



Security Solution for System Engineers

Objectifs

Après avoir suivi le cours, les stagiaires seront capables de :

- Reconnaître les menaces modernes dans l'entreprise
- Reconnaître les contrôles de sécurité modernes
- Choisir les contrôles adaptés en fonction des menaces et de l'environnement
- Appliquer les recommandations de sécurité dans l'architecture et le design
- Identifier les besoins clients, les limitations de l'environnement et construire une solution optimale en fonction de ces paramètres
- Positionner les produits Cisco dans différents scénarii clients

SSSE

3250 € HT
Version : 3.0
5 jours

A qui s'adresse ce cours ?

Ce cours s'adresse aux professionnels des réseaux dont le travail consiste à concevoir et à déployer les fonctionnalités de sécurité Cisco® dans un réseau.

Ce cours est également recommandé à toute personne participant à l'une des nombreuses certifications CCSP® (Cisco® Certified Security Professional), à l'une des trois certifications Cisco® Security Specialist (ASA, IPS, IOS Security) ou à la certification professionnelle INFOSEC (Information Systems Security) agréée par la NSA (National Security Agency) et le CNSS (Committee on National Security Systems).

Pré-requis

Il est recommandé de suivre le cours DESGN et d'avoir un niveau intermédiaire dans les systèmes d'exploitation, entre autre Microsoft

Contenu du stage

1. Les menaces

- 1.1. Principes généraux
- 1.2. Attaques physiques
- 1.3. Attaques sur l'infrastructure réseau
- 1.4. Attaques sur les systèmes et les applications
- 1.5. Attaques sur les utilisateurs

2. Contrôle de sécurité

- 2.1. Contrôle organisationnel
- 2.2. Type de contrôle
- 2.3. Principe de sécurité
- 2.4. Distribution des contrôles entre le réseau et les Endpoints
- 2.5. Services de chiffrement
- 2.6. Management de l'authentification et d'identité
- 2.7. Contrôle réseau
- 2.8. Contrôle système
- 2.9. Contrôle d'application

3. Solutions de protection de l'infrastructure réseau

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00



- 3.1. Présentation des menaces, contrôles et besoins du client
- 3.2. Recommandations sur l'architecture et le design
- 3.3. Etude de cas

4. Solutions pour l'accès Internet

- 4.1. Présentation des menaces, contrôles et besoins client
- 4.2. Recommandation sur l'architecture et le design
- 4.3. Etude de cas

5. Solutions pour les services d'entreprise exposé et les Data Center

- 5.1. Présentation des menaces, contrôles et besoins client
- 5.2. Recommandation sur l'architecture et le design
- 5.3. Etude de cas

6. Solutions pour la protection des communications unifiées

- 6.1. Présentation des menaces, contrôles et besoins client
- 6.2. Recommandation sur l'architecture et le design
- 6.3. Etude de cas

7. Solutions pour la protection des WAN

- 7.1. Présentation des menaces, contrôles et besoins client
- 7.2. Recommandation sur l'architecture et le design
- 7.3. Etude de cas

8. Solutions pour la protection des Access Remote

- 8.1. Présentation des menaces, contrôles et besoins client
- 8.2. Recommandation sur l'architecture et le design
- 8.3. Etude de cas

9. Solutions pour la protection du Wireless

- 9.1. Présentation des menaces, contrôles et besoins client
- 9.2. Recommandation sur l'architecture et le design
- 9.3. Etude de cas

10. Solutions pour la protection du management

- 10.1. Présentation des menaces, contrôles et besoins client
- 10.2. Recommandation sur l'architecture et le design
- 10.3. Etude de cas

Déroulement du stage

	Jour 1	Jour 2	Jour 3	Jour 4	Jour 5
MATIN	Introduction Les menaces	Contrôle de sécurité	Solutions de protection de l'infrastructure réseau	Communications unifiées WAN	Wireless
APRES-MIDI	Contrôle de sécurité	Solutions de protection de l'infrastructure réseau	Accès Internet Services d'entreprise exposé et les Data Center	Access Remote	Management

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

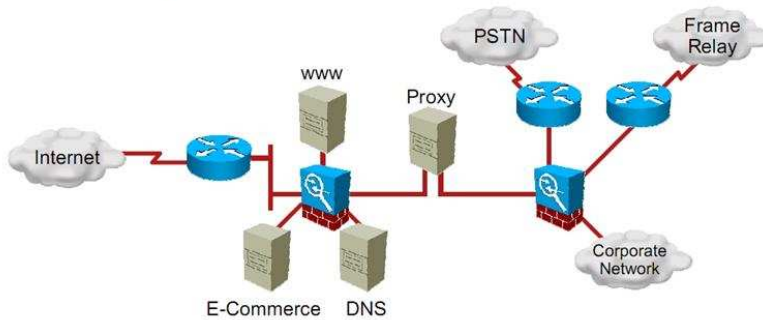
All other trademarks mentioned in this Web site are the property of their respective owners.



Laboratoires pratiques

- Lab 1-1: Démonstration des menaces modernes
- Lab 3-1: Démonstration des protection de l'infrastructure
- Lab 4-1: Démonstration de la protection de l'Accès Internet
- Lab 5-1: Protection des services exposés de l'entreprise
- Lab 7-1: Démonstration d'une demande VPN en full-meshed
- Lab 8-1: Démonstration des Accès distants sécurisé

Examples of Preventive Controls



Select name from
Medical_1 where drugs =...

Access denied



Oracle
Server

Medical_1 Table

DB Records	DB Records	...	DB Records
---------------	---------------	-----	---------------

Access rights:
User1= read, modify
User2 = read

© 2008 Cisco Systems, Inc. All rights reserved.

SSSE v3.0—2-45

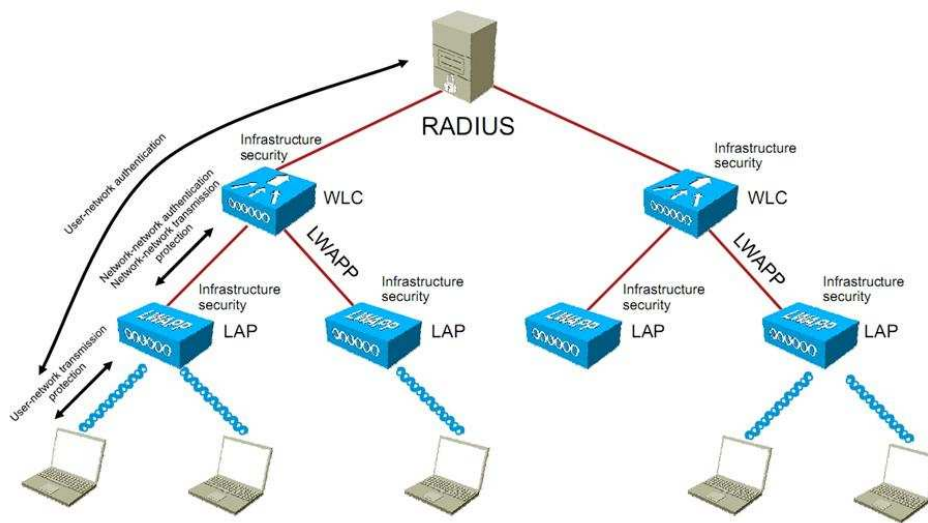
Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.



Enterprise Wireless Topologies: Lightweight APs with WLCs



© 2008 Cisco Systems, Inc. All rights reserved.

SSSE v3.0-9-18

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Networking Academy are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this Web site are the property of their respective owners.