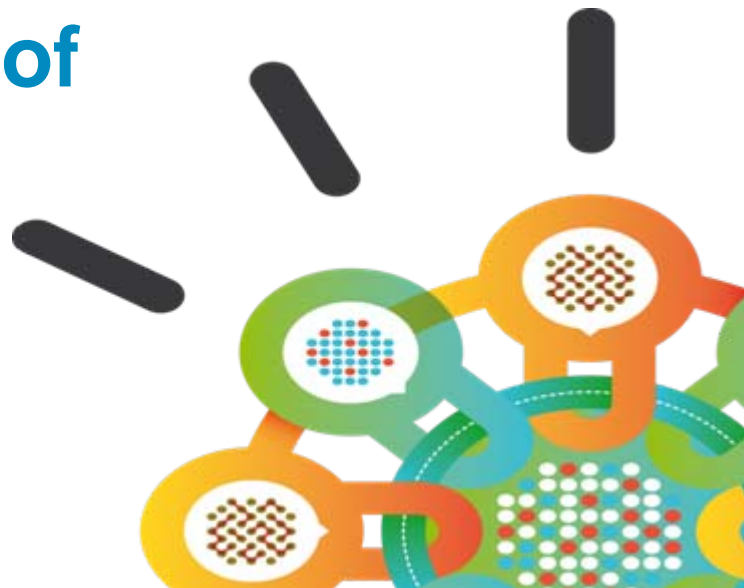


Security Intelligence.
Think Integrated.

No One is Immune to Being Hacked: Strategies for Staying Out of the Headlines

QRadar Security Intelligence
Platform





“Our most formidable challenge is getting companies to detect they have been compromised ...”



*Kim Peretti, senior counsel,
US Department of Justice (DoJ)*



Source: <http://www.scmagazine.com/rsa-conference-gonzalez-may-receive-largest-ever-us-hacking-sentence/article/165215/> – March 2010



Attacks from All Sides

Cyber vandals

Cyber warfare

Targets of opportunity

Nation states

Cyber crime

Hacktivists

Targets of choice

Cyber terrorism

Corporate espionage

Cyber espionage

Client-side vulnerabilities

Insiders

APTs

Data exfiltration



'Flame' cyber espionage worm

- Successor to Duqu and Stuxnet
- Targeted Attack!
- What is it?
 - Sophisticated Attack Toolkit
 - Backdoor, Trojan, Worm-Like
- Exploits Current Vulnerabilities

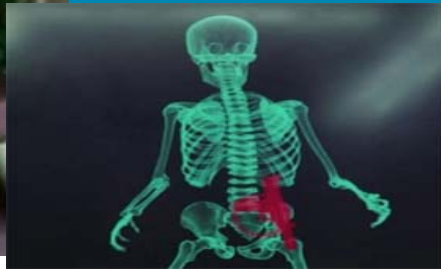
...but all is not lost...

Choose the Right Technology



Protection technology is critical, but choose wisely

There is no magic security technology



People and Processes First

A lesson from airport security:

Instead of expensive equipment, use what works

In Israel

- No plane departing Ben Gurion Airport has ever been hijacked
- Use human intelligence
- “Questioning” looks for suspicious behavior
- Simple metal detectors

Scotland Yard

- 24+ men planned to smuggle explosive liquids
- Foiled beforehand because of intelligence
- Before they even got to the airport

What Can Help You Defend Against an APT?

❖ Focus on both prevention and detection

- A truly advanced and persistent adversary will breach your defenses
- How quickly you detect the breach will determine its impact

❖ Smart *preventive* measures reduce weaknesses...

- Control your endpoints – Make sure patches are up to date
- Audit Web applications
- Find and remediate bad passwords
- Monitor device configurations for errors and vulnerabilities

❖ And advanced *detection* finds intrusions faster & assesses impact

- Flow analytics and network anomaly detection
- User anomaly detection
- Reconnaissance detection
- Stealthy malware detection
- Database monitoring



Security Intelligence Use Cases



How Security Intelligence Can Help

- **Continuously monitor** all activity and correlate in real-time
- Gain visibility into *unauthorized or anomalous* activities
 - **Server (or thermostat) communicating with IP address in China**
 - Unusual Windows service -- backdoor or spyware program
 - **Query by DBA to credit card tables during off-hours – possible SQL injection attack**
 - Spike in network activity -- high download volume from SharePoint server
 - **High number of failed logins to critical servers -- brute-force password attack**
 - Configuration change -- unauthorized port being enabled for exfiltration
 - **Inappropriate use of protocols -- sensitive data being exfiltrated via P2P**

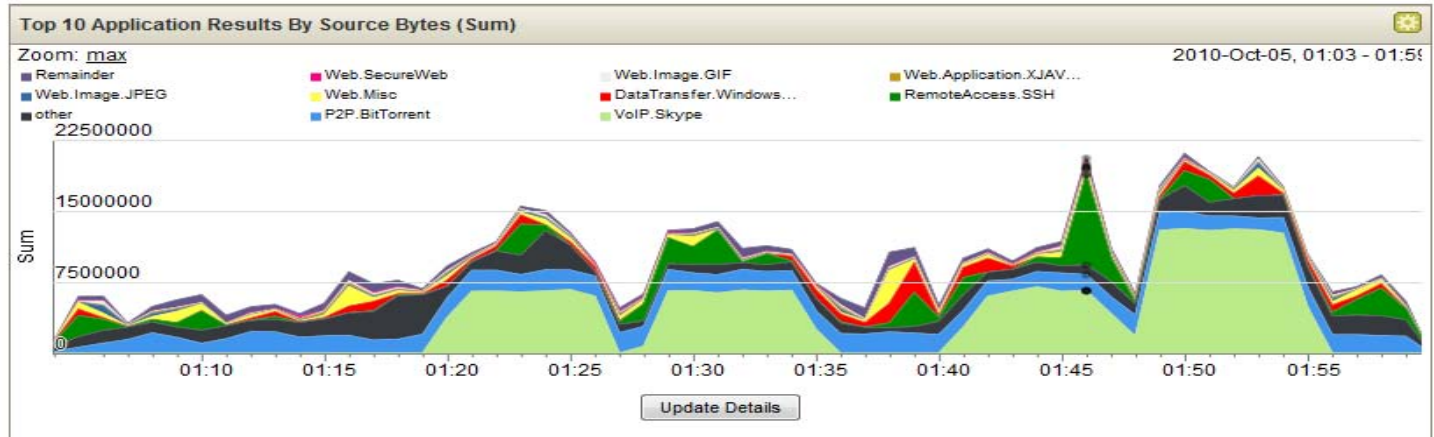


Why Should You Care?

- Detect suspicious behavior
 - Privileged actions being conducted from a contractor's workstation
 - DNS communications with external system flagged as malicious
- Detect policy violations
 - Baseline against reality (CMDB)
 - Social media, P2P, External File Sharing, etc.
- Detect APTs
 - File accesses out of the norm—behavior anomaly detection
 - Least used applications or external systems; occasional traffic
- Detect fraud
 - Determine baselines on credit pulls or trading volumes, and detect anomalies
 - Correlate eBanking PIN change with large money transfers
- Forensic evidence for prosecution
- Impact analysis
- Compliance
 - Change & configuration management
- Metrics

Network Activity Monitoring (Network Flows)

- Attackers can stop logging and erase their tracks, but can't cut off the network
- Helps detect day-zero attacks with no signature; provides visibility into attacker communications
- Network activity can build up an asset database and profile assets
- Useful for non-security related issues as well



Application and Threat Detection with Forensic Evidence

Potential Botnet Detected?
This is as far as traditional SIEM can go

Magnitude	Description	Event count	Relevance
Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow	6 events in 1 categories		
Attacker/Src: 10.103.6.6 (dhcp-workstation-103.6.6.acme.org)	Start: 2009-09-29 11:21:01		
Target(s)/Dest: Remote (5)	Duration: 0s		
Network(s): other	Assigned to: Not assigned		
Notes: Botnet Scenario This offense captures Botnet command channel activity from an internal host. The botnet node communicates with IRC servers running on non-standard ports (port 80/http), which would typically bypass many detection techniques. This sc...			

IRC on port 80?
IBM Security QRadar QFlow detects a covert channel

First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Cor	Source Flags
11:19	tcp_ip	10.103.6.6	48657	62.64.54.11	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	50296	192.106.22.13	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	51451	62.181.209.20	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A

Irrefutable Botnet Communication
Layer 7 flow data contains botnet command control instructions

```

Source Payload
108 packets,
8850 bytes

UTF Hex Base64
NICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombPROTOCTL NAMESX
PROTOCTL NAMESX
PROTOCTL NAMESX
NOTICE Defender :!VERSION xchaHOT
JOIN #botnet_command_channel
JOIN #botnet_command_channel
    
```

Application layer flow analysis can detect threats others miss

Detecting Insider Fraud and Data Loss

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 (a)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

	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-vr	N/A	Suspicious Pattern Detected
❑	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vr	N/A	Remote Access Login Failed

Who?
An internal user

What?
Oracle data

QRadar Has Completed Your Request

Go to APNIC results

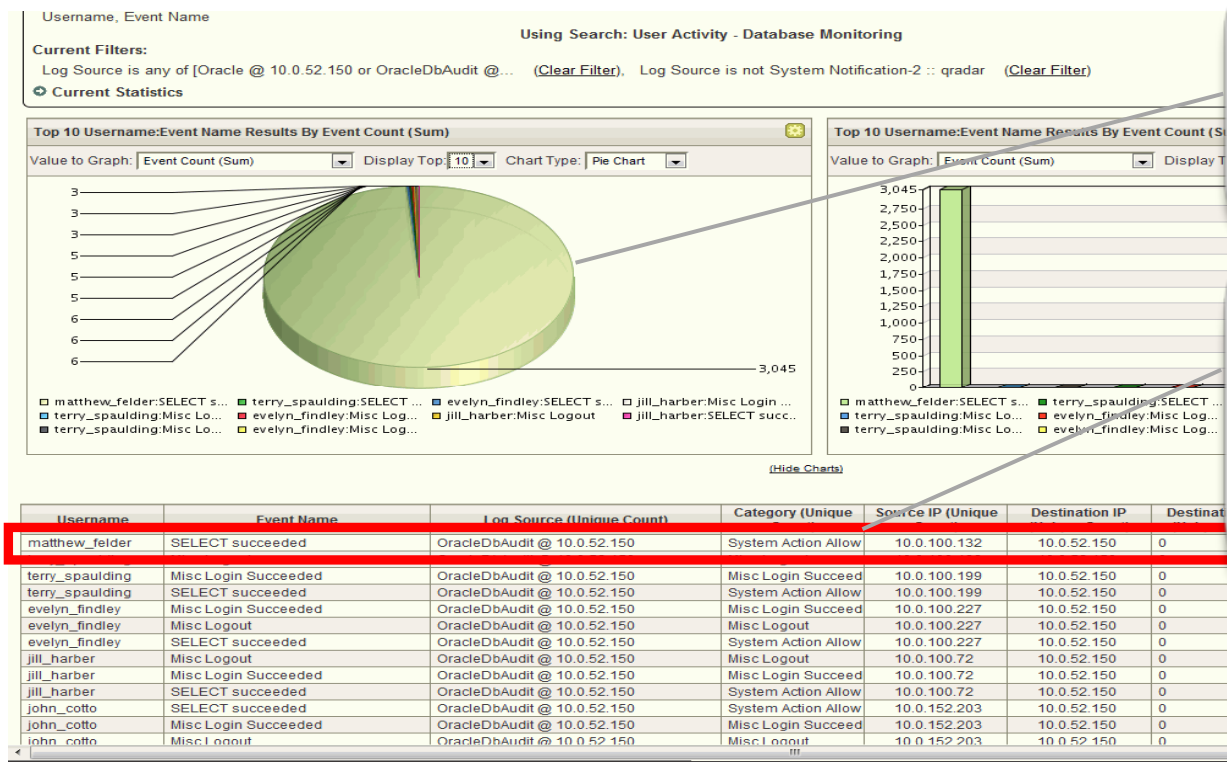
[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL

Where?
Gmail

Threat detection in the post-perimeter world
User anomaly detection and application level visibility are critical to identify inside threats

User Activity Monitoring to Combat Advanced Persistent Threats



User & Application Activity Monitoring alerts on a user anomaly for Oracle database access.

Identify the user, normal access behavior, and the anomaly behavior – with all source & destination information to quickly resolve the threat.

Predicting Risks to Your Business

Assess assets with high-risk input manipulation vulnerabilities

Questions	Name	Group	Return Type	Importance Factor	Severity
Are systems with Client Side scripts which communicate to the Internet	Client Side Scripts	Client Side	Script	4	High
Are systems with Client Side scripts which communicate to the Internet	Client Side Scripts	Client Side	Script	4	High
Are systems with Client Side scripts which communicate to the Internet	Client Side Scripts	Client Side	Script	4	High
Are systems with Client Side scripts which communicate to the Internet	Client Side Scripts	Client Side	Script	4	High
Are systems with Client Side scripts which communicate to the Internet	Client Side Scripts	Client Side	Script	4	High
Are systems with Client Side scripts which communicate to the Internet	Client Side Scripts	Client Side	Script	4	High

Description: Find assets that are susceptible to vulnerabilities with one of the following classifications (Input Manipulation) and are susceptible to vulnerabilities with CVE scores greater than 8.

Asset Results:

Name	Weight	Destination Ports	Protocols	File Access	Values	File Counts	Accesses	Denials
10.2.0.10	100	443	HTTP	Full	Full	Full	Full	Full

Which assets are affected?
How should I prioritize them?

What are the details?
Vulnerability details, ranked by risk score

How do I remediate the vulnerability?

ID	Description	Severity
9723	Multiple Vendor LDAP Server NULL Bind Connection Information Disclosure	7
9723	Microsoft Windows smc.sys Kernel Driver SMB2 Malformed NEGOTIATE PROTOCOL REQUEST Remote DoS	10
202	Microsoft Windows Installation ADMIN\$ Share Arbitrary Access	10

Days of Exposure	
36 days	

Description	Microsoft Windows contains a flaw that may allow a malicious user to execute arbitrary code. The issue is triggered when a malicious SMB2 packet with an & (ampersand) character in a Process ID High header field, causing an attempted dereference of an out-of-bounds memory location, resulting in a loss of integrity.
Classification	Location: Remote / Network Access Attack Type: Denial of Service, Input Manipulation Impact: Loss of Confidentiality, Loss of Availability Solution: Patch / RCS Exploit: Exploit Public, Exploit Commercial Disclosure: Vendor Verified, Uncoordinated Disclosure
Solution	Currently, there are no known workarounds or upgrades to correct this issue. However, Microsoft Corporation has released a patch to

Pre-exploit Security Intelligence
Monitor the network for configuration and compliance risks, and prioritize them for mitigation

Exceeding Regulation Mandates

Offense 2862			
Magnitude	High	Relevance	2
Description	Policy - Internal - Clear Text Application Usage containing Compliance Policy Violation - QRadar Classify Flow	Event count	1 events in 1 category
Attacker/Src	10.103.12.12 (dhep-workstation-103-12-12.some.org)	Start	2009-09-29 15:09:00
Target(s)/Dest	10.101.3.30 (Accounting Fileserver)	Duration	0s
Network(s)	IT.Server.main	Assigned to	Not assigned
Notes	PCI Violation Use Case PCI DSS specifies that insecure protocols may not be used. This scenario describes how to identify such activity. In this offense the system has captured cleartext network activity (telnet and FTP) b		

PCI compliance at risk?
Real-time detection of possible violation



Event Name	Log Source	Source IP	Source Port	Destination IP	Destination Port
Compliance Policy Violation - C	Flow Classification Engine-5	10.103.12.12	1482	10.101.3.30	23

Unencrypted Traffic
IBM QRadar QFlow saw a cleartext service running on the Accounting server
PCI Requirement 4 states: Encrypt transmission of cardholder data across open, public networks

Compliance Simplified
Out-of-the-box support for all major compliance and regulatory standards
Automated reports, pre-defined correlation rules and dashboards

Consolidating Data Silos

System Summary	
Current Flows Per Second	1.4M
Flows (Past 24 Hours)	1.3M
Current Events Per Second	17,384
New Events (Past 24 Hours)	677M
Updated Offenses (Past 24 Hours)	588
Data Reduction Ratio	1153571 : 1

Analyzing both flow and event data – only IBM QRadar can do this

Reducing big data to manageable volumes

Advanced correlation for analytics across silos

Offense 160		Relevance	5	Severity	10	Credibility	8
Magnitude	[Progress bar]						
Description	Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Aggressive Remote Scanner Detected		Offense Type	Source IP			
Source IP(s)	202.153.48.66		Event/Flow count	19984 events and 355 flows in 12 categories.			
Destination IP(s)	Local (315)		Start	2010-10-01 07:51:00			
Network(s)	Multiple (2)		Duration	2m 52s			
			Assigned to	Not assigned			
Notes							
Vulnerability Correlation Use Case							
Illustrates a scenario involving correlation of vulnerability data with IDS alerts							
An attacker originating from China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250).							
The first systems scanned are not vulnerable, but the final system's asset profile has had vulnerability data imported from a Ne							

Most Data Sources

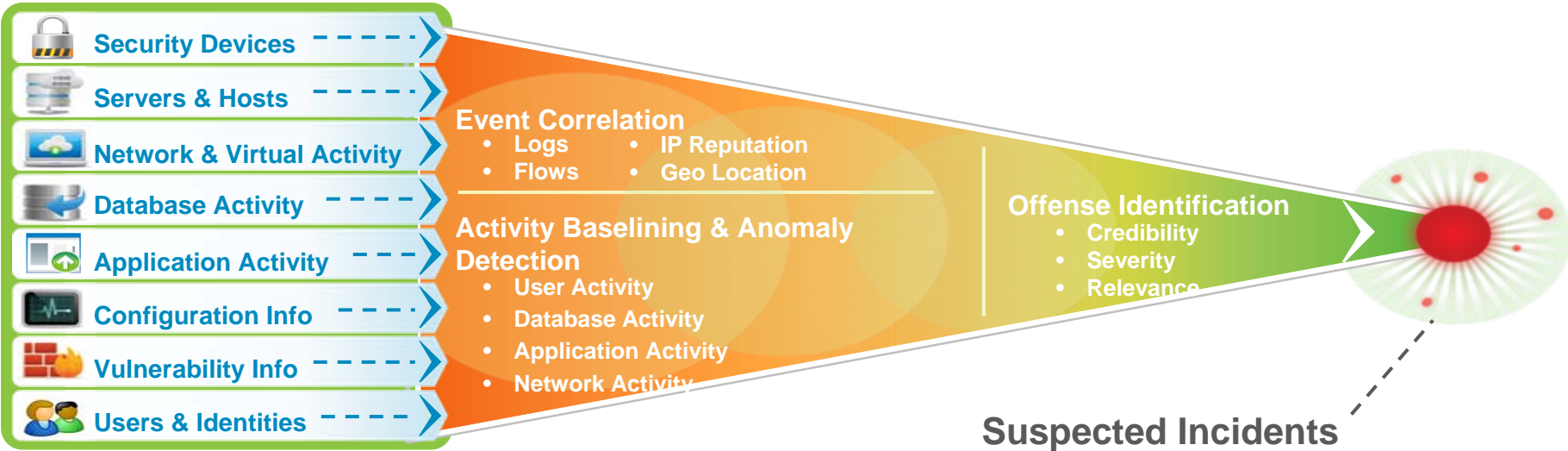


Intelligence



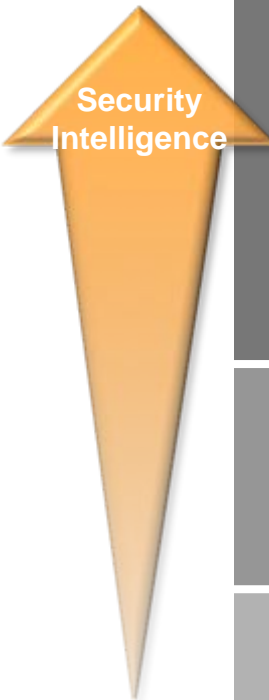
Most Accurate and Actionable Insight

Context and Correlation Drive Deep Insight



Extensive Data Sources + **Deep Intelligence** = **Exceptionally Accurate and Actionable Insight**

Security Intelligence is Enabling Progress to Optimized Security



Security Intelligence: Information and event management Advanced correlation and deep analytics External threat research				
Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Secure systems
Proficient	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus
	People	Data	Applications	Infrastructure

Solving Complex Problems for Clients

Major Electric Utility	Detecting threats	<ul style="list-style-type: none">• Discovered 500 hosts with “Here You Have” virus, which other solutions missed
Fortune 5 Energy Company	Consolidating data silos	<ul style="list-style-type: none">• 2 Billion logs and events per day reduced to 25 high priority offenses
Branded Apparel Maker	Detecting insider fraud	<ul style="list-style-type: none">• Trusted insider stealing and destroying key data
\$100B Diversified Corporation	Predicting risks against your business	<ul style="list-style-type: none">• Automating the policy monitoring and evaluation process for configuration change in the infrastructure
Industrial Distributor	Addressing regulatory mandates	<ul style="list-style-type: none">• Real-time extensive monitoring of network activity, in addition to PCI mandates

What to do next?



Download the Gartner SIEM Magic Quadrant Report:

bit.ly/SIEM-MQ



Read the Q1 Labs Blog: blog.q1labs.com



Subscribe to Q1 Labs Newsletter: bit.ly/Q1-subscribe



Follow us on Twitter: [@q1labs](https://twitter.com/q1labs) [@ibmsecurity](https://twitter.com/ibmsecurity)

ibm.com/security



© Copyright IBM Corporation 2012. 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.

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.