

BusinessConnect and SolutionsConnect

It's time to make bold moves.

Next generation security analytics

Vijay Dheap

Global Product Manager - IBM Master Inventor

Big Data Security Intelligence & Mobile Security

IBM Security Solutions



Please Note:

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.

Today's challenges

Escalating Attacks

Designer Malware



Spear Phishing



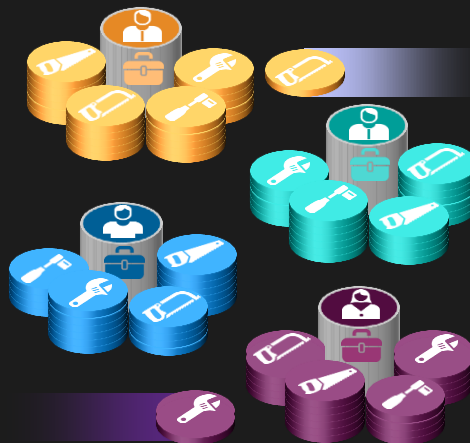
Persistence



Backdoors



Increasing Complexity



Resource Constraints



ITSecurityJobs.com

Sorry, no applicants found

We are in an era of continuous breaches

Operational Sophistication
 IBM X-Force® declared
Year of the Security Breach

Near Daily Leaks of Sensitive Data

40% increase
 in reported data breaches and incidents

Relentless Use of Multiple Methods

500,000,000+ records
 were leaked, while the future shows no sign of change



2011

2012

2013

Attack types

- SQL injection
- Spear phishing
- DDoS
- Third-party software
- Physical access
- Malware
- XSS
- Watering hole
- Undisclosed

Challenges compounded by volume of data/transactions/issues



200,000+ Facebook, Twitter, Linked-in 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 and phishing emails a week



External network scanned 10 times a day



100,000+ vulnerabilities in the network



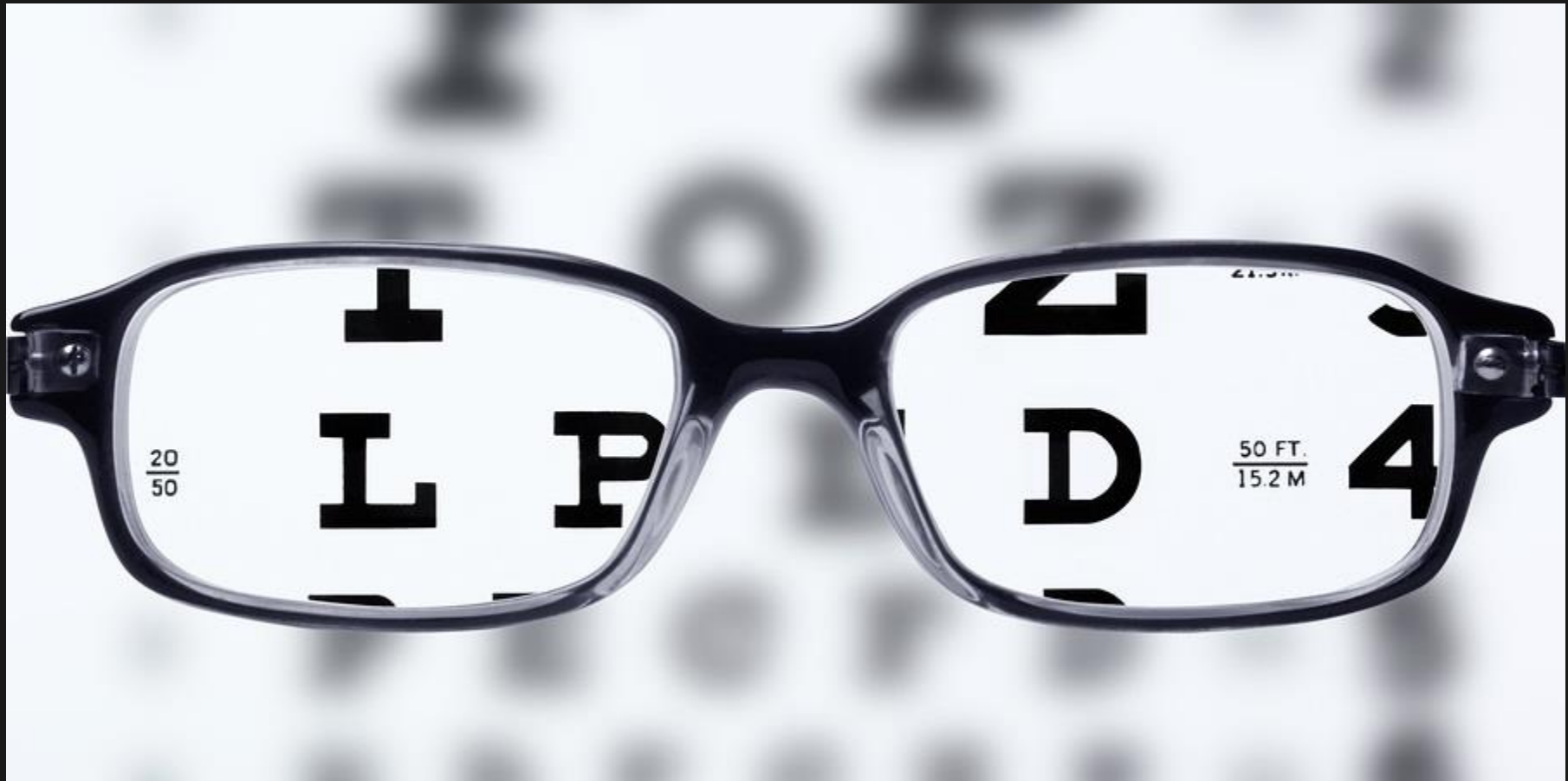
5 network alerts per minute



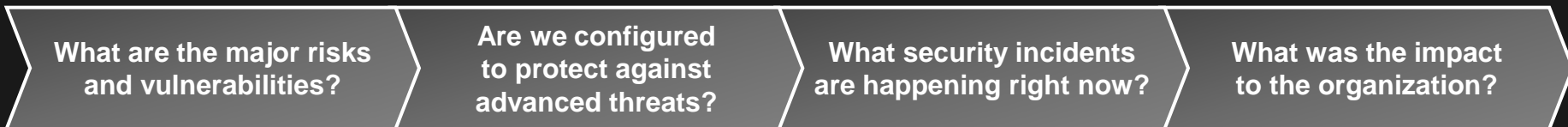
100+ potentially malicious web site visits per day



20 Network configuration changes a week



Security Intelligence is asking the right questions, and getting answers



Vulnerability

Pre-Exploit

Exploit

Post-Exploit

Remediation



PREDICTION / PREVENTION PHASE

REACTION / REMEDIATION PHASE

- Gain visibility over gaps
- Detect deviations
- Prioritize vulnerabilities

- Automatically detect threats
- Gather situational awareness
- Quickly investigate incidents

IBM's solution for Security Intelligence



INTELLIGENT

Correlation, analysis and massive data reduction



IBM QRadar
Security Intelligence
Platform



AUTOMATED

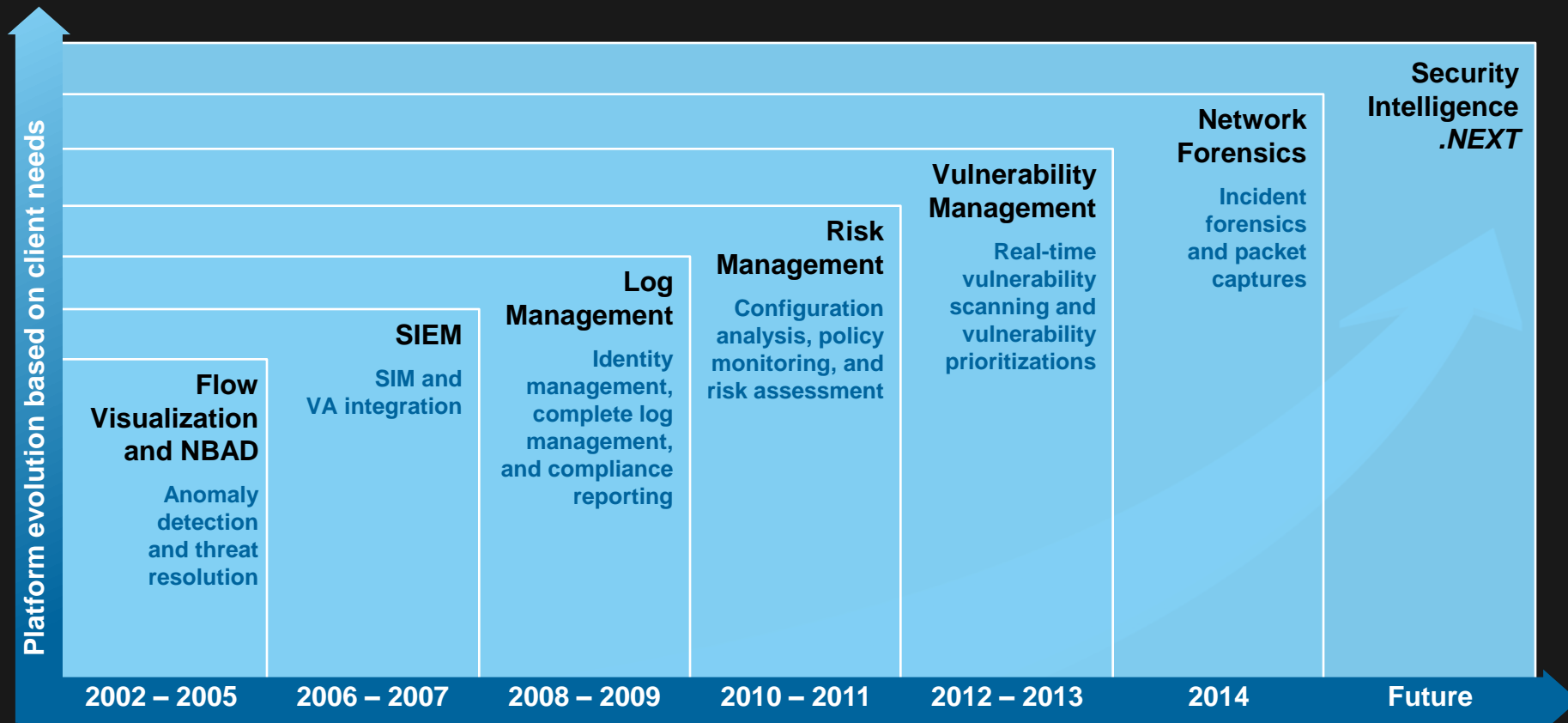
Driving simplicity and accelerating time-to-value



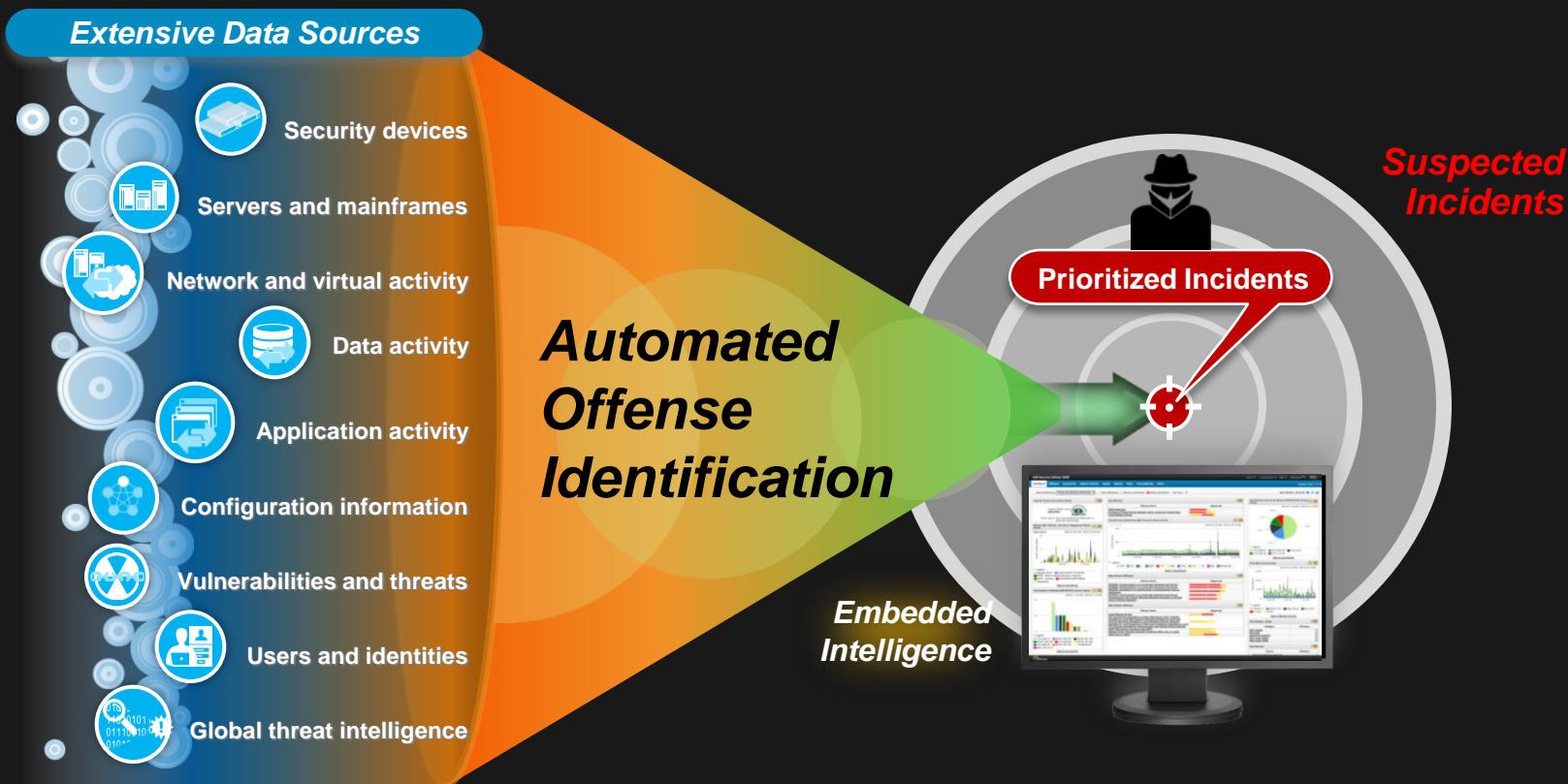
INTEGRATED

Unified architecture delivered in a single console

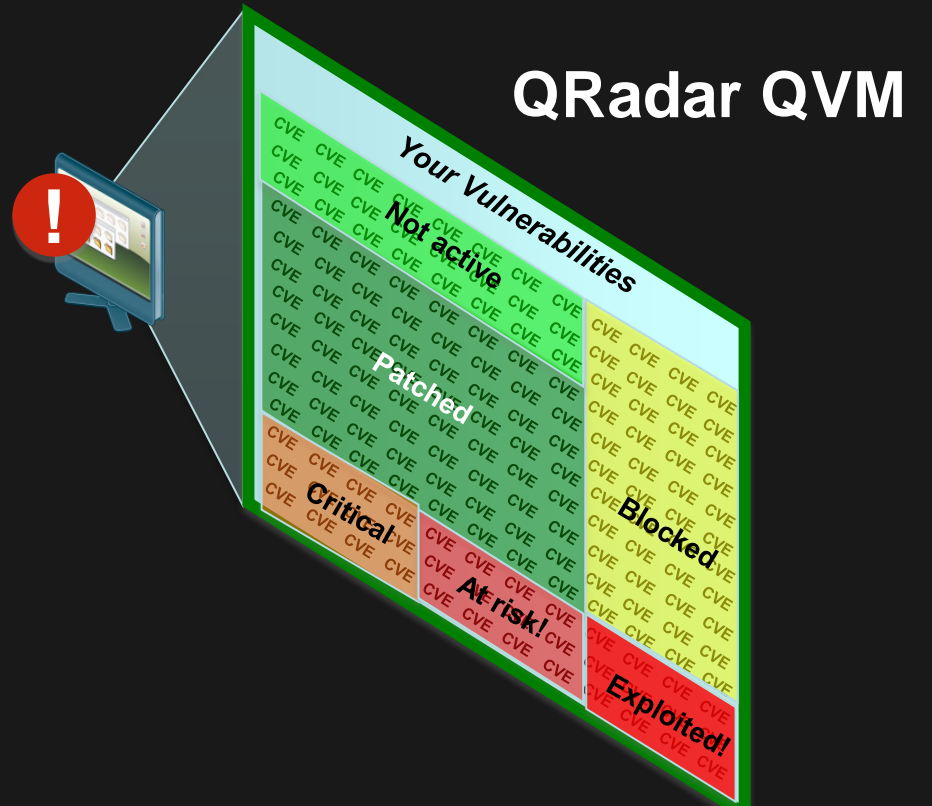
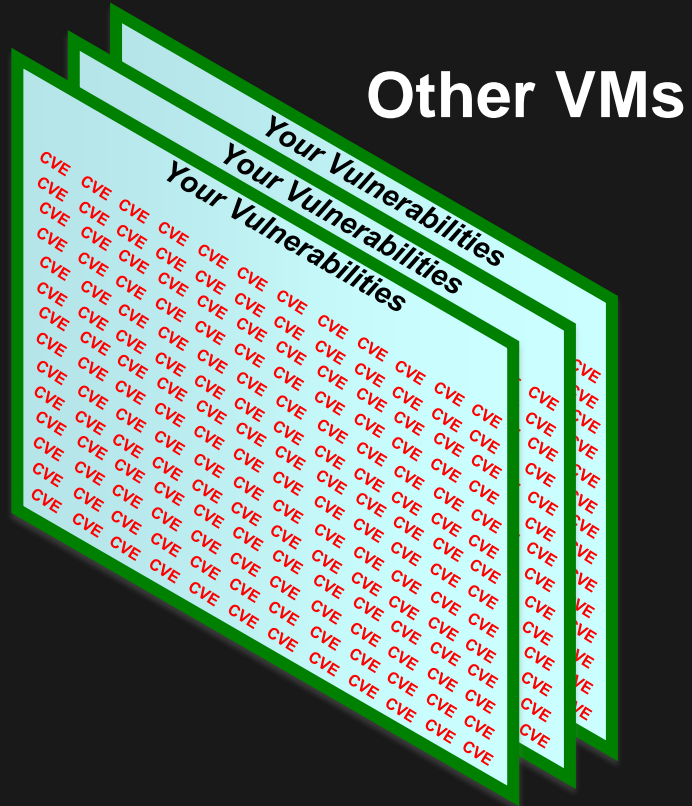
Evolving IBM Security Intelligence strategy based on client needs



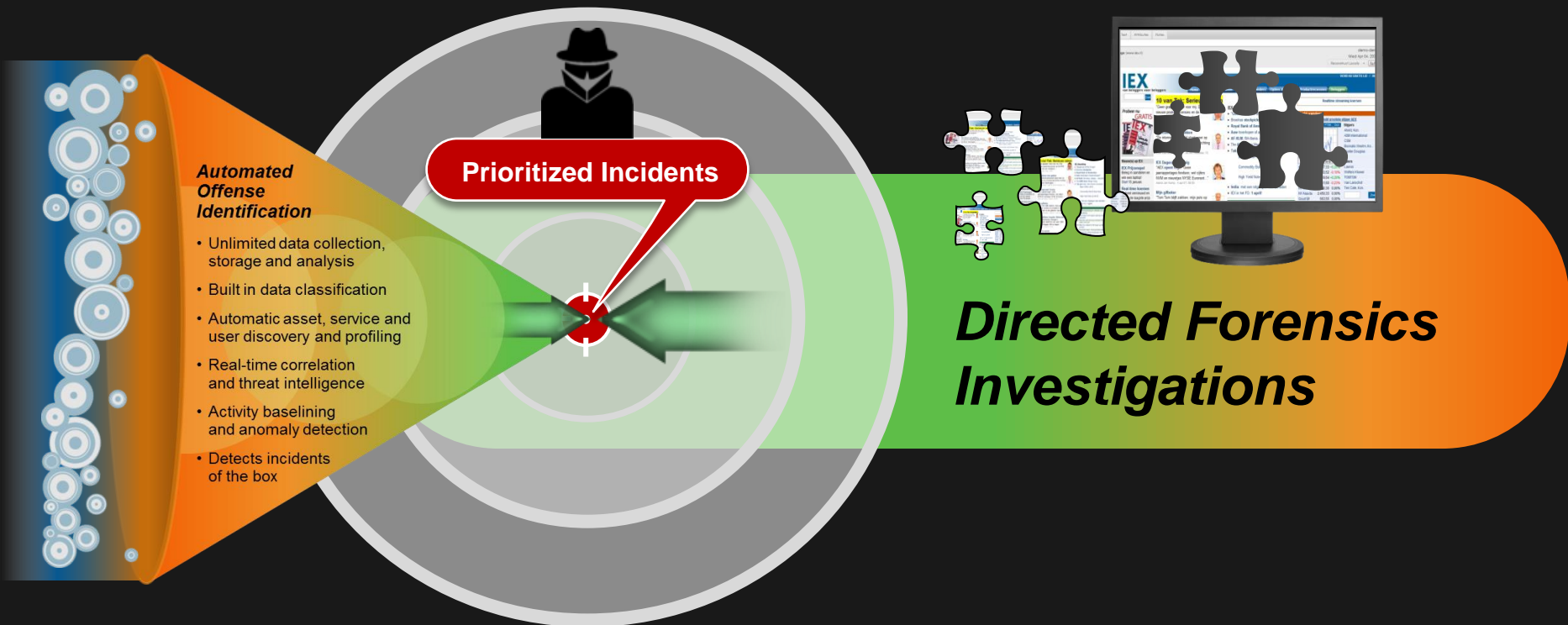
Embedded intelligence offers automated offense identification



Strengthened by integrated vulnerability insights



And giving high-fidelity evidence beyond just detecting an incident



An integrated, unified architecture in a single web-based console

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

IBM Security QRadar SIEM
admin | Preferences | Help | Messages 6 | IBM

Dashboard | Offenses | Log Activity | Network Activity | Assets | Forensics | Reports | Risks | Vulnerabilities | Admin
System Time: 6:21 AM

Show Dashboard: Threat and Security Monitoring | New Dashboard | Rename Dashboard | Delete Dashboard | Add Item...

Refresh Paused: 00:01:00

Vulnerability Count / Risk

Legend

- Medium
- High
- Low
- Warning
- Unknown

My Offenses

Offense Name	Magnitude
DDOS Detected	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>
OS Attack: MS SMB2 Validate Provider Callback CVE-2009-3103	<div style="width: 80%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>
Risk: assess devices (i.e. firewalls) that allow banned protocols from the Internet	<div style="width: 60%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>
XForce: Communication to a known Bot Command and Control containing Web.HTTPWeb	<div style="width: 40%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>
XForce: Connection to a known Malware site is detected	<div style="width: 20%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></div>

Top Category Types

Category	Offenses
Firewall_Permit	72
Potential Botnet Connection	59
Misc_Exploit	45
ACL_Deny	26
Web_Exploit	23

Top Systems Attacked (Event Count)

Reset Zoom | 21/10/2013 04:17 - 21/10/2013 10:17

Legend

- 0
- 80

[View in Log Activity](#)

Flow Bias (Total Bytes)

10/21/13 12:21 AM - 10/21/13 6:21 AM

Legend

- Mostly In
- Mostly Out
- Near Same
- Other
- Out Only
- In Only

[View in Network Activity](#)

Top Sources

Source	Offenses
10.0.110.239	15

Answering questions to help prevent and remediate attacks

Offense 907
Summary Display ▾ | Events | Connections | Flows | View Attack Path | Actions ▾ | Print | ?

Magnitude	What was the attack?	Status	Relevance	8	Severity	5	Is the attack credible?
Description	Potential Data Loss	Offense Type	Source IP				
Source IP(s)	10.0.110.221 (dhcp-221-users-2.acme.com)	Event/Flow 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				
		Assigned to	admin				

Offense Source Summary

IP	10.0.110.221	Location	Users.Users-2
Magnitude	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange);"></div>	Vulnerabilities	0
Username	compliance	MAC Address	00:0E:0C:B4:D8:EE
Host Name	dhcp-221-users-2.acme.com	Weight	0
Asset Name	dhcp-221-users-2.acme.com	Events/Flows	15,310
Offenses	8		

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

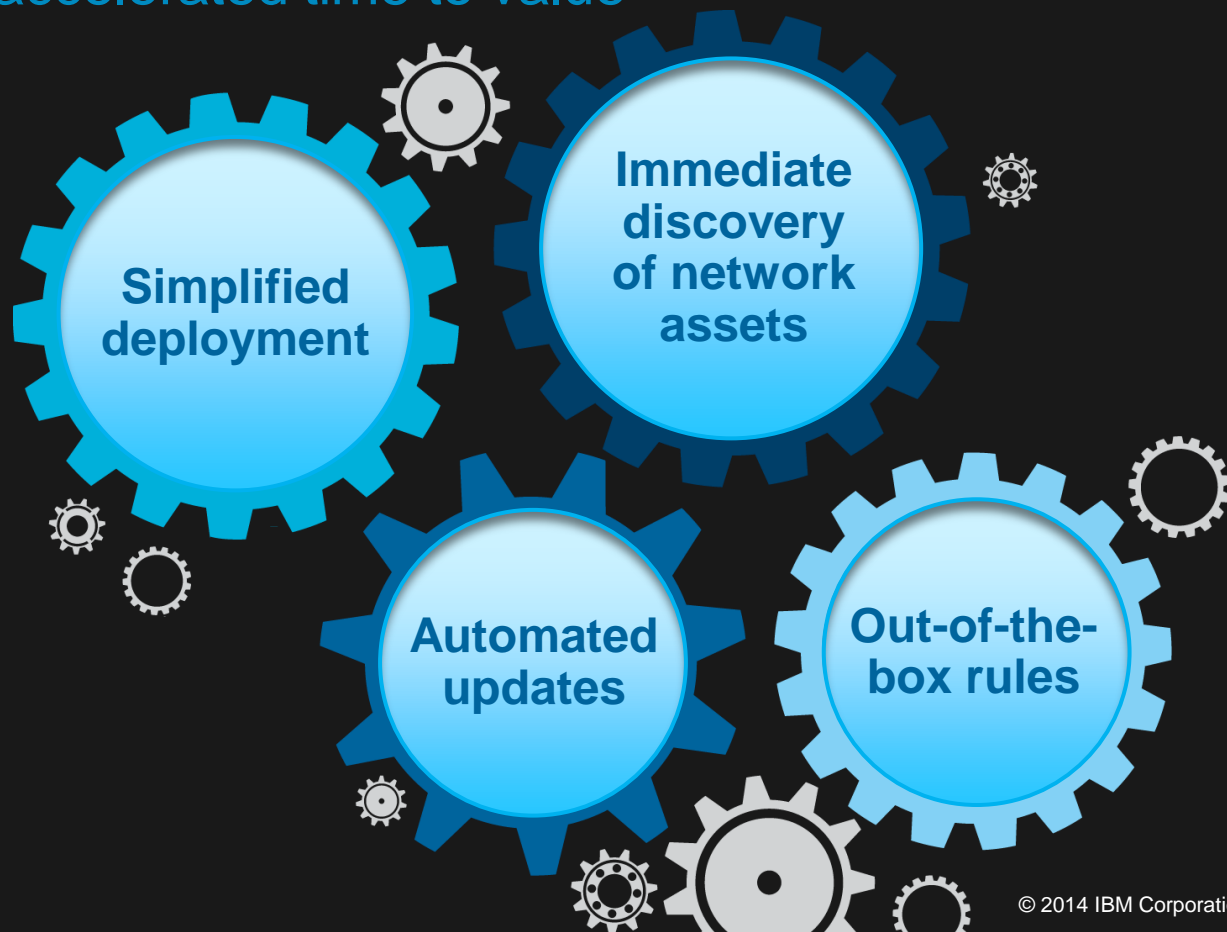
Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	Weight	Offenses	Detected	Resources
dhc...	<div style="width: 100%; height: 10px; background: linear-gradient(to right, yellow, orange);"></div>	Users.Users-2	No	8	21	0s	15,310

Driving simplicity and accelerated time to value

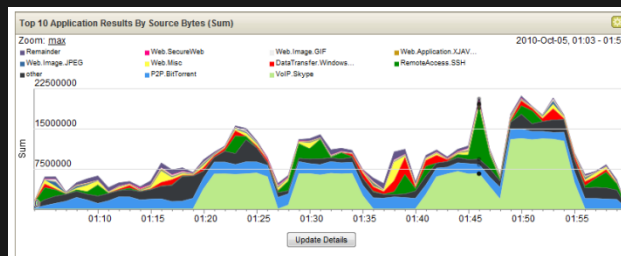
IBM QRadar is nearly three times faster to implement across the enterprise than other SIEM solutions.

2014 Ponemon Institute
Independent Research



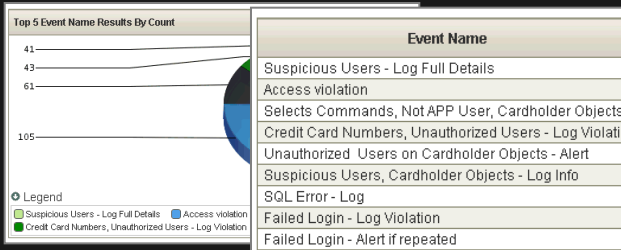
Differentiated by deep network and user activity analytics

Behavior monitoring and flow analytics



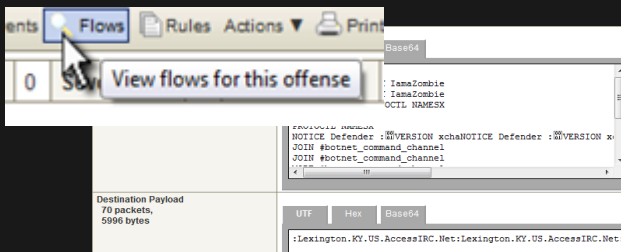
Network Traffic Doesn't Lie

Activity and data access monitoring



Improved Breach Detection

Stealthy malware detection



Irrefutable Botnet Communication

Intuitive data exploration and navigation reduces impact

Survey: 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

ID	Date	Protocol	Description	Priority
1	2007/04/04 00:24:14 PM	SMTP	Email Message	3
2	2007/04/04 00:24:14 PM	SMTP	Email Message	1
3	2007/04/04 00:24:14 PM	SMTP	Email Message	1
4	2007/04/04 00:24:14 PM	SMTP	Email Message	1
5	2007/04/04 00:24:14 PM	SMTP	Email Message	1
6	2007/04/04 00:24:14 PM	SMTP	Email Message	1
7	2007/04/04 00:24:14 PM	SMTP	Email Message	1
8	2007/04/04 00:24:14 PM	SMTP	Email Message	1
9	2007/04/04 00:24:14 PM	SMTP	Email Message	1
10	2007/04/04 00:24:14 PM	SMTP	Email Message	1
11	2007/04/04 00:24:14 PM	SMTP	Email Message	1
12	2007/04/04 00:24:14 PM	SMTP	Email Message	1
13	2007/04/04 00:24:14 PM	SMTP	Email Message	1
14	2007/04/04 00:24:14 PM	SMTP	Email Message	1
15	2007/04/04 00:24:14 PM	SMTP	Email Message	1
16	2007/04/04 00:24:14 PM	SMTP	Email Message	1
17	2007/04/04 00:24:14 PM	SMTP	Email Message	1
18	2007/04/04 00:24:14 PM	SMTP	Email Message	1
19	2007/04/04 00:24:14 PM	SMTP	Email Message	1
20	2007/04/04 00:24:14 PM	SMTP	Email Message	1
21	2007/04/04 00:24:14 PM	SMTP	Email Message	1
22	2007/04/04 00:24:14 PM	SMTP	Email Message	1
23	2007/04/04 00:24:14 PM	SMTP	Email Message	1
24	2007/04/04 00:24:14 PM	SMTP	Email Message	1
25	2007/04/04 00:24:14 PM	SMTP	Email Message	1
26	2007/04/04 00:24:14 PM	SMTP	Email Message	1
27	2007/04/04 00:24:14 PM	SMTP	Email Message	1
28	2007/04/04 00:24:14 PM	SMTP	Email Message	1
29	2007/04/04 00:24:14 PM	SMTP	Email Message	1
30	2007/04/04 00:24:14 PM	SMTP	Email Message	1
31	2007/04/04 00:24:14 PM	SMTP	Email Message	1
32	2007/04/04 00:24:14 PM	SMTP	Email Message	1
33	2007/04/04 00:24:14 PM	SMTP	Email Message	1
34	2007/04/04 00:24:14 PM	SMTP	Email Message	1
35	2007/04/04 00:24:14 PM	SMTP	Email Message	1
36	2007/04/04 00:24:14 PM	SMTP	Email Message	1
37	2007/04/04 00:24:14 PM	SMTP	Email Message	1
38	2007/04/04 00:24:14 PM	SMTP	Email Message	1
39	2007/04/04 00:24:14 PM	SMTP	Email Message	1
40	2007/04/04 00:24:14 PM	SMTP	Email Message	1
41	2007/04/04 00:24:14 PM	SMTP	Email Message	1
42	2007/04/04 00:24:14 PM	SMTP	Email Message	1
43	2007/04/04 00:24:14 PM	SMTP	Email Message	1
44	2007/04/04 00:24:14 PM	SMTP	Email Message	1
45	2007/04/04 00:24:14 PM	SMTP	Email Message	1
46	2007/04/04 00:24:14 PM	SMTP	Email Message	1
47	2007/04/04 00:24:14 PM	SMTP	Email Message	1
48	2007/04/04 00:24:14 PM	SMTP	Email Message	1
49	2007/04/04 00:24:14 PM	SMTP	Email Message	1
50	2007/04/04 00:24:14 PM	SMTP	Email Message	1
51	2007/04/04 00:24:14 PM	SMTP	Email Message	1
52	2007/04/04 00:24:14 PM	SMTP	Email Message	1
53	2007/04/04 00:24:14 PM	SMTP	Email Message	1
54	2007/04/04 00:24:14 PM	SMTP	Email Message	1
55	2007/04/04 00:24:14 PM	SMTP	Email Message	1
56	2007/04/04 00:24:14 PM	SMTP	Email Message	1
57	2007/04/04 00:24:14 PM	SMTP	Email Message	1
58	2007/04/04 00:24:14 PM	SMTP	Email Message	1
59	2007/04/04 00:24:14 PM	SMTP	Email Message	1
60	2007/04/04 00:24:14 PM	SMTP	Email Message	1

View | Text | Attributes | Notes

MSN File Transfer

GeneralDemo-demo5.pcap-000c29cbe49a-20070404 Wed Apr 04 2007

- 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: 21d28e2c05d8a25305340d561a802258366f629dbd3556e71c5bd3d0083fb2

Filename: details.doc

Filepath: /var/www/html/files/GeneralDemo/demo5.pcap/msn/2007/04/04/13.49/33/791/details.doc

Author: bert

Comments:

Content-Leng:

Content-Type: text/html

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

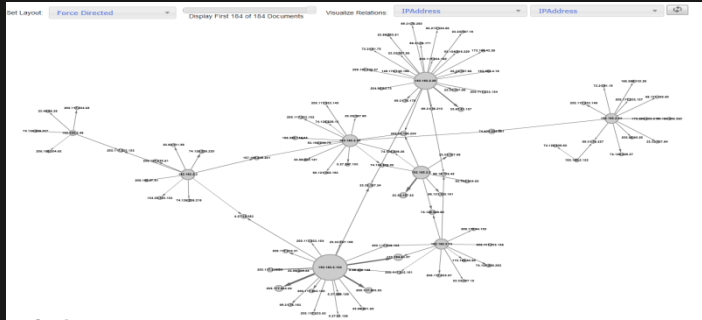
Keywords:

FileMetadata

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

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

Revision-Number: 1



Client example: An international energy company reduces billions of events per day to find those that should be investigated

An international energy firm analyzes

2 billion

events per day to find

20-25

potential offenses to investigate



Business challenge

- Reducing huge number of events to find the ones that need to be investigated
- Automating the process of analyzing security data

Solutions (QRadar SIEM, QFlow, Risk Manager)

Combined analysis of historical data with real-time alerts to gain a ‘big picture’ view and uncover patterns of unusual activity humans miss and immediately block suspected traffic

Client example: A financial information provider hardens defenses against threats and fraud

financial information provider tracks

250 activity baselines

and saved

50-80%

on staffing versus alternative solutions



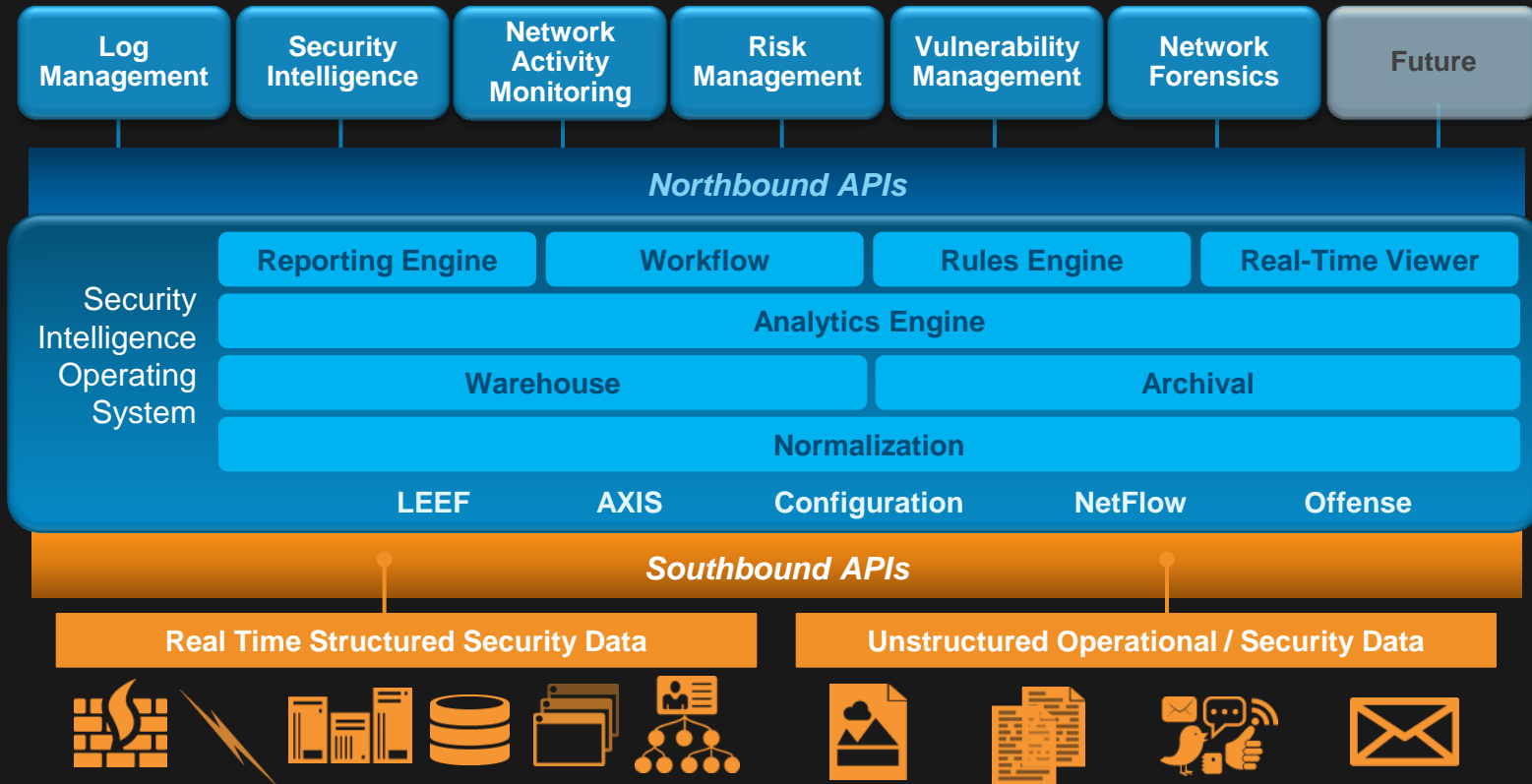
Business challenge

- Detect wide range of security threats affecting public-facing Web applications
- Help identify subtle changes in user behavior that could indicate fraud or misuse

Solutions (QRadar SIEM, QFlow, X-Force, Network IPS)

Combine analysis of historical data with real-time alerts to gain a ‘big picture’ view and uncover patterns of unusual activity humans miss and immediately block suspected traffic

Delivering intelligence through a purpose-built, extensible platform



Consolidation and integration help reduce costs and increase visibility



Traditional SIEM
6 products from 6 vendors are needed



IBM Security Intelligence and Analytics

<i>Flows</i>	Arbor Networks	Lancope	Riverbed Technology		
<i>Packets</i>	RSA	Solera Networks			
<i>Vulnerabilities</i>	Qualys	Rapid 7	Tenable Network Security		
<i>Configurations</i>	AlgoSec	FireMon	Skybox Security	Tufin	RedSeal Networks
<i>Logs</i>	LogLogic	Splunk			
<i>Events</i>	HP ArcSight	McAfee	RSA		



IBM QRadar
 Security Intelligence Platform

An integrated, unified architecture in a single web-based console

Intelligence, integration, automation to stay ahead of the threat

Identify and quickly remediate

Deploy comprehensive security intelligence and incident forensics

Address regulation mandates

Automate data collection and configuration audits

Consolidate data silos

Collect, correlate and report on data in one integrated solution

Detect insider fraud

Adopt next-generation SIEM with identity correlation

Better predict risk

Engage entire lifecycle of risk management for network and security infrastructures

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.