SSFAMP (SECURING CISCO NETWORKS WITH FIREAMP FOR ENDPOINTS)

Objetivo

Securing Cisco Networks With FireAMP for Endpoints (SSFAMP) proporciona aos alunos os conhecimentos necessários para instalar, configurar, gerenciar e realizar atividades de suporte ao produto. É curso desenvolvido para capacitação operacional do produto, com utilização intensiva de laboratórios. Esse é um curso oficial desenvolvido pela Cisco Learning High-Touch Delivery. O aluno vai aprender a implantar e gerenciar a solução AMP Cisco, abrangendo a criação de políticas para grupos de dispositivos de usuários (endpoints) e a implementação de conectores. O aluno também vai aprender a utilizar as ferramentas disponíveis no SorceFIRE FireAMP para detectar e analisar a presença de softwares maliciosos (“malwares”) Este curso combinado com a leitura dos materiais fornecidos e com as atividades práticas em laboratórios, e garantem a implementação e gerenciamento com sucesso de uma solução Cisco SourceFire FireAMP. Este curso ele é preparatório para a realização do exame Securing Cisco Networks with Sourcefire FireAMP (500-275). O curso possuí duas modalidades de oferta, com carga horária de dois dias (16 horas) sendo presencial (Instructor-Led Classroom) ou virtual (Instructor-Led Virtual). Após completar este treinamento o aluno estará apto à: • Descrever uma solução com Cisco Sourcefire FireAMP; • Descrever as ameaças para a segurança em torno de ataques com softwares maliciosos (malware); • Descrever e navegar pela interface de configuração e gerência (GUI) do produto, como por exemplo as informações em “Dashboards” e seus componentes; • Gerenciar os mecanismos de detecção de softwares maliciosos; • Descrever a configuração avançada de políticas para dispositivos usuários (endpoints); • Descrever como implantar e distribuir o conector SourceFIRE FireAMP; • Descrever o processo de análise de arquivos (file analysis) e relatórios disponíveis no FireAMP; • Descrever a oferta de nuvem privada.

Público Alvo

O público primário inclui os indivíduos os profissionais que demandam conhecimentos para instalar, operar, prestar suporte e otimizar uma solução Cisco SourceFire FireAMP.

Pré-Requisitos

Para maior aproveitamento é recomendado que o aluno possua conhecimentos fundamentais no protocolo TCP/IP e de sistemas para detecção de softwares maliciosos(Malware).

Carga Horária

16 horas (2 dias).

Conteúdo Programático

SSFAMP: FireAMP Overview and Architecture

Overview
This module will give a general overview of FireAMP, its major components, and the products available in the FireAMP product suite. It will also describe the architecture of FireAMP and how each of the products and components interact with each other.
Objectives
? Discuss malware and the need for threat protection
? Describe the architecture and components of FireAMP
? Discuss the FireAMP Private Cloud architecture
? Perform a Private Cloud installation

SSFAMP: Console Interface and Navigation
Overview
This module will provide a general tour of the FireAMP interface to help familiarize you with the product. It will include descriptions of the menu items and an overview of the various dashboard elements.
Objectives
? Describe the differences between the public cloud and the private cloud
? Review the first use setup
? View and discuss the dashboard and its components
? Review the menu system and identify how to navigate the console
? Describe some public cloud features not currently implemented in the private cloud interface

SSFAMP: Outbreak Control
Overview
This module covers various aspects of managing malware detection including mechanisms for directly specifying files you want to be alerted about, files you do not want to be alerted about, and IP addresses with which endpoints may or may not be allowed to communicate.
Objectives
On completing this module, you will be able to meet these objectives:
? Describe how to customize detection with simple and advanced custom detections
? Discuss application control through the use of application blocking and whitelisting
? Describe DFC and how to customize blacklists and whitelists to control which IP addresses with which endpoints can and cannot communicate

SSFAMP: Endpoint Policies
Overview
This module focuses on creating policies for the endpoints in your FireAMP deployment. It will also demonstrate how to apply the various lists you created previously.
Objectives
On completing this module, you will be able to meet these objectives:
? Create a policy for FireAMP endpoints
? List all the features and settings contained in a policy
? Discuss policy creation strategies and best practices

SSFAMP: Groups and Deployment
Overview
This module illustrates how to work with groups of hosts inside the FireAMP console. This will allow the administrator the flexibility to have different policies within a deployment. An important consideration during the planning phase of a deployment is whether to use FireAMP to complement an existing antivirus deployment, or to

use it on its own. For complementary deployments, you will need to exclude the parts of the endpoint file system that houses the existing AV software, so this module will discuss how to perform this function. It will also describe the available deployment methods.
Objectives
? Describe group creation inside the FireAMP console
? Describe how to exclude parts of the endpoint file system
? Describe how to distribute the FireAMP agent

SSFAMP: Analysis
Overview
This module reviews the various malware analysis features available in the FireAMP console. These are powerful features that can give you a high degree of visibility during and after a malware attack. This is essential for not only monitoring the events that are produced by the system but also giving you tools for diagnosing what caused them and understanding the scope of outbreaks in your environment.
This module also discusses the reporting features of the product to help administrators analyze malware activity in their environments.
Objectives
? Discuss Events and the Events page features
? Describe detections and quarantine events, and how to use the features of the page to get more specific information
? Learn how to set filters in Event View pages and configure subscriptions for event notifications
? Describe the File Analysis page and define what is contained in each of its components.
? Discuss the Search page and how to use it to access File and Device Trajectory.
? Review the Threat Root Cause page.
? Discuss the Prevalence feature.
? Learn how to use the reporting features.

SSFAMP: Analysis Case Studies
Overview
This module will review some malware attacks and describe how to use the FireAMP product to detect and remediate each attack.
Objectives
? Dissect an actual malware attack using sample malware which has been rendered harmless
? Trace an attack back to its origin using the tools available in the FireAMP console

SSFAMP: Accounts
Overview
Items under the Accounts menu allow you to manage your FireAMP console. User management, defaults, audit logs, and demo data can all be accessed from this menu. This module will outline all of the features of the Accounts menu.
Objectives
? Discuss user management
? Describe how to manage system defaults
? View audit log data
• Understand what demo data does and how you can utilize the data

•
Laboratórios

? Lab 1: Performing the Initial Setup
? Lab 2: Initialize the Private Cloud
? Lab 3: Accessing the Sourcefire FireAMP Console
? Lab 4: Reviewing the Interface
? Lab 5: Simple Custom Detection
? Lab 6: Advanced Custom Detection
? Lab 7: Application Blocking
? Lab 8: Whitelisting