

Protecting Against Malware Threats with Cisco AMP for Endpoints v5.0

Course#: SSFAMP
Duration: 3 Days
Price: 0.00

Course Description

Through expert instruction and hands-on lab exercises, the SSFAMP - Protecting Against Malware Threats with Cisco AMP for Endpoints v5.0 course will teach how to implement and use this powerful solution through a number of step-by-step attack scenarios. You'll learn how to build and manage a Cisco AMP for Endpoints deployment, create policies for endpoint groups, and deploy connectors. You will also analyze malware detections using the tools available in the AMP for Endpoints console.

Objectives

- Identify the key components and methodologies of Cisco Advanced Malware Protection (AMP)
- Recognize the key features and concepts of the AMP for Endpoints product
- Navigate the AMP for Endpoints console interface and perform first-use setup tasks
- Identify and use the primary analysis features of AMP for Endpoints
- Use the AMP for Endpoints tools to analyze a compromised host
- Describe malware terminology and recognize malware categories
- Analyze files and events by using the AMP for Endpoints console and be able to produce threat reports
- Use the AMP for Endpoints tools to analyze a malware attack and a ZeroAccess infection
- Configure and customize AMP for Endpoints to perform malware detection
- Create and configure a policy for AMP protected endpoints
- Plan, deploy, and troubleshoot an AMP for Endpoints installation
- Describe the AMP Representational State Transfer (REST) API and the fundamentals of its use
- Describe all the features of the Accounts menu for both public and private cloud installations

Audience

Security administrators

Security consultants
Network administrators
Systems engineers
Technical support personnel
Cisco integrators, resellers, and partners

Prerequisites

Technical understanding of TCP/IP networking and network architecture
Technical understanding of security concepts and protocols

Understanding Networking Fundamentals

CCNA-Implementing and Administering Cisco Solutions v1.0 Boot Camp

Content

Classroom Live Outline

Introduction to Cisco AMP Technologies
AMP for Endpoints Overview and Architecture
Console Interface and Navigation
Using AMP for Endpoints
Detecting an Attacker A Scenario
Modern Malware
Analysis
Analysis Case Studies
Outbreak Control
Endpoint Policies
AMP REST API
Accounts

Classroom Live Labs

Request Cisco AMP for Endpoints User Account (e-learning version only)

Accessing AMP for Endpoints

Attack Scenario

Attack Analysis

Analysis Tools and Reporting

Zbot Analysis

Outbreak Control

Endpoint Policies

Groups and Deployment

Testing Your Policy Configuration

REST API

User Accounts (optional)