Formation Palo Alto Cortex XDR: Investigation and Response

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

La première partie de cette formation donnée par un instructeur vous aidera à investiguer des attaques depuis la console Cortex XDR, gérer les incidents et analyser les artefacts de sécurité via différents modules comme la vue IP. Également, vous verrez comment exécuter des scripts Python sur vos endpoints.
La deuxième partie de la formation vous aidera à utiliser les datas présentes dans Cortex XDR pour vous protéger contre les attaques avancées. Vous aurez la possibilité de voir la vue de causalité de Cortex, voir l'API et récupérer les logs fournis par vos endpoints. Cette formation se concluera en parlant des requêtes XQL et deux autres utilisations de Cortex XDR Pro basées sur le XQL.

Référence	PAN-EDU-262
Durée	2 jours (14h)
Tarif	2 145 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 18 au 19 septembre 2025
du 4 au 5 décembre 2025

VOIR TOUTES LES DATES

Objectifs

| Enquêter et gérer les incidents
| Décrire la causalité Cortex XDR et les concepts analytiques
| Analyser les alertes à l'aide des vues Causalité et Chronologie
| Exécuter des scripts à distance
| Planifier des requêtes dans le Centre de requêtes
| Créer et gérer les règles Cortex XDR BIOC et IOC
| Travailler avec les actifs et les inventaires Cortex XDR
| Rechercher des ensembles de données
| Collecter des données externes

Public

| Analystes et Ingénieurs en cybersécurité
| Personnes travaillant dans un SOC

Prérequis

| Il est vivement recommandé d'avoir suivi la formation PAN-EDU-260
| Être familiarisé avec l'analyse d'événements de sécurité

Programme de la formation

Incidents Cortex XDR
Concepts de causalité et d'analyse
Analyse de causalité des alertes
Actions de réponse avancées
Créer des requêtes de recherche
Construire des règles XDR
Introduction à XQL
Collecte de données externes

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.