Course Description

McAfee Active Response Administration 2.0

Education Services Instructor-led Training

Earn up to 16 CPEs after completing this course

Our McAfee® Active Response Administration 2.0 course provides an in-depth introduction to the tasks crucial to set up and administer McAfee Active Response. McAfee Active Response is part of the Endpoint Threat Defense and Response solution and provides unified security components that work together through an open, integrated approach with shared visibility, threat intelligence, and simplified work flows. This course combines lectures and practical lab exercises, with significant time allocated for hands-on interaction with the McAfee Active Response user interface, as well as detailed instructions for installing and configuring this solution.

Agenda At A Glance

Day 1

- Welcome
- Solution Overview
- Planning the Deployment
- Installing McAfee Active Response Software
- Deploying McAfee Active Response Clients
- Configuring McAfee Active Response

Agenda At A Glance (continued)

Day 2

- Using the McAfee Active Response Threat Workspace, Health Status, and Remediation History
- Managing Policies, Collectors, Searches, Reactions, and Triggers

Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with system endpoint security.

Course Description

Learning Objectives

Welcome
Become familiar with McAfee information and support resources and feedback mechanisms.

Solution Overview
Describe the McAfee Active Response solution, its features, and its functionality.

Planning the Deployment
Describe the business, software, hardware, and component requirements to consider when planning deployment.

Installing McAfee Active Response Software
Describe how to add McAfee Active Response extensions to the McAfee ePolicy Orchestrator® (McAfee ePO™) server and how to configure McAfee ePO proxy server and McAfee ePO Cloud Bridge server settings.

Deploying McAfee Active Response Clients
Describe the ways to deploy the software to endpoints, deploy it, and verify the success of the deployment.

Configuring McAfee Active Response
Describe how to configure the McAfee Active Response service from McAfee ePO, how to use McAfee ePO policies to configure McAfee Active Response, and the permission sets that McAfee Active Response creates to manage access to its resources.

Using the McAfee Active Response Threat Workspace, Health Status, and Remediation History
Describe the Threat Workspace, how to use the Threat Workspace's timeline to see what the malware did, how to kill or leave threats and mark them as malicious or trustworthy, along with describing the Health Status dashboard and the Remediation History screen.

Managing Policies, Collectors, Searches, Reactions, and Triggers
Describe how to use policies, collectors, search, reactions, and triggers, and describe how McAfee Active Response is useful in the Incident Response Lifecycle.

Recommended Pre-Work

- Solid knowledge of Windows, system administration, and network technologies.
- Solid knowledge of computer security, command line syntax, malware/anti-malware, virus/antivirus, and web technologies.
- Prior experience using McAfee ePO software.

Related Courses

- McAfee ePolicy Orchestrator Administration
- McAfee Endpoint Security Administration

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

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