IBM **Security**

Gain Automated, Intelligent Analytics and Insights with IBM Security QRadar SIEM

Can you relate to these security challenges in your hybrid cloud environment?

Cybersecurity threats are becoming more advanced and more persistent which leads to many challenges for your Security Operations staff and organization.

Lack of visibility across your hybrid environment creates blind spots for attackers to take advantage and impedes threat investigation and response times

Too many **disconnected security tools** leads to an overwhelming amount of data and, often, not enough automation leading to alert fatigue

Outdated detection + skills shortage makes it difficult to determining which alerts are critical to the security and compliance of your organization

IBM Security QRadar SIEM addresses these challenges

Product Overview

IBM Security QRadar SIEM provides comprehensive visibility and insights into the most critical threats, enabling security teams to better detect and respond to threats across hybrid environments.

A leading security information and event management (SIEM) and security analytics platform, QRadar provides deep integrations with a broad range of Azure services, advanced rules, reports, searches, and dashboards so that teams can easily visualize and prioritize threats wherever and whenever they occur.

Product Benefits

- **Insights across environments.** Gain centralized visibility across Microsoft Azure and hybrid cloud environments via a single pane of glass
- **Real-time security analytics.** Correlate data across users, networks, and Microsoft Azure native services to gain deep insights into key threats including cloud misconfigurations, policy changes, and suspicious user activity
- **Prioritize threats.** Connect related events to ensure steams only receive a single alert for an incident to reduce response time
- **Comprehensive insights.** Leverage deep integrations with Microsoft Azure native services to ingest a broad spectrum of Microsoft Azure logs and flows into QRadar SIEM for rapid and accurate threat detection to identify cloud misconfigurations, policy changes, and suspicious user activity

IBM

Why QRadar?

- Fully integrated NDR
- 700+ integrations
- Automatic parsing and normalizing of logs
- 1,500 out-of-the-box use cases aligned to MITRE ATT&CK
- Intuitive, automatic query builder
- User behavior analytics
- Threat Intelligence & Support for STIX/TAXII
- Helps show evidence of compliance & declaration of conformity with applicable regulatory statues and internal audits for the environments that QRadar SIEM is monitoring.
- Breadth of services and partners

IBM Security QRadar on Azure

Customers with mission critical workloads can rest easy knowing the integration between IBM and Azure products allows IBM customers to increase the value of their IBM investments by combining those with the value from Microsoft. Whether this is IBM integration with Azure native services and storage solutions, or simply scalable, resilient, elastic provisioning of IBM software into the cloud, organizations get more agility in procurement via the integration of IBM Solutions with Azure Marketplace.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM **Security**