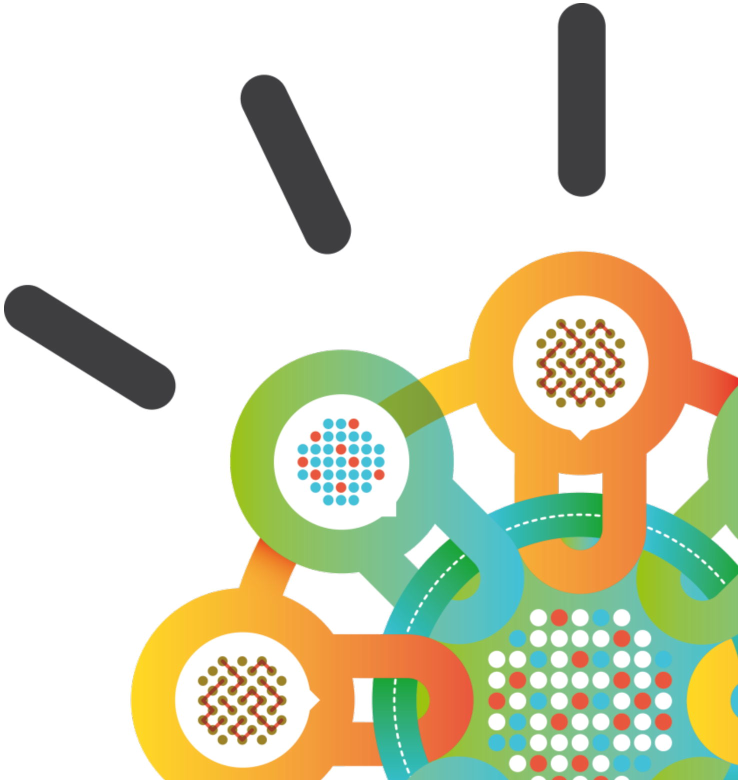
Security Intelligence.
Think Integrated.

WELCOME

Joe Ruthven

BUE - IBM Security Systems, MEA



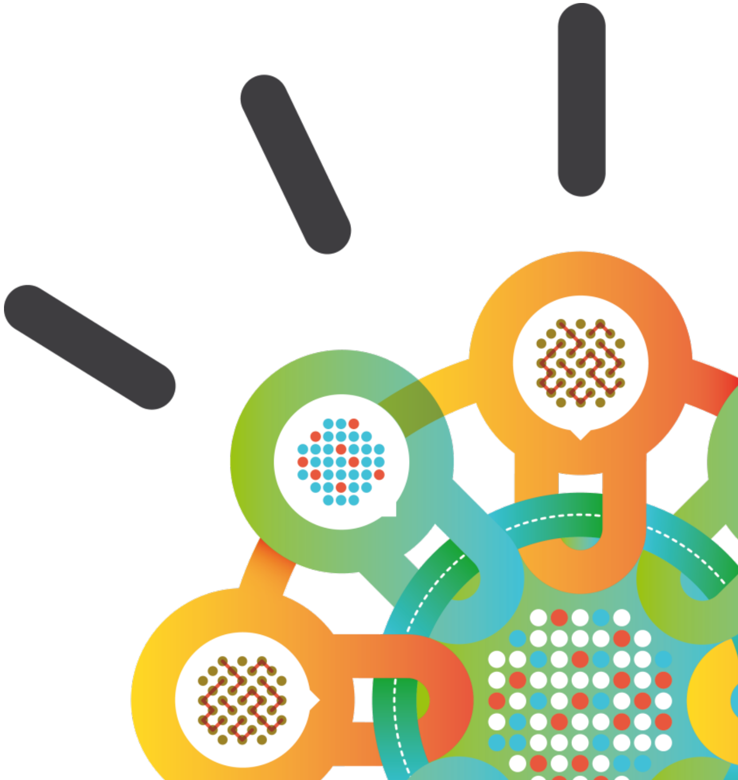
Time	Topic	Speakers
9:05am - 9:45am	Security Stream Kickoff-Security and compliance Overview and X Force	Joe Ruthven and Sukhdev Singh
9:45am - 10:25am	Threat	Lekgale Mokota
10:25am - 10:40am	Break	
10:40am - 11:10am	Q1 Labs Security Intelligence Strategy and Roadmap – How to use Security Intelligence for detecting threats and exceeding compliance mandates	Murray Benadie
11:10am - 11:40am	Driving Effective Application Security in the Enterprise: An End to End Approach to Addressing One of the Biggest Threats to a Business	Sukhdev Singh
11.40am - 12:10pm	Identity Intelligence: Enabling Secure Cloud and Mobile Access	Kevin Mckerr (Puleng)
12:10pm - 12:15 pm	Closing and Questions	
12:15pm	Lunch and Networking	

Security Intelligence.
Think Integrated.

IBM Security

Intelligence, Integration and Expertise

August 2012



Joe Ruthven
BUE IBM Security Systems
IBM Middle East and Africa
joer@za.ibm.com

The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks…

DATA EXPLOSION

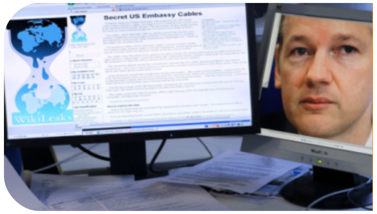
The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

EVERYTHING IS EVERYWHERE

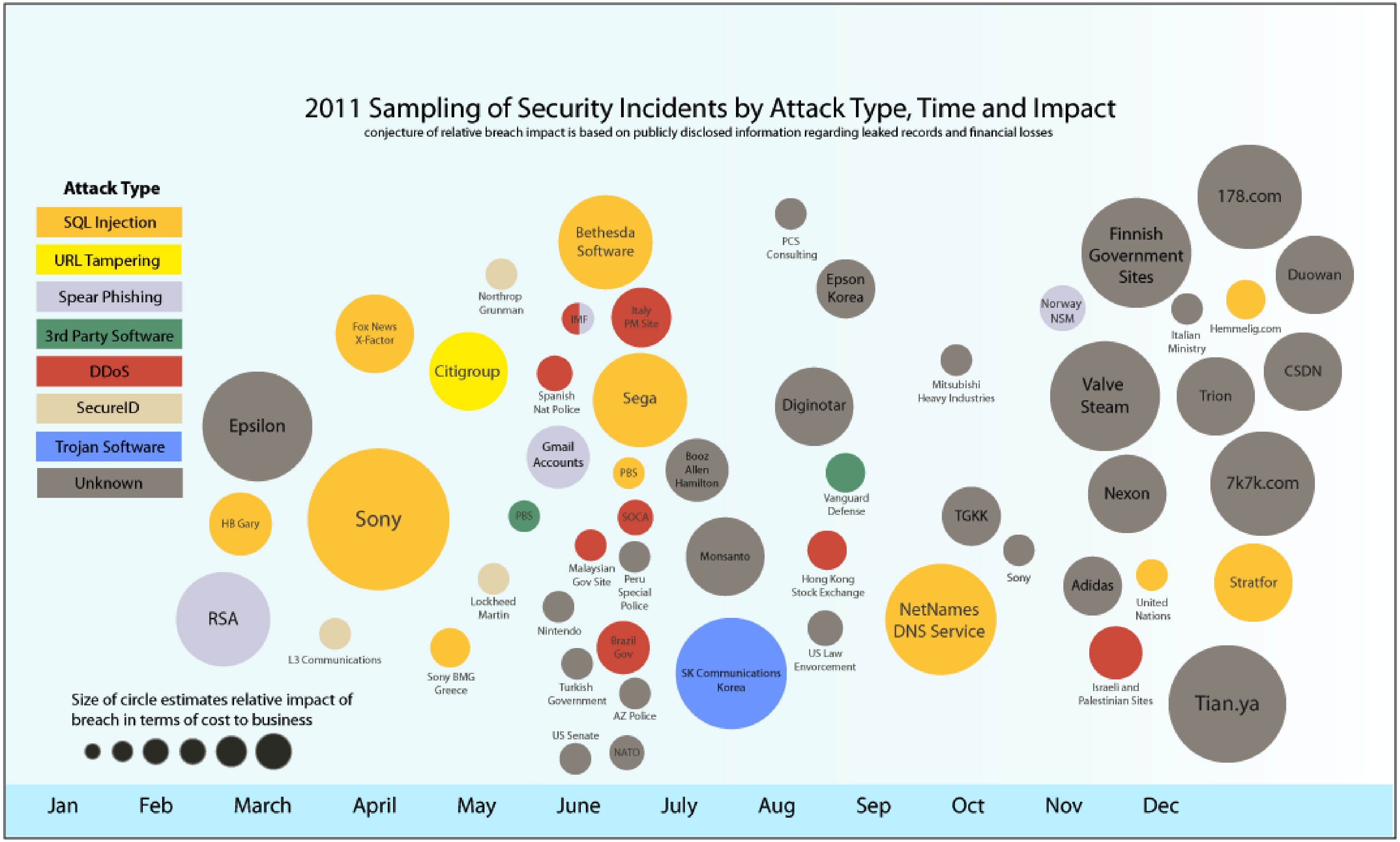
Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more



ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new actors with new motivations from cyber crime to terrorism to state-sponsored intrusions

Targeted Attacks Shake Businesses and Governments

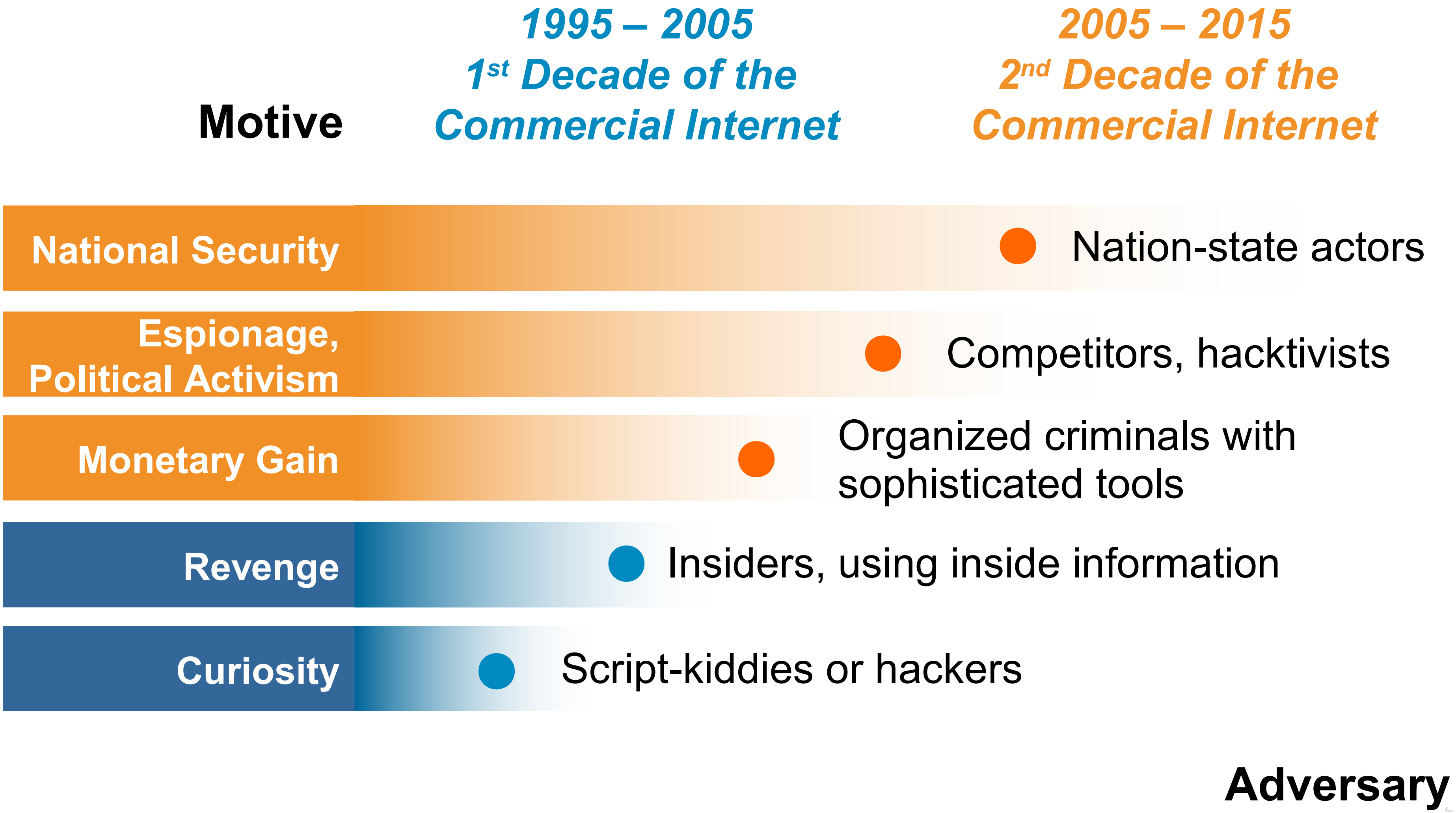


2011 Sampling of Security Incidents by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Size of circle estimates relative impact of breach in terms of cost to business

Motivation and sophistication is evolving rapidly



Motive

1995 – 2005
1st Decade of the Commercial Internet

2005 – 2015
2nd Decade of the Commercial Internet

National Security ● Nation-state actors

Espionage, Political Activism ● Competitors, hacktivists

Monetary Gain ● Organized criminals with sophisticated tools

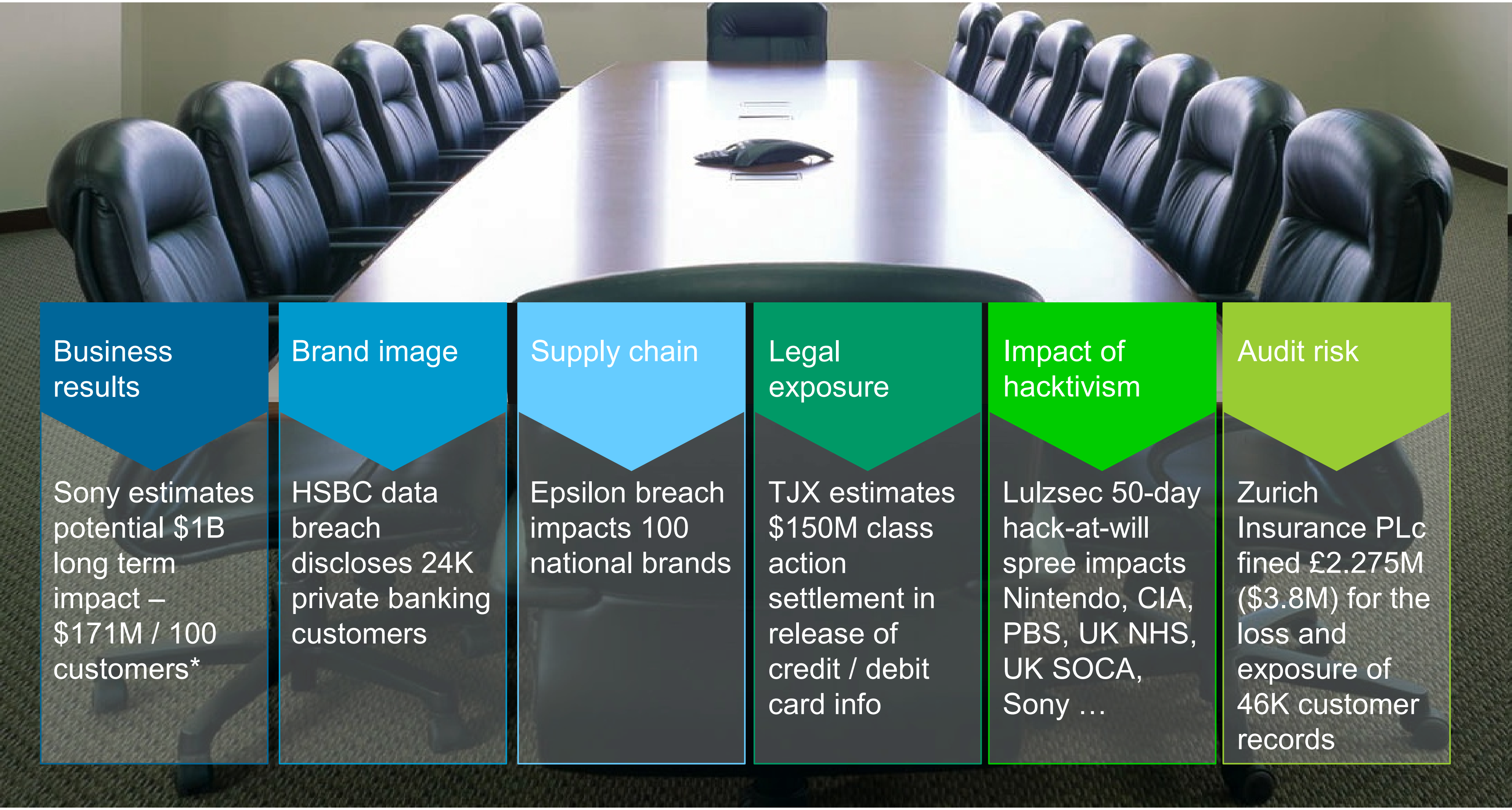
Revenge ● Insiders, using inside information

Curiosity ● Script-kiddies or hackers

Adversary

JK 2012-04-26

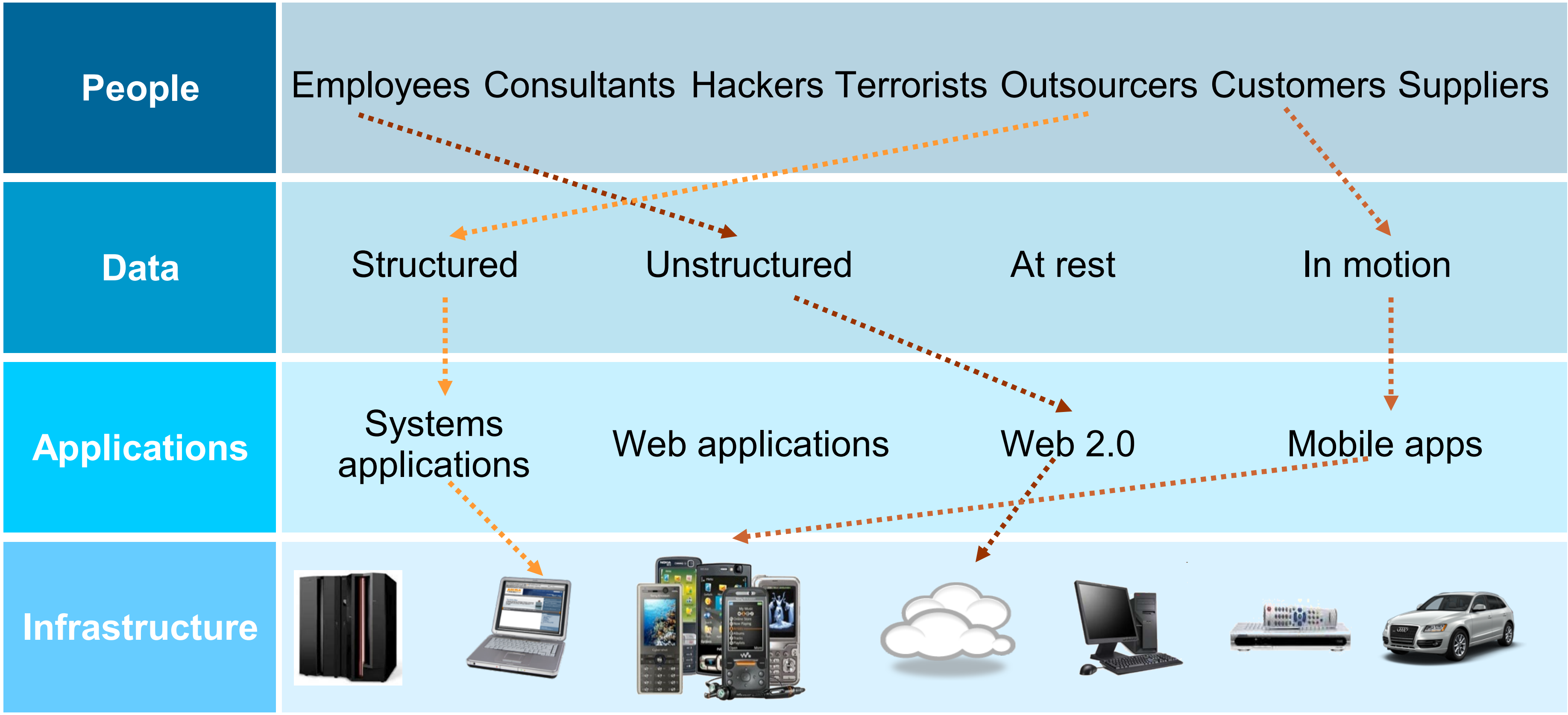
IT Security is a board room discussion



Business results	Brand image	Supply chain	Legal exposure	Impact of hacktivism	Audit risk
Sony estimates potential $1B long term impact – $171M / 100 customers*	HSBC data breach discloses 24K private banking customers	Epsilon breach impacts 100 national brands	TJX estimates $150M class action settlement in release of credit / debit card info	Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony …	Zurich Insurance PLc fined £2.275M ($3.8M) for the loss and exposure of 46K customer records

*Sources for all breaches shown in speaker notes

Solving a security issue is a complex, four-dimensional puzzle



People

Employees Consultants Hackers Terrorists Outsourcers Customers Suppliers

Data

Structured Unstructured At rest In motion

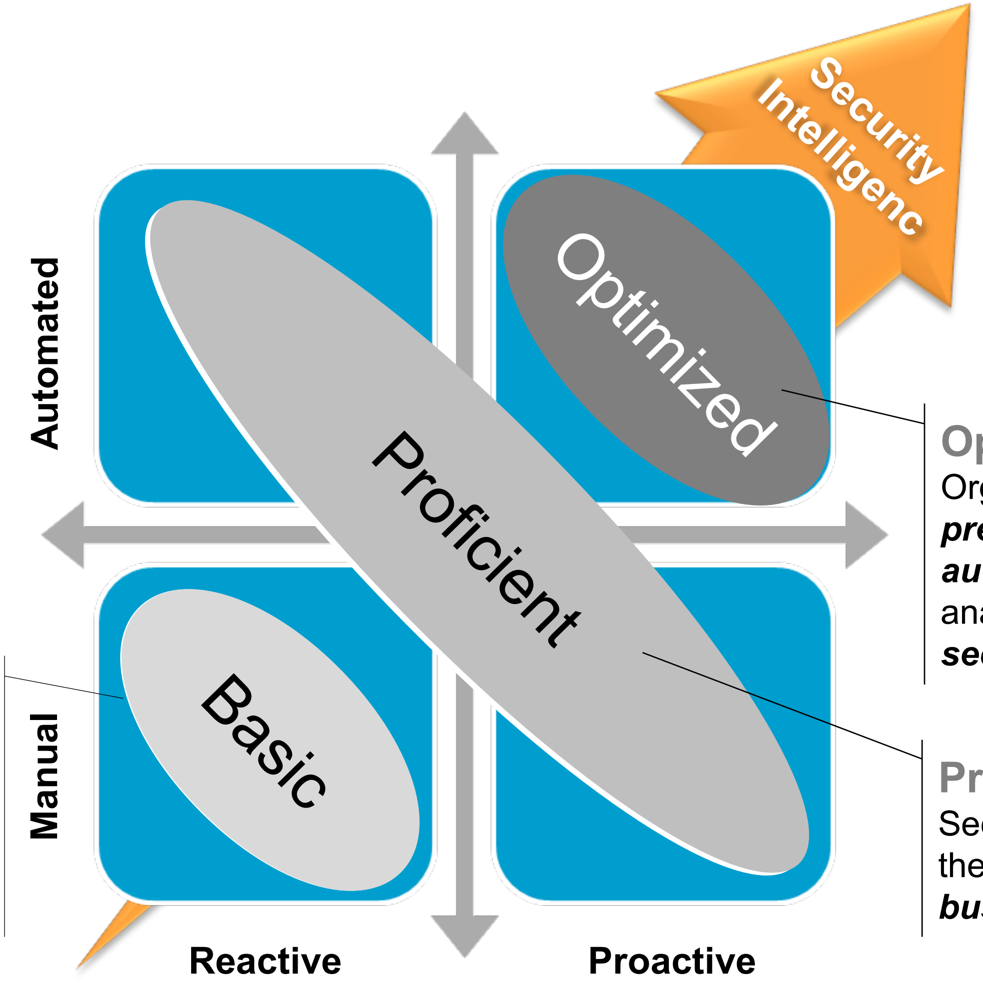
Applications

Systems applications Web applications Web 2.0 Mobile apps

Infrastructure

It is no longer enough to protect the perimeter – silo’d point products will not secure the enterprise

In this “new normal”, organizations need an intelligent view of their security posture

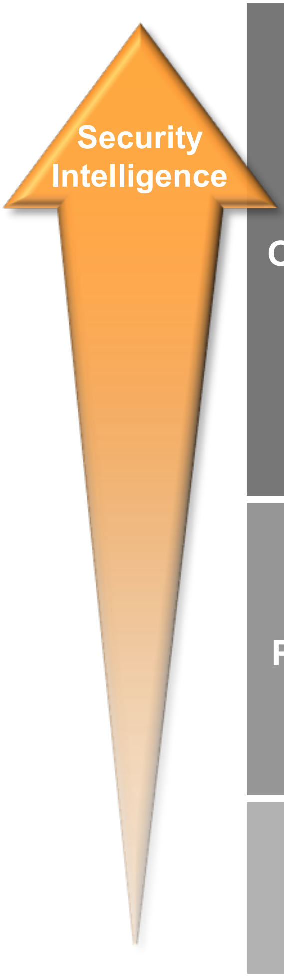


Optimized
Organizations use ***predictive and automated*** security analytics to drive toward ***security intelligence***

Proficient
Security is layered into the ***IT fabric*** and ***business operations***

Basic
Organizations employ ***perimeter protection***, which regulates access and feeds manual reporting

Security Intelligence is enabling progress to optimized security



Security Intelligence:
Information and event management
Advanced correlation and deep analytics
External threat research

	People	Data	Applications	Infrastructure
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

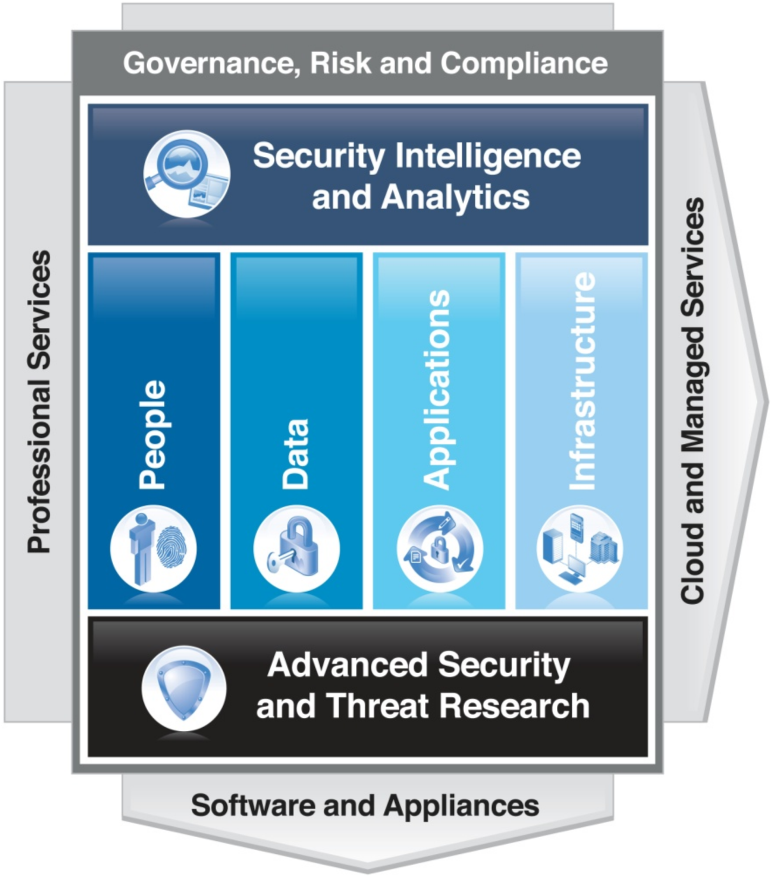
IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

IBM Security Systems

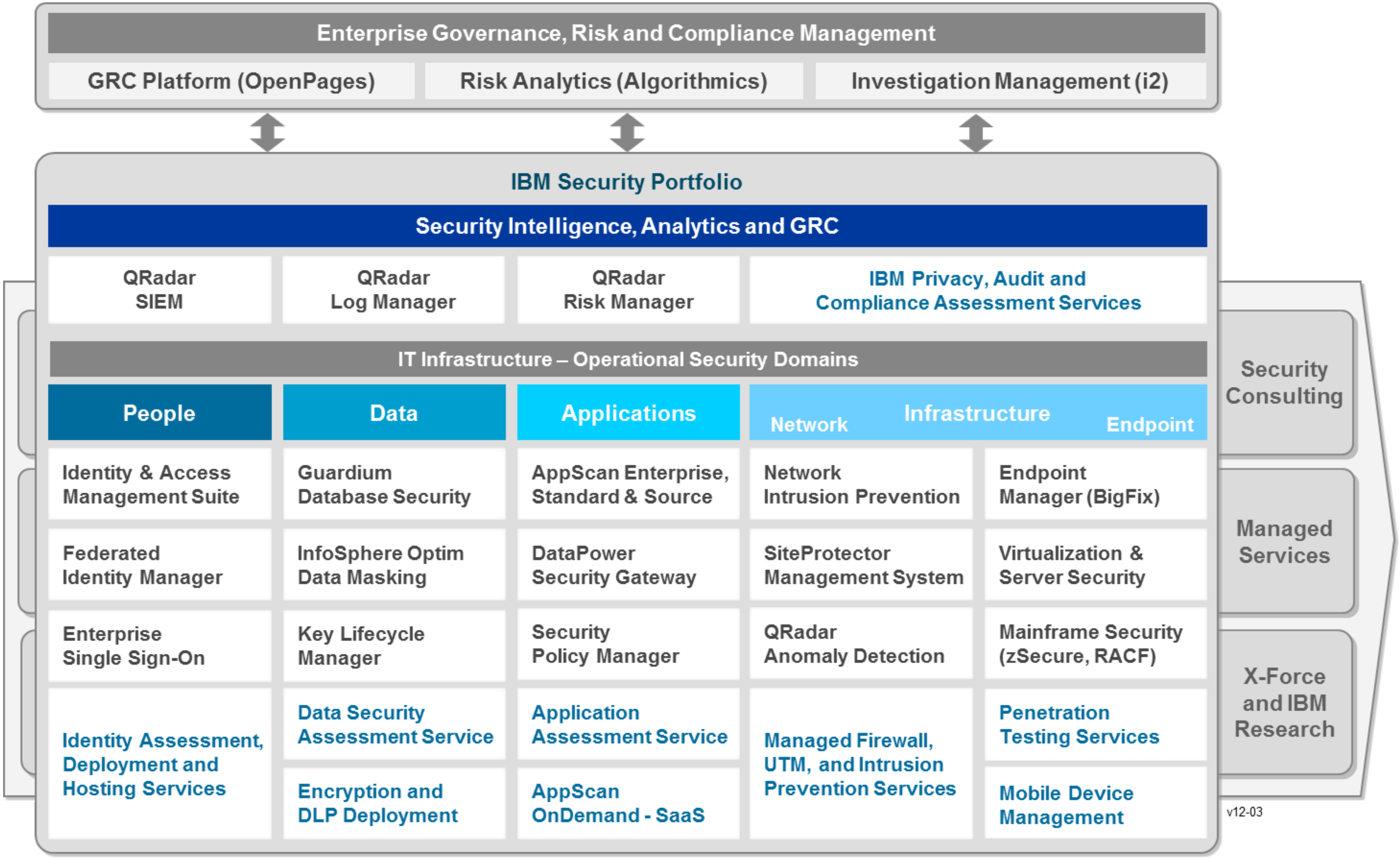
- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

Intelligence • Integration • Expertise

IBM Security Framework


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Intelligence: Leading products and services in every segment



Enterprise Governance, Risk and Compliance Management

GRC Platform (OpenPages) | Risk Analytics (Algorithmics) | Investigation Management (i2)

IBM Security Portfolio

Security Intelligence, Analytics and GRC

QRadar SIEM | QRadar Log Manager | QRadar Risk Manager | IBM Privacy, Audit and Compliance Assessment Services

IT Infrastructure – Operational Security Domains

People	Data	Applications	Infrastructure	
			Network	Endpoint
Identity & Access Management Suite	Guardium Database Security	AppScan Enterprise, Standard & Source	Network Intrusion Prevention	Endpoint Manager (BigFix)
Federated Identity Manager	InfoSphere Optim Data Masking	DataPower Security Gateway	SiteProtector Management System	Virtualization & Server Security
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection	Mainframe Security (zSecure, RACF)
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service	Application Assessment Service	Managed Firewall, UTM, and Intrusion Prevention Services	Penetration Testing Services
	Encryption and DLP Deployment	AppScan OnDemand - SaaS		Mobile Device Management

Security Consulting

Managed Services

X-Force and IBM Research

v12-03

Products Services

Analysts recognize IBM’s superior products and performance

Domain		Report	Analyst Recognition					
Security Intelligence, Analytics and GRC		Security Information & Event Management (SIEM)	2011	★			2010	★
		Enterprise Governance Risk & Compliance Platforms	2011	★	2011	★		
People		User Provisioning / Administration	2011	★			2010	★
		Role Management & Access Recertification			2011	★		
		Enterprise Single Sign-on (ESSO)	2011*	★				
		Web Access Management (WAM)	2011*	★				
Data		Database Auditing & Real-Time Protection			2011	★		
Applications		Static Application Security Testing (SAST)	2010	★			2010	★
		Dynamic Application Security Testing (DAST)	2011	★				
Infrastructure	Network	Network Intrusion Prevention Systems (NIPS)	2010	★			2010	★
	Endpoint	EndPoint Protection Platforms (EPP)	2010	★				

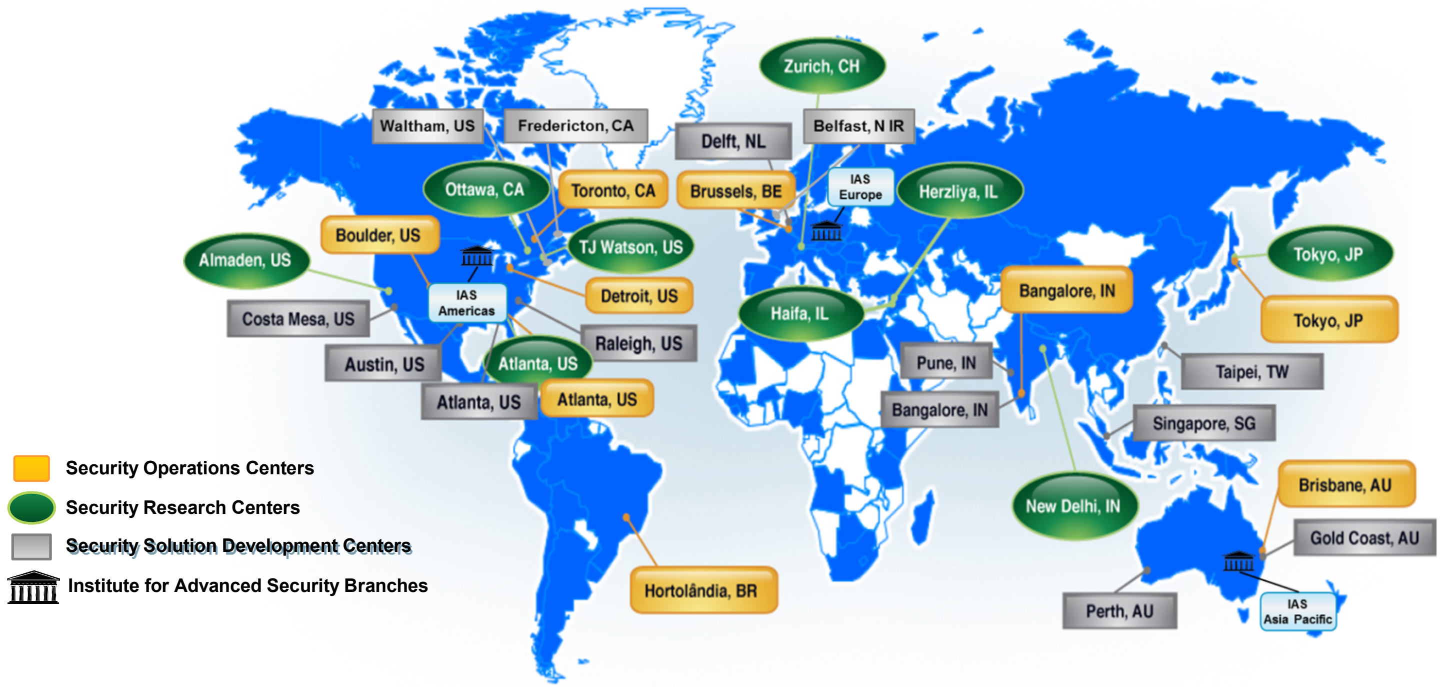
Gartner ★ Challenger ★ Leader ★ Visionary ★ Niche Player

IDC Analyze the Future ★ Leader (#1, 2, or 3 in segment)

FORRESTER ★ Leader ★ Strong Performer ★ Contender

* Gartner MarketScope

Expertise: Unmatched global coverage and security awareness



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

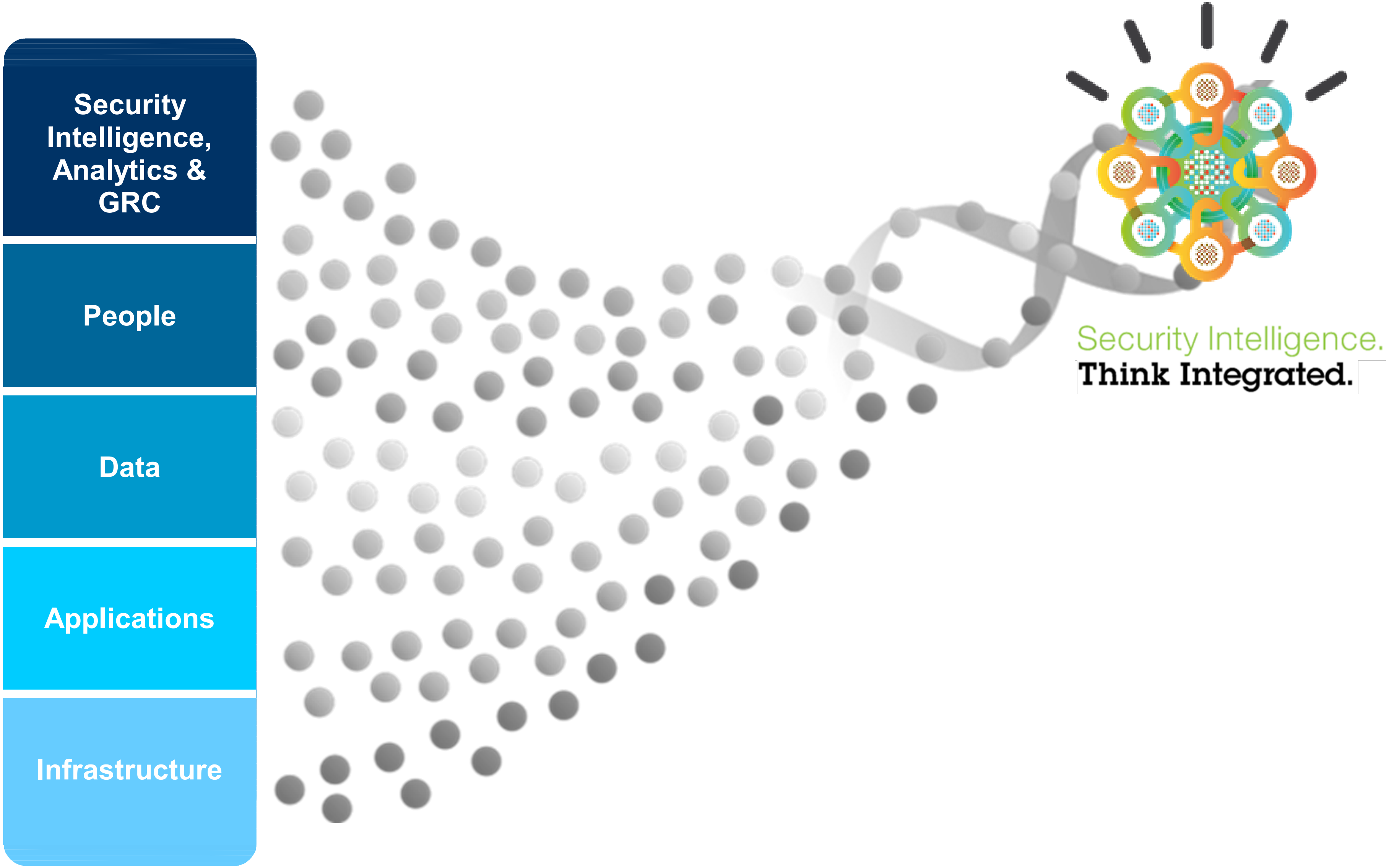
Millions of unique malware samples

X FORCE

World Wide Managed Security Services Coverage

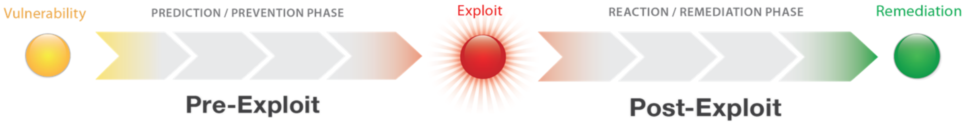
- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 9B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

Intelligent solutions provide the DNA to secure a Smarter Planet



Security Intelligence.
Think Integrated.

Ahead of the Threat



Sukhdev Singh

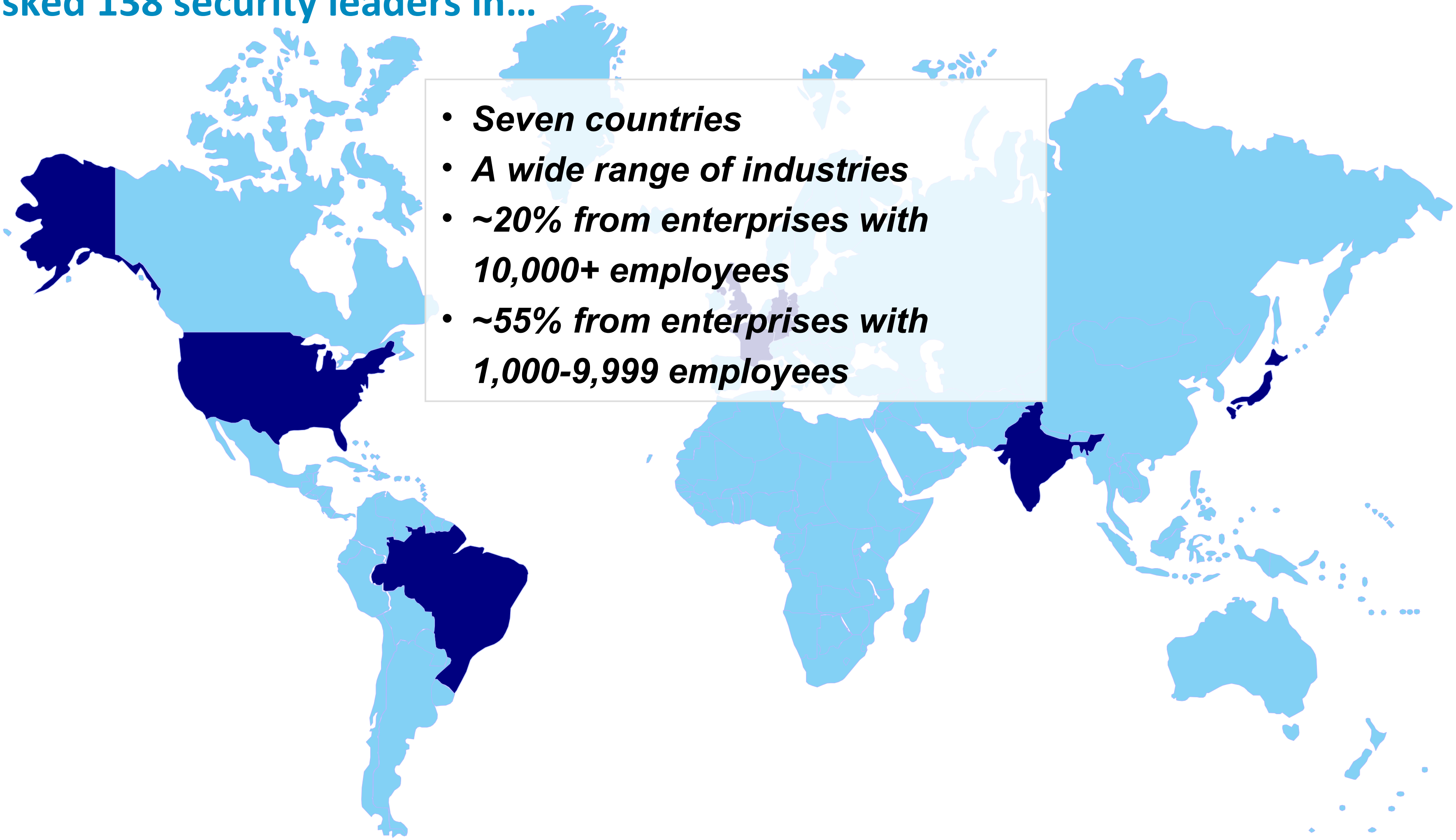
CISSP ,CISSM, X Force Expert, Certified Enterprise Architect …

Technical Leader – Growth Markets, IBM Security Systems

© 2012 IBM Corporation

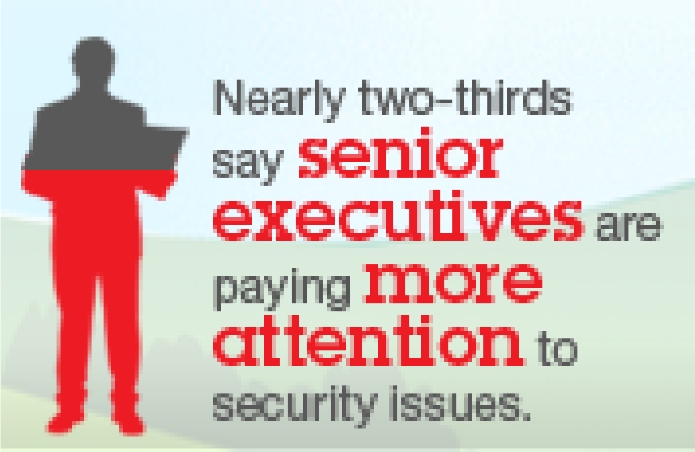
2012 IBM Chief Information Security Officer Assessment

To obtain a global snapshot of security leaders' strategies and approaches, we asked 138 security leaders in…

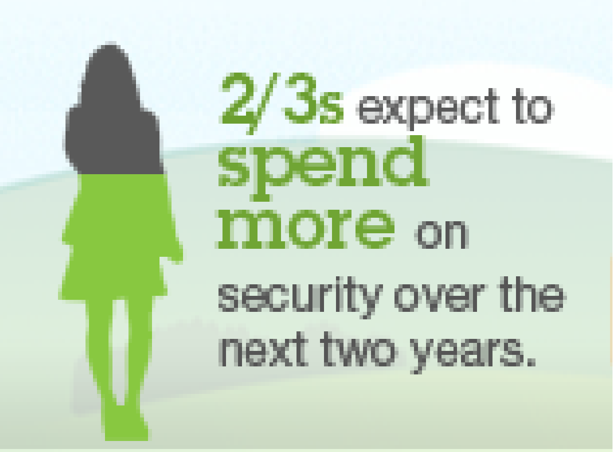


- *Seven countries*
- *A wide range of industries*
- *~20% from enterprises with 10,000+ employees*
- *~55% from enterprises with 1,000-9,999 employees*

Security leaders shared their views on how the security landscape is changing

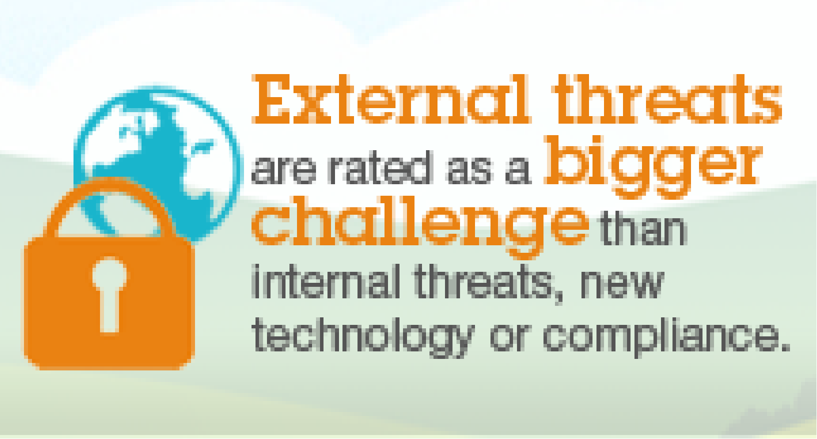


Nearly two-thirds say **senior executives** are paying **more attention** to security issues.

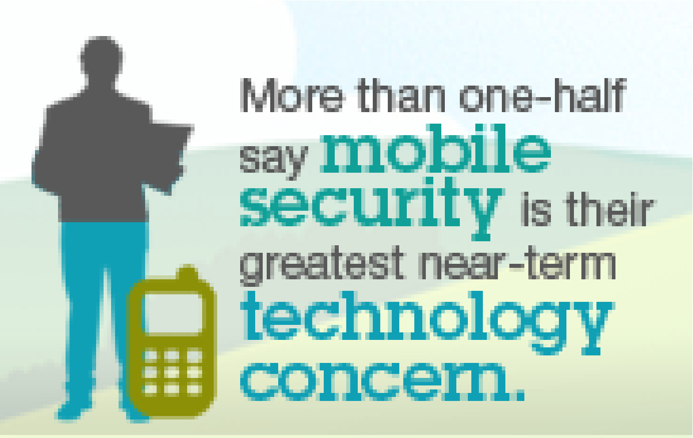


2/3s expect to **spend more** on security over the next two years.

- 87% expect double-digit increases
- 11% expect increases of > 50%.



External threats are rated as a **bigger challenge** than internal threats, new technology or compliance.



More than one-half say **mobile security** is their greatest near-term **technology concern.**

Source: IBM Center for Applied Insights

X-Force research

One of the most renowned commercial security research & development groups in the world

The mission of the IBM X-Force® research and development team is to:

- **Research and evaluate threat and protection issues**
- **Deliver security protection for today's security problems**
- **Develop new technology for tomorrow's security challenges**
- **Educate the media and user communities**

X FORCE

X-Force Research

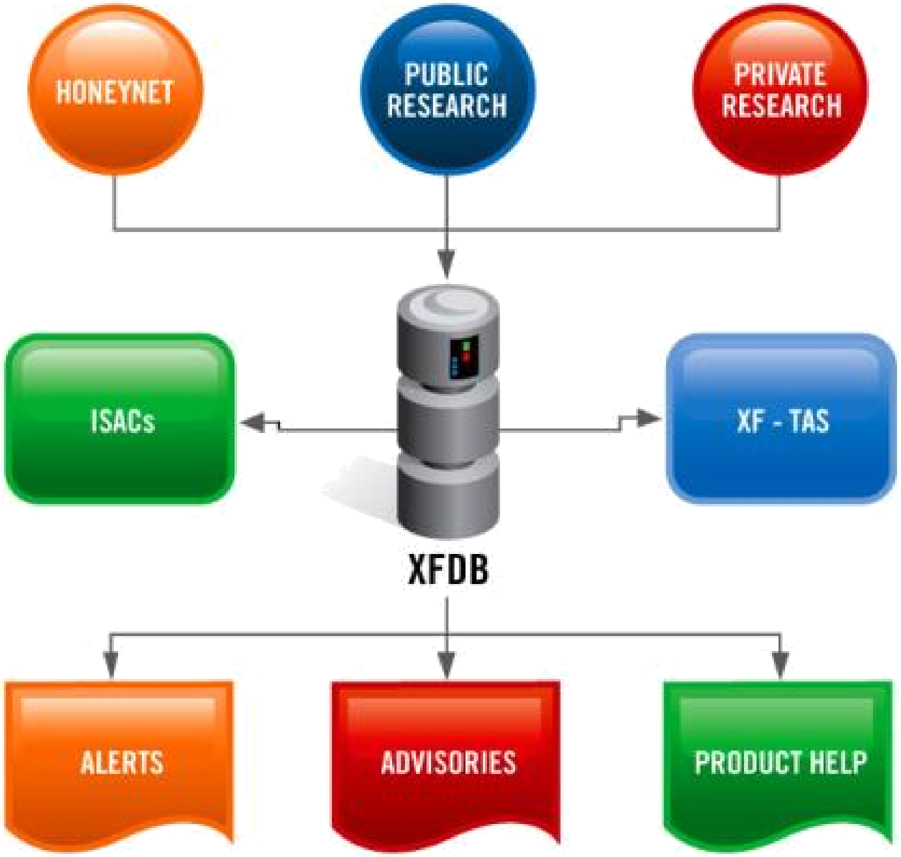
14B	analyzed Web pages & images
40M	spam & phishing attacks
60K	documented vulnerabilities
13B	security events daily

Provides Specific Analysis of:

- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

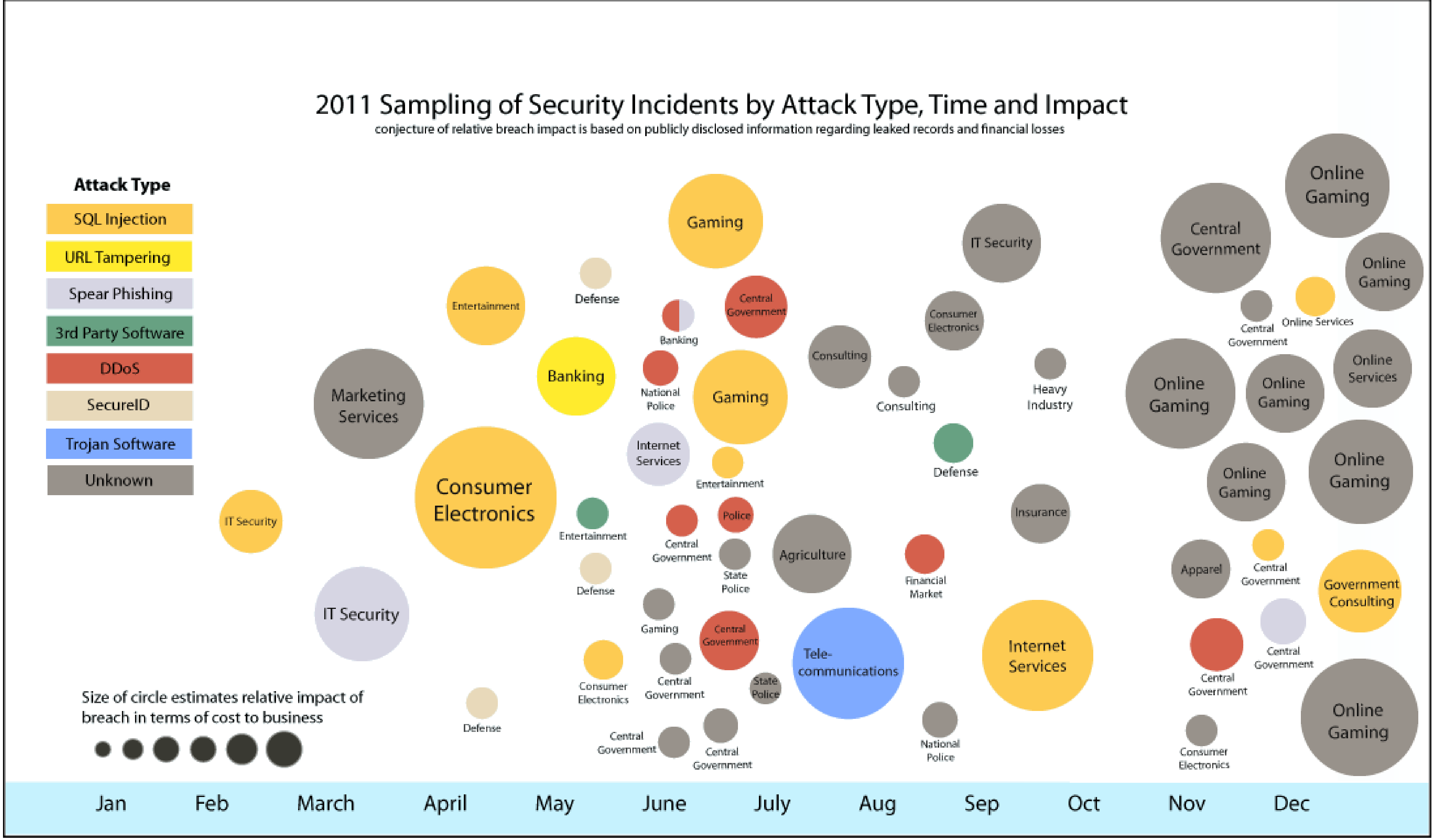
We analyze them all…

- Most comprehensive Vulnerability Database in the world
  - Over **65,000** unique vulnerabilities cataloged
  - Entries date back to the 1990's
- Updated daily by a dedicated research team
- The X-Force database currently tracks over...
  - 8000 Vendors
  - 17,000 Products
  - 40,000 Versions



Cyber breaches are having a growing impact

2011 Sampling of Security Breaches by Attack Type, Time and Impact



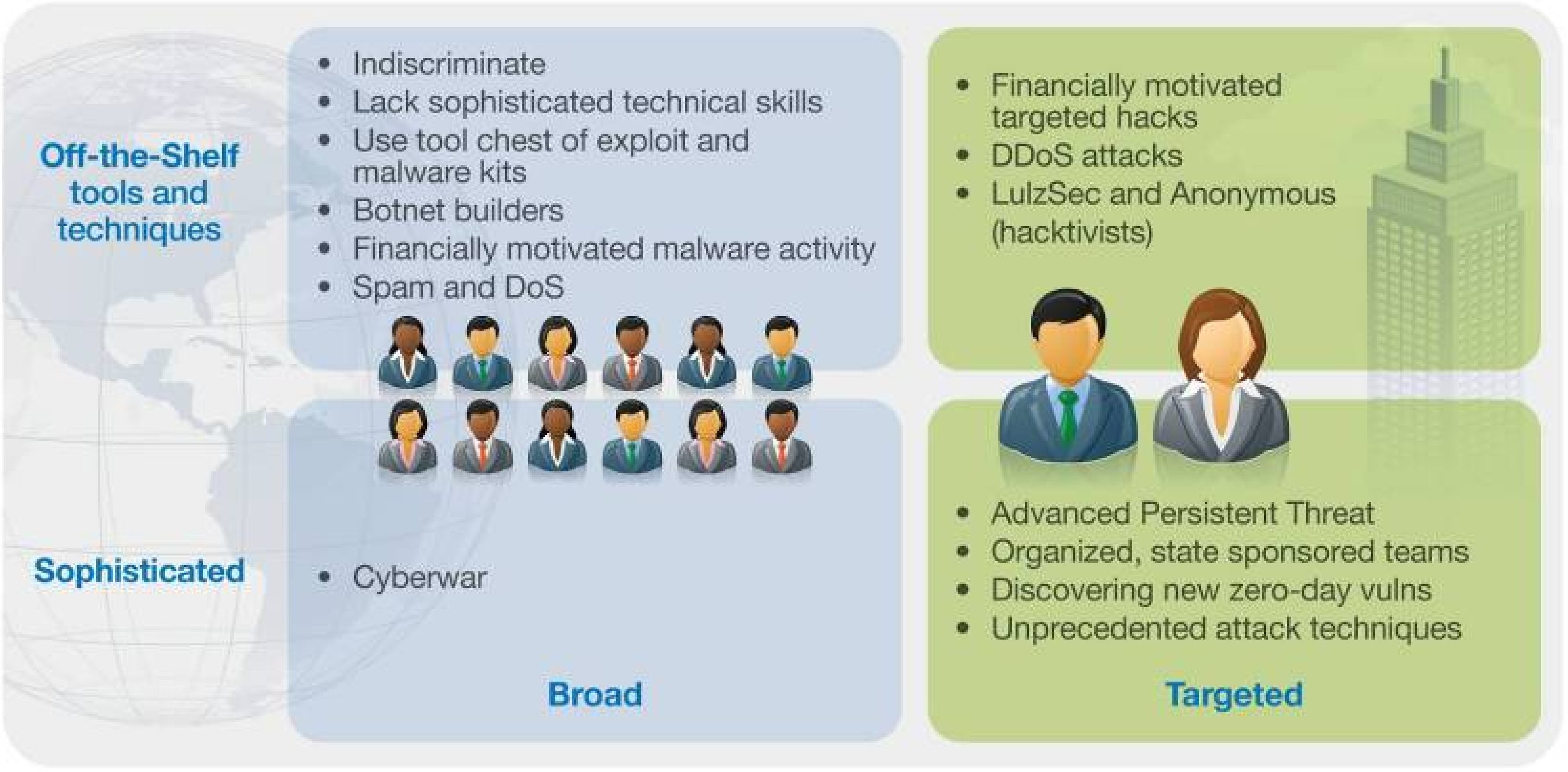
2011 Sampling of Security Incidents by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

"The Year of the Security Breach" – IBM's X-Force® R&D

Who is attacking our networks?

Attacker Types and Techniques 2011



Off-the-Shelf tools and techniques

- Indiscriminate
- Lack sophisticated technical skills
- Use tool chest of exploit and malware kits
- Botnet builders
- Financially motivated malware activity
- Spam and DoS

- Financially motivated targeted hacks
- DDoS attacks
- LulzSec and Anonymous (hacktivists)

Sophisticated

- Cyberwar

- Advanced Persistent Threat
- Organized, state sponsored teams
- Discovering new zero-day vulns
- Unprecedented attack techniques

Broad

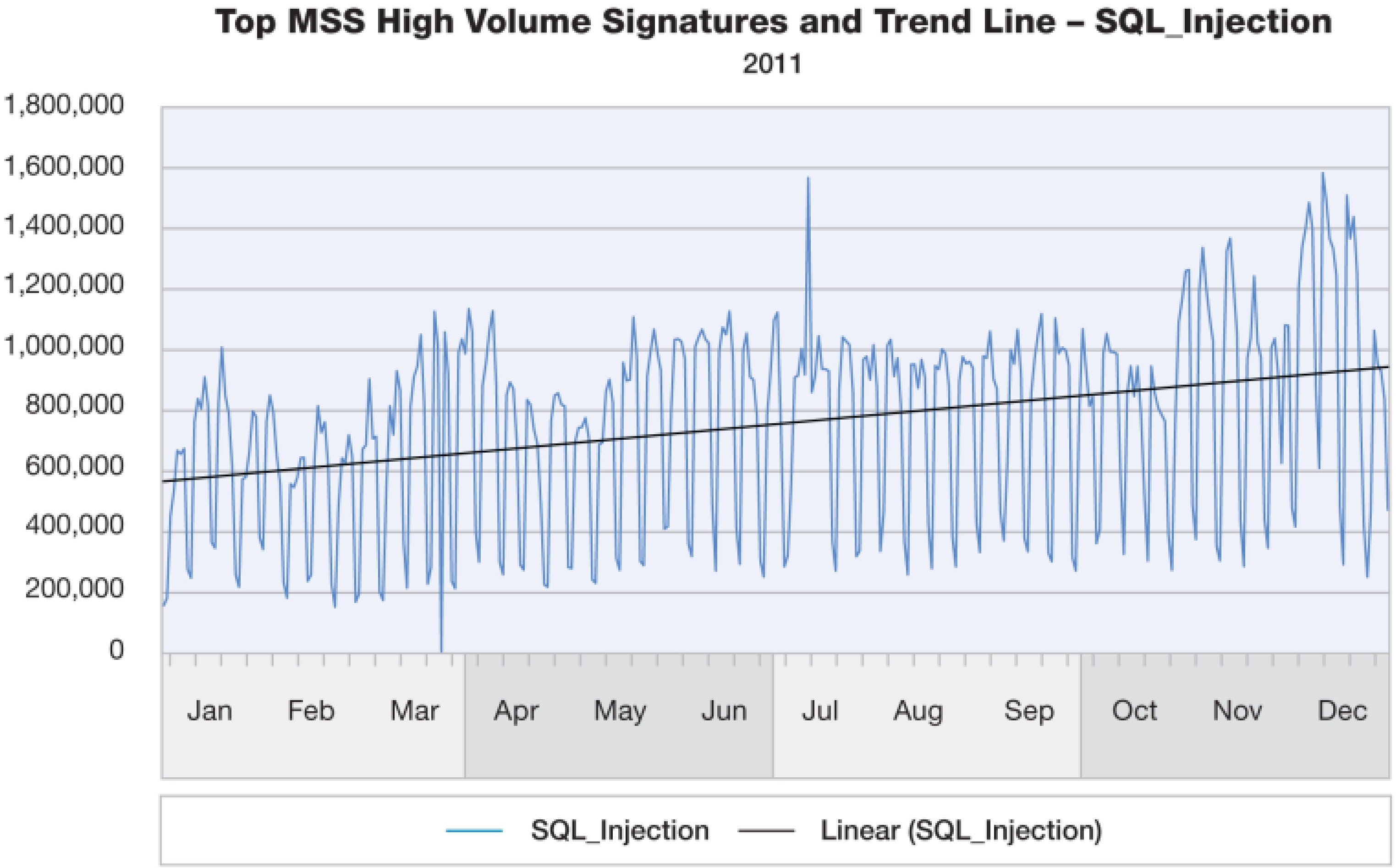
Targeted

Source: IBM X-Force® Research and Development

Key Messages from the 2011 Trend Report

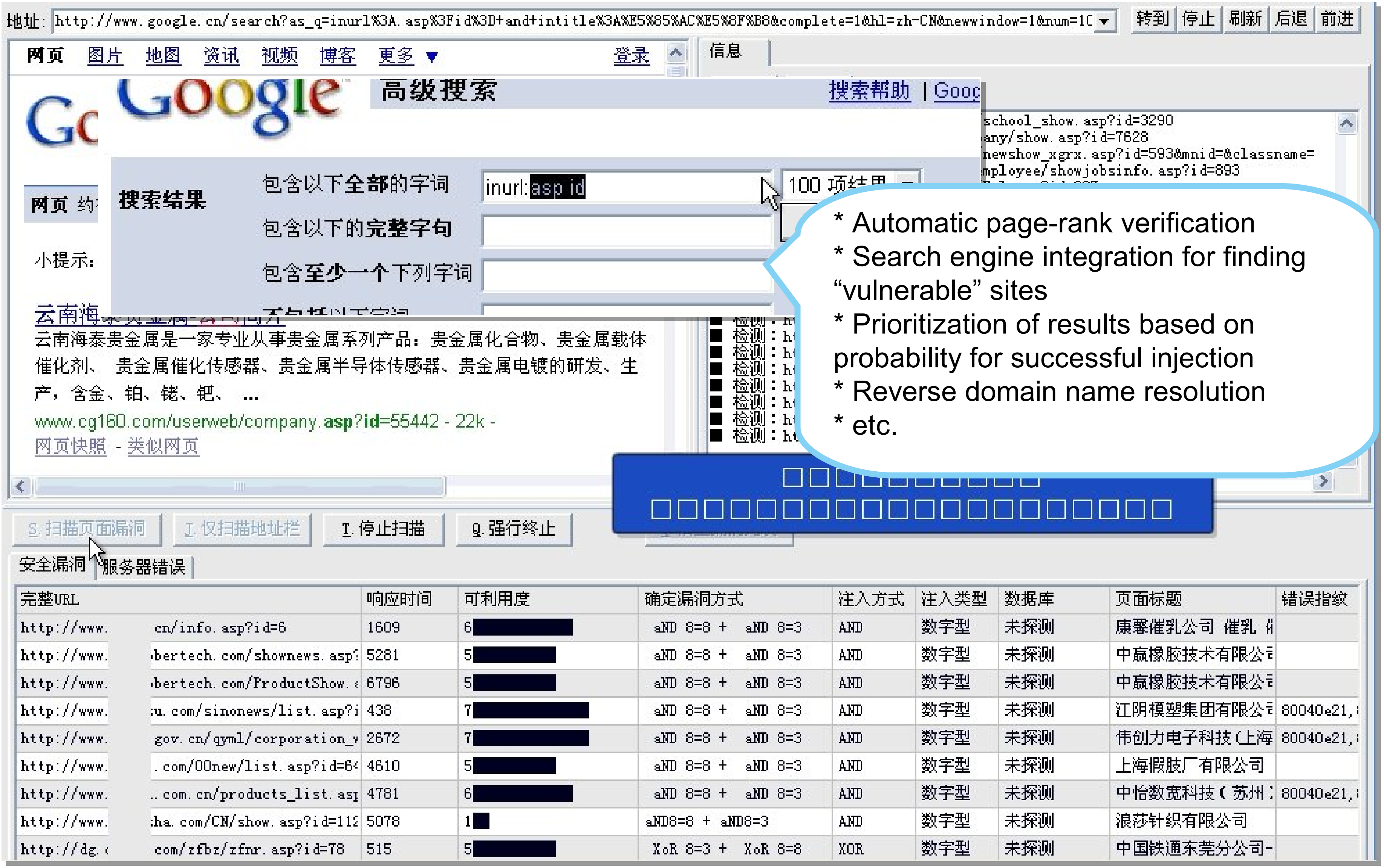
- New Attack Activity
  - Rise in Shell Command Injection attacks
  - Spikes in SSH Brute Forcing
  - Rise in phishing based malware distribution and click fraud
- Progress in Internet Security
  - Fewer exploit releases
  - Fewer web application vulnerabilities
  - Better patching
- The Challenge of Mobile and the Cloud
  - Mobile exploit disclosures up
  - Cloud requires new thinking
  - Social Networking no longer fringe pastime

SQL injection attacks against web servers



Source: IBM X-Force® Research and Development

SQL Injection Attack Tools



转到 | 停止 | 刷新 | 后退 | 前进
网页 图片 地图 资讯 视频 博客 更多 ▼ 登录
信息
Google 高级搜索
搜索帮助 | Goog
网页 约
小提示:
S.扫描页面漏洞 | I.仅扫描地址栏 | T.停止扫描 | Q.强行终止
安全漏洞 | 服务器错误

地址: http://www.google.cn/search?as_q=inurl%3A.asp%3Fid%3D+and+intitle%3A%E5%85%AC%E5%8F%B8&complete=1&hl=zh-CN&newwindow=1&num=1C

搜索结果

包含以下全部的字词: inurl:asp id

包含以下的完整字句:

包含至少一个下列字词:

100 项结果

云南海泰贵金属是一家专业从事贵金属系列产品：贵金属化合物、贵金属载体催化剂、 贵金属催化传感器、贵金属半导体传感器、贵金属电镀的研发、生产，含金、铂、铑、钯、 ...

www.cg160.com/userweb/company.asp?id=55442 - 22k -

网页快照 - 类似网页

```
school_show.asp?id=3290
any/show.asp?id=7628
newshow_xgrx.asp?id=593&mnid=&classname=
mployee/showjobsinfo.asp?id=893
```

完整URL	响应时间	可利用度	确定漏洞方式	注入方式	注入类型	数据库	页面标题	错误指纹
http://www.　cn/info.asp?id=6	1609	6 ■	aND 8=8 + aND 8=3	AND	数字型	未探测	康馨催乳公司 催乳 催	
http://www.　bertech.com/shownews.asp?	5281	5 ■	aND 8=8 + aND 8=3	AND	数字型	未探测	中赢橡胶技术有限公司	
http://www.　bertech.com/ProductShow.a	6796	5 ■	aND 8=8 + aND 8=3	AND	数字型	未探测	中赢橡胶技术有限公司	
http://www.　u.com/sinonews/list.asp?i	438	7 ■	aND 8=8 + aND 8=3	AND	数字型	未探测	江阴模塑集团有限公司	80040e21,
http://www.　gov.cn/qyml/corporation_v	2672	7 ■	aND 8=8 + aND 8=3	AND	数字型	未探测	伟创力电子科技(上海	80040e21,
http://www.　.com/00new/list.asp?id=64	4610	5 ■	aND 8=8 + aND 8=3	AND	数字型	未探测	上海假肢厂有限公司	
http://www.　..com.cn/products_list.asp	4781	6 ■	aND 8=8 + aND 8=3	AND	数字型	未探测	中怡数宽科技(苏州)	80040e21,
http://www.　ha.com/CN/show.asp?id=112	5078	1 ■	aND8=8 + aND8=3	AND	数字型	未探测	浪莎针织有限公司	
http://dg.　com/zfbz/zfnr.asp?id=78	515	5 ■	XoR 8=3 + XoR 8=8	XOR	数字型	未探测	中国铁通东莞分公司-	

* Automatic page-rank verification

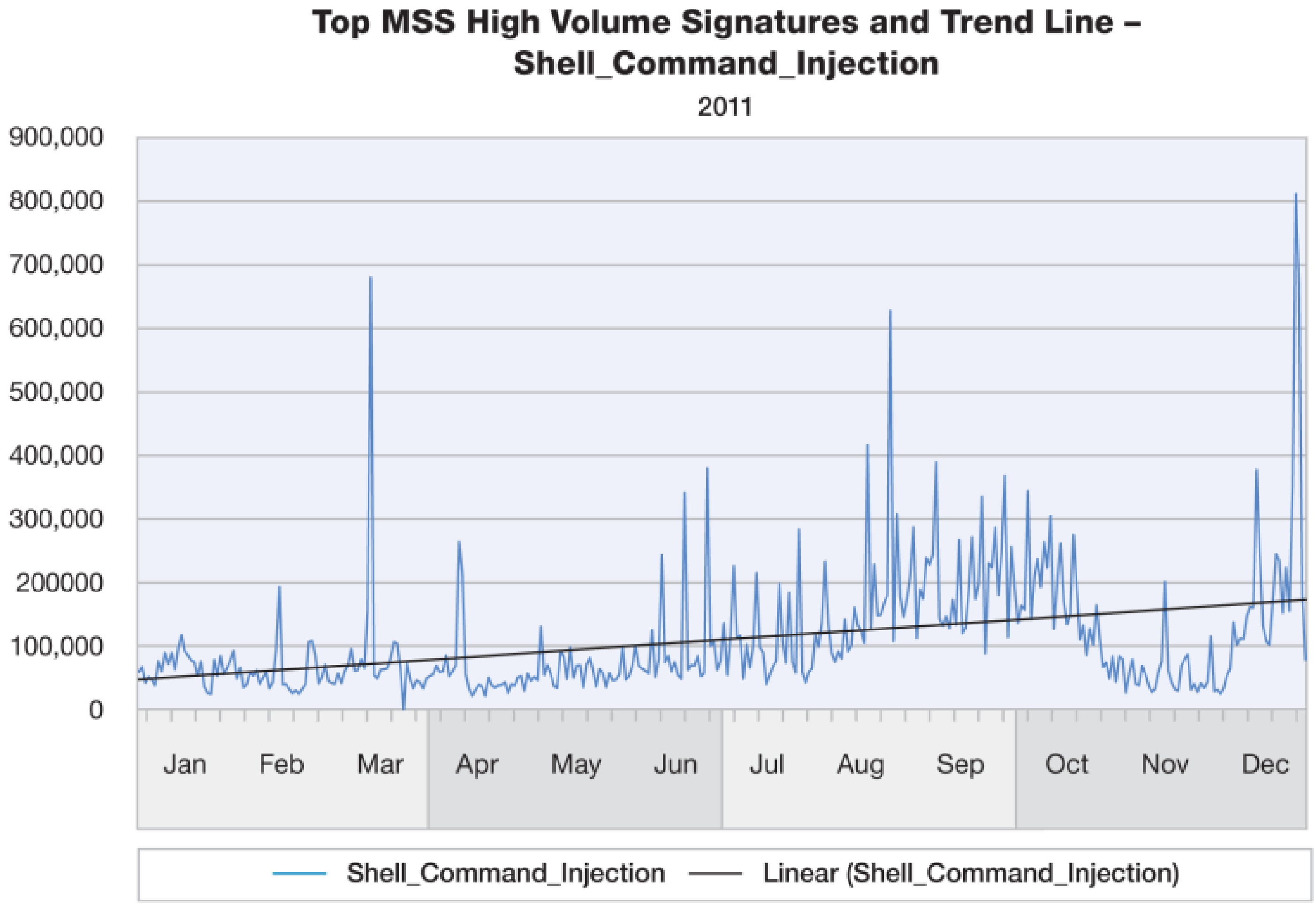
* Search engine integration for finding "vulnerable" sites

* Prioritization of results based on probability for successful injection

* Reverse domain name resolution

* etc.

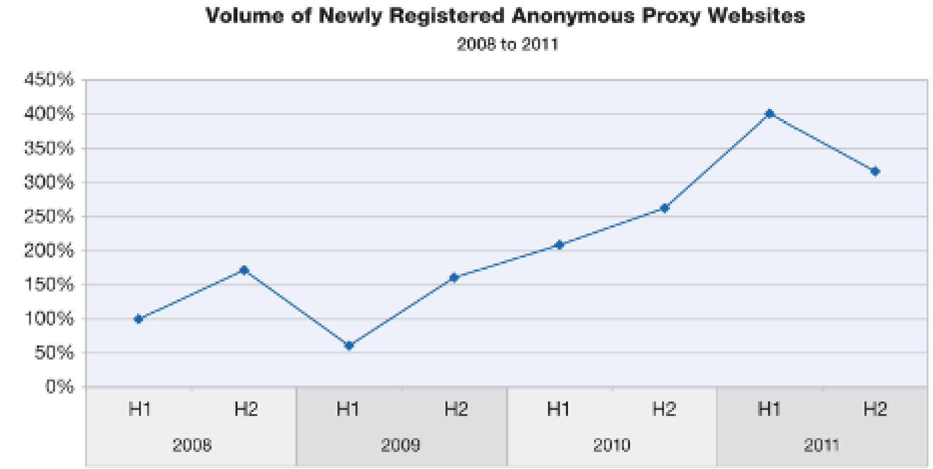
Shell Command Injection attacks



Source: IBM X-Force® Research and Development

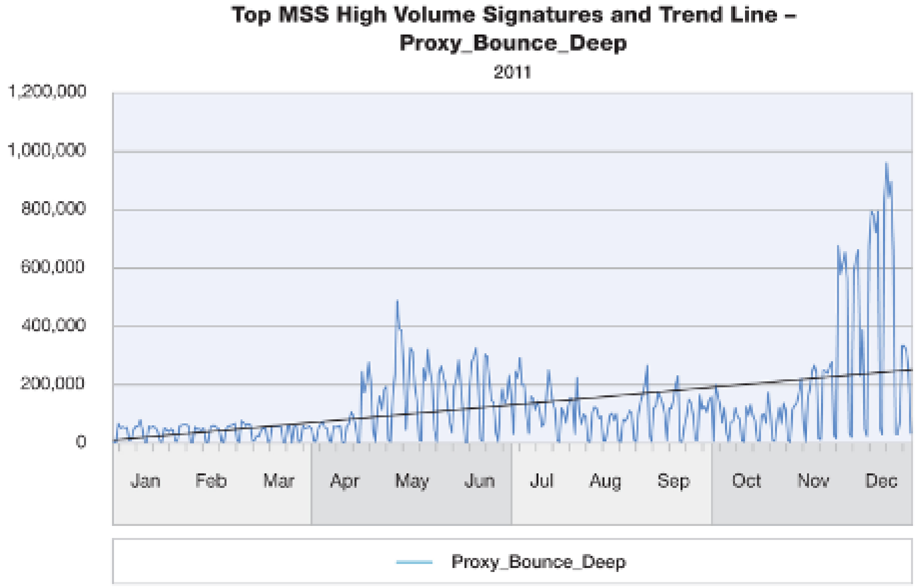
Anonymous proxies on the rise

- Approximately 4 times more anonymous proxies than seen 3 years ago
- Some used to hide attacks, others to evade censorship



Source: IBM X-Force® Research and Development

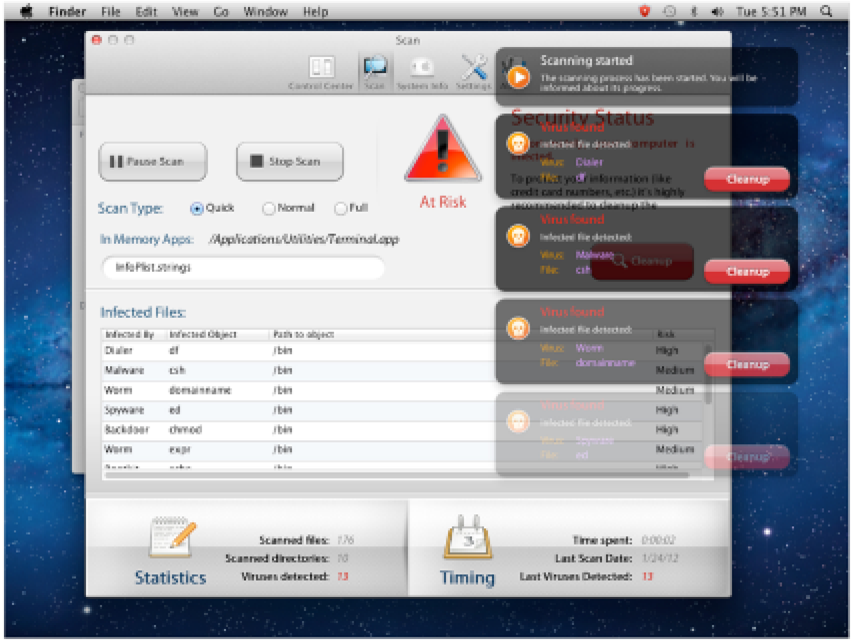
- Signature detects situations where clients are attempting to access websites through a chain of HTTP proxies
- Could represent
  - legitimate (paranoid) web surfing
  - attackers obfuscating the source address of launched attacks against web servers



Source: IBM X-Force® Research and Development

MAC malware

- 2011 has seen the most activity in the Mac malware world.
  - Not only in volume compared to previous years, but also in functionality.
- In 2011, we started seeing Mac malware with functionalities that we've only seen before in Windows® malware.



Scan Type: ● Quick ○ Normal ○ Full

In Memory Apps: /Applications/Utilities/Terminal.app

InfoPlist.strings

Infected Files:

Infected By	Infected Object	Path to object	Risk
Dialer	df	/bin	High
Malware	csh	/bin	Medium
Worm	domainname	/bin	Medium
Spyware	ed	/bin	High
Backdoor	chmod	/bin	High
Worm	expr	/bin	Medium

Scanning started

The scanning process has been started. You will be informed about its progress.

Security Status

Virus found

Infected file detected:

Virus: Dialer

File: df

Virus found

Infected file detected:

Virus: Malware

File: csh

Virus found

Infected file detected:

Virus: Worm

File: domainname

Virus found

Infected file detected:

Virus: Spyware

File: ed

Scanned files: 176

Scanned directories: 10

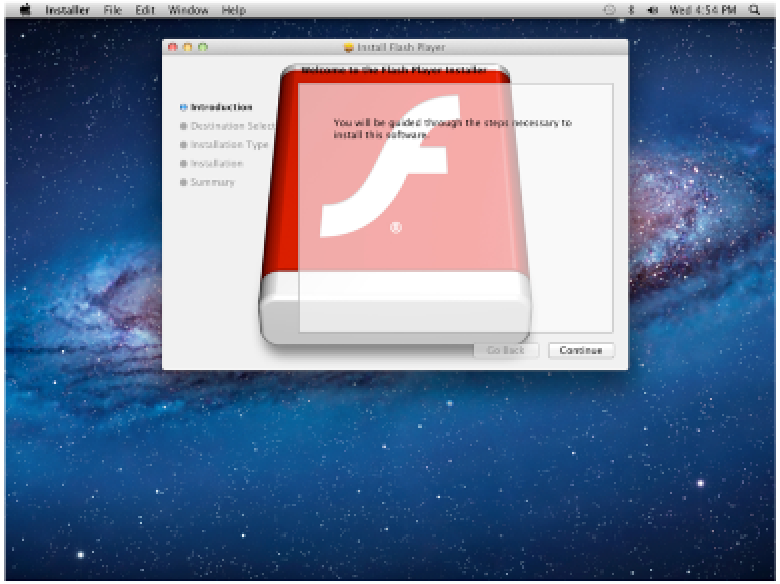
Viruses detected: 13

Time spent: 0:00:02

Last Scan Date: 1/24/12

Last Viruses Detected: 13

Source: IBM X-Force® Research and Development



Welcome to the Flash Player Installer

You will be guided through the steps necessary to install this software.

Source: IBM X-Force® Research and Development

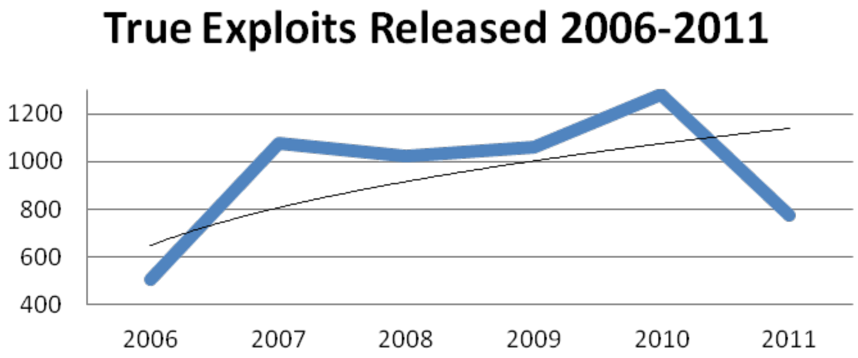
Key Messages from the 2011 Trend Report

- New Attack Activity
  - –Rise in Shell Command Injection attacks
  - Spikes in SSH Brute Forcing
  - Rise in phishing based malware distribution and click fraud
- Progress in Internet Security
  - Fewer exploit releases
  - Fewer web application vulnerabilities
  - Better patching
- The Challenge of Mobile and the Cloud
  - Mobile exploit disclosures up
  - Cloud requires new thinking
  - Social Networking no longer fringe pastime

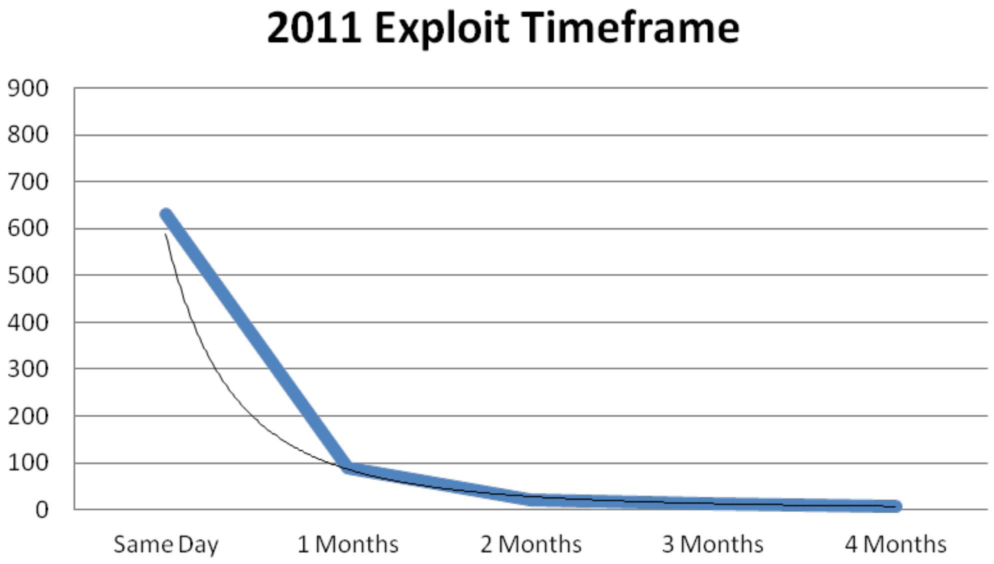
We Track All Public Exploits…

Public exploit disclosures up in 2010 down in 2011

- Approximately 14.9% of the vulnerabilities disclosed in 2010 had public exploits, which is down slightly from the **15.7%** 2009.
- **2011** has seen less public exploits than 1H 2010
- The vast majority of public exploits are released the same day or in conjunction with public disclosure of the vulnerability.


True Exploits Released 2006-2011

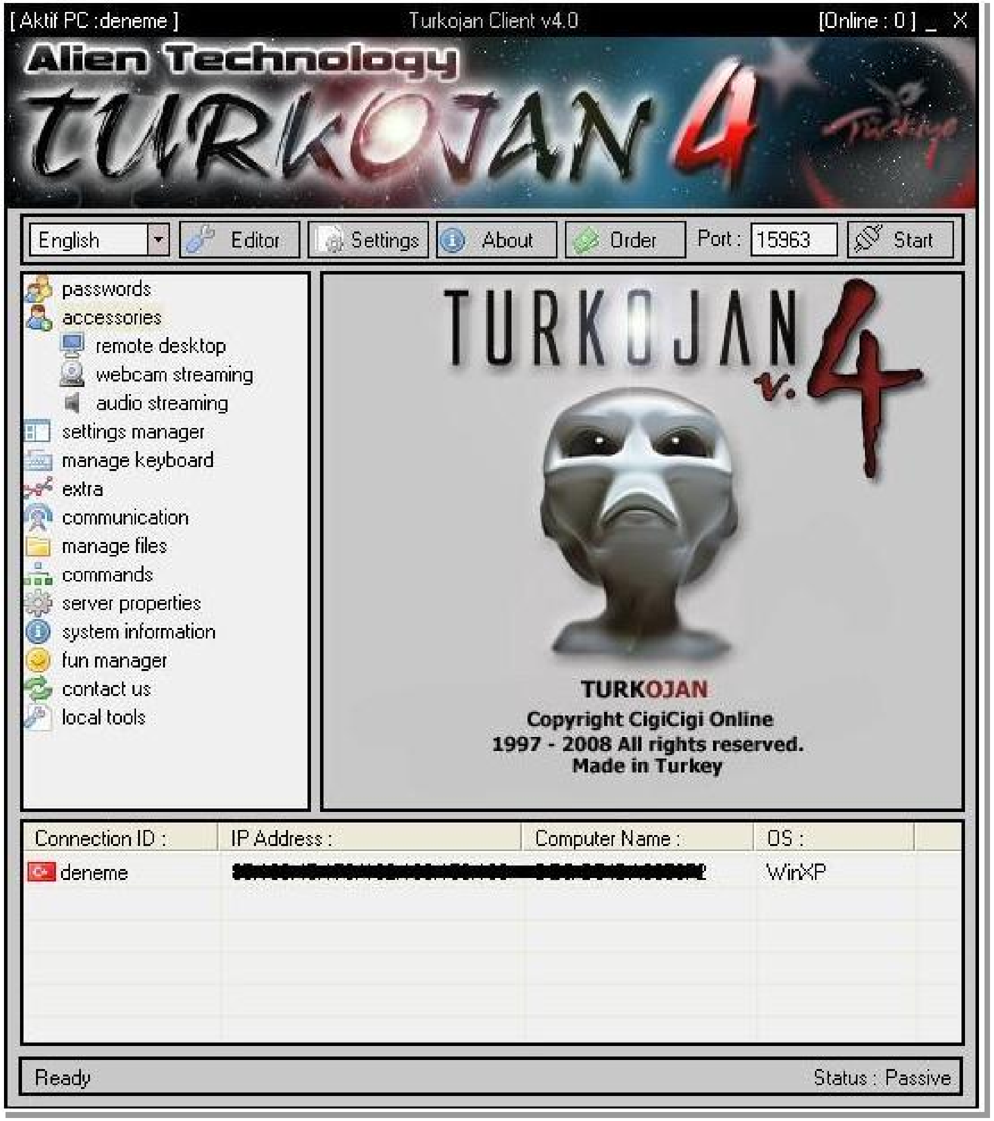
True Exploits	504	1078	1025	1059	1280	778
Percentage of Total	7.3%	16.5%	13.4%	15.7%	14.9%	11.0%


2011 Exploit Timeframe

Exploit Timing	0 Days	1 Month	2 Months	3 Months	4 Months
0 Days	852	308	23	12	6

Turkojan – 1997 and still going strong

- Constructor/Turkojan
- V.4 New features
  - Remote Desktop
  - Webcam Streaming
  - Audio Streaming
  - Remote passwords
  - MSN Sniffer
  - Remote Shell
  - Advanced File Manager
  - Online & Offline keylogger
  - Information about remote computer
  - Etc..



[Aktif PC :deneme] Turkojan Client v4.0 [Online : 0]

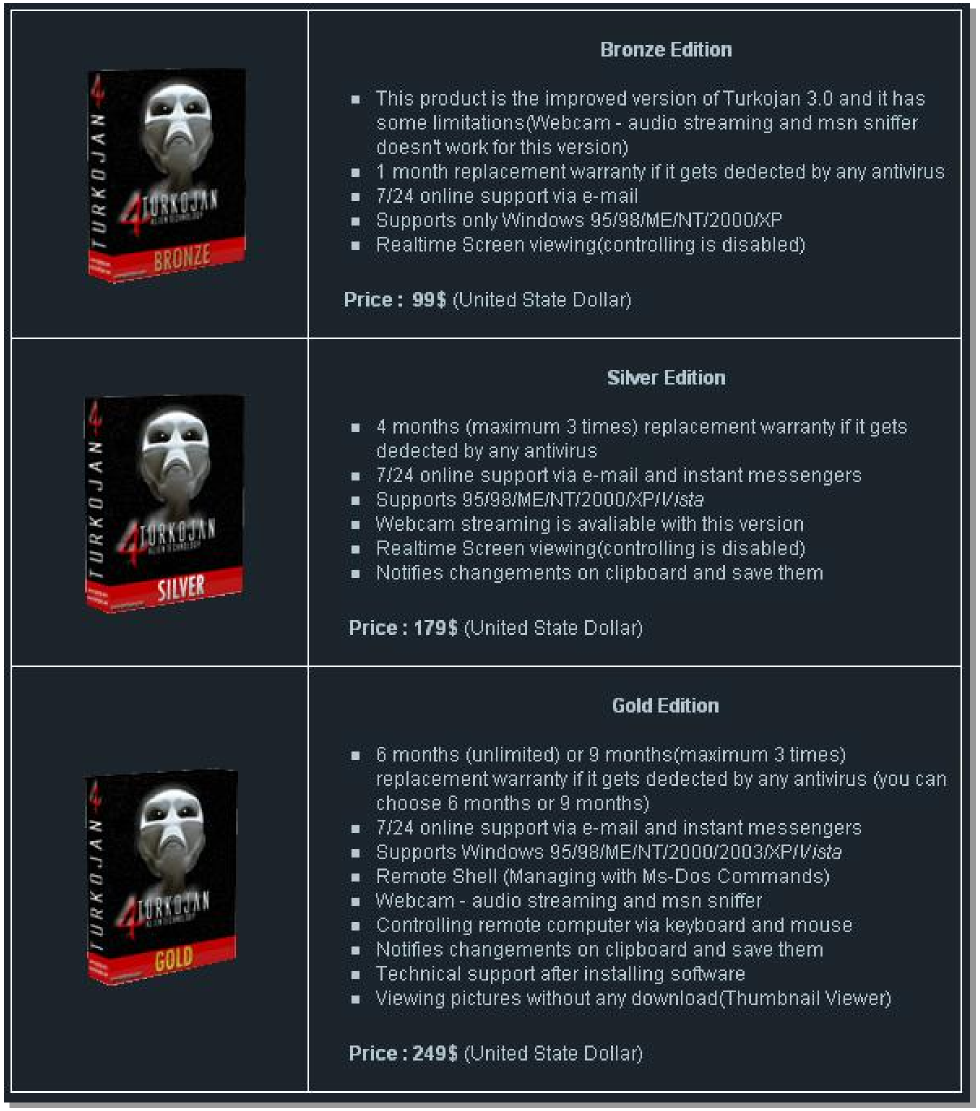
Port : 15963

TURKOJAN
Copyright CigiCigi Online
1997 - 2008 All rights reserved.
Made in Turkey

Connection ID :	IP Address :	Computer Name :	OS :
deneme	[redacted]		WinXP

Ready Status : Passive

It’s just business…



Bronze Edition

- This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)
- 1 month replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail
- Supports only Windows 95/98/ME/NT/2000/XP
- Realtime Screen viewing(controlling is disabled)

Price : 99$ (United State Dollar)

Silver Edition

- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/*Vista*
- Webcam streaming is avaliable with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies changements on clipboard and save them

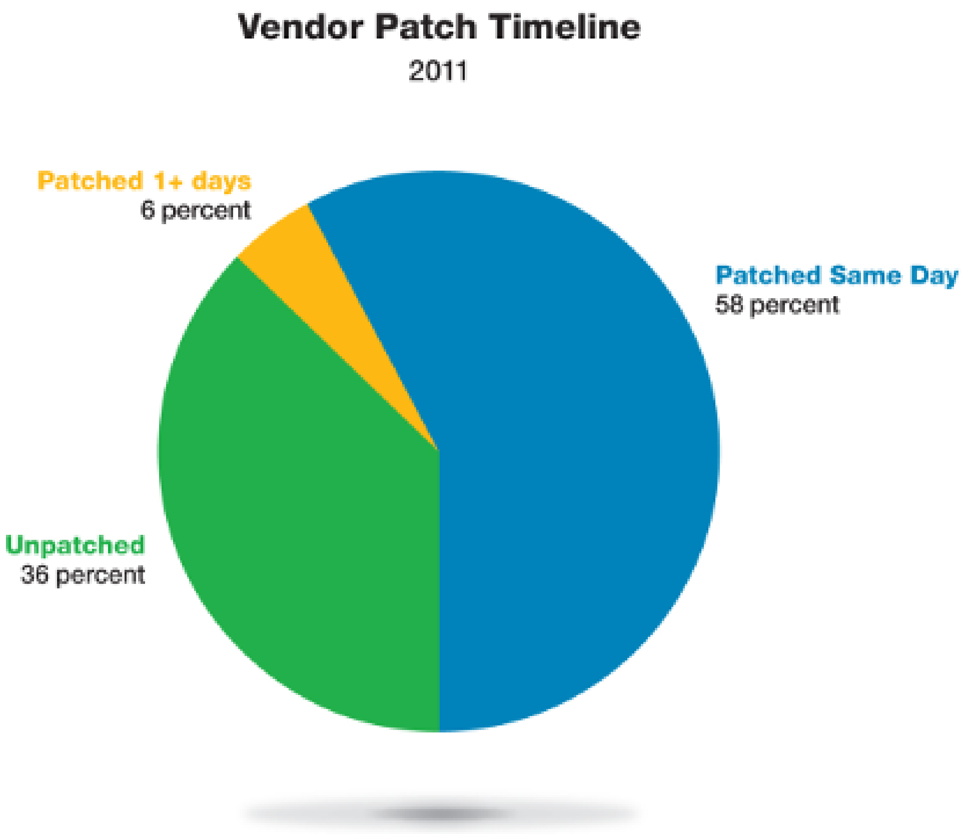
Price : 179$ (United State Dollar)

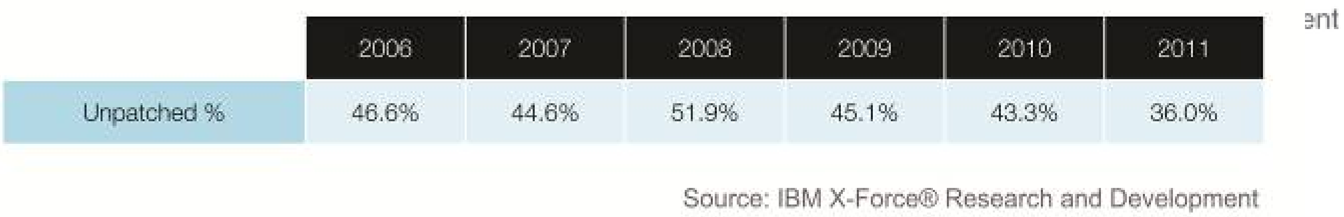
Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/*Vista*
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249$ (United State Dollar)

Better patching





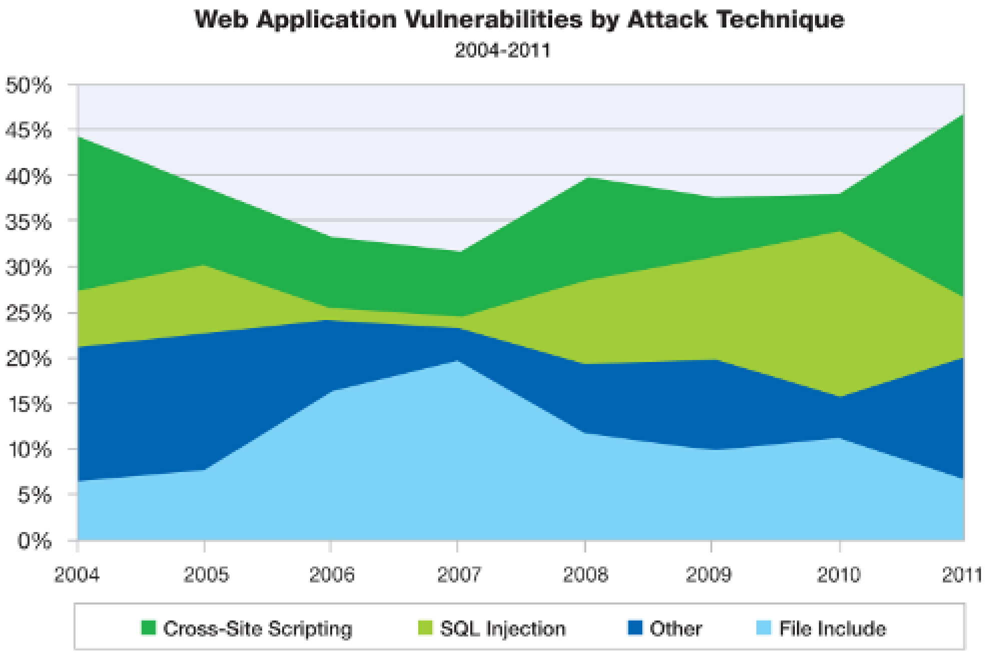
ent

	2006	2007	2008	2009	2010	2011
Unpatched %	46.6%	44.6%	51.9%	45.1%	43.3%	36.0%

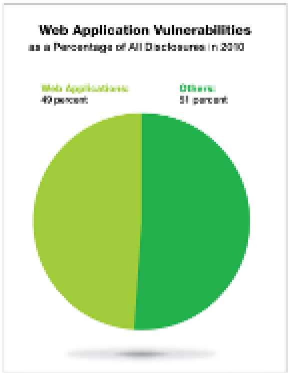
Source: IBM X-Force® Research and Development

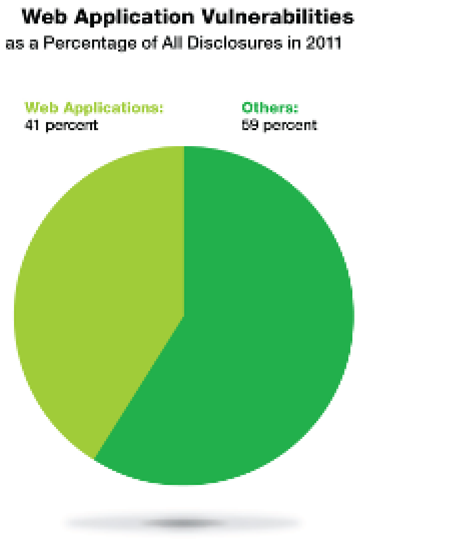
Decline in web application vulnerabilities

- In 2011, 41% of security vulnerabilities affected web applications
  - Down from 49% in 2010
  - Lowest percentage seen since 2005



Source: IBM X-Force® Research and Development

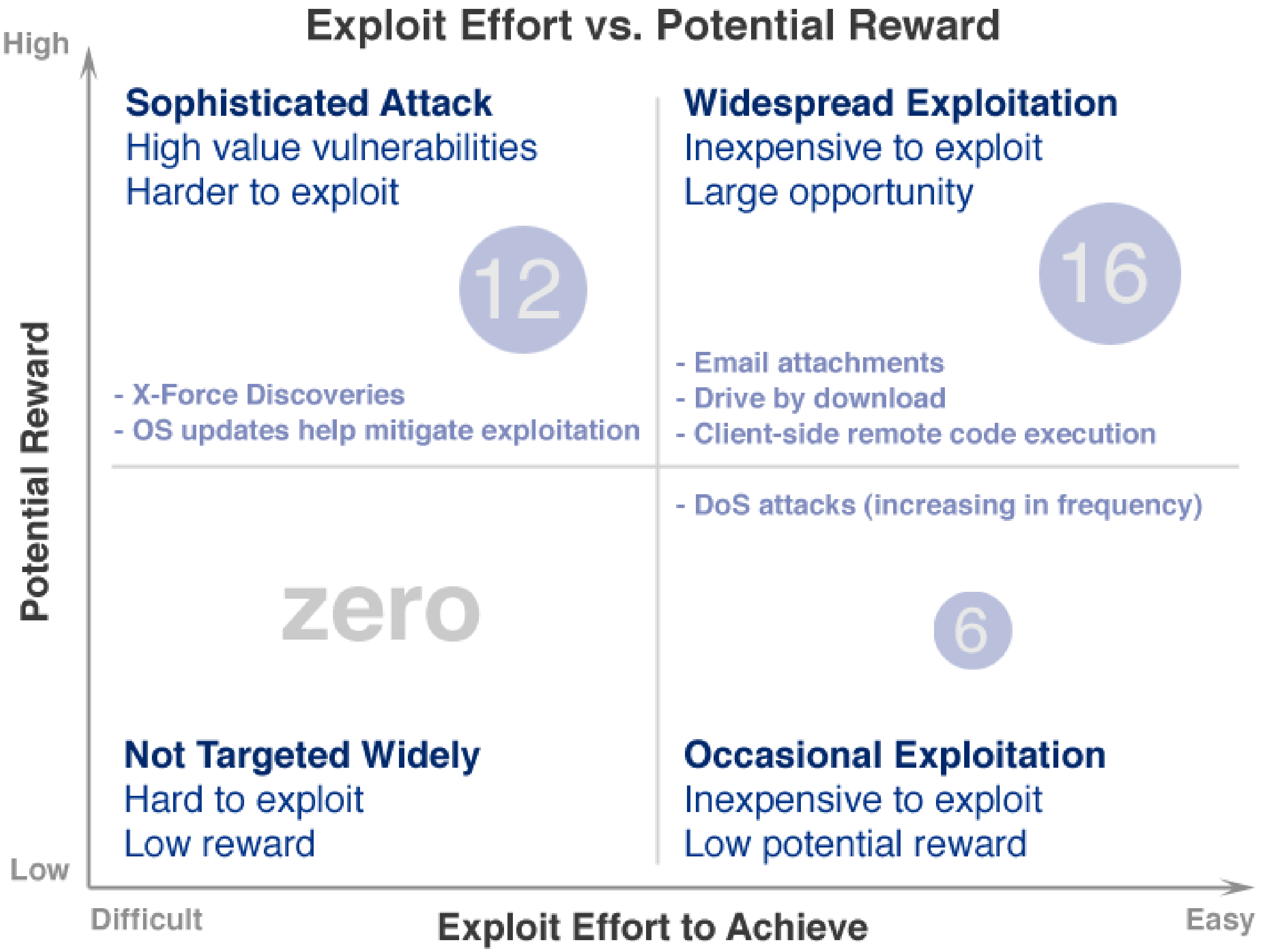




Source: IBM X-Force® Research and Development

Predict what the attacker will exploit

- **34 X-Force alerts and advisories in 2011**
- 16 high value, cheap-to-exploit
  - Publicly available exploits for most of them
- 12 harder to exploit but high value
  - This is a higher number that in previous years



Exploit Effort vs. Potential Reward

Sophisticated Attack
High value vulnerabilities
Harder to exploit

- X-Force Discoveries
- OS updates help mitigate exploitation

Widespread Exploitation
Inexpensive to exploit
Large opportunity

- Email attachments
- Drive by download
- Client-side remote code execution
- DoS attacks (increasing in frequency)

Not Targeted Widely
Hard to exploit
Low reward

Occasional Exploitation
Inexpensive to exploit
Low potential reward

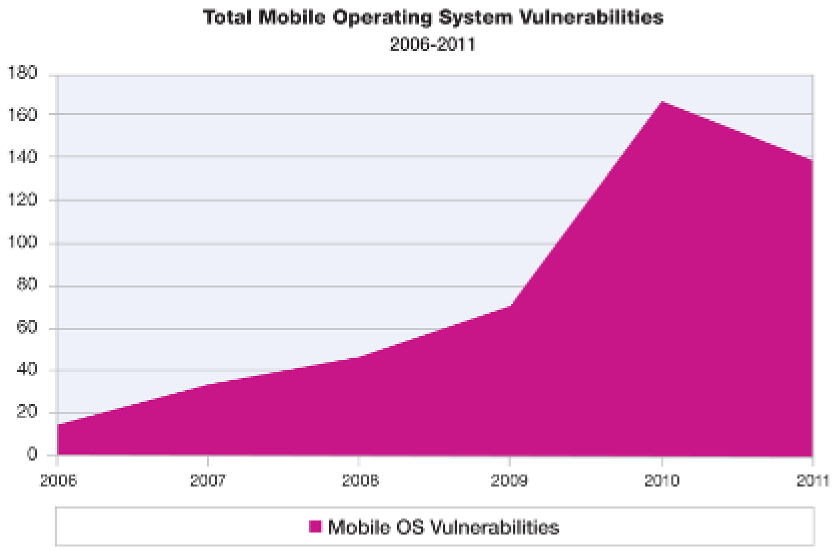
Key Messages from the 2011 Trend Report

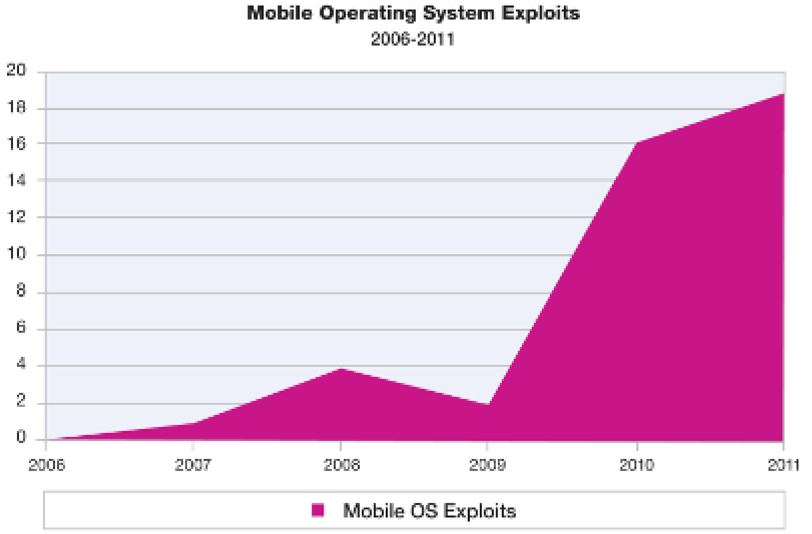
- New Attack Activity
  - Rise in Shell Command Injection attacks
  - Spikes in SSH Brute Forcing
  - Rise in phishing based malware distribution and click fraud
- Progress in Internet Security
  - Fewer exploit releases
  - Fewer web application vulnerabilities
  - Better patching
- The Challenge of Mobile and the Cloud
  - Mobile exploit disclosures up
  - Cloud requires new thinking
  - Social Networking no longer fringe pastime

Mobile OS vulnerabilities & exploits

- Continued interest in Mobile vulnerabilities as enterprise users request a “bring your own device” (BYOD) strategy for the workplace

- Attackers finding these devices represent lucrative new attack opportunities





ion

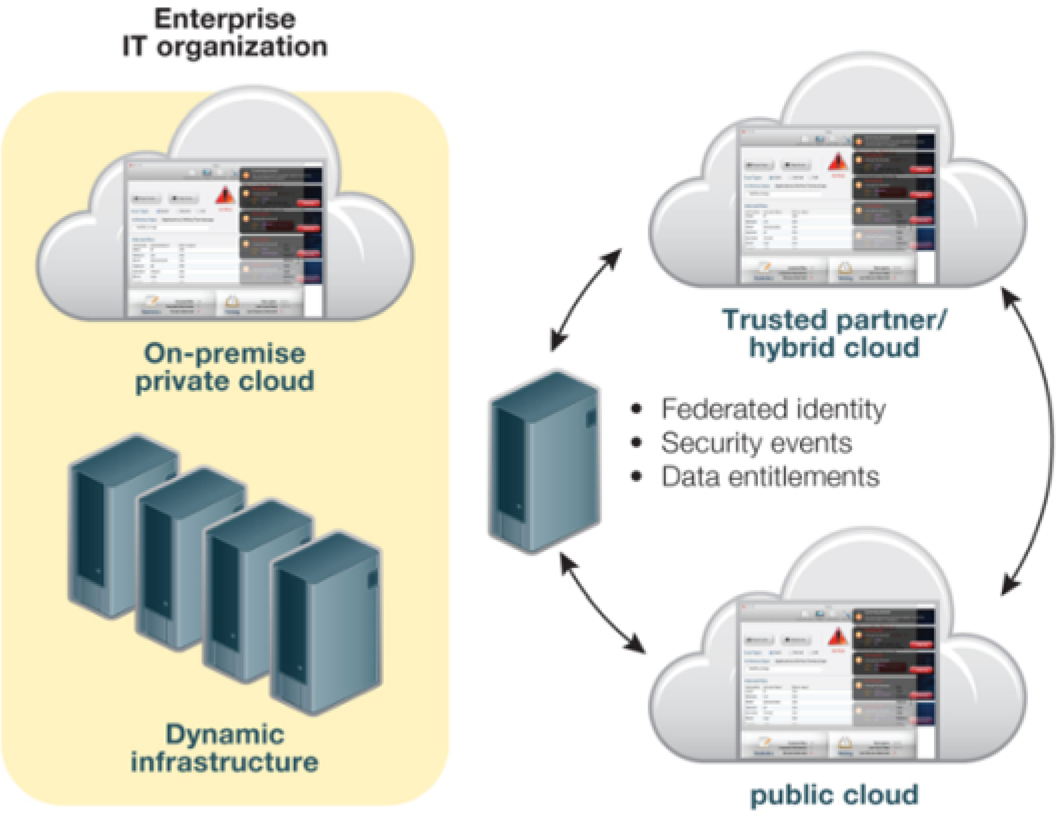
Source: IBM X-Force® Research and Development

Challenges of cloud security

- We saw a number of high profile cloud breaches in 2011 affecting well-known organizations and large populations of their customers

- Customers looking at cloud environments should consider:
  - Cloud-appropriate workloads
  - Appropriate service level agreements (SLAs)
  - Lifecycle approaches to deployment that include exit strategies should things not work out

Securing access to cloud-based applications and services

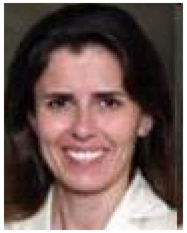


Social Networking – no longer a fringe pastime

- Attackers finding social networks ripe with valuable information they can mine to build intelligence about organizations and its staff:
  - Scan corporate websites, Google, Google News
    - Who works there? What are their titles?
    - Create index cards with names and titles
  - Search Linkedin, Facebook, Twitter profiles
    - Who are their colleagues?
    - Start to build an org chart
  - Who works with the information the attacker would like to target?
    - What is their reporting structure?
    - Who are their friends?
    - What are they interested in?
    - What are their work/personal email addresses?

IBM’s own strategy: Ten essential practices for security leaders

Kristin Lovejoy
IBM Vice President, IT Risk

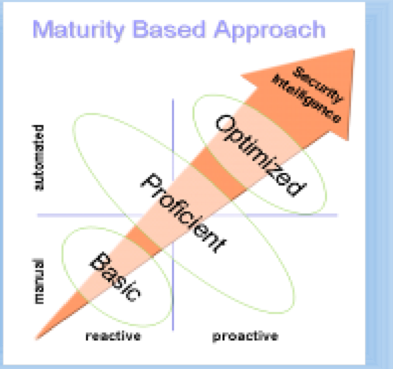


5. Take a Hygienic Approach to Managing Infrastructure

6. Control Network Access

4. Secure Services, By Design

7. Address New Complexity of Cloud and Virtualization



3. Secure the Workplace of the Future (Endpoint)

8. Assure Supply Chain Security Compliance

2. Manage Incidents

9. Protect Structured & Unstructured Data

1. Build a Risk Aware Culture & Management System

10. Manage the Identity Lifecycle

IBM Security Systems

IBM Security Intelligence

Q1 Labs

INTERNET SECURITY SYSTEMS™

watchfire®

OUNCE LABS
an IBM company

SCOM

ENCENTUATE®
An IBM Company

consul
an IBM company

access360™
A Better Way To Manage Access Rights

BIGFIX
An IBM Company

NISC
National Interest Security Company, An IBM Company

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

princeton softech
an IBM® Company

DATAPOWER

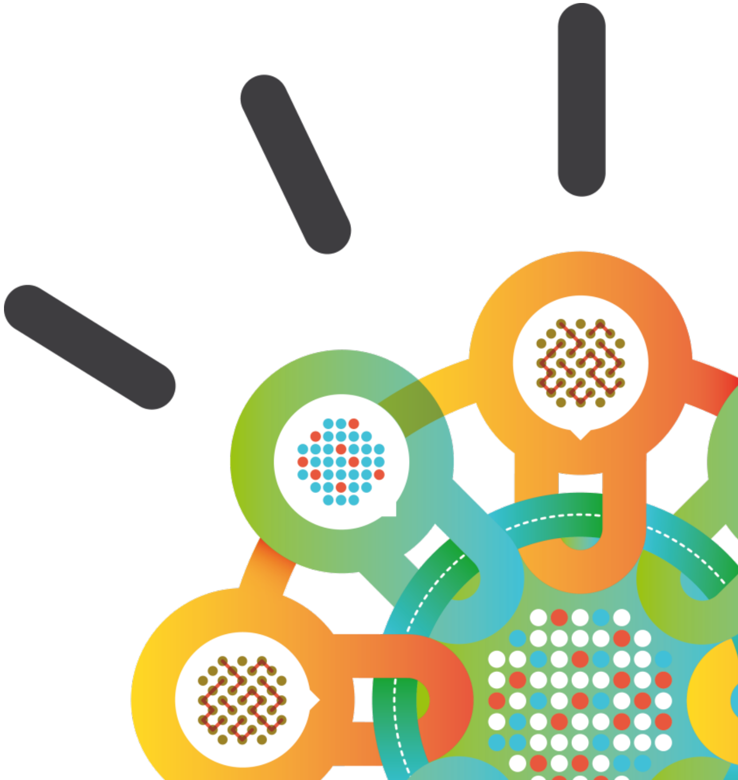
METAMERGE

ibm.com/security

Time	Topic	Speakers
9:05am - 9:45am	Security Stream Kickoff-Security and compliance Overview and X Force	Joe Ruthven and Sukhdev Singh
9:45am - 10:25am	Threat	Lekgale Mokota
10:25am - 10:40am	Break	
10:40am - 11:10am	Q1 Labs Security Intelligence Strategy and Roadmap – How to use Security Intelligence for detecting threats and exceeding compliance mandates	Murray Benadie
11:10am - 11:40am	Driving Effective Application Security in the Enterprise: An End to End Approach to Addressing One of the Biggest Threats to a Business	Sukhdev Singh
11.40am - 12:10pm	Identity Intelligence: Enabling Secure Cloud and Mobile Access	Kevin Mckerr (Puleng)
12:10pm - 12:15 pm	Closing and Questions	
12:15pm	Lunch and Networking	

Security Intelligence.
Think Integrated.

What is the IBM Vision for Infrastructure Security



IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

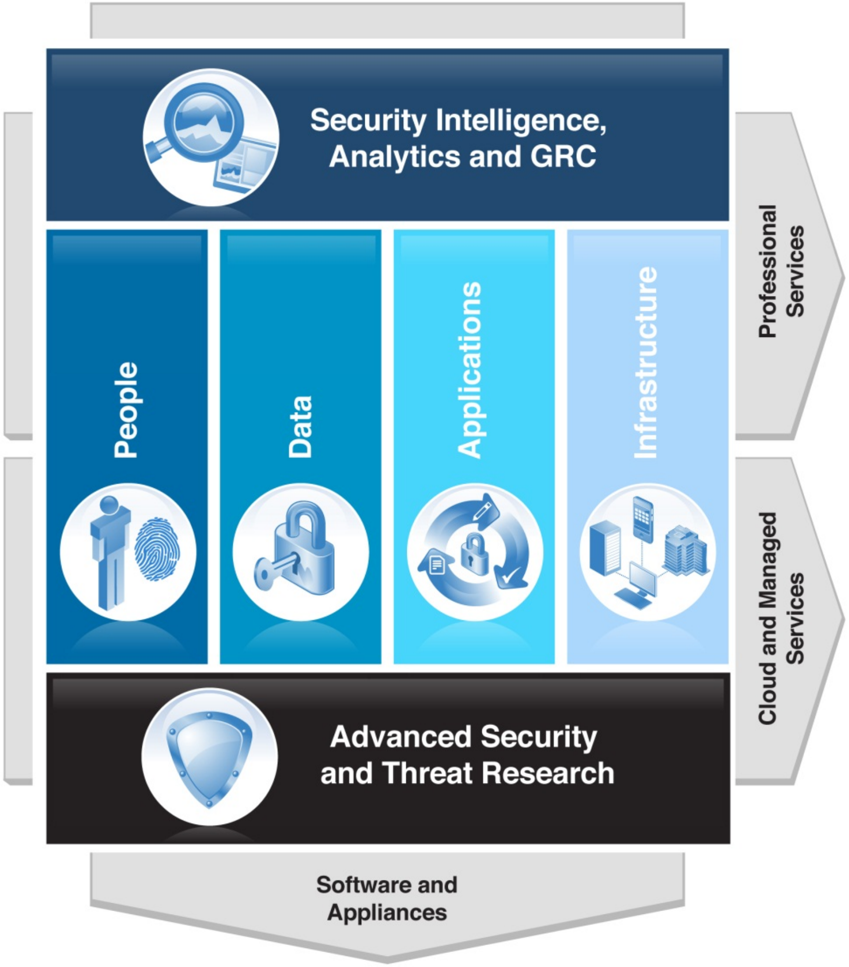
IBM Security Systems

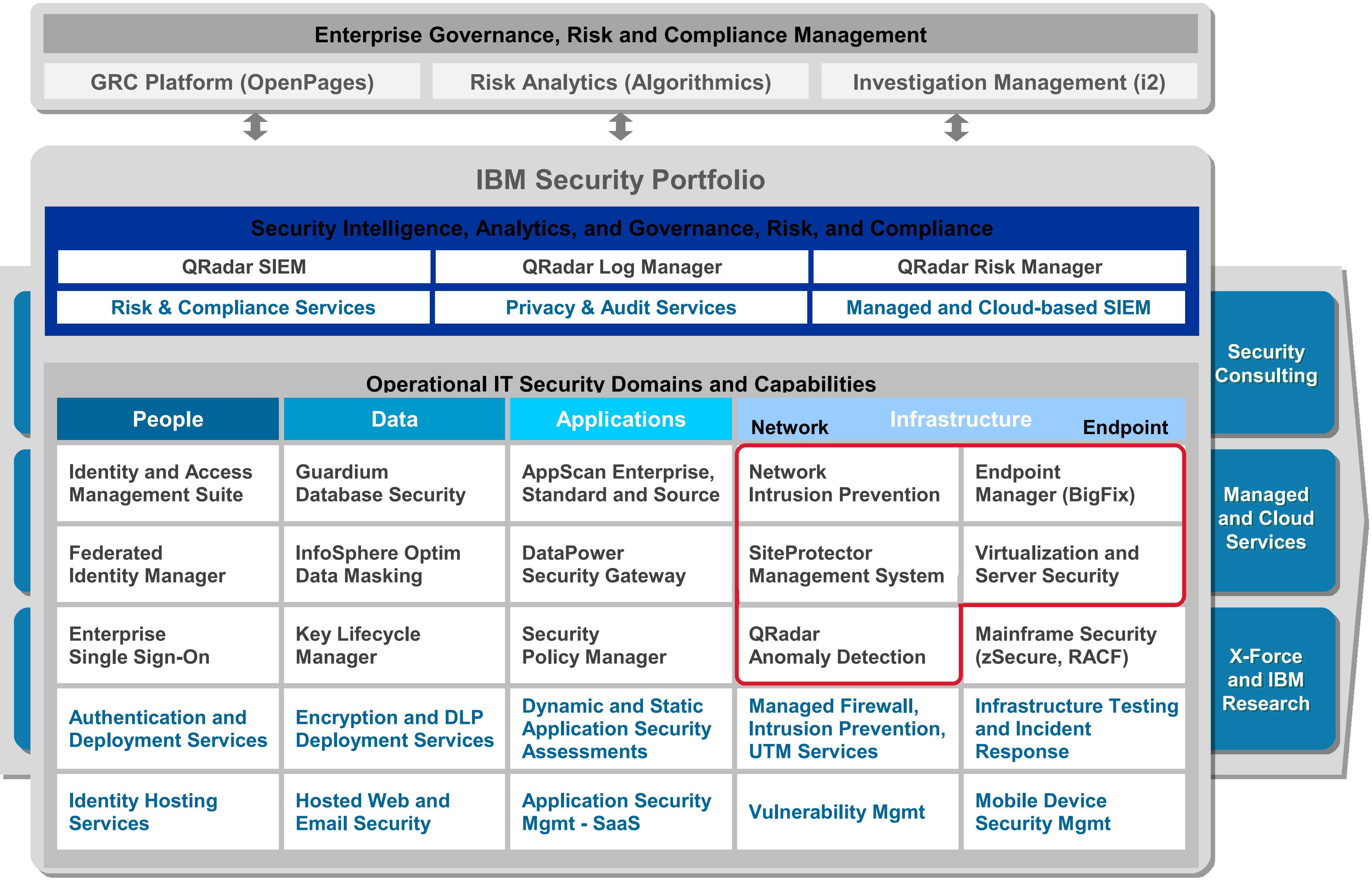
- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

Intelligence • Integration • Expertise

IBM Security Framework

IBM Security Framework


Security Intelligence, Analytics and GRC
People
Data
Applications
Infrastructure
Professional Services
Cloud and Managed Services
Advanced Security and Threat Research
Software and Appliances



Enterprise Governance, Risk and Compliance Management

GRC Platform (OpenPages)	Risk Analytics (Algorithmics)	Investigation Management (i2)

IBM Security Portfolio

Security Intelligence, Analytics, and Governance, Risk, and Compliance

QRadar SIEM	QRadar Log Manager	QRadar Risk Manager
Risk & Compliance Services	Privacy & Audit Services	Managed and Cloud-based SIEM

Operational IT Security Domains and Capabilities

People	Data	Applications	Infrastructure Network	 Endpoint
Identity and Access Management Suite	Guardium Database Security	AppScan Enterprise, Standard and Source	Network Intrusion Prevention	Endpoint Manager (BigFix)
Federated Identity Manager	InfoSphere Optim Data Masking	DataPower Security Gateway	SiteProtector Management System	Virtualization and Server Security
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection	Mainframe Security (zSecure, RACF)
Authentication and Deployment Services	Encryption and DLP Deployment Services	Dynamic and Static Application Security Assessments	Managed Firewall, Intrusion Prevention, UTM Services	Infrastructure Testing and Incident Response
Identity Hosting Services	Hosted Web and Email Security	Application Security Mgmt - SaaS	Vulnerability Mgmt	Mobile Device Security Mgmt

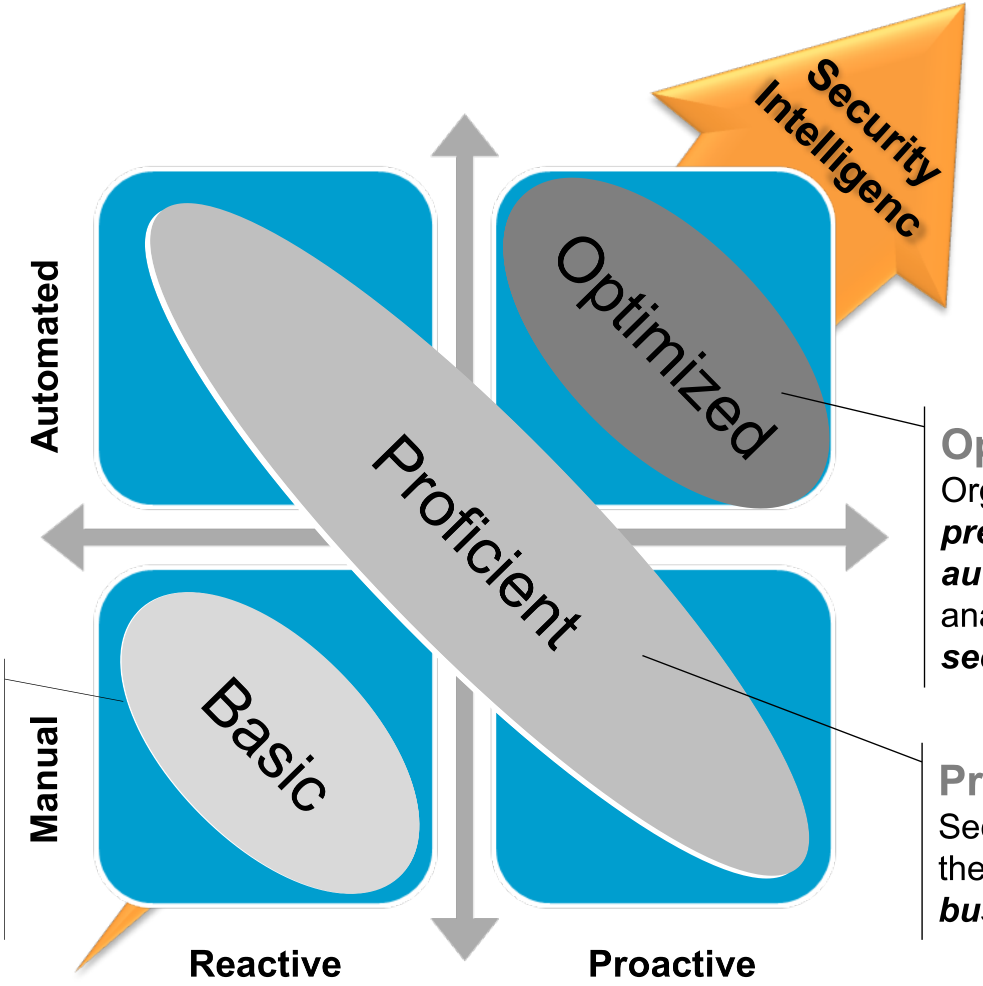
Security Consulting

Managed and Cloud Services

X-Force and IBM Research

Products Services

In this “new normal”, organizations need an intelligent view of their security posture

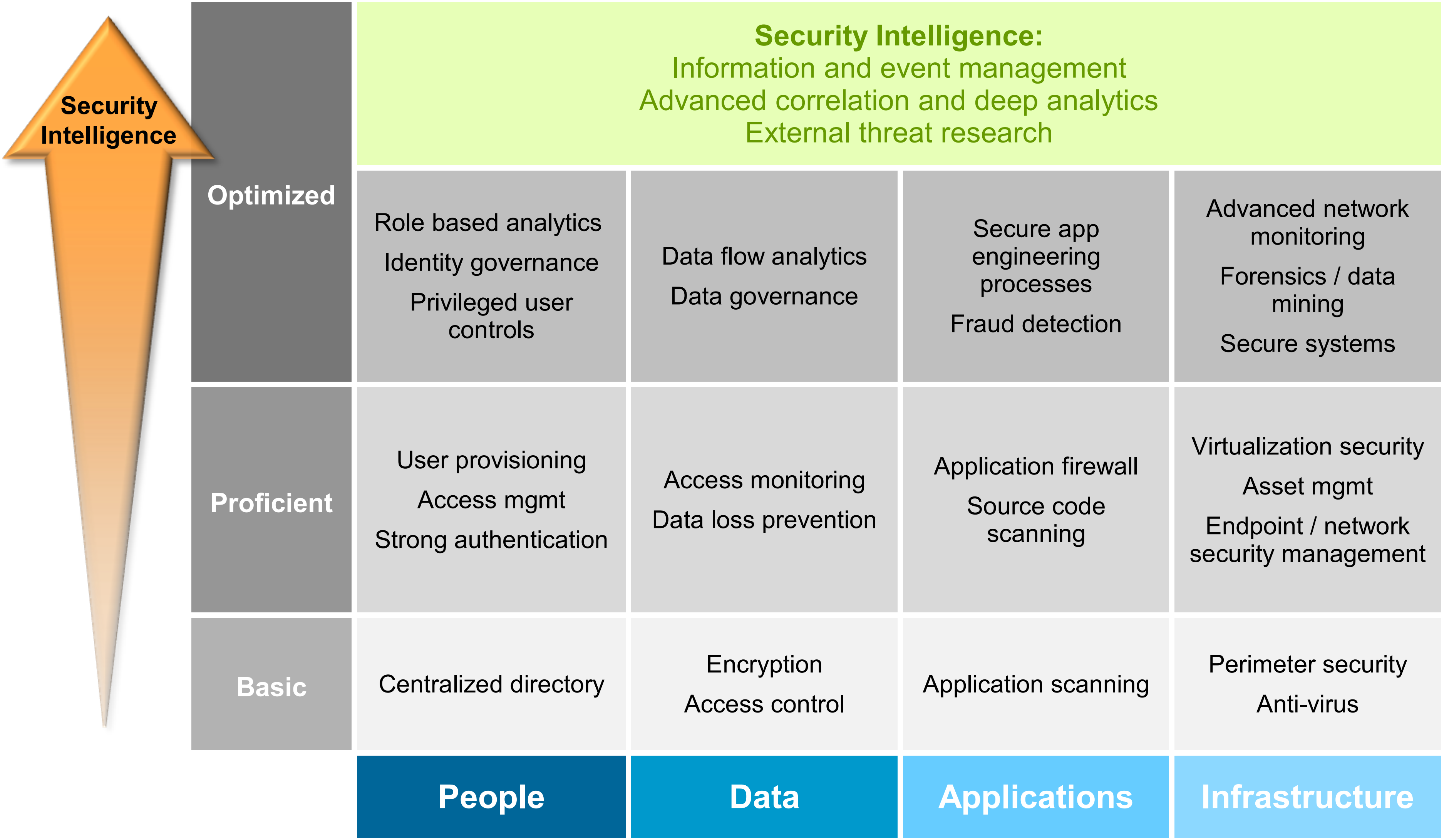


Optimized
Organizations use ***predictive and automated*** security analytics to drive toward ***security intelligence***

Proficient
Security is layered into the ***IT fabric*** and ***business operations***

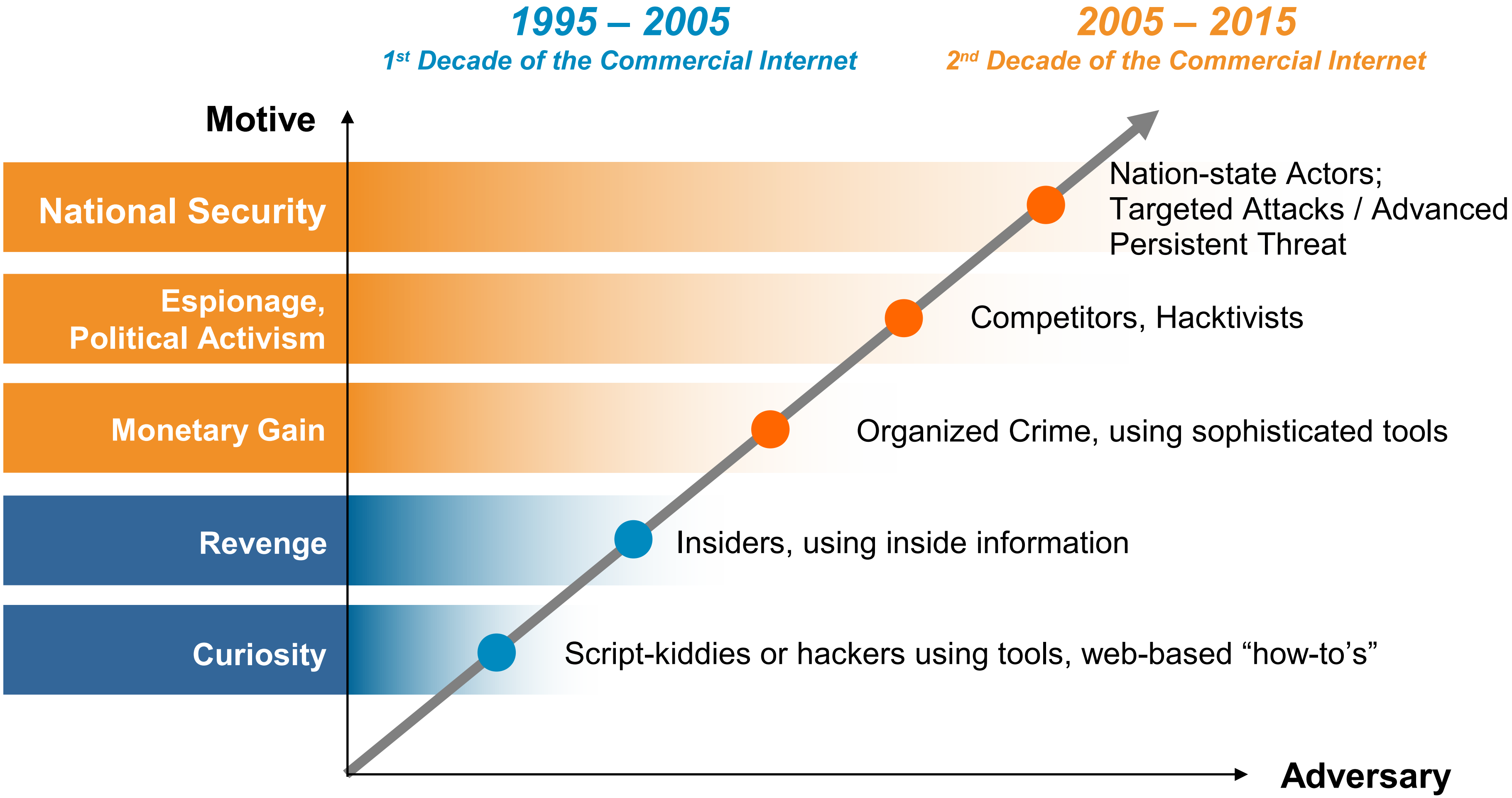
Basic
Organizations employ ***perimeter protection***, which regulates access and feeds manual reporting

Security Intelligence is enabling progress to optimized security



	People	Data	Applications	Infrastructure
Optimized	**Security Intelligence:** Information and event management Advanced correlation and deep analytics External threat research			
	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

Advanced Threats: The sophistication of Cyber threats, attackers and motives is rapidly escalating


1995 – 2005
1st Decade of the Commercial Internet
2005 – 2015
2nd Decade of the Commercial Internet
Motive
National Security
Espionage, Political Activism
Monetary Gain
Revenge
Curiosity
Nation-state Actors; Targeted Attacks / Advanced Persistent Threat
Competitors, Hacktivists
Organized Crime, using sophisticated tools
Insiders, using inside information
Script-kiddies or hackers using tools, web-based “how-to’s”
Adversary

Techniques used by attackers are bypassing traditional defenses

Advanced

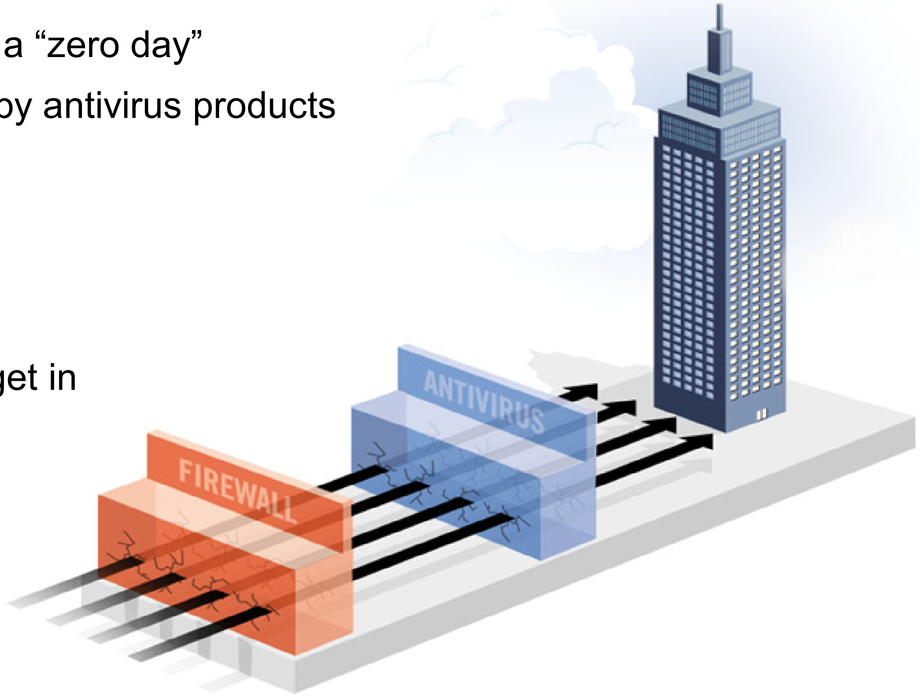
- Using exploits for unreported vulnerabilities, aka a “zero day”
- Advanced, custom malware that is not detected by antivirus products
- Coordinated attacks using a variety of vectors

Persistent

- Attacks lasting for months or years
- Attackers are dedicated to the target – they will get in
- Resistant to remediation attempts

Threat

- Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
- Not random attacks – they are actually “out to get you”



These methods have eroded the effectiveness of traditional defenses including firewalls, intrusion prevention systems and antivirus - ***leaving holes in the network***

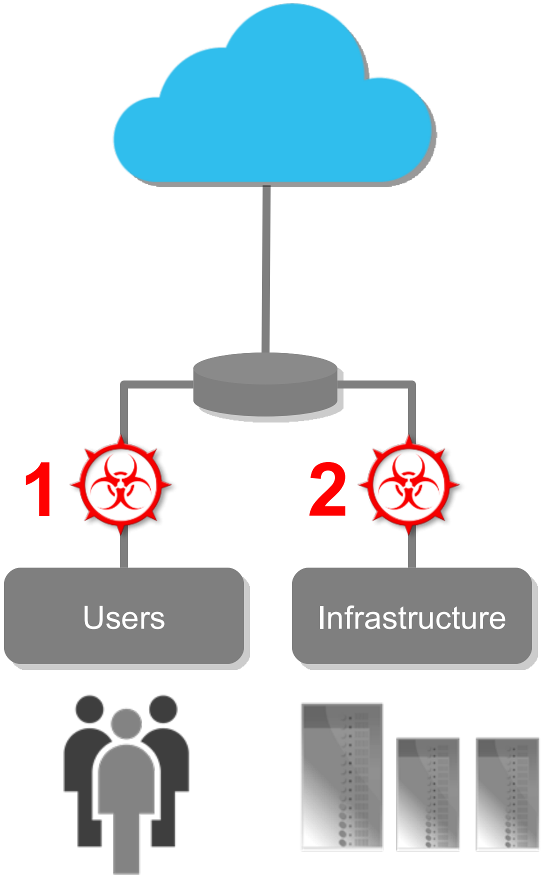
Closer look at the attack vectors of today's threats

1. User Attacks (Client-side)

- **Drive-by Downloads:** User browses to a malicious website and/or downloads an infected file using an unpatched browser or application
- **Targeted Emails:** Email containing an exploit or malicious attachment is sent to an individual with the right level of access at the company

2. Infrastructure Attacks (Server-side)

- **SQL Injection:** Attacker sends a specially crafted message to a web application, allowing them to view, modify, or delete DB table entries
- **General Exploitation:** Attacker identifies and exploits a vulnerability in unpatched or poorly written software to gain privileges on the system



Despite the growing number of techniques used to gain access, one fact remains constant:
a remote attacker must gain access over the corporate network

What is the IBM Vision for Infrastructure Security

IBM Advanced Threat Protection

Our strategy is to protect our customers with advanced threat protection at the network layer - by strengthening and integrating network security, analytics and threat Intelligence capabilities

1. Advanced Threat Protection Platform

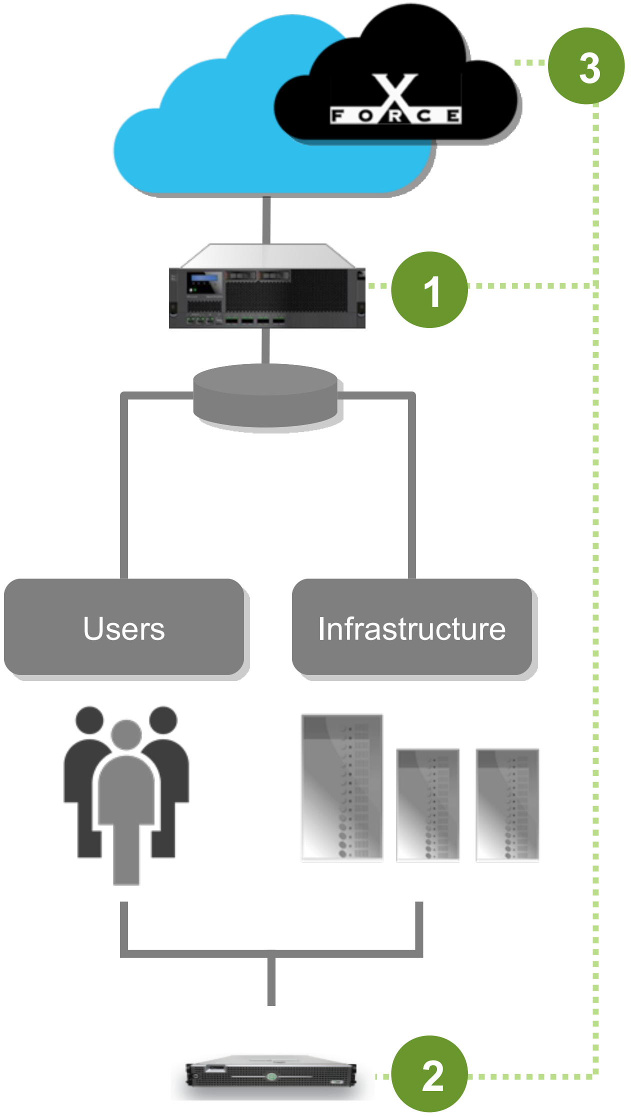
Evolve our Intrusion Prevention System to become a Threat Protection Platform – providing packet, content, file and session inspection to stop threats from entering the corporate network

2. QRadar Security Intelligence Platform

Build tight integration between the Network Security products, X-Force intelligence feeds and QRadar Platform product with purpose-built analytics and reporting for threat detection and remediation

3. X-Force Threat Intelligence

Increase investment in threat intelligence feeds and feedback loops for our products. Leverage the existing Cobion web and email filtering data, but expand into botnet, IP reputation and Managed Security Services data sets



The Requirements for an Advanced Threat Protection Platform

Security Intelligence

What are the threats affecting my business? · Are we configured to protect against these threats? · What is happening right now? · What was the impact?

Security Information and Event Management ▪ Log Management ▪ Configuration Monitoring ▪ Vulnerability Management

Threat Intelligence and Research

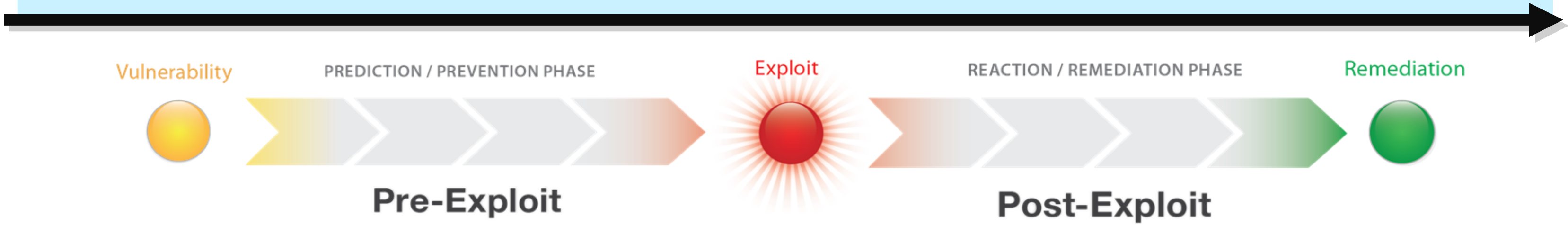
What are the latest vulnerabilities? · What websites are malicious or suspicious? · Who is infected or conducting attacks? · What network traffic is associated with botnets?

Vulnerability Research ▪ Malicious URLs ▪ Spam / Phishing Emails ▪ IP Reputation ▪ Botnet Domains

Advanced Threat Protection

Is someone trying to break into my network? · Is this file hiding an attack or sensitive data? · Is this application allowed on my network? · What evidence do we have of an intrusion?

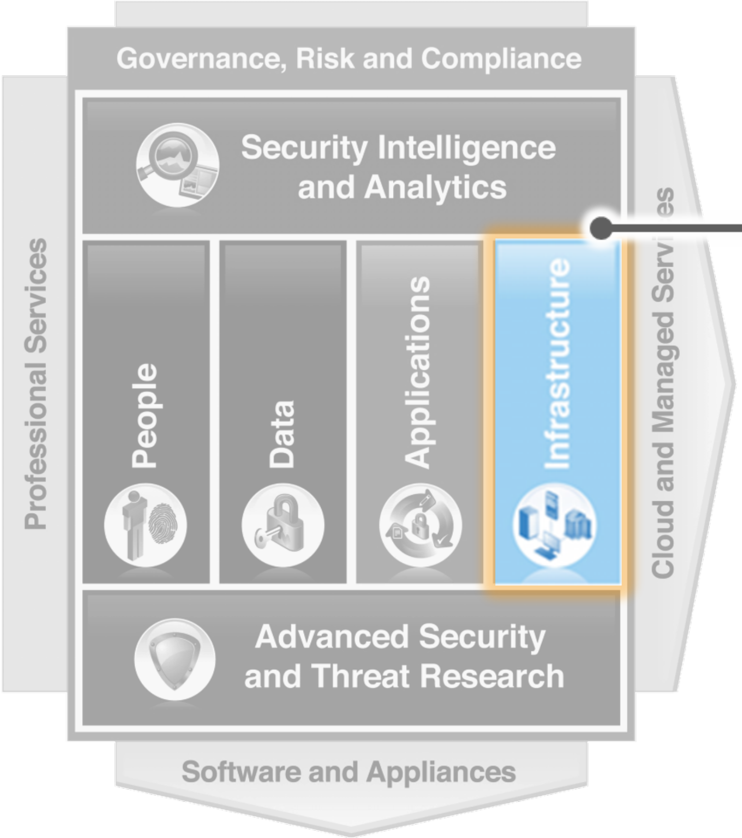
Intrusion Prevention ▪ Content Inspection ▪ Malware Analysis ▪ Application Control ▪ Network Forensics



Infrastructure (Network)

Area of Focus

Guard against sophisticated attacks using an Advanced Threat Protection Platform with insight into users, content and applications


Governance, Risk and Compliance
Security Intelligence and Analytics
Professional Services
People
Data
Applications
Infrastructure
Cloud and Managed Services
Advanced Security and Threat Research
Software and Appliances

Portfolio Overview

IBM Security Network Intrusion Prevention (IPS)

•Delivers Advanced Threat Detection and Prevention to stop targeted attacks against high value assets

•Proactively protects systems with IBM Virtual Patch® technology.

•Protects web applications from threats such as SQL Injection and Cross-site Scripting attacks

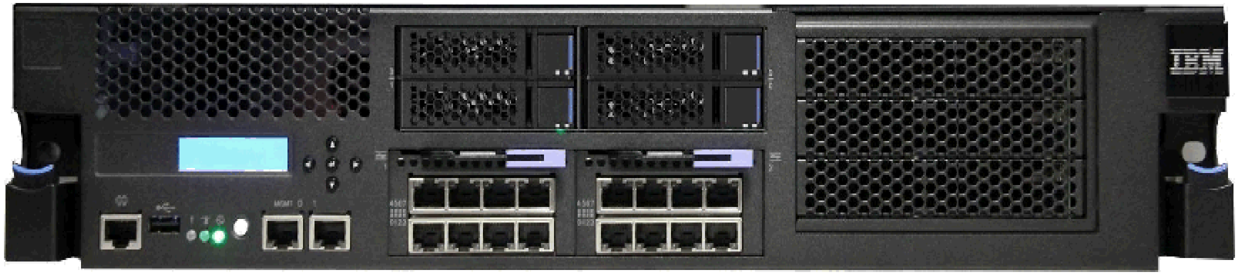
•Integrated Data Loss Prevention (DLP) monitors data security risks throughout your network

•Provides Ahead of the Threat® protection backed by world renowned IBM X-Force Research

IBM Security SiteProtector

•Provides central management of security devices to control policies, events, analysis and reporting for your business

Introducing **IBM Security Network Protection XGS 5000**



	NEW WITH XGS	NEW WITH XGS
PROVEN SECURITY	ULTIMATE VISIBILITY	COMPLETE CONTROL
Extensible, 0-Day protection powered by X-Force®	Understand the Who, What and When for all network activity	Ensure appropriate application and network use

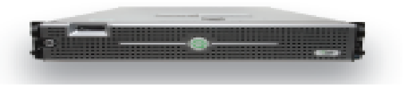
IBM Security Network Protection XGS 5000 builds on the proven security of IBM intrusion prevention solutions by delivering the addition of next generation *visibility* and *control* to help balance security and business requirements

QRadar Network Anomaly Detection

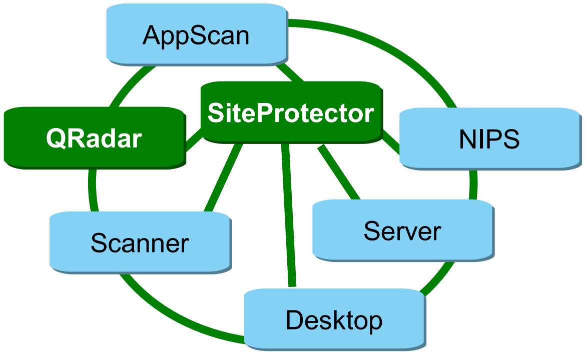
Optimized for the Advanced Threat Protection Platform

- **QRadar Network Anomaly Detection** is an optimized version of QRadar which *complements* SiteProtector to provide deep network visibility and real-time insight to identify threats; upgradeable to full QRadar SIEM
- Market-leading network behavioral analytics improves proficiency in threat detection empowering customers with proactive Threat Protection
- Meets the needs of new and existing **SiteProtector/IPS customers** who desire greater **visibility** into their network
- Integration of network flow capture with behavioral analysis and anomaly detection provides greater security intelligence:
  - Traffic profiling for added protection from **Low and Slow** and **zero-day threats**
  - Correlation of threat data, flow data and system and application vulnerabilities for **enhanced incident analysis**
- Includes support for **identity sources** to associate user activity with incidents; and support for **vulnerability data** to correlate attack with vulnerable assets
- Appliance (2Q12) and VMware Image (future)

Q1 Labs®
Total Security Intelligence | An IBM Company



- SiteProtector as core for command & control
- QRadar Network Anomaly Detection for enhanced analytics
- QRadar QFlow and VFlow collectors provide Network Awareness via deep packet inspection
- Integrated policy management & workflows within SiteProtector facilitate a **rapid response to threat** and **more proactive visibility**.



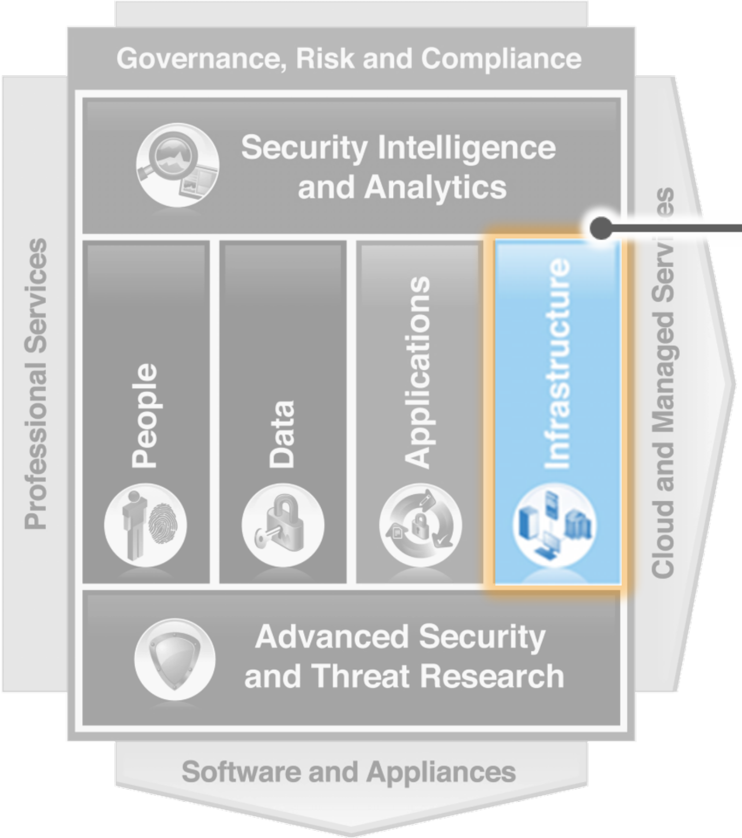
Visibility **Protection**

Suspicious Behavior → Proactive Prevention

Infrastructure (Endpoint and Server)

Area of Focus

Ensuring endpoints, servers, and mobile devices remain compliant, updated, and protected against todays threats


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Portfolio Overview

IBM Endpoint Manager for Security and Compliance

•Addresses distributed environments with endpoint and security management in a single solution

IBM Endpoint Manager for Core Protection

•Real-time protection from malware and other threats

IBM Endpoint Manager for Mobile Devices

- Secure and manage traditional endpoints as well as iOS, Android, Symbian, and Microsoft devices

IBM Security Server Protection

- Multilayered protection against threats, supporting a broad range of operating systems

IBM Security Virtual Server Protection for VMware

- Dynamic security for virtualization with VM rootkit detection, auditing, network intrusion prevention

IBM Security Virtual Server Protection for VMware

Customers get robust, efficient security for their virtualized data centers

- Customers transitioning to virtualized data centers or cloud deployment architectures face additional security threats – VSP can help mitigate these risks
- **Virtual Server Protection** is integrated with the hypervisor and optimized for virtualized deployments to maximize data center capacity
- Provides visibility into intra-VM network traffic along with traffic between the virtual and physical infrastructures
- Supports ESX 4.1 and 5.0 as well as 10Gb Ethernet
- Create and manage security policies across multiple VMware ESX servers
- Facilitate auditing and compliance requirements by capturing and aggregating relevant events

Core Capabilities

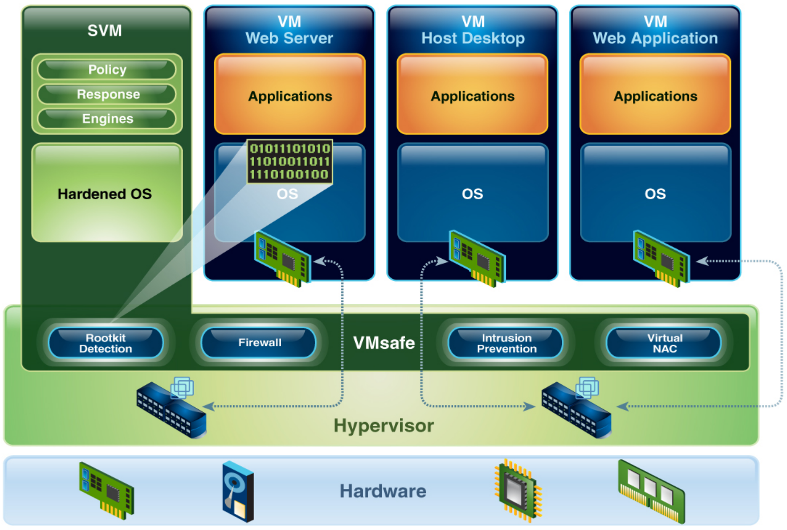
Agentless Protection -- Powered by IBM Research and X-Force technology to provide deep packet inspection, firewall, network segmentation, and rootkit detection with no in-guest VM footprint

Improve governance in the virtual data center by reducing VM sprawl, quarantining insecure VMs, and maintaining real-time visibility across the environment

Maximize virtualization ROI by optimizing the security footprint on your physical systems

Move to IBM Virtual Server Protection

Manage risk with a solution optimized for your virtual data center environment



IBM Security Endpoint Defense

Customers get proactive security for their critical systems, powered by X-Force

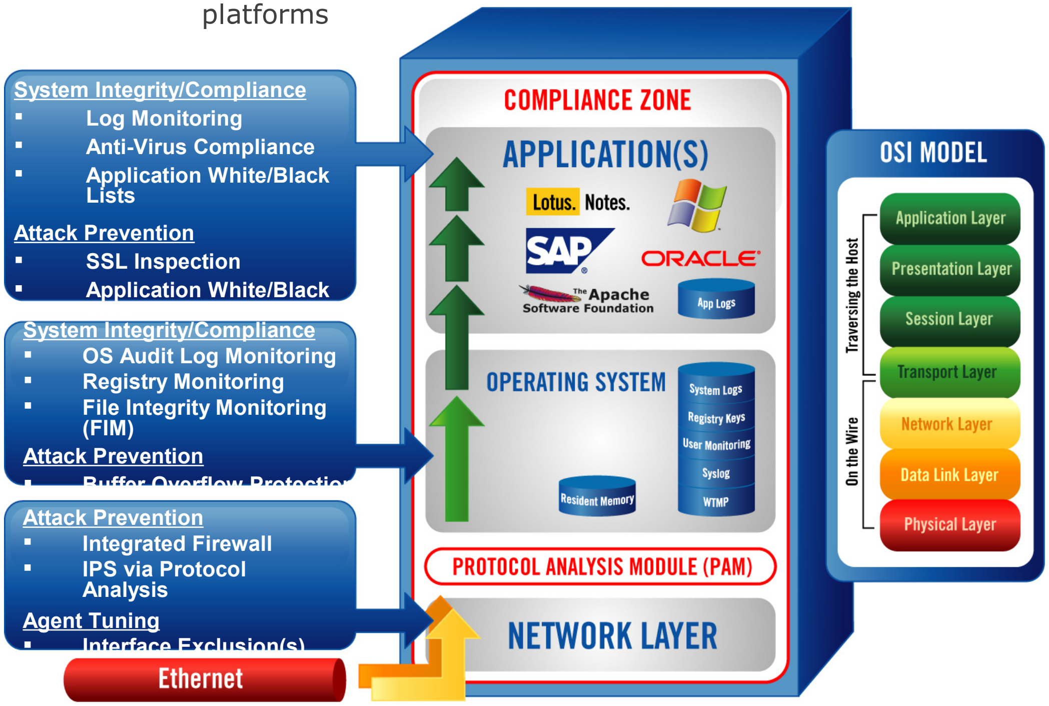
- Customers can protect their critical endpoints with preventive technology and intelligence from IBM X-Force
- Broaden situational awareness by monitoring critical files, OS audit logs, ASCII text logs, and the Windows registry for changes
- Inspect SSL-encrypted network traffic for potential threats
- Enforce security policies based on network location to ensure the right level of protection for the mobile workforce
- Supports Windows, Linux, and UNIX
- Facilitate auditing and compliance by capturing and aggregating security events

Core Capabilities

Host-level Protection -- Identify potential threats with technology from IBM X-Force, while monitoring critical files, OS subsystems, and applications

Proactive defense helps you to stay ahead of the threat, by using a vulnerability-centric approach to protect against whole classes of exploits

Centralize administration of security across a heterogeneous environment by providing robust security across multiple OS platforms



System Integrity/Compliance
- Log Monitoring
- Anti-Virus Compliance
- Application White/Black Lists

Attack Prevention
- SSL Inspection
- Application White/Black

System Integrity/Compliance
- OS Audit Log Monitoring
- Registry Monitoring
- File Integrity Monitoring (FIM)

Attack Prevention
- Buffer Overflow Protectio

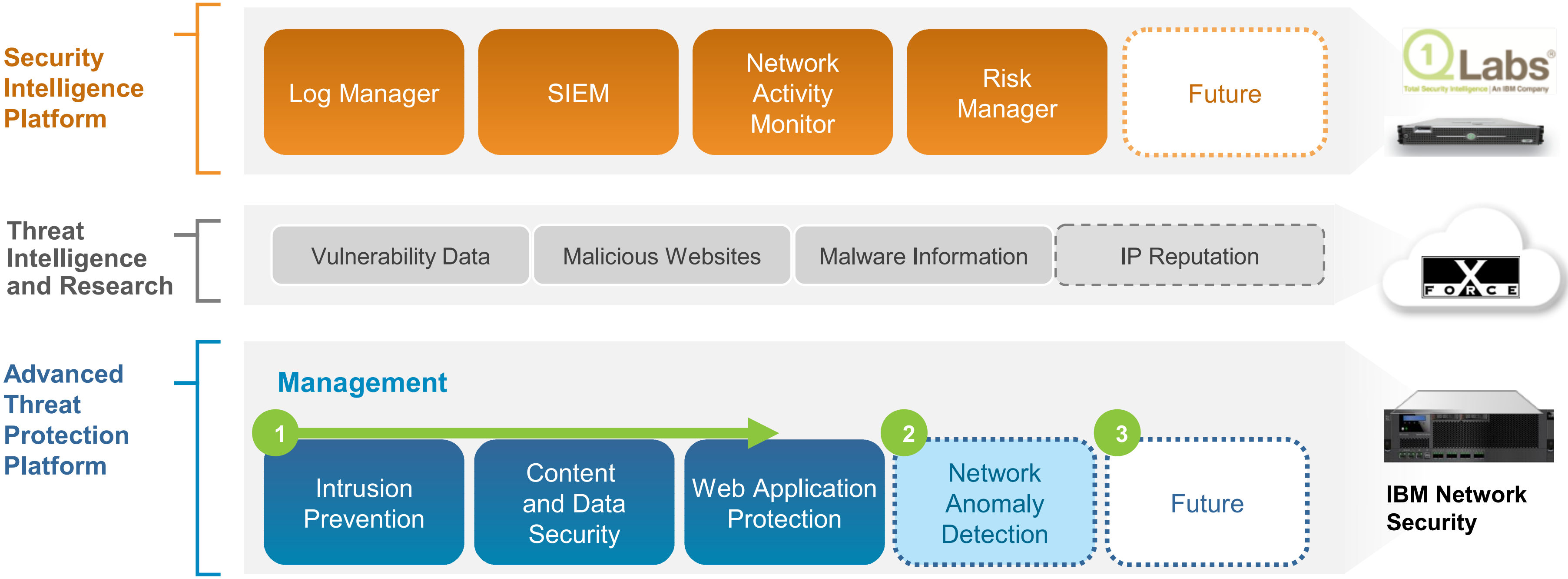
Attack Prevention
- Integrated Firewall
- IPS via Protocol Analysis

Agent Tuning
- Interface Exclusion(s)

IBM Advanced Threat Protection Platform Solves Key Customer Challenges

IT Security Problem	IBM ATPP Helps. . .
Incident response efforts take too long, impacting confidence in IT	Block malicious traffic
We experience too much downtime due to uncertainty over virus and malware outbreaks	Block malicious traffic
Internal executive reporting is limited, unable to demonstrate effectiveness of security systems	Report on blocked threats
IT compliance reporting is slow and manual	Provide comprehensive compliance reports
Unique network traffic patterns and unpredictable events cause planning and availability issues	Write and import custom rules and utilize freely available open source files
We don’t have efficient tools to proactively analyze network traffic to find unusual user behavior and other anomalies	Integrated analysis of network flow data and integration with SiteProtector
Lack the ability to manage user access to web and non-web applications and internet sites	Controls to manage user access at granular level and decrease bandwidth utilization

SUMMARY: Advanced Threat Protection Platform helps protect Customer Networks Today and Tomorrow


Security Intelligence Platform
Log Manager
SIEM
Network Activity Monitor
Risk Manager
Future
QLabs
Total Security Intelligence | An IBM Company
Threat Intelligence and Research
Vulnerability Data
Malicious Websites
Malware Information
IP Reputation
X FORCE
Advanced Threat Protection Platform
Management
1
Intrusion Prevention
Content and Data Security
Web Application Protection
2
Network Anomaly Detection
3
Future
IBM Network Security

1. 1Q12: Launched IBM Security Network IPS Powered by X-Force
2. 2Q12: Launch QRadar Network Anomaly Detection
3. Future: Platform Expansion

This is just the beginning,
We have more exciting
things to tell you
about next quarter !

Learn More about the Advanced Threat Protection Platform

Learn More about IBM Security http://www.ibm.com/security

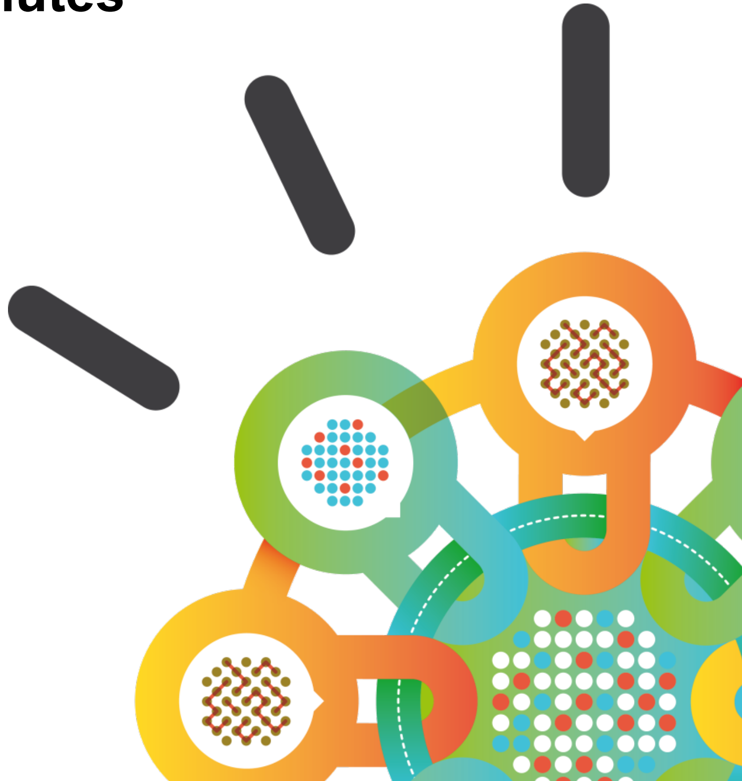
Learn more what the Aberdeen Group has to say about Threat Management http://aberdeen.reg.meeting-stream.com/threat_management/default.aspx?cid=ibm

ibm.com/security

Security Intelligence.
Think Integrated.

Intermission

Next presentation to start promptly in 15 minutes



Time	Topic	Speakers
9:05am - 9:45am	Security Stream Kickoff-Security and compliance Overview and X Force	Joe Ruthven and Sukhdev Singh
9:45am - 10:25am	Threat	Lekgale Mokota
10:25am - 10:40am	Break	
10:40am - 11:10am	**Q1 Labs Security Intelligence Strategy and Roadmap – How to use Security Intelligence for detecting threats and exceeding compliance mandates**	Murray Benadie
11:10am - 11:40am	Driving Effective Application Security in the Enterprise: An End to End Approach to Addressing One of the Biggest Threats to a Business	Sukhdev Singh
11.40am - 12:10pm	Identity Intelligence: Enabling Secure Cloud and Mobile Access	Kevin Mckerr (Puleng)
12:10pm - 12:15 pm	Closing and Questions	
12:15pm	Lunch and Networking	

Q1 Labs

Total Security Intelligence | An IBM Company

Q1Labs.com

Q1 Labs & QRadar SIEM

QRadar SIEM enables security professionals to gain the visibility they need to protect their networks and better protect IT assets from a growing landscape of advanced threats as well as meet current and emerging compliance mandates.

August 2012

The Security Intelligence Leader

Who Q1Labs is:

- 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 (1 customer - 14 Billion events per day)
- Five-year average annual revenue growth of 70%+

Now part of IBM Security Systems:

- Unmatched security expertise and breadth of integrated capabilities

The Security Intelligence Leader

Who Zenith Systems is:

- Started in 2001
- Implemented solutions in most SA corporates

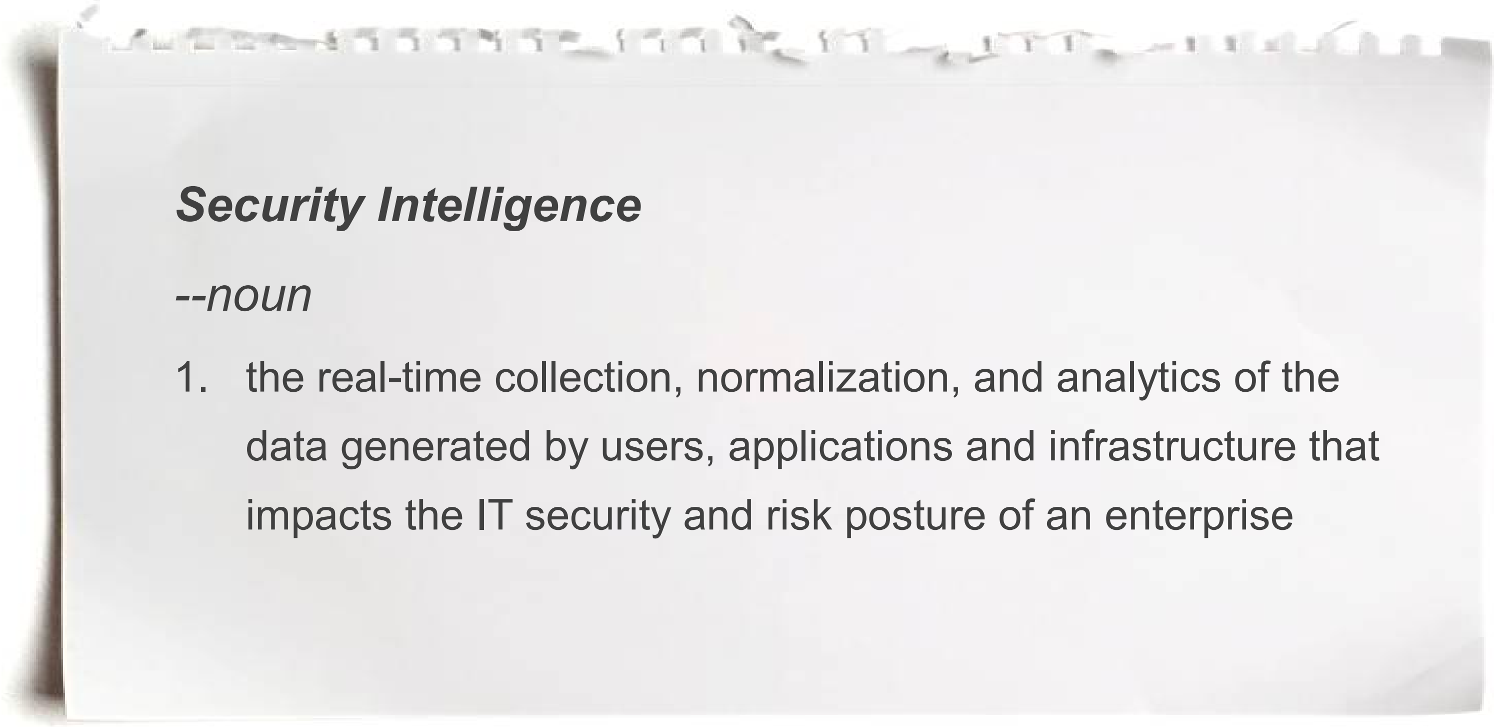
Focused on QRadar:

- 4 year relationship with Q1
- Certified reseller
- Comprehensive pre and post sales capability
- IBM BP

Deployed in Many SA/African organisations:

- RMB
- First Rand
- Post office
- Allan Gray
- Access Bank
- Standard Chartered ZW

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

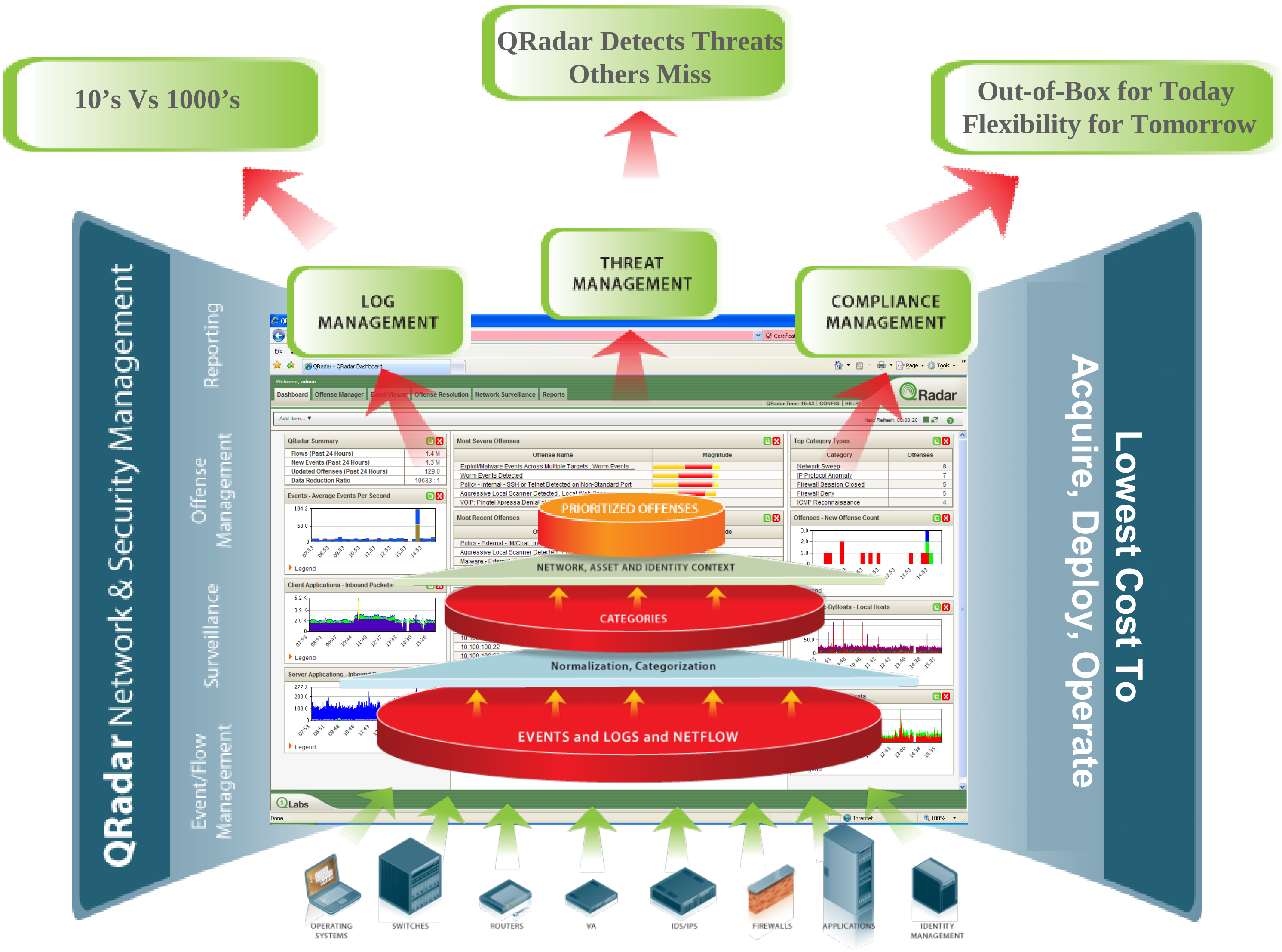
Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

Security Intelligence?

Why it matters

1. Cyber Crime is a global business (not if – when a breach will happen)
2. Cyber Crime is One of the biggest threats to business and delivery
3. Internal and External Threats
4. Compliance / legislation
5. 80% of breach evidence contained in logs.
    1. Volume Overwhelming (160 000 eps, 16 Billion / day)
6. Lack of Integration /correlation Silos
7. Skills Shortages

What is QRadar SIEM/Log Manager



QRadar Summary	
Flows (Past 24 Hours)	1.4 M
New Events (Past 24 Hours)	1.3 M
Updated Offenses (Past 24 Hours)	129.0
Data Reduction Ratio	10633 : 1

Category	Offenses
Network Sweep	8
IP Protocol Anomaly	7
Firewall Session Closed	5
Firewall Deny	5
ICMP Reconnaissance	4

Most Severe Offenses:

- Exploit/Malware Events Across Multiple Targets , Worm Events ...
- Worm Events Detected
- Policy - Internal - SSH or Telnet Detected on Non-Standard Port
- Aggressive Local Scanner Detected , Local Web Scanner D...
- VOIP: Pingtel Xpressa Denial ...

Solving Customer Challenges with Total Security Intelligence

SRP

Detecting threats others miss

- Discovered 500 hosts with "Here You Have" virus, which all other security products missed

Chevron

Consolidating data silos

- 2 Billion logs and events per day reduced to 25 high priority offenses

GUCCI

Detecting insider fraud

- Trusted insider stealing and destroying key data

Cargill

Predicting risks against your business

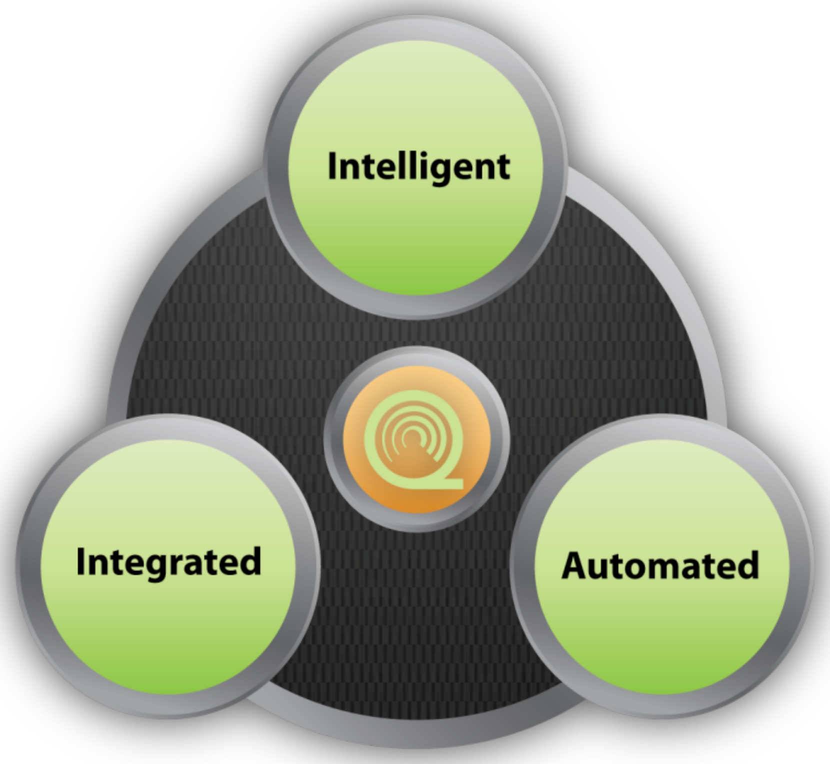
- Automating the policy monitoring and evaluation process for config. change in the infrastructure

WEBB

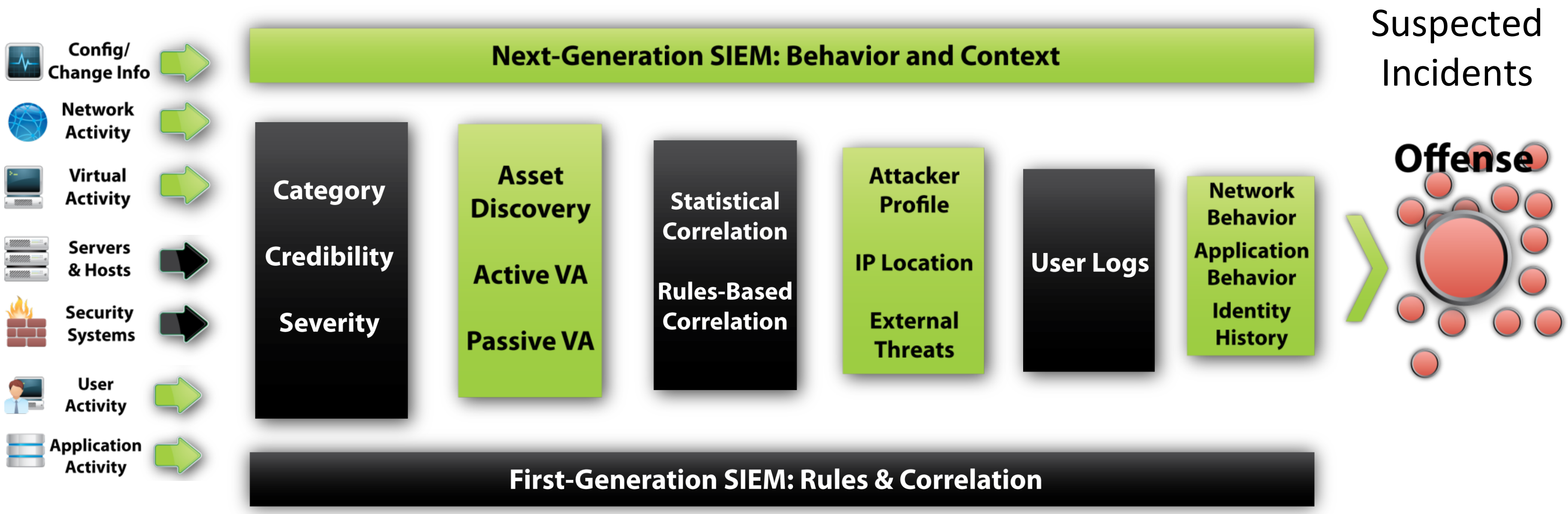
Exceeding regulation mandates

- Real-time monitoring of all network activity, in addition to PCI mandates

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



Next-Generation SIEM: Total Intelligence



Config/ Change Info

Network Activity

Virtual Activity

Servers & Hosts

Security Systems

User Activity

Application Activity

Next-Generation SIEM: Behavior and Context

Category

Credibility

Severity

Asset Discovery

Active VA

Passive VA

Statistical Correlation

Rules-Based Correlation

Attacker Profile

IP Location

External Threats

User Logs

Network Behavior

Application Behavior

Identity History

First-Generation SIEM: Rules & Correlation

Suspected Incidents

Offense

Threats and Fraud Detected That Others Miss

QRadar gave Texas A&M a live window into all network activity. They were able to address issues that ranged from mitigating external threats to enforcing internal policies.

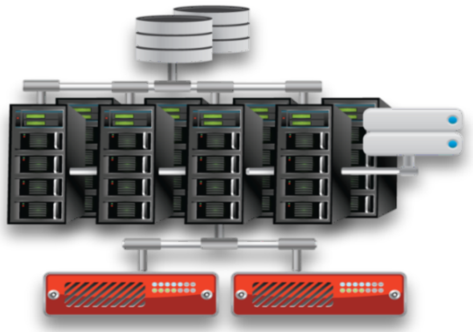
Massive Data Reduction

"With QRadar, Wayne State University now detects issues that would previously have gone unnoticed. QRadar prioritizes the events, indicates the severity and credibility of an event.

Wayne State University

Integrated: Unified Platform for Scale & Ease of Use

Bolted Together Solution



- Scale problems
- Non-integrated reporting & searching
- No local decisions
- Multi-product administration
- Duplicate log repositories
    - ➢ ***Operational bottlenecks***

QRadar Integrated Solution

- Highly scalable
- Common reporting & searching
- Distributed correlation
- Unified administration
- Logs stored once
    - ➢ ***Total visibility***

Fully Integrated Security Intelligence

Log Management

QRadar® Log Manager

QRadar® Log Manager Free Edition

- Turnkey log management
- SME to Enterprise
- Upgradeable to enterprise SIEM

SIEM

QRadar® SIEM

- Integrated log, threat, risk & compliance mgmt.
- Sophisticated event analytics
- Asset profiling and flow analytics
- Offense management and workflow

Risk Management

QRadar® Risk Manager

- Predictive threat modeling & simulation
- Scalable configuration monitoring and audit
- Advanced threat visualization and impact analysis

Network Activity & Anomaly Detection

QRadar® SIEM

QRadar QFlow

- Network analytics
- Behavior and anomaly detection
- Fully integrated with SIEM

Network and Application Visibility

QRadar QFlow

QRadar VFlow

- Layer 7 application monitoring
- Content capture
- Physical and virtual environments

Q1 Labs® Total Security Intelligence | An IBM Company

Fully Integrated Security Intelligence

Log Management

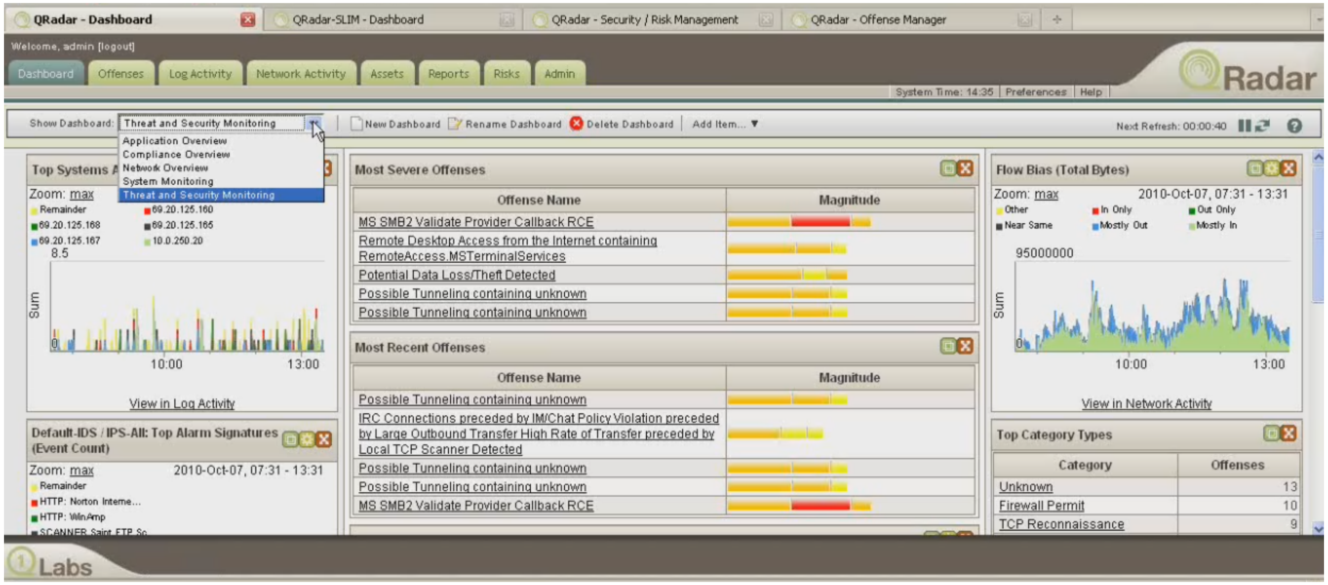
SIEM

Risk Management

Network Activity & Anomaly Detection

Network and Application Visibility

One Console Security



Most Severe Offenses

Offense Name	Magnitude
MS SMB2 Validate Provider Callback RCE	
Remote Desktop Access from the Internet containing RemoteAccess.MSTerminalServices	
Potential Data Loss/Theft Detected	
Possible Tunneling containing unknown	
Possible Tunneling containing unknown	

Most Recent Offenses

Offense Name	Magnitude
Possible Tunneling containing unknown	
IRC Connections preceded by IM/Chat Policy Violation preceded by Large Outbound Transfer High Rate of Transfer preceded by Local TCP Scanner Detected	
Possible Tunneling containing unknown	
Possible Tunneling containing unknown	
MS SMB2 Validate Provider Callback RCE	

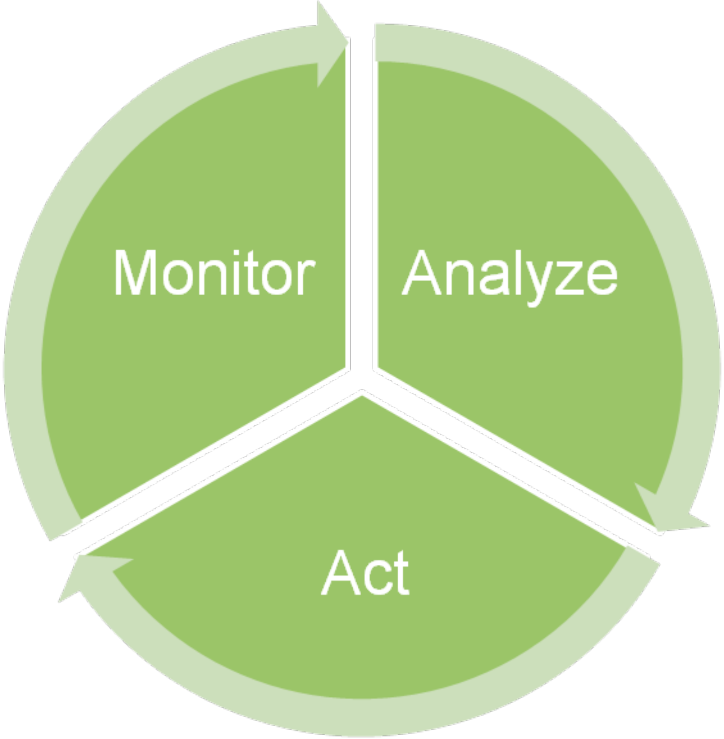
Top Category Types

Category	Offenses
Unknown	13
Firewall Permit	10
TCP Reconnaissance	9

Built on a Single Data Architecture

Automated: No need for additional staff

- Auto-discovery of log sources, applications and assets
- Asset auto-grouping
- Centralized log mgmt
- Automated configuration audits



- Asset-based prioritization
- Auto-update of threats
- Auto-response
- Directed remediation

- Auto-tuning
- Auto-detect threats
- Thousands of pre-defined rules and role based reports
- Easy-to-use event filtering
- Advanced security analytics

QRadar SIEM Technical Overview

QRadar SIEM

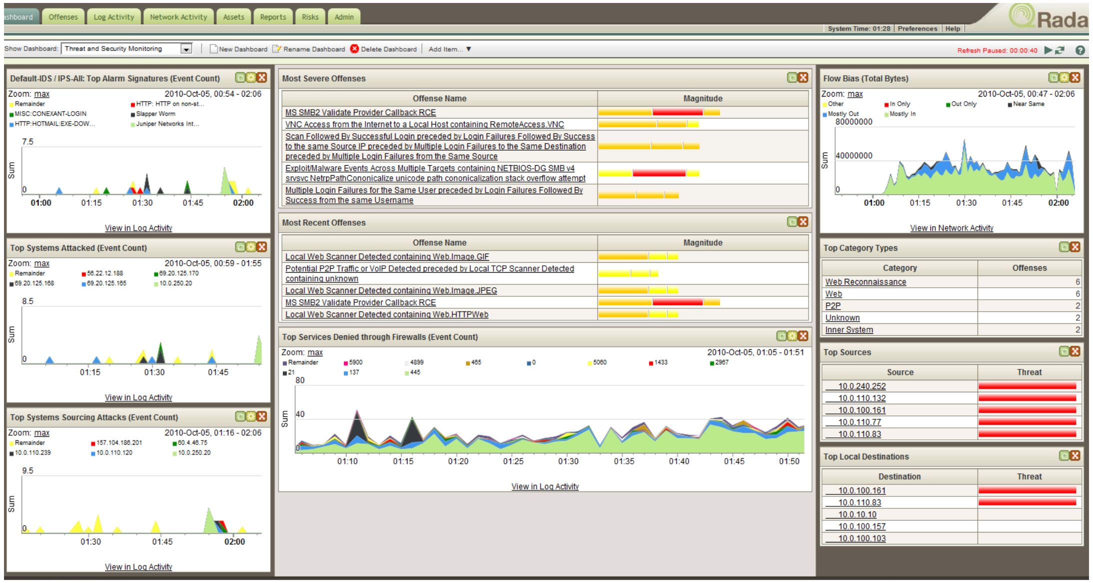
Benefits

- ✓ Reduce the risk and severity of security breaches
- ✓ Remediate security incidents faster and more thoroughly
- ✓ Ensure regulatory and internal policy compliance
- ✓ Reduce manual effort of security intelligence operations

Total Security Intelligence | An IBM Company

QRadar SIEM
Product Tour: Integrated Console

- Single browser-based UI
- Role-based access to information & functions
- Customizable dashboards (work spaces) per user
- Real-time & historical visibility and reporting



Most Severe Offenses

Offense Name	Magnitude
MS SMB2 Validate Provider Callback RCE	
VNC Access from the Internet to a Local Host containing RemoteAccess.VNC	
Scan Followed By Successful Login preceded by Login Failures Followed By Success to the same Source IP preceded by Multiple Login Failures to the Same Destination preceded by Multiple Login Failures from the Same Source	
Exploit/Malware Events Across Multiple Targets containing NETBIOS-DG SMB v4 srvsvc NetrpPathCononicalize unicode path cononicalization stack overflow attempt	
Multiple Login Failures for the Same User preceded by Login Failures Followed By Success from the same Username	

Most Recent Offenses

Offense Name	Magnitude
Local Web Scanner Detected containing Web.Image.GIF	
Potential P2P Traffic or VoIP Detected preceded by Local TCP Scanner Detected containing unknown	
Local Web Scanner Detected containing Web.Image.JPEG	
MS SMB2 Validate Provider Callback RCE	
Local Web Scanner Detected containing Web.HTTPWeb	

Top Category Types

Category	Offenses
Web Reconnaissance	6
Web	6
P2P	2
Unknown	2
Inner System	2

Top Sources

Source	Threat
10.0.240.252	🟥
10.0.110.132	🟥
10.0.100.161	🟥
10.0.110.77	🟥
10.0.110.83	🟥

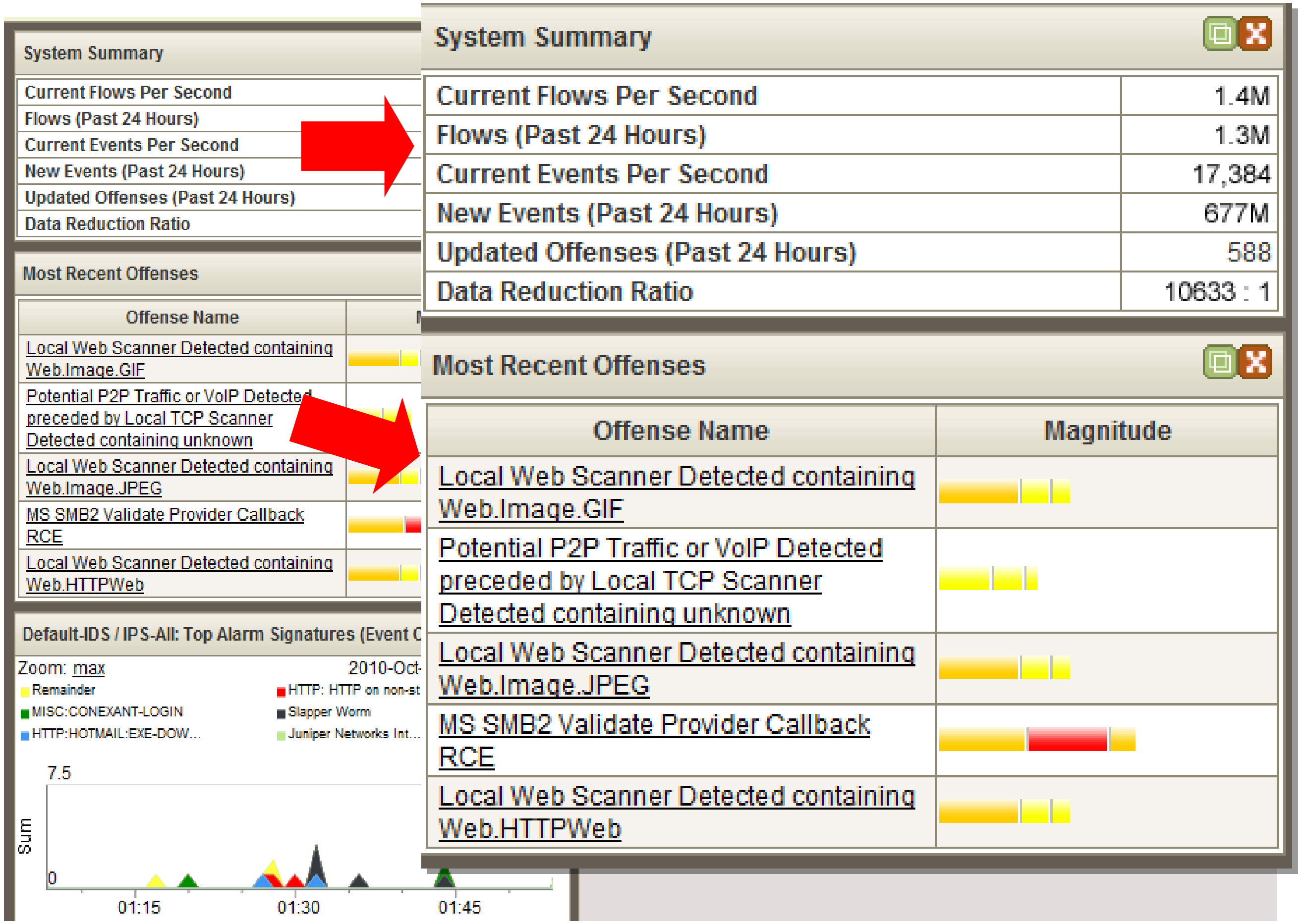
Top Local Destinations

Destination	Threat
10.0.100.161	🟥
10.0.110.83	🟥
10.0.10.10	
10.0.100.157	
10.0.100.103	

- Advanced data mining and drill down
- Easy to use rules engine with out-of-the-box security intelligence

QRadar SIEM

Product Tour: Data Reduction & Prioritization



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	10633 : 1

Most Recent Offenses

Offense Name	Magnitude
Local Web Scanner Detected containing Web.Image.GIF	
Potential P2P Traffic or VoIP Detected preceded by Local TCP Scanner Detected containing unknown	
Local Web Scanner Detected containing Web.Image.JPEG	
MS SMB2 Validate Provider Callback RCE	
Local Web Scanner Detected containing Web.HTTPWeb	

Previous 24hr period of network and security activity (2.7M logs)

↓

QRadar correlation & analysis of data creates offenses (129)

↓

Offenses are a complete history of a threat or violation with full context about accompanying network, asset and user identity information

↓

Offenses are further prioritized by business impact

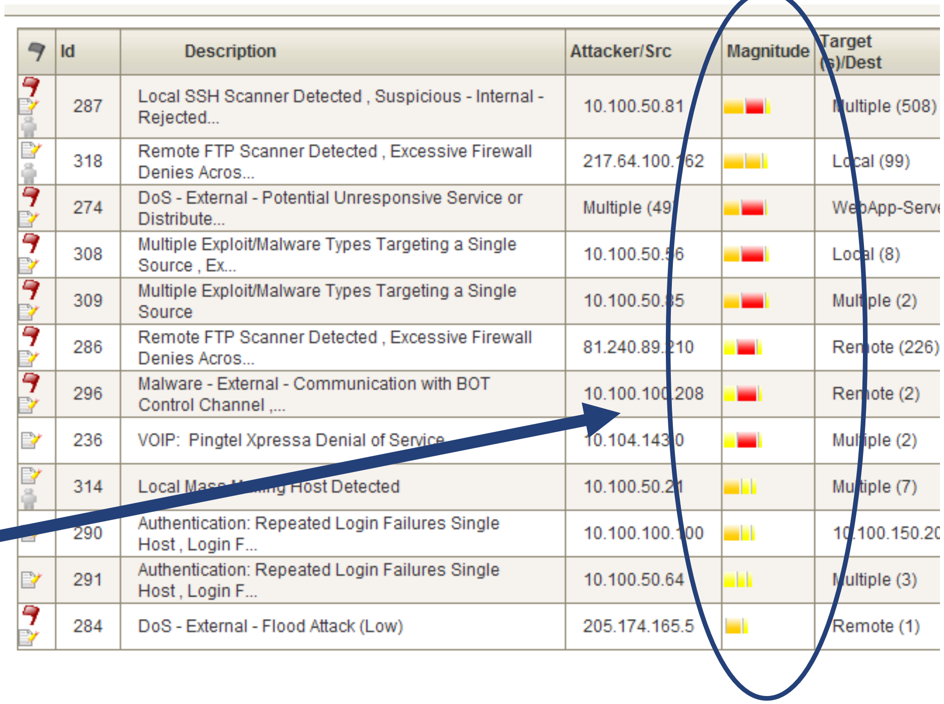
QRadar SIEM

Product Tour: Intelligent Offense Scoring

QRadar judges "magnitude" of offenses:

- *Credibility:*
  A false positive or true positive?
- *Severity:*
  Alarm level contrasted with target vulnerability
- *Relevance:*
  Priority according to asset or network value

Priorities can change over time based on situational awareness

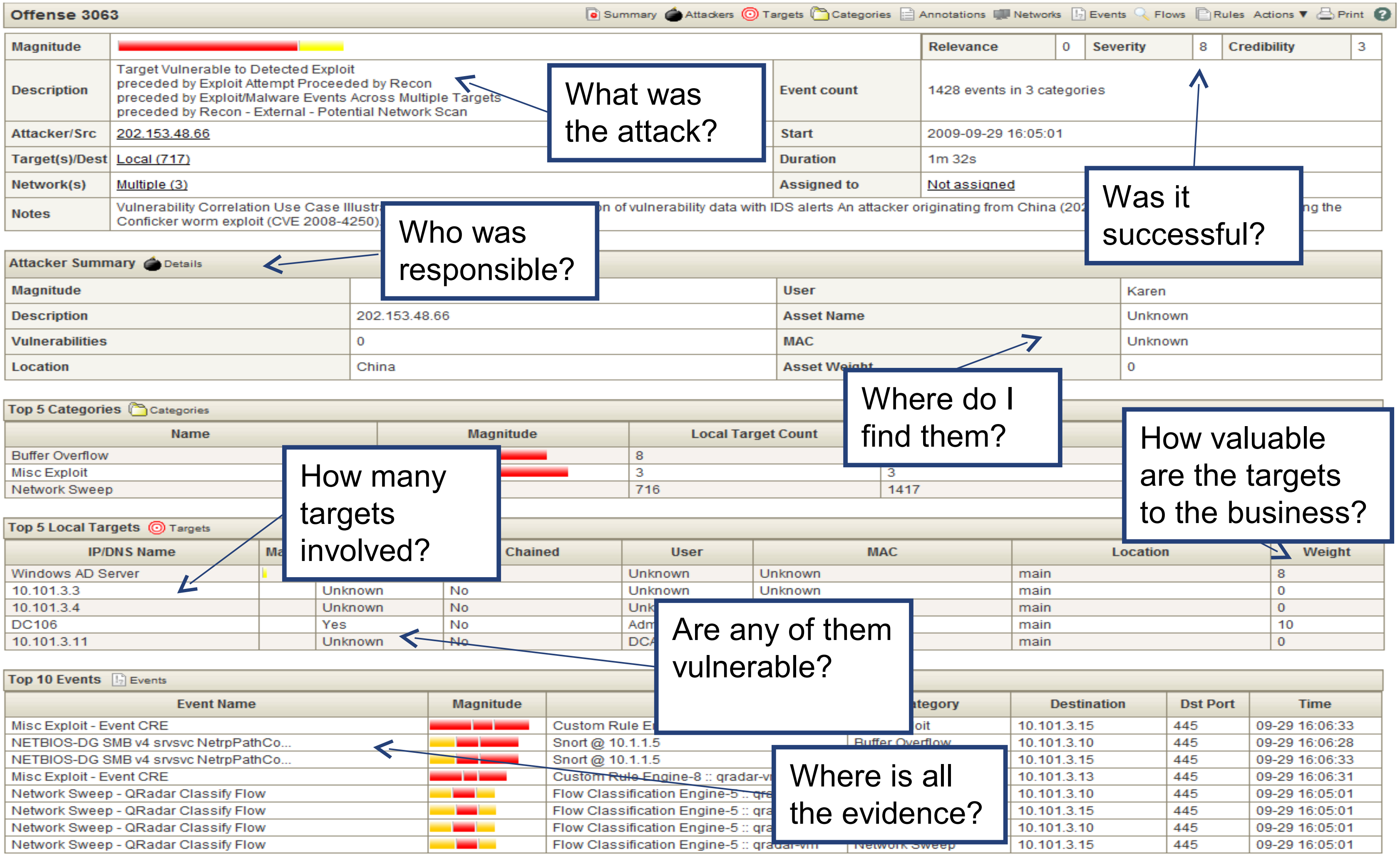


Id	Description	Attacker/Src	Magnitude	Target (s)/Dest
287	Local SSH Scanner Detected , Suspicious - Internal - Rejected...	10.100.50.81	🟨🟥	Multiple (508)
318	Remote FTP Scanner Detected , Excessive Firewall Denies Acros...	217.64.100.162	🟨🟨	Local (99)
274	DoS - External - Potential Unresponsive Service or Distribute...	Multiple (49	🟨🟥	WebApp-Serv
308	Multiple Exploit/Malware Types Targeting a Single Source , Ex...	10.100.50.56	🟨🟥	Local (8)
309	Multiple Exploit/Malware Types Targeting a Single Source	10.100.50.85	🟨🟥	Multiple (2)
286	Remote FTP Scanner Detected , Excessive Firewall Denies Acros...	81.240.89.210	🟨🟥	Remote (226)
296	Malware - External - Communication with BOT Control Channel ,...	10.100.100.208	🟨🟥	Remote (2)
236	VOIP: Pingtel Xpressa Denial of Service	10.104.143.0	🟨🟥	Multiple (2)
314	Local Mass Mailing Host Detected	10.100.50.21	🟨	Multiple (7)
290	Authentication: Repeated Login Failures Single Host , Login F...	10.100.100.100	🟨	10.100.150.2
291	Authentication: Repeated Login Failures Single Host , Login F...	10.100.50.64	🟨	Multiple (3)
284	DoS - External - Flood Attack (Low)	205.174.165.5	🟨	Remote (1)

QRadar SIEM

Product Tour: Offense Management

Clear, concise and comprehensive delivery of relevant information:



Offense 3063   Summary   Attackers   Targets   Categories   Annotations   Networks   Events   Flows   Rules   Actions ▼   Print

Magnitude			Relevance	0	Severity	8	Credibility 3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	Event count	1428 events in 3 categories				
Attacker/Src	202.153.48.66	Start	2009-09-29 16:05:01				
Target(s)/Dest	Local (717)	Duration	1m 32s				
Network(s)	Multiple (3)	Assigned to	Not assigned				
Notes	Vulnerability Correlation Use Case Illustr … n of vulnerability data with IDS alerts An attacker originating from China (202 … ng the Conficker worm exploit (CVE 2008-4250)						

Attacker Summary   Details

Magnitude		User	Karen
Description	202.153.48.66	Asset Name	Unknown
Vulnerabilities	0	MAC	Unknown
Location	China	Asset Weight	0

Top 5 Categories   Categories

Name	Magnitude	Local Target Count	
Buffer Overflow		8	
Misc Exploit		3	3
Network Sweep		716	1417

Top 5 Local Targets   Targets

IP/DNS Name	Ma		Chained	User	MAC	Location	Weight
Windows AD Server				Unknown	Unknown	main	8
10.101.3.3		Unknown	No	Unknown	Unknown	main	0
10.101.3.4		Unknown	No	Unk		main	0
DC106		Yes	No	Adm		main	10
10.101.3.11		Unknown	No	DCA		main	0

Top 10 Events   Events

Event Name	Magnitude		ategory	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule E	oit	10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5	Buffer Overflow	10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5		10.101.3.15	445	09-29 16:06:33
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-v		10.101.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qra		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qra		10.101.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qra		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01

What was the attack?

Was it successful?

Who was responsible?

Where do I find them?

How valuable are the targets to the business?

How many targets involved?

Are any of them vulnerable?

Where is all the evidence?

QRadar SIEM
Product Tour: Out-of-the-Box Rules & Searches

1000’s of real-time correlation rules and analysis tests

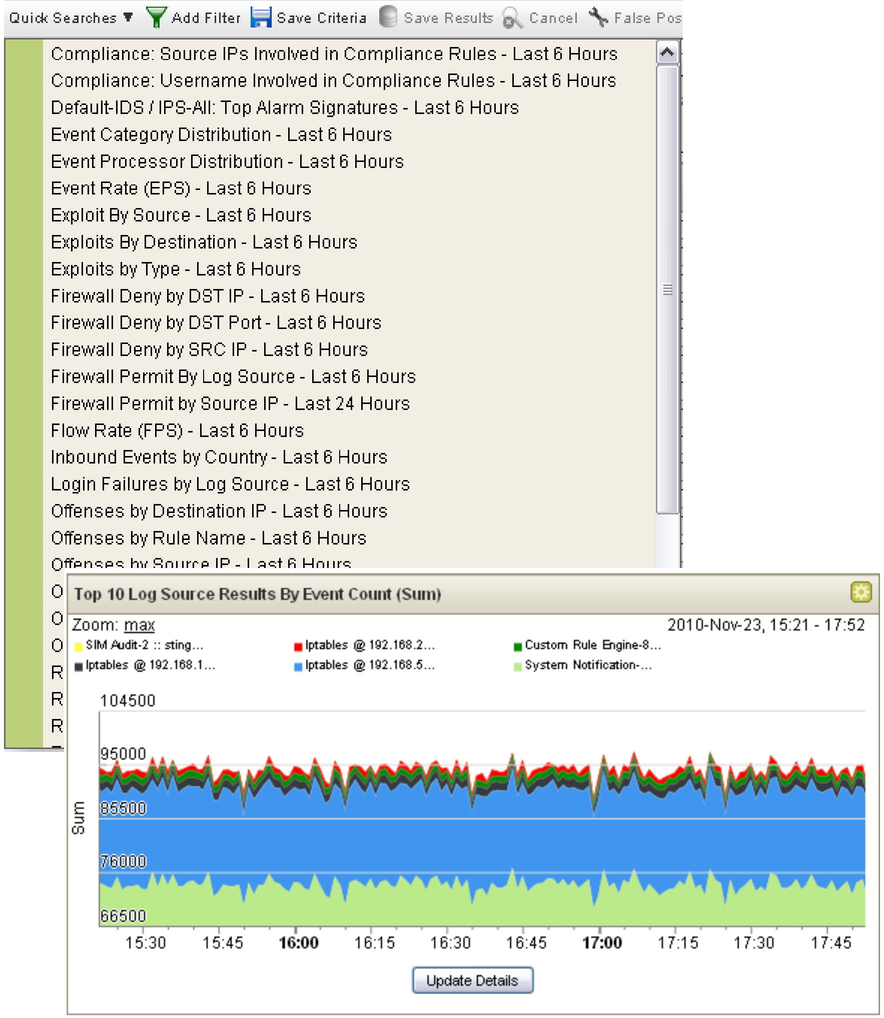
100’s of out-of-the-box searches and views of network activity and log data

- Provides quick access to critical information

Custom log fields

- Provides flexibility to extract log data for searching, reporting and dashboards. Product ships with dozens of pre-defined fields for common devices.

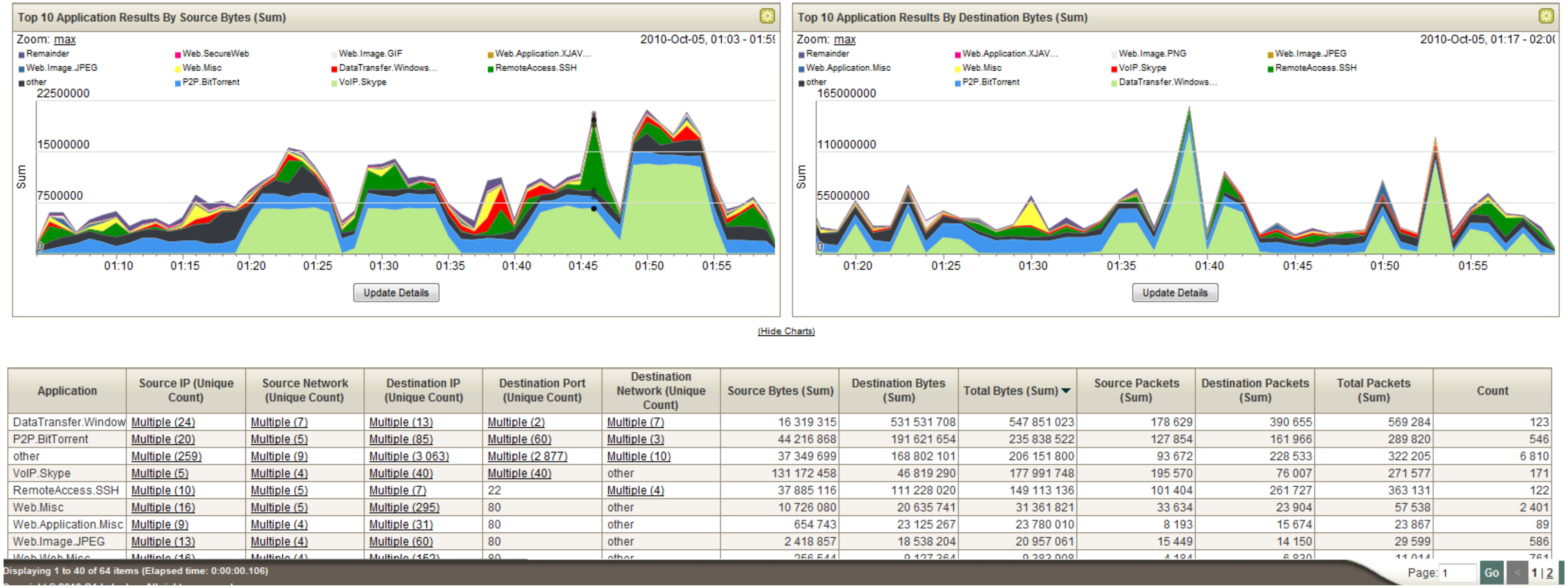
Default log queries/views



Compliance: Source IPs Involved in Compliance Rules - Last 6 Hours
Compliance: Username Involved in Compliance Rules - Last 6 Hours
Default-IDS / IPS-All: Top Alarm Signatures - Last 6 Hours
Event Category Distribution - Last 6 Hours
Event Processor Distribution - Last 6 Hours
Event Rate (EPS) - Last 6 Hours
Exploit By Source - Last 6 Hours
Exploits By Destination - Last 6 Hours
Exploits by Type - Last 6 Hours
Firewall Deny by DST IP - Last 6 Hours
Firewall Deny by DST Port - Last 6 Hours
Firewall Deny by SRC IP - Last 6 Hours
Firewall Permit By Log Source - Last 6 Hours
Firewall Permit by Source IP - Last 24 Hours
Flow Rate (FPS) - Last 6 Hours
Inbound Events by Country - Last 6 Hours
Login Failures by Log Source - Last 6 Hours
Offenses by Destination IP - Last 6 Hours
Offenses by Rule Name - Last 6 Hours
Offenses by Source IP - Last 6 Hours

Product Tour: Flows for Network Intelligence

- Detection of day-zero attacks that have no signature
- Policy monitoring and rogue server detection
- Visibility into all attacker communication
- Passive flow monitoring builds asset profiles & auto-classifies hosts
- Network visibility and problem solving (not just security related)



Top 10 Application Results By Source Bytes (Sum)

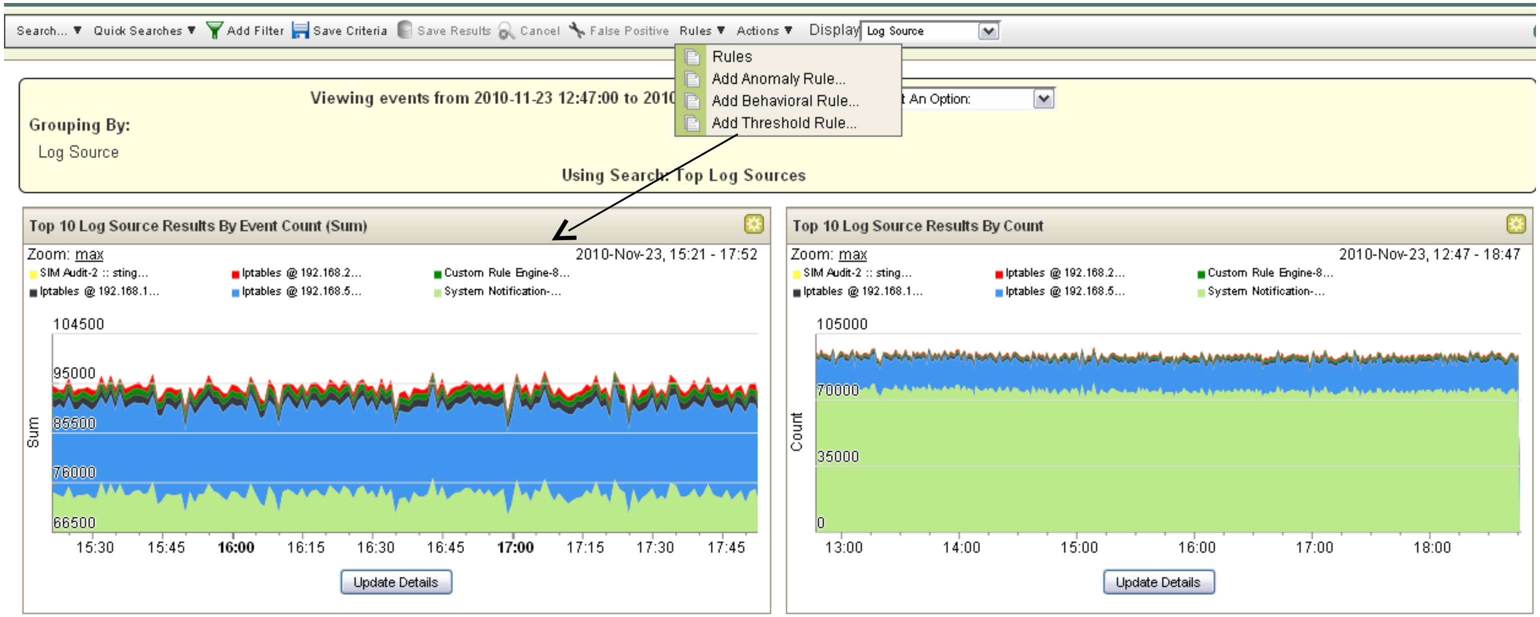
Top 10 Application Results By Destination Bytes (Sum)

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)	Total Bytes (Sum) ▼	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Count
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708	547 851 023	178 629	390 655	569 284	123
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654	235 838 522	127 854	161 966	289 820	546
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101	206 151 800	93 672	228 533	322 205	6 810
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290	177 991 748	195 570	76 007	271 577	171
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020	149 113 136	101 404	261 727	363 131	122
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741	31 361 821	33 634	23 904	57 538	2 401
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267	23 780 010	8 193	15 674	23 867	89
Web.Image.JPEG	Multiple (13)	Multiple (4)	Multiple (60)	80	other	2 418 857	18 538 204	20 957 061	15 449	14 150	29 599	586
Web.Web.Misc	Multiple (16)	Multiple (4)	Multiple (152)	80	other	256 544	9 127 364	9 383 908	4 184	6 830	11 014	761

Displaying 1 to 40 of 64 items (Elapsed time: 0:00:00.106)

QRadar SIEM
Product Tour: Flows for Application Visibility

- Flow collection from native infrastructure
- Layer 7 data collection and analysis
- Full pivoting, drill down and data mining on flow sources for advanced detection and forensic examination
- Visibility and alerting according to rule/policy, threshold, behavior or anomaly conditions across network and log activity



Viewing events from 2010-11-23 12:47:00 to 2010

Grouping By:
Log Source

Using Search: Top Log Sources

Top 10 Log Source Results By Event Count (Sum)

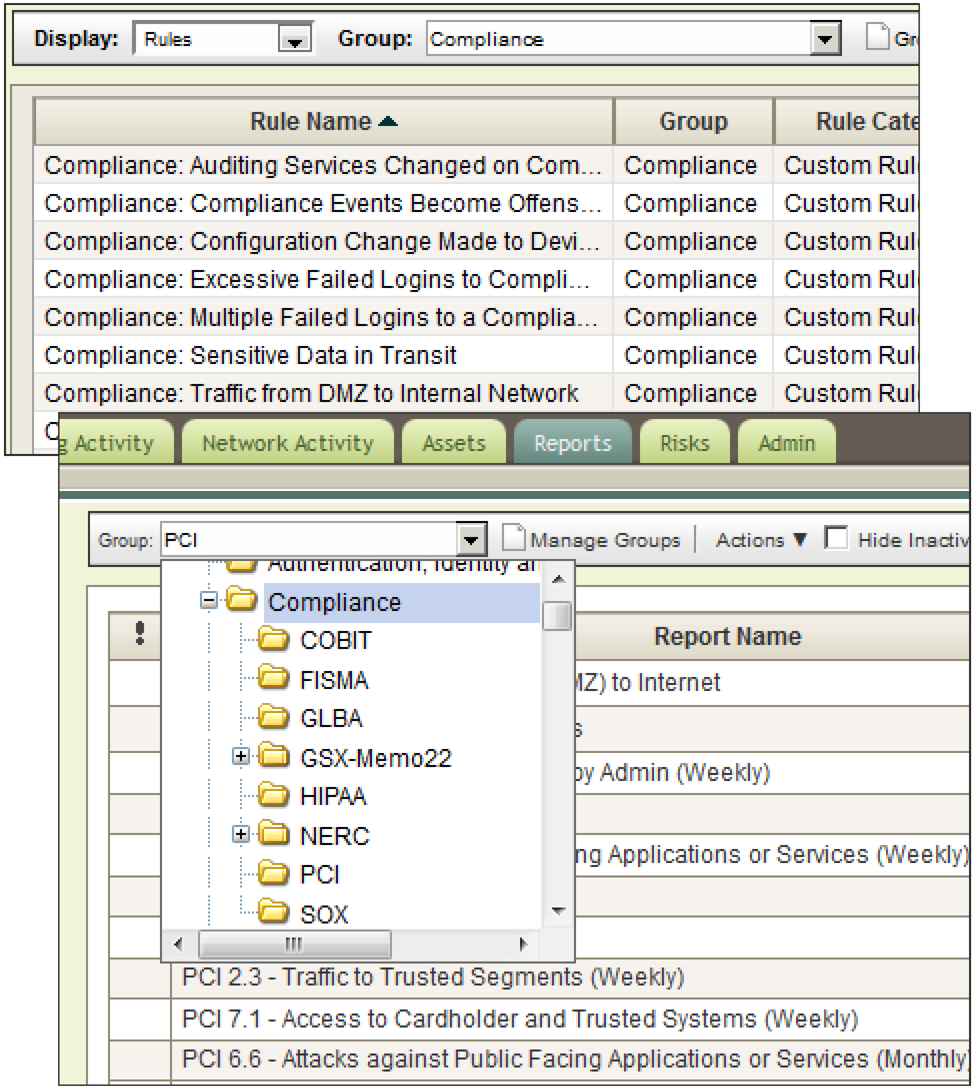
2010-Nov-23, 15:21 - 17:52

Top 10 Log Source Results By Count

2010-Nov-23, 12:47 - 18:47

QRadar SIEM

Product Tour: Compliance Rules and Reports



Rule Name ▲	Group	Rule Cate
Compliance: Auditing Services Changed on Com...	Compliance	Custom Rul
Compliance: Compliance Events Become Offens...	Compliance	Custom Rul
Compliance: Configuration Change Made to Devi...	Compliance	Custom Rul
Compliance: Excessive Failed Logins to Compli...	Compliance	Custom Rul
Compliance: Multiple Failed Logins to a Complia...	Compliance	Custom Rul
Compliance: Sensitive Data in Transit	Compliance	Custom Rul
Compliance: Traffic from DMZ to Internal Network	Compliance	Custom Rul

!	Report Name
	MZ) to Internet
	s
	by Admin (Weekly)
	ng Applications or Services (Weekly)
	PCI 2.3 - Traffic to Trusted Segments (Weekly)
	PCI 7.1 - Access to Cardholder and Trusted Systems (Weekly)
	PCI 6.6 - Attacks against Public Facing Applications or Services (Monthly)

- Out-of-the-box templates for specific regulations and best practices:
  - COBIT, SOX, GLBA, NERC, FISMA, PCI, HIPAA, UK GCSx
- Easily modified to include new definitions
- Extensible to include new regulations and best practices
- Can leverage existing correlation rules

QRadar SIEM
Use Cases

QRadar SIEM excels at the most challenging use cases:

- ✓ Complex threat detection
- ✓ Malicious activity identification
- ✓ User activity monitoring
- ✓ Compliance monitoring
- ✓ Fraud detection and data loss prevention
- ✓ Network and asset discovery

Use Case: Complex Threat Detection

Problem Statement

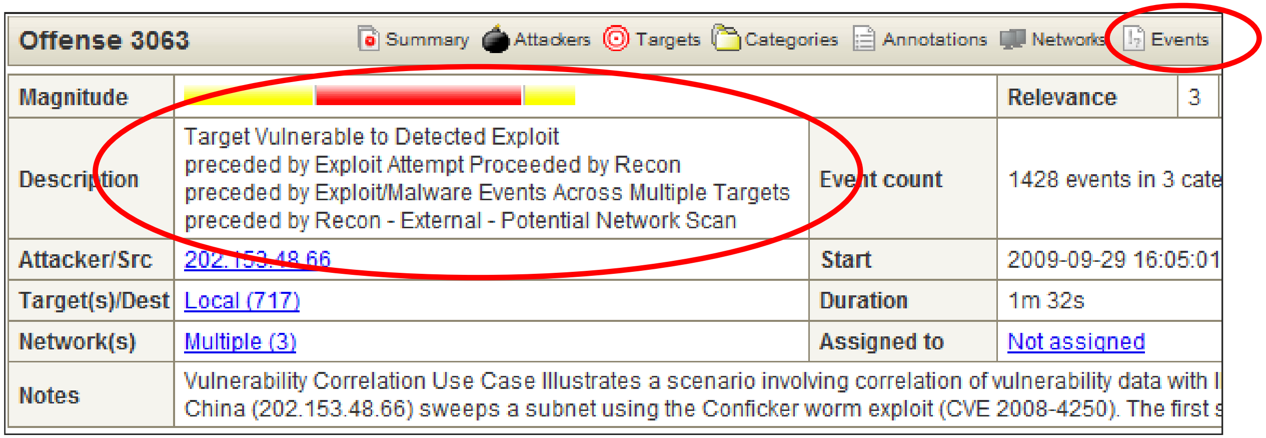
- Finding the single needle in the ‘needle stack’
- Connecting patterns across many data silos and huge volumes of information
- Prioritizing attack severity against target value and relevance
- Understanding the impact of the threat

Required Visibility

- Normalized event data
- Asset knowledge
- Vulnerability context
- Network telemetry

QRadar SIEM

Use Case: Complex Threat Detection



Offense 3063

Magnitude		Relevance	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	Event count	1428 events in 3 cate
Attacker/Src	202.153.48.66	Start	2009-09-29 16:05:01
Target(s)/Dest	Local (717)	Duration	1m 32s
Network(s)	Multiple (3)	Assigned to	Not assigned
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with I China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first s		

Sounds Nasty…

But how do we know this?

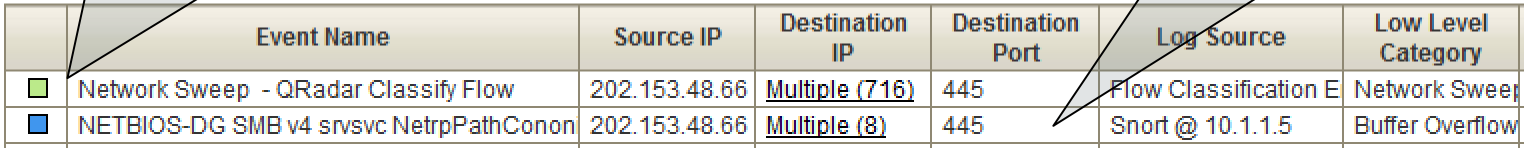
The evidence is a single click away.

Network Scan

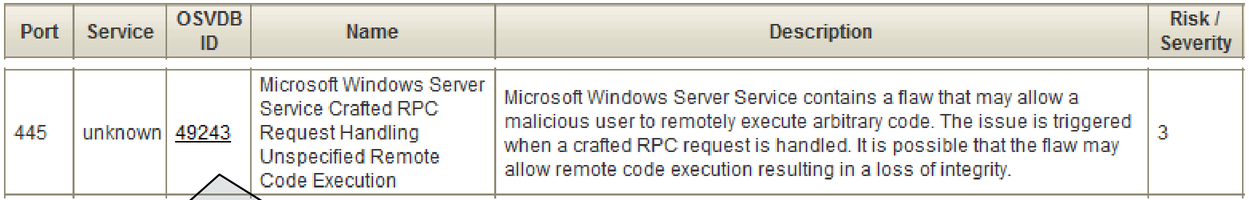
Detected by QFlow

Buffer Overflow

Exploit attempt seen by Snort



	Event Name	Source IP	Destination IP	Destination Port	Log Source	Low Level Category
🟩	Network Sweep - QRadar Classify Flow	202.153.48.66	Multiple (716)	445	Flow Classification E	Network Sweep
🟦	NETBIOS-DG SMB v4 srvsvc NetrpPathConon	202.153.48.66	Multiple (8)	445	Snort @ 10.1.1.5	Buffer Overflow



Port	Service	OSVDB ID	Name	Description	Risk / Severity
445	unknown	49243	Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution	Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity.	3

Targeted Host Vulnerable

Detected by Nessus

Total Security Intelligence

Convergence of Network, Event and Vulnerability data

QRadar SIEM

Use Case: Malicious Activity Identification

Problem Statement

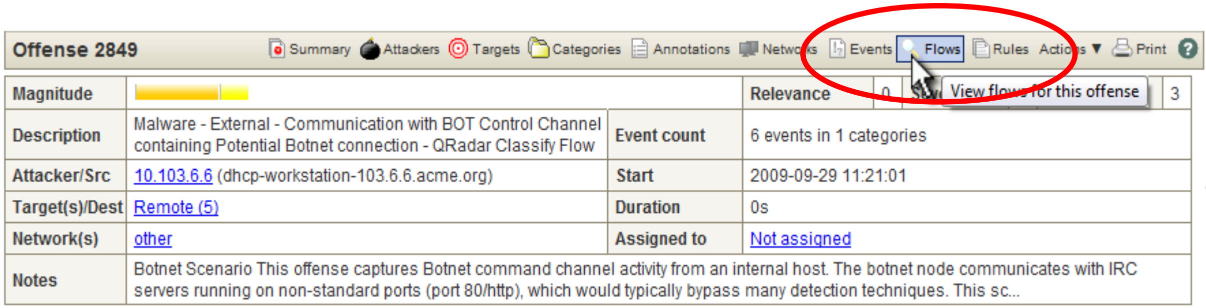
- Distributed infrastructure
- Security blind spots in the network
- Malicious activity that promiscuously seeks ‘targets of opportunity’
- Application layer threats and vulnerabilities
- Siloed security telemetry
- Incomplete forensics

Required Visibility

- Distributed detection sensors
- Pervasive visibility across enterprise
- Application layer knowledge
- Content capture for impact analysis

QRadar SIEM

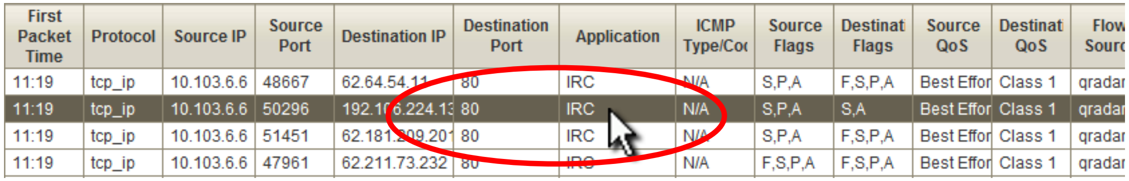
Use Case: Malicious Activity Identification



Magnitude		Relevance	0 … 3
Description	Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow	Event count	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...		

Potential Botnet Detected?

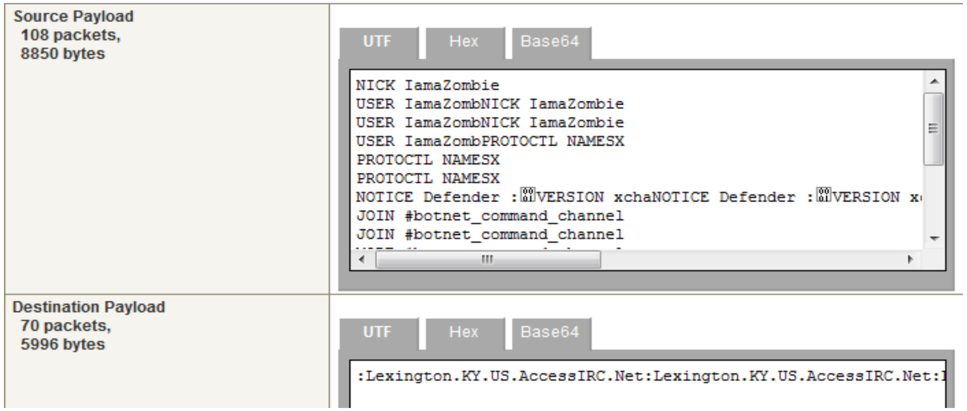
This is as far as traditional SIEM can go.



First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Coc	Source Flags	Destinat Flags	Source QoS	Destinat QoS	Flow Sourc
11:19	tcp_ip	10.103.6.6	48667	62.64.54.11	80	IRC	N/A	S,P,A	F,S,P,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	50296	192.106.224.13	80	IRC	N/A	S,P,A	S,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	51451	62.181.209.201	80	IRC	N/A	S,P,A	F,S,P,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A	F,S,P,A	Best Effor	Class 1	qradar

IRC on port 80?

QFlow enables detection of a covert channel.



Source Payload
108 packets,
8850 bytes

```
NICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombPROTOCTL NAMESX
PROTOCTL NAMESX
PROTOCTL NAMESX
NOTICE Defender :␁VERSION xchaNOTICE Defender :␁VERSION x
JOIN #botnet_command_channel
JOIN #botnet_command_channel
```

Destination Payload
70 packets,
5996 bytes

```
:Lexington.KY.US.AccessIRC.Net:Lexington.KY.US.AccessIRC.Net:
```

Irrefutable Botnet Communication

Layer 7 data contains botnet command and control instructions.

QRadar SIEM

Use Case: User Activity Monitoring

Problem Statement

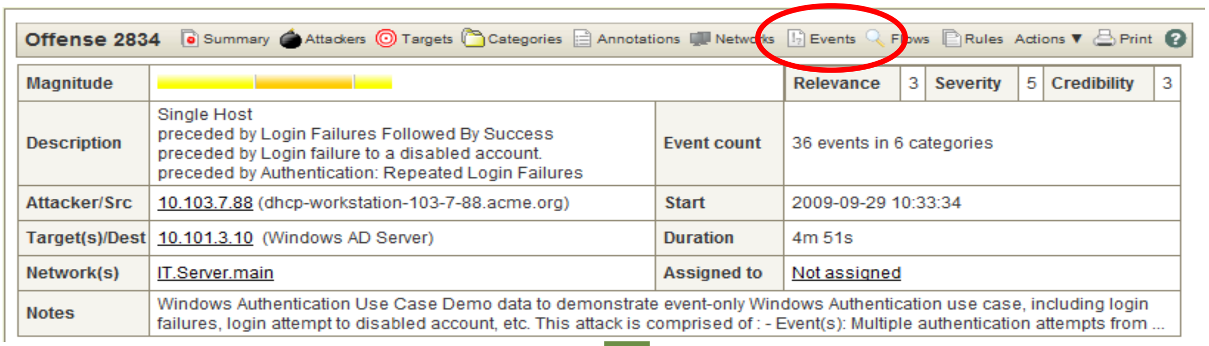
- Monitoring of privileged and non-privileged users
- Isolating ‘Stupid user tricks’ from malicious account activity
- Associating users with machines and IP addresses
- Normalizing account and user information across diverse platforms

Required Visibility

- Centralized logging and intelligent normalization
- Correlation of IAM information with machine and IP addresses
- Automated rules and alerts focused on user activity monitoring

QRadar SIEM

Use Case: User Activity Monitoring

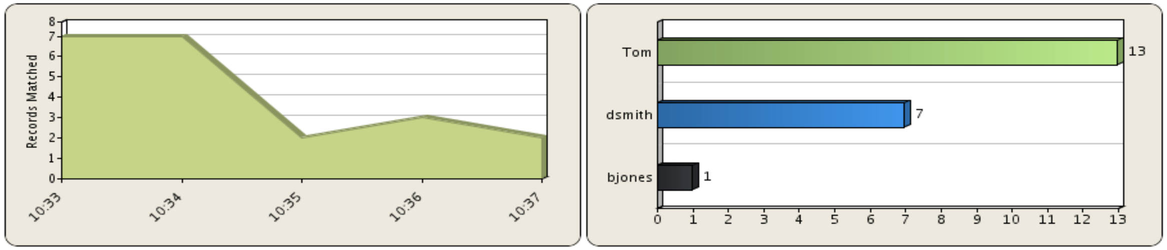


Offense 2834

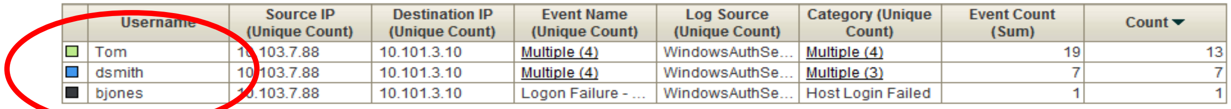
Magnitude			Relevance	3	Severity	5	Credibility 3
Description	Single Host preceded by Login Failures Followed By Success preceded by Login failure to a disabled account. preceded by Authentication: Repeated Login Failures	Event count	36 events in 6 categories				
Attacker/Src	10.103.7.88 (dhcp-workstation-103-7-88.acme.org)	Start	2009-09-29 10:33:34				
Target(s)/Dest	10.101.3.10 (Windows AD Server)	Duration	4m 51s				
Network(s)	IT.Server.main	Assigned to	Not assigned				
Notes	Windows Authentication Use Case Demo data to demonstrate event-only Windows Authentication use case, including login failures, login attempt to disabled account, etc. This attack is comprised of : - Event(s): Multiple authentication attempts from ...						

Authentication Failures

Perhaps a user who forgot his/her password?



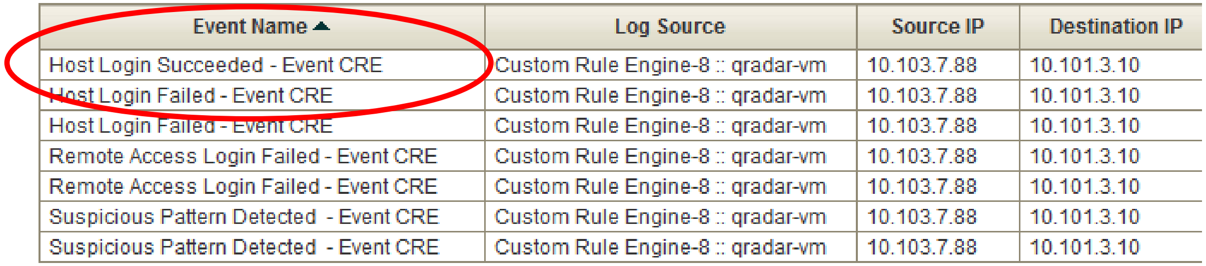
(Hide Charts)



	Username	Source IP (Unique Count)	Destination IP (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Category (Unique Count)	Event Count (Sum)	Count ▼
🟩	Tom	10.103.7.88	10.101.3.10	Multiple (4)	WindowsAuthSe...	Multiple (4)	19	13
🟦	dsmith	10.103.7.88	10.101.3.10	Multiple (4)	WindowsAuthSe...	Multiple (3)	7	7
■	bjones	10.103.7.88	10.101.3.10	Logon Failure - ...	WindowsAuthSe...	Host Login Failed	1	1

Brute Force Password Attack

Numerous failed login attempts against different user accounts



Event Name ▲	Log Source	Source IP	Destination IP
Host Login Succeeded - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Host Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Host Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Remote Access Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Remote Access Login Failed - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Suspicious Pattern Detected - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10
Suspicious Pattern Detected - Event CRE	Custom Rule Engine-8 :: qradar-vm	10.103.7.88	10.101.3.10

Host Compromised

All this followed by a successful login.

Automatically detected, no custom tuning required.

QRadar SIEM

Use Case: Compliance Monitoring

Problem Statement

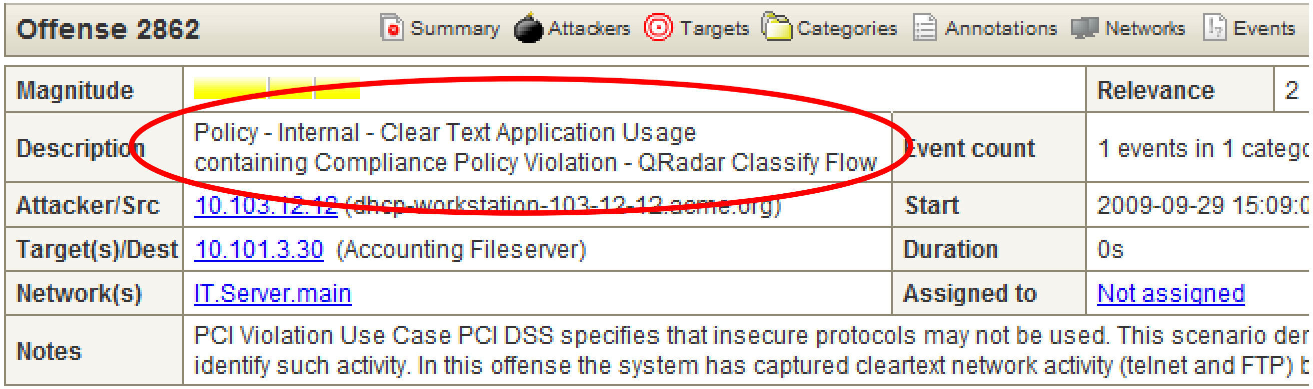
- Validating your monitoring efforts against compliance requirements
- Ensuring that compliance goals align with security goals
- Logs alone don’t meet compliance standards

Required Visibility

- Application layer visibility
- Visibility into network segments where logging is problematic

QRadar SIEM

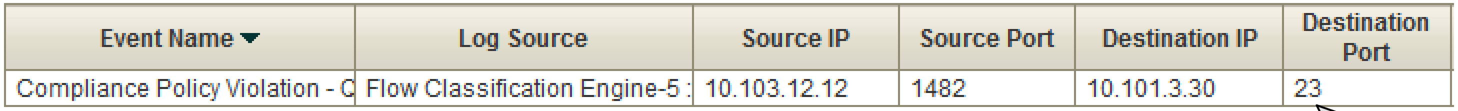
Use Case: Compliance Monitoring



Offense 2862

Magnitude		Relevance	2
Description	Policy - Internal - Clear Text Application Usage containing Compliance Policy Violation - QRadar Classify Flow	Event count	1 events in 1 catego
Attacker/Src	10.103.12.12 (dhcp-workstation-103-12-12.acme.org)	Start	2009-09-29 15:09:0
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 der identify such activity. In this offense the system has captured cleartext network activity (telnet and FTP) b		

PCI Compliance at Risk?



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

Unencrypted Traffic

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.

QRadar SIEM

Use Case: Fraud & Data Loss Prevention

Problem Statement

- Malicious activity against ‘targets of choice’
- Privileged or knowledgeable users internal to the network
- Fraud patterns that are ‘low and slow’ by nature
- Associating suspicious patterns across network, security, application and host layers in the infrastructure

Required Visibility

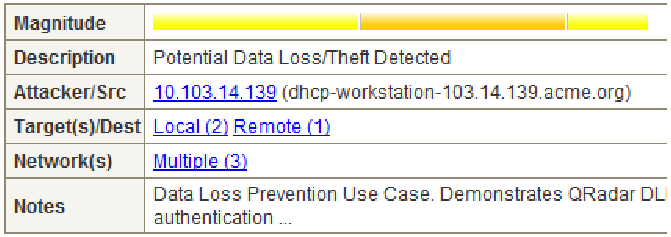
- Ability to take and normalize telemetry across many diverse sources
- Correlation of host and asset profiles with IAM infrastructure
- Integration of 3rd party intelligence sources

QRadar SIEM

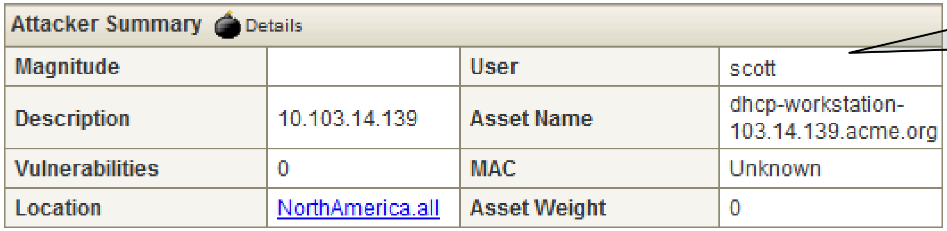
Use Case: Fraud & Data Loss Prevention

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 (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

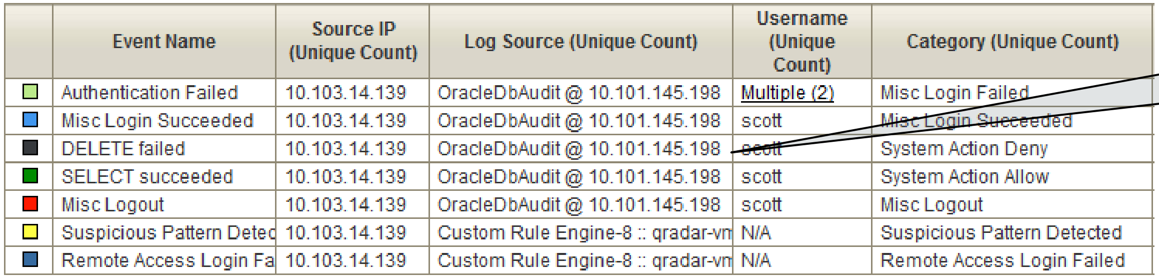


Attacker Summary Details

Magnitude		User	scott
Description	10.103.14.139	Asset Name	dhcp-workstation-103.14.139.acme.org
Vulnerabilities	0	MAC	Unknown
Location	NorthAmerica.all	Asset Weight	0

Who?

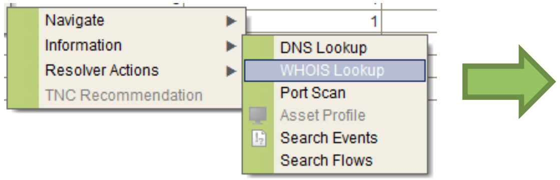
An internal user

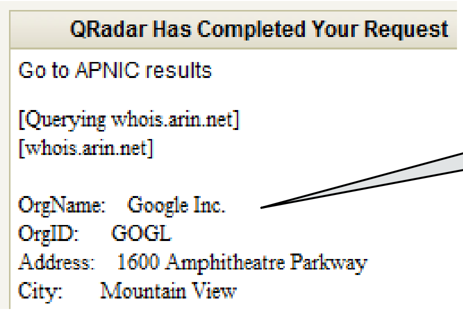


	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
🟩	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
🟦	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
⬛	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 SIEM

Use Case: Network and Asset Discovery

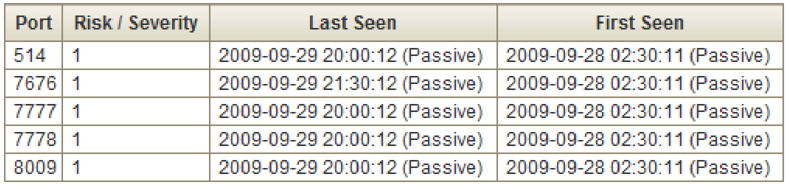
Problem Statement

- Integration of asset information into security monitoring products is labor intensive
- Assets you don’t know about pose the greatest risk
- Asset discovery and classification is a key tenet of many compliance regulations
- False positive noise jeopardizes effectiveness of a SIEM solution

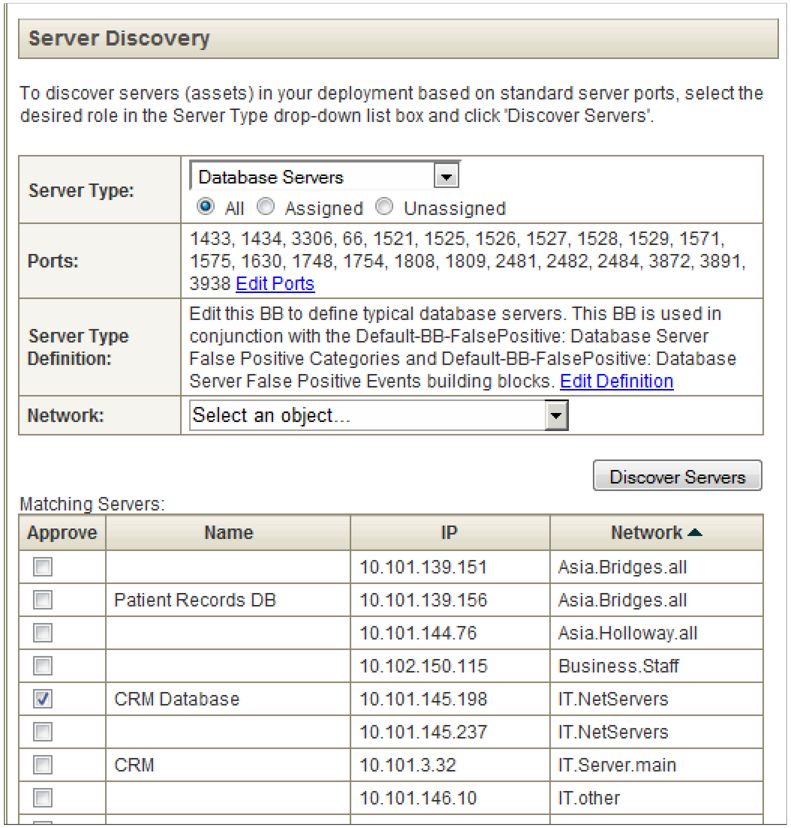
Required Capability

- Real-time knowledge of all assets on a network
- Visibility into asset communication patterns
- Classification of asset types
- Tight integration into pre-defined rules

QRadar SIEM
Use Case: Network and Asset Discovery



Port	Risk / Severity	Last Seen	First Seen
514	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
7676	1	2009-09-29 21:30:12 (Passive)	2009-09-28 02:30:11 (Passive)
7777	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
7778	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
8009	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)



Server Discovery

To discover servers (assets) in your deployment based on standard server ports, select the desired role in the Server Type drop-down list box and click 'Discover Servers'.

Server Type:	Database Servers ▾ ● All ○ Assigned ○ Unassigned
Ports:	1433, 1434, 3306, 66, 1521, 1525, 1526, 1527, 1528, 1529, 1571, 1575, 1630, 1748, 1754, 1808, 1809, 2481, 2482, 2484, 3872, 3891, 3938 Edit Ports
Server Type Definition:	Edit this BB to define typical database servers. This BB is used in conjunction with the Default-BB-FalsePositive: Database Server False Positive Categories and Default-BB-FalsePositive: Database Server False Positive Events building blocks. Edit Definition
Network:	Select an object... ▾

Matching Servers:

Approve	Name	IP	Network ▲
□		10.101.139.151	Asia.Bridges.all
□	Patient Records DB	10.101.139.156	Asia.Bridges.all
□		10.101.144.76	Asia.Holloway.all
□		10.102.150.115	Business.Staff
☑	CRM Database	10.101.145.198	IT.NetServers
□		10.101.145.237	IT.NetServers
□	CRM	10.101.3.32	IT.Server.main
□		10.101.146.10	IT.other

Automatic Asset Discovery

Creates host profiles as network activity is seen to/from

Passive Asset Profiling

Identifies services and ports on hosts by watching network activity

Server Discovery

Identifies & classifies server infrastructure based on these asset profiles

Correlation on new assets & services

Rules can fire when new assets and services come online

Enabled by ***QRadar QFlow and QRadar VFlow***

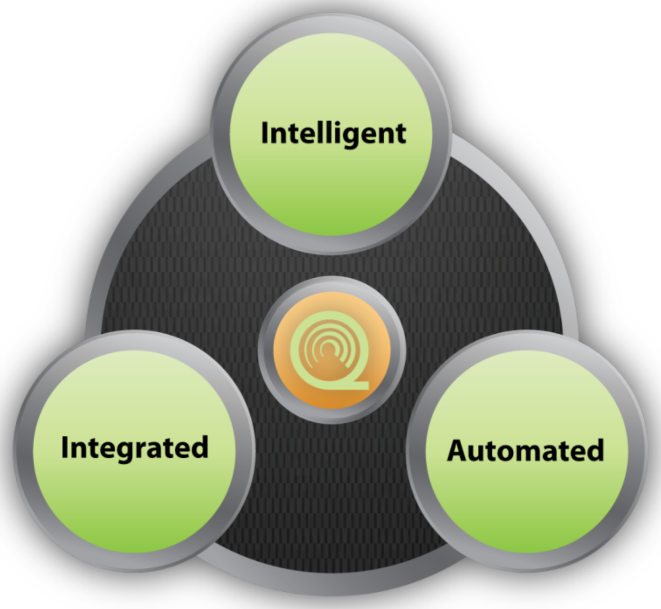
Total Security Intelligence | An IBM Company

QRadar SIEM

Intelligent, Integrated and Automated

- Intelligent offense management
- Layer 7 application visibility
- Identifies most critical anomalies

- Distributed architecture
- Highly scalable
- Analyze logs, flows, assets and more



- Easy deployment
- Rapid time to value
- Operational efficiency

QRadar SIEM

Summary

QRadar SIEM delivers full visibility and actionable insight for

Total Security Intelligence.

Deepest Content Insight

Broadest Correlation

Greatest Scalability

Providing complete network and security intelligence, delivered simply, for any customer

Thank You!

Zenith Systems (Q1Labs/IBM Partner)
Business Centre, William Nicole Rd
Fourways, Johannesburg
email: sales@zenithsystems.co.za

Time	Topic	Speakers
9:05am - 9:45am	Security Stream Kickoff-Security and compliance Overview and X Force	Joe Ruthven and Sukhdev Singh
9:45am - 10:25am	Threat	Lekgale Mokota
10:25am - 10:40am	Break	
10:40am - 11:10am	Q1 Labs Security Intelligence Strategy and Roadmap – How to use Security Intelligence for detecting threats and exceeding compliance mandates	Murray Benadie
11:10am - 11:40am	**Driving Effective Application Security in the Enterprise: An End to End Approach to Addressing One of the Biggest Threats to a Business**	Sukhdev Singh
11.40am - 12:10pm	Identity Intelligence: Enabling Secure Cloud and Mobile Access	Kevin Mckerr (Puleng)
12:10pm - 12:15 pm	Closing and Questions	
12:15pm	Lunch and Networking	

Security Intelligence.

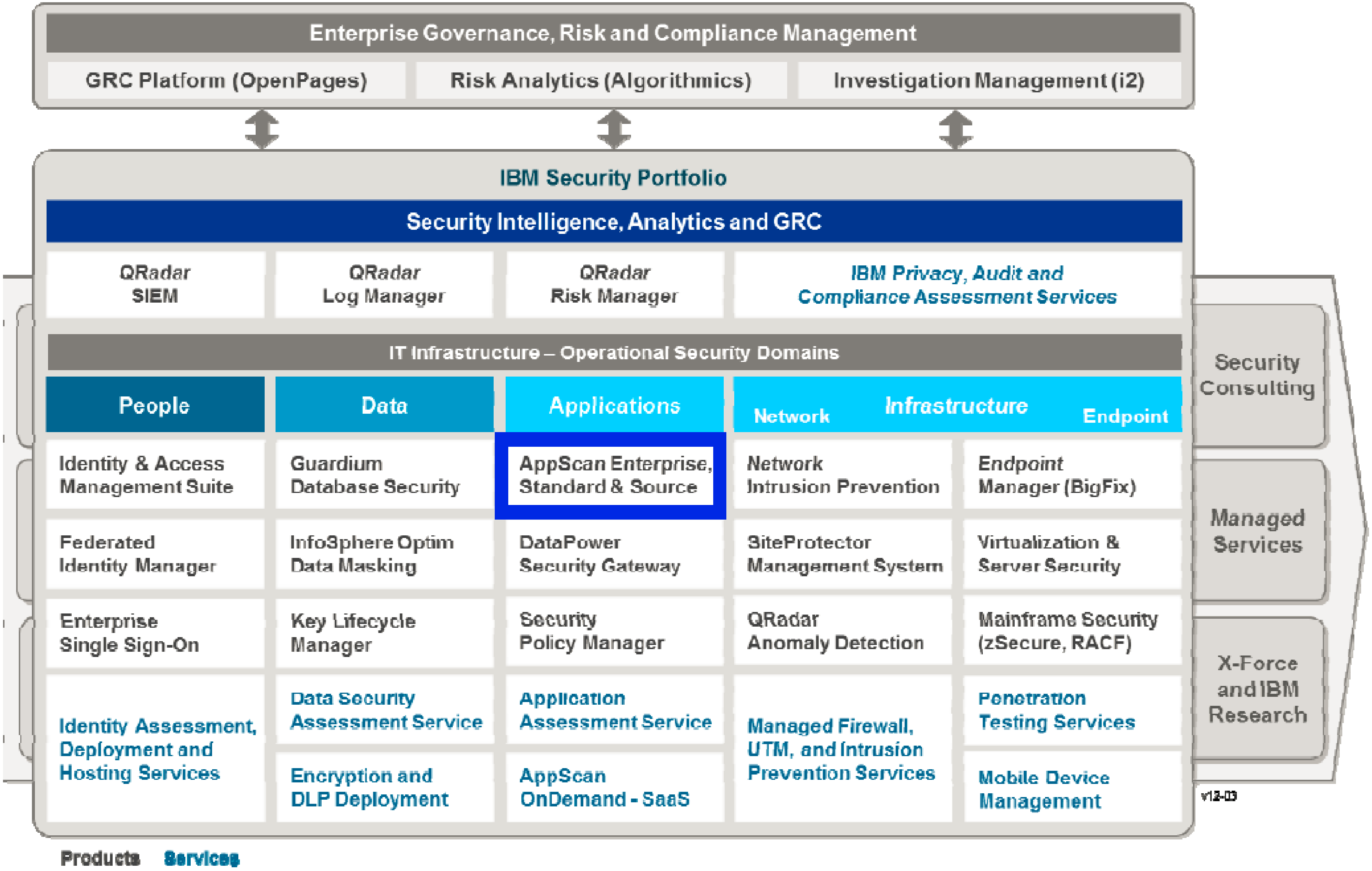
Think Integrated.

Driving Effective Application Security

Sukhdev Singh

CISSP ,CISSM, X Force Expert, Certified Enterprise Architect …

Technical Leader , Growth Markets, IBM Security Systems



Enterprise Governance, Risk and Compliance Management

GRC Platform (OpenPages) | Risk Analytics (Algorithmics) | Investigation Management (i2)

IBM Security Portfolio

Security Intelligence, Analytics and GRC

QRadar SIEM | QRadar Log Manager | QRadar Risk Manager | *IBM Privacy, Audit and Compliance Assessment Services*

IT Infrastructure – Operational Security Domains

People	Data	Applications	Infrastructure	
			Network	Endpoint
Identity & Access Management Suite	Guardium Database Security	AppScan Enterprise, Standard & Source	Network Intrusion Prevention	Endpoint Manager (BigFix)
Federated Identity Manager	InfoSphere Optim Data Masking	DataPower Security Gateway	SiteProtector Management System	Virtualization & Server Security
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection	Mainframe Security (zSecure, RACF)
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service	Application Assessment Service	Managed Firewall, UTM, and Intrusion Prevention Services	Penetration Testing Services
	Encryption and DLP Deployment	AppScan OnDemand - SaaS		Mobile Device Management

Security Consulting

Managed Services

X-Force and IBM Research

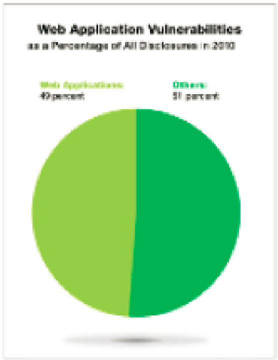
v12-03

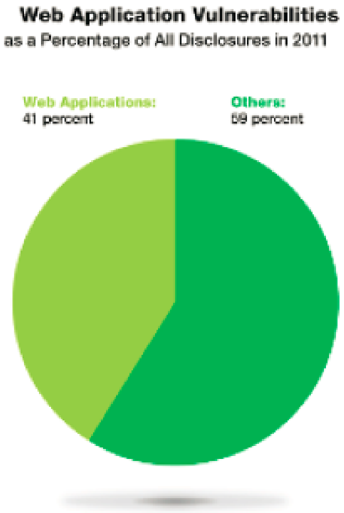
Products **Services**

Application security challenges: vulnerabilities

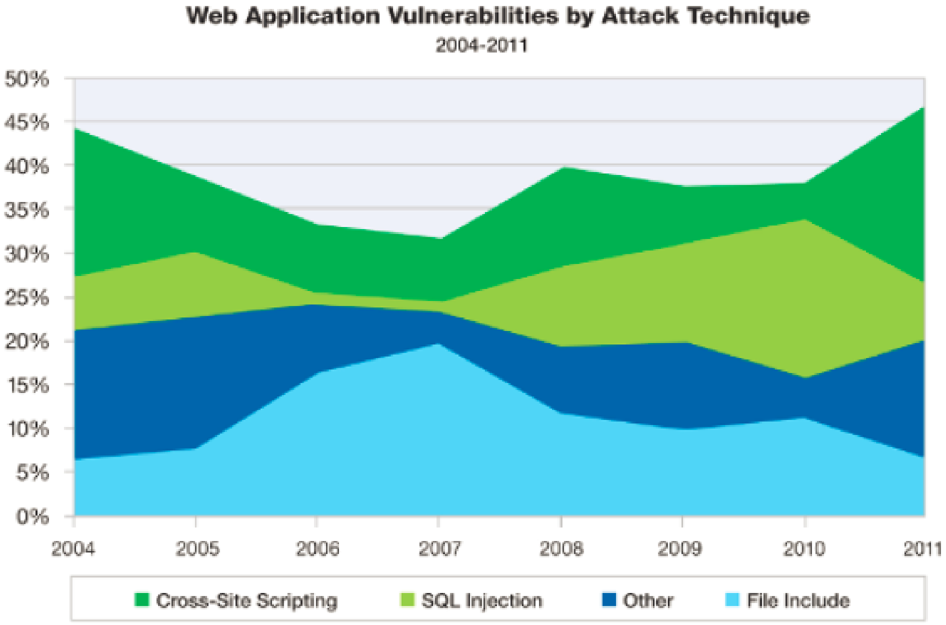
In 2011, 41% of security vulnerabilities affected web applications

- Down from 49% in 2010
- Lowest percentage seen since 2005


Web Application Vulnerabilities
as a Percentage of All Disclosures in 2010


Web Application Vulnerabilities
as a Percentage of All Disclosures in 2011

Source: IBM X-Force® Research and Development


Web Application Vulnerabilities by Attack Technique
2004-2011

Source: IBM X-Force® Research and Development

The Myth: "Our Site Is Safe"

We Have Firewalls and IPS in Place

Port 80 & 443 are open for the right reasons

We Audit It Once a Quarter with Pen Testers

Applications are constantly changing

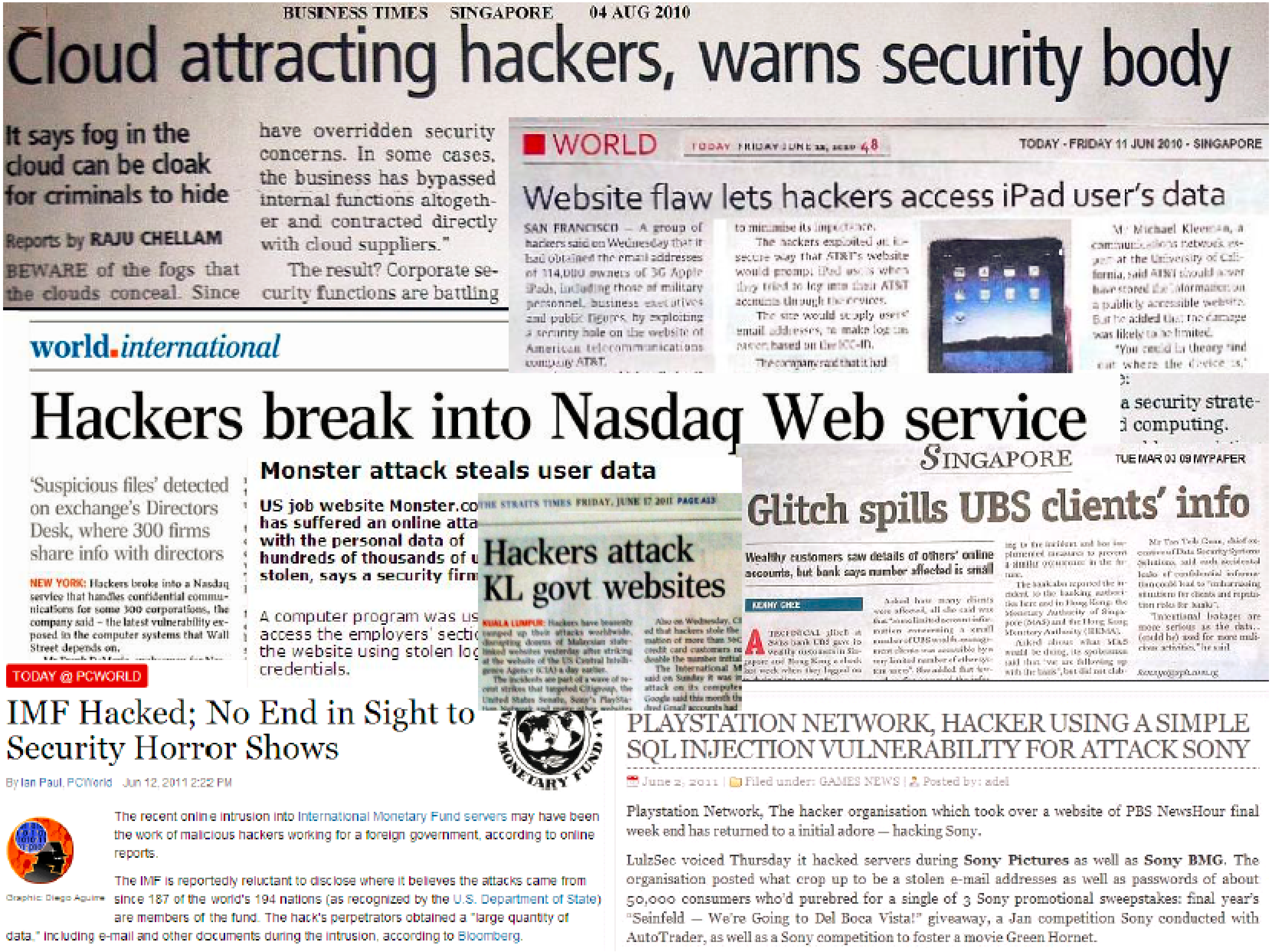
We Use Network Vulnerability Scanners

Neglect the security of the software on the network/web server

We Use SSL Encryption

Only protects data between site and user not the web application itself

Over the past 20 years, we have invested much resources and efforts in network and infrastructure security.



BUSINESS TIMES SINGAPORE 04 AUG 2010

Cloud attracting hackers, warns security body

It says fog in the cloud can be cloak for criminals to hide

Reports by RAJU CHELLAM

BEWARE of the fogs that the clouds conceal. Since

have overridden security concerns. In some cases, the business has bypassed internal functions altogether and contracted directly with cloud suppliers."

The result? Corporate security functions are battling

a security strategy

d computing.

WORLD TODAY FRIDAY JUNE 11, 2010 48 TODAY - FRIDAY 11 JUN 2010 - SINGAPORE

Website flaw lets hackers access iPad user's data

SAN FRANCISCO — A group of hackers said on Wednesday that it had obtained the email addresses of 114,000 owners of 3G Apple iPads, including those of military personnel, business executives and public figures, by exploiting a security hole on the website of American telecommunications company AT&T.

to minimise its importance.

The hackers exploited an insecure way that AT&T's website would prompt iPad users when they tried to log into their AT&T accounts through the devices.

The site would supply users' email addresses, to make log-on easier, based on the ICC-ID.

The company said that it had

Mr Michael Kleeman, a communications network expert at the University of California, said AT&T should never have stored the information on a publicly accessible website. But he added that the damage was likely to be limited.

"You could in theory find out where the device is,"

world.*international*

Hackers break into Nasdaq Web service

'Suspicious files' detected on exchange's Directors Desk, where 300 firms share info with directors

NEW YORK: Hackers broke into a Nasdaq service that handles confidential communications for some 300 corporations, the company said – the latest vulnerability exposed in the computer systems that Wall Street depends on.

Monster attack steals user data

US job website Monster.co has suffered an online atta with the personal data of hundreds of thousands of u stolen, says a security firm

A computer program was us access the employers' sectio the website using stolen log credentials.

THE STRAITS TIMES FRIDAY, JUNE 17 2011 PAGE A22

Hackers attack KL govt websites

KUALA LUMPUR: Hackers have brazenly ramped up their attacks worldwide, disrupting dozens of Malaysian state-linked websites yesterday after striking at the website of the US Central Intelligence Agency (CIA) a day earlier.

The incidents are part of a wave of recent strikes that targeted Citigroup, the United States Senate, Sony's PlayStation Network and many other websites

Also on Wednesday, Ci ed that hackers stole the mation of more than 360 credit card customers double the number initial

The International M said on Sunday it was attack on its compute Google said this month th lion Gmail accounts had

SINGAPORE TUE MAR 03 09 MYPAPER

Glitch spills UBS clients' info

Wealthy customers saw details of others' online accounts, but bank says number affected is small

KENNY CHEE

A TECHNICAL glitch at Swiss bank UBS gave its wealthy customers in Singapore and Hong Kong a shock last week when they logged on

Asked how many clients were affected, all she said was that "some limited account information concerning a small number of UBS wealth management clients was accessible by a very limited number of other users". She added that

ing to the incident and has implemented measures to prevent a similar occurrence in the future.

The bank also reported the incident to the banking authorities here and in Hong Kong: the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA).

Asked about what MAS would be doing, its spokesman said that "we are following up with the bank", but did not elaborate.

Mr Tan Teik Guan, chief executive of Data Security Systems Solutions, said such accidental leaks of confidential information could lead to "embarrassing situations for clients and reputation risks for banks".

"Intentional leakages are more serious as the data... (could be) used for more malicious activities," he said.

kennyc@sph.com.sg

TODAY @ PCWORLD

IMF Hacked; No End in Sight to Security Horror Shows

By Ian Paul, PCWorld Jun 12, 2011 2:22 PM

Graphic: Diego Aguirre

The recent online intrusion into International Monetary Fund servers may have been the work of malicious hackers working for a foreign government, according to online reports.

The IMF is reportedly reluctant to disclose where it believes the attacks came from since 187 of the world's 194 nations (as recognized by the U.S. Department of State) are members of the fund. The hack's perpetrators obtained a "large quantity of data," including e-mail and other documents during the intrusion, according to Bloomberg.

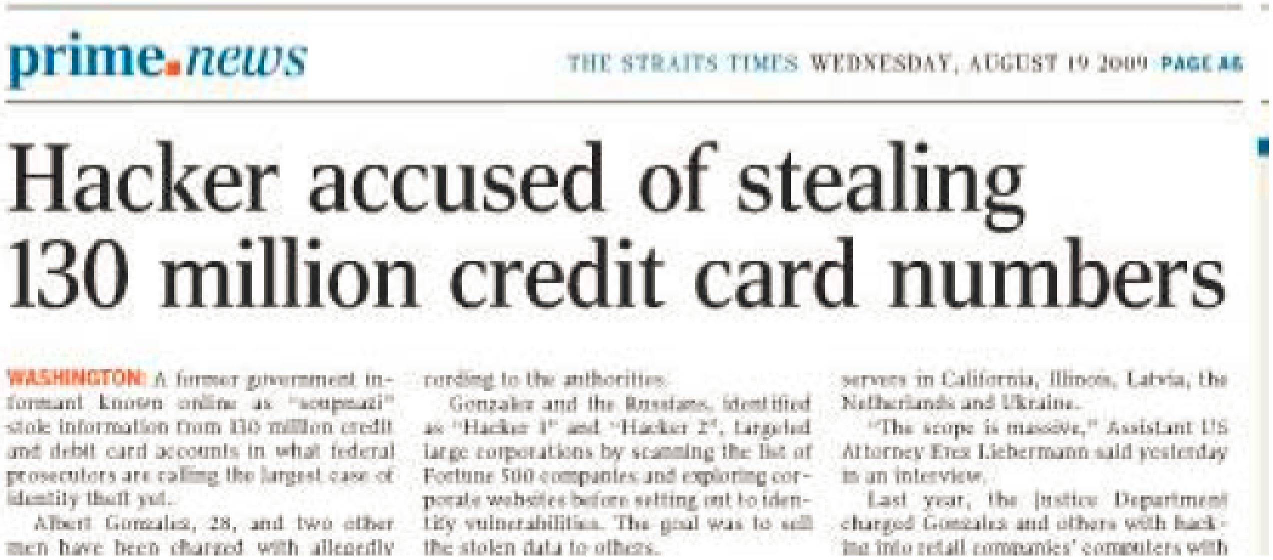
PLAYSTATION NETWORK, HACKER USING A SIMPLE SQL INJECTION VULNERABILITY FOR ATTACK SONY

June 2, 2011 | Filed under: GAMES NEWS | Posted by: adel

Playstation Network, The hacker organisation which took over a website of PBS NewsHour final week end has returned to a initial adore — hacking Sony.

LulzSec voiced Thursday it hacked servers during **Sony Pictures** as well as **Sony BMG**. The organisation posted what crop up to be a stolen e-mail addresses as well as passwords of about 50,000 consumers who'd purebred for a single of 3 Sony promotional sweepstakes: final year's "Seinfeld — We're Going to Del Boca Vista!" giveaway, a Jan competition Sony conducted with AutoTrader, as well as a Sony competition to foster a movie Green Hornet.

2009:



prime.news THE STRAITS TIMES WEDNESDAY, AUGUST 19 2009 PAGE A6

Hacker accused of stealing 130 million credit card numbers

WASHINGTON: A former government informant known online as "soupnazi" stole information from 130 million credit and debit card accounts in what federal prosecutors are calling the largest case of identity theft yet.

Albert Gonzalez, 28, and two other men have been charged with allegedly

cording to the authorities.

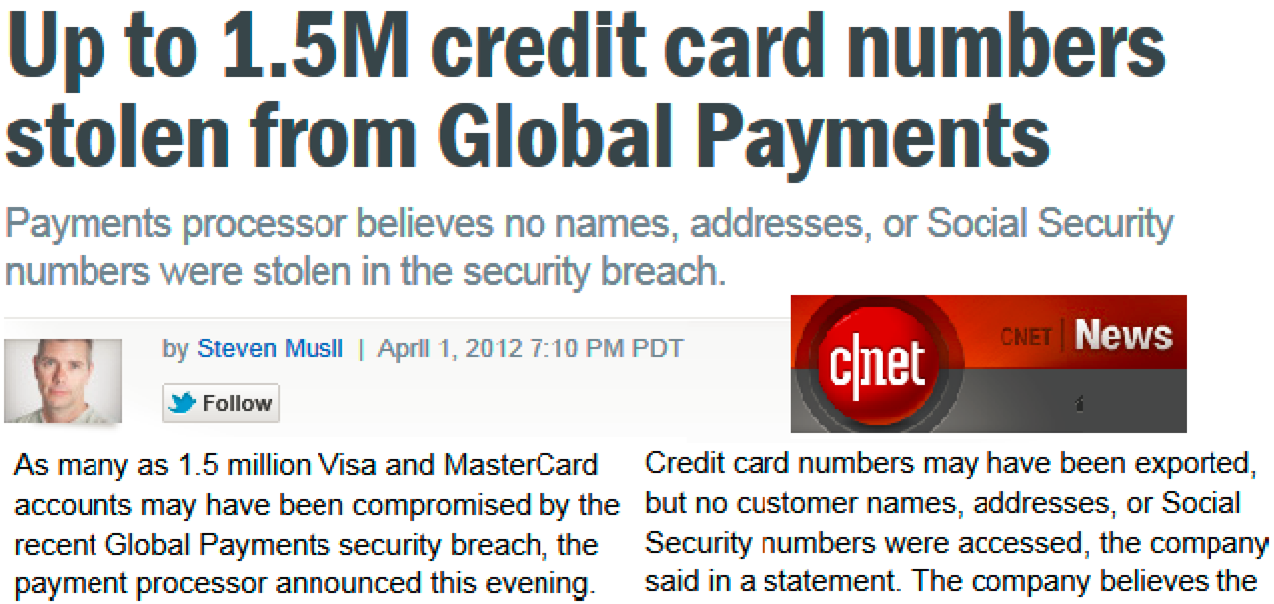
Gonzalez and the Russians, identified as "Hacker 1" and "Hacker 2", targeted large corporations by scanning the list of Fortune 500 companies and exploring corporate websites before setting out to identify vulnerabilities. The goal was to sell the stolen data to others.

servers in California, Illinois, Latvia, the Netherlands and Ukraine.

"The scope is massive," Assistant US Attorney Erez Liebermann said yesterday in an interview.

Last year, the Justice Department charged Gonzalez and others with hacking into retail companies' computers with

2012:



Up to 1.5M credit card numbers stolen from Global Payments

Payments processor believes no names, addresses, or Social Security numbers were stolen in the security breach.

by Steven Musil | April 1, 2012 7:10 PM PDT

As many as 1.5 million Visa and MasterCard accounts may have been compromised by the recent Global Payments security breach, the payment processor announced this evening.

Credit card numbers may have been exported, but no customer names, addresses, or Social Security numbers were accessed, the company said in a statement. The company believes the

A new mixed attack type

(ISC)2™
International Standard for Information Security
CSSLP
Certified Secure Software Lifecycle Professional

HACKERS ARE NOW ATTACKING SOFTWARE APPLICATIONS

Applications can be CRASHED to reveal source, logic, script or infrastructure information that can give a hacker intelligence

Applications can be COMPROMISED to make it provide unauthorized entry access or unauthorized access to read, copy or manipulate data stores, or reveal information that it otherwise would not.

- Eg. Parameter tampering, cookie poisoning

Applications can be HIJACKED to make it perform its tasks but for an authorized user, or send data to an unauthorized recipient, etc.

- Eg. *Cross-site Scripting, SQL Injection*

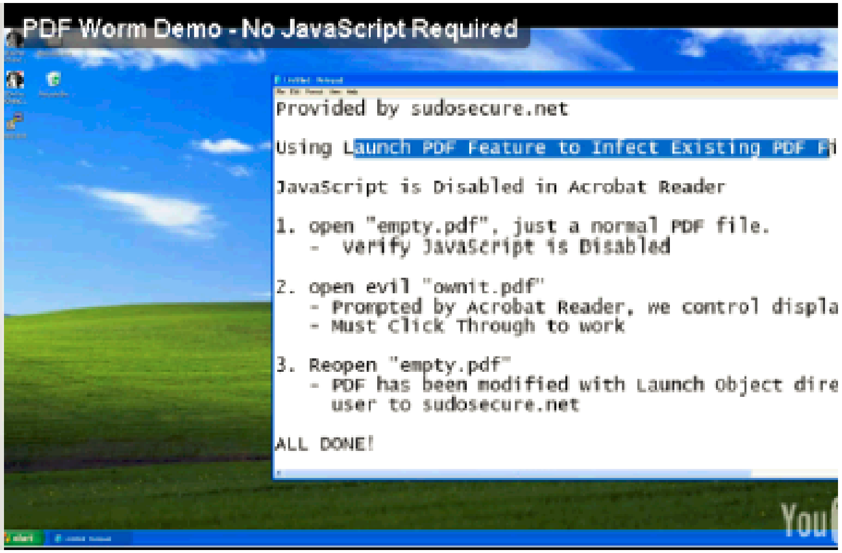
April 5, 2010 3:32 PM PDT

Exploits not needed to attack via PDF files

by Elinor Mills

9 com

77 retweet Share 23


PDF Worm Demo - No JavaScript Required

```
Provided by sudosecure.net

Using Launch PDF Feature to Infect Existing PDF Fi

JavaScript is Disabled in Acrobat Reader

1. open "empty.pdf", just a normal PDF file.
   -  verify JavaScript is Disabled

2. open evil "ownit.pdf"
   - Prompted by Acrobat Reader, we control displa
   - Must Click Through to work

3. Reopen "empty.pdf"
   - PDF has been modified with Launch Object dire
     user to sudosecure.net

ALL DONE!
```

Jeremy Conway created a video to show how his PDF hack works.

Malware on Web Applications

Malware can be delivered in many ways:

- E-mail, IM, network vulnerabilities…

Today, Malware is very often delivered via Web Applications:

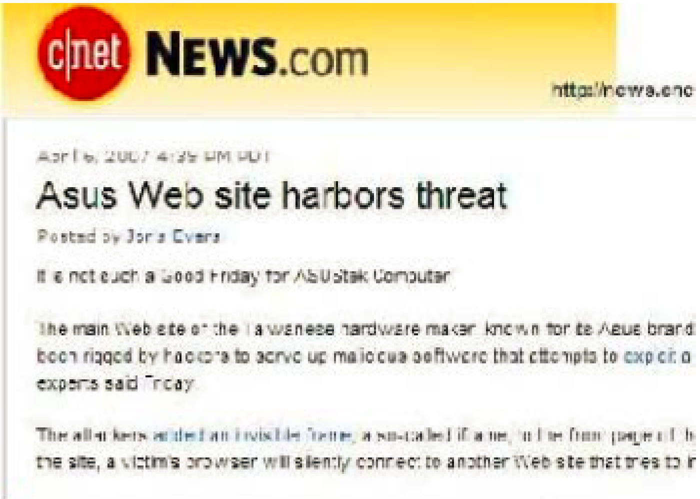
- Aims to infect those browsing the site
- Installed via Client-Side (e.g. Browser) Vulnerabilities & Social Engineering

Malicious content can be downloaded:

- From the web application itself
- Through frames & images leading to other websites
- Through links leading to malicious destinations

Legitimate Sites Hijacked to distribute Malware!

- McAfee, Asus, US Govt Staff Travel Site, Wordpress.org, SuperBowl, …



April 6, 2007 4:35 PM PDT

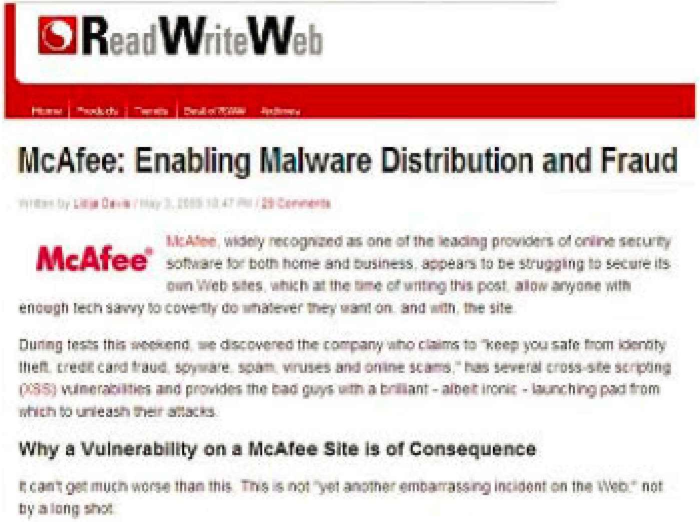
Asus Web site harbors threat

Posted by Joris Evers

It is not such a Good Friday for AsusTek Computer.

The main Web site of the Taiwanese hardware maker, known for its Asus brand, been rigged by hackers to serve up malicious software that attempts to exploit a experts said Friday.

The attackers added an invisible frame, a so-called iframe, to the front page of the site, a victim's browser will silently connect to another Web site that tries to i



McAfee: Enabling Malware Distribution and Fraud

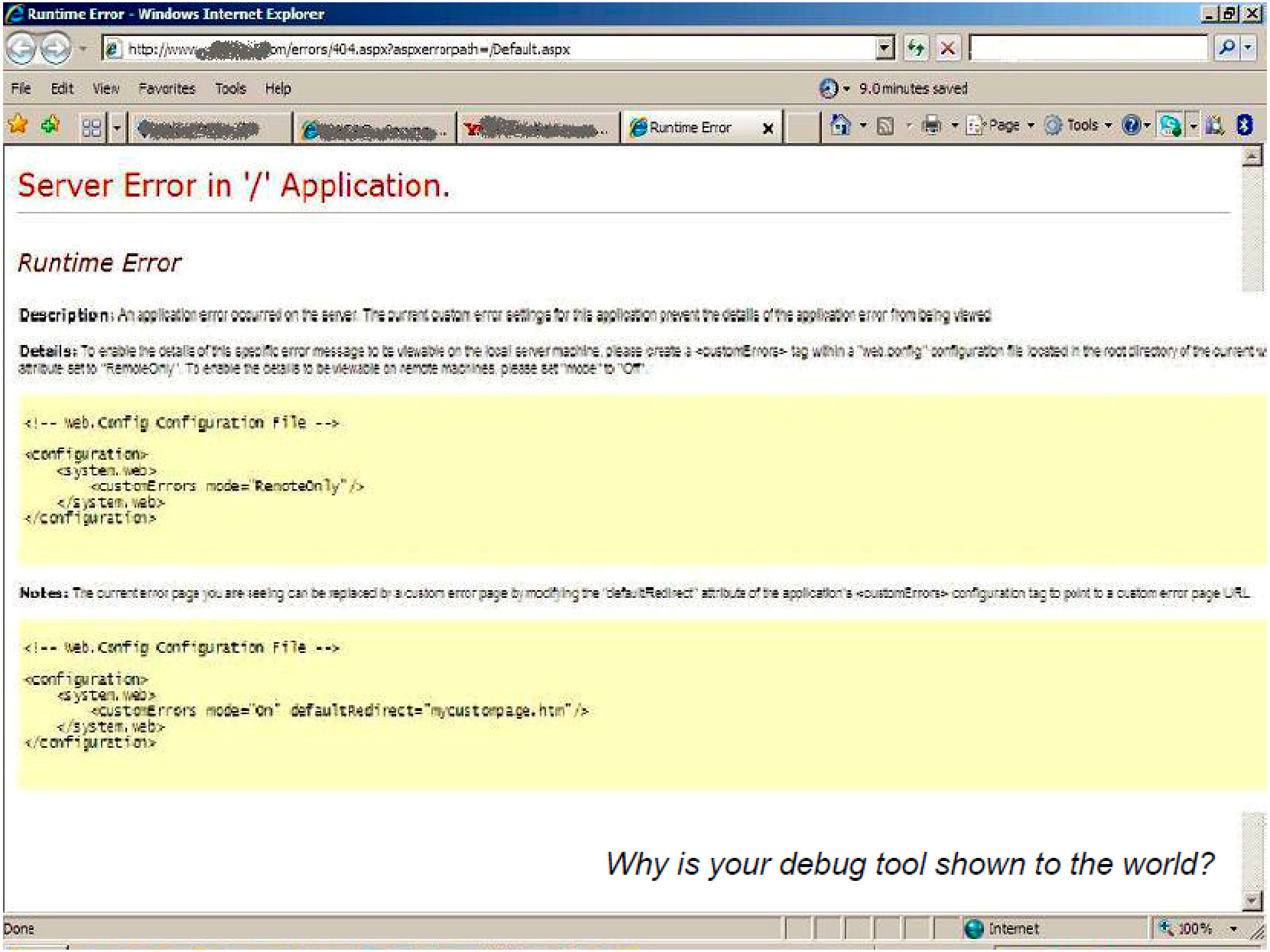
Written by Lidija Davis / May 3, 2009 10:47 PM / 29 Comments

McAfee, widely recognized as one of the leading providers of online security software for both home and business, appears to be struggling to secure its own Web sites, which at the time of writing this post, allow anyone with enough tech savvy to covertly do whatever they want on, and with, the site.

During tests this weekend, we discovered the company who claims to "keep you safe from identity theft, credit card fraud, spyware, spam, viruses and online scams," has several cross-site scripting (XSS) vulnerabilities and provides the bad guys with a brilliant - albeit ironic - launching pad from which to unleash their attacks.

Why a Vulnerability on a McAfee Site is of Consequence

It can't get much worse than this. This is not "yet another embarrassing incident on the Web," not by a long shot.


Runtime Error - Windows Internet Explorer
http://www.[redacted]om/errors/404.aspx?aspxerrorpath=/Default.aspx
File Edit View Favorites Tools Help
9.0 minutes saved
[redacted]
[redacted]
[redacted]
Runtime Error
Page
Tools
Done
Internet
100%

Server Error in '/' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed.

Details: To enable the details of this specific error message to be viewable on the local server machine, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current w attribute set to "RemoteOnly". To enable the details to be viewable on remote machines, please set "mode" to "Off".

```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="RemoteOnly"/>
    </system.web>
</configuration>
```

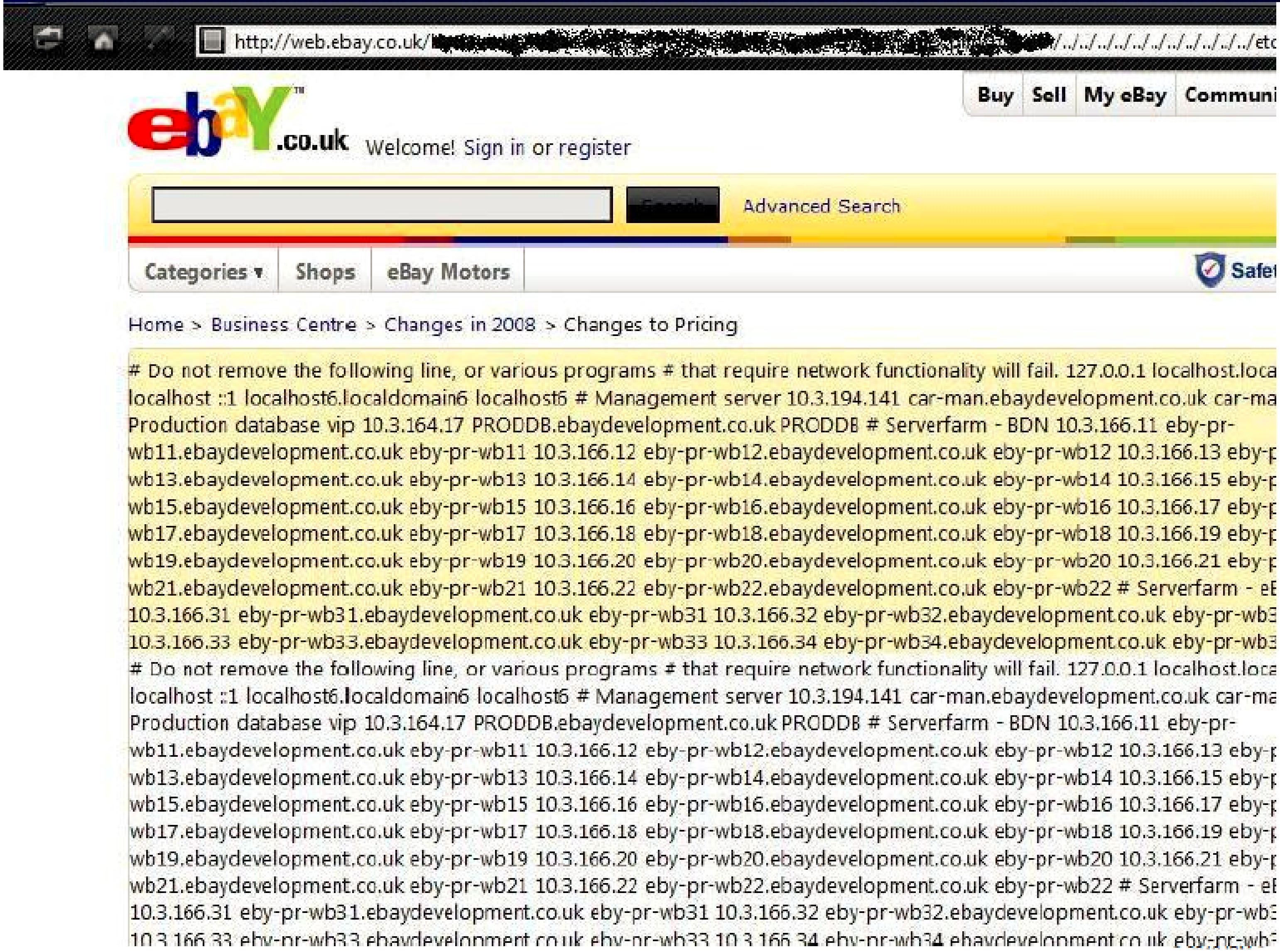
Notes: The current error page you are seeing can be replaced by a custom error page by modifying the "defaultRedirect" attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="On" defaultRedirect="mycustompage.htm"/>
    </system.web>
</configuration>
```

Why is your debug tool shown to the world?

Attackers use directory traversal attacks to read arbitrary files on web servers, such as SSL private keys and password files.



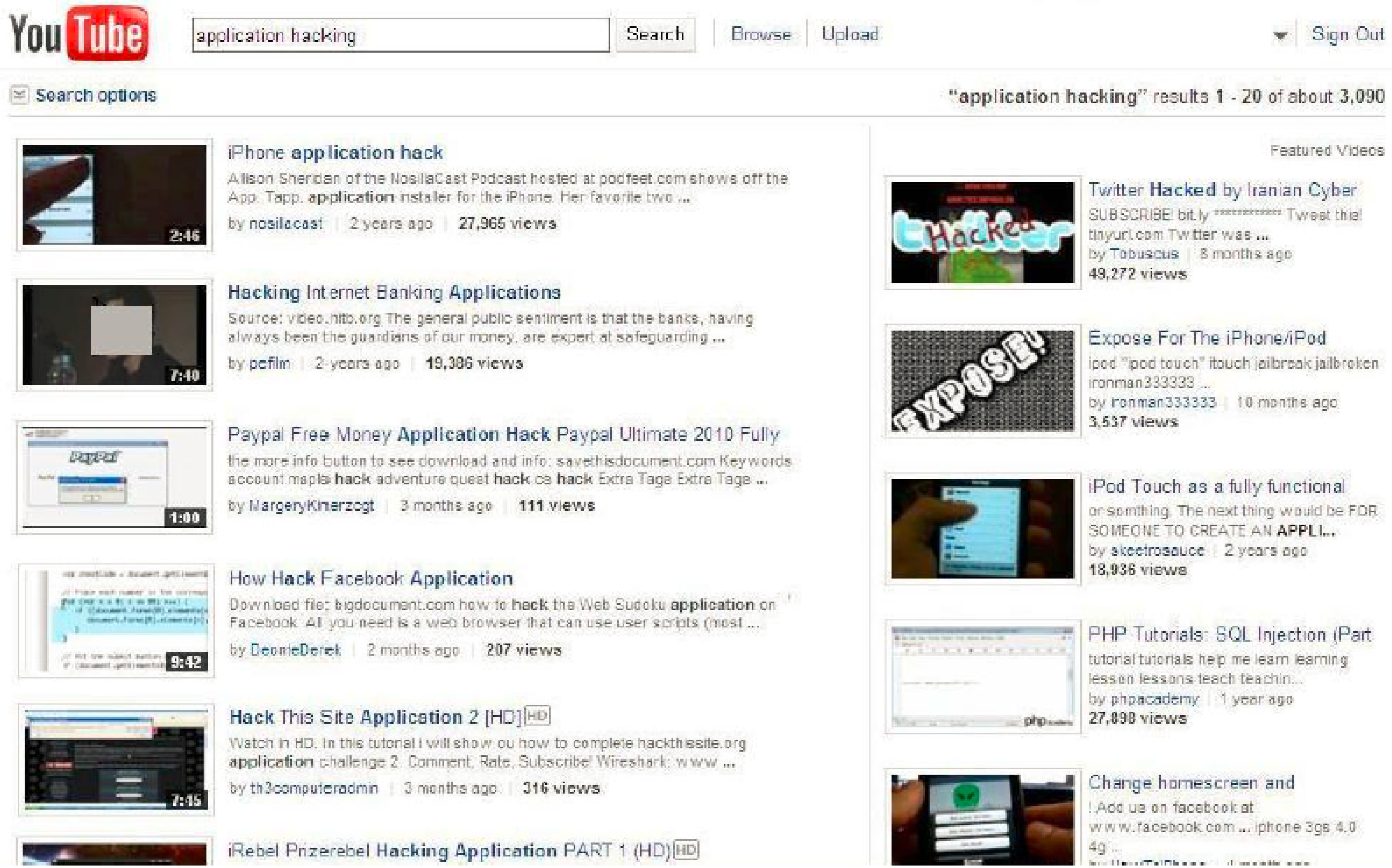
http://web.ebay.co.uk/[redacted]/../../../../../../../../../../../etc
Buy
Sell
My eBay
Communi
ebY.co.uk
Welcome! Sign in or register
Advanced Search
Categories ▾
Shops
eBay Motors
Safet

Home > Business Centre > Changes in 2008 > Changes to Pricing

```
# Do not remove the following line, or various programs # that require network functionality will fail. 127.0.0.1 localhost.loca
localhost ::1 localhost6.localdomain6 localhost6 # Management server 10.3.194.141 car-man.ebaydevelopment.co.uk car-ma
Production database vip 10.3.164.17 PRODDB.ebaydevelopment.co.uk PRODDB # Serverfarm - BDN 10.3.166.11 eby-pr-
wb11.ebaydevelopment.co.uk eby-pr-wb11 10.3.166.12 eby-pr-wb12.ebaydevelopment.co.uk eby-pr-wb12 10.3.166.13 eby-p
wb13.ebaydevelopment.co.uk eby-pr-wb13 10.3.166.14 eby-pr-wb14.ebaydevelopment.co.uk eby-pr-wb14 10.3.166.15 eby-p
wb15.ebaydevelopment.co.uk eby-pr-wb15 10.3.166.16 eby-pr-wb16.ebaydevelopment.co.uk eby-pr-wb16 10.3.166.17 eby-p
wb17.ebaydevelopment.co.uk eby-pr-wb17 10.3.166.18 eby-pr-wb18.ebaydevelopment.co.uk eby-pr-wb18 10.3.166.19 eby-p
wb19.ebaydevelopment.co.uk eby-pr-wb19 10.3.166.20 eby-pr-wb20.ebaydevelopment.co.uk eby-pr-wb20 10.3.166.21 eby-p
wb21.ebaydevelopment.co.uk eby-pr-wb21 10.3.166.22 eby-pr-wb22.ebaydevelopment.co.uk eby-pr-wb22 # Serverfarm - eE
10.3.166.31 eby-pr-wb31.ebaydevelopment.co.uk eby-pr-wb31 10.3.166.32 eby-pr-wb32.ebaydevelopment.co.uk eby-pr-wb3
10.3.166.33 eby-pr-wb33.ebaydevelopment.co.uk eby-pr-wb33 10.3.166.34 eby-pr-wb34.ebaydevelopment.co.uk eby-pr-wb3
```

```
# Do not remove the following line, or various programs # that require network functionality will fail. 127.0.0.1 localhost.loca
localhost ::1 localhost6.localdomain6 localhost6 # Management server 10.3.194.141 car-man.ebaydevelopment.co.uk car-ma
Production database vip 10.3.164.17 PRODDB.ebaydevelopment.co.uk PRODDB # Serverfarm - BDN 10.3.166.11 eby-pr-
wb11.ebaydevelopment.co.uk eby-pr-wb11 10.3.166.12 eby-pr-wb12.ebaydevelopment.co.uk eby-pr-wb12 10.3.166.13 eby-p
wb13.ebaydevelopment.co.uk eby-pr-wb13 10.3.166.14 eby-pr-wb14.ebaydevelopment.co.uk eby-pr-wb14 10.3.166.15 eby-p
wb15.ebaydevelopment.co.uk eby-pr-wb15 10.3.166.16 eby-pr-wb16.ebaydevelopment.co.uk eby-pr-wb16 10.3.166.17 eby-p
wb17.ebaydevelopment.co.uk eby-pr-wb17 10.3.166.18 eby-pr-wb18.ebaydevelopment.co.uk eby-pr-wb18 10.3.166.19 eby-p
wb19.ebaydevelopment.co.uk eby-pr-wb19 10.3.166.20 eby-pr-wb20.ebaydevelopment.co.uk eby-pr-wb20 10.3.166.21 eby-p
wb21.ebaydevelopment.co.uk eby-pr-wb21 10.3.166.22 eby-pr-wb22.ebaydevelopment.co.uk eby-pr-wb22 # Serverfarm - eE
10.3.166.31 eby-pr-wb31.ebaydevelopment.co.uk eby-pr-wb31 10.3.166.32 eby-pr-wb32.ebaydevelopment.co.uk eby-pr-wb3
10.3.166.33 eby-pr-wb33.ebaydevelopment.co.uk eby-pr-wb33 10.3.166.34 eby-pr-wb34.ebaydevelopment.co.uk eby-pr-wb3
```

Don't Try This At Home



"application hacking" results **1** - **20** of about **3,090**

iPhone application hack
Allison Sheridan of the NosillaCast Podcast hosted at podfeet.com shows off the App. Tapp. **application** installer for the iPhone. Her favorite two ...
by nosillacast | 2 years ago | **27,965 views**

Hacking Internet Banking Applications
Source: video.hitb.org The general public sentiment is that the banks, having always been the guardians of our money, are expert at safeguarding ...
by pefilm | 2 years ago | **19,386 views**

Paypal Free Money Application Hack Paypal Ultimate 2010 Fully
the more info button to see download and info: savethisdocument.com Keywords account maple **hack** adventure quest **hack** cs **hack** Extra Tage Extra Tage ...
by MargeryKinerzogt | 3 months ago | **111 views**

How Hack Facebook Application
Download file: bigdocument.com how to **hack** the Web Sudoku **application** on Facebook. All you need is a web browser that can use user scripts (most ...
by DeonieDerek | 2 months ago | **207 views**

Hack This Site Application 2 [HD]
Watch in HD. In this tutorial I will show ou how to complete hackthissite.org **application** challenge 2. Comment, Rate, Subscribe! Wireshark: www ...
by th3computeradmin | 3 months ago | **316 views**

iRebel Prizerebel Hacking Application PART 1 (HD)

Featured Videos

Twitter Hacked by Iranian Cyber
SUBSCRIBE! bit.ly ************ Tweet this! tinyurl.com Twitter was ...
by Tobuscus | 8 months ago
49,272 views

Expose For The iPhone/iPod
ipod "ipod touch" itouch jailbreak jailbroken ironman333333 ...
by ironman333333 | 10 months ago
3,537 views

iPod Touch as a fully functional
or somthing. The next thing would be FOR SOMEONE TO CREATE AN **APPLI**...
by skeetrosauce | 2 years ago
18,936 views

PHP Tutorials: SQL Injection (Part
tutorial tutorials help me learn learning lesson lessons teach teachin...
by phpacademy | 1 year ago
27,898 views

Change homescreen and
! Add us on facebook at www.facebook.com ... iphone 3gs 4.0 4g ...

Why do hackers attack Apps?

Because they know you have firewalls

- So they need to find a new weak spot to hack through and steal or compromise your data

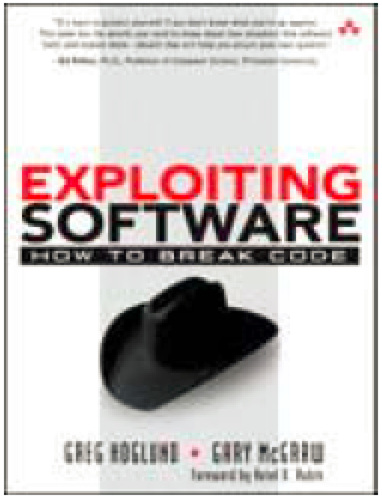
Because firewalls do not protect against app attacks!

- Very few people are actively aware of application security issues
- **Most IT security professionals, from network & sys-admin side, have little experience or interest in software development. Programmers have little experience or interest in security or infrastructure.**
  - IT security staff are also often overworked and are focusing on other issues

Because web sites have a large footprint; cloud makes it even bigger.

Because they can!

- **Many organizations today still lack a software development security policy!**
  - Many applications especially legacy ones still in use, were not built defensively
  - **Applications today are hundreds of thousands of lines long**
  - **It is a nightmare to QA the application, and requires discipline**
    - **So many people, even if aware, will skip or procrastinate this tedious process**
  - **Additional loss of control when outsourcing development work**



Issues Affecting Application Development

No developer goes to work with the intention of writing bad code.

- Developers are often not trained or experienced in secure coding techniques, and have never needed to worry about this before
- Developers face pressures of demands for quality and functionality, and are often short on timeline, resources, information, budget, quality assurance tools investment.
- ***Plus heavy demands on outsourcing parties ….***

OUR GOAL IS TO WRITE BUG-FREE SOFTWARE. I'LL PAY A TEN-DOLLAR BONUS FOR EVERY BUG YOU FIND AND FIX.
S. Adams E-mail: SCOTTADAMS@AOL.COM
YAHOO!
WE'RE RICH
YES!!! YES!!! YES!!!
11/13 © 1995 United Feature Syndicate, Inc.(NYC)
I HOPE THIS DRIVES THE RIGHT BEHAVIOR.
I'M GONNA WRITE ME A NEW SUV THIS AFTER-NOON!

3 Reasons why Hacks WORK

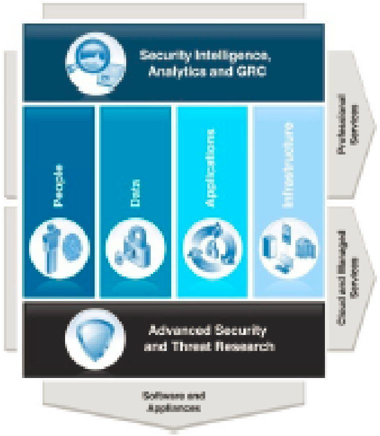
1. Weak Software
   - Buffer Overflows
   - OS/Application Vulnerabilities
2. Weak Configuration
   - Default Configurations
   - Weak Passwds
   - Failure to Harden
3. Weak People
   - Malicious CODE
   - Social Engineering
   - Insider Threat

Why should customers be doing application vulnerability scanning?

What is missing with point solutions?

- Vulnerability scanners
  - Traditional vulnerability scanners don't cover web applications
- Penetration testing
  - Effective at finding vulnerabilities but not scalable for ongoing tests
  - Not focused on remediation
- Network firewall and IPS
  - Generic Web application protection (if any) so most custom web applications not covered
  - Most IPS solutions focus on exploits as opposed to web application vulnerabilities
- Web application firewall
  - Expensive point product to deploy and manage
  - Can be effective, but difficult to deploy, tune and manage
  - Building policies can be as time consuming as remediating the vulnerability

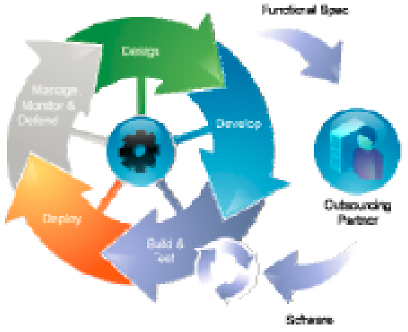
IBM Security Framework



Security Intelligence, Analytics and GRC
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

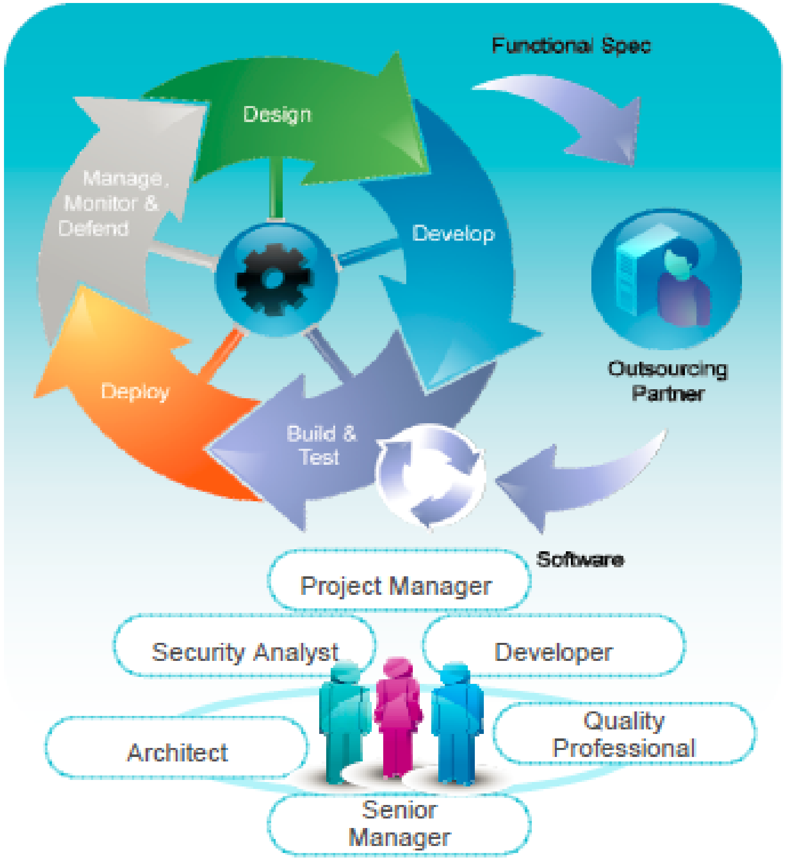
Why are Web applications so vulnerable?

- Developers are mandated to deliver functionality on-time and on-budget - but not to develop secure applications
- Developers are not generally educated in secure code practices
- Product innovation is driving development of increasingly complicated software

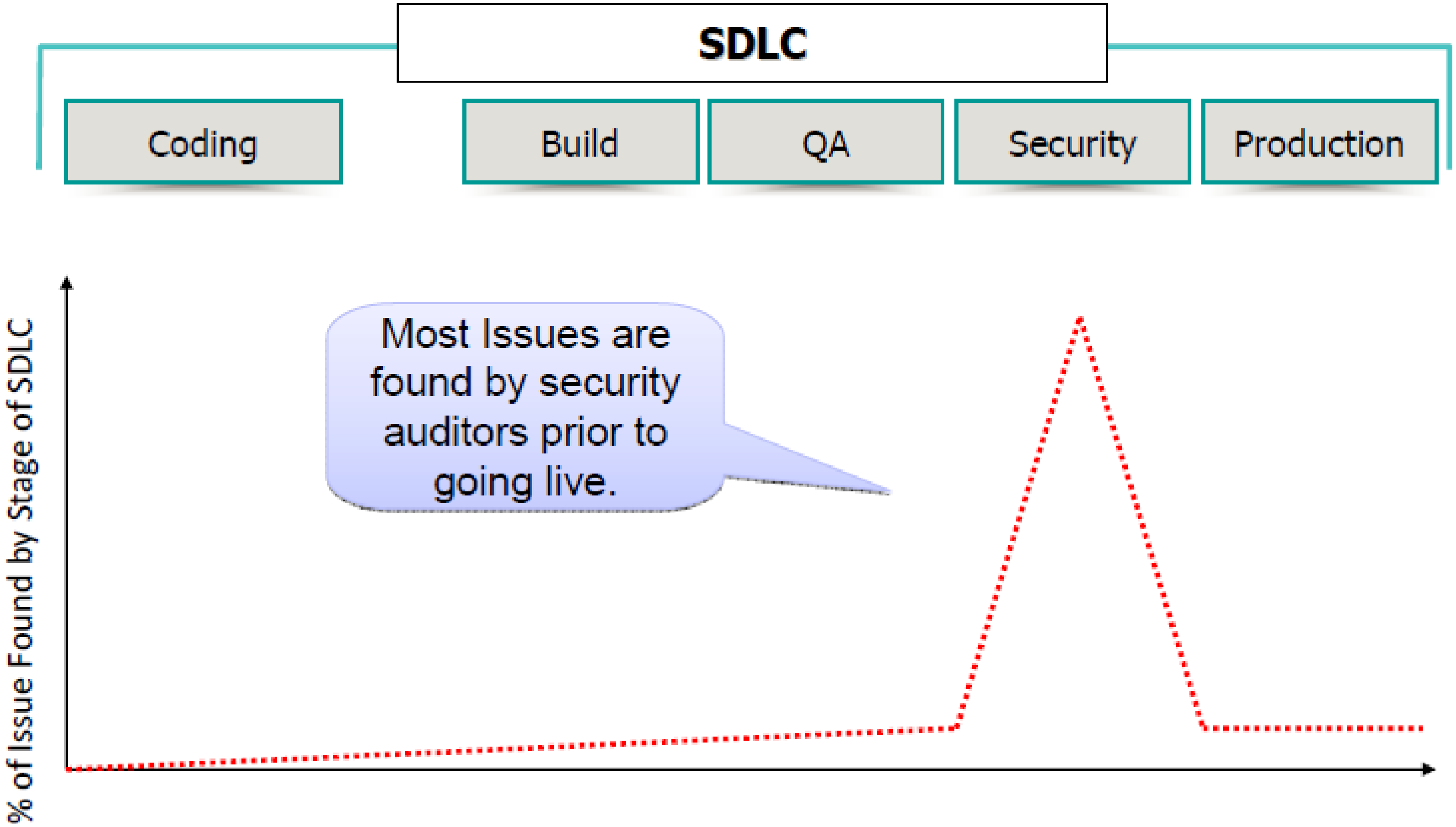


Organizations need to take a proactive approach to Application Security

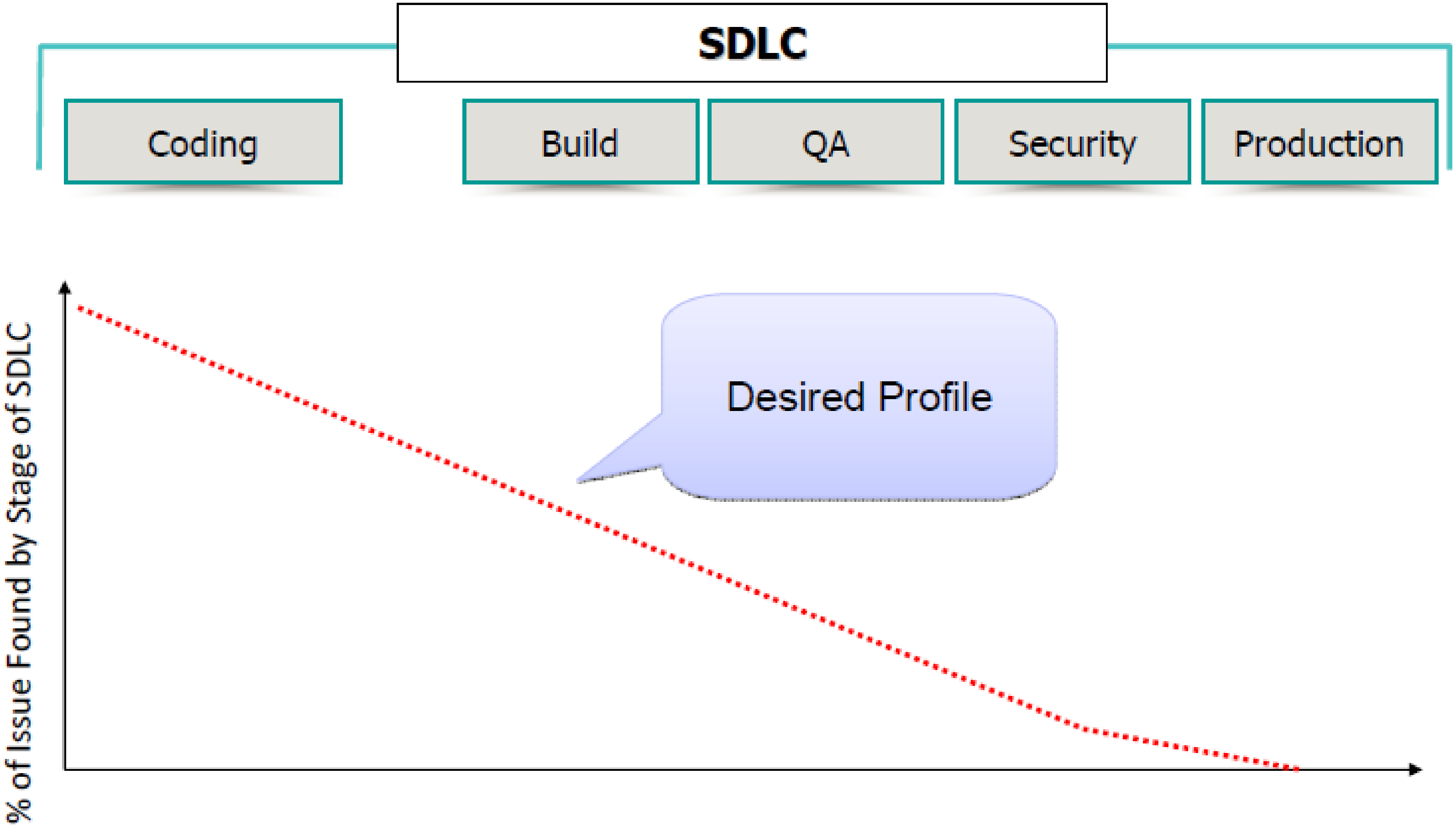
- **Embed and integrate security testing early** in the development lifecycle to support agile delivery demands
- Adopt a **Secure by Design** approach to enable the design, delivery and management of smarter software and services
- Bridge the gap between "Security" and "Development" through **joint collaboration and visibility**, enabling regulatory compliance



Security Testing Within the Software Lifecycle



Security Testing Within the Software Lifecycle



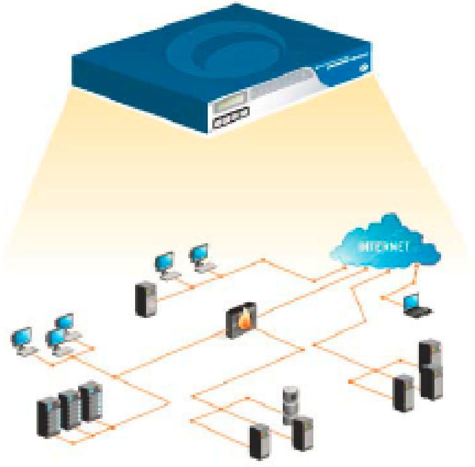
Finding and Fixing Vulnerabilities with AppScan

Automates Application Security Testing

Same process for whitebox & blackbox

1 → 2 → 3

Scan applications



Analyze

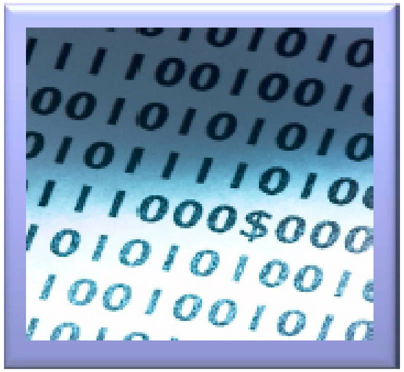
(identify issues)

Report

(detailed & actionable)

Cost is a significant driver

80% of development costs are spent identifying and correcting defects!*

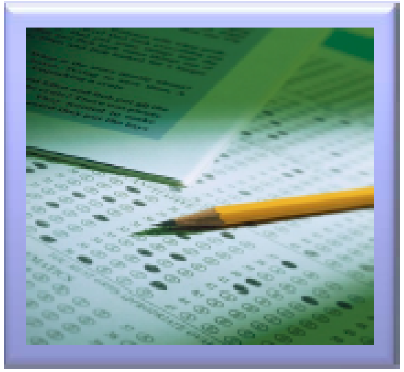


During the CODING phase

$80/defect

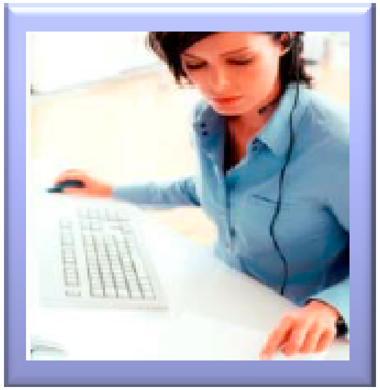
During the BUILD phase

$240/defect



During the QA/TESTING phase

$960/defect



Once released as a product

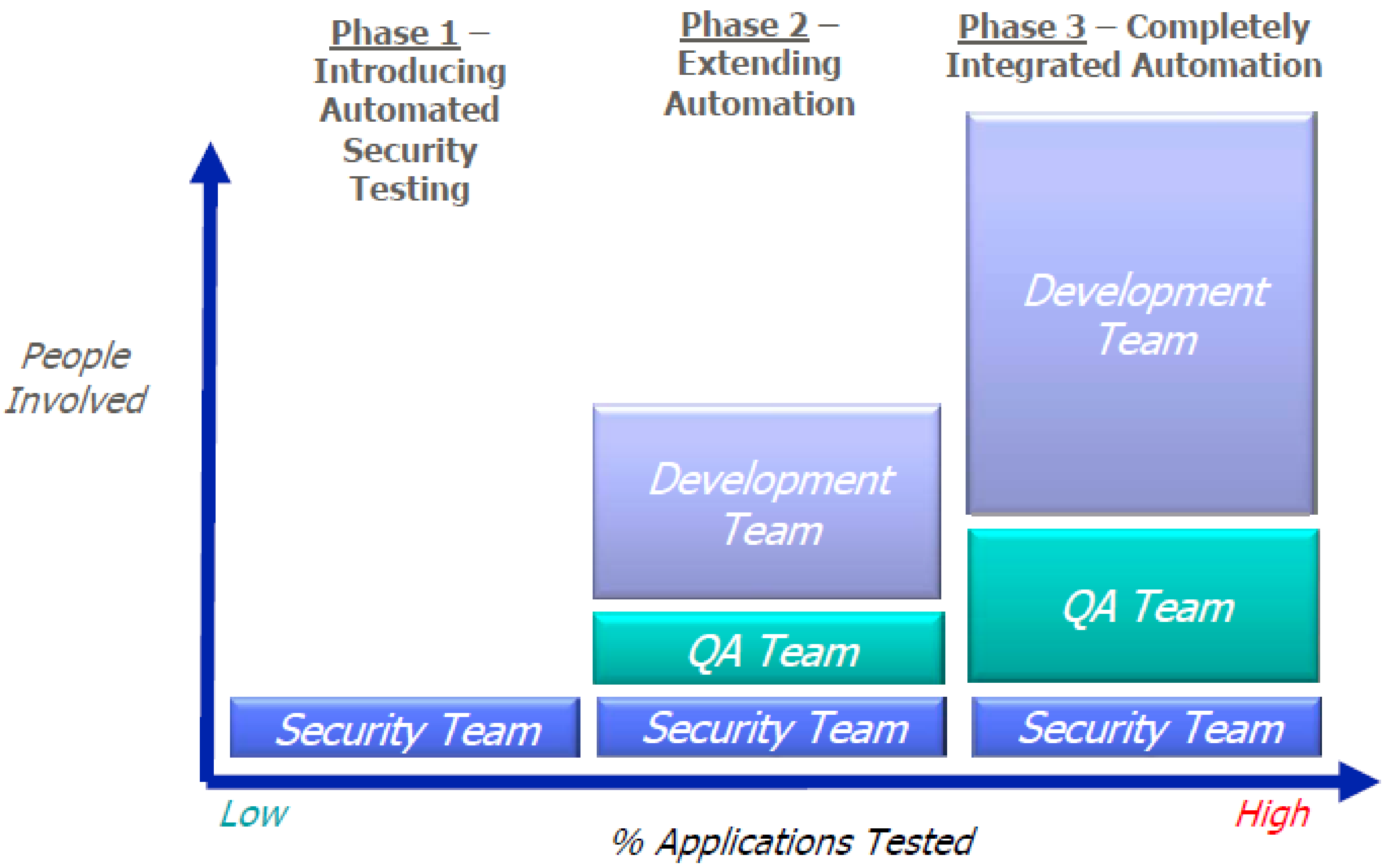
$7,600/defect

+

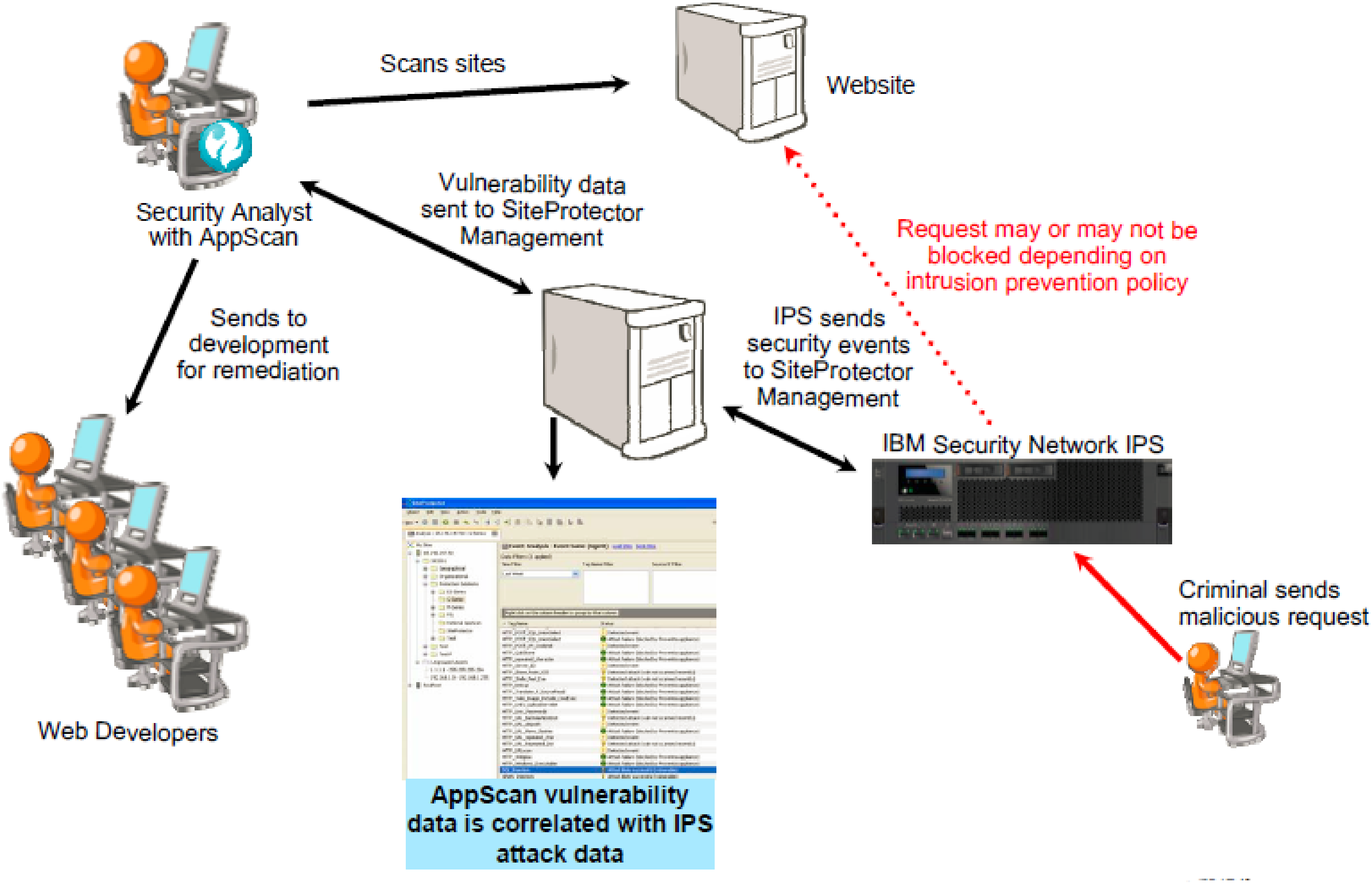
Law suits, loss of customer trust, damage to brand

*National Institute of Standards & Technology
Source: GBS Industry standard study
Defect cost derived in assuming it takes 8 hrs to find, fix and repair a defect when found in code and unit test.
Defect FFR cost for other phases calculated by using the multiplier on a blended rate of $80/hr.

The Need to Scale Security Testing

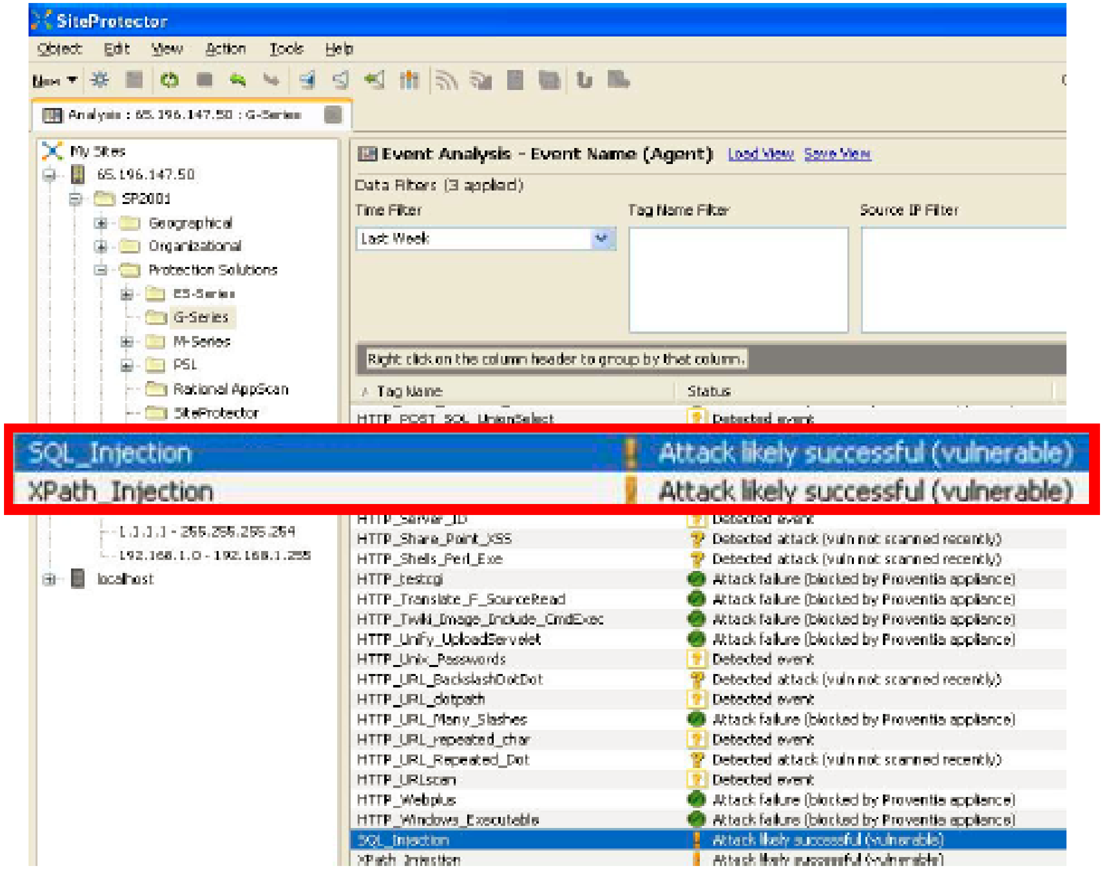


Integrating Vulnerability Scanning and IPS


Scans sites
Website
Security Analyst with AppScan
Vulnerability data sent to SiteProtector Management
Request may or may not be blocked depending on intrusion prevention policy
Sends to development for remediation
IPS sends security events to SiteProtector Management
IBM Security Network IPS
Web Developers
Criminal sends malicious request
AppScan vulnerability data is correlated with IPS attack data

More Intelligent Insight into Web Application Threats

- Correlates vulnerability data with actual attacks
- Understand which attacks have a high probability of success
- Increased insight helps in tuning IPS Web protection module
- Prioritize vulnerability remediation efforts based exposure



Event Analysis - Event Name (Agent)

Data Filters (3 applied)

Time Filter: Last Week

Tag Name Filter

Source IP Filter

Right click on the column header to group by that column.

Tag Name	Status
HTTP_POST_SQL_UnionSelect	Detected event
HTTP_Server_ID	Detected event
HTTP_Share_Point_XSS	Detected attack (vuln not scanned recently)
HTTP_Shells_Perl_Exe	Detected attack (vuln not scanned recently)
HTTP_testcgi	Attack failure (blocked by Proventia appliance)
HTTP_Translate_F_SourceRead	Attack failure (blocked by Proventia appliance)
HTTP_Twiki_Image_Include_CmdExec	Attack failure (blocked by Proventia appliance)
HTTP_Unify_UploadServelet	Attack failure (blocked by Proventia appliance)
HTTP_Unix_Passwords	Detected event
HTTP_URL_BackslashDotDot	Detected attack (vuln not scanned recently)
HTTP_URL_dotpath	Detected event
HTTP_URL_Many_Slashes	Attack failure (blocked by Proventia appliance)
HTTP_URL_repeated_char	Detected event
HTTP_URL_Repeated_Dot	Detected attack (vuln not scanned recently)
HTTP_URLscan	Detected event
HTTP_Webplus	Attack failure (blocked by Proventia appliance)
HTTP_Windows_Executable	Attack failure (blocked by Proventia appliance)
SQL_Injection	Attack likely successful (vulnerable)
XPath_Injection	Attack likely successful (vulnerable)

SQL_Injection ! Attack likely successful (vulnerable)

XPath_Injection ! Attack likely successful (vulnerable)

THINK- Proactive Security

What are you currently doing around application security? How are you addressing Web application attacks?

Would you like to reduce the attack surface related to Web application attacks by finding and fixing them at the source?

Would you like a way to engage your developers to help them create more secure applications and reduce your overall risk?

Would you be interested in finding out more about Web vulnerabilities in your environment so you can work towards fixing them, and also have better information to tune the Web protections within your IPS platform?

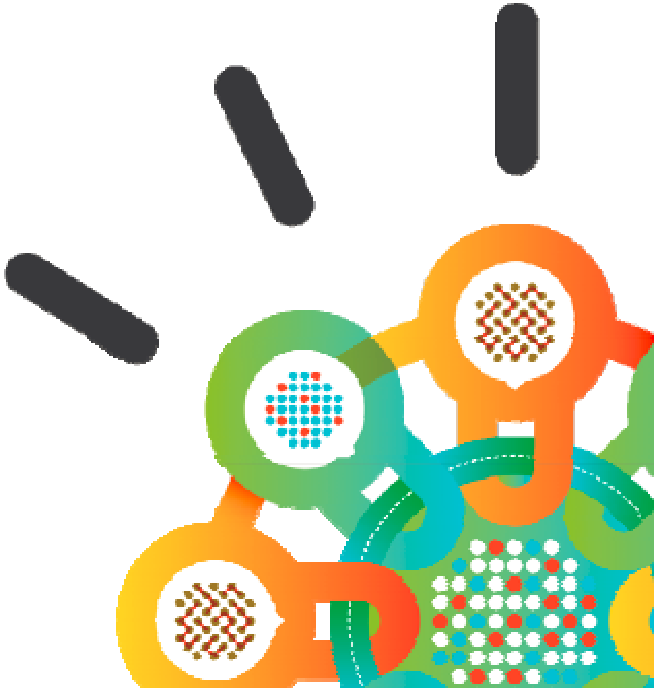
Benefits

AppScan – find and fix vulnerabilities to minimize risk and exposure

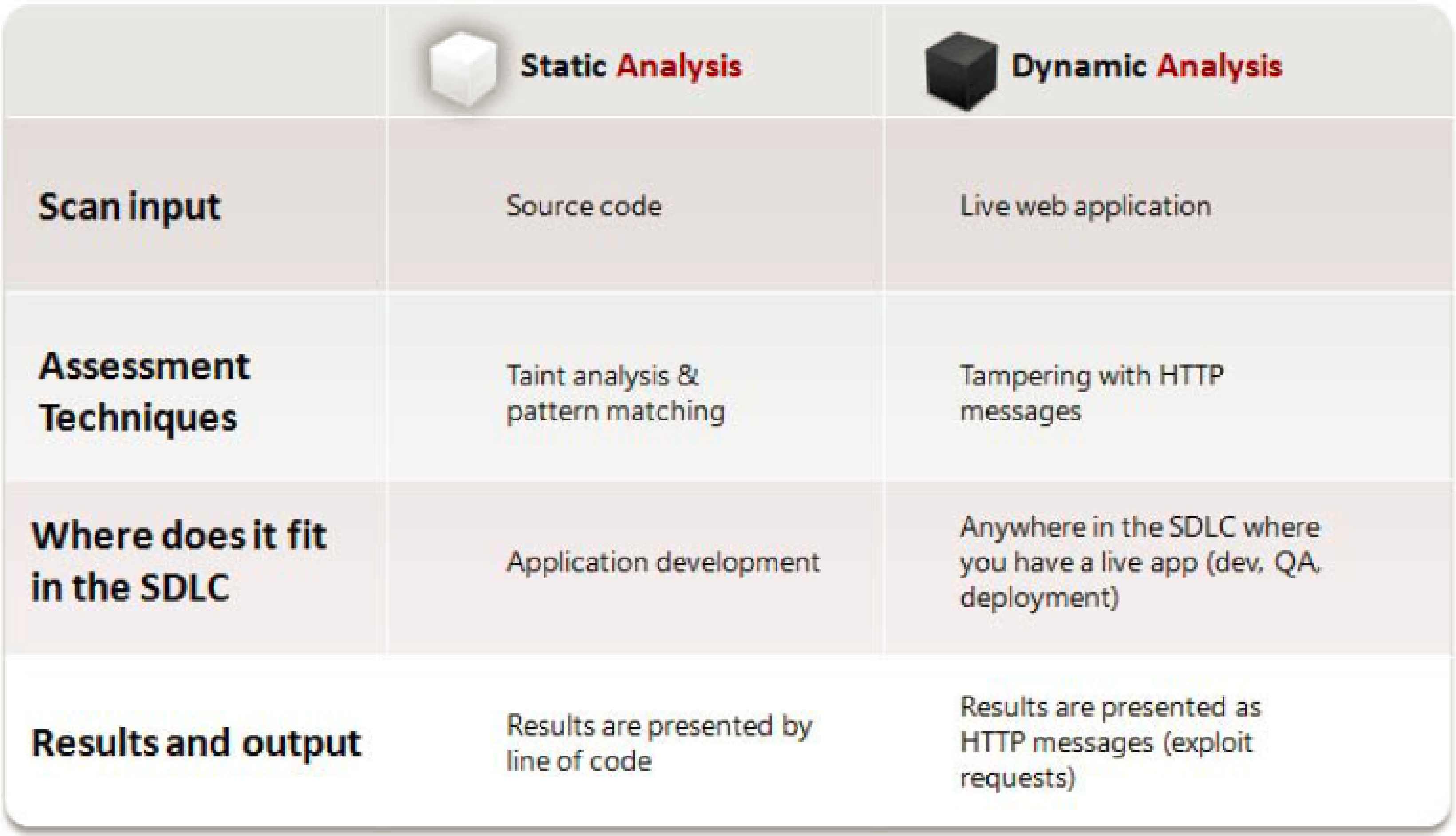
Intrusion Prevention – block Web application attacks in real-time while vulnerabilities are being found

QRadar solutions to raise visibility and insight even further

- Black Box vs White Box
- Dynamic vs Static



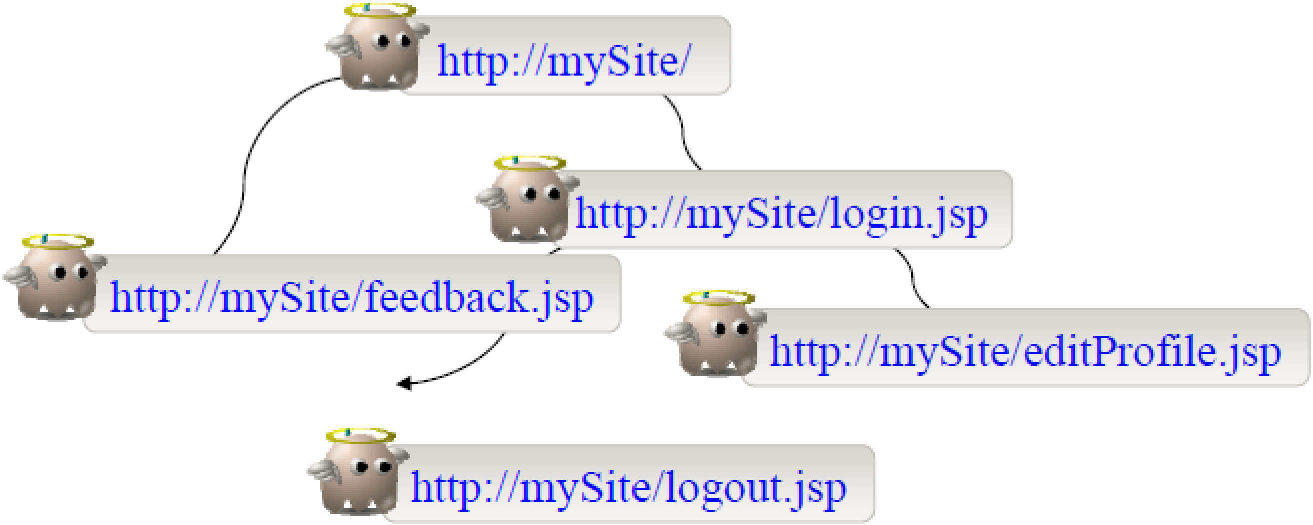
Differences Between DAST and SAST Approaches



	Static Analysis	Dynamic Analysis
Scan input	Source code	Live web application
Assessment Techniques	Taint analysis & pattern matching	Tampering with HTTP messages
Where does it fit in the SDLC	Application development	Anywhere in the SDLC where you have a live app (dev, QA, deployment)
Results and output	Results are presented by line of code	Results are presented as HTTP messages (exploit requests)

How Black Box Scanners Work

Stage 1: Crawling as an honest user



http://mySite/

http://mySite/login.jsp

http://mySite/feedback.jsp

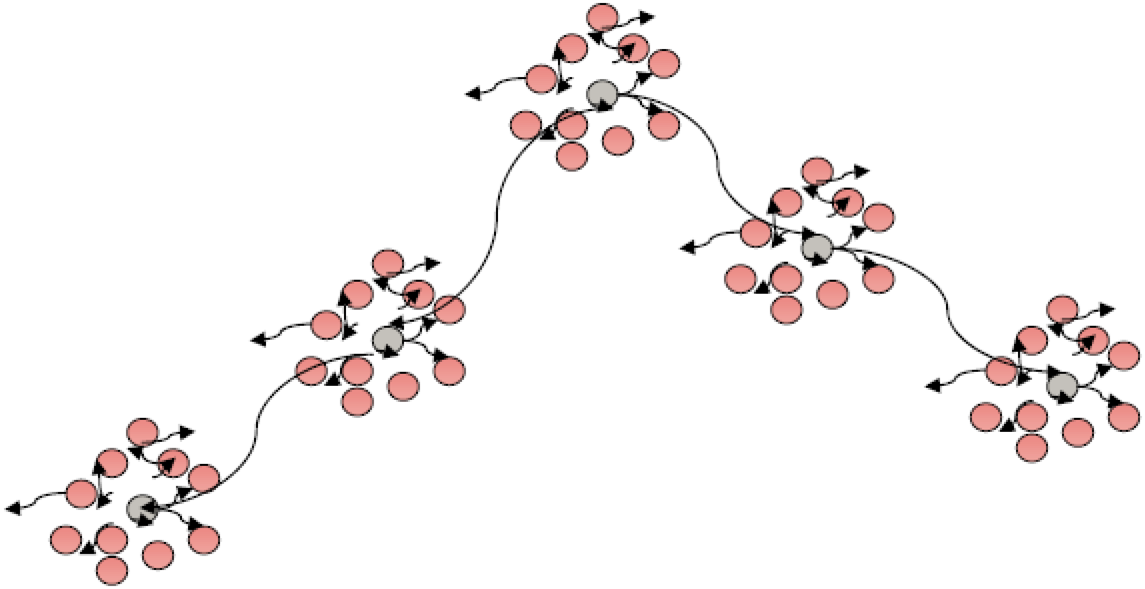
http://mySite/editProfile.jsp

http://mySite/logout.jsp

How Black Box Scanners Work

Stage 1: Crawling as an honest user

Stage 2: Testing by tampering requests



“Hacker in the Box”

Black-box Analysis

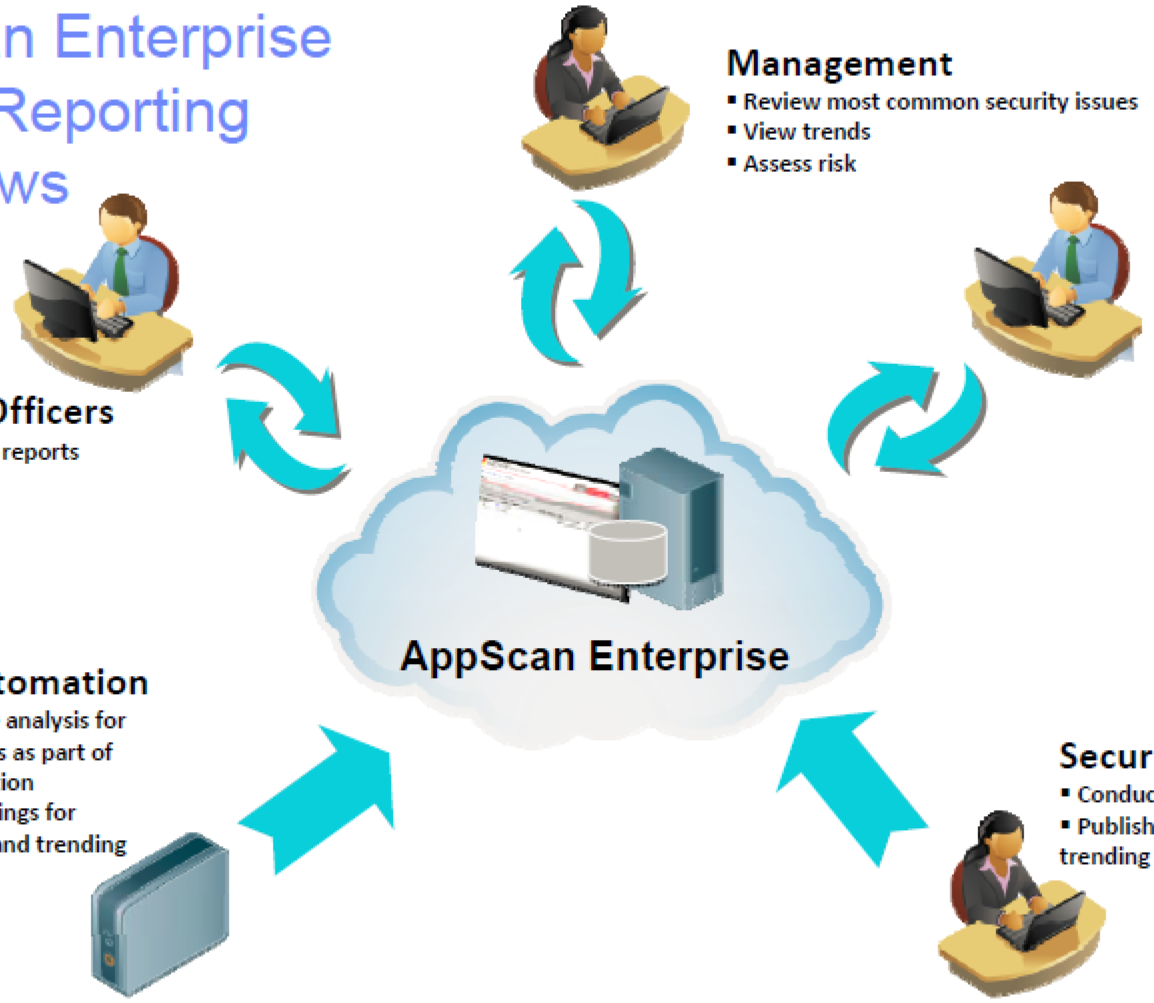
- Accuracy
- Code coverage
- Source free
- HTTP awareness only
- Multi-component support
- Requires deployed application
- Few Prerequisites
- Works as a remote attacker

White-box Analysis

- Over approximation
- Code/path coverage
- Limited to given code
- More than HTTP validations
- Support per language/framework
- No need to deploy application
- Support partial applications
- Integration/deployment issues

Challenges for each type of analysis differ!

AppScan Enterprise Server Reporting Workflows



Management

- Review most common security issues
- View trends
- Assess risk

Developers

- View assessment results
- Remediate issues
- Assign issue status

Compliance Officers

- Review compliance reports

Build automation

- Source code analysis for security issues as part of build verification
- Publish findings for remediation and trending

Security specialists

- Conduct security assessments
- Publish findings for remediation and trending

Tools:

- AppScan Source for Automation
- AppScan Standard Edition CLI

Tools:

- AppScan Standard Edition
- AppScan Source Edition

Who can benefit: Application Security Testing and Risk Management

	Penetration Testing		Vulnerability (Risk) Management	Secure Development
	Security consultants	Small Security Teams & Security Auditors	Enterprise Security Teams	Security (development is the user and influencer)
Use case	Clients recognize they don't have AppSec expertise and engage consultants for "assessment" which typically includes penetration testing of deployed applications. Consultants want a tool to automate testing and allow them to concentrate on more advanced testing/attacks that are not easily automated. Compliance (PCI) is often the original driver for assessment	Client has 1-3 headcount dedicated to AppSec. Teams often get started after a consultant's assessment. Client seeks to do its own testing rather than rely on consultants for annual pen-test. Compliance (PCI) is often the original driver	Client has an AppSec team to manage application risk across the lifecycle. Testing focused on production apps and pre-production audit Risk management plan includes: • Inventory of applications • Scheduled, recurring scans of all applications • Monitoring and tracking of vulnerabilities and resolution • AppSec feeds into Enterprise Security Intelligence	Client's security team has convinced development execs to include security testing in one or more phases of SDLC: • Coding • Build • QA/Test • Pre-production security test Objective to build secure applications, minimize risk & reduce remediation costs
Buying criteria	• Advanced security testing • Coverage of latest web applications (AJAX, Flash, web services) • Reports that summarize findings for clients	• Ease of use (easy scan set up) • Reports that summarize findings for compliance or be given to development organization for remediation • Advanced security testing with high confidence in the results	• Central control with view of application risk across enterprise • Advanced security testing with precise results • ALM integration • Application coverage: ERP, mainframe, cloud, mobile • Integration with other security solutions: SIEM, WAF, etc.	• Precise results with few false positives • Language support: COBOL, C++, Objective C, ABAP, etc • Ease of use for non-security users • Integration with development processes – IDE, defect tracking, test plans, etc.
Offering	AppScan Standard	AppScan Standard	AppScan Enterprise AppScan Source	AppScan Enterprise AppScan Source

Thank
You

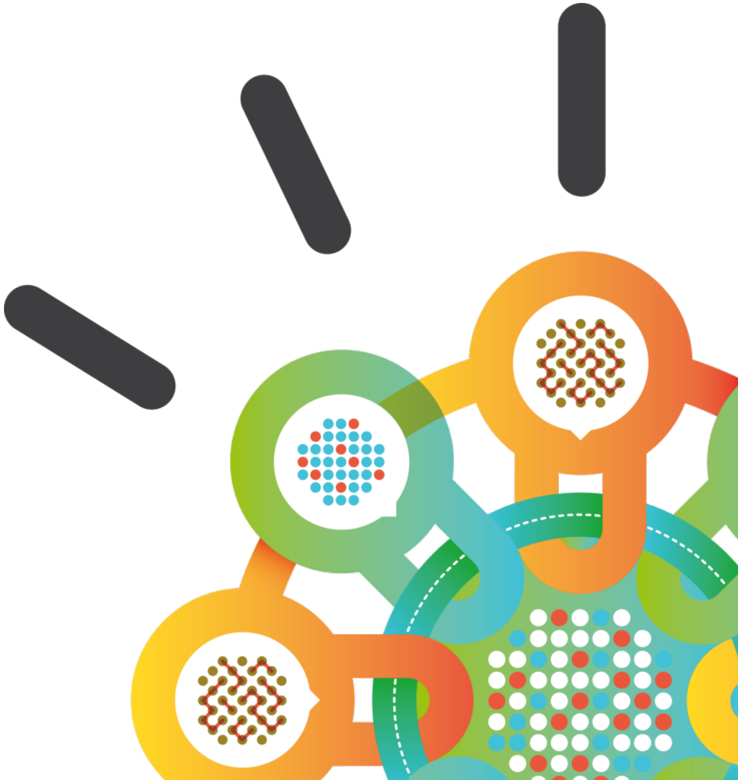
Time	Topic	Speakers
9:05am - 9:45am	Security Stream Kickoff-Security and compliance Overview and X Force	Joe Ruthven and Sukhdev Singh
9:45am - 10:25am	Threat	Lekgale Mokota
10:25am - 10:40am	Break	
10:40am - 11:10am	Q1 Labs Security Intelligence Strategy and Roadmap – How to use Security Intelligence for detecting threats and exceeding compliance mandates	Murray Benadie
11:10am - 11:40am	Driving Effective Application Security in the Enterprise: An End to End Approach to Addressing One of the Biggest Threats to a Business	Sukhdev Singh
11.40am - 12:10pm	**Identity Intelligence: Enabling Secure Cloud and Mobile Access**	Kevin Mckerr (Puleng)
12:10pm - 12:15 pm	Closing and Questions	
12:15pm	Lunch and Networking	

Security Intelligence.
Think Integrated.

PULENG
IDENTITY

pu-leng *n.*
Tswana, *rain (used as greeting for good fortune)*

A Tswana word that means a place of rain and a symbol of knowledge and wealth.



Identity Management (IdM) describes the management of individual identities, their authentication, authorisation, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks.

Technical

-User Access

-Account Provisioning

-User Authentication

-Identity Federation

-Password Management

Business

-Access to information & resources

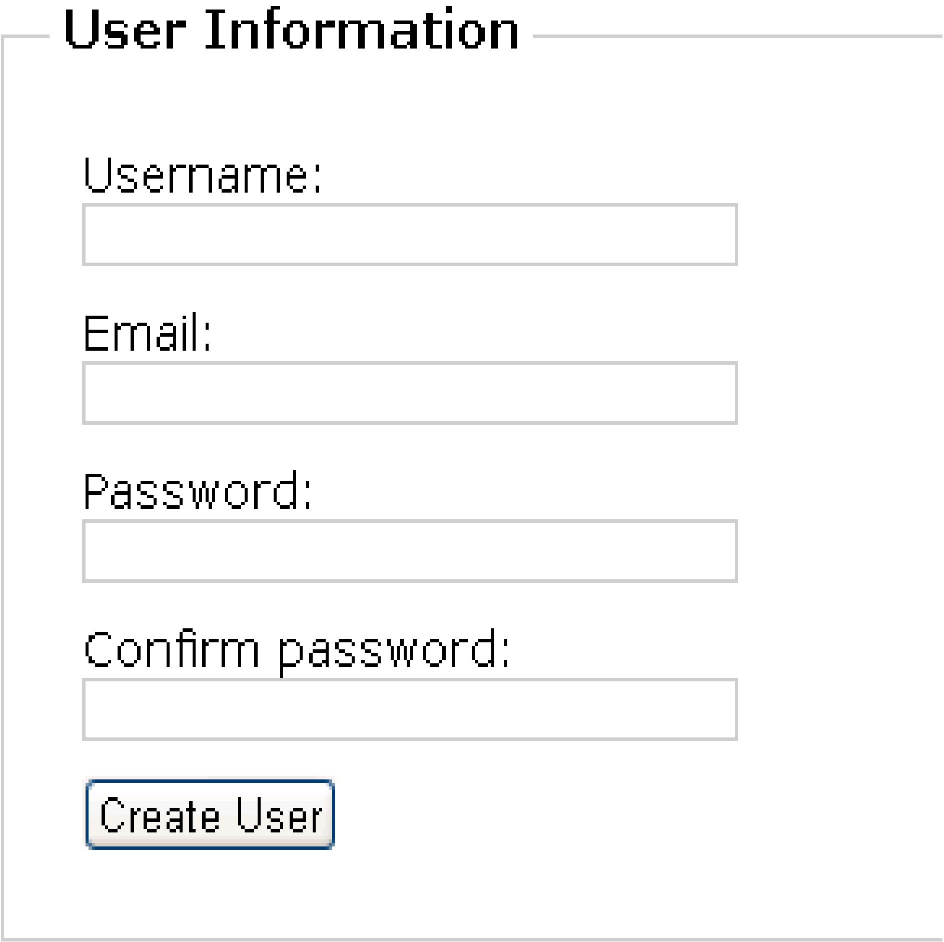
-Unique Customer Experience

-Channel Convergence

-Single View of Customer

-Governance, Risk, Compliance

Fiduciary Responsibility



User Information

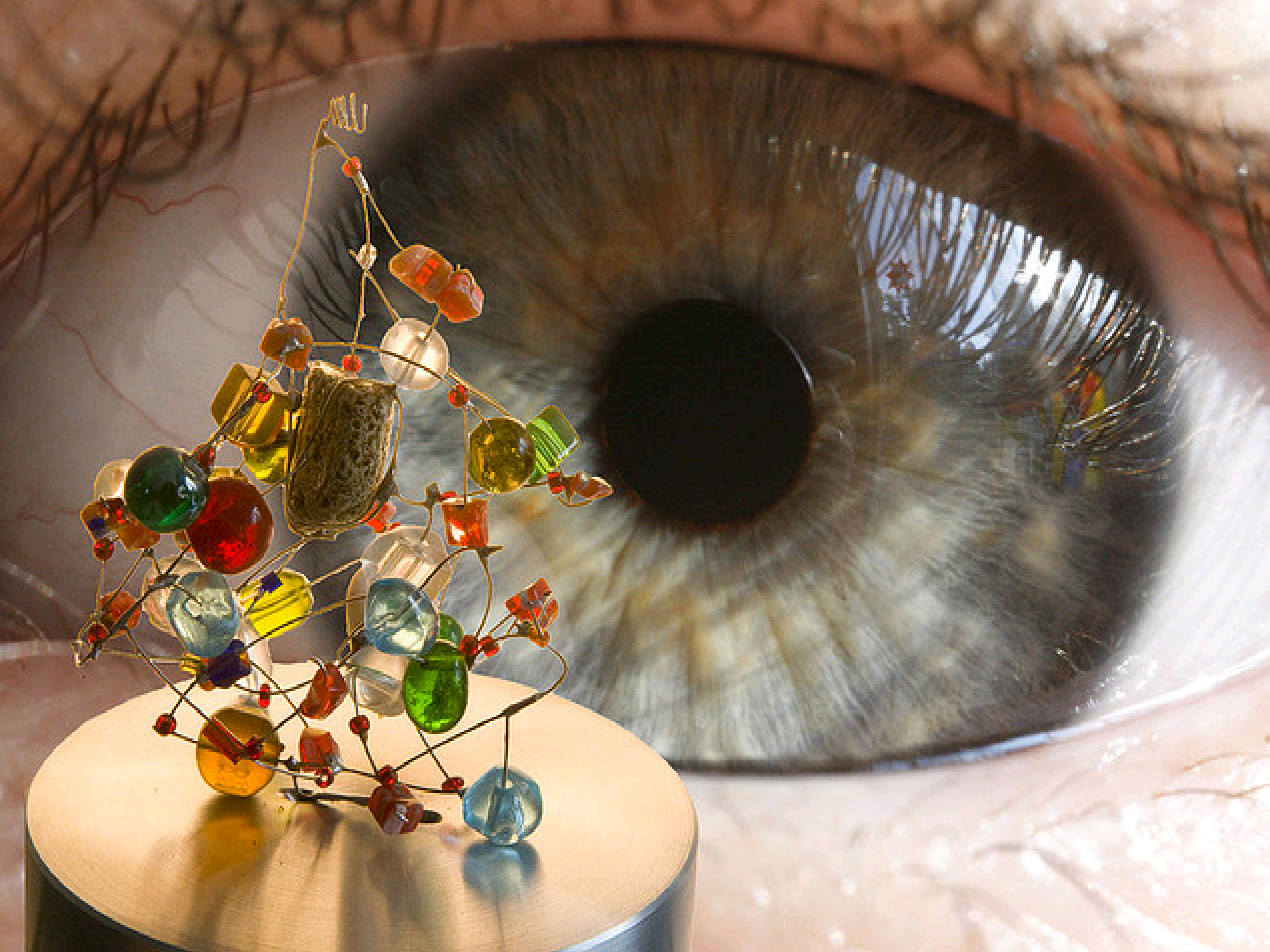
Username:

Email:

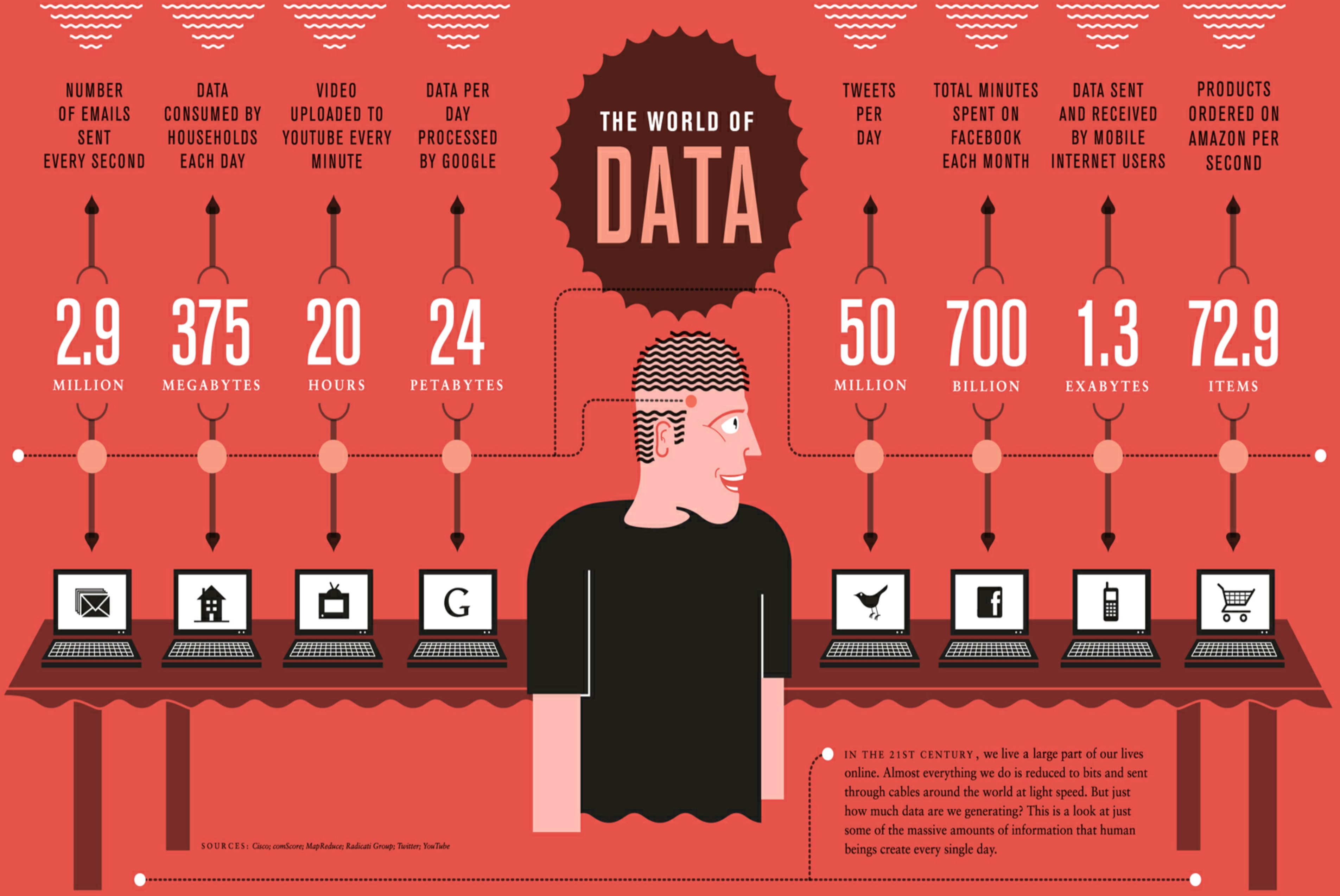
Password:

Confirm password:

13:55



THE WORLD OF DATA



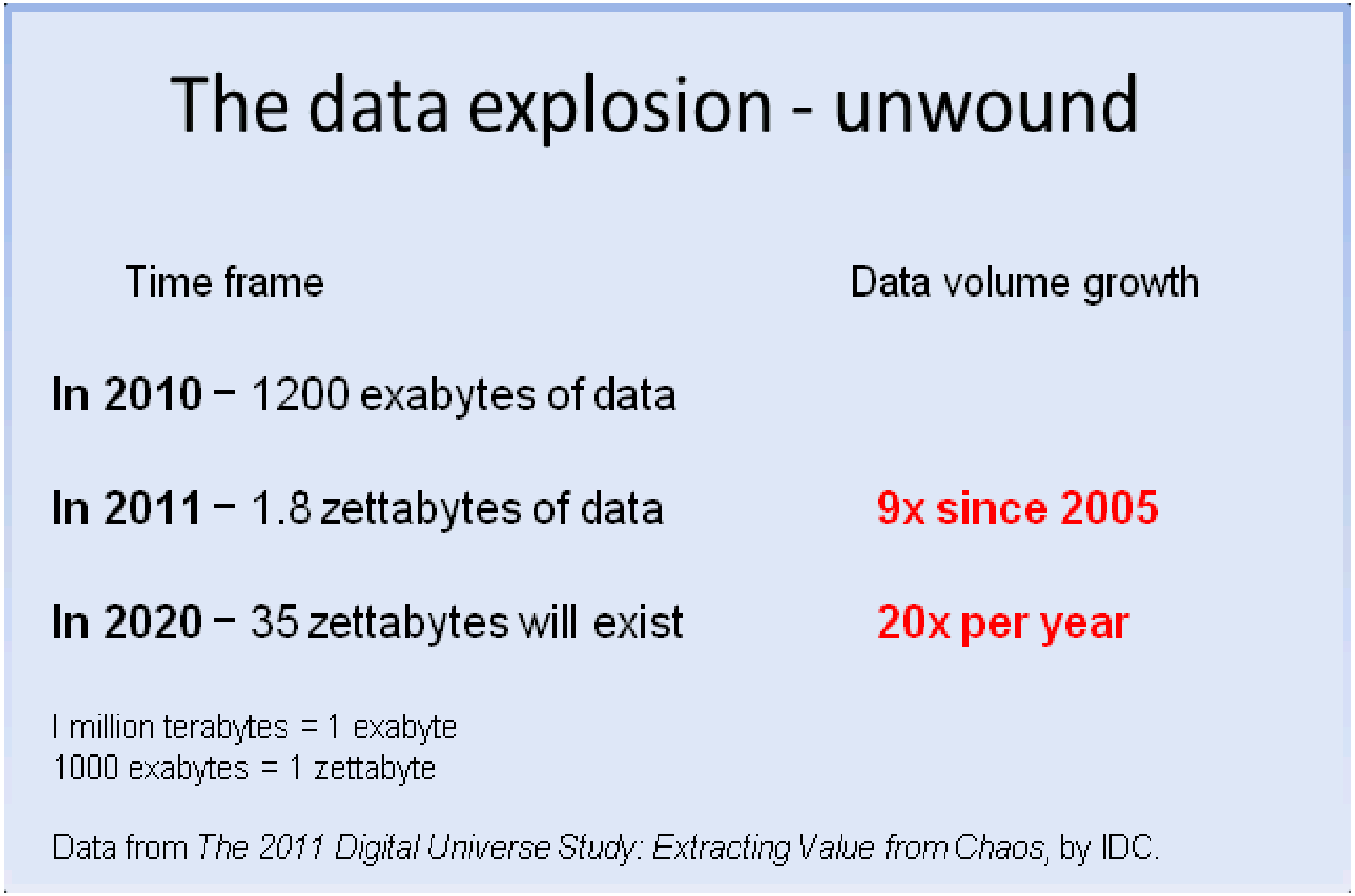
NUMBER OF EMAILS SENT EVERY SECOND	2.9	MILLION
DATA CONSUMED BY HOUSEHOLDS EACH DAY	375	MEGABYTES
VIDEO UPLOADED TO YOUTUBE EVERY MINUTE	20	HOURS
DATA PER DAY PROCESSED BY GOOGLE	24	PETABYTES
TWEETS PER DAY	50	MILLION
TOTAL MINUTES SPENT ON FACEBOOK EACH MONTH	700	BILLION
DATA SENT AND RECEIVED BY MOBILE INTERNET USERS	1.3	EXABYTES
PRODUCTS ORDERED ON AMAZON PER SECOND	72.9	ITEMS

IN THE 21ST CENTURY, we live a large part of our lives online. Almost everything we do is reduced to bits and sent through cables around the world at light speed. But just how much data are we generating? This is a look at just some of the massive amounts of information that human beings create every single day.

SOURCES: *Cisco; comScore; MapReduce; Radicati Group; Twitter; YouTube*

A COLLABORATION BETWEEN GOOD AND OLIVER MUNDAY

IN PARTNERSHIP WITH IBM



The data explosion - unwound

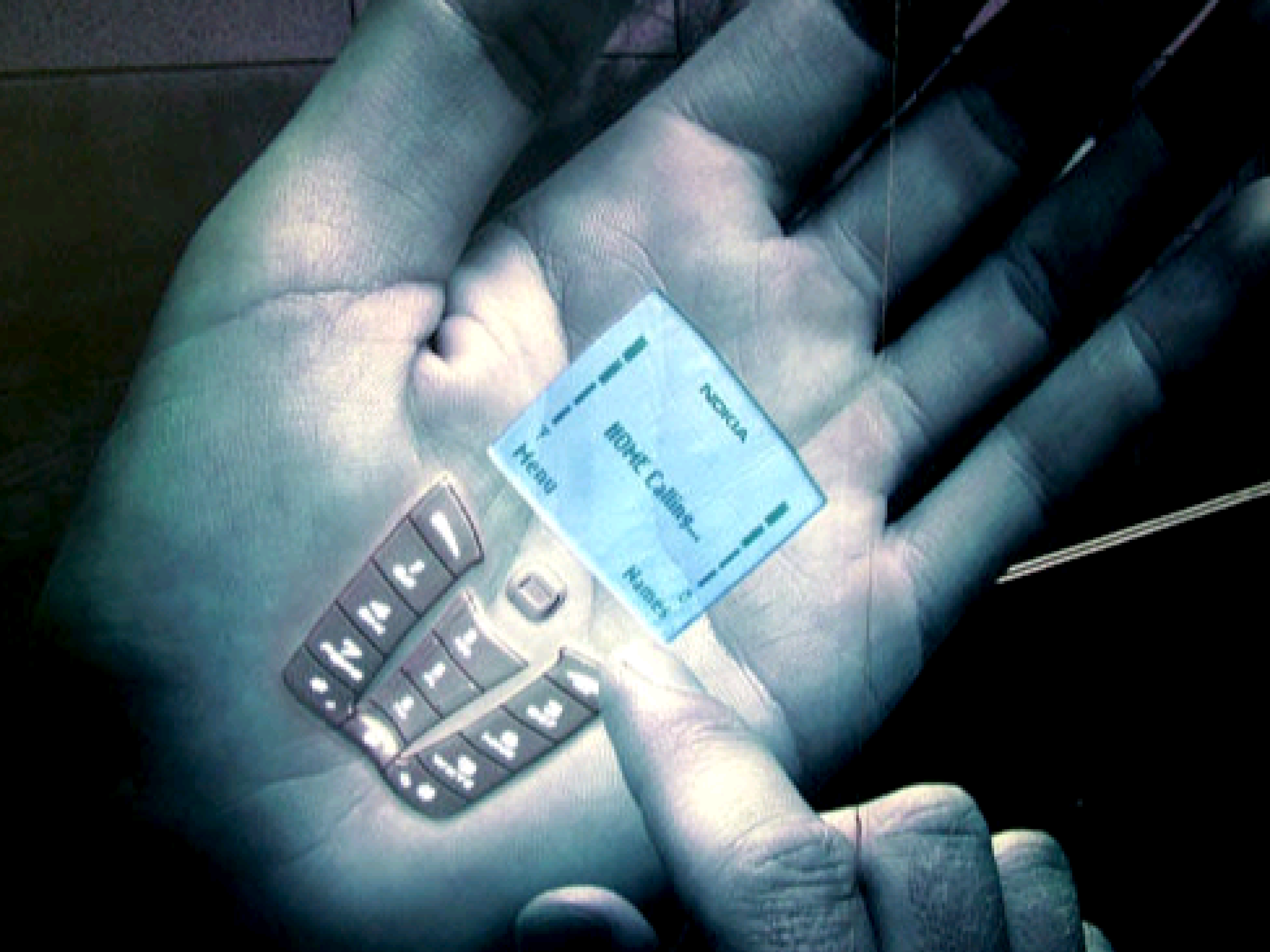
Time frame	Data volume growth
In 2010 – 1200 exabytes of data	
In 2011 – 1.8 zettabytes of data	**9x since 2005**
In 2020 – 35 zettabytes will exist	**20x per year**

l million terabytes = 1 exabyte
1000 exabytes = 1 zettabyte

Data from *The 2011 Digital Universe Study: Extracting Value from Chaos*, by IDC.

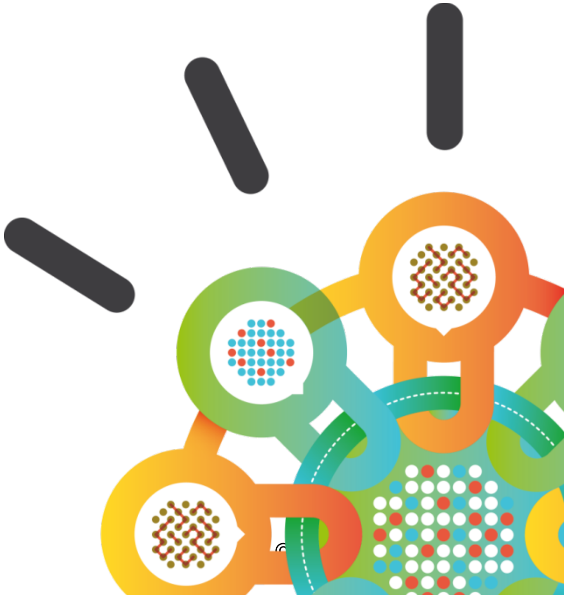
It's a sunny day.

morph

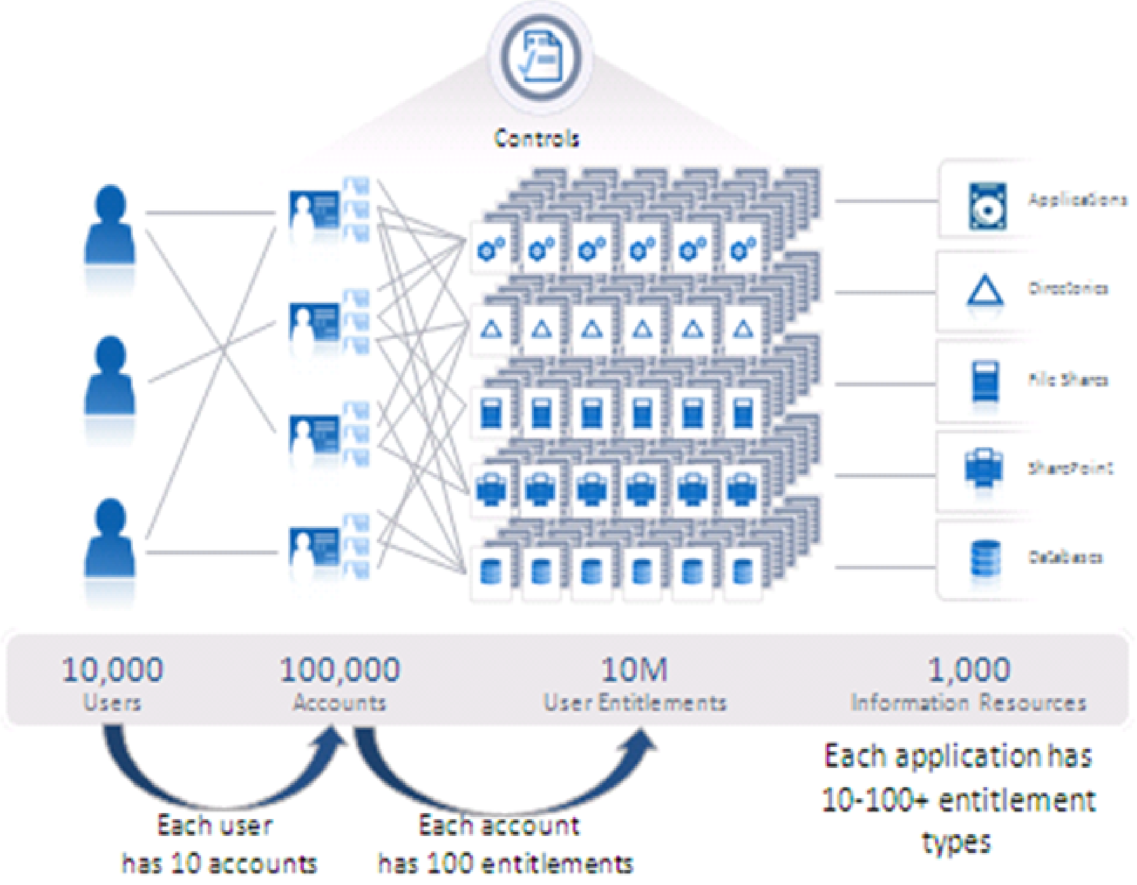


NOKIA
Calling...
Menu
Names

> “In short, if you have the image in your mind that a successful cybersecurity strategy is a moat, your strategies, laws and regulations will fail. A moat does not protect from attacks from within, which constitute nearly 80 percent of all cybercrimes.”



Challenges: Complexity and Scale



10,000 Users

100,000 Accounts

10M User Entitlements

1,000 Information Resources

Each user has 10 accounts

Each account has 100 entitlements

Each application has 10-100+ entitlement types

RED ALERT

Who has access
to what?

RFP

-Consultant defines requirements + 6 months

-RFP Send out & Vendor Response + 2 months

-Evaluation & Testing + 3 months

-Selection & Contracting + 2 months

-Rollout + 3 – 6 – 9 months

-Response Time = 15 – 22 months

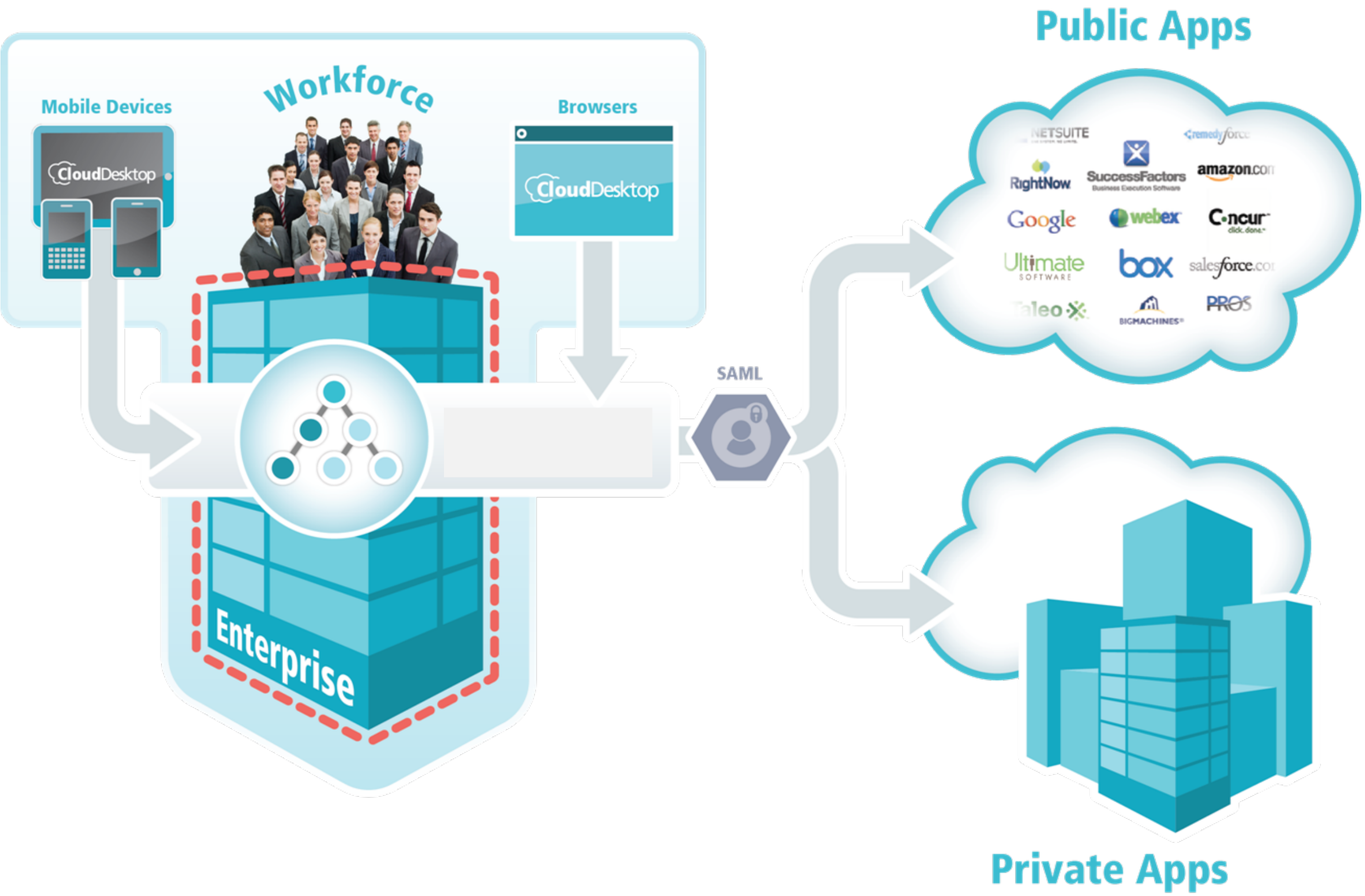
A new way is needed!!

-Packaged Solutions

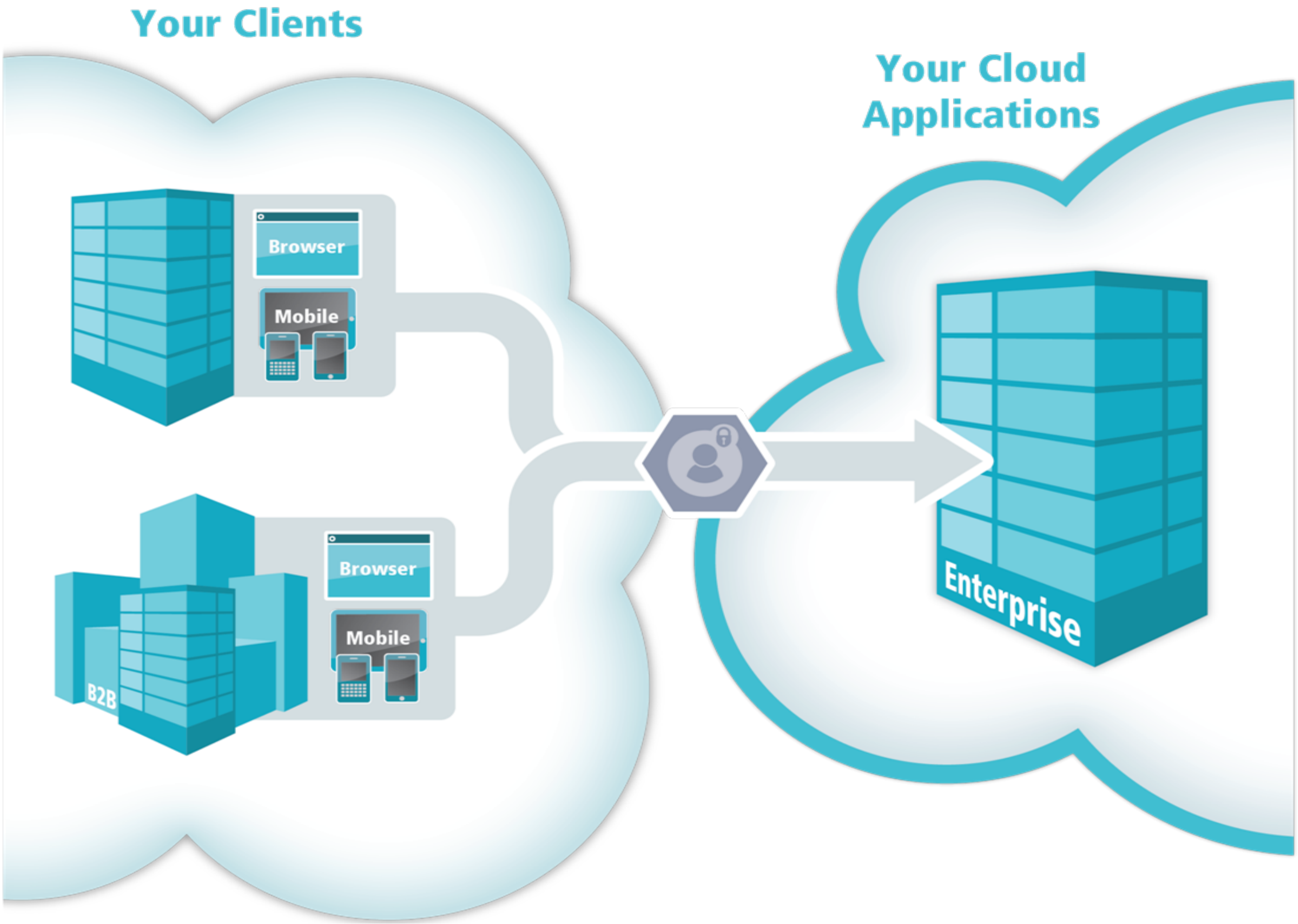
-Specific function

-At a fixed cost and timeframe

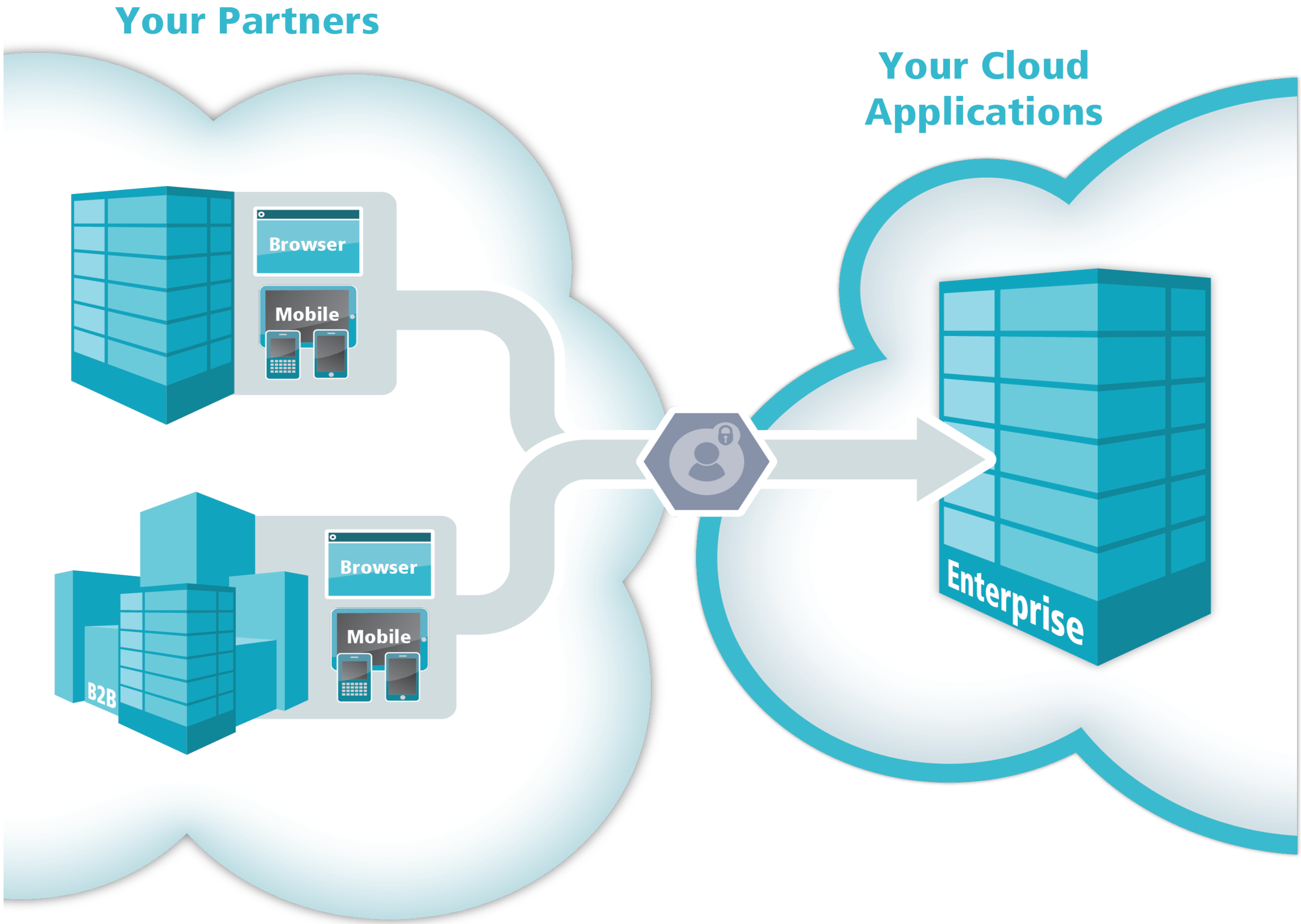
-Delivering immediate countermeasures



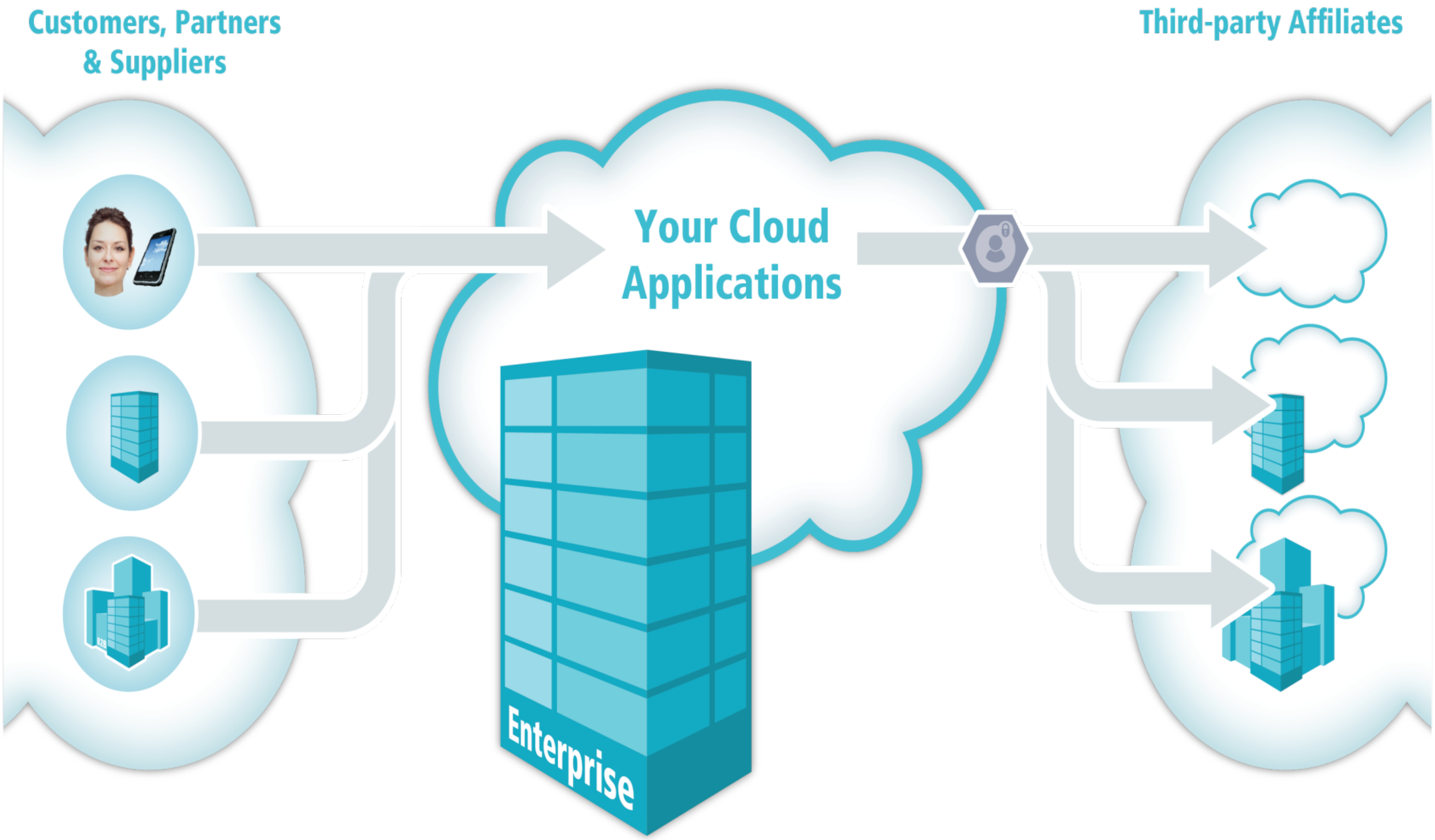
#1 Secure Cloud Apps for Your Employees



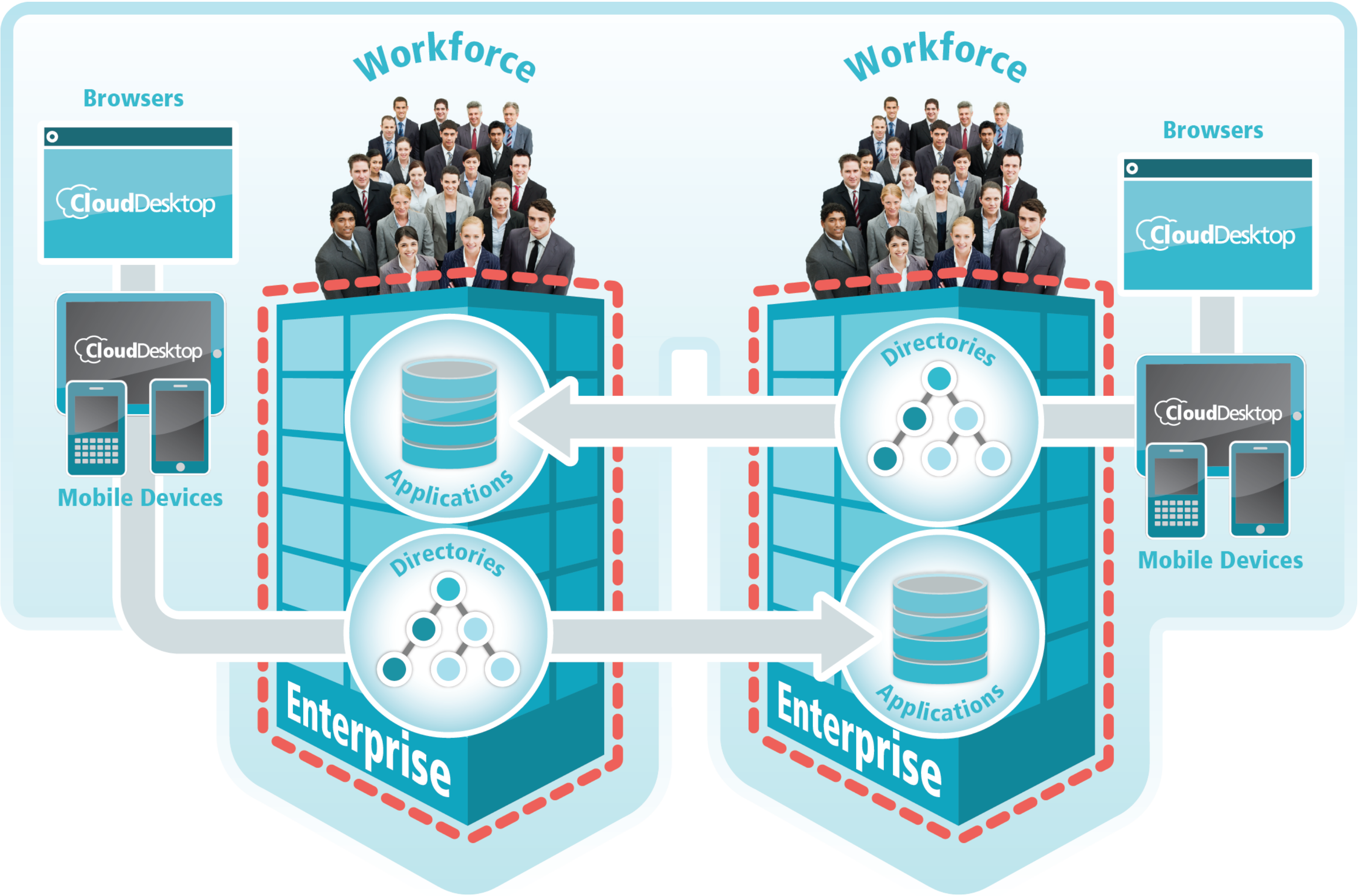
#2 Secure Your Client-Facing Apps



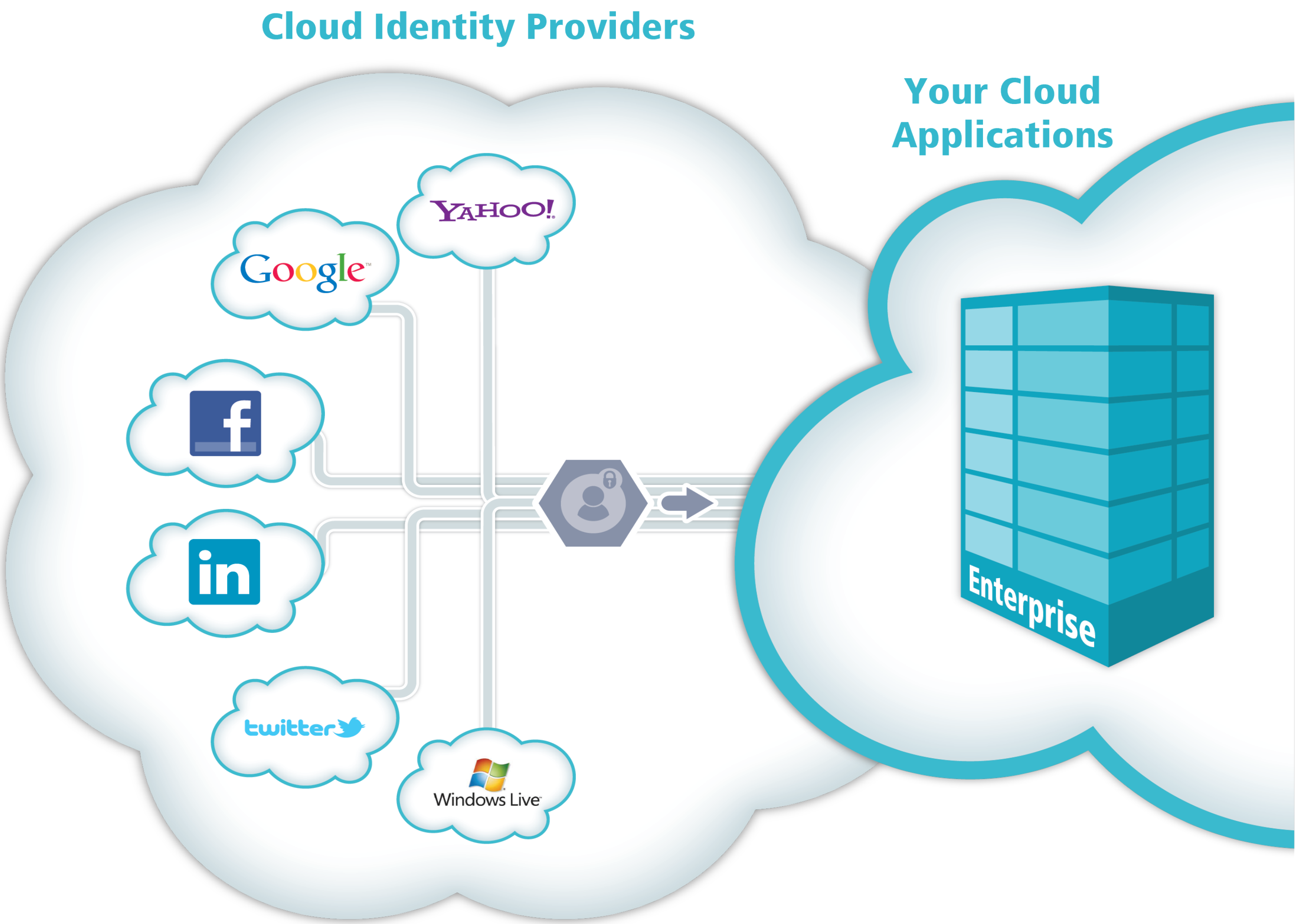
#3 Secure Your Partner-Facing Apps



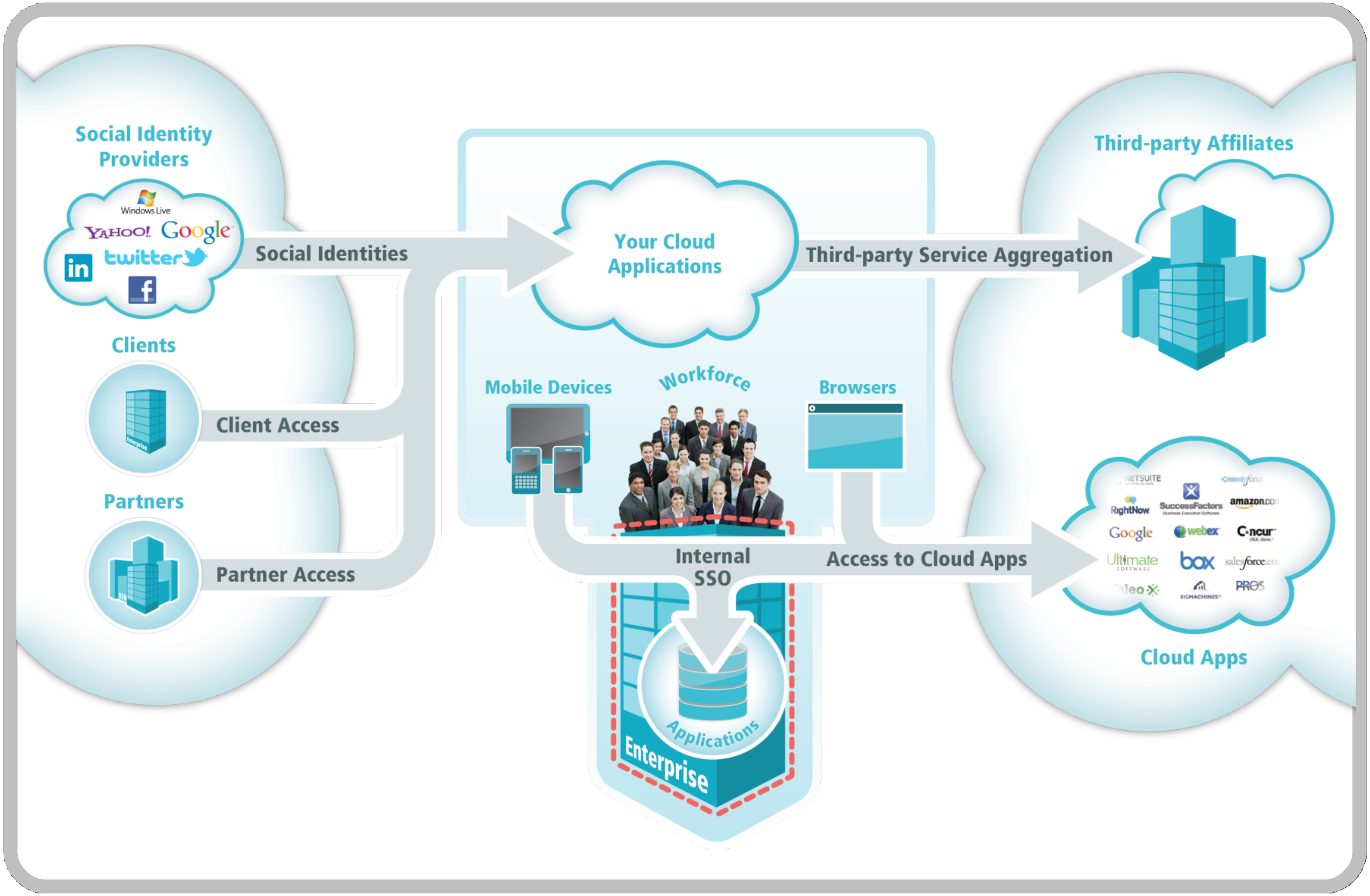
#4 Third Party App Integration



#5 Internal Single Sign-on



#6 Social Identity / Client Facing Apps



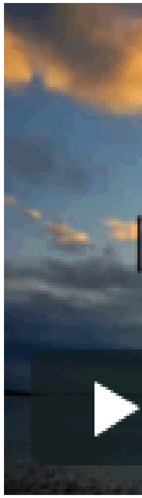
How it fits together☺

RED ALERT

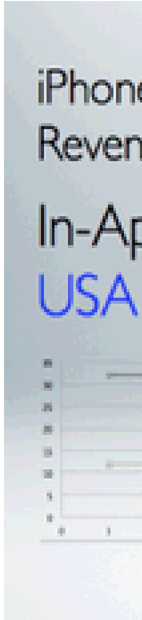
1. Who has access to what?
2. Sort out my passwords!
3. Enable Self Service

[Editor's Pick] Smartphone Users Are Almost 33% More Likely To Become Victims of Identity Theft Then the General Public, in the US

by CHARLES STEPHENS on Mar 21, 2012 · 6:00 am



PRODUC



Mail&Guardian
AFRICA'S BEST READ

Six simple ways to prevent identity theft

13 SEP 2010 20:43 - FIONA ZERBST

Recommend 0 Tweet 0

& ORIGINAL

Identity theft is far more common than people think and it costs the economy about R1-billion each year.

Identity theft is far more common than people think and it costs the economy about R1-billion each year.

As the white-collar crime of choice, it's fairly easy to pull off.

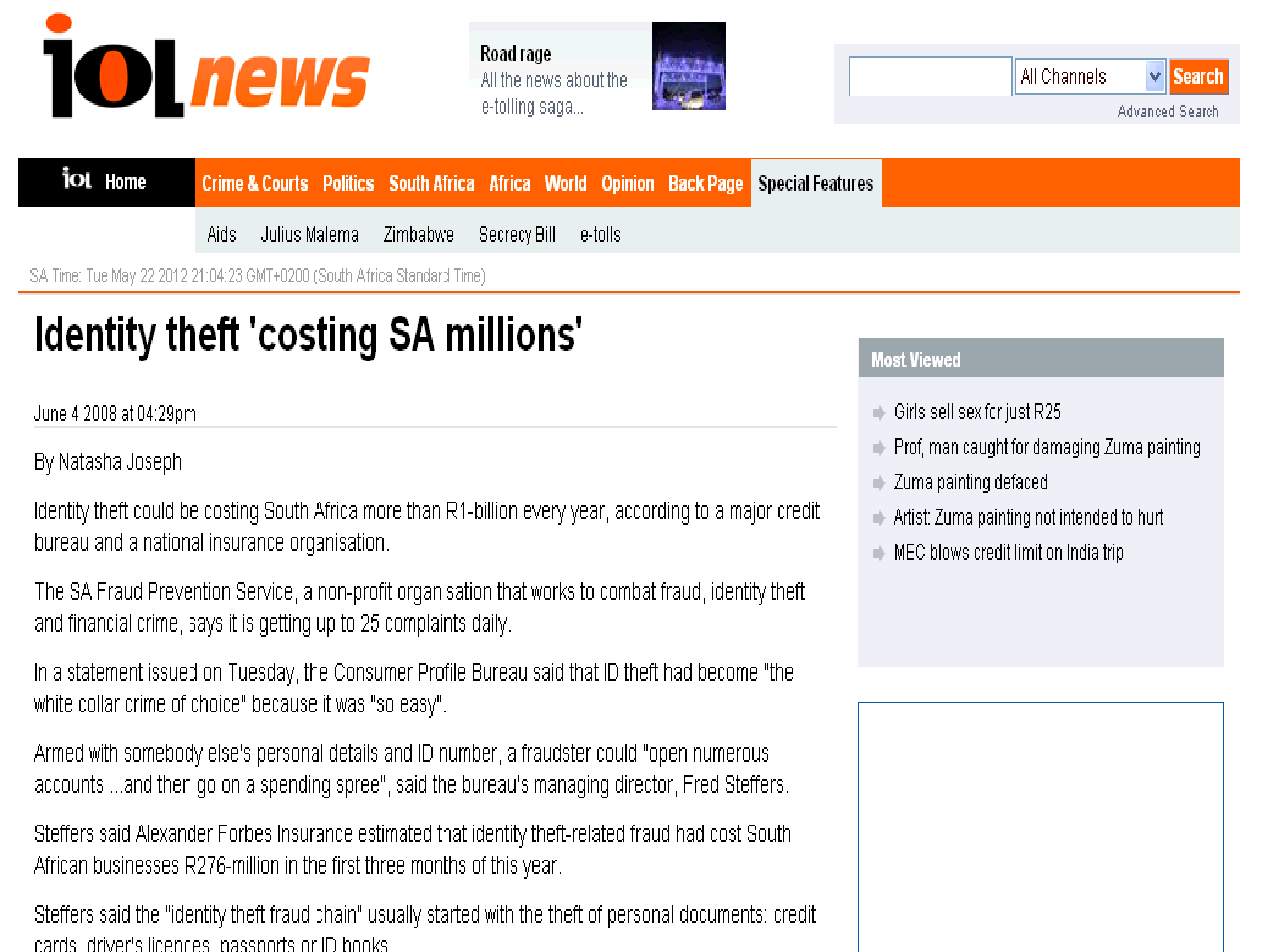
There are about 20 cases reported in South Africa every day, so follow these tips to be safe rather than sorry:

- Safeguard your ID book and passport—if you lose them or they are stolen, report the theft to the police immediately and register for the South African Fraud Prevention Service's free protective registration service. You will need to supply a case number.

- Check and double-check your bank statements and your credit card statements every month and

CONNECT

JOIN UP



iol news

Road rage
All the news about the e-tolling saga...

All Channels Search
Advanced Search

iol Home Crime & Courts Politics South Africa Africa World Opinion Back Page Special Features

Aids Julius Malema Zimbabwe Secrecy Bill e-tolls

SA Time: Tue May 22 2012 21:04:23 GMT+0200 (South Africa Standard Time)

Identity theft 'costing SA millions'

June 4 2008 at 04:29pm

By Natasha Joseph

Identity theft could be costing South Africa more than R1-billion every year, according to a major credit bureau and a national insurance organisation.

The SA Fraud Prevention Service, a non-profit organisation that works to combat fraud, identity theft and financial crime, says it is getting up to 25 complaints daily.

In a statement issued on Tuesday, the Consumer Profile Bureau said that ID theft had become "the white collar crime of choice" because it was "so easy".

Armed with somebody else's personal details and ID number, a fraudster could "open numerous accounts ...and then go on a spending spree", said the bureau's managing director, Fred Steffers.

Steffers said Alexander Forbes Insurance estimated that identity theft-related fraud had cost South African businesses R276-million in the first three months of this year.

Steffers said the "identity theft fraud chain" usually started with the theft of personal documents: credit cards, driver's licences, passports or ID books.

Most Viewed

- Girls sell sex for just R25
- Prof, man caught for damaging Zuma painting
- Zuma painting defaced
- Artist: Zuma painting not intended to hurt
- MEC blows credit limit on India trip

Parliament condemns R42m Postbank hacking

SAPA | January 16, 2012 | 3 Comments | Tweet 7 | Like 0

The theft of R42 million from SA Post Office financial institution Postbank was condemned by Parliament's communications portfolio committee on Monday

The theft of R42 million from SA Post Office financial institution Postbank was condemned by Parliament's communications portfolio committee on Monday.

Portfolio chairman Eric Kholwane said the bank's security network needed to be tightened to prevent such a "hi-tech cyber heist".

He appreciated the discovery of the theft and welcomed an investigation by the National Intelligence Agency and the police.

SAPA

Sapa, or the South African Press Association, is a non-governmental news agency that was established in 1938. Sapa provides all forms of media, and is...

FOLLOW | Full Profile | E-mail

passport
social networking
travel
steal
trash
elderly
credit cards
privacy
social security number
websites
identity theft
shred
employer
bank account
date of birth
credit
address
driver's license
vulnerable
policy numbers
phone
trusting
lock
statements
name
safety
open
mail
target
dreamstime.com

PULENG
IDENTITY