資訊安全管控與SOC建置

報告日期	中華民國108年11月25日
報告單位	中科院資訊通信研究所
報 告 人	陳國鐘 組長

目錄

- 前言
- 資訊安全要素
- SOC歷史演進
- SOC關鍵核心
- SOC建置
- 結語

目錄

- 前言
- 資訊安全要素
- SOC歷史演進
- SOC關鍵核心
- SOC建置
- 結語

資通科技運用

資通科技(ICT)以數位形式、智慧運用帶動各產業轉型，朝向智慧生活邁進。

智慧生活 ⬆ 產業轉型 ⬆ 智慧運用 ⬆ 通資電科技

- 智慧終端
- Fintech｜精準醫療｜翻轉教育
- 工業4.0｜零售業4.0
- 智慧教育｜智慧照護｜智慧交通
- 智慧監控｜智慧安全｜智慧農業
- 雲端運算｜物聯網｜大數據/人工智慧
- 數位科技、智慧科技

4

資通安全問題(1/2)

- 行政院資安處處長簡宏偉表示:
  - 目前臺灣最常見的攻擊除了社交工程郵件外，就是APT（進階持續性威脅）攻擊。
  - 以2018年的統計數字為例，每個月有2億次的掃描，攻擊次數每個月平均3千萬次，2018年成功攻擊的次數為262次，達三級以上的資安事件則為6起，政府部門也會積極關注三級以上的資安事件協助處理。

iThome 108.11.4

5

資通安全問題(2/2)

影響企業持續營運前五大威脅、衝擊和趨勢

	威脅（Threats）	衝擊（Disruptions）	趨勢（Trends）
第一名	網路攻擊	無預警的資訊與通訊中斷	使用互聯網進行惡意攻擊
第二名	資料外洩	惡劣氣候	社群媒體的影響
第三名	無預警的資訊與通訊中斷	公共服務中斷	流失重要員工
第四名	安全事故	網路攻擊	新法規和更嚴謹的監管審查
第五名	惡劣氣候	安全事故	互聯網相關服務的普及和高度採用

資安相關

資料來源：英國持續營運管理協會，2017年5月

6

網路攻擊型態

- 新科技帶來創新創意和生活便利，但也帶來新的資安威脅和挑戰，稍有不慎即造成經濟重大損失。
- 網路攻擊型態：
  - 物聯網攻擊
  - 雲端攻擊
  - 行動裝置攻擊
  - APT攻擊
  - DDOS攻擊

資安威脅暴增

- 勒索病毒、DDOS 攻擊、變臉詐騙、商業流程入侵及零時差漏洞等惡意攻擊頻傳，數位經濟活動面臨資訊安全威脅。

資料來源：台灣經濟研究院

資安攻擊新型態

- 新型態的勒索攻擊不斷出現

物聯網資安威脅

- 物聯網時代「萬物皆聯網、萬物皆可駭」。
- 駭客利用遠端操控方式對目標附近之監視器進行操控，取得目標周遭環境清楚影像，獲得進一步攻擊資訊，展開另一波攻擊:
  - 帳號與密碼洩露造成監視裝置內容洩露。
  - 物聯網裝置遭遠端監控。
  - 聯網裝置遭植入木馬。

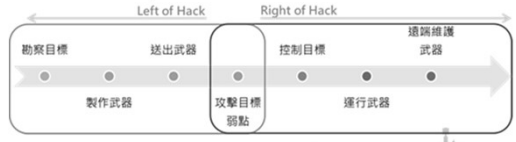
實際案例

網路攻擊鏈(Cyber Kill Chain)

Source: 洛克希德馬丁公司的 Cyber Kill Chain®框架模型

APT 進階持續性滲透攻擊

- 攻擊者從觀察目標、製作攻擊工具、送出攻擊工具、攻擊目標弱點、控制目標、於目標執行工具，至遠端維護攻擊工具，循序漸進控制目標，並立足於目標以能進行更進一步的攻擊。
- 此種攻擊過程即APT 攻擊 (Advanced Persistent Threat，進階持續性滲透攻擊)。



網路攻擊行為已不如過往那樣單純。從一個「Kill Chain (攻擊鏈)」可以知道一次網路攻擊可能分成好幾個步驟，分析師可從中了解最新的攻擊戰術、技術和程序的與如何防範。

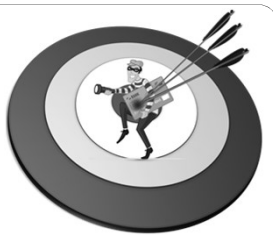
13

目錄

- 前言
- 資訊安全要素
- SOC歷史演進
- SOC關鍵核心
- SOC建置
- 結語

資訊安全管控

- 為維護資訊的機密性、完整性、可用性與驗證不可否認性，「資訊安全管控機制」遂因應而生！
- 面對當前網路環境威脅環伺，駭客可能透過各種管道破換前述任一個資訊確保要素，稍有不慎，可能釀成重大損失(財務、信譽...)。



SOC的建置便是運用科技能量與專業人員，落實資訊安全管控機制，達到網路威脅消弭之目的！

15

資安聯防架構

- 關鍵基礎設施八大領域機構，均要完成早期預警、持續監控、通報應變及協處改善等四大面向資安整備，以建立資安聯防架構。

16

資料來源：行政院資安處

目錄

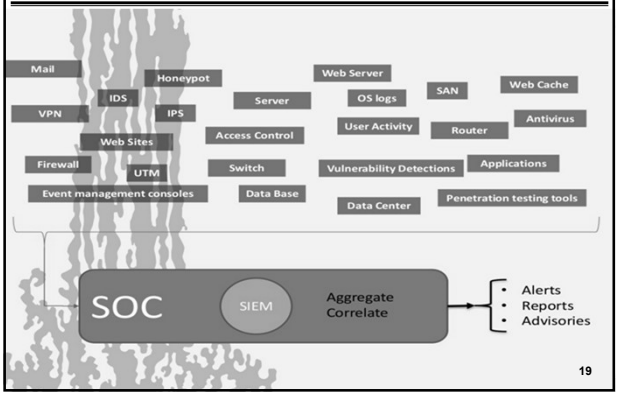
- 前言
- 資訊安全要素
- SOC歷史演進
- SOC關鍵核心
- SOC建置
- 結語

何謂SOC?(1/3)

- 何謂 SOC(Security Operaction Center)?
  - 負責網路安全的監控中心，有資安專家即　時對企業或機構的網路環境進行安全監控　與處理。
  - 可以自行建置，或是委託可資信賴的廠商　提供服務。
- SOC 提供的服務？
  - 監控與管理用戶 之資訊安全系統與設備。
  - 執行定期網路安全掃描，達到全天候之安全與回應。
  - 遠端執行用戶防火牆、入侵偵測系統、VPN、防毒系統之架設、設定與管理。
  - 資安事件處理。
  - 資料分析、評估與預警。
  - 提供資安環境改善建議。

18

何謂SOC?(2/3)



19

何謂SOC?(3/3)

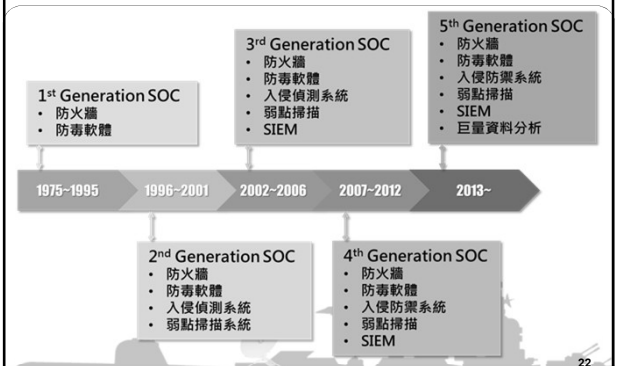
20

安全新挑戰

- 1974年為Ethernet (中文譯為「乙太網路」)的起始年，除帶來許多新穎的機會與發展，同時也開啟安全風險的另類挑戰。
- 早期網際網路的發展以軍事用途為主，後才逐漸普及於政府單位、教育機構、及普羅大眾。因此，自1975年迄今，隨著科技的不斷進展與駭客手法翻新，SOC的演進與發展也擴展至5代的歷史。

21

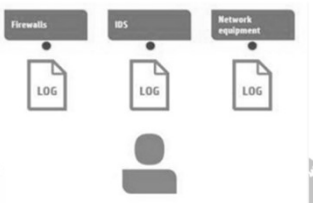
SOC歷史發展(1/5)



22

SOC歷史發展(2/5)

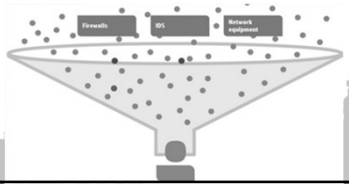
- 1st SOC
  - 第一代SOC由軍方與政府單位催生，防火牆與防毒軟體為其主要防護作為，營運內容則為監控與管理前述防護措施。
    - McAfee防毒軟體於1987年誕生。



23

SOC歷史發展(2/5)

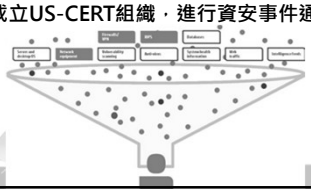
- 2nd SOC
  - 入侵偵測系統(Intrusion Detection System, IDS)於第二代SOC扮演極重要的角色，同時逐漸導入弱點掃描概念，並逐漸形塑SOC營運管理應有的相關程序。
    - 開源入侵偵測軟體Snort於1998年誕生。



24

SOC歷史發展(3/5)

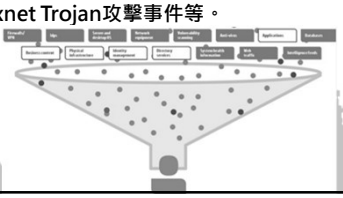
- 3rd SOC
  - Security Information Event Management(Monitoring)概念為第三代SOC的主要發展重點，亦即所謂的SIEM。
    - 殭屍網路(Botnet，或稱「傀儡網路」)與蠕蟲爆發等攻擊態樣日趨嚴重，如2003年爆發的SQL Slammer攻擊。
    - 2003年，美國成立US-CERT組織，進行資安事件通報與情資交換。



25

SOC歷史發展(4/5)

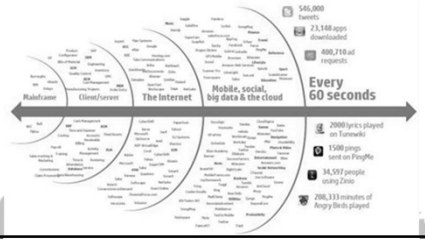
- 4th SOC
  - 第四代SOC除強化各相關技術外，亦深化「防禦」與「災害控制」的概念，盡可能抵禦進階的攻擊手法。
    - 以國家為首的網路戰、更大規模的網路犯罪、或激進駭客主義逐漸成形，如2007年愛沙尼亞事件、2010年的Stuxnet Trojan攻擊事件等。



26

SOC歷史發展(5/5)

- 5th SOC
  - 為加快安全管控反應速度，第五代SOC置重點於「主動化、自動化、智能化」，主要的關鍵技術便是巨量資料分析與機器學習的導入應用。



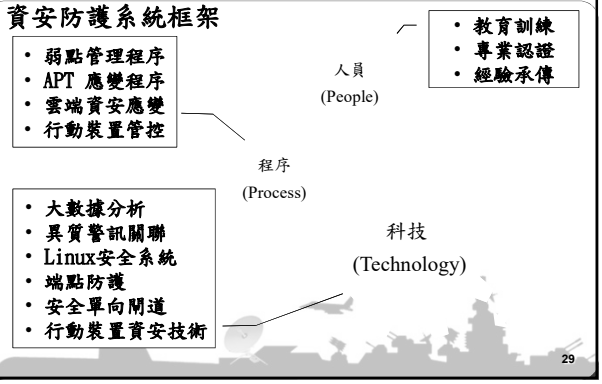
27

目錄

- 前言
- 資訊安全要素
- SOC歷史演進
- SOC關鍵核心
- SOC建置
- 結語

SOC核心三元素(1/3)

資安防護系統框架



29

SOC核心三元素(2/3)

- 人員
  - SOC各樣標準作業程序的建立與實踐、或是相關資安設備的操作維運，須仰賴專業人員的幫助，故人員是SOC核心三要素中極為重要的一環，也是企業組織必須用心經營的一塊，包含選用與延聘、職責劃分、教育訓練、職涯規劃等。
- 程序
  - 標準作業程序的建立與導入，可協助SOC整體營運管理過程有所遵循，同時能加快營運人員面對突發事件之反應速度。

30

SOC核心三元素(3/3)

- 科技
  - 科技主要用途在於輔助人員依相關作業程序完成特定任務。
  - 自第一代SOC以來，與SOC相關的科技已蓬勃發展，包括防火牆、防毒軟體、入侵防禦系統、SIEM等，或近來新興的巨量資料分析技術、使用者行為分析技術等。

31

目錄

- 前言
- 資訊安全要素
- SOC歷史演進
- SOC關鍵核心
- SOC建置
- 結語

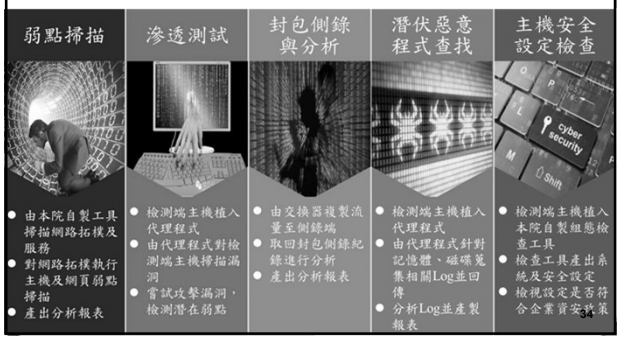
定期健整與檢測

- 平時定期健檢-常規性安全評估與檢測
- 狀況發生應處、緩解
- 事後鑑識、調修防禦機制

33

資安健檢

- 資安健檢技術能量，區分五大類



34

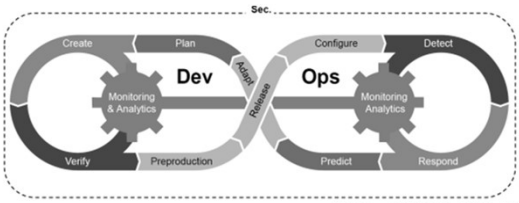
資安鑑識

- 資安鑑識技術能量，區分四大類

35

安全性軟體發展生命週期(SSDLC)

- 物聯網 萬物皆可駭的時代-因應IoT物聯網雲端時代的衝擊，應將資安概念引進在整個系統設計、開發、生產、部署、運用以及後續維運的整個過程。



圖源：Gartner JSI17 13B John A Wheeler EN DL.pptx

36

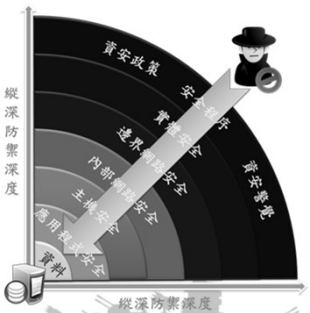
科技運用(1/3)

- 2011年，Lockheed-Martin提出Cyber Kill Chain架構，描述駭客為達攻擊目的所必須經過的各個步驟。

37

科技運用(2/3)

- 如能阻斷Cyber Kill Chain的任一環節，便愈有可能阻止一場攻擊行動。因此，遂衍生出Defense in Depth(中文譯為縱深防禦)，亦即透過多層次的防護機制，來強化受保護主體的安全，避免駭客長驅直入至受保護主體。



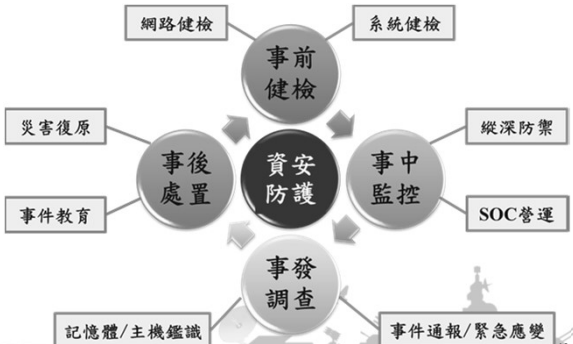
38

科技運用(3/3)

- SOC營運管理，最終會以情態牆收容與顯示，作為7*24監控、分析與處置。

39

資安防護循環(1/2)



40

資安防護循環(2/2)

事前健檢	事中監控
系統健檢：掌握組織各式系統之弱點資訊。	縱深防禦：增加駭客攻擊成本。
網路健檢：掌握組織網路架構可能弱點。	SOC營運：即時監控網路安全狀況。
事發調查	**事後處置**
事件通報/緊急應變：整理事件資訊回報CERT，並應變處理。	災害復原：依災害復原計畫執行。
記憶體/主機鑑識：調查入侵管道、方式等資訊。	事件教育：學習本次資安事件教訓。

41

作業程序建議(1/4)

- SOC營運過程包含偵測、分析與處置，各階段均需建立相關的標準作業程序，以供值勤人員參酌，並迅速作出反應與故障排除。

42

作業程序建議(2/4)

偵測類標準作業程序

1. 架構設計
   ① 偵測案例設計程序。
   ② 使用者與資產模型建立程序。
2. 設定管理
   ① SIEM部署架構程序。
   ② 資安事件收容設計程序。
   ③ 客製化監控儀表板設計程序。
3. 系統管理
   ① 系統權限管理程序。
   ② 系統維護與更新程序。
   ③ 機房門禁管理程序。

作業程序建議(3/4)

分析類標準作業程序

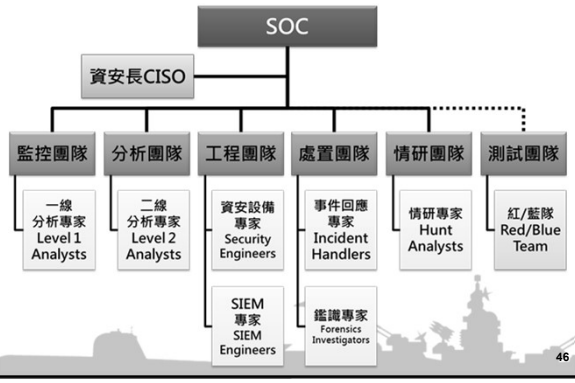
1. 事件調查
   ① 資料視覺化程序。
   ② 資安事件基礎調查程序。
   ③ 資安事件進階調查程序。
2. 威脅情資
   ① 威脅情資匯入程序。
   ② 威脅情資關聯程序。
3. 持續精進
   ① 防火牆調校程序。
   ② 入侵偵測系統調校程序。
   ③ SIEM關聯引擎調校程序。

作業程序建議(4/4)

處置類標準作業程序

1. 災害復原
   ① 災害復原計畫。
   ② 業務持續營運計畫。
2. 事件學習
   ① 資安事件案例宣導程序。
   ② 資訊安全再教育程序。
3. 通報管理
   ① 緊急事件通報程序。
   ② 事件總結報表計畫。

人員組織架構



角色執掌(1/5)

角色	編制	執掌
資安長 (CISO)	隸屬高階管理團隊，建議員額1員	擔任SOC高階管理者，負責帶領與管理團隊達成營運目標與績效指標，並維持整體營運過程之和諧，同時確保提供之服務符合「服務協議書(Service Level Agreements, SLA)」。
一線分析專家 (Level 1 Analysts)	隸屬監控團隊，建議員額至少4員	擔任SOC一線分析人員，負責資安事件即時監控，並視嚴重等級提升事件層級(Event Escalation)另須兼負SOC營運監控之協處窗口，維持正確的聯絡資訊，同時更新相關的文件。

角色執掌(2/5)

角色	編制	執掌
二線分析專家 (Level 2 Analysts)	隸屬分析團隊，建議員額至少3員	擔任SOC二線分析人員，負責規劃與制定相關分析作業之執行程序與子程序，同時持續蒐羅執行上的問題建議，以協助改善整體營運流程。此外，亦須針對一線分析團隊所提升之資安案件進行深度調查與分析，並適時提供處置建議供高階管理團隊參考。
資安設備專家 (Security Engineers)	隸屬工程團隊，建議員額至少4員	擔任SOC前端資安設備工程師，負責防火牆、入侵偵測/防禦系統、防毒軟體、弱點掃描等設備之架構規劃與建置維運。

角色執掌(3/5)

角色	編制	執掌
SIEM專家 (SIEM Engineers)	隸屬工程團隊，建議員額至少2員	擔任SIEM核心工程師，負責SIEM部署架構規劃建置，及相關參數設定、測試、上線部署等作業。
事件回應專家 (Incident Handlers)	隸屬處置團隊，建議員額至少2員	擔任SOC資安案件反應管理者，負責資安案件觸發時，能即時啟動調查與處置作業，並與單位高階管理團隊保持良好互動，以確保資安案件發生時，相關緊急應變程序能順利啟動。

角色執掌(4/5)

角色	編制	執掌
鑑識專家 (Forensics Investigators)	隸屬處置團隊，建議員額至少3員	擔任SOC資安案件調查人員，負責SOC資安案件鑑識調查任務，運用高端技術與工具，完成數位採證、數位鑑識、證據保存等作業，協助發掘案件根因與入侵管道及手法。
情研專家 (Hunt Analysts)	隸屬情研團隊，建議員額至少3員，可為專屬團隊，或由SOC營運團隊中各專業領域人員擇優組成。	擔任SOC情資數據分析工程師，負責從大量的歷史資料中，運用各式查詢、分析技巧，或塑模、假說等方式，識別與發掘潛藏的異常行為或惡意活動，以預判是否有新的攻擊威脅正在醞釀。

角色執掌(5/5)

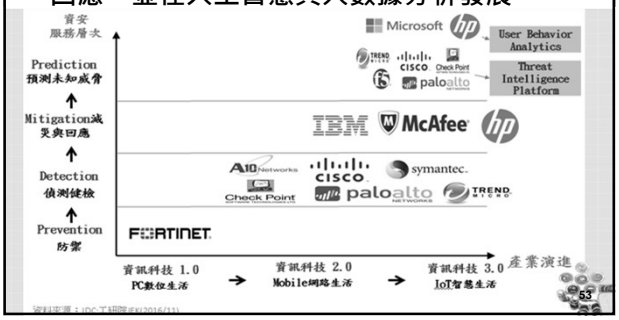
角色	編制	執掌
紅/藍隊 (Red/Blue Team)	隸屬測試團隊，建議員額至少4員，如單位政策許可，則建議委外辦理，毋須納編置正式團隊組成。	擔任SOC滲透測試團隊，運用各式工具，模擬駭客攻擊行為，驗證單位資安防護程度與應變速度。

目錄

- 前言
- 資訊安全要素
- SOC歷史演進
- SOC關鍵核心
- SOC建置
- 結語

結語(1/4)

- 資全發展趨向:從傳統防禦提升至事件減災與回應，並往人工智慧與大數據分析發展



結語(2/4)

- 因此，為有效降低因網路安全漏洞肇生之危害，確有必要於組織內部落實資訊安全管控，而透過SOC的建置，則為目前較佳且完整之解決方案。
- 本所自民國95年迄今，協助各單位建立資安監控系統，並自主研發端點電腦資產管理系統。近期針對新興智慧型手機應用技術，亦研發MDM管控程式與社群軟體通訊加密程式，於資安領域技術具備一定能量。

結語(3/4)

資安監控管理中心(SOC)
示意圖

智慧型手機管控

結語(4/4)

- 本所通過TAF認證，具有資安健檢與鑑識能量。
- 本所同時通過ISO 27001認證，專業團隊亦具備相關資訊安全證照。
- 歡迎一同參與科技研發行列。

感謝聆聽

E-Mail:gjong@ms13.hinet.net