Course Outline

The Protecting Against Malware Threats with Cisco AMP for Endpoints v6.0
Course SSFAMP: 3 days Instructor Led

All Cisco courses are delivered by a Cisco Authorized Platinum Learning Partner

About this course
Protecting Against Malware Threats with Cisco AMP for Endpoints (SSFAMP) v6.0 is a 3-day course that shows you how to deploy and use Cisco® AMP for Endpoints, a next-generation endpoint security solution that prevents, detects, and responds to advanced threats. Through expert instruction and hands-on lab exercises, you will learn 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, Cisco Threat Grid, and the Cisco Orbital Advanced Search Tool.

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

At course completion
After completing this course, students will be able to:
- 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
- Analyze files and events by using the AMP for Endpoints console and be able to produce threat reports
- 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
- Use Cisco Orbital to pull query data from installed AMP for Endpoints connectors.
- 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

Course Outline

- Introducing to Cisco AMP Technologies
- Introducing AMP for Endpoints Overview and Architecture
- Navigating the Console Interface
- Using Cisco AMP for Endpoints
- Identifying Attacks
- Analyzing Malware

Course Outline

- Managing Outbreak Control
- Creating Endpoint Policies
- Working with AMP for Endpoint Groups
- Using Orbital for Endpoint Visibility
- Introducing AMP REST API
- Navigating Accounts

Lab Outline

- AMP Account Self-Registration
- Accessing AMP for Endpoints
- Attack Scenario
- Analysis Tools and Reporting
- Outbreak Control
- Endpoint Policies
- Groups and Deployment
- Testing Your Configuration
- Endpoint Visibility Using Orbital
- REST API
- Endpoint Isolation Using Cisco AMP API
- User Accounts