

<b>Course Name:</b>	Protecting your Corporate Network
<b>Duration:</b>	2 Day
<b>Medium of Instruction:</b>	Cantonese (terminology & handout in English)
<b>Award of Certificate:</b>	Certificate of Attendance

### **Nature and Objectives:**

Your corporate network infrastructure may be one of the most important asset / facility that support your business operations, and hence proper protection of it become necessary for your business survival. A network connecting different computers, components and other networks is however a breeding ground for vulnerabilities. Without a proper strategy, it is difficult to protect your corporate network effectively. The 2-day intensive hands-on workshop aims to equip participants with a strategic approach to protect your corporate network.

### **Who Should Attend:**

System and Network Administrators / Engineers / Analysts, Technical Engineers / Managers, Data Security Officers, Information Security Analysts / Managers, IT Auditors and Managers, Network Managers, Security Consultants and System Integrators.

### **Course Outline:**

#### **Fundamental**

- Network Attacks and Countermeasures
- Network Security Policy and Strategies
- Secure Network Architecture Design Principles and Approach

#### **Part A – Secure your Network Perimeter**

- First Line of Defense - Perimeter router
- Configuring the Perimeter Router
- Firewalls and Intrusion Prevention Systems
- The Firewall Environment
  - Features, Models, Components & Benefits
  - Open Source firewalls
  - Firewall Configuration
  - Securing Public Services in the DMZ
  - Logging in the Firewall Environment
- Configuring the Web Proxy Server

#### **Part B - Intrusion Detection**

- Complementary the Intrusion Detection Systems and Firewall
- Network based and Host bases Intrusion Detection technologies
- Install and configure SNORT IDS Sensor
- Optimal the IDS signatures in network environments
- IDS signatures and determine the immediate threat posed to the network
- Customized intrusion detection signatures
- Reduce alarms and possible false positives

#### **Part C – Strengthen your Internal Networks / Systems**

- Switches and Choke Router/Internal Firewalls
- Email security – Anti-Spam, Anti-Virus
- Telnet, SMTP, and POP3 vulnerabilities
- OS Hardening

#### **Part D - Remote Access Controls**

- Secure Remote Access
- VPN Services - IPSec and SSL VPN