Professional Program in Cyber Security

Certification: Professional Certificate in Cyber Security
Training Provider: Alltix Educators

This program prepares students to understand and defend modern digital infrastructures against cyber threats. Students will develop skills in **network security, ethical hacking, threat analysis, and cyber defense strategies** used by organizations worldwide.

The program focuses on **practical learning, real world simulations, and modern cyber security technologies** used by security professionals.

Level 1 – Cyber Security Fundamentals

Duration: 3 Months (Beginner)

This level introduces students to the **core principles of cyber security, digital threats, and system protection techniques**.

Learning Objectives

Students will learn:

• Foundations of cyber security
• Understanding cyber threats and vulnerabilities
• Network security fundamentals
• Basic ethical hacking concepts
• Cyber security best practices

Course Modules

Module 1 – Introduction to Cyber Security

- Evolution of cyber security
- Types of cyber threats
- Understanding cyber attacks
- Security principles and frameworks

Module 2 – Computer Systems & Networking

- Basics of computer systems
- Network architecture and protocols
- IP addressing and communication
- Understanding internet infrastructure

Module 3 – Cyber Threat Landscape

- Malware types (viruses, trojans, ransomware)
- Phishing and social engineering attacks
- Cyber attack methodologies
- Case studies of major cyber incidents

Module 4 – Security Fundamentals

- Authentication and access control
- Password security
- Encryption basics
- Secure communication methods

Module 5 – Ethical Hacking Introduction

- Understanding ethical hacking
- Penetration testing concepts
- Vulnerability assessment basics

Module 6 – Practical Security Exercises

Students will perform basic **cyber security analysis and threat identification exercises**.

Level 2 – Cyber Security Specialist

Duration: 6 Months (Intermediate)

This level focuses on **practical security operations, penetration testing, and threat analysis techniques**.

Learning Objectives

Students will learn:

• Vulnerability assessment techniques
• Ethical hacking methodologies
• Network security monitoring
• Security incident response

Course Modules

Module 1 – Network Security

- Firewall technologies
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Network monitoring techniques

Module 2 – Ethical Hacking Techniques

- Penetration testing process
- Reconnaissance and information gathering
- Exploiting vulnerabilities
- Privilege escalation techniques

Module 3 – Web Application Security

- Web vulnerabilities (SQL injection, XSS)

- Secure web application development
- Web penetration testing techniques

Module 4 – Digital Forensics

- Introduction to digital forensics
- Evidence collection techniques
- Incident investigation methods
- Cyber crime analysis

Module 5 – Security Operations

- Security monitoring tools
- Threat intelligence analysis
- Security incident response procedures

Module 6 – Hands-On Security Labs

Students will perform **real-world cyber attack simulations and defensive security exercises**.

Level 3 – Advanced Cyber Security & Ethical Hacking

Duration: 1 Year (Advanced)

This level prepares students for **professional cyber security careers**, focusing on advanced threat defense and enterprise security architecture.

Learning Objectives

Students will learn:

• Advanced penetration testing
• Security infrastructure design
• Threat intelligence and cyber defense
• Enterprise security management

Course Modules

Module 1 – Advanced Ethical Hacking

- Advanced penetration testing techniques
- Exploit development basics
- Red team vs blue team strategies
- Advanced vulnerability exploitation

Module 2 – Security Architecture

- Designing secure systems
- Enterprise security frameworks
- Risk management strategies
- Security policy development

Module 3 – Cloud Security

- Cloud infrastructure security
- Identity and access management
- Data protection in cloud environments

Module 4 – Cyber Threat Intelligence

- Threat intelligence collection
- Malware analysis fundamentals
- Advanced cyber attack detection

Module 5 – Security Automation

- Security monitoring automation
- AI in cyber security defense
- Automated threat detection systems

Module 6 – Capstone Security Project

Students will develop a **complete cyber security defense framework or perform a simulated enterprise penetration test**.

Practical Training

Students will gain hands-on experience with:

• Cyber security labs
• Ethical hacking simulations
• Network security monitoring tools
• Vulnerability scanning and penetration testing

Program Benefits

Students completing the program will:

• Understand modern cyber threats and defense strategies
• Learn ethical hacking and penetration testing techniques
• Develop skills to protect digital infrastructures
• Gain hands-on experience with cyber security tools
• Build a professional cyber security portfolio

Career Opportunities

Graduates may pursue careers such as:

• Cyber Security Analyst
• Ethical Hacker
• Network Security Engineer
• Security Operations Analyst
• Penetration Tester

Certification

Students who successfully complete the program will receive a **Professional Certificate in Cyber Security from Alltix Educators**.