DAWAN

Plan de la formation

www.dawan.fr

Formation Wazuh : Sécuriser son infrastructure

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 225,00 € (standard) 1 780,00 € (remisé)
Public :	Administrateurs système
Pré-requis :	Avoir les bases en cybersécurité
Objectifs :	Maitriser Wazuh afin de mieux sécuriser son infrastructure
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 :	RéS102319-F
Note de satisfaction des participants:	4,43 / 5
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

Jour 1 : Configuration Initiale

La configuration de base :

- Méthodes de déploiement : All-in-One ou Distributed / standalone ou docker-compose.
- Les decodeurs et les règles.
- L’envoi automatique de mails critiques.
- La détection de vulnérabilités et les benchmarks CIS.
- Les vue sur le dashboard

Atelier pratique :

- Corrélation de règles et création des vues custom

Jour 2 : Configuration avancée

Surveillance des logs Windows et Linux :

- Vérification de l’intégrité (hash) en temps réel & gestion des whitelists.
- Réponse active personnalisée.
- Gestion des logs
- Audit de pentest pour tester l’efficacité

Jour 3 : Configuration supplémentaire

Intégration de Suricata et le Machine Learning d'Opensearch