EduGroupe
Accompagner pour réussir

Cortex XSIAM : Opérations de sécurité et automatisation

Référence : **PAN-EDU-270** Durée : **4 jours** Certification : **XSIAM Analyst**

CONNAISSANCES PREALABLES

• Les participants doivent être familiarisés avec le déploiement de produits d'entreprise, les réseaux et les concepts de sécurité.

PROFIL DES STAGIAIRES

• 1-Ingénieurs et responsables SOC/CERT/CSIRT/XSIAM, MSSP. • 2-Partenaires fournisseurs de services/intégrateurs de systèmes. • 3-Consultants en services professionnels internes et externes. • 4-Ingénieurs commerciaux, intervenants en cas d'incident et chasseurs de menaces.

OBJECTIFS

• A la fin de cette formation Cortex XSIAM, vous serez capable de :. • Déployer, configurer et installer les agents XDR et configurer les groupes d'agents et les profils. • Enquêter sur les incidents, examiner les actifs et les artefacts, et comprendre la chaîne de causalité. • Créer des règles de corrélation, utiliser XQL pour interroger les journaux et analyser les incidents à l'aide des outils et des ressources disponibles.

CERTIFICATION PREPAREE

Certification Palo Alto Networks XSIAM Analyst. Il s'agit de la certification technique de 3ème niveau (Specialist) sur les produits Palo Alto Networks - Security Operations, qui regroupe 4 niveaux de certifications. Le passage de l'examen (en anglais) s'effectue ultérieurement en centre agréé Pearson Vue et dure en moyenne 1h30. Elle est valable 2 ans.

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

Introduction à Cortex XSIAM
Éléments des opérations de sécurité
Modèle de maturité
Déploiement et configuration des agents
Ingestion des sources de données
Visibilité
Modèle de données
Analyse
Alerte et détection
Gestion de la surface d'attaque
Automatisation
Traitement des incidents / SOC

Certification Palo Alto Networks XSIAM Analyst

- Cette formation prépare au passage de la certification Palo Alto Networks XSIAM Analyst
- Le prix de cette formation ne comprend pas le voucher pour le passage de l'examen (en anglais) qui s'effectue ultérieurement en centre agréé Pearson Vue et dure en moyenne 1h30

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.