+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 Swimlane Turbine SOAR

3 jours (21 heures)

Présentation

Swimline Turbine est une solution avancée d'orchestration, d'automatisation et de réponse aux incidents (SOAR), offrant une gestion efficace des processus de sécurité en intégrant des outils de cybersécurité et en automatisant les workflows pour réduire le temps de réponse aux menaces.

Notre formation Swimlane Turbine SOAR est conçue pour vous rendre pleinement opérationnel sur la plateforme Swimlane et pour vous permettre de prouver vos compétences.

Cette formation vous préparera à gérer, automatiser et orchestrer efficacement les processus de sécurité en utilisant Swimlane Turbine, vous permettant ainsi de répondre plus rapidement et efficacement aux incidents de sécurité dans votre organisation.

Cette formation se déroulera sur la version 10.19 de Swimlane

Objectifs

- **Comprendre l'architecture et les concepts SOAR**
- Développez les compétences nécessaires pour atténuer les menaces et répondre aux incidents de manière plus efficace
- Améliorer les processus de gestion des incidents

Public visé

Cette formation s'adresse principalement aux professionnels de la sécurité informatique, tels que :

- Ingénieurs SOC (Security Operations Center) et SOAR

- Analystes de sécurité
- Administrateurs de sécurité
- Responsables de la gestion des incidents
- Consultants en cybersécurité
- Professionnels en gestion des risques

Pré-requis

- Connaissance de base en cybersécurité, scripting et automatisation
- Connaissance des outils de sécurité
- Compréhension des API et des Webhooks (recommandé)

Note : Ambient-IT n'est pas propriétaire de Swimlane turbine©, Swimlane Turbine© est une marque déposée de Swimlane©

PROGRAMME DE NOTRE FORMATION SWIMLANE TURBINE

INTRODUCTION & CONFIGURATION À SWIMLANE

- Introduction à Swimlane Turbine
- Présentation des cas d'utilisation de SOAR et de son rôle dans l'automatisation des processus de sécurité
- Gestion des licences et configuration
- Installation de l'Appliance
- Configuration de base via la console Web et l'interface en ligne de commande (CLI)
- Mise à jour de l'Appliance

CONFIGURATION DES COMPOSANTS ET PLAYBOOKS

- Configuration des profils utilisateurs
- Déploiement d'une solution SOAR : préparation et prérequis
- Définition du scope du projet et planification du déploiement
- Configuration des environnements SOAR
  - Intégration des applications et sources de données
  - Création des stratégies d'enrichissement et des politiques de traitement des logs
- Développement de playbooks pour l'automatisation des processus de réponse aux incidents

AUTOMATISATION ET ORCHESTRATION DES INCIDENTS

- Mise en place de workflows automatisés pour les incidents courants
- Orchestration des outils de sécurité
- Création et gestion des tâches dans les playbooks
- Automatisation des réponses aux incidents : identification et gestion des menaces
- Cas pratiques : développement de playbooks pour des incidents types (phishing, malwares)

GESTION ET AVANCÉE ET OPTIMISATION

- Architecture avancée
- Optimisation des workflows et des playbooks
- Gestion des utilisateurs et des rôles
- Mise en œuvre de l'intelligence de menace (Threat Intelligence) dans les playbooks
- Support, dépannage et résolution des problèmes courants
- Sécurisation et sauvegarde des données

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.