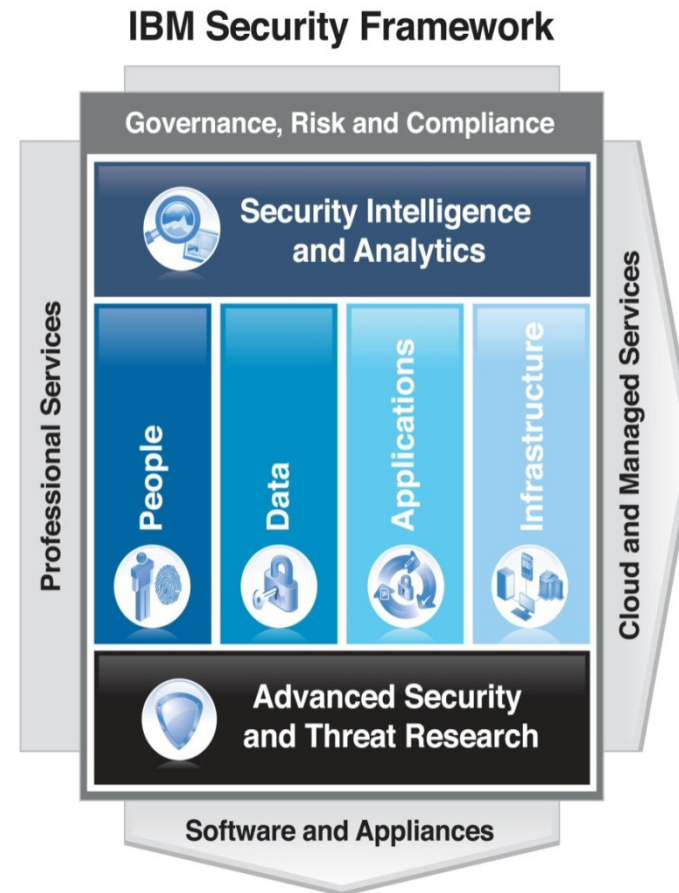# IBM QRadar Security Intelligence

Nico de Smidt

NdS@nl.ibm.com

IBM Security Systems

- Only vendor in the market with end-to-end coverage of the security foundation
- $1.8B investment in innovative technologies
- 6K+ security engineers and consultants
- Award-winning X-Force® research
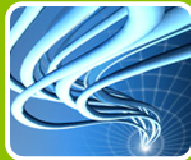- Largest vulnerability database in the industry

IBM Security Framework

Governance, Risk and Compliance

Security Intelligence and Analytics

People | Data | Applications | Infrastructure

Professional Services

Cloud and Managed Services

Advanced Security and Threat Research

Software and Appliances

Customer 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
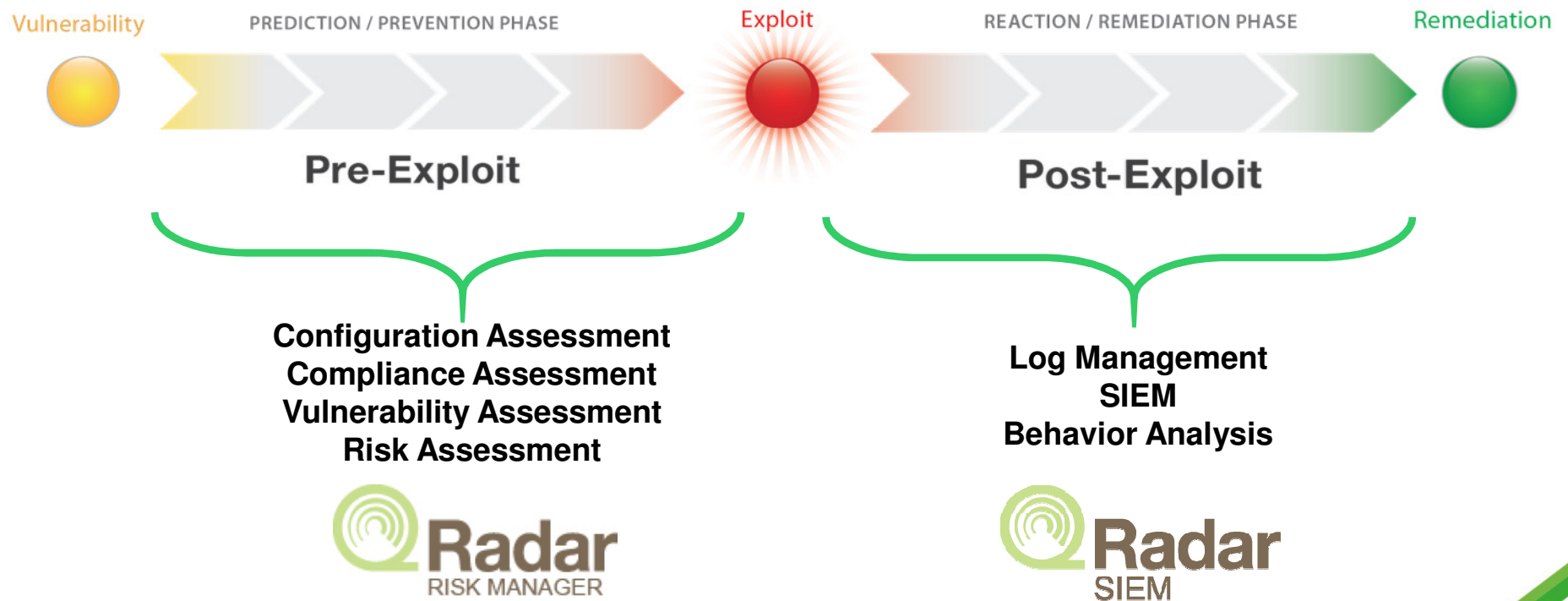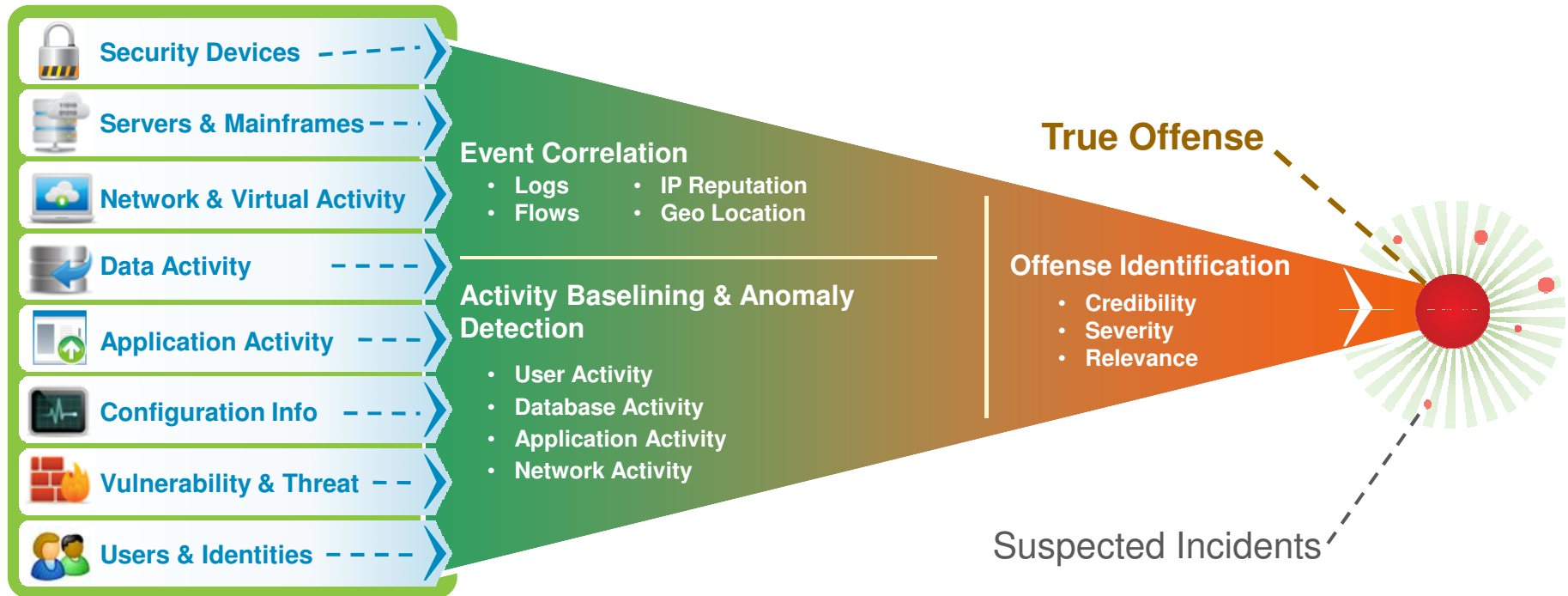
Addressing regulation mandates

- Automated data collection and configuration audits

Full Compliance and Security Intelligence Time line

| What are the external and internal threats? | Are we configured to protect against these threats? | What is happening right now? | What was the impact? |

Vulnerability | PREDICTION / PREVENTION PHASE | **Exploit** | REACTION / REMEDIATION PHASE | **Remediation**

Pre-Exploit **Post-Exploit**

**Configuration Assessment
Compliance Assessment
Vulnerability Assessment
Risk Assessment**

**QRadar
RISK MANAGER**

**Log Management
SIEM
Behavior Analysis**

**QRadar
SIEM**

Context and Correlation Drive Security Intelligence

IBM

- Security Devices
- Servers & Mainframes
- Network & Virtual Activity
- Data Activity
- Application Activity
- Configuration Info
- Vulnerability & Threat
- Users & Identities

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

| Infra, People, Application, Data | + | Deep Intelligence | = | Exceptionally Accurate and Actionable Insight |

Fully Integrated Security Intelligence in One Console

Challenge 1: Detecting Threats Others Miss

IBM

Potential Botnet Detected?
This is as far as traditional SIEM can go

Offense 2849	🔴 Summary 💣 Attackers 🎯 Targets 📁 Categories 📄 Annotations 🖥 Networks 📄 Events ▪ Flows 📄 Rules Actions ▼ 🖨

Magnitude		Relevance	0 View flows for this offense
Description	Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow	Event count	6 events in 1 categories
Attacker/Src	10.103.6.6 (dhcp-workstation-103.6.6.acme.org)	Start	2009-09-29 11:21:01
Target(s)/Dest	Remote (5)	Duration	0s
Network(s)	other	Assigned to	Not assigned
Notes	Botnet Scenario This offense captures Botnet command channel activity from an internal host. The botnet node communicates with IRC servers running on non-standard ports (port 80/http), which would typically bypass many detection techniques. This sc...		

IRC on port 80?
IBM Security QRadar QFlow detects a covert channel

First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Code	Source Flags
11:19	tcp_ip	10.103.6.6	48667	62.64.54.11	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	50296	192.106.224.13	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	51451	62.181.209.20	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A

Irrefutable Botnet Communication
Layer 7 flow data contains botnet command control instructions

Source Payload
108 packets,
8850 bytes

UTF	Hex	Base64

```
NICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombPROTOCTL NAMESX
PROTOCTL NAMESX
PROTOCTL NAMESX
NOTICE Defender :␁VERSION xchaNOT
JOIN #botnet_command_channel
JOIN #botnet_command_channel
```

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	310633 : 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:

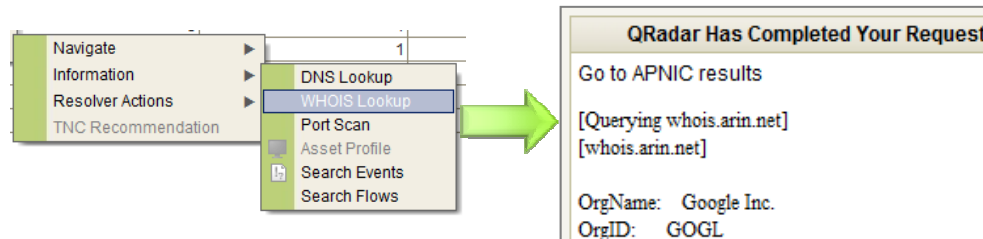# Challenge 3: Detecting Insider Fraud

Potential Data Loss
Who? What? Where?

Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.1X.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

Navigate	▶	1
Information	▶	DNS Lookup
Resolver Actions	▶	WHOIS Lookup
TNC Recommendation		Port Scan
		Asset Profile
		Search Events
		Search Flows

QRadar Has Completed Your Request

Go to APNIC results

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

OrgName: Google Inc.
OrgID: GOGL

Where?
Gmail

Assets with High-Risk 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?

Challenge 5: Addressing Regulatory Mandates

PCI compliance at risk?

Real-time detection of possible violation

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

Get an Intelligent View into your Security Posture

Security Intelligence

Optimized
Organizations use **predictive and automated** security analytics to drive toward **security intelligence**

Proficient
Security is layered into the **IT fabric** and **business operations**

Basic
Organizations employ **perimeter protection**, which regulates access and feeds manual reporting

Optimized

Proficient

Basic

Automated

Manual

Reactive

Proactive
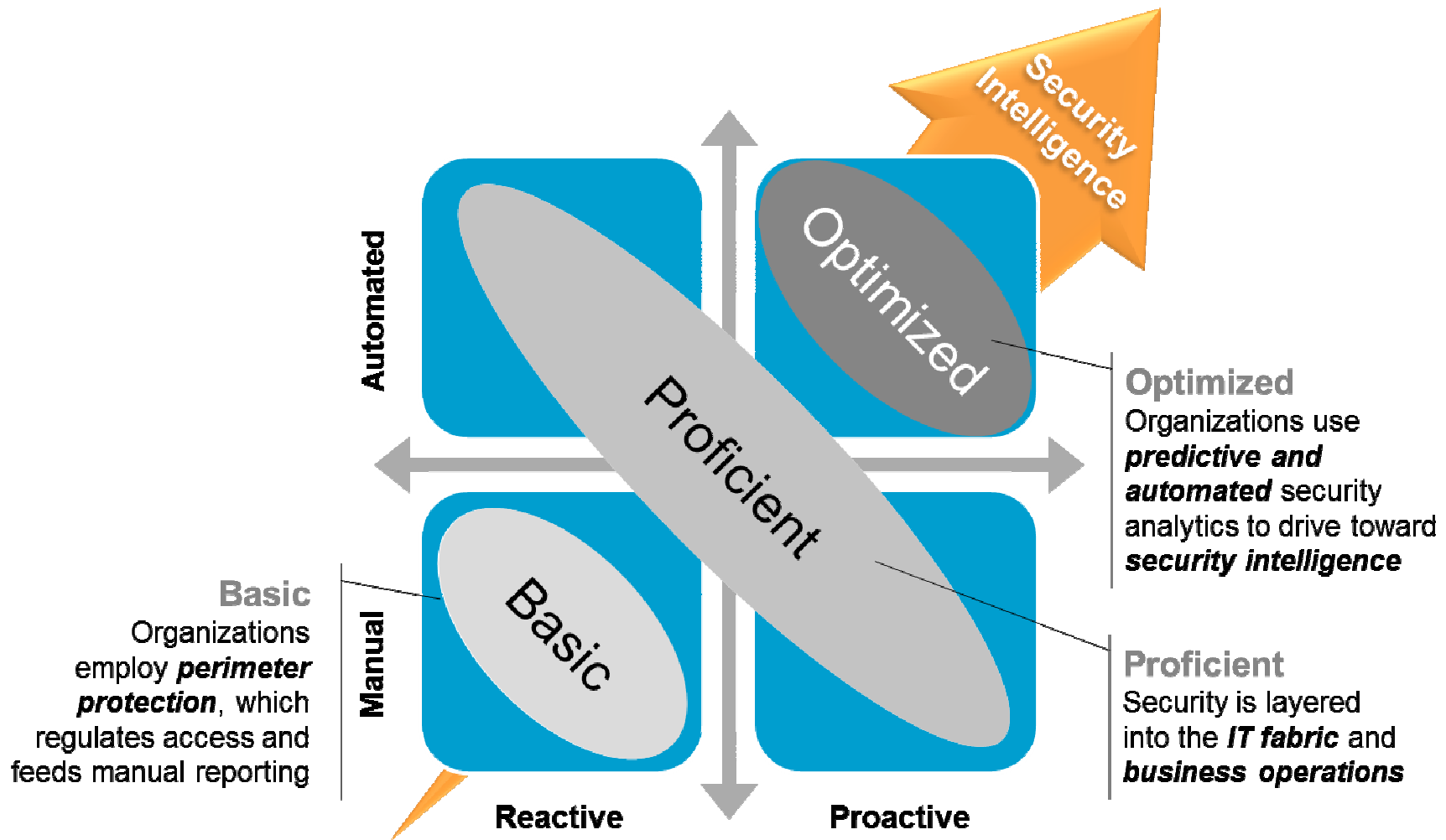
- Real-time context driven correlation and anomaly detection
  - ➤ *Impact: More accurate threat detection, in real-time*

- Integrated flow analytics with Layer 7 application visibility
  - ➤ *Impact: Superior situational awareness and threat identification*

- Automated data collection, asset discovery and asset profiling
  - ➤ *Impact: Reduced manual effort, fast time to value, lower-cost operation*

- Easy to use and edit correlation rules, reports and dashboards
  - ➤ *Impact: Maximum insight, business agility and lower cost of ownership*

- Scalability for largest deployments
  - ➤ *Impact: QRadar supports your business needs at any scale*

ibm.com/security