106年

國家資通安全防護整合服務計畫

領域SOC實務建置指引

(V1.0)

中華民國106年3月

修訂歷史紀錄表

項次	計畫資訊			發行紀錄		說明
	年度	版次	修訂日期	版次	日期	
1	106	V1.0	106/3	V1.0	106/3	新編
2						
3						

資料來源：技服中心整理

目　次

1. 前言 1
1.1. 目的 1
1.2. 適用對象 1
2. 角色權責與分工 3
2.1. 國家層級(N-SOC) 3
2.2. 各 CI 領域層級(各領域 SOC) 3
2.3. 各 CI 提供者層級(CI-SOC) 3
3. 建置實務 4
3.1. 規劃階段 5
3.2. 執行階段 19
3.3. 查核階段 30
3.4. 改善階段 33
4. 結論 35
5. 參考文獻 36
6. 附件 37
附件 1　STIX 第一版 9 大模組介紹 ..... 附件 1-1
附件 2　領域 SOC 事件調查情資回饋 STIX 封裝範例 ..... 附件 2-1
附件 3　每月事件誤報情資回饋 STIX 封裝範例 ..... 附件 3-1

圖 目 次

圖 1　行政院國家資通安全會報組織架構 2
圖 2　角色權責與分工示意圖 3
圖 3　PDCA 建置步驟示意圖 5
圖 4　SOC 建置團隊參考架構 5
圖 5　領域 SOC 建置流程 19
圖 6　領域 SOC 事件情資收容處理運作架構 22
圖 7　跨層級 SOC 運作流程示意 23
圖 8　領域 SOC 監看 CI-SOC 資安情資運作流程 24
圖 9　領域 SOC 監看資料查驗流程圖 25
圖 10　領域 SOC 情資處理流程 26
圖 11　資安威脅情資應用情境示意 27
圖 12　每月事件調查真實事件情資回饋示意 29
圖 13　領域 SOC 連通測試流程圖 31

表 目 次

表 1　SOC 建置需求分析 7
表 2　通用之情資交換格式 13
表 3　政府領域事件類型分類 16
表 4　領域 SOC 服務內容 17
表 5　SOC 管理文件參照表 20
表 6　節錄 STIX 官方情資範本 28
表 7　領域 SOC 資訊回傳流程測試項目 32
表 8　領域 SOC 收容機制運作演練項目 33

1. 前言

為了落實推動國家關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)，特制定領域資訊安全監控中心(Security Operation Center, SOC)實務建置指引，作為關鍵基礎設施領域層級與關鍵基礎設施提供者，於執行領域 SOC 建置與維運的作業參考。各領域層級可依循本指引，再根據各領域特性，調整為各領域實務上適用的規範。

1.1. 目的

本指引主要協助關鍵基礎設施(Critical Infrastructure, CI)領域主管機關相關人員，於辦理領域資安監控作業前，視各類關鍵基礎設施型態，於各關鍵基礎設施領範圍，訂定關鍵基礎設施資安監控與資訊回傳規範。評估關鍵基礎設施安全現況，以有效掌握關鍵基礎設施資訊安全之運行，預防資安事件發生。

協助關鍵基礎設施領域主管機關，強化領域資安監控作業之運作管理，以符合各關鍵基礎設施領域主管機關資安監控與資訊回傳管理規範之要求。

1.2. 適用對象

本指引適用對象為行政院「國家資通安全會報」於網際防護體系下設「關鍵資訊基礎設施安全管理組」，並依 8 大領域區分之主政機關，詳見圖 1。

如有建置領域 SOC 需求之政府機關(構)或民間企業組織，亦可使用本指引做為建置領域 SOC 之參考資料。

●8 大領域， 共計 7 個主政機關

– 通訊傳播分組，主政機關：通傳會

– 衛生醫療分組，主政機關：衛福部

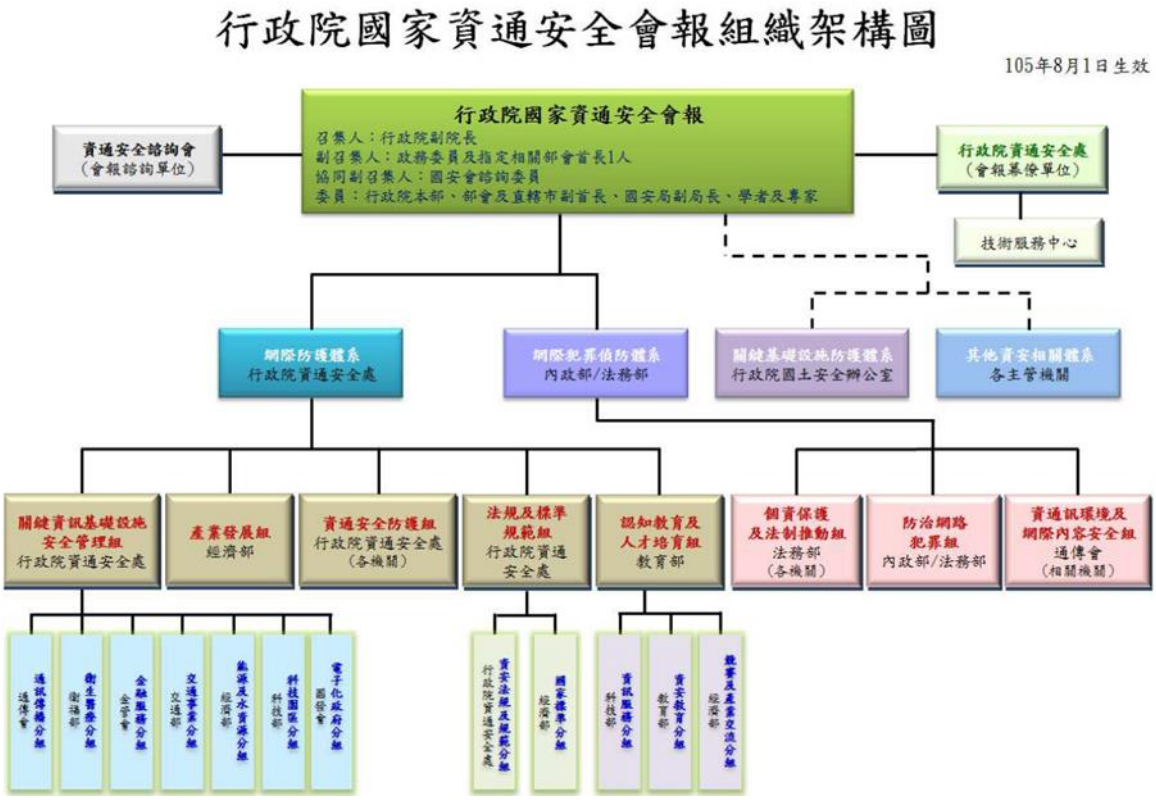
– 金融服務分組，主政機關：金管會

– 交通事業分組，主政機關：交通部

– 能源及水資源分組，主政機關：經濟部

– 科技園區分組，主政機關：科技部

– 電子化政府分組，主政機關：國發會



資料來源：行政院國家資通安全會報[1]

圖1　行政院國家資通安全會報組織架構

2. 角色權責與分工

本指引針對國家層級、各 CI 領域層級與各 CI-SOC 層級規劃相對應之角色與其權責分工詳見圖 2，並分述如下:

2.1.國家層級(N-SOC)

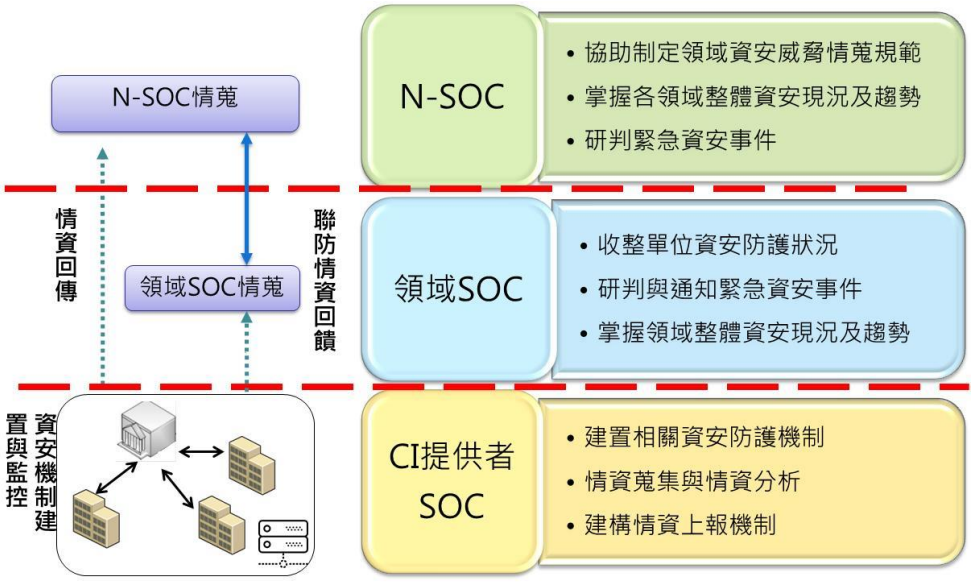
制定關鍵基礎設施資安威脅情蒐規範，掌握我國整體資安現況以及趨勢，收容領域主管單位關鍵基礎設施情資。

2.2.各 CI 領域層級(各領域 SOC)

主責領域內資安監看情資彙整，掌握領域整體資安現況以及趨勢，建構縱向該領域之 SOC 監看機制。

2.3.各 CI 提供者層級(CI-SOC)

掌握該單位資安情資狀況與建構事件情資向上回傳機制。



資料來源：技服中心整理

圖2　角色權責與分工示意圖

3. 建置實務

本指引將以領域 SOC 之建置作業為模型，逐步說明建置 SOC 之參考步驟，以 Plan-Do-Check-Act(PDCA)循環之各階段作業項目進行，詳見圖 3。

●規劃階段(Plan)

領域 SOC 應規劃建置團隊，確認領域 SOC 之服務項目與內容，並擬定建置計畫。

●執行階段(Do)

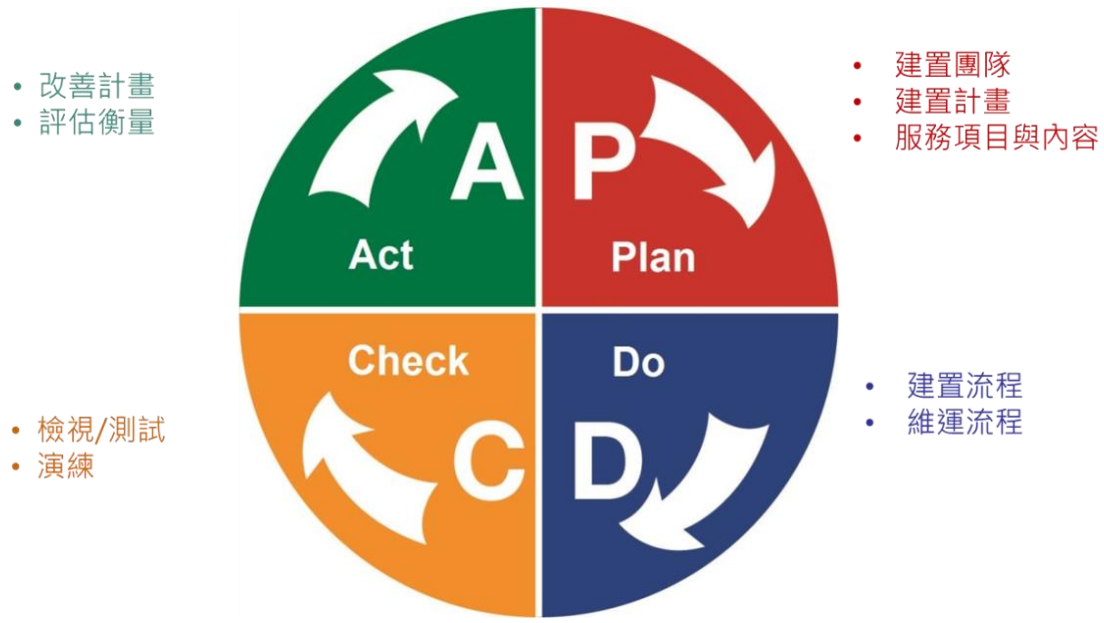
領域 SOC 應就建置時期與後續維運作業，訂定與實作相關規範與作業程序。

●查核階段(Check)

領域 SOC 應訂定檢視與測試相關程序，並定期執行。此外，應落實業務項目之演練作業，以利執行人員熟悉相關作業項目與程序。

●改善階段(Act)

領域SOC應規範管理審查機制，確保領域SOC之運作符合預期目標。此外，應依據管理審查內容訂定改善計畫，並落實追蹤。



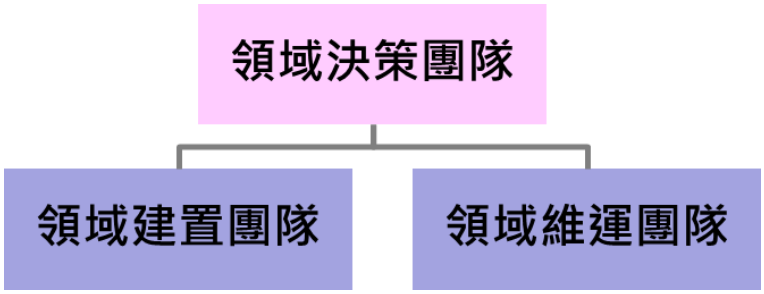
資料來源：技服中心整理

圖3　PDCA 建置步驟示意圖

3.1.規劃階段

3.1.1. 建置團隊

團隊建置詳見圖 4，分為領域決策團隊、領域建置團隊與維運執行團隊，相關分工及對應職掌敘述如下:



資料來源：技服中心整理

圖4　SOC 建置團隊參考架構

●領域決策團隊

– 擬定與控管建置計畫，確認建置時程與推動時程。

– 確認計畫執行資源，包含單位執行之人力與預算。

– 透過良好的協調機制，促進橫向跨組織的聯繫，整合各關係人與資源，並縱向溝通傳達確保落實情形。

●領域建置團隊

– 確認領域 SOC 監看項目，包含領域規範制定、監控範圍定義與情資交換規格制訂。

– 實際執行建置計畫並依工作項目分組，適時報告執行進度及狀況。

●領域維運團隊

– 針對監看資料進行實際收容與分析。

– 負責領域內資安事件研判與回傳監看資訊至 N-SOC。

– 負責確保領域內監看業務之正常運作。

3.1.2. 建置計畫

建置領域 SOC 應先完成需求分析，以了解所在 CI 領域之特殊業務與相關情資需求，並識別領域內資安監控情資範圍與對象，以妥善配置相關資源。

3.1.2.1. 需求分析

SOC 建置需求主要分為資安防護機制建置、領域事件情蒐分析、N-SOC 資訊介接與領域聯防情資回饋工作項目，針對 N-SOC、領域 SOC 及 CI-SOC 所需之功能建置需求評估建議詳見表 1。

表1　SOC 建置需求分析

作業項目	國家層級 (N-SOC)	各 CI 領域層級 (領域 SOC)	各 CI 提供者層級 (CI-SOC)
資安防護機制建置，資安監看與事件處理	可選擇項目	可選擇項目 (或僅接收)	必要項目
領域事件情蒐分析	必要項目	必要項目	配合事件處理
N-SOC 資訊介接	必要項目	必要項目	必要項目
領域聯防情資回饋	必要項目	必要項目	可選擇項目 (或僅接收)
設置特定資安工作小組	可選擇項目	可選擇項目	可選擇項目

資料來源：技服中心整理

●訂定轄下單位責任等級對應監看與防護範圍

領域主管單位針對下屬單位進行組織安全防護層級分類，如政府領域遵循之行政院國家資通安全會報制訂之「政府機關（構）資通安全責任等級分級作業規定」[3]，針對政府機關、學研機關(構)與各事業分組，根據組織人數、擁有資產價值分類內容等依據分類其資安責任等級及應辦事項，包含防禦機制強度、防護縱深、ISMS 推動作業及監控管理等項目，相關防護縱深所規範之資安機制亦應納入監控機制範圍，而針對領域之特殊性，可針對領域整體骨幹與共用基礎防護機制進行監看，包含：

– 內外部資安威脅情蒐機制

– IDS 與 IPS 威脅阻擋/防禦機制

– DDoS 偵測/防禦機制

– 領域重要共通性服務，如 DNS 服務架構

●資訊系統分類分級與彙整

針對資訊系統分類與分級項目之規劃，可依據行政院國家資通安全會報制定之「資訊系統分級與資安防護基準作業規定」[4]，針對資訊系統分類分級與鑑別機制處理程序中所述之方法，進行資訊資產清冊彙整，參考「資訊系統風險評鑑參考指引」[5]進行後續風險評鑑，並參考「資訊系統分級與資安防護基準作業規定」與「安全控制措施參考指引」[6]選擇安全控制措施，除確保所鑑別安全等級符合機關安全需求外，亦可作為規範資訊資產之監控防護對應等級之設備日誌保留與納入監控範圍使用。

●情資分析

領域 SOC 情資分析目標如下：

– 規劃與建構一具整併商業或自建的資安事件管理 (Security Information and Event Management, SIEM)與情資收容架構

– 建立異質資訊情資處理(Extract-Transform-Load, ETL)與分析流程，將收容之資安情資進行萃取（extract）、轉置（transform）、載入（load）與正規化處理後，導至資安監控分析平台，資訊分析項目包含如下：

➢跨單位之綜整資訊

領域內跨單位之綜整資訊分析上，可針對所屬子領域間分析，亦可針對子領域與資安威脅進行交叉分析。此外，針對掃描刺探、阻斷服務，亦或新興弱點漏洞進行領域資安分析。

◆跨 SOC 與跨機關之事件

綜整領域資訊，分析事件威脅來源出現跨領域 SOC 與跨領域子機關，評估分析跨 SOC 與跨機關之事件的威脅風險。

◆分散式阻斷服務攻擊綜覽

資安威脅活動可能對特定對象與領域進行分散式阻斷服務攻擊，故須針對領域內之資安情資全盤分析，即時掌握威脅影響範圍。

◆新興威脅綜整分析

新興漏洞與弱點發現初期常遭受零日攻擊，綜整分析相關弱點威脅、手法與影響範圍，進而提出因應措施。

◆領域子類別與資安威脅交叉分析

交叉分析領域子類別與其遭受的資安威脅，了解各子類別面對資安

威脅的同異程度。

➢領域綜整資訊分析

領域內綜整資訊分析上，可針對各領域子類別分析與各資安情資類型進行分析，亦可針對領域整體骨幹與共用基礎防護機制所蒐集與偵測之資訊。

◆領域整體威脅趨勢

依據資安事件情資進行趨勢分析，分析項目可包含各月資安事件趨勢分析、資安威脅類別趨勢分析、威脅來源趨勢分析以及威脅手法分析。

◆威脅來源分析

資安事件威脅來源分析，可區分國內外威脅來源，並針對國家與國內各 ISP 進行細部分類，了解領域資安威脅來源與威脅類別。

➢領域情資分析與聯防

領域情資分析與聯防上，可彙整 N-SOC 介接情資、共用基礎防護機制情蒐資訊與外部開源情資(Open Source Intelligence, OSINT) ，關聯 CI-SOC 收容之資安事件情資，產製事件共通之攻擊手法、弱點及威脅等聯防情資，作為提供領域內 CI-SOC 與回傳至 N-SOC 之聯防機制應用。

3.1.2.2. 建置資源

建置資源評估需確認計畫執行資源，包含單位執行之人力與預算，各 CI 間之建置 SOC 可參考技服中心「SOC 參考指引」[7]之所述之(1)監控中心實體環境(2)人力資源(3)資安服務系統(4)維運計畫四個面向進行資源與預算之評估，包含：

- 各資安設備管理成本
- 資安事件監看需求資源，包含外部情資整併與內部資訊收容
- 資安事件監看能量取得方式成本比較，包含委外、自建與協同維運方式，作為監看模式、預算資源與相關程序建立投入選擇參考使用

另外，亦須確認建置時程與資源之關聯性，包含監看執行單位之 SOC 建置、資料收容流程、監看能量部署與對外連通流程，皆為建置資源評估須考量之項目。

3.1.2.3. 規範與規格

領域監控規範制定上，針對 CI-SOC 單位資安監控機制收容項目可至少包含下列項目：

- 防護縱深上規範包含項目：如防火牆、防毒軟體、網頁應用程式防火牆(WAF)、APT 偵測及防護機制。
- 網路通訊安全、重要資訊服務安全防護與監控，包含相關網路行為、重要服務活動行為日誌留存與偵測。
- 領域專屬增修監控項目
  - 領域特殊法規、規範衍生之資安需求，如政府領域「行政院及所屬各機關資訊安全管理規範」[8]、金融領域的「金融監督管理委員會資訊安全

政策」[9]與「電信事業資通安全管理作業要點」[10]。

– 評估資安需求衍生之領域特殊法規、規範，如通訊領域之電信法等相關安全規範、製造產業安全規範、PCI DSS 3.0。

●收容情資規格制定(情資交換格式與協定制定)

– 通用之情資交換格式請詳見表 2，並進行說明。

表2　通用之情資交換格式

項次	情資交換格式名稱	情資類型	說明
1	Common Vulnerabilities and Exposures (CVE)	資安漏洞	提供已公開的資安漏洞資訊，訊息內容包含漏洞編號、名稱、描述及影響平台等，可作為漏洞資訊之識別、分享及防護使用。
2	Common Weakness Enumeration (CWE)	軟體設計漏洞與弱點	CWE 為描述架構、設計及程式碼中的軟體安全漏洞之通用標準，可作為軟體安全工具評估標準。亦提供軟體開發人員進行弱點識別、緩解及預防工作使用。
3	Common Attack Pattern Enumeration and Classification (CAPEC)	事件攻擊模式	提供常見攻擊特徵與模式的共同分類資訊與方法，作為攻擊模式的共同描述標準，可用於資安需求分析、安全架構設計、資安規範制定、安全測試及驗證使用
4	Malware Attribute Enumeration and Characterization (MAEC)	惡意程式	針對惡意程式行為、手法及攻擊模式提供標準描述語言以進行編碼與傳送，可降低研究人員在分析工作上的模糊性與不準確性，MAEC 可與 STIX 結合，提供惡意軟體與網路威脅之關聯資訊。
5	Open Vulnerability Assessment Language	資安漏洞影響範圍	用於系統評估漏洞與影響範圍的框架，提供系統資訊描述、系統特定狀態表達及檢測結果等資訊描述，可作為弱點檢測

項次	情資交換格式名稱	情資類型	說明
	(OVAL)		工具發展與流程整合使用。
6	Cyber Observable eXpression (CybOX)	資安情資	CybOX 提供一套標準且可擴展的語法，用來觀察紀錄系統操作的行為與內容，包含 HTTP sessions、X509 憑證及系統配置等資訊，可做為判斷威脅的指標，為 STIX 主要構成元素。
7	Incident Object Description Exchange Format (IODEF)	資安事件	政府領域 G-ISAC 情資交換平台以 XML 為基礎的「國際資通訊安全事故訊息交換格式 (Incident Object Description Exchange Format, IODEF)」所制定之開放標準，訊息類型包含資安訊息情報（ANA）、網頁攻擊情報（DEF）、資安預警情報（EWA）、入侵事件情報（INT）及回饋情報（FBI）等 5 種情報類型。
8	Common Event Format (CEF)	資安設備情資	一種基於 key 與 values 的資料傳遞格式，可以針對多種設備自定義相關資訊，並透過 syslog 形式傳送，提供既有的 SIEM 平台上進行跨平台的資料處理。
9	Structured Threat Information eXpression (STIX)	資安情資	一種資訊安全情資封裝架構，以擴展標記語言(Extensible Markup Language, XML)格式進行撰寫與封裝，便利於 XML 能以巢狀迴圈封裝資訊並且具有高度的可解讀性，方便人類與機器進行解讀，同時 XML 也有良好的擴展性，能透過編

項次	情資交換格式名稱	情資類型	說明
			寫將既有資訊進行擴展。

資料來源：技服中心整理

– 情資收容交換機制

領域 SOC 除了制訂情資交換格式，亦需要進行情資交換機制的確立，俾利針對 CI-SOC 資安情資進行彙整監看，資安情資收容架構機制主要包含傳統以 SSH 與 FTP 進行檔案收容外，亦有針對異質資訊進行收容與監看之商業資安日誌收容架構，包含有 Splunk、ArcSight 及 NetIQ Log manager 等商業收容架構，而現今開源分散式資料收容架構，如 Elasticsearch, Logstash, and Kibana(ELK)亦可作為單位建置資料收容與基礎分析架構可行之解決方案。

– 事件類型定義

現行政府領域參考 US-CERT，將事件類型分為系統服務、政策規則、掃描刺探、阻斷服務、惡意程式、入侵攻擊及尚需調查等 6 類，其定義詳見表 3。

表3　政府領域事件類型分類

事件類型	情資類型
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。
政策規則類	為違反機關之資安政策所造成的事件
掃描刺探類	為偵測到掃描事件或漏洞利用的非成功攻擊事件
阻斷服務類	為遭到大量惡意阻斷服務事件
惡意程式類	為偵測到主機含有惡意程式如：木馬、後門等
入侵攻擊類	為系統遭攻擊成功獲取非法權限
尚需調查類	為可疑但跡證不足，需更多資料關聯證明是否為

事件類型	情資類型
	資安事件

資料來源：技服中心整理

3.1.2.4. 建置前準備

建置領域 SOC 應完成擬訂建置計畫，包含作業項目細部執行內容，並訂定各階段里程碑，至少應包含領域 SOC 之各大核心功能。相關系統資訊安全依據可參考「資訊系統委外開發 RFP 資安需求範本」[11]。

3.1.3. 服務項目與內容

根據需求分析所彙整之核心項目與附加功能詳見表 4。

表4　領域 SOC 服務內容

功能	項目	項目說明	查核內容
核心功能	資安監看機制建置	▪建置相關資安監看機制 ▪資安監看與事件分析	▪資安事件回傳聯通測試成功 ▪各種資安類型事件回傳資料驗證無誤 ▪各 CI-SOC 回傳資訊統計功能建立
	領域事件情蒐分析	▪收整單位資安防護狀況 ▪研判與通知緊急資安事件 ▪情資蒐集與情資分析 ▪掌握領域整體資安	領域內每週/月概況統計產製

功能	項目	項目說明	查核內容
		現況及趨勢	
	N-SOC 資訊介接	▪情資蒐集與情資分析 ▪建構情資上報機制	N-SOC 回傳聯通測試成功
附加功能	領域聯防情資回饋	產製領域內跨 CI 之共同威脅情資供分享	每週/月資安情資回饋機制建立

資料來源：技服中心整理

領域 SOC 服務內容詳細說明如下：

●核心功能

– 資安監看機制建置

資安監看機制建置，涵蓋需求分析階段所述之重要資訊資產之行為紀錄與相關資安設備之情資收容類型，以及監看資訊收容架構之建立，亦包含資安事件監看與能量之完備。

– 領域事件情蒐分析

領領 SOC 之情蒐分析主要包含完成情資收容架構與能量之建立，收整 CI-SOC 情資以確保各 CI 單位之資安防護狀況。透過對收容事件之分類與內外部情資綜整分析後，掌握領域整體資安現況及趨勢。

– N-SOC 資訊介接

與 N-SOC 資訊介接上，領域 SOC 須建立資訊回傳機制，針對領域內綜合彙整分析情資，研判領域內威脅等級，除針對緊急事件進行資訊回傳，並協助針對相關聯防威脅情資所關聯之事件情資，以達國家整體資安威

脅綜整分析與聯防機制之用。

●附加功能

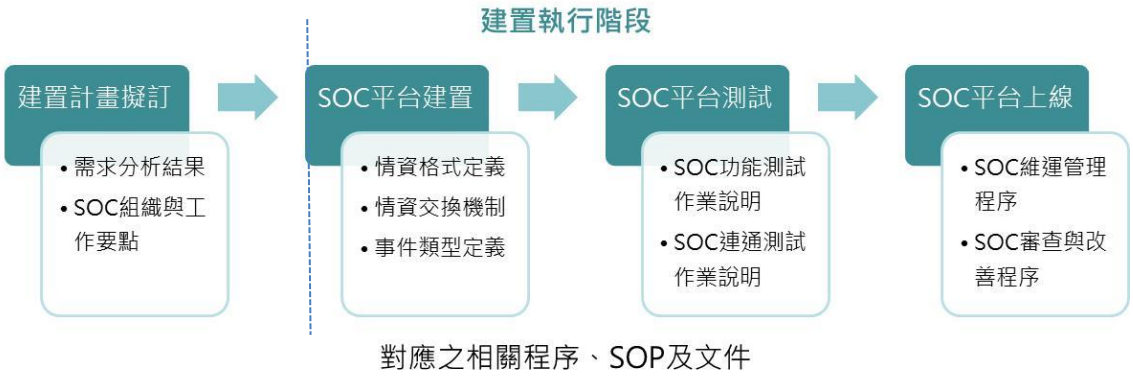
– 領域聯防情資回饋

領域 SOC 依據 CI-SOC 回傳事件情資進行彙整，並提供領域聯防情資供 CI 提供者進行阻擋。聯防情資可依據領域事件情資進行規劃，分享彙整情資可依據情資類型進行匯聚包含：情資來源單位、資安威脅類別、威脅來源國家別及惡意程式種類等，並針對跨轄下 CI-SOC 威脅攻擊資訊萃取出之入侵攻擊指標資訊(Indicator of Compromise, IoC)提供給領域 CI-SOC 進行聯防偵測與防護。

3.2.執行階段

3.2.1. 建置流程

領域 SOC 建置流程詳見圖 5，建置流程應分別進行建置計畫擬訂、SOC 平台建置、SOC 平台測試及 SOC 平台上線等步驟。



資料來源：技服中心整理

圖5　領域 SOC 建置流程

領域 SOC 應訂定維運所需之相關管理程序與文件，詳見表 5。

表5　SOC 管理文件參照表

項次	文件類型	文件內容
1	領域 SOC 管理政策/規章	▪領域 SOC 管理規範內容 ▪領域 SOC 會員申請與核定規範
2	連通程序資料	▪聯防監控事件紀錄資料回傳標準作業程序 ▪機關申請聯防監控報表系統帳號申請及異動書 ▪機關申請聯防監控報表系統帳號申請及異動書 ▪聯防監控資訊回傳作業帳號申請及異動書 ▪連通測試書 ▪資料回傳定期稽核檢測步驟 Checklist ▪稽核問題紀錄單
3	資料交換技術文件	▪自建機關事件單 XML 範本 ▪廠商事件單 XML 範本 ▪事件資料數據回傳欄位與格式規範 ▪機關服務列表範例 ▪關聯規則 ID 對照總表範例

資料來源：技服中心整理

●領域 SOC 管理政策/規章

建置領域 SOC 應遵循相關作業程序與文件，以落實日常之維運管理。並建立 CI-SOC 會員申請管道，進行資格審查，落實篩選適宜之 CI-SOC 加入領域 SOC。

●連通程序資料

訂定領域 SOC 連通程序相關資料，含回傳標準作業程序、帳號申請書、

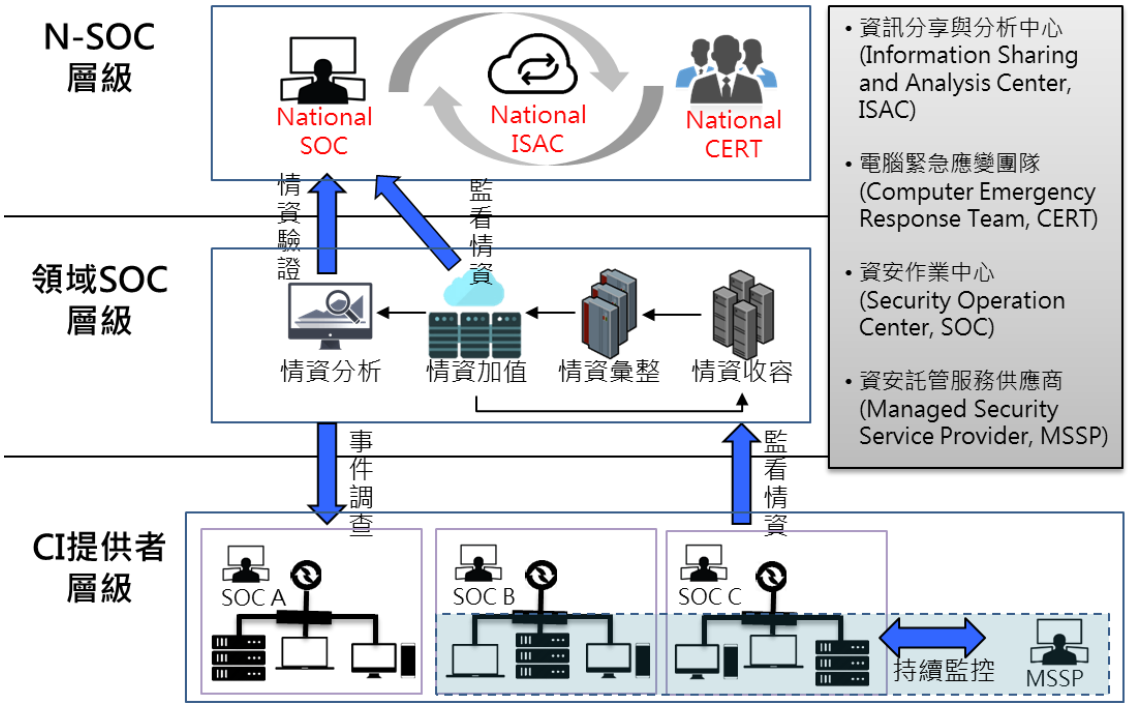
檢測步驟確認單，可參考技術服務中心「聯防監控_事件紀錄資料回傳標準作業程序」、「聯防監控資訊回傳作業帳號申請及異動書」、「連通測試書」、「資料回傳定期稽核檢測步驟 Checklist」與「稽核問題紀錄單」。

- 資料交換技術文件

制定領域 SOC 情資收容規範，對 CI-SOC 明確定義資料回傳格式與情資內容，可參考技術服務中心「自建機關事件單 XML 範本」、「廠商事件單 XML 範本」及「事件資料數據回傳欄位與格式規範」。此外，領域事件情資傳送予 N-SOC 需符合 N-SOC 情資規範與格式。

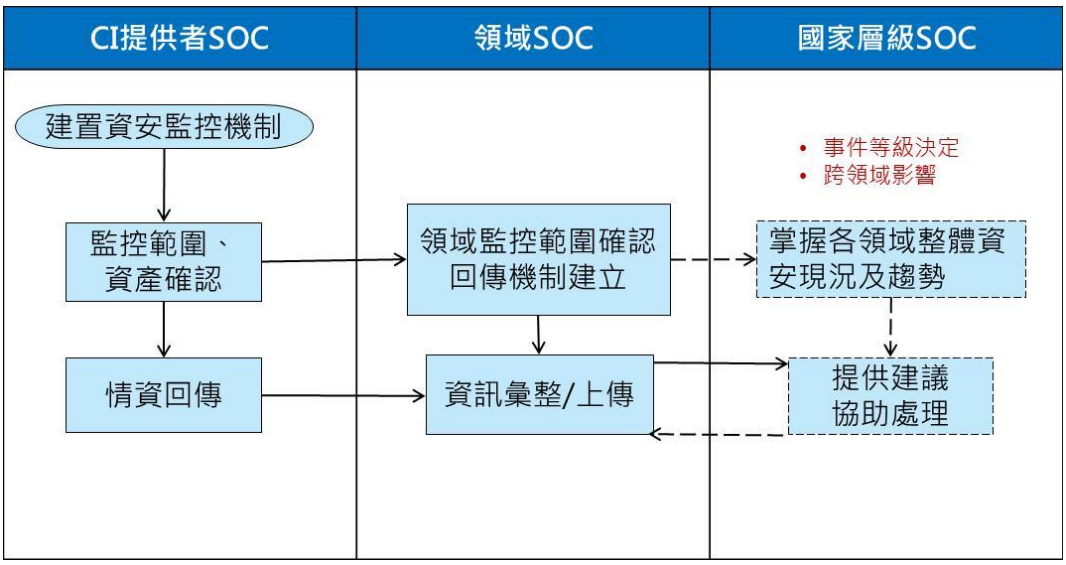
3.2.2. 維運流程

CI-SOC、領域 SOC 及 N-SOC 彼此間運作架構及流程詳見圖 6 與圖 7。領域 SOC 收容 CI-SOC 事件情資進行情資彙整、加值與分析，並適時針對重大事件支援 CI-SOC 進行事件調查。同時，領域 SOC 及時回傳情資予 N-SOC，並固定回報真實情資資訊予 N-SOC，確保情資準確性。



資料來源：技服中心整理

圖6　領域 SOC 事件情資收容處理運作架構



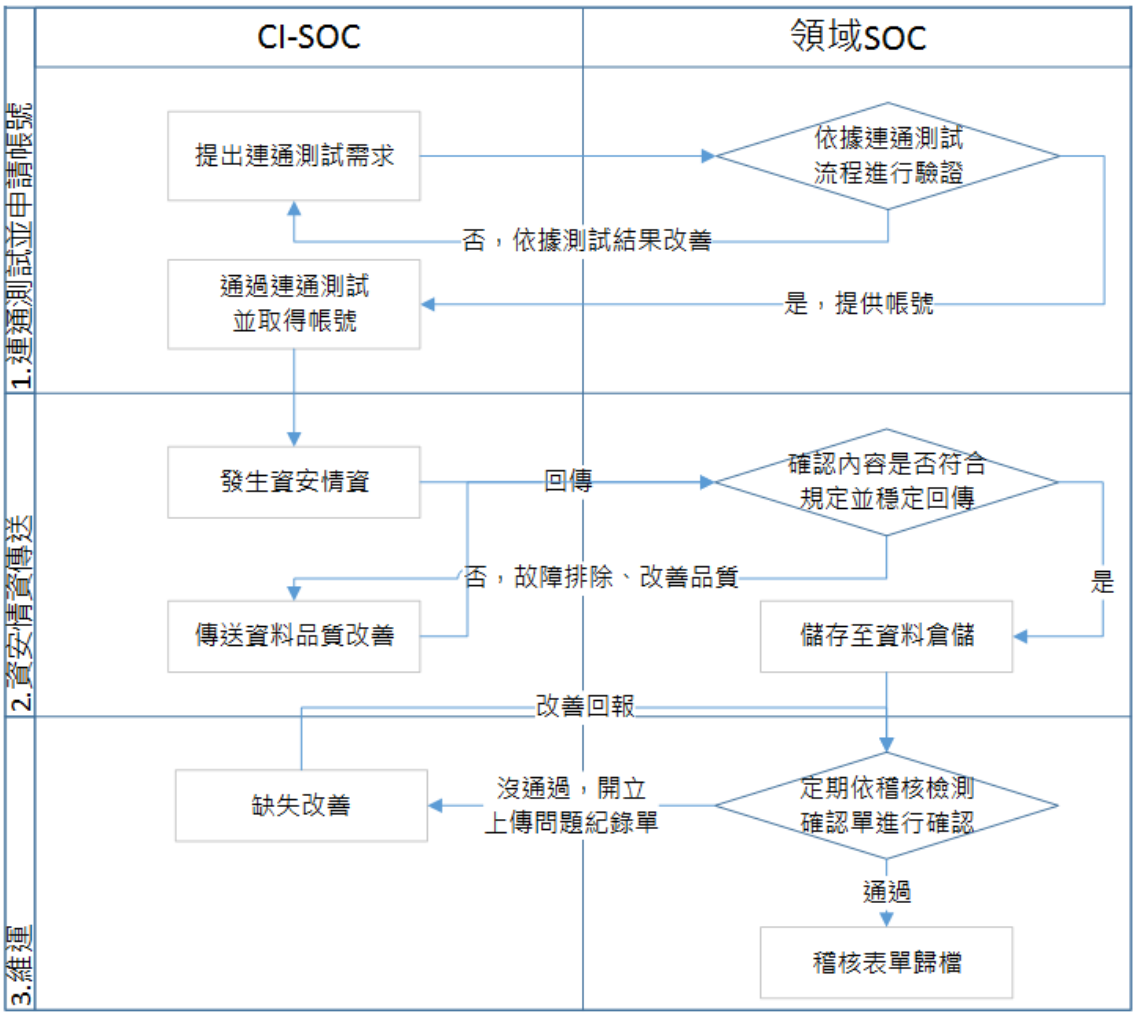
資料來源：技服中心整理

圖7　跨層級 SOC 運作流程示意

領域 SOC 監看說明如下所述：

●領域 SOC 監看 CI-SOC 資安情資運作流程

CI-SOC 應回傳事件紀錄資料予所屬領域 SOC，確認資安事件資料成功匯入平台之資料倉儲中，由領域 SOC 周期性進行資料稽核檢測，確保資料一致性，領域 SOC 監看 CI-SOC 資安情資運作流程詳見圖 8，各流程說明如下：



資料來源：技服中心整理

圖8　領域 SOC 監看 CI-SOC 資安情資運作流程

– 連通測試並申請帳號

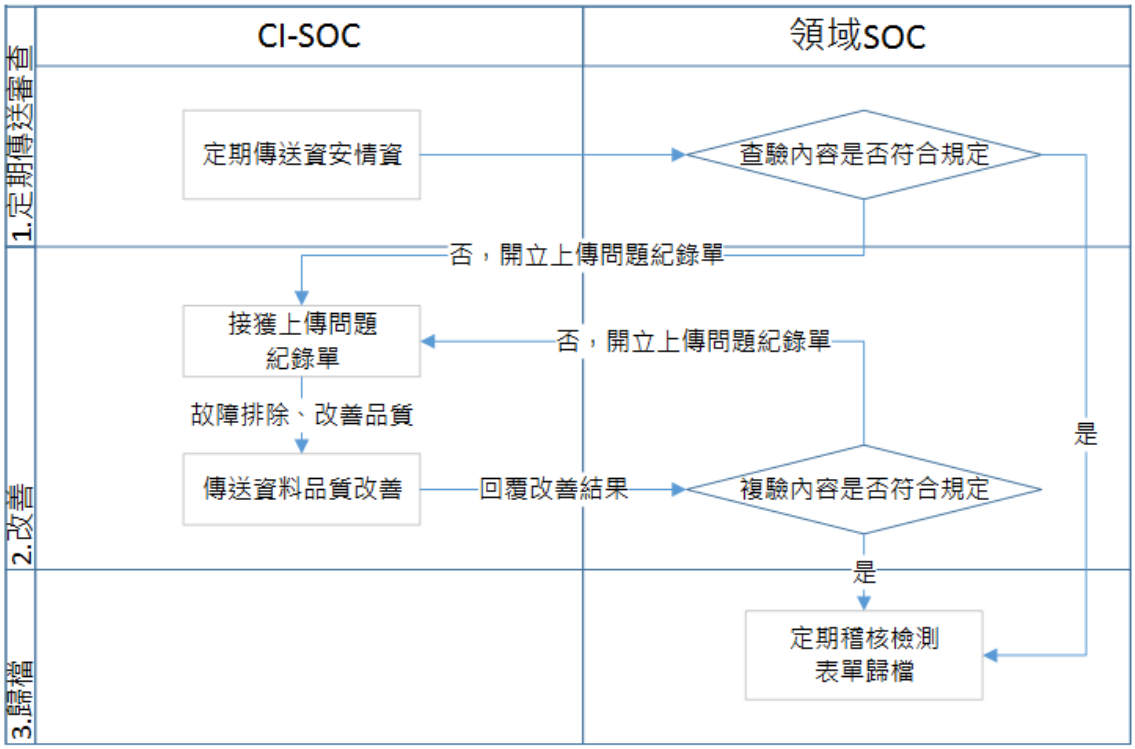
此階段詳見圖 8，CI-SOC 需依據所屬上級領域 SOC 規範先進行相容性檢測，提送資安情資內容，由領域 SOC 查驗內容是否符合規定，符合規定後才可申請帳號，進行資料連通測試。連通測試 3 個月後，領域 SOC 應提供測試報告予 CI-SOC，並應就缺失部分限期改善。

– 資安情資傳送

只要發生資安情資，CI-SOC 需依據規定回傳至所屬上級領域 SOC，由領域 SOC 監看彙整，確認內容是否符合規定並穩定回傳，有問題 CI-SOC 應即進行障礙排除，品質改善，最後儲存至資料倉儲中。

●領域 SOC 維運管理

領域 SOC 除了對 CI-SOC 提出連通測試時進行審查和改善建議外，應定期進行查核作業，每月針對監看的資安情資進行彙整，依定期稽核檢測步驟確認單進行上傳資料確認，逐項測試驗證是否符合作業要求，未符合者，領域 SOC 應開立上傳問題紀錄單，限期 CI-SOC 改善，審查與改善程序詳見圖 9。

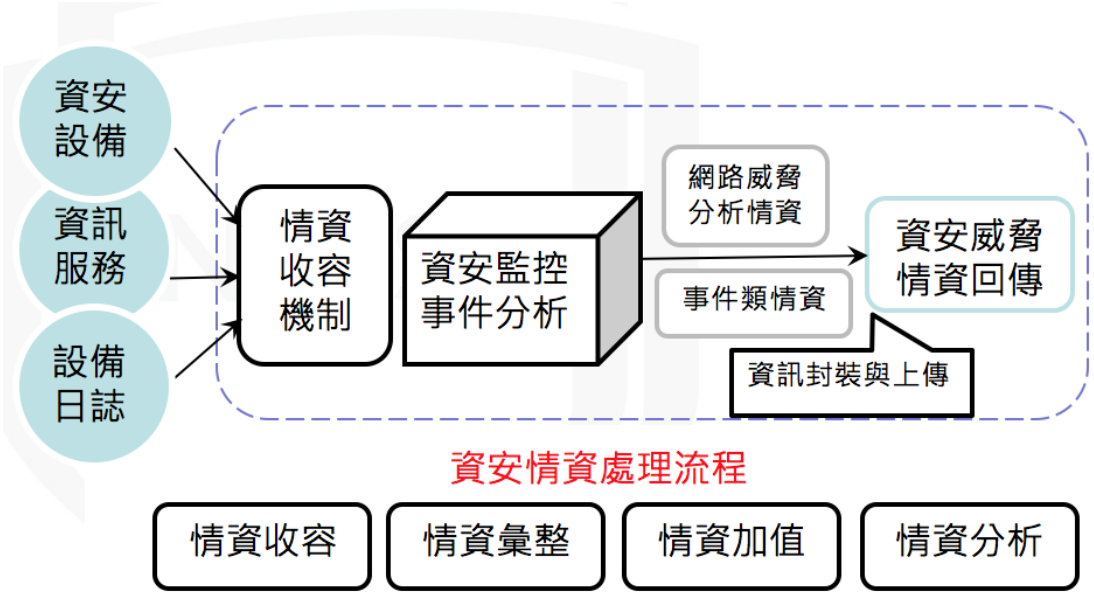


資料來源：技服中心整理

圖9　領域 SOC 監看資料查驗流程圖

●領域 SOC 情資處理流程

領域 SOC 事件收容處理流程分為情資收容、情資彙整、情資加值及情資分析，流程示意詳見圖 10，並對各流程進行說明。



資料來源：技服中心整理

圖10 領域 SOC 情資處理流程

情資收容部分，由各 CI-SOC 固定回傳監看事件情資予領域 SOC 建置之資訊收容機制情資彙整部分，回傳之所有事件情資，包含資安設備類、資安服務與重要主機之服務日誌，依領域 SOC 內部情資規範進行正規劃與彙整情資加值部分，針對內部與外部之相關資安威脅情蒐資訊與彙整之情資進行關聯與加值，提供分析使用情資分析部分，領域 SOC 可針對領域內之資安威脅進行綜整分析，並產製相關聯防情資，將領域內綜整情資與聯防資訊回傳送至 N-SOC。。

●N-SOC 情資介接

– 領域 SOC 層級向上互動

領域 SOC 應將監看情資回傳至 N-SOC，以利 N-SOC 掌握各領域整體資安現況及趨勢。

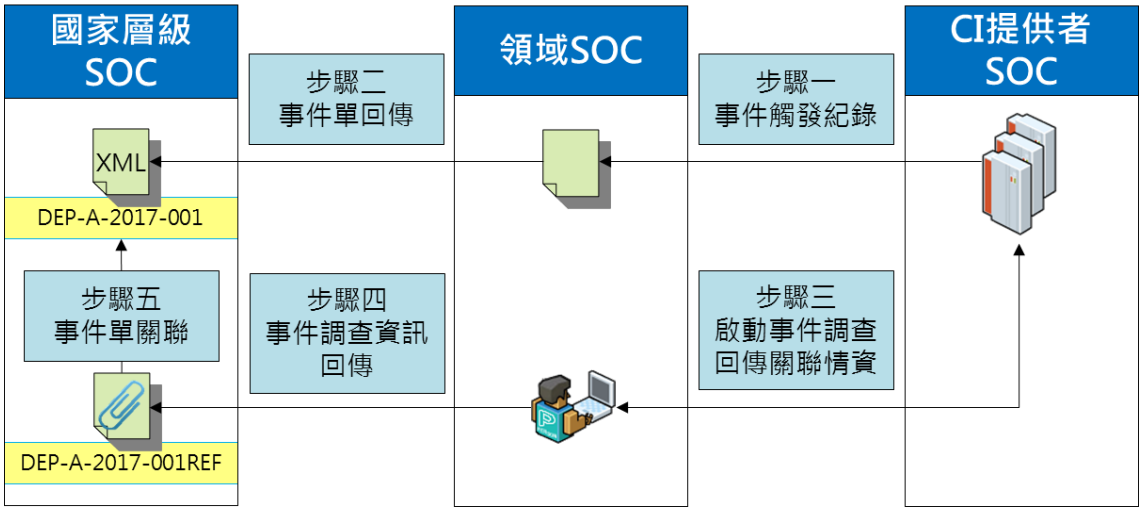
– 領域 SOC 層級向下互動

領域 SOC 應彙整與分析情資後分享予 CI-SOC 及協助 CI-SOC 之事故處理。

3.2.3. 應用情境

●領域 SOC 事件情資回傳與事件調查情資回饋

領域 SOC 固定收容轄下 CI-SOC 之事件觸發情資，彙整後依據 N-SOC 制定情資規範回傳給 N-SOC，後續啟動事件調查深入了解事件觸發根因與蒐集相關事件情資，並回傳事件關聯情資予 N-SOC，此應用情境處理流程分為 5 步驟，應用情境詳見圖 11，並說明如下。



資料來源：技服中心整理

圖11 資安威脅情資應用情境示意

– 步驟一：領域 SOC 接收轄下 CI-SOC 之觸發情資

– 步驟二：彙整 CI-SOC 事件觸發情資並依規範將事件單回傳 N-SOC

– 步驟三：領域 SOC 啟動事件調查，蒐集事件關聯情資並分析事件

– 步驟四：領域 SOC 回傳事件調查關聯情資

– 步驟五：N-SOC 整合事件單與事件關聯情資

領域 SOC 調查觸發事件所蒐集的情資可能包含中繼站黑名單 IP、惡意網路連結、惡意程式/檔案、OpenIOC 規則、資安漏洞/弱點情資及相關郵件資訊等，後續領域 SOC 需彙整相關情資以 STIX 封裝回傳給 N-SOC 進行事件單關聯彙整，STIX 官方網站包含相關資安情資範例，僅取部分情資類型列表供參考，詳見表 6。

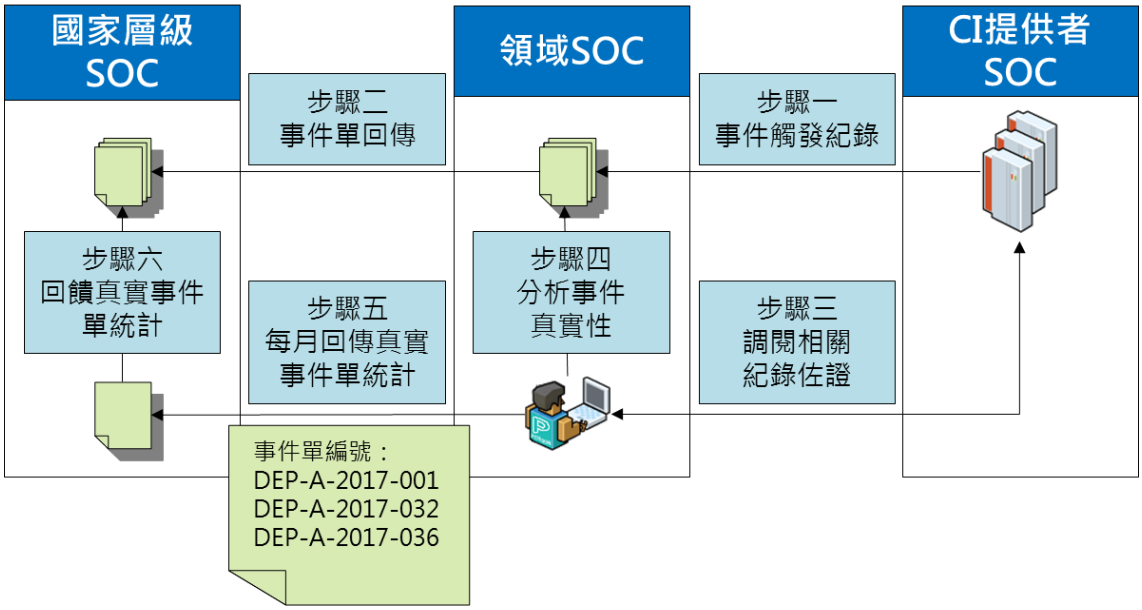
表6 節錄 STIX 官方情資範本

項次	STIX 官方範本名稱	說明
1	Command and Control IP List	C2 黑名單情資
2	Indicator for Malicious URL	惡意網路連結情資
3	Malware Indicator for File Hash	惡意程式/檔案情資
4	OpenIOC Test Mechanism	OpenIOC 情資
5	Identifying a Threat Actor Profile	駭客資訊情資
6	Incident Essentials - Who, What, When	威脅事件描述
7	CVE in an Exploit Target	資安漏洞/弱點情資
8	Assets Affected in an Incident	資安事件影響資產情資
9	Kill Chains in STIX	網際狙殺鍊階段情資
10	Malicious E-mail Indicator With Attachment	惡意電子郵件附件情資

資料來源：技服中心整理

●每月事件調查真實事件情資回饋

由於 SOC 資訊回傳機制為收取領域內 CI 設備偵測之事件，彙整情資後回傳予 N-SOC，而經二線分析人員驗證與調查後，未造成實際資安風險將分類至誤判事件。領域 SOC 每月固定回饋當月無造成真正資安威脅事件統計數據，以利 N-SOC 進行事件情資過濾與分析，此應用情境詳見圖 12，並說明如下。



資料來源：技服中心整理

圖12 每月事件調查真實事件情資回饋示意

– 步驟一：領域 SOC 接收轄下 CI-SOC 之觸發情資

– 步驟二：彙整 CI-SOC 事件觸發情資並依規範將事件單回傳 N-SOC

– 步驟三：領域 SOC 啟動事件調查，蒐集事件關聯情資

– 步驟四：領域 SOC 啟動事件調查，分析事件真實性

– 步驟五：領域 SOC 每月回傳真實事件單統計資訊

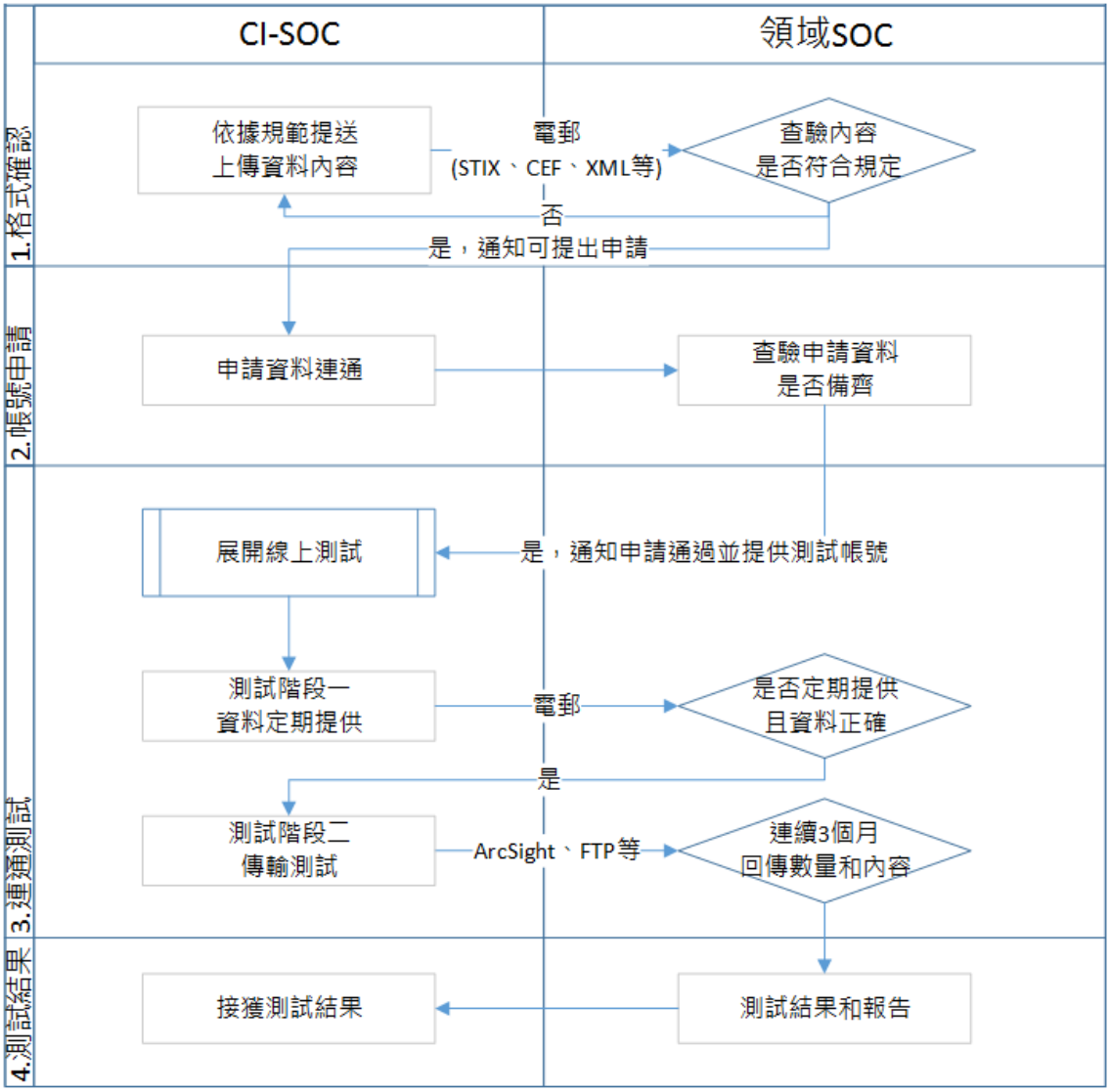
– 步驟六：N-SOC 內部進行真實事件單清整

3.3.查核階段

3.3.1. 檢視/測試

●SOC 連通測試

領域 SOC 監看 CI-SOC 資安情資前，需與 CI-SOC 進行資料連通測試，確認回傳的資安情資格式符合規範，穩定且正確傳送，CI-SOC 與領域 SOC 於連通測試的流程詳見圖 13。



資料來源：技服中心整理

圖13 領域 SOC 連通測試流程圖

●領域 SOC 資訊回傳流程測試

領域 SOC 資訊回傳流程主要確認監看防護資訊回傳能力及確認運作狀況，詳見表 7。

－監看防護資訊回傳

領域 SOC 確認防護資訊回傳概況，包含資訊收容與回傳能力、資訊回

傳格式及資訊回傳即時性。

– 確認運行概況

領域 SOC 維運查核項目，包含定期/不定期檢視事件收容數量統計與事件處理時間。

表7　領域 SOC 資訊回傳流程測試項目

查核目的	驗證項目	統計區間	執行情形
監看防護資訊回傳	確認資訊收容與回傳能力	季/年	
	資訊回傳格式	季/年	
	資訊回傳即時性	季/年	
確認運行概況	定期/不定期檢視事件收容數量統計	季/年	
	定期/不定期檢視事件處理時間	季/年	

資料來源：技服中心整理

3.3.2. 演練

●CI 領域層級收容機制運作演練

CI 領域層級收容機制運作演練主要目標為確認監看權責與涵蓋範圍，並針對落實程度進行確認，相關項目整理詳見表 8。

表8　領域 SOC 收容機制運作演練項目

查核目的	執行方式範例
確認監看權責與涵蓋範圍	▪確認收容的範圍與防護能力 ▪收容對象清單更新(權責範圍涵蓋確認) ▪收容設備類型與涵蓋範圍重新檢視(資訊涵蓋範圍確認)
確認落實情形	▪N-SOC 資訊介接執行效率 ▪事件類之必要資訊回傳能力 ▪情資類之產製與分享能力評估 ▪SOC 權責單位執行效率 ▪事件處理能力 ▪跨單位綜整威脅與應變能力分析 ▪事件誤判與機制調教能力

資料來源：技服中心整理

3.4.改善階段

3.4.1. 改善計畫

由於資安威脅手法樣態眾多，新型態資訊服務發展蓬勃，故針對新型態之資訊服務所衍生之資安議題,領域 SOC 可以專案任務編組與常態會議形式,針對衍生之新型態資安威脅進行手法分析、風險評估與防護策略訂定，如金融區塊鏈(Block Chain)與物聯網(Internet of Things, IoT)等議題，確保相關監看機制、綜整分析能量規劃、聯防架構調整及應變機制能回饋至現有流程，以達有效運作與持續改善之目的。

3.4.2. 評估衡量

●SOC 機制管理執行評估

組織內部定期/不定期管理會議，以確認組織運行方向，是否符合組織願景與目標。

●領域監看與分析能量能量評估

組織內部定期/不定期管理會議，以評估 SOC 監看與分析能量，是否達到領域資安聯防之成效。

●定期追蹤機制

指派特定人員定期追蹤改善項目，並落實回報權責主管。

4. 結論

本指引主要針對領域內 SOC 監看機制之建立過程中，各領域主管機關與 CI-SOC 之角色與對應之權責進行說明，並針對建置過程中，規劃階段所需考量之相關項目，包含人力、資源及架構範圍進行說明，並針對建置過程所需建立之相關程序與機制運作檢核提供建議，並提供相關後續檢核與改善建議，作為領域規範與建置領域參考使用，惟仍後續規劃與建置推動上，需考量下列議題：

- 關鍵基礎設施監看機制建置差異性

  各關鍵基礎設施運作架構與防護重點差異極大外，涉及國家、關鍵基礎設施安全政策及相關法規之規定，需針對領域特性規劃與調整監看機制與收容架構，以確保監看防護之涵蓋廣度。

- 領域與 CI- SOC 資訊收容與防護策略

  領域 SOC 初期以收容重要監看資訊為重要目標，並著重於領域內資安聯防情資的分享與偵測防護，重要 CI-SOC 資訊可同時回傳至 N-SOC，以達資安縱深防護聯防機制之成效。

5. 參考文獻

[1]行政院資通安全處(106 年 2 月)。「106 年國家資通安全防護整合服務計畫」需求說明書。未出版。

[2]組織架構(民 105 年 8 月 1 日)。行政院國家資通安全會報。民 106 年 3 月 7 日，取自：https://www.nicst.ey.gov.tw/。

[3]行政院資通安全會報。「政府機關（構）資通安全責任等級分級作業規定」。

[4]行政院資通安全會報。「資訊系統分級與資安防護基準作業規定」。

[5]行政院資通安全會報。「資訊系統風險評鑑參考指引」。

[6]行政院資通安全會報。「安全控制措施參考指引」。

[7]行政院資通安全會報技術服務中心。「SOC 參考指引」。

[8]行政院資通安全會報。「行政院及所屬各機關資訊安全管理規範」。

[9]金融監督管理委員會。「金融監督管理委員會資訊安全政策」。

[10]國家通訊傳播委員會。「電信事業資通安全管理作業要點」。

[11]行政院資通安全會報技術服務中心。「資訊系統委外開發 RFP 資安需求範本」。

[12]US-CERT, Information Sharing Specifications for Cybersecurity (https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity)

6. 附件

附件 1 第一版 9 大模組介紹

附件 2 領域 SOC 事件調查情資回饋 STIX 封裝範例

附件 3 每月事件誤報情資回饋 STIX 封裝範例

附件1 STIX 第一版 9 大模組介紹

STIX 第一版發行的官方白皮書詳細敘述其架構與相關技術，其架構主要可分為 9 大模組，模組之間或模組本身可具有關聯性與上下關係，詳細模組說明如下。

STIX9 大模組說明

項次	模組名稱	模組說明
1	資安威脅觀察資料 (Observables)	敘述資安威脅事件中所觀察到的相關資料，內容可包含資料來源、資料名稱、內容敘述、資料真實性及相關資安威脅事件等
2	資安威脅模式 (Indicator)	敘述資安威脅可能被觀察到的活動模式，內容可包含威脅模式名稱、模式描述、有效時間、攻擊手法、觀察資料及網際狙殺鍊階段(cyber kill chain)等
3	資安威脅事件 (Incident)	敘述資安威脅事件，內容可包含事件名稱、事件描述、事件類型、受害者、影響範圍與影響資產等
4	資安威脅手法 (Tactics, Techniques, and Procedures, TTP)	敘述資安威脅策略、技術與手法，內容可包含資安漏洞、攻擊模式、惡意程式、使用工具、受害者及網際攻擊狙殺鍊階段等
5	資安威脅活動 (Campaign)	敘述資安威脅活動資訊，內容可包含一群駭客、攻擊手法、威脅模式與相關事件，甚至可推演關聯至其他相關資安威脅活動
6	資安威脅者 (Threat Actors)	敘述資安威脅者的特徵與描述資訊，內容可包含相關基本描述、資安威脅活動、威脅手法、情資來源及動機等

項次	模組名稱	模組說明
7	資安威脅目標 (Exploit Target)	敘述被惡意利用的資安漏洞、弱點及設定檔，內容可包含目標名稱、目標描述、資安漏洞、資安弱點、因應措施、處理狀況及相關資安威脅手法等
8	資安威脅防護措施 (Course of Action)	敘述面對資安威脅所做的應變與預防措施，內容可包含防護措施名稱、描述、效用、使用成本、應用範圍及相關防護措施等
9	資安威脅報告(Reports)	綜整各模組資訊而成資安威脅報告，也可處理難以單一套用至其他模組的資安資訊，設計此模組以文字格式彈性封裝資安資訊

資料來源：技服中心整理

附件2 領域 SOC 事件調查情資回饋 STIX 封裝範例

STIX 第一版封裝事件調查情資欄位關聯表與封裝架構詳見圖 1 與圖 2，STIX 封裝架構分為 3 部分，分別利用 STIX Header 表示事件識別碼，方便與回傳之事件情資進行關聯；資安威脅事件(Incident) 表格內含事件 IP 情資；資安威脅手法(TTP)表格內含事件調查情資網路連線位址、惡意程式名稱、惡意程式檔案類型及 SHA256 雜湊值。

STIX Header	
Description	Short description is used for referencing an event with event-id
Short_Description	DEP-A-2017-001REF

Indicator	
ID	example:indicator-bb78de37-3975-4f0f-a8cc-aa247837cab9
Type	IP Watchlist
Observable	
Object	example:Address-96bb7531-234e-475a-a0ef-87202790448c
Properties	
Address_Value	199.180.102.68
idref	example:ttp-da60e709-38d8-4d22-a561-bdc6dd49b611

TTP	
ID	example:ttp-da60e709-38d8-4d22-a561-bdc6dd49b611
Title	C2 Behavior
Resources	
Infrastructure	
Type	C2 Behavior
Observable	
Properties	
Value	www.aaa.com
Observable	
Properties	
Value	www.bbb.com
Observable	
Properties	
File_Name	aaa.exe
File_Extension	.exe
Hashes	
File_Extension	SHA256
Simple_Hash_Value	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

資料來源：技服中心整理

圖1　STIX 封裝中繼站黑名單觸發事件調查情資

```
<stix:STIX_Package
        xmlns:stix="http://stix.mitre.org/stix-1"
        xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
        xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2"
        xmlns:ttp="http://stix.mitre.org/TTP-1"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
        xmlns:cybox="http://cybox.mitre.org/cybox-2"
        xmlns:indicator="http://stix.mitre.org/Indicator-2"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:stixCommon="http://stix.mitre.org/common-1"
        xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
        xmlns:example="http://example.com"
        xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
        xmlns:xlink="http://www.w3.org/1999/xlink"
          id="example:Package-c1141faf-3caf-45c2-97c9-da0ed487f1d4" version="1.2">
    <stix:STIX_Header>
        <stix:Description>Short description is used for referencing an event with event-id</stix:Description>
        <stix:Short_Description>DEP-A-2017-001REF</stix:Short_Description>
    </stix:STIX_Header>
    <stix:Indicators>
```

```
        <stix:Indicator id="example:indicator-bb78de37-3975-4f0f-a8cc-aa247837cab9"
timestamp="2017-02-21T05:57:57.052682+00:00" xsi:type='indicator:IndicatorType'>
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</indicator:Type>
            <indicator:Observable id="example:Observable-f005c749-7a7c-4bf0-8d5b-2049b12a215d">
                <cybox:Object id="example:Address-96bb7531-234e-475a-a0ef-87202790448c">
                    <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
                        <AddressObj:Address_Value condition="Equals">199.180.102.68</AddressObj:Address_Value>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
            <indicator:Indicated_TTP>
                <stixCommon:TTP idref="example:ttp-da60e709-38d8-4d22-a561-bdc6dd49b611" xsi:type='ttp:TTPType'/>
            </indicator:Indicated_TTP>
        </stix:Indicator>
    </stix:Indicators>
    <stix:TTPs>
        <stix:TTP id="example:ttp-da60e709-38d8-4d22-a561-bdc6dd49b611" timestamp="2017-02-21T05:57:57.052289+00:00"
xsi:type='ttp:TTPType'>
            <ttp:Title>C2 Behavior</ttp:Title>
            <ttp:Resources>
                <ttp:Infrastructure>
                    <ttp:Type>C2 Behavior</ttp:Type>
```

```
                    <ttp:Observable_Characterization cybox_major_version="2" cybox_minor_version="1"
cybox_update_version="0">
                        <cybox:Observable id="example:Observable-9ac76a27-9e6d-40b8-9e0e-57f14777561c">
                            <cybox:Object id="example:URI-05c8d576-9750-4f4d-b063-ae9d4ad640ea">
                                <cybox:Properties xsi:type="URIObj:URIObjectType" type="Domain Name">
                                    <URIObj:Value>www.aaa.com</URIObj:Value>
                                </cybox:Properties>
                            </cybox:Object>
                        </cybox:Observable>
                        <cybox:Observable id="example:Observable-fb5d7dab-8a76-4f15-96fa-dea86276c067">
                            <cybox:Object id="example:URI-10576493-b170-4eb5-8d99-b18078f21352">
                                <cybox:Properties xsi:type="URIObj:URIObjectType" type="Domain Name">
                                    <URIObj:Value>www.bbb.com</URIObj:Value>
                                </cybox:Properties>
                            </cybox:Object>
                        </cybox:Observable>
                        <cybox:Observable id="example:Observable-8e6a6214-b50f-4629-873d-3872f2200318">
                            <cybox:Object id="example:File-0e8861de-1c22-47ee-a29e-cf3c34164fa0">
                                <cybox:Properties xsi:type="FileObj:FileObjectType">
                                    <FileObj:File_Name>aaa.exe</FileObj:File_Name>
                                    <FileObj:File_Extension>.exe</FileObj:File_Extension>
                                    <FileObj:Hashes>
                                        <cyboxCommon:Hash>
```

```
                                        <cyboxCommon:Type condition="Equals"
xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>
                                        <cyboxCommon:Simple_Hash_Value
condition="Equals">e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855</cyboxCommon:Simple_Hash_Value>
                                    </cyboxCommon:Hash>
                                </FileObj:Hashes>
                            </cybox:Properties>
                        </cybox:Object>
                    </cybox:Observable>
                </ttp:Observable_Characterization>
            </ttp:Infrastructure>
        </ttp:Resources>
    </stix:TTP>
</stix:TTPs>
</stix:STIX_Package>
```

圖2　領域 SOC 事件調查情資回饋 STIX 封裝內容

附件3 每月事件誤報情資回饋 STIX 封裝範例

以下提供 STIX 第一版封裝事件誤判情資欄位關聯表與封裝架構詳見圖 1 與圖 2，STIX 封裝架構分為二部分，STIX Header 敘述該月所有事件情資數量以及誤報情資數量；資安威脅觀察資料(Observables)表示誤報事件情資之事件識別碼，便於 N-SOC 進行事件關聯。

STIX Header	
Title	January false alarm events report
Package_Intent	100 events trigger in January
Description	This is a report pointing out which 3 events are false alarms during January

Observables	
Observable	
Title	REF is in Description
Description	DEP-A-2017-001
Observable	
Title	REF is in Description
Description	DEP-A-2017-032
Observable	
Title	REF is in Description
Description	DEP-A-2017-036

資料來源：技服中心整理

圖1 STIX 封裝每月事件誤報情資回饋

```
<stix:STIX_Package
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:stix="http://stix.mitre.org/stix-1"
        xmlns:cybox="http://cybox.mitre.org/cybox-2"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:stixCommon="http://stix.mitre.org/common-1"
        xmlns:example="http://example.com"
        xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
        xmlns:xlink="http://www.w3.org/1999/xlink"
         id="example:Package-f6654d2f-dc31-40d5-ad19-599c78ab8f42" version="1.2">
    <stix:STIX_Header>
        <stix:Title>January false alarm events report</stix:Title>
        <stix:Package_Intent>100 events trigger in January</stix:Package_Intent>
        <stix:Description>This is a report pointing out which 3 events are false alarms during January</stix:Description>
    </stix:STIX_Header>
    <stix:Observables cybox_major_version="2" cybox_minor_version="1" cybox_update_version="0">
        <cybox:Observable id="example:Observable-93d1fb02-5fd3-4cdb-bea8-0008b8013496">
            <cybox:Title>REF is in Description</cybox:Title>
            <cybox:Description>DEP-A-2017-001</cybox:Description>
        </cybox:Observable>
        <cybox:Observable id="example:Observable-91bbc10b-44a2-4980-a77e-9095e994339b">
            <cybox:Title>REF is in Description</cybox:Title>
```

```
            <cybox:Description>DEP-A-2017-032</cybox:Description>
        </cybox:Observable>
        <cybox:Observable id="example:Observable-3c8889ef-2e3b-4cba-ba4d-cf3cd6364cd4">
            <cybox:Title>REF is in Description</cybox:Title>
            <cybox:Description>DEP-A-2017-036</cybox:Description>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

圖2　每月事件誤報情資回饋 STIX 封裝內容