Palo Alto Networks Cortex 3.2 XDR Pro : 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 ou 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

• Investiguer les attaques via la page incidents, gérer le risque, assigner les incidents et clôturer ces derniers. • Analyser les artefacts en utilisant des modes de vue avancés comme la vue IP ou la vue de Hash. • Utiliser les fonctionnalités Cortex XDR Pro : Exécution de script python et gestion des EDL. • Décrire Cortex XDR Analytics. • Analyser les alertes en utilisant les vues de causalité et de chronologie. • Créer et gérer les requêtes XQL dans le centre de requêtes. • Créer et gérer les règles Cortex XDR BIOC et IOC. • Travailler avec l'ingestion de logs ou d'alertes externes. • Faire des requêtes XQL. • Créer des règles de corrélation grâce aux requêtes XQL.

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 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 des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Incidents Cortex XDR

Les différentes vues d'investigation

Actions de réponse à incident

Vue de causalité et moteur d'Analytics

Analyse des alertes de causalité

Construire des requêtes XQL

Construire des règles BIOC et IOC

Récupération de data externe

Introduction au XQL

Règles de Corrélation et de Parsing

*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*