EDUCATION SERVICES

Detection and Prevention with Endpoint Security Expert Rules Essentials

Self-Paced Online Training

Highlights

Duration

3-hours

Who Should Attend

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

Prerequisites

- Working knowledge of Microsoft Windows administration
- Working knowledge of system administration concepts
- Basic understanding of computer security concepts
- General understanding of internet services
- Prior experience using Trellix Endpoint Security and Trellix ePolicy Orchestrator

How to Register

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

This course provides comprehensive training on the capability of ENS Expert Rules. Through video lectures and interactive activities you will learn how Expert Rules work, how to create and use them, and how to use and edit AAC-based Expert Rules.

Learning Objectives

After completing this course, learners should be able to:

- Define and describe Arbitrary Access Control (AAC) and legacy Host IPS based Expert Rules
- Use the ENS Console to create, check, and enforce rules
- Use aacinfo.exe and baretail.exe to investigate rule functionalities
- Use NOTEPAD++ to create and edit expert rules
- Design, develop, and test Expert Rules that block the creation of file, folder, process, and registry key

Agenda at a Glance

1. Course Introduction
2. Introducing Expert Rules
3. Writing Expert Rules
4. Using Expert Rules
5. Conclusion

Visit Trellix.com to learn more.

092023-13