

Palo Alto Networks – Cortex XDR – La vue d'ensemble : comment administrer et investiguer

4 jours (28 heures)

Expertise

à partir de

3 890 € 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 rôle des composants Cortex XDR, notamment les agents de terminaux, les collecteurs XDR, les pare-feux nouvelle génération (NGFW) et les machines virtuelles Broker, dans la sécurisation des réseaux et des appareils
- Utiliser XQL pour interroger et analyser les journaux afin de permettre une ingestion efficace des données et la détection des menaces
- Concevoir et mettre en oeuvre des workflows pour rationaliser les opérations de sécurité.

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

À qui s'adresse cette formation ?

Professionnels de la sécurité (notamment les analystes SOC, CERT, CSIRT et XDR, les responsables, les intervenants en cas d'incident et les chasseurs de menaces), consultants en services professionnels, ingénieurs commerciaux et partenaires de prestation de services.

Prérequis

Avoir une compréhension fondamentale des principes de cybersécurité et une expérience dans l'analyse des incidents et l'utilisation d'outils de sécurité pour les enquêtes. Il est également recommandé d'être familiarisé avec les déploiements d'entreprise, le réseau et les bases de la 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 XDR – La vue d'ensemble : comment administrer et investiguer

Présentation de Cortex XDR

Composants logiciels

Intégrations

XQL

Ingénierie de détection

Automatisation de la plateforme

Optimisation du système

Tableaux de bord et rapports

Sécurité des e-mails

Terminaux

Alertes et détection

Vulnérabilité et analyse forensique

Automatisation de la plateforme

Gestion des cases

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