IBM - QRadar SOAR - Foundations

Optimisez la gestion de vos incidents de sécurité avec QRadar SOAR

Présentiel ou en classe à distance

1 jour (7 h) Réf.: IBMBQ405

QRadar SOAR (Security Orchestration, Automation, and Response) est une plateforme développée par IBM pour automatiser et orchestrer les processus de sécurité. Elle permet aux équipes de sécurité de gérer et de répondre plus rapidement aux incidents en intégrant des outils de sécurité et des flux de travail automatisés. La solution est conçue pour simplifier la gestion des incidents et améliorer la réactivité des équipes en intégrant des modules comme le Breach Response, qui aide à coordonner les réponses aux violations de sécurité. De plus, QRadar SOAR offre une interface intuitive, permettant de gérer les incidents, les utilisateurs et d'intégrer des systèmes tiers, ce qui en fait un choix stratégique pour renforcer la posture de sécurité d'une organisation.
Se former à QRadar SOAR permet aux professionnels de la sécurité d'acquérir les compétences nécessaires pour déployer et configurer cette solution au sein de leur infrastructure de sécurité. Une maîtrise de l'architecture et des fonctionnalités de QRadar SOAR, telles que la gestion des cas, la conception de playbooks, et l'intégration avec des solutions tierces, est essentielle pour améliorer l'efficacité des processus de réponse aux incidents. La formation vous permet de comprendre et d'exploiter pleinement le potentiel de cette plateforme pour réduire les délais de réponse et automatiser des tâches répétitives. Pour les administrateurs SOC, les analystes de sécurité et les intervenants sur incidents, cette formation est un atout précieux pour optimiser la gestion des incidents et renforcer la résilience face aux cybermenaces.

A qui s'adresse cette formation ?

Pour qui

- Administrateurs SOC
- Analystes SOC
- Analystes de sécurité

Prérequis

- Aucun.

Programme

1 - Introduction à QRadar SOAR

- Présentation des patterns architecturaux de QRadar SOAR, une solution clé pour l'orchestration de la sécurité et l'automatisation des réponses aux incidents.
- Installation du produit, configuration de la licence et de l'accès, étapes essentielles pour une mise en place réussie de QRadar SOAR dans votre architecture de sécurité.
- Exploration de la console SOAR pour gérer efficacement les incidents et surveiller les activités de sécurité.

2 - Gestion des incidents et intégration des emails

- Utilisation des capacités de gestion des incidents avec le module Breach Response de QRadar, permettant une réponse rapide aux violations de sécurité.
- Intégration du système de messagerie pour la gestion des utilisateurs et des cas, optimisant ainsi la réactivité et la collaboration au sein des équipes de sécurité.

3 - Création de playbooks et intégrations tierces

- Conception de playbooks SOAR, une étape cruciale pour automatiser les processus de réponse aux incidents et réduire le temps de réaction face aux cybermenaces.
- Intégration de solutions tierces avec QRadar SOAR, permettant une gestion centralisée des incidents de sécurité avec des outils IBM et non-IBM.

Les objectifs de la formation

- Expliquer les patterns architecturaux de QRadar SOAR pour son intégration réussie dans une architecture de sécurité.
- Installer et configurer QRadar SOAR, y compris la gestion de la licence et des accès.
- Gérer des cas de sécurité et utiliser le module Breach Response pour répondre efficacement aux incidents.
- Créer des playbooks SOAR pour automatiser et orchestrer les processus de sécurité, réduisant ainsi le temps de réponse aux menaces.
- Intégrer solutions tierces avec QRadar SOAR pour une gestion complète des incidents.

Evaluation

- Cette formation ne fait pas l'objet d'une évaluation des acquis.

Les points forts de la formation

- Une formation complète basée sur l'alternance d'exposés et d'exercices pratiques qui favorise une mise en pratique immédiate des acquis à l'issue de la formation.
- Spécialistes de la technologie, les intervenants apportent leurs conseils et leur expérience.
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).