

BusinessConnect and SolutionsConnect

It's time to make bold moves.

Following the advanced and persistent threat - Trail of Breadcrumbs

DELIVERING CLARITY TO CYBER SECURITY INVESTIGATIONS

Jason Corbin -

Director - Security Intelligence Strategy and Product Management

IBM Security Systems



Harsh realities for many enterprise network CISOs



Attackers spend an estimated **243 days** on a victim's network before being discovered

In 2013, it took organizations **32 days** on average to resolve a cyber-attack

Annual cost of cyber-crime in the U.S. now stands at **\$11.56 million** per organization

In 2012, **38%** of targets were **attacked again** once the original incident was remediated.

63% of victims made aware of their breaches by an external organization

Has our organization been compromised?

When was our security breached?

What type of attack is it?

How to avoid becoming a repeat victim?

How do we identify the attack?

What resources and assets are at risk?

Advanced attackers follow a five-stage attack chain



ATTACK CHAIN

1 Break-in



Reconnaissance, spear phishing, and remote exploits to gain access

2 Latch-on



Malware and backdoors installed to establish a foothold

3 Expand



Lateral movement to increase access and maintain a presence

4 Gather



Acquisition and aggregation of confidential data

5 Exfiltrate

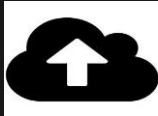


Data exfiltration to external networks

Challenges compounded by volume of data/transactions/issues



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



500+ files uploaded to internet sites a day



2,000+ files a day downloaded from the internet



30% of network use is remote



2 laptops a week go AWOL



20 new IT assets a week



3000+ SPAM/Fishing emails a week



External network scanned 10 times a day



100,000+ vulnerabilities in the network



5 network alerts per minute



100+ potentially malicious web site visits per day



20 Network configuration changes a week

Endpoint Alerts
Logs
External Threat Feeds
Flows Vulnerabilities
Documents Events
Identity Packets
Device Configuration

Reduce Data and Prioritize Incidents Quickly..Then Drill Down!

IBM



Automated Offense Identification

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

Prioritized Incidents

Suspected Incidents

Directed Forensics Investigations

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

Embedded Intelligence



Complex Threat Detection



Offense 3063		Summary	Attackers	Targets	Categories	Annotations	Networks	Events
Magnitude							Relevance	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan				Event count	1428 events in 3 categories		
Attacker/Src	202.153.48.66				Start	2009-09-29 16:05:01		
Target(s)/Dest	Local (717)				Duration	1m 32s		
Network(s)	Multiple (3)				Assigned to	Not assigned		
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with network scan data. A host in China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first scan detected a buffer overflow vulnerability on a host.							

Sounds Nasty...

But how do we know this?

The evidence is a single click away.

Network Scan
Detected by QFlow



Buffer Overflow
Exploit attempt

	Event Name	Source IP	Destination IP	Destination Port	Log Source	Low Level Category
	Network Sweep - QRadar Classify Flow	202.153.48.66	Multiple (716)	445	Flow Classification E	Network Sweep
	NETBIOS-DG SMB v4 srvsvc NetrpPathConon	202.153.48.66	Multiple (8)	445	Snort @ 10.1.1.5	Buffer Overflow

Port	Service	OSVDB ID	Name	Description	Risk / Severity
445	unknown	49243	Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution	Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity.	3

Targeted Host Vulnerable
Detected by Nessus

Total Security Intelligence
Convergence of Network, Event and Vulnerability data

Potential Data Loss?
Who? What? Where?

Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

Attacker Summary			
Magnitude		User	scott
Description	10.103.14.139	Asset Name	dhcp-workstation-103.14.139.acme.org
Vulnerabilities	0	MAC	Unknown
Location	NorthAmerica.all	Asset Weight	0

Who?
An internal user

	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
	DELETE failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Deny
	SELECT succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Allow
	Misc Logout	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Logout
	Suspicious Pattern Detect	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Suspicious Pattern Detected
	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Remote Access Login Failed

What?
Oracle data

- Navigate
- Information
- Resolver Actions
- TNC Recommendation
- DNS Lookup
- WHOIS Lookup**
- Port Scan
- Asset Profile
- Search Events
- Search Flows



QRadar Has Completed Your Request

Go to APNIC results

[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View

Where?
Gmail

Full Packet Capture

- Capture packets off the network
- Include other, related structured and unstructured content stored within the network



Retrieval & Session Reconstruction

- For a selected security incident, retrieve all the packets (time bounded)
- Re-assemble into searchable documents including full payload displayed in original form



Forensics Activity

- Navigate to uncover knowledge of threats
- Switch search criteria to see hidden relationships

1fo-ren-sic *adjective* \fə-ˈren(t)-sik, -ˈren-zik\ : relating to the ability of discovery

- Search is Fundamental to Discovery
- Index Everything = Search Everything
 - Flow meta-data
 - Protocol Meta-data
 - Message Content
 - File Content
 - File Meta-data
 - File Flows
- Forensic Data is Unstructured Polymorphic Data
 - Search Engines are a Perfect solution
 - Index Once Search Everything
 - Easy and Familiar Search Methodology
 - Correlate & Assimilate Disparate Data and Events
 - Second Response times for Terabytes of data
 - Powerful Search Engine Query Language (Boolean, Phonetic, & Proximity Searches)
- Enables virtually any Security Analyst to Conduct Forensics

The screenshot displays the IBM Security QRadar SIEM interface. At the top, there are navigation tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Forensics, Reports, Risks, Vulnerabilities, and Admin. A search bar contains the term "Secret" and indicates "Searching 85,345 documents." Below the search bar are buttons for "Surveyor", "Epersonas", "Export", and "Visualize". The main area shows a table with search results. The table has columns for Row, Sel, Ret, Time Stamp, Application Protocol, Description, and Content. The results list various events such as "MSN File Transfer", "Email Message", and "Web Page" with their respective timestamps and protocols.

Row	Sel	Ret	Time Stamp	Application Protocol	Description	Content
001	<input type="checkbox"/>	1	2007/04/04 01:52:00 PM	msn	MSN File Transfer	Acts of Incorporation REPL
002	<input checked="" type="checkbox"/>	1	2007/04/04 01:47:59 PM	smtp	Email Message	Hi Piet,I was wondering, c
003	<input type="checkbox"/>	1	2007/04/04 01:56:17 PM	smtp	Email Message	Dear sirs,I would like to t
004	<input type="checkbox"/>	1	2014/02/07 07:34:50 PM	http	Web Page	ReplayShareEmbedRelatedA
005	<input type="checkbox"/>	1	2014/02/07 07:34:50 PM	http	Web Page	ReplayShareEmbedRelatedA
006	<input type="checkbox"/>	1	2014/02/07 07:34:50 PM	http	Web Page	ReplayShareEmbedRelatedA
007	<input type="checkbox"/>	1	2014/02/07 07:26:31 PM	http	Web Page	ScoresTeamsPlayersPlayer
008	<input type="checkbox"/>	1	2014/02/07 07:35:04 PM	http	Web Page	Sign inUpload SearchShow
009	<input type="checkbox"/>	2	2014/02/07 07:25:44 PM	http	Web Page	You are logged into YouTu
010	<input type="checkbox"/>	2	2014/02/07 07:45:11 PM	http	Web Page	Andy TosswillUploadDashb
011	<input type="checkbox"/>	2	2014/02/07 07:41:43 PM	http	Web Page	Andy TosswillUploadDashb
012	<input type="checkbox"/>	2	2014/02/07 07:39:10 PM	http	Web Page	You are logged into YouTu
	<input type="checkbox"/>	2	2014/02/07 07:43:20 PM	http	Web Page	Andy TosswillUploadDashb

Reconstructing Sessions - Inspectors

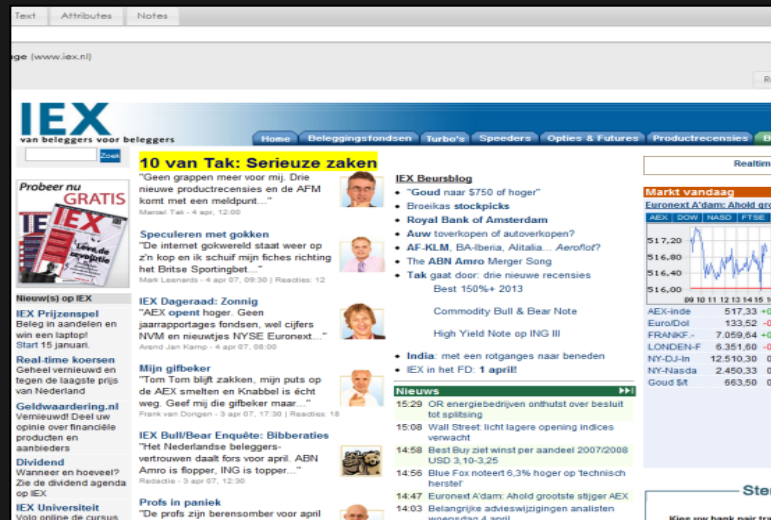


QRadar Incident Forensics rebuilds entire sessions from packets using its Inspector Framework

1fo-ren-sic *adjective* \fə-'ren(t)-sik, -'ren-zik\ : relating to the ability to reconstruct an event

Inspectors Glean Information From Packets

- To provide a **Rich Search Environment**
 - IPAddress = 192.168.6.27 AND WebHost = bank AND Content: credentials
 - Port = [774 TO 899] AND File = emailist.doc
- To Enable a User to **Visually** Reconstruct Sessions & Events
 - Web Pages
 - Social Networking Sites
 - Documents
 - Instant Messaging
 - Protocols



The Inspector Framework is extensible, therefore new inspectors can be built for specialized protocols and custom applications

QRadar Incident Forensics has several features to deliver intelligence to the security analyst to assist in the forensics investigation

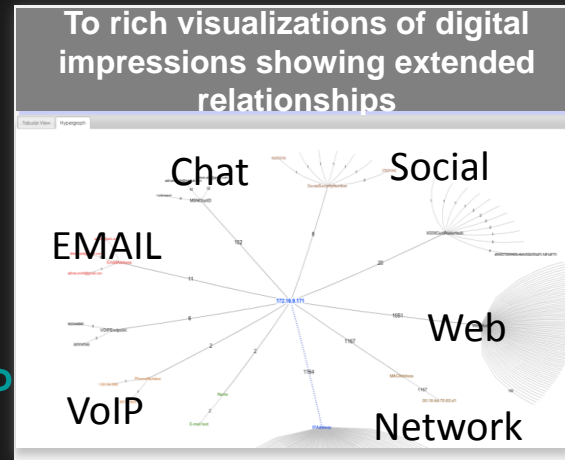
Digital Impressions: Compiled set of associations to identify identity trails

Suspect Content: Defined set of rules on content that signify suspicious activity



Content Categorization: Dynamic categorization of content based metadata and XForce feeds enables analyst to filter out the noise

Entity Alert
Scanning IP
Botnet



Searching 1,075 of 1,075 documents

Search Filters	Filter Type	Include	Exclude
ServerIPAddress		<input type="checkbox"/>	<input type="checkbox"/>
InitiatorIPAddress		<input type="checkbox"/>	<input type="checkbox"/>
ClientMACAddress		<input type="checkbox"/>	<input type="checkbox"/>
ResponderIPAddress		<input type="checkbox"/>	<input type="checkbox"/>
ServerMACAddress		<input type="checkbox"/>	<input type="checkbox"/>
ClientIPAdress		<input type="checkbox"/>	<input type="checkbox"/>
ApplicationProtocol		<input type="checkbox"/>	<input type="checkbox"/>
WebCategory		<input type="checkbox"/>	<input type="checkbox"/>
EmailAddress		<input type="checkbox"/>	<input type="checkbox"/>
WebHost		<input type="checkbox"/>	<input type="checkbox"/>
Case		<input type="checkbox"/>	<input type="checkbox"/>
UserQuery		<input type="checkbox"/>	<input type="checkbox"/>

Available Time Range: [Feb 17 2014 10:06:44] to [Feb 17 2014 10:14:13] Reset Range Apply Range

Select Filter: Default [X] [Y] [Z]

music chat fashion
health nudity law
history artshacking portals blogs
advertisements violence
astrology militancy
vehicles shopping finance
dating drugs sports
jobs pornscience

Case:DataLoss AND Collection:DataLoss.pcap Secret

Searching 83,601 documents.

Survivor Digital Impression Export Visualize

Results sorted by relevance to search (Document with word "secret")

ID	Color	Star	Doc Icon	Count	Date	Time	Protocol	Description	Content	Case	Collection
001	Red	Star	Doc	1	2014/02/17		http	Email Attachment	Project BluePrintTOP SECRETThis is ...	DataLoss	DataLoss.pcap
002	Green	Star	Doc	3	2014/02/17		http	Microsoft Word Document	Project BluePrintTOP SECRETThis is ...	DataLoss	DataLoss.pcap
003	Red	Star	Doc	4	2014/02/17		unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap
004	Red	Star	Doc	4	2014/02/17	10:06:46 AM	unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap
005	Red	Star	Doc	4	2014/02/17	10:06:46 AM	unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap
006	Red	Star	Doc	4	2014/02/17	10:06:46 AM	unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap
007	Red	Star	Doc	4	2014/02/17	10:06:50 AM	unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap
008	Red	Star	Doc	4	2014/02/17	10:06:47 AM	unknown	Unknown Session	EKEPEIEOFDFEEPEOEFACACACACACAFHE...	DataLoss	DataLoss.pcap
009	Red	Star	Doc	4	2014/02/17	10:06:52 AM	unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap
010	Red	Star	Doc	4	2014/02/17	10:06:58 AM	unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap
011	Red	Star	Doc	4	2014/02/17	10:06:56 AM	unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap
012	Red	Star	Doc	4	2014/02/17	10:07:02 AM	unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap
013	Red	Star	Doc	4	2014/02/17	10:07:04 AM	unknown	Unknown Session	isatapisatap	DataLoss	DataLoss.pcap

https://172.16.60.150/forensics/doc.php?gui=searchgrid&docid=DataLoss-DataLoss.pcap-000c2936ffdc-20140217150816049-164-12&caseid=DataLoss

Server: GSE
Alternate-Protocol: 80:quic

File Metadata +/-

FileHash	921c80855fb1a166cd04c4b02116983e9b63f2f475707d7c0afe5f7441914766
Filename	Blueprint.doc
Filepath	/opt/ibm/forensics/html/files/DataLoss/DataLoss.pcap/http/2014/02.17/15.07/05/408/Blueprint.doc
FileMetadata	Application-Name: Microsoft Office Word Author: Vijay Dheap Character Count: 134 Comments: Company: IBM Content-Length: 152064 Content-Type: application/msword Creation-Date: 2014-02-17T14:34:00Z Edit-Time: 600000000 Keywords: Last-Author: ADMINIBM Last-Save-Date: 2014-02-17T14:34:00Z Page-Count: 1 Revision-Number: 2 Template: Normal.dotm Word-Count: 23 subject: title: xmpTPg:NPages: 1
Content-Type	application/msword

Protocol Metadata +/-

ProtocolMetadata	HTTP-version: HTTP/1.1 HTTP-Reason: OK
------------------	---

Digital Impression +/-

WebHost	mail.google.com
---------	-----------------

Other Metadata +/-

CollectionType	1532450a2a3a15f4
----------------	------------------

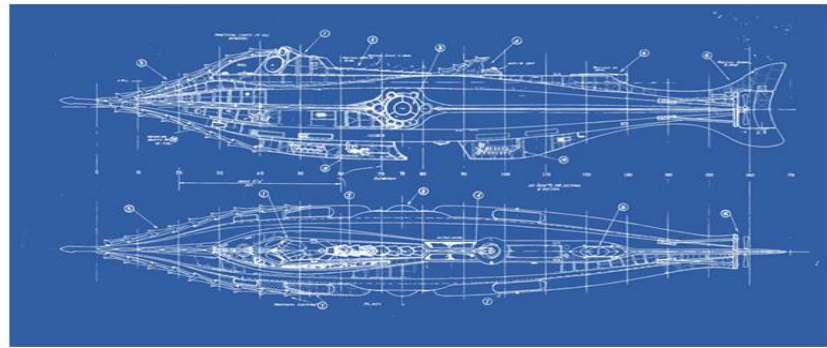
Page 1 of 10 150

All file meta-
data indexed
and searchable

Project BluePrint

TOP SECRET

This is our new innovative solution to meet new world dynamics. We project that this will change the way we do business.



QRadar Incident Forensics Document - Mozilla Firefox: IBM Edition

https://172.16.60.150/forensics/doc.php?gui=searchgrid&docid=DataLoss-DataLoss.pcap-000c2936ffdc-20140217150816049-164-12&caseid=DataLoss

View Text Attributes Notes

DataLoss-DataLoss.pcap-000c2936ffdc-20140217150816049-164-12
Mon Feb 17, 2014 10:08:16 AM

Microsoft Word Document
(mail.google.com) Export Document

- This document was captured at Feb 17 2014 10:08:16
- It was part of a http (tcp) session that started at Feb 17 2014 10:07:05
- The Server was at 74.125.226.214 (MAC:c8:6c:87:1e:94:2b) on port 80.
- The Client was at 192.168.2.24 (MAC:00:1c:c0:a4:14:82) on port 59053.

Http Metadata +/-

Host	mail.google.com
URI	/mail/u/0/?ui=2&ik=5DkEymdIwRwqFyzX2CCmv%7CC5e7340bf53e6703&attid=f_hrrvo6m70
URI-base	/mail/u/0/
URI-args	ui=2&ik=849518902b&view=up&fcid=hrrvo6m9j6cj&rt=j&act=fup&oauth=AG9B_P-5DkEymdIwRwqFyzX2CCmv%7CC5e7340bf53e6703&attid=f_hrrvo6m70
HTTP-RequestMethod	POST
HTTP-Status	200
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:27.0) Gecko/20100101 Firefox/27.0
WebCategory	Webmail / Unified Messaging Chat Instant Messaging
WebCategoryGroup	Information / Communication Information / Communication Information / Communication

Http Headers +/-

```
Host: mail.google.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:27.0) Gecko/20100101 Firefox/27.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/msword
Content-Disposition: attachment; filename="Blueprint.doc"
```

IPAddress (2)			
1	199.189.86.110	53	
2	192.168.2.24	53	

MACAddress (2)			
1	00:1c:c0:a4:14:82	53	
2	c8:6c:87:1e:94:2b	53	

EmailAddress (1)			
1	seanqforen@70-88-250-221-ma-nh-me-ne.hfc.comcastbusiness.net	53	

Search for [seanqforen@70-88-250-221-ma-nh-me-ne.hfc.comcastbusiness.net](#)

Get Relations for [seanqforen@70-88-250-221-ma-nh-me-ne.hfc.comcastbusiness.net](#)

Add EmailAddress [seanqforen@70-88-250-221-...](#) to Include Filter Default

Add EmailAddress [seanqforen@70-88-250-221-...](#) to Exclude Filter Default

IRC Chat Message

Mon Feb 17, 2014 10:11:17 AM

Refresh Export Document

IRC conversation for: seanqforensics

No Avatar Mon, 10:11 am seanqforensics: JOIN #qforensics

seanqforensics: PRIVMSG #qforensics :good your here, did you get the files?
shawnqforensics: :shawnqforensics!shawnqfore@70-88-250-221-ma-nh-me-ne.hfc.comcastbusiness.net PRIVMSG #qforensics :yeah, I got our files
shawnqforensics: :shawnqforensics!shawnqfore@70-88-250-221-ma-nh-me-ne.hfc.comcastbusiness.net PRIVMSG #qforensics :yeah, I got our files
seanqforensics: PRIVMSG #qforensics :great. I better get a nice bonus for this when you hire me on

No Avatar me-ne.hfc.comcastbusiness.net JOIN #qforensics

No Avatar Mon, 10:11 am seanqforensics: PRIVMSG #qforensics :good your here, did you get the files?





No Avatar Mon, 10:11 am seanqforensics: PRIVMSG #qforensics :good your here, did you get the files?

No Avatar Mon, 10:12 am shawnqforensics: :shawnqforensics!shawnqfore@70-88-250-221-ma-nh-me-ne.hfc.comcastbusiness.net PRIVMSG #qforensics :yeah, I got our files

No Avatar Mon, 10:12 am shawnqforensics: :shawnqforensics!shawnqfore@70-88-250-221-ma-nh-me-ne.hfc.comcastbusiness.net PRIVMSG #qforensics :yeah, I got our files

No Avatar Mon, 10:12 am seanqforensics: PRIVMSG #qforensics :great. I better get a nice bonus for this when you hire me on

Summary: QRadar Security Intelligence Enables....

-  **1 Forensics From an Offence**
-  **2 Investigating Relationships**
-  **3 Following the Trail**
-  **4 Closing the Case**

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 and other countries. All other trademarks are the property of their respective owners.

