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

Challenges

Security analysts struggle with alert fatigue, disconnected tools, and lack of scalability

As cybersecurity threats become more advanced and persistent, ensuring compliance regulations are met is a critical part of your organization's security. Having too many tools comes with an overwhelming amount of data and, often, not enough automation leading to alert fatigue. When your security team is sifting through alerts 24/7, determining which alerts are critical to the security and compliance of your organization is near impossible. IBM Security QRadar Information and Event Management makes it easier to manage your security tools, data, policies, and team member, making it easier and more efficient to manage the security of your organization.

The IBM Solution

IBM Security QRadar SIEM

Gain comprehensive, centralized visibility to detect and investigate cybersecurity threats in both AWS Cloud and hybrid cloud workloads with IBM Security QRadar SIEM. QRadar SIEM correlates events across your environment so you can quickly uncover the root cause and scope of threats, helping accelerate investigation processes. Eliminate silos and chain-related events to unite users and networks into a single, prioritized offense to solve issues quickly. QRadar SIEM can quickly and securely scale as business needs change, paving the way for increased innovation with a broad range of Amazon Web Services (AWS) solutions. Together, AWS Cloud native services and QRadar SIEM provide full visibility and control across the threat landscape to keep workloads protected and running smoothly.

Benefits

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

Complete visibility

Leverage deep integrations with AWS native services to ingest a broad spectrum of AWS logs and network flows into QRadar SIEM.

Real-time security analytics

Automatically analyze and correlate activity across networks, users, endpoints, and cloud platforms to detect known and unknown threats.

Prioritized high-fidelity alerts

Use QRadar SIEM's ability to correlate security events across multiple data sources into a single offense to reduce response time.

Deployment

See real value with no fine tuning or complex customizations for day 1 detection out of the box (OOTB). QRadar SIEM has 1,500+ use cases OOTB, automatic parsing and normalizing of logs, an intuitive, automatic query builder, and a breadth of services and partners.

Contact IBM

IBM on AWS

For customers with mission critical workloads, they can rest easy knowing that AWS and IBM are working together to ensure highly available and secure workloads. Integration between AWS and IBM products and services allows IBM customers to increase the value of their IBM investments by combining those with the value from AWS. Whether this is IBM integration with AWS native artificial intelligence (AI) services, native 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 AWS Marketplace.

mohawk COLLEGE

Case Study: ReliaQuest

Background

As organizations accelerate their move to cloud to drive business innovation and customer success, ReliaQuest drives a unified approach to security for their clients, extending threat management capabilities across on-premise, hybrid and multi-cloud environments.

Solution

By helping IBM QRadar SIEM customer integrate and correlate data from AWS, ReliaQuest delivers industry-leading visibility and robust threat coverage at every phase of the attack lifecycle.

Benefits

ReliaQuest achieved flexibility in deployment models to meet their clients' needs, deep visibility into the most critical threats across AWS environments with a core set of repeatable use cases, and the ability to combine AWS security event logs with flows to correlate disparate events into a single offense.

Features

- **Fully integrated NDR**
- **700+ integrations**
- **1,500 OOTB detection capabilities aligned to MITRE ATT&CK**

Visit AWS Marketplace or IBM to purchase.

Get started with IBM solutions on AWS

Contact IBM

aws PARTNER Premier Tier Services

- L1 MSSP Services Competency
- Security Services Competency
- Security Software Competency