Endpoint Security Essentials – Monitoring and Reporting
Self-Paced Online Training

Highlights

Duration
1-hour

Who Should Attend
This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with system endpoint security.

Prerequisites
Students taking this course should have a working knowledge of Windows operating systems, system administration, and network technologies. Basic understanding of computer security, command line syntax, malware/anti-malware, virus/anti-virus, and web technologies is recommended. Prior experience or working knowledge of ePolicy Orchestrator is also required.

How to Register
This course is available for purchase at https://trellix-training.netexam.com

This course provides an in-depth introduction to the tasks you can perform to monitor and report on Trellix Endpoint Security (ENS). ENS provides dashboards, queries, reports, log files, and events to monitor your ENS deployment. Endpoint Security combines the Threat Prevention, Adaptive Threat Protection, Firewall, and Web Control modules to take immediate action against potentially dangerous applications, downloads, websites, and files. This course is designed as a practical starting point for someone who is new to supporting Endpoint Security.

Learning Objectives

- Use the Endpoint Security dashboards available on the ePolicy Orchestrator to monitor the ENS deployment and operations.
- Use ePolicy Orchestrator Queries and Reports to monitor and report on the operation of Endpoint Security.
- Access and use the Endpoint Security log files to troubleshoot the ENS deployment and analyze threat detections.
- View the Endpoint Security Event logs to monitor and analyze events that are detected in your environment.
- Use the Story Graph feature to analyze threats that have been detected in your environment.
- Use Protection Workspace to monitor and understand threat protection in an ePO managed environment.
- Monitor and report on security status using ePO dashboards, reports, and logs

Agenda at a Glance

1. Introduction
2. Dashboards, Queries, and Reports
3. Log Files and Events
4. Protection Workspace
5. Conclusion