CYBERSEC 2025
臺灣資安大會

FINSEC FORUM

FINSEC FORUM

數位鑑識
不該是你處理事件應變的重點

陳詰昌

台新金控/銀行

資安長

TAIPEI

【關於我們】

ISC2 Taipei Chapter 是 ISC2 在台灣的分會組織，致力於推廣資安專業知識、交流與社群互助。

成員包括經 ISC2 認證的資安專家，及各領域資安專業人士。

【成立宗旨】

提升台灣資安專業社群的能見度與凝聚力。

【使命與活動】

- 推廣資安認證與專業發展
- 舉辦技術講座、各種資安研討活動
- 促進會員交流與跨界合作
- 參與國際資安社群互動

加入 ISC2 Taipei Chapter 讓您的資安之旅，有專家同行！

https://www.isc2chapter.tw

contact@isc2chapter.tw

從一銀ATM盜領案說起

事件應變最重要的目的是什麼？

高度類似俄羅斯科技黑幫手法，調查局證實一銀ATM遭植木馬，駭客遠端遙控大吐鈔

調查局證實一銀ATM遭植入木馬，盜領者遠端透過銀行內網遙控ATM吐鈔，多名APT資安研究專家研判，一銀受駭情況，與俄羅斯黑幫鎖定攻擊50間俄羅斯銀行的手法類似，都使用暗中將惡意程式植入Wincor廠牌ATM，竄改吐鈔限制，可控制多臺ATM來盜領。該集團已偷騙俄羅斯50家銀行，甚至包括歐、美銀行。

文/ 黃彥棻 | 2016-07-12 發表

讚 8 分享

一銀ATM盜領案：調查局找到更多駭客使用的ATM控制程式

調查局在第一銀行40部德利多富的ATM硬碟中找到更多駭客使用的工具程式跡證，包括3支程式及1個指令檔，用以控制ATM顯示系統資訊、控制吐鈔模組、刪除工具程式及相關資料，讓外界對一銀ATM盜領的手法有更進一步的瞭解，未來將調查這些工具程式如何被植入ATM。

文/ 蘇文彬 | 2016-07-13 發表

讚 0 分享

《獨家》調查局揭露：一銀ATM盜領惡意程式指定在7月發作，逾期失效

調查局表示，資安鑑識人員透過數位鑑識方式發現，一銀ATM盜領發現的4支惡意程式中，具有以往惡意程式少見的指定日期發作的功能。也就是說，這些惡意程式不論是顯示ATM的資訊或者是執行吐鈔功能等，都只在今年7月份執行才有效，一旦逾期，該惡意程式將不會發作。此外，為了隱匿自己的行蹤，這些惡意程式也會利用微軟內建的「sdelete.exe」刪除功能，刪除足跡

文/ 黃彥棻 | 2016-07-15 發表

讚 0 分享

Thor's CC® QOTD

What is the primary goal of a security IR (Incident Response) plan?

A. To prevent security incidents from happening.

B. To minimize the impact of a security incident on an organization.

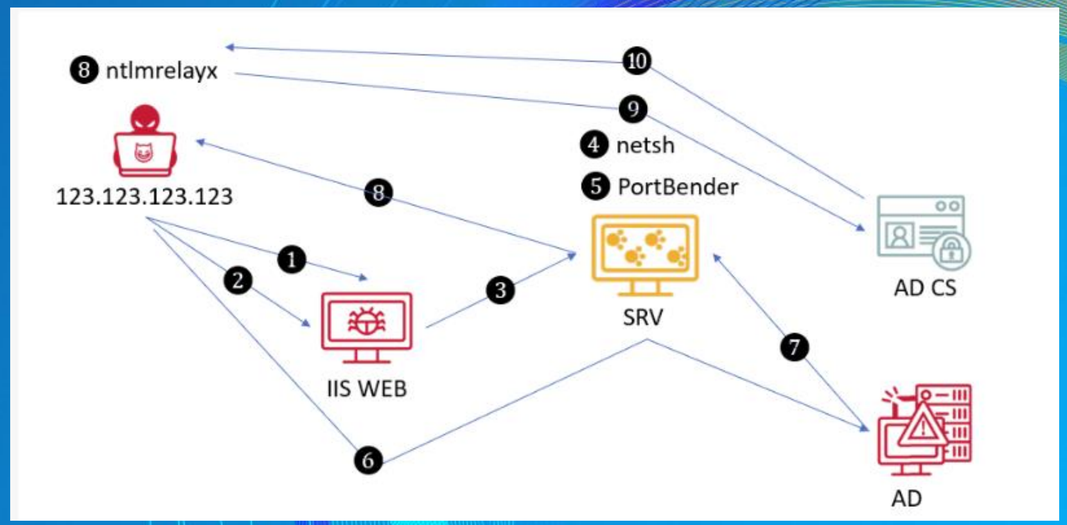
C. To identify the root cause of a security incident.

D. To ensure compliance with industry regulations.

每次發生重大資安事件

隔天敲碗要...IoC呢? 入侵途徑呢?

檔案名稱	SHA256 Hash
av-1m.exe	EE854E9F98D0DF34C34551819889336C16B9BFE76E391356CB17B55D59CF28CF
av.exe	3B2081042038C870B1A52C5D5BE965B03B8DD1C2E6D1B56E5EBB7CF3C157138D
bb.exe	2CC975FDB21F6DD20775AA52C7B3DB6866C50761E22338B08FFC7F7748B2ACAA
crazyhunter.exe	F72C03D37DB77E8C6959B293CE81D009BF1C85F7D3BDAA4F873D3241833C146B
crazyhunter.sys	5316060745271723C9934047155DAE95A3920CB6343CA08C93531E1C235861BA
go.exe	754D5C0C494099B72C050E745DDE45EE4F6195C1F559A0F3A0FDDBA353004DB6
go2.exe	983F5346756D61FEC35DF3E6E773FF43973EB96AABAA8094DCBFB5CA17821C81
go3.exe	F72C03D37DB77E8C6959B293CE81D009BF1C85F7D3BDAA4F873D3241833C146B
ru.bat	15160416EC919E0B1A9F2C0DC8D8DC044F696B5B4F94A73EC2AC9D61DBC98D32
ru.bat	731906E699ADDC79E674AB5713C44B917B35CB1EABF11B94C0E9AD954CB1C666
zam64.sys	2BBC6B9DD5E6D0327250B32305BE20C89B19B56D33A096522EE33F22D8C82FF1
zam64.sys	BDF05106F456EE56F97D3EE08E9548C575FC3188AC15C5CE00492E4378045825
ta.bat	527ED180062E2D92B17FF72EA546BB5F8A85AD8B495E5B0C08B6637B9998ACF2
CrazeHunter.zip	D202B3E3E55DF4E424F497BA864AB772BAAF2B8FE10B578C640477F8A8A8610C



圖摘自iThome馬偕醫院遭加密勒贖案報導

過度聚焦數位鑑識現象

03.媒體壓力:只想知道誰攻擊

尤其是中國駭客就爽翻了
少談企業怎麼應對衝擊、如何復原

02.法遵稽核:有報告才能交代

主管機關要求提供鑑識報告作為稽核依據
個資有無外洩法律責任

04. 技術腦:技術人員本能

技術人員習慣追根究底忘記優先順序
應變優先於追查

05. 缺乏訓練與SOP演練

發生後各自做自己覺得重要的事
IT 或 MIS「順便」兼做資安亂成一團

01. 鑑識誤解:以為找到駭客 = 止損

找到惡意程式=解決所有問題
找到駭客身分=防堵攻擊

06. 管理與技術層溝通斷層

沒有事件應變流程只剩拼命查原因
技術人員孤軍奮戰，邊修邊查邊猜

別忘了應變目的在減輕事件對組織的衝擊

法律合規
- 違規罰款
- 監管成本
- 法律訴訟

財務損失
- 直接成本
- 間接成本
- 保險費用

營運中斷
- 營業損失
- 客戶流失
- 供應鏈斷

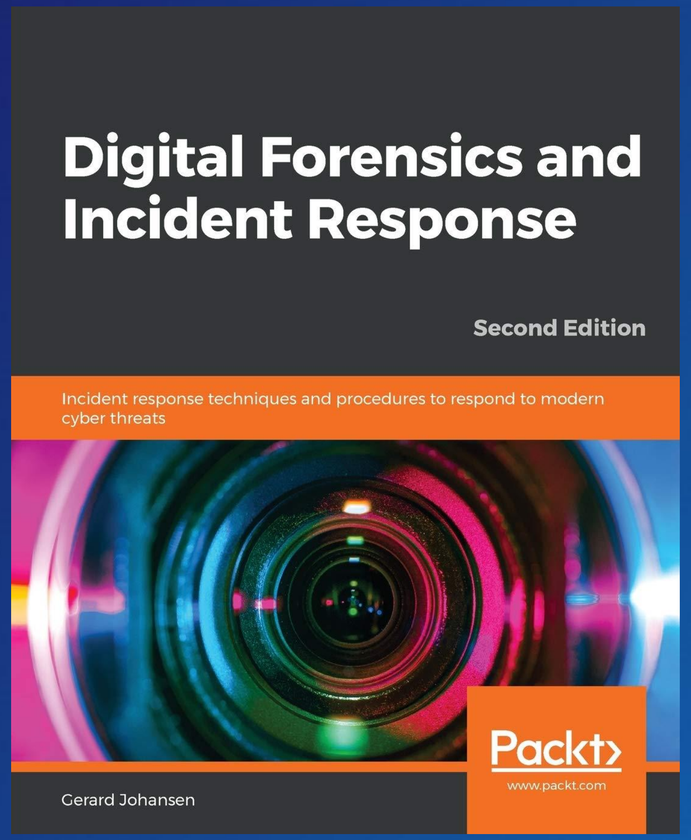
聲譽信任
- 品牌形象
- 客戶信任
- 投資意願

資安培訓強調紅隊攻擊多於藍隊防禦

事件應變聚焦數位鑑識多於減少損失

DFIR (Digital Forensics & Incident Response)

數位鑑識Digital Forensics

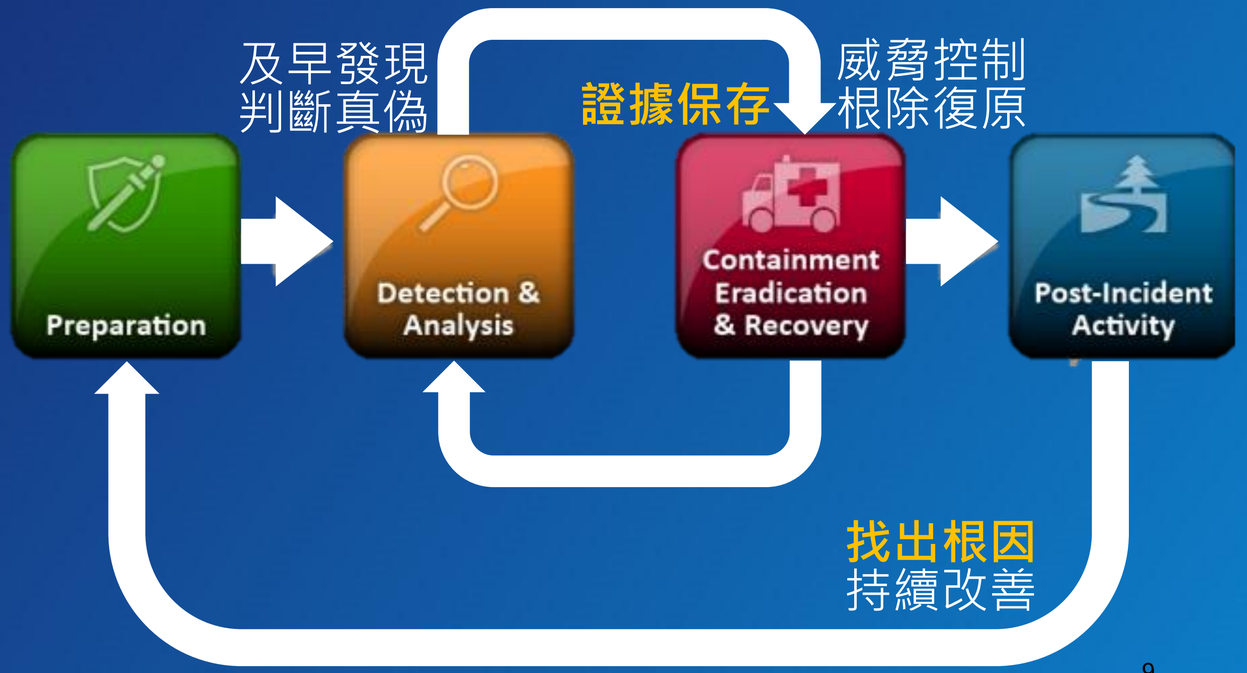


- 數位鑑識是刑事科學(Forensics Science)的一個分支，是發現與解釋數位證據之過程。
- 目的是識別、保存數位證據原始狀態，並透過分析和驗證方法嘗試去重建過去客觀事實，讓法律事實與客觀事實落差減少。
- 法律事實強調證據能力與證據力，因此數位鑑識重視資格（人、實驗室）、程序(合法性與紀錄)、證據同一性（監管鏈）、再現性（工具）

識別 → 保存 → 分析 → 記錄 → 呈現

事件應變 Incident Response

事件應變是**風險管理**的一部分，在事件發生時，以系統性、策略性方法用來偵測、隔離、復原及解決駭侵產生議題。



事件應變核心

- 危機管理
- 風險控制
- 業務持續
- 即時通報

數位鑑識與證據保存比較

	數位鑑識 Digital Forensics	證據保存 Evidence Preservation
定義	分析與調查數位證據以**重建事件客觀事實**	**識別、蒐集與保護**與事件相關資料
目的	找出攻擊者、手法與事件經過(Timeline)等	確保蒐集資料未被竄動或毀損
時機	**事件後期**(post mortem)進行分析	**事件初期或偵測異常**時立即進行
人員	資安分析師、鑑識專家(多委外處理)	IT人員、First Responder(企業內部人員)
工具	專業工具(Encase、Volatility、IDA pro等)，參考NIST CFTT符合再現性要求	初階取證工具(如sysinternals)、Write Blocker
能力	門檻高，需要專業知識與調查技巧	基礎為主，重點是「不破壞原始資料」
法律	**證據能力、證據力及證據完整性**等	**Chain of Custody、封存過程紀錄**

事件管理應處架構

事件管理(策略)

- 管理層危機管理與決策、資源配置
- 應對整體資安事件的衝擊影響、通報、合規、溝通與後續改進，確保企業營運不中斷
- 管的住事件、保的住營運

事件應變(流程)

- 應變流程與跨部門協調合作(角色分工)
- 快速、有效地應對資安事件，遏止影響範圍擴散、復原服務及保存證據
- 應變快、通報準、復原穩

事件處理(技術)

- 技術處理與實踐操作
- 第一線人員負責執行技術面的偵測、隔離、復原與分析
- 查的清、封的住、修的好

資安主管角色

策略領導

- 制定資安政策與事件管理策略
- 向董事會溝通資安風險與治理計畫
- 確保符合法規（如金融資安法規、個資法）
- 與高層及外部利害關係人協調溝通

治理推動

- 建立 Incident Response Framework
- 組織 CSIRT、模擬演練
- 主導事件等級分類與通報決策
- 推動資安文化與意識提升

技術與應變指揮

- 監督資安事件偵測與調查
- 決定是否啟動應變、隔離、通報
- 支持證據保存、鑑識與恢復作業
- 與 SOC、IT 團隊協作應變處理

金融資安主管額外應關注重點

監管合規議題

主管機關監管與法規要求
如資通防護基準、上市公司重大訊息發布應注意事項、個資法等

業務持續議題

資安事件造成服務中斷可能造成客訴與法律糾紛
如證券交易服務客訴

通報及輿情

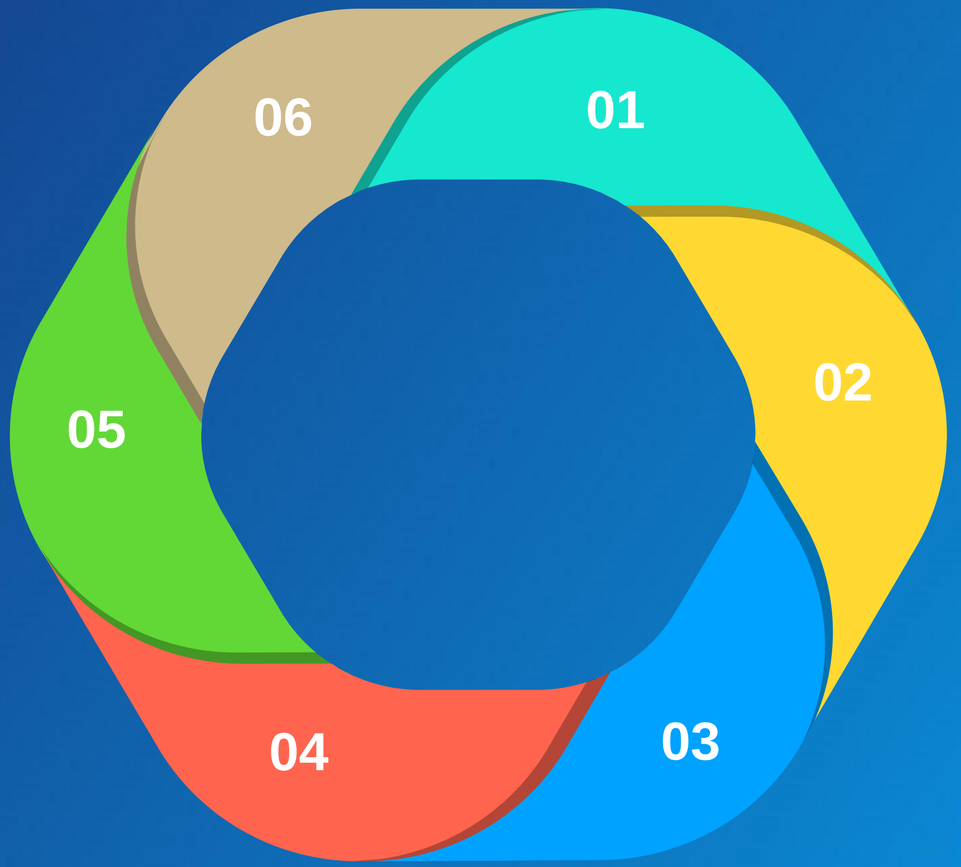
主管機關通報、客戶溝通與媒體說明
如重大訊息公告時機、重大偶發通報、通知客戶及媒體說明等

CSIRT能力提昇應對挑戰

06 – 技術力
- 日誌分析與異常查找
- SOC/SIEM/EDR實操

05 – 協作力
- 跨部門分工與協作
- 明確權責分工矩陣

04 – 通報力
- 整體資安事件通報機制
- 對高層及主管機關報告



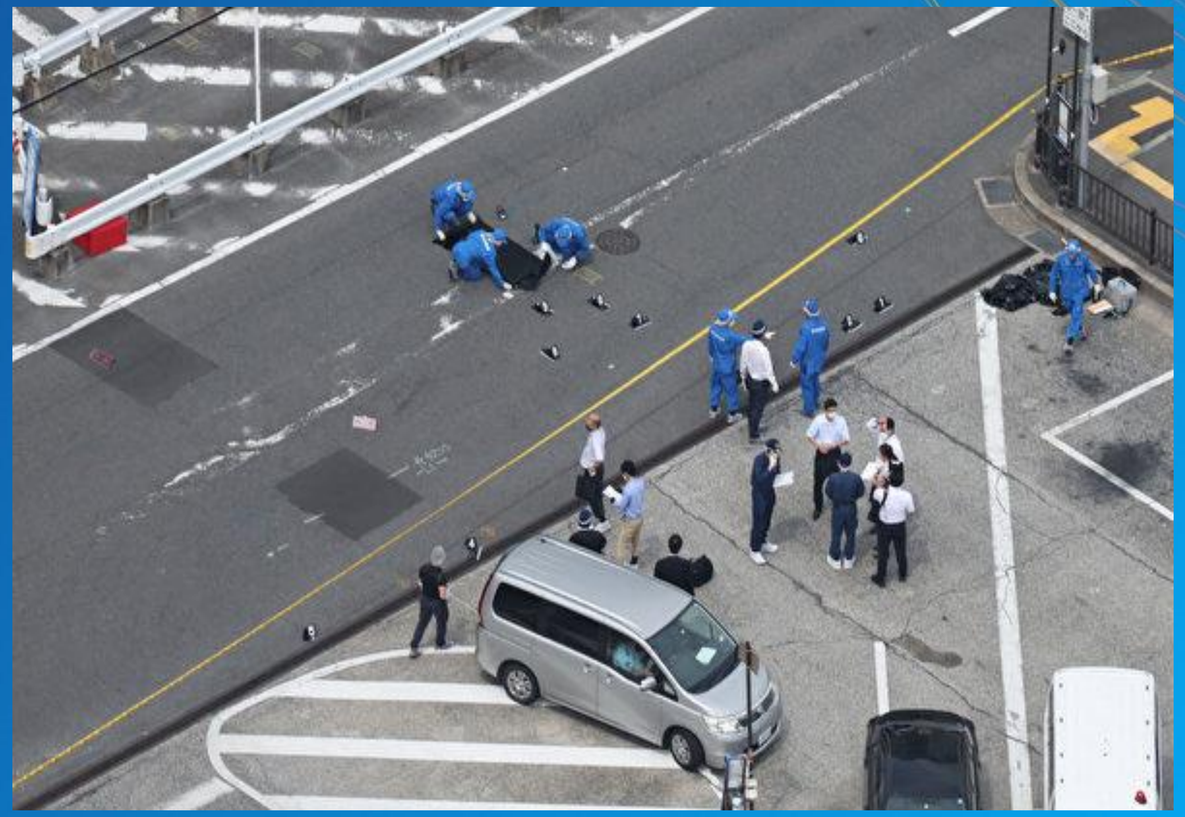
01 – 演練力
- 會演才會做
- 評估與檢討

02 – 流程力
- 快速回報並標準化處理
- 建立PlayBook快速應變

03 – 學習力
- 事件案例分享學習
- 案例轉為應對策略

聰明的你會先減少衝擊? 還是鑑識?

多數司法人員只在乎抓人起訴判罪，而減少被害人損失非其主要目標
委外資安團隊只在乎查明被駭原因，而減少事件衝擊非其主要考量目標



CYBERSEC 2025
臺灣資安大會

資安不是舞台上的主角(BU/IT)，
而是幕後默默守護演出順利的人。
感謝各位低調的資安英雄!