

# FortiAnalyzer Administrateur

## Préparation à la certification Fortinet Network Security

Cours Pratique de 2 jours - 14h

Réf : FND - Prix 2024 : 1 660€ HT

Vous apprendrez comment inscrire puis gérer vos équipements avec FortiAnalyzer. Vous explorerez les fondamentaux de la journalisation et de la gestion des rapports. L'intérêt de FortiAnalyzer est l'ajout de la valeur aux journaux remontés par un parc d'équipements FortiGate.

### OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Décrire l'utilité de FortiAnalyzer

Décrire les modes de fonctionnement de FortiAnalyzer

Comprendre la journalisation dans un environnement Security Fabric Fortinet

Gérer les domaines administratifs (ADOM)

Configurer des accès administrateurs sécurisés

Configurer les paramètres réseau

Gérer les quotas de disque

Effectuer une sauvegarde de la configuration du système

Gérer le RAID et la haute disponibilité

Inscrire puis gérer les FortiGate

Décrire les flux de travail (workflow) du fichier journal

Effectuer des sauvegardes de journaux

Comprendre la notion de connecteurs Fabric

Gérer les rapports

### MÉTHODES PÉDAGOGIQUES

Pédagogie active favorisant l'implication personnelle et les échanges entre participants.

Travaux pratiques individuels ou en groupe.

### CERTIFICATION

Ce cours est conçu à l'intention des candidats qui souhaitent passer l'examen Fortinet NSE6 – FortiAnalyzer Administrator. La réussite à cet examen (badge) intervient en tant qu'électif dans le parcours de certification Fortinet Certified Professional - Network Security.

### PARTICIPANTS

Ce cours s'adresse à toute personne déployant, configurant et sécurisant FortiAnalyzer.

### PRÉREQUIS

Connaissances des concepts TCP/IP et pare-feu requises pour suivre ce stage. Il est également conseillé d'avoir suivi la formation FNA – FortiOS ou d'avoir les connaissances équivalentes.

### COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

### MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques... Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

### MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

### MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

### ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

## LE PROGRAMME

dernière mise à jour : 02/2024

### 1) Introduction et réglages initiaux

- Fonctionnalités clés.
- Configuration initiale.
- Exemples d'usages.

### 2) Administration / Gestion

- Les ADOM.
- Comptes administrateurs.
- Surveiller les événements et les tâches d'administration.
- Gérer les quotas de disque.
- Sauvegarder le système, meilleures pratiques.

### 3) RAID et haute disponibilité

- Protéger les données de journaux à l'aide de RAID.
- Utiliser la haute disponibilité.

### 4) Gestion des dispositifs

- Inscrire / Enregistrer les dispositifs FortiGate.
- Dépanner les communications défailtantes entre les dispositifs FortiGate et FortiAnalyzer.
- Gérer les dispositifs enregistrés.

### 5) Journaux et gestion des rapports

- Gérer les données des journaux.
- Notions liées aux rapports.
- Gérer les rapports.

## LES DATES

---

Nous contacter