OVERVIEW

Professional Services for Sophos XDR Training

SOPHOS

Sophos XDR training - per person

Product Code:
PCEZTCCAA

SKU:
PRPCEA00ZZPCAA

SSU value:
1

This course is designed for technical professionals who will be administering Sophos Central and are looking to enhance their threat hunting skills using Sophos XDR.

This course is provided in a virtual classroom utilizing a Zoom meeting. This course is completed in one session and is expected to take up to 8 hours.

The training consists of presentations and practical lab exercises to reinforce the content taught. To access the training labs, you will need to allow outbound access from your network for RDP using TCP port 3389.

Objectives

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

- Understand modern cyber attacks
- Construct queries using the Sophos XDR interface
- Search for Indicators of Compromise (IOC)
- Trace the source of process, network, and file activity
- Query devices for vulnerabilities / missing patches
- Perform Threat Graph analysis and remediation
- Use Investigations to identify potential IOCs

Prerequisites

This course covers advanced concepts using the Live Discover from the Threat Analysis Center.

- Participants should be familiar with the Sophos Central Dashboard.
- Experience with Windows networking and the ability to troubleshoot issues.
- A good understanding of IT security.

Lab environment

Each participant will be provided with a pre-configured environment which simulates a company using Windows devices.

Sophos XDR training - single organization

This course is designed for technical professionals who will be administering Sophos Central and are looking to enhance their threat hunting skills using Sophos XDR.

This course is provided in a virtual classroom utilizing a Zoom meeting. This course is completed in one session and is expected to take up to 8 hours.

You can have up to 4 people from your team attend this training on the same day.

The training consists of presentations and practical lab exercises to reinforce the content taught. To access the training labs, you will need to allow outbound access from your network for RDP using TCP port 3389.

Product Code:
PR01SO00ZZPCAA

SKU:
PR01SO00ZZPCAA

SSU value:
Contact your Sophos representative to learn more.

Objectives

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

- Understand modern cyber attacks
- Construct queries using the Sophos XDR interface
- Search for Indicators of Compromise (IOC)
- Trace the source of process, network, and file activity
- Query devices for vulnerabilities / missing patches
- Perform Threat Graph analysis and remediation
- Use Investigations to identify potential IOCs

Prerequisites

This course covers advanced concepts using the Live Discover from the Threat Analysis Center.

- Attendees should be familiar with the Sophos Central Dashboard.
- Experience with Windows networking and the ability to troubleshoot issues.
- A good understanding of IT security.

Lab environment

Each participant will be provided with a pre-configured environment which simulates a company using Windows devices.

SOPHOS

To learn more please contact your Sophos representative or visit: sophos.com/professional-services

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

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

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

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

Updated November 2025