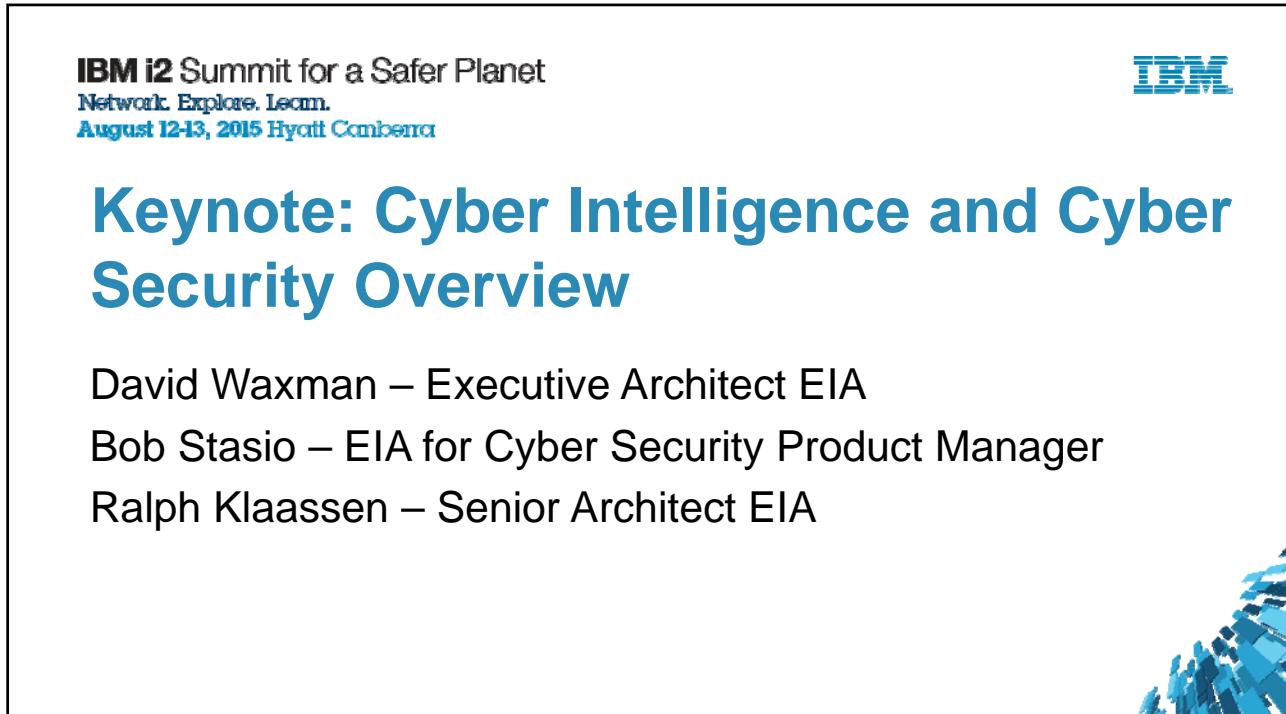




The banner features the IBM logo in blue at the top left. To its right is a large, abstract graphic composed of numerous overlapping blue rectangles of varying shades, creating a sense of depth and motion. Below the graphic, the text "IBM i2 Summit for a Safer Planet" is displayed in a bold, black, sans-serif font. Underneath this, the tagline "Network. Explore. Learn." appears in a smaller, gray font. At the bottom, the event details "August 12-13, 2015" and "Hyatt Canberra" are shown in blue.



The slide banner is identical to the one above it, featuring the IBM logo, the "IBM i2 Summit for a Safer Planet" title, the tagline "Network. Explore. Learn.", the date "August 12-13, 2015", and the location "Hyatt Canberra".

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.

2

The growth of asymmetric threats is changing the landscape

Information security has become a human vs. human problem

The Register
Biting the hand that feeds IT

'Bogus IT guys' slurp £1.3m
Cybercops cuff 8 blokes

'Engineer' slipped remote-hack hardware INSIDE branch, says Met

Remote control device

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

A male posing as an IT technician deployed a \$30USD remote control device on a bank branch office computer

The crooks connected to the device from a nearby hotel, then accessed the bank's servers

The hackers logged into a bank terminal and shifted ~\$2.1M USD through 128 transfers into mule accounts

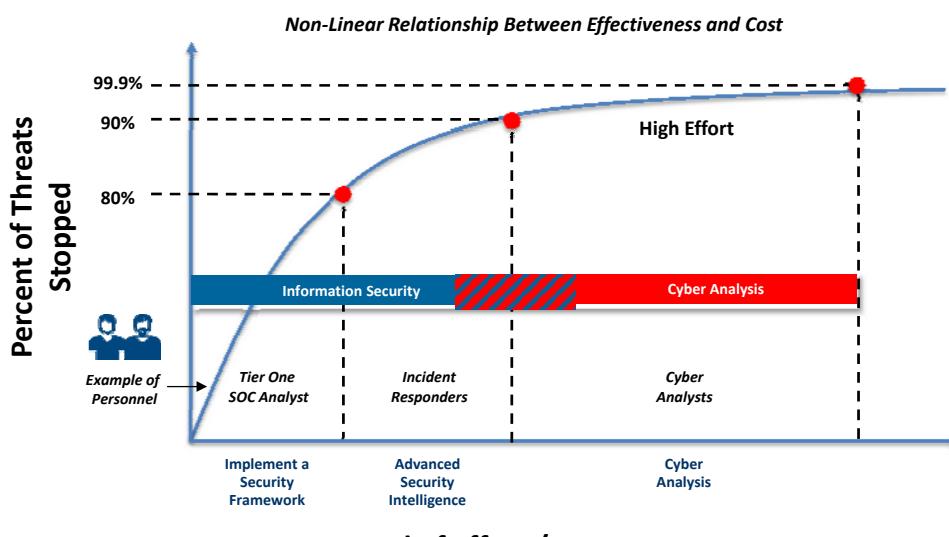
The gang responsible for the theft was caught 13 months later only due to attempting the same attack at another bank

4

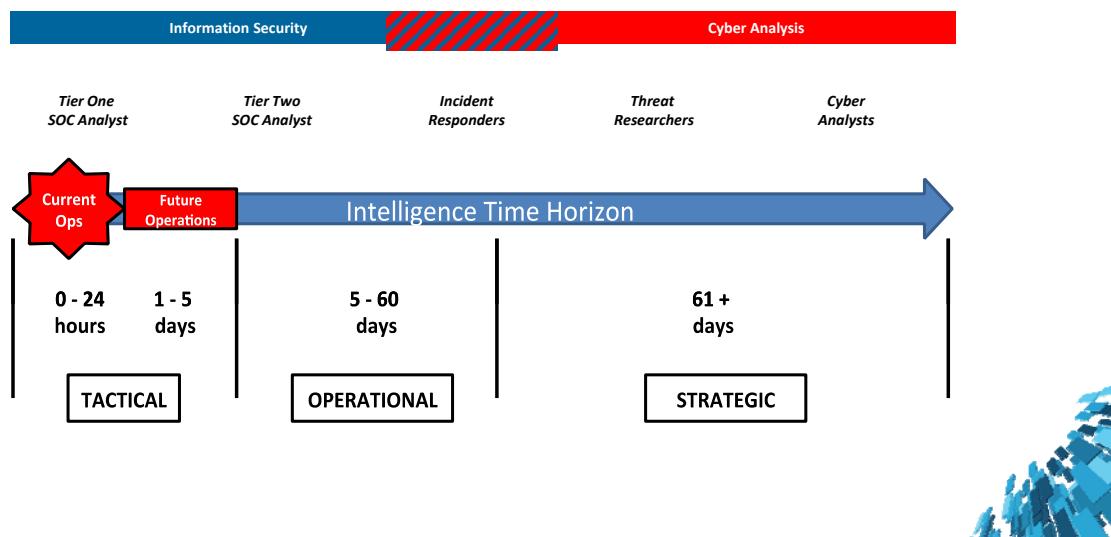
Today's attackers are sophisticated and relentless



Both security and analysis must address the problem



Intelligence as a Time Horizon



7

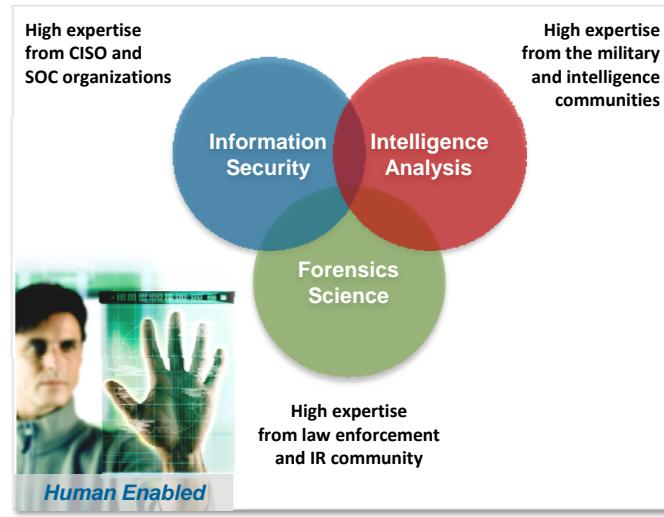
Learning from medical analogies



	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

o

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

Cyber Analysis



Mostly IT Sources	
PCAP Alerts	SIEM
System Logs	SSO/AD
Vulnerability Scans	
Mostly Human Sources	
Behavioral Data	Account Creation
HR Data	Badge Logs
Reviews	Access Logs



Mostly External Sources

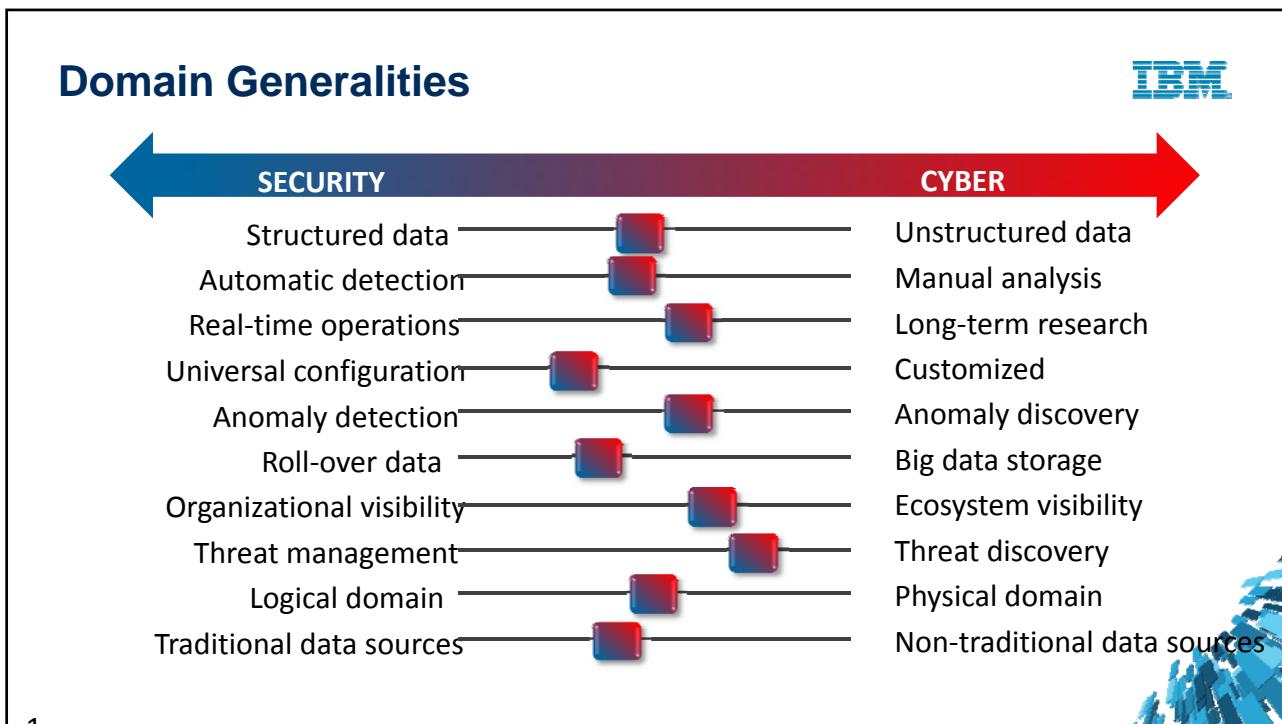
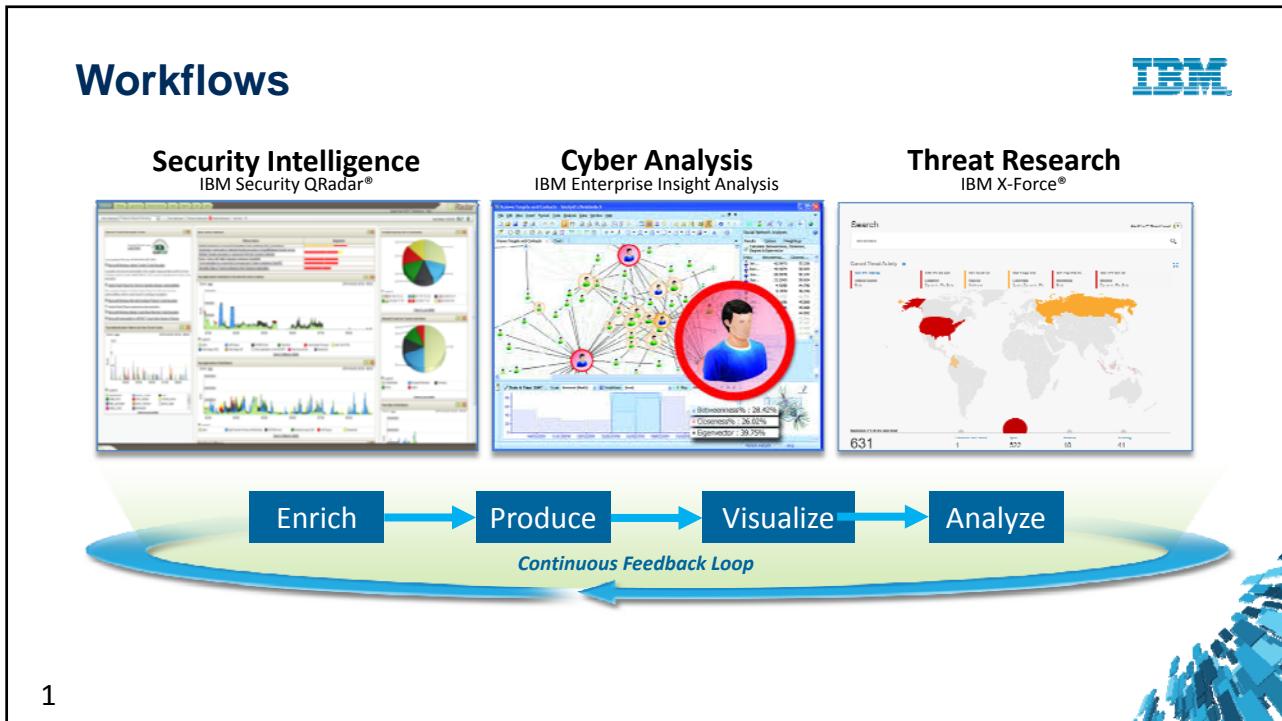
Hacker Forums	Social Media
Intel Vendors	Government Alerts
Threat Indicators	Community Info



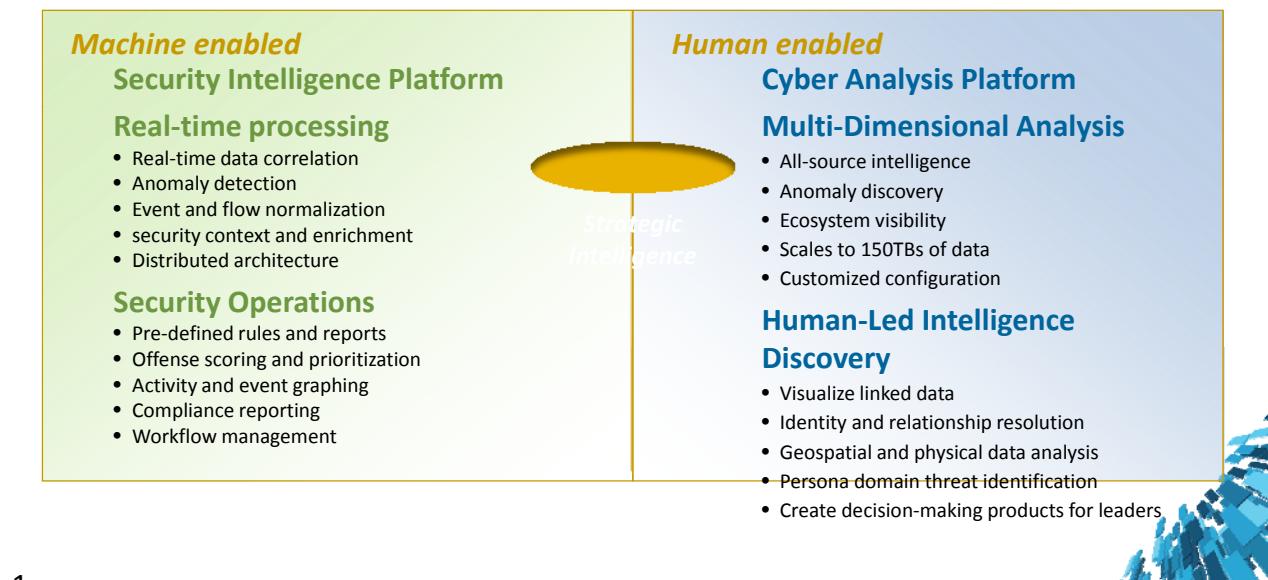
Cyber Analysis Results

- 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

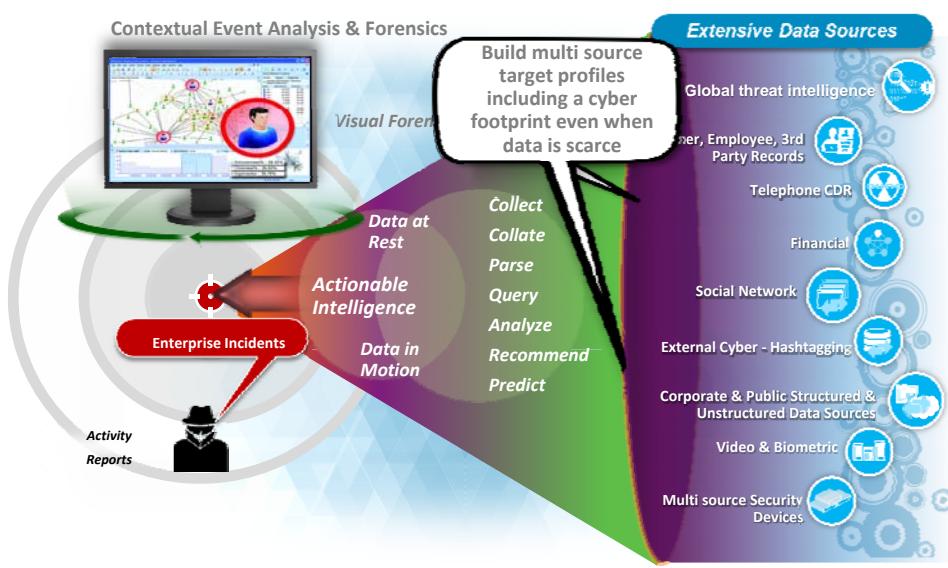


IBM's Strategic Threat Analysis Capability



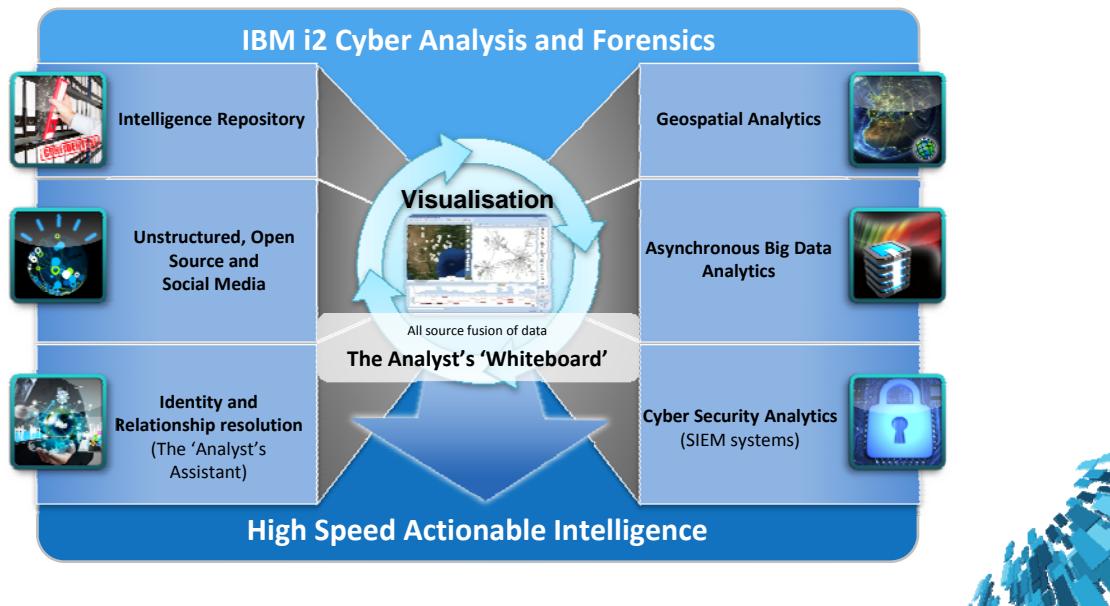
1

IBM i2 brings the Cyber and Intelligence domains together



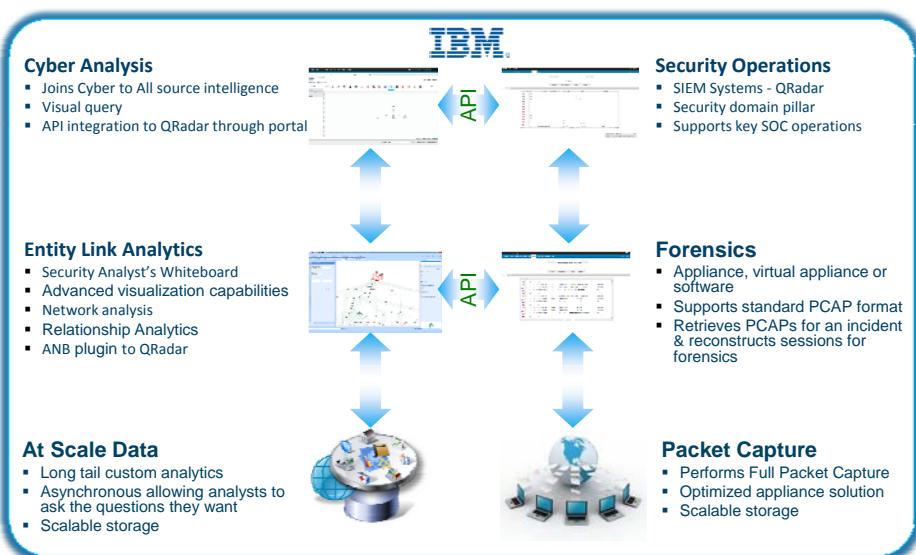
1

Solution Overview



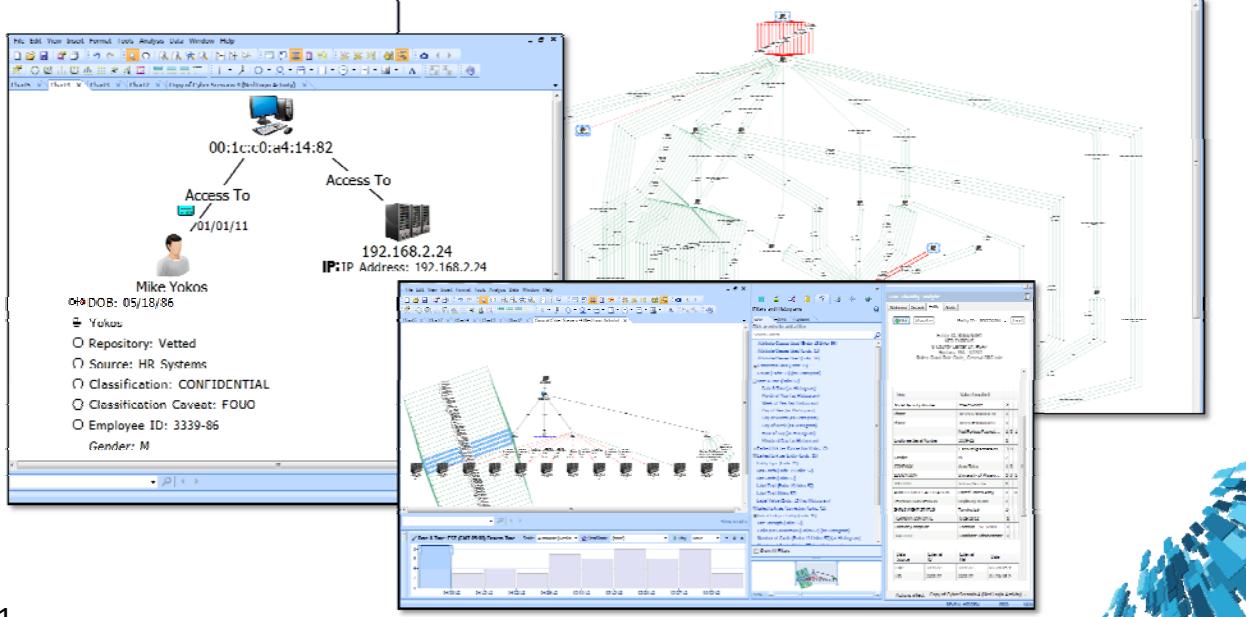
1

IBM i2 Cyber Incident Forensics Deployment Model



1

Screenshots



1

Disclaimer slide



Copyright © 2015 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice. Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, DOORS®, Enterprise Document Management System™, Global Business Services ®, Global Technology Services®, Maximo®, MQIntegrator®, MQSeries®, Netcool®, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Tivoli®, Trusteer®, urban(code)®, WebSphere®, Worklight®, X-Force® and System z® are trademarks of International Business Machines Corporation, 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 "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml

1

