Palo Alto Networks Cortex XDR Pro : Cloud Service Operations
PAN-EDU-260

MIEL

Centre Agréé :
N°11 91 03 54 591

Pour contacter le service formation :
01 60 19 16 27

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

Formations sur Paris, Bievres (91) et en régions

PRESENTATION DE LA FORMATION

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.

DUREE DE LA FORMATION

3 jours

PUBLIC CONCERNE

Ingénieurs Sécurité des Endpoints, Administrateurs systèmes, et Ingénieurs support technique.

PRE-REQUIS

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

CONTENU DE COURS

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 ;

Niveau du cours : Intermédiaire

Format du cours : Ce cours allie théorie et pratique sur un environnement de lab.

Version logicielle : Palo Alto Networks Cortex XDR Pro per endpoint and Pro per TB

Voici le détail des points abordés pendant la formation :

Jour 1 - 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

Jour 1 - Module 2 : Utiliser les applications Cortex
- Cortex et Cortex Hub
- Etapes d'activation de Cortex via le Hub

Jour 1 - Module 3 : Cortex XDR, déploiement et console
- Interface Web Cortex
- Communication des agents et création de groupes
- Politiques et profils

Jour 1 - 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

Jour 2 - 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

Jour 2 - Module 6 : Exceptions et réponses
- Evènements de sécurité
- Exceptions
- Actions et réponses
- Exécution de scripts

Jour 2 - Module 7 : Etude comportementale
- Analyse de menaces comportementales
- Etude du lien de causalité Cortex
- Analytics et Machine learning

Jour 2 - Module 8 : Règles XDR
- Règles BIOC (comportementales)
- Règles IOC et exceptions

Jour 3 - Module 9 : Management d'incident
- Alertes et incidents
- Alertes externes
- Exclusion d'alertes et profil d'exclusion

Jour 3 - Module 10 : Analyse d'alertes Cortex
- Analyse d'alertes avancée
- Vue de causalité
- Vue chronologique

Jour 3 - Module 11 : Recherche et investigation
- Query builder et Query center
- Queries planifiées et non-planifiées

Jour 3 - Module 12 : Troubleshooting

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

CERTIFICATION PREPAREE

Cette formation prépare à la certification associée.