South Asia

Certified Enterprise Security Associate

Duration	40 Hours
Technology	Network Security & Enterprise Security
Training Mode	Instructor Led Training

Description: -

With the rise in advanced persistent threats, it is inevitable that organizations will be targeted. Defending against attacks is an ongoing challenge, with new threats emerging all the time, including the next generation of threats.

These three questions must be answered:

1. What is the risk?
2. Is it the highest priority risk?
3. What is the most cost-effective way to reduce the risk?

You will learn: -

- Practical Tips & Tricks on addressing high-priority security problems
- Foundation of Detection, Response and Prevention
- Security road-map
- Security-matrix
- Identify visible weakness of a system using various tools
- Create an effective policy and design a checklist
- Utilize Windows & Linux command-line tools to analyse a system for high risk items
- Design a network-architecture using VLAN, NAC and 802.1x based indicators
- Build a network visibility map
- Sniff network communication protocols

South Asia

Course Outline: -

1. Network Security Essentials 480 mins

Introduction

Network Defense Architecture

- Network Architecture
- Attacks Against Network Devices
- Network Topologies
- Network Design

Protocols and Packet Analysis

- Network Protocols Overview
- Layer 3 Protocols
    i. Internet Protocol
    ii. Internet Control Message Protocol
- Layer 4 Protocols
    i. Transmission Control Protocol
    ii. User Datagram Protocol

Tcpdump

Network Device Security

- Network Devices
- Network Device Security

Virtualization and Cloud

- Virtualization Overview
- Virtualization Security
- Cloud Overview

- Cloud Security

Securing Wireless Networks

- The Pervasiveness of "Wireless" Communications
- Traditional Wireless: IEEE 802.11 and Its Continual Evolution
- Personal Area Networks
- 5G Cellular (Mobile) Communication
- The Internet of Things

2. Defense-In-Depth 480 mins

Introduction

- Defense-in-Depth Overview
    - Risk = Threats x Vulnerabilities
    - Confidentiality, Integrity, and Availability
- Strategies for Defense-in-Depth
- Core Security Strategies

Identity and Access Management

- Digital Identity
    i. Authentication
    ii. Authorization
    iii. Accountability
- Identity Access Management
- Access Control
    i. Controlling Access
    ii. Managing Access
    iii. Monitoring Access

Authentication and Password Security

- Authentication Types

- Password Management
    i. Password Techniques
    ii. Password (Passphrase) Policies
    iii. Password Storage
    iv. How Password Assessment Works

- Password Cracking Tools
    i. John the Ripper
    ii. Hashcat
    iii. Mimikatz

- Multi-Factor Authentication
- Adaptive Authentication

Center for Internet Security (CIS) Controls

- Introduction to the CIS Controls
- The CIS Controls
- Case Study: Sample CIS Control

Data Loss Prevention

- Loss or Leakage
    i. Data Loss
    ii. Data Leakage
    iii. Ransomware

- Preventative Strategies
- Redundancy (On-Premise and Cloud)
- Data Recovery

- Related Regulatory Requirements
    i. IT ACT 2008

ii. GDPR
iii. CCPA

- Data Loss Prevention Tools
- Defending Against Data Exfiltration

Security Plans and Risk Management

- Security Plans
- Risk Management
- Security Governance
- How Do I Identify a Risk?

i. Quantifying Risk
ii. Probability
iii. Impact Types
iv. Asset Classification

- Risk-Level Matrices
- Risk Analysis

i. CIA Triad
ii. Least Privilege & Separation of Duties
iii. IAAA
iv. Prevent/Detect/Corrective Action
v. Due Care
vi. Due Diligence

- Risk Treatment Actions
- Risk & Compliance

i. Rules of the Road
ii. Identifying Vulnerabilities and threats
iii. Mapping and Scoring Assessment Maturity Rating
iv. Safeguards and Storage
v. Measuring Response Effectiveness

- Healthcare Security and Compliance

- HIPAA Security rules using NIST Security Frameworks

    i. Identify
    ii. Protect
    iii. Detect
    iv. Respond
    v. Recover

- Security Rules Safeguard and How to apply them in a Health Care Settings

    i. Administrative Safeguards
    ii. Physical safeguards
    iii. Technical safeguards

- Compliance Program

    i. Security Axioms
    ii. Security Vs Compliance
    iii. Supervisory Safeguards
    iv. Assessment Vs Audits

- Other Frameworks

    i. NIST
    ii. CIS Critical Security Controls
    iii. HITRUST
    iv. GDPR
    v. ISO

- Security Policies
- Security Standards

South Asia

3. Vulnerability Management and Response 480 mins

Vulnerability Assessments

- Introduction to Vulnerability Assessments
- Steps to Perform a Vulnerability Assessment
- Criticality and Risks

Penetration Testing

- What and Why of Penetration Testing
- Types of Penetration Testing
- Penetration Testing Process
- Penetration Testing Tools

Attacks and Malicious Software

- High-Profile Breaches and Ransomware
- Common Attack Techniques
- Malware and Analysis

Web Application Security

- Web Application Basics
    i. Cookies
    ii. HTTPS
- Developing Secure Web Apps
    i. OWASP Top Ten
    ii. Basics of Secure Coding
    iii. Web Application Vulnerabilities
    iv. Authentication
    v. Access Control
    vi. Session Tracking / Maintaining State
- Web Application Monitoring

- Web Application Firewall (WAF)

    i. Monolithic Architecture and Security Controls
    ii. Microservice Architecture

- Attack Surface

Security Operations and Log Management

- Logging Overview
- Setting Up and Configuring Logging
- Logging Management Basics
- Key Logging Activity

Digital Forensics and Incident Response

- Introduction to Digital Forensics

    i. What is Digital Forensics?
    ii. Digital Forensics in Practice
    iii. The Investigative Process
    iv. Remaining Forensically Sound
    v. Examples of Digital Forensics Artifacts
    vi. DFIR Subdisciplines
    vii. Digital Forensics Tools

- Incident Handling Fundamentals
- Multi-Step Process for Handling an Incident
- Incident Response: Threat Hunting

4. Data Security Technologies 480 mins

Cryptography

- Cryptosystem Fundamentals
- General Types of Cryptosystems

    i. Symmetric
    ii. Asymmetric

iii. Hashing

- Steganography

Cryptography Algorithms and Deployment

- Cryptography Concepts
- Symmetric, Asymmetric, and Hashing Cryptosystems
- Cryptography Attacks

Applying Cryptography

- Data in Transit

  i. Virtual Private Networks

- Data at Rest

  i. Data Encryption
  ii. Full Disk Encryption
  iii. GNU Privacy Guard (GPG)

- Key Management

  i. Public Key Infrastructure (PKI)
  ii. Digital Certificates
  iii. Certificate Authorities

Network Security Devices

- Firewalls

  i. Overview
  ii. Types of Firewalls
  iii. Configuration and Deployment

- NIDS

  i. Types of NIDS
  ii. Snort as a NIDS

- NIPS

    i. Methods of Deployment

Endpoint Security

- Endpoint Security Overview
- Endpoint Security Solutions
- HIDS Overview
- HIPS Overview

5. Operating System Security 480 mins

Windows Security

- Windows Security Infrastructure

    i. Windows Family of Products
    ii. Windows Workgroups and Accounts
    iii. Windows Active Directory and Group Policy

- Windows as a Service

    i. End of Support
    ii. Servicing Channels
    iii. Windows Update
    iv. Windows Server Update Services
    v. Third Party Patch Management

- Windows Access Controls

    i. NTFS Permissions
    ii. Shared Folder Permissions
    iii. Registry Key Permissions
    iv. Active Directory Permissions

v. Privileges
vi. BitLocker Drive Encryption

- Enforcing Security Policy

i. Applying Security Templates
ii. Employing the Security Configuration and Analysis Snap-in
iii. Understanding Local Group Policy Objects
iv. Understanding Domain Group Policy Objects
v. Administrative Users
vi. AppLocker
vii. User Account Control
viii. Recommended GPO settings

Network Services and Cloud Computing

- Server Core and Server Nano
- Best Way to Secure a Service
- Packet Filtering
- IPsec Authentication and Encryption
- Internet Information Server (IIS)
- Remote Desktop Services
- Windows Firewall
- Microsoft Azure and Microsoft 365 (Office 365)

Automation, Auditing, and Forensics

- Verifying Policy Compliance
- Creating Baseline System Snapshots
- Gathering Ongoing Operational Data
- Employing Change Detection and Analysis (Threat Hunting)

Linux Security

- Linux Fundamentals
- Operating System Comparison

- Linux Vulnerabilities
- Linux Operating System
    i. Shell
    ii. Kernel
    iii. Filesystem
    iv. Linux Unified Key Setup
- Linux Security Permissions
- Linux User Accounts
- Pluggable Authentication Modules
- Built-in Commands
    i. Windows / *NIX Comparison
    ii. Leveraging Built-in Commands for Threat Hunting
- Service Hardening
- Package Management

Linux Security Enhancements and Infrastructure

- Operating System Enhancements
    i. SELinux
    ii. AppArmor
- Linux Hardening
- Source Routing
- IPv6
- Address Space Layout Randomization (ASLR)
- Kernel Module Security
- SSH Hardening
- CIS Hardening Guides and Utilities

- Log Files
    i. Key Log Files
    ii. Syslog
    iii. Syslog Security
    iv. Log Rotation
    v. Centralized Logging
    vi. Auditing

- Firewalls: Network and Endpoint
- File-integrity Checking
- Rootkit Detectors

Containerized Security

- Chroot
- Virtualization
    i. Containers vs. Virtual Machines

- Containers
    i. LXC
    ii. Cgroups and Namespaces
    iii. Docker
    iv. Docker Images

- Container Orchestration
    i. Kubernetes

- Container Security
    i. Docker Best Practices
    ii. Vulnerability Scanning Tools
    iii. Secure Configuration Baselines
    iv. Terraform

Mobile OS Security

- Android vs. iOS
- Android Security
    i. Android Security Features
    ii. What You Need to Know About Android
    iii. Android Fragmentation
    iv. Android Security Fix Process
- Apple iOS Security
    i. Apple iOS Security Features
    ii. What You Need to Know About iOS
    iii. iOS Updates
- Mobile Problems and Opportunities
- Mobile Device Management (MDM)
- Unlocking, Rooting, and Jailbreaking
- Mitigating Mobile Malware
    i. Android Malware
    ii. iOS Malware