SSFAMP (PROTECTING AGAINST MALWARE THREATS WITH CISCO AMP FOR ENDPOINTS) 5.0

Objetivo

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

PÃºblico Alvo

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

PrÃ©-Requisitos

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

Carga HorÃ¡ria

24 horas (3 dias).

ConteÃºdo ProgramÃ¡tico

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)