FICHE DE SYNTHESE FORMATION CSNA

Certified Stormshield Network Administrator

STORMSHIELD SAS organisme de formation, n° déclaration d'activité : 11922154792

Introduction

Cette formation a pour but de présenter la gamme et les fonctionnalités de base du produit Next Generation Firewall / UTM.

Etant reconnue par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) comme ayant une forte valeur d'usage dans un cadre professionnel, cette certification est recensée à l'Inventaire de la Commission Nationale de la Certification Professionnelle (fiche 2870). Elle est éligible au Compte Personnel de Formation (CPF) de la Liste établie par le COPANEF (comité paritaire interprofessionnel national pour l'emploi et la formation) : code CPF 219933, soit pour les salariés de toutes les branches professionnelles et les demandeurs d'emploi de la France entière. La formation CSNA est également labellisée SecNum*edu* – Formation continue par l'ANSSI.

Public

Responsables informatique, Administrateurs réseaux, tous techniciens informatique.

Modalités pédagogiques et objectifs de la formation

La formation se déroule en face à face pédagogique en salle, en alternant cours théorique et travaux pratiques.

Les stagiaires reçoivent un support de cours imprimé. Le support de cours est composé du cours, des travaux pratiques (Labs) et de leurs corrections. Afin de pouvoir mettre en pratique les éléments du cours, les stagiaires ont à leur disposition un environnement technique complet.

Afin de maintenir l'expertise du stagiaire, toutes les mises à jour du support de cours sont accessibles au format PDF durant 3 ans sur notre plateforme https://institute.stormshield.eu. Le stagiaire trouvera également sur cette plateforme un environnement virtuel lui permettant de manipuler le produit et rejouer les Labs en toute autonomie.

A l'issue de la formation, les stagiaires auront acquis les compétences suivantes :

- prendre en main un firewall SNS et connaître son fonctionnement
- configurer un firewall dans un réseau
- définir et mettre en oeuvre des politiques de filtrage et de routage
- configurer des proxys
- configurer des politiques d'authentification
- mettre en place différents types de réseaux privés virtuels (VPN et VPN SSL)

Lieu, durée et inscriptions

Stormshield propose des sessions de formation dans ses locaux de Paris, Lille et Lyon.

Nos formateurs peuvent également se déplacer sur site à partir de 5 personnes pour assurer les formations.

Stormshield se repose également sur son réseau de distribution et ses partenaires de formation afin de dispenser les formations.

La formation Administrateur se déroule sur trois jours insécables pour une durée totale de 21 heures. Les stagiaires sont convoqués à 9h30 le premier jour de la formation et à 9h les jours suivants (sauf indication

contraire de la part du formateur ou de la part de Stormshield). Toutes les demandes d'inscription doivent être envoyées à votre centre de formation certifié Stormshield Network (SNTC), ou au service formation Stormshield (training@stormshield.eu). Les effectifs maximum sont de 8 personnes par session.

Tarif

Le prix public s'élève à 2100€ HT pour trois journées de formation en salle et deux passages de certification en ligne.

Pré requis et matériel

Bonnes connaissances TCP/IP. Avoir suivi une formation IP préalable est un plus.

Les stagiaires devront se munir d'un PC portable avec un système d'exploitation Windows de préférence (physique ou virtuel en accès réseau par pont) avec droits d'administrateur afin de réaliser les exercices ; et disposant des logiciels suivants : Firefox, PuTTY (ou tout autre client SSH), WinSCP (ou client SCP équivalent), Wireshark, VirtualBox ou équivalent Vmware (Vmware player ou Vmware workstation).

Description détaillée

Jour 1

- Présentation des stagiaires (tour de table)
- Cursus des formations et certifications
- Présentation de l'entreprise et des produits Stormshield
- Prise en main du firewall
    - Enregistrement sur l'espace client et accès à la base de connaissances
    - Initialisation du boitier et présentation de l'interface d'administration
    - Configuration système et droits d'administration
    - Installation de la licence et mise à jour de la version du système
    - Sauvegarde et restauration d'une configuration
- Logs et monitoring
    - Présentation des familles de traces
    - Rapports d'activités embarqués
    - Prise en main des outils d'administration
- Les objets
    - Notion d'objet et types d'objets utilisables
    - Objets réseau et routeur
- Configuration réseau
    - Modes de configuration d'un boitier dans un réseau
    - Types d'interfaces (ethernet, modem, bridge, VLAN, GRETAP)
    - Types de routage et priorités

Jour 2

- Translation d'adresses (NAT)

- Translation sur flux sortant (masquage)
- Translation sur flux entrant (redirection)
- Translation bidirectionnelle (bimap)

- Filtrage
  - Généralités sur le filtrage et notion de stateful
  - Présentation détaillée des paramètres d'une règle de filtrage
  - Ordonnancement des règles de filtrage et de translation
- Protection applicative
  - Mise en place du filtrage URL
  - Filtrage SMTP et mécanismes antispam
  - Configuration de l'analyse antivirale et de l'analyse par détonation Breach Fighter
  - Module de prévention d'intrusion et profils d'inspection de sécurité

Jour 3

- Utilisateurs & authentification
  - Configuration des annuaires
  - Présentation des différentes méthodes d'authentification (LDAP, Kerberos, Radius, Certificat SSL, SPNEGO, SSO)
  - Enrôlement d'utilisateurs
  - Mise en place d'une authentification explicite via portail captif
- Les réseaux privés virtuels
  - Concepts et généralités VPN IPSec (IKEv1 IKEv2)
  - Site à site avec clé pré-partagée
  - Virtual Tunneling Interface
- VPN SSL
  - Principe de fonctionnement
  - Configuration

Examen de certification

La certification consiste en un examen effectué en ligne (1h30, 70 questions).

Le score minimum de certification est de 70%.

L'examen est ouvert automatiquement le jour suivant la fin de la formation pour une durée de trois semaines sur la plateforme https://institute.stormshield.eu. En cas d'échec ou d'impossibilité de passer l'examen dans ce créneau, un deuxième et dernier passage d'examen est ouvert automatiquement dans la foulée pour une durée d'une semaine supplémentaire.