

McAfee Enterprise Security Manager for Engineers-I

Education Services Instructor-led Training

McAfee® 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 McAfee Enterprise Security Manager engineers to understand, communicate, and use the features provided by McAfee Enterprise Security Manager. Through hands-on lab exercises, you will learn how to optimize the McAfee Enterprise Security Manager by using McAfee-recommended best practices and methodologies. **Earn up to 32 CPEs after completing this course.**

Audience

This course is aimed at McAfee customers acting as McAfee Enterprise Security Manager engineers, responsible 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

- Course Introduction
- McAfee Enterprise Security Manager Overview
- Devices
- McAfee Enterprise Log Manager and McAfee Enterprise Log Search

Day 3

- Query Filters
- Correlation
- Watch Lists and Alarms
- Reports

Day 2

- McAfee Enterprise Security Manager Views
- Data Sources
- Aggregation
- Policy Editor

Day 4

- System Management
 - Troubleshooting
 - Redundancy
 - Wrap-Up Scenario
-

COURSE DESCRIPTION

Learning Objectives

McAfee Enterprise Security Manager Overview

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

Devices

Configure and customize receiver data sources and data source profiles.

McAfee Enterprise Log Manager and McAfee Enterprise Log Search

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

McAfee Enterprise Security Manager Views

Effectively navigate the McAfee Enterprise Security Manager dashboard and create custom McAfee 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 McAfee Enterprise Security Manager policies within the policy editor.

Query Filters

Apply filters in views and create filter sets.

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 McAfee 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.

COURSE DESCRIPTION

Troubleshooting

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

Redundancy

Understand high-availability and disaster recovery configuration techniques and design.

Wrap-Up Scenario

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

Related Courses

- McAfee Enterprise Security Manager for Engineers-II
- McAfee Enterprise Security Manager for Analysts-I
- McAfee Enterprise Security Manager for Analysts-II

Learn More

To order, or for further information, please call 1 888 847 8766 or email SecurityEducation@mcafee.com.



2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 3020_0517
MAY 2017