View Full Course Details including Latest Schedule Online

CISCO

SSFAMP v5.0 Certification Training

Due to Covid-19 safety restrictions PhoenixTS will temporarily be unable to provide food to our students who attend class at our Training Center; however, our Break Areas are **currently open** where students will find a constant supply of Coffee, Tea and Water. Students may bring their own lunch and snacks to eat in our breakrooms or at their seat in the classroom or eat out at one of the many nearby restaurants.

Course Overview

Our 3 day, instructor led SSFAMP (Protecting Against Malware Threats with Cisco AMP for Endpoints v5.0) training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online 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.

After taking this course, you should be able to:

- 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

Schedule

Currently, there are no public classes scheduled. Please contact a Phoenix TS Training Consultant to discuss hosting a private class at 240-667-7757.

Course 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

Lab Outline

- 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)

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Due to Covid-19 safety restrictions PhoenixTS will temporarily be unable to provide food to our students who attend class at our Training Center; however, our Break Areas are **currently open** where students will find a constant supply of Coffee, Tea and Water. Students may bring their own lunch and snacks to eat in our breakrooms or at their seat in the classroom or eat out at one of the many nearby restaurants.

Starting at **$3,000**

ATTENTION

For GSA pricing or Contractor quotes call 240.667.7757

GSA

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

10420 Little Patuxent Parkway Suite 500 Columbia, MD 21044