

IBM QRadar SIEM Advanced Topics

Varighed: 2 Days Kursus Kode: BQ205G Leveringsmetode: Virtuel deltagelse

Beskrivelse:

QRadar SIEM provides deep visibility into network, 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.

This 2-day instructor-led course walks you through various advanced topics about QRadar such as custom log sources, reference data collections and custom rules, X-Force data and the Threat Intelligence app, UBA and QRadar Advisor, tuning and custom action scripts. The course also discusses integration with IBM SOAR. Hands-on exercises reinforce the skills learned.

The lab environment for this course uses the IBM QRadar SIEM 7.5 platform.

Virtuel deltagelse

Et V&C Select kursus indholder nøjagtig det samme som et almindeligt kursus. Før kursusstart modtager man kursusmaterialet. Dernæst logger man på kurset via internettet og ser via sin pc den selvsamme præsentation som de øvrige deltagere, man kommunikerer via chat med underviseren og de øvrige deltagere på kurset. Denne uddannelsesmodel er både tids-og omkostningsbesparende og kan være et oplagt alternativ til almindelig klasseundervisning, hvis man f.eks. har et begrænset rejsebudget.

Målgruppe:

This course is designed for security administrators and security analysts.

Agenda:

- Learn how to create custom log sources
- Discover how to work with reference data collections and custom rules
- Use X-Force data and Threat Intelligence app
- Use the Use Case Manager app
- Learn how to use UBA and QRadar Advisor
- Discover Tuning
- Explore Custom action scripts
- Discuss Integration with IBM SOAR

Forudsætninger:

Students should be knowledgeable about the following topics:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog
- Foundational skills for the IBM QRadar Security Intelligence Platform (at least the skills that are taught in the IBM QRadar SIEM Foundations - BQ104 course)

Indhold:

Unit 1: Custom log sources

Unit 2: Reference data collections and custom rules

Unit 3: IBM X-Force Threat Intelligence in QRadar

Unit 4: User Behavior Analytics and Advisor with Watson

Unit 5: Tuning

Unit 6: Custom action scripts

Unit 7: IBM SOAR integration

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