

Certified Stormshield Network Troubleshooting and Support (CSNTS)

CATEGORIE : B

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Spécifique : ■ **Support à l'entreprise - Systèmes d'information et de télécommunication**

Réseaux et sécurité informatique - Cybersécurité, Protection des données - Cette certification peut être utilisée par tous les services informatiques ou les prestataires informatiques, quel que soit le domaine d'activité de l'entreprise. Elle s'adresse notamment aux personnels des sociétés souhaitant atteindre le niveau d'expertise Stormshield le plus élevé, ainsi qu'aux candidats ayant pour objectif de devenir un ingénieur support ou formateur expert sur nos Firewalls (pare-feux) Stormshield Network Security.

Code(s) NAF : **62.01Z**

Code(s) NSF : **326n**, **326**, **326r**

Code(s) ROME : **M1804**, **M1803**, **M1801**, **M1810**, **M1802**

Formacode : **24293**

Date de création de la certification : **01/09/2014**

Mots clés : **Cyber sécurité**, **SECURITE**, **RESEAUX**, **firewall**

Identification

Identifiant : **2873**

Version du : **19/07/2017**

Références

Consensus, reconnaissance ou recommandation :

Formalisé :

- [Les pare-feu Stormshield font partie des produits « qualifiés » par l'ANSSI donc « recommandés » \(voire, d'usage obligatoire pour certains usages\) pour les administrations et les entreprises sensibles du secteur privé.](#)

Non formalisé :

- [Offres d'emploi indiquant la nécessité d'une connaissance en environnement STORMSHIELD](#)
- [Témoignages de clients certifiés](#)

Norme(s) associée(s) :

—

Descriptif

Objectifs de l'habilitation/certification

La certification **Certified Stormshield Network Troubleshooting and Support (CSNTS)** atteste de la capacité du candidat à analyser une configuration réseau, à diagnostiquer des anomalies, à réaliser et interpréter des captures de trafic réseaux, à produire des relevés d'informations complets dans le cadre de la résolution d'incidents techniques. Elle sanctionne également la capacité à réaliser un diagnostic des configurations des Firewalls (pare-feux) SNS en haute disponibilité, avec authentification ou avec des proxies.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- Néant

Descriptif général des compétences constituant la certification

La certification CSNTS permet au candidat d'acquérir les compétences suivantes :

Connaître l'organisation du système de fichiers ainsi que les démons et processus d'un Firewall Stormshield Network
Localiser, explorer et manipuler les différents fichiers de configuration et de journalisation des activités (logs)
Distinguer des particularités et anomalies dans une configuration réseau et routage
Réaliser et étudier des captures de trafic réseaux
Etudier une politique de sécurité et en identifier les directives générales et les paramètres particuliers
Identifier les traitements appliqués aux connexions en cours
Produire un relevé d'informations adapté, complet et exploitable pour l'établissement d'un diagnostic
Configurer des politiques de tunnels VPN IPSec, identifier les mécanismes activés et en diagnostiquer les dysfonctionnements
Analyser et diagnostiquer une configuration en haute disponibilité
Identifier les rôles des différents paramètres d'une configuration d'authentification des utilisateurs
Analyser la configuration des proxies (explicites ou implicites) et leurs mécanismes particuliers

Public visé par la certification

Tous publics

Modalités générales

Pour la préparation à la certification, une formation de 15 modules sur 4 jours est proposée aux candidats. Elle est délivrée en classe avec un instructeur, elle inclut des travaux pratiques avec du matériel physique dédié. De plus, durant les 3 années suivant la formation, le candidat a accès à des ressources complémentaires pour maintenir ses connaissances sur notre plateforme <https://insitute.stormshield.eu>.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

La certification CSNTS permet de renforcer la crédibilité professionnelle de son détenteur et récompense son expertise des Firewalls Stormshield. Elle constitue un repère dans le domaine de la sécurité informatique, apportant ainsi une réelle valeur ajoutée au CV des candidats et améliorant leur employabilité. Elle représente le niveau le plus élevé des trois certifications SNS.

Le programme Partner Connect de Stormshield permet aux personnes certifiées en recherche d'emploi d'identifier les sociétés partenaires intéressées par leur profil.

L'accès à la mise à jour des supports de cours et à l'environnement de travaux pratiques durant 3 ans permet de maintenir cette expertise.

Pour l'entité utilisatrice

La maîtrise des firewalls SNS qualifiés par l'Agence nationale de la sécurité des systèmes d'information permet aux entreprises de suivre les recommandations de cet organisme.

La certification garantit à l'entreprise utilisatrice d'avoir du personnel qualifié pour protéger son réseau informatique contre les cyber-attaques, et d'accéder au support technique Niveau 2 Stormshield.

Pour les sociétés spécialisées dans les réseaux informatiques, la certification permet d'être reconnues comme étant des acteurs majeurs dans le monde de la cybersécurité et de travailler avec une plus grande clientèle via le programme Partner Connect de Stormshield. Cette certification est nécessaire pour atteindre le niveau de partenariat le plus élevé.

Evaluation / certification

Pré-requis

Avoir obtenu la certification CSNE (Stormshield Network Expert) dans les 3 ans précédant la formation CSNTS.

Compétences évaluées

La totalité des compétences des modules de formation sont évaluées lors de la certification, notamment :

Connaître l'organisation du système de fichiers ainsi que les démons et processus d'un Firewall Stormshield Network

Localiser, explorer et manipuler les différents fichiers de configuration et de journalisation des activités (logs)

Distinguer des particularités et anomalies dans une configuration réseau et routage

Réaliser et étudier des captures de trafic réseaux

Etudier une politique de sécurité et en identifier les directives générales et les paramètres particuliers

Identifier les traitements appliqués aux connexions en cours

Produire un relevé d'informations adapté, complet et exploitable pour l'établissement d'un diagnostic

Configurer des politiques de tunnels VPN IPSec, identifier les mécanismes activés et en diagnostiquer les dysfonctionnements

Analyser et diagnostiquer une configuration en haute disponibilité

Identifier les rôles des différents paramètres d'une configuration d'authentification des utilisateurs

Analyser la configuration des proxies (explicites ou implicites) et leurs mécanismes particuliers

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

Certified Stormshield Network Troubleshooting and Support (CSNTS)

Centre(s) de passage/certification

- Une plateforme dédiée et spécifique, <https://institute.stormshield.eu>, - a été mise en place pour les passages de certifications. Elle donne également l'accès aux ressources de formation.

La validité est Temporaire

3 ans

Possibilité de certification partielle : non

Matérialisation officielle de la certification :

Diplôme avec numéro de certification unique.

Plus d'informations

Statistiques

Environ 30 certifications par an.

Autres sources d'information

<https://www.stormshield.com/fr/produits-et-services/services/formations/>