IBM i2 Enterprise Insight Analysis for Cyber Threat Hunting

Counter and mitigate more attacks with cyber threat hunting

Highlights

- Quickly identify threats, threat actors and hidden connections with multi-dimensional visual analysis and advanced analytics
- Visualize cyber incidents by ingesting and analyzing large, disparate silos of data sets with unprecedented speed
- Securely share insights and intelligence within, across and among organizations, in a familiar chart format
- Open your cyber security aperture with comprehensive analysis, in near real-time

Executive summary

Securing your infrastructure, your customer interactions and protecting your data are critical to preserving your reputation and your bottom line. Many cyber attacks remain undetected for up to eight months[1] and can cost an organization an average of 11 million USD.[2]

Today's cyber actors are becoming more sophisticated, agile and capable of getting past any network security. Organizations must evolve, replacing traditional defensive security strategies with a proactive, intelligence-driven offense to prevent and disrupt these threats.

IBM® i2® Enterprise Insight Analysis is a next generation intelligence solution that enables organizations to incorporate cyber threat hunting into their security strategy and turn their defense into a proactive offense.It helps organizations uncover critical insights about their threats and threat actors so they can mitigate and counter more threats with a combination of multi-dimensional visualte analysis capabilities and advanced analytics.

Sources of cyber threats

Cyber threats vary greatly and so do the methods of attack. To counter those various sources, organizations need intelligence to fortify themselves from both internal and external threats. Organizations face five critical sources of cyber danger:

- **Commercial and industrial cyber espionage** for theft and competitive advantage
- **Government cyber espionage** for technical and political advantage
- **Organized crime** for financial gain through the acquisition and theft of data and goods
- **Terrorist activity** designed to harm both businesses and governments, including damage to physical infrastructure by unauthorized entry to their industrial control systems
- **Hacktivism** of IT assets resulting in public embarrassment, loss of public confidence and damage to the value of the brand

These threats are further complicated by the agility of the attackers against the less agile, traditional defense systems. Additional threats include:

- Mobility of threat actors and groups
- Changing alliances among threat actors and groups
- Unknown threats from new software applications and solutions
- Constantly changing malware footprint
- New protection challenges resulting from crumbling IT perimeters
- Constantly changing online and offline data environments

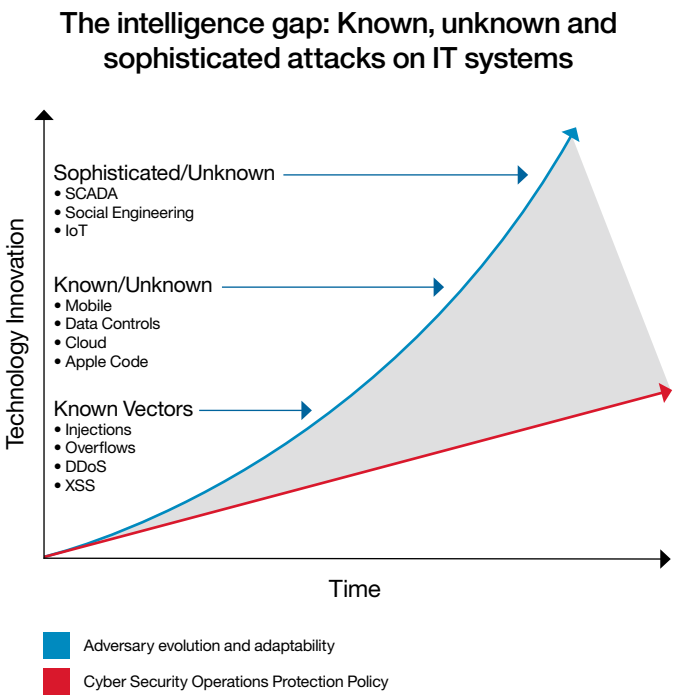

Figure 1: As new IT innovations emerge, so do new attacks on IT systems. Traditional cyber security measures cannot prevent or deter these attacks due to their speed and frequency. However, IBM i2 Enterprise Insight Analysis for cyber threat hunting can help organizations close this gap by serving as a cyber security force multiplier.

The solution: cyber threat hunting

Fortifying cyber security requires proactive cyber threat analysis that identifies threat actors, their purpose, intentions, infrastructure and weaknesses. To accomplish these goals, organizations need investigative solutions that extend to areas not addressed and conquered by traditional security solutions, because a strategy based on protection alone is not sufficient anymore. Organizations must evaluate non-traditional data sources.

With the IBM i2 Enterprise Insight Analysis solution, organizations can proactively develop a comprehensive understanding of their attack surfaces and vulnerabilities and develop referenceable attack scenarios to help speed investigations and remediation. To prevent future attacks, organizations can identify and investigate attackers after an incident. All insights become part of the organization's cyber security strategy and tactics, resulting in an intelligent approach to cyber security.

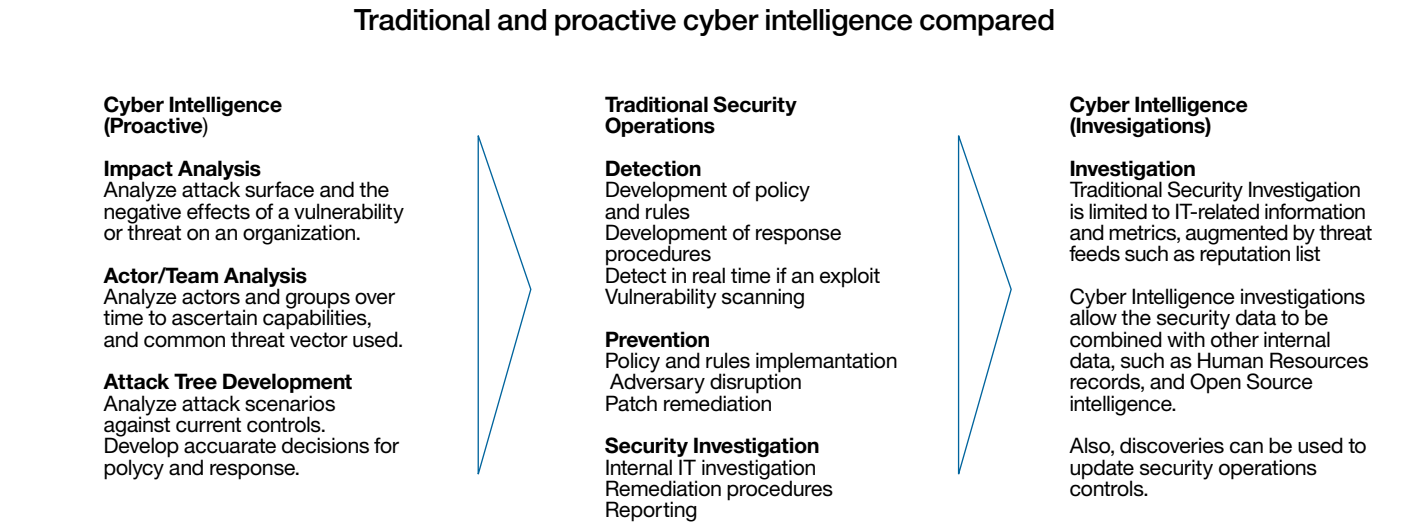

Figure 2: Cyber threat hunting provides both proactive and post-incident actionable intelligence.

Effective cyber threat hunting solutions address these unrelenting threats with the following crucial cyber analysis capabilities:

- Rich extraction, analysis and visualization capabilities
- Data on demand connectors
- Social engineering data layering techniques
- Ability to share clear analysis results among organizations and law enforcement

World-class big data and advanced analytics

Automated data and advanced analytics engine

IBM i2 Enterprise Insight Analysis integrates seamlessly with IBM's big data solutions providing users with critical reliability, scalability and outstanding performance. These systems are designed to handle more than 1,000 concurrent operational queries with continuous ingest. Continuous data ingest enables loading data dispersed across the enterprise, in various silos, at the same time. This minimizes the latency created by batch loading data on infrequent schedules simultaneously to support real-time mission analysis and decision making on the latest operational data during the loading process.

Industry-leading, multi-dimensional intelligence analysis

Developed with over 20 years of analyst input, IBM i2 Enterprise Insight Analysis delivers a powerful multi-dimensional visual analysis environment that helps users simplify complex networks, and detect non-obvious relationships and patterns. It also features a powerful recommendation engine that provides "assisted analysis." This works by reconciling duplicate entities masked by aliases and enabling users to set alerts to proactively track new and critical information—24x7.

Increase accuracy

- **Test hypotheses and query terabytes of data in seconds**
- **Uncover relationships separated by several degrees**
- **Receive automatic alerts when data is added or altered**
- **Uncover non-obvious relationships by applying multi-dimensional visual analytics**
- **Uncover temporal, network hierarchies and critical geospatial insights**

Features	Benefits
A 24x7 automated identity resolution and recommendation engine	Alerts analyst when new information is available and when data has been altered
A scalable, modular and extensible design	Cost effectively scales with organizations needs and challenges
Advanced analytics that perform at critical speed	Manage, integrate and analyze multi-source data and get results in near real-time
Data on-demand connectors	Connectors to streaming data help users analyze data in near real-time
Dynamic and multi-dimensional analysis	Discover hidden connections and trends with geospatial, temporal and relationship analytics
Collaboration features	Provides secure information sharing among organizations
Open design	Uncover more insights by customizing and developing mission specific analytics, without the need of services or support

Increase efficiency

- **i2 Enterprise Insight Analysis Recommendation Engine Add-On provides an automated identity resolution engine, consolidating massive data sets 24x7**
- **Search and automatically process and analyze unstructured data**
- **Perform link, temporal and geospatial queries and run network analytics across hundreds of terabytes of data in seconds**

IBM i2 Enterprise Insight Analysis solution features and benefits

Post-incident analysis

The IBM i2 Enterprise Insight Analysis platform uses powerful post-incident analysis to perform attribution, correlate the links and entities, make real-world connections, and identify your network vulnerabilities. This solution can help your organization with the following cyber challenges:

- Rich extraction, analysis and visualization capabilities that turn large quantities of cyber data into actionable intelligence
- Rapid pattern analysis that quickly identifies characteristics and bad actors in attacks
- Social network analysis capability that identifies distribution of power and communication patterns in cyber networks
- Sophisticated analytical database for managing and analyzing multi-source data
- Data sharing and layering to pool cyber investigative data with other data sources

Add depth to your breach investigations

IBM i2 Enterprise Insight Analysis uses existing security infrastructure, additional non-security-related infrastructure data, and open source data. These multiple sources identify and investigate the breach, the methods used in the breach, and to trace the events to the specific individual responsible for the breach. It also uses layered data from social media sites to ascertain who is attacking your organization, their specific and individual locations, targets, and their associates. With this knowledge, your organization can adapt procedures, defensive policy changes, or both.

External breach investigation

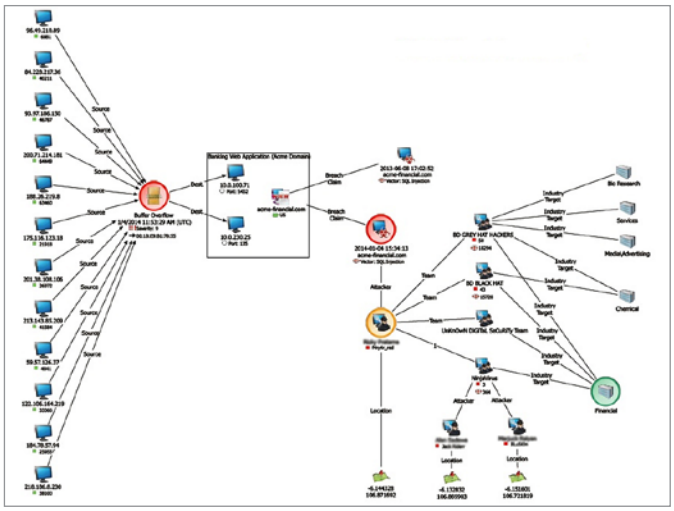

Figure 3: IBM i2 Enterprise Insight Analysis adds depth and breadth to your external breach investigations.

A cost-effective solution that supports operational efficiency

- Integrate with and use current infrastructures, systems and data
- Commercial 'off-the-shelf' design minimizes need for developer support
- Improve operational and situational awareness with dashboard and key performance indicators
- Uncover non-obvious relationships by applying multi-dimensional visual analytics
- Flexible and agile design can be easily extended with third-party and IBM applications to meet changing needs

Implement intelligent insider threat investigations

Insider threats pose unique challenges because of their legal and accepted access to the environment. The IBM i2 Enterprise Insight Analysis solution uses your existing security infrastructure and adds external intelligence data to overcome the challenges of investigating insiders. It also uses social media data, human resource data, expense data, inexplicable travel data, and even data about your insider threat's known associates.

External breach investigation

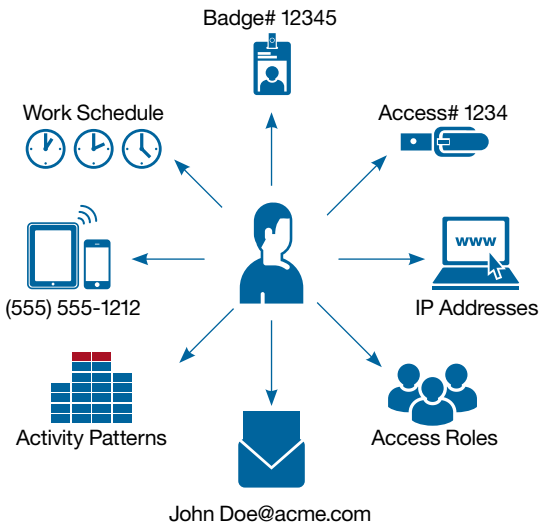

Figure 4: Threat forecasting can help focus internal and external threat investigation efforts.

Turn the tables with threat actor and team analysis

Use the IBM i2 Enterprise Insight Analysis solution to investigate both external and internal threat actors and their associations, preferred data targets and methods, and how threat actors capitalize on the leaked data.

Threat actor and team analysis, also known as threat forecasting, enables risk analysis that compares threats against known and discovered impacts, pinpointing exactly where the defensive teams need to concentrate their remediation efforts.

Take comprehensive action with risk analysis

For an accurate assessment of a breach's impact, your organization needs a comprehensive view of existing security controls and the strategies used by the organization. IBM i2 Enterprise Insight Analysis provides the platform you need to develop attack trees, create and analyze scenarios, create effective response plans, assess current controls, and direct precise remediation efforts.

Improve malware analysis with a holistic approach

Merging security product data and open source intelligence for malware analysis provides a holistic approach to malware analysis. With IBM i2 Enterprise Insight Analysis, you can visualize the connection between malware and behavior, and can study the impact and remediation needed to clear the infection.

The IBM i2 Enterprise Insight Analysis solution also enables easy correlation and tracing of a malware source. You can profile the entire malware system no matter which URLs threat actors use for their data distribution. For example, you can correlate an IP to a domain, and then trace the subsequent links associated with the configuration, distribution, and deposit architecture.

Malware infection investigation

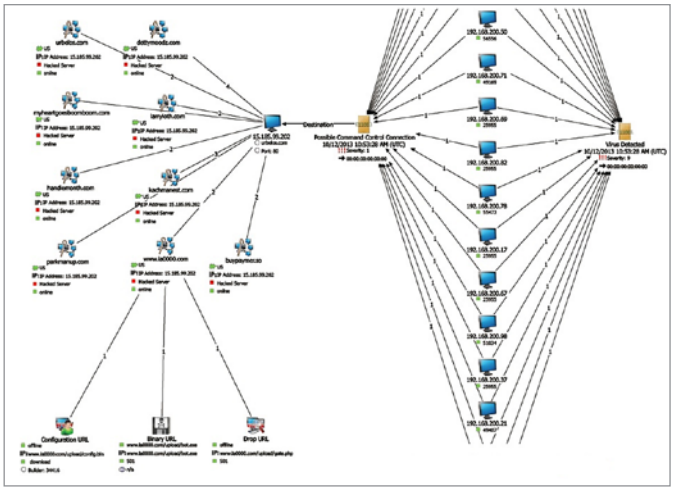

Figure 5: An example of a threat actor investigation an social network linkages between entities.

The IBM i2 Enterprise Insight Analysis solution in action

Intelligence agencies, governments, military and defense agencies, law enforcement, and commercial enterprises worldwide apply IBM i2 solutions to a broad spectrum of cyber threat analysis situations:

- Attribution of attacks and bad actors through IP and DNS resolution and geospatial mapping
- Social network analysis of botnets and other cyber attack networks
- IT network analysis and vulnerability mapping
- Identification of spam, phishing and malware
- Mitigation of insider threats and data leaks
- Tracking and analysis of advanced persistent threats

For more information

To learn more about IBM i2 Enterprise Insight Analysis, contact your IBM representative, or visit: ibm.biz/IBMi2EIA

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

1 **ibm.com**/sales/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSI_SE_TM_USEN&htmlfid=SEW03031USEN&attachment=SEW03031USEN.PDF

2 1 8 Ponemon Institute 2013 Cost of Cyber-Crime study

Please Recycle

ZZS03196-USEN-06