Benefits of Doing a SOC Course (Splunk and IBM QRadar)

1. **Comprehensive Threat Detection and Monitoring**:
    a. You will learn how to effectively monitor network activity, detect potential threats, and identify vulnerabilities using **SIEM tools** like Microsoft Azure Sentinel and IBM QRadar. These platforms help aggregate and correlate data from various sources to provide visibility into security events in real-time.
    b. **Sentinel** helps organizations detect, investigate, and respond to security threats across their entire enterprise., while **QRadar** excels in threat detection through advanced correlation rules.
2. **Incident Response and Forensics**:
    a. By mastering these tools, you gain the ability to track security incidents, investigate root causes, and take corrective measures, helping organizations respond quickly and efficiently to cyber threats.
    b. Sentinel and QRadar both support forensic analysis and incident response workflows, which are crucial for managing security incidents end-to-end.
3. **Hands-on Experience in SIEM Operations**:
    a. Through practical labs, you will experience real-world scenarios in Security Operations Centers (SOC), making you ready for operational roles in cybersecurity.
    b. You will get hands-on with both **rule-based and behavior-based threat detection**, enhancing your ability to create custom rules, dashboards, and reports.
4. **Compliance and Reporting**:

   a. Azure Sentinel and IBM QRadar are commonly used for meeting compliance requirements (e.g., **PCI-DSS**, **GDPR**, **HIPAA**). You will learn to generate reports and configure the platforms to align with regulatory standards, which is critical for businesses.
5. **Career Advancement**:
   a. Gaining expertise in Azure Sentinel and IBM QRadar opens doors to roles like **SOC Analyst**, **SIEM Engineer**, **Threat Hunter**, and **Incident Responder**.
   b. Certifications in these tools can lead to higher salaries and job prospects due to the rising demand for skilled SOC professionals.
6. **Automation and Efficiency**:
   a. Sentinel and QRadar both offer automation capabilities (e.g., **playbooks** and **SOAR integration**), enabling you to automate routine tasks, such as alert generation and response actions. This reduces manual effort and speeds up threat resolution.

Prerequisites for SOC (Microsoft Azure Sentinel and IBM QRadar) Course:

1. **Basic Networking Knowledge**:
   a. Understanding of **TCP/IP**, **subnetting**, **ports**, and **protocols**. Knowledge of **OSI layers** and how network traffic works is essential for configuring and interpreting logs in SIEM systems.
2. **Basic Cybersecurity Concepts**:
   a. Familiarity with cybersecurity terms like **firewalls**, **IDS/IPS**, **malware**, **DDoS**, **threat intelligence**, and **incident response**.
3. **Operating Systems Knowledge**:
   a. Understanding of both **Windows** and **Linux** operating systems. Many logs and events analyzed in SOC environments come from these OSes, so knowing their structure and behavior is important.
4. **Log Management Concepts**:

   a. Basic understanding of how logs are generated, collected, and stored. Familiarity with log formats such as **syslog**, **Windows Event Logs**, and **JSON** will help you effectively ingest data into SIEM platforms.
5. **Scripting and Automation (optional)**:
   a. Some knowledge of scripting languages such as **Python** or **Bash** may be helpful in automating tasks within these SIEM tools or integrating them with other platforms.
6. **SIEM Basics**:
   a. If you're new to SIEM tools, having a general understanding of how SIEMs work can be beneficial. This includes the flow of events, event correlation, alerting, and reporting.

Recommended Prerequisite Learning Paths:

- **Basic Cybersecurity Courses** (e.g., **CompTIA Security+**)
- **Networking Certifications** (e.g., **CCNA**, **CompTIA Network+**)
- **Introductory SIEM Training** on Sentinel or QRadar basics (free modules are often available online)

This ensures that you have the foundational knowledge to excel in a SOC environment using Sentinel or IBM QRadar.

common syllabus for Security Operations Centre (SOC) training, focusing on popular SIEM platforms like **Microsoft Azure Sentinel** and **IBM QRadar**. This syllabus is a general guide for students or professionals interested in learning how to manage and operate in a SOC using these platforms.

1. Introduction to SOC

- What is SOC?
- Importance of SOC in Cybersecurity

- SOC Roles and Responsibilities
- Overview of SIEM (Security Information and Event Management)
- Introduction to Threat Intelligence

Estimated Time: 3 hours

2. Basic Network and Security Concepts

- Understanding of TCP/IP, Ports, and Protocols
- Understanding OSI Model
- Security Threats: Malware, Phishing, Ransomware
- Firewalls, IDS/IPS, Antivirus, and Security Controls
- Key Concepts of Vulnerability, Exploitation, and Risk

Estimated Time: 5 hours

3. Azure Sentinel Fundamentals

- Architecture of SIEM
- Components of SIEM
- Subscription and Pricing
- KQL (Kusto Query Language): Basic you Need for Sentinel and Security
- What is LAW (Log Analytic Workspace)
- How to collect the Log?
- Start using the connector
- What is Sentinel Workbook
- What are Analytic Rules?
- How to detect suspicious activity?
- Generating an incident
- Why Automation is needed?
- Let’s talk about SOAR?
- Get to know about Logic App.
- What is Playbook?

- Implement of Automation in the Sentinel

Estimated Time: 12-16 hours

4. IBM QRadar Fundamentals

- Overview of IBM QRadar SIEM
- Installation and Configuration of QRadar
- Collecting Logs: Log Sources and Protocols
- Rule-Based Event Correlation in QRadar
- Working with Offenses and Investigations
- Creating and Customizing Dashboards in QRadar
- Report Generation and Alerts in QRadar

Estimated Time: 10-12 hours

5. Security Incident Monitoring and Detection

- Event Monitoring and Analysis
- Real-time Monitoring of Security Events
- Event Correlation using SIEM
- Incident Detection and Investigation Techniques
- False Positives and False Negatives in Alerts
- Using Threat Intelligence for Enrichment

Estimated Time: 8 hours

6. Incident Response and Remediation

- Introduction to Incident Response (IR)
- SOC Tiered Incident Escalation (L1, L2, L3)
- Forensics in Incident Response
- Handling Different Types of Security Incidents
    - Malware, Insider Threats, DDoS

- Automating Incident Response using Playbooks

Estimated Time: 8 hours

7. Security Analytics

- Introduction to Security Analytics
- User and Entity Behavior Analytics (UEBA)
- Use of Machine Learning for Threat Detection
- Case Studies: Threat Detection with Splunk and QRadar

Estimated Time: 6 hours

8. Case Studies and Practical Labs

- Real-world SOC Scenarios
- Hands-on Lab Exercises with Sentinel and IBM QRadar
- Detecting and Investigating Threats in SOC
- Handling Security Incidents End-to-End

Estimated Time: 10-15 hours (Labs)

Total Duration:

- **Sentinel Training:** ~50 hours
- **QRadar Training:** ~40 hours

The course can be adjusted based on the learners' proficiency and training requirements. Both Sentinel and QRadar offer rich functionality, so the duration and depth of each topic may vary depending on the audience.