Trellix

DATASHEET

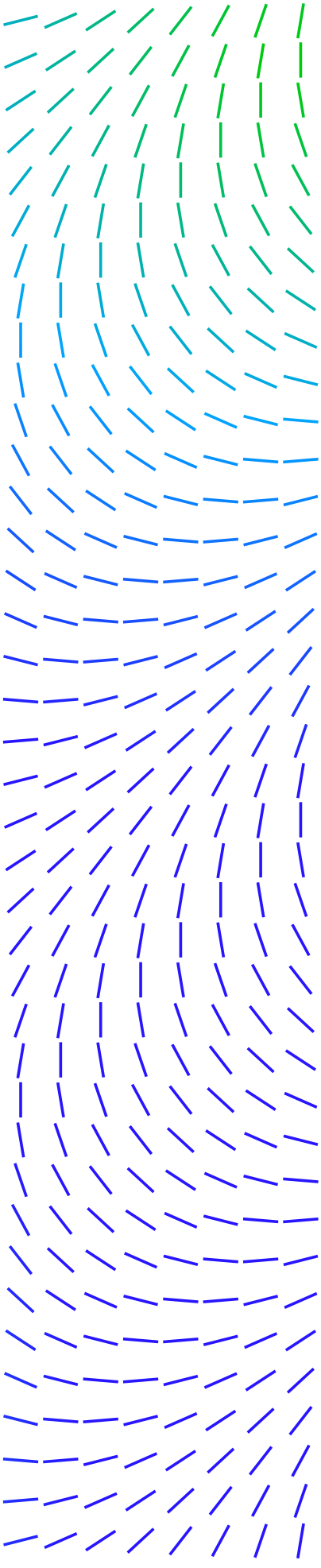
Enterprise Security Manager Administration 101

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

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



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

Day 3

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

Day 4

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

Course Learning Objectives

Enterprise Security Manager Overview

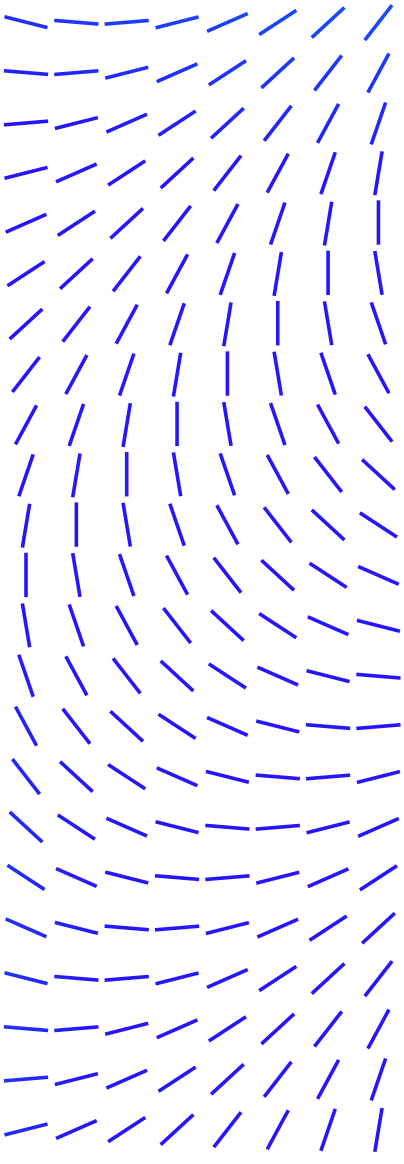
Define Enterprise Security Manager and SIEM concepts, identify appliances and their features, and describe the Enterprise Security Manager solution component architecture.

Devices

Configure and customize receiver data sources and data source profiles.

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.



Enterprise Log Manager and Enterprise Log Search

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

Enterprise Security Manager Views

Effectively navigate the Enterprise Security Manager dashboard and create custom 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 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

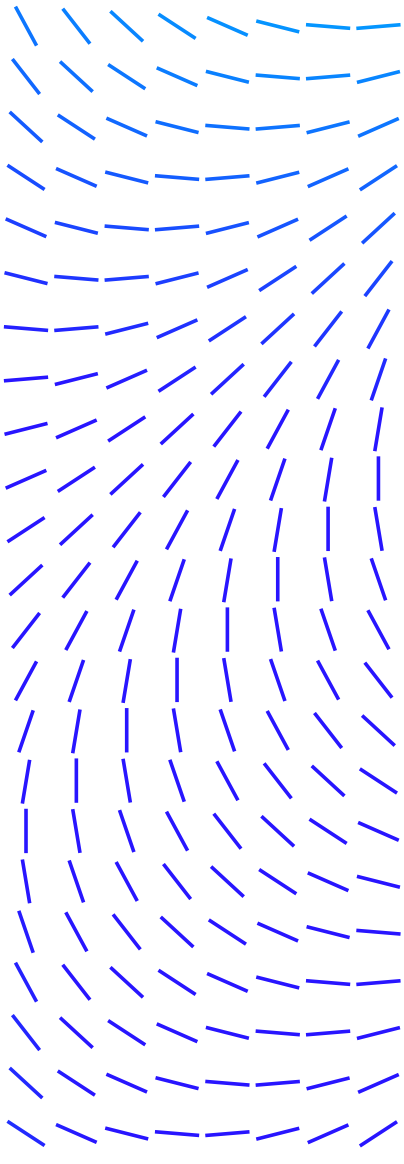
Perform routine maintenance on Enterprise Security Manager, including updates and clearing policy modifications and rule updates.

Recommended Pre-Work

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

Related Courses

- Enterprise Security Manager Administration 201



Troubleshooting

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

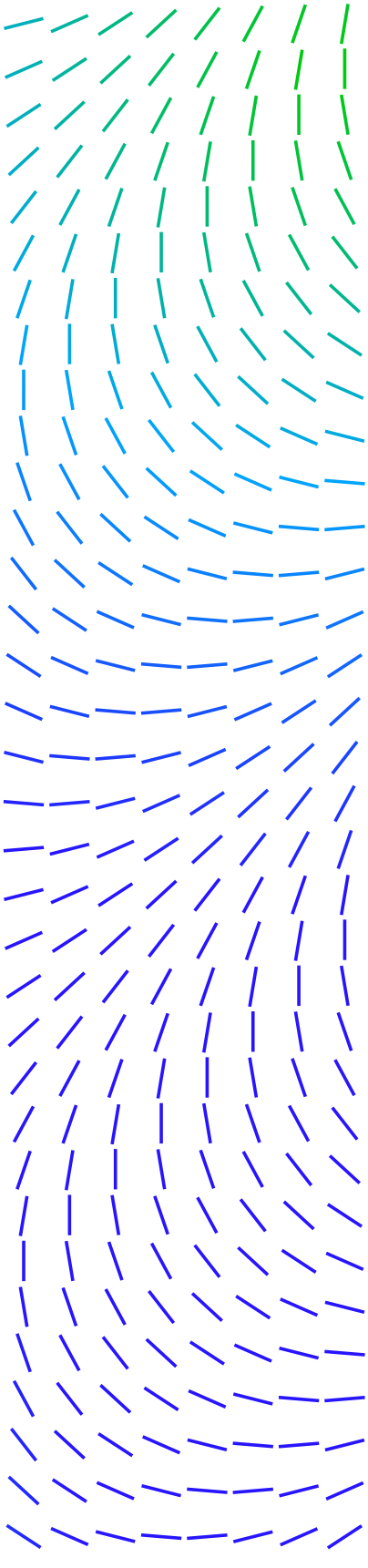
Use Case Design

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

.

Trellix

Copyright © 2022 Musarubra US LLC



DATASHEET

Trellix

Copyright © 2022 Musarubra US LLC