# Executive Summary

| Qualification | Occupational Certificate: Cybersecurity Analyst |
|---|---|
| Purpose | The purpose of this qualification is to prepare a learner to operate as a Cybersecurity Analyst. Cybersecurity Analysts protect assets such as networks, computer systems and information assets from malicious attacks and threats. They assess and mitigate risks and potential intrusions and identify risks and vulnerabilities. On completion of this qualification, the learner will be able to investigate cybersecurity issues and challenges, analyse how cybercrime can affect businesses, respond effectively to cybersecurity threats, and evaluate the design of security solutions. |
| Qualification ID | 118986 |
| NQF Level | 5 |
| Minimum Credits | 173 |
| Duration | One year |
| Field | Physical, Mathematical, Computer, and Life Sciences |
| Subfield | Information Technology and Computer Sciences |
| Quality Partner | MICT SETA |
| Entry Requirements | NQF Level 4 qualification |

**Head Office**
3rd Floor, South Wing
20 Skeen Boulevard
Bedfordview

**Centre of Leadership Excellence**
3rd Floor, North Wing
20 Skeen Boulevard
Bedfordview

**Telephone**
+27 11 856 4700

**Website**
www.klmempowered.com

**Contacts**
Lyn Mansour: +27 82 330 5160
Portia Matuludi: +27 67 421 0051
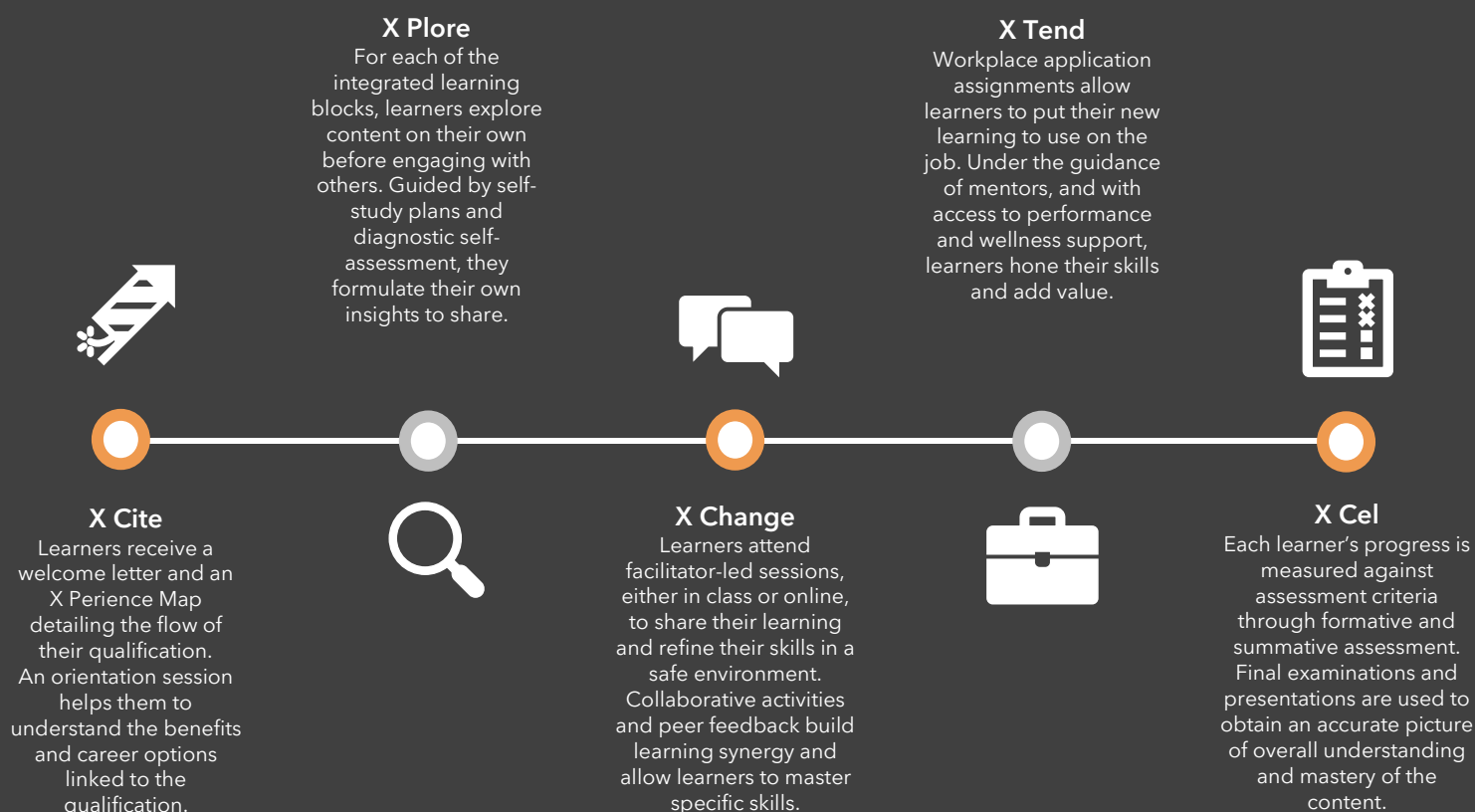Clayton Lendrum: +27 66 478 2706

## Qualification Overview

As Information and Communication Technology (ICT) adoption rates increase so does cybercrime and, in direct relation, the need for ICT security and integrity systems is recognised as being of paramount importance. This qualification will assist in fulfilling the obvious and serious need for cyber security experts, will have a direct, positive impact on the ICT sector and will consequently benefit the economy as well.

Qualifying learners will be able to:

- Analyse, identify, and solve potential and actual security risks, vulnerabilities and inefficiencies to safeguard information systems from malicious cybersecurity attacks.
- Protect organisation's digital assets from both internal and external threats by maintaining cybersecurity attack mitigation and incident response capability.
- 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.
- Execute response procedures to mitigate cyber-attacks and secure information assets, intellectual property, and computer systems.
- Execute recovery protocols and procedures to restore data and/or assets affected by cybersecurity incidents.

## The KLM Empowered Learning X Perience

**X Plore**
For each of the integrated learning blocks, learners explore content on their own before engaging with others. Guided by self-study plans and diagnostic self-assessment, they formulate their own insights to share.

**X Tend**
Workplace application assignments allow learners to put their new learning to use on the job. Under the guidance of mentors, and with access to performance and wellness support, learners hone their skills and add value.

**X Cite**
Learners receive a welcome letter and an X Perience Map detailing the flow of their qualification. An orientation session helps them to understand the benefits and career options linked to the qualification.

**X Change**
Learners attend facilitator-led sessions, either in class or online, to share their learning and refine their skills in a safe environment. Collaborative activities and peer feedback build learning synergy and allow learners to master specific skills.

**X Cel**
Each learner's progress is measured against assessment criteria through formative and summative assessment. Final examinations and presentations are used to obtain an accurate picture of overall understanding and mastery of the content.

## Qualification Outline

- The Occupational Certificate: Cybersecurity Analyst consists of the following Knowledge, Practical and Work Experience Modules.
- Workplace Experience Modules are completed throughout the learning journey and assessed every quarter.
- Formative and summative assessments are conducted at regular intervals to prepare learners for the External Integrated Summative Assessment (EISA).

## Knowledge Modules

| ID | Title | Level | Credits |
|----|-------|-------|---------|
| KM-01 | Introduction to Cybersecurity | 4 | 8 |
| KM-02 | Fundamentals of Network Security and Defence | 5 | 12 |
| KM-03 | Cybersecurity and Cyber Threats and Attacks | 5 | 12 |
| KM-04 | Introduction to Cybersecurity Governance and Ethics | 4 | 4 |
| KM-05 | Fundamentals of Design Thinking and Innovation | 4 | 1 |
| KM-06 | Logical Thinking and Basic Calculations | 4 | 3 |
| KM-07 | Computers, Devices, and Computing Systems | 4 | 6 |
| KM-08 | Data and Database Vulnerabilities | 4 | 3 |
| KM-09 | Introduction to 4IR and Future Skills | 4 | 4 |

## Practical Modules

| ID | Title | Level | Credits |
|----|-------|-------|---------|
| PM-01 | Ensure Compliance in terms of Legal Cybersecurity Requirements and National and International Standards | 5 | 4 |
| PM-02 | Assess Risks and Vulnerabilities and Current Security Measures | 5 | 20 |
| PM-03 | Implement Protection, Prevention, and Detection Measures to Mitigate Risk, Violations, and Vulnerabilities | 5 | 20 |
| PM-04 | Apply Logical Thinking and Maths | 4 | 6 |
| PM-05 | Apply Basic Scriptwriting for Cybersecurity Toolsets | 4 | 4 |
| PM-06 | Access and Visualise Structured Data Using Spreadsheets | 4 | 5 |
| PM-07 | Apply Design Thinking Methodologies | 4 | 4 |
| PM-08 | Function Ethically and Efficiently as a Member of a Multidisciplinary Team | 4 | 5 |

## Work Experience Modules

The focus of the work experience modules is to provide the learner an opportunity to implement cybersecurity solutions and services under authentic working conditions and to develop confidence by working under the supervision of a workplace mentor. This also provides for the exposure of learners to the complexities of dealing with workplace demands, the pressures of work, and the dynamics of stakeholder management.

| ID | Title | Level | Credits |
|----|-------|-------|---------|
| WM-01 | Compliance with Legal Cybersecurity Requirements | 5 | 12 |
| WM-02 | Cybersecurity Risk Assessment and Mitigation | 5 | 20 |
| WM-03 | Cybersecurity Detection, Protection, and Prevention | 5 | 20 |

*The Greatness Effect*