Generative AI: Boost Your Cybersecurity Career

Provider: IBM (Coursera)
Completion Date: September 9, 2025

Overview

This course explored how generative AI enhances cybersecurity by improving analytics, incident response, and forensic investigations. It addressed risks in large language models (LLMs), including bias, prompt injection, and data poisoning, and emphasized governance and ethical considerations. Hands-on labs applied generative AI for malware detection, content filtering, and preventing malicious code execution.

Key Topics Covered

- Generative AI fundamentals vs. conventional AI
- Security risks in LLMs: bias, data leakage, prompt injection, inadequate sandboxing
- SIEM and SOC integration with generative AI
- Cybersecurity analytics: descriptive, predictive, prescriptive, and behavioral
- AI-enhanced incident response, playbooks, and threat hunting
- Applications in vulnerability management, user behavior analytics, and content filtering
- Ethical, regulatory, and compliance considerations for AI use

Practical Applications

- Using generative AI to analyze threats and anomalies overlooked by conventional AI
- Automating playbooks for incident response and forensic analysis
- Detecting malware and keyloggers through AI-driven code inspection
- Enhancing SIEM/EDR functions for faster detection and response
- Supporting compliance reporting and governance with AI-based monitoring

Personal Reflection

This course demonstrated how generative AI can strengthen cybersecurity by enhancing threat detection and response. I learned to evaluate LLM risks, automate playbooks, and apply AI for analytics and compliance. These skills complement my GRC and technical training, preparing me to manage AI-driven security risks and leverage AI as a defensive tool.