WHAT'S THE PROGRAMME ABOUT?

The Cloud is Powerful. The Threats Are Faster.

Cloud computing has transformed business—delivering speed, scale, and innovation. But this power comes with rising risks: ransomware, data breaches, and smarter cyberattacks exploiting cloud complexity. **AI and machine learning** are reshaping the defence landscape, while **quantum computing** threatens to disrupt today's encryption and security foundations.

This programme will take participants inside the **future of cloud security**—unpacking real risks, exploring how AI/ML can protect (and challenge) systems, and preparing for the quantum era. You'll leave with strategies to safeguard data, strengthen resilience, and lead with confidence in a constantly evolving threat environment.

Why Attend?

- Cloud threats are growing faster than traditional defences can manage
- AI, ML, and quantum technologies are rewriting the rules of cybersecurity
- Boards, regulators, and executives face increasing pressure to ensure resilience
- This programme gives you the frameworks, foresight, and strategies to act now

What You'll Gain

By joining this half-day programme, you will:

- Gain **clarity on today's top cloud risks** and how to mitigate them
- Learn how **AI and ML strengthen security**—and where they introduce new vulnerabilities
- Understand the **quantum threat** and what it means for cloud data and encryption
- Build an **actionable roadmap** for resilience—covering strategy, governance, and team readiness

ICF COMPETENCY LEVEL

- Core – Risk Management (Proficiency Level 3)
- Functional (Technical) - Digital Technology Application (Proficiency Level 3)
- Functional (Process) - Compliance (Proficiency Level 3)

TARGET AUDIENCE

Individuals

Cyber Security Officers, Cyber Security Analysts, Cyber Crime Investigators, Information System Officers, Network Engineers, Digital and Innovation Officers, System Analysts, Professional Hackers, Compliance Officers, Legal Officers, Internal Auditors

Organisations

Capital Market Intermediaries, Public Listed Companies (PLCs), Government-Linked Investment Companies (GLICSs), Cybersecurity Firms, Technology Companies, Regulatory and Supervisory Bodies who are keen to learn on cybersecurity and data privacy.

PROGRAMME OUTLINE

9.00 am — Cloud Computing and Cybersecurity Today

- Overview of cloud service models (IaaS, PaaS, SaaS)
- Cloud fundamentals & why securities matters
- Attack vectors and vulnerabilities relevant to business organisations e.g.: Capital Market Intermediaries, Public Listed Companies
- Top cloud risks and how would companies address them

Session Summary: Cloud Computing and Cybersecurity Today
Gain a clear understanding of cloud service models and why security is critical. Explore common attack vectors and vulnerabilities affecting industries like Capital Market Intermediaries and Public Listed Companies, and examine the top cloud risks with practical strategies to address them.

10.00 am — Cybersecurity Innovations in Cloud Era

- Evolution of cybersecurity challenges in the cloud era
- The role of AI and ML in managing cloud security
- Ensuring governance and compliance in cloud security
- Case study analysis of major cloud security breaches and key takeaways

Session Summary: Cybersecurity Innovations in the Cloud Era
Explore how cybersecurity challenges have evolved with the rise of cloud adoption. Learn how AI and ML are reshaping cloud security, the importance of governance and compliance, and uncover key lessons from major cloud security breaches.

11.00 am — Break

11.15 am — Quantum Computing: The Next Frontier in Cloud Security

- Understanding the quantum threat
- Impact of quantum computing on encryption: Are we safe?
- Implication for cloud and data
- Preparing for the quantum era

Session Summary: Quantum Computing – The Next Frontier in Cloud Security
Understand the emerging quantum threat and its impact on encryption. Explore implications for cloud data and learn strategies to prepare your organisation for the quantum era.

12.15pm — Building Resilient Cloud Security Strategies for the Future

- Applying cloud security strategy through principles of zero trust in cloud setups
- Adopting advanced cloud infrastructure, protocols, and intelligent security technologies for comprehensive cloud protection
- Challenges in upskilling teams to safeguard the people, clients and data
- The role of the board, senior management in overseeing cloud risk and aligning with security strategies

Session Summary: Building Resilient Cloud Security Strategies for the Future
Learn how to apply zero-trust principles and advanced security technologies to protect cloud environments. Explore challenges in upskilling teams, safeguarding people and data, and the role of leadership in aligning cloud risk with organisational strategy.

1.15 pm — End of Programme

Visit **www.sidc.com.my** for More SIDC Training Programmes **TODAY !**

SIDC
www.sidc.com.my

Securities Industry Development Corporation (765264K)
3, Persiaran Bukit Kiara, Bukit Kiara, 50490 Kuala Lumpur, Malaysia
Email: sidc@sidc.com.my Website: www.sidc.com.my

Find us on Youtube, Linkedin, Facebook & Instagram at Securities Industry Development Corporation - SIDC

** The SIDC reserves the right to amend the programme as deemed appropriate as without prior notice.*

For enquiries on registration, please contact: **+603 6204 8439 / 8274** | Register today at **www.sidc.com.my**

Get in touch and speak to our friendly team:

Farith Jamal | +6014 653 2578 | Farith.Jamal@sidc.com.my
Abdul Qaiyum | +6017 871 3242 | Qaiyum.Ghazali@sidc.com.my
Sarah Dalina | +6011 2711 9658 | Sarah.Dalina@sidc.com.my
Syed Imran | +6017 743 0773 | imran.nasir@sidc.com.my
Wan Mohd Farid | +6012 641 7589 | FaridK@sidc.com.my