XDR Training - Single Organization

OEM: Sophos • Code: PR01SO00ZZPCAA

COURSE DESCRIPTION

Note: This service is only available in the EMEA region. 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. Services are delivered remotely using secure collaboration tools for teleconferencing and screen sharing. This course is provided in a virtual classroom utilizing a virtual 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.

AUDIENCE PROFILE

- This section doesn't contain any content.

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.

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- On completion of this course, participants 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

Module 1: Lab environment

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