+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 04/12/2024

S'inscrire

# Formation Cortex XSOAR

3 jours (21 heures)

## Présentation

Cortex Xsoar est une plateforme SOAR (Security Orchestration, Automation and Response) développée par Palo Alto Networks, qui vise à centraliser la gestion des incidents de sécurité, automatiser les tâches répétitives et, orchestrer les outils de sécurité. Elle aide les équipes de sécurité à automatiser les tâches répétitives, orchestrer les workflows de réponse aux incidents et améliorer leur efficacité globale dans la gestion des menaces.

Ce cours met l'accent sur l'optimisation des opérations de sécurité en utilisant les fonctionnalités de XSOAR pour automatiser les processus répétitifs et améliorer la gestion des incidents.

Vous apprendrez à comprendre les bases des SOAR et de XSOAR , ainsi qu'à explorer ses composants clés comme les types d'incidents, les intégrations et les instances. Vous apprendrez à développer des automatisations et des playbooks pour répondre efficacement aux incidents et à concevoir des workflows automatisés pour améliorer la productivité.

À la fin de la formation, vous serez capable de créer des workflows automatisés sophistiqués et des intégrations au sein de XSOAR, améliorant ainsi considérablement la réponse de votre organisation aux incidents de sécurité et renforçant la gestion globale de la sécurité.

Notre formation se basera sur la dernière version de la technologie on-prem ou on-premises

## Objectifs

- Automatiser efficacement la gestion des incidents de sécurité
- Maîtriser le développement personnalisé avec Cortex XSOAR
- Optimiser les workflows de sécurité grâce à l'automatisation avancée

## Public visé

- Ingénieurs en automatisation de la sécurité
- Ingénieur en sécurité
- Intégrateur de systèmes

## Pré-requis

- Connaissances de base en Linux
- Familiarité avec APIs et Webhooks
- Savoir rédiger et comprendre des scripts Python

## PROGRAMME DE NOTRE FORMATION CORTEX XSOAR

### INTRODUCTION & APERÇU D'XSOAR

- Qu'est-ce Cortex XSOAR ?
- Différences entre les différentes versions (on-prem, cloud)
- Pourquoi l'utiliser ?
- Fonctionnalités de base
- Présentation de l'architecture
- Exploration de l'interface utilisateur et configuration

### CONCEPTS CLÉS DE CORTEX XSOAR

- Gestion et classification des incidents de sécurité XSOAR
- Configuration des intégrations et gestions des instances
- Utilisation des listes pour stocker et gérer des informations
- Intégration de sources de renseignements sur les incidents
- Création de playbooks automatisés et ajout de contexte pertinents

### DÉVELOPPEMENT DE PLAYBOOK

- Mise en place de la gestion des erreurs dans le playbooks et utilisation de métadonnées
- Application de filtres pour transformer, manipuler et affiner les données
- Créations de sous-playbooks
- Compréhension de différents types de tâches sur XSOAR
- Utilisation des boucles dans les playbooks

### DÉVELOPPEMENT DE SCRIPT D'AUTOMATISATION

- Configuration et utilisation de l'IDE (environnement de développement intégré) pour coder et tester les scripts
- Utilisation de la classe Demisto et des fonctions du serveur commun
- Utilisation des images Docker pour faciliter le déploiement et l'exécution des scripts
- Création et déploiement de scripts d'automatisation dans XSOAR

- Exploitation de l'API XSOAR pour intégrer des applications externes

### DÉVELOPPEMENT D'INTEGRATION

- Analyse des différentes catégories d'intégrations dans XSOAR et exploration des cas d'utilisation
- Étude des commandes, méthodes et fonctions disponibles
- Introduction au processus de développement d'intégrations dans XSOAR
- Approfondissement des techniques de développement d'intégrations

### PRÉ-TRAITEMENT ET POST-TRAITEMENT

- Création et gestion des règles de prétraitement dans XSOAR
- Développement de scripts de prétraitement
- Utilisation de scripts de post-traitement pour affiner, analyser ou transformer les données après leur traitement principal

### CRÉATION ET AUTOMATISATION DES WORKFLOWS

- Présentation des outils et méthodes pour automatiser les cas d’usage
- Compréhension du lien entre cas d’usage et workflows automatisés
- Analyse des bénéfices de l’automatisation dans les processus métier
- Étapes pour transformer un cas d’usage en workflow automatisé
- Étude pratique : Mise en œuvre d’un workflow automatisé à partir d’un exemple concret

### BONUS

- Ressources supplémentaires : Liens vers des guides, livres blancs et tutoriels pertinents
- Suggestions pour aller plus loin (ex. certifications, modules experts)

## Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

## Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

## Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

## Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

## Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

## Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.