

SSFAMP

Protecting Against Malware Threats with Cisco AMP for Endpoints

The Protecting Against Malware Threats with Cisco AMP for Endpoints (SSFAMP) v6.0 course 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.

Course Contents

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

E-Book You will receive the original course documentation from Cisco in English language as a Cisco E-Book. In the Cisco Digital Learning Version, the content of the courseware is integrated into the learning interface instead.

Target Group

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

Prerequisites

To fully benefit from this course, you should have the following knowledge and skills:

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

The recommended Cisco offering may help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA)

Processing time

approx. 18 hours

This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

www.expertech-training.com/go/CSFA

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Cisco Digital Learning

This course is available in the Cisco Digital Learning Library. These recently developed, multi-modal training events include HD videos moderated by lecturers with stored searchable text and subtitles, as well as exercises, labs, and explanatory text and graphics. We provide this offer to you via our myExpertech learning portal. Effective of the activation of the account, access to the courses will be granted for a duration of 6 months. In the case of packet solutions (Cisco Digital Learning Subscriptions), this time period will amount to 12 months.

| Cisco Digital Learning | Prices, excl. of V.A.T. |
|------------------------|-------------------------|
| 6 Monate Freischaltung | € 1,000 |

| Training | Prices, excl. of V.A.T. |
|---------------------------|-------------------------|
| Classes in Germany | 3 Days € 3,495 |
| Online Training | 3 Days € 3,495 |
| Date/course venue | Course language English |
| 26/08-28/08/24 Online | 07/10-09/10/24 Online |
| 23/09-25/09/24 Online | |

Status 06/27/2024



Table of Contents

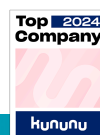
SSFAMP – Protecting Against Malware Threats with Cisco AMP for Endpoints

Course Outline

- Module 1: Modern Malware
- Module 2: Operating Systems and Vulnerabilities
- Module 3 : Exploit Kits and Botnets
- Module 4: Attack Vectors and Trends
- Module 5: Introduction to Cisco AMP Technologies
- Module 6: AMP for Endpoints Overview and Architecture
- Module 7: Console Interface and Navigation
- Module 8: Outbreak Control
- Module 9: Endpoint Policies
- Module 10: Groups and Deployment
- Module 11: Analysis
- Module 12: Analysis Case Studies
- Module 13: Accounts

Lab Outline

- Lab 1: Sample Malware Behavior
- Lab 2: Accessing AMP for Endpoints
- Lab 3: Outbreak Control
- Lab 4: Endpoint Policies
- Lab 5: Groups and Deployment
- Lab 6: Analysis
- Lab 7: Zbot Analysis
- Lab 8: User Accounts



ExperTeach Benelux B.V.

Ceresstraat 1 · 4811 CA Breda · Phone: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@exper-teach.de · www.exper-teach-training.com