COURSE DESCRIPTION

McAfee Enterprise Security Manager Administration 201

McAfee® 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 provides attendees with hands-on training on the design, setup, configuration, communication flow, and data source management of the McAfee Enterprise Security Manager appliances. In addition, the course prepares McAfee Enterprise Security Manager analysts to use and communicate the features provided by the solution. Through hands-on lab exercises and use case scenarios, you will learn how to optimize the solution by using McAfee-recommended best practices and methodologies.

Earn up to 32 CPEs after completing this course.*

* Student must self-report for CPE credits. We cannot guarantee any specific quantity, as it is up to the program or certification group to determine what they will or will not accept.

Agenda at a Glance

Day 1
- Welcome
- Contextual Configurations
- Advanced Data Source Options
- Alarms, Actions, Notifications, and Reports

Day 2
- Data Streaming Bus
- Advanced Syslog Parser
- McAfee Enterprise Security Manager Tuning and Best Practice
- Performance Troubleshooting

Audience

This course is aimed at McAfee customers acting as McAfee Enterprise Security Manager engineers who are responsible for configuration and management of the solution and also for McAfee Enterprise Security Manager analysts who are responsible for monitoring activity on systems, networks, databases, and applications. Attendees should have a good understanding of computer security concepts and a general understanding of networking and application software. Attendees should have at least one year of experience managing the McAfee Enterprise Security Manager solution.

Connect With Us

Agenda at a Glance

Day 3
- Advanced Correlation
- Analyst Tasks
- Use Case Overview
- Management Directives Use Cases

Day 4
- Organizational Policies Use Cases
- Compliance Use Cases
- Current Threats and Vulnerabilities Use Cases
- Incident Identification Use cases

Learning Objectives

Contextual Configurations

Review McAfee Enterprise Security Manager architecture and configuration tasks. Define Asset Manager and how to manage assets and asset groups. Define and configure data enrichment using the Data Enrichment Wizard. Integrate vulnerability assessment (VA) tool with McAfee Enterprise Security Manager.

Advanced Data Source Options

Configure Auto Learn to listen to incoming events. Install and configure the SIEM Collector Agent.

Alarms, Actions, Notifications, and Reports

Build and edit advanced alarms. Build and edit templates. Use remote commands. Create report queries. Configure notifications.

Data Streaming Bus

Review the benefits of the Data Streaming Bus device. Add Data Streaming Databus (DSB). Configure Data Routing. Configure Data Sharing. Create Message Forwarding Rules.

Advanced Syslog Parser

Understand Regex and available resources. Understand how to handle unknown events. Create custom parsing rules.

McAfee Enterprise Security Manager Tuning and Best Practice

Understand Event Tuning methodology. Configure events filtering on McAfee® Event Receiver (McAfee ERC). Identify key strategies for tuning correlation rules. Apply best practice to enhance McAfee Enterprise Security Manager performance.

Performance Troubleshooting

Discuss common performance issues. Describe possible causes and fixes. Learn how to avoid performance issues.

Advanced Correlation

Utilize advanced rule correlation options. Configure deviation-based rule correlation. Configure risk correlation.

Recommended Pre-Work

It is recommended that students have a working knowledge of:
- McAfee Enterprise Security Manager (SIEM)
- Networking and system administration concepts
- Moderate understanding of computer security concepts
- Experience with network security concepts and practices

Related Courses

- McAfee Enterprise Security Manager Administration 101 (pre-requisite)

COURSE DESCRIPTION

Analyst Tasks

Make tuning recommendations according to your analysis. Identify events for immediate action, delayed action and no action (triage). Perform actions to maximize the usefulness of McAfee Enterprise Security Manager output.

Use Cases Overview

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

Management Directives Use Cases

Create use cases from management directives.

Compliance Use Cases

Create use cases from regulations to validate compliance.

Current Threat and Vulnerability Use Cases

Research current threats and vulnerabilities. Create use cases from current threats and vulnerabilities.

Incident Use Cases

Investigate incidents. Create use cases to quickly identify previously remediated incidents.

Learn More

To order, or for further information, please email SecurityEducation@mcafee.com.

McAfee

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com