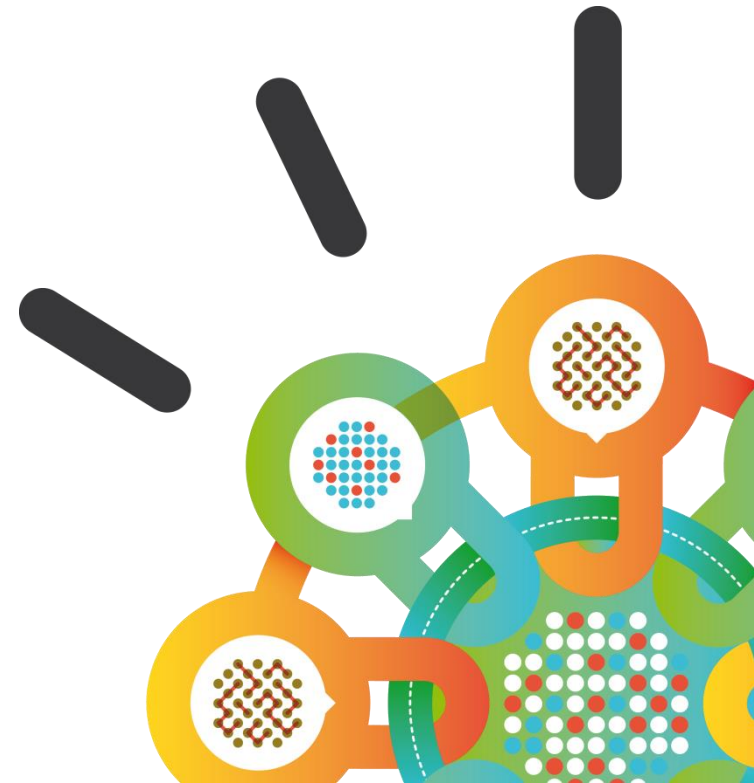


Security Intelligence.
Think Integrated.

QRadar Workshop POT

2014 Rev. 1.02

Introduction & Agenda



Instructor Introduction

- **Erasmus Volpe**
IBM SWG Security Systems
Email: erasmo.volpe@ch.ibm.com

- **Christian Messmer**
IBM SWG Security Systems
Email: christian.messmer@de.ibm.com



Please silence phones while in workshop, thanks.

Objectives

- Einführung in die Security Intelligence Produkt QRadar



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.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

No IBM course material may be reproduced in whole or in part without the prior written permission of IBM.

AGENDA Nachmittag

13:30 - 14:10 QRadar World (QVM, QRiskManager, QRadar 7.2.3)

14:10 - 14:50 Introducing QRadar Forensic

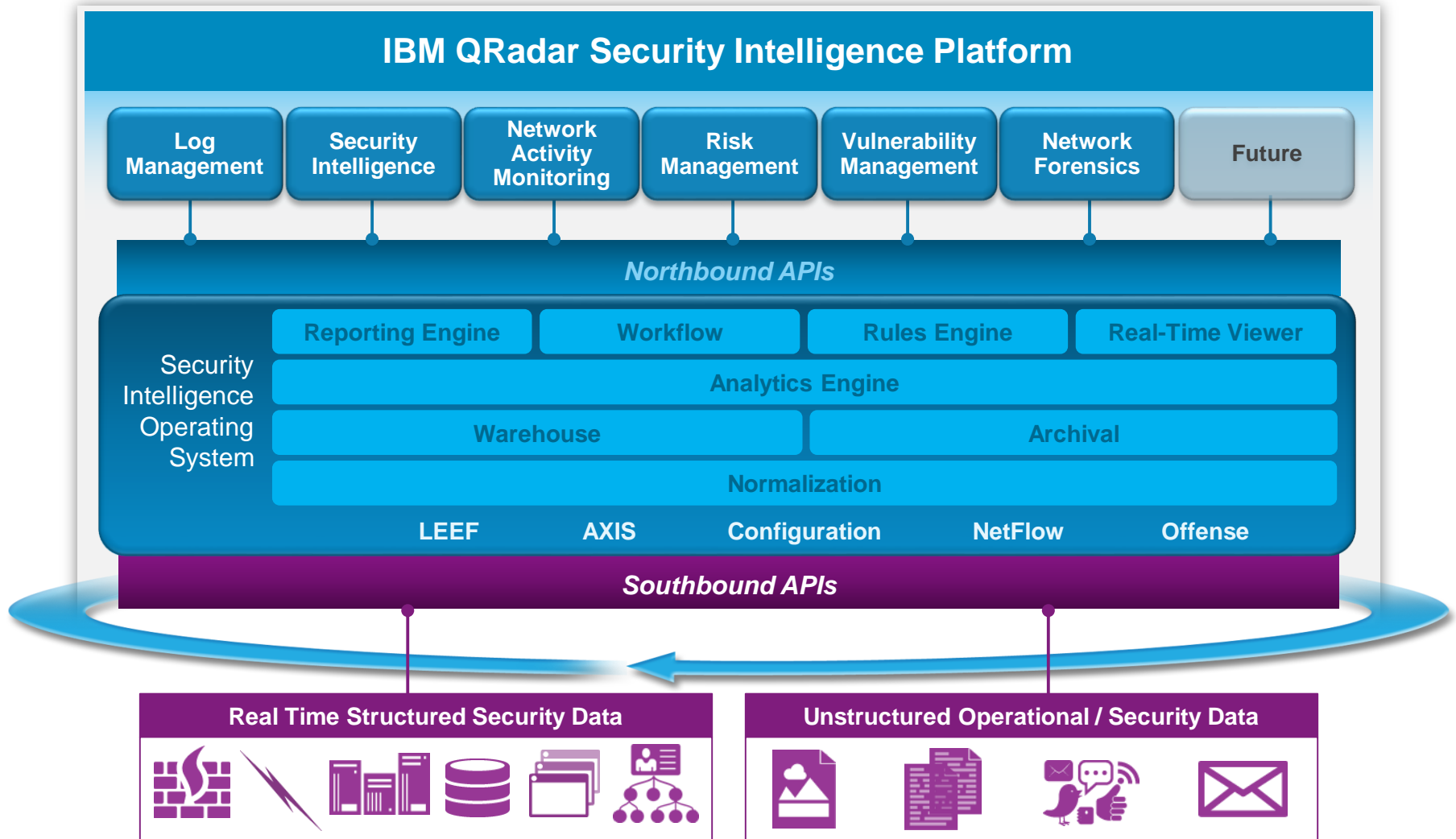
14:50 - 15:20 Break

15:20 - 17:00 Hands on and Lab Session

17:00 - 17:30 Open Table Discussion

17:30 - 19:00 Networking

Delivering multiple security capabilities through a purpose-built, extensible platform



Vulnerability Management



Today's Vulnerability Management deployments... cannot interpret the “sea” of vulnerabilities

Not Active: Are the applications being used?

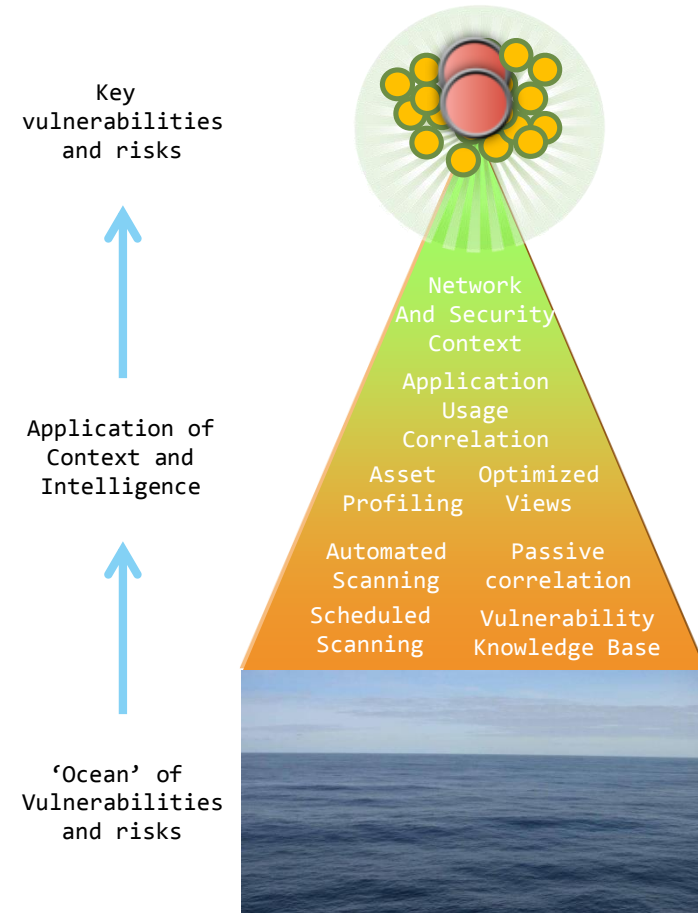
Patched: Are my vulnerabilities patched?

Blocked: Are there IPS and Firewall rules mitigating my vulnerabilities?

Critical: Are any of my web application vulnerabilities causing compliance failures?

At Risk: Are any potential threat sources accessing my web application?

Exploited: Have any of my vulnerabilities been exploited, where else am I vulnerable?



QRadar Vulnerability Manager

Helps interpret 'sea' of vulnerabilities

Not Active: By leveraging QFlow, QVM can tell if the vulnerable application is active

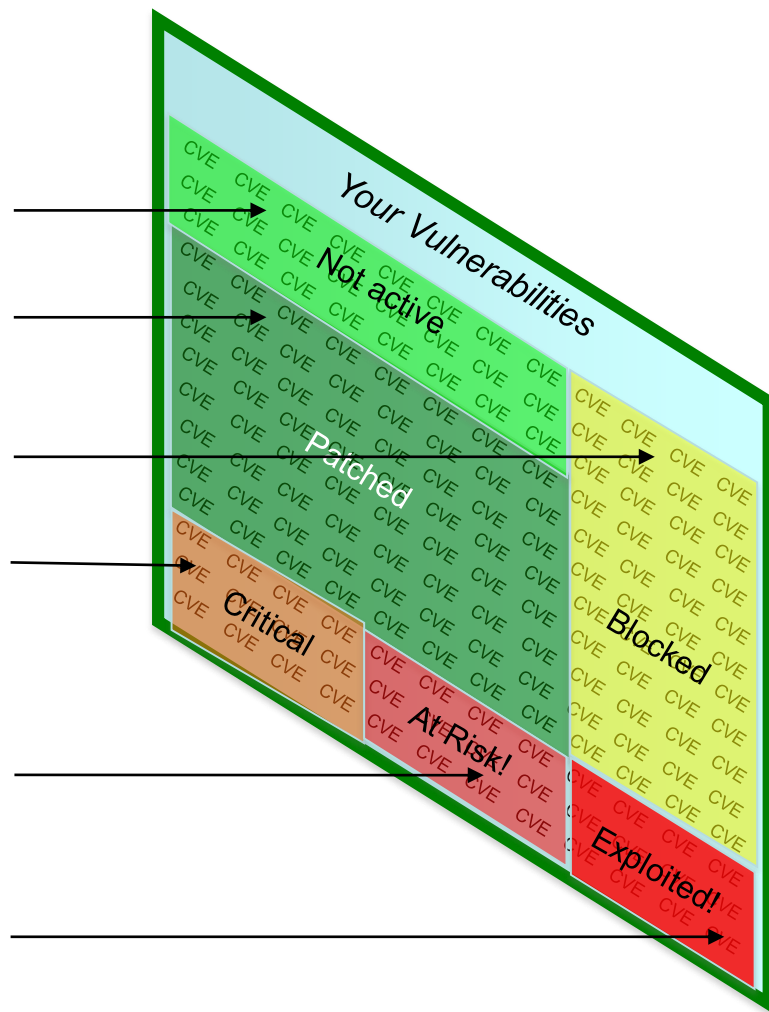
Patched: By leveraging Endpoint Manager, QVM understands what vulnerabilities will be patched

Blocked: By leveraging QRM, QVM can understand what vulnerabilities are blocked by firewalls and IPSs

Critical: By leveraging its vulnerability knowledge base, remediation flow and QRM policies, QVM can identify business critical vulnerabilities

At Risk: By utilizing X-Force threat, privileged user access, and SIEM security incident data, coupled with QFlow network traffic visibility, QVM can tell if vulnerable assets are communicating with potential threats

Exploited: By leveraging SIEM correlation and IPS data, QVM can reveal what vulnerabilities have been exploited



How QVM improves third-party vulnerability data

Benefit	QVM with 3 rd party scanner	QVM native scanning
Event driven and on-demand scanning	No	Yes
Asset model and watch list based scanning	No	Yes
Scan from existing QRadar appliances and managed hosts	No	Yes
Asset, vulnerability and traffic-based vulnerability management*	Yes	Yes
Custom vulnerability scores and context aware risk scoring*	Yes	Yes
Context aware vulnerability management (correlate network, threat, and vulnerabilities)	Yes	Yes
Incorporate firewall and network topology analysis into vulnerability risk assessment**	Yes	Yes
Comprehensive vulnerability filtering, reporting and dashboards	Yes	Yes
Holistic vulnerability view	Yes	Yes
Vulnerability assignment, remediation and exception processes	Yes	Yes

* Requires QRadar Risk Manager Light

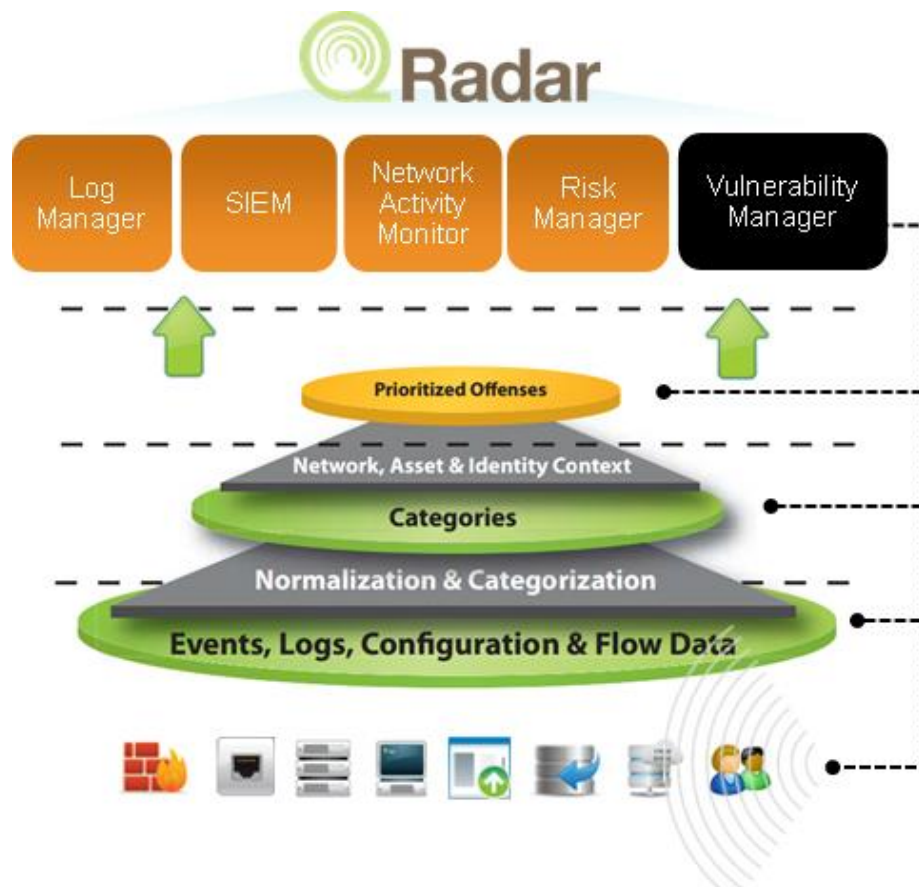
** Requires QRadar Risk Manager Full

Security Intelligence Strengthened...

by integrated vulnerability insights

First VA solution integrated with Security Intelligence

- Improves visibility
 - Intelligent, event-driven scanning, asset discovery, asset profiling and more
 - Dramatically improving actionable information through rich context
- Reduces data load
 - Bringing rich context to Vulnerability Management
- Breaks down silos
 - Leveraging all QRadar integrations and data
 - Unified vulnerability view across all products
 - Reducing total cost of ownership through product consolidation

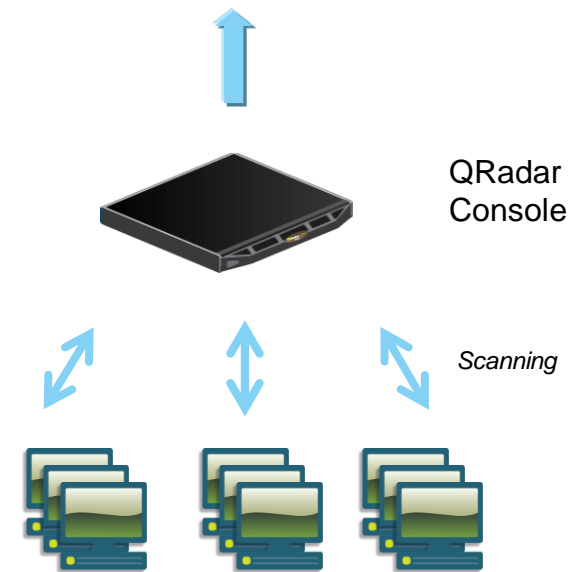


Security Intelligence is extending and transforming vulnerability management – just as it did with logs, events, flows and risk management.

Deployment scenarios

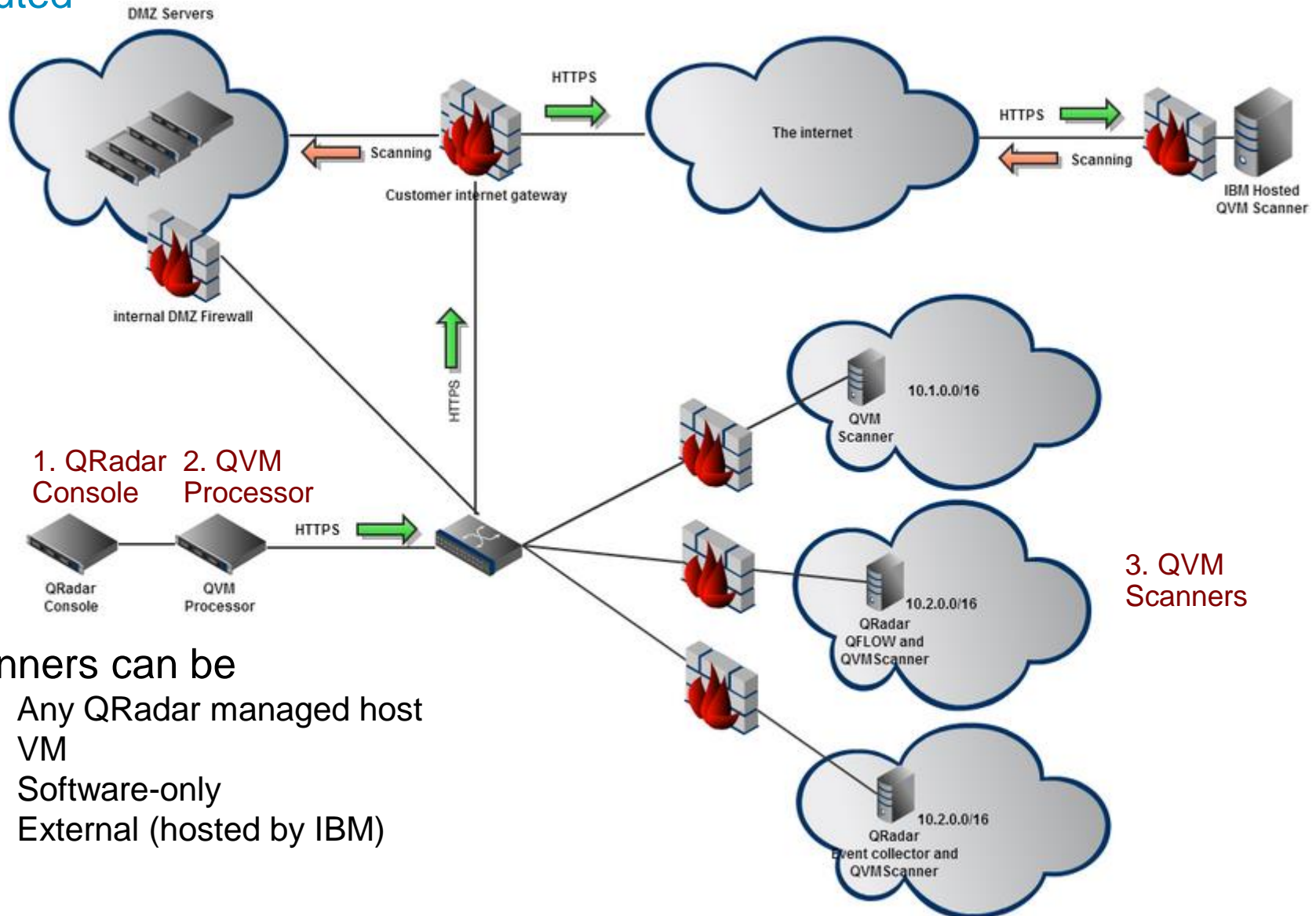
AIO

- All-In-One
 1. QRadar Console
 2. QVM Processor
 3. QVM Scanner
- Zero software install
- License key enablement
- Simple evaluation process for existing customers
- Distributed scanning required for larger deployments (larger than a POC)



Deployment scenarios

Distributed



- Scanners can be
 - Any QRadar managed host
 - VM
 - Software-only
 - External (hosted by IBM)

Scanner

Methods used to detect vulnerabilities

Active Tests

Passive Tests

Authenticated Scanning

- Database matching
- OVAL methods

Early Warnings



Hosts discovered:	2
Tools executing:	28
Tools queued:	124
Tools finished in last 5 minutes:	30
Estimated time to complete:	0
Current checks:	SSH - 2002-1644 x 1
	SSH - Default Accounts x 1
	SSL - Authenticity Check x 1
	SSH - 2002-1359 x 1
	ssl_anon_ciphers x 1
	FTP - anonchk x 1
	SMB Login x 2
	SSH - dropbear x 1
	FTP - Check Auth x 1
	openssl_detect x 1
	CGI Scanner - n x 1
	SSL - Get Certificate Info x 1
	Web Application Scanning x 1
	SSH - 2006-0705 x 1
	PortScan x 1
	SSL - Selfsigned Certificate x 1
	SSH - 2002-1646 x 1
	Netbios - NULL Session x 2
	ssl_weak_ciphers x 1
	subversion_detect x 1
	SSH - 2002-1360 x 1
	Conficker - Detection x 2
	CGI Check - 2001-0212 x 1
	ssl_weak_hash x 1
	FTP - Get Version x 1

QRadar Incident Forensic

Network Forensic

The screenshot shows the IBM Security Systems dashboard with several navigation tabs at the top: Log Management, NextGen SIEM, Activity Monitoring, Risk Management, Vulnerability Management, and Network Forensics. A red arrow points to the 'Network Forensics' tab, which is highlighted by a blue callout. The dashboard content includes:

- Current Threat Level:** 1 (ALERTCON)
- Offense Name and Magnitude Table:**

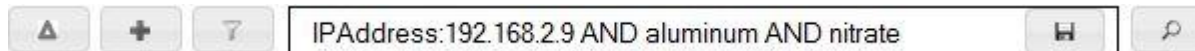
Offense Name	Magnitude
BotNet Detected by X-Force IP Reputation Feed containing IRC Connections	High
Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Assessable Remote Scanner Detected	Medium
Policy Chat or IM Traffic Detected containing Chat MSN	Low
Communication to a known Bot Command and Control containing Chat IRC	Low
Sensitive Data in Transit containing Web Facebook Application	Low
- Top Applications Outbound to the Internet (Source Bytes):** Line chart showing traffic volume from 03:00 to 08:00.
- Top Applications (Total Bytes):** Line chart showing total traffic volume from 03:00 to 08:00.
- Inbound Events by Country (real-time):** Pie chart showing traffic distribution by country.
- Flow Bias (Total Bytes):** Line chart showing flow bias from 02:35 to 08:35.
- Top Authentication Failures by User (Event Count):** Bar chart showing authentication failures by user.

What is QRadar Incident Forensics?

“QRadar Incident Forensics captures all the content of all the packets in a flow and indexes the payload as well as the metadata to enable fast search driven data exploration.”

What gets indexed? EVERYTHING!!

(well, sort of....)



PCAP example with Wireshark

Wireshark interface showing a captured network packet (Frame 11) and its detailed structure. The packet is an encrypted application data (SSL) packet.

No.	Time	Source	Destination	Protocol	Info
5	2009-01-23 20:50:26.711344	10.88.229.196	10.88.229.209	TCP	[TCP segment of a (reassembled) PDU]
6	2009-01-23 20:50:26.711545	10.88.229.196	10.88.229.209	TLSv1	Server Hello, Certificate, Server Hello Done
7	2009-01-23 20:50:26.711616	10.88.229.209	10.88.229.196	TCP	38353 > https [ACK] Seq=121 Ack=1449 win=...
8	2009-01-23 20:50:26.711647	10.88.229.209	10.88.229.196	TCP	38353 > https [ACK] Seq=121 Ack=1530 win=...
9	2009-01-23 20:50:26.713357	10.88.229.209	10.88.229.196	TLSv1	Client Key Exchange, Change Cipher Spec, ...
10	2009-01-23 20:50:26.717451	10.88.229.196	10.88.229.209	TLSv1	Change Cipher Spec, Encrypted Handshake Message
11	2009-01-23 20:50:26.717792	10.88.229.209	10.88.229.196	TLSv1	Application Data
12	2009-01-23 20:50:26.763286	10.88.229.196	10.88.229.209	TLSv1	Application Data
13	2009-01-23 20:50:26.763288	10.88.229.196	10.88.229.209	TLSv1	Application Data
14	2009-01-23 20:50:26.802843	10.88.229.209	10.88.229.196	TCP	38353 > https [ACK] Seq=485 Ack=2140 win=...
15	2009-01-23 20:50:26.815833	10.88.229.209	10.88.229.196	TLSv1	Application Data
16	2009-01-23 20:50:26.816144	10.88.229.209	10.88.229.196	TLSv1	Application Data
17	2009-01-23 20:50:26.816538	10.88.229.196	10.88.229.209	TCP	https > 38353 [ACK] Seq=2140 Ack=1577 win=...

Frame 11 (248 bytes on wire, 248 bytes captured)

- Ethernet II, Src: HewlettP_c3:c6:01 (00:14:c2:c3:c6:01), Dst: vmware_a2:58:b1 (00:50:56:a2:58:b1)
- Internet Protocol, Src: 10.88.229.209 (10.88.229.209), Dst: 10.88.229.196 (10.88.229.196)
- Transmission Control Protocol, Src Port: 38353 (38353), Dst Port: https (443), Seq: 303, Ack: 1573, Len: 182
- Secure Socket Layer
 - TLSv1 Record Layer: Application Data Protocol: http
 - Content Type: Application Data (23)
 - Version: TLS 1.0 (0x0301)
 - Length: 177
 - Encrypted Application Data: 166813911B828BE9E3710FC1F3BDCB91D1B9840376F1521D...

```

0040  0e 63 17 03 01 00 b1 16 68 13 91 1b 82 8b e9 e3  .C.... h.....
0050  71 0f c1 f3 bd cb 91 d1 b9 84 03 76 f1 52 1d 7f  q..... .v.R.
0060  d8 bd c1 76 1a 1c 0e d6 f3 4b 84 7c a5 04 38 71  ..v.... .K|.8q
0070  a5 50 1f 07 be 0c 5e d2 f0 36 9c 4c fb 36 18 6c  .P...A. .6.L.6.l
0080  93 19 6a a3 9e 04 f4 e5 2c 75 ad b0 7e d3 9b 86  .j.... .u.~...
0090  94 b3 67 87 f7 af f4 2a 32 7d fc b9 0b 5d 4b 15  .g.... * 2}...]k.
00a0  46 df 44 7c cb 08 2b 4a 53 c2 e6 23 24 62 c7 53  F.D|..+J s. # $ b . S
00b0  cc c0 49 51 b5 b8 59 6a bd 6a f8 27 0f 95 c1 41  .IQ.Yj .j. ...A
00c0  40 ca 28 1e b7 3e a1 08 aa ca b1 38 42 6f d2 c3  @.(.>... .8Bo.
00d0  6f 86 d8 77 fc 9f a6 40 e4 6d dc fe 82 0b 02 2a  o.w...@ .m.....*
00e0  63 6a 76 04 dc 97 95 95 b4 e8 ac 31 65 0a fb 55  cjv.... .1e..U
00f0  45 d6 6d 63 df 2a 7e 93  E.mc.*~.
    
```

Payload is encrypted application data (ssl.app_data), 177 bytes

Packets: 33 Displayed: 33 Marked: 0

What is QRadar Incident Forensics?

Web Page Reconstruction

IBM Security QRadar SIEM
admin | Preferences | Help | Messages | System Time: 2:40 PM

Dashboard Offenses Log Activity Network Activity Assets Forensics Reports Vulnerabilities Admin

Back to search results

Filter List

Searching **12,475** documents. 0 documents bookmarked.

Id	Date	Protocol	Description	Relevancy (1)
174	2014/02/19 01:06:39 PM	SSLTLS	X509 Certificate	1
175	2014/02/19 01:06:39 PM	SSLTLS	X509 Certificate	1
176	2014/02/19 01:06:39 PM	SSLTLS	X509 Certificate	1
177	2014/02/19 01:06:39 PM	HTTP	Image File	1
178	2014/02/19 01:06:40 PM	HTTP	Video Content	1
179	2014/02/19 01:06:42 PM	SSLTLS	X509 Certificate	1
180	2014/02/19 01:06:42 PM	SSLTLS	X509 Certificate	1
181	2014/02/19 01:06:48 PM	SSLTLS	TLSv1.2 Session	1
182	2014/02/19 01:06:52 PM	SSLTLS	X509 Certificate	1
183	2014/02/19 01:06:52 PM	SSLTLS	X509 Certificate	1
184	2014/02/19 01:06:52 PM	SSLTLS	X509 Certificate	1
185	2014/02/19 01:06:52 PM	SSLTLS	X509 Certificate	1
186	2014/02/19 01:06:52 PM	SSLTLS	X509 Certificate	1
187	2014/02/19 01:06:52 PM	SSLTLS	X509 Certificate	1
188	2014/02/19 01:07:26 PM	SSLTLS	TLSv1.2 Session	1
189	2014/02/19 01:07:26 PM	SSLTLS	TLSv1.2 Session	1
190	2014/02/19 01:07:26 PM	SSLTLS	TLSv1.2 Session	1
191	2014/02/19 01:07:26 PM	SSLTLS	TLSv1.2 Session	1
192	2014/02/19 01:07:26 PM	SSLTLS	TLSv1.2 Session	1
193	2014/02/19 01:07:26 PM	SSLTLS	TLSv1.2 Session	1
194	2014/02/19 01:07:26 PM	HTTP	Web Page	1
195	2014/02/19 01:07:26 PM	SSLTLS	TLSv1.2 Session	1
196	2014/02/19 01:07:26 PM	SSLTLS	TLSv1.2 Session	1
197	2014/02/19 01:07:26 PM	SSLTLS	TLSv1.2 Session	1

Query: Case:Case2 AND Collection:joelaptop.pcap

View Text Attributes Notes

Case2-joelaptop.pcap-000c2996a528-20140219180726437-487-1
Wed Feb 19, 2014 01:07:26 PM

Web Page (espn.com)

Hybrid Reconstruction Refresh Export Document

What is QRadar Incident Forensics?

Social Network Conversation Reconstruction

View | Text | Attributes | Notes


SocNet- chats20090312.pcap - 0800272739f6- 20090312160 418103-67-4
MSN Avatar Transfer Thu Mar 12, 2009 04:04:18 PM
Refresh Export Document


MSN conversation for: pjohnstone@gmail.com


No Avatar Thu, 04:03 pm [Avatar upload from **pjohnstone@gmail.com** : avatar.png]


No Avatar Thu, 04:04 pm **saimmyon@hotmail.com**: Did I tell you about the aluminum nitrate? Shipment goes out next Saturday.

No Avatar Thu, 04:04 pm [Avatar upload from **saimmyon@hotmail.com** : avatar.png]

 Thu, 04:04 pm **pjohnstone@gmail.com**: to the dejavu warehouse?

 Thu, 04:04 pm **saimmyon@hotmail.com**: Which DejaVu office should we use?

 Thu, 04:04 pm **pjohnstone@gmail.com**: probably the one is Pakistan

 Thu, 04:05 pm **saimmyon@hotmail.com**: Good thinking.


What is QRadar Incident Forensics?


Social Network Conversation Reconstruction


View Text Attributes Notes


Facebook Conversation qtest-jaymarino_fb.pcap-0 800272739f6-2010021614414 1755-137-13-1
(www.facebook.com) Tue Feb 16, 2010 02:41:41 PM


Facebook Home conversation for: unknown.

 **Jay Marino:** Some shots of flying into Hyannis on Cape Cod
Tuesday, Feb 16, 2010 at 02:41 pm:



 **Jay Marino:** Some photos of an Angel Flight I did into Hyannis airport on Cape Cod
Tuesday, Feb 16, 2010 at 02:41 pm:

 **Jay Marino:** Airplanes that I have owned or flown
Tuesday, Feb 16, 2010 at 02:41 pm:



Metadata

View Text Attributes Notes

AdminOnly-Offense6.pcap-005056b423bc-20080422175328701-1-1
Tue Apr 22, 2008 02:53:28 PM

Web Page (www.youtube.com) Export Document

Show Context: 1 2 5 15 60 Minutes

- This document was captured at Apr 22 2008 14:53:28
- It was part of a http (tcp) session that started at Apr 22 2008 14:53:28
- The Server was at 208.65.153.253 (MAC:00:18:19:65:51:ff) on port 80.
- The Client was at 10.0.82.117 (MAC:00:11:25:d6:4b:5b) on port 1595.

Http Metadata +/-

Host	www.youtube.com
URI	/results?search_query=nba&search_type=
URI-base	/results
URI-args	search_query=nba&search_type=
HTTP-RequestMethod	GET
HTTP-Status	200
User-Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SU 3.011; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648)
WebCategory	Social Networking Social Media
WebCategoryGroup	Social Networking Entertainment / Culture

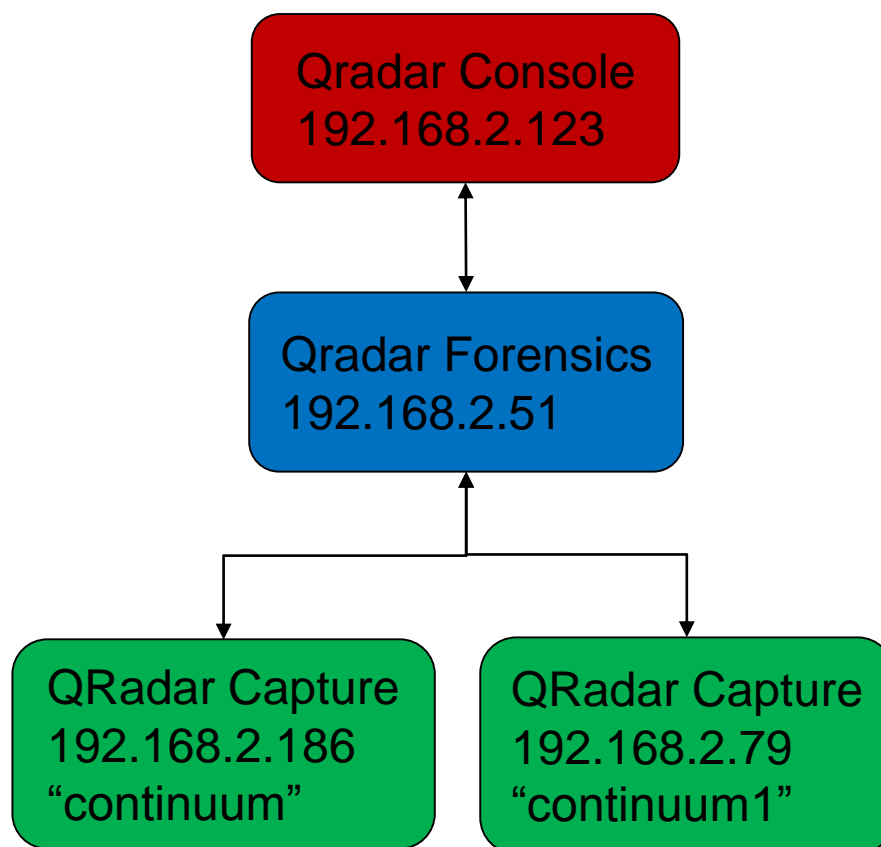
Http Headers +/-

File Metadata +/-

FileHash	7e23219981fff7629737091371705a3ba4714c4e76c15181a7fc1ad274ddfa75
Filename	results.html
Filepath	/opt/ibm/forensics/html/files/AdminOnly/Offense6.pcap/http/2008/04.22/17.53/28/692/www.youtube.com/results.html
FileMetadata	Content-Encoding: UTF-8
	Content-Length: 75008
	Content-Type: text/html
	description: Share your videos with friends and family keywords: video,sharing,camera phone,video phone title: YouTube - Broadcast Yourself.
Content-Type	text/html

WorkFlow Configuration – Multiple Capture Devices

- Forensics can be configured connect to multiple capture devices
- Multiple devices are viewed by Forensics as a single ‘logical’ device



Document Viewer Attributes

View Text Attributes Notes

JoeTempCase-joelaptop.pcap-000c2996a528-20140219180726437-487-1
 Wed Feb 19, 2014 01:07:26 PM

Web Page (espn.go.com) Export Document

- This document was captured at Feb 19 2014 13:07:26
- It was part of a http (tcp) session that started at Feb 19 2014 13:07:26
- The Server was at 68.71.212.186 (MAC:c8:6c:87:1e:94:2b) on port 80.
- The Client was at 192.168.2.9 (MAC:3c:97:0e:b9:cb:b3) on port 52359.

Http Metadata +/-

Host	espn.go.com
URI	/
URI-base	/
HTTP-RequestMethod	GET
HTTP-Status	200
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
WebCategory	News / Magazines Search Engines / Web Catalogs / Portals Sports
WebCategoryGroup	Information / Communication Information / Communication Lifestyle

Http Headers +/-

File Metadata +/-

FileHash	4fe3aeb56cbf16698fce18ac8a8ae21cb62e53a4eb0e1b4bffbeeffca0618ab7
Filename	__ROOT__.html
Filepath	/opt/ibm/forensics/html/files/JoeTempCase/joelaptop.pcap/http/2014/02.19/18.07/26/341/espn.go.com/__ROOT__.html
Content-Encoding: UTF-8	
Content-Length: 197901	
Content-Type: text/html	
X-UA-Compatible: IE=edge,chrome=1	
description: ESPN.com provides comprehensive sports coverage. Complete sports information including NFL, MLB, NBA, College Football, College Basketball scores and news.	
google-site-verification: xuj1ODRluWa0frM-BjIr_aSHoUC7HB5C1MgmYAM_GkA	
googlebot: index, follow	

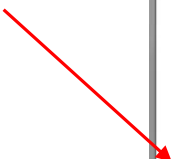
Common Attributes
(all documents)



Protocol Specific Attributes



Additional Attributes



Document Viewer Attributes

pop3

Standard Mail Headers +/-

From	"Michael Bolan" <michaelbolan@comcast.net>
To	"Andrew E. Copeland" <acopeland@sendza.com>
Subject	Re: Friday -
UserName	acopeland
UserPassword	password

All Mail Headers +/-

File Metadata +/-

Protocol Metadata +/-

ProtocolMetadata	ServerGreeting: +OK Microsoft Exchange Server 2003 POP3 server version 6.5.7226.0 MsgId: 68
------------------	--

FTP

File Metadata +/-

FileHash	d9b35ff6b750c3c77d146c44a9825f3f24937f2ec309870b91e4918b2e8c67
Filename	repomd.xml
Filepath	/opt/ibm/forensics/html/files/LoginFail/enpulse3.pcap/ftp-data/2008/04.2
FileMetadata	Content-Type: application/xml
Content-Type	application/xml

Protocol Metadata +/-

ProtocolMetadata	ServerGreeting: mirror NcFTPD Server (free educational license) ready. UserName: anonymous UserPassword: anonymous@
------------------	---

IMAP

Standard Mail Headers +/-

All Mail Headers +/-

File Metadata +/-

Protocol Metadata +/-

ProtocolMetadata	MsgId: 263 MessageFlags: \Recent InternalDate: 24-Apr-2008 14:23:40 -0400 UID: 264 RFC822.SIZE: 48467
------------------	---

DHCP

Protocol Metadata +/-

ProtocolMetadata	TransactionId: 733305565 DhcpServer: 192.168.100.1 SubnetMask: 255.255.255.0 LeaseTime: 24 hours Router: 192.168.100.1 DnsServer: 192.168.100.2 DnsServer: 208.67.222.222 DnsServer: 208.67.220.220 DomainName: internal.sendza.com
------------------	---

Forensics Administration – Admin Console

- New Forensics Section in Admin Console
- This will appear in the admin console once forensics license is applied to the QRadar Console

Forensics



Setup Incident Forensics



Server Management



Case Management



User Assignment



Schedule Actions

Hands on

Hands on