# FortiAnalyser

Durée : 1 Jours

## Résumé

Dans ce cours d'une journée, les étudiants apprendront les fondamentaux de l'utilisation de FortiAnalyzer 6.2 pour la journalisation et le reporting centralisés. Ils apprendront à configurer et à déployer FortiAnalyzer, ainsi qu'à identifier les menaces et les modèles d'attaques grâce à la journalisation, à l'analyse et au reporting. Enfin, les étudiants examineront quelques techniques de dépannage utiles.
Dans des laboratoires interactifs, les étudiants exploreront l'administration et la gestion ; enregistreront des dispositifs pour la collecte de journaux avec FortiAnalyzer ; utiliseront FortiAnalyzer pour collecter des journaux de manière centralisée ; réaliseront une analyse judiciaire des journaux basée sur des attaques réseau simulées ; créeront des rapports ; et exploreront des solutions aux problèmes de configuration courants.

## Public visé

Toute personne responsable de la gestion quotidienne des dispositifs FortiAnalyzer et des informations de sécurité FortiGate.

## Objectifs

Après avoir suivi ce cours, vous serez en mesure de :

- Décrire les caractéristiques et concepts clés de FortiAnalyzer
- Déployer une architecture appropriée
- Utiliser des contrôles d'accès administratifs
- Surveiller les événements et tâches administratifs

- Gérer les ADOMs
- Configurer RAID
- Enregistrer les dispositifs pris en charge
- Dépanner les problèmes de communication
- Gérer le quota de disque
- Gérer les dispositifs enregistrés
- Protéger les informations de journalisation
- Afficher et rechercher des journaux
- Dépanner et gérer les journaux
- Surveiller les événements
- Générer et personnaliser des rapports
- Personnaliser les graphiques et les ensembles de données
- Gérer les rapports
- Dépanner les rapports

---

## Contenu

- Introduction et configuration initiale
- Administration et gestion
- Enregistrement des dispositifs et communication
- Journalisation
- Rapports