**Name:Abirami R**

**Assignment Title: Understanding SOC, SIEM, and QRadar**

**Objective:** The objective of this assignment is to explore the concepts of Security Operations Centers (SOCs), Security Information and Event Management (SIEM) systems, and gain hands-on experience with IBM QRadar, a popular SIEM tool.

**Instructions:**

**1. Introduction to SOC:** Begin by providing a comprehensive overview of what a Security Operations Center (SOC) is. Explain its purpose, key functions, and the role it plays in an organization's cybersecurity strategy.

**2. SIEM Systems:** Explore the concept of Security Information and Event Management (SIEM) systems. Discuss why SIEM is essential in modern cybersecurity and how it helps organizations monitor and respond to security threats effectively.

**3. QRadar** Overview: Research IBM QRadar and describe its key features, capabilities, and benefits as a SIEM solution. Include information on its deployment options (on-premises vs. cloud).

**4. Use Cases:** Provide real-world use cases and examples of how a SIEM system like IBM QRadar can be used in a SOC to detect and respond to security incidents.