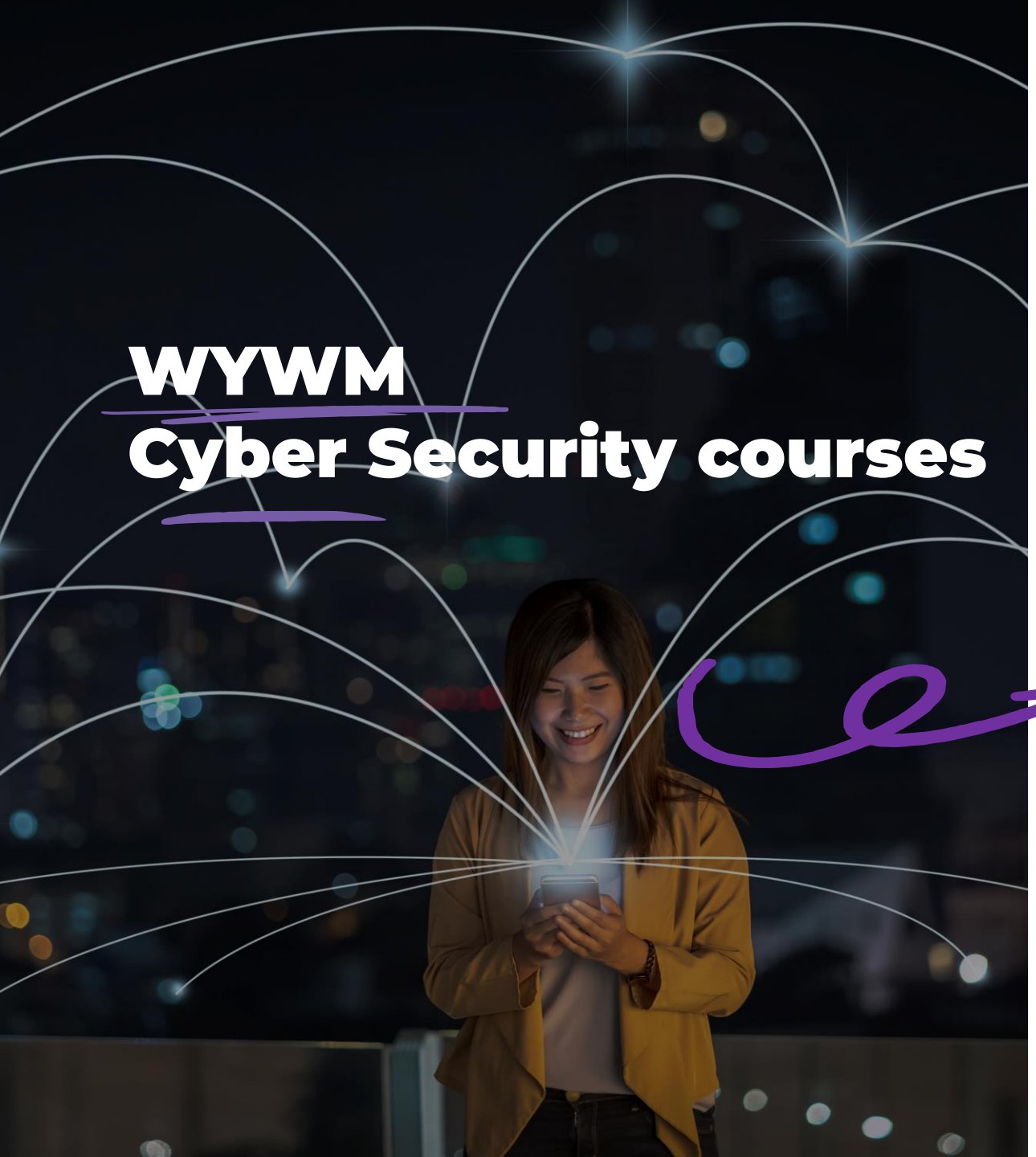
WYWM Cyber Pathway

WYWM Cyber Pathway

What is it about?

The Cyber Pathway teaches in-demand skills for one of the largest and fastest growing industries in the world.

Regardless of whether your background is technical or not, this pathway is designed to help you apply your existing knowledge to developing skills in the cyber security world.



WYWM
Cyber Security courses

- IT Fundamentals
- Networking Fundamentals
- Linux Fundamentals
- OSINT Introduction
- Cyber Security Analyst
- Red Team Essentials
- Red Team Operator – Windows Buffer Overflow
- Cyber Security Awareness
- How To Protect your Data
- What is Social Engineering
- Phishing Attacks
- Linux Privilege Escalation

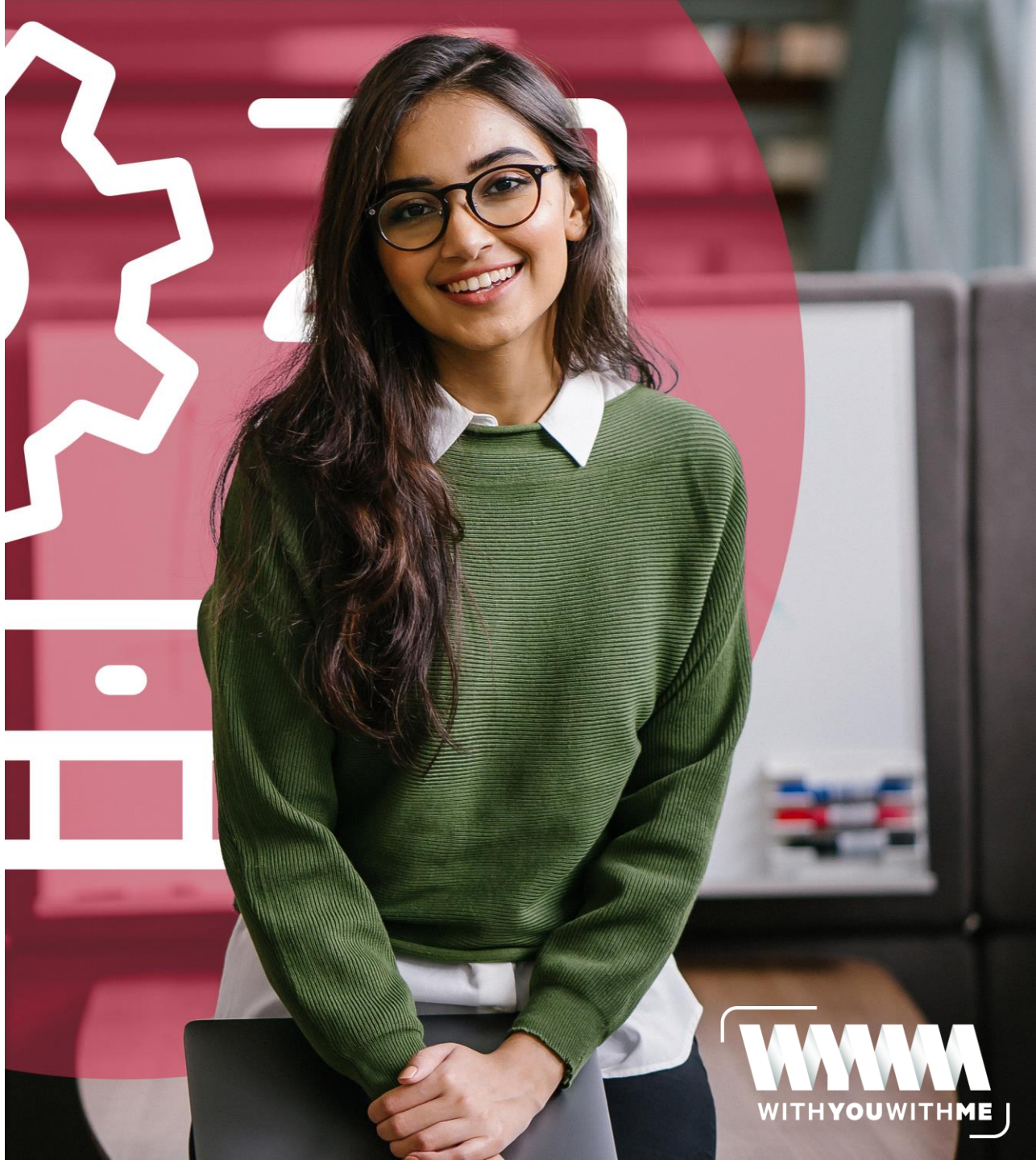
IT Fundamentals

Learning objectives
This is a great course to complete if you are considering a career in technology.

IT Fundamentals offers an overview of:

- Hardware
- Software
- Operating Systems
- IT Horizon Topics

Prerequisites:	Nil
Course Hours:	3.5 hrs
Assessments:	Formative Quizzes
Difficulty:	Beginner

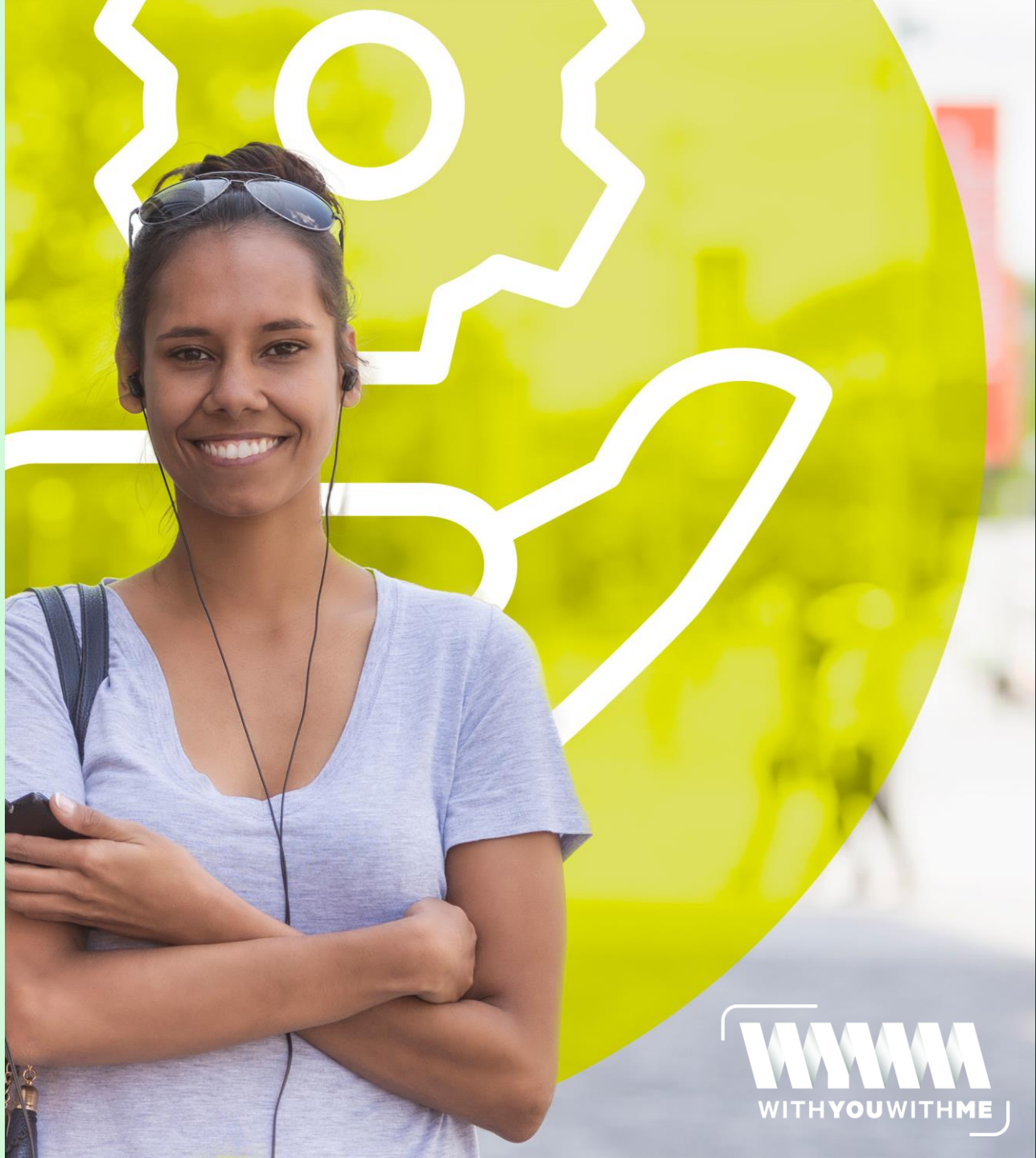


Networking Fundamentals

Learning objectives
This course provides an overview of the introductory topics for basic networking and is designed to teach you how computer networks work, from a small local area network through to the wider internet.

Delve into the purpose of networks and how we benefit from these technologies, understand network address structures of IPv4 and IPv6 and common hardware like switches, routers and cabling. Plus, learn other essential parts that make networks work including the OSI model, common network services, wireless networks and more.

Prerequisites:	Nil
Course Hours:	8-12 hrs
Assessments:	Formative Quizzes & Final Summative Assessment
Difficulty:	Beginner

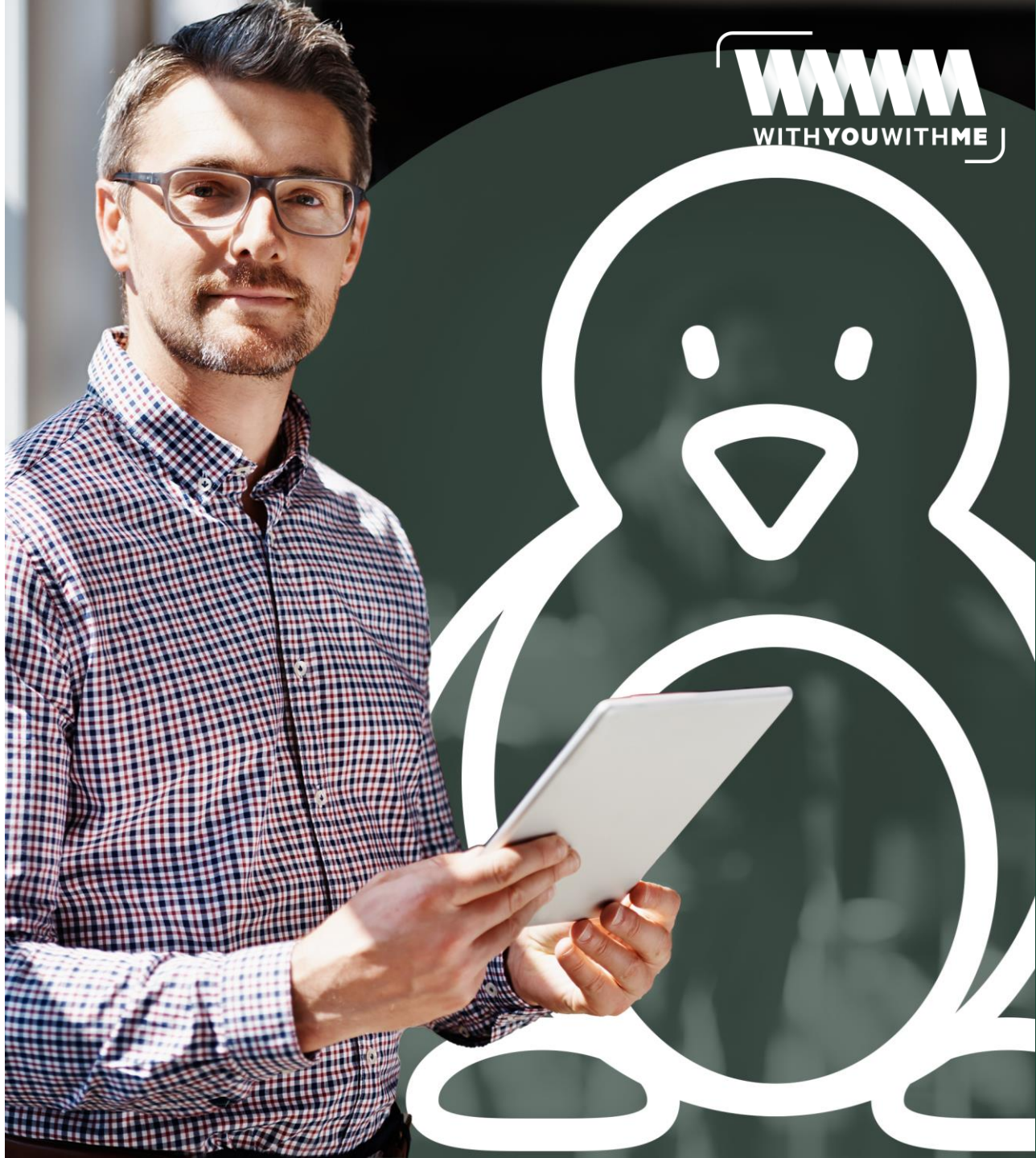


Linux Fundamentals

Learning objectives
The Linux Fundamentals course is catered for those who have no prior knowledge or experience with Linux.

You don't have to be a programmer, or even know how to write code. The concepts and skills you will learn throughout this course will give you an understanding of Linux's power, as well as its simplicity.

Prerequisites:	Nil
Course Hours:	20 hrs
Assessments:	Formative Quizzes
Difficulty:	Beginner



OSINT Introduction

Learning objectives
As an introduction to OSINT (Open Source Intelligence), this course is designed to educate students on the impact publicly available information can have on individuals and organisations.

Objectives:
- Explain what is Open Source Intelligence and how it is obtained
- Understand the positives/negatives paradigms of Open Source Intelligence
- Understand the base concepts of data considerations.

Prerequisites:	Nil
Course Hours:	4-6 hrs
Assessments:	Yes
Difficulty:	Beginner

Cyber Security Analyst

Learning objectives
This course provides an understanding of how to implement technical requirements for the defensive and offensive protection of a computer network.

You can browse, watch and read the content at your own pace however, as this course is accredited by the American National Standards Institute (ANSI) and the United Kingdom's National Cyber Security Centre (NCSC), your progress will be monitored by an instructor and you will need to complete timetabled assessment tasks to receive a completion certificate.

Topics include:

- Introduction to cyber
- The SOC and Tier 1 Analyst
- Operating system security
- Analysing advanced threats
- Incident response
- SIEMs and network traffic

Prerequisites:	Networking Fundamentals IT Fundamentals Linux Fundamentals
Course Hours:	100 hrs
Assessments:	Formative & Summative Quizzes & Practical Assessments
Difficulty:	Intermediate

Red Team Essentials (RTE)

Learning objectives
During this course, you will learn how to:

- Design, plan and execute a penetration test using a provided standard testing methodology
- Research and investigate attack techniques and describe mitigations for them
- Provide a detailed report on your penetration testing activities conducted within a Capstone project which highlights your activities, results, issues encountered and the residual risk

Prerequisites:	Linux Fundamentals Networking Fundamentals
Course Hours:	30 hrs
Assessments:	Formative & Summative Quizzes & Practical Assessments
Difficulty:	Beginner

Red Team Operator
Windows Buffer Overflow

Learning objectives
In this course, you will learn how to use Immunity Debugger, Mona Modules, and msfvenom to create fully developed buffer overflow exploits in Python2 and Python3 for the Windows platform.

We will also cover the common issues encountered and how to resolve them.

Prerequisites:	Red Team Essentials
Course Hours:	10 hrs
Assessments:	Summative Assessment
Difficulty:	Beginner

Cyber Security Awareness

Learning objectives
This course is designed to give you a basic understanding of cyber security.

It will guide you through what information security is, and some of the key points you need to be aware of as you navigate the digital world.

Prerequisites:	Nil
Course Hours:	3 hrs
Assessments:	Formative Quizzes
Difficulty:	Beginner

How to Protect your Data

Learning objectives
In this course, learn what constitutes confidential data, why we need to keep it safe and the best practice approaches to maintaining security in both cyberspace and physical facilities.

Prerequisites:	Nil
Course Hours:	3 hrs
Assessments:	Formative Quizzes
Difficulty:	Beginner

What is Social Engineering?

Learning objectives
In this course, you'll learn what social engineering is, how it works, the different types of social engineering and how to recognise social engineering attacks.

Prerequisites:	Nil
Course Hours:	1.5 hrs
Assessments:	Formative Quizzes
Difficulty:	Beginner

Phishing Attacks

Learning objectives
This course will teach you how to identify phishing attacks, business email compromise attacks, phone scams, vishing attacks and malware. Plus, understand how best to handle these incidents and how to avoid further attacks.

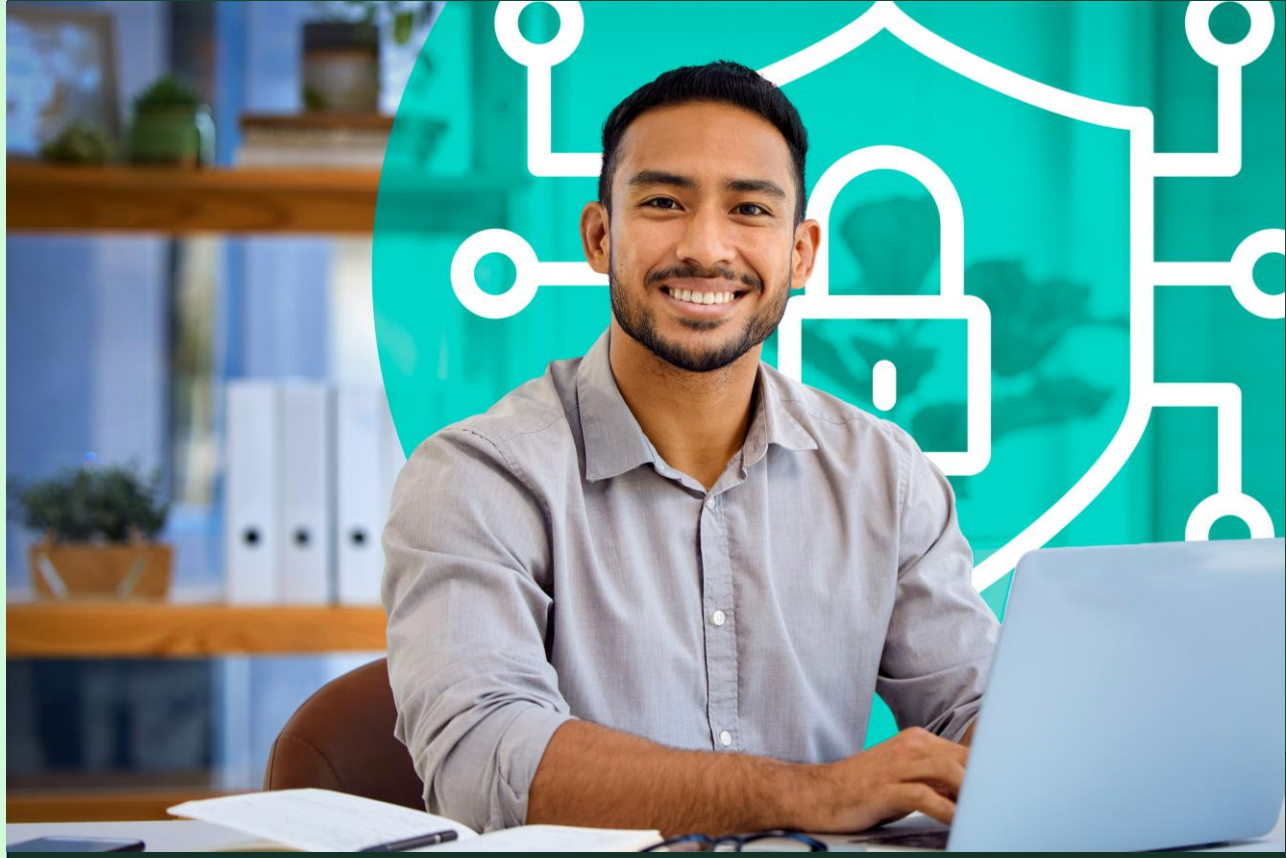
Prerequisites:	Nil
Course Hours:	2.5 hrs
Assessments:	Formative Quizzes
Difficulty:	Beginner

Linux Privilege Escalation

Learning objectives
In this course, you will learn beginner and intermediate privilege escalation and local machine lateral movement techniques. Each lesson includes a bundled lab and practical activities.

You'll discover how to:

- Enumerate, validate and exploit privilege escalation vulnerabilities in GNU/Linux environments
- Identify and exploit insecure scripting for lateral movement and privilege escalation
- Provide a detailed report on your privilege escalation activities within a Capstone project which highlights your activities, results, issues encountered and the residual risk



Prerequisites:	Red Team Essentials
Course Hours:	50-80 hrs
Assessments:	Formative Quizzes & Summative Assessment (Capstone)
Difficulty:	Beginner

Start your training now

We have thousands of hours and multiple digital learning pathways you can access whenever, wherever for free. Whether you want to upskill for a new role, advance your current career with continuous development or simply learn a new skill out of curiosity, our digital skills training is free for the under-represented communities we support.

Sign up now