ANTICIPATE

Secure the Next 2016

F5加乘IBM 全面洞察安全危機

Alfred Horng
Senior Consultant
IBM Security

F5加乘IBM, 強化網路安全防禦性

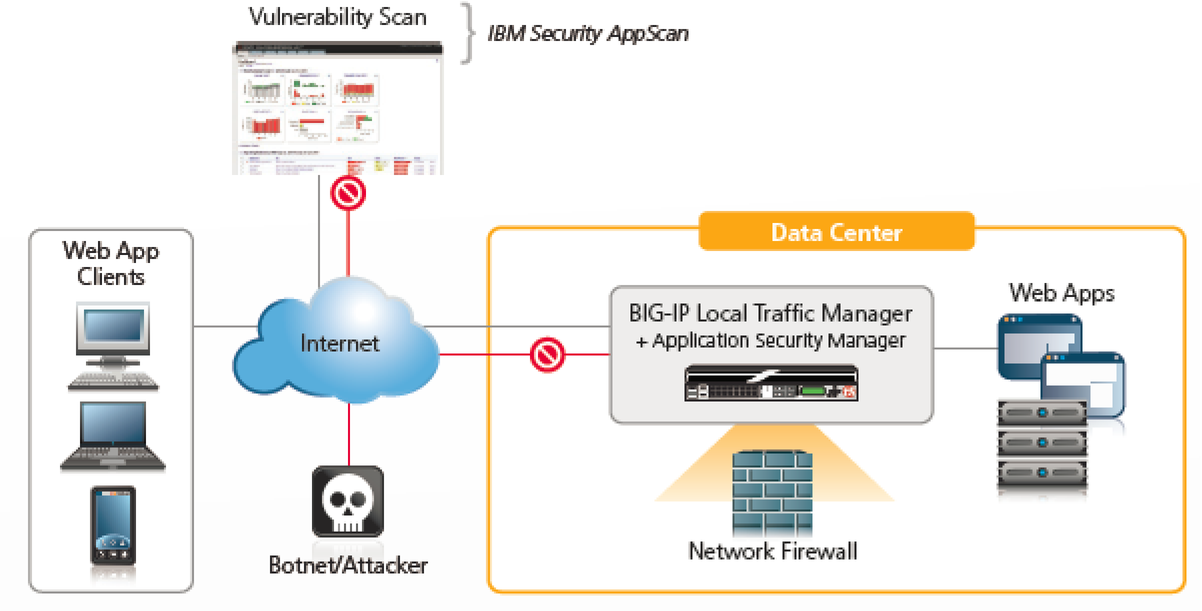
Agenda:

- F5與IBM Security的整合實例
- 對抗安全威脅應該合縱連橫，協同防禦
- F5 與 QRadar 整合實例
- 透過X-Force智慧情報提供即時的威脅情報
- F5 BIG-IP ASM與Guardium的整合

F5 / IBM Solutions for The co-operative bank

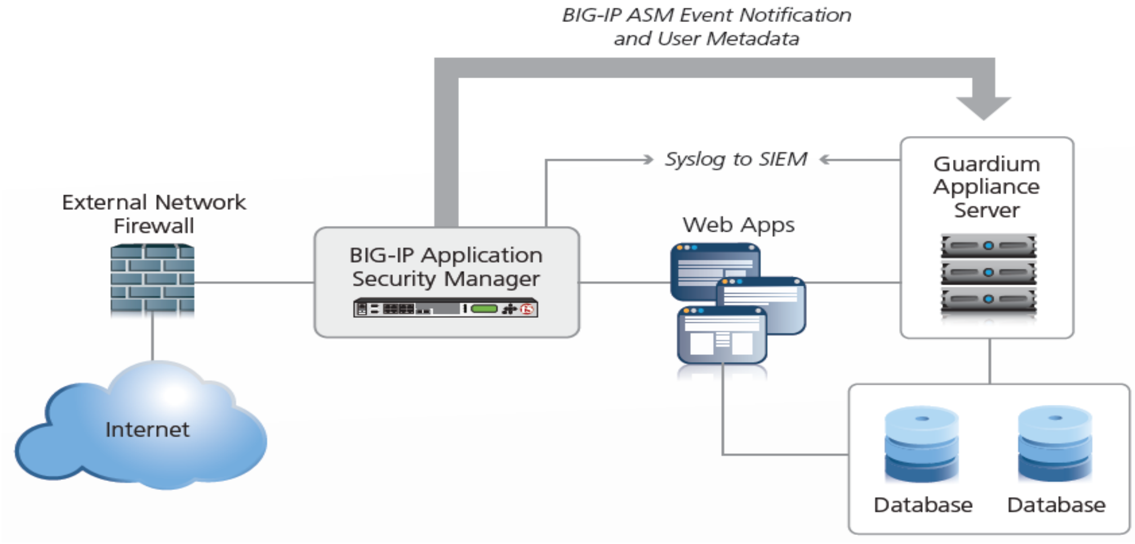
Value for Application Security

- AppScan Interactive Application Security Testing
  - Web application threat and vulnerability assessment tool
  - – AppScan assessment reports can be directly imported into ASM to quickly and easily deploy policies to mitigate vulnerabilities until the application can be patched



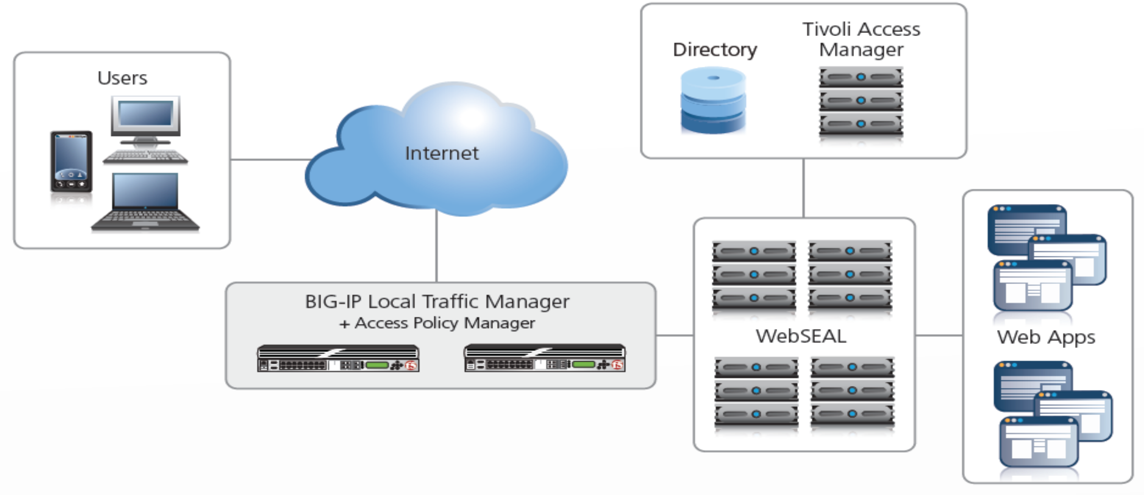
Value for Database Activity Monitor

- Guardium
  - Defense in-depth with layered security at the web application and database tiers
  - Richer forensic data logs through correlating user metadata for SQL injection attacks
  - Consolidated reporting for streamlined compliance and audit
  - High availability of Guardium S-TAP Collectors


BIG-IP ASM Event Notification and User Metadata
Syslog to SIEM
Guardium Appliance Server
External Network Firewall
BIG-IP Application Security Manager
Web Apps
Internet
Database
Database

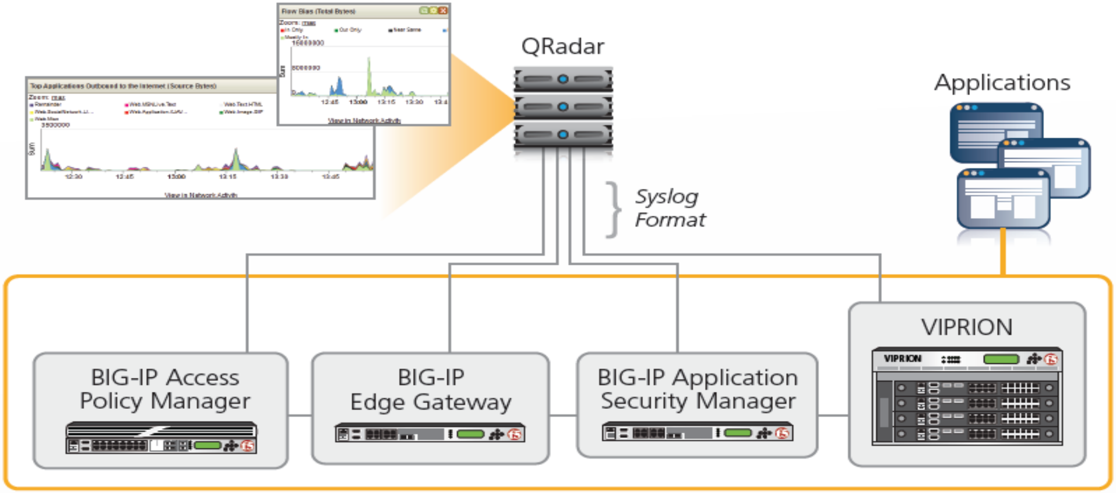
Value for Access Management

- Security Access Manager
  - High availability and scalability of IBM Security Access Manager (formerly Tivoli Access Manager) WebSeal policy enforcement point agents
  - Secure web access with SSL-VPN connection and endpoint security policy enforcement
  - Single sign-on

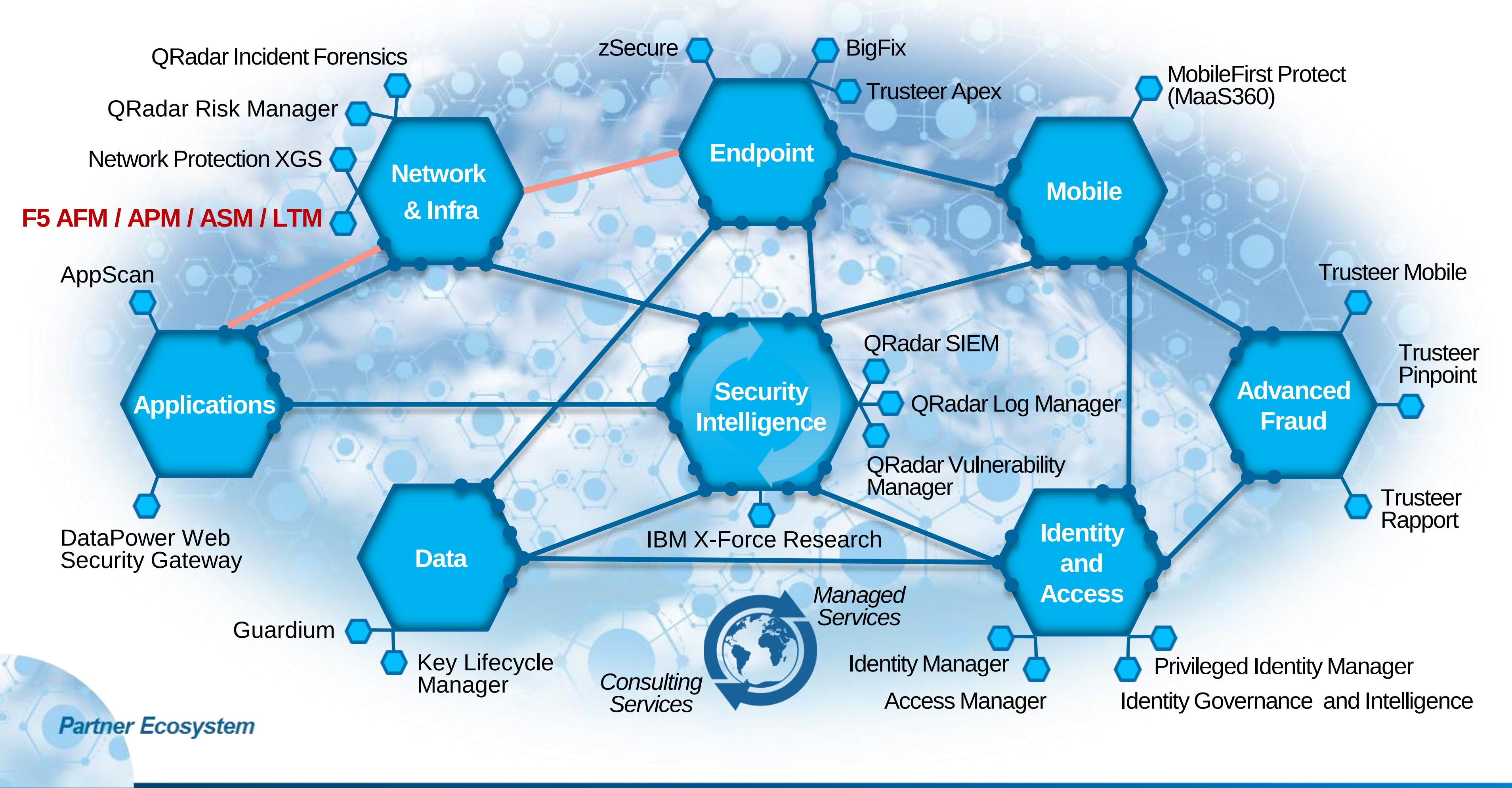


Value for Security Intelligence

- QRadar
  - Increased visibility into application and traffic events by pulling data from BIG-IP into the QRadar SIEM via syslog
  - Lower security compliance and management costs
  - Enhanced security posture analysis
  - Enhanced scalability and availability through syslog load balancing


QRadar
Applications
Syslog Format
VIPRION
BIG-IP Access Policy Manager
BIG-IP Edge Gateway
BIG-IP Application Security Manager

IBM 提供企業最完整與最深入的資安解決方案



IBM QRadar 提供全面的風險與事件調查與分析能力

涵蓋了資安維運的事前、事中及事後各階段

- 有那些內部和外部的威脅？
- 目前配置，是否可以防止這些威脅？
- 目前發現了那些安全事件？
- 該事件會造成什麼影響？

弱點　Prediction/Prevention　攻擊　Reaction/Remediation　補救

Risk Management, Compliance Management,
Vulnerability Management, Configuration Management

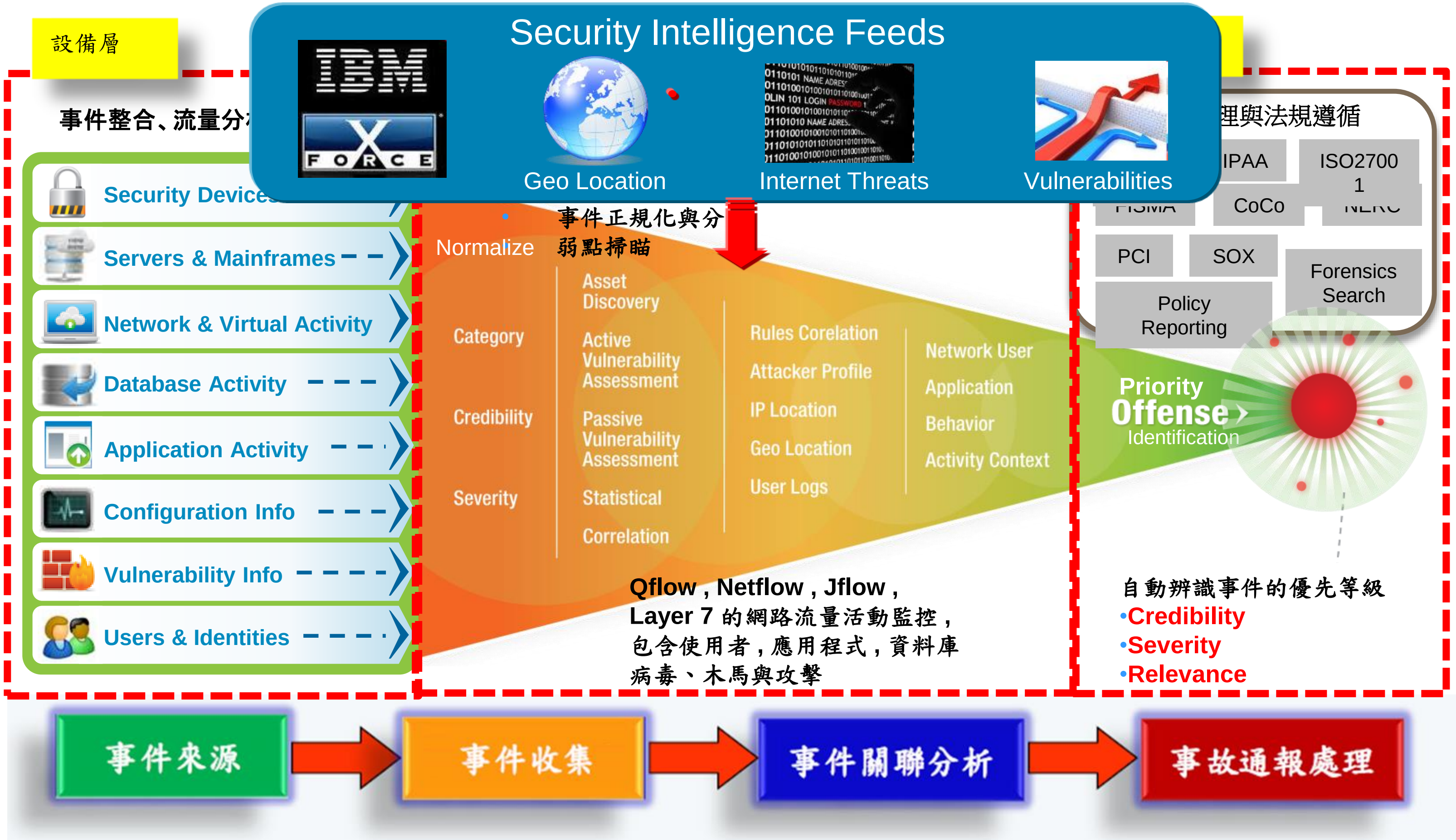
Log Management, SIEM, Incident Management
Network & Application Anomaly Detection.

積極的風險管理

風險管理 → 弱點管理 → 配置管理 → 事件管理 → 可視化管理

利用全方位的安全智能，掌控全局

收集Network Devices、Security Devices、OS、 Applications…等的日誌， 結合網路流量分析，
自動將安全事件關聯起來，進行行為分析、內文比對，並產生各種合規報表，並隨時反映在儀表板上



設備層

事件整合、流量分

Security Intelligence Feeds

Geo Location

Internet Threats

Vulnerabilities

Security Device

Servers & Mainframes

Network & Virtual Activity

Database Activity

Application Activity

Configuration Info

Vulnerability Info

Users & Identities

事件正規化與分

弱點掃瞄

Normalize

Category

Credibility

Severity

Asset Discovery

Active Vulnerability Assessment

Passive Vulnerability Assessment

Statistical

Correlation

Rules Corelation

Attacker Profile

IP Location

Geo Location

User Logs

Network User

Application

Behavior

Activity Context

理與法規遵循

IPAA

ISO2700 1

FISMA

CoCo

NERC

PCI

SOX

Forensics Search

Policy Reporting

Priority Offense Identification

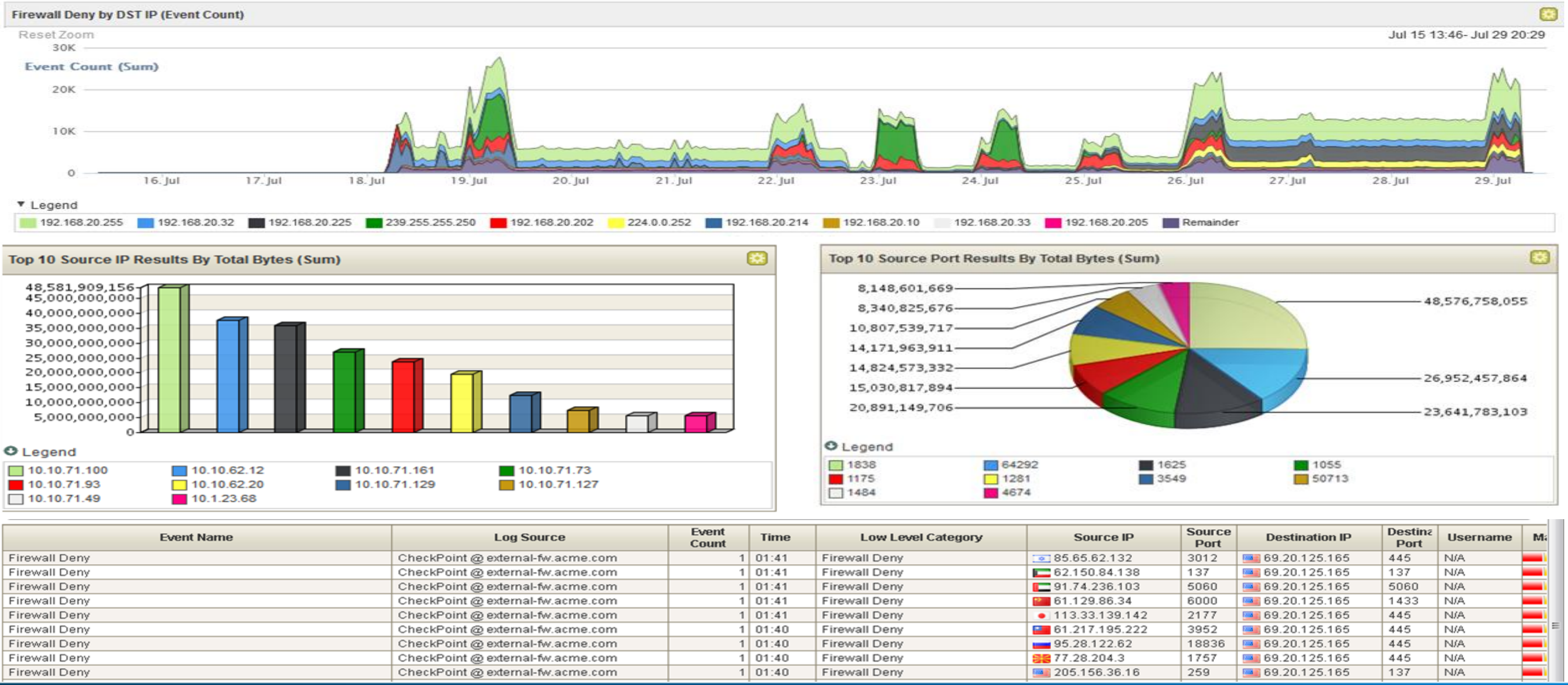
Qflow , Netflow , Jflow ,
Layer 7 的網路流量活動監控，
包含使用者，應用程式，資料庫
病毒、木馬與攻擊

自動辨識事件的優先等級
- Credibility
- Severity
- Relevance

事件來源 → 事件收集 → 事件關聯分析 → 事故通報處理

IBM QRadar 日誌管理平台

1. 日誌欄位正規化與分類，並可彈性擴充，IP 會自動顯示來源國家
2. 提供各種不同面向的趨勢圖、長條圖及圓餅圖供統計分析

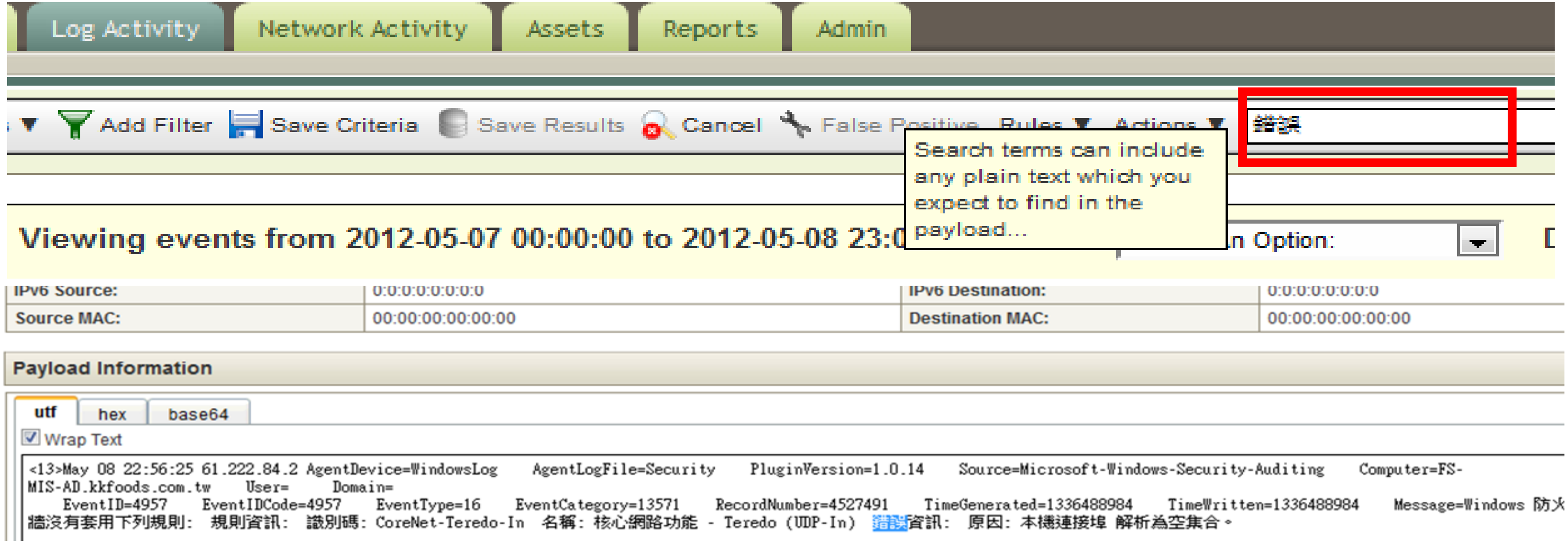


Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Ma
Firewall Deny	CheckPoint @ external-fw.acme.com	1	01:41	Firewall Deny	85.65.62.132	3012	69.20.125.165	445	N/A	
Firewall Deny	CheckPoint @ external-fw.acme.com	1	01:41	Firewall Deny	62.150.84.138	137	69.20.125.165	137	N/A	
Firewall Deny	CheckPoint @ external-fw.acme.com	1	01:41	Firewall Deny	91.74.236.103	5060	69.20.125.165	5060	N/A	
Firewall Deny	CheckPoint @ external-fw.acme.com	1	01:41	Firewall Deny	61.129.86.34	6000	69.20.125.165	1433	N/A	
Firewall Deny	CheckPoint @ external-fw.acme.com	1	01:41	Firewall Deny	113.33.139.142	2177	69.20.125.165	445	N/A	
Firewall Deny	CheckPoint @ external-fw.acme.com	1	01:40	Firewall Deny	61.217.195.222	3952	69.20.125.165	445	N/A	
Firewall Deny	CheckPoint @ external-fw.acme.com	1	01:40	Firewall Deny	95.28.122.62	18836	69.20.125.165	445	N/A	
Firewall Deny	CheckPoint @ external-fw.acme.com	1	01:40	Firewall Deny	77.28.204.3	1757	69.20.125.165	445	N/A	
Firewall Deny	CheckPoint @ external-fw.acme.com	1	01:40	Firewall Deny	205.156.36.16	259	69.20.125.165	137	N/A	

© 2016 IBM Corporation

搜尋引擎 (Search Engine)

使用關鍵字，可快速搜尋
1 .任何欄位與內容
2.原始日誌內容
找出安全或有問題的事件，並可設成即時告警的條件



Viewing events from 2012-05-07 00:00:00 to 2012-05-08 23:0

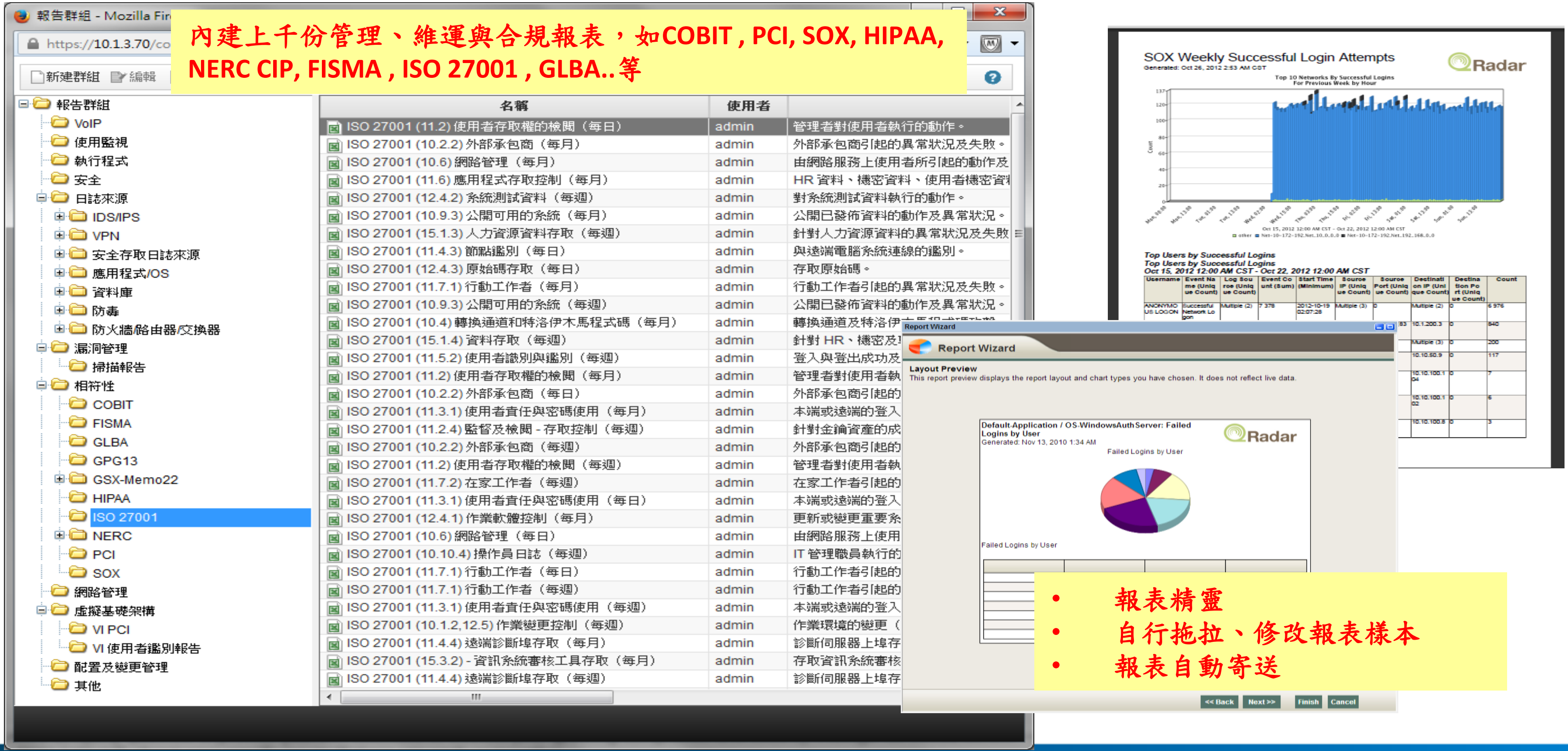
IPv6 Source:	0:0:0:0:0:0:0:0	IPv6 Destination:	0:0:0:0:0:0:0:0
Source MAC:	00:00:00:00:00:00	Destination MAC:	00:00:00:00:00:00

Payload Information

```
<13>May 08 22:56:25 61.222.84.2 AgentDevice=WindowsLog    AgentLogFile=Security    PluginVersion=1.0.14    Source=Microsoft-Windows-Security-Auditing    Computer=FS-
MIS-AD.kkfoods.com.tw    User=    Domain=
    EventID=4957    EventIDCode=4957    EventType=16    EventCategory=13571    RecordNumber=4527491    TimeGenerated=1336488984    TimeWritten=1336488984    Message=Windows 防火
牆沒有套用下列規則: 規則資訊: 識別碼: CoreNet-Teredo-In 名稱: 核心網路功能 - Teredo (UDP-In) 錯誤資訊: 原因: 本機連接埠 解析為空集合。
```

自動化合規分析檢查與報表功能

內建(Built-In) 超過2000種最佳實務報表與規則，滿足各種規範:



名稱	使用者	
ISO 27001 (11.2) 使用者存取權的檢閱（每日）	admin	管理者對使用者執行的動作。
ISO 27001 (10.2.2) 外部承包商（每月）	admin	外部承包商引起的異常狀況及失敗。
ISO 27001 (10.6) 網路管理（每月）	admin	由網路服務上使用者所引起的動作及
ISO 27001 (11.6) 應用程式存取控制（每月）	admin	HR 資料、機密資料、使用者機密資
ISO 27001 (12.4.2) 系統測試資料（每週）	admin	對系統測試資料執行的動作。
ISO 27001 (10.9.3) 公開可用的系統（每月）	admin	公開已發佈資料的動作及異常狀況。
ISO 27001 (15.1.3) 人力資源資料存取（每週）	admin	針對人力資源資料的異常狀況及失敗
ISO 27001 (11.4.3) 節點鑑別（每日）	admin	與遠端電腦系統連線的鑑別。
ISO 27001 (12.4.3) 原始碼存取（每日）	admin	存取原始碼。
ISO 27001 (11.7.1) 行動工作者（每月）	admin	行動工作者引起的異常狀況及失敗。
ISO 27001 (10.9.3) 公開可用的系統（每週）	admin	公開已發佈資料的動作及異常狀況。
ISO 27001 (10.4) 轉換通道和特洛伊木馬程式碼（每月）	admin	轉換通道及特洛伊
ISO 27001 (15.1.4) 資料存取（每週）	admin	針對 HR、機密及
ISO 27001 (11.5.2) 使用者識別與鑑別（每週）	admin	登入與登出成功及
ISO 27001 (11.2) 使用者存取權的檢閱（每月）	admin	管理者對使用者執
ISO 27001 (10.2.2) 外部承包商（每日）	admin	外部承包商引起的
ISO 27001 (11.3.1) 使用者責任與密碼使用（每月）	admin	本端或遠端的登入
ISO 27001 (11.2.4) 監督及檢閱 - 存取控制（每週）	admin	針對金鑰資產的成
ISO 27001 (10.2.2) 外部承包商（每週）	admin	外部承包商引起的
ISO 27001 (11.2) 使用者存取權的檢閱（每週）	admin	管理者對使用者執
ISO 27001 (11.7.2) 在家工作者（每週）	admin	在家工作者引起的
ISO 27001 (11.3.1) 使用者責任與密碼使用（每日）	admin	本端或遠端的登入
ISO 27001 (12.4.1) 作業軟體控制（每月）	admin	更新或變更重要系
ISO 27001 (10.6) 網路管理（每日）	admin	由網路服務上使用
ISO 27001 (10.10.4) 操作員日誌（每週）	admin	IT 管理職員執行的
ISO 27001 (11.7.1) 行動工作者（每日）	admin	行動工作者引起的
ISO 27001 (11.7.1) 行動工作者（每週）	admin	行動工作者引起的
ISO 27001 (11.3.1) 使用者責任與密碼使用（每週）	admin	本端或遠端的登入
ISO 27001 (10.1.2,12.5) 作業變更控制（每週）	admin	作業環境的變更（
ISO 27001 (11.4.4) 遠端診斷埠存取（每月）	admin	診斷伺服器上埠存
ISO 27001 (15.3.2) - 資訊系統審核工具存取（每月）	admin	存取資訊系統審核
ISO 27001 (11.4.4) 遠端診斷埠存取（每週）	admin	診斷伺服器上埠存

內建上千份管理、維運與合規報表，如COBIT , PCI, SOX, HIPAA, NERC CIP, FISMA , ISO 27001 , GLBA..等

SOX Weekly Successful Login Attempts

Generated: Oct 26, 2012 2:53 AM CST

QRadar
Top 10 Networks By Successful Logins
For Previous Week by Hour
Count

Top Users by Successful Logins

Oct 15, 2012 12:00 AM CST - Oct 22, 2012 12:00 AM CST

Report Wizard

Layout Preview

This report preview displays the report layout and chart types you have chosen. It does not reflect live data.

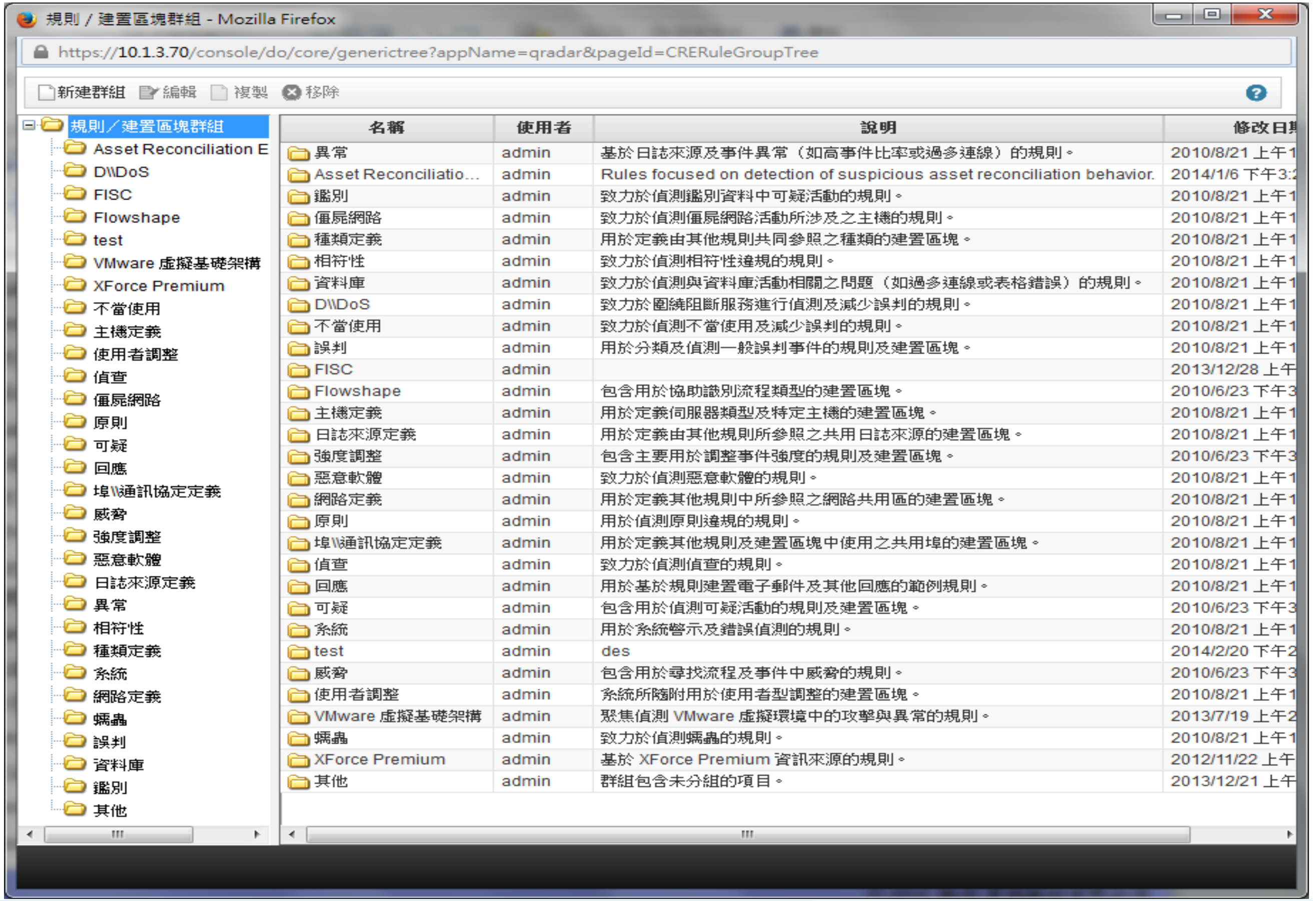
Default Application / OS-WindowsAuthServer: Failed Logins by User

Generated: Nov 13, 2010 1:34 AM

- 報表精靈
- 自行拖拉、修改報表樣本
- 報表自動寄送

QRadar SIEM提供超過600個預設Best Practice 的 即時性攻擊與外洩事件關聯分析規則 (Out-of-the-Box Rules)為業界最多

- **Default Build-in Attack Rules**
  - Anomaly異常 (15)
  - Authentication認證 (15)
  - Botnet殭屍網絡 (7)
  - Compliance合規 (14)
  - Database資料庫 (11)
  - DDoS攻擊 (38)
  - Exploit 利用 (16)
  - Malware惡意軟件 (14)
  - Policy 違反政策 (51)
  - Recon偵察 (95)
  - Suspicious 可疑 (25)
  - Threats 威脅 (39)
  - Worms 蠕蟲 (4)
  - System系統 (10)
  - VMWare 系統 (23)
  - Breach 外洩 (2)
- **Anomaly Detection Rule**
- **Threshold Detection Rule**
- **Behavior Detection rules**

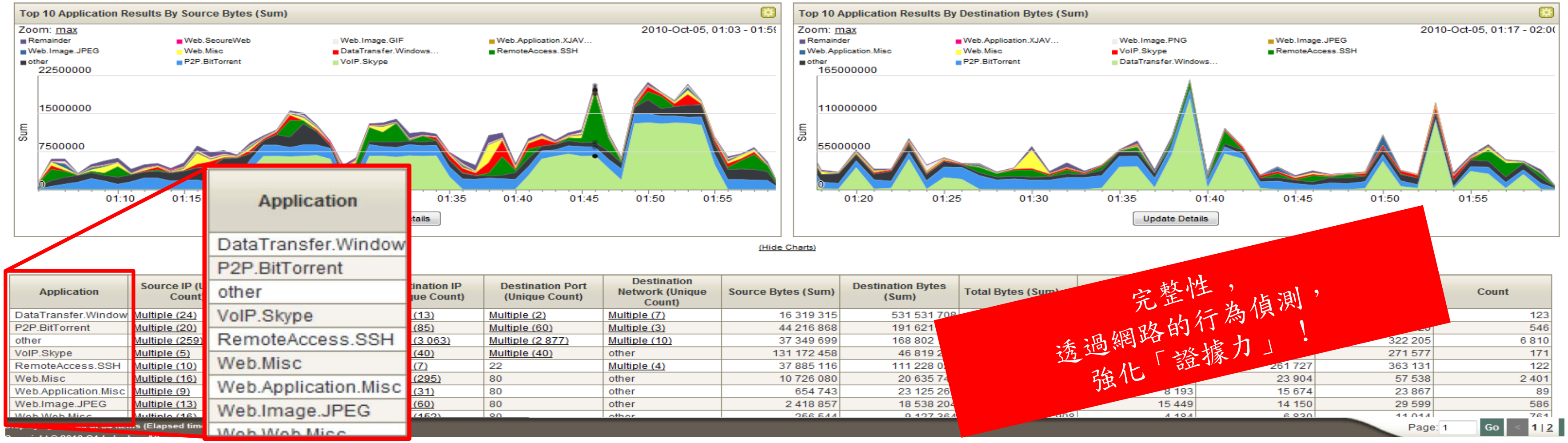


名稱	使用者	說明	修改日其
異常	admin	基於日誌來源及事件異常（如高事件比率或過多連線）的規則。	2010/8/21 上午1
Asset Reconciliatio...	admin	Rules focused on detection of suspicious asset reconciliation behavior.	2014/1/6 下午3:2
鑑別	admin	致力於偵測鑑別資料中可疑活動的規則。	2010/8/21 上午1
僵屍網路	admin	致力於偵測僵屍網路活動所涉及之主機的規則。	2010/8/21 上午1
種類定義	admin	用於定義由其他規則共同參照之種類的建置區塊。	2010/8/21 上午1
相符性	admin	致力於偵測相符性違規的規則。	2010/8/21 上午1
資料庫	admin	致力於偵測與資料庫活動相關之問題（如過多連線或表格錯誤）的規則。	2010/8/21 上午1
D\\DoS	admin	致力於圍繞阻斷服務進行偵測及減少誤判的規則。	2010/8/21 上午1
不當使用	admin	致力於偵測不當使用及減少誤判的規則。	2010/8/21 上午1
誤判	admin	用於分類及偵測一般誤判事件的規則及建置區塊。	2010/8/21 上午1
FISC	admin		2013/12/28 上午
Flowshape	admin	包含用於協助識別流程類型的建置區塊。	2010/6/23 下午3
主機定義	admin	用於定義伺服器類型及特定主機的建置區塊。	2010/8/21 上午1
日誌來源定義	admin	用於定義由其他規則所參照之共用日誌來源的建置區塊。	2010/8/21 上午1
強度調整	admin	包含主要用於調整事件強度的規則及建置區塊。	2010/6/23 下午3
惡意軟體	admin	致力於偵測惡意軟體的規則。	2010/8/21 上午1
網路定義	admin	用於定義其他規則中所參照之網路共用區的建置區塊。	2010/8/21 上午1
原則	admin	用於偵測原則違規的規則。	2010/8/21 上午1
埠\\通訊協定定義	admin	用於定義其他規則及建置區塊中使用之共用埠的建置區塊。	2010/8/21 上午1
偵查	admin	致力於偵測偵查的規則。	2010/8/21 上午1
回應	admin	用於基於規則建置電子郵件及其他回應的範例規則。	2010/8/21 上午1
可疑	admin	包含用於偵測可疑活動的規則及建置區塊。	2010/6/23 下午3
系統	admin	用於系統警示及錯誤偵測的規則。	2010/8/21 上午1
test	admin	des	2014/2/20 下午2
威脅	admin	包含用於尋找流程及事件中威脅的規則。	2010/6/23 下午3
使用者調整	admin	系統所隨附用於使用者型調整的建置區塊。	2010/8/21 上午1
VMware 虛擬基礎架構	admin	聚焦偵測 VMware 虛擬環境中的攻擊與異常的規則。	2013/7/19 上午2
蠕蟲	admin	致力於偵測蠕蟲的規則。	2010/8/21 上午1
XForce Premium	admin	基於 XForce Premium 資訊來源的規則。	2012/11/22 上午
其他	admin	群組包含未分組的項目。	2013/12/21 上午

© 2016 IBM Corporation

Network Security Intelligence – DPI技術，分析網路網路封包與安全行為

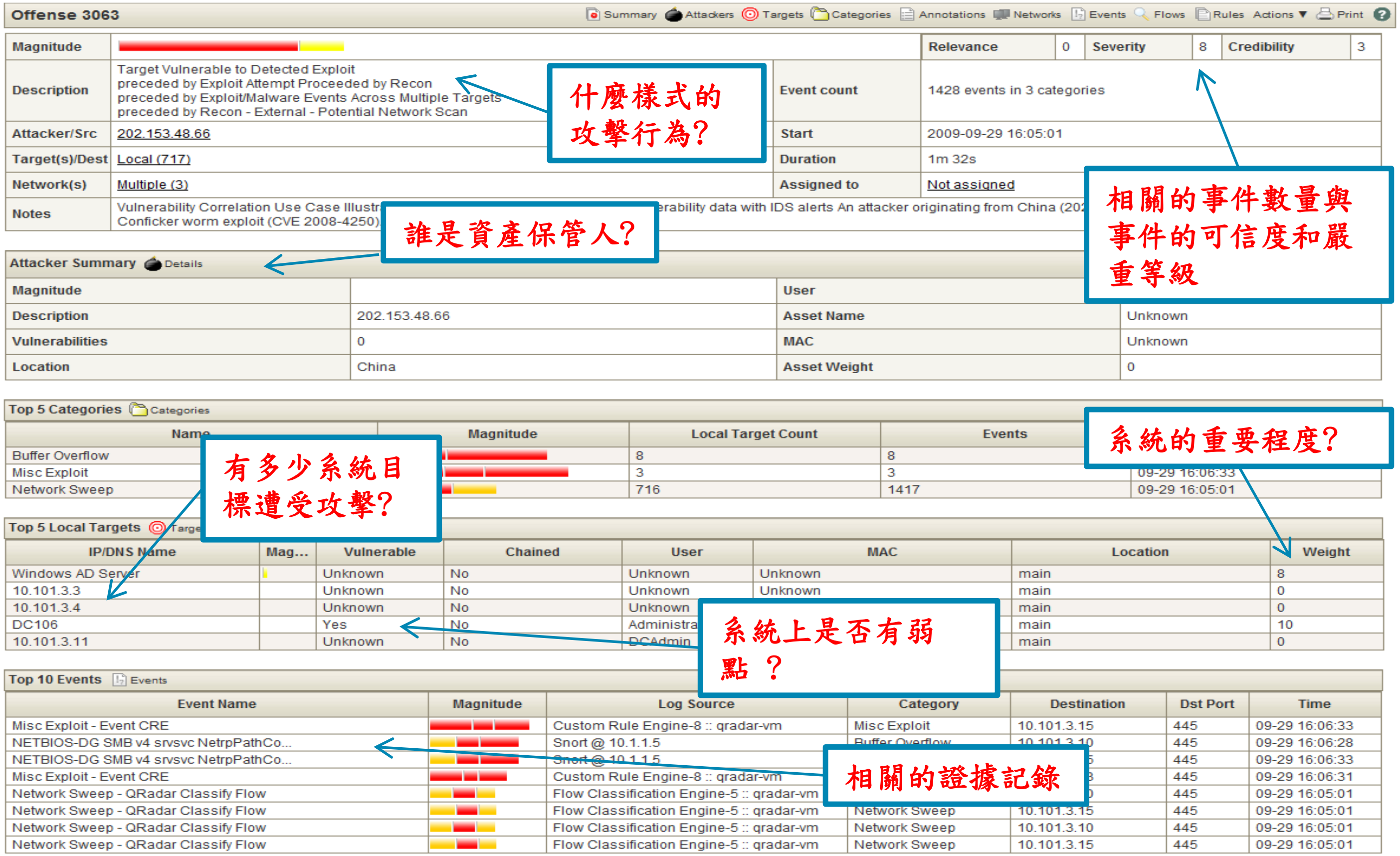
- QRadar 支援二類Flow 收集與分析方式:
  - 網路設備之NetFlow, CFlow, JFlow, SFlow, VFlow
  - 使用Mirror Port 進行 Layer 7 流量與內容解析 (Qflow)
- 預設提供
  - 1000+ 應用程式通訊自動辨識
  - 100+ Flow 異常偵測之規則與應用.



Application	Source IP (U Count)	ination IP ue Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)				Count
DataTransfer.Window	Multiple (24)	(13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708					123
P2P.BitTorrent	Multiple (20)	(85)	Multiple (60)	Multiple (3)	44 216 868	191 621					546
other	Multiple (259)	(3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802				322 205	6 810
VoIP.Skype	Multiple (5)	(40)	Multiple (40)	other	131 172 458	46 819 2				271 577	171
RemoteAccess.SSH	Multiple (10)	(7)	22	Multiple (4)	37 885 116	111 228 0			261 727	363 131	122
Web.Misc	Multiple (16)	(295)	80	other	10 726 080	20 635 74			23 904	57 538	2 401
Web.Application.Misc	Multiple (9)	(31)	80	other	654 743	23 125 26		8 193	15 674	23 867	89
Web.Image.JPEG	Multiple (13)	(60)	80	other	2 418 857	18 538 204		15 449	14 150	29 599	586
Web.Web.Misc	Multiple (16)	(152)	80	other	256 544	9 127 364		4 184	6 830	11 014	761

完整性，
透過網路的行為偵測，
強化「證據力」！

完整呈現資安事件資訊與內容



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 erability data with IDS alerts An attacker originating from China (202 Conficker worm exploit (CVE 2008-4250)						

Attacker Summary Details

Magnitude		User	
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	Events	
Buffer Overflow	🟥	8	8	
Misc Exploit	🟥	3	3	09-29 16:06:33
Network Sweep	🟥🟨	716	1417	09-29 16:05:01

Top 5 Local Targets Targe

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	Administra		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		5	445	09-29 16:06:33
Misc Exploit - Event CRE	🟥	Custom Rule Engine-8 :: qradar-vm		3	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow	🟨🟥🟨	Flow Classification Engine-5 :: qradar-vm		0	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

什麼樣式的攻擊行為?

相關的事件數量與事件的可信度和嚴重等級

誰是資產保管人?

有多少系統目標遭受攻擊?

系統的重要程度?

系統上是否有弱點 ？

相關的證據記錄

Open Ecosystem

Juniper Networks · ForeScout · Blue Coat · Vormetric · SecurIT · RAZ-LEE Experts @ Security and Compliance · CorreLog · SOURCEfire

Cisco · Trend Micro · Kaspersky lab · f5 · FireEye · AuthenWare Security Redefined · ONWIRE

websense Essential Information Protection · lastline · paloalto networks · FORTINET · Nanogate · radware

SafeNet · SentryCom Ltd.

ARXAN Protecting the App Economy · Bit9

Alert Enterprise · toopher

Ready for IBM Security Intelligence

IBM **PartnerWorld**

100+ ecosystem partners, 500+ QRadar integrations

HID · enterasys Secure Networks · emillion · STEALTHbits Technologies · ARUBA networks · Entrust · NUANCE · ilantus The Identity Management People

IDology Inc. · DAMBALLA · VIRTUALFORGE we harden your software · PRi pontis research · VSSA · PhoneFactor · Positive Technologies · PIREAN · Tangentia

Prolifics · charismathics · gemalto · observe it people audit · cilasoft · NOVELL · Core Security · ARBOR Networks · beyondtrust

BIO-key · RSA The Security Division of EMC · tenable network security · N · CYBERARK · CORVIR IT Solution Experts · AKROS · RF IDeas · STONESOFT A McAfee Group Company · VERDASYS

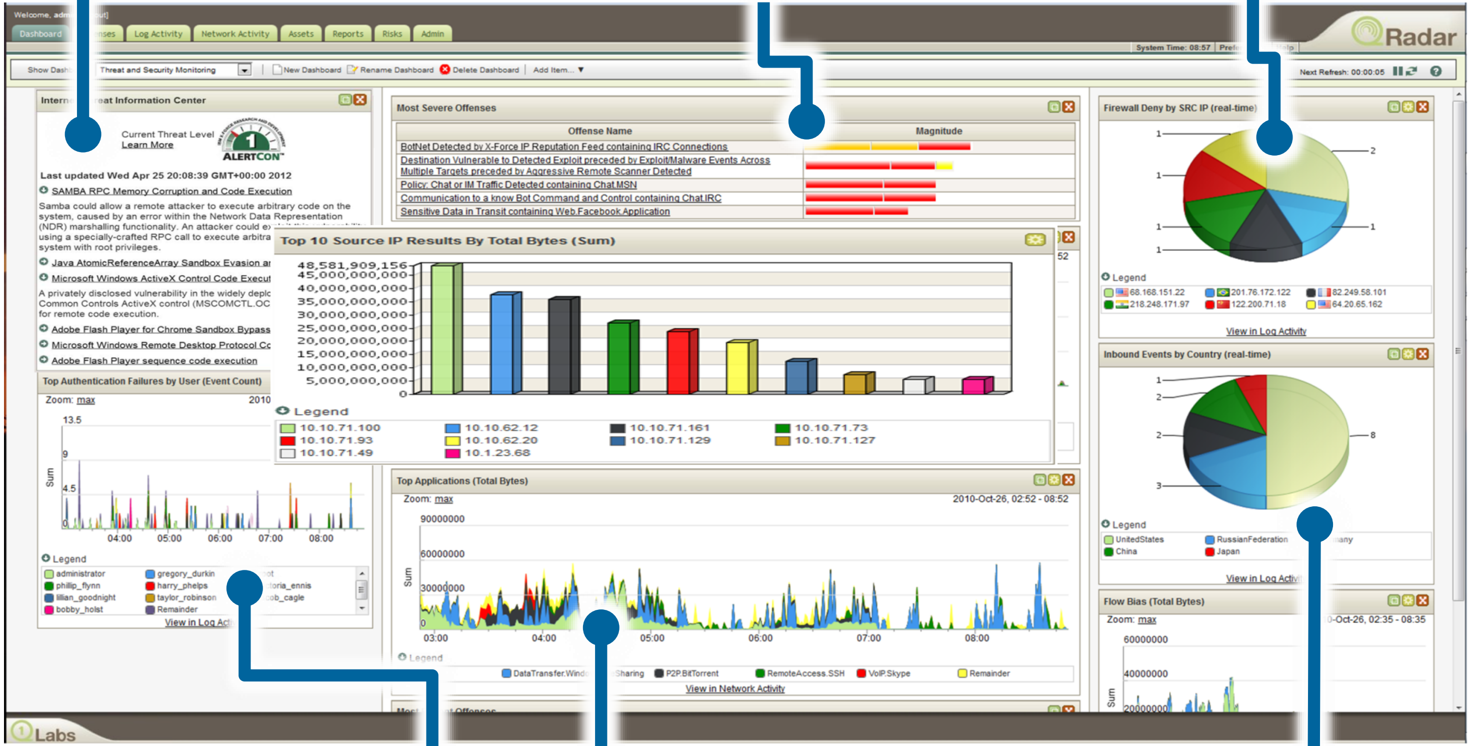
QRadar 提供深入可訂製的視覺化Dashboard

- Dashboard
- Offenses
- Log Activity
- Network Activity
- Assets
- Investigation
- Reports
- Administration

IBM X-Force® 資訊安全威脅通報中心

即時、優先要處理的資安事故威脅與攻擊

相關系統存取狀態



Intern eat Information Center

Current Threat Level
Learn More

Last updated Wed Apr 25 20:08:39 GMT+00:00 2012

SAMBA RPC Memory Corruption and Code Execution

Samba could allow a remote attacker to execute arbitrary code on the system, caused by an error within the Network Data Representation (NDR) marshalling functionality. An attacker could ex using a specially-crafted RPC call to execute arbitra system with root privileges.

Java AtomicReferenceArray Sandbox Evasion ar

Microsoft Windows ActiveX Control Code Execut

A privately disclosed vulnerability in the widely deplo Common Controls ActiveX control (MSCOMCTL.OC for remote code execution.

Adobe Flash Player for Chrome Sandbox Bypass

Microsoft Windows Remote Desktop Protocol Co

Adobe Flash Player sequence code execution

Top Authentication Failures by User (Event Count)

Most Severe Offenses

Offense Name	Magnitude
BotNet Detected by X-Force IP Reputation Feed containing IRC Connections	
Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Aggressive Remote Scanner Detected	
Policy: Chat or IM Traffic Detected containing Chat.MSN	
Communication to a know Bot Command and Control containing Chat.IRC	
Sensitive Data in Transit containing Web.Facebook.Application	

Top 10 Source IP Results By Total Bytes (Sum)

Top Applications (Total Bytes)

Firewall Deny by SRC IP (real-time)

Inbound Events by Country (real-time)

Flow Bias (Total Bytes)

使用者認證與授權

即時使用者應用程式行為分析

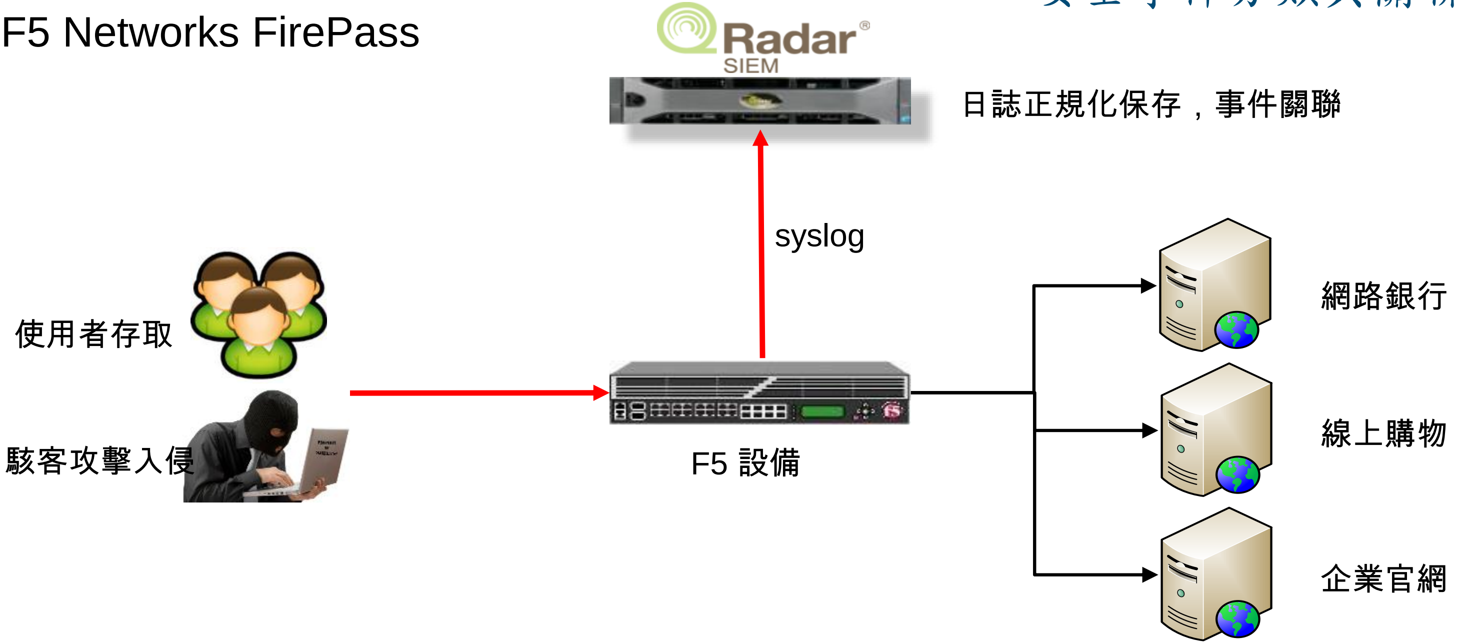
資安事件排行

QRadar支援各種F5相關日誌的收錄與解析

- QRADAR 對F5 預設支援：
  - F5 Networks BIG-IP AFM
  - F5 Networks BIG-IP APM
  - F5 Networks BIG-IP ASM
  - F5 Networks BIG-IP LTM
  - F5 Networks FirePass

透過QRadar強化F5網路安全的洞悉能力

- 應用系統連接的深入剖析
- 趨勢分析
- 動態查詢
- 統計圖表
- 安全事件分類與關聯



Radar SIEM

日誌正規化保存，事件關聯

syslog

使用者存取

駭客攻擊入侵

F5 設備

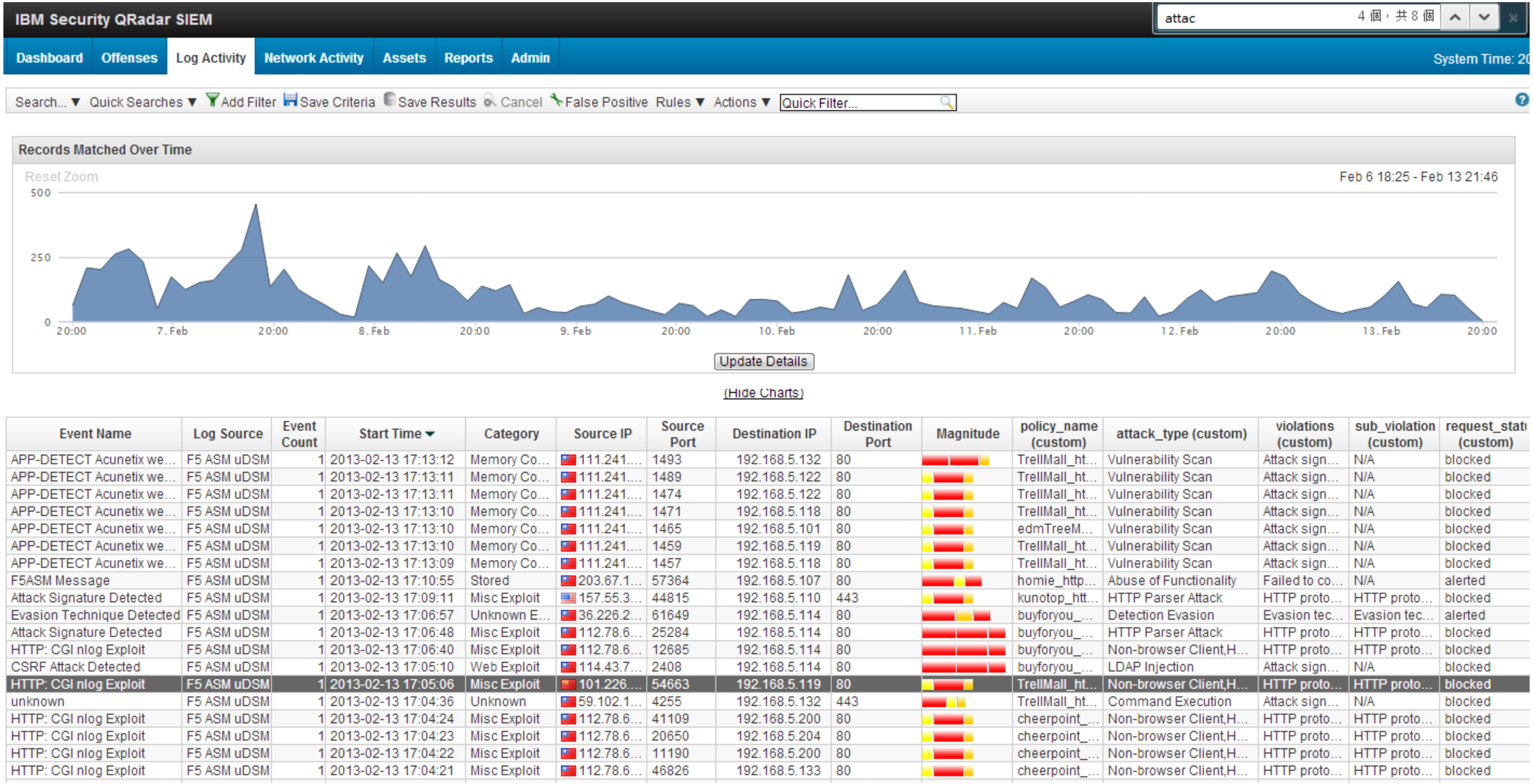
網路銀行

線上購物

企業官網

© 2016 IBM Corporation

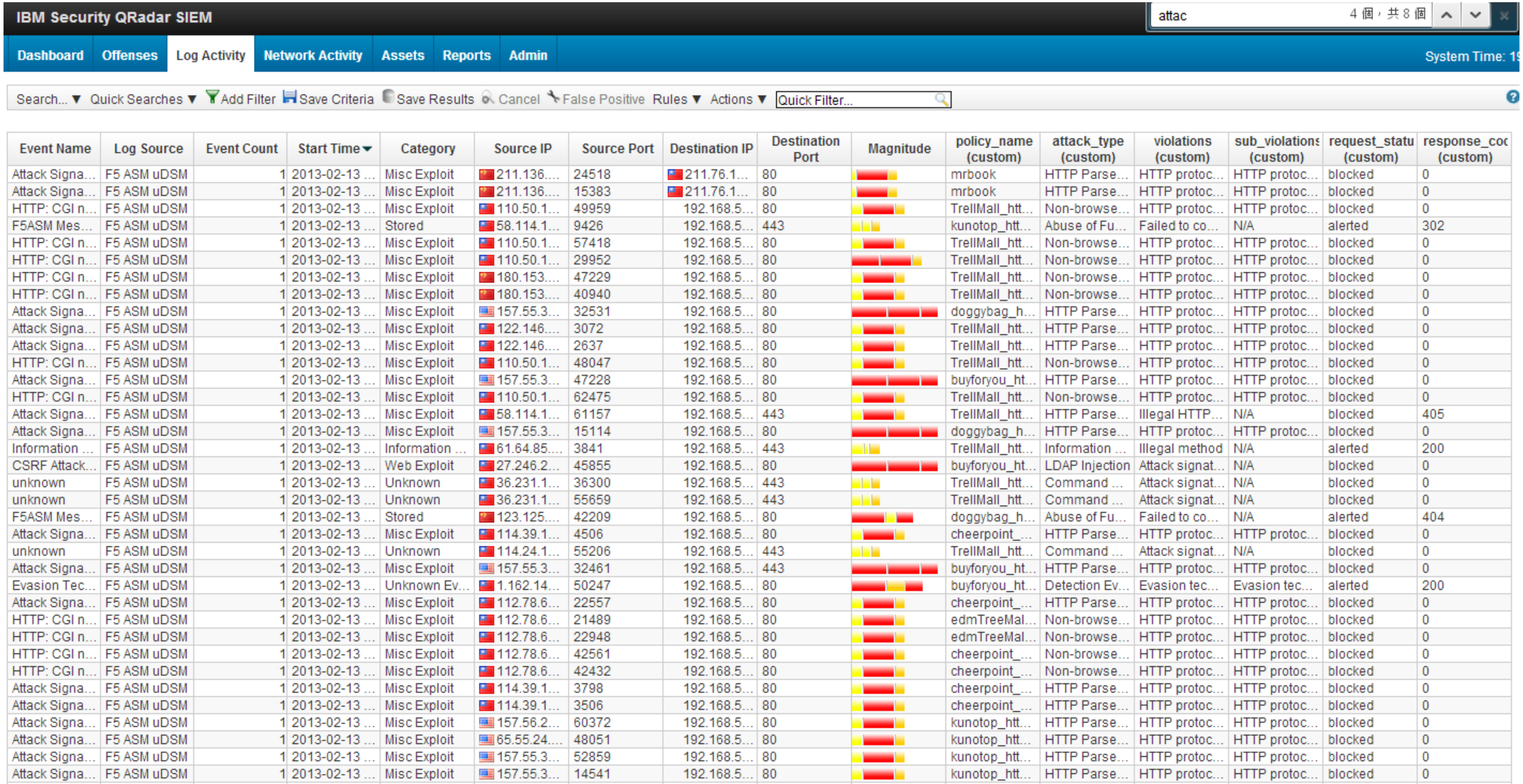
QRADAR針對F5 的事件趨勢分析



Event Name	Log Source	Event Count	Start Time ▾	Category	Source IP	Source Port	Destination IP	Destination Port	Magnitude	policy_name (custom)	attack_type (custom)	violations (custom)	sub_violation (custom)	request_stat (custom)
APP-DETECT Acunetix we...	F5 ASM uDSM	1	2013-02-13 17:13:12	Memory Co...	111.241....	1493	192.168.5.132	80		TrellMall_ht...	Vulnerability Scan	Attack sign...	N/A	blocked
APP-DETECT Acunetix we...	F5 ASM uDSM	1	2013-02-13 17:13:11	Memory Co...	111.241....	1489	192.168.5.122	80		TrellMall_ht...	Vulnerability Scan	Attack sign...	N/A	blocked
APP-DETECT Acunetix we...	F5 ASM uDSM	1	2013-02-13 17:13:11	Memory Co...	111.241....	1474	192.168.5.122	80		TrellMall_ht...	Vulnerability Scan	Attack sign...	N/A	blocked
APP-DETECT Acunetix we...	F5 ASM uDSM	1	2013-02-13 17:13:10	Memory Co...	111.241....	1471	192.168.5.118	80		TrellMall_ht...	Vulnerability Scan	Attack sign...	N/A	blocked
APP-DETECT Acunetix we...	F5 ASM uDSM	1	2013-02-13 17:13:10	Memory Co...	111.241....	1465	192.168.5.101	80		edmTreeM...	Vulnerability Scan	Attack sign...	N/A	blocked
APP-DETECT Acunetix we...	F5 ASM uDSM	1	2013-02-13 17:13:10	Memory Co...	111.241....	1459	192.168.5.119	80		TrellMall_ht...	Vulnerability Scan	Attack sign...	N/A	blocked
APP-DETECT Acunetix we...	F5 ASM uDSM	1	2013-02-13 17:13:09	Memory Co...	111.241....	1457	192.168.5.118	80		TrellMall_ht...	Vulnerability Scan	Attack sign...	N/A	blocked
F5ASM Message	F5 ASM uDSM	1	2013-02-13 17:10:55	Stored	203.67.1...	57364	192.168.5.107	80		homie_http...	Abuse of Functionality	Failed to co...	N/A	alerted
Attack Signature Detected	F5 ASM uDSM	1	2013-02-13 17:09:11	Misc Exploit	157.55.3...	44815	192.168.5.110	443		kunotop_htt...	HTTP Parser Attack	HTTP proto...	HTTP proto...	blocked
Evasion Technique Detected	F5 ASM uDSM	1	2013-02-13 17:06:57	Unknown E...	36.226.2...	61649	192.168.5.114	80		buyforyou_...	Detection Evasion	Evasion tec...	Evasion tec...	alerted
Attack Signature Detected	F5 ASM uDSM	1	2013-02-13 17:06:48	Misc Exploit	112.78.6...	25284	192.168.5.114	80		buyforyou_...	HTTP Parser Attack	HTTP proto...	HTTP proto...	blocked
HTTP: CGI nlog Exploit	F5 ASM uDSM	1	2013-02-13 17:06:40	Misc Exploit	112.78.6...	12685	192.168.5.114	80		buyforyou_...	Non-browser Client,H...	HTTP proto...	HTTP proto...	blocked
CSRF Attack Detected	F5 ASM uDSM	1	2013-02-13 17:05:10	Web Exploit	114.43.7...	2408	192.168.5.114	80		buyforyou_...	LDAP Injection	Attack sign...	N/A	blocked
HTTP: CGI nlog Exploit	F5 ASM uDSM	1	2013-02-13 17:05:06	Misc Exploit	101.226....	54663	192.168.5.119	80		TrellMall_ht...	Non-browser Client,H...	HTTP proto...	HTTP proto...	blocked
unknown	F5 ASM uDSM	1	2013-02-13 17:04:36	Unknown	59.102.1...	4255	192.168.5.132	443		TrellMall_ht...	Command Execution	Attack sign...	N/A	blocked
HTTP: CGI nlog Exploit	F5 ASM uDSM	1	2013-02-13 17:04:24	Misc Exploit	112.78.6...	41109	192.168.5.200	80		cheerpoint_...	Non-browser Client,H...	HTTP proto...	HTTP proto...	blocked
HTTP: CGI nlog Exploit	F5 ASM uDSM	1	2013-02-13 17:04:23	Misc Exploit	112.78.6...	20650	192.168.5.204	80		cheerpoint_...	Non-browser Client,H...	HTTP proto...	HTTP proto...	blocked
HTTP: CGI nlog Exploit	F5 ASM uDSM	1	2013-02-13 17:04:22	Misc Exploit	112.78.6...	11190	192.168.5.200	80		cheerpoint_...	Non-browser Client,H...	HTTP proto...	HTTP proto...	blocked
HTTP: CGI nlog Exploit	F5 ASM uDSM	1	2013-02-13 17:04:21	Misc Exploit	112.78.6...	46826	192.168.5.133	80		cheerpoint_...	Non-browser Client,H...	HTTP proto...	HTTP proto...	blocked

QRADAR針對F5所收集的日誌欄位呈現

- 包含F5 Policy Name , attack type , request status , response code , request…, 可針對這些條件過濾，再進行分析

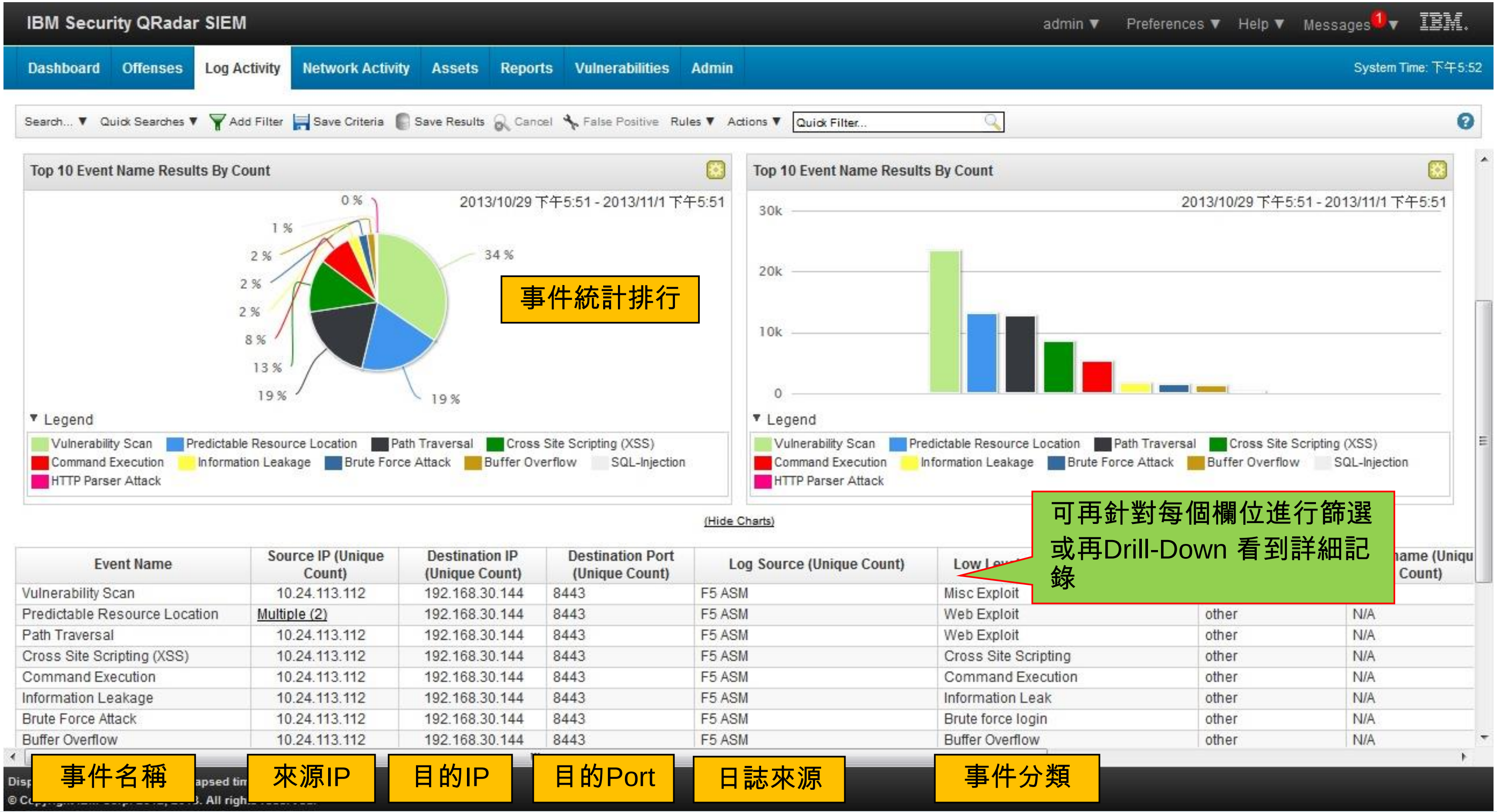


Event Name	Log Source	Event Count	Start Time	Category	Source IP	Source Port	Destination IP	Destination Port	Magnitude	policy_name (custom)	attack_type (custom)	violations (custom)	sub_violations (custom)	request_statu (custom)	response_coc (custom)
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	211.136....	24518	211.76.1...	80		mrbook	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	211.136....	15383	211.76.1...	80		mrbook	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	110.50.1...	49959	192.168.5...	80		TrellMall_htt...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
F5ASM Mes...	F5 ASM uDSM	1	2013-02-13 ...	Stored	58.114.1...	9426	192.168.5...	443		kunotop_htt...	Abuse of Fu...	Failed to co...	N/A	alerted	302
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	110.50.1...	57418	192.168.5...	80		TrellMall_htt...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	110.50.1...	29952	192.168.5...	80		TrellMall_htt...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	180.153....	47229	192.168.5...	80		TrellMall_htt...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	180.153....	40940	192.168.5...	80		TrellMall_htt...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	157.55.3...	32531	192.168.5...	80		doggybag_h...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	122.146....	3072	192.168.5...	80		TrellMall_htt...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	122.146....	2637	192.168.5...	80		TrellMall_htt...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	110.50.1...	48047	192.168.5...	80		TrellMall_htt...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	157.55.3...	47228	192.168.5...	80		buyforyou_ht...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	110.50.1...	62475	192.168.5...	80		TrellMall_htt...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	58.114.1...	61157	192.168.5...	443		TrellMall_htt...	HTTP Parse...	Illegal HTTP...	N/A	blocked	405
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	157.55.3...	15114	192.168.5...	80		doggybag_h...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Information ...	F5 ASM uDSM	1	2013-02-13 ...	Information ...	61.64.85....	3841	192.168.5...	443		TrellMall_htt...	Information ...	Illegal method	N/A	alerted	200
CSRF Attack...	F5 ASM uDSM	1	2013-02-13 ...	Web Exploit	27.246.2...	45855	192.168.5...	80		buyforyou_ht...	LDAP Injection	Attack signat...	N/A	blocked	0
unknown	F5 ASM uDSM	1	2013-02-13 ...	Unknown	36.231.1...	36300	192.168.5...	443		TrellMall_htt...	Command ...	Attack signat...	N/A	blocked	0
unknown	F5 ASM uDSM	1	2013-02-13 ...	Unknown	36.231.1...	55659	192.168.5...	443		TrellMall_htt...	Command ...	Attack signat...	N/A	blocked	0
F5ASM Mes...	F5 ASM uDSM	1	2013-02-13 ...	Stored	123.125....	42209	192.168.5...	80		doggybag_h...	Abuse of Fu...	Failed to co...	N/A	alerted	404
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	114.39.1...	4506	192.168.5...	80		cheerpoint_...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
unknown	F5 ASM uDSM	1	2013-02-13 ...	Unknown	114.24.1...	55206	192.168.5...	443		TrellMall_htt...	Command ...	Attack signat...	N/A	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	157.55.3...	32461	192.168.5...	443		buyforyou_ht...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Evasion Tec...	F5 ASM uDSM	1	2013-02-13 ...	Unknown Ev...	1.162.14...	50247	192.168.5...	80		buyforyou_ht...	Detection Ev...	Evasion tec...	Evasion tec...	alerted	200
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	112.78.6...	22557	192.168.5...	80		cheerpoint_...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	112.78.6...	21489	192.168.5...	80		edmTreeMal...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	112.78.6...	22948	192.168.5...	80		edmTreeMal...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	112.78.6...	42561	192.168.5...	80		cheerpoint_...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
HTTP: CGI n...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	112.78.6...	42432	192.168.5...	80		cheerpoint_...	Non-browse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	114.39.1...	3798	192.168.5...	80		cheerpoint_...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	114.39.1...	3506	192.168.5...	80		cheerpoint_...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	157.56.2...	60372	192.168.5...	80		kunotop_htt...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	65.55.24....	48051	192.168.5...	80		kunotop_htt...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	157.55.3...	52859	192.168.5...	80		kunotop_htt...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0
Attack Signa...	F5 ASM uDSM	1	2013-02-13 ...	Misc Exploit	157.55.3...	14541	192.168.5...	80		kunotop_htt...	HTTP Parse...	HTTP protoc...	HTTP protoc...	blocked	0

© 2016 IBM Corporation

F5 日誌統計分析 – 事件種類統計

- 可調閱F5 ASM 所記錄的相關日誌，並進行不同面向的統計。



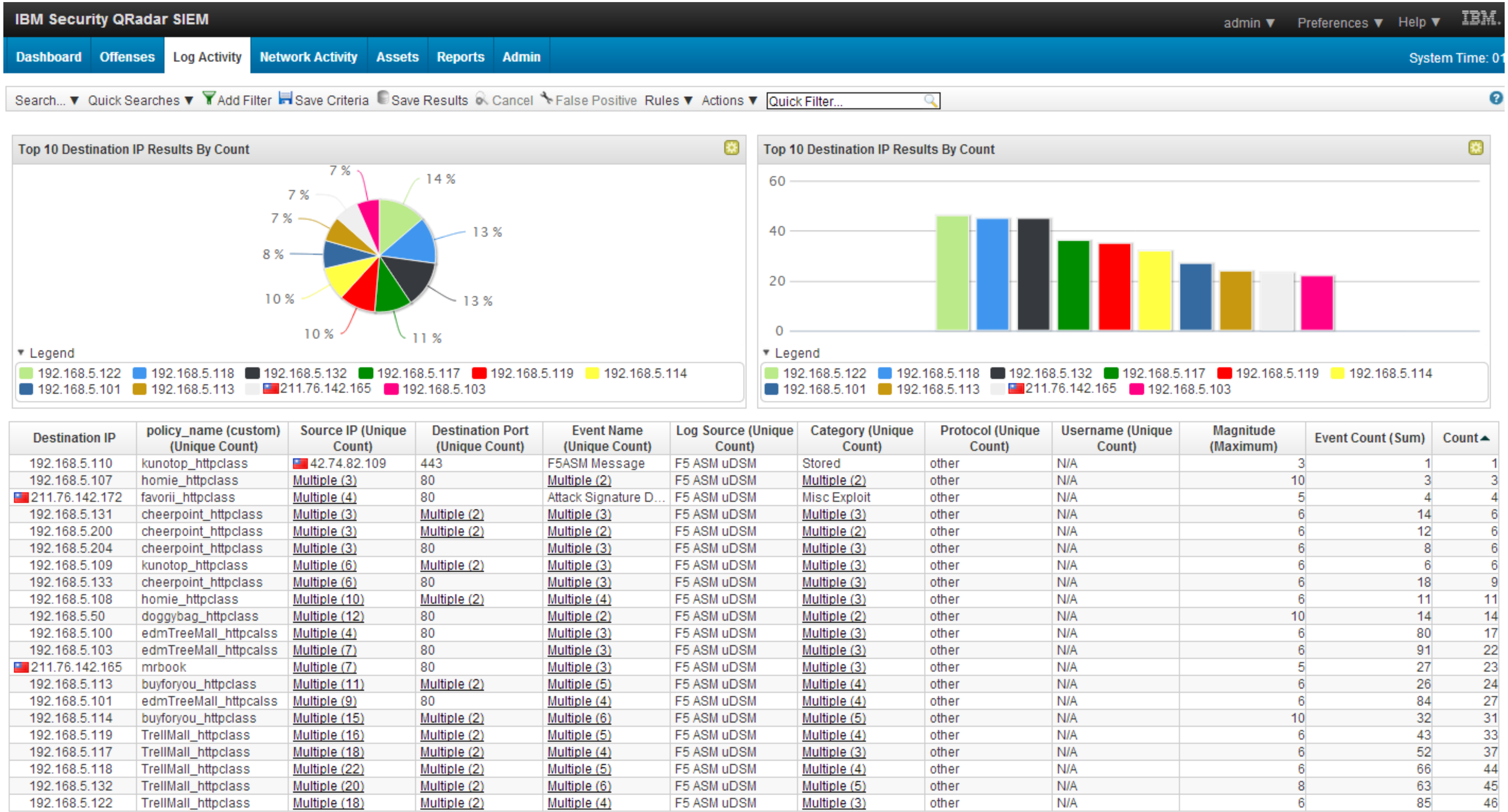
事件統計排行

可再針對每個欄位進行篩選或再Drill-Down 看到詳細記錄

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Low Lev		name (Uniqu Count)
Vulnerability Scan	10.24.113.112	192.168.30.144	8443	F5 ASM	Misc Exploit		
Predictable Resource Location	Multiple (2)	192.168.30.144	8443	F5 ASM	Web Exploit	other	N/A
Path Traversal	10.24.113.112	192.168.30.144	8443	F5 ASM	Web Exploit	other	N/A
Cross Site Scripting (XSS)	10.24.113.112	192.168.30.144	8443	F5 ASM	Cross Site Scripting	other	N/A
Command Execution	10.24.113.112	192.168.30.144	8443	F5 ASM	Command Execution	other	N/A
Information Leakage	10.24.113.112	192.168.30.144	8443	F5 ASM	Information Leak	other	N/A
Brute Force Attack	10.24.113.112	192.168.30.144	8443	F5 ASM	Brute force login	other	N/A
Buffer Overflow	10.24.113.112	192.168.30.144	8443	F5 ASM	Buffer Overflow	other	N/A

事件名稱　來源IP　目的IP　目的Port　日誌來源　事件分類

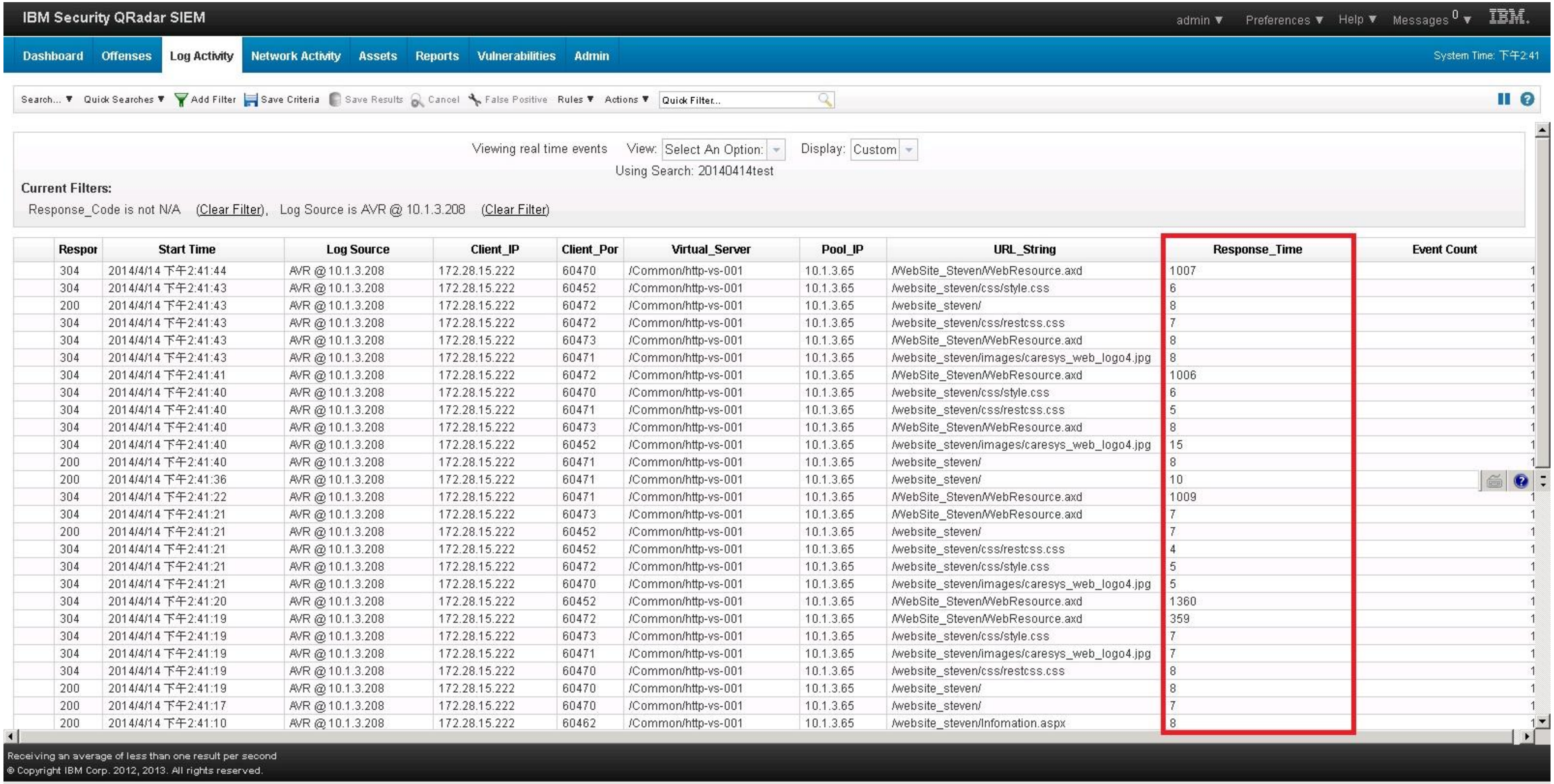
事件統計數 by F5 後端 Server



Destination IP	policy_name (custom) (Unique Count)	Source IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count ▲
192.168.5.110	kunotop_httpclass	42.74.82.109	443	F5ASM Message	F5 ASM uDSM	Stored	other	N/A	3	1	1
192.168.5.107	homie_httpclass	Multiple (3)	80	Multiple (2)	F5 ASM uDSM	Multiple (2)	other	N/A	10	3	3
211.76.142.172	favorii_httpclass	Multiple (4)	80	Attack Signature D...	F5 ASM uDSM	Misc Exploit	other	N/A	5	4	4
192.168.5.131	cheerpoint_httpclass	Multiple (3)	Multiple (2)	Multiple (3)	F5 ASM uDSM	Multiple (3)	other	N/A	6	14	6
192.168.5.200	cheerpoint_httpclass	Multiple (3)	Multiple (2)	Multiple (2)	F5 ASM uDSM	Multiple (2)	other	N/A	6	12	6
192.168.5.204	cheerpoint_httpclass	Multiple (3)	80	Multiple (3)	F5 ASM uDSM	Multiple (3)	other	N/A	6	8	6
192.168.5.109	kunotop_httpclass	Multiple (6)	Multiple (2)	Multiple (3)	F5 ASM uDSM	Multiple (3)	other	N/A	6	6	6
192.168.5.133	cheerpoint_httpclass	Multiple (6)	80	Multiple (3)	F5 ASM uDSM	Multiple (3)	other	N/A	6	18	9
192.168.5.108	homie_httpclass	Multiple (10)	Multiple (2)	Multiple (4)	F5 ASM uDSM	Multiple (3)	other	N/A	6	11	11
192.168.5.50	doggybag_httpclass	Multiple (12)	80	Multiple (2)	F5 ASM uDSM	Multiple (2)	other	N/A	10	14	14
192.168.5.100	edmTreeMall_httpcalss	Multiple (4)	80	Multiple (3)	F5 ASM uDSM	Multiple (3)	other	N/A	6	80	17
192.168.5.103	edmTreeMall_httpcalss	Multiple (7)	80	Multiple (3)	F5 ASM uDSM	Multiple (3)	other	N/A	6	91	22
211.76.142.165	mrbook	Multiple (7)	80	Multiple (3)	F5 ASM uDSM	Multiple (3)	other	N/A	5	27	23
192.168.5.113	buyforyou_httpclass	Multiple (11)	Multiple (2)	Multiple (5)	F5 ASM uDSM	Multiple (4)	other	N/A	6	26	24
192.168.5.101	edmTreeMall_httpcalss	Multiple (9)	80	Multiple (4)	F5 ASM uDSM	Multiple (4)	other	N/A	6	84	27
192.168.5.114	buyforyou_httpclass	Multiple (15)	Multiple (2)	Multiple (6)	F5 ASM uDSM	Multiple (5)	other	N/A	10	32	31
192.168.5.119	TrellMall_httpclass	Multiple (16)	Multiple (2)	Multiple (5)	F5 ASM uDSM	Multiple (4)	other	N/A	6	43	33
192.168.5.117	TrellMall_httpclass	Multiple (18)	Multiple (2)	Multiple (4)	F5 ASM uDSM	Multiple (3)	other	N/A	6	52	37
192.168.5.118	TrellMall_httpclass	Multiple (22)	Multiple (2)	Multiple (5)	F5 ASM uDSM	Multiple (4)	other	N/A	6	66	44
192.168.5.132	TrellMall_httpclass	Multiple (20)	Multiple (2)	Multiple (6)	F5 ASM uDSM	Multiple (5)	other	N/A	8	63	45
192.168.5.122	TrellMall_httpclass	Multiple (18)	Multiple (2)	Multiple (4)	F5 ASM uDSM	Multiple (3)	other	N/A	6	85	46

© 2016 IBM Corporation

針對後端Web 回應時間的分析 F5 - Server Latency-Response Time



Viewing real time events View: Select An Option: Display: Custom

Using Search: 20140414test

Current Filters:

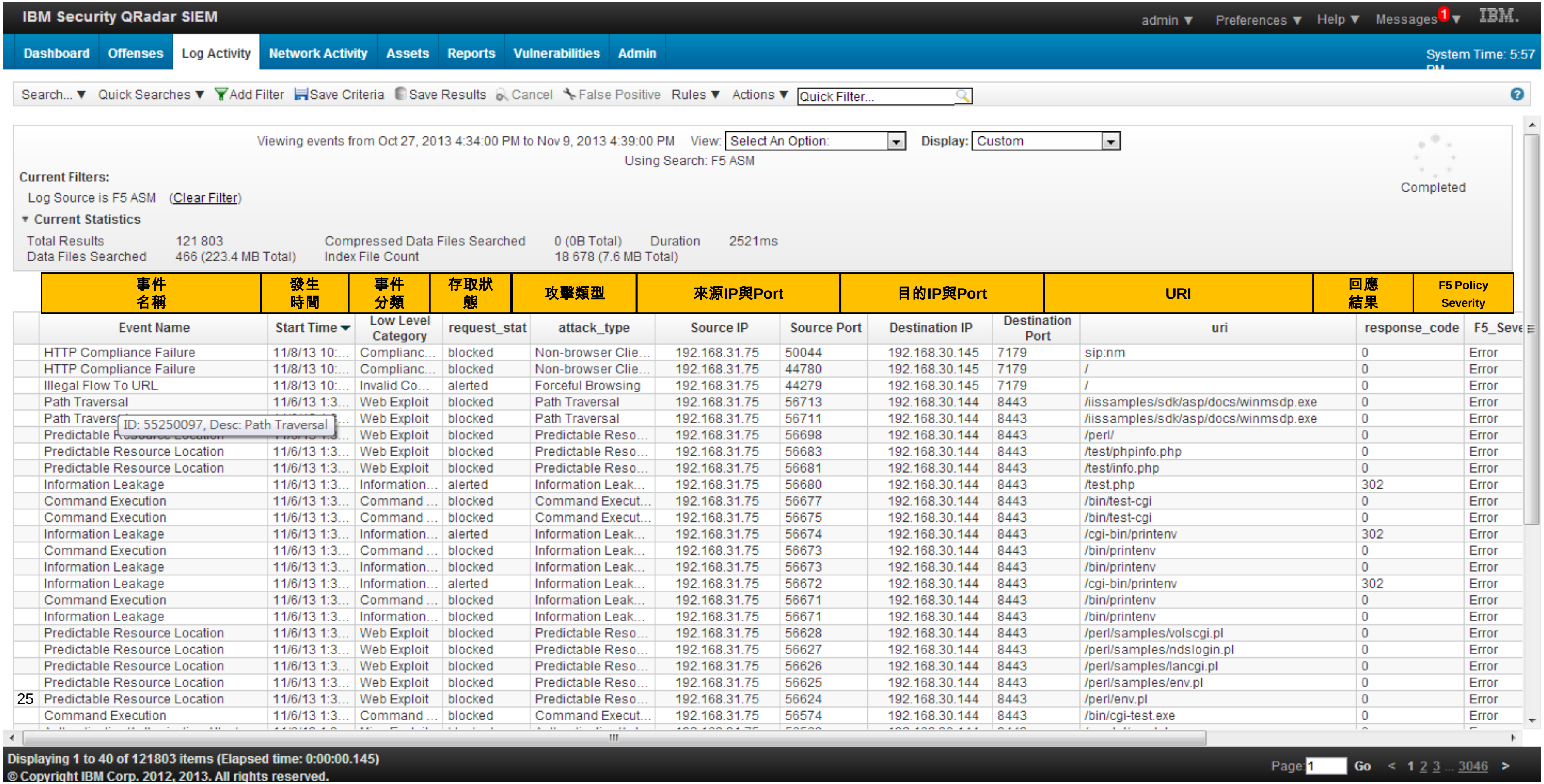
Response_Code is not N/A (Clear Filter), Log Source is AVR @ 10.1.3.208 (Clear Filter)

Respor	Start Time	Log Source	Client_IP	Client_Por	Virtual_Server	Pool_IP	URL_String	Response_Time	Event Count
304	2014/4/14 下午2:41:44	AVR @ 10.1.3.208	172.28.15.222	60470	/Common/http-vs-001	10.1.3.65	/WebSite_Steven/WebResource.axd	1007	1
304	2014/4/14 下午2:41:43	AVR @ 10.1.3.208	172.28.15.222	60452	/Common/http-vs-001	10.1.3.65	/website_steven/css/style.css	6	1
200	2014/4/14 下午2:41:43	AVR @ 10.1.3.208	172.28.15.222	60472	/Common/http-vs-001	10.1.3.65	/website_steven/	8	1
304	2014/4/14 下午2:41:43	AVR @ 10.1.3.208	172.28.15.222	60472	/Common/http-vs-001	10.1.3.65	/website_steven/css/restcss.css	7	1
304	2014/4/14 下午2:41:43	AVR @ 10.1.3.208	172.28.15.222	60473	/Common/http-vs-001	10.1.3.65	/WebSite_Steven/WebResource.axd	8	1
304	2014/4/14 下午2:41:43	AVR @ 10.1.3.208	172.28.15.222	60471	/Common/http-vs-001	10.1.3.65	/website_steven/images/caresys_web_logo4.jpg	8	1
304	2014/4/14 下午2:41:41	AVR @ 10.1.3.208	172.28.15.222	60472	/Common/http-vs-001	10.1.3.65	/WebSite_Steven/WebResource.axd	1006	1
304	2014/4/14 下午2:41:40	AVR @ 10.1.3.208	172.28.15.222	60470	/Common/http-vs-001	10.1.3.65	/website_steven/css/style.css	6	1
304	2014/4/14 下午2:41:40	AVR @ 10.1.3.208	172.28.15.222	60471	/Common/http-vs-001	10.1.3.65	/website_steven/css/restcss.css	5	1
304	2014/4/14 下午2:41:40	AVR @ 10.1.3.208	172.28.15.222	60473	/Common/http-vs-001	10.1.3.65	/WebSite_Steven/WebResource.axd	8	1
304	2014/4/14 下午2:41:40	AVR @ 10.1.3.208	172.28.15.222	60452	/Common/http-vs-001	10.1.3.65	/website_steven/images/caresys_web_logo4.jpg	15	1
200	2014/4/14 下午2:41:40	AVR @ 10.1.3.208	172.28.15.222	60471	/Common/http-vs-001	10.1.3.65	/website_steven/	8	1
200	2014/4/14 下午2:41:36	AVR @ 10.1.3.208	172.28.15.222	60471	/Common/http-vs-001	10.1.3.65	/website_steven/	10	
304	2014/4/14 下午2:41:22	AVR @ 10.1.3.208	172.28.15.222	60471	/Common/http-vs-001	10.1.3.65	/WebSite_Steven/WebResource.axd	1009	1
304	2014/4/14 下午2:41:21	AVR @ 10.1.3.208	172.28.15.222	60473	/Common/http-vs-001	10.1.3.65	/WebSite_Steven/WebResource.axd	7	1
200	2014/4/14 下午2:41:21	AVR @ 10.1.3.208	172.28.15.222	60452	/Common/http-vs-001	10.1.3.65	/website_steven/	7	1
304	2014/4/14 下午2:41:21	AVR @ 10.1.3.208	172.28.15.222	60452	/Common/http-vs-001	10.1.3.65	/website_steven/css/restcss.css	4	1
304	2014/4/14 下午2:41:21	AVR @ 10.1.3.208	172.28.15.222	60472	/Common/http-vs-001	10.1.3.65	/website_steven/css/style.css	5	1
304	2014/4/14 下午2:41:21	AVR @ 10.1.3.208	172.28.15.222	60470	/Common/http-vs-001	10.1.3.65	/website_steven/images/caresys_web_logo4.jpg	5	1
304	2014/4/14 下午2:41:20	AVR @ 10.1.3.208	172.28.15.222	60452	/Common/http-vs-001	10.1.3.65	/WebSite_Steven/WebResource.axd	1360	1
304	2014/4/14 下午2:41:19	AVR @ 10.1.3.208	172.28.15.222	60472	/Common/http-vs-001	10.1.3.65	/WebSite_Steven/WebResource.axd	359	1
304	2014/4/14 下午2:41:19	AVR @ 10.1.3.208	172.28.15.222	60473	/Common/http-vs-001	10.1.3.65	/website_steven/css/style.css	7	1
304	2014/4/14 下午2:41:19	AVR @ 10.1.3.208	172.28.15.222	60471	/Common/http-vs-001	10.1.3.65	/website_steven/images/caresys_web_logo4.jpg	7	1
304	2014/4/14 下午2:41:19	AVR @ 10.1.3.208	172.28.15.222	60470	/Common/http-vs-001	10.1.3.65	/website_steven/css/restcss.css	8	1
200	2014/4/14 下午2:41:19	AVR @ 10.1.3.208	172.28.15.222	60470	/Common/http-vs-001	10.1.3.65	/website_steven/	8	1
200	2014/4/14 下午2:41:17	AVR @ 10.1.3.208	172.28.15.222	60470	/Common/http-vs-001	10.1.3.65	/website_steven/	7	1
200	2014/4/14 下午2:41:10	AVR @ 10.1.3.208	172.28.15.222	60462	/Common/http-vs-001	10.1.3.65	/website_steven/Infomation.aspx	8	1

Receiving an average of less than one result per second

© Copyright IBM Corp. 2012, 2013. All rights reserved.

詳細的F5 ASM 事件正規化



Viewing events from Oct 27, 2013 4:34:00 PM to Nov 9, 2013 4:39:00 PM View: Select An Option: Display: Custom

Using Search: F5 ASM

Current Filters:

Log Source is F5 ASM (Clear Filter)

▼ Current Statistics

Total Results	121 803	Compressed Data Files Searched	0 (0B Total)	Duration	2521ms
Data Files Searched	466 (223.4 MB Total)	Index File Count	18 678 (7.6 MB Total)		

	事件 名稱	發生 時間	事件 分類	存取狀 態	攻擊類型	來源IP與Port		目的IP與Port		URI	回應 結果	F5 Policy Severity
	Event Name	Start Time ▼	Low Level Category	request_stat	attack_type	Source IP	Source Port	Destination IP	Destination Port	uri	response_code	F5_Seve
	HTTP Compliance Failure	11/8/13 10:...	Complianc...	blocked	Non-browser Clie...	192.168.31.75	50044	192.168.30.145	7179	sip:nm	0	Error
	HTTP Compliance Failure	11/8/13 10:...	Complianc...	blocked	Non-browser Clie...	192.168.31.75	44780	192.168.30.145	7179	/	0	Error
	Illegal Flow To URL	11/8/13 10:...	Invalid Co...	alerted	Forceful Browsing	192.168.31.75	44279	192.168.30.145	7179	/	0	Error
	Path Traversal	11/6/13 1:3...	Web Exploit	blocked	Path Traversal	192.168.31.75	56713	192.168.30.144	8443	/iissamples/sdk/asp/docs/winmsdp.exe	0	Error
	Path Travers	...	Web Exploit	blocked	Path Traversal	192.168.31.75	56711	192.168.30.144	8443	/iissamples/sdk/asp/docs/winmsdp.exe	0	Error
	Predictable R	...	Web Exploit	blocked	Predictable Reso...	192.168.31.75	56698	192.168.30.144	8443	/perl/	0	Error
	Predictable Resource Location	11/6/13 1:3...	Web Exploit	blocked	Predictable Reso...	192.168.31.75	56683	192.168.30.144	8443	/test/phpinfo.php	0	Error
	Predictable Resource Location	11/6/13 1:3...	Web Exploit	blocked	Predictable Reso...	192.168.31.75	56681	192.168.30.144	8443	/test/info.php	0	Error
	Information Leakage	11/6/13 1:3...	Information...	alerted	Information Leak...	192.168.31.75	56680	192.168.30.144	8443	/test.php	302	Error
	Command Execution	11/6/13 1:3...	Command ...	blocked	Command Execut...	192.168.31.75	56677	192.168.30.144	8443	/bin/test-cgi	0	Error
	Command Execution	11/6/13 1:3...	Command ...	blocked	Command Execut...	192.168.31.75	56675	192.168.30.144	8443	/bin/test-cgi	0	Error
	Information Leakage	11/6/13 1:3...	Information...	alerted	Information Leak...	192.168.31.75	56674	192.168.30.144	8443	/cgi-bin/printenv	302	Error
	Command Execution	11/6/13 1:3...	Command ...	blocked	Information Leak...	192.168.31.75	56673	192.168.30.144	8443	/bin/printenv	0	Error
	Information Leakage	11/6/13 1:3...	Information...	blocked	Information Leak...	192.168.31.75	56673	192.168.30.144	8443	/bin/printenv	0	Error
	Information Leakage	11/6/13 1:3...	Information...	alerted	Information Leak...	192.168.31.75	56672	192.168.30.144	8443	/cgi-bin/printenv	302	Error
	Command Execution	11/6/13 1:3...	Command ...	blocked	Information Leak...	192.168.31.75	56671	192.168.30.144	8443	/bin/printenv	0	Error
	Information Leakage	11/6/13 1:3...	Information...	blocked	Information Leak...	192.168.31.75	56671	192.168.30.144	8443	/bin/printenv	0	Error
	Predictable Resource Location	11/6/13 1:3...	Web Exploit	blocked	Predictable Reso...	192.168.31.75	56628	192.168.30.144	8443	/perl/samples/volscgi.pl	0	Error
	Predictable Resource Location	11/6/13 1:3...	Web Exploit	blocked	Predictable Reso...	192.168.31.75	56627	192.168.30.144	8443	/perl/samples/ndslogin.pl	0	Error
	Predictable Resource Location	11/6/13 1:3...	Web Exploit	blocked	Predictable Reso...	192.168.31.75	56626	192.168.30.144	8443	/perl/samples/lancgi.pl	0	Error
	Predictable Resource Location	11/6/13 1:3...	Web Exploit	blocked	Predictable Reso...	192.168.31.75	56625	192.168.30.144	8443	/perl/samples/env.pl	0	Error
25	Predictable Resource Location	11/6/13 1:3...	Web Exploit	blocked	Predictable Reso...	192.168.31.75	56624	192.168.30.144	8443	/perl/env.pl	0	Error
	Command Execution	11/6/13 1:3...	Command ...	blocked	Command Execut...	192.168.31.75	56574	192.168.30.144	8443	/bin/cgi-test.exe	0	Error

ID: 55250097, Desc: Path Traversal

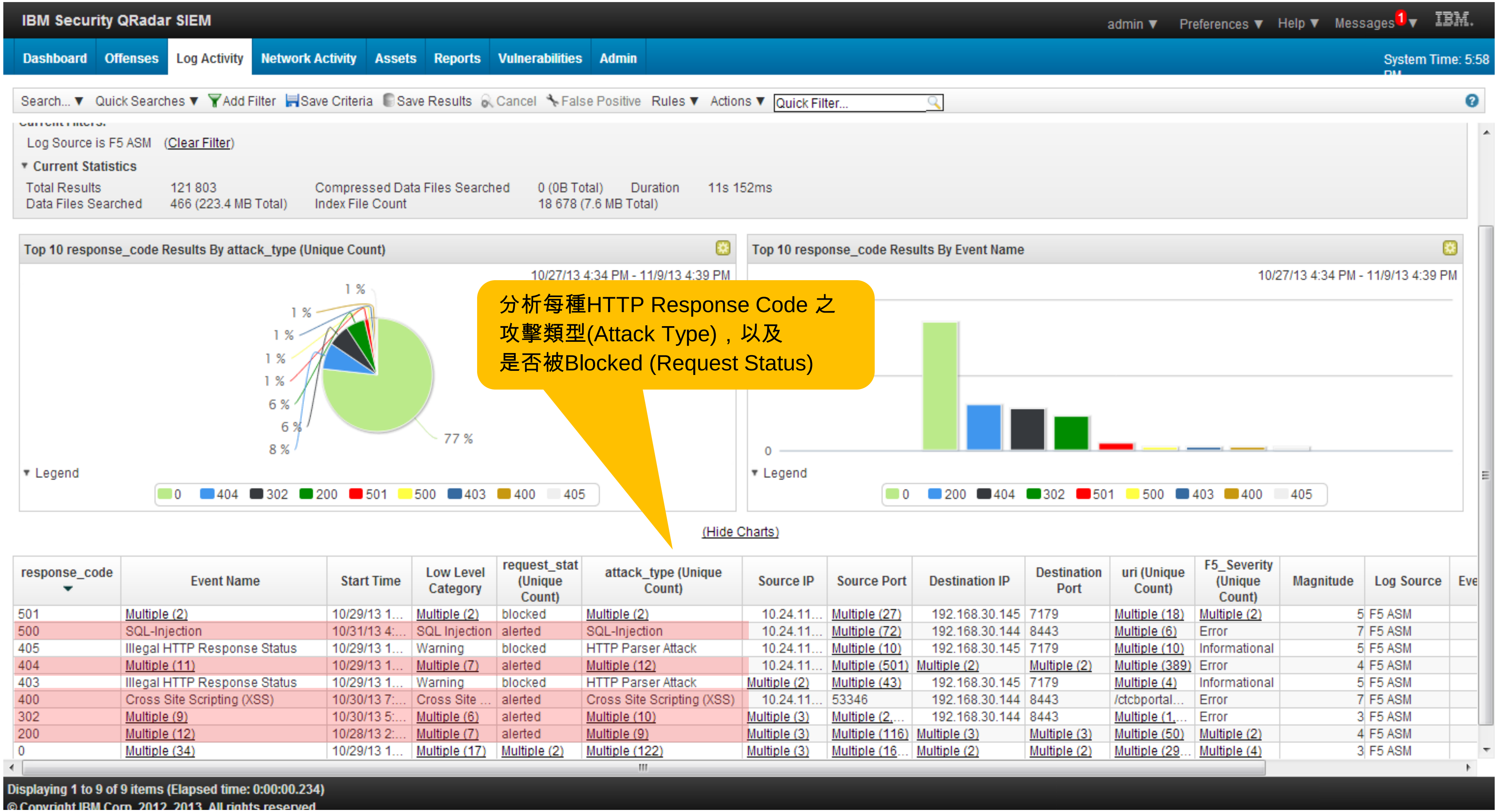
Displaying 1 to 40 of 121803 items (Elapsed time: 0:00:00.145)

© Copyright IBM Corp. 2012, 2013. All rights reserved.

Page: 1 Go < 1 2 3 ... 3046 >

© 2016 IBM Corporation

F5 ASM 日誌統計分析 – 回應代碼 v.s 攻擊



IBM Security QRadar SIEM
admin ▼ Preferences ▼ Help ▼ Messages 1 ▼ IBM.
Dashboard Offenses Log Activity Network Activity Assets Reports Vulnerabilities Admin
System Time: 5:58 PM
Search... ▼ Quick Searches ▼ Add Filter Save Criteria Save Results Cancel False Positive Rules ▼ Actions ▼ Quick Filter...

Current Filters:

Log Source is F5 ASM (Clear Filter)

▾ Current Statistics

Total Results	121 803	Compressed Data Files Searched	0 (0B Total)	Duration	11s 152ms
Data Files Searched	466 (223.4 MB Total)	Index File Count	18 678 (7.6 MB Total)		

Top 10 response_code Results By attack_type (Unique Count)

10/27/13 4:34 PM - 11/9/13 4:39 PM

1 %
1 %
1 %
1 %
1 %
6 %
6 %
8 %
77 %
▾ Legend
🟩 0 🟦 404 ■ 302 🟩 200 🟥 501 🟨 500 🟦 403 🟧 400 □ 405

Top 10 response_code Results By Event Name

10/27/13 4:34 PM - 11/9/13 4:39 PM

分析每種HTTP Response Code 之攻擊類型(Attack Type)，以及是否被Blocked (Request Status)

(Hide Charts)

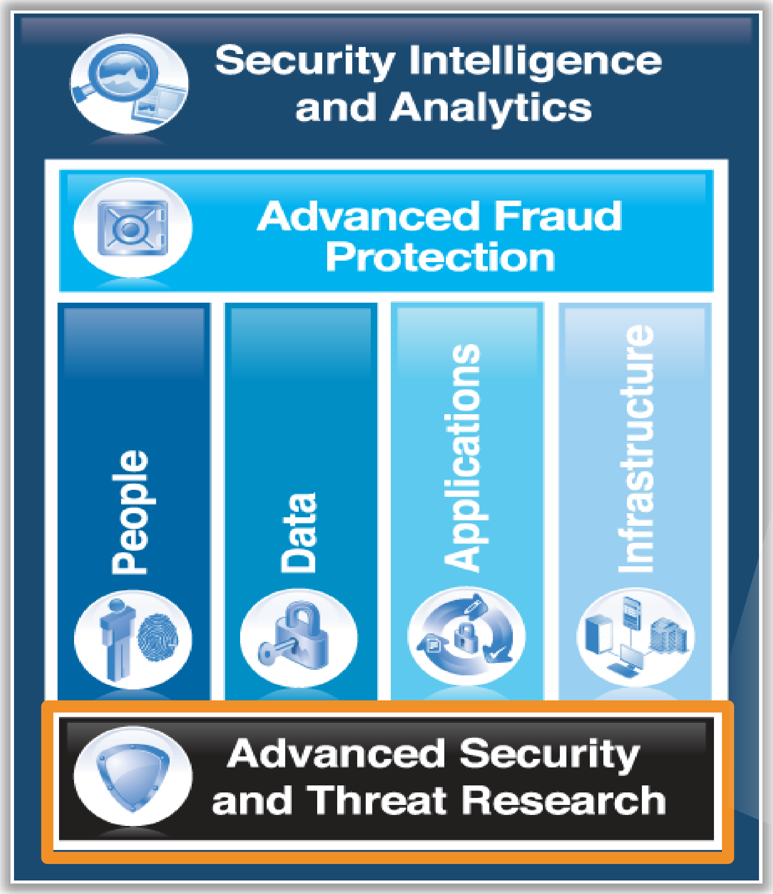
response_code ▾	Event Name	Start Time	Low Level Category	request_stat (Unique Count)	attack_type (Unique Count)	Source IP	Source Port	Destination IP	Destination Port	uri (Unique Count)	F5_Severity (Unique Count)	Magnitude	Log Source	Eve
501	Multiple (2)	10/29/13 1...	Multiple (2)	blocked	Multiple (2)	10.24.11...	Multiple (27)	192.168.30.145	7179	Multiple (18)	Multiple (2)	5	F5 ASM	
500	SQL-Injection	10/31/13 4:...	SQL Injection	alerted	SQL-Injection	10.24.11...	Multiple (72)	192.168.30.144	8443	Multiple (6)	Error	7	F5 ASM	
405	Illegal HTTP Response Status	10/29/13 1...	Warning	blocked	HTTP Parser Attack	10.24.11...	Multiple (10)	192.168.30.145	7179	Multiple (10)	Informational	5	F5 ASM	
404	Multiple (11)	10/29/13 1...	Multiple (7)	alerted	Multiple (12)	10.24.11...	Multiple (501)	Multiple (2)	Multiple (2)	Multiple (389)	Error	4	F5 ASM	
403	Illegal HTTP Response Status	10/29/13 1...	Warning	blocked	HTTP Parser Attack	Multiple (2)	Multiple (43)	192.168.30.145	7179	Multiple (4)	Informational	5	F5 ASM	
400	Cross Site Scripting (XSS)	10/30/13 7:...	Cross Site ...	alerted	Cross Site Scripting (XSS)	10.24.11...	53346	192.168.30.144	8443	/ctcbportal...	Error	7	F5 ASM	
302	Multiple (9)	10/30/13 5:...	Multiple (6)	alerted	Multiple (10)	Multiple (3)	Multiple (2,...	192.168.30.144	8443	Multiple (1,...	Error	3	F5 ASM	
200	Multiple (12)	10/28/13 2:...	Multiple (7)	alerted	Multiple (9)	Multiple (3)	Multiple (116)	Multiple (3)	Multiple (3)	Multiple (50)	Multiple (2)	4	F5 ASM	
0	Multiple (34)	10/29/13 1...	Multiple (17)	Multiple (2)	Multiple (122)	Multiple (3)	Multiple (16...	Multiple (2)	Multiple (2)	Multiple (29...	Multiple (4)	3	F5 ASM	

Displaying 1 to 9 of 9 items (Elapsed time: 0:00:00.234)

© Copyright IBM Corp. 2012, 2013. All rights reserved.

© 2016 IBM Corporation

IBM X-Force


Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

X-Force 的使命：

- 監控並評估快速變化的威脅環境；
- 研究新的攻擊技術，提供面向明天安全挑戰的保護；
- 教育我們的客戶和公眾；
- 發佈威脅情報，使得 IBM 安全解決方案更加智能；

IBM X-Force 監控和分析不斷變化的資安威脅環境

覆蓋面

20,000+ 多台合約設備

3,700+ 全球託管用戶

15B+ 每天事件

133 受監控的國家（MSS）

1,000+ 安全專利

100M+ 客戶免於詐欺交易

深度

23B 分析的 web 頁面和圖片

7M 每天垃圾郵件 & 釣魚攻擊

81K 記錄的漏洞

860K 惡意 IP 地址

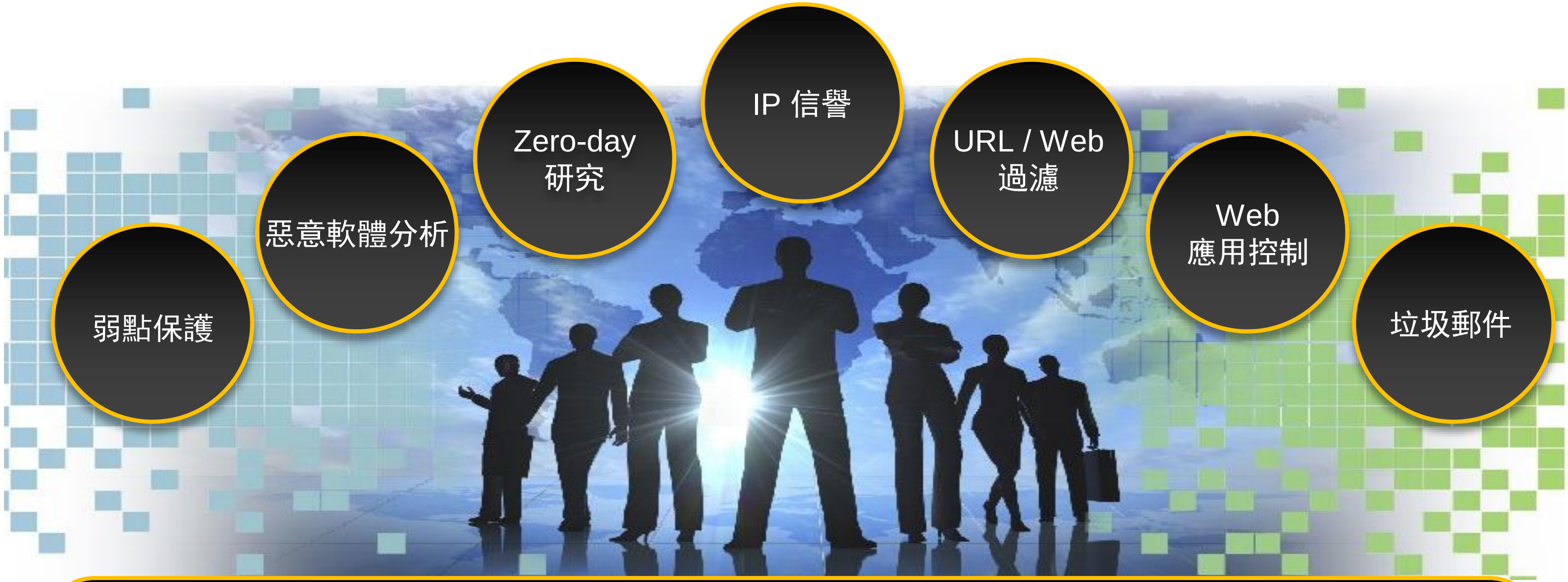
1000+ 每天收集惡意軟體樣本

上百萬惡意軟體樣本

© 2016 IBM Corporation

IBM X-Force® 研發

專家級分析並在全球分享數據

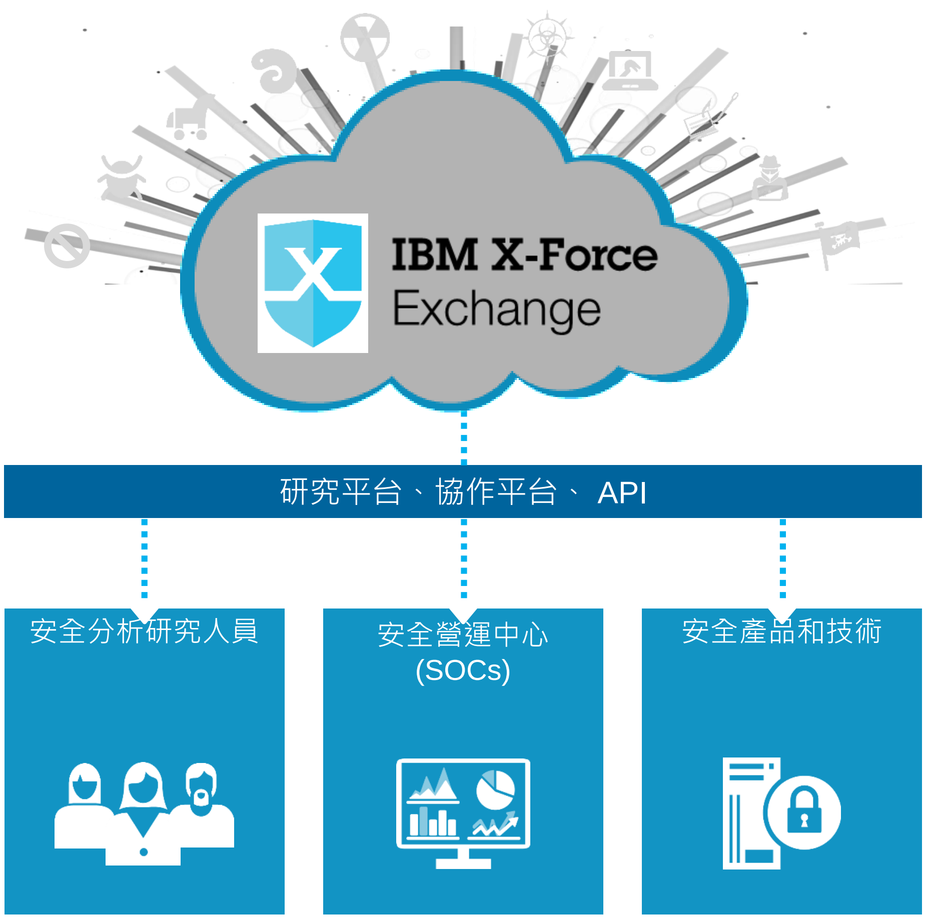


The IBM X-Force 使命

- **監控**並評估快速變化的資訊安全威脅環境；
- **研究**新的攻擊技術並開發對未來安全威脅的保護
- **教育**用戶和大眾
- **整合並**分發安全保護和智能，使得 IBM 解決方案更加智能；

© 2016 IBM Corporation

IBM X-Force Exchange: http://xforce.ibmcloud.com



研究平台、協作平台、 API

安全分析研究人員

安全營運中心
(SOCs)

安全產品和技術

全新的平台使用、共享安全情報
IBM X-Force Exchange 是：

開放

強健的平台，用於存取豐富的安全情報數據

可行的

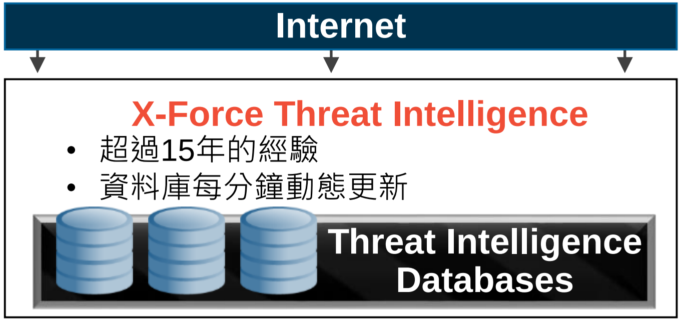
整合化的解決方案幫助快速阻止威脅

社交化

分享安全情報的協作平台

IBM X-Force 的信譽和影響力為其背書

資安情報共享開放平台 - IBM X-Force Exchange



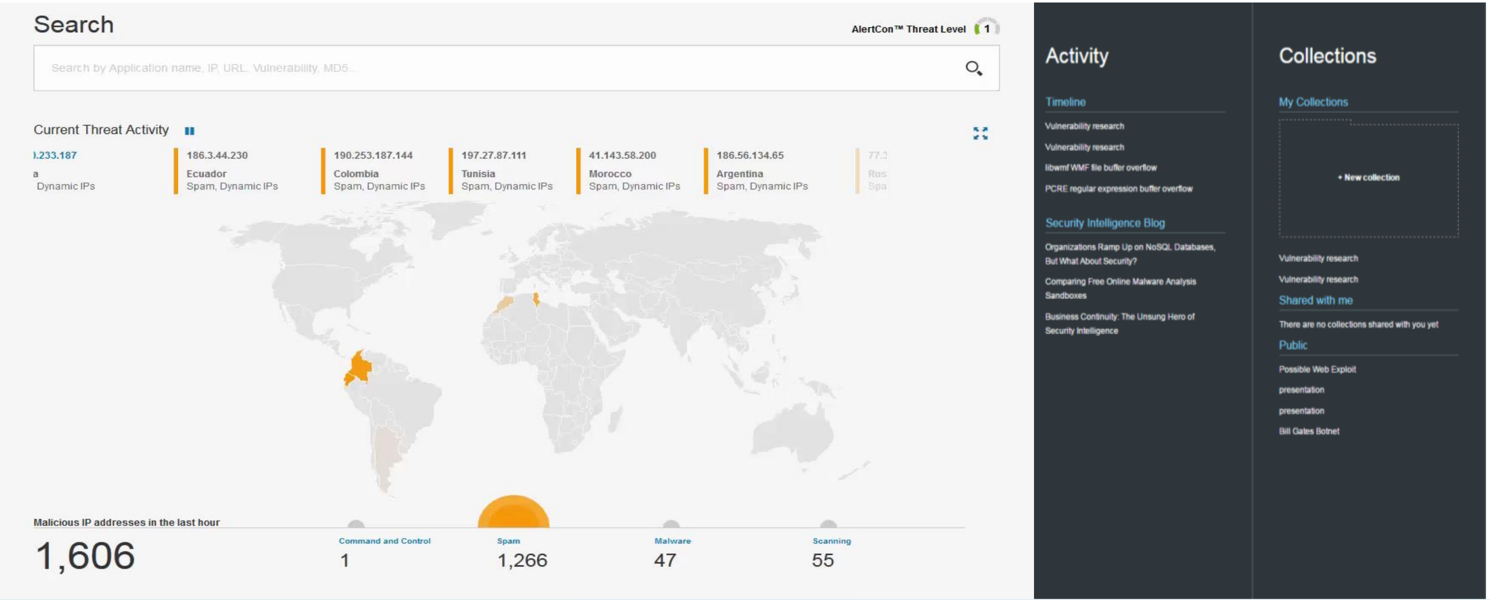
Internet

X-Force Threat Intelligence

- 超過15年的經驗
- 資料庫每分鐘動態更新

Threat Intelligence Databases

http://xforce.ibmcloud.com



Search

AlertCon™ Threat Level 1

Search by Application name, IP, URL, Vulnerability, MD5...

Current Threat Activity

).233.187
a
Dynamic IPs

186.3.44.230
Ecuador
Spam, Dynamic IPs

190.253.187.144
Colombia
Spam, Dynamic IPs

197.27.87.111
Tunisia
Spam, Dynamic IPs

41.143.58.200
Morocco
Spam, Dynamic IPs

186.56.134.65
Argentina
Spam, Dynamic IPs

77.
Rus
Spa

Malicious IP addresses in the last hour

1,606

Command and Control	Spam	Malware	Scanning
1	1,266	47	55

Activity

Timeline

- Vulnerability research
- Vulnerability research
- libwmf WMF file buffer overflow
- PCRE regular expression buffer overflow

Security Intelligence Blog

- Organizations Ramp Up on NoSQL Databases, But What About Security?
- Comparing Free Online Malware Analysis Sandboxes
- Business Continuity: The Unsung Hero of Security Intelligence

Collections

My Collections

+ New collection

- Vulnerability research
- Vulnerability research

Shared with me

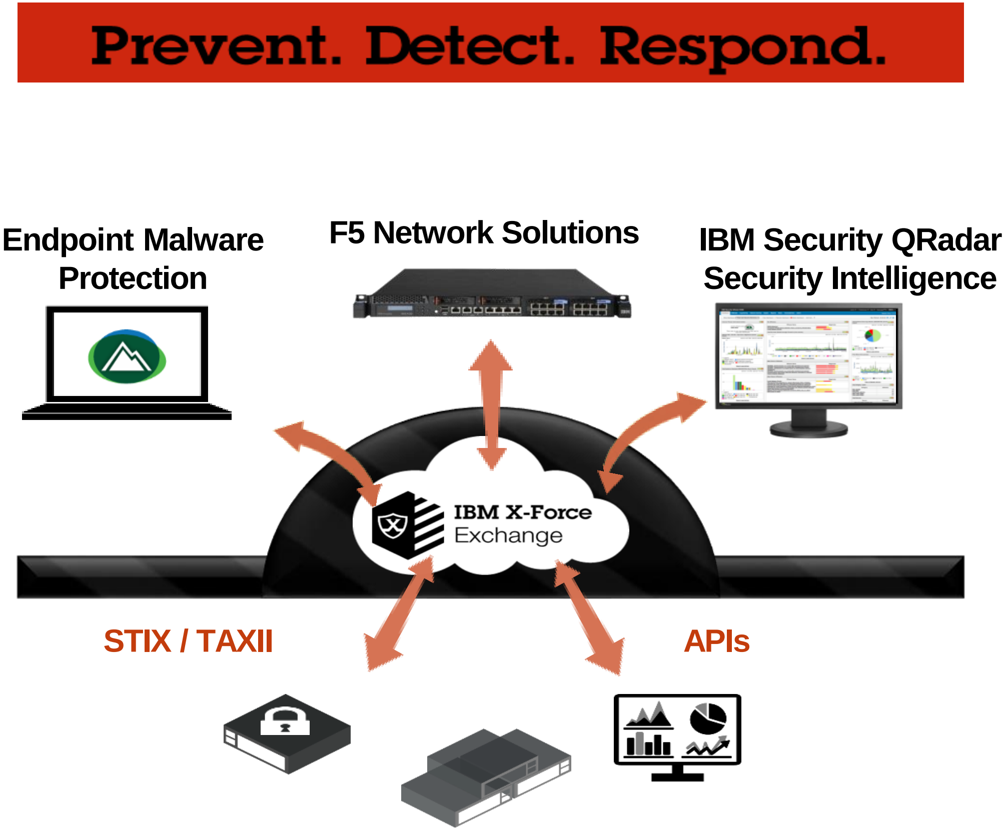
There are no collections shared with you yet

Public

- Possible Web Exploit
- presentation
- presentation
- Bill Gates Botnet

可行動

綜合的解決方案，幫助快速阻止威脅


Prevent. Detect. Respond.
Endpoint Malware Protection
F5 Network Solutions
IBM Security QRadar Security Intelligence
IBM X-Force Exchange
STIX / TAXII
APIs

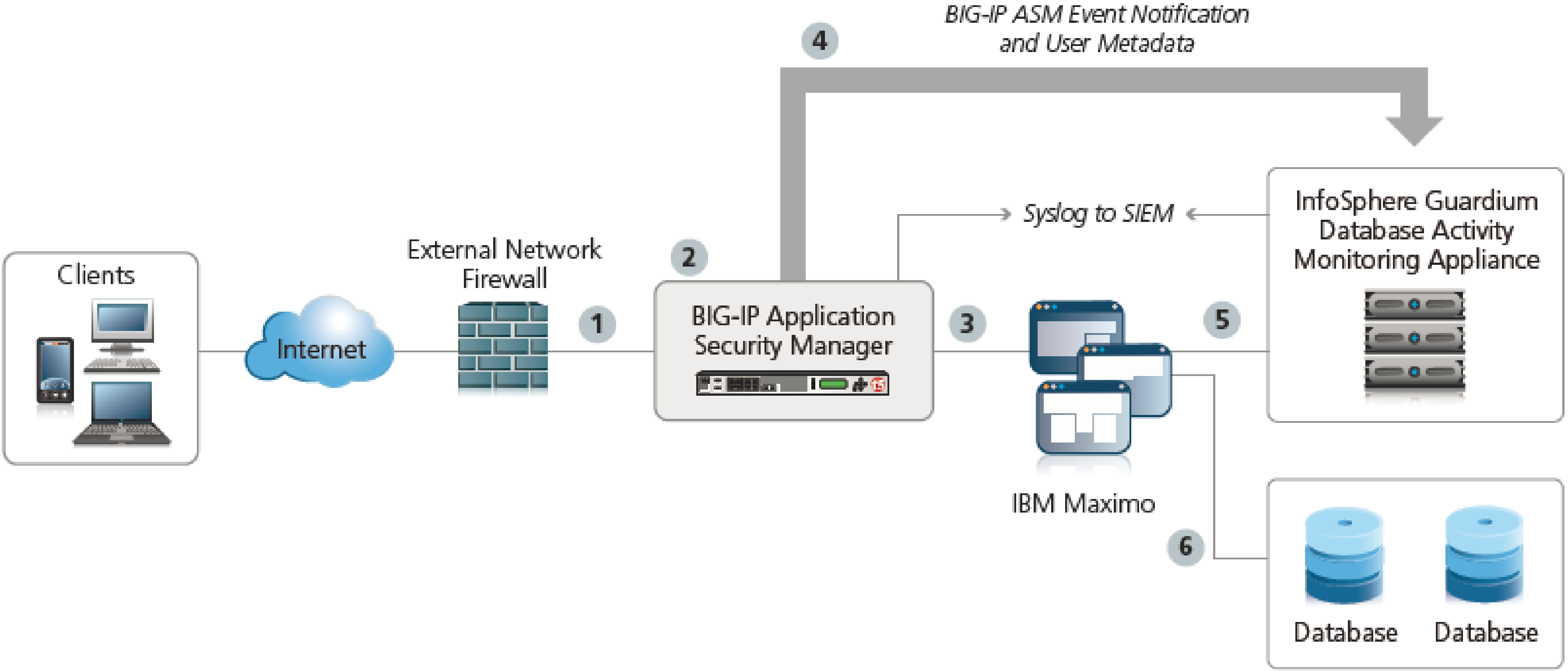
IBM 威脅保護系統的基石

- 威脅情報每分每秒都在發生著變化；
- 與 IBM 安全產品自動化整合，交付可行動的情報資訊；

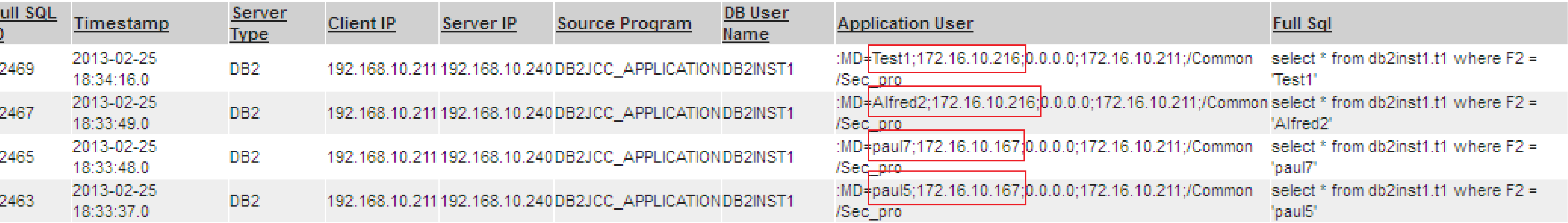
推送資訊到執行點，提供及時地保護

- 設計支持第三方整合，支持 STIX 和 TAXII, 建立了自動化威脅情報資訊共享的標準；
- 利用 API ，您的安全產品也可獲得情報資訊；

F5 ASM & Guardium for application user identifier



Guardium sample report – end user identifier by F5 ASM



ull SQL)	Timestamp	Server Type	Client IP	Server IP	Source Program	DB User Name	Application User	Full Sql
2469	2013-02-25 18:34:16.0	DB2	192.168.10.211	192.168.10.240	DB2JCC_APPLICATION	DB2INST1	:MD=Test1;172.16.10.216;0.0.0.0;172.16.10.211;/Common /Sec_pro	select * from db2inst1.t1 where F2 = 'Test1'
2467	2013-02-25 18:33:49.0	DB2	192.168.10.211	192.168.10.240	DB2JCC_APPLICATION	DB2INST1	:MD=Alfred2;172.16.10.216;0.0.0.0;172.16.10.211;/Common /Sec_pro	select * from db2inst1.t1 where F2 = 'Alfred2'
2465	2013-02-25 18:33:48.0	DB2	192.168.10.211	192.168.10.240	DB2JCC_APPLICATION	DB2INST1	:MD=paul7;172.16.10.167;0.0.0.0;172.16.10.211;/Common /Sec_pro	select * from db2inst1.t1 where F2 = 'paul7'
2463	2013-02-25 18:33:37.0	DB2	192.168.10.211	192.168.10.240	DB2JCC_APPLICATION	DB2INST1	:MD=paul5;172.16.10.167;0.0.0.0;172.16.10.211;/Common /Sec_pro	select * from db2inst1.t1 where F2 = 'paul5'

© 2016 IBM Corporation

IBM Guardium 產品架構

Data & File Activity Monitoring

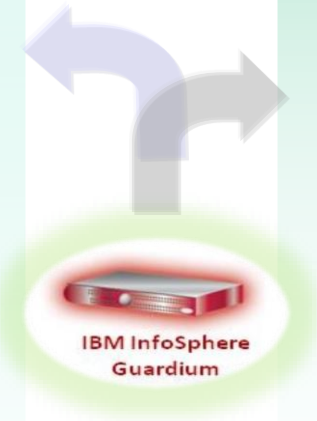
For data security & compliance

Standard DAM

- 資料發現與分類
- 即時活動監控
- 應用程式使用者解析
- 安全告警及稽核報告
- 合規流程

Advanced DAM

- 未獲授權連線阻斷
- 使用者隔離
- 機敏資料遮罩



硬體，軟體或虛擬裝置

Vulnerability Assessment

Best practice & secure configuration

- 組態評估
- 弱點評估
- 弱點掃描
- 建議的補救措施
- 資料保護
- 組態稽核系統
- 權限報告

Central Management & Aggregation

Manage and use large deployments as a single federated system

Guardium 支援最複雜的 IT 環境…

支援資料庫、大數據環境、檔案等

應用程式

- IBM CICS WebSphere
- ORACLE Siebel PeopleSoft E-Business
- SAP

資料庫

- IBM DB2 Informix
- IBM IMS
- MariaDB FOUNDATION
- ORACLE
- Microsoft SQL Server
- SYBASE
- MySQL
- PostgreSQL

資料倉儲

- IBM Netezza PureData for Analytics
- ORACLE Exadata
- TERADATA
- SAP HANA
- Greenplum DB

海量資料環境

- hadoop
- SQL
- IBM InfoSphere BigInsights
- Cassandra
- cloudera
- mongoDB
- hortonworks
- CouchDB
- Pivotal

雲端環境

- IBM SOFTLAYER
- amazon webservices™
- Windows Azure

資料庫工具

- IBM Optim Archival
- IBM Master Data Management
- IBM Data Stage

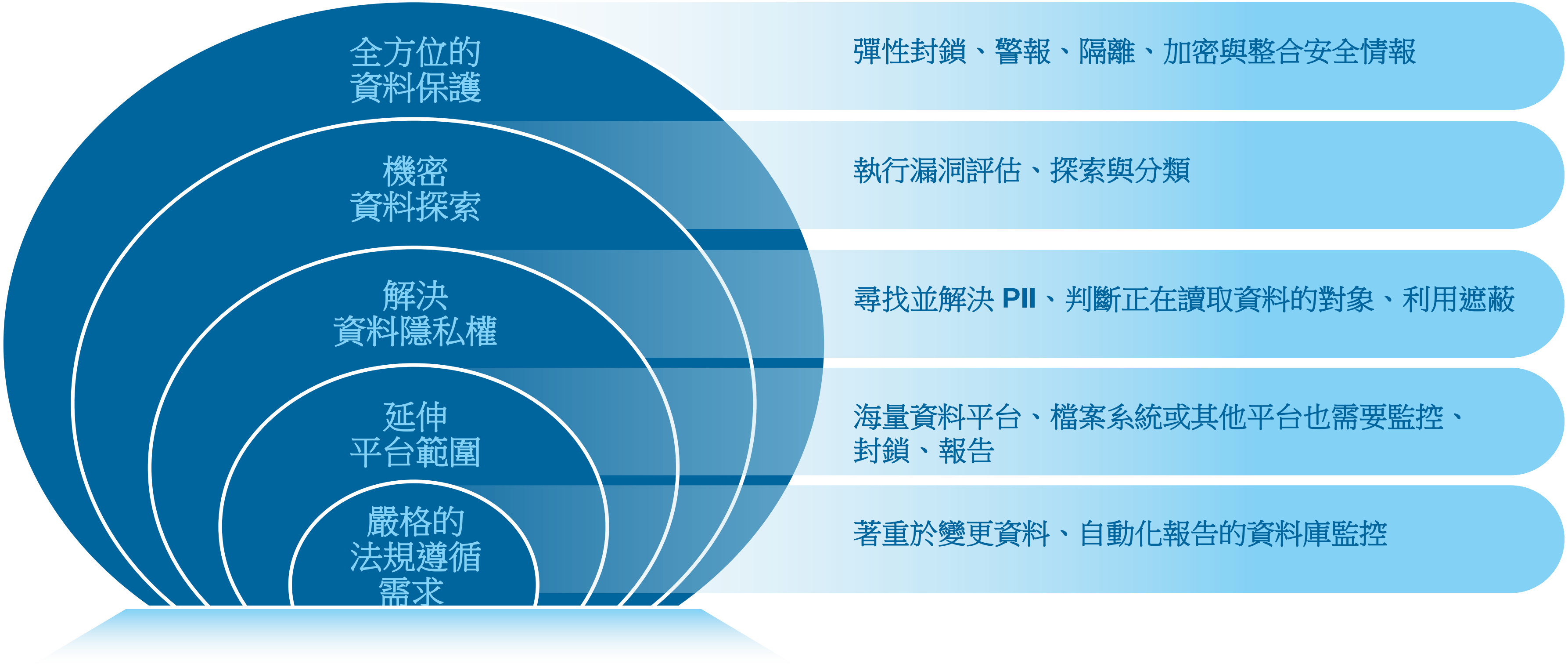
企業 內容管理程式

- Microsoft Office SharePoint

檔案

- IBM VSAM z/OS Datasets
- FTP
- Windows、Linux、Unix

IBM Guardium 可支援整個資料保護過程



彈性封鎖、警報、隔離、加密與整合安全情報

執行漏洞評估、探索與分類

尋找並解決 **PII**、判斷正在讀取資料的對象、利用遮蔽

海量資料平台、檔案系統或其他平台也需要監控、封鎖、報告

著重於變更資料、自動化報告的資料庫監控

© 2016 IBM Corporation

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, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM

IBM **Security**

Intelligence. Integration. Expertise.

© Copyright IBM Corporation 2016. 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.