IMPACTFUL
Powered by LRMG

QCTO
Quality Council for Trades & Occupations

IT SKILLS PROGRAMMES

CYBERSECURITY DEFENDER

QUALIFICATION TYPE:
SKILLS PROGRAMME ID (SP- 220330)

TRAINING DAYS: 68

Designed to support your Workplace Skills Plan and build job-ready IT capability

Build cybersecurity capability and protect organisations

Cyber threats are constant, and the impact on operations, data, and reputation can be severe. Organisations need people who can detect, respond to, and prevent security risks in real time.

This Cybersecurity Defender skills programme builds practical capability to protect systems, identify threats, and respond to incidents. Learners develop hands-on skills in security tools, risk mitigation, and system protection to strengthen your organisation's cyber resilience.

On successful completion of this skills programme and successful FISA (Final Integrated Summative Assessment), learners will be awarded: **QCTO Certificate: Cybersecurity Defender**
(An accredited, credit-bearing Skills Programme certificate)

We work closely with you to understand your objectives, guide you through the requirements, and support the implementation of skills programmes that deliver real impact.

NQF LEVEL 4

CREDITS 60

WHO SHOULD ENROL?

- Organisations strengthening cybersecurity capability and risk readiness
- Teams responsible for systems, networks, and data protection
- Individuals starting a career in IT or cybersecurity
- Aspiring professionals building security and threat detection skills

WHAT MAKES THIS COURSE DIFFERENT?

This skills programme is designed to move you from learning to doing

- Build strong foundations in cybersecurity, risk, and governance
- Apply skills in practical environments that simulate real-world threats
- Gain hands-on experience detecting, preventing, and responding to cyber incidents

WHAT IS THE ENTRY CRITERIA?

- NQF Level 4

CYBERSECURITY DEFENDER

SKILLS PROGRAMME

The purpose of this skills programme is to prepare learners to operate as Cybersecurity Analysts who protect networks, computer systems, and information assets from malicious attacks and threats through:

- Provide a solid foundation in cybersecurity principles and governance
- Identify, prevent, and respond to cyber threats and attacks
- Develop practical skills in security tools, encryption, and mobile protection
- Equip learners to protect, detect, and test systems through hands-on application
- Prepare learners for cybersecurity roles and advanced certifications
- Risk Assessment & Mitigation
- Security Design & Maintenance
- Community & Economic Impact

The skills your team will build

These exit level outcomes show the skills you'll have built:

- Understand core cybersecurity principles and governance
- Identify and mitigate cyber threats and attacks
- Gain practical skills in security tools, encryption, mobile protection
- Learn to respond to incidents and adopt smart security habits.
- Apply hands-on techniques to protect, detect, and test systems
- Improve personal and organisational cyber resilience
- Boost career opportunities in a high-demand field
- Build a foundation for advanced cybersecurity certifications

Assessment designed to show what you can do

Learners are assessed throughout the programme using a variety of methods, which may include practical tasks, written assignments, short projects, demonstrations, and presentations. Evidence of learning is collected and recorded for monitoring, feedback, and quality assurance. Where the curriculum is delivered in modules, internal summative assessments are conducted at the end of each module and results are recorded. After completing all modules, learners must complete a Final Integrated Supervised Assessment (FISA) that integrates the key outcomes of the skills programme. The FISA is implemented through one assessment process, which may be conducted using either of the following supervised methods:

Face-to-face Assessment

The FISA is conducted in person under direct supervision, using approved assessment instruments and a rubric and/or checklist to confirm that all required competencies have been demonstrated

Virtual delivery via e-assessment

The FISA may be conducted virtually via our secure e-assessment platform (Questionmark). This assessment is conducted under supervised conditions and is further strengthened through the use of proctoring, which provides real-time monitoring and verification of learner identity and assessment conditions. Proctoring enhances the integrity, credibility, and reliability of the FISA by reducing the risk of malpractice, ensuring compliance with assessment rules, and confirming that the assessment is conducted fairly, consistently, and in line with approved assessment requirements

The FISA is supervised, with a pass mark set at 75%

CYBERSECURITY DEFENDER

QUALIFICATION TYPE:

This detailed overview outlines how the skills programme is structured to develop capability progressively, from foundational knowledge, through applied practical skills, to integrated workplace experience. Each module is aligned to the credit requirements of the nationally recognised skills programme

KNOWLEDGE COMPONENTS

Module 1: Cyber Defence Introduction

- Introduction to cybersecurity
- Cybersecurity basics
- Cybersecurity governance fundamentals
- A cyber secure organisation
- Basics of threat intelligence

Module 2: Cyber Threats and Attacks

- Social engineering
- Physical vulnerability and security
- Malware and ransomware

Module 3: Cybersecurity

- End-user access point security
- Types of cybersecurity software/tools
- Encryption
- Personal security
- Mobile Security
- Password protection

Module 4: Responding to Cybersecurity Incidents

- Protect files and devices
- Protect the wireless network
- Practice smart cyber security habits
- Act Now! after a cyberattack or data breach

APPLICATION COMPONENTS

Module 1: Cyber Defence Introduction

- Introduction to cybersecurity
- Cybersecurity basics
- Cybersecurity governance fundamentals
- A cyber secure organisation
- Basics of threat intelligence

Module 2: Cyber Defence Introduction

- Introduction to cybersecurity
- Cybersecurity basics
- Cybersecurity governance fundamentals
- A cyber secure organisation
- Basics of threat intelligence

Module 3: Cyber Defence Introduction

- Introduction to cybersecurity
- Cybersecurity basics
- Cybersecurity governance fundamentals
- A cyber secure organisation

Basics of threat intelligence