

Sophos Taegis XDR Advanced Search Training

OEM: Sophos • Code: PROSVC-T-ADT-R / SKU: PSTW2S00ZZPCAA

COURSE DESCRIPTION

The Advanced Search Training session provides deeper insight into the use of this core Taegis function to allow your resources to conduct the actions to fully utilize the Taegis Data Lake and perform proactive security actions like Threat Hunting. 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 session.

COURSE OBJECTIVES

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

- This interactive training session provides the following outcomes:
- Recap on Taegis Schema and Detectors
- Explaining Normalized Events vs Original Data
- Using Normalized fields in the Advanced Search
- Query vs Builder Advanced Search
- Options for configuring Time Ranges
- Overview & demonstration of Logical Types
- Overview & demonstration of Search Operators & Strings
- Overview & demonstration of Search Functions
- Creating and using Aggregated Searches
- Creating & sharing & saving Searches
- Creating Operational Reports
- Using the Advanced Search for Data Validation
- Using the Advanced Search for Alert Triage

