GENERATIVE AI & CYBERSECURITY

INDUSTRY-READY PROGRAM

A 7-Day Hands-On Immersive Curriculum

For B.Tech / M.Tech / BCA / MCA Students
Offered in Collaboration with the Innovation Foundation

Introduction

In today's rapidly evolving technology landscape, cybersecurity and Generative AI have emerged as two of the most critical and in-demand skill sets across every industry. Organizations are actively seeking professionals who can not only defend digital infrastructure but also build and deploy intelligent AI-powered systems that drive innovation.

Recognizing this need, we are pleased to propose a **7-Day Industry-Ready Program in Cybersecurity and Generative AI**, designed in collaboration with the Innovation Foundation, exclusively for B.Tech, M.Tech, BCA, and MCA students. This hands-on, immersive program is structured to take students from foundational concepts to practical, real-world application — with no prior experience assumed.

The program is divided into two complementary tracks. The first three days focus on **Cybersecurity Foundations**, building core competencies in Linux, networking, system hardening, and both defensive and offensive security techniques, culminating in a Capture The Flag (CTF) challenge that tests everything students have learned. The remaining days shift focus to **Generative AI Engineering**, where students explore Large Language Models, build real applications using LangChain, work with vector databases and retrieval-augmented generation (RAG), and step into the emerging world of autonomous AI agents using the CrewAI framework.

Every technical day is anchored in hands-on projects rather than theory alone, ensuring students leave with practical, demonstrable skills — not just conceptual knowledge. The program concludes with a dedicated session on resume building, LinkedIn optimization, and industry readiness, ensuring students can effectively translate what they've learned into career opportunities.

By the end of this program, participants will have built a working portfolio of cybersecurity and Generative AI projects, gained confidence in tools and techniques used across the industry today, and received clear guidance on certifications and next steps for continued learning.

This document outlines the day-wise curriculum, learning outcomes, and delivery details of the program for review and approval.

Days 1–3: Cybersecurity Foundations

Day 1 – Linux & Network Mechanics

- The CIA Triad: Confidentiality, Integrity, Availability
- Linux fundamentals: file navigation, essential commands (ls, cd, pwd, cat, man, find)
- SSH access and secure remote connections
- TCP/IP model, IP addresses, ports, and protocols (TCP vs. UDP)
- Network diagnostics: ping, traceroute, netstat/ss
- Secure vs. insecure protocols (SSH vs. Telnet/HTTP)
- Hands-on Lab: OverTheWire Bandit (Levels 0–3), network diagnostics

Day 2 – Defensive Security: Analysis & Hardening

- Privilege principles and Linux file permissions
- User management, password policies, strong authentication
- Secure file transfer practices
- Network defense concepts and packet sniffing fundamentals
- Wireshark: capturing/filtering traffic, identifying protocols (HTTP, DNS, ARP)
- Live demo: spotting clear-text credentials in traffic
- Hands-on Lab: File permission hardening with chmod; Wireshark packet analysis

Day 3 – Offensive Security: Vulnerabilities & Capture The Flag

- OWASP Top 10 overview and web request lifecycle
- Introduction to command injection and vulnerability scanning (nmap)
- Browser developer tools for source/traffic inspection
- Intro to CTF competitions (PicoCTF structure), ethical hacking principles
- Responsible disclosure and career paths in cybersecurity
- Hands-on Lab: Web reconnaissance, PicoCTF challenges, team-based CTF

Days 4–6: Generative AI Engineering

Day 4 – Foundations of Generative AI, LLMs & LangChain Basics

- What is Generative AI: key concepts, evolution from rule-based systems to GPT/ChatGPT

- LLM basics: Transformers, attention mechanism, architecture behind GPT, BERT, T5
- Prompt engineering fundamentals
- What is LangChain: core components — LLM interface, Prompt Templates, Chains, Memory
- Hands-on Projects: *summarizedialogue-using-prompt-engineering, Question-Answering-app*

Day 5 – LangChain Applications, Vector Databases & RAG

- Connecting LLMs to structured data (SQL, CSVs) and content generation workflows
- What is a vector database; understanding vectors and embeddings
- Similarity search: cosine similarity, Euclidean distance, nearest-neighbor search
- How vector databases power RAG (Retrieval-Augmented Generation) pipelines
- Hands-on Projects: *Multi-Document QA System using RAG, FAISS & Cohere, Chat with your CSV Data*

Day 6 – Agentic AI & CrewAI

- What are AI agents? How agents reason and choose tools dynamically
- Introduction to Agentic AI and the CrewAI framework
- Designing multi-agent crews: roles, tasks, collaboration
- Hands-on Projects: *Tailoring-job-applications-using-CrewAI, Agentic AI Stock Advisor*

Day 7 – Resume Building, LinkedIn Optimization & Industry-Ready Workshop

- Building a resume that showcases your talent
- LinkedIn profile optimization: headline, summary, skills, project showcase
- Industry expectations, interview tips, common job roles in security & GenAI
- Certifications and next steps for continued learning
- Valedictory session: project showcase, feedback, and closing remarks

Total: **7 Days × 2 Hours/Day = 14 Hours**