McAfee ePolicy Orchestrator Administration (5.10)

(Customized Designed Course Content)

Day 1

- Welcome
- Security Solutions and McAfee ePolicy Orchestrator
- Overview
- Planning a McAfee ePolicy Orchestrator Deployment
- Installing McAfee ePolicy Orchestrator Software
- Managing Permission Sets and Users
- Creating and Populating the System Tree
- Using the Tag Catalog
- Sorting the System Tree
- McAfee® Agent
- System Information
- Client Tasks
- Managing Policies
- Policy and Client Task Approval

Day 2

- Deploying Software for Managed Systems
- Repositories
- Product and Server Maintenance with Repositories
- Managing Dashboards and Monitors
- Working with Queries and Reports
- Automatic Responses and Notifications

Day 3

- Database Maintenance and Server Utilities
- Disaster Recovery
- Agent Handlers
- Rogue System Detection
- Configuring Rogue System Detection

Day 5

- Endpoint Security Threat Prevention (Virus and Malware Protection)
  - (Blocks threats from accessing systems, scans files automatically when they are accesses, and runs targeted scans for malware on client systems)

- Application and Change Control (AKA Whitelisting/ Solidcore)
  - Application Control Blocks unauthorized executables on Servers, Corporate Desktops, and Fixed-function devices. Change Control monitors and prevents changes to the file system.
  - Observe Mode:
    - ACC monitors the system for which executable files and scripts are accessed by the system and updates its inventory with hash values.
  - Enable Mode:
    - Once the inventory of files has been reviewed and trusted, only trusted files are permitted to execute.
    - Modification to executable and trusted data files is blocked.
    - Files can be excluded based on type (.txt, log) or directory. (such as D:\)
  - The list of known and permitted files is referred to as the Whitelisting

- USB Device Control (Windows Only)
  - USB devices are whitelisted based on serial number.
  - Only permitted USB drives can be accessed on the managed device.

Day 5 Agenda: In replication of Day 5 extraction

1. Install Endpoint Security Protection.
   a. Enable Engine
   b. Create Policy
   c. Apply Policy
2. Download Malware from Internet
   a. Install Malware
   b. If block, add exception to execute installation.
   c. Scans files and Skip Critical Drives/Folder Location.
   d. Improve application performance.
3. USB Control
   a. Block USB detection
   b. Block USB Mass Storage
   c. Block file execution using USB
4. Monitor Executables
   a. Process
   b. Inventory
   c. Block executables
   d. Permit Hash based access

The above course is designed to cover as 2 hours theory and 6 hours Lab.