The Awakening of Cyber Analysis
IBM i2 Safer Planet

Bob Stasio – Sr. Product Manager, Cyber Analysis

FIN 4 Group Arrested

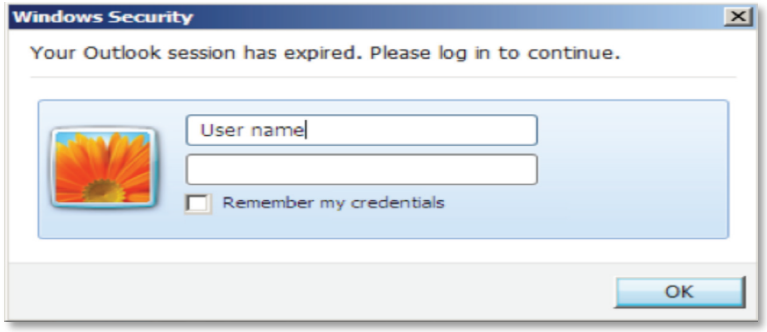


Fig. 1: Malicious prompt to capture credentials

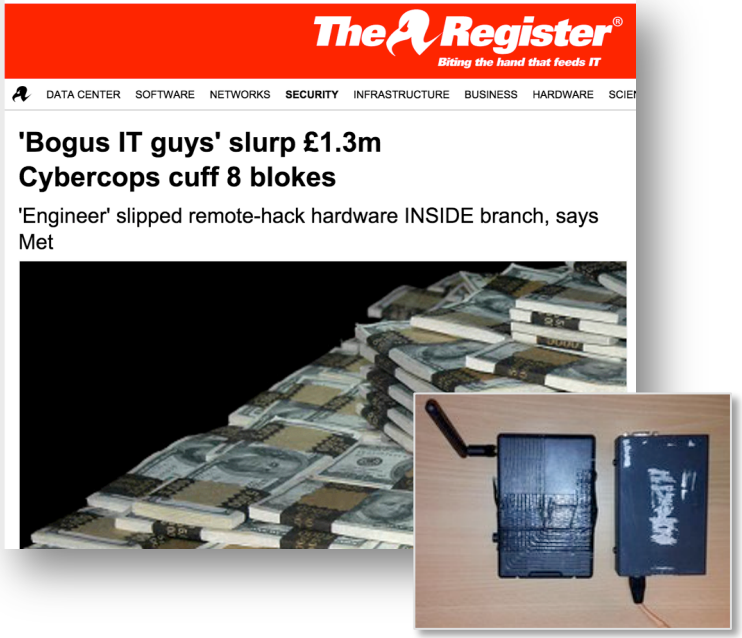
Fig. 2: Generic lure document

$100 MILLION DOLLARS IN PROFIT SINCE 2013

32 PEOPLE INVOLVED IN MULTIPLE COUNTRIES

The growth of asymmetric threats is changing the landscape

Information security has become a human vs. human problem



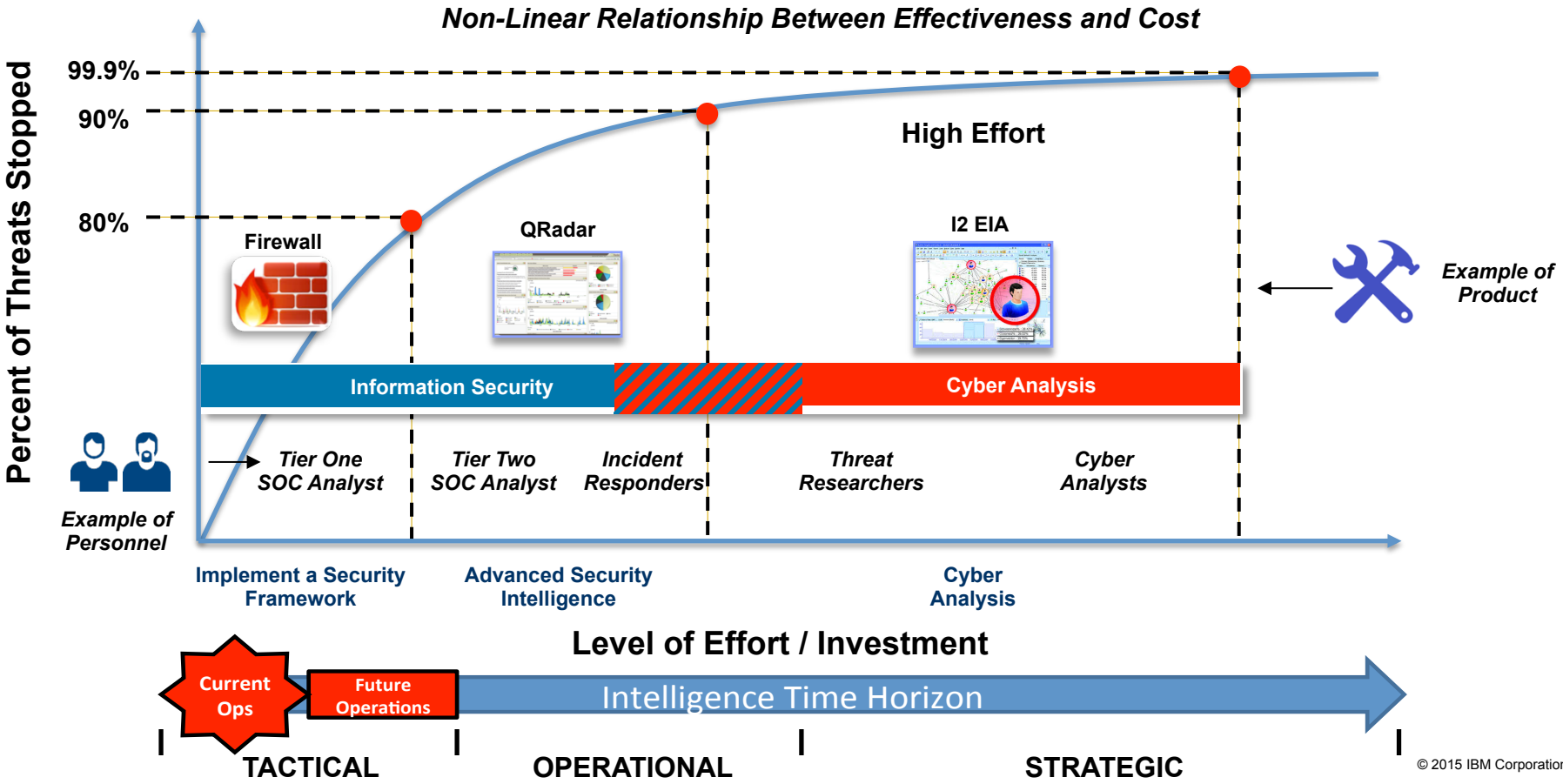
Remote control device

Hackers negate tens of millions of dollars in security infrastructure with a $30USD device!

1. A male posing as an IT technician deployed a $30USD remote control device on a bank branch office computer
2. The crooks connected to the device from a nearby hotel, then accessed the bank's servers
3. The hackers logged into a bank terminal and shifted ~$2.1M USD through 128 transfers into mule accounts

The gang responsible for the theft was caught 13 months later only due to attempting the same attack at another bank

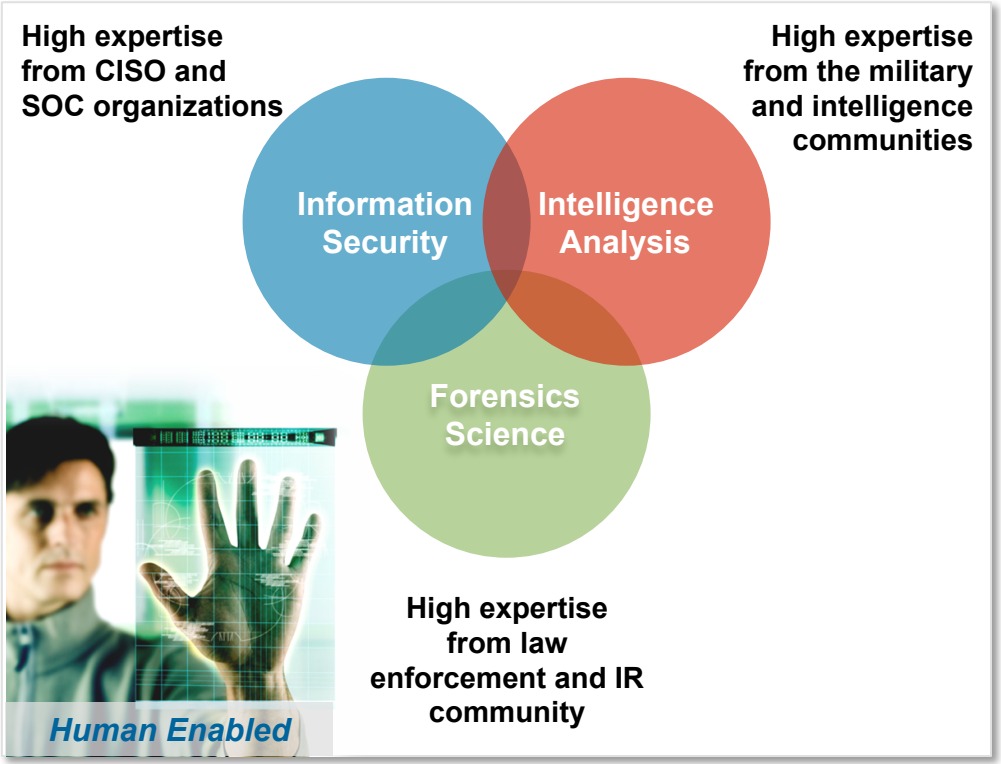
Both security and analysis must address the problem



Learning from medical analogies

	MEDICAL		SECURITY	
	Threat Example	**Mitigation Strategy**	**Threat Example**	**Mitigation Strategy**
Tier One – Hygiene	Common hospital associated infections	Washing hands, wearing masks and scrubs	Commodity threat, individual hackers with widely-used tools	Changing passwords, removing unused services, patching
Tier Two – Specialization	Emergent situations (e.g. chest pain, gunshot wound)	Creation of critical care and preventative medicine discipline	Organized crime, semi-tailored fraud and crimeware tools	Visibility, monitoring, alerting, response, real-time security analytics
Tier Three – Research	Genetic diseases and cancer	Research and tailored genetic treatments	Advanced Persistent Threat, nation-state, high resources	Cyber analysis, threat intelligence trend analysis, campaign tracking

The cyber analysis discipline addresses the human dimension



The Cyber Analysis Discipline

Cyber Analysis is a new discipline and profession with three subcomponents

- **Information Security** blends aspects of network defense, confidentiality, assurance, and malware threats
- **Intelligence Analysis** brings the art of the intel cycle where information is directed, collected, processed, analyzed, produced, and disseminated
- **Forensics Science** blends aspects of the investigative process, evidence handling, and latent evidence discovery

Why You Need Cyber Analysis

Information Security alone is not enough, companies need to open the aperture:

The domain of CYBER is the discipline of examining multi-dimensional security…a threat can come from an external hacker or an insider threat

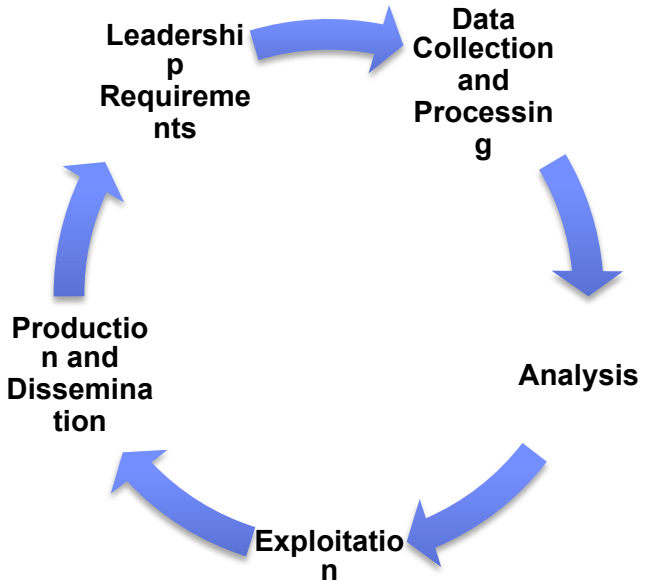
Security Analytics: The art of aggregating, correlating, and automating information technology (IT) related data in order to detect, discover, and understand information security threats.

Cyber Analysis: The art of human-led analysis of security and non-security related data from logical and physical domains in order to research trends, discover anomalies, provide context, create relationships, and uncover hidden issues.

Cyber Intelligence: Evidenced-based knowledge and actionable advice concerning security related issues.

Security Intelligence: Actionable information derived from the analysis of security-relevant data available to an organization.

Accelerate Decision Making with The Intelligence Cycle



- 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)

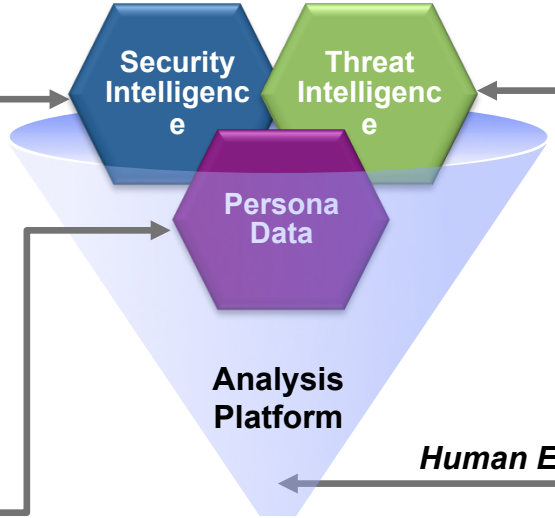
Cyber Analysis

Mostly IT Sources

- PCAP
- SIEM
- Alerts
- SSO/AD
- System Logs
- Vulnerability Scans

Mostly Human Sources

- Behavioral Data
- Account Creation
- HR Data
- Badge Logs
- Reviews
- Access Logs



Mostly External Sources

- Hacker Forums
- Social Media
- Intel Vendors
- Government Alerts
- Threat Indicators
- Community Info

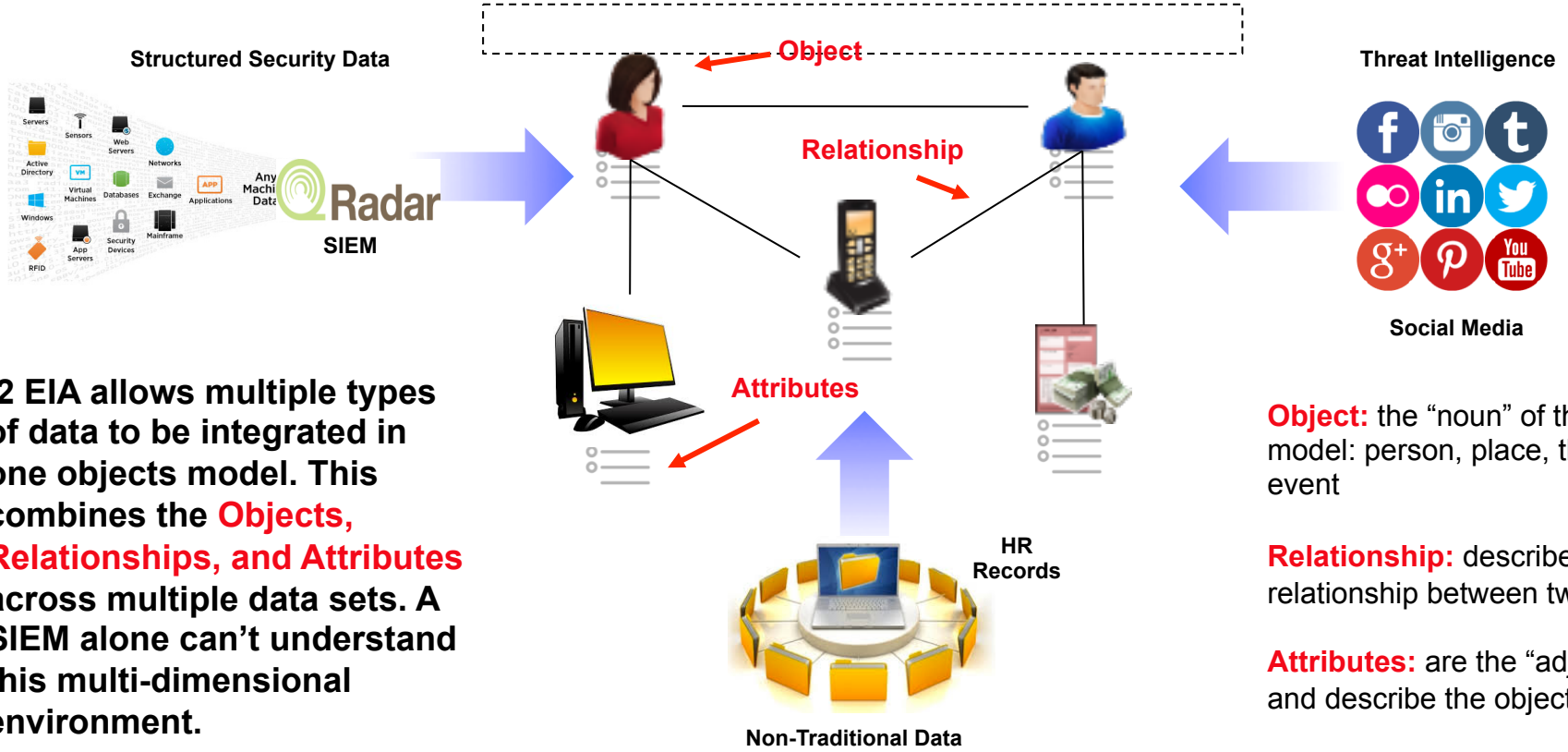
Human Enabled

Cyber Analysis Results

- Integrated data feeds
- Enterprise awareness
- Compliance monitoring
- Threat discovery
- Risk management
- Enable decisions

Leveraging an analytical platform and internal and external information feeds, Cyber Analysts can help form a deep understanding of the threats targeting your organization

Why i2 EIA is Vitally Important: One Schema, One Object Model



i2 EIA allows multiple types of data to be integrated in one objects model. This combines the Objects, Relationships, and Attributes across multiple data sets. A SIEM alone can't understand this multi-dimensional environment.

Object: the "noun" of the data model: person, place, thing or an event

Relationship: describes the relationship between two objects

Attributes: are the "adjective" and describe the objects

Build a Sophisticated Intelligence Capability

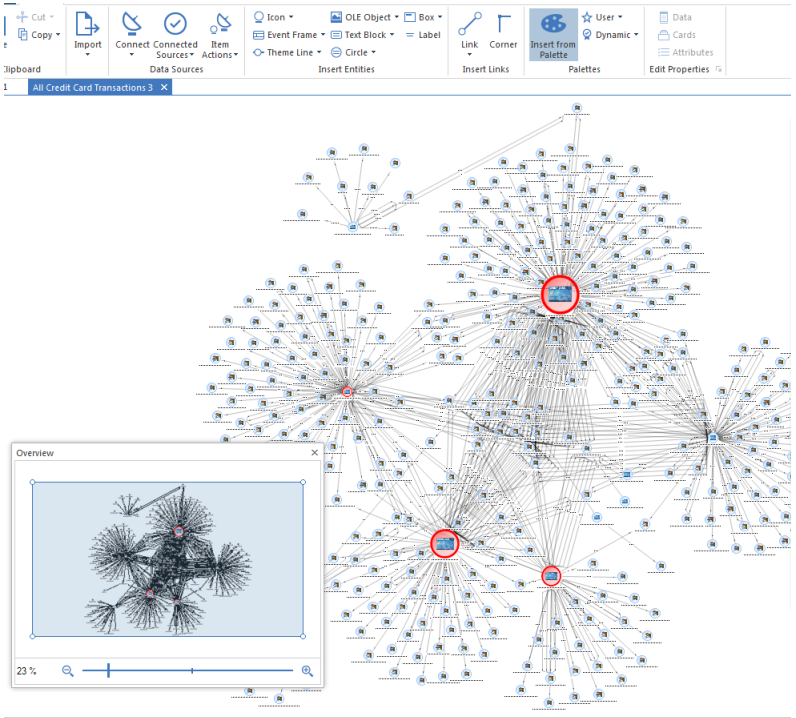
Human guided intelligence analysis to uncover evidence of criminality awareness of links, networks, anomalies, trends.

What we are looking at

- People, Objects, Locations, Events
- Structured & Unstructured
- Deep & Dark Web
- External data
- Social Networks

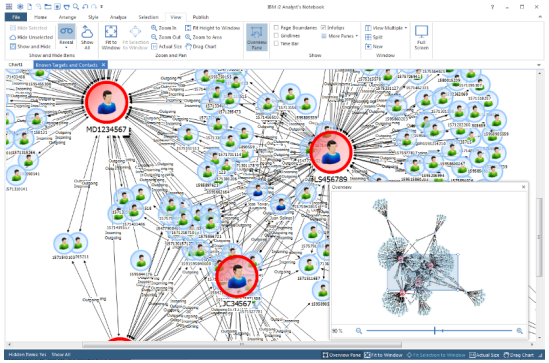
What we are looking for

- Networks
- Relationships
- Patterns in the data
- Anomalies in geography, timing, sequencing

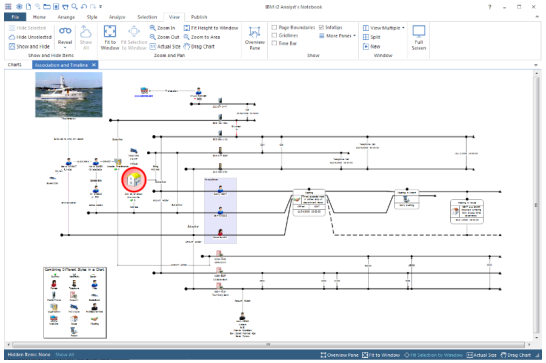


i2 EIA Delivers Integrated Multi-Dimensional Analysis Capabilities

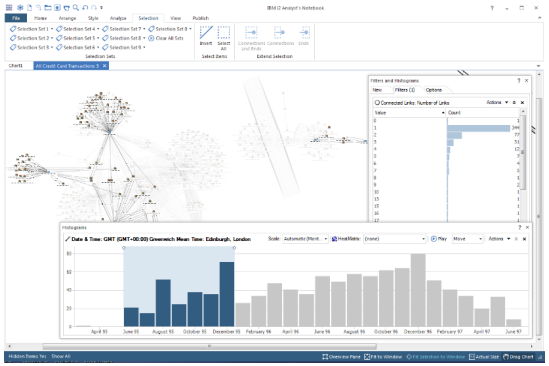
Network & Link analysis



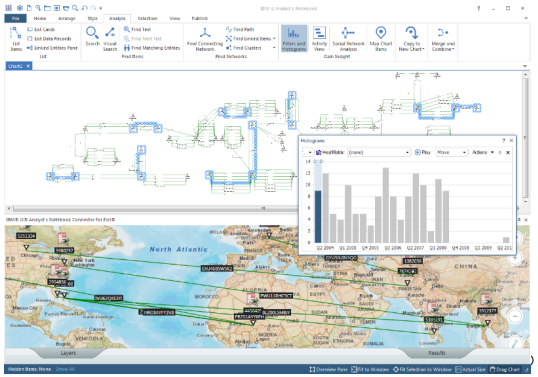
Transactional timelines



Analytical Tools: histograms, activity heat maps, and Social Network Analysis



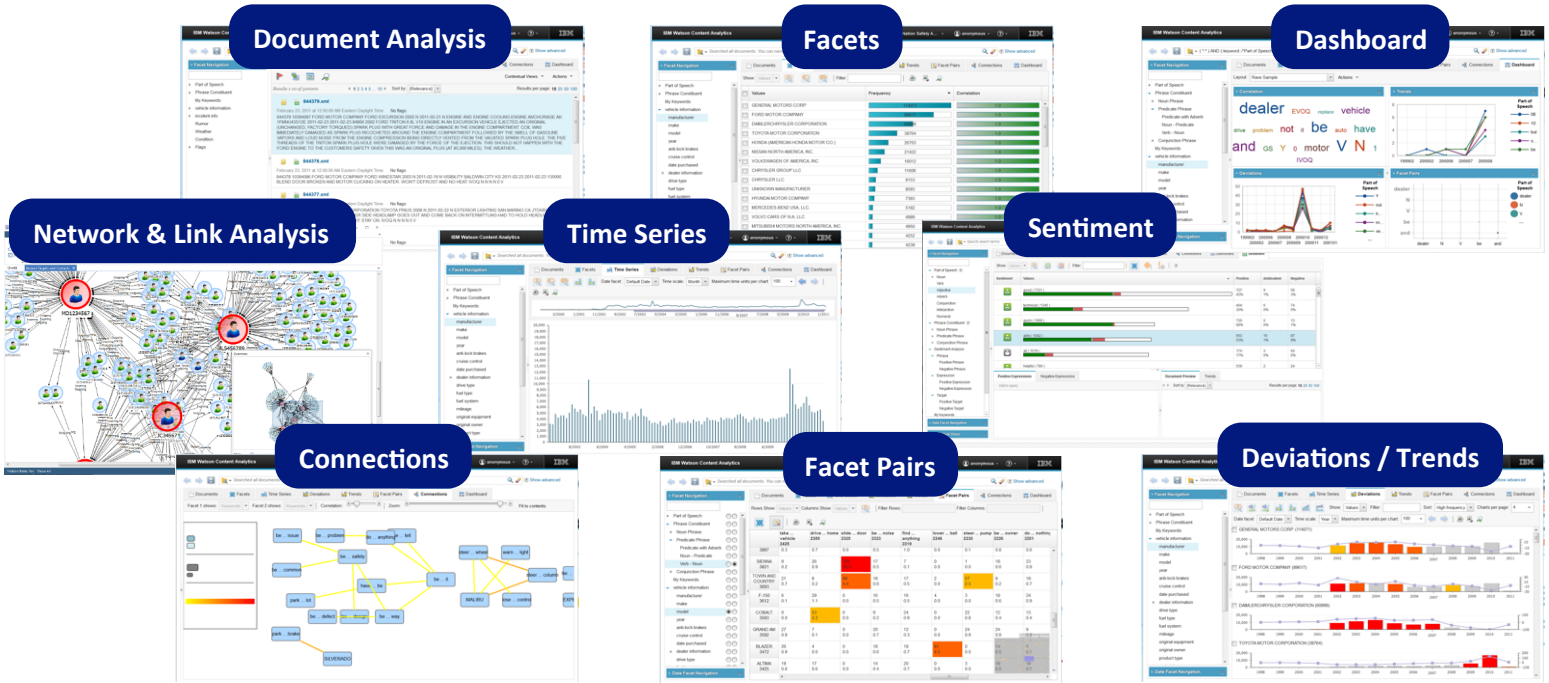
Geospatial Interoperability



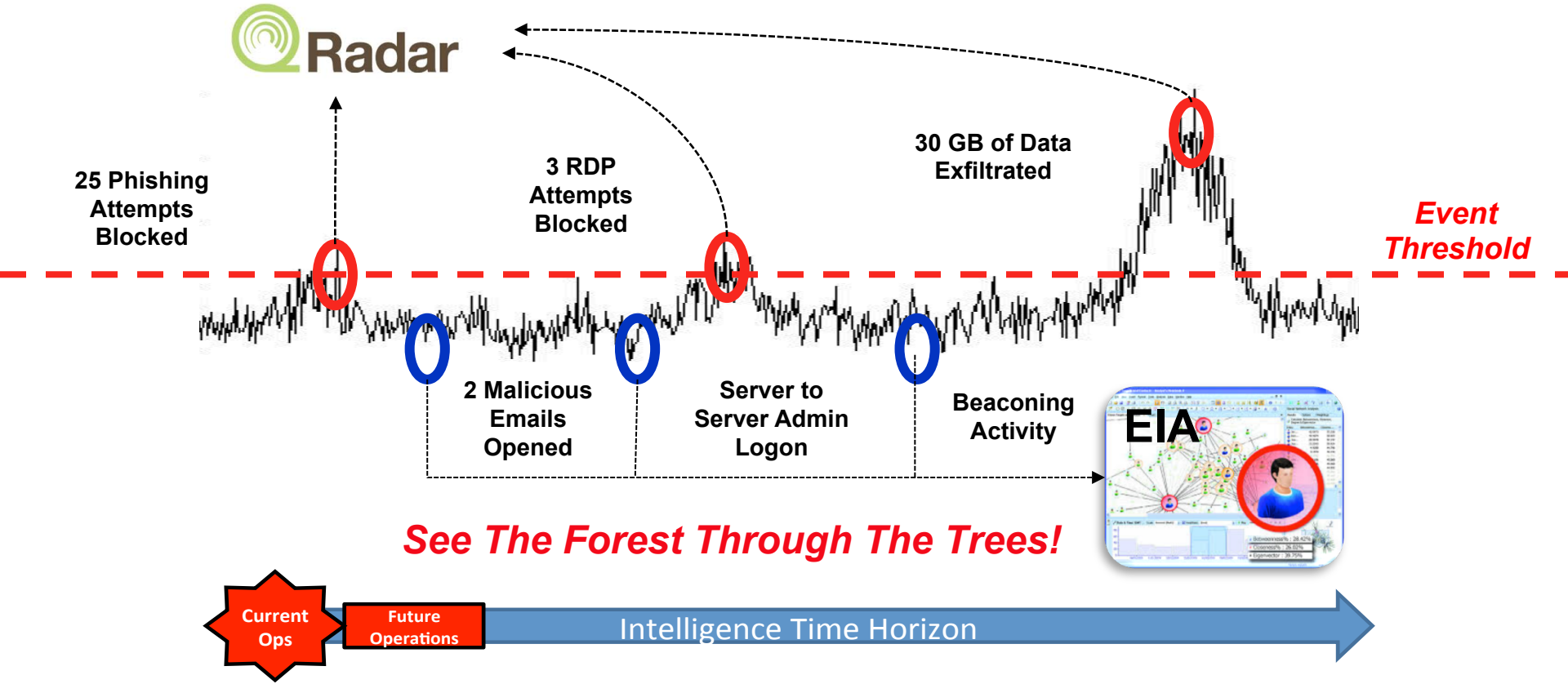
i2 EIA Delivers Integrated Multi-Dimensional Analysis

To exploit data in many ways for many users…

Capabilities



Tipping, Queuing, and Anomaly Research Example



Four Main Pain Points in Cyber Security Today

Hidden Threats Hiding in Network

How do I find the signals in the noise?

Where Should Analysts Look

How to find a needle in a stack of needles?

Lack of Actionable Intelligence

How do leaders make decisions?

Too Much Data, Too Many Sources

How do I put the picture together?

IMPACT

$35 MILLION - SONY

1,400 PEOPLE - ISIS HIT LIST

$162 MILLION - TARGET

14 MONTHS - OBY CLEANUP

USE CASES

- Finding beaconing
- Strange admin logs
- Employees caching info
- IP theft and exfiltration

- SIEM tipping and queuing
- External physical threats
- Host intrusion correlation
- Ext. breach discovery

- Intelligence led security
- Understand vendor risk
- Incident reporting
- Risk analysis

- APT kill chain analysis
- Darkweb integration
- IOC historical search
- Vulnerability prioritization

Contributing Factors to The Cyber Security Problem

Increased data sources

The amount of devices on a network is expanding exponentially, organizations need to sift through data from their many devices and unstructured data from vendors.

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.[1]

Sophistication of the attackers

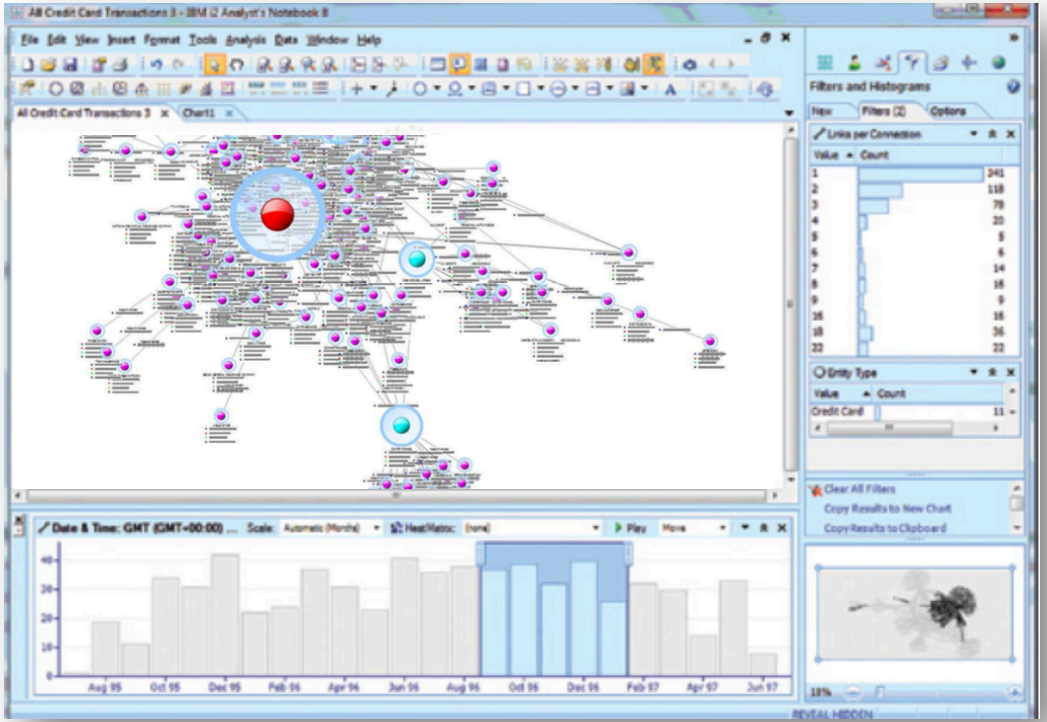
"But, cyber attacks are growing every day in strength and velocity across the globe." — Jamie Dimon, JPMorgan's chairman and Chief Executive [2]

Little Attention to Resilience

Organizations tend to spend a majority of their resources on perimeter security and monitoring at gateway "chokepoints". When an adversary gets onto the network there is little ability to detect and respond before the damage is done.

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 Perlroth, 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

How i2 EIA Helps You Find Cyber Threats Quickly



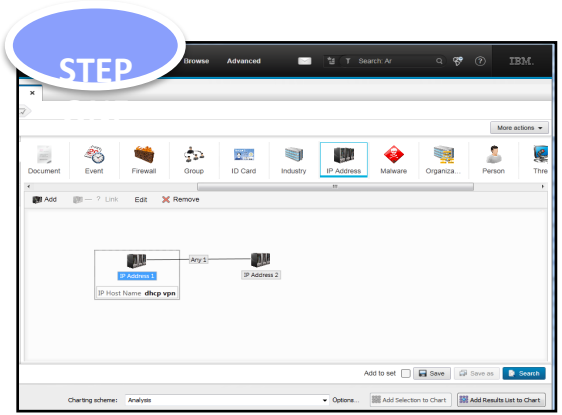
Visualize and Investigate

See data from multiple sources in a unique object model for exploration

- **Visual Query** lets you query your data without technical or database skills, improving the quality and productivity of investigations
- **Find Path** allows your to uncover relationships between billions of potential paths within seconds
- **Conditional Formatting** spreads the skills of your master analysts by adding emphasis to objects and relationships to make issues immediately visible

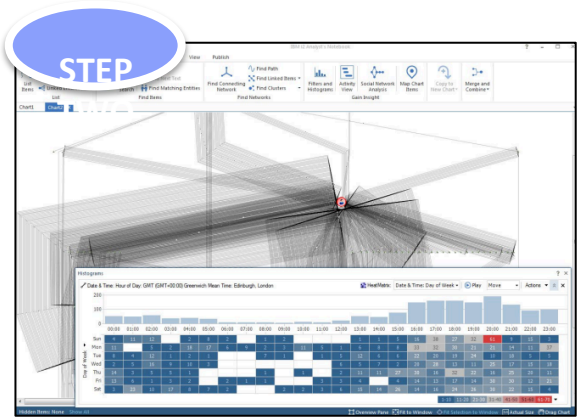
How i2 EIA Helps You Find Cyber Threats Quickly

Example: Is there evidence of undetected malware in my network?



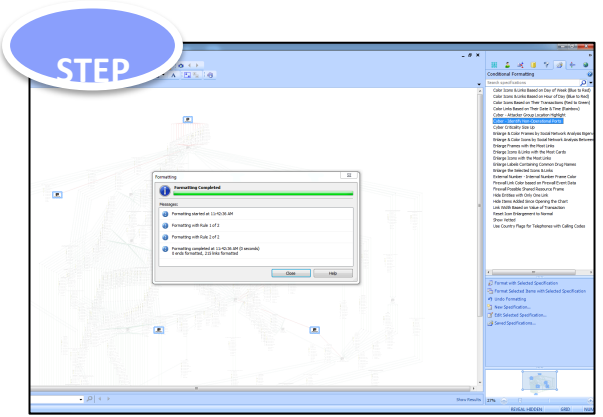
Search Proxy Logs

Analyze your logs by simply drawing the query you would like to run, including any parameters like a specified time period



Discover Beaconing Activity

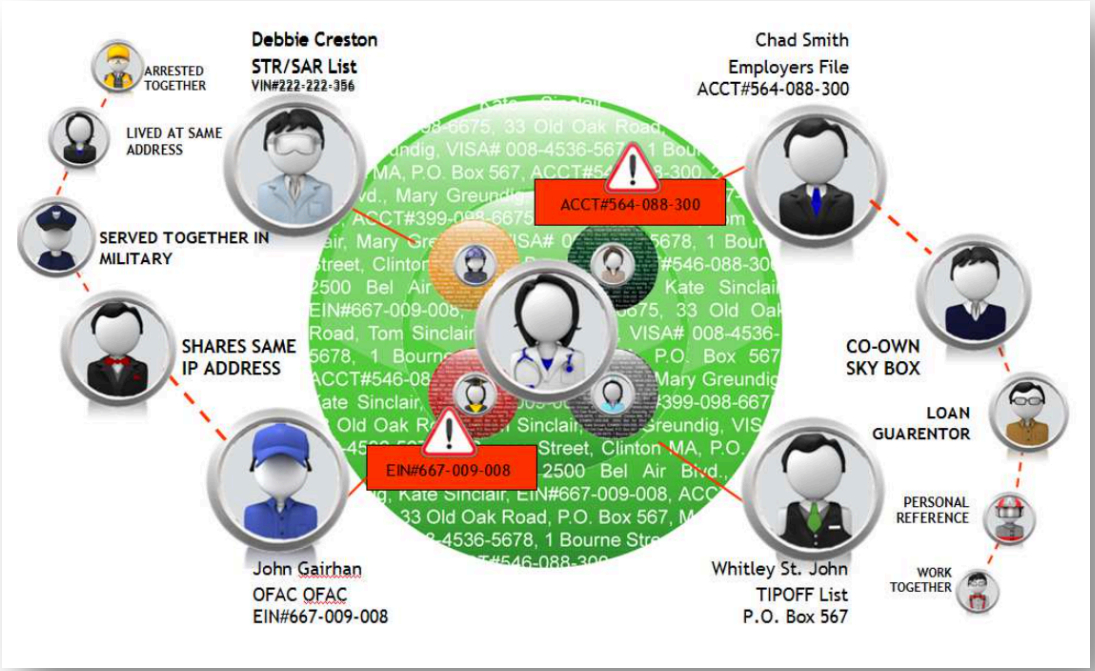
Utilize the find path feature to discover relationship between C2 nodes and proxy logs. Temporal visualizations shows periodic activity



Save Parameters for Alerting

Setup conditional formatting to search for the same factors and show emphasis between relationships and objects when being examined on the chart

How i2 EIA Helps You Discover Patterns and Anomalies



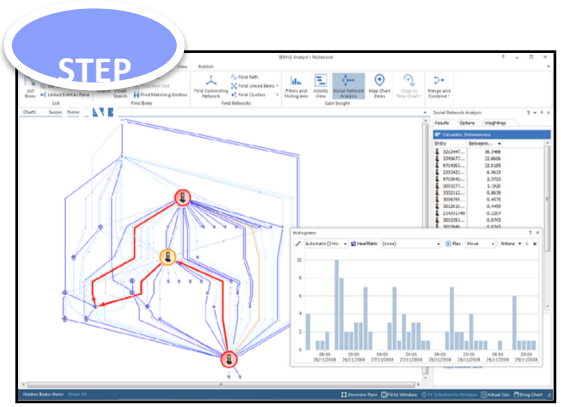
Robust Analytics Built Right In

Deep algorithms that become better over time in detecting non-obvious events

- **Entity Resolution** allows you to merge like objects and find out “Who is Who” and “Who knows who” – alerting you in real-time
- **Recommendation Engine** discover key patterns, events, and relationships that are nearly impossible to detect through manual analysis
- **Social Network Analysis (SNA)** ranks relationships between objects using multiple network analysis algorithms including K-Core,

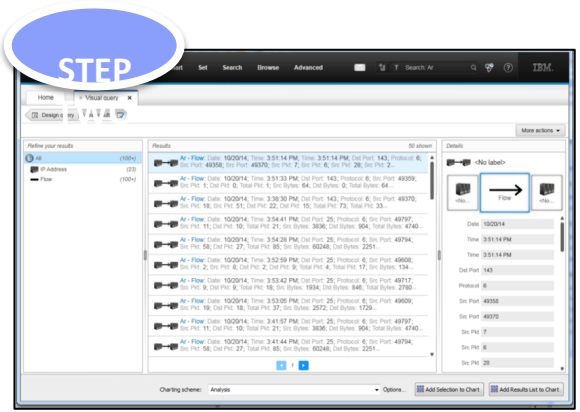
How i2 EIA Helps You Discover Patterns and Anomalies

Example: Are there insider threats compromising intellectual property?



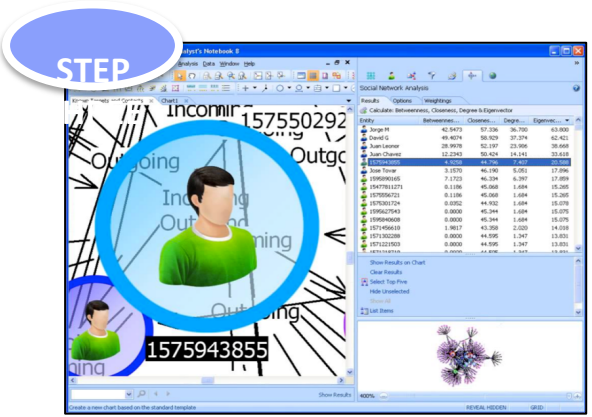
Discover Odd Patterns

Analyzing email and chat communication data to uncover patterns of employees communicating across business units uncharacteristically



Confirm Malicious Behavior

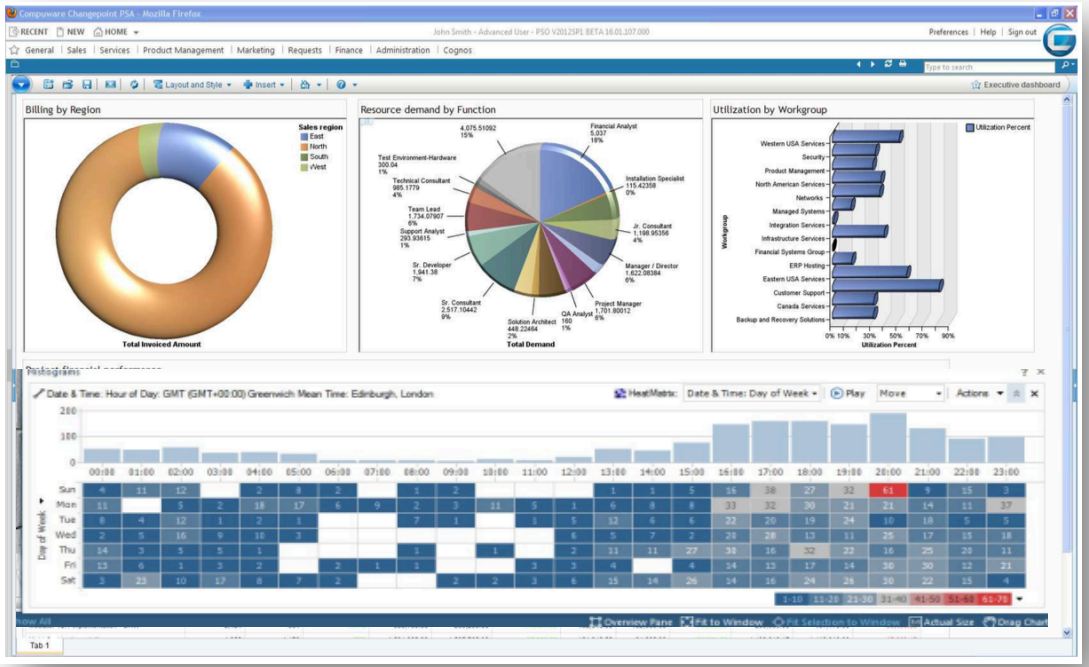
After identifying persons of interest, search proxy logs to confirm that a group of developers have been caching code to personal accounts



Determine Extent of Network

Searching social media, we find that a group of developers plan to leave an create a rival startup. Using SNA, we can identify a network of potential individuals involved

How i2 EIA Helps You Create Actionable Intelligence



Go From Discovery to Action

Create custom dashboards and reporting from many sources of data

- **Operational Awareness** configures a dashboard with your Key Performance Indicators (KPIs) to monitor health
- **Reporting Functionality** creates custom reports from your data and chart findings to share with leadership
- **i2 Web Client** allows non-analysts to interact with and understand an ongoing investigation with a straight forward web browser interface

How i2 EIA Helps You Create Actionable Intelligence

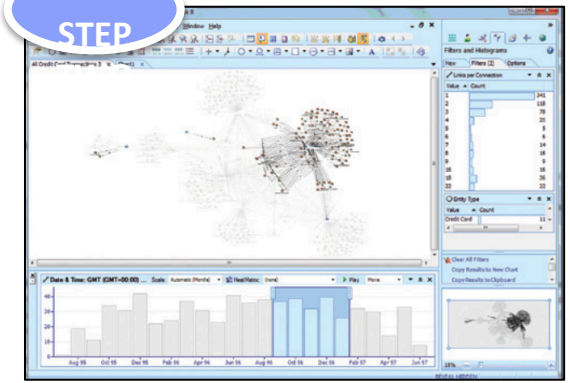
Example: What are the most critical areas of the network to concentrate on?

STEP

See KPIs in Real Time

Monitor all business units for network use, incidents, and compliance to understand enterprise risk in real time

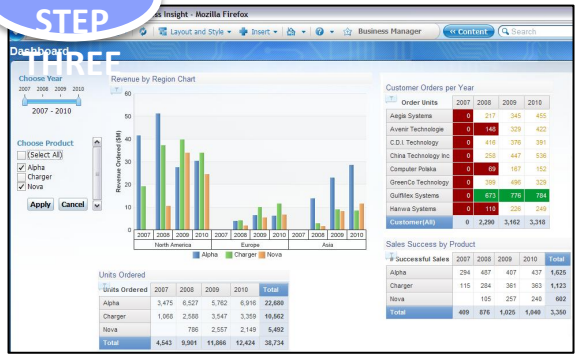
STEP



Vulnerabilities & Criticality

Compare vulnerability scans from each business unit with the network criticality and threat level. Rack and stack the most critical components under high threat

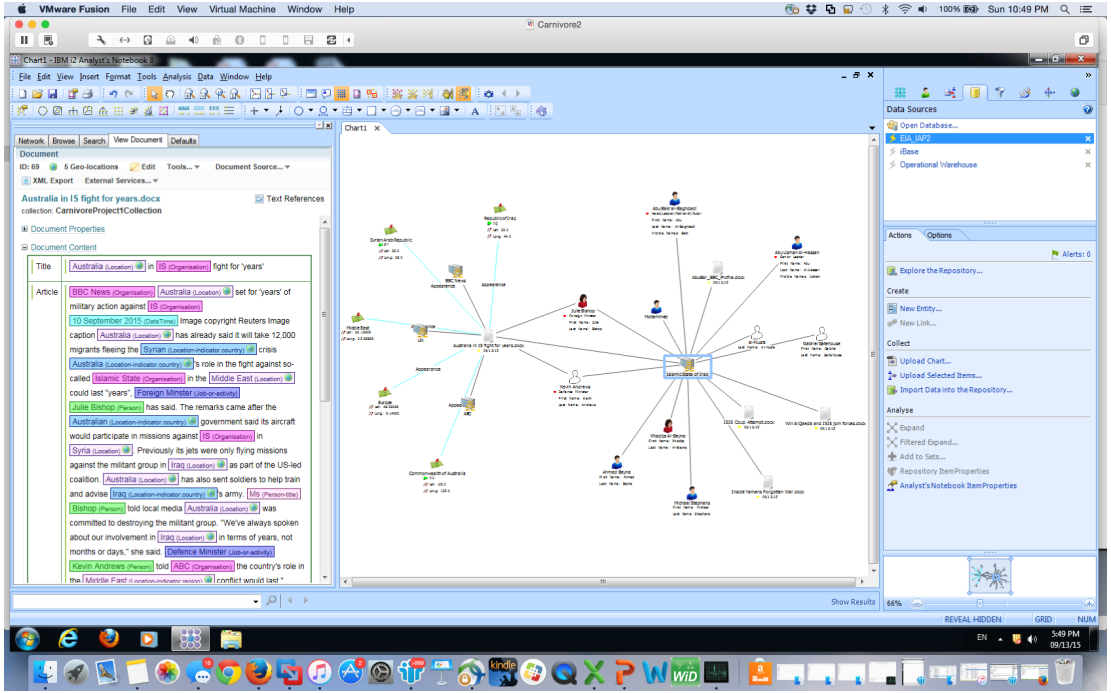
STEP



Produce Statistical Reporting

Create periodic reporting to show business units where to focus security controls in order to most effectively mitigate risk

How i2 EIA Helps You Understand Multi-Dimensional Data



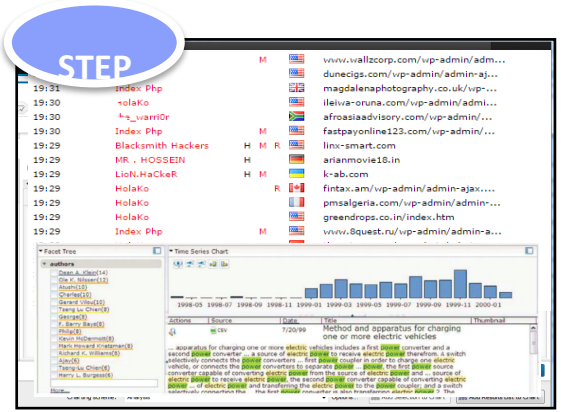
Provide Structure to Chaos

Merge structured and unstructured data into a single custom object model

- **Entity and Relationship Extraction** creates entities from feeds like email, social media, and outside news sources in real-time
- **Entity Link Analysis** automatically can infer relationships between entities in your object model
- **Context and Correlation** leverages powerful analytic engines to provide context and expose insights

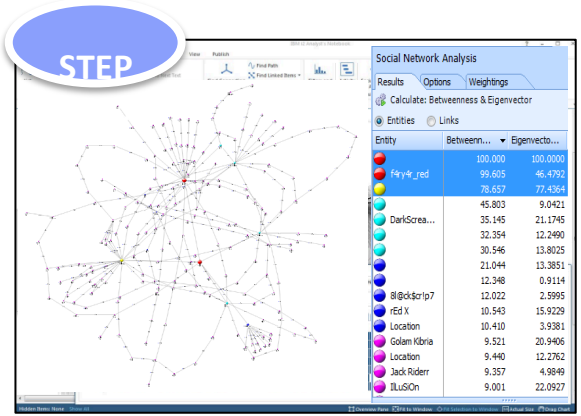
How i2 EIA Helps You Understand Multi-Dimensional Data

Example: How can I find who would attack me from threat intelligence?



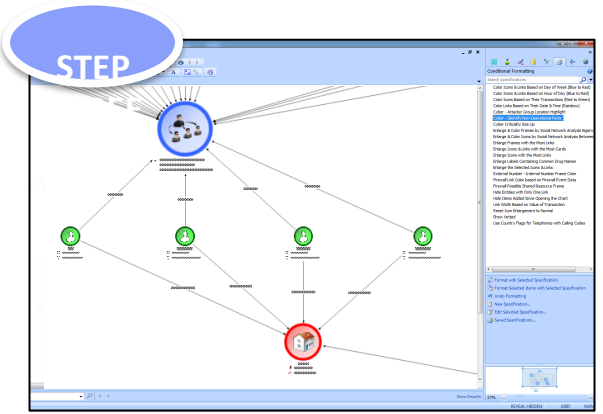
Sift Through Threat Reporting

Identify and extract key data objects from various email, news feeds, community, and vendor threat intelligence



Conduct Link Analysis

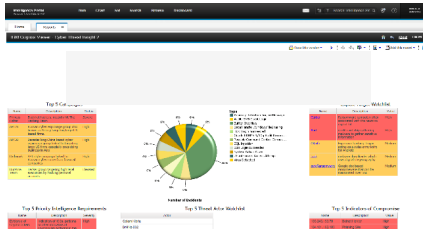
Use entity link analysis to understand which threat groups have to closest relationship to techniques which match your network and organization profile



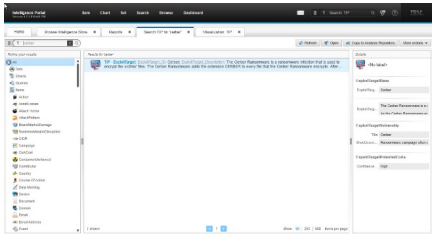
Compare to Dark Web Data

Focus on the key groups relevant to you. Through vendor feeds, observe their activity on the dark web to determine if they are planning and attack

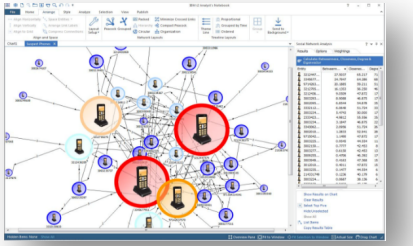
Executive & Operational Dashboard



Triage & Investigations



Analyst Workbench



User Interface Layer

Analytics Layer

Statistical

Scoring and

Third Party

api

Storage Layer

Vetted Intelligence Data Store

Operational Warehouse

Extraction Layer

Structured & Unstructured Data Extraction

Ad Hoc

API

RT/NRT

Data Source Layer

Case Management

SIEM

HR Records

Wiki

Logs

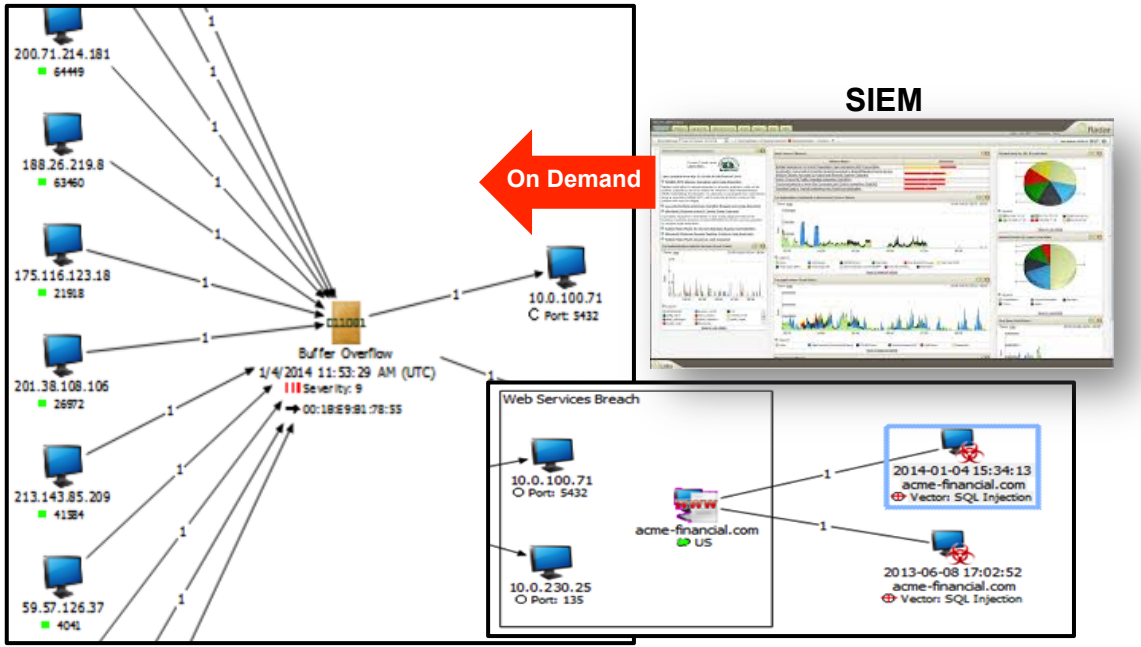
Social Media

Threat Intelligence

News

Malware

Tactical Cyber Intelligence Operations



"An investigation that would have taken me all day in Splunk took me 10 clicks with i2."
-Brian Olson, VP Security Operations & Architecture

Northern Trust

Extending Investigations and Function

On Demand Access to SIEM data, notable events, and alerts:

- **Expand on an Alert** analysts can ties together an alert to multiple previous events, opening up the investigation
- **Enable Hunting** explore the SIEM data in a different way, uncovering patterns of interest and unseen events
- **Light Weight Deployment** i2 EIA takes advantage of the SIEM data warehouse and seamlessly connects 10 analysts to the system getting up and running in less than 30 days

EIA Cyber Analysis Use Cases

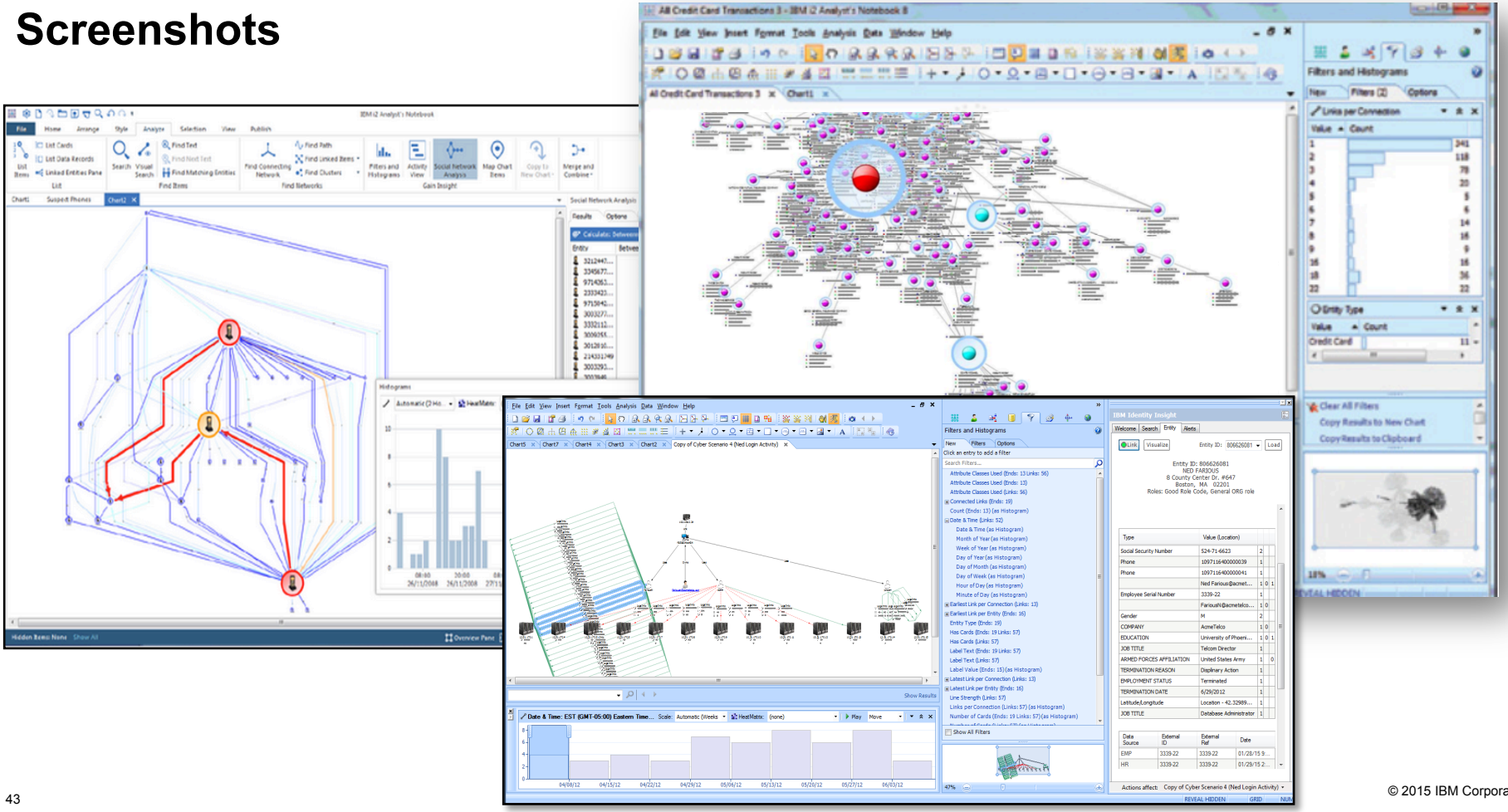
General Use Cases

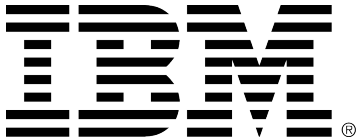
- Advanced Persistent Threat Discovery
- Insider Threat Identification and Investigation
- Disgruntled Employee Identification
- Employee Sensitive Data Caching
- Asset Vulnerability vs. Criticality Comparison
- Threat Campaign Tracking
- Strategic Report Production for Leadership
- HIPS and IDS Correlation
- External Scanning Pattern Analysis
- Spear-phishing Identification and Impact Analysis
- Pirated Software Use Identification
- Threat Intelligence Integration into Incidents
- Big Data Analysis Search Across Large Data Sets

Financial Sector Use Cases

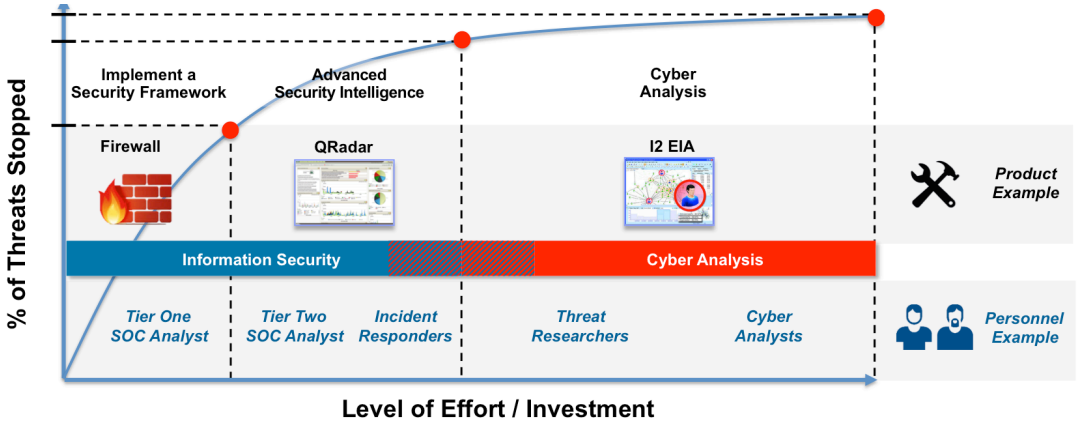
- Fraud Detection and Investigation
- Retrace Trades for Compliance
- Insider Trading Identification and Investigation
- Executive Information Security Protection
- Reputation and Brand Awareness
- Integration of State-Level Threat Reporting
- Vendor Risk Management Compliance Tracking
- Identify Employees with Competitive “Side Jobs”
- Identify Individuals Leaking info to Media
- Discover Customer Data Leaked Online
- Discover Leaked Sensitive Documents Online
- Darkweb Data Aggregation and Discovery
- Social Media Monitoring and Investigation

Screenshots





Cyber Analysis builds on Security Intelligence



Customer Pain Points after a SIEM:

Hidden Threats Hiding in Network
How do I find the signals in the noise?

Lack of Actionable Intelligence
How do leaders make decisions?

Where Should Analysts Look
How to find a needle in a stack of needles?

Too Much Data, Too Many Sources
How do I put the picture together?

i2 Key Complimentary areas to QRadar

- Unstructured data transformation
- Non-traditional data (e.g. news, SM)
- Trend analysis and visualization
- Discover “unknown, unknowns”
- User defined analytics
- Data enrichment and correlation
- Investigation and discovery tooling
- Intelligence report creation
- Advanced link analysis
- Streamline workflow w/ many sources
- Geospatial integration
- Analyst object customization
- Non-obvious relationship discovery
- Entity connection discovery
- Strategic Threat Campaign tracking

Why You Should Care About a Joint Sales Strategy

Security Intelligence

IBM Security QRadar®

splunk>

"The Splunk Killer for Security Intelligence"

- QRadar is the market leading security intelligence platform with out-of-the-box rules, analytics, and reporting
- i2 is integrated with QRadar for extensive visualization and multi-dimensional analysis
- Splunk requires custom integration with a 3rd party product to provide visualization

Cyber Analysis

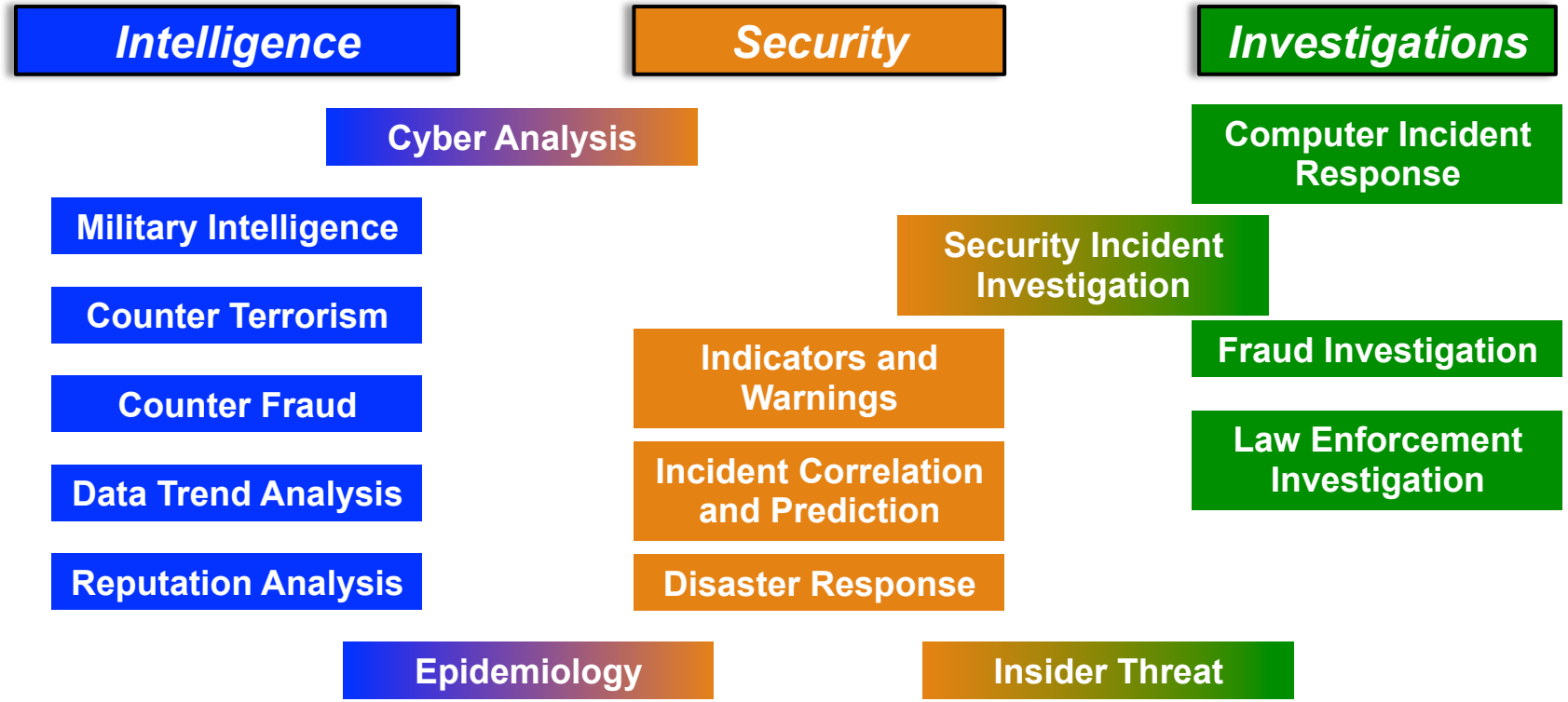
IBM Enterprise Insight Analysis

Palantir

"The Palantir Killer for Cyber Analysis"

- i2 integrates with QRadar, the industry leading SIEM
- Palantir has no internal security expertise
- Custom integration with Palantir and a SIEM requires significant investment in resources and/or services

I2 Enterprise Insight Analysis – Use Cases



Cyber Analysis: Human Enabled Intelligence

Intelligence Focus Process

Collect data on my network

Raw Data

→ **Logs, PCAP, Alerts, Scans**
IDS, Firewall, Vulnerabilities

Firewall

Matching "known bad" signatures against my data

Indicators

→ **IOC Matching**
IOC Feed, Log aggregator

Uncover "known bad" patterns in my data

Analytics

→ **Trends, Patterns**
UBA, Algorithms, Offenses

QRadar

Generalized statistics to discover bad things in my data

Heuristics

→ **Anomalies, Outliers**
Clustering, Rec. Engine

Machine assisted learning that understands the bad things to look for

Cognitive

→ **Context related awareness**
User defined search, Watson Explorer

i2 EIA

Testing theories, validating hypothesis by asking questions of the data and reaching evidence based conclusions

Theorizing

→ **Forming a hypothesis**
Visualization, investigation

Legal Disclaimer

- © IBM Corporation 2015. All Rights Reserved.
- The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.
- References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.
- If the text contains performance statistics or references to benchmarks, insert the following language; otherwise delete:
  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.
- If the text includes any customer examples, please confirm we have prior written approval from such customer and insert the following language; otherwise delete:
  All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.
- Please review text for proper trademark attribution of IBM products. At first use, each product name must be the full name and include appropriate trademark symbols (e.g., IBM Lotus® Sametime® Unyte™). Subsequent references can drop "IBM" but should include the proper branding (e.g., Lotus Sametime Gateway, or WebSphere Application Server). Please refer to http://www.ibm.com/legal/copytrade.shtml for guidance on which trademarks require the ® or ™ symbol. Do not use abbreviations for IBM product names in your presentation. All product names must be used as adjectives rather than nouns. Please list all of the trademarks that you use in your presentation as follows; delete any not included in your presentation. IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, WebSphere, UC2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.
- If you reference Adobe® in the text, please mark the first use and include the following; otherwise delete:
  Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- If you reference Java™ in the text, please mark the first use and include the following; otherwise delete:
  Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- If you reference Microsoft® and/or Windows® in the text, please mark the first use and include the following, as applicable; otherwise delete:
  Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.
- If you reference Intel® and/or any of the following Intel products in the text, please mark the first use and include those that you use as follows; otherwise delete:
  Intel, Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- If you reference UNIX® in the text, please mark the first use and include the following; otherwise delete:
  UNIX is a registered trademark of The Open Group in the United States and other countries.
- If you reference Linux® in your presentation, please mark the first use and include the following; otherwise delete:
  Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others.
- If the text/graphics include screenshots, no actual IBM employee names may be used (even your own), if your screenshots include fictitious company names (e.g., Renovations, Zeta Bank, Acme) please update and insert the following; otherwise delete: All references to [insert fictitious company name] refer to a fictitious company and are used for illustration purposes only.