探索機器推論應用在資安事件分析的旅程

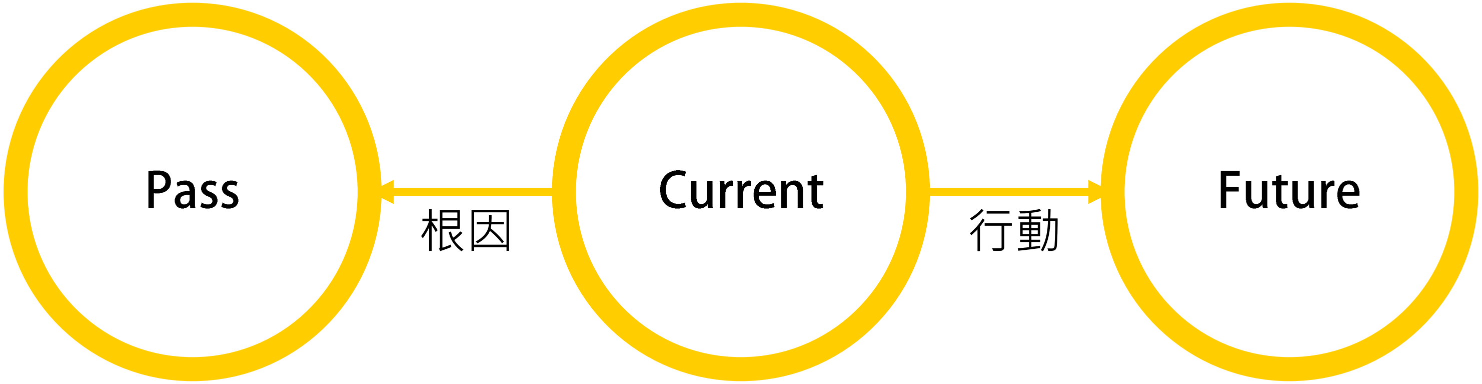
劉順德 2016.7.13

簡介

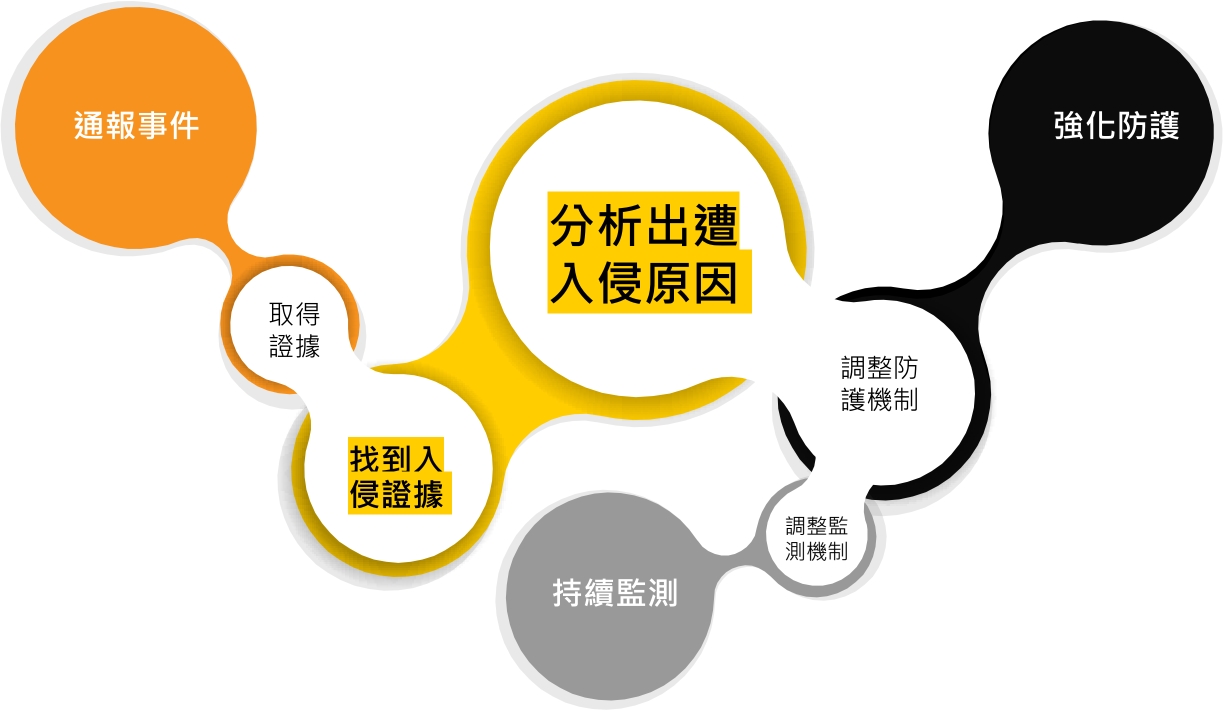
- 現職：中華電信大數據辦公室商業分析科
- 學歷：國立中央大學資訊管理博士
- 經歷：
  中華電信研究院資通安全研究所研究員(~2016)
- 專長：
  網路攻擊偵測技術結合大數據技術
  新興資安威脅分析技術
  數位鑑識技術
- 個人興趣
  機器學習/人工智能
  網路安全攻擊偵測與防護技術
  雲端資安
- Email：rogerliu@cht.com.tw

資安事件分析

理解事件發生原因及影響，提供控制措施、降低再發生或減少損失的作為

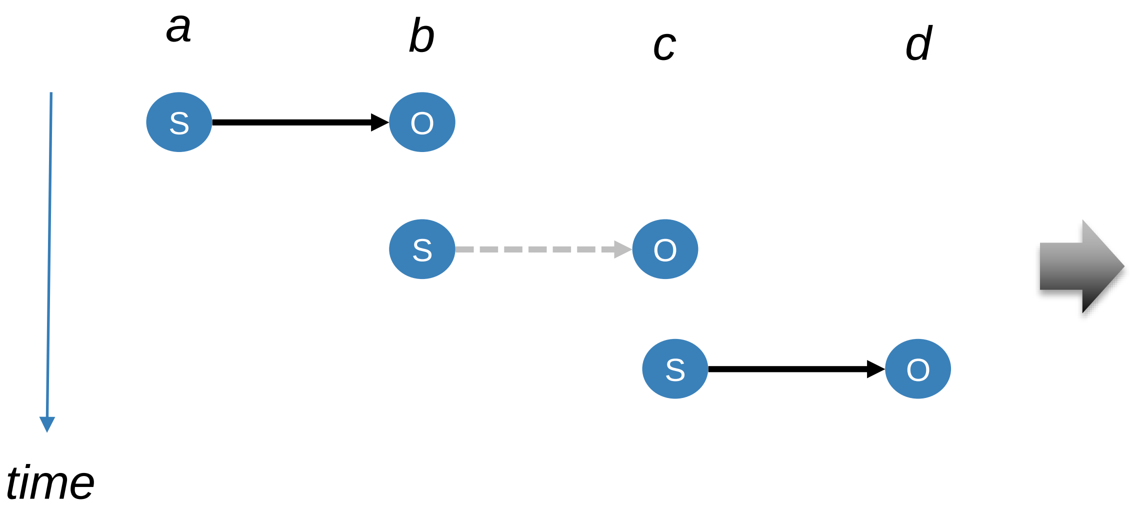


理想的資安事件分析



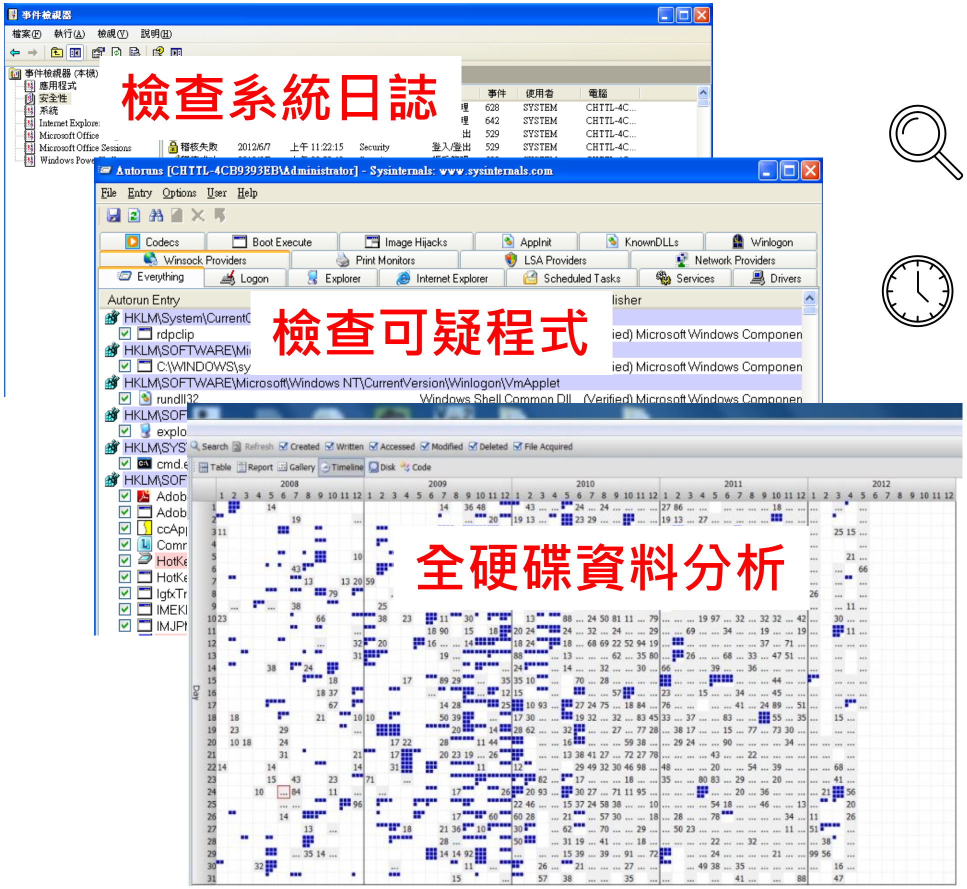
Event-based Correlation

E: <T, Subject, Object, Action>



a → *b*
c → *d*

資安事件分析的挑戰



```
理 628 SYSTEM CHTTL-4C...
理 642 SYSTEM CHTTL-4C...
出 529 SYSTEM CHTTL-4C...
稽核失敗 2012/6/7 上午 11:22:15 Security 登入/登出 529 SYSTEM CHTTL-4C...
```

```
HKLM\System\CurrentC
☑ rdpclip                                  ied) Microsoft Windows Componen
HKLM\SOFTWARE\Mi
☑ C:\WINDOWS\sy                            ied) Microsoft Windows Componen
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet
☑ rundll32            Windows Shell Common Dll   (Verified) Microsoft Windows Componen
HKLM\SOF
☑ explo
HKLM\SYS
☑ cmd.e
HKLM\SOF
☑ Adob
☑ Adob
☑ ccApp
☑ Comr
☑ HotKe
☑ HotKe
☑ IgfxTr
☑ IMEKI
☑ IMJPI
```

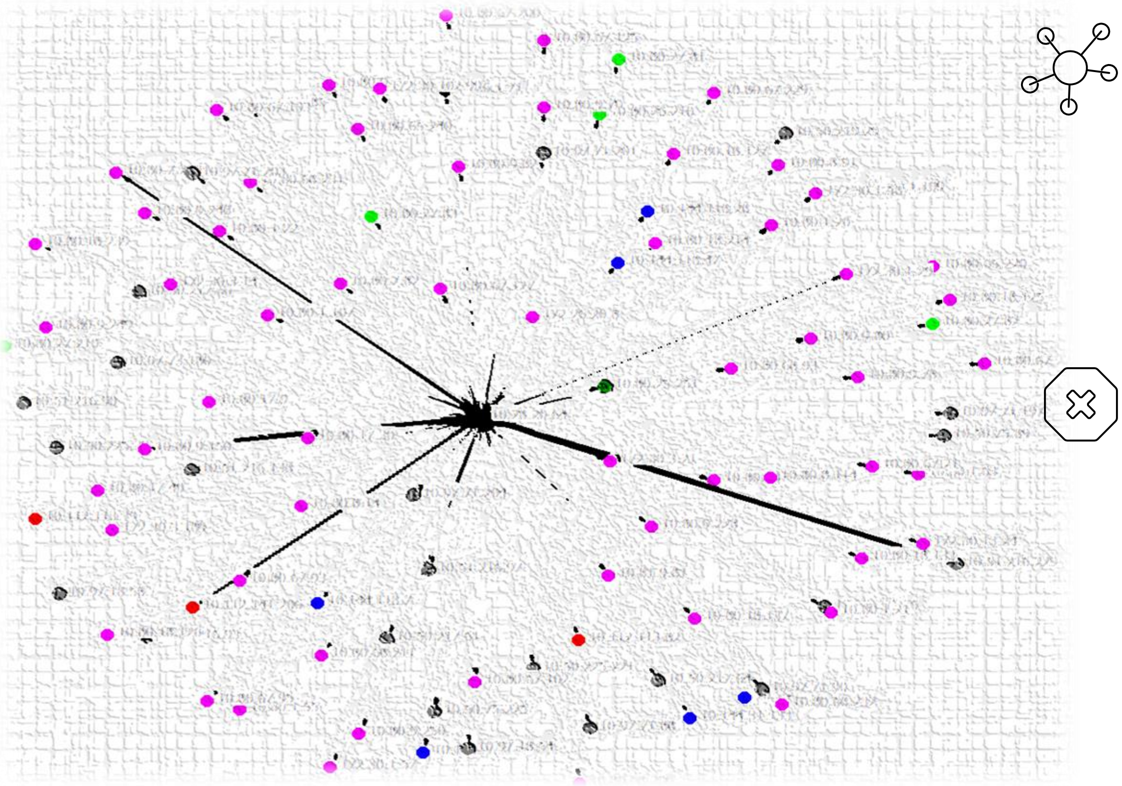
檢查系統日誌

檢查可疑程式

全硬碟資料分析

- 大量非結構化的資料
- 限定時間完成

常發生的問題 --Network



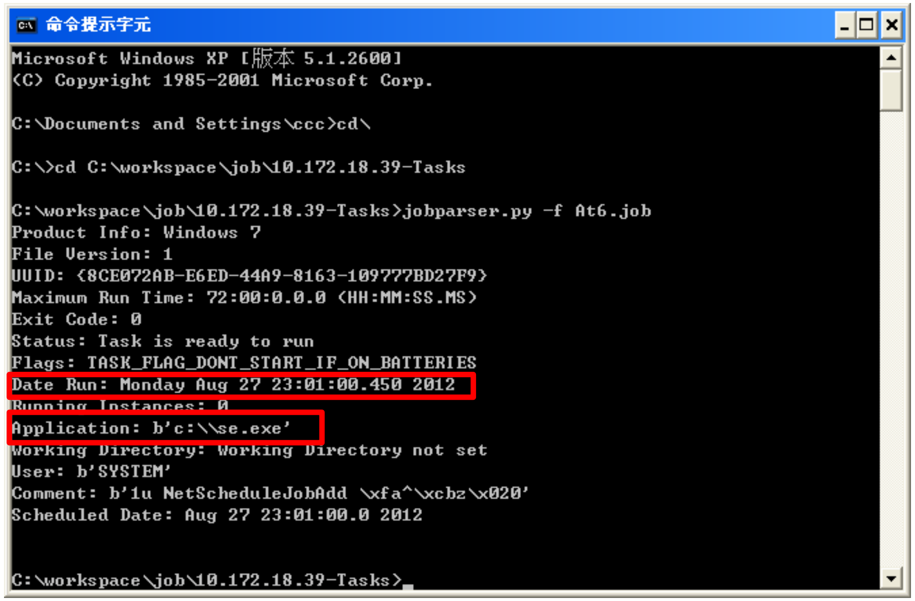
過多的可能連線關係

Policy

未保留日誌？

Sampling

常發生的問題--Host



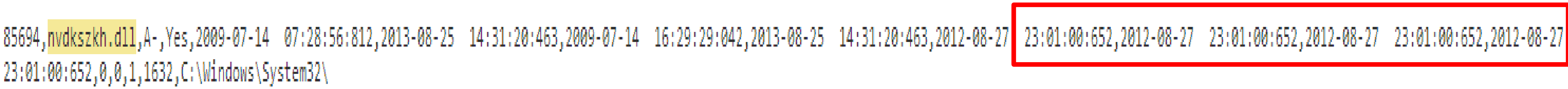
```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ccc>cd\

C:\>cd C:\workspace\job\10.172.18.39-Tasks

C:\workspace\job\10.172.18.39-Tasks>jobparser.py -f At6.job
Product Info: Windows 7
File Version: 1
UUID: {8CE072AB-E6ED-44A9-8163-109777BD27F9}
Maximum Run Time: 72:00:0.0.0 (HH:MM:SS.MS)
Exit Code: 0
Status: Task is ready to run
Flags: TASK_FLAG_DONT_START_IF_ON_BATTERIES
Date Run: Monday Aug 27 23:01:00.450 2012
Running Instances: 0
Application: b'c:\\se.exe'
Working Directory: Working Directory not set
User: b'SYSTEM'
Comment: b'1u NetScheduleJobAdd \xfa^\xcbz\x020'
Scheduled Date: Aug 27 23:01:00.0 2012


C:\workspace\job\10.172.18.39-Tasks>_
```

關鍵檔案鏈結中斷

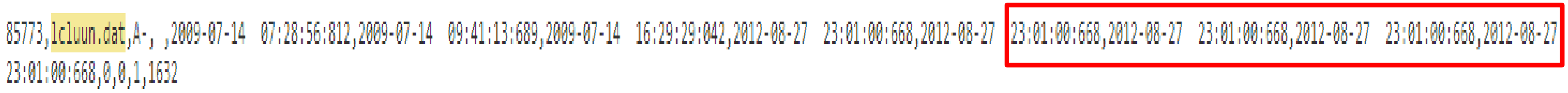
Reference

零碎的關聯

Time-related



```
85694,nvdkszkh.dll,A-,Yes,2009-07-14  07:28:56:812,2013-08-25  14:31:20:463,2009-07-14  16:29:29:042,2013-08-25  14:31:20:463,2012-08-27  23:01:00:652,2012-08-27  23:01:00:652,2012-08-27  23:01:00:652,2012-08-27
23:01:00:652,0,0,1,1632,C:\Windows\System32\
```



```
85773,lcluun.dat,A-, ,2009-07-14  07:28:56:812,2009-07-14  09:41:13:689,2009-07-14  16:29:29:042,2012-08-27  23:01:00:668,2012-08-27  23:01:00:668,2012-08-27  23:01:00:668,2012-08-27  23:01:00:668,2012-08-27
23:01:00:668,0,0,1,1632
```

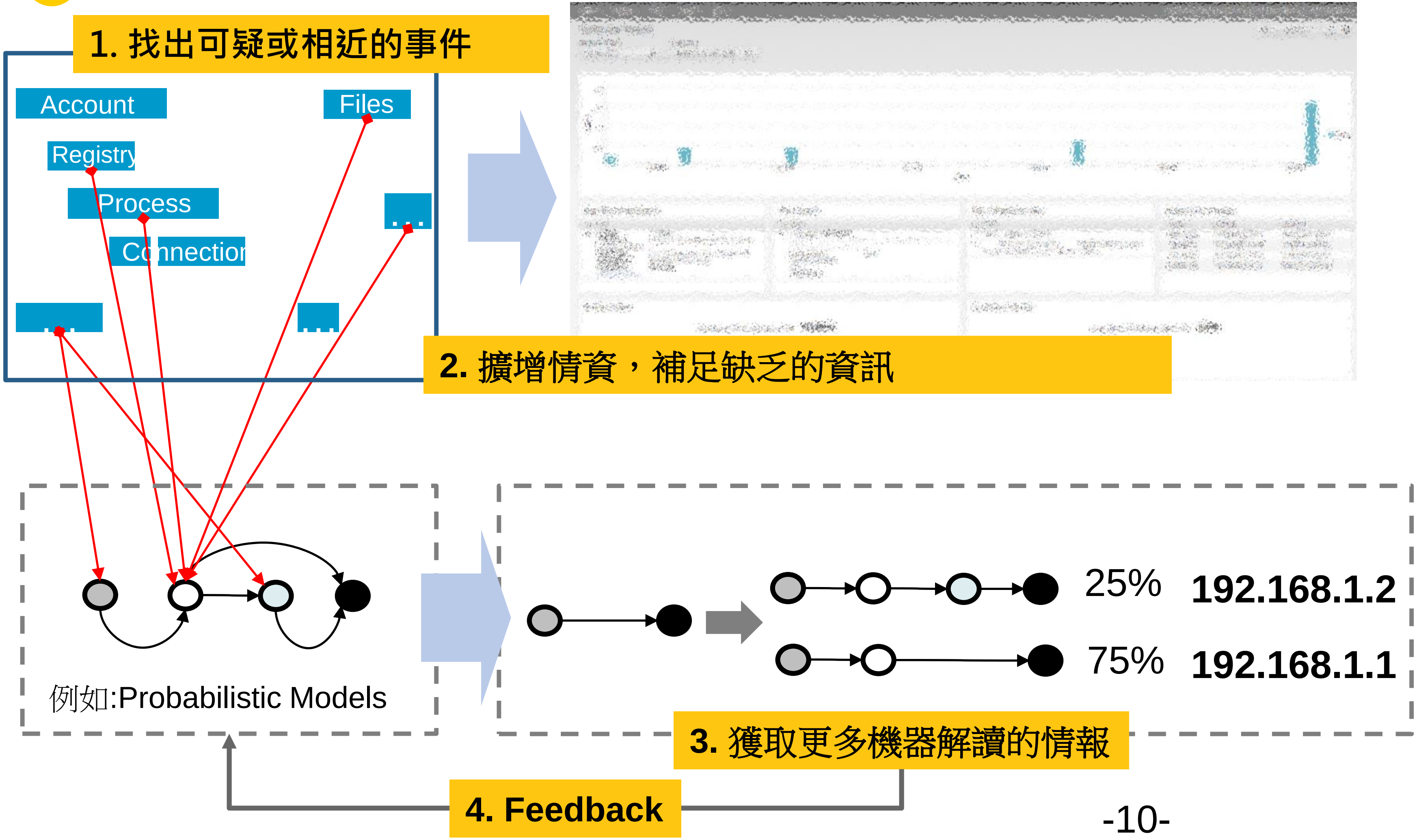
有可能讓機器共同協作嗎？

***A**ugmented **I**ntelligence*

Enhancement of human intelligence

提供控制措施、降低再發生或減少損失的作為

Reuse best practices



1. 找出可疑或相近的事件

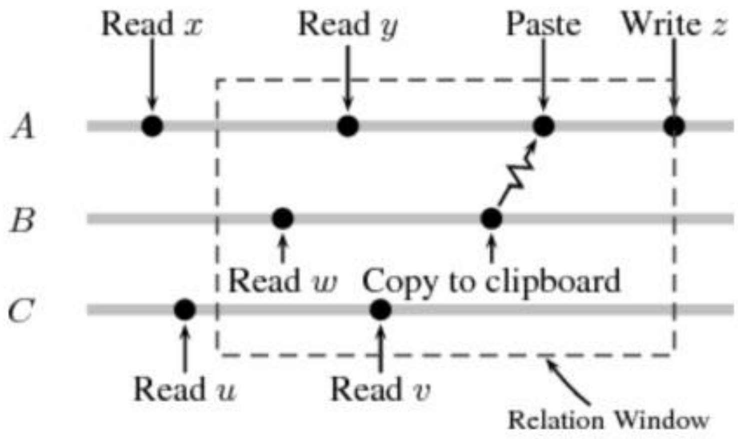
2. 擴增情資，補足缺乏的資訊

例如:Probabilistic Models

3. 獲取更多機器解讀的情報

4. Feedback

找出可疑或相近的事件



A, B, C: Process
x, y, z, w, u, v, z: Files

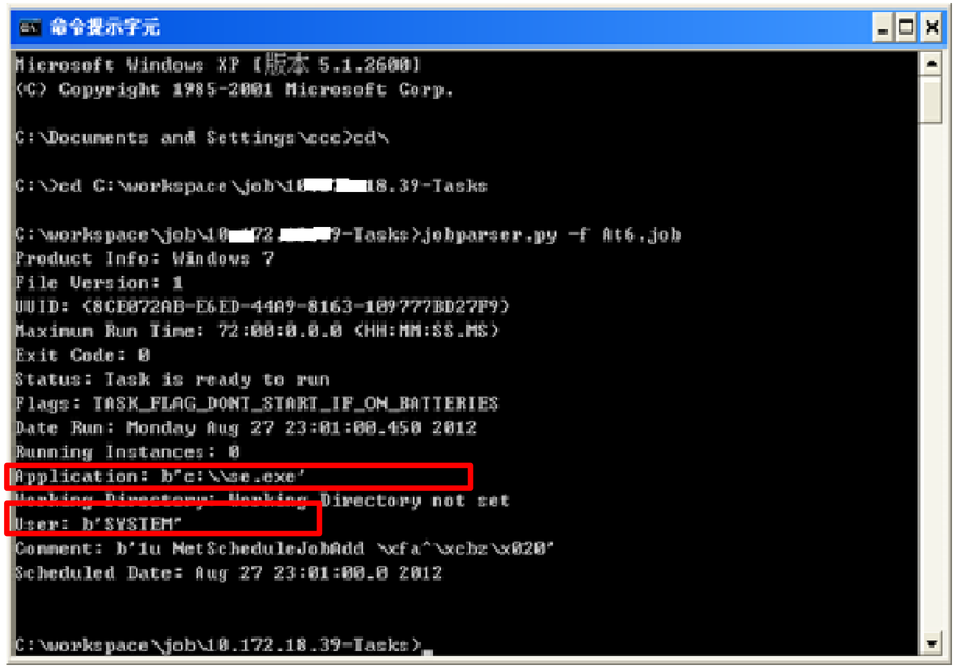
- Temporal approach

1. <y, w, v> → z
2. <y> → z

- Causal approach

1. <y, w>→z

Case: Temporal Approach



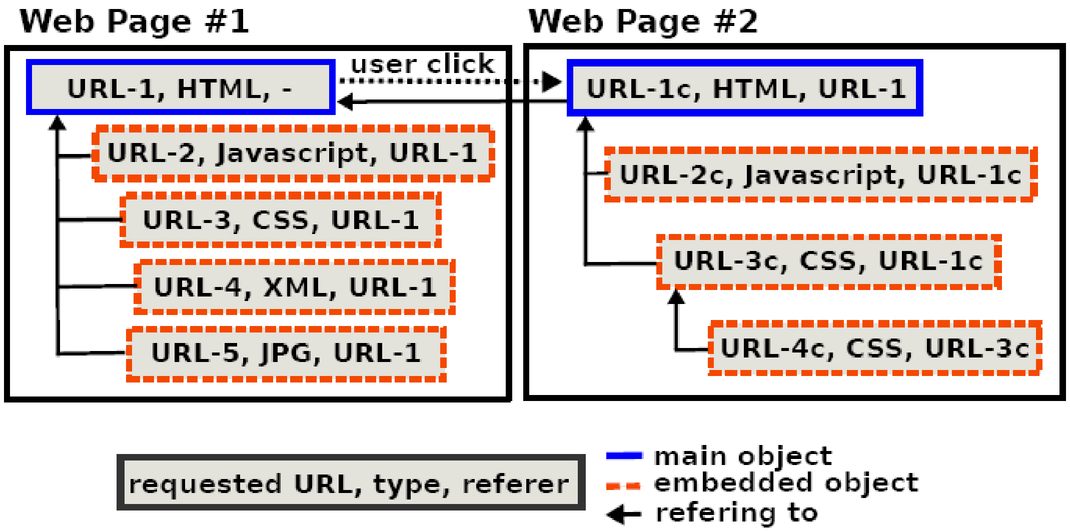
```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ccc>cd\

C:\>cd C:\workspace\job\10[redacted]18.39-Tasks

C:\workspace\job\10[redacted]72.[redacted]9-Tasks>jobparser.py -f At6.job
Product Info: Windows 7
File Version: 1
UUID: (8CE072AB-E6ED-44A9-8163-109777BD27F9)
Maximum Run Time: 72:00:0.0.0 (HH:MM:SS.MS)
Exit Code: 0
Status: Task is ready to run
Flags: TASK_FLAG_DONT_START_IF_ON_BATTERIES
Date Run: Monday Aug 27 23:01:00.450 2012
Running Instances: 0
Application: b'c:\\se.exe'
Working Directory: Working Directory not set
User: b'SYSTEM'
Comment: b'1u NetScheduleJobAdd \xfa^\xcbz\x020'
Scheduled Date: Aug 27 23:01:00.0 2012


C:\workspace\job\10.172.18.39-Tasks>_
```

前後15~30秒鐘相關的檔案

JOB: timestamp, user, process, run_user, file_name, file_path, timestamp_schedule
FILE: timestamp, user, process, name, path, c_time, m_time, a_time, hash, size

```
85694,nvdkszkh.dll,A-,Yes,2009-07-14  07:28:56:812,2013-08-25  14:31:20:463,2009-07-14  16:29:29:042,2013-08-25  14:31:20:463,2012-08-27  23:01:00:652,2012-08-27  23:01:00:652,2012-08-27  23:01:00:652,2012-08-27
23:01:00:652,0,0,1,1632,C:\Windows\System32\

85773,lcluun.dat,A-, ,2009-07-14  07:28:56:812,2009-07-14  09:41:13:689,2009-07-14  16:29:29:042,2012-08-27  23:01:00:668,2012-08-27  23:01:00:668,2012-08-27  23:01:00:668,2012-08-27  23:01:00:668,2012-08-27
23:01:00:668,0,0,1,1632
```

Case: Advanced Temporal Approach



Data source: Gold mining in a River of Internet Content Traffic

1. Filter

↘98.4%

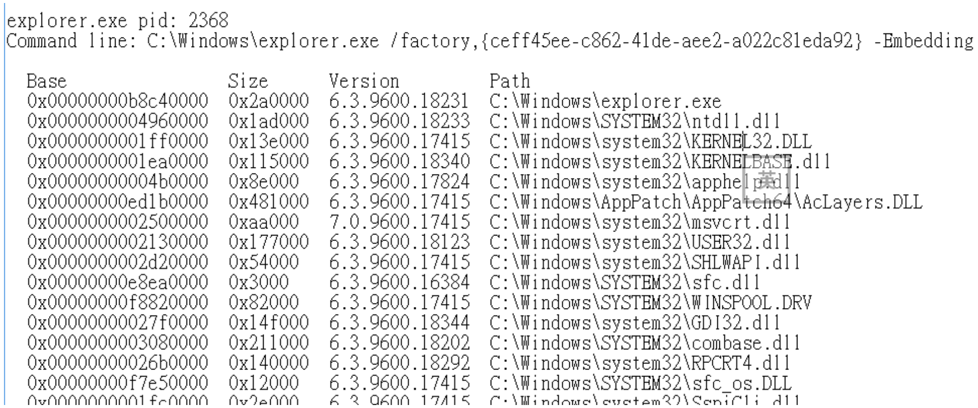
2. Merge by Time Slot

10~15秒鐘視為相關行為

HTTP: timestamp, sip, sport, url, dport, useragent, size
TCP: timestamp, user, process, sip, sport, dip, dport, status

Case: Causal Approach

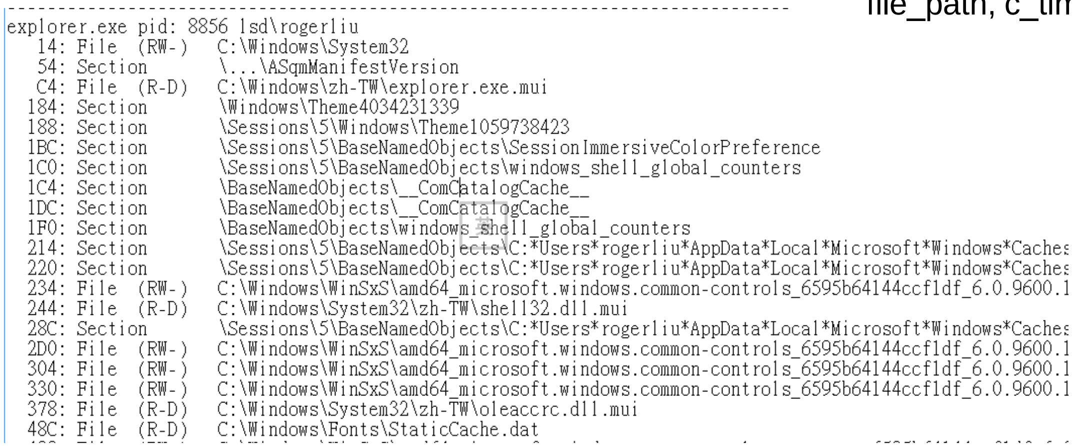
Import DLLs



```
explorer.exe pid: 2368
Command line: C:\Windows\explorer.exe /factory,{ceff45ee-c862-41de-aee2-a022c81eda92} -Embedding

  Base                Size      Version          Path
  0x00000000b8c40000  0x2a0000  6.3.9600.18231   C:\Windows\explorer.exe
  0x0000000004960000  0x1ad000  6.3.9600.18233   C:\Windows\SYSTEM32\ntdll.dll
  0x000000001ff0000   0x13e000  6.3.9600.17415   C:\Windows\system32\KERNEL32.DLL
  0x000000001ea0000   0x115000  6.3.9600.18340   C:\Windows\system32\KERNELBASE.dll
  0x00000000004b0000  0x8e000   6.3.9600.17824   C:\Windows\system32\apphelp.dll
  0x00000000ed1b0000  0x481000  6.3.9600.17415   C:\Windows\AppPatch\AppPatch64\AcLayers.DLL
  0x0000000002500000  0xaa000   7.0.9600.17415   C:\Windows\system32\msvcrt.dll
  0x0000000002130000  0x177000  6.3.9600.18123   C:\Windows\system32\USER32.dll
  0x0000000002d20000  0x54000   6.3.9600.17415   C:\Windows\system32\SHLWAPI.dll
  0x00000000e8ea0000  0x3000    6.3.9600.16384   C:\Windows\SYSTEM32\sfc.dll
  0x00000000f8820000  0x82000   6.3.9600.17415   C:\Windows\SYSTEM32\WINSPOOL.DRV
  0x00000000027f0000  0x14f000  6.3.9600.18344   C:\Windows\system32\GDI32.dll
  0x0000000003080000  0x211000  6.3.9600.18202   C:\Windows\SYSTEM32\combase.dll
  0x00000000026b0000  0x140000  6.3.9600.18292   C:\Windows\system32\RPCRT4.dll
  0x00000000f7e50000  0x12000   6.3.9600.17415   C:\Windows\SYSTEM32\sfc_os.DLL
  0x000000001fc0000   0x2e000   6.3.9600.17415   C:\Windows\system32\SspiCli.dll
```

Open Files

FILE: timestamp, user, process, file_name, file_path, c_time, m_time, a_time, hash, size



```
--------------------------------------------------------------------------------
explorer.exe pid: 8856 lsd\rogerliu
   14: File  (RW-)   C:\Windows\System32
   54: Section       \...\ASqmManifestVersion
   C4: File  (R-D)   C:\Windows\zh-TW\explorer.exe.mui
  184: Section       \Windows\Theme4034231339
  188: Section       \Sessions\5\Windows\Theme1059738423
  1BC: Section       \Sessions\5\BaseNamedObjects\SessionImmersiveColorPreference
  1C0: Section       \Sessions\5\BaseNamedObjects\windows_shell_global_counters
  1C4: Section       \BaseNamedObjects\__ComCatalogCache__
  1DC: Section       \BaseNamedObjects\__ComCatalogCache__
  1F0: Section       \BaseNamedObjects\windows_shell_global_counters
  214: Section       \Sessions\5\BaseNamedObjects\C:*Users*rogerliu*AppData*Local*Microsoft*Windows*Caches
  220: Section       \Sessions\5\BaseNamedObjects\C:*Users*rogerliu*AppData*Local*Microsoft*Windows*Caches
  234: File  (RW-)   C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9600.1
  244: File  (R-D)   C:\Windows\System32\zh-TW\shell32.dll.mui
  28C: Section       \Sessions\5\BaseNamedObjects\C:*Users*rogerliu*AppData*Local*Microsoft*Windows*Caches
  2D0: File  (RW-)   C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9600.1
  304: File  (RW-)   C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9600.1
  330: File  (RW-)   C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9600.1
  378: File  (R-D)   C:\Windows\System32\zh-TW\oleaccrc.dll.mui
  48C: File  (R-D)   C:\Windows\Fonts\StaticCache.dat
```

擴增資料，補充缺乏的部分

Unknown URL
Unknown IP
Unknown Process
Unknown Executable
Unknown Port
Unknown DLL
Unknown Event
…

Cache DB

從擴增的歷程找出
事件相關性

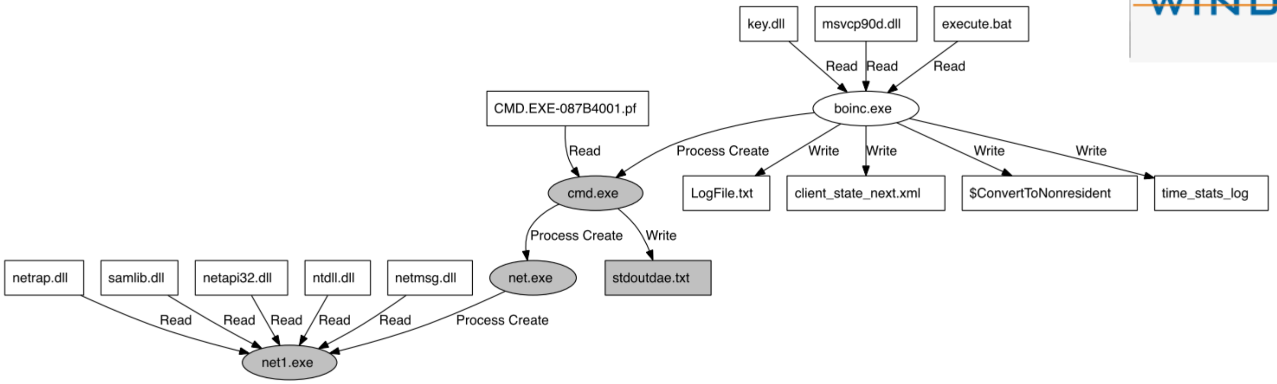
virustotal

URLVoid

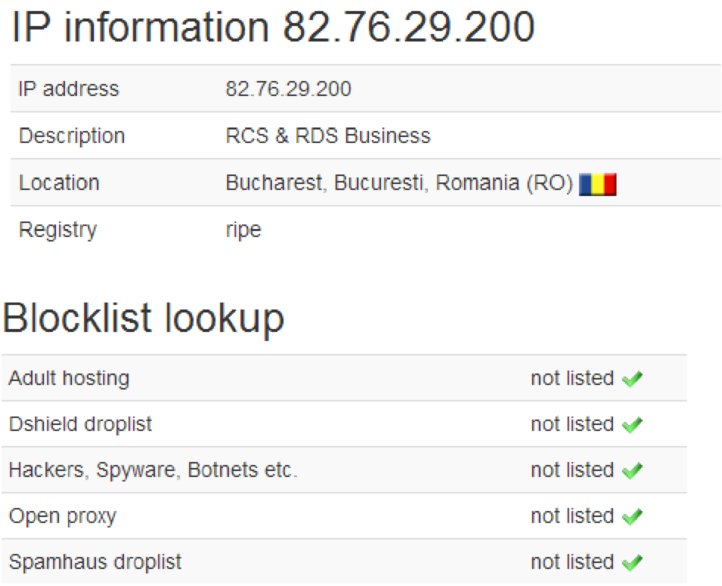
Metadefender™
APPLICATIONS AND THREAT INTELLIGENCE PLATFORM

Malware Knowledge Base

Randy Franklin Smith's ULTIMATE WINDOWS SECURITY .COM



Example

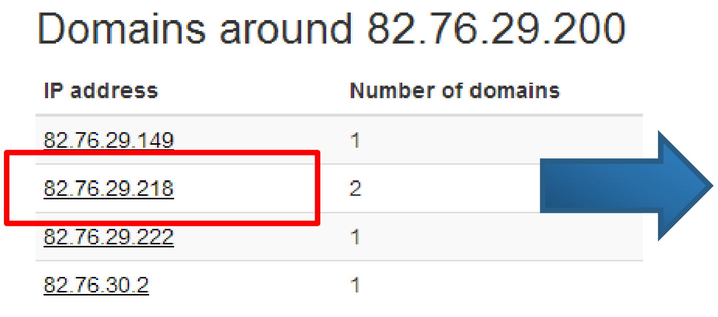


IP information 82.76.29.200

IP address	82.76.29.200
Description	RCS & RDS Business
Location	Bucharest, Bucuresti, Romania (RO)
Registry	ripe

Blocklist lookup

Adult hosting	not listed ✓
Dshield droplist	not listed ✓
Hackers, Spyware, Botnets etc.	not listed ✓
Open proxy	not listed ✓
Spamhaus droplist	not listed ✓

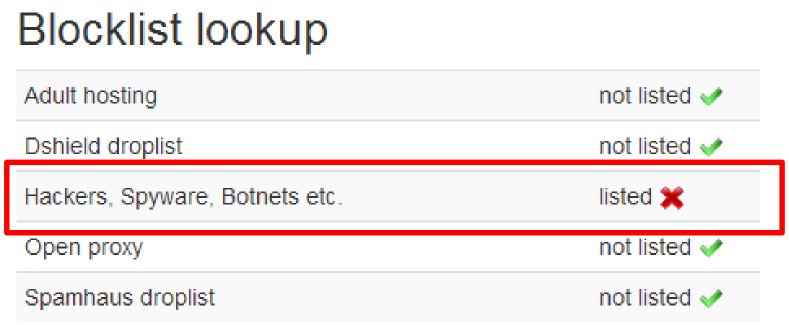


Domains around 82.76.29.200

IP address	Number of domains
82.76.29.149	1
82.76.29.218	2
82.76.29.222	1
82.76.30.2	1

地圖
衛星檢視
布夫泰亞 Buftea
Buciumeni
奧托佩尼 Otopeni
Tunari
Afumați
基蒂拉 Chitila
Sector 1
沃倫塔里 Voluntari
Găneasa
Dragomirești-Vale
Fundeni
Brănești
Ciorogârla
Roșu
布加勒斯特 București
Cernica
Domnești
Rahova
Cățelu
Tânganu
布拉加迪魯 Bragadiru
Sector 4
Glina
米赫伊萊什蒂 Mihăilești
Jilava
Dărăști-Ilfov
Berceni
Frumușani
E60
E81
E85

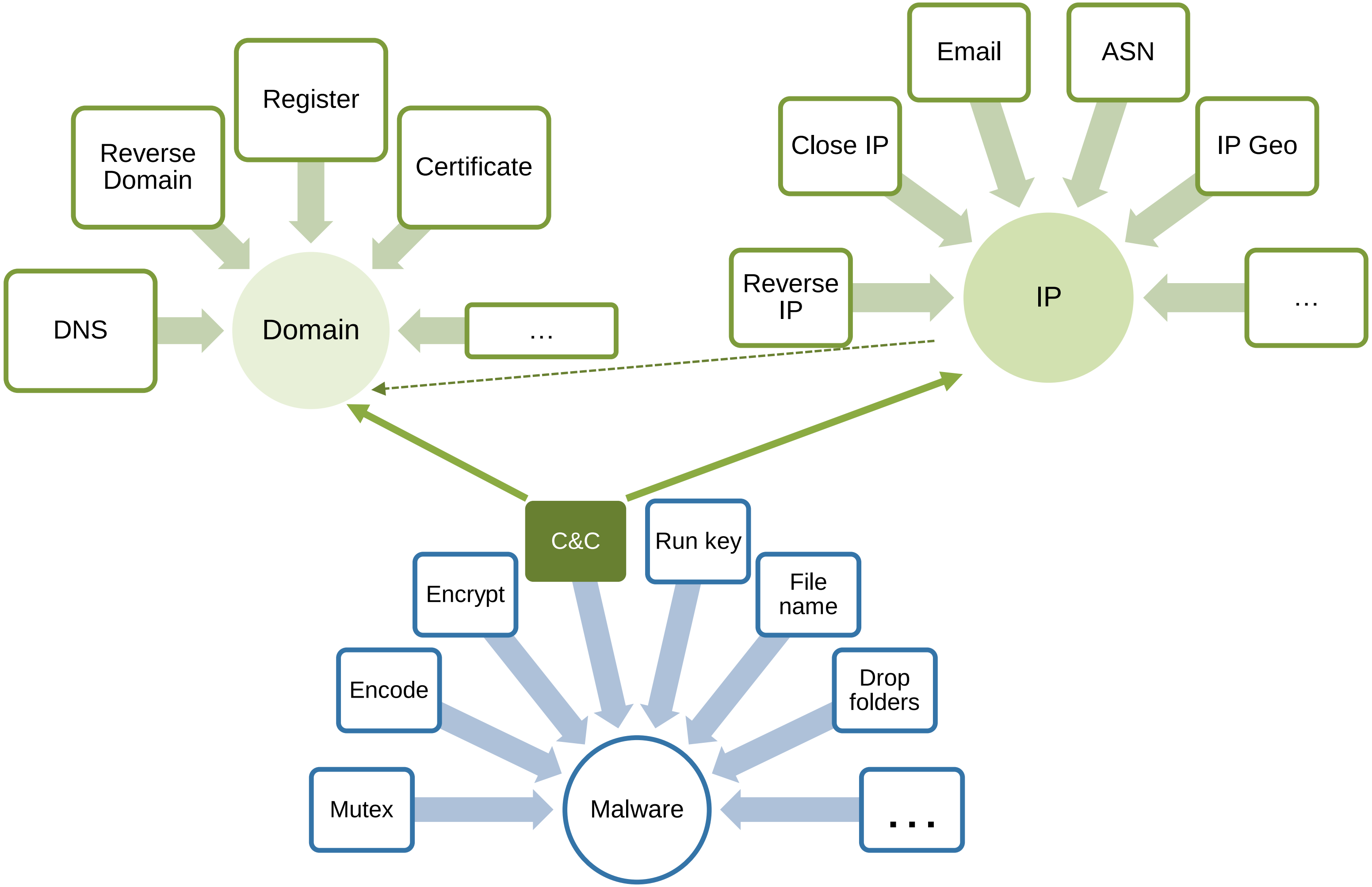
找到另一個可疑IP 82.76.29.218



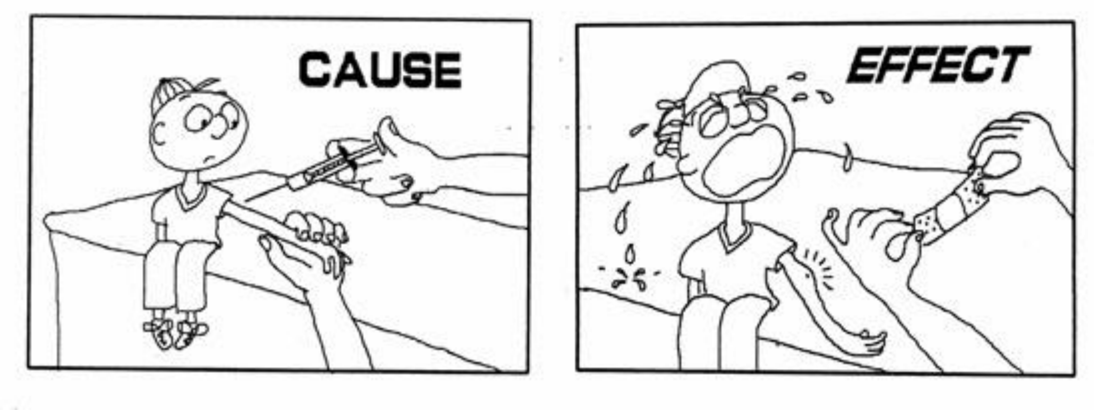
Blocklist lookup

Adult hosting	not listed ✓
Dshield droplist	not listed ✓
Hackers, Spyware, Botnets etc.	listed ✗
Open proxy	not listed ✓
Spamhaus droplist	not listed ✓

擴增資料關係


Register
Reverse Domain
Certificate
DNS
Domain
…
Email
ASN
Close IP
IP Geo
Reverse IP
IP
…
C&C
Run key
Encrypt
File name
Encode
Drop folders
Mutex
Malware
…

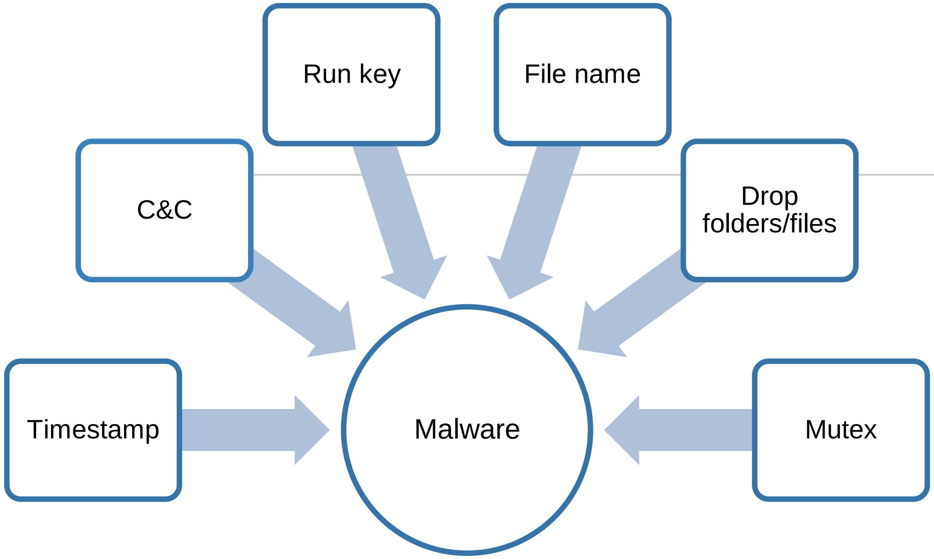
獲取更多機器解讀的情報



Data source: http://esl.cmswiki.wikispaces.net/Activities+and+Strategies+--+Cause+and+Effect

定義Effect

- 已知惡意程式
- 已知惡意網址
- 已知資安告警事件
- 已知高風險連線
- 未簽章的自動啟動檔案
- 未簽章的可執行檔案
- 遠端登入事件
- 帳號建立事件
- ....



Run key

File name

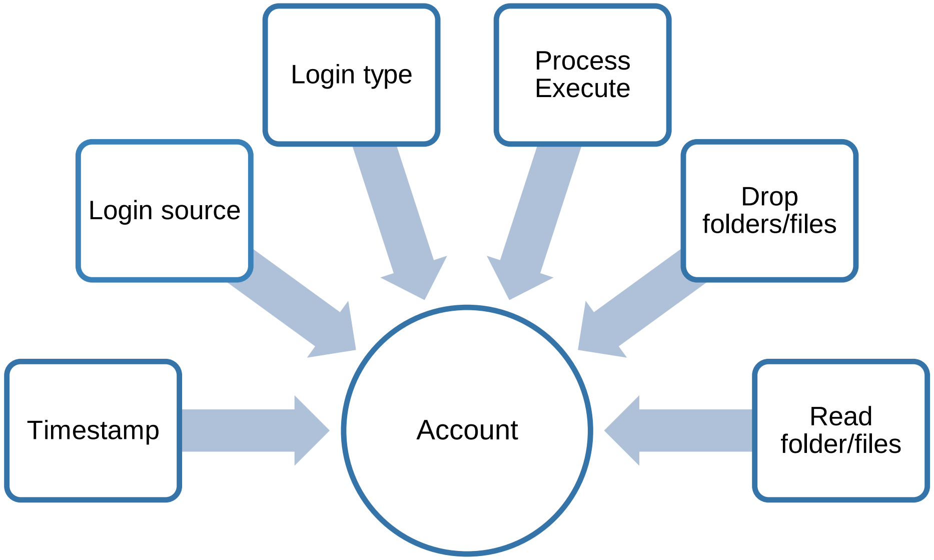
C&C

Drop folders/files

Timestamp

Malware

Mutex



Login type

Process Execute

Login source

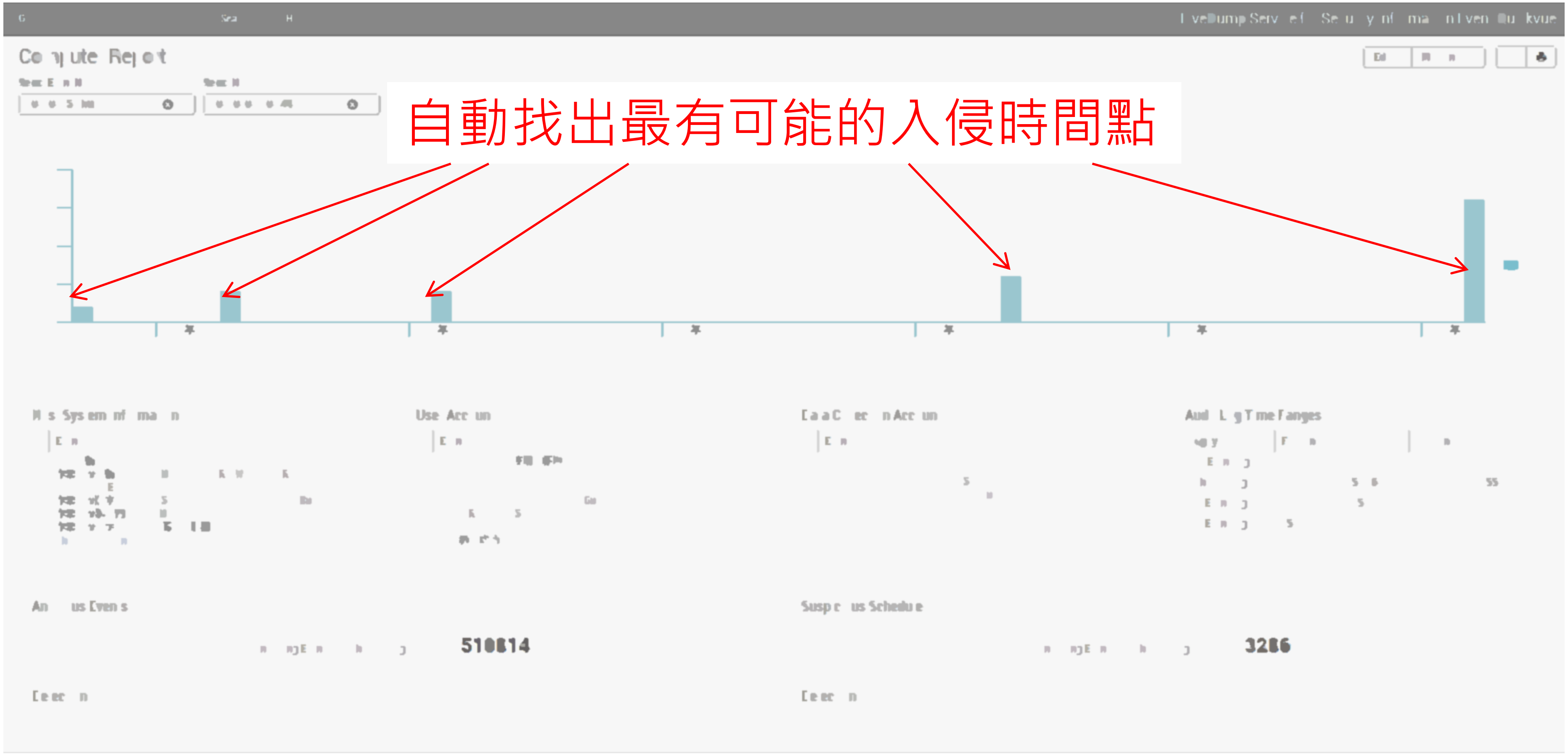
Drop folders/files

Timestamp

Account

Read folder/files

點出可能的發生時間點



Compute Report

自動找出最有可能的入侵時間點

User Account

Audit Log Time Ranges

Anomalous Events

510814

Suspicious Schedule

3286

定義關係

<T, Cause, Effect, Artifact>

FILE: <timestamp, (user, process), (file_name, file_path, c_time, m_time, a_time, hash, size..), MFT>
PROCESS: <timestamp, (user, process), (process, file_name, file_path…), PSLIST>
….

HTTP: <timestamp, (user, process), (sip, sport, url, dport, useragent, size…), PROXY>
TCP: <timestamp, (user, process), (sip, sport, dip, dport, status..), NETSTAT>
….

malware: <timestamp, (user, process), (file_name, file_path, c_time, m_time, a_time, hash, size..), SANDBOX>
…

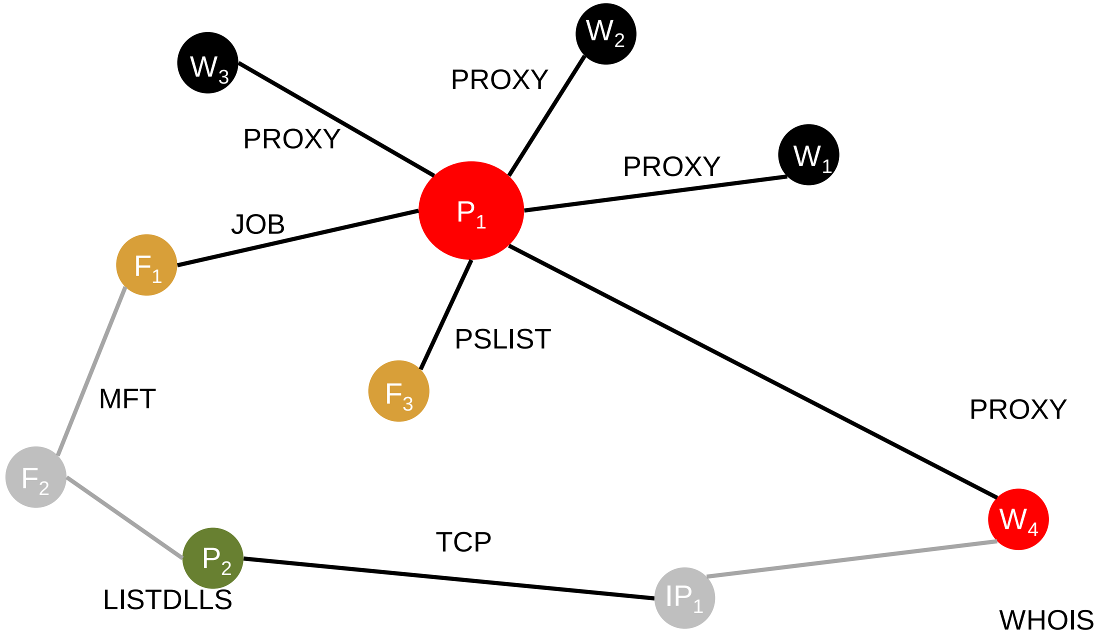
關係的斷點不代表沒關係，只是**證據不足**而已

擴大關係

策略一：補償最少的空事件，可以得到最大關係圖

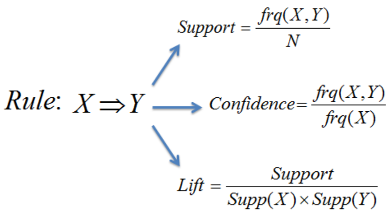
策略二：指定一個事件為中心，依時間順序，由內而外持續補償空事件

…



JOB: <timestamp, (SYSTEM,AT.exe), SYSTEM, se.exe, c:\\, HH:MM:SS>
FILE: <timestamp, (SYSTEM, NULL), (nvdszhk.dll, c:\system\32, c_time, m_time, a_time, hash, size..), MFT>
FILE: <timestamp, (SYSTEM, se.exe), (nvdszhk.dll, c:\system\32, c_time, m_time, a_time, hash, size..), MFT>

一群電腦中找出最可能受駭的電腦



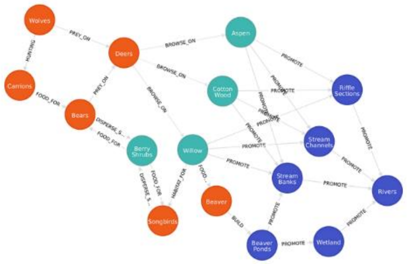
$$\textit{Rule}:\ X \Rightarrow Y$$

$$Support = \frac{frq(X,Y)}{N}$$

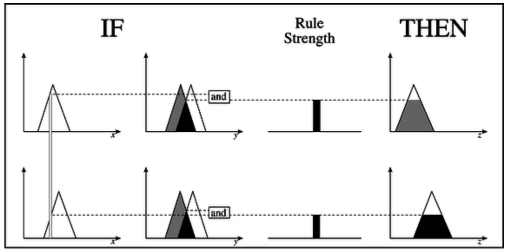
$$Confidence = \frac{frq(X,Y)}{frq(X)}$$

$$Lift = \frac{Support}{Supp(X) \times Supp(Y)}$$

Associated Rules

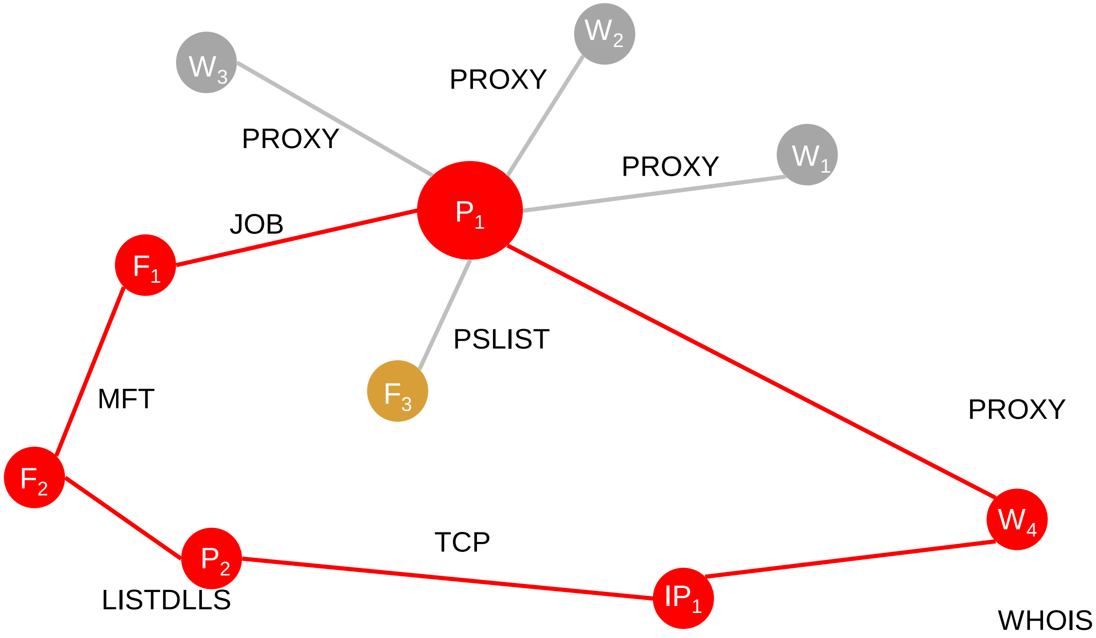


Link analysis



Fuzzy

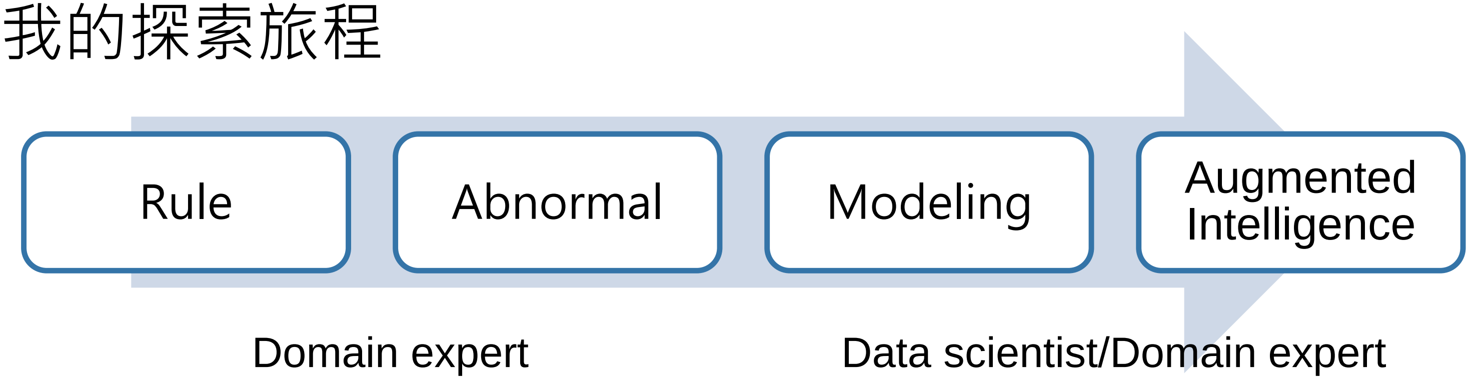
Feedback



Supervised learning → Add/ Adjust the rules

結論

- 我的探索旅程



Rule

Abnormal

Modeling

Augmented Intelligence

Domain expert

Data scientist/Domain expert

- 定義清楚分析的目的