Providing Your Business: Total Security Intelligence

Steve Jenkins,

VP of European Sales

Q1 Labs, an IBM Company

PCTY2012

Pulse Comes to You

Optimizing the World's Infrastructure

30th May 2012, London

What is Security Intelligence?

Security Intelligence

--noun

1. the real-time collection, normalization, and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

Q1 Labs- The Security Intelligence Leader

Who we are:

- Innovative Security Intelligence software company
- One of the largest and most successful SIEM vendors
- Leader in Gartner 2011, 2010, 2009 Magic Quadrant

Award-winning solutions:

- Family of next-generation Log Management, SIEM, Risk Management, Security Intelligence solutions

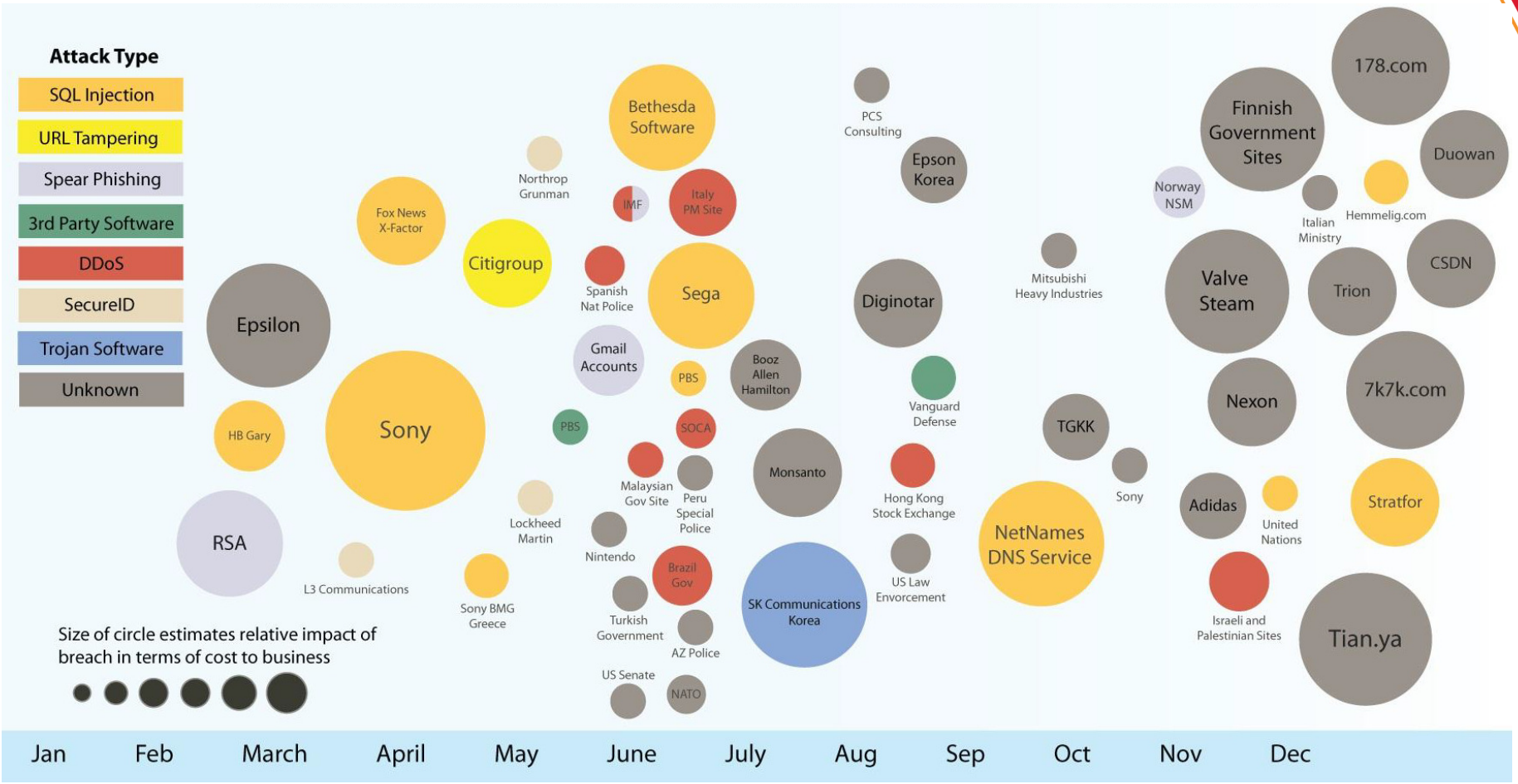
Proven and growing rapidly:

- Thousands of customers worldwide
- Five-year average annual revenue growth of 70%+

Now part of IBM Security Systems:

- Unmatched security expertise and breadth of integrated capabilities

Why we are here-
Attacks are top of mind in the boardroom



Attacks from all sides

Have we learned anything?

SUBWAY (2011)
Theft of credit card data from 80,000 customers

Romanians accessed POS systems in NH, NY, OH & CA then exfiltrated data to compromised server in PA

CYBER-CRIME

US CHAMBER OF COMMERCE (2010)
Theft of intellectual property

Chinese hackers used spearphishing to steal employee credentials & install malware

CYBER-ESPIONAGE

SONY (2011)
Brand impact, remedies & lost business = $1B loss est.

Hackers exploited Web application vulnerability to access back-end customer databases

CYBER-ACTIVISM

EU Directive- Privacy is essential

- EU Justice Commissioner, Viviane Reding, at the Digital Life Design (DLD) conference in Munich Jan 2012
- All 27 European member states will be governed by the new rules, which could see companies being fined 2 per cent of global turnover if their customers' privacy is breached
- Under the new rules, all UK companies that suffer a security breach will have to inform the Information Commissioner within 24 hours of discovering a breach
- Companies with more than 250 employees will have to appoint a privacy officer

Total Security Intelligence:
Latest Threats & Combating them

- Predicting an attack
- Reducing your data silos
- Managing risk & configuration
- Exceeding regulatory mandates

Total Security Intelligence:
Latest Threats & Combating them

- Predicting an attack
- Reducing your data silos
- Managing risk & configuration
- Exceeding regulatory mandates

Predicting an attack:
IBM's Global Expertise

IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration

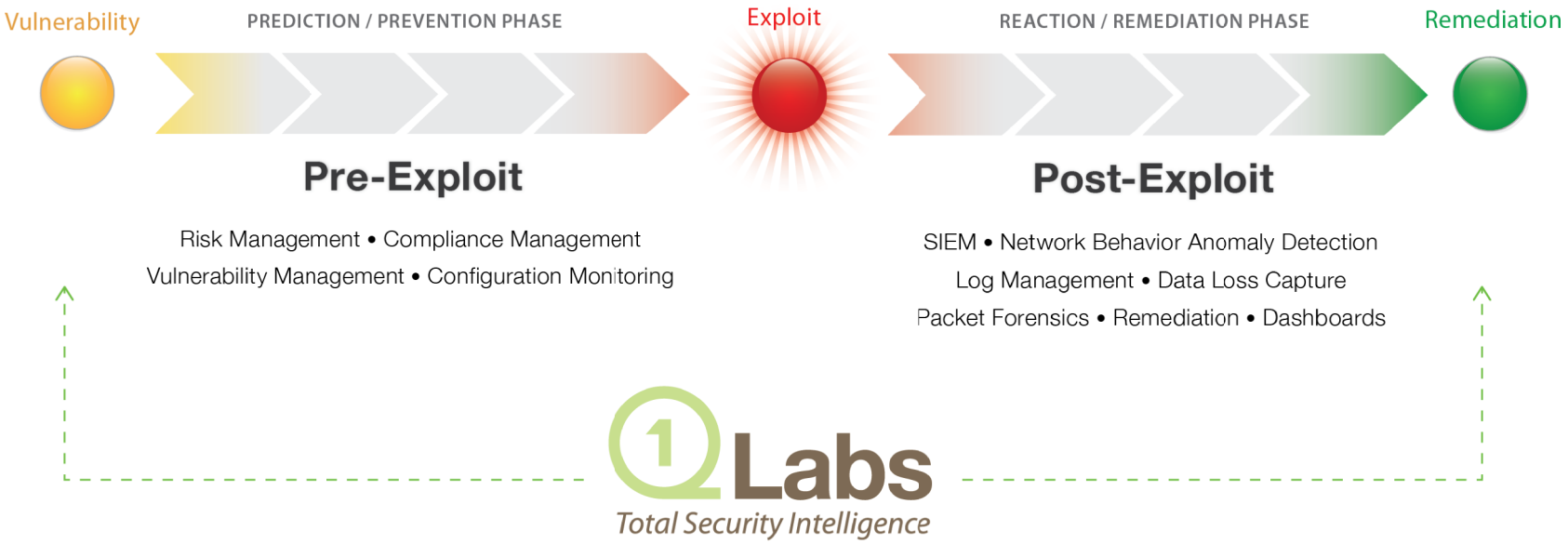
10B analyzed Web pages & images
150M intrusion attempts daily
40M spam & phishing attacks
46K documented vulnerabilities
Millions of unique malware samples

X-FORCE

World Wide Managed Security Services Coverage

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 9B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

Predicting an attack:
Be proactive not reactive



Predicting an attack:
Case Study

- European Bank
- On-line banking system targeted
- DDOS attack, three times
- Had ‘security’ in place
- Early warning capability

Predicting an attack:
How it looks on QRadar

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source	Flow Interfac
	14:54	Multiple (1017)	Multiple (1017)	172.16.15.10	0	tcp_ip	other	390 528 (C)	N/A	6 102	N/A	N/A	vm153_211	vm153_211:eth2
	14:55	Multiple (1020)	Multiple (1020)	172.16.15.10	0	tcp_ip	other	326 400 (C)	N/A	5 100	N/A	N/A	vm153_211	vm153_211:eth2
	14:56	Multiple (1022)	Multiple (1022)	172.16.15.10	0	tcp_ip	other	392 448 (C)	N/A	6 132	N/A	N/A	vm153_211	vm153_211:eth2
	14:57	Multiple (1023)	Multiple (1023)	172.16.15.10	0	tcp_ip	other	392 832 (C)	N/A	6 138	N/A	N/A	vm153_211	vm153_211:eth2
	14:58	Multiple (1023)	Multiple (1023)	172.16.15.10	0	tcp_ip	other	327 360 (C)	N/A	5 115	N/A	N/A	vm153_211	vm153_211:eth2
	14:55	172.16.153.35	61375	172.16.155.99	902	udp_ip	other	112 (C)	0	1	0	N/A	vm153_211	vm153_211:eth0

Multiple IP's trying to go through one IP

Flow Information

Protocol:	tcp_ip	Application:	other				
Magnitude:	(3)	Relevance:	3	Severity:	1	Credibility:	5
First Packet Time:	2012-04-13 14:54:00	Last Packet Time:	2012-04-13 14:54:56	Storage Time:	2012-04-13 14:56:00		
Event Name:	HTTPWeb						
Low Level Category:	HTTP In Progress						
Event Description:	Detected via application state based decoding						

Source and Destination Information

1017 Source(s):	81.10.0.39:0 81.10.1.216:0 81.10.0.1:0 81.10.3.217:0 81.10.3.240:0 81.10.1.233:0 81.10.0.82:0 81.10.3.13:0	Destination IP:	172.16.15.10:0

Drilling into one superflow record showing all IP records contribute to one rule

Offense 2 (All Categories)

Offense 2

Display ▼ Events Flows Actions ▼ Print

Magnitude		Status		Relevance	4	Severity	0	Credibility	3
Description	Potential DDoS Against Single Host (TCP) containing HTTPWeb	Offense Type		Destination IP					
		Event/Flow count		9 events and 1409236 flows in 2 categories					
Source IP(s)	Multiple (4)	Start		2012-04-12 15:42:00					
Destination IP(s)	172.16.15.10	Duration		23h 23m					
Network(s)	Net-10-172-192.Net_172_16_0_0	Assigned to		Unassigned					

Offense Source Summary

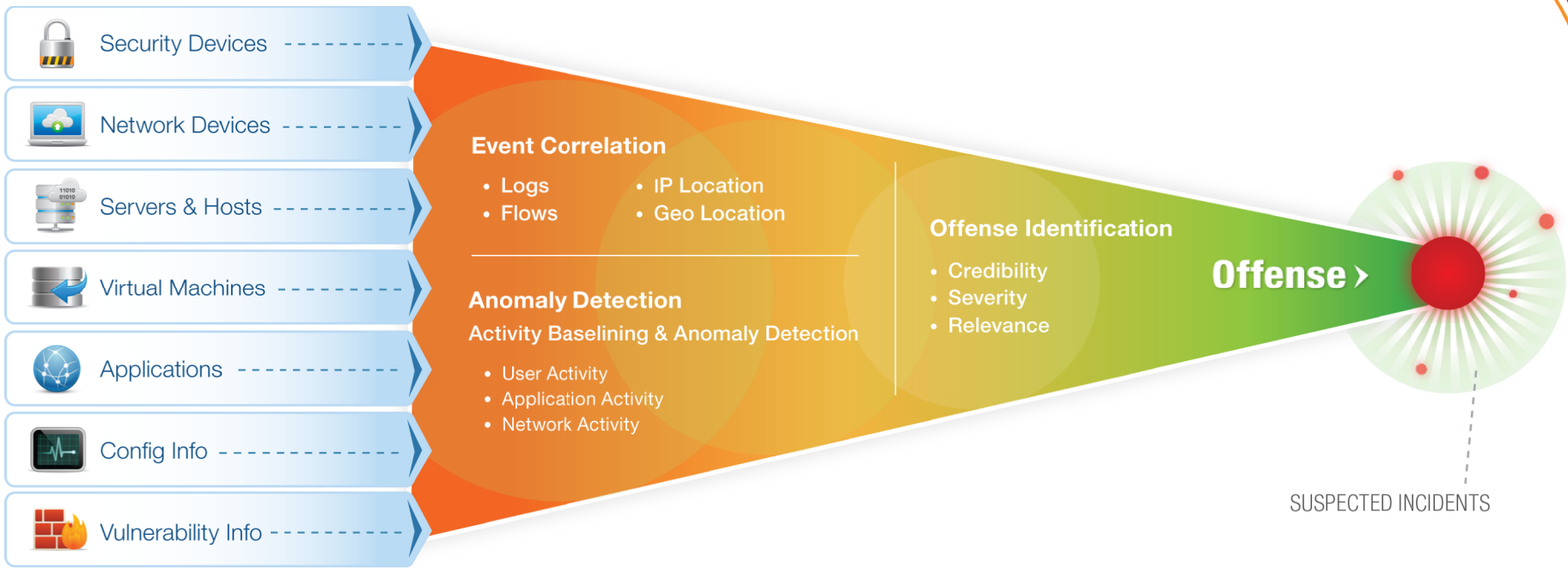
IP	172.16.15.10	Location	Net-10-172-192.Net_172_16_0_0
Magnitude		Vulnerabilities	0
User	Unknown	MAC	Unknown
Host Name	Unknown		
Asset Name	Unknown	Asset Weight	0
Chained	Yes		
Offenses	1	Events/Flows	1409245

All pulled together in one offence which is detected and raised immediately to the security team

Total Security Intelligence:
Latest Threats & Combating them

- Predicting an attack
- Reducing your data silos
- Managing risk & configuration
- Exceeding regulatory mandates

Big Data:
Reduce your data silo down



Most Sources + Most Intelligence = Most Accurate & Actionable Insight

Big Data:
Case studies

- 2 Billion events a day
- 20-25 potential offences
- Automation
- Time to resolution

- Compliance
- Numbers of potential offences
- Automation
- Manageable number

Big Data:
How it looks on QRadar

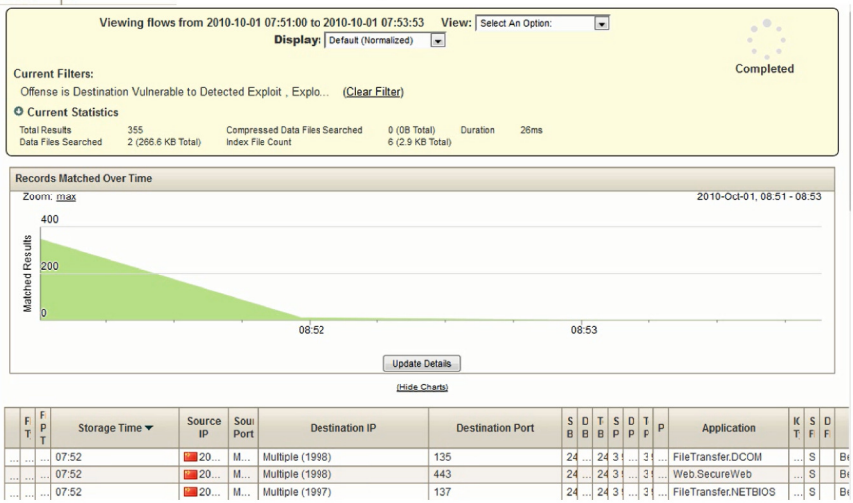
Offense 160 — Display ▼ | Events | Connections | Flows | View Attack Path | Actions ▼ | Print

Magnitude		Relevance 0	Severity 10	Credibility
Description	Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Aggressive Remote Scanner Detected	Offense Type	Source IP
		Event/Flow count	19984 events and 355 flows in 12 categories.
Source IP(s)	202.153.48.66	Start	2010-10-01 07:51:00
Destination IP(s)	Local (315)	Duration	2m 52s
Network(s)	Multiple (2)	Assigned to	Not assigned

Single incident derived from ~20k events and 355 flows

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port
Misc Exploit - Event CRE	Custom Rule Engine-8 :: qradar	1	07:53	Misc Exploit	202.153.48.66	0
NETBIOS-DG SMB v4 srvsvc...	Snort @ snort.acme.com	1	07:53	Buffer Overflow	202.153.48.66	0
NETBIOS-DG SMB v4 srvsvc...	Snort @ snort.acme.com	1	07:53	Buffer Overflow	202.153.48.66	0
NETBIOS-DG SMB v4 srvsvc...	Snort @ snort.acme.com	1	07:53	Buffer Overflow	202.153.48.66	0
NETBIOS-DG SMB v4 srvsvc...	Snort @ snort.acme.com	1	07:53	Buffer Overflow	202.153.48.66	0
Misc Exploit - Event CRE	Custom Rule Engine-8 :: qradar	1	07:53	Misc Exploit	202.153.48.66	0
NETBIOS-DG SMB v4 srvsvc...	Snort @ snort.acme.com	1	07:53	Buffer Overflow	202.153.48.66	0

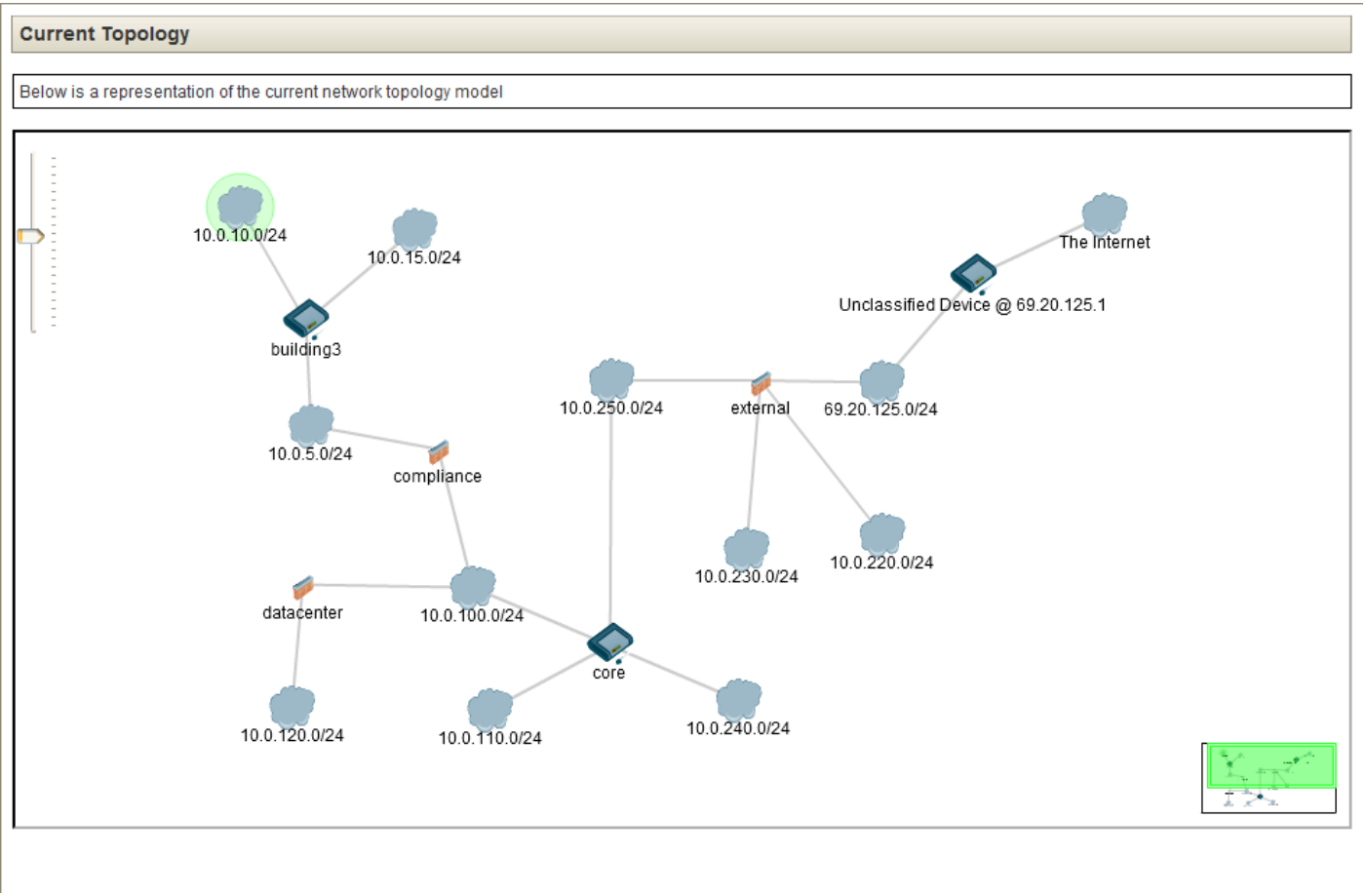
- QRadar automatically pulls all related events and flows into onto single security incident
- Highlights the magnitude/importance
- Reduction into manageable daily number



Total Security Intelligence:
Latest Threats & Combating them

- Predicting an attack
- Reducing your data silos
- Managing risk & configuration
- Exceeding regulatory mandates

Managing risk efficiently:
Real time analysis & configuration



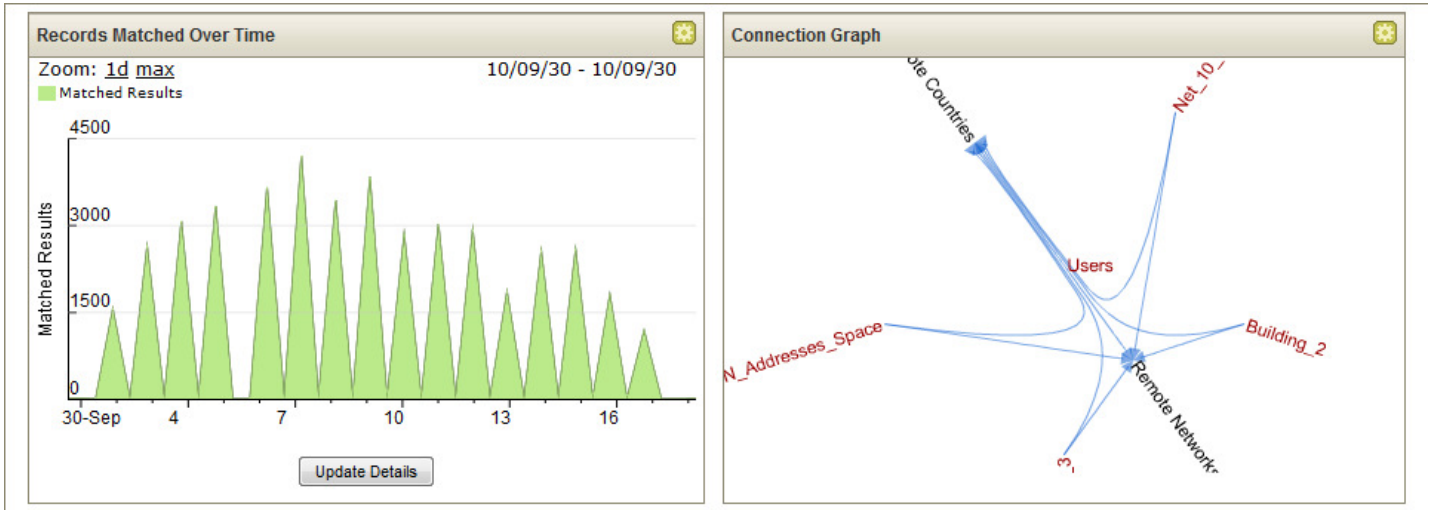
Network topology and open paths of attack add context

Rules can take exposure into account to:

- Prioritize offenses and remediation
- Enforce policies
- Play out what-if scenarios

Real time analysis & configuration: Prioritized Response

Network monitoring + configuration management = deeper level of forensics & accurate impact analysis



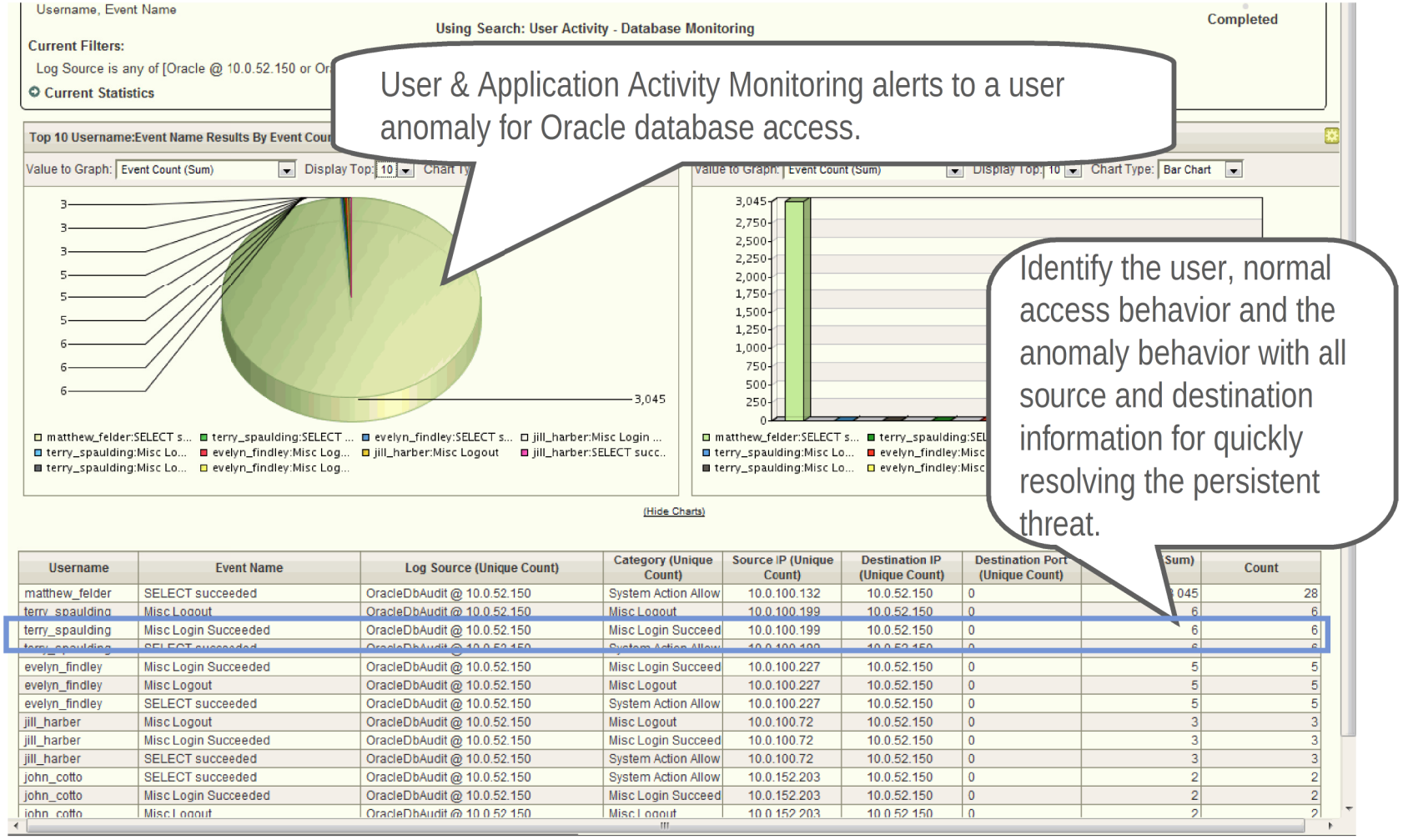
Last Packet Time	Source Type	Source	Destination Type	Destination	Protocol	Destination Port	Flow Application	Flow Source	Flow C
18:11	Host	10.0.15.20	Host	10.0.15.20	Reserved	0	N/A	N/A	N/A
17:58	Host	10.0.1.231	Remote	NorthAmerica.UnitedStates : c	UDP	3544	N/A	N/A	N/A
17:56	Host	10.0.1.231	Remote	NorthAmerica.UnitedStates : c	TCP	80	N/A	N/A	N/A
17:52	Host	10.0.120.70	Host	10.0.120.70	Reserved	0	N/A	N/A	N/A
17:49	Host	10.0.1.231	Remote	Europe.Estonia : other	TCP	80	N/A	N/A	N/A
17:49	Host	10.0.1.231	Remote	Europe.Macedonia : other	UDP	30789	N/A	N/A	N/A
17:49	Host	10.0.1.231	Remote	Europe.Greece : other	UDP	24005	N/A	N/A	N/A
17:48	Host	10.0.1.231	Remote	Europe.Romania : other	UDP	34177	N/A	N/A	N/A
17:48	Host	10.0.1.231	Remote	Europe.Bulgaria : other	UDP	48219	N/A	N/A	N/A
17:48	Host	10.0.1.231	Remote	Europe.RussianFederation : c	UDP	52794	N/A	N/A	N/A
17:48	Host	10.0.1.231	Remote	NorthAmerica.UnitedStates : c	UDP	23917	N/A	N/A	N/A

Managing risk & configuration:
Case study

- Remote office location
- Network behaviour analysis
- Unusual traffic volumes, not the norm
- Identified device, isolated
- Security called

Managing risk & configuration:
How it looks on QRadar

User Behaviour Monitoring & APTs



Username	Event Name	Log Source (Unique Count)	Category (Unique Count)	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Sum)	Count
matthew_felder	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.132	10.0.52.150	0	045	28
terry_spaulding	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.100.199	10.0.52.150	0	6	6
terry_spaulding	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.100.199	10.0.52.150	0	6	6
terry_spaulding	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.199	10.0.52.150	0	6	6
evelyn_findley	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.100.227	10.0.52.150	0	5	5
evelyn_findley	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.100.227	10.0.52.150	0	5	5
evelyn_findley	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.227	10.0.52.150	0	5	5
jill_harber	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.100.72	10.0.52.150	0	3	3
jill_harber	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.100.72	10.0.52.150	0	3	3
jill_harber	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.72	10.0.52.150	0	3	3
john_cotto	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.152.203	10.0.52.150	0	2	2
john_cotto	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.152.203	10.0.52.150	0	2	2
john_cotto	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.152.203	10.0.52.150	0	2	2

Total Security Intelligence:
Latest Threats & Combating them

- Predicting an attack
- Reducing your data silos
- Managing risk & configuration
- Exceeding regulatory mandates

Regulatory Mandates:
Being both compliant and secure

- Companies today are under growing executive pressure to comply with mandates such as SOX, GPG-13, PCI, NERC
- Compliance is more than simply generating reports
- 3 key factors need to be fulfilled:

Accountability

Proving surveillance to report on who did what and when

Transparency

Visibility into the security controls, the business applications and the assets that are being protected

Measurability

Metrics and reporting around IT risks within a company

Regulatory Mandates:
Case study

- Employee
- Downloading information
- Erasing files
- Time stamped

Regulatory Mandates:
How it looks on QRadar

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 ...

Potential Data Loss?

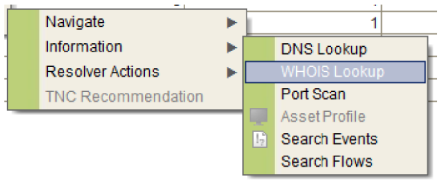
Who? What? Where?

Attacker Summary	Details		
Magnitude		**User**	Karen
Description	10.103.14.139	**Asset Name**	dhcp-workstation-103.14.139.acme.org
Vulnerabilities	0	**MAC**	00:05:9A:3C:79:00
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 Detec	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



QRadar Has Completed Your Request

Go to APNIC results

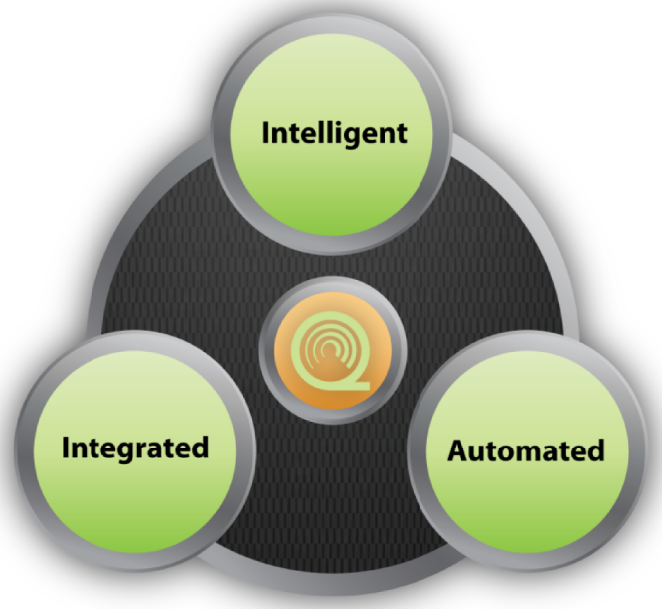
[Querying whois.arin.net]
[whois.arin.net]

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

Where?
Gmail

QRadar: The Most Intelligent, Integrated, Automated Security Intelligence Platform

- Proactive threat management
- Identifies most critical anomalies
- Rapid, complete impact analysis



- Eliminates silos
- Highly scalable
- Flexible, future-proof

- Easy deployment
- Rapid time to value
- Operational efficiency

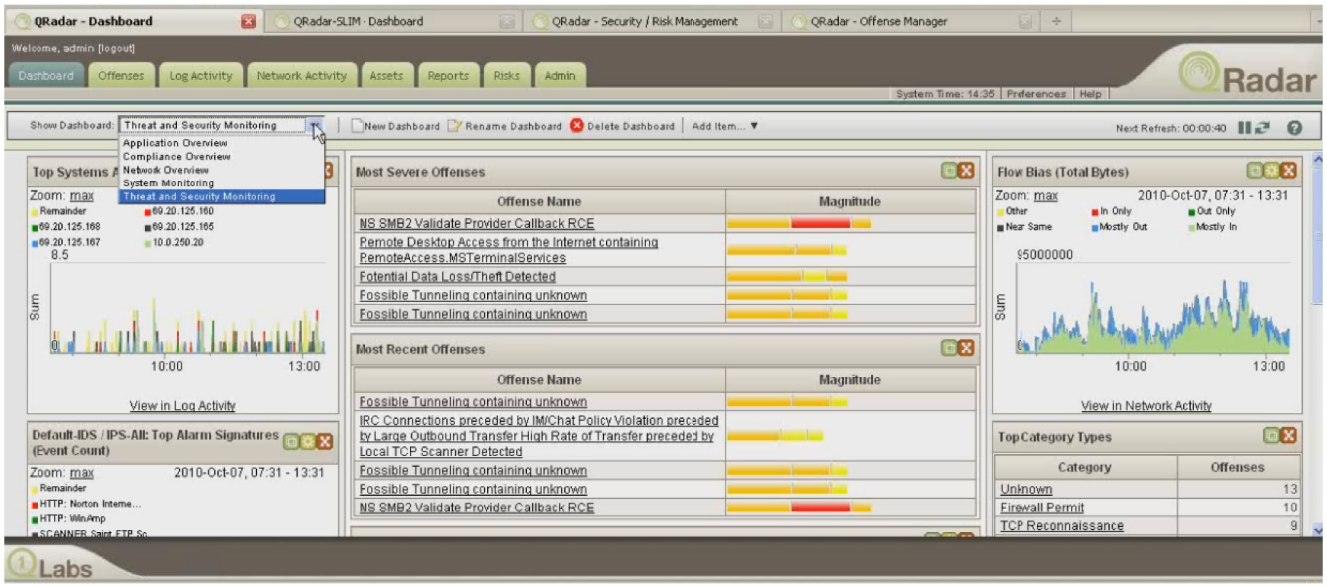
Fully Integrated Security Intelligence

Log Management	Radar Log Manager Radar Log Manager Free Edition	• Turnkey log management • SME to Enterprise • Upgradeable to enterprise SIEM
SIEM	Radar SIEM	• Integrated log, threat, risk & compliance mgmt. • Sophisticated event analytics • Asset profiling and flow analytics • Offense management and workflow
Risk Management	Radar Risk Manager	• Predictive threat modeling & simulation • Scalable configuration monitoring and audit • Advanced threat visualization and impact analysis
Network Activity & Anomaly Detection	Radar SIEM Radar QFlow	• Network analytics • Behavior and anomaly detection • Fully integrated with SIEM
Network and Application Visibility	Radar QFlow Radar VFlow	• Layer 7 application monitoring • Content capture • Physical and virtual environments

Fully Integrated Security Intelligence

- Log Management
- SIEM
- Risk Management
- Network Activity & Anomaly Detection
- Network and Application Visibility

One Console Security



Built on a Single Data Architecture

Summary

Security breaches are becoming more advanced

- People, data, applications and infrastructure all need to be covered

New EU Directive being proposed

- Most likely to come into action 2014

Knowledge in advance

- Be proactive and use measures to highlight potential threats before they occur

Highlight the key threats

- Reduce your data silo to a manageable number

Compliance is more than report generation

- Accountability, transparency and measurability

Q1 Labs, an IBM Company can help businesses with these issues

- Expert and proven “Total Security Intelligence”

What to do next?

- Read our blog
  http://blog.q1labs.com/
- Follow us on Twitter:
  @q1labs @ibmsecurity
- Watch our recent webcasts
  http://q1labs.com/resource-center/media-center.aspx
- Download the Gartner SIEM Critical Capabilities Report
  http://q1labs.com/resource-center/analyst-reports/details.aspx?id=17

Thank You!

Q1 Labs, an IBM Company
email: STEVEJEN@uk.ibm.com
Phone: 07787543327
www.q1labs.com

Acknowledgements, disclaimers and trademarks

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication 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 this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation 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. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml