DAWAN

Plan de la formation

www.dawan.fr

Formation Certified Stormshield Endpoint Expert (STOTR-CSEE)

Durée :	2 jours (14 heures)
Tarifs inter-entreprise :	2 363,00 CHF HT (standard) 1 890,40 CHF HT (remisé)
Public :	Administrateurs systèmes et sécurité, responsables de projets, techniciens informatiques et support, ayant validé le cursus CSEA
Pré-requis :	L'accès à cette formation est réservé aux personnes ayant réussi l'examen CSEA dans les 3 ans précédant la formation CSEE
Objectifs :	Mettre à jour et modifier la solution, tout en assurant la stabilité de l'environnement - Développer les jeux de règles pour optimiser la sécurité et l'efficacité du système - Maintenir la compatibilité avec d'autres produits de sécurité - Mettre en place une politique de contrôle des périphériques - Mettre en place des mesures pour protéger les utilisateurs nomades - Maîtriser les fonctionnalités de la solution pour analyser les informations collectées - Créer des Indicateurs de Compromission (IoCs) pour améliorer la prévention des menaces.
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 :	RéS102501-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

Récapitulatif du cours Administration

Revoir les concepts fondamentaux de l’administration des systèmes de sécurité
Consolider les acquis sur la gestion des règles et des mises à jour
Atelier : Réaliser un quiz sur les notions clés de l’administration

Présenter des jeux de règles et la créer des exceptions

Définir le rôle des jeux de règles dans la sécurisation des systèmes
Identifier les scénarios nécessitant des exceptions et apprendre à les gérer
Atelier : Créer et tester une exception sur un scénario de blocage d’application légitime

Connaitre les bonnes pratiques de la mise à jour de SES Evolution

Comprendre l’importance des mises à jour pour la protection du système
Identifier les étapes clés pour une mise à jour sans interruption de service
Appliquer une méthodologie sécurisée pour tester et déployer les mises à jour

Atelier : Simuler une mise à jour et analyser son impact sur un environnement de test

Créer des jeux de règles personnalisées 1e partie

Identifier les besoins spécifiques en termes de filtrage et de protection
Configurer des jeux de règles adaptés aux usages de l'entreprise
Tester et valider les règles avant leur mise en production
Atelier : Élaborer un jeu de règles bloquant des applications non autorisées

Présentation et mise en pratique du contrôle des périphériques de stockage

Expliquer les enjeux liés à l'utilisation des périphériques de stockage externes
Configurer des règles pour restreindre ou autoriser certains périphériques
Tester les règles et analyser leur efficacité
Atelier : Déployer une stratégie de contrôle des clés USB et observer les restrictions appliquées

Comprendre et mettre en pratique le contrôle du réseau pour les utilisateurs nomades

Comprendre les risques liés aux connexions réseau en mobilité
Configurer des restrictions et sécuriser les accès des utilisateurs nomades
Mettre en œuvre une politique adaptée pour protéger les données
Atelier : Simuler une connexion distante et tester les restrictions mises en place

Créer des jeux de règles personnalisées 2e partie

Approfondir la configuration des règles avancées de sécurité
Intégrer des critères spécifiques pour affiner la détection et la protection
Tester et ajuster les règles selon les résultats obtenus
Atelier : Mettre en place une règle de détection des comportements suspects

Analyser une cyberattaque

Identifier les étapes d'une cyberattaque et ses mécanismes d'intrusion
Étudier un cas concret et retracer l'attaque à partir des logs
Déterminer les actions correctives pour renforcer la sécurité
Atelier : Reproduire une attaque simulée et analyser les traces laissées dans les journaux

Comprendre et mettre en pratique de la création d’Indicateurs de Compromission (IoCs)

Expliquer le concept des IoCs et leur rôle dans la détection des menaces
Identifier et collecter des indicateurs pertinents pour l’analyse de compromission
Mettre en place un système de détection basé sur les IoCs
Atelier : Configurer et tester un IoC pour détecter une activité malveillante sur un poste client