網路安全預警機制

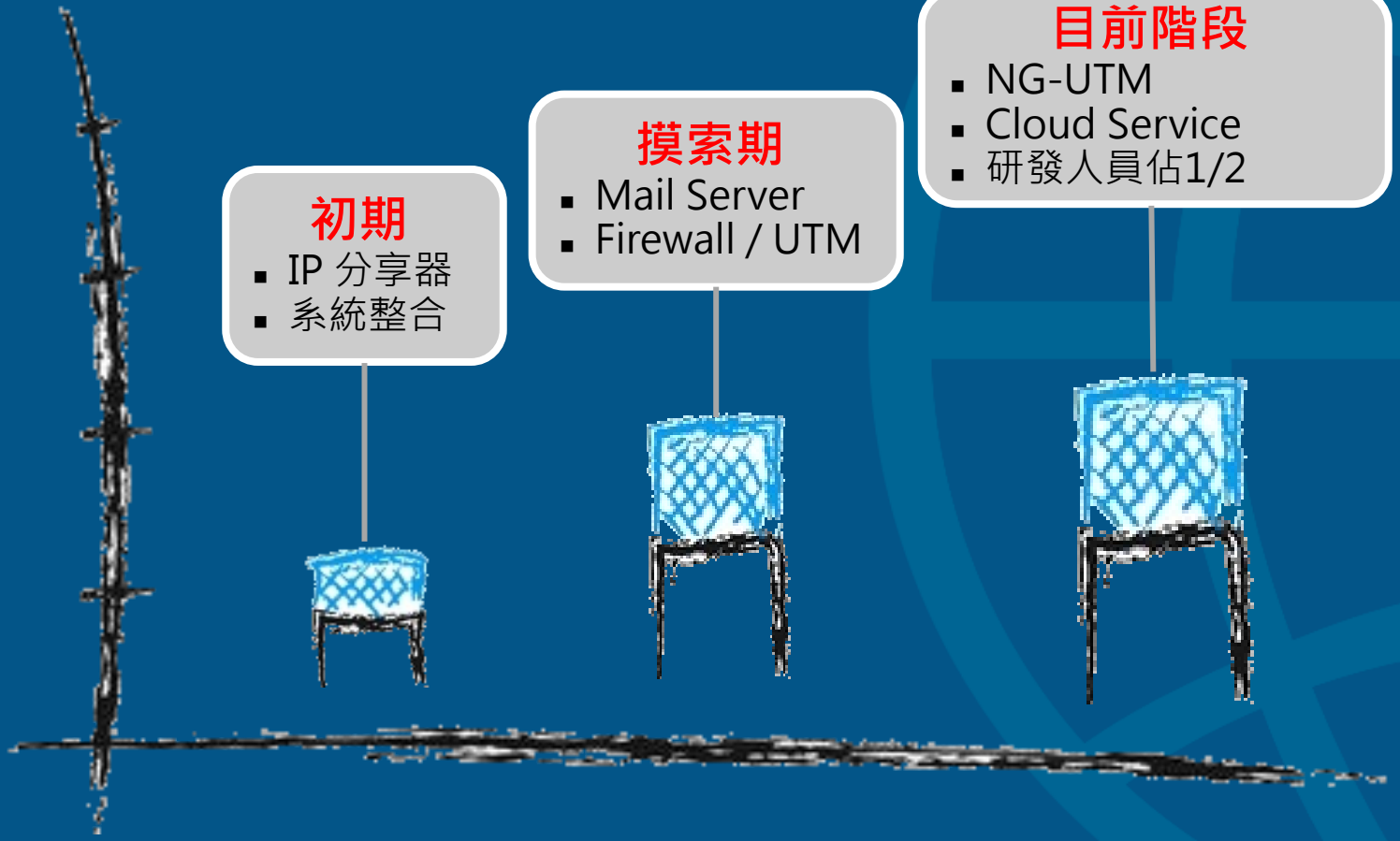
眾至資訊總經理　王常帆

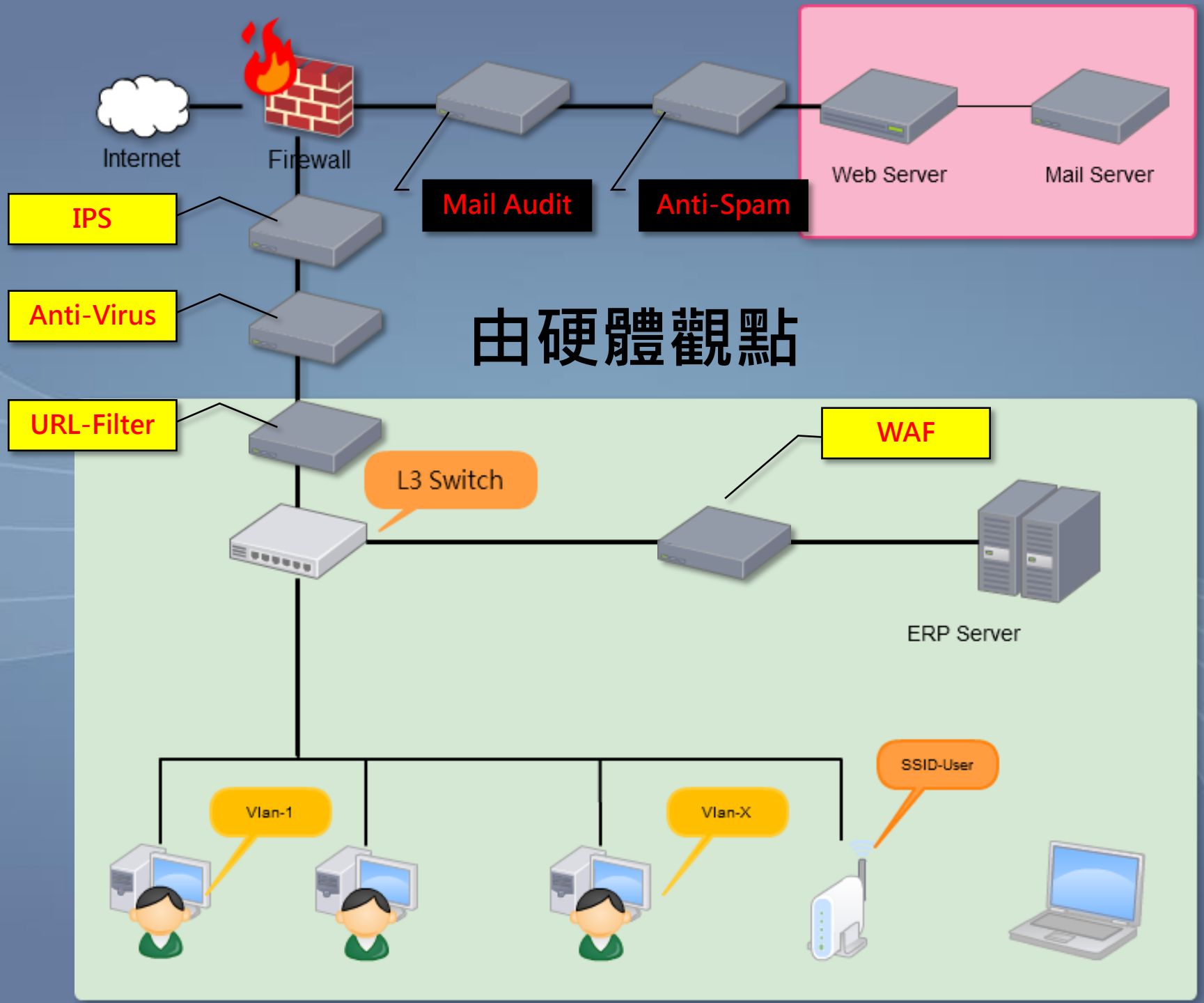
事前(預警) > 事中(阻擋) > 事後(鑑識)

AGENDA

- 了解你的網路？
- 攻擊發生之前，有啥蛛絲馬跡？
- 回到最初—DNS 。
- 由網路使用者行為分析，找出異常---早期預警。

Who is ShareTech ?




Internet
Firewall
Mail Audit
Anti-Spam
Web Server
Mail Server
IPS
Anti-Virus
URL-Filter
由硬體觀點
WAF
L3 Switch
ERP Server
SSID-User
Vlan-1
Vlan-X

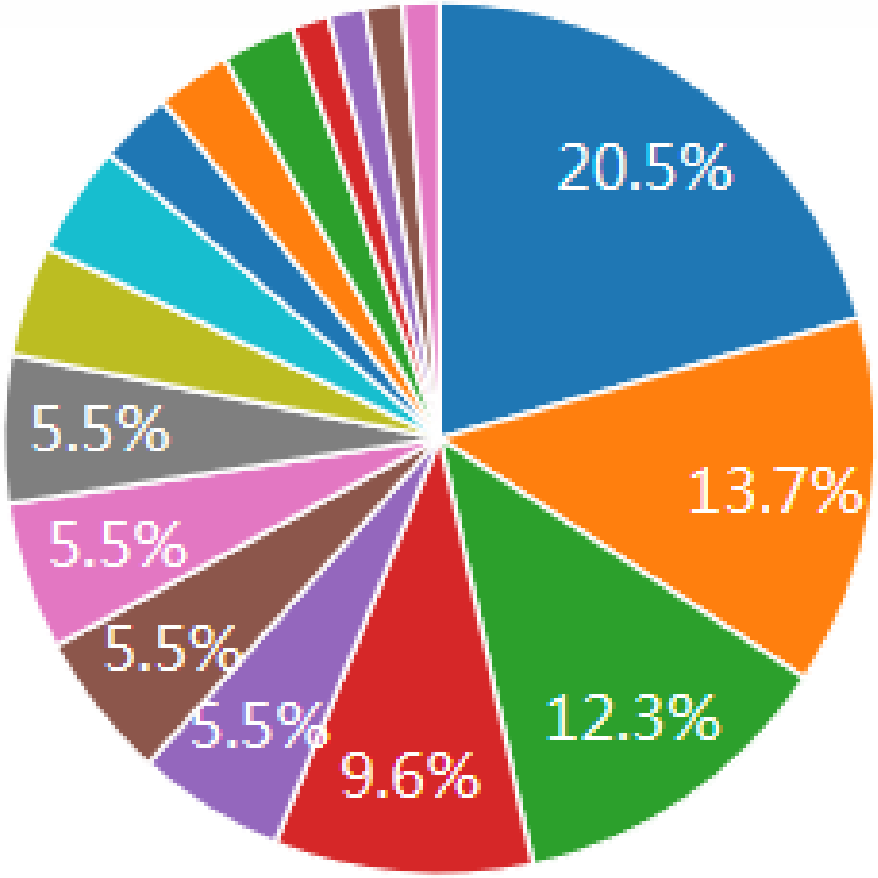
能閱讀的網路封包

```
tcp      6 589 ESTABLISHED src=192.168.8.187 dst=137.116.169.
213 sport=1853 dport=443 packets=344 bytes=679280 src=137.116
.169.213 dst=192.168.190.116 sport=443 dport=1853 packets=533
 bytes=258829 [ASSURED] mark=256  mark64=0x3b4104000000100 d
elta-time=5188 use=1
icmp     1 9 src=192.168.190.116 dst=192.168.190.1 type=8 cod
e=0 id=47436 packets=3 bytes=180 src=192.168.190.1 dst=192.16
8.190.116 type=0 code=0 id=47436 packets=3 bytes=180 mark=838
8608  mark64=0x800000 delta-time=3 use=1
```

了解你的網路？

- 何時(Time)、從哪裡來(Source)、到哪裡(Destination)、做甚麼事Port/Application。
- 持續多久(Continue)、傳了多少量(In/Out-Bytes)。

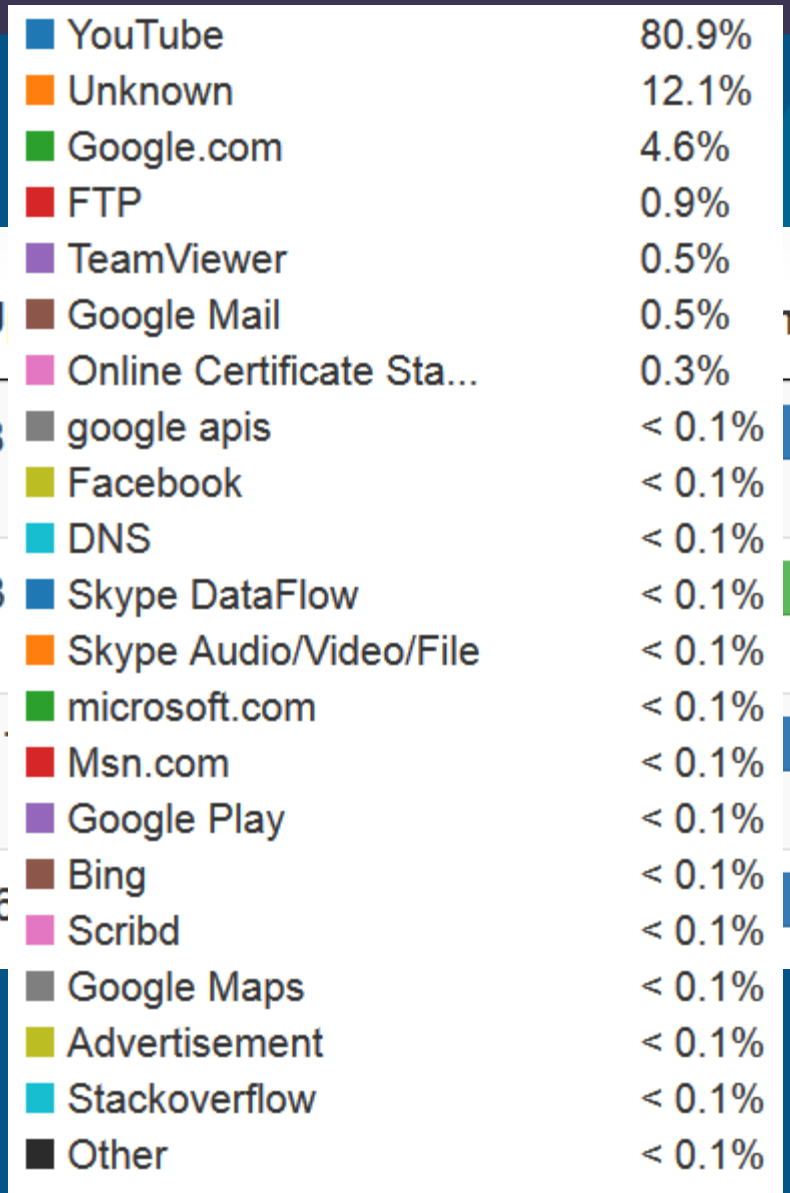
加入 DPI 辨識後



- Online Certificate Status Protocol
- TeamViewer
- STUN
- Skype DataFlow
- PChome TW
- NTP
- HTTP-Download
- SAMBA
- Google.com
- Skype Audio/Video/File
- microsoft.com

整理完之後

192.168.188.161



Source IP	U	n	Total Flows	Detail
192.168.190.116	48		4.01 GB	
191.0	3	D	3.53 GB	
192.168.190.70	11		3.05 GB	
192.168.190.181	46		1.43 GB	

Q : 找好人還是壞人？

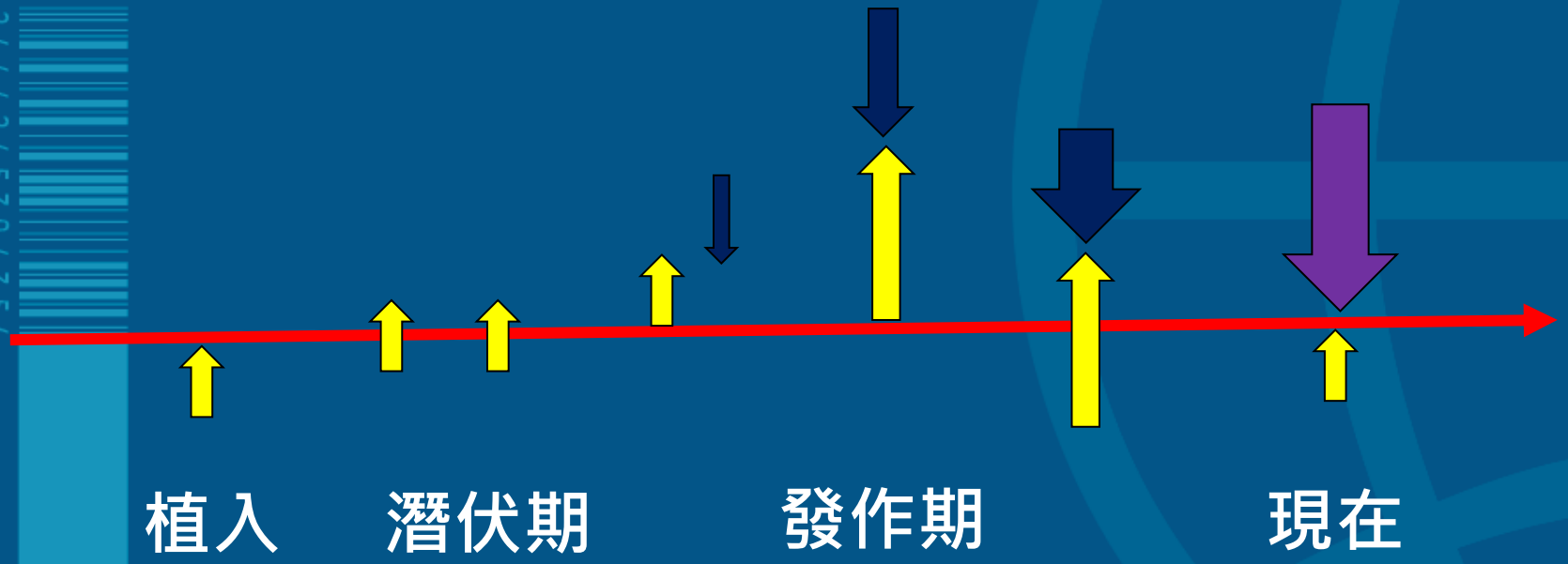
Q : 是 人做的 還是 機器做的？

攻擊發生之前有蛛絲馬跡？

- Virus、IPS 都屬於已知特徵值比對。

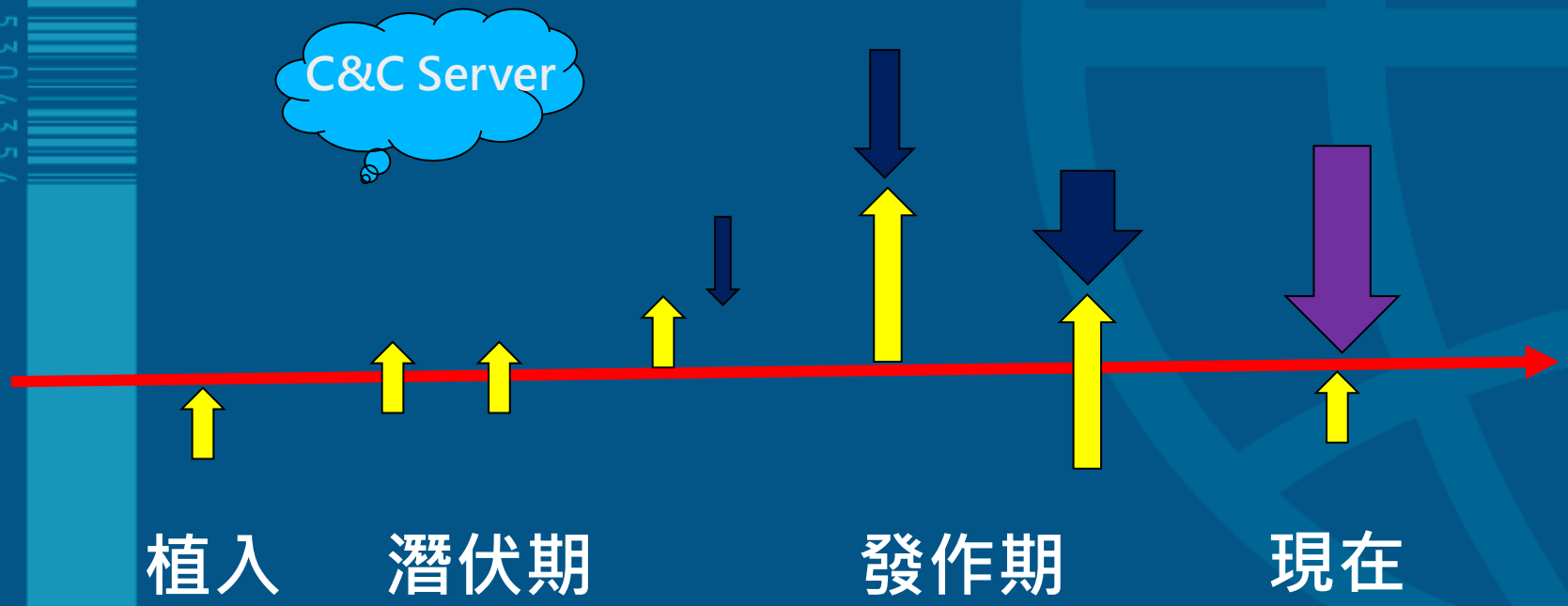
- 觀察指標
  - Unknown application
  - DNS 量化
  - 重複使用奇怪的 port
  - 時間軸行為

攻擊的週期行為



你是駭客，植入後會怎麼做

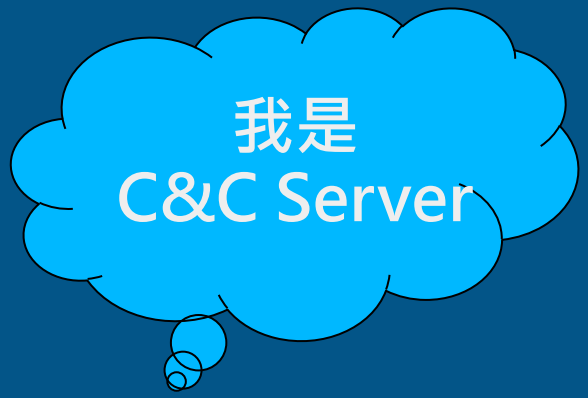
- 不管是勒索或是竊取資料，跟 C&C Server 回報，等候命令。



怎麼預知潛伏期的連線？

- 送出 DNS 查詢。
- 建立 連線 ，尤其是加密連線。
- 送出 資料。

- Q1 : 駭客會用固定的 Domain ?
- Q2 : 讓你查不到也能阻止未知攻擊



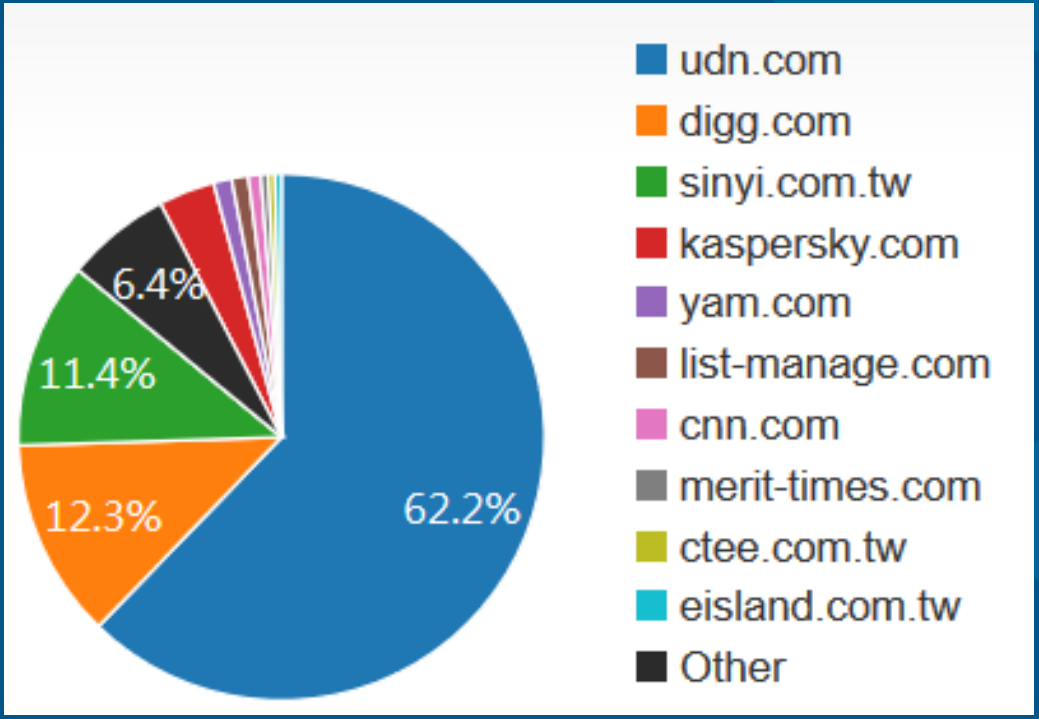
回到最初—DNS

- 由 DNS Server Log 分析
- 由 UTM 攔截 DNS Request
- 因為 DNS 是明碼

dst_ip	id	query
A85F0101	45803	1.0.0.127.email-bl.rambler.ru
C1DD7135	26957	prod.registrar.skype.com
08080808	1099	sharetech.com.tw.multi.uribl.com
08080808	22090	sharetech.com.tw.bl.open-whois.org
08080808	64889	sharetech.com.tw.multi.surbl.org
08080808	23244	sharetech.com.tw.dob.sibl.support-intelligence.net
08080808	62497	dns1.sharetech.com.tw
08080808	31934	dns2.sharetech.com.tw
173DC783	58893	production.skype-registar.akadns.net

異常的 DNS 查詢行為

- 大量的 DNS 查詢
- 失效網域 查詢 (DGA)
- 查詢跟 URL 黑名單有關



找出可疑的人

- DNS 異常指數：
  - 量化每一個人 DNS 對時間軸
  - 查詢次數
  - Domain
  - 成功 or 無回應
- 監測 DNS 主機通聯記錄
- 懷疑 > 監控 > 預警

早期預警—使用者行為分析

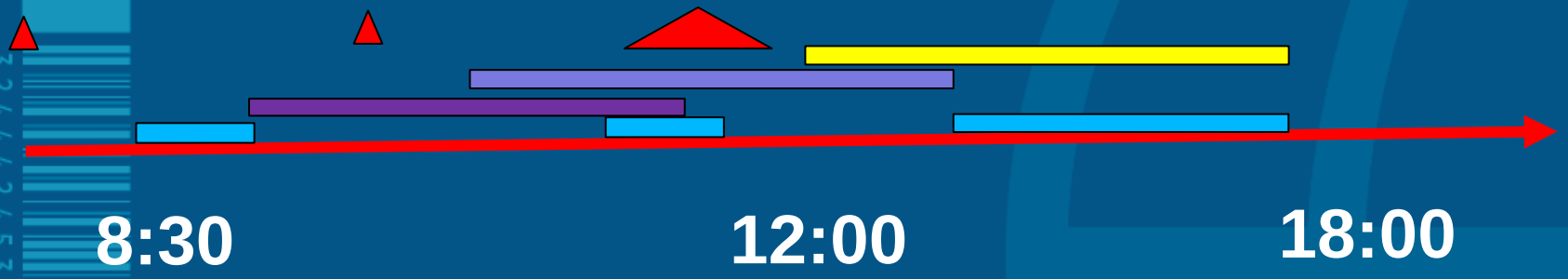
- 單從 DNS 查詢行為並沒辦法準確判斷
- 搭配 網路行為，才能分辨出異常

- 甚麼是網路行為？
  - 應用程式 + 時間軸
  - 通聯對象

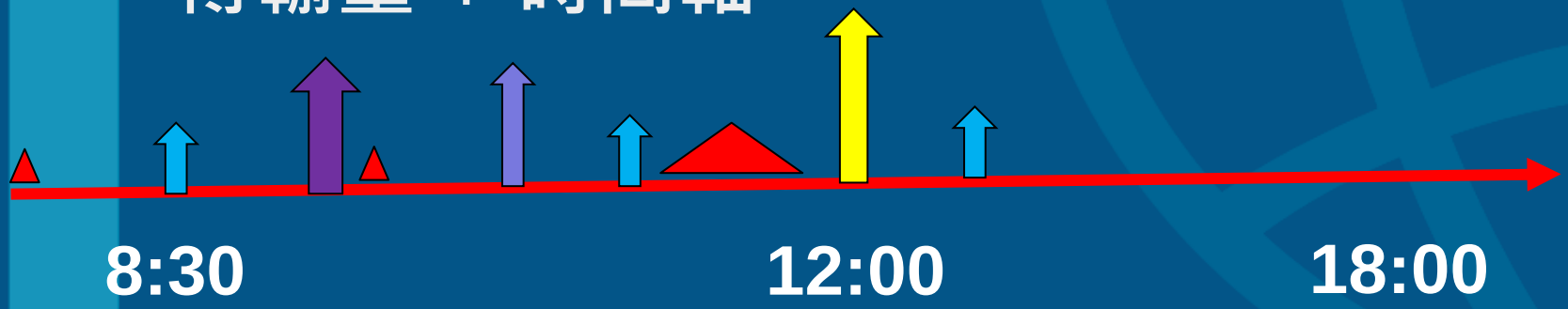
  - 跟過去的網路行為比

行為分析 – APP+時間軸

- 應用程式 + 時間軸



- 傳輸量 + 時間軸



APP+時間軸

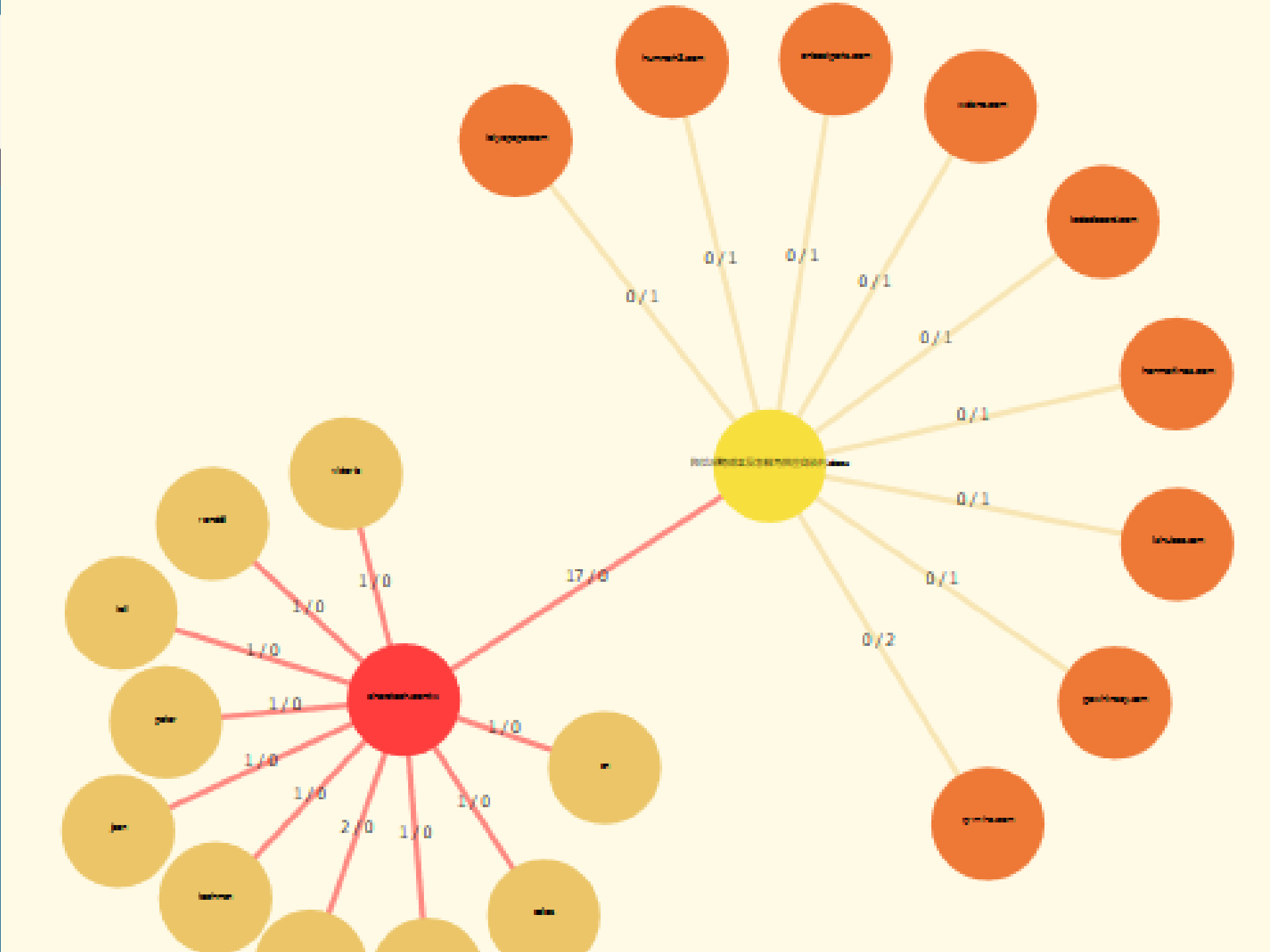
- 時間範圍：**2018-03-08 00:00:00 ~ 2018-03-08 15:05:48**
- 來源 IP：**192.168.190.106**
- 應用程式：**Unknown1111_0**

1 / **449** 跳至 1 頁數 、每頁 16 筆 GO

日期	持續時間 (s)	協定	來源 IP	目的 IP	通訊埠	上傳流量
2018-03-08 08:25:12	7	tcp	192.168.190.106	210.59.146.245	61579->80	0.55 KB
2018-03-08 08:25:12	7	tcp	192.168.190.106	210.59.146.245	61578->80	0.58 KB
2018-03-08 08:25:29	10	udp	192.168.190.106	111.221.77.151	7697->40022	0.06 KB
2018-03-08 08:25:29	10	udp	192.168.190.106	157.55.130.153	7697->40021	0.08 KB
2018-03-08 08:25:29	10	udp	192.168.190.106	157.55.56.147	7697->40023	0.07 KB
2018-03-08 08:25:29	10	udp	192.168.190.106	157.55.130.168	7697->40034	0.07 KB
2018-03-08 08:25:29	10	udp	192.168.190.106	157.55.130.176	7697->40041	0.06 KB
2018-03-08 08:25:29	10	udp	192.168.190.106	157.56.52.30	7697->40038	0.06 KB
2018-03-08 08:25:29	10	udp	192.168.190.106	75.158.42.53	7697->25138	0.04 KB

誰最需要 APP+時間軸

- Server : 尤其是服務正常就沒人管的，例如：Mail Server 、Web Server ..
- 無法安全更新的設備，例如：Windows XP
- IoT Device


0 / 1
0 / 1
0 / 1
0 / 1
0 / 1
0 / 1
0 / 1
0 / 1
0 / 2
17 / 0
1 / 0
1 / 0
1 / 0
1 / 0
1 / 0
1 / 0
1 / 0
2 / 0
1 / 0

行為分析 – unknown port

- 奇怪的 Port ，例如，9653、1234...
- 藏在 SSL， TCP 443 中的 Unknown APP 最難找。

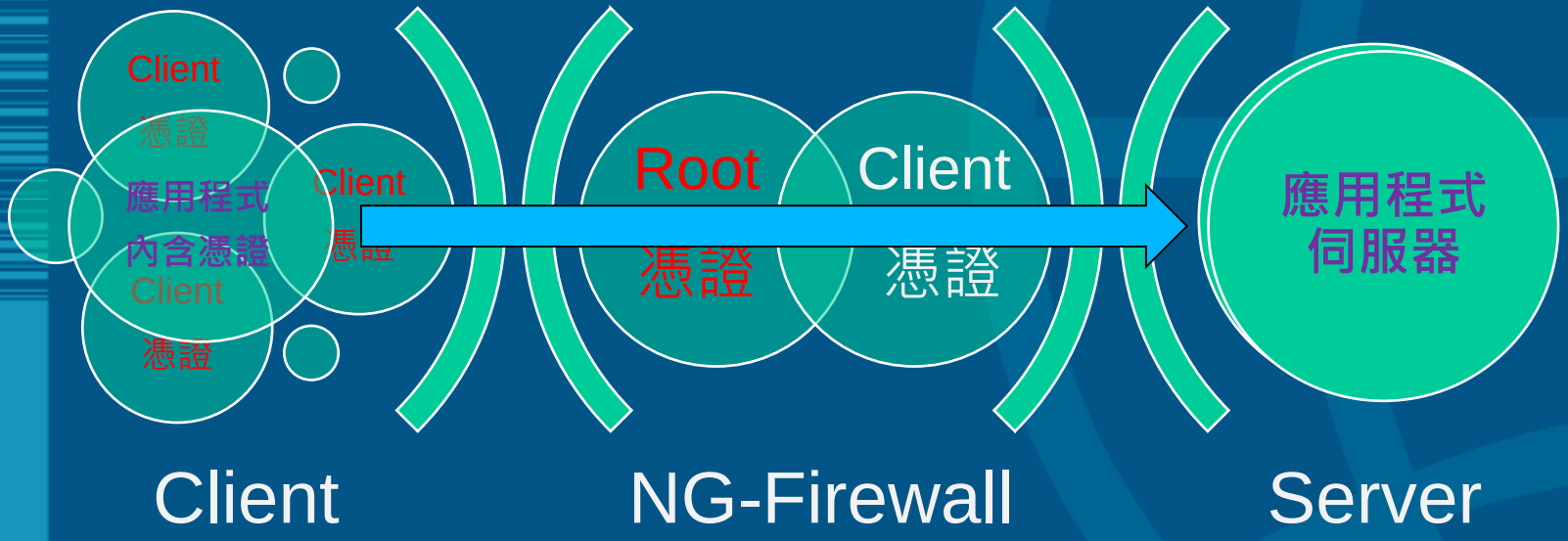
  - 網站 : https://www.xyz.com
  - URL : https://www.xyz.com/sports/

Unknown app -- SSL

- SSL 保護好人還是壞人？
- IPS 特徵值幾乎沒有 https
- MAIL / FTP 還可以用 Proxy 方式解掉加密。

- 想看 SSL 內傳遞資訊，憑證是關鍵，方法有 2 個。
  - 駭客技術 : Man-in-the middle
  - 偽裝成常駐程式 : 桌面維護軟體 / 防毒軟體

行為分析 – SSL 解析

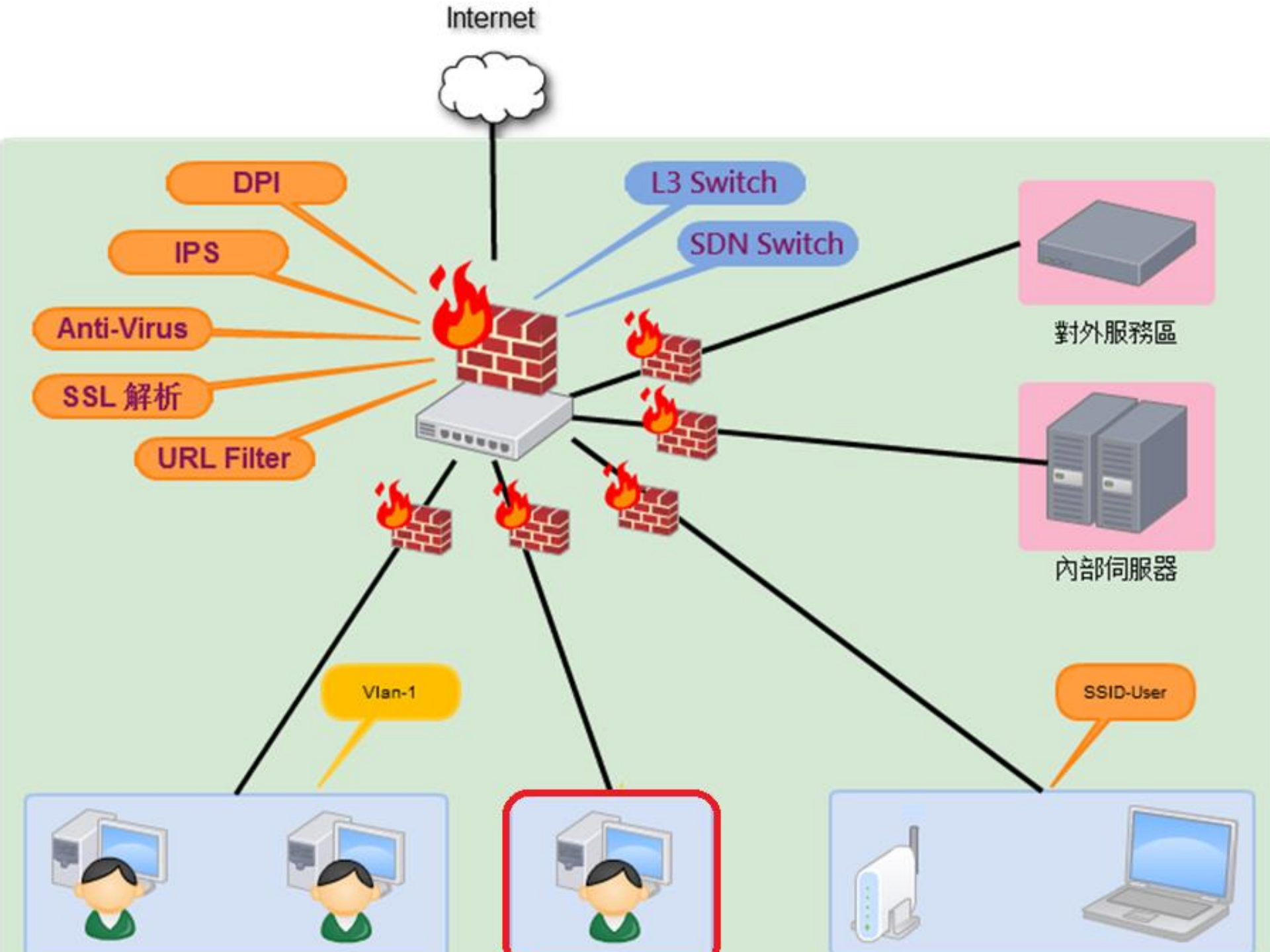

Client
憑證
應用程式
內含憑證
Client
憑證
Client
憑證
Root
憑證
Client
憑證
應用程式
伺服器
Client
NG-Firewall
Server

找到了 該怎辦？

- 我只是預警，管理者要 “手動” 介入處理？
- 問題是：目前都沒特徵值可用

手動處理機制

- 全封了
- 通知 Firewall 封掉網址或 port


Internet
DPI
IPS
Anti-Virus
SSL 解析
URL Filter
L3 Switch
SDN Switch
對外服務區
內部伺服器
Vlan-1
SSID-User