Sécurité de la téléphonie IP (Partie 2): Sécurisation de solutions Cisco

Durée:
2 jours

Niveau:
Avancé, Expert

Sécurité de la téléphonie IP (Partie 2): sécurisation de solutions Cisco (mise en pratique)

Cette formation constitue la suite logique de la première partie: il est proposé de mettre en oeuvre les concepts acquis sur des solutions Cisco de téléphonie IP.

Le stagiaire apprendra à sécuriser les solutions à plusieurs niveaux: l'infrastructure de communication, les fonctions VoIP/ToIP et les fonctions purement téléphoniques. La formation couvre les solutions CUCM et CUCM Express.

Objectifs:
Savoir sécuriser une solution de téléphonie sur IP Cisco.
Faire le lien entre les objectifs de sécurité et les outils de sécurisation envisageables.

Pré-requis :
Avoir suivi la partie 1 de la formation « Sécurité de la ToIP », avoir suivi les formations « Téléphonie IP Cisco: CUCM » et « Téléphonie IP Cisco: CUCM Express » ou avoir des connaissances équivalentes.

Public :
Ce cours est destiné aussi bien à des ingénieurs et administrateurs ToIP Cisco ainsi qu'à des ingénieurs sécurité.

Cours magistraux illustrés de nombreux travaux pratiques et labs.

Outils de sécurisation génériques
Infrastructure réseaux
Intégration dans une architecture sécurisée
Passerelles VoIP

Pratique: sécurisation d'une architecture à base de CallManager Express
Authentification des postes téléphoniques
Chiffrement des flux media
COR (Class of Restrictions)
Limitation des renvois et transferts
Prise en compte des horaires d'appels
Sécurisation de l'IOS et des outils d'administration

Pratique: sécurisation d'une architecture à base de CallManager
Durcissement des téléphones
Authentification des postes téléphoniques
Chiffrement des flux media
Restriction d'appels (CSS et Partitions)
Limitation des renvois et transferts
Limitation d'appels surtaxés et internationaux
Prise en compte des horaires d'appels
Sécurisation SRST
Sécurisation des passerelles VoIP
Sécurisation de la messagerie vocale (Cisco Unity)
Sécurisation des interfaces aux applications tierces (CTI, TAPI, JTAPI)
Sécurisation des outils d'administration