COURSE DESCRIPTION

McAfee Enterprise Security Manager for Engineers-II

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 Solution 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 Enterprise Security Manager engineers, responsible for configuration and management of their McAfee Enterprise Security Manager solution. Attendees should have at least one year of experience managing the McAfee Enterprise Security Manager Solution.

Agenda at a Glance

Day 1
- Course Introduction
- McAfee Security Manager Overview
- McAfee Enterprise Security Manager Views

Day 2
- Data Sources
- Policy Editor

Day 3
- Query Filters
- Correlation
- Alarms, Actions, and Reports

Day 4
- Troubleshooting
- Workflow and Final Exam

Learning Objectives

McAfee Enterprise Security Manager Overview

Review the McAfee Enterprise Security Manager solution's abilities and configuration.

McAfee Enterprise Security Manager Views

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

Data Sources

Configure advanced Data Source settings, such as Auto-Learning Data Sources, Assets, Data Enrichment, and Case Management.

Policy Editor

Use the Policy Editor to configure Rules, Rule Filtering, Normalization, Aggregation, Variables, and Tuning.

Query Filters

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

Correlation

Utilize Optimized Risk Management techniques for both Event and Risk-Based Correlation and Historical correlation to manage the Correlation Engines.

Alarms, Actions, and Reports

Become aware of what is happening in your environment by configuring alarms, actions, reports, and watch lists.

Troubleshooting

Review key elements such as Logs, Commands, and Actions that can be taken to resolve issues.

Workflow and Final Exam

Apply knowledge learned in a hands-on practical final exam.

Recommended Pre-Work

It is recommended that students have completed the McAfee Enterprise Security Manager for Engineers-I course and have at least one-year of experience using McAfee Enterprise Security Manager appliances.

Related Courses

- McAfee Enterprise Security Manager for Engineers-I
- 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**.

McAfee
Together is power.

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