Sophos Endpoint Architect Course Overview

This course provides an in-depth study of Sophos Endpoint, designed for experienced technical professionals who will be planning, installing, configuring, and supporting deployments in production environments.

Sophos Academy

SOPHOS

Delivery

This course is available online via the Training Portal, or as an instructor-led classroom course. Please contact your CAM or CAE to find out more about the availability of classroom courses in your region.

Electronic copies of the supporting documents for the course are provided to each trainee via the training portal.

Duration

This course will take approximately **3 days (24 hours)** to complete.

Assessment

To complete this course, trainees must take and pass an online assessment.

Trainees will have **3 hours** to complete the assessment; the pass mark is **80%** and trainees will have **3 attempts** to pass.

Lab Environment

Each trainee is provided with a pre-configured environment that simulates a company network with two sites, a head office, and a branch office.

Objectives

On completion of this course, trainees will be able to:

- Plan and deploy complex installations of Sophos Endpoint
- Explain the core configuration concepts of Sophos Endpoint and demonstrate how to configure and implement them
- Perform manual clean-up of threats
- Proactively investigate suspicious activities
- Perform preliminary troubleshooting and basic support steps

Prerequisites

Prior to taking this training, trainees must:

- Have completed and passed the **Sophos Endpoint – Certified Engineer** course
- Have completed any subsequent delta modules up to version 5.0

We recommend that trainees have the following knowledge and experience:

- Windows networking and the ability to troubleshoot issues
- A good understanding of IT security
- Linux command line for common tasks
- Configuring Active Directory group policies

If you are uncertain whether you meet the necessary prerequisites, please email us at globaltraining@sophos.com and we will be happy to help.

Course Agenda

Module	Chapter	Duration
1. User Management		
Chapters	▪ Sophos Central Role-based User Access ▪ Advanced Directory Synchronization in Sophos Central ▪ Configuring Federated Authentication in Sophos Central	20 minutes
Lab Tasks	**Lab Preparation** ▪ Register for a Sophos Central Trial **User Management** ▪ Install and Configure AD Sync Utility ▪ Configure role-based user access	35 minutes
2. Sophos Endpoint Agent Deployment		
Chapters	▪ Sophos Endpoint Agent Deployment Strategy ▪ Automating Sophos Endpoint Agent Deployment on Windows ▪ Automating Sophos Endpoint Agent Deployment on macOS ▪ Automating Sophos Endpoint Agent Deployment on Linux	25 minutes
Lab Tasks	**Preparation** ▪ Install Sophos Endpoint on a Windows Server ▪ Deploy an Update Cache and Message Relay **Sophos Endpoint Agent Deployment** ▪ Install Sophos Endpoint for Linux ▪ Use AD GPO to deploy multiple Windows devices ▪ Enable Server Lockdown	80 minutes
3. Updating and Communication		
Chapters	▪ Advanced Sophos Endpoint Updating ▪ Controlling Sophos Endpoint Updates ▪ Considerations when using Sophos Endpoint Update Cache and Message Relays ▪ Advanced update Cache and Message Relays	20 minutes
4. Virtual Protection		
Chapters	▪ Protecting Azure hosted virtual servers ▪ Protecting AWS hosted virtual servers	15 minutes
5. Device Management		
Chapters	▪ Managing Server Protection for Linux	10 minutes
Lab Tasks	▪ Create Server Groups ▪ Manage Tamper Protection	15 minutes

6. Policies		
Chapters	▪ Advanced Sophos Endpoint Control Policies ▪ Advanced Sophos Endpoint Data Loss Prevention ▪ Advanced Sophos Endpoint Policies and Exclusions ▪ Getting Started with Partner Global Policies ▪ Advanced Server Lockdown ▪ Getting Started with Server File Integrity Monitoring	70 minutes
Lab Tasks	**Investigation Preparation** ▪ Preparation for a later lab task **Policies** ▪ Configure and Test Threat Protection Policies ▪ Configure and Test Web Control ▪ Configure and Test App Control ▪ Configure and Test DLP using CCLs ▪ Configure and Test Exclusions ▪ Manage Server Lockdown ▪ Test Linux Server Protection	90 minutes
7. Remediation and Reports		
Chapters	▪ Getting Started with SIEM Integration with Sophos Central ▪ Linux Server Protection threat Detection and Remediation ▪ Advanced Sophos Endpoint Threat Remediation ▪ Getting Started with Sophos Endpoint Forensic Snapshots	25 minutes
Lab Tasks	▪ Configure SIEM with Splunk ▪ Release a file from SafeStore ▪ Remediate a Linux Server ▪ Create a Forensic Snapshot and Interrogate the database	95 minutes
8. Detection and Response		
Chapters	▪ Sophos Data Lake APIs ▪ Writing Live Discover Queries ▪ Live Discover Queries Writing Scenarios	30 minutes
Lab Tasks	▪ Use Live Discover to locate unauthorized programs ▪ Investigate a Detection	40 minutes
12. Course Review		
Chapters	▪ How to find help from Sophos ▪ Course review	10 minutes

Further Information

If you require any further information on this course, please contact us at globaltraining@sophos.com.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com