@ASK Training
Attitude | Skills | Knowledge

up to 90% SkillsFuture Funding

Balance Fee SkillsFuture Credit & PSEA Claimable

Balance Fee SkillsFuture Enterprise Credit Claimable

(32 HRS)

CYBERSECURITY AND ETHICAL HACKING

Course **Synopsis**

This course equips participants with advanced knowledge and practical skills to identify, assess, and mitigate cybersecurity threats across organisational systems, networks, and applications. It focuses on vulnerability management, network security, endpoint protection, and application security to strengthen organisational defence capabilities.

Participants will apply **vulnerability assessment techniques**, **analyse threat intelligence**, and **implement remediation strategies** such as **patching**, **configuration hardening**, and **compensating controls**. The course also develops competencies in incident response, digital forensics, and security monitoring, enabling participants to detect and respond to cyber incidents effectively.

Participants will further analyse indicators of malicious activity across malware, network, and application attacks, and apply security governance, risk management, and compliance practices to support secure operations. Aligned with the **CompTIA Security+** syllabus, this course aims to prepare participants for the CompTIA Security+ certification examination and equips them with skills to perform cybersecurity and ethical hacking functions in enterprise environments.

Course Code: *TGS-2026064504*

Prerequisites

Completed the following courses awarded by @ASK Training:

- Cybersecurity Essentials

Language:

- Attained at least WPLN level 5 OR
- Obtained Grade C6 for GCE O level English OR
- Other equivalent qualifications

Academic:

- Obtained at least a pass or C6 at GCE O Level in at least 3 subjects OR
- Candidates with other qualifications will be considered on a case-by-case basis OR
- Mature candidates (⩾ 30 years old) with 8 years of relevant working experience

Total Training Hours:

- 32 hours, including a 2-hour assessment
- Written Assessment
- Practical Assessment

Learning **Units**

Learning Unit 1
Explain Vulnerability Management

Learning Unit 2
Evaluate Network Security Capabilities

Learning Unit 3
Assess Endpoint Security Capabilities

Learning Unit 4
Enhance Application Security Capabilities

Learning Unit 5
Explain Alerting and Monitoring Concepts

Learning Unit 6
Analyse Indicators of Malicious Activity

Learning Unit 7
Summarise Security Governance Concepts

Learning Unit 8
Explain Risk Management Processes

Learning Unit 9
Summarise Data Protection and Compliance Concepts

Course **Objectives**

By the end of this course, learners should be able to:

- Apply the CVE framework and vulnerability assessment tools.
- Differentiate false positives vs. false negatives in scan results.
- Conduct structured log reviews to detect anomalies and indicators of compromise.
- Select appropriate remediation strategies (patching, configuration, compensating controls).
- Configure and apply ACLs, IDS/IPS, and web filtering.
- Use detection methods to protect against unauthorized access and malicious activity and strengthen network infrastructure against web-based threats.
- Implement mobile device hardening (encryption, external media controls, location restrictions).
- Secure mobile connectivity (Wi Fi, Bluetooth, NFC, GPS, cellular, tethering, mobile payments).
- Apply endpoint security alignment with organizational requirements.
- Configure secure application protocols (TLS, secure directory services, SNMP, DNS filtering).
- Apply secure coding techniques and application protection mechanisms.
- Use sandboxing to reduce vulnerabilities and strengthen application resilience.
- Apply incident response procedures (preparation, detection, containment, eradication, recovery).

Course **Objectives**

By the end of this course, learners should be able to:

- Conduct digital forensics using appropriate data sources.
- Use SIEM, IDS/IPS, and log analysis to monitor and investigate incidents.
- Identify indicators of compromise across malware, physical, network, and application attacks.
- Correlate evidence to detect malicious activity and support investigations.
- Apply organisational governance requirements (policies, procedures, standards).
- Describe legal environment, accountability, and compliance frameworks.
- Apply secure, compliant, and accountable practices.
- Identify organisational risks and apply risk management strategies.
- Conduct business impact analysis to support continuity planning.
- Apply vendor assessment methods and review legal agreements.
- Validate security controls through attestation, assessments, and penetration testing.
- Apply data governance principles (classification, sovereignty, privacy, compliance).
- Implement data protection controls (monitoring, reporting, DLP, breach response).
- Deliver security awareness training programs to promote responsible workplace behaviour.

Programme **Fee**

S$1,200
(exclusive of 9% GST)

PROGRAMME FEE AFTER ELIGIBLE SSG SUBSIDIES:

From S$152.40

(inclusive of 9% GST) after 90% SSG Subsidies

Self-Sponsored	Course Fee before Subsidy and GST	Eligible Funding	Nett Fees Payable incl. 9% GST
Singapore Citizens ⩾ **40 years old**	S$1,200.00	90% SkillsFuture Funding	S$152.40
Singapore Citizens, PRs or LTVP+ Holders ⩾ **21 years old**		70% SkillsFuture Funding	S$392.40

SkillsFuture Credits can be used on top of existing subsidies

Company-Sponsored	Course Fee before Subsidy and GST	Eligible Funding	Nett Fees Payable incl. 9% GST
Small-to-Medium Enterprise (SME) Singaporean Citizens, PRs or LTVP+ Holders ⩾ 21 years old	S$1,200.00	90% SkillsFuture Funding	S$152.40
Non-SME Singaporean Citizens, PRs or LTVP+ Holders ⩾ 21 years old		70% SkillsFuture Funding	S$392.40
Non-SME Singaporean Citizens ⩾ 40 years old		90% SkillsFuture Funding	S$152.40

Singapore Citizens 21 years old and above who meet special criteria* may be eligible for Additional Course Fee Funding Support (AFS) of 95% Subsidy. AFS is only eligible for SkillsFuture Career Transition Programme applicants.

Contact Us

+ 65 64846723
+ 65 94303852
information@asktraining.com.sg
https://asktraining.com.sg/

Follow Us

@ask.training.sg
ASK Training
@ASK Training
@ask_training

Find Us

8 Jurong Town Hall Road
#27-01 The JTC Summit
Singapore 609434

10 Anson Road
#06-11 Inernational Plaza
Singapore 079903