POINTDUTY
OPEN SOURCE INTELLIGENCE
DATA CAPTURE SUITE

IBM Security
Intelligence. Integration. Expertise.

Data Analytics from a Security Perspective

Presentation by:

David Dixon, IBM, UK and

Christopher Hawkes, Point Duty Pty Ltd, Australia

WINS World Institute for Nuclear Security

Scope

1. The Security Threat Domain
2. Data Analytics
3. Example Open Source Intelligence Use Case/Process
4. Questions

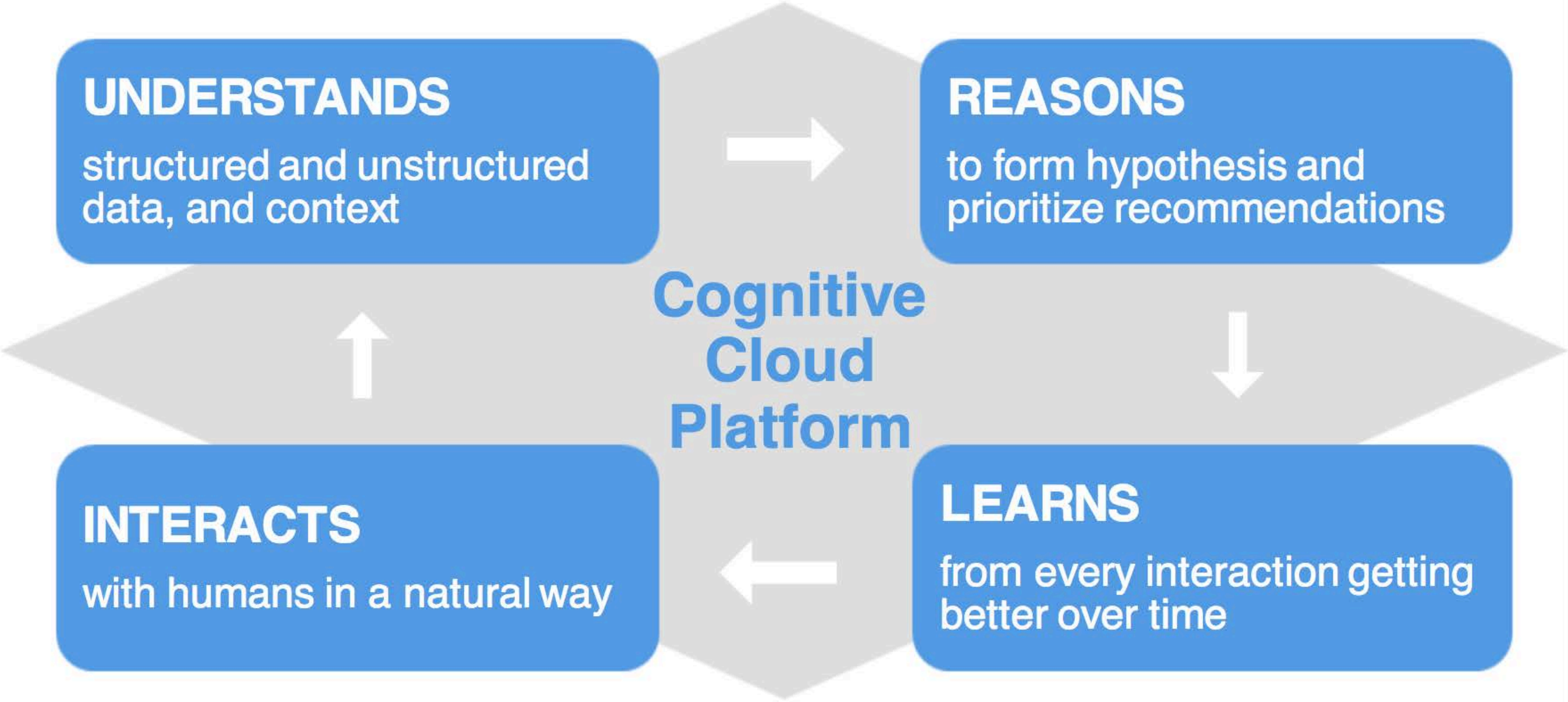
Security Threat Domain

Multiple Views of the 'Security Threat'

1. Physical and Virtual Threat to Nuclear Infrastructure
   - Physical Threat – Often Recoverable, low chance of disaster
   - Virtual Threat – Often not-recoverable and higher chance of disaster
2. Soft Threat of Data and IP Theft and Migration to Weapons Proliferation or Corporate Espionage
   - Many great examples of IP and Data Theft
   - Academics a source of knowledge loss and a target of influence… or just a target.
3. Ideological Shift against Nuclear Energy Technology
   - The ideology of all things Nuclear a shifting sands of political and social views
4. Counter Proliferation Activities
   - Those already active will remain so

Data Analytics

Cognitive means…..



UNDERSTANDS

structured and unstructured data, and context

REASONS

to form hypothesis and prioritize recommendations

LEARNS

from every interaction getting better over time

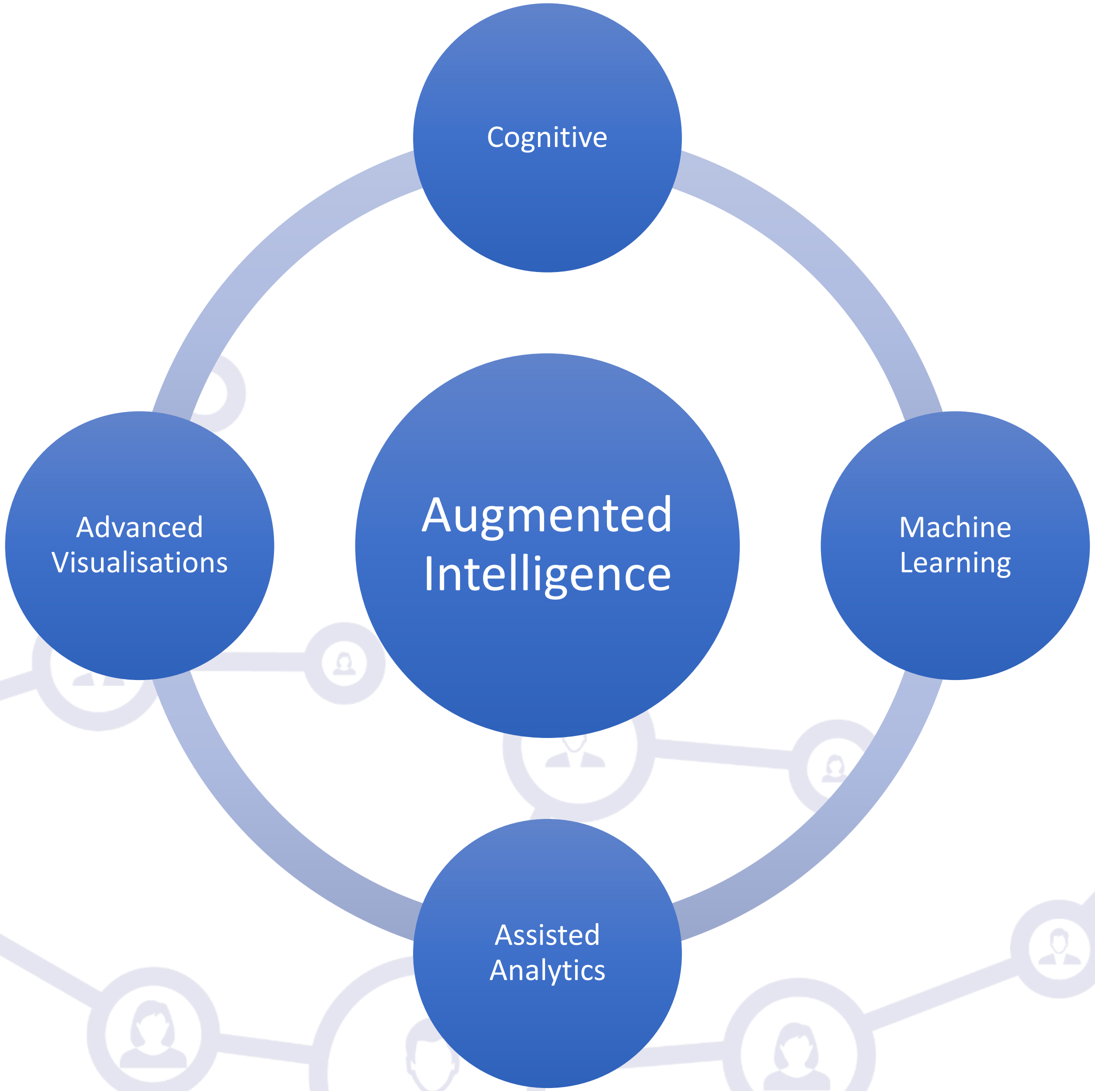
INTERACTS

with humans in a natural way

POINTDUTY
OPEN SOURCE INTELLIGENCE
DATA CAPTURE SUITE

A potential Intelligence Assistant

IBM Security
Intelligence. Integration. Expertise.



Fighting through the jargon to find the right application for the job

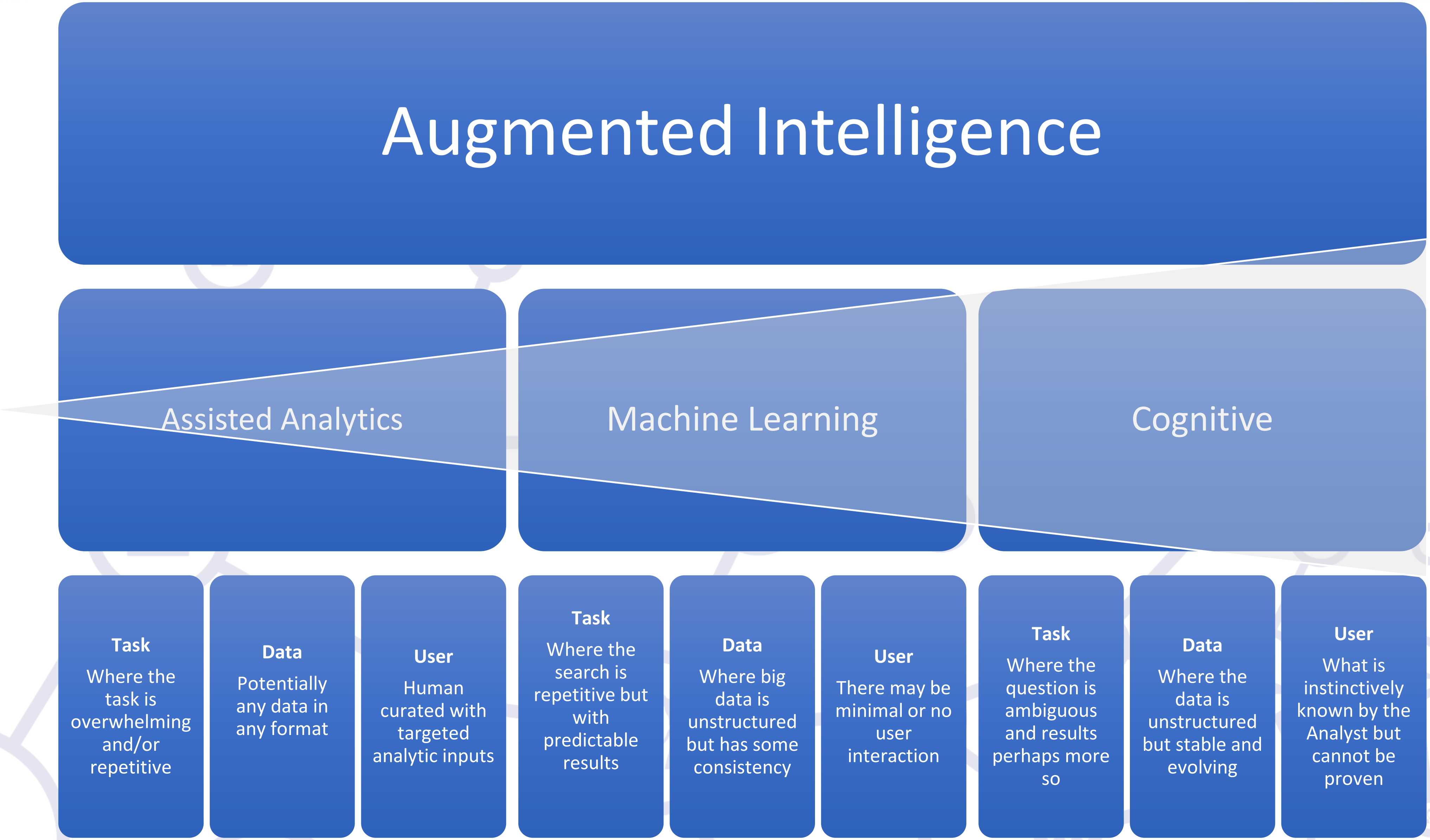
- Cognitive Computing
  - Simulation of human thought processes in a computerized model, involving self-learning systems that use data mining, pattern recognition and natural language processing to mimic the way the human brain works; makes a new class of problems computable, addressing **complex situations** that are characterized by ambiguity and uncertainty
- Machine Learning
  - Giving computers the ability to learn without being explicitly programmed; a method of data analysis that automates analytical model building, using algorithms that iteratively learn from data to find **hidden insights** without being explicitly programmed where to look

- Assisted Analytics
  - Combines a rules based approach with human generated algorithms to identify outliers and non-obvious insights based upon historical information and the expertise of the creator of the analytic.
- Advanced Visualisations
  - Allows a human to understand data with multiple dimensions to identify patterns and other insights based upon their experience and intuition

POINTDUTY
OPEN SOURCE INTELLIGENCE
DATA CAPTURE SUITE

Aligning the characteristics of tasks against capability

IBM Security
Intelligence. Integration. Expertise.



Augmented Intelligence

Assisted Analytics

Task
Where the task is overwhelming and/or repetitive

Data
Potentially any data in any format

User
Human curated with targeted analytic inputs

Machine Learning

Task
Where the search is repetitive but with predictable results

Data
Where big data is unstructured but has some consistency

User
There may be minimal or no user interaction

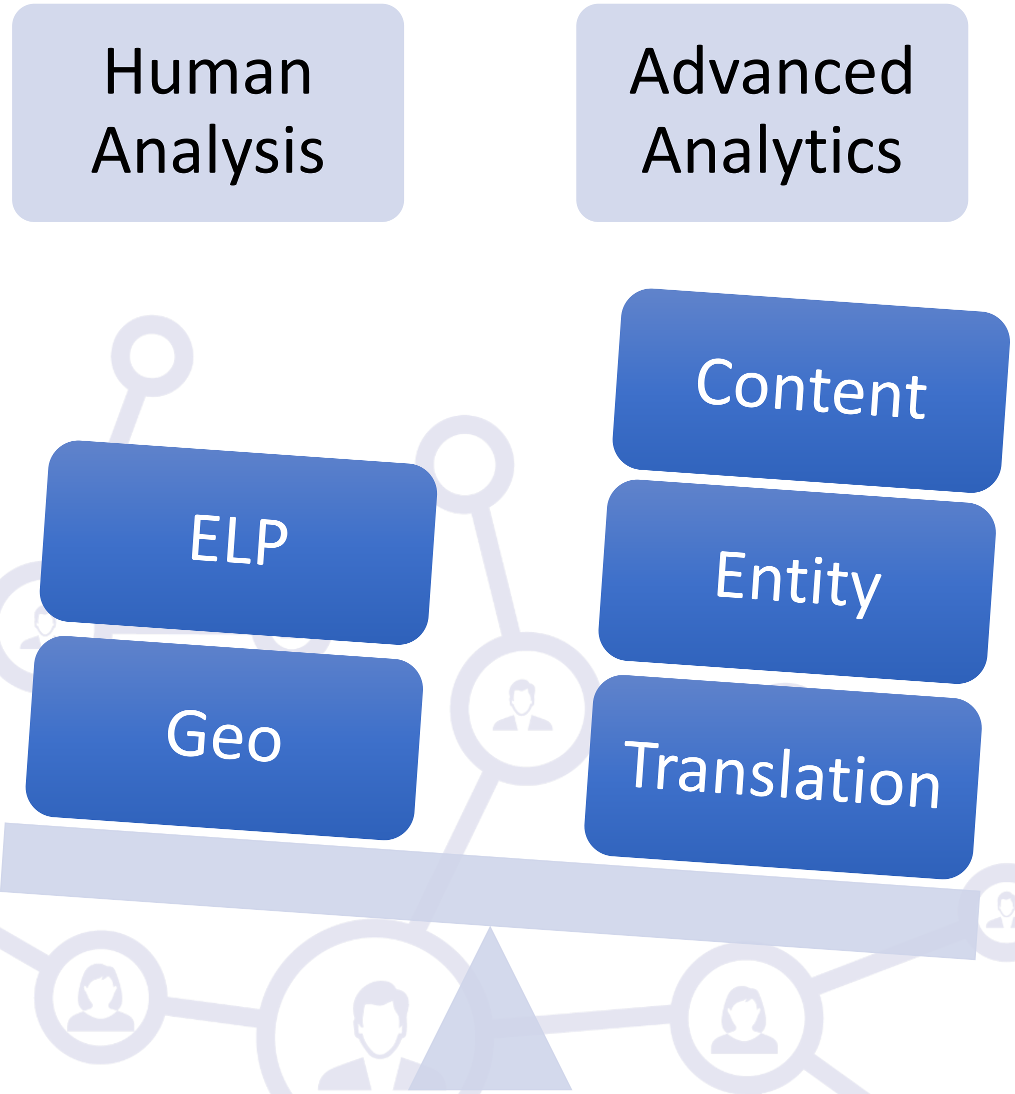
Cognitive

Task
Where the question is ambiguous and results perhaps more so

Data
Where the data is unstructured but stable and evolving

User
What is instinctively known by the Analyst but cannot be proven

Where are we today……



Human Analysis

Advanced Analytics

ELP

Geo

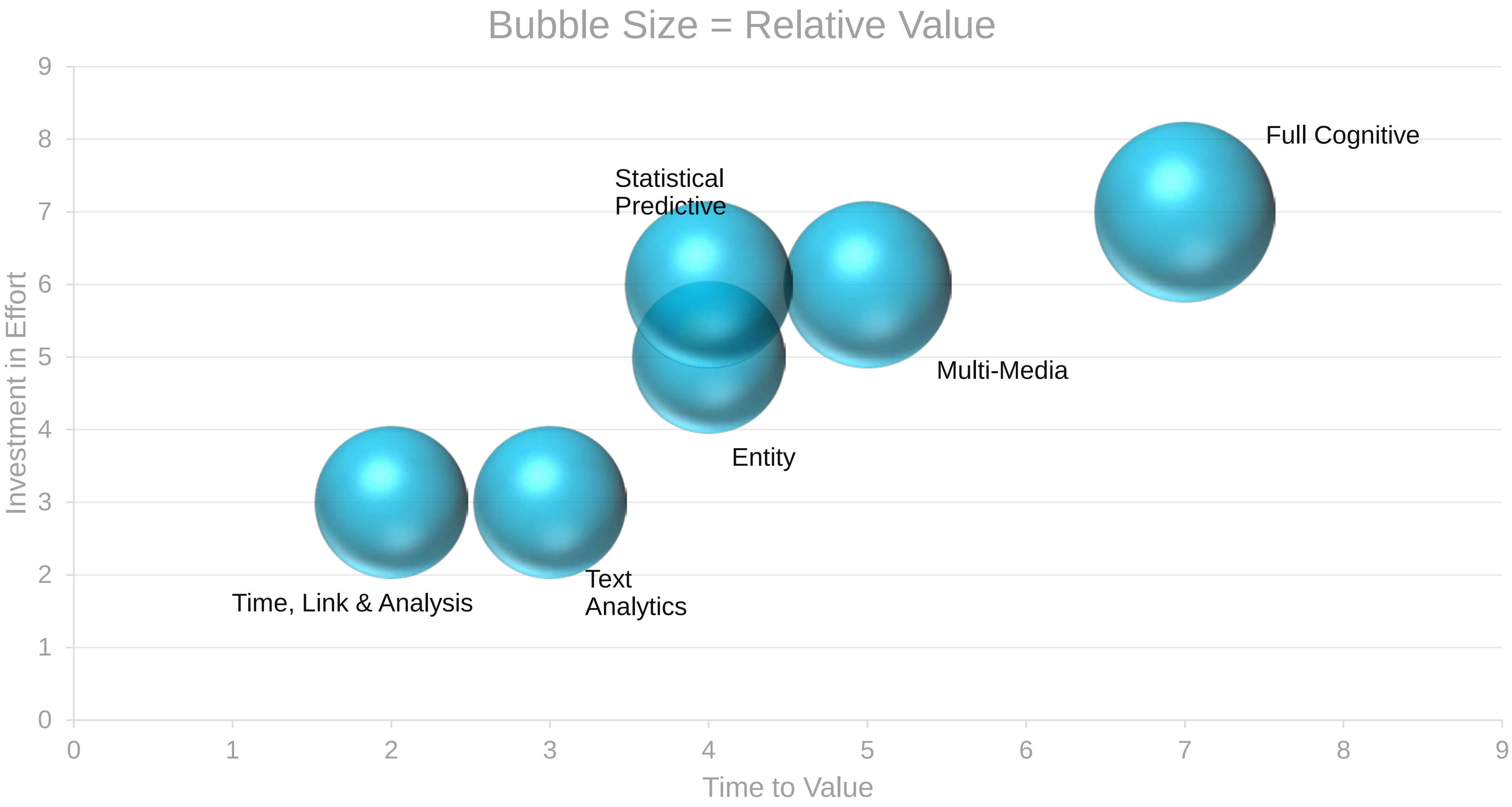
Content

Entity

Translation

Significant benefits but the dependency on new skill sets is escalating….

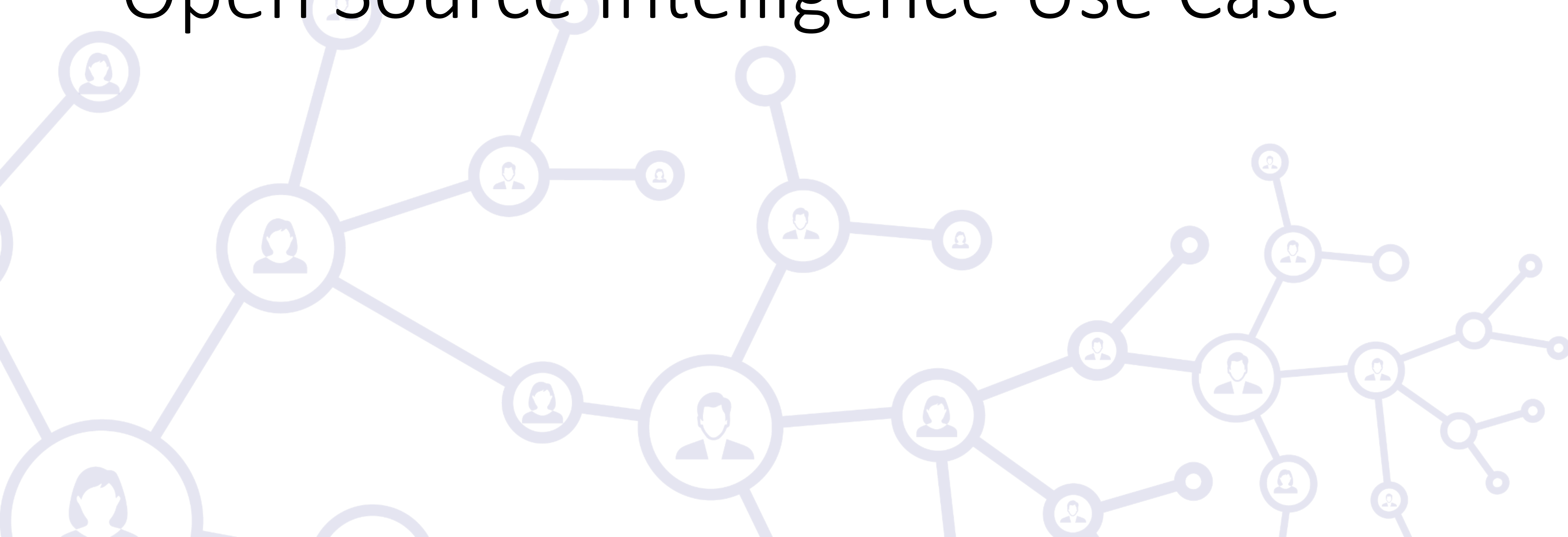
Trading off time, investment and value



POINTDUTY
OPEN SOURCE INTELLIGENCE
DATA CAPTURE SUITE

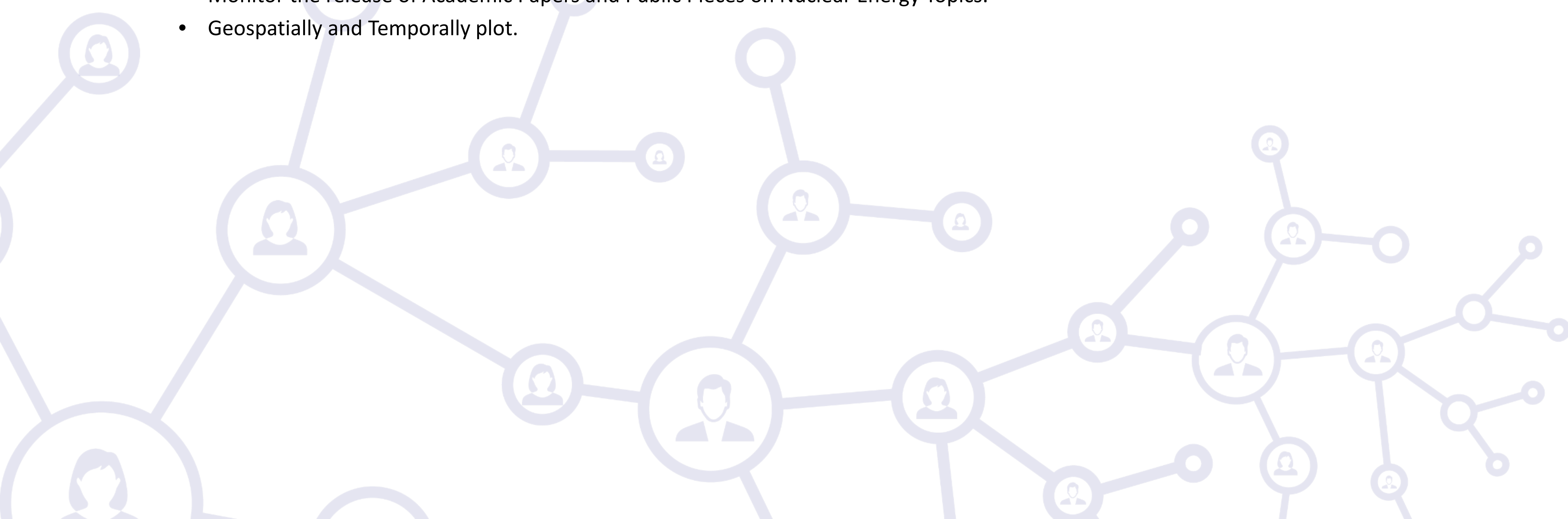
IBM Security
Intelligence. Integration. Expertise.

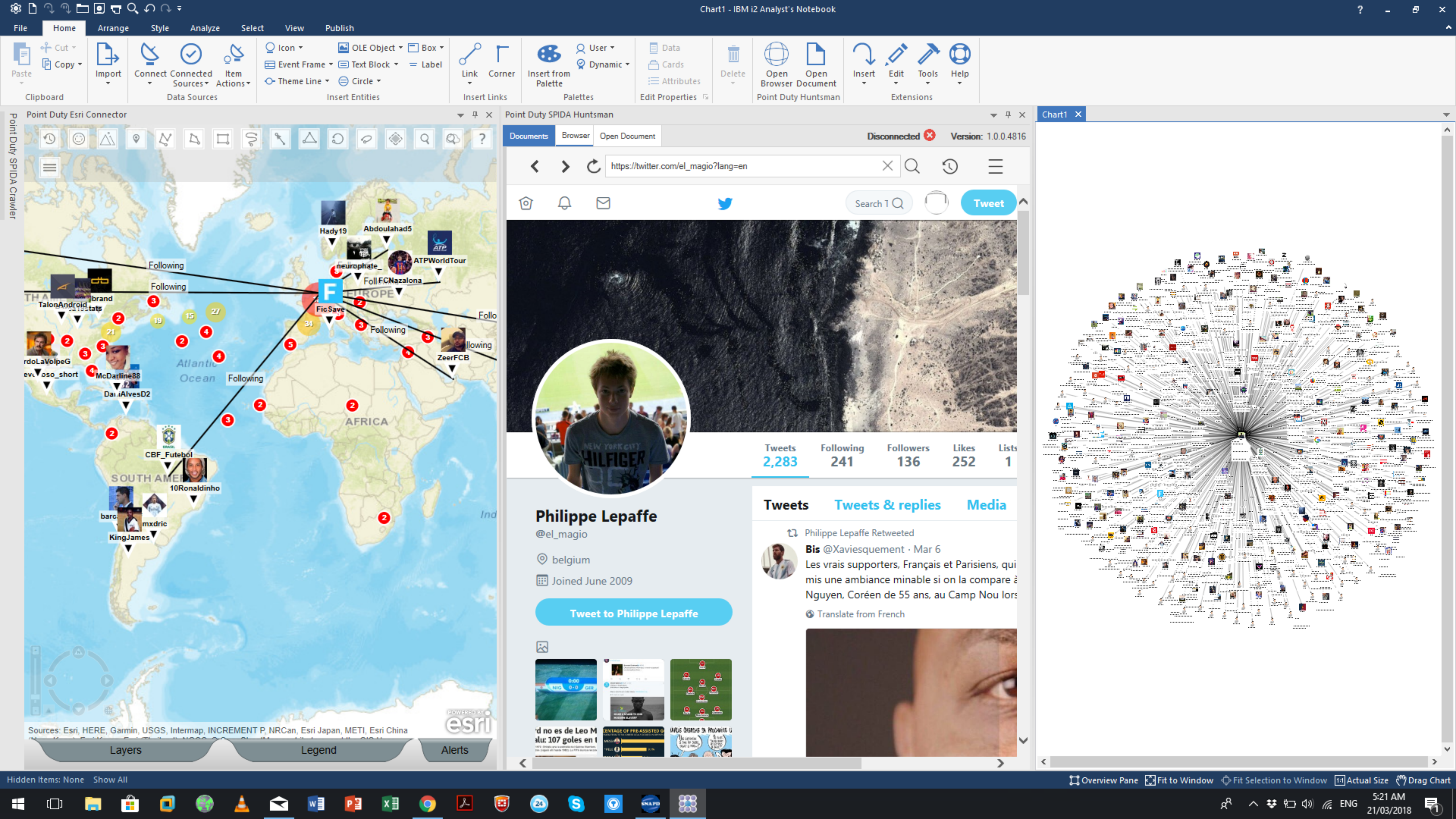
Open Source Intelligence Use Case



Use Case/Process – OSINT Scenario

1. Processes
   - Identify Students in a region who study Nuclear Physics, associate with known Physicists or Engineers, Establish their group of Friends and Group them.
   - Identify any sensitive files from your organisation and see if they exist in the P2P networks, or Deep and Dark Web.
   - Analyse and Monitor web content that is across the spectrum of Nuclear Ideals and Identify influencers in both directions.
   - Monitor the release of Academic Papers and Public Pieces on Nuclear Energy Topics.
   - Geospatially and Temporally plot.





Disconnected Version: 1.0.0.4816

https://twitter.com/el_magio?lang=en

Tweets	Following	Followers	Likes	Lists
2,283	241	136	252	1

Philippe Lepaffe
@el_magio

belgium

Joined June 2009

Philippe Lepaffe Retweeted

Bis @Xaviesquement · Mar 6

Les vrais supporters, Français et Parisiens, qui mis une ambiance minable si on la compare à Nguyen, Coréen de 55 ans, au Camp Nou lors

Translate from French

Sources: Esri, HERE, Garmin, USGS, Intermap, INCREMENT P, NRCan, Esri Japan, METI, Esri China

Hidden Items: None Show All

5:21 AM
21/03/2018

Questions and Discussion