



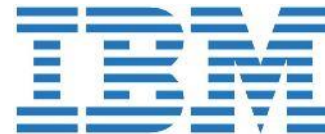
# Turn Your Overwhelming Data into Actionable Intelligence

**December 09, 2014**

---

Moderator:  
Steve LeSueur  
Contributing Editor,  
1105 Public Sector Media Group

Sponsored by:



IBM i2

# IBM i2 Enterprise Insight Analysis

for Cyber Intelligence



# Agenda

1

Setting the stage

2

Realities and current challenges

3

Attributes of the market and targeted industry

4

Solution definition and benefits

5

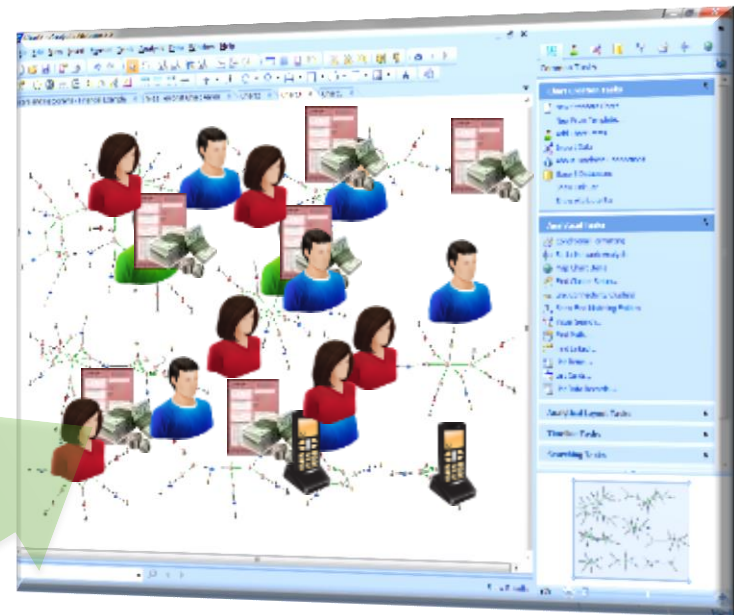
Solution takeaways

## Data by the numbers

- Over 100 terabytes of information
- 1.7 million unique geospatial entities
- Over 100 million unique phone numbers
- Over 120 million unique identities
- 1 billion records per day ingested
- Over 1 billion entities: people, locations, vehicles, organizations and so on
- Over 1 trillion call data records

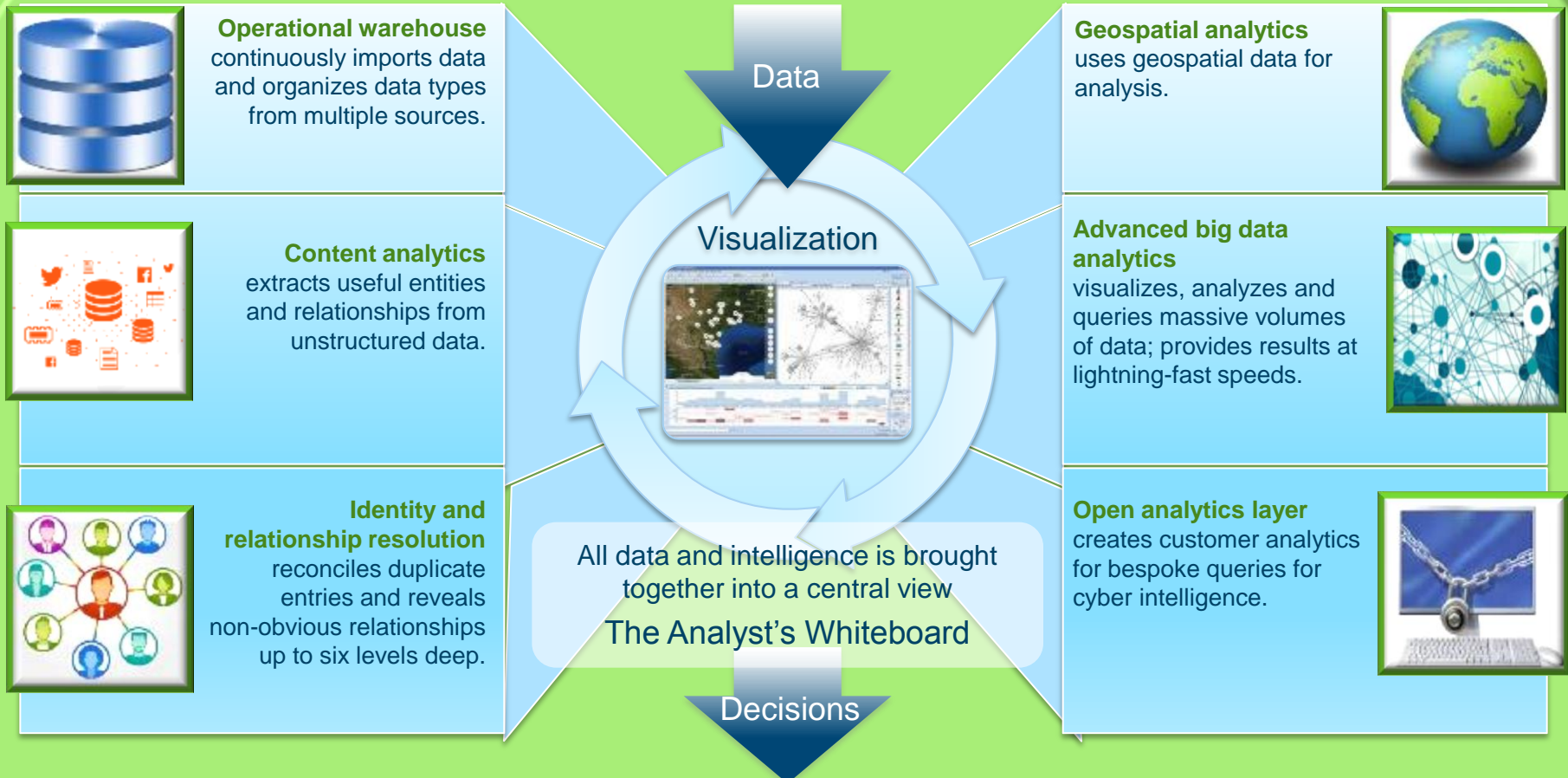
Source: <enter source of facts here>

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1																										
2																										
3																										
4																										
5																										
6																										
7																										
8																										
9																										
10																										
11																										
12																										
13																										
14																										
15																										
16																										
17																										
18																										
19																										
20																										
21																										
22																										
23																										
24																										
25																										
26																										
27																										
28																										
29																										
30																										
31																										
32																										
33																										
34																										
35																										
36																										
37																										
38																										
39																										
40																										
41																										
42																										
43																										
44																										
45																										
46																										
47																										
48																										
49																										
50																										



One goal: Transform  
overwhelming data feeds  
into actionable intelligence

# Introducing IBM i2 Enterprise Insight Analysis



Accelerate the data-to-decision process  
by turning overwhelming data into insights.

## Why the environment is changing so fast



### Internet of things

The amount of devices on a network is expanding exponentially, resulting in more ways to gain unauthorized access.



### Shortage of talent

The cost of skilled personnel is rising, while cyber talent is at an abundant shortage. There is a shortage of skilled security people, security people who can actually 'do' security versus pass a multiple-choice test on security.<sup>1</sup>



### Sophistication of the attackers

“But, cyber attacks are growing every day in strength and velocity across the globe.” — Jamie Dimon, JPMorgan’s chairman and Chief Executive <sup>2</sup>



### Big data

Organizations need to be able to “make sense” of multiple silos of cyber data and provide the ability to predict attacks before an occurrence.

1. Bob Violino, “Today’s top skill sets in security -- and why they’re in demand,” *CSO Online*, 18 June 2014: <http://www.csoonline.com/article/2365182/security-leadership/todays-top-skill-sets-in-security-and-why-theyre-in-demand.html>
2. Silver-Greenberg, JESSICA; Goldstein, Matthew; and Perloth, Nicole, “JPMorgan Chase Hacking Affects 76 Million Households,” *New York Times, Dealbook*, 2 October 2014: [http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?\\_php=true&\\_type=blogs&\\_r=1](http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=1)

## Why there is a need for actionable insight

### Traditional approach

Reactive

Time taken to achieve the desired result

Enterprise amnesia

Output difficult to explain

Custom solutions, hard to scale

### Intelligent approach

Proactive

Results achieved in seconds

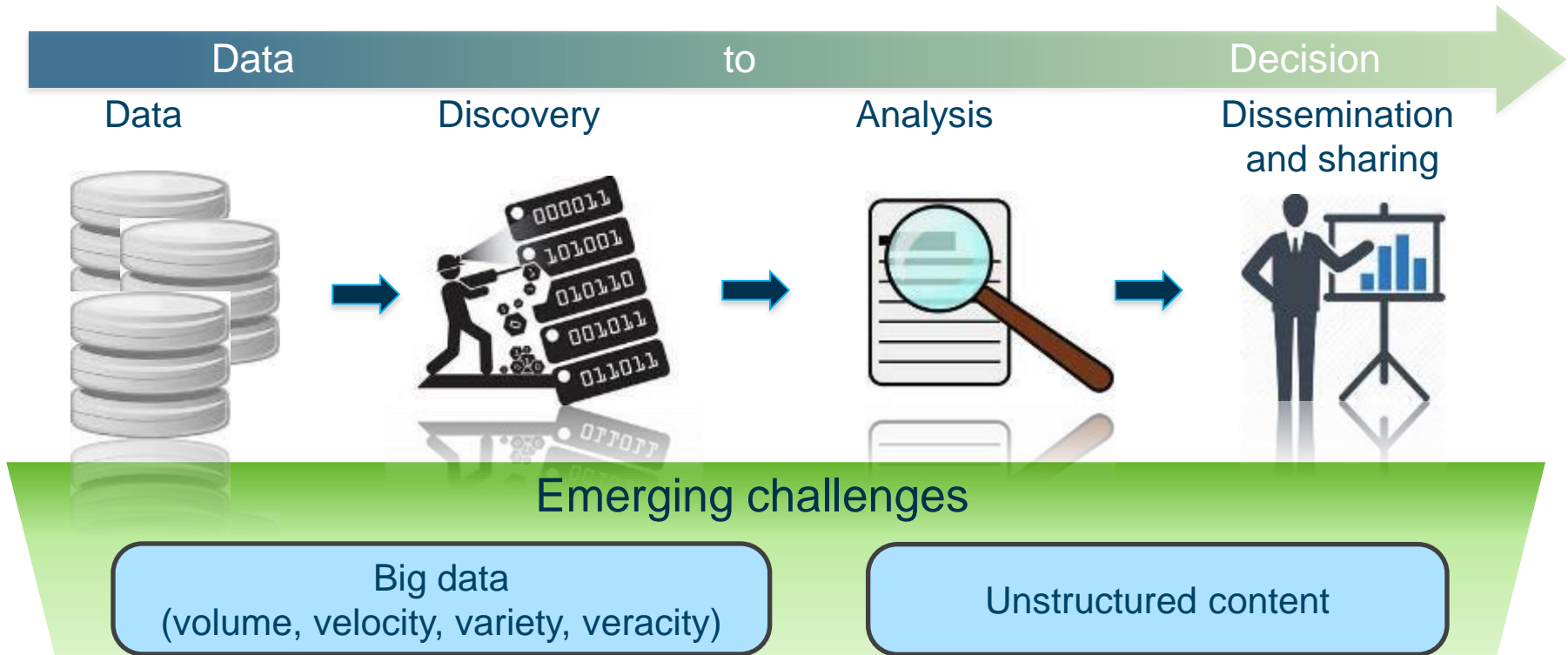
Data-to-decision support analytics

User friendly advance visualization

Flexible scalable platform



# Accelerating the data-to-decision process



- Collate, aggregate and manage **overwhelming data volumes** (terabytes) of information
- Multiple, discrete **silos** of information
- Valuable **insight locked up** in unstructured or semistructured data and documents
- Accurate and timely target acquisition (finding the needle in the needle-stack)
- Finding hidden patterns **and non-obvious relationships**, using reactive to proactive or predictive methods
- Struggling to find the who, what, when and where by **avoiding cognitive traps**
- More time information management (IM) than **information exploitation** (IE) (analysis)



## Wide application of i2 Enterprise Insight Analysis

### Retail



- Gain actionable customer insight from buying patterns in the product mix.
- Identify illegal transactions made by using black market credit cards.
- Use merchandise optimization to prevent overstock or understock issues.

### Cyber Intelligence



- Benefit from real-time analysis of ongoing breaches.
- Link information from physical and cyber events.
- Gain the ability to make accurate decisions for policy and response.

### National Security and Defense



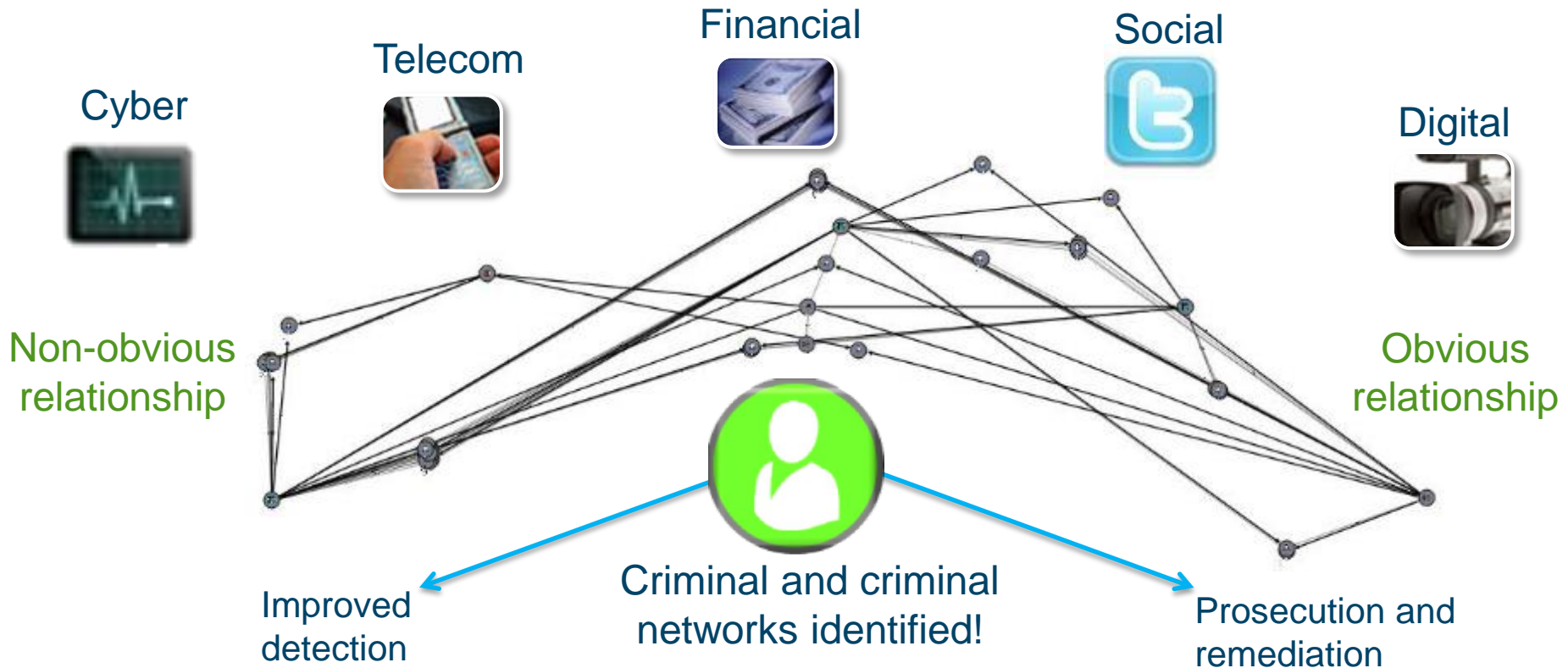
- Ingest, fuse and analyze data from multiple intelligence sources at scale and speed.
- Accelerate the data-to-decision process with actionable insights.
- Gain operational efficiencies.

### Energy & Utilities: Futures



- Develop a comprehensive understanding of system vulnerabilities and attacks on critical infrastructure.
- Identify the who, what, where, when and why.
- Mitigate and disrupt attacks.

## Holistic data analysis for true actionable insight



IBM® i2® Enterprise Insight Analysis operates against information from **across the enterprise**, uncovering hidden criminal identities (entity analytics) and criminal organizations (network analytics) that are invisible when running against individual data and **analytic silos**.

## Increases analyst efficiency



- Solution powered by an integrated data system that can handle more than 1,000 concurrent operational queries with **continuous ingest**
- 24x7 automated entity resolution and a **recommendation engine**
- Link, temporal and geospatial queries, in addition to network analytics across hundreds of **terabytes of data in seconds**
- The ability to search, automatically process and analyze **unstructured data**
- **Collaboration facilitated** between geospatial and operational intelligence analysts
- Support for **information sharing with a security rich platform**

## Increases analyst accuracy



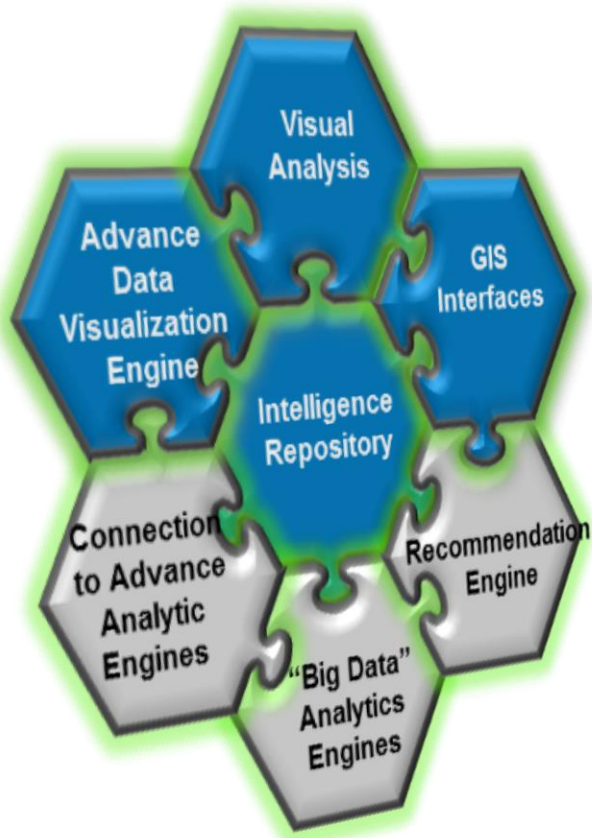
- Hypotheses testing and query data in seconds
- Uncovered relationships separated by several degrees
- Automatic alerts when data is added or altered
- Non-obvious relationship discovery by applying multidimensional visual analytics
- Temporal and network hierarchies, in addition to critical geospatial insights
- Complete, visual and situational awareness

## A cost-effective solution for operational effectiveness



- Cost effective
  - Maximize and take advantage of current infrastructures, systems and data.
  - Maintain, deploy and integrate without long-term support contracts, thanks to a commercial off-the-shelf design.
  - Improve operational and situational awareness with a dashboard and KPIs.
- Operational interoperability
  - Use other best-of-breed applications, such as Esri.
- Technical interoperability
  - Open standards-based architecture and query services.
  - Open source developer essentials (SDK).
  - Open source data connectors.

## The six S's of IBM i2 Enterprise Insight Analysis



cale to cover all your data sets



peed measured in seconds



upplemented search by using recommendation engines



etup of your own analytics



creen advance visualization



patial temporal analytics



Limitless powers to change data to decisions



IBM i2 Enterprise Insight Analysis



## Key points to keep in mind

1

It delivers a **fully engineered solution** that is not a loosely connected bundle of products.

2

It is an engineered product that accelerates the data-to-decision process at **speed** and at **scale**.

3

**Overwhelming data** is having major influences on organizations (positively and negatively).

4

Ask to see a full demo to help you explore the potential to **turn your data into actionable insight**.

## Demonstration

Data

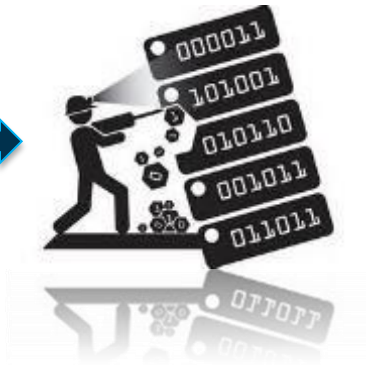
to

Decision

Data



Discovery



Analysis

Dissemination  
and sharing

# Cyber intelligence: Security alert

Security alert about unusual activity

More detailed search using cyber intelligence

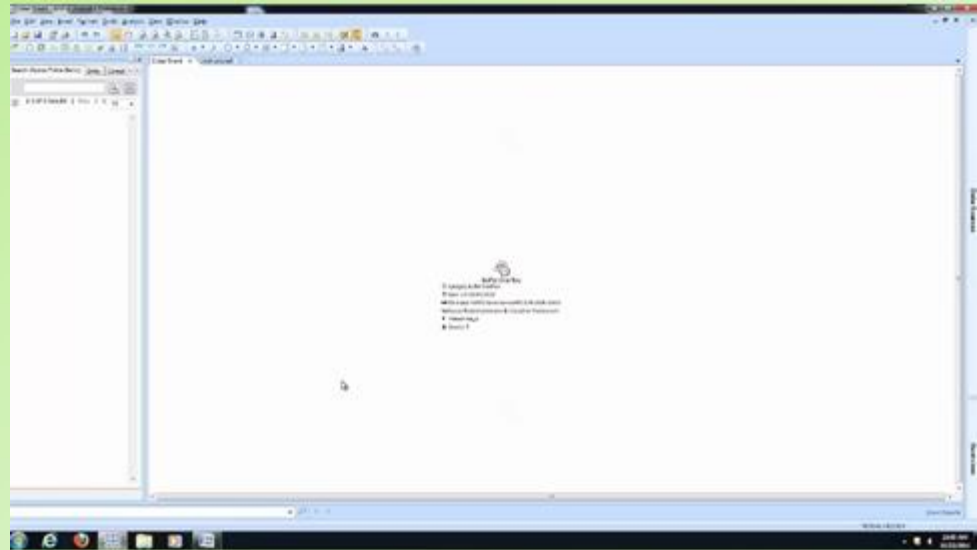
Find out who the attacker could be

Find what the attack is hiding

Find out more information about the attacker

Making it real

## Enterprise Insight Analysis



A buffer overflow is detected in one of the servers, throwing an alert, which is how most investigations usually start.

# Cyber intelligence: More detailed search

Security alert about unusual activity

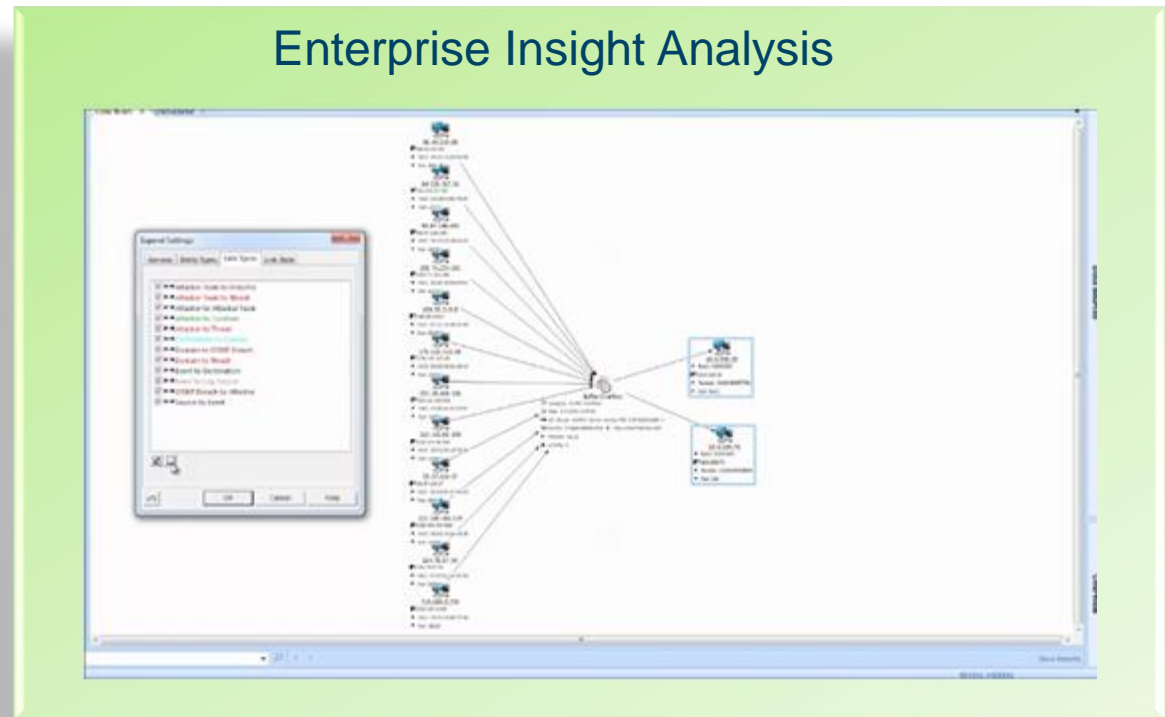
More detailed search using cyber intelligence

Find out who the attacker could be

Find out who the attacker is linked to

Find out more information about the attacker

Making it real



The analyst brings in all known related information: the attack sources and types. Domains and servers are targeted. The attack is a buffer overflow attack, targeting ports 135 and 5432.

# Cyber intelligence: Suspected attacker

Security alert about unusual activity

More detailed search using cyber intelligence

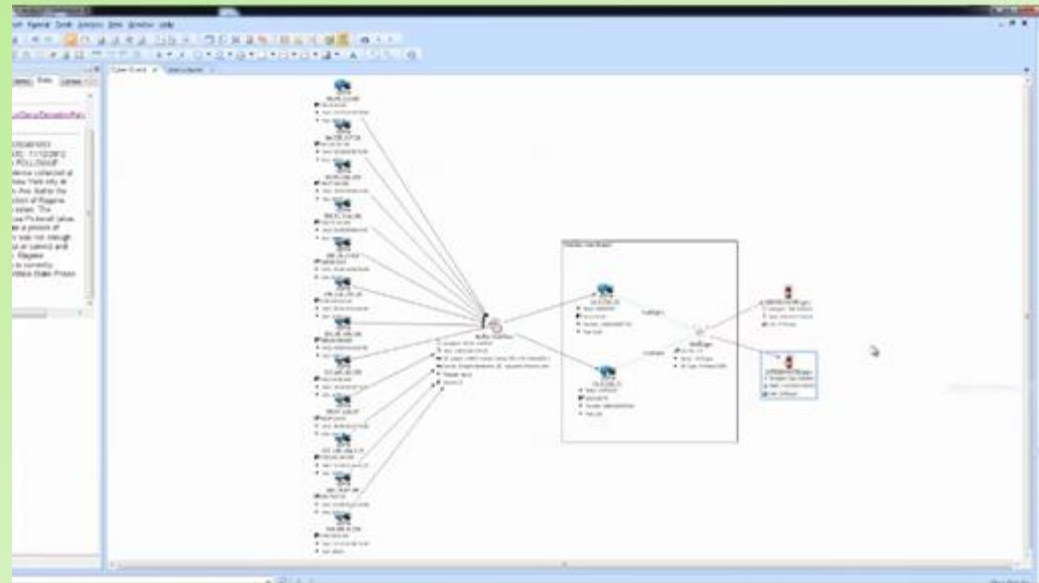
Find out who the attacker could be

Find out who the attacker is linked to

Find out more information about the attacker

Making it real

## Enterprise Insight Analysis



A new claim shows that the original attack (buffer overflow) was used to obfuscate the real attack, an SQL injection attack on port 5432. OSInt gives the real attack and an alias to the hacker claiming it.

# Cyber intelligence: Attacker links

Security alert about unusual activity

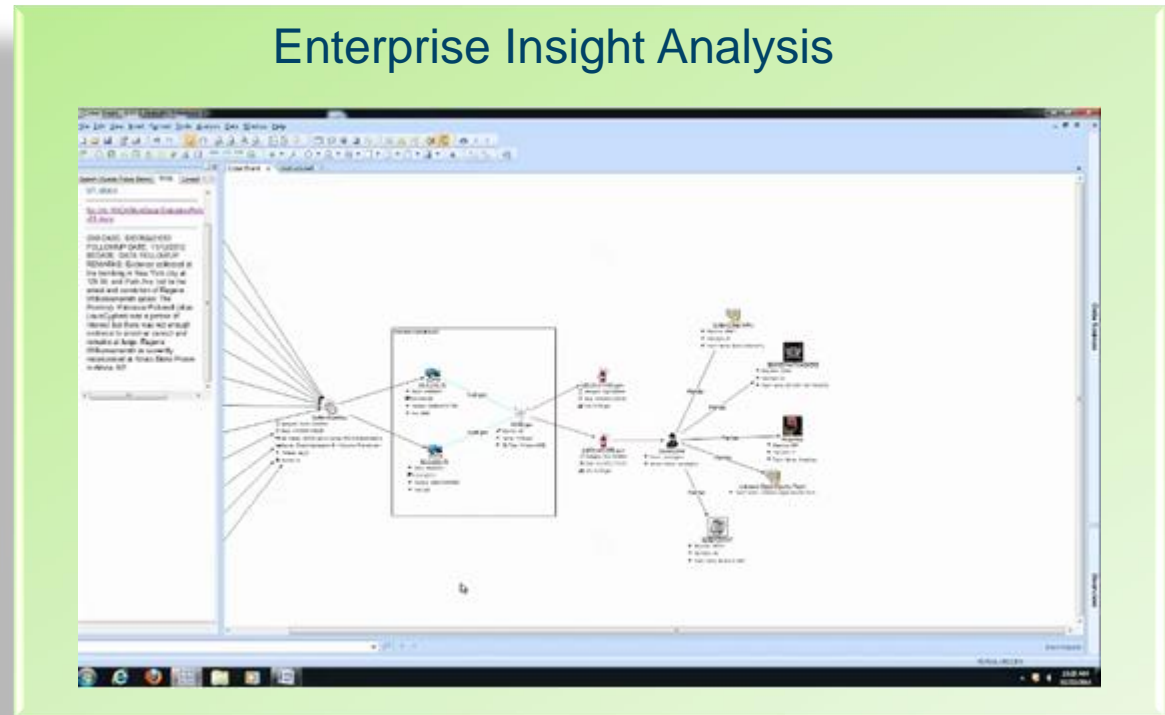
More detailed search using cyber intelligence

Find out who the attacker could be

Find out who the attacker is linked to

Find out more information about the attacker

Making it real



Network and geospatial attributes were collected by the social media crawler. The attacker location is found by plotting in the map. Social network analysis helps to find the most influential members of the network.

# Cyber intelligence: More information about the attacker

Security alert about unusual activity

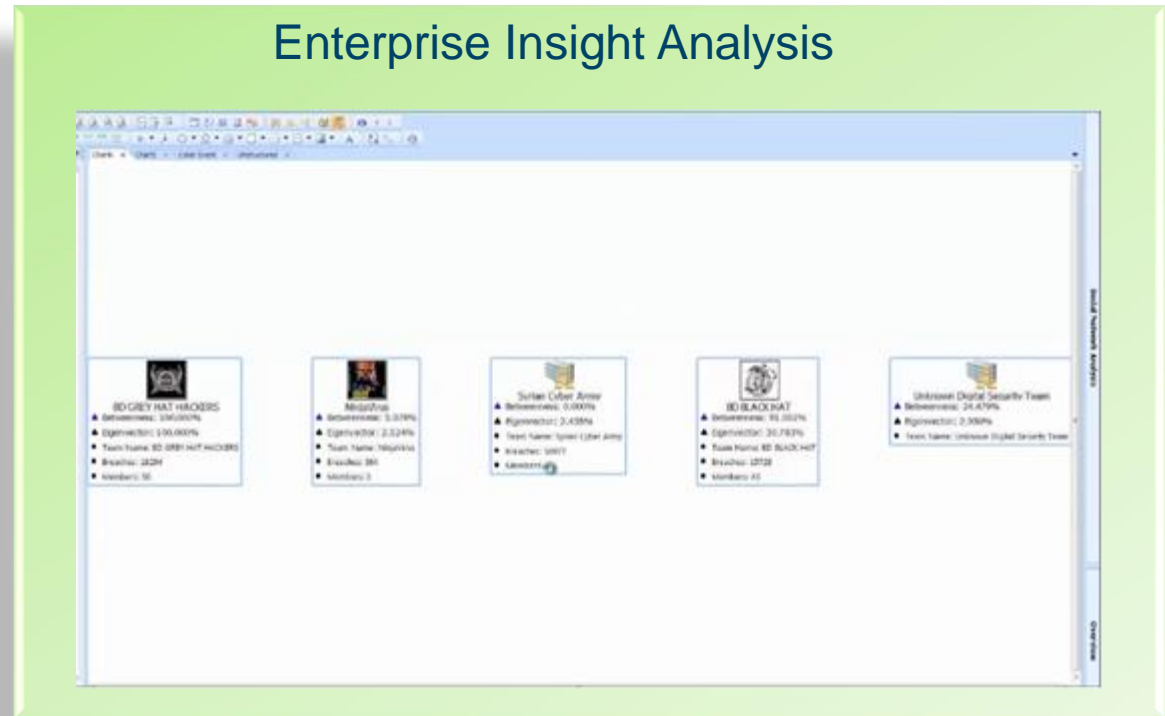
More detailed search using cyber intelligence

Find out who the attacker could be

Find out who the attacker is linked to

Find out more information about the attacker

Making it real



Combining social media crawling and IBM InfoSphere® Identity Insight, the analyst links the attacker's alias to a real name and a hacker group. OSInt data helps link threat actors and teams. In this case, the hacker is associated with five teams.



# Cyber intelligence: Making it real

Security alert about unusual activity

More detailed search using cyber intelligence

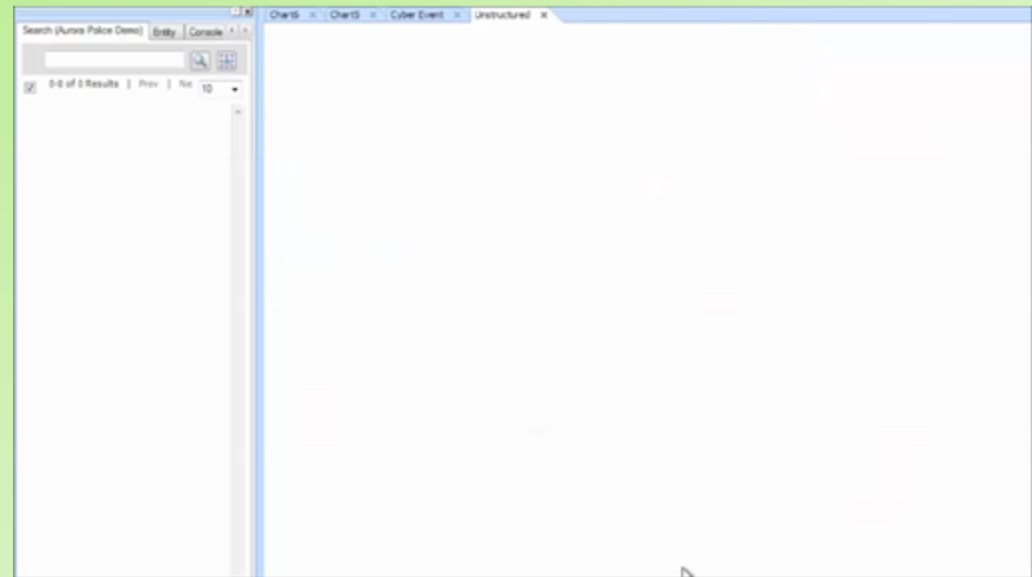
Find out who the attacker could be

Find out who the attacker is linked to

Find out more information about the attacker


Making it real

## Enterprise Insight Analysis




The analyst has information about the attack and attacker, including others that will likely be targeted. The analyst can block future attacks that use similar attributes.


# Solution definition and benefits (six S's): Scalability


cales to cover all your data sets

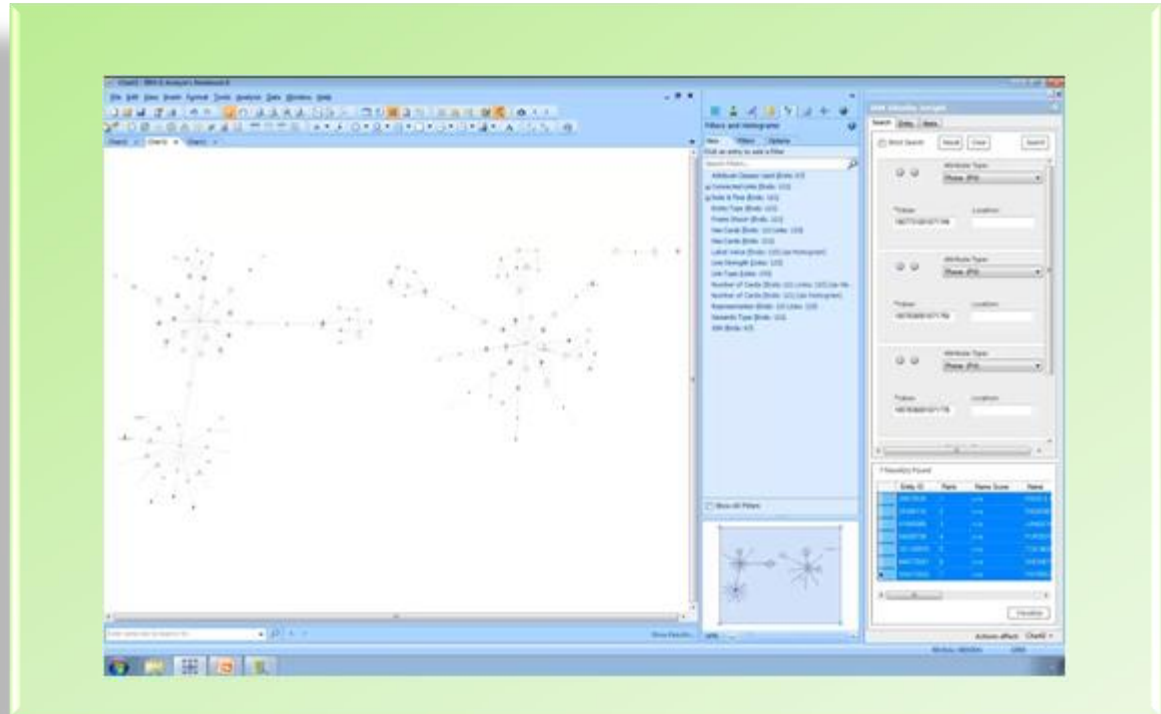
peed measured in seconds

creen advance visualization

plements with recommendation engines

et up your own analytics

patial temporal analytics



- Filter large-scale data sets to create smaller subsets
- Support for server-side sets

## Solution definition and benefits (six S's): Speed



cales to cover all your data sets



peed measured in seconds



creen advance visualization



plements with recommendation engines



et up your own analytics




patial temporal analytics





- Take advantage of capacity and performance analytics speed in seconds (over 100 TB).
- Find a path over many hops and entity types.


## Solution definition and benefits (six S's): Screen advance visualization

 scales to cover all your data sets

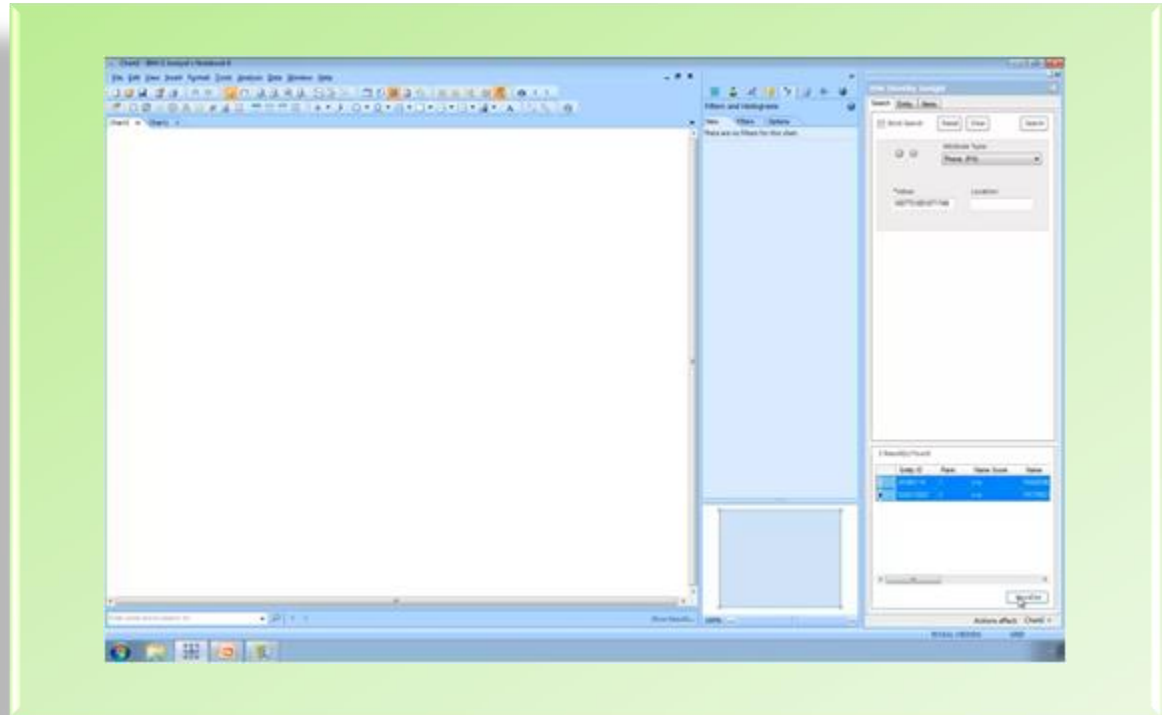
 speed measured in seconds

 screen advance visualization

 supplements with recommendation engines

 set up your own analytics

 spatial temporal analytics




- Explore large-scale data sets with advanced visualizations.


# Solution definition and benefits (six S's): Supplements


 cales to cover all your data sets

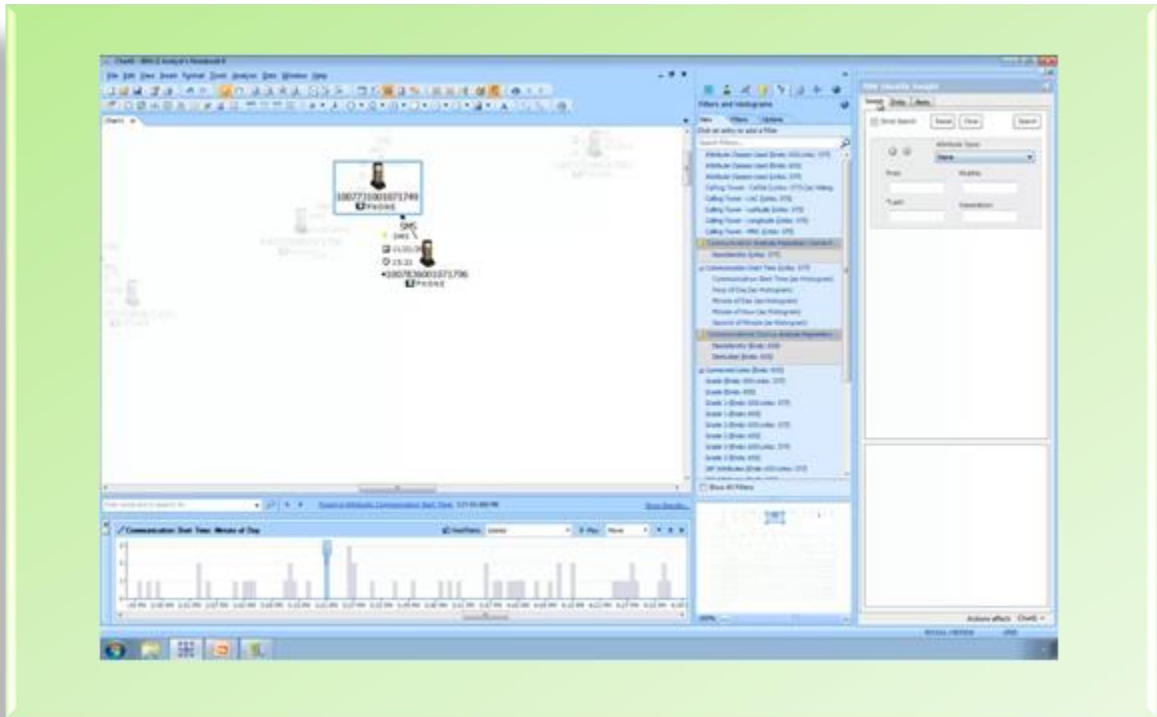
 peed measured in seconds

 creen advance visualization

 upplements with recommendation engines

 et up your own analytics

 patial temporal analytics



- Assist the analyst; provide a recommendation engine:
  - ASK: Enable the analyst to query for recommendations
  - TELL: Alert the analyst to a situation in real time
  - FIND: Find paths between entities by using recommendations

## Solution definition and benefits (six S's): Set up analytics

Scalable to cover all your data sets

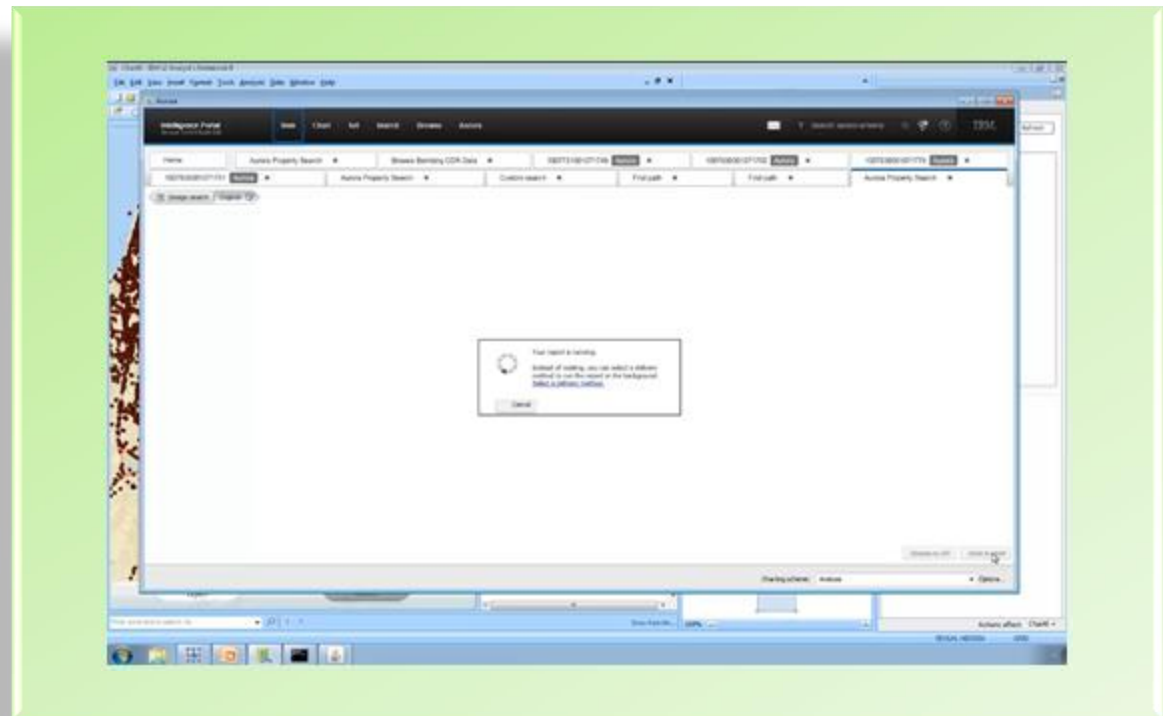
Speed measured in seconds

Screen advance visualization

Supplements with recommendation engines

Set up your own analytics

Spatial temporal analytics



- Enable clients to maintain, integrate and extend (that is, create their own analytics) without external support.

# Solution definition and benefits (six S's): Spatial temporal analytics



cales to cover all your  
data sets



peed measured in  
seconds



creen advance  
visualization



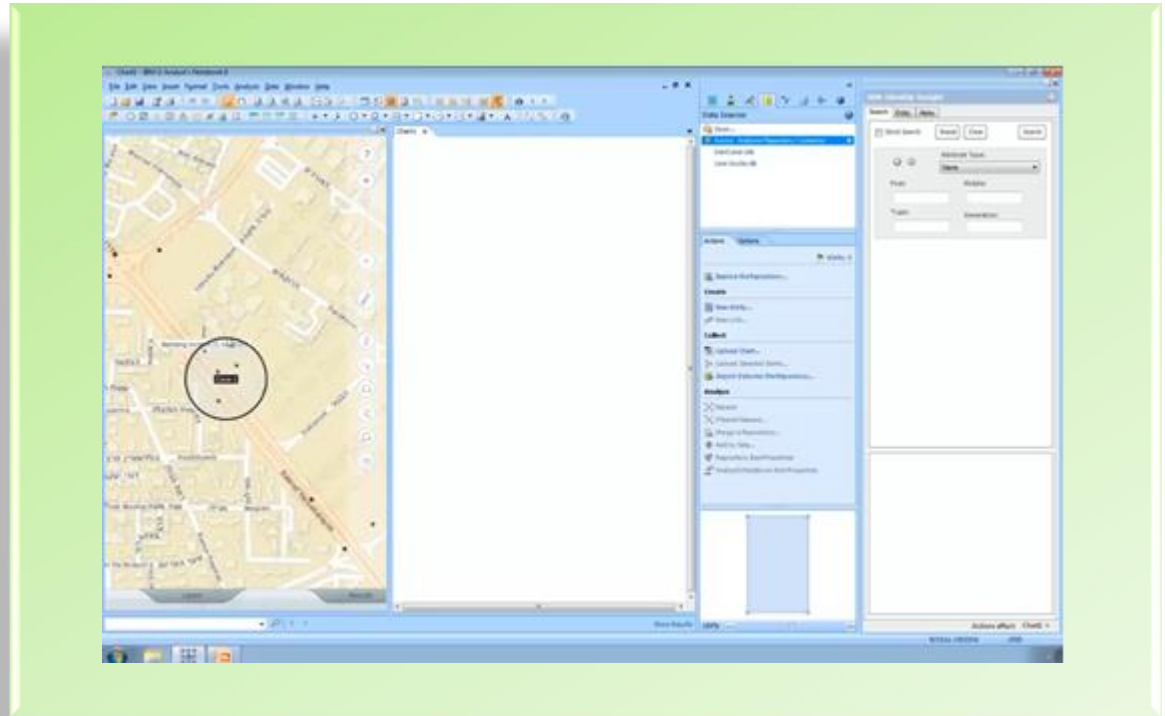
upplements with  
recommendation engines



et up your own analytics



patial temporal analytics



- Use geospatial integration for query and filter support.



THANK YOU

# Trademarks

© Copyright IBM Corporation 2014

IBM Corporation  
Software Group  
Route 100  
Somers, NY 10589

Produced in the United States of America  
November 2014

IBM, the IBM logo [ibm.com](http://ibm.com), DataStage, i2, InfoSphere and PureData are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “[Copyright and trademark information](#)” at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml).

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

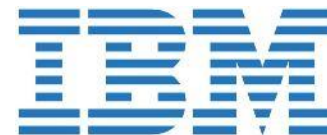


## Audience Q&A

---

Moderator:  
Steve LeSueur  
Contributing Editor,  
1105 Public Sector Media Group

Sponsored by:





Thank you for attending.