IBM Big Data Security Intelligent Platform

Baron Wu
IBM Security Specialist

Innovate2013
The IBM Technical Summit
開發者大會

Stay ahead.

Topic

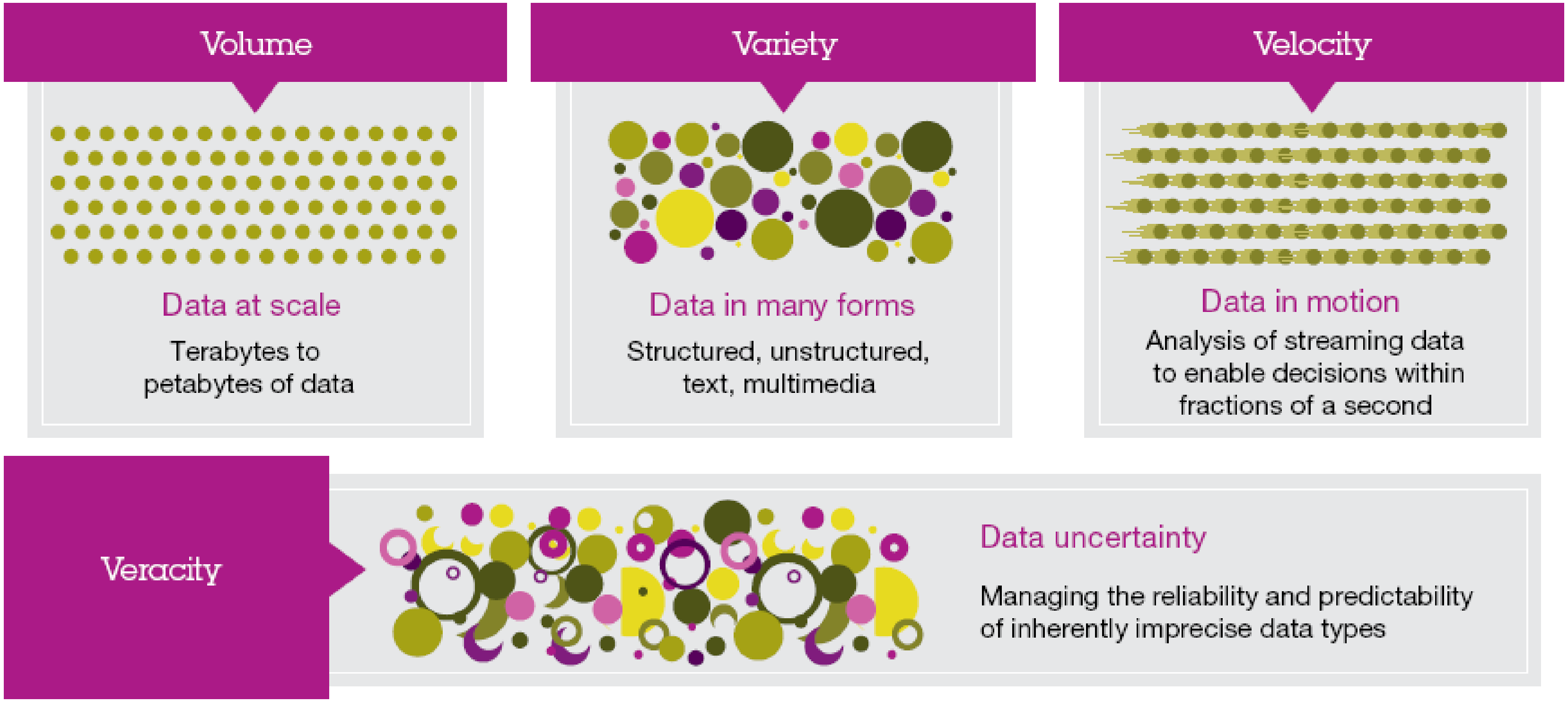
- 何謂Big Data 與構成之要素
- Big Data 資安之條件
- Big Data時代，機密資料保護能力必須再進化
- IBM 針對 Big Data 資安要件之解決方案
- 這樣就夠了嗎??
- Big Data 與SIEM 之結合

何謂Big Data 與構成之要素

巨量 － 海量資料的特色就在於： 龐大。 企業資料包羅萬端，很容易便達到數兆位元組，甚至千兆位元組之譜。

即時性 － 海量資料通常具有時效性，一旦串流至企業便須立即使用，方能發揮其最大價值。

多樣性 － 海量資料的範疇不僅止於結構化資料，還包含各類非結構化的資料： 諸如文字、音訊、視訊、點擊串流 (click stream)、日誌檔等等。



Volume

Data at scale

Terabytes to petabytes of data

Variety

Data in many forms

Structured, unstructured, text, multimedia

Velocity

Data in motion

Analysis of streaming data to enable decisions within fractions of a second

Veracity

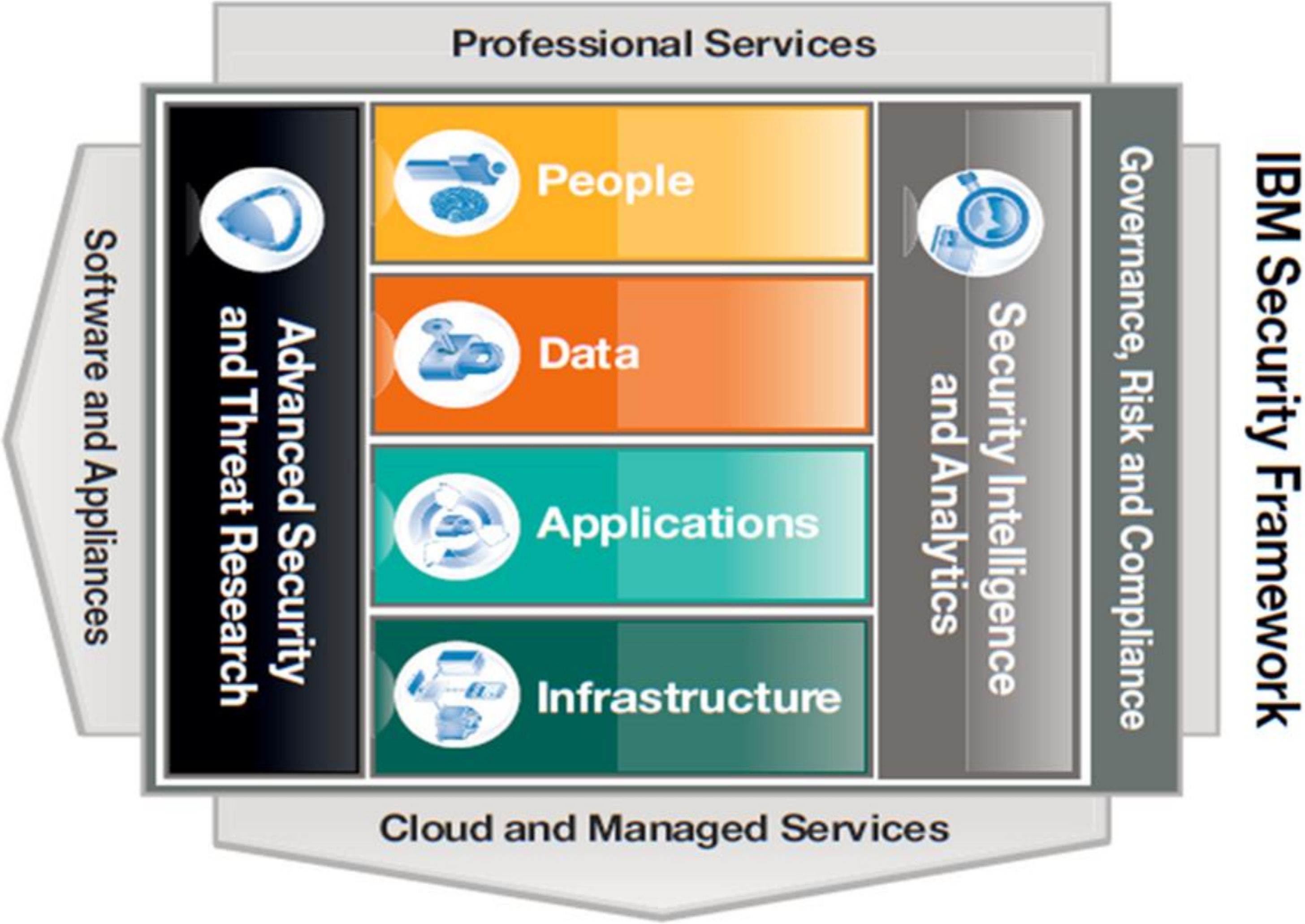
Data uncertainty

Managing the reliability and predictability of inherently imprecise data types

Big Data時代，機密資料保護能力必須再進化

伴隨雲端運算、行動應用及社群媒體崛起，使資料產生速度加劇，若企業能善用分析這些資料，即可從中挖掘擷出珍貴資訊、優化商業決策，這也讓Big Data議題因而火熱。但企業莫忘記海量資料仍是資料，亦是機密外洩的潛在缺口，肯定需要嚴加保護；尤其新版個資法上路，任何涉及個人資料的數據，從蒐集、處理、應用、傳遞至銷毀等過程之稽核軌跡，都應切實管控，一般交易型資料如此，海量資料亦然。

Big Data 資訊安全之要素


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

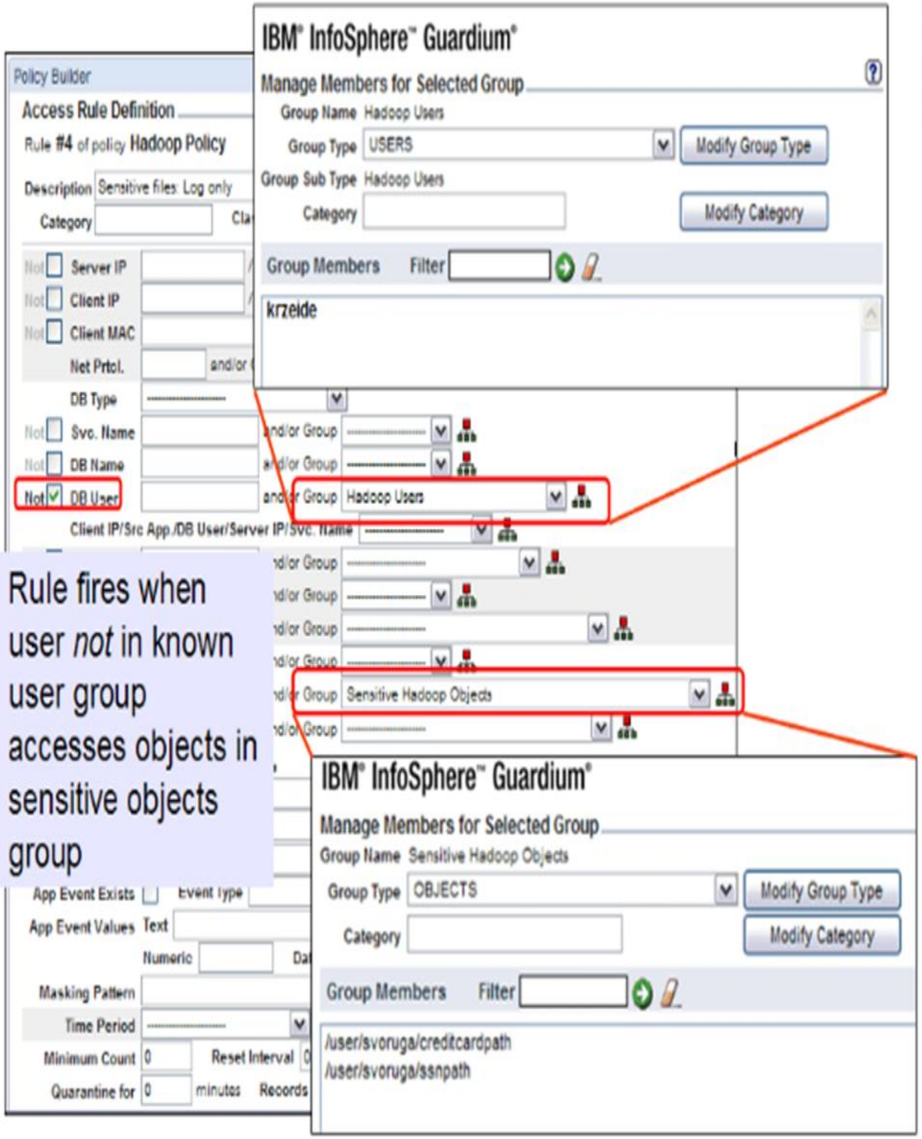
人員認證及授權管理 (People Access Control)

- Who can access??
- What can be accessed??
- When to access??

Big Data 資料稽核管理（Data Auditing and control）

Big Data的資料是經過萃取的，對企業來說是非常有價值性的。

- 誰存取過資料(內部? 外部?)
- 存取的資料內容為何
- 是否是公司機密資料
- 什麼時間點取得的



Policy Builder

Access Rule Definition

Rule #4 of policy Hadoop Policy

Description: Sensitive files: Log only

Category:

Not □ Server IP

Not □ Client IP

Not □ Client MAC

Net Prtol. and/or

DB Type: ----------

Not □ Svc. Name, and/or Group: ----------

Not □ DB Name, and/or Group: ----------

Not ☑ DB User, and/or Group: Hadoop Users

Client IP/Src App./DB User/Server IP/Svc. Name: ----------

and/or Group: Sensitive Hadoop Objects

App Event Exists □ Event Type

App Event Values: Text, Numeric

Masking Pattern

Time Period: ----------

Minimum Count: 0, Reset Interval: 0

Quarantine for: 0 minutes, Records

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group

Group Name: Hadoop Users

Group Type: USERS

Group Sub Type: Hadoop Users

Category:

Group Members, Filter:

krzeide

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group

Group Name: Sensitive Hadoop Objects

Group Type: OBJECTS

Category:

Group Members, Filter:

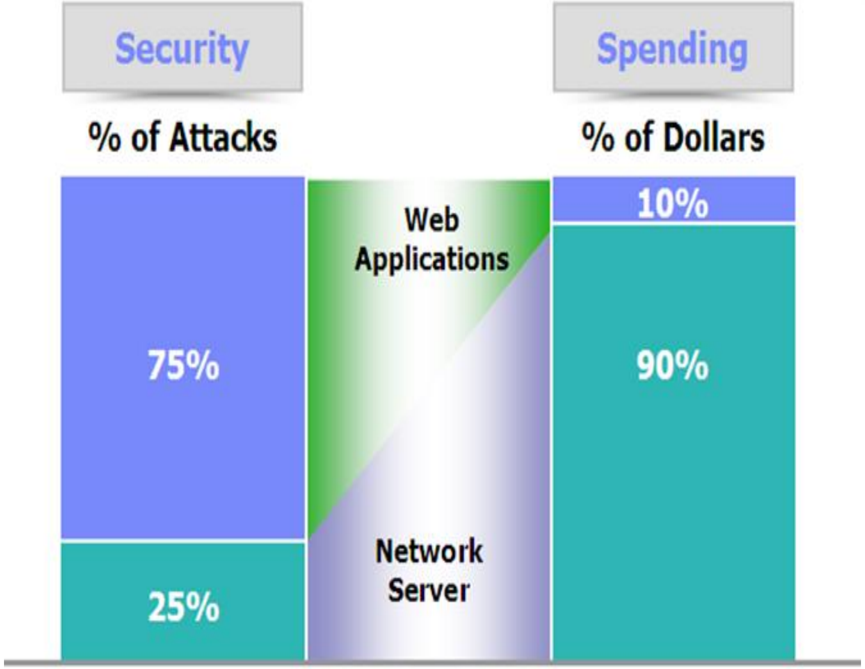
/user/svoruga/creditcardpath
/user/svoruga/ssnpath

Rule fires when user *not* in known user group accesses objects in sensitive objects group

Big Data 應用層面之安全性

Big Data的使用需要人及應用系統介面來做為存取或者查詢，但目前應用層是最容易被攻擊的部分。

- 企業的Web層到底有多少弱點
- 這些弱點是否可以修補
- 這些弱點會否讓我的資料被竊取
- 企業內部之程式碼及Web是否合規



75% 的駭客攻擊是針對Web應用系統而來的

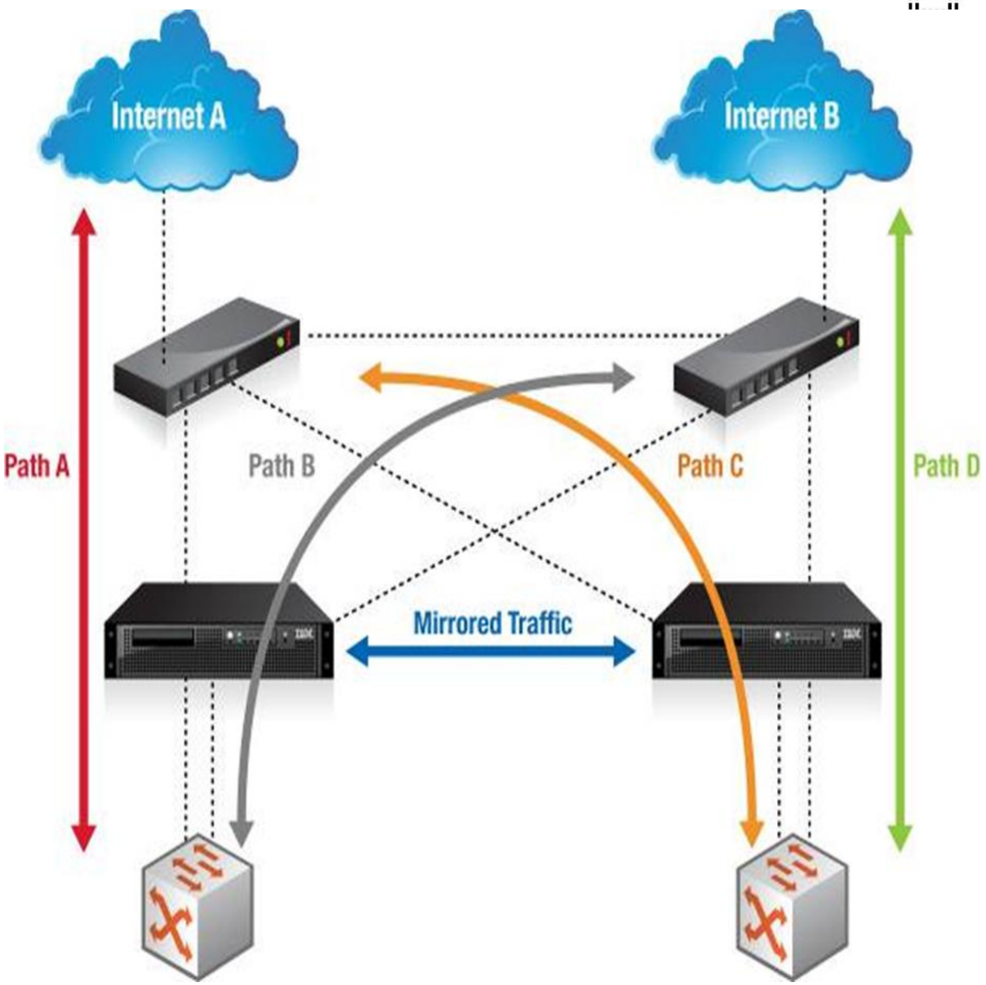
2/3 的Web應用系統是具有嚴重漏洞的

Gartner

Big Data Infra 層面之安全性

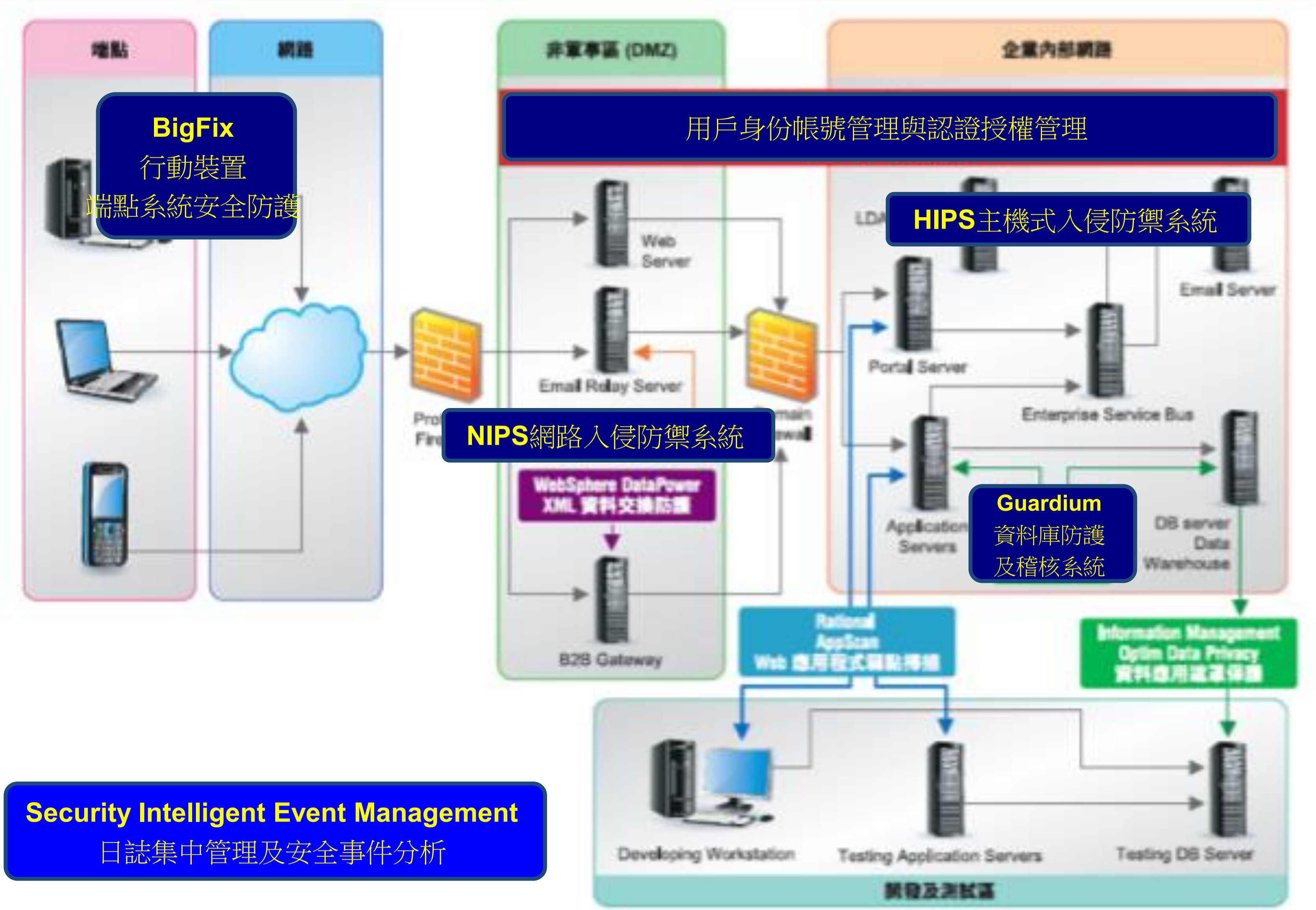
企業內部幾乎都有所謂的防火牆，IPS，IDS來偵測不正當之入侵及抵擋的動作。

- 可偵測異常網路流量
- 可 Block不正當的網路封包
- 阻擋不當IP進入企業網路



這樣就夠了嗎????

IBM 資訊安全解決方案概要



BigFix
行動裝置
端點系統安全防護

用戶身份帳號管理與認證授權管理

HIPS主機式入侵防禦系統

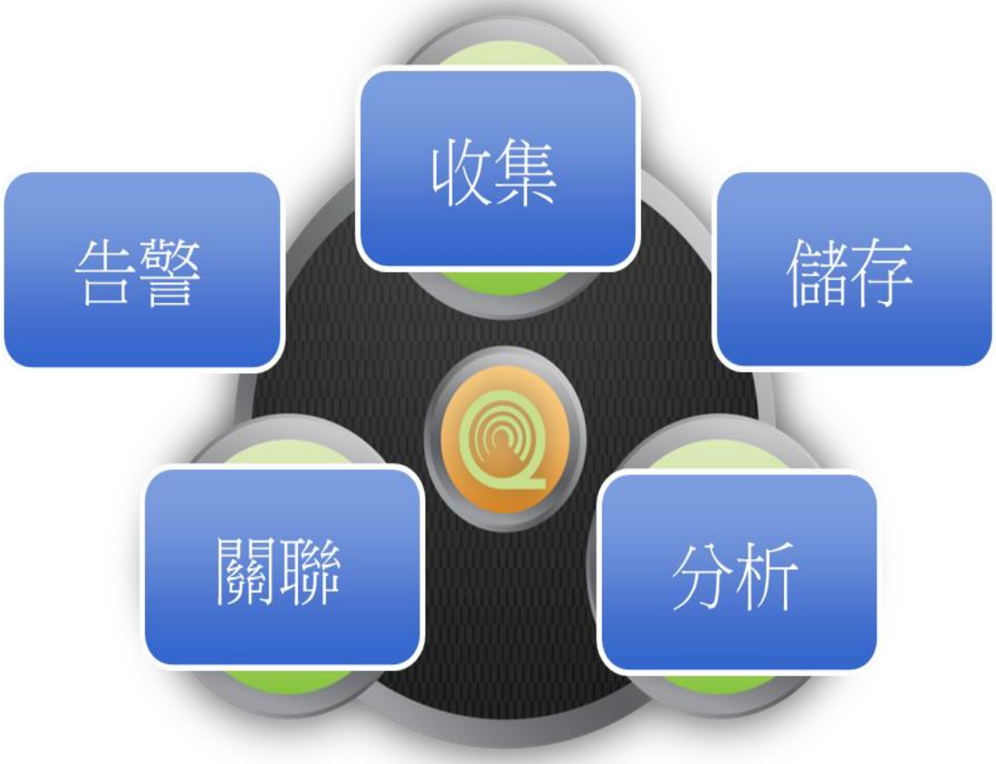
NIPS網路入侵防禦系統

Guardium
資料庫防護
及稽核系統

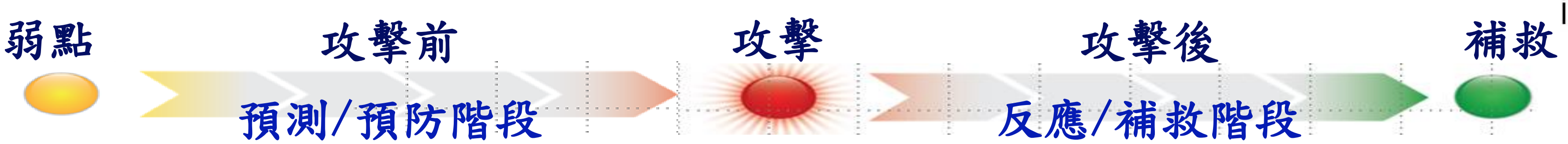
Security Intelligent Event Management
日誌集中管理及安全事件分析

企業目前所面臨的Big Data Security 之挑戰

- 是否可以即時知道所有攻擊之關聯
- 是否可以知道企業內部有哪些設備有弱點存在
- 是否可以防止日誌報告被篡改
- 企業目前本身的IT合規性是否維持在一定的水準
- 當系統有異常狀況，是否可即時告警
- 針對Layer 7的異常活動，是否可以及時阻止



IBM SIEM 提供全面的風險管理與事件調查影響分析能力



組態風險管理

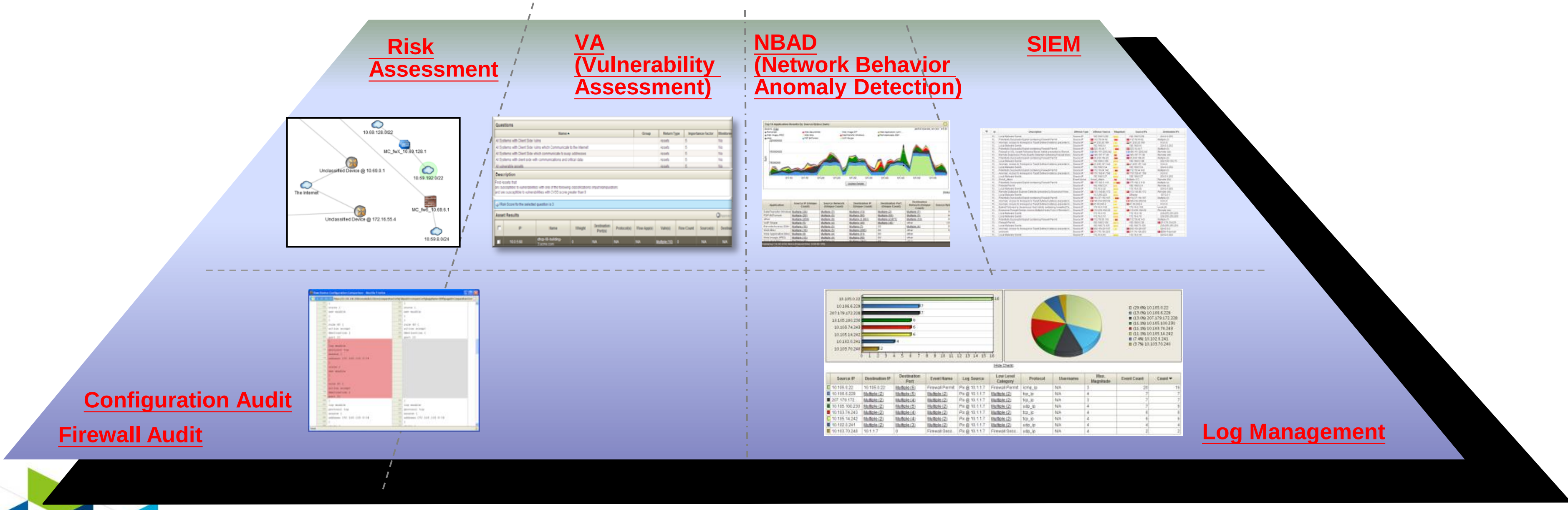
弱點與資產管理

網路活動異常檢測

資安事件關聯分析

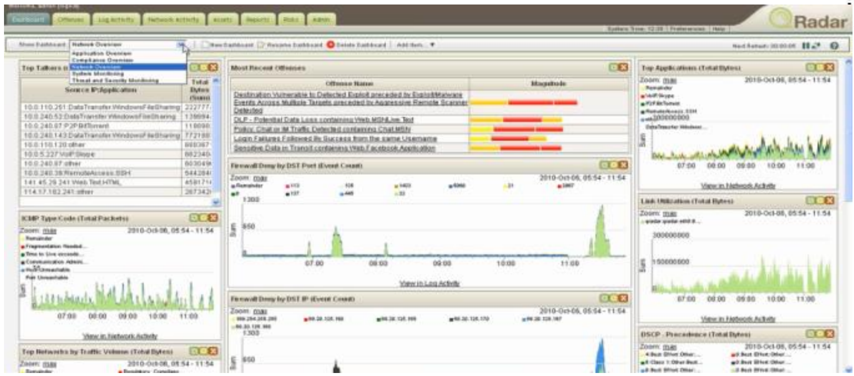
日誌管理

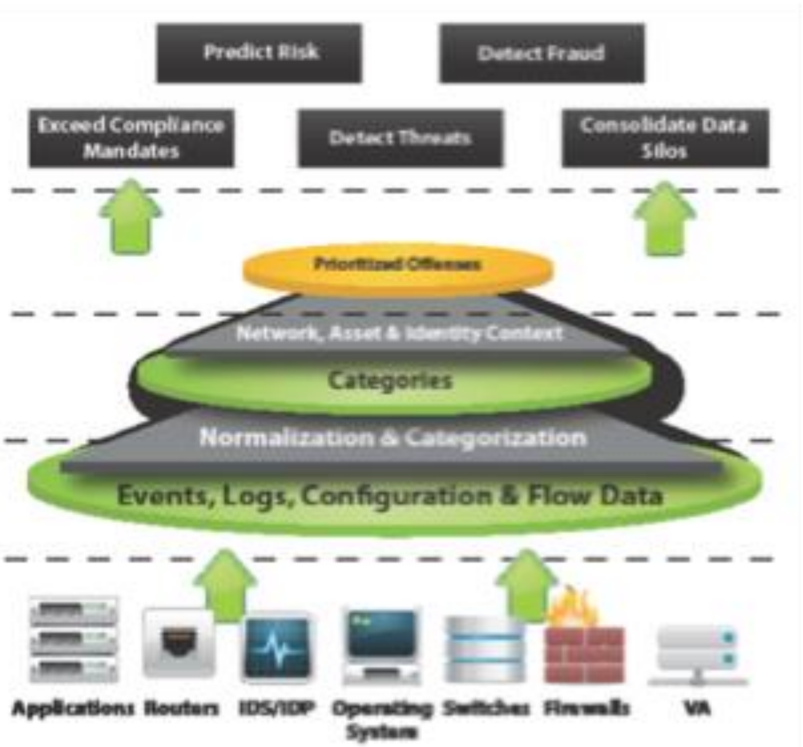
IBM 智能安全與風險管理 -- 提倡積極的五大步驟


Risk Assessment
VA (Vulnerability Assessment)
NBAD (Network Behavior Anomaly Detection)
SIEM
Configuration Audit
Firewall Audit
Log Management

可視化管理：威脅、記錄管理與法規遵循的即時可視性

- ❒ IBM SIEM 提供了一個高效能、安全風險分析管理平台 (embedded database)
- ❒ 先進的數據相關性技術，透過Agentless方式，結合不同的即時數據收集（日誌，事件，Layer 7 流量，網路攻擊，資產弱點，使用者/木馬/病毒/蠕蟲..等網路活動），並加入正規化(normalized)
- ❒ 證據壓縮與保存– 提供日誌防篡改與完整性檢查 (不可否認性)
- ❒ 及時和歷史事件的可視性和合規報告
- ❒ 支援關鍵字模糊搜尋 (Search Engine) 與 稽核日誌的自動彙整(Aggregation)

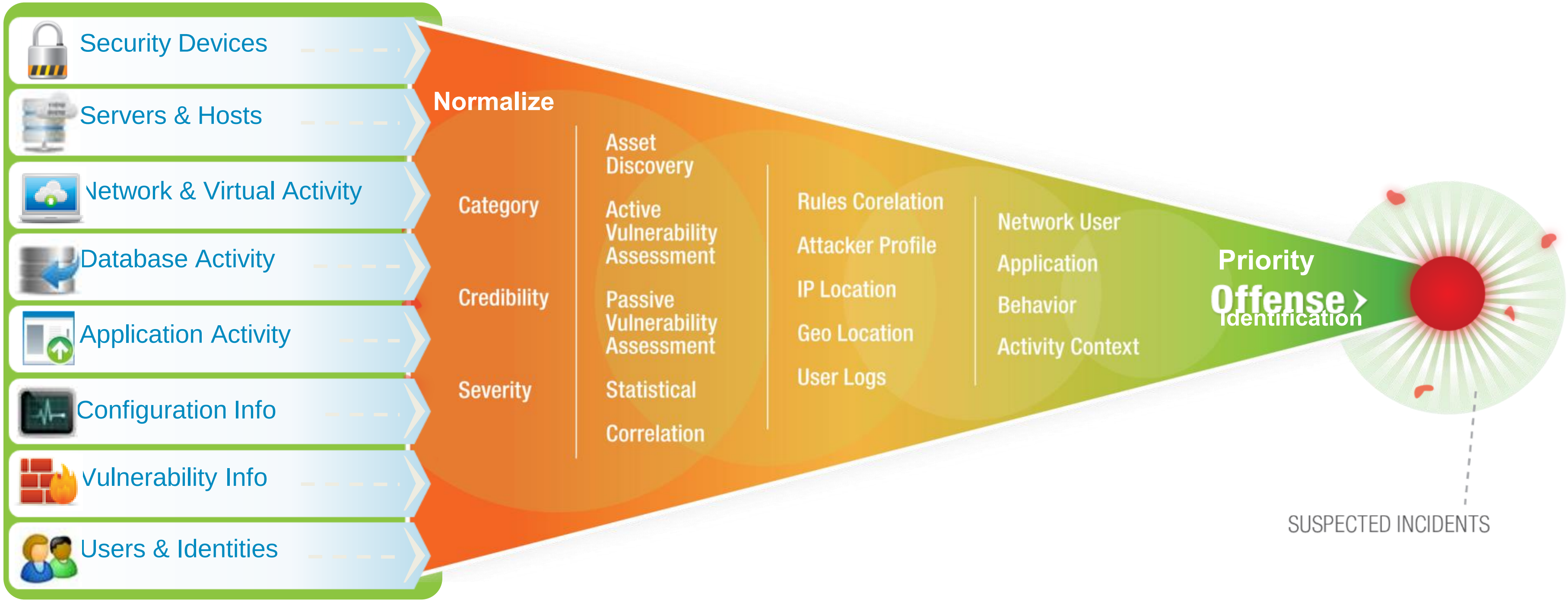

Radar
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Risks
Admin
Top Talkers
Most Recent Offenses
Top Applications (Total Bytes)
ICMP Type Code (Total Packets)
Firewall Deny by DST Port (Event Count)
Link Utilization (Total Bytes)
Firewall Deny by DST IP (Event Count)
Top Networks by Traffic Volume (Total Bytes)
DSCP - Precedence (Total Bytes)



Innovate2013
The IBM Technical Summit

日誌集中管理及分析方案提供廣泛的安全事件即時收集

收集***Desktop***、***Network Devices***、***Security Devices***、***mainframe***、***OS…***等的日誌，將安全事件關聯起來，產生各種合規報表，並隨時反映在儀表板上

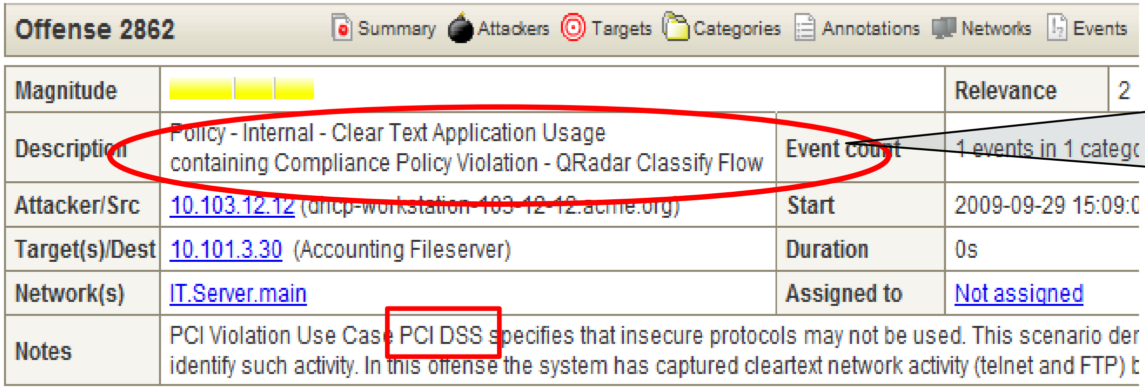


Sources

＋ Intelligence

＝ Most Accurate & Actionable Insight

自動化合規檢查與報表



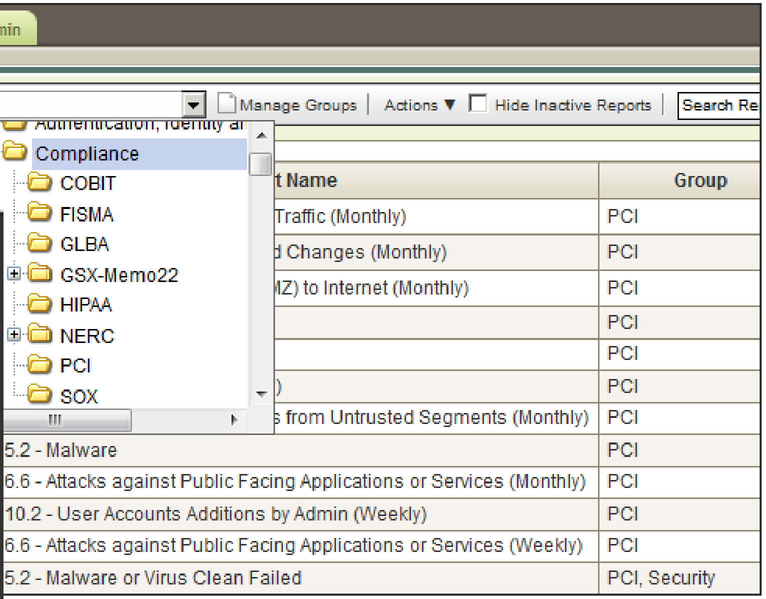
Offense 2862

Magnitude		Relevance	2
Description	Policy - Internal - Clear Text Application Usage containing Compliance Policy Violation - QRadar Classify Flow	Event count	1 events in 1 categ
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		

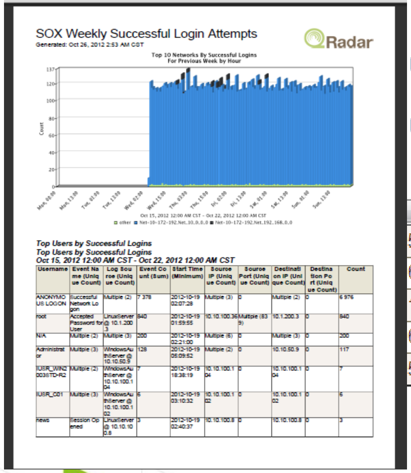
- 自動檢查事件是否違反法規 (Rule)

被QRadar 發現了一個在持卡人服務器上運行的 明文的服務 (未加密的資料流)

違反PCI法規第四條



t Name	Group
Traffic (Monthly)	PCI
d Changes (Monthly)	PCI
MZ) to Internet (Monthly)	PCI
	PCI
	PCI
)	PCI
s from Untrusted Segments (Monthly)	PCI
5.2 - Malware	PCI
6.6 - Attacks against Public Facing Applications or Services (Monthly)	PCI
10.2 - User Accounts Additions by Admin (Weekly)	PCI
6.6 - Attacks against Public Facing Applications or Services (Weekly)	PCI
5.2 - Malware or Virus Clean Failed	PCI, Security



SOX Weekly Successful Login Attempts

Generated: Oct 26, 2012 2:53 AM CST

Top Users by Successful Logins
Top Users by Successful Logins
Oct 15, 2012 12:00 AM CST - Oct 22, 2012 12:00 AM CST

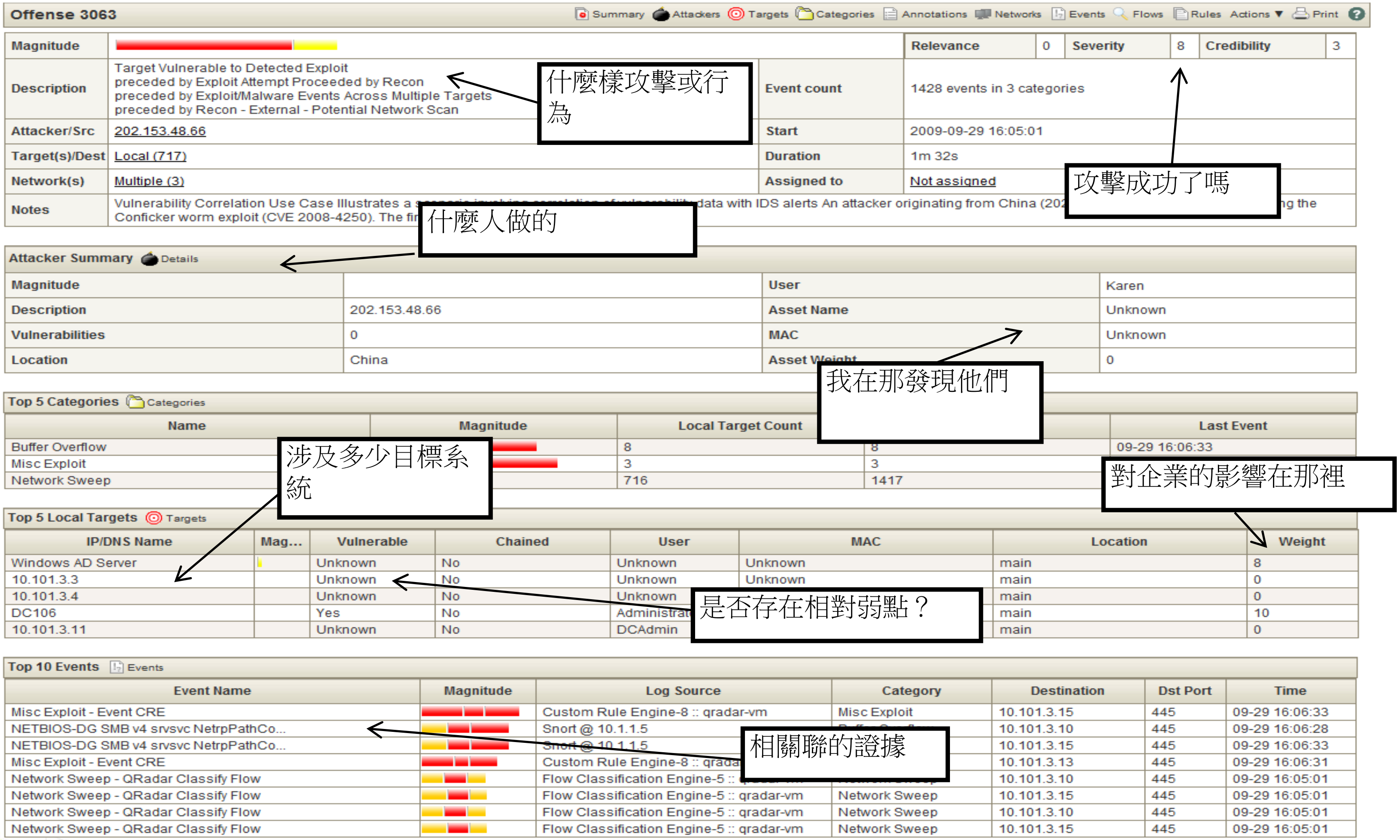
Username	Event Name (Unique Count)	Log Source (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Source IP (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Count
ANONYMOUS LOGON	Successful Network Logon	Multiple (2)	7 378	2012-10-19 02:07:28	Multiple (3)	0	Multiple (2)	0	6 976
root	Accepted Password for User	LinuxServer @ 10.1.200.3	840	2012-10-19 01:59:55	10.10.100.36	Multiple (839)	10.1.200.3	0	840
N/A	Multiple (2)	Multiple (3)	200	2012-10-19 02:21:00	Multiple (6)	0	Multiple (3)	0	200
Administrator	Multiple (3)	WindowsAuthServer @ 10.10.50.9	128	2012-10-19 05:09:52	Multiple (2)	0	10.10.50.9	0	117
IUSR_WIN2003STD-R2	Multiple (2)	WindowsAuthServer @ 10.10.100.104	7	2012-10-19 18:38:19	10.10.100.104	0	10.10.100.104	0	7
IUSR_C01	Multiple (3)	WindowsAuthServer @ 10.10.100.102	6	2012-10-19 03:10:32	10.10.100.102	0	10.10.100.102	0	6
news	Session Opened	LinuxServer @ 10.10.100.8	3	2012-10-19 02:40:37	10.10.100.8	0	10.10.100.8	0	3

- 內建各種合規檢查報告
- 可自行拖拉、修改報表樣本
- 報表自動寄送

超過2000種最佳實務報表與規則，滿足各種規範，如COBIT , PCI, SOX, HIPAA, NERC CIP, FISMA , UK GCSx and GLBA..等

事件管理：資安事件的分析、追蹤、管理與舉證

以不同的角度與面向來探勘與追蹤各種資安事件



Offense 3063

Magnitude			Relevance	0	Severity	8	Credibility
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 Illustrates a s... data with IDS alerts An attacker originating from China (202... ng the Conficker worm exploit (CVE 2008-4250). The fir						

Credibility: 3

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		Last Event
Buffer Overflow		8	8	09-29 16:06:33
Misc Exploit		3	3	
Network Sweep		716	1417	

Top 5 Local Targets Targets

IP/DNS Name	Mag...	Vulnerable	Chained	User	MAC	Location	Weight
Windows AD Server		Unknown	No	Unknown	Unknown	main	8
10.101.3.3		Unknown	No	Unknown	Unknown	main	0
10.101.3.4		Unknown	No	Unknown		main	0
DC106		Yes	No	Administrat		main	10
10.101.3.11		Unknown	No	DCAdmin		main	0

Top 10 Events Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm	Misc Exploit	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 :: qrada		10.101.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	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
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	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

什麼樣攻擊或行為

攻擊成功了嗎

什麼人做的

我在那發現他們

涉及多少目標系統

對企業的影響在那裡

是否存在相對弱點？

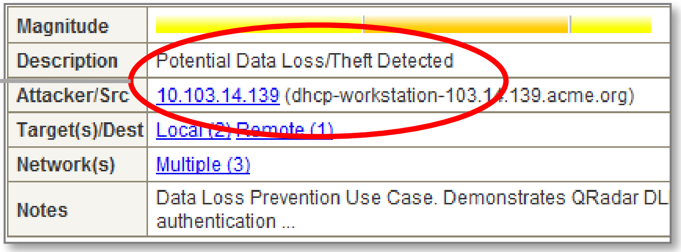
相關聯的證據

Innovate2013
The IBM Technical Summit

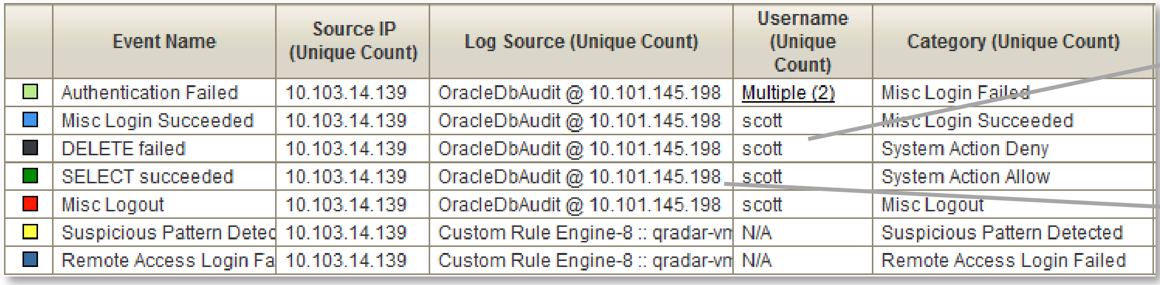
Use case: Detecting Insider Fraud

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 ...



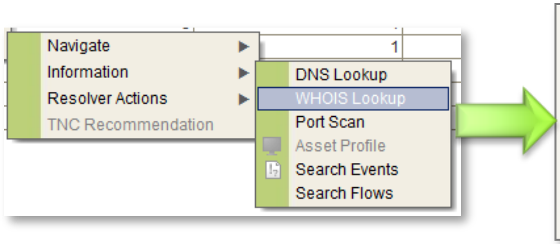
	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
🟩	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
🟦	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded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

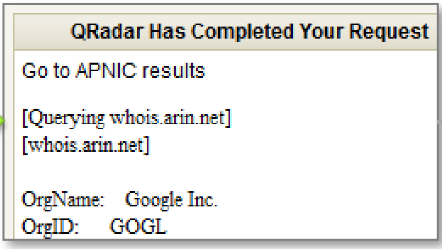
Who?

An internal user

What?

Oracle data





QRadar Has Completed Your Request

Go to APNIC results

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

OrgName:    Google Inc.
OrgID:      GOGL
```

Where?

Gmail

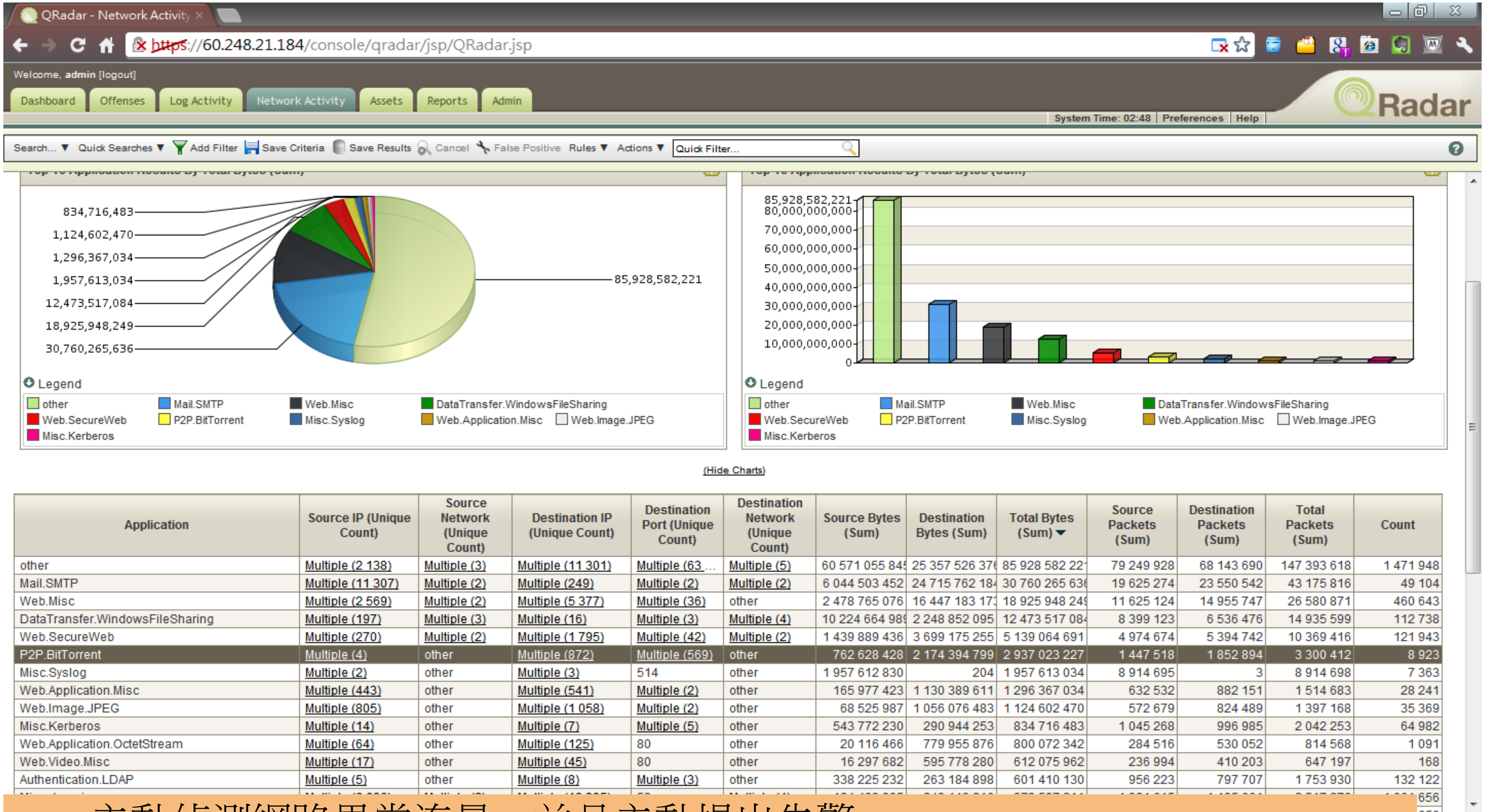
Threat detection in the post-perimeter world

User anomaly detection and application level visibility are critical to identify inside threats

Use Case：網路流量與異常分析 Top application

了解某個使用者的網路活動

Drill-down 網路流量內容-使用P2P.BitTorrent 下載，佔用大量頻寬

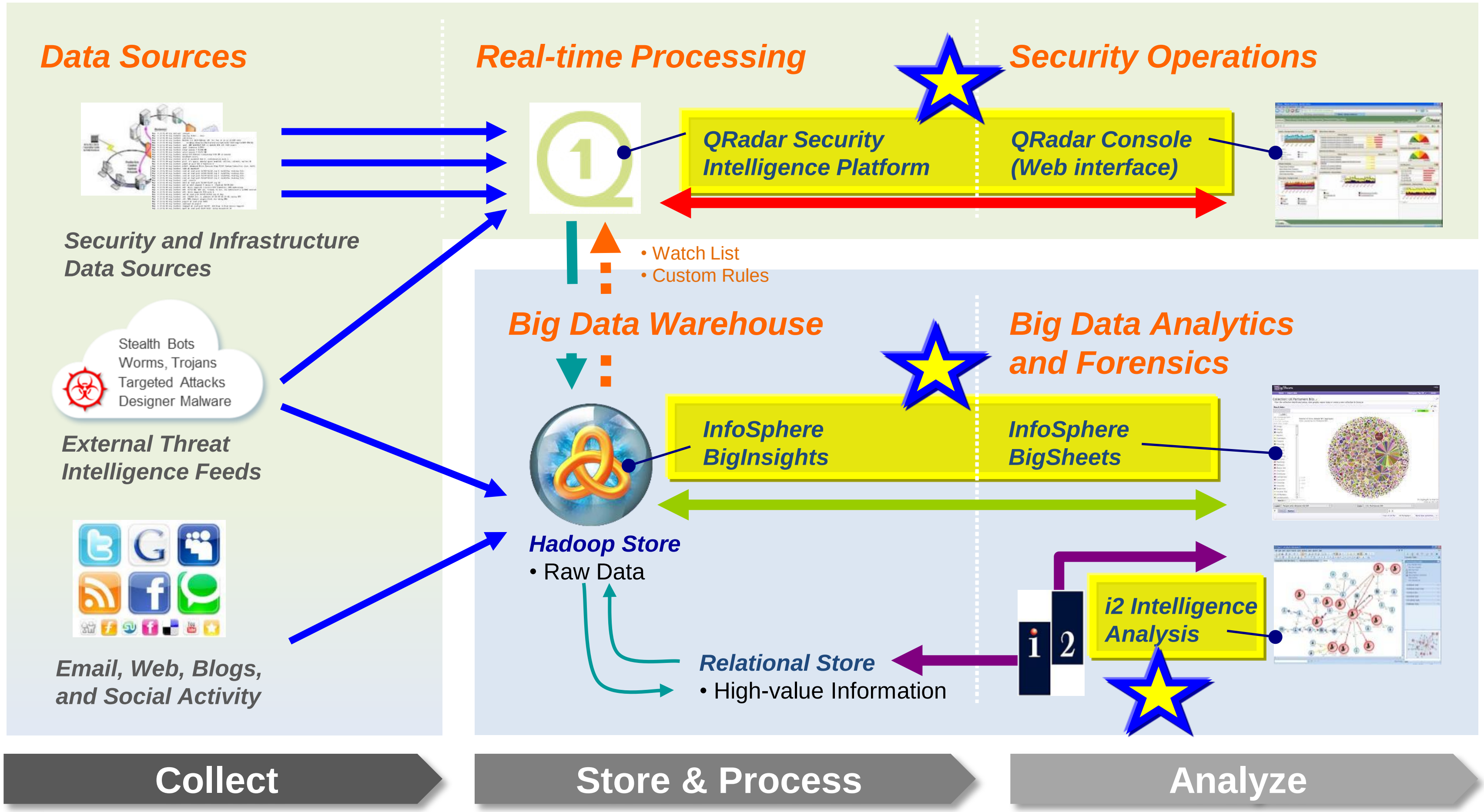


Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum) ▼	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Count
other	Multiple (2 138)	Multiple (3)	Multiple (11 301)	Multiple (63 ...	Multiple (5)	60 571 055 84	25 357 526 37	85 928 582 22	79 249 928	68 143 690	147 393 618	1 471 948
Mail.SMTP	Multiple (11 307)	Multiple (2)	Multiple (249)	Multiple (2)	Multiple (2)	6 044 503 452	24 715 762 18	30 760 265 63	19 625 274	23 550 542	43 175 816	49 104
Web.Misc	Multiple (2 569)	Multiple (2)	Multiple (5 377)	Multiple (36)	other	2 478 765 076	16 447 183 17	18 925 948 24	11 625 124	14 955 747	26 580 871	460 643
DataTransfer.WindowsFileSharing	Multiple (197)	Multiple (3)	Multiple (16)	Multiple (3)	Multiple (4)	10 224 664 98	2 248 852 095	12 473 517 08	8 399 123	6 536 476	14 935 599	112 738
Web.SecureWeb	Multiple (270)	Multiple (2)	Multiple (1 795)	Multiple (42)	Multiple (2)	1 439 889 436	3 699 175 255	5 139 064 691	4 974 674	5 394 742	10 369 416	121 943
P2P.BitTorrent	Multiple (4)	other	Multiple (872)	Multiple (569)	other	762 628 428	2 174 394 799	2 937 023 227	1 447 518	1 852 894	3 300 412	8 923
Misc.Syslog	Multiple (2)	other	Multiple (3)	514	other	1 957 612 830	204	1 957 613 034	8 914 695	3	8 914 698	7 363
Web.Application.Misc	Multiple (443)	other	Multiple (541)	Multiple (2)	other	165 977 423	1 130 389 611	1 296 367 034	632 532	882 151	1 514 683	28 241
Web.Image.JPEG	Multiple (805)	other	Multiple (1 058)	Multiple (2)	other	68 525 987	1 056 076 483	1 124 602 470	572 679	824 489	1 397 168	35 369
Misc.Kerberos	Multiple (14)	other	Multiple (7)	Multiple (5)	other	543 772 230	290 944 253	834 716 483	1 045 268	996 985	2 042 253	64 982
Web.Application.OctetStream	Multiple (64)	other	Multiple (125)	80	other	20 116 466	779 955 876	800 072 342	284 516	530 052	814 568	1 091
Web.Video.Misc	Multiple (17)	other	Multiple (45)	80	other	16 297 682	595 778 280	612 075 962	236 994	410 203	647 197	168
Authentication.LDAP	Multiple (5)	other	Multiple (8)	Multiple (3)	other	338 225 232	263 184 898	601 410 130	956 223	797 707	1 753 930	132 122
												656

- 主動偵測網路異常流量，並且主動提出告警。
- 針對佔據頻寬前十名應用程式進行排名與統計，快速分析頻寬使用狀況。

Big Data 也可提供豐富的內容來讓SIEM Rule 更完整

Big Data Security Solution – components in Yellow



Data Sources

Security and Infrastructure Data Sources

Stealth Bots
Worms, Trojans
Targeted Attacks
Designer Malware

External Threat Intelligence Feeds

Email, Web, Blogs, and Social Activity

Real-time Processing

QRadar Security Intelligence Platform

Security Operations

QRadar Console (Web interface)

- Watch List
- Custom Rules

Big Data Warehouse

Hadoop Store
- Raw Data

Relational Store
- High-value Information

Big Data Analytics and Forensics

InfoSphere BigInsights

InfoSphere BigSheets

i2 Intelligence Analysis

Collect

Store & Process

Analyze

Where IBM stands (IBM Security)

Figure 1. Magic Quadrant for Security Information and Event Management

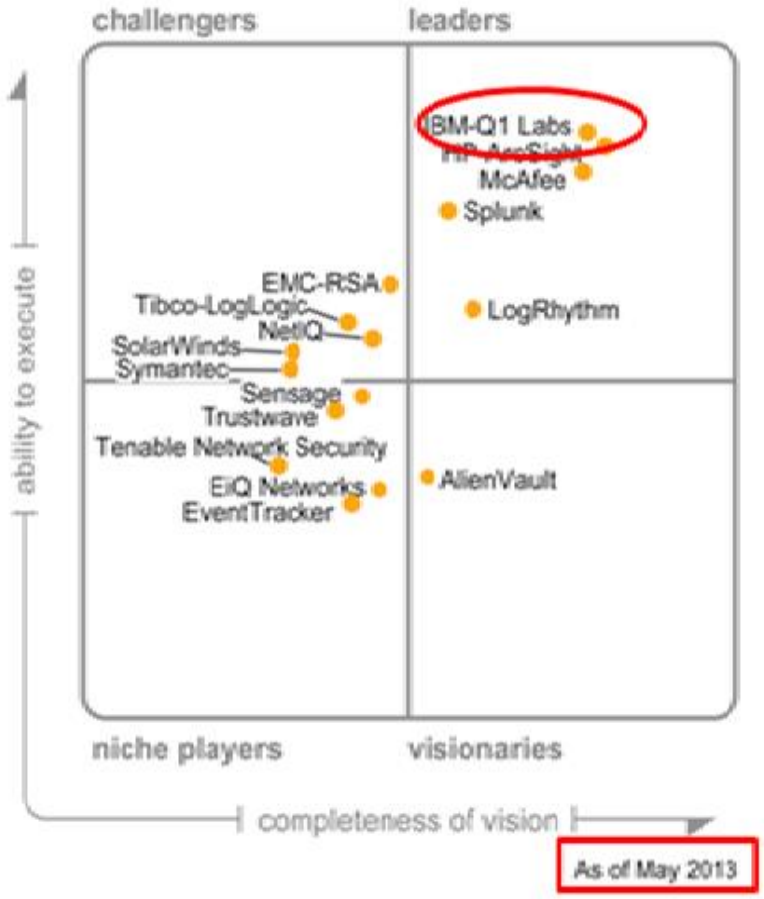
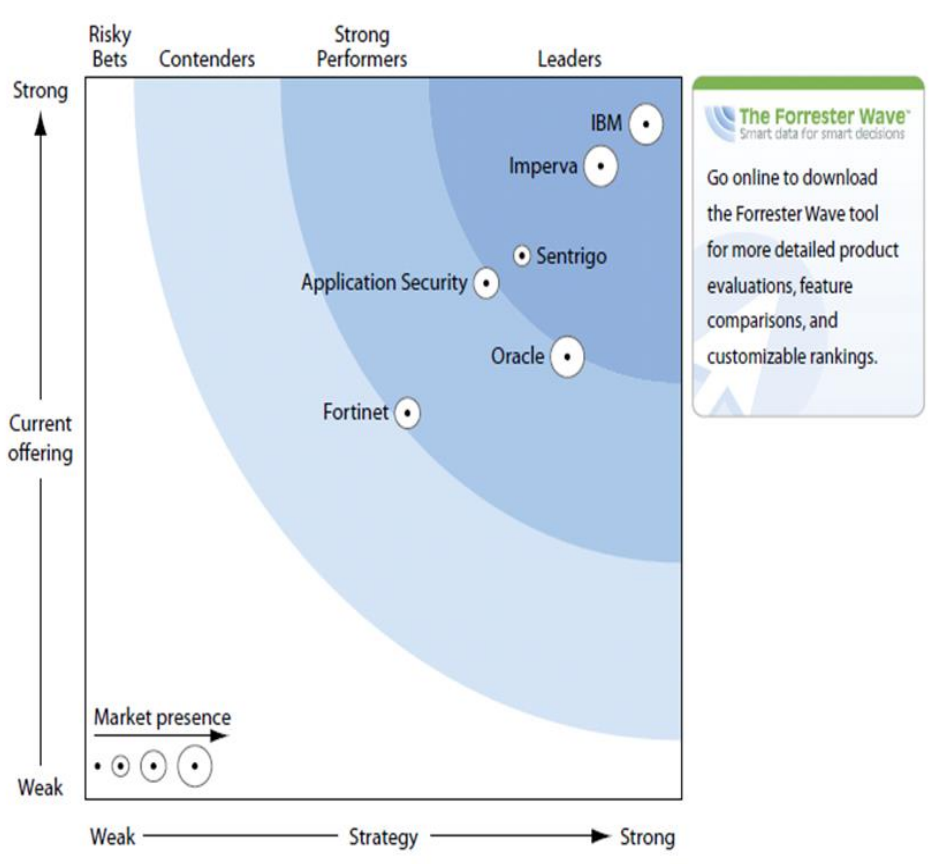


Figure 2 Forrester Wave™: Database Auditing And Real-Time Protection, Q2 '11



Source: Forrester Research, Inc.

ibm.com/security

© Copyright IBM Corporation 2012. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.