



**Enterprise Computing Solutions - Education Services**

## **TRAINING OFFERING**

---

**Vous pouvez nous joindre ici**

Email: [training.ecs.fr@arrow.com](mailto:training.ecs.fr@arrow.com)  
Phone: 01 49 97 50 00

# SOPHOS    Sophos Central Architect

**CODE:**            **DURÉE:**            **PRIX H.T.:**

SOP\_AT15        24 Hours (3 Jours)        €1,800.00

## Description

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

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.

## Objectifs

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

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

## Audience

Experienced technical professionals

## Prérequis

Prior to taking this training, trainees should:

- Have completed and passed the Sophos Central Endpoint and Server Protection – Certified Engineer course
- Have completed any subsequent delta courses up to version 3.0

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](mailto:globaltraining@sophos.com) and we will be happy to help

## Programme

1. Sophos Central Overview  
Getting started with SURF Lab Tasks Register and activate Sophos Central
2. Sophos Central User Management  
Sophos Central role-based user access Advanced directory synchronization in Sophos Central  
Configuring federated authentication in Sophos Central Lab Tasks Install and configure Windows AD sync utility  
Configure role-based access Deployment preparation tasks : Deploy Sophos protection to a Windows server  
Deploy an Update Cache and a Message Relay
3. Sophos Central Agent Deployment  
Sophos Central Agent deployment strategy Automating Sophos Central Agent deployment on Windows  
Automating Sophos Central Agent deployment on macOS Automating Sophos Central Agent deployment on Linux  
Migrating from SEC to Sophos Central Lab Tasks Install Sophos server protection for Linux  
Use AD group policy to deploy Sophos protection to multiple devices Enable server lockdown (preparation for a later lab task)
4. Sophos Central Updating and Communication  
Advanced Sophos Central updating Controlling Sophos Central updates  
Considerations for using Sophos Central Update Caches and Message Relays  
Advanced Sophos Central Update Cache and Message Relay deployment Lab Tasks Enable manually controlled updates  
Create server groups Manage tamper protection
5. Sophos Central Virtual Protection  
Protecting Azure hosted virtual servers with Sophos Central Protecting AWS hosted virtual servers with Sophos Central  
Simulation tasks Configure automated deployment on Azure hosted virtual servers  
Configure automated deployment on AWS hosted virtual servers
6. Sophos Central Policies  
Advanced Sophos Central control policies Advanced Sophos Central data loss prevention  
Advanced Sophos Central policies and exclusions Getting started with Sophos Central partner global policies  
Advanced Sophos Central server lockdown Lab Tasks Prepare for a later lab task Configure and test threat protection policies  
Configure and test web control Configure and test application control Configure and test data control using CCLs  
Configure and test exclusions Manage server lockdown Test Linux server protection
7. Sophos Central Remediation and Reports  
Getting started with SIEM integration with Sophos Central Advanced Sophos Central threat remediation  
Getting started with Sophos Central forensic snapshots Lab Tasks Configure SIEM with Splunk Release a file from SafeStore  
Remediate a Linux server Create a forensic snapshot and interrogate the database
8. Sophos Central XDR  
Sophos XDR Data Lake APIs Sophos Central XDR Live Discover query pivoting  
Writing queries for Sophos Central XDR Live Discover Writing scenarios for Sophos Central XDR Live Discover queries  
Using Sophos Central XDR for IT operations Using Sophos Central XDR for threat hunting Lab Tasks  
Use Live Discover to locate unauthorized programs Investigate a detection using Sophos Central XDR
9. Course Review

How to find help from Sophos Course review

## Informations supplémentaires

If you require any further information on this course, please contact Sophos at [globaltraining@sophos.com](mailto:globaltraining@sophos.com)

## Dates de session

Sur demande. [Merci de nous contacter](#)

## Informations Complémentaires

Cette formation est également disponible sous forme de formation sur site. Veuillez nous contacter pour en savoir plus.