

Sophos Taegis XDR Scenario Based Training

OEM: Sophos • Code: PROSVC-T-SBT-R / SKU: PSTW2E00ZZPCAA

COURSE DESCRIPTION

Scenario-Based Training (SBT) is an interactive workshop that enables your SecOps team to use Sophos Taegis XDR more efficiently and effectively in their continuous efforts to protect and defend your environment against threats faster and more efficiently. The scenarios for the SBT use current attack vectors aligned to tactics and techniques from the MITRE ATT&CK framework and use existing data in your XDR instance. Services are delivered remotely using secure collaboration tools for teleconferencing and screen sharing. This training will take up to 4 hours.

AUDIENCE PROFILE

- This section doesn't contain any content.

PREREQUISITES

- Participants should have completed the Taegis Analyst training prior to undertaking this session.

COURSE OBJECTIVES

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

- Each scenario includes the following:
 - Creating advanced searches.
 - Extracting Mitre tactics and techniques that Taegis identifies.
 - Creating and appending data to Investigations.
- One of our expert consultants facilitates the interactive workshop that consists of fictional attack scenarios based on current real-world threats. Your SecOps team uses your XDR instance—just like they would in their everyday tasks—to complete SecOps activities during the workshop.
- Participation in the SBT is highly recommended for enhancing understanding of functions and features available within XDR. A Sophos Engineer will challenge your SecOps team to demonstrate extensive use of XDR features and provide them with professional guidance to adopt and optimize XDR.
- During the SBT, your SecOps team will learn to effectively use XDR to do the following:
 - Develop and use advanced searches to collect primary artifacts and identify alert entities.
 - Conduct proactive security functions.
 - Create and update investigations.
 - Triage and investigate alerts.
 - Analyse telemetry using Taegis functionality.

- Report on investigation findings.

COURSE OUTLINE
