McAfee HIPs – Host Intrusion Prevention System Administration

Course Content –

Module 1: Introduction to McAfee Host Intrusion Prevention

- Vulnerabilities, Exploits, Buffer Overflows, Attacks, Threats
- Protection Levels
- Host Intrusion Prevention
- Components and Features
- Supported Operating Systems
- New Features

Module 2: Security Connected and ePolicy Orchestrator Overview

- Introducing McAfee Security Connected
- The manifestation of Security Connected
- Security Connected Framework
- Integration with Third-Party Products
- Security Connected Solution Platform
- Solution Overview
- New for this Release
- Basic Solution Components
- Web Interface
- Menu Pages
- Customizing the User Interface
- Architecture and Communication
- User Interface
- Functional Process Logic
- Data Storage

Module 3: Managing Dashboards and Monitors

- Dashboards Overview
- Accessing the Dashboards Page
- Types of Dashboards
- Duplicating and Adding Dashboards
- Assigning Dashboard Permissions
- Dashboard Permissions Guidelines
- Deleting a Dashboard
- Adding Monitors to a Dashboard

- Dashboards Server Settings
- Editing the Automatic Refresh Interval
- Assigning Default Dashboards
- Configuring Dashboard Monitors
- Resizing, Moving, and Removing Monitors
- Concurrent Users (Console Connections)
- Results of Load
- Designing Dashboards
- Changing the Default Session Timeout

Module 4: McAfee Agent

- Agent Components
- Agent-Server Secure Communication Keys
- Communication after Agent Installation
- Typical Agent-to-Server Communication
- McAfee Agent-to-Product Communication
- Forcing Agent Activity from Server
- Wake-up Calls and Wake-up Tasks
- Locating Agent Node Using DNS
- Using System Tray Icon
- Forcing McAfee Agent Activity from ClientAgent Files and Directories
- Using Log Files
- Installation Folders

Module 5: HIPS Server Planning and Installation

- HIPS Installation on the ePO Server
- Requirements
- Extensions
- Adding Software to the Master Repository
- Software Manager
- Installing Host IPS Extensions on the ePO Server
- Checking in the Host IPS Client
- Package into the Master Repository
- Upgrading and Migrating Policies

Module 6: Windows Host IPS Client

- Host IPS installation requirements
- Installing the Client Remotely using ePO and Directly on the Client Computer
- Post-Installation Client Changes
- Registry Implementation

- Client Services and Client-side Component Relationship
- Downgrading and Removing the Client
- Direct Client-Side Management
- Verifying the Client is Running
- Allowing the Disable of Features
- Enabling Timed Group
- Unlocking the Windows Client Interface
- Responding to Spoof Detected Alerts
- Managing IPS Protection, Rules, Host Firewall Policy Options, and Blocked Hosts List
- Verifying Host IPS Events are Triggered Correctly
- Client Logging and Troubleshooting
- Investigating Performance Issues

Module 7: Host IPS General Policies

- General Policies Overview
- Configuring the Client User Interface Policy
- Configuring Display Options
- Enabling Advanced Functionality and Client Control
- Trusted Networks Policy and Trusted Application
- Creating and Editing Executables
- Working with Multiple Instance Policies
- Marking Applications as Trusted

Module 8: Intrusion Prevention Policies

- Intrusion Prevention Overview
- Benefits of Host Intrusion Prevention
- IPS Options, Protection, Rules
- Configuring IPS Options
- Using Preconfigured Policies
- Creating and Editing Policies
- Setting Protective Reaction for Signature Severity Levels
- Moving from Basic to Advanced Protection

Module 9: IPS Rules Policies

- Overview of the IPS Rules
- Host Intrusion Prevention Clients
- IPS Protection with IPS Rules Policies
- Host and Network IPS Signature Rules
- Signature and Behavioral Rules
- Signatures and Severity Levels

- Working with IPS Rules Policies and Signatures
- Multiple Instance Policies
- Effective Policy for IPS Signatures
- Multiple Instance Policies and the Effective Policy
- VirusScan Access Protection and IPS Rules

Module 10: IPS Rules Policies – Application Protection

- Application Blocking and Hooking
- Prevent an Executable from Running (Black List)
- Create, Editing or Viewing Executable Details
- Blocking and Allowing Application Hooking
- Customizing and Managing Rules
- Process Hooking

Module 11: Configuring IPS Exceptions

- Exception Rules
- Configuring IPS Rules Exceptions
- Creating Exceptions for Network IPS Rules
- Applying OS Patches
- Creating Trusted Applications
- Adjusting Signature Severity Levels
- Tuning Methods

Module 12: Working with IPS Events

- Events and Event Logging
- List of the HIPS Events Supported by ePO
- Reacting to Events
- Viewing Host IPS Events
- Filtering Events
- Creating an Exception Based on a Selected Event
- Analyzing Events
- Viewing Systems on which Selected Events Occur
- Viewing Common Vulnerabilities and Exposures (CVE) Information
- Creating Event-based Exceptions
- IPS Signature Events
- General Methodology for Reviewing Updates, Patch Systems and Applications

Module 13: Creating IPS Client Rules

- IPS Client Rules Overview
- Refining Policies Based on Use
- Learning Mode

- Adaptive Mode
- Placing Clients in Adaptive or Learn Mode
- Adaptive Mode Sequence
- Managing IPS Client Rules
- Create Exceptions Using IPS Client Rules
- Reviewing Detail for IPS Client Rules
- Retaining Existing Client Rules
- Using the Property Translator Server Task

Module 14: Custom Signatures

- Custom Signatures Overview
- Methods for Creating Custom Signatures
- Creating a Custom Signature
- Using the Signature Creation Wizard
- Creating Windows/Unix Files and Directories
- Creating Signatures-Windows Registry
- Using the Linux or Solaris Option to Create Signatures
- Adding and Editing Sub-rules
- Viewing General Information about Signature
- Editing the Severity Level, Client Exception Permission, and Log Status of a Signature
- Custom Signatures Components
- File Rule Types and Examples
- Troubleshooting Custom Signatures

Module 15: Automatic Responses and Threat Notification

- Threat Notification and Tracing
- Event Types, Formats, and Life Cycle
- Automatic Response Process
- Creating, Editing, Viewing, and Deleting Automatic Responses for Specific Event Types
- Setting Filters, Aggregating Events, and Configuring Rule Actions
- Creating Issues Executing Scheduled Tasks, and Running External Commands.
- Variables Used in Notifications
- Creating and Editing Automatic Responses
- Filtering Events
- Throttling and Aggregation
- Default Automatic Response Rules
- Planning Automatic Responses
- Determining Events Forwarding
- Automatic Responses Permission Set

- Managing Issues
- Creating Contacts

Module 16: Firewall Policies

- Host IPS Firewall Overview
- Firewall Protocol Support
- Allowing Unsupported Protocols and Bridged Traffic
- Understanding the State Table
- Stateful Filtering and Protocol Tracking
- How Firewall Rules Work
- Firewall DNS Blocking
- Working with Firewall Options Policies
- Startup Protection and Protection Options
- trusted source/Global Threat Intelligence

Module 17: Firewall Rules Policies

- Configuring Firewall Policies
- Firewall Rules Console
- Default Policies
- Typical Corporate Environment Policy
- Firewall Groups
- Creating New Firewall Rule
- Using the Firewall Rule Builder
- Using the Host IPS Catalog
- Adding Rules from the Catalog
- Creating Firewall Rule Groups
- Adaptive Mode versus Learn Mode
- Managing Firewall Client Rules
- Refining Policies Based on Use
- Responding To Firewall Alerts
- Stateful Filtering in Adaptive or Learn Mode
- Retaining Existing Client Rules
- Firewall Theory
- Basic Design Philosophies
- Firewall Design Considerations
- Firewall Planning

Module 18: Firewall Rule Groups

- Host IPS Firewall Groups
- Location-enabled Firewall Groups

- Connection-aware Firewall Groups
- Matching for Location-Aware Groups
- Timed Groups in Firewall Policy

Module 19: Host Intrusion Prevention Maintenance

- Server Tasks in ePO
- Clearing Events
- Generating Host IPS Reports/Queries
- Reports
- Dashboards and Queries
- Running Predefined Host IPS Queries
- Creating Custom Host IPS Queries
- Client-side Policy Reporting
- Default Dashboards
- Vulnerability Shielding Updates
- McAfee Agent Update Task
- Manual Content Updating
- McAfee Internet Sites
- Creating an ePO Server Pull Task
- Testing McAfee Host Intrusion Prevention Client
- Adaptive Mode versus Learn Mode
- Managing Firewall Client Rules
- Refining Policies Based on Use
- Responding To Firewall Alerts
- Stateful Filtering in Adaptive or Learn Mode
- Retaining Existing Client Rules
- Firewall Theory
- Basic Design Philosophies
- Firewall Design Considerations
- Firewall Planning

Module 20 – Host IPS Implementation and Best Practices

- Pre-Installation Considerations and Deployment Planning
- Best Practices
- Step 1: Strategy and Planning
- Lab or Real World?
- Confirm Your Rollout Strategy
- Timing and Expectations
- Preparing the Environment

- Step 2: Prepare the Pilot Environment
- Using ePolicy Orchestrator
- Step 3: Installation and Initial Configuration
- Managing Protection
- “Out-of-the-Box” Protection
- Multiple Policy Instances
- Notify End Users and Plan Escape Hatches
- Enlist the Help Desk Team
- Install Host IPS to Pilot Hosts
- Check Pilot Systems for Proper Operation
- Step 4: Initial Tuning
- Host IPS Configuration and Initial Tuning
- Tuning Methods
- Fine-Tuning Policies
- Security Tightening
- Follow these Processes
- More Tuning
- Create Exceptions
- Create Trusted Applications
- Run Queries
- Step 5: Optional Adaptive Mode
- Adaptive Mode: Refine Policies Based on Use
- Understanding Adaptive Mode
- Adaptive Mode Limitations
- Best Practices with Adaptive Mode
- Potential Pitfalls in IPS Deployments
- Step 6: Enhanced Protection and Advanced Tuning
- Heightened Protection and Advanced Tuning
- Step 7: Maintenance and Expansion Beyond IPS
- Server Maintenance
- Domain Controllers and Host IPS

Module 21 – ClientControl Utility

- Deploying Host IPS with 3rd Party Product
- ClientControl Logging
- Command Line Syntax
- Major Arguments
- Argument – /help

- Argument – /start and /stop
- Stopping Host IPS Services
- Argument – /log
- Argument – /engine
- Argument – /export
- Argument – /readNaiLic
- Argument- /exportConfig
- Argument – /defConfig
- Argument – /startupIPSProtection
- Argument – /execInfo
- Argument – /fwPassthru
- fwinfo Utility

Module 22 – Linux Client

- Linux Client Installation Requirements
- Policy Enforcement with the Linux Client
- Notes about the Linux Client
- Removing the Linux Client
- Troubleshooting the Linux Client
- HIPTS – Troubleshooting Tool
- Verifying Linux Installation Files
- Stopping and Restarting the Linux Client

Module 23 – Solaris Client

- Solaris Client Installation Requirements
- Policy Enforcement with the Solaris Client
- Solaris Zone Support
- Installing the Solaris Client
- Removing the Solaris Client
- Troubleshooting the Solaris Client
- HIPTS – Troubleshooting Tool
- Verifying Solaris Installation Files
- Stopping and Restarting the Solaris Client

Module 24 – Troubleshooting Host IPS Forums and Security Advisories

- KnowledgeBase Articles for Host IPS
- MERTool
- Client Issues
- Identify the Versions
- Host IPS Engines

- Installation Issues
- McAfee Agent Logs
- Policy, Event, and Client Rule Issues
- Policy Update Issues
- Verifying Policies – Static Configuration
- Verifying Policies – Dynamic Policy
- fwinfo.exe
- Verifying Policies – FireCore Policy
- Troubleshooting Host IPS
- Troubleshooting the Host IPS Firewall
- Troubleshooting Firewall Issues
- Activity Log
- Applying Service Packs
- Escalation Process