Managing Virus, Trojans & Malware using Symantec Endpoint Protection

(Customized Course)

DAY ONE:

One: Introduction and defining malicious software

- Viruses
- Worms
- Trojans
- Rootkits
- Malware
- Types of viruses
- Types of worms
- Types of Trojans
- Types of rootkits
- Types of malware

LAB: Identifying the characteristics of malicious software

Two: Fundamentals of Windows Processes

- Threads
- Handles
- SAT (Security Access Token)
- Windows Server Architecture
- User mode versus kernel mode
- Rings of the Intel Architecture

LAB: User mode and kernel mode analysis

Three: Basic Process Analysis

- Process context
- Process priority
- Process image
- Process memory
- Process components
- Process path
- Process ports
- Process cpu interaction
- Identifying rogue process and Trojans

LAB: Basic Process Analysis

DAY TWO

Four: Advanced Process Analysis

- Process antecedence
- Process description
  - Vendor
  - Version
  - Location
- Process links into the registry
- Process links into the file system
- Process internal communication

LAB: Advanced Process Analysis

Five: Fundamentals of Linux, UNIX and OpenVMS Processes

- Dissecting memory artifacts
- Init process
- Reading process information
- Privilege level of processes
- Process context
- Process priority
- Process image
- Process memory
- Process components
- Process path
- Process ports
- Process cpu interaction
- Identifying rogue process and trojans
- Controlling processes

LAB: *Nix processes

Six: *Nix Process and File Analysis

- Processes that opened ports
- Running processes
- Open files
- Internal routing
- Loaded kernel modules
- Mounted file systems
- Path to a process

- File system structure and time analysis
- Syslog analysis
- Identifying suspicious processes and files

LAB: Process and File Analysis

DAY THREE

Seven: Malware Fundamentals

- Malware Ecosystem
- Sophistication and advances
- Characteristics of
- Challenges of detection
- Morphing of rootkits
- Detecting rootkits
  - Traditional
  - Hooking
  - DKOM
- Evasion techniques

LAB: Malware Detection Challenges

Eight: Introduction to Symantec Endpoint Protection Manager (SEPM)

- Technologies
- Components
- Policies
- Design
- Types of protections

Nine: Initial Configuration of SEPM

- Accessing the SEPM
- Console
- Remote
- Dashboards
- Policy types and components
- Licensing
- Managing products

LAB: Initial Configuration of SEPM

DAY FOUR:

Ten: Configuring Groups and Clients

- Managing groups
  - Adding
  - Moving
  - Renaming
  - Disabling and enabling group inheritance

LAB: Groups

- Managing clients
  - User mode
  - Computer mode
  - Unmanaged
  - Managed
  - Detection of unknown devices
  - Running commands on

LAB: Clients

Eleven: Policy Configuration and Customization

- Management
- Shared
- Non-shared
- Adding, Editing and assigning policies
- Updating policies
  - Push
  - Pull
- Updating policies
  - Manual

LAB: Policies

Twelve: Monitoring via policies

- Deploying monitoring policies
  - Detecting what applications a client runs
  - Detecting startup of services
  - Configuring a management server for policy monitoring
- Application searching and reporting

LAB: Monitoring

DAY FIVE

Thirteen: Working with Clients

- Installation packages
  - Features
  - Settings
- Exporting packages
- Deploying packages
  - Managed
  - Un-managed

LAB: Clients

Fourteen: Updating Definitions and Content

- Types of content
- Methods of delivering content
- Live update
  - Using a local content distribution server
  - Configuring settings and rules
- Distribution tools

LAB: Manual content updating

Fifteen: Communication between clients and management servers

- Management servers
  - Adding
  - Configuring connection order
  - Communication settings for different locations
- Troubleshooting
  - Testing connectivity with ICMP
  - Using the http protocol to test connectivity
  - Debugging communication problems

LAB: Communication troubleshooting

Sixteen: Logging

- Types
- Viewing
- Filters
- Exporting to syslog

LAB: Logging