EduGroupe
Accompagner pour réussir

Palo Alto Networks Cortex 3.6 XDR Pro : Investigation and Reponse

Référence : **PAN-EDU-262** Durée : **2 jours (14 heures)** Certification : **Aucune**

Connaissances préalables

- 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 préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 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 et de réflexions

Formateur

- Consultant-Formateur expert Palo Alto

Méthodes d'évaluation 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

EduGroupe
Accompagner pour réussir

Contenu du cours

1. Incidents Cortex XDR

-

2. Concepts de causalité et d'analyse

-

3. Analyse de causalité des alertes

-

4. Actions de réponses avancées

-

5. Créer des requêtes de recherche

-

6. Construire des règles XDR

-

7. Actifs Cortex XDR

-

8. Introduction à XQL

-

9. Collecte de données externes

-

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.