IBM QRadar Security Intelligence Platform

Providing actionable intelligence for enterprise security and compliance

Highlights

- Integrate security information and event management (SIEM), anomaly detection, log management, vulnerability management, risk management, and incident forensics into a single, unified solution
- Leverage a single architecture to analyze log, flow, vulnerability, user and asset data
- Use real-time correlation and behavioral anomaly detection to identify advanced threats
- Identify high-priority incidents among billions of data points
- Gain 360-degree visibility into network, application and attacker activity
- Automate regulatory compliance with collection, correlation and reporting

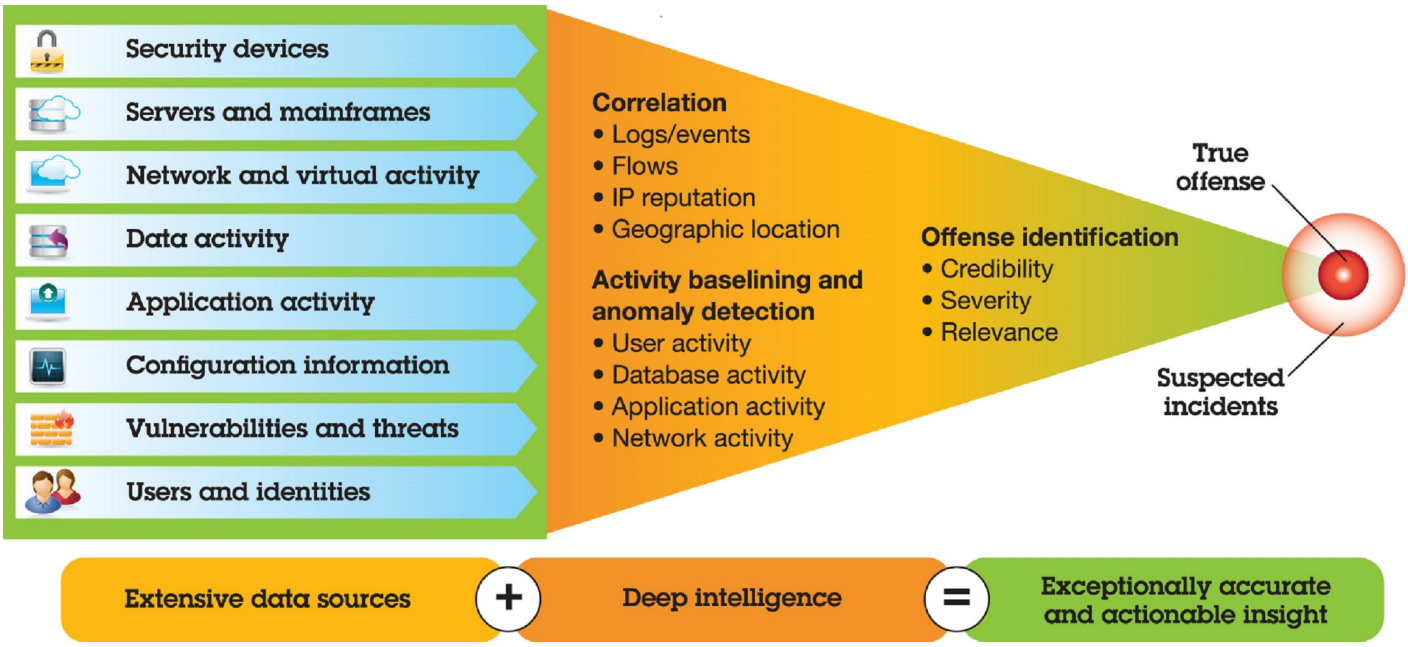
IBM® QRadar® Security Intelligence Platform integrates SIEM, log management, anomaly detection, vulnerability management, risk management and incident forensics into a unified solution. By using intelligence, integration and automation to provide 360-degree security insight, this solution delivers superior threat detection, greater ease of use and potentially lower total cost of ownership.

The QRadar Security Intelligence Platform uses intelligence, integration and automation to deliver security and compliance benefits that are invaluable on today's smarter planet, where instrumented, interconnected and intelligent businesses collect, process, use and store more information than ever before.

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 QRadar Security Intelligence Platform is an integrated family of products that can help detect threats that otherwise would be missed. It helps detect and defend against threats by applying sophisticated analytics to more types of data. In doing so, it helps identify high-priority incidents that might otherwise get lost in the noise.

The IBM QRadar Security Intelligence Platform can help solve a number of business problems including:

- Consolidating data silos into one integrated solution
- Identifying insider theft and fraud
- Managing vulnerabilities, configurations, compliance and risks
- Conducting forensic investigations of incidents and offenses
- Addressing regulatory mandates



Delivering intelligence, integration and automation

The QRadar Security Intelligence Platform uses intelligence, integration and automation designed to deliver security and compliance benefits that are invaluable on today’s smarter planet, where instrumented, interconnected and intelligent businesses collect, process, use and store more information than ever before.

Consolidate data silos

Although a wealth of information exists in organizations’ log, network flow and business process data, this information is often held in silos and ignored or underutilized. QRadar converges network, security and operations views into a unified and flexible solution. It breaks down the walls between silos by correlating logs with network flows and a multitude of other data, presenting virtually all relevant information on a single screen. This helps enable superior threat detection and a much richer view of enterprise activity.

Detect insider fraud

Some of the gravest threats to an organization come from the inside, yet organizations often lack the intelligence needed to detect malicious insiders or outside parties that have compromised user accounts. By combining user and application monitoring with application-layer network visibility, organizations can better detect meaningful deviations from normal activity, helping to stop an attack before it completes.

Predict and remediate risks and vulnerabilities

Security, network and infrastructure teams strive to manage risk by identifying vulnerabilities and prioritizing remediation before a breach occurs. The QRadar Security Intelligence Platform integrates risk, configuration and vulnerability management with SIEM capabilities, including correlation and network flow analytics, to help provide better insight into critical vulnerabilities. As a result, organizations can remediate risks more effectively and efficiently.

Conduct Forensics Analysis

QRadar integrated incident forensics helps IT security teams reduce the time spent investigating security incidents, and eliminates the need for specialized training. It expands security

data searches to include full packet captures and digitally stored text, voice, and image documents. It helps present clarity around what happened when, who was involved, and what data was accessed or transferred in a security incident. As a result, it helps remediate a network breach and can help prevent it from succeeding again.

Address regulatory compliance mandates

Many organizations wrestle with passing compliance audits while having to perform data collection, monitoring and reporting with increasingly limited resources. To automate and simplify compliance tasks, QRadar provides collection, correlation and reporting on compliance-related activity, backed by numerous out-of-the-box report templates.

Leveraging easier-to-use security analytics

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

Intelligence

By analyzing more types of data and using more analytics techniques, QRadar can often detect threats missed by other solutions and help provide network visibility that others cannot.

Integration

With a common application platform, database and user interface, this platform delivers massive log management scale 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 all log management, flow analysis, incident management, configuration management, risk and vulnerability management, incident forensics, dashboard and reporting functions.

Automation

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, develop-ment 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

Software Group

Route 100

Somers, NY 10589

Produced in the United States of America

September 2014