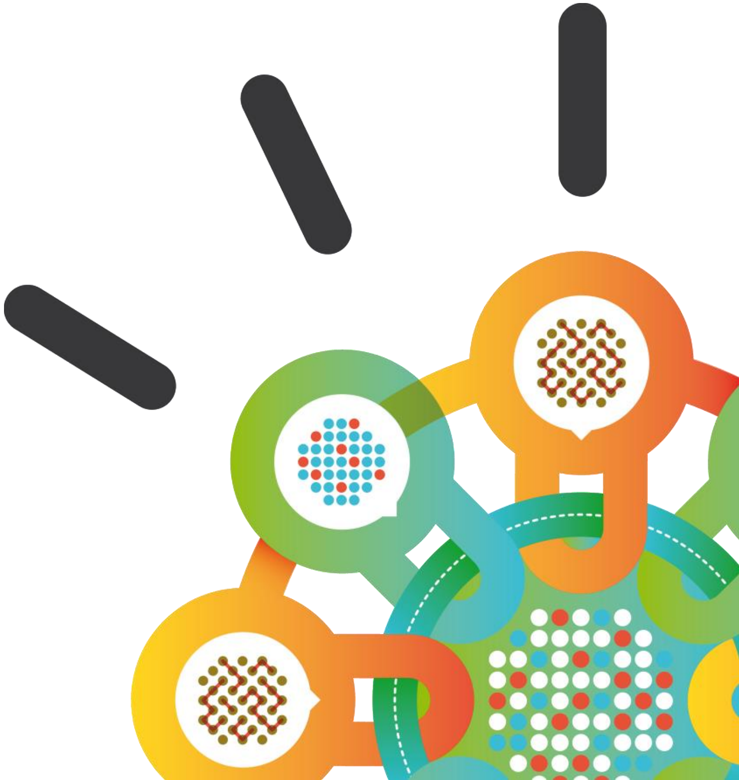
Security Intelligence.
Think Integrated.

Attain Clarity of your Security Posture with new IBM Security QRadar Incident Forensics

Jay Bretzmann
Product Marketing

October, 2014



QRadar Incident Forensics – Hands-on Workshop

- QRadar Overview – 10min
- Instructor Tutorial – 20min
- Search Case #1 – 30min
- Search Case #2 – 30min
- Wrap-up

Traditional customer challenges employing network forensics

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

Difficulty identifying true incidents hidden in mounds of data

Dependency on specialized skills to conduct detailed investigations

Disparate tools with limited intelligence inhibit productivity and efficacy in analysing incidents

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

Ponemon Institute LLC Research Findings

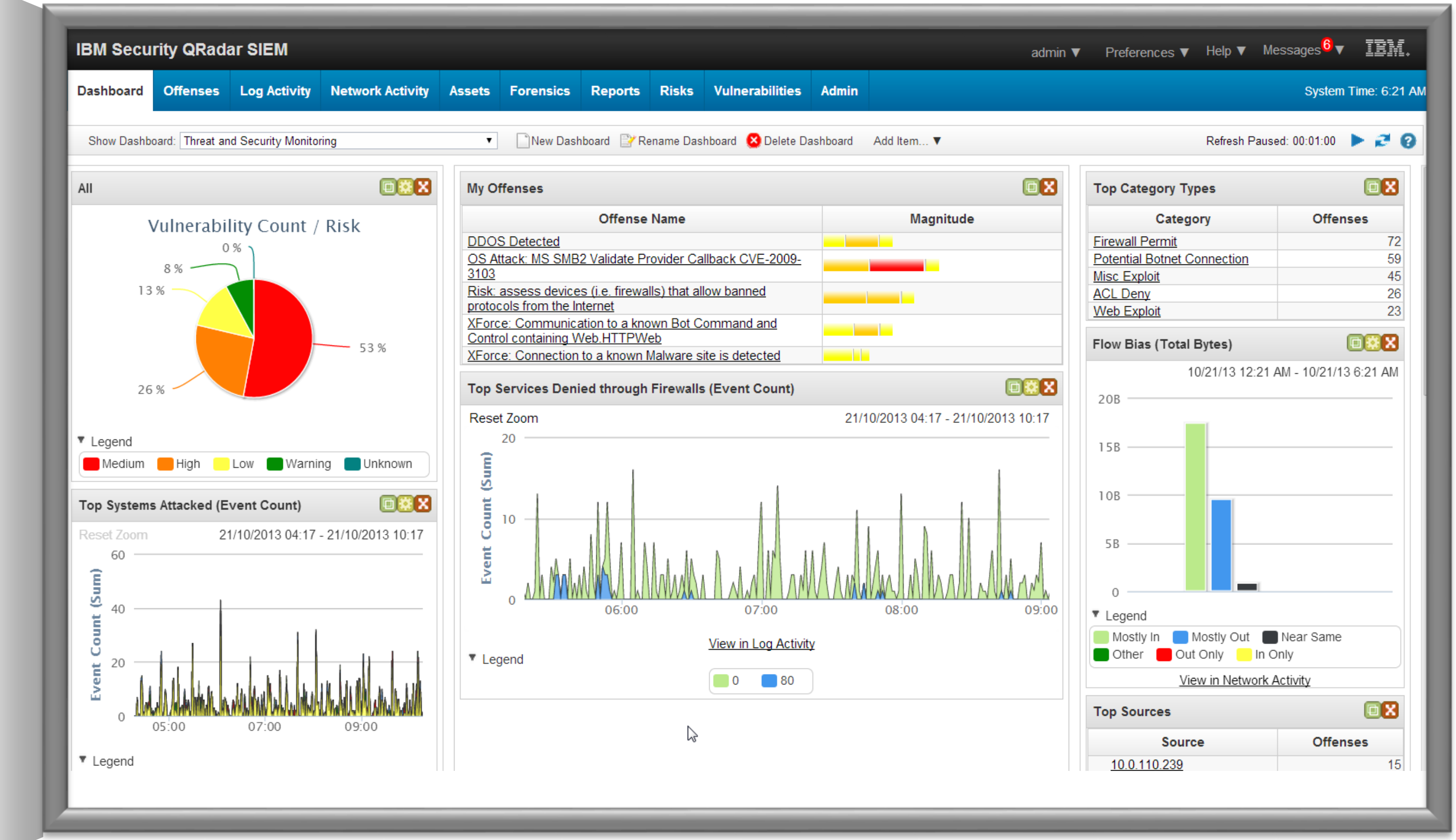
Network forensics industry benchmarks

Average time required to complete one investigation regarding a suspected security breach?	• 58.7 hours
Average time required to complete one forensic investigation from detection to containment for a security breach?	• 6.8 days
Percentage of organizations using a particular member of the IT security team for investigations?	• 71%
Percent of forensic investigators/analysts employed with advanced degrees?	• 56%

IBM QRadar Security Intelligence Platform

An integrated, unified architecture in single web-based console

- Log Management
- Security Intelligence
- Network Activity Monitoring
- Risk Management
- Vulnerability Management
- Network Forensics



My Offenses

Offense Name	Magnitude
DDOS Detected	
OS Attack: MS SMB2 Validate Provider Callback CVE-2009-3103	
Risk: assess devices (i.e. firewalls) that allow banned protocols from the Internet	
XForce: Communication to a known Bot Command and Control containing Web HTTPWeb	
XForce: Connection to a known Malware site is detected	

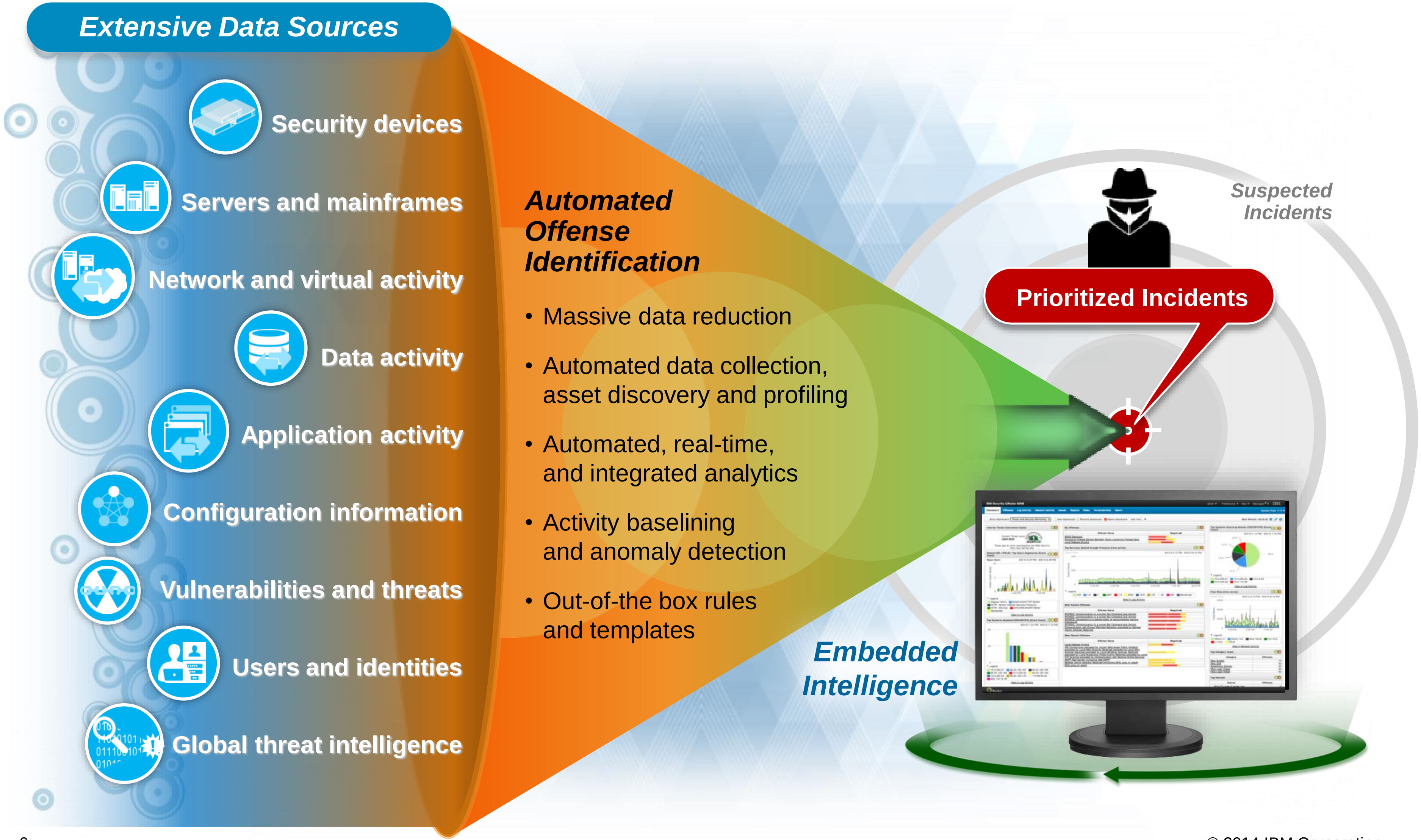
Top Category Types

Category	Offenses
Firewall Permit	72
Potential Botnet Connection	59
Misc Exploit	45
ACL Deny	26
Web Exploit	23

Top Sources

Source	Offenses
10.0.110.239	15

Big Data approach to automated offense identification



Extensive Data Sources

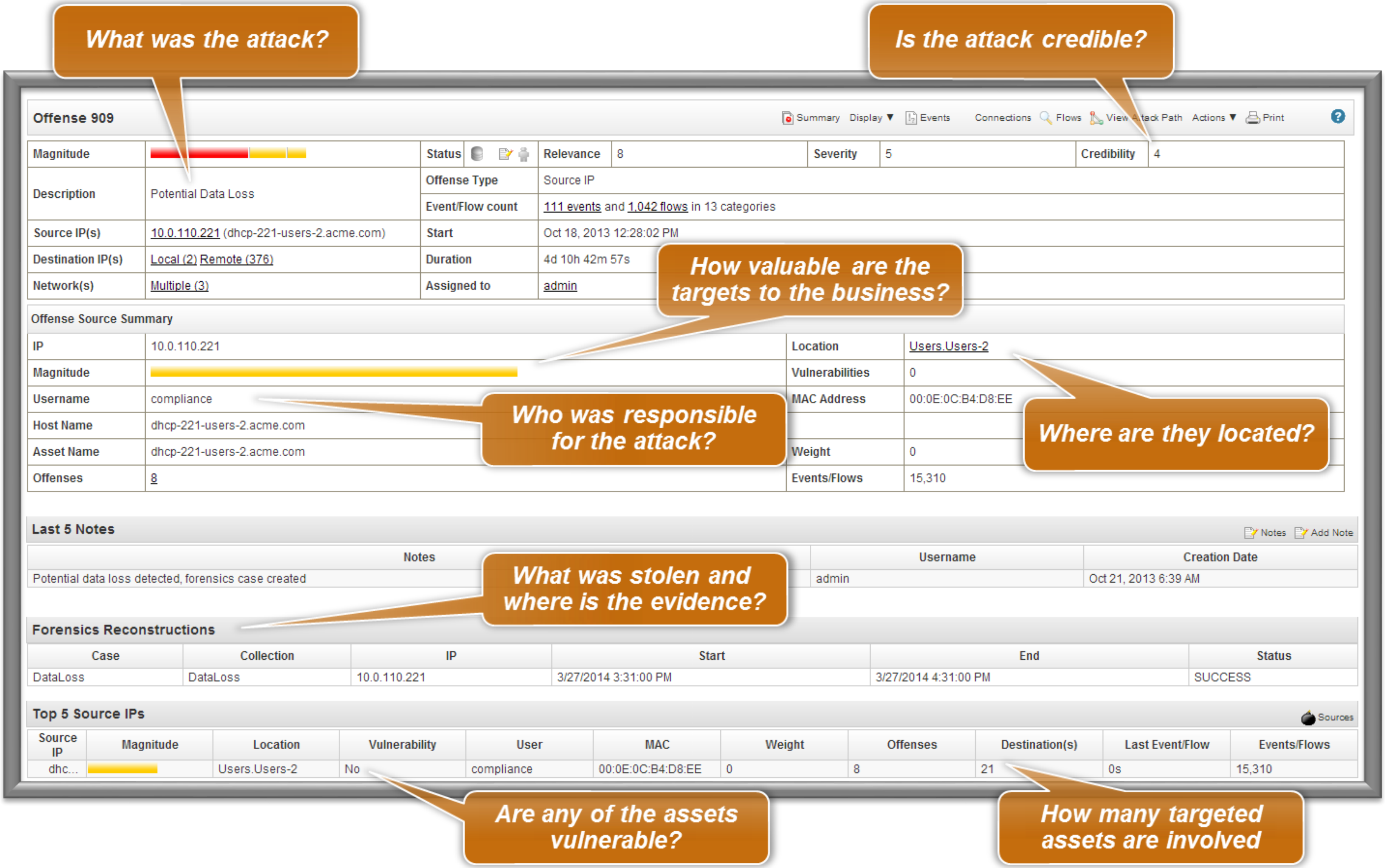
- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Application activity
- Configuration information
- Vulnerabilities and threats
- Users and identities
- Global threat intelligence

Automated Offense Identification

- Massive data reduction
- Automated data collection, asset discovery and profiling
- Automated, real-time, and integrated analytics
- Activity baselining and anomaly detection
- Out-of-the box rules and templates

Embedded Intelligence

Answering questions to help prevent and remediate attacks



What was the attack?
Is the attack credible?
How valuable are the targets to the business?
Who was responsible for the attack?
Where are they located?
What was stolen and where is the evidence?
Are any of the assets vulnerable?
How many targeted assets are involved

Offense 909

Summary
Display ▼
Events
Connections
Flows
View Attack Path
Actions ▼
Print

Magnitude	🟥🟨	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	🟨	Vulnerabilities	0
Username	compliance	MAC Address	00:0E:0C:B4:D8:EE
Host Name	dhcp-221-users-2.acme.com		
Asset Name	dhcp-221-users-2.acme.com	Weight	0
Offenses	8	Events/Flows	15,310

Last 5 Notes

Notes	Username	Creation Date
Potential data loss detected, forensics case created	admin	Oct 21, 2013 6:39 AM

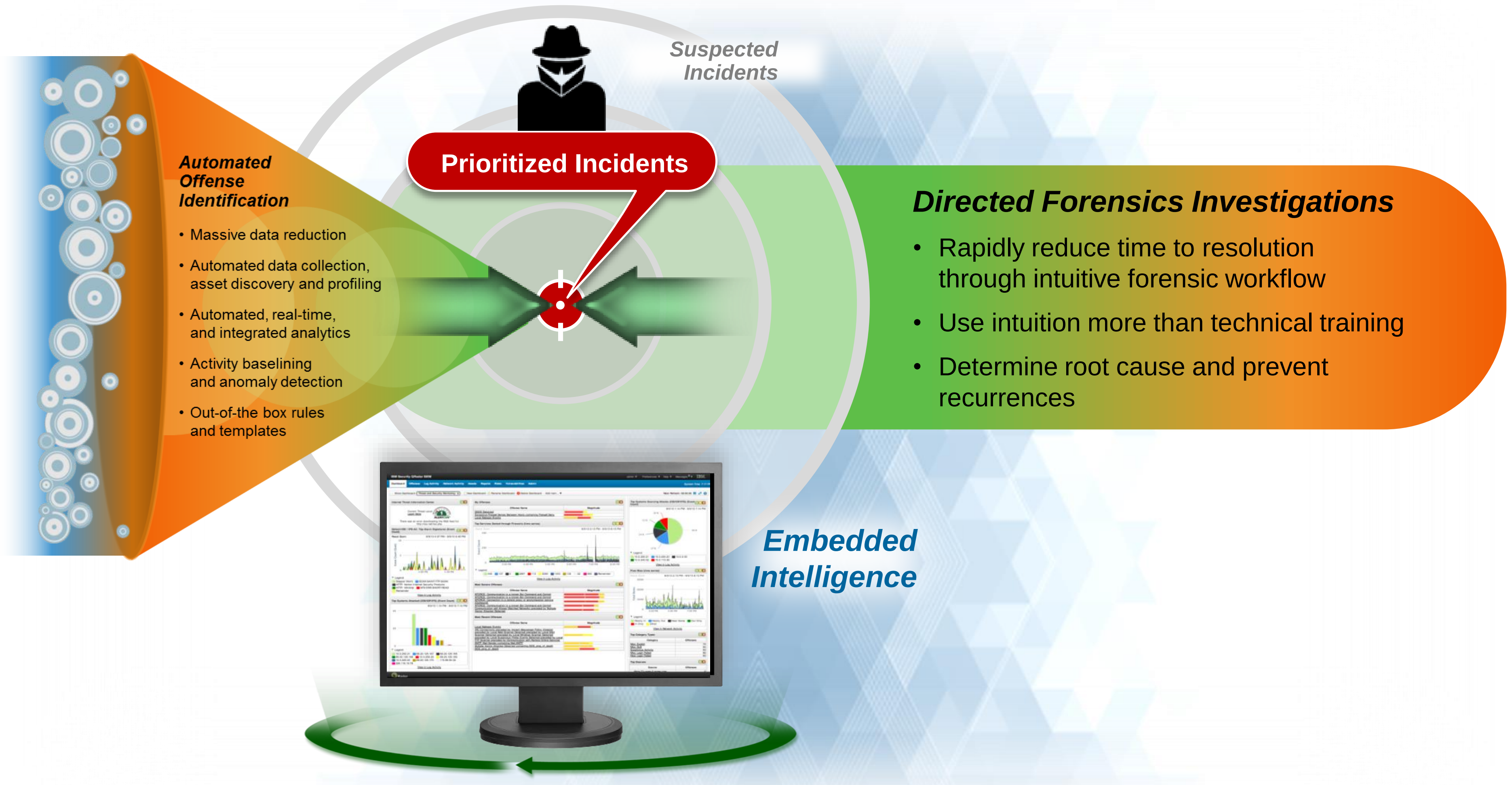
Forensics Reconstructions

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	Events/Flows
dhc...	🟨	Users.Users-2	No	compliance	00:0E:0C:B4:D8:EE	0	8	21	0s	15,310

Extend clarity around incidents with in-depth forensics data



Suspected Incidents

Prioritized Incidents

Automated Offense Identification

- Massive data reduction
- Automated data collection, asset discovery and profiling
- Automated, real-time, and integrated analytics
- Activity baselining and anomaly detection
- Out-of-the box rules and templates

Directed Forensics Investigations

- Rapidly reduce time to resolution through intuitive forensic workflow
- Use intuition more than technical training
- Determine root cause and prevent recurrences

Embedded Intelligence

IBM Security QRadar Incident Forensics

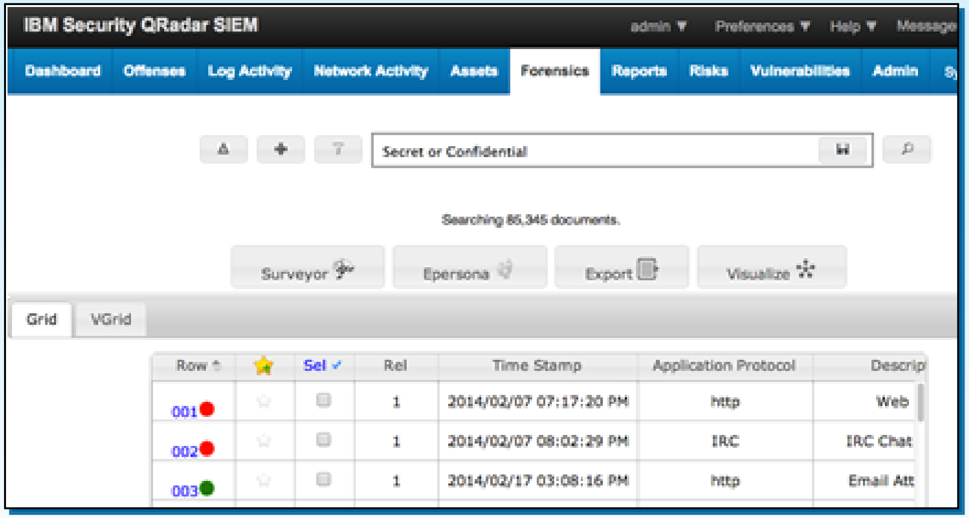
Intuitive investigation of security incidents

QRadar® Incident Forensics

Drastic reduction of investigation time

Evidence gathering against malicious entities

Root cause identification of successful breaches



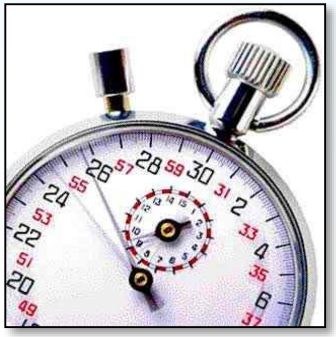
Secret or Confidential

Searching 86,345 documents.

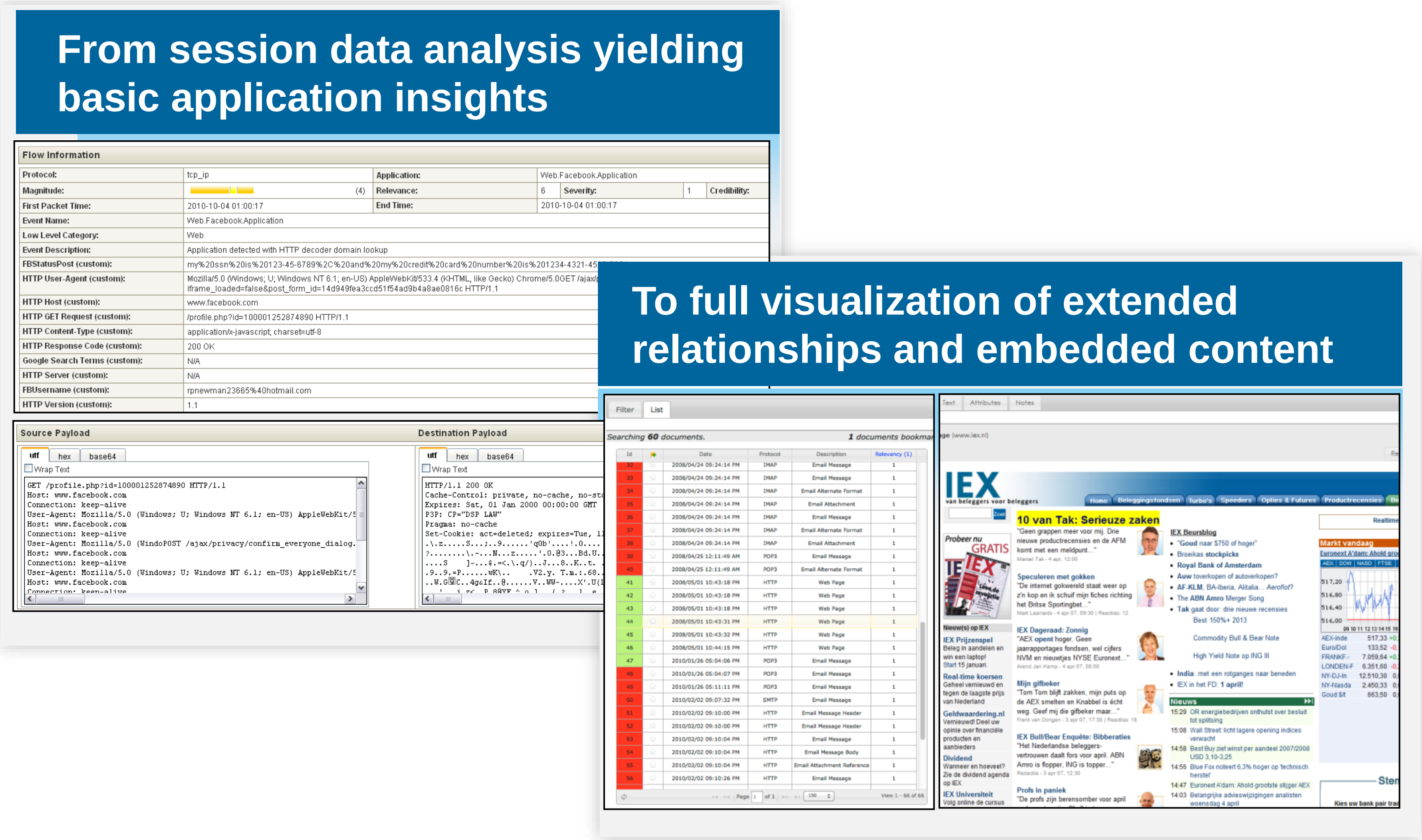
Row	★	Sel ✓	Rel	Time Stamp	Application Protocol	Descrip
001 ●	☆	□	1	2014/02/07 07:17:20 PM	http	Web
002 ●	☆	□	1	2014/02/07 08:02:29 PM	IRC	IRC Chat
003 ●	☆	□	1	2014/02/17 03:08:16 PM	http	Email Att

> *"Research findings indicate enterprise organizations want increased awareness of advanced threats without the need for additional resources and forensics expertise."*
>
> **Jon Oltsik, Enterprise Systems Group (ESG)**

Win the race against time



Better clarity into network activity



From session data analysis yielding basic application insights

Flow Information

Protocol:	tcp_ip	Application:	Web.Facebook.Application				
Magnitude:	(4)	Relevance:	6	Severity:	1	Credibility:	
First Packet Time:	2010-10-04 01:00:17	End Time:	2010-10-04 01:00:17				
Event Name:	Web.Facebook.Application						
Low Level Category:	Web						
Event Description:	Application detected with HTTP decoder domain lookup						
FBStatusPost (custom):	my%20ssn%20is%20123-45-6789%2C%20and%20my%20credit%20card%20number%20is%201234-4321-45						
HTTP User-Agent (custom):	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0GET /ajax/p iframe_loaded=false&post_form_id=14d949fea3ccd51f54ad9b4a8ae0816c HTTP/1.1						
HTTP Host (custom):	www.facebook.com						
HTTP GET Request (custom):	/profile.php?id=100001252874890 HTTP/1.1						
HTTP Content-Type (custom):	application/x-javascript; charset=utf-8						
HTTP Response Code (custom):	200 OK						
Google Search Terms (custom):	N/A						
HTTP Server (custom):	N/A						
FBUsername (custom):	rpnewman23665%40hotmail.com						
HTTP Version (custom):	1.1						

Source Payload

utf | hex | base64

☐ Wrap Text

```
GET /profile.php?id=100001252874890 HTTP/1.1
Host: www.facebook.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/5
Host: www.facebook.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (WindoPOST /ajax/privacy/confirm_everyone_dialog.
Host: www.facebook.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/5
Host: www.facebook.com
Connection: keep-alive
```

Destination Payload

utf | hex | base64

☐ Wrap Text

```
HTTP/1.1 200 OK
Cache-Control: private, no-cache, no-sto
Expires: Sat, 01 Jan 2000 00:00:00 GMT
P3P: CP="DSP LAW"
Pragma: no-cache
Set-Cookie: act=deleted; expires=Tue, 1l
.\.z.....S...;..9......'q0b'....!.0....
?........\.-...N...z.....'.0.@3...Bd.U..
....S    ]~...$.=<.\.q/)..J...8..K..t. .
.9..9.=P......wK\..    .V2.y. T.m.:.68..
..W.G罒C..4g&If..@......V..WW-....X'.U(I
```

To full visualization of extended relationships and embedded content

Filter | List

*Searching **60** documents.* *__1__ documents bookmar*

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

Page 1 of 1 | 150 | View 1 - 66 of 66

Text | Attributes | Notes

ge (www.iex.nl)

IEX van beleggers voor beleggers

Home | Beleggingsfondsen | Turbo's | Speeders | Opties & Futures | Productrecensies

Zoek

Probeer nu GRATIS

10 van Tak: Serieuze zaken

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

Marcel Tak - 4 apr, 12:00

Speculeren met gokken

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

Mark Leenards - 4 apr 07, 09:30 | Reacties: 12

IEX Dageraad: Zonnig

"AEX opent hoger. Geen jaarrapportages fondsen, wel cijfers NVM en nieuwtjes NYSE Euronext..."

Arend Jan Kamp - 4 apr 07, 08:00

Mijn gifbeker

"Tom Tom blijft zakken, mijn puts op de AEX smelten en Knabbel is écht weg. Geef mij die gifbeker maar..."

Frank van Dongen - 3 apr 07, 17:30 | Reacties: 18

IEX Bull/Bear Enquête: Bibberaties

"Het Nederlandse beleggers-vertrouwen daalt fors voor april. ABN Amro is flopper, ING is topper..."

Redactie - 3 apr 07, 12:30

Profs in paniek

"De profs zijn berensomber voor april

Nieuw(s) op IEX

IEX Prijzenspel Beleg in aandelen en win een laptop! Start 15 januari.

Real-time koersen Geheel vernieuwd en tegen de laagste prijs van Nederland

Geldwaardering.nl Vernieuwd! Deel uw opinie over financiële producten en aanbieders

Dividend Wanneer en hoeveel? Zie de dividend agenda op IEX

IEX Universiteit Volg online de cursus

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 woensdag 4 april

Realtime

Markt vandaag

Euronext A'dam: Ahold gro

AEX-inde	517,33	+0,
Euro/Dol	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,

Sten

Kies uw bank pair trad

Client example: U.S. financial organization shortens investigations backlog with integrated network forensics

Accelerate incident investigations

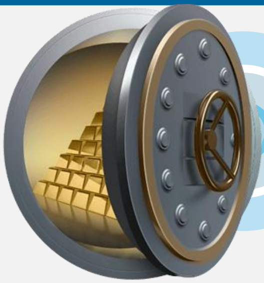
Prior network forensics point solution averaging

Hours

to investigate an incident as either false positive or true threat reduced to

Minutes

using integrated capability



Business challenge

- Completing daily lists of QRadar offense investigations to avoid building backlogs
- Quickly ruling out false positives to spend more time on true threat remediation plans
- Eliminate outsourcing of forensics analysis

IBM Security Solutions (QRadar SIEM, QRadar QFlow, QRadar Incident Forensics)

Single console Web-based interface provides clear direction regarding potential scope and risk for identified incidents. Right-click integration and Forensics dashboard provide ultimate clarity revealing underlying conditions supporting offense.

Find out more on Incident Forensics

Visit our website :
www.ibm.com/software/products/en/qradar-incident-forensics

Read our expert perspectives**:**
www.securityintelligence.com

Keep up to date with our latest news**:**
@IBMSecurity

Now it’s your turn to try it!

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.