

# Palo Alto Networks – Cortex XDR – Investigation et analyse

2 jours (14 heures)

Expertise

à partir de

**2 145 € HT** par personne (TVA en vigueur)

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

## Objectifs

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

- Enquêter sur les cas, analyser les actifs et artefacts clés et interpréter la chaîne de causalité
- Interroger et analyser les journaux à l'aide de XQL afin d'en extraire des informations pertinentes
- Mettre en pratique des outils et ressources avancés pour une analyse complète des cas.

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

## À qui s'adresse cette formation ?

Analystes SOC, CERT, CSIRT et XDR, responsables, intervenants en cas d'incident et 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

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 – Investigation et analyse

Introduction à Cortex XDR

Terminaux

XQL

Alertes et détection

Vulnérabilité et analyse forensic

Automatisation de la plateforme

Gestion des cases

Tableaux de bord et rapports

## 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