Module 1: Deployment Scenarios

- Identify some of the common challenges when deploying Central
- Deploy Update Caches
- Set up Message Relays
- Configure AD Sync Utility
- Identify where Update Caches and Message Relays should be used
- Labs:
- Register and activate a Sophos Central evaluation
- Install Server Protection
- Install and Configure AD Sync Utility
- Deploy an Update Cache and Message Relay

Module 2: Client Deployment Methods

- Identify the recommended steps for deploying Sophos Central
- Explain the installation process, and identify the different types of installer
- Automate deployment for Windows, Linux and Mac computers
- Migrate endpoints from Enterprise Console
- Locate installation log files
- Remove third-party products as part of a deployment
- Labs:
- Enable Server Lockdown
- Deploy using Active Directory Group Policy
- Use the Competitor Removal Tool
- Deploy to a Linux Server using a Script

Module 3: Endpoint Protection Policies

- Describe the function and operation of each of the components that make up an Endpoint Protection and Intercept X
- Configure policies to meet a customer's requirements and follow best practice
- Test and validate Endpoint Protection
- Configure exclusions
- Configure Data Loss Prevention
- Labs:
- Test Threat Protection Policies
- Configure and Test Exclusions
- Configure Web Control Policies
- Configure Application Control Policies
- Data Control Policies
- Configure and test Tamper Protection

Module 4: Server Protection Policies

- Configure Server Protection Policies

- Configure and Manage Server Lockdown
- Labs:
- Configure Sever Groups and Policies
- Manage Server Lockdown
- Test Linux Server Protection

Module 5: Protecting Virtual Servers

- Connect AWS and Azure accounts to Sophos Central
- Deploy Server Protection to AWS and Azure
- Deploy and Manage Sophos for Virtual Environments
- Labs:
- Download the installer for the Security Virtual Machine
- Install the Security Virtual Machine (SVM) on a Hyper-V Server
- Configure Threat Protection policies to apply to the Security VMs and the Guest VMs they protect
- Perform a manual installation of the Guest VM Agent and view logs
- Test and configure a script to deploy the GVM Agent
- Manage Guest VMs from the Central Console
- Test Guest VM Migration

Module 6: Logging and Reporting

- Explain the types of alert in Sophos Central
- Use the Sophos Central logs and reports to check the health of your estate
- Export data from Sophos Central into a SIEM application
- Locate client log files on Windows, Mac OS X and Linux
- Labs:
- Configure SIEM with Splunk

Module 7: Managing Infections

- Identify the types of detection and their properties
- Explain how computers might become infected
- Identify and use the tools available to cleanup malware
- Explain how the quarantine works and manage quarantined items
- Cleanup malware on a Linux server
- Labs:
- Source of Infection Tool
- Release a File from SafeStore
- Disinfect a Linux Server

Module 8: Endpoint Detection and Response

- Explain what EDR is and how it works
- Demonstrate how to use threat cases and run threat searches

- Explain how to use endpoint isolation for admin initiated and automatic isolation
- Demonstrate how to create a forensic snapshot and interrogate the database
- Labs:
- Create a forensic snapshot and interrogate the database
- Run a threat search and generate a threat case

Module 9: Management

- Use the Controlled Updates policies appropriately
- Enable multi-factor authentication
- Use the Enterprise Dashboard to manage multiple sub-estates
- Identify the benefits of the Partner Dashboard
- Identify common licensing requirements
- Labs:
- Enable Manually Controlled Updates
- Enable Multi-Factor Authentication