

FICHE DE SYNTHÈSE FORMATION CSNE

Intitulé **STORMSHIELD NETWORK Expert**
 Cris Réseaux organisme de formation
 N° Déclaration d'activité : 93130819313

Introduction

Cette formation a pour but de présenter les fonctionnalités avancées du produit de Next Generation Firewall/ UTM 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 à l'Inventaire de la Commission Nationale de la Certification Professionnelle ([fiche 2871](#)). Elle est éligible au Compte Personnel de Formation (CPF) : **code CPF 236246**, soit pour les salariés de toutes les branches professionnelles et les demandeurs d'emploi de la France entière. La formation CSNE est également labellisée SecNumedu – Formation continue par l'ANSSI. La formation est éligible aux financements par les OPCO (Numéro Datadock 0016999).

Public

Responsables informatique, administrateurs réseaux, tous techniciens informatiques, ayant validé le cursus administrateur.

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 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.

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, et après une révision des connaissances de base, les stagiaires seront capables :

- D'utiliser de manière avancée l'IHM,
- De configurer avec précision le moteur de prévention d'intrusions,
- De mettre en place une PKI et une authentification transparente,
- De mettre en place un VPN IPsec par certificat,
- De créer un cluster haute disponibilité.

Lieu, durée et inscriptions

Cris Réseaux propose des sessions de formation dans ses différents locaux : Aix en -Provence, Nantes, Lyon, Toulouse, Strasbourg, Paris et Lille.

Nos formateurs peuvent également se déplacer sur site pour assurer les formations.

La formation CSNE - Expert se déroule sur trois jours insécables pour une durée totale de 21 heures. Les stagiaires sont convoqués à 9h (sauf indication contraire de la part du formateur ou de la part de Cris Réseaux).

Pré requis et matériel

L'accès à cette formation est réservé aux personnes ayant réussi l'examen CSNA dans les 3 ans précédant la formation CSNE...

Bonnes connaissances TCP/IP (routage, phases d'établissement d'une connexion TCP, structure d'un paquet IP...).

Afin de réaliser les exercices, 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). 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.
- Infrastructure à clés publiques o Qu'est-ce que la cryptographie ? o Les types de chiffrement o PKI Stormshield Network o Création d'une autorité de certification, d'un certificat utilisateur et d'un certificat serveur

Jour 2

- Proxy SSL o Principe de fonctionnement o Paramétrages du proxy SSL
- VPN IPsec avancé o Fonctionnement détaillé et mécanisme de NAT traversal o Support du Dead Peer Detection (DPD) o Architecture VPN en étoile et chainage o NAT dans IPsec o Architecture VPN IPsec avec tunnel de secours o Configuration d'un VPN site à site avec utilisation de certificats o Configuration d'un VPN nomade

Jour 3

- GRE et GRE-TAP o Principe de fonctionnement o Configuration et mise en place –
- Authentification transparente o Principe de fonctionnement o Méthode d'authentification SPNEGO o Méthode d'authentification par certificat SSL –
- Haute disponibilité o Principe de fonctionnement o Assistant de création et de configuration d'un cluster HA o Configuration des interfaces réseaux o Configuration avancée

Examen de certification

La certification consiste en un examen effectué en ligne (2h, 90 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.