FICHE DE SYNTHESE FORMATION CSNA

Intitulé **STORMSHIELD NETWORK ADMIN (NT-CSNA)**
Cris Réseaux organisme de formation
N° Déclaration d'activité : 93130819313

Introduction

Cette formation a pour but de présenter les fonctionnalités avancées du produit Stormshield Network Security.
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 au Répertoire Spécifique mis en place par France Compétences soit pour les salariés de toutes les branches professionnelles et les demandeurs d'emploi de la France entière.
La formation CSNA est également labellisée SecNumedu – Formation continue par l'ANSSI.
La formation est éligible aux financements par les OPCO.

Public

Responsables informatique, administrateurs réseaux, tous techniciens 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 au système de visio Cisco Webex et utilisation de la plateforme de formation).
- La formation alterne cours théorique et travaux pratiques.
- Les stagiaires reçoivent un support de cours en format PDF composé du cours, sur leur adresse e-mail renseignée sur la fiche d'inscription. Le support de cours est composé 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 virtuel.
- Ressources :
  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 la plateforme https://institute.stormshield.eu.
  Le stagiaire trouvera également sur cette plateforme un environnement virtuel lui permettant de manipuler le produit et rejouer les TP-Labs en toute autonomie.
  Il peut également consulter différentes ressources sur le site de Cris Réseaux :
  https://www.cris-reseaux.com/service-technique/ressources/

Objectifs de la formation

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 œuvre des politiques de filtrage et de routage
- configurer un contrôle d'accès aux sites web en http et https (proxy)
- configurer des politiques d'authentification
- mettre en place différents types de réseaux privés virtuels (VPN IPSec et VPN SSL).

Lieu, durée et inscriptions

Cris Réseaux propose des sessions de formation inter-entreprise en présentiel ou en distanciel.

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

En présentiel et Distanciel la formation Administrator - CSNA dure 21 heures, réparties en trois journées consécutives de 7h/J.

Toutes les demandes d'inscription doivent être envoyées à notre service de formation formation@cris-reseaux.com.

L'effectif maximum est de 8 personnes par session.

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.

Modalités, délais d'accès et Tarifs :

Nous contacter.

Prérequis Technique :

Public issu du technique en réseau et informatique.
Il est demandé aux stagiaires souhaitant s'inscrire en formation CSNA de valider au préalable qu'ils disposent des connaissances nécessaires pour participer à la formation grâce au test d'autoévaluation au lien suivant: https://institute.stormshield.eu/courses/CSNAPREREQUISITEFR/?language=french

Pré requis matériel :

Les prérequis matériels dépendent du format de la session.

En présentiel :

- PC portable avec une interface réseau filaire et 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, en dernière version : Chrome ou Firefox avec Javascript installé pour l'accès à la plateforme CyberRange pour la réalisation des travaux pratiques (seuls ces navigateurs sont supportés). - Accès internet avec un débit minimal de 2Mb/s - Un 2ème écran est fortement recommandé (22'' ou plus)

Pour les formations distancielles, les stagiaires doivent avoir une webcam et un micro fonctionnels, ainsi que les droits d'installation pour le logiciel de visio

Description détaillée

Jour 1

- Présentation des stagiaires (tour de table)
  Le cursus des formations et certifications, Présentation de Stormshield et des produits Stormshield,
- Fonctions standards et optionnelles : 1. Les fonctions standards 2. Les options logicielles et matérielles 3. Packs de maintenance.
- Prise en main du firewall : 1. Enregistrement sur l'espace client et accès à la base de connaissances 2. Connexion sur le portail WEB et présentation du tableau de bord o Injection de la licence et mise à jour de la version du système 3. Configuration système et droits d'administration 4. Sauvegarde et restauration d'une configuration.
  - LAB 1 : Prise en Main du Firewall
- Monitoring et logs : Présentation des familles de logs ; Rapports d'activités embarqués Installation et prise en main des outils : Real Time Monitor et Event Reporter.
- Les objets : Notion d'objet et types d'objets utilisables, Objets réseau et routeur.
  - LAB 2 : Les Objets
- Configuration réseau o Modes de configuration d'un boitier dans un réseau o Types d'interfaces (ethernet, modem, bridge, VLAN) o Types de routage et priorités
  - LAB 3 : Configuration Réseau

Jour 2

- Translation d'adresses (NAT) o Translation sur flux sortant (masquage) o Translation sur flux entrant (redirection) o Translation bidirectionnelle (bimap).
  - LAB 4 : Translation d'adresses

- Filtrage : Généralités sur le filtrage et notion de stateful o Présentation détaillée des paramètres d'une règle de filtrage o Mise en œuvre d'une translation destination dans une règle de filtrage, Ordonnancement des règles de filtrage et de translation.
    - LAB 5 : Filtrage
- Protection applicative : Mise en place du filtrage URL o Filtrage SMTP et mécanismes antispam ; Configuration et activation de l'analyse antivirale ; Module de prévention d'intrusion et profils d'inspection de sécurité
    - LAB 6 : Filtrage de contenu (HTTP et HTTPS)

Jour 3

- Authentification et utilisateurs : Présentation des différentes méthodes d'authentification (LDAP, Kerberos, Radius, Certificat SSL, SPNEGO, SSO); Configuration des annuaires, Enrôlement d'utilisateurs ; Mise en place d'une authentification explicite via portail captif
    - LAB 7 : Authentification
- Les réseaux privés virtuels : VPN IPSec - concepts et généralités (IKEv1 IKEv2) ; Site à site avec clé pré-partagée ; Virtual Tunneling Interface ; Correspondant dynamique ;
    - LAB 8 : VPN IPsec (Site a site)
- VPN SSL - Principe de fonctionnement – Configuration.
    - LAB 9 : VPN SSL
    -

Examen de certification

La certification consiste en un examen effectué en ligne (1h30, 70 questions), à la date convenue avec le Service Formation. 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.