



Skyhigh Secure Web Gateway Administration for On Premise Appliances

Skyhigh
Security

Description synthétique de la formation

4 Jours

Cette formation est conçue pour vous présenter les concepts, l'architecture, l'interface utilisateur et l'administration du produit Secure Web Gateway (SWG).

Elle se concentre uniquement sur la version on-premise de SWG basée sur les appliances physiques et virtuelles

Objectifs pédagogiques

- **Vue d'ensemble de la solution Secure Web Gateway** : savoir décrire la solution SWG et ses fonctionnalités principales, ses avantages et les améliorations récentes.
- **Planification de l'installation** : Donner des exemples de bonnes pratiques pour implémenter la solution
- **Installation** : Décrire les étapes basiques de l'installation d'une appliance
- **Configuration système** : Identifier les paramètres initiaux pour la configuration système
- **Vue d'ensemble des stratégies** : Expliquer l'objectif des règles et des groupes de règles
- **Journalisation** : Comprendre l'administration des fonctions de journalisation d'une appliance pour surveiller la façon dont les opérations de filtrage et autres activités sont effectuées.
- **Tableaux de bord et surveillance** : Accéder, naviguer et interpréter le contenu des tableaux de bord de SWG
- **Dépannage** : Exploiter les outils de dépannage et connaître les ressources utiles

Public Concerné

Cette formation s'adresse aux administrateurs systèmes et réseaux, responsables de la sécurité, aux auditeurs et/ou consultants concernés par la protection web.

Pré-requis

- Connaissance réseau sur les protocoles et fonctionnalités : TCP/IP, DNS, NTP, HTTP, proxy web
- Connaissances en matière de sécurité informatique, de syntaxe de ligne de commande, anti-virus et technologies web



Contenu du cours détaillé

Jour 1 :

- Introduction
- Vue d'ensemble de la solution
- Planification de l'installation
- Installation
- Configuration système
- Vue d'ensemble des stratégies
- Configuration des règles, des groupes de règles et des listes

Jour 2 :

- Global Threat Intelligence et analyse d'URL
- Filtrage par type de média et Prévention contre la fuite des données
- Analyse des codes malveillants
- Gestion de l'authentification et des comptes
- Analyse des flux HTTPS

Jour 3 :

- Gestion des quotas et du coaching
- Cache web, Next Hop proxies, pages de progression et pages de blocage
- Journalisation
- Tableaux de bords et rapports
- Intégration avec Trellix ePO

Jour 4 :

- Intégration Reverse Proxy et ICAP
- Administration avancée
- Résolution des problèmes de base
- Vue d'ensemble d'ATD et de l'intégration

Mode d'évaluation

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

Certification visée (si applicable)

- Skyhigh Security - Skydiver Tower Operator Certification