Securing Cisco Wireless Enterprise Networks - On Demand (WISECURE 1.1)

Modality: Self-Paced Learning

Duration: 28 Hours

SATV Value:

CLC:

NATU:

SUBSCRIPTION: No

About the course:

Increase your information on the products and technologies of Cisco with e-learning in contributions from Cisco and Cisco's approved learning accomplices. The courses of E-learning aims around a collection of Cisco advances to set you up for the certification exams of Cisco and to pick up Cisco product information. The offerings of e-learning are made to be engaging and interactive with students who have a preference for self-study.

Some Self-paced courses of Cisco give access to hands-on virtual lab works out, allowing you the chance to exercise troubleshooting and configuration on real platforms of Cisco.

Course Objective:

- Explain Approaches and areas of Security in a Wi-Fi Design
- Challenges of Network Access and Access Control Security
- Plan and Deploy Endpoint and Security of Client
- Security Roaming and Mobility
- Deploy and Design Platforms for Cisco ISE and Management
- Network Security Architecture of Cisco
- Current Standards and Features of Secure Wi-Fi Infrastructure
- Define and deploy the standards and features of Wi-Fi Access Control
- Plan and Deploy Monitoring Capabilities
- Monitoring, Management, and Configuring Parameters
- Rogue Mitigation and Detection in Wi-Fi Environment

Audience:

- Security Architect
- Security Manager
- Network Administrator

Prerequisite:

- Basic knowledge on Cisco platform

- Interconnecting Cisco Networking

Course Outline:

Module 1 Define Security Approaches in a Wi Fi Design

- Security Areas in a Wi-Fi Design
- Security Challenges for IT Organizations
- Security Approaches in Wi-Fi Designs
- Policy Enforcement
- Cisco Prime Infrastructure
- Cisco ISE/ISE as a Policy Platform
- Network Access Challenges and Secure Access Control
- Network Monitoring
- Prime Infrastructure Converged Approach and Security Dashboard
- Cisco ISE Dashboard and ISE Alarms

Module 2 Design and Deploy Endpoint and Client Security

- Defining Endpoint, Client Standards and Features
- X.509 v3
- PKI
- IEEE 802.1X
- EAP, EAP-TLS and PKI with EAP-TLS
- PEAP and PEAP Deployment
- EAP-FAST
- RADIUS
- Configure WPA and WPA2 in a Wi-Fi Environment
- Security Mobility and Roaming

Module 3 Design and Deploy Cisco ISE and Management Platforms

- Cisco Network Security Architecture
- User Access Trends
- Cisco ISE Architecture, Components and Licensing
- End Device Analysis with Cisco ISE Profiling
- Create Policies in Cisco ISE
- Configure Guest Access
- Cisco CMX Visitor Connect
- Secure BYOD/BYOD Management and Monitoring
- Cisco ISE and ISE GUI

Module 4 Secure Wi Fi Infrastructure

- Current Standards and Features
- Client and Infrastructure Mode and MFP
- MFP vs IEEE802.11w
- VLANs vs ACLs

- MFP Configuration
- IEEE 802.11w PMF
- Identity-Based Networking
- SMNPv3 in Wi-Fi environment

Module 5 Design and Deploy Wi Fi Access Control

- Wi-Fi access control standards and features
- ACLs and Firewall Functionality
- Configure ACLs in Wi-Fi environment

Module 6 Design and Deploy Monitoring Capabilities

- Threat and Interference Mitigation Approaches in Wi-Fi
- Primary Security Concerns
- Rogue Detection and Mitigation in Wi-Fi Environment
- Management, Monitoring and Configuring Parameters
- Cisco CleanAir
- Cisco Prime Infrastructure Air Quality Monitoring and Reporting
- Monitoring RRM

Labs:

- Configuring WPA2 Access
- Configuring 802.1X Access
- Configuring RADIUS Integration
- Configuring a Basic Access Policy
- Configuring Hotspot Guest Access
- CWA and Self-Registered Guest Operations
- Configuring Secure Administrative Access
- Configuring a Basic Authentication Policy for an AP
- Implementing Profiling
- Profiling and Device Onboarding
- Cisco ISE Profiling Reports
- Guest Reports
- Live Logs and Client 360 View
- Security Report Operations
- Using System Security Verification Tools