Trellix EDUCATION SERVICES

Enterprise Security Manager Administration

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 hands-on lab exercises, you will learn how to optimize the Enterprise Security Manager by using Trellix recommended best practices and methodologies.

Learning Objectives

- Define Trellix SIEM concepts, identify appliances, and describe the SIEM solution component architecture
- Navigate and configure the features provided in this release
- Add, import, and configure data sources
- Navigate Enterprise Log Manager (ELM) and configure settings and data storage
- Navigate Enterprise Log Search (ELS) and configure settings and searches
- Navigate the ESM UI dashboard and create custom ESM data views
- Locate events, filter data, and manage cases
- Modify default aggregation of events and flows to meet company requirements
- Navigate and configure the Policy Editor to closely reflect your actual environment
- Use correlation to identify events of interest, isolate correlated events, then modify the rule to suit requirements
- Create and configure watchlists and alarms
- Create and configure reports
- Perform routine maintenance on ESM, including updates and clearing policy modifications and rule updates
- Perform basic ESM product troubleshooting
- Describe High Availability and Disaster Recovery configuration techniques and design
- Practice using the ESM dashboards and views using real world examples

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
- Architecture Overview
- Devices and Settings
- ESM User Interface and Views

Day 2:

- Data Sources
- Working with the ELM and ELS
- Event Analysis
- Aggregation

Day 3:

- Watchlists and Policy Editor
- Query Filters
- Rule Correlation
- Alarms

Day 4:

- Workflow and Analysis
- Reports
- System Maintenance and Troubleshooting
- Introduction to Use Case Design

Trellix

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.

Copyright © 2023 Musarubra US LLC