Cybersecurity Nexus Fundamentals Training

ISACA Malaysia Chapter

Workshop Overview

Cybersecurity is a growing and rapidly changing field, and it is crucial that the central concepts that frame and define this increasingly pervasive field are understood by professionals who are involved and concerned with the security implications of Information Technologies. The CSX Fundamentals training is designed for this purpose, as well as to provide insight into the importance of cybersecurity and the integral role of cybersecurity professionals.

This training event will also prepare participants for the CSX Fundamentals (CSXF) Examination by ISACA. *Note: The CSXF exam, which is an online computer based examination, is not included in this training and must be registered separately with ISACA International.*

Who Should Attend

This programme is designed for people who is looking to gain hands on skillset in cybersecurity and to begin building their skillset and knowledge in this crucial area. You may be a fresh graduate or an experienced professional in any fields – from new assurance / security / risk / compliance professionals to experienced Management personnel who needs to understand and/or deal with this new emerging risk area.

What You Will Learn

- ✓ Understand basic cybersecurity concepts and definitions
- ✓ Identify cybersecurity roles
- ✓ Understand basic security architecture principles
- ✓ Understand malware analysis concepts
- ✓ Recognise the techniques for detecting host-and-network-based intrusions via intrusion detection technologies
- ✓ Understand vulnerability assessment management
- ✓ Recognise penetration testing phases
- ✓ Understand high level network security, including remote access technology and systems administration concepts
- ✓ Understand system hardening and virtualisation
- ✓ Recognise system lifecycle management principles
- ✓ Understand / Review the OWASP top ten
- ✓ Differentiate between events and incidents
- ✓ Define types of incidents and identify elements of an incident response plan
- ✓ Be aware of the basic procedures for processing digital forensic data
- ✓ Recognise new and emerging information technology and identify the associated security implications

14 CPE hours

Your Trainer

Alan Yau Ti Dun

Alan is currently holding a senior role as Chief Technical Officer at a Cybersecurity Consultancy and Security Operation Center organisation and has over 15 years of experience in Information Security, Governance and Controls. He has extensive experience in leading engagements and serving clients in the area of Information Security.

This includes Next Generation Security Operation Center, Information Technology Cybersecurity Infrastructure Review, Penetration Testing, IT Audit, ISO27001 Implementation, ISO27001:2013 Transition, Swift Assessment Review, Security Incident Management and Response, Managed Security Services, Business Continuity Planning, Secure Email and other areas.

Throughout his career Alan has supplemented his hands on experience through extensive cybersecurity research. This has played a significant role in helping him develop training material and conference talks. He is a regular speaker at conferences with topics ranging from technical to governance.

He is also CSXF Trainer, PECB Certified Trainer and Certified Mile2 Instructor and have conducted specific training sessions which include Mile2 Certified Training, ISACA Boot Camp, Cybersecurity Fundamental Training and Security Awareness Training.

Qualifications / Professional Affiliations

- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)
- Certified in Governance of Enterprise IT (CGEIT)
- Certified In Risk Information System Control (CRISC)
- Certified Information Systems Security Professional (CISSP)
- PECB Certified ISO/IEC 27001 Lead Auditor
- PECB Certified ISO/IEC 27001 Lead Implementer
- PECB Certified ISO/IEC 27005 Lead Risk Manager
- PECB Certified ISO/IEC 38500 Lead IT Corporate Governance
- Certified Penetration Testing Consultant (CPTC)
- Certified Penetration Testing Engineer (CPTE)
- Certified Digital Forensic Examiner (CDFE)
- Certified Network Forensic Examiner (CNFE)
- Certified Incident Handling Engineer (CIHE)
- Certified Information System Security Officer (CISSO)
- Cybersecurity Nexus Fundamentals Certificate (CSXF)
- Certificate of Cloud Security Knowledge (CCSK)
- Ethical Network Security Administrator (ENSA)
- COBIT 5 Foundation
- ITIL Foundation V3
- ISACA Malaysia Chapter
  - ❑ Director 2015/16, 2016/17 , 2017/18, 2018/19
  - ❑ CSX Liaison Officer

Cybersecurity Nexus Fundamentals Training - Programme

Day One

9:00 AM : Session 1

- ❑ Cybersecurity Nexus Program Introduction
- ❑ Cybersecurity Trend
- ❑ Cybersecurity In Malaysia

10:30 AM : Morning Break

11:00 AM : Session 2 Cybersecurity Overview

Topic 1-Introduction to Cybersecurity
Topic 2-Difference Between Information Security and Cybersecurity
Topic 3-Cybersecurity Objectives
Topic 4-Cybersecurity Roles
Topic 5-Cybersecurity Domains

11:30 AM : Session 3 Cybersecurity Concepts

Topic 1-Risk
Topic 2-Common Attack Types & Vectors
Topic 3-Policies & Procedures
Topic 4-Cybersecurity Controls

12:30 PM : Lunch

2:00 PM : Session 4 Security Architecture

Topic 1-Overview of Security Architecture
Topic 2-The OSI Model
Topic 3-Defense in Depth
Topic 4-Firewalls, IDS/IPS, Web Application / Database Firewall

3:30 PM : Afternoon Break

4:00 PM : Session 4 Security Architecture Principle Continue….

Topic 5-Isolation and Segmentation
Topic 6-Monitoring, Detection and Logging
Topic 7-Encryption Fundamentals

5:00 PM : Day 1 Session Wrap Up

Day Two

9:00 AM : Session 5 Security Of Network, System, Apps and Data

Topic 1-Process Controls-Risk Assessments
Topic 2-Process Controls-Vulnerability Management
Topic 3-Process Controls-Penetration Testing
Topic 4-Network Security
Topic 5-0perating System Security
Topic 6-Application Security
Topic 7-Data Security

10:30 AM : Morning Break

11:00 AM : Session 6 Incident Response

Topic 1-Event vs. Incident
Topic 2-Security Incident Response
Topic 3-Investigations, Legal Holds and Preservation
Topic 4-Forensics
Topic 5-Disaster Recovery and Business Continuity Plans

12:30 PM : Lunch

2:00 PM : Session 7 Security Implications & Adoption Of Evolving Technology

Topic 1-Current Threat Landscape
Topic 2-Advanced Persistent Threats
Topic 3-Mobile Technology-Vulnerabilities, Threats and Risk
Topic 4 Consumerization Of IT & Mobile Devices
Topic 5-Cloud & Digital Collaboration

3:30 PM : Afternoon Break

4:00 PM : Session 8 Regulation In Malaysia

Topic 1-Cybersecurity Risk Circular (BNM)
Topic 2-Industry Communication To Enhance Cybersecurity Measures (Bursa)
Topic 3-NIST

5:00 PM : Programme Wrap Up

Details and Registrations

Event: **Cybersecurity Nexus Fundamentals Training**

Date: 27 – 28 August 2018

Venue: Info Trek Sdn Bhd
Unit-350, 3rd Floor, AmCorp Mall, 18 Persiaran Barat,
Petaling Jaya, Selangor Darul Ehsan, 46050
http://www.info-trek.com/

Fees: RM 1,880 for ISACA members

RM 2,480 for non members

Contact: Mr Seelan, ISACA Office Administrator

Mobile: 017 219 6225 | Email: officeadmin@isaca.org.my

Important Notice

As good practice, ISACA Malaysia Chapter is informing you that your personal data will be processed, retained and used by ISACA Malaysia Chapter in relation to this training event. Your personal data may also be retained and used by ISACA Malaysia Chapter to market and promote training events conducted by ISACA Malaysia Chapter.

Note: This is an editable PDF.

Participant Name	Designation	Membership No	Email

Organisation & Contact Details			
Organisation Name			
Address			
Contact Person			
Telephone		Department	
Fax		Email	

Reservations & Registrations:

Places are LIMITED. Please register as early as possible. Registration will only be confirmed upon receipt of registration form, followed by payment, if applicable. If payment is applicable, upon receipt of the registration, the fee will be a debt due to ISACA Malaysia Chapter.

ISACA Malaysia Chapter reserves the right to change the venue, date, speakers, and programme or to cancel the programme should unavoidable circumstances arise. If applicable, a full refund of fees will be made in the event of cancellation.

Payment Details:

Fees are not refundable once registration is confirmed, however, replacements may be sent. Cheques should be made payable to “Information Systems Audit And Control Association” and mailed to: ISACA Malaysia Chapter, Unit 916, 9th Floor, Block A, Damansara Intan, No.1, Jalan SS 20/27, 47400 Petaling Jaya, Selangor.

Alternatively, payment can be banked into: Maybank Account number – 512231822725. Bank in slip or Internet Banking confirmation MUST be faxed to 03-7726 1257 or emailed to officeadmin@isaca.org.my, with a cover note stating Event Name, Organisation / Participant(s) Name and Amount Banked In. Payment will not be recognised without this cover note.