CyberOps Associate

Course Details:

Target Audience: Students enrolled in technology degree programs at higher education institutions; IT professionals who wants to pursue a career in Security Operations.
Estimated Time to Completion: 70 hours (3 weeks)

Prerequisites: Introduction to Cybersecurity, Cybersecurity Essentials

Course Delivery: Instructor-led

Learning Component Highlights:

- 8 chapters and 12 practice labs
- 10 Cisco Packet Tracer activities
- 40+ interactive activities & quizzes
- 1 final exam

Course Recognitions: Certificate of Completion, Letter of Merit, Digital Badge

Recommended Next Course: CyberOps Associate

Course Outline:

- Defining the Security Operations Center
- Understanding Network Infrastructure and Network Security Monitoring Tools
- Exploring Data Type Categories
- Understanding Basic Cryptography Concepts
- Understanding Common TCP/IP Attacks
- Understanding Endpoint Security Technologies
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Resources for Hunting Cyber Threats
- Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity

For more enquiry:
aliyuthayo@sec-conceptsnetworks.com
+234 803 913 4906

- Identifying Patterns of Suspicious Behavior
- Conducting Security Incident Investigations
- Using a Playbook Model to Organize Security Monitoring
- Understanding SOC Metrics
- Understanding SOC Workflow and Automation
- Describing Incident Response
- Understanding the Use of VERIS
- Understanding Windows Operating System Basics
- Understanding Linux Operating System Basics

Lab outline

- Use NSM Tools to Analyze Data Categories
- Explore Cryptographic Technologies
- Explore TCP/IP Attacks
- Explore Endpoint Security
- Investigate Hacker Methodology
- Hunt Malicious Traffic
- Correlate Event Logs, Packet Captures (PCAPs), and Alerts of an Attack
- Investigate Browser-Based Attacks
- Analyze Suspicious Domain Name System (DNS) Activity
- Explore Security Data for Analysis
- Investigate Suspicious Activity Using Security Onion
- Investigate Advanced Persistent Threats
- Explore SOC Playbooks
- Explore the Windows Operating System
- Explore the Linux Operating System