國立臺灣大學管理學院碩士在職專班資訊管理組

碩士論文

Executive MBA Program in Information Management

College of Management

National Taiwan University

Master Thesis

企業資訊安全營運管理之績效評估

IT Security Operations Management: Performance Evaluation

黃瓊瑩

Huang Chiung-Ying

指導教授：孫雅麗 博士

Advisor: Yeali S. SUN, Ph.D.

中華民國 100 年 1 月

January, 2011

國立臺灣大學碩士學位論文
口試委員會審定書

企業資訊安全營運管理之績效評估

IT Security Operations Management:

Performance Evaluation

本論文係黃瓊瑩君（學號 P96747011）在國立臺灣大學管理學院碩士在職專班資訊管理組完成之碩士學位論文，於民國 100 年 1 月 18 日承下列考試委員審查通過及口試及格，特此證明

口試委員：_____（指導教授）

_____

_____

_____

_____

_____

系主任、所長 _____

誌　謝

從事資訊安全領域的工作，已經快 20 年了，近年專注於資訊安全事件即時偵測與防禦工作，透過 SOC (Secuirty Operations Center) 全年無休進行 7 x 24 監控服務，及早發現資訊安全風險並處理資訊安全問題。在實際工作中，企業經營者均體認資訊安全對現代企業 IT 營運的重要性，但對於資訊安全防護上的投資，是否獲得合理的效益，卻沒有一個客觀評估的方法。

本論文整理實務上能客觀評估資訊安全績效的方法，加以分類並設計可行績效指標，雖然工作上累積的資料非常多，但要有系統整理才發現並不容易，尤其只能利用公餘的時間進行，進度非常緩慢。感謝指導老師孫教授的指導，老師鼓勵除了技術內容以外，內容盡量要有「高階管理者思維」，可作為管理者評估效益與決策的最佳指標。要達到此目的，最直接具體的方法是將評估方式轉換為 $ (dollar sign)，可有效回應經營階層關心的問題。

本論文中將實際案例換算成實際的財物損失，對我個人是突破也是最大收穫。嘗試用財務報表的數字與相關法律來解釋投資效益的問題，是指導老師與台大 EMBA 課程帶給我的成長，很高興可以踏出第一步，並感謝恩師孫教授的悉心指導與鼓勵。

黃瓊瑩　謹識

于台大管理學院

中華民國一百年一月

中文摘要

企業經營者均體認資訊安全對企業 IT 營運的重要性，但投資在資訊安全防護上的資源，是否得到合理效益，如何評估資訊安全營運管理的績效？由於資訊安全涉及複雜的技術與管理問題，且攻擊手法與變化甚為快速，每一個環節都有可能衍生風險，過去沒有問題的 IT 環境，不保證現在或未來仍能固若金湯、安全無虞。企業除了自行聘用資訊安全專長的員工負責企業本身的安全，也可以選擇委外專業的資訊安全服務廠商，提供企業資訊安全服務。

本論文探討資訊安全營運管理的技術架構，並設計「技術管理」與「營運管理」的績效評估指標，用來衡量資訊安全營運管理表現的良窳。這些指標可以當作日常營運管理的工具，隨時了解整體營運管理的表現，及時採取各種矯正或改善措施，控制資訊安全風險。本論文進一步依照所設計績效評估指標，就真實發生的個案，計算實際金錢損失以衡量投資效益。

各項績效評估指標，依照 **S**pecific, **M**easureable, **A**ttainable, **R**epeatable, **T**ime-dependent 的 S.M.A.R.T 原則設計，內容均為量化的單位如小時、次數、百分比等，避免個人主觀 (Subjective) 認定不同，而有不同判斷。各項指標可以合理的代價（時間、金錢、人力）有效取得，具備可操作性。有了適當的績效評估指標，本論文運用真實個案，嘗試回答以下管理者關心的問題。

- 投入的資訊安全成本，是否獲得「合理效益」 ？
- 要「投資多少」資源，才能達到安全的程度？
- 資訊安全的狀態「比」過去好嗎？

關鍵字：資訊安全防護管理中心、績效評估指標、SMART 原則

THESIS ABSTRACT

SENIOR PUBLIC ADMINISTRATION
COLLEGE OF MANAGEMENT
NATIONAL TAIWAN UNIVERSITY

NAME： Chiung-ying, HUANG **MONTH/YEAR：JANUARY, 2011**

ADVISER：Yeali S. SUN, Ph.D.

TITLE：IT Security Operations Management: Performance Evaluation

Information Security is a pivotal component in modern business activities without questions. Enterprise should exercise due care to perform the ongoing maintenance necessary to keep IT systems in proper working order, or to abide by what is commonly expected in a situation. IT head is responsible to implement countermeasures to provide protection from those threats. By developing and implementing security policies, procedures, and standards, shows that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees from possible threats. It is especially important if the due care situation exists because of a contract, regulation, or law.

However, there's been a lack of well-defined performance evaluations indexes to understand the return of investment regarding information security operations. The thesis designs "technical management" and "operational management" performance indexes to help enterprise top management level to evlautie the return regarding the money paid for security operations. Moreover, real security incident cases are discussed and the financial losses are calculated as well to response the concerns from the top management viewpoints:

- Am I spending the right amount of money?
- How much should I pay for information security?
- Am I better off than I was this time last year?

The indexes designed in the thesis are evaluated to a number, percentage or time elapsed. They are contextually **s**pecific, **m**easureable, **a**ttainable (cheap to gather) **r**epeatable and **t**ime-dependent. In addition, all of the indexed are clear, unambiguous and can be consistently measured without subjective distortion.

Keywords：Security Operations Center, Key Performance Indicator, Performance Evaluation Indexes, SMART Criteria

目　錄

圖目錄

表目錄

方程式目錄

第一章　緒　論

第一節、研究背景與動機

電腦運用普及與網際網路的蓬勃發展，帶給企業急速而巨大的衝擊，也改變了現代人們的生活模式。隨著數位經濟時代來臨，e 化是企業跨足國際市場的趨勢，企業為了符合全球化商業脈動，營運資訊的數位化，更是不可缺少的競爭力。早期電腦系統多為封閉式環境，用途多為專屬功能（Proprietary System）其資訊安全顧慮相對較低，然而隨著資訊便利與網際網路多元化的應用，各種資訊安全問題層出不窮，資訊安全變成令人非常擔憂的問題。對資訊化依賴愈高，一旦電腦系統或資料檔案發生資訊安全問題，往往造成營運中斷、企業機密外洩、顧客個資外流、衍生法律訴訟等難以彌補的損失。因此沒有資訊安全，就等於沒有資訊化，其重要性可想而知。

企業或政府機關，為了解決資訊安全的問題，編列預算購買各種資訊安全設備，聘請專業人員管理、維護、處理各種資訊安全事件，投入的資源非常龐大。依據主計處統計，2008 年我國投入資安部分的經費逾 71 億元，占資訊總投資的 5.20％，較 2007 年增加逾 2 億元[13]。

但如何看待或衡量資訊安全投資的效益呢？在真實的世界裡，企業高階管理者（CEO）與資訊安全負責人（CSO）往往以不同構面來評估資訊安全投資的績效，最明顯的差異是溝通語言不同。CSO 關心的是威脅、風險、控制等技術內容，確認各種安全風險是否有效控制；CEO 關心的是成本、生產力與投資效益（ROI）。同一個企業不同角色人員，對於公司目標雖然無明顯差異，僅就資訊安全效益的衡量，就很難有共通、統一與客觀的衡量方法，遑論不同企業、不同領域如何評估投資是否達到預期效益，企業高階管理階層需要了解資訊安全營運管理問題有：

- 投入的資訊安全成本，是否獲得「合理效益」 ？
- 要「投資多少」資源，才能達到安全的程度？
- 資訊安全的狀態「比」過去好嗎？

本論文根據實務經驗，設計評估企業資訊安全營運管理績效的方法，客觀的計算、衡量管理績效，並回答上述的管理問題。

第二節、研究目的

資訊安全績效評估須要有方法衡量，沒有衡量指標，就無法有效的管理 (You can't manage what you can't measure)，本論文嘗試就技術面、營運面，設計資訊安全績效評估架構(Framework)，作為企業衡量資訊安全績效良窳的依據。績效評估的項目，搭配適當的測量指標(Security Metrics)，以量化的方式來呈現各評估項目表現，並具備「S.M.A.R.T.」原則。S.M.A.R.T.原則是進行成員組織、目標制定和控制，達到更好工作績效的方法，由管理學大師彼得·杜拉克於 1954 年首先提出。在 1981 年 12 月《管理評論》(Management Review)，是目前最早與更完整的 S.M.A.R.T.原則探討文獻[5]，廣泛應用在企業界。

S.M.A.R.T.原則中的五個字母分別對應了五個英文單詞：Specific（明確性）、Measurable（可衡量性）、Attainable（可達成性）、Relevant（相關性）和 Time-bound（時限性）。

- **S**pecific（Contextually Specific）- 與決策者所關心的事項具體與明確相關，並可據以採取對應的行動或做成決策。
- **M**easurable（Number, Percentage, Unit of Measure） - 可測量的量化內容，並有對應量測單位如小時、次數、百分比等。
- **A**ttainable（Gather under reasonable costs）-蒐集原始資料經過整理、分析後，可以依照計算出來的結果滿足所關心的問題，具備實務上的可操作性。Attainable 另一層的意思，是指在合理的代價（時間、金錢、人力）下可有效取得。
- **R**epeatable（Consistently Measured）- 可穩定、長期蒐集與計算，不同人重複相同步驟，可以得到相同的結果並避免個人主觀 (Subjective) 認定不同，而有不同判斷。
- **T**ime-Dependent（Single-point-in-time view）- 量測的內容是某一時間點的表現，與時間直接相關。

資訊安全測量指標，需要有對應的資訊安全營運管理服務來滿足，此服務包含軟、硬體、人員與流程等。依據企業本身的規模、安全要求與人力等，服務的提供者可以是「企業本身（自建）」、「部分委外（協同維運）」或「完全委外」等不同模式。專責提供資訊安全服務的中心，稱為資訊安全防護管理中心 (SOC –

Security Operation Center)，是以資安監控防護平台為基礎，進行 7x24 資安防護維運，監控異常狀況，處理突發攻擊事件的專責單位。

SOC 收集資安監控日誌資訊：如防火牆、入侵偵測系統、防毒系統等，然後進行事件分析、通報、調查與處理等。當 IT 系統大量導入，成為企業活動命脈時，SOC 資訊安全服務是企業保障資訊安全的方法。不管是「自建」、「協同維運」或「完全委外」，其所需要的安全績效衡量指標應該相同，作為投資效益衡量的依據。

第二章　文獻探討

第一節、COBIT 簡介

COBIT 是美國資訊系統審計與控制協會（ISACA）和 IT 治理委員會（IT Governance Institute - ITGI）於 1992 年草擬，全名為：Control Objectives for Information & related Technology（簡稱 COBIT）[3]，是一系列關於 IT 治理（IT Governance）最佳實務的管理框架（Management Framework）。COBIT 為企業管理、稽核和 IT 人員提供通用的測量、呈現和處理方法，幫助企業使用 IT 技術時，可以有效進行治理與控制，以滿足企業的經營目標（Business Goal）。COBIT 協助使用者認識和瞭解企業資訊系統，以決定系統的安全性，及透過資訊治理來保護企業資訊資產。2007 年最新 4.1 版中，提出 IT 治理開放性框架及相關工具集，協助組織透過控制、度量、標準來管理 IT 資源，提升 IT 價值並透過適當的監控作業，確保各種控制均如預期運作，降低 IT 風險。為了滿足經營目標，COBIT 的主要特性有「聚焦業務」、「流程導向」、「以控制為基礎」、「以度量驅動」，以下逐項說明。

一、聚焦業務 (Business-Focused)

COBIT 架構訴求對象不侷限於 IT、稽核人員或使用者，更重要的還包含了管理指引與業務流程的負責人(Business Process Owner)。為了提供企業滿足經營目標所需之資訊，企業必須投資與管理資訊資源，並透過結構化的流程與服務，確保資訊的交付（圖 1）。

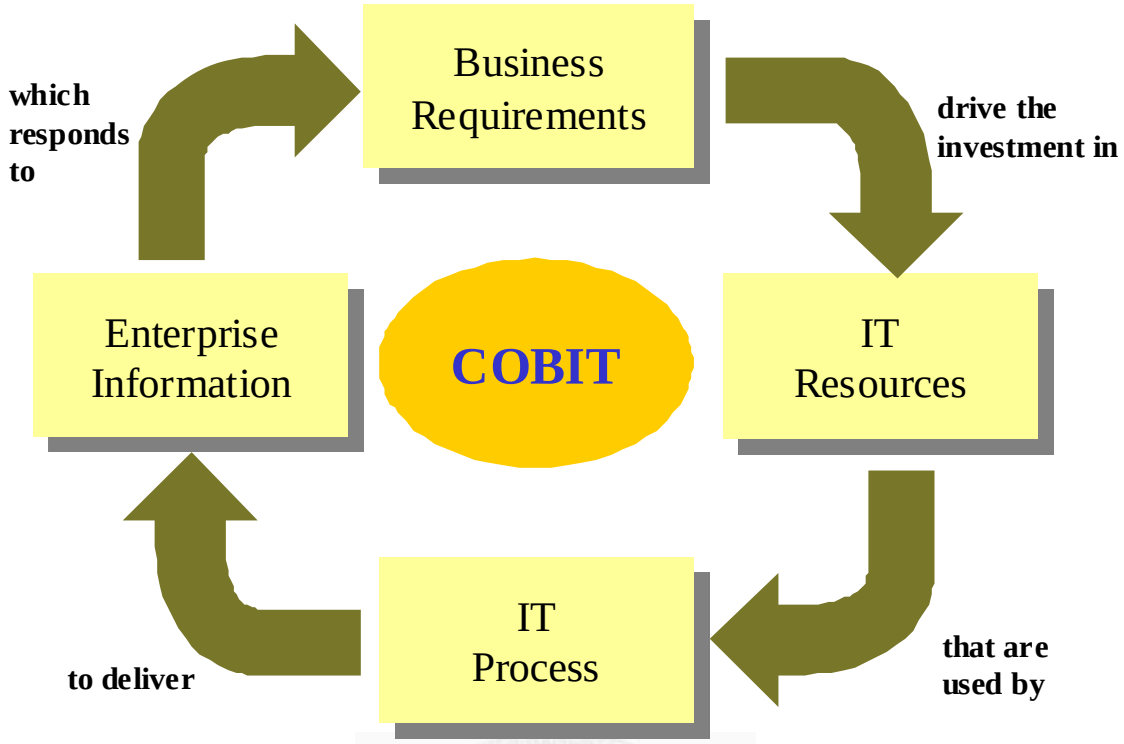


圖 1.基本COBIT結構

管理與控制資訊的提供，是 COBIT 確保與經營目標一致的核心，且要兼顧品質、監督、安全等需求，資訊必須符合七項資訊準則（表 1 ）。

表1 COBIT 資訊準則 (Information Criteria)

準則	內容
有效性（Effectiveness）	一致、適用、及時與正確提供營運活動相關的資訊
效率（Efficiency）	最佳運用資源，以最具生產力與經濟效益提供資訊
機密性（Confidentiality）	保障企業機密，不受未經授權揭露
完整性（Integrity）	符合企業預期的準確與完整內容
可用性（Availability）	確保企業維持穩定不中斷的可用性
遵循性（Compliance）	符合企業與法規之規範
可靠性（Reliability）	提供公司治理與組織運作的資訊

二、 流程導向 (Process-Oriented)

COBIT 過程及監控範圍包含四個部分（表 2 ）。

表2 COBIT 四大領域與說明

領域	說明	管理議題
計畫與組織	用來找出為達成經營目標最	● IT 是否與經營目標一致

Plan and Organize	佳方案的 IT 策略（Strategy/Tactics）與所關心事項，並透過不同的構面計畫、溝通與管理來完成。	● 資源利用是否最佳化 ● 企業成員是否均瞭解 IT 目標 ● IT 風險是否清楚且有效管理 ● IT 品質是否適當滿足企業需求
獲得與建置 Acquire and Implement	透過 IT 策略的瞭解，辨認、發展、獲得 IT 解決方案，並建置與整合到業務流程中。	● 新方案是否滿足經營需求 ● 新方案是否如期、如預算的交付 ● 新系統是否如預期正確運作 ● 異動不會干擾既有業務運作
交付與支援 Deliver and Support	服務交付、安全與不中斷管理、服務支援、設備與資料管理。	● 服務交付是否合乎業務優先次序 ● 成本是否最優化 ● 有生產力與安全的使用 IT 系統 ● 適當的資訊安全保護(C.I.A.)
監控與評估 Monitor and Evaluate	透過常態性的監控與評估控制需求，確保 IT 流程的品質與符合度。	● IT 效能有效監控並提早發現問題 ● 確認內部控制有效性與高效率 ● IT 效能連結經營目標 ● 適當的資訊安全保護(C.I.A.)

三、 控制為基礎 (Control Based)

COBIT 訂定 34 個控制目標，並將 210 個相關工作項目組織起來（圖 3）。

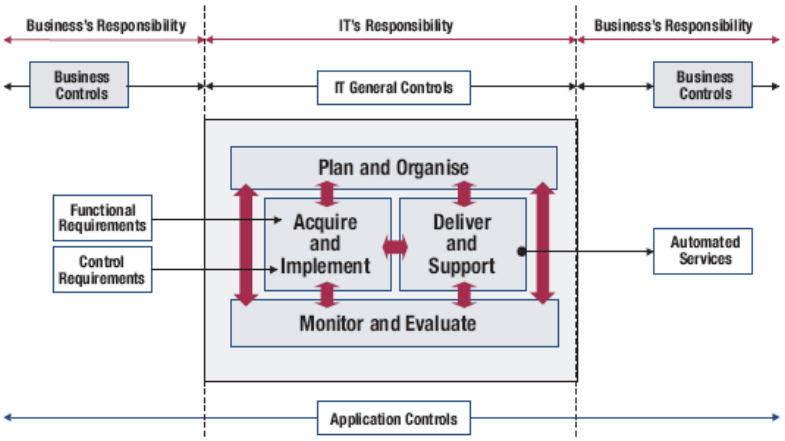


圖 2.COBIT四個領域的關聯

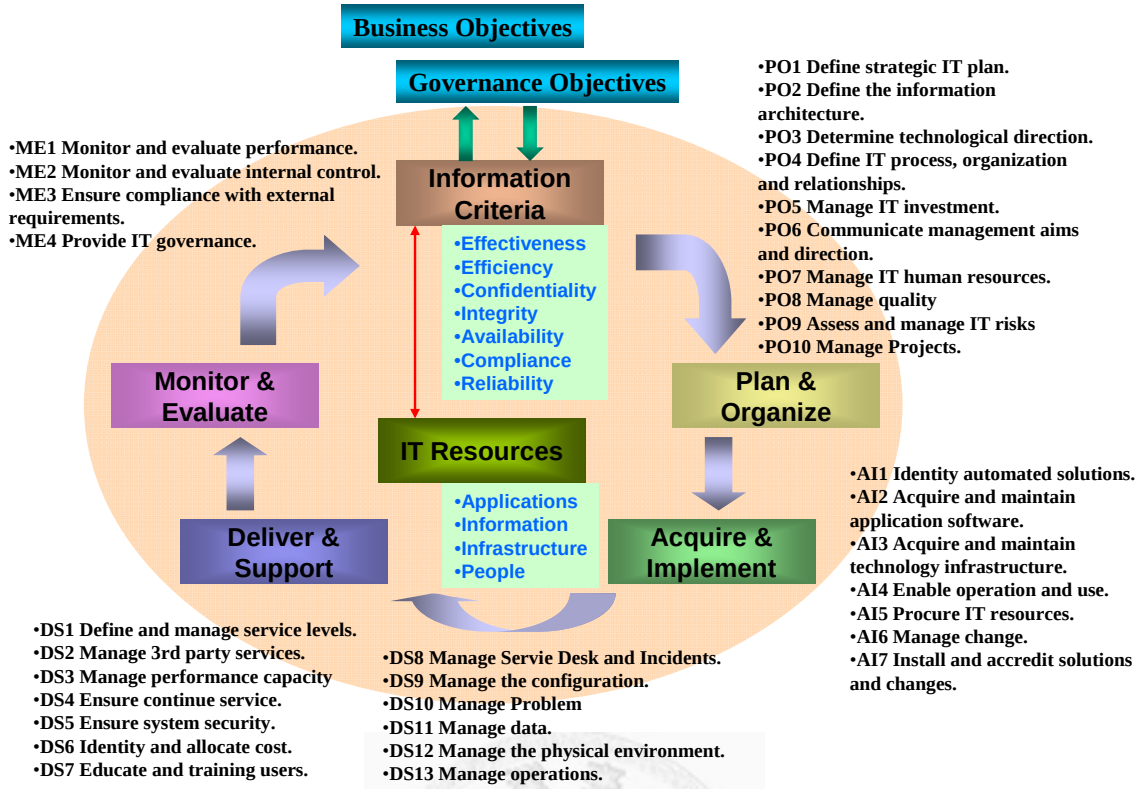


圖 3.COBIT框架

四、以度量驅動 (Measurement-Driven)

經營目標由上而下定義，再決定需要多少 IT 目標來達成；而 IT 目標是由一個或多個作業流程來實現，因此 IT 目標協助定義不同的作業流程目標，作業流程目標會由多個活動來滿足（圖 4）。度量這些目標的有以下兩種類型：

- 成果度量 (outcome measure) – 判斷目標是否達成，一般是在相關結果已經發生之後，也可稱為落後指標（lag indicators）。
- 績效度量 (performance measure) – 度量目標達成的可能性高低，是在結果已經產出之前的度量，也可稱為領先指標（lead indicators）（圖 5）。

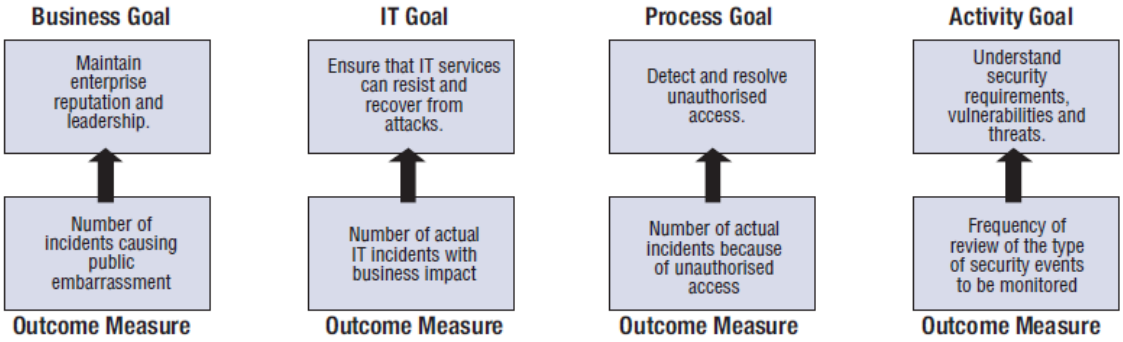


圖 4.目標與成果度量

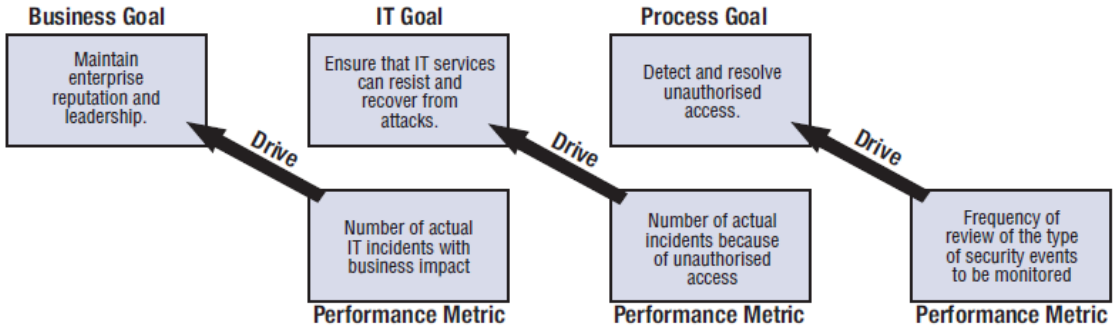


圖 5.績效驅動範例

五、COBIT 與績效評估指標

COBIT 是一個較為完整與廣泛的管理框架，且有流程、控制與度量的概念，對於 SOC 的績效度量，有較多可以參考的地方。但 COBIT 是廣義的 IT Governance 框架，不是單獨針對 IT Security Govarnmance 的管理框架。但是 IT Security Governance 是 IT Governance 是的一部份，有關 IT Governance 所需注意與管理的項目，均可做為 IT Security Governance 的參考。

本論文之績效指標，將比對 COBIT 的控制目標(參考第六章 第二節、與 COBIT 控制目標比較)，檢視本論文設計指標的完整度與涵蓋情況。

第二節、CVSS –共通弱點評分系統

一、 概述

CVSS (Common Vulnerability Scoring System)是由美國國家基礎建設諮詢委員會 (NIAC) 委託製作，並且受到 Cisco、 Symantec 、ISS 和 eBay 等支持。CVSS 與一般專用的評估系統不同，它是使用標準的數學方程式，來判定威脅的嚴重性，列入評估標準的因素，還包括安全弱點能否被遠端利用，或是攻擊者是否需要登入，才能利用此一弱點。為數不少的商業點腦安全業者和非營利組織已經發展出許多可列出系統弱點資料的先進系統工具。

IT 管理必須在許多不同的硬體和軟體平台間識別和評估弱點。他們需要為那些會構成最大風險的弱點定義出優先權和補救。但是，有這麼多次的修復，每次都用不同的方式得到不同的弱點嚴重分數，IT 管理者如何能將這些堆積如山的漏洞數據轉換為可管理的有用資訊？共通弱點評分系統（CVSS 的）是一個開放的框架內，它具有以下優點：

- Standardized Vulnerability Scores:

當一個組織將那些不同軟體和硬體平台的弱點正規化的時候，它可以使用一個單一的弱點管理政策。這一個政策可能類似於一個服務水平協議（SLA），指出一個特別的弱點必須要多快被驗證和補救。

- Open Framework:

“什麼樣的特性讓這個弱點得到這個分數？為什麼會跟昨天公佈的分數不同？”，根據 CVSS，任何人都可以看到個別的特性來推算分數。

- Prioritized Risk:

當環境的分數被計算出來之後，其弱點的分數就代表著這個組織真正的風險。使用者可以瞭解這些弱點之間的重要性。

二、 內容

CVSS 度量由三個度量群組組成：Base, Temporal and Environmental，如（圖 6）。

圖 6.CVSS Metrics Groups

- Base: 代表內在和基本特徵的弱點，是不會隨著時間和用戶環境推移的固定評量。
- Temporal: 代表弱點程度，會隨時間變化，但不會隨著用戶環境有所變化。
- Environmental: 弱點與用戶的環境有關聯且有獨特性。

這種客觀的態度為用戶提供了清晰且直觀的表示方法，使用者根據上述 Temporal 和 Environmental 群組更精確顯示出環境裡獨特的風險。當 base metrics 的值代入後，方程式計算出 0~10 的分數（圖 7）Vector 來解釋每一個弱點的分數。

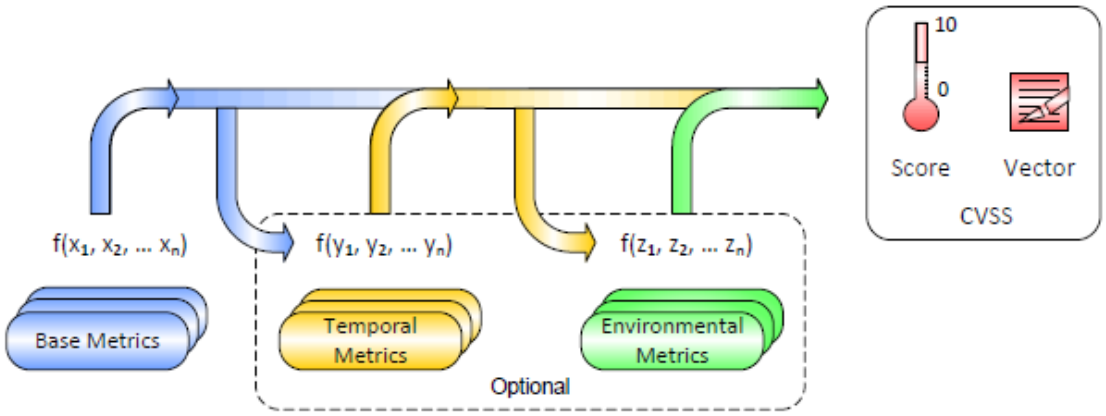


圖 7.CVSS Metrics and Equations

Base score 指派值給 Temporal 和 Environmental Metrics，Temporal 並不是必要的，根據不同目的，Base 通常已經足夠使用。如果需要 Temporal Score，方程式將會把 Temporal Metrics 與 Base Score 產生時間評分(Temporal Score)從 0 到 10。同樣，如果 Environmental Score 是必要的，對環境的方程式將結合 Environmental Metrics 與 Temporal Score 產生環境評分範圍從 0 到 10。

第三節、銀行業資訊安全損失估算方法

有關資訊安全事件，屬於作業風險，本節先說明巴塞爾資本協定對於作業風險的定義，之後再探討我國金管會依據巴塞爾資本協定，規範銀行認列作業風險損失的原則，作為本論文探討銀行個案時，計算財務損失的依據。

一、 巴塞爾資本協定與作業風險

1974 前聯邦德國赫爾斯塔銀行（Herstatt Bank）和美國的富蘭克林國民銀行（Franklin National Bank）倒閉，兩家國際著名銀行倒閉後，銀行業了解國際性銀行監管主體發生問題，衍生了兩個基本監管思維：

- 任何銀行國外機構都不能逃避監管。
- 母國和地主國應共同承擔相應職責。

1988 年 7 月國際清算銀行(Bank for International Settlement, BIS)的巴塞爾銀行監理委員會（Basel Committee on Banking Supervision, BCBS），公佈以信用風險為主的跨國規範，通過了《關於統一國際銀行的資本計算和資本標準的報告》（簡稱《巴塞爾報告》，即 BASEL I）。1996 年巴塞爾銀行監理委員會針對巴塞爾資本協定提出修正案，以期標準化國際上的風險控管制度，提升國際金融服務的風險控管能力。該修正案將市場風險納入資本需求的計算；2001 年 1 月公佈了新巴塞爾資本協定草案第二版即 BASEL II，修正之前的信用風險評估標準，且再加入了作業風險的參數，將三種風險納入銀行資本計提考量，以期規範國際型銀行風險承擔能力，另：

- 2003 年 4 月公佈第三版草案。
- 2004 年 6 月正式定稿公佈新巴賽爾資本協定，並希望在 2006 年年底以前，大多數的國家都能採用此架構。
- 而我國亦於 2007 年開始配合實施。

彙總前述巴賽爾資本協定的發展歷史，新巴賽爾資本協定主要變革在於基本架構的演進。除了現行強調的「最低資本適足率要求」外，增加「監理機關的監理審查」及「市場紀律」，形成三大支柱。同時在計提最低資本適足率要求時，除考慮信用風險與市場風險外，亦增加作業風險的因素。

「作業風險」指的是來自於內部作業、人員及系統的不當或失誤，或因外部事件所造成損失的風險。包含法律風險，但排除策略及信譽風險。作業風險並不

是近來才發生的，資訊系統(IT)、人為因素、詐欺等作業風險事件所引起的損害及不確定性已存在很久，在作業風險這個名稱出現後，這些風險始被重新定位並成為管理決策之重要輔助工具之一。Basel II 的作業風險規範詐欺、流程疏失、營運中斷、人力資源管理、法律債務等風險進行綜合管理。作業風險所需資本計算方式，有基本指標法(Basic Indicator Approach)、標準法(Standardized Approach)及進階衡量法(Advanced Measurement Approaches；AMA)等三種，分述如下：

- 基本指標法

以基本指標法計提作業風險所需資本，係依據金融機構前三年中為正值的營業毛利乘上固定比率 15%，當做任一年的營業毛利為負值或零時，應不列入計算平均值。其中，營業毛利(Gross Income)定義為：淨利息收益加上淨非利息收益，不扣除各項提存、營業費用，支付給委外服務提供者的費用，不計算銀行簿上已實現之有價證券買賣損益，及不計入特殊或異常項目及保險利得等[20]。

- 標準法

本法將銀行的業務分為八項業務別：企業財務規劃(corporate finance)、財務交易與銷售(trading & sales)、消費金融(retail banking)、商業金融(commercial banking)、收付清算(payment & settlement)、代理業務(agency services)、資產管理(asset management)和消費經紀(retail brokerage)。計算各業務別所需資本的方法是用銀行的營業毛利乘以各業務適用的係數(β)，再予以加總。

總資本需求額是每一年度各業務別法定資本的簡單加總後的三年平均值，在任一年中，任一業務別若有負值的資本計提(由於營業毛利為負)，可抵銷掉其他業務別中為正值的資本計提；任一年中所有業務別加總後之資本計提額為負值時，則當年對分子的貢獻值為零。

- 進階衡量法

進階衡量法是指在監理機關審核同意後允許符合品質及量化條件之銀行，依據內部作業風險衡量系統計提作業風險所需資本。銀行於正式採用進階衡量法之前一年，其適足資本必須分別以進階衡量法及原計算方式進行試算。

二、 我國對作業風險損失的認列規範

新巴塞爾資本協定(英文簡稱 Basel II)目的在標準化國際上的風險控管制度，提升國際金融服務的風險控管能力。在此協定中因作業風險所產生的損失，則應該由該期的實際收益依照比例直接計算，而不需考慮風險控制後的變化。我國金管會銀行局，參酌新巴塞爾資本協定的規範，於民國 98 年 7 月 27 日銀局(法)字第 09800303590, 09800303591 號函，要求由銀行公會與聯徵中心共同研商於 98 年 12 月前辦理作業風險外部損失資料庫。另依銀行公會 98 年 8 月 10 日全風字第 0980002071A 號函請本國銀行與農業金庫配合於 98 年年底前進行作業風險資料報送[15][23]。在此函文中規範：

- 作業風險的定義 - 起因於銀行內部作業、人員及系統之不當或失誤，或因外部事件造成銀行損失之風險，包括法律風險，但排除策略風險及信譽風險。
- 損失之認定 - 不以列入損益表為依據，應視是否實際產生支付金額或資產減損為準。
- 金額之估計 - 機會成本不納入考量，且不作風險相關金額分攤，以避免人為判斷影響報送基礎，故金額估算以截至資料填報基準日，直接損失的實際支付金額為準(不扣除回收金額)，故應報送總直接損失。

舉例來講：銀行的催收系統中斷一小時，導致催收一百萬的帳款無法進行；或者 ATM 提款機因為網路中斷，顧客無法進行跨行提款交易等，此類營運中斷的事件，屬於作業風險的規範範圍。實際損失之認定：

- 不考慮風險控制後的變化: 催收系統一小時就恢復，仍可繼續完成中斷期間未催收的作業，但實際損失認定過程，不考慮風險控制後之變化，仍應認列損失一百萬。
- 不考慮機會成本: ATM 提款機發生網路中斷，客戶可以選擇使用他行 ATM，也可能過一段時間等系統恢復正常後，再回來使用原來的 ATM，手續費只是延後收入，並未損失。但這類的機會成本，不在認定損失的考慮範圍，因此需認定該客戶在中斷期間為完成交易衍生的手續費收入損失。
- 不考慮策略風險與信譽風險: ATM 提款機發生網路中斷，對客戶產生不

便，對於銀行信譽產生負面影響，客戶可能會選擇轉移到其他銀行。此類因信譽風險衍生的損失，不在認定損失的考慮範圍。

第四節、個人資料保護法的罰則

我國個人資料保護法，規範個人資料保護的範圍、方式與罰則。本節先說明有關個人資料保護法對於個資外洩的罰款規定，作為本論文探討個資外洩個案時，計算財務賠償金額的依據。計算可能賠償金額，是用來衡量資訊安全對企業的效益方法。

一、 概述

隨著近年來詐騙事件與外洩事件頻傳，讓人逐漸了解一般個人資料若不慎外流，會造成相當大的傷害，例如金融業或網路購物業者，擁有眾多且龐大的客戶資料，營業過程對大量客戶資料進行蒐集、處理或利用，因此需確保個人資料的安全與保密性，若疏忽對個人資料的保護，可能會讓企業蒙受大金額罰鍰的損失。

我國於 99 年 5 月 26 日，總統公布《個人資料保護法》[18]，法案中將個人資料保護的範圍將過去醫療、電信、大眾傳播、金融等八大行業，擴大至所有公民營機關，也就是說無店面零售業、個人、團體也都納入規範圍，並加重民事及刑事的責任或對負責人科處同一額度之罰鍰，更提供民眾主動投訴機制，並賦予主管機關、直轄市或縣政府可依職權實施行政檢查。

新法增訂個人之醫療、基因、性生活、健康檢查及犯罪前科等 5 種資料為特種資料，特種資料原則上不得蒐集、處理或利用(§6)；特定目的外利用個人資料，避免列入定型化契約之約定條款而作概括同意，應由當事人單獨為書面同意(§7、§19) ；蒐集資料原則上，均需明確告知當事人蒐集機關名稱、目的等資料。不論直接或間接蒐集個人資料，均有告知當事人之義務(§8、§9)。對於資料正確性與通知義務，及資料外洩或被竊取時，資料持有者應以適當方式通知當事人(§11、§12)。若有違反本法規定時，應主動或依當事人之請求，刪除或停止蒐集、處理或利用其個人資料(§20)。

二、 個人資料管理規範與罰則

非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。對於同一原因事實造成多數當事人權利受侵

害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。(§28)

非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。(§27)

非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰 (§50)。

由上述法律的規範，我們可以試算如果企業洩漏一筆客戶的個人資料，如果被當事人依法提出損害賠償，需賠償新臺幣 500 元以上 20,000 元以下的罰款。這是一個客觀的金錢損失指標，如果可以證明資訊安全服務，有效防止多少筆個人資料外洩，可以參酌個資法的條文，計算可能的賠償金額，這是另一種用來衡量資訊安全對企業的效益方法。

第三章　SOC 資訊安全服務概述

第一節、服務概述

面對這種威脅四伏的情況，入侵偵測系統、入侵防禦系統、標榜多種防毒與防駭功能的資安設備一一出爐，但是買了這些系統或設備就能高枕無憂嗎？入侵偵測系統的高誤報率(False Positive)，讓許多使用者搖頭嘆息，面對每天成千上萬的警訊，多半只能將這些警訊紀錄儲存，束之高閣，沒有時間逐項檢視處理。如果未經適當的調整，入侵偵測系統每天可能產生數千項甚至數萬項的警訊，遠超過人為處理的能量。

入侵防禦系統雖然標榜具有偵測及阻絕入侵行為的能力，但在誤報無法減低的情況下，隨意阻絕偵測到的誤報可能造成正常使用者的斷線與抱怨，問題並無法有效的解決。就算使用者有能力和時間調整入侵偵測系統或入侵防禦系統，將誤報的比例減低到合理的程度，但幾乎不可能完全消除誤報，人為的介入審視與判斷仍不可避免。這類封包導向的偵測系統，之所以會產生過多的誤報，主要是欠缺足夠的環境資訊來做判斷。就如同一位資安專家進行資安事件的判讀，必須兼顧下列因素才能提高正確率與合理性，避免見樹不見林的毛病：

- 被攻擊標的物防禦狀況與系統弱點
- 被攻擊標的物的價值高低
- 其他資安設備或網路設備所發生的相關事件

許多單位漸漸發現將資安資訊彙整、集中分析，才能有效的提高入侵偵測、資安風險監控與處理的效能，因應市場的需求，資安資訊管理系統(Security Information & Event Management System；簡稱 SIEM)便誕生了。若欠缺適當的工具來蒐集、整合、分析、顯示成千上萬原始事件，再有能力的資安專家也難以判斷與處理。SIEM 系統通常可以蒐集各種資安設備和網路設備的資安相關資料，經過正規化(Normalization)調整資料格式為一致，再交給關聯分析系統進行分析，參考資訊資產的屬性與價值，最後推論出值得進一步檢視的事件，再交由作業流程控管系統自動派工給資安專家，進行分析和研判，並進行必要的應變處理。

SOC 是負責管理、維運 SIEM 系統的單位，除了 SIEM 軟、硬體的建置以外，還需要有人員、流程的搭配，才能提供穩定與高品質的服務。

第二節、SOC 平台之技術架構

SOC 服務乃是以資安監控防護平台為基礎，進行機關、企業端的 7x24 資安防護維運，監控網路環境異常狀況，處理突發的攻擊事件。防護平台的嚴謹度與功能乃是防護成功與否的重要關鍵，整理 SOC 處理邏輯如（圖 8）所示，包括下述之功能模組：

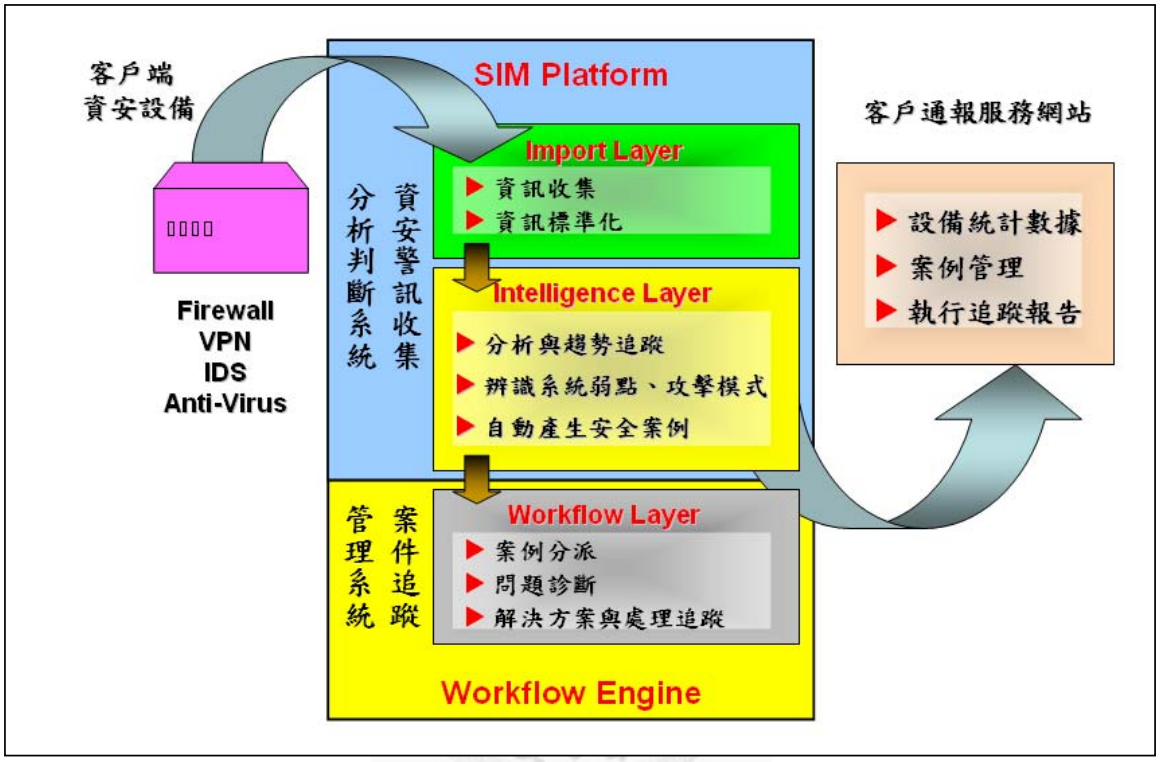


圖 8.SOC邏輯功能圖

- 收集客戶端的資安監控軟硬體維運資訊：如防火牆、入侵偵測系統、防毒系統等。
- SOC 平台前端資訊收集正規化（Import Layer/SIEM, Security Information Management Platform）：將各種客戶端設備的資訊進行正規化（Normalization）與過濾（Filtering），以利於後端一致性的處理與判斷。
- SOC 平台事件智慧判斷（Intelligence Layer/SIEM Platform）：所收集到的資訊安全事件資訊，與過去已知之案例進行智慧型的比對，以及對不同的資料群間作關聯性的分析，判斷出最有可能的攻擊型態與來源。
- 事件處理與派工（Workflow Layer）：對於所判定的攻擊行為進行因應處理作業，包括事件發生時優先隔離問題，再進行深入處理之程序，以及問題處理之分派、進展追蹤與層報等。

- 客戶服務入口網站：將事件處理進展資訊透過網站機制供客戶參考，或是提供客戶登錄與追蹤問題的管道。

以另一個角度觀之，上述之處理邏輯亦可視之由「資料來源層」、「安全日誌收集層」、「安全事件分析層」與「營運管理層」所組成（圖 9）。

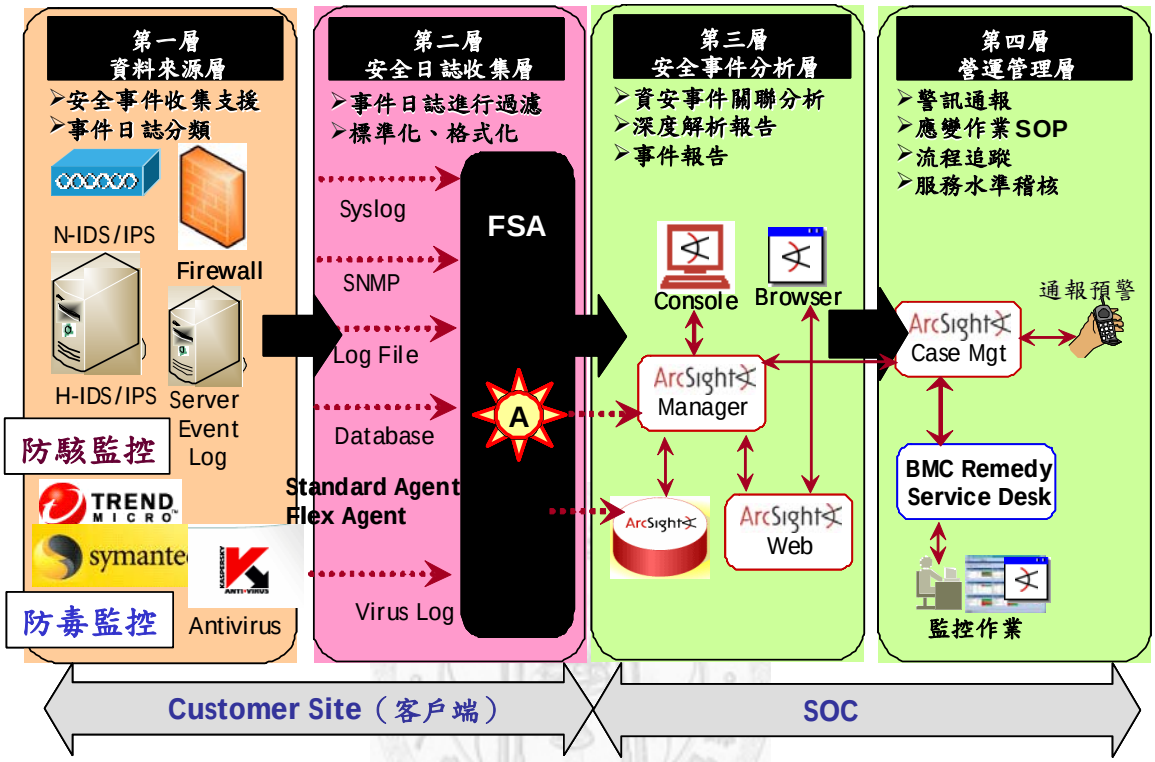


圖 9.四層式資料處理架構圖

在上述的四層架構中：

- 「資料來源層」為被監控之設備。
- 「安全日誌收集層」為收集監控設備原始事件資訊之層次，包括內含安裝於 FSA 的日誌收集 Agent 與收集防毒資訊之 Agent。
- 「安全事件分析層」為智慧型判斷分析之核心 SIEM/SIEM（Security Information & Event Management 或 Security Information Management）。
- 營運管理層為負責驅動營運作業流程之系統，包括提供營運異常事件之警示、通報、查詢、層報、追蹤與統計等功能。

SOC 平台支援各種網路、資安設備監控作業，包括 Firewall，網路型入侵偵測／防禦系統（IDS/IPS），主機型入侵偵測系統（Host IDS），防毒偵測系統等。前端設備（FSA / Front-End Security Appliance）接收各項監控設備之原始事件資料，並傳送至後端的監控平台進行事件的匯整與關聯性分析。

一、前端事件收集器（FSA）

FSA（Front-end Security Appliance）部署於客戶端的前端設備，主要功用為收集各項監控資安設備的原始事件資訊，經過聚合、過濾與壓縮後送回後端系統，以分析出真正有威脅性的事件。FSA 具有集中管理、高可靠度、高安全性、快速更新等特點，是一個理想的資安前端設備。

二、SIEM/SIEM 系統

SIEM（Security Information & Event Management, SIM or SIEM）乃是 SOC 平台智慧判斷能力的核心模組，為一整合性的資訊安全事件管理平台，主要提供用戶更為即時且有效的資訊安全管理。SIEM 系統收集各資訊安全設備、網路設備、作業系統、應用程式之日誌，配合 SOC 營運人員之經驗，對這些資訊加以過濾、正規化及關聯分析，從成千上萬錯綜複雜之日誌檔中即時獲知單位或客戶端之資訊安全狀態。

三、營運管理系統

營運管理平台用來管理資安事件之處理流程，內含維運經驗及客戶維運需求，是 SOC 營運效率與服務水準之精髓所在。營運管理平台提供資訊安全服務管理一個整合性的基礎，基於 ITIL 最佳實務方法論，將設計相關流程並加以自動化，包括監控、傳送與管理異常事件之服務請求、異動服務請求，顯示受到事件或問題衝擊的服務，並顯示相關的組態資訊與管理資訊，以提供營運組織做服務優先順序的決策，採取適當的回應動作。

表3 營運管理系統與ITIL服務流程關係表

營運管理系統		ITIL 服務管理流程
Service Desk	Incident Management	Incident Management（事件管理）
	Problem Management	Problem Management（問題管理）
	Task Tracking	Change Management（異動管理）
Service Level Management		Service Level Management（SLM，服務水準管理）
CMDB		Configuration Management（組態管理）
SIEM 平台		

第三節、 組織與人力

質量俱備的技術人員，必須透過良好的組織分工設計，方能發揮團隊戰力。以 Acer SOC 為例，資安監控中心 7x24 維運組織與專業支援，透過不同分工、不同層次之技術人員分層負責。

一、 維運組織範例

維運組織共分為一線、二線至三線的技術人員，負責資安、設備監控與事件處理。以某一台灣 SOC 為例，維運組織（圖 10）分工權責分別為：

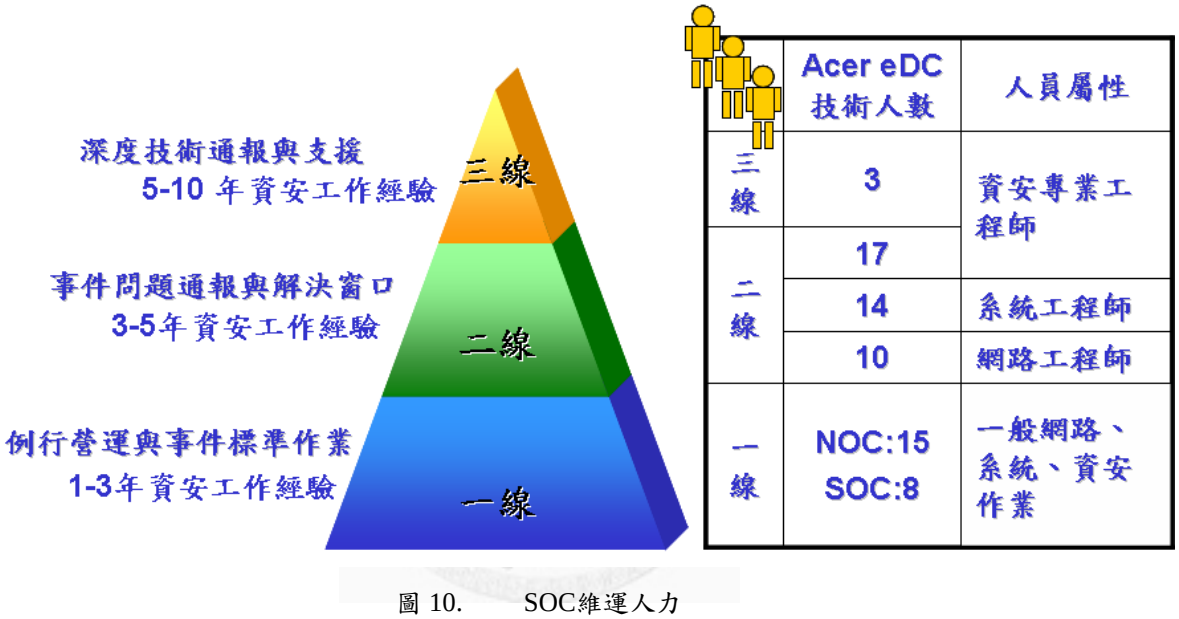


圖 10. SOC維運人力

- 一線監控人員

  一線監控維運人員共約 20~30 人，全年無休不間斷提供穩定監控服務；主要責任為依據 SOP 進行快速的問題標準診斷與解決程序。

- 二線監控工程師

  受過平台技術移轉專業訓練，負責由蒐集之原始資料中透過 SOC 平台功能與本身經驗挖掘異常現象，診斷潛在之資安問題，必要時發出資安警訊通報，並進行鑑識工作。

- 三線資安專家

  受過 MSS 訓練，並具備超過十年以上之資訊安全工作經驗；負責檢核複雜之資安通報，對受侵之鑑識結果進行覆核，並對二線技術人員提供技術諮詢。

二、 專業支援組織

專業支援組織在於提供營運所需各種專業服務能力，(圖 11) 各區塊之項目，包括：

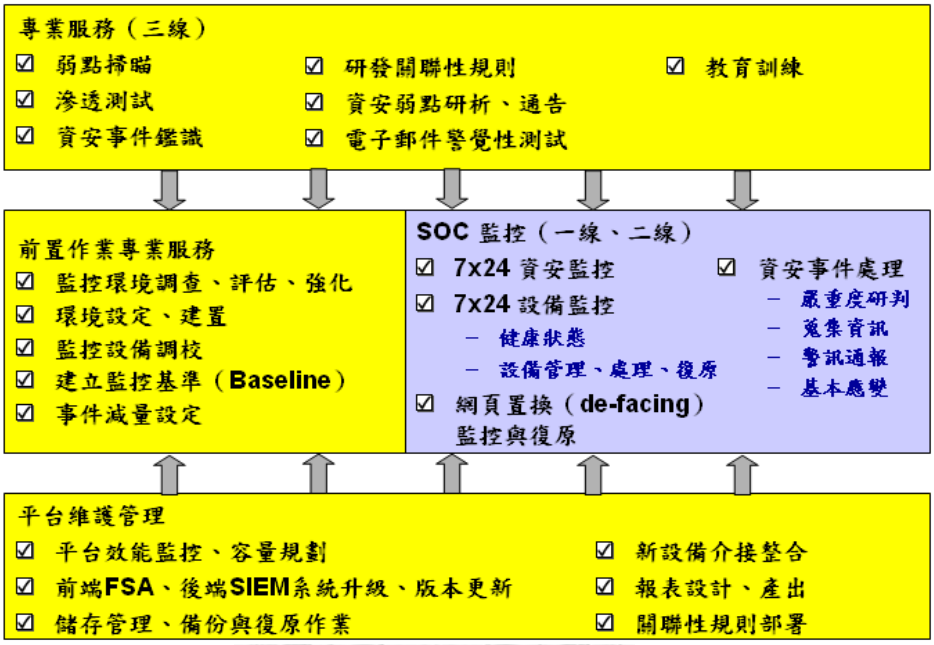


圖 11. SOC分工

- 監控前置作業

主要內容在於針對新加入的客戶監控環境進行瞭解，運用弱點掃瞄工具進行環境評估與強化，安裝設定監控之硬軟體設備，調校資安設備，導入資安設備之事件資訊以建立監控基準，以及進行事件減量之設定。俟測試驗證所有的監控部署均為正確，才能交接給資安監控人員進行 7X24 的監控作業。

- 專業服務

專業服務在於提供監控維運所需的弱點掃瞄、資安事件鑑識工作。此外，客戶通常希望搭配 SOC 監控能有教育訓練、電子郵件社交工程測試以及國際重大資安警訊分析通報服務，亦屬專業服務組織之範圍。而依據營運經驗不斷開拓新的關聯性分析規則，使資安監控精準度能不斷提升，更是專業服務組織價值所在。

- 平台維護管理

主要工作在於管理 SOC 平台軟硬體系統，並依據運轉狀況進行前瞻的容量規劃，使平台維持於尖峰穩定狀況。此外也負責維護前端 FSA、後端 SIEM 系統，對資料庫之儲存空間進行管理與備份作業。如遇特殊之新資安設備需導入時，負

責客製化之銜接開發整合。此外，報表客製化、關聯性分析規則之部署等，亦為平台組織的責任範圍。

此外，亦需搭配系統管理與網路管理相關人才，對於 SOC 的維運也有相當的幫助，支援工作包括：監控平台維護管理、系統與網路支援作業、技術資訊與工具的提供等。NOC 一線人員對於簡易的資安事件亦可提供相關支援，例如網頁竄改事件之通報與處理。由於資安問題包羅萬象，常涉及網路與系統問題，因此整合此類專案之部門，得以發揮完整的資安防護能力。

第四節、資安事件管理作業

一、 資安事件之通報

資安事件警訊通報是 SOC 人員依據系統分析處理的資安原始訊息，輔以人員本身豐富的資安知識與經驗分析，對客戶所進行之通報，目的在提醒客戶檢查與比對警訊通報內容與實際環境狀況，判定是否發生異常事件。

SOC 將於客戶 SLA 協議的時效內，以電子郵件、電話通知客戶權責人員，並於 SOC 營運管理系統中詳細記錄。在發佈警訊通報時，將依分工權責領域決定通報對象（表 4 ），讓相關管理者即時獲得通知，達到真正責任劃分與即時問題診斷的目的。

表4 通報對象表

對象	說明	對應人員
管理	單位內，具有政策擬定、規範發佈等職責之人員	資訊主管、單位管理人
網路	單位內之技術人員，如網路設備、資訊設備…相關負責人	Router, Switch, Firewall, 入侵偵測設備等之管理者
系統	單位內之系統人員，如程式設計、網站網頁、伺服器系統…相關負責人	Web/Mail Server，應用系統、重要主機管理者

二、 資安事件通報之回饋與改善

由於 SOC 監控之各種網路、主機與應用程式的設定和彼此間互動關係複雜，資安事件難免有誤判。為提升 SOC 資安事件通報之精準度，必須對應檢核客戶環境實際狀況後進行通報回饋作業。SOC 資安通報均含可疑電腦之 IP 位址，客戶端權責窗口接獲通報後應檢視該 IP 主機是否有通報所述之異常行為。如該主機之正常行為被 SOC 誤判為異常，則需透過 SOC 之入口網站（圖 12）回饋此資訊，以便 SOC 調整偵測規則，避免未來持續誤判。

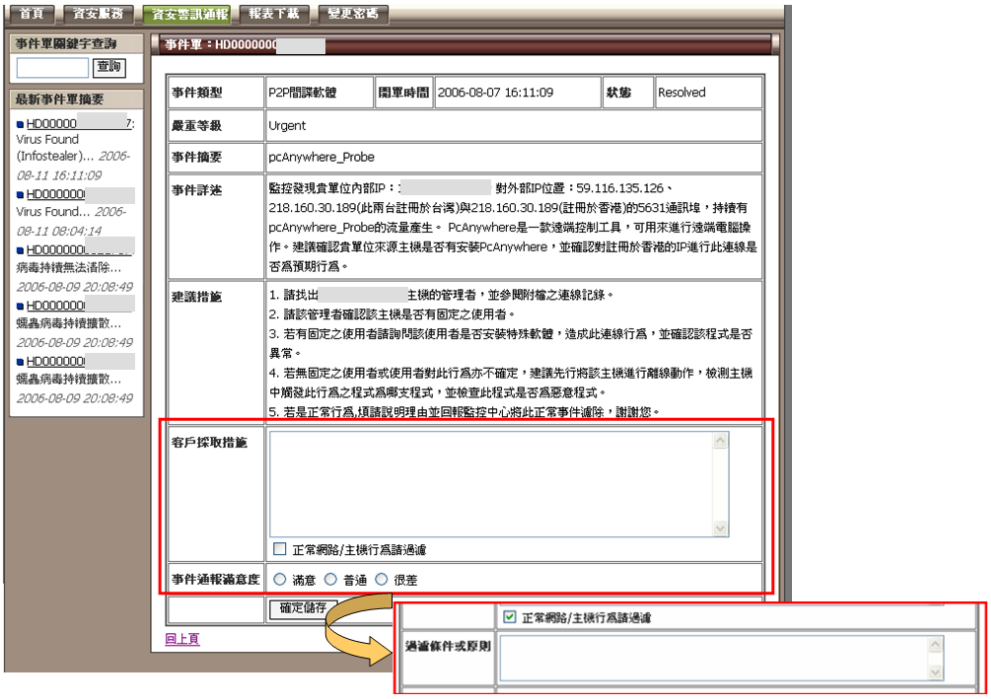


圖 12.　　通報回饋改善網頁

三、 事件之處理（追蹤、鑑識與復原）

SOC 對於事件之處理，係依循 ISO/IEC TR 18044[7]流程四個階段的精神。除了第一、二階段之事前準備與監控、偵測外，處理作業上係集中力量於第三階段的「封鎖與復原階段」，執行封鎖作業與證據蒐集、事故還原外，以及事後的蒐集與存證（經驗學習），以完成事件之處理。

依據 ISO/IEC TR 18044 第三、四階段之精神，SOC 設計出事件通報之作業分工與流程（圖 14），除進行通報適當對象（客戶權責人員或駐點服務人員）外，亦需進行通報之追蹤，確認負責現場事件處理之人員已收到通報，同時瞭解事件之複雜度以及是否需要後端提供遠端與現場支援與諮詢等。

如遇資安事件於指定時間內無法圓滿解決，或 SOC 工程師研判事件複雜度達一定程度，則會啟動「重大資安事件流程」，除將事件處理升級、投入更多資源外，也將持續回報客戶、宏碁相關主管處理之進展。

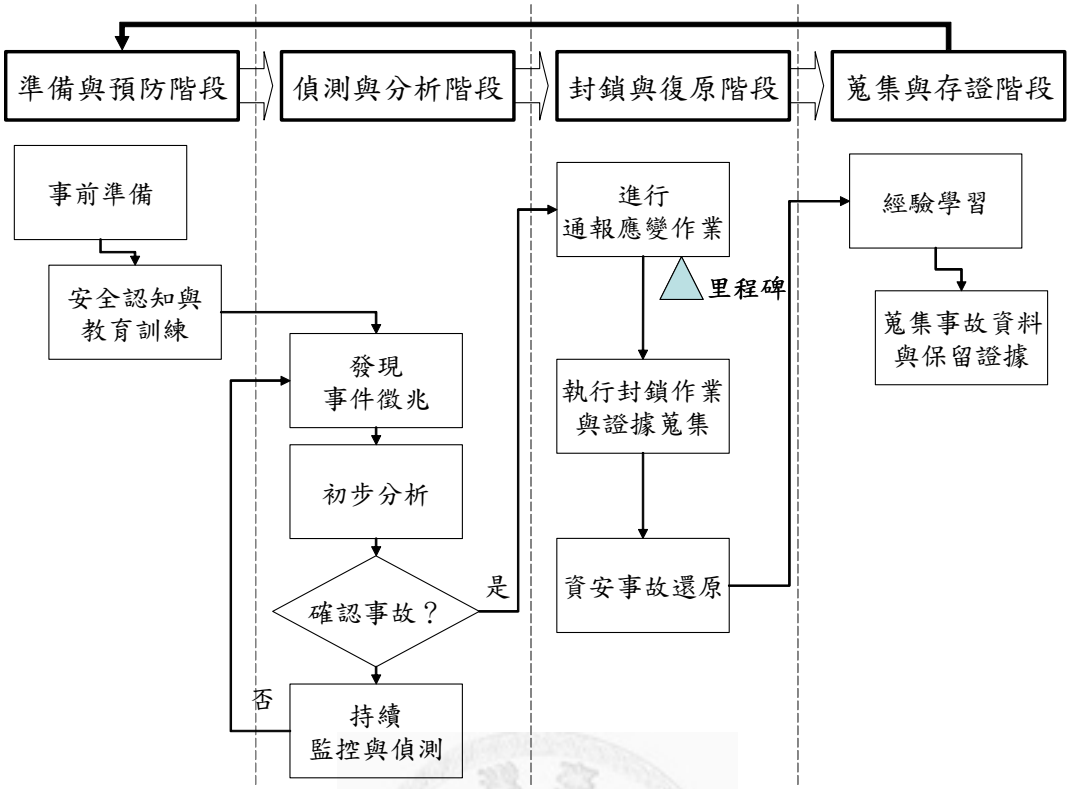


圖 13.　　ISO/IEC TR 18044資安事件作業流程

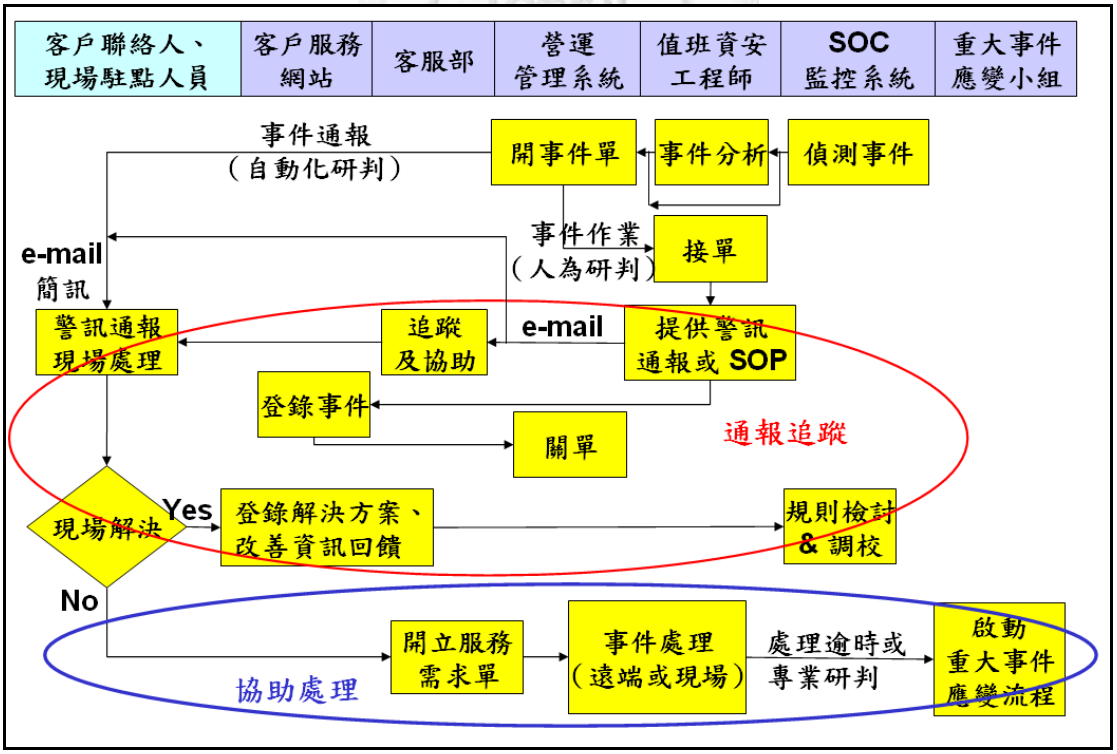


圖 14.　　資安事件通報與處理

（一） 事件鑑識

一旦確認客戶環境遭受入侵，則需進行鑑識，找出入侵管道，並確認是否感

染惡意程式，進行清除作業。SOC 依據過去眾多事件的鑑識經驗，設計了「惡意程式清除與採證 SOP」，作為惡意程式清除之依循。SOP 乃是擷取經驗智慧的精髓，並參照 SANS（SysAdmin, Audit, Networking, and Security）國際組織的建議精神，依圖 15「鑑識→排除→根除→回復→追蹤」五個階段進行作業。主要工作項目包括：

- 鑑識：分析事件資訊，尋找攻擊來源，並評估威脅與衝擊。
- 排除：隔離受害主機，控制損害程度，並防堵事件繼續擴大。
- 根除：確認問題根源，據以調整系統或政策。
- 回復：恢復系統至未受害前之狀態。
- 追蹤：持續觀察事件是否復發。

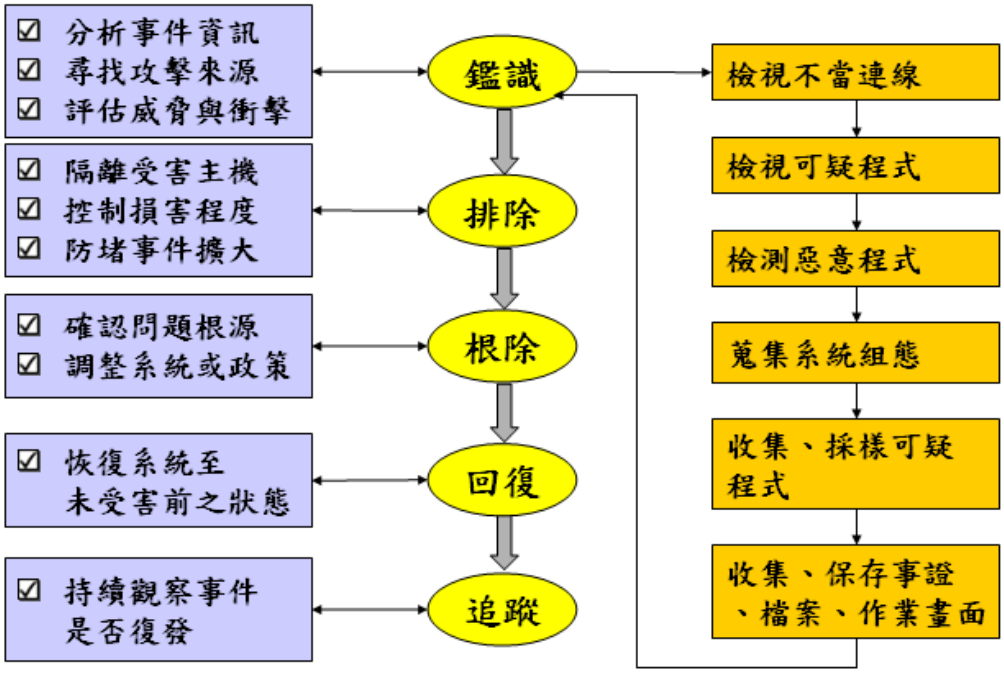


圖 15.　　SANS事件處理程序

上述步驟中，事件之鑑識為技術相當複雜之作業，全賴資安技術人員之經驗與知識，配合現場狀況之判斷，執行機動作業。鑑識工作共包括下述程序：

- 檢視不當連線
- 檢視可疑程式
- 利用工具檢測惡意程式
- 蒐集系統組態
- 收集、採樣可疑程式
- 收集、保存事證、檔案與作業畫面

（二） 系統復原程序

系統復原程序建立前，應先調查現行系統環境，記錄系統、網路、服務等設定參數；再行調查現行系統軟體，記錄系統安裝軟體清單，最後再建立復原程序與流程，據以進行復原作業。在人員搭配上，系統復原前須先知會硬體供應商以及系統管理、應用軟體管理維護、網路管理人員，以便於復原作業發生問題之第一時間聯絡相關人員排除問題。

系統復原工作極為細緻，SOC 以從事的復原工作經驗為基礎，提供系統復原的諮詢服務，並適時提出建議及風險評估，以及對應之處理方案。

（三） 事件處理報告

資安事件排除後，Acer SOC 將交付資安事件處理報告書，其項目包括：

- 資安事件發生之原因

  說明資安事件的整體始末，以及使用的系統漏洞或入侵攻擊方法的說明。

- 處理的過程

  包括事件整體的過程、入侵或攻擊過程、鑑識及追查過程。

- 事件分析判斷

  分析判斷所有事件所代表的意義與訊息。

- 檢測鑑識所使用的工具

  如：網路工具（TcpView 等）、程序檢查工具（ProceView 等）、間諜程式移除工具（Microsoft Windows Malicious Software Removal Tool）、系統基本程式（如防毒軟體、系統工具等系統具有的合法軟體），以及其他臨時依當時情況所使用的軟體或工具。

- 蒐證的紀錄及相關資訊

  包括：被入侵攻擊系統的關鍵記錄（Logs）或事件（Events）、系統程序及網路連線狀態紀錄、入侵或惡意程式檔案、網路設備或系統偵測之事件紀錄（Firewall、IDS、IPS、Anti-Virus Gateway、Anti-Virus Server 等），以及被入侵攻擊系統軟硬體設備資料。

- 事件之結論與改善建議

  總結所有鑑識過程、入侵方式、事件影響、強化改善建議等資料及具體改善建議。

第五節、SOC 營運技術與智慧

仔細分析網路上的攻擊行為，將會發現有很重要的特徵：各種攻擊事件有先後次序的關係，例如一個系統被成功攻擊之前，攻擊者需先建立進入點；要建立進入點之前，就要先可以通過各種管制點或逃避偵測；要知道哪裡有可能的進入點，就要先進行偵查或刺探，以決定要選擇哪一個目標為入侵標的。

依照這樣的時序關係，我們搭配在 IT 環境不同節點的不同功能資安設備，綜合各種事件的比對與分析，可以協助我們儘早掌握入侵事件，並進行後續的通報、阻絕與處理等等。典型的資安防禦架構（圖 16）[11]，各組成元件說明如下。

- 實體安全：利用特殊設備（如門禁、指紋辨識），限制存取電腦系統。
- 偵查獲取情報：攻擊者利用各種資訊技術或其他方法，瞭解企業的網路架構或電腦系統的位置與提供之服務內容。
- 預警聯防：表示防護端者利用各種偵測技巧，標定可能的偵查行為並預警，常見的有誘捕系統（honeypot）將不尋常的連線行為儘早辨識出來。或使用各種弱點掃瞄工具，自行偵測、發掘潛在的資安弱點。
- 攻擊標的分析：目標分析是指攻擊者分析偵察獲取情報，評估標的特徵與可能的弱點，攻擊者也可以與駭客社群，獲取各種工具或手法。
- 威脅分析與補丁：威脅分析是防守端採取的防守行為，以進一步確定潛在的攻擊者和他們的動機。防守者還可以進行滲透測試之類的檢測，以攻擊者的思維，對防守端的環境進行攻擊。一般滲透測試會找第三方專家來負責，以便找出高風險的問題，並預先加以補強與防範。
- 試探存取系統：試探存取是指那些在之前偵查獲取情報實取得的基本用戶名，並嘗試是否可以登錄系統，並取得權限（如 root）的行為。
- 入侵偵測與防禦：防守方利用各種監控設備，找出符合攻擊特徵的事件，並加以記錄或阻擋。
- 閘道進出管制：用戶進出管制是指防守方以電子方式來限制登錄系統所採取的措施，這些控制可能包含有多重密碼，整合防火牆、IC 卡等，用來決定或限制用戶的進出、登入、權限等行為。
- 入侵系統：實際進入系統並獲得其控制權。
- 發起攻擊：實際攻擊，可能發生在單一事件或一個波段的攻擊事件中。

- 消除入侵痕跡：掩蓋入侵者所採取的行動，掩飾並消除了入侵的證據。
- 即時監控、事件回應：綜合所有蒐集到事件綜合分析研判攻擊方的活動，7 x 24 監控攻擊事件可能造成的風險高低與影響範圍。並根據事先約定的通報程序或處理方式，發出通知或進行事件處理。在有威脅的事件發生多久內要完成通知、處理等，稱作服務水準（SLA – Service Level Agreement）。
- 系統損壞：系統受損指的是攻擊所損失或影響之服務、資料或系統功能。系統受損程度，也代表攻擊產生之影響強度高低，也代表系統的可靠程度或存活力高低。
- 系統受損反應：系統反應是指被攻擊後系統的變化（例如導航系統螢幕消失，或收到不知情的國際電話帳單），這些反應是攻擊所造成的後果。例如系統進入一個非預期的運作模式，甚至死當，並利用意外的運作模式，盜取所需的資訊。
- 災害評估：鑑定系統失去的功能和資訊，並評估影響範圍。防守方在攻擊後對業務或任務操作的影響。最理想情況是在攻擊發生便進行此分析，如此一來，對於各種攻擊行為資料保管相關人員皆可依循其標準作業流程來處理。
- 鑑識採樣：還原攻擊過程、採集攻擊留下之證據或植入之檔案。
- 反應復原：將系統回復受攻擊前之狀態。
- 後續追蹤：檢查系統運作，確認相關之處理以確實排除攻擊所後發生之影響，並恢復正常。

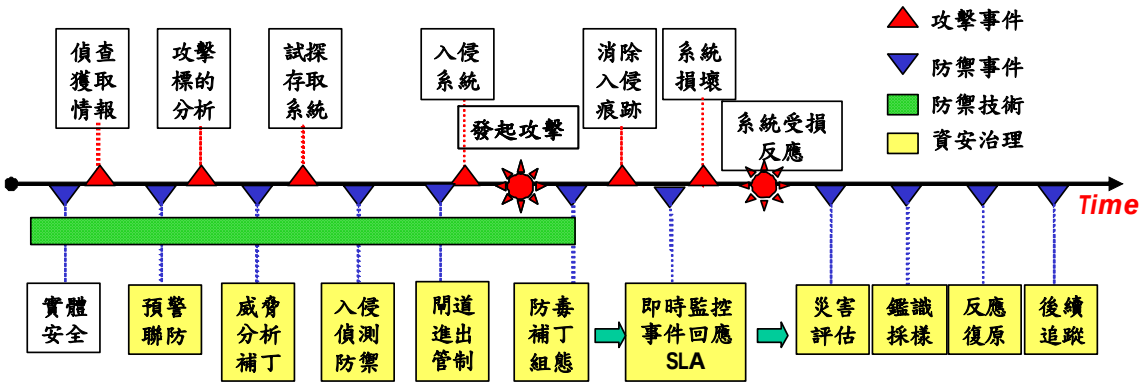


圖 16.　　縱深防禦架構

第六節、SOC 績效評估架構

績效評估需要搭配相關的度量指標（Metrics）加以衡量，在牛津字典中[10]，Metric is a system or standard of measurement. 在 IT 領域之中[2]，將 IT portfolio management 分成兩個主要的構面：

- value delivery- 包含降低成本、增加營收、提高生產力、降低循環時間、降低停頓(downtime)時間等。
- process improvement - 主要聚焦在有效度(effectiveness)上，關心相關的流程(process)是否有改善，流程是否提供預期的價值，流程是否適當的涵蓋 IT 的活動等。

度量指標要反應某一關注領域績效好壞與量化關注領域特徵，並提供時序性比較基礎，瞭解不同時間績效變化。參考上述的構面與典型的資安防禦架構（圖 16），將資訊安全衡量指標區分為「技術管理構面」與「營運管理構面」（圖 17）。

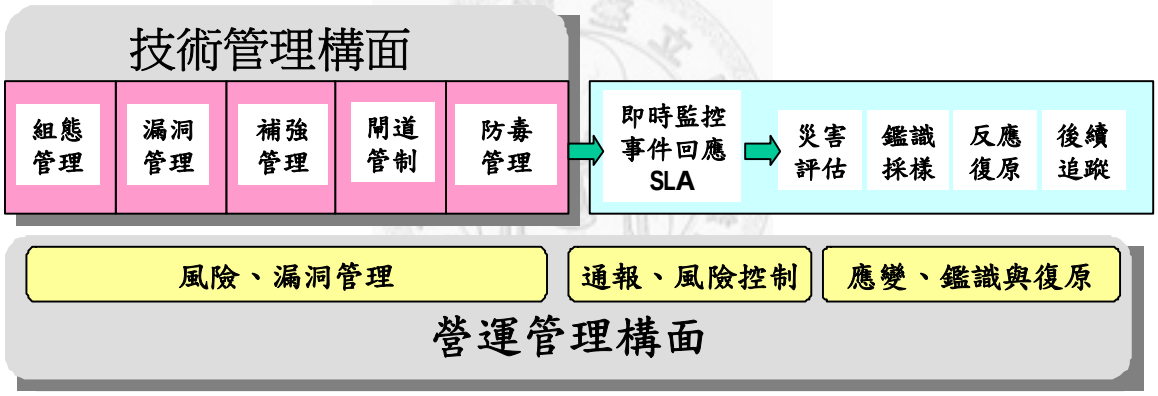


圖 17.　　績效評估構面

- 技術管理構面：針對各項單一設備的表現，各種設備需正確運作，修正組態錯誤、潛在資源誤用、發掘資安風險事件等，以達到提高生產力、降低停頓(downtime)時間等目的。技術管理構面將根據所收集的單一設備所產出 Log 加以統計、交叉分析，並根據這些結果衡量各個設備的運作狀態是否在合理與最佳狀態。
- 營運管理構面：（圖 17）所示，整體安全服務涵蓋的範圍包含「風險、漏洞管理」、「通報、風險控制」、「應變、鑑識與復原」等，要綜合管理這些領域，需要有完整的流程與量化的指標來了解安全管理方案的有效性。透過此方式降低人為主觀的判斷，並掌握各種安全控制是否如預期運作，與需要改善的項目與落實責任的歸屬(accountability)等。

第四章　技術管理指標

第一節、組態管理

企業資訊系統需要透過各種正確的組態設定與安裝的版本，合宜的原始設定等，才能正確運作，滿足企業的營運目標。

- 使用標準版本(Standard Build)主機數量與比率：很多系統的原廠預設值（Default Setting），不一定符合企業的資訊安全要求，例如使用 Microsoft 標準安裝，預設會啟用很多的網路服務。這些網路服務不盡然都是企業所需，企業會客製化（customized）適合使用的版本，並完成相關的安全設定後供內部使用。度量企業所有主機使用標準版本的數量與比重，可以了解 IT 安全控制的程度。
- 企業關鍵系統監控數量與比率：企業系統運作的各種狀態與重要事件，需要納入及時監控，以早期發現各種異常，降低營運的風險。
- 日誌(Log)紀錄完整度與涵蓋度：日誌是記載系統活動過程的重要紀錄，各種日誌是否正確啟動、有效保存，啟用日誌的紀錄的範圍等，是各種安全問題的診斷與處理重要依據。有效的日誌管理，才能完成各種事件的監控、通報、處理與追蹤，越完整的日誌管理，整體的安全控制就有更好的基礎。
- 系統校時涵蓋度：企業內部 IT 系統很多，當有問題要處理或診斷時，分散在各處不同的事件，需要靠統一與精準的時間做為還原事件全貌的依據。
- 緊急組態調整反映時間：企業有時會設計緊急組態調整的程序，例如當有部分網段發生病毒蔓延的狀況發生時，需要緊急設定交換器，切斷某一網段的通訊。此類緊急組態調整，是否快速完成，反映資安事件緊急回應有效程度。

第二節、弱點管理

弱點是各種系統設計瑕疵、邏輯錯誤或是設定錯誤等，可以讓非授權人員取得權限。有些弱點可以透過 Patch 的安裝補強，但有一些設計瑕疵（如使用預設密碼）、程式設計漏洞（如 SQL Injection）等，需要修改原始程式或調整組態才能補強。平時這些弱點並不會有甚麼影響，但對於攻擊者卻是絕佳的利用管道。實務上我們會使用弱點掃瞄工具（Vulnerability Scanning Tool）如 Qulays, Foundstone, WebInspect 等軟體，對系統進行檢查，並產出弱點掃瞄報告。了解 IT 環境弱點的分佈、嚴重度與數量多寡，是重要的安全控制評估指標（圖 18）。

- 弱點分佈指標：依照嚴重等級、系統功能別、資產重要性等，計算弱點數量與比重，可以了解企業整體 IT 環境弱點管理的有效程度（圖 19）。
- 每一主機弱點指標：計算每一個單一主機的弱點分佈狀況，了解特定主機弱點管理的有效程度（表 5 ）。
- 弱點發掘的延遲時間：系統出現弱點以後，多快的時間可以發現。
- 弱點補強的循環時間：發現弱點以後，需要經過確認、測試與實際部署等過程，有一些弱點還要修改程式碼才能解決，計算此一完整循環耗費的時間，可以了解弱點補強效率的好壞。

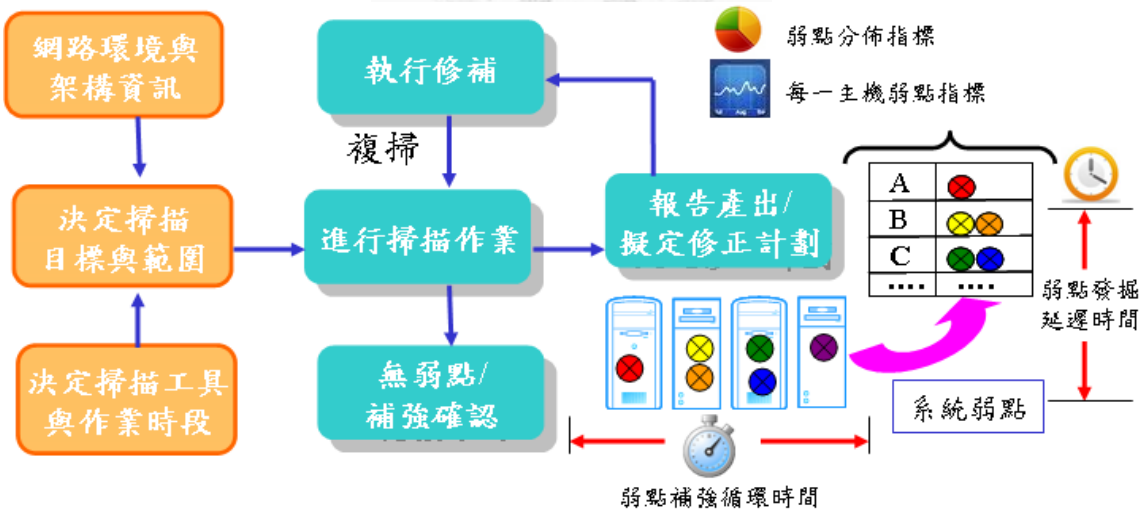


圖 18.　　弱點掃瞄流程與績效評估指標

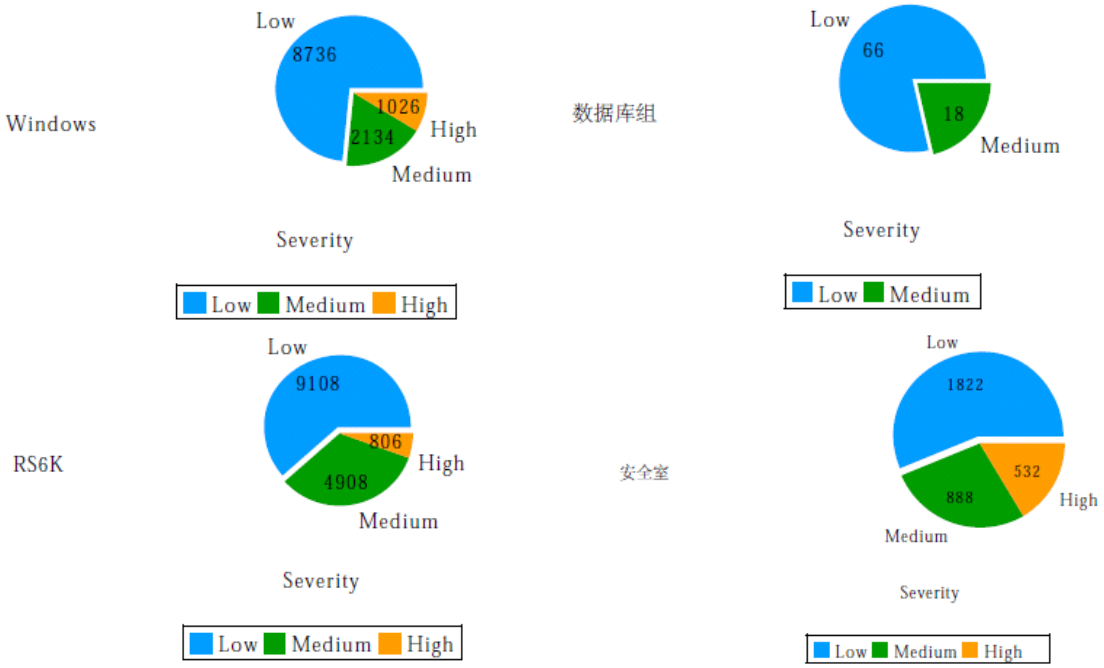


圖 19.　　弱點分佈指標範例

表5 每一主機弱點指標

序號	URL / IP	Q1	Q2	Q3	Q4
1	https://mail.xxx.gov.tw:443	0	0	0	0
2	https://reporter.xxx.gov.tw:443	0	0	2	2
3	http://info.xxx.gov.tw:80	2	3	1	1
4	http://tpi.org.tw:80	6	0	0	0
5	http://www.xxx.tw:80	0	N/A	N/A	N/A
6	http://taiwanxx.xxx.gov.tw:80	42	39	47	46
7	http://laxx.xxx.gov.tw:80	0	0	0	0

第三節、補強管理

企業資訊系統更新 Patch 的速度與範圍，直接反應整體安全程度的好壞。沒有及時 Patch 的系統，將會導致其他各種安全控制機制失效，也等於是建築在沙灘上的城堡，再多的防護也無法讓城堡穩固的屹立不搖。Patch 部署的過程，需要大量人力介入，包含哪些主機要優先安裝哪些 Patch，安裝前要進行確認與測試。由於 Patch 對資訊安全至關重要，我們覺得應有以下的度量指標來評估補強管理的績效：

- 未達 Patch Level 主機數量與比重－尚未更新到目前 Patch Level 的數量與分佈。所謂的 Patch Level 是指企業對於不同用途的主機，會設定不同的 Patch Level，例如重要業務主機，可能只安裝 critical patch，但一般個人電腦，Patch Level 可能不管 patch 的等級，一律無條件安裝更新。
- 未及時 Patch 的延遲時間－Patch 程式公布到實際安裝到目標主機生效的時間差，此時間越短則系統暴露在安全風險的程度越低。
- 更新 Patch 的循環時間－Patch 實際安裝到目標主機之前，要經過 Patch 項目確認、測試與實際安裝部署，這一段處理的過程稱為 Patch 循環時間（Patch Cycle Time）。
- Patch 時間影響服務水準程度－服務水準(Service Level Agreement)是指承諾客戶須滿足的服務時效與穩定度（如每個月排定維護時間 12 小時以內或各種服務中斷不能超過 4 小時等）。進行 Patch 作業時，難免會有短暫的服務影響，因此 Patch 更新的過程，需評估對服務水準的影響程度。

第四節、閘道管制

一、 閘道安全設備

閘道安全控制，指架設在網路通訊路徑上，進行安全管制、事件偵測功能的設備。這些常見的設備，執行各種安全管理政策，辨識安全風險事件，並可依照設定進行阻擋或記錄。在實際環境之中（表 6 ），負責閘道安全的設備還有很多不同功能的設備（如防毒牆、上網管制、頻寬管理）等等，我們選擇目前較為常見且與資訊安全直接相關的設備，設計可用的度量指標。

表6 閘道安全控制設備

項目	功能說明
防火牆 (Firewall)[21]	防火牆具備下列三種重要的基本功能： ● 存取管控(Access Control)：指依據系統管理者所設定的存取控制規則，決定網路交通的許可或拒絕。存取管控的條件包括資料封包的來源位址、目標位址、連接的網路服務協定種類以及使用者的身分等。防火牆對於所有的網路流通會依規則判斷，只有可信任的來源位址可以連到被允許的目標位址，且只能以特定的使用者身分使用特定的網路服務。存取管控甚至可以做到控制網路服務的某些特定指令是否允許其執行，例如 FTP 可以限制只能下載檔案，不能上傳或刪除。 ● 身分識別(Authentication)：即驗證身分，作為服務授權的參考。防火牆必須有效地識別網路使用者及主機的身分，以控管使用權限、確認責任歸屬。 ● 安全稽核：防火牆應能詳細記錄網路流通的狀況，並記錄安全相關事件，以供系統管理者分析之用。一般安全稽核的內容包括：網路服務的連通或拒絕、身分辨識、網路通信發生的時間及持續的時間、資料傳輸位元數、執行時發生的異常狀態、系統組態的修改、某些協定的特殊指令、系統核心接收到的特殊封包等等。
入侵偵測/防禦	即時檢測是 IDS 的核心理念(另有 IPS 設備俱備主動防禦功能)，

系統 (IDS/IPS)	IDS 具備以下功能： ● 線上作業(In-Line)- IDS/IPS 線上過濾所有異常封包，IPS 確認不包含異常活動或可疑內容後，方可進入內部網路。 ● 即時偵測 – IDS 及時偵測網路行為，IPS 可即時阻斷攻擊。 ● 高精確的偵測能力-辨識攻擊特徵的能力須準確無慮，以免誤報新的攻擊特徵也必須定期更新。 ● 高效能與低延遲 - 在實際運作時的封包處理速度必須接近線速 (wire speed)，而且設備在啟用所有攻擊特徵後，須達到宣稱的執行效能。 ● 可靠性與可用性 -須具備故障復原(Failover) 的功能，將工作切換到另一個替換群組的裝置。 ● 自我學習與調整能力 - 具備自我學習與調整能力，依據所在網路環境，分析新的攻擊特徵以更新特徵碼，並提供新的安全防禦策略。
AP 防火牆 (AP Firewall)	網站安全問題，大多數的人聯想到的都是透過網路防火牆或入侵偵測防禦系統進行網站的安全管理與保護。然而美中不足的是，無論是防火牆或是入侵偵測防禦系統，所能夠達成的保護範圍都只僅限於在網路層或系統層的安全屏障，AP Firewall 針對常見之網站應用程式攻擊進行安全檢測及防禦之外，也可透過其客製化的能力對特定應用程式的特殊用途，或特別的安全過濾需求進行過濾規則的制訂，AP Firewall 具備下列基本功能： ● Application Firewall – 可提供企業最佳的 WEB 攻擊保護，包含有效地過濾掃瞄網路層的通訊協定及應用程式內容，執行所定義的安全政策，進而有效地阻擋如 Cross Site Scripting、Buffer Overflows、Forceful browsing 及 SQL injection 等惡意攻擊行為，並且可監看所有網頁應用程式伺服器的流量，及每位員工動態應用程式特徵，自動地辨識合法通訊及拒絕非法的通訊封包。 ● Security Gateway–除了提供 Application Firewall 功能外，還

	提供了效能加速功能使得網站的可用性提高，而內建的流量管理功能，不只可以增加網頁應用程式的運算效能，增加機器的信賴度及可延性，有效節省建置成本，並且還提供了 Load Balance、Health Check、TCP Pooling 和 Catching 等功能，增加了網路伺服器的效能。

二、 技術內涵與度量指標

定期針對監控相關資料進行彙整分析，並產出分析報告，說明資安服務的整體防禦能力現況。報告分為短期性的即時報表（日報、週報）與長期性的分析統計報表（月報），各有不同之使用邏輯。分析報告項目主要包括防火牆與入侵偵測系統，透過二者資料之交叉分析找出問題。防火牆資料拆解成下述類別（圖 20），再與入侵偵測系統進行比對：

- 主機、通訊埠之流量
- 通過與被阻擋之流量
- 流量之數量統計排名

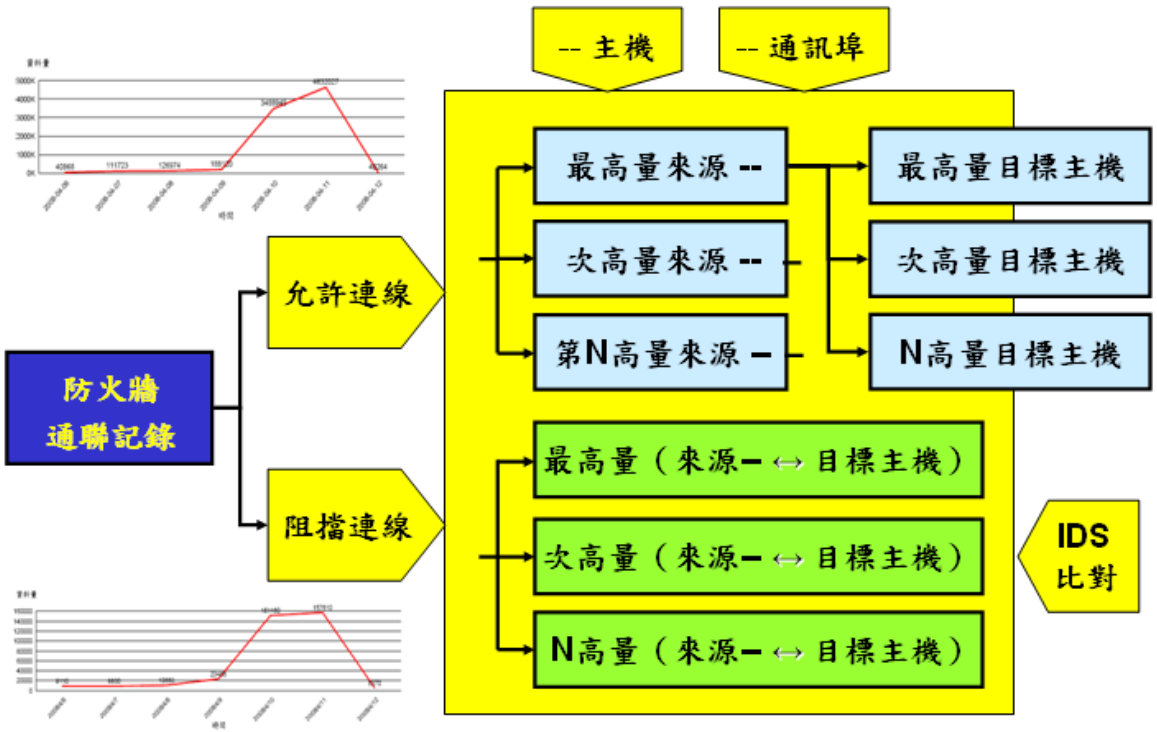


圖 20.　　防火牆資料分析與IDS交叉分析

入侵偵測系統之資料則拆解成二個尺度，並進行交叉比對分析（圖 21）：

- 觸發事件主機（包括觸發事件之連線來源、連線目標）之排名：並對主機下之各種事件進行分析。
- 觸發事件類別之排名：並對各事件下之各主機進行分析。

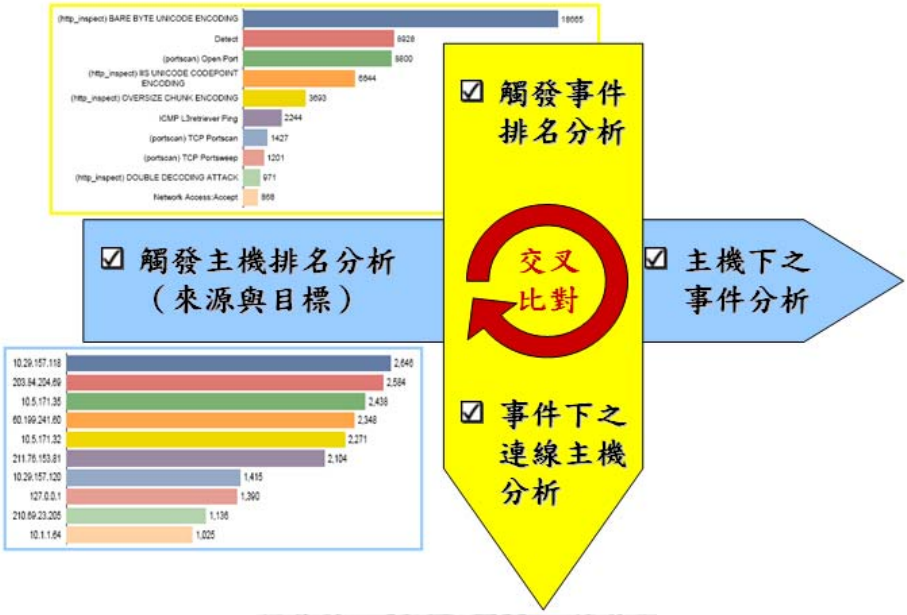


圖 21.　　入侵偵測系統資料分析邏輯

在此分析邏輯前提下，分析報表再細分細部項目如下：

- 資安警訊通報事件（表 7 、圖 22）：統計該期間資安監控警訊通報事件以及事件內涵，俾對該期間內資安事件有全盤性的瞭解。
- 防火牆/IDS 原始事件量統計（圖 23）：顯示防火牆、IDS 設備原始事件量在統計期間內對時間之分佈，藉以確認交通流量是否符合組織營運特性。
- 防火牆主要連線來源、目標主機與通訊埠統計（圖 27）：來源主機並分列允許與阻擋之連線，可以檢視連線之來源與目標是否符合單位之營運特性，或有潛在之攻擊。
- 防火牆阻擋事件統計（圖 25）：如內部連往外部之流量被防火牆阻擋，則隱含內部之使用者網路連線行為恐有違反資安政策，或與中繼站黑名單不當連線的行為。如有連往內部主機之大量交通遭阻擋時，應是有明顯攻擊，亦應仔細追蹤其來源；尤其是源自於單位內部某些網段之攻擊，

更應迅速處理。

- IDS 攻擊來源與目標統計（圖 26）：IDS 可以提供觸發攻擊特徵事件之統計，包括來源與目標，可做為檢核或修訂資安防禦對策之參考。

表7 資安警訊通報事件列表

編號	事件單號	登錄日期	嚴重等級	事件類型	事件摘要	事件描述
1	HD0000000389278	2007/8/6 09:33	Medium	P2P/閒諜程式	(P2P)點對點下載確認	監控發現貴單內部IP位置：[192.168.5.155]之主機以PORT_1323持續與外部多部主機PORT_13大量連線。
2	HD0000000389784	2007/8/8 11:16	Medium	P2P/閒諜程式	閒諜程式活動確認	貴單位IP位置為[192.168.5.155]之主機持續藉由80 Port與目標IP位置為209.133.35.207(位於美國)之主機進行連線作業。
3	HD0000000391212	2007/8/13 15:33	High	異常網路行為	異常網路連線行為確認	發現內部 IP 位置 [192.168.5.109]持續對目標IP 218.145.28.224位置 PORT_8008連線。
4	HD0000000391438	2007/8/14 09:32	Medium	異常網路行為	可疑連線行為確認	貴單位IP位置為[192.168.5.184]之主機持續藉由9100 Port與內部IP位置為[10.78.4.36]之主機進行連線作業。
5	HD0000000392536	2007/8/18 03:05	Medium	P2P/閒諜程式	(P2P)對外開特殊Port大量連線	監控發現貴單內部IP位置：[192.168.200.9]之主機持續與外部多部主機Port_21、25、53大量連線。

連線目標主機的第一名事件列表

Parameter Name	Parameter Value
TimeZone	Asia/Taipei
Start	八月 01 2007 00:00:00
End	八月 31 2007 23:59:00
TargetAddress	192.168.200.3

事件名稱	原始事件量
(portscan) Open Port	4946
(http_inspect) IIS UNICODE CODEPOINT ENCODING	1070
WEB-CGI calendar access	1069
(portscan) TCP Portsweep	1028
WEB-MISC robots.txt access	836
ATTACK-RESPONSES 403 Forbidden	519
(http_inspect) BARE BYTE UNICODE ENCODING	175

連線來源主機的第一名事件列表

Parameter Name	Parameter Value
TimeZone	Asia/Taipei
Start	八月 01 2007 00:00:00
End	八月 31 2007 23:59:00
AttackerAddress	192.168.200.253

事件名稱	事件量
(portscan) Open Port	17642
(portscan) TCP Portsweep	4802
(portscan) TCP Portscan	39
(http_inspect) BARE BYTE UNICODE ENCODING	24
(http_inspect) OVERSIZE CHUNK ENCODING	3

圖 22.　　主要事件主機之事件內涵

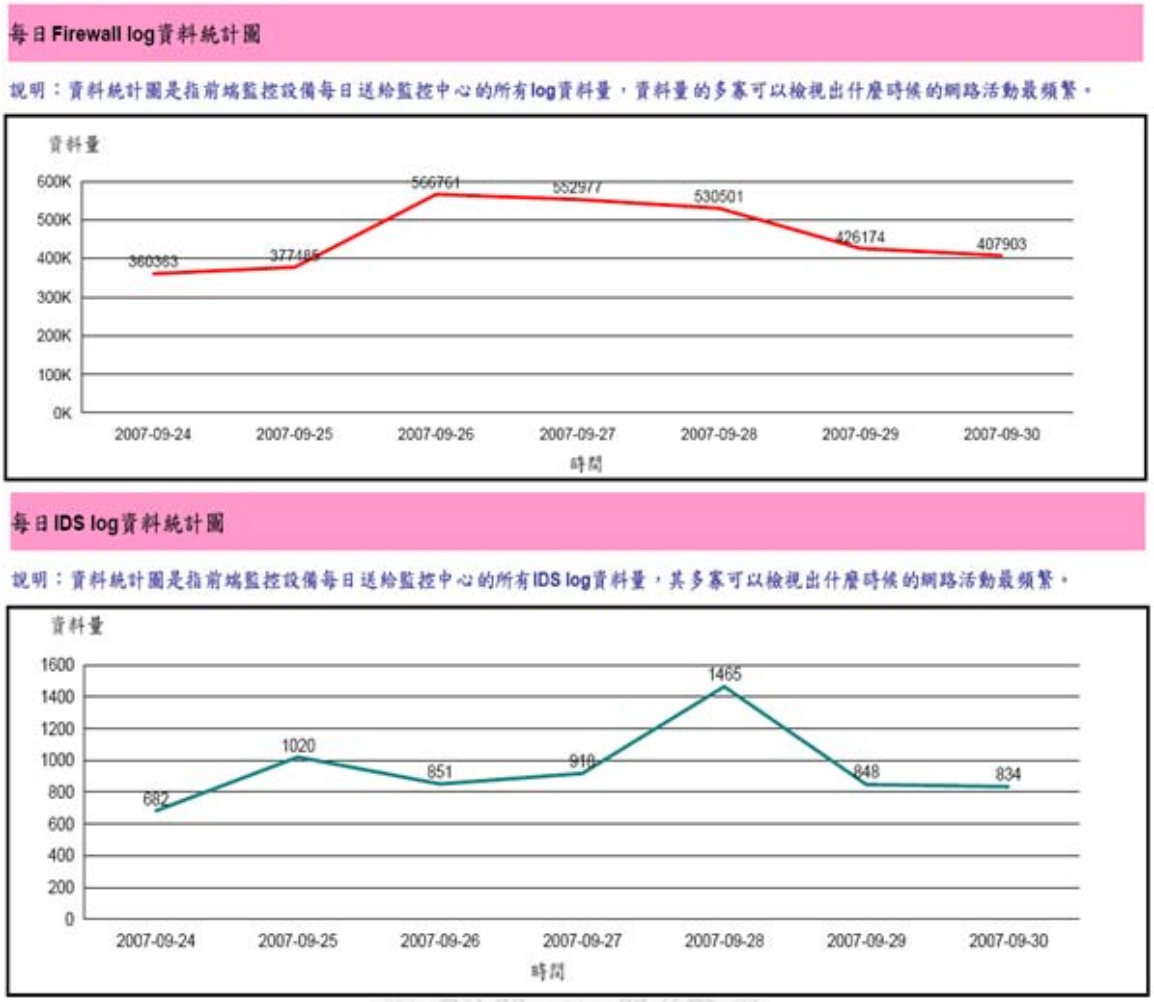
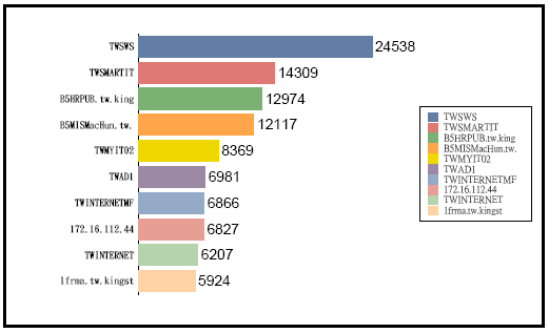


圖 23.　　防火牆/IDS連線數量統計

圖 24.　　防火牆連線來源主機排序－允許、阻擋

防火牆阻擋連線主機前十名

說明：可以檢視出哪些主機的最常違反網路連線規定，太頻繁的不當連線，可能是使用不當程式所造成。



防火牆阻擋連線PORT前十名

說明：可以檢視哪些連線目標Port最常違反防火牆的規則，並可檢視出內部主機是否有不合理的連線行為以及防火牆規則是否合理。

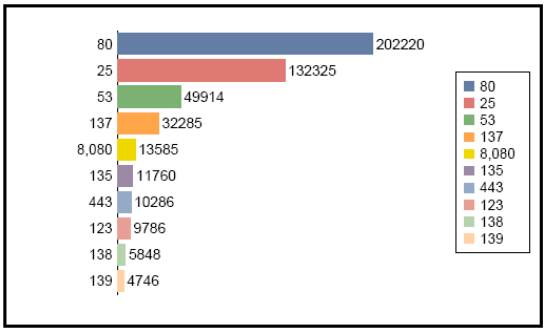
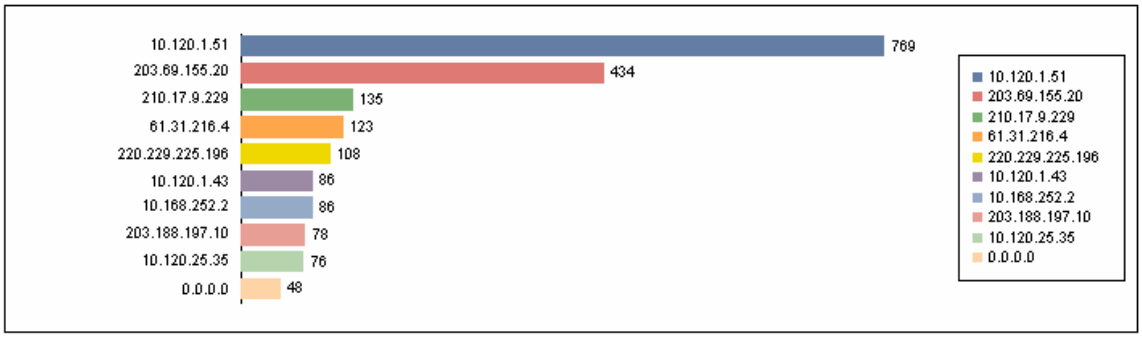


圖 25.　防火牆阻擋連線排序統計－主機、通訊埠

前十大被攻擊目標主機

說明：可以檢視出哪些連線目標主機最常觸發IDS的攻擊事件。若是目標主機為客戶所使用 的範圍，那就需注意加強保護該主機。若是目標主機為Internet上 的主機，那就需要注意內部有哪些主機進行對外的攻擊。



前十大攻擊來源主機

說明：可以檢視出哪些來源主機最常觸發IDS的攻擊事件。若是攻擊來源主機為客戶所使用 的範圍，那就需要注意該主機可能已經被植入惡意程式。若是攻擊來源主機為Internet上 的主機，那就需注意該主機的後續行為，必要時可以直接以防火牆進行阻擋。

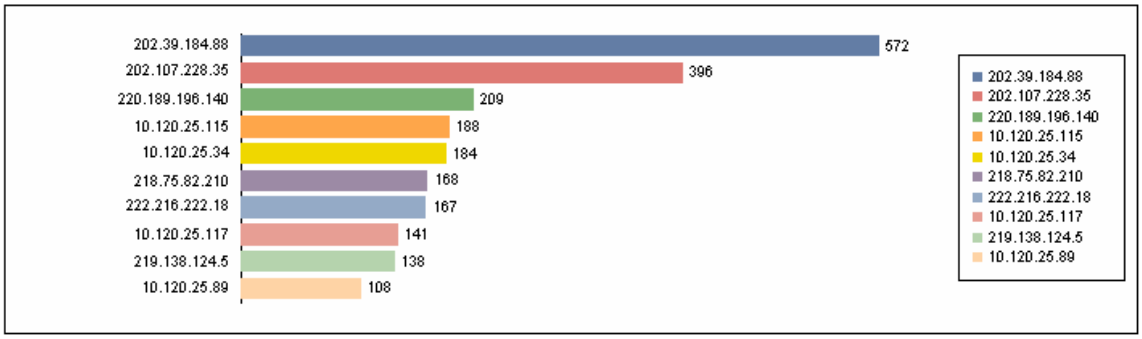
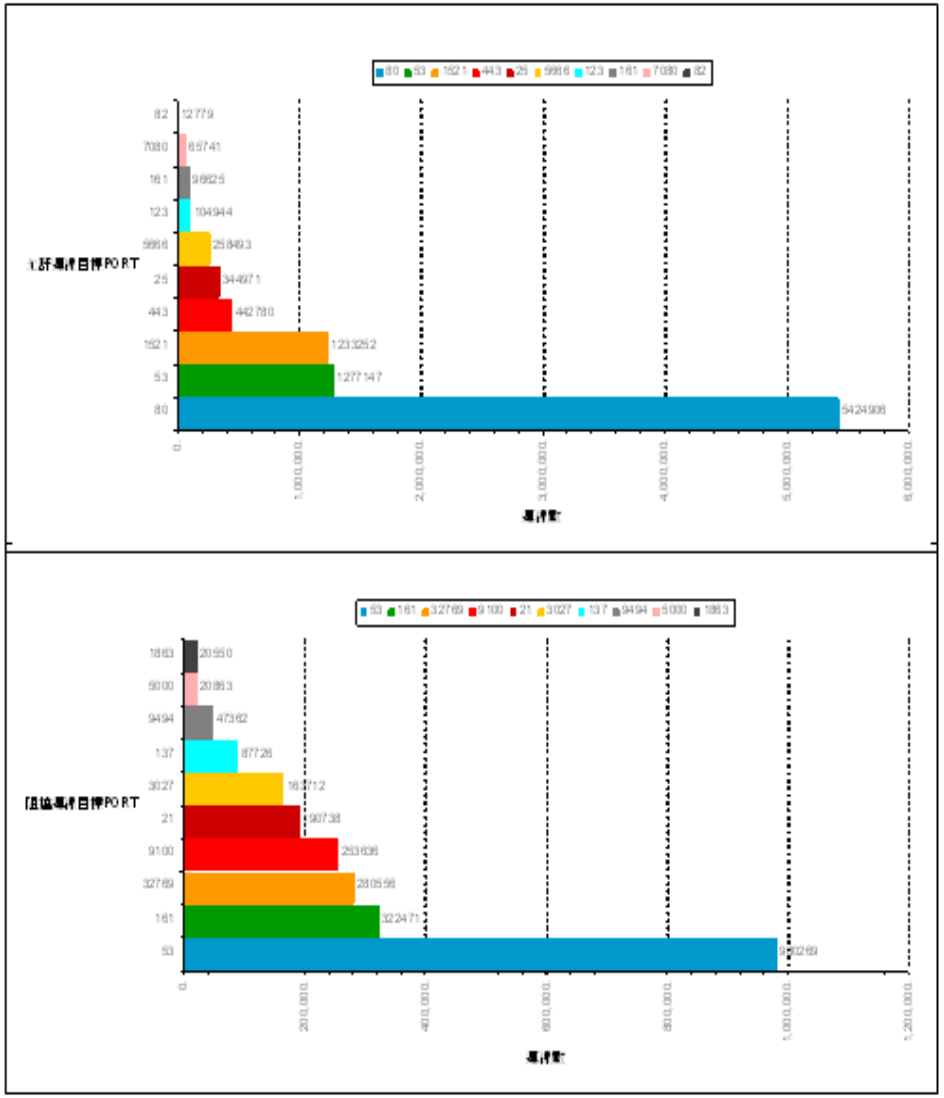


圖 26.　IDS攻擊來源、對象排序統計



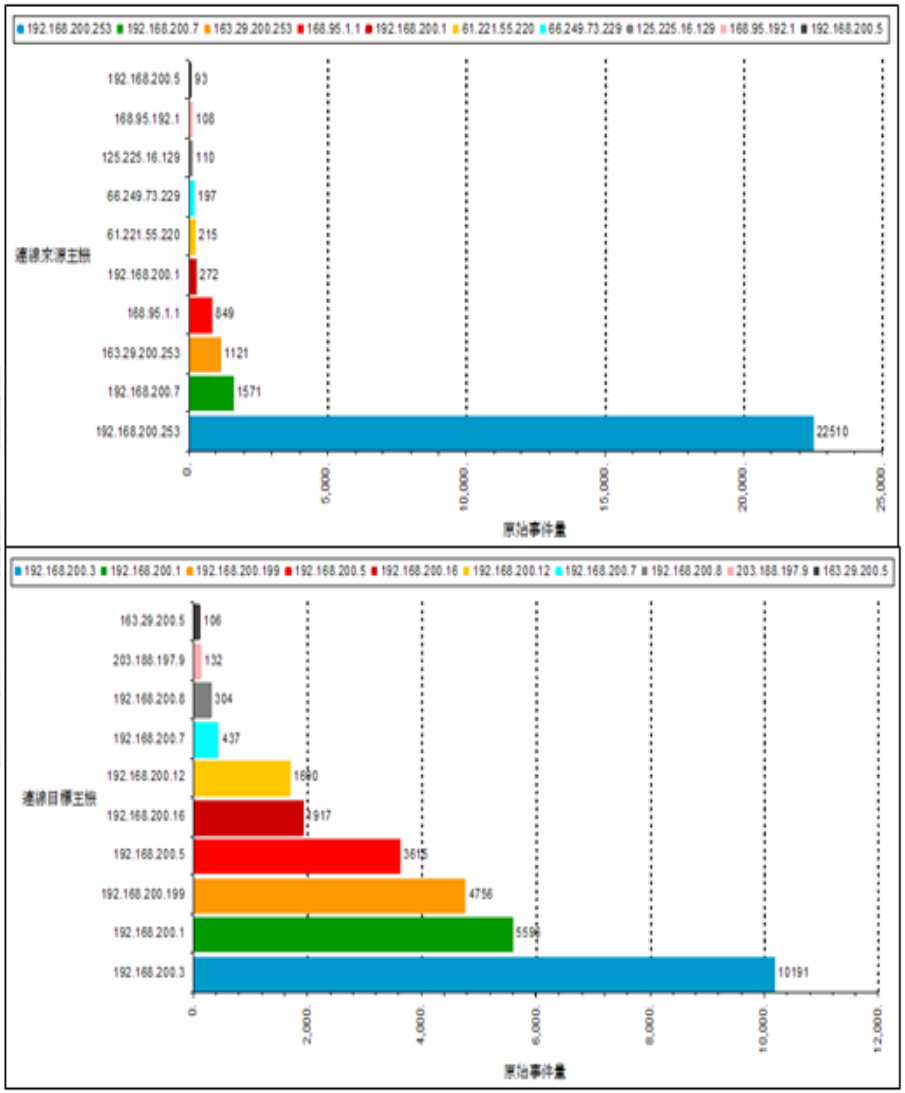


圖 27.　　連線來源/目標主機排序與防火牆阻擋/允許連線目標Port排序

第五節、防毒管理

防毒軟體針對各種已知的病毒(Virus)、惡意程式(Malware)、蠕蟲(Worm)、間諜程式(Spyware)，加以偵測與清除。現在 IT 環境幾乎都有部署防毒軟體，防毒軟體的表現，如果利用防毒軟體偵測到多少病毒來衡量，並不是一個理想的度量指標，因為電腦中毒在所難免，如果有即時清除，並不是嚴重或需關心的風險。此指標，無法回答防毒軟體整體的有效程度。取而代之的建議使用「部署涵蓋度（Coverage Percentage）」與「病毒健康狀態評分(Virus Scoring）」作為衡量的指標，這兩個指標的意義為：

- 部署涵蓋度－了解實際防毒軟體部署的落差（Implementation Gap）程度，有多少企業的主機尚未完成防毒軟體的安裝。涵蓋度越高，表示防毒的安全控制越佳。
- 病毒健康狀態評分 –反映企業內部病毒控制的狀態，分數約高代表越健康(0-100 分)，。

一、 防毒軟體部署涵蓋度

防毒軟體應於每一部主機都安裝，已安裝防毒軟體的數量，可以透過防毒軟體的中控台取得總數量。沒有安裝防毒軟體的主機，在防毒軟體的中控台不會有註冊登記的資料。為了要掌握企業內還有多少主機沒有安裝防毒軟體，可以透過線上掃瞄工具，檢測有多少活動的 IP，再由此數據與防毒中控台的登記內容比對，即可以算出部署涵蓋度。防毒軟體部署涵蓋度的計算方法如下，其中 *Coverage%* 表示部署涵蓋度，*AVInstalled* 表示已經安裝防毒軟體主機數量，*TotalNumber* 表示利用掃瞄工具檢測出來的主機數量。

$$Coverage\% = \frac{AVInstalled}{TotalNumber}$$

方程式 1: 防毒部署涵蓋度

SEP Setup Rate(%)	Host Infection Rate (%)
87	2

圖 28.　　防毒部署涵蓋度與感染率

（圖 28）顯示，Symantec SEP 防毒軟體的部署涵蓋率為 87%。

二、 病毒健康狀態評分

對於病毒中控台轄下所有主機，每小時更新一次狀態並予評分，並儲存於資料庫提供趨勢分析使用。評分標準需要從防毒中控台取得以下四個參數：

- 已經安裝防毒軟體總數(AVInstalled) ：防毒中控台登記的主機數量。
- 未納管(None)：新加入網路的電腦，未在防毒中控台中註冊、登記。此類電腦違反對電腦的控管政策，扣分最重。
- 重大(Critical)：該電腦感染大量病毒（預設 1 小時內染超過 10 個病毒），或過長時間（預設連續七天）未向管理工具回報，病毒碼太舊（預設病毒碼版本落後兩個版次或以上）等，均歸屬到重大。
- 警告(Warning)：一定時間未與管理工具回報（預設三天），或一定時間內未更新病毒碼（預設三天）。

有了以上的參數以後，設計公式，計算分數。

$$VirusScoring = 1 - \frac{(None \times 3 + Cririal \times 2 + Warining)}{(None + AVInstalled)}$$

方程式 2: 病毒健康狀態評分

以上計算方式：

- 最佳狀態為 100% – 代表 None=0, Critical=0, Warning=0，也就是說沒有未納管主機，且沒有發生重大或警告的事件。
- 最差狀態為-200% - 代表 AVInstall=0 (因為 AVinstalled=0, 所以 Critical=0, Warning=0）

表8 病毒評分試算

None	AvInstalled	Cririal	Warning	Scoring	說明
0	100	0	0	100.00%	全部電腦都安裝了防毒軟體，沒有發生Critical與Warning的事件
0	100	10	10	70.00%	全部電腦都安裝了防毒軟體，發生10%與Critical與Warning事件
20	80	10	10	10.00%	80%電腦安裝了防毒軟體，發生10%與Critical與Warning事件
50	50	10	10	-80.00%	50%電腦安裝了防毒軟體，發生10%與Critical與Warning事件
80	20	10	10	-170.00%	20%電腦安裝了防毒軟體，發生10%與Critical與Warning事件
100	0	0	0	-200.00%	全部電腦都沒安裝防毒軟體，Critical, Warning事件為零

（表 8 ）試算某一企業，以電腦總數為 100 台為例，不同的防毒覆蓋率狀況下，試算其最終病毒評分，(圖 29）是實際評分結果的即時狀態畫面。

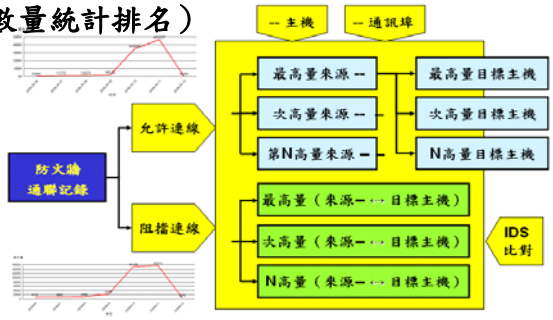
	單位甲	單位乙	單位丙	單位丁	單位戊	單位己	單位庚	統計
未納管	0	3	0	0	0	0	0	3
重大	8	1	0	5	0	11	0	25
警告	4	1	0	3	3	4	0	15
總數	574	880	340	997	965	1275	403	5434
評分	95.12	98.19	100	98.19	99.69	97.1	100	98.33
連線狀態	正常	正常	正常	正常	正常	正常	正常	
10天以上未更新節點	節點狀態	節點狀態	節點狀態	節點狀態	節點狀態	節點狀態	節點狀態	
全部更新	更新	更新	更新	更新	更新	更新	更新	

	單位甲	單位乙	單位丙	單位丁	單位戊	單位己	單位庚
今日	95.12	98.19	100	98.19	99.69	97.1	100
一周	98.54	96.63	99.94	96.34	94.87	97.79	99.66
一月	98.88	97.21	99.9	96.58	97.44	97.23	99.79
半年	98.46	96.06	99.38	96	97.11	95.5	98.12
一年	98.46	96.06	99.38	96	97.11	95.5	98.12

圖 29.　病毒健康評分範例

第六節、技術管理指標彙總

表9 技術管理指標彙總表

<table>
<tr><th colspan="2">組態管理</th><th colspan="2">系統弱點管理</th></tr>
<tr><td colspan="2">☑使用標準版本主機數量與比率(%) I
☑關鍵系統監控數量與比率(%) II
☑日誌記錄完整度與涵蓋度(%) III
☑系統校時涵蓋度(%) IV
☑緊級組態調整反映時間 V</td><td colspan="2">☑弱點嚴重度分佈指標 (%) VI
☑每一主機弱點分佈 (%) VII
☑弱點發掘的延遲時間 VIII
☑弱點補強循環時間 IX</td></tr>
<tr><th colspan="2">系統補強管理</th><th colspan="2">防毒管理</th></tr>
<tr><td colspan="2">☑未達Patch Level數量(%) X
☑Patch延遲時間 XI
☑Patch時間服務水準影響時間 XII</td><td colspan="2">☑防毒軟體部署涵蓋度 (%) XIII
☑健康狀態評分(-200%～100%) XIIII</td></tr>
<tr><th colspan="4">網路閘道安全 XV</th></tr>
<tr><td colspan="2">☑防火牆監控統計資料（主機&通訊埠之流量、通過&被阻擋之流量、流量之數量統計排名）
 
</td><td colspan="2">☑入侵偵測系統監控統計資料（觸發事件主機排名、觸發事件類別之排名）
 
</td></tr>
</table>

第五章　營運管理指標

在技術管理部份，已經對個別設備設計各種度量指標，主要目的是要確保所有設備均運作在正常的狀態，並透過績效評估指標的測量，來有效管理這些設備。但是單一設備的表現，無法呈現整理營運品質的良窳，營運管理有別於技術管理，是將各種不同來源的日誌，加以綜合分析比對後，得出關心的度量指標，本章說明營運管理指標的內容。

第一節、風險研判與分級

一、 分級研判的不同階段

資安事件通常源自系統運用關聯性分析規則對原始事件進行初步的篩選，再輔以技術人員的專業判斷。資安事件產生時必須同時對其嚴重性（優先度）加以分級，以便在後續處理能據以決定該投入的資源、通報對象的等級、處理的時效。資安事件分級處理分為三個階段：「原始事件階段（設備原始定義）」、「系統分析階段（系統關聯性分析結果）」、「專業分析階段與通報（最終研判）」（圖 30）。

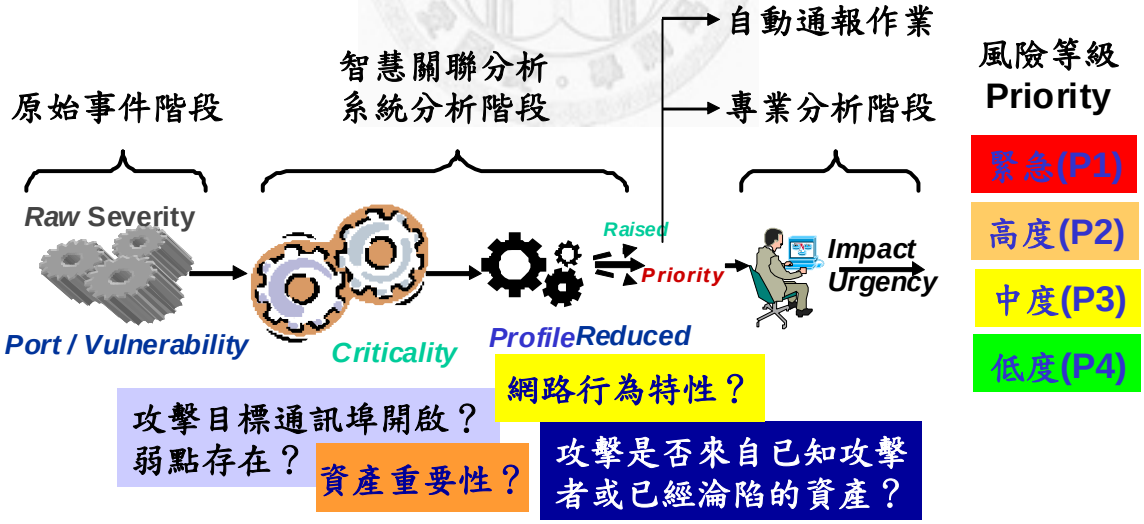


圖 30.　　資安事件風險研判與分級

上述三階段之主要內涵如下：

- 原始事件階段：將監控設備的原始事件資訊權重一致化，以利後續的作業分析。

- 系統分析階段：利用系統內建的資產資料與分析功能，將事件賦予符合監控環境實務狀況的重要性。
- 專業分析階段與通報：如資安事件是屬於高精準度的類別，則由系統直接發出通報；否則則由資安工程師以其專業判斷確認事件的真偽與優先度，再進行通報。

綜合而言，三個階段的分級處理是否完善，必須仰賴「SOC 平台功能」、「完整環境資訊」、「營運人員能力與經驗」三方面的密切配合，於以下分別詳細說明。

（一） 原始事件階段

此階段之作業目的是將不同廠牌、不同資安設備所產生的各種事件不同等級定義，化為一致的優先等級，稱為「優先等級正規化」。網路、資安設備將原始的事件訊息送到 SOC 資安系統後端平台後，系統會依據設備送進來的訊息內容，比對系統內的等級對應表，重新賦予 0 到 10 的優先等級。原始事件階段主要依賴 SOC 平台內建資料庫的完整度，只要 SOC 支援該型設備，則優先等級便可以決定。

（二） 系統規則分析階段

當 SOC 平台後端對原始事件正常化後，會依據內建的關聯性規則與各種環境資訊（如：系統弱點或是資產重要度）調整事件等級。判斷的依據包括：

- 對資產之瞭解與掌握度。
- 目標被攻擊的容易程度，例如：目標 Port 是否開放、是否存在對應弱點。
- 攻擊者、受害者的歷史紀錄：如是否來自已知的攻擊者、事件是否來自已淪陷資產。
- 資產重要性。

SOC 後端系統會依據上述四項目的資訊，賦予 0~10 的權重，經過加權的方式得出一個綜合優先度，加權分析之邏輯（圖 31）。

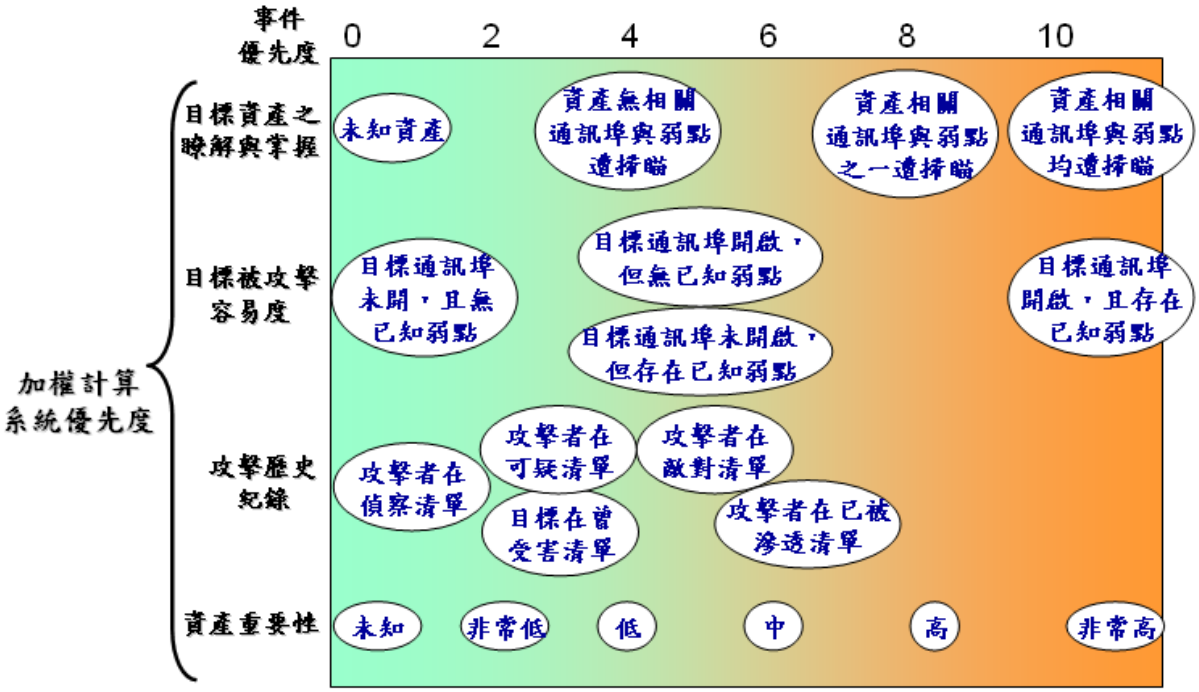


圖 31.　　系統分析事件優先度邏輯

二、 事件分級計算方法

由於 SOC 平台是可以跨越不同設備進行分析的，所以 SOC 平台在取得最基礎的優先等級後，還會根據實際情況將等級予以增減，以便更符合實際的監控狀況，提升監控水準。舉例來說，若部署在防火牆外的入侵偵測系統，偵測到多個外部主機對內部的攻擊行為，但是該攻擊已遭防火牆阻擋。此時我們就會希望將入侵偵測系統 agent 所回報的事件等級予以減分，甚至降為 0 分，以便我們能夠更專心的處理其他真正可能會造成影響的問題，所以我們就會需要一些變數和演算法，來對事件等級進行加權或減分。

（一） 平台計算

SOC 平台事件的優先等級，會依據下面四個變數值，對 agent 所回報的事件等級予以增減。（表 10 ）的參數，下表中數值最小值為 0，最大值為 10。

表10 優先權計算加權變數

變數	說明	數值
模式可信程度 - (Model Confidence	資料庫沒有這個資產	0
	有該資產但是沒有對開啟的通訊埠及弱點進行掃瞄	4

對目標資產瞭解程度)	有該資產但是只對開啟的通訊埠或弱點均進行掃瞄	8
	有該資產且有對開啟的通訊埠及弱點進行掃瞄	10
相關性 – (Relevance 目標容易被攻擊的程度)	目標通訊埠未開且沒有存在已知弱點	0
	目標通訊埠是開啟狀態但是沒有存在已知弱點	4
	目標通訊埠是關閉狀態但存在有已知的弱點	8
	目標通訊埠是開啟狀態而且存在有已知弱點	10
嚴重度 - (Severity 攻擊者與受害者的歷史記錄)	攻擊者在已滲透清單中	6
	攻擊者在敵對清單中	5
	攻擊者在可疑清單中	3
	攻擊者在偵察名單中	1
	目標在曾經受害清單中	3
資產重要性 – (Asset Critically)	非常高	10
	高	8
	中	6
	低	4
	非常低	2
	未知	0

- 「相關性 (Relevance)」為 0 時優先權永遠為 0；其值為 10 時，優先權等同 agent 回報的事件等級。
- 「模式可信程度(Model Confidence)」有可能降低「相關性」所產生的影響。如果「模式可信程度」為 0，則「相關性」在整體計算中不產生任何影響；如果其值為 10，則優先權計算遵守前一敘述。綜合上述兩項因子的一般性加權公式為：

$$\text{優先權} = \left(\frac{\text{相關性}}{\text{相關性} + \text{模式可信度} - \text{相關性} \times \frac{\text{模式可信度}}{10}}\right)$$

方程式 3: 優先權計算

- 如果「嚴重度(Severity)」為 10，將 agent 回報的事件等級加 30%。其加權公式為：

$$(1+\text{嚴重程度}\times\frac{3}{100})$$

方程式 4: 嚴重度影響優先權計算

- 如果「資產重要性」為 10，則將 agent 回報的事件等級加 20%；但若低於 8，則反而減少其值。其加權公式為：

$$[1+\frac{(\text{資產重要性}-8)}{10}]$$

方程式 5: 資產重要性影響優先權計算

- SOC 平台最後的優先權，則是由上面四個加權因子，經過加權公式計算後得來。

依據上述原則，當事件的封包內容或是行為模式合乎攻擊行為的規則時，就會觸發對應的警訊；例如：2 分鐘內發現 login Fail 的次數超過 5 次，就會觸發嘗試猜測密碼失敗的警訊。此時系統會再依據攻擊的來源或是被攻擊主機的資產價值，以及其弱點資料庫、開啟 Port 的資訊等，與資安設備所採取的動作進行交叉式比對分析，進行第二次的優先等級判斷，再一次的重新賦予 0 到 10 的優先等級。（表 11 ）。

表11 交叉分析決定事件最終優先等級

	IDS	FW	資產價值	弱點	優先等級
Alert1	Attack	Drop	Low	-	0
Alert2	Attack	Accept	Low	-	2
Alert3	Attack	Accept	Medium	Mismatch	4
Alert4	Attack	Accept	Medium	Match	8
Alert5	Attack	Accept	High	Match	10

由於資產特性、弱點資料庫、開啟的 Port 的屬性緣故，一個原始等級為 9 的高等級事件，可以因為被攻擊主機並未開啟相關的 Port 而可能會成為一個中等級為 5 的資安警訊。反之，一個原始事件等級為 6 的事件，可能因為該主機不僅有開啟被攻擊的 Port，而且是公司重要的網站，而觸發一個等級為 10 的嚴重警訊。

綜合上述，事件優先度的系統分析是否有效，SOC 平台先天性能的優劣並非唯一的因素，幾項後天之營運管理因素更為關鍵：

- 設備資產資訊是否完整定義
- 設備資產弱點是否透過弱點掃瞄完整建立，並定期更新
- 各項設備相關互動的關聯性分析規則是否完整建立

因此 SOC 平台建置完整度、維運經驗的豐富度，對於事件優先度的訂定是相當重要的。

（二） 專業分析與通報階段

某些類型之資安事件型態如出現頻繁，則應視為標準事件，將其分級、通報作業加以系統化、自動化，並配合設計通報的標準樣版內容。一旦規則觸發，只需載入事件資訊至樣版檔案，便可即時發出通報。SOC 依據豐富的維運經驗，自動化通報事件的比例持續提升，不但可以掌握時效，也可保證通報內容的完整性，並留下更多時間給監控維運工程師去處理需要人為專業判斷的事件。

如資安事件尚未納入自動化、標準化之範疇，則需啟動 SOC 資安工程師的專業分析程序；因此就通報品質而言，除 SOC 系統本身的功能優劣外，維運人員的素質也是極為關鍵。一般 SOC 平台內建之各種偵測規則雖然已經十分精確，仍無法保證 100%精確，需要有一定程度的人為專業分析，確認事件本身的真實性，以達到降低誤判率、提高準確度的目的。專業分析的影響項目有三：

- 影響程度(Impacy)：規則觸發之後，資安工程師會參酌事件圖驗證事件的真實度，瞭解比對事件內容，剔除明顯的誤判行為。
- 緊急程度(Urgency) ：每一個系統到影響後，要恢復的緊急程度不一樣，需要越快恢復的事件，其實件的等級越高。
- 參酌網路現況交換的資安情報：根據最新資安情報，如 Zero Day Attack 等事件；亦會依據網路時勢進行嚴重度之研判。資安工程師將參酌此類情報，研判該事件的影響程度。

Urgency	high	medium	low
可用度急迫性	需立即恢復	允許短暫中斷	不具迫切性
處理時間急迫性	需於24小時內處理	容忍極限為2-5天	可容忍6天(含)以上
當二個指標中的任一項條件成立時，選擇最高值為緊急程度			

Priority	影響程度 (Impact)			
緊急程度 (Urgency)		High (7-10)	Medium (4-6)	Low (0-3)
		一級資產遭受攻擊/感染，或病毒具感染力	非一級資產遭受攻擊且病毒不具感染力	事故不會造成危害或是誤判
	high	1	2	3
	medium	2	3	4
	low	3	4	4

圖 32.　　Priority判定原則

SOC 最終的風險通報分級共定義四個等級：Low（低）、Medium（中）、High（高）、Urgent（緊急），其中除 Low（低）等級外皆會進行通報：

- Low（低 1-3）：事件不會造成危害或是誤判，客戶不需處理。對於 Low 的警訊，將不會通報客戶。
- Medium （中 4-7）：事件有可能會影響資訊安全，但是沒有立即的危害，但是仍建議客戶進行後續的調查與處理。
- High（高 8-9）：事件有明顯的攻擊意圖，客戶應該儘速處理。
- Urgent（緊急 10）：事件已經嚴重影響資訊安全，且通常發布資安警訊的同時，攻擊行為仍舊持續中，需請客戶立即著手處理。SOC 依據與客戶簽訂的服務水準協定，進行必要的電話，簡訊，Email 通知相關人員。

通常 SOC 會將下列事件列為緊急事件：

- 惡意程式攻擊（入侵工具、後門木馬型）。
- 資訊作業服務遭惡意中斷。
- 非經授權的機密資訊存取成功。
- 重要資料遭竄改、刪除或盜用。
- 網頁惡意入侵竄改。
- 內部主機跳板攻擊。

緊急事件之作業需要使用者、維護廠商、系統管理者及資安事件專家之整體合作，方能在短時間之內有效回應，降低對原有作業之影響。最終警訊通報的等

級，如遇有下述特殊需求，亦可調整其等級：

- 與客戶有特殊約定者（例如同樣是刺探行為，A 客戶認為不需通報，但是 B 客戶認為極為重要）。
- 特殊敏感期間的事件，如兩岸國慶期間、國際駭客大規模攻擊、攻防演練期間等，將提昇等級。
- 符合國際資安情報之事件特性者，將提昇等級。
- 當事件同時觸發多種不同嚴重等級時，取最高等級發佈。
- 當通報過的事件重複發生時，必要時提升等級後再次發報。

第二節、風險等級指標

風險等級由上一節中，綜合參考各種因素後，最後給予 Priority 1-4 的等級。根據資安事件風險等級，可以設計風險等級測量指標[17]。

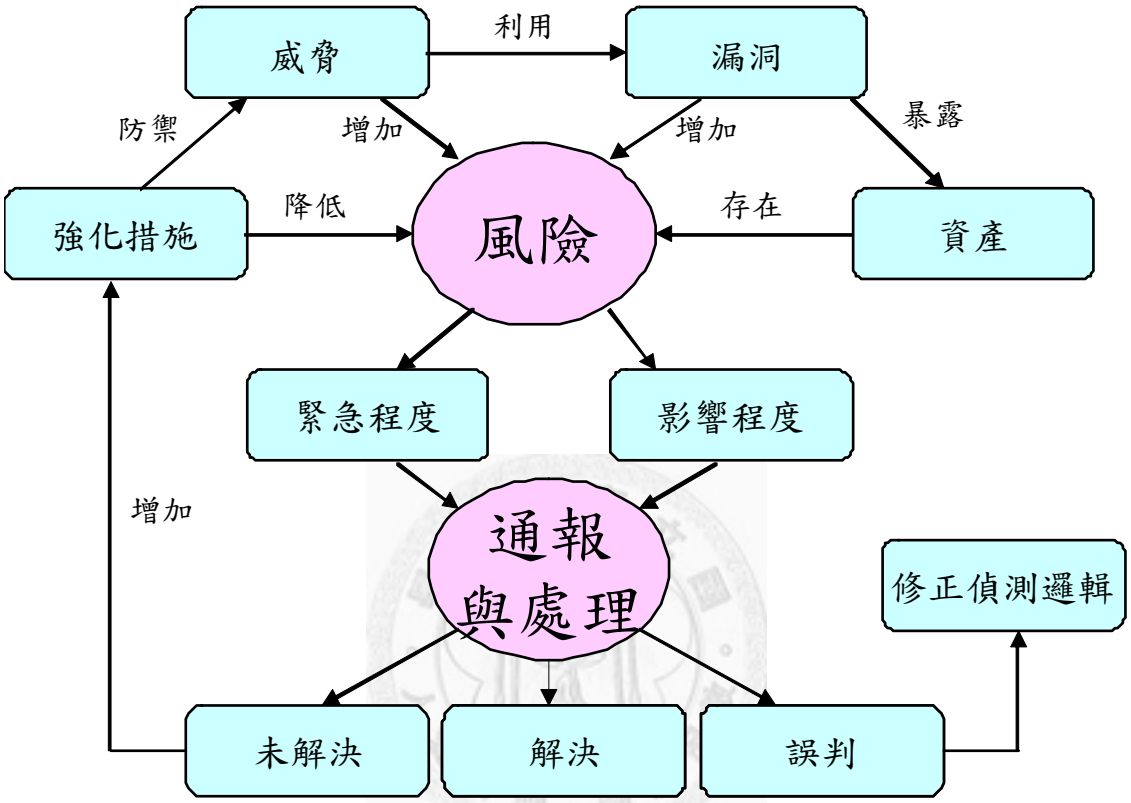


圖 33. 風險等級指標

一、 總風險與總避險指標

風險係數			總風險(Risk)
Priority (P*i*)	權重 (W*i*)	發生次數(N*i*)	
1	10	N1	$R = \sum_{i=1}^{4} (Wi \times Ni), Ni \in N$
2	7	N2	
3	4	N3	
4	1	N4	

方程式 6: 總風險指標

每一個分類出來的風險等級，代表不同風險嚴重度，可賦予不同權重如（方程式 6），得到總風險指標。此指標是指在某一個統計區間內，發生資安事件的整體風險程度，數值越高，代表風險越大。

避險係數			總避險 (Hedged-Risk)
Priority (P*i*)	權重 (W*i*)	解決數量(R*i*)	
1	10	R1	$HR = \sum_{i=1}^{4} (Wi \times Ri), Ri \in N$
2	7	R2	
3	4	R3	
4	1	R4	

方程式 7: 總避險指標

每一個風險事件，發出通報後，將會有處理流程加以處理，處理完成的代表該風險已經解決，該風險已經有效規避。我們可以根據處理完成的數量，計算總避險指標（方程式 7），避險指標越高，代表處理風險的能力越強，整體的風險越低。

二、 風險收斂比

有了上述總風險指標（*R*）與總避險指標（*HR*），可以計算風險收比 Risk Convergence Ratio:

$$RC\% = \frac{HR}{R}$$

方程式 8: 風險收斂比

RC%越高（最高=100%），代表風險控制能力越強，RC%越低，表示風險控制能力越低。

第三節、關聯分析規則品質指標

關聯分析規則是將收集到的原始事件，與過去已知案例進行智慧型比對，以及對不同的資料群間作關聯性的分析，判斷出最有可能的攻擊型態與來源。由於 SOC 平台是可以跨越不同設備進行分析，SOC 平台服務的有效性、效率與準確性，關聯分析規則的品質有決定性的影響。本節設計關聯分析規則品質的測量指標，包含以下幾個部份：

- 規則設計數量：關聯性分析規則越多，表示 SOC 的營運智慧越充足。
- 規則觸發量：關聯性分析規則設計完成，除了多寡以外，還要檢討觸發的次數，檢視關聯分析規則的品質，如某一規則完全不觸發或觸發數量過低，需檢討關聯性規則設計邏輯的妥適性；反之若規則觸發太多，是否條件設計太過寬鬆，導致觸發的頻率過高的狀況發生。
- 規則自動化數量：透過上述檢討與調整後，對於精準度甚高，且可以套用通報範本的規則，則可以加以自動化處理。自動化程度越高，需要投入的人力資源相對的較低，寶貴的人力資源，可用來繼續發掘值得關注的資安事件，並設計新關聯分析規則。
- 規則停用數量：觸發的規則，若證實誤報（如邏輯錯誤或因為環境特性，不會符合設計的條件），則應該停用。SOC 不應該一味追求很多的關聯分析規則，而是要有精準與高品質的規則。本項指標可以用來淘汰貢獻度不佳或是因為環境、時空變動而不適用的規則。
- 半自動通報規則數量：通報數量減去自動通報數量，就是半自動通報規則的數量，此數量代表需要人工介入，耗費人力的程度。半自動規則越少，值班人力的工作負荷越低，反之則越高。

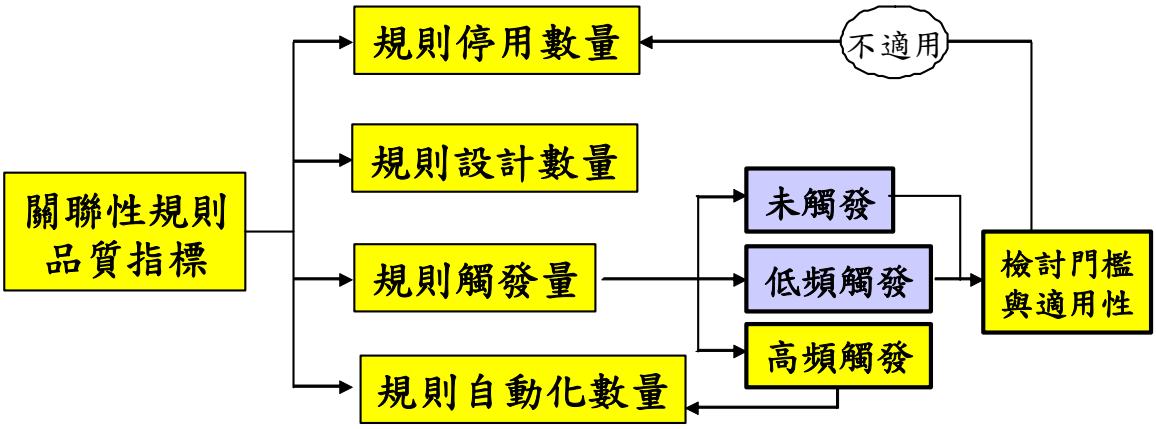


圖 34.　　關聯性規則品質指標

一、 規則數量

關聯性規則數量統計，可以直接由 SOC 平台計算規則的數量，了解關聯分析規則變化的趨勢。(圖 34) 是關聯分析規則數量統計的範例，可由此指標評量 SOC 營運品質的參考項目之一。

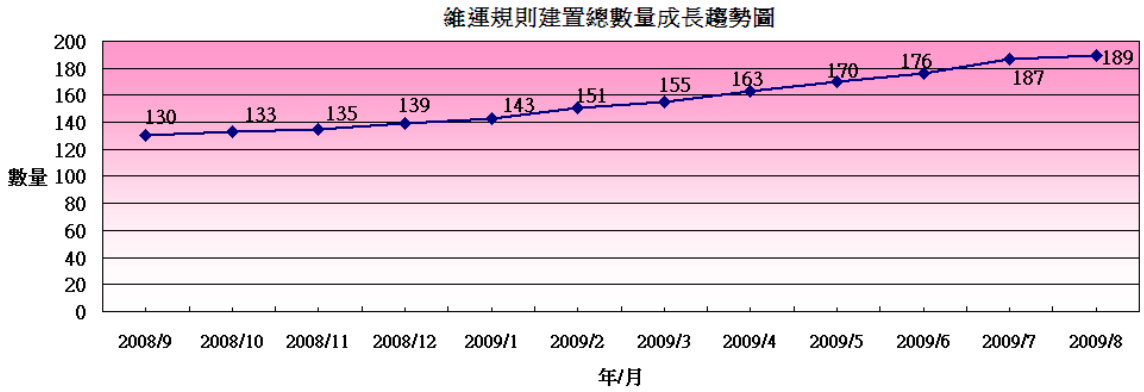


圖 35.　　關聯性規則數量折線圖

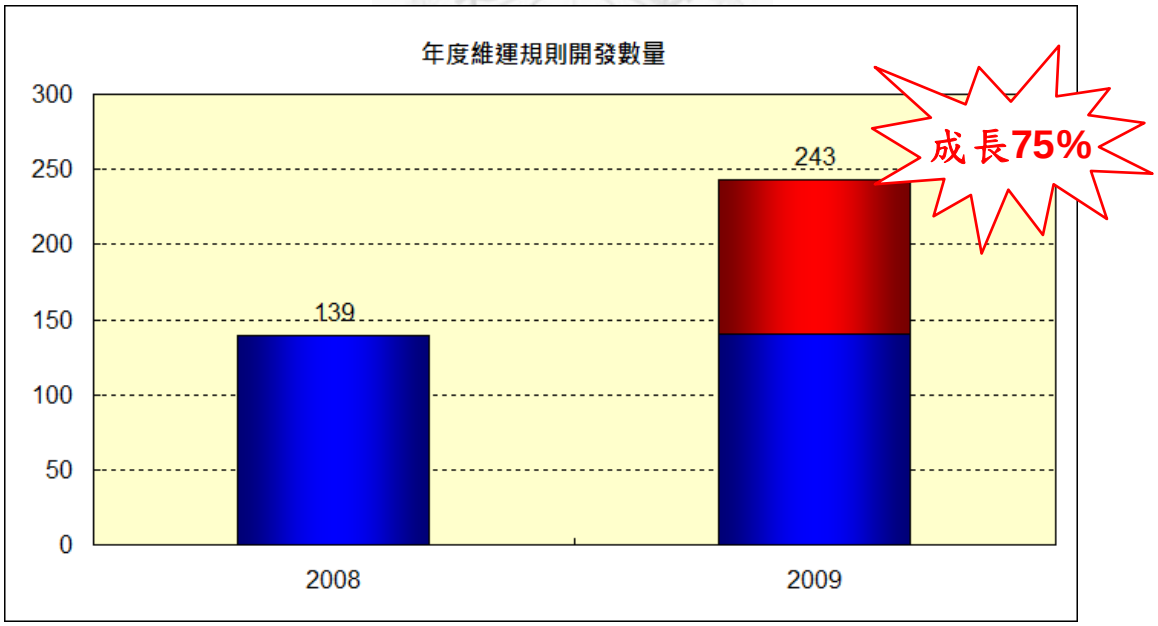


圖 36.　　關聯性規則數量比較圖

關聯規則數量不需追求絕對數量的多數，有幾個因素影響讓關聯規則的數量：

- 資安事件的攻擊手法改變，過去適用的分析規則不再有效，透過 (圖 34) 規則停用的檢討程序，會使關聯規則數量下降。
- 環境發生異動或監控標的增加，造成關聯分析規則的門檻、邏輯與關聯分析的內容發生改變，造成關聯規則變多。

二、 規則觸發數量

規則觸發數量統計用來衡量每一個規則貢獻度，並依照以下原則檢討規則是否需要調整：

- 對於觸發數量很高者：了解條件是否過於寬鬆，如果過於寬鬆，應酌予調整門檻或條件，以免相同的事件不斷重複通報。如果條件合宜，那要了解觸發的原因，並加以解決（如 IDS 需要調校，降低 False Positive），減少相同規則不斷觸發的次數。
- 對於觸發數量很低者：了解條件是否過於嚴格，如果過於嚴格，應酌予調整門檻或條件，放寬符合的標準。如果條件合宜，需要再度確認規則有無邏輯的錯誤，導致永遠不會發生而不自知。

透過上述的方式，可以控制規則的品質，以免濫竽充數或是規則無用，虛耗 SOC 的運算資源，（表 12 ）是規則修正與調整的範例。

表12 規則調整表

調整規則名稱	日班建議調整項目
(Auto)(木馬)內網網路芳鄰對外異常連線	此規則為Discovery平台上週觸發第1名，甲公司佔絕大多數，調查後發現，其目標IP多入內部主機網段192.168.0.0/24，內對內的網路芳鄰屬正常現象。將內部主機網段192.168.0.0/16加入"/所有過濾規則/客戶過濾規則/甲公司/目標為客戶IP"中
(Auto)(異常)對外單一主機大量阻擋	此規則為Discovery平台上週觸發第2名，調查後，其行為大部分為對外單一主機單一port大量阻擋，故將條件"目標連線埠"加入"欄位不相同時進行彙總"於三個平台之中
(Auto)(入侵)內對外可疑傳送行為	此規則為Enterprise平台上週觸發第1名，乙公司佔絕大多數，調查後此規則條件為2分鐘15筆、傳送位元組>接收位元組且其大小大於1MB。經調查乙公司業務需要，傳送之公司交易紀錄，多為600k-1.5M之間，修訂規則大於1.5MB才告警。
(Auto)(異常)(IPS)單一來源IP觸發大量阻擋事件	此規則為Freedom平台上週觸發第1名，未集中發生於某一客戶。調查後，此類事件並無明顯異常，目前門檻值太低，建議將門檻值由5分鐘5筆調整為5分鐘20筆。
(Auto)(入侵)外部刺探掃描行為	此規則為Discovery平台上週觸發第3名，丙公司佔絕大多數，調查後發現，其來源IP為微軟與Google網段皆可濾除，與對目標IP 10.19.0.13 Arcsight主機可濾除，門檻值由10分鐘100筆已不需調整。

三、 規則停用數量

（表 13 ）是規則觸發統計的範例，可以看出排名第一的規則，是需要優先檢討的對象。相同的規則在不同的環境，也會有不同的表現，因此需要就實際的運作環境，作為調整規則的依據。

表13 規則觸發數量統計表

排名	自動通報-規則名稱		通報數量
1	對外部大量主機連線被FW阻擋	TOP3發佈客戶	423
		行政院衛生署-○醫院	159
		行政院衛生署- ○醫院	42
		○汽車-資安監控委外服務案	34
2	點對點軟體連線行為	TOP3發佈客戶	257
		○發展協會	86
		○電視-資訊安全分析監控服務案	60
		○汽車-資安監控委外服務案	24
3	駭客中繼站轉向連線行為	TOP3發佈客戶	200
		曜揚科技- ○局	37
		內政部○署	27
		行政院衛生署- ○醫院	24
4	已知中繼站連線行為	TOP3發佈客戶	89
		行政院衛生署- ○醫院	27
		○發展協會	21
		○電視-資訊安全分析監控服務案	16
5	內對內主機大量連線遭防火牆阻擋	TOP3發佈客戶	51
		○局	14
		○發展協會	10
		○公司	6

以（表 13 ）為例，關聯規則「對外部大量主機連線被 FW 阻擋」，實際現場調查的結果，大多為 Skype 的連線造成，對於允許使用 Skype 的企業，並不構成安全風險。但此類通報將耗費調查人力，造成人力額外的負擔，有必要加以檢討修正。檢討本規則的判斷邏輯為：

- 事件來源：防火牆事件
- 類別結果：Failure (防火牆加以阻擋的意思)
- 連線目的：非企業主機 (排除對企業自有主機連線行為)
- 除發條件：五分鐘內觸發 900 次以上。

思考問題：

- 客戶主機清單完整否？
- 900 次門檻是否過高？
- 是否因 Skype 等軟體造成誤判與 Skype 活動貢獻次數過多？

表14 事件處理結果範例

序號	單號	類型	處理結果
1	HD0000000666061	對外部大量主機連線被FW阻擋	查無可疑程式,使用者有自行安裝webshots軟體,應該為此軟體所導致
2	HD0000000667744	內對內主機大量連線遭防火牆阻擋	於172.19.1.102的host中發現172.18.1.2 localhost紀錄,疑似為連線的原因,已經先將此筆紀錄移除
3	HD0000000667745	對外部大量主機連線被FW阻擋	為FortiGuard Analysis and Management Service contract validation之連線行為
4	HD0000000668487	對外部大量主機連線被FW阻擋	為McAfee Site Advisor連線行為
5	HD0000000670599	內對內主機大量連線遭防火牆阻擋	為Vmware ESX Server,應為合法連線行為
6	HD0000000673175	對外部大量主機連線被FW阻擋	查無可疑程式,使用者有Skype,應該為Skype所導致
7	HD0000000674020	對外部大量主機連線被FW阻擋	查無可疑程式,使用者有Skype,應該為Skype所導致
8	HD0000000674291	內對內主機大量連線遭防火牆阻擋	為Vmware ESX Server,應為合法連線行為
9	HD0000000676281	對外部大量主機連線被FW阻擋	查無可疑程式,使用者有Skype,應該為Skype所導致
10	HD0000000676322	對外部大量主機連線被FW阻擋	查無可疑程式,使用者有Skype,應該為Skype所導致
11	HD0000000676391	對外部大量主機連線被FW阻擋	查無可疑程式,使用者有Skype,應該為Skype所導致

調整方向：

- 確實排除客戶使用網段：建立客戶使用網段清單（思考：針對目標為客戶使用網段，存在“內對內連線”特性）
- 濾除已知現象：Port Sweep 與 Port Scan 觸發主機清單濾除
- 已知特定服務濾除：如 Patch Server, 防毒主機的更新活動濾除
- 封鎖 IP 濾除：已知的封鎖 IP 事件，不需持續通報，可以濾除。

已知 Skype 活動濾除：Skype 軟體使用將出現一定的 Pattern，首先找尋 Supernode，並嘗試連往其 TCP/80 及 TCP/443 埠，且以上動作於 3 秒內完成，隨即針對相同外部 IP 嘗試 High Port 連線，且連續嘗試連往固定 IP 之同一 High Port 的 TCP 與 UDP（傳輸通訊協定）連線。

經過以上的檢討與調整之後，原有「對外部大量主機連線被 FW 阻擋」規則停用，並新增一個「內部主機對外違反防火牆安全政策事件」規則，以改善此現象。

四、 規則自動化數量

以（圖 37）為例，2009 年自動通報數量為 4, 710 個，佔 2009 年通報總量的 46%，而人工通報（或半自動通報）則有 5,604 個，人工通報部分亦較 2008 年增加 1,498 個，成長率約為 36%。

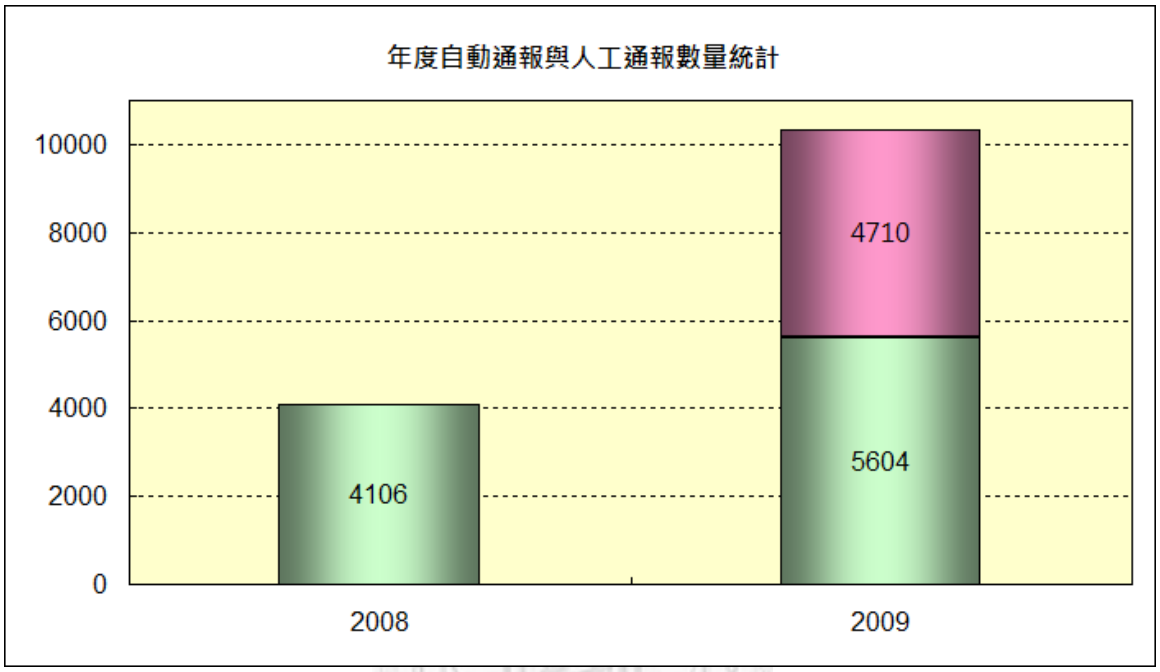


圖 37. 自動通報數量統計

自動通報也不能追求絕對數字的最大化，自動通報可以有高效率、精準與品質統一的好處；相反的卻會有內容僵化與欠缺專業分析的缺點。我們除了檢視自動化通報的比率以外，還要檢討值班人員是否過度仰賴自動通報，而疏於發掘、研究新的關聯規則。因此關聯分析規則自動化的指標，還要看人工通報的比重多寡，綜合的衡量自動通報的數量是否平衡。

五、 半自動規則數量

半自動規則，需要人工介入，藉由值班人員的專業經驗，判斷是否需要通報或可能為誤報。半自動通報數量越多，對於值班人員的工作負荷越高。

第四節、事件通報質、量指標

一、事件通報頻率的控制

符合分析規則，成立為通報事件後進行通報，通報的數量不會等於規則觸發數量，一個資安通報（如病毒事件）發出到完全解決，需要一定的時間，在完全解決前，該行為仍然持續發生中，實務上相同的事件，在通報後一定時間內，不會反複通報，至於應該多久時間內不重複通報，與客戶約定於服務條件中。

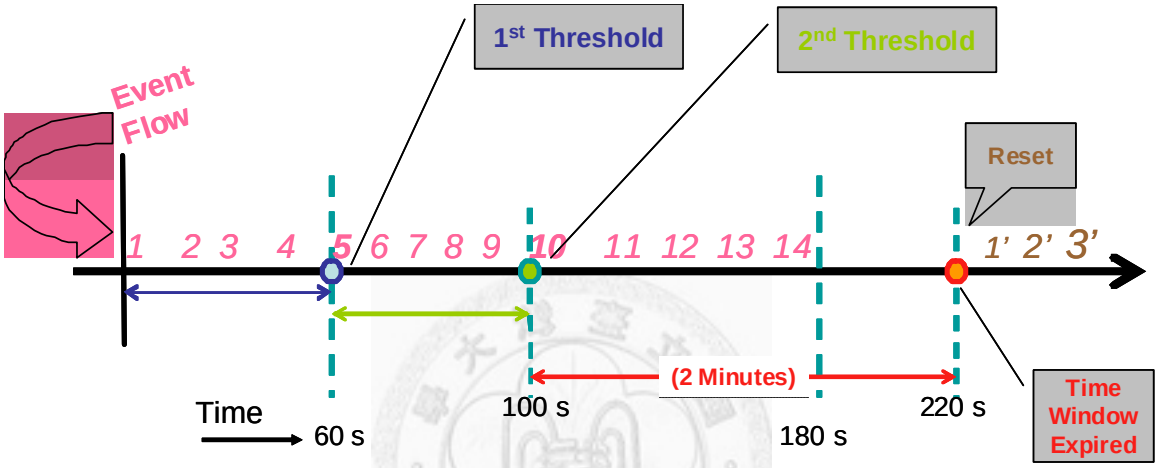


圖 38.　規則觸發時機控制

各種分析規則，一般會伴隨時間區間與發生次數當作是否成立的依據，例如暴力密碼猜測，不會偵測到一次密碼錯誤，就認為是暴力密碼猜測事件。（圖 38）是規則觸發時機的基本控制方法：

- 設定時間區間：可根據事件的本質，決定觸發彈性門檻條件（如 2 分鐘、5 個相同事件）
- 觸發之時機：On First Event，On Every Event ，On First Threshold，On Every Threshold 或是 On Time Window Expired 多種不同觸發時機。

以暴力密碼登入為例，設定 2 分鐘內有 5 次密碼錯誤，就判定為暴力密碼登入。在（圖 38）中，橫軸的數字，代表密碼錯誤登入事件發生，設定不同的條件，其觸發時機的差異（表 15 ）。

表15 事件觸發條件

	觸發點	觸發次數
On first event	5	1
On every event	5,6,7,8,9,10,11,12,13,14	10

On first threshold	5	1
On every threshold	5, 10	2
On Time Window Expired	Time window expired (1')	1

規則觸發後，依照（圖 30）的原則，決定風險等級後通報。本節設計事件通報質、量指標，包含以下幾個部份：

- 事件通報數量：瞭解整體事件通報的數量，比較變化與趨勢。
- 事件通報時效：瞭解一個通報，耗時多久完成通報，此時間可以做為偵測效率快慢的指標。
- 通報精準度：瞭解通報處理結果，分為「正常行為」、「誤判」等，作為通報精準度調整的依據。

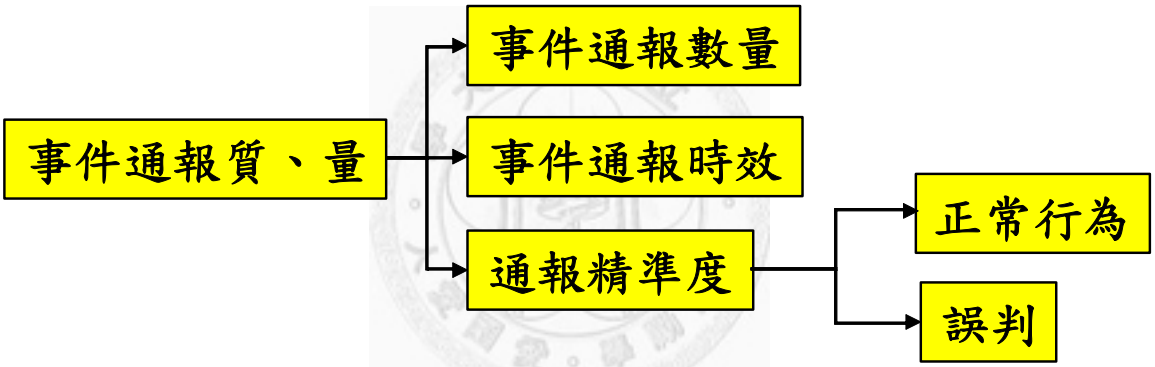


圖 39.　事件通報質、量指標

二、 事件通報數量

事件通報數量，可以分成每月的通報數量統計圖（圖 40），通報類別統計圖（圖 40），來瞭解資安事件的變化。

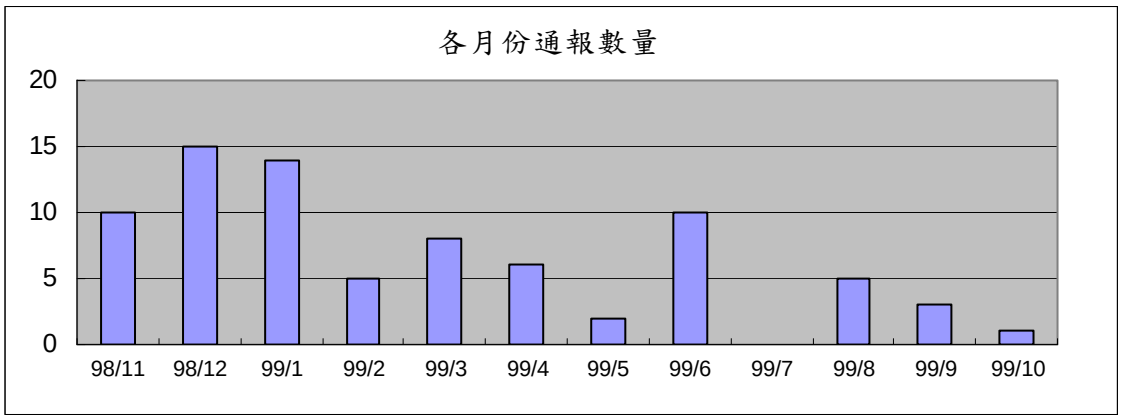


圖 40. 通報數量統計圖

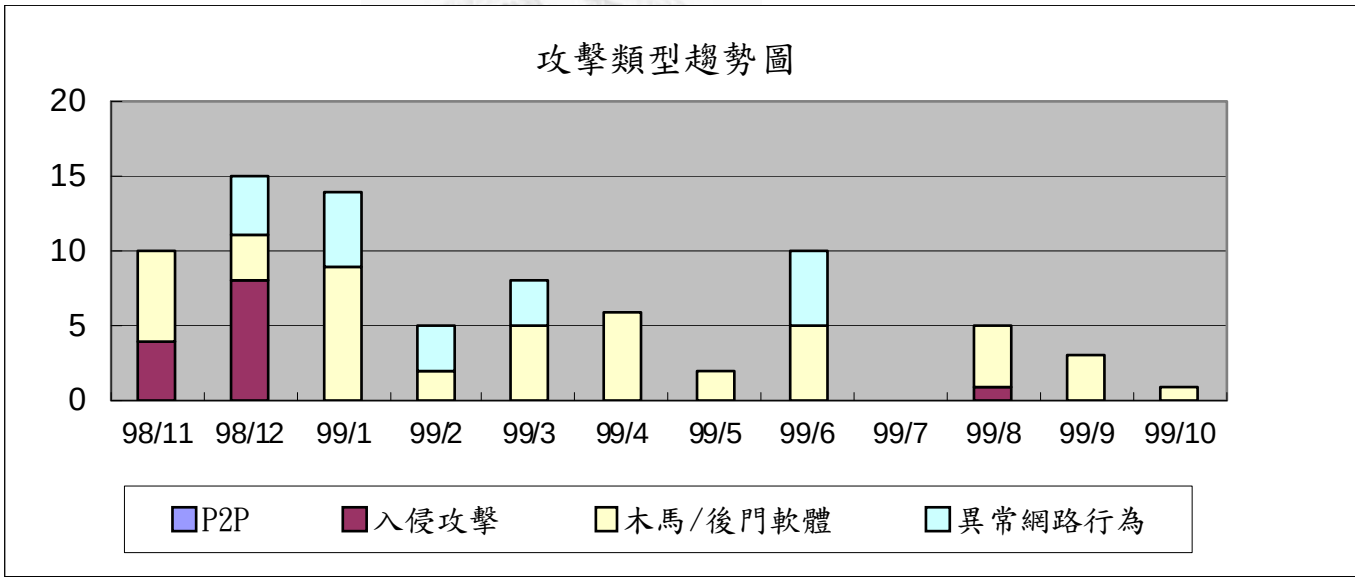


圖 41. 通報類別統計圖

以（圖 41）為例，在 98 年 11, 12 月時，入侵攻擊事件明顯高於其他各月份，經查證該單位為政府機關，入侵攻擊均為行政院資通安全會報進行資安攻防演練所造成，屬於預期的活動，可以解釋該時段攻擊事件增加的現象。

三、 事件通報時效

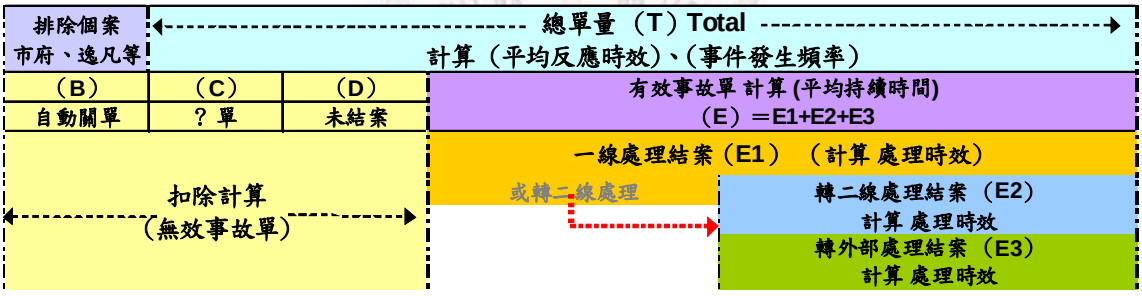
除了自動通報事件，通報時效幾乎是即時外，其他需要專業人員研判、分析後才決定是否要通報，測量通報的時效。衡量通報時效，有兩個重要的管理意義：

- 瞭解維運的效率：原則上希望所有關心的安全風險都能在第一時間發現，這第一時間到底多快，可以透過本指標測量。
- 瞭解人員負荷：值班的作業人員工作量與實際負荷可以有客觀測量指標。

一線人員負責通報，因此一線人員的通報時間，為通報時效。二、三線是事件處理，事件處理的時效，將於（第五章 第五節、三、p.72）中討論。（圖 42）顯示，SOC 通報時效。以 9/2-9/29 共 28 天內為例，總開單數量為 1926 筆，平均一張問題單的處理時效為 9 分 50 秒。如果每一個一線工作人員，一天的投入工時為 8 小時 x0.8（扣除合理的休息時間），則可以估算每一個時段，需要投入 2 個人，此數字可以做為人員工作量負荷的衡量基礎。

平均每天 Ticket 數量	每個 Ticket 耗時	需投入總時間	每人每天工作時數 (以 8 小時 x0.8)計算	至少應投入人數
68	9 分 50 秒	668 分 40 秒	384 分	2 人

表16 通報時效與人力負荷分析表



Site:LT+NH by Weekly 09/02~09/29	第一週 09/02-09/08	第二週 09/09-09/15	第三週 09/16-09/22	第四週 09/23-09/29	Total
有效計算單量 E＝T-B-C-D	834	906	1132	1184	4056（E） E＝T-B-C-D
事故單 持續時間 Avg	2:26:00	2:13:06	2:30:07	2:49:40	2:31:02
1st 處理量（E1）	380	429	507	610	1926
1st 通報時效Avg	0:05:29	0:14:09	0:07:24	0:11:31	0:09:50
2nd 處理量（E2）	378	393	558	501	1830
2nd 處理時效Avg	3:05:31	3:34:24	4:27:32	6:06:17	4:26:13
3rd 處理量（E3）	76	84	67	73	300
3rd 處理時效Avg	9:04:27	7:30:37	5:21:19	8:38:26	7:42:01

圖 42. SOC事件通報時效

四、 事件通報精準度

各種通報處理，均需要回饋回 Workflow 系統，註記處理結果。處理的結果可以分為以下幾種：

- 正常 – 此通報屬於正常行為，需要修正規則，未來不要再加以通報。例如網管主機會對網路內各系統蒐集系統資訊，看起來像是 Port Scan 或 Port Sweep 行為，此行為符合資安事件偵測規則，但是為預期的特定系統所發生，此類事件歸類到正常行為。
- 誤判 – 此通報所指稱的事件，實際驗證後，發現為誤判。誤判時需要調整偵測設備（如 IPS）或關聯分析規則，以降低誤判的比重。

（圖 43）統計圖，呈現事件通報後，有 9%的誤報狀況。

False Postive Count	Closed Count	All Count	False-Postive Rate(%)	Closed Rate (%)
193	1430	2052	9	70

圖 43. 事件誤報率

第五節、事件處理質、量指標

通報發出去以後，將依據分工，由不同專長人員進行事件處理，處理過程，可分為已經解決或者無法解決。對於已經解決者，又可以設計不同的衡量指標，包含以下幾個部份：

- 中繼站數量：截獲新種惡意程式，檢測其對外連線標的，稱為中繼站。連線標的查獲越多，表示事件處理的品質越好，處理的能力越高。
- 新種惡意程式數量：查獲的新種惡意程式數量，數量越多，表示處理能力越好。
- 解決時效：通報發出去以後，多快的速度完成處理，也是一個適當的衡量指標，用來表達事件處理質量好壞的依據。
- 無法解決 – 此問題在一定時間內無法釐清原因或是解決。當無法解決的數量偏高時，需要了解原因，或實施適當的教育訓練，提升技術人員的技術能力，降低無法解決的數量。

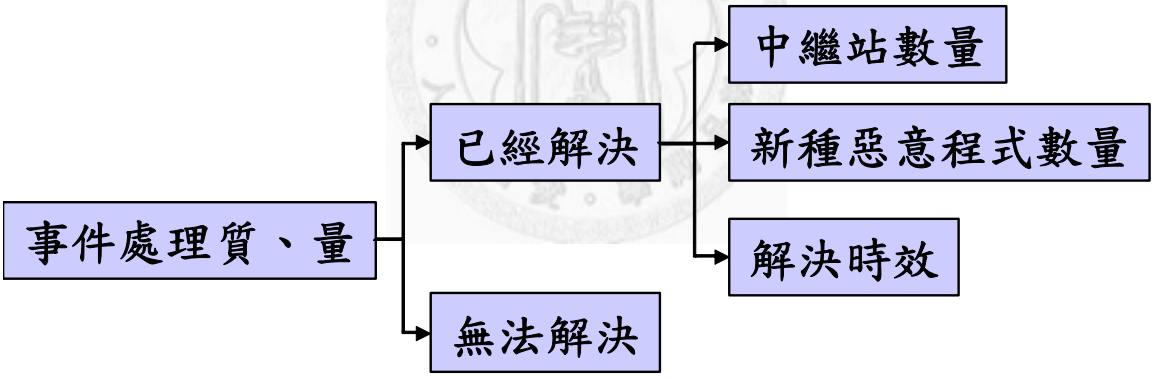


圖 44.　事件處理質、量指標

一、中繼站數量

在破獲惡意程式之同時，SOC 亦會對程式行為加以瞭解，通常亦會對應破獲與惡意程式背後協作之惡意網站、中繼站。（圖 45）為相對之惡意網站、中繼站成長趨勢，此一數量亦可作為分析規則、資安通報準確度之佐證。另外值得注意的中繼站也會因為時、空環境的改變而失效。因此也要有適當的方法來確認、驗證中繼站的有效度。

- 中繼站新增

目前中繼站之取得共有三個來源，分別為“由設備連線紀錄取得”與“由惡意程式、釣魚郵件取得”。

（一） 由設備連線紀錄取得

根據頻寬管理器、入侵偵測系統或防火牆等相關設備取得異常之連線行為，進而推斷連線的來源 IP 或目的 IP、FQDN 可能為中繼站，此時並沒有足夠的證據確認該 IP 與 FQDN 是否真的為中繼站，此時會將相關資訊交由相關資安工程師進行驗證，驗證後若為中繼站則將此 IP 與 FQDN 加入中繼站 IP 與 FQDN 資料庫。

（二） 由惡意程式、釣魚郵件取得

進行事件調查或分析惡意程式時，可取得中繼站 IP 與 FQDN，此類資訊將直接加入中繼站 IP 與 FQDN 資料庫。

- 中繼站排除

透過通報數量統計計算週期內中繼站 IP、FQDN 與通報數量的關係表，進而對中繼站進行排除，中繼站排除分為“中繼站 IP 排除”與“中繼站 FQDN 排除”兩部分敘述如下。

（一） 中繼站 IP 排除

中繼站 IP 排除前必須進行數據的分析，統計週期內中繼站 IP 通報數量，若通報數量為 0 則排除，若通報數量不為 0 則由資安工程師進行驗證。通報數量多不表示真的為中繼站，因此需要由資安工程師對中繼站 IP 進行驗證，若驗證後不為中繼站 IP 則排除，若為中繼站 IP 則進行中繼站與惡意程式關聯紀錄。根據客戶回報資料或資安工程師調查之結果進行中繼站與惡意程式關聯紀錄，以作為中繼站 IP 排除之額外加權指數。

（二） 中繼站 FQDN 排除

中繼站 FQDN 排除較為簡單，只要週期內查詢不到 FQDN 即可排除。

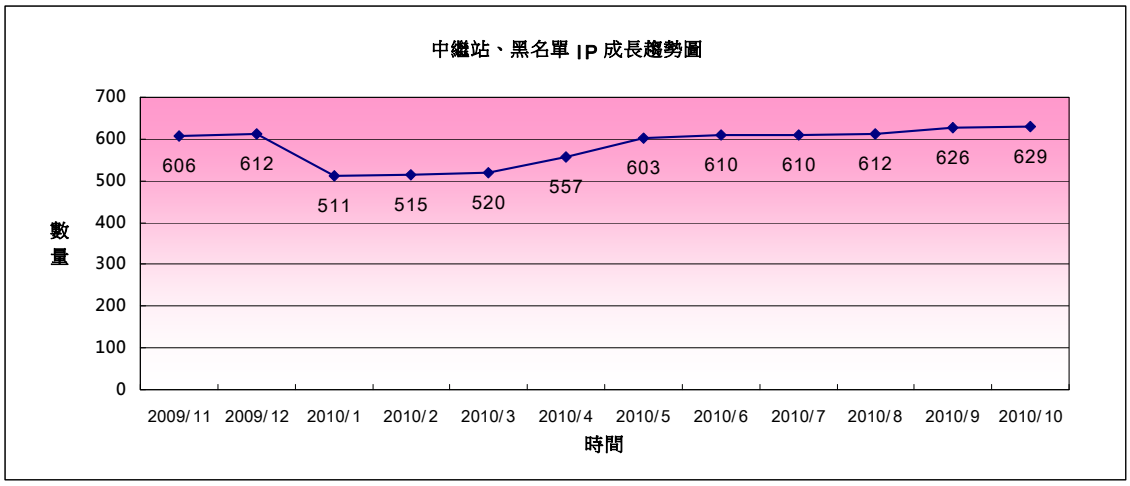


圖 45.　　中繼站、黑名單IP成長趨勢圖

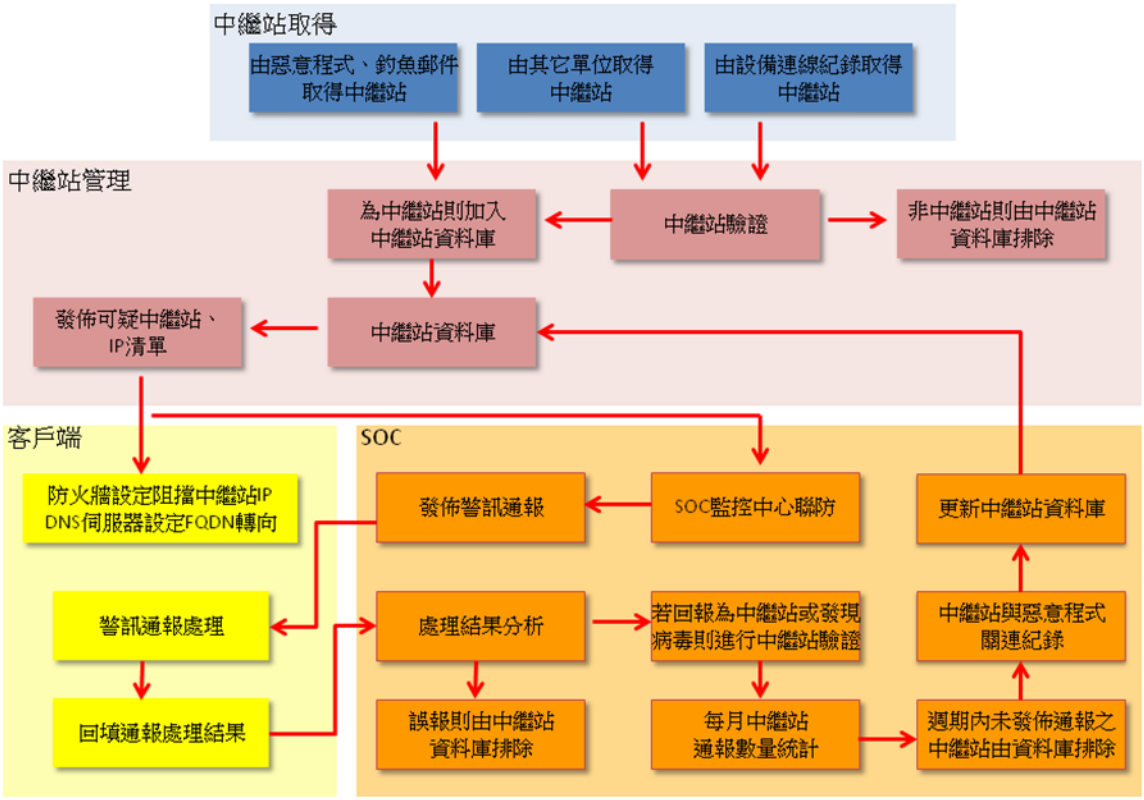


圖 46.　　中繼站管理流程

二、 新種惡意程式數量

目前多數機關、企業面臨重大的資安威脅在於駭客透過社交工程手法，將新種惡意程式植入用戶之受害電腦，然後控制受害者設備或竊取受害者電腦中的資料。欲解決此一問題，除了一再對使用者強調開啟郵件與網站瀏覽的警覺性外，過去實並無積極有效的對策。而經驗顯示，一般使用者資安意識再如何強化仍有其極限，誤點社交工程郵件或不意瀏覽惡意網站的狀況並無法完全消弭。在市場上沒有萬能防毒軟體系統的前提下，一旦惡意程式在用戶端內部網路植入肆虐

時，SOC 技術必須能超越防毒系統的限制破解內部網路的新種惡意程式。

SOC 透過關聯分析各種不同設備產生的原始事件，找出異常的連線行為，然後透過鑑識人員的調查，找出背後的惡意程式。（圖 47）是查獲新種惡意程式的數量統計，可以用來衡量事件處理的品質。

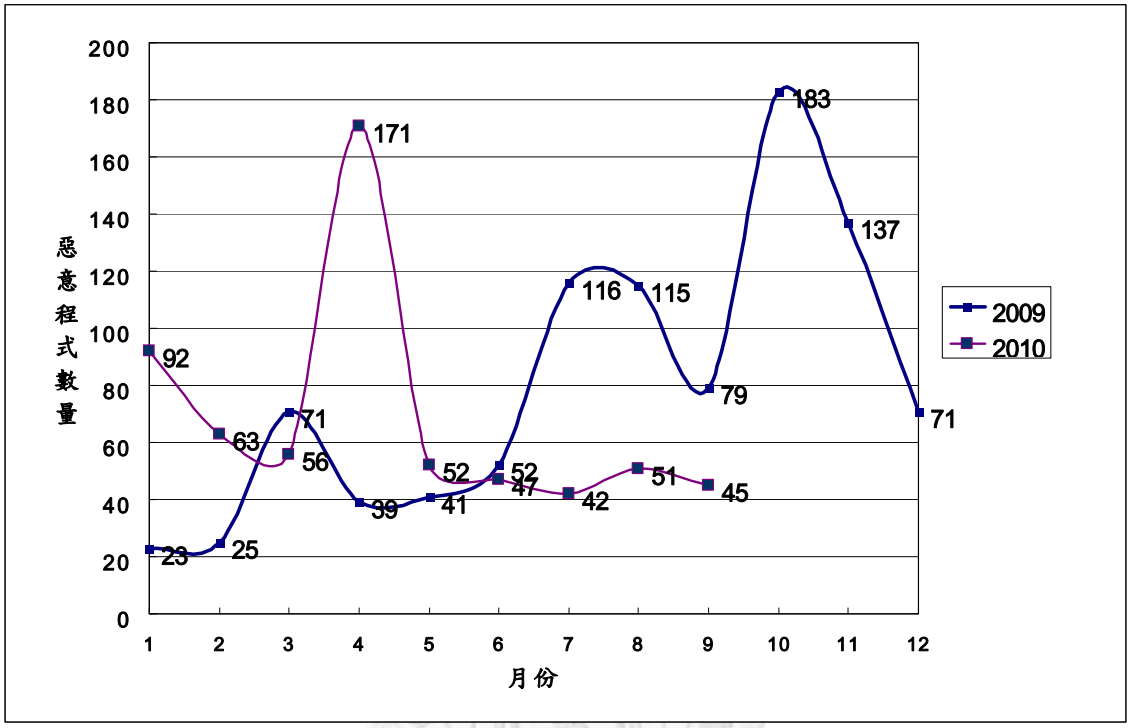
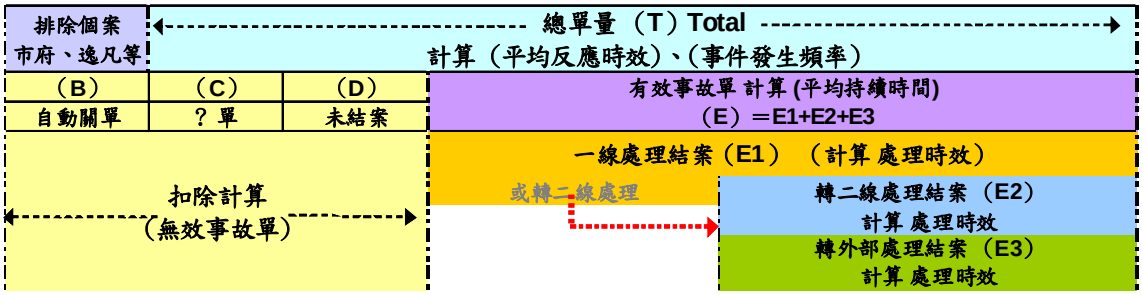


圖 47.　　新種惡意程式數量

三、　解決時效

（圖 48）顯示，SOC 二、三線的事件處理時效，此指標可以務用來測量事件完成處理的速度，並同時量測人員的負荷是否恰當。



Site:LT+NH by Weekly 09/02~09/29	第一週 09/02-09/08	第二週 09/09-09/15	第三週 09/16-09/22	第四週 09/23-09/29	Total
有效計算單量 E＝T-B-C-D	834	906	1132	1184	4056（E） E＝T-B-C-D
事故單 持續時間 Avg	2:26:00	2:13:06	2:30:07	2:49:40	2:31:02
1st 處理量（E1）	380	429	507	610	1926
1st 通報時效Avg	0:05:29	0:14:09	0:07:24	0:11:31	0:09:50
2nd 處理量（E2）	378	393	558	501	1830
2nd 處理時效Avg	3:05:31	3:34:24	4:27:32	6:06:17	4:26:13
3rd 處理量（E3）	76	84	67	73	300
3rd 處理時效Avg	9:04:27	7:30:37	5:21:19	8:38:26	7:42:01

圖 48.　事件處理時效分析表

第六節、平台管理指標

平台管理，是指 SOC 平台本身的營運狀態好壞的指標，包含：

- 平台可用度指標 (Availability) – 系統中斷時間(downtime)的長短，用來衡量平台停止運作的時間長短。
- 平台容量管理指標 (Capacity) – 包含資料庫容量與系統資源（CPU, Memory, Disk）等的耗用情況，用來衡量平台的容量是否充足。

一、可用度（Availability）

可用度指標的計算方法為：

$$1-\frac{downtime}{time}$$

方程式 9: 系統可用度

其中 downtime 表示量測周期（如一周、一個月等）內系統停頓的時間，time 表是量測的周期，（表 17 ）是某一周的可用度統計，顯示可用度為 100%。

表17 系統可用度

Total Poll Time (min)	Time Unavailabilities (min)	Percent Availabilities (%)
10129.733	0	100

（圖 49）是每一個月系統可用度的統計表範例。

資源名稱	資源說明	可用率	可用率趨勢統計				
			Jul	Jun	May	Apr	Mar
龍潭 ArcSight -Discovery 監控服務平台 – DB 主機	ArcSight DB 主機	100%	100%	100%	100%	96.24%	
龍潭 ArcSight -Discovery 監控服務平台 – Manager 主機	ArcSight Manager 主機	100%	100%	100%	100%	100%	

圖 49. 系統可用度統計表

二、容量管理指標（Capacity）

容量管理包含幾個系統資源使用度的指標（圖 50）：

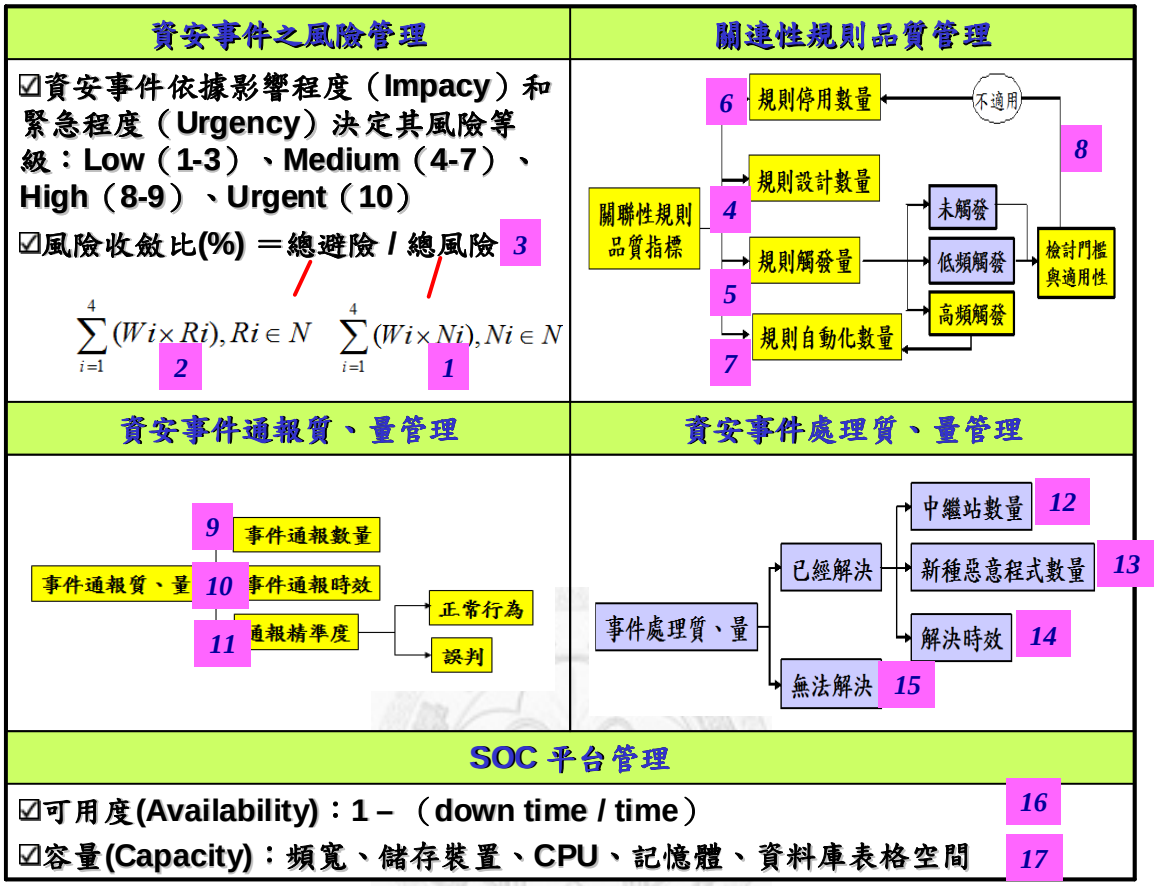
- 頻寬 -各種原始事件源源不絕送到 SOC 平台，需計算耗用的頻寬，並觀察是否有異常流量發生。
- 儲存裝置 (Storage) – 儲存空間是否足夠的指標。
- CPU
- Memory
- 資料庫表格空間 (Tables) –各種原始事件均存放在資料庫中，資料庫中各種資料表格，是否空間足夠，需要隨時測量與管理。

項目名稱	上限量	使用量	使用率	使用率趨勢統計				
				Jul	Jun	May	Apr	Mar
SAN Storage 2T Discovery	1.8T	1.5T	83.8%	84.7%	84.6%	81.91%	76.82%	72.22%
SAN Storage 2T Enterprise	1.8T	1.6T	91.6%	93.13%	92.5%	91.96%	91.87%	90.91%
SAN Storage 1.6T/4.8T Freedom	1.6T	0.4T	10%					

資源名稱	監控項目	使用率	使用率趨勢統計				
			Jul	Jun	May	Apr	Mar
龍潭 ArcSight Discovery 監控服務平台 –DB 主機	CPU	9.25%	6.78%	7.25%	18.21%	19.77%	17.13%
	Memory	75.1%	79.78%	79.98%	83.12%	81.48%	99.62%
	Tablespace Usage%（Arc_event_data / arc_event_index）	70.3% / 85.2%	83.9% / 84%	72.4% / 78.3%	32.6% / 40.1%	30.7% / 38.9%	78%
龍潭 ArcSight Discovery 監控服務平台 – Manager 主機	CPU	27.46%	21.65%	17.55%	15.17%	13.65%	11.29%
	Memory	74.31%	85.3%	88.78%	74.39%	71.67%	66.67%
	FileSystem	49.33%	41.08%	45.98%	53.14%	46.94%	47.32%

圖 50.　　系統可用性統計

第七節、技術管理指標彙總



（圖 51）整理 SOC 營運管理與各項管理指標的關係。

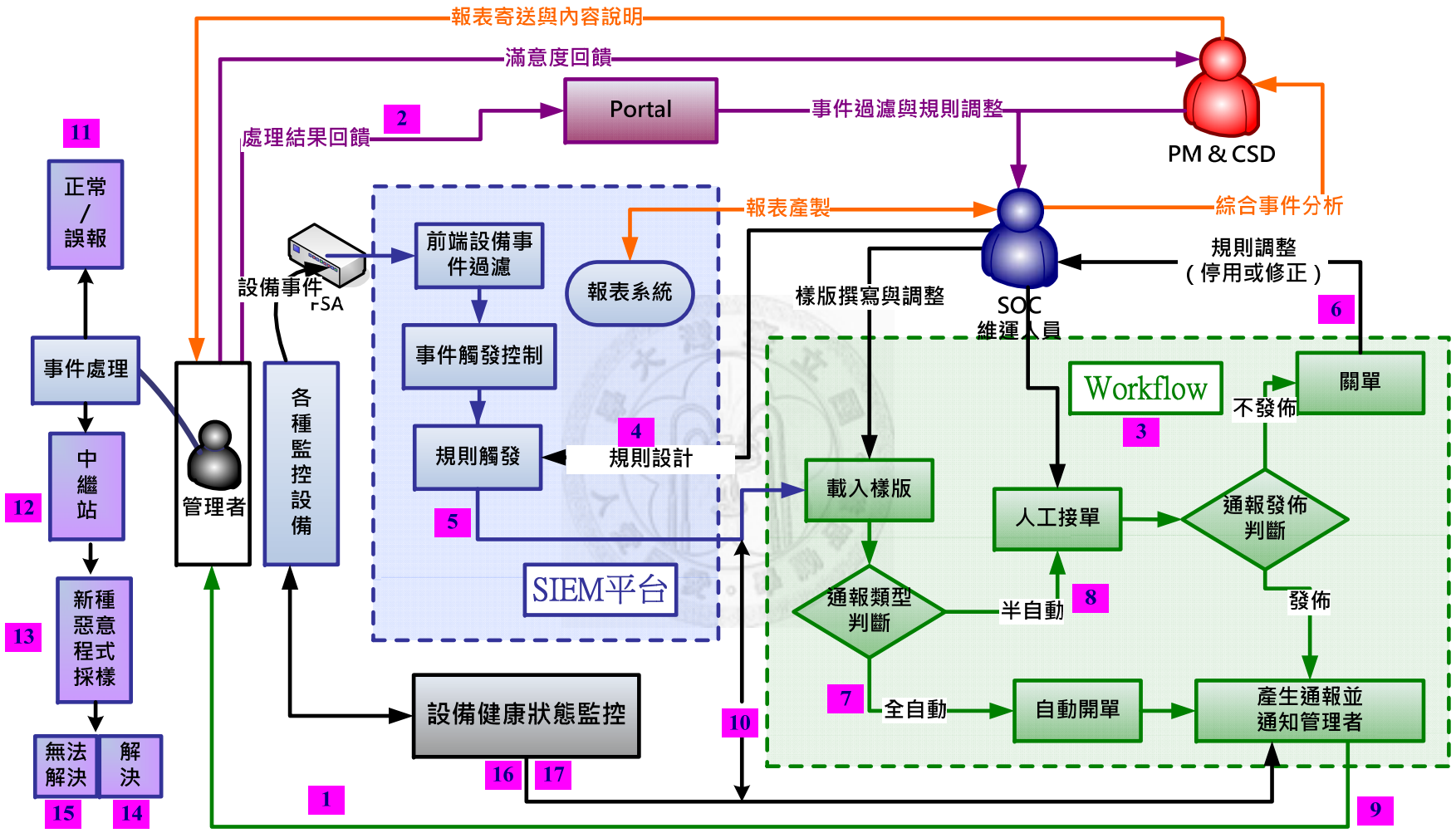


圖 51.　　SOC營運流程與績效指標關係圖

第六章　績效指標彙整與投資效益分析

第一節、績效評估指標彙整

各項績效指標，整理如（表 18 ）。

表18 績效指標總表

指標項目	內容	編號
技術管理指標(**T**echnical Management Indexes)		
組態管理 (**C**onfiguration)	使用標準版本(Standard Build)主機數量與比率	I
	企業關鍵系統監控數量與比率	II
	日誌(Log)紀錄完整度與涵蓋度	III
	系統校時涵蓋度	IV
	緊急組態調整反映時間	V
弱點管理 (**V**ulnerability)	弱點分佈指標	VI
	每一主機弱點指標	VII
	弱點發掘的延遲時間	VIII
	弱點補強的循環時間	IX
補強管理 (**P**atch)	未達 Patch Level 主機數量	X
	未及時 Patch 的延遲時間	XI
	Patch 時間影響服務水準程度	XII
閘道管制 (**G**ateway)	Firewall 績效度量指標	XIII
	IDS/IPS 績效度量指標	
	AP Firewall 績效度量指標	
防毒管理 (**A**nti-Virus)	防毒軟體部署涵蓋度	XIV
	病毒健康狀態評分	XV
營運管理指標(**O**perational Management Indexes)		
風險指標 (**R**isk)	總風險	1
	總避險	2
	風險收斂比	3
關聯分析規則品質指標	規則設計數量	4

(**C**orrelation Rule)	規則觸發量	5
	規則停用數量	6
	規則自動化數量	7
	半自動通報規則數量	8
事件通報質、量指標 (**N**otify)	事件通報數量	9
	事件通報時效	10
	通報精準度	11
事件處理質、量指標 (**I**ncident Handling)	中繼站數量	12
	新種惡意程式數量	13
	解決時效	14
	無法解決數量	15
平台管理指標 (**P**latform)	可用度	16
	容量管理	17

第二節、與 COBIT 控制目標比較

本節整理 COBIT 的控制目標與資訊安全績效評估指標對應，資訊安全績效只能涵蓋 IT Security Governance 的部份，是屬於整體 IT Goverance 的一部份。

表19 COBIT - Plan & Organize與績效指標關係

編號	內容	技術管理指標	營運管理指標
P01	Define strategic IT plan.	滿足 IT security plan 目標。	
PO2	Define the information architecture.	滿足 IT secuirty information architecture 目標。	
P03	Determine technological direction.	滿足 security service technical direction 的決定，以符合企業業務目標。	
P04	Define IT process, organization and relationships.	定義 IT 設備與功能管理流程與角色。	定義整體營運流程與角色。
P05	Manage IT investment.	綜合提供投資效益的評估依據。	
P06	Communicate management aims and direction.	滿足 Security Management 與高層管理的溝通需求。	
P07	Manage IT human resources.	N/A	7, 8, 10, 14
P08	Manage quality	提供整體 Security Management 的品質管理。	
P09	Assess and manage IT risks	VI, VII, VIII, IX, X, XIIII	1, 2, 3, 12, 13, 14, 15
P10	Manage Projects.	提供整體 Security Project 的管理指引。	

表20 COBIT – Acquire & Implement 與績效指標關係

編號	內容	技術管理指標	營運管理指標
AI1	Identity automated solutions.	N/A	7
AI2	Acquire and maintain application software.	組態管理、弱點管理、補強管理、防毒管理。	N/A
AI3	Acquire and maintain technology infrastructure.	閘道安全管理	16, 17
AI4	Enable operation and use.	整體指標支持整體的營運與使用。	
AI5	Procure IT resources.	整體指標支持整體 Security Resource 獲得的項目。	
AI6	Manage change.	IX, XII	V, IX, XI, XII
AI7	Install and accredit solutions and changes.	I, V, VIII, X, XII	4, 5, 6, 7, 8

表21 COBIT – Deliver & Support與績效指標關係

編號	內容	技術管理指標	營運管理指標
DS1	Define and manage service levels.	V, IX, XI, XII	8, 10, 14
DS2	Manage 3rd party services.	與整體的 IT Governance 需求相同，一併處理。	
DS3	Manage performance capacity	N/A	16, 17
DS4	Ensure continue service.	N/A	16, 17
DS5	Ensure system security.	I~XIIII	N/A
DS6	Identity and allocate cost.	整體指標協助了解投資效益。	
DS7	Educate and training users.	N/A	15
DS8	Manage Service Desk and Incidents.	N/A	本類指標提供 Service Desk 與 Incident 管理。
DS9	Manage the configuration.	組態管理指標	N/A
DS10	Manage Problem.	N/A	15
DS11	Manage data.	與整體的 IT Governance 需求相同，一併處理。	
DS12	Manage the physical environment.		
DS13	Manage operations.	N/A	本類指標提供 Service Desk 與 Incident 管理。

表22 COBIT – Monitor & Evaluate與績效指標關係

編號	內容	技術管理指標	營運管理指標
ME1	Monitor and evaluate performance.	提供整體 Security Managemet 的績效評估。	
ME2	Monitor and evaluate internal control.	提供整體內部控制的績效評估指標。	
ME3	Ensure compliance with external requirements.	與整體的 IT Governance 需求相同，一併處理。	
ME4	Provide IT governance.	提供 IT Security Goverance。	

第三節、績效評估指標與個案研究

本章將運用上述各章節所設計的績效評估指標，試算企業投資在資訊安全的效益，並回答本論文於第壹章研究動機中所提出的問題：

- 投入的資訊安全成本，是否獲得「合理效益」？
- 要「投資多少」資源，才能達到安全的程度？
- 資訊安全的狀態「比」過去好嗎？

由於每一個企業的 IT 環境不完全相同，本章選擇真實案例，再依據真實環境選擇部份績效評估指標，計算資訊安全的效益。選擇個案包含：

- 銀行：該銀行委外給 SOC 業者提供 7 x 24 監控服務，於今年 6 月間，SOC 業者早期發現 Worm 爆發現象，並導致總行資訊設備斷線，發生作業中斷的狀況。本案例依照金管會銀行局有關作業風險損失認列的準則[15][23]，計算該事件對銀行發生的實際收入損失，並對照本論文設計的部份績效評估指標，檢視資訊安全服務對該銀行的效益。
- 某醫療機構 ：委外 SOC 業者發現某醫療機構有病患病歷外洩問題，依據此實際案例，根據《個人資料保護法》[18]罰則，計算賠償責任。此部份金額為被駭客利用後，竊取病患病歷需承擔的實際損失。由計算出來的賠償規模，對照本論文設計的部份績效評估指標，檢視資訊安全服務對醫院效益。

相關案例資訊，基於對客戶保密義務，揭露過程已經做同比率或符合原始趨勢同幅度調整，技術架構亦酌予修改（如監控標的 Sonicwall FW 調整為 PIX FW），與客戶真實狀況不完全一致。相關財務報表、統計數字、或圖形，特別做降低解析度處理，以達到保護客戶真實身分的目的。但以上資訊的修訂，均不影響整體的架構、分析邏輯、計算結果與結論。

第四節、案例分析：銀行

一、 資訊安全監控架構

各分行透過網路與總部機房連線，進行每日銀行交易。IT 環境單純，資安設備兩個防火牆與 IPS 一部，保護 DMZ 區（圖 52）。因人力有限，委外專業 SOC 服務商提供 7 x 24 監控服務，服務內容與費用如（表 23 ）。

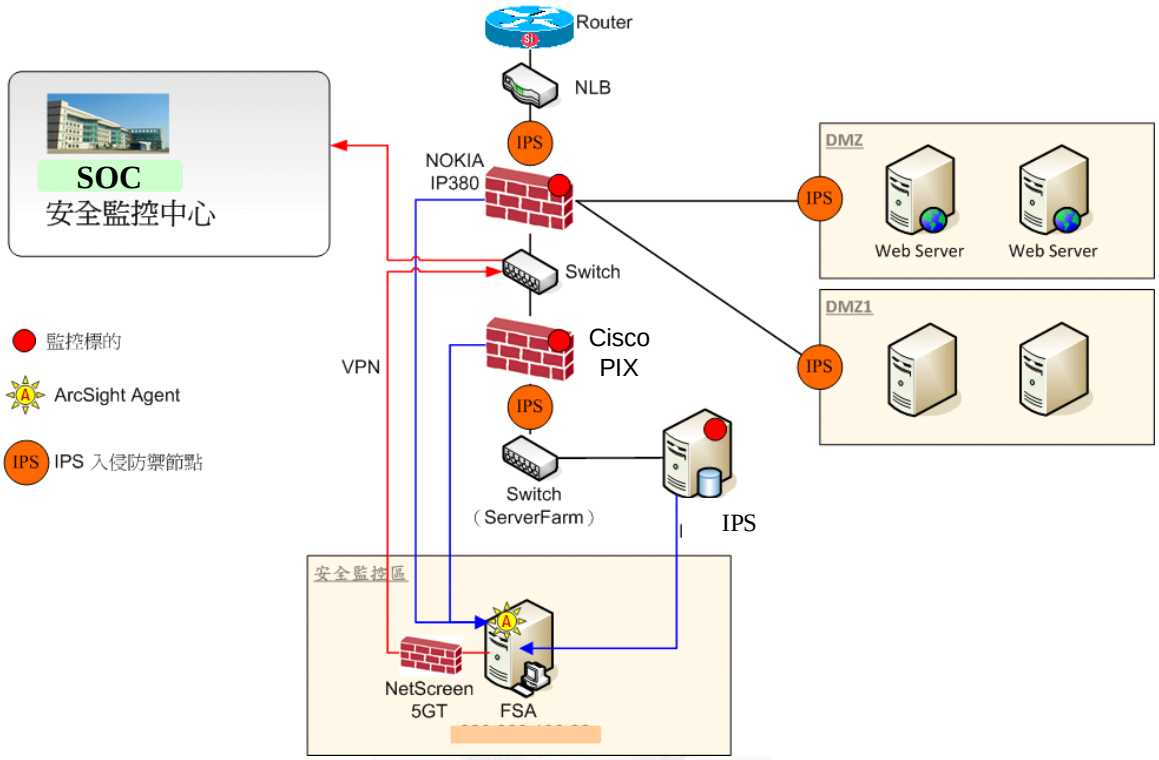


圖 52. 案例一資安監控架構

表23 監控內容與費用

項目	內容	服務標的	數量	單位	每月服務單價	每月服務總價
1	防火牆監控服務 (7 x 24)	Firewall x 2 即時監控服務費用	2	台	14,000	28,000
2	網路型入侵偵測系統監控服務	IPS 事件即時監控服務費用(7x24)	1	台	14,000	14,000
					每月服務費用 (未稅)	42,000
					一年服務總價(未稅)	504,000

二、 資安事件實例

（一） 現象

SOC 在 2010/6/9 上午 06:36，透過防火牆監控，首度發現在總部有一台主機，有 Worm 擴散蔓延的現象。由於清晨客戶還沒有上班，先通之機房 OP 連絡主機負責人，緊急通知客戶的主機管理者會同 SOC 業者的鑑識人員到場處理，爾後透過防火牆監控在 7:00, 7:30，Worm 蔓延情形越來越嚴重，有擴大趨勢（圖 53、圖 54）。紅色點為來源主機，白色點為目標主機，藍色圓形為防火牆觸發的事件。

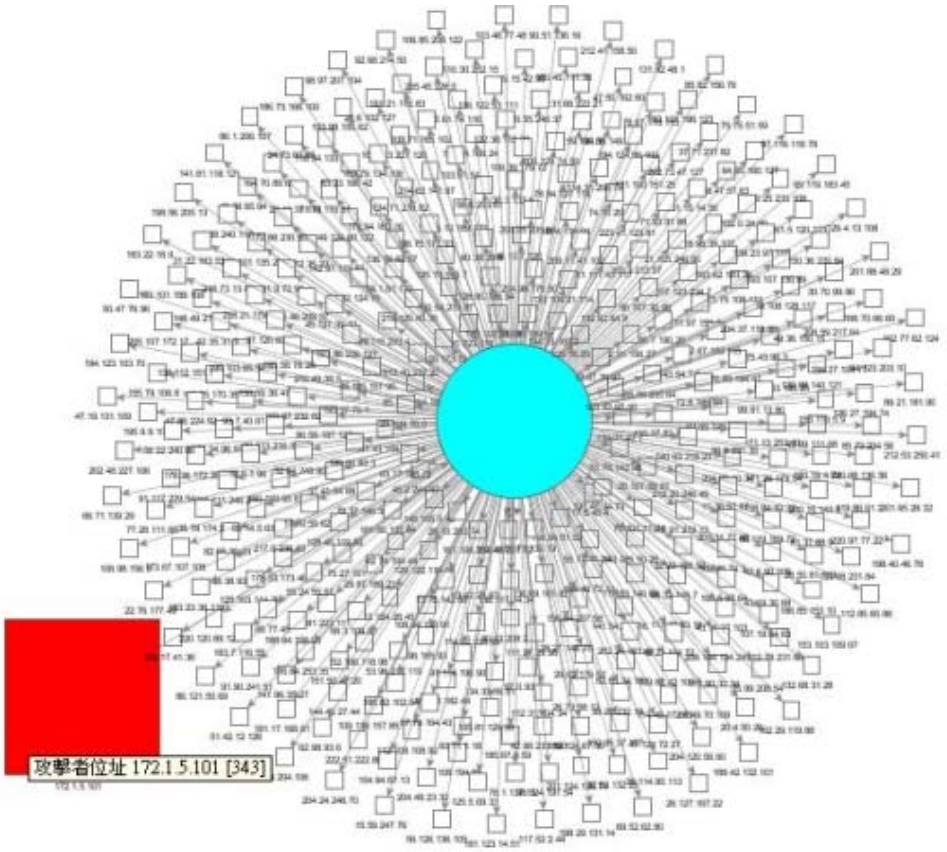


圖 53. 清晨首度發現Worm蔓延

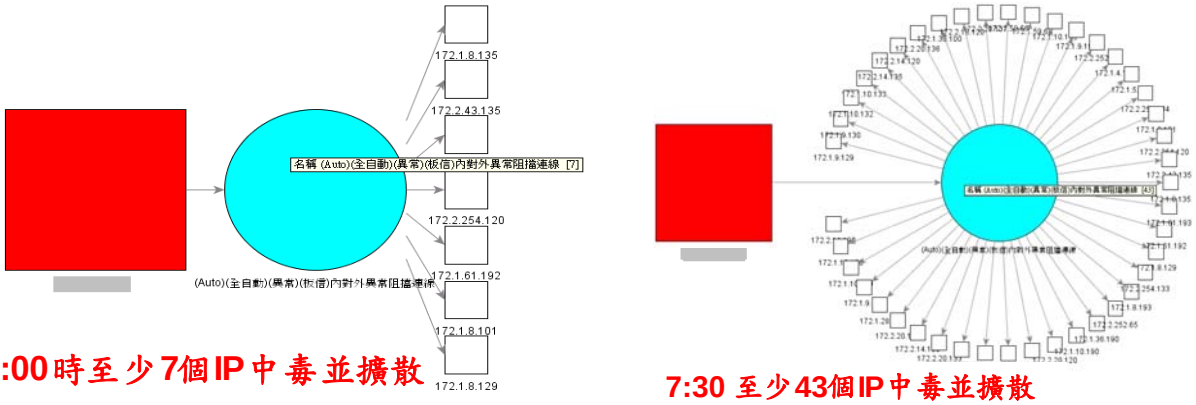


圖 54. Worm擴大蔓延

（二） 處理過程

客戶收到通知開始處理，資訊機房主機均感染 Worm，並對外發起大量的封包，總部對外網路已經癱瘓。SOC 業者鑑識人員處理發現是感染 Conficker 病毒，由於 Conficker 是 2008 年末的病毒早有 patch 補強，但客戶 Patch 管理沒落實，重要主機還停留在 Windows XP SP1。Conficker 是破壞力非常強的 worm，專門攻擊 Windows 漏洞（圖 55）[4]。

> Conficker, also known as Downup, Downadup and Kido, is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. It uses flaws in Windows software and Dictionary attacks on administrator passwords to co-opt machines and link them into a virtual computer that can be commanded remotely by its authors. Conficker has since spread rapidly into what is now believed to be the largest computer worm infection since the 2003 SQL Slammer, with more than seven million government, business and home computers in over 200 countries now under its control. The worm has been unusually difficult to counter because of its combined use of many advanced malware techniques.

圖 55. Confilcer說明

三、 業務影響分析

（一） 整體手續費影響分析

從發現第一個病毒現象客戶 6:30 開始處理，一直到早上 11:30 左右才全部排除恢復正常。該日 9:00-11:30 期間，總部網路完全中斷，所有分行均受影響，無法進行線上作業，網路中斷時間約 5 小時。客戶如果沒有即時透過 SOC 監控發現此問題，開始營業時網路無正常提供服務，嚴重影響銀行的日常業務活動，本案例 SOC 替客戶爭取到 2.5 小時的提早處理時間 (6:30-9:00)。銀行的網路發生問題，直接影響的是分行的各項臨櫃作業無法執行，所衍生的影響是手續費收入。手續費收入，主要有以下幾項收入來源（圖 56）：

- 非臨櫃交易 –ATM 提款機與網路 ATM 銀行等交易，此部份交易分散在全天 24 小時內都持續進行，因此本次斷線對手續費影響時間為 5 小時。
- 臨櫃交易- 這是手續費收入的最主要來源，此類交易集中在白天營業時間共 6.5 小時內（9:00am-15:30pm），本次斷線對臨櫃交易手續費影響時間為 2.5 小時。

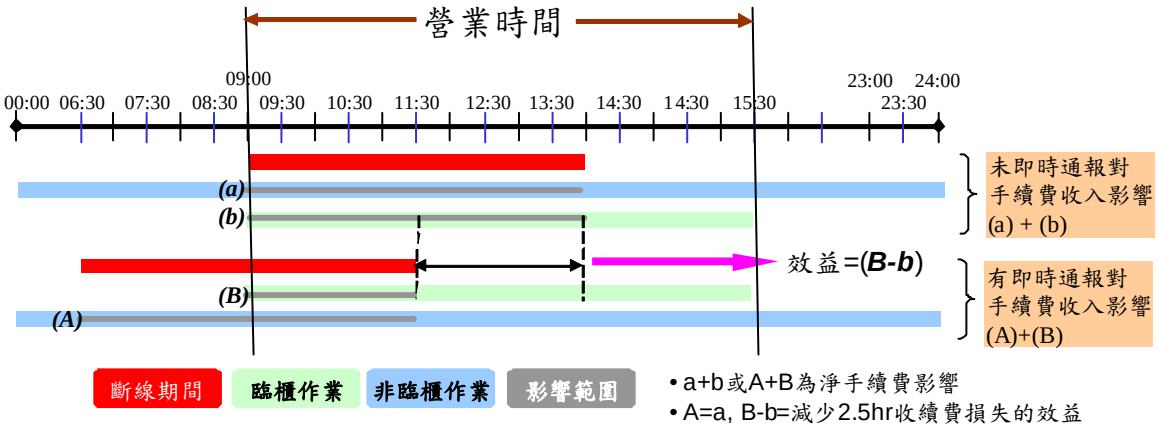


圖 56.　　手續費影響時段分析

手續費計算方法：

- 根據該銀行損益表，推算每日平均手續費淨收入 ***x***（此收入涵蓋所有臨櫃與非臨櫃交易）。
- 依據行政院金管會金融機構自動化服務概況統計[16]（表 26 ），取得該銀行平均每日 ATM 交易次數，據以計算 ATM 的手續費收入 ***y***。
- 根據財金資訊季刊第 64 期，台灣金融卡多元應用-網路 ATM 之應用與發展[14]，網路 ATM 交易筆數約占跨行轉帳年總交易筆數 23.4%。根據此比重，推算網路 ATM 的手續費收入 ***z***。

斷線期間對手續費的影響 ***TotalLoss*** 計算方式如下：

$$TotalLoss = (x - y - z) \times \frac{2.5}{6.5} + (y + z) \times \frac{5}{24}$$

方程式 10: 銀行手續費影響計算式

（二） 手續費淨收入

（表 27 ）是該銀行公布的民國 99 年第二季損益表（民國 99 年 1 月 1 日到民國 99 年 6 月 30 日），依據損益表中的手續費淨收入，估算每天手續費收入（表 24 ）：

項目	金額	備註
平均每天手續費淨收入	$ 1,863	(2季以120工作天估算)

表24 手續費淨收入 (單位千元)

依照此方式計算出每天手續費淨收入 ***x*** = 1,863,000 元。

（三） 非臨櫃交易：ATM 交易手續費影響

ATM 交易不需臨櫃作業，對於斷線期間無法執行作業的用戶，依照行政院金管會金融機構自動化服務概況統計[16]（表 26 ），該銀行平均每天交易次數約為 5,830 次（已經扣除查詢、失敗等不收手續費的交易次數）。這些交易中有一定比率為本行交易是沒有手續費收入，依照實務訪談，一般 ATM 交易約 60%是跨行且有手續費收入，（表 25 ）是 ATM 交易手續費費 y = 47,221 元。

項目	金額	備註
ATM每日平均交易次數	5,829.8	註1
每次手續費淨收入(元)	13.5	註2
總金額(以全部跨行交易計算)	78,701.9	
實際影響總金額(以60%為跨行交易計算	47,221.1	註3

表25 ATM手續費損失估算 (單位元)

註 1：以每月 30 個交易天計算。

註 2:跨行交易手續費 17 元其中 3.5 元付給財金公司,ATM 提供者淨收入 13.5 元。

註 3：中國信託蔡滋森副總經理訪談後的數據。

表26 99年9月底金融機構自動化服務概況表

8-1 金融機構自動化服務概況表

8-1 Automatic Service Machines of Financial Institutions

民國99年 9月底 End of Sept. 2010

金融機構別 by Institution	發行金融卡數 (張) Card Issued	通用金融卡數 (張) Card in Circulations	設置台數 (台) Set of Machines	交易次數（次） Case of Transactions 本月 Current Month	交易次數（次） Case of Transactions 本年累計 Accumulated	交易金額（新臺幣百萬元） Amount of Transactions (NT$ Million) 本月 Current Month	交易金額（新臺幣百萬元） Amount of Transactions (NT$ Million) 本年累計 Accumulated
總計 Total	153,890,671	76,367,985	25,630	55,326,417	487,487,066	701,356	6,251,528
本國銀行 Domestic Banks	107,373,543	59,929,815	20,666	41,551,911	364,709,669	574,614	5,048,542
A銀行 #	5,562,729	3,305,855	607	2,426,562	21,778,637	30,227	252,573
B銀行	5,519,278	1,950,621	751	1,751,777	16,128,438	20,675	196,548
C商業銀行	6,581,031	4,749,047	1,078	3,357,911	29,184,978	51,554	452,064
D商業銀行 #	7,597,424	4,086,423	826	2,610,059	23,052,328	28,717	257,838
E商業銀行 #	9,339,285	5,020,010	776	2,746,019	24,253,828	29,232	261,203
F商業銀行 #	7,513,645	4,447,105	634	2,449,445	21,793,588	42,729	379,589
G儲蓄銀行	2,151,412	1,120,076	272	642,487	5,776,131	6,562	58,604
H銀行 #	4,704,675	3,263,363	1,307	2,409,345	21,474,963	27,501	246,494
I商業銀行 #	6,108,435	3,087,998	1,808	2,833,743	23,964,963	37,309	317,574
J銀行	795,878	541,454	110	263,285	2,447,701	2,516	27,837
K商業銀行 #	3,760,826	2,013,723	508	2,076,682	17,956,085	32,526	289,882
L商業銀行	155,286	110,458	90	98,207	986,201	670	9,632
M商業銀行 #	2,462,287	1,517,635	615	1,470,801	12,828,945	21,624	192,133
N商業銀行	665,799	431,343	124	152,007	1,274,044	1,898	19,651

（四） 非臨櫃交易：網路 ATM 交易手續費影響分析

網路 ATM ，結合「金融卡」 及「晶片讀卡機」，透過網路連至金融機構網站，全天候透過網際網路上進行各項金融交易 (包括：餘額查詢、自行或跨行轉帳、約定或非約定帳戶轉帳等)，與實體 ATM(除提領現金外)無異，持卡人可在家或任何可上網地方，輕鬆完成各類金融交易。目前金管會銀行局並未針對網路 ATM 的交易量，提供交易次數統計，根據財金資訊季刊第 64 期，台灣金融卡多元應用-網路 ATM 之應用與發展一文的資料[14]，網路 ATM 交易筆數約占跨行轉帳年總交易筆數 23.4%。以上一節的估算，ATM 手續費損失（表 25 ）約 47,221 元，網路 ATM 手續費為 ATM 手續費 23.4%，計算得 $z = 11{,}050$ 元。

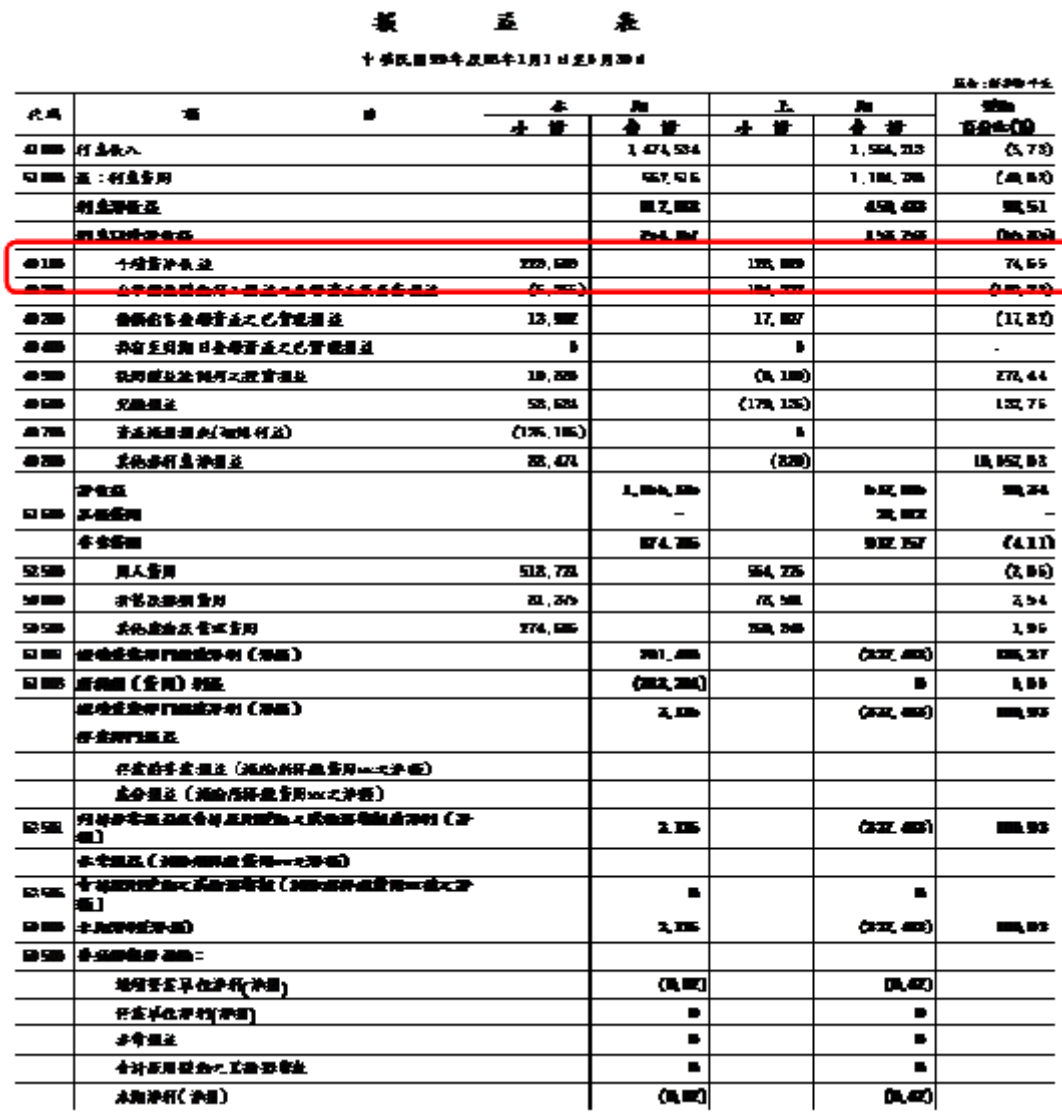


表27 99年第二季損益表

（五） 手續費總影響

手續費淨收入 $x = 1{,}863{,}000$；ATM 交易手續費費 $y = 47{,}221$ 元；網路 ATM 手續費 $z = 11{,}050$ 元。依據「方程式 10: 銀行手續費影響」，計算收續費總損失為：

$$TotalLoss = (x - y - z) \times \frac{2.5}{6.5} + (y + z) \times \frac{5}{24} =$$

$$(1863000 - 47221 - 11050) \times \frac{2.5}{6.5} + (47221 + 11050) \times \frac{5}{24} = 702266$$

方程式 11: 斷線期間手續費淨影響

四、 資訊安全指標分析

（表 28 ）檢視目前銀行運用各項指標的概況，在「技術指標」部份，基本的預防工作都沒有實施，SOC 的監控其實都是事件發生後才盡快通知，往往都已經造成損害了；最好的防護該是預防勝於事後監控與處理。透過本論文設計的指標，可以自我盤點尚未落實的工作，配置適當資源（人力、費用）來強化銀行的安全防護，消弭資安事故於無形。

指標項目	內容	編號		效益
組態管理 (**C**onfiguration)	使用標準版本(Standard Build)主機數量與比率	I	○	完整且標準配置版本的主機，可免已知病毒感染風險
	企業關鍵系統監控數量與比率	II	○	僅監控 FW, IPS，其他關鍵業務主機均未納入，應擴大範圍，強化偵測能力。
	日誌(Log)紀錄完整度與涵蓋度	III	○	防毒等設備未納入，可提早發現大量病毒未清理狀況。
	系統校時涵蓋度	IV	◎	已落實可確保日誌時間正確性，提高分析準確度。
	緊急組態調整反映時間	V	○	緊急異動預先準備，可提高系統穩定度，降低調整過程衍生的風險。
弱點管理 (**V**ulnerability)	弱點分佈指標	VI	○	沒有實施，應該立刻規劃進行，及早發現弱點，才能預先補強，將安全事件事件預先防範，使風險降到最低。
	每一主機弱點指標	VII		
	弱點發掘的延遲時間	VIII		
	弱點補強的循環時間	IX		
補強管理 (**P**atch)	未達 Patch Level 主機數量	X	○	沒有實施，若完成補強，不會發生手續費損失的事故。
	未及時 Patch 的延遲時間	XI		
	Patch 時間影響服務水準程度	XII		
閘道管制	Firewall 績效度量指標	XIII	◎	例行管理確保運作正常，可保障 SOC 及時發現異常。
	IDS/IPS 績效度量指標			

(**G**ateway)	AP Firewall 績效度量指標		╳	沒有購置。
防毒管理 (**A**nti-Virus)	防毒軟體部署涵蓋度	XIV	○	如納入日常防毒監控,可提早發現病毒大量感染現象。
	病毒健康狀態評分	XV		
風險指標 (**R**isk)	總風險	1	◎	已由委外 SOC 業者提供，保證風險有效控制。
	總避險	2		
	風險收斂比	3		
關聯分析規則品質指標 (**C**orrelation Rule)	規則設計數量	4	◎	已由委外 SOC 業者提供，保證分析規則的準確性。
	規則觸發量	5		
	規則停用數量	6		
	規則自動化數量	7		
	半自動通報規則數量	8		
事件通報質、量指標(**N**otify)	事件通報數量	9	◎	已由委外 SOC 業者提供。
	事件通報時效	10	◎	SOC 即時與精準通報，第一時間通知客戶提早解決。
	通報精準度	11	◎	
事件處理質、量指標(**I**ncident Handling)	中繼站數量	12	◎	已由委外 SOC 業者提供 7x24 服務，非上班時間仍提供服務，縮短斷線時間。
	新種惡意程式數量	13	◎	
	解決時效	14	◎	
	無法解決數量	15	◎	
平台管理 (**P**latform)	可用度	16	◎	已由委外 SOC 業者提供。
	容量管理	17		

表28 各項指標應用分析

註：◎：適用，已經用在本案例且發揮直接效益。

○：適用，但本客戶未落實，應納入強化績效。

╳：本項指標不適用。

五、 綜合討論

（一） 投入的資訊安全成本，是否獲得「合理效益」

綜合以上分析，本項資訊安全服務，獲得合理效益，理由為：

- 銀行客戶付給服務商一年共 504 千元（表 23 ），但以 2010/6/9 上午發生的資安事件為例，因 SOC 提早發現，減少銀行的手續費淨收入損失約 702,266 元。
- SOC 業者提供的即時通報與處理服務，在本案例每一小時的效益為 280,906 元。
- 本銀行因為規模甚小，ATM 設備僅有 124 部，所以此次斷線的影響可以忽略。但如果是大規模的銀行（表 26 ）排名第一的 A 銀行，2010.9 月份的交易次數高達 2,426,562 次，換算每天約 8 萬餘次，短暫的斷線會有嚴重的損失。

（二） 要「投資多少」資源，才能達到安全的程度

本案僅提供資安監控服務，預防勝於治療，事先的防範才是治本之道。Conficker 的感染，是因為主機的 Patch 沒有落實，因此該銀行應該還要投資弱點掃瞄作業和 Patch 管理，可以提升到安全的程度。投資的規模與金額，視弱點掃瞄的頻率與數量決定，透過此項作業，可以確保類似問題不再發生。（表 28 ）中的「組態管理」、「弱點管理」、「補強管理」等，都是該銀行所迫切需要投資的資源，可評估自行採購工具與負責執行，或是委外實施。

（三） 資訊安全的狀態「比」過去好嗎

（圖 57）可以看出，銀行整體的資安事件通報，除了上述 Conficker 事件以外，之後幾個月份呈現下降趨勢。由於銀行環境相對穩定，在沒有重大的環境異動下，各種網路與系統的行為為固定，因此整體的資安規則觸發狀況不會有大幅度的波動。透過（圖 57）的指標，清楚的回答目前資訊安全的狀態，比過去「好」。

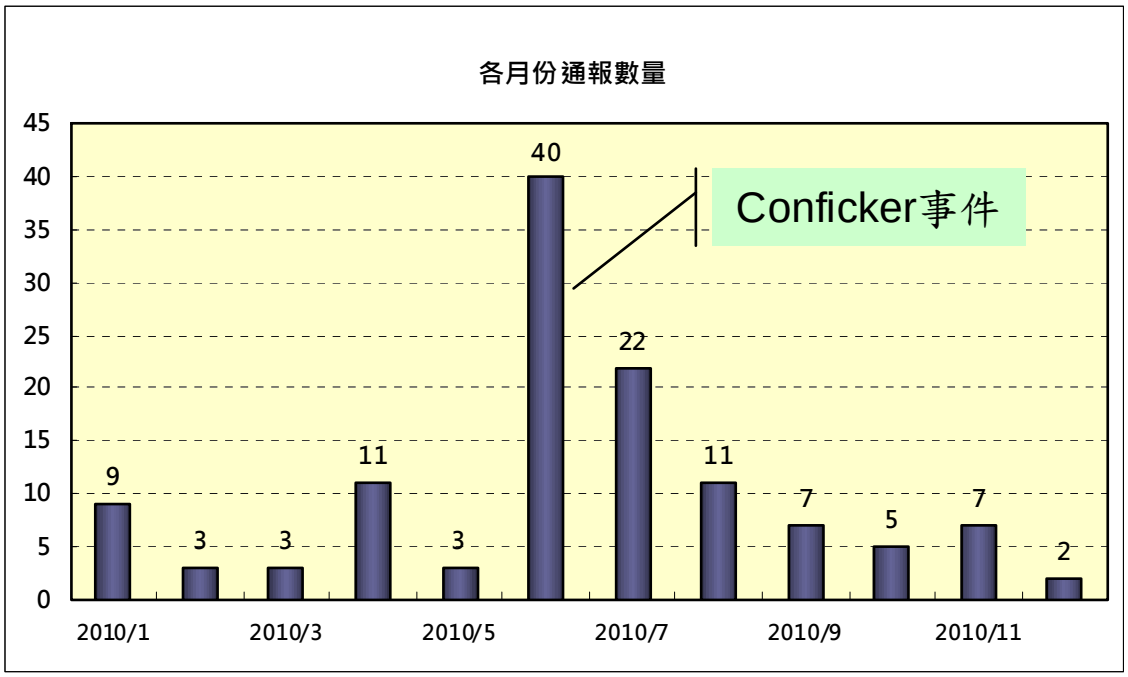


圖 57.　　事件通報數量趨勢圖

第五節、案例分析：醫療機構

一、 網站弱點與個資洩漏

進入「○○健康資訊管理系統」需通過身分驗證機制（帳號與密碼），方可進入系統。測試過程中發現雖然身份登入網頁已對 SQL 攻擊字串做過濾，但最後一關檢查身份正確與否的網頁卻沒有阻擋SQL攻擊字串，直接對ic_pass.asp插入SQL攻擊字串繞過系統驗證機制，成功登入系統取得使用者權限，（圖 58）為攻擊流程說明。

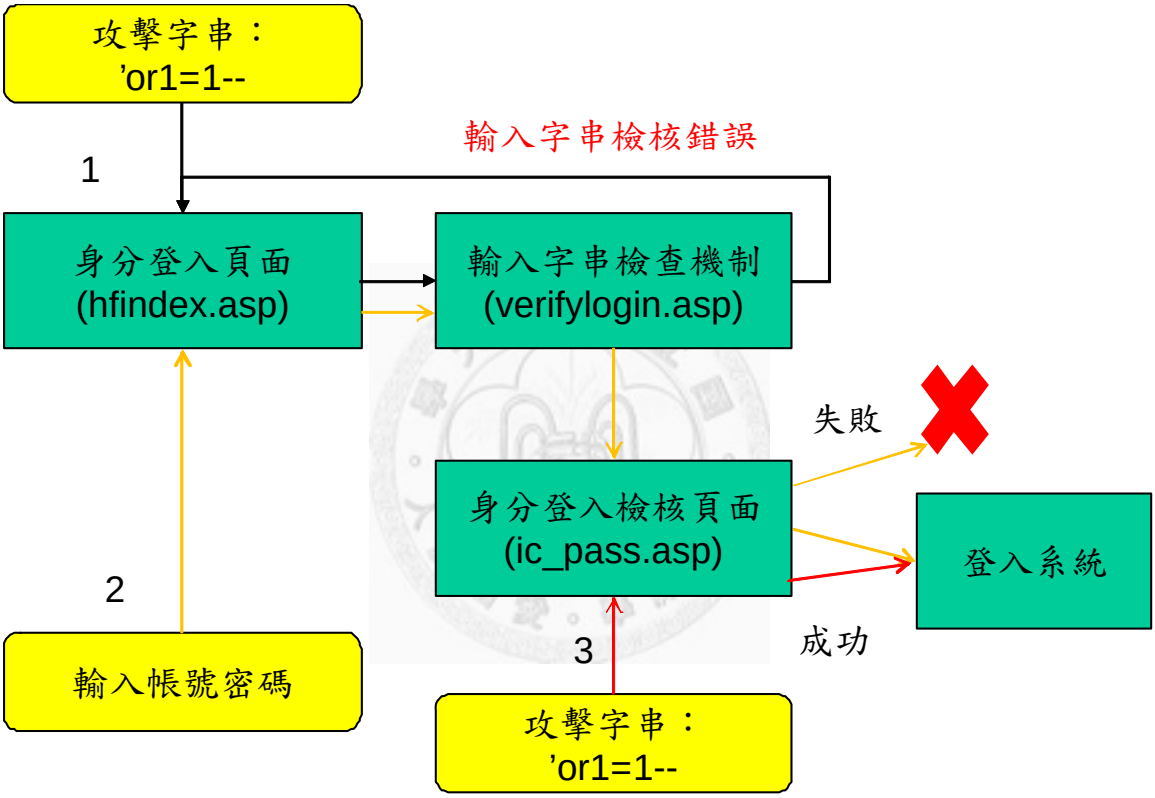


圖 58. 攻擊流程說明

將 SQL 字串跳過 verifylogin.asp 的檢核，直接傳給 ic_pass.asp 處理，該頁面會因為輸入的字串判斷恆為真，而直接登入系統。登入系統後可取得許多屬於個人隱私的資料，包括系統使用者本身及其所屬病人之病歷資料如（圖 59）。使用支攻擊指令範例如:

http://○○○.○○○.tw/ic_pass.asp?ID=' or 1=1--

圖 59. 病歷處方與診斷資料

二、 業務影響分析

由 SQL Injection 登入，可取得約 98~180 位病人病歷資料，其中包含姓名、地址、身分證字號、眷屬資料與治療細節（診斷、處方與用藥）等。由於本案例提早由 SOC 業者發現，並通知補強，並未被駭客利用竊取病患資料成功。這些網站弱點在上線時就已經存在，如果被有心人士知悉並成功竊取民眾病歷，後果不堪設想。包含：

- 賠償責任：依照我國個人資料資料保護法的規定[18]，洩漏民眾個人資料，每一筆賠償責任為 500 元以上 20,000 元以下罰金。若以洩漏 100 個病歷資料為計算基礎，賠償以最低 500 元計算，則要至少要賠償 5 萬元台幣。但我們知道病歷資料是所有個人資料中最為敏感與重要的，雖然還沒有判例根據新的法律作成判決，但因為病歷資料的特殊敏感性，我們認為合理賠償金額不會是最低的 500 元。本事件如果不幸為有心人士發現並竊取病患病歷資料，其賠償責任應遠高於 5 萬元，最高可能高達 3,600,000 元（以最高 2 萬元計算，洩漏 180 筆病歷）。
- 行政責任：除了財務上的賠償以外，恐怕會有嚴重的行政責任。此部份雖然無法量化，但嚴重程度恐怕非金錢所能衡量。

- 信譽損失：除了以上責任以外，民眾會對醫院喪失信心，設想洩漏得病歷中，若有愛滋病患或是某名人的病歷，將使民眾恐慌，其結果亦難以用金錢衡量。

三、 綜合討論

（一） 投入的資訊安全成本，是否獲得「合理效益」

綜合以上分析，本項資訊安全服務，「有」獲得合理效益，理由為：就所阻止之個資洩漏賠償責任而言，避免賠償金額約在 5 萬~360 萬之間。本案實際支付給廠商的服務費用，每年約 150 萬左右。但如果加計行政責任與信譽損失，本項資訊安全服務，有「合理效益」。

（二） 要「投資多少」資源，才能達到安全的程度

既有系統，很多是有一段歷史的老舊系統，透過委外服務商的檢測，找出存在已久的問題。但還有多少類似的系統遺留類似設計上的問題，仍需逐一檢查確認。再投資多少資源於這些老舊系統的設計與調整，才能達到安全的程度？此部份的投資，需視系統設計調整的複雜度決定投資的規模，有些無法修改的只能重新設計，有些有維護廠商的系統，在原合約中已經涵蓋，則無需增加投資。

（三） 資訊安全的狀態「比」過去好嗎

（圖 60）是該醫療機構通報數量趨勢圖，除 2010 年 11 月，整體數量呈穩定的下降趨勢，在沒有重大的環境異動下，資安狀態是穩定的逐漸改善。詳細分析 2010 年 11 月的巨幅成長，發現是其中甲、乙兩個部門所產生，扣除此兩部門通報，全部呈穩定緩慢下降的趨勢，資訊安全狀態比「過去好」。但甲、乙兩個部門則相反，資訊安全狀態比「過去不好」。有此指標，則可以針對惡化的單位，深入了解原因與改善之道，以降低資訊安全風險。

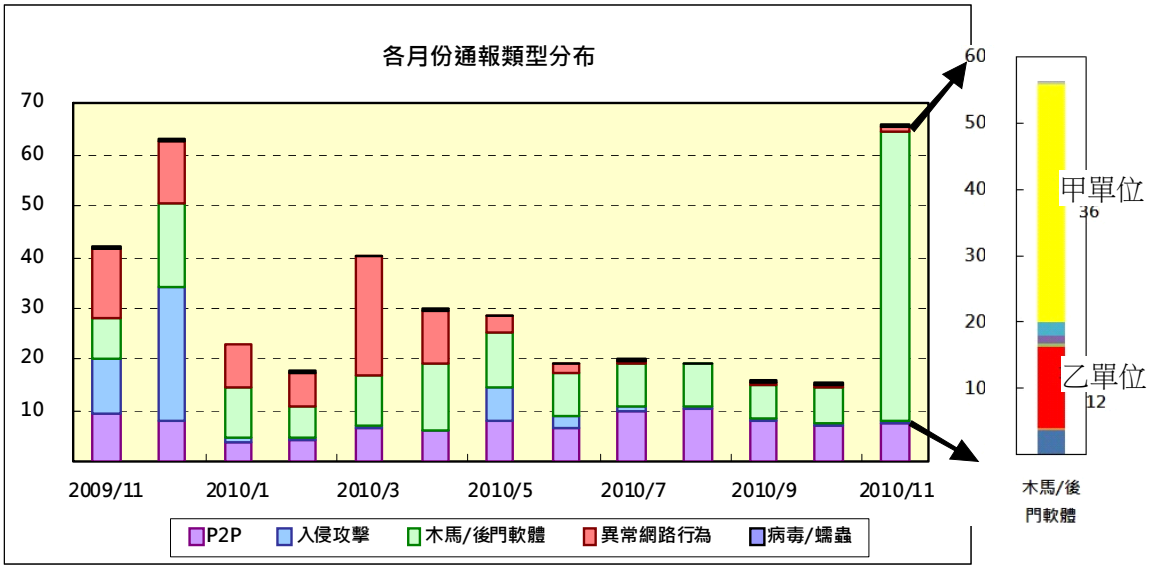


圖 60.　　事件通報數量趨勢圖

第七章　結論與建議

第一節、研究結論

一、　客觀可行的績效衡量指標

本論文就技術管理面、營運管理面，設計資訊安全績效評估架構(Framework)，作為企業衡量資訊安全績效良窳的依據。各項績效評估指標遵循「S.M.A.R.T.」原則，可客觀與準確計算，免除人為主觀判斷的差異。各指標均量化為單位如小時、次數、百分比等，各項指標可以合理的代價（時間、金錢、人力）有效取得，具備可操作性。有了適當的績效評估指標，則管理階層可以有效衡量與評估投資效益是否合理，哪些項目需要加強、哪些部份在預期之中。

二、　回答管理者關心的投資效益問題

在發生資訊安全事件以後，本論文依據所造成的影響，參酌銀行作業安全作業安全損失的認定方法，計算實際財務損失，可以精確的衡量投資效益。在非銀行領域，依照我國個人資料保護法的罰則，計算賠償的金額，供實際負責的管理者衡量資訊安全營運管理的投資效益。以上方法，可以廣泛用來衡量不同企業的損失，並能精確的反應負面影響的範圍與大小。透過真實個案的探討，回答企業高階管理階層最關心的資訊安全績效問題：

- 投入的資訊安全成本，是否獲得「合理效益」？
- 要「投資多少」資源，才能達到安全的程度？
- 資訊安全的狀態「比」過去好嗎？

三、　盡責管理 (Due Care)的證明

各種資安事件層出不窮，就算所有的安全機制均穩定與有效的運作，也不能保證絕不會有新種惡意程式或攻擊手法，此類事件發生依舊會對企業產生危害與損失。此類事件發生時，企業首要證明是否已經採取必要且符合現有科技平均水準的管理作為，盡職的保護企業資源、員工與客戶免受資訊安全事件的危害。個資法通過後，要求企業必須採行適當之安全措施，以防止個人資料被竊取、竄改、毀損、或洩漏。企業需確認對於所擁有的個人資料，已經有善盡善良管理人的職

責，將個人資料外洩的風險盡可能降到最低。

資訊安全的政策制訂與各項防護機制的施行良窳，對企業高階經理人至關重要，有了這些績效評估指標，可以證明企業善盡 "due care" 與 "due diligence" 的有力證據；一旦公司的資產遭到不當的使用或破壞，相關資安政策文件與資安營運管理的各種日誌與數據，企業是否盡善良管理人之注意義務，將影響企業需負擔過失責任的賠償規模的大小。

有訴訟發生時，企業若已經採用符合當今科技水準的管理措施，並且可以提出各種數據與佐證，證明善盡善良管理人的責任，可將企業賠償責任降到最低，是對企業永續經營與股東權益最好的保障。

第二節、後續研究建議

本論文就資訊安全營運管理的角度，設計績效衡量指標，瞭解營運管理的效率與品質，並進一步評估投資績效。在投資績效部份，仍有幾個值得後續探討的方向，值得後續研究釐清：

- 本論文的真實個案，其投資績效是以付給委外資安專業廠商的合約金額為評價的基礎。就銀行與醫院療機構個案而言，確實有很高的投資效益。但反過來從資訊安全服務供應商角度，所收的服務費用定價是否合理？是否與對客戶所獲得的效益取得平衡？本論文尚未討論。一個極端的例子是委外廠商定價過低，導致全部資訊安全服務案都獲得很「高」的投資報酬率，是否代表委外廠商應酌予提高服務費用，取得平衡？
- 對於沒有發生資訊安全案例的客戶，其投資績效又要如何計算？各種安全控制均有效防患損失於未然，全年度都沒有發生因資訊安全衍生的損失。也就是說整體健康狀況在很好的狀況之下，那是否代表委外廠商的服務費用可以酌予降低？
- 本論文設計的績效評估指標項目很多，未來可考慮研究綜合所有指標，計算一個最終的積分或燈號（如綠、黃、紅燈），這樣可以讓高階管理者一目瞭然營運管理的狀態，更為直覺與簡單。

有關資訊安全營運管理績效評估的研究，目前仍然很缺乏，這是值得耕耘與

深入研究的資訊安全管理題目，唯有客觀與有效的衡量方法，可以讓企業經營者與資訊安全提供者，取得雙贏的成果，降低企業營運風險，最大化企業營運績效。

參考文獻

[1] A Complete Guide to the Common Vulnerability Scoring System, Version 2.0, Forum of Incident and Security Teams (FIRST) and the Common Vulnerability Scoring System-Special Interest Group (CVSS-SIG)., June 2007.

[2] Maizlitsh B. and Handler R., IT Portfolio Management: Step by Step, John Wiley & Sons, 2005, p. 53.

[3] COBIT 4.1 - Control Objectives for Information and related Technology, IT Governance Institute (ITGITM), 2007.

[4] Conficker, Wikipedia, , http://en.wikipedia.org/wiki/Conficker

[5] Doran, George T. "There's a S.M.A.R.T. way to write managements's goals and objectives." and Miller, Arthur F. & Cunningham, James A "How to avoid costly job mismatches" Management Review, Nov 1981, Volume 70 Issue 11.

[6] Federal Information Security Management Act (TITLE III—Information Security), December 2002.

[7] ISO/IEC - Information technology — Security techniques — Information security incident management, First edition, 2004-10-15.

[8] ISO/IEC 27006 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.

[9] Jaquith Andrew, “Security Metrics, Replacing Fear, Uncertainty, and Doubt”, Addison Wesley, 4th Printing, October 2008.

[10] The New Oxford American Dictionary, Second Edition, Hardback, Mar 2005, ISBN13: 9780195170771, ISBN10: 0195170776, Oxford University Press.

[11] Zavidniak Paul, Dr. D’Amico Anita and McCallam Dennis H., “Achieving Information Resiliency”, Information Security Technical Report, Vol 4, No. 3 (1999) 54-62, Elsevier Science Ltd.

[12] 九十四年度國家資通安全技術服務與防護管理計畫：資安規範整體發展藍圖。執行機構：財團法人資訊工業策進會。行政院研考會委託。

[13] 中華民國 97 年電腦應用概況報告，行政院主計處電子處理資料中心，中華民國 98 年 9 月編印。

[14] 台灣金融卡多元應用-網路 ATM 之應用與發展，李成全，財金資訊季刊第 64

期，2010/03/30。

[15] 金管會銀行局 98 年 7 月 27 日銀局(法)字第 09800303590、09800303591 號函，由銀行公會與聯徵中心共同研商於 98 年 12 月前辦理作業風險外部損失資料庫。

[16] 金融機構自動化服務概況，行政院金融監督管理委員會銀行局統計室，2010/11/15。

[17] 計算機信息系統安全等級保護管理要求，GA/T 391-2002, 中華人民共和國公共安全行業標準，2002/7/18 實施。

[18] 總統令：個人資料保護法，中華民國 99 年 5 月 26 日，華總一義字第 09900125121 號。

[19] 國家資通安全政策研討會，行政院國家資通安全會報，中華民國 98 年 6 月。

[20] 淺談 BASEL II，蔡明熹，http://blog.sina.com.tw/ases_1995/category.php?pbgid=33445&categoryid=134682，2007/10/01。

[21] 慎選合適的企業防火牆，資訊與電腦 208 期(民國 86 年 11 月)：頁 95-96。

[22] 資訊安全通訊：Vol.14 Number 1, P11, 中華民國資訊安全學會。

[23] 銀行公會 98 年 8 月 10 日全風字第 0980002071A 號函，作業風險資料報送。