Trellix EDUCATION SERVICES

Enterprise Security Manager Essentials for System Administrators

Self-Paced Online Training

Highlights

Duration

4 hours

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://training-catalog.trellix.com.

Introduction

Trellix Enterprise Security Manager (ESM provides near real-time visibility into the activity on all your systems, networks, databases, and applications. This enables you to detect, correlate, and remedy threats in minutes across your entire IT infrastructure. This course prepares Trellix SIEM engineers and analysts to understand, communicate, and use the features provided by Trellix Enterprise Security Manager. Through hands-on lab exercises, you will learn how to deploy, configure, and administer the Trellix SIEM solution.

Learning Objectives

After completing this course, learners should be able to:

- Review the installation and deployment options for ESM Server and devices.
- Recall how to add, import, and configure data sources.
- Navigate the ESM dashboard and create custom ESM data views.
- Recall how to modify default aggregation of events and flows to meet company requirements.
- Use correlation to identify events of interest, isolate correlated events, then modify the rule to suit requirements.
- Create and configure watchlists and alarms.
- Perform routine maintenance on ESM, including updates and clearing policy modifications and rule updates.
- Perform basic ESM product troubleshooting.

Who Should Attend

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

Course Outline

1. Introduction
2. Deployment
3. Configuration
4. Administration

Visit Trellix.com to learn more.