DAWAN

Plan de la formation

www.dawan.fr

Formation Fondamentaux + Certified Stormshield Network Operational Technology (NT FCSNOT)

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	3 775,00 CHF HT (standard) 3 020,00 CHF HT (remisé)
Public :	Automaticiens, responsables informatique, administrateurs réseaux, tous techniciens informatiques déployant de la sécurité réseau dans un environnement OT, n'ayant pas suivi la formation ni validé la certification CSNA
Pré-requis :	Avoir de bonnes connaissances TCP/IP, une formation réseau préalable est un plus.
Objectifs :	Prendre en main un firewall SNS et connaître son fonctionnement - Configurer un firewall dans un réseau - Définir et mettre en œuvre des politiques de filtrage et de routage - Configurer un contrôle réseau applicatif sur des automates - Configurer des politiques d'authentification - Mettre en place de réseaux privés virtuels (VPN IPsec) - Intégrer un firewall SNS à différentes architectures réseaux - Approfondir le fonctionnement de l'IPS - Configurer le mode sûreté (bypass)
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.

Modalités d’évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	RéS102500-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	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

Présentation de l’entreprise et des produits Stormshield

Découvrir l’entreprise Stormshield et ses solutions de cybersécurité
Identifier les produits et leurs domaines d’application
Comprendre l’approche de Stormshield en matière de protection réseau
Atelier : Analyser un cas d’usage d’une solution Stormshield dans un environnement industriel

Prise en main du firewall

S’enregistrer sur l’espace client et accéder aux ressources techniques
Initialiser le boîtier et explorer l’interface d’administration
Configurer le système et gérer les droits d’administration
Installer la licence et mettre à jour la version du système
Sauvegarder et restaurer une configuration du firewall
Atelier : Effectuer l’initialisation et la configuration de base d’un firewall Stormshield

Traces et supervisions

Identifier et analyser les différentes catégories de traces
Surveiller les événements réseau via les outils de supervision
Générer des rapports et interpréter les graphiques d'historiques
Atelier : Exploiter les journaux de traces pour identifier une tentative d'intrusion

Les objets

Définir les notions et types d'objets utilisables dans le firewall
Configurer des objets réseau et les intégrer aux règles de sécurité
Gérer et organiser les objets pour optimiser la lisibilité des règles
Atelier : Créer et utiliser des objets réseau pour sécuriser une infrastructure

Configuration réseau

Déterminer les modes de configuration d'un firewall dans un réseau
Configurer et paramétrer les interfaces réseau (Ethernet, bridge, VLAN, GRETAP)
Définir et prioriser les types de routage en fonction des besoins
Atelier : Configurer un firewall avec plusieurs VLAN et observer le routage des flux

Translation d'adresses (NAT)

Mettre en place une translation d'adresse sur flux sortant (déguisement)
Configurer une translation d'adresse sur flux entrant (redirection)
Optimiser la gestion des règles NAT pour une meilleure sécurité
Atelier : Configurer une redirection de port pour permettre un accès distant sécurisé

Filtrage

Expliquer les principes du filtrage et la notion de suivi de connexion (stateful)
Configurer en détail les paramètres d'une règle de filtrage
Organiser et ordonner les règles de filtrage et de translation
Atelier : Définir et tester une règle de filtrage bloquant un trafic non autorisé

Protection applicative industrielle

Analyser les protocoles industriels pour identifier les risques
Mettre en place une protection applicative standard contre les menaces connues

Développer des protections applicatives personnalisées adaptées aux besoins spécifiques

Atelier : Détecter et bloquer une tentative de communication non autorisée sur Modbus TCP