MILPARK EDUCATION

immersive online

Advanced Occupational Certificate:

CYBERSECURITY PRACTITIONER

NQF Level 6 | SAQA ID 122068

QCTO Quality Council for Trades & Occupations

BANK SETA

Learnership Registration No. 32Q320181231735

PROTECTING DIGITAL ASSETS. BUILDING CYBER RESILIENCE.

This qualification equips **cybersecurity professionals** with the knowledge, practical skills, and **workplace experience** required to identify threats, investigate incidents, manage risks, and safeguard critical information systems in an increasingly connected world. Offered by **Milpark Education**, a **trusted higher education institution since 1997**, this qualification combines **industry-relevant knowledge, practical skills, and workplace experience** to help learners **realise their potential and achieve their career goals.**

CONTENT

01. Description and Programme Purpose

Qualification Overview

The **Advanced Occupational Certificate: Cybersecurity Practitioner** (SAQA ID 122068) is an occupational qualification designed to prepare your employees to become skilled cybersecurity **professionals capable of protecting organisations'** digital systems, networks, applications, and information assets from cyber threats.

The programme integrates theoretical knowledge, practical skills training, and workplace-based learning to develop competencies in **cybersecurity intelligence gathering**, threat analysis, cybercrime investigation, **digital forensics**, risk assessment, and the **implementation of security controls.**

Become More

THREATS. RISKS. SOLUTIONS.

Equipping practitioners with the **capabilities to identify** vulnerabilities and **implement effective** security strategies.

The purpose of the **qualification is to equip employees** in the organisation with the **ability to identify** vulnerabilities, investigate cybersecurity incidents, analyse and evaluate cyber threats, and develop and **manage effective risk mitigation** strategies that protect organisational information and technology infrastructure.

Employees who complete the qualification will be able to **support cybersecurity** governance, compliance, and incident **response processes** while applying ethical, legal, and professional practices to enhance organisational resilience and safeguard critical information assets in an in **creasingly complex digital environment.**

02. Who Should Enrol

This programme is **designed for employees** in the organisation who are passionate about technology and want to build a career in **protecting organisations** from cyber threats. It is well suited to **Cybersecurity Analysts**, IT support professionals, network and systems administrators, and other **ICT practitioners** who are looking to deepen their cybersecurity expertise and move into **more specialised roles.**

Whether your **employees are looking to enhance** their current skills, **expand their career opportunities**, or take on greater responsibility in safeguarding digital environments, this **programme provides the practical** and workplace-based experience needed to succeed in the **fast-growing** field of cybersecurity.

03. Programme Outcomes

Graduate Competencies

Successful **completion of this qualification** should enable your employees to:

- Conduct advanced **cyber intelligence** operations, including denial and deception techniques, to gather and **analyse cybersecurity** intelligence.
- **Evaluate and interpret** cybersecurity information to **identify its relevance**, significance, and intelligence value.

- **Investigate cyber incidents** and digital crimes, using appropriate forensic methods to examine ICT systems, networks, and digital evidence.
- Implement cybersecurity **risk management strategies** by identifying threats and applying preventative and mitigation measures.
- **Demonstrate ethical, legal, and professional practice** in cybersecurity operations, investigations, and decision-making.

04. Programme structure

Qualification Framework

The **Advanced Occupational Certificate: Cybersecurity Practitioner** (SAQA ID 122068) is a **120-credit, NQF Level 6 qualification** that combines theoretical knowledge, practical skills training, and workplace experience. The **programme covers cybersecurity** information analysis, **cybersecurity investigations**, data collection, threat analysis, and cybercrime investigations, while providing your **employees with hands-on exposure** to real-world cybersecurity processes.

This integrated approach ensures employees in the **organisation are equipped** to identify threats, investigate cyber incidents, manage cybersecurity risks, and **protect organisational information systems effectively.**

Major: Advanced Occupational Certificate: Cybersecurity Practitioner 120 credits

	Knowledge Modules	Practical Skills Modules	Work Experience Modules
Compulsory (all)	1. Theories and application principles of analysing cybersecurity information (20/6)	3. Execute Data Collection Operations (8/6)	6. Cyber Security Data Collection Management Processes (12/6)
	2. Concepts and Principles of Cybersecurity Investigations (20/6)	4. Conduct Threat Analysis (12/6)	7. Threat Warning and analysis Processes (18/6)
		5. Conduct Cyber Investigations (12/6)	8. Cyber Crime Investigation Processes (18/6)
Total credits	**40**	**32**	**48**

SECURE. MONITOR. RESPOND.

Building the **practical skills needed** to protect systems, investigate incidents, and manage cyber risks.

05. Module Descriptions

5.1 Knowledge Modules:

Theories and application principles of analysing cybersecurity information

This module introduces your **employees to the theories**, frameworks, and techniques used to collect, interpret, analyse, and evaluate **cybersecurity information** and intelligence to **support informed security** decision-making.

Concepts and Principles of Cybersecurity Investigations

This module focuses on the principles, methodologies, **legal considerations**, and **best practices involved** in investigating cybersecurity incidents, cybercrime, and digital security breaches.

5.2 Practical Modules:

Execute Data Collection Operations

Employees develop practical skills in gathering, recording, and preserving cybersecurity data from **various digital sources** while maintaining the **integrity and reliability** of the information collected.

Conduct Threat Analysis

This **module equips your employees** with the practical ability to identify, assess, and analyse cybersecurity threats, vulnerabilities, and **risks to support proactive security measures** and incident response.

Conduct Cyber Investigations

Employees **gain hands-on experience** in investigating cybersecurity incidents and cybercrimes, including evidence collection, analysis, and reporting in accordance with **legal and professional standards.**

5.3 Work Experience Modules:

Cyber Security Data Collection Management Processes

This **workplace module exposes** your employees to real-world processes for managing and coordinating **cybersecurity data collection** activities within an organisational environment.

Threat Warning and analysis Processes

Employees apply threat monitoring, intelligence analysis, and early warning processes in the workplace to identify and **assess emerging cyber** risks and support effective security responses.

Cyber Crime Investigation Processes

This **module provides workplace experience** in supporting and participating in cybercrime investigations, including evidence management, incident documentation, and **investigative procedures used in professional cybersecurity** environments.

06. Minimum Admission Requirements

The admission criteria for the **Advanced Occupational Certificate: Cybersecurity Practitioner** are as follows:

Applicants should have:

Cybersecurity Analyst (NQF Level 5) or an equivalent qualification

CYBER INTELLIGENCE. DIGITAL TRUST. BUSINESS CONTINUITY.

Developing **skilled practitioners** who help organisations **protect their technology infrastructure** and critical information assets.

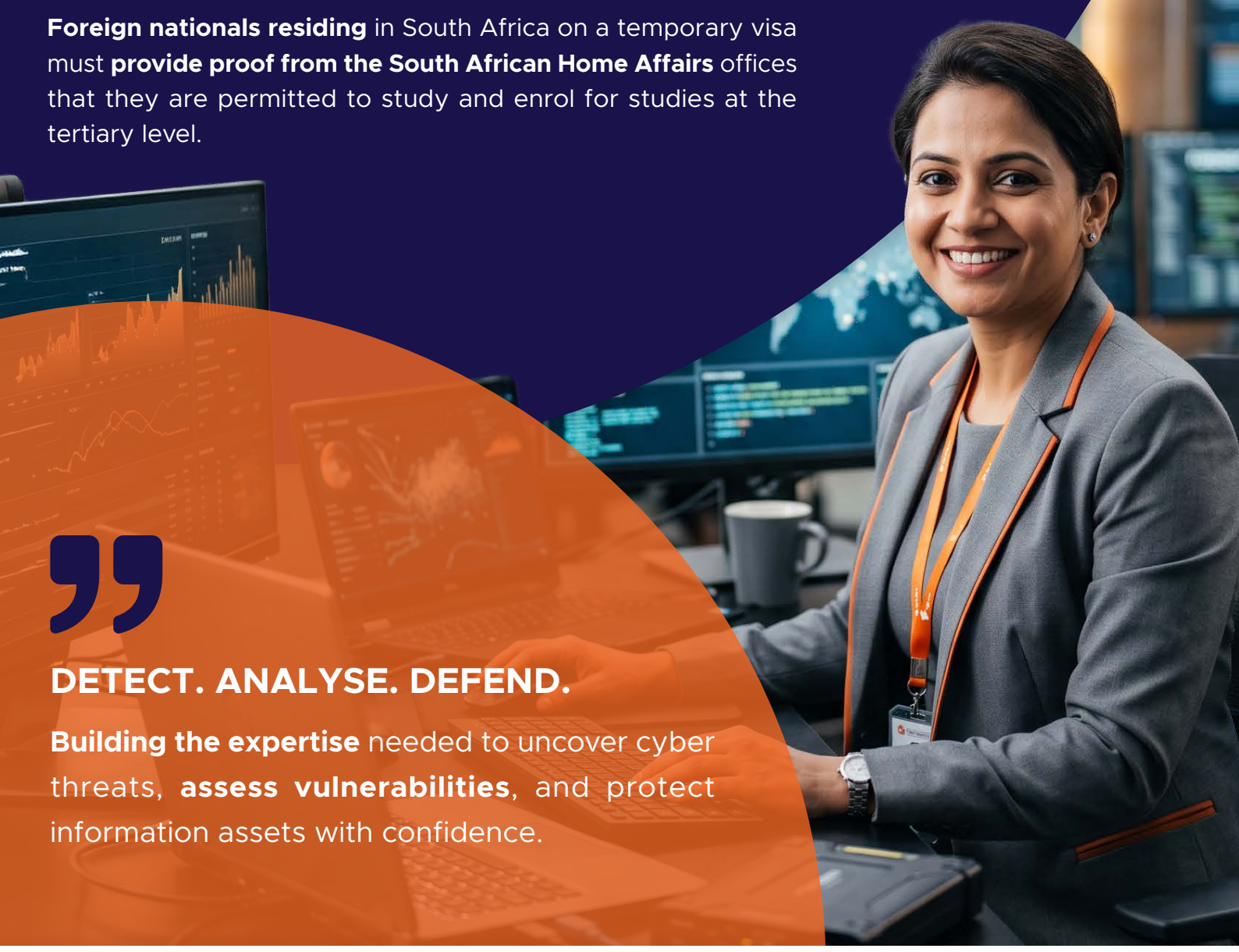
Other / International certificates:

Further to the **requirements for admission** provided above, foreign nationals or South African nationals seeking to apply for admission onto the qualification, based on a **non-South African/ foreign** senior school leaving certificate, must obtain and submit to Milpark a Certificate of Exemption from Universities South Africa (USAf) ***(www.usaf.ac.za)***.

Applicants with foreign senior school leaving certificates who have already completed the equivalent of a South African Grade 12, are advised to **submit their USAf Certificate** of Exemption at the time of applying online for the Milpark bachelor's degree.

Any foreign national or South African national seeking admission based on a **non-South African/foreign tertiary qualification** must obtain and submit to Milpark a Certificate of Exemption from Universities South Africa (USAf) ***(www.usaf.ac.za)*** at the time of applying for admission onto the qualification. ***www.saqa.org.za***

Foreign nationals residing in South Africa on a temporary visa must **provide proof from the South African Home Affairs** offices that they are permitted to study and enrol for studies at the tertiary level.



DETECT. ANALYSE. DEFEND.

Building the expertise needed to uncover cyber threats, **assess vulnerabilities**, and protect information assets with confidence.

Recognition of Prior Learning (RPL) applications:

Milpark admits a small number of candidates onto its programme via **Recognition of Prior Learning** (RPL). **Applicants interested** in applying via RPL will be considered individually by the relevant Head of School.

Applicants will be required to provide evidence as outlined below when **applying for admission via the RPL route:**

- **Curriculum vitae** – applicant must have 10 years of relevant work experience.
- Applicant must have a **matric qualification**, even if they performed poorly on it.
- **Personal motivational letter**, advising how the qualification will assist them and how the qualification links with their line of work.
- Evidence from **performance in the workplace** (e.g. direct line manager motivational letter, evidence from workplace appraisal)
- **Evidence from prior** achievement
- Certified academic **transcript/statement** of result.

Learn More About The RPL Requirements

07. Delivery & Technology Access

Mode of Delivery

Distance Learning Online (DLO) is one of the key modes of learning offered by the **Milpark School of Commerce.**

It provides a fully digital, guided, and **flexible study experience** that supports independent learning while **maintaining structured engagement**. Through Milpark's online platform, **your employees can access all their learning** materials, including prescribed textbooks, and participate in live **classes and interactive discussion forums.**

DLO is designed to foster meaningful interaction while allowing employees of your business to learn at their own pace. With **comprehensive resources** and flexible access, it accommodates varying levels of connectivity and provides an inclusive **learning journey that caters** to diverse employee contexts.

Access to Technology

Through the *myMilpark* **and** *myCourses* **online tuition** and support environments, students have **access to all course materials** (including formative and summative assessments), discussion opportunities, administrative **services and a wealth of external resources.**

Minimum requirements to study online and complete assessments and online proctored assessments

A **laptop or personal computer** (PC) with one of the **following operating systems**:

- Windows 10+
- macOS 10.11+
- Ubuntu 18.04+
- Chrome 58+

- Continuous (daily) access to a **stable internet connection** with an upload and download speed of at least 5 Mbps.
- A **camera/webcam** (720p resolution)
- Speakers and a microphone **OR** headphones
- 2GB free **RAM** (memory)
- 250MB **free disk space.**

View Technical Requirements **How To Check Your RAM**

08. Employee Support

Library access

The **Milpark Library provides access to e-books** in a virtual library called Cyberlibris (Scholartext). Lecturers may create **smart bookshelves per course or module** for your employees to access (these shelves can contain prescribed and recommended books).

Employees can also create their own personal smart bookshelves containing resources for their studies. Having access to a digital library means that **thousands of employees can access books and resources** from anywhere, at the same time, online.

There is **no need to make reservations and requests**, and **no limit to the time an employee has to access a book**. With the implementation of Cyberlibris, employees also have access to full-text resources via ProQuest (global), Emerald (global), Ebsco (global) and Sabinet (South African publications), to assist with research and to enrich their learning experience.

Access to the Library is included in the module fee.

THINK. DETECT. PROTECT.

Developing cybersecurity professionals who can identify threats and **defend critical digital environments.**

Online Lecturer

Comprehensive employee support services are available. Employees are provided with administrative support by **Student Services**. To assist with understanding content, your employees have **access to online lecturers** whom they can contact individually. Employees who experience study and/or personal problems have access to a counsellor. **All support services are available to registered employees via myMilpark (myCourses).**

09. Rules of Progression

Compulsory modules have to be **completed by all employees.**

10. Assessment

The **Advanced Occupational Certificate: Cybersecurity Practitioner** uses a combination of **formative and summative assessments** to evaluate employees' knowledge and practical skills. Throughout the programme, your **employees complete assignments**, tests, practical cybersecurity tasks, workplace activities, and a **portfolio of evidence to demonstrate competence** in areas such as threat analysis, cyber investigations, digital forensics, and risk management.

After **successfully completing** the required knowledge, practical, and work experience modules, your employees must undertake the **External Integrated Summative Assessment** (EISA), conducted through the QCTO, which assesses their ability to apply cybersecurity concepts and skills in real-world scenarios before they can be awarded the qualification

Employees are advised to consult the module orientation and assessment guidelines provided for each module to ensure they understand how their **final mark will be calculated.**

11. Duration

Distance online learning employees have a **minimum of 1 year** and a **maximum of 3 years** to complete the qualification.

12. Certification

Upon **successful completion** of the programme and the required External Integrated Summative Assessment (EISA), your employees will be awarded the **Advanced Occupational Certificate: Cybersecurity Practitioner** (SAQA ID 122068, NQF Level 6, 120 Credits), which is registered on the **Occupational Qualifications Sub-Framework** (OQSF) and **quality assured** through the Quality Council for Trades and Occupations (QCTO).

13. Further Studies

Milpark Education is committed to the process of lifelong learning and to opening up access to higher education. The **Advanced Occupational Certificate: Cybersecurity Practitioner** (NQF Level 6) provides a strong foundation for further studies at Milpark Education.

SECURE SYSTEMS. PROTECT DATA.

Building the **expertise needed to safeguard information** and strengthen organisational resilience.

Employees who completed the qualification can progress to qualifications to further their studies in information technology, cybersecurity, digital forensics, and information security-related fields, including the **Bachelor of Business Administration** (BBA), and **Bachelor of Commerce** (BCom) degrees, subject to meeting the relevant admission requirements.

By continuing their studies, **employees who completed** this qualification can **further strengthen their technical expertise**, expand their career opportunities, and progress into senior cybersecurity, risk management, and information **security leadership roles.**

14. Pricing & Disclaimer

Pricing

All module fees include one round of formative and summative assessments (supplementary examinations excluded). Module **fees do not include the cost of prescribed textbooks**, which will be for the employer's or employee's own account. **The prescribed book list will be available** on myMilpark, on registration.

Disclaimer

The content of this **brochure is accurate at the time** of going to print. Milpark Education reserves the right to change the programme content due to changes in legislation, as well as for market requirements and other reasons. **Notice of such changes will be published on our website.**

MILPARK EDUCATION

GET IN TOUCH

Build Cybersecurity Capability with a Trusted Learning Partner

Investing in cybersecurity talent should be simple. That's why we partner with organisations to deliver a streamlined, **end-to-end learning solution that develops the knowledge**, practical skills, and workplace experience required to **strengthen cybersecurity capability** and protect digital environments.

The Cybersecurity Practitioner programme combines **industry-aligned learning** with dedicated support, helping organisations develop professionals who can identify cyber threats, analyse risks, investigate incidents, and contribute to the security and resilience of critical information systems.

From onboarding and learner support to programme coordination and reporting, we work as an extension of your team to ensure a seamless and effective learning experience.

Speak to us about how we can tailor the programme to your organisation's needs and support your long-term talent development and cybersecurity objectives.

Enquire Now

Engage With Us

www.milpark.ac.za

Deneb House
3rd Floor | 368 Main Road
Observatory | Cape Town
7925 | PO Box 44235
Claremont | 7735