因應資安法施行-
資安情資分享規範說明

行政院國家資通安全會報技術服務中心

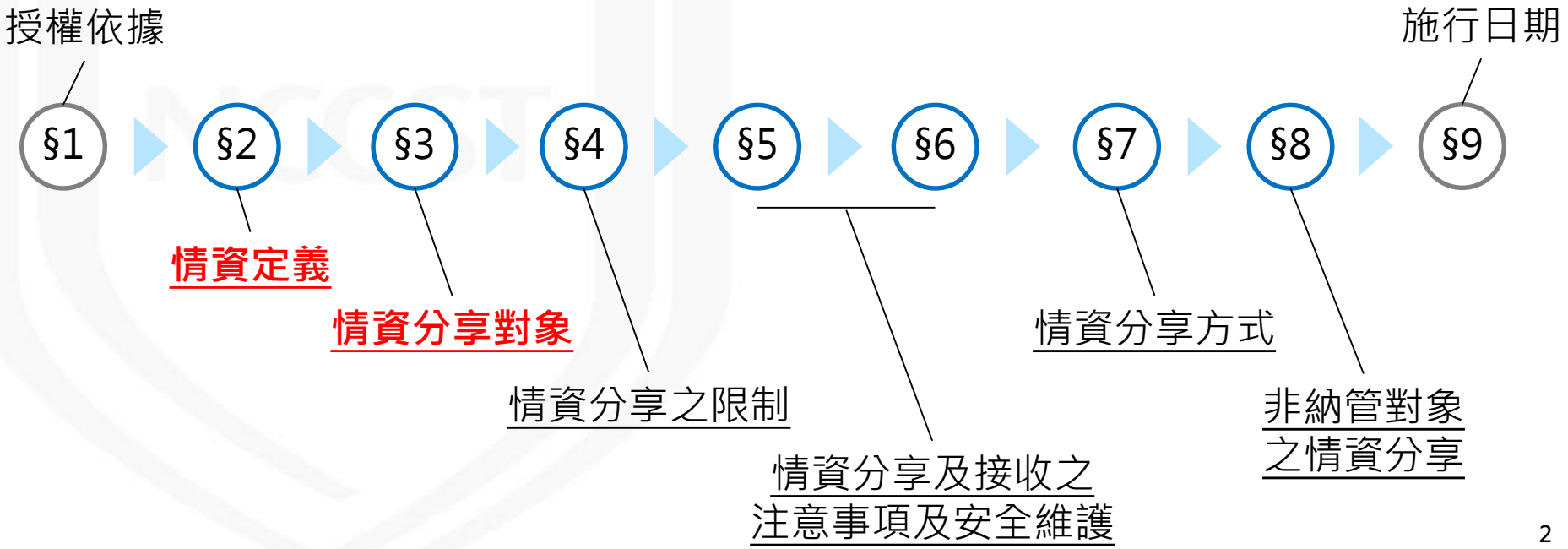
108年5月

大綱

- 前言
- 聯防監控架構說明
- 聯防監控情資回饋
- 聯防監控作業流程說明
- 推動時程與工作項目

資通安全情資分享相關規定

- 資通安全管理法(第8條)
  - 主管機關應建立資通安全情資分享機制
  - 前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之
- 資通安全情資分享辦法



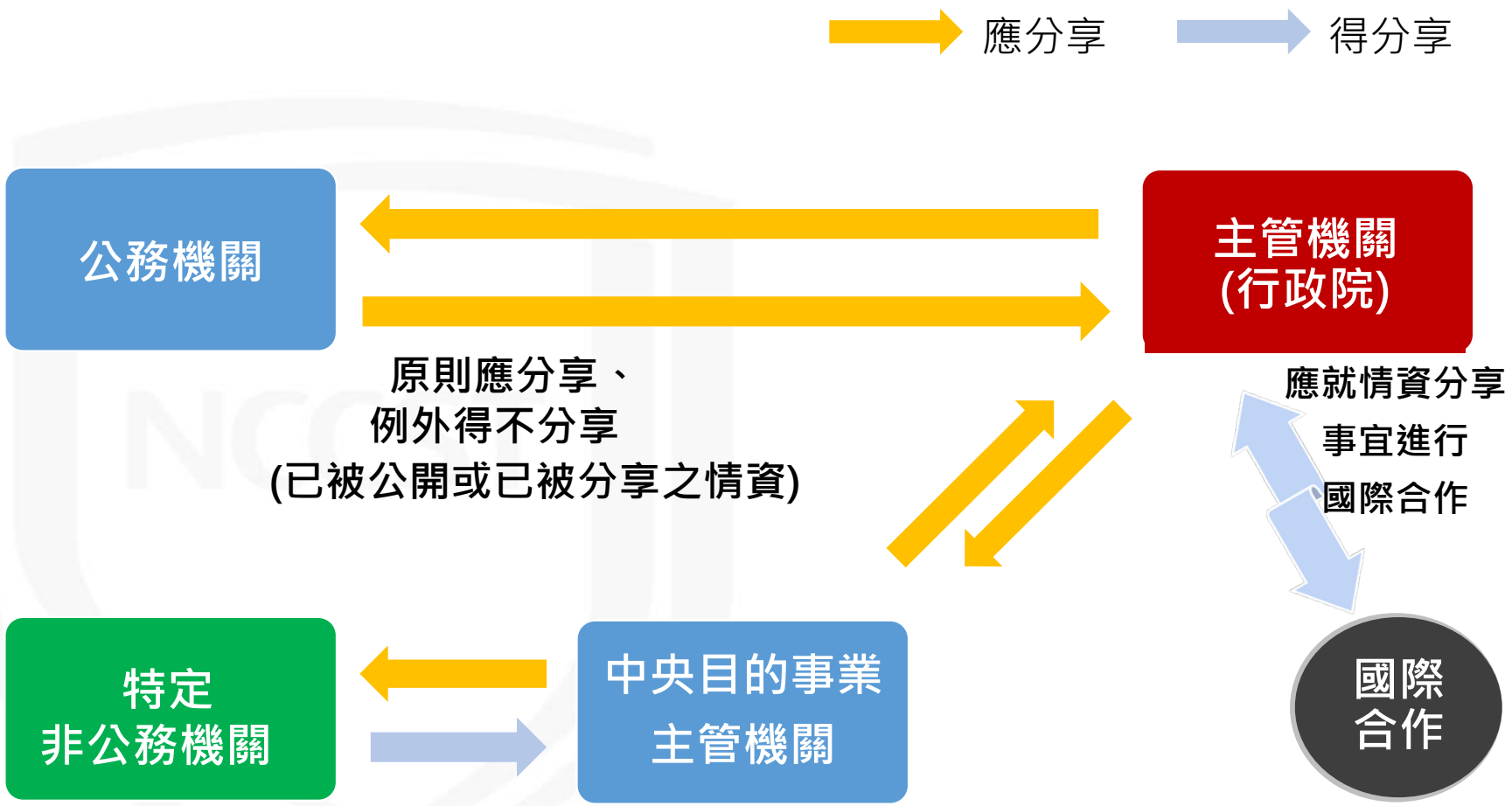
資安情資定義內容

§1 ▶ §2 ▶ §3 ▶ §4 ▶ §5 ▶ §6 ▶ §7 ▶ §8 ▶ §9

一、	**惡意偵察/情蒐活動**	惡意活動偵測紀錄、資安事件單、關聯事件單、疑似攻擊探測紀錄、關聯分析結果
二、	**系統安全漏洞**	漏洞資訊
三、	**使安控失效或利用漏洞方法**	攻擊手法
四、	**惡意程式相關資訊**	惡意程式、中繼站資訊、受害者資訊、惡意IP/DN、惡意郵件來源
五、	資安事件之損害或影響	中繼站黑名單阻擋統計
六、	**偵測、預防或降低損害措施**	惡意程式分析報告、惡意活動趨勢分析、攻擊應變措施
七、	**其他技術性資訊**	資安趨勢報告、領域監控分析報告

資安情資分享對象

§1 §2 §3 §4 §5 §6 §7 §8 §9



資通安全責任等級分級辦法

- 應辦事項：附表一至附表八
- 資通系統防護分級及防護基準：附件九與附表十

辦理項目	辦理內容	資安責任等級				
		A	B	C	D	E
資通安全威脅偵測管理機制	**完成威脅偵測機制建置，並持續維運**	★	★			
	公務機關依主管機關指定之方式提交監控管理資料	★	★			
資通安全防護 (啟用，並持續使用及適時進行軟、硬體之必要更新或升級)	• 防毒軟體 • 網路防火牆 • 電子郵件過濾機制(具有郵件伺服器者)	★	★	★	★	
	• 入侵偵測及防禦機制(IDS/IPS) • 應用程式防火牆(具有對外服務之核心資通系統者)	★	★			
	• APT攻擊防禦機制	★				

「★」表示：機關初次受核定或等級變更後一年內需完成項目

公務機關應辦事項說明

- 依據資安情資分享辦法，進行情資分享
  - 包括資通系統之惡意偵察或情蒐活動等相關情資
- 依據資安責任等級分級辦法，辦理相關之應辦事項

  A、B級應建置資通安全威脅偵測管理(SOC)機制
  - 建置威脅偵測機制，並持續維運
  - 依指定之方式提交監控管理資料，內容應包含資通安全防護項目
  - 資通安全防護項目應納入監控管理機制

資安情資來源類型

- **資通安全威脅偵測管理機制**
  - 應包含資通安全防護項目
    - 現有資安防護設施與對外服務核心資通系統之安全防護機制
- **惡意偵察或情蒐活動相關情資**
  - 如DNS警示紀錄、EDR端點防護、MDR防護紀錄、DDoS防護機制及HoneyPot機制等

資通安全防護項目	資安偵蒐機制
防毒軟體	DNS警示紀錄
網路防火牆	EDR端點防護
應用程式防火牆	MDR防護紀錄
入侵偵測及防禦機制	DDoS防護機制
進階持續性威脅攻擊防禦措施	HoneyPot機制
電子郵件過濾機制	

大綱

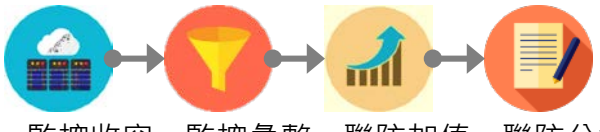
- 前言
- 聯防監控架構說明
- 聯防監控情資回饋
- 聯防監控作業流程說明
- 推動時程與工作項目

N-SOC聯防監控架構

國家層級

N-ISAC

N-SOC



N-SOC監控情資透過N-ISAC API進行交換

情資分享

事件收容

領域聯防SOC(8大領域)

區域聯防SOC(6都)

領域/區域(6都)

政府領域聯防(G-SOC)

情資分享

監控情資

情資分享

事件追蹤

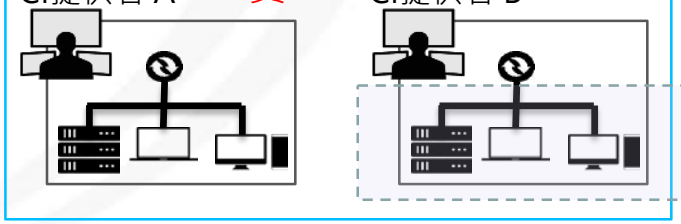
CI提供者 A

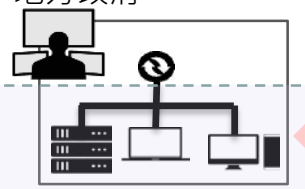
CI提供者 B

地方政府

MSSP

CI提供者/地方政府

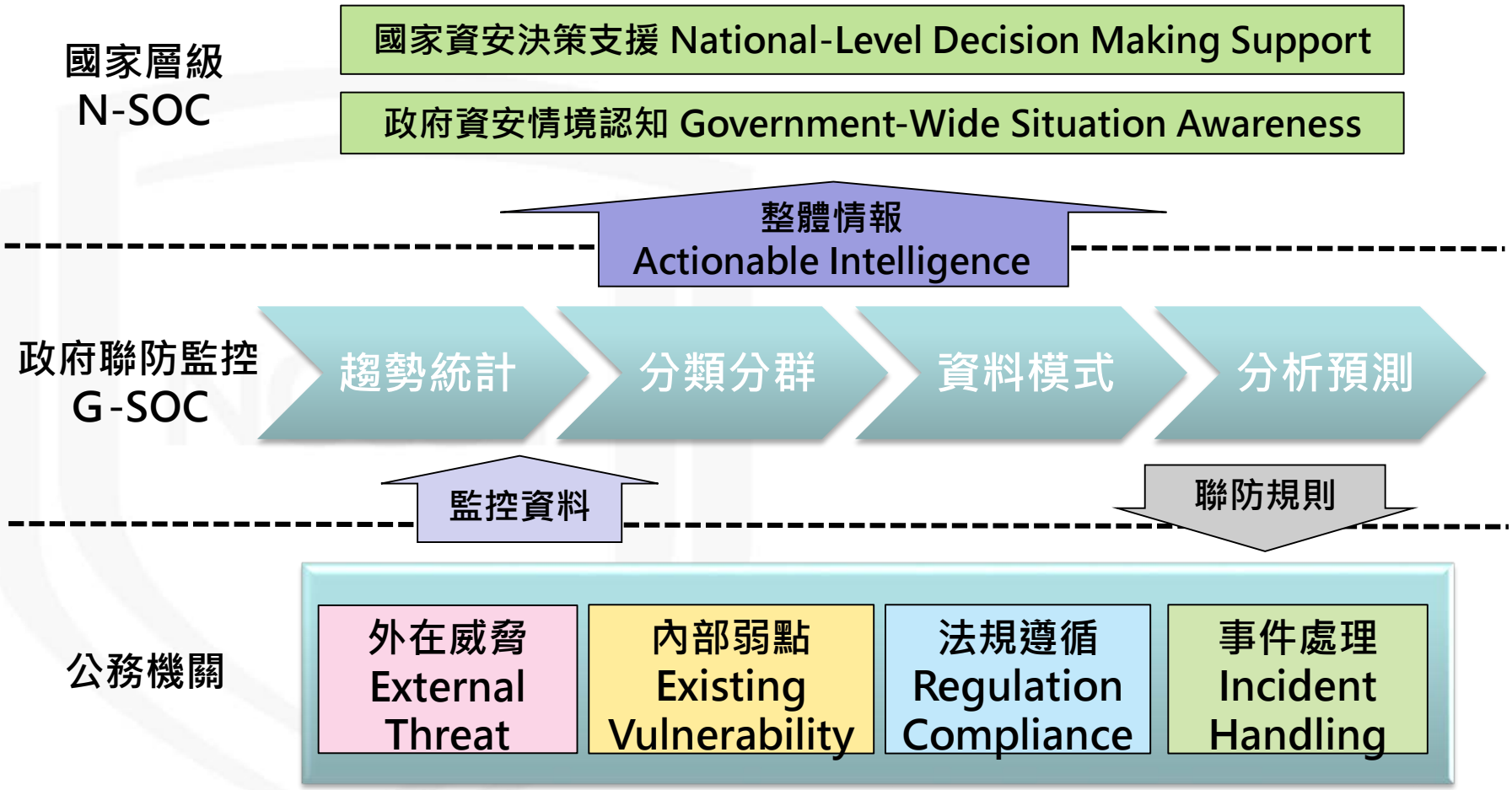




持續監控

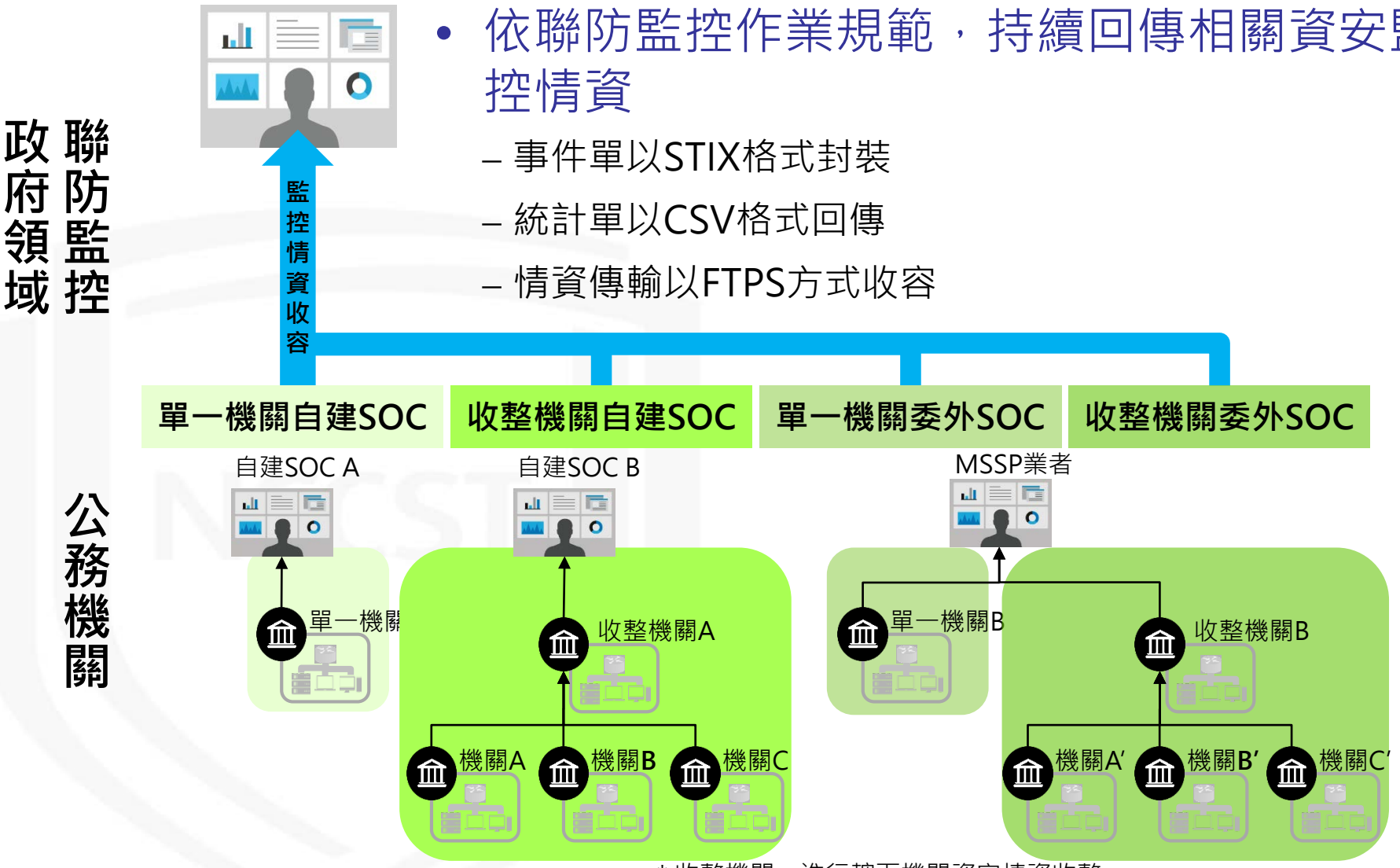
政府領域聯防監控(G-SOC)

- 建立政府資安情境認知(Situation Awareness)
- 支援政府資安決策(Decision Making)與推動公私資安協同合作



G-SOC聯防監控情資收容架構

- 依聯防監控作業規範，持續回傳相關資安監控情資
  - 事件單以STIX格式封裝
  - 統計單以CSV格式回傳
  - 情資傳輸以FTPS方式收容

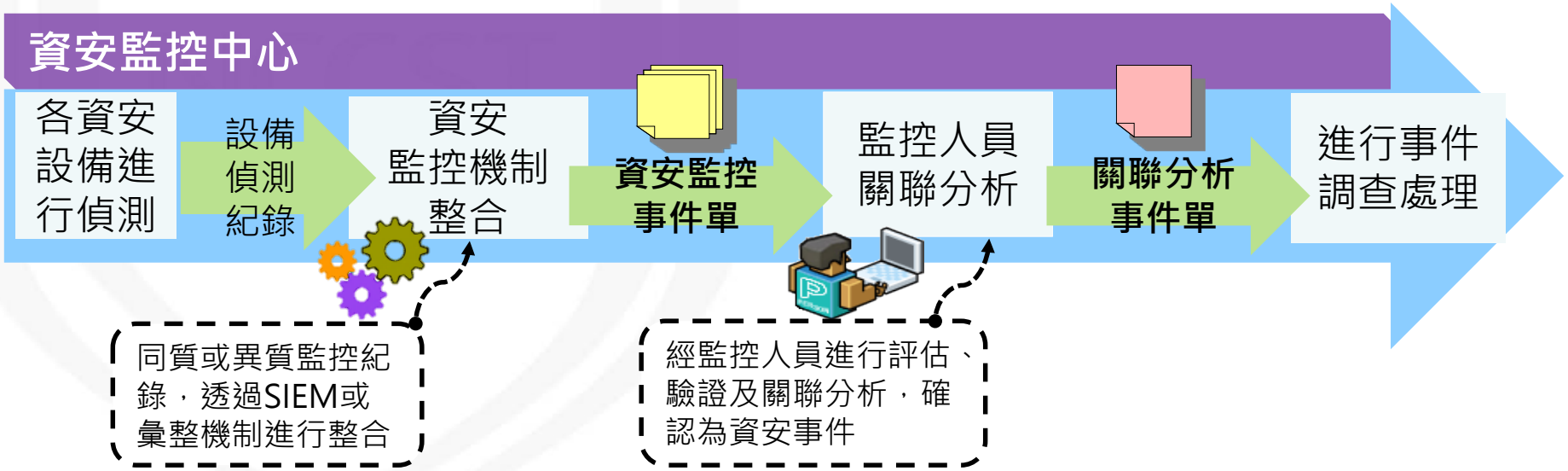


* 收整機關：進行轄下機關資安情資收整
* 資安託管服務供應商(Managed Security Service Provider, MSSP)

G-SOC聯防監控情資說明(1/2)

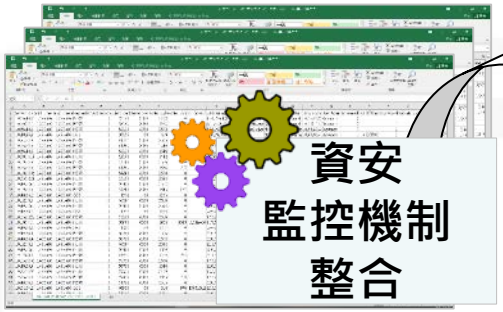
- 機關需回傳以下資安監控情資至G-SOC

項次	情資內容	情資說明	回傳頻率
1	資安監控事件單	資安監控機制整合產製之資安監控事件單	即時
2	關聯分析事件單	SOC分析人員對「資安監控事件單」進行影響性評估、驗證及關聯分析資訊而成	即時
3	健康狀況統計單	所有轄下機關(含單位本身)監控機制存活狀況	每月

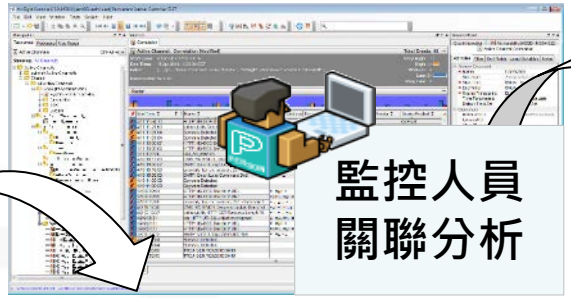


G-SOC聯防監控情資說明(2/2)

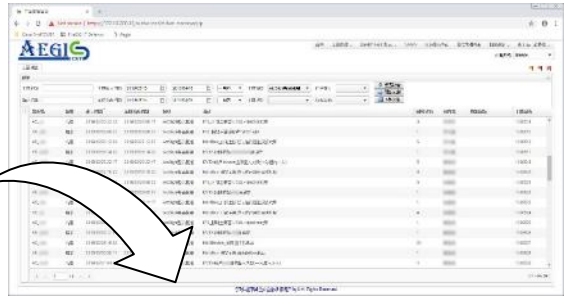
- 資安監控情資範例說明



資安
監控機制
整合



監控人員
關聯分析



資安設備監控紀錄

- 惡意連線紀錄
- 漏洞探測紀錄
- 惡意程式下載紀錄

fortigate阻擋(210.69.x.x)
連線50次

資安監控事件單

- 惡意程式類事件
- 後門報到行為
- 受害單位資訊
- 觸發設備資訊

內部電腦(210.69.x.x)連線
至C&C網站(http://mal.site)

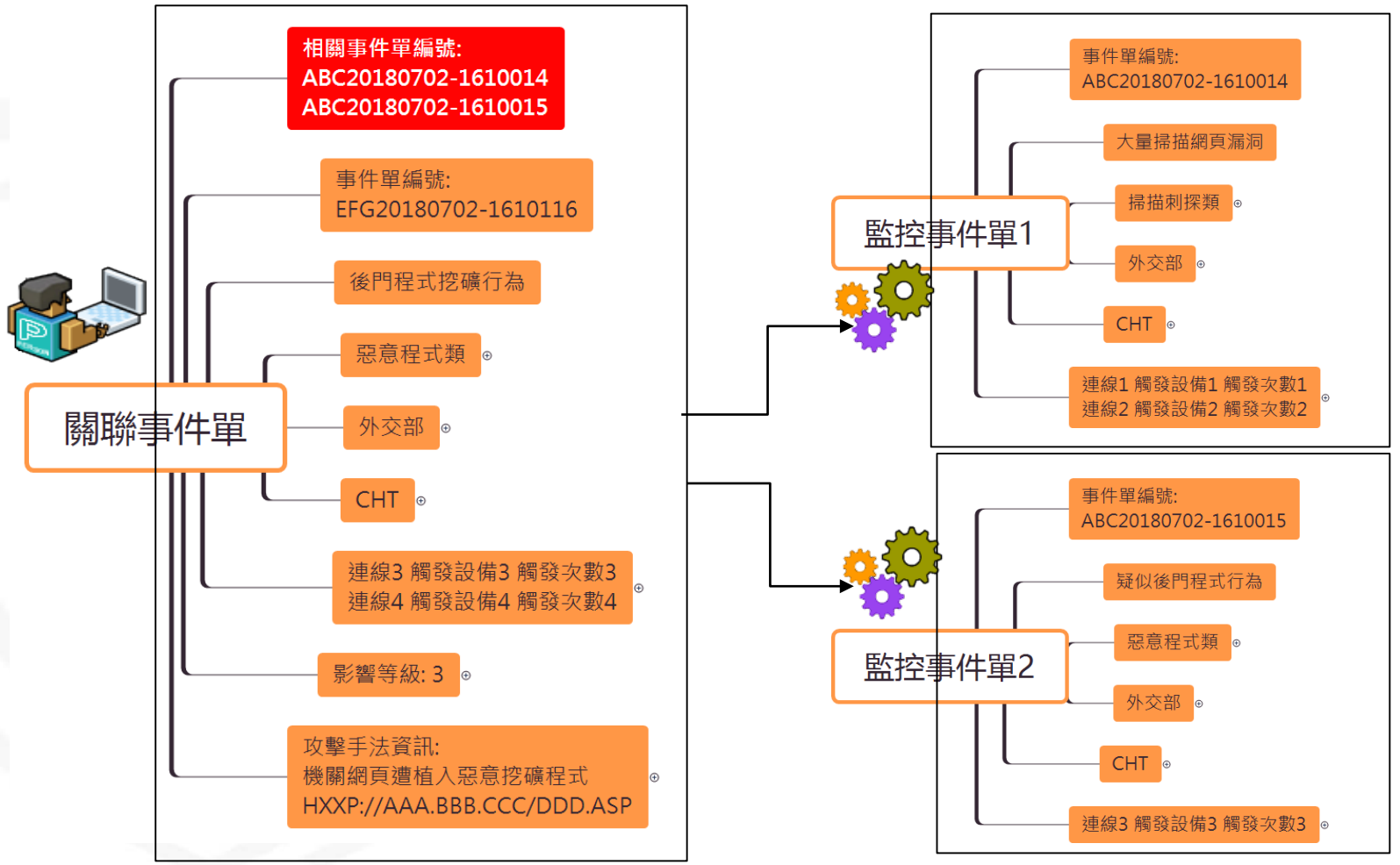
關聯分析事件單

- 資安監控事件單彙整資訊
- 事件影響等級
- 攻擊手法資訊
  - 事件IoC萃取資訊
  - 事件IoA萃取資訊
  - CVE漏洞資訊
- 其他彙整情資

機關網頁伺服器遭入侵，
下載勒索惡意程式，
資料庫資料遭到加密

關聯分析事件範例

- 關聯分析事件單彙整資安監控事件情資
  - 以事件單編號做參照



健康狀況統計單

- 每個月5號前回傳上月健康狀況統計單
- 以CSV格式檢附相關資訊
  - 機關OID代碼、機關名稱、機關等級、設備名稱與型號、設備代號、資安防護類型及觸發次數

機關OID代碼	機關名稱	機關等級	設備名稱與型號	設備代號	資安防護類型	觸發次數
	行政院國家資通安全會報技術服務中心	A	PaloAlto PA-3020	NCCST_PaloAlto_1	網路防火牆	50
	行政院國家資通安全會報技術服務中心	A	PaloAlto PA-3020	NCCST_PaloAlto_2	網路防火牆	0
	行政院國家資通安全會報技術服務中心	A	SonicALL NSA240	NCCST_SonicAll_1	入侵偵測及防禦機制	100

大綱

- 前言
- 聯防監控架構說明
- 聯防監控情資回饋
- 聯防監控作業流程說明
- 推動時程與工作項目

G-SOC聯防監控情資回饋(1/6)

- 機關應就所接受之情資，進行後續聯防措施
  - 辨識其來源之可靠性及時效性
  - 及時進行威脅與弱點分析及研判潛在風險
  - 採取對應之預防或應變措施

- 機關如何取得資安聯防監控月報？
  - 技服中心每月發布警訊ANA，告知至通報應變網站下載
    1. 機關至通報應變網站聯防監控專區下載
    2. 未有通報應變網站帳號之機關可向上級機關索取

G-SOC聯防監控情資回饋(2/6)

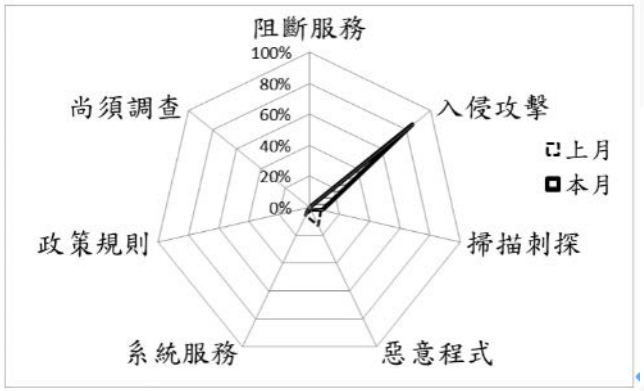
- 彙整跨機關情資與自建威脅情蒐機制，產製資安聯防監控月報
  - 提供政府領域整體事件綜覽與防護建議
  - 提供近期威脅事件及防護策略
  - 政府領域威脅趨勢、專題式威脅手法分析
  - 入侵偵測與威脅防護指標

情資內容	情資說明
資安聯防監控月報	彙整樣態分析及領域威脅評估 • 跨機關監控綜覽 • 跨機關威脅種類分析 • 聯防監控回饋建議

G-SOC聯防監控情資回饋(3/6)

- 威脅種類分析
  - 威脅種類：統計各業務列別機關整體威脅類型趨勢變化
  - 交叉分析：依機關類型與事件類別進行交叉分析，評估各類型機關資安威脅狀況

威脅趨勢變化



跨資安責任等級交叉分析

業務＼事件	1. 入侵攻擊類	2. 惡意程式類	3. 阻斷服務類	4. 掃描刺探類	5. 政策規則類	6. 系統服務類	7. 尚須調查類	1～7合計
A級機關	15.2 / 21.7	7.0 / 9.6	4.9 / 2.7	5.2 / 4.6	1.9 / 2.2	1.1 / 1.3	0.2 / 0.5	35.5 / 42.6
B級機關	0.5 / 0.6	0.1 / 0.2	0 / 0	1.1 / 0.9	0 / 0	0 / 0	0 / 0	1.7 / 1.7
C級機關	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
合計	15.7 / 22.3	7.1 / 9.8	4.9 / 2.7	6.3 / 5.5	1.9 / 2.2	1.1 / 1.3	0.2 / 0.5	37.2 / 44.3

G-SOC聯防監控情資回饋(4/6)

重點關注威脅類行分析

表2　資安事件類別主要影響機關業務類別與事件彙整

項次	資安事件類別	主要機關業務類別	主要觸發事件
1	系統服務類	• 教育科學文化	• 網頁服務中止
2	入侵攻擊類	• 外交國防法務 • 教育科學文化 • 非行政院所屬	• 外部入侵攻擊行為 • 弱點與漏洞利用
3	阻斷服務類	• 內政衛福勞動	• 外部主機疑似進行阻斷服務攻擊
4	惡意程式類	• 內政衛福勞動 • 教育科學文化 • 經濟能源農業	• 病毒存取行為 • 單一主機感染病毒
5	政策規則類	• 綜合行政	• 特殊權限異動案件 • 稽核原則變更案件
6	掃描刺探類	• 綜合行政 • 內政衛福勞動 • 交通環境資源	• 外部主機執行掃描探測攻擊 • 弱點掃描行為 • 外部主機嘗試 SQL-Injection 攻擊
7	尚需調查類	• 內政衛福勞動 • 教育科學文化	• 網路異常行為

跨機關威脅種類趨勢變化

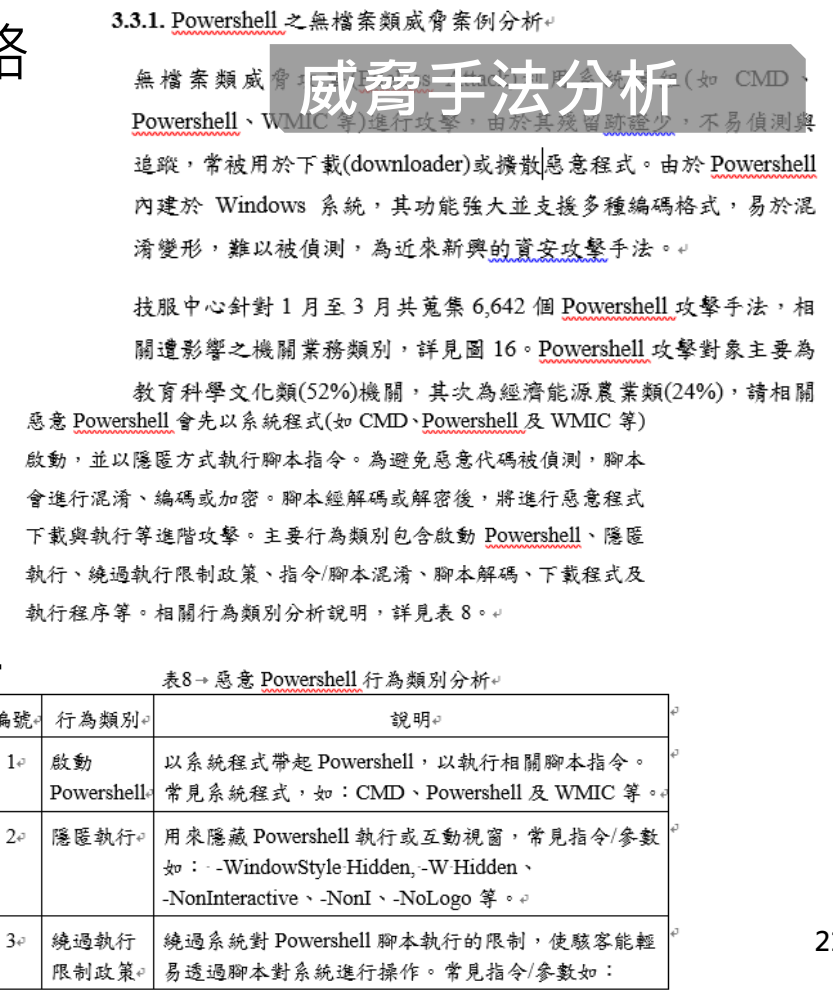
業務＼事件	1. 入侵攻擊類	2. 惡意程式類	3. 阻斷服務類	4. 掃描探刺類	5. 政策規則類	6. 系統服務類	7. 尚需調查類	1～7合計
綜合行政	0 / 0	0 / 0	0 / 0	0.1 / 0.1	0 / 0	0 / 0	0 / 0	0.1 / 0.1
內政衛福勞動	0.5 / 0.9	0.2 / 0.5	1.1 / 0.7	1.7 / 1.9	0 / 0	0 / 0	0 / 0	3.5 / 4.0
外交國防法務	4.3 / 7.4	2.2 / 2.4	0.2 / 0.2	0.3 / 0.4	0.2 / 0.3	0 / 0	0.1 / 0.2	7.3 / 10.9
交通環境資源	2.1 / 1.2	0.6 / 1.4	1.8 / 0.8	1.0 / 0.4	0.8 / 0.6	0 / 0	0 / 0	6.3 / 4.4
財政主計金融	1.9 / 1.4	0.3 / 0.2	0.1 / 0.2	0.8 / 0.6	0.2 / 0.2	0 / 0	0 / 0	3.3 / 2.6
經濟能源農業	0.1 / 0.2	0.1 / 0	0 / 0	0.4 / 0.4	0 / 0	0 / 0	0 / 0	0.6 / 0.6
教育科學文化	1.6 / 5.2	0.9 / 1.9	0 / 0.1	2.0 / 1.1	0 / 0.3	1.5 / 1.8	0 / 0	6.0 / 10.4
非行政院所屬	0 / 0	0 / 0	0 / 0	0 / 0.1	0 / 0	0 / 0	0 / 0	0 / 0.1
合計	10.5 / 16.3	4.3 / 6.4	3.2 / 2.0	6.3 / 5.0	1.2 / 1.4	1.5 / 1.8	0.1 / 0.2	27.1 / 33.1

G-SOC聯防監控情資回饋(5/6)

- 聯防監控回饋建議
  - –針對近期整體跨領域/機關觀測到網路威脅與攻擊手法，進行手法分享與提供防護策略

威脅事件手法分享/防護策略

Apache Struts2漏洞(CVE-2017-5638)遭利用植入挖礦程式
D-Link特定無線路由器存在資訊洩漏疑慮
Smominru殭屍網路程式進行虛擬貨幣挖礦行為
Memcached分散式快取系統遭利用作為DDoS放大攻擊
惡意電子郵件手法分析 -CVE-2017-11882 -CVE-2017-0199 -LokiBot
Powershell之無檔案類威脅案例分析



3.3.1. Powershell 之無檔案類威脅案例分析

威脅手法分析

無檔案類威脅[illegible]參數[illegible]（如 CMD、Powershell、WMIC 等）進行攻擊，由於其痕跡蹤少，不易偵測與追蹤，常被用於下載(downloader)或擴散惡意程式。由於 Powershell 內建於 Windows 系統，其功能強大並支援多種編碼格式，易於混淆變形，難以被偵測，為近來新興的資安攻擊手法。

技服中心針對 1 月至 3 月共蒐集 6,642 個 Powershell 攻擊手法，相關遭影響之機關業務類別，詳見圖 16。Powershell 攻擊對象主要為教育科學文化類(52%)機關，其次為經濟能源農業類(24%)，請相關

惡意 Powershell 會先以系統程式(如 CMD、Powershell 及 WMIC 等)啟動，並以隱匿方式執行腳本指令。為避免惡意代碼被偵測，腳本會進行混淆、編碼或加密。腳本經解碼或解密後，將進行惡意程式下載與執行等進階攻擊。主要行為類別包含啟動 Powershell、隱匿執行、繞過執行限制政策、指令/腳本混淆、腳本解碼、下載程式及執行程序等。相關行為類別分析說明，詳見表 8。

表8→惡意 Powershell 行為類別分析

編號	行為類別	說明
1	啟動 Powershell	以系統程式帶起 Powershell，以執行相關腳本指令。常見系統程式，如：CMD、Powershell 及 WMIC 等。
2	隱匿執行	用來隱藏 Powershell 執行或互動視窗，常見指令/參數如：-WindowStyle Hidden, -W Hidden、-NonInteractive、-NonI、-NoLogo 等。
3	繞過執行限制政策	繞過系統對 Powershell 腳本執行的限制，使駭客能輕易透過腳本對系統進行操作。常見指令/參數如：

G-SOC聯防監控情資回饋(6/6)

- 萃取並回饋入侵偵測與威脅防護指標，提供跨機關偵測、分析與聯防使用

情資內容	情資說明
威脅清單(聯防監控指標)	• 受害偵測指標 (IoC) • 威脅攻擊指標 (IoA) • IP/DN/URL Watchlist

威脅樣態
公文附件下載系統受害偵測指標
選舉議題社交工程郵件受害偵測指標
Powershell之無檔案類威脅受害偵測指標
中國菜刀網頁型後門攻擊指標
少爺殭屍網路攻擊指標

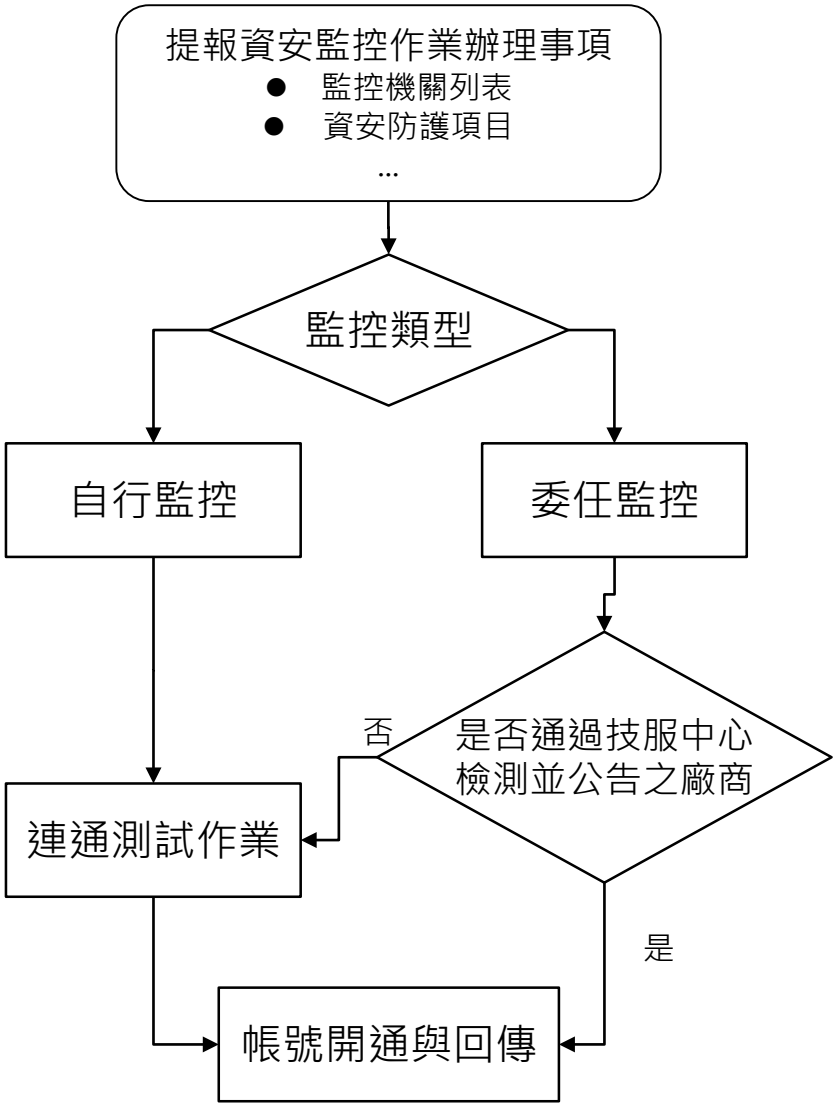
編號	IP	國別	附註/掃描 IP 數量
1	61.218.234.194	TW	實際入侵並影響機關
2	123.242.230.115	HK	實際入侵並影響機關
3	132.232.17.124	CN	36
4	103.51.145.179	HK	16
5	154.8.168.70	CN	10
6	103.244.89.19	HK	9
7	103.40.163.234	HK	7

大綱

- 前言
- 聯防監控架構說明
- 聯防監控情資回饋
- 聯防監控作業流程說明
- 推動時程與工作項目

聯防監控提報與情資回傳作業

- 機關需於資通安全作業管考系統提報資安監控作業辦理事項
- 情資回傳作業
  - 自行監控機關
    - ➢完成連通測試後，辦理帳號開通與情資回傳
  - 委外監控機關
    - ➢通過技服中心檢測並公告之SOC監控廠商
      - ♦辦理情資回傳
    - ➢尚未通過技服中心檢測並公告之SOC監控廠商
      - ♦完成連通測試後，辦理帳號開通與情資回傳



聯防監控回傳類型與權責

自行監控機關	• 自行進行監控，並自行執行收容、分析及回傳作業之公務機關	• 收容機關之資安防護機制清冊 • 定期提供並更新所管理之資通安全防護機制資訊 • 執行資安情資收容與回傳作業
委外監控機關	• 委任監控服務廠商(Managed Security Service Provider, MSSP)進行監控，並委由廠商執行收容、分析及回傳作業之公務機關	• 收容機關之資安防護機制清冊 • 定期提供並更新所管理之資通安全防護機制資訊 • 確保委外資安情資收容與回傳作業運作

情資回傳作業說明

- 管考系統應檢附文件
  - 監控機關列表與資安防護項目
    - 主管機關代為收整者，若為主管機關閘道口設備，歸屬主管機關，其他歸屬為下屬機關
    - 格式同健康狀況統計單

機關OID代碼	機關名稱	機關等級	設備名稱與型號	設備代號	資安防護類型
	行政院國家資通安全會報技術服務中心	A	PaloAlto PA-3020	NCCST_PaloAlto_1	網路防火牆
	行政院國家資通安全會報技術服務中心	A	PaloAlto PA-3020	NCCST_PaloAlto_2	網路防火牆
	行政院國家資通安全會報技術服務中心	A	SonicALL NSA240	NCCST_SonicAll_1	入侵偵測及防禦機制

資安監控範圍異動作業說明

- 為確保資安威脅偵測機制情資回傳之有效性，機關應依管考規定每年進行回報，若有異動時，於資通安全作業管考系統更新下列資訊
  - 機關監控涵蓋範圍異動
    - 檢附調整後的監控機關列表與資安防護清冊
  - 委外監控廠商異動資訊
    - 新委外監控廠商進行連通測試，驗證收容機關與資安防護項目是否正確
  - 資安防護項目異動
    - 檢附監控機關列表與資安防護清冊

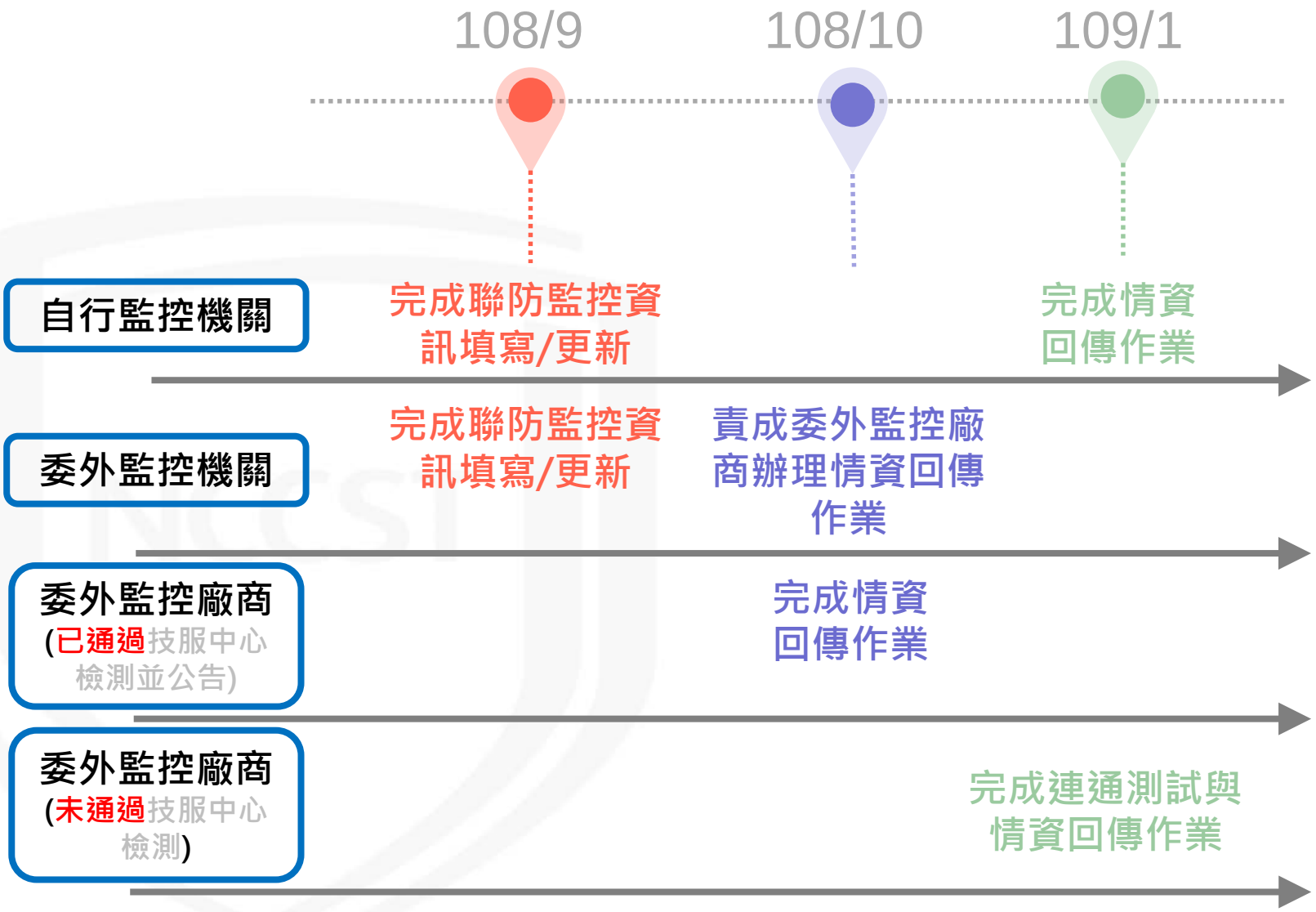
定期檢核與缺失改善

- 技服中心將定期 / 非定期進行檢核，確保資安監控回傳機制之有效性
  - 事件單是否正常回傳
  - 收容機關是否正確
  - 資安防護項目是否符合最低要求
- 相關辦理情形將提供行政院資安處參辦

大綱

- 前言
- 聯防監控架構說明
- 聯防監控情資回饋
- 聯防監控作業流程說明
- 推動時程與工作項目

後續辦理事項時程表


108/9
108/10
109/1
自行監控機關
完成聯防監控資訊填寫/更新
完成情資回傳作業
委外監控機關
完成聯防監控資訊填寫/更新
責成委外監控廠商辦理情資回傳作業
委外監控廠商
(已通過技服中心檢測並公告)
完成情資回傳作業
委外監控廠商
(未通過技服中心檢測)
完成連通測試與情資回傳作業

後續辦理事項說明

- 機關應於108年底完成情資回傳作業
  - 108年8月底前完成管考系統填寫/更新聯防監控資訊
  - 委外監控機關
    - 委外監控廠商已通過技服中心檢測並公告
      - 108年10月前開始情資回傳作業
    - 委外監控廠商未通過技服中心檢測
      - 機關應責成委外監控廠商於108年底前完成連通測試與情資回傳作業
  - 自行監控機關
    - 108年底前完成連通測試與情資回傳作業
- 109年起機關將使用STIX格式回傳
  - 現行聯防監控回傳格式將使用至108年底
- 後續將辦理說明會，針對聯防監控作業配合事項進行詳細說明

報告完畢
敬請指教

附件1
資安監控事件分類規則說明

資安監控事件分類規則說明(1/2)

- 依照US-CERT: Federal Agency Incident Categories，分為7類；技服中心依需求新增系統服務類
  - 入侵攻擊類：系統遭攻擊成功獲取非法權限
  - 阻斷服務類：遭到大量惡意阻斷服務事件
  - 惡意程式類：偵測到主機含有惡意程式，如木馬、後門等
  - 政策規則類：違反機關之資安政策所造成的事件

監控事件分類	入侵攻擊類	阻斷服務類
事件主旨範例	• 內部電腦連線至C&C網站 • 網頁遭受竄改 • 內部主機執行掃描探測攻擊	• 防火牆服務阻斷攻擊 • 外部主機阻斷服務攻擊
監控事件分類	**惡意程式類**	**政策規則類**
事件主旨範例	• 後門/間諜程式行為 • 病毒擴散案件 • 惡意物件程式下載案件	• P2P連線行為 • 非上班時間任何登入嘗試 • 遠端存取控制行為案件

資安監控事件分類規則說明(2/2)

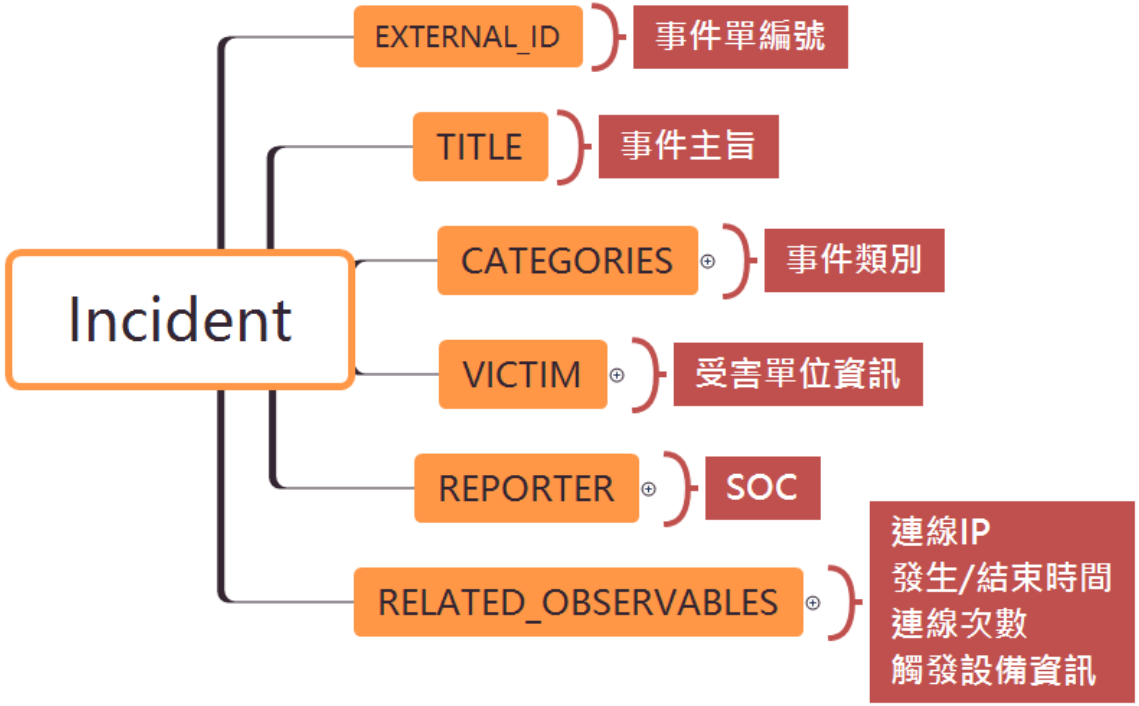
- 依照US-CERT: Federal Agency Incident Categories分為7類，技服中心依需求新增系統服務類
  - 掃描刺探類：偵測到掃描事件或漏洞利用的非成功攻擊事件
  - 尚需調查類：可疑但跡證不足，需更多資料關聯證明是否為資安事件
  - 經同意之網路攻防演練類：網路攻防演練所造成的事件
  - 系統服務類：為預期與非預期之設備維修或系統更新造成之中斷服務事件

監控事件分類	掃描刺探類	尚需調查類
	偵測到掃描事件或漏洞利用的非成功攻擊事件	可疑但跡證不足，需更多資料關聯證明是否為資安事件
事件主旨範例	• Apache Struts 2漏洞探測 • 多帳號與系統密碼猜測行為 • 外部主機嘗試XSS攻擊	• 內部電腦異常流量 • PHP 異常執行案件 • 可疑對外連線
監控事件分類	**經同意之網路攻防演練類**	**系統服務類**
事件主旨範例	• 政府機關攻防演練案件	• 網頁服務中止 • 網路設備介面關閉

附件2
收容情資欄位STIX格式說明

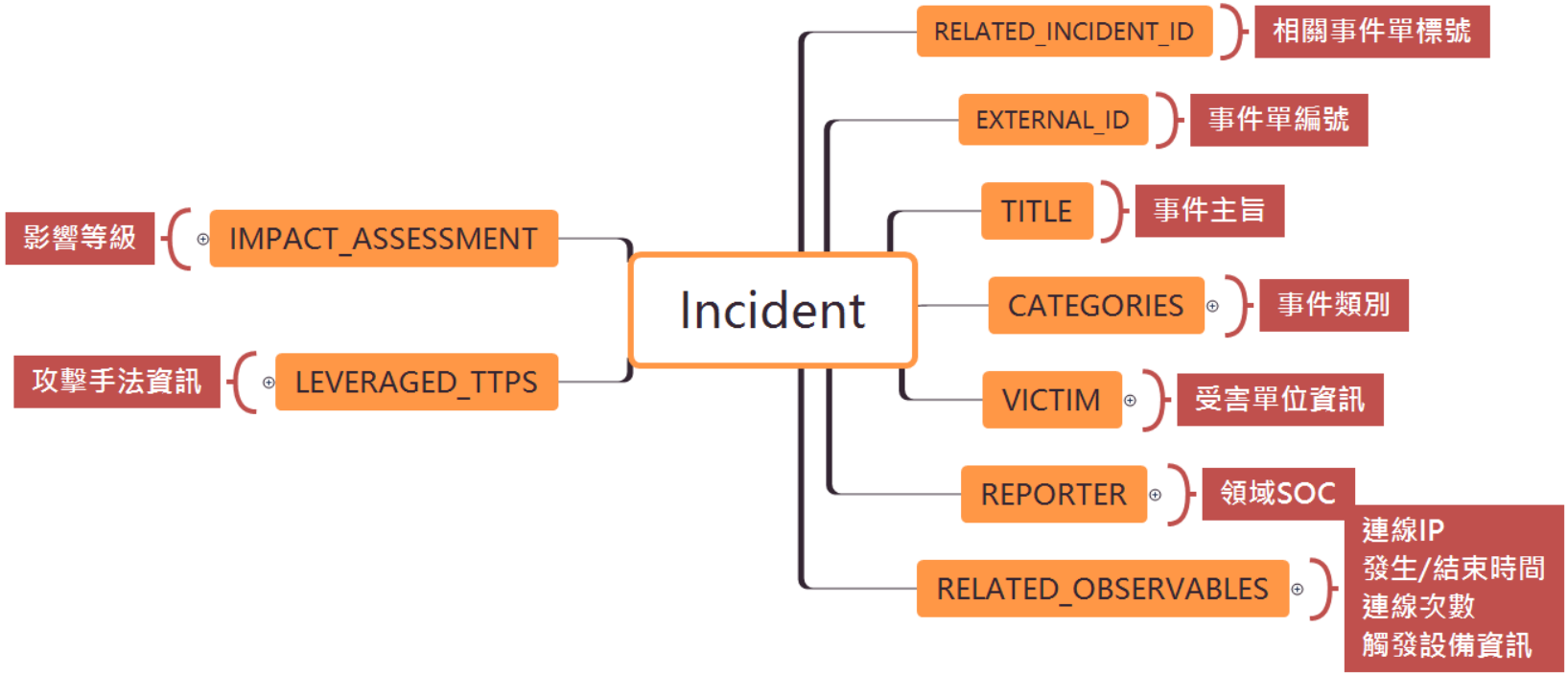
資安監控事件單欄位

- 包含6大項資訊(總計18個欄位資訊)
- 提供資安監控機制整合之事件



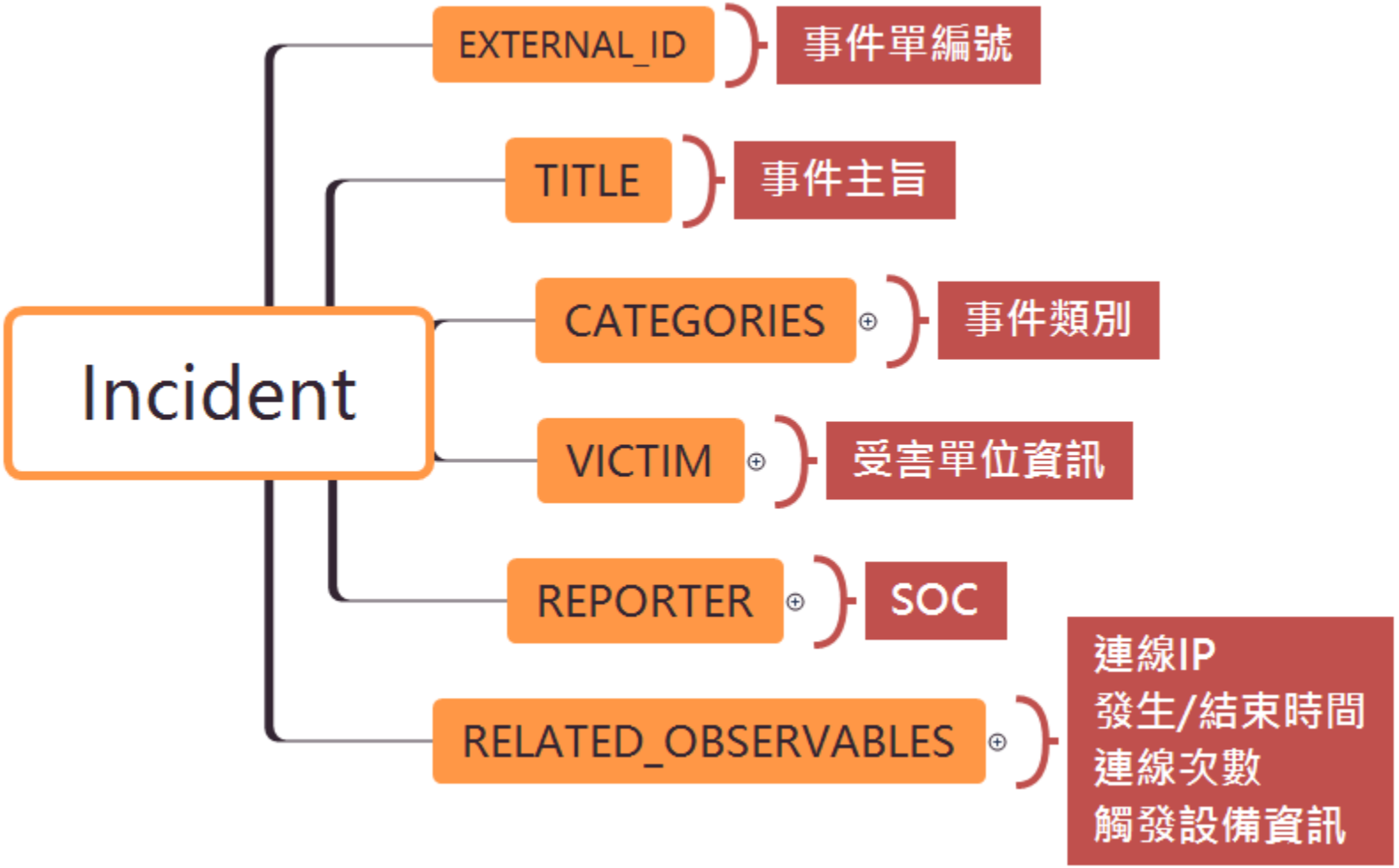
關聯分析事件單欄位

- 包含9大項資訊(總計32個欄位資訊)
- 影響等級與攻擊手法資訊
  - 主要為監控分析人員評估事件影響等級，並對事件進行威脅與手法資訊描述



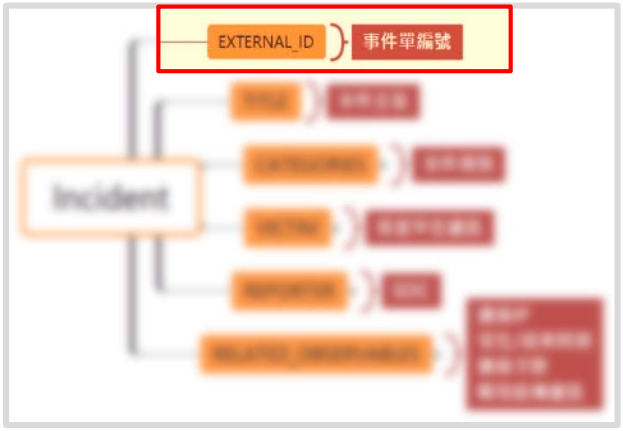
資安監控事件單(1/9)

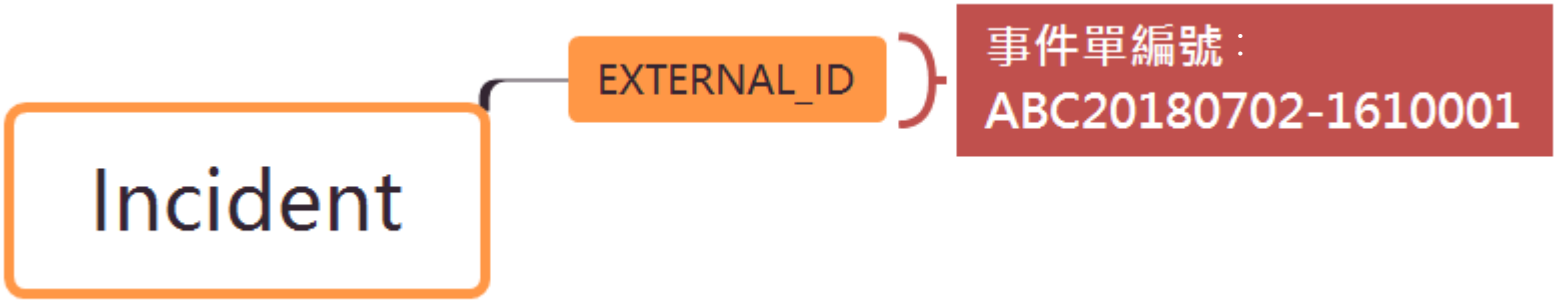
- 包含6大項資訊(總計18個欄位資訊)



資安監控事件單架構(2/9)

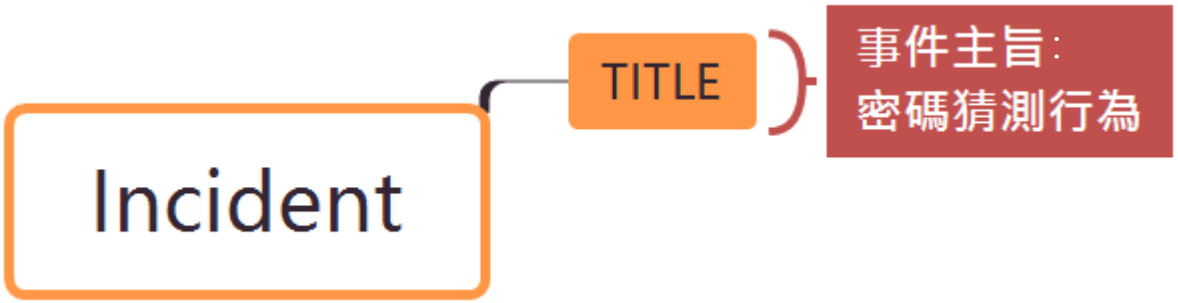
- 事件單編號(External_ID)
  - –資安監控事件單編號





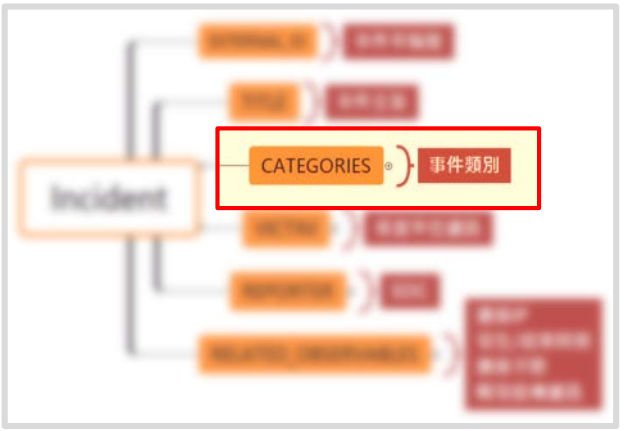
資安監控事件單架構(3/9)

- 事件主旨(Title)
  - –監控觸發事件主旨

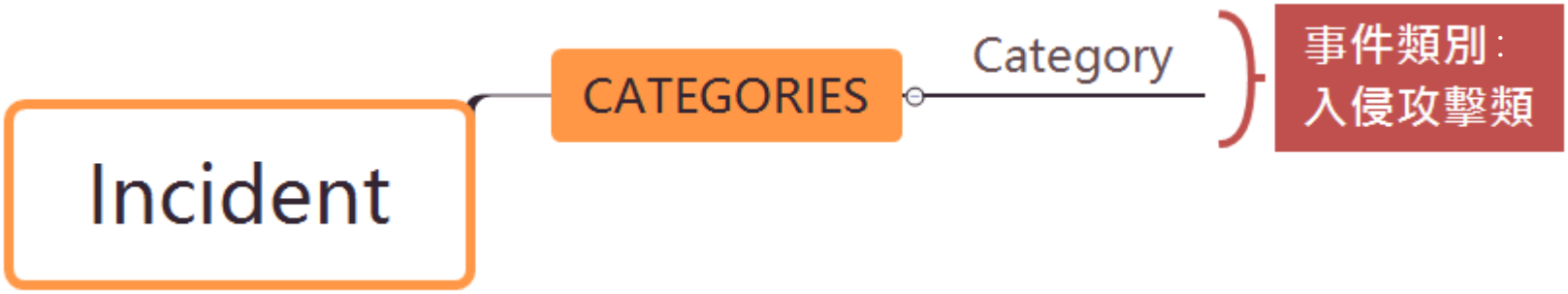


資安監控事件單架構(4/9)

- 事件類別(Category)
  - 依照技服中心公布事件8大類別進行分類，詳細事件分類說明與範例請見附件1

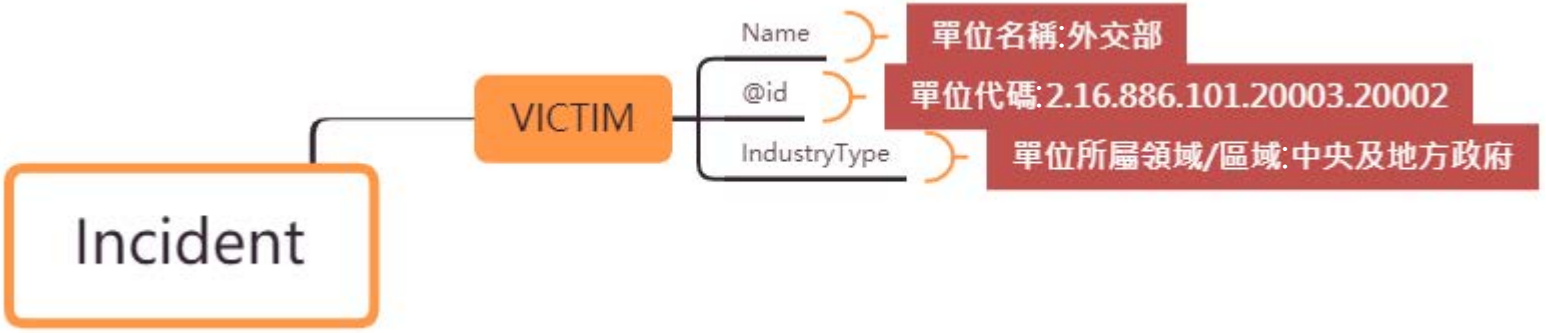


項次	事件類別	項次	事件類別
1	入侵攻擊類	5	阻斷服務類
2	惡意程式類	6	政策規則類
3	掃描刺探類	7	尚需調查類
4	經同意之網路攻防演練	8	系統服務類



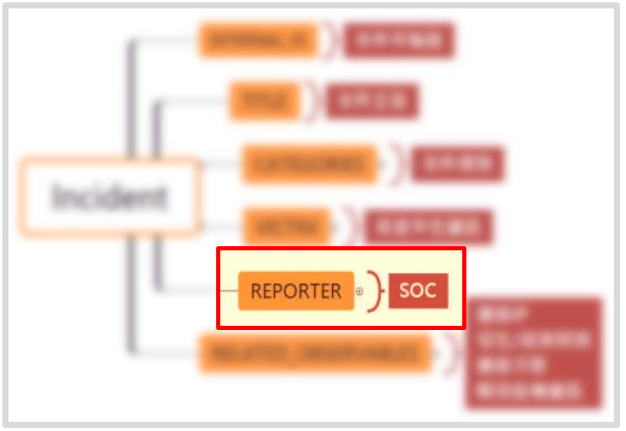
資安監控事件單架構(5/9)

- 受害單位資訊(Victim)
  - 單位名稱
  - 單位代碼(選填)
    - 公務機關填寫機關OID
  - 單位所屬領域/區域
    - 統一填寫「中央及地方政府」



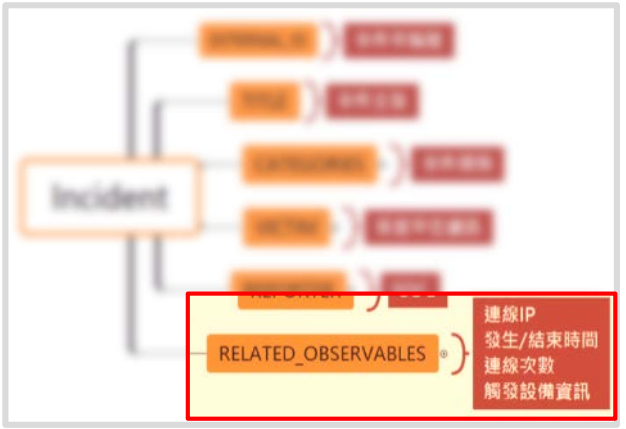
資安監控事件單架構(6/9)

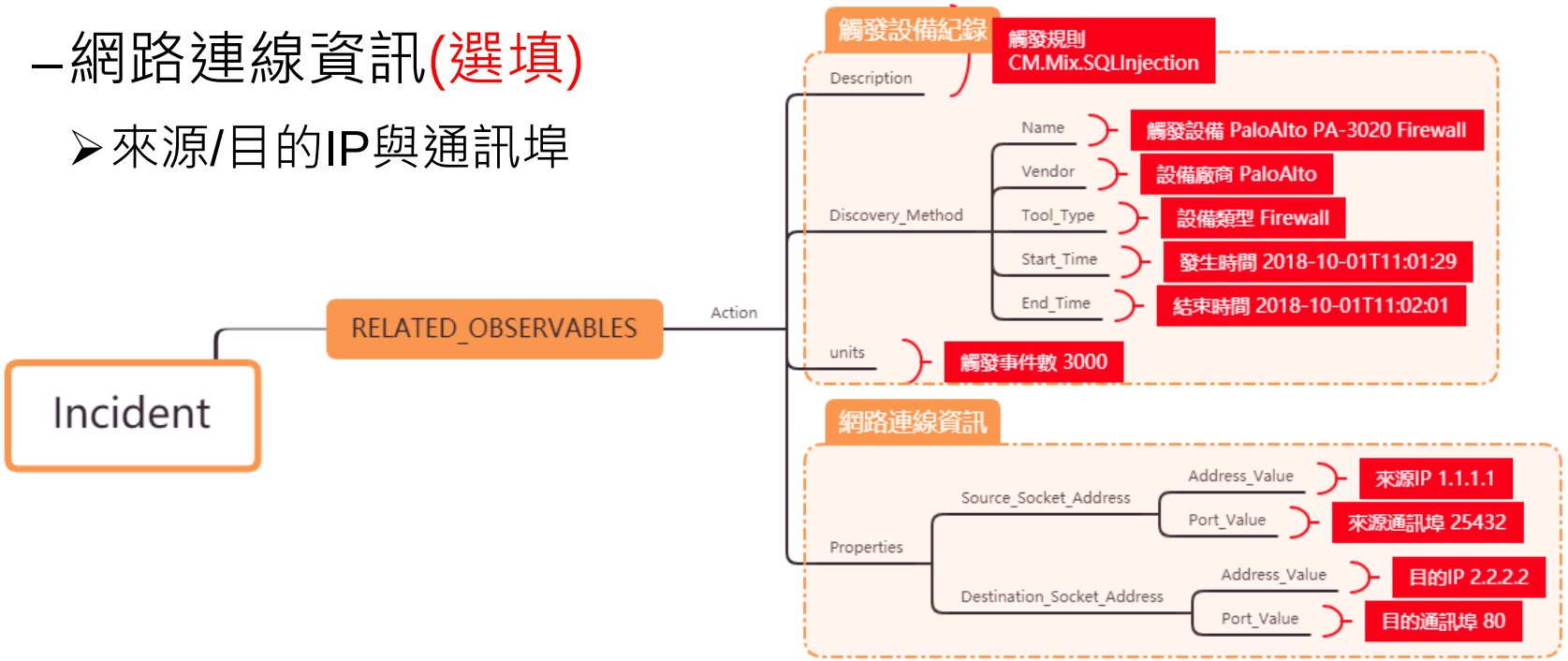
- 資安監控單位(Reporter)
  - 填寫監控執行會員名稱
    - 自建SOC
    - MSSP業者



資安監控事件單架構(7/9)

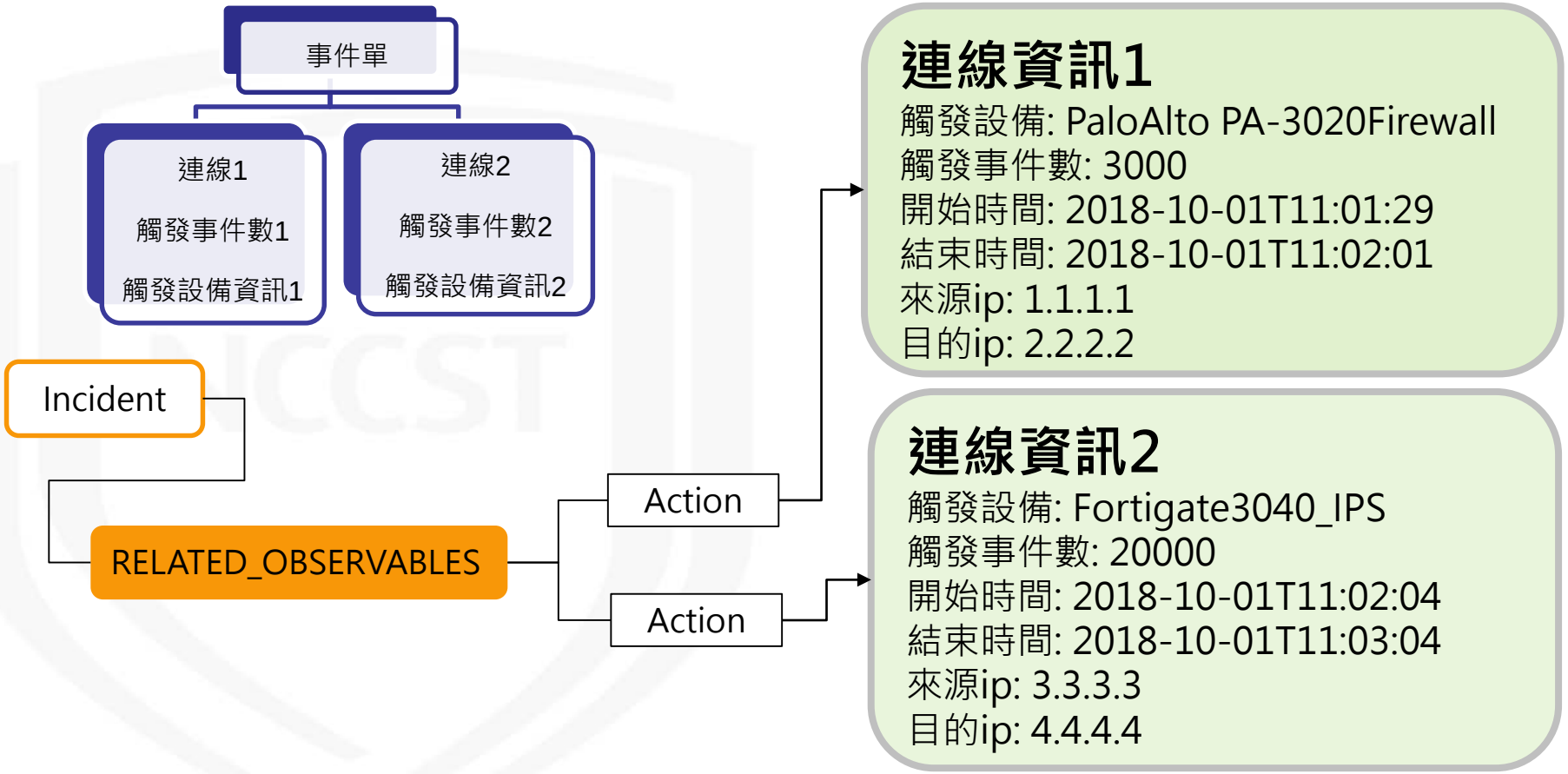
- 監控觸發紀錄 (Related_observables)
  - 觸發設備資訊
    - 觸發規則、設備、設備廠商、設備類型、發生時間、結束時間、觸發事件數
  - 網路連線資訊(選填)
    - 來源/目的IP與通訊埠





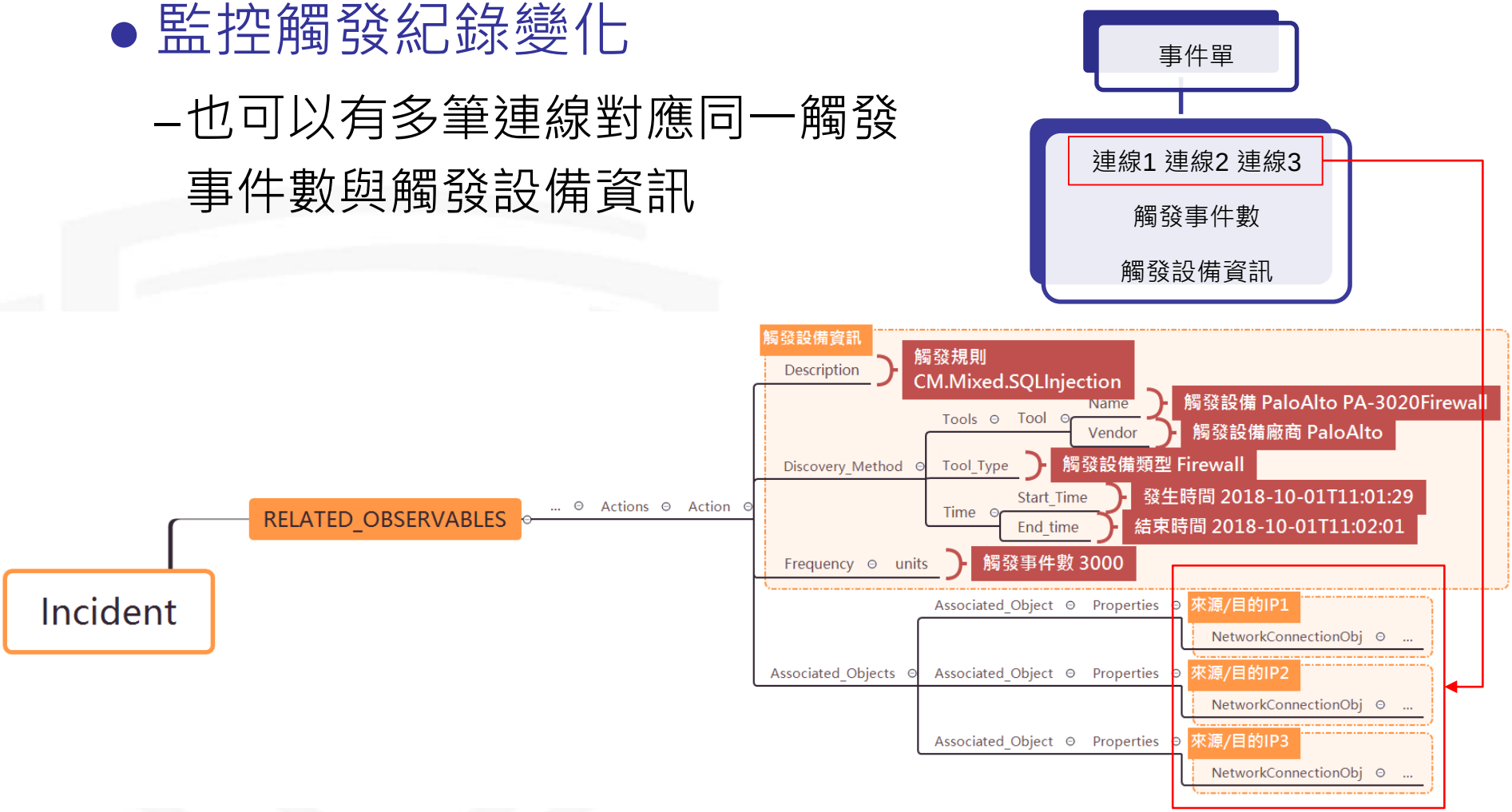
資安監控事件單架構(8/9)

- 監控觸發紀錄變化
  - 可包含多筆連線IP對應個別觸發事件數與觸發設備資訊



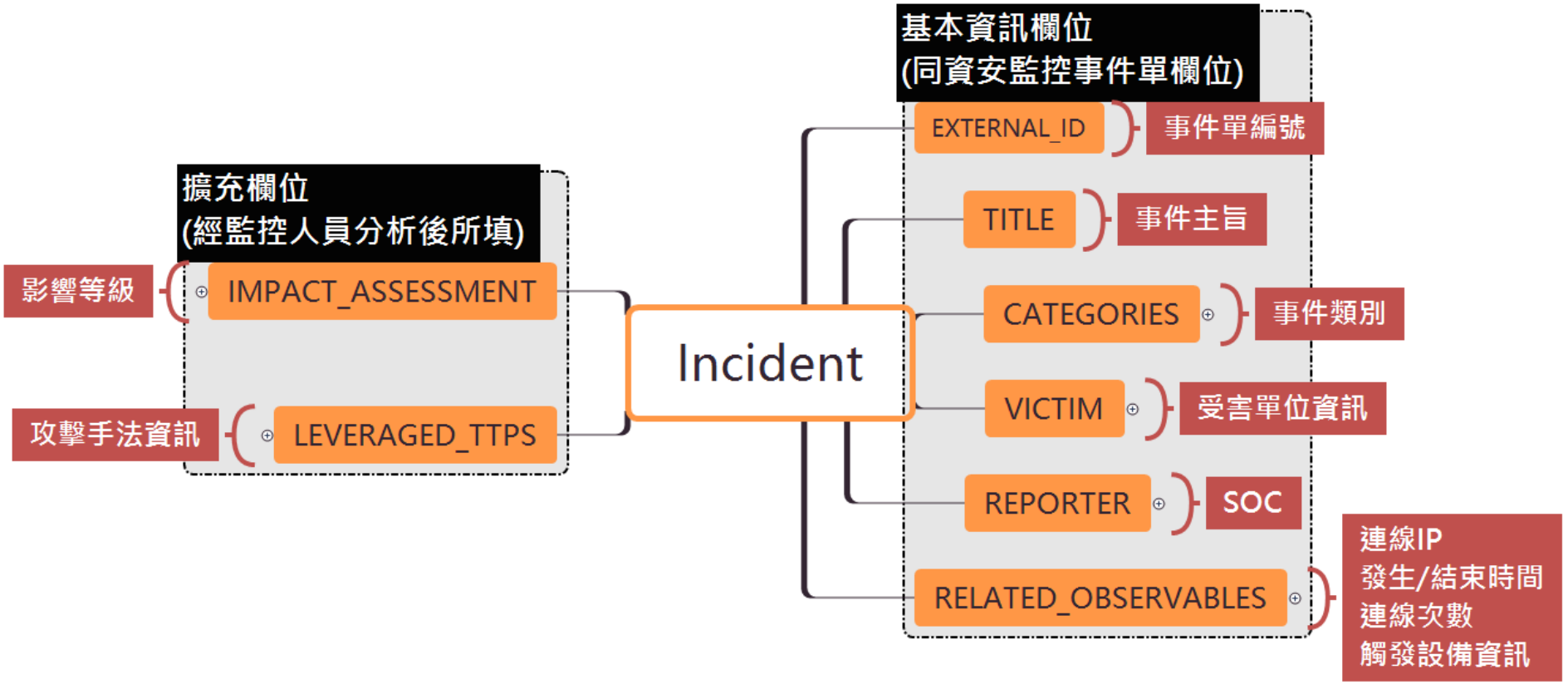
資安監控事件單架構(9/9)

- 監控觸發紀錄變化
  - 也可以有多筆連線對應同一觸發事件數與觸發設備資訊



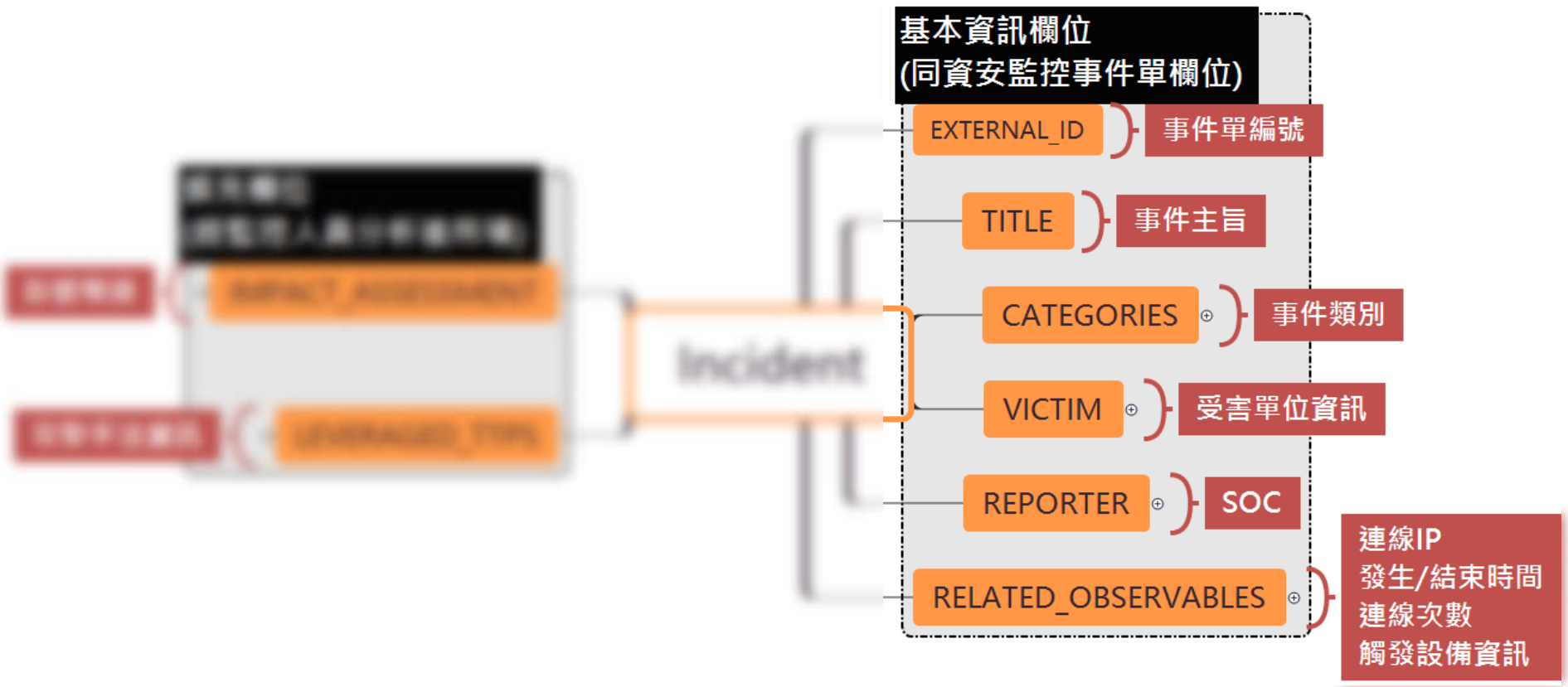
關聯分析事件單(1/7)

- 包含8大項資訊(總計31個欄位資訊)



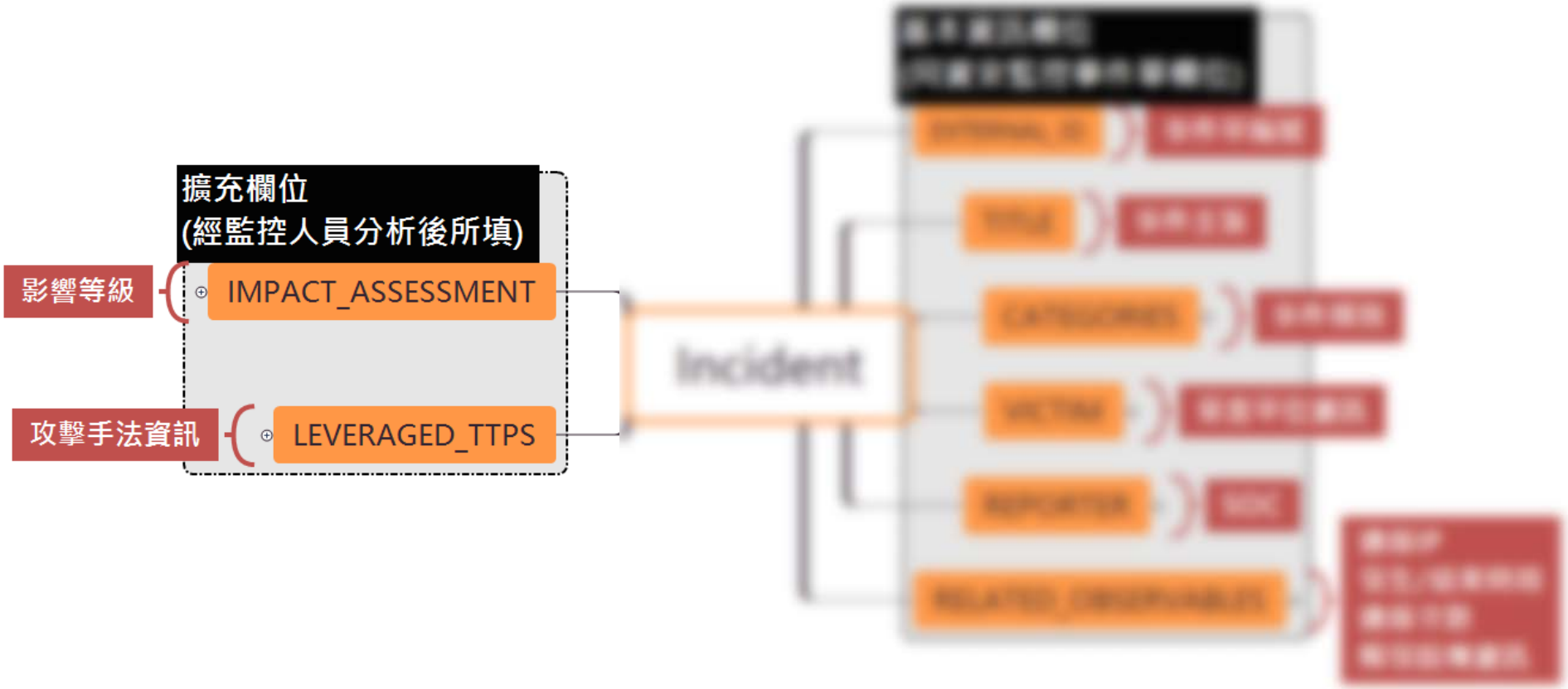
關聯分析事件單(2/7)

- 基本資訊欄位(同資安監控事件單)



關聯分析事件單(3/7)

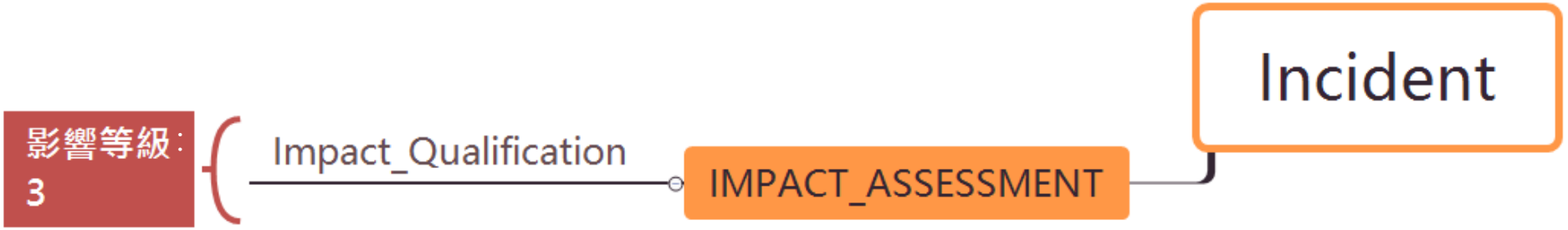
- 擴充欄位(經人員分析所填)
  - –共13個欄位資訊



關聯分析事件單(4/7)

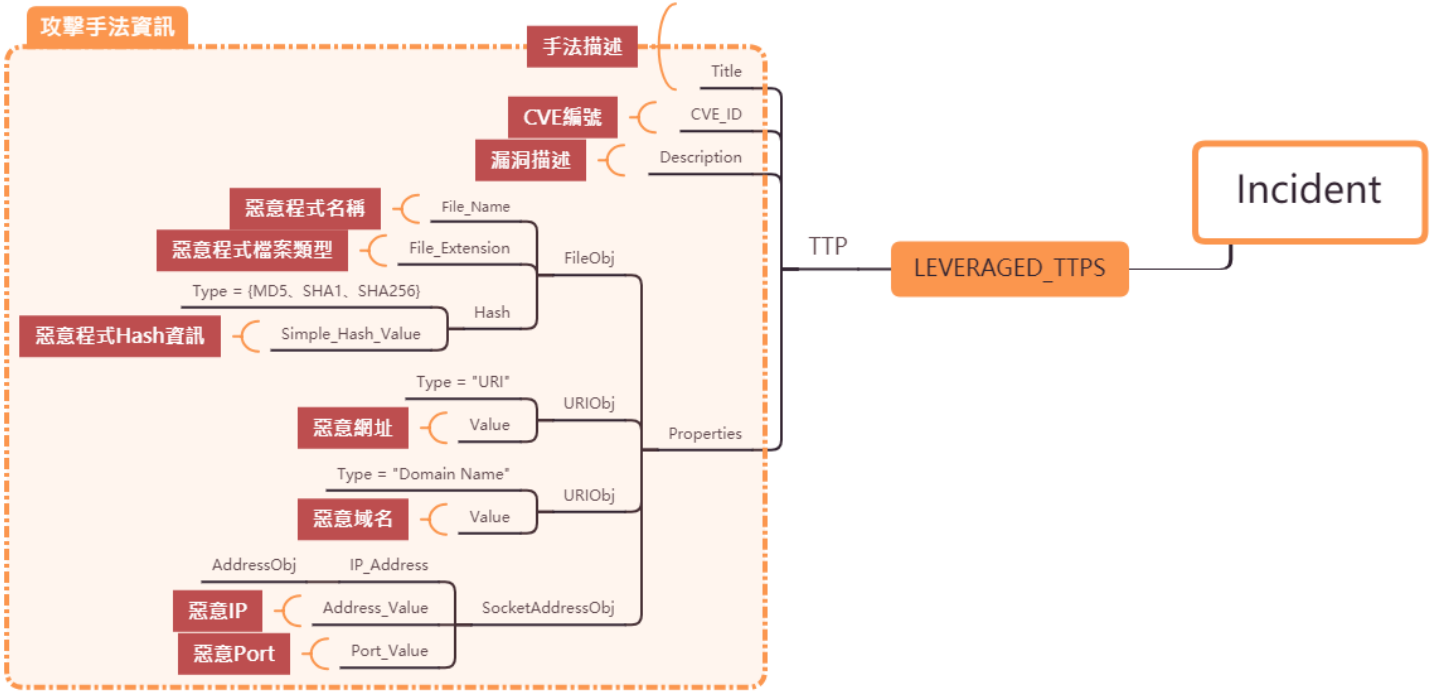
- 影響等級
  (Impact_assessment)

嚴重等級	CVSS 3.0 對應值	說明
4	9.0 - 10.0	定義為此情資內容(事件、威脅、弱點) 所可能造成衝擊的嚴重程度，將根據其CIA衝擊程度、影響範圍、攻擊模式等加權值評定
3	7.0 - 8.9	
2	4.0 - 6.9	
1	0.0 - 3.9	



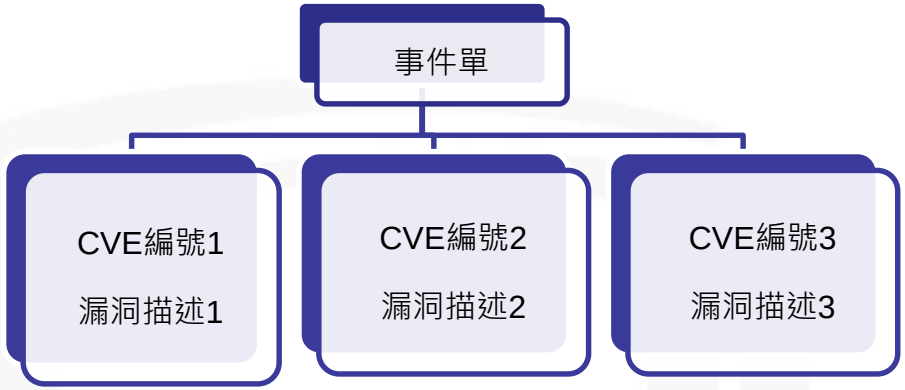
關聯分析事件單(5/7)

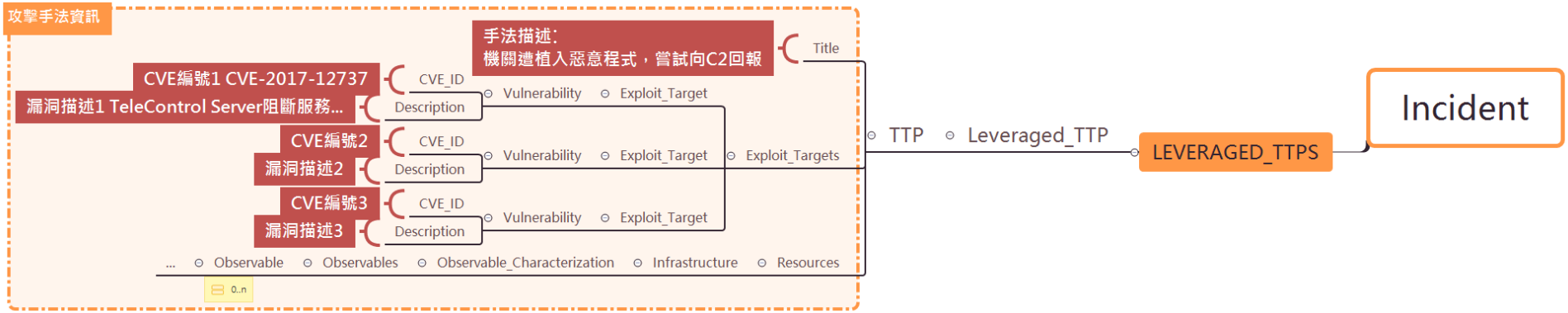
- 攻擊手法資訊(Leveraged_TTPS)
  - 攻擊手法資訊
    - 手法描述
    - CVE編號、漏洞描述(選填)
    - 惡意IOC(選填)
      - IP、DN、URL或惡意程式



關聯分析事件單(6/7)

- 攻擊手法資訊變化
  - –涵蓋多CVE編號資訊





關聯分析事件單(7/7)

- 攻擊手法資訊變化
  - –涵蓋多惡意網域資訊