IBM QRadar SIEM Foundations

Durée: 3 Jours **Réf de cours: BQ105G** **Méthodes d'apprentissage: Classe à distance**

Résumé:

IBM Security QRadar offre une visibilité approfondie sur l'activité des réseaux, des terminaux, des utilisateurs et des applications. Il assure la collecte, la normalisation, la corrélation et le stockage sécurisé des événements, des flux, des actifs et des vulnérabilités. Les attaques suspectes et les violations de politiques sont mises en évidence en tant qu'infractions.
Dans ce cours, vous apprendrez à connaître l'architecture de la solution, à naviguer dans l'interface utilisateur et à enquêter sur les infractions. Vous recherchez et analysez les informations à partir desquelles QRadar a conclu à une activité suspecte. Des exercices pratiques renforcent les compétences acquises.
Mise à jour 31 07 2024

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Ce cours est destiné aux analystes sécurité, aux architectes techniques sécurité, aux responsables sécurité, aux administrateurs réseau et aux administrateurs système utilisant QRadar SIEM.

Objectifs pédagogiques:

- À l'issue de ce cours, vous devriez être en mesure d'effectuer les activités suivantes :
- Décrire comment QRadar collecte des données pour détecter des activités suspectes
- Décrire l'architecture de QRadar et les flux de données
- Naviguer dans l'interface utilisateur
- Définir les sources de logs, les protocoles et les détails des événements
- Découvrir comment QRadar recueille et analyse les informations sur le flux du réseau
- Décrire le moteur de règles personnalisées de QRadar
- Utiliser l'application Use Case Manager
- Découvrir et gérer les informations sur les équipements
- Apprendre à connaître une variété d'applications QRadar, d'extensions de contenu et d'App Framework
- Analyser les infractions en utilisant l'interface utilisateur de QRadar et l'application Analyst Workflow
- Rechercher, filtrer, grouper et analyser les données de sécurité
- Utiliser AQL pour des recherches avancées
- Utiliser QRadar pour créer des rapports personnalisés
- Explorer la gestion des données agrégées
- Définir des rapports sophistiqués à l'aide des tableaux de bord Pulse
- Découvrir les tâches administratives de QRadar

Pré-requis:

Avant de suivre ce cours, assurez-vous que vous possédez les connaissances suivantes :

- Infrastructure informatique
- Fondamentaux de la sécurité informatique

- Linux - Windows
- Réseau TCP/IP
- Syslog

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

BQ205G IBM Security QRadar SIEM Notions avancées

Contenu:

Chapitres :

- Unit 1 Architecture QRadar
- Unit 2 QRadar UI - Vue d'ensemble
- Unit 3 QRadar - Sources de logs
- Unit 4 QRadar flows et QRadar Network Insights
- Unit 5 QRadar Custom Rule Engine (CRE)
- Unit 6 QRadar Use Case Manager app
- Unit 7 QRadar - Actifs
- Unit 8 Extensions de QRadar
- Unit 9 Travailler avec les offenses
- Unit 10 QRadar - Recherche, filtrage et AQL
- Unit 11 QRadar - Rapports et tableaux de bord
- Unit 12 QRadar - Console d'administration

Des exercices pratiques complets sont fournis pour permettre aux participants d'avoir un aperçu du travail de routine d'un analyste de la sécurité informatique qui utilise la plateforme QRadar SIEM. Les exercices couvrent les sujets suivants :

- Exercices sur l'architecture
- Aperçu de l'interface utilisateur exercices
- Exercices sur les sources de logs
- Exercices sur les flux et QRadar Network Insights
- Exercices sur le moteur de règles personnalisées (CRE)
- Gestionnaire de cas d'utilisation exercices
- Exercices sur les environnements
- Exercices App Framework
- Travailler avec les offenses
- Recherche, filtrage et exercices AQL
- Exercices sur les rapports et les tableaux de bord
- Exercices sur les tâches de l'administrateur QRadar

L'environnement de travail de ce cours utilise la plateforme IBM QRadar SIEM 7.5.

Méthodes pédagogiques :

Un support de cours officiel sera remis aux participants.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement