QRadar EDR: Foundations

Duration: 2 Days   **Course Code: BQ505G**   **Delivery Method: Virtual Learning**

Overview:

In this course, you learn about the IBM Security® QRadar® EDR architecture and how to position the product within your company's landscape of security solutions. You gain skills around how to install the QRadar EDR Hive on your premises and the EDR Agents on your endpoints. You can review the user interface and how to navigate the EDR Dashboard while investigating endpoint threats.
This course applies to version 3.12 of the on-premises 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:

Security operations center (SOC) AdministratorSOC AnalystSecurity AnalystIncident ResponderManaged Service Security Provider (MSSP)

Objectives:

- In this course, you learn to perform the following tasks:
- Navigate the QRadar EDR Dashboard
- Describe the QRadar EDR architecture
- Install the on-premises QRadar EDR Hive and configure the initial setup
- Deploy the QRadar EDR Agent on your endpoints
- Investigate threats on endpoints
- Manage endpoints
- Understand and respond to alerts and trends
- Act upon behavioral malware and ransomware attacks
- Configure notifications and Simple Mail Transfer Protocol
- Set up forwarding alerts
- Define policies
- Handle downloaded and quarantined files from your endpoints
- Set up users, groups, and clients
- Configure Hive-Cloud Score
- Create applications
- Monitor audit logs

Content:

Getting started

- Dashboard overview
- Architecture
- QRadar EDR on-prem installation
- Downloading, installing, and updating the QRadar EDR Agent

Protecting your endpoints

- Investigating threats on endpoints
- Managing endpoints
- Understanding and responding to alerts and trends
- Acting upon behavioral malware and ransomware attacks
- Hunting for threats on your endpoint using a QRadar EDR lab

Administering your environment

- Configuring notifications and Simple Mail Transfer Protocol (SMTP)
- Setting up forwarding alerts
- Defining policies
- Handling downloaded and quarantined files from your endpoints
- Setting up users, groups, and clients
- Configuring Hive-Cloud Score
- Creating applications
- Monitoring audit logs

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