行政院及所屬各機關出國報告

(出國類別：實習)

「實習資通安全與集中維運相關技術」報告

服務機關：中華電信股份有限公司數據通信分公司

出國人：　職　稱　　姓名

副工程師　游峰鵬

助理工程師　藍建智

服務機關：中華電信股份有限公司電信研究所

出國人：　職　稱　　姓名

助理研究員　鄭皓陽

助理研究員　廖慧如

出國地點：美國

出國期間：92年10月12日 至 92年10月22日

報告日期：92年12月1日

系統識別號:C09203807

公 務 出 國 報 告 提 要

頁數: 31　含附件: 否

報告名稱:

實習資通安全與集中維運相關技術

主辦機關:

中華電信數據通信分公司

聯絡人／電話:

／

出國人員:

藍建智　中華電信數據通信分公司　網際網路處　助理工程師
游峰鵬　中華電信數據通信分公司　網際網路處　副工程師
廖慧如　中華電信研究所　專案研究計畫 專案十五 分項三　助理研究員
鄭皓陽　中華電信研究所　專案研究計畫 專案十五 分項三　助理研究員

出國類別: 實習

出國地區: 美國

出國期間: 民國 92 年 10 月 12 日 -民國 92 年 10 月 26 日

報告日期: 民國 92 年 12 月 22 日

分類號/目: H6／電信　H6／電信

關鍵詞:　資通安全與集中維運相關技術,SOC

內容摘要:

本次的實習資通安全與集中維運課程，乃學習藉由網路集中監控的過程，掌握及處理最新的電腦病毒/蠕蟲疫情、電腦及網路系統弱點及駭客資訊，並且針對資安威脅資訊、事件相關性及未知威脅，進行資料之分析統計，辨別哪些是危急、迫切的安全告警，以解決層出不窮的資安問題。本份出國報告詳細的描述實習課程所獲取的一些技術與經驗，這些技術與經驗分爲三部份，一爲學習如何由網際網路業者(ISP) NOC中心的觀點出發，規劃建置其自己的安全維運中心(SOC)? 本次出國實習課程之一即是學習身爲ISP 的AT&T在擁有骨幹網路的同時，如何藉由安全設備的佈署、偵測、監控分析來建構整體的安全機制，隨時掌控網際網路上進行的非法活動或病毒入侵，並因應可能發生的資安事件，以避免事件(病毒)的擴大，提升網路服務品質及客戶滿意度。二爲學習SOC的核心功能『資安管理系統Security Information Management(SIM) 』的技術與應用，因SIM爲一項新技術，各家廠商產品及技術差異性極大，此份報告詳細敘述並比較了三種不同的SIM特性與功能，藉由學習及掌握SIM最新技術發展，才能有效的規劃與運用相關技術來建置HiNet安全維運中心。三爲實習如何規劃建置及維運安全維運中心(SOC)的相關技術，這些技術包括系統的監控與管理功能、專業安全人才的需求、維運機制的建立及資安事故的應變處理等等，報告中敘述了國外相關的經驗與技術，利用該技術將用於HiNet安全維運中心的規劃建置。 本報告書共分五個單元，第一單元說明本次實習之目的。第二單元敘述實習行程及課程。第三單元敘述一網際網路服務業者(ISP)藉由骨幹網路安全裝置的佈署及所建立的安全機制，掌控網際網路上所進行的非法活動，並進而對阻斷服務(DOS)攻擊及分散式阻斷服務

(DDOS)攻擊提供一個快速的解決方法。第四單元則敘述有關『安全維運中心 (Security Operation Center，SOC) 』建置的相關技術與解決方案。第五單元爲實習心得與結論。

本文電子檔已上傳至出國報告資訊網

摘要

本次的實習資通安全與集中維運課程，乃學習藉由網路集中監控的過程，掌握及處理最新的電腦病毒/蠕蟲疫情、電腦及網路系統弱點及駭客資訊，並且針對資安威脅資訊、事件相關性及未知威脅，進行資料之分析統計，辨別哪些是危急、迫切的安全告警，以解決層出不窮的資安問題。

本份出國報告詳細的描述實習課程所獲取的一些技術與經驗，這些技術與經驗分為三部份，一為學習如何由網際網路業者(ISP) NOC中心的觀點出發，規劃建置其自己的安全維運中心(SOC)? 本次出國實習課程之一即是學習身為 ISP 的 AT&T 在擁有骨幹網路的同時，如何藉由安全設備的佈署、偵測、監控分析來建構整體的安全機制，隨時掌控網際網路上進行的非法活動或病毒入侵，並因應可能發生的資安事件，以避免事件(病毒)的擴大，提升網路服務品質及客戶滿意度。二為學習 SOC 的核心功能『資安管理系統 Security Information Management(SIM) 』的技術與應用，因 SIM 為一項新技術，各家廠商產品及技術差異性極大，此份報告詳細敘述並比較了三種不同的 SIM 特性與功能，藉由學習及掌握 SIM 最新技術發展，才能有效的規劃與運用相關技術來建置 HiNet 安全維運中心。三為實習如何規劃建置及維運安全維運中心(SOC)的相關技術，這些技術包括系統的監控與

管理功能、專業安全人才的需求、維運機制的建立及資安事故的應變處理等等，報告中敘述了國外相關的經驗與技術，利用該技術將用於HiNet安全維運中心的規劃建置。

本報告書共分五個單元，第一單元說明本次實習之目的。第二單元敘述實習行程及課程。第三單元敘述一網際網路服務業者(ISP)藉由骨幹網路安全裝置的佈署及所建立的安全機制，掌控網際網路上所進行的非法活動，並進而對阻斷服務(DOS)攻擊及分散式阻斷服務(DDOS)攻擊提供一個快速的解決方法。第四單元則敘述有關『安全維運中心 (Security Operation Center，SOC) 』建置的相關技術與解決方案。第五單元為實習心得與結論。

目次：

壹、實習目的.....P.4

貳、實習行程及實習課程 P.5

參、網際網路服務業者(ISP)安全技術.....P.6

肆、『安全維運中心』(SOC)建置 P.17

伍、實習心得與結論 P.29

壹、實習目的

隨著網路技術的進步與應用的普及，網路已經進入到我們的工作與日常生活中，但是近年來層出不窮的網路攻擊事件，不禁讓人對網路的安全打了問號，從CodeRed、Nimda、Slammer、Blaster等病毒造成數以百萬計主機的傷害，到資料的竄改、竊取，以及中共網軍入侵事件等。尤其近三年來網際網路的使用產生劇烈變動，寬頻網路的推動，大大地改變人們對網際網路的使用習慣。連線速度的增加，不僅僅代表下載網頁的速度變快，更意味著病毒的傳播或網路攻擊的影響將比以前更嚴重。由於對網際網路的依賴愈來愈重，個人電腦連上網際網路的時間增加，這意味著來自網際網路的安全風險也隨著增加。你永遠不知道有多少人(不管是有心或無心)在網際網路上等著竊取你的資料、等著對你發動攻擊。

面對今日如此複雜的網際網路環境，如何有效的、合乎成本的建立我們資通安全防護機制以降低網際網路安全的威脅，對本分公司是刻不容緩的任務。為達成這項艱鉅的任務，需從多個方面、多個層次來考量，國外有許多豐富的資安發展經驗與技術，非常值得我們學習與借鏡，藉由本次出國研習相關的資通安全與集中維運方面的技術與經驗，將可用來進一步來強化本分公司資通安全作業環境，並建立本分公司完善的資通安全的預警、監控管理、通報與事件應變機制，以大幅提升資通安全防護與應變能力。

貳、 實習行程及實習課程

職等奉派至美國實習『資通安全與集中維運相關技術』，實習時間自民國九十二年十月十一日至九十二年十月二十二日為期十二天。本次實習課程計有：

(1) 研習『AT&T SOC deployment and operation』

(2) 研習『Managed Security Service and SOC Infrastructure Training』

(3) 研習『Incident Management and Security Response Training』

參、 網際網路服務業者(ISP)安全技術

3.1 概說

AT&T提供包含Voice over IP、Managed Internet Services、Web Hosting、WorldNet以及與其他直接連接於骨幹網路上的服務，在近年來層出不窮的網路攻擊事件中，也造成其服務品質的影響以及用戶商譽的損失，尤其是阻斷服務攻擊(Denial of Service, DOS)以及分散式阻斷服務攻擊(Distributed Denial of Service, DDOS)。由於一般的用戶端安全設備(例如防火牆或入侵偵測系統)僅能對非法、惡意的封包或曾經發生過的攻擊行為進行偵測或阻擋，但對於DOS/DDOS的攻擊卻無法防禦，因此對於DOS/DDOS之類的攻擊行為就非常仰賴網際網路服務業者的機制來偵測與排除。而ISP對於DOS/DDOS攻擊的排除往往曠日費時，更由於大部分DOS/DDOS攻擊都來自外部網路，追查不易，因此AT&T藉由DOS偵測裝置的佈署，來增進對於網際網路上正在進行的活動(合法或非法)進一步的了解，並且透過對於所蒐集資料的統計、分析，能加速對DOS/DDOS攻擊事件的排除，並且能對下一次的攻擊事件進行預測。

由於AT&T對於安全上的需求會比較偏向整個網路架構的觀點，也就是從ISP的角度來觀看相關的安全佈署，因此相關的安全佈署，蠻值得同為ISP 的HiNet學習。

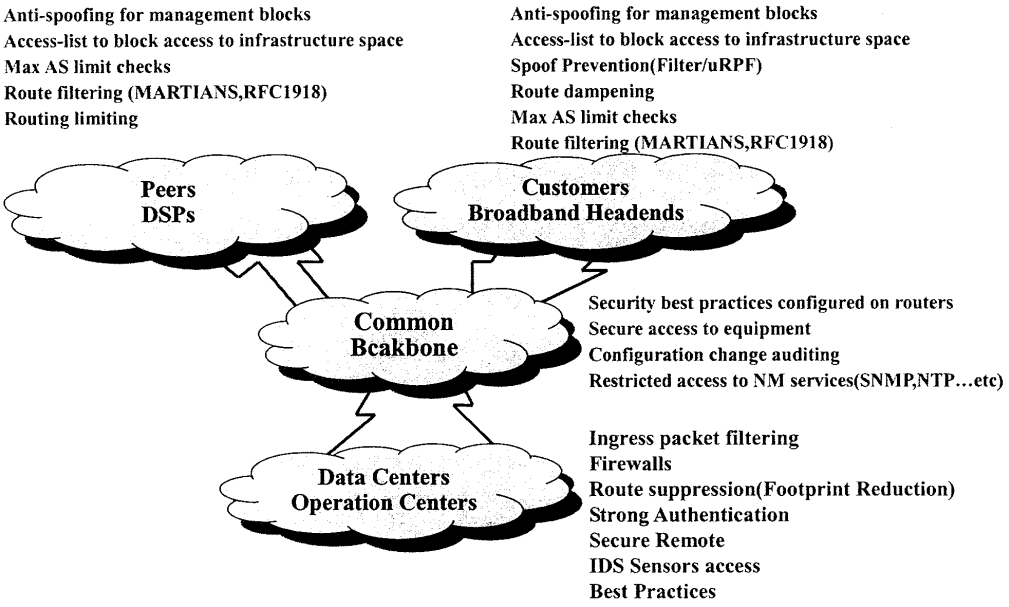
3.2 AT&T的安全機制

DOS/DDOS 的攻擊模式可分為四種:來源 IP 位址假造的 DOS 攻擊、來源 IP 位址未假造的 DOS 攻擊、來源 IP 位址假造的 DDOS 攻

擊、來源 IP 位址未假造的 DDOS 攻擊，對於這些攻擊的防護，AT&T 的機制(如附圖一)可劃分為五項措施：

(1).預防(Prevention)

對於攻擊發生前之準備措施，AT&T 所採取的措施是藉由安全策略的施行可對潛在的攻擊達到預防的效果，主要分為下列幾種方法：



附圖一:預防措施

◆ Spoof prevention at the edge

→ 透過在所維運網路邊界上的一些安全機制，對於假冒來源 IP 位址(Spoofed Source IP Address) 的封包進行過濾。例如 RFC 1918 保留了三個網段的 IP Address-10.0.0.0 /8、172.16.0.0 /16 ~ 172.31.255.255 /16、192.168.0.0/24~192.168.255.255/24 - 提供

給企業內部使用，所以帶有這三個網段 IP Address 的封包不應該在網際網路環境中出現，因此對於來源位址及目的地位址為這三段 IP Address 的封包都應該被過濾掉或丟棄。

◆ Packet selection at the edge

→ 透過在所維運網路邊界上的一些安全機制，對於進入網路內的封包進行篩選或過濾。例如對於所有接取路由器，都會有一個上載介面連接到骨幹路由器，這個介面的 IP Address 基本上僅會做為內部路由協定交換資料使用或是偵錯時的 ICMP 封包經過，因此對於目的地位址為這些 IP Address 的流量如果超出 ICMP 的範圍，就可視為一種攻擊封包或攻擊前的偵測封包而予以丟棄，來保障接取路由器的安全。

◆ Packet rate-limit at the edge

→ 在所維運網路邊界上對部分型態的封包進行流量限制 (Rate - limit)。以 ICMP 的 echo 封包(也就是 Ping 指令)為例，在正常的網路流量中所佔的比例不應該超過 5%，因此就可在網路邊界上對 ICMP 的 echo 封包進行流量管制，以避免透過 ICMP 的 echo 封包所進行的 DOS/DDOS 攻擊。

◆ Route suppression and dampening

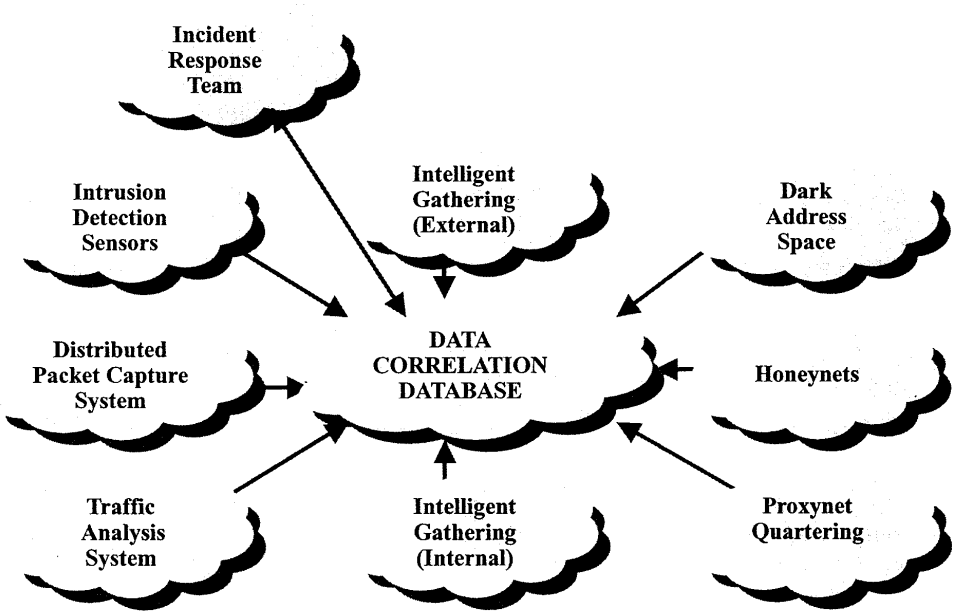
→ 對於與其他網際網路服務業者或 BGP 路由協定的連線，透過路由限制(Route Suppression)的方式，來避免因錯誤組態 (Mis-configuration)所造成的錯誤路由現象；透過路由壓抑

(Route Dampening)的方式，來預防因路由震盪(Flapping)所造成的不穩定狀態。

◆ Routing protocol protection

→ 對於其他網際網路服務業者或 BGP 路由協定的連線，限制所接收的路由(Routing)數目; 對所維運網路上的路由協定，透過認證金鑰(Authentication Key)的方式進行封包交換，以避免對路由協定的惡意攻擊; 對於一般用戶間的路由協定僅透過靜態路由(Static Route)方式設定，以避免內部路由協定受到用戶干擾。

(2).預測(Prediction)



附圖二:預測機制

藉由安全裝置的佈署，例如流量分析系統(Traffic Analysis System)、入侵偵測感應器(Intrusion Detection Sensor)、封包捕捉系統(Packet Capture System)等，可以蒐集網路上流竄的可能攻擊封包、異常流量等資訊，並且藉由關聯性統計、分析，可以對整個網路上正在進行的攻擊(或攻擊前)活動進行了解，雖然所蒐集到的資料無法告知我們下一次的攻擊何時發生，但卻可以預測可能發生的攻擊模式、攻擊的強度大小及可能發動這些攻擊的地區。

若要預測可能的攻擊威脅，就必須做到下列幾個動作：

◆ Analysis of port scanning and enumeration

→ 一般的網路攻擊再發動前，都會對主機通訊埠進行掃描，以了解該主機的弱點在哪裡或是是否能透過該通信埠進行感染。以之前的疾風病毒為例，當主機受到感染後就會對網路上的其他主機攻擊，並藉由對方主機埠 135 的安全漏洞進行病毒傳播，而受害主機的 IP Address 是隨機選擇的。因此在病毒傳播的過程中流量分析系統、入侵偵測感應器、封包捕捉系統等裝置都會看到針對埠 135 連線的流量異常增加，這些資料就可做為網路攻擊事件即將發生的訊號，讓網路服務業者可以提早因應。

◆ Detection of distributed agents

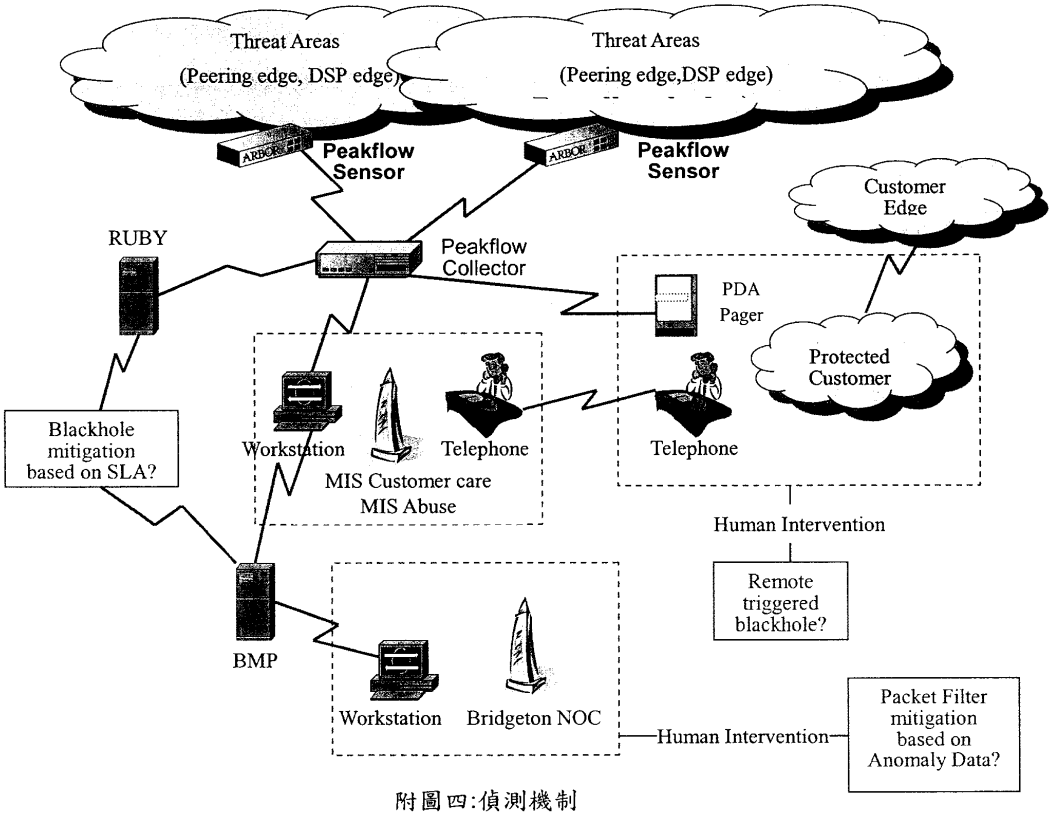
→ 流量分析系統、入侵偵測感應器、封包捕捉系統等裝置除了

監測異常流量的增加外，還可統計出發出異常流量的主機分佈的情形，做為回應機制的參考。

◆ Trojan tracking and Quartering

→ 對於部分的病毒或是駭客使用的木馬程式，還可透過 Honeynet (或 Honeypot)的機制，進行木馬程式的追蹤與捕捉，並分析其攻擊行為。木馬程式的追蹤與捕捉有助於我們了解駭客慣用的工具或行為，增加我們對網路安全的了解。

(3).偵測(Detection)



附圖四:偵測機制

在 AT&T 的網路裡，佈署著 Arbor 所生產的 Peakflow 設備，並且藉由該設備蒐集網路流量資料進行分析與偵測，當 DOS/DDOS 攻擊發生的初期，藉由佈署的安全裝置發出告警訊息，可以在網路發生大量異常封包的初期，即時處理，減少網路或用戶受影響的時間。例如當安全裝置發現針對某一固定 IP Address 的 ICMP 封包超過一個臨界值時，就發出告警訊息通知相關人員，已採取相對應的行動。

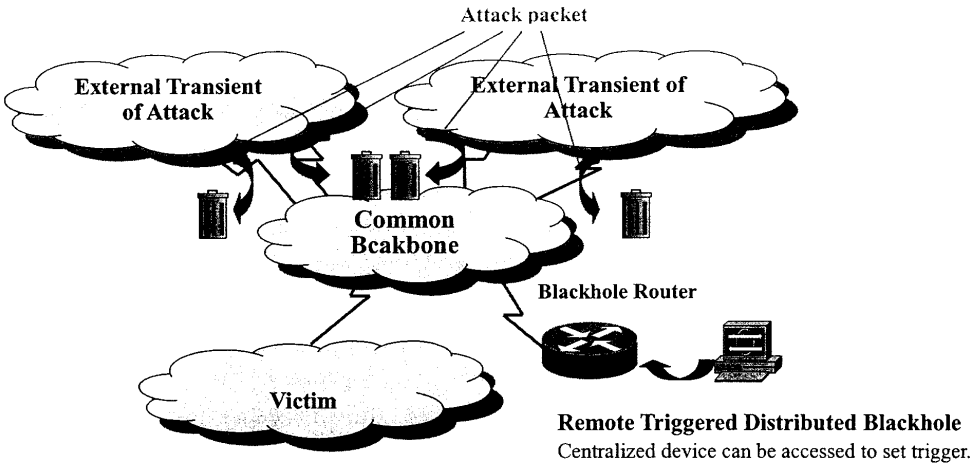
(4).減輕 (Mitigation)

當 DOS/DDOS 攻擊發生之時，除了直接影響受攻擊網路外，與該網路介接在同一個路由器的其他用戶或該攻擊封包所經過路徑的所有路由器都會受到間接影響，因此必須先採取適當的措施以減輕攻擊的影響，主要分為下列幾種方法

◆ Blackholing

→ 透過將攻擊封包全部導向 Null 0(Blackhole)的方式，減輕受攻擊網路的影響，以恢復受攻擊網路或受影響之路由器的正常運作，主要適用於下述狀況

- 被攻擊主機不存在或非提供主要服務的主機。
- 受攻擊用戶能忍受被攻擊主機暫時的服務中斷。
- 分散式的阻斷攻擊(DDOS)，攻擊封包為非固定 IP Address 或假造的隨機 IP Address。



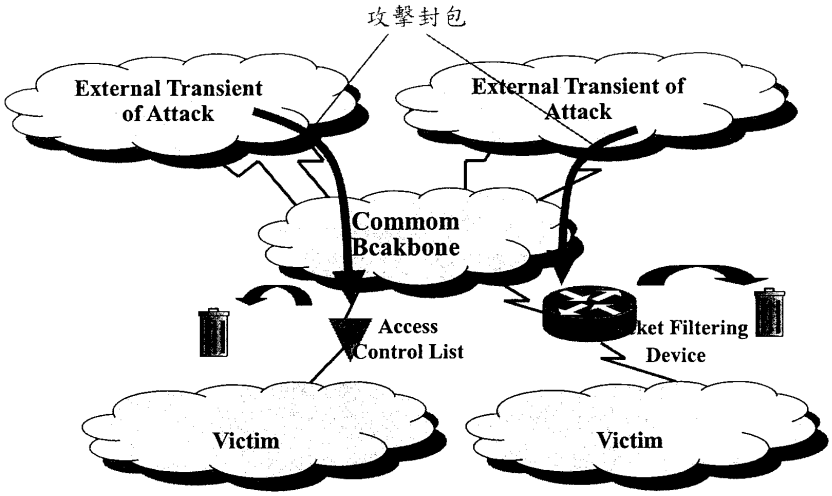
附圖四:減輕機制-blackhole

◆ Packet filtering

→ 透過於路由器上設定存取控制清單(Access Control List)的方式將所有的攻擊封包過濾掉(Packet Filtering)，主要適用於下述狀況。

- 攻擊封包為固定 IP Address。
- 對阻絕服務攻擊(DOS)非常有效。
- 可立即恢復受攻擊主機的正常運作。

不管是 Blackholing 技術或 Packet Filtering 技術，當我們對攻擊行為進行處理時，上述機制應該建置在遠離受攻擊用戶的地方，最好的地方就是在所維運網路的邊界，以降低對網路的影響。



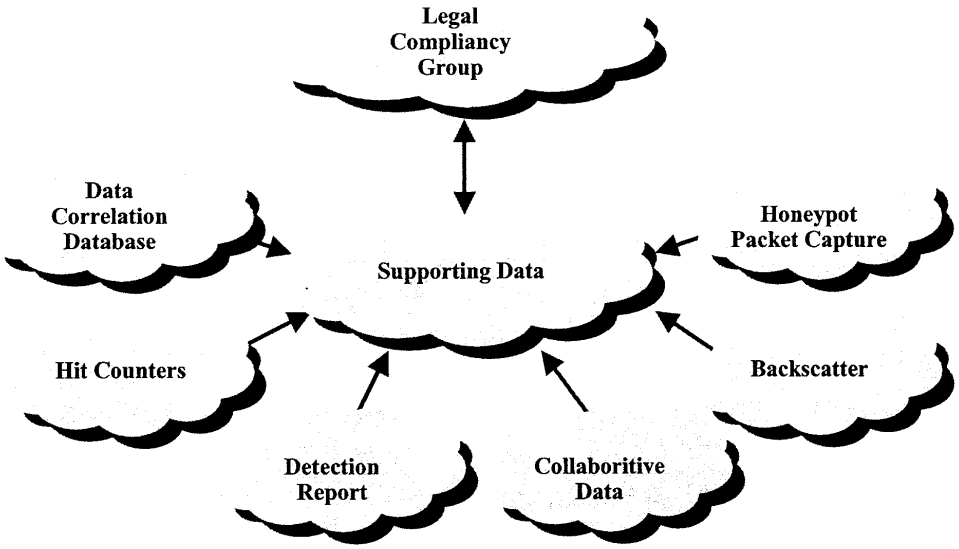
附圖五:減輕機制-Packet Filtering

(5).調查 (Prosecution)

經過減輕(Prosecution)的程序雖然能減緩(或解除)受攻擊主機(或網路)所受到的影響，但是攻擊仍然存在，因此最後的步驟，就是對攻擊源頭進行追查。為了要確認攻擊的源頭，必須具備下列幾個項目：

◆ Traceback abilities

→ 傳統的追溯(Traceback)方式，都是透過路由器一步一步往回查，不僅曠日費時，往往需要最優秀的工程師去執行這項動作。但透過上述安全裝置的佈署，不但可快速的阻絕攻擊，更可節省人力的耗損。



附圖六:佐證資料

◆ Peering/Customer collaboration

→『網際網路帶給人們最美好的事情是透過它可以連接到任何人; 網際網路帶給人們最糟糕的事情也是透過它可以連接到任何人』，正因為透過網際網路我們可以連接到任何人，所以對網際網路安全的維護並不是單一業者的努力就足夠。必須結合各業者及用戶的力量，透過共同研究的方式，找出方法來解決網路安全的問題。

◆ Peering/Customer cooperation

→對於攻擊事件的處理與源頭的追查，也必須透過業者與客戶的共同合作，才能達到最好的效果。尤其是平時就必須建立所謂的『熱線電話』，雖然一般網際網路業者都有所謂的客服中心，但這些服務人員大都不是真正的網路管理者，當攻

擊事件發生時，並沒有能力處理。因此與各業者及用戶間真正有能力、有權限處理的人員建立聯絡管道，對於攻擊事件的追查與排除都會有所助益。

◆ Supporting data

→上述安全設備所蒐集的資訊及整個攻擊事件的處理過程，都應該詳細紀錄，除了可作為日後追究相關責任的資料外，也可以作為相關處理程序檢討改進的依據。

肆、『安全維運中心』(SOC)建置

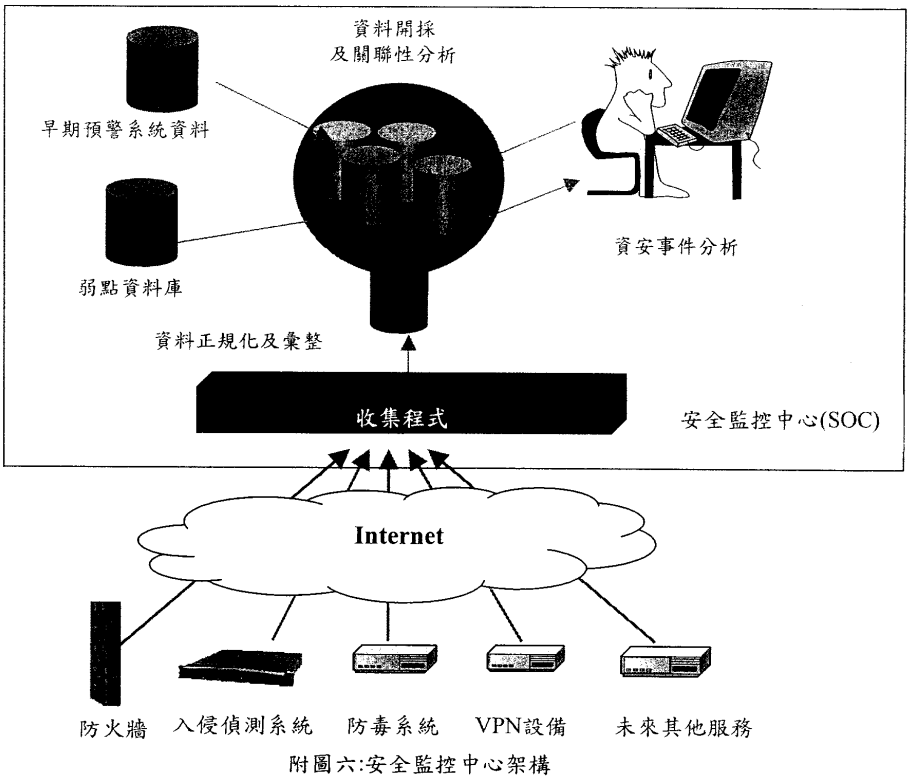
4.1 概說

有人會問，為什麼需要『安全維運中心』呢？『安全維運中心』能為我作些什麼？『安全維運中心』(SOC)的主要任務之一是監控管理客戶的資訊安全狀態，包括對安全設備的狀態監控、更新及設定資訊安全設備、以及提供用戶有關資訊安全的建議等工作。也許又有人會問，上述的工作交給網管人員不可以嗎？主要是因為防火牆及入侵偵測系統這些安全裝置，每天會產生大量複雜且難以管理的告警資料，其中包含有急需處理的資訊安全事件，但是也存在許多安全裝置誤判的假安全事件。對於一般的網管人員而言，要從不同廠牌的安全設備所產生之格式不一的告警訊息中判斷出真正的資訊安全事件，並且能正確且迅速的加以處置、因應，是一件非常困難的事，所以『安全監控中心』的主要功能即是提供客戶專業的資訊安全服務，以協助客戶管理資訊安全設備及處理資訊安全事件。那麼為什麼我不自己建立一個『安全監控中心』？主要是因為『安全監控中心』的建立在人力及金錢的投資相當龐大，往往不是單一企業願意承擔的，這也就是為什麼企業願意接受『安全監控中心』所提供之『資安管理服務』(MSS)的原因。

4.2『安全監控中心』的建置

在實習的過程中，我們瞭解到監控管理客戶的資安狀態是『安全監控中心』的重要工作之一，但是由於需要控管的資訊安全設備數量及種類繁多，且每個設備所產生的事件紀錄也很驚人，如何有效地蒐集彙整分散在各處且內容、格式各異的設備事件紀錄，進一步透過關聯性分析(Correlation Analysis)的處理程序，找出需要處理的『資安事故』並排定嚴重等級與應採取的行動，是在實習過程中各個『安全監控中心』都會討論到的核心技術，這也是『安全監控中心』能否有效經營的關鍵因素之一。

附圖六即為『安全監控中心』在管理客戶資安狀態時的處理流程圖，首先必須取得客戶之相關設備的安全狀態資訊，而防火牆、入侵偵測系統(IDS)、或提供關鍵服務的主機等設備正是維護資安防線的關鍵設備，因此把這些設備的事件紀錄(event log)傳送至『安全監控中心』，作進一步的彙整、分析及研判，再由『安全監控中心』人員提供正確且有效的處理建議與回應方式。

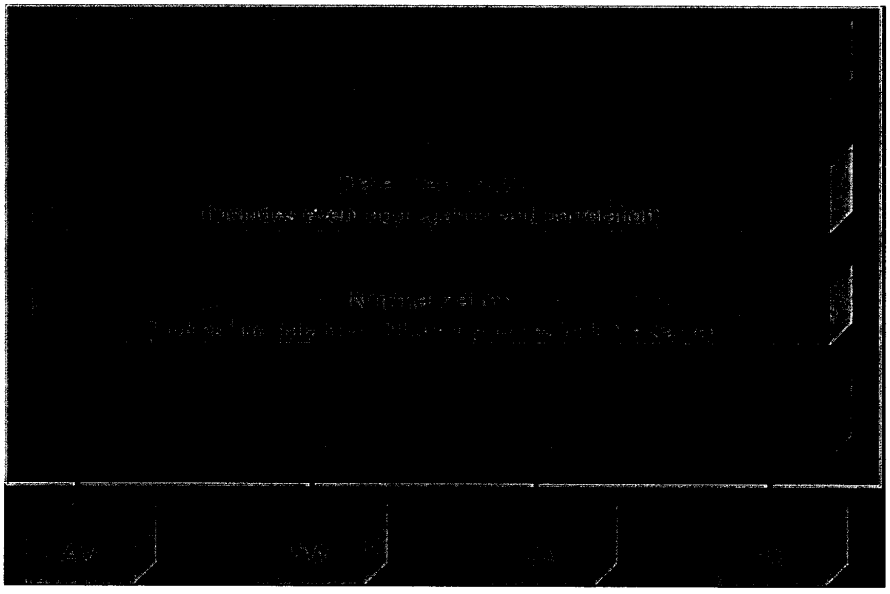


附圖六:安全監控中心架構

在此次研習中，我們看到了賽門鐵克(Symantec)公司的 Calterian、Incident Manager (IM)與 netForensics 公司的 Security Information Management (SIM)等三種可用於建置安全監控中心的解決方案，各解決方案在事件紀錄的蒐集和彙整、進一步分析建立這些事件的關聯性、研判可能發生的資安事故、及提供管理介面供相關人員執行資安事故的管理與回應程序等方面的做法都各有相似及相異處，詳細的比較項目及說明請參考 4.3 節的內容。不過，在進行 Calterian、IM、與 netForensics SIM 之解決方案的比較前，必須先就

整個資安事故的辨識與管理流程有更詳盡的說明，以便瞭解 4.3 節比較表中的項目及意義。

附圖七為『資安事故』之辨識與管理流程圖，共可分為 4 個階段，首先在『事件蒐集』階段，必須從各個安全設備(如：防毒產品、防火牆、弱點評估產品、入侵偵測系統...等等)或系統主機取得需要分析的事件紀錄；接著經過『正規化』(Normalization)程序的階段，將各種異質的事件紀錄轉換為標準格式的事件；再透過『事件簡化』階段的事件彙整和建立關聯性之程序，研判可能發生的資安事故；最後一個階段利用圖形化的管理介面或報告將資安事故的結果及用以研判的事件紀錄呈現給相關人員，以輔助相關人員作事故的回應與處理。



附圖七：『資安事故』之辨識與管理流程圖

接下來為 4 個階段的工作項目及說明：

→ 事件蒐集階段：負責蒐集各家廠商之資訊安全相關設備的事件紀錄，可能的蒐集方式有直接在設備上安裝『代理程式』(Agent)，或指定設備將事件紀錄傳送給獨立的『代理程式』，之後由代理程式負責傳送事件紀錄給執行『正規化』的元件。

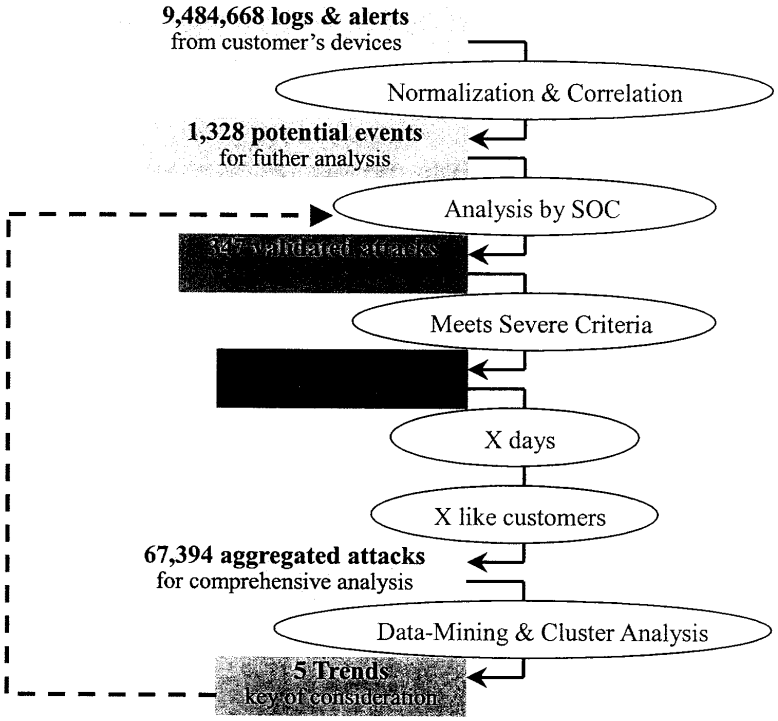
→ 正規化(Normalization)階段：由於各廠商之資安設備的事件紀錄並未採用相同的儲存格式及內容，所以為了減低下一個階段處理資料的複雜度，需要把蒐集到各種形式的事件紀錄對應轉換為一個共通的標準格式，此標準格式可能會定義儲存的格式(如：XML、Database)，與事件紀錄的欄位(如：事件 ID、時間、來源、事件描述等)。此處理程序稱之為正規化。

→ 事件簡化階段：先將大量的事件紀錄經過精鍊處理後，再透過建立關聯性的程序，判別可能發生的資安事故，分為以下兩個程序：

- 彙整(Aggregation)：將大量正規化後的事件紀錄作精鍊及最佳化的處理，例如：消除多餘或重複的項目，判斷事故類型及歸類，稱之為彙整程序。
- 建立關聯性(Correlation)：負責判別相關事件是否為需要管理之『資安事故』的技術。一般而言，建立關聯性的自動化方式有兩類：

i. 根據事先定義的規則：規則的來源可以由廠商或使用者提供，可研判是否發生資安事故的規則像是當一段時間內，出現特定的樣板(pattern)時，且符合一定的規則，就可將這些相關事件結合為一個資安事故。

ii. 根據事件嚴重性的加權：每個資安事件都具備一個可能帶來之影響的嚴重性權值，所以可由資安事件的嚴重性累積，將資安事件提升為資安事故。



附圖八：『資安事件』之處理流程圖

藉由關聯性的分析，不但可簡化事件紀錄(event log)並從中判斷出真正的資安事件，進而發佈資安事故警訊。並可從所蒐

集到的資料判斷出網路異常狀況的統計或趨勢，做為早期預警的機制。

→ 視覺化(Visualization)階段：提供相關人員立即查詢資訊安全狀態的介面，介面類型可能有方便即時監控的主控台介面，可依需求查詢資安狀態的安全網站(security portal)，以及定期發佈的報告等形式。

經由事件紀錄的蒐集、彙整、分析，建立這些事件的關聯性之後，對於資安事件的判斷又可分為兩種模式: 避免False Negative產生的模式及避免False Positive產生的模式。所謂的避免False Negative產生的模式是指關聯性系統不對資安事件作過多的研判，管理介面所顯示的僅是經關聯性系統處理、比對過的資料，至於該資料的嚴重性及其所代表的意義，完全交由專業人員作進一步的判讀及處理，其優點是不會漏掉任何一件可能危害到資訊安全的事件，而缺點就是需要大量的專業處理人員，賽門鐵克的Calterian就是使用這種模式；避免False Positive產生的模式之處理方式正好與避免False Negative產生的模式相反，它必須倚靠關聯性系統的判斷，解讀出系統所認為真正關鍵且迫切的安全事件，再將相關的處理措施顯示於管理介面上，其優點是管理人員僅需提供適當的訓練即可勝任，而缺點就是關聯性系統可能因為誤判或是設計不良，而無法篩選出真正的安全事件，賽門鐵克的

IM 以及 netForensics 的 SIM 都是使用這種模式。

經過上述的處理過程後，資安事件應變小組就會對相關安全事故進行研究，尋求解決的辦法，並提供遭受攻擊的客戶適當的安全建議及更新組態檔設定；對於其他未受攻擊的用戶，則提供資安事件的早期預警訊息。除此之外，『安全監控中心』並會對該事件(或現象)進行追蹤觀察，藉以掌握後續的發展趨勢。

4.3 解決方案的比較

接下來的內容將說明所實習之『安全監控中心』(SOC)的解決方案在『資安事故』之辨識與管理程序上的做法與比較。以下為 3 個解決方案的簡介：

- Symantec Calterian：由賽門鐵克購併之 Riptech 公司所研發的『資安管理服務』(Managed Security Service，MSS)解決方案。整個系統共花費 30 個資訊安全專家、4 年的時間完成研發建置，是一套可以建置及維運『安全監控中心』(SOC)的完整解決方案。
- Symantec Incident Manager (IM)：可即時對企業各處的安全設備所產生之事件紀錄進行關聯性分析，以辨別資安事故，並排定處理的優先順序。此解決方案透過資安事故辨識、完整的資安事故生命週期追蹤、動態地排序資安事故與採取行動的優先順序，讓企業將安全事件轉換為有優先順序、可供行動參考的情報資料。

- netForensics Security Information Management (SIM)：SIM 解決方案採即時方式蒐集、分析整個企業中所有安全裝置的事件紀錄，並建立起事件的關聯性，經過關聯性處理程序所得之結果，會顯示在一個集中式、即時式的主控台，供相關人員作即時的處理與回應。

表 1 Calterian、IM、netForensics SIM 之技術比較

比較項目	Symantec Calterian	Symantec Incident Manager (IM)	netForensics SIM
事件蒐集階段			
系統需求	必須在控管設備上安裝 Rimporter『代理程式』(Agent)。	SESA Agent / Collector	不需要在控管設備上安裝任何的軟體程式，但必須佈署 netForensics『代理程式』，負責事件蒐集的工作。
需安裝之『代理程式』的數量	根據控管設備的數量。	根據接收之資料格式(syslog...)的種類。	根據接收之資料格式(syslog...)的種類。
傳送事件的安全性－在『代理程式』與接收系統之間	採用 SSL 進行資料的加密。	採用 SSL 進行資料的加密。	提供附加的安全功能進行資料的加密(IPSec)。
蒐集事件的途徑	網路	網路	1. 網路 2. 檔案
支援的產品	➢ Check Point FW-1/VPN-1 ➢ CISCO PIX ➢ NetScreen ➢ Symantec Enterprise Firewall ➢ Symantec VelociRaptor ➢ CISCO IDS Host Sensor ➢ Entercept ➢ ISS RealSecure Host Sensor ➢ Symantec Intruder Alert ➢ CISCO IDS Network Sensor ➢ Enterasys Dragon ➢ ISS RealSecure Network Sensor ➢ Snort ➢ Symantec ManHunt ➢ Symantec NetProwler ➢ Symantec Gateway Security ➢ NOKIA	➢ Symantec ESM Bridge v5.5 ➢ ISS RealSecure ➢ Workgroup Manager 6.x ➢ RealSecure Network Sensor 7.0/6.5 ➢ RealSecure Host Sensor ➢ RealSecure Server Sensor ➢ RealSecure ISA Server ➢ Symantec Enterprise Firewall 7.0 ➢ Checkpoint NG w/SP3 on Win2K ➢ Cisco PIX 6.2 ➢ Symantec Host IDS 4.1 for Windows, and Solaris ➢ Symantec Intruder Alert Bridge v3.6 ➢ Symantec Anti-Virus 8.x ➢ Symantec SMTP Gateway 3.1.1 ➢ Symantec Event	➢ Cisco Secure PIX ➢ Cisco Secure IDS ➢ Cisco Secure ACS ➢ Cisco IOS Firewall / IDS / ACL ➢ Cisco VPN Concentrators ➢ Cisco Routers, Switches, Content ➢ Cisco Info Center, VMS, CSPM ➢ Psionic IPS ➢ Okena – Host based IDS ➢ Arbor ➢ Check Point Firewall-1 ➢ Computer Associates ➢ CyberGuard ➢ Enterasys ➢ Entercept – Host based IDS ➢ ISS Real Secure - Host/NW IDS ➢ McAfee ➢ Microsoft Windows ➢ Netscreen ➢ Secure Computing

		Collector for Enterasys Dragon	Sidewinder ➢ Snort ➢ Symantec ➢ Tripwire ➢ UNIX Log Data ➢ Other devices via Universal Agent
提供資料格式或內容的訂作服務	無 (請見說明 1)	是 (請見說明 2)	是 (請見說明 3)
正規化階段			
經正規化後的資安事件數量	未知 (請見說明 1)	將 5,564 個事件對應至 2,356 個標準事件。	將 20,000 個事件對應至 100 個 netForensics 所定義的 Alarm ID (nF 事件)。
共通的標準格式	未知 (請見說明 1)	Symantec Enterprise Security Architecture (SESA)	XML
資料庫平台	Microsoft SQL	IBM DB2	Oracle
事件簡化階段			
彙整程序			
資安事件的類別 (category)	未知 (請見說明 1)	18 大類，79 個子類。	分為以下 9 個類別： ➢ 阻絕攻擊(Denial of Service) ➢ 試圖偵查 (Reconnaissance Attempts) ➢ 系統狀態／組態設定(System Status / Configuration) ➢ 未知／可疑 (Unknown / Suspicious) ➢ 電腦病毒／木馬程式(Virus / Trojan) ➢ 違背政策(Policy Violations) ➢ 應用程式滲透 (Application Exploits) ➢ 鑑別／存取／授權 (Authentication / Access / Authorization) ➢ 迴避(Evasion)
自訂資安事件的類別	未知 (請見說明 1)	是	是

建立關聯性程序			
判別『資安事故』的方式	人工 (請參考說明 4)	自動	自動
建立關聯性的方式	Data Mining 方式	➢ 以規則為基礎(rule based)。	➢ 以規則為基礎(rule based)。 ➢ 根據事件的『嚴重性』(Severity) 權值。
建立關聯性的預設規則(rule)數量	無	32	40
提供使用者自訂建立關聯性的規則	無	是	是
可結合企業的資產評估	無	是 (請見說明 5)	是
建立關聯性之標的	降低『誤判為假』(False Negative)的情況。	降低『誤判為真』(False Positive)的情況。	降低『誤判為真』(False Positive)的情況。
整合弱點評估技術	否	是	是
視覺化階段			
客戶的身份認證機制	SecurID (one-time password)	無	無

說明：

1. 由於 Calterian 為 Symantec 提供『資安管理服務』(MSS)的工具與技術，並非一套產品。
2. SESA Software Development Environment (SDE) 提供完整的 Application Programmer Interfaces (APIs)集合，以整合其他產品的安全事件資訊至 SESA 平台。(消息來源：Symantec 公司的參考資料)
3. 針對 netForensics『代理程式』無法接收的資料格式，可依客戶需求在兩星期內訂製出一個『代理程式』。(消息來源：netForensics 公司的說明)
4. 先將資安事件關聯為『警示』(alert)，再經由人為判斷是否為『事故』(incident)。
5. 根據每項資產的相對機密性、完整性及可用性來進行『資安事故』的分級。

伍、 實習心得與結論

經由此次的實習課程，除學習到上述章節所詳述的資通安全技術外，我們也歸納了以下幾項心得與結論。

一、 HiNet提供了多種網路與加值服務，各類資安威脅如資料竊取、駭客入侵、病毒(蟲)與 DoS/DDoS 攻擊等等，對 HiNet 均會造成不同程度傷害與損失，但尤其以 DoS/DDoS 攻擊所造成的影響最大範圍最廣，不止會造成業務無法正常提供服務，也會影響 HiNet 廣大用戶正常上網的權益，因此，我們必須特別針對這類攻擊建立偵測與防護機制。同為 ISP 的 AT&T 也意識到 DoS/DDoS 攻擊對其威脅甚大，特別採取主動偵測與防護機制，據其統計，所建立的機制大幅縮短了 DoS 攻擊的處理時間。

二、 HiNet 要建置自己的安全維運中心(SOC)，並提供資安服務，可採取以下兩種方式來達成，一為直接引進整套 SOC 完整的解決方案，這是最快也是獲得完整技術的方式，但所需成本非常高。另一種則藉由學習國外營運經驗與技術，評估採用合適的 SOC 監控系統，配合自行開發相關系統與運作程序，建立自主的技術與培養專業資安人才，這種方式在系統功能、擴充能力或有不足，建置時程或有耽

擱，但可大幅節省建置成本，因此，採用哪一種方式來進行，尚需進一步評估。

三、 紐約州政府(NYS)委託 Symantec 為其建置安全維運中心(SOC)，Symantec 為其規劃建置了一個成功的衛星 SOC 運作模式，即紐約州政府(NYS)的 SOC 為 Symantec VA SOC 的衛星 SOC。衛星 SOC 運作模式的特色在於在紐約州政府所監控到的資安訊息均不在衛星 SOC 做分析處理，直接送至 Symantec VA SOC 中心做有效的、準確的分析判斷後，再送回衛星 SOC 做必要的因應處理。因此，衛星 SOC 並不需要建置有功能強大的監控系統，也不需要有非常專業的安全技術分析員，既可節省人力及成本，也可做最有效的安全監控。HiNet 未來可利用這種模式為其他政府民間機關建立其自己的 SOC，既經濟又實用。

四、 面對各式各樣的資安威脅，如建立一個資安實驗室來驗證測試包括惡意程式、病毒(蟲)、駭客入侵等攻擊手法、防護技術與解決方法外，則能建立包括弱點、病毒(蟲)、安全事件相關知識庫(Knowledge Base)，不但於資安事件發生時，可即時地用來提供建議解決的方法，也可進一步作為員工教育訓練資安事件攻防及因應處理的實際研究案例。