

# Insider Threat

Threat hunting enable analysts to discover advanced threats faster and at scale.



**Mike Kehoe**

MBA, Hons. BSc. Electronic / Electrical Engineering , H. Dip. EE , MA (Maths)

IBM i2 Global Leader , Commercial Crime

Mikekehoe@ie.ibm.com









## Who are we Threat Hunting ?



An individual or group of individuals who have **abuse their rights** in being connected to our organizations, both internal and external.

- Employees
- Partners
- Contractors
- Suppliers
- Customer

## When should we go INSIDER Threat Hunting ?



On Entry to the organizations via **Due Diligence** screening



As part of inline operational monitoring



# Why is there a need for INSIDER Threat Hunting ?

## Ryanair target of £3m bank transfer scam

© 29 April 2015

f t e Share



Financially driven  
External

## Tesla Breach: Malicious Insider Revenge

Tesla employee "making direct code changes to the Tesla Manufacturing Operating System under false usernames and exporting large amounts of highly sensitive Tesla data to unknown third parties."

Revenge

## Eco-terrorist attacks on energy infrastructure on tap for 2018

Ideology driven

## Ashley Madison hack victims receive blackmail letters

Forced /  
Compromised

5,300 Wells Fargo employees fired over 2 million phony accounts

Financially driven  
Internal

## *THE COLLAPSE OF BARINGS: THE OVERVIEW; Young Trader's \$29 Billion Bet Brings Down a Venerable Firm*

Private  
Remediation

## Japanese trader makes £22 billion mistake

A trader working in the Japanese branch of the Swiss bank UBS mistakenly ordered £22 billion of bonds while trying to buy just £220,000.

Ignorance



# Why is there a need for INSIDER Threat Hunting ?

To stop the **3R's** of organizational impact



Reputational



Regulatory

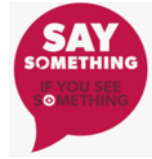


Revenue

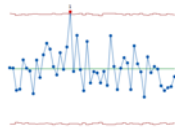


# Where can the tell tail signs be seen of an INSIDER threat ?

## Trigger Points to go INSIDER threat hunting



- On Request via **suspicious activity report** via see-something / Say something



- Rules Engine Alert raised



- Concerning External information discovered ( OSINT , Open Source Intelligence)



- Exploratory Investigations

## IBM i2 – A Global Presence

- Founded in 1990 and based out of Cambridge UK
- 25+ years experience working with analysts and investigators
- Acquired by IBM in 2011
- Pervasive in market with over 4500 clients
- More than 450,000 users in 150 countries in 18 languages
- Used by 8 of the top 10 largest companies, 12 of top 20 banks
- 100% of UK police forces
- 80% of National Security agencies worldwide
- Every US Federal Law Enforcement agency and organization
- 4000 US Police jurisdictions
- 25 of the 28 NATO member countries



# IBM i2 – An Industrial Presence

## Law Enforcement & Defense



Counter Terrorism  
Intelligence Analysis  
Border Security  
Target Analysis and Defense  
Force Protection  
Organized Crime  
Event Management  
Insider



## Government



Industry Oversight & Compliance  
Securities Investigations  
Anti-Money Laundering  
Benefit Fraud  
Troubled Families



## Banking & Insurance



Fraud Investigations  
Risk Management  
Anti-Money Laundering  
Security Investigations  
Industry Oversight & Compliance  
Insider



## Retail, Pharma & Distribution



Loss Prevention  
Asset & Profit Protection  
Fraud Investigations  
Brand Protection  
Counterfeit Goods  
Track & Trace  
Anti-illicit Trade



## Private Sector, OT



Fraud Investigations  
Securities Investigations  
Anti-Money Laundering  
Industry Oversight & Compliance  
Telco cloning of data  
Insider



## How to go INSIDER threat Hunting ?..... Link Analytics



We all have a digital footprint

# How to go INSIDER threat Hunting ?..... Link Analytics



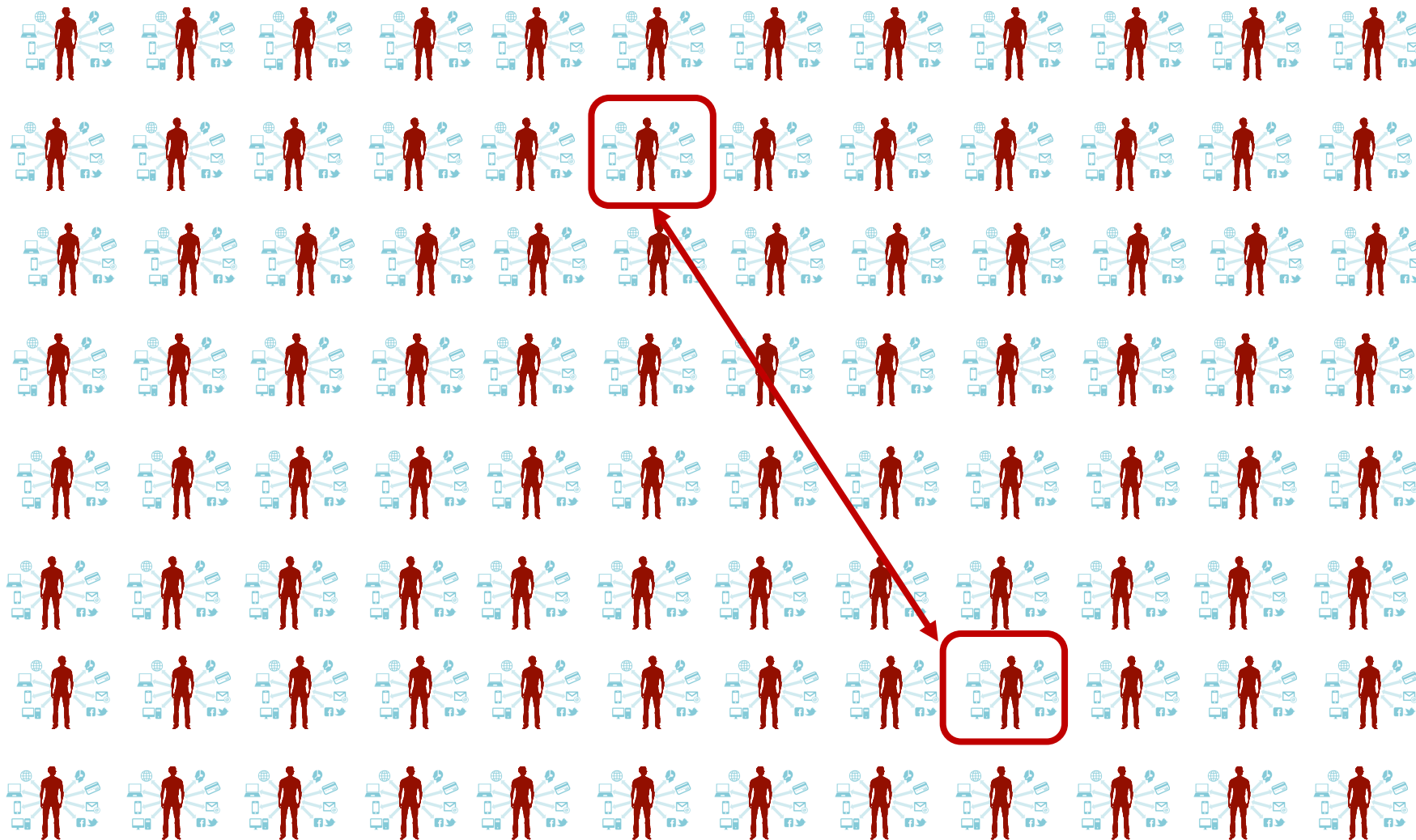
Our digital footprint has attributes across **temporal, geospatial** and **operational** domains



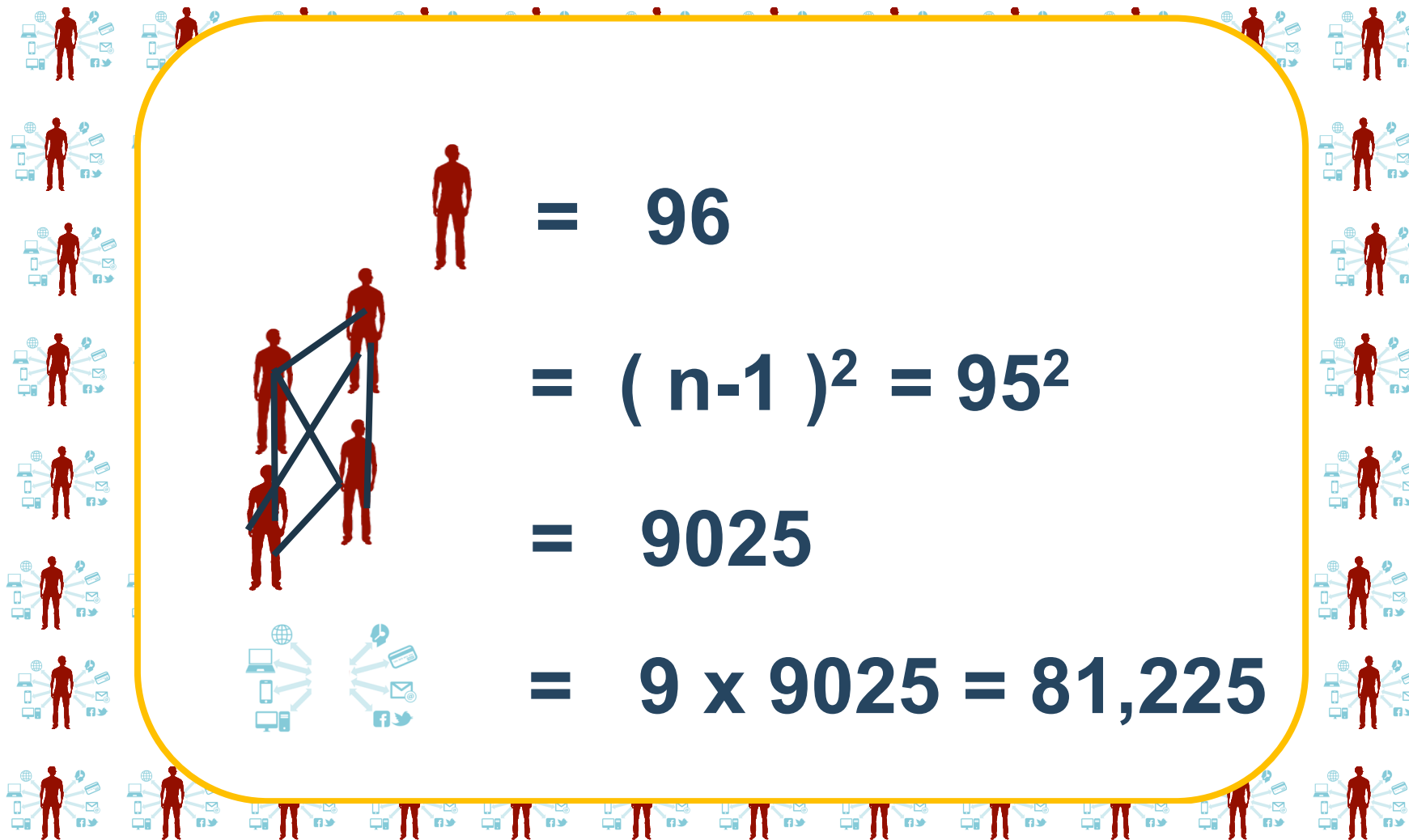
## Entity Link Property (ELP)

|               |   |
|---------------|---|
| Name (M)      | : Richardo Gomes                          |
| Name (M)      | : Richard Gomez                           |
| Address (H)   | : 11035 Burns Ave., Westchester, IL 60153 |
| Address (H)   | : 11035 Burns Dr, Westchester, IL 60153   |
| CUST#         | : 796                                     |
| CUST#         | : 857                                     |
| ACCT#         | : D2712151385121742                       |
| ACCT# Card    | : V97859240062 <b>operational</b>         |
| Phone         | : 064-413-9611                            |
| Phone         | : 069-906-1853                            |
| Phone         | : 028-891-0646                            |
| IP            | : 123 456 789 1011                        |
| DL            | : H160-65-120A9 FL                        |
| Date Of Birth | : 1976-08-05                              |
| Activity Time | : 13.26 <b>temporal</b>                   |
| Activity Date | : 04/10/2017                              |
| Location      | : Dublin <b>geospatial</b>                |

# How to go INSIDER threat Hunting ?..... Link Analytics



# How to go INSIDER threat Hunting ?..... Link Analytics





# How to go INSIDER threat Hunting..... Data on the Pattern of Life

• CDR



• CCTV



• Social Media



• Browser history



• Associations



• HR record



• Case History



• Emails



• SAR



• Threat Reports

• Door Access

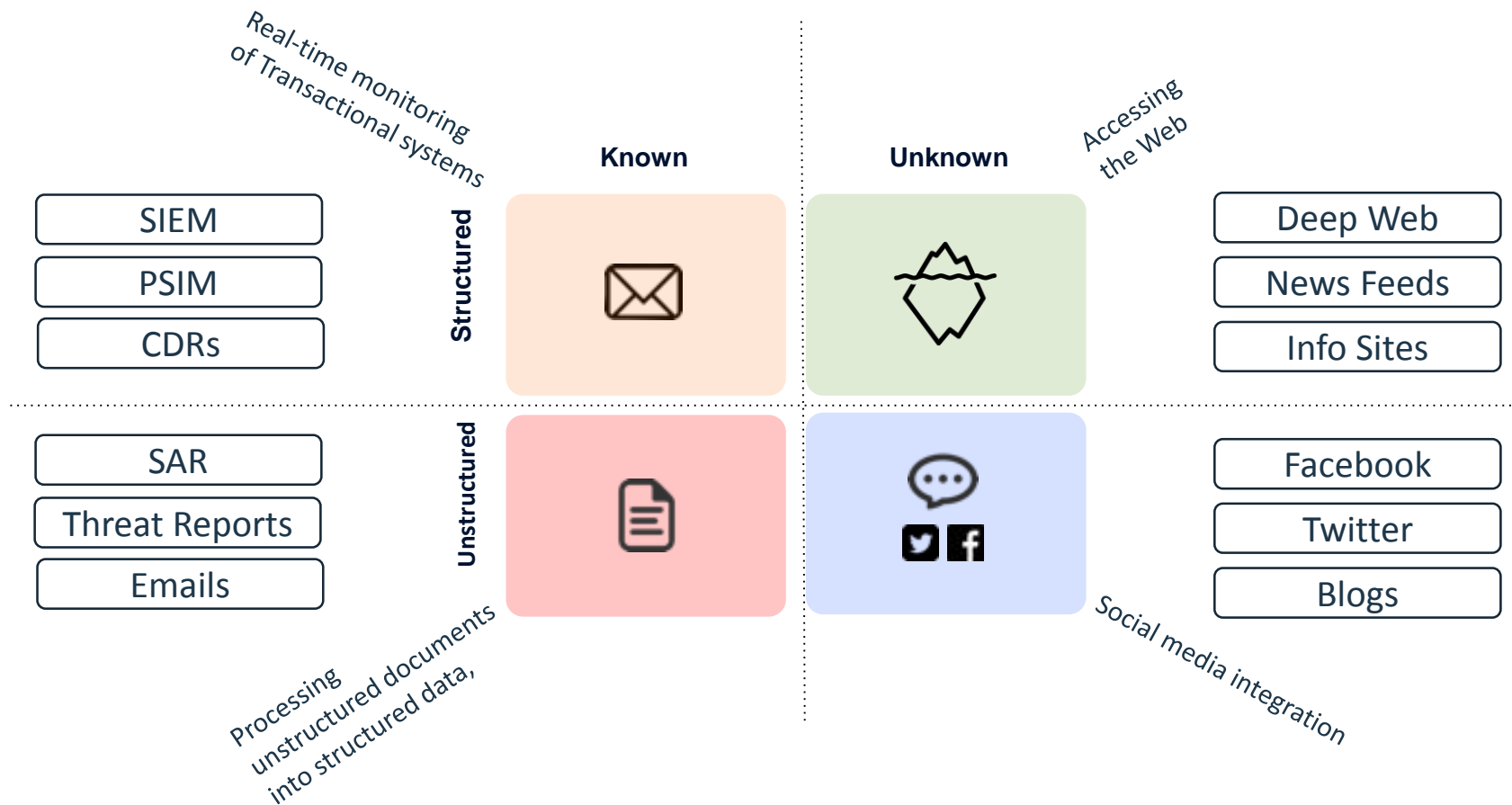


Small signals with non obvious connections



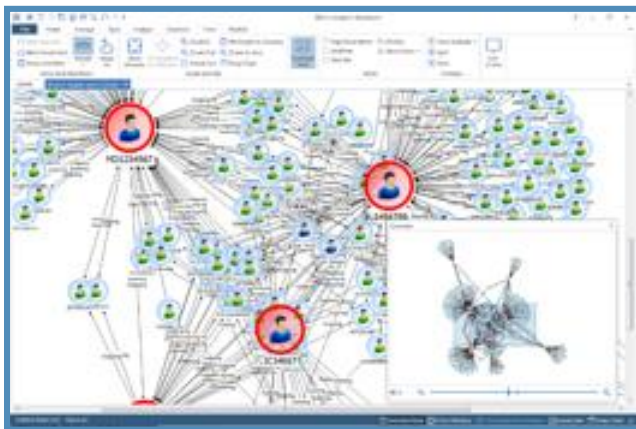
# How to go INSIDER threat Hunting..... Data

Ensure to connect to the **4 quadrates of data**





# How to go INSIDER threat Hunting..... Investigations



Link Analytics Who knows Who



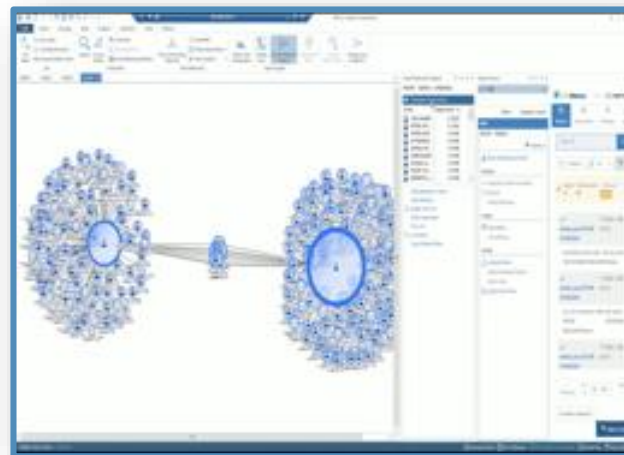
Heatmaps of abnormal activities



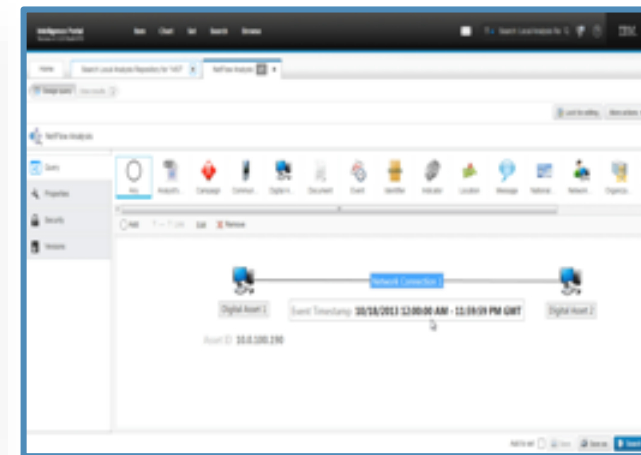
Transactional events of what happen next



Geospatial where its happen



Social Media



Identity resolution



# How to go INSIDER threat Hunting..... Defense in depth

## Tier One.... Transaction

## Tier Two ... Correlation

## Tier Three... Investigation

Detect using rule based systems

- *Privileged Access Management (PAM)*
- *Physical Security Information Mgt (PSIM)*
- *User Activity Monitoring (UAM)*

Uncover of anomalies with enterprise data correlation

- *User Behaviour Analytics (UBA)*
- *Security Information and Event Management System (SIEM)*

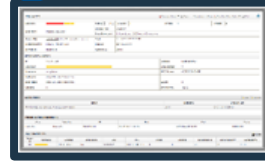
Discovery of non obvious patterns using Threat Hunting

- *Link Analytics*
- *OSINT*
- *SARs*

# How to go INSIDER threat Hunting..... Defense in depth

## LAYERED DEFENSES

 Tier One



- Privileged Access Management (PAM)
- Physical Access systems (PSIM)
- User Activity Monitoring (UAM)

# How to go INSIDER threat Hunting..... Defense in depth

## LAYERED DEFENSES

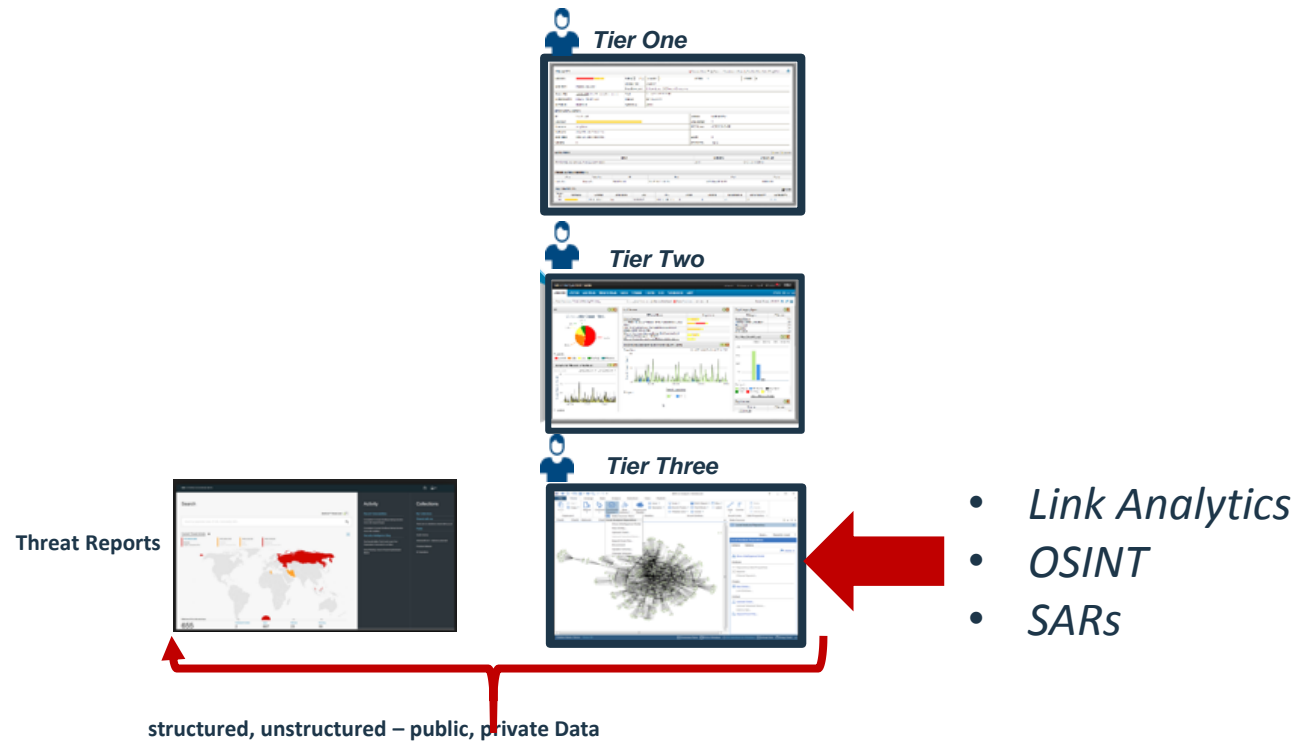


- *User Behaviour Analytics (UBA)*
- *Security Information and Event Management System (SIEM)*

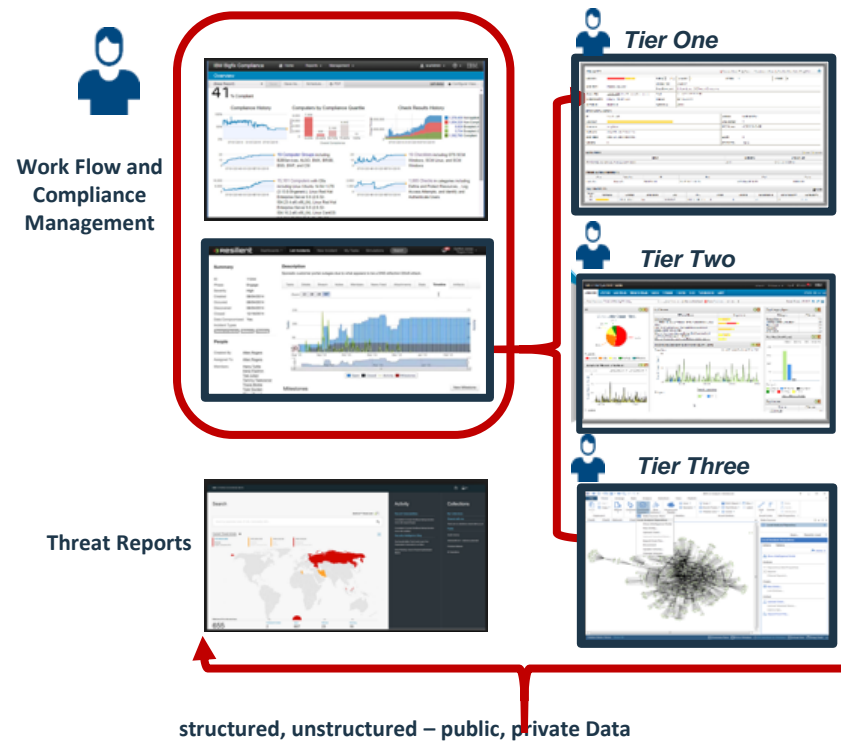




# How to go INSIDER threat Hunting..... Defense in depth



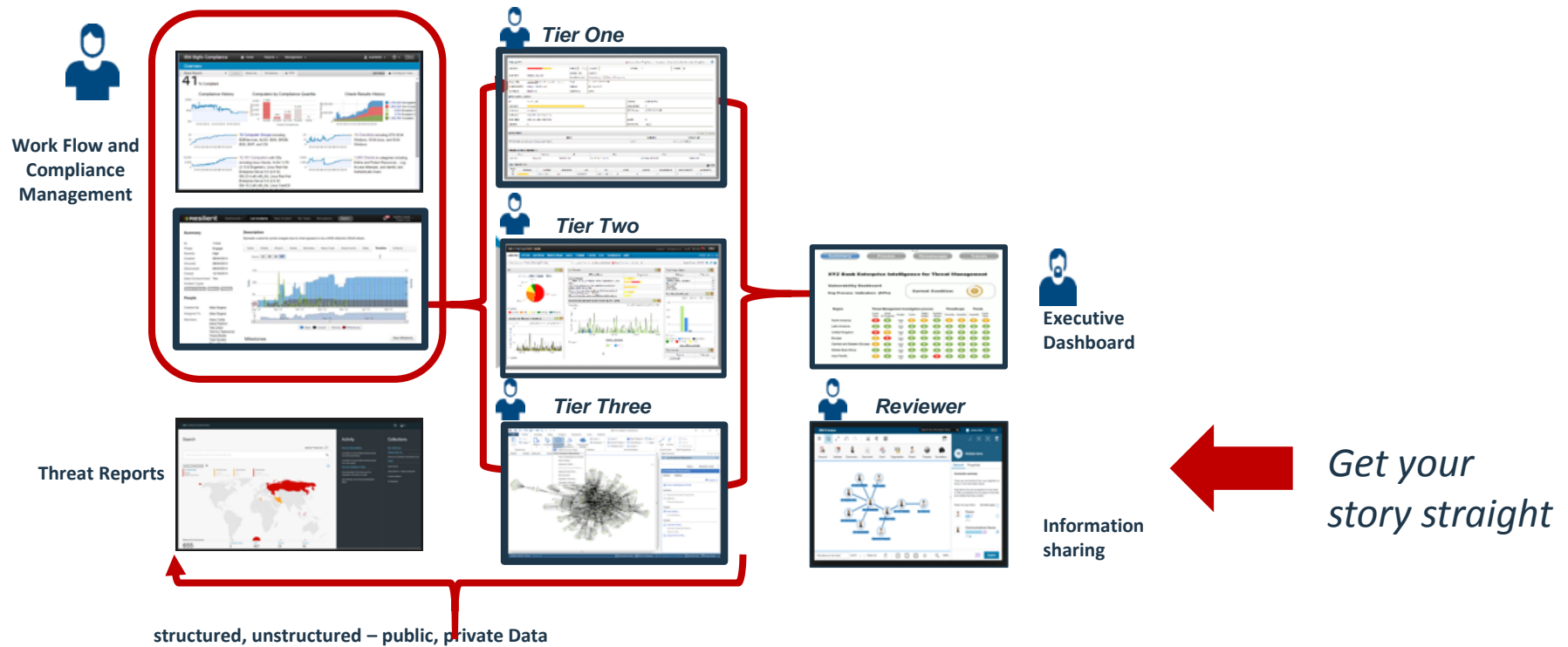
# How to go INSIDER threat Hunting..... Defense in depth



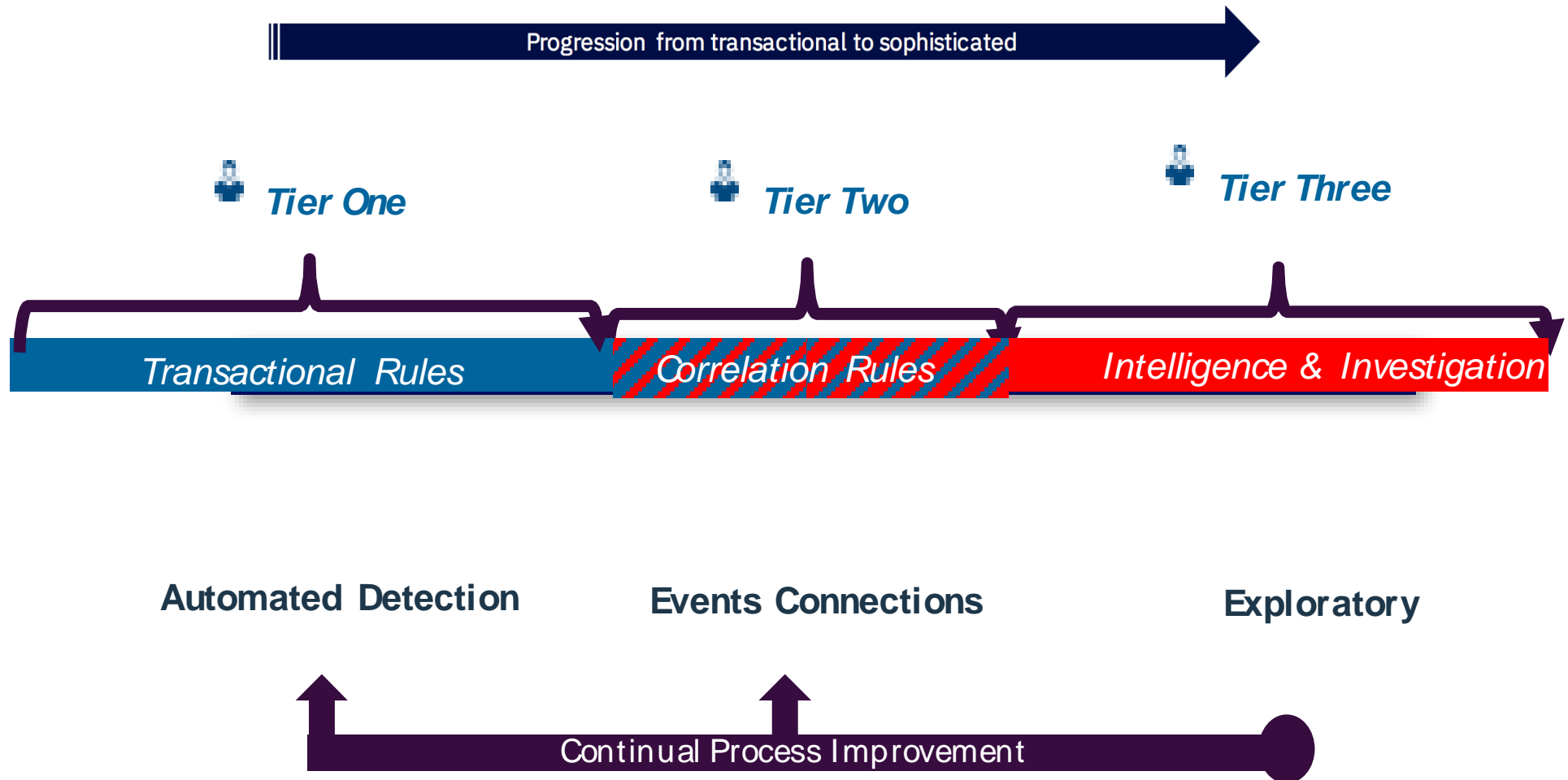
# How to go INSIDER threat Hunting..... Defense in depth



# How to go INSIDER threat Hunting..... Defense in depth



# Defense in depth continual process improvement



# Demo Time



Recommendation Engine

Identity Resolution

Collaboration

Geospatial

Link Analytics

Actionable Intelligence

Heat Maps

Social Network Analytics

Visual Query

OSINT


All Search





# THANK YOU

## FOLLOW US ON:

-  [ibm.com/security](https://ibm.com/security)
-  [securityintelligence.com](https://securityintelligence.com)
-  [xforce.ibmcloud.com](https://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2017. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.