

Réf: IPS - 4 jours

Implementing Cisco Intrusion Prevention System v6 (IPS)

Ce cours fournit les compétences nécessaires pour mettre en œuvre, installer et configurer une solution Cisco de prévention contre les intrusions.

Objectifs :

- Configurer et gérer les sondes IPS Cisco
- Visualiser et répondre aux alarmes IPS

Public concerné :

Ingénieurs, Consultants.

Pré-requis :

- Avoir suivi le cours SND *Securing Cisco Network Devices*. Posséder les connaissances de base sur Windows. Connaître la terminologie et les concepts de la sécurité réseau.

Tests et certification :

Ce cours prépare à la certification CCSP (Cisco Certified Security Professional) ainsi que la certification Cisco IPS Specialist (avec le SND).

Contenu :

Présentation de la détection d'intrusion et des technologies de protection contre les intrusions

- Terminologie et technologies de la détection d'intrusion
- Examiner les produits Cisco IPS
- Examiner les solutions de sondes IPS
- Examiner les techniques pour tenter d'échapper à la détection

Installation des sondes Cisco IPS 42XX

- Installer une sonde IPS à l'aide de CLI
- Utiliser Cisco IDM
- Configurer les paramètres de base de la sonde

Signatures Cisco IPS

- Configurer les signatures et alertes Cisco IPS
- Personnaliser les signatures

Configuration avancée de Cisco IPS

- Améliorer le tuning avancé des sondes IPS
- Assurer la surveillance et la gestion des alarmes
- Configurer une sonde virtuelle
- Configurer les caractéristiques avancées des sondes
- Configurer l'IP Blocking

Périphériques Additionnels

- Installer le module IDSM sur les commutateurs Catalyst 6500
- Installer le module AIP-SSM sur les ASA

Administration

- Assurer la maintenance des sondes IPS
- Gérer les sondes IPS