

Occupational Certificate: **CYBERSECURITY ANALYST**

NQF: 5

SAQA ID 118986

CREDIT: 173

Description

This qualification prepares learners to work as cybersecurity analysts, focusing on protecting networks, computer systems, and information resources from malicious attacks. It involves assessing and mitigating risks, identifying vulnerabilities, and addressing security issues to ensure regulatory compliance.

The qualification teaches learners about cybersecurity issues, their impact on communities, society, the ICT sector, and the economy. It also teaches how cybercrime disrupts businesses, responds to incidents, and analyzes results. Learners will also evaluate the design of efficient security solutions and learn about fundamental network security concepts like firewalls, intrusion detection systems, and VPNs.

Career Fields

With this qualification, successful learners could pursue a career as a:

- Cybersecurity Consultant
- Threat Intelligence Analyst
- Network Security Analyst
- Security Engineer
- Incidence Response
- Cybersecurity Analyst
- Management and Administration
- Vulnerability Analyst
- Testing and Hacking

Programme Outline

Knowledge Modules:

- Introduction to Cybersecurity
- Fundamentals of Network Security and Defence
- Cybersecurity and Cyber Threats and Attacks
- Introduction to Cybersecurity Governance, Legislation and Ethics
- Fundamentals of Design Thinking and Innovation
- Logical Thinking and Basic Calculations
- Computers, Devices and Computing Systems
- Data and Database Vulnerabilities
- Introduction to 4IR and Future Skills

Practical Skill Modules

- Ensure Compliance in terms of Legal Cybersecurity Requirements and National and International Standards.
- Assess Risks and Vulnerabilities and Current Security Measures
- Implement Protection, Prevention and Detection Measures to Mitigate Risk, Violations and Vulnerabilities
- Apply Logical Thinking and Maths
- Apply Basic Scriptwriting for Cybersecurity Toolsets.
- Access and Visualise Structured Data Using Spreadsheets
- Apply Design Thinking Methodologies
- Function Ethically and Effectively as a Member of a Multidisciplinary

Work Experience Modules

- Compliance with Legal Cybersecurity Requirements
- Cybersecurity Risk Assessment and Mitigation
- Cybersecurity Detection, Protection and Prevention Processes

Admission requirements

The minimum entry requirement for this qualification is:

- NQF Level 4 qualification

Integrated Assessment

During the roll out of the programme formative and summative assessments will be conducted. Learners are also required to complete a Final Integrated Summative Assessment (FISA).

Upon successful completion of the FISA, learners will be issued with a Statement of Results (SOR) from iFundi.

This SOR is the entry requirement for undertaking the External Integrated Summative Assessment (EISA).

EISA is a single, national assessment undertaken at accredited assessment centres. It is an integral and critical component of QCTO's quality assurance system, as it ensures that the assessment of occupational qualifications, part-qualifications and trades is standardised, consistent and credible. This leads to competent learners being awarded Occupational Certificates. Qualifying for External Assessment: To qualify for an external assessment, learners must provide proof of completion of all required knowledge and practical modules by means of statements of results and a record of completed work experience.

Type of programme

The programme duration is to be determined in accordance with convenience and training format adopted by the client. Programmes can be offered in blended or online framework. The schedule is developed in consultation with the client.

Articulation

This qualification provides opportunities for horizontal and vertical articulation options.

Horizontal articulation:

- Higher Certificate in Computer Forensics, NQF Level 05.

Vertical articulation:

- Advanced Certificate in Information Security, NQF Level 06.

