FORTINET - NSE5 - FortiAnalyser

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Toute personne en charge de la gestion des logs et de la mise en place de rapports sur le FortiAnalyzer

Objectifs de la formation

• 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 datasets • Créer un dataset, un chart puis utiliser ce dernier dans un rapport • Générer des rapports à la demande ou programmés

Description sommaire

La plateforme FortiAnalyzer de Fortinet assure les fonctions de journalisation, d'analyse et de reporting réseau au sein d'un seul système. Cette journée de formation vous apprendra à utiliser FortiAnalyzer. Dans un premier temps, vous découvrirez l'interface d'administration, apprendrez à inscrire de nouveaux équipements et à sécuriser les communications avec le FortiAnalyzer. Puis vous manipulerez les logs et les archives, les rapports existants et configurerez des rapports personnalisés. À l'issue de cette formation, vous aurez une solide compréhension du FortiAnalyzer et saurez comment le déployer dans des environnements simples ou complexes.

Contenu du plan de cours

• Introduction au FortiAnalyzer • Configuration et administration • Inscription des équipements qui enverront leurs logs sur le FortiAnalyzer • Les logs et les archives • Les rapports

Approche et méthode pédagogique

La formation repose sur une approche pratique centrée sur des laboratoires techniques, permettant aux participants de manipuler directement les logs, les équipements et les rapports. Elle combine démonstrations guidées et exercices progressifs, afin de développer une maîtrise opérationnelle du FortiAnalyzer. L'apprentissage est orienté vers des cas concrets d'analyse et de surveillance, proches des réalités terrain.

Recommandations

Avoir suivi la formation Certification NSE 4 - FortiGate I et II : Network Security Professional (NSE4) ou contenu équivalent est un vrai plus pour aborder cette formation dans de bonnes conditions