

## Formation Wazuh : Sécuriser son infrastructure

■ <b>Durée :</b>	3 jours (21 heures)
■ <b>Tarifs inter-entreprise :</b>	2 225,00 CHF (standard) 1 780,00 CHF (remisé)
■ <b>Public :</b>	Administrateurs système
■ <b>Pré-requis :</b>	Avoir les bases en cybersécurité
■ <b>Objectifs :</b>	Maitriser Wazuh afin de mieux sécuriser son infrastructure

■ <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>	RÉS102319-F
----------------------	-------------

■ <b>Note de satisfaction des participants:</b>	4,43 / 5
---	----------

■ <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.
---------------------------	--

## ■ 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](mailto: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