

Sophos Taegis XDR Custom Parser Training

OEM: Sophos • Code: PROSVC-T-TCP-R / SKU: PSTW1N00ZZPCAA

COURSE DESCRIPTION

The Custom Parser Training session provides a blend of theory and practical application to teach Sophos Taegis operators how to analyse logs and create parsers for those data sources which are not currently supported within Sophos Taegis XDR. This interactive session will educate operators in how to integrate data sources into Taegis and then create the required parsers to align the ingested data with the relevant Taegis schema. An introduction into how to create parsers where attendees will be able to create example parsers based upon a fictional data source will also be included. 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 Administrator and Analyst training.

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
- Overview on Taegis Parsing
- Explaining Logs vs Events
- Explaining Taegis Custom Integration Options
- Overview on different types of log formats
- Proposed methodology for Parser Creation
- Example tooling to create Parsers
- Sampling & analysing logs
- Creating Parent & Standalone Parsers
- Creating Child Parsers
- Testing Parsers
- Validating Parsers using the Advanced Search

- Creating Custom Alerts

COURSE OUTLINE
