

Palo Alto Networks – Cortex XSIAM – Opérations de sécurité, intégration et automatisation

3 jours (21 heures)

Expertise

à partir de

2 915 € HT par personne (TVA en vigueur)

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Décrire le fonctionnement des agents, des collecteurs XDR, des NGFW et des VM Broker
- Interroger et analyser les journaux à l'aide de XQL pour l'ingestion et la détection des données
- Configurer les fonctionnalités de Threat Intel Management, automatiser les workflows et appliquer les EDL et les règles d'indicateurs.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Ingénieurs et responsables SOC / CERT / CSIRT / XSIAM, MSSP et partenaires de services / intégrateurs de systèmes, consultants internes et externes en services professionnels et ingénieurs commerciaux, ingénieurs SIEM et ingénieurs en automatisation.

Prérequis

Etre familiarisé avec le déploiement de produits d'entreprise, les réseaux et les concepts de sécurité.

L'apprenant s'engage à respecter les prérequis nécessaires via un questionnaire qui lui sera transmis en amont de la formation.

Programme

1 Pendant votre formation

Palo Alto Networks – Cortex XSIAM – Opérations de sécurité, intégration et automatisisation

Présentation de Cortex XSIAM

Composants logiciels

XQL

Ingénierie de la détection

Intégrations

Automatisation

Gestion des menaces

Gestion de la surface d'attaque

Personnalisations de l'interface utilisateur

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap