

## Formation CSNE - Certified Stormshield Network Expert

<b>Durée :</b>	3.0 jour(s)
<b>Objectifs :</b>	<ul style="list-style-type: none"> <li>• Utiliser de manière avancée l'IHM,</li> <li>• Configurer avec précision le moteur de prévention d'intrusions,</li> <li>• Mettre en place une PKI et une authentification transparente,</li> <li>• Mettre en place un VPN IPsec par certificat,</li> <li>• Configurer un cluster haute disponibilité.</li> </ul>
<b>Public :</b>	<ul style="list-style-type: none"> <li>• Responsables informatiques, Administrateurs réseaux, Techniciens informatiques</li> </ul>
<b>Prérequis :</b>	<ul style="list-style-type: none"> <li>• L'accès à cette formation est réservé aux personnes ayant réussi la <a href="#">certification CSNA</a> dans les 3 ans</li> </ul>
<b>Modalités et moyens pédagogiques</b>	<p>La formation alterne cours théorique et travaux pratiques. Deux modalités sont proposées :</p> <ul style="list-style-type: none"> <li>• en présentiel, dans les locaux de Stormshield</li> <li>• en distanciel, avec présence à distance du formateur grâce à un système de visio et du portail web: <a href="http://maformation.vaelia.fr">maformation.vaelia.fr</a></li> </ul>
<b>Modalités d'évaluation</b>	<ul style="list-style-type: none"> <li>• Auto évaluation des acquis, exercices pratiques et/ou échanges avec le formateur.</li> <li>• Deux passages de certification CSNE permettent aux stagiaires de valider leurs acquis.</li> </ul>
<b>Moyens d'encadrement</b>	<p>Un formateur expert spécialisé en Stormshield Network Security dont les compétences ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou Vaelia.</p>
<b>Satisfaction globale :</b>	<p>/5  <i>Calculée à partir des évaluations stagiaires sur les 12 derniers mois.</i></p>

## Jour 1

### 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

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

## Jour 2

### Proxy SSL

- Principe de fonctionnement
- Paramétrages du proxy SSL

### VPN IPSec avancé

- Fonctionnement détaillé et mécanisme de NAT traversal
- Support du Dead Peer Detection (DPD)
- Architecture VPN en étoile et chainage
- 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

### GRE et GRE-TAP

- Principe de fonctionnement
- Configuration et mise en place

## Jour 3

### Authentification transparente

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

### Haute disponibilité

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