Q1Labs.com

Security Intelligence Platform

Joseph Skocich,
WW Sales Integration Executive
Q1 Labs, an IBM Company
November 2012

jskocich@us.ibm.com

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

The Security Intelligence Leader

Who we are:

- Innovative Security Intelligence software company
- One of the largest and most successful SIEM vendors
- Leader in Gartner 2012, 2011, 2010, 2009 Magic Quadrant

Award-winning solutions:

- Family of next-generation Log Management, SIEM, Risk Management, Security Intelligence solutions

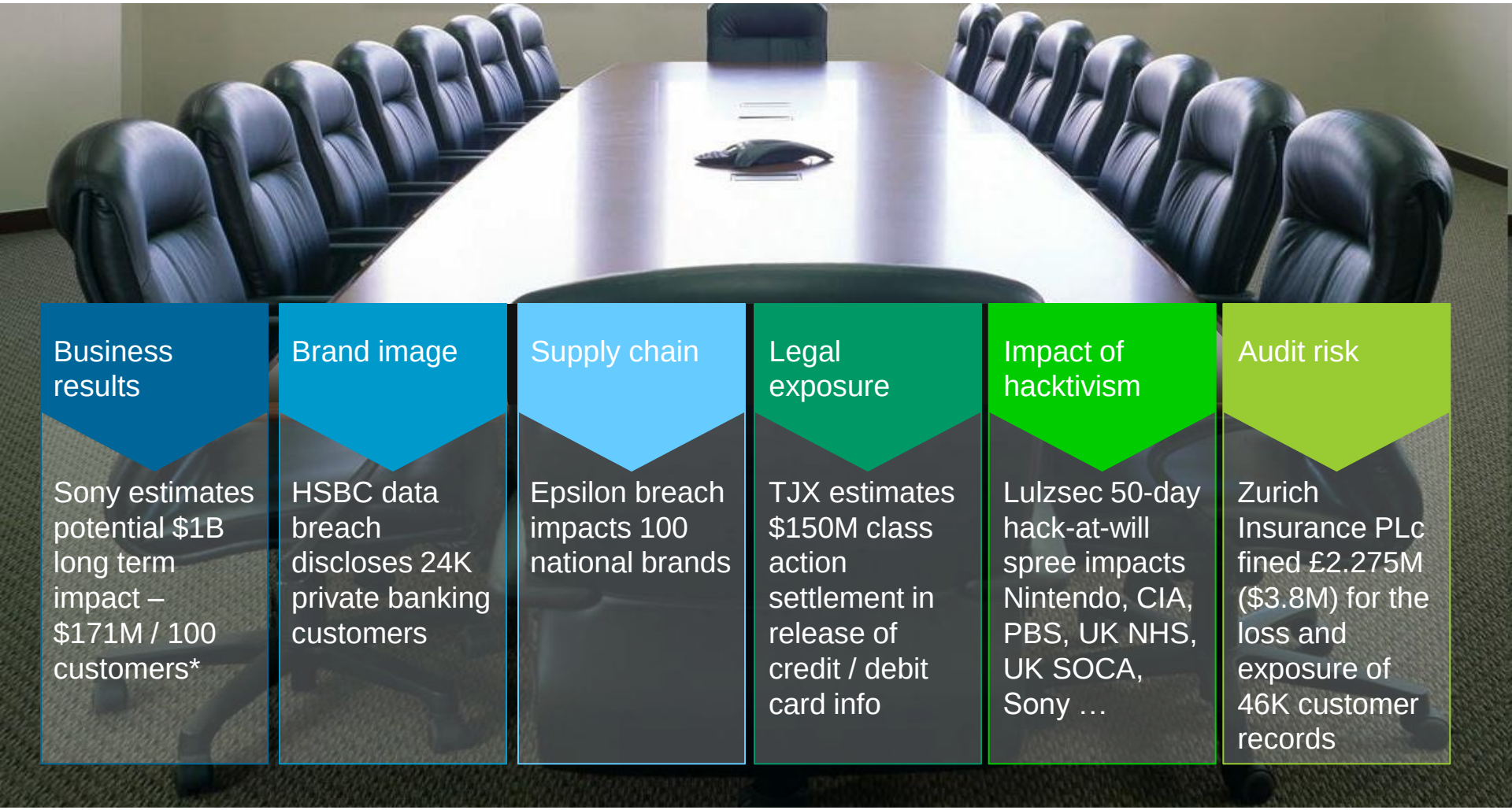
Proven and growing rapidly:

- Thousands of customers worldwide
- Five-year average annual revenue growth of 70%+

Now part of IBM Security Systems:

- Unmatched security expertise and breadth of integrated capabilities

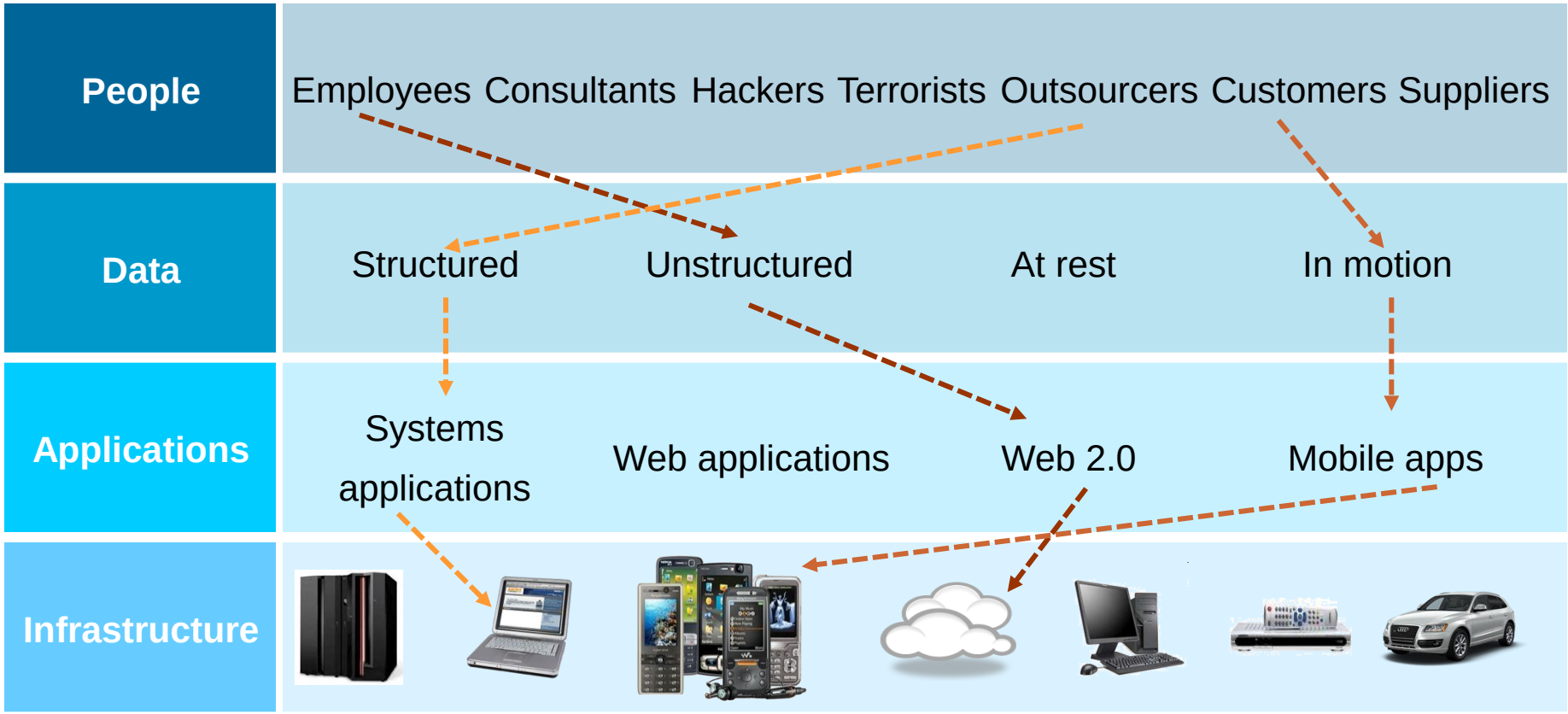
IT Security is a board room discussion



Business results	Brand image	Supply chain	Legal exposure	Impact of hacktivism	Audit risk
Sony estimates potential $1B long term impact – $171M / 100 customers*	HSBC data breach discloses 24K private banking customers	Epsilon breach impacts 100 national brands	TJX estimates $150M class action settlement in release of credit / debit card info	Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony …	Zurich Insurance PLc fined £2.275M ($3.8M) for the loss and exposure of 46K customer records

*Sources for all breaches shown in speaker notes

Solving a security issue is a complex, four-dimensional puzzle



It is no longer enough to protect the perimeter – siloed point products will not secure the enterprise

Q1 Labs: Solving Customer Challenges with Total Security Intelligence

Detecting threats others miss

- Discovered 500 hosts with “Here You Have” virus, which all other security products missed

Consolidating data silos

- 2 Billion logs and events per day reduced to 25 high priority offenses

Detecting insider fraud

- Trusted insider stealing and destroying key data

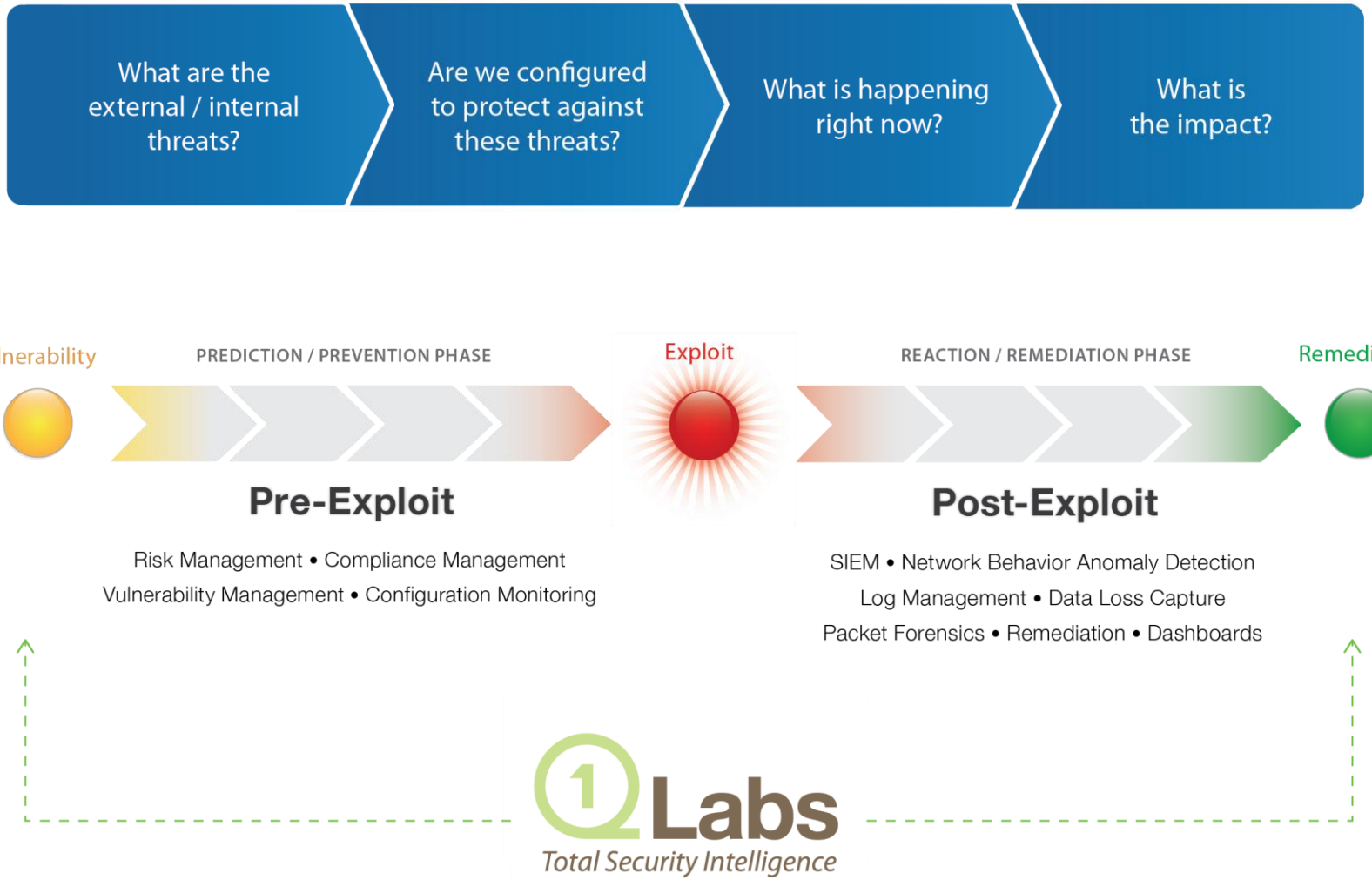
Predicting risks against your business

- Automating the policy monitoring and evaluation process for config. change in the infrastructure

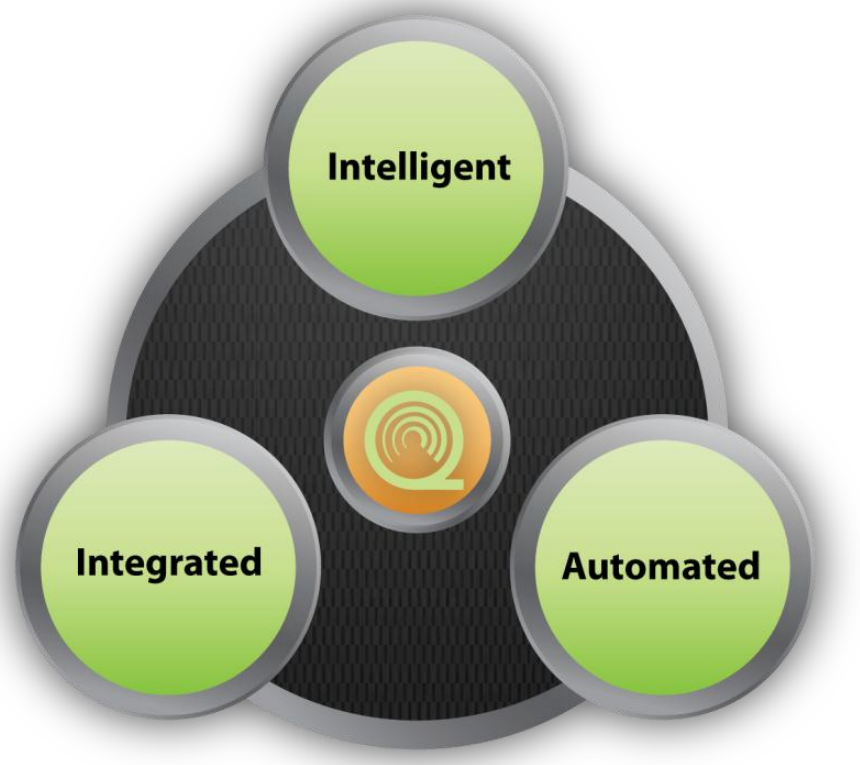
Exceeding regulation mandates

- Real-time monitoring of all network activity, in addition to PCI mandates

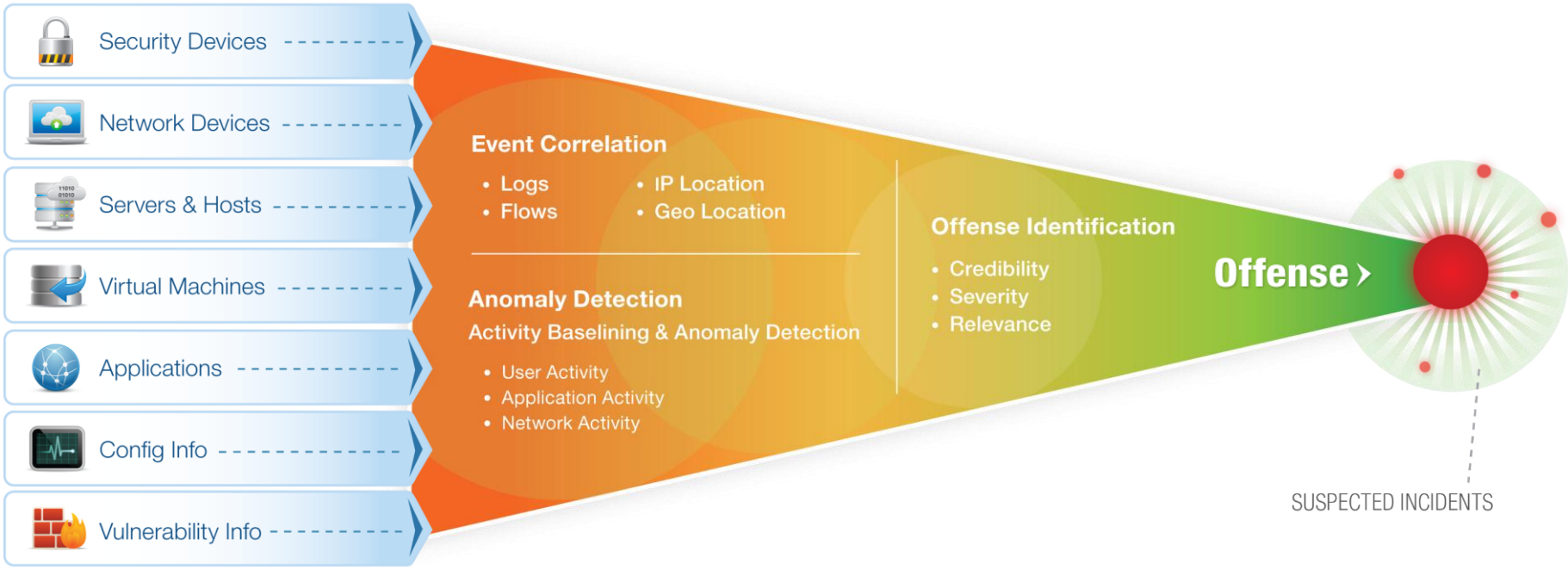
Solutions for the Full Compliance and Security Intelligence Timeline



QRadar: The Most Intelligent, Integrated, Automated Security Intelligence Platform



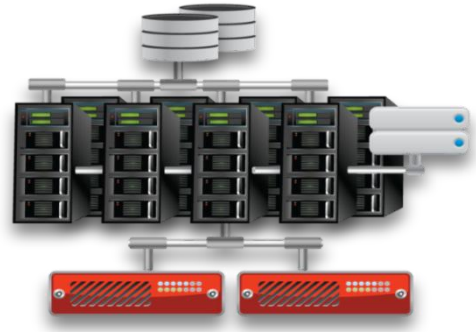
Intelligent:
Context & Correlation Drive Deepest Insight



Most Sources + Most Intelligence = Most Accurate & Actionable Insight

Integrated:
Unified Platform for Scale & Ease of Use

Bolted Together Solution



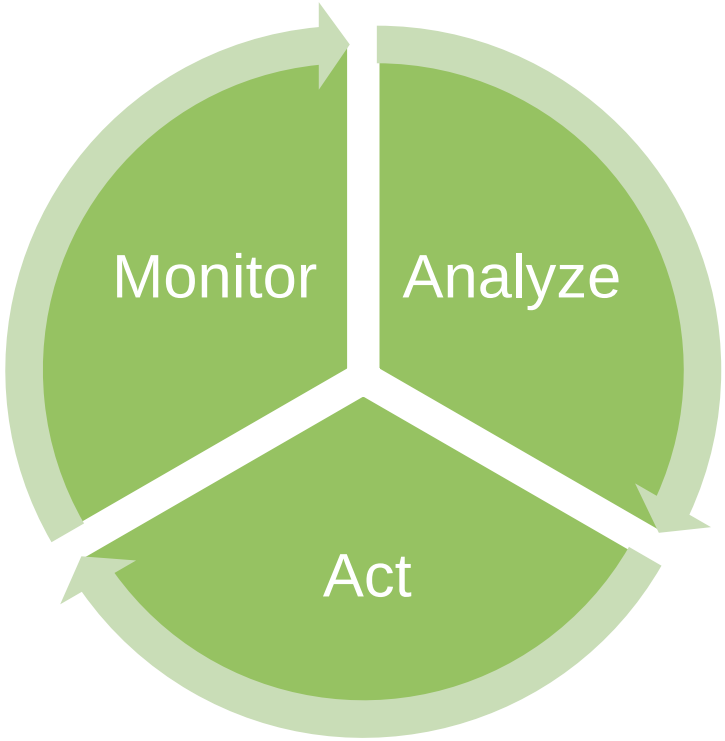
- Scale problems
- Non-integrated reporting & searching
- No local decisions
- Multi-product administration
- Duplicate log repositories
  - ***Operational bottlenecks***

QRadar Integrated Solution

- Highly scalable
- Common reporting & searching
- Distributed correlation
- Unified administration
- Logs stored once
  - ***Total visibility***

Automated:
No need for additional staff

- Auto-discovery of log sources, applications and assets
- Asset auto-grouping
- Centralized log mgmt
- Automated configuration audits



- Asset-based prioritization
- Auto-update of threats
- Auto-response
- Directed remediation

- Auto-tuning
- Auto-detect threats
- Thousands of pre-defined rules and role based reports
- Easy-to-use event filtering
- Advanced security analytics

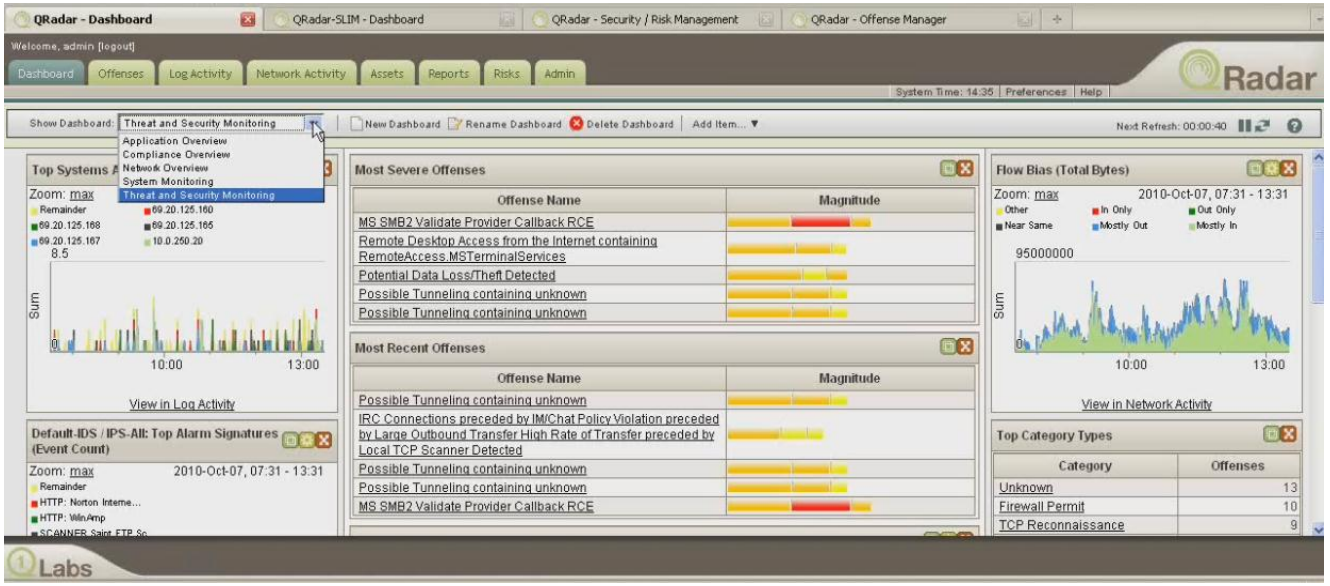
Fully Integrated Security Intelligence

Log Management	Radar Log Manager  Radar Log Manager Free Edition 	• Turnkey log management • SME to Enterprise • Upgradeable to enterprise SIEM
SIEM	Radar SIEM 	• Integrated log, threat, risk & compliance mgmt. • Sophisticated event analytics • Asset profiling and flow analytics • Offense management and workflow
Risk Management	Radar Risk Manager 	• Predictive threat modeling & simulation • Scalable configuration monitoring and audit • Advanced threat visualization and impact analysis
Network Activity & Anomaly Detection	Radar SIEM  Radar QFlow 	• Network analytics • Behavior and anomaly detection • Fully integrated with SIEM
Network and Application Visibility	Radar QFlow  Radar VFlow 	• Layer 7 application monitoring • Content capture • Physical and virtual environments

Fully Integrated Security Intelligence

- Log Management
- SIEM
- Risk Management
- Network Activity & Anomaly Detection
- Network and Application Visibility

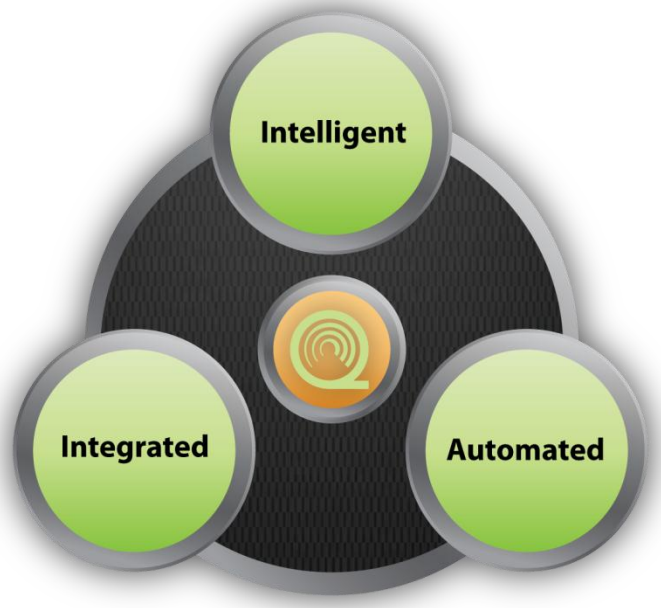
One Console Security



Built on a Single Data Architecture

QRadar: The Most Intelligent, Integrated, Automated Security Intelligence Platform

- Proactive threat management
- Identifies most critical anomalies
- Rapid, complete impact analysis



- Eliminates silos
- Highly scalable
- Flexible, future-proof

- Easy deployment
- Rapid time to value
- Operational efficiency

Summary

1. Most intelligent, integrated and automated solution
2. Most sophisticated threat analytics and compliance automation
3. Rapid time to value, with low staffing requirements
4. Easily scales as deployments and security data grow
5. Established market leadership with excellent support
6. Easy to do business with, backed by best channel relationships
7. IBM's unmatched security expertise and breadth of integrated capabilities

What to do next?

- Read our blog:

  http://blog.q1labs.com/

- Follow us on Twitter:

  @q1labs @ibmsecurity

- Watch our recent webcasts:

  http://q1labs.com/resource-center/media-center.aspx

- Download the 2012 Gartner SIEM Report

  http://q1labs.com/resource-center/analyst-reports/details.aspx?id=150

Thank You!

Q1 Labs, an IBM Company
jskocich@us.ibm.com
Q1Labs.com