Course Description

McAfee Enterprise Security Manager for Engineers-II

Education Services Instructor-led Training

Earn up to 32 CPEs after completing this course

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 Enterprise Security Manager Engineers 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 Solution by using McAfee-recommended best practices and methodologies.

Agenda At A Glance

Day 1

- Course Introduction
- Overview, Installation, and Configuration
- Enterprise Security Manager Interface Views

Day 2

- Data Sources
- Policy Editor

Agenda At A Glance (continued)

Day 3

- Query Filters
- Correlation
- Alarms, Watchlists, and Actions

Day 4

- Troubleshooting
- Workflow and Final Exam

Audience

Intel® Security Customers, acting as Enterprise Security Manager Engineers, responsible for configuration and management of their Enterprise Security Manager Solution. Attendees should have at least one year of experience managing the Enterprise Security Manager Solution.

intel Security

Course Description

Learning Objectives

Overview, Installation, and Configuration
Review the Enterprise Security Manager Solution's abilities and configuration.

Enterprise Security Manager Interface Views
Effectively navigate the Enterprise Security Manager Interface desktop, and create custom 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, Watchlists, and Actions
Become aware of what is happening in your environment by configuring alarms, actions, reports, and watchlists.

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 Enterprise Security Manager for Engineers-I course and have at least one-year of experience using McAfee Enterprise Security Manager appliances.

Related Courses

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

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

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com