IBM Security QRadar SIEM 7.2 Administration and Configuration (3 Days)

Description

QRadar SIEM provides deep visibility into network, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, assets, topologies, and vulnerabilities. Suspected attacks and policy breaches are highlighted as offenses. In this course, you learn how to configure and administer QRadar SIEM, create Universal DSMs and Log Source Extensions, and create event, flow and anomaly rules. Using the skills taught in this course, you can maintain QRadar SIEM, work with log sources, analyze the offenses created by rules and if necessary fine-tune them. Hands-on exercises reinforce the skills learned.

Audience

This course is for:

- security analysts
- security technical architects
- offense managers
- network administrators
- QRadar SIEM administrators
- and professional services

Prerequisites

You should have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Log files and events
- QRadar SIEM user interface
- Successfully completed IBM Security QRadar SIEM 7.1 MR2 Foundations

Skills Taught

- Configure and administer QRadar SIEM
- Create and deploy a Universal DSM
- Create event, flow and anomaly rules
- Fine tune rules

Course Outline

Unit 1: Initial configuration and administration

Unit 2: Custom Log Sources

Unit 3: Rule creation and fine tuning