

面對資安威脅大海嘯來襲

您該如何快速效率的自保自救

Speaker: 黃繼民 Jim Huang

前言

本課程內容以近期資安事件為例，透過事件分析與歷史學習方式，提供各位學員能藉此瞭解現今新一代資安威脅的模式特性，如何以具效率且精確的資安應變思維。

文中引用國內主要資安新聞媒體iThome報導作為討論案例，特此感謝。

大綱簡介

- 資安威脅大於你可想像的程度
- 資安與駭客的距離 = 漏洞
- 建置聰明效率的資安攻防策略
- 資安法規遵循是提升資安體質的王道
- 結論 | Q&A

資安威脅大於你可想像的程度

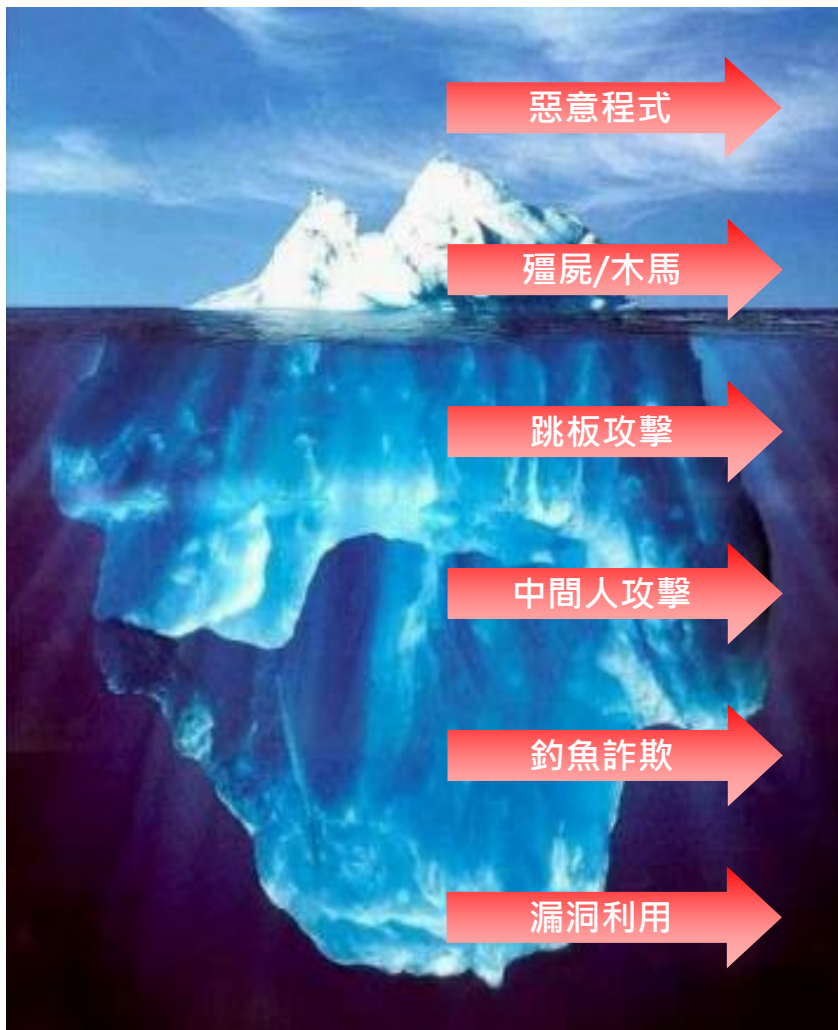


漏洞攻擊崛起

事件年份	事件主角介紹	事件影響介紹
2001	<ul style="list-style-type: none">Code Red會自行尋找並感染具IIS漏洞的電腦蠕蟲。Nimda「瑞士萬用刀」之稱，每15秒一次的攻擊頻率，只要一台電腦未清乾淨就會蔓延再生。	<ul style="list-style-type: none">造成26億美元的生產力損失與伺服器清除成本
2003	<ul style="list-style-type: none">Blast 疾風病毒，自帶修正程式更新功能，高速感染	<ul style="list-style-type: none">導致多家航空公司班機被迫延後或取消
2005	<ul style="list-style-type: none">ZOTOB蠕蟲利用MS05-039的隨插即用中的漏洞，通過TCP埠445散布。只感染未經修補的 Windows2000。	<ul style="list-style-type: none">美國多家主要媒體包括CNN及New York Time等系統當機
2008	<ul style="list-style-type: none">Conficker惡意程式針對利用 MS08-067的安全弱點攻擊電腦系統。	<ul style="list-style-type: none">高達 9 百萬台電腦受到感染，並衍生出多個變種至2018年一月 偵測數量仍維持在 2 萬以上
2014	<ul style="list-style-type: none">Heartbleed安全漏洞，源起OpenSSL加密的缺陷臭蟲 (Bug)	<ul style="list-style-type: none">網路史上最嚴重的安全漏洞，影響了全球網路加密資料的傳輸安全
2014	<ul style="list-style-type: none">Shellshock 針對Linux及Unix環境的資安漏洞	<ul style="list-style-type: none">包括Linux、Unix、Mac OS、網路設備、及任何使用Bash的網頁系統與Android等。
2015	<ul style="list-style-type: none">Angler 最成功的漏洞攻擊包，定期加入新的漏洞攻擊碼	<ul style="list-style-type: none">勒索攻擊興起
2016	<ul style="list-style-type: none">Mirai 專門針對Linux韌體IoT裝置的惡意軟體，之後也發展針對Windows系統。	<ul style="list-style-type: none">造成數十萬的聯網裝置成為殭屍網路節點創下高達1 Tbps的DDoS 攻擊流量
2017 ~2018	<ul style="list-style-type: none">EternalBlue(永恆之藍)漏洞攻擊利用MS17-010微軟安全性弱點	<ul style="list-style-type: none">造就引發全球恐慌的WannaCry(想哭)及Petya勒索軟體衍生包括SambaCry及WannMine挖礦軟體台積電機台產線大停機入侵家用網路裝置成為殭屍機器，台灣居首位

參考來源:趨勢科技《電腦病毒30演變史》

現今資安威脅有高達90%是利用弱點漏洞！！



已知的攻擊威脅
(Known Knowns)

已知的未知威脅
(Known Unknowns)

未知的攻擊威脅
(Unknown Unknowns)

存在的漏洞
(未公布/未發現/未修補)

未知的資產
(IP/裝置/服務/帳號/權限)

錯誤的設定配置
(版本/組態/架構/結構)

人為的疏失
(操作/保管/授權/政策)

長期的空窗
(探查/盤點/更新/維護/反映)

過度的信任
(物/人/事/時/地)

令人傷心不止的WannaCry (想哭) 事件



- NSA美國國家安全局 遭到影子搨客組織入侵。
- 影子搨客釋出大量駭客工具於黑市。
- 永恆之藍 造成驚世攻擊WannaCry
- 變種攻擊手法 推陳出新....至今(尚未平息)!!

WannaCry威脅兩年未除 上月攻擊達6000萬次

Marcus Hutchins

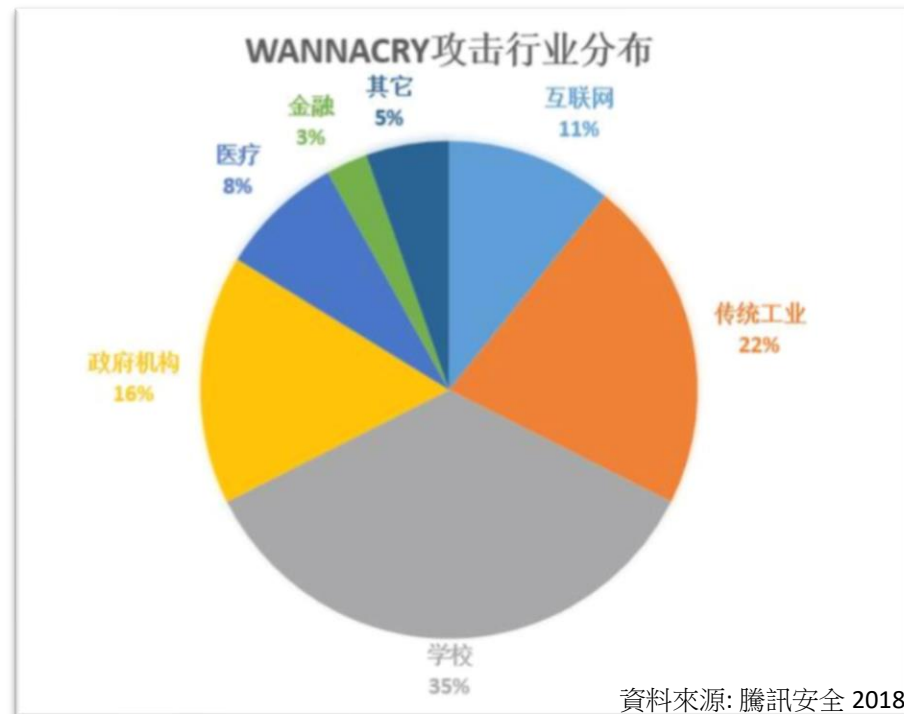
By StartupBeat on July 10, 2019

Like 10 people like this. Sign Up to see what your friends like.

全球散播勒索軟件WannaCry，自2017年5月起肆虐，文件會被加密鎖定，苦主必須向黑客支付贖金，例如加密貨幣。然而，這威脅至今未見緩解，仍潛伏各地數千網絡中。

科技媒體TechCrunch報道，當年有英國安全研究員MalwareTech，在電腦病毒發現了一個傳播開關（Kill Switch），向一個未註冊網域名稱發出請求。研究員花費8.29英鎊搶註網域後，病毒擴散渠道遭即時中斷，單是今年6月已攔截6000萬次攻擊。

資料來源:信報財經新聞



WannaCry.永恆之藍.EternalBlue

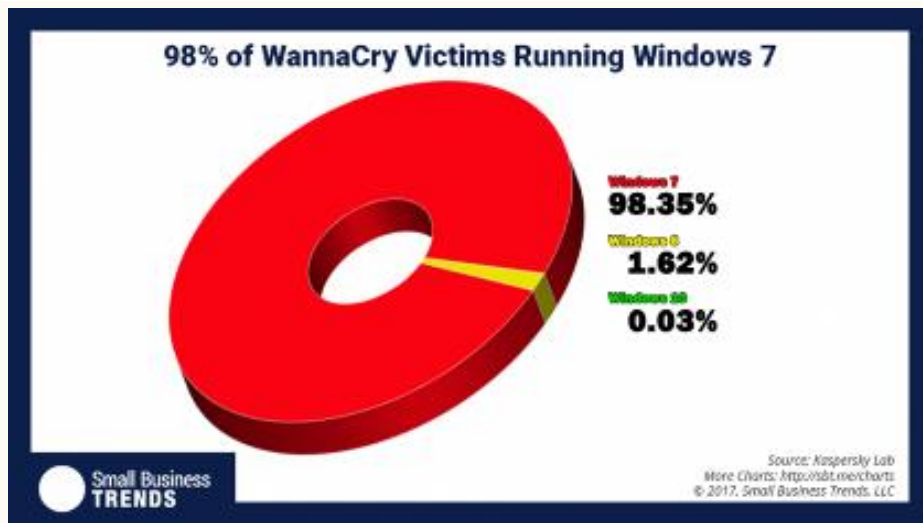
WannaCry's

EternalBlue

On Windows 10

- 2017年5月 爆發史上影響最大、傳播速度最快的全球性勒索攻擊WannaCry.
- 2017年6月 變種攻擊Petya 及 Not Petya 出現，針對主開機紀錄(MBR)·Win更新無效.
- 2017年6月 SambaCry 現身針對Linux系統設備(Server, NAS, IoT裝置).
- 2018年8月 台積電產線中毒事件禍首為WannaCry的變形種，損失新台幣26億元.

同樣令人想哭的抉擇...



Windows 7 明年初將會停止免費支援

Windows 7

Microsoft 採取收費式提供安全性更新

XFASTEST



惡意攻擊快速變種演化

- # EternalBlue(永恆之藍)
- # SMB漏洞利用 (SMBv1)
- # Port 445
- # MS17-010
- # 跨平台的威脅
- # 從「勒索」到「奴役」

WannaMine



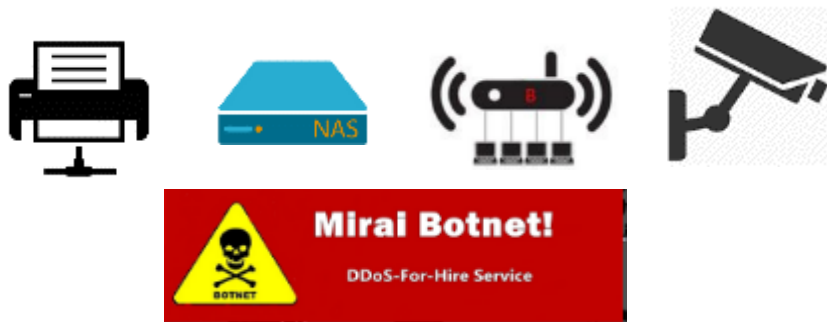
WannaCry

攻擊手法不斷試探著...



假設:

1. 受駭裝置不只是“網路印表機”？
2. 同樣的問題是否會發生在其他系統裝置？
3. 是否會被利用作為“跳板攻擊”？
4. 攻擊目標會否針對校務系統及基礎服務？
5. 被視為“攻擊來源”的影響性？



Country	Percentage	Rank
Taiwan	21%	1
China	14%	2
Indonesia	14%	2
Thailand	11%	3
India	10%	4

資料來源: TREND 趨勢科技

資安防護方法萬靈丹(真的嗎?)

新聞

勒索軟體鎖定NAS用戶，包括群暉科技、威聯通用戶都應提高警覺

包括群暉科技、威聯通等NAS用戶，都面臨駭客使用勒索軟體加密檔案、要求贖金的威脅。群暉科技追蹤發現此波攻擊發現，疑為Stealth Worker駭客組織所發動，要求使用者支付0.06個比特幣，約為新臺幣1.8萬元贖金。群暉科技呼籲用戶儘速升級儲存作業系統到最新版以自保，並應避免使用常見的Admin管理員預設帳號及弱密碼。

文 / 黃彥霖 | 2019-07-24 發表

讚 5.5 萬 按讚加入iThome粉絲團

Synology®

產品

解決方案

支援與下載

安全性

關於我們

搜尋

< 新聞稿



本校數學科網路儲存硬碟NAS遭勒索軟體入侵，將電腦裏的檔案加密無法開啟檔案，請所有教職員工儘速將所有個人重要檔案做好備份

本校數學科網路儲存硬碟NAS遭勒索軟體CryptoLocker入侵，將電腦裏的檔案加密，讓使用者無法開啟檔案，也沒辦法破解加密，藉此勒索300美元的解密贖金

網路犯罪 · 地下經濟興起

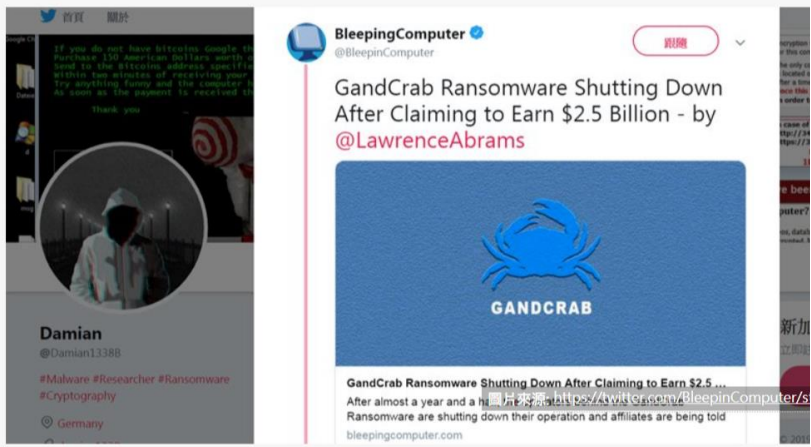
新聞

GandCrab勒索軟體賺了20億美元後宣佈

勒索軟體GandCrab作者聲稱將關閉惡意程式，更催促受害者儘速付款，否則資料便無法救回

文/ 林妍瀟 | 2019-06-03 發表

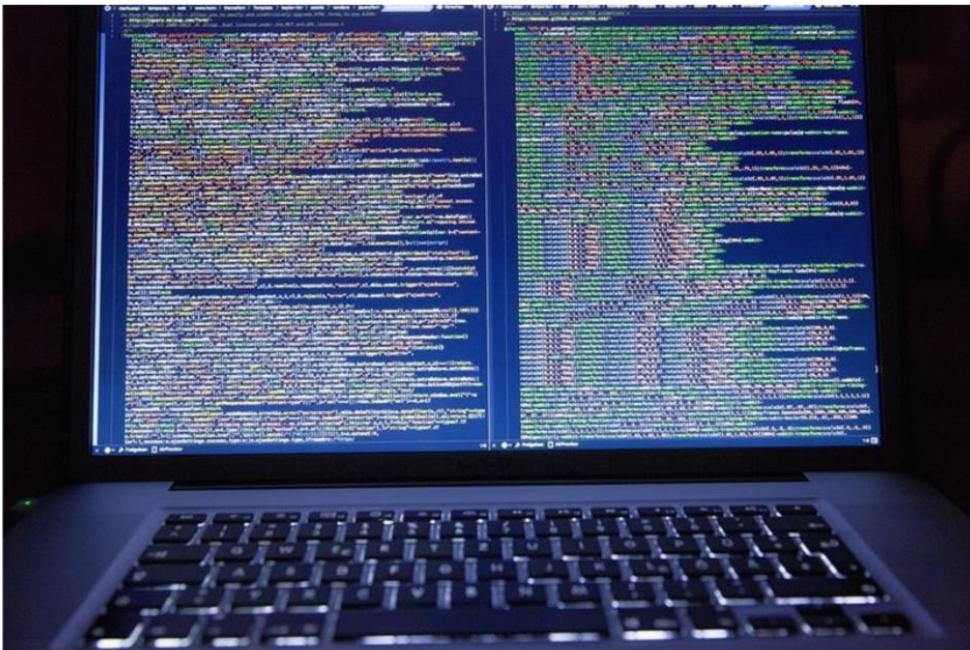
讚 5.5 萬 按讚加入iThon



資料來源: iThome

北韓駭客生財有道 網軍實力超乎想像

最新更新：2017/10/17 21:42



根據估計，北韓每年發動網路攻擊獲利可能多達10億美元（約台幣303億元），約是北韓年均出口總值的1/3。此為示意圖。（圖取自Pixabay圖庫）

資料來源: 中央通訊社外電

XX 服務取得更加便利，工作更有效率！



駭客服務

	密碼竊取工具 \$900		社交工程病毒 \$1500
	雲端服務帳戶 \$200/個	DDoS攻擊服務 \$200/hr	
完整個人資料 \$40/筆			客製化遠端連線工具 \$10萬
	勒索軟體 \$3000起		

「駭客攻擊即服務」的時代來臨了

「DDoS服務」(DDoS as a Service)

Akamai發現「受雇型DDoS」鎖定Joomla等SaaS應用程式展開
攻擊

2015-03-12

網管人

Akamai資訊安全事業單位資深副總裁兼總經理Stuart Scholly表示：「軟體即服務（Software-as-a-Service；SaaS）供應商提供的網路應用程式漏洞，讓其持續淪為網路犯罪者的武器。他們現在又發展新型的DDoS（Distributed Denial of Service；分散式阻斷服務）攻擊方式及受雇型DDoS（DDoS-for-Hire）工具，鎖定易被入侵的Joomla外掛程式展開攻擊，在無窮盡的網路應用程式漏洞上再添一筆。企業必須準備好應對DDoS攻擊的防護計畫，以緩解DDoS可能利用數百萬台基於雲端的SaaS伺服器阻斷服務流量。」



iThome 分享了 1 則貼文。

2017年2月6日 · 🌐

因為購買DDoS攻擊服務的價格相當便宜，平均大約是1分鐘的DDoS攻擊流量只要1美元來看，甚至還有15分鐘的便宜DDoS試用服務。

駭客如果透過購買這類的DDoS攻擊服務，然後加上一封勒索信件，可以獲得7個~10個不等比特幣的贖金的話，是非常划算的投資和交易啊~

資安威脅已經超過你我可想像的程度

新聞

遭網路攻擊，路易斯安那州宣布進入緊急狀態

路易斯安那州在一個月傳出4起學校系統遭網路攻擊事件，導致電腦、電話與網路系統被迫中斷，州長宣布全州進入緊急狀態，召集各方資源與人力阻止資料遺失

文/ 陳曉莉 | 2019-07-26 發表

讚 5.5 萬

該州光是在今年7月就傳出有4個學區的學校系統遭到勒索軟體攻擊，其中，Sabine Parish的電腦系統與中央辦公室的電話系統都因此而停止運作，Monroe市學校系統的網路亦被迫中斷。

新聞

約翰尼斯堡電廠感染勒索軟體，居民半天無電可用

約翰尼斯堡的城市電力（City Power）公司遭惡意程式感染，使用戶近12小時無法用電，在恢復供電後，城市電力至今仍未說明勒索軟體的名稱。

文/ 林妍濤 | 2019-07-26 發表

讚 5.5 萬

按讚加入iThome粉絲團

讚 20

分享

基隆市府網站被勒索病毒入侵掛點3天 議員憂機密被盜

f 分享

LINE 分享

留言

列印

存新聞

2019-05-07 12:46 聯合報 記者游明煌／即時報導

讚 0 分享

基隆市政府全球資訊網上4日傳出被勒索病毒入侵，掛點3天，至今外部網路民眾已可上網，但內部網路仍未恢復，多名議員今天在市議會臨時會擔心資安恐出現問題，機密資料、民眾個資是否外洩。市政府研考處長黃駿逸說，市民個資未外洩，內部作業系統受影響，預估今天下午後可以全部恢復正常。

資安攻擊頻傳 從政府到企業都受駭



公共部門

2018年4月

高雄果菜公司
駭客鎖住交易電腦，威脅48小時之內付贖金；果菜公司最後以比特幣支付贖金

2018年12月

台灣高鐵
台灣駭客用手機駭入高鐵票務系統成功

2019年1月

台北市衛生局
298萬筆台北市民個人資料外洩

2019年6月

銓敘部
59萬筆資料外流，24萬名公務員個資曝光



金融服務業

2016年7月

第一銀行
東歐駭客集團入侵，盜領8327萬元

2017年2月

13家證券公司
台灣史上第一次，證券公司集體受到駭客勒索，並且對多家券商發動攻擊

2017年5月

雄獅旅遊
中國駭客入侵，36萬名消費者個人資料外洩

2017年10月

遠東銀行
被盜轉6010萬美元，最後仍有16萬美元尚未追回

科技業

2016年11月

華義
華義遊戲伺服器受到駭客攻擊，勒贖比特幣，價值台幣近百萬元

2018年8月

台積電
台積電生產線嚴重停擺

2019年3月

廣達
東歐駭客在紐約認罪，坦承竊取廣達身分，向臉書和谷歌詐取貨款約38億元台幣

2019年3月

華碩
軟體更新檔被入侵，導致上萬台電腦受影響

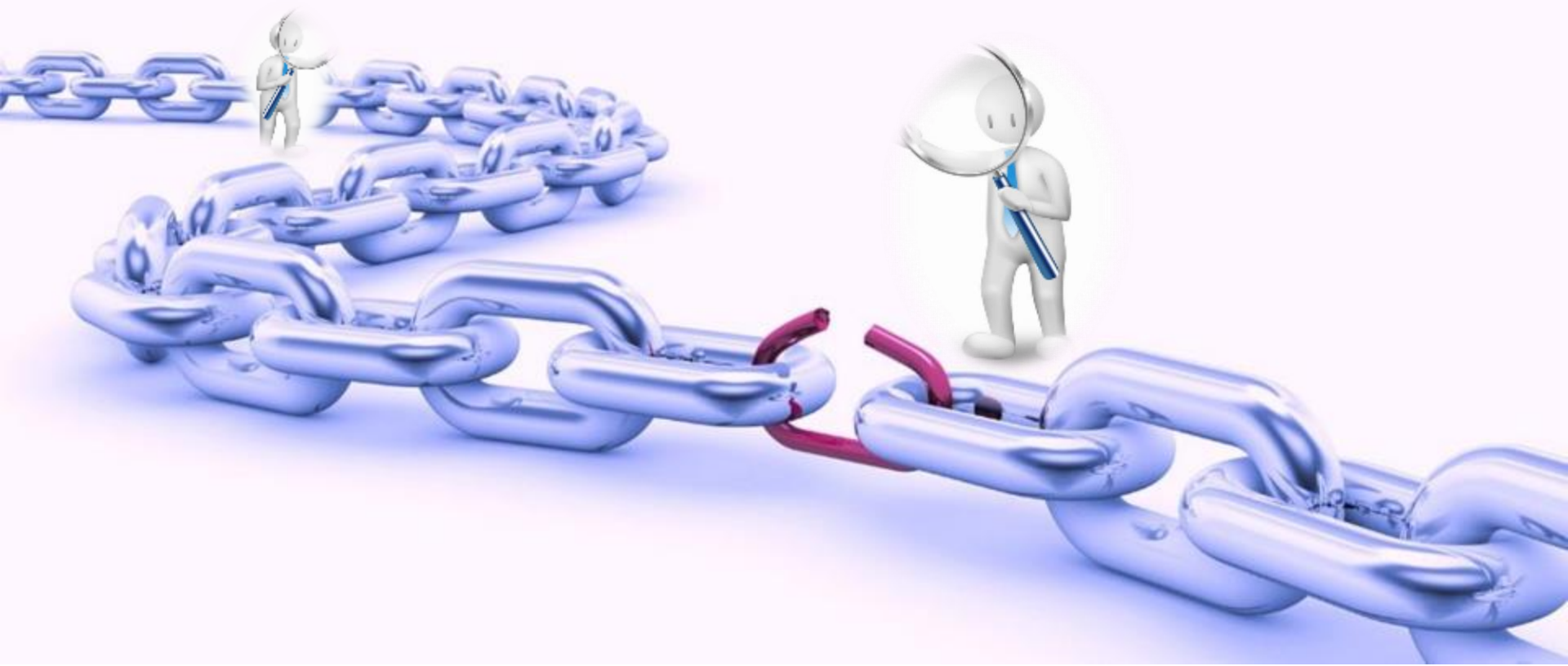
2019年4月

友訊
友訊和TOTOLINK共近2萬台家用路由器被駭客入侵，讓用戶進入假網站，騙取密碼

大綱簡介

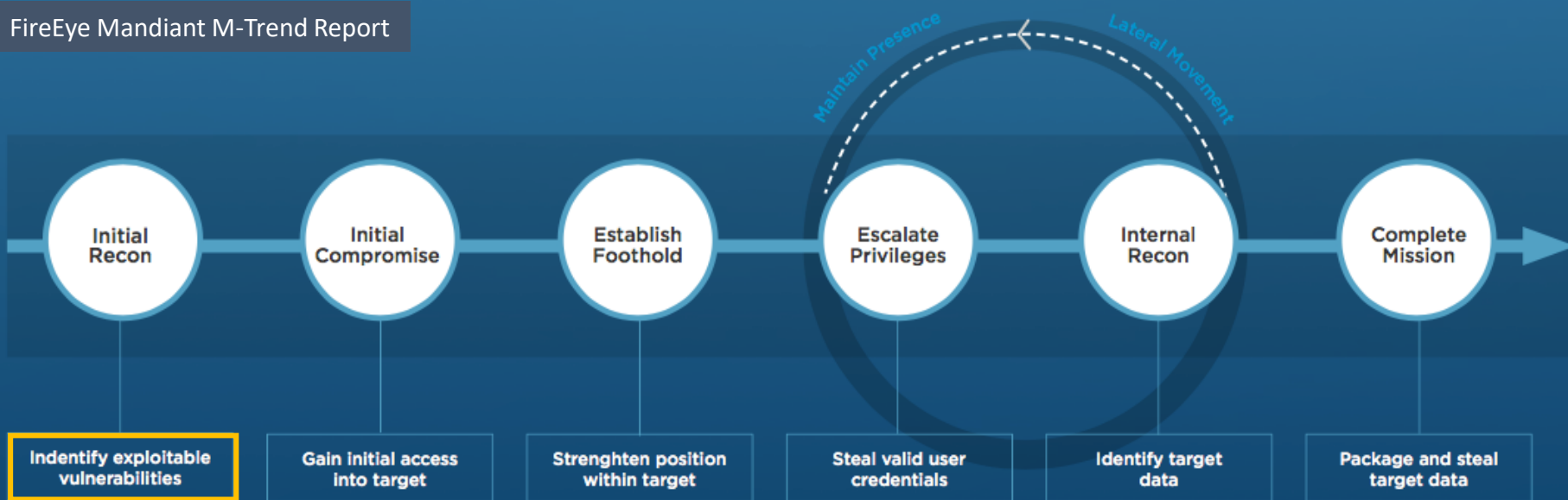
- 資安威脅大於你可想像的程度
- 資安與駭客的距離 = 漏洞
- 建置聰明效率的資安攻防策略
- 資安法規遵循是提升資安體質的王道
- 結論 | Q&A

「弱點/漏洞」重要嗎？



「弱點漏洞」是現今資安攻擊的「起手式」

FireEye Mandiant M-Trend Report



識別可利用的弱點

侵入應用程式或OS
的漏洞 (Exploit)

回 Call 控制中心

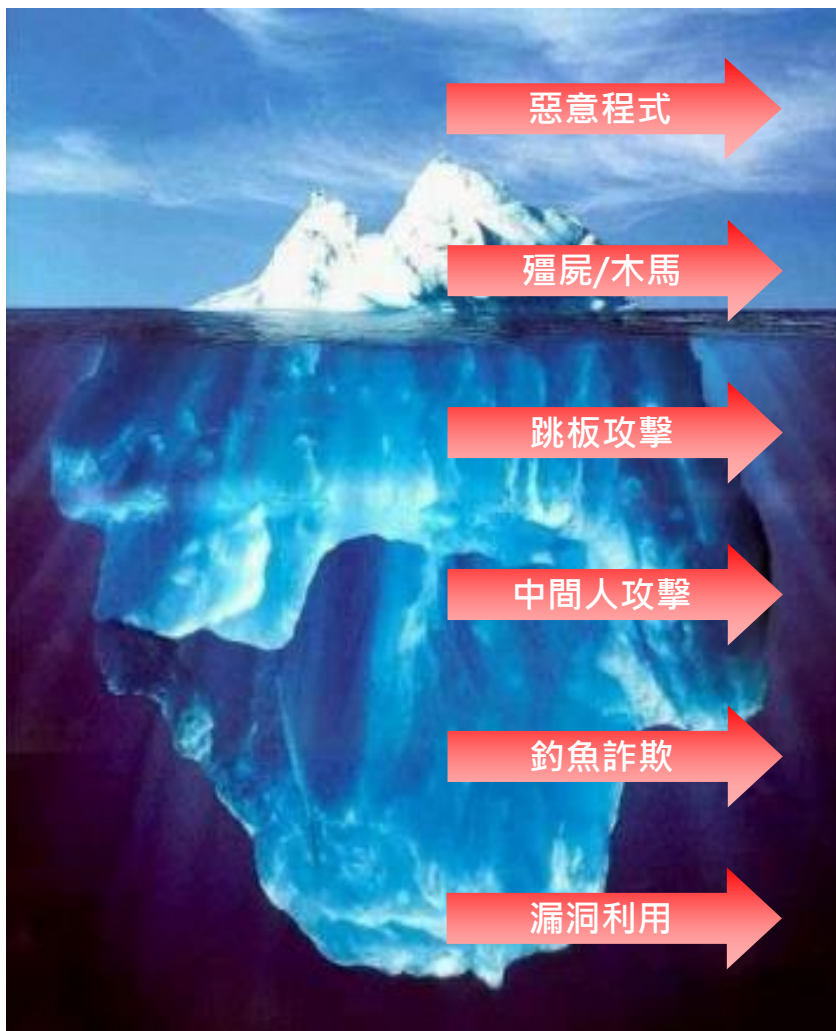
下載惡意軟體本體

橫向散播

資料竊取



現今資安威脅有高達90%是利用弱點漏洞！！



已知的攻擊威脅
(Known Knowns)

已知的未知威脅
(Known Unknowns)

未知的攻擊威脅
(Unknown Unknowns)

存在的漏洞
(未公布/未發現/未修補)

未知的資產
(IP/裝置/服務/帳號/權限)

錯誤的設定配置
(版本/組態/架構/結構)

人為的疏失
(操作/保管/授權/政策)

長期的空窗
(探查/盤點/更新/維護/反映)

過度的信任
(物/人/事/時/地)

安全崩壞只需要**1**個正確的點

阿基里斯 vs. 阿基里德



你所認為的安全



駭客



弱點

安全脆弱度只需要1個正確的點

新聞

政府電子公文系統被駭，主管單位竟企圖遮掩

行政院電子公文交換系統遭到駭客入侵，但負責國家資安的資通安全辦公室卻沒有在第一時間對外公開受駭事實，反而企圖隱匿

文/ 黃彥霖 | 2013-05-31 發表



張貼日期：2019/06/03

【資安漏洞預警通知】校園數位學習平台 WMP 智慧大師含有 Command Injection 漏洞

主旨：【資安漏洞預警通知】校園數位學習平台 WMP 智慧大師含有 Command Injection 漏洞

■ 內容說明：

- 本次通報的漏洞屬於Command Injection的高風險漏洞，如果管理者未在網站的輸入表單中過濾敏感字

新聞

美國大學所使用的ERP系統遭駭客入侵，62所學校受害

全球超過1,400個大專院校使用的ERP系統含有安全漏洞，雖然系統廠商已經釋出修補後的版本，但目前美國已有62間學校的ERP系統因為尚未更新版本，而遭駭客入侵

文/ 陳曉莉 | 2019-07-22 發表

讚 5.5 萬 按讚加入iThome粉絲團

讚 133 分享

計算機與通訊中心
網路系統組 敬啟

案例借鏡：第一銀行事件

第一銀行ATM盜領事件遭駭流程追追追

2018 台積電事件



資料來源：法務部調查局，iThome整理，2016年7月

猜猜看，以下弱點有甚麼共通處？



OpenSSH



Meltdown



Spectre

- ✓ 歷史悠久
- ✓ 使用率普遍
- ✓ 經常使用
- ✓ 習以為常



Zip Slip目錄走訪漏洞

Samba
CVE-2017-14746
CVE-2017-15275



SMB弱點
RDP 弱點

弱點已無處不在

目標類型	常見系統
作業系統	Windows, Linux, Mac, Solaris, BSD, UNIX...
虛擬化系統	VMware, Hyper-V, Xen, KVM, OpenStack...
應用程式軟體	Office, LibreOffice, PDF, Wordpress, and more...
應用服務元件	Apache, Tomcat, SSL, RDP, and more...
資料庫	Oracle, MS SQL, MySQL, PostgreSQL, MongoDB...
網路裝置	Router, Switch, Printer, NAS, VPN, WiFi, and more...
資安系統	Firewall, IPS, UTM, AV, Spam, DDoS, APT, and more...
其他科技	Cloud, Git, Container, and unknown...

當漏洞發生在資安位置上



Cisco表示，Cisco Registered Envelope Service (CRES) 及網路會議服務Webex Messenger Service已首先獲得修復，且其代管服務皆未受到影響。目前還在調查中的產品包括Cisco IOS、安全產品Identity Service Engine、Secure Access Control Server、Cloud Web Security、Catalyst 6500 Series 及7600 Series Firewall Services等，而Cisco也會持續更新評估狀況，一旦有修補程式也會立即發佈通知。

另一家網路設備大廠Juniper也發佈安全公告，列出受HeartBleed漏洞威脅的產品，包括作業系統 Junos OS 13.3R1、安全存取的用戶端軟體Odyssey client 5.6r5以上、數個版本的Web存取軟體Network Connect (windows版本) 等，與SSL VPN連網產品Juniper SSL VPN (IVEOS) 7.4r1、SSL VPN (IVEOS) 8.0r1、以及桌面與行動終端軟體Junos Pulse (Android及iOS版本)等。其中有些已獲得修補。

資安系統的安全必須重視

新聞 思科與Fortinet坦承防火牆漏洞遭「方程式」外流攻擊工具鎖定

駭客組織「影子搭客」釋出宣稱竊自「方程式」的300MB檔案，其中包括針對防火牆的各種攻擊工具，研究人員發現這些工具開發已有3年之久，而且針對防火牆漏洞進行攻擊是有效的，思科及Fortinet已證實某些工具可危害旗下的防火牆產品。

文/ 陳曉莉 | 2016-08-18 發表

讚 5.3萬 按讚加入iThome粉絲團

讚 4 分享

新聞 思科修補VPN產品風險指數10的遠端程式碼執行漏洞

漏洞存在於思科的Adaptive Security Appliance軟體上名為WebVPN的SSL VPN功能，使其啟動時一區記憶體重複釋放。這使得攻擊者可以傳送多個經改進的XML封包到受影響裝置上的webvpn組態介面，進而遠端執行任意程式碼並取得系統完整控制權，或導致受害系統重置。

文/ 林妍濤 | 2018-01-31 發表

讚 5.3萬 按讚加入iThome粉絲團

讚 96 分享

新聞 快修補！思科爆重大遠端程式碼執行漏洞，850萬台交換器拉警報

漏洞存在於IOS及IOS XE的Smart Install中，思科指出漏洞可讓未經驗證的遠端攻擊者驅動裝置重新載入，造成阻斷服務或是任意程式碼執行攻擊。

文/ 林妍濤 | 2018-03-30 發表

讚 5.3萬 按讚加入iThome粉絲團

讚 507 分享

新聞 思科：逾80款路由器、交換器產品受Linux DoS漏洞影響

FragmentStack為一可導致阻斷服務的漏洞，影響Linux核心3.9以上版本，在8月已揭露，思科本週發出安全公告，指旗下88款產品，包括vEdge路由器系列、Nexus交換機系列等均受到影響，將在今年9月到明年2月間陸續修補。

文/ 林妍濤 | 2018-09-27 發表

讚 5.3萬 按讚加入iThome粉絲團

讚 297 分享

Anti DDoS

新聞 趨勢PC-cillin密碼管理驚爆漏洞，防毒軟體恐成PC遭駭幫兇，Google專家直批荒謬

發現此漏洞的谷歌抓蟲大隊Google Project Zero研究員Tavis Ormandy表示，任何惡意網站，可以利用趨勢防毒軟體密碼管理功能的這個漏洞，來執行本地端的任何指令，甚至暗中下令刪除硬碟資料都可以。

文/ 黃彥蓉 | 2016-01-12 發表

讚 5.5萬 按讚加入iThome粉絲團

讚 0 分享

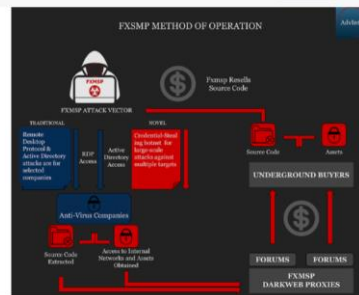
新聞 防毒軟體程式碼驚傳外洩，Symantec、趨勢科技、McAfee遭到點名

自上週傳出3間防毒軟體大廠的程式碼遭到外洩到暗網上，本周這起事件有了新的發現，根據駭客組織與地下買家的對話內容，3家廠商是Symantec、趨勢科技，以及McAfee，而他們也都對此事做出回應。

文/ 周敏怡 | 2019-05-15 發表

讚 6.5萬 按讚加入iThome粉絲團

讚 614 分享



數位政府
Digital Government
高峰會 2019
公務同仁更懂得
強化使用者體驗設計

iThome Security
數位專訊 2019年5月21日

成為朋友中第一個知道這個人

iThome Security
13小時前

新聞 臺灣研究人員攻陷Palo Alto、Fortinet與Pulse Secure等SSL VPN服務漏洞

臺灣資安業者戴夫寇爾 (Devcore) 準備在今年黑帽大會上，展示如何攻陷Palo Alto Networks、Fortinet與Pulse Secure所提供的SSL VPN服務。

文/ 陳曉莉 | 2019-07-24 發表

讚 5.5萬 按讚加入iThome粉絲團

讚 1,276 分享

信任鏈破壞 (Broken Trust Chain)

- 防護: Firewall, IPS, Anti-Virus, Intrusion Security Gate, Endpoint Security, IAM, ... etc.
 - 檢測: APT, Sandbox, Code review, ...etc.
 - 分析: Log Analysis management, SIEM, SOC, ...etc.
 - 合規: PCI-DSS, ISO-27001, HIPAA, ...etc.
 - 探勘: Vulnerability Scan, Penetration Test, ...etc.
- 零信任網路 (Zero Trust)
- 零信任 ≠ 不信任
零信任 = 別倚賴信任



開源軟體(Open Source Software) 安全隱憂

OPEN SOURCE SECURITY ANALYSIS 2016 REPORT

Recent Black Duck On-Demand security audits of 200 commercial applications confirm the importance of open source in application development, and also highlight the persistent challenges organizations face in effectively securing and managing their open source.



Average amount of open source code in each application.

105

Average number of open source components found in each application



67% of applications reviewed contained known open source security vulnerabilities



40% of known open source security vulnerabilities in each application were rated "severe"



On average the companies were using 100% more open source than they originally believed

1,894 DAYS



Average age of known open source security vulnerabilities



22.5

Average number of known open source security vulnerabilities in each application



10% of the applications included the Heartbleed vulnerability

資料來源: Black Duck Software

“開源” 不等於 節流。

新聞 十多個Apache HTTP Server版本含有允許駭客取得最高權限漏洞

從2015年發表的2.4.17到今年2月發表的2.4.38共十多個版本Apache HTTP Server都有安全缺陷，用戶最好儘快升級到4月1日釋出的2.4.39版本

文/ 陳曉莉 | 2019-04-06 發表

讚 5.6 萬 按讚加入iThome粉絲團 讚 1,212 分享



Apache HTTP Server 2.4.39 Released

April 01, 2019

新聞 安全顧問揭露MySQL含有可竊取用戶檔案的設計漏洞

MySQL客戶端有個LOAD DATA敘述，如果在客戶端指定了LOCAL關鍵字，便會允許伺服器端載入客戶端的檔案，MySQL團隊也特別對此在操作手冊中提出了警告

文/ 陳曉莉 | 2019-01-22 發表

讚 5.6 萬 按讚加入iThome粉絲團 讚 274 分享

MySQL 8.0 Reference Manual / ... / Security Issues with LOAD DATA LOCAL

新聞 研究人員再揭PHP反序列化安全漏洞，恐使WordPress曝露遠端程式攻擊風險

2009年曾有研究人員揭露PHP反序列化潛藏的風險，最近英國資安公司Secarma再揭露PHP的反序列化漏洞，成功開採該漏洞，可攻陷WordPress與Typo3內容管理平台，執行遠端程式攻擊。

文/ 陳曉莉 | 2018-08-20 發表

新聞 Drupal修補遠端程式攻擊漏洞

這個被列為嚴重等級的安全漏洞，在某些情況下會允許駭客自遠端執行PHP程式，8.5.x以前的Drupal 8版本無法透過更新進行修補

文/ 陳曉莉 | 2019-02-22 發表

讚 5.6 萬 按讚加入iThome粉絲團 讚 91 分享

Drupal™

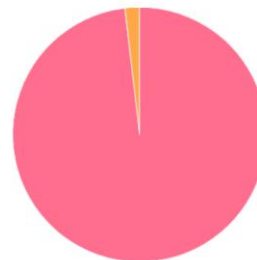
新聞 WordPress網站的安全漏洞有98%來自外掛程式

Imperva調查顯示，儘管WordPress是駭客最常鎖定的內容管理平臺，但全球的WordPress網站漏洞，有高達98%其實是來自於第三方外掛程式

文/ 陳曉莉 | 2019-05-17 發表

讚 5.6 萬 按讚加入iThome粉絲團 讚 512 分享

WordPress third party vendor vulnerabilities in 2018



WordPress Core
Third party

imperva

Imperva的研究顯示，去年發現的WordPress網站漏洞，高達98%源自於外掛程式。

“開源” 不等於 節流 · ·

2019 PHP5網站技術支援到期，恐將成為資安孤兒

PHP 5將在2018年12月31日邁向終點，但是，全球與臺灣企業網站升級速度仍緩慢，企業必須先意識到這樣的風險存在

文/ 羅正漢 | 2018-12-04 發表

讚 5.5 萬 按讚加入iThome粉絲團

讚 1,390 分享

PHP版本終止支援列表

版本	正式版本釋出時間	主要更新支援結束日期	安全更新支援結束日期
5.4	2012年3月1日	2014年9月14日	2015年9月14日 (終止支援)
5.5	2013年6月20日	2015年7月10日	2016年7月10日 (終止支援)
5.6	2014年8月28日	2017年1月19日	2018年12月31日 (剩餘1個月)
7.0	2015年12月3日	2017年12月3日	2018年12月3日 (剩不到1周)
7.1	2016年12月1日	2018年12月1日	2019年12月1日 (剩餘1年)
7.2	2017年11月30日	2019年11月30日	2020年11月30日 (剩餘2年)

資料來源：php.net，iThome整理，2018年11月

“開源” 不等於 節流 . . .

新聞

Git爆任

新聞

Git由於在處理子服務皆已預設拒絕

文/ 李建興 | 2018

新聞

駭客鎖

近期許多開發人員特幣來換回資料

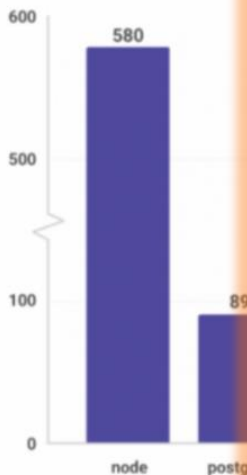
文/ 陳曉莉 | 2019-

報告：前十大熱門Docker映像檔都有至少30個以上的漏洞

Snyk掃描Docker Hub中最多開發者使用的Docker映像檔，發現官方的Node.js映像檔含有580個易受攻擊的系統函式庫

文/ 李建興 | 2019-02-28 發表

Number of OS



#容器安全 #Docker

Docker揭露最新容器漏洞，攻擊者能透過容器將惡意程式植入Linux主機

容器安全是現在最熱門的資安議題之一，Docker公司最近又揭露了一個容器上的TOCTOU (time of check to time of use) 弱點的新漏洞CVE-2018-15664，攻擊者可將任意程式碼植入系統。攻擊者能透過Docker copy指令，來修改容器中的Symbolic links，用內藏惡意程式的偽裝檔案，覆蓋掉原本在Linux主機上的檔案，甚至可以寫入需要root權限的目錄下，進而入侵系統。Docker容器變成了攻擊者的入侵跳板。這個漏洞影響所有的Docker版本，在CVSS 3.0版的風險評分是5.8，屬於中度風險的漏洞。

Web應用服務的安全準則

開發準則

OSSTMM 開源安全測試方法

SSDLC 安全軟體發展生命週期

檢測準則

程式源碼安全

網頁應用安全

系統漏洞安全

防護準則

FW

IPS

WAF

HIDS

DDoS

稽核準則

OWASP - Top 10



The OWASP Top 10 grid includes: Funct Access Control, SQL Injection, Broken Auth / Session, Direct Object Ref, Security Misconfig, Cross Site Request Forgery, Vulnerable Components, Cross Site Scripting, Unvalidated Redirects, and Data Exposure.

新聞

Java、Python安全漏洞可能讓攻擊者繞過防火牆

一位研究者發現，Java和Python的FTP協定注入漏洞恐讓攻擊者突破受害者系統的防火牆防護，而讓來自網際網路上的（惡意）TCP連線，能存取內部主機系統的1024到65535連接埠。

文 / 林妍濤 | 2017-02-23 發表

讚 5.5 萬 | 按讚加入iThome粉絲團 | 讚 0 | 分享



圖片來源: 甲骨文

從資安怎麼看待「弱點(漏洞)」

弱點漏洞

不管嚴重等級是高(High)還是低(Low)

只要可以利用，就是好弱點

如果容易利用，那就是絕佳好弱點

受駭目標不管是高階或低階

只要可以利用，就是好目標！

弱點漏洞是怎麼發生？

- 不當的設計(Bad Design)
 - 例: 作業系統, 應用程式, 元件, 技術...
- 不當的實作(Bad Implementation)
 - 例: 網路規劃, 系統規劃, 存取控制...
- 不當的組態設定(Bad Configuration)
 - 例: 預設密碼, 未依循規範政策...
- 過時的組態設定(Stale Configuration)
 - 例: 沒有修補或更新...
- 被利用的方式
 - 例: Bypass, 加密通訊, 白名單, 社交工程...

資安趨勢部落格 > 漏洞攻擊 > 未來四年之內，零時差漏洞出現的頻率很可能提高到每天一次

未來四年之內，零時差漏洞出現的頻率很可能提高到每天一次

POSTED ON 2017 年 07 月 18 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

Share

零時差漏洞(也就是從未被發現的新漏洞)最近出現的頻率越來越高,更糟的是,這些危險的漏洞經常都是在駭客攻擊事件發生之後,人們才知道漏洞的存在。

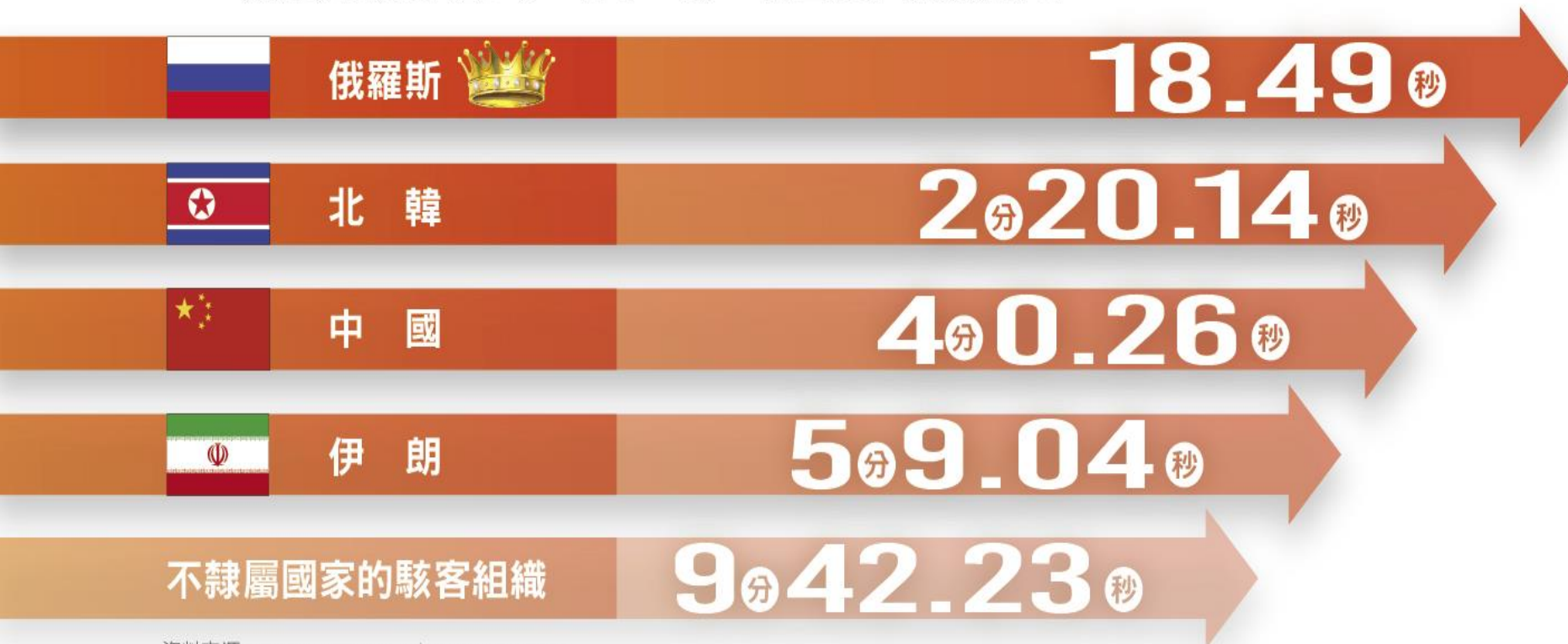
根據網路資安研究機構 Cybersecurity Ventures 創辦人暨總編輯 Steven Morgan 指出,零時差漏洞的出現頻率在未來四年之內很可能提高到每天一次(在 2015 年時大約每週一次)。



從漏洞曝光時，就是開始與駭客競速！

各國駭客實力比一比

——顛覆系統要花多少時間？前4名全是國家級駭客！



資料來源：Breakout Times by Adversary for 2018

<https://www.wealth.com.tw/home/articles/21383>

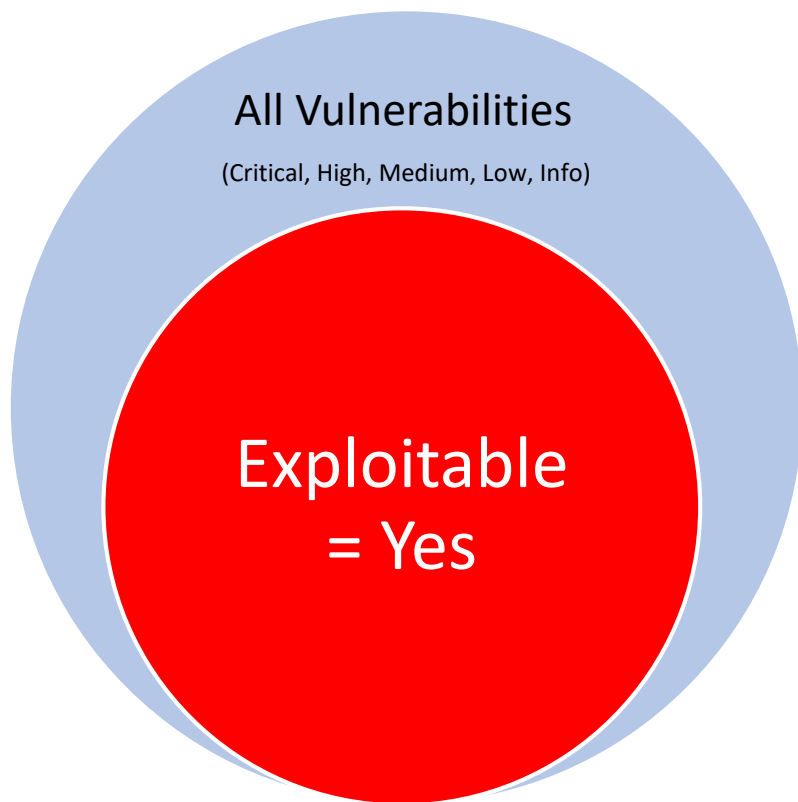
可利用的弱點漏洞 Exploitable

漏洞弱點不一定是絕對&立即威脅，必須搭配適當的條件才能被利用。

具備可利用性 (Exploitable) 代表該弱點漏洞已具可立即使用的攻擊程式碼 並被分享於相關滲透測試與漏洞工具包(Exploit Kits)。



2018年度網路安全報告



最常見的漏洞是嚴重性低,但風險甚高

安全性解決方案公司和忠科合作夥伴 SAINT Corporation 的資深專家表示,低嚴重性漏洞留存多年,是因為公司不知道它們存在,或不認為它們存在重大風險。然而,這些微小安全缺口可能有若重大影響,讓惡意人士有機可乘,能夠入侵系統。

SAINT 研究人員研究 2016 年和 2017 年從 10,000 多台主機收集的漏洞掃描資料。該公司制定研究中所有組織最常偵測到的熱門漏洞列表,其表明最常發生低嚴重性漏洞(請參閱圖 39)。(請注意:研究中包含的一些組織有多個主機。)

圖 39 最常偵測到的低嚴重性漏洞,2016 年至 2017 年



來源: SAINT Corporation

判讀報告是門學問

財務報告

醫療檢查報告

中華民國證券櫃檯買賣中心
 全國商業總會
 民國 107 年 5 月 22 日 星期三 中華民國 107 年 5 月 22 日

單位：新台幣千元

代 碼	名 稱	107 年 5 月 21 日		106 年 12 月 31 日		106 年 9 月 30 日	
		金 額	占 比	金 額	占 比	金 額	占 比
1101	現金及約當現金 (附註六)	\$ 877,702,555	28	\$ 533,371,056	28	\$ 554,725,261	29
1111	透過損益按公允價值衡量之金融資產 (附註六)	902,912	-	546,721	-	5,074,865	-
1118	透過其他綜合損益按公允價值衡量之金融資產 (附註六)	82,713,444	4	-	-	-	-
1129	採用成本法衡量之金融資產 (附註六)	-	-	98,574,185	5	73,082,797	4
1138	採用權益法之金融資產 (附註六)	-	-	3,988,265	-	14,146,374	1
1154	短期金融負債 (附註十三)	9,888,742	1	-	-	-	-
1155	短期金融資產 (附註十三)	-	-	34,364	-	-	-
1159	應收之金融資產 (附註十三)	56,852	-	-	-	-	-
1178	應付短期票據 (附註十三)	16,649,575	1	121,120,345	6	108,202,829	6
1188	應付短期存款 (附註十三)	1,375,523	-	1,184,124	-	484,259	-
1210	其他應收帳項 (附註十三)	328,078	-	171,825	-	132,451	-
514	存貨 (附註十五)	85,315,839	4	73,980,747	4	56,949,402	3
515	其他流動資產 (附註十五)	11,607,544	1	7,265,116	-	5,791,488	-
525	非流動資產 (附註十五)	39,652,521	2	4,277,483	-	3,375,338	-
110X	金融資產合計	973,114,666	40	897,285,533	42	928,161,823	42
1207	透過損益按公允價值衡量之金融負債 (附註六)	8,028,944	-	-	-	-	-
1207	應付短期金融負債 (附註十三)	-	-	30,803,529	1	30,499,458	1
1209	應付短期存款 (附註十三)	13,020,241	1	-	-	-	-
1245	應付長期金融負債 (附註十三)	-	-	4,874,252	-	4,874,252	-
1250	應付長期金融負債 (附註十三)	18,287,027	1	27,861,488	1	29,843,022	1
1800	不動產、廠房及設備 (附註十七)	1,078,546,287	51	1,262,542,222	65	1,037,264,143	54
1810	無形資產 (附註十八)	13,674,285	1	34,373,148	1	34,273,454	1
1843	遞延所得稅資產 (附註十九)	12,987,942	1	32,305,643	1	30,444,491	-
1819	存貨 (附註十五)	2,121,289	-	1,503,414	-	872,006	-
1898	其他非流動資產 (附註十九)	1,522,211	-	2,683,428	-	1,824,321	-
189X	非流動資產合計	1,178,092,140	50	1,326,698,655	67	1,109,655,158	57
200X	資產總計	\$2,051,156,826	100	\$1,893,884,163	100	\$1,936,816,981	100
210	資本公積金	-	-	-	-	-	-
220	盈餘公積金	-	-	-	-	-	-
230	未分配盈餘	-	-	-	-	-	-
240	其他權益	-	-	-	-	-	-
250	負債合計	\$1,140,662,159	56	\$1,140,662,159	60	\$1,140,662,159	59
260	權益合計	\$910,494,667	44	\$753,222,004	40	\$796,154,822	41

癌症標檢 Tumor Markers

人類絨毛激素【男】β-HCG <1.2 uIU/ml <G

放射線檢查 Radiology Examination

胸部正面X光 Chest X-ray 無異狀

腰椎骨質密度檢查之平均骨密度 BMD 0.88 (g/cm²)

腰椎骨質密度檢查之骨密度百分比 BMD 87 (%)

腰椎骨質密度檢查之T-score T-score: -1.1 >=-1.0

右髌骨骨質密度檢查之平均骨密度 BMD 0.85 (g/cm²)

右髌骨骨質密度檢查之骨密度百分比 BMD 91 (%)

右髌骨骨質密度檢查之T-score T-score: -0.6 >=-1.0

靜態心臟圖檢 ECG 正常(心跳次數: 70次/分)

十二導程心臟圖檢查 12-lead ECG 正常(心跳次數: 70次/分)

腹部超音波 Abdominal Ultrasound

腹部超音波(肝臟) Liver 物及脂肪肝; 肝臟數規實體, 大小小於2公分

腹部超音波(膽囊) Gallbladder 無異狀

檢查項目	正常參考值	5/24	5/25	5/26	5/29	第二次入院	6/24	
WBC	4~10 10 ⁹ /μL	11.8		17.1	11.6			7.5
RBC	4.5~5.9 10 ¹² /μL	4.41		3.88	3.53			4.09
Platelet	150~440 10 ⁹ /μL	467		397	359			296
Hgb	14~18 g/dL	14.2		12.2	11.2			13.1
BUN	7~20 mg/dL	16			19			12
Creatine	0.7~1.5 mg/dL	1.2			1.1			1.13
CK	≤171 U/L	1526	4550	3080				
CK-MB	≤16.0 U/L	207	490	197				
C.R.P	≤3.0 mg/L	11.5		97.3	154.9			
Cholesterol	≤200 mg/dL	204						
TG	≤150 mg/dL	301						
HDL-C	≥40 mg/dL	39						
LDL-C	≤130 mg/dL	122						
PT	8~12 sec	9.5	10.0			10		
APTT	23.9~34.9	27.5	32.0	37.4		28.5		

備註：紅色字體代表檢查數值異常

天呀... 弱掃報告又來了.

- 文字語言問題
- 字義解讀問題
- 專業知識
- 處理經驗
- 急於尋求答案

看懂弱掃報告的準備工作

- 弱掃的目的

- 系統弱掃 (系統漏洞, 應用程式漏洞, 服務漏洞, 密碼猜測, 組態設定 等)
- 網站弱掃 (系統弱掃, 網頁應用弱掃, 源碼檢測 等)

- 弱掃工具與方法

- 常見系統弱掃工具: Tenable/Nessus, Nmap/Zenmap, OpenVAS 等
- 掃描方式: 網路掃描 或 授權(深層)掃描.

- 必須認識的關鍵字

- CVE (弱點編號)
- CVSS (弱點風險評分)
- Severity (風險等級)
- Exploit Available (弱點可利用)
- Solution (修補解決方案建議)

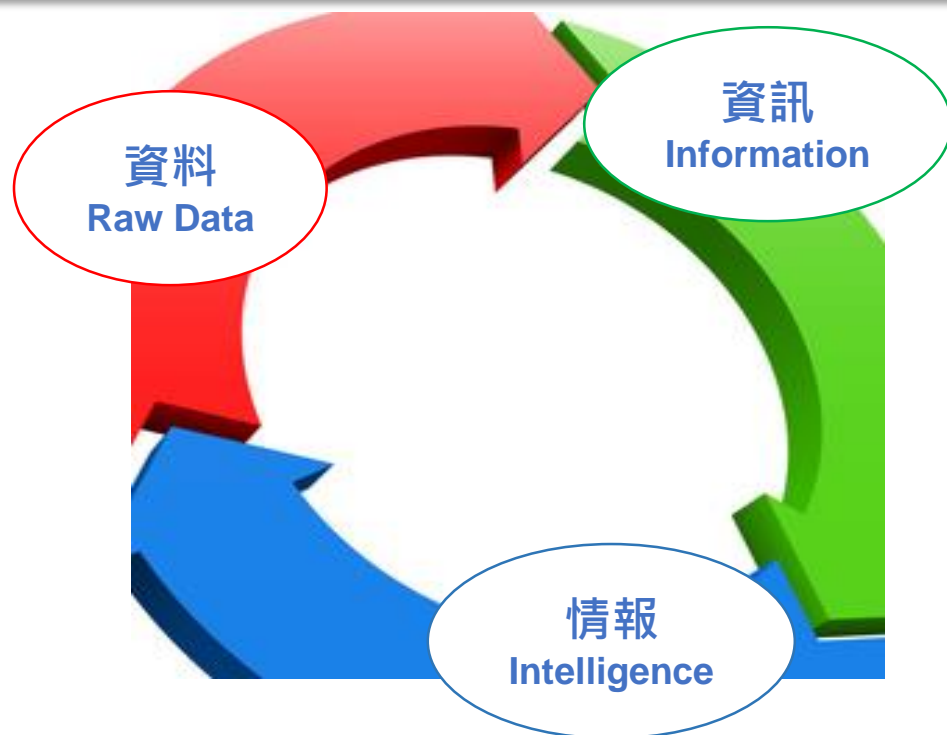
建立方便看懂的弱掃報告

● 定義報告結構化

- 目標資產資訊
- 掃瞄執行時間
- 整體狀態彙總
- 建立索引並階層排序
- 別吝於拆分報告內容

● 相關資源的幫助

- 翻譯工具, 例: Google Chrome 網頁翻譯外掛功能
- 搜尋工具, 例: Google Search
- 弱點相關資訊網站, 例: [CVE Details](#), [Vuldb](#), [Exploit-db](#), [Tenable](#) 等
- 資安訊息相關網站, 例: [iThome security](#), [TW-CERT](#), [TACERT](#) 等



CVE (通用弱點披露)

- CVE 為全球主要的弱點資料維護組織，收集各種資安弱點並給予編號以便於公眾查閱。
- CVE 現由美國非營利組織MITRE所屬的National Cybersecurity FFRDC所營運維護。
- 每一個經CVE確認的弱點披露都會賦予一個專屬的編號(格式：CVE-YYYY-NNNN)。
- CVE 弱點資訊為現今全球所公認的弱點參考標準。

The screenshot shows the CVE website interface. At the top, there is a navigation bar with links for 'CVE List', 'CNAs', 'Board', 'About', and 'News & Blog'. On the right, there is a logo for 'NVD' (National Vulnerability Database) with the text 'Go to for: CVE Lists CVE IDs Adversary Search'. Below the navigation bar is a search bar with buttons for 'Search CVE List', 'Download CVE', 'Data Feeds', 'Request CVE IDs', and 'Update a CVE Entry'. A counter indicates 'TOTAL CVE Entries: 105419'. The main content area includes a paragraph explaining that CVE is a list of entries with identification numbers, descriptions, and public references for publicly known cybersecurity vulnerabilities. It also states that CVE entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD). Below this are three main sections: 'CNA Participation Growing Worldwide' with a world map, 'Latest CVE News' with a list of recent news items, and 'Newest CVE Entries' with a list of tweets from @CVEEncs.

<https://cve.mitre.org/>

CVE 的注意事項



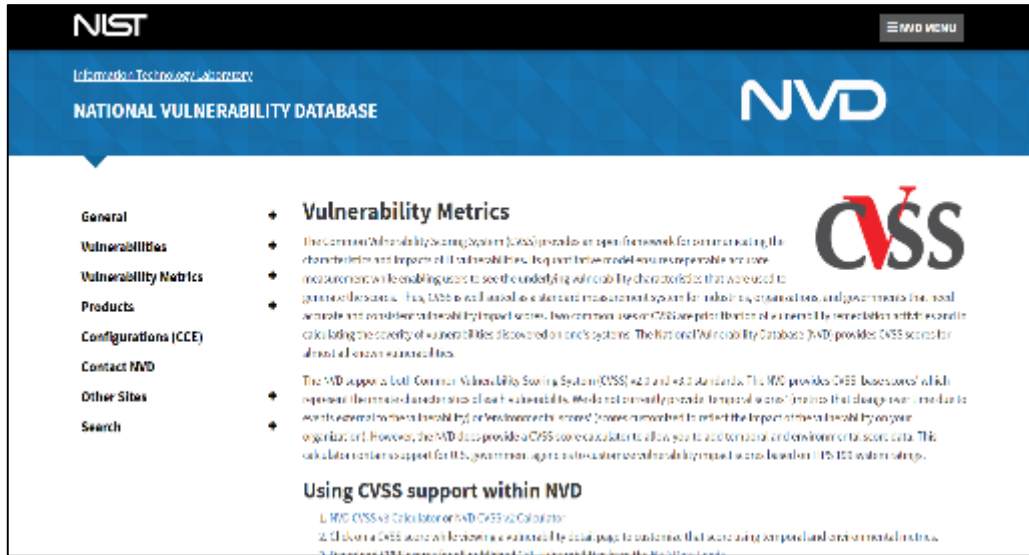
TIP!

- CVE不是唯一的弱點資料來源! (其他組織或製造商公佈, 例: 微軟MS)
- 多數的弱掃工具 是依據CVE公佈弱點資訊, 建立掃描檢測方式, 但各家的方法不盡相同.
- 掃描發現的弱點不一定具有CVE編號! (可能已發現存在攻擊威脅但尚未完成驗證階段, 亦可視為「未知威脅Unknow Threat」).
- 發現的弱點並須經過CVE組織確認驗證程序後, 才會給予CVE編號.
- 零日漏洞(Zero-day exploit 或 0-Day) 通常指「還沒有修補程式方法的漏洞」.
- 同一弱點威脅可能具備有多個CVE, 需視修補建議方式評估達成.

SMB弱點

CVE-ID
CVE-2017-0144 Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.
References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

CVSS (通用弱點評分系統)



- CVSS 由美國國家基礎建設諮詢委員會 (NIAC) 委託製作。
- 為目前全球主要的弱點評分標準。
- CVSS的評分標準包含多種項目所訂出弱點的危險分數。
- CVSS 評分從0分到10分, 0代表沒有發現弱點, 而10則代表最高風險。

NVD Vulnerability Severity Ratings

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
Low	0.0-3.9	None	0.0
Medium	4.0-6.9	Low	0.1-3.9
High	7.0-10.0	Medium	4.0-6.9
		High	7.0-8.9
		Critical	9.0-10.0

- CVSS v3為最新的評分方式, 將弱點風險分成五個等級。
- 弱掃工具將CVSS所公布各個弱點的風險等級作為預設標準, 但使用者可依實際環境調整*。

Exploit-DB (可利用弱點資料庫)

- Exploit-db 為全球主要的可利用弱點資料庫，由知名資安訓練組織Offensive Security維護。
- 收集來自全球白帽提交的各類漏洞訊息及利用代碼。
- 資料類型包括4大類: Remote Exploits, Web Application Exploits, Local & Privilege Escalation Exploits, Denial of Service & PoC Exploits.

The screenshot displays the Exploit-DB website interface. The main heading is "Web Application Exploits" with a sub-note: "This exploit category includes exploits for web applications." Below this, it indicates "23,077 total entries" and provides pagination controls. A table lists various exploits with columns for Date, D (Download), A (Author), V (Verified), Title, Platform, and Author. Three red arrows point from the table to yellow callout boxes:

- An arrow from the 'D' column points to a box labeled "Verification".
- An arrow from the 'A' column points to a box labeled "Download Vulnerable Application".
- An arrow from the 'V' column points to a box labeled "Download Exploit Code".

Date	D	A	V	Title	Platform	Author
2018-08-02	✓	-	✓	ASUS DSL-N12E C1 1.1.2.3_345 - Remote Command Execution	Hardware	Fakhri Zulkifli
2018-08-02	✓	-	✓	Universal Media Server 7.1.0 - SSDP Processing XML External Entity Injection	XML	Chris Moberly
2018-08-02	✓	-	✓	CoSoc's Endpoint Protector 4.5.0.1 - Authentication	PHP	0x09AL
2018-08-02	✓	-	✓	ParseResponse FB Inboxer Add-on 1.2 - 'search_field'	PHP	AkkuS
2018-08-02	✓	-	✓	TI Online Examination System v2 - Arbitrary File Download
2018-08-02	✓	✓	✓	WityCMS 0.6.2 - Cross-Site Request Forgery (Password Reset)
2018-08-02	✓	-	✓	Chartered Accountant - Auditor Website 2.0.1 - Cross-Site Request Forgery
2018-07-30	✓	✓	✓	H2 Database 1.4.19 - Information Disclosure	...	owodella

<https://www.exploit-db.com/>

值得關注的可利用弱點 (Exploitable)



可被利用的弱點，威脅度大於高風險弱點！

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群 搜尋

比WannaCry更狠！新網路蠕蟲EternalRocks現身，駭客利用7種NSA駭客工具攻擊Windows電腦

研究人員發現，除了勒索蠕蟲WannaCry之外，5月初發現新網路蠕蟲EternalRocks，同樣鎖定SMB漏洞來發動攻擊，但是，其他攻擊者也可以植入其他惡意軟體到遭受EternalRocks感染的電腦

WannaCry所使用的EternalBlue和DoublePulsar兩種駭客工具之外，還使用了其他NSA開發的5種駭客工具，包括EternalChampion、EternalRomance、EternalSynergy、ArchiTouch和SMBTouch等。

這7種駭客工具具有3個不同的用途，第一、EternalBlue、EternalChampion、EternalRomance和EternalSynergy專門攻擊SMB漏洞。第二、ArchiTouch和SMBTouch則是偵測目標電腦是否存在SMB漏洞。第三、駭客利用DoublePulsar傳播蠕蟲到其他存有SMB漏洞的Windows電腦。

根據Bleeping Computer表示，EternalRocks可能會繞過電腦防毒軟體的偵測，造成受害者不易察覺遭入侵。而且，它沒有設置kill switch的功能，快速在網路上掃描易遭攻擊的電腦IP，隨機發動攻擊。不僅如此，駭客能夠利用EternalRocks和其他惡意程式結合，如勒索軟體、銀行木馬、RATs和其他攻擊程式。

Exploit-db公佈可利用code及方法

Date	D	Title
2017-08-01	🇮🇱	[Hebrew] Digital Whisper Security Magazine #85
2017-08-01	🇮🇱	[Hebrew] Digital Whisper Security Magazine #84
2017-07-16	🇺🇸	How to exploit ETERNALROMANCE/SYNERGY on Windows Server 2016
2017-07-12	🇺🇸	Hidden Network: Detecting Hidden Networks created with USB Devices
2017-07-03	🇫🇷	[French] SYN FLOOD ATTACK for IP CISCO Phone
2017-06-29	🇺🇸	How to Exploit ETERNALBLUE on Windows Server 2012 R2
2017-06-29	🇪🇸	[Spanish] How to Exploit ETERNALBLUE on Windows Server 2012 R2
2017-06-28	🇮🇷	[Persian] Xpath Injection
2017-06-26	🇺🇸	How to Write Fully Undetectable Malware - English Translation
2017-06-21	🇺🇸	Blind SQL Injection Attacks
2017-06-19	🇮🇹	[Italian] How to write Fully Undetectable malware
2017-06-15	🇺🇸	Web Application Penetration Testing Techniques

弱點資訊參考資源

CVE Details
The ultimate security vulnerability database

Enter a CVE id, product, vendor, vulnerability type...

Current CVSS Score Distribution For All Vulnerabilities

CVSS Score	Number of Vulnerabilities	Percentage
0.0	422	3.03
1.0	812	5.89
2.0	2425	17.62
3.0	2271	16.61
4.0	17915	130.00
5.0	13372	97.36
6.0	12567	92.16
7.0	22129	162.84
8.0	22	0.16
9.0	1232	9.06
10.0	2622	19.19
Average	2622	19.19

CVSS Score Legend: 0.0 (Green), 1.0 (Light Green), 2.0 (Yellow), 3.0 (Orange), 4.0 (Light Orange), 5.0 (Yellow), 6.0 (Light Green), 7.0 (Green), 8.0 (Light Blue), 9.0 (Blue), 10.0 (Dark Blue)

<https://www.cvedetails.com/>

VulDB

CVSS Current Top 5

1. CVE-2019-11464 (Microsoft Exchange Server) - 9.8
2. CVE-2019-11463 (Microsoft Exchange Server) - 9.8
3. CVE-2019-11462 (Microsoft Exchange Server) - 9.8
4. CVE-2019-11461 (Microsoft Exchange Server) - 9.8
5. CVE-2019-11460 (Microsoft Exchange Server) - 9.8

Exploit Price Current Top 5

1. CVE-2019-11464 (Microsoft Exchange Server) - \$1000
2. CVE-2019-11463 (Microsoft Exchange Server) - \$1000
3. CVE-2019-11462 (Microsoft Exchange Server) - \$1000
4. CVE-2019-11461 (Microsoft Exchange Server) - \$1000
5. CVE-2019-11460 (Microsoft Exchange Server) - \$1000

<https://vuldb.com/>

tenable | Spot, Connect, Discover, Assess, Remediate

Newest Plugins

ID	Name	Product	Family	Severity
E1024	Windows 10/11/8/7/XP/2008/2003/2000/Server/2008 R2/2008 R2 SP1/2008 R2 SP2/2008 R2 SP3/2008 R2 SP4/2008 R2 SP5/2008 R2 SP6/2008 R2 SP7/2008 R2 SP8/2008 R2 SP9/2008 R2 SP10/2008 R2 SP11/2008 R2 SP12/2008 R2 SP13/2008 R2 SP14/2008 R2 SP15/2008 R2 SP16/2008 R2 SP17/2008 R2 SP18/2008 R2 SP19/2008 R2 SP20/2008 R2 SP21/2008 R2 SP22/2008 R2 SP23/2008 R2 SP24/2008 R2 SP25/2008 R2 SP26/2008 R2 SP27/2008 R2 SP28/2008 R2 SP29/2008 R2 SP30/2008 R2 SP31/2008 R2 SP32/2008 R2 SP33/2008 R2 SP34/2008 R2 SP35/2008 R2 SP36/2008 R2 SP37/2008 R2 SP38/2008 R2 SP39/2008 R2 SP40/2008 R2 SP41/2008 R2 SP42/2008 R2 SP43/2008 R2 SP44/2008 R2 SP45/2008 R2 SP46/2008 R2 SP47/2008 R2 SP48/2008 R2 SP49/2008 R2 SP50/2008 R2 SP51/2008 R2 SP52/2008 R2 SP53/2008 R2 SP54/2008 R2 SP55/2008 R2 SP56/2008 R2 SP57/2008 R2 SP58/2008 R2 SP59/2008 R2 SP60/2008 R2 SP61/2008 R2 SP62/2008 R2 SP63/2008 R2 SP64/2008 R2 SP65/2008 R2 SP66/2008 R2 SP67/2008 R2 SP68/2008 R2 SP69/2008 R2 SP70/2008 R2 SP71/2008 R2 SP72/2008 R2 SP73/2008 R2 SP74/2008 R2 SP75/2008 R2 SP76/2008 R2 SP77/2008 R2 SP78/2008 R2 SP79/2008 R2 SP80/2008 R2 SP81/2008 R2 SP82/2008 R2 SP83/2008 R2 SP84/2008 R2 SP85/2008 R2 SP86/2008 R2 SP87/2008 R2 SP88/2008 R2 SP89/2008 R2 SP90/2008 R2 SP91/2008 R2 SP92/2008 R2 SP93/2008 R2 SP94/2008 R2 SP95/2008 R2 SP96/2008 R2 SP97/2008 R2 SP98/2008 R2 SP99/2008 R2 SP100	Windows	Windows	CRITICAL
E1025	Windows 10/11/8/7/XP/2008/2003/2000/Server/2008 R2/2008 R2 SP1/2008 R2 SP2/2008 R2 SP3/2008 R2 SP4/2008 R2 SP5/2008 R2 SP6/2008 R2 SP7/2008 R2 SP8/2008 R2 SP9/2008 R2 SP10/2008 R2 SP11/2008 R2 SP12/2008 R2 SP13/2008 R2 SP14/2008 R2 SP15/2008 R2 SP16/2008 R2 SP17/2008 R2 SP18/2008 R2 SP19/2008 R2 SP20/2008 R2 SP21/2008 R2 SP22/2008 R2 SP23/2008 R2 SP24/2008 R2 SP25/2008 R2 SP26/2008 R2 SP27/2008 R2 SP28/2008 R2 SP29/2008 R2 SP30/2008 R2 SP31/2008 R2 SP32/2008 R2 SP33/2008 R2 SP34/2008 R2 SP35/2008 R2 SP36/2008 R2 SP37/2008 R2 SP38/2008 R2 SP39/2008 R2 SP40/2008 R2 SP41/2008 R2 SP42/2008 R2 SP43/2008 R2 SP44/2008 R2 SP45/2008 R2 SP46/2008 R2 SP47/2008 R2 SP48/2008 R2 SP49/2008 R2 SP50/2008 R2 SP51/2008 R2 SP52/2008 R2 SP53/2008 R2 SP54/2008 R2 SP55/2008 R2 SP56/2008 R2 SP57/2008 R2 SP58/2008 R2 SP59/2008 R2 SP60/2008 R2 SP61/2008 R2 SP62/2008 R2 SP63/2008 R2 SP64/2008 R2 SP65/2008 R2 SP66/2008 R2 SP67/2008 R2 SP68/2008 R2 SP69/2008 R2 SP70/2008 R2 SP71/2008 R2 SP72/2008 R2 SP73/2008 R2 SP74/2008 R2 SP75/2008 R2 SP76/2008 R2 SP77/2008 R2 SP78/2008 R2 SP79/2008 R2 SP80/2008 R2 SP81/2008 R2 SP82/2008 R2 SP83/2008 R2 SP84/2008 R2 SP85/2008 R2 SP86/2008 R2 SP87/2008 R2 SP88/2008 R2 SP89/2008 R2 SP90/2008 R2 SP91/2008 R2 SP92/2008 R2 SP93/2008 R2 SP94/2008 R2 SP95/2008 R2 SP96/2008 R2 SP97/2008 R2 SP98/2008 R2 SP99/2008 R2 SP100	Windows	Windows	CRITICAL
E1026	Windows 10/11/8/7/XP/2008/2003/2000/Server/2008 R2/2008 R2 SP1/2008 R2 SP2/2008 R2 SP3/2008 R2 SP4/2008 R2 SP5/2008 R2 SP6/2008 R2 SP7/2008 R2 SP8/2008 R2 SP9/2008 R2 SP10/2008 R2 SP11/2008 R2 SP12/2008 R2 SP13/2008 R2 SP14/2008 R2 SP15/2008 R2 SP16/2008 R2 SP17/2008 R2 SP18/2008 R2 SP19/2008 R2 SP20/2008 R2 SP21/2008 R2 SP22/2008 R2 SP23/2008 R2 SP24/2008 R2 SP25/2008 R2 SP26/2008 R2 SP27/2008 R2 SP28/2008 R2 SP29/2008 R2 SP30/2008 R2 SP31/2008 R2 SP32/2008 R2 SP33/2008 R2 SP34/2008 R2 SP35/2008 R2 SP36/2008 R2 SP37/2008 R2 SP38/2008 R2 SP39/2008 R2 SP40/2008 R2 SP41/2008 R2 SP42/2008 R2 SP43/2008 R2 SP44/2008 R2 SP45/2008 R2 SP46/2008 R2 SP47/2008 R2 SP48/2008 R2 SP49/2008 R2 SP50/2008 R2 SP51/2008 R2 SP52/2008 R2 SP53/2008 R2 SP54/2008 R2 SP55/2008 R2 SP56/2008 R2 SP57/2008 R2 SP58/2008 R2 SP59/2008 R2 SP60/2008 R2 SP61/2008 R2 SP62/2008 R2 SP63/2008 R2 SP64/2008 R2 SP65/2008 R2 SP66/2008 R2 SP67/2008 R2 SP68/2008 R2 SP69/2008 R2 SP70/2008 R2 SP71/2008 R2 SP72/2008 R2 SP73/2008 R2 SP74/2008 R2 SP75/2008 R2 SP76/2008 R2 SP77/2008 R2 SP78/2008 R2 SP79/2008 R2 SP80/2008 R2 SP81/2008 R2 SP82/2008 R2 SP83/2008 R2 SP84/2008 R2 SP85/2008 R2 SP86/2008 R2 SP87/2008 R2 SP88/2008 R2 SP89/2008 R2 SP90/2008 R2 SP91/2008 R2 SP92/2008 R2 SP93/2008 R2 SP94/2008 R2 SP95/2008 R2 SP96/2008 R2 SP97/2008 R2 SP98/2008 R2 SP99/2008 R2 SP100	Windows	Windows	CRITICAL
E1027	Windows 10/11/8/7/XP/2008/2003/2000/Server/2008 R2/2008 R2 SP1/2008 R2 SP2/2008 R2 SP3/2008 R2 SP4/2008 R2 SP5/2008 R2 SP6/2008 R2 SP7/2008 R2 SP8/2008 R2 SP9/2008 R2 SP10/2008 R2 SP11/2008 R2 SP12/2008 R2 SP13/2008 R2 SP14/2008 R2 SP15/2008 R2 SP16/2008 R2 SP17/2008 R2 SP18/2008 R2 SP19/2008 R2 SP20/2008 R2 SP21/2008 R2 SP22/2008 R2 SP23/2008 R2 SP24/2008 R2 SP25/2008 R2 SP26/2008 R2 SP27/2008 R2 SP28/2008 R2 SP29/2008 R2 SP30/2008 R2 SP31/2008 R2 SP32/2008 R2 SP33/2008 R2 SP34/2008 R2 SP35/2008 R2 SP36/2008 R2 SP37/2008 R2 SP38/2008 R2 SP39/2008 R2 SP40/2008 R2 SP41/2008 R2 SP42/2008 R2 SP43/2008 R2 SP44/2008 R2 SP45/2008 R2 SP46/2008 R2 SP47/2008 R2 SP48/2008 R2 SP49/2008 R2 SP50/2008 R2 SP51/2008 R2 SP52/2008 R2 SP53/2008 R2 SP54/2008 R2 SP55/2008 R2 SP56/2008 R2 SP57/2008 R2 SP58/2008 R2 SP59/2008 R2 SP60/2008 R2 SP61/2008 R2 SP62/2008 R2 SP63/2008 R2 SP64/2008 R2 SP65/2008 R2 SP66/2008 R2 SP67/2008 R2 SP68/2008 R2 SP69/2008 R2 SP70/2008 R2 SP71/2008 R2 SP72/2008 R2 SP73/2008 R2 SP74/2008 R2 SP75/2008 R2 SP76/2008 R2 SP77/2008 R2 SP78/2008 R2 SP79/2008 R2 SP80/2008 R2 SP81/2008 R2 SP82/2008 R2 SP83/2008 R2 SP84/2008 R2 SP85/2008 R2 SP86/2008 R2 SP87/2008 R2 SP88/2008 R2 SP89/2008 R2 SP90/2008 R2 SP91/2008 R2 SP92/2008 R2 SP93/2008 R2 SP94/2008 R2 SP95/2008 R2 SP96/2008 R2 SP97/2008 R2 SP98/2008 R2 SP99/2008 R2 SP100	Windows	Windows	CRITICAL

<https://www.tenable.com/plugins>

twcert

日期	標題	廠商	標題
2019-07-23	Microsoft Exchange Server (CVE-2019-11464)	Microsoft	Exchange Server (CVE-2019-11464)
2019-07-23	Microsoft Exchange Server (CVE-2019-11463)	Microsoft	Exchange Server (CVE-2019-11463)
2019-07-23	Microsoft Exchange Server (CVE-2019-11462)	Microsoft	Exchange Server (CVE-2019-11462)
2019-07-23	Microsoft Exchange Server (CVE-2019-11461)	Microsoft	Exchange Server (CVE-2019-11461)
2019-07-23	Microsoft Exchange Server (CVE-2019-11460)	Microsoft	Exchange Server (CVE-2019-11460)

漏洞公告

日期	標題	廠商	標題
2019-07-23	Microsoft Exchange Server (CVE-2019-11464)	Microsoft	Exchange Server (CVE-2019-11464)
2019-07-23	Microsoft Exchange Server (CVE-2019-11463)	Microsoft	Exchange Server (CVE-2019-11463)
2019-07-23	Microsoft Exchange Server (CVE-2019-11462)	Microsoft	Exchange Server (CVE-2019-11462)
2019-07-23	Microsoft Exchange Server (CVE-2019-11461)	Microsoft	Exchange Server (CVE-2019-11461)
2019-07-23	Microsoft Exchange Server (CVE-2019-11460)	Microsoft	Exchange Server (CVE-2019-11460)

<https://www.twcert.org.tw/Default.aspx>

善用網路資源查找資安資訊

- 國內主要IT資安媒體



- 全球主要的搜尋引擎



善用工具(2) 商業弱掃廠商的資訊資源

The image shows a screenshot of the NIST National Vulnerability Database (NVD) page for CVE-2017-0143. The page is titled "NIST Information Technology Laboratory NATIONAL VULNERABILITY DATABASE NVD". The main heading is "CVE-2017-0143 Detail".

Annotations include:

- A red box around the "See Also" section on the left, containing links to Microsoft security advisories and other resources.
- A red box around the "Reference Information" section at the bottom, listing various identifiers for this vulnerability.
- Red arrows pointing from the "See Also" box to the "Description" section and from the "Reference Information" box to the "Description" section.

See Also

- <https://technet.microsoft.com/library/security/MS17-010>
- <http://www.wisec.org/0101737feb>
- <http://www.wisec.org/01018c79d1>
- <http://www.wisec.org/0101f569cf>
- <https://github.com/stamparm/EternalRocks/>
- <http://www.wisec.org/0101ad6360>

Reference Information

- CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
- BID: 96703, 96704, 96705, 96706, 96707, 96708
- MSRT: W01-010
- MSIDs: 4102210, 4102211, 4102215, 4102216, 4102219, 410221
- 7, 4012606, 4013198, 4013428, 4012998
- WWW: 2017-01-10
- KBID-ID: 01001, 01002

Current Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows 10; Windows 10 Gold, 10H1, and 10H2; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability". This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Source: NIST
Description Last Modified: 03/16/2017

Dependencies: 01002, 01003

QUICK INFO

- CVE Dictionary Entry:** 151-2017-0143
- NVD Published Date:** 01/10/2017
- NVD Last Modified:** 03/16/2017

報告範本(高階)

以階層式摘要表示

Table of Contents

掃描結果摘要

所有主機弱點

10.8.13.186

10.8.13.195

掃描結果摘要 第一階 總覽整體狀態

弱點數量(依風險)

弱點數量(依主機)

IP Address
10.8.13.195
10.8.13.186

所有主機弱點 第二階

10.8.13.186

IP Address: 10.8.13.186

MAC Address: 34-99-71-00-fc:c2

Total: 35

Vulnerabilities: Critical: 0, High: 0, Medium: 3, Low: 0, Info: 32

各級風險弱點數量統計

Severity
Critical
High
Medium
Low
Info

第三階 顯示該主機弱點詳細資訊

嚴重風險等級弱點

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port	Exploit?
5696	Microsoft Office Unsupported Version Detection	Windows	Critical	10.8.13.186	TCP	445	No

Plugin Text:

Plugin Output:
 Installed product : Office 2007
 End of support date : October 10, 2017
 Supported versions : Office 2010 / 2013 / 2016

Synopsis: The remote host contains an unsupported version of Microsoft Office.
Description: According to its version, the installation of Microsoft Office on the remote Windows host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
Solution: Upgrade to a version of Microsoft Office that is currently supported.
See Also: <http://support.microsoft.com/gp/office>

CVE:

高風險等級弱點

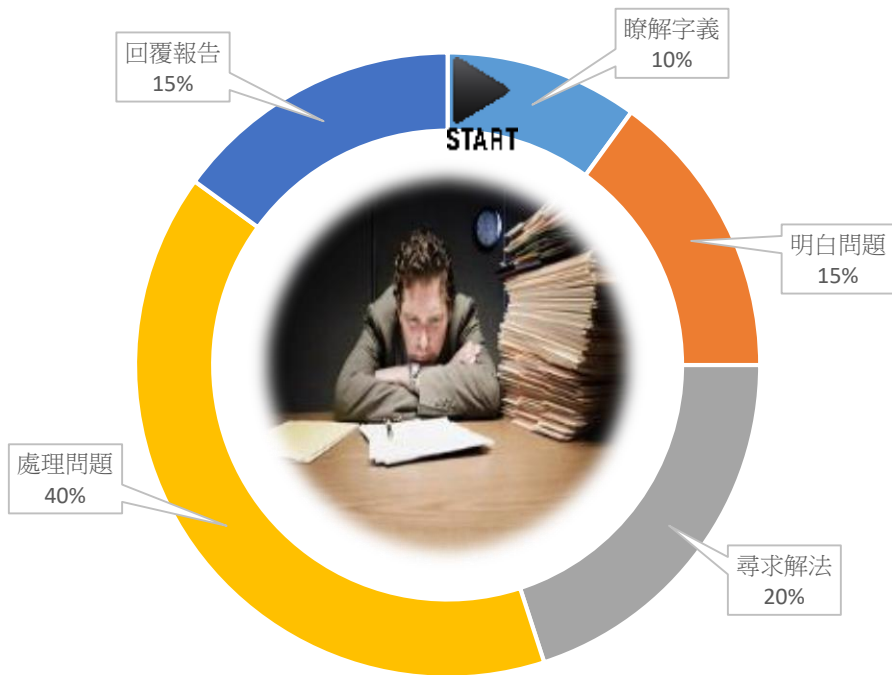
Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port	Exploit?
8725	MS15-124: Cumulative Security Update for Internet Explorer (3116100)	Windows : Microsoft Bulletins	High	10.8.13.186	TCP	445	Yes

Plugin Text:

Plugin Output:
 ASLR hardening settings for Internet Explorer in KB3125869 have not been applied. The following DWORD keys must be created with a value of 1:
 - HKLM\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ALLOW_USERS32_EXCEPTION_HANDLER_HARDENING\iexplore.exe
 - HKLM\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ALLOW_USERS32_EXCEPTION_HANDLER_HARDENING\iexplore.exe

Synopsis: The remote host has a web browser installed that is affected by multiple vulnerabilities.
Description: The version of Internet Explorer installed on the remote host is missing Cumulative Security Update 3116100. It is, therefore, affected by multiple vulnerabilities, the majority of which are remote code execution vulnerabilities. An unauthenticated, remote attacker can exploit these issues by convincing a user to visit a specially crafted website, resulting in the execution of arbitrary code in the context of the current user.
Solution: Microsoft has released a set of patches for Windows Vista, 2006, 7, 2000 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10.
See Also: <https://technet.microsoft.com/library/security/MS15-124>
CVE: CVE-2015-6063, CVE-2015-6134, CVE-2015-6135, CVE-2015-6136, CVE-2015-6138, CVE-2015-6139, CVE-2015-6140, CVE-2015-6141, CVE-2015-6142, CVE-2015-6143, CVE-2015-6144, CVE-2015-6145, CVE-2015-6146, CVE-2015-6147, CVE-2015-6148, CVE-2015-6149, CVE-2015-6150, CVE-2015-6151, CVE-2015-6152, CVE-2015-6153, CVE-2015-6154, CVE-2015-6155, CVE-2015-6156, CVE-2015-6157, CVE-2015-6158, CVE-2015-6159, CVE-2015-6160, CVE-2015-6161, CVE-2015-6162, CVE-2015-6164

弱掃報告 是幫助避免資安風險的基礎



資料

資訊

情報
分析

計畫

處理

減少
弱點曝光
(風險空窗期)

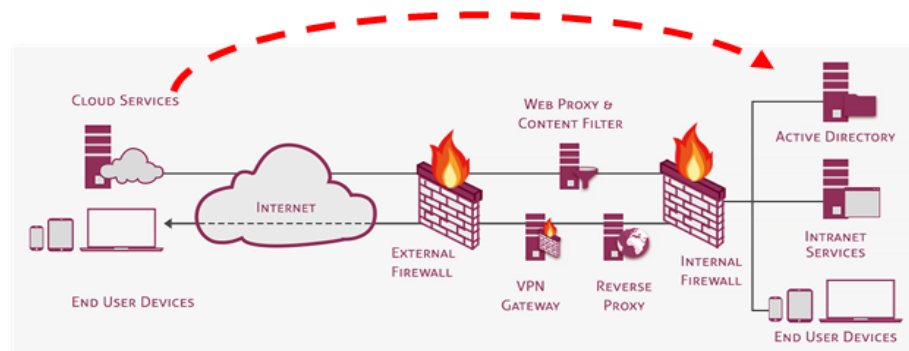
大綱簡介

- 資安威脅大於你可想像的程度
- 資安與駭客的距離 = 漏洞
- 建置聰明效率的資安攻防策略
- 資安法規遵循是提升資安體質的王道
- 結論 | Q&A

Are You O.K? 傳統資安攻防策略

- 外部攻擊者利用社交工程攻擊成功後

- 利用作業系統或應用程式的漏洞，以零時差漏洞攻擊取得系統權限
- 試圖獲取內部人員的身分帳號資訊，尤其是高權限的身分(帳號密碼)
- 而這些，**防毒軟體**大多是看不到的...



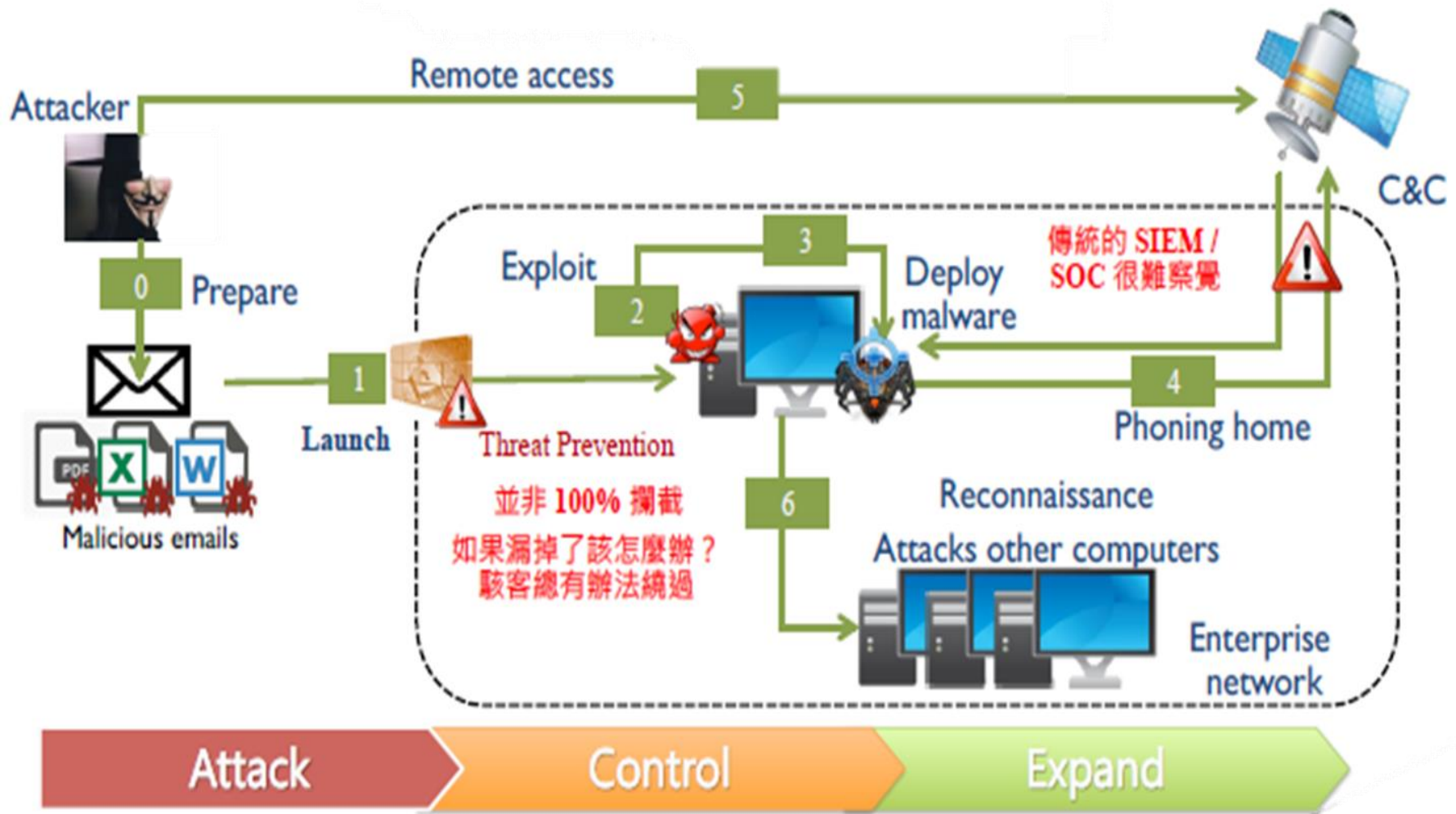
甚至: 防火牆, 入侵防禦, 防毒閘道...

"You can't secure what you can't see" “看不見，就擋不住”

- Dark Reading, 10 Security Best Practices, Nimmy Reichenberg,

但，要全部看到，需要花費多高的人力成本？

以進階持續威脅(APT)攻擊為例



不同世代的資安威脅趨勢

Gen I



病毒

1980'後期 -
PC攻擊 - 單點破壞

防毒軟體

Gen II



網路

1990'中期 -
外部網路攻擊

防火牆

Gen III



應用程式

2000s -
應用程式漏洞與系統弱點

入侵偵測系統(IPS)

Gen IV



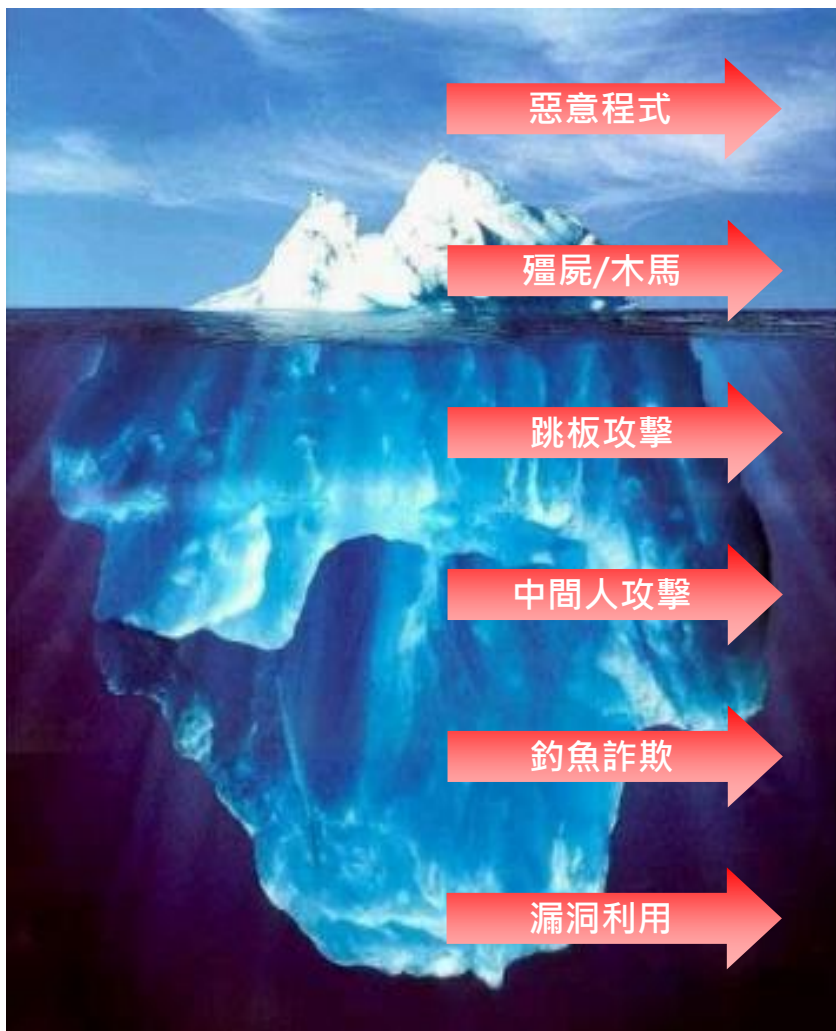
內容負載

2010 -
多元型態惡意內容

沙箱檢測與殭屍防護

資料來源: Check Point

資安威脅的成因



惡意程式

殭屍/木馬

跳板攻擊

中間人攻擊

釣魚詐欺

漏洞利用

已知的攻擊威脅
(Known Knowns)

已知的未知威脅
(Known Unknowns)

未知的攻擊威脅
(Unknown Unknowns)

存在的漏洞
(未公布/未發現/未修補)

未知的資產
(IP/裝置/服務/帳號/權限)

錯誤的設定配置
(版本/組態/架構/結構)

人為的疏失
(操作/保管/授權/政策)

長期的空窗
(探查/盤點/更新/維護/反映)

過度的信任
(物/人/事/時/地)

現代資安威脅的特性



現代資安防護的議題領域

國內法規: 資通安全管理法, 電子銀行安控, 金融機構資訊系統安全基準, 個資法

辦法機制: 金估法, 證券商資通安全檢查機制

國際規範: PCI-DSS, OWASP

資安治理: ISMS, ISO-27001

規範符合落實

系統弱點安全

網頁應用安全

社交工程

滲透測試

資安檢測

白/黑名單管制

弱點及異常通訊監測

Virtual Patch防護

自動化裝置安全

次世代端點防護

無毒化文件

行動裝置安全

資料安全

基礎架構安全

新世代網路安全開道

DNS安全防護

HTTPS流量加解密

特權存取安全

進階威脅攻擊

0-day及惡意程式威脅

APT威脅防護

SIEM及威脅情資

AI人工智慧防護

DDOS攻擊

DDoS防護

流量清洗

DNS DDoS防護

新科技安全

雲端服務

容器Container

ICS及OT安全

現代資安議題

現代資安防護策略

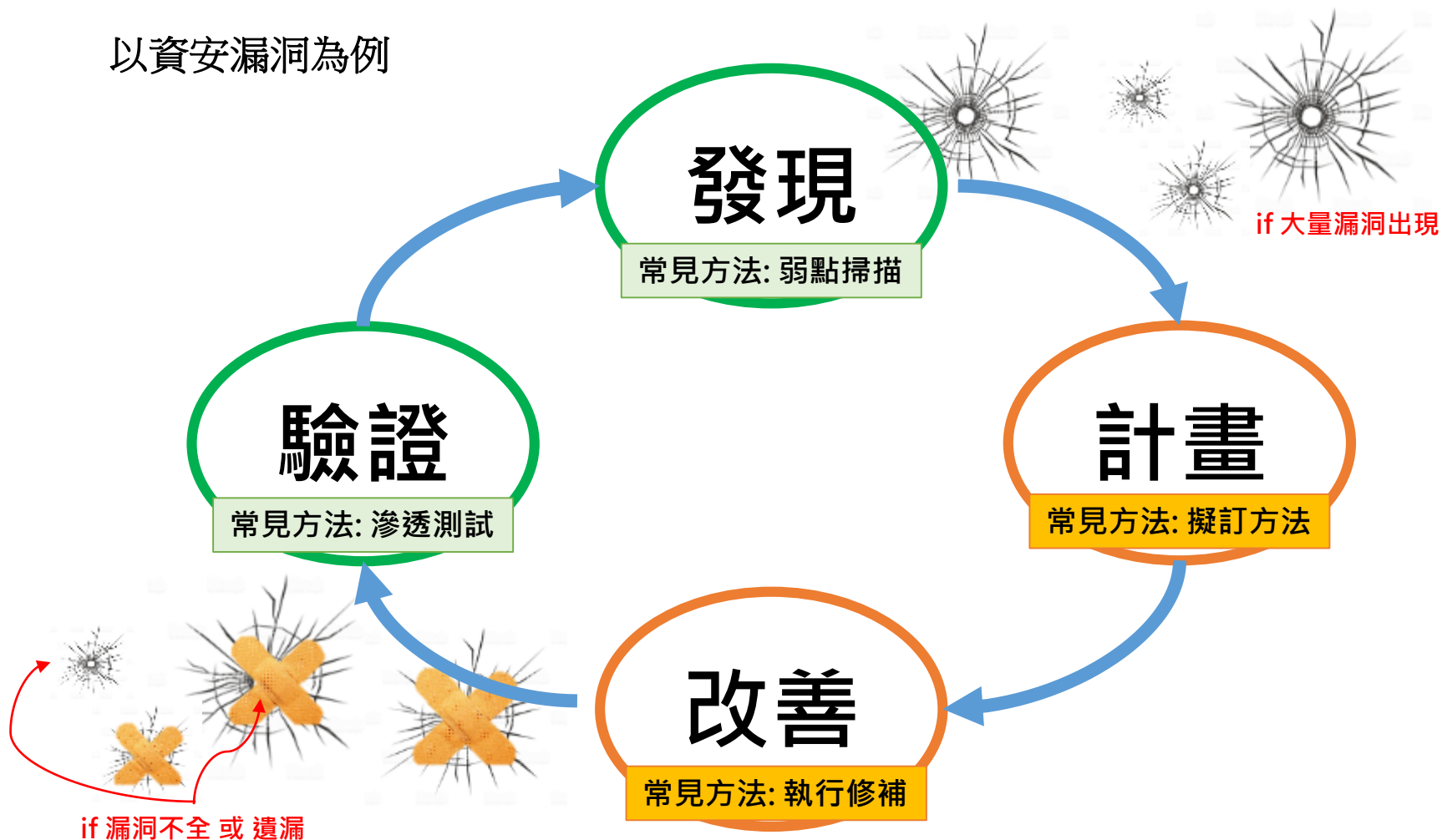
資安健檢 · 攻防演練

<h2>事前</h2>	<table border="0"><tr><td data-bbox="691 282 904 468"><h3>資產管理</h3><ul style="list-style-type: none">• 架構拓樸• 資產清單• 帳號權限</td><td data-bbox="1031 282 1325 554"><h3>資安風險管理</h3><ul style="list-style-type: none">• 漏洞監測管理• 網路監測• 風險分析• 威脅情資• 攻擊預測</td><td data-bbox="1406 282 1696 511"><h3>存取管理</h3><ul style="list-style-type: none">• 網路存取控制• 系統存取控制• 應用服務控制• 特權稽核控制</td></tr></table>	<h3>資產管理</h3> <ul style="list-style-type: none">• 架構拓樸• 資產清單• 帳號權限	<h3>資安風險管理</h3> <ul style="list-style-type: none">• 漏洞監測管理• 網路監測• 風險分析• 威脅情資• 攻擊預測	<h3>存取管理</h3> <ul style="list-style-type: none">• 網路存取控制• 系統存取控制• 應用服務控制• 特權稽核控制
<h3>資產管理</h3> <ul style="list-style-type: none">• 架構拓樸• 資產清單• 帳號權限	<h3>資安風險管理</h3> <ul style="list-style-type: none">• 漏洞監測管理• 網路監測• 風險分析• 威脅情資• 攻擊預測	<h3>存取管理</h3> <ul style="list-style-type: none">• 網路存取控制• 系統存取控制• 應用服務控制• 特權稽核控制		
<h2>事中</h2>	<h3>資安攻擊防禦</h3> <ul style="list-style-type: none">• 資安漏洞補強 (e.g. Virtual Patch)• 已知攻擊防護 (e.g. 邊際防護, 端點防護)• 未知威脅預先防禦 (e.g. 沙箱分析, 異常行為分析, AI)• 進階威脅防禦 (e.g. 資料外洩, 無毒害文檔,)• 身分識別驗證 (e.g. 安全憑證, 多因子驗證)			
<h2>事後</h2>	<h3>存在威脅的防堵措施</h3> <ul style="list-style-type: none">• SIEM戰情中心• 情資交換• 稽核日誌紀錄• 告警通報• 鑑識調查			

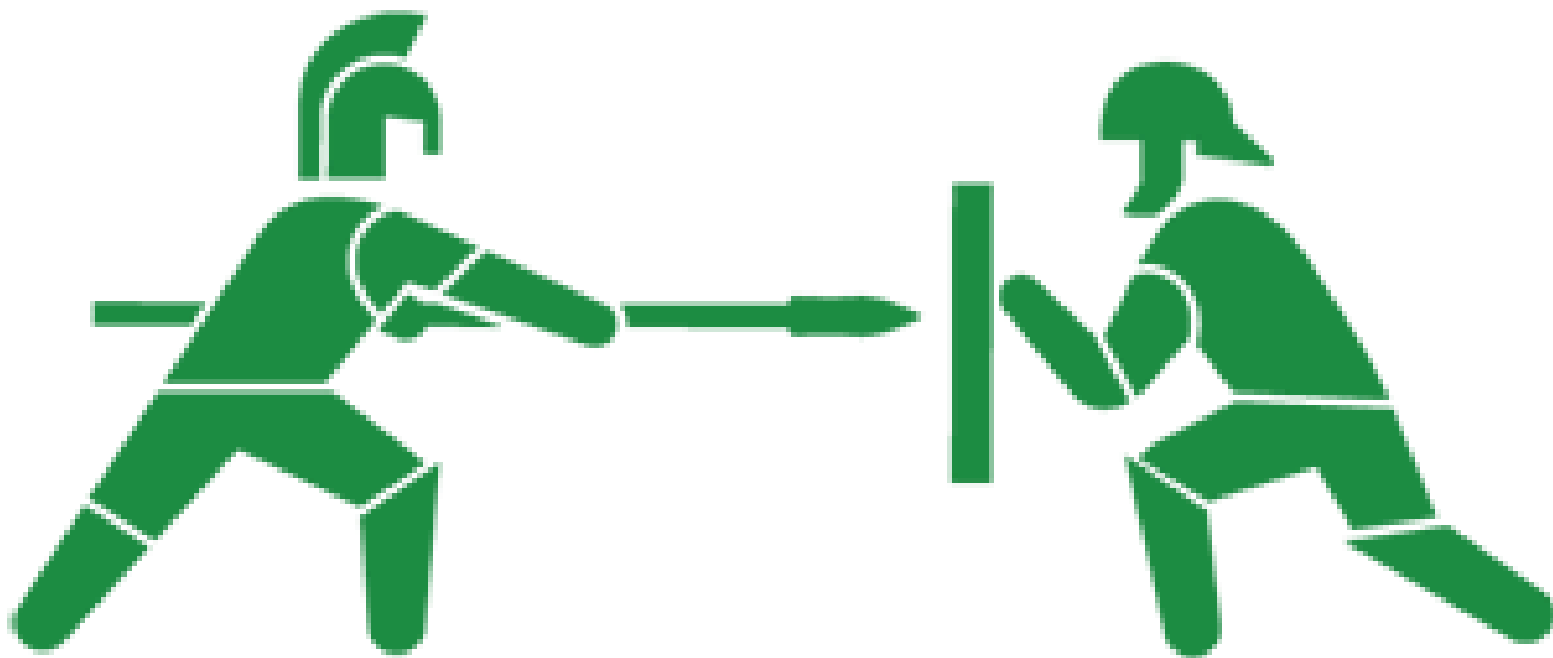
資安治理 · 政策 · 規範

現代資安防護方法

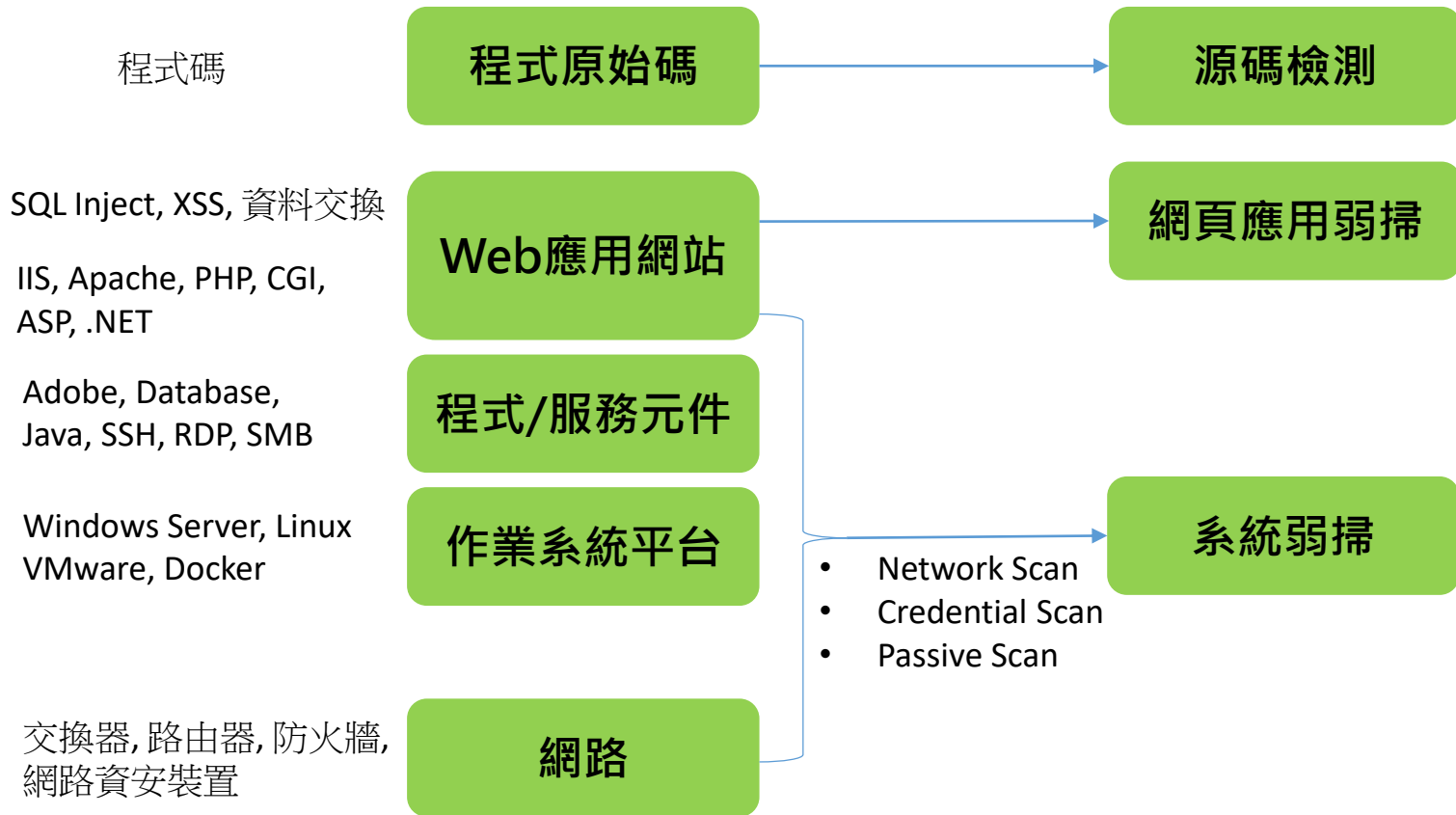
以資安漏洞為例



弱點掃描 vs. 滲透測試

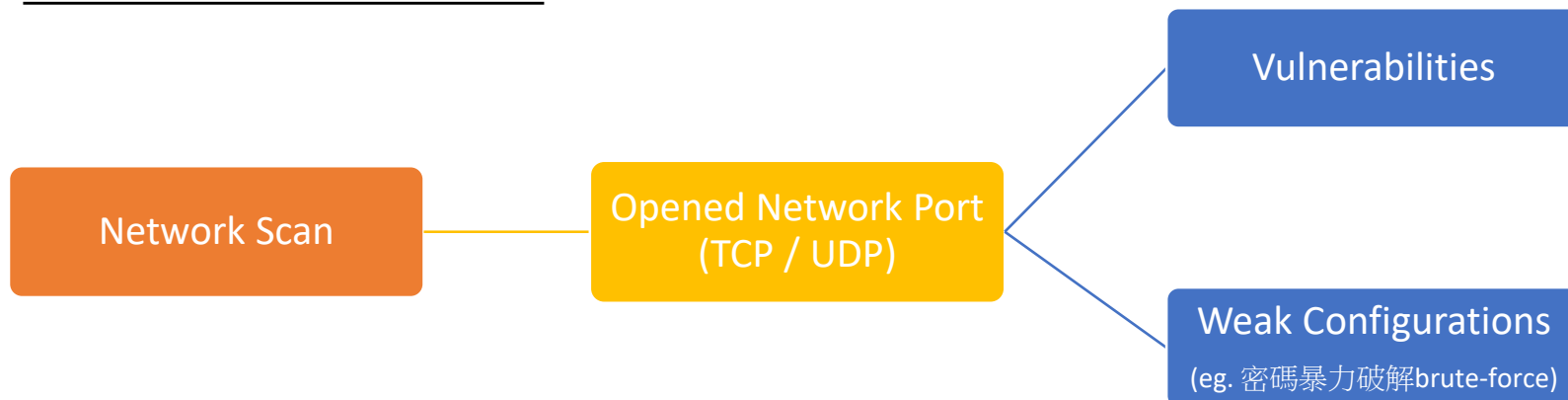


弱點掃描的主要方式



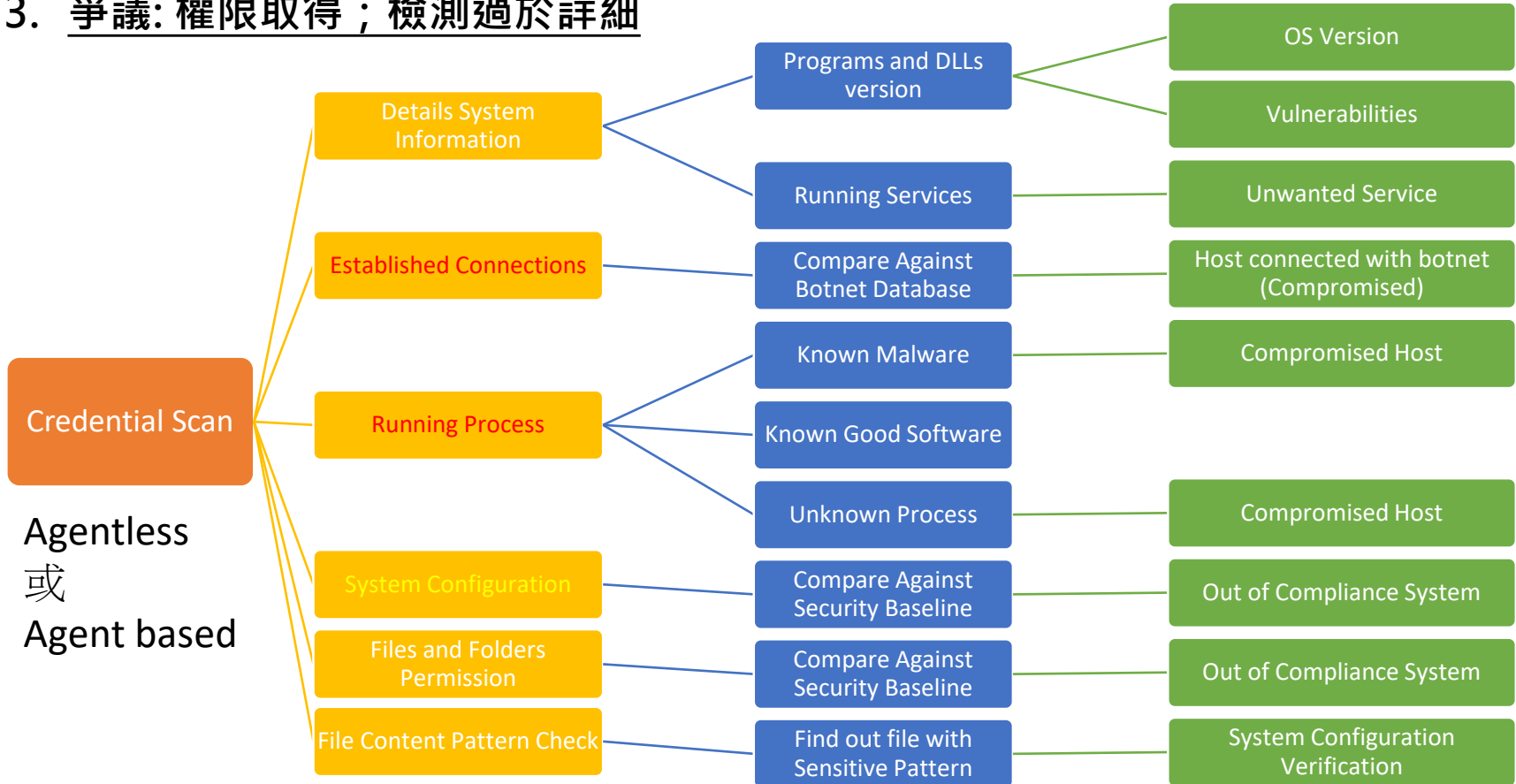
網路掃描 (Network Scan)

1. 檢測目標系統存在使用的網路埠進行探測與比對
2. 也稱“基本掃描”
3. 爭議：識別的準確性問題



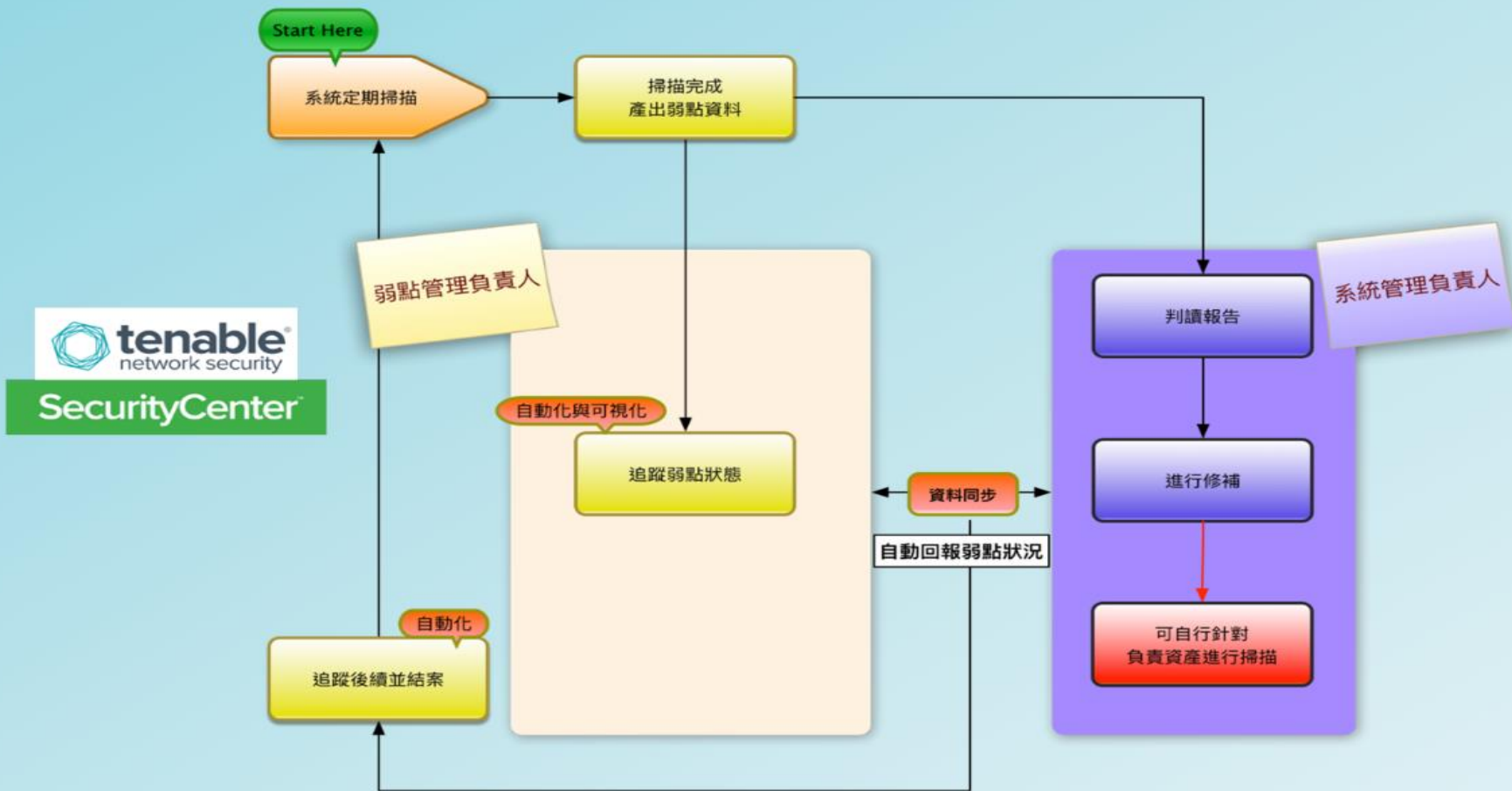
授權掃描 (Credential Scan)

1. 授予權限登入目標系統進行檢測
2. 也稱 “深層掃描”
3. 爭議: 權限取得 ; 檢測過於詳細



建立高效率的弱點安全管理

作業自動化+情報可視化的弱點管理方法



效率化第一步: 選擇弱點掃描系統工具

● 弱掃的目的

- 任務導向: 系統弱掃 或 網站弱掃 或 更多類型 (應用程式, 網路設備, 資安設備, 聯網裝置 等)
- 需求導向: 資安管理需求? 資安事件需求? 一般合規需求? 合規稽核需求?

● 付費專業軟體 或 開源免費軟體

- 付費專業軟體: 例如 Tenable
- 開源免費軟體: 例如 Nmap/Zenmap 或 OpenVAS.

● 必須支援符合國際主要標準

- 具備最新且完整的CVE 弱點資料庫
- 支援 CVSS v3 評分標準資訊 及 風險等級(5等)
- 具備 Exploit Available (弱點可利用)資訊
- 具備Solution 修補解決方案建議 及 相關資訊參考

● 具有可自動化的管理方式

● 具有分析統計能力的報告方式



效率化第二步: 建立規則

人 事 物

管理者群組建立:

- 群組: 網路(網段)、主機、系統、專案負責.
- 權限: 檢視權限、管理範圍、弱掃執行、風險管理

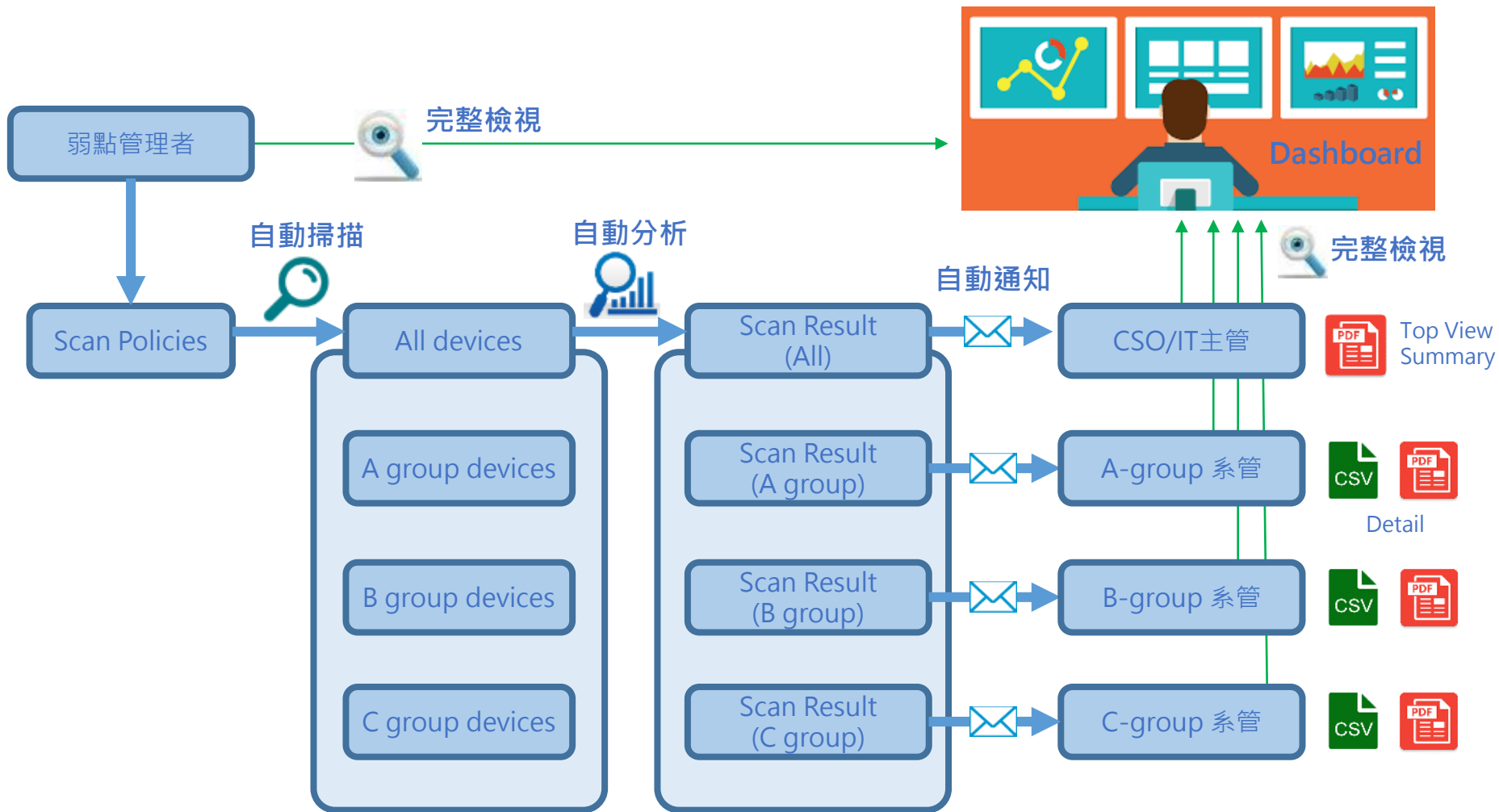
弱掃政策建立:

- 一般掃描政策.
- 進階掃描政策.
- 掃描頻率與週期

資產群組建立:

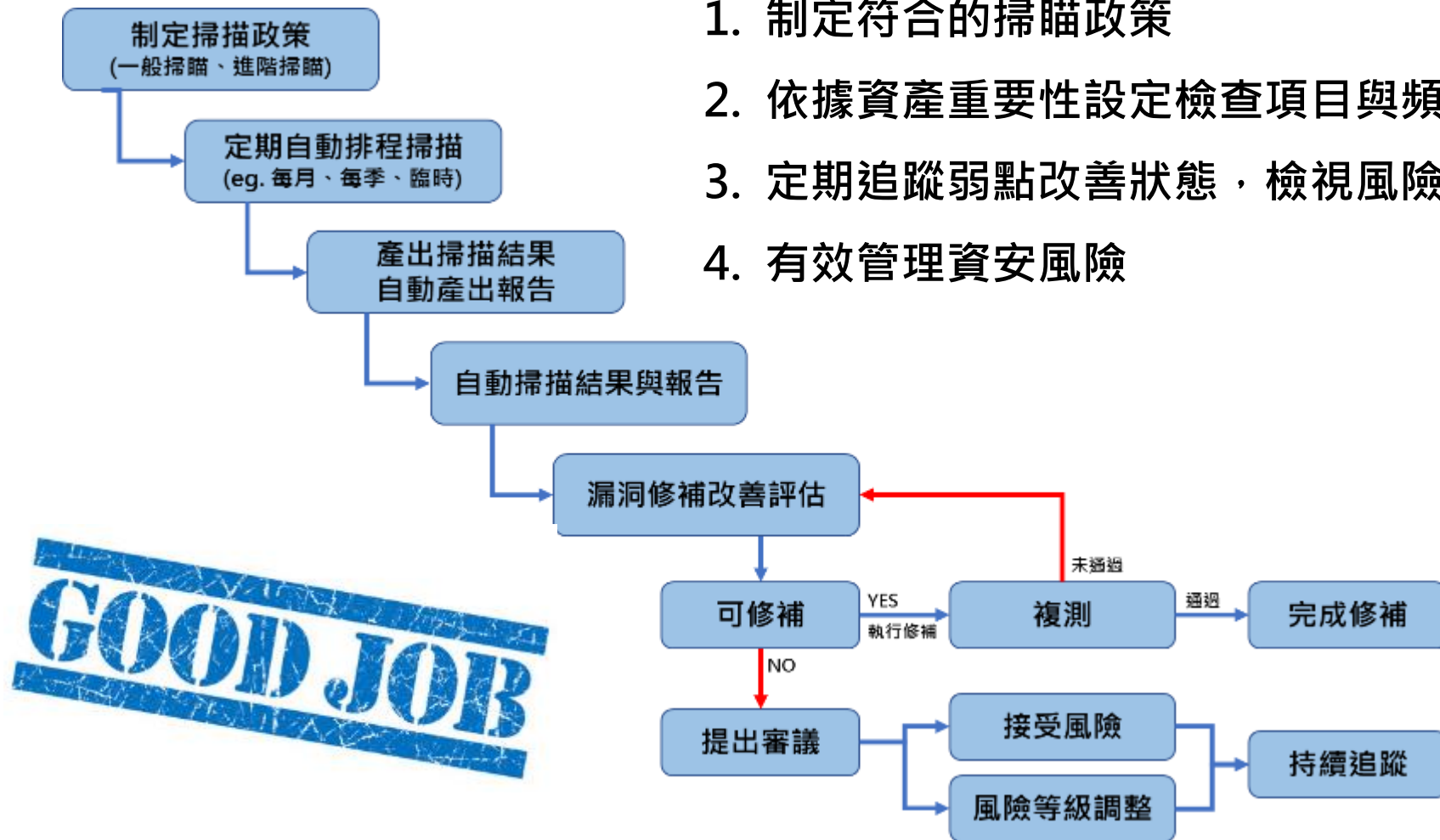
- IP範圍型態
- 作業系統型態 (Windows, Linux, UNIX, 其他)
- 應用服務型態 (Web Application, Database, VM, 其他)
- 裝置類型 (Server, Network, IP Camera, NAS, Printer, 其他)
- 專案任務型態 (校務系統, 交易系統, 會員系統, 其他)

效率化第三步: 作業流程自動化



配合資安治理政策，建立弱點風險管理機制

1. 制定符合的掃描政策
2. 依據資產重要性設定檢查項目與頻率
3. 定期追蹤弱點改善狀態，檢視風險程度
4. 有效管理資安風險



整體弱點狀態檢視

The screenshots show the SecurityCenter Vulnerability Analysis dashboard with various filters and sorting options:

- 依風險等級統計** (Filter by Risk Level): Shows a summary of vulnerabilities categorized by risk level.
- 依嚴重等級的漏洞列表** (List of vulnerabilities by severity): Displays a table of vulnerabilities sorted by severity.
- 依所有IP檢視漏洞列表** (List of vulnerabilities by all IP addresses): Shows a bar chart and table of vulnerabilities across all IP addresses.
- 依所有漏洞列表** (List of all vulnerabilities): Displays a detailed table of all vulnerabilities with columns for Plugin ID, Plugin Name, Family, Severity, and CVE ID.

The screenshots show the SecurityCenter Vulnerability Analysis dashboard with specific sorting and ranking options:

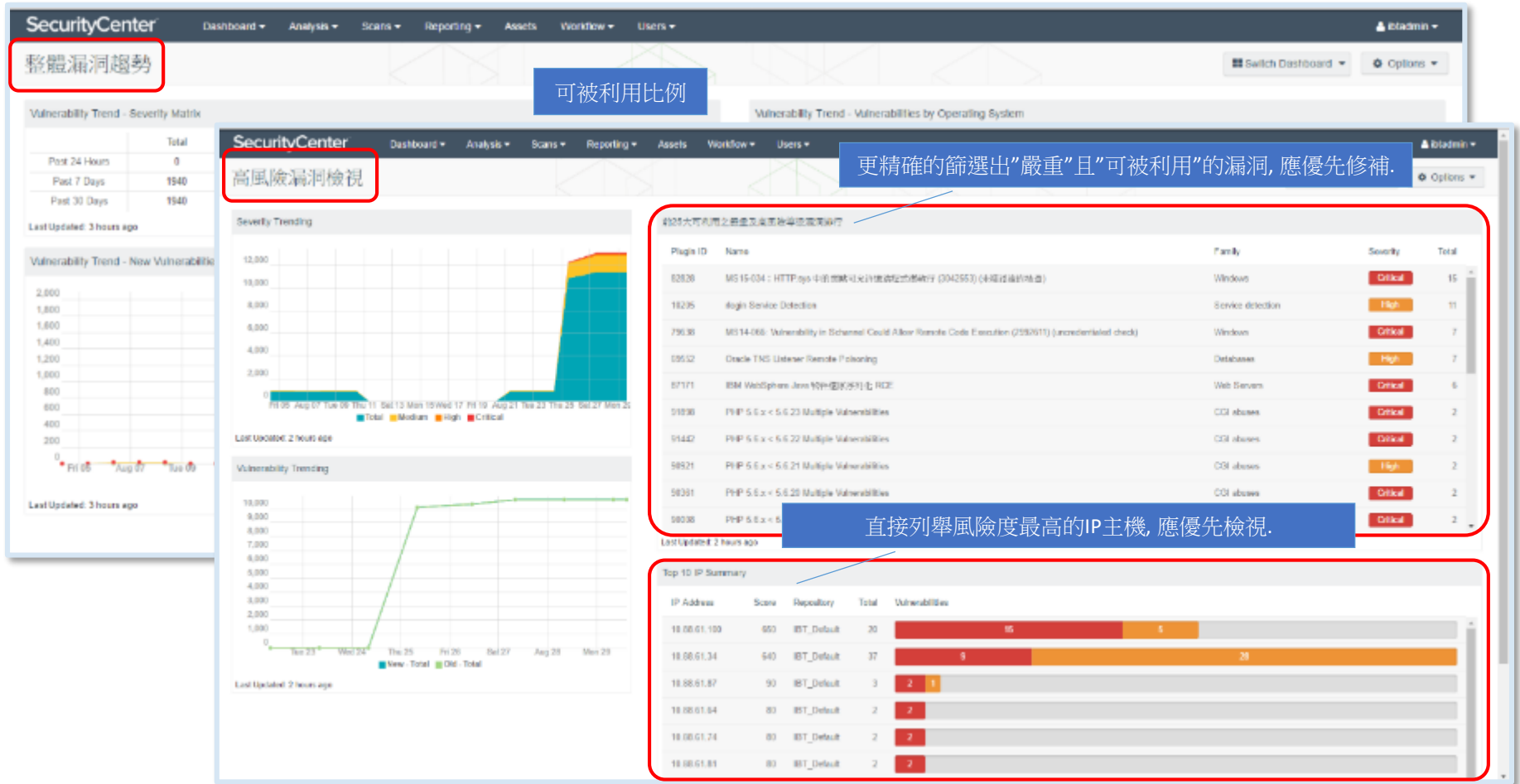
- 前10大漏洞項目 TopN 排行方式** (Top 10 largest vulnerability items): A table showing the top 10 vulnerabilities by severity.
- 前10大IP列表** (Top 10 IP addresses): A table showing the top 10 IP addresses with the highest number of vulnerabilities.

Plugin ID	Name	Family	Severity	Total
51192	無法信任 SSL 憑證	General	Medium	6
57682	SSL 自稱簽署憑證	General	Medium	4
57608	需要 SMB 簽署	Misc.	Medium	3
85332	MS15-082: Vulnerability in RDP Could Allow Remote	Windows: Mi...	Medium	2

IP Address	Score	Repository	Total	Vulnerabilities
192.168.3.16	4112	DMZ	715	321, 140, 240
192.168.3.12	2046	DMZ	295	104, 112
192.168.3.129	591	DMZ	154	90
192.168.3.132	140	DMZ	137	129
192.168.3.10	20	DMZ	90	82
192.168.3.1	18	DMZ	63	
192.168.3.2	3	DMZ	15	
192.168.3.254	3	DMZ	5	
192.168.3.3	0	DMZ	1	
192.168.3.4	0	DMZ	1	

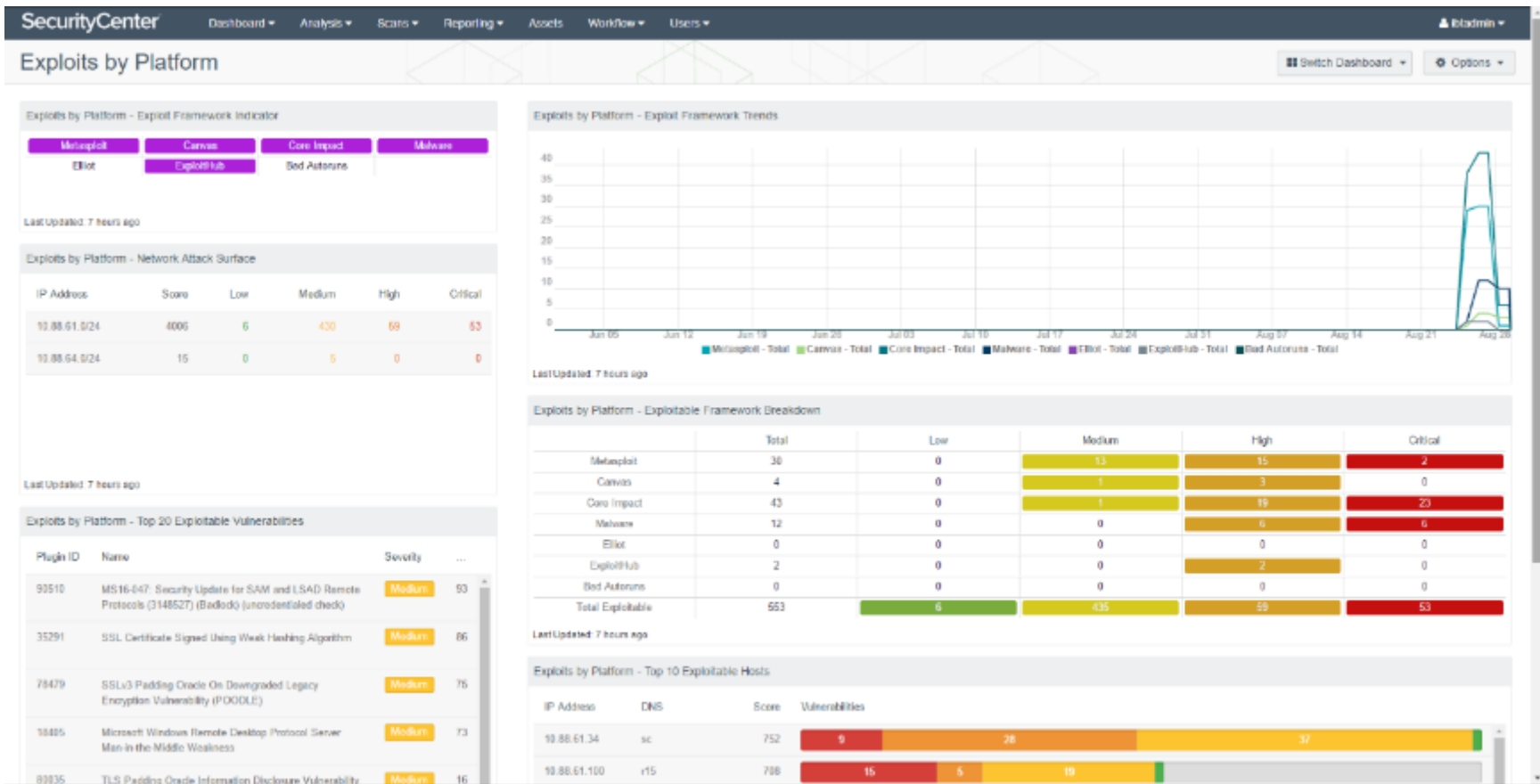
Last Updated: 3 days ago

弱點分布情報快速檢視



可利用弱點分析

可利用弱點套件(Exploitable)分析



弱點篩選過濾發現

內建多層的過濾條件, 直覺的操作介面, 加速各個管理者對於漏洞的分析與反應.

The screenshot displays the SecurityCenter Vulnerability Analysis interface. The top navigation bar includes Dashboard, Analysis, Scans, Reporting, Assets, Workflow, and Users. The main header shows 'Vulnerability Analysis' and 'Options'. The left sidebar contains a 'Filters' section with the following settings:

- Exploit Available: Yes (highlighted with a red box and a callout '過濾條件為"可被利用"')
- Repositories: IBT_Default
- Severity: Critical, High (highlighted with a red box and a callout '過濾條件為"嚴重及高風險"')
- Address: All
- Plugin Name: All

The main table displays a list of vulnerabilities with the following columns: Plugin ID, Name, Family, Severity, Host Total, and Total. The row for '87171 IBM WebSphere Java 物件序列化 RCE' is highlighted with a red box.

Plugin ID	Name	Family	Severity	Host Total	Total
82828	MS15-034 : HTTP.sys 中的弱點可允許遠端式跨站字串 (CSRF) (昇級認證的檢查)	Windows	Critical	12	15
79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unauthenticated check)	Windows	Critical	7	7
87171	IBM WebSphere Java 物件序列化 RCE	Web Servers	Critical	6	6
85887	PHP 5.6.x < 5.6.13 多個弱點	CGI abuses	Critical	1	2
88679	PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities	CGI abuses	Critical	1	2
88694	PHP 5.6.x < 5.6.18 Multiple Vulnerabilities	CGI abuses	Critical	1	2
91442	PHP 5.6.x < 5.6.22 Multiple Vulnerabilities	CGI abuses	Critical	1	2
91898	PHP 5.6.x < 5.6.23 Multiple Vulnerabilities	CGI abuses	Critical	1	2
76690	RHEL 6 : nss and nssrpm (RHSA-2014-0917)	Red Hat Local Security Checks	Critical	1	1
81469	RHEL 6 : samba (RHSA-2015-0250)	Red Hat Local Security Checks	Critical	1	1
81470	RHEL 6 : samba (RHSA-2015-0251)	Red Hat Local Security Checks	Critical	1	1
81473	RHEL 6 : samba (RHSA-2015-0254)	Red Hat Local Security Checks	Critical	1	1
81474	RHEL 6 : samba (RHSA-2015-0255)	Red Hat Local Security Checks	Critical	1	1
84258	RHEL 6 / 7 : cups (RHSA-2015-1123)	Red Hat Local Security Checks	Critical	1	1
84788	RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2015-1229) (Bat Mitzvah) (Logjam)	Red Hat Local Security Checks	Critical	1	1

Case Study

環境規模: 某金融單位國內外共計2000多台Server

傳統弱掃方式

WannaCry
事件通報

確認弱點資訊
(3天)

本次WannaCry事件的弱點資訊公布速度快，因此在設定漏洞掃描政策得以加快速度。但若以其他重大弱點未能有相關資訊可立即取得下，則必須耗費更多時間在弱點資訊的搜找與確認上。

執行弱點掃描作業
(15天)

現有弱掃工具為單一工作站，必須分區段逐一安排掃描作業，亦無法透過增派人力方式達到平行多工處理。由於掃描的主機數量多，容易拖緩弱掃工具本身的效能，或造成中斷。

弱掃結果彙整分析
(10天)

現行必須將各區段的弱掃結果透過人工方式個別彙整分析，並進一步依據資產規類比對後產出對應各系管人員的報告，再進行個別對應的案件通報。如需針對不同條件之統計分析，則所需耗費時間也會大幅增加。

弱點結果派送
(3天)

將弱點彙整的報告結果派送至各相關人員，並逐一通知及確認修補時程。

系統平台導入後弱掃方式

WannaCry
事件通報

確認弱點資訊
(1天)

本次專案弱掃系統廠商提供快速的情報資訊，弱點資料更新頻率為每日更新，可減少弱點資訊搜找的時間。

執行弱點掃描作業
(3-5天)

本次專案弱掃系統提供多個弱點掃描器的授權部署，並且可由中央管理設定排程自動執行掃描作業，並將掃描結果自動回報儲放於中央系統。並且可以僅針對指定的弱點項目(如本次WannaCry)進行指定盤查，可減少掃描作業對主機的耗能與時間。整體可加速弱掃速率，並減少作業所耗用的人力時間成本。

弱掃結果彙整分析
(1天)

本次專案弱掃系統於弱掃作業過程便已將結果回報儲放於中央系統資料庫，可直接套用相關的報告範本(如WannaCry)自動進行彙整及分析統計。可同時依據不同的管理者角色需求，產生對應的報告數據內容。具有專業的Know-How，大幅減少人工作業的時間，並且加速弱掃報告的提供。

弱點結果派送
(1天)

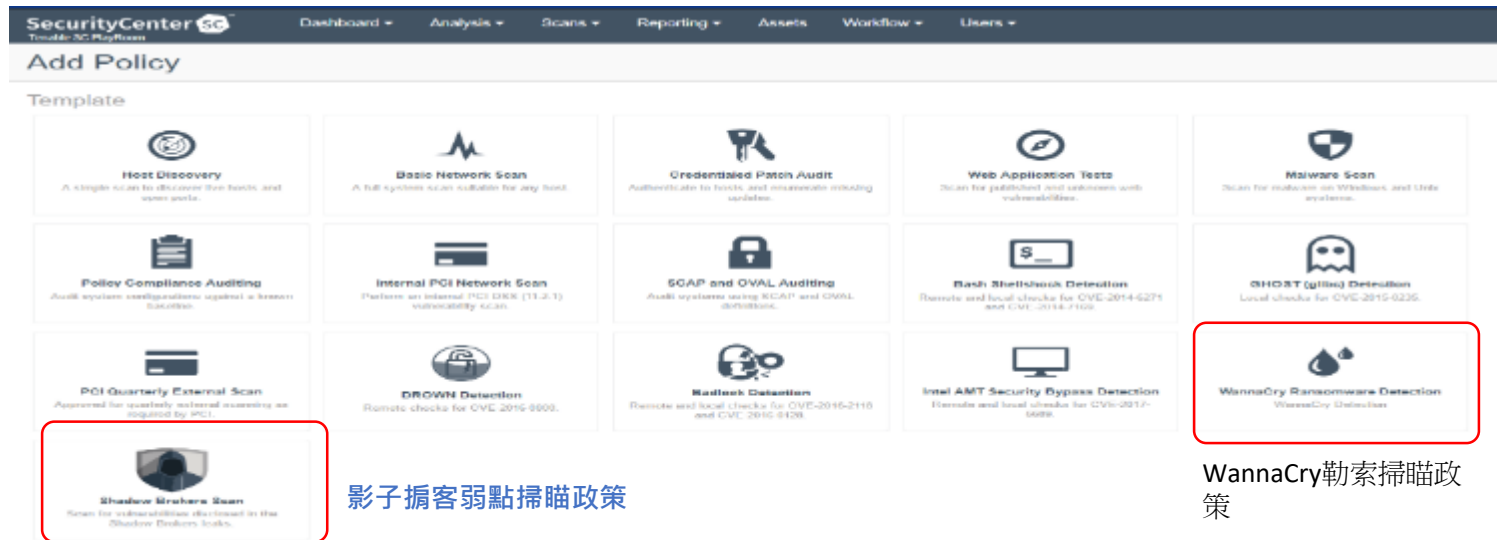
本次專案弱掃系統可針對資產對應建立弱掃結果派的規則，自動將弱掃報告透過email寄送給各相關人員。透過稽催功能可自動通知及確認修補時程，並進行追蹤與提醒。

縮減作業時間，加快反應速度
快速掌握弱點，降低風險空窗
提升資安效率，避免威脅損失



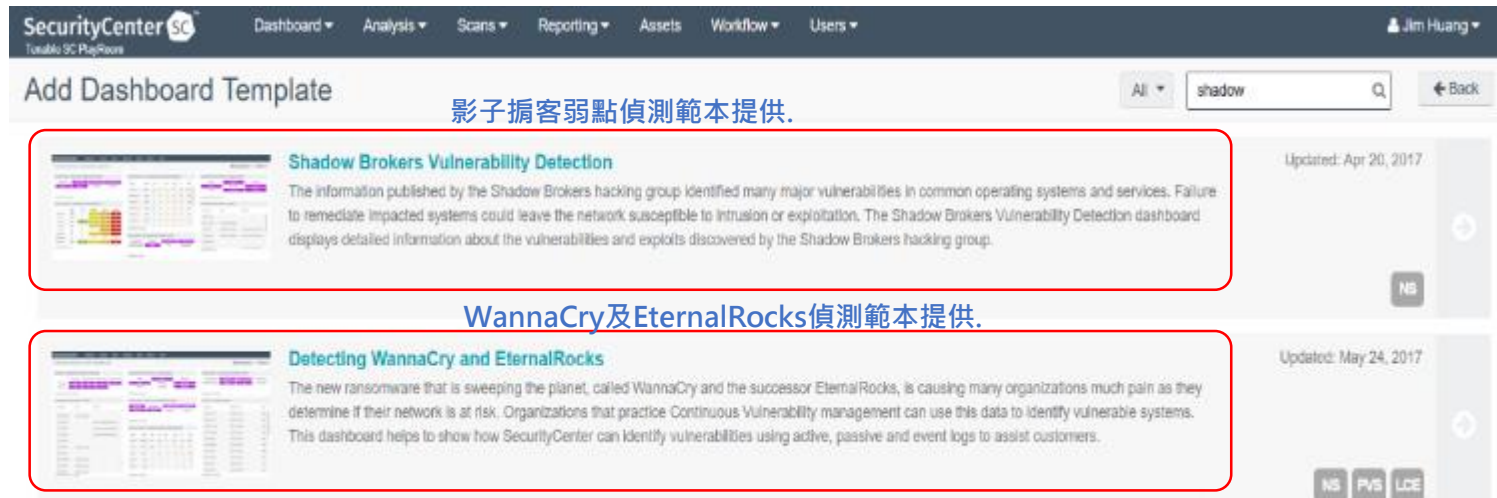
Case Study

提供重大威脅的弱點掃描政策，管理者可直接選用。



The screenshot shows the 'Add Policy' interface in SecurityCenter. It features a grid of scan templates. Two templates are highlighted with red boxes: 'Shadow Brokers Scan' (labeled '影子擷客弱點掃描政策') and 'WannaCry Ransomware Detection' (labeled 'WannaCry勒索掃描政策'). Other visible templates include Host Discovery, Basic Network Scan, Credentialed Patch Audit, Web Application Tests, Malware Scan, Policy Compliance Auditing, Internal PCI Network Scan, SCAP and OVAL Auditing, Bash Shellshock Detection, GHOST (gitlab) Detection, PCI Quarterly External Scan, DROWN Detection, Mallock Detection, and Intel AMT Security Bypass Detection.

提供相關的儀表板檢視範本，管理者可偵測已掃描結果進行快速過濾分析。



The screenshot shows the 'Add Dashboard Template' interface. A search filter 'shadow' is applied. Two dashboard templates are highlighted with red boxes: 'Shadow Brokers Vulnerability Detection' (labeled '影子擷客弱點偵測範本提供') and 'Detecting WannaCry and EternalRocks' (labeled 'WannaCry及EternalRocks偵測範本提供'). The 'Shadow Brokers' template is updated as of Apr 20, 2017, and the 'WannaCry' template is updated as of May 24, 2017.

Case Study

WannaCry及EternalRocks
偵測範本，自動針對已掃描
結果進行分析。

The screenshot displays the SecurityCenter SC dashboard with the following sections:

- WannaCry - Suspected and Confirmed Vulnerabilities:**

	Suspected	Confirmed (Ac...)	Confirmed (Pa...)	Confirmed (Ev...)
Cumulative	4	2	0	0
Mitigated	2	2	0	-

Last Updated: Less than a minute ago
- Shadow Brokers - Codenamed Vulnerabilities and Exploits:**
 - DoublePulsar, EclipsedWing, EducatedScholar, EmeraldThread, EskimoRoll, FlameP, Metasploit, PoisonIvy

Last Updated: Less than a minute ago

- WannaCry - Connection Summary:**

Source IP	Destination IP	Count
172.16.132.183	216.216.112.149	336
172.16.132.183	212.44.64.202	330
172.10.133.4	172.10.133.1	180
172.16.132.183	172.16.132.185	28
172.16.133.21	172.16.133.4	7
- Shadow Brokers - Unsupported and Outdated Products:**
- Windows 2000, Windows XP, Windows Server 20..., Windows Vista, Microsoft Exchange, SMDv1, IIS, Lotus Domino

Last Updated: Less than a minute ago
- Executive Summary - Outstanding Patches by Operating System:**

Family	Sc...	I...	Low	H...	T...
--------	-------	------	-----	------	------

自動套用WannaCry相關
的弱點項目進行過濾。

The screenshot displays the SecurityCenter SC dashboard with the following sections:

- Vulnerability Analysis:**
 - Filters:**
 - CVE ID: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
 - Plugin Type: Active
 - Address: All
 - Plugin Name
 - IP Summary:**

IP Address	NetBIOS	Score	Total	Vulnerabilities
172.16.132.185	TESTLABDEMO03	00	2	2
172.16.132.186	WORKGROUP\DA-WIN	00	2	2

自動比對過濾出存在WannaCry弱點的主機IP。

Case Study

效益

1. 透過WSUS 派送更新相關的修補程式.
2. 透過弱掃系統Tenable SC 稽核修補完整性，並發現存在弱點系統.
3. 結合資安防護系統，針對主要弱點加以偵測防護，防止內部橫向擴散.
4. 達成 提早預防、持續監測、全面防護的最大資安防護網.

The screenshot shows the Check Point SmartDashboard interface. The top navigation bar includes 'Install Policy', 'SmartConsole', and '593/593'. The main menu contains various security services: Data Loss Prevention, IPS, Threat Prevention, Anti-Spam & Mail, Mobile Access, IPSec VPN, Compliance, QoS, and More. The 'Protections' section is active, displaying a search filter 'Look for: MS17-010' and a dropdown menu set to 'All'. Below the search bar, a table lists several protections for Microsoft Windows SMB vulnerabilities. The 'Default_Protection' and 'Recommended' columns for each entry are highlighted with a red box, showing 'Prevent' actions.

Protection	Confide...	Perf...	Industry Refere...	Relea...	?	?	?	Default_Protection	Recommended
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0143)	Medium	Med...	CVE-2017-0143	3/14/2017	Red	Blue	R...	Prevent	Prevent
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0144)	Medium	Med...	CVE-2017-0144	3/14/2017	Red	Blue	R...	Prevent	Prevent
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0145)	Medium	Med...	CVE-2017-0145	3/14/2017	Red	Blue	R...	Prevent	Prevent
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0146)	Medium	Med...	CVE-2017-0146	3/14/2017	Red	Blue	R...	Prevent	Prevent
Microsoft Windows SMB Information Disclosure (MS17-010: CVE-2017-0147)	Medium	Med...	CVE-2017-0147	3/14/2017	Red	Blue	R...	Prevent	Prevent
Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0148)	Medium	Med...	CVE-2017-0148	5/16/2017	Red	Blue	R...	Prevent	Prevent

關於「滲透測試 (簡稱PT)」

定義：

滲透測試是指藉由具備資安知識與經驗、技術人員受僱主所託，針對僱主的目標系統模擬駭客的手法進行攻擊測試，藉以發掘安全漏洞並提出改善方法的善意行為。(By 維基百科)

目的：

- 瞭解入侵者可能利用的途徑
- 瞭解系統及網路的安全強度
- 瞭解弱點並強化安全

方法論：

- OSSTMM
- OWASP Testing Guide
- SSDLC

方式：

- 白箱: 提供「檢測目標」的弱點資訊，由滲透測試者檢測；確認安全保戶強度。
- 黑箱: 只告知「檢測目標」，由滲透測試者自行發揮；模擬真實駭客攻擊。
- 灰箱: 上述二者的混和方式，常用在資訊不清楚的調查上。
- 雙黑箱: 授權合法的攻防演練。



白箱測試 vs. 黑箱測試 的優缺差異

以Web系統為例:

	優點	缺點
白箱測試	<ol style="list-style-type: none">1.弱點偵測正確率高2.提供較適當修正建議	<ol style="list-style-type: none">1.離線掃描2.僅能偵測程式碼上的弱點3.需提供程式碼
黑箱測試	<ol style="list-style-type: none">1.能偵測網站本身與程式碼的弱點2.弱點偵測範圍較為廣泛3.模擬駭客攻擊	<ol style="list-style-type: none">1.誤報率高2.需人工驗證3.需線上掃描4.耗時5.破壞性攻擊

防護架構檢測

網站系統檢測

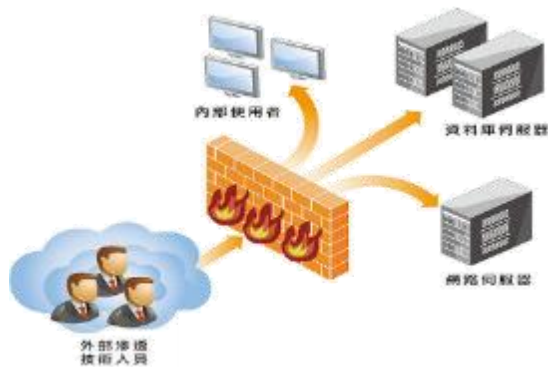
穿透檢測

原始碼檢測

周邊安全檢測

專業滲透測試服務的程序

注意！「甲方」與「乙方」必須達成共識與同意。
避免觸犯法律（刑法「告訴乃論」）



常見的滲透測試議題

□ 訊息蒐集

□ 目標探測

□ 弱點評估

□ Web掃描

□ 社交工程

□ 資料庫探測與攻擊

□ 密碼破解

□ 漏洞利用

□ 提權工具

□ 持續控制工具

□ 無線網路攻擊

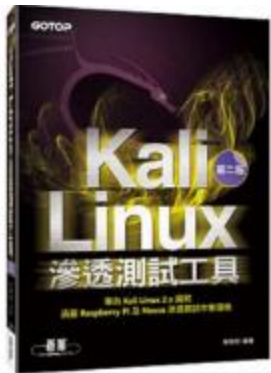
□ 壓力測試

□ 測試報告

學習資訊參考



<https://www.kali.org/>



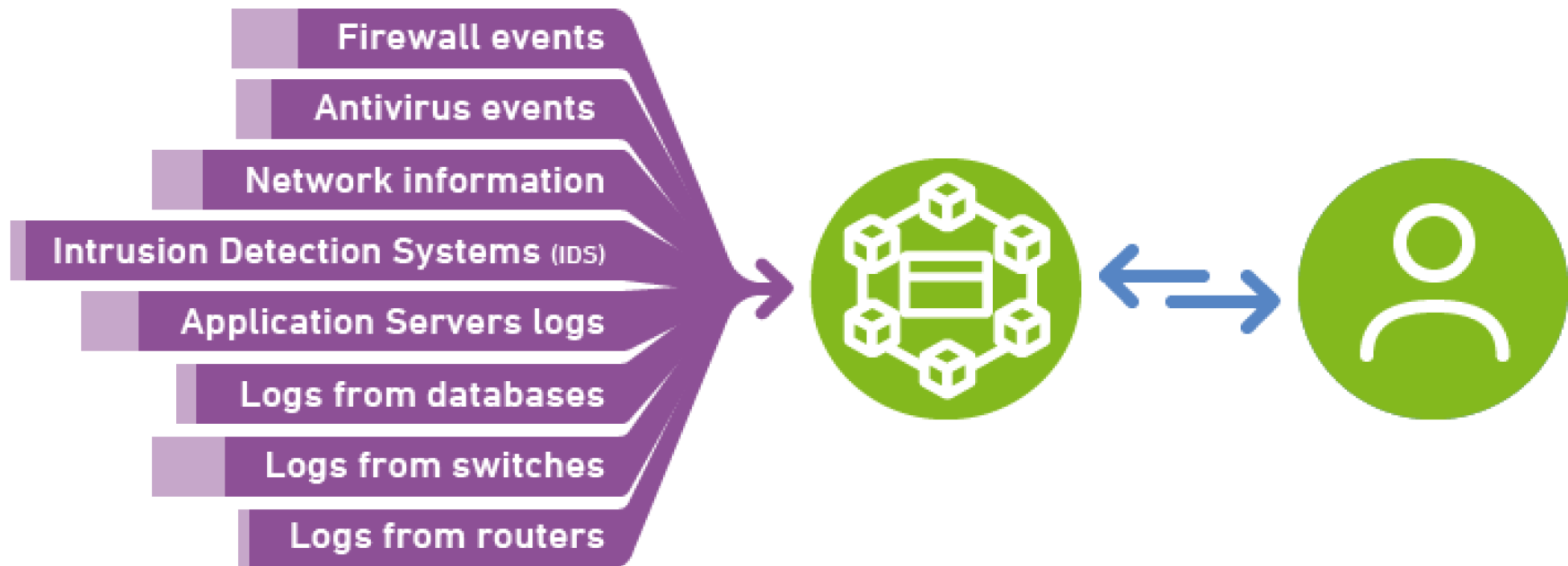
資安威脅防護方法

Complete Security by Supplementing Traditional Defenses



資料來源: FireEye

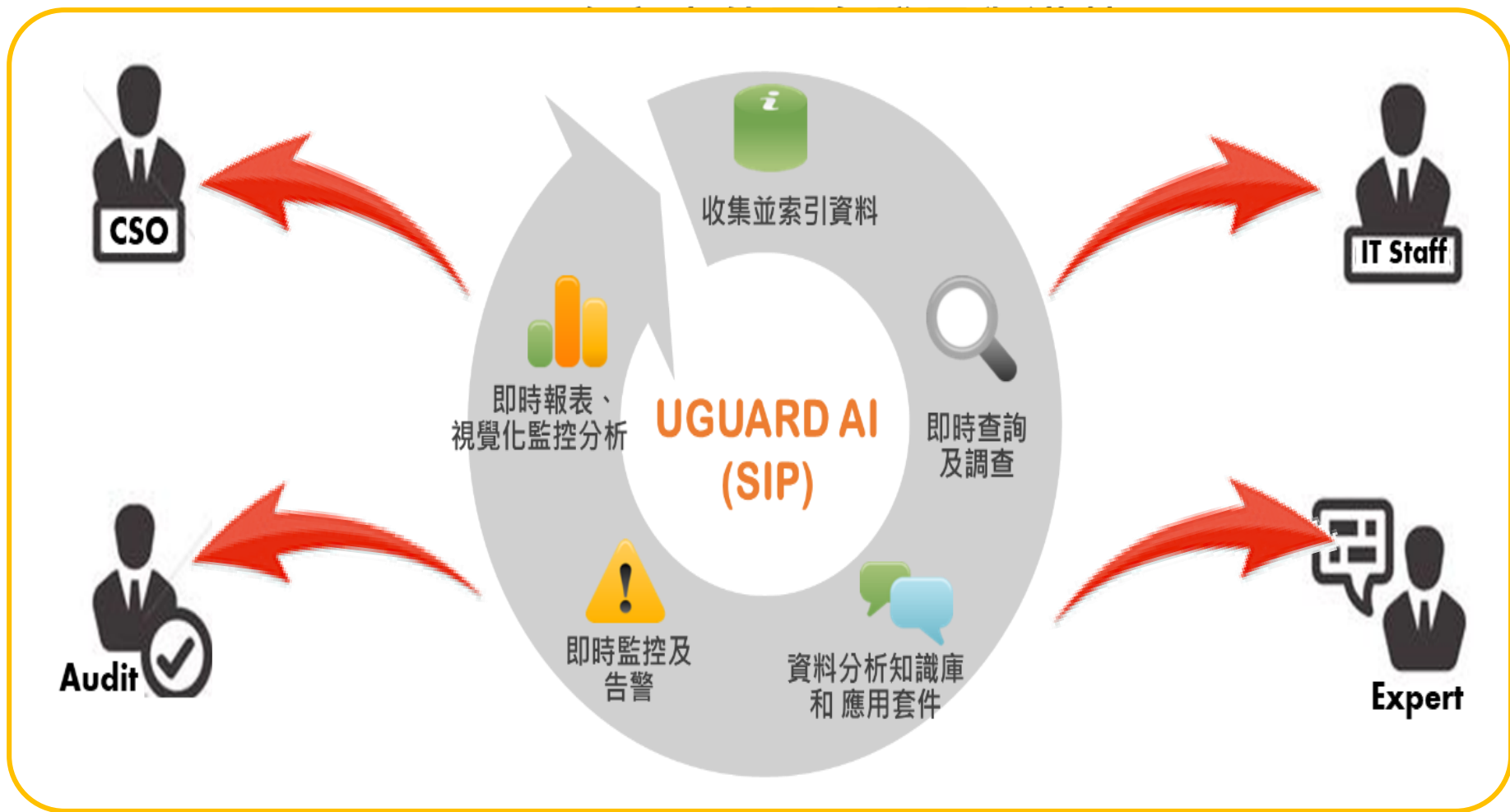
SIEM 資安事件戰情中心



DATA → SIEM ↔ SOC



SIEM 資安事件戰情中心



SIEM 資安事件戰情中心



APT 進階持續威脅偵測

- 主機: 10.210.202.55
- 行為: Port Scan, Host Sweep, 密碼猜測, 多帳號登入

本儀表板針對APT常見之行為進行監測

1. 此一儀表板針對APT常見之行為進行監測
2. 當來源IP觸發多種條件即可能該IP已被使用進行APT的進行

Port Scan掃描行為(Reconnaissance1)

src_ip	dest_ip	dest_port	event_time	dvc	src_ip	dest_ip
10.210.202.55(Private)	10.1.3.254(Private)	100,1000,10000...	999 2019-02-20 16:42:04-2019-02-20 17:13:02	FG1000	10.210.202.55(Private)	10.1.3.50(Private),10.1.4.254(P...
10.210.202.55(Private)	10.1.3.50(Private)	100,1000,10000...	1000 2019-02-20 16:42:11-2019-02-21 13:36:50	FG1000	10.210.202.55(Private)	10.1.3.50(Private),10.1.4.254(P...
10.210.202.55(Private)	10.1.4.254(Private)	10,100,1000...	4999 2019-02-20 16:37:17-2019-02-20 17:05:00	FG1000	10.210.202.55(Private)	10.1.3.50(Private),10.1.4.254(P...
10.210.202.55(Private)	10.1.4.50(Private)	10,100,1000...	4999 2019-02-20 16:37:16-2019-02-21 14:57:34	FG1000	10.210.202.55(Private)	10.1.0.10(Private),10.1.0.101(P...
10.210.202.55(Private)	10.1.0.10(Private)	10,100,1000...	1024 2019-02-20 16:20:19-2019-02-20 16:55:14	ISSDU		

來源
IP:10.210.202.55 觸
發Port scan

來源
IP:10.210.202.55 觸
發host sweep

來源
IP:10.210.202.55 觸
發密碼猜測

來源
IP:10.210.202.55 使用
多個帳號登入成功

密碼猜測行為(Reconnaissance3)

src_ip	src_user	src_host	數量	event_time	dvc_ip	src_ip	src_user	src_host	數量
10.210.202.55	hlhuang	MOTC-DC01\$ MOTC-DC04\$	37	2019-01-14 13:09:21-2019-01-15 17:46:44	10.210.202.201 10.210.202.202	10.210.202.55	rayyen	MOTC-DC01\$	1
10.210.202.55	lisa	MOTC-DC01\$ MOTC-DC04\$	158	2019-01-14 14:16:51-2019-01-19 09:31:25	10.210.202.201 10.210.202.202	10.210.202.55	yuhua	MOTC-DC01\$	3
10.210.202.55	10.210.202.55	qq	MOTC-DC01\$	4
10.210.202.55	10.210.202.55	ghr	MOTC-DC01\$	1

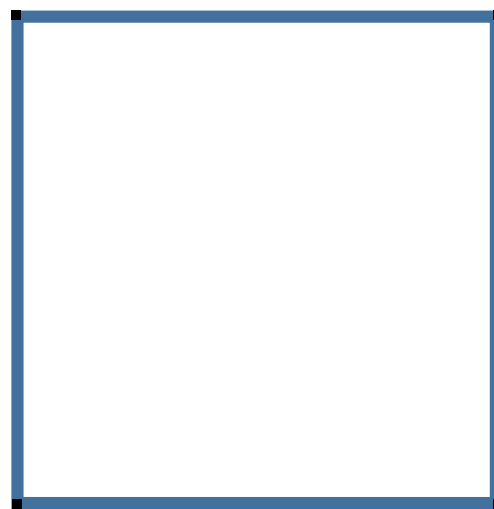
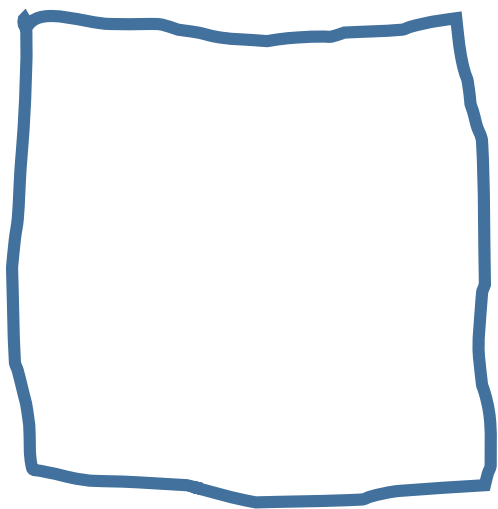
使用者帳號登入成功紀錄(Reconnaissance4)

src_ip	src_user	src_host	數量
10.210.202.55	rayyen	MOTC-DC01\$	1
10.210.202.55	yuhua	MOTC-DC01\$	3
10.210.202.55	qq	MOTC-DC01\$	4
10.210.202.55	ghr	MOTC-DC01\$	1

大綱簡介

- 資安威脅大於你可想像的程度
- 資安與駭客的距離 = 漏洞
- 建置聰明效率的資安攻防策略
- 資安法規遵循是提升資安體質的王道
- 結論 | Q&A

無規矩不成方圓



主要資安法規

國際資安管理法規:

- 資訊安全管理: ISMS, BS7799, ISO/IEC 27001, ISO 27799, NIST 800-53
- 雲端安全暨個資保護: ISO/IEC 27017, 27018
- 個資保護: BS 10012, GDPR
- 網路安全框架: Cybersecurity Framework (CFS)
- 資安管理指南: NIST CIS Control v7 (前身SANS Top20)
- 產業領域: PCI-DSS, HIPPA, Sarbanes Oxley

國內資安管理法規:

- 資通安全管理法
- 個人資料保護法施行細則
- 教育體系資通安全管理規範
- 金融機構辦理電腦系統安全評估辦法
- 金融機構辦理電子銀行業務安全控管作業基準

遵循資安規範的目的

- 規範是專家Know-how的產物
- 規範是值得參考的指導原則
- 規範的控制方法是資安防護設計的參酌依據
- 規範是提供企業建立資安工作的稽核Baseline



- 甚麼叫做好
- 究竟做多好
- 怎麼做到好
- 好到怎麼樣
- 還有哪不好

資安規範不是緊箍咒



階段導入

局部導入

策略導入

V7.1

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

資通安全管理法

資通安全管理法架構

(108年1月1日施行)

資通安全管理法（母法）

資通安全管理法施行細則（子法）

資通安全責任等級分級辦法（子法）

資通安全事件通報及應變辦法（子法）

特定非公務機關資通安全維護計畫實施情形稽核辦法（子法）

資通安全情資分享辦法（子法）

公務機關所屬人員資通安全事項獎懲辦法（子法）

八大關鍵基礎設施領域



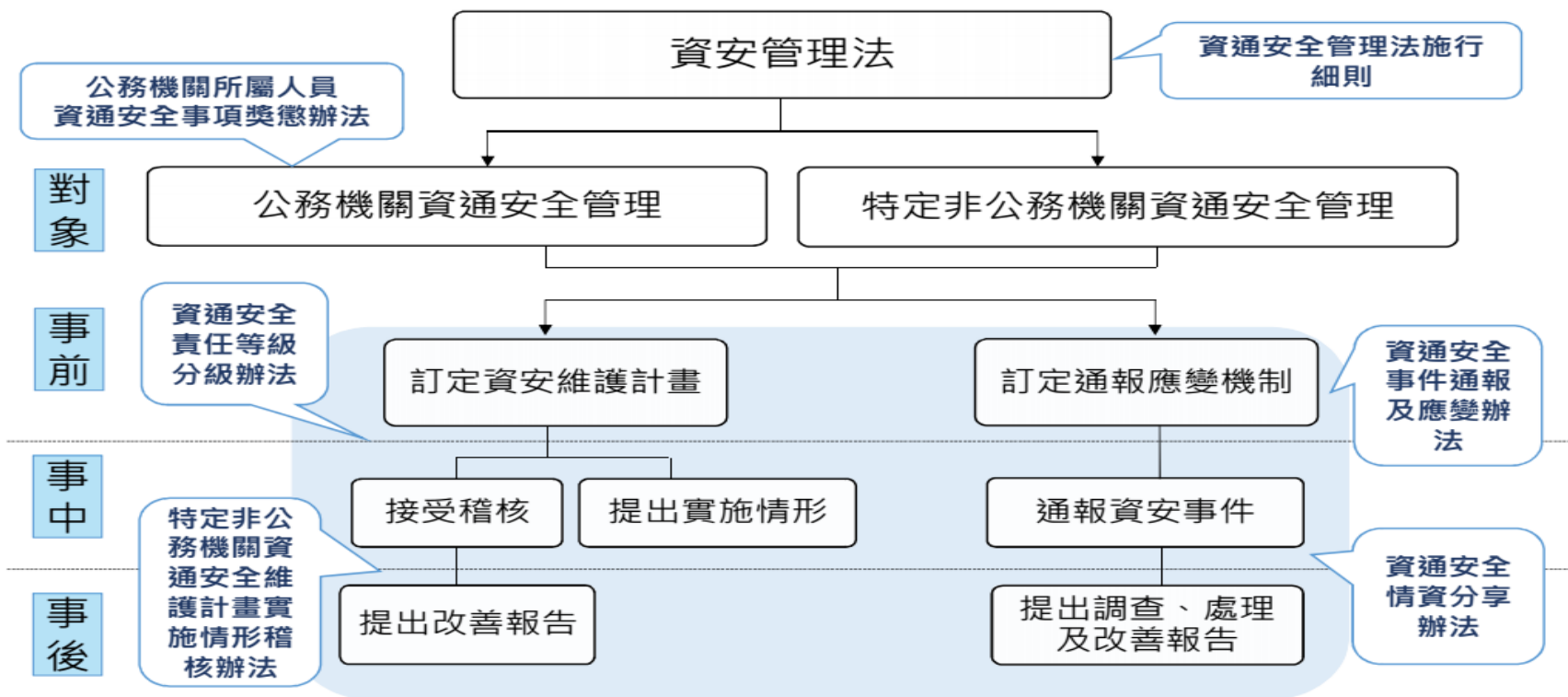
主部門	次部門
能源	電力、石油、天然氣、化學與核能材料
水資源	水源、水庫、淨水系統、供水線路
通訊傳播	通訊、傳播
交通	陸運、空運、海運、氣象、郵政及物流
銀行與金融	銀行、證券、金融市場與外匯
緊急救援與醫院	緊急醫療部門、緊急應變體系
中央與地方政府機關	重要人員、重要場所設施、資訊與網路應用服務、重要文化資產與象徵
高科技園區	科學工業與生醫園區、軟體園區與工業區

行政院資通安全處

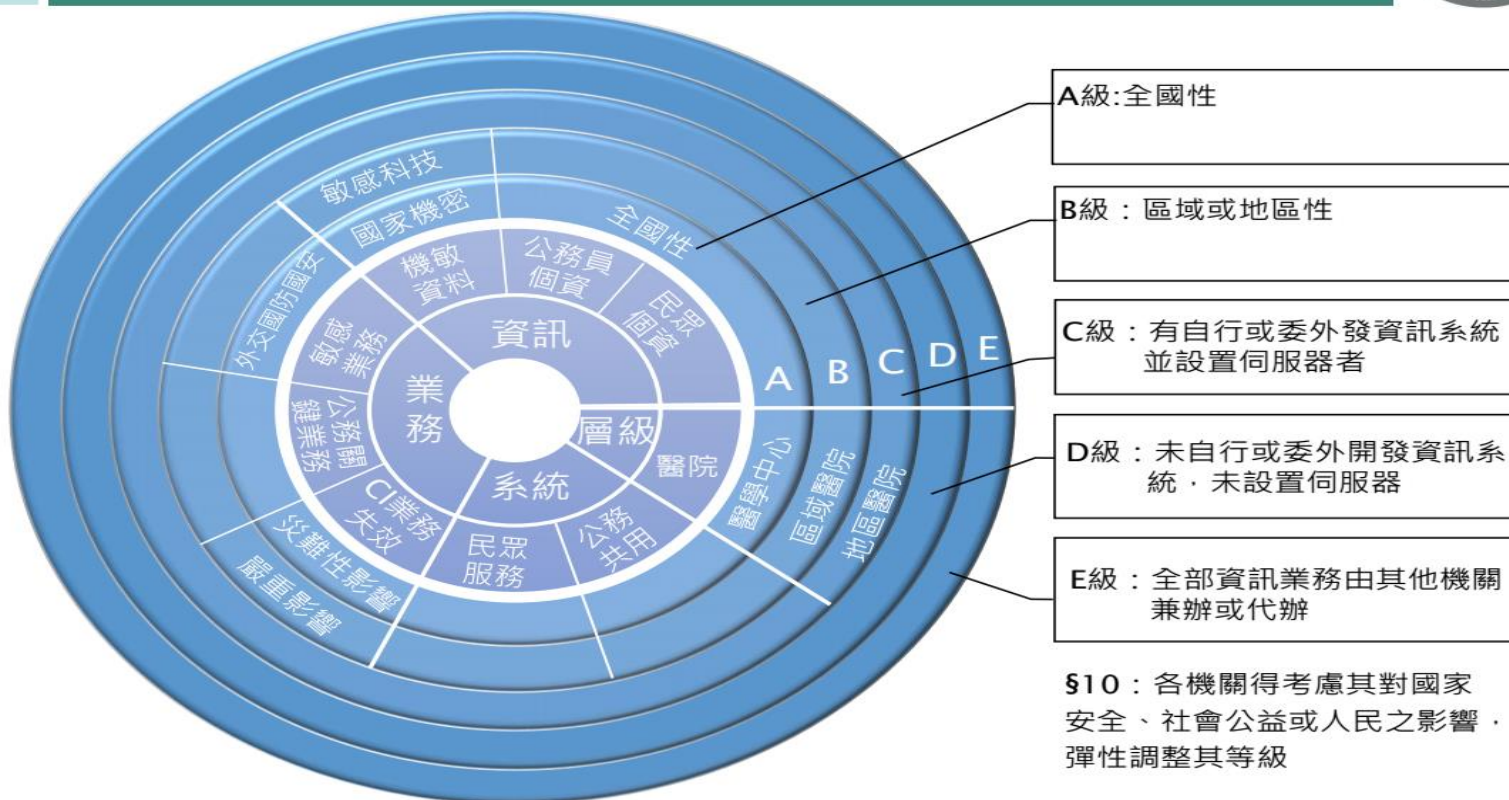
17

資通安全管理法

本法資安管理架構



資通安全責任等級分級原則

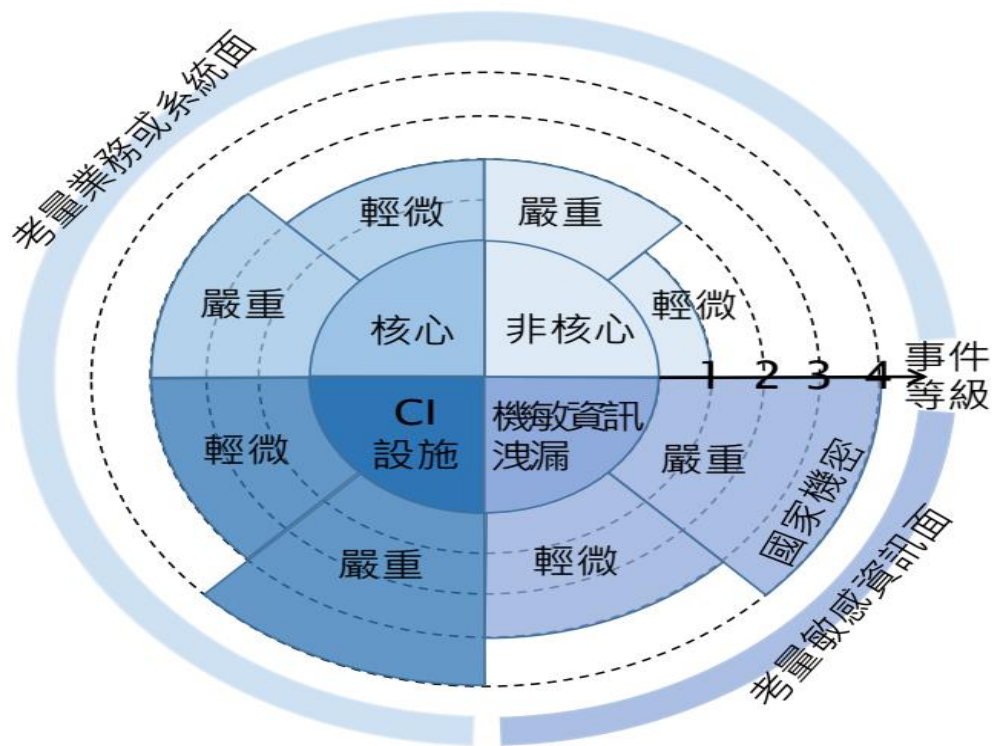


行政院資通安全處

18



資通安全事件分級



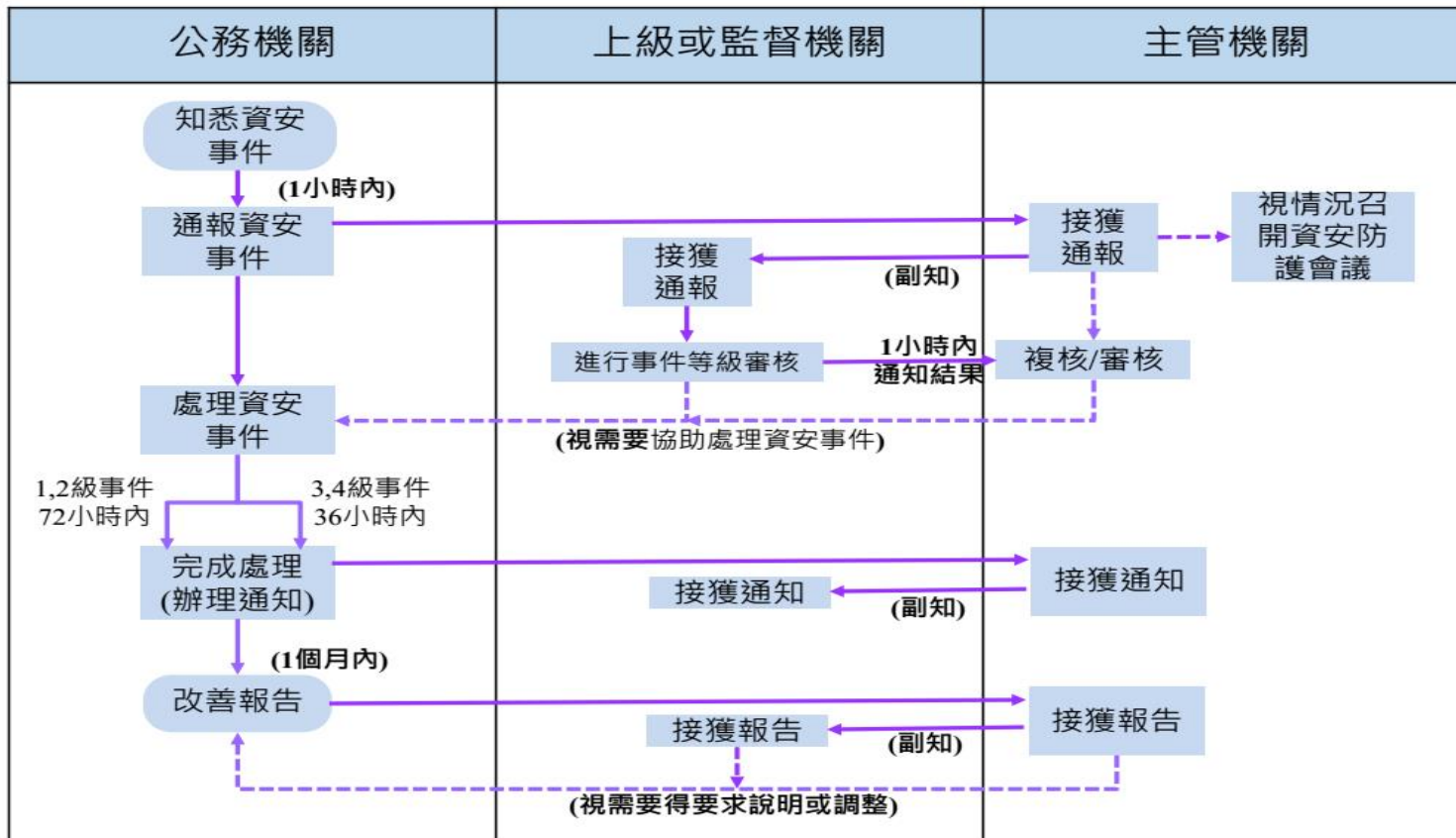
事件輕微或嚴重-考慮C,I,A三面向

- 機密性
 - 業務資訊遭洩漏
- 完整性
 - 業務資訊遭竄改
 - 資通系統遭竄改
- 可用性
 - 資訊系統受影響或停頓，是否於可接受時間內回復

同一資安事件影響二個以上機關，等級向上提升一級

資通安全管理法

事件通報流程-公務機關



資通安全責任等級 A 級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置四人；須以專職人員配置之。
	內部資通安全稽核		每年辦理二次。
	業務持續運作演練		全部核心資通系統每年辦理一次。
	資安治理成熟度評估		每年辦理一次。

資通安全責任等級 A 級之公務機關應辦事項

技術面	具有郵件伺服器者，應備電子郵件過濾機制	續使用及適時進行軟、硬體之必要更新或升級。
	入侵偵測及防禦機制	
	具有對外服務之核心資通系統者，應備應用程式防火牆	
	進階持續性威脅攻擊防禦措施	

方案工具規劃建議

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理二次。
		系統滲透測試	全部核心資通系統每年辦理一次。
	資通安全健診	網路架構檢視	每年辦理一次。
		網路惡意活動檢視	每年辦理一次。
		使用者端電腦惡意活動檢視	每年辦理一次。
		伺服器主機惡意活動檢視	每年辦理一次。
		安全設定檢視	每年辦理一次目錄伺服器設定及防火牆連線設定之檢視。
	資通安全監控管理機制		初次受核定或等級變更後之一年內，完成監控機制建置，並持續維運。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
具有郵件伺服器者，應備電子郵件過濾機制			
入侵偵測及防禦機制			
具有對外服務之核心資通系統者，應備應用程式防火牆			
	進階持續性威脅攻擊防禦措施		

方案建議:

- 資安健檢
- 弱掃及滲透測試
- Anit-Bot
- Anti-Virus/Malware
- Anit-Spam/Phishing
- Application Control
- NGFW
- IPS & Virtual Patch
- APT protect
- SIEM

資通安全責任等級 A 級之公務機關應辦事項

認知 與訓練	資通安全 教育訓練	資通安全及資訊 人員	每年至少四名人員各接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		一般使用者及主 管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專 業證照及職 能訓練證書	資通安全專業證 照	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有四張以上，並持續維持證照之有效性。
		資通安全職能評 量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有四張以上，並持續維持證書之有效性。

資通安全專業證照清單:

<https://nicst ey.gov.tw/Page/D94EC6EDE9B10E15/e5193bd4-f035-4c26-b2a1-96ec98dcef8e>

資通安全管理法 參考資訊源



行政院國家資通安全會報

National Information & Communication Security Taskforce

回首頁 | 網站導覽 | English | 行政院 字級 小 中 大

關鍵字搜尋

搜尋

進階搜尋

會報簡介

資安政策

作業規範

重點活動

資安訊息

相關連結

資安法專區

文件報告

首頁 > 資安法專區 > 資安管理法

資安法專區

▶ 資安管理法

範本文件

歷次新聞稿

歷次座談會

資安管理法



資通安全管理法常見問題

日期：108-03-05 資料來源：資通安全處

資通安全管理法常見問題

📄 相關檔案

資通安全管理法FAQ_1080305v2.2

<https://nicst ey.gov.tw/Page/EB237763A1535D65>

資通安全管理法 參考資訊源

經濟部工業局，由行政院資通安全處指導並委託財團法人工業技術研究院與財團法人電信技術中心提供《資通安全管理法》採購指引懶人包



1. 《資通安全管理法》懶人包

透過流程圖及Step-by-Step大富翁方式快速協助各機關所屬資通安全責任等級與查閱懶人包內容



2. 《資通安全管理法》採購指引懶人包

採用管理、技術與認知訓練三構面方式呈現各應辦事項之參考實作方式、參考採購需求項目及相關建議資安服務/產品及廠商



3. 《資通安全管理法》採購指引廠商名錄

採用管理、技術與認知訓練三構面方式呈現參考資安服務/產品及廠商名錄



附錄

- 《資通安全管理法》推動參考資安專欄
- 《資通安全管理法》採購指引懶人包諮詢窗口
- 《資通安全管理法》採購指引懶人包相關連結



大綱簡介

- 資安威脅大於你可想像的程度
- 資安與駭客的距離 = 漏洞
- 建置聰明效率的資安攻防策略
- 資安法規遵循是提升資安體質的王道
- 結論 | Q&A

資安工作



資安工作

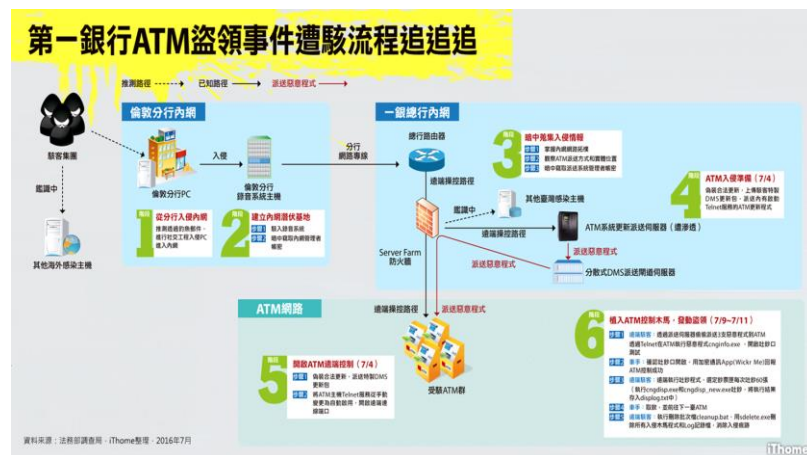
- 戰略 (資安目標/目的)
- 戰術 (資安方案/工具)
- 戰技 (執行技術/能力)



假想議題: 資料外洩



- 區段化 (Segmentation)
- 專題任務化 (Project Task)
- 零信任安全 (Zero Trust)



“天下武功无坚不摧，
唯快不破！”

—— 李小龍



Q&A

