2012 IBM軟體用戶大會

史上最強王牌組合

智慧、行動、安全應用，出奇制勝新格局

鬼牌殺手-技高一籌的資安防護術
超完美智慧資安秘技，嚴防內神通外鬼

廖宗文

Senior I/T Specialist

IBM Software Tivoli

IBM

議程

- IBM資安框架
- 資安管理現況
- 現有資安管理的解決方式
- 所衍生及面臨到的問題
- 次世代的資安管理的新思維
- 實施的考量
- 次世代資安管理功能

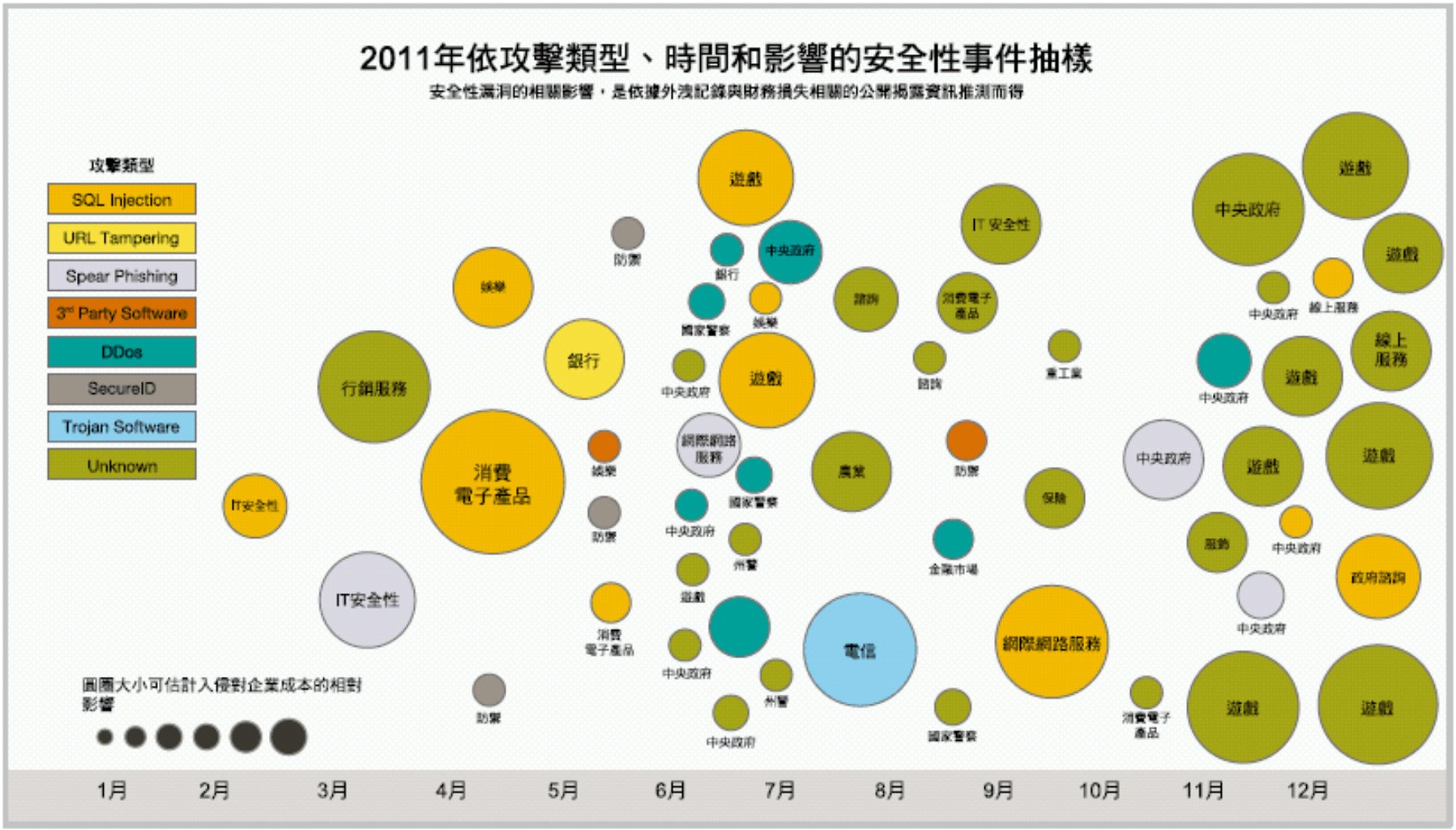
9.是否使用自動識別設備，以鑑別來自特定地點或設備之連線?
10.對於異常登入程序，是否留有紀錄，並有專人定期檢視
11.是否訂定行動式電腦設備之管理政策

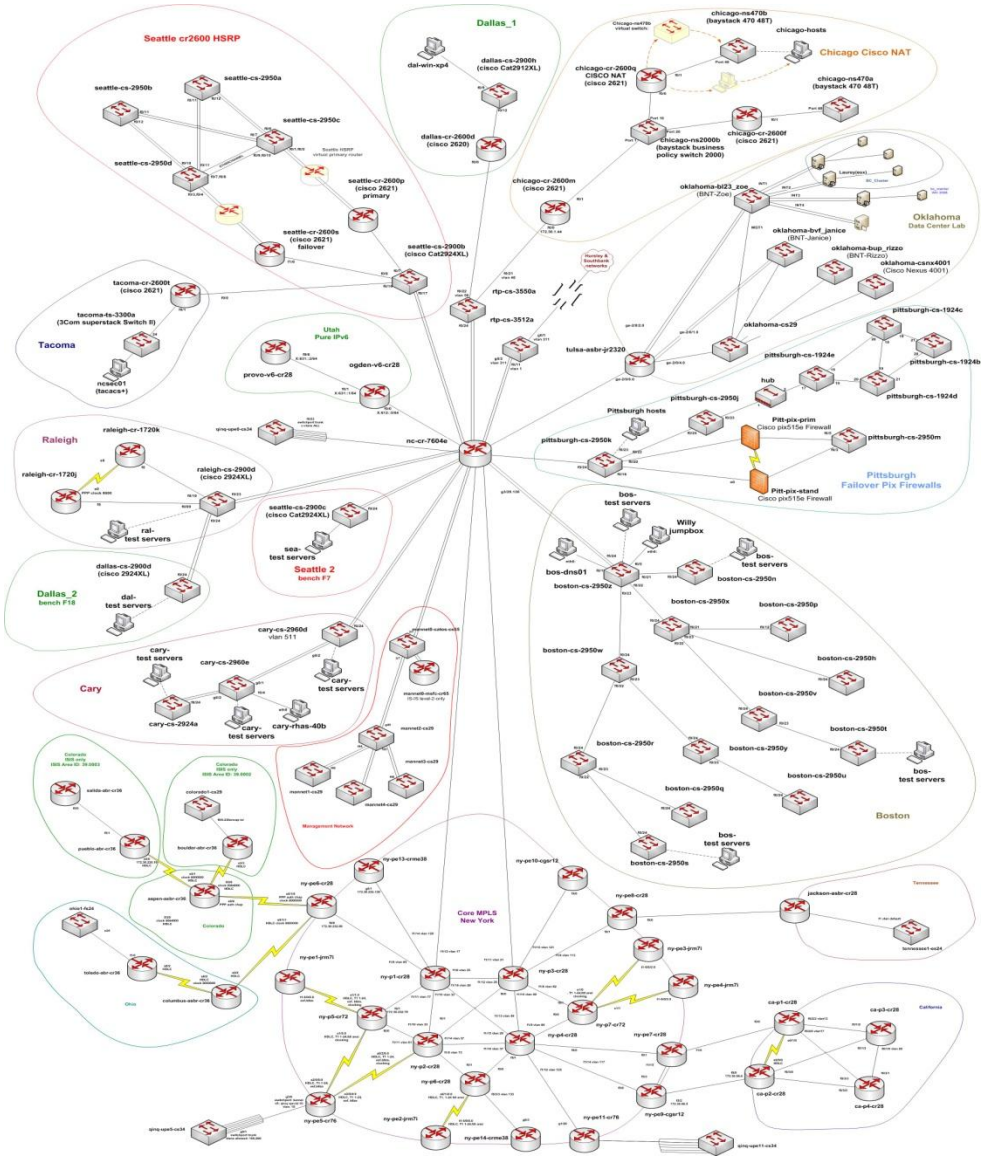
1.是否有監視設備或其他可偵測未經授權使用的設備，以防止資訊設施被不當使用?
2.組織中對於所經管或處理之資訊，涉有個人隱私及個人資料之保護是否有妥適之保護機制？
3.機密性、敏感性資料之存取、變更、訂正是否有進行監控並進行完整的軌跡紀錄？
4.是否留有詳細的管理者與操作員之作業日誌？
5.是否建立各項監控系統之使用程序並定期審查監控？
6.對於非法或異常登錄、使用資訊系統之行為是否具有警示及阻斷之措施？

10.對高敏感性的資料在傳輸或儲存中是否使用加密技術？
12.原始程式庫之存取行為，是否留有稽核日誌?
13.測試作業是否避免以真實資料進行？
14.委外開發之系統上線前是否偵測有無惡意程式？
15.稽核時時所揭示之機敏資訊是否進行不可識別性之處理？
16.稽核時的存取行為是否作監控與並留有記錄？
17可攜式的電腦設備是否訂有嚴謹的保護及監控措施？
18.內外部郵件往來是否有適當的郵件稽核制度

1.是否定期對電腦系統及資料儲存媒體進行弱點掃描？
2.資訊系統是否定期進行安全技術符合性的檢查(如滲透測試或系統弱點檢測)
3.是否定期與適時檢測網路運作環境之安全漏洞？

1.組織內資訊設備之存取軌跡是否依法進行紀錄及保存？
2.組織重要紀錄(如資料庫紀錄、系統日誌、操作日誌、稽核日誌)是否依安全等級加以保護儲存(如檔案加密或數位簽章)?
4.資安事件日誌之記錄內容是否包括使用者識別碼、登入登出之日期時間、電腦的識別資料或其網址、事件描述及矯正措施等事項
5.資安事件中相關證據資料是否有適當保護措施?以作為問題分析及法律必要依據。


2011年依攻擊類型、時間和影響的安全性事件抽樣
安全性漏洞的相關影響，是依據外洩記錄與財務損失相關的公開揭露資訊推測而得
攻擊類型
SQL Injection
URL Tampering
Spear Phishing
3rd Party Software
DDos
SecureID
Trojan Software
Unknown
圓圈大小可估計入侵對企業成本的相對影響
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月
遊戲
中央政府
IT安全性
消費電子產品
行銷服務
銀行
娛樂
防禦
國家警察
諮詢
農業
電信
網際網路服務
保險
州警
企業市場
線上服務
政府諮詢



複雜的IT環境，需要太多的資安工具來作防護，資安的管理將會是現在式。

- 如何有效的管理
- 資安訊息的收集
- 資安有效訊息的萃取
- 實時資安告警產生
- 提供實用的報告


安全性
智慧
安全性智慧：
資訊及事件管理
進階關聯性與深度分析
外部威脅研究
最佳化
角色式分析
身分識別管理
權限使用控制
資料流程分析
資料管理
安全性應用程式
處理程序
詐欺偵測
進階網路監控
鑑識/資料探勘
安全性豐富的系統
精通
使用者分配
存取管理
強式驗證
資料庫弱點監控
存取監控
資料遺失防止
應用程式防火牆
原始碼掃描
虛擬安全性
資產管理
端點/網路安全性
基本
集中式目錄
加密
存取控制
應用程式掃描
週邊安全性
防毒
人
資料
應用程式
基礎設施

允許企業組織改善監控、分析與活動的自動化作業

操作人員：
自動部署

分析：
自動排列優先順序

稽核人員：
自動報告

主管：
節省成本

監控

- 自動探索記錄來源
- 自動探索應用程式
- 自動探索資產
- 資產自動分組
- 集中化的記錄管理
- 自動化的配置稽核

分析

- 自動調整
- 自動偵測威脅
- 數千項預先定義的規則
- 容易使用的事件篩選
- 進階的安全性鑑識

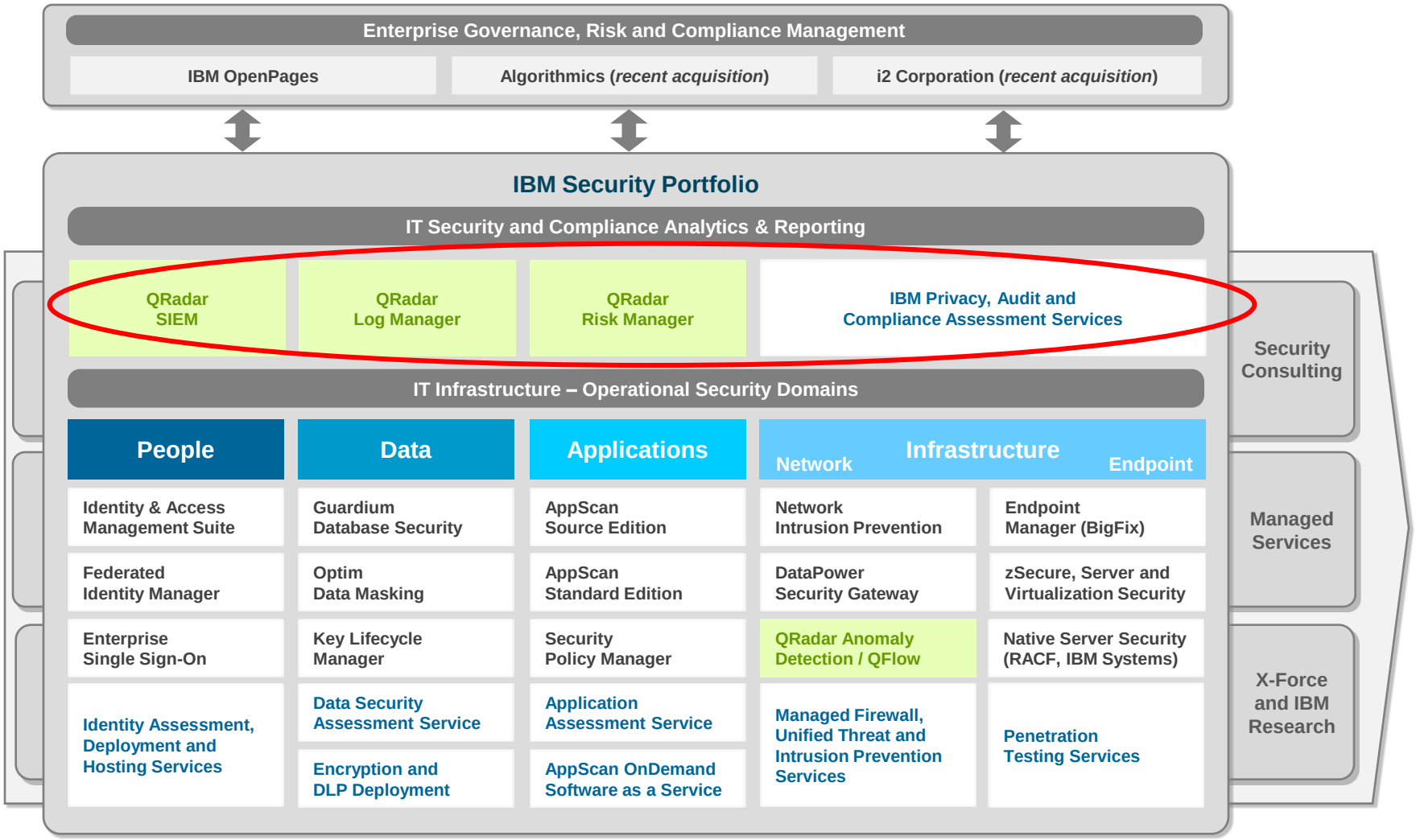
活動

- 數千個預先定義的報告
- 根據資產排列優先順序
- 自動更新威脅
- 自動回應
- 定向修復

IBM 資訊安全性架構


管理、風險與法規遵循
安全性智慧與分析
人
資料
應用程式
基礎設施
進階安全性與威脅研究
專業服務
雲端及管理的服務
軟體及裝置

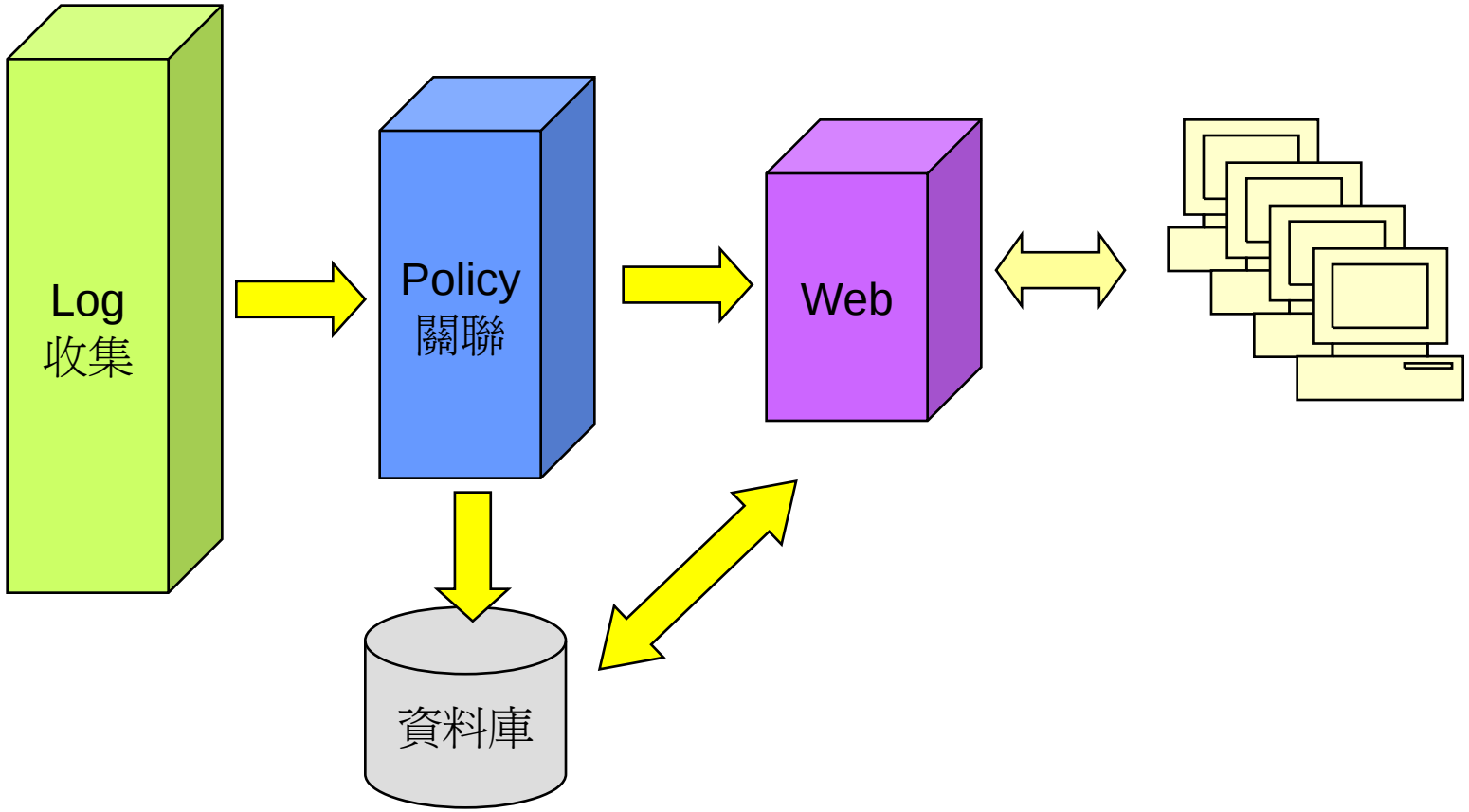
IBM 資通安全對應機制



資安管理現況

- 網際網路的方便，駭客攻擊層出不窮
- 內部資安的管控不易
- 太多不同種類資安設備，管理繁雜且不易
- 資安資料的收集，面臨到複雜環境，廣泛收集方式，及時呈現需求
- 事件處理及時性的需求
- 符規管理完整性的需求
- 面對資安海量的訊息，如何達到最有效告警。
- 在有限的人力下，達到預期的效果。

現有資安管理的解決方式



所衍生及面臨到的問題

- 不同資安設備整合的問題
- 擴容的問題
- 未來性 – 新資安設備整合的問題
- SIEM與其他系統整合的問題
- 實施上的問題
- 考量是否有資安技術支援及訊息更新

次世代的資安管理的新思維

- 智能化
  - 廣泛的資安事件收集，正規化，關聯處理
  - 網路的預警機制
- 整合性
  - 擴容升級的解決方案
  - 統一管控單一管理畫面，整合其他系統
  - 居高彈性，確保未來資安設備的整合
- 自動化
  - 部署簡易
  - 快速成效
  - 維運高效

何為智能化

Security Intelligence

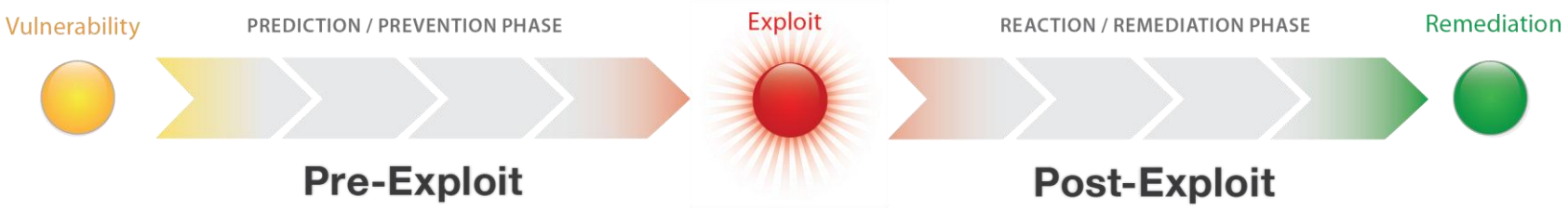
--noun

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

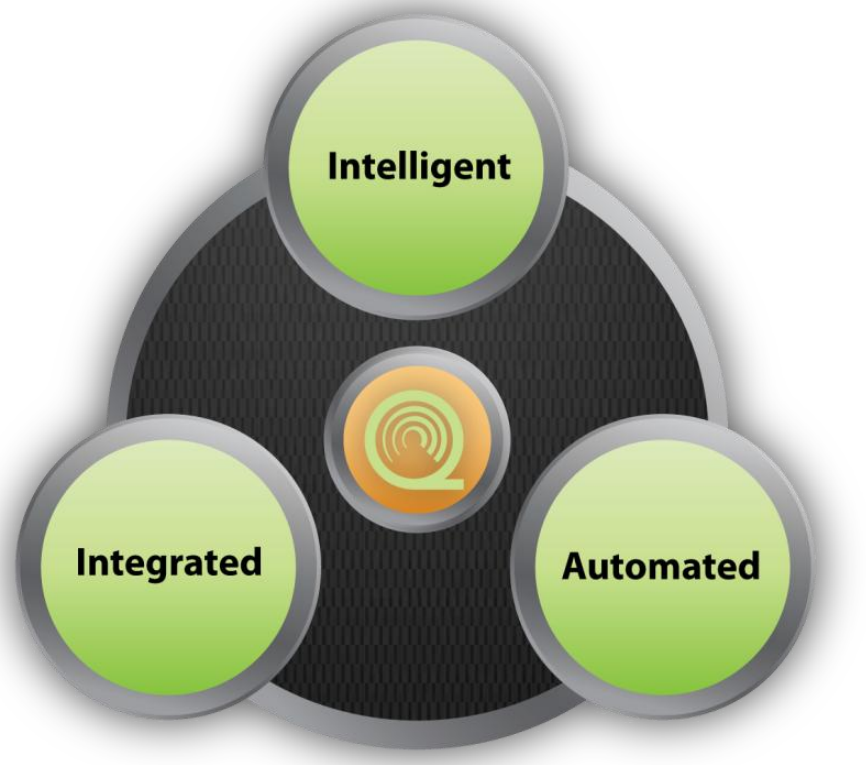
Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

智能化的解決方案

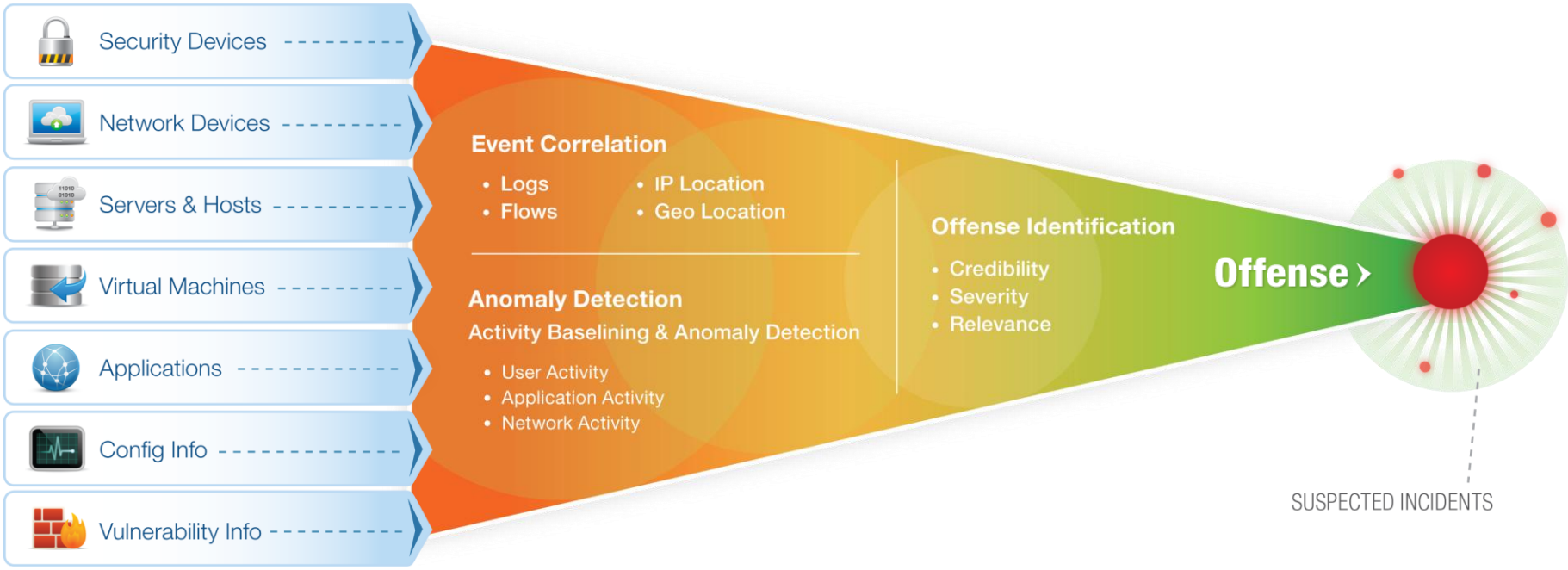

What are the external / internal threats?
Are we configured to protect against these threats?
What is happening right now?
What is the impact?


Vulnerability
PREDICTION / PREVENTION PHASE
Exploit
REACTION / REMEDIATION PHASE
Remediation
Pre-Exploit
Risk Management • Compliance Management
Vulnerability Management • Configuration Monitoring
Post-Exploit
SIEM • Network Behavior Anomaly Detection
Log Management • Data Loss Capture
Packet Forensics • Remediation • Dashboards

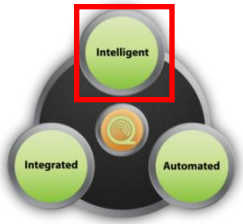
資安管理平臺特性—智能，整合，自動



智能化:
深入內容監控及關聯

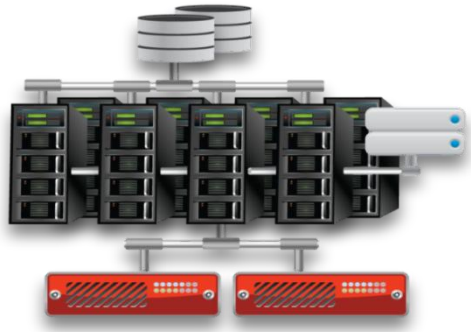


Most Sources + Most Intelligence = Most Accurate & Actionable Insight



整合性：
簡單的擴容及建置操作

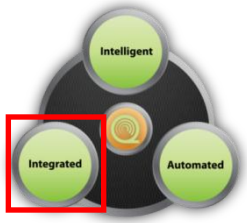
Bolted Together Solution



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

QRadar Integrated Solution

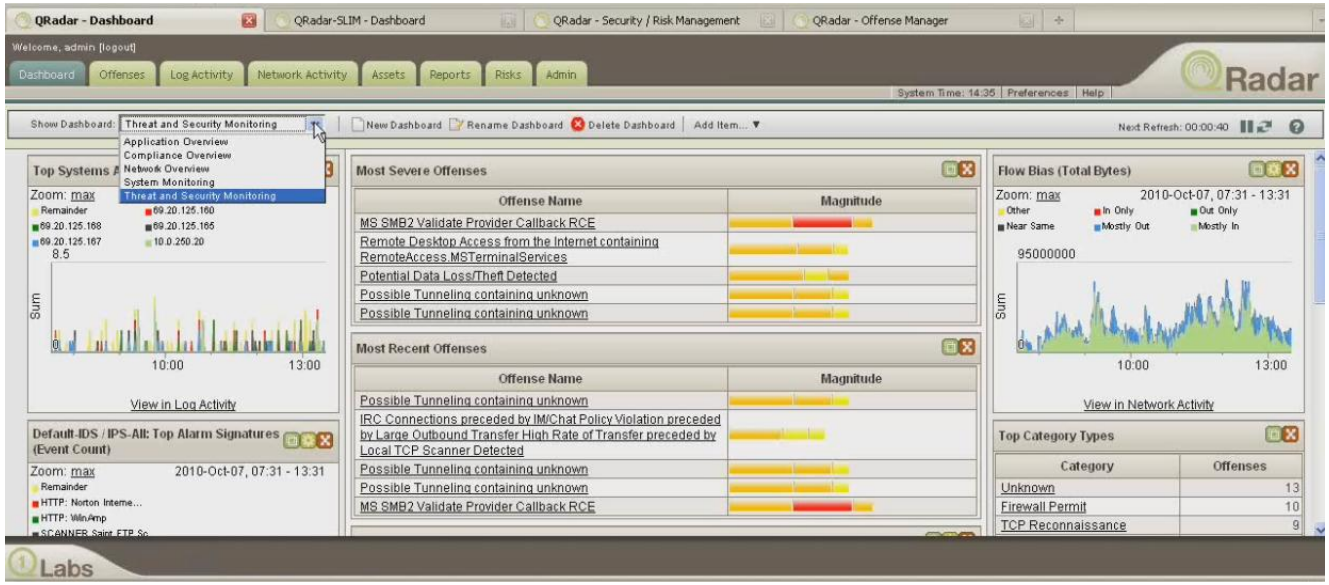
- Highly scalable
- Common reporting & searching
- Distributed correlation
- Unified administration
- Logs stored once
  - ***Total visibility***



單一智能性的完全整合資安訊息呈現

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

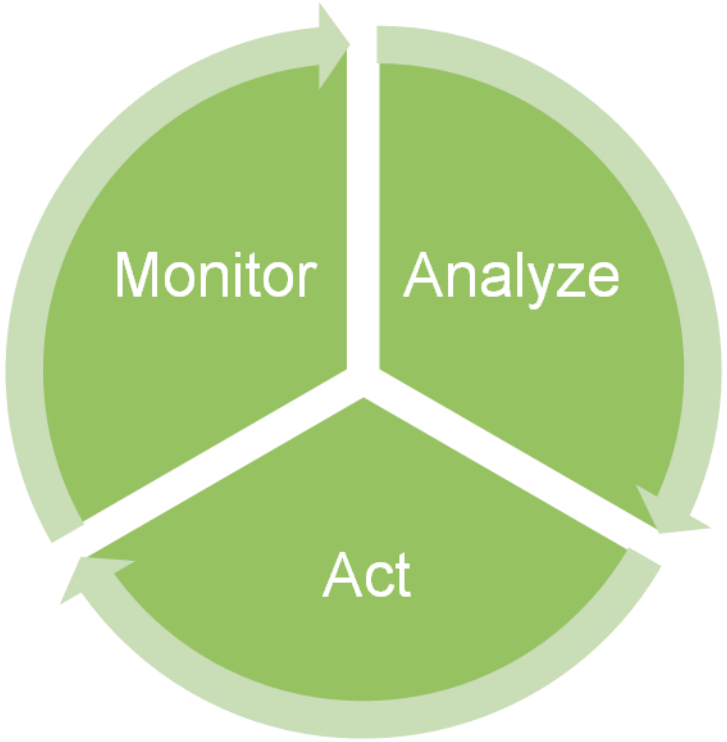
One Console Security



Built on a Single Data Architecture

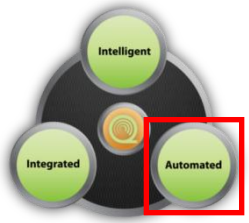
自動化:
沒有額外的客製

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



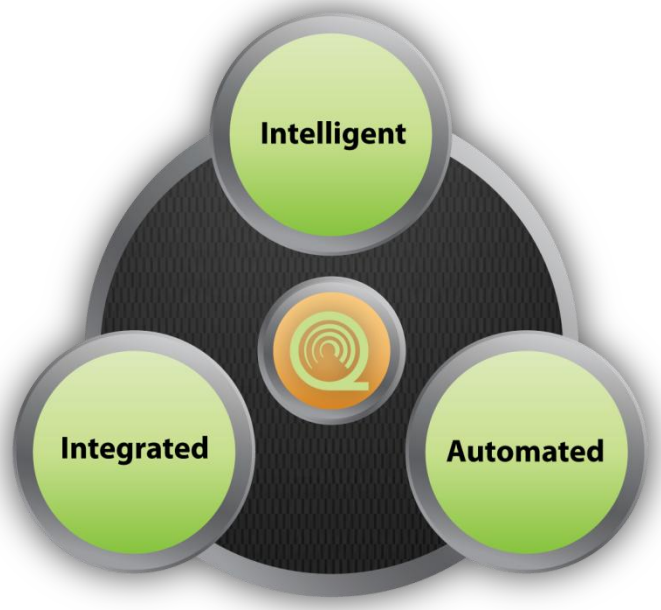
- Asset-based prioritization
- Auto-update of threats
- Auto-response
- Directed remediation

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



資安管理平臺特性—智能，整合，自動

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



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

- Easy deployment
- Rapid time to value
- Operational efficiency

案例：複雜的威脅分析

問題陳述

- 搜尋資料如同大海撈針
- 跨資安設備的海量資料比對攻擊模式
- 對被攻擊目標的資產價值及相關資產，需要有優先告警級別區分
- 了解威脅的影響

焦點分析

- 正規化事件
- 資產訊息
- 弱點內容
- 網路監控

案例：複雜的威脅分析

Offense 3063 Summary | Attackers | Targets | Categories | Annotations | Networks | Events

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

案例：詐欺和資料外泄防護

問題陳述

- 驗證資安監控對應符規的要求
- 確保符規目標符合資安的目的
- 日誌本身不符合符規標準

焦點分析

- 應用層可視性
- 有問題網段的可視性

Potential Data Loss?

Who? What? Where?

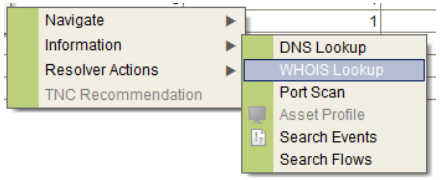
Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

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]

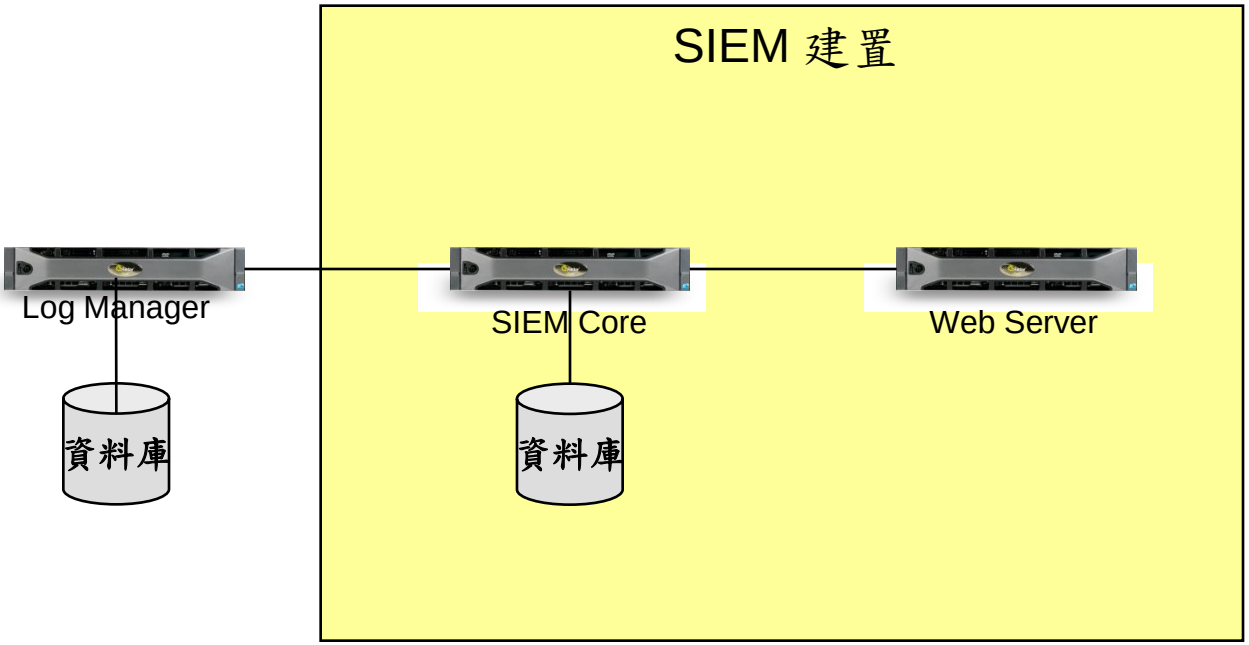
OrgName: Google Inc.
OrgID: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View

Where?
Gmail

實施的考量

- 如何逐步實施
  - Log Management
  - SIEM
- 升級建置時的考量
  - Log Management與SIEM平臺的整合
  - 因擴容及效能所延伸的問題
  - 操作及維護的問題

現有客戶面臨升級的情況



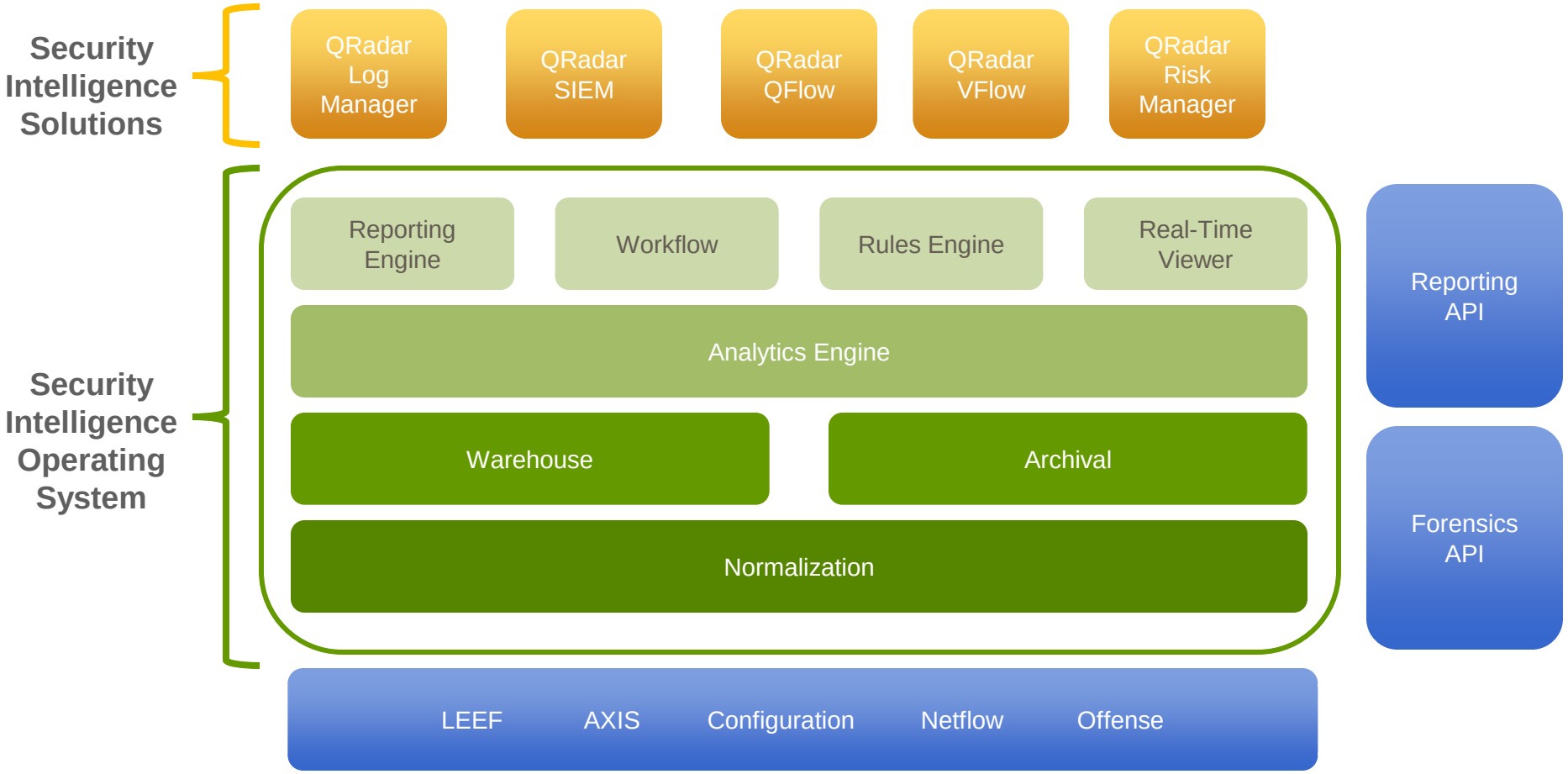
Sizing，Project Planning，
Deployment，Test，On line

升級至SIEM，需要化較多的資源及時間，曠日費時

逐步計劃，無痛升級

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

QRadar 產品線:
建置在共同的功能平臺

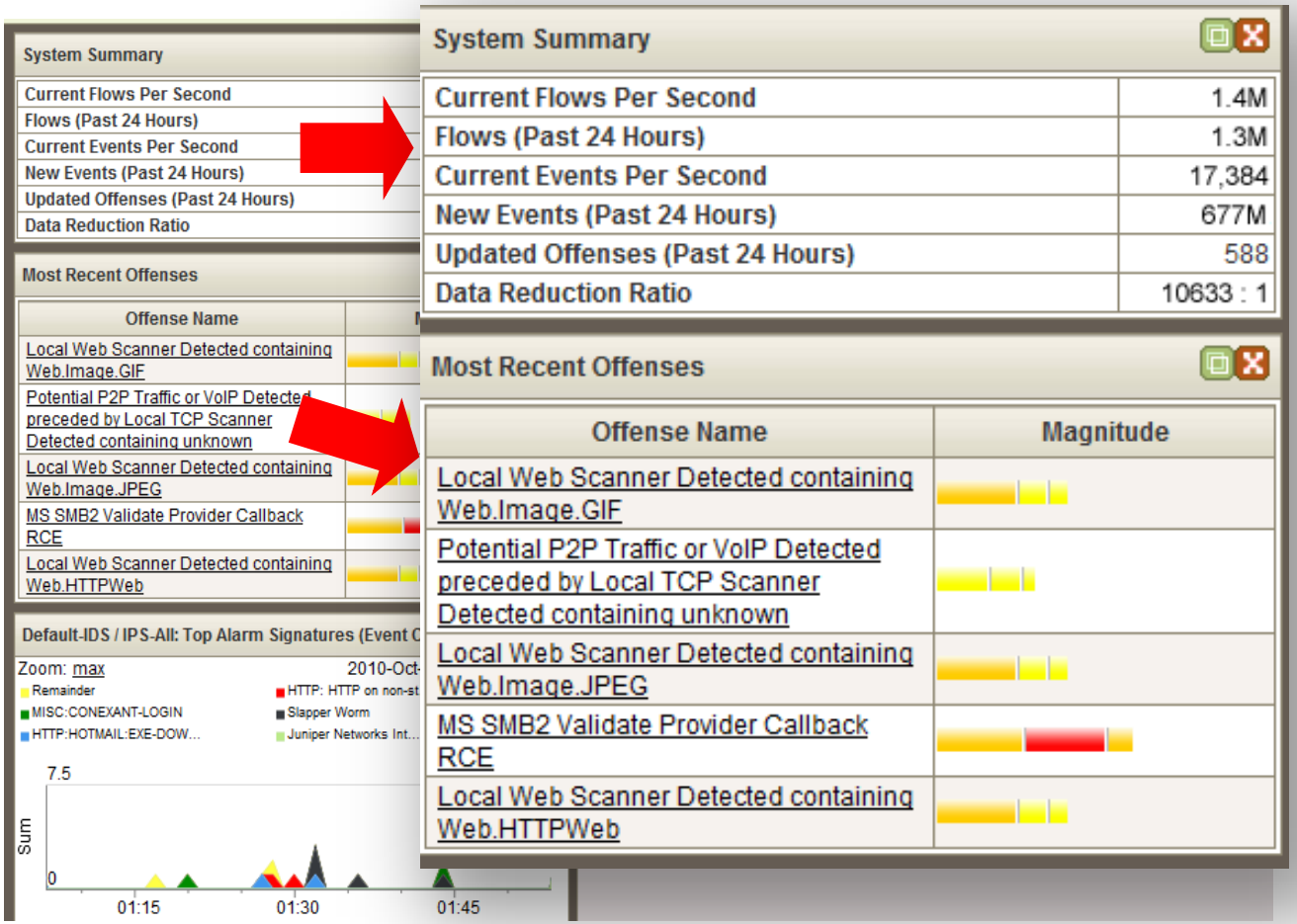


Intelligent, Integrated, Automated – One Console Security

SIEM
整合界面

- Single browser-based UI
- Role-based access to information & functions
- Customizable dashboards (work spaces) per user
- Real-time & historical visibility and reporting
- Advanced data mining and drill down
- Easy to use rules engine with out-of-the-box security intelligence

SIEM
資料精簡和資安事件優先化（Prioritization）



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

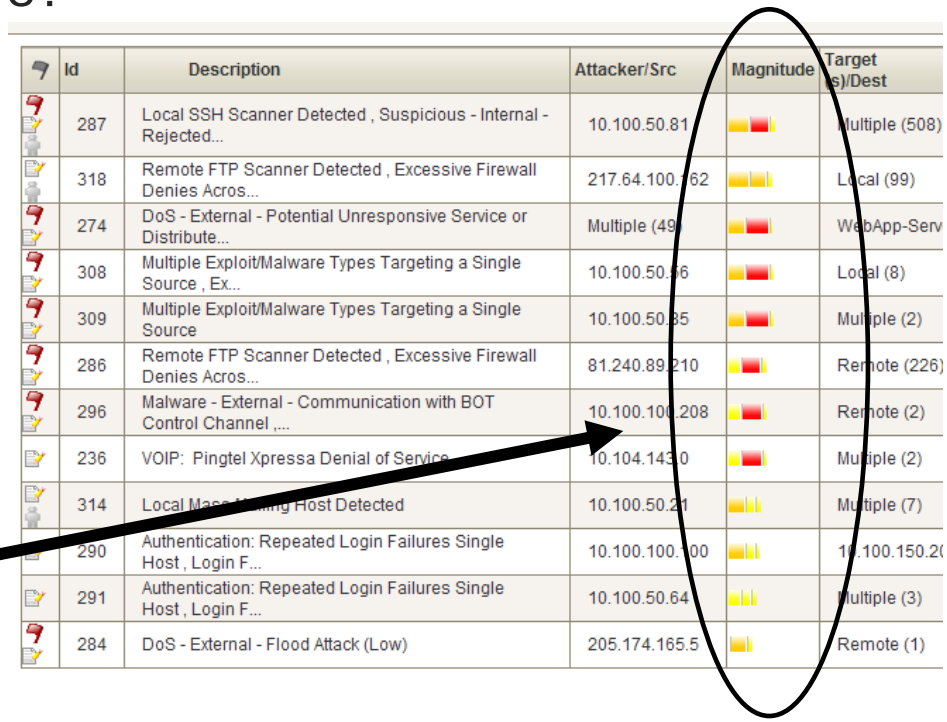
Offenses are further prioritized by business impact

SIEM
智能防禦儀表板

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

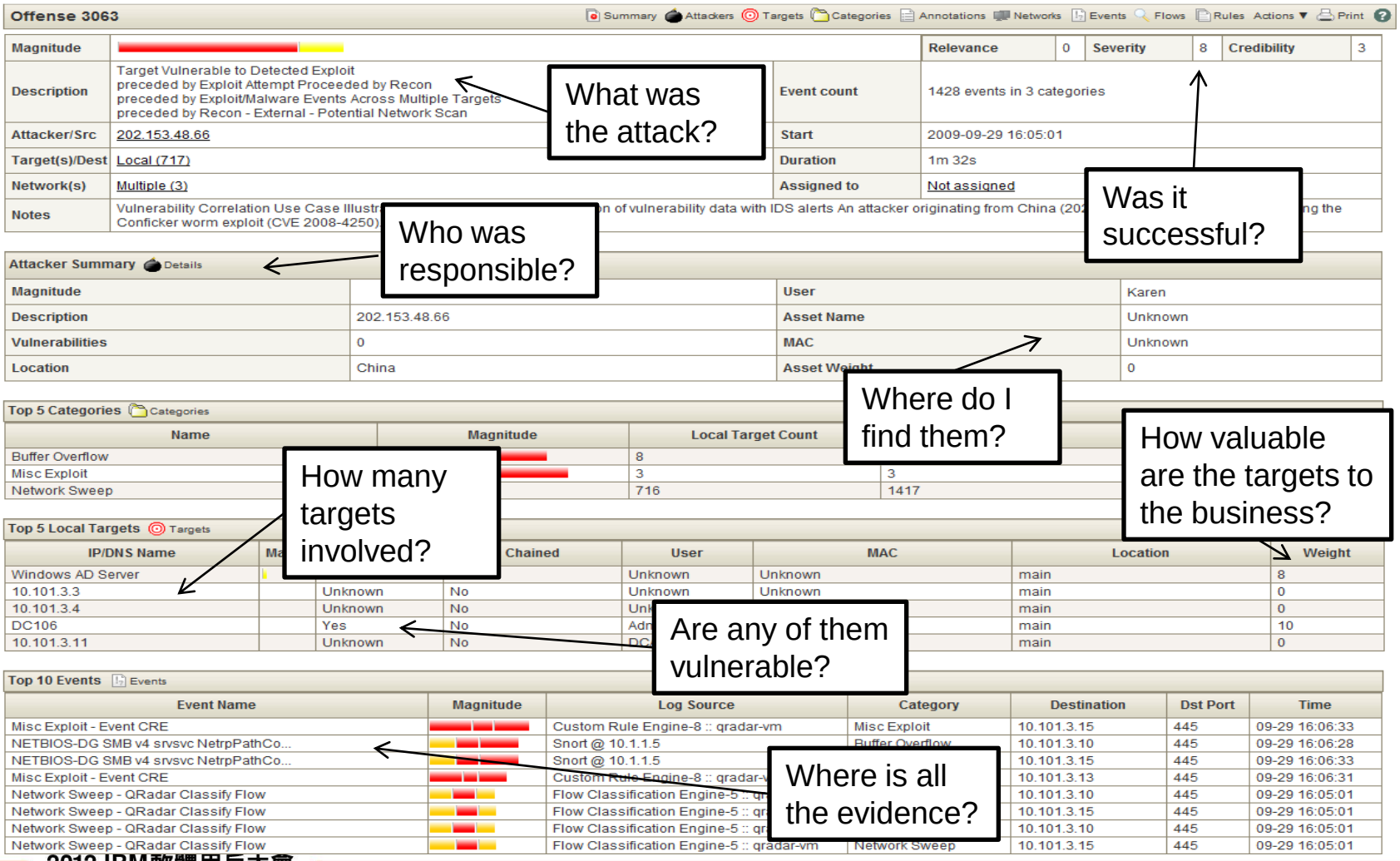
Priorities can change over time based on situational awareness



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...	10.100.50.66		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 [illegible] Host Detected	10.100.50.21		Multiple (7)
290	Authentication: Repeated Login Failures Single Host , Login F...	10.100.100.100		10.100.150.20
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)

SIEM
防護管理訊息

Clear, concise and comprehensive delivery of relevant information:



SIEM
規則及搜尋功能

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

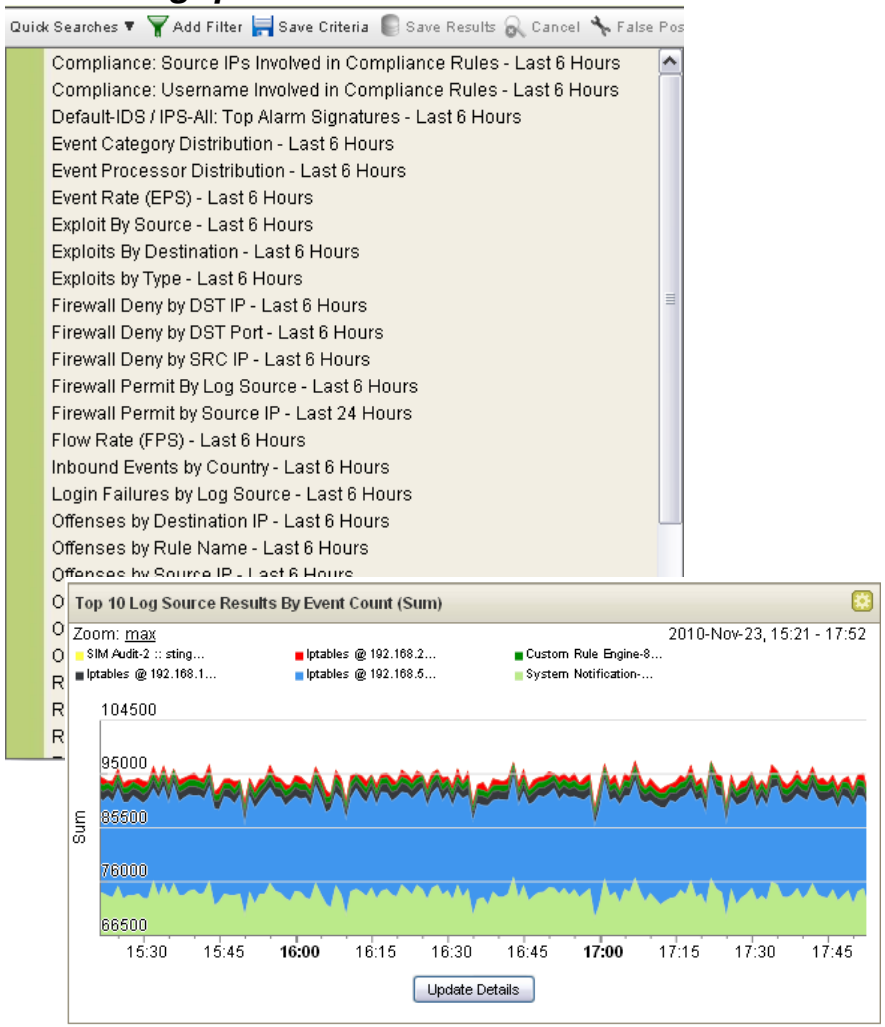
100’s of out-of-the-box searches and views of network activity and log data

- Provides quick access to critical information

Custom log fields

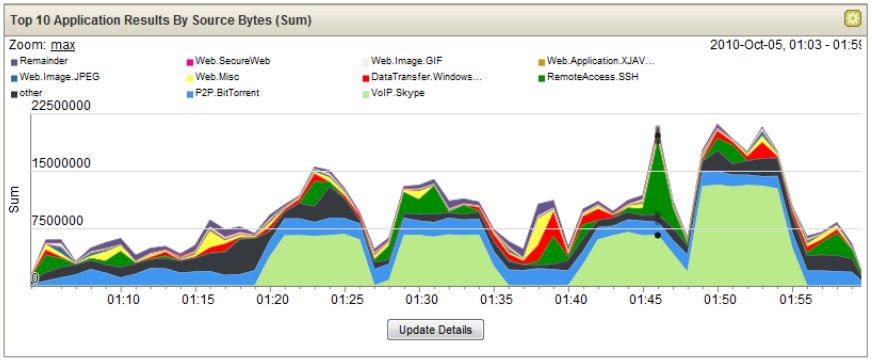
- Provides flexibility to extract log data for searching, reporting and dashboards. Product ships with dozens of pre-defined fields for common devices.

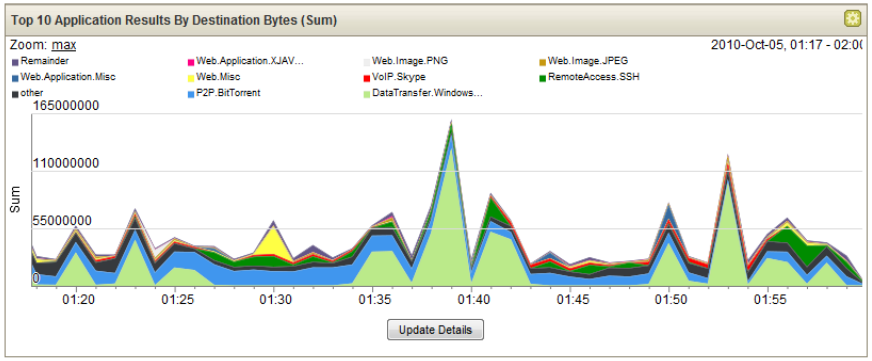
Default log queries/views



SIEM
網路流量智能管理

- 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)





(Hide Charts)

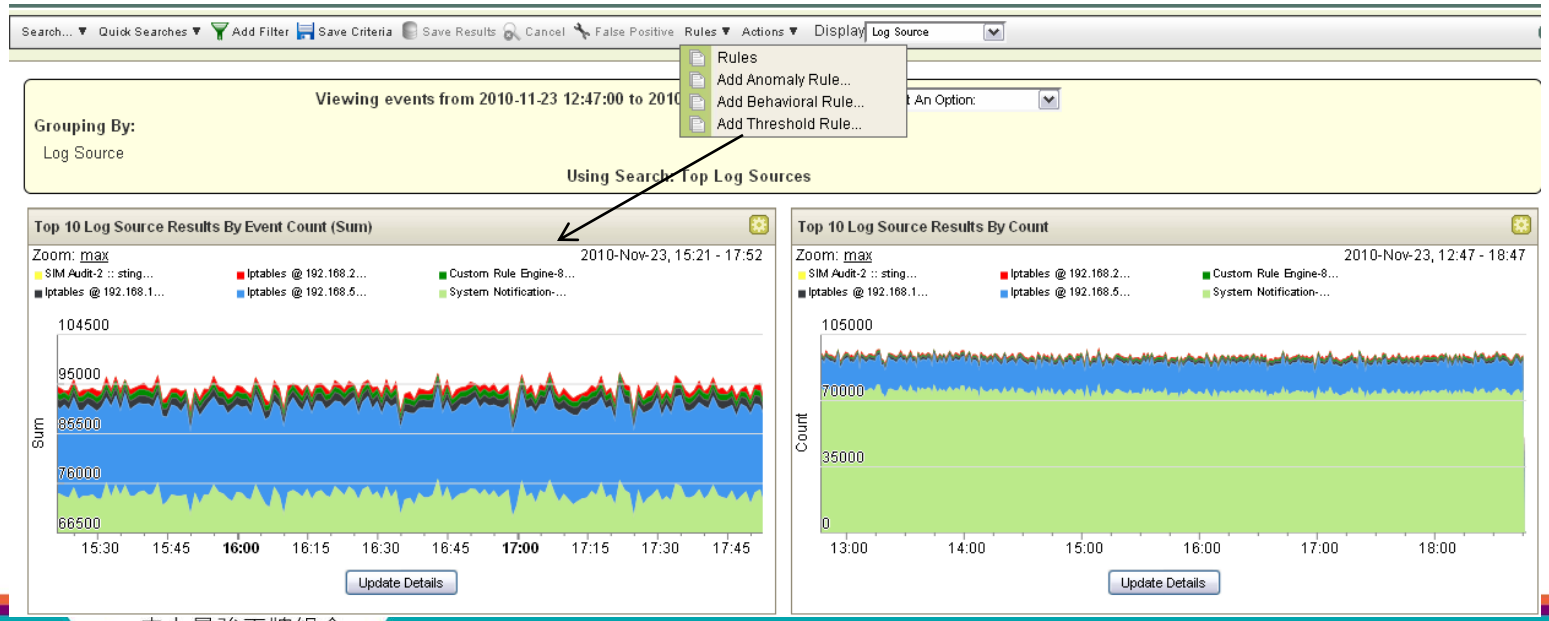
Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Count
DataTransfer.Window	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	266 544	9 127 364	9 393 908	4 194	6 930	11 014	761

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

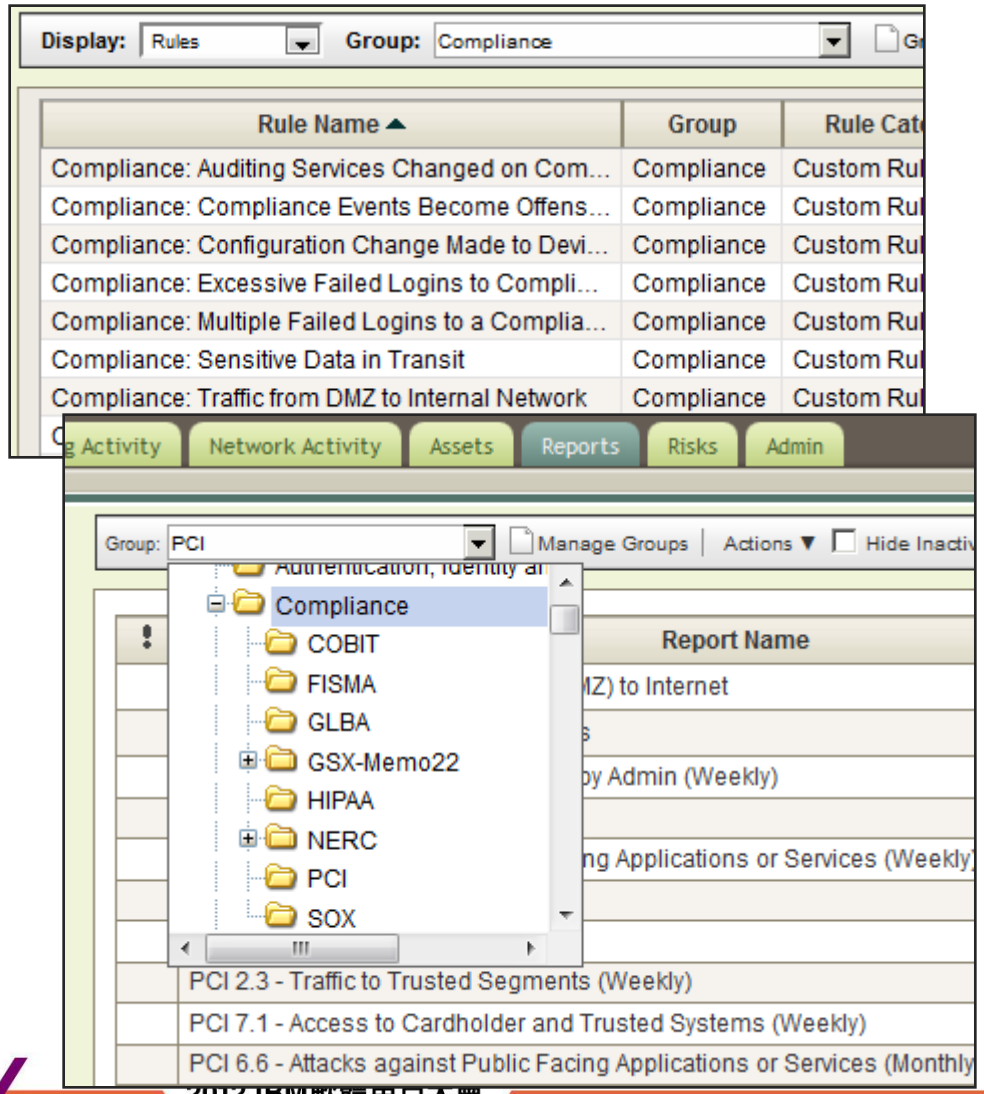
Page: 1 Go < 1 | 2

SIEM
網路流量上AP分析

- 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



SIEM
合規管理：規則及報表



- 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


Thank
You