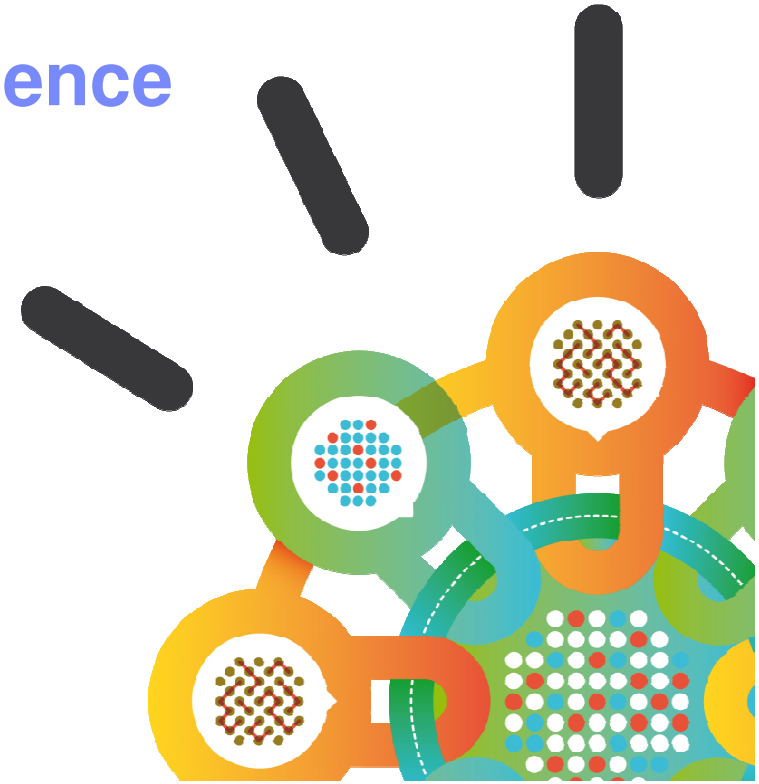
Security Intelligence.
Think Integrated.

Defend your network and keep the attackers at bay with Security Intelligence

IBM QRadar Security Intelligence

Rob Whitters
IBM Security – Technical Professional

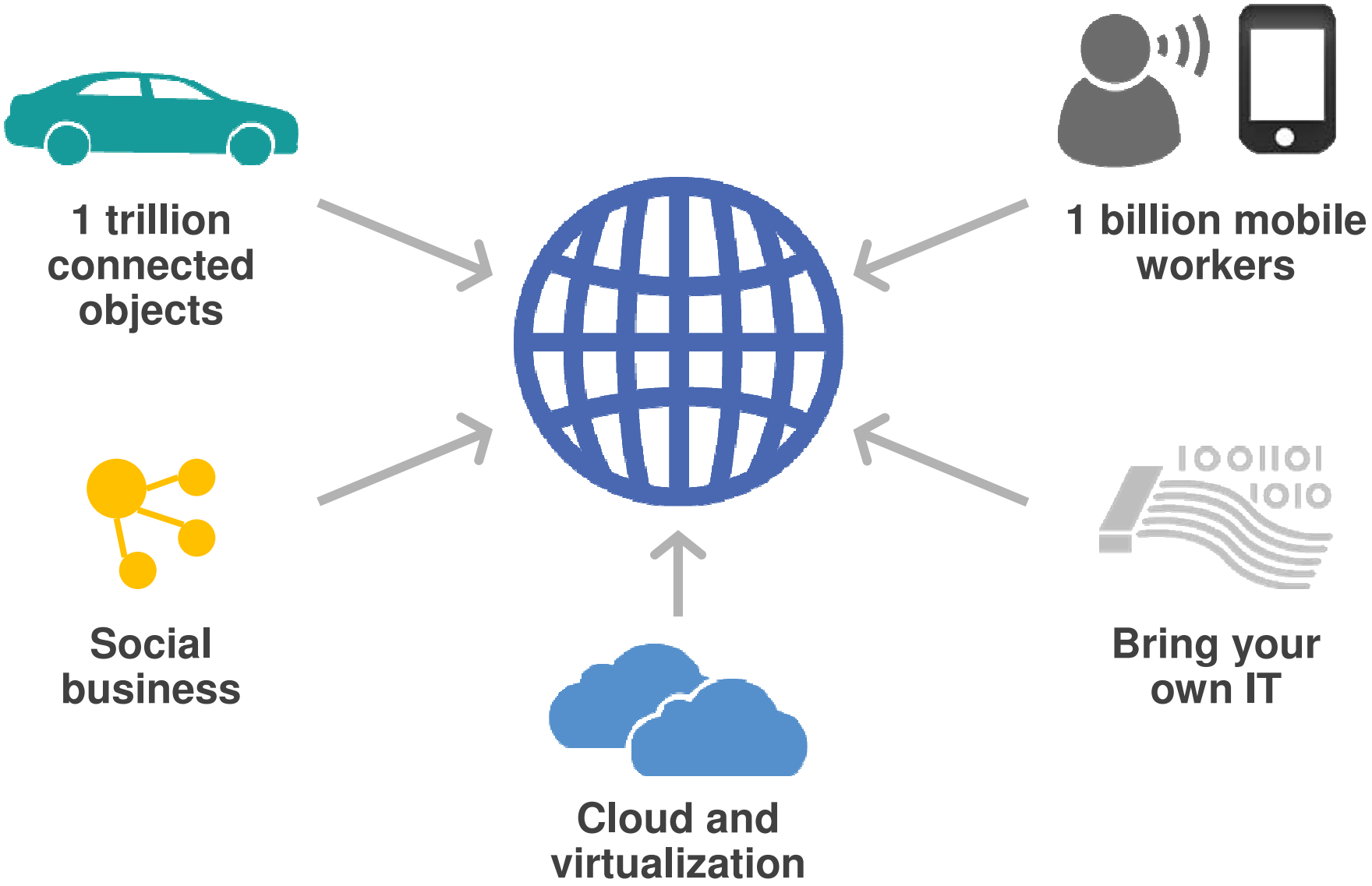
Infosecurity Europe
April 2013



Agenda

- The evolving IT security challenge
- Security Intelligence defined
- IBM QRadar Security Intelligence Platform and use cases
- Case study examples

Innovative technology changes everything



Motivations and sophistication are rapidly evolving

National Security

Nation-state actors
Stuxnet

Espionage, Activism

Competitors and Hacktivists
Aurora

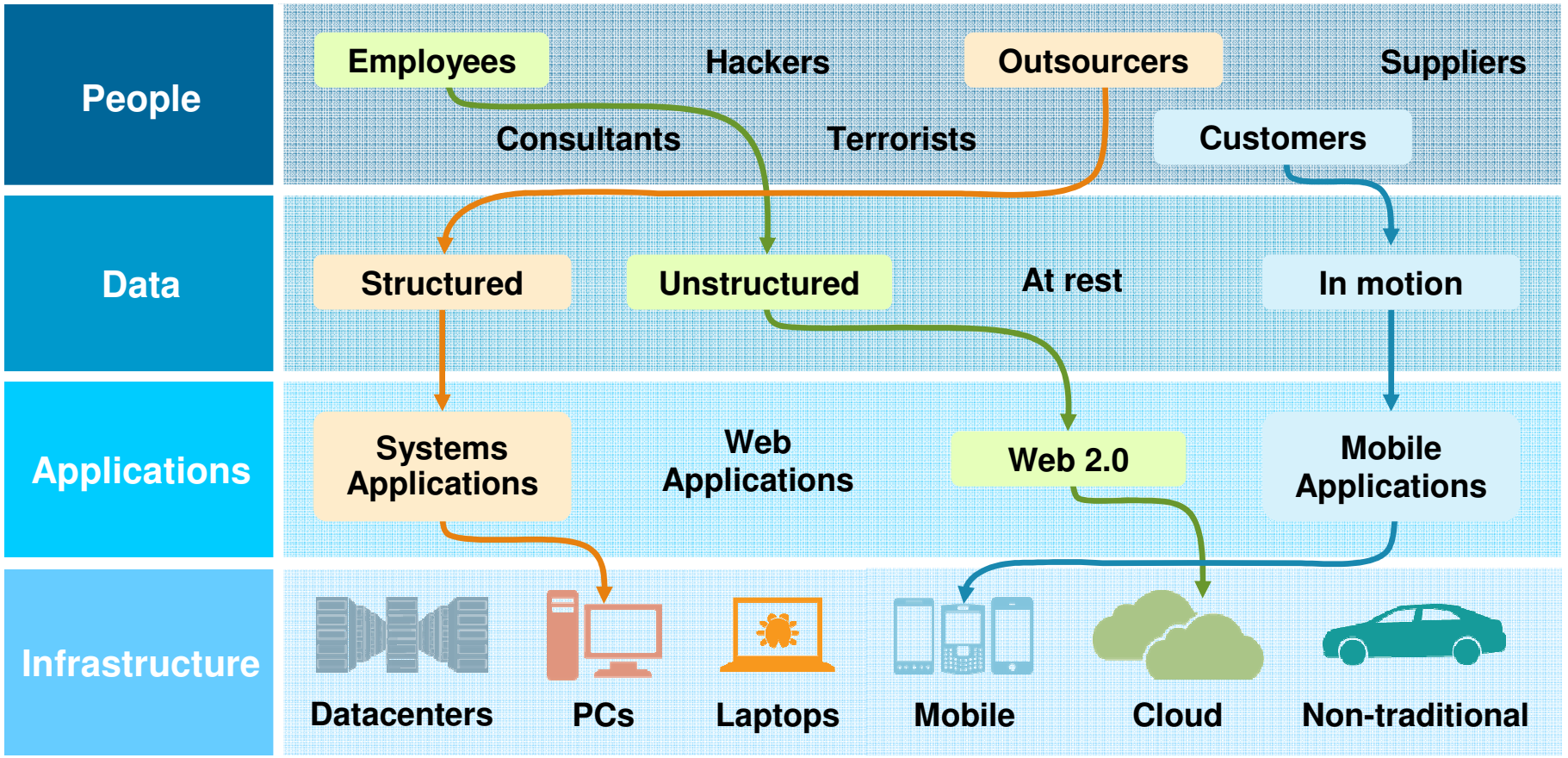
Monetary Gain

Organized crime
Zeus

Revenge, Curiosity

Insiders and Script-kiddies
Code Red

Security challenges are a complex, four-dimensional puzzle …



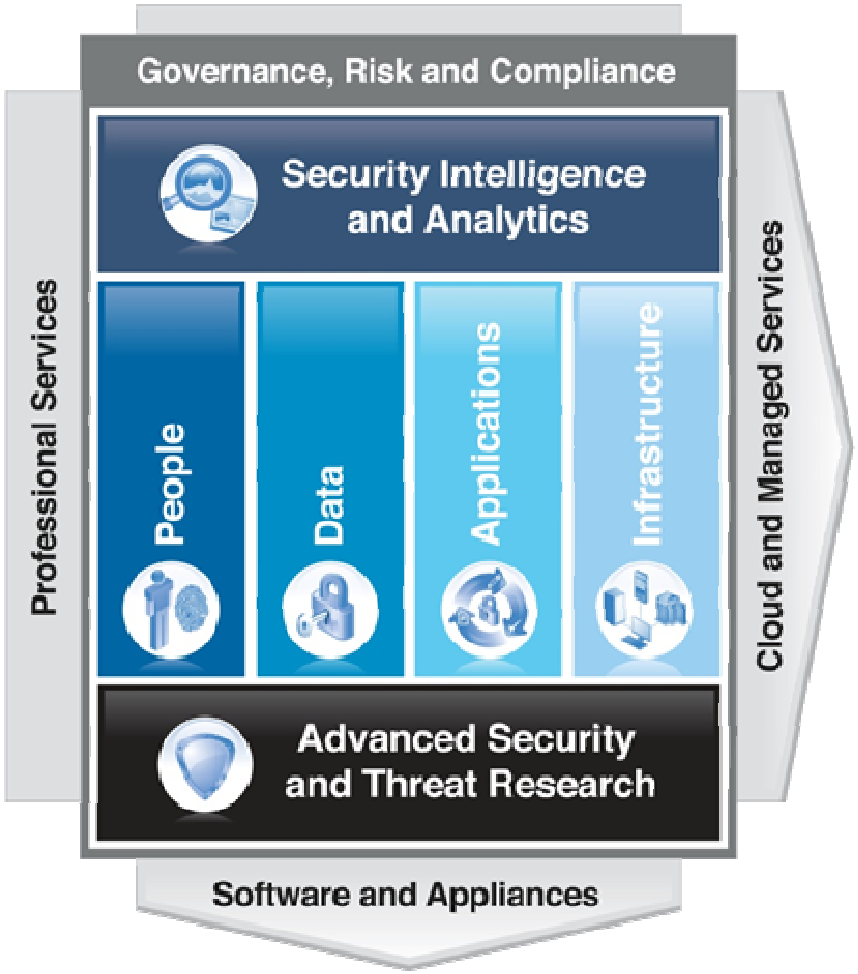
… that requires a new approach

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

What challenges does Security Intelligence help with?

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

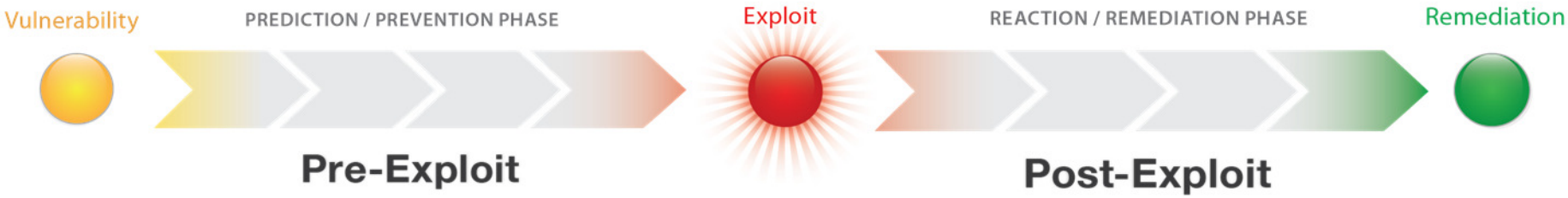
- Full life cycle of compliance and risk management for network and security infrastructures

Addressing regulation mandates

- Automated data collection and configuration audits

IBM QRadar Security Intelligence Platform

Solutions for the Full Security Intelligence Timeline



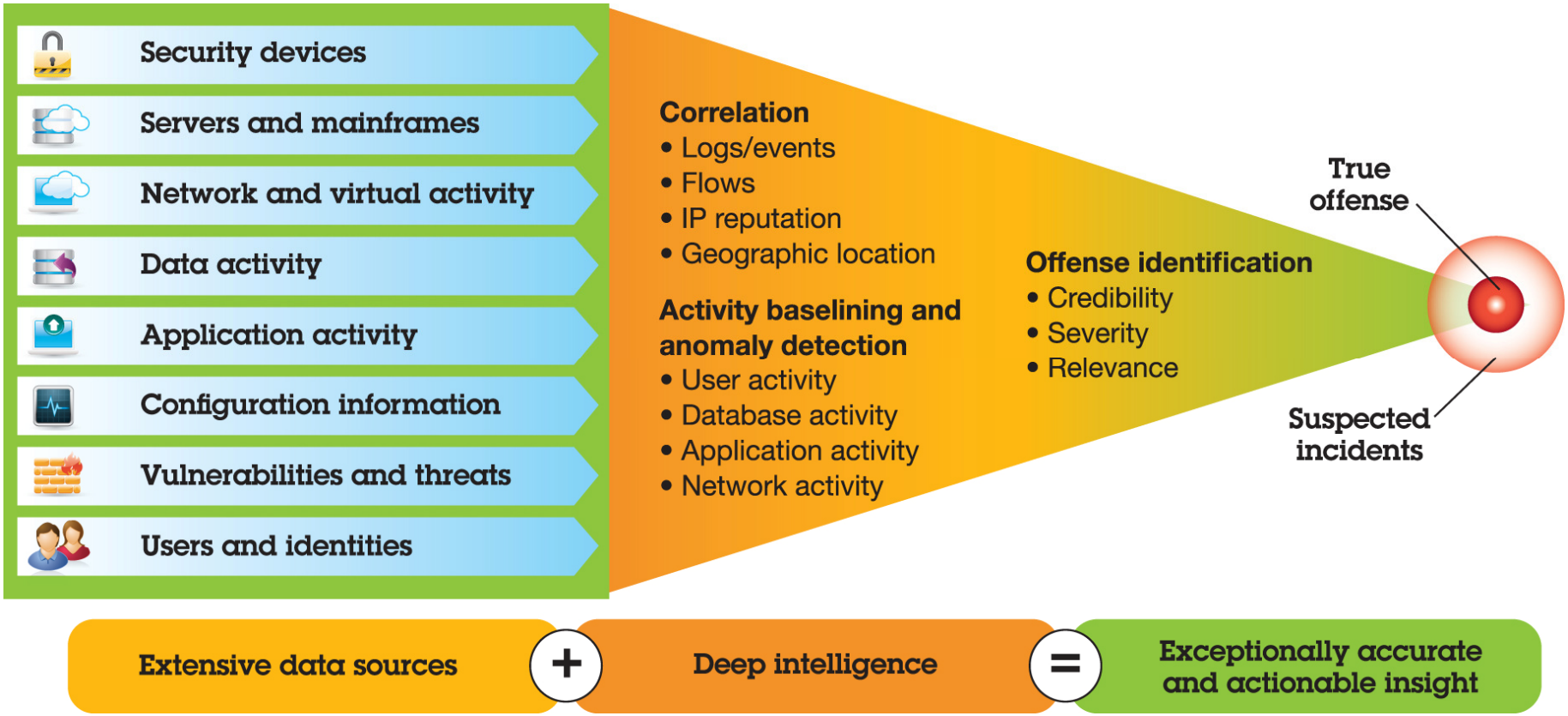
Prediction & Prevention

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

Reaction & Remediation

SIEM. Log Management. Incident Response.
Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Loss Prevention.

Taking in data from a wide spectrum of sources



Using a fully integrated architecture and interface

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

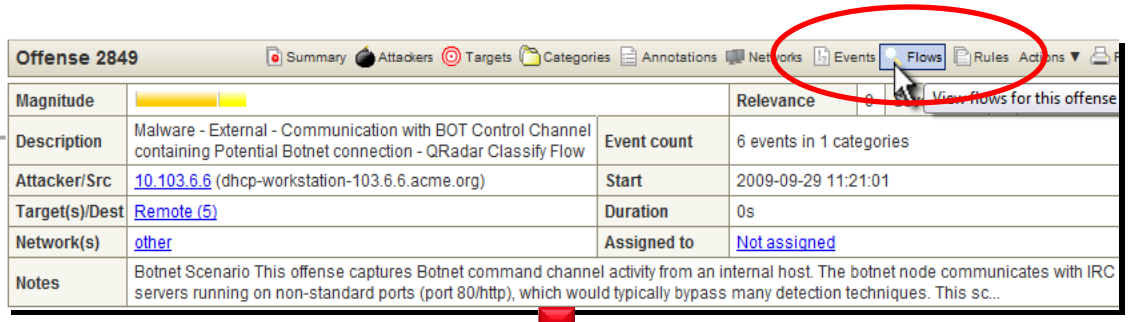
One Console Security

Built on a Single Data Architecture

Challenge 1: Detecting Threats

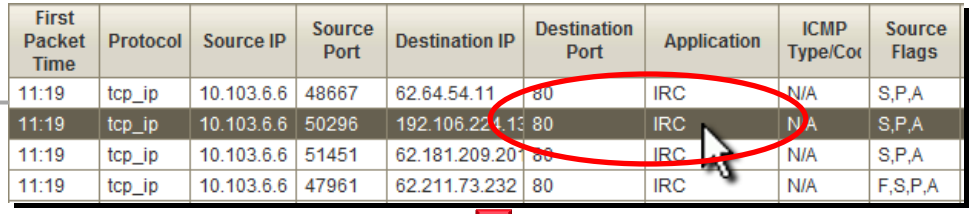
Potential Botnet Detected?

This is as far as traditional SIEM can go



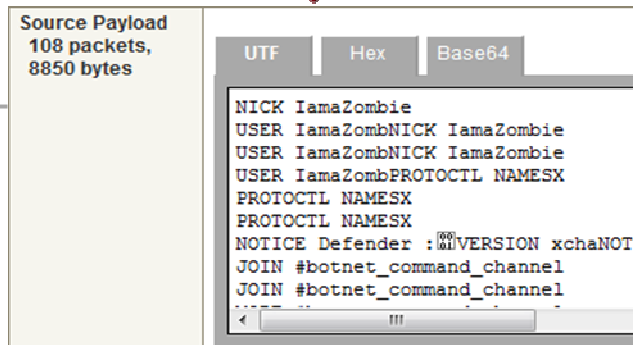
IRC on port 80?

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 help 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

Produces manageable list of daily 'offences' to research

Challenge 3: Detecting Insider Fraud & Misuse

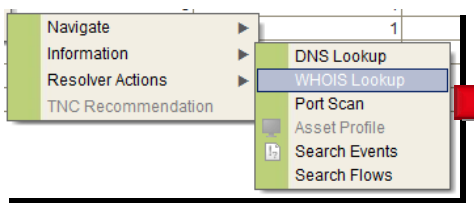
Potential Data Loss
Who? What? Where?

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

Helps spot insider threats using anomaly detection & application level visibility

Challenge 4 : Better Predicting Real Risks to the Environment

Clear & concise delivery of the most relevant information …

Offense 3063 — Summary | Attackers | Targets | Categories | Annotations | Networks | Events | Flows | Rules | Actions | Print

Magnitude				Relevance	0	Severity	8	Credibility	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan		Event count	1428 events in 3 categories			
Attacker/Src	202.153.48.66		Start	2009-09-29 16:05:01			
Target(s)/Dest	Local (717)		Duration	1m 32s			
Network(s)	Multiple (3)		Assigned to	Not assigned			
Notes	Vulnerability Correlation Use Case Illustr…on of vulnerability data with IDS alerts An attacker originating from China (202…ng the Conficker worm exploit (CVE 2008-4250)						

What was the attack?

Was it successful?

Who was responsible?

Attacker Summary — Details

Magnitude		User	Karen
Description	202.153.48.66	Asset Name	Unknown
Vulnerabilities	0	MAC	Unknown
Location	China	Asset Weight	0

Where do I find them?

Top 5 Categories — Categories

Name	Magnitude	Local Target Count	
Buffer Overflow		8	8
Misc Exploit		3	3
Network Sweep		716	1417

How valuable are they to the business?

How many targets involved?

Top 5 Local Targets — Targets

IP/DNS Name	Ma…		Chained	User	MAC	Location	Weight
Windows AD Server		Unknown	No	Unknown	Unknown	main	8
10.101.3.3		Unknown	No	Unknown	Unknown	main	0
10.101.3.4		Unknown	No	Unk…		main	0
DC106		Yes	No	Adm…		main	10
10.101.3.11		Unknown	No	DC…		main	0

Are any of them vulnerable?

Top 10 Events — Events

Event Name	Magnitude		Category	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm	Misc Exploit	10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo…		Snort @ 10.1.1.5	Buffer Overflow	10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo…		Snort @ 10.1.1.5		10.101.3.15	445	09-29 16:06:33
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-…		10.101.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qr…		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qr…		10.101.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qr…		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01

Where is all the evidence?

Challenge 5 : Addressing Compliance Mandates

QRadar Example: Access and Authentication Rule for Regulatory Compliance

Apply this rule Default-Rule-Compliance: Excessive Failed Logins to Cor on events which are detected by the system

- and when we see an event match any of the following Default-BB-ComplianceDefinition: GLBA Servers, Default-BB-ComplianceDefinition: HIPAA Servers, Default-BB-ComplianceDefinition: SOX Servers, Default-BB-ComplianceDefinition: PCI Servers
- and when we see any of these Default-BB-CategoryDefinition: Authentication Failures with the same destination IP more than 10 times, across more than 0 destination IP(s) within 10 minutes

Notes (Enter your notes about this rule)

Reports excessive authentication failures to a compliance server within 10 minutes.

Evolving along with the changing threat landscape

First Gen: Collection

- Log collection
- Signature-based detection

Today: Intelligence

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

Extending Security Intelligence for new use cases

Structured, analytical, repeatable

Creative, exploratory, intuitive

Security Intelligence Platform

Real-time Processing

- Real-time data correlation
- Anomaly detection
- Event and flow normalization
- Security context and enrichment
- Distributed architecture

Security Operations

- Pre-defined rules and reports
- Offense scoring and prioritization
- Activity and event graphing
- Compliance reporting
- Workflow management

IBM Security Intelligence with Big Data

Big Data Platform

Big Data Warehouse

- Long-term, multi-PB storage
- Unstructured and structured
- Distributed Hadoop infrastructure
- Preservation of raw data
- Enterprise integration

Analytics and Forensics

- Advanced visuals and interaction
- Predictive and decision modeling
- Ad hoc queries
- Interactive visualizations
- Collaborative sharing tools
- Pluggable, intuitive UI

Introducing IBM Security Intelligence with Big Data

Security Intelligence Platform

IBM Security QRadar

- Data collection and enrichment
- Event correlation
- Real-time analytics
- Offense prioritization

QRadar

Real-time streaming

Insights

Advanced Threat Detection

Big Data Platform

IBM InfoSphere BigInsights

- Hadoop-based
- Enterprise-grade
- Any data / volume
- Data mining
- Ad hoc analytics

Custom Analytics

Traditional data sources

Non-traditional

QRadar Customer Case Studies

Case study: An international energy company reduces billions of events per day to find the handful 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, QRadar QFlow)

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

Case Study: 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 maintaining 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: Fashion Designer deploys SIEM for compliance; detects insider fraud & obtains evidence for court

Fashion Designer

Using deep forensic analysis, detect insider fraud and provide evidence 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 documents exact timing of events
- Layer 7 (application layer) network flows prove activity

Learn more about Security Intelligence today

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

Download the IBM X-Force 2012 Trend & Risk Report: bit.ly/xforce-12

Subscribe to IBM Security Systems Newsletter: bit.ly/ibm-sec-news

Read the IBM Institute for Advanced Security Blog: bit.ly/IAS-blog

Follow us on Twitter: @ibmsecurity

ibm.com/security

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.