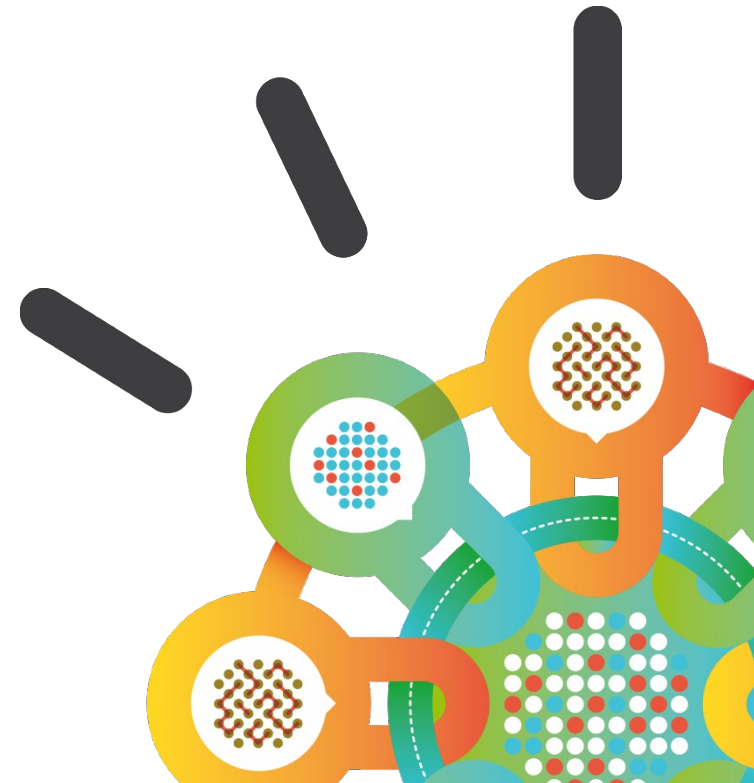


Security Intelligence.
Think Integrated.

Attain Clarity of Your Security Posture with Enhanced Incident Forensics Capabilities

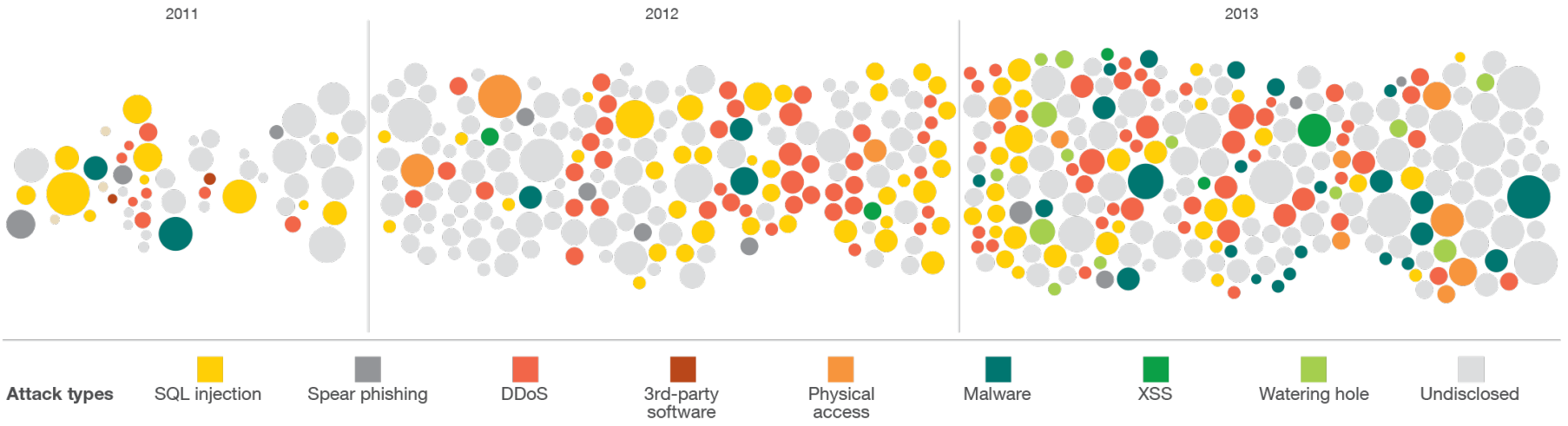
April 2014



Reported attacks continue to increase

A historical look at security incidents by attack type, time and impact, 2011 to 2013

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



500,000,000+ Billion records
of personally identifiable information (PII) were leaked in 2013

Source: IBM X-Force® Research 2013 Trend and Risk Report

Today's challenges

Escalating Attacks

Designer Malware

Spear Phishing

Persistence

Backdoors

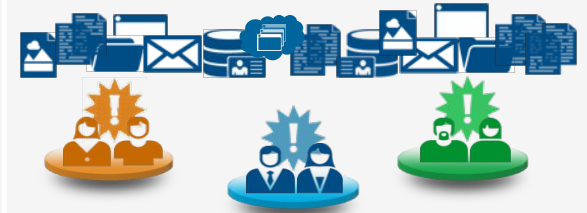
- Increasingly sophisticated attack methods
- Disappearing perimeters
- Accelerating security breaches

Increasing Complexity



- Constantly changing infrastructure
- Too many products from multiple vendors; costly to configure and manage
- Inadequate and ineffective tools

Resource Constraints



ITSecurityJobs.com

Sorry, no applicants found

- Struggling security teams
- Too much data with limited manpower and skills to manage it all
- Managing and monitoring the increasing regulatory compliance demands

Some examples of what a typical enterprise has to deal with



200,000+ face book, twitter, linked-in etc accesses a day



10000+ SPAM/Fishing emails a week



500+ files uploaded to internet sites a day



External network scanned 50 times a day



2,000+ files a day downloaded from the internet



100,000+ vulnerabilities in the network



30% of network use is remote



5 network alerts per minute



2 laptops a week go AWOL



100+ potentially malicious web site visits per day



20 new IT assets a week



20 Network configuration changes a week

A Clear & Present Threat...



- Has our organization been compromised?
- When was our security breached?
- How do we identify the attack?
- What type of attack is it?
- What resources and assets are at risk?
- How to avoid becoming a repeat victim?

When responding to incidents, every second is precious

Critical gaps exist in available threat mitigation offerings to recover from an incident

Difficulty identifying true incidents hidden in mounds of data



Determining where to begin a forensics investigation leads to lost productivity and time-intensive ad-hoc analysis

Inability to quickly retrace and analyze incidents without starting over



Lack of an integrated “security camera” leaves critical gaps in quickly understanding key elements of the attack

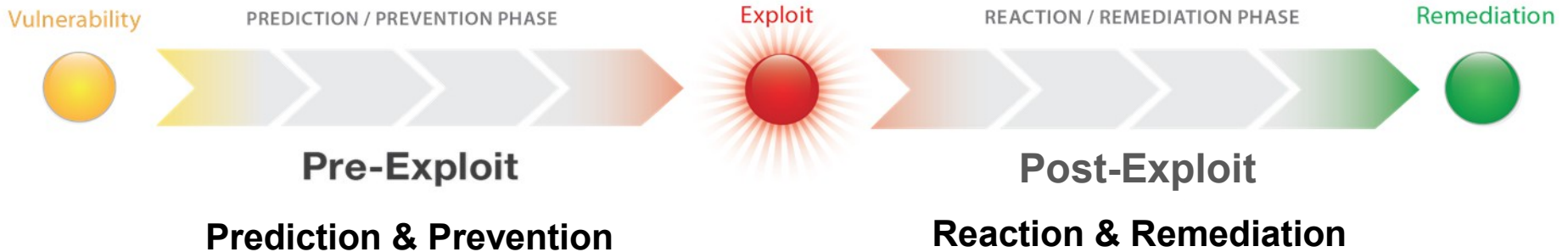
Dependency on specialized skills to conduct detailed investigations



Technically skilled analysts required to drive network forensics security investigations

Security teams must reduce the time to detect and respond to threats.
Confusion and wasted time aid the attacker.

The Lifecycle of a Cyber Threat



Gain Visibility Over the Organization's Security Posture

Detect Deviations from the Norm and Initiate Preventive Procedures

Attain Awareness of Vulnerabilities and Assess Exposures

Discover Anomalies and Investigate to Evaluate the Risk

Explore and Analyze Data to Devise Countermeasures for the Attack

Formulate New Security Best Practices to Adapt to Emerging Threats



Embedded intelligence offers automated offense identification

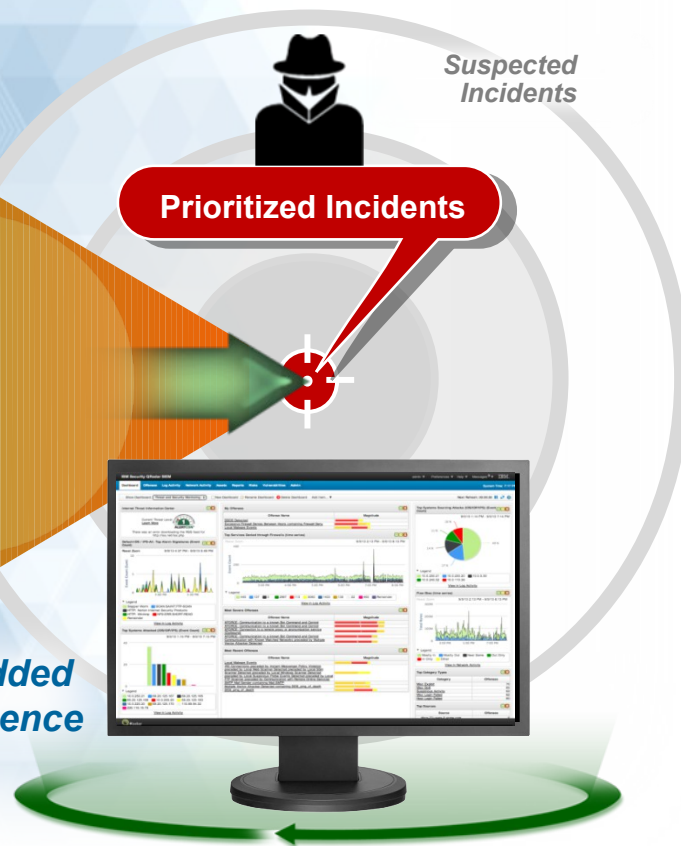
Extensive Data Sources

- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Application activity
- Configuration information
- Vulnerabilities and threats
- Users and identities
- Global threat intelligence

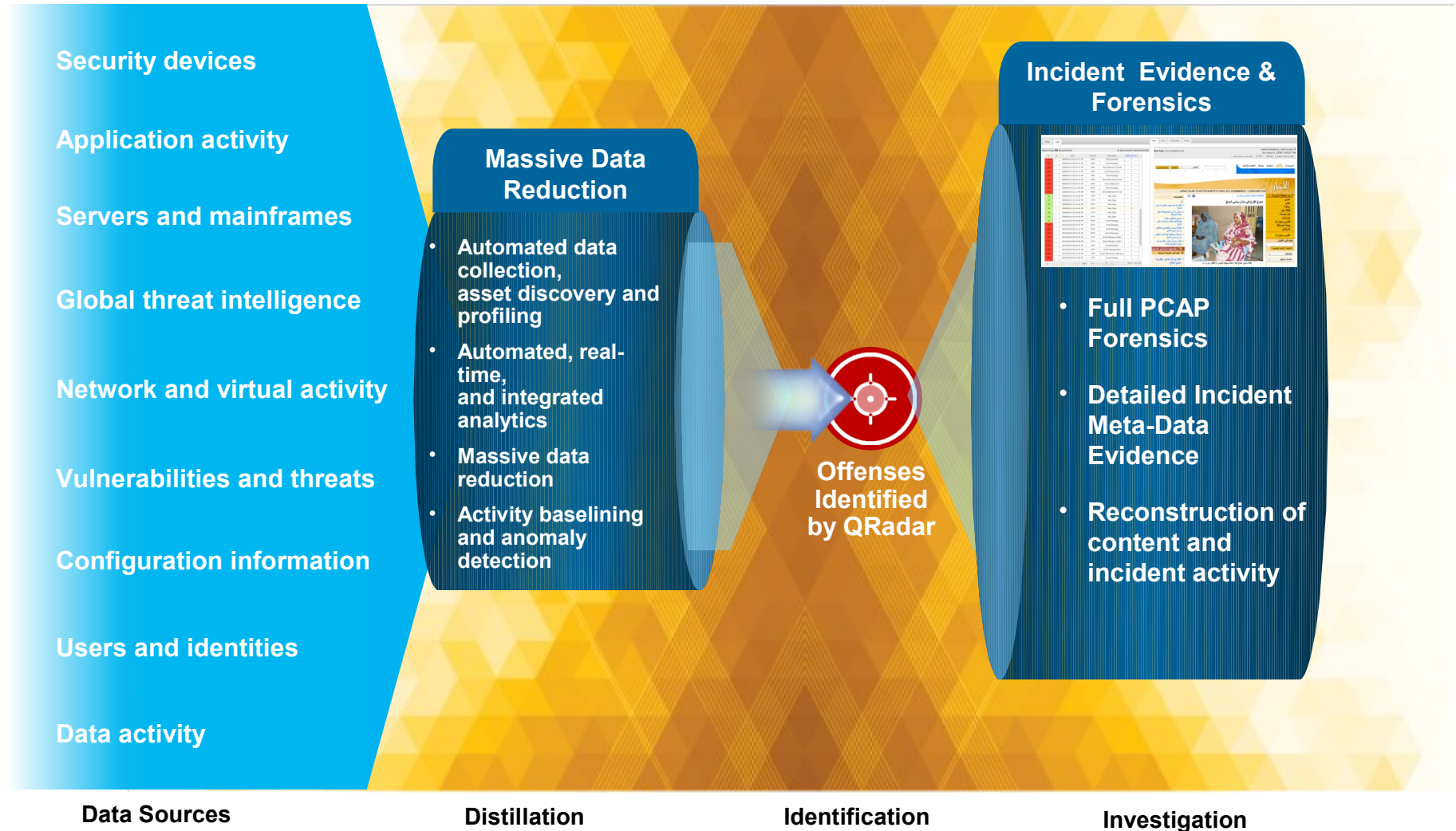
Automated Offense Identification

- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box

Embedded Intelligence



Extending the embedded intelligence of QRadar to deliver high clarity around incident investigations



Why IBM Security QRadar Incident Forensics?

1

Extension of QRadar Security Intelligence Platform

- Built off high accuracy QRadar offense discovery
- Improve efficiency of investigations

2

Expands Data Available for Incident Forensics

- Data-in-motion and data-at-rest
- Structured and unstructured data

3

Has Scalable Search Infrastructure

- Index all the data
- Correlate all the data
- Prioritize search performance

4

Builds Intelligence

- Automated detection and assembly of identities
- Automated detection of suspicious content/activity
- Content categorization informs data exclusion
- Reveals linkages between entities

5

Enables Intuitive Investigative Analysis

- Simple search engine interface
- Visual analytics
- Retrace activity in chronological order with reconstructed content

Answering questions to help prevent and remediate attacks

Offense 909 Summary Display Events Connections Flows View Attack Path Actions Print

Magnitude	<div style="width: 75%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>	Status		Relevance	8	Severity	5	Credibility	4
Description	Potential Data Loss	Offense Type	Source IP						
		Event/Flow count	111 events and 1,042 flows in 13 categories						
Source IP(s)	10.0.110.221 (dhcp-221-users-2.acme.com)	Start	Oct 18, 2013 12:28:02 PM						
Destination IP(s)	Local (2) Remote (376)	Duration	4d 10h 42m 57s						
Network(s)	Multiple (3)	Assigned to	admin						

Offense Source Summary

IP	10.0.110.221	Location	Users.Users-2
Magnitude	<div style="width: 80%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	Vulnerabilities	
Username	compliance	MAC Addresses	
Host Name	dhcp-221-users-2.acme.com	Weight	0
Asset Name	dhcp-221-users-2.acme.com	Events/Flows	113/310
Offenses	8		

Last 5 Notes

Notes
Potential data loss detected, forensics case created

Forensics Reconstructions

Case	Collection	IP	Start	End	Status
DataLoss	DataLoss	10.0.110.221	3/27/2014 3:31:00 PM	3/27/2014 4:31:00 PM	SUCCESS

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow
dhc...	<div style="width: 80%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>	Users.Users-2	No	compliance	00:0E:0C:B4:D8:EE	0	8	21	0s

- What was the attack?
- Is it credible?
- Who was responsible?
- Where do I find them?
- What was stolen?
- How many targets involved?
- How valuable are the targets to the business?
- Are any of them vulnerable?
- Where is all the evidence?

Incident Forensics tell you what happened

Offense 909 Summary Display Events Connections Flows View Attack Path Actions Print

Magnitude	<div style="width: 100%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>	Status		Relevance	8	Severity	5	Credibility	4
Description	Potential Data Loss	Offense Type	Source IP						
Source IP(s)	10.0.110.221 (dhcp-221-users-2.acme.com)	EventFlow count	111 events and 1,042 flows in 13 categories						
Destination IP(s)	Local (2) Remote (376)	Start	Oct 18, 2013 12:28:02 PM						
Network(s)	Multiple (3)	Duration	4d 10h 42m 57s						
Offense Source		Assigned to	admin						

Filter List

IP

Magnitude

Username

Host Name

Asset Name

Offenses

Last 5 Note

Potential data

Forensics

DataLoss

Top 5 Source

Source IP

dhc...

Text Attributes Notes

Searching **60** documents. 1 documents bookmarked (www.iex.nl)

Id	Date	Protocol	Description	Relevancy (1)
32	2008/04/24 09:24:14 PM	IMAP	Email Message	1
33	2008/04/24 09:24:14 PM	IMAP	Email Message	1
34	2008/04/24 09:24:14 PM	IMAP	Email Alternate Format	1
35	2008/04/24 09:24:14 PM	IMAP	Email Attachment	1
36	2008/04/24 09:24:14 PM	IMAP	Email Message	1
37	2008/04/24 09:24:14 PM	IMAP	Email Alternate Format	1
38	2008/04/24 09:24:14 PM	IMAP	Email Attachment	1
39	2008/04/25 12:11:49 AM	POP3	Email Message	1
40	2008/04/25 12:11:49 AM	POP3	Email Alternate Format	1
41	2008/05/01 10:43:18 PM	HTTP	Web Page	1
42	2008/05/01 10:43:18 PM	HTTP	Web Page	1
43	2008/05/01 10:43:18 PM	HTTP	Web Page	1
44	2008/05/01 10:43:31 PM	HTTP	Web Page	1
45	2008/05/01 10:43:32 PM	HTTP	Web Page	1
46	2008/05/01 10:44:15 PM	HTTP	Web Page	1
47	2010/01/26 05:04:06 PM	POP3	Email Message	1
48	2010/01/26 05:04:07 PM	POP3	Email Message	1
49	2010/01/26 05:11:11 PM	POP3	Email Message	1
50	2010/02/02 09:07:32 PM	SMTP	Email Message	1
51	2010/02/02 09:10:00 PM	HTTP	Email Message Header	1
52	2010/02/02 09:10:00 PM	HTTP	Email Message Header	1
53	2010/02/02 09:10:04 PM	HTTP	Email Message	1
54	2010/02/02 09:10:04 PM	HTTP	Email Message Body	1
55	2010/02/02 09:10:04 PM	HTTP	Email Attachment Reference	1
56	2010/02/02 09:10:26 PM	HTTP	Email Message	1

IEX van beleggers voor beleggers

Home Beleggingsfondsen Turbo's Speeders Opties & Futures Productrecensies

10 van Tak: Serieuze zaken

"Geen grappen meer voor mij. Drie nieuwe productrecensies en de AFM komt met een meldpunt..."

Speculeren met gokken

"De internet gokwereld staat weer op z'n kop en ik schuif mijn fiches richting het Britse Sportingbet..."

Nieuws op IEX

IEX Prijzenspel

Real-time koersen

Geldwaardering.nl

Dividend

IEX Universiteit

IEX Beursblog

- "Goud naar \$750 of hoger"
- Broeikas stockpicks
- Royal Bank of Amsterdam
- Auw toverkopen of autoverkopen?
- AF-KLM, BA-Iberia, Alitalia... Aeroflot?
- The ABN Amro Merger Song
- Tak gaat door: drie nieuwe recensies
- Best 150%+ 2013
- Commodity Bull & Bear Note
- High Yield Note op ING III
- India: met een rotganges naar beneden
- IEX in het FD: 1 april!

Nieuws

- 15:29 OR energiebedrijven onthutst over besluit tot splitsing
- 15:08 Wall Street licht lagere opening indices verwacht
- 14:58 Best Buy ziet winst per aandeel 2007/2008 USD 3,10-3,25
- 14:56 Blue Fox noteert 6.3% hoger op technisch herstel
- 14:47 Euronext A'dam: Ahold grootste stijger AEX
- 14:03 Belangrijke advieswijzigingen analisten

Markt vandaag

Euronext A'dam: Ahold gro...

AEX DOW NASD FTSE

517,20

516,80

516,40

516,00

09 10 11 12 13 14 15 16

AEX-inde 517,33 +0

EuroDol 133,52 -0

FRANKF- 7,059,64 +0

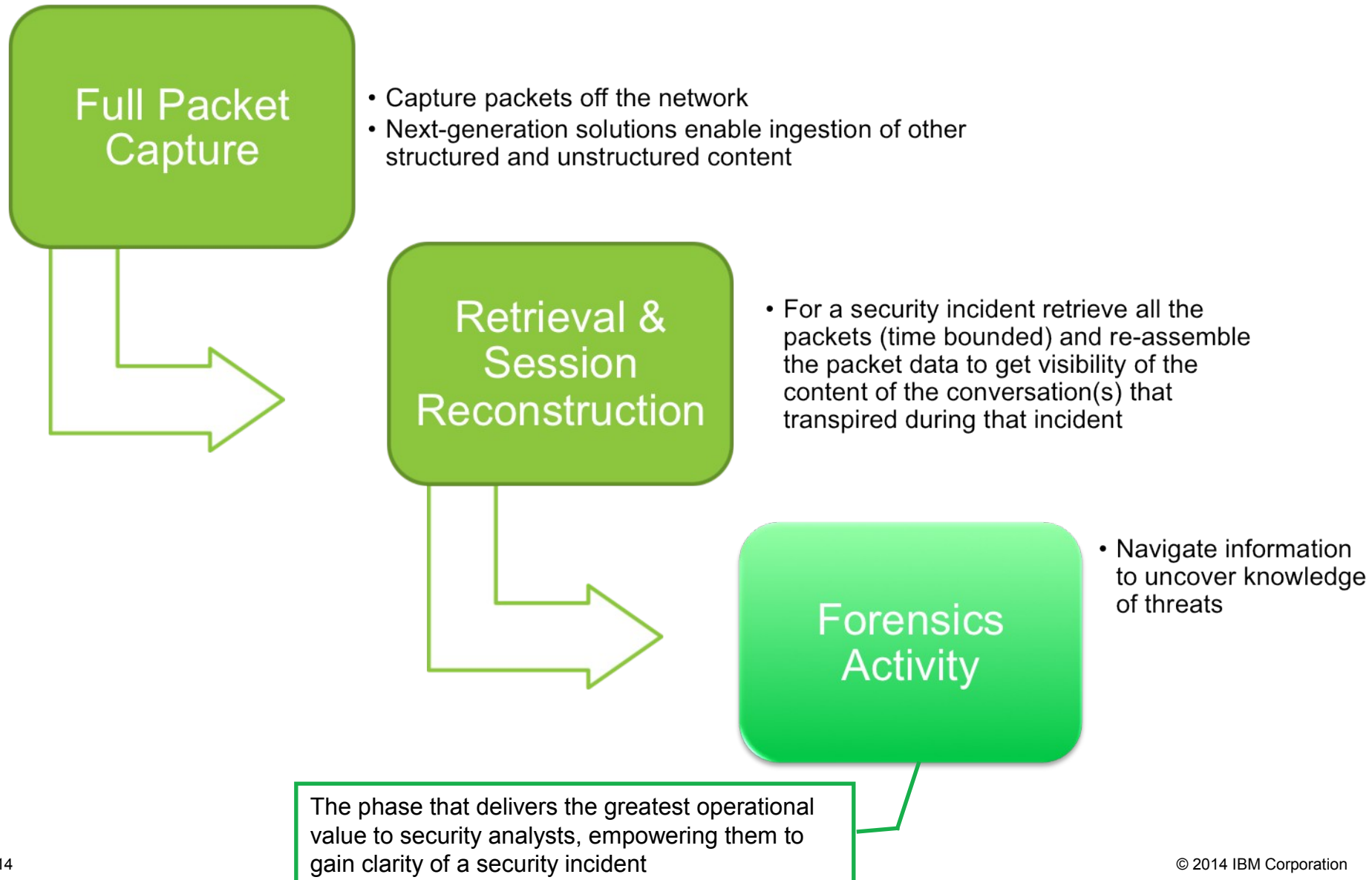
LONDEN-F 6,351,60 -0

NY-DJ-in 12,510,30 0

NY-Nasda 2,450,33 0

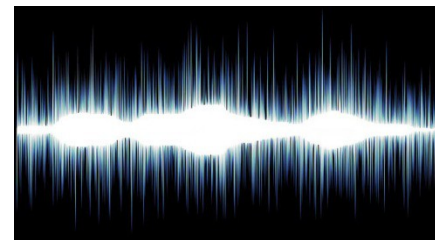
Goud \$t 663,50 0

How Network Forensics is Done...



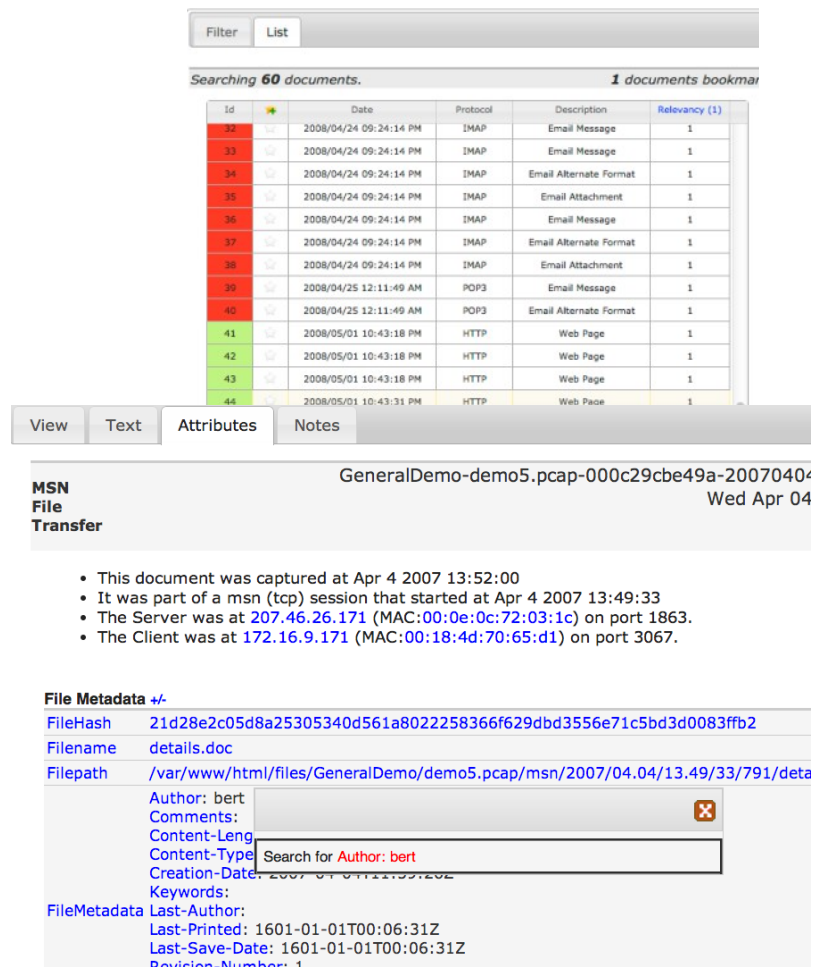
QRadar Incident Forensics delivers *High Fidelity* forensics and comprehensive situational awareness

- Ingests PCAPs, XML files and documents or archives converting and storing everything in rich document format
- Applies search engine technology to highly indexed, file-based store using multiple types of metadata:
 - Network metadata
 - File metadata
 - Identity metadata
- Returns detailed, multi-level search results in seconds



Making forensics fast and clear - Intuitive Data Exploration and Navigation

- Empower security analysts to operate like seasoned forensics specialists by offering capabilities that can be powered by intuition and logical deduction
- **Surveyor:** Retrace the activities in a chronological order
- **Searchable Results:** Quickly pivot on data items to go where the data takes you
- **Visual Analytics:** Navigate the data using visual indications of correlations between data items



Filter List

Searching 60 documents. 1 documents bookmark

Id	Date	Protocol	Description	Relevancy (1)
32	2008/04/24 09:24:14 PM	IMAP	Email Message	1
33	2008/04/24 09:24:14 PM	IMAP	Email Message	1
34	2008/04/24 09:24:14 PM	IMAP	Email Alternate Format	1
35	2008/04/24 09:24:14 PM	IMAP	Email Attachment	1
36	2008/04/24 09:24:14 PM	IMAP	Email Message	1
37	2008/04/24 09:24:14 PM	IMAP	Email Alternate Format	1
38	2008/04/24 09:24:14 PM	IMAP	Email Attachment	1
39	2008/04/25 12:11:49 AM	POP3	Email Message	1
40	2008/04/25 12:11:49 AM	POP3	Email Alternate Format	1
41	2008/05/01 10:43:18 PM	HTTP	Web Page	1
42	2008/05/01 10:43:18 PM	HTTP	Web Page	1
43	2008/05/01 10:43:18 PM	HTTP	Web Page	1
44	2008/05/01 10:43:31 PM	HTTP	Web Page	1

View Text Attributes Notes

MSN File Transfer GeneralDemo-demo5.pcap-000c29cbe49a-20070404 Wed Apr 04

- This document was captured at Apr 4 2007 13:52:00
- It was part of a msn (tcp) session that started at Apr 4 2007 13:49:33
- The Server was at 207.46.26.171 (MAC:00:0e:0c:72:03:1c) on port 1863.
- The Client was at 172.16.9.171 (MAC:00:18:4d:70:65:d1) on port 3067.

File Metadata +/-

FileHash 21d28e2c05d8a25305340d561a8022258366f629dbd3556e71c5bd3d0083ffb2

Filename details.doc

Filepath /var/www/html/files/GeneralDemo/demo5.pcap/msn/2007/04.04/13.49/33/791/deta

Author: bert

Comments:

Content-Leng

Content-Type

Creation-Date: 2007-04-04 13:49:33

Keywords:

FileMetadata Last-Author:

Last-Printed: 1601-01-01T00:06:31Z

Last-Save-Date: 1601-01-01T00:06:31Z

Revision-Number: 1

IBM Security QRadar Incident Forensics deployment model

QRadar Security Intelligence

- Seamlessly integrated, single UI
- New 'Forensics Tab'
- Supports incident investigation workflow



QRadar Incident Forensics

- Scalable storage
- Appliance, virtual appliance or software
- Integrates with standard PCAP formats



QRadar Packet Capture

- Up to 10Gb/s
- 2U, 20 Core, 128GB ram
- Scalable storage options
 - 40TB -> 90 TB -> 100'sTB
 - 1 day -> Week's-> Month's
- 1 to N Appliances



Next generation network forensics: know what happened, fast

Our Security Intelligence platform delivers powerful capabilities to limited IT security resources



Introducing QRadar Incident Forensics:

Leveraging the strengths of QRadar to optimize the process of investigating and gathering evidence on advanced attacks and data breaches

Tells you exactly when an incident occurred

- Integrated with QRadar SIEM, leveraging the accuracy of built-in security analytics to discover true offenses
- Applies search engine technology to a highly-indexed, file-based store using multiple types of metadata
- Returns detailed, multi-level search results in seconds

Allows you to quickly Retrace full incident activity

- Full packet capture for complete session reconstruction
- Unified view of all flow, user, event, and forensic information
- Retrace activity in chronological order with reconstructed content

Provides assistance with navigating investigations

- Visually construct threat actor relationships - helping answer what the entity is, and with whom and how it communicates
- Builds detailed user and application profiles helping discover extended relationships across multiple IDs

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security



© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials 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 these materials 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 these materials 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. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.