Course Description

McAfee Enterprise Security Manager for Analysts-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 Analysts to understand, communicate, and use the features provided by McAfee Enterprise Security Manager. Through hands-on lab exercises, you will learn how to utilize Enterprise Security Manager by using McAfee-recommended best practices and methodologies.

Agenda At A Glance

Day 1

- Course Introduction
- Enterprise Security Manager Overview
- Enterprise Security Manager Interface Views
- Data Sources

Day 2

- Application Data Monitor and Database Event Monitor
- Aggregation
- Policy Editor

Agenda At A Glance (continued)

Day 3

- Query Filters
- Correlation
- Alarms and Watchlists

Day 4

- Reports
- Enterprise Log Manager
- Wrap-Up Scenario and Final Exam

Audience

Intel® Security Customers, acting as 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.

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.

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.

Application Data Monitor and Database Event Monitor
Differentiate between Application Data Monitor and Database Event Monitor features, and use Application Data Monitor and 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 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.

Alarms and Watchlists
Create and configure Alarms and Watchlists.

Reports
Create and configure reports.

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

Wrap-Up Scenario and Final Exam
Use the Enterprise Security Manager Interface 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 Enterprise Security Manager and SIEM terminology.

Related Courses

- Enterprise Security Manager for Engineers-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