

BusinessConnect and SolutionsConnect

It's time to make bold moves.

Next generation security analytics

Jason Corbin -

Director - Security Intelligence Strategy and Product Management

IBM Security Systems



We are in an era of continuous breaches

Operational
Sophistication

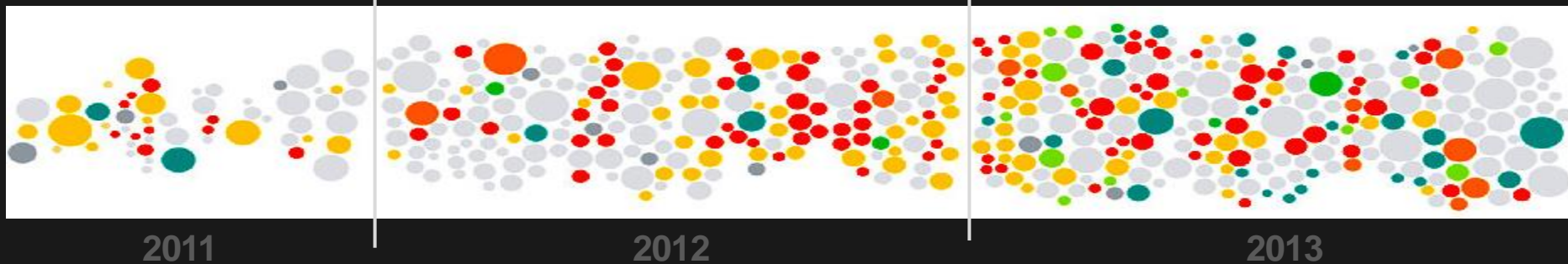
IBM X-Force® declared
**Year of the
Security Breach**

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


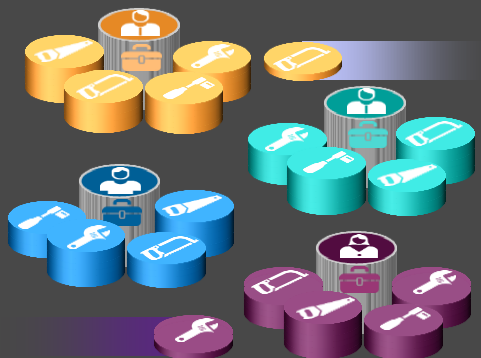
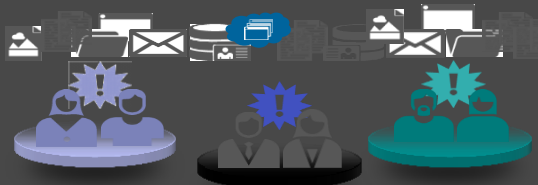


Watering
hole



Undisclosed

Today's challenges

Escalating Attacks	Increasing Complexity	Resource Constraints
<p><i>Designer Malware</i></p> <p><i>Spear Phishing</i></p> <p><i>Persistence</i></p> <p><i>Backdoors</i></p>  <ul style="list-style-type: none"> Increasingly sophisticated attack methods Disappearing perimeters Accelerating security breaches 	 <ul style="list-style-type: none"> Constantly changing infrastructure Too many products from multiple vendors; costly to configure and manage Inadequate and ineffective tools 	 <p>ITSecurityJobs.com</p> <p>Sorry, no applicants found</p> <ul style="list-style-type: none"> Struggling security teams Too much data with limited manpower and skills to manage it all Managing and monitoring increasing compliance demands

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

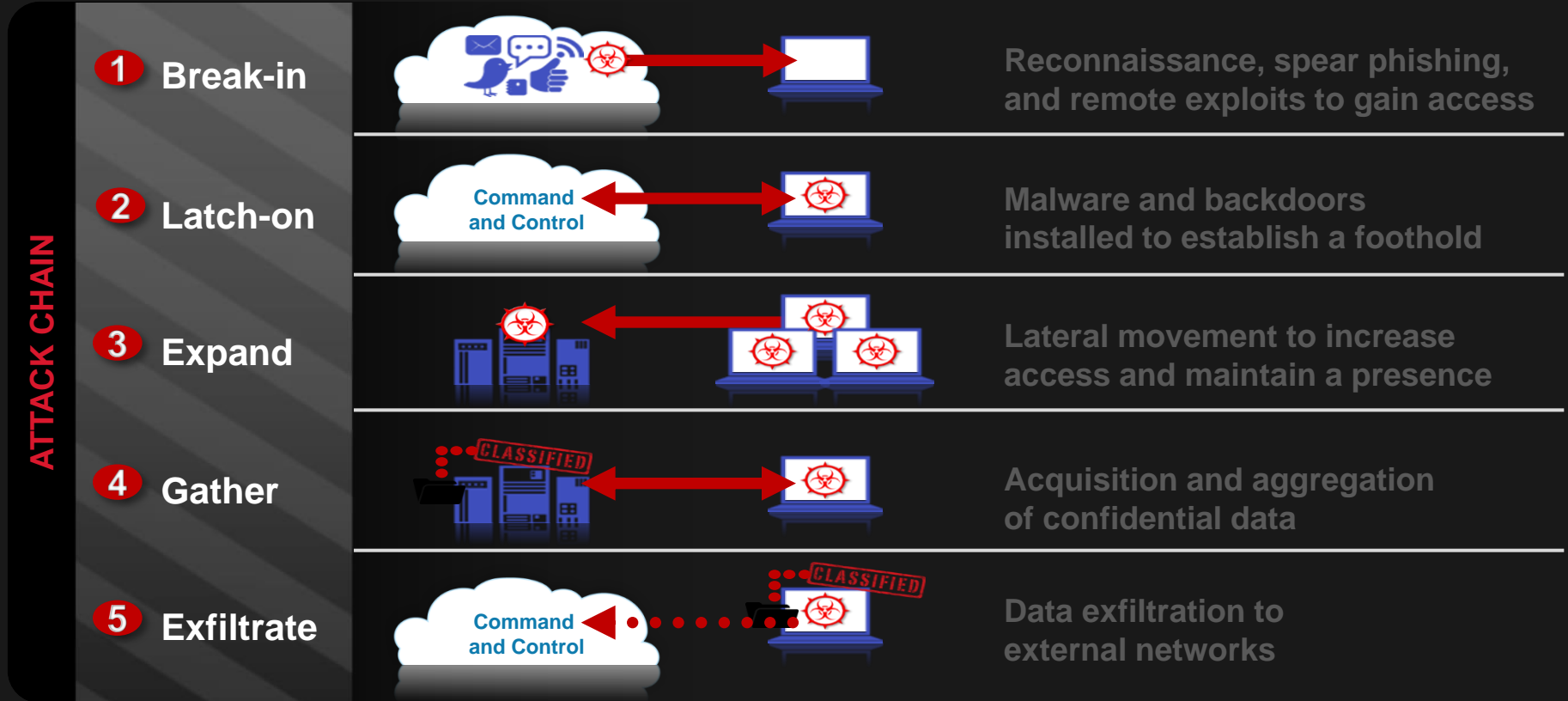


100+ potentially malicious web site visits per day

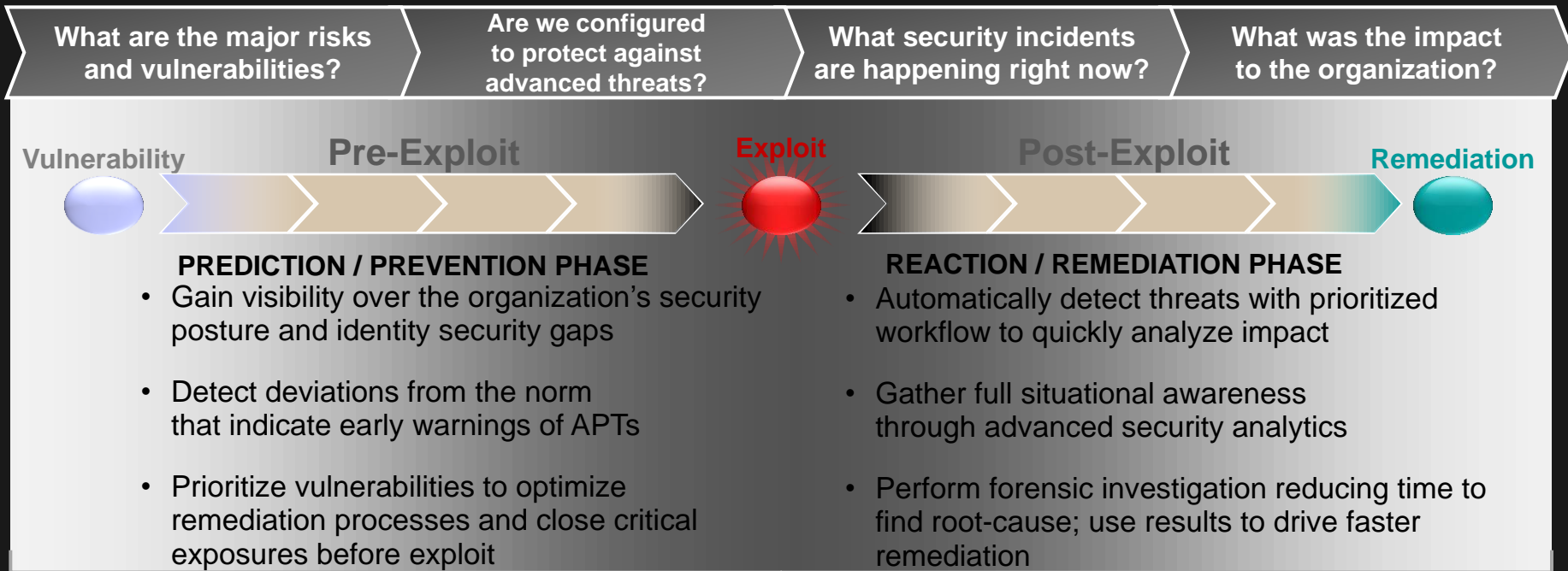


20 Network configuration changes a week

Advanced attackers follow a five-stage attack chain



Ask the right questions



Security Intelligence

The actionable information derived from the analysis of security-relevant data available to an organization

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



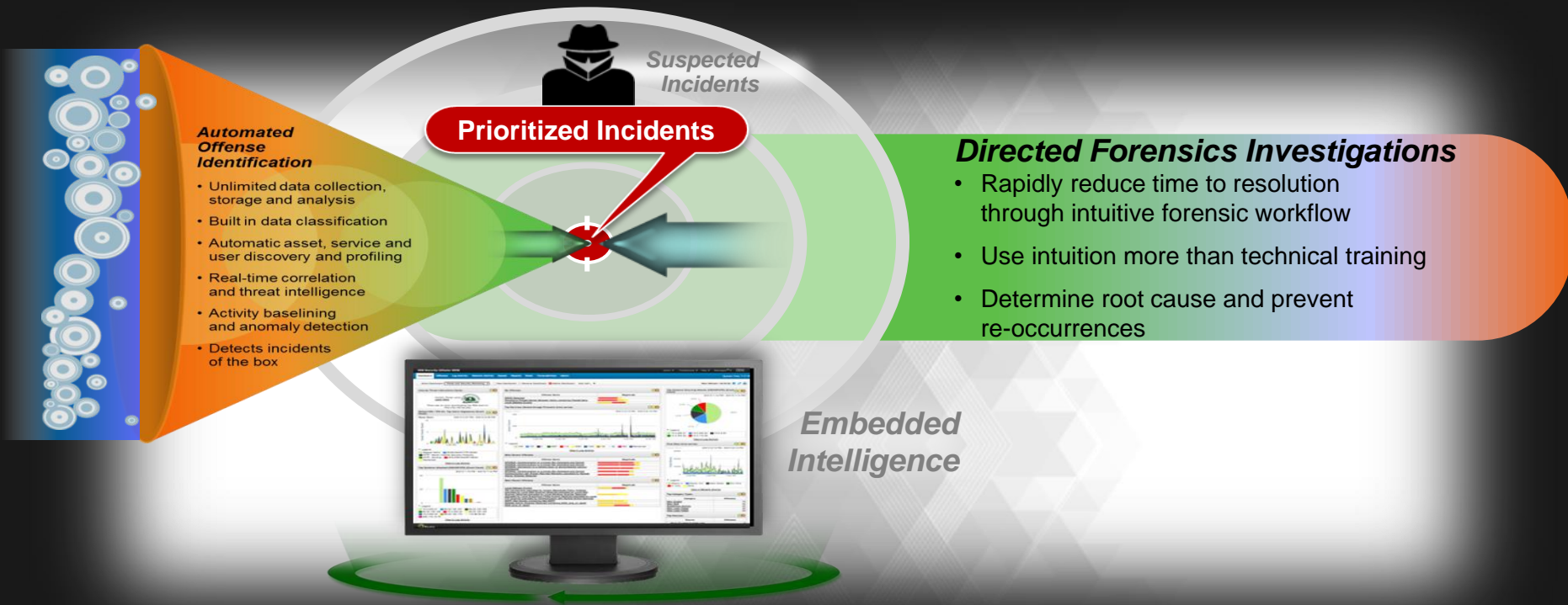
Suspected Incidents

Prioritized Incidents





Security Intelligence goes beyond detecting an incident: Extend clarity around incidents with in-depth forensics data





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	<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						
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: 90%; height: 10px; background: linear-gradient(to right, yellow, orange, red);"></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 Add Note

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

Forensics Reconstructions

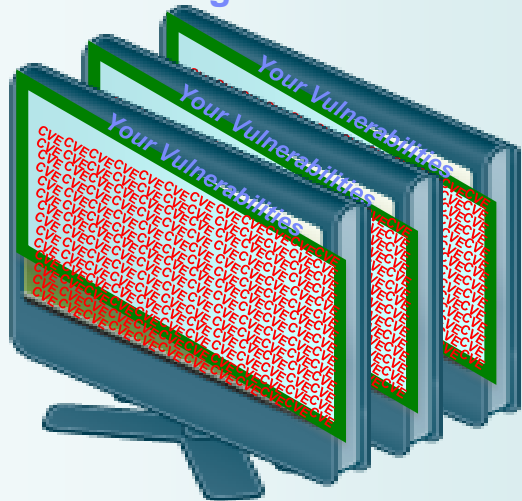
Case	Collection	IP	Start	End	Status
DataLoss	DataLoss	10.0.110.221	3/27/2014 3:31:00 PM	3/27/2014 4:31:00 PM	SUCCESS

Top 5 Source IPs Sources

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
dhc...	<div style="width: 75%; height: 10px; background: linear-gradient(to right, red, orange, yellow);"></div>	Users.Users-2	No	compliance	00:0E:0C:B4:D8:EE	0	8	21	0s	15,310

Strengthened by integrated vulnerability insights

Existing vulnerability management tools



Security Intelligence Integration

- Improves visibility
 - Intelligent, event-driven scanning, asset discovery, asset profiling and more
- Reduces data load
 - Bringing rich context to Vulnerability Management
- Breaks down silos
 - Leveraging all QRadar integrations and data
 - Unified vulnerability view across all products

QRadar Vulnerability Manager

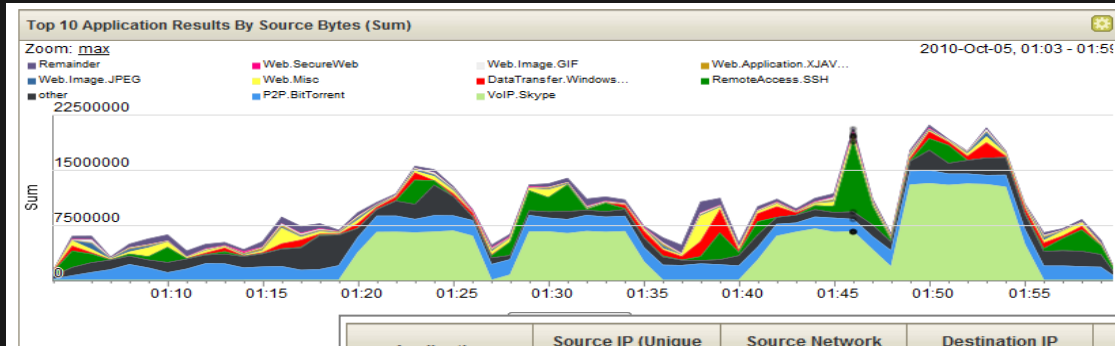


Answers delivered:

- Real-time scanning
- Early warning capabilities
- Advanced pivoting and filtering

Differentiated by Deep network activity analytics

- Network traffic doesn't lie. Attackers can stop logging and erase their tracks, but can't cut off the network (flow data)
 - Deep packet inspection for Layer 7 flow data
 - Pivoting, drill-down and data mining on flow sources for advanced detection and forensics
- Helps detect anomalies that might otherwise get missed



Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267

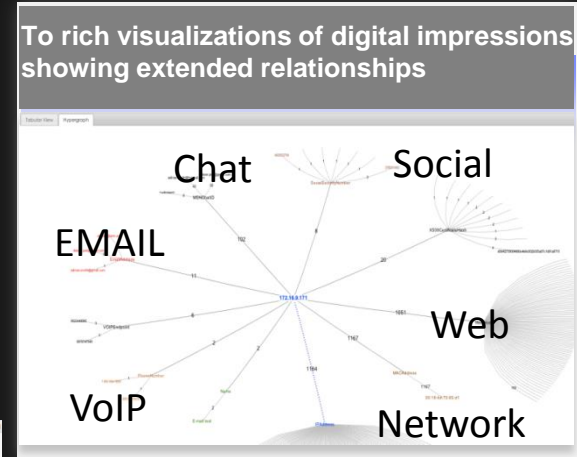
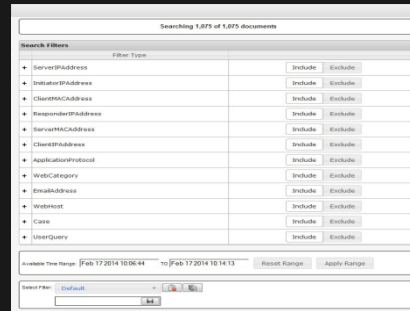
Clarity Through Forensics

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

Intuitive Data Exploration and Navigation Reduces Impact

Empower security analysts to operate like seasoned forensics specialists by offering capabilities that can be powered by intuition and logical deduction

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

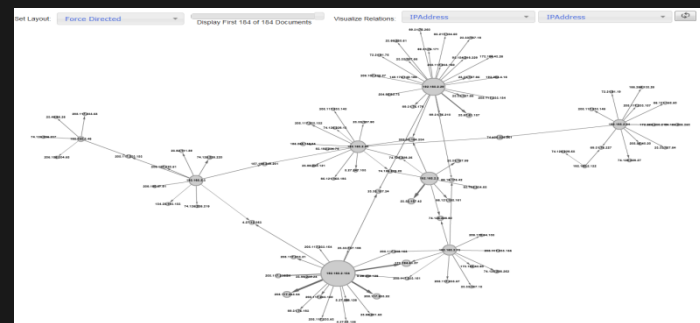
ID	Name	Type	Score
1	20070404-00-24-14.PDF	PDF	1
2	20070404-00-24-14.PDF	PDF	1
3	20070404-00-24-14.PDF	PDF	1
4	20070404-00-24-14.PDF	PDF	1
5	20070404-00-24-14.PDF	PDF	1
6	20070404-00-24-14.PDF	PDF	1
7	20070404-00-24-14.PDF	PDF	1
8	20070404-00-24-14.PDF	PDF	1
9	20070404-00-24-14.PDF	PDF	1
10	20070404-00-24-14.PDF	PDF	1
11	20070404-00-24-14.PDF	PDF	1
12	20070404-00-24-14.PDF	PDF	1
13	20070404-00-24-14.PDF	PDF	1
14	20070404-00-24-14.PDF	PDF	1
15	20070404-00-24-14.PDF	PDF	1
16	20070404-00-24-14.PDF	PDF	1
17	20070404-00-24-14.PDF	PDF	1
18	20070404-00-24-14.PDF	PDF	1
19	20070404-00-24-14.PDF	PDF	1
20	20070404-00-24-14.PDF	PDF	1
21	20070404-00-24-14.PDF	PDF	1
22	20070404-00-24-14.PDF	PDF	1
23	20070404-00-24-14.PDF	PDF	1
24	20070404-00-24-14.PDF	PDF	1
25	20070404-00-24-14.PDF	PDF	1
26	20070404-00-24-14.PDF	PDF	1
27	20070404-00-24-14.PDF	PDF	1
28	20070404-00-24-14.PDF	PDF	1
29	20070404-00-24-14.PDF	PDF	1
30	20070404-00-24-14.PDF	PDF	1

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 21d28e2c05d8a25305340d561a8022258366f629dbd3556e71c5bd3d083fbf2
 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
 Creation-Date: 2007-04-04 13:52:00
 FileMetadata
 Last-Printed: 1601-01-01T00:06:31Z
 Last-Save-Date: 1601-01-01T00:06:31Z
 Revision-Number: 1



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 System Time: 6:21 AM

Dashboard Offenses Log Activity Network Activity Assets Forensics Reports Risks Vulnerabilities Admin

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

All Vulnerability Count / Risk

Legend: ■ Medium ■ High ■ Low ■ Warning ■ Unknown

Top Systems Attacked (Event Count)

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

Legend: ■ 0 ■ 80

My Offenses

Offense Name	Magnitude
DDOS Detected	[Progress bar]
OS Attack: MS_SMB2 Validate Provider_Callback CVE-2009-3103	[Progress bar]
Risk: assess devices (i.e. firewalls) that allow banned protocols from the Internet	[Progress bar]
XForce: Communication to a known Bot Command and Control containing Web HTTPWeb	[Progress bar]
XForce: Connection to a known Malware site is detected	[Progress bar]

Top Services Denied through Firewalls (Event Count)

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

Legend: ■ 0 ■ 80

[View in Log Activity](#)

Top Category Types

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

Flow Bias (Total Bytes)

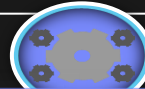
10/21/13 12:21 AM - 10/21/13 6:21 AM

Legend: ■ Mostly In ■ Mostly Out ■ Near Same ■ Other

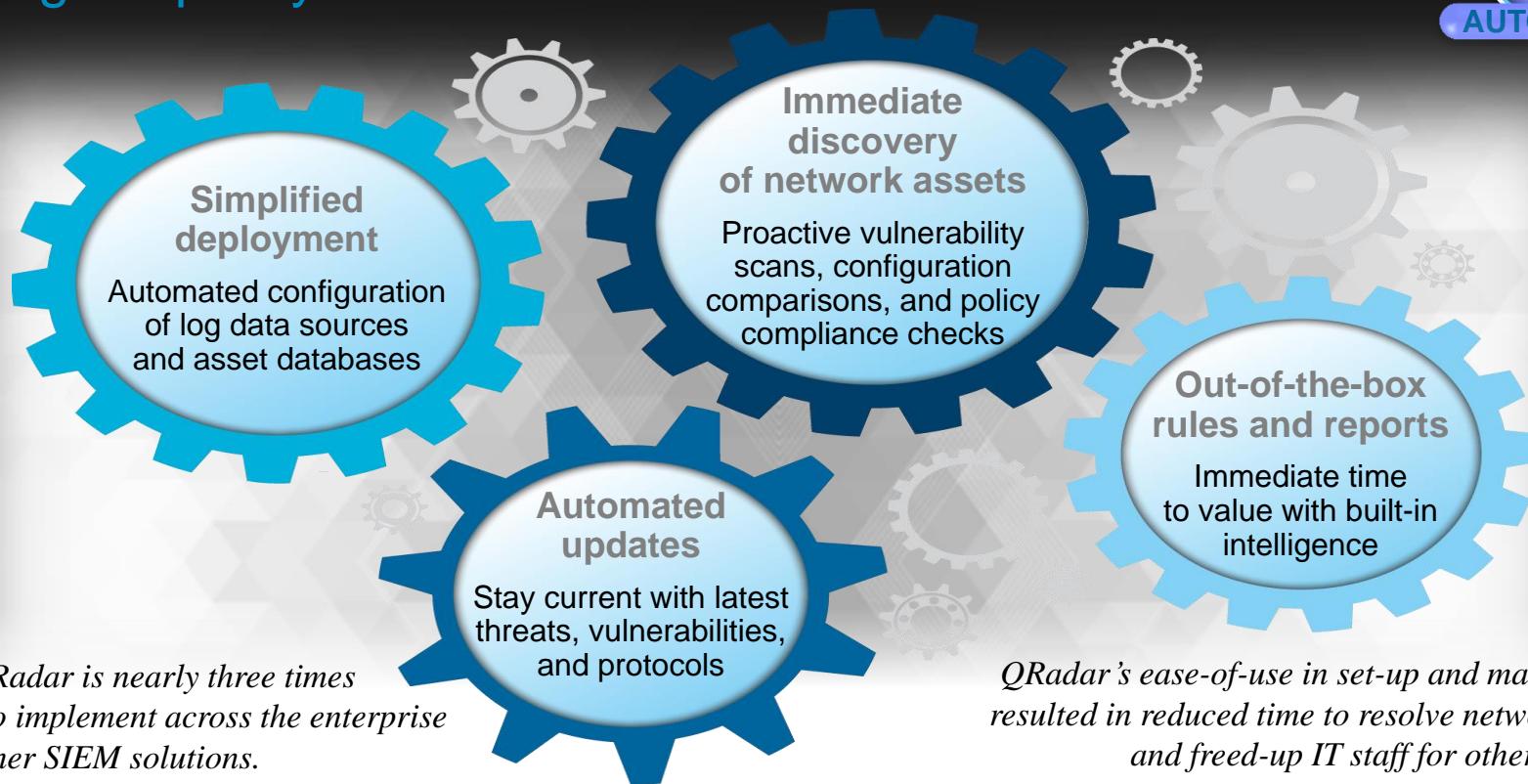
[View in Network Activity](#)

Top Sources

Source	Offenses
10.0.110.239	15



Driving simplicity and accelerated time to value



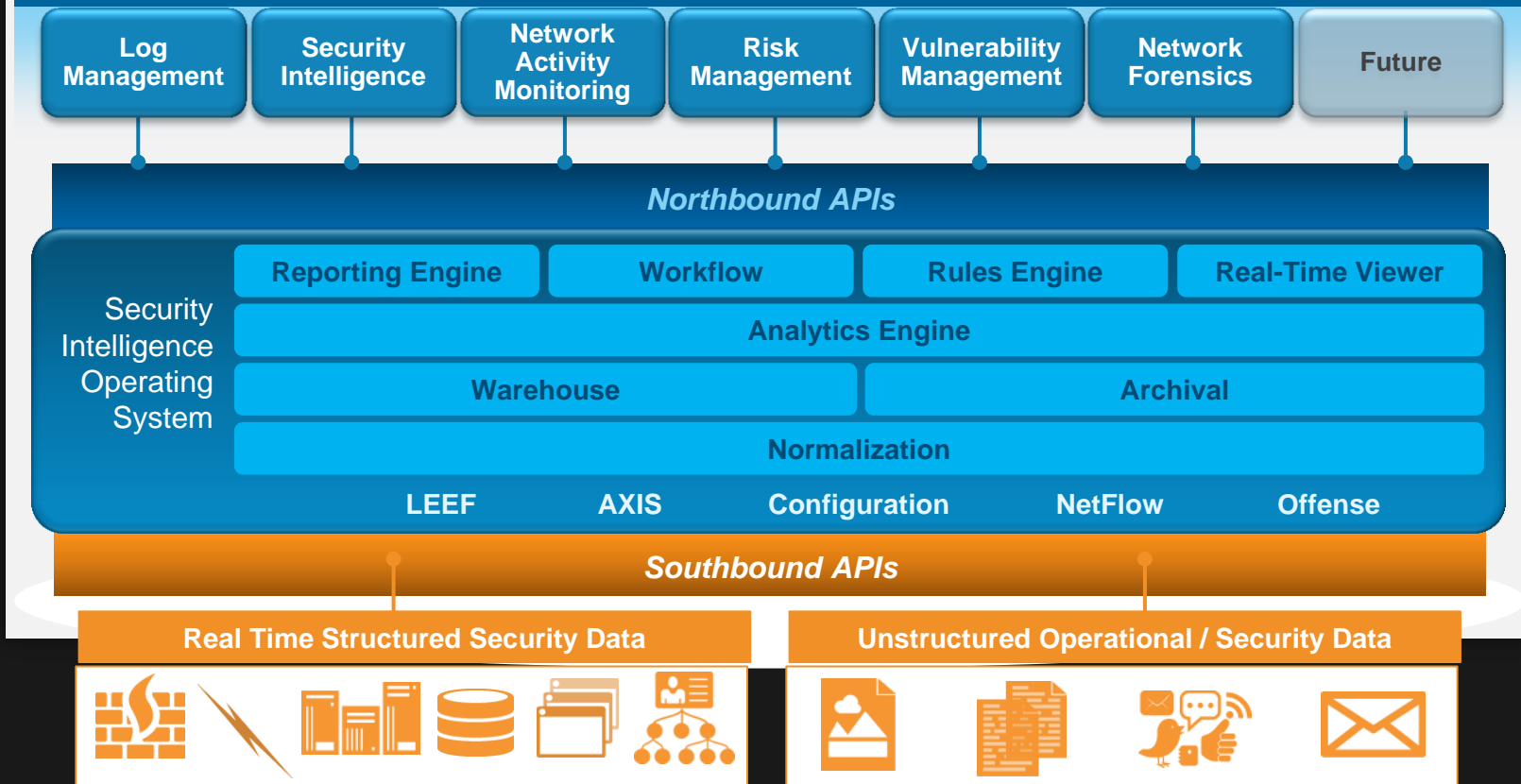
IBM QRadar is nearly three times faster to implement across the enterprise than other SIEM solutions.

2014 Ponemon Institute, LLC
Independent Research Report

QRadar's ease-of-use in set-up and maintenance resulted in reduced time to resolve network issues and freed-up IT staff for other projects.

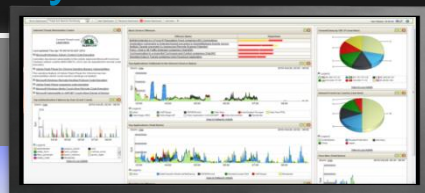
Private U.S. University
with large online education community

IBM QRadar Security Intelligence Platform



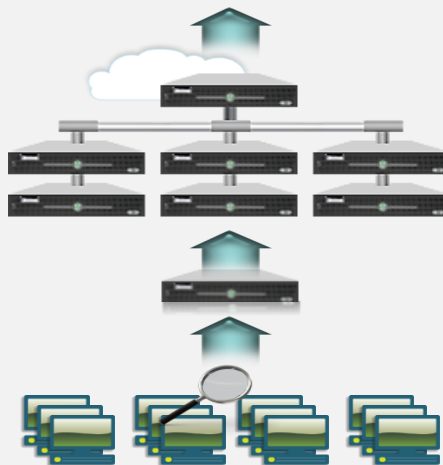
Optimized appliance and software architecture for high performance and rapid deployment in any environment

IBM QRadar Security Intelligence Platform



Scalable appliance architecture

- Easy-to-deploy, scalable model using stackable distributed appliances
- Does not require third-party databases or storage



Shared modular infrastructure

- Offers automatic failover and disaster recovery
- Virtual deployments well suited for cloud environments

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

Detect insider fraud

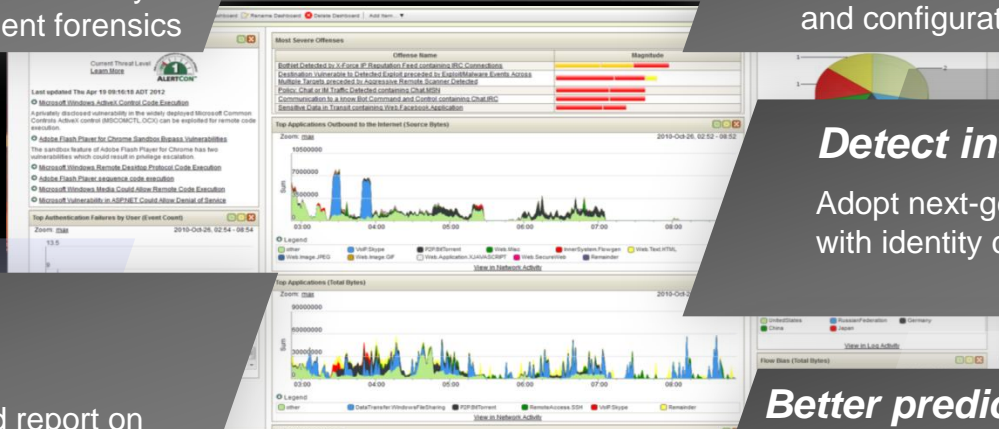
Adopt next-generation SIEM with identity correlation

Consolidate data silos

Collect, correlate and report on data in one integrated solution

Better predict business risks

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