

Cortex XDR The full picture : How to administrate and investigate

Référence : **PAN-EDU-26X**

Durée : **4 jours (28 heures)**

Certification : **Aucune**

Connaissances préalables

- Les participants doivent avoir une compréhension fondamentale des principes de cybersécurité et une expérience dans l'analyse des incidents et l'utilisation d'outils de sécurité pour les enquêtes
- Ils doivent être familiarisés avec les déploiements d'entreprise, le réseau et les bases de la sécurité

Profil des stagiaires

- Ce cours s'adresse à un large éventail de professionnels de la sécurité, notamment les analystes SOC, CERT, CSIRT et XDR, les responsables, les intervenants en cas d'incident et les chasseurs de menaces
- Il convient également aux consultants en services professionnels, aux ingénieurs commerciaux et aux partenaires de prestation de services

Objectifs

- Décrire le rôle des composants Cortex XDR, notamment les agents de terminaux, les collecteurs XDR, les pare-feu nouvelle génération (NGFW) et les machines virtuelles Broker, dans la sécurisation des réseaux et des appareils
- Utiliser XQL pour interroger et analyser les journaux afin de permettre une ingestion efficace des données et la détection des menaces
- Concevoir et mettre en œuvre des workflows pour rationaliser les opérations de sécurité
- Appliquer des listes dynamiques externes et des règles d'indicateurs pour faire respecter les politiques de sécurité
- Enquêter sur les cas, analyser les actifs et artefacts clés, et interpréter la chaîne de causalité
- Interroger et analyser les journaux à l'aide de XQL afin d'en extraire des informations pertinentes
- Utiliser des outils et ressources avancés pour une analyse complète des cas

Certification préparée

- Aucune

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

Présentation du cours

Présentation de Cortex XDR

Composants logiciels

Intégrations

XQL

Ingénierie de détection

Automatisation de la plateforme

Optimisation du système

Tableaux de bord et rapports

Sécurité des e-mails

Terminaux

Alertes et détection

Vulnérabilité et analyse forensique

Automatisation de la plateforme

Gestion des cases

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.