



如何以R做為事件蒐集及分析的利器

Microsoft MVP 黃建笙



山女八王第一！



我有一個問題!!



請問，什麼叫做安全？

為何你不敢讓你只有4歲大的女兒！

自己走100公尺到幼兒園上學去？



流汗會感冒!! 可能有人口販子!! 我不放心!!

還不會看紅綠燈!! 治安不好!! 怕她會迷路!!

離開我三公尺就是不行!! 社會風氣不好!!

滿山滿谷的魔人!! 車子太多!! 她才4歲耶!!

寄生獸、巨人!! 沒有警察!! 有爆料公社!!

就是危險!! 她的腳會酸!! 路上瘋子多!!

台灣專產馬路三寶!! 路上有石頭!! 可能有野狗!!

有蝴蝶!! 還不懂得保護自己!! 不良少年!!



精準的來說!

你對於這個環境缺乏了...

可受到**控制**的能力!

可被**信任**的因素!



什麼是事件處理

方丈英文教學

事件: Event
事故: Incident



事件、事故!!

那一個壞透了~~!?



事件

事故

日本料理 44

吃啥？

今晚您想點哪一道？



事件：有好有壞廣義詞

事故：壞到底的狹義詞



所以要如何手工打造事件蒐
集分析？

別想太多真的細拆三天三夜也
講不完

一般而言

這種框架
我們稱為專家系統





以神奇寶貝大師為目標 一直進行著修煉

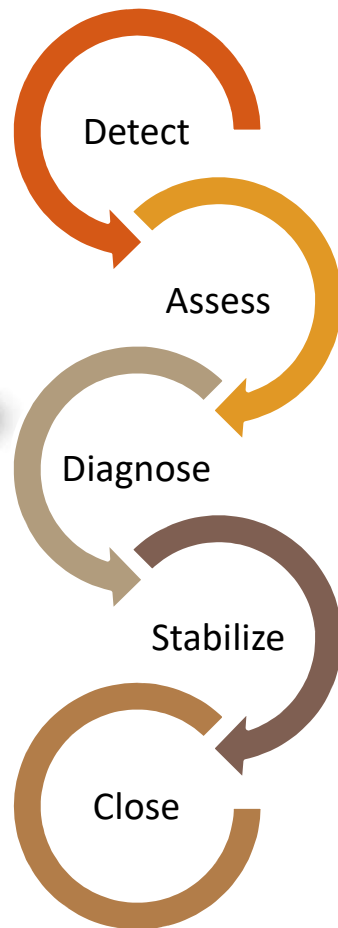
專家系統的組成是...

~~變種DNA 脂肪酸和2又1/2杯香蕉泥
可以回收 非常環保~~



專家系統的組成是...

1. 演算系統
2. 資料儲存



偵測

- 來自四面八方的事件

評測

- 有無事故在內

診斷

- 關聯發生的主因

驅穩

- 做出回應並減少衝擊

結束

- 完成事故回應及處理

偵測的廣度決定分析
事故的始末

演算系統決定了事件
關聯及分析的強度



事件分析該做什麼?

上述的五個流程需要什麼??

裝置必須納管

時時監控



過人的專業知識

駕馭神兵利器



帥軍出征的果斷

有如馮迪索般
強力執行的意志力



.....

你們還在一定是瘋了!!





回歸到原點

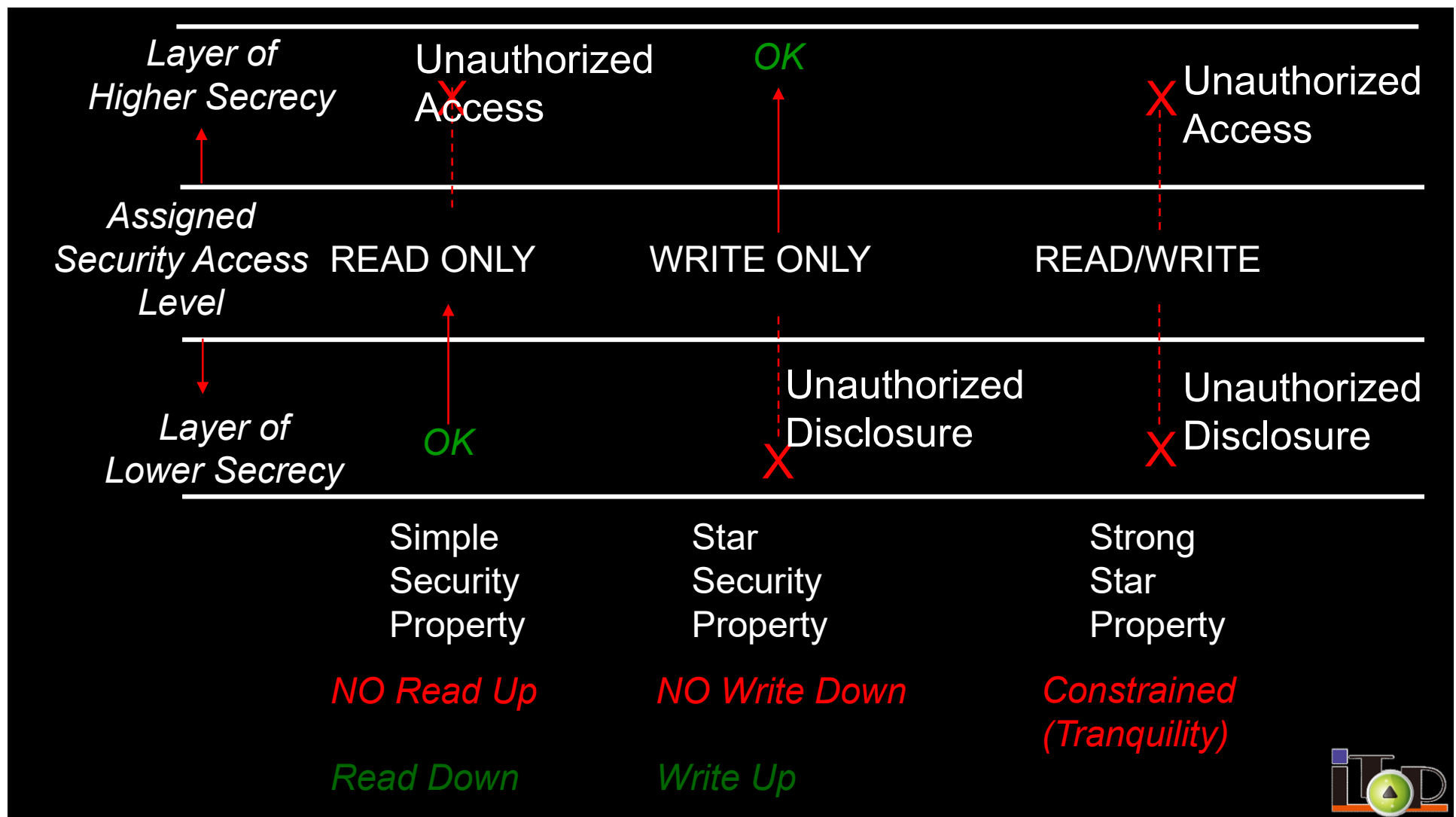
- 用什麼方法蒐集資料?
 - Syslog, txt import, Windows event
- 用什麼方法儲存資料?
 - Mysql, noSQL, MS SQL
- 用什麼方法分析資料?
 - Log parser, R language...一拖拉庫

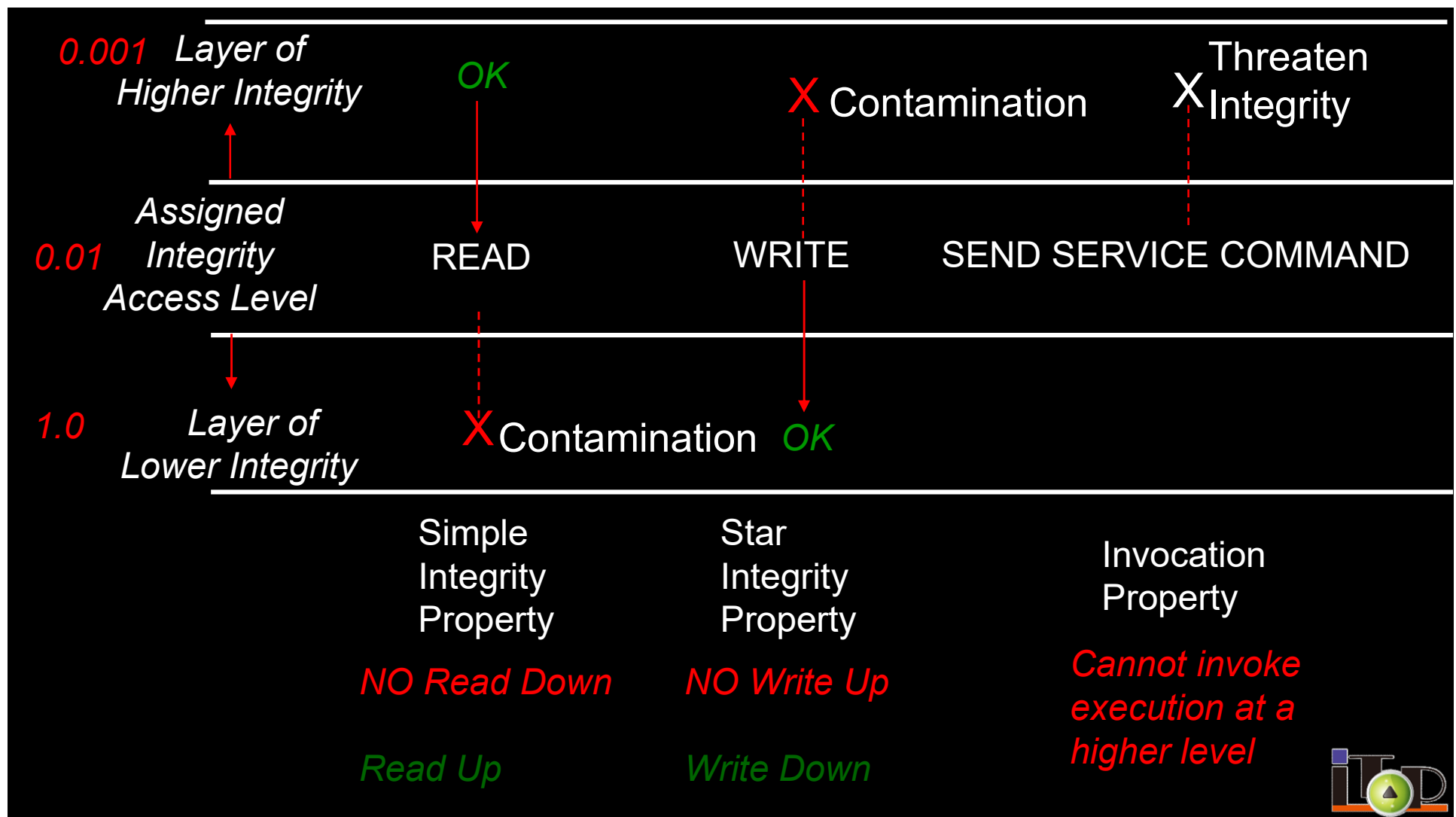
那些問題需要關注？

不是要滴水不漏，是要合理管控！！

誰可以把資料寫進去!!
誰可以讀資料出來!!







那...事件管理應該用
機密還是一致性?





那些事件應該發出告警？

典型的入侵程序



無預警的重開機重要嗎？

微軟說重開治百病







正常開關機記錄

| 等級 | 日期和時間 | 來源 | 事件識別碼 | 工作類別 |
|----|----------------------|----------|-------|------|
| 資訊 | 2015/7/7 下午 12:00:00 | EventLog | 6013 | 無 |
| 資訊 | 2015/7/6 下午 11:45:33 | EventLog | 6013 | 無 |
| 資訊 | 2015/7/6 下午 11:45:33 | EventLog | 6005 | 無 |
| 資訊 | 2015/7/6 下午 11:45:33 | EventLog | 6009 | 無 |
| 資訊 | 2015/7/6 下午 11:45:02 | EventLog | 6006 | 無 |
| 資訊 | 2015/7/6 下午 12:00:00 | EventLog | 6013 | 無 |
| 資訊 | 2015/7/5 下午 11:45:30 | EventLog | 6013 | 無 |
| 資訊 | 2015/7/5 下午 11:45:30 | EventLog | 6005 | 無 |
| 資訊 | 2015/7/5 下午 11:45:30 | EventLog | 6009 | 無 |
| 資訊 | 2015/7/5 下午 11:45:02 | EventLog | 6006 | 無 |
| 資訊 | 2015/7/5 下午 12:00:00 | EventLog | 6013 | 無 |
| 資訊 | 2015/7/4 下午 11:45:31 | EventLog | 6013 | 無 |
| 資訊 | 2015/7/4 下午 11:45:31 | EventLog | 6005 | 無 |
| 資訊 | 2015/7/4 下午 11:45:31 | EventLog | 6009 | 無 |
| 資訊 | 2015/7/4 下午 11:45:02 | EventLog | 6006 | 無 |
| 資訊 | 2015/7/4 下午 12:00:00 | EventLog | 6013 | 無 |
| 資訊 | 2015/7/3 下午 11:45:32 | EventLog | 6013 | 無 |
| 資訊 | 2015/7/3 下午 11:45:32 | EventLog | 6005 | 無 |
| 資訊 | 2015/7/3 下午 11:45:32 | EventLog | 6009 | 無 |



正常的開關機順序

6009：系統已啟動至windows登入畫面前

6005：系統服務啟動完成

6013：自動報時

6006：系統關機

正常的開關機順序



Windows登入畫面前

正常的開關機順序

Windows 登入畫面前



正常的開關機順序

Windows 登入畫面前



正常的開關機順序

Windows 登入畫面前



你說重開機可怕嗎？



回到剛才那個問題

那些件事該關注?!



作業系統偵查-事件記錄



| Windows 事件 ID | Windows client 事件 ID | 事件類型 | 描述 |
|---|---|---------|---|
| 512, 513, 514, 515, 516, 518, 519, 520 | 4608, 4609, 4610, 4611, 4612, 4614, 4615, 4616 | 系統事件 | 本地系統Process，例如系統啟動，關閉和系統時間的改變。 |
| 517 | 4612 | 清除的稽核日誌 | 所有稽核日誌清除事件 |
| 528, 540 | 4624 | 成功使用者登錄 | 所有使用者登錄事件 |
| 529, 530, 531, 532, 533, 534, 535, 536, 537, 539 | 4625 | 登錄失敗 | 所有使用者登錄失敗事件 |
| 538 | 4634 | 成功使用者退出 | 所有使用者退出事件 |
| 560, 562, 563, 564, 565, 566, 567, 568 | 4656, 4658, 4659, 4660, 4661, 4662, 4663, 4664 | 物件存取 | 當存取一給定的物件（檔案，目錄等）存取的類型(例如讀，寫，刪除)，存取是否成功或失敗，誰實施了這一行為 |
| 612 | 4719 | 稽核政策改變 | 稽核政策的改變 |

作業系統偵查-事件記錄

| Windows 事件 ID | Windows client 事件 ID | 事件類型 | 描述 |
|---|---|----------------|---|
| 624, 625, 626, 627, 628, 629, 630, 642, 644 | 4720, 4722, 4723, 4724, 4725, 4726, 4738, 4740 | 使用者帳號改變 | 使用者帳號的改變，像使用者帳號建立，刪除， 改變密碼等等 |
| (631 to 641) and (643, 645 to 666) | 4727 to 4737, 4739 to 4762 | 使用者群組改變 | 對一個使用者群組的所有改變，例如新增或移 除一個全局組或本地組，從全局組或本地新增 或移除成員等等 |
| 672, 680 | 4768, 4776 | 成功使用者帳號驗 證 | 當一個網域使用者帳號在網域控制站認證時， 產生使用者帳號成功登錄事件。 |
| 675, 681 | 4771, 4777 | 失敗使用者帳號驗 證 | 失敗使用者帳號登錄事件，當一個網域使用者 帳號在網域控制站認證時，產生不成功使用者 帳號登錄事件。 |
| 682, 683 | 4778, 4779 | Host Session狀態 | Session重新連接或斷開 |



如何來分析這些事件

複習一下上一次的議題



當你看到一棟房子
裡面有你極度想要的東西





你會先上下打量一下
要怎麼進去!!





嘗試著開鎖!!





無聲的破窗!!

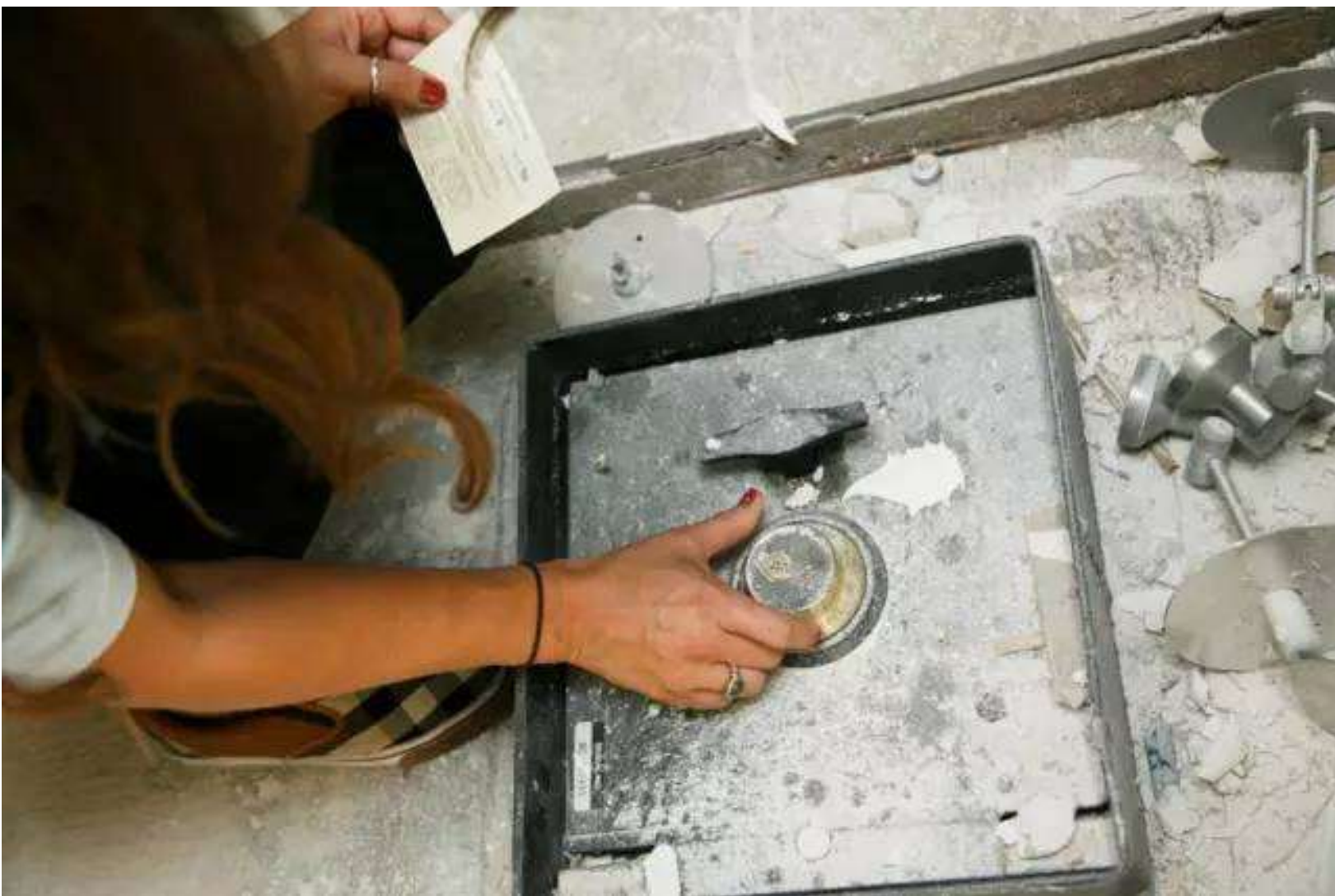




找到寶物!!

開始解開結界、開箱、貼粉專!!





榮登高富帥!!

迎娶白富美!!

成為人人稱羨的神仙伴侶!!





聽老衲一句話!!!

作夢爽一下就好，別當真啊!!





但事實相去不遠!!

一樣的行為!

應用在網站安全上是相同的!



典型的入侵程序

爬蛛

- 先找找網頁上有連結的，有那一些!!

憑經驗猜

- 多數用常見的名稱進行猜測(會出現大量的404)

開鎖

- 猜中後，可以開始針對你想隱藏的目錄會檔案進行存取(猜中了302、304、403、405)



典型的入侵程序

爬蛛

- 先找找網頁上有連結的，有那一些!!

憑經驗猜

- 多數用常見的名稱進行猜測(會出現大量的404)

開鎖

- 猜中後，可以開始針對你想隱藏的目錄會檔案進行存取(猜中了302、304、403、405)




我們可以這麼解釋

1. 某個入侵者會先大量的爬取，出現大量的200。
2. 接下來開始要猜猜看資源在那裡，出現大量的404
3. 當資源被猜中時，最常出現的是302、304、403、405
4. 最後就開始使用奇淫技巧，出現大量的500。
 - ◆ 檔案下載模組下載
 - ◆ 利用弱點或程式邏輯漏洞
 - ◆ 有外掛模組可上傳檔案，污染主機。
5. 得手資源



這樣的log量才多少行?



```
c:\Program Files (x86)\Log Parser 2.2>LogParser.exe "select count (*) from
C:\Users\Jason\OneDrive\LOG\20170304webattack\tpappw3clog\*.log" -i:w3c
COUNT(ALL *)
-----
6391922
Statistics:
-----
Elements processed: 6391922
Elements output:      1
Execution time:      96.24 seconds (00:01:36.24)
```

```
Statistics:
-----
Elements processed: 6391922
Elements output:      1
Execution time:      96.24 seconds (00:01:36.24)
```



找出有問題的記錄



統計狀態碼

以IP為基礎
統計狀態碼

以狀態碼統計URI

統計該IP
詢問的內容

針對特定的URI過濾

過濾每個URI
連線內容

首先統計一下IP與狀態的關係吧

```
c:\Program Files (x86)\Log Parser 2.2>LogParser.exe "select c-ip,sc-status  
, count(*) into f:\IPstatus.csv from C:\Users\Jason\OneDrive\LOG\20170304w  
ebattack\tpappw3clog\*.log group by c-ip,sc-status" -i:w3c -o:csv
```

Task completed with parse errors.

Parse errors:

7931 parse errors occurred during processing (To see details about the parse

error(s), execute the command again with a non-zero value for the "-e" argument)

Statistics:

Elements processed: 6391372

Elements output: 175996

Execution time: 100.33 seconds (00:01:40.33)



| | | 加總 - COUNT(ALL *) 欄標籤 | | | | | | | | | | | | | | |
|----|-----------------|-----------------------|-------|-----|-------|------|-----|-----|-------|-----|-----|------|----------|-------|-------|--|
| | | 列標籤 | 200 | 301 | 302 | 304 | 400 | 403 | 404 | 405 | 406 | 500 | 501 (空白) | 總計 | | |
| | | 66.249.77.31 | 86632 | 271 | 229 | 231 | | 1 | 143 | | | | | 87507 | | |
| | | 91.209.196.35 | 56681 | 221 | 11896 | | 244 | 23 | 11633 | 549 | | 3417 | 21 | 5 | 84690 | |
| | | 210.242.157.166 | 40970 | | 30490 | 2040 | | 37 | 70 | | | | | 73607 | | |
| | | 66.249.77.28 | 139 | | 43954 | 1 | | | | | | 3 | | 44097 | | |
| | | 66.249.79.173 | 29406 | 90 | 19 | 78 | | | 44 | | | | | 29637 | | |
| 1 | c-ip | 68.180.228.34 | 14870 | 311 | 10246 | 89 | | | 81 | 2 | | | | 25599 | | |
| 5 | 66.249.77.28 | 66.249.77.1 | 17858 | 99 | 69 | 78 | | | 46 | | | | | 1 | 18151 | |
| 6 | 210.242.157.166 | 119.176.134.95 | 7505 | | 7400 | 4 | | | 4 | | | | | | 14913 | |
| 10 | 66.249.79.149 | 66.249.79.149 | 54 | | 14716 | | | | | | | 3 | | | 14773 | |
| 11 | 91.209.196.35 | 176.9.50.244 | 12480 | 359 | 16 | | | | 48 | | | | | | 12903 | |
| 13 | 91.209.196.35 | 66.249.77.3 | 7963 | 62 | 9 | 54 | | | 29 | | | | | 2 | 8119 | |
| 15 | 68.180.228.34 | 61.216.146.174 | 3965 | | 3713 | 107 | | | 14 | | | | | | 7799 | |
| 16 | 119.176.134.95 | 220.134.40.219 | 4737 | | 252 | 1812 | | | 53 | | | | | | 6854 | |
| 19 | 66.249.77.29 | 66.249.77.29 | 40 | | 6272 | 1 | | | 1 | | | 4 | | 2 | 6320 | |
| 22 | 61.216.146.174 | 220.134.69.59 | 4676 | | 92 | 1418 | | | 26 | | | | | | 6212 | |
| 24 | 91.209.196.35 | 61.220.222.25 | 4691 | | 77 | 1365 | | | 51 | | | | | | 6184 | |
| 25 | 66.249.77.30 | 66.249.79.153 | 5977 | 41 | 9 | 38 | | | 19 | | | | | | 6084 | |
| 27 | 1.34.93.195 | 210.242.157.166 | 4649 | 48 | 1252 | | | | 28 | | | | | | 5977 | |
| 29 | 66.249.79.153 | 220.134.40.219 | 2894 | | 334 | 2525 | | 117 | 99 | | | | | | 5969 | |
| 31 | 210.242.157.166 | 1.34.93.195 | 3709 | 1 | 357 | 1320 | | | 53 | | | | | | 5440 | |
| 34 | 220.134.40.219 | 211.22.104.189 | 3971 | 43 | 1146 | | | | 17 | | | | | | 5177 | |
| 36 | 54.219.188.185 | 211.20.189.162 | 4396 | 3 | 230 | 78 | | | 357 | | | | | | 5064 | |
| 42 | 220.134.69.59 | 203.66.245.250 | 4441 | | 364 | 184 | | | 37 | | | | | | 5026 | |
| 45 | 66.249.82.92 | 54.219.188.185 | 2549 | | 1513 | | | | 833 | 4 | | 17 | 1 | | 4917 | |
| 48 | 61.220.222.25 | 123.193.117.210 | 3113 | 3 | 454 | 1318 | | | 6 | | | | | | 4894 | |
| 53 | 211.22.104.189 | 122.118.4.242 | 2700 | 1 | 57 | 822 | | | 7 | | | | | | 3587 | |
| 54 | 123.193.117.210 | 93.158.152.22 | 2829 | 133 | 456 | 5 | | | 63 | | | | | | 3486 | |
| 56 | 66.249.82.94 | 114.43.64.112 | 2359 | | 272 | 787 | | | 6 | | | | | | 3424 | |
| 59 | 218.161.55.152 | 218.161.55.152 | 1884 | | 123 | 1278 | | | 12 | | | | | | 3297 | |
| 60 | 66.249.82.93 | 61.221.35.159 | 2506 | 1 | 88 | 587 | | | 8 | | | | | | 3190 | |
| 62 | 110.75.145.1 | | | | | | | | | | | | | | | |
| 63 | 123.194.96.130 | | | | | | | | | | | | | | | |
| 65 | 110.75.145.2 | | | | | | | | | | | | | | | |
| 66 | 66.249.79.157 | | | | | | | | | | | | | | | |



再來統計一下IP、狀態及URI

```
c:\Program Files (x86)\Log Parser 2.2>LogParser.exe "select c-ip,sc-status,cs-uri-stem, count(*) into f:\IPstatusuri-91.209.196.35.csv from C:\Users\Jason\OneDrive\LOG\20170304webattack\tpappw3clog\*.log where c-ip='91.209.196.35' group by c-ip,sc-status,cs-uri-stem" -i:w3c -o:csv
```

Task completed with parse errors.

Parse errors:

7931 parse errors occurred during processing (To see details about the parse

error(s), execute the command again with a non-zero value for the "-e" argument)

Statistics:

Elements processed: 6391372

Elements output: 16142

Execution time: 93.50 seconds (00:01:33.50)



| | A | B | C | D |
|----|---------------|-----------|---|--------------|
| 1 | c-ip | sc-status | cs-uri-stem | COUNT(ALL *) |
| 2 | 91.209.196.35 | 501 | /upload/toIdz9O0.htm | 1 |
| 3 | 91.209.196.35 | 501 | /tools/Btk7gpDQ.htm | 1 |
| 4 | 91.209.196.35 | 501 | /Nessus409045921.html | 1 |
| 5 | 91.209.196.35 | 501 | /common/appServer/jvmReport.jsf | 1 |
| 6 | 91.209.196.35 | 501 | /blog/index.php | 13 |
| 7 | 91.209.196.35 | 501 | /3HFwKp0r.htm | 1 |
| 8 | 91.209.196.35 | 501 | /2012layout/Z01nN4cT.htm | 1 |
| 9 | 91.209.196.35 | 501 | /2012layout/img/Zr7nTfdJ.htm | 1 |
| 10 | 91.209.196.35 | 501 | /2012layout/css/tGDmgulr.htm | 1 |
| 11 | 91.209.196.35 | 500 | /wordpress/ | 4 |
| 12 | 91.209.196.35 | 500 | /UYmTXdvH.rem | 1 |
| 13 | 91.209.196.35 | 500 | /UserVerify_1.aspx | 11 |
| 14 | 91.209.196.35 | 500 | /UoRm8Vcf. | 1 |
| 15 | 91.209.196.35 | 500 | /u4b0qqzk.aspx | 4 |
| 16 | 91.209.196.35 | 500 | /status.xsl. | 2 |
| 17 | 91.209.196.35 | 500 | /ShoppingCartTW-tcb.aspx | 1 |
| 18 | 91.209.196.35 | 500 | /ShoppingCartOversea.aspx | 1 |
| 19 | 91.209.196.35 | 500 | /ShoppingCart.aspx | 9 |
| 20 | 91.209.196.35 | 500 | /Shoppingcart.aspx | 8 |
| 21 | 91.209.196.35 | 500 | /search=<script>alert('XSS')</script> | 2 |
| 22 | 91.209.196.35 | 500 | /scripts/u4b0qqzk.aspx | 2 |
| 23 | 91.209.196.35 | 500 | /scripts/search=<script>alert('XSS')</script> | 1 |
| 24 | 91.209.196.35 | 500 | /scripts/plcpt5n.aspx | 2 |
| 25 | 91.209.196.35 | 500 | /scripts/nessus"><script>alert('django_admin_xss.nasl')</script>/ | 1 |

如何以R來轉換分析的工作



#載入IIS Log

Require(data.table)

Setwd("Log File Directory")

取得所有的LOG檔案清單

log_files <- Sys.glob("*.log")



#將所有的檔案讀入並且聯集他們

```
IIS <- do.call( "rbind", lapply( log_files, read.csv, sep = " ",  
header = FALSE, comment.char = "#", na.strings = "-" ) )
```

```
# 附予欄位名稱 – 從第一行的LOG檔案頭標示的檔案讀入  
colnames(IIS) <- c("date", "time", "s_ip", "cs_method",  
"cs_uri_stem", "cs_uri_query", "s_port", "cs_username",  
"c_ip", "cs_User_Agent", "sc_status", "sc_substatus",  
"sc_win32_status", "sc_bytes", "cs_bytes", "time-taken")
```



#將這個變更回寫到data.table

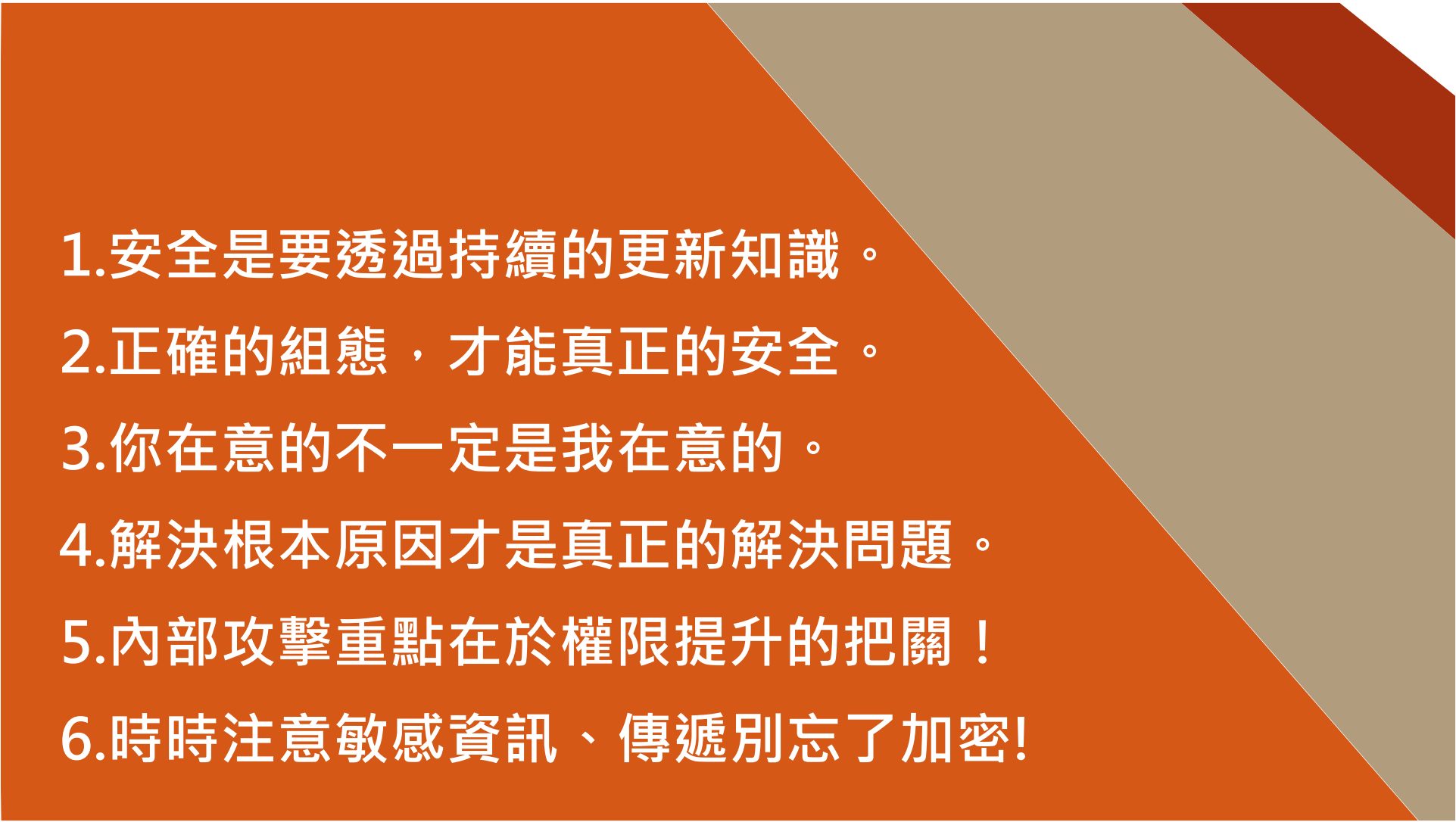
```
IIS <- data.table( IIS )
```

#完成查詢，列出狀態、使用者名稱，查詢的URI及伺服端的反應狀態

```
IIS[, .N, by =  
list(sc_status,cs_username,cs_uri_stem,sc_win32_status) ]
```




本日小結

- 
- 1.安全是要透過持續的更新知識。
 - 2.正確的組態，才能真正的安全。
 - 3.你在意的不一定是我在意的。
 - 4.解決根本原因才是真正的解決問題。
 - 5.內部攻擊重點在於權限提升的把關！
 - 6.時時注意敏感資訊、傳遞別忘了加密！



Q&A

Thank you

