Course Description

McAfee Enterprise Security Manager for Engineers-I

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 by using McAfee-recommended best practices and methodologies.

Agenda At A Glance

Day 1

- Course Introduction
- Enterprise Security Manager Overview
- Devices
- Enterprise Log Manager

Day 2

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

Agenda At A Glance (continued)

Day 3

- Query Filters
- Correlation
- Alarms and Watchlists
- Reports

Day 4

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

Audience

Intel® Security Customers, acting as 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.

intel Security

Course Description

Learning Objectives

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

Devices
Configure and customize receiver data sources and data source profiles.

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

Enterprise Security Manager Interface Views
Effectively navigate the Enterprise Security Manager Interface desktop, and create custom 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 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.

Alarms and Watchlists
Create and configure Alarms and Watchlists.

Reports
Create and configure reports.

System Management
Perform routine maintenance on Enterprise Security Manager, including updates and clearing policy modifications and rule updates.

Troubleshooting
Perform troubleshooting steps associated with login issues, operating systems and browser specific issues, hardware issues, and Enterprise Security Manager Interface issues.

High Availability
Understand High Availability and Disaster Recovery configuration techniques and design.

Wrap-Up Scenario
Understand how the Enterprise Security Manager Interface Dashboards and Views are used to identify specific events and incidents.

Recommended Pre-Work

- It is recommended that students have a working knowledge of networking and system administration concepts.

Related Courses

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

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