IBM - QRadar EDR - Foundations

Renforcez la sécurité de votre entreprise en maîtrisant QRadar EDR

Présentiel ou en classe à distance

2 jours (14 h) Réf.: IBMBQ505

Formation officielle

IBM

Idéal en Distanciel

QRadar EDR (Endpoint Detection and Response) est une solution de sécurité avancée développée par IBM pour protéger les points de terminaison d'une organisation contre les menaces en constante évolution, comme les malwares et les ransomwares. Elle repose sur une architecture centralisée où le QRadar EDR Hive collecte et analyse les données en temps réel provenant des agents installés sur les endpoints. Grâce à cette approche, les équipes de sécurité peuvent détecter rapidement les comportements malveillants et y répondre de manière proactive. Cette technologie combine les avantages de l'analyse comportementale et de l'intelligence artificielle pour fournir une vue complète des menaces et de leurs évolutions à travers l'ensemble du réseau.
Se former à QRadar EDR est essentiel pour tout professionnel de la sécurité cherchant à renforcer la protection des endpoints de son organisation. En maîtrisant l'installation, la configuration et l'administration de cette plateforme, les participants deviennent capables de répondre rapidement aux alertes et de mener des enquêtes efficaces sur les incidents de sécurité. De plus, ce type de formation permet de comprendre les mécanismes sous-jacents aux attaques ciblant les terminaux, d'améliorer la gestion des fichiers téléchargés ou mis en quarantaine, et de configurer des politiques de sécurité avancées. La capacité à utiliser QRadar EDR pour détecter, analyser et neutraliser les menaces avant qu'elles n'atteignent le coeur du système est un atout majeur pour tout professionnel de la cybersécurité.

A qui s'adresse cette formation ?

Pour qui

- Administrateurs SOC
- Analystes Sécurité

Prérequis

- Aucun.

Programme

1 - Introduction

- Découvrir l'interface utilisateur de QRadar EDR et comment naviguer efficacement à travers le tableau de bord pour visualiser les menaces détectées sur vos endpoints.
- Comprendre l'architecture QRadar EDR et à positionner cette technologie dans votre environnement de sécurité informatique.
- Installer QRadar EDR en local en configurant le QRadar EDR Hive et les agents QRadar EDR sur les endpoints de votre entreprise.
- Déployer et mettre à jour l'agent QRadar EDR sur vos endpoints pour assurer une surveillance continue des menaces.

2 - Protection de vos endpoints

- Utiliser QRadar EDR pour investiguer les menaces sur vos endpoints en analysant les comportements suspects et en examinant les alertes générées par le système.

- Gérer les endpoints au sein de votre entreprise et à appliquer des mesures de sécurité en temps réel
- Comprendre les alertes générées par QRadar EDR et réagissez rapidement pour limiter l'impact des menaces détectées.
- Développer des compétences pour répondre aux attaques de malwares et ransomwares en utilisant les capacités d'analyse comportementale de QRadar EDR.
- Mettre en pratique vos connaissances à travers un laboratoire d'analyse des menaces en utilisant QRadar EDR sur des endpoints.

3 - Administrer votre environnement

- Configurer des notifications pour alerter les administrateurs sur les événements de sécurité via le protocole SMTP.
- Configurer les alertes pour qu'elles soient transmises à des systèmes tiers pour une gestion centralisée des incidents de sécurité.
- Créer des politiques de sécurité pour mieux gérer les comportements malveillants et les attaques sur les endpoints.
- Gérer les fichiers téléchargés et mis en quarantaine pour éviter toute propagation de malwares ou de ransomwares.
- Configurer des utilisateurs, groupes et clients pour garantir la sécurité et la confidentialité des accès à votre plateforme QRadar EDR.
- Optimiser l'analyse des menaces en configurant le Hive-Cloud Score pour obtenir une évaluation plus précise des risques.
- Développer des applications personnalisées pour étendre les fonctionnalités de QRadar EDR selon les besoins spécifiques de votre organisation.
- Surveiller les journaux d'audit pour suivre les activités suspectes et garantir la conformité avec les politiques de sécurité.

Les objectifs de la formation

- Naviguer efficacement sur le tableau de bord QRadar EDR et analyser les alertes de sécurité.
- Comprendre l'architecture QRadar EDR et installer la plateforme sur vos serveurs locaux.
- Déployer l'agent QRadar EDR sur les endpoints pour renforcer leur protection contre les malwares et ransomwares.
- Investiguer et gérer les menaces sur vos endpoints, en appliquant des politiques de sécurité adaptées.
- Répondre rapidement aux alertes générées par QRadar EDR et agir sur les comportements malveillants.
- Configurer des notifications, des alertes et des rapports pour mieux surveiller les menaces et garantir une réponse rapide.

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).