FICHE DE SYNTHESE FORMATION CSNTS

Certified Stormshield Network Troubleshooting & Support (NT-CSNTS)

STORMSHIELD SAS organisme de formation

N° déclaration d'activité : 11922154792

Introduction

Cette formation a pour but d'exposer des outils et méthodes pour collecter les informations nécessaires à l'étude et à la correction de problèmes en utilisant l'interface en ligne de commande (CLI) des produits UTM Stormshield Network.

Cette formation s'adresse aux personnels des sociétés souhaitant atteindre le niveau de partenariat Stormshield le plus élevé, ainsi qu'aux candidats ayant pour objectif de devenir un ingénieur support ou formateur expert sur nos produits UTM.

Public

Responsables informatique, administrateurs réseau, tout technicien informatique.

Modalités pédagogiques

La formation est délivrée soit en présentiel (en face à face pédagogique en salle), soit en distanciel (présence à distance du formateur grâce à un système de visio et utilisation de la plateforme CyberRange d'Airbus). La formation alterne cours théorique et travaux pratiques.

Les stagiaires reçoivent un support de cours 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.

Objectifs de la formation

A l'issue de la formation, et après une révision des connaissances de base, les stagiaires seront capables :

- de connaître l'organisation du système de fichiers ainsi que les démons et processus d'une appliance Stormshield Network
- de localiser, explorer et manipuler les différents fichiers de configuration et de journalisation des activités (logs)
- de distinguer des particularités et anomalies dans une configuration réseau et routage
- de réaliser et d'étudier des captures de trafic réseau
- d'étudier une politique de sécurité et d'en identifier les directives générales et les paramètres particuliers
- d'identifier les traitements appliqués aux connexions en cours
- de produire un relevé d'informations adapté, complet et exploitable pour l'établissement d'un diagnostic

- de configurer des politiques de tunnels VPN IPSec, d'identifier les mécanismes activés et d'en diagnostiquer les dysfonctionnements
- d'analyser et de diagnostiquer une configuration en haute disponibilité

Lieu et durée

Stormshield propose des sessions de formation inter-entreprise en présentiel dans ses locaux de Paris, Lille et Lyon, ou en distanciel.

Nos formateurs peuvent également intervenir en formation intra-entreprise (sur site ou à distance) à partir de 5 personnes.

La formation Troubleshooting and Support dure 28 heures, réparties en quatre journées consécutives de 7h00 dans le cadre d'une formation présentielle, ou 3 journées de 7h00 et 2 demi-journées de 3h30 dans le cadre d'une formation à distance.

L'effectif maximum est de 6 personnes par session.

Modalités d'inscription

Toutes les demandes d'inscription doivent être envoyées à un distributeur « centre de formation Stormshield » (STC), ou au service formation Stormshield (training@stormshield.eu). L'inscription est confirmée et définitive à la réception du bon de commande.

Une procédure de prise en charge par un OPCO avec subrogation de paiement est possible. L'accord de prise en charge dans le cadre d'un financement par un OPCO avec subrogation de paiement doit être fourni à Stormshield au plus tard le 1er jour de la formation. A défaut, la formation sera facturée directement à la société du stagiaire dès le dernier jour de la formation.

Nos conditions générales de vente sont consultables au lien **https://www.stormshield.com/fr/conditions-generales-de-vente-et-de-service/**

Accueil de stagiaires en situation de handicap

Dans le cadre de nos formations, l'accueil des personnes en situation de handicap est possible après évaluation de la nature du handicap. Afin d'anticiper au mieux les besoins et étudier les compensations nécessaires, il est demandé de le signaler dès la prise de contact avec le service formation.

Tarif

Le prix public s'élève à 3950€ HT pour les 28 heures de formation et deux passages de certification en ligne.

Prérequis et matériel

Le stagiaire doit avoir une certification CSNE en cours de validité.

Connaissances approfondies en TCP/IP et shell UNIX.

Les prérequis matériels dépendent du format de la session.

En présentiel :

- PC portable avec une interface réseau filaire et avec un système d'exploitation Windows de préférence (physique ou virtuel en accès réseau par pont) avec droits d'administrateur ; et

disposant des logiciels suivants : Firefox, PuTTY (ou tout autre client SSH), WinSCP (ou client SCP équivalent), Wireshark, VirtualBox ou équivalent VMWare (VMWare Workstation Player ou Pro).

En distanciel :

- Navigateur web : Chrome 50 (ou supérieur) ou Firefox 50 (ou supérieur) avec Javascript installé pour l'accès à la plateforme CyberRange pour la réalisation des travaux pratiques (seuls ces navigateurs sont supportés). Le stagiaire doit avoir les droits d'installation de plugin pour gérer la visio
- PC avec 6Go de RAM et un processeur de type I3, sans de contrainte disque dur
- Accès internet avec un débit minimal de 2Mb/s
- Un 2ème écran est fortement recommandé (22'' ou plus)

Programme détaillé de la formation

- Présentation des stagiaires (tour de table)
- Introduction
- Système d'exploitation et commandes UNIX liées
  - Méthodes d'accès au shell et paramètres
  - SSH : fonctionnalités
  - Système de fichier et commandes associées
  - Répertoires et commandes associées
  - Environnement système et utilisateur
  - Fichiers et commandes associées
- Logs
  - Logs locaux : localisation, caractéristiques, syntaxe, catégories
  - Commandes associées
  - Fichiers de configuration
  - Logd, logctl, journalisation des messages noyau
- Fichiers de configuration
  - Répertoires, structure et syntaxe générale
  - Sauvegarde (*.na), decbackup, tar
  - Configuration usine
- Objets
  - Syntaxe des objets
  - Objets dynamiques et FQDN
- Réseau et routage
  - Paramètres des interfaces réseau
  - Le bridge et les commandes associées
  - Routage : fonctions de routage et leur priorité
  - Routes par défaut et routes statiques
  - Gatemon et les objets routeurs
  - Routage dynamique
  - Commandes relatives, affichage des routes

- Mode verbose
- LAB Réseau et routage

- Capture et analyse de trafic
  - Introduction et conseils
  - Syntaxe générale et arguments
  - Filtres usuels
  - Exemples commentés et préparation pour faire de bonnes captures
  - Analyse de trafics par tcpdump (flux TCP, UDP/icmp)
  - LAB network/tcpdump

- ASQ : les étapes d'analyse
  - Analyse pas à pas des couches réseau
  - Commandes associées
  - Paramètres globaux
  - Profils et paramètres particuliers
  - ASQ asynchrone : différents cas et watermarking
  - ASQ verbose mode
  - LAB paramètres ASQ
- ASQ : politique de sécurité
  - Répertoires et fichiers de configuration, syntaxe des règles
  - Filtre : commandes associées
  - Filtre : exemple de règles chargées (action, niveau d'inspection, plugin, PBR, QoS, interfaces, proxy)
  - Filtre : traduction des groupes et des listes
  - NAT : rappels (NAT Dynamique, NAT Statique par port, NAT statique/Bimap, Non NAT)
  - NAT : commandes associées
  - NAT : syntaxe des règles chargées
  - LAB NAT et Filtrage
- ASQ : Stateful et tables d'états
  - Table des adresses protégées
  - Table des hôtes
  - Table des connexions : exemples d'états de connexion (NAT, vconn, FTP plugin, async, lite...)
  - LAB ASQ Stateful tracking
- Démons et Processus
  - Liste et rôle
  - Démon Superviseur
  - Commandes relatives
- Eventd : le gestionnaire d'événements
- VPN IPSec
  - Implémentation IKE/IPSec Stormshield Network
  - Fichiers de configuration
  - Politique de sécurité (SPD, SAD)

- Les négociations IKE
- Négociations : mode Main et mode Aggressive
- ISAKMP et IPsec SA
- Propositions IKE
- Particularités : NAT-T, DPD, Keepalive, SharedSA, Politique None, SPD Cache
- Commandes associées
- Analyse d'une IPSec-SA
- Logs
- Notifications de « delete SA »
- Capture et analyse du trafic ISAKMP
- Particularités des correspondants dynamiques
- Mode Verbose, erreurs courantes
- LAB ISAKMP/IPsec

- PKI et certificats
  - Rappels et directives globales
  - Répertoire de CA
  - Astuces de configuration
  - Vérification des certificats
- Haute disponibilité
  - Généralités
  - Fichiers de configuration
  - Commandes relatives
  - Etapes d'activation, gestion des interfaces réseau
  - Processus et trafics impliqués
  - Réplications/synchronisation
  - Evènements et logs HA

Examen de certification

La certification consiste en un examen effectué en ligne (3h, 60 questions).

L'examen comporte des QCM et des questions ouvertes sur les fonctionnalités, paramétrages et méthodes de dépannage avancées à mettre en œuvre pour répondre exhaustivement à des rapports d'incidents issus de nos clients.

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 six mois 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.