IBM QRadar Security Intelligence Platform

Actionable intelligence for enterprise security using the IBM QRadar Sense Analytics Engine

Highlights

- Use IBM QRadar Security Intelligence Platform, powered by the IBM Sense Analytics Engine™, to perform real-time event correlation and behavioral anomaly detection to detect advanced threats
- Integrate security information and event management (SIEM), anomaly detection, log management, vulnerability management, risk management, incident forensics and incident response into a single platform with unified visibility
- Leverage a highly scalable architecture to analyze log, flow, vulnerability, user and asset data
- Obtain a view of high priority security incidents among billions of data points
- Collaborate and take action using the IBM Security App Exchange and IBM X-Force® threat intelligence
- Help automate regulatory compliance with data collection, correlation and reporting

Organizations today are exposed to a greater volume and variety of attacks than in the past. Advanced attackers are clever and patient, leaving just a whisper of their presence. The IBM QRadar Security Intelligence Platform is an integrated family of products that can help detect threats that otherwise would be missed. It helps defend against attacks by applying sophisticated analytics to many types of data. In doing so, it identifies high-priority incidents that might otherwise get lost in the noise.

IBM® QRadar® Security Intelligence Platform integrates SIEM, log management, anomaly detection, vulnerability management, risk management, and incident forensics and response into a single, scalable, unified solution. Using an advanced Sense Analytics Engine, it analyzes security data and user behavior and provides superior threat detection, rapid time-to-value, greater ease-of-use and lower total cost of ownership.

In addition, the IBM QRadar Security Intelligence Platform integrates with IBM X-Force threat intelligence information to provide a proactive approach to security. This is complemented by the ability to collaborate with IBM, business partners, and your peers, and download IBM and third-party developed extensions from the IBM Security App Exchange. These extensions deliver enhanced visualizations, deep integrations and incident response technologies to address security threats.

The IBM QRadar Security Intelligence Platform supports a number of use cases including:

- Advanced threat detection
- Insider threat identification
- Risk and vulnerability management
- Forensics investigation
- Incident response
- Compliance reporting
- Securing the Cloud

Integrated IBM QRadar Security Intelligence Platform

Advanced threat detection: IBM QRadar aggregates security logs and network flows, and uses its Sense Analytics Engine to help identify advanced threats. Using behavioral-based analytics, it detects anomalies and suspicious activities, performs event aggregation and correlation, assesses severity, and provides security analysts with a manageable list of prioritized offenses requiring investigation.

Insider threat identification: IBM Sense Analytics performs automated asset, service, and user discovery and profiling. After profiling user behavior and determining a baseline, QRadar detects deviations from normal and generates alerts for items to be investigated. It then supports quick and easy forensics analysis and incident response for rapid insider threat resolution.

Risk and vulnerability management: QRadar senses the addition of new network assets, scans them to detect vulnerabilities, identifies configuration errors and out-of-policy conditions, and generates network topology views that identify potential attack paths. It then prioritizes the vulnerabilities and risks discovered to help organizations develop corrective action plans.

Forensics investigation: QRadar can quickly and easily recover the network packets associated with a security offense, and reconstructs the step-by-step actions of an attacker to enable rapid problem investigation and remediation, along with prevention of future recurrences.

Incident response: IBM QRadar Security Intelligence senses and discovers advanced threats and initiates the incident response process. Integration with Resilient Systems enables the automation of response processes, and allows the generation of a playbook that makes security alerts quickly actionable, provides valuable intelligence and incident context, and helps security teams rapidly take action.

Compliance reporting: QRadar automatically senses and discovers log sources, network devices, and configurations. It analyzes data

collected to help identify conditions that are non-compliant with internal policies and regulations. It includes customizable reports for best practices, internal policies and regulations including COBIT, SOX, GLBA, NERC, FISMA, PCI, HIPAA, UK GCSx and more.

Securing the cloud: QRadar SIEM can monitor and detect abnormal use of a wide range of cloud applications such as Microsoft Office 365, Amazon Web Services CloudTrail, Salesforce.com, Google Cloud Identity & Access Management, and more. QRadar can also help secure infrastructures whether they are deployed on premises, in the cloud, or based on a hybrid model.

IBM QRadar Security Intelligence Platform

The QRadar Security Intelligence Platform provides a unified architecture for storing, correlating, querying and reporting on log, flow, vulnerability, and user and asset data. It combines sophisticated analytics with out-of-the-box rules, reports and dashboards. While it is powerful and scalable for Fortune 500 corporations and major government agencies, it is also intuitive and flexible enough for small and midsize organizations. Users benefit from faster time-to-value, potentially lower cost of ownership, greater agility, and enhanced protection against security and compliance risks.

Using advanced Sense Analytics, QRadar can analyze many types of data and detect threats missed by other solutions and help provide network visibility that others cannot. In addition, clients benefit from the ability to collaborate with IBM, Business Partners, and their peers using the IBM Security App Exchange, where they can download extensions to QRadar to obtain additional capabilities and value.

With a common application platform, database and user interface, this platform delivers massive log management scalability without compromising the real-time intelligence of SIEM and network behavior analytics. It provides a common solution for all searching, correlation, anomaly detection and reporting functions. A single, intuitive user interface provides seamless access to log management, flow analysis, incident management, configuration management, risk and vulnerability management, incident forensics and response, user behavior analysis, and reporting functions. And it can be expanded easily using low-cost QRadar Data Nodes for increased storage and search performance.

The QRadar Security Intelligence Platform is simple to deploy and manage, offering extensive out-of-the-box integration modules and security intelligence content. By automating many asset discovery, data normalization and tuning functions, while providing out-of-the-box rules and reports, the solution is designed to reduce the complexity that often cripples other products.

Why IBM?

IBM operates the world's broadest security research, development and delivery organization. This comprises 10 security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM solutions empower organizations to reduce their security vulnerabilities and focus more on the success of their strategic initiatives. These products build on the threat intelligence expertise of the IBM X-Force® research and development team to provide a preemptive approach to security. As a trusted partner in security, IBM delivers the solutions to keep the entire enterprise infrastructure, including the cloud, protected from the latest security risks.

For more information

To learn more about the IBM QRadar Security Intelligence Platform, contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

IBM Corporation

Security Systems

Route 100

Somers, NY 10589

Produced in the United States of America

June 2016

Please Recycle