Palo Alto Networks Cortex XDR 3.6 : Investigation and Reponse

Référence : **PAN-EDU-262** Durée : **2 jours** Certification : **PCDRA**

CONNAISSANCES PREALABLES

• 1-Il est vivement recommandé par l'éditeur pour les participants d'avoir suivi la formation PAN-EDU-260 Palo Alto Networks Cortex XDR : Prevention and déployment ou de posséder les connaissances et compétences équivalentes. • 2-Êttre familiarisé avec l'analyse d'événements de sécurité. • 3-Avoir des connaissances de base en langue anglaise car le support de cours est en langue anglaise.

PROFIL DES STAGIAIRES

• Analystes et Ingénieurs en cybersécurité. • Personnes travaillant dans un SOC.

OBJECTIFS

• Enquêter et gérer les incidents. • Décrire la causalité Cortex XDR et les concepts analytiques. • Analyser les alertes à l'aide des vues Causalité et Chronologie. • Travailler avec les actions Cortex XDR Pro telles que l'exécution de scripts à distance. • Créer et gérer des requêtes de recherche à la demande et les planifier dans le Centre de requêtes. • Créer et gérer les règles Cortex XDR BIOC et IOC. • Travailler avec les actifs et les inventaires Cortex XDR. • Écrire des requêtes XQL pour rechercher des ensembles de données et visualiser les ensembles de résultats. • Travailler avec la collecte de données externes de Cortex XDR.

CERTIFICATION PREPAREE

Palo Alto Networks Certified Detection and Remediation Analyst. Il s'agit de la seule certification technique existant sur les produits Palo Alto Networks Cortex XDR

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique 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 des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Incidents Cortex XDR

Concepts de causalité et d'analyse

Analyse de causalité des alertes

Actions de réponses avancées

Créer des requêtes de recherche

Construire des règles XDR

Actifs Cortex XDR

Introduction à XQL

Collecte de données externes

Certification Palo Alto Networks Certified Detection and Remediation Analyst

- Cette formation prépare au passage de la certification Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA)

*Notre **référent handicap** se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.*