Sophos Taegis XDR Analyst Training

OEM: Sophos • Code: PROSVC-T-ANT-R / SKU: PSTW1E00ZZPCAA

COURSE DESCRIPTION

Sophos Taegis Analyst Training is an engineer run session which will provide fundamental insights into Alert and Investigation handling for Sophos Taegis XDR. These interactive sessions are designed to help your security professionals understand the analytical workflow of Taegis and how to explore the data it contains. 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

- This section doesn't contain any content.

COURSE OBJECTIVES

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

- Listed below are the planned topics for training platform administrators:
- Recap of Taegis XDR and its architecture
- Recap of Taegis XDR Schema Types
- Introduction to Taegis Detectors and Alerting
- MITRE ATT&CK Framework Overview and Taegis XDR applicability
- Overview of Taegis Event types
- Custom Rule Creation
- Working with Investigations
- Introducing Entities, Entity Graphs & Relationships
- Using Auto Investigations
- Alert Suppression in Taegis XDR
- Exploring the Taegis Data Lake with the Advanced Search
- Custom Dashboard and widget creation
- Creating operational reports using the Advanced Search
- Creating executive level reports using the Report Library

© Koenig Solutions

COURSE OUTLINE

© Koenig Solutions