Formation Cortex XSOAR 6.2 : automatisation et orchestration

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

Cette formation est conçue pour permettre à un ingénieur SOC, CERT, CSIRT ou SOAR de commencer à travailler avec les intégrations Cortex XSOAR, les playbooks, les mises en page des incidents et d'autres fonctionnalités 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 playbook pour automatiser un flux de travail d'analyste typique 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.

Référence	EDU-380
Durée	4 jours (28h)
Tarif	3 400 €HT
Repas	repas inclus

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Objectifs

| Configurer des intégrations, créer des tâches et développer des playbooks.
| Créer des présentations d'incidents qui permettent aux analystes de trier et d'enquêter efficacement sur les incidents
| Identifier comment catégoriser les informations d'événements et mapper ces informations
| Développer des automatisations, gérer le contenu, les données d'indicateurs et les magasins d'artefacts
| Planifier les tâches, organiser les utilisateurs et leurs rôles
| Superviser la gestion des cas

Public

| Ingénireurs SOC, CERT, CSIRT ou SOAR

Prérequis

| Connaitre Cortex XSOAR Analyst
| Il est recommandé d'avoir une expérience en écriture de scripts, dans l'utilisation de Python et JavaScript, et l'utilisation d'objets de données JSON

Programme de la formation

Core functionality and Feature Sets.
Enabling and Configuring Integrations.
Playbook Development.
Classification and Mapping.
Layout Builder.
Solution Architecture.
Docker.
Automation Development & Debugging.
Content Management.
Indicators.
Jobs and Job Scheduling.
Users and Role Management.
Integration Development

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.

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.