DAWAN

Plan de la formation

www.dawan.fr

Formation Certified Stormshield Endpoint Administrator (STOTR-CSEA)

Durée :	2 jours (14 heures)
Tarifs inter-entreprise :	2 363,00 € HT (standard) 1 890,40 € HT (remisé)
Public :	Administrateurs systèmes et sécurité, responsables de projets, techniciens informatiques et support
Pré-requis :	Connaissances système et sécurité Microsoft Windows client. Connaissances Microsoft Active Directory.
Objectifs :	À l'issue de la formation, les stagiaires seront capables de : installer et administrer la solution SES Evolution. déployer des agents SES Evolution sur un parc de postes et serveurs à protéger. mettre en place une politique pour protéger le système. récolter des informations concernant une attaque et des signaux faibles. mettre en place une politique de configuration conditionnelle. rechercher les menaces cachées.
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 :	RéS102502-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

Découvrir Stormshield et les produits Stormshield

Explorer l'entreprise Stormshield et ses solutions de cybersécurité
Identifier les différentes gammes de produits et leurs cas d'usage
Comprendre l'approche Stormshield en matière de protection des systèmes
Atelier : Analyser un cas d'usage de Stormshield dans un environnement professionnel

Comprendre l'architecture de Stormshield Endpoint Security Evolution

Décrire l'architecture de SES Evolution et ses composants
Comprendre le fonctionnement du serveur, des agents et des interactions réseau
Identifier les points clés de sécurité dans l'architecture
Atelier : Cartographier l'architecture d'un déploiement SES Evolution en entreprise

Installer et configurer le serveur SES Evolution

Installer et paramétrer le serveur SES Evolution
Configurer les bases de données et les services associés
Vérifier le bon fonctionnement du serveur après installation
Atelier : Installer un serveur SES Evolution et valider son bon fonctionnement

Prendre en main la console d'administration

Explorer l’interface et les fonctionnalités de la console SES Evolution
Naviguer dans les différentes sections et comprendre leur utilité
Personnaliser les paramètres pour répondre aux besoins de l’entreprise
Atelier : Configurer un tableau de bord personnalisé sur la console d’administration

Gérer et installer les agents SES Evolution

Déployer et configurer les agents SES Evolution sur des postes clients
Vérifier la communication entre les agents et le serveur
Gérer les mises à jour et la maintenance des agents
Atelier : Installer et tester un agent SES Evolution sur un poste de travail

Configurer les politiques de sécurité et les politiques conditionnelles

Comprendre les politiques de sécurité et leur rôle dans la protection des postes
Configurer une politique conditionnelle adaptée aux usages de l’entreprise
Tester l’impact des politiques sur les agents déployés
Atelier : Créer une politique conditionnelle bloquant un accès réseau suspect

Analyser et filtrer les logs : identifier les menaces et les faux positifs

Examiner les logs pour détecter les événements suspects
Distinguer une menace réelle d’un faux positif
Optimiser le filtrage des logs pour une meilleure lisibilité
Atelier : Analyser des logs et ajuster les règles de détection pour réduire les faux positifs

Collecter et transférer des événements externes (Remontées de logs Microsoft dans SES)

Configurer l’intégration de sources de logs externes dans SES Evolution
Automatiser la remontée des événements critiques
Analyser les logs externes pour améliorer la détection des menaces
Atelier : Intégrer des logs Microsoft dans SES et détecter une activité suspecte

Déployer et tester la protection anti-ransomware

Expliquer le fonctionnement de la protection anti-ransomware de SES Evolution
Configurer une stratégie de défense contre les attaques de chiffrement

Tester la détection et la réponse à une simulation d’attaque
Atelier : Simuler une attaque par ransomware et observer la réaction de SES Evolution

Chasser les menaces et appliquer la remédiation

Identifier les techniques de chasse aux menaces sur un système protégé
Exploiter les outils de SES Evolution pour détecter des comportements malveillants
Appliquer des actions de remédiation en réponse à une menace détectée
Atelier : Traquer un processus suspect et appliquer une remédiation via SES Evolution

Assurer la maintenance et le dépannage de l’agent SES

Diagnostiquer les problèmes courants des agents SES Evolution
Appliquer les bonnes pratiques de maintenance pour garantir la stabilité du système
Mettre en œuvre des solutions de dépannage en cas de dysfonctionnement
Atelier : Simuler un incident sur un agent et effectuer un dépannage pas à pas