Protecting Against Malware Threats with Cisco AMP for Endpoints

Durée: 3 Jours **Réf de cours: SSFAMP** **Version: 6.0**

Résumé:

The Protecting Against Malware Threats with Cisco AMP for Endpoints (SSFAMP) 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 several 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.

Public visé:

Anyone involved in the deployment and utilisation of Cisco AMP for Endpoints

Objectifs pédagogiques:

- **After completing 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
- 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

Pré-requis:

Attendees should meet the following prerequisites:

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

Test et certification

Recommended as preparation for the following exam:

- There is currently no exam aligned to this course

Contenu:

Introducing to Cisco AMP Technologies

- Cisco Talos
- AMP Threat-Centric Security Model
- Protection Framework
- Retrospection Framework
- Cisco SecureX

Introducing AMP for Endpoints Overview and Architecture

- Cisco AMP for Endpoints
- Cisco AMP Cloud Architecture
- Cisco AMP Private Cloud
- Cisco AMP for Endpoints Integration

Navigating the Console Interface

- Activating Your Cisco Account
- Quick Start Configuration and Deployment
- Console Dahsboard
- Menu System

Using Cisco AMP for Endpoints

- Exploring Your Environment with the AMP Console
- System Operations

Identifying Attacks

- Identifying and Containing a Low Prevelance Threat
- Using CVE with AMP for Endpoints
- Using File Trajectory to Track a Threat

Analyzing Malware

- Analyzing Events
- Using Cisco Threat Grid
- File Analysis
- Further Analysis Features
- Reporting

Managing Outbreak Control

- Managing Malware Detections
- Managing Indications of Compromise

Creating Endpoint Policies

- Configuring Endpoint Policies - Basics
- Configuring Endpoint Policies - Advanced Settings

Working with AMP for Endpoint Groups

- Examining Groups
- Configuring Exclusions
- Preparing for a Deployment
- Deployng Windows Connectors
- Windows Installation and the Connector Interface
- Troubleshooting Cisco AMP for Endpoints

Using Orbital for Endpoint Visibility

- Introducing Cisco Orbital
- Orbital Console
- Using Cisco Orbital to Obtain Endpoint Information
- Osquery Syntax

Introducing AMP REST API

- Examining the AMP REST API
- REST API Documentation and Resources
- Query Response Data Structure: JSON
- REST API Authentication
- Performing REST API Transactions
- Using REST API Data in other Applications

Navigating Accounts

- User Administration

Further Account Options

Labs

- 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

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.

• Evaluation : Chaque participant, à l'issue de la formation, répond à un questionnaire d'évaluation qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.