Quality Thought®

Cyber Security

Mode of Training: Online Training

Name of Trainer: Mr. Rajesh Kumar

Course Curriculum

CURRICULUM FOR ENDPOINT SECURITY – CEP 1

1. Introduction to Cyber Security
2. What is Cyber Security
3. Significance of Cyber Security
4. Layers of Cyber Security
5. Guiding principles of Cyber Security
6. Cyber-attacks and their impact
7. Familiarity with Security terminologies
8. Cyber Security career mapping
9. Introduction to Endpoint Security
10. Endpoint Devices and their functionality
11. Functional aspects of Endpoint Security
12. Technical elements of Endpoint Security
13. Significance of Endpoint Security
14. Understanding of Core elements of Endpoint Security
    a. Anti-Virus
    b. URL Filtering
    c. Data Loss Prevention
    d. Endpoint Detection and Response
    e. SCCM
    f. Encryption
    g. Multi-factor authentication
15. Popular Endpoint products
16. Operational aspects of Endpoint security
17. Overview of EPP and EDR
18. Assessment and Certification

CURRICULUM FOR ENDPOINT SECURITY – CEP 2

1. Introduction to Cyber Security
2. What is Cyber Security
3. Significance of Cyber Security
4. Layers of Cyber Security
5. Guiding principles of Cyber Security
6. Cyber-attacks and their impact

7. Familiarity with Security terminologies
8. Cyber Security career mapping
9. Introduction to Endpoint Security
10. Endpoint Devices and their functionality
11. Functional aspects of Endpoint Security
12. Technical elements of Endpoint Security
13. Understanding Core elements of Endpoint Security
    a. Anti-Virus
    b. URL Filtering
    c. Data Loss Prevention
    d. Endpoint Detection and Response
    e. SCCM
    f. Encryption
    g. Multi-factor authentication
14. Popular Endpoint products
15. Operational aspects of Endpoint security
16. Overview of EPP and EDR
17. Assessment and Certification

Technical Demonstration of:

- ✓ Symantec Endpoint Security
- ✓ McAfee Endpoint Security
- ✓ TrendMicro Deep Security

Symantec Endpoint Security

- Introduction to Symantec Endpoint Security
- Architecture of Symantec Endpoint
- Features of Symantec Endpoint Protection Manager
- Client and Policy Deployment
  - Administering clients
  - Configuring Groups
  - Active Directory integration with SEPM
  - Client Configuration modes
  - General Client Settings and Tamper Protection
- Introduction to Antivirus, Insight and Sonar
  - Virus and Spyware protection needs and Solution
  - Reputation and Insight
  - Administrator defined scans
  - Auto protect
  - Download Insight
  - Sonar
- Introduction to Network Threat Protection, Application and Device Control

    - The Firewall
    - Intrusion Prevention
    - Application and Device Control
- Content updates
    - Live Update
    - Group Update Provider
- Overview of Symantec Endpoint Protection Manager Installation
- Overview of Symantec EDR

McAfee Endpoint Security

- Introduction to McAfee Endpoint
- Components of McAfee Endpoint
    - McAfee Agent
    - McAfee ePolicy Orchestrator
        - Overview of McAfee ePO
        - High Level steps on installation of McAfee ePO
        - Policy Management Overview
        - Monitoring and Reporting
    - McAfee VirusScan Enterprise
        - Policies of McAfee VirusScan Enterprise
        - Common issues in McAfee VirusScan Enterprise
- Difference between EPP and EDR
- Introduction to McAfee EDR Solution

- Overview of Security Modules
    - Threat Prevention
    - Firewall
    - Web control
    - Adaptive Threat Prevention
- Overview of McAfee MVision
    - Key features of McAfee MVision
    - McAfee Cloud ePO Virtual tour

TREND MICRO DEEP SECURITY

Product Overview

- Introduction to Deep Security
- Deep Security Components
- Deep Security modules
- Deep Security deployment options

- **Deep Security Manager**

    - On Prem vs SAAS model
    - Deep Security Manager architecture
    - Virtual tour of Deep Security Manager

- **Deep Security Agent**

    - Deep Security Agent architecture
    - Deploying Deep Security Agents
    - Upgrading Deep Security Agents

Security Modules in Depth

- **Protecting Servers from Malware - Antimalware**

    - Anti-malware scanning techniques
    - Enabling anti-malware protection
    - Smart Scan

- **Blocking Malicious Websites – Web Reputation**

    - Enabling web reputation
    - Setting the security level

- **Detecting Changes to Protected Servers – Integrity Monitoring**

    - Enabling integrity monitoring
    - Running recommendation scans
    - Detection changes to baseline objects