# Trellix SIEM 11.6 Advanced

## 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 Administration

### Learn More

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

Trellix Enterprise Security Manager—the heart of our Security Information and Event Management (SIEM) solution—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 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

### Contextual Configurations

Utilize Asset Manager and how to manage assets and asset groups. Define and configure data enrichment using the Data Enrichment Wizard and Integrate vulnerability assessment (VA) tool with ESM.

### Advanced Data Sources

Configure Auto Learn to listen to incoming events after installing and configuring the SIEM Collector Agent.

### Alarms, Actions, and Notifications

Describe alarms, build and edit templates, use remote commands, create report queries, and configure notifications.

### Data Streaming Bus

Display adding Data Streaming Databus (DSB) and configuring data routing, data sharing, and creating message forwarding rules.

### Advanced Syslog Parser

Understand Regex and available resources. Discussion on handling of unknown events and creating custom parsing rules.

### Aggregation

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

### Current Threat and Vulnerability Use Cases

Research current threats and vulnerabilities. Create use cases from current threats and vulnerabilities.

### ESM and Tuning Best Practice

Learn Event Tuning methodology. Configure events filtering on ERC and Identify key strategies for tuning correlation rules. Learn best practice to enhance ESM performance.

### Advanced Correlation

Utilize advanced rule correlation options and deviation-based rule correlation and risk correlation.

## Agenda at a Glance

**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

**Days 3:**

- Advanced correlation
- Analyst tasks
- Use case overview
- Management directives use cases

**Days 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.