IBM QRadar SIEM Advanced Topics

Durée: 2 Jours **Réf de cours: BQ205G** **Méthodes d'apprentissage: Virtual Learning**

Résumé:

QRadar SIEM offre une visibilité approfondie sur l'activité du réseau, 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.
Ce cours de 2 jours avec formateur vous guide à travers divers sujets avancés sur QRadar, tels que les sources de logs personnalisées, les collections de données de référence et les règles personnalisées, les données X-Force et l'application Threat Intelligence, UBA et QRadar Advisor, le paramétrage et les scripts d'action personnalisés.
Le cours aborde également l'intégration avec IBM SOAR. Des exercices pratiques renforcent les compétences acquises. L'environnement de laboratoire pour ce cours utilise la plateforme IBM QRadar SIEM 7.5.
Mise à jour 31 07 2024

Public visé:

Ce cours est destiné aux administrateurs et aux analystes sécurité possédant déjà des compétences de base sur QRadar.

Objectifs pédagogiques:

- A l'issue de cette formation, les participants auront étudié les points suivants :
- Apprendre à créer des sources de logs personnalisées
- Découvrir comment travailler avec des collections de données de référence et des règles personnalisées
- Utiliser les données X-Force et l'application Threat Intelligence
- Utiliser l'application Use Case Manager
- Apprendre à utiliser UBA et QRadar Advisor
- Découvrir le Tuning
- Explorer les scripts d'action personnalisés
- Aborder l'intégration avec IBM SOAR

Pré-requis:

Les participants doivent avoir des connaissances sur les sujets suivants :

- Infrastructure informatique
- Principes fondamentaux de la sécurité informatique
- Linux - Windows
- Réseau TCP/IP
- Syslog
- Compétences fondamentales pour la plateforme IBM QRadar Security Intelligence Platform (au moins les compétences enseignées dans le cours IBM QRadar SIEM Foundations - BQ105G ou BQ105XG - Elearning)

Test et certification

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

BQ610G QRadar UBA: Detecting Insider Threats

Contenu:

Unit 1 : Personnalisation des sources de logs

Unit 2 : Collections de données de référence et règles personnalisées

Unit 3 : IBM X-Force Threat Intelligence dans QRadar

Unit 4 : Analyse du comportement utilisateur et outil Advisor avec Watson

Unit 5 : Tuning et paramètrage

Unit 6 : Scripts d'action personnalisés

Unit 7 : Intégration IBM SOAR

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