## **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







#### Disclaimer

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

#### **Prohibited Uses**

Licensee may not use or authorize others to use the Program, alone or in combination with other services or products, in support of any of the following high risk activities: design, construction, control, or maintenance of nuclear facilities, mass transit systems, air traffic control systems, automotive control systems, weapons systems, or aircraft navigation or communications, or any other activity where program failure could give rise to a material threat of death or serious personal injury.







## **INSIDER Threat Hunting using investigations platforms**

## Agenda

- WHAT
- WHO
- WHEN
- WHY
- WHERE
- HOW









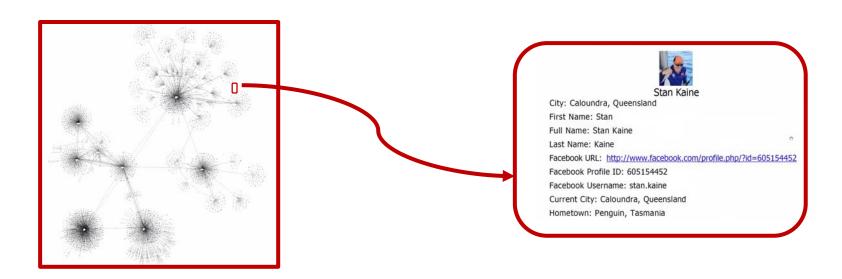
## What is Threat Hunting?

A Threat hunting's goal is:- Discovering any issue that can cause harm to an organisation's operation and/or its stakeholders

The combination of machine-led analytics and human-led analysis capabilities that helps you quickly **find hidden connections** and critical patterns **buried in internal, external and open-source data.** 

Ensuring that massive data sets can yield actionable intelligence.

.....Faster then the speed of threat









## 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?

To **STOP** organizational harm

For an insider to cause harm to an organization 4 things must happen

- 1. They must have a reason
- 2. They will want to remained concealed
- 3. Their needs are placed above the needs of the organization
- 4. They do recon\*

#### **INSIDER Motivation Categories**

#### Passive:-

Ignorance

**Private Remediation** 

#### Active\*:-

Financially driven

Ideology driven

Revenge

Forced / Compromised







## Why is there a need for INSIDER Threat Hunting?



#### **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

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











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

































We all have a digital footprint

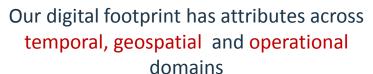






#### Entity Link Property (ELP)



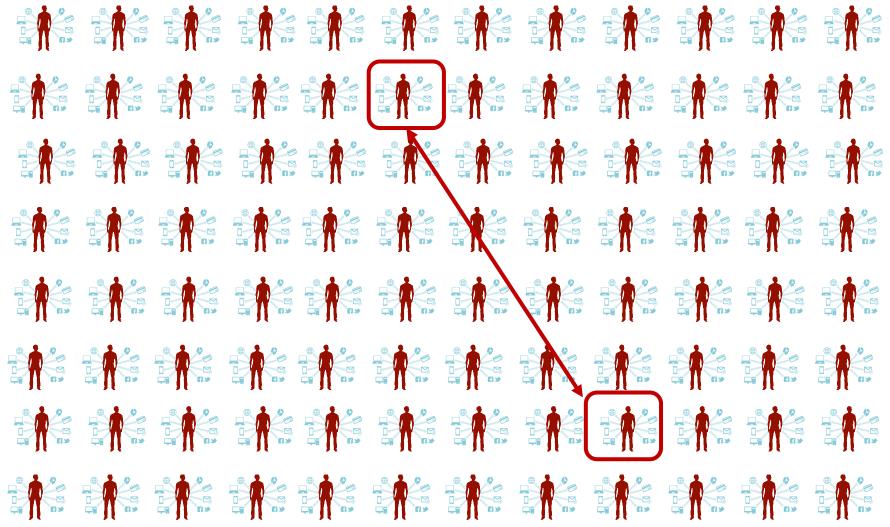








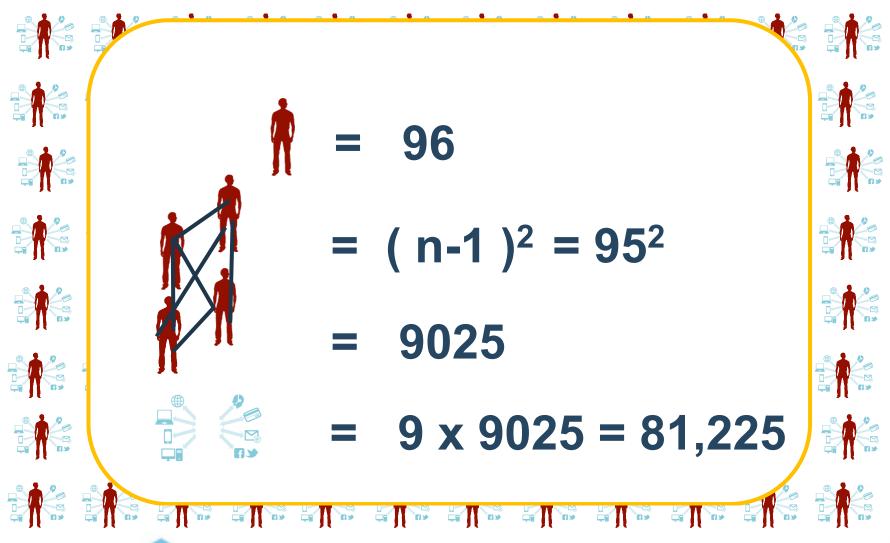










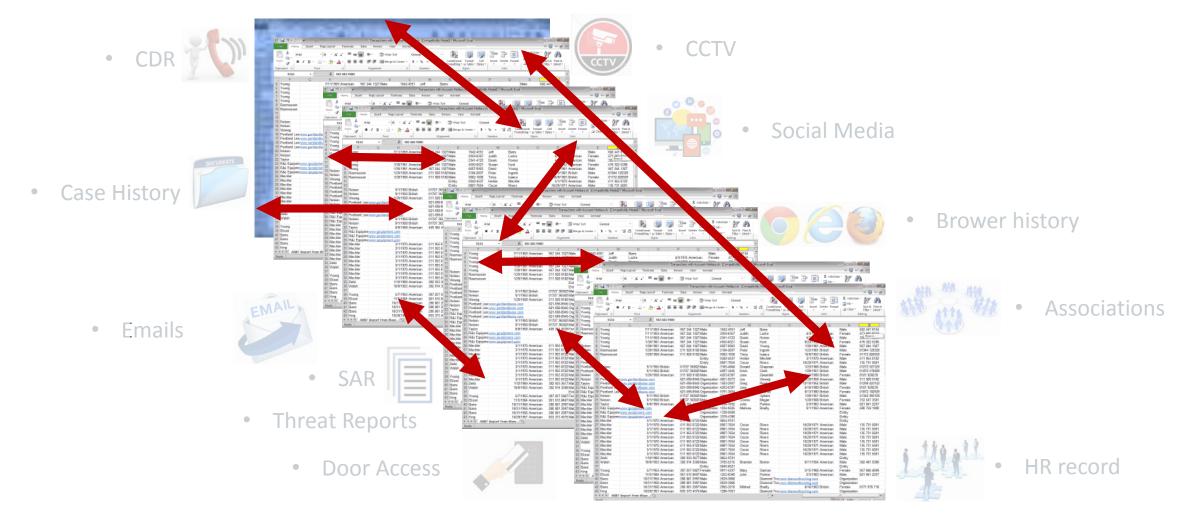








## **How** to go INSIDER threat Hunting...... **Data on the Pattern of Life**



Small signals with non obvious connections



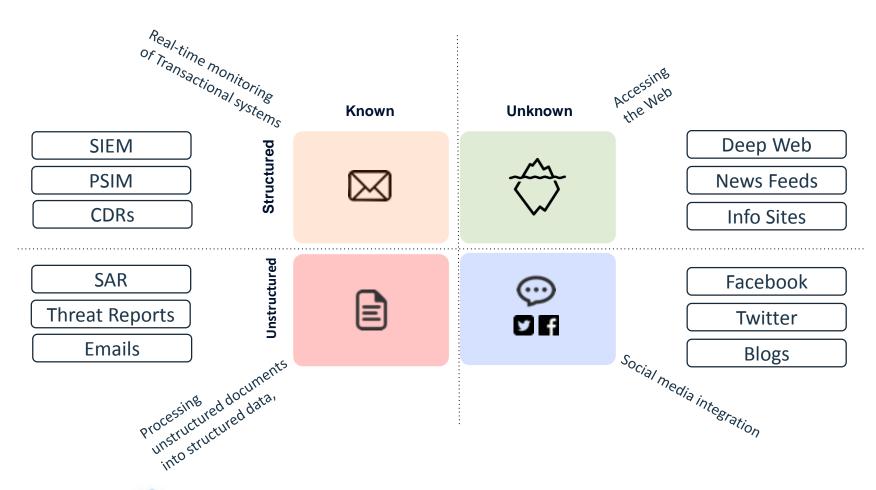




/28/2018

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

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



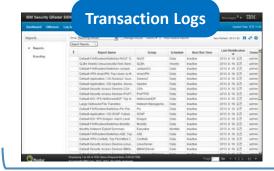


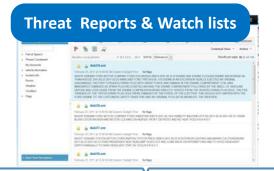




## **How** to go INSIDER threat Hunting...... **Process**

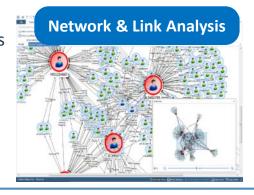
Ingest data from many sources



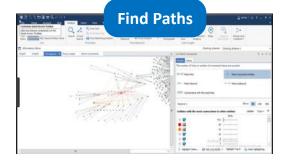




Analyze suspicious patterns with intuitive features & functions







Deliver actionable intelligence integrated approach to protecting an organization



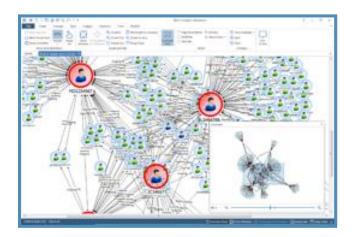








## **How** to go INSIDER threat Hunting...... **Investigations**



Link Analytics Who knows Who

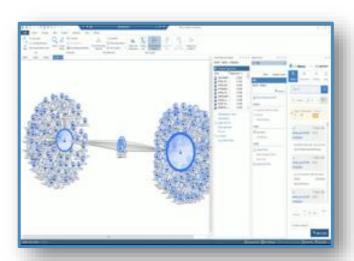


Geospatial where its happen



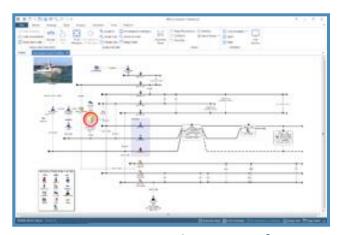


Heatmaps of abnormal activities

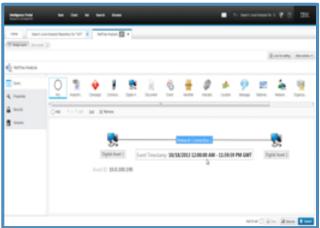


Social Media





Transactional events of what happen next



Identity resolution



Tier One.... Transaction

### Tier Two ... Correlation

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

Discovery of non obvious patterns using Threat Hunting

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

Tier Three... Investigation

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







**LAYERED DEFENSES** 



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







**LAYERED DEFENSES** 



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

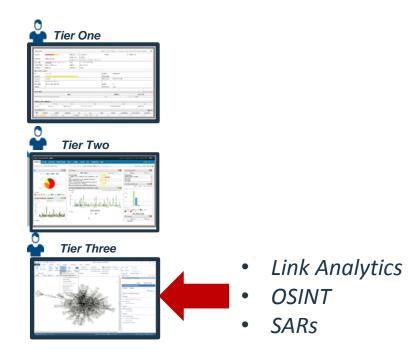






**LAYERED DEFENSES** 

**INTELLIGENCE** and **INTEGRATION** 



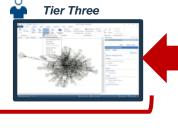












- **Link Analytics**
- **OSINT**
- SARs

structured, unstructured – public, private Data



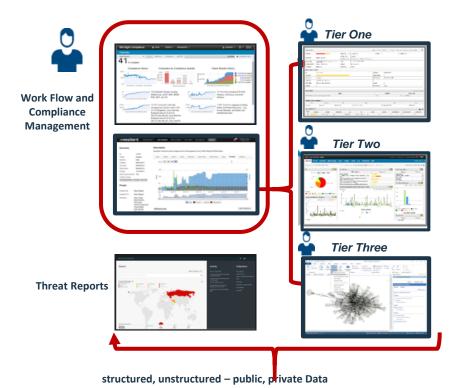




LAYERED DEFENSES

**INTELLIGENCE** and **INTEGRATION** 

Al and ORCHESTRATION, COLLABORATION





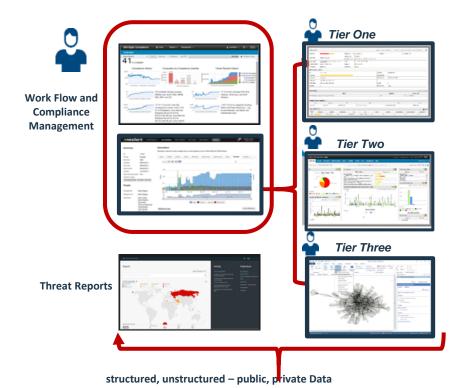




**LAYERED DEFENSES** 

**INTELLIGENCE** and INTEGRATION

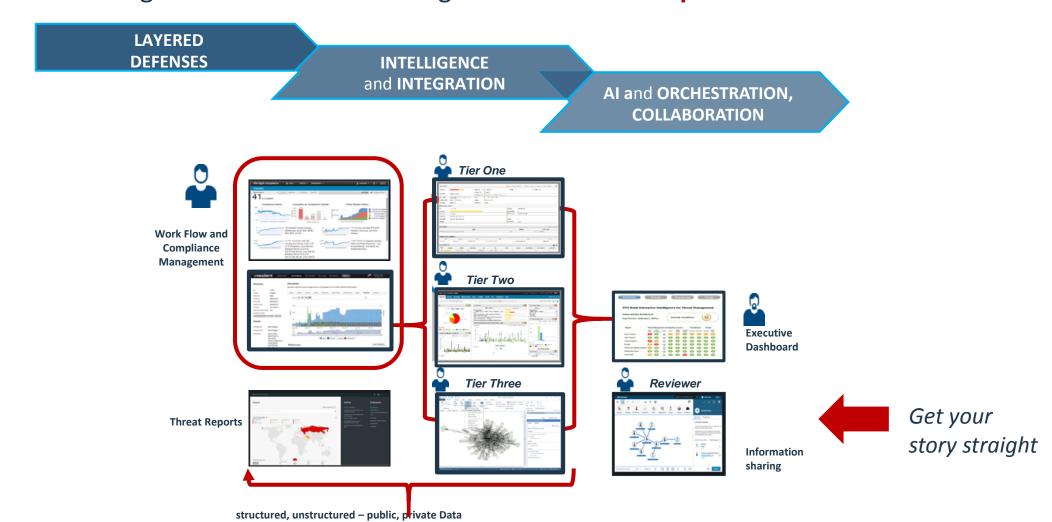
AI and ORCHESTRATION, **COLLABORATION** 









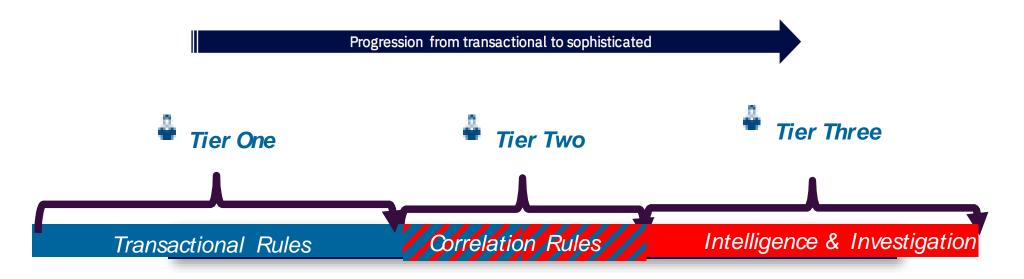








## **Defense in depth continual process improvement**











## **Demo Time**



**Recommendation Engine** 

**Identity Resolution** 

**Collaboration** 

Geospatial

**Link Analytics** 

**Actionable Intelligence** 

**OSINT** 

**Heat Maps** 

**Social Network Analytics** 

**Visual Query** 

All Search







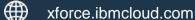


# THANK YOU

#### **FOLLOW US ON:**









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.

