

### **Enterprise Computing Solutions - Education Services**

## NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com Phone: +420 597 488 811

# **SOPHOS** Sophos Certified Architect Central EndPoint und Server

Kód: DÉLKA: CENA:

SOP CACES 24 Hours (3 DENNÍ) Kč bez DPH 45,300.00

#### **Description**

Školení je vedeno virtuálně v anglickém jazyce.

Cena školení je 1 500 GBP bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem.

The course is available either online via the Partner 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.

It consists of presentations and practical lab exercises to reinforce the taught content, and electronic copies of the supporting documents for the course will be provided to each trainee through the online portal.

The course is expected to take 3 days (24 hours) to complete, of which approximately 9 hours will be spent on the practical exercises.

#### Cíle

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

Design an installation considering all variables

Undertake a multi-site installation appropriate for a customer environment

Explain the function of core components, how they work, and how to configure them

Track the source of infections and cleanup infected devices

Perform preliminary troubleshooting and basic support of customer environments

#### Určeno pro

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.

#### Vstupní znalosti

Prior to taking this training you should:

Have completed and passed the Sophos Central Endpoint and Server Protection - Certified Engineer course

We recommend students have the following knowledge and experience:

Experience with Windows networking and the ability to troubleshoot issues

A good understanding of IT security

Experience using the Linux command line for common tasks

Experience configuring Active Directory Group Policies

Experience creating and managing virtual servers or desktops

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

#### **Program**

Module 1: User Management (30 mins)
Review how users are added to Sophos Central
Explain how API credentials are created in Sophos Central
Enable and manage multi-factor authentication (MFA)
Install and configure the AD Sync Utility Tool
Configure Azure AD in Sophos Central
Labs (20 mins)
Register and activate a Sophos Central evaluation

Install and Configure AD Sync Utility Enable multi-factor authentication

Module 2: Deployment Scenarios (60 mins)

Identify some of the common challenges when deploying Central

**Deploy Update Caches** 

Set up Message Relays

Identify where Update Caches and Message Relays should be used

Identify common licensing requirements

Labs (60 mins)

Deploy Sophos protection to a Windows Server

Deploy an Update Cache and Message Relay

Module 3: Deployment (90 mins)

Identify the recommended steps for deploying Sophos Central

Explain the installation process of the Sophos Protection agent

Automate deployment for Windows, Linux, and Mac computers

Migration endpoints from Sophos Enterprise Console (SEC)

Remove third-party products as part of deployment

Use the Controlled Updates policies appropriately

Labs (90 mins)

Deploy Sophos protection to a Linux server

Prepare and deploy using an Active Directory Group

Complete the installation on DC and CLIENT

Enable manually controlled updates

Enable Server Lockdown (preparation for a later lab task)

Module 4: Protecting Virtual Servers (80 mins)

Deploy and manage Sophos for Virtual Environments

Deployment options for Azure hosted virtual servers

Deployment options for AWS hosted virtual servers

Optional Simulations (20 mins)

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** 

Simulation Labs (30 mins)

Configure automatic deployment for an Azure virtual server

Configure automatic deployment for an AWS virtual server

Module 5: Protection Features (120 mins)

Test and validate Endpoint Protection

Configure exclusions

Configure Data Loss Prevention

Configure Tamper Protection

Configure Server Protection Policies

Configure and Manage Server Lockdown

Set up File Integrity Monitoring

Labs (90 mins)

Prepare for a later lab task

Configure and test threat protection policies

Configure and test data control using CCLs

Configure and Test Exclusions

Configure and test Tamper Protection

Configure Sever Groups and Policies

Manage Server Lockdown

Test Linux Server Protection

Module 6: Logging and Reporting (45 mins)

Review why an alert will appear in Sophos Central

Identify the types of events

Remediate alerts and define alert notifications

Review which reports to use to run a health check

Export data from Sophos Central into a SIEM application

Locate client log files on Windows, Mac OS X and Linux

Labs (20 mins)

#### Configure SIEM with Splunk

Module 7: Managing Infections (45 mins)
Review the types of detections and their properties
Identify and use the tools available to manually cleanup malware
Explain how the quarantine works and manage quarantined items
Cleanup malware on a Linux server
Labs (40 mins)
Release a File from SafeStore
Disinfect a Linux Server

Module 8: Endpoint Detection and Response (80 mins)
Explain what EDR is and how it works
Demonstrate how to use threat cases
Explain Live Discover, data lake and pivoting
Use Live Discover to actively hunt threats
Explain how to use endpoint isolation for admin initiated and automatic isolation
Demonstrate how to create a forensic snapshot and interrogate the database
Explain how to use Live Response to perform IT administration tasks
Labs (45 mins)
Create a forensic snapshot and interrogate the database
Use Live Discover to locate unauthorized programs

#### Zkoušky a certifikace

To become a Sophos Certified Architect, trainees must take and pass an online assessment. The assessment tests their knowledge of both the presented and practical content. The pass mark for the assessment is 80% and is limited to 3 attempts.

#### Termíny školení

Termíny školení na vyžádání, kontaktujte nás prosím

#### Dodatečné informace

Školení je možné zajistit na míru. Kontaktujte nás pro bližší informace.