SAGA
A NOVENTIQ Company

IBM QRadar SIEM

IBM QRadar Security Information and Event Management (SIEM) is designed to provide security teams with centralized visibility into enterprise-wide security data and actionable insights into the highest priority threats. Actionable alerts provide greater context into potential incidents, enabling security analysts to swiftly respond to limit the attackers' impact. QRadar is purpose-built to address security use cases and intentionally designed to easily scale with limited customization effort required.

KEY FEATURES

- Collecting, parsing, and normalizing both log and flow data with more than 450 pre-built log sources
- Automatically analyze and correlate activity across multiple data sources including logs, events, network flows, user activity, vulnerability information and threat intelligence to identify known and unknown threats.
- Anomaly detection capabilities to identify changes in behavior that could be indicators of an unknown threat.
- Default setting compliance packages for General Data Protection Regulation (GDPR), the Federal Information Security Management Act (FISMA), Sarbanes-Oxley (SOX), HIPAA, ISO 27001, Payment Card Industry Data Security Standard (PCI DSS) and more.
- The flexible, scalable architecture of QRadar is designed to support both large and small organizations with a variety of needs.

KEY BENEFITS

- Gain comprehensive, centralized visibility into disparate security data
- Rapidly detect threats by automating security intelligence
- Ability to detect slight changes in network, user or system behavior that may indicate unknown threats, such as malicious insiders, compromised credentials or fileless malware.
- Better manage compliance with pre-built content, rules and reports
- Easily scale with changing needs

KEY DELIVAREBLES

- Security comprehensive platform managed from a single interface.
- Intelligent analytics to a vast amount of security data providing security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions.
- Aggregated security events into single, prioritized alerts known as "offenses".
- Reports for compliance and audit