COURSE DESCRIPTION

McAfee Enterprise Security Manager for Analysts-II

Education Services Instructor-led Training

McAfee® Enterprise Security Manager—the heart of our security information and event management (SIEM) appliances—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 lab exercises, you will learn how to plan, design, and document the McAfee Enterprise Security Manager use cases by implementing 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 Interface Views
- Analyst Tasks

Day 2
- Use Cases Overview
- Use Cases Related to Management Directives

Day 3
- Use Cases Related to Organizational Policy
- Use Cases Related to Compliance

Day 4
- Use Cases Related to Current Threats
- Use Cases Related to Incident Identification

Audience

This course is aimed at McAfee customers acting as McAfee Enterprise Security Manager analysts, responsible for the planning, design, and documentation of use cases. 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 Interface Views

Effectively navigate the McAfee Enterprise Security Manager Interface desktop, and create custom McAfee Enterprise Security Manager data views.

Analyst Tasks

Make tuning recommendations according to your analysis, identify events for immediate action, delayed action or no action, and perform actions to maximize the usefulness of McAfee Enterprise Security Manager output.

Use Cases Overview

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

Use Cases Related to Management Directives

Create use cases from management directives related to sensitive data exfiltration and file deletion.

Use Cases related to Organizational Policy

Create use cases from organizational policies around email controls, web controls, denial-of-service (DoS) events and logs.

Use Cases Related to Compliance

Create use cases from regulations to validate compliance.

Use Cases Related to Current Threats

Research current threats and vulnerabilities and create use cases from your research.

Use Cases Related to Incident Identification

Investigate incidents and create use cases to quickly identify previously remediated incidents.

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.
- Students should attend the McAfee Enterprise Security Manager Analyst-I course prior to attending this course.

Related Courses

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