

Cortex XSIAM Investigation and Analysis

Référence : **PAN-EDU-272**

Durée : **2 jours (14 heures)**

Certification : **XSIAM Analyst**

Connaissances préalables

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

Profil des stagiaires

- Ingénieurs et responsables SOC/CERT/CSIRT/XSIAM
- MSSP et partenaires de services/intégrateurs de systèmes
- Consultants internes et externes en services professionnels
- Ingénieurs commerciaux
- Intervenants en cas d'incident et chasseurs de menaces

Objectifs

- Enquêter sur les incidents, analyser les actifs et les artefacts clés, et interpréter la chaîne de causalité
- Interroger et analyser les journaux en utilisant XQL pour extraire des informations significatives
- Utiliser des outils et des ressources avancés pour une analyse complète des incidents

Certification préparée

- Cette formation prépare à la Certification Palo Alto Networks XSIAM Analyst. Il s'agit de la certification technique de 3ème niveau (Specialist) sur les produits Palo Alto Networks - Network Security, qui regroupe 4 niveaux de certifications. L'examen dure en moyenne 1h30 et sa validité est de 2 ans. Pour plus de détails [cliquer ici](#).

Méthodes pédagogiques

- 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 et de réflexions
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

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

Contenu du cours

Introduction à Cortex XSIAM

Endpoints

XQL

Alertes et détection

Threat Intel Management

Automatisation

Attack Surface Management

Gestion d'incidents

Tableaux de bord et rapports

Certification Palo Alto Networks XSIAM Analyst

- Aucune certification technique préalable n'est nécessaire pour passer cette certification
- Le prix de cette formation ne comprend pas le voucher pour le passage de l'examen (en anglais) qui s'effectue ultérieurement auprès de Pearson Vue

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:01.71.19.70.30) ou par mail à <mailto:referent.handicap@edugroupe.com> pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.