Applications of Generative AI in Cybersecurity

Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course Dates: Monday, January 12, 2026

Duration: 1 day

Estimated Time Commitment: 7 hours

Instructional Hours: 7 contact hours

Delivery Format: Synchronous online (Zoom)

Target Audience: IT and cybersecurity practitioners

Required Prerequisites / Background: Experience in at least one area of cybersecurity (e.g., defensive security, forensics, ethical hacking)

CEUs: 0.7, **CPEs:** 9

Course Instructor(s): Dr. Jeremy Straub ● jstraub@uwf.edu

Course Description

In the rapidly evolving landscape of cybersecurity, the integration of generative artificial intelligence (AI) presents both innovative solutions and new challenges. This course is designed for students eager to explore the intersection of these two dynamic fields. Throughout the course, students will delve into the foundational concepts of generative AI, including its algorithms, methodologies, and applications. Key learning objectives include understanding how generative AI can enhance threat detection and response strategies by analyzing vast datasets to identify patterns and anomalies. Students will also explore the development of AI-driven security protocols and automated systems that can adapt to emerging threats in real-time. The course will cover ethical considerations and the potential risks associated with deploying AI in security contexts, including issues of privacy, bias, and misinformation. By the end of the course, students will have an understanding of how generative AI can be leveraged for both defensive and offensive cybersecurity strategies

Course Topics and Schedule

Module	Title
1	Introduction to Generative AI
2	Generative AI for Threat Detection
3	AI-Driven Security Protocols and Automated Systems

4	Generative AI for Vulnerability Discovery
5	Ethical Considerations of AI in Cybersecurity
6	Defensive Cybersecurity Strategies with Generative AI
7	Offensive Cybersecurity Strategies with Generative AI

Module 1: Introduction to Generative AI
This module provides a foundational understanding of generative AI. Students will learn about the core concepts, algorithms (e.g., GANs, VAEs, transformers), and methodologies behind generative models. We will explore the history of generative AI, its evolution, and its current state-of-the-art techniques. The module will also cover the mathematical underpinnings of these models, providing students with the necessary theoretical background to understand how they work. Examples of different types of generative models and their applications in various fields will be discussed to illustrate the versatility of this technology. This module sets the stage for understanding how generative AI can be applied to cybersecurity.

Module 2: Generative AI for Threat Detection
This module explores how generative AI can be used to enhance threat detection capabilities. Students will learn how generative models can analyze vast datasets of network traffic, system logs, and other security data to identify patterns and anomalies that may indicate malicious activity. We will discuss techniques for training generative models to detect novel attacks and zero-day exploits. The module will also cover the use of generative AI for creating synthetic data to train and evaluate threat detection systems. Students will learn how to implement and evaluate generative AI-based threat detection systems.

Module 3: AI-Driven Security Protocols and Automated Systems
This module focuses on the development of AI-driven security protocols and automated systems that can adapt to emerging threats in real-time. Students will learn how generative AI can be used to create adaptive security policies and automated response mechanisms. We will discuss techniques for using generative models to generate security rules and configurations. The module will also cover the use of AI for automating incident response and remediation. Students will learn how to design and implement AI-driven security systems that can proactively defend against cyberattacks.

Module 4: Generative AI for Vulnerability Discovery
This module explores the use of generative AI in discovering vulnerabilities in software and systems. Students will learn how generative models can be used to generate test cases and fuzzing inputs to identify security flaws. We will discuss techniques for using generative AI to automatically generate exploits for discovered vulnerabilities. The module will also cover the use of AI for analyzing code and identifying potential security weaknesses. Students will learn how to use generative AI to improve the security of software and systems.

Module 5: Ethical Considerations of AI in Cybersecurity
This module delves into the ethical considerations and potential risks associated with deploying AI in security contexts. Students will explore issues of privacy, bias, and misinformation. We will discuss the ethical implications of using AI for surveillance and monitoring. The module will also cover the potential for AI to be used for malicious purposes, such as creating deepfakes or generating propaganda. Students will learn how to develop and deploy AI systems in a responsible and ethical manner.

Module 6: Defensive Cybersecurity Strategies with Generative AI
This module focuses on defensive cybersecurity strategies that leverage generative AI. Students will learn how to use generative models to create realistic simulations of cyberattacks for training and testing purposes. We will discuss techniques for using generative AI to improve security awareness and educate users about potential threats. The module will also cover the use of AI for creating adaptive security defenses that can respond to evolving threats. Students will learn how to implement and manage defensive cybersecurity strategies using generative AI.

Module 7: Offensive Cybersecurity Strategies with Generative AI
This module explores offensive cybersecurity strategies that leverage generative AI. Students will learn how to use generative models to create sophisticated phishing attacks and social engineering campaigns. We will discuss techniques for using generative AI to generate malware and exploits. The module will also cover the use of AI for reconnaissance and information gathering. Students will learn about the ethical and legal implications of using generative AI for offensive purposes. This module is intended to provide a comprehensive understanding of the potential uses and misuses of generative AI in cybersecurity.

NOTE: This syllabus contains AI generated content and AI-generated content will be presented throughout this course.