CYBERSECURITY
OPERATIONS SPECIALIST

Course Duration: 5 days
Time: 9am – 5.30pm

Overview

The current cyber threat landscape is in a state where knowledge is important but no longer sufficient. Cybersecurity Operations Specialist equips you and your team with the essential skillsets and competency to keep an organisation secure. In addition to the imparting of knowledge, it focuses on the cognitive and analytical abilities of learners. It also equips learners with cyber defence operational skillsets. In this course, you will learn to build up your foundation through the understanding of cybersecurity concepts, familiarise with functionality of various security products and enhance your operational proficiency through simulated cyber-attacks in a controlled environment. This is a course developed for practitioners by practitioners.

ST Engineering

Learning Outcomes

Appreciate the entire kill-chain of various cyber-attacks

Develop improved response to cyber attacks

Enhance decision-making and teamwork in the event of cyber-attacks

Course Structure

Day 1

Cybersecurity Imperatives

- Cyber threats, trends, terms and terminologies
- CIA, AAA, standards, audit, compliance and regulations
- Cryptography and applications

Network Technologies and Security

- Introduction to network systems, types and devices
- Secure network protocol (SSL/TLS, SSH)
- Introduction to network security devices (Firewall, IPS/IDS, SIEM, etc.)

Server Systems and Logs

- Types and functions of servers (web, database, mail, AD, etc.)
- OS, servers and their event logs (Windows, Linux, IIS, Apache, Mssql, sendmail etc.)

Day 2

Attack Methodology and Types

- Attack phases
- Types of vulnerabilities and attacks
- Web-based attack

Security Operations Centre and Incident Response

- Different types of information security incident
- Information security incident management framework
- Overview to SOC concepts and operations
- Threat identification, threat correlation, threat aggregation, threat filtering
- Incident handling, response management, notification and reporting

Security Products and Hands-On

- Checkpoint Firewall, Security Information and Event Management(SIEM)
- Monitoring tools such as Wireshark, Process Monitor

Cyber-Attack Scenario-based Exercises

- Exposure to real-world cyber-attack scenarios
- Developing detection, and response skills through team-based exercises

Assessment

Assessment	Incident Report	Practical Performance	Written Test
Description	Assess learners on their mastery of the Performance Statement and Underpinning Knowledge	Assess learners on their understanding of the competencies	Assess learners on their mastery and understanding of the Performance Statements, Underpinning Knowledge and competencies
Format	Written Exam	Labs	Written Exam
Duration	30 mins	180 mins	60 mins

Who should attend?

- Cyber Security Professionals
- IT Professionals / Engineers
- System / Network Administrators
- Information Security Managers and Executives
- Project Managers, Risk Managers and Compliance Managers

Training Venue

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

Contact Us

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

Terms and Conditions

1. Assessment fee is inclusive as part of the course fee for the first time. Re-assessment fee and booking fee applies for participants who did not pass during the course.

2. ST Electronics (Info-Security) Pte Ltd reserves the right to make amendments to the course agenda and dates without prior notice.

3. ST Electronics (Info-Security) Pte Ltd reserves the right to change the date or venue without prior notice.

4. ST Electronics (Info-Security) Pte Ltd reserves the right to cancel or reschedule the course due to class size or unforeseen circumstances.

ST Engineering Electronics Ltd.
www.stengg.com
mktg.infosec@stengg.com

DOP 0420