MORINGA
Discover · Grow · Transform

CompTIA Cybersecurity Analyst (CYSA+) Bootcamp

Part-Time Online classes

In partnership with:

CompTIA CySA+ CompTIA Authorized Partner DELIVERY PARTNER

Introduction

Africa's top Tech Bootcamp, Moringa School partners with CompTIA to offer this 20-week Cybersecurity Analyst Course for any person looking to get a CYSA+ qualification.

In this course, you will learn from CompTIA-certified and industry expert trainers to gain in-demand skills that prepare you for well-paying jobs like cybersecurity analyst, security operations center (SOC) analyst, and many more. By the end of the 20 weeks, learners will earn a certificate of completion from Moringa and a **CYSA+ certification from CompTIA.**

Why Learn Cybersecurity At Moringa?

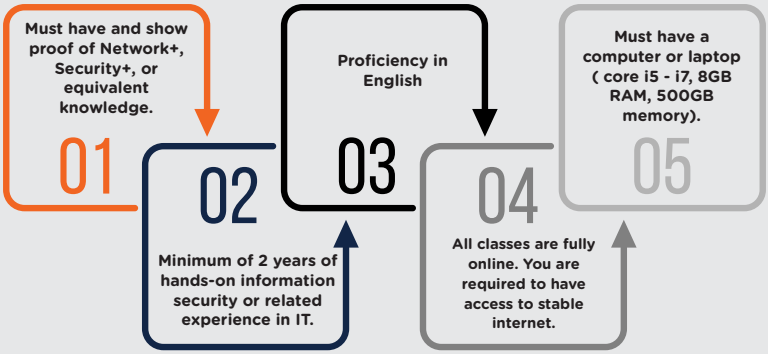
This is a certification for cyber professionals tasked with incident detection, prevention, and response through continuous security monitoring.
Moringa School guarantees you the following:

1. **Practical & project-based learning**
2. **Access to industry-relevant cybersecurity labs & projects on Let's Defend Labs**
3. **Dedicated Technical mentor support**
4. **Highly Discounted Exam vouchers to sit for the certification exam in comparison to the market price**
5. **Dual certification - A certificate of completion from Moringa & CYSA+ from CompTIA**
6. **Comprehensive training & preparation for the CompTIA CYSA+ Certification exams**

Who is this course for?

This course is tailored for aspiring cybersecurity analysts, security engineers, and IT professionals seeking to advance their careers in cybersecurity or enhance existing skills, this CYSA+ course will empower you to excel in the fast-paced world of cybersecurity.

What are the requirements to join?



Cybersecurity Bootcamp Course Overview

Curriculum Developed by - CompTIA

Course Duration - 20 weeks

Mode of learning - Part-Time Classes

Training Delivery - Online Classes every Mon - Fri from 6.00 pm - 9.00 pm (live lectures, self-learning, and Technical Mentor Support available)

Tuition Fees - Ksh 200,000

Exam Fees - USD 181

N.B - The tuition & exam fees can be paid in full before the start of class or in installments. Download the fee payment plan for more details.

Fee Payment Options Available

Curriculum Outline

Week 1: Orientation & Introduction

- Course Overview
- System configurations and installations

Week 2: Vulnerability Response, Handling & Management

- Cybersecurity Leadership Concepts
- Assisted Lab: Exploring The Lab Environment
- Control Types and Methods
- Assisted Lab: Configuring Controls
- Patch Management Concepts

Week 3: Threat Intelligence and Threat Hunting Concepts

- Threat Actor Concepts
- Active Threats
- Assisted Lab: Reviewing IoC and Threat Intelligence Sources
- Threat-Hunting Concepts
- PBQ: Performing Threat Intelligence
- Assisted Lab: Performing Threat-hunting

Week 4: System and Network Architecture Concepts

- System and Network Architecture Concepts
- PBQ: Analyzing Network Infrastructures
- Applied Lab: Performing System Hardening
- Identity and Access Management (IAM)
- Assisted Lab: Configuring Centralized Logging
- Operational Visibility
- Assisted Lab: Assess Time Sync Errors

Curriculum Outline

Week 5: Process Improvement In Security Operations

- Leadership In Security Operations
- Assisted Lab: Configuring Automation
- Technology for Security Operations
- PBQ: Responding to A Security Incident

Week 6: Vulnerability Scanning Methods

- Compliance Requirements
- Vulnerability Scanning Methods
- PBQ: Implementing Vulnerability Scanning Methods
- PBQ: Analyzing Vulnerability Scans
- Assisted Lab: Performing Asset Discovery
- Assisted Lab: Performing Passive Scanning
- Assisted Lab: Performing Vulnerability Scanning

Week 7: Performing Vulnerability Analysis

- Vulnerability Scoring Concepts
- PBQ: Analyzing Data to Prioritize Vulnerabilities
- Vulnerability Context Considerations
- Assisted Lab: Establishing Context Awareness

Week 8: Communicating Vulnerability Information

- Effective Communication Concepts
- Assisted Lab: Analyzing Vulnerability Scans
- Vulnerability Reporting Outcomes and Action Plans
- PBQ: Performing Vulnerability Assessment
- Assisted Lab: Detecting Legacy Systems

Week 9: Health Break

Curriculum Outline

Week 10 - 11: Incident Response Activities & Communication tions

- Incident Response Planning
- Adaptive Lab: Performing Playbook Incident Response
- Applied Lab: Performing IoC Detection and Analysis
- Applied Lab: Performing Post-Incident Forensic Analysis
- Applied Lab: Collecting Forensic Evidence
- Incident Response Communication
- PBQ: Performing Incident Response Reporting
- Assisted Lab: Performing Root Cause Analysis

Week 12 - 13: SOFT SKILLS

Week 14 -15: Analyzing Potentially Malicious Activity

- Malicious Activity
- Assisted Lab: Using File Analysis Techniques
- Assisted Lab: Analyzing Potentially Malicious Files
- Applied Lab: Using Network Sniffers
- Attack Methodology Frameworks
- Techniques for Identifying Malicious Activity
- PBQ: Identifying Malicious Activity
- Applied Lab: Researching DNS and IP Reputation

Week 16: Application Vulnerability Assessment

- Web Vulnerabilities
- Applied Lab: Performing Web Vulnerability Scanning
- Cloud Vulnerabilities
- PBQ: Analyzing Cloud Vulnerability Assessment Output
- Assisted Lab: Analyzing Cloud Vulnerabilities

Curriculum Outline

Week 17: Exploring Scripting Tools and Analysis Concepts

- Scripting Languages
- PBQ: Identifying Programming Languages
- Malicious Activity Through Analysis
- PBQ: Identifying Malicious Activity Through Analysis

Week 18: Application Security and Attack Mitigation Best Practices

- Secure Software Development Practices
- Assisted Lab: Exploiting Weak Cryptography
- Controls to Mitigate Successful Application Attacks
- PBQ: Applying Security Solutions for Software Assurance
- Assisted Lab: Performing Directory Traversal and Command Injection
- Assisted Lab: Performing and Detecting XSS, LFI/RFI, SQLi, SCRF
- Controls to Prevent Attacks
- Assisted Lab: Performing and Detecting Privilege Escalation
- Applied Lab: Detecting and Exploiting Security Misconfiguration

Week 19 - 20: EXAM PREP & FINAL ASSESSMENT

Contact Details

General Inquiries:
+254 711 082 146

Corporate Inquiries:
+254 738 368 319

Admissions Inquiries:
020 7643 533

WhatsApp Inquiries:
+254 712 293 878

General Inquiries
contact@moringaschool.com

Corporate Inquiries:
corporate@moringaschool.com

Admissions Inquiries:
admissions@moringaschool.com

Ngong Lane, Ngong Lane Plaza, 1st Floor, Nairobi Kenya
Victoria Plaza, 5th Floor, Westlands, Nairobi Kenya

Facebook | LinkedIn | Twitter | YouTube
@moringaschool

www.moringaschool.com

MORINGA
Discover · Grow · Transform