IBM QRadar SIEM - Les bases

Analyser les évènements du SI pour identifier les menaces

Présentiel ou en classe à distance

3 jours (21 h) Réf.: IBMBQ105

Formation officielle

IBM Security QRadar est une solution puissante de gestion des informations et des événements de sécurité (SIEM) qui offre une visibilité approfondie sur les activités des réseaux, des points de terminaison, des utilisateurs et des applications. Elle permet de collecter, normaliser, corréler et stocker de manière sécurisée les événements, flux, actifs et vulnérabilités. Les attaques suspectes et les violations de politiques sont mises en évidence sous forme d'incidents.
Dans cette formation, vous apprendrez l'architecture de la solution, comment naviguer dans l'interface utilisateur et comment enquêter sur les incidents. Vous explorerez les données à partir desquelles QRadar conclut une activité suspecte. Des exercices pratiques renforceront les compétences acquises.

A qui s'adresse cette formation ?

Pour qui

- Analystes Sécurité
- Architectes techniques de Sécurité
- Responsables des incidents
- Administrateurs réseau
- Administrateurs systèmes

Prérequis

- Posséder des connaissances dans les domaines suivants : infrastructure informatique, fondamentaux de la sécurité informatique, Linux, Windows, les réseaux TCP/IP et Syslog

Programme

1 - IBM Security QRadar 7.5 – Fondamentaux

- Introduction à QRadar, son architecture et ses composants clés.

2 - Architecture de QRadar

- Explication détaillée de l'architecture de QRadar et des flux de données.
  Atelier

  Exercices d'architecture pour comprendre les flux de données de QRadar

3 - Interface utilisateur de QRadar – Aperçu

- Une exploration de l'interface utilisateur de QRadar et des astuces de navigation.

4 - QRadar – Source de journaux

- Comprendre les sources de journaux, les protocoles et la collecte des détails des événements.
  Atelier

  Gestion des sources de journaux et configuration

5 - Flux QRadar et QRadar Network Insights

- Comment QRadar analyse les informations sur les flux réseau et améliore la visibilité.
  Atelier

  Flux et Informations sur le réseau pour surveiller le trafic

6 - Moteur de règles personnalisé (CRE) de QRadar

- Introduction à la création et à la gestion des règles personnalisées dans QRadar.
  Atelier

  Exercices sur le moteur de règles personnalisé (CRE) pour créer et affiner les règles de sécurité

7 - Application Use Case Manager de QRadar

- Utilisation de l'application Use Case Manager pour organiser et gérer les cas de sécurité.

8 - QRadar – Actifs

- Découvrir et gérer les informations sur les actifs dans QRadar.

9 - Extensions de QRadar

- Aperçu des applications QRadar, des extensions de contenu et du cadre des applications.

10 - Travailler avec les incidents

- Comment analyser, enquêter et gérer les incidents dans QRadar.
  Atelier

  Analyse des incidents à l'aide des applications de workflow QRadar

11 - QRadar – Recherche, filtrage et AQL

- Techniques avancées de recherche, de filtrage et de requêtes avec AQL (Advanced Query Language).

12 - QRadar – Rapports et tableaux de bord

- Création de rapports personnalisés et construction de tableaux de bord avancés.
  Atelier

  Recherche avancée et création de rapports avec AQL et génération de tableaux de bords

13 - QRadar – Console d'administration

- Tâches administratives telles que la gestion des utilisateurs, la configuration et la vérification de la santé du système.
  Atelier

  Tâches administratives comme la gestion des actifs et des extensions

Les objectifs de la formation

- Comprendre le processus de collecte des données QRadar pour détecter les activités suspectes.
- Naviguer dans l'interface utilisateur de QRadar et utiliser ses principales fonctionnalités.
- Définir les sources de journaux, les protocoles et comprendre les détails des événements.
- Apprendre les bases du moteur de règles personnalisé (CRE) de QRadar.

- Utiliser l'application Use Case Manager pour gérer les cas de sécurité.
- Analyser les incidents et les informations sur les flux réseau.
- Créer et gérer des rapports personnalisés à l'aide des outils de reporting de QRadar.
- Utiliser AQL (Advanced Query Language) pour des recherches plus complexes.
- Découvrir les tâches administratives de QRadar pour une gestion efficace.

Evaluation

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

Les points forts de la formation

- Une formation opérationnelle : les apports théoriques sont systématiquement accompagnés de phases de mise en pratique qui favorisent un ancrage durable des acquis.
- Les conseils de professionnels ayant exploité la solution
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).