Palo Alto Networks: Cortex XSOAR 6.2: Automation and Orchestration

Durée: 4 Jours **Réf de cours: PAN-EDU-380**

Résumé:

La formation Cortex™ XSOAR 6.8 : Automatisation et orchestration (EDU-380) est une formation de quatre jours dispensée par un instructeur qui vous aidera à :Configurer les intégrations, créer des tâches et développer des playbooks.Construire des schémas d'incidents qui permettent aux analystes de trier et d'enquêter efficacement sur les incidentsIdentifier comment catégoriser les informations sur les événements et mapper ces informations sur des champs d'affichageDévelopper des automatismes, gérer le contenu, les données d'indicateurs et les magasins d'artefacts, planifier des tâches, organiser les utilisateurs et leurs rôles, superviser la gestion des cas et favoriser la collaboration.

Mise à jour : 13.02.2024

Public visé:

Security-operations (SecOps), ou ingénieurs en sécurité, orchestration, automatisation et réponse , fournisseurs de services de sécurité gérés, partenaires de prestation de services, intégrateurs de systèmes et ingénieurs de services professionnels.

Objectifs pédagogiques:

- Cette formation est conçue pour permettre à un ingénieur SOC, CERT, CSIRT ou SOAR de commencer à travailler avec les intégrations de Cortex XSOAR, les playbooks, les mises en page d'incidents et d'autres fonctionnalités du système pour faciliter l'orchestration des ressources, l'automatisation des processus, la gestion des cas et le flux de travail des analystes.
- Le troisième module du cours présente un processus complet de développement de playbooks pour l'automatisation d'un flux de travail typique d'un analyste pour traiter les incidents de phishing. Cette vue de bout en bout du processus de développement fournit un cadre pour des discussions plus ciblées sur des sujets individuels qui sont couverts dans les modules suivants.

Pré-requis:

Les participants doivent suivre la formation en ligne Cortex XSOAR Analyst.

Une expérience de l'écriture de scripts, de l'utilisation de Python,de JavaScript, et de l'utilisation d'objets de données JSON est un plus.

Cependant, il n'est pas nécessaire de savoir écrire du code pour suivre cette fomration

Contenu:

1- Fonctionnalités de base et ensembles de fonctionnalités

2 - Activation et configuration des intégrations

3 - Développement d'un playbook

4 - Classification et cartographie

5 - Création de la mise en page

6 - Architecture de la solution

7 - Docker

8 - Développement de l'automatisation et débogage

9 - Gestion de contenu

10 - Indicateurs

11 - Jobs et planification des tâches

12 - Gestion des utilisateurs et des rôles

13 - Développement de l'intégration

Méthodes pédagogiques :

Le programme technique développé et autorisé par Palo Alto Networks et dispensé par les partenaires de formation agréés de Palo Alto Networks contribue à fournir les connaissances et l'expertise qui vous préparent à protéger notre mode de vie numérique. Nos certifications reconnues valident votre connaissance du portefeuille de produits Palo Alto Networks et votre capacité à prévenir les cyberattaques réussies, à activer les applications en toute sécurité et à automatiser les réponses efficaces aux événements de sécurité.
Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement