

Nouveau Certifiante

Formation Cortex XSIAM: Security Operations, Integration and Automation (XSIAM-SOIA)

Réf. SF34613

Prenez en main la plateforme Cortex XSIAM de Palo Alto Networks et transformez vos opérations de sécurité grâce à l'automatisation, l'analyse avancée et une détection des menaces unifiée.

3 j
Durée

3 000 € HT
Inter / participant

0
Sessions à venir

Objectifs pédagogiques

- ✓ Maîtriser l'architecture Cortex XSIAM : rôle des agents, collecteurs XDR, pare-feux nouvelle génération et VMs Broker
- ✓ Exploiter le langage XQL pour interroger les journaux, corrélérer les événements et affiner la détection
- ✓ Concevoir des règles de détection personnalisées adaptées aux menaces de votre environnement
- ✓ Intégrer des sources de données tierces et orchestrer des workflows de réponse automatisés
- ✓ Configurer le Threat Intel Management et appliquer des listes de blocage dynamiques (EDL) et des règles d'indicateurs
- ✓ Cartographier et superviser la surface d'attaque de votre organisation
- ✓ Personnaliser les tableaux de bord et l'interface pour optimiser le travail des analystes
- ✓ Se préparer à l'examen de certification Palo Alto Networks Certified XSIAM Engineer

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Architectes, Ingénieurs télécoms et réseaux

Prérequis Expérience préalable dans le déploiement de solutions de sécurité d'entreprise et bonne maîtrise des fondamentaux réseau et cybersécurité.

Programme détaillé

Contenu du cours

Découverte de Cortex XSIAM
Composants logiciels de la plateforme
Requêtes et analyse avec XQL
Ingénierie de la détection
Intégrations et connecteurs
Automatisation des workflows
Gestion du renseignement sur les menaces
Analyse de la surface d'attaque
Personnalisation de l'interface utilisateur

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

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 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

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