FortiAnalyzer — Centralized Log & Analytics

Fortinet Security Analytics — Programme Complet

22 Modules	5 Blocs Thématiques	Certification Fortinet NSE

Bloc 1 — Introduction à FortiAnalyzer

M01	Architecture FortiAnalyzer et rôle dans le Security Fabric
M02	Installation et configuration initiale (VM / appliance)
M03	Gestion des licences et des administrateurs
M04	Interface GUI et navigation dans FortiAnalyzer

✓ *Examen Checkpoint : Fondements FortiAnalyzer*

Bloc 2 — Collecte et Gestion des Logs

M05	Enregistrement des appareils Fortinet (FortiGate, FortiAP, FortiSwitch)
M06	Configuration des politiques de log et des niveaux de sévérité
M07	Stockage des logs : local, NAS et archivage
M08	Compression, chiffrement et rétention des logs
M09	Collecte de logs tiers via Syslog et CEF

✓ *Examen Checkpoint : Collecte et gestion des logs*

Bloc 3 — Analyse, Recherche et Corrélation

M10	Log viewer : recherche, filtres et vues personnalisées
M11	FortiView : tableaux de bord temps réel et analytique
M12	Corrélation d'événements et détection d'incidents
M13	Threat Hunting et investigation forensique

✓ *Examen Checkpoint : Analyse et corrélation des événements*

Bloc 4 — Rapports et Tableaux de Bord

M14	Création de rapports personnalisés et templates
M15	Planification et envoi automatique de rapports
M16	Tableaux de bord personnalisés et widgets
M17	Conformité : rapports PCI-DSS, HIPAA et ISO 27001

✓ *Examen Checkpoint : Rapports et tableaux de bord*

Bloc 5 — Administration Avancée et Haute Disponibilité

M18	ADOM (Administrative Domain) : création et gestion
M19	FortiAnalyzer HA : clustering et réplication
M20	Sauvegarde, restauration et migration FortiAnalyzer
M21	Intégration avec FortiSIEM et FortiSOAR
M22	API REST FortiAnalyzer et automatisation des tâches

✓ *Examen Checkpoint : Administration avancée et HA FortiAnalyzer*

Évaluations Finales

Examen Blanc FortiAnalyzer

Préparation à la certification officielle Fortinet

Examen Final FortiAnalyzer

Certification Fortinet NSE — Log & Analytics
