IBM QRadar Security Intelligence
April 2013
Today’s Challenges

Detecting threats
- Arm yourself with comprehensive security intelligence

Consolidating data silos
- Collect, correlate and report on data in one integrated solution

Detecting insider fraud
- Next-generation SIEM with identity correlation

Better predicting risks to your business
- Full life cycle of compliance and risk management for network and security infrastructures

Addressing regulation mandates
- Automated data collection and configuration audits
Organizations Need an Intelligent View into Their Security Posture

- Basic: Organizations employ perimeter protection, which regulates access and feeds manual reporting.
- Reactive: Security is reactive, focusing on immediate response.
- Automated: Security processes are automated, reducing manual work.
- Proficient: Security is layered into the IT fabric and business operations.
- Optimized: Organizations use predictive and automated security analytics to drive toward security intelligence.
What is Security Intelligence?

**Security Intelligence**

---*noun*

1. the real-time collection, normalization, and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation
Helping Organizations Progress in Their Security Maturity

<table>
<thead>
<tr>
<th>Security Intelligence</th>
<th>Security Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced threat detection</td>
<td>Advanced threat detection</td>
</tr>
<tr>
<td>Network anomaly detection</td>
<td>Network anomaly detection</td>
</tr>
<tr>
<td>Predictive risk management</td>
<td>Predictive risk management</td>
</tr>
</tbody>
</table>

| People | Data | Applications | Infrastructure |
|--------|------|--------------|----------------|----------------|
| People | People | People | People | People |
| Optimized | Optimized | Optimized | Optimized | Optimized |
| Proficient | Proficient | Proficient | Proficient | Proficient |
| Basic | Basic | Basic | Basic | Basic |

People
- Role based analytics
- Identity governance
- Privileged user controls

Data
- Data flow analytics
- Data governance

Applications
- Secure app engineering processes
- Fraud detection

Infrastructure
- Advanced network monitoring
- Forensics / data mining
- Securing systems

Security Intelligence

Proficient
- User provisioning
- Access mgmt
- Strong authentication
- Access monitoring
- Data loss prevention
- Application firewall
- Source code scanning
- Virtualization security
- Asset mgmt
- Endpoint / network security management
- Real-time event correlation
- Network forensics

Basic
- Centralized directory
- Encryption
- Access control
- Application scanning
- Perimeter security
- Anti-virus
- Log management
- Compliance reporting

© 2013 IBM Corporation
## Solving Customer Challenges

<table>
<thead>
<tr>
<th>Major Electric Utility</th>
<th>Detecting threats</th>
<th>• Discovered 500 hosts with “Here You Have” virus, which other solutions missed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortune 5 Energy Company</td>
<td>Consolidating data silos</td>
<td>• 2 Billion logs and events per day reduced to 25 high priority offenses</td>
</tr>
<tr>
<td>Branded Apparel Maker</td>
<td>Detecting insider fraud</td>
<td>• Trusted insider stealing and destroying key data</td>
</tr>
<tr>
<td>$100B Diversified Corporation</td>
<td>Predicting risks against your business</td>
<td>• Automating the policy monitoring and evaluation process for configuration change in the infrastructure</td>
</tr>
<tr>
<td>Industrial Distributor</td>
<td>Addressing regulatory mandates</td>
<td>• Real-time extensive monitoring of network activity, in addition to PCI mandates</td>
</tr>
</tbody>
</table>
Context and Correlation Drive Deepest Insight

Event Correlation
- Logs
- Flows
- IP Reputation
- Geo Location

Activity Baselining & Anomaly Detection
- User Activity
- Database Activity
- Application Activity
- Network Activity

Offense Identification
- Credibility
- Severity
- Relevance

True Offense

Suspected Incidents

Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight
# Security Intelligence Product Offerings

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRadar Log Manager</td>
<td>QRadar Log Manager collects, archives, analyzes and reports on events across a distributed network. It helps address regulatory and policy compliance, while reducing manual compliance and reporting activities.</td>
</tr>
<tr>
<td>QRadar SIEM</td>
<td>QRadar SIEM provides extensive visibility and actionable insight to help protect networks and IT assets from a wide range of advanced threats. It helps detect and remediate breaches faster, address compliance, and improve the efficiency of security operations.</td>
</tr>
<tr>
<td>QRadar QFlow</td>
<td>QRadar QFlow complements QRadar SIEM by providing deep content visibility. It gathers Layer 7 flow data via deep packet inspection, enabling advanced threat detection through analysis of packet content.</td>
</tr>
<tr>
<td>QRadar QFlow</td>
<td>QRadar VFlow provides content visibility into virtual network traffic, delivering comparable functionality to QRadar QFlow but for virtual environments.</td>
</tr>
<tr>
<td>QRadar Risk Manager</td>
<td>QRadar Risk Manager identifies and reduces security risks through device configuration monitoring, vulnerability prioritization, and threat simulation and visualization. It can help prevent many security breaches while improving operational efficiency and compliance.</td>
</tr>
</tbody>
</table>
QRadar: Applying Intelligence, Integration, Automation

- Proactive threat management
- Identifies critical anomalies
- Rapid, extensive impact analysis

- Bridges silos
- Highly scalable
- Flexible & adaptable

- Easy deployment
- Rapid time to value
- Operational efficiency
Fully Integrated Security Intelligence

Log Management
- Turn-key log management and reporting
- SME to Enterprise
- Upgradeable to enterprise SIEM

SIEM
- Log, flow, vulnerability & identity correlation
- Sophisticated asset profiling
- Offense management and workflow

Network Activity & Anomaly Detection
- Network analytics
- Behavioral anomaly detection
- Fully integrated in SIEM

Network and Application Visibility
- Layer 7 application monitoring
- Content capture for deep insight & forensics
- Physical and virtual environments

Configuration & Vulnerability Management
- Network security configuration monitoring
- Vulnerability prioritization
- Predictive threat modeling & simulation