Trellix

DATASHEET

Enterprise Security Manager Administration 201

Education Services Instructor-led Training

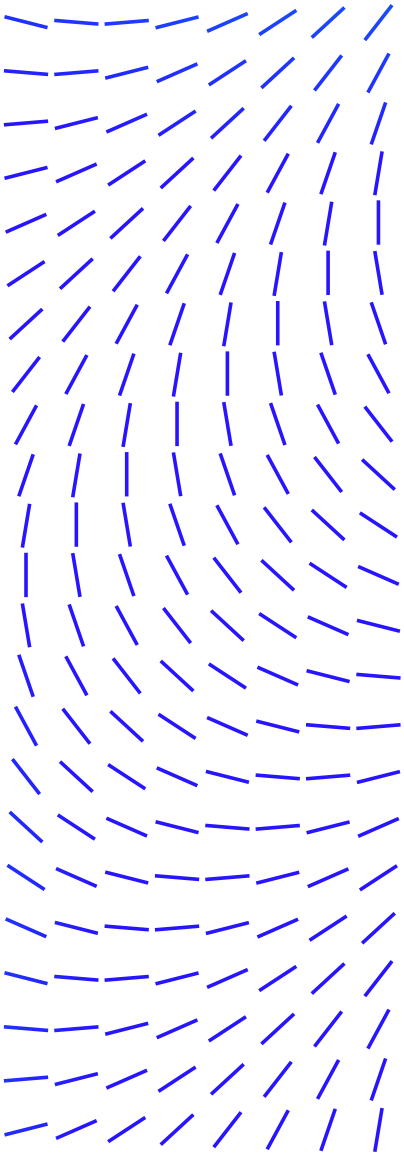
Introduction

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 Enterprise Security Manager 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 recommended best practices and methodologies.

> This course continues to prepare Enterprise Security Manager engineers and analysts to understand, communicate, and use the features provided by Enterprise Security Manager

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.



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 Practice
- Performance Troubleshooting

Day 3

- Advanced Correlation
- Analyst 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

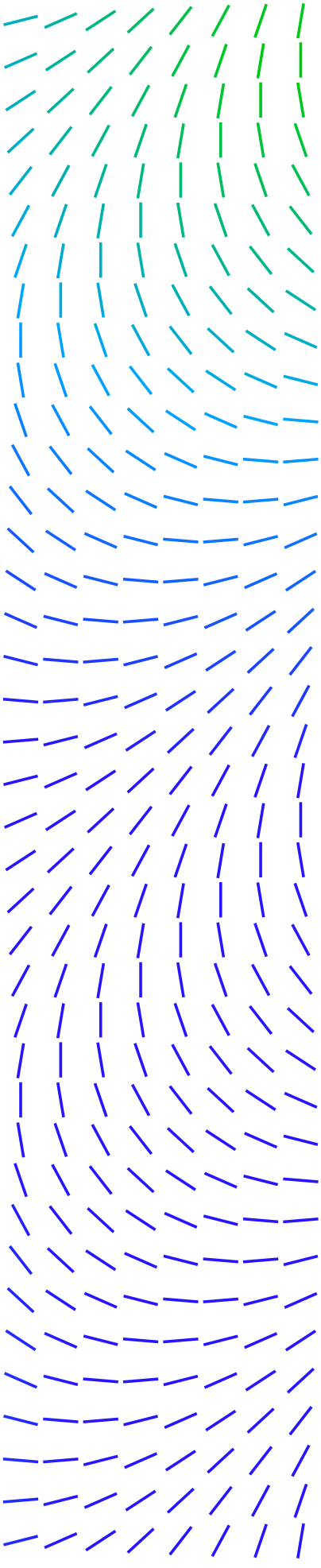
Course Learning Objectives

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, 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.

Analyst Tasks

Make tuning recommendations according to your analysis while Identifying events for immediate action, delayed action and no action (triage).

Use Case Overview

Define use cases and follow a process to develop well defined use cases.

Management Event Use Cases

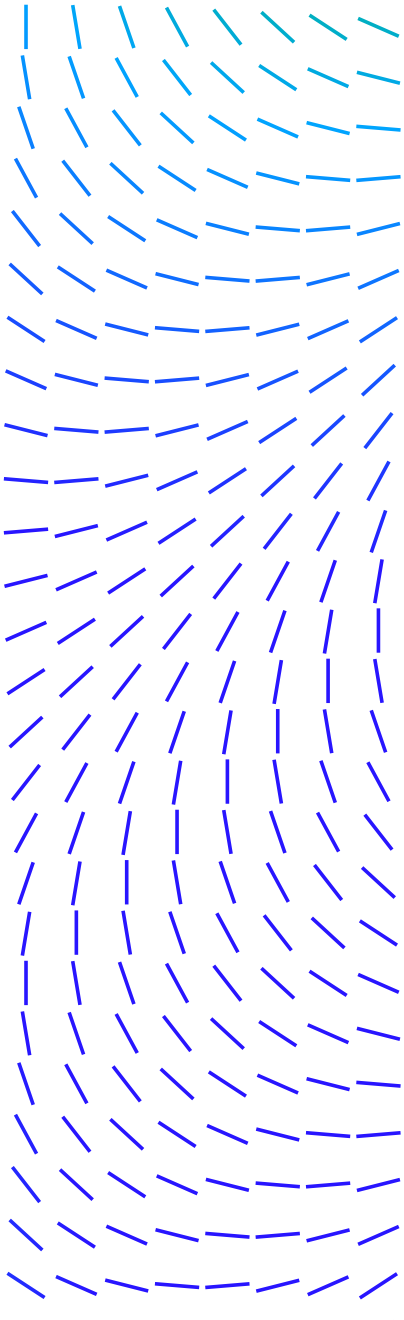
Create use cases from management directives.

Organizational Use Case Policies

Create use cases from organizational policies

Recommended Pre-Work

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



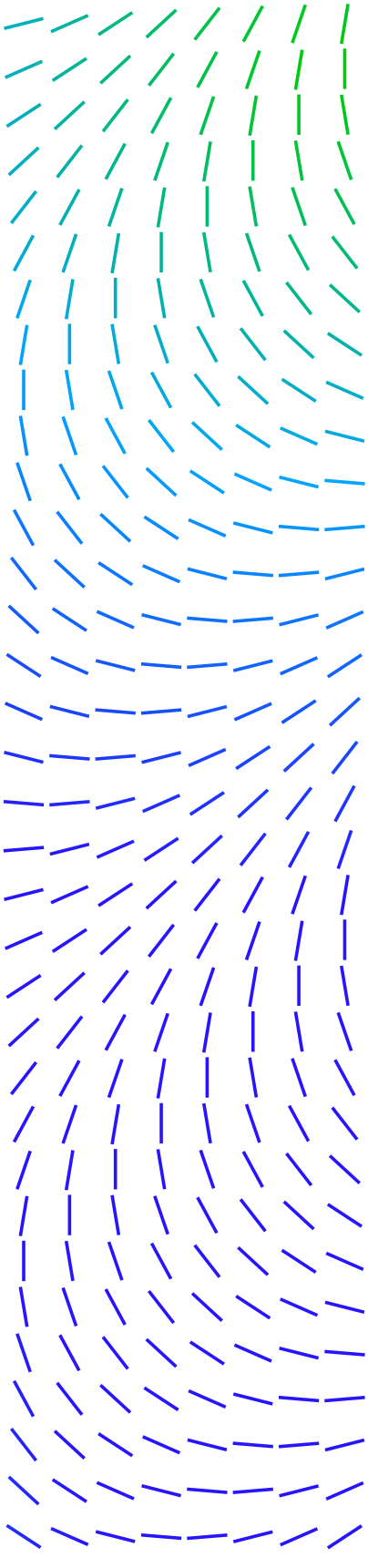
Compliance Use Cases

Create use cases from regulations to validate compliance.

Incident Identification Use Cases

Create use cases to quickly identify previously remediated incidents.

.



DATASHEET

Trellix