[PAN-EDU-262]

- **Objectifs**
  - **Enquêter et gérer les incidents**
  - **Décrire la causalité Cortex XDR et les concepts analytiques**
  - **Analyser les alertes à l'aide des vues Causalité et Chronologie**
  - **Travailler avec les actions Cortex XDR Pro telles que l'exécution de scripts à distance**
  - **Créer et gérer des requêtes de recherche à la demande et les planifier dans le Centre de requêtes**
  - **Créer et gérer les règles Cortex XDR BIOC et IOC**
  - **Travailler avec les actifs et les inventaires Cortex XDR**
  - **Écrire des requêtes XQL pour rechercher des ensembles de données et visualiser les ensembles de résultats**
  - **Travailler avec la collecte de données externes de Cortex XDR**
- **Public visé :** Analystes en cybersécurité, Administrateurs Système et les personnes en charge du déploiement.
- **Prérequis**
  - Avoir suivi la formation PAN-EDU-260 (Cortex XDR: Prevention and Deployment)
  - Être familiarisés avec l'analyse d'événements de sécurité.
- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Cyberdefense

Palo Alto Networks Cortex XDR 3.6 : Investigation and Response

Programme de formation

- **Module 1 : Incidents Cortex XDR**
- **Module 2 : Concepts de causalité et d'analyse**
- **Module 3 : Analyse de causalité des alertes**
- **Module 4 : Actions de réponses avancées**
- **Module 5 : Créer des requêtes de recherche**
- **Module 6 : Construire des règles XDR**
- **Module 7 : Actifs Cortex XDR**
- **Module 8 : Introduction à XQL**
- **Module 9 : Collecte de données externes**

[PAN-EDU-262] Palo Alto Networks Cortex XDR 3.6 : Investigation and Response

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas, démonstrations et cas pratiques sur des labs hébergés
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des études de cas et travaux pratiques
- QCM en fin de formation

CERTIFICATION PREPAREE :
Certification Palo Alto Networks "Next-Generation Firewall Engineer" (3ème niveau/Specialist) sur les 4 niveaux de certification que regroupe le Network Security).
Durée de validité : 2 ans

Durée	2 jours (14 heures)
Groupe de formation	De 3 à 10 participants
Langue	Français / Anglais
Mode de déploiement	Présentiel / Distanciel / E-learning
Modalités	Intra / Inter / Sur-mesure
Tarif	Sur devis / 2 145€ HT par participant / Sur devis

*Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (durée : environ 1h30 - en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue.

Demande de devis – Modalités et délais d'accès

- **Pour toute demande inter**, nous vous invitons à **consulter le planning des sessions** et à compléter le **bulletin d'inscription accessible en fin de catalogue**
- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).

Cyberdefense