Securing Cisco Networks with Sourcefire FireAMP (SSFAMP)

Course Summary

Description

The Protecting Against Malware Threats with Cisco© AMP for Endpoints is an instructor-led, lab-based, hands-on course offered by Cisco Learning Services. It is a lab-intensive course that introduces students to the powerful features of Cisco AMP for Endpoints software. Day one of this 3-day virtual class covers modern threats, vulnerabilities, and Cisco Advanced Malware Protection (AMP) technologies. Days two and three detail the Cisco AMP for Endpoints product architecture and how it can be used to protect against malware.

Objectives

After taking this course, students will be able to:

- Describe malware terminology and recognize malware categories
- Describe the architecture and individual security features of Windows, Apple Mac, and Linux operating systems and the concept of vulnerabilities
- Describe the components and behavior of exploit kits and botnets
- Describe modern attack vectors and trends
- Recognize the key components and methodologies of Cisco Advanced Malware Protection
- 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
- 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
- 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
- Describe all features of the Accounts menu for both public and private cloud installations

Topics

- Modern Malware
- Operating Systems and Vulnerabilities
- Exploit Kits and Botnets
- Attack Vectors and Trends
- Introduction to Cisco AMP Technologies
- AMP for Endpoints Overview and Architecture
- Console Interface and Navigation
- Outbreak Control
- Endpoint Policies
- Groups and Deployment
- Analysis
- Analysis Case Studies
- Accounts

Audience

This course is designed for technical professionals who need to know how to deploy and manage Sourcefire FireAMP software in their network environments. The primary audience for this course includes: Security administrators, Security consultants, Network Administrators, System Engineers, Technical support personnel.

Prerequisites

Before taking this course, students should have TCP/IP experience including the major protocols, common services, and basic network traffic routing. They should understand general information security fundamentals and the fundamentals of how operating systems work, including OS configuration structures, file system I/O and basic OS usage and management.

Duration

Three days

ProTech protechtraining.com *"Charting the Course ...*

... to Your Success!"

Securing Cisco Networks with Sourcefire FireAMP (SSFAMP)

Course Outline

I. Modern Malware

II. Operating Systems and Vulnerabilities

III. Exploit Kits and Botnets

IV. Attack Vectors and Trends

V. Introduction to Cisco AMP Technologies

VI. AMP for Endpoints Overview and Architecture

VII. Console Interface and Navigation

VIII. Outbreak Control

IX. Endpoint Policies

X. Groups and Deployment

XI. Analysis

XII. Analysis Case Studies

XIII. Accounts

XIV. Labs:

A. Sample Malware Behavior
B. Accessing AMP for Endpoints
C. Outbreak Control
D. Endpoint Policies
E. Groups and Deployment
F. Analysis
G. Zbot Analysis
H. User Accounts