QRadar UBA: Detecting Insider Threats

Cursusduur: 1 Dag **Cursuscode: BQ610G** **Trainingsmethode: Virtual Learning**

Beschrijving:

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.

Virtueel en Klassikaal™

Virtueel en Klassikaal™ is een eenvoudig leerconcept en biedt een flexibele oplossing voor het volgen van een klassikale training. Met Virtueel en Klassikaal™ kunt u zelf beslissen of u een klassikale training virtueel (vanuit huis of kantoor)of fysiek op locatie wilt volgen. De keuze is aan u! Cursisten die virtueel deelnemen aan de training ontvangen voor aanvang van de training alle benodigde informatie om de training te kunnen volgen.

Doelgroep:

Security Analyst

Doelstelling:

- 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 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.

Cursusinhoud:

Unit 1: Architecture and Overview

Unit 2: Setup

- Installation
- Configuration
- User Import
- Machine Learning configuration

Unit 3: Tuning

Unit 4: An overview to detecting and investigating insider threats

Unit 5: Student exercise

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.com/nl-nl/

Iepenhoeve 5, 3438 MR Nieuwegein