

Certifiante Sessions garanties disponibles

Formation FortiAnalyzer Analyst, préparation à l'examen Fortinet NSE 5

Réf. SF34163

Développez les réflexes d'un analyste SOC : centralisez les logs, détectez les menaces et automatisez la réponse avec FortiAnalyzer !

2 j
Durée

2 000 € HT
Inter / participant

14
Sessions à venir

Objectifs pédagogiques

- ✓ Expliquer les objectifs d'un SOC, ses responsabilités et ses rôles, ainsi que la place de FortiAnalyzer dans ce dispositif.
- ✓ Décrire l'intégration de FortiAnalyzer à la Security Fabric et le fonctionnement du logging au sein de l'écosystème.
- ✓ Comprendre les déploiements et modes de fonctionnement de FortiAnalyzer, ainsi que la normalisation des logs.
- ✓ Rechercher, filtrer et analyser les journaux (champs normalisés, vues logs, filtres sauvegardés, tableaux de bord, FortiView).
- ✓ Configurer et administrer la détection : gestionnaires d'événements, événements, indicateurs et paramètres d'incident.
- ✓ Créer et mener l'analyse d'incidents, incluant l'identification de menaces actuelles ou potentielles (incidents, alertes outbreak, statistiques de volume).
- ✓ Exploiter FortiAI et les fonctions de threat hunting pour accélérer l'investigation et le diagnostic.
- ✓ Produire et maintenir des rapports, et automatiser la réponse via automation stitches et playbooks (création, variables, supervision, import/export).

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Ingénieurs télécoms et réseaux

Prérequis Connaissances équivalentes aux formations : FortiGate Operator et FortiAnalyzer Administrator (ou expérience comparable). Maîtrise de la syntaxe SQL SELECT.

Programme détaillé

Concepts SOC et Security Fabric

Objectifs, responsabilités et rôles d'un SOC
Rôle de FortiAnalyzer dans un SOC
Intégration FortiAnalyzer / Security Fabric
Mécanismes de journalisation dans la Security Fabric
Déploiements FortiAnalyzer au sein de la Fabric
Modes de fonctionnement de FortiAnalyzer

Flux de logs et navigation

Analyse, parsing et normalisation des journaux
Validation des parseurs de logs
Recherche à partir des champs normalisés
Consultation et recherche dans la vue des logs
Filtres enregistrés et création de tableaux de bord
Lecture des données de synthèse via FortiView
Tableaux de bord et fonctionnalités des widgets

Événements, indicateurs et incidents

Configuration des gestionnaires d'événements
Administration et suivi des événements

Mise en place des indicateurs
Création d'incidents
Analyse d'incidents
Paramétrage et réglages liés aux incidents

FortiAI, threat hunting et dépannage

Principes de fonctionnement et cas d'usage de FortiAI
Démarche de threat hunting
Exploitation du graphique de comptage de logs
Utilisation de la table d'analytique SIEM des logs
Compréhension des alertes d'outbreak
Collecte de statistiques de volumétrie des logs

Rapports

Exécution et ajustement des rapports prédéfinis
Personnalisation (macros, graphiques personnalisés, jeux de données)
Configuration d'un stockage externe pour les rapports
Regroupement de rapports
Import et export de rapports et graphiques
Association de rapports à des incidents
Administration et résolution des problèmes liés aux rapports

Playbooks

Création de nouveaux playbooks
Utilisation de variables dans les tâches
Supervision et suivi d'exécution des playbooks
Import et export de playbooks
Configuration d'une automation stitch
Activation d'une automation stitch via un gestionnaire d'événements

Prochaines sessions

DATE	LIEU	STATUT
05/11/2026	à distance	Sur confirmation
10/12/2026	Paris	Sur confirmation
10/12/2026	à distance	Sur confirmation
14/01/2027	à distance	Sur confirmation
18/02/2027	à distance	Sur confirmation
11/03/2027	Paris	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Abderrahmane B. — Formatrice Solutions Constructeurs & Éditeurs

Abderrahmane intervient sur des formations portant sur les solutions de sécurité des constructeurs et éditeurs. Parmi les formations qui lui sont confiées figurent notamment « Fortinet, SD-WAN Architect » et...

Ils nous font confiance

Cette année notre filière Cybersécurité et Protection des Données a accompagné plus de 69 entreprises dont :

AVEM MÉTROPOLE DE LYON ACTIMAGE CONSULTING SAS ADISTA ADVENTIEL AIGA ALCYOR ALDORIA ALSTOM ALTEN SA +59 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com