

Formation FortiAnalyzer de Fortinet

(EDU-NSE5)

1 jour (7 heures)

Présentation

FortiAnalyzer Network Security Logging, Analysis, et Reporting Appliances regroupent en toute sécurité les données des journaux de Fortinet Security Appliances. Une suite complète de rapports facilement personnalisables vous permet d'analyser et de visualiser rapidement les menaces, les inefficacités et l'utilisation du réseau. Cette formation se basera sur la dernière version de l'outil : [FortiAnalyzer 6.4](#).

Objectifs

- Décrire les fonctionnalités du FortiAnalyzer
- Déployer la bonne architecture par rapport aux besoins exprimés par vos clients
- Administrer les ADOMs
- Configurer les RAID
- Inscrire les équipements qui enverront les logs
- Chiffrer les communications entre les équipements et le FortiAnalyzer (SSL et IPSEC)
- Visualiser et analyser les logs
- Surveiller les événements et mettre en place des alertes
- Appliquer des quotas disque pour chaque équipement
- Sauvegarder, restaurer et exporter des logs
- Utiliser l'archive de contenu
- Comprendre les différentes étapes du traitement des logs
- Comprendre les requêtes SQL utilisées dans les datasses
- Créer un dataset, un char puis utiliser ce dernier dans un rapport
- Générer des rapports à la demande ou programmer

Public visé

À tous ceux qui sont en charge de la gestion des logs et de la mise en place de rapports sur le FortiAnalyzer.

Prérequis

- Le suivi des cours Fortigate I et II est un plus.

Programme

1. Introduction au FortiAnalyzer
2. Configuration et administration
3. Inscription des équipements qui

enverront leurs logs sur le FortiAnalyzer4. Les logs et les archives5. Les rapports

Format du cours

Instructeur qui présentera chacun des modules. Exercices pratiques à la fin de chaque module.

Certification

Les cours FortiAnalyzer et FortiManager préparent au passage de la certification NSE5.

Sociétés concernées

Cette formation s'adresse aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiple permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.