Security

Securing Cloud Deployments with Cisco Technologies

SECCLD

Version : 1.0
4 Jours

Objectifs

A l'issue de ce cours, le stagiaire sera en mesure d'atteindre ses objectifs :

- Comparer les différents modèles de services et de déploiement dans le nuage
- Mettre en œuvre la solution de sécurité Cisco pour SaaS à l'aide de Cisco Cloudlock Micro Services
- Déployer des solutions de sécurité dans le nuage en utilisant Cisco AMP for Endpoints, Cisco Umbrella et Cisco Cloud Email Security
- Définir les solutions de sécurité en nuage de Cisco pour la protection et la visibilité en utilisant les appliances virtuelles de Cisco et Cisco Stealthwatch Cloud
- Décrire le réseau en tant que capteur et exécutant à l'aide de Cisco Identity Services Engine (ISE), Cisco Stealthwatch Enterprise et Cisco TrustSec®.
- Mettre en œuvre Cisco Firepower NGFW Virtual (NGFWv) et Cisco Stealthwatch Cloud pour assurer la protection et la visibilité dans les environnements AWS.
- Expliquer comment protéger l'infrastructure de gestion du cloud à l'aide d'exemples spécifiques, de meilleures pratiques définies et des capacités de reporting d'AWS.

Public Concerné

- Architectes de la sécurité
- Architectes de l'informatique en nuage
- Ingénieurs sécurité
- Ingénieurs en informatique dématérialisée
- Ingénieurs système
- Intégrateurs et partenaires Cisco

Pré-requis

Avant de suivre ce cours, le stagiaire doit posséder les compétences et les connaissances suivantes :

- Connaissance des bases de l'informatique en nuage et des logiciels de virtualisation
- Capacité à exécuter les commandes de base d'un système d'exploitation de type UNIX
- Connaissance de la sécurité Cisco CCNP® ou compréhension des domaines suivants :

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

- Déploiement de Cisco Adaptive Security Appliance (ASA) et Adaptive Security Virtual Appliance (ASAv), et opérations Cisco IOS® Flexible NetFlow.
- Déploiement de Cisco NGFW (Cisco Firepower Threat Defense [FTD]), Cisco Firepower et Cisco Firepower Management Center (FMC)
- Opérations de sécurité du contenu Cisco, y compris Cisco Web Security Appliance (WSA)/ Cisco Email Security Appliance (ESA)/Cisco Cloud Web Security (CWS)
- Déploiement de Cisco AMP pour le réseau et les points d'extrémité
- Opérations Cisco ISE et architecture Cisco TrustSec
- Fonctionnement du VPN

Plan du cours détaillé

1. **Présentation de l'informatique dématérialisée et de la sécurité de l'informatique dématérialisée**

- Décrire l'évolution de l'informatique en nuage
- Expliquer les modèles de services de l'informatique dématérialisée
- Explorer les responsabilités en matière de sécurité dans le cadre du modèle de service Infrastructure as a Service (IaaS)
- Explorer les responsabilités en matière de sécurité dans le cadre du modèle de service PaaS (Platform as a Service)
- Explorer les responsabilités en matière de sécurité dans le cadre du modèle de service SaaS
- Décrire les modèles de déploiement de l'informatique dématérialisée
- Décrire les bases de la sécurité dans le nuage

2. **Mise en œuvre de la solution de sécurité Cisco pour le contrôle d'accès au SaaS**

- Explorer les défis de sécurité pour les clients utilisant le SaaS
- Décrire l'analyse du comportement des utilisateurs et des entités, la prévention de la perte de données (DLP) et le pare-feu des applications
- Décrire Cloud Access Security Broker (CASB)
- Décrire Cisco CloudLock en tant que CASB
- Décrire OAuth et les attaques OAuth

3. **Déploiement des solutions de sécurité dans le nuage de Cisco pour les points finaux et la sécurité du contenu**

- Décrire les solutions de sécurité dans le nuage de Cisco pour les points finaux
- Décrire l'architecture AMP pour les points finaux
- Décrire Cisco Umbrella
- Décrire Cisco Cloud Email Security
- Concevoir une sécurité complète des points finaux

4. **Présenter les solutions de sécurité de Cisco pour la protection et la visibilité du cloud**

- Décrire la virtualisation des fonctions de réseau (NFV)
- Décrire les architectures sécurisées de Cisco pour les entreprises (Cisco SAFE)
- Décrire Cisco NGFWv/Cisco Firepower Management Center Virtual (FMCv)/Cisco AMP for Networks
- Décrire Cisco ASAv
- Décrire le Cisco Services Router 1000V (CSR1Kv)
- Décrire Cisco Stealthwatch Cloud
- Décrire le modèle de confiance zéro de Cisco Tetration Cloud

5. **Décrire le réseau en tant que capteur et agent d'exécution**

- Décrire Cisco Stealthwatch Enterprise
- Décrire les fonctions et les personas de Cisco ISE
- Décrire Cisco TrustSec
- Décrire l'intégration de Cisco Stealthwatch et de Cisco ISE
- Décrire Cisco Encrypted Traffic Analytics (ETA)

6. **Mise en œuvre des solutions de sécurité Cisco dans AWS**

- Expliquer les offres de sécurité AWS
- Décrire AWS Elastic Compute Cloud (EC2) et Virtual Private Cloud (VPC)
- Découvrir les solutions de sécurité Cisco dans AWS
- Expliquer Cisco Stealthwatch Cloud dans AWS

7. **Décrire la gestion de la sécurité dans le nuage**

- Décrire la gestion du cloud et les API
- Expliquer la protection des API
- Illustrer un exemple d'API : Intégration à l'ISE à l'aide de pxGrid
- Identifier les meilleures pratiques SecDevOps
- Illustrer un outil de gestion de la sécurité dans le nuage de Cisco Exemple : Cisco Defense Orchestrator
- Illustrer un outil de gestion de la sécurité dans le cloud de Cisco Exemple : Cisco CloudCenter™
- Décrire l'infrastructure centrée sur l'application (ACI) de Cisco
- Décrire les outils de reporting AWS

Laboratoire

- Explorer le tableau de bord Cisco Cloudlock et la sécurité des utilisateurs
- Explorer la sécurité des applications et des données de Cisco Cloudlock
- Explorer les points d'extrémité Cisco AMP
- Effectuer l'analyse des points d'extrémité à l'aide de la console AMP Endpoint
- Examiner le tableau de bord Umbrella

- Examiner Cisco Umbrella Investigate
- Explorer la protection contre les ransomwares par email grâce à Cisco Cloud Email Security
- Protection contre les ransomwares DNS par Cisco Umbrella
- Explorer la protection contre les ransomwares par fichier grâce à Cisco AMP for Endpoints
- Explorer un exemple d'exécution de ransomware
- Mettre en œuvre Cisco ASAv dans ESXi
- Configurer et tester les fonctions de base de Cisco ASAv Network Address Translation (NAT)/Access Control List (ACL)
- Explorer Cisco Stealthwatch Cloud
- Explorer les paramètres d'alerte, les listes de surveillance et les capteurs de Stealthwatch Cloud
- Explorer le réseau en tant que capteur et agent d'exécution
- Explorer Cisco Stealthwatch Enterprise
- Déployer NGFWv et FMCv dans AWS
- Dépannage du FTD et du FMC dans AWS - Scénario 1
- Dépannage FTD et FMC dans AWS - Scénario 2
- Dépannage FTD et FMC dans AWS - Scénario 3
- Explorer les capacités de reporting d'AWS

Mode d'évaluation des acquis

Evaluation par le formateur oralement chaque jour et auto-évaluation formalisée sur le Moodle.