



IBM Security i2 Enterprise Insight Analysis

Investigate Add-On

Finding hidden connections across multiple, disparate, unconnected data sources in order to detect vulnerabilities and disrupt threats, both cyber and physical, can be a huge challenge. Without quick and easy direct access to an organization's intelligence repository, non-analyst users need to ask analysts for information on individuals of interest and other entities or they use other methods to obtain the information. It can be inefficient and take valuable time away from investigation, for both the non-analyst, operational user, and the analyst.

IBM Security i2 solutions are widely used by government and private sector organizations to detect, disrupt and defeat advanced physical and cyber threats faster. The IBM Security i2 Enterprise Insight Analysis solution offers powerful, robust, enterprise level intelligence analysis capabilities for analysts, including sharing and collaboration. The use cases span across national security & defense, law enforcement, fraud investigations or cyber threat hunting and investigations.

i2 Investigate Add On extends the i2 Enterprise Insight Analysis solution beyond trained analysts, allowing operational, non-analyst users to conduct fast target investigation to answer common questions quickly and easily. This comprehensive "360-view"

Highlights

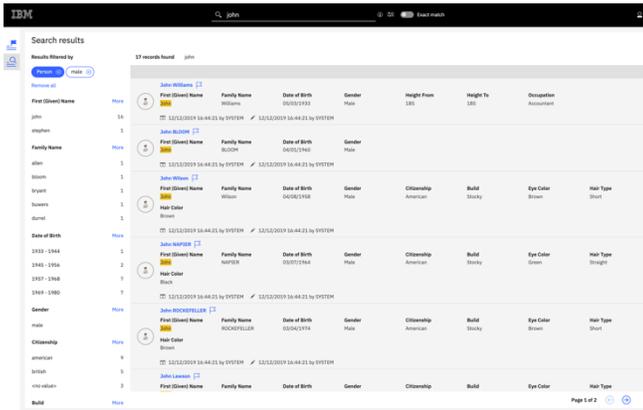
- Allows non-analysts to find hidden connections quickly
 - Offers simple, yet powerful search & discovery function
 - Requires no training or knowledge of analyst techniques
-



capability requires no training to use and no specific knowledge of the data ontology or analyst techniques. It can make an analyst more productive by reducing interruptions throughout the working day to answer basic questions by non-analysts and speeds up information flow to non-analyst end users. This capability is another proof point of IBM's vision for automating tradecraft, a concept which leverages technology innovation to augment, not replace, the analyst.

Key Capabilities of the i2 Enterprise Insight Analysis Investigate Add-On

- Makes rich intelligence data available to a broader group of users in a secure, cost effective way
- Offers these users the ability to easily traverse read-only data from the “information store” via a web browser
- Allows users to feel confident to explore safely with no ability to change, remove or damage the data
- Can be used by anyone with basic web skills such as web browser search and web-based product purchase
- Aligns to a data schema and uses the security model of the i2 Enterprise Insight Analysis information store
- Configurable at deployment to ensure relevant contextual common questions can be answered automatically.



Non-analyst can easily search and traverse data.

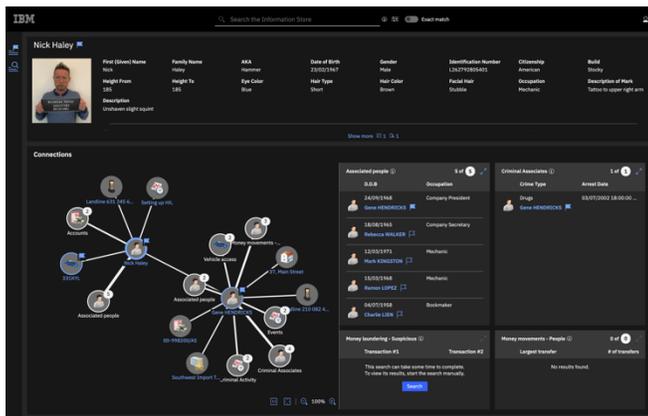
The Investigate Add-On in action

The following scenario profiles the tool in action, and provides an example of a law enforcement use case:

- A police detective wants to learn more about an individual and a company.
- The task is to find if the 2 entities exist in the database and what connections might exist -- in just a few minutes.
- User starts by searching by full name (or just last name) of the individual.
- Based on a dynamic, faceted list of hits, user can filter the returned results to find the individual in question.
- Clicking on that individual, a 360-view is shown that includes 2 sections. The first shows the real-time known data about the individual in the database.
- The second section shows connections made by the system using a subject record (the individual) as the “seed” for additional automatic searches.
- User sees the resulting highlight panels, with pre-defined patterns of common, multiple-degree searches, as well as a simple visualization of this information.



- User can then click on an associate to see that individual's 360-view and can search further on other entities, e.g. addresses, vehicles and bank accounts.
- User then looks up the company. In this case, the request is to perform a “find path” between individual and company – searching for the shortest connection.
- With the target investigation complete, the detective shares the person of interest with a colleague, who also has access to the tool, via a simple URL.



360-view with individual's known data and connections.



Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

© Copyright IBM Corporation 2020.

IBM, the IBM logo, and ibm.com 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 <https://www.ibm.com/legal/us/en/copytrade.shtml>, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:



All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Offering Name, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security/intelligence-analysis/i2