

FortiSIEM

Réf. FCP-SIEM · Fortinet · Cybersécurité ·

Formation certifiante

DURÉE 2 jours	NIVEAU Avancé	MODALITÉS Présentiel · Live · Intra	VOUCHER EXAMEN Inclus
-------------------------	-------------------------	---	---------------------------------

Présentation

Cette formation avancée vous apprend à déployer et exploiter FortiSIEM pour la collecte, la corrélation et l'analyse des événements de sécurité et de performance. Vous couvrez la découverte des actifs, les règles de corrélation et la gestion des incidents. Elle est idéale pour les analystes SOC et ingénieurs sécurité.

Objectifs pédagogiques

- Déployer l'architecture FortiSIEM (Supervisor, Collectors, Workers)
- Découvrir et inventorier les actifs dans la CMDB
- Collecter et normaliser les logs multi-sources
- Créer des règles de corrélation et des analytics
- Gérer les incidents et les notifications
- Concevoir des tableaux de bord et des rapports de conformité

Programme détaillé

1. Module 1 — Architecture et déploiement

- Composants FortiSIEM
- Modes de déploiement
- Collectors et Workers
- Licensing

2. Module 2 — Découverte et CMDB

- Discovery des équipements
- CMDB et device types
- Monitoring de performance
- Business services

3. Module 3 — Logs et corrélation

- Parsing et normalisation
- Règles de corrélation
- Watch lists
- Analytics

4. Module 4 — Incidents et reporting

- Gestion des incidents
- Notifications et remediation
- Dashboards
- Rapports de conformité

Prérequis

Connaissances des concepts de sécurité réseau, des logs et de l'administration systèmes et réseaux.

Public visé

Analystes SOC, ingénieurs et administrateurs sécurité, responsables supervision.

Ce qui est inclus

- Support de cours officiel Fortinet FortiSIEM
- Labs pratiques de corrélation et gestion d'incidents
- Voucher d'examen de certification FCP
- Attestation de réussite Advancia Training
- Formateur certifié Fortinet, pauses café et déjeuner inclus

Certification

Formation certifiante contribuant au cursus FCP ; l'examen élective FortiSIEM se présente au format QCM d'environ 30 questions. Advancia Training est centre d'examen agréé Pearson VUE.

750 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible