# Understanding SOC, SIEM, and QRadar

## 1. Introduction to SOC

Security Operation Centre (SOC) is a centralised function within an organisation employing people, processes, and technology to continuously monitor and improve an organisation's security posture while preventing, detecting, analysing, and responding to cyber security incidents.

Key functions of the SOC are

- Preparation and Preventative Maintenance
- Continuous Proactive Monitoring
- Alert Ranking and Management
- Threat Response
- Recovery and Remediation
- Root Cause Investigation
- Security Refinement and Improvement
- Compliance Management

The SOC plays a critical role in an organisation's cyber security strategy by serving as the front line defense against cyber threats. It helps in early threat detection, reducing the impact of security incidents, minimising downtime, and ensuring compliance with security policies and regulations, ultimately enhancing the overall resilience and security of the organisation.

## 2. SIEM Systems

Security Information and Event Management (SIEM) systems collect and aggregate security-related data from various sources, such as network devices, servers, and applications, to provide a comprehensive view of an organisation's security posture.

Core functions of SIEM are

- **Log management:** SIEM systems gather vast amounts of data in one place, organise it, and then determine if it shows signs of a threat, attack, or breach.
- **Event correlation:** The data is then sorted to identify relationships and patterns to quickly detect and respond to potential threats.
- **Incident monitoring and response:** SIEM technology monitors security incidents across an organisation's network and provides alerts and audits of all activity related to an incident.

Overall, SIEM systems play a vital role in enhancing an organization's ability to monitor and respond effectively to security threats, ultimately strengthening its cybersecurity posture.

## 3. QRadar Overview

IBM QRadar is a powerful Security Information and Event Management (SIEM) solution known for its robust features, capabilities, and benefits in enhancing an organisation's cyber security posture.

Key features of Qradar are

- **Log Management:** QRadar collects and stores logs and events from a wide range of sources, including network devices, servers, applications, and security tools.
- **Threat Detection:** QRadar uses threat intelligence feeds and behavioural analytics to detect known and unknown threats, improving detection accuracy.
- **Incident Response:** It provides automated incident response capabilities, enabling security teams to respond swiftly to security incidents and breaches.
- **User Behaviour Analytics (UBA):** QRadar UBA analyses user and entity behaviour to detect insider threats and abnormal activities.
- **Integration:** QRadar integrates seamlessly with a wide range of security technologies, allowing for enhanced visibility and interoperability within the security stack.

Deployment options include

- **On-Premises**: Organisations can deploy QRadar on their own infrastructure, providing complete control over the SIEM environment. This option is suitable for organisations with stringent data privacy and compliance requirements.
- **Cloud**: IBM offers QRadar on Cloud, a managed SIEM service hosted in the cloud. This option is beneficial for organisations seeking scalability, ease of management, and reduced infrastructure overhead.

Benefits of using IBM Qradar

- **Enhanced Security**: QRadar's advanced analytics and threat detection capabilities help organisations identify and mitigate security threats effectively.
- **Simplified Compliance**: It aids in meeting regulatory compliance requirements by providing reporting and auditing features.
- **Scalability**: QRadar can scale to accommodate the evolving needs of organisations, whether deployed on-premises or in the cloud.
- **Integration**: Its ability to integrate with other security tools and technologies enhances an organisation's overall security posture.
- **Efficiency**: Automation and orchestration features streamline incident response, reducing manual effort and response time.
- **Threat Intelligence**: Integration with threat intelligence feeds ensures that organisations stay up-to-date on the latest threat intelligence.

## 4. Use Cases

IBM Qradar can be used within a SOC to detect and respond to security incidents.
Some major use cases include

- **Malware detection** - QRadar SIEM can detect the presence of malware by analysing network traffic and identifying suspicious patterns or communication with known malicious IP addresses.
- I**nsider threat detection** - QRadar can monitor user behaviour and identify insider threats by recognising unusual access patterns, data exfiltration, or unauthorised access to sensitive information.
- **Anomaly detection** - QRadar employs behavioural analytics to identify anomalies in user or system behaviour that may indicate unauthorised access or system compromise.
- **Threat intelligence integration** - QRadar integrates with threat intelligence feeds to correlate security events with known threats, vulnerabilities, or indicators of compromise.
- **Incident response automation** - QRadar can automate incident response processes, such as blocking IP addresses, isolating compromised systems, or resetting user credentials in response to specific security incidents.