Professional Services for XDR Training

Updated October 2023

Contents

SKU – PRPCEA00ZZPCAA

XDR Training – Per Person

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.

It consists of presentations and practical lab exercises to reinforce the taught content.

Objectives

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

- Understand modern cyber attacks
- Construct queries using the 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 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 student will be provided with a pre-configured environment which simulates a company using Windows devices.

SKU - PR01SO00ZZPCAA

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 enrolled in the training.

It consists of presentations and practical lab exercises to reinforce the taught content.

Objectives

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

- Understand modern cyber attacks
- Construct queries using the 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 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 student will be provided with a pre-configured environment which simulates a company using Windows devices.

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