



**NEXTGEN CAMPUS**  
TOWARDS THE NEXT GENERATION OF IT

# STUDENT HANDBOOK

## Certificate in AI-Driven Cyber Security and Ethical Hacking

*Your guide to the course — general information, how your weeks and months work, how the course ends, and every module in detail*

**6**

MONTHS

**496**

LEARNING HOURS

**42**

MODULES

**Blended**

DELIVERY

### INSIDE THIS HANDBOOK

- |                                                |                                                       |
|------------------------------------------------|-------------------------------------------------------|
| <b>1</b> Welcome and course at a glance        | <b>2</b> What you will learn and how                  |
| <b>3</b> Weekly timetable                      | <b>4</b> Course journey: weeks, months and course end |
| <b>5</b> Assessment, capstone and Project Book | <b>6</b> Student guidelines and support               |
| <b>7</b> Module details — all 42 modules       |                                                       |

NextGen Campus (Pvt) Ltd • TVEC Registered Training Institute P01/1159 • Head Office, Nugegoda

+94 11 251 5215 • +94 77 810 0810 • [info@nextgencampus.lk](mailto:info@nextgencampus.lk) • [www.nextgencampus.lk](http://www.nextgencampus.lk)

Edition: October 2026 • Version 2026\_NGC\_FNL\_V1.9

## PART A General Information

### 1 Welcome to NextGen Campus

Welcome to the Certificate in AI-Driven Cyber Security and Ethical Hacking. This handbook is your guide to the course: how it is organised, how you will learn and be assessed, what is expected of you, and what every module covers. Please read it carefully and keep it with you throughout the course.

NextGen Campus has trained IT professionals since 2013. Our programmes are directly job-targeted: every module combines instructor-led teaching with hands-on labs, real industry tools and practical use of AI, so that you finish ready for work.

### 2 Course at a Glance

|                             |                                                                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Course</b>               | Certificate in AI-Driven Cyber Security and Ethical Hacking                                                                                                                 |
| <b>Duration</b>             | Six months (26 weeks; 24 teaching weeks) · 6 months                                                                                                                         |
| <b>Delivery</b>             | Blended (online and on campus)                                                                                                                                              |
| <b>Class days and times</b> | Tuesday 6.30 – 11.30 PM — online lecture<br>Friday 6.30 – 10.30 PM — campus lab, Room A, once every 4 weeks<br>Sunday 8.30 AM – 12.30 PM — campus lab group session, Room B |
| <b>Total learning hours</b> | 496 hours — 96 h lectures · 340 h practical (labs and capstone) · 60 h Student Project Book                                                                                 |
| <b>Medium</b>               | English                                                                                                                                                                     |
| <b>Intakes</b>              | January–February and June–July each year                                                                                                                                    |
| <b>Course fee</b>           | Rs. 45,000.00                                                                                                                                                               |
| <b>On completion</b>        | NextGen Campus Certificate and Academic Transcript                                                                                                                          |
| <b>Training institute</b>   | NextGen Campus (Pvt) Ltd — TVEC Registered Training Institute P01/1159                                                                                                      |
| <b>Course status</b>        | Proposed for TVEC course registration                                                                                                                                       |

### 3 About the Course

The Certificate in AI-Driven Cyber Security and Ethical Hacking is a six-month, 496-hour non-NVQ course of 42 taught modules and a final enterprise project, progressing learners from IT Security Assistant to Junior Penetration Tester / SOC Analyst level.

**Purpose** To train job-ready junior security analysts, penetration testers and SOC analysts who can assess, defend and monitor enterprise systems responsibly, using AI-assisted tools within legal and ethical boundaries.

**Job-level progression** IT Security Assistant (weeks 1–4) → Junior Penetration Tester (weeks 5–10) → Network Security Technician (weeks 11–13) → Systems Security Administrator (weeks 14–17) → SOC Analyst (weeks 18–21) → AI-enabled Security Analyst (weeks 22–24), completing the Final Enterprise Cyber-Security Project.

**Structure** 42 taught modules in six phases, plus Module 43, the Final Enterprise Cyber-Security Project. All offensive work is performed only in an isolated laboratory against authorised targets.

### 4 What You Will Be Able to Do

By the end of the course you will be able to:

- Apply security, networking, Windows and Linux foundations and defence-in-depth principles.
- Conduct the authorised ethical-hacking lifecycle from OSINT to controlled validation and reporting.
- Defend networks with firewalls, IDS/IPS, VPNs and wireless security.

- Secure identities, endpoints, servers and web applications.
- Monitor, detect, analyse and respond to incidents, including basic digital forensics.
- Apply cloud-security, AI-in-cyber and AI-security principles, and use AI tools responsibly.
- Prepare professional findings, business-impact statements and remediation plans.
- Plan, complete and defend an authorised enterprise security assessment.

## 5 Who the Course Is For and What You Need

**Entry requirements** Learners need G.C.E. O/L with passes in Mathematics and English, plus basic computer literacy. Basic networking knowledge is recommended — for example, the Certificate in Computer Hardware and Networking. A signed ethical conduct agreement is required before laboratory access.

**Who it is for** IT support staff, school leavers, undergraduates, working professionals and career changers aiming for cyber-security roles.

**What you need** a laptop or computer with reliable internet for LMS laboratories (campus lab available by arrangement).

## 6 How You Will Learn

| Learning activity     | Hours        | What it involves                                                                                                           |
|-----------------------|--------------|----------------------------------------------------------------------------------------------------------------------------|
| Lectures              | 96 h         | Live online lectures with your trainer (5 h a week)                                                                        |
| Campus lab practicals | 39 h         | Hands-on sessions in the campus lab (Room A / Room B), on a rotating schedule                                              |
| LMS module labs       | 261 h        | Hands-on labs for every module on the NextGen LMS — about 11 h a week, done in your own time and monitored by your trainer |
| Capstone project      | 40 h         | Final project built on campus over dedicated capstone days                                                                 |
| Student Project Book  | 60 h         | Your professional record of lab work, reflections and the Management Module                                                |
| <b>Total</b>          | <b>496 h</b> |                                                                                                                            |

### About the LMS module labs

Every module has a set of hands-on labs on the NextGen LMS. Complete them each week, between your classes — they are where most of your practical skills are built.

Your trainer monitors lab completion on the LMS and uses it to give you feedback before each module assessment. Completing all LMS labs is required for the award.

Use a laptop or computer with reliable internet. If you do not have one, ask about using the campus lab.

## 7 Your Weekly Timetable

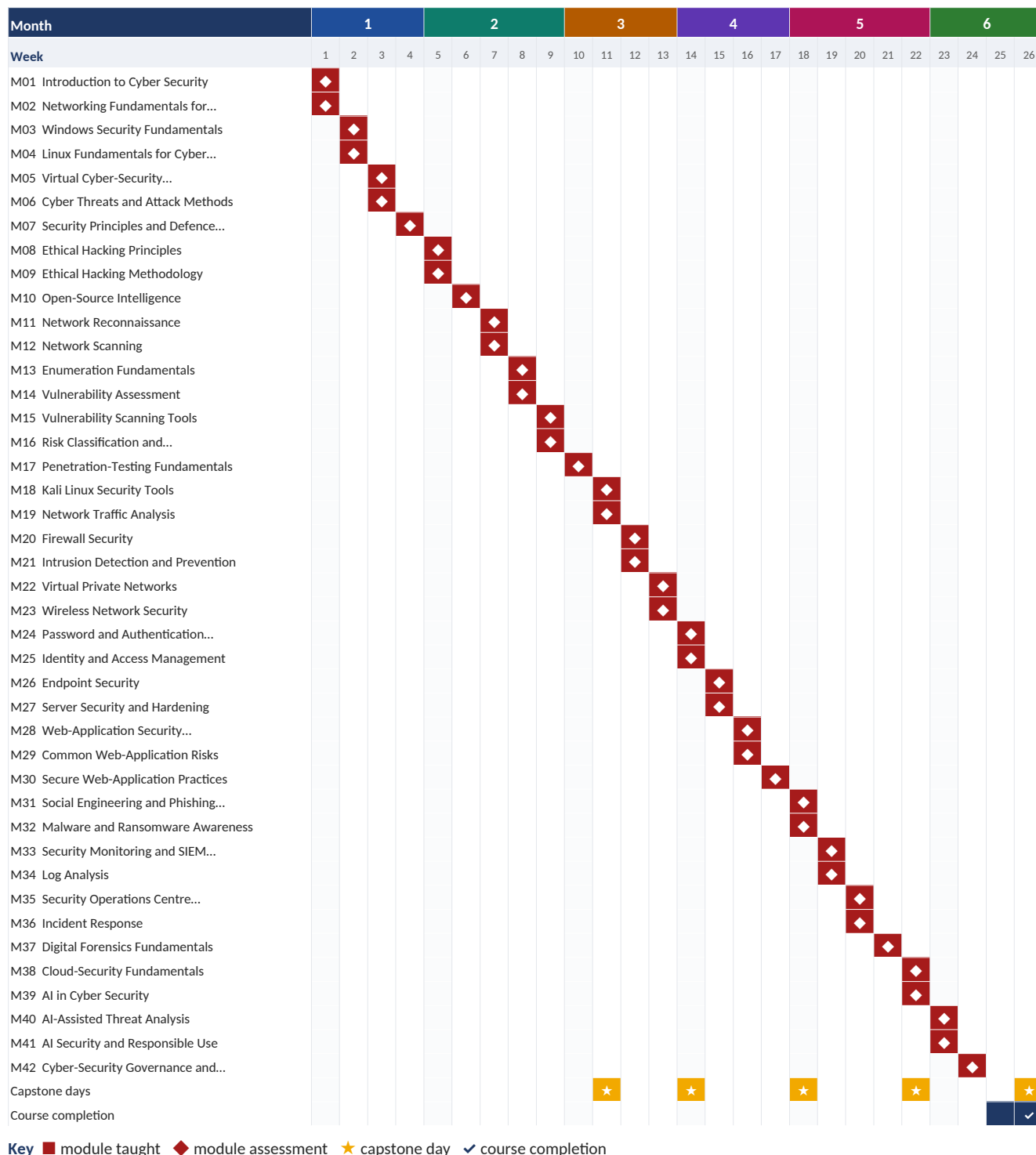
| Days    | Time               | Where  | Session                                                                  |
|---------|--------------------|--------|--------------------------------------------------------------------------|
| Tuesday | 6.30 – 11.30 PM    | Online | Online live lecture                                                      |
| Friday  | 6.30 – 10.30 PM    | Room A | Campus lab practical (your batch attends once every 4 weeks)             |
| Sunday  | 8.30 AM – 12.30 PM | Room B | Campus lab practical in groups of 20 (your group is notified in advance) |

*Rotating campus lab dates for your batch are published on the LMS at the start of each month.*

Room A and Room B are at the NextGen Campus Head Office, Nugegoda. Regular classes do not run on poya days or public holidays, which are used for capstone days.

## 8 Your Course Journey

The course runs for 26 weeks over 6 months. The chart shows when each module is taught, when you sit each module assessment (◆), and when the capstone days take place.



## Month by month

| Month   | Weeks       | What you study                                                                                                                                                                                                                                                                                                                          | Milestones                                                                                                                                                                                                                                                          |
|---------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Month 1 | Weeks 1–4   | M01 Introduction to Cyber Security<br>M02 Networking Fundamentals for Security<br>M03 Windows Security Fundamentals<br>M04 Linux Fundamentals for Cyber Security<br>M05 Virtual Cyber-Security Laboratory Setup<br>M06 Cyber Threats and Attack Methods<br>M07 Security Principles and Defence in Depth                                 | ◆ <b>Module assessment:</b> M01, M02, M03, M04, M05, M06, M07                                                                                                                                                                                                       |
| Month 2 | Weeks 5–9   | M08 Ethical Hacking Principles<br>M09 Ethical Hacking Methodology<br>M10 Open-Source Intelligence<br>M11 Network Reconnaissance<br>M12 Network Scanning<br>M13 Enumeration Fundamentals<br>M14 Vulnerability Assessment<br>M15 Vulnerability Scanning Tools<br>M16 Risk Classification and Prioritisation                               | ◆ <b>Module assessment:</b> M08, M09, M10, M11, M12, M13, M14, M15, M16                                                                                                                                                                                             |
| Month 3 | Weeks 10–13 | M17 Penetration-Testing Fundamentals<br>M18 Kali Linux Security Tools<br>M19 Network Traffic Analysis<br>M20 Firewall Security<br>M21 Intrusion Detection and Prevention<br>M22 Virtual Private Networks<br>M23 Wireless Network Security                                                                                               | ◆ <b>Module assessment:</b> M17, M18, M19, M20, M21, M22, M23<br>★ <b>Capstone day (week 11)</b>                                                                                                                                                                    |
| Month 4 | Weeks 14–17 | M24 Password and Authentication Security<br>M25 Identity and Access Management<br>M26 Endpoint Security<br>M27 Server Security and Hardening<br>M28 Web-Application Security Fundamentals<br>M29 Common Web-Application Risks<br>M30 Secure Web-Application Practices                                                                   | ◆ <b>Module assessment:</b> M24, M25, M26, M27, M28, M29, M30<br>★ <b>Capstone day (week 14)</b>                                                                                                                                                                    |
| Month 5 | Weeks 18–22 | M31 Social Engineering and Phishing Awareness<br>M32 Malware and Ransomware Awareness<br>M33 Security Monitoring and SIEM Fundamentals<br>M34 Log Analysis<br>M35 Security Operations Centre Fundamentals<br>M36 Incident Response<br>M37 Digital Forensics Fundamentals<br>M38 Cloud-Security Fundamentals<br>M39 AI in Cyber Security | ◆ <b>Module assessment:</b> M31, M32, M33, M34, M35, M36, M37, M38, M39<br>★ <b>Capstone day (week 18)</b><br>★ <b>Capstone day (week 22)</b>                                                                                                                       |
| Month 6 | Weeks 23–26 | M40 AI-Assisted Threat Analysis<br>M41 AI Security and Responsible Use<br>M42 Cyber-Security Governance and Reporting                                                                                                                                                                                                                   | ◆ <b>Module assessment:</b> M40, M41, M42<br>★ <b>Capstone day (week 26)</b><br>Week 25: Final Project Completion and Project Book Finalisation<br>Week 26: Final Project Panel Defence and Course Completion<br>✓ <b>Project Book submitted; course completion</b> |

## A typical week

| Monday                                                                                                          | Tuesday                                     | Wednesday      | Thursday       | Friday                                                                            | Saturday       | Sunday                                                                               |
|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------|----------------|----------------|-----------------------------------------------------------------------------------|----------------|--------------------------------------------------------------------------------------|
| LMS labs ≈ 2 h                                                                                                  | Online lecture<br>6.30 – 11.30 PM<br>online | LMS labs ≈ 2 h | LMS labs ≈ 2 h | Campus lab<br>6.30 – 10.30 PM<br>when your batch is<br>rostered<br>LMS labs ≈ 2 h | LMS labs ≈ 2 h | Campus lab<br>8.30 AM – 12.30 PM<br>when your batch is<br>rostered<br>LMS labs ≈ 2 h |
| Student Project Book about 2.5 h a week: update it after each class and lab with your evidence and reflections. |                                             |                |                |                                                                                   |                |                                                                                      |

LMS lab hours are a guide — about 11 h a week in total; you can arrange them across the week to suit you.

## How the course ends

| 1<br>Week 24                                                                                                | 2<br>Week 25                                                                           | 3<br>Week 26                                                                   | 4<br>End of course                                                                                          | 5<br>After the course                                                                                        | 6<br>Award                                                                            |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Final module</b><br>M42 Cyber-Security<br>Governance and<br>Reporting and the final<br>module assessment | <b>Completion week</b><br>Final Project Completion<br>and Project Book<br>Finalisation | <b>Capstone day</b><br>Final Project Panel<br>Defence and Course<br>Completion | <b>Project Book</b><br>Submit your completed<br>Student Project Book,<br>including the<br>Management Module | <b>Results</b><br>Marks are confirmed<br>and your final grade is<br>published: Distinction,<br>Merit or Pass | <b>Certificate</b><br>NextGen Campus<br>Certificate and Academic<br>Transcript issued |

**If you need a re-sit** A learner who fails a module MCQ may re-sit it once within one month. A learner who fails the capstone panel defence may re-present once within three months.

## 9 Assessment and Grading

| Component             | How you are assessed                                           | Weight      | When                 |
|-----------------------|----------------------------------------------------------------|-------------|----------------------|
| Continuous assessment | MCQ assessment at the end of each core module                  | 40%         | End of each module   |
| Practical examination | Capstone project with panel presentation and technical defence | 40%         | Poya Day 5 (week 26) |
| Student Project Book  | Project book submission, including the Management Module       | 20%         | End of course        |
| <b>Total</b>          |                                                                | <b>100%</b> |                      |

| Distinction   | Merit     | Pass      | Fail      |
|---------------|-----------|-----------|-----------|
| 70% and above | 60% – 69% | 50% – 59% | Below 50% |

**Attendance** Minimum 85% attendance at Tuesday sessions and all five capstone poya days.

**Ethics** Any breach of the ethical conduct agreement results in withdrawal of lab access and may lead to removal from the course.

**Formative practical checks** The weekly practical checks and question types are formative. They are recorded as LMS laboratory completion and give learners feedback before each module MCQ; there is no final written examination.

**MCQ assessments** Each end-of-module MCQ assessment is completed under supervision on the LMS and covers the module learning outcomes.

**Re-sits** A learner who fails a module MCQ may re-sit it once within one month. A learner who fails the capstone panel defence may re-present once within three months.

### Award requirements — to receive your certificate

You must maintain a minimum attendance of 85%, complete all core-module MCQ assessments and LMS laboratories, submit the Student Project Book and pass the capstone practical examination, achieving an overall mark of at least 50%, to qualify for the certificate.

## 10 Capstone Project

The programme concludes with Module 43, the Final Enterprise Cyber-Security Project — an authorised, end-to-end security assessment of a simulated enterprise environment, delivered physically over five poya days (9.00 AM – 5.00 PM) at the NextGen Campus Head Office, Nugegoda, inside an isolated lab. Each day is scheduled after the phase it builds on. Students document assets, vulnerabilities, risks, controls, findings and recommended improvements, then present and defend the project to a panel.

| Day          | When          | Focus                                                                                                         | Hours |
|--------------|---------------|---------------------------------------------------------------------------------------------------------------|-------|
| Poya Day 1   | After week 10 | Scope and rules of engagement; asset discovery, OSINT, scanning and enumeration of the enterprise environment | 8     |
| Poya Day 2   | After week 13 | Vulnerability assessment and controlled validation of network, endpoint and web targets                       | 8     |
| Poya Day 3   | After week 17 | Defensive review: firewall, IDS/IPS, endpoint, server and web hardening recommendations                       | 8     |
| Poya Day 4   | After week 21 | Monitoring and response: SIEM detections, log analysis and an incident-response runbook                       | 8     |
| Poya Day 5   | Week 26       | Findings report, business-impact and remediation plan, panel presentation and technical defence               | 8     |
| <b>Total</b> | <b>40</b>     |                                                                                                               |       |

### What you will deliver

- Signed scope and rules of engagement
- Asset inventory and reconnaissance findings
- Validated vulnerability assessment with risk ratings
- Findings report with business-impact and remediation plan
- Panel presentation and technical defence

## 11 Student Project Book

The Student Project Book is a guided professional record developed throughout the course. It documents the student's laboratory work, findings and project outcomes, and contains the Management Module, which builds the professional and management skills expected of a security professional.

The Project Book contains module-by-module laboratory records and LMS evidence, Management Module activities and reflections, capstone planning and final documentation, and a professional technical portfolio. It is reviewed by the trainer at the end of each module.

Bring your Project Book up to date every week. It is assessed at the end of the course and counts for 20% of your final mark.

## 12 Your Certificate

When you meet the award requirements you receive the NextGen Campus Certificate — Certificate in AI-Driven Cyber Security and Ethical Hacking — together with an Academic Transcript showing every module and your final grade (Distinction, Merit or Pass).

**Industry certifications** The modules are aligned to these industry certifications: CompTIA Security+ aligned; PenTest+ - CEH-style methodology; Security+ - Network+ aligned; Security+ - CySA+ aligned; CySA+ - SC-200 pathway; Cloud & AI security. Certification exam fees are not included in the course fee unless NextGen Campus states otherwise.

## 13 Student Guidelines

- Attend at least 85% of your scheduled classes and all capstone sessions. Inform your course coordinator in advance if you cannot attend.
- Be on time for every class, online or on campus. For online classes, join with your camera available and your full name displayed.
- Complete your LMS module labs every week and keep your Project Book up to date — do not leave them to the end of a module.
- Do your own work. Copying, sharing answers or submitting someone else's work is not allowed in any assessment.
- Use AI tools responsibly: use them to learn and to check your work, check every AI output, never paste confidential or personal data, and say when you used AI in your Project Book.
- Look after campus equipment and follow lab safety instructions, including ESD precautions when handling hardware.
- Security testing is done only on authorised NextGen lab systems. You must sign the ethical conduct agreement before lab access; any breach leads to withdrawal of lab access and may lead to removal from the course.
- Keep your LMS login private and check the LMS and your email regularly for announcements, timetable changes and assessment dates.

## 14 Help and Contact

|                                |                                                                                                                                            |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Head Office</b>             | NextGen Campus (Pvt) Ltd, Nugegoda, Sri Lanka                                                                                              |
| <b>Phone</b>                   | +94 11 251 5215 · +94 77 810 0810                                                                                                          |
| <b>Email</b>                   | info@nextgencampus.lk                                                                                                                      |
| <b>Website</b>                 | www.nextgencampus.lk                                                                                                                       |
| <b>LMS support</b>             | Use the help desk on the NextGen LMS for login, lab environment and technical questions. A weekly online Q&A session is held for LMS labs. |
| <b>Your course coordinator</b> | Introduced at orientation — contact them about attendance, batches, re-sits and any personal circumstances.                                |



## PART B Module Details

The course has 42 modules, studied in the order below. Each module lists its aim, what you will learn, what you will be able to do, and the hands-on labs you will complete.

| Code | Module                                   | Lecture h | Lab h | Industry alignment               |
|------|------------------------------------------|-----------|-------|----------------------------------|
| M01  | Introduction to Cyber Security           | 2         | 6.25  | CompTIA Security+ aligned        |
| M02  | Networking Fundamentals for Security     | 2         | 6.25  | CompTIA Security+ aligned        |
| M03  | Windows Security Fundamentals            | 2         | 6.25  | CompTIA Security+ aligned        |
| M04  | Linux Fundamentals for Cyber Security    | 2         | 6.25  | CompTIA Security+ aligned        |
| M05  | Virtual Cyber-Security Laboratory Setup  | 2         | 6.25  | CompTIA Security+ aligned        |
| M06  | Cyber Threats and Attack Methods         | 2         | 6.25  | CompTIA Security+ aligned        |
| M07  | Security Principles and Defence in Depth | 4         | 12.5  | CompTIA Security+ aligned        |
| M08  | Ethical Hacking Principles               | 2         | 6.25  | PenTest+ - CEH-style methodology |
| M09  | Ethical Hacking Methodology              | 2         | 6.25  | PenTest+ - CEH-style methodology |
| M10  | Open-Source Intelligence                 | 4         | 12.5  | PenTest+ - CEH-style methodology |
| M11  | Network Reconnaissance                   | 2         | 6.25  | PenTest+ - CEH-style methodology |
| M12  | Network Scanning                         | 2         | 6.25  | PenTest+ - CEH-style methodology |
| M13  | Enumeration Fundamentals                 | 2         | 6.25  | PenTest+ - CEH-style methodology |
| M14  | Vulnerability Assessment                 | 2         | 6.25  | PenTest+ - CEH-style methodology |
| M15  | Vulnerability Scanning Tools             | 2         | 6.25  | PenTest+ - CEH-style methodology |
| M16  | Risk Classification and Prioritisation   | 2         | 6.25  | PenTest+ - CEH-style methodology |
| M17  | Penetration-Testing Fundamentals         | 4         | 12.5  | PenTest+ - CEH-style methodology |
| M18  | Kali Linux Security Tools                | 2         | 6.25  | Security+ - Network+ aligned     |
| M19  | Network Traffic Analysis                 | 2         | 6.25  | Security+ - Network+ aligned     |
| M20  | Firewall Security                        | 2         | 6.25  | Security+ - Network+ aligned     |
| M21  | Intrusion Detection and Prevention       | 2         | 6.25  | Security+ - Network+ aligned     |
| M22  | Virtual Private Networks                 | 2         | 6.25  | Security+ - Network+ aligned     |
| M23  | Wireless Network Security                | 2         | 6.25  | Security+ - Network+ aligned     |
| M24  | Password and Authentication Security     | 2         | 6.25  | Security+ - CySA+ aligned        |
| M25  | Identity and Access Management           | 2         | 6.25  | Security+ - CySA+ aligned        |
| M26  | Endpoint Security                        | 2         | 6.25  | Security+ - CySA+ aligned        |

| Code                     | Module                                    | Lecture h | Lab h      | Industry alignment        |
|--------------------------|-------------------------------------------|-----------|------------|---------------------------|
| M27                      | Server Security and Hardening             | 2         | 6.25       | Security+ - CySA+ aligned |
| M28                      | Web-Application Security Fundamentals     | 2         | 6.25       | Security+ - CySA+ aligned |
| M29                      | Common Web-Application Risks              | 2         | 6.25       | Security+ - CySA+ aligned |
| M30                      | Secure Web-Application Practices          | 4         | 12.5       | Security+ - CySA+ aligned |
| M31                      | Social Engineering and Phishing Awareness | 2         | 6.25       | CySA+ - SC-200 pathway    |
| M32                      | Malware and Ransomware Awareness          | 2         | 6.25       | CySA+ - SC-200 pathway    |
| M33                      | Security Monitoring and SIEM Fundamentals | 2         | 6.25       | CySA+ - SC-200 pathway    |
| M34                      | Log Analysis                              | 2         | 6.25       | CySA+ - SC-200 pathway    |
| M35                      | Security Operations Centre Fundamentals   | 2         | 6.25       | CySA+ - SC-200 pathway    |
| M36                      | Incident Response                         | 2         | 6.25       | CySA+ - SC-200 pathway    |
| M37                      | Digital Forensics Fundamentals            | 4         | 12.5       | CySA+ - SC-200 pathway    |
| M38                      | Cloud-Security Fundamentals               | 2         | 6.25       | Cloud & AI security       |
| M39                      | AI in Cyber Security                      | 2         | 6.25       | Cloud & AI security       |
| M40                      | AI-Assisted Threat Analysis               | 2         | 6.25       | Cloud & AI security       |
| M41                      | AI Security and Responsible Use           | 2         | 6.25       | Cloud & AI security       |
| M42                      | Cyber-Security Governance and Reporting   | 4         | 12.5       | Cloud & AI security       |
| <b>Total for modules</b> |                                           | <b>96</b> | <b>300</b> |                           |

Lab hours are LMS module labs and campus lab practicals. Capstone and Project Book hours are in addition to the module hours.

## M01 Introduction to Cyber Security 2 h lecture · 6.25 h labs

Phase 1 — Security Foundations · Aligned to CompTIA Security+ aligned

**Aim** Understand the purpose of cyber security and how organisations protect systems, networks, applications and data. Students explore common security terminology, professional roles and the confidentiality, integrity and availability principles.

### What you will learn

- Purpose of cyber security
- CIA triad
- Security terminology
- Threats, vulnerabilities and risk
- Security roles and the industry

### You will be able to

- Explain the purpose of cyber security and the CIA triad
- Describe common security terminology and threats
- Outline security roles and career paths

### Hands-on LMS labs — 6.25 hours

- Map the CIA triad to real business scenarios
- Build a personal security glossary on the LMS

### Using AI in this module

- Use an AI assistant to explain security terms, verified against trusted sources

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M02 Networking Fundamentals for Security 2 h lecture · 6.25 h labs

Phase 1 — Security Foundations · Aligned to CompTIA Security+ aligned

**Aim** Learn how devices communicate through TCP/IP networks. Students study IP addressing, ports, protocols, DNS, routing, switching and network devices to understand how traffic can be analysed and protected.

### What you will learn

### You will be able to

- OSI and TCP/IP models
- IP addressing and subnetting
- Ports and protocols
- DNS and routing
- Switches, routers and firewalls
- Explain the TCP/IP model and common protocols
- Describe IP addressing, ports and DNS
- Explain how switching and routing move traffic

#### Hands-on LMS labs — 6.25 hours

- Map protocols to layers and ports
- Trace a packet through a small network in a simulator

#### Using AI in this module

- AI-assisted explanation of protocols and packet flows

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

### M03 Windows Security Fundamentals 2 h lecture · 6.25 h labs

Phase 1 — Security Foundations · Aligned to CompTIA Security+ aligned

**Aim** Explore Windows users, groups, permissions, services, updates, firewalls and event logs. Students learn how secure configurations reduce common operating-system risks.

#### What you will learn

- Users, groups and NTFS permissions
- Services and startup
- Windows Update
- Windows Defender Firewall
- Event Viewer and security logs

#### You will be able to

- Manage Windows users, groups and permissions
- Configure updates, services and the firewall
- Read Windows event logs for security events

#### Hands-on LMS labs — 6.25 hours

- Harden a Windows workstation to a checklist
- Find security events in Event Viewer

#### Using AI in this module

- AI-assisted interpretation of Windows event logs

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

### M04 Linux Fundamentals for Cyber Security 2 h lecture · 6.25 h labs

Phase 1 — Security Foundations · Aligned to CompTIA Security+ aligned

**Aim** Develop practical Linux skills using the command line. Students manage files, permissions, users, processes, services, network settings and logs within a controlled environment.

#### What you will learn

- Shell navigation and file management
- Users, groups and file permissions
- Processes and services (systemd)
- Networking commands
- Logs under /var/log

#### You will be able to

- Navigate and manage files from the Linux shell
- Manage users, permissions, processes and services
- Inspect network settings and system logs

#### Hands-on LMS labs — 6.25 hours

- Complete guided command-line exercises
- Investigate a Linux system from the logs

#### Using AI in this module

- AI-assisted help with shell commands, verified by the learner

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M05 Virtual Cyber-Security Laboratory Setup****2 h lecture · 6.25 h labs***Phase 1 — Security Foundations · Aligned to CompTIA Security+ aligned*

**Aim** Build a safe virtual laboratory using approved virtualisation technologies. Students configure isolated Windows, Linux and security-testing machines for practical training.

**What you will learn**

- Virtualisation with VirtualBox/VMware
- Host-only and internal networks
- Snapshots and safe rollback
- Lab rules and isolation
- Code of conduct

**You will be able to**

- Build an isolated virtual laboratory
- Configure Windows, Linux and Kali machines
- Apply lab rules and the code of conduct

**Hands-on LMS labs — 6.25 hours**

- Build the isolated lab used for the rest of the course
- Configure host-only networking and snapshots

**Using AI in this module**

- AI-assisted troubleshooting of lab setup issues

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M06 Cyber Threats and Attack Methods****2 h lecture · 6.25 h labs***Phase 1 — Security Foundations · Aligned to CompTIA Security+ aligned*

**Aim** Study malware, ransomware, phishing, social engineering, credential attacks and unauthorised access. Students learn how these threats affect organisations and how layered controls reduce risk.

**What you will learn**

- Malware and ransomware
- Phishing and social engineering
- Credential attacks
- Unauthorised access
- Layered controls

**You will be able to**

- Describe common threats and attack methods
- Explain how threats affect organisations
- Match layered controls to threats

**Hands-on LMS labs — 6.25 hours**

- Classify sample threats by type and impact
- Map controls to a threat scenario

**Using AI in this module**

- AI-assisted threat classification and summaries

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M07 Security Principles and Defence in Depth****4 h lecture · 12.5 h labs***Phase 1 — Security Foundations · Aligned to CompTIA Security+ aligned*

**Aim** Understand least privilege, Zero Trust concepts, segmentation, access control and layered security. Students learn how multiple controls work together to protect organisational systems.

**What you will learn**

- Least privilege
- Zero Trust principles
- Segmentation
- Access control models
- Defence in depth

**You will be able to**

- Apply least privilege and Zero Trust concepts
- Design network segmentation and access control
- Explain how layered controls combine

**Hands-on LMS labs — 12.5 hours**

- Design a layered defence for a small business
- Review a network for segmentation gaps

**Using AI in this module**

- AI-assisted review of a defence-in-depth design

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M08 Ethical Hacking Principles****2 h lecture · 6.25 h labs**

Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology

**Aim** Learn the legal, ethical and professional responsibilities of security testing. Students study authorisation, scope, evidence handling, reporting and responsible disclosure.

**What you will learn**

- Legal and ethical responsibilities
- Authorisation and scope
- Rules of engagement
- Evidence handling
- Responsible disclosure
- Computer Crimes Act No. 24 of 2007

**You will be able to**

- Explain the legal and ethical basis of testing
- Define authorisation, scope and rules of engagement
- Apply evidence handling and responsible disclosure

**Hands-on LMS labs — 6.25 hours**

- Draft a rules-of-engagement document
- Review a disclosure case study

**Using AI in this module**

- AI-assisted drafting of engagement paperwork, reviewed by the learner

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M09 Ethical Hacking Methodology****2 h lecture · 6.25 h labs**

Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology

**Aim** Explore the main stages of an authorised security assessment, including planning, reconnaissance, scanning, analysis, controlled validation, reporting and remediation.

**What you will learn**

- Planning and scoping
- Reconnaissance
- Scanning
- Analysis
- Controlled validation
- Reporting and remediation

**You will be able to**

- Describe the stages of an authorised assessment
- Plan an engagement end to end
- Link each stage to its deliverables

**Hands-on LMS labs — 6.25 hours**

- Plan a full engagement for a lab scenario
- Produce a stage-by-stage checklist

**Using AI in this module**

- AI-assisted planning checklists, verified against the methodology

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M10 Open-Source Intelligence****4 h lecture · 12.5 h labs***Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology*

**Aim** Learn how publicly available information can reveal organisational risks. Students use responsible information-gathering methods while respecting privacy and legal boundaries.

**What you will learn**

- OSINT sources and methods
- DNS and domain information
- Social-media exposure
- Metadata
- Privacy and legal limits

**You will be able to**

- Gather open-source information responsibly
- Identify organisational exposure from public data
- Respect privacy and legal boundaries

**Hands-on LMS labs — 12.5 hours**

- Run authorised OSINT on a fictional organisation
- Document exposure and recommendations

**Using AI in this module**

- AI-assisted OSINT summaries, with sources verified

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M11 Network Reconnaissance****2 h lecture · 6.25 h labs***Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology*

**Aim** Understand how security professionals identify hosts, networks, services and exposed systems within an authorised scope. Students document discovered assets and possible risks.

**What you will learn**

- Host discovery
- Network mapping
- Service identification
- Asset documentation
- Scope control

**You will be able to**

- Identify hosts, networks and services in scope
- Map an authorised network
- Document assets and risks

**Hands-on LMS labs — 6.25 hours**

- Map an authorised lab network
- Produce an asset inventory

**Using AI in this module**

- AI-assisted asset documentation

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M12 Network Scanning****2 h lecture · 6.25 h labs***Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology*

**Aim** Use approved scanning tools to identify active hosts, open ports and services within controlled laboratories. Students learn how scan results support vulnerability assessment.

**What you will learn**

- Nmap scan types
- Port and service detection
- Timing and safety
- Reading scan output
- From scanning to assessment

**You will be able to**

- Scan for active hosts, ports and services
- Interpret scan output
- Use scans to support vulnerability assessment

**Hands-on LMS labs — 6.25 hours**

- Scan and enumerate lab targets with Nmap
- Document open ports and services

**Using AI in this module**

- AI-assisted interpretation of scan results

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M13 Enumeration Fundamentals 2 h lecture · 6.25 h labs

Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology

**Aim** Learn how security professionals gather detailed information about users, shares, services and system configurations. Students practise safe enumeration in simulated environments.

**What you will learn**

- SMB and share enumeration
- User and group enumeration
- Service banners
- SNMP basics
- Recording findings

**You will be able to**

- Enumerate users, shares and services
- Gather configuration detail safely
- Record enumeration findings

**Hands-on LMS labs — 6.25 hours**

- Enumerate a lab server
- Build an enumeration findings sheet

**Using AI in this module**

- AI-assisted organisation of enumeration notes

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M14 Vulnerability Assessment 2 h lecture · 6.25 h labs

Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology

**Aim** Identify weaknesses in systems, applications and network devices using authorised assessment methods. Students learn how to validate findings and avoid inaccurate conclusions.

**What you will learn**

- Assessment methods
- Common weaknesses
- Validation and false positives
- Evidence
- Assessment reporting

**You will be able to**

- Identify weaknesses across systems and devices
- Validate findings to remove false positives
- Record assessment results clearly

**Hands-on LMS labs — 6.25 hours**

- Assess a lab environment and validate findings
- Write a vulnerability assessment record

**Using AI in this module**

- AI-supported triage of findings, verified by the learner

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M15 Vulnerability Scanning Tools 2 h lecture · 6.25 h labs

Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology

**Aim** Gain exposure to vulnerability-scanning platforms used to identify outdated software, insecure services and configuration weaknesses. Students review findings and prioritise remediation.

### What you will learn

- Vulnerability scanners (OpenVAS/Greenbone)
- Scan configuration
- Reading reports
- False positives
- Remediation priorities

### You will be able to

- Run authorised vulnerability scans
- Review and interpret scanner output
- Prioritise remediation

### Hands-on LMS labs — 6.25 hours

- Run a scan against lab targets
- Prioritise the findings for remediation

### Using AI in this module

- AI-assisted summarisation of scan reports

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M16 Risk Classification and Prioritisation 2 h lecture · 6.25 h labs

Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology

**Aim** Learn how vulnerabilities are classified according to likelihood, impact and business importance. Students prepare clear risk summaries for technical and non-technical audiences.

### What you will learn

- Likelihood and impact
- CVSS
- Business context
- Risk registers
- Communicating risk

### You will be able to

- Classify risk by likelihood and impact
- Prioritise by business importance
- Communicate risk to any audience

### Hands-on LMS labs — 6.25 hours

- Score findings with CVSS
- Write a risk summary for management

### Using AI in this module

- AI-assisted drafting of risk summaries

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M17 Penetration-Testing Fundamentals 4 h lecture · 12.5 h labs

Phase 2 — Ethical Hacking & Security Assessment · Aligned to PenTest+ - CEH-style methodology

**Aim** Understand how controlled penetration testing validates whether identified weaknesses could create business risk. Activities remain limited to approved training environments.

### What you will learn

- Purpose of penetration testing
- Controlled validation
- Exploitation basics (Metasploit)
- Evidence capture
- Staying in scope

### You will be able to

- Explain how controlled testing validates risk
- Safely validate a weakness in the lab
- Record evidence professionally

**Hands-on LMS labs — 12.5 hours**

- Validate a known weakness in the lab
- Capture evidence for a report

**Using AI in this module**

- AI-assisted exploit research, verified against lab evidence

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M18 Kali Linux Security Tools****2 h lecture · 6.25 h labs**

Phase 3 — Network & Infrastructure Defence · Aligned to Security+ - Network+ aligned

**Aim** Explore the Kali Linux interface and selected tools used for authorised scanning, analysis and testing. Students learn responsible tool selection and documentation.

**What you will learn**

- Kali interface and tool categories
- Common tools
- Responsible tool selection
- Documentation
- Updates and maintenance

**You will be able to**

- Navigate Kali Linux and its tool categories
- Select the right tool for a task
- Document tool use responsibly

**Hands-on LMS labs — 6.25 hours**

- Use selected Kali tools on lab targets
- Document tool use and results

**Using AI in this module**

- AI-assisted guidance on tool selection

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M19 Network Traffic Analysis****2 h lecture · 6.25 h labs**

Phase 3 — Network & Infrastructure Defence · Aligned to Security+ - Network+ aligned

**Aim** Use Wireshark and related tools to inspect authorised network traffic. Students identify protocols, communication patterns and signs that may require investigation.

**What you will learn**

- Packet capture
- Wireshark filters
- Protocol analysis
- Communication patterns
- Indicators of concern

**You will be able to**

- Capture and filter traffic in Wireshark
- Identify protocols and patterns
- Spot signs that need investigation

**Hands-on LMS labs — 6.25 hours**

- Analyse captures for anomalies
- Write investigation notes from a capture

**Using AI in this module**

- AI-assisted explanation of packet captures

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M20 Firewall Security****2 h lecture · 6.25 h labs***Phase 3 — Network & Infrastructure Defence · Aligned to Security+ - Network+ aligned*

**Aim** Understand hardware and software firewalls, rule design, network zones and traffic filtering. Students review how misconfigured rules can expose systems.

**What you will learn**

- Firewall types
- Rule design
- Network zones
- Traffic filtering
- Common misconfigurations

**You will be able to**

- Design firewall rules and zones
- Filter traffic between zones
- Identify misconfigured rules

**Hands-on LMS labs — 6.25 hours**

- Configure firewall rules for a lab network
- Review a ruleset for exposure

**Using AI in this module**

- AI-assisted firewall rule review

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M21 Intrusion Detection and Prevention****2 h lecture · 6.25 h labs***Phase 3 — Network & Infrastructure Defence · Aligned to Security+ - Network+ aligned*

**Aim** Explore how intrusion-detection and prevention systems monitor traffic and generate alerts. Students analyse simulated alerts and recommend suitable response actions.

**What you will learn**

- IDS vs IPS
- Signatures and anomalies
- Alert analysis
- Tuning
- Response actions

**You will be able to**

- Explain how IDS/IPS monitor traffic
- Analyse alerts
- Recommend response actions

**Hands-on LMS labs — 6.25 hours**

- Deploy and tune an IDS in the lab
- Analyse simulated alerts

**Using AI in this module**

- AI-assisted alert prioritisation

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M22 Virtual Private Networks****2 h lecture · 6.25 h labs***Phase 3 — Network & Infrastructure Defence · Aligned to Security+ - Network+ aligned*

**Aim** Learn how site-to-site and remote-access VPNs protect communication. Students explore encryption, authentication and secure remote-working requirements.

**What you will learn**

- VPN types
- IPsec and SSL/TLS
- Encryption and authentication
- Remote working
- VPN weaknesses

**You will be able to**

- Explain site-to-site and remote-access VPNs
- Describe VPN encryption and authentication
- Apply secure remote-working requirements

**Hands-on LMS labs — 6.25 hours**

- Configure a VPN between lab sites
- Test secure remote access

**Using AI in this module**

- AI-assisted VPN configuration review

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M23 Wireless Network Security 2 h lecture · 6.25 h labs

Phase 3 — Network & Infrastructure Defence · Aligned to Security+ - Network+ aligned

**Aim** Understand wireless standards, encryption, access-point security and common configuration weaknesses. Students assess authorised wireless environments and recommend improvements.

**What you will learn**

- Wi-Fi standards
- WPA2/WPA3
- Access-point security
- Common weaknesses
- Site assessment

**You will be able to**

- Explain wireless standards and encryption
- Secure access points
- Assess wireless configuration weaknesses

**Hands-on LMS labs — 6.25 hours**

- Assess an authorised wireless setup
- Recommend wireless improvements

**Using AI in this module**

- AI-assisted wireless configuration review

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M24 Password and Authentication Security 2 h lecture · 6.25 h labs

Phase 4 — Access, Endpoint, Server & Web Security · Aligned to Security+ - CySA+ aligned

**Aim** Explore password policies, multifactor authentication, credential risks and secure authentication practices. Students perform controlled password-strength auditing without targeting unauthorised systems.

**What you will learn**

- Password policies
- Multifactor authentication
- Credential risks
- Hashing basics
- Controlled auditing

**You will be able to**

- Design password policies and MFA
- Explain credential risks
- Audit password strength responsibly

**Hands-on LMS labs — 6.25 hours**

- Audit password strength on lab accounts
- Design an authentication policy

**Using AI in this module**

- AI-assisted policy drafting

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M25 Identity and Access Management****2 h lecture · 6.25 h labs***Phase 4 — Access, Endpoint, Server & Web Security · Aligned to Security+ - CySA+ aligned*

**Aim** Learn how organisations manage users, groups, roles and permissions. Students apply least privilege and role-based access principles to business scenarios.

**What you will learn**

- Identity lifecycle
- Groups and roles
- RBAC
- Least privilege
- Access reviews

**You will be able to**

- Manage users, groups and roles
- Apply least privilege and RBAC
- Design access for a business scenario

**Hands-on LMS labs — 6.25 hours**

- Design RBAC for a business scenario
- Run an access review

**Using AI in this module**

- AI-assisted access-model review

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M26 Endpoint Security****2 h lecture · 6.25 h labs***Phase 4 — Access, Endpoint, Server & Web Security · Aligned to Security+ - CySA+ aligned*

**Aim** Understand antivirus, endpoint detection, system updates, application control, device policies and secure configurations used to protect organisational endpoints.

**What you will learn**

- Antivirus and EDR
- Updates and patching
- Application control
- Device policies
- Secure configuration

**You will be able to**

- Configure endpoint protection and updates
- Apply application control and device policies
- Harden endpoint configurations

**Hands-on LMS labs — 6.25 hours**

- Harden an endpoint to a baseline
- Configure application control

**Using AI in this module**

- AI-assisted endpoint hardening checklist

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M27 Server Security and Hardening****2 h lecture · 6.25 h labs***Phase 4 — Access, Endpoint, Server & Web Security · Aligned to Security+ - CySA+ aligned*

**Aim** Learn how to reduce server risks through updates, service management, permissions, firewall settings, logging, auditing and removal of unnecessary components.

**What you will learn**

- Patching
- Service management
- Permissions
- Firewall and logging
- Auditing and baselines

**You will be able to**

- Harden servers with updates and least service
- Configure permissions, firewall and logging
- Audit servers against a baseline

**Hands-on LMS labs — 6.25 hours**

- Harden a lab server to a baseline
- Audit a server for weaknesses

**Using AI in this module**

- AI-assisted hardening review

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M28 Web-Application Security Fundamentals****2 h lecture · 6.25 h labs**

Phase 4 — Access, Endpoint, Server & Web Security · Aligned to Security+ - CySA+ aligned

**Aim** Understand how web applications process users, sessions, databases and input. Students learn how insecure design and configuration can lead to security weaknesses.

**What you will learn**

- Web application architecture
- Users and sessions
- Input handling
- Databases
- Insecure design

**You will be able to**

- Explain how web applications work
- Describe sessions, input and database handling
- Explain how insecure design creates risk

**Hands-on LMS labs — 6.25 hours**

- Explore a lab web application
- Map its trust boundaries

**Using AI in this module**

- AI-assisted explanation of web application flows

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M29 Common Web-Application Risks****2 h lecture · 6.25 h labs**

Phase 4 — Access, Endpoint, Server & Web Security · Aligned to Security+ - CySA+ aligned

**Aim** Explore recognised web-security risks such as insecure access control, weak authentication, injection and unsafe data handling through controlled demonstrations.

**What you will learn**

- OWASP Top 10
- Broken access control
- Injection (SQLi)
- Cross-site scripting
- Unsafe data handling

**You will be able to**

- Identify OWASP Top 10 risks
- Demonstrate injection and access-control flaws safely
- Explain the impact of each risk

**Hands-on LMS labs — 6.25 hours**

- Test DVWA and OWASP Juice Shop
- Record findings with impact

**Using AI in this module**

- AI-assisted explanation of web risks, verified in the lab

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M30 Secure Web-Application Practices****4 h lecture · 12.5 h labs***Phase 4 — Access, Endpoint, Server & Web Security · Aligned to Security+ - CySA+ aligned*

**Aim** Learn how validation, secure authentication, patching, encryption and security testing reduce web-application risk. Students prepare practical remediation recommendations.

**What you will learn**

- Input validation
- Secure authentication
- Patching
- Encryption
- Security testing
- Remediation

**You will be able to**

- Apply input validation and secure authentication
- Use patching, encryption and testing
- Write remediation recommendations

**Hands-on LMS labs — 12.5 hours**

- Remediate flaws in a lab web application
- Write remediation recommendations

**Using AI in this module**

- AI-assisted remediation guidance

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M31 Social Engineering and Phishing Awareness****2 h lecture · 6.25 h labs***Phase 5 — Threat Detection, Monitoring & Response · Aligned to CySA+ - SC-200 pathway*

**Aim** Understand how attackers manipulate users through phishing, impersonation and false urgency. Students analyse simulated messages and design awareness controls.

**What you will learn**

- Social engineering
- Phishing and impersonation
- False urgency
- Message analysis
- Awareness controls

**You will be able to**

- Explain social-engineering techniques
- Analyse phishing messages
- Design awareness controls

**Hands-on LMS labs — 6.25 hours**

- Analyse simulated phishing messages
- Design an awareness campaign

**Using AI in this module**

- AI-assisted phishing message analysis

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.***M32 Malware and Ransomware Awareness****2 h lecture · 6.25 h labs***Phase 5 — Threat Detection, Monitoring & Response · Aligned to CySA+ - SC-200 pathway*

**Aim** Study common malware behaviours, delivery methods and business impact. Students learn basic indicators, prevention measures and response procedures without creating malware.

**What you will learn**

- Malware types
- Delivery methods
- Ransomware impact
- Indicators of compromise
- Prevention and response

**You will be able to**

- Describe malware behaviours and delivery
- Recognise basic indicators
- Apply prevention and response procedures

**Hands-on LMS labs — 6.25 hours**

- Identify indicators from a safe sample report
- Draft a ransomware response checklist

**Using AI in this module**

- AI-assisted indicator summaries

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M33 Security Monitoring and SIEM Fundamentals 2 h lecture · 6.25 h labs**

Phase 5 — Threat Detection, Monitoring & Response · Aligned to CySA+ - SC-200 pathway

**Aim** Understand how security teams collect and review logs from endpoints, servers, applications and network devices. Students explore alert handling and security-event correlation.

**What you will learn**

- SIEM concepts
- Log sources
- Correlation rules
- Alert handling
- Dashboards

**You will be able to**

- Explain SIEM log collection and correlation
- Handle alerts
- Correlate security events

**Hands-on LMS labs — 6.25 hours**

- Connect log sources to a SIEM
- Correlate events into an alert

**Using AI in this module**

- AI-assisted event correlation

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M34 Log Analysis 2 h lecture · 6.25 h labs**

Phase 5 — Threat Detection, Monitoring & Response · Aligned to CySA+ - SC-200 pathway

**Aim** Review Windows, Linux, firewall and application logs within simulated incidents. Students identify unusual activity and prepare basic investigation notes.

**What you will learn**

- Windows logs
- Linux logs
- Firewall and application logs
- Spotting anomalies
- Investigation notes

**You will be able to**

- Analyse Windows, Linux and firewall logs
- Identify unusual activity
- Prepare investigation notes

**Hands-on LMS labs — 6.25 hours**

- Investigate a simulated incident from logs
- Write investigation notes

**Using AI in this module**

- AI-assisted log analysis, verified by the learner

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

### M35 Security Operations Centre Fundamentals 2 h lecture · 6.25 h labs

Phase 5 — Threat Detection, Monitoring & Response · Aligned to CySA+ - SC-200 pathway

**Aim** Explore SOC responsibilities, analyst workflows, alert triage, escalation and incident documentation. Students practise basic analyst activities through guided scenarios.

#### What you will learn

- SOC roles and tiers
- Analyst workflow
- Alert triage
- Escalation
- Documentation

#### You will be able to

- Describe SOC roles and workflows
- Triage and escalate alerts
- Document incidents

#### Hands-on LMS labs — 6.25 hours

- Run a guided SOC shift scenario
- Triage and escalate alerts

#### Using AI in this module

- AI-assisted alert triage

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

### M36 Incident Response 2 h lecture · 6.25 h labs

Phase 5 — Threat Detection, Monitoring & Response · Aligned to CySA+ - SC-200 pathway

**Aim** Learn the main stages of incident response: preparation, detection, analysis, containment, recovery and review. Students prepare response plans for common cyber incidents.

#### What you will learn

- Preparation
- Detection and analysis
- Containment
- Recovery
- Review
- NIST SP 800-61

#### You will be able to

- Describe the incident-response lifecycle
- Contain and recover from an incident
- Prepare a response plan

#### Hands-on LMS labs — 6.25 hours

- Respond to a simulated incident end to end
- Write an incident-response plan

#### Using AI in this module

- AI-assisted incident timelines and reports

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

### M37 Digital Forensics Fundamentals 4 h lecture · 12.5 h labs

Phase 5 — Threat Detection, Monitoring & Response · Aligned to CySA+ - SC-200 pathway

**Aim** Understand digital evidence, chain of custody, data preservation and basic forensic processes. Students learn how evidence must be handled professionally.

#### What you will learn

- Digital evidence
- Chain of custody
- Data preservation
- Imaging
- Basic analysis

#### You will be able to

- Explain digital evidence and chain of custody
- Preserve data correctly
- Follow a basic forensic process

**Hands-on LMS labs — 12.5 hours**

- Preserve and image evidence in the lab
- Analyse an image with Autopsy

**Using AI in this module**

- AI-assisted organisation of forensic notes

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M38 Cloud-Security Fundamentals 2 h lecture · 6.25 h labs**

Phase 6 — Cloud, AI & Governance · Aligned to Cloud & AI security

**Aim** Explore shared responsibility, cloud identity, access control, secure storage, network protection and monitoring across cloud environments.

**What you will learn**

- Shared responsibility
- Cloud identity and access
- Secure storage
- Network protection
- Cloud monitoring

**You will be able to**

- Explain the shared responsibility model
- Secure cloud identity, storage and networks
- Monitor cloud environments

**Hands-on LMS labs — 6.25 hours**

- Secure a lab cloud workload
- Review cloud monitoring alerts

**Using AI in this module**

- AI-assisted cloud security review

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

**M39 AI in Cyber Security 2 h lecture · 6.25 h labs**

Phase 6 — Cloud, AI & Governance · Aligned to Cloud & AI security

**Aim** Understand how artificial intelligence supports threat detection, anomaly identification, phishing analysis, alert prioritisation and security automation.

**What you will learn**

- AI for threat detection
- Anomaly detection
- Phishing analysis
- Alert prioritisation
- Security automation

**You will be able to**

- Explain how AI supports cyber defence
- Describe anomaly and phishing detection
- Explain security automation with AI

**Hands-on LMS labs — 6.25 hours**

- Use an AI feature to prioritise alerts
- Compare AI-assisted and manual detection

**Using AI in this module**

- The dedicated AI-in-defence module

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M40 AI-Assisted Threat Analysis 2 h lecture · 6.25 h labs

Phase 6 — Cloud, AI & Governance · Aligned to Cloud & AI security

**Aim** Use approved AI tools to summarise security information, organise investigation notes and support defensive analysis while maintaining privacy and verification requirements.

### What you will learn

- AI summarisation
- Investigation support
- Verification
- Privacy and data handling
- Responsible use

### You will be able to

- Summarise security information with AI
- Organise investigation notes
- Verify AI output and protect privacy

### Hands-on LMS labs — 6.25 hours

- Summarise an incident with AI and verify it
- Organise investigation notes with AI

### Using AI in this module

- Approved AI tools with human verification

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M41 AI Security and Responsible Use 2 h lecture · 6.25 h labs

Phase 6 — Cloud, AI & Governance · Aligned to Cloud & AI security

**Aim** Explore risks involving AI-generated content, prompt manipulation, data exposure, inaccurate outputs and unauthorised automation. Students learn responsible AI-governance principles.

### What you will learn

- AI-generated content risks
- Prompt injection
- Data exposure
- Inaccurate outputs
- AI governance
- OWASP Top 10 for LLM Applications

### You will be able to

- Identify AI-specific risks
- Mitigate prompt manipulation and data exposure
- Apply responsible AI governance

### Hands-on LMS labs — 6.25 hours

- Test and mitigate prompt injection on a lab chatbot
- Draft an AI-use policy

### Using AI in this module

- The dedicated AI-security module

Assessment: end-of-module MCQ assessment and LMS laboratory completion.

## M42 Cyber-Security Governance and Reporting 4 h lecture · 12.5 h labs

Phase 6 — Cloud, AI & Governance · Aligned to Cloud & AI security

**Aim** Understand policies, standards, risk registers, compliance awareness and professional reporting. Students prepare clear findings, business impact statements and remediation plans.

### What you will learn

- Policies and standards
- Risk registers
- Compliance awareness
- Professional reporting
- Business impact
- Personal Data Protection Act No. 9 of 2022

### You will be able to

- Explain security policies, standards and risk registers
- Apply compliance awareness
- Write professional reports and remediation plans

**Hands-on LMS labs — 12.5 hours**

- Write a professional findings report
- Prepare a remediation plan

**Using AI in this module**

- AI-assisted report drafting, verified by the learner

*Assessment: end-of-module MCQ assessment and LMS laboratory completion.*

