
- best practices. (KSAT ID: 5915)
- Knowledge of current AI and machine learning systems design and
- performance analysis models, algorithms, and tools. (KSAT ID: 7011)
- Knowledge of the benefits and limitations of AI capabilities. (KSAT ID:
- 7048)
- Skill in explaining AI concepts and terminology. (KSAT ID: 7065)

Course Information

Materials: All course materials will be provided by the instructor free of cost; the following are some online resources

Optional and additional online resources can be found in the following:

- Introduction to LLM, https://developers.google.com/machine-learning/resources/intro-llms

- AI for cyber security, https://www.blackberry.com/us/en/solutions/endpoint-security/cybersecurity-ai
- Prompt engineering for Generative AI, https://developers.google.com/machine-learning/resources/prompt-eng?hl=en
- Adversarial Attacks, https://www.analyticsvidhya.com/blog/2022/09/machine-learning-adversarial-attacks-and-defense

Technical Specifications:

Participants need access to a computer with stable internet connection. They will be required to access the course Leaning Management System (LMS) portal, Canvas and the EC-Council web portal. By enrolling for this course, you agree to abide by the Computing Resource Usage Agreement provided to you.

Grading:

The course is designed for course completion. Students should complete all assignments and take time to review any incorrect answers. Students shall receive a grade of either complete or incomplete at the conclusion of the course. Participants must earn a total of 70% or higher on graded assessments to earn a course completion grade. Students will receive a course completion certificate from EC-Council and UWF Continuing Education and a digital badge.

Course Overview / Schedule

Modules and Lessons	Assessment
Module 1: Decoding Generative AI and Large Language Models (LLMs) • Introduction to Generative AI (GenAI) and LLMs • Inner Workings of LLMs • Broad Application Spectrum of LLMs	Knowledge Check / Quiz
Module 2: LLM Architecture o Design Patterns and Security Controls o Architecture Design Patterns of LLM-powered Applications o Security in LLM-powered Application Architecture	Knowledge Check / Quiz, Lab
Module 3: LLM Technology Stacks and Security Consideration o Choosing the Right Technology Stack for LLM Applications o Maximizing Security in LLM Technology Stacks	Knowledge Check / Quiz, Lab
Module 4: Open-sourced vs. Closed-sourced LLMs	Knowledge Check / Quiz

o Evaluating Open vs. Closed-sourced LLMs o Tools for Evaluating Open-sourced LLMs o Closed-sourced LLMs in Specific	
Module 5: Hands-on o Prompt Engineering and LLM Fine-tuning	Knowledge Check / Quiz