SCOPIO
SECURITY

CYBERSECURITY ACADEMY BROCHURE

With Collins Erughe

Month 1

Introduction to Information Technology (IT)

Week 1: Understanding Computers and Operating Systems

- Day 1: Introduction to computer hardware components and their functions.
- Day 2: Overview of operating systems: Windows, Linux, and macOS.
- Day 3: Basic navigation and file management in Windows and Linux.

Week 2: Operating Systems

- Day 7: Introduction to Windows system administration
- Day 8: Introduction to Linux system
- Day 9: Installing and configuring a virtualized Windows and Linux system.

Week 3: Cybersecurity Concepts and Threat Landscape

- Day 10: Understanding different types of cyber threats (malware, phishing, ransomware, social engineering).
- Day 11: Introduction to attack vectors and the Cyber Kill Chain framework.
- Day 12: Overview of cybersecurity frameworks (NIST, MITRE ATT&CK) and their importance in security operations.

Week 4: Networking Fundamentals

- Day 4: Understanding network topologies and architectures.
- Day 5: Introduction to the OSI and TCP/IP models.
- Day 6: Basics of IP addressing

Month 2 & 3

Beginner-Level Cybersecurity

Week 5: Cybersecurity Fundamentals

- Day 13: Introduction to cybersecurity concepts: Confidentiality, Integrity, Availability (CIA Triad).
- Day 14: Overview of common cyber threats and attack vectors.
- Day 15: Understanding cybersecurity laws, ethics, and the role of a Security Operations Center (SOC).

Week 6: Security Policies and Procedures

- Day 16: Introduction to security policies, standards, and guidelines.
- Day 17: Understanding risk management and assessment.
- Day 18: Developing and implementing security policies within an organization.

Week 7: Introduction to Cryptography

- Day 19: Basics of encryption and decryption.
- Day 20: Understanding symmetric and asymmetric cryptography.
- Day 21: Overview of hashing and digital signatures.

Week 8: Introduction to Security Tools

- Day 25: Overview of antivirus, firewalls, and intrusion detection systems.
- Day 26: Introduction to Security Information and Event Management (SIEM) systems.
- Day 27: Hands-on lab: Configuring and using basic security tools.

Week 9: Hands-on Lab Sessions

- Day 22: Setting up a virtual lab environment for practice.
- Day 23: Simulating basic network attacks and monitoring.
- Day 24: Analyzing logs and identifying potential threats.

Week 10: Network Security Basics

- Day 28: Understanding network security fundamentals.
- Day 29: Introduction to Virtual Private Networks (VPNs) and secure communication.
- Day 30: Basics of wireless security and common vulnerabilities.

Week 11: Endpoint Security

- Day 31: Overview of endpoint security solutions and their importance.
- Day 32: Understanding malware types, behaviors, and analysis basics.
- Day 33: Hands-on lab: Basic malware analysis in a controlled environment.

Week 12: Incident Response Fundamentals

- Day 34: Introduction to incident response lifecycle and methodologies.
- Day 35: Understanding Indicators of Compromise (IoCs) and attack methodologies.
- Day 36: Basics of threat intelligence and its role in incident detection.

Month 4 & 5

Advanced Cybersecurity Concepts

Week 13: Advanced Network Security

- Day 37: Deep dive into Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
- Day 38: Network traffic analysis and packet capturing techniques.
- Day 39: Hands-on lab: Analyzing network traffic for suspicious activities.

Week 14: Vulnerability Management

- Day 40: Understanding vulnerability assessment and management processes.
- Day 41: Overview of common vulnerability scanning tools.
- Day 42: Hands-on lab: Performing a vulnerability scan and analyzing results.

Week 15: Security Orchestration, Automation, and Response (SOAR)

- Day 43: Introduction to SOAR platforms and their role in SOC operations.
- Day 44: Automating incident response workflows.
- Day 45: Hands-on lab: Implementing a basic SOAR playbook.

Week 16: Compliance and Legal Considerations

- Day 46: Understanding regulatory requirements and compliance standards (e.g., GDPR, HIPAA).
- Day 47: Legal aspects of cybersecurity and data protection.
- Day 48: Case studies on compliance failures and lessons learned.

Week 17: Advanced Threat Intelligence

- Day 49: Gathering and analyzing threat intelligence from various sources.
- Day 50: Integrating threat intelligence into SOC operations.
- Day 51: Hands-on lab: Developing a threat intelligence report.

Week 18: Security Device Management

- Day 52: Managing and configuring firewalls, IDS/IPS, and other security devices.
- Day 53: Monitoring and maintaining security device health and performance.
- Day 54: Hands-on lab: Configuring and managing a firewall.

Week 19: Cloud Security Fundamentals

- Day 55: Introduction to cloud computing and its security implications.
- Day 56: Understanding cloud service models (IaaS, PaaS, SaaS) and deployment models.
- Day 57: Overview of cloud security best practices and common threats.

Week 20: Advanced Security Monitoring

- Day 58: Understanding log management and analysis in security operations.
- Day 59: Advanced use of SIEM tools for threat detection and response.
- Day 60: Hands-on lab: Configuring alerts and analyzing data in a SIEM platform.

Month 6

Introduction to Security Blue Team Operations

Week 21: SOC Basics and Structure

- Day 61: Introduction to the Security Operations Center (SOC): roles and responsibilities.
- Day 62: Overview of SOC workflows and processes.
- Day 63: Tools and technologies used in SOC operations.

Week 22: Threat Hunting and Analysis

- Day 64: Introduction to threat hunting: concepts and methodologies.
- Day 65: Identifying and analyzing Indicators of Compromise (IoCs).
- Day 66: Hands-on lab: Conducting a basic threat hunt.

Week 23: Incident Response in Depth

- Day 67: Deep dive into the incident response process: detection, containment, eradication, recovery.
- Day 68: Understanding and creating incident reports.
- Day 69: Hands-on lab: Simulating an incident response scenario.

Week 24: Final Review and Career Preparation

- Day 70: Review of key concepts and tools covered in the course.
- Day 71: Resume building and interview preparation for a SOC Analyst role.
- Day 72: Capstone project: Setting up and running a mini SOC, including threat monitoring and incident response.

CYBERSECURITY TRAINING PROGRAM: BEGINNER TO BLUE TEAM ANALYST IN 6 MONTHS

COURSE OVERVIEW

This 6-month cybersecurity training program is designed to take students with little or no IT experience and turn them into job-ready candidates for entry-level roles in cybersecurity, particularly in Security Operations Centers (SOCs). The program follows a progressive structure, starting with foundational IT knowledge, building up to core cybersecurity concepts, and culminating in hands-on defensive security operations training.

CYBERSECURITY TRAINING PROGRAM: BEGINNER TO BLUE TEAM ANALYST IN 6 MONTHS

COURSE FORMAT

- Duration: 6 Months (24 Weeks)
- Pace: Structured, guided daily lessons (3 days/week)
- Style: Combination of theory, hands-on labs, and real-world projects
- Goal: Prepare students for junior cybersecurity roles such as SOC Analyst, Security Analyst, or Threat Intelligence Analyst

MONTH-BY-MONTH BREAKDOWN

MONTH 1: INTRODUCTION TO INFORMATION TECHNOLOGY (IT)

- This foundational month ensures students understand the basics of computers and networks:
- Learn computer hardware and operating systems (Windows, Linux, macOS)
- Explore basic file systems, virtualization, and system installation
- Dive into networking basics: IP addressing, OSI/TCP models, and topologies

MONTH-BY-MONTH BREAKDOWN

MONTH 2 & 3: BEGINNER-LEVEL CYBERSECURITY

Students are introduced to the cybersecurity world, including:

- Cyber threat types (malware, phishing, ransomware, etc.)
- Core cybersecurity principles (CIA triad, risk management)
- Laws and ethics in cybersecurity
- Basic security tools and practices (firewalls, antivirus, SIEM)
- Introduction to cryptography and its real-world uses
- Hands-on labs simulating simple attacks and defenses

MONTH-BY-MONTH BREAKDOWN

MONTH 4 & 5: ADVANCED CYBERSECURITY CONCEPTS

At this stage, students begin working with more technical, real-world security practices:

- Endpoint protection and malware analysis
- Incident response and threat intelligence
- Vulnerability management and penetration testing basics
- Use of industry tools such as IDS/IPS systems, SOAR platforms, and SIEMs
- Cloud security, advanced monitoring, and regulatory compliance

MONTH-BY-MONTH BREAKDOWN

MONTH 6: INTRODUCTION TO BLUE TEAM OPERATIONS

The final month focuses on preparing students for real-world SOC environments:

- Deep dive into SOC workflows, tools, and analyst responsibilities
- Threat hunting, log analysis, and incident response simulations
- Resume building and interview prep
- Final capstone project: setting up and running a mini Security Operations Center (SOC)

WHAT STUDENTS WILL LEARN

By the end of the course, students will:

- Understand how IT systems work, including networks and operating systems
- Be familiar with common cyber threats and how they work
- Know how to implement basic defensive measures and respond to threats
- Be able to set up and use cybersecurity tools like firewalls, SIEMs, and IDS
- Have hands-on experience in real-world SOC scenarios, including detecting and responding to incidents
- Be ready to apply for cybersecurity roles with a strong foundational skill set and a practical capstone project

WHO THIS COURSE IS FOR

This course is perfect for:

- Beginners with little or no IT background
- Career switchers looking to break into cybersecurity
- Entry-level IT professionals looking to upskill into a security role
- Students or recent graduates with an interest in defending digital systems

SCOPIO SECURITY

THANK YOU!