Trellix

EDUCATION SERVICES

Enterprise Security Manager Advanced Topics

Instructor-Led Training

Highlights

Duration

4-days

Prerequisites

Students taking this course should have a working knowledge of networking and system administration concepts, a good understanding of computer security concepts, and a general understanding of networking and application software.

How to Register

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

Private sessions are available. For further details and pricing, please contact your Trellix account representative.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities. To view our full course catalog, please visit https://trellix-training.netexam.com.

This course prepares Trellix SIEM engineers and analysts to understand, communicate, and use the features provided by Trellix Enterprise Security Manager. Through demonstration, explanation, and hands-on lab exercises, you will learn how to utilize the Enterprise Security Manager by using Trellix-recommended best practices and methodologies.

Learning Objectives

After completing this course, learners should be able to:

- Review the ESM solution's abilities and configuration options
- Define and configure advanced data sources topics such as Asset Manager, Data Enrichment, Auto Learn, SIEM Collector, and Vulnerability Assessment
- Configure custom parsing rules
- Implement best practice recommendations in tuning ESM to enhance performance and events visibility
- Configure Deviation based correlation rules and utilize techniques for both Event and Risk-Based Correlation
- Make tuning recommendations according to your analysis and identify events for immediate action, delayed action, or no action
- Perform actions to maximize the usefulness of Enterprise Security Manager
- Create well-defined use cases and follow a process to implement them

Who Should Attend

This course is intended for Enterprise Security Manager users responsible for monitoring activity on systems, networks, databases, applications, and for configuration and management of the Enterprise Security Manager solution.

Course Outline

Day 1:

- Welcome
- Contextual Configurations
- Advanced Data Source Options
- Alarms, Actions, Notifications, and Reports

Day 2:

- Data Streaming Bus
- Advanced Syslog Parser
- ESM Tuning and Best Practices
- Performance Troubleshooting

Day 3:

- Advanced Correlation
- Analysts Tasks
- Use Case Overview
- Management Directives Use Cases

Day 4:

- Organizational Policies Use Cases
- Compliance Use Cases
- Current Threats and Vulnerabilities Use Cases
- Incident Identification Use Cases

Trellix

Visit Trellix.com to learn more.

092023-19