QRadar EDR: Integrating with QRadar SIEM

Duration: 1 Day Course Code: BQ530G Delivery Method: Virtual Learning

Overview:

In this course you learn how to integrate QRadar EDR and SIEM by creating an API application in QRadar EDR and by adding a new log source in QRadar SIEM to add endpoint detection and alerts to QRadar SIEM. Integrating QRadar EDR and SIEM amplifies the power of QRadar XDR (extended detection and response) by leveraging AI and automation opportunities. Having advanced and automated response capabilities enables analysts to focus on the fight in front of them.
This course applies to version 3.12 of the on-premises IBM Security QRadar EDR offering.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

This course is tailored to IT security analysts in a Security Operations Center (SOC) environment who are tasked with endpoint protection and threat hunting, as well as QRadar EDR administrators, incident responders, and managed service security providers (MSSP).

Objectives:

- In this course you learn to do these activities:
- Configure an API application in QRadar EDR
- Install a new log source in QRadar SIEM
- Configure the correct protocol for a log source in QRadar SIEM
- Analyze endpoint alerts from the SIEM dashboard using data from EDR

Content:

Unit 1: Integrating with QRadar SIEM

- Configure an API application in QRadar EDR
- Install a new log source in QRadar SIEM
- Configure the correct protocol for a log source in QRadar SIEM
- Analyze endpoint alerts from the SIEM dashboard using data from EDR

Unit 2: QRadar EDR - integrating with QRadar SIEM - Lab

- Exercise 1 - Configuring QRadar EDR and QRadar SIEM integration
- Exercise 2 - BitTorrent is run on an endpoint
- Exercise 3 â€“ Malware detected (tryme.exe)

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK