IBM QRadar SIEM Foundations

Varighed: 3 Days Kursus Kode: BQ104G

Beskrivelse:

IBM Security QRadar enables deep visibility into network, endpoint, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, assets, and vulnerabilities. Suspected attacks and policy breaches are highlighted as offenses. In this course, you learn about the solution architecture, how to navigate the user interface, and how to investigate offenses. You search and analyze the information from which QRadar concluded a suspicious activity. Hands-on exercises reinforce the skills learned.

In this 3-day instructor-led course, you learn how to perform the following tasks: Describe how QRadar collects data to detect suspicious activitiesDescribe the QRadar architecture and data flowsNavigate the user interfaceDefine log sources, protocols, and event detailsDiscover how QRadar collects and analyzes network flow informationDescribe the QRadar Custom Rule EngineUtilize the Use Case Manager appDiscover and manage asset informationLearn about a variety of QRadar apps, content extensions, and the App FrameworkAnalyze offenses by using the QRadar UI and the Analyst Workflow appSearch, filter, group, and analyze security dataUse AQL for advanced searchesUse QRadar to create customized reportsExplore aggregated data managementDefine sophisticated reporting using Pulse DashboardsDiscover QRadar administrative tasks

Extensive lab exercises are provided to allow students an insight into the routine work of an IT Security Analyst operating the IBM QRadar SIEM platform. The exercises cover the following topics: Architecture exercisesUI Overview exercisesLog Sources exercisesFlows and QRadar Network Insights exercisesCustom Rule Engine (CRE) exercisesUse Case Manager app exercisesAssets exercisesApp Framework exercisesWorking with Offenses exercises.Search, filtering, and AQL exercisesReporting and Dashboards exercisesQRadar Admin tasks exercises

The lab environment for this course uses the IBM QRadar SIEM 7.4 platform.

Målgruppe:

This course is designed for security analysts, security technical architects, offense managers, network administrators, and system administrators using QRadar SIEM.

Agenda:

- After completing this course, you should be able to perform the following tasks:
- Describe how QRadar collects data to detect suspicious activities
- Describe the QRadar architecture and data flows
- Navigate the user interface
- Define log sources, protocols, and event details
- Discover how QRadar collects and analyzes network flow information
- Describe the QRadar Custom Rule Engine
- Utilize the Use Case Manager app
- Discover and manage asset information
- Learn about a variety of QRadar apps, content extensions, and the App Framework
- Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Search, filter, group, and analyze security data
- Use AQL for advanced searches
- Use QRadar to create customized reports
- Explore aggregated data management
- Define sophisticated reporting using Pulse Dashboards
- Discover QRadar administrative tasks

Forudsætninger:

Before taking this course, make sure that you have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog

Indhold:

Unit 12: QRadar Admin Console

Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

training@globalknowledge.dk

www.globalknowledge.com/da-dk/

Global Knowledge, Stamholmen 110, 2650 Hvidovre