DESCRIPTIF DE COURS

Palo Alto Networks Cortex XDR Pro : Cloud Service Operations

PAN-EDU-260

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-260

Palo Alto Networks® Cortex XDR™ Prevention Analysis and Response vous protège contre l'exploitation des vulnérabilités sophistiquées et les attaques utilisant des malwares inconnus.

Suite à ces 3 jours de formation, délivrés par un formateur certifié, les stagiaires seront aptes à configurer Cortex XDR Prevent et Cortex XDR Pro, à installer l'agent et à réagir le plus efficacement possible aux alertes remontées.

Ce cours combine théorie et ateliers pratiques.

DUREE DE LA FORMATION

3 jours, soit 21 heures

PUBLIC CONCERNE

Ce cours est recommandé pour les Ingénieurs Sécurité des Endpoints, Administrateurs systèmes, et Ingénieurs support technique.

PRE-REQUIS

Les stagiaires devront être familiers avec les concepts de sécurité en entreprise.

OBJECTIFS DE LA FORMATION

Les stagiaires vont apprendre comment Cortex protège contre l'exploitation de vulnérabilités et les attaques utilisant des Malwares.

Pendant les labs, les stagiaires vont :

- Explorer et configurer la plateforme Cloud Cortex XDR et installer les agents Cortex sur les périphériques
- Construire des policy rules et des profiles, activer et désactiver la protection des processus

DESCRIPTIF DE COURS

CONTENU DE COURS

Module 1 : Cortex XDR, une vue d'ensemble

- Comment les attaques sophistiquées fonctionnent-elles aujourd'hui ?
- Prévention des menaces multi-méthodes Cortex
- Composants et ressources Cortex

Module 2 : Utiliser les applications Cortex

- Cortex et Cortex Hub
- Etapes d'activation de Cortex via le Hub

Module 3 : Cortex XDR, déploiement et console

- Interface Web Cortex
- Communication des agents et création de groupes
- Politiques et profils

Module 4 : Flux de protection contre les logiciels malveillants

- Vue d'ensemble des modules de protection contre les programmes malveillants
- Restrictions Profiles, Malware Profiles et Scanning
- Protection comportementale contre les menaces

Module 5 : Flux de protection contre l'exploitation de vulnérabilité

- « Application Exploit Prevention »
- Techniques d'exploitation et mécanismes de défense
- Protection contre les menaces et profils de sécurité

Module 6 : Exceptions et réponses

- Evènements de sécurité
- Exceptions
- Actions et réponses
- Exécution de scripts

Module 7 : Etude comportementale

- Analyse de menaces comportementales
- Etude du lien de causalité Cortex
- Analytics et Machine learning

Module 8 : Règles XDR

- Règles BIOC (comportementales)
- Règles IOC et exceptions

Module 9 : Management d'incident

- Alertes et incidents
- Alertes externes
- Exclusion d'alertes et profil d'exclusion

Module 10 : Analyse d'alertes Cortex

- Analyse d'alertes avancée
- Vue de causalité
- Vue chronologique

Module 11 : Recherche et investigation

- Query builder et Query center
- Queries planifiées et non-planifiées

Module 12 : Troubleshooting

- Méthodologie et ressource
- Outils de troubleshooting Cortex
- Travailler avec le support technique

CERTIFICATION PREPAREE

Palo Alto Networks Micro-Credential for XDR Analyst (en cours de construction par l'éditeur)

Il s'agit de la seule Micro-Credential technique 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 ligne (durée de l'examen non connue pour le moment).

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 du Micro-Credential for XDR Analyst.

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.

DESCRIPTIF DE COURS

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 : 2 650€ HT / personne (inter-entreprises)