



NEXTGEN CAMPUS
TOWARDS THE NEXT GENERATION OF IT

STUDENT HANDBOOK

Diploma in Multi-Cloud & Cyber Security Engineering +Ai

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

12
MONTHS

1,240
LEARNING HOURS

14
MODULES

Blended
DELIVERY

INSIDE THIS HANDBOOK

- | | |
|--|---|
| 1 Welcome and course at a glance | 2 What you will learn and how |
| 3 Weekly timetable | 4 Course journey: weeks, months and course end |
| 5 Assessment, capstone and Project Book | 6 Student guidelines and support |
| 7 Module details — all 14 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 • www.nextgencampus.lk

Edition: October 2026 • Version 2026_NGC_FNL_V1.9

PART A General Information

1 Welcome to NextGen Campus

Welcome to the Diploma in Multi-Cloud & Cyber Security Engineering +Ai. 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

Course	Diploma in Multi-Cloud & Cyber Security Engineering +Ai
Duration	One year (50 teaching weeks) · 12 months
Delivery	Blended (online and on campus)
Class days and times	Saturday 1.30 – 5.30 PM — online lecture Sunday 9.00 AM – 5.00 PM — online lecture Saturday 6.30 – 10.30 PM — campus lab, Room A, once every 4 weeks Friday 9.00 AM – 1.00 PM — campus lab group session, Room B
Total learning hours	1,240 hours — 600 h lectures · 520 h practical (labs and capstone) · 120 h Student Project Book
Medium	English
Intakes	January–February and June–July each year
Course fee	Rs. 120,000.00 · Registration fee Rs. 3,000.00 (one-time)
On completion	NextGen Campus Diploma and Academic Transcript
Training institute	NextGen Campus (Pvt) Ltd — TVEC Registered Training Institute P01/1159
Course status	Proposed for TVEC course registration

3 About the Course

The Diploma in Multi-Cloud & Cyber Security Engineering +Ai is a one-year, 1,240-hour non-NVQ programme of 14 modules in five phases, anchored by a major enterprise-network capstone, progressing learners from IT Support Technician to AI-enabled Multi-Cloud & Security Engineer.

Purpose To train job-ready infrastructure, multi-cloud and cyber-security engineers who can build, run, secure and defend hybrid environments across on-premises, Microsoft Azure, Microsoft 365 and AWS, using AI-assisted tools responsibly. The diploma is anchored by a major capstone (45% of the final mark): the NextGen enterprise reference network, built and defended across the year.

Microsoft 365 currency (2026). MS-102 retires in October 2026; this diploma uses its current replacements — MD-102 (Endpoint Administrator) and AB-650 (Microsoft 365 and AI Services Administrator).

Job-level progression IT Support Technician (weeks 1–3) → Junior Network Engineer (3–8) → Systems Administrator (8–17) → Cloud Administrator (17–25) → Microsoft 365 / Endpoint Administrator (25–29) → Cloud Security Engineer (29–33) → Multi-Cloud Engineer (33–37) → Security Analyst / Ethical Hacker (37–45) → SOC Analyst (46–48) → AI-enabled Multi-Cloud & Security Engineer (48–50).

Phases Phase 1 Infrastructure & Network Foundations (M01–M05, weeks 1–17); Phase 2 Microsoft Cloud Engineering (M06–M09, weeks 17–33); Phase 3 Multi-Cloud with AWS (M10, weeks 33–37); Phase 4 Cyber-Security Engineering & Operations (M11–M13, weeks 37–48); Phase 5 AI for Engineers (M14, weeks 48–50).

4 What You Will Be Able to Do

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

- Support users, hardware and operating systems professionally.
- Design, configure and troubleshoot enterprise networks to CCNA level.
- Build virtualised Windows Server infrastructure, including migration.
- Administer Microsoft Azure (AZ-104), and Microsoft 365 and Windows endpoints with Intune and Copilot (MD-102 and AB-650).
- Engineer cloud security with Entra ID, Defender, Purview and Sentinel.
- Design and deploy resilient AWS solutions and map services across clouds.
- Perform authorised ethical security assessments and report findings.
- Operate defensive controls, SIEM, incident response and forensics.
- Apply AI tools, Copilot and agents responsibly in engineering and security.

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, or equivalent, plus basic computer literacy. No prior networking experience is required.

Who it is for school leavers, IT support staff, undergraduates, working professionals and career changers aiming for infrastructure, cloud or security roles.

What you need a laptop or computer with reliable internet for LMS labs (campus lab available by arrangement); signed ethical conduct agreement before security labs.

6 How You Will Learn

Learning activity	Hours	What it involves
Lectures	600 h	Live online lectures with your trainer (11 h a week)
Campus lab practicals	78 h	Hands-on sessions in the campus lab (Room A / Room B), on a rotating schedule
LMS module labs	402 h	Hands-on labs for every module on the NextGen LMS — about 8.1 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	120 h	Your professional record of lab work, reflections and the Management Module
Total	1,240 h	

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
Saturday	1.30 – 5.30 PM	Online	Online live lecture
Sunday	9.00 AM – 5.00 PM	Online	Online live lecture
Saturday	6.30 – 10.30 PM	Room A	Campus lab practical (your batch attends once every 4 weeks)

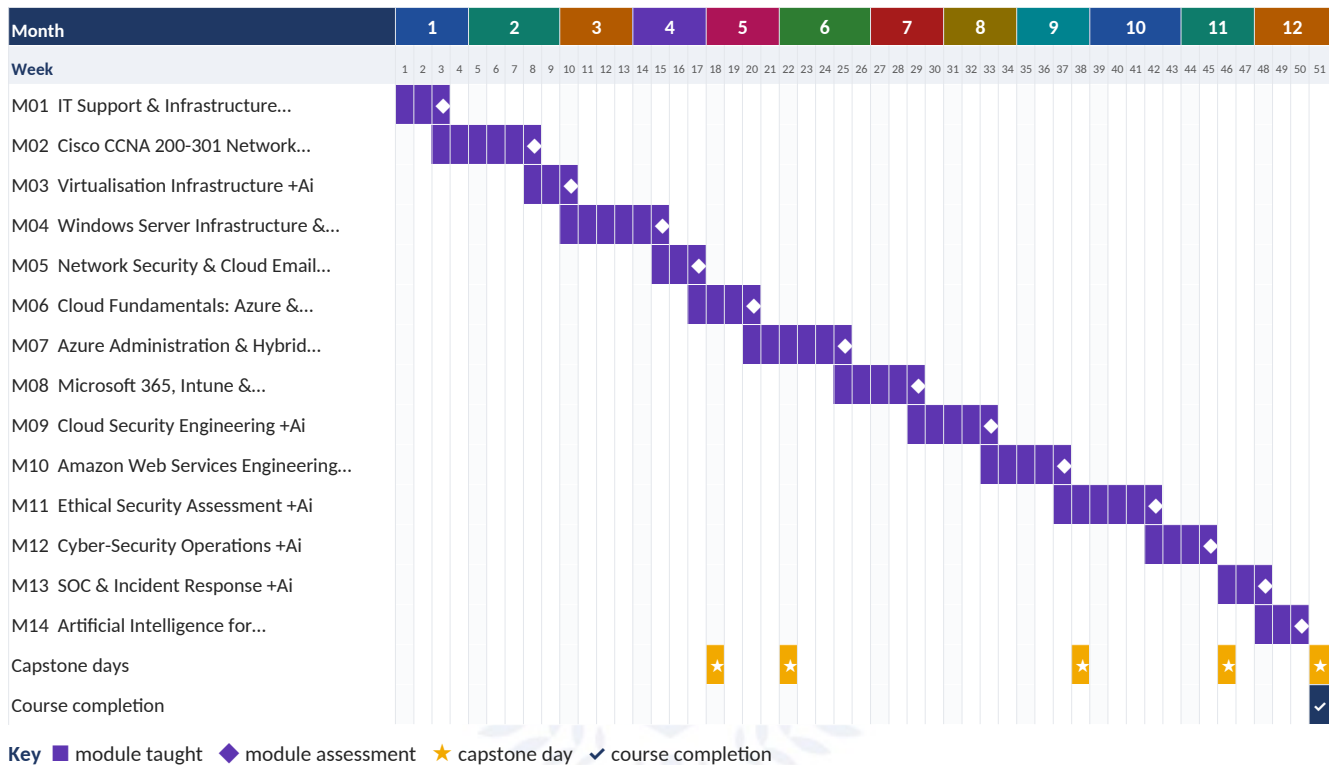
Days	Time	Where	Session
Friday	9.00 AM – 1.00 PM	Room B	Campus lab practical in groups of 20 (your group is notified in advance)

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 51 weeks over 12 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 IT Support & Infrastructure Operations +Ai M02 Cisco CCNA 200-301 Network Engineering +Ai	◆ Module assessment: M01
Month 2	Weeks 5–9	M02 Cisco CCNA 200-301 Network Engineering +Ai M03 Virtualisation Infrastructure +Ai	◆ Module assessment: M02
Month 3	Weeks 10–13	M03 Virtualisation Infrastructure +Ai M04 Windows Server Infrastructure & Migration +Ai	◆ Module assessment: M03
Month 4	Weeks 14–17	M04 Windows Server Infrastructure & Migration +Ai M05 Network Security & Cloud Email Security +Ai M06 Cloud Fundamentals: Azure & Microsoft 365 +Ai	◆ Module assessment: M04, M05
Month 5	Weeks 18–21	M06 Cloud Fundamentals: Azure & Microsoft 365 +Ai M07 Azure Administration & Hybrid Infrastructure +Ai	◆ Module assessment: M06 ★ Capstone day (week 18)
Month 6	Weeks 22–26	M07 Azure Administration & Hybrid Infrastructure +Ai M08 Microsoft 365, Intune & Endpoint Administration +Ai	◆ Module assessment: M07 ★ Capstone day (week 22)

Month	Weeks	What you study	Milestones
Month 7	Weeks 27–30	M08 Microsoft 365, Intune & Endpoint Administration +Ai M09 Cloud Security Engineering +Ai	◆ Module assessment: M08
Month 8	Weeks 31–34	M09 Cloud Security Engineering +Ai M10 Amazon Web Services Engineering +Ai	◆ Module assessment: M09
Month 9	Weeks 35–38	M10 Amazon Web Services Engineering +Ai M11 Ethical Security Assessment +Ai	◆ Module assessment: M10 ★ Capstone day (week 38)
Month 10	Weeks 39–43	M11 Ethical Security Assessment +Ai M12 Cyber-Security Operations +Ai	◆ Module assessment: M11
Month 11	Weeks 44–47	M12 Cyber-Security Operations +Ai M13 SOC & Incident Response +Ai	◆ Module assessment: M12 ★ Capstone day (week 46)
Month 12	Weeks 48–51	M13 SOC & Incident Response +Ai M14 Artificial Intelligence for Engineers	◆ Module assessment: M13, M14 ★ Capstone day (week 51) Week 51: Poya Day 5 — capstone ✓ Project Book submitted; course completion



A typical week

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
LMS labs ≈ 1.5 h	LMS labs ≈ 1.5 h	LMS labs ≈ 1.5 h	LMS labs ≈ 1.5 h	Campus lab 9.00 AM – 1.00 PM <i>when your batch is rostered</i> LMS labs ≈ 1.5 h	Online lecture 1.30 – 5.30 PM <i>online</i> Campus lab 6.30 – 10.30 PM <i>when your batch is rostered</i>	Online lecture 9.00 AM – 5.00 PM <i>online</i>
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 8.1 h a week in total; you can arrange them across the week to suit you.

How the course ends

1 Week 50	2 Week 51	3 End of course	4 After the course	5 Award
Final module M14 Artificial Intelligence for Engineers and the final module assessment	Capstone day Poya Day 5 — capstone	Project Book Submit your completed Student Project Book, including the Management Module	Results Marks are confirmed and your final grade is published: Distinction, Merit or Pass	Diploma NextGen Campus Diploma and Academic 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
Capstone final project	Enterprise network build with panel presentation and technical defence	45%	Across the year; panel on Poya Day 5
Continuous assessment	MCQ at the end of each module; weekly capstone build tasks	35%	End of each module; weekly
Student Project Book	Project book, including the Management Module and capstone build log	20%	Throughout; submitted at the end
Total		100%	

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

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

Capstone weighting The capstone is the largest single component (45%). It is not a one-off build: learners add to the enterprise network every week through capstone tasks recorded in the Project Book, so the final poya days consolidate and defend a system that has grown all year.

Formative practical checks The weekly practical checks are formative and recorded as LMS laboratory completion.

MCQ assessments Each end-of-module MCQ is completed under supervision on the LMS.

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 diploma

You must maintain a minimum attendance of 85%, complete all 14 module MCQs and the LMS laboratories, submit the Student Project Book (including the capstone build log), and build, present and defend the enterprise reference network, achieving an overall mark of at least 50%, to qualify for the diploma.

10 Capstone Project

The diploma is anchored by one major final project: the NextGen Campus enterprise reference network (Final Project V1.9). It has a Head Office (HO) site behind a proxy/firewall, a Disaster-Recovery (DR) site with a replica domain controller, and a Microsoft Azure site connected by a site-to-site VPN. The HO site runs the full server estate from the architecture diagram — domain controller (AD/DNS), additional domain controller, file server, SCCM, DHCP, WDS, WSUS, SQL database server, Exchange, a member domain controller, an endpoint-protection (COP/Virus Guard) server, a backup server, a VPN server, core and access switching and wireless. Learners build this environment progressively through the year, then defend it against a simulated external hacker in an attack-and-defend exercise. The 40-hour capstone is delivered over five physical poya days at the NextGen Campus Head Office, Nugegoda, each scheduled after the phase it builds on, with the panel defence on the final day. Weekly capstone tasks in the Project Book feed the build all year.

Day	When	Focus	Hours
Poya Day 1	After week 17	HO site network: core and access switching, VLANs, routing, wireless (AP_1), addressing and the proxy/firewall (DG-001); site documentation	8
Poya Day 2	After week 21	HO server estate: DC (AD/DNS), additional and member DCs, File, DHCP, WDS, WSUS and SCCM servers; SQL and Exchange; endpoint-protection and backup servers; DR site replica DC	8
Poya Day 3	After week 37	Azure site and hybrid link: Azure resources, site-to-site VPN from HO to Azure, Microsoft 365 and endpoint integration, and AWS components	8
Poya Day 4	After week 45	Security hardening and defence: firewall, VPN and endpoint hardening, Defender and Sentinel monitoring, and the external-hacker attack-and-defend exercise	8
Poya Day 5	After week 50	Business continuity: DR failover test and backup restore; full documentation and cost/DR plan; panel presentation and technical defence of the enterprise network	8
Total	40		

What you will deliver

- Enterprise architecture diagram and IP plan (HO, DR and Azure)
- Working HO network: switching, routing, VLANs, wireless and proxy/firewall
- Full HO server estate and a DR-site replica domain controller
- Azure site with a working site-to-site VPN, plus Microsoft 365, endpoint and AWS integration
- Security hardening across the estate and evidence from the external-hacker attack-and-defend exercise
- DR failover and backup-restore test results, cost/DR plan and full documentation
- Panel presentation and technical defence of the complete enterprise network

11 Student Project Book

The Student Project Book is a guided professional record developed throughout the year (about 2.4 hours a week). It documents laboratory work, design decisions and project outcomes, and contains the seven-unit Management Module.

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 Diploma — Diploma in Multi-Cloud & Cyber Security Engineering +Ai — 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 A+ / Network+ foundations; Cisco CCNA 200-301; VMware / AZ-800 (Hyper-V); AZ-800 / AZ-801 Windows Server Hybrid; CompTIA Security+; AZ-900 · Microsoft 365 fundamentals; AZ-104 Azure Administrator; MD-102 Endpoint Administrator · AB-650 M365 & AI Services; SC-900 · AZ-500 / SC-500 pathway; AWS CLF-C02 · SAA-C03; CEH · PenTest+; CompTIA Security+ / CySA+; CySA+ · SC-200; AB-900 · AI-901. 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

Head Office	NextGen Campus (Pvt) Ltd, Nugegoda, Sri Lanka
Phone	+94 11 251 5215 · +94 77 810 0810
Email	info@nextgencampus.lk
Website	www.nextgencampus.lk
LMS support	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.
Your course coordinator	Introduced at orientation — contact them about attendance, batches, re-sits and any personal circumstances.

PART B Module Details

The course has 14 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	IT Support & Infrastructure Operations +Ai	30	20	CompTIA A+ / Network+ foundations
M02	Cisco CCNA 200-301 Network Engineering +Ai	60	50	Cisco CCNA 200-301
M03	Virtualisation Infrastructure +Ai	20	15	VMware / AZ-800 (Hyper-V)
M04	Windows Server Infrastructure & Migration +Ai	60	50	AZ-800 / AZ-801 Windows Server Hybrid
M05	Network Security & Cloud Email Security +Ai	30	25	CompTIA Security+
M06	Cloud Fundamentals: Azure & Microsoft 365 +Ai	30	15	AZ-900 · Microsoft 365 fundamentals
M07	Azure Administration & Hybrid Infrastructure +Ai	60	50	AZ-104 Azure Administrator
M08	Microsoft 365, Intune & Endpoint Administration +Ai	50	40	MD-102 Endpoint Administrator · AB-650 M365 & AI Services
M09	Cloud Security Engineering +Ai	45	40	SC-900 · AZ-500 / SC-500 pathway
M10	Amazon Web Services Engineering +Ai	50	45	AWS CLF-C02 · SAA-C03
M11	Ethical Security Assessment +Ai	60	50	CEH · PenTest+
M12	Cyber-Security Operations +Ai	45	40	CompTIA Security+ / CySA+
M13	SOC & Incident Response +Ai	35	30	CySA+ · SC-200
M14	Artificial Intelligence for Engineers	25	10	AB-900 · AI-901
Total for modules		600	480	

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

M01 IT Support & Infrastructure Operations +Ai 30 h lecture · 20 h labs

Phase 1 — Infrastructure & Network Foundations · Aligned to CompTIA A+ / Network+ foundations

Aim Builds the IT-support and infrastructure foundation — hardware, operating systems, the service desk, and TCP/IP networking basics — that every later module builds on.

What you will learn

- Hardware and OS installation
- Troubleshooting and ticketing
- TCP/IP and IP addressing
- DNS and routing basics
- Professional communication

You will be able to

- Support hardware, operating systems and users professionally
- Explain TCP/IP, IP addressing and core services
- Work the service-desk ticket lifecycle

Hands-on LMS labs — 20 hours

- Build and troubleshoot a workstation
- Resolve service-desk tickets

Using AI in this module

- Copilot-assisted knowledge-base articles

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

M02 Cisco CCNA 200-301 Network Engineering +Ai 60 h lecture · 50 h labs

Phase 1 — Infrastructure & Network Foundations · Aligned to Cisco CCNA 200-301

Aim Delivers the full Cisco CCNA 200-301 pathway — addressing, switching, routing, security and automation — the networking core of the diploma.

What you will learn

- IPv4/IPv6 and subnetting
- VLANs, STP and EtherChannel
- OSPF and static routing
- NAT, DHCP and IP services
- ACLs, SSH and AAA
- Automation and REST APIs

You will be able to

- Configure VLANs, trunking and inter-VLAN routing
- Configure OSPF, NAT, DHCP and ACLs
- Secure and automate Cisco devices

Hands-on LMS labs — 50 hours

- Build multi-switch and multi-router networks
- Secure devices and validate with show commands

Using AI in this module

- AI review of Cisco configurations

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

M03 Virtualisation Infrastructure +Ai 20 h lecture · 15 h labs

Phase 1 — Infrastructure & Network Foundations · Aligned to VMware / AZ-800 (Hyper-V)

Aim Builds virtualisation skills on VMware and Hyper-V — the platform for the servers built later.

What you will learn

- Hypervisors
- VMware ESXi and vCenter
- Hyper-V
- Virtual switches and storage
- Snapshots and templates

You will be able to

- Deploy VMs on VMware ESXi and Hyper-V
- Configure virtual switches, datastores and snapshots
- Explain HA and live migration

Hands-on LMS labs — 15 hours

- Build a Hyper-V host
- Deploy VMs from templates

Using AI in this module

- AI-generated PowerShell for Hyper-V

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

M04 Windows Server Infrastructure & Migration +Ai 60 h lecture · 50 h labs

Phase 1 — Infrastructure & Network Foundations · Aligned to AZ-800 / AZ-801 Windows Server Hybrid

Aim Develops Windows Server infrastructure end to end — AD, DNS, DHCP, Group Policy, file, WSUS, WDS and RDS — plus a structured domain migration.

What you will learn

- AD DS, DNS, DHCP
- OUs and Group Policy
- File and print services
- WSUS and WDS
- Remote Desktop Services

You will be able to

- Deploy AD DS, DNS and DHCP with resilience
- Design OUs and Group Policy; configure file, WSUS, WDS and RDS
- Plan and execute a domain migration

- Domain migration and FSMO roles

Hands-on LMS labs — 50 hours

- Build a domain with an additional DC
- Deploy WSUS/WDS
- Migrate a domain to Windows Server 2025

Using AI in this module

- AI-generated PowerShell for AD

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

M05 Network Security & Cloud Email Security +Ai 30 h lecture · 25 h labs

Phase 1 — Infrastructure & Network Foundations · Aligned to CompTIA Security+

Aim Secures the network and email — firewalls, IDS/IPS, VPNs, and email security with SPF, DKIM and DMARC.

What you will learn

- Network-security principles and Zero Trust
- Firewalls and web proxy
- IDS/IPS
- VPNs and encryption
- Cloud email security

You will be able to

- Design firewall policy and deploy a VPN
- Configure IDS/IPS
- Secure email with SPF, DKIM and DMARC

Hands-on LMS labs — 25 hours

- Deploy a firewall, proxy and VPN
- Configure email authentication

Using AI in this module

- AI-assisted firewall rule review

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

M06 Cloud Fundamentals: Azure & Microsoft 365 +Ai 30 h lecture · 15 h labs

Phase 2 — Microsoft Cloud Engineering · Aligned to AZ-900 · Microsoft 365 fundamentals

Aim Introduces the Microsoft cloud — Azure fundamentals (AZ-900) and Microsoft 365 fundamentals — as the base for the cloud-engineering phase.

What you will learn

- Cloud concepts
- Azure architecture and services
- Cost and governance (AZ-900)
- Microsoft 365 services and licensing

You will be able to

- Describe Azure architecture, services and pricing
- Describe Microsoft 365 services and licensing
- Apply the shared responsibility model

Hands-on LMS labs — 15 hours

- Deploy first Azure resources
- Tour the Microsoft 365 admin center

Using AI in this module

- Copilot in Azure overview

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

M07 Azure Administration & Hybrid Infrastructure +Ai**60 h lecture · 50 h labs***Phase 2 — Microsoft Cloud Engineering · Aligned to AZ-104 Azure Administrator*

Aim Builds Azure administration and hybrid infrastructure (AZ-104) — identity, compute, storage, networking, monitoring and hybrid connectivity.

What you will learn

- Entra ID and RBAC
- VMs, App Service and storage
- Virtual networking and hybrid connectivity
- Monitoring and backup (AZ-104)

You will be able to

- Manage Entra identity, RBAC and governance
- Deploy compute, storage and virtual networks
- Connect on-premises to Azure; monitor and back up

Hands-on LMS labs — 50 hours

- Deploy a secured Azure environment
- Build a site-to-site VPN to Azure

Using AI in this module

- Copilot in Azure; AI-assisted KQL

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

M08 Microsoft 365, Intune & Endpoint Administration +Ai**50 h lecture · 40 h labs***Phase 2 — Microsoft Cloud Engineering · Aligned to MD-102 Endpoint Administrator · AB-650 M365 & AI Services*

Aim Administers the modern workplace — Windows endpoints with Intune and Autopilot (MD-102) and Microsoft 365 with Copilot and agents (AB-650).

What you will learn

- Endpoint enrolment, Autopilot, compliance and apps (MD-102)
- Microsoft 365 tenant, Exchange, SharePoint, Teams (AB-650)
- Purview protection
- Microsoft 365 Copilot readiness and agent governance
- Hybrid identity with Entra Connect

You will be able to

- Enrol and manage Windows endpoints with Intune and Autopilot (MD-102)
- Configure Microsoft 365 tenants, workloads and governance (AB-650)
- Enable and govern Microsoft 365 Copilot and agents

Hands-on LMS labs — 40 hours

- Autopilot-deploy and secure a device
- Configure a tenant and Copilot readiness
- Govern an agent

Using AI in this module

- Microsoft 365 Copilot administration; AI-assisted Intune troubleshooting

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

M09 Cloud Security Engineering +Ai**45 h lecture · 40 h labs***Phase 2 — Microsoft Cloud Engineering · Aligned to SC-900 · AZ-500 / SC-500 pathway*

Aim Engineers cloud security — identity protection, Defender for Cloud, Key Vault, Purview and Microsoft Sentinel.

What you will learn

- PIM and Conditional Access
- Defender for Cloud and secure score
- Key Vault and data security
- Microsoft Sentinel and KQL

You will be able to

- Secure identity with PIM and Conditional Access
- Raise posture with Defender for Cloud
- Detect and respond with Sentinel

Hands-on LMS labs — 40 hours

- Harden an Azure workload
- Build Sentinel detections

Using AI in this module

- AI-assisted KQL and incident summaries

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

M10 Amazon Web Services Engineering +Ai 50 h lecture · 45 h labs

Phase 3 — Multi-Cloud with AWS · Aligned to AWS CLF-C02 · SAA-C03

Aim Builds AWS engineering skills — IAM, VPC, EC2, storage, databases and resilient architecture — for true multi-cloud work.

What you will learn

- AWS global infrastructure
- IAM and VPC
- EC2 and storage
- RDS and resilient design
- Azure-AWS mapping

You will be able to

- Configure IAM, VPC and EC2
- Deploy S3, RDS, load balancing and auto scaling
- Map Azure services to AWS

Hands-on LMS labs — 45 hours

- Build a secure AWS VPC and workload
- Design a highly available architecture

Using AI in this module

- Amazon Q for configuration help

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

M11 Ethical Security Assessment +Ai 60 h lecture · 50 h labs

Phase 4 — Cyber-Security Engineering & Operations · Aligned to CEH · PenTest+

Aim Develops authorised ethical security assessment — reconnaissance, scanning, exploitation and web-application testing — inside an isolated lab.

What you will learn

- Ethics, law and scope
- OSINT and reconnaissance
- Scanning and enumeration
- Exploitation and web testing
- Reporting

You will be able to

- Plan an authorised assessment
- Scan, enumerate and assess vulnerabilities
- Exploit and report safely

Hands-on LMS labs — 50 hours

- Assess an isolated lab environment
- Write an assessment report

Using AI in this module

- AI-assisted vulnerability triage, verified

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

M12 Cyber-Security Operations +Ai 45 h lecture · 40 h labs

Phase 4 — Cyber-Security Engineering & Operations · Aligned to CompTIA Security+ / CySA+

Aim Builds defensive cyber-security operations — hardening, firewalls, IDS/IPS, web and endpoint security, and phishing and malware defence.

What you will learn**You will be able to**

- Traffic analysis
- Firewalls and IDS/IPS
- Hardening and IAM
- Web-application security
- Phishing and malware defence
- Harden systems and networks
- Operate IDS/IPS and firewalls
- Defend against phishing and malware

Hands-on LMS labs — 40 hours

- Tune IDS and harden a server
- Run a phishing simulation

Using AI in this module

- AI-assisted event correlation

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

M13 SOC & Incident Response +Ai 35 h lecture · 30 h labs

Phase 4 — Cyber-Security Engineering & Operations · Aligned to CySA+ · SC-200

Aim Builds SOC and incident-response skills — SIEM, log analysis, the incident lifecycle and digital forensics.

What you will learn

- SOC operations and SIEM
- Log analysis
- Incident response (NIST SP 800-61)
- Digital forensics

You will be able to

- Operate a SIEM and analyse logs
- Run the incident-response lifecycle
- Preserve and analyse evidence

Hands-on LMS labs — 30 hours

- Investigate a simulated incident
- Preserve and analyse evidence

Using AI in this module

- AI-assisted incident timelines

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

M14 Artificial Intelligence for Engineers 25 h lecture · 10 h labs

Phase 5 — AI for Engineers · Aligned to AB-900 · AI-901

Aim Applies AI across engineering and security — Microsoft 365 Copilot and agents, Azure AI, AI in cyber security, and responsible AI.

What you will learn

- AI for engineers
- Microsoft 365 Copilot and Copilot Studio (AB-900)
- Azure AI (AI-901)
- AI in cyber security
- Responsible AI and PDPA

You will be able to

- Administer Microsoft 365 Copilot and agents
- Build with Azure AI
- Use AI in security responsibly

Hands-on LMS labs — 10 hours

- Build a grounded AI assistant
- Use Security Copilot and verify output

Using AI in this module

- The dedicated AI module

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