Cortex XDR 2 : Prévention, Analyse et Réponse (EDU-260)

Ce cours, dispensé par un formateur certifié, vous apprendra à :

- ✓ Différencier les différents composants de l'écosystème Cortex XDR ;
- ✓ Décrire Cortex, le Data Lake, le portail Support et le hub ;
- ✓ Activer Cortex XDR, déployer les agents et travailler avec la console de management ;
- ✓ Travailler avec la console de management de Cortex XDR, décrire ses différents menus et utiliser ses nombreux tableaux et filtres ;
- ✓ Créer des packages d'installation de l'agent Cortex XDR, des groupes de endpoints, des politiques de sécurité et les profils associés ;
- ✓ Créer, manager des profils de protection contre les malwares et exploits, et réaliser des actions de réponse ;
- ✓ Décrire les challenges de détection avec les menaces comportementales ;
- ✓ Différencier les règles Cortex XDR de type BIOC & IOC, les créer et les manager ;
- ✓ Décrire les concepts de la chaîne de causalité et analyses associées ;
- ✓ Trier les alertes et incidents, les hiérarchiser et créer des politiques d'exclusion ;
- ✓ Travailler avec les vues disponibles (Causalité, Chronologie) et investiguer à travers des recherches dans le Query Center.

Modules du cours

1. Introduction à l'écosystème Cortex XDR
2. Travailler avec les applications Cortex
3. Démarrer en sécurité du endpoint
4. Protection contre les malwares
5. Protection contre les exploits
6. Exceptions et actions de réponse
7. Analyse comportementale des menaces
8. Règles Cortex XDR
9. Management des incidents
10. Vues analytiques sur les alertes
11. Recherches et investigation
12. Troubleshooting basique

Périmètre

Niveau : Intermédiaire

Durée : 3 jours

Format : Cours et labs

Plateforme : Palo Alto Networks Cortex XDR PRO par endpoint et par To.

Objectifs

L'objectif de cette formation Palo Alto Networks Cortex XDR est d'améliorer sensiblement les connaissances des étudiants sur les points décrits ci-dessus.

Audience cible

Ingénieurs cybersécurité, analyse cybersécurité et spécialistes SOC.

Pré-requis

Les participants doivent être familiers avec les principaux concepts de la sécurité d'entreprise.

Programme éducatif Palo Alto Networks

Le programme éducatif développé par Palo Alto Networks et délivré par les centres de formation autorisés aident dans l'acquisition des connaissances et de l'expertise préparant à la bonne mise en place de la protection digitale des entreprises. Les certifications associées valident les connaissances des étudiants (portfolio du constructeur, capacités à prévenir les attaques et à activer de façon sécurisée les applications au sein de l'entreprise).