Sophos Endpoint Administrator

Course Outline

Module 1: Enduser Protection deployment scenarios

- Review of Enduser Protection features and components
- Factors to consider when designing solutions
- Single site deployments
- Multi site deployments
- Air-gapped network
- Roaming users
- Selecting the right solution for a customer's requirements

Module 2: Sophos Enterprise Console deployment

- Factors to consider when designing SEC deployments
- Management server requirements
- Database design considerations
- Remote console requirements
- Firewall configuration
- High availability
- Selecting the right solution for a customer's requirements
- The installation process
- Troubleshooting installation

Module 3: Deploying Enduser Protection

- Determining the information required to plan endpoint deployment
- Supported platforms
- Deployment strategy
- Removing other endpoint products
- Setup.exe command line parameters
- Protecting computers automatically
- Deployment packager
- Installation log files
- Mac deployment
- Linux deployment
- Selecting the right solution for a customer's requirements

Module 4: Update Managers and Autoupdate

- Factors to consider when designing an updating infrastructure
- Introduction to AutoUpdate
- SUM updating overview
- Software subscriptions
- HTTP Updating
- Deploying multiple CIDs and Update Managers
- Selecting the right solution for a customer's requirements
- Installing additional SUMs
- AutoUpdate components
- Troubleshooting SUM
- Troubleshooting AutoUpdate

Module 5: Remote Management System

- Factors to consider when designing an updating infrastructure
- Management architecture
- Remote Management System (RMS)
- RMS component communication
- RMS troubleshooting
- Message relays
- Selecting the right solution for a customer's requirements

Module 6 : Threat Protection

- Anti-virus and HIPS review
- Configuring exclusions
- Live Protection overview
- Sophos Extensible List (SXL)
- Live protection architecture
- Live protection DNS lookups
- Web protection and control
- Web protection HTTP lookups
- Malicious Traffic Detection (MTD)
- MTD components
- Windows Filtering Platform (WFP)
- Testing MTD

Module 7: Advanced device and data control policies

- Review of device control
- Device control event viewer
- Unique device instance IDs
- Device exemptions
- Review of data control

- Content Control List (CCL)
- Latest SophosLabs Content Control Lists
- How to create a custom CCL
- Data control exclusions

Module 8: Advanced firewall configuration

- Review of Sophos Client Firewall (SCF)
- Firewall rule types
- Rule processing order
- Primary / secondary location configuration
- Client firewall logs and LogViewer

Module 9: Auditing and reporting

- Auditing configuration
- Email alerting
- Sophos Reporting Interface
- Sophos Log Writer

Module 10: Server management and upgrades

- Backup and restore data and configuration
- PurgeDB
- Database and server migration
- Upgrading servers
- The diagnose tool