Palo Alto Networks : Cortex XDR

Référence : **PAN-EDU-260** Durée : **3 jours** Certification : **Oui**

CONNAISSANCES PREALABLES

• Être familiers avec les concepts de sécurité en entreprise.

PROFIL DES STAGIAIRES

• Administrateurs systèmes. • Ingénieurs Sécurité des Endpoints. • Ingénieurs support technique.

OBJECTIFS

• Apprendre comment Cortex protège contre l'exploitation de vulnérabilités et les attaques utilisant des Malwares.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Palo Alto

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

JOUR 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

Utiliser les applications Cortex

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

Cortex XDR, déploiement et console

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

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

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

Exceptions et réponses

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

Etude comportementale

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

Règles XDR
- Règles BIOC (comportementales)
- Règles IOC et exceptions

JOUR 3

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

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

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

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