

QRadar UBA: Detecting Insider Threats

Durée: 1 Jour **Réf de cours: BQ610G** **Méthodes d'apprentissage: Virtual Learning**

Résumé:

Learn how to detect insider threats triggered by anomalous or malicious user behavior. Get ready to install, configure, and tune IBM Security® QRadar UBA and the Machine Learning app. Improve your skill to investigate user behavior with UBA and expand your threat detection capabilities across your network with the QRadar® Advisor with Watson app.
Mise à jour 19/12/2024

Public visé:

Security Analyst

Objectifs pédagogiques:

- After this course participants should be able to:
- Analyze UBA concepts, such as the senseValue variable, risk scores, and the IBM Sense DSM.
- Identify how QRadar rules are connected to UBA and how user information is imported into the app.
- Install and configure the app, as well as the User Import tool and the Machine Learning app.
- Tune UBA settings to improve the application's behavior and performance.
- Analyze how UBA can help you detect and investigate insider threats.
- Analyze how to use the UBA Dashboard.
- Investigate how to detect malicious user behavior.

Pré-requis:

■

Contenu:

Unit 1: Architecture and Overview

Unit 3: Tuning

Unit 5: Student exercise

Unit 2: Setup

Unit 4: An overview to detecting and investigating insider threats

- Installation
- Configuration
- User Import
- Machine Learning configuration

Méthodes pédagogiques :

Un support de cours officiel sera fourni 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