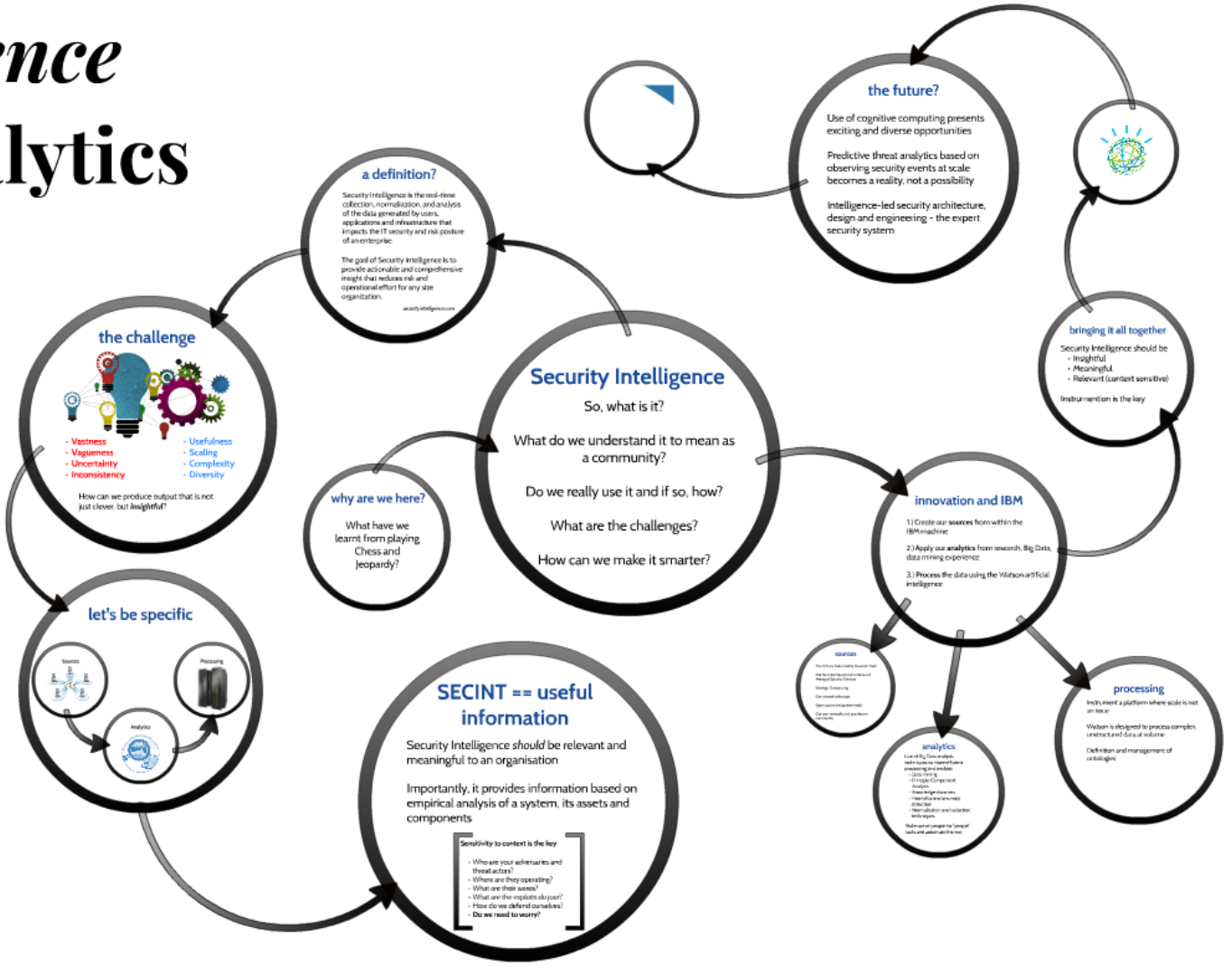
Security Intelligence in the Age of Analytics

Leigh Chase
IBM Security Services

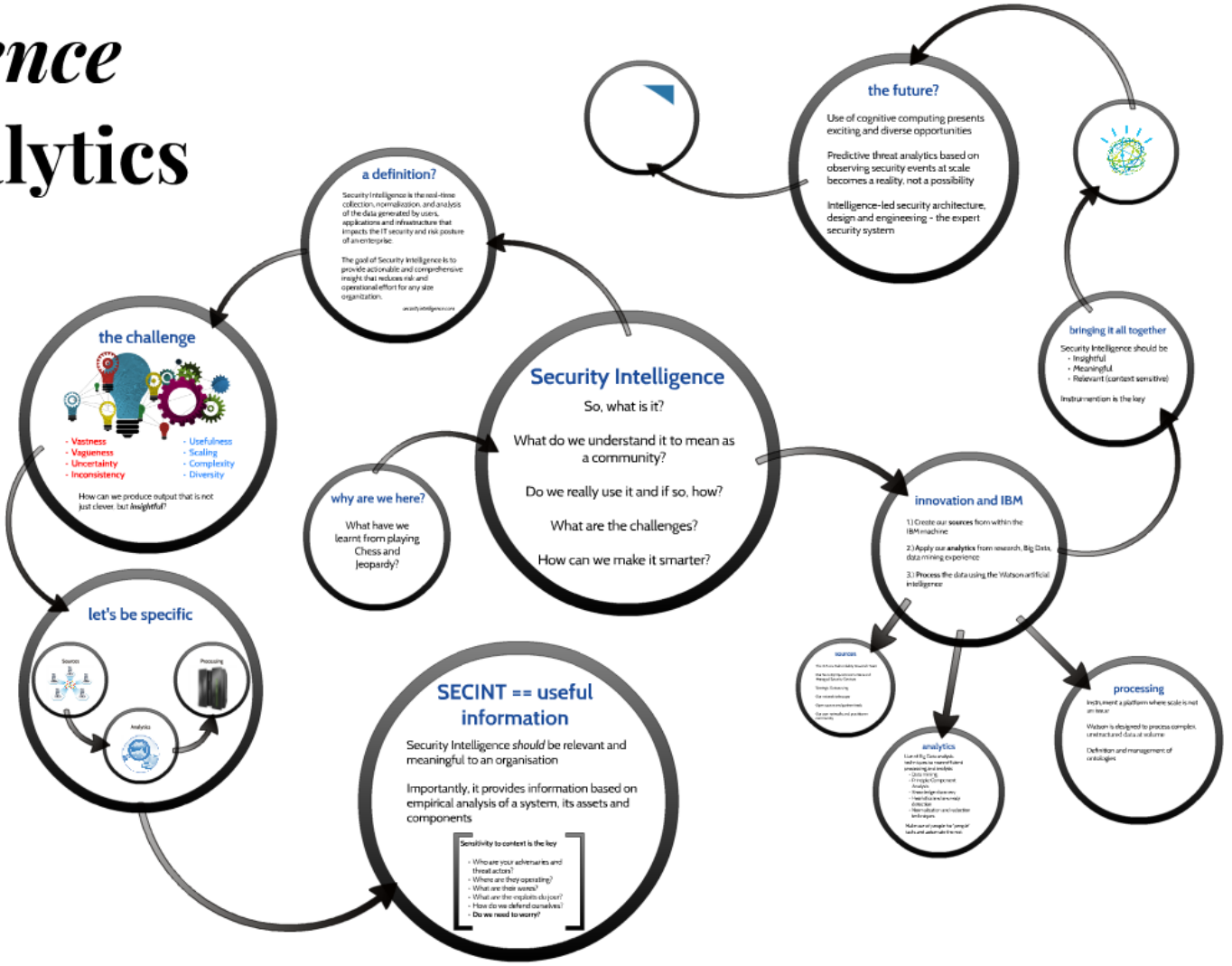


ibm.com/security

securityintelligence.com

Security Intelligence in the Age of Analytics

Leigh Chase
IBM Security Services



ibm.com/security

securityintelligence.com

in the Age of Ana

Leigh Chase
IBM Security Services

why are we here?

What have we learnt from playing Chess and Jeopardy?

Security Intelligence

So, what is it?

What do we understand it to mean as a community?

Do we really use it and if so, how?

What are the challenges?

How can we make it smarter?

a definition?

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

The goal of Security Intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort for any size organization.

securityintelligence.com

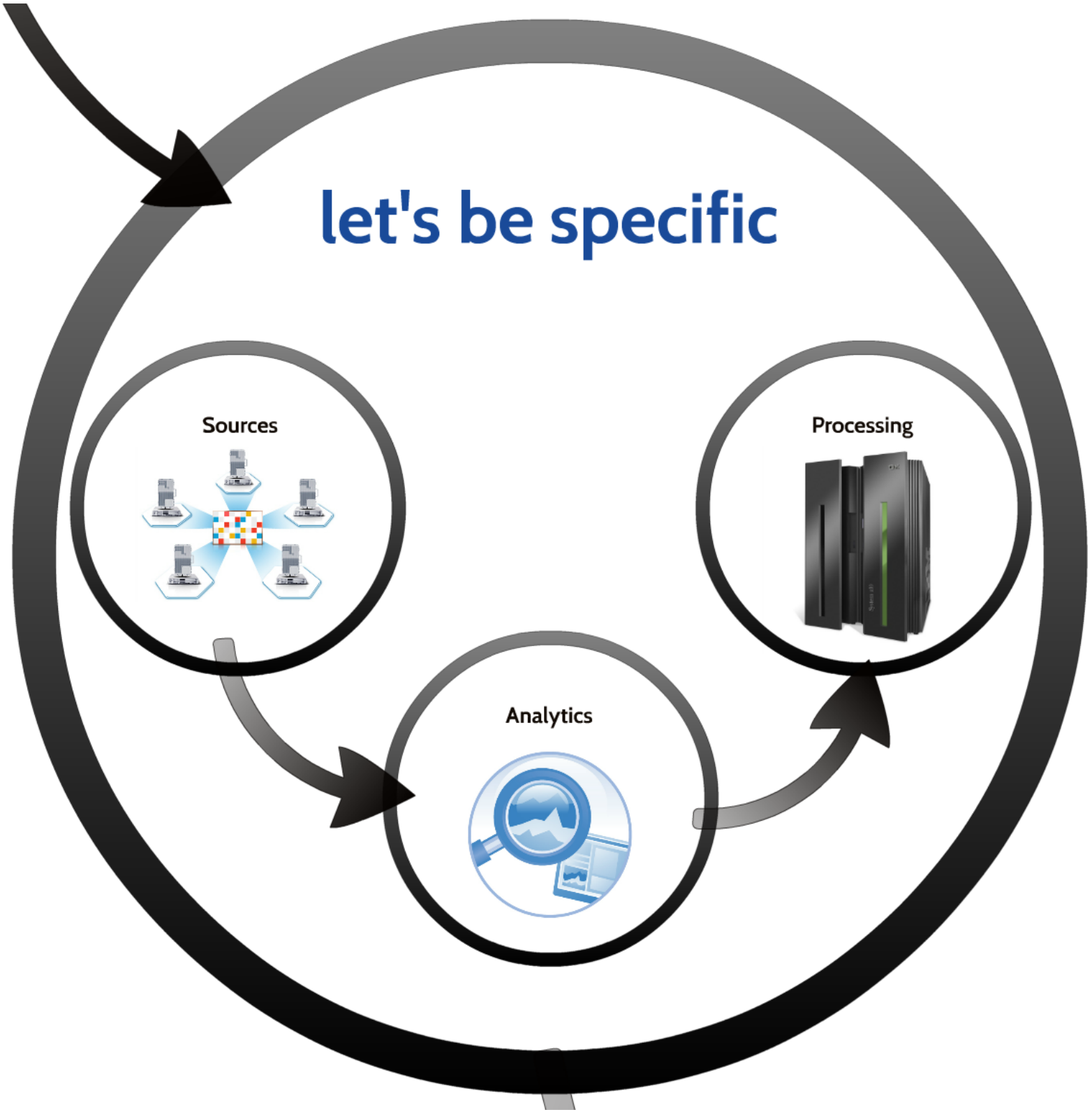
the challenge

- Vastness
- Vagueness
- Uncertainty
- Inconsistency

- Usefulness
- Scaling
- Complexity
- Diversity

How can we produce output that is not just clever, but ***insightful***?

let's be specific



SECINT == useful information

Security Intelligence *should* be relevant and meaningful to an organisation

Importantly, it provides information based on empirical analysis of a system, its assets and components

Sensitivity to context is the key

- Who are your adversaries and threat actors?
- Where are they operating?
- What are their wares?
- What are the exploits du jour?
- How do we defend ourselves?
- **Do we need to worry?**

Sensitivity to context is the key

- Who are your adversaries and threat actors?
- Where are they operating?
- What are their wares?
- What are the exploits du jour?
- How do we defend ourselves?
- **Do we need to worry?**

Security Intelligence

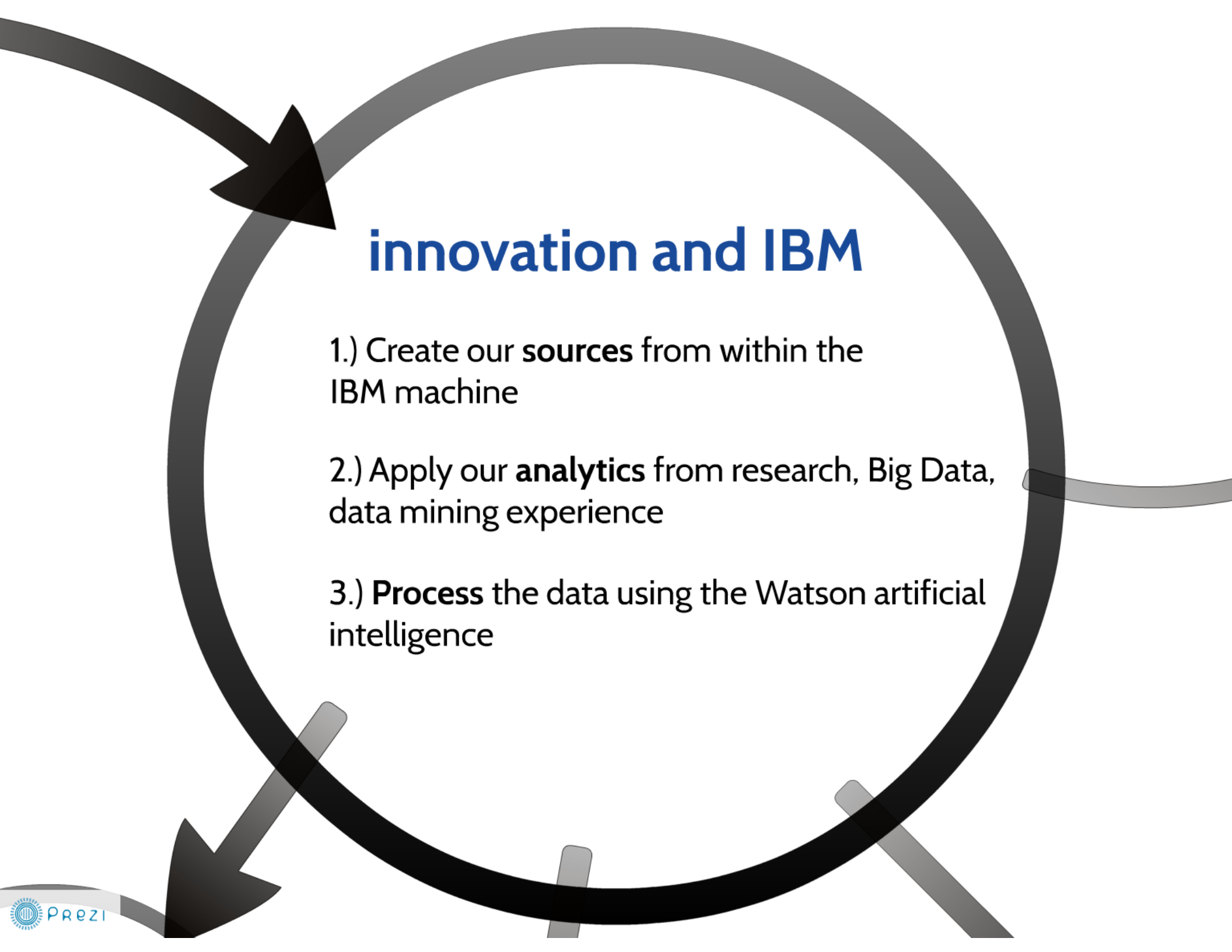
So, what is it?

What do we understand it to mean as a community?

Do we really use it and if so, how?

What are the challenges?

How can we make it smarter?


innovation and IBM
1.) Create our **sources** from within the IBM machine
2.) Apply our **analytics** from research, Big Data, data mining experience
3.) **Process** the data using the Watson artificial intelligence

sources

The X-Force Vulnerability Research Team

Our Security Operations Centres and Managed Security Services

Strategic Outsourcing

Our network telescope

Open source and partner feeds

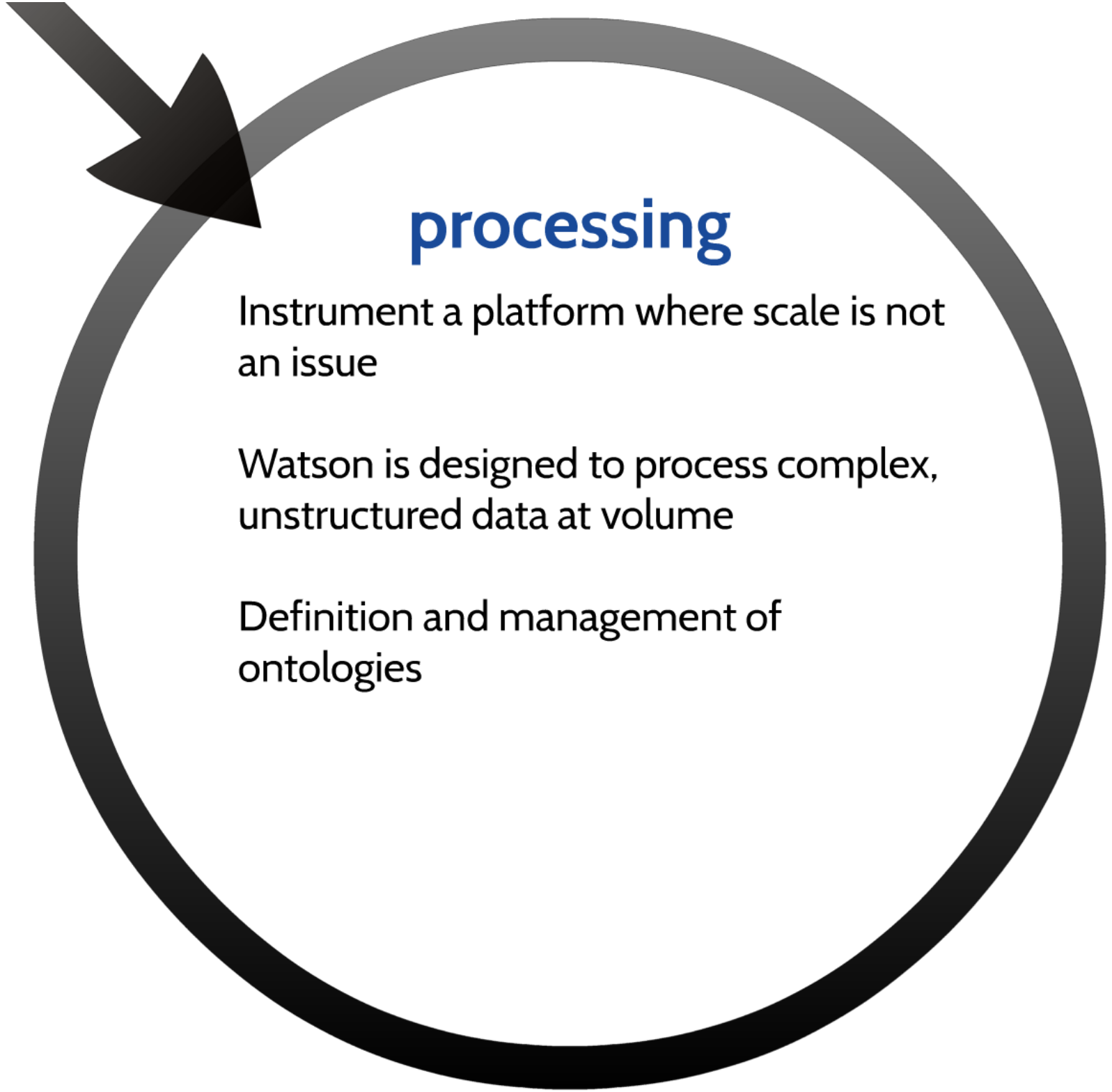
Our own networks and practitioner community

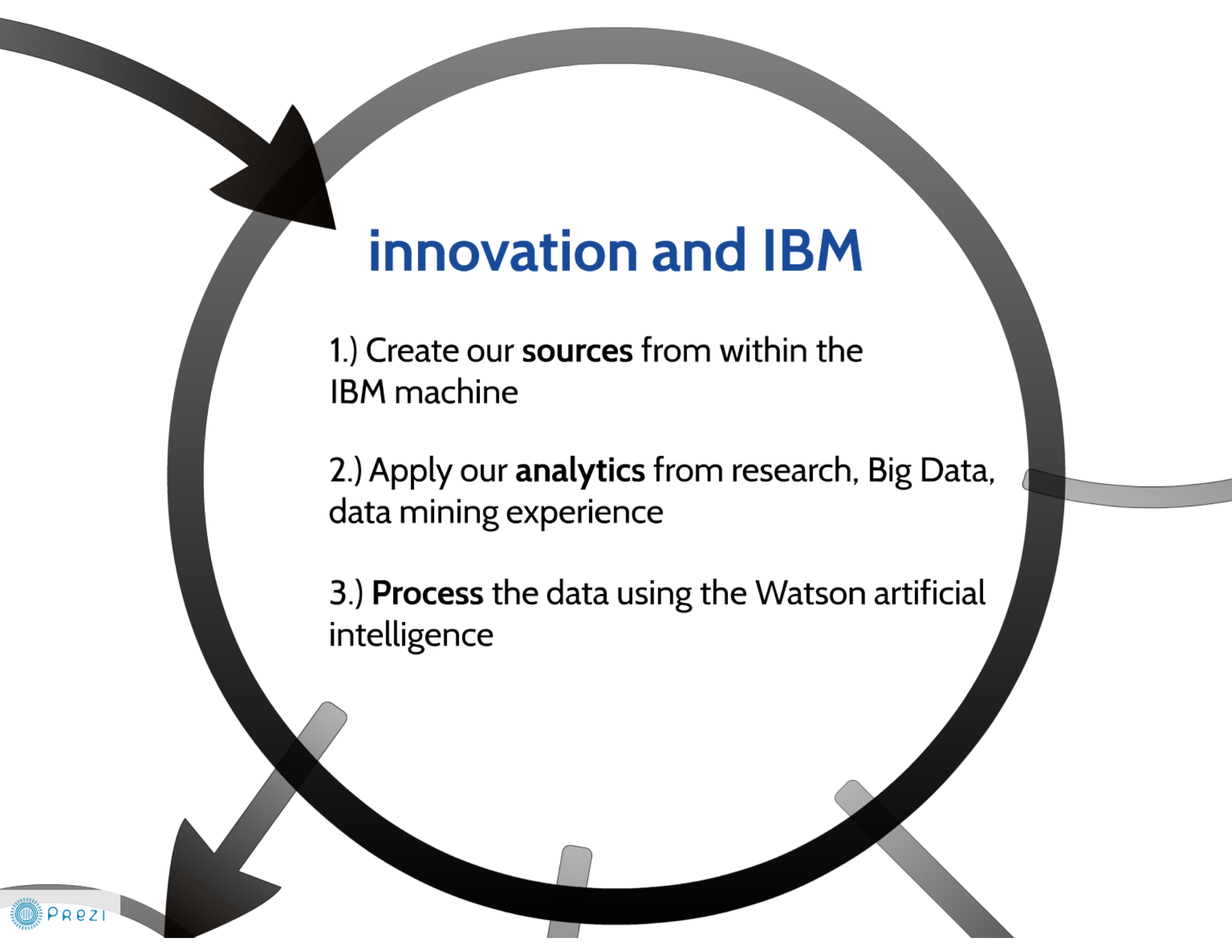
analytics

Use of Big Data analysis techniques to more efficient processing and analysis

- Data mining
- Principle Component Analysis
- Knowledge discovery
- Heuristics and anomaly detection
- Normalisation and reduction techniques

Make use of people for 'people' tasks and automate the rest


processing
Instrument a platform where scale is not an issue
Watson is designed to process complex, unstructured data at volume
Definition and management of ontologies

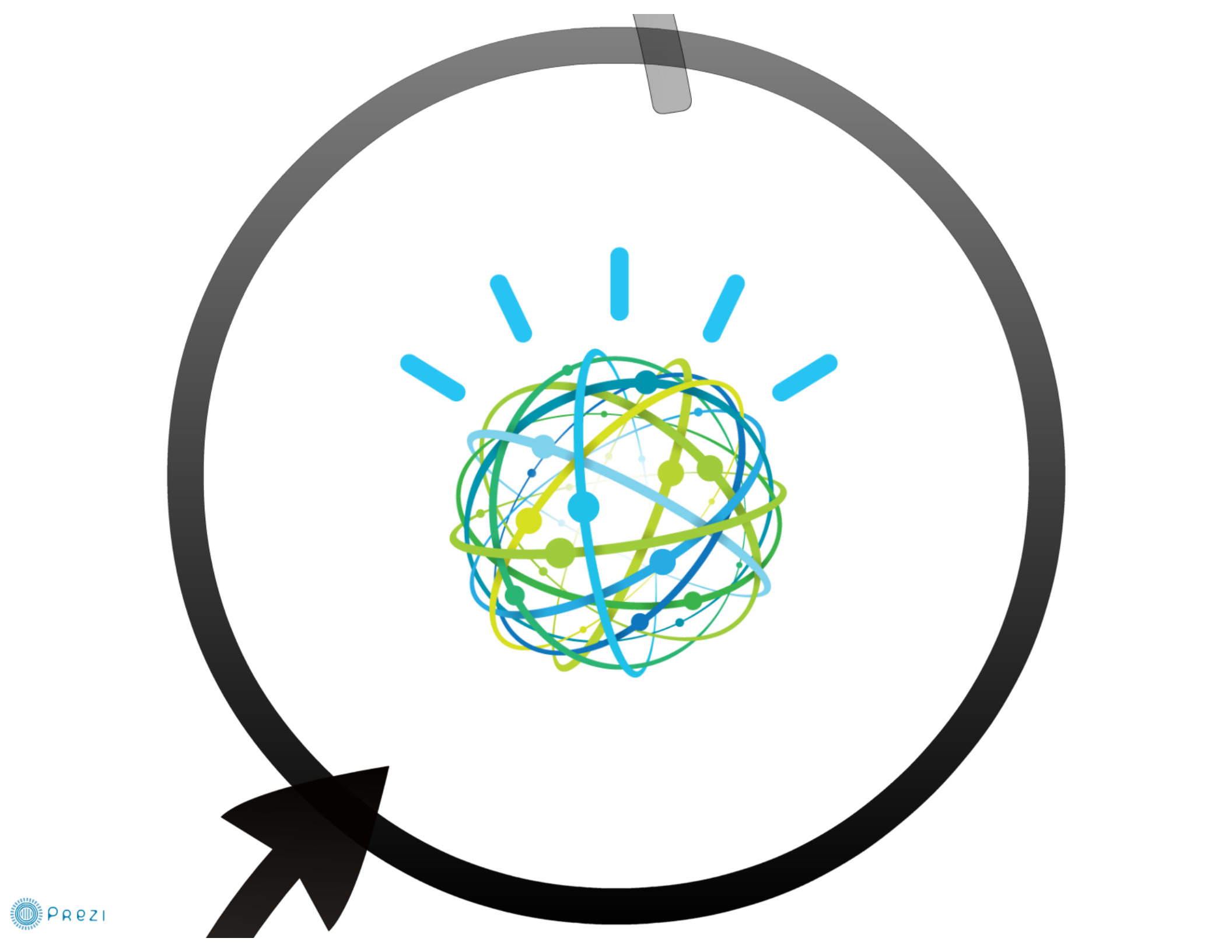

innovation and IBM
1.) Create our **sources** from within the IBM machine
2.) Apply our **analytics** from research, Big Data, data mining experience
3.) **Process** the data using the Watson artificial intelligence

bringing it all together

Security Intelligence should be

- Insightful
- Meaningful
- Relevant (context sensitive)

Instrumention is the key



the future?

Use of cognitive computing presents exciting and diverse opportunities

Predictive threat analytics based on observing security events at scale becomes a reality, not a possibility

Intelligence-led security architecture, design and engineering - the expert security system

ibm.com/security

securityintelligence.com