



DESCRIPTIF DE COURS

Palo Alto Networks Cortex™ XDR 3.6: Prevention and Deployment

PAN-EDU-260

PRESENTATION DE LA FORMATION PAN-EDU-260

Cette formation dispensée par un instructeur agréé vous montrera comment vous protéger des attaques sur vos postes de travail. Après une vue rapide des différents composants de Cortex XDR, cette formation couvrira la console Cortex XDR ainsi que les différentes étapes de création des agents, profils de sécurité et des politiques de sécurité.

Cette formation vous permet d'apprendre les actions de réponse, ajuster les profils de sécurité ainsi que de travailler avec les alertes de Cortex XDR. La formation se terminera par des discussions sur les techniques d'investigations de problèmes liés à Cortex, la mise en place d'une Broker VM et le déploiement de Cortex XDR.

Ce cours combine théorie et ateliers pratiques.

DUREE DE LA FORMATION

3 jours, soit 21 heures

PUBLIC CONCERNE

Ce cours est recommandé pour les Analystes en cybersécurité, Administrateurs Système et les personnes en charge du déploiement.

PRE-REQUIS

Les participants doivent être familiarisés avec les déploiements d'entreprise, le réseau et les bases de la sécurité.

OBJECTIFS DE LA FORMATION

L'alternance des modules de cours avec des sessions de labs devrait vous permettre de :

- Décrire l'architecture et les composants de la famille Cortex XDR.
- Utiliser la console web Cortex XDR, les rapports et les dashboards
- Créer des packages d'installation, des groupes d'endpoints et des stratégies d'agent Cortex XDR.
- Déployer l'agent sur les endpoints
- Créer et gérer des profils de prévention contre les exploits et les logiciels malveillants
- Examiner les alertes et classez-les par ordre de priorité à l'aide de stratégies de score, de favori ou d'exclusion.
- Gérer les exceptions à l'aide des profils de sécurité Cortex
- Initier et suivre les actions de réponse dans le centre d'action Cortex
- Chercher et résoudre les problèmes de l'agent Cortex
- Installer une Broker VM et activer l'applet Local Agents Settings
- Déployer l'agent Cortex et comprendre les différents modes d'activation
- Travailler avec le portail de support et la gateway Cortex XDR pour l'authentification et les autorisations des utilisateurs

APPELEZ LE 01 60 19 16 27

MIEL

5 Parc Burospace
91570 BIEVRES
SIRET : 33131183700032

Centre Agréé :
N°11 91 03 54 591

Pour consulter le
planning des formations
: www.miel.fr/formation

Formations sur Paris,
Bievres (91) et en
régions

Pour les Personnes en
Situation de Handicap
(PSH), contactez le
Service Formation.

Coordonnées Service
Formation et
Réclamations
01 60 19 16 27
formation@miel.fr



DESCRIPTIF DE COURS

CONTENU DE COURS

Module 1 : Présentation de Cortex XDR

Module 2 : Principaux composants du Cortex XDR

Module 3 : Console de gestion Cortex XDR

Module 4 : Profils et politiques

Module 5 : Protection contre les logiciels malveillants

Module 6 : Protection contre les exploits

Module 7 : Alertes Cortex XDR

Module 8 : Exclusions et exceptions

Module 9 : Mesures de réponse

Module 10 : Dépannage de base

Module 11 : Aperçu de la Broker VM

Module 12 : Considérations de déploiement

CERTIFICATION PREPAREE

PCDRA: Palo Alto Networks Certified Detection and Remediation Analyst
Durée de validité : 2 ans

Il s'agit de la seule certification technique existant sur les produits Palo Alto Networks Cortex XDR.

PASSAGE DE LA CERTIFICATION

Le prix de cette formation **ne comprend pas** le voucher pour le passage de l'examen (en anglais), qui s'effectuera ultérieurement en centre de certification Pearson VUE (durée de l'examen : 90 minutes).

Pour plus de détails cliquer sur le lien suivant :

[Schéma de suivi des formations / certifications Palo Alto Networks](#)

PREREQUIS CERTIFICATION

Aucune certification technique ne sera nécessaire pour être détenteur de la certification PCDRA (Palo Alto Networks Certified Detection and Remediation Analyst).

APPELEZ LE 01 60 19 16 27



DESCRIPTIF DE COURS

FREQUENCE DE LA FORMATION

La formation PAN-EDU-260 est planifiée au rythme d'une session par trimestre (inter-entreprises).

Miel se réserve le droit d'annuler une session jusqu'à 5 jours avant sa date de début en cas d'insuffisance d'inscriptions (3 personnes minimum).

MODALITES D'EVALUATION DES ACQUIS

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques (des labs de formation fournis par l'éditeur)
- Et, en fin de formation, par un questionnaire d'auto-évaluation

MODALITES D'ACCES

Cette formation est disponible en présentiel ou en classe à distance, avec un programme et une qualité pédagogique identiques.

SUPPORT DE FORMATION

Ce cours allie théorie, démonstrations, discussions interactives mais aussi exercices pratiques.

Le support de cours est disponible sur le portail de l'éditeur au format électronique (en anglais).

Les labs / exercices se basent sur des labs hébergés sur du matériel Palo Alto Networks chez MIEL et disponibles aussi à distance.

TARIF DE LA FORMATION

Prix public : 2 915€ HT / personne (inter-entreprises)

APPELEZ LE 01 60 19 16 27