Network & Internet Security for IT Professionals.

หลักการและเหตุผล :

การรักษาความปลอดภัยในระบบคอมพิวเตอร์นับวันจะยิ่งมีความสำคัญมากยิ่งขึ้น ทั้งในองค์กรภาครัฐและเอกชน เรื่องของ Security หรือระบบความปลอดภัยในระบบเครือข่ายยังเป็นเรื่องใหม่สำหรับประเทศไทย จึงมีความจำเป็นอย่างสูงที่ต้องทำให้บุคคลากรด้านคอมพิวเตอร์ของเราได้มีความรู้ความสามารถเท่าทันบรรดา Hacker หรือไวรัสใหม่ๆที่มากันอย่างต่อเนื่อง เมื่อเรามีความเข้าใจด้าน Computer Security ดีพอ เราจึงจะสามารถดูแลระบบและป้องกันเครือข่ายคอมพิวเตอร์ ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

วัตถุประสงค์ :

- เพื่อให้ผู้เข้ารับการอบรมมีความเข้าใจพื้นฐานด้าน Systems & Network Security อย่างลึกซึ้ง
- เพื่อให้สามารถมีความรู้เท่าทันการโจมตีของ Hacker และ Cracker
- เพื่อให้เข้าใจหลักการ CIA TRIAD (Confidentiality, Integrity, Availability) รวมทั้ง Accountability
- เพื่อศึกษากฎหมายพื้นฐานด้านไอที
- เพื่อให้สามารถป้องกันระบบของหน่วยงาน ที่ผู้เข้าอบรมรับผิดชอบอยู่อย่างมีประสิทธิภาพ
- ศึกษาและเข้าใจ Information Security Process, Internet Architecture, VPN, E-Commerce security, Encryption, Intrusion Detection.
- ศึกษาและเข้าใจการรักษาความปลอดภัยของระบบปฏิบัติการ Unix, Windows NT

หลักสูตรนี้เหมาะสำหรับ :

- System Engineer, System Administration
- ผู้บริหารระบบเครือข่าย เช่น EDP Manager, MIS Manager
- ช่างเทคนิคระดับสูง
- ผู้สนใจด้าน Computer Security ทั่วไป

คุณสมบัติผู้เข้าอบรม :

- สามารถใช้งาน Microsoft Windows ได้เป็นอย่างดี
- มีความรู้ และประสบการณ์เกี่ยวกับระบบเครือข่ายคอมพิวเตอร์
- ผ่านงานด้าน IT มาไม่ต่ำกว่า 3 ปี
- เคยใช้งาน และดูแลระบบปฏิบัติการ Windows Server และ Linux

หลักสูตรต่อเนื่อง/เกี่ยวเนื่อง :

- Fundamentals Wireless LAN Security
- Implementing Wireless LAN Technology

เนื้อหาหลักสูตร :

- Top Ten information security paradigm
- Information security Management Framework
- Information security awareness guide
- Information security web resources
- What Is Information Security?
  - Defining Information Security
  - Brief History of Security
  - Why Security Is a Process, Not Point Products
- Types of Attacks
  - Access Attacks
  - Modification Attacks
  - Denial-of-Service Attacks
  - Repudiation Attacks

- Information Security Services
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
- Networking Fundamental for Security Professional
  - The OSI Network Model
  - The TCP/IP Network Model
  - Data Encapsulation
  - Ethernet Fundamental
  - Fundamental of IP and Routing
  - Fundamental of TCP and UDP
  - Case study (Network Sniffer in TCP/IP Network)
- Legal Issues in Information Security
  - U.S. Criminal Law
  - State Laws
  - Examples of Laws in Other Countries
  - Prosecution
  - Civil Issues
  - Privacy Issues
- Policy
  - Policy Is Important
  - Types of Policy
  - Creating Appropriate Policy
  - Deploying Policy
  - Using Policy Effectively
- Managing Risk
  - What Is Risk?
  - Identifying the Risk to an Organization
  - Measuring Risk
  - Case study (Risk identification on a real network)
- Information Security Process
  - Assessment
  - Policy
  - Implementation
  - Awareness Training
  - Audit
- Information Security Best Practice
  - Administrative Security
  - Technical Security
- Internet Architecture
  - Services to Offer
  - Services Not to Offer
  - Communications Architecture
  - Demilitarized Zone
  - Firewalls
  - Network Address Translation
  - Case study (Firewall design on a real network)

- Virtual Private Networks
  - Defining Virtual Private Networks
  - User VPN
  - Site VPN
  - Standard VPN techniques
  - Case study (Site and User VPN design)
- E-commerce Security Needs
  - E-commerce Services
  - Availability
  - Client-Side Security
  - Server-Side Security
  - Application Security
  - Database Server Security
  - E-Commerce Architecture
- Encryption
  - Encryption Concepts
  - Private Key Encryption
  - Public Key Encryption
  - Digital Signatures
  - Practical Session (PGP on your system)
- Hacker Techniques
  - A Hacker's Motivation
  - Historical Hacking Techniques
  - Methods of the Untargeted Hacker
  - Methods of the Targeted Hacker
  - Practical Session on Hacking tools
- Intrusion Detection
  - Types of Intrusion Detection Systems
  - Setting Up an IDS
  - Managing an IDS
  - Practical Session (Snort IDS on Windows)
- Windows Security Issues
  - Setting up the System
  - User Management
  - System Management

วิทยากร :

อาจารย์อาทิตย์ ซื่อสัตย์สิทธิกร

- Microsoft® Certified Professional
- Microsoft® Certified Technology Specialist
- Microsoft® Certified IT Professional
- Microsoft® Certified Solutions Associate
- Microsoft® Certified Solutions Expert
- CompTIA. Security+ certified

จำนวนชั่วโมงในการฝึกอบรม : 5 วัน (30 ชั่วโมง)

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

ค่าลงทะเบียนอบรม :

ค่าลงทะเบียน (บาท/คน) (ราคารวมภาษีมูลค่าเพิ่มแล้ว)	
ทุนสนับสนุน (70%)	ชำระเพิ่ม (30%)
13,300	5,700*

* หากไม่สามารถเข้ารับการอบรมได้และไม่ได้แจ้งสละสิทธิ์ล่วงหน้าก่อนการอบรม 2 สัปดาห์ หรือ 14 วันทำการก่อนวันอบรม จะต้องชำระค่าลงทะเบียนในราคาเต็ม หรือในอัตรา 100%
** สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

สถานที่ฝึกอบรม :

สถาบันพัฒนาบุคลากรแห่งอนาคต
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

วิธีการการสำรองที่นั่ง :

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ
โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887
โทรสาร: 0 2644 8110
Website: www.nstdaacademy.com/depa_EEC
E-mail: training@nstda.or.th