Overview

The world is interconnected more than ever resulting in a larger attack surface across organisations. This is further exacerbated by increasingly sophisticated cyber threats and attacks.

At present, many organisations still face a lack of skilled and competent cybersecurity practitioners to help keep their cyberspace secure. Furthermore, while most organisations have incident response plans, they have not been subjected to stress testing as these organisations have yet to experience actual cyber breaches.

This means that most organisations suffer from a lapse in cyber operational-readiness and are insufficiently prepared to respond to a cyber-breach.

We offer learners exposure to practical hands-on cyber attacks that increase higher knowledge retention rate compared to traditional theoretical table-top exercises. Learners will be taught to defend against weaponised malware in a virtual environment which experimentation of different methods and solutions without compromising live production environments. Learners will also learn stress test incident response SOPs and Playbooks. For the training, we offer up to 30 IT and OT attack scenarios. Customisation of scenarios are also available upon request.
Learning Outcomes

Gain exposure to practical hands-on cyber attacks that facilitate higher knowledge retention rates compared to traditional theoretical table-top exercises.

Defend against weaponised malware in a virtualised environment that allows different methods and solutions to be tested without compromising live production environments.

Stress test Incident Response SOPs and/or Playbooks in time-critical attack scenarios to reveal gaps for remedial tactical action.

Course Structure

Day 1
- Familiarisation of cyber range tools and network
- Threat landscape sharing and discussion
- Cyber Attack Scenario 1
- Debrief

Day 2
- Cyber Attack Scenario 2
- Post Scenario Debrief
- Cyber Attack Scenario 3
- Post Scenario Debrief
- Hacking method and techniques demo

Day 3
- Cyber Attack Scenario 4
- Post Scenario Debrief
- Exercise learnings and outcome round table discussion
- Overall debrief and certificate presentation

Course Fee
Please contact us for details

Contact Us
Email: cyber.academy@stengg.com
Tel: +(65) 6513 9535

Training Venue
80 Jurong East Street 21 #04-02
Devan Nair Institute
Singapore 609607

Terms and Conditions
1. Prices are subjected to Government Service Tax (GST).
2. Course fee is inclusive of refreshments.
3. ST Electronics (Info-Security) Pte Ltd reserves the right to make amendments to the course agenda and dates without prior notice.