IBM QRadar SIEM

1. **Introduction**
   - Introduction and Course objectives
   - What is Organization environment looks like
   - Security Types
2. **OS Basics**
   - Types of OS and differences
   - Installation of Windows and Linux OS
   - Overview of Server Management
   - Checking the events at OS level
3. **Networking Basics**
   - Type of Networks, TCP/IP Networking
   - Class of IP ranges and subnets
   - Type of Network connectivity devices
4. **Introduction to Cloud and Virtualization**
   - What is virtualization
   - How virtualization works and its benefits
   - What is Cloud Computing
   - Benefits of Cloud Computing
   - Cloud technology overview and vendors
   - Cloud Computing Models (Private, Public, Hybrid and Community)
   - Cloud Services (IaaS, PaaS, SaaS)
5. **IT Infrastructure and Security Fundamentals**
   - What will make IT infrastructure
   - What are other SIEM tools available in the market
6. **Introduction to IBM Qradar SIEM**
   - Overview and History of Qradar SIEM
   - Key Concepts, HA and Capabilites of Qradar SIEM
7. **IBM Qradar SIEM Component Architecture and Data Flows**
   - Type of Qradar software availability
   - Qradar Deployment Overview
   - Qradar Installations
   - Event Collector and Event Processor
   - Flow Collector and Flow Processor

- Magistrate and Aerial Database

8. **Logs Collection**
   - WinCollect
   - Syslog Method
   - Log source creation and Management
9. **Qradar Console Management/User interface**
   - Dashboard
   - Types of Dashboards
   - Dashboard customization
10. **Log Activity**
    - Real time log streaming
    - Filter criteria and Event Search
    - False positive and Tuning
11. **Network Activity**
    - Real time flow streaming
    - Filter criteria and Flow Search
    - False positive and Tuning

12. **Offenses, Rules and Reports**
    - Offense Management
    - Rules and building blocks
    - Report management
13. **Managing custom log sources**
14. **Using and creating rules**
15. **Assets and Vulnerability Assessment**
    - Asset discovery, importing and exporting assets
    - vulenerabilityassessment
16. **Risks Management and Admin**
    - Risk Assessment
    - Qradar Administration
17. **Backup**
    - Types of Backup