NOVIAONE SCHOOL OF BANKING

CYBERSECURITY ANALYST

DURATION
18 Months
33 Classes (pending additional requirements)
6 Work Experience Coaching Sessions

ENTRY REQUIREMENTS
Matric and working in a cybersecurity environment for at least 2 years with an experienced cybersecurity analyst as a coach/mentor

TOTAL NUMBER OF DAYS OUT OF THE OFFICE
33 Days
9h00 - 16h00

Assignments and workplace evidence required.

INTRODUCTION

This qualification focuses on expanding essential cybersecurity abilities and providing a larger foundation from which the learner can specialise in specific systems or areas of cyber protection. It builds on the existing knowledge and skills the learner may have.

OVERVIEW OF THE HIGH-LEVEL PROGRAMME

Module 1: 4IR & Future Skills
Module 2: Computers, Devices and Systems
Module 3: Logical Thinking & Basic Calculations
Module 4: Data & Database Vulnerabilities
Module 5: Introduction to Cybersecurity
Module 6: Cybersecurity Governance, Legislation & Ethics
Module 7: Network Security and Defence
Module 8: Cybersecurity & Cyber Threats
Module 9: Design Thinking, Innovation & Cybersecurity Toolset Scripting

WORK EVIDENCE

The focus of the work experience is on providing the student with an opportunity to get exposure to cyber security as a practice. Prescribed workplace evidence must be collected and endorsed by the student's mentor/supervisor in the workplace and submitted to NVO for final assessment.

OUTCOMES

1. Analyse, identify, and solve potential and actual security risks, vulnerabilities and inefficiencies to safeguard information system assets from cybersecurity attacks.
2. Protect an organisation's digital assets from both internal and external threats by maintaining cybersecurity attack mitigation and incident response capability.
3. Execute ethical cybersecurity monitoring in line with cybersecurity policies to provide defence to a level of confidentiality, integrity, and availability equal with the threat to assets and their value to the company.
4. Execute response procedures to mitigate cyber-attacks and secure information assets, intellectual property, and computer systems.
5. Execute recovery protocols and procedures as per a recovery plan to restore data and/or assets.

EXTERNAL INTEGRATED SUMMATIVE ASSESSMENT (EISA)

NVO will issue a Statement of Results (SoR) once the programme and all assessments have been completed successfully.
EISA (External Integrated Summative Assessment) exam to be booked directly with MictSETA once NVO programme is completed.
If applicable, the exam fee is payable directly to MictSETA. The Novia One mock examination will be venue based to simulate exam conditions as applied by the EISA exam.
Students will receive a certificate of competence against the qualification directly from QCTO after successfully passing the EISA.