Formation : Certified Stormshield Network Expert (NT-CSNE)

Cours pratique - 3j - 21h00 - Réf. CNJ
Prix : 2600 € H.T.

★★★★★ 5 / 5

Cette formation a pour but de présenter les fonctionnalités avancées du produit Stormshield Network Security. Reconnue par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) comme ayant une forte valeur d'usage dans un cadre professionnel, la certification CSNE est labellisée SecNumedu - Formation continue.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Utiliser l'IHM de manière avancée
- Configurer avec précision le moteur de prévention d'intrusions
- Mettre en place une PKI et une authentification transparente
- Mettre en place un VPN IPsec par certificat
- Créer un cluster haute disponibilité

Public concerné

Responsables informatique, administrateurs réseaux, tous techniciens informatique ayant obtenu la certification CSNA.

Prérequis

Formation réservée aux personnes ayant réussi l'examen CSNA dans les 3 années précédentes. Bonnes connaissances TCP/IP (routage, phases d'établissement d'une connexion TCP, structure d'un paquet IP…)

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

PARTICIPANTS

Responsables informatique, administrateurs réseaux, tous techniciens informatique ayant obtenu la certification CSNA.

PRÉREQUIS

Formation réservée aux personnes ayant réussi l'examen CSNA dans les 3 années précédentes. Bonnes connaissances TCP/IP (routage, phases d'établissement d'une connexion TCP, structure d'un paquet IP…)

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

Certification

La certification consiste en un examen effectué en ligne (2h, 90 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. Certification SecNumedu.
Comment passer votre examen ?

Méthodes et moyens pédagogiques

Méthodes 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 participants 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 participants ont à leur disposition un environnement technique complet. Afin de maintenir l'expertise du participant, 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 participant trouvera également sur cette plateforme un environnement virtuel lui permettant de manipuler le produit et rejouer les Labs en toute autonomie.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Présentation des participants (tour de table)

2 Présentation détaillée du moteur de prévention d'intrusion Stormshield Network

- Différences entre la prévention et la détection d'intrusion.
- Le moteur de prévention d'intrusion.
- Les différents types d'analyses.
- Les profils protocolaires et applicatifs.

3 Infrastructure à clés publiques

- Bases de chiffrement symétrique et asymétrique.
- Les types de chiffrements.
- PKI Stormshield Network.
- Création d'une autorité de certification, d'une identité serveur et d'une identité utilisateur.

4 Proxy SSL

- Principe de fonctionnement.
- Paramétrages du proxy SSL.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

5 VPN IPSec avancé

- Fonctionnement détaillé et mécanisme de NAT traversal.
- Support du Dead Peer Detection (DPD).
- Architecture VPN en étoile et chaînage.
- NAT dans IPSec.
- Architecture VPN IPsec avec tunnel de secours.
- Configuration d'un VPN site à site avec utilisation de certificats.
- Configuration d'un VPN nomade.

6 GRE et GRETAP

- Principe de fonctionnement.
- Configuration et mise en place.

7 Authentification transparente

- Principe de fonctionnement.
- Méthode d'authentification SPNEGO.
- Méthode d'authentification par certificat SSL.

8 Haute disponibilité

- Principe de fonctionnement.
- Assistant de création et de configuration d'un cluster HA.
- Configuration des interfaces réseaux.
- Configuration avancée.

Dates et lieux

CLASSE À DISTANCE
2026 : 3 juin, 23 sep., 16 déc.

PARIS LA DÉFENSE
2026 : 27 mai, 16 sep., 9 déc.