FortiSIEM — Security Information & Event Management

Fortinet SIEM & SOC Analytics — Programme Complet

24 Modules	6 Blocs Thématiques	Certification Fortinet NSE

Bloc 1 — Introduction à FortiSIEM et au SOC

M01	Concepts SIEM : collecte, corrélation et réponse aux incidents
M02	Architecture FortiSIEM : Supervisor, Worker et Collector
M03	Installation et déploiement FortiSIEM (VM / cloud)
M04	Interface GUI FortiSIEM : navigation et tableaux de bord SOC

✓ *Examen Checkpoint : Fondements SIEM et architecture FortiSIEM*

Bloc 2 — Collecte et Normalisation des Événements

M05	Découverte automatique des assets et inventaire réseau
M06	Collecte de logs : Syslog, SNMP, WMI, API et agents
M07	Parseurs FortiSIEM : normalisation et enrichissement des logs
M08	Collecte de logs Fortinet : FortiGate, FortiAP, FortiSwitch
M09	Collecte de logs tiers : Cisco, Windows, Linux, Azure, AWS

✓ *Examen Checkpoint : Collecte et normalisation des événements*

Bloc 3 — Corrélation et Détection des Menaces	
M10	Règles de corrélation : création et personnalisation
M11	MITRE ATT&CK; : mapping des règles aux techniques d'attaque
M12	User and Entity Behavior Analytics (UEBA)
M13	Threat Intelligence : intégration des IOC et feeds externes
M14	Machine Learning : détection des anomalies comportementales
✓ Examen Checkpoint : Corrélation et détection des menaces	

Bloc 4 — Gestion des Incidents et Réponse	
M15	Gestion des incidents : création, escalade et résolution
M16	Playbooks de réponse aux incidents (SOAR FortiSIEM)
M17	Intégration FortiSIEM avec FortiSOAR pour l'automatisation
M18	Forensique numérique : investigation et recherche d'IOC
✓ Examen Checkpoint : Gestion des incidents et réponse aux menaces	

Bloc 5 — Rapports, Conformité et Tableaux de Bord	
M19	Rapports de conformité : PCI-DSS, HIPAA, GDPR, ISO 27001
M20	Tableaux de bord SOC personnalisés et KPIs
M21	Planification et export des rapports FortiSIEM
✓ Examen Checkpoint : Rapports et conformité réglementaire	

Bloc 6 — Administration Avancée et Haute Disponibilité	
M22	FortiSIEM HA : clustering Supervisor et Workers
M23	Sauvegarde, restauration et migration FortiSIEM
M24	API REST FortiSIEM et intégration avec les outils SOC tiers
✓ Examen Checkpoint : Administration avancée et HA FortiSIEM	

Évaluations Finales

Examen Blanc FortiSIEM / SOC
Préparation à la certification officielle Fortinet

Examen Final FortiSIEM
Certification Fortinet NSE — SIEM & SOC Analytics