Protecting Against Malware Threats with Cisco AMP for Endpoints

DURATION: 3 DAYS

COURSE OVERVIEW

This lab-intensive course introduces students to the powerful features of Cisco AMP for Endpoints software. A number of step by step attack scenarios will provide an understanding of the operational uses of the product.

Students will learn how to build and manage a Cisco AMP for Endpoints deployment, create policies for endpoint groups, and deploy connectors .The AMP for Endpoints console provides powerful tools that will enable you to analyze malware detections.

TARGET AUDIENCE

Technical professionals who need to know how to deploy and manage Cisco AMP for Endpoints software in their network environments.

COURSE OBJECTIVES

After completing this course you should be able to:

1. Identify the key components and methodologies of Cisco Advanced Malware Protection (AMP)
2. Recognize the key features and concepts of the AMP for Endpoints product
3. Navigate the AMP for Endpoints console interface and perform first-use setup tasks
4. Identify and use the primary analysis features of AMP for Endpoints
5. Use the AMP for Endpoints tools to analyze a compromised host
6. Describe malware terminology and recognize malware categories
7. Analyze files and events by using the AMP for Endpoints console and be able to produce threat reports
8. Use the AMP for Endpoints tools to analyze a malware attack and a ZeroAccess infection
9. Configure and customize AMP for Endpoints to perform malware detection

10. Create and configure a policy for AMP-protected endpoints
11. Plan, deploy, and troubleshoot an AMP for Endpoints installation
12. Describe the AMP Representational State Transfer (REST) API and the fundamentals of its use
13. Describe all the features of the Accounts menu for both public and private cloud installations

COURSE CONTENT

Module 1: Introduction to Cisco AMP Technologies

Module 2: AMP for Endpoints Overview and Architecture

Module 3: Console Interface and Navigation

Module 4: Using AMP for Endpoints

Module 5: Detecting an Attacker— A Scenario

Module 6: Modern Malware

Module 7: Analysis

Module 8: Analysis Case Studies

Module 9: Outbreak Control

Module 10: Endpoint Policies

Module 11: Groups and Deployment

Module 12: AMP REST API

Module 13: Accounts

Labs:

Lab 1: Accessing AMP for Endpoints
Lab 2: Attack Scenario
Lab 3: Attack Analysis
Lab 4: Analysis Tools and Reporting
Lab 5: Z bot Analysis
Lab 6: Outbreak Control
Lab 7: Endpoint Policies

Lab 8: Groups and Deployment

Lab 9: Testing Your Policy Configuration

Lab 10: REST API

Lab 11: User Accounts (optional)

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

Technical understanding of TCP/IP networking and network architecture - **ICND2 Recommended**

Technical understanding of security concepts and protocols - **IINS Recommended**

TEST CERTIFICATION

Recommended preparation for the following exams:

500-275 - Securing Cisco Networks with Source fire Fire AMP Endpoints