DESCRIPTIF DE COURS

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

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

PRESENTATION DE LA FORMATION PAN-EDU-262

La première partie de cette formation donnée par un instructeur vous aidera à investiguer des attaques depuis la console Cortex XDR, gérer les incidents et analyser les artefacts de sécurité via différents modules comme la vue IP. Également, vous verrez comment exécuter des scripts Python sur vos endpoints.

La deuxième partie de la formation vous aidera à utiliser les datas présentes dans Cortex XDR pour vous protéger contre les attaques avancées. Vous aurez la possibilité de voir la vue de causalité de Cortex, voir l'API et récupérer les logs fournis par vos endpoints. Cette formation se concluera en parlant des requêtes XQL et deux autres utilisations de Cortex XDR Pro basées sur le XQL.

Ce cours combine théorie et ateliers pratiques.

DUREE DE LA FORMATION

2 jours, soit 14 heures

PUBLIC CONCERNE

Ce cours est recommandé pour les Analystes et Ingénieurs en cybersécurité et les personnes travaillant dans un SOC.

PRE-REQUIS

Il est vivement recommandé par l'éditeur pour les participants d'avoir suivi la formation PAN-EDU-260 (Cortex XDR: Prevention and Deployment).
Les participants doivent être familiarisés avec l'analyse d'événements de sécurité.

OBJECTIFS DE LA FORMATION

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

- 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

DESCRIPTIF DE COURS

CONTENU DE COURS

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

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).

FREQUENCE DE LA FORMATION

La formation PAN-EDU-262 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 : 2 145€ HT / personne (inter-entreprises)