Microtel
Training institute

FORTINET - FORTIANALYZER - NSE5

CURSUS:
SÉCURITÉ DES SYSTÈMES D'INFORMATION

CODE DE LA FORMATION:
FT-SC-FORTIANALYZER

ÉDITEUR OU CONSTRUCTEUR:
FORTINET

DURÉE:
1 JOUR

PUBLIC:

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

OBJECTIFS:

A l'issue de cette session qui se déroule sur une journée vous serez en mesure de :

- 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 rapp

CONTENU:

1. Introduction au FortiAnalyzer
2. Configuration et administration
3. Inscription des équipements qui enverrontleurs logs sur le FortiAnalyzer
4. Les logs et les archives
5. Les rapports