IBM i2 Summit for a Safer Planet
Network. Explore. Learn.
August 12-13, 2015 Hyatt Canberra

IBM

Keynote: Cyber Intelligence and Cyber Security Overview

David Waxman – Executive Architect EIA
Bob Stasio – EIA for Cyber Security Product Manager
Ralph Klaassen – Senior Architect EIA

Important 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.

3

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

4

Today's attackers are sophisticated and relentless

This group can bypass ***any*** static network security given enough time and resources

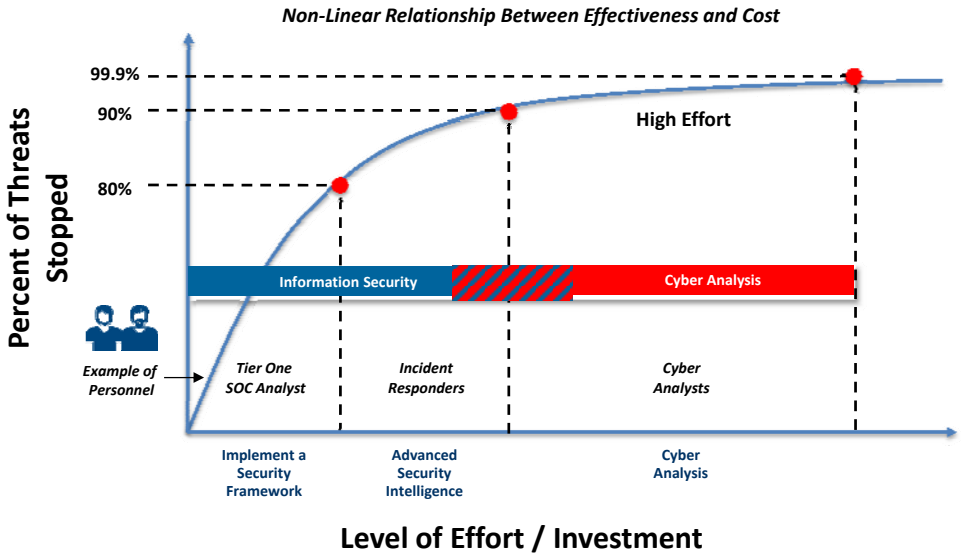
Use security intelligence and cyber analysis to detect their presence through anomalies

- Command and control
- Proliferation
- Exfiltration

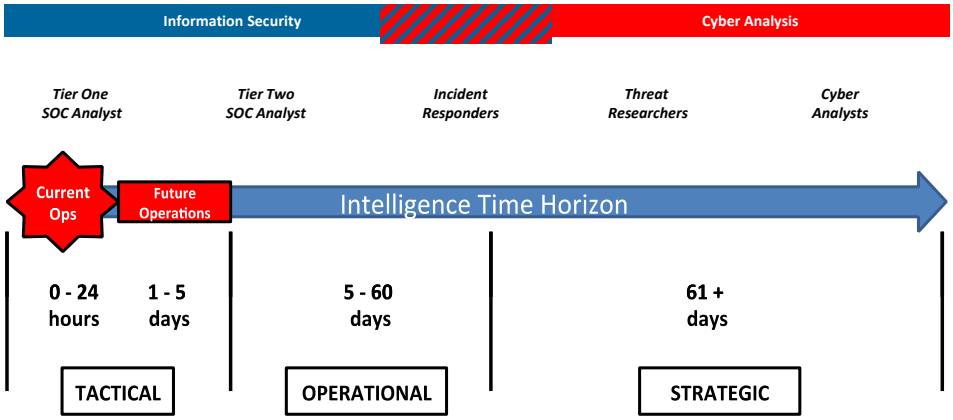
Most effectively mitigated by implementing an integrated framework of security controls

5

Both security and analysis must address the problem



Intelligence as a Time Horizon



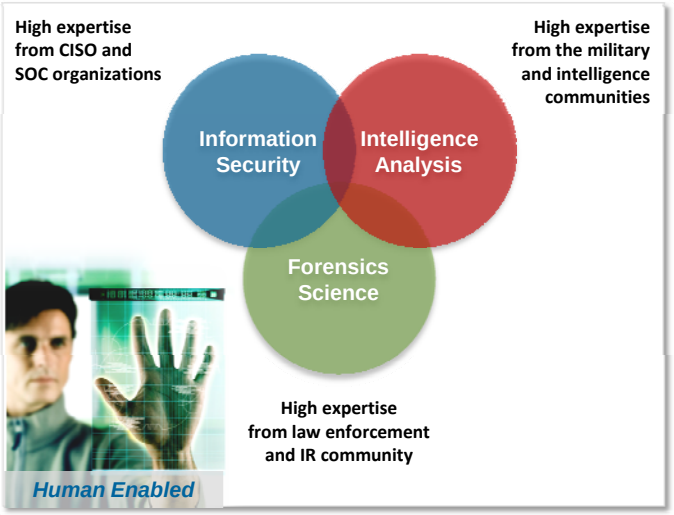
7

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

8

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

9

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

1

Workflows

Security Intelligence
IBM Security QRadar®

Cyber Analysis
IBM Enterprise Insight Analysis

Threat Research
IBM X-Force®

Enrich → Produce → Visualize → Analyze

Continuous Feedback Loop

1

Domain Generalities

SECURITY	CYBER
Structured data	Unstructured data
Automatic detection	Manual analysis
Real-time operations	Long-term research
Universal configuration	Customized
Anomaly detection	Anomaly discovery
Roll-over data	Big data storage
Organizational visibility	Ecosystem visibility
Threat management	Threat discovery
Logical domain	Physical domain
Traditional data sources	Non-traditional data sources

1

IBM's Strategic Threat Analysis Capability

Machine enabled

Security Intelligence Platform

Real-time processing

- Real-time data correlation
- Anomaly detection
- Event and flow normalization
- security context and enrichment
- Distributed architecture

Security Operations

- Pre-defined rules and reports
- Offense scoring and prioritization
- Activity and event graphing
- Compliance reporting
- Workflow management

Strategic Intelligence

Human enabled

Cyber Analysis Platform

Multi-Dimensional Analysis

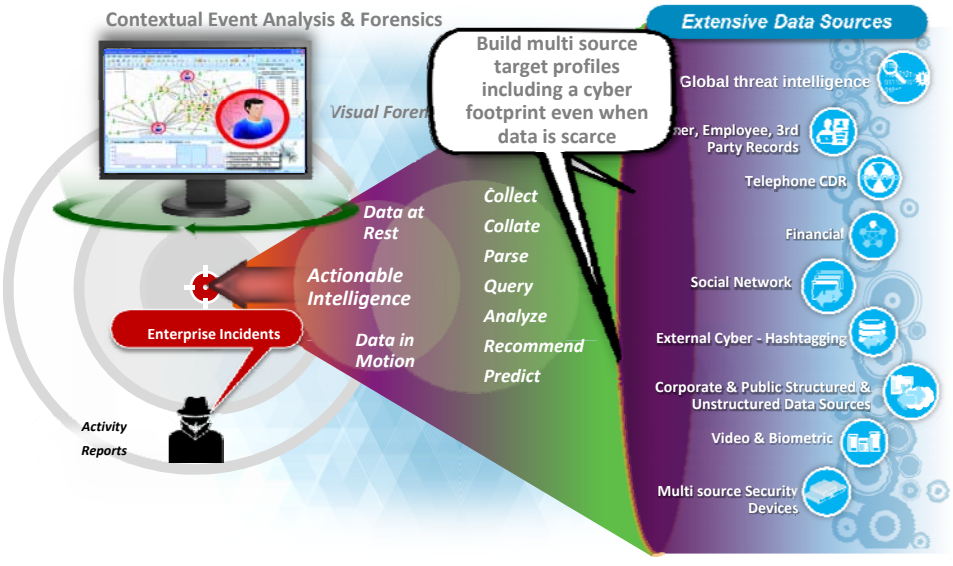
- All-source intelligence
- Anomaly discovery
- Ecosystem visibility
- Scales to 150TBs of data
- Customized configuration

Human-Led Intelligence Discovery

- Visualize linked data
- Identity and relationship resolution
- Geospatial and physical data analysis
- Persona domain threat identification
- Create decision-making products for leaders

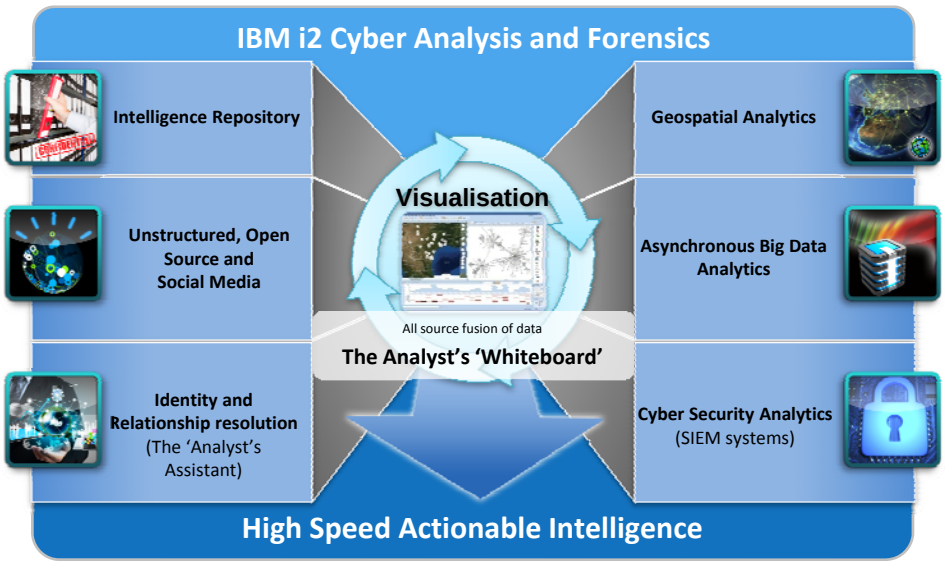
1

IBM i2 brings the Cyber and Intelligence domains together

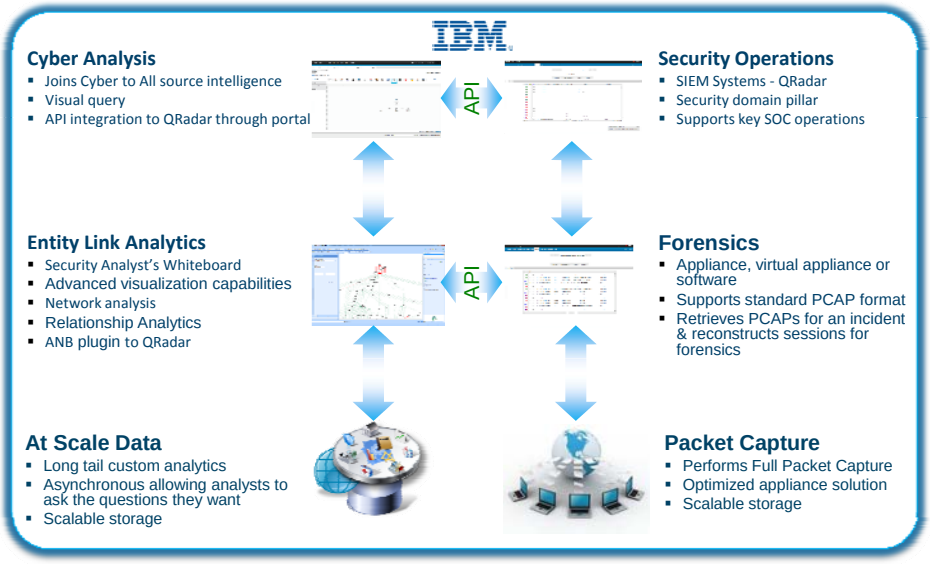


1

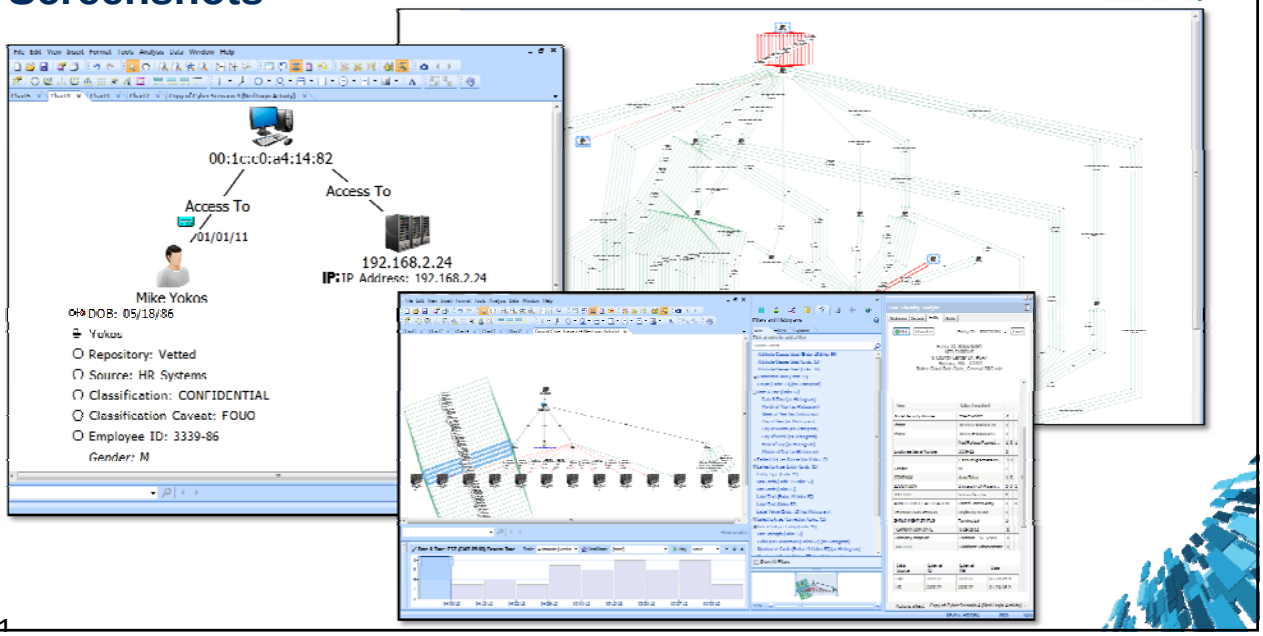
Solution Overview



IBM i2 Cyber Incident Forensics Deployment Model



Screenshots



1

Disclaimer slide

1


IBM
IBM i2 Summit for a Safer Planet
Network. Explore. Learn.
August 12-13, 2015 Hyatt Canberra
Thank You