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

Mis à jour le 10/01/2025

S'inscrire

Formation IBM QRadar SOAR

3 jours (21 heures)

Présentation

Notre formation IBM QRadar SOAR vous enseignera la maîtrise nécessaire pour automatiser votre sécurité grâce à l'intégration de workflows. Notre programme couvre l'ensemble des fonctionnalités de l'outil afin que vous puissiez efficacement analyser et traiter les cyberattaques.

Dans ce cours, vous apprendrez tout d'abord à comprendre la SOAR en profondeur et la place qu'occupe IBM QRadar SOAR au sein de votre environnement informatique. À travers une démonstration pratique, vous apprendrez à manipuler l'interface et à configurer vos alertes.

Vous découvrirez les bonnes pratiques d'usage, la gestion des rôles, des incidents, et des flux de travail. L'automatisation et l'orchestration de la réponse aux menaces avec IBM QRadar SOAR.

Comme pour toutes nos formations, nous vous présenterons la dernière version du logiciel : IBM QRadar SOAR V51.0.0

Objectifs

- Comprendre l'importance d'un SOAR dans la cybersécurité et ses différentes fonctions
- Savoir installer et configurer QRadar
- Maîtriser l'intégration des systèmes tiers
- Utiliser les fonctionnalités avancées de QRadar
- L'intégration des données structurée en JSON

Public visé

- **Analystes Cybersécurité**
- Analystes SOC
- Gestionnaires SOC

- Ingénieur en sécurité
- DevSecOps
- Administrateur Réseau

Pré-requis

Connaissances de base des réseaux et des systèmes.

Pré-requis matériel

Un accès à IBM QRadar SOAR.

Programme de notre formation IBM QRadar SOAR

INTRODUCTION AU SOAR

- Comprendre l'importance d'un SOAR
- Le rôle du SOAR dans la cybersécurité
- SIEM vs SOAR
- Directives et architecture d'un SOAR
- Configuration initiale de QRadar SOAR
- Connexion avec QRadar SIEM et d’autres outils

PRÉSENTATION DE QRADAR

- Les composants
- Les flux de données
- Prise en main de l'interface
- Les concepts fondamentaux de QRadar
- Les fonctionnalités principales de l'outil

GESTION ET ADMINISTRATION

- Installer QRadar
- Configuration
- Procédures de migration
- Mise à niveau
- Comprendre le cycle de vie des incidents
- Stratégies de gestion des sauvegardes et de restauration des données
- Sécurité et gestion des accès utilisateurs
- Gestion des cas et priorisation des réponses
- Troubleshooting

Automatisation et Orchestration

- Introduction aux concepts de playbooks
- Étudier la structure JSON des playbooks
- Création de workflows automatisés
- Workflows contre le phishing
- Workflows contre les ransomware
- Automatisation des tâches SOC
- Intégration avec les outils d’analyse des menaces

SURVEILLANCE AVEC QRADAR

- Surveillance et interprétation des notifications de QRadar
- Comment utiliser les tableaux de bord
- Enquêter sur les anomalies détectées
- Configuration des notifications
- Les bonnes pratiques de surveillance
- Stratégies pour le suivi des changements d'actifs
- Détection des risques associés
- Pratiques recommandées pour la maintenance des informations relatives aux actifs

Perfectionnement de QRadar SOAR

- Intégration des systèmes tiers
  - Antivirus
  - Pare-feu
  - Plateformes cloud
- Utilisation des APIs pour personnaliser les flux de travail
- Analyse des métriques SOC pour identifier les goulots d’étranglement
- Exploiter les APIs QRadar pour intégrer des données structurées en JSON

CONSOLE D'ADMINISTRATION

- Utiliser la console d'administration
- Défense contre les attaques multi-vecteur
- Compromission interne
- Bonnes pratiques pour la gestion des configurations et des paramètres de sécurité

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.