Security Intelligence.
Think Integrated.

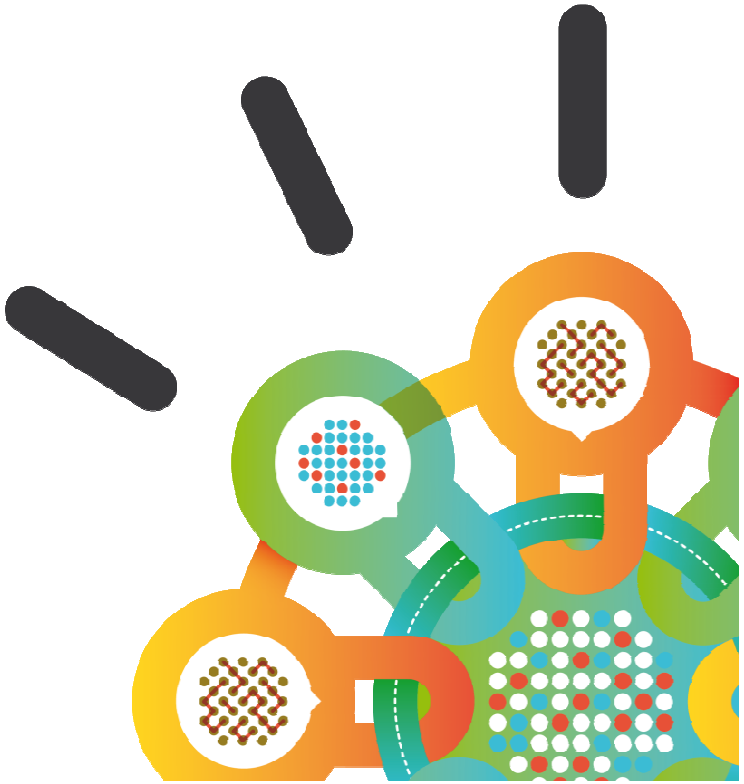
Stepping-up to the IT Network Security Challenge

IBM QRadar Security Intelligence

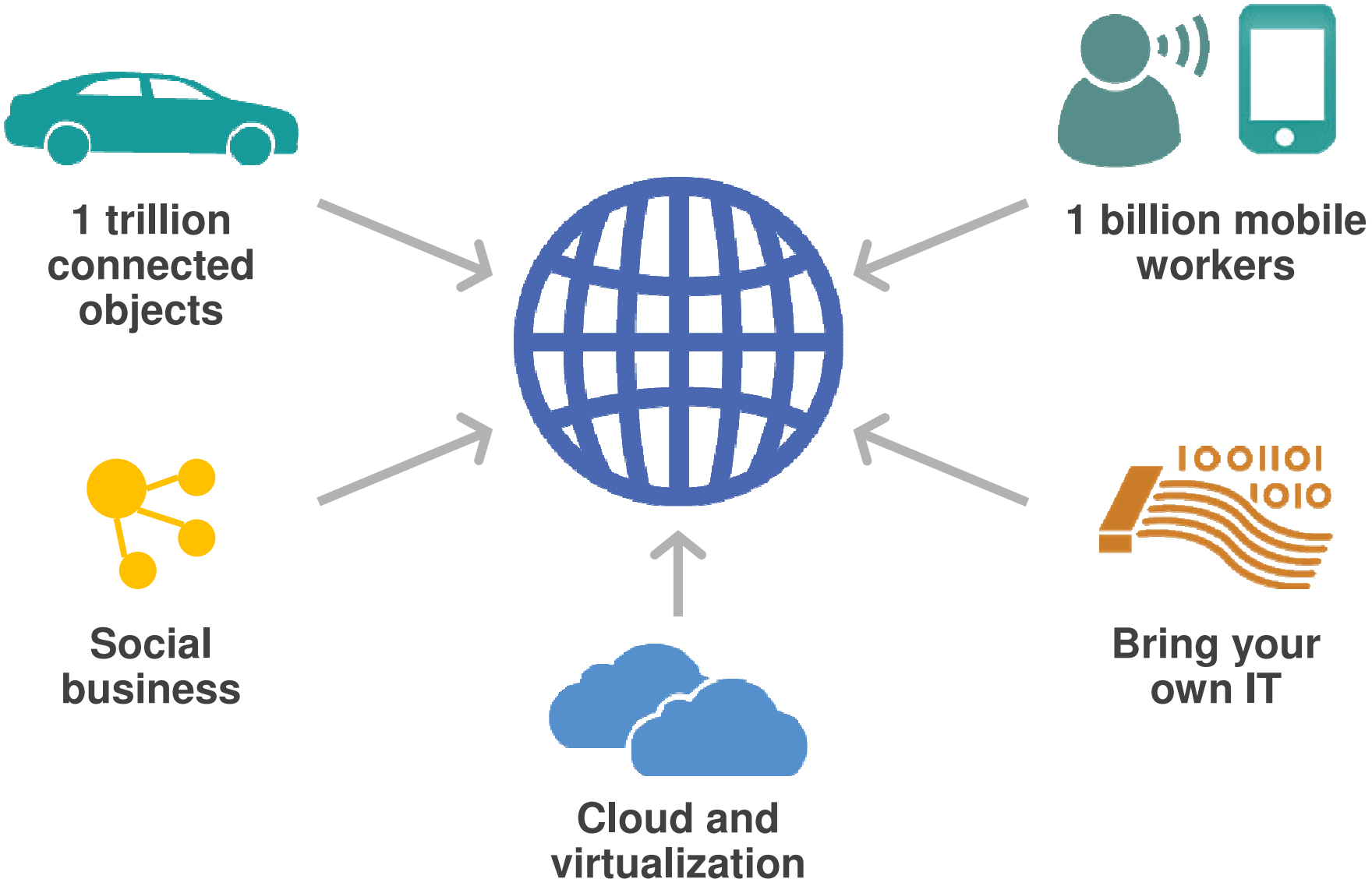
Rob Whitters

QRadar SIEM Technical Specialist

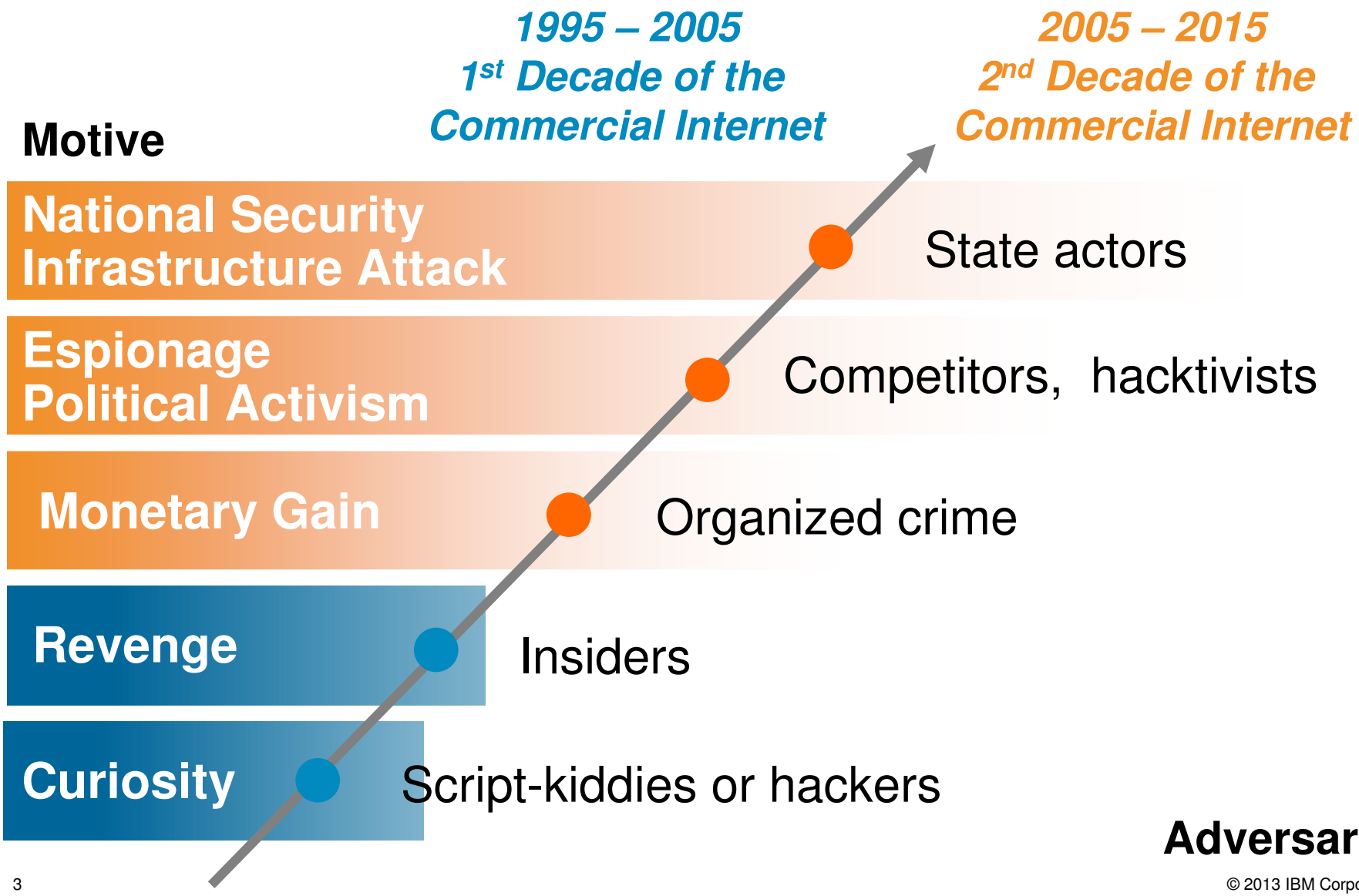
Infosec 2013



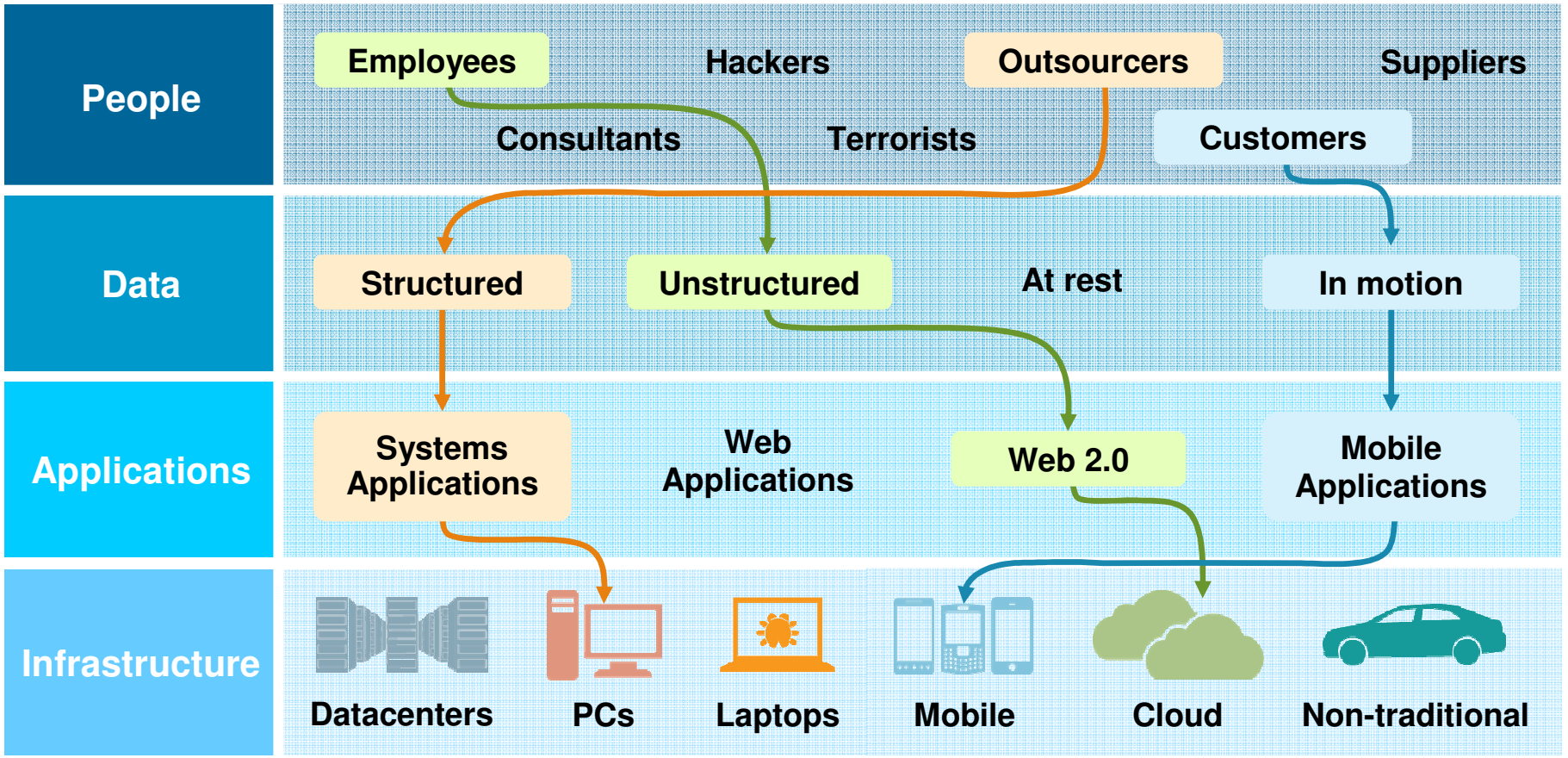
Innovative technology changes everything



Motivations and sophistication are rapidly evolving



Security challenges are a complex, four-dimensional puzzle …



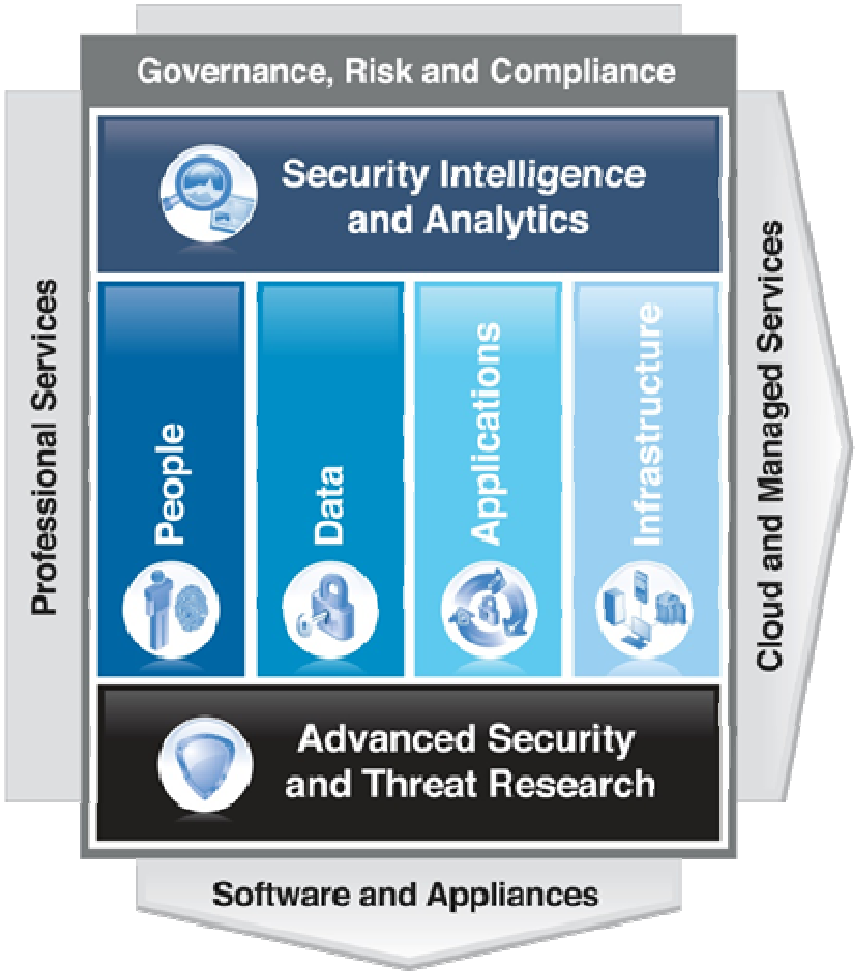
… that requires a new approach

IBM delivers solutions across a security framework

Intelligence

Integration

Expertise



Security Intelligence Defined

What is Security Intelligence?

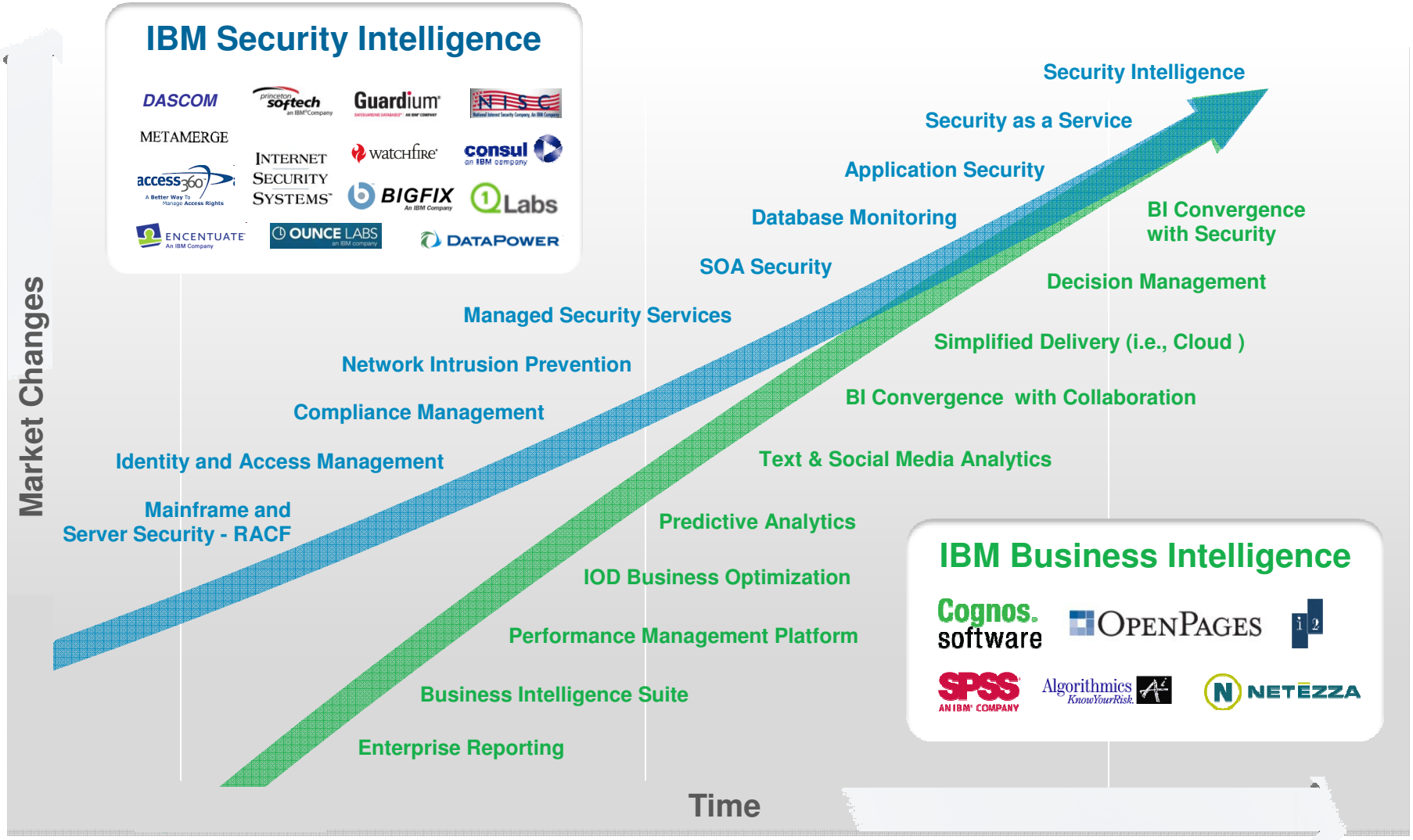
Security Intelligence

--noun

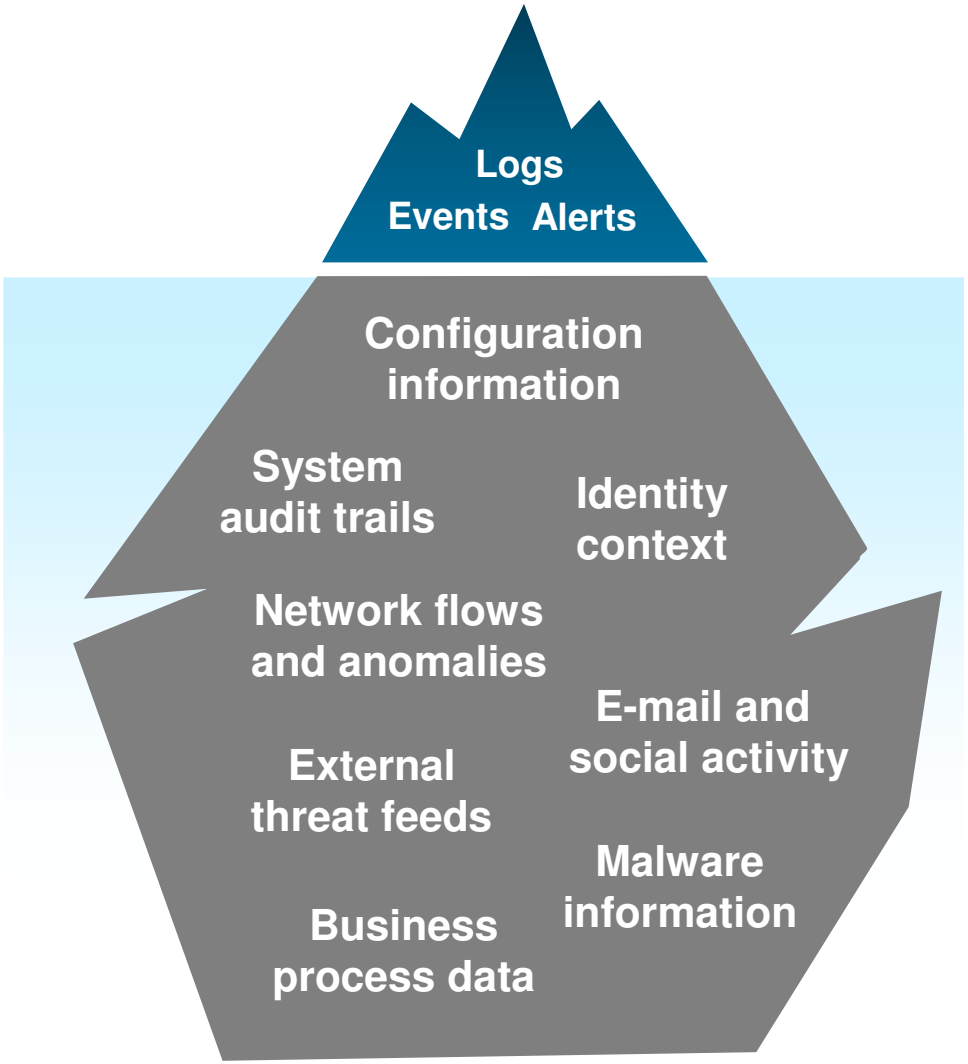
1. the real-time collection, normalization and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

Security Intelligence & Business Intelligence offer insightful parallels



Evolving along with changing threat landscape



Then: Collection

- Log collection
- Signature-based detection

Now: Intelligence

- Real-time monitoring
- Context-aware anomaly detection
- Automated correlation and analytics

QRadar Security Intelligence Platform

A quick introduction

QRadar:

- Foundational acquisition for IBM Security Systems Division completed October, 2011
- Nexus for integration of IBM security software offerings

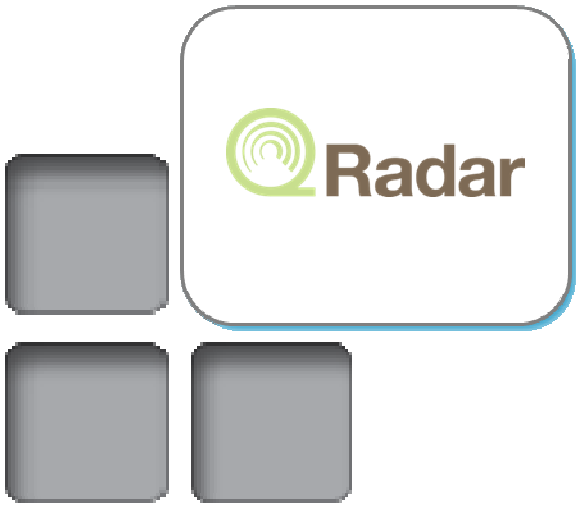
Award winning solutions:

- Family of next-generation Log Management, SIEM, Risk Management, security intelligence solutions
- Common database, common user interface
- Leader in Gartner SIEM Magic Quadrants 2009 - 2012

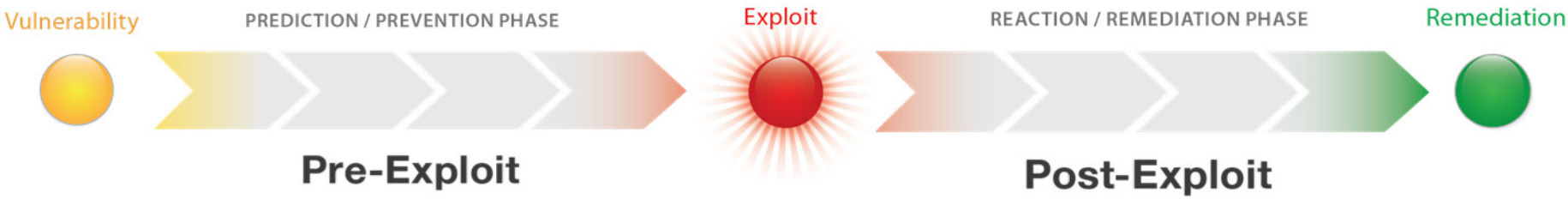
Executing, growing rapidly:

- +3000 customers worldwide spanning North America, EMEA and Asia Pacific
- Integration with IBM X-Force including information about software vulnerabilities, malware, spam, phishing, web-based threats, and general cyber criminal activity

Gartner
Magic Quadrant



Solutions for the full Security Intelligence timeline



Pre-Exploit

Prediction & Prevention

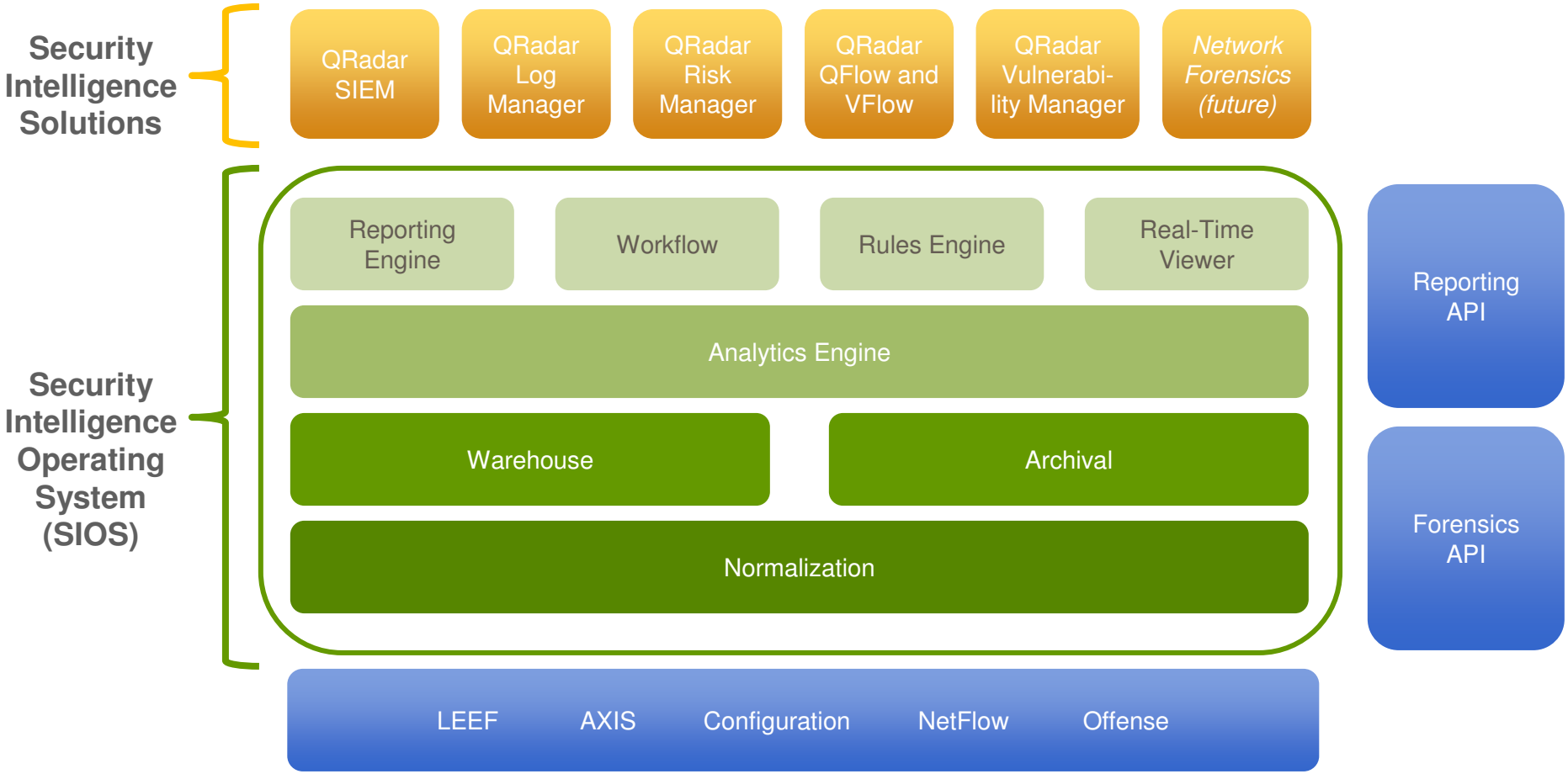
Risk Management. Vulnerability Management.
Configuration and Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management.
Reporting and Scorecards.

Post-Exploit

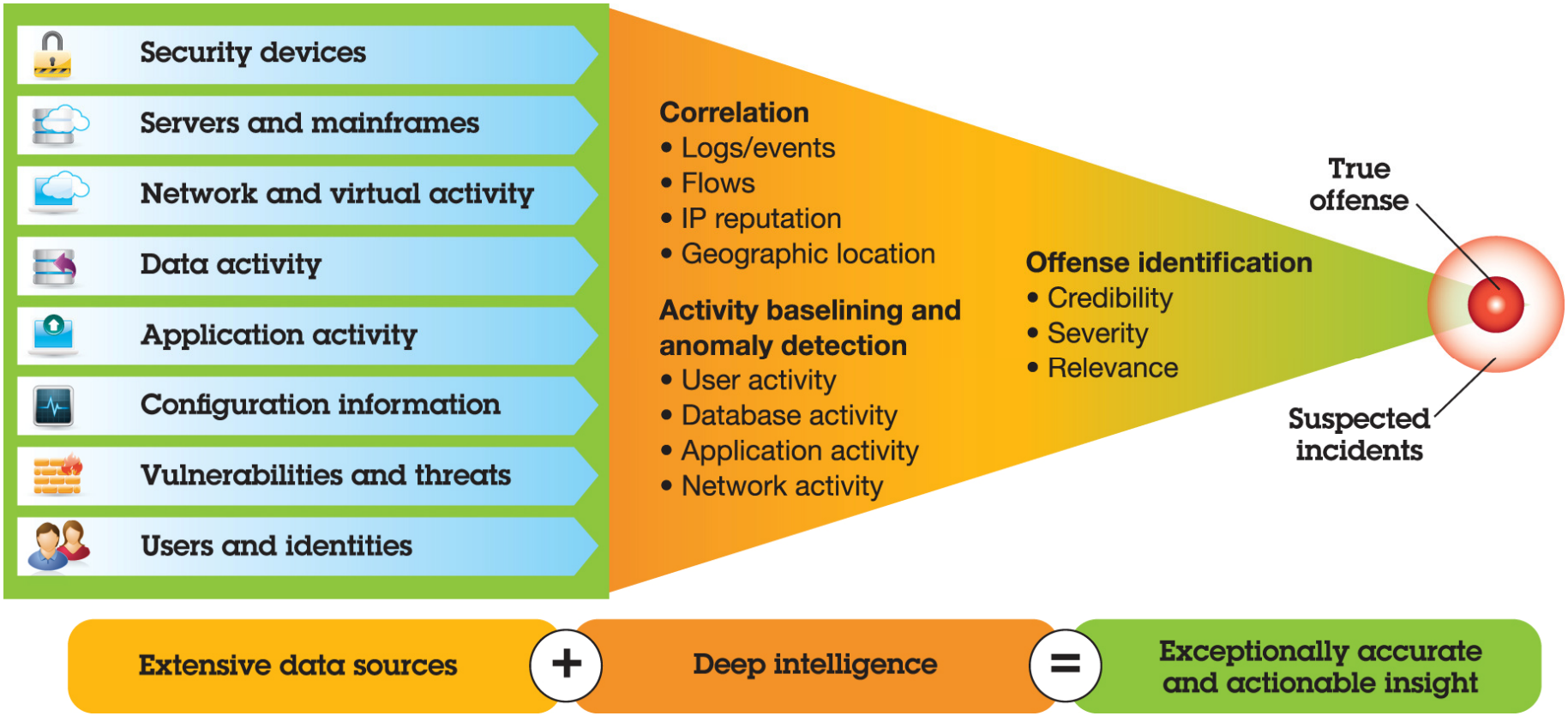
Reaction & Remediation

Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Leak Prevention.
Security Information and Event Management.
Log Management. Incident Response.

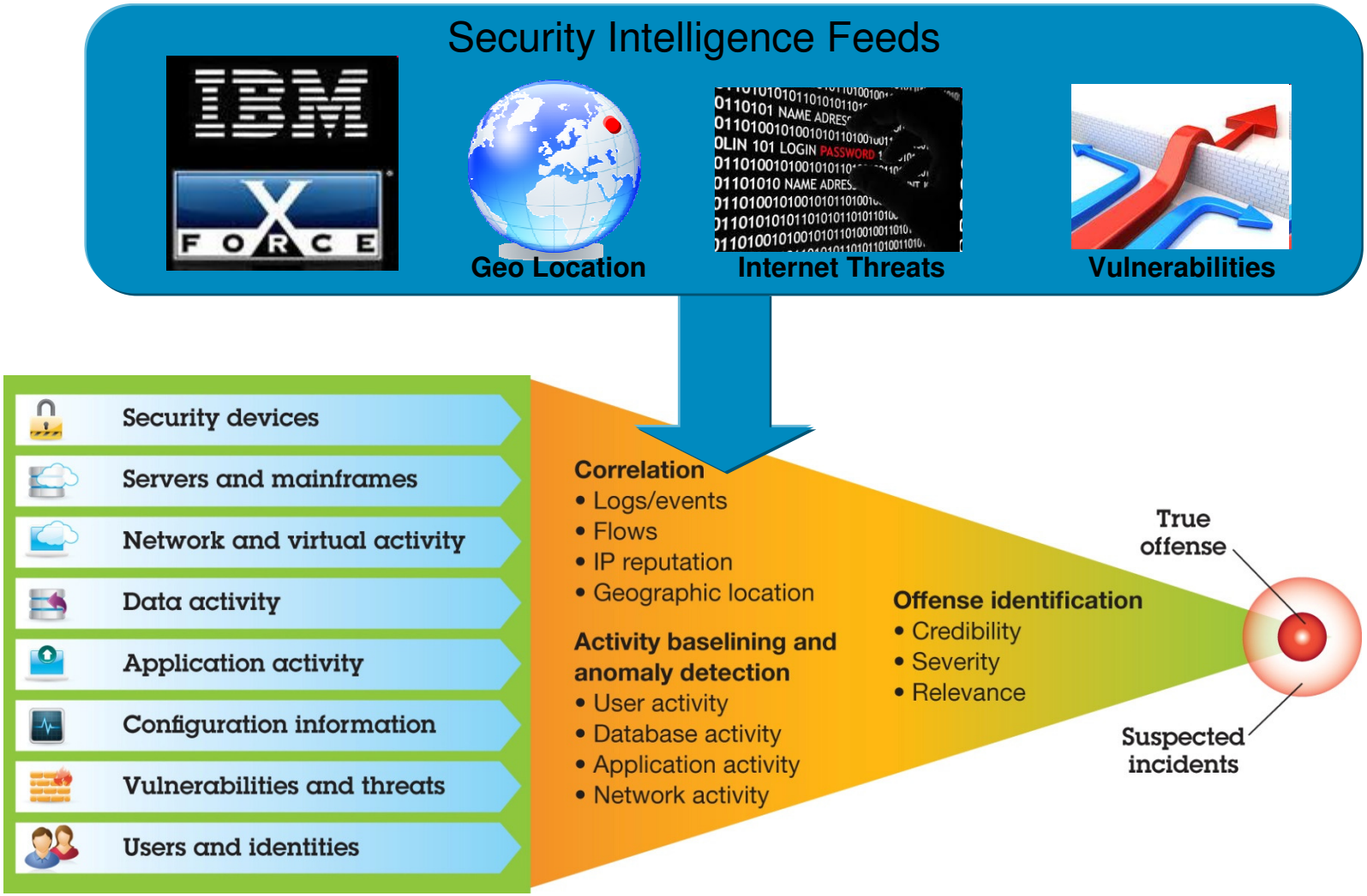
Built upon common foundation of QRadar SIOS



Taking in data from wide spectrum of feeds



And continually adding context for increased accuracy



Using fully integrated architecture and interface

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

One Console Security

Built on a Single Data Architecture

QRadar's unique advantages

- Scalability for largest deployments, using an embedded database and unified data architecture
  - ➢ *Impact: QRadar supports your business needs at any scale*

- Real-time correlation and anomaly detection based on broadest set of contextual data
  - ➢ *Impact: More accurate threat detection, in real-time*

- Intelligent automation of data collection, asset discovery, asset profiling and more
  - ➢ *Impact: Reduced manual effort, fast time to value, lower-cost operation*

- Integrated flow analytics with Layer 7 content (application) visibility
  - ➢ *Impact: Superior situational awareness and threat identification*

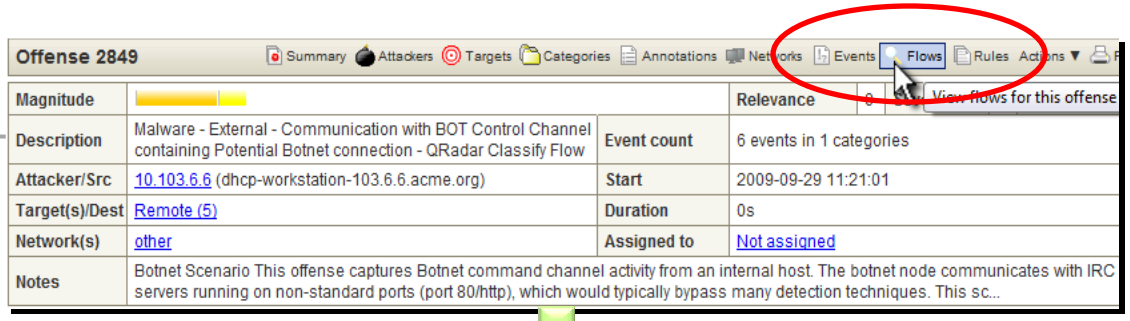
- Flexibility and ease of use enabling "mere mortals" to create and edit correlation rules, reports and dashboards
  - ➢ *Impact: Maximum insight, business agility and lower cost of ownership*

Security Intelligence Use Cases

Challenge 1: Detecting Threats

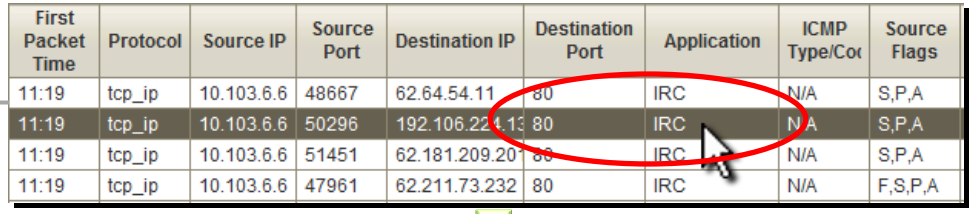
Potential Botnet Detected?

This is as far as traditional SIEM can go



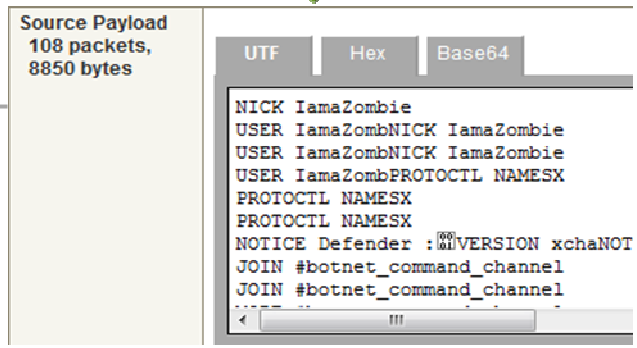
IRC on port 80?

IBM Security QRadar QFlow detects a covert channel



Irrefutable Botnet Communication

Layer 7 flow data contains botnet command control instructions



Application layer flow analysis can detect threats others miss

Challenge 2: Consolidating Data Silos

System Summary	
Current Flows Per Second	1.4M
Flows (Past 24 Hours)	1.3M
Current Events Per Second	17,384
New Events (Past 24 Hours)	677M
Updated Offenses (Past 24 Hours)	588
Data Reduction Ratio	1153571 : 1

Analyzing both flow and event data. Only IBM Security QRadar fully utilizes Layer 7 flows.

Reducing big data to manageable volumes

Advanced correlation for analytics across silos

Offense 160 Display ▼ Events Connections Flows View Attack Path Actions ▼ Print

Magnitude		Relevance 5	Severity 10 Credibility 8
Description	Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Aggressive Remote Scanner Detected	Offense Type	Source IP
		Event/Flow count	19984 events and 355 flows in 12 categories.
Source IP(s)	202.153.48.66	Start	2010-10-01 07:51:00
Destination IP(s)	Local (315)	Duration	2m 52s
Network(s)	Multiple (2)	Assigned to	Not assigned

Notes

Vulnerability Correlation Use Case
Illustrates a scenario involving correlation of vulnerability data with IDS alerts

An attacker originating from China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250).

The first systems scanned are not vulnerable, but the final system's asset profile has had vulnerability data imported from a Ne

Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

Challenge 3: Detecting Insider Fraud

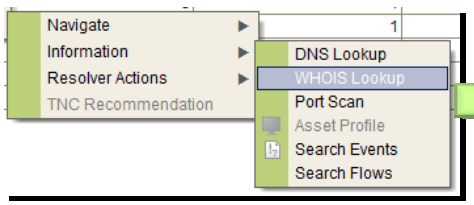
Potential Data Loss
Who? What? Where?

Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
	DELETE failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Deny
	SELECT succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Allow
	Misc Logout	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Logout
	Suspicious Pattern Detec	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Suspicious Pattern Detected
	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Remote Access Login Failed

Who?
An internal user

What?
Oracle data



QRadar Has Completed Your Request

Go to APNIC results

[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL

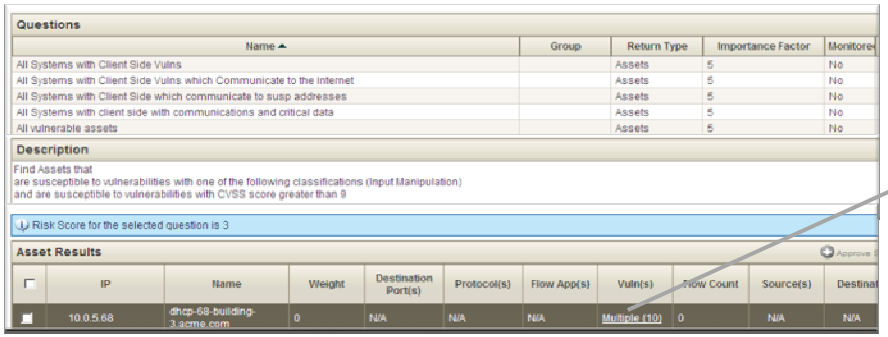
Where?
Gmail

Threat detection in the post-perimeter world

User anomaly detection and application level visibility are critical to identify inside threats

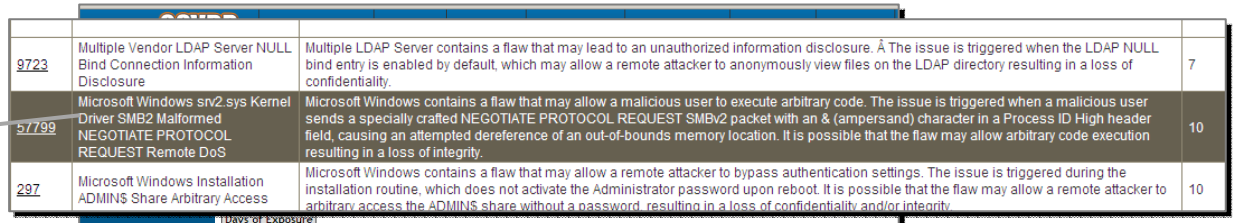
Challenge 4: Better Predicting Risks to Your Business

Assess assets with high-risk input manipulation vulnerabilities

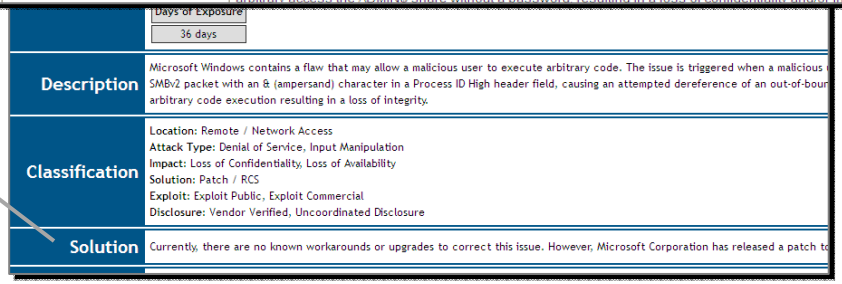


Which assets are affected?
How should I prioritize them?

What are the details?
Vulnerability details, ranked by risk score



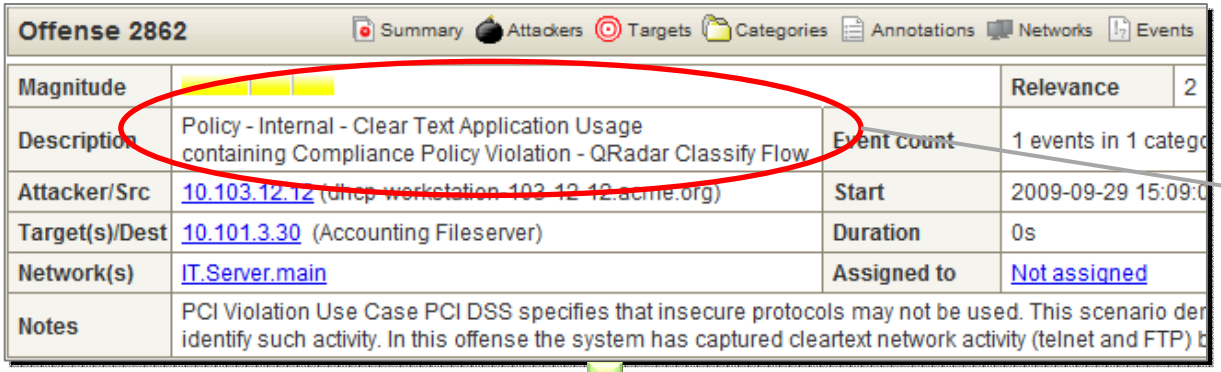
How do I remediate the vulnerability?



Pre-exploit Security Intelligence

Monitor the network for configuration and compliance risks, and prioritize them for mitigation

Challenge 5: Addressing Regulatory Mandates



Offense 2862 — Summary | Attackers | Targets | Categories | Annotations | Networks | Events

Magnitude		Relevance	2
Description	Policy - Internal - Clear Text Application Usage containing Compliance Policy Violation - QRadar Classify Flow	Event count	1 events in 1 categ
Attacker/Src	10.103.12.12 (dhcp-workstation-103-12-12.acme.org)	Start	2009-09-29 15:09:0
Target(s)/Dest	10.101.3.30 (Accounting Fileserver)	Duration	0s
Network(s)	IT.Server.main	Assigned to	Not assigned
Notes	PCI Violation Use Case PCI DSS specifies that insecure protocols may not be used. This scenario der identify such activity. In this offense the system has captured cleartext network activity (telnet and FTP) b		

PCI compliance at risk?

Real-time detection of possible violation

Event Name	Log Source	Source IP	Source Port	Destination IP	Destination Port
Compliance Policy Violation - C	Flow Classification Engine-5 :	10.103.12.12	1482	10.101.3.30	23

Unencrypted Traffic

IBM Security QRadar QFlow saw a cleartext service running on the Accounting server

PCI Requirement 4 states: Encrypt transmission of cardholder data across open, public networks

Compliance Simplified

Out-of-the-box support for major compliance and regulatory standards

Automated reports, pre-defined correlation rules and dashboards

QRadar customer case studies

Case study:
An international energy company reduces billions of events per day to find those that should be investigated

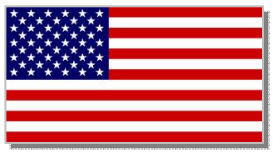
An international energy firm analyzes

2,000,000,000

events per day to find

20 – 25

potential offences to investigate



Business challenge:

- Reducing huge number of events to find the ones that need to be investigated
- Automating the process of analyzing security data

Solution: (QRadar SIEM, QFlow)

Real-time correlation of hundreds of data sources, anomaly detection to help identify “low and slow” threats, flexibility for easy customization and expansion

Security Intelligence and Analytics: A financial information provider hardens defenses against threats and fraud

Optimize risk management

Tracks 250 activity baselines dynamically adjusted over time

Saved 50-80% on staffing vs. alternative solutions

Business challenge:

- Detect wide range of security threats affecting public-facing Web applications
- Help identify subtle changes in user behavior that could indicate fraud or misuse

Solution: (QRadar SIEM, QFlow)

Real-time correlation of hundreds of data sources, anomaly detection to help identify “low and slow” threats, flexibility for easy customization and expansion

Security Intelligence and Analytics: A credit card firm simplifies complexity, reduces costs and optimizes resources

Optimize risk management

50% reduction in cost of deployment, tuning and maintenance vs. competitor

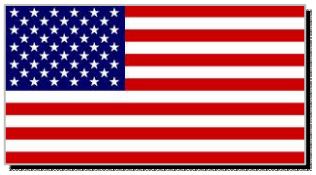
Business challenge:

- 8-year old SIEM technology did not provide visibility into and protection from current threats
- High cost of tuning and maintenance of incumbent SIEM product

Solution: (QRadar SIEM)

Advanced security analytics engine for real-time threat detection and analysis

Scalable architecture to meet client's large data and infrastructure requirements



Case study:
A financial information provider hardens defenses against threats and fraud

A European Bank

250

activity baselines dynamically adjusted over time and saved on staffing versus alternative solutions

Business challenge:

- On-line banking system targeted
- DDOS attack, three times
- Had ‘security’ in place
- Early warning capability

Solution: (QRadar SIEM, QFlow)

Real-time correlation of hundreds of data sources, anomaly detection to help identify DDoS to “low and slow” threats.

Security Intelligence and Analytics: Growth markets payments processor achieves PCI compliance / exceeds regulatory mandates

Re-engineer profitable growth

Global electronic payments firm operates in 32 countries and processes over 2 billion transactions per year

Business challenge:

- Protect client data at the heart of this business
- PCI compliance for processing of >$25 billion in annual transactions
- Rapidly implement proven solution, 0 tolerance for delays or errors

Solution: (QRadar SIEM, IBM Security Network IPS)

- Integrated solution to provide visibility into PCI and data exposure risks
- Expert implementation services based on decades of financial industry experience
- Client passed PCI audit four weeks after purchase

Case study:
Fashion Designer uses compliance mandate to detect insider fraud & use evidence in court

Fashion Designer

Using deep forensic analysis, ability to detect insider fraud to be used in court

Business challenge:

- Employee
- Downloading information
- Erasing files
- Time stamped

Solution: (QRadar SIEM)

Ability to detect who, what and how specific events occurred. Saving of raw files allowed for exact timings and application layer 7 provided methods used

Next Steps

Download the Gartner SIEM Magic Quadrant Report: bit.ly/SIEM_MQ

Subscribe to True Blue Newsletter: subscribe

Read the QRadar Labs Blog: blog.q1labs.com

Follow us on Twitter: @q1labs @ibmsecurity

ibm.com/security

Backup Material

Backed by unmatched global coverage & security awareness

IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration

10B analyzed Web pages & images
150M intrusion attempts daily
40M spam & phishing attacks
46K documented vulnerabilities
Millions of unique malware samples

X-FORCE

World Wide Managed Security Services Coverage

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 9B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)