Trellix

Trellix SIEM 11.6 Administration

Education Services Instructor-Led Training

Earn up to 32 CPEs after completing this course

Audience

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

Recommended Pre-Work

It is recommended that students have a working knowledge of networking and system administration concepts.

Related Courses

- Trellix SIEM Advanced

Learn More

To order, or for further information, please email SecurityEducation@trellix.com.

Trellix SIEM 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 optimize the Trellix Enterprise Security Manager by using Trellix recommended best practices and methodologies.

Learning Objectives

Trellix Enterprise Security Manager Overview
Define Trellix Enterprise Security Manager and SIEM concepts, identify appliances and their features, and describe the Trellix Enterprise Security Manager solution component architecture.

Devices
Configure and customize receiver data sources and data source profiles.

Trellix Enterprise Log Manager and Trellix Enterprise Log Search
Configure Trellix Enterprise Log Manager settings and mirror Trellix Enterprise Log Manager data storage.

Trellix Enterprise Security Manager Views
Effectively navigate the Trellix Enterprise Security Manager dashboard and create custom Trellix Enterprise Security Manager data views.

Data Sources
Locate events and manage cases using a variety of data sources, assets, and enriched data.

Aggregation
Customize event and flow aggregation fields on a per- signature basis, and define the advantages and nuances associated with event and flow aggregation.

Policy Editor
Create, modify, and delete Trellix Enterprise Security Manager policies within the policy editor.

Query Filters

Apply filters in views, create filter sets, use string normalization, and understand the basic syntax of regular expressions.

Correlation

Configure and deploy custom correlation rules within the correlation editor.

Watch Lists and Alarms

Create and configure watch lists and alarms.

Reports

Create and configure reports.

System Management

Perform routine maintenance on Trellix Enterprise Security Manager, including updates and clearing policy modifications and rule updates.

Troubleshooting

Perform troubleshooting steps associated with login issues, operating systems and browser-specific issues, hardware issues, and Enterprise Security Manager dashboard issues.

Use Case Design

Understand how the Trellix Enterprise Security Manager interface dashboards and views are used to identify specific events and incidents.

Agenda at a Glance

Day 1:

- Course Introduction
- Architecture Overview
- Devices and Settings
- ESM Interface and Views

Day 2:

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

Days 3:

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

Days 4:

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

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.