Palo Alto Networks - Cortex™ XDR 3.6 : Investigation and Response (EDU-262)

Cours officiel, préparation aux examens Palo Alto Networks

Cours Pratique de 2 jours - 14h
Réf : PA5 - Prix 2025 : 1 820 HT

Avec la formation, vous apprendrez à enquêter sur les attaques via les pages d'incidents de Cortex XDR. Vous verrez les chaînes de causalité, les alertes, les logs, le log stitching et les vues Causalité et Chronologie. Vous utiliserez des actions de réponse avancées (remédiation, EDL, scripts à distance), créerez des requêtes de recherche simples, des règles XDR et explorerez des vues spécialisées (IP, Hash). Une introduction au langage XQL et aux intégrations via l'API Cortex XDR est également incluse.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Enquêter sur les incidents et les gérer

Décrire les concepts de causalité et d'analyse de Cortex XDR

Analyser les alertes avec les vues Causalité et Chronologie

Utiliser les actions Pro de Cortex XDR comme l'exécution de scripts à distance

Créer et gérer des requêtes de recherche à la demande ou planifiées dans le Centre de requêtes

Créer et gérer les règles Cortex XDR de type BIOC et IOC

Travailler avec les actifs et inventaires de Cortex XDR

Rédiger des requêtes XQL pour interroger les ensembles de données et visualiser les résultats

Utiliser la collecte de données externes de Cortex XDR

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel au format numérique et en anglais. Bonne compréhension de l'anglais à l'écrit.

CERTIFICATION

Cette formation est recommandée dans le cadre du parcours de préparation aux certifications suivantes : Security Operations Professional, XDR Engineer.

LES DATES

CLASSE À DISTANCE	PARIS
2025 : 24 nov.	2025 : 17 nov.

PARTICIPANTS

Analystes et ingénieurs en cybersécurité, spécialistes des opérations de sécurité.

PRÉREQUIS

Avoir suivi le cours EDU-260 (Cortex XDR: Prevention and Deployment).

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.