



Migration Benefits

- Continuous innovation to address evolving threats, including UBA, cloud security, Machine Learning and AI
- Real-time analysis on the most high-risk activity
- AI-powered capabilities to improve effectiveness and efficiency of analysis
- Real time scanning and analysis of the risks and vulnerabilities in the environment
- Flexible platform enables you to scale up a deployment quickly, and extend capabilities via the IBM Security App Exchange
- Built-in logic to enables fast rule creation



Legacy SIEM Migration

Break free from the limitations of an obsolete SIEM - adopt the leader in Gartner's Magic Quadrant

Challenges

With a continuously changing threat landscape and an evolving modern, mobile enterprise, it is critical that SIEM vendors continue to invest in their solutions to help their customers effectively defend against current and future threats. Not all SIEM providers have had the vision and ability to execute, as necessary to help arm their customers. As a result, their customers are struggling to build in new use cases, such as the ability to detect insider threats or uncover critical risks in cloud environments, and these organizations have been left exposed.

This leaves security management teams with a dilemma. They feel forced to choose between either continuing to invest in one-off development projects to protect their companies from new and evolving threats, or replacing their legacy SIEM with a different technology that is better suited to address the evolving threats and stay ahead of the game.

To make such a migration successful, companies need to partner with the right solution and the help of experienced experts. IBM QRadar can help you overcome the challenges resulting from obsolete SIEM solutions, and IBM Security's team of experts can help make the migration process seamless and pain-free.

Migration

IBM Security has helped dozens of companies migrate their legacy SIEM solutions to gain the benefits of QRadar. Their experience, skills, technology and resources will give you a smooth migration path.

The IBM QRadar team will partner with you through a three steps process:

1. Assess & Plan:

- The IBM QRadar team will engage and partner with you to launch the project and define requirements
- The output will include a migration plan that covers log sources, rules, other security data sets and analytics requirements

2. Deployment:

- The IBM QRadar team will begin the QRadar configuration
- Data collection will be transitioned to QRadar
- Tuning will help you isolate results to prioritized offenses so you can focus on what actually needs your attention

3. Completion:

- Rules and analytics will be then customized to address the unique needs within your environment
- The QRadar team will provide hands-on training and mentoring to enable your team to effectively support your new solution on an on-going basis

This approach will run at a pace that is right for individual customers, whether that is a big bang or phased parallel approach.

QRadar Solution

IBM QRadar is able to automatically analyze millions of events together with network data, vulnerability data and user information to identify high risk activities and provide security analysts with prioritized, meaningful and actionable alerts to potential security incidents. The use of the additional context sensitive data provides visibility into critical threats without creating unnecessary, distractions and noise. Using embedded AI and machine learning, threat data is automatically analyzed to quickly and accurately determine the scope and root cause of a potential incident. As a result, security analysts can accurately detect and respond to incidents early in the attack cycle to more effectively prevent data theft and system damage. In addition, QRadar provides advanced analytic support for security analysts to support their activities such as threat hunting and post offence investigation.

For more information

To learn more about this offering contact your IBM

representative or IBM Business Partner, or visit: ibm.com



© Copyright IBM Corporation 2018

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2018

IBM, the IBM logo, ibm.com, are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.



Please Recycle
