MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

CERTIFIED CYBER SECURITY SPECIALIST

"Mastering Defensive Strategies, Threat Detection, and Cyber Risk Mitigation"

Schedule

Date	Venue	Fees (Face-to-Face)
21 – 25 Jun 2026	Doha, Qatar	USD 3495 per delegate

► **Available delivery methods:** Face-to-Face & Online Training, In-House Training

Introduction

As cyber threats escalate in scale, sophistication, and frequency, organizations require skilled professionals who can defend systems, detect attacks, and respond effectively to incidents. The Certified Cyber Security Specialist program is designed to provide a hands-on, practical foundation in cybersecurity, equipping participants with the skills needed to protect critical digital infrastructure.

The course covers core security principles, threat identification, network protection, incident response, and vulnerability management. Aligned with international frameworks (NIST, ISO 27001, CIS Controls), this training provides real-world simulations, attack/defense labs, and tool-based exercises to build a competent cyber defense posture.

Objectives

By the end of this course, participants will be able to:

- Understand the fundamentals of information and network security
- Identify and assess different types of cyber threats and attack vectors
- Apply security controls to protect data, applications, and endpoints
- Conduct basic vulnerability assessments and interpret scan results
- Respond to and recover from cyber incidents using structured frameworks

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Why Attend

- Strengthen your ability to identify and prevent cyberattacks
- Gain hands-on experience with cybersecurity tools and platforms
- Build a foundation for globally recognized certifications (CompTIA Security+, CEH, etc.)
- Understand how to implement layered defense strategies in real-world environments
- Support your organization\'s cybersecurity policies, risk posture, and compliance efforts

Target Audience

This program is designed for:

- IT and Network Administrators
- Cybersecurity Officers and Analysts
- System Engineers and SOC Personnel
- IT Audit, Risk, and Compliance Professionals
- Anyone pursuing a professional cybersecurity career

Individual Benefits

Key competencies that will be developed include:

- Threat detection, response, and containment
- Firewall, IDS/IPS, endpoint protection configuration
- Vulnerability and patch management fundamentals
- Incident response planning and coordination
- Use of tools such as Wireshark, Nessus, Metasploit, and SIEMs

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Improved cybersecurity posture and reduced breach risk
- Better alignment with regulatory and governance frameworks
- Stronger protection of critical infrastructure and customer data
- Faster detection and mitigation of security incidents
- A more skilled and capable in-house cybersecurity workforce

Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – Cyber threat landscape, standards, best practices
- Case Studies – Real-world breaches, ransomware attacks, and lessons learned
- Workshops – Network analysis, vulnerability scanning, phishing simulations
- Peer Exchange – Role-based scenarios and incident walkthroughs
- Tools – Wireshark, Nessus, Nmap, Metasploit, endpoint security solutions

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Course Outline

Training Hours: 7:30 AM – 3:30 PM Daily Format: 3–4 Learning Modules | Coffee breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: Cybersecurity Foundations and Threat Landscape

- Module 1: Principles of Information Security (07:30 – 09:30) • Confidentiality, integrity, availability, authentication
- Module 2: Cyber Threat Types and Actors (09:45 – 11:15) • Malware, phishing, DDoS, insiders, APTs
- Module 3: Understanding Cyber Kill Chain and Attack Lifecycle (11:30 – 01:00) • Reconnaissance, exploitation, persistence
- Module 4: Workshop – Threat Simulation Scenario (02:00 – 03:30) • Map attack stages using a recent case study

Day 2: Network Security and Access Control

- Module 5: Network Defense Mechanisms (07:30 – 09:30) • Firewalls, IDS/IPS, segmentation, VPNs
- Module 6: Access Control and Identity Management (09:45 – 11:15) • Authentication, authorization, least privilege
- Module 7: Secure Network Architecture (11:30 – 01:00) • DMZ, honeypots, zero-trust models
- Module 8: Workshop – Configure Firewall and ACLs (02:00 – 03:30) • Lab setup with rule creation and port blocking

Day 3: Endpoint Security and Vulnerability Management

- Module 9: Endpoint Threats and Mitigation (07:30 – 09:30) • Antivirus, patching, endpoint detection & response
- Module 10: Vulnerability Assessment Tools and Techniques (09:45 – 11:15) • Scanning with Nessus, OpenVAS
- Module 11: Patch and Configuration Management (11:30 – 01:00) • CVE prioritization, remediation process
- Module 12: Workshop – Run Vulnerability Scan and Analyze Results (02:00 – 03:30) • Live demo and result interpretation

Day 4: Incident Response and Security Operations

- Module 13: Introduction to Incident Response (07:30 – 09:30) • Preparation, detection, containment, recovery
- Module 14: Security Information and Event Management (SIEM) (09:45 – 11:15) • Log correlation, alert tuning, dashboards
- Module 15: Case Study – Breach Detection and Reporting (11:30 – 01:00) • Analyze breach response timeline
- Module 16: Workshop – Draft an Incident Response Playbook (02:00 – 03:30) • Team-based scenario response planning

Day 5: Cybersecurity Governance, Policy, and Final Simulation

- Module 17: Cybersecurity Frameworks and Compliance (07:30 – 09:30) • NIST, ISO 27001, GDPR, CIS Controls
- Module 18: Building a Security Policy and Awareness Program (09:45 – 11:15) • User behavior, phishing awareness, acceptable use
- Module 19: Final Simulation – Multi-Stage Cyber Attack Response (11:30 – 01:00) • Group incident simulation and reporting
- Module 20: Course Wrap-Up and Certification Review (02:00 – 03:30) • Review of key tools and techniques; feedback session

Certification

Participants will receive a Certificate of Completion as a Certified Cyber Security Specialist, validating their capabilities in safeguarding systems, detecting and responding to threats, and supporting cybersecurity resilience across organizational environments.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: **+601116373203**	EMAIL: **info@mawaevents.net**