Icrust Digital Academy
Learn Digital Skills. Build Your Future.

Phone: 0805555646 Facebook: facebook.com/icrustdigitalacademy Website: icrustacademy.ng

Cybersecurity Curriculum

Start a beginner-friendly cybersecurity path and understand security basics, risk, and threat awareness.

Duration: 8 weeks
Format: Online classes with foundational labs
Level: Beginner Friendly

Program Overview

A practical cybersecurity curriculum covering security foundations, networks, threats, incident response, and analyst tools including Linux, SQL, and Python basics.

What Students Will Achieve

- Understand how organisations protect systems, people, and data
- Identify common threats, vulnerabilities, and defensive controls
- Work with core analyst tools and environments such as Linux and SQL
- Practice threat detection, incident response, and security reporting

Tools and Platforms

Security labs | Network utilities | Browser tools | Documentation workflows

Curriculum Modules

Module 01: Cybersecurity Foundations and Risk Awareness

Develop the core mindset, vocabulary, and principles behind defensive security work.

- Security goals, risk concepts, and security roles
- Common attack types, fraud, phishing, and social engineering
- Confidentiality, integrity, availability, and governance basics

Practical Output: A threat-and-risk briefing document

Module 02: Networks, Systems, and Access Control

Understand how systems communicate and where defensive controls are applied.

- Network fundamentals, protocols, and device roles
- Authentication, authorisation, and access management basics
- Security controls for endpoints, users, and internal systems

Practical Output: A network security mapping exercise

Module 03: Linux, SQL, and Analyst Tooling

Build familiarity with technical environments commonly used by cybersecurity analysts.

- Linux navigation, file permissions, and command-line basics
- SQL queries for reviewing logs and records
- Working with datasets and simple analyst workflows

Practical Output: A lab workbook using Linux and SQL tasks

Module 04: Threats, Vulnerabilities, and Security Monitoring

Learn how to think like a defender when reviewing exposure and suspicious activity.

- Threat actors, vulnerabilities, and attack surfaces
- Log analysis, alert review, and suspicious activity patterns
- Basic SIEM concepts and monitoring workflows

Practical Output: A threat review and alert triage exercise

Module 05: Incident Response and Defensive Operations

Practice structured response steps when issues are detected.

- Incident lifecycle, escalation, and containment logic
- Evidence handling, reporting, and communication
- Hardening and response playbook thinking

Practical Output: An incident report with response recommendations

Module 06: Automation, Portfolio Labs, and Career Readiness

Package your security learning into practical outputs and next-step readiness.

- Python basics for simple security tasks and automation logic
- Portfolio labs and security documentation
- Career pathway guidance for entry-level cybersecurity roles

Practical Output: A portfolio-ready cybersecurity case study

Capstone Project

Complete a security operations style case study where you review alerts, investigate suspicious activity, document findings, and recommend response actions.

Icrust Digital Academy

Learn Digital Skills. Build Your Future.

Phone: 0805555646 Facebook: facebook.com/icrustdigitalacademy Website: icrustacademy.ng

Student Support

- Mentorship and guided support throughout the learning journey
- Certificate of completion after successful participation
- Career guidance to help position students for opportunities