

**SkillNexa Cybersecurity Academy**

**Cybersecurity Engineering Capstone**

**University & Career Preparation Track**

**Program Level:** Engineering Capstone  
**Total Duration:** 96 Hours  
**Delivery:** Cohort-Based + Instructor-Led + Hands-On Labs  
**Pathway:** Foundation → Practitioner → Specialist → **Engineering Capstone**

---

**Program Goal**

Students transition from cybersecurity specialist to engineering capstone.

Students learn:

- Security engineering
  - Secure system design
  - Penetration testing
  - AI security
  - Cyber risk management
  - Security research
  - Industry-focused projects
  - A cybersecurity portfolio
  - Technical project experience
  - Research presentation skills
  - Exposure to university-level cybersecurity concepts
  - Career readiness
- 

**Program Structure Overview**

| Module   | Topic                                     | Hours    |
|----------|-------------------------------------------|----------|
| Module 1 | Advanced Security Engineering             | 20 Hours |
| Module 2 | Penetration Testing & Security Assessment | 24 Hours |

|              |                                            |                 |
|--------------|--------------------------------------------|-----------------|
| Module 3     | AI & Cybersecurity                         | 16 Hours        |
| Module 4     | Cybersecurity Governance & Risk Management | 16 Hours        |
| Module 5     | Senior Cybersecurity Capstone Project      | 20 Hours        |
| <b>Total</b> |                                            | <b>96 Hours</b> |

## **Course Curriculum**

### **MODULE 1 — ADVANCED SECURITY ENGINEERING**

#### **1.1 Secure Architecture Fundamentals**

##### **LAB 1.1**

#### **1.2 Zero Trust Security**

##### **LAB 1.2**

#### **1.3 Security Design Principles**

##### **LAB 1.3**

#### **1.4 Enterprise Security Architecture**

##### **LAB 1.4**

#### **1.5 Security Engineering Project**

### **MODULE 1 ASSESSMENT**

### **MODULE 2 — PENETRATION TESTING & SECURITY ASSESSMENT**

#### **2.1 Introduction to Penetration Testing**

##### **LAB 2.1**

## **2.2 Security Assessment Planning**

### **LAB 2.2**

## **2.3 Vulnerability Analysis**

### **LAB 2.3**

## **2.4 Controlled Security Testing**

### **LAB 2.4**

## **2.5 Security Reporting**

### **LAB 2.5**

## **2.6 Penetration Testing Project**

## **MODULE 2 ASSESSMENT**

## **MODULE 3 — AI & CYBERSECURITY**

## **3.1 AI in Cybersecurity**

### **LAB 3.1**

## **3.2 AI-Powered Cyber Threats**

### **LAB 3.2**

## **3.3 AI Security Risks**

### **LAB 3.3**

## **3.4 Responsible AI & Cybersecurity**

### **Lab 3.4**

## **MODULE 3 ASSESSMENT**

## **MODULE 4 — CYBERSECURITY GOVERNANCE & RISK MANAGEMENT**

### **4.1 Security Policies**

#### **LAB 4.1**

### **4.2 Cybersecurity Risk Management**

#### **LAB 4.2**

### **4.3 Business Impact**

#### **LAB 4.3**

### **4.4 Cybersecurity Frameworks**

#### **LAB 4.4**

### **4.5 Governance Project**

## **MODULE 4 ASSESSMENT**

## **MODULE 5 — SENIOR CYBERSECURITY ENGINEERING CAPSTONE**

### **5.1 Capstone Project Selection**

### **5.2 Capstone Planning**

#### **LAB 5.2**

### **5.3 Capstone Design & Development**

#### **LAB 5.3**

### **5.4 Technical Documentation**

## **5.5 Cybersecurity Portfolio**

### **LAB 5.5**

## **5.6 Capstone Presentation**

## **MODULE 5 ASSESSMENT**

## **FINAL ASSESSMENT**