



ICAS 網路入侵偵測日誌雲端分析平台

ICAS: An inter-VM IDS-log Cloud Analysis System

Yao-Tsung Wang

jazz@nchc.org.tw

Wei-Yu Chen

waue@nchc.org.tw



專家說：雲端每個環節都有安全問題

ZDNet Taiwan - 專家談雲端：每個環節都有安全問題 - 新聞

2010/08/10 19:50:02

專家談雲端：每個環節都有安全問題

ZDNet記者曠文濤／台北報導 雲端的安全問題不是無解，只是不管是雲端服務供應商或者想要建立私有雲的企業用戶，都必須考量到每個環節。

微軟亞太區全球技術支援中心專案經理、同時也是ZDNet專欄作家林宏嘉今（10）日在ZDNet舉行的IT Priorities圓桌論壇中表示，**雲端的安全議題涉及了IaaS、PaaS乃至於SaaS的每個層面**。當然有些問題是原本就存在：例如在討論到IaaS時，就涉及到了**機房的管理**和**硬體設備的可用性**等；但是講到PaaS時，企業用戶倘若要選擇開原碼的作業系統，必須考量到後續的**安全維護**；在SaaS的層次，企業用戶必須確保每一個分區（partition）的安全更新和**資料安全**。

目前正如火如荼建立台灣第一個校園私有雲的台大計算機及資訊網路中心主任孫雅麗則呼應道，Amazon的雲端服務證實了在Hypervisor層有駭客入侵，也就是意味著過去大家在討論如何防範**虛擬機器的資料安全**，但是威脅已經深化到了更下一層。這些問題都有待解決。

「有些問題甚至是來自於內部，舉例而言，MIS可能會把存在記憶體裡的資料倒出來，或者在Hypervisor層就植入了可以蒐集資料的程式，」孫雅麗說。

安全議題是目前台灣企業對雲端持保留態度的最大主因，這也是何以台灣的大型企業對於雲端的想法，還是
偏好建立私有雲。畢竟對用戶而言，資料放在自己家，還和其他企業，甚至具競爭對手「共處」，

雲端資安的範疇

用雲端
處理資安

**Dealing Security
issues using Cloud**

**Data Security
In the Cloud**

雲端資料
安全性

雲內部
的資安管制

**Security Issues
Inside the Cloud**

端本身
的資安威脅

**Security Threats
to Internet of Things**

先來談談「端的安全」

用雲端
處理資安

**Dealing Security
issues using Cloud**

**Data Security
In the Cloud**

雲內部
的資安管制

**Security Issues
Inside the Cloud**

雲端資料
安全性

端本身
的資安威脅

**Security Threats
to Internet of Things**

以前你只有電腦需要防毒，現在



端

symbian
OS



多元，中小廠

Diversify ,
SMB

物聯網的時代來臨

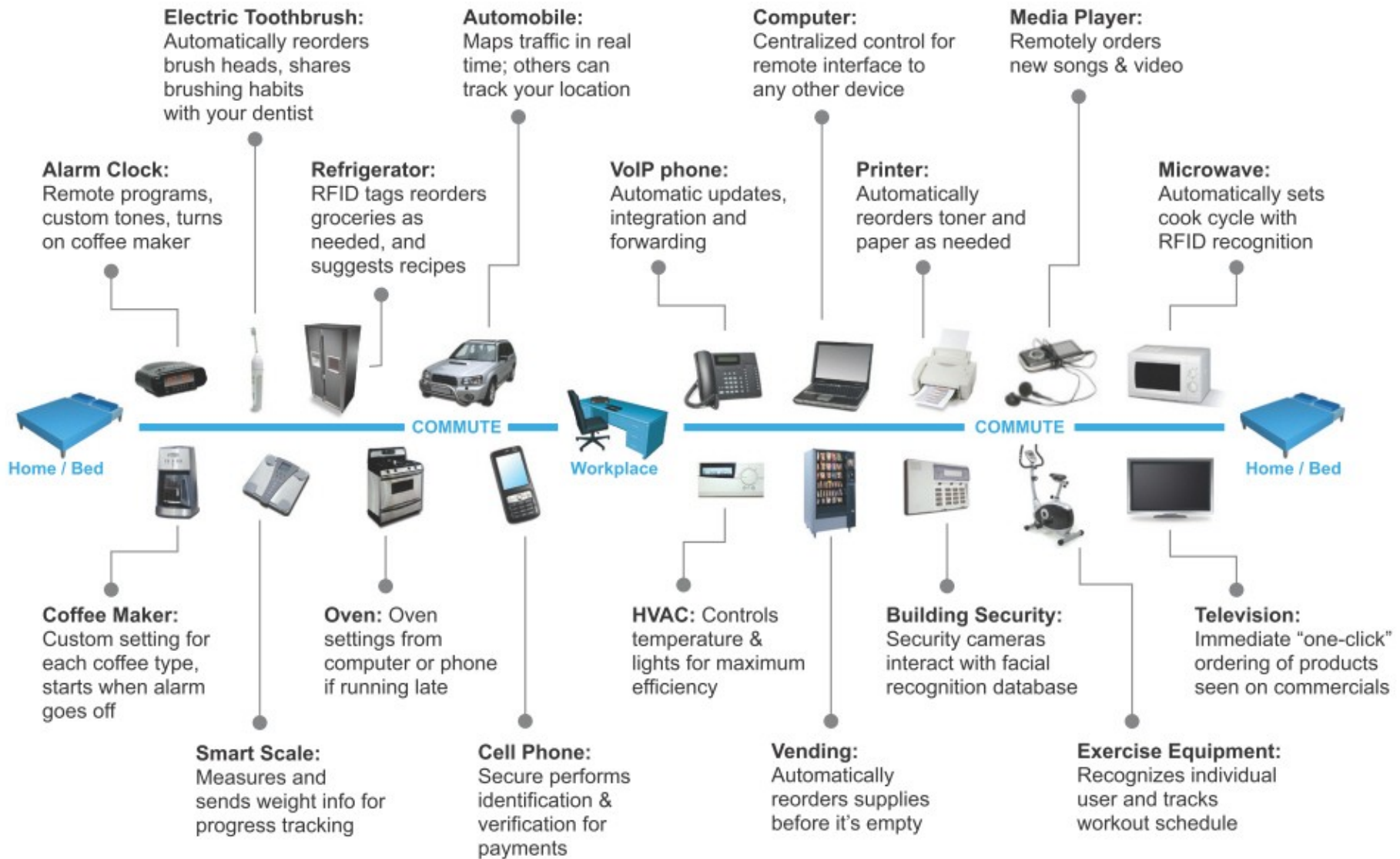
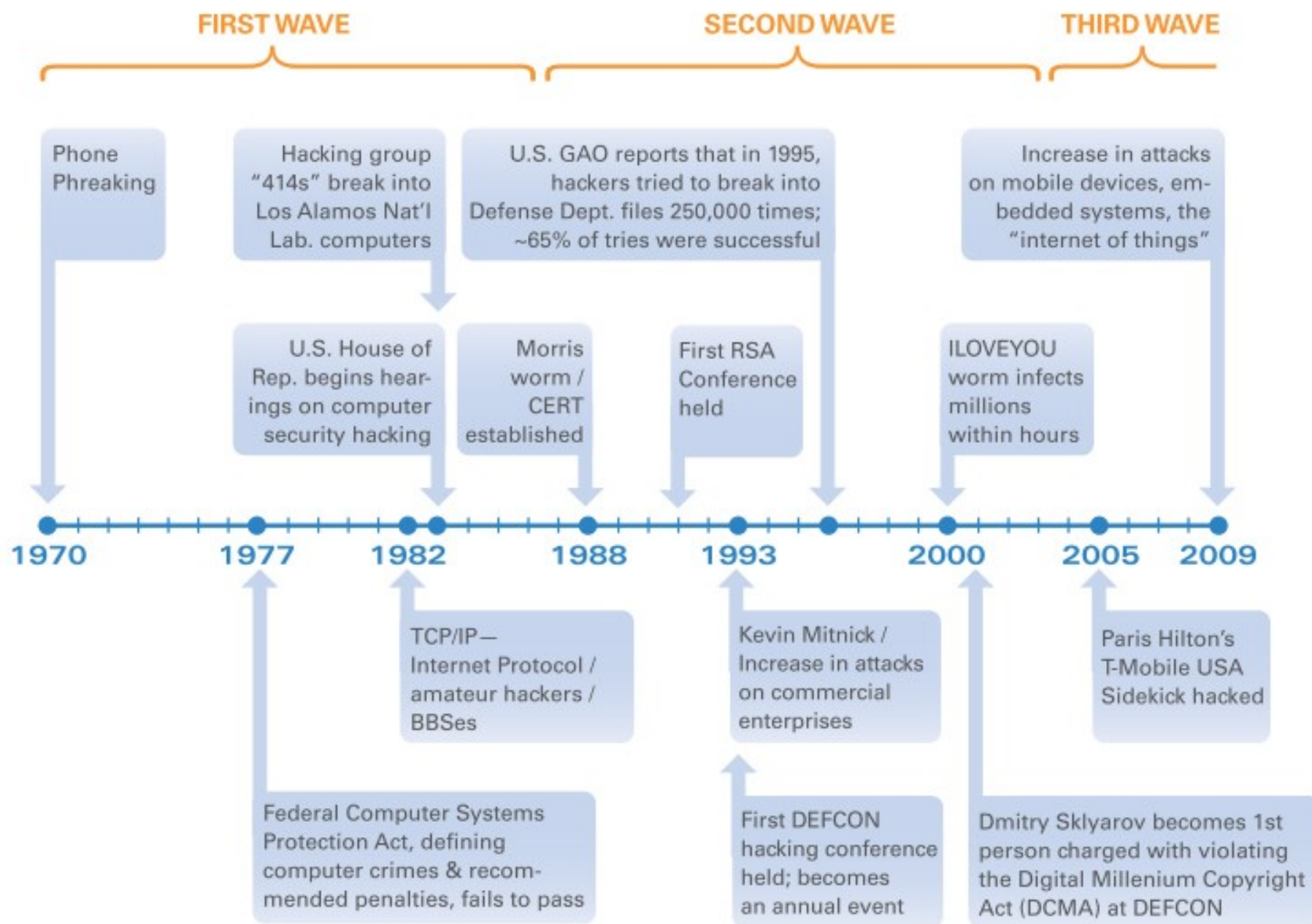
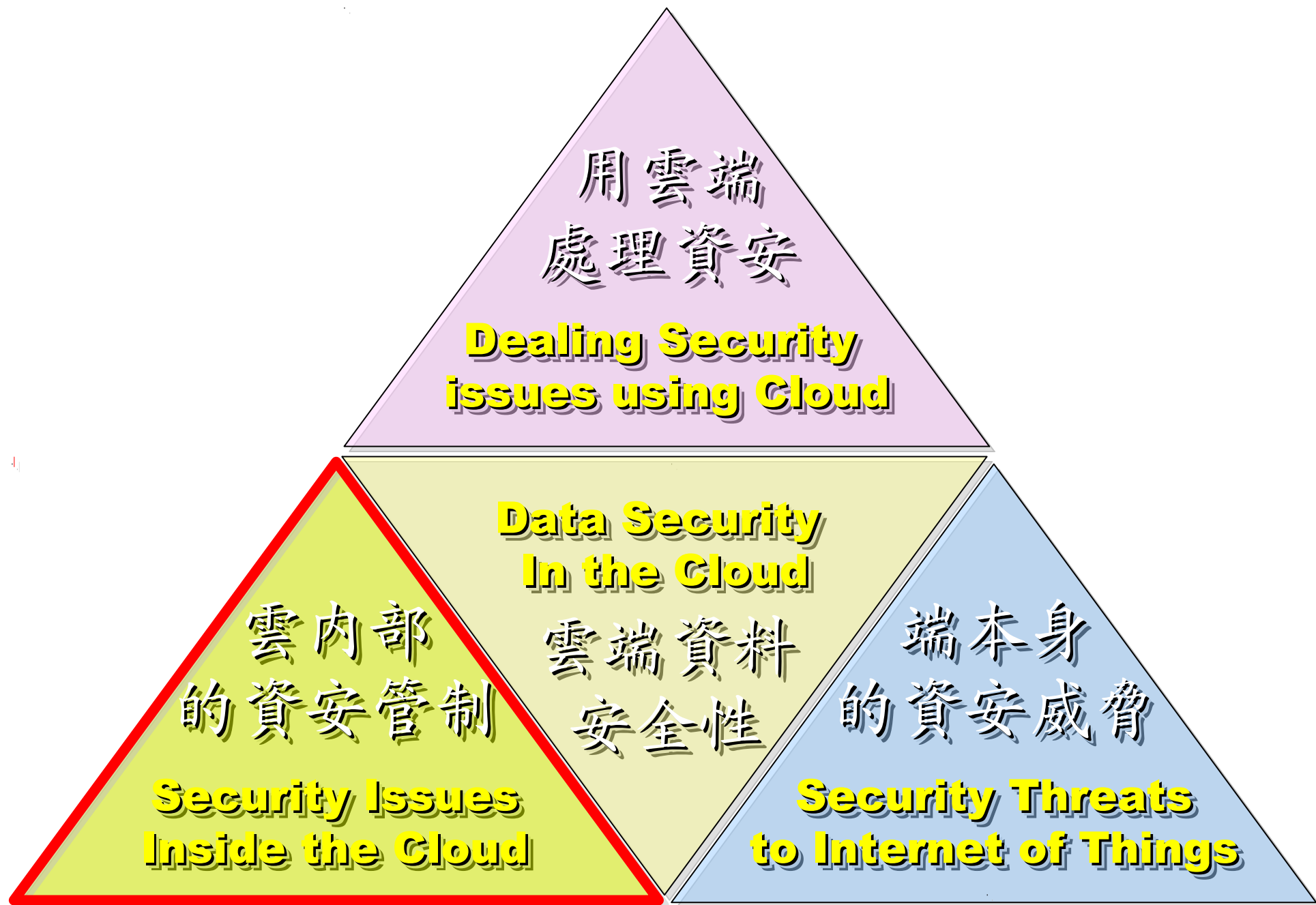


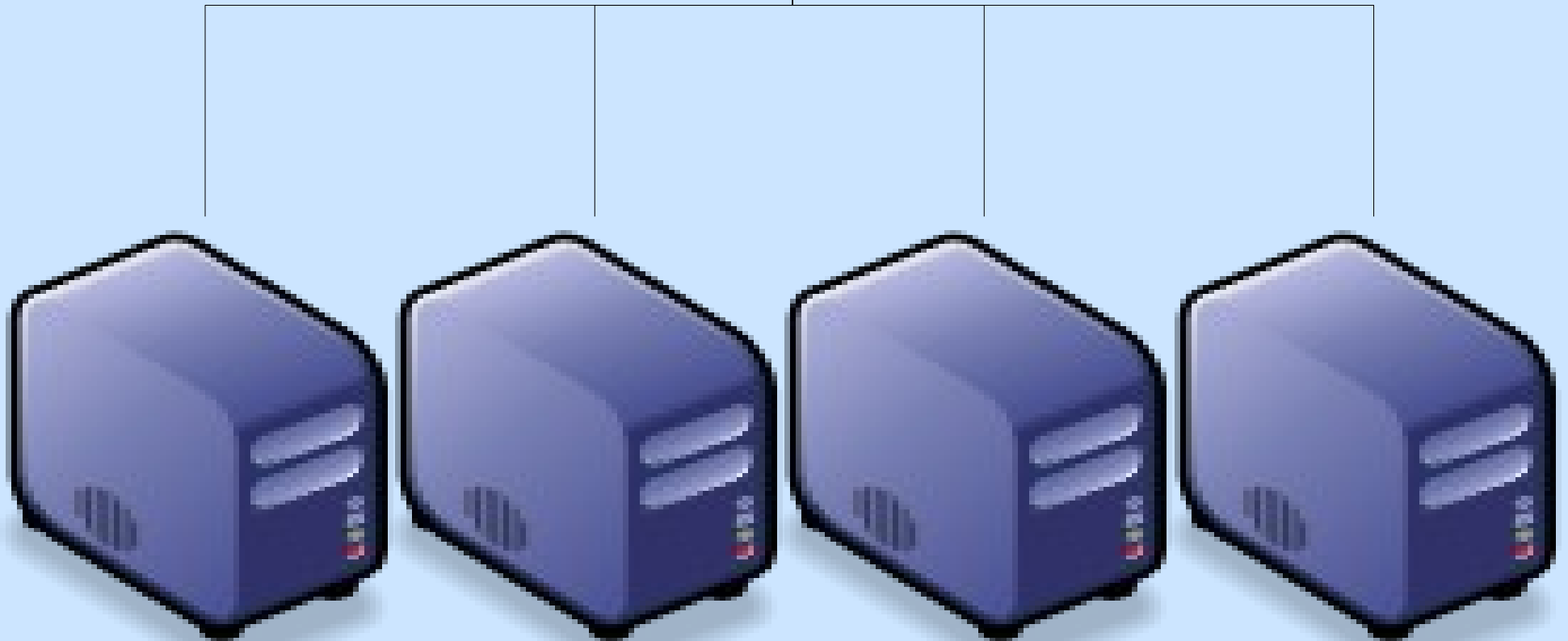
Figure 3. The Internet of Things

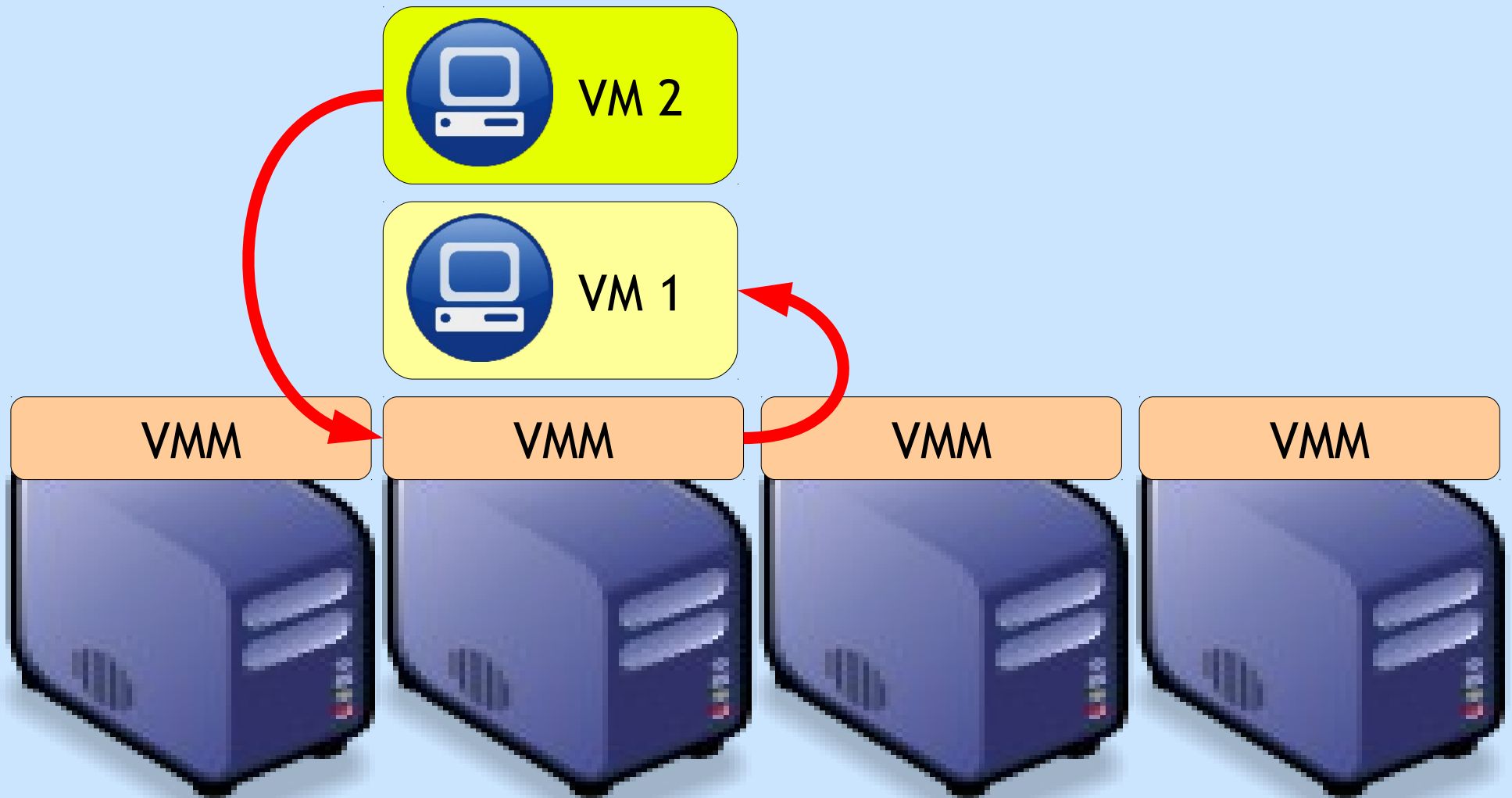
第三波網路入侵對象將鎖定在『物聯網』



再來談談「雲的安全」

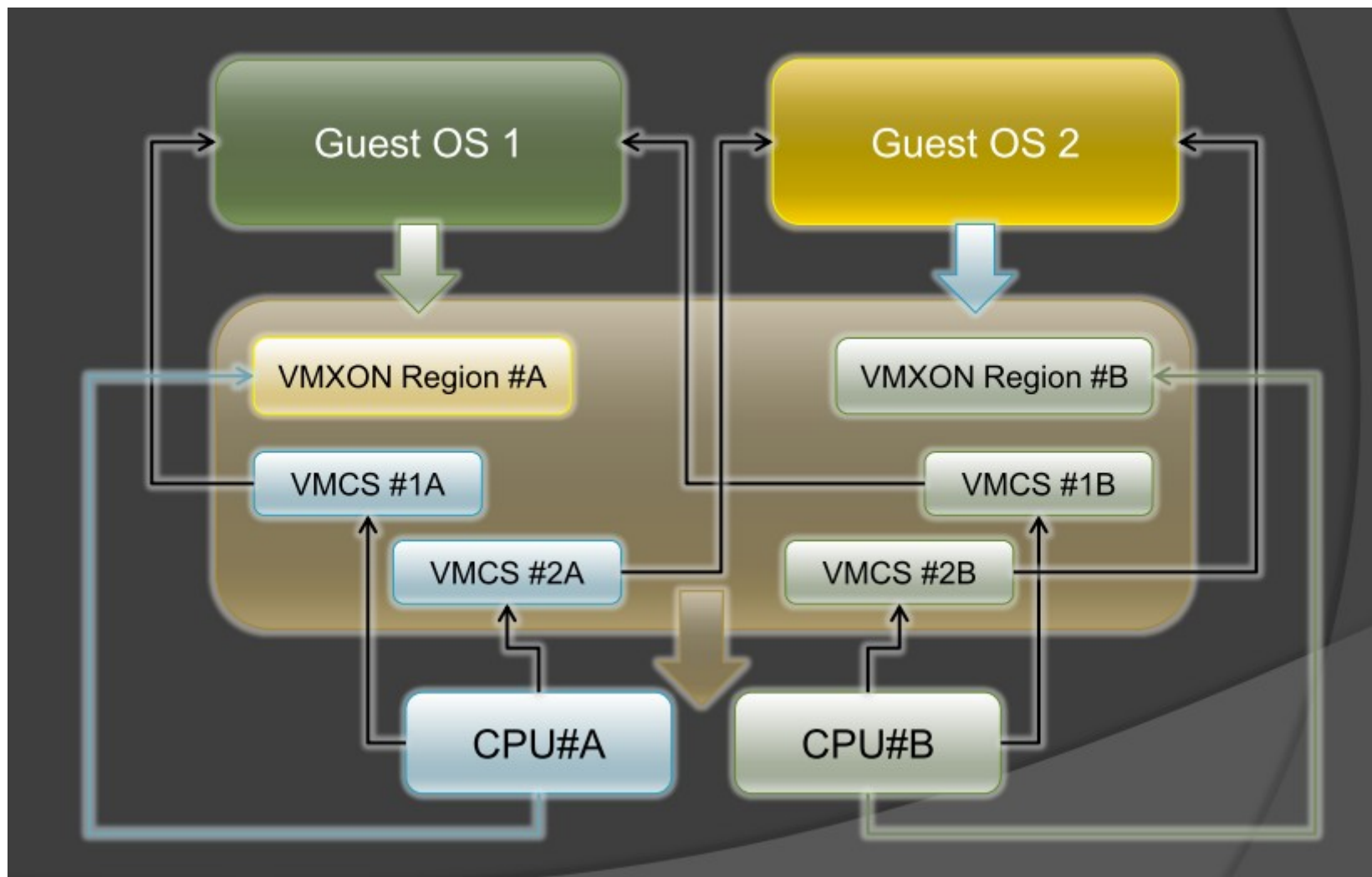






虛擬化衍生的新興資安問題

透過虛擬機器，竊取鍵盤輸入、植入後門



圖片來源： Hacks in Taiwan Conference 2010

http://www.hitcon.org/hit2010/download/6_New%20Battlefield%20For%20Malware%20Game.pdf

王大寶 & PK / Hypervisor - New Battlefield For Malware Game 虛擬機 - 惡意程式攻防的新戰場



Virtual Switch



VM 2



VM 1

VMM

VMM

VMM

VMM



三談「資料安全」

用雲端
處理資安

**Dealing Security
issues using Cloud**

**Data Security
In the Cloud**

雲端資料
安全性

雲內部
的資安管制

**Security Issues
Inside the Cloud**

端本身
的資安威脅

**Security Threats
to Internet of Things**

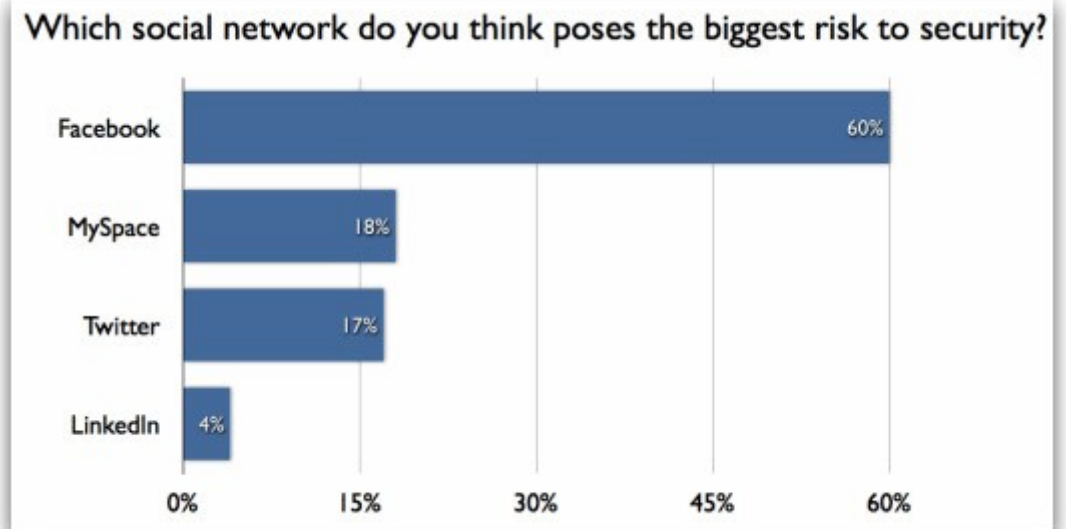
Ex. 無名照片外流、臉書個資外洩

轟動一時黑澀會妹妹容瑄親密自拍照片外流



圖片來源：

[Wikileaks and Facebook Privacy / Security: Do we care?](#)



圖片來源：

Report Ranks Facebook As Greatest Corporate Security Risk

<http://www.allfacebook.com/facebook-corporate-risk-2010-02>

進入今天的主題：用雲端處理傳統資安問題

今天的重點

用雲端
處理資安

**Dealing Security
issues using Cloud**

**Data Security
In the Cloud**

雲端資料
安全性

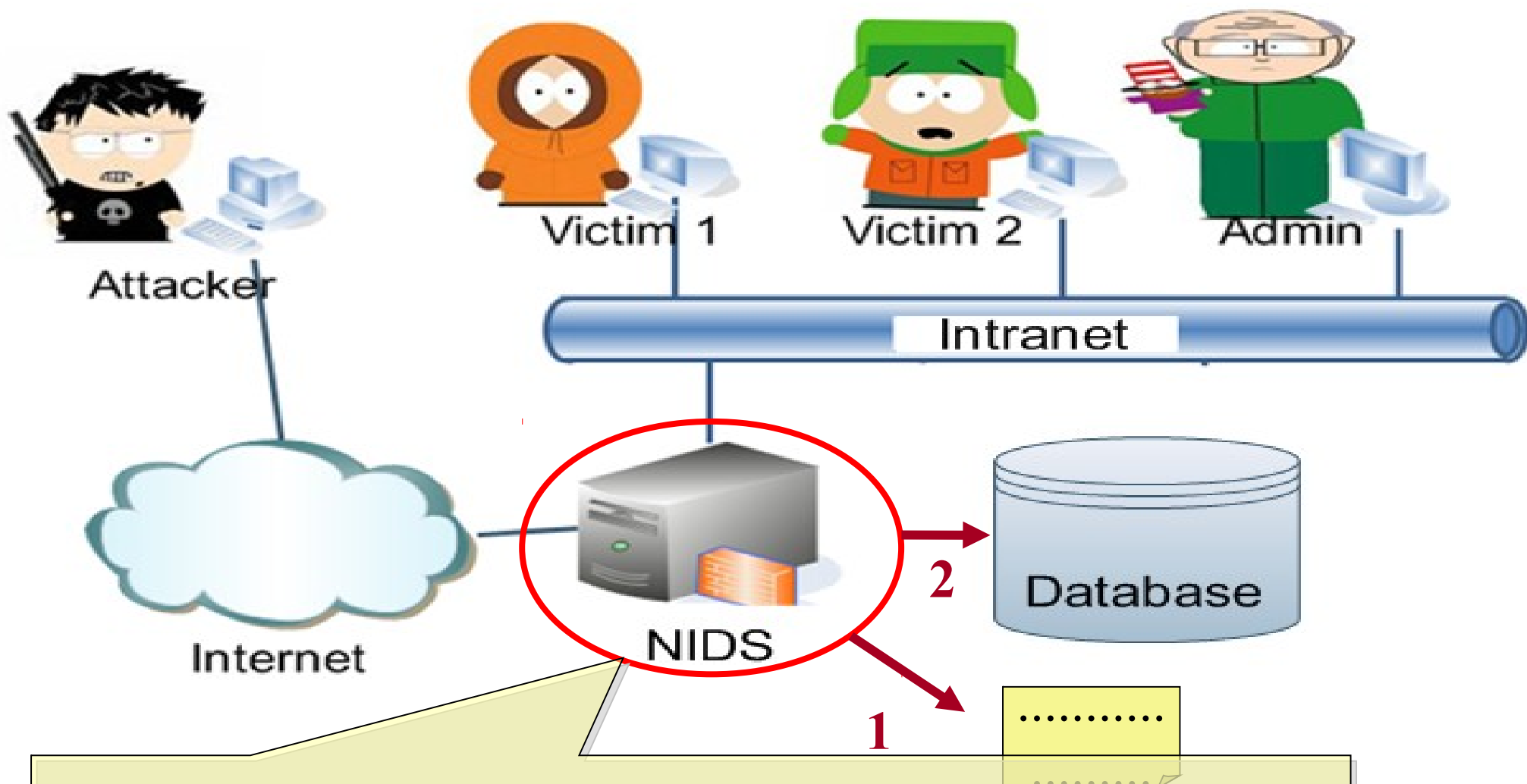
雲內部
的資安管制

**Security Issues
Inside the Cloud**

端本身
的資安威脅

**Security Threats
to Internet of Things**

使用入侵偵測系統 (NIDS) 來找出入侵訊息



當入侵偵測系統偵測到網路上有異常封包時，就會產生警訊以告知有攻擊發生。警訊通常有兩種形式：

1. 紀錄成 log 檔
2. 紀錄到資料庫

傳統 NIDS 的警訊型態 (1) 紀錄在日誌檔內

入侵偵測系統所產生警訊日誌檔內一小段內容

[**] [1:538:15] NETBIOS SMB IPC\$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
09/04-17:53:56.363811 168.150.177.165:1051 -> 168.150.177.166:139
TCP TTL:128 TOS:0x0 ID:4000 IpLen:20 DgmLen:138 DF
AP Seq: 0x2E589B8 Ack: 0x642D47F9 Win: 0x4241 TcpLen: 20

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
09/04-17:53:56.385573 168.150.177.164:1032 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:80 IpLen:20 DgmLen:161
Len: 133

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
09/04-17:53:56.386910 168.150.177.164:1032 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:82 IpLen:20 DgmLen:161
Len: 133

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
09/04-17:53:56.388244 168.150.177.164:1032 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:84 IpLen:20 DgmLen:161
Len: 133

[**] [1:538:15] NETBIOS SMB IPC\$ unicode share access [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
09/04-17:53:56.405923 168.150.177.164:1035 -> 168.150.177.166:139
TCP TTL:128 TOS:0x0 ID:94 IpLen:20 DgmLen:138 DF
AP Seq: 0x82073DFF Ack: 0x2468EB82 Win: 0x4241 TcpLen: 20

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
09/04-17:53:56.417045 168.150.177.164:45461 -> 168.150.177.1:1900
UDP TTL:1 TOS:0x0 ID:105 IpLen:20 DgmLen:161
Len: 133

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
09/04-17:53:56.420759 168.150.177.164:45461 -> 168.150.177.1:1900
UDP TTL:1 TOS:0x0 ID:117 IpLen:20 DgmLen:160
Len: 132

[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
09/04-17:53:56.422095 168.150.177.164:45461 -> 168.150.177.1:1900
UDP TTL:1 TOS:0x0 ID:118 IpLen:20 DgmLen:161
Len: 133

[**] [1:2351:10] NETBIOS DCERPC ISystemActivator path overflow attempt little endian unicode [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
09/04-17:53:56.442445 198.8.16.1:10179 -> 168.150.177.164:135
TCP TTL:105 TOS:0x0 ID:49809 IpLen:20 DgmLen:1420 DF
A Seq: 0xF9589BBF Ack: 0x82CCF5B7 Win: 0xFFFF TcpLen: 20
[Xref => <http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx>][Xref => <http://cgi.nessus.org/plugins/dump.php?id=11808>][Xref => <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0352>][Xref => <http://www.securityfocus.com/bid/8205>]

[**] [122:3:0] (portscan) TCP Portsweep [**]
[Priority: 3]
09/04-17:53:56.499016 198.8.16.1 -> 168.150.177.166
PROTO:255 TTL:0 TOS:0x0 ID:1750 IpLen:20 DgmLen:168

傳統 NIDS 的警訊型態 (2) 紀錄在資料庫內

以下為利用瀏覽器透過網頁方式呈現警訊資料庫的內容

Basic Analysis and Security Engine (BASE): Query Results - Mozilla

File Edit View Go Bookmarks Tools Window Help

Basic Analysis and Security Engine (BASE)

Home | Search | AG Maintenance [Back]

Added 0 alert(s) to the Alert cache

Queried DB on : Thu October 14, 2004 22:04:44

Meta Criteria	any
IP Criteria	any
TCP Criteria	any
Payload Criteria	any

Summary Statistics

- Sensors
- Unique Alerts (classifications)
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-50 of 81 total

<input type="checkbox"/>	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
<input type="checkbox"/>	#0-(1-84)	[snort] NETBIOS SMB IPC\$ share unicode access	2004-10-08 11:25:41	192.168.1.100:1613	192.168.1.4:139	TCP
<input type="checkbox"/>	#1-(1-83)	[snort] NETBIOS SMB IPC\$ share unicode access	2004-10-08 11:25:31	192.168.1.100:1608	192.168.1.4:139	TCP
<input type="checkbox"/>	#2-(1-82)	[snort] NETBIOS SMB IPC\$ share unicode access	2004-10-08 11:25:05	192.168.1.100:1601	192.168.1.4:139	TCP
<input type="checkbox"/>	#3-(1-80)	[snort] (http_inspect) OVERSIZE CHUNK ENCODING	2004-10-04 22:25:41	192.168.1.4:42164	67.19.245.228:80	TCP
<input type="checkbox"/>	#4-(1-81)	[snort] (http_inspect) OVERSIZE CHUNK ENCODING	2004-10-04 22:25:41	192.168.1.4:42163	67.19.245.228:80	TCP

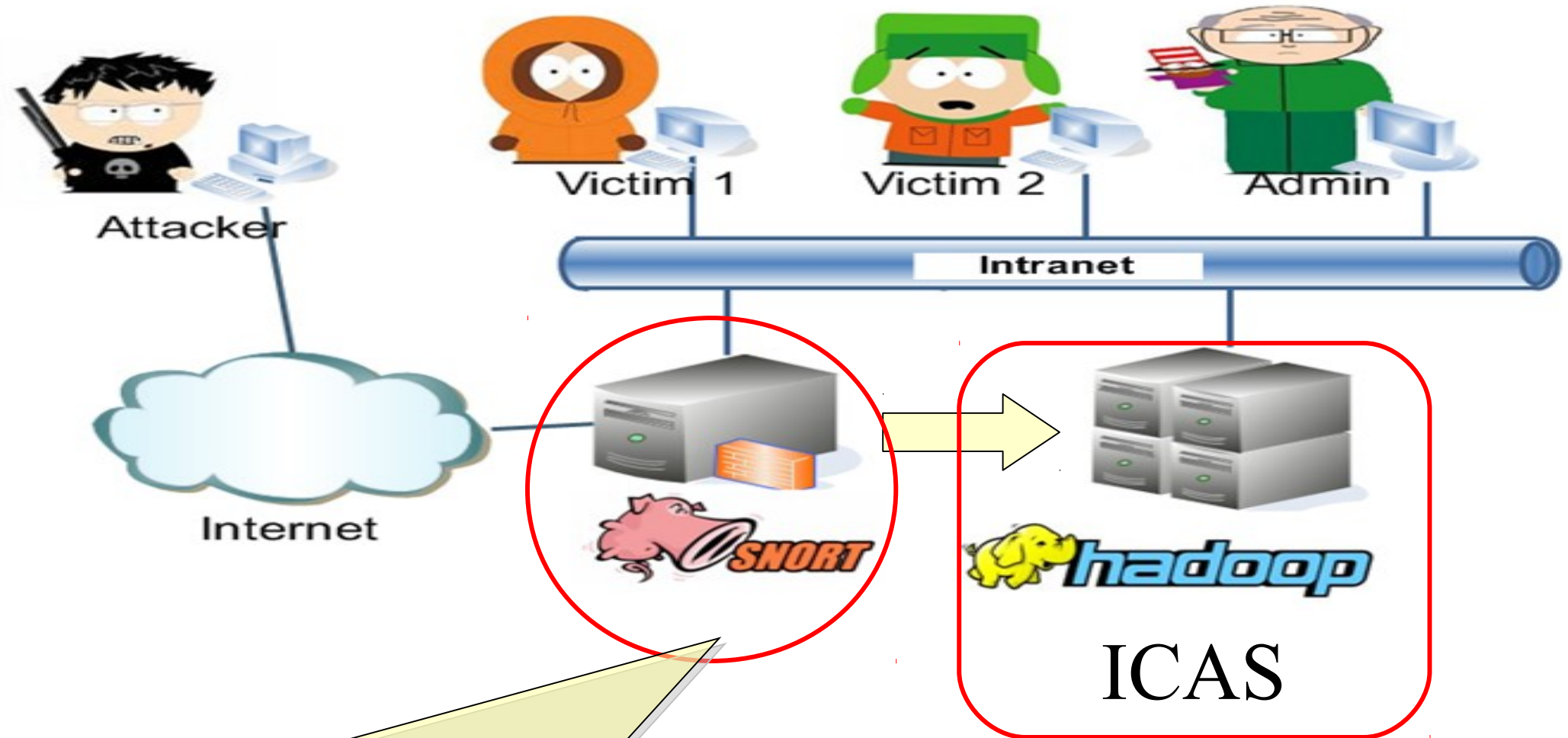
以上作法的缺點

- 警訊僅被『忠實』地被記錄下來，無法顯示彼此間的關聯性，因此系統管理者難以瞭解全部攻擊情形
- 過多的警訊，使得容易忽略重要內容
- 完全依賴單一資料庫，當資料量一大，該台主機的讀寫效率將成為瓶頸

使用雲端運算的解決方案：ICAS

- ICAS, *IDS Cloud Analysis System*
- 利用雲端運算的特性提供以下好處
 - 對大量資料有高效率
 - 一般主機的叢集
 - 有錯誤容忍
- 分析演算法
 - 整合
 - 關聯

透過 ICAS 協助分析 IDS 的警訊

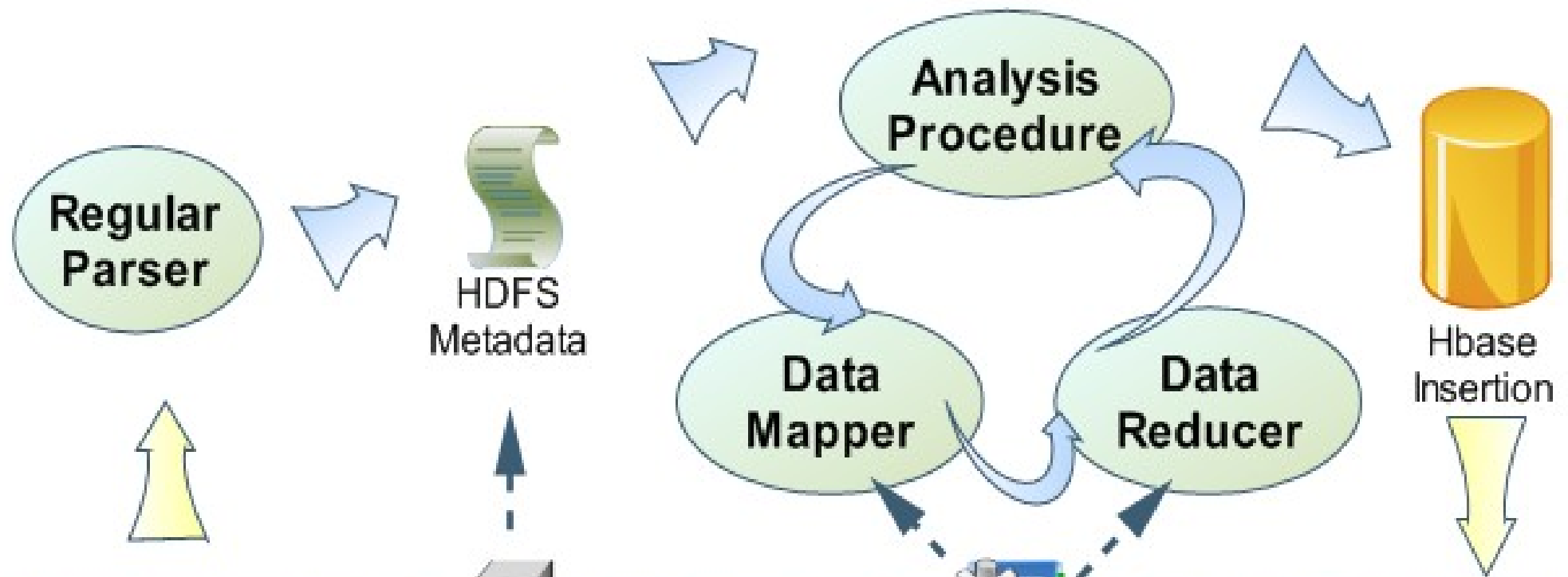


可多個 NIDS 共同產生警訊後，傳送至 ICAS，分析演算法目前有 ICAS-I 及 ICAS-II

ICAS-I

- 將任意個原始警訊檔上傳到運行 ICAS-I 演算法的 Hadoop 檔案系統空間（HDFS）
- 利用 Hadoop 的 MapReduce 平台架構所設計的演算法來分析資料
- 分析完後的資料塞入分散式資料庫 HBase 內

ICAS-I 流程圖



Intrusion
Detection
System



HDFS



JobTracker



Cloud Platform



Database

ICAS-I 整合後的警訊結果

Destination IP	Attack Signature	Source IP	Destination Port	Source Port	Packet Protocol	Timestamp
Host_1	Trojan	Sip1	80	4077	tcp	T1
Host_1	Trojan	Sip2	80	4077	tcp	T2
Host_1	Trojan	Sip1	443	5002	tcp	T3
Host_2	Trojan	Sip1	443	5002	tcp	T4
Host_3	D.D.O.S	Sip3	53	6007	udp	T5
Host_3	D.D.O.S	Sip4	53	6008	tcp	T5
Host_3	D.D.O.S	Sip5	53	6007	udp	T5
Destination IP	Attack Signature	Source IP	Destination Port	Source Port	Packet Protocol	Timestamp

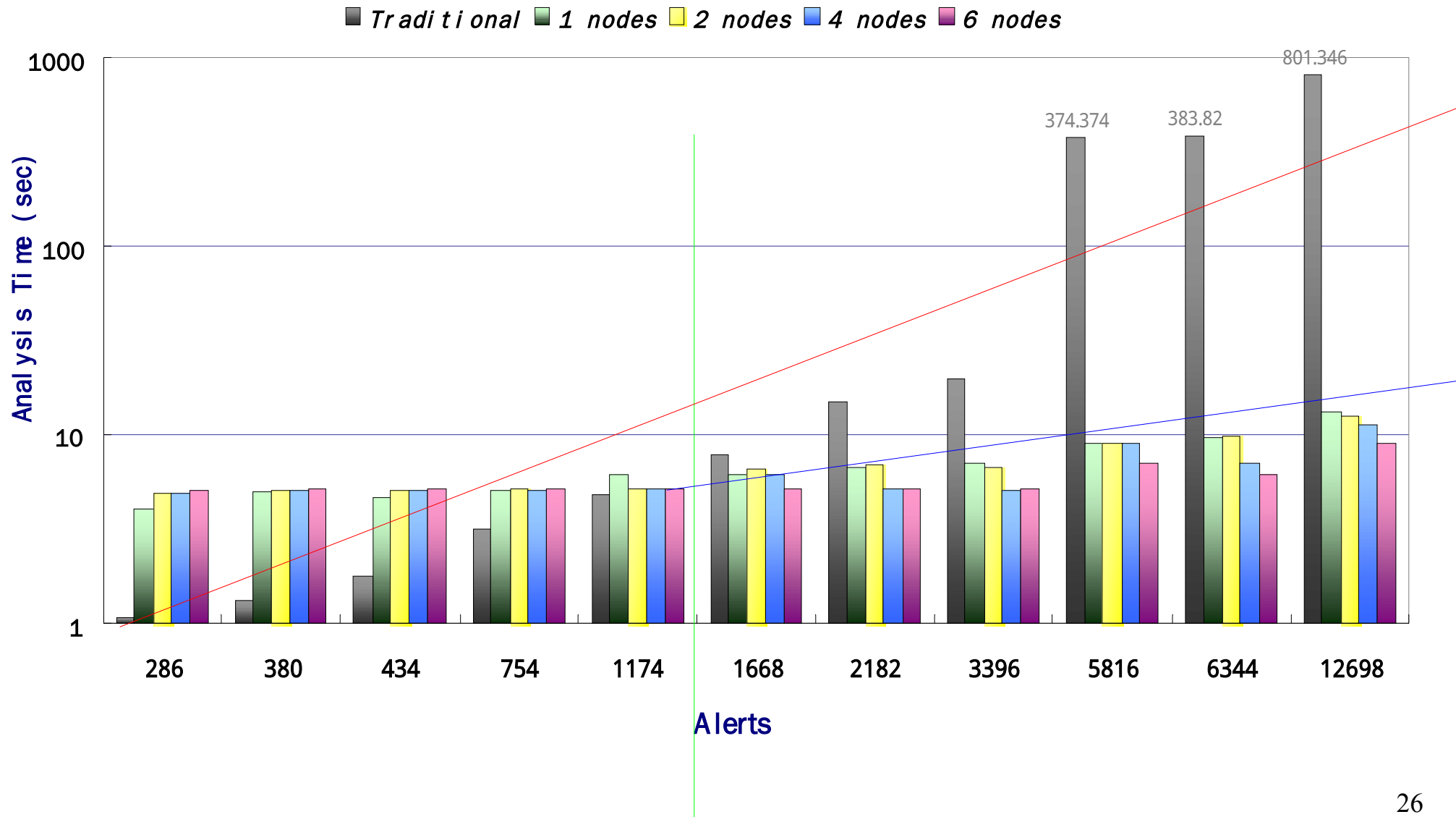
Key		Values				
Host_1	Trojan	Sip1,Sip2	80,443	4077,5002	tcp	T1,T2,T3
Host_2	Trojan	Sip1	443	5002	tcp	T4
Key		Values				

ICAS-I 效能數據的環境

- Machine:
 - CPU : Intel quad-core, Memory : 2 GB,
- OS : Linux : Ubuntu 8.04 server
- Software : version
 - Hadoop : 0.16.4
 - Hbase : 0.1.3
 - Java : 6
- Alerts Data Sets
 - MIT Lincoln Laboratory, Lincoln Lab Data Sets
 - Computer Security group at UCDavis, tcpdump file

ICAS-I 效能分析時間圖

The Consuming Time of Each Number of Data Sets



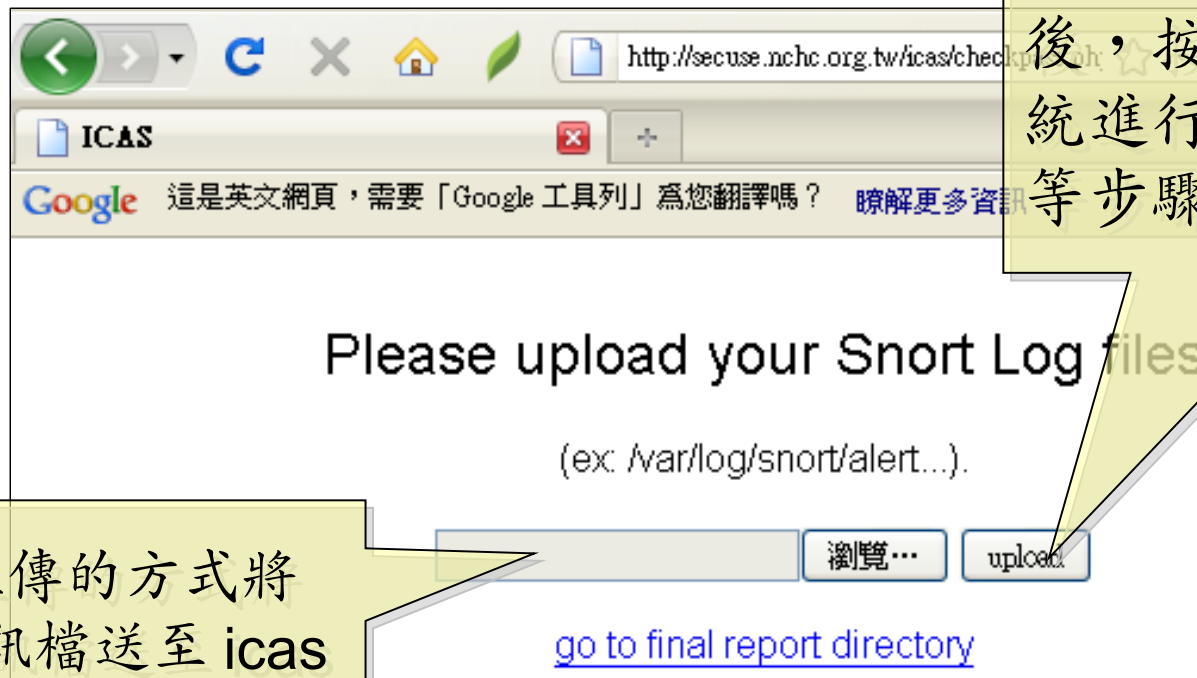
ICAS-I 效能數據表

Throughput Data Overall

Origianl Alerts	Analysis Time (sec)					Results	Reduction Rate
	Traditional	1 nodes	2 nodes	4 nodes	6 nodes		
286	1.068	4.087	4.869	4.864	5.077	30	89.51%
380	1.333	4.94	5.069	5.067	5.097	11	97.11%
434	1.76	4.61	5.066	5.068	5.09	9	97.93%
754	3.145	5.066	5.079	5.038	5.096	16	97.88%
1174	4.73	6.066	5.093	5.089	5.097	33	97.19%
1668	7.909	6.07	6.56	6.071	5.082	16	99.04%
2182	14.949	6.671	6.95	5.166	5.088	16	99.27%
3396	19.901	7.053	6.654	5.076	5.091	68	98.00%
5816	374.374	9.081	9.076	9.07	7.076	66	98.87%
6344	383.82	9.68	9.872	7.069	6.069	72	98.87%
12698	801.346	13.096	12.367	11.367	9.083	36	99.72%

ICAS-II

- ICAS-I 僅將資料塞入資料庫，然而還是文字的敘述
- ICAS-II 將輸入的任意多個警訊整合成一張警訊關聯圖
- 資料的來源可以透過以下兩種方式上傳到分析平台
 - 系統自動設定以 SCP 傳送到 ICAS 工作目錄
 - 管理者透過 ICAS 網頁上傳

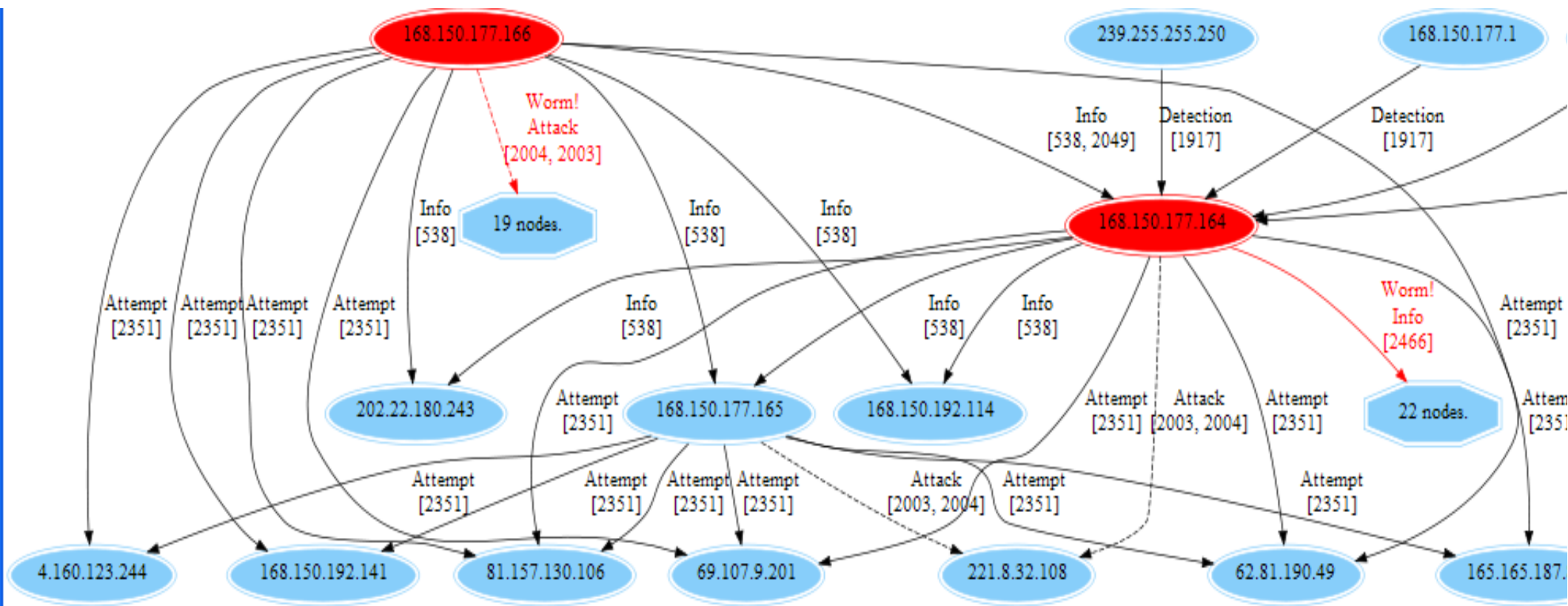


一旦選定需分析的日誌檔後，按下 upload 鈕，系統進行上傳→分析→繪圖等步驟

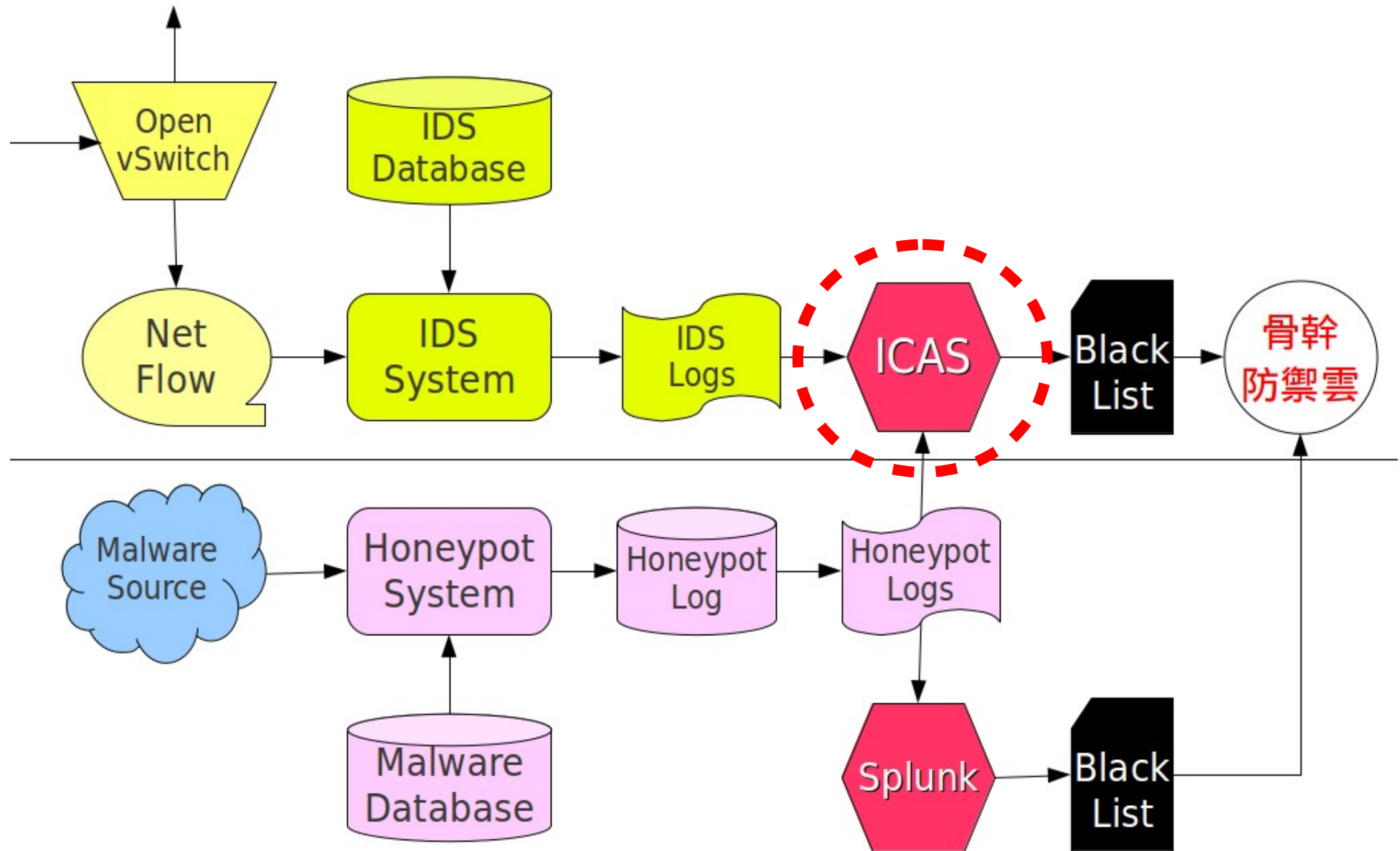
透過網頁上傳的方式將 snort 的警訊檔送至 icas 分析

ICAS-II 所產生的報表：警訊關聯圖

- 經過 ICAS-II 分析後，可以得到此警訊關聯圖。
- 圖中橢圓形代表節點，箭頭及線上文字代表攻擊方向與攻擊方法。
- 標為紅色則是經過系統分析之後，被判定有攻擊行為的節點與方法。
- 此圖說明 IP 168.150.177.166 與 168.150.177.164 有進行蠕蟲的攻擊行為



架設 ICAS 於 NCHC Cloud WebOS 可以用來監控 Inter-VM 的攻擊





工作項目四
雲端骨幹聯防系統

學術骨幹網路 (Ex. TWAREN, TANET)

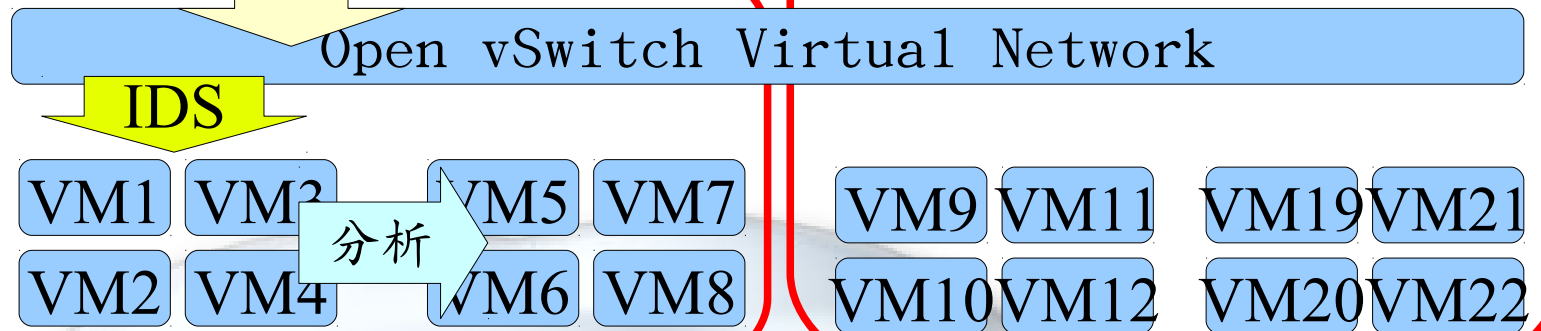
工作項目二
雲端單一登入系統



工作項目五
雲端資安實驗平台

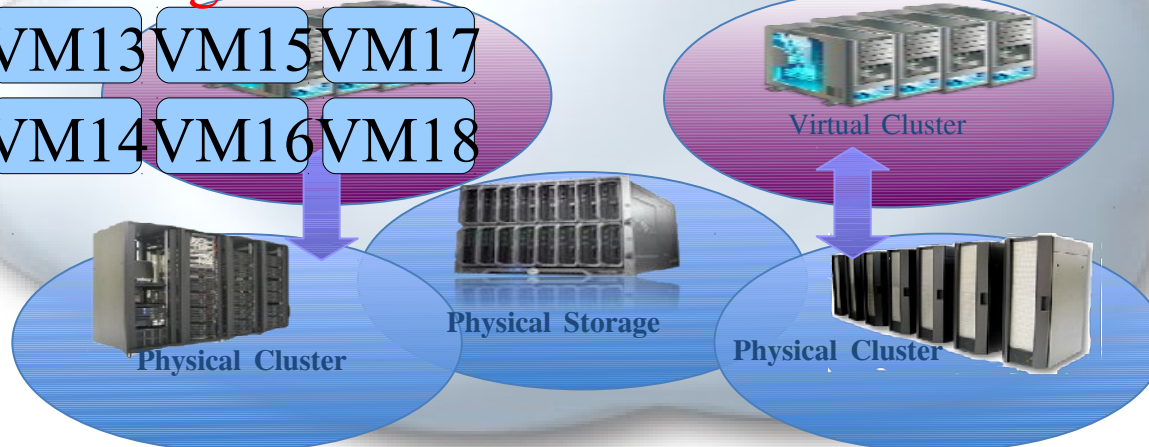
工作項目三
虛擬網路安全分析

工作項目三
雲端系統日誌分析



雲端環境監控
雲端共用平台
工作項目一

VM13 VM15 VM17
VM14 VM16 VM18



ICAS 展示網站

http://icas.classcloud.org

Welcome to Use ICAS!

此為網路入侵偵測日誌(Intrusion Detection System Log, IDS-Log)雲端分析平台，主要目的為定期自動蒐集各個入侵偵測節點的警訊資料，統一整理成關聯警訊，並且分析成攻擊圖。

雲端資安警訊列表

瀏覽攻擊圖

上傳日誌檔

說明

雲端資安警訊列表

IDS 代表蒐集警訊的入侵偵測系統，目前共有三類

- * snort = 1
- * IDP8200 = 2
- * NK7Admin = 3

P 代表 嚴重性 (priority), 1~3, 1 為最嚴重, 需優先處理

C 代表 合併總數 (count) 代表符合此規則的合併總數

S 代表 Snort Signature ID, 可於 <http://www.snortid.com/> 網站查詢相關的更多資訊

列表

Show 25 筆資料

來源IP 目標IP 起始時間 結束時間

S 代表 Snort Signature ID, 可於 <http://www.snortid.com/> 網站查詢相關的更多資訊。ps：其他入侵偵

列表

Show 25 筆資料

來源IP	目標IP	起始時間	結束時間	P	IDS
140.110.134.160	140.110.134.198	20110705_182333	20110707_103419	2	1
140.110.134.197	140.110.134.198	20110705_182210	20110707_105932	2	1
140.110.134.253	224.0.0.13	20110705_182154	20110707_105952	2	1
140.110.138.166	140.110.134.198	20110706_162227	20110706_162600	2	1
140.110.4.1	140.110.134.198	20110707_092822	20110707_092822	2	1
140.113.130.221	0.0.0.0	20030811_130500	20030811_130500	1	2
140.113.130.221	phe96.sro.nchc.org.tw	20030811_130500	20030811_130500	1	2
168.95.1.1	140.110.104.84	20110301_144100	20110301_144100	1	3
173.255.255.222	140.110.134.198	20110706_174453	20110706_180516	1	1
211.233.68.183	140.110.134.198	20110707_032258	20110707_032351	1	1

Showing 1 to 10 of 11 entries

ICAS 展示網站

<http://icas.classcloud.org>

雲端資安警訊列表

瀏覽攻擊圖

上傳日誌檔

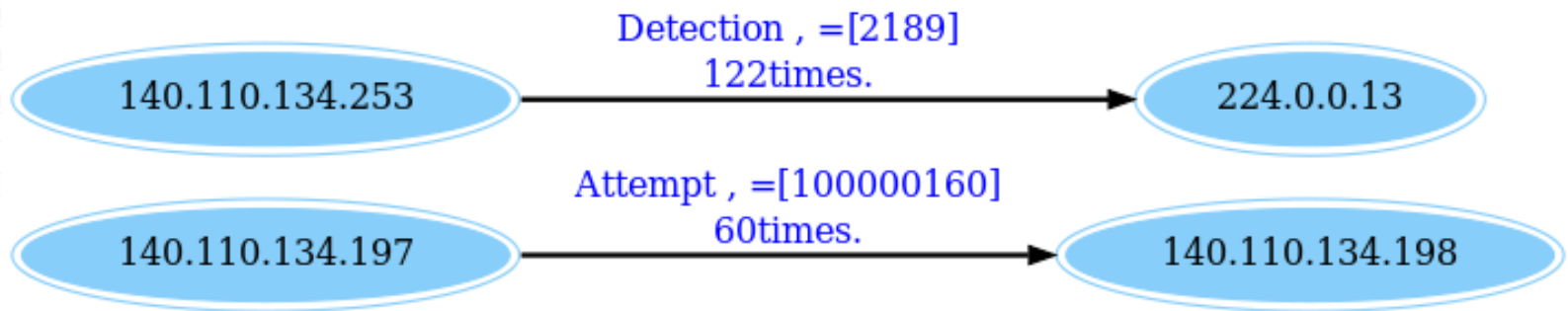
瀏覽攻擊圖

▶ 最新攻擊圖

▼ 歷史攻擊圖

20110705/	06-Jul-2011 15:18	-
20110706/	07-Jul-2011 00:00	-
20110707_000004.svg	07-Jul-2011 00:00	3.8K
20110707_010003.svg	07-Jul-2011 01:00	3.8K
20110707_020003.svg	07-Jul-2011 02:00	3.8K
20110707_030004.svg	07-Jul-2011 03:00	3.8K
20110707_040003.svg	07-Jul-2011 04:00	5.1K
20110707_050003.svg	07-Jul-2011 05:00	3.8K
20110707_060004.svg	07-Jul-2011 06:00	3.8K
20110707_070004.svg	07-Jul-2011 07:00	3.8K
20110707_080004.svg	07-Jul-2011 08:00	3.8K
20110707_090004.svg	07-Jul-2011 09:00	3.8K
20110707_100004.svg	07-Jul-2011 10:00	3.8K
20110707_110004.svg	07-Jul-2011 11:00	3.8K

Apache/2.2.17 (Ubuntu)



ICAS 信件通報



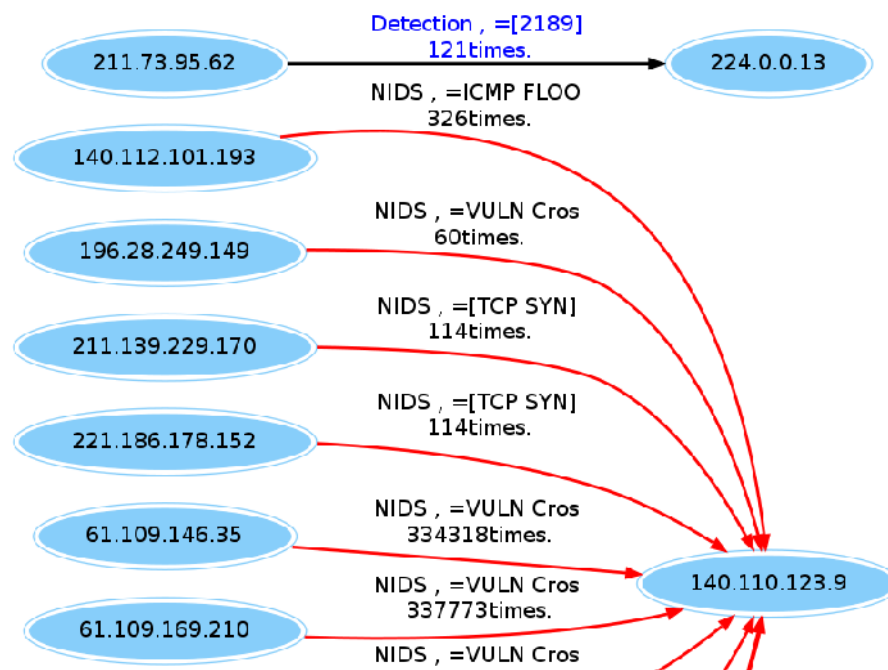
ICAS Alarm @ 211.73.95.39

Tue, Sep 27, 2011 at 18:53

Attack List

src ip	dst ip	prio	time range	detail	ds	count	dst port list
113.108.62.89	211.73.95.39	2	20110927_173754-20110927_173754	COMMUNITY SIP TCP/IP message flooding directed to SIP proxy	snort	1	80
121.229.207.131	211.73.95.39	2	20110927_175939-20110927_175939	ICMP PING NMAP	snort	1	0
140.112.101.193	140.110.123.9	1	20110926_214300-20110926_214300	ICMP FLOOD	rk/admin	326	0
196.28.249.149	140.110.123.9	1	20110904_180100-20110904_180100	VULN Cross-Site Scripting -7	rk7admin	60	80
211.139.229.170	140.110.123.9	1	20110927_142900-20110927_142900	TCP SYN	rk7admin	114	80
211.73.95.62	224.0.0.13	2	20110927_171553-20110927_181500	BAD-TRAFFIC IP: Proto 103 PIM	snort	121	0
211.75.160.211	211.73.95.39	3	20110927_174510-20110927_174510	ICMP PING CyberKit 2.2 Windows	snort	1	0
221.186.178.152	140.110.123.9	1	20110927_142900-20110927_142900	TCP SYN	rk7admin	114	80
61.109.146.35	140.110.123.9	1	20110901_150500-20110927_170600	VULN Cross-Site Scripting -7	rk7admin	334318	80
61.109.169.210	140.110.123.9	1	20110901_151900-20110927_171400	VULN Cross-Site Scripting -7	rk7admin	337773	80
61.109.169.221	140.110.123.9	1	20110901_150300-20110927_170300	VULN Cross-Site Scripting -7	rk7admin	344210	80
61.126.247.250	140.110.123.9	1	20110927_142900-20110927_142900	TCP SYN	rk7admin	114	80
67.195.113.247	140.110.123.9	1	20110904_201900-20110904_201600	CGI webdriver access	rk7admin	112	80
78.106.74.173	140.110.123.9	1	20110927_054500-20110927_054500	VULN SQL injection union select attempt	rk7admin	92	80

Graph Show





Questions?

Slides - <http://trac.nchc.org.tw/cloud>

Jazz Wang
Yao-Tsung Wang
jazz@nchc.org.tw

