Media Release
For Immediate Publication

Singapore Computer Society Launches Skills Pathway to Meet Demand for Cybersecurity Talents

SINGAPORE, 9 July 2024 - To bolster Singapore's cybersecurity talent pool, Singapore Computer Society (SCS) has launched a Skills Pathway for Cybersecurity in collaboration with founding employers, supported by the Cyber Security Agency of Singapore (CSA) and Association of Information Security Professionals (AiSP).

The initiative was developed by SCS in its role as a Skills Development Partner appointed by SkillsFuture Singapore. It was launched today by Minister for Education, Mr Chan Chun Sing, at the SkillsFuture Forum 2024. Minister of State for Education, Ms Gan Siow Huang, also witnessed the launch.

The Skills Pathway for Cybersecurity is wholly employer-centric and industry-led, as it was developed with the active involvement of 13 founding employers such as CSA, Ensign InfoSecurity, GovTech, NCS, ST Engineering and Synapxe. The full list of all 13 founding employers can be found in the Factsheet.

Supported by a dedicated advisory committee, this initiative offers guidance for individuals aspiring to enter the cybersecurity field, including mid-career individuals looking to transit into this dynamic sector. The initiative aims to foster the growth of skilled professionals in cybersecurity by providing industry-relevant training leading to industry-recognised certifications. It also offers opportunities for individuals to be considered for internships and job interviews.

Over the next year, the Skills Pathway for Cybersecurity will pave the way towards CSA's national initiative to develop a professional framework for the cybersecurity workforce, similar to those in more established fields like professional engineers and accountants. This framework, announced by Senior Minister of State for Digital Development and Information, Mr Tan Kiat How in October 2023, will raise the standards and recognition in the cybersecurity profession.

Ensuring Industry-Relevant Training And Industry-Recognised Certifications

The Skills Pathway for Cybersecurity offers opportunities for individuals to attain industry-recognised certifications that will enhance employability and boost career opportunities. The advisory committee, comprising founding employers, plays a pivotal role in ensuring the initiative's relevance and effectiveness. They guide the identification of essential skills and curation of courses and certifications to meet current industry demands.

The Skills Pathway for Cybersecurity initiative opens doors to promising career opportunities in cybersecurity, allowing individuals to significantly contribute to safeguarding Singapore's digital landscape. The initiative will prepare individuals for four entry-level cybersecurity job roles: Cyber SOC Analyst, Cyber Incident Response and Forensics Analyst, Cyber Threat Intelligence Analyst, and Cyber Penetration Tester. Individuals can choose from a list of employer-curated courses and certifications. While these are entry-level roles, the initiative offers opportunities to expand to other roles and career pathways in the cybersecurity field.

The full list of training courses and certifications can be found in the Factsheet.

SSG will support the Skills Pathway for Cybersecurity by enabling individuals to tap on available funding support from SSG to offset out-of-pocket fees for the certifications' training courses and examinations.

Empowering Singaporeans To Secure Quality Careers in Cybersecurity

SCS is an appointed Skills Development Partner by SSG, to strengthen the nexus between skills sets of individuals with the evolving needs of businesses.

President of Singapore Computer Society, Mr Sam Liew commented, "In today's digital world, cybersecurity is critical for all companies. This initiative demonstrates our commitment to building a strong cybersecurity workforce in Singapore. This employer-led initiative addresses the significant gap in the cybersecurity sector, ensuring training and certifications are aligned with industry needs. By providing the necessary tools and knowledge, we enable Singaporeans to secure quality jobs and enhance the nation's digital resilience."

Chief Executive of SkillsFuture Singapore, Mr Tan Kok Yam, commented, "When industry is clear about its skills needs, Singaporeans will have more confidence to pursue upskilling. We are pleased that SCS has pioneered the Skills Pathway for Cybersecurity, for employers to clearly signal their cybersecurity skills requirements to potential employees, including mid-careerists looking to level up their career options. We will work with our Skills Development Partners and other potential collaborators, to tailor similar solutions for their profession or industry sector."

For more information about the Skills Pathway for Cybersecurity, please visit skillspathway.scs.org.sg.

For media queries, please contact:

Shafeeqah Ahmad	Pek Ting Yu
HP: +65 9090 2798	HP: +65 9299 5867
shafeeqah@aprw.asia	tingyu@aprw.asia

About Singapore Computer Society

The SCS is the leading Infocomm and digital media society for industry professionals, leaders, students, and tech enthusiasts. Established in 1967, SCS has a thriving membership base of over 56,000 members today. Through 14 Chapters and five Special Interest Groups, SCS remains steadfast in its commitment to establishing a strong reputation as the voice of Singapore's Infocomm and digital media community. SCS strives to add value to its members' professional and personal development goals. From publications to training and development, networking opportunities and more, SCS supports its members by fuelling their ambition to connect, collaborate and be inspired with innovation and excellence.

For more information, please visit https://www.scs.org.sg/

MEDIA FACTSHEET

Overview

Singapore Computer Society (SCS) launched a Skills Pathway for Cybersecurity in collaboration with founding employers, supported by the Cyber Security Agency of Singapore (CSA) and Association of Information Security Professionals (AiSP). The initiative was developed by SCS in its role as a Skills Development Partner appointed by SkillsFuture Singapore.

The main objectives of Skills Pathway for Cybersecurity are to:

- Offer clear guidance for individuals aspiring to enter the cybersecurity field
- Foster the growth of skilled professionals in cybersecurity

Key Features

- Employer-centric and industry-led
- Industry-relevant training and industry-recognised certifications
- Structured pathways for internship and job interview opportunities
- Individuals can tap on available funding support from SSG to offset out-of-pocket fees for the certifications' training courses and examinations.

Founding Employers

1. Cyber Security Agency of Singapore (CSA)
2. Digital and Intelligence Service (DIS)
3. Defence Science and Technology Agency (DSTA)
4. Ensign InfoSecurity
5. GIC
6. Government Technology Agency (GovTech)
7. HTX (Home Team Science & Technology Agency)
8. NCS
9. Singapore Airlines
10. Singtel
11. ST Engineering
12. Synapxe
13. Temasek

Advisory Committee

The committee ensures the relevance and effectiveness of the initiative by identifying essential skill sets and ensuring the relevance of the certification.

Advisory Committee comprises the Cyber Security Agency of Singapore, SkillsFuture Singapore, Association of Information Security Professionals, and all 13 founding employers (list above).

More Details on Skills Pathway for Cybersecurity

The Skills Pathway for Cybersecurity is a skills development and recognition initiative that equips individuals with the skills and opportunities needed to enter

and advance in the cybersecurity field, starting with four entry-level job roles—Cyber SOC Analyst, Cyber Incident Response and Forensics Analyst, Cyber Threat Intelligence Analyst, and Cyber Penetration Tester.

Skills Pathway for Cybersecurity is structured into two levels:

- **Level 1: Apprentice**
  - Individuals will gain fundamental and essential knowledge necessary for entry into the cybersecurity sector.
  - By earning a Level 1 Certification, individuals may be considered for internship interview opportunities with key industry employers, with skills-first hiring considerations playing a significant role.
- **Level 2: Entry Level Job**
  - Individuals will hone their skills further, earning a Level 2 Certification and acquiring more than three months of relevant work experience.
  - Those who fulfill these requirements will be considered for interview opportunities for in-demand roles, ensuring a seamless transition into employment.
  - Employers will also assess candidates for their practical skills and experience as part of a skills-first hiring approach.

There is no need for individuals to complete Level 1 to progress to Level 2.

Employer-curated Courses and Certification Listing

Level 1		
Course	**Certification**	**Certifying body**
AiSP Qualified Information Security Associate (QISA)	AiSP Qualified Information Security Associate (QISA) Exam	AiSP
AWS Cloud Practitioner Essentials (AWS Certified Cloud Practitioner)	AWS Certified Cloud Practitioner Exam	AWS
CompTIA Security+ Training	CompTIA Security+ Exam	CompTIA
CREST Practitioner Intrusion Analyst (CPIA)	CREST Practitioner Intrusion Analyst (CPIA) Exam	CREST
CREST Practitioner Security Analyst (CPSA)	CREST Practitioner Security Analyst (CPSA) Exam	CREST
CREST Practitioner Threat Intelligence Analyst (CPTIA)	CREST Practitioner Threat Intelligence Analyst (CPTIA) Exam	CREST
EC-Council Certified Ethical Hacker (CEH)	EC-Council Certified Ethical Hacker (CEH) Exam EC-Council Certified Ethical Hacker (CEH) Practical Exam	EC-Council
ISA/IEC 62443 Cybersecurity Fundamentals Specialist	ISA/IEC 62443 Cybersecurity Fundamentals Specialist Exam	ISA/IEC62443
ISACA Cybersecurity Fundamentals Certificate	ISACA Cybersecurity Fundamentals Certificate Exam	ISACA
ISACA Cybersecurity Audit	ISACA Cybersecurity Audit Exam	ISACA

Level 1		
ISC2 Certified in Cybersecurity	ISC2 Certified in Cybersecurity (CC) Exam	ISC2
NUS-ISS Fundamentals of Cybersecurity	NUS-ISS Fundamentals of Cybersecurity Certificate	NUS-ISS
OffSec Network Penetration Testing Essentials (Pen100)	OffSec Network Penetration Testing Essentials (Pen100) Exam	OffSec
OffSec Security Operations Essentials (SOC100)	OffSec Security Operations Essentials (SOC100) Exam	OffSec
Intro to Cloud Computing and Security (SEC 388)	(No certification for this course)	SANS
Introduction to Cyber Security (SEC 301)	GIAC Information Security Fundamentals (GISF)	SANS
Security Essentials (SEC 401)	GIAC Security Essentials (GSEC)	SANS
Blue Team Fundamentals: Security Operations and Analysis (SEC 450)	GIAC Security Operations (SOC) Certification (GSOC)	SANS
Cloud Security Essentials (SEC 488)	GIAC Cloud Security Essentials Certification (GCLD)	SANS

Level 2		
Course	**Certification**	**Certifying body**
CREST Registered Intrusion Analyst (CRPIA)	CREST Registered Intrusion Analyst (CRPIA) Exam	CREST
CREST Registered Penetration Tester (CRT)	CREST Registered Penetration Tester (CRT) Exam	CREST
CREST Registered Threat Intelligence Analyst (CRTIA)	CREST Registered Threat Intelligence Analyst (CRTIA) Exam	CREST
Cybersecurity Development Programme (CSDP)	Cybersecurity Development Programme Certificate of Completion	CSA
Cyber Specialists Cadet Course (CSCC)	Cyber Specialists Cadet Course Certification of Completion	DIS
Certified in the Governance of Enterprise IT (CGEIT)	ISACA Certified in the Governance of Enterprise IT (CGEIT) Exam	ISACA
ISACA Certified Information Systems Auditor	ISACA Certified Information Systems Auditor (CISA) Exam	ISACA
ISACA Certified in Risk and Information Systems Control	ISACA Certified in Risk and Information Systems Control (CRISC) Exam	ISACA
ISC2 Certified Information Systems Security Professional	ISC2 Certified Information Systems Security Professional (CISSP) Exam	ISC2

Level 2		
OffSec Penetration Testing with Kali Linux (PEN200)	OffSec Certified Professional (OSCP) Exam	OffSec
OffSec Foundational Security Operations and Defensive Analysis (SOC200)	OffSec Foundational Security Operations and Defensive Analysis (OSDA) Exam	OffSec
Windows Forensic Analysis (FOR 500)	GIAC Certified Forensic Examiner (GCFE)	SANS
Network Monitoring and Threat Detection In-Depth (SEC 503)	GIAC Certified Intrusion Analyst Certification (GCIA)	SANS
Hacker Tools, Techniques, and Incident Handling(SEC 504)	GIAC Certified Incident Handler Certification (GCIH)	SANS
Advanced Incident Response, Threat Hunting, and Digital Forensics (FOR 508)	GIAC Certified Forensic Analyst (GCFA)	SANS
Enterprise Cloud Forensics and Incident Response (FOR 509)	GIAC Cloud Forensics Responder (GCFR)	SANS
Continuous Monitoring and Security Operations (SEC 511)	GIAC Continuous Monitoring Certification (GMON)	SANS
Cloud Security and DevSecOps Automation(SEC 540)	GIAC Cloud Security Automation (GCSA)	SANS
Cloud Security Monitoring and Threat Detection (SEC 541)	GIAC Cloud Threat Detection (GCTD)	SANS

Level 2		
Web App Penetration Testing and Ethical Hacking (SEC 542)	GIAC Web Application Penetration Tester (GWAPT)	SANS
Enterprise Penetration Testing (SEC 560)	GIAC Penetration Tester Certification | GPEN	SANS
Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR 572)	GIAC Network Forensic Analyst (GNFA)	SANS
iOS and Android Application Security Analysis and Penetration Testing (SEC 575)	GIAC Mobile Device Security Analyst (GMOB)	SANS
Cyber Threat Intelligence (FOR 578)	GIAC Cyber Threat Intelligence (GCTI)	SANS

The list of courses and certifications will progressively be added into SSG's MySkillsFuture website to allow individuals to search and apply for their preferred courses/certifications.