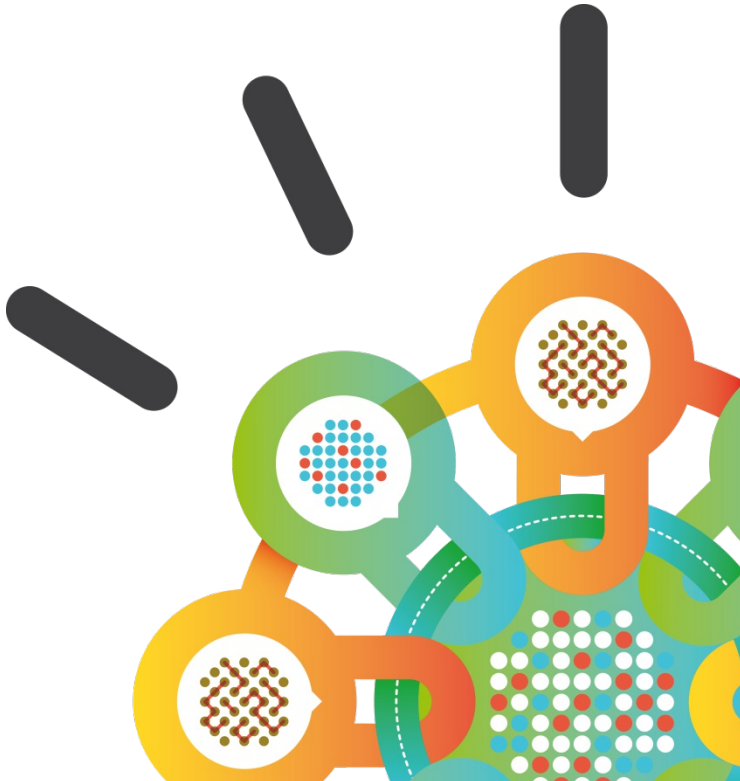
Security Intelligence.
Think Integrated.

Ahead of the threat with Security Intelligence

PITB Information Security Conference 2013



Zoaib Nafar
Brand Technical Sales Lead
IBM Security Systems

The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks…

DATA EXPLOSION

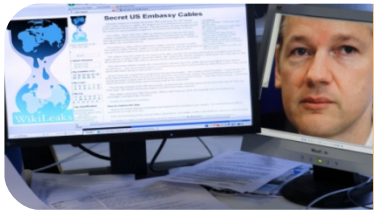
The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

EVERYTHING IS EVERYWHERE

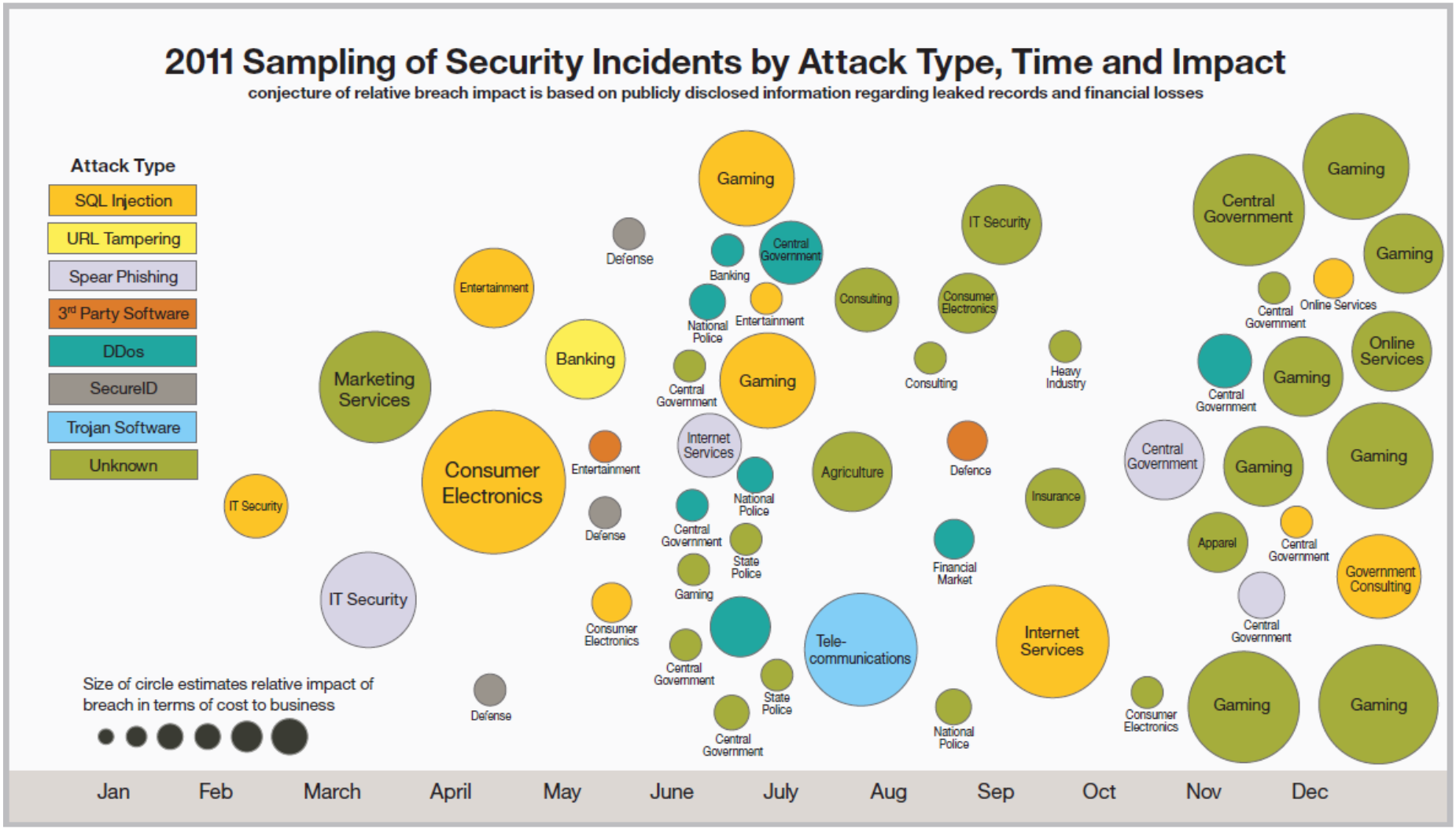
Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more



ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new actors with new motivations from cyber crime to terrorism to state-sponsored intrusions

Year of the security breach



Source: IBM X-Force Reseach

Motivations and sophistication are rapidly evolving

National Security

Advanced Persistent Threats

Nation-state actors
Stuxnet
(June 2010)

Espionage, Activism

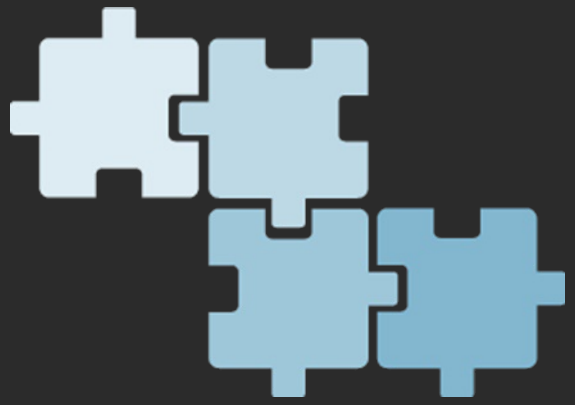
Competitors and Hacktivists
Aurora
(January 2010)

Monetary Gain

Organized crime
Zeus
(2007)

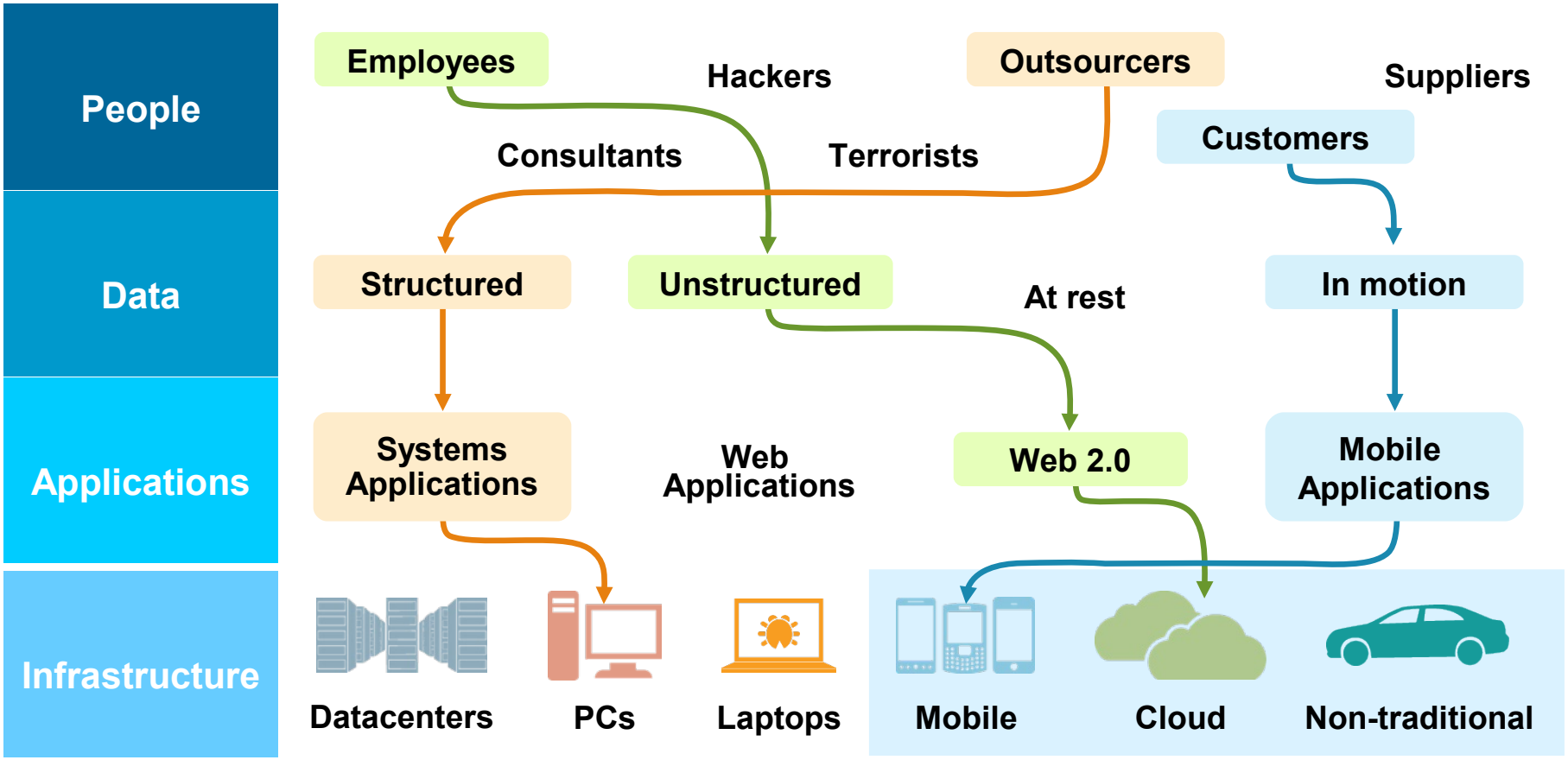
Revenge, Curiosity

Insiders and Script-kiddies
Code Red
(2001)



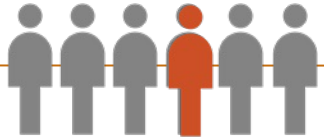
How do we solve this?

Security challenges are a complex, four-dimensional puzzle …



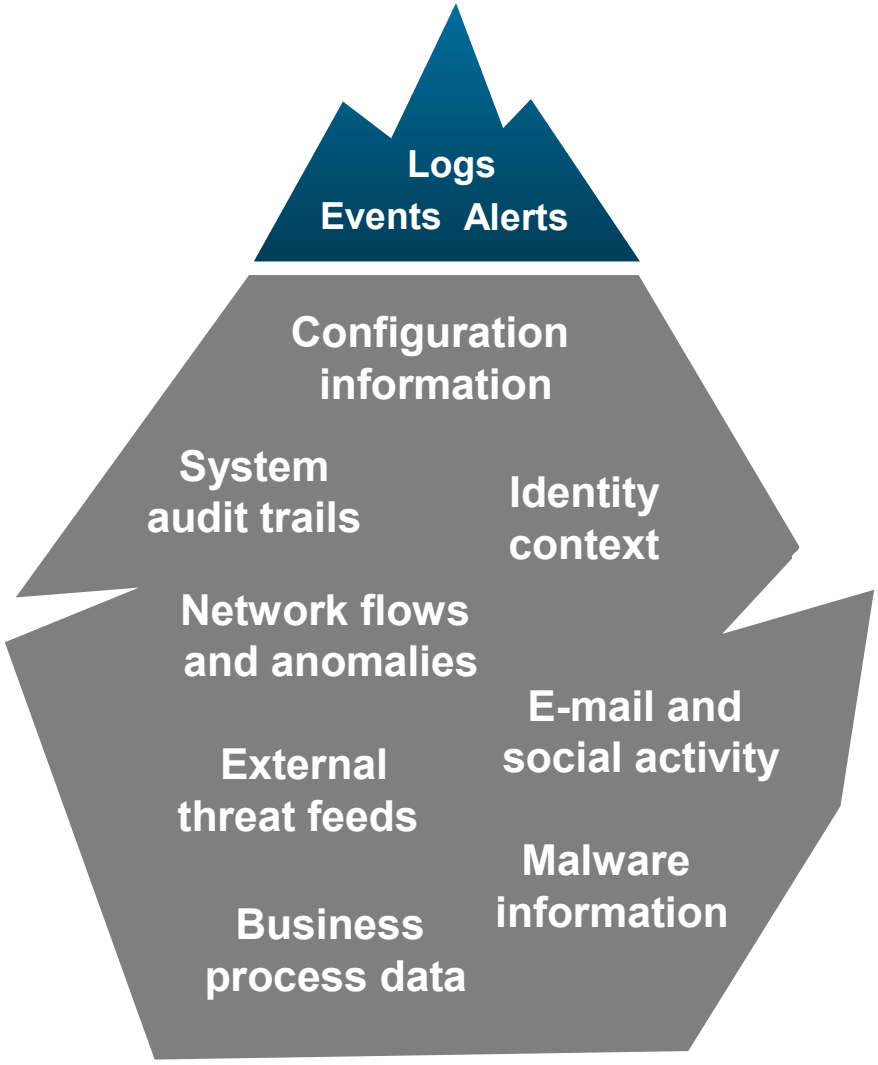
… that requires a new approach

Thinking differently about security

	Then		Now
People	Administration		Insight
Data	Basic-control		Laser-focused
Applications	Bolt-on		Built-in
Infrastructure	Thicker walls		Smarter defenses

Collect and Analyze Everything

Security Intelligence

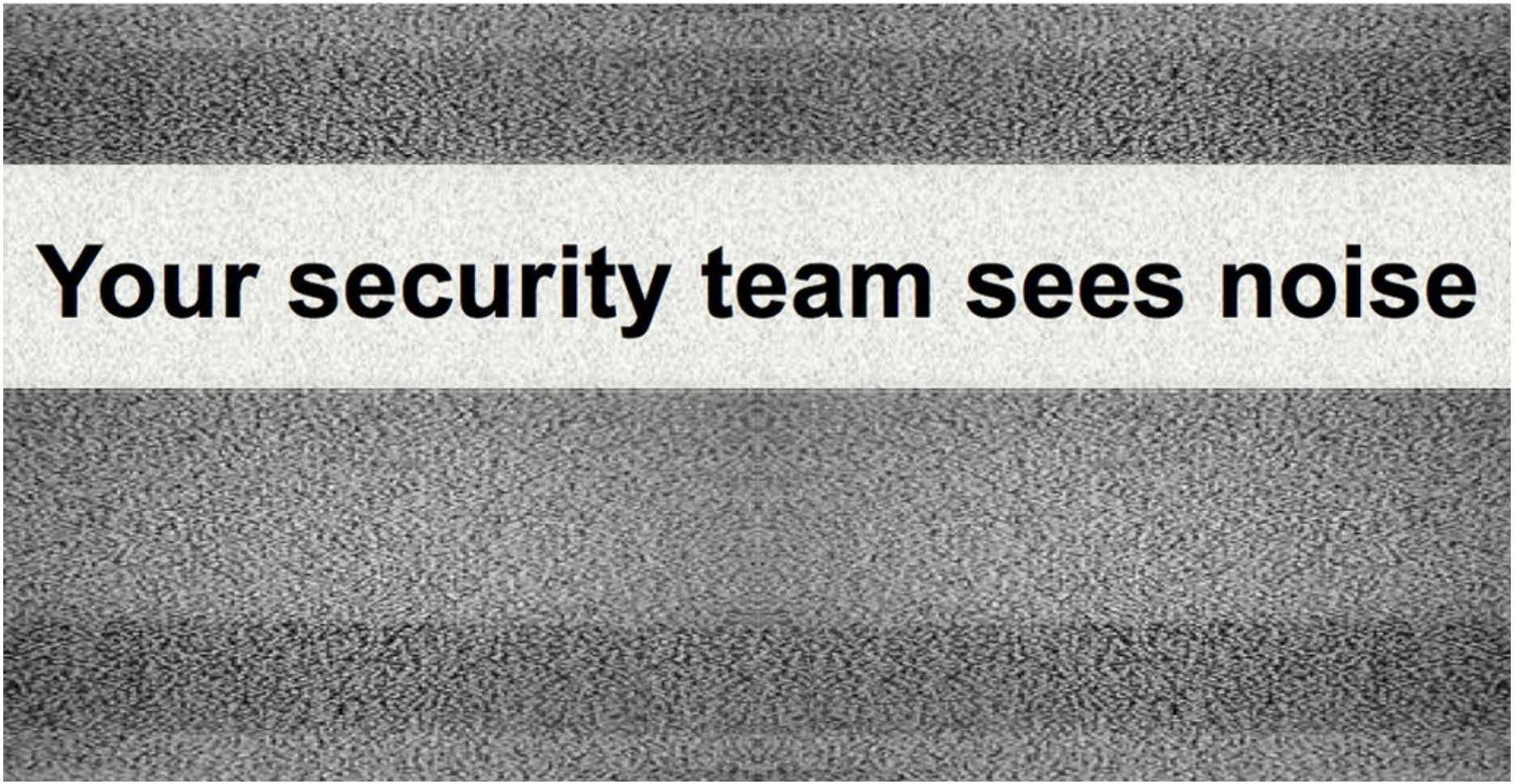


Then: Collection

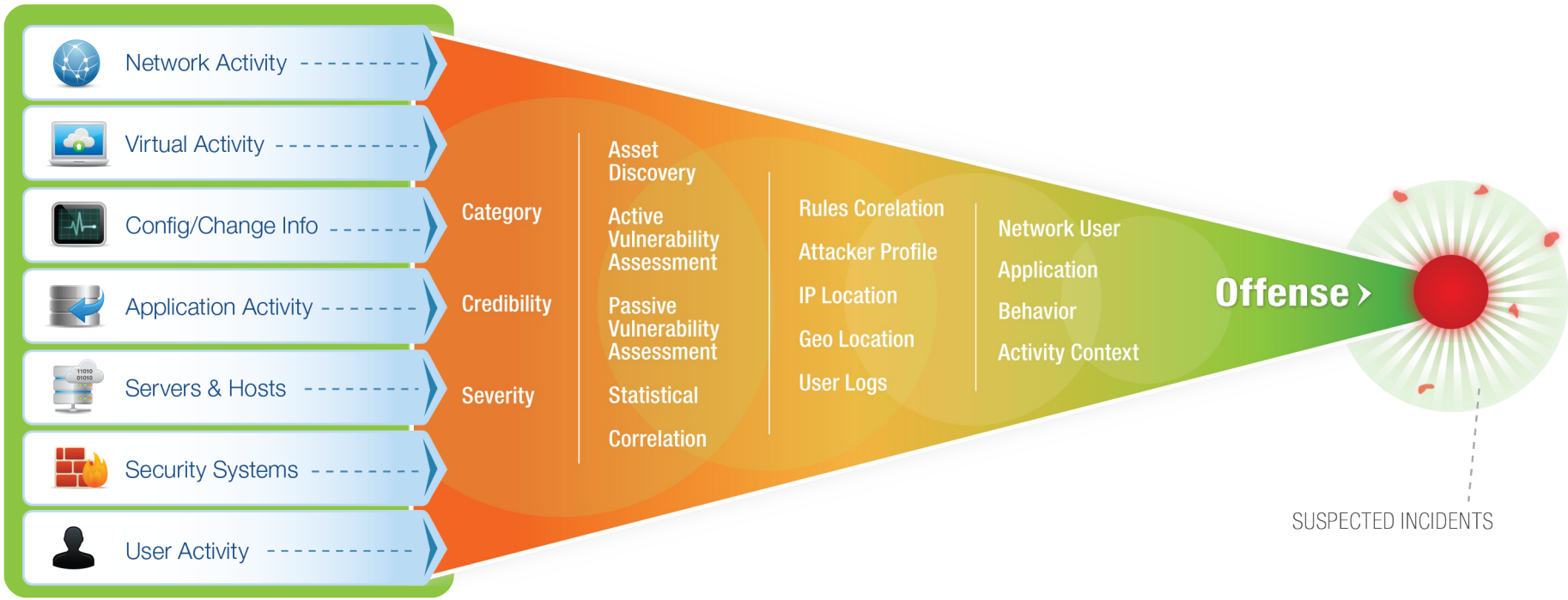
- Log collection
- Signature-based detection

Now: Intelligence

- Real-time monitoring
- Context-aware anomaly detection
- Automated correlation and analytics
- Insight from Big Data



Finding the needle in the haystack



Sources + Intelligence = Most Accurate & Actionable Insight

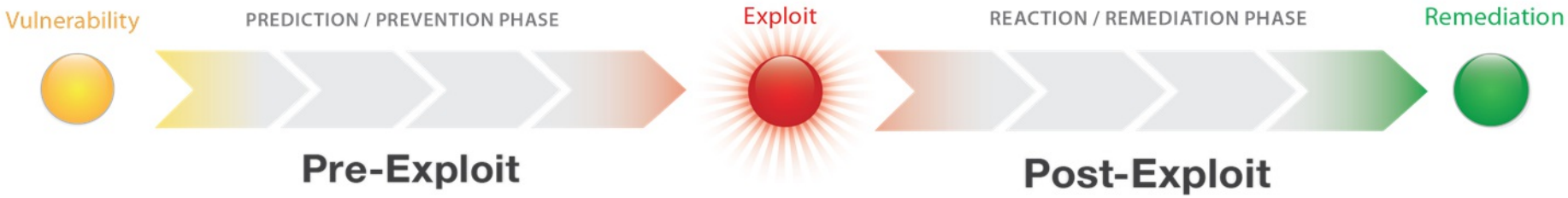
Dealing with Advanced Persistent Threats

What are the external and internal threats?

Are we configured to protect against these threats?

What is happening right now?

What was the impact?



Prediction & Prevention

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

Reaction & Remediation

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

Security Intelligence

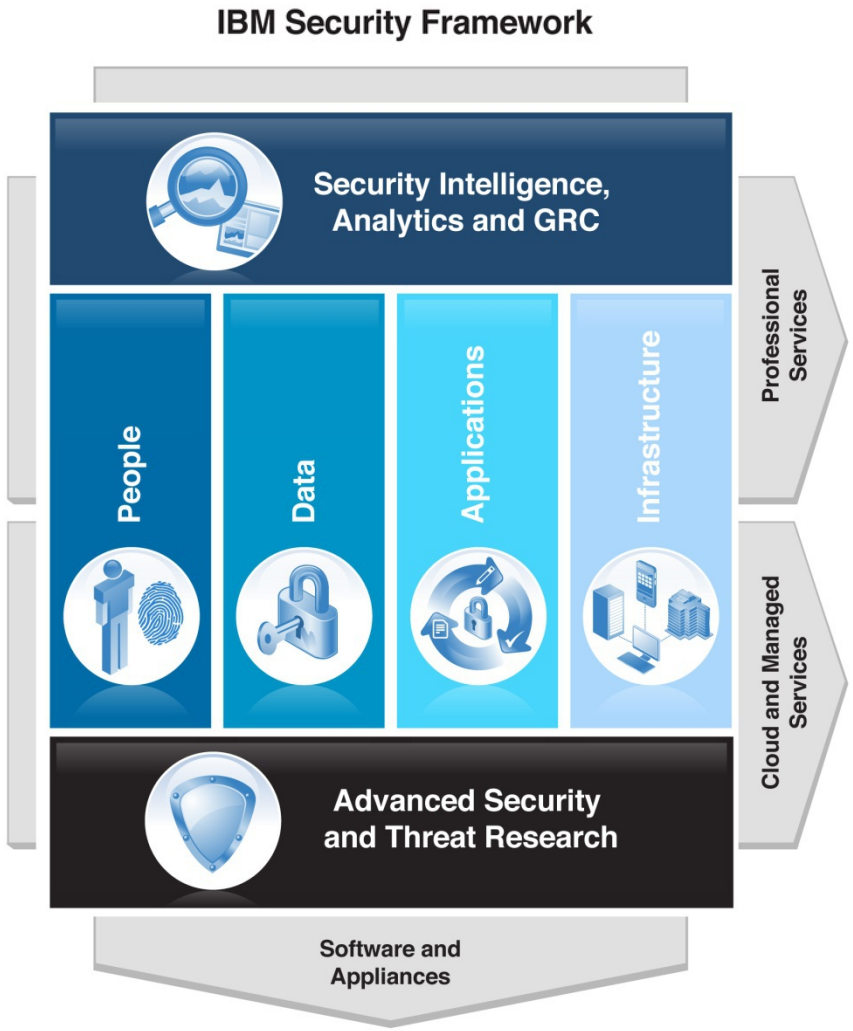
Applying these principles

IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

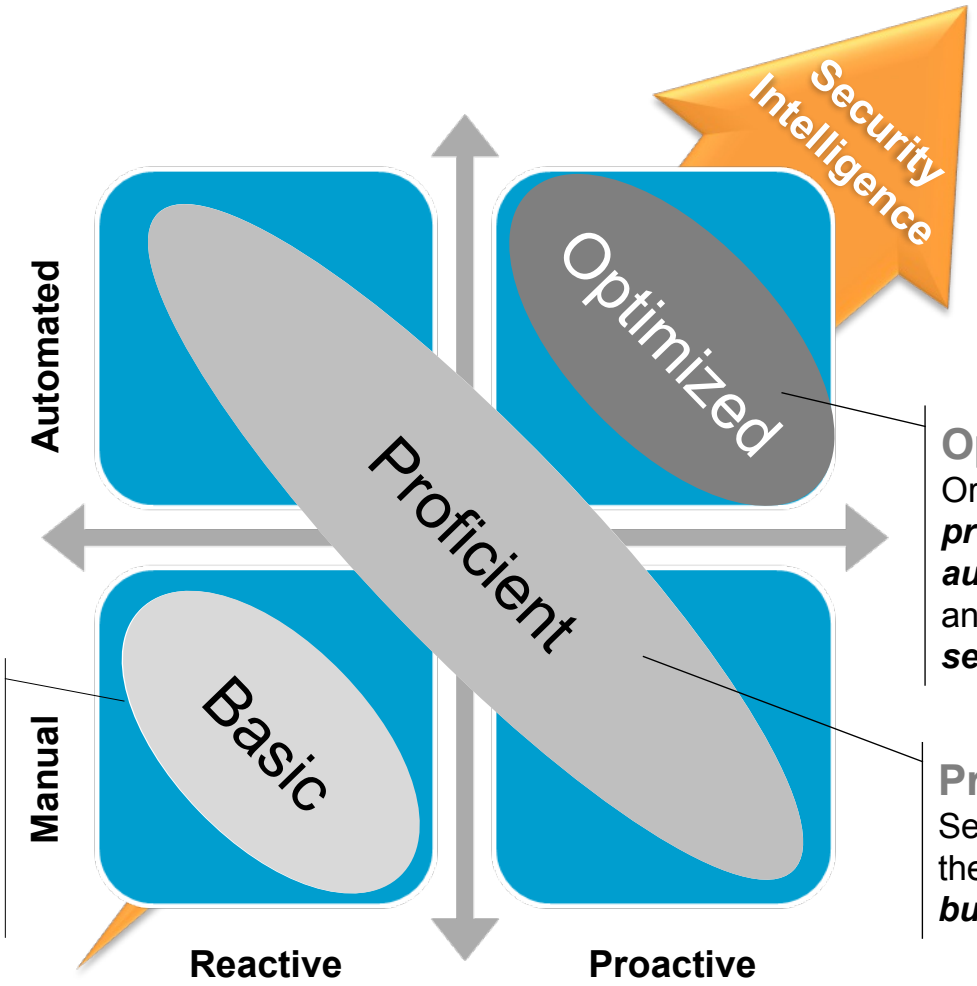
IBM Security Systems

- **End-to-end coverage** of the security foundation
- Award-winning X-Force® research
- **64k** documented vulnerabilities - largest in the industry
- **14B/mo** analyzed webpages and images
- **13B/day** analyzed security events

Intelligence • Integration • Expertise



In this “new normal”, organizations need an intelligent view of their security posture

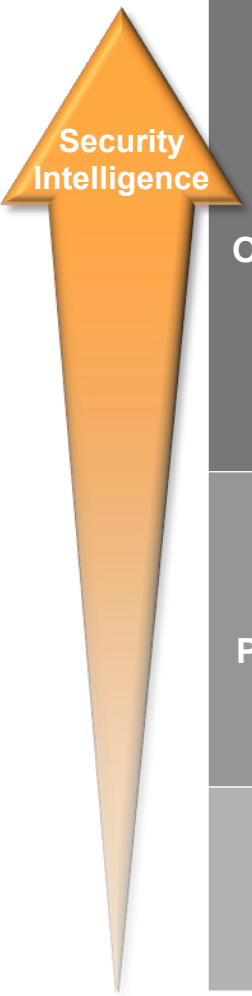


Basic
Organizations employ ***perimeter protection***, which regulates access and feeds manual reporting

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

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

Controls-based view of IBM solutions driving Security Intelligence



	Security Intelligence: Flow analytics / predictive analytics Security information and event management Log management			
Optimized	Identity governance Fine-grained entitlements Privileged user management	Data governance Encryption key management	Fraud detection Hybrid scanning and correlation	Multi-faceted network protection Anomaly detection Hardened systems
Proficient	User provisioning Access management Strong authentication	Data masking / redaction Database activity monitoring Data loss prevention	Web application protection Source code scanning	Virtualization security Asset management Endpoint / network security management
Basic	Directory management	Encryption Database access control	Application scanning	Perimeter security Host security Anti-virus
	People	**Data**	**Applications**	**Infrastructure**

12-01

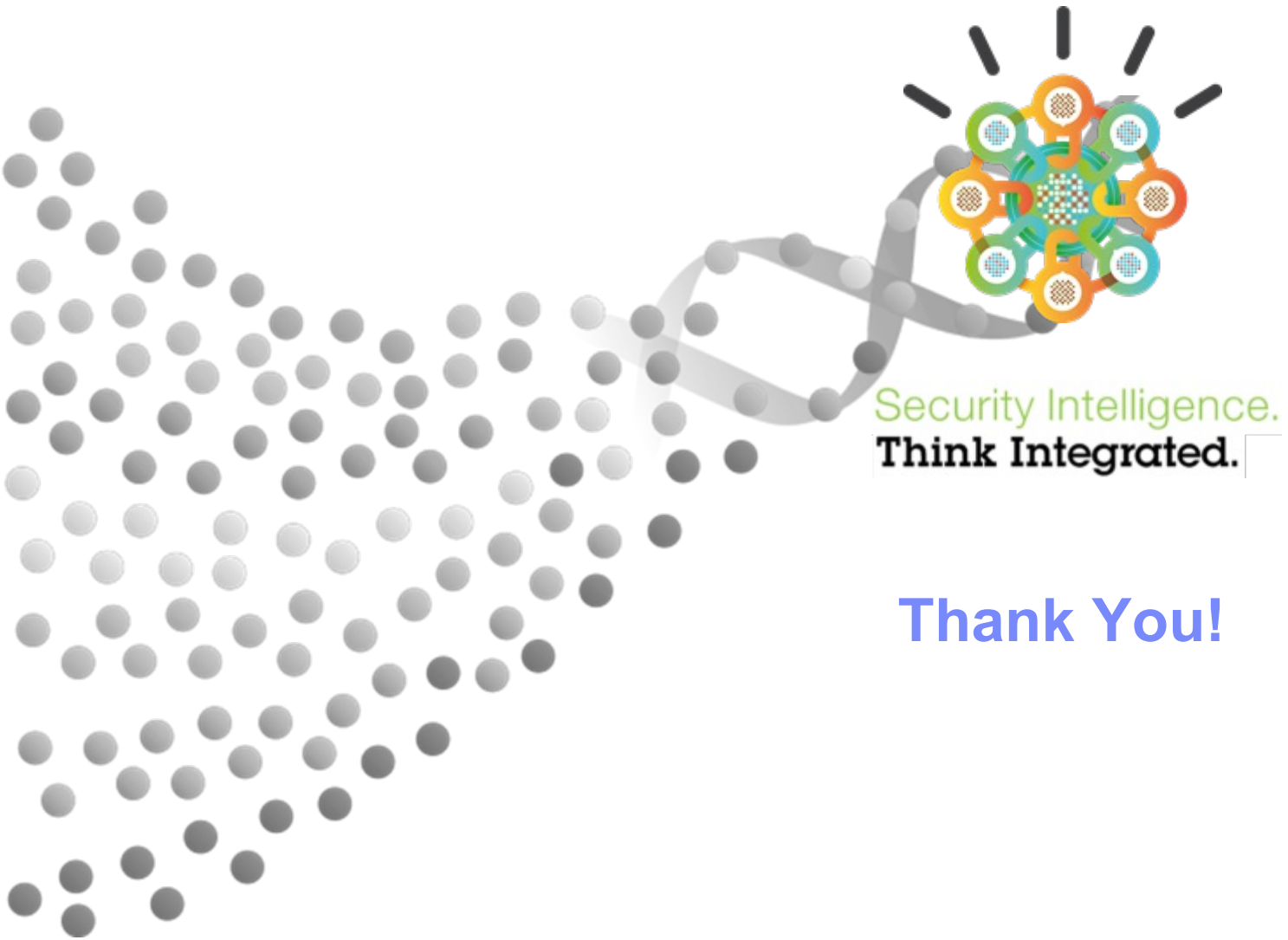
Security Intelligence, Analytics & GRC

People

Data

Applications

Infrastructure



Thank You!