IBM - QRadar EDR : Intégration avec QRadar SIEM

Renforcez la sécurité de vos endpoints et maîtrisez l'intégration de QRadar EDR avec QRadar SIEM

Présentiel ou en classe à distance

1 jour (7 h) Réf.: IBMBQ530

Formation officielle

IBM

Idéal en Distanciel

QRadar EDR (Endpoint Detection and Response) est une solution avancée de détection et de réponse aux menaces sur les terminaux, qui permet aux entreprises de sécuriser les appareils finaux contre les attaques potentielles. L'intégration de QRadar EDR avec QRadar SIEM (Security Information and Event Management) permet d'amplifier la puissance de détection et de réponse étendues (XDR) en fournissant une visibilité centralisée sur les événements de sécurité à travers l'ensemble du réseau. Cette intégration utilise l'intelligence artificielle (IA) et l'automatisation pour aider à détecter, analyser et répondre rapidement aux menaces en temps réel. L'architecture API permet à QRadar EDR de transférer des alertes et des données de sécurité vers le SIEM, facilitant ainsi l'analyse et la prise de décision rapide lors d'incidents de sécurité.
Se former à l'intégration de QRadar EDR avec QRadar SIEM permet aux professionnels de la sécurité informatique de développer des compétences clés en gestion des menaces. Grâce à cette formation, vous apprendrez à configurer et à exploiter les puissantes capacités d'alertes et de détection de QRadar pour mieux protéger les points d'entrée de votre infrastructure. La maîtrise de ces outils vous permettra non seulement de renforcer la sécurité de vos terminaux, mais aussi d'optimiser la réponse aux incidents en automatisant certaines tâches critiques. De plus, en utilisant cette solution, les analystes peuvent se concentrer sur la gestion des menaces plutôt que sur la collecte manuelle des données de sécurité, un atout précieux dans un environnement en constante évolution.

A qui s'adresse cette formation ?

Pour qui

- Analystes SOC
- Analystes Sécurité
- Administrateurs QRadar EDR

Prérequis

- Aucun.

Programme

1 - Intégration avec QRadar SIEM

- Configurer une application API dans QRadar EDR pour connecter efficacement le système à votre QRadar SIEM. Cette étape permet une intégration transparente des données de détection des menaces et des alertes de sécurité entre les deux plateformes.
- Installer une nouvelle source de logs dans QRadar SIEM et configurer le bon protocole pour la collecte et l'analyse des données provenant de QRadar EDR.
- Analyser les alertes des endpoints à partir du dashboard SIEM, afin de détecter les menaces de manière proactive.

2 - QRadar EDR - Intégration avec QRadar SIEM - Lab

- Configurer l'intégration de QRadar EDR et QRadar SIEM, tout en testant la détection des menaces sur des terminaux via les alertes générées par le système.

- Exécuter différents scénarios, comme l'exécution de BitTorrent sur un endpoint et la détection de malware (exemple : tryme.exe)
- Simuler et comprendre comment l'intégration peut améliorer la détection et la réponse aux menaces en temps réel.

Les objectifs de la formation

- Configurer une application API dans QRadar EDR pour permettre l’intégration avec QRadar SIEM et améliorer la visibilité sur les événements de sécurité.
- Installer une source de logs dans QRadar SIEM et configurer le bon protocole pour cette source, afin de permettre une collecte de données fluide et précise.
- Analyser les alertes des endpoints en utilisant les données de QRadar EDR sur le dashboard SIEM, ce qui permettra d’identifier rapidement les menaces et d’y répondre efficacement.
- Exécuter des scénarios réels comme la détection de malware pour tester la capacité du système à réagir aux menaces sur les terminaux.

Evaluation

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

Les points forts de la formation

- Permet de créer, modifier et optimiser des sources de données sans dépendre des équipes IT.
- Apprentissage à travers des exercices concrets pour une maîtrise rapide des modules de données Cognos.
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).