IBM QRadar SIEM - Notions avancées

Identifier rapidement les menaces les plus "discrètes"

Présentiel ou en classe à distance

2 jours (14 h) Réf.: IBMBQ205

Formation officielle

IBM QRadar SIEM offre une visibilité approfondie sur les activités réseau, utilisateur et application. Il permet de collecter, normaliser, corréler et stocker de manière sécurisée les événements, les flux, les actifs et les vulnérabilités. Les attaques suspectes et les violations de politiques sont mises en évidence sous forme d'incidents.
Cette formation vous guide à travers des sujets avancés sur QRadar tels que les sources de journaux personnalisées, les collections de données de référence et les règles personnalisées, l'intégration des données X-Force et l'application Threat Intelligence, l'analyse comportementale des utilisateurs (UBA) et QRadar Advisor, ainsi que l'ajustement des règles et les scripts d'actions personnalisées. Le cours aborde également l'intégration avec IBM SOAR. Des exercices pratiques permettront de renforcer les compétences acquises.

A qui s'adresse cette formation ?

Pour qui

- Administrateurs de sécurité
- Analystes de sécurité

Prérequis

- Connaissances de l'infrastructure informatique, des principes fondamentaux de la sécurité informatique, de Linux, de Windows, de la mise en réseau TCP/IP, et de syslog
- Vous devez également avoir suivi la formation "IBM QRadar SIEM - Les bases"

Programme

1 - Sources de journaux personnalisées

- Configurer et créer des sources de journaux personnalisées pour mieux capturer les données spécifiques aux systèmes ou applications.

2 - Collecte de données de référence et règles personnalisées

- Utiliser les données de référence pour enrichir vos analyses et définissez des règles personnalisées pour améliorer la détection et la réponse.

3 - IBM X-Force Threat Intelligence dans QRadar

- Découvrir comment intégrer les données X-Force pour renforcer la détection des menaces en temps réel avec des informations de renseignement sur les menaces.

4 - Analyse du comportement des utilisateurs et Advisor avec Watson

- Explorer l'analyse comportementale des utilisateurs (UBA) et comment QRadar Advisor, assisté par Watson, peut aider à identifier des comportements suspects et des anomalies.

5 - Réglages

- Ajuster les configurations de QRadar pour éviter les faux positifs, affiner les alertes et améliorer l'efficacité du système.

6 - Scripts d'action personnalisés

- Créer des scripts d'actions personnalisées pour automatiser la réponse aux incidents et optimiser les flux de travail de sécurité.

7 - Intégration IBM SOAR

- Intégrer QRadar avec IBM SOAR (Security Orchestration, Automation, and Response) pour automatiser les réponses aux incidents et orchestrer des actions sur les événements de sécurité.

Les objectifs de la formation

- Créer des sources de journaux personnalisées adaptées aux besoins spécifiques de votre environnement.
- Travailler avec les collections de données de référence et les règles personnalisées pour améliorer la collecte et l'analyse des données.
- Utiliser les données X-Force et l'application Threat Intelligence pour améliorer la détection des menaces.
- Explorer les fonctionnalités de l'analyse comportementale des utilisateurs (UBA) et QRadar Advisor avec Watson.
- Effectuer des ajustements (tuning) dans QRadar pour affiner les alertes et les analyses.
- Créer des scripts d'actions personnalisées pour automatiser les processus et répondre aux incidents de manière plus efficace.
- Discuter de l'intégration de QRadar avec IBM SOAR pour automatiser et orchestrer les réponses aux incidents.

Evaluation

- Cette formation fait l'objet d'une évaluation formative.

Les points forts de la formation

- L'apprentissage par la pratique : de nombreuses mises en situation permettent aux participants de tester en salle les pratiques et méthodes enseignées
- Le partage de bonnes pratiques pour exploiter le plus efficacement possible toute la puissance de la solution
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).