

## Formation Certified Stormshield Network Troubleshooting & Support (NT-CSNTS)

■ <b>Durée :</b>	4 jours (28 heures)
■ <b>Tarifs inter-entreprise :</b>	5 000,00 € HT (standard) 4 000,00 € HT (remisé)
■ <b>Public :</b>	Responsables informatique, administrateurs réseau, tout technicien informatique
■ <b>Pré-requis :</b>	Le stagiaire doit avoir une certification CSNE en cours de validité. Connaissances approfondies en TCP/IP et shell UNIX
■ <b>Objectifs :</b>	Mieux appréhender les spécificités des protocoles industriels dont S7, OPC UA et Modbus TCP - Intégrer un boîtier SNS à une architecture simple existante - Mettre en place des règles de sécurité spécifiques à des protocoles industriels - Personnaliser les signatures applicatives en fonction des automates utilisés - Configurer le mode sûreté (bypass)
■ <b>Modalités pédagogiques, techniques et d'encadrement :</b>	<ul style="list-style-type: none"><li>• Formation synchrone en présentiel et distanciel.</li><li>• Méthodologie basée sur l'Active Learning : 75 % de pratique minimum.</li><li>• Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat.</li><li>• Un formateur expert.</li></ul>
■ <b>Modalités d'évaluation :</b>	<ul style="list-style-type: none"><li>• Définition des besoins et attentes des apprenants en amont de la formation.</li><li>• Auto-positionnement à l'entrée et la sortie de la formation.</li><li>• Suivi continu par les formateurs durant les ateliers pratiques.</li><li>• Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.</li></ul>
■ <b>Sanction :</b>	Attestation de fin de formation mentionnant le résultat des acquis
■ <b>Référence :</b>	RÉS102507-F

■ <b>Note de satisfaction des participants:</b>	Pas de données disponibles
■ <b>Contacts :</b>	commercial@dawan.fr - 09 72 37 73 73
■ <b>Modalités d'accès :</b>	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
■ <b>Délais d'accès :</b>	Variable selon le type de financement.
■ <b>Accessibilité :</b>	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

## Maîtriser le système d'exploitation et les commandes UNIX liées

Méthodes d'accès au shell et paramètres

SSH : fonctionnalités

Système de fichier et commandes associées

Répertoires et commandes associées

Environnement système et utilisateur

Fichiers et commandes associées

## Analyser et exploiter les logs

Logs locaux : localisation, caractéristiques, syntaxe, catégories

Commandes associées

Fichiers de configuration

Logd, logctl, journalisation des messages noyau

**Atelier : Extraire et analyser des logs système pour identifier un incident**

## Gérer et modifier les fichiers de configuration

Répertoires, structure et syntaxe générale

Sauvegarde (\*.na), debackup, tar

Configuration usine

**Atelier : Sauvegarder et restaurer une configuration système**

## Créer et manipuler les objets réseau

Comprendre la syntaxe des objets

Gérer les objets dynamiques et FQDN

**Atelier : Configurer et tester un objet FQDN dynamique**

## Configurer et optimiser le réseau et le routage

Paramétrer les interfaces réseau

Utiliser le bridge et ses commandes associées

Gérer les fonctions de routage et leur priorité

Définir et modifier les routes par défaut et les routes statiques

Utiliser Gatemon et manipuler les objets routeurs

Configurer et exploiter le routage dynamique

Commandes relatives, affichage des routes

Mode verbose

LAB Réseau et routage

**Atelier : Configurer et tester des routes statiques et dynamiques**

## Maîtriser la capture et l'analyse de trafic

Comprendre les principes de la capture réseau et les bonnes pratiques

Utiliser la syntaxe et les arguments adaptés

Appliquer des filtres usuels pour affiner l'analyse

Étudier des exemples commentés et préparer des captures efficaces

Analyser le trafic réseau avec tcpdump (flux TCP, UDP, ICMP)

Exploiter un environnement LAB pour capturer et analyser le trafic

**Atelier : Réaliser une capture de trafic et analyser un échange réseau avec tcpdump**

## Décomposer les étapes d'analyse ASQ

Analyser les couches réseau étape par étape

Utiliser les commandes associées pour investiguer

Configurer et interpréter les paramètres globaux

Exploiter les profils et paramètres spécifiques

Étudier le fonctionnement de l'ASQ asynchrone et du watermarking

Activer et exploiter l'ASQ en mode verbose

Expérimenter avec un LAB sur les paramètres ASQ

**Atelier : Ajuster les paramètres ASQ et observer les impacts sur l'analyse réseau**

## Appliquer une politique de sécurité ASQ

Identifier et modifier les fichiers de configuration et la syntaxe des règles

Exploiter les commandes associées au filtrage

Déchiffrer des règles de filtrage et comprendre leurs actions (inspection, plugins, PBR,

QoS, proxy)

Gérer la traduction des groupes et des listes

Revoir les principes du NAT et appliquer différentes stratégies (Dynamique, Statique, Bimap)

Manipuler les commandes et la syntaxe des règles de NAT

Tester des scénarios en LAB sur NAT et filtrage

**Atelier : Créer et tester des règles de filtrage et NAT sur une infrastructure simulée**

## Comprendre le fonctionnement Stateful et les tables d'états ASQ

Analyser la table des adresses protégées et des hôtes

Étudier la table des connexions et identifier les différents états (NAT, vconn, FTP plugin, async)

Manipuler un LAB sur le suivi des états de connexion ASQ Stateful

**Atelier : Observer et analyser les connexions en temps réel dans les tables d'états**

## Gérer les Démons et Processus

Lister et comprendre le rôle des démons du système

Analyser le fonctionnement du démon Superviseur

Utiliser les commandes associées à la gestion des processus

**Atelier : Diagnostiquer et redémarrer un démon critique sur un firewall**

## Exploiter Eventd : le gestionnaire d'événements

## Configurer et sécuriser un VPN IPSec

Implémenter IKE/IPSec sur un Stormshield Network

Gérer les fichiers de configuration du VPN

**Atelier : Mettre en place un tunnel VPN IPSec entre deux équipements**

Politique de sécurité (SPD, SAD)

Comprendre le processus de négociation IKE

Comparer le mode Main et le mode Aggressive

Analyser ISAKMP et IPsec SA

Configurer les propositions IKE et gérer les particularités (NAT-T, DPD, Keepalive, SharedSA)

Manipuler les commandes et analyser une IPSec-SA

Étudier les logs et identifier les erreurs courantes

Capturer et analyser le trafic ISAKMP

Gérer les correspondants dynamiques et interpréter le mode Verbose

Travailler sur un LAB dédié à l'ISAKMP/IPSec

**Atelier : Analyser une négociation IKE et résoudre une erreur de connexion VPN**

### **Gérer les certificats et la PKI**

Revoir les concepts et directives globales de la PKI

Manipuler les répertoires de CA

Appliquer des astuces de configuration pour améliorer la gestion des certificats

Vérifier et diagnostiquer des certificats SSL

**Atelier : Importer et configurer un certificat SSL pour une connexion sécurisée**

### **Assurer la haute disponibilité**

Comprendre les principes de la haute disponibilité et ses implications

Modifier et exploiter les fichiers de configuration associés

Utiliser les commandes relatives à la gestion HA

Activer et gérer les interfaces réseau dans un environnement HA

Analyser les processus et les flux réseau impliqués

Mettre en place la réplication et la synchronisation des configurations

Suivre les événements et logs liés à la haute disponibilité

**Atelier : Déployer un cluster HA et vérifier la bascule automatique en cas de panne**