COURSE DESCRIPTION

McAfee Enterprise Security Manager for Analysts-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 analysts 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.**

Agenda at a Glance

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

Day 2
- McAfee Application Data Monitor and McAfee Database Event Monitor
- Aggregation
- Policy Editor

Day 3
- Query Filters
- Correlation
- Watch Lists and Alarms

Day 4
- Reports
- McAfee Enterprise Log Manager and McAfee Enterprise Log Search
- Wrap-Up Scenario

Audience

This course is aimed at McAfee customers acting as McAfee Enterprise Security Manager analysts, responsible for monitoring activity on systems, networks, databases, and applications using the McAfee Enterprise Security Manager solution. Attendees should have a good understanding of computer security concepts and a general understanding of networking and application software.

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.

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.

McAfee Application Data Monitor and McAfee Database Event Monitor

Differentiate between McAfee Application Data Monitor and McAfee Database Event Monitor features, and use McAfee Application Data Monitor and McAfee Database Event Monitor data sources to locate specific events.

Aggregation

List and define the advantages and nuances associated with event and flow aggregation.

Policy Editor

Navigate the McAfee Enterprise Security Manager Policy Editor, and describe how advanced syslog parser rules parse events received over syslog.

Query Filters

Apply filters in views, create filter sets, use string normalization, and understand the basic syntax of regular expressions.

Correlation

Design complex correlation rules for multiple use cases.

Watchlists and Alarms

Create and configure watch lists and alarms.

Reports

Create and configure reports.

McAfee Enterprise Log Manager and McAfee Enterprise Log Search

Search the McAfee Enterprise Log Manager and McAfee Enterprise Log Search for events information.

Wrap-Up Scenario and Final Exam

Use the McAfee Enterprise Security Manager dashboards and views to identify specific events such as theft of confidential information and use of weak passwords.

Recommended Pre-Work

It is recommended that students understand their role as an analyst and are familiar with McAfee Enterprise Security Manager and SIEM terminology.

Related Courses

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