SECUR201 (IMPLEMENTING AN INTEGRATED THREAT DEFENSE SOLUTION) 1.0

Objetivo

After taking this course, you should be able to: â¢ Describe the current network security landscape and the Cisco Integrated Threat Defense (ITD) solution; â¢ Describe the key components of the ITD solution and their use in the network; â¢ Configure the Cisco Identity Services Engine (ISE) for a baseline of operation in the ITD solution; â¢ Configure the integration between the Cisco StealthwatchÂ® and Cisco ISE platforms; â¢ Configure the integration between the Cisco FirepowerÂ® and ISE platforms; â¢ Configure the integration between Cisco Firepower and Cisco Advanced Malware Protection (AMP) for Endpoints.

PÃºblico Alvo

This course is designed for technical professionals who need to know how to deploy a Cisco Integrated Threat Defense solution in their network environment.

PrÃ©-Requisitos

To fully benefit from this course, you should have the following knowledge: â¢ Technical understanding of TCP/IP networking and network architecture â¢ Technical understanding of security concepts and protocols â¢ Familiarity with Cisco ISE, Stealthwatch, Firepower, and AMP

Carga HorÃ¡ria

16 horas (2 dias).

ConteÃºdo ProgramÃ¡tico

Course Introduction
Course Overview
Course Goal

Introducing the Cybercrime Landscape
Current Cybersecurity Landscape
Impact of a Breach
Cybercrime Industry

Effective Security Solution Requirements
Modern Attack Vectors
The Need for an Integrated Security Solution
The BDA Security Model

Cisco ITD Solution Architecture
ITD Solution Architecture
ITD Solution Components
ITD Use Case Scenario

Cisco ISE
ISE Product Basics
ISE Product Features for ITD
Supported ISE Integrations

Cisco Stealthwatch
Stealthwatch Product Basics
Stealthwatch System Components
Netflow & Stealthwatch

Cisco Firepower
Supported StealthwatchIntegrations
Firepower Product Basics
Firepower System Components
Supported Firepower Integrations

Cisco AMP
AMP Product Basics
AMP System Components
Supported AMP Integrations

Other Cisco ITD Products
Integrating WSA witch ISE
Integrating Third-Party SIEM Products
Threat-Centric NAC For ISE

Identity Services Engine Integrations Setup
Integrating Cisco ISE with AD Microsoft
Integrating Cisco ISE with Cisco ASAv
Cisco ITD Certificate-Based Authentication Review
Cisco ISE CA Authority Benefits
pxGrid Framework
Using Cisco ISE Certifcates & pxGrid
Monitoring & Verfiy Cisco ISE CA Operation

Stealthwatch with Identity Services Engine Integration
Stealthwatch Integration Benefits
Stealthwatch Integration Basic Process
Stealthwatch Integration Prerequisites
Stealthwatch Configuration Process
Verifying Stealthwatch Integration
Manual Quarentine Endpoint Basics
Anyconnect NVM Integration with Stealthwatch

Firepower with Identity Services Engine Integration
Firepower Integration Benefits
Firepower Integration Process Basics
Firepower pxGrid Operation & Verification
Configure Cisco Firepower FMC for Rapid Threat Containment (RTC)
Configure Cisco Firepower FMC for Endpoint Quarantine
Verifying Firepower Integration with ISE
Verifying RTC Malware Event Trigger

Firepower with AMP for Endpoints Integrations
AMP For Endpoints Integration Benefits
AMP For Endpoints Integration Process Basics
Configuring integration between AMP & Cisco Firepower FMC
Verifying AMP For Endpoints Events

Lab outline
Lab 1: Integrating ISE and Active Directory
Lab 2: Integrating ISE and Cisco Adaptive Security Appliance (ASA)
Lab 3: Configuring pxGrid and Client Certificates
Lab 4: Integrating Stealthwatch with Identity Services Engine
Lab 5: Integrating Network Visibility Module (NVM) with AnyConnect
Lab 5: Integrating Firepower with Identity Services Engine
Lab 6: Integrating AMP for Endpoints with Firepower