IBM QRadar SIEM Foundations (3 Day)

IBM QRadar SIEM provides deep visibility into network, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, asset profiles, and vulnerabilities. QRadar SIEM classifies suspected attacks and policy violations as offenses.

In this 3-day instructor-led course, you learn how to perform the following tasks:

- Describe how QRadar SIEM collects data to detect suspicious activities
- Describe the QRadar SIEM component architecture and data flows
- Navigate the user interface
- Investigate suspected attacks and policy breaches
- Search, filter, group, and analyze security data
- Investigate the vulnerabilities and services of assets
- Use network hierarchies
- Locate custom rules and inspect actions and responses of rules
- Analyze offenses created by QRadar SIEM
- Use index management
- Navigate and customize the QRadar SIEM dashboard
- Use QRadar SIEM to create customized reports
- Use charts and filters
- Use AQL for advanced searches
- Analyze a real world scenario

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:

- Using the QRadar SIEM user interface
- Investigating an Offense triggered by events
- Investigating the events of an offense
- Investigating an offense that is triggered by flows
- Using rules
- Using the Network Hierarchy
- Index and Aggregated Data Management
- Using the QRadar SIEM dashboard
- Creating QRadar SIEM reports
- Using AQL for advanced searches
- Analyze a real-world large-scale attack

The lab environment for this course uses the IBM QRadar SIEM 7.3 platform.

Skills Gained

After completing this course, you should be able to perform the following tasks:

- Describe how QRadar SIEM collects data to detect suspicious activities
- Describe the QRadar SIEM component architecture and data flows
- Navigate the user interface
- Investigate suspected attacks and policy violations
- Search, filter, group, and analyze security data
- Investigate events and flows
- Investigate asset profiles
- Describe the purpose of the network hierarchy
- Determine how rules test incoming data and create offenses
- Use index and aggregated data management
- Navigate and customize dashboards and dashboard items
- Create customized reports
- Use filters
- Use AQL for advanced searches
- Analyze a real world scenario

Who Can Benefit

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

Prerequisites

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

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

Course Outline

- Unit 1: Introduction to IBM QRadar
- Unit 2: IBM QRadar SIEM component architecture and data flows
- Unit 3: Using the QRadar SIEM User Interface
- Unit 4: Investigating an Offense Triggered by Events
- Unit 5: Investigating the Events of an Offense
- Unit 6: Using Asset Profiles to Investigate Offenses
- Unit 7: Investigating an Offense Triggered by Flows
- Unit 8: Using Rules
- Unit 9: Using the Network Hierarchy
- Unit 10: Index and Aggregated Data Management
- Unit 11: Using the QRadar SIEM Dashboard
- Unit 12: Creating Reports
- Unit 13: Using Filters
- Unit 14: Using the Ariel Query Language (AQL) for Advanced Searches
- Unit 15: Analyzing a Real-World Large-Scale Attack
- Appendix A: A real-world scenario introduction to IBM QRadar SIEM
- Appendix B: IBM QRadar architecture