Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Cours officiel, préparation à l'examen 350-701 SCOR

Cours Pratique de 5 jours
Réf : PZL - Prix 2022 : 4 060€ HT

La formation "Implémenter et exploiter les technologies Cisco Security Core", vous apprendra à sécuriser les réseaux, le cloud, les contenus, les terminaux, les accès réseau, leur visibilité et leur contrôle. Vous allez acquérir une expérience pratique du déploiement du pare-feu Cisco Firepower® Next-Generation et du pare-feu Cisco Adaptive Security Appliance (ASA) et plus encore.

PARTICIPANTS

Intégrateurs et partenaires Cisco, ingénieurs conseil en systèmes, administrateurs réseau, concepteurs de réseau, ingénieurs réseau, gestionnaires de réseau, ingénieurs sécurité, etc.

PRÉREQUIS

Avoir suivi le cours CCNA ou avoir des connaissances équivalentes. Connaissances des réseaux Ethernet et TCP/IP. Connaissances pratiques de Windows et des réseaux Cisco IOS.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Décrire les concepts et les stratégies de sécurité de l'information au sein du réseau

Décrire les attaques courantes TCP/IP, d'applications réseau et de terminaux

Décrire comment les technologies de sécurité réseau fonctionnent ensemble pour se protéger contre les attaques

Mettre en place un contrôle d'accès sur l'appliance Cisco ASA et le pare-feu Cisco Firepower de nouvelle génération

Décrire et mettre en œuvre la sécurité du contenu de messagerie de base fournie par Cisco Email Security Appliance

Décrire et mettre en œuvre les fonctions de sécurité du contenu web fournies par le Cisco Web Security Appliance

Décrire les capacités de sécurité de Cisco Umbrella®, les modèles de déploiement, la gestion des stratégies, etc.

Présenter les VPN et décrire les solutions et algorithmes de cryptographie

Décrire les solutions de connectivité sécurisée de point à point Cisco

Expliquer comment déployer les VPN IPsec point à point et les VPN IPsec point à point NGFW

Décrire et déployer les solutions de connectivité d'accès à distance sécurisée Cisco

Décrire comment configurer l'authentification 802.1X et le protocole EAP

Fournir une compréhension de base de la sécurité des points d'accès

Décrire l'architecture et les caractéristiques de base de l'AMP pour les points d'accès

Examiner les différentes défenses des dispositifs Cisco qui protègent le plan de contrôle et de gestion

Configurer et vérifier les contrôles du plan de données de la couche 2 et de la couche 3 du logiciel Cisco IOS

Décrire les solutions Stealthwatch Enterprise et Stealthwatch Cloud de Cisco

Décrire les principes de base, les attaques courantes dans le cloud ainsi que la manière de sécuriser le cloud

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel en anglais. Durée de la formation : 5 jours en classe et 3 jours d'autoapprentissage.

CERTIFICATION

Pour l'obtention de la certification Cisco Certified Network Professional Security (CCNP Security), la réussite de l'examen 350-701 SCOR est requise ainsi que la réussite de l'un des examens suivants (au choix) : 300-710 SNCF, 300-715 SISE, 300-720 SESA, 300-725 SWSA et 300-730 SVPN.

LE PROGRAMME

dernière mise à jour : 12/2021

1) Décrire les concepts de sécurité de l'information (autoformation)
- Présentation de la sécurité des informations.
- Actifs, vulnérabilités et contre-mesures.
- Gestion des risques.

2) Décrire les attaques TCP/IP courantes (autoformation)
- Vulnérabilités TCP/IP héritées.
- Vulnérabilités IP.
- Vulnérabilités ICMP (Internet Control Message Protocol).

3) Décrire les attaques courantes d'applications réseau (autoformation)
- Attaques par mot de passe.
- Attaques basées sur le système de nom de domaine (DNS).
- Tunnellisation du système de nom de domaine (DNS).

4) Décrire les attaques courantes des terminaux (autoformation)
- Débordement de tampon.
- Logiciels malveillants.
- Attaque de reconnaissance.

5) Décrire les technologies de sécurité réseau
- Stratégie de défense en profondeur.
- Défense tout au long du continuum d'attaque.
- Présentation de la segmentation et de la virtualisation du réseau.

6) Déployer le pare-feu Cisco ASA
- Types de déploiement du Cisco Adaptive Security Appliance (ASA).
- Niveaux de sécurité de l'interface Cisco ASA.
- Objets et groupes d'objets Cisco ASA.

7) Déployer le pare-feu de nouvelle génération Cisco Firepower
- Déploiements Cisco Firepower Next-Generation (NGFW).
- Traitement et politiques des paquets NGFW.
- Objets Cisco Firepower Next-Generation NGFW.

8) Déployer la sécurité du contenu des e-mails
- Présentation de la sécurité du contenu de messagerie Cisco.
- Présentation du protocole SMTP (Simple Mail Transfer Protocol).
- Présentation du pipeline de messagerie.

9) Déployer la sécurité du contenu web
- Présentation de l'appliance de sécurité Web Cisco (WSA).
- Options de déploiement.
- Authentification des utilisateurs du réseau.

10) Déployer Cisco Umbrella® (autoformation)
- Architecture de Cisco Umbrella®.
- Déploiement de Cisco Umbrella®.
- Client d'itinérance Cisco Umbrella®.

11) Expliquer les technologies VPN et la cryptographie
- Définition du réseau privé virtuel (VPN).
- Types de réseaux privés virtuels (VPN).
- Communications sécurisées et services cryptographiques.

12) Présentation des solutions VPN sécurisées de site à site Cisco

- Topologies de réseau privé virtuel (VPN) de site à site.
- Présentation du réseau privé virtuel IPsec.
- Cartes cryptographiques statiques IPsec.

13) Déployer VPN IPsec point à point basés sur VTI Cisco IOS

- VTI Cisco IOS.
- Configuration VPN VTI statique point à point IPsec Internet Key Exchange (IKE) v2.

14) Déployer VPN IPsec point à point sur Cisco ASA et Cisco Firepower NGFW

- VPN point à point sur Cisco ASA et Cisco Firepower NGFW.
- Configuration VPN point à point Cisco ASA.
- Configuration VPN point à point Cisco Firepower NGFW.

15) Présentation des solutions VPN d'accès à distance sécurisé de Cisco

- Composants VPN d'accès à distance.
- Technologies VPN d'accès à distance.
- Présentation de Secure Sockets Layer (SSL).

16) Déploiement des VPN SSL d'accès à distance

- Concepts de configuration de l'accès à distance sur Cisco ASA et Cisco Firepower NGFW.
- Profils de connexion.
- Stratégies de groupe.

17) Expliquer les solutions d'accès réseau sécurisé de Cisco

- Accès réseau sécurisé Cisco.
- Composants d'accès au réseau sécurisé Cisco.
- Rôle Authentication, Authorization, Accounting (AAA) dans la solution d'accès réseau sécurisé de Cisco.

18) Décrire l'authentification 802.1X

- 802.1X et protocole d'authentification extensible (EAP).
- Méthodes du protocole d'authentification extensible (EAP).
- Rôle du service Remote Authentication Dial-in User Service (RADIUS) dans les communications 802.1X.

19) Configurer l'authentification 802.1X

- Configuration du commutateur Cisco Catalyst® 802.1X.
- Configuration du contrôleur de réseau local sans fil Cisco (WLC) 802.1X.
- Configuration 802.1X du moteur de services d'identité de Cisco (ISE).

20) Description des technologies de sécurité des terminaux (autoformation)

- Pare-feu personnel basé sur l'hôte.
- Antivirus basé sur l'hôte.
- Système de prévention des intrusions basé sur l'hôte.

21) Déployer Cisco AMP (Advance Malware Protection) pour les terminaux (autoformation)

- Architecture de Cisco AMP pour terminaux.
- Moteurs de détections de Cisco AMP pour terminaux.
- Sécurité rétrospective avec Cisco AMP.

22) Présentation de la protection de l'infrastructure réseau (autoformation)

- Identification des plans de périphérique réseau.
- Contrôles de sécurité du plan de contrôle.
- Contrôles de sécurité du plan de gestion.

23) Déployer les contrôles de sécurité du plan de contrôle (autoformation)
- Lifecycle Advantage (LCA) d'infrastructure.
- Contrôle de sécurité du plan de contrôle.
- Protection du plan de contrôle.

24) Déployer les contrôles de sécurité du plan de données de couche 2 *
- Présentation des contrôles de sécurité du plan de données de couche 2.
- Atténuation des attaques basées sur le réseau local virtuel (VLAN).
- Atténuation des attaques par le protocole STP (Spanning Tree Protocol).

** (autoformation)*

25) Déployer les contrôles de sécurité du plan de données de couche 3 *
- Liste de contrôle d'accès (ACL) anti-usurpation d'infrastructure.
- Transfert de chemin inverse Unicast.
- IP Source Guard.

** (autoformation)*

26) Déployer les contrôles de sécurité du plan de gestion (autoformation)
- Accès à la gestion sécurisée Cisco.
- Protocole de gestion de réseau simple version 3.
- Accès sécurisé aux appareils Cisco.

27) Déployer les méthodes de télémétrie du trafic (autoformation)
- Protocole de temps réseau (NTP).
- Journalisation et exportation des événements des appareils connectés et du réseau.
- Surveillance du trafic réseau à l'aide de NetFlow.

28) Déployer Cisco Stealthwatch Enterprise (autoformation)
- Présentation des offres Cisco Stealthwatch.
- Composants requis pour Cisco Stealthwatch Enterprise.
- Assemblage de flux et déduplication.

29) Décrire le cloud et les attaques cloud courantes (autoformation)
- Évolution du cloud computing.
- Modèles de services cloud.
- Responsabilités de sécurité dans le cloud.

30) Sécuriser le cloud (autoformation)
- Approche Cisco centrée sur les menaces en matière de sécurité réseau.
- Sécurité de l'environnement physique du cloud.
- Sécurité des applications et des charges de travail.

31) Déployer Cisco Steathwatch Cloud (autoformation)
- Cisco Stealthwatch Cloud pour la surveillance du cloud public.
- Cisco Stealthwatch Cloud pour la surveillance des réseaux privés.
- Opérations cloud de Cisco Stealthwatch.

32) Décrire la mise en réseau définie par logiciel
- Concepts de réseau définis par logiciel.
- Programmabilité et automatisation du réseau.
- Plateformes et interface de programmation des applications (API) Cisco.

33) Travaux pratiques officiels
- Configurer les paramètres réseau et le NAT sur Cisco ASA.
- Configurer les stratégies de contrôle d'accès de Cisco ASA.

- Configurer Cisco Firepower NGFW NAT.
- Configurer la stratégie de contrôle d'accès de Cisco Firepower NGFW.
- Configurer la stratégie de découverte et d'IPS de Cisco Firepower NGFW.
- Configurer la stratégie anti-logiciels malveillants et la stratégie de gestion de fichiers de Cisco NGFW
- Configurer les auditeurs, la table d'accès à l'hôte (HAT) et la table d'accès des destinataires (RAT)...
- Configurer les stratégies de messagerie.
- Configurer les services proxy, l'authentification et le déchiffrement HTTPS.
- Appliquer un contrôle d'utilisation acceptable et une protection contre les logiciels malveillants.
- Examiner le tableau de bord d'Umbrella.
- Examiner Cisco Umbrella Investigate.
- Explorer le DNS Ransomware Protection par Cisco Umbrella®.
- Configurer le tunnel VTI statique point à point IKEv2 /IPsec.
- Configurer le VPN point à point entre Cisco ASA et Cisco Firepower NGFW.
- Configurer le VPN d'accès à distance sur le Cisco Firepower NGFW.
- Découvrir Cisco Advanced Malware Protection (AMP) pour les terminaux.
- Effectuer une analyse des terminaux à l'aide de la console Advanced Malware Protection (AMP) for Endpoints.
- Explorer File Ransomware Protection par Cisco Advanced Malware Protection (AMP) for Endpoints Console.
- Découvrir Cisco Stealthwatch Enterprise v6.9.3.
- Explorer Cognitive Threat Analytics (CTA) dans Stealthwatch Enterprise v7.0.
- Explorer le tableau de bord Cisco Cloudlock et la sécurité des utilisateurs.
- Explorer l'application Cisco Cloudlock et la sécurité des données.
- Explorer Cisco Stealthwatch Cloud.
- Explorer les paramètres d'alerte, les listes de surveillance et les capteurs de Stealthwatch Cloud.

LES DATES

CLASSE A DISTANCE
2022 : 26 sept., 14 nov.