



PROGRAM OVERVIEW

CYBER DEFENSE AND NETWORK SECURITY PROGRAM

CYBER DEFENSE AND NETWORK SECURITY PROGRAM



COURSE OVERVIEW

The Cyber Defense and Network Security Program provides structured training in modern cybersecurity principles, network protection strategies, and defensive security operations used in professional IT environments. The program focuses on how cyber threats impact real organizations, how secure network environments are designed, and how defensive security teams monitor, detect, and respond to potential risks.

LEARNING OUTCOMES

By completing this program, you will be able to:

- Explain core cybersecurity threat types and attack vectors
- Understand network security architecture and protection layers
- Identify common system and network vulnerabilities
- Apply basic defensive security monitoring principles
- Interpret security alerts and risk indicators

CAREER PATHWAYS

- IT Security Support
- Cybersecurity Operations Support
- Network Security Support
- Security Monitoring Support Roles
- Infrastructure Security Support

LEARNING APPROACH

We use a structured, mentor-guided learning model that combines theory, practice, and real project development. Classes focus on small group interaction, guided practice, and portfolio project creation.

STUDENT DELIVERABLES

- Cybersecurity scenario analysis exercises
- Network security case study tasks
- Security risk identification practice
- Basic security monitoring simulations
- Final cybersecurity scenario project

VISION

Whether participants are preparing for technology careers, upgrading professional skills, or entering cybersecurity for the first time, this program focuses on practical security knowledge applicable in real working environments.

WHAT YOUR JOURNEY WILL LOOK LIKE

BEGINNER LEVEL	CYB101 Cybersecurity Fundamentals Threat types, attack vectors, security principles, defense mindset	NET102 Network Fundamentals & Architecture OSI model, IP basics, routing concepts, network communication flow
	SYS103 Operating Systems & Access Security Basics User permissions, authentication basics, system security foundations	OPS104 Security Monitoring & Threat Awareness Logs, alerts, monitoring basics, recognizing abnormal activity
MIDDLE LEVEL	NET202 Network Security & Traffic Protection Firewalls, ACL concepts, segmentation, secure communication basics	SYS203 Server Security & Infrastructure Protection Windows/Linux security basics, service security, access hardening
	OPS204 Security Logging, Events & Risk Analysis Log analysis, event correlation basics, incident signals	CYB201 Applied Cyber Defense Tools & Practices IDS/IPS concepts, monitoring tools, vulnerability awareness
ADVANCED LEVEL	CYB301 Security Operations & Incident Response Fundamentals Incident workflow, detection → response → recovery lifecycle	NET302 Security Architecture & Defense Strategy Layered defense, zero trust concepts, infrastructure protection planning
	SYS303 Cloud & Modern Infrastructure Security Cloud risk basics, identity security, infrastructure exposure risks	OPS304 Cyber Defense Scenario Project Real case simulation, defense strategy planning, final presentation

WHERE YOU WILL BE AFTER EACH LEVEL

How This Program Improves Your Professional Value

After Level 1	After Level 2	After Level 3
Understand cyber threats and basic defense principles	Analyze security risks and monitoring data	Evaluate real security scenarios and defense strategies
Identify basic network security risks	Understand system and network protection methods	Support security monitoring and response workflows
Understand how organizations protect systems	Work with security tools and monitoring concepts	Contribute to security operations support environments

PROFESSIONAL CERTIFICATION

Certification is awarded based on successful completion of structured training modules, practical exercises, and final applied assessment tasks.

Certification confirms completion of cybersecurity and network defense training aligned with modern industry security concepts.

ARE YOU READY TO BECOME A DIGITAL SECURITY ARCHITECT?

Discover how hackers think, how systems are protected, and how to engineer secure technologies for the modern world.



CONTACT US

Business hours

Monday to Sunday 9.00am – 5.00pm

Counselling hours for course enquiries

Monday to Friday 9.00am – 5.00pm

Closed on public holidays.

Enquiries

T +60 19 627 0308

E kualalmp@nova-academy.io

Address

A2-6-3 Soho Suites KLCC,
20, Jalan Perak,
50450 Kuala Lumpur
Malaysia

SCAN HERE



SCAN HERE
TO REGISTER