Palo Alto Networks Cortex™ XDR 3.6: Prevention and Deployment

Prix : 2 915 €HT

Durée : 3 jours

Code de Référence : PAN260

Catalogue Palo Alto Networks

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.

Objectifs de la formation

A l'issue de cette formation Palo Alto Networks, vous serez capable 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

Public

Cette formation Palo Alto s'adresse aux analystes en cybersécurité, administrateurs système et les personnes en charge du déploiement.

Prérequis

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

Vous souhaitez faire vérifier vos prérequis ? Contactez-nous pour l'organisation d'un entretien téléphonique avec un de nos consultants formateurs.

Programme de la formation

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

Méthodes pédagogiques

Cette formation Palo Alto est rythmée par une alternance d'exposés et de travaux pratiques. Les exercices réalisés lors des travaux pratiques permettent la mise en œuvre des connaissances acquises.

Méthodes d'évaluation 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

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.

Certification préparée

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.