怎樣找到你最需要的弱點工具

黃繼民 Jim Huang

副處長| 資安管理平台發展處

數聯資安股份有限公司

jim@issdu.com.tw

大綱簡介

- 前言
- 為什麼一定要掃描弱點
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

前言

漏洞帶來的恐怖教訓

WannaCry

WannaCry (想哭)

勒索軟體攻擊

令人傷心不止的WannaCry (想哭) 事件

2017年5月 WannaCry攻擊全球爆發

- 美國國安局NSA 遭到駭客組織-影子掮客入侵.
- 影子掮客在黑市釋出大量工具，包括永恆之藍.
- 永恆之藍(EternalBlue) 造成WannaCry.
- 利用微軟系統的檔案分享協定SMB漏洞攻擊.
- 勒索金額: 300~600美金或等值比特幣.
- 變種攻擊手法 推陳出新....至今(尚未平息)!!

2018年8月 台積電受駭事件

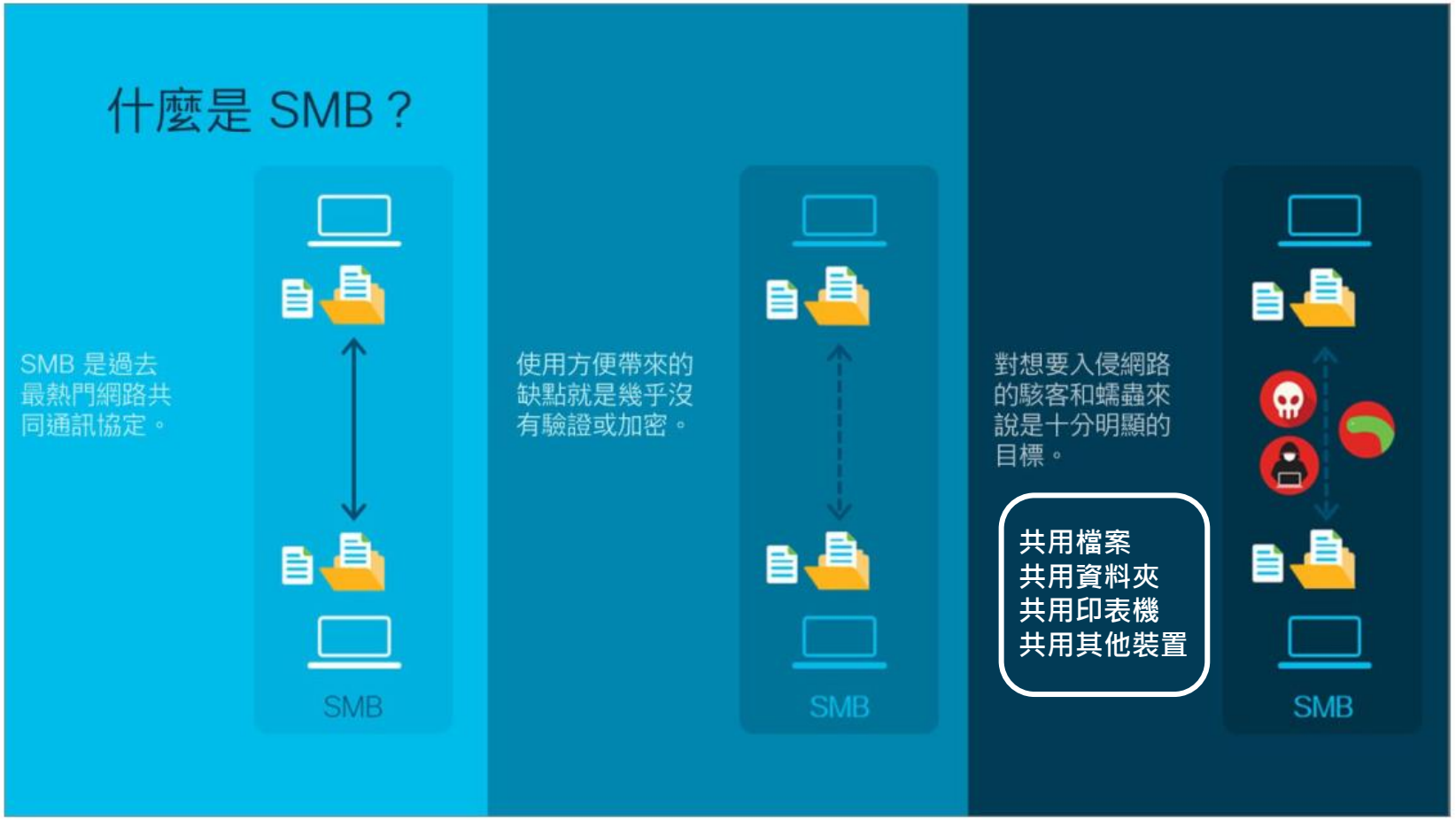
2019年10月 趨勢科技研究報告

即使漏洞修補了兩年, WannaCry 仍是 使用 EternalBlue 漏洞攻擊手法中最多的

2019 年 10 月 23 日 Trend Labs 趨勢科技全球技術支援與研發中心

即使在 EternalBlue(永恆之藍)漏洞已經修補了兩年多後，EternalBlue 仍舊非常活躍。即使到了 2019 年，WannaCry 還是所有使用 EternalBlue 攻擊手法的惡意程式當中偵測數量最多的。它的偵測數量幾乎是所有其他勒索病毒數量加總的四倍。

為何針對SMB進行攻擊



攻擊根源: 永恆之藍 EternalBlue

- 涵蓋所有微軟Windows系統 (包括停產的Win XP, Win7, 及Server 2003等).
- 主要漏洞利用SMBv1 檔案分享通訊協定，通訊埠445 及 139.
- 修補建議: MS17-010 或 關閉SMBv1.
- 2017年 6月出現變種攻擊Petya 及 Not Petya.
- 2017年 6月出現變種攻擊SambaCry 針對Linux系統(Server, NAS, IoT裝置).
- 2018年 駭客利用「永恆之藍」入侵家用型網路，台灣受攻擊次數連三週高居全球首位.
- 2019年漏洞搜尋系統Shodan統計，全球有上百萬個連網設備存在風險，台灣排名第5名.

同樣令人想哭的抉擇...

升版?

維持?

修補?

其他?

防護?

機率?

穩定性?

人力?

費用?

時間?

SMB漏洞惡夢並未結束...

https://www.issdu.com.tw/news_detail.php?id=119&type=security

大綱簡介

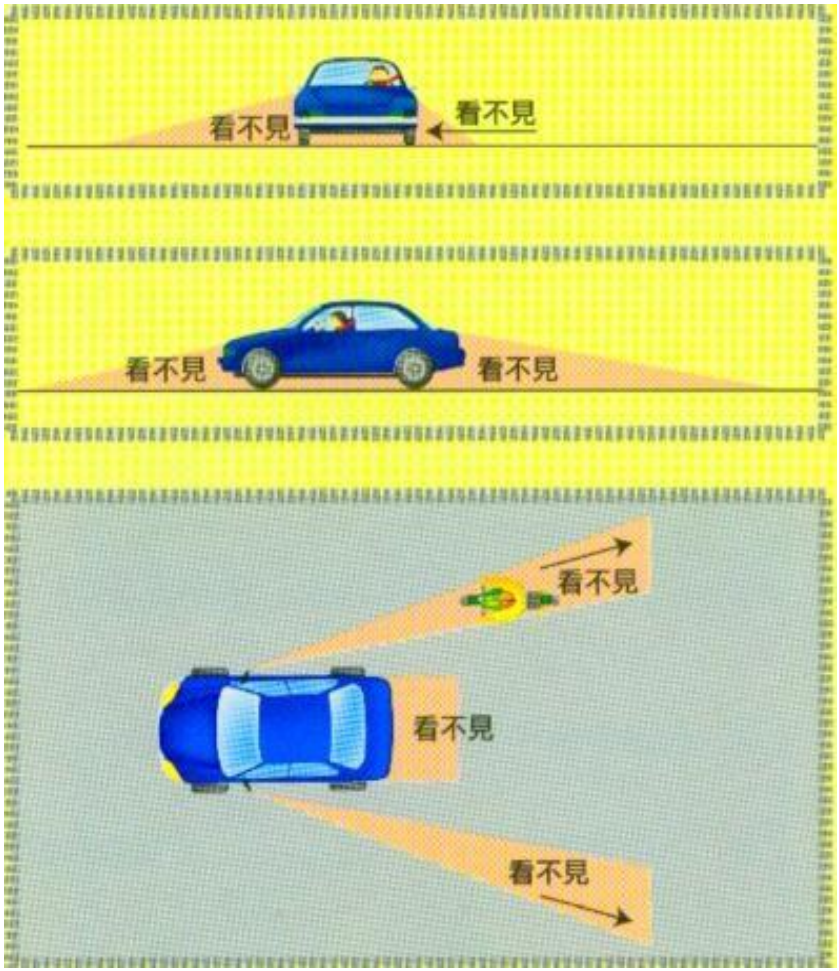
- 前言
- 為什麼一定要掃描弱點
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

弱點 Vulnerability

Blind Side

看不見

弱點



弱點掃描：掌握風險

從安全的視角

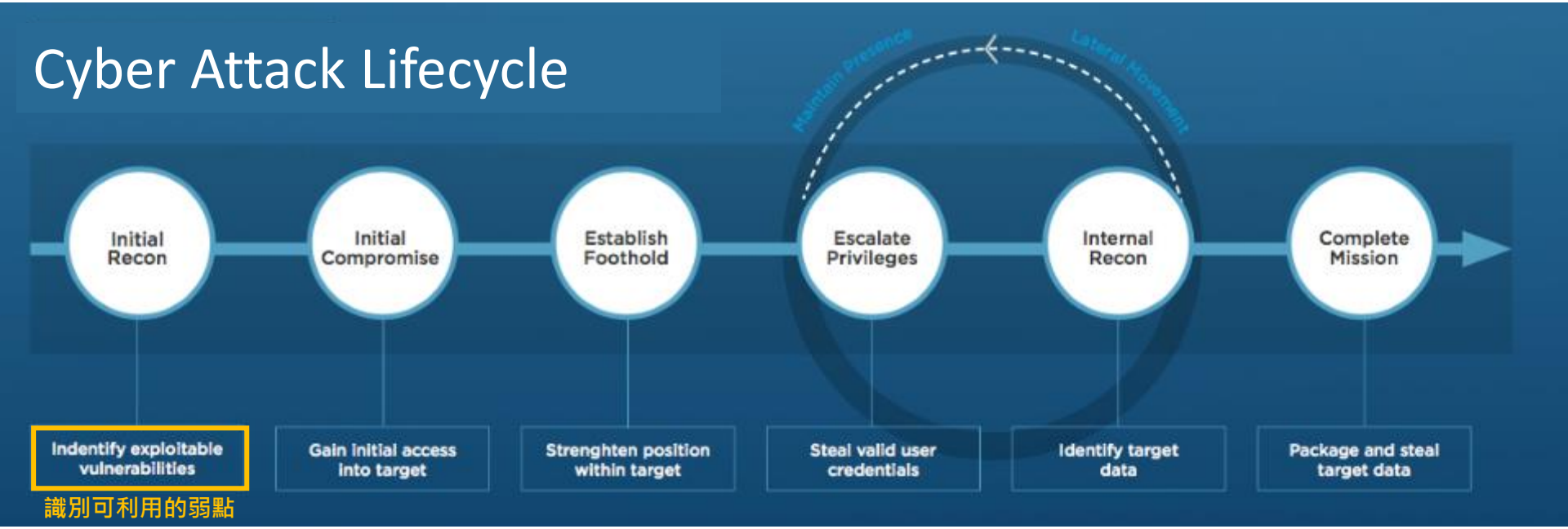
掌握存在的弱點，提早應對準備，避免風險暴露.

漏洞攻擊崛起

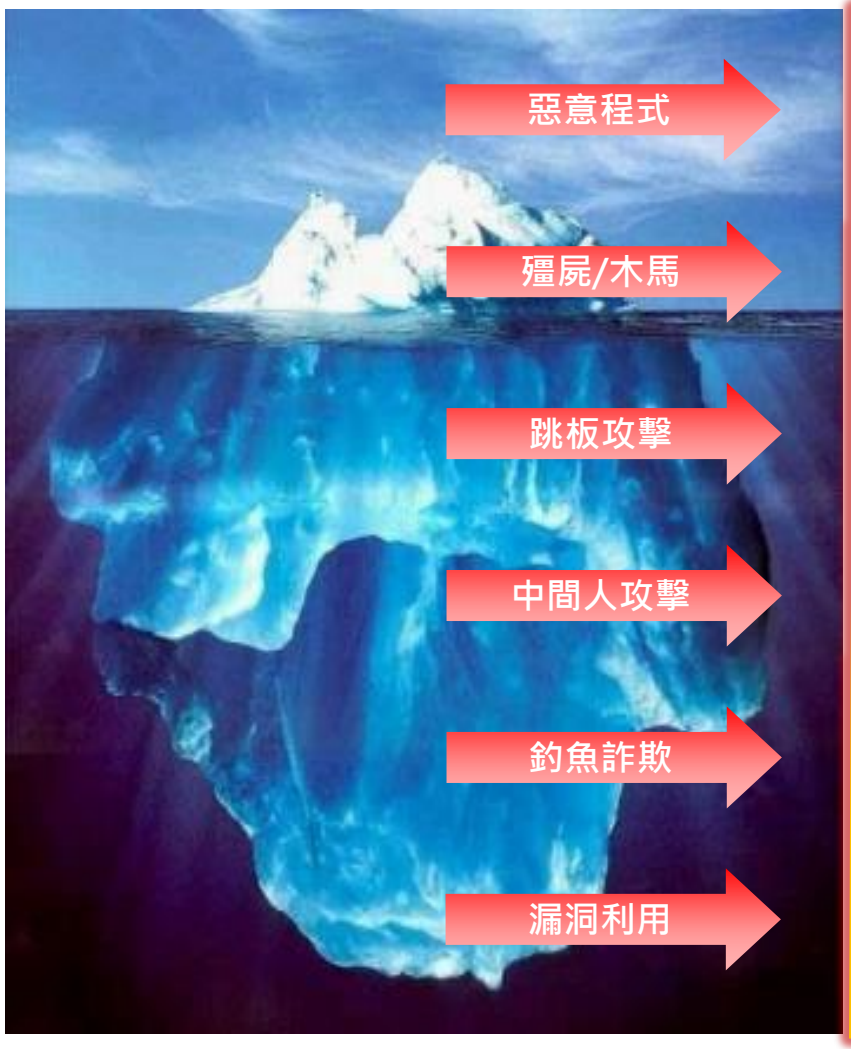
事件年份	事件主角介紹	事件影響介紹
2001	• Code Red會自行尋找並感染具IIS漏洞的電腦蠕蟲. • Nimda「瑞士萬用刀」之稱，每15秒一次的攻擊頻率，只要一台電腦未清乾淨就會蔓延再生.	• 造成26 億美元的生產力損失與伺服器清除成本
2003	• Blast 疾風病毒，自帶修正程式更新功能，高速感染	• 導致多家航空公司班機被迫延後或取消
2005	• ZOTOB蠕蟲利用MS05-039的隨插即用中的漏洞，通過TCP埠445散布.只感染未經修補的 Windows2000.	• 美國多家主要媒體包括CNN及New York Time等系統當機
2008	• Conficker惡意程式針對利用 MS08-067的安全弱點攻擊電腦系統.	• 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	• Heartbleed安全漏洞，源起OpenSSL加密的缺陷臭蟲(Bug)	• 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	• Shellshock 針對Lunix及Unix環境的資安漏洞	• 包括Liunx、Unix、Mac OS、網路設備、及任何使用Bash的網頁系統與Android等.
2015	• Angler 最成功的漏洞攻擊包，定期加入新的漏洞攻擊碼	• 勒索攻擊興起
2016	• 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.	• 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	• EternalBlue(永恆之藍)漏洞攻擊利用MS17-010微軟安全性弱點	• 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》

「弱點利用」是現今資安攻擊的主要手法



現今資安威脅: 90%利用弱點漏洞 !!



已知的攻擊威脅 (Known Knowns)	存在的漏洞 (未公布/未發現/未修補)
已知的未知威脅 (Known Unknowns)	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)
未知的攻擊威脅 (Unknown Unknowns)	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)

改變對弱點的認知

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	MS Office, LibreOffice, PDF, Apache, Zoom, and more…
網路通訊協定	SMB, DNS, SSL, RDP, SSH, 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…

弱點的共通性

- ✓ 歷史悠久
- ✓ 用戶眾多
- ✓ 使用率高
- ✓ 習以為常

Zip Slip目錄走訪漏洞

當弱點發生在「對」的位置上，災難就形成！

2014年公布至今持續延燒

當弱點發生在...作業系統

新聞

美國土安全部發布史上第三次緊急指令，要各聯邦機構限時修補Windows DNS Server的安全漏洞

美國所有以Windows Server作為DNS伺服器的聯邦機構，應於指定時限內，修補或緩解微軟針對Windows DNS重大RCE漏洞釋出的安全更新

文/ 陳曉莉 | 2020-07-17 發表

讚 6.1萬 按讚加入iThome粉絲團 讚 582 分享

CYBERSECURITY INFRASTRUCTURE SECURITY EMERGENCY COMMUNICATIONS NATIONAL RISK MANAGEMENT

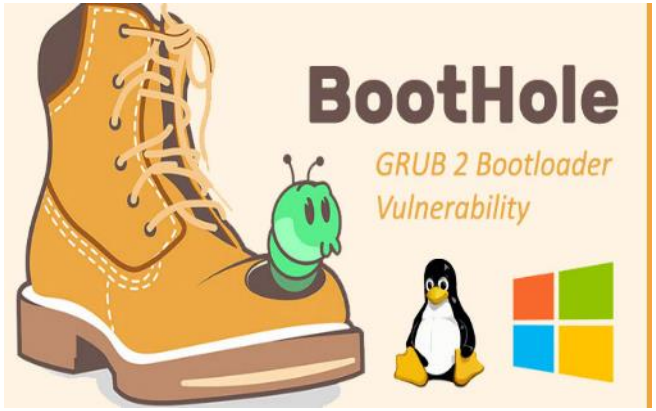
EMERGENCY DIRECTIVE (ED 20-03) WINDOWS DNS SERVER VULNERABILITY

Original release date: July 16, 2020

#SIGRed

TWCERT/CC

Linux Sudo 指令漏洞，可使受限用戶直接取得 root 權限



當弱點發生在...網路設備

新聞

修補了嗎？F5 BIG-IP重大RCE漏洞已出現攻擊程式

安全廠商NCC Group誘捕系統從7月4日起，已偵測到大量開採F5 BIG-IP高風險漏洞的攻擊行為

文/ 林妍溱 | 2020-07-07 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 209 分享

新聞

Citrix閘道系統重大漏洞已出現攻擊程式，修補程式還在路上

官方繼12月提供暫時緩解方案後，周一釋出Citrix ADC和Citrix Gateway 11.1及12.0的更新版本，針對其他受影響產品的第二波修補，預計本周五釋出

文/ 林妍溱 | 2020-01-21 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 0 分享

新聞

思科私有協定CDP遭爆含有5個零時差漏洞，危及數千萬裝置

CDP為思科私有的資料連結層（Layer 2）網路協定，主要用來發現本地端的思科設備資訊，以用來對照該網路上的思科產品，被應用在交換器、路由器、IP Phone與IP Cameras等思科裝置上，這些產品若缺乏CDP便無法正常運作

文/ 陳曉莉 | 2020-02-07 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 534 分享

新聞

HP電腦使用8年的技術支援軟體含有多項安全漏洞，即使新版也仍有漏洞未補完

研究人員發現，內建於HP Windows電腦的HP Support Assistant含有多項漏洞，雖然HP已經著手處理，但最新版軟體仍有漏洞未補完

文/ 林妍溱 | 2020-04-06 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 223 分享

Netgear 部份
路由器產品新發現
多個嚴重資安漏洞

TWCERT/CC

當弱點發生在...資安設備

新聞

駭客正在開採思科的CVE-2020-3452安全軟體漏洞

思科上周修補存在於Adaptive Security Appliance（ASA）與Firepower Threat Defense（FTD）軟體的安全漏洞，目前已出現攻擊程式與實際的開採行動

文/ 陳曉莉 | 2020-07-28 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 119 分享

新聞

部份Fortinet產品加密金鑰漏洞，可讓駭客竊聽用戶活動

安全研究人員發現Fortinet防火牆產品FortiGate及端點安全產品Forticlient，因程式撰寫問題導致加密金鑰曝露，可能讓駭客得以攔截用戶資料，或是操控、弱化FortiGuard雲端服務防護能力，Fortinet目前已釋出修補程式

文/ 林妍溱 | 2019-11-26 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 724 分享

新聞

Juniper修補防火牆、路由器可能導致DoS的漏洞

Juniper作業系統軟體Junos OS含有三項安全漏洞，可能導致阻斷服務（DoS）攻擊，業者提醒用戶更新至最新版本以完成修補

文/ 林妍溱 | 2020-07-13 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 133

新聞

Palo Alto Networks修補其防火牆作業系統的重大安全漏洞

美國軍方針對Palo Alto Networks防火牆作業系統PAN-OS的CVE-2020-2021漏洞發出警告，表示這是個容易遭國外駭客覬覦的漏洞，因為開採難度低，卻可能危及組織機密與健全

新聞

駭客企圖開採已修補的Sophos防火牆漏洞來散布勒索軟體

Sophos在4月底修補XG Firewall漏洞後，駭客隨即改變攻擊策略，企圖透過相同漏洞來散布勒索軟體，該公司再度呼籲用戶確認是否完成修補

當弱點發生在...資安系統

新聞

小心了，新版Thanos勒索軟體服務採用了可繞過大多數防毒軟體的RIPlace技術

去年11月揭露的RIPlace攻擊技術，能讓勒索軟體靠開採Windows作業系統的設計漏洞，來破壞受駭單位的原始檔案，當時尚未發現有勒索軟體採用該技術，不過，近期新版Thanos勒索軟體已加入RIPlace技術，即使號稱可偵測勒索軟體的十多種防毒工具，也無法識破其攻擊行動

勒索軟體即服務

文/ 陳曉莉 | 2020-06-15 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 887 分享

TWCERT/CC

Windows Defender Applicaton Control

安控機制可被跳過的漏洞

新聞

研究人員公布IBM企業安全工具的零時差漏洞

IBM開發的企業安全軟體Data Risk Manager（IDRM），被揭露含有4項安全漏洞，研究人員表示，IDRM遭駭可能危害整個企業，因為它不僅存放各種安全工具的憑證，也含有系統的漏洞資訊

文/ 陳曉莉 | 2020-04-22 發表

讚 6.1 萬 按讚加入iThome粉絲團

Multiple Vulnerabilities in IBM Data Risk Manager

新聞

賽門鐵克企業防毒出現能讓駭客任意竄改檔案的漏洞 Accenture揭露相關細節

IT顧問公司Accenture最近針對一個在1月初，發現的賽門鐵克企業版防毒（Symantec Endpoint Protection，SEP）用戶端軟體漏洞，揭露相關細節，並且展示概念性驗證攻擊，呼籲使用者儘速修補

文/ 周峻佑 | 2020-07-14 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 7 分享

當弱點發生在...聯網系統

TWCERT/CC

國內門禁設備商修復產品資安漏洞，請立即更新韌體

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/ 黃彥棻 | 2019-07-24 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 1,473 分享

新聞

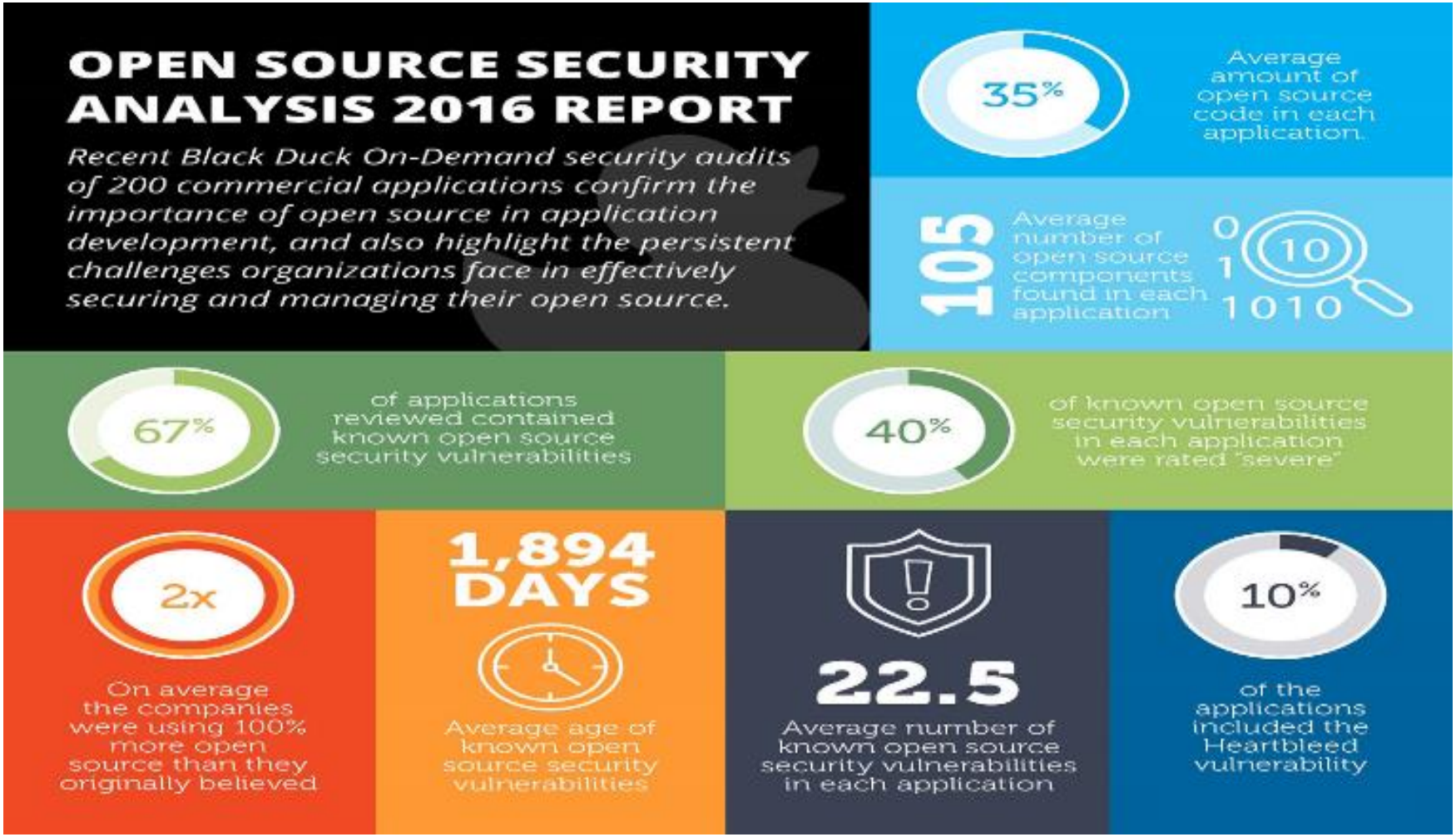
QNAP軟體有RCE漏洞，波及數十萬臺NAS硬體

漏洞出現在QNAP Photo Station及一些CGI程式中，受影響的Photo Station版本包括6.0.3、5.2.11和5.4.9版，QNAP去年底完成修補

文/ 林妍溱 | 2020-05-21 發表

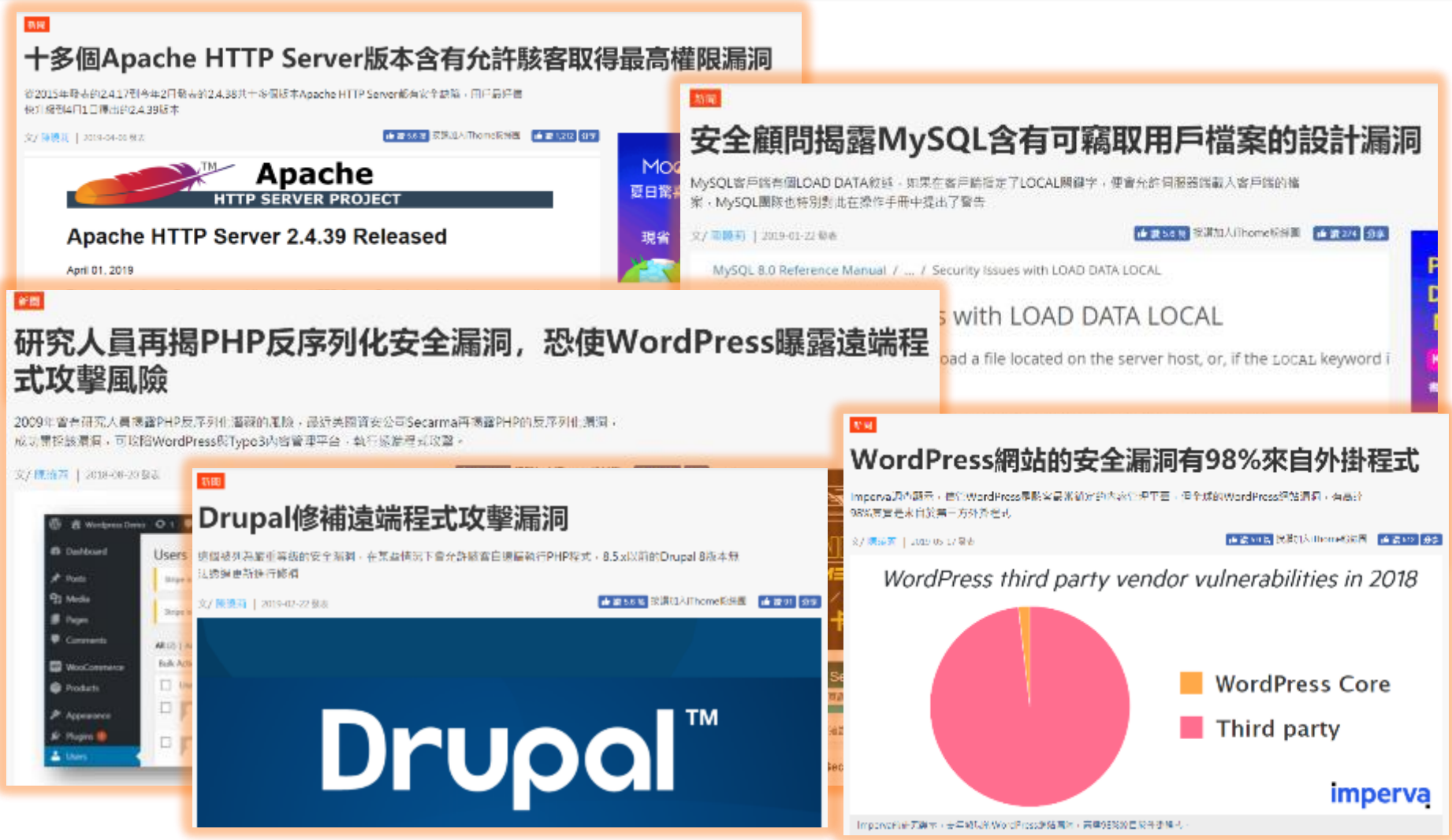
讚 6.1 萬 按讚加入iThome粉絲團 讚 630 分享

開源軟體(Open Source)也是安全隱憂



資料來源: Black Duck Software

“開源”不等於 節流 ·



“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

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

MySQL、Jenkins是漏洞最多的兩個開源碼專案

RiskSense追蹤54個主要開源專案從2015年至今公開的CVE漏洞代碼，發現過去3年來的漏洞數量，呈現逐年倍增的趨勢

文/ 林妍溱 | 2020-06-10 發表

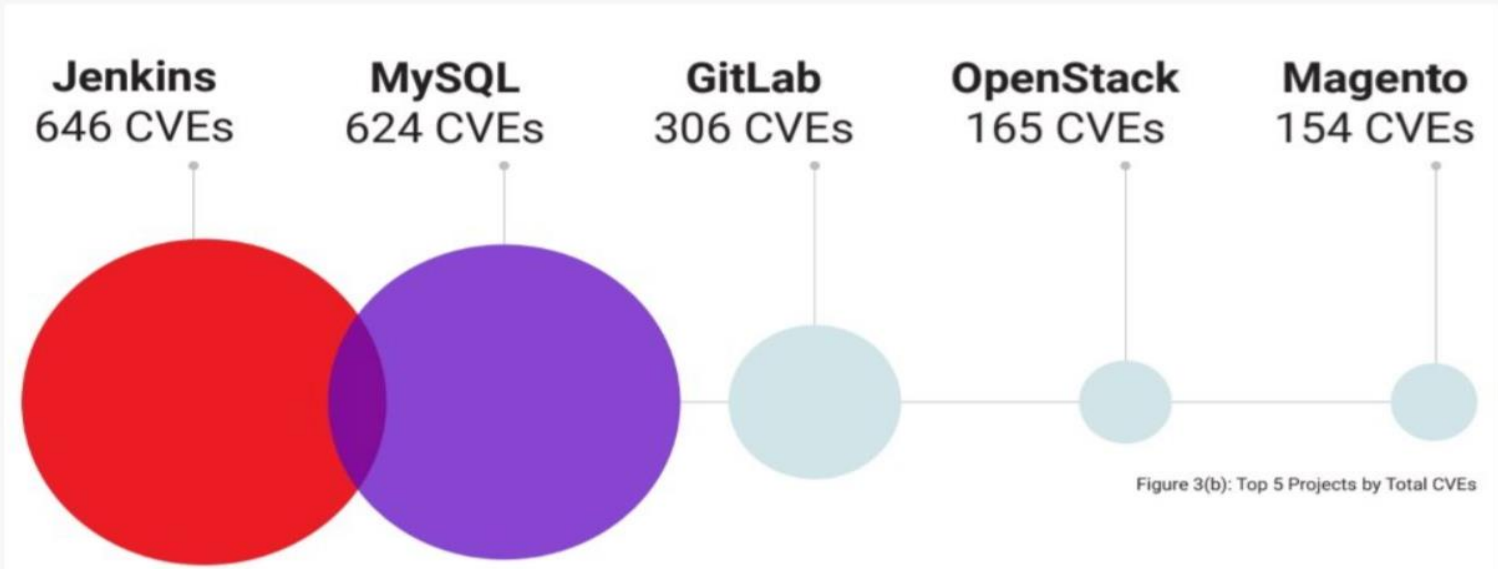
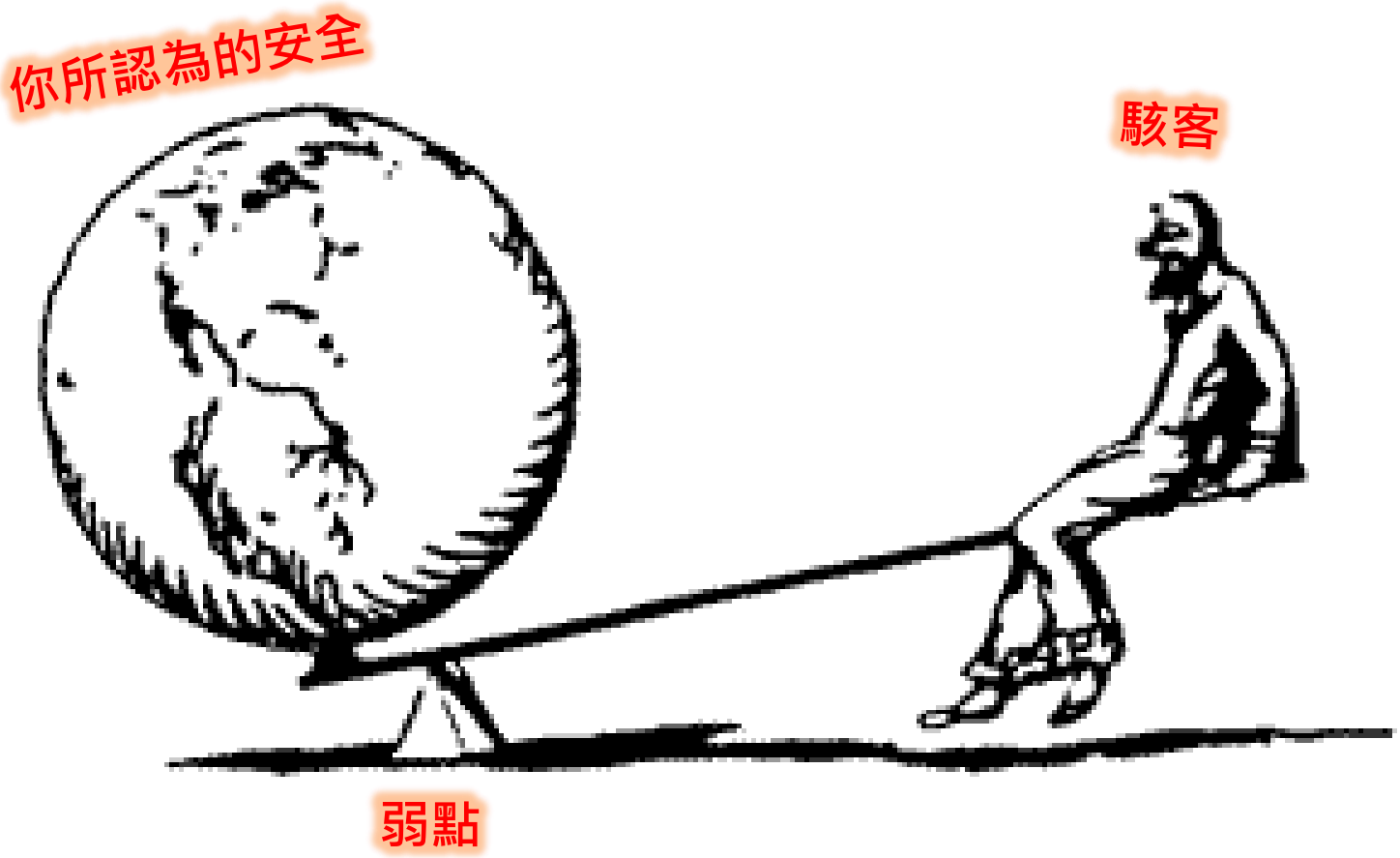


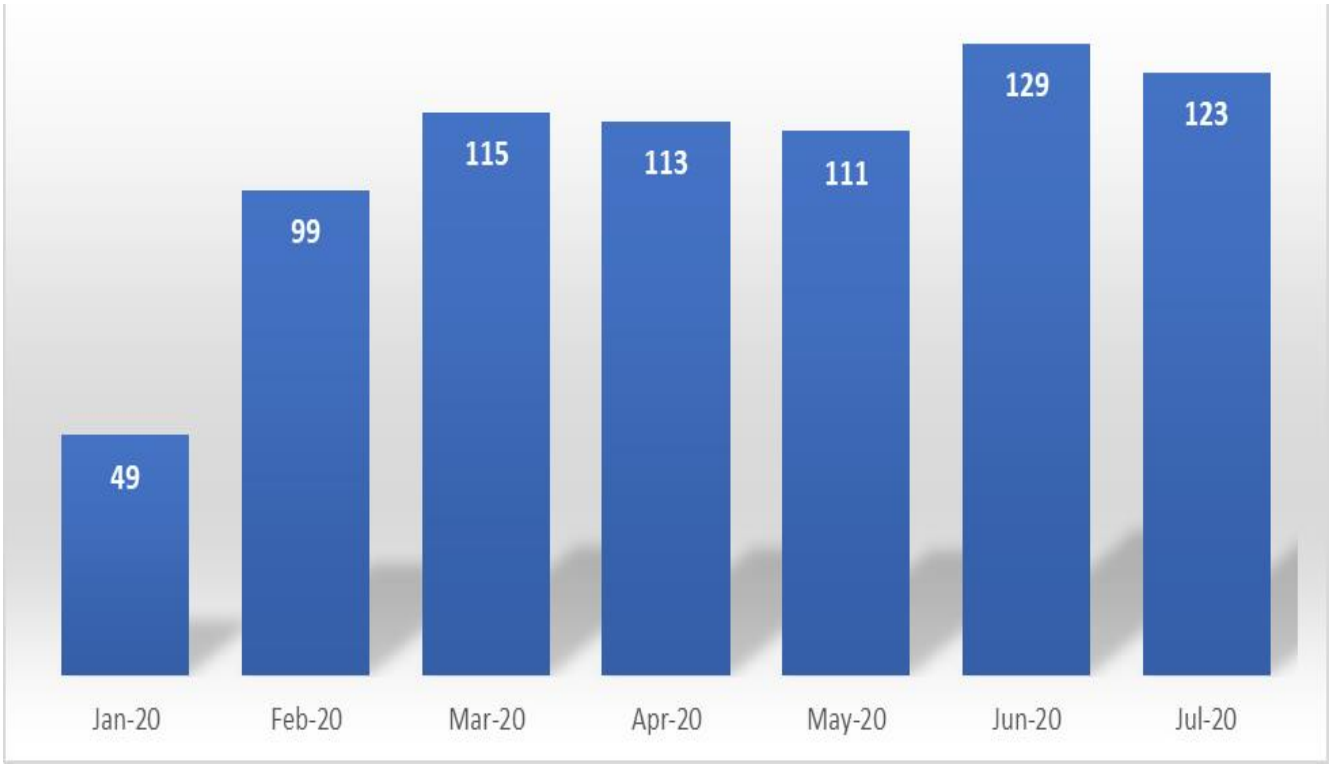
Figure 3(b): Top 5 Projects by Total CVEs

RiskSense檢視54項主要的開源專案，從2015年到2020年3月底的公開CVE漏洞代碼，專案含有漏洞數量最多的前二大，是持續整合工具Jenkins（646項漏洞），以及資料庫軟體MySQL（624項漏洞）。（Photo by RiskSense）

安全脆弱度，只需要一個正確的點



弱點正不斷的產生中



弱點造成信任鏈破壞 (Broken Trust Chain)

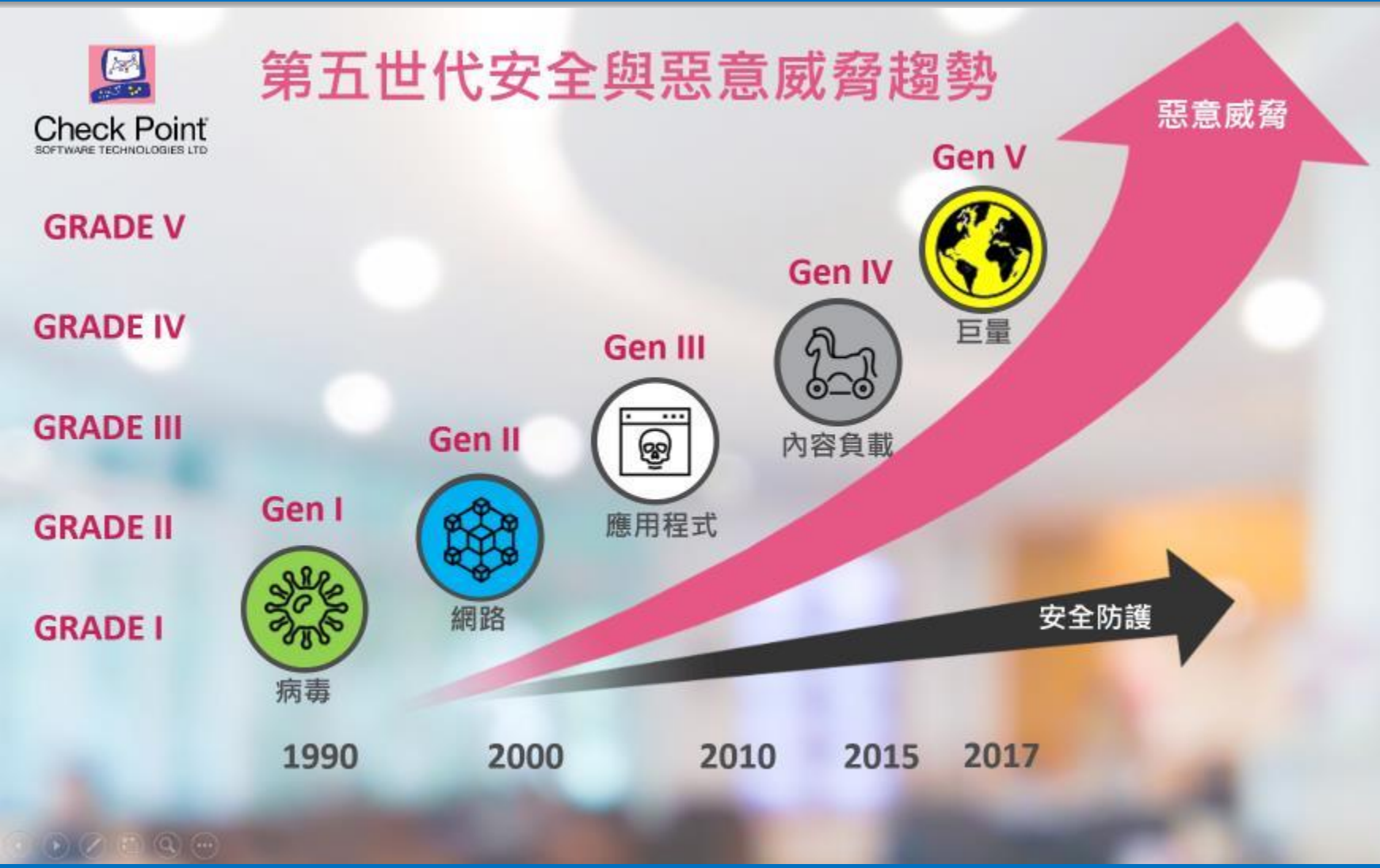
零信任 (Zero Trust)

零信任=別倚賴信任
勤快主動的發現弱點

大綱簡介

- 前言
- 為什麼一定要掃描弱點
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

不同世代的安全威脅演進



不同世代威脅與安全防護對照

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

Gen V

巨量

- 立即防禦威脅(不單僅是偵測威脅)
- 可即時反應與迅速回覆
- 全面防堵所有安全突破口:
  雲、端點、網路、行動裝置

安裝防毒軟體 不等於 做好資安防護

iThome 新聞 產品評測 技術 專題 AI & Big Data Cloud DevOps GDPR 資安 研討會

賽門鐵克疾呼防毒軟體已死

知名防毒軟體廠商賽門鐵克資深副總裁Brian Dye接受華爾街日報採訪時表示，80年代所發展出來的惡意軟體解決方案，現今已不再有效，惡意軟體攔截率僅剩45%，防毒軟體將不再是業者的搖錢樹

文/ 李建興 | 2014-05-21 發表

讚 4.9 萬 按讚加入iThome粉絲團 讚 0 分享 G+

防毒軟體

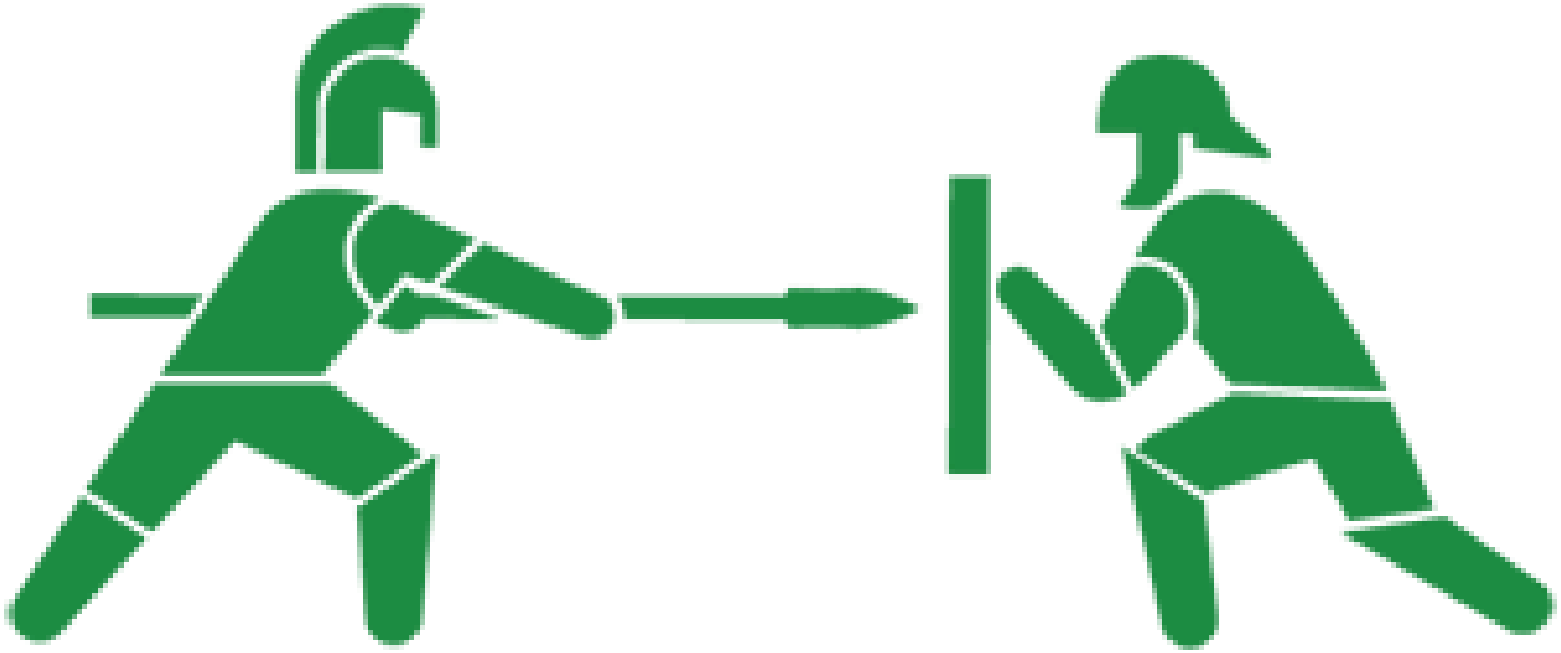
病毒特徵

入侵防護
(FW/IPS/NGFW)

- **防惡意程式**
  - **進階威脅防護**
    - 機器學習
    - 漏洞威脅防護
  - **次世代防毒**
    (NGAV/EDR)
- **防木馬程式**
- **防勒索軟體**

弱點掃瞄與滲透測試之間...?

對抗? 演練?

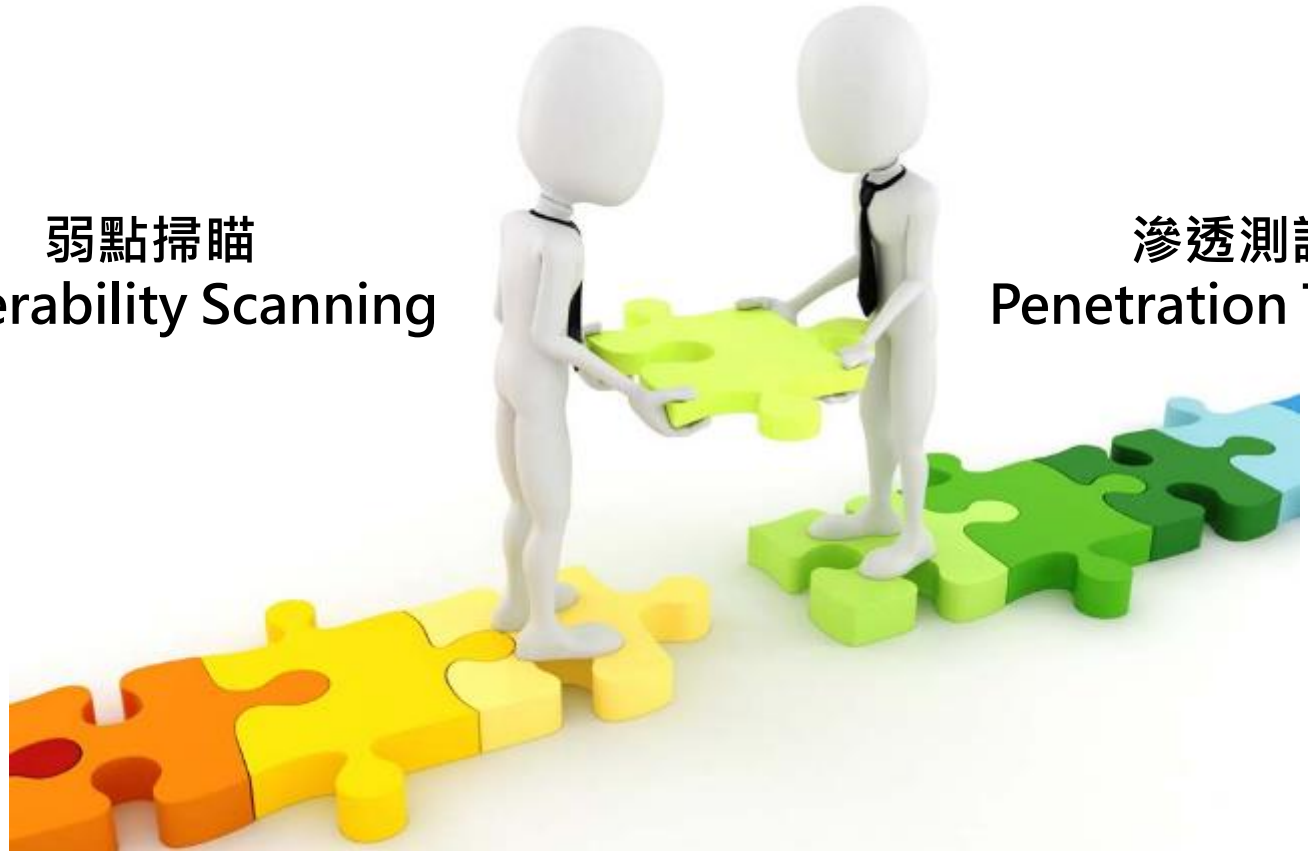


弱點掃瞄與滲透測試 是相互合作搭配

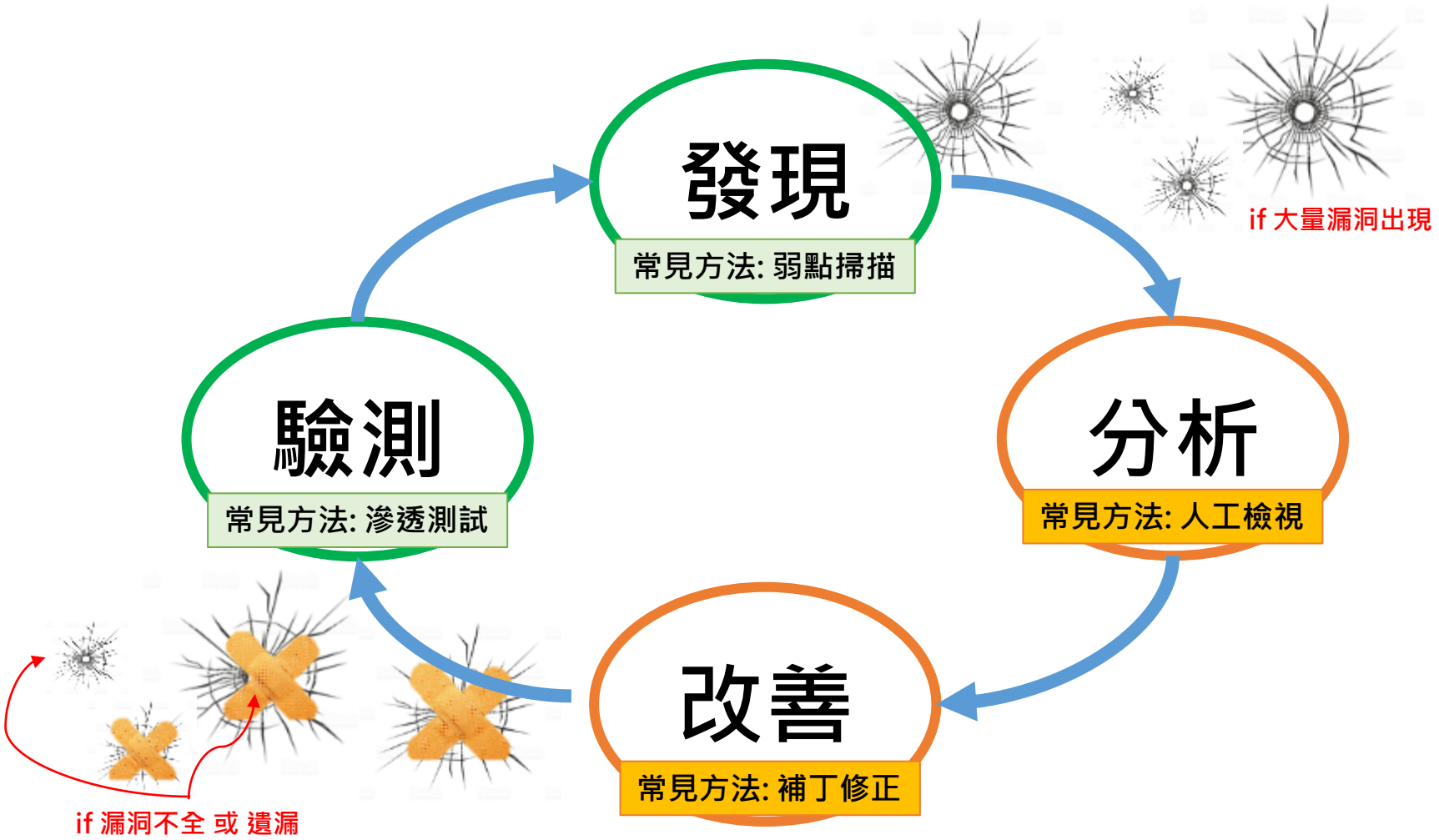
目的相同 的 不同檢驗方式.

弱點掃瞄
Vulnerability Scanning

滲透測試
Penetration Testing



弱點掃瞄與滲透測試 是相互合作搭配



建立高效率的弱點安全管理

5 Best Practices for Building an Effective Vulnerability Management

資料來源 https://www.acacompliancegroup.com/blog/5-best-practices-building-effective-vulnerability-management-program

從資安怎麼看待「弱點(漏洞)」

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 Configuratior
  - 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

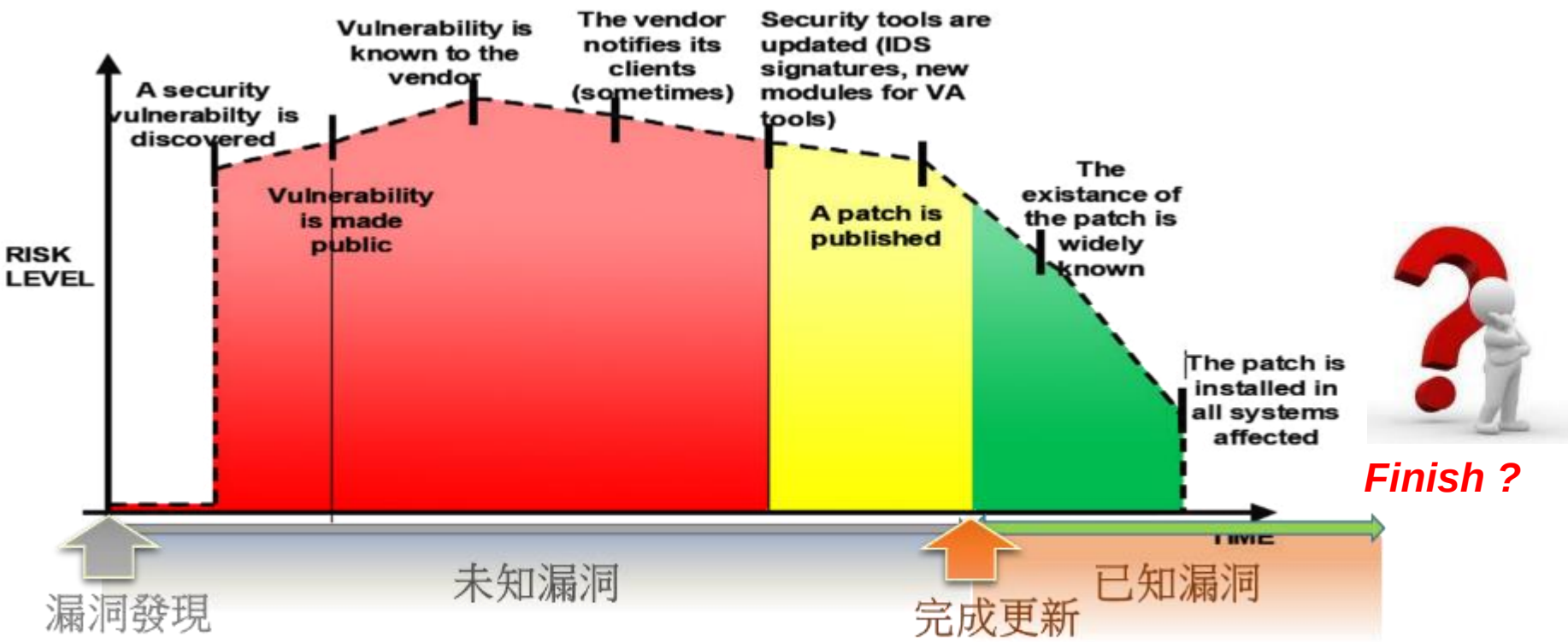
Share

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)。

Zero-Day Attack 零日攻擊威脅

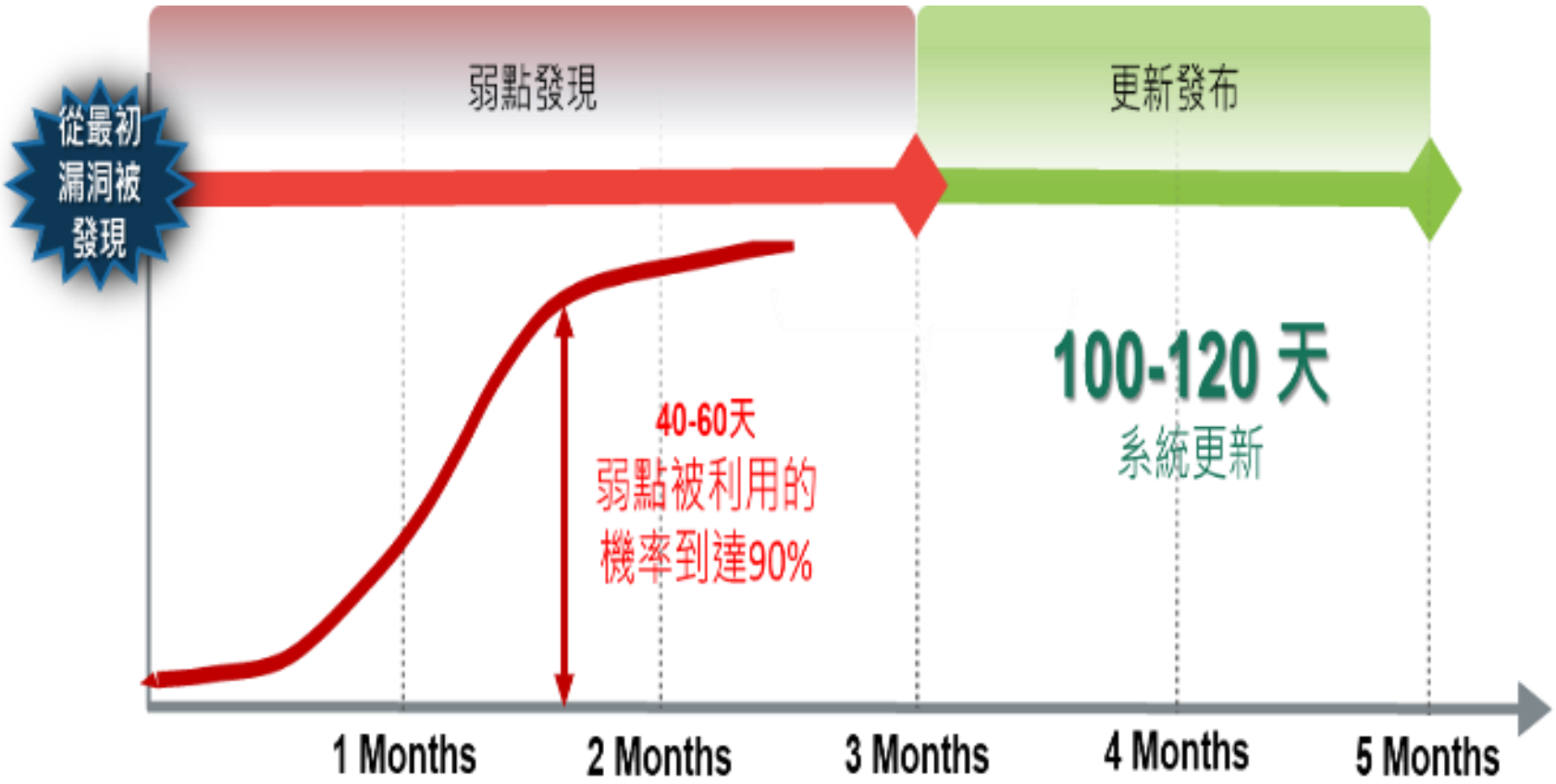
Window of Vulnerability



Finish ?

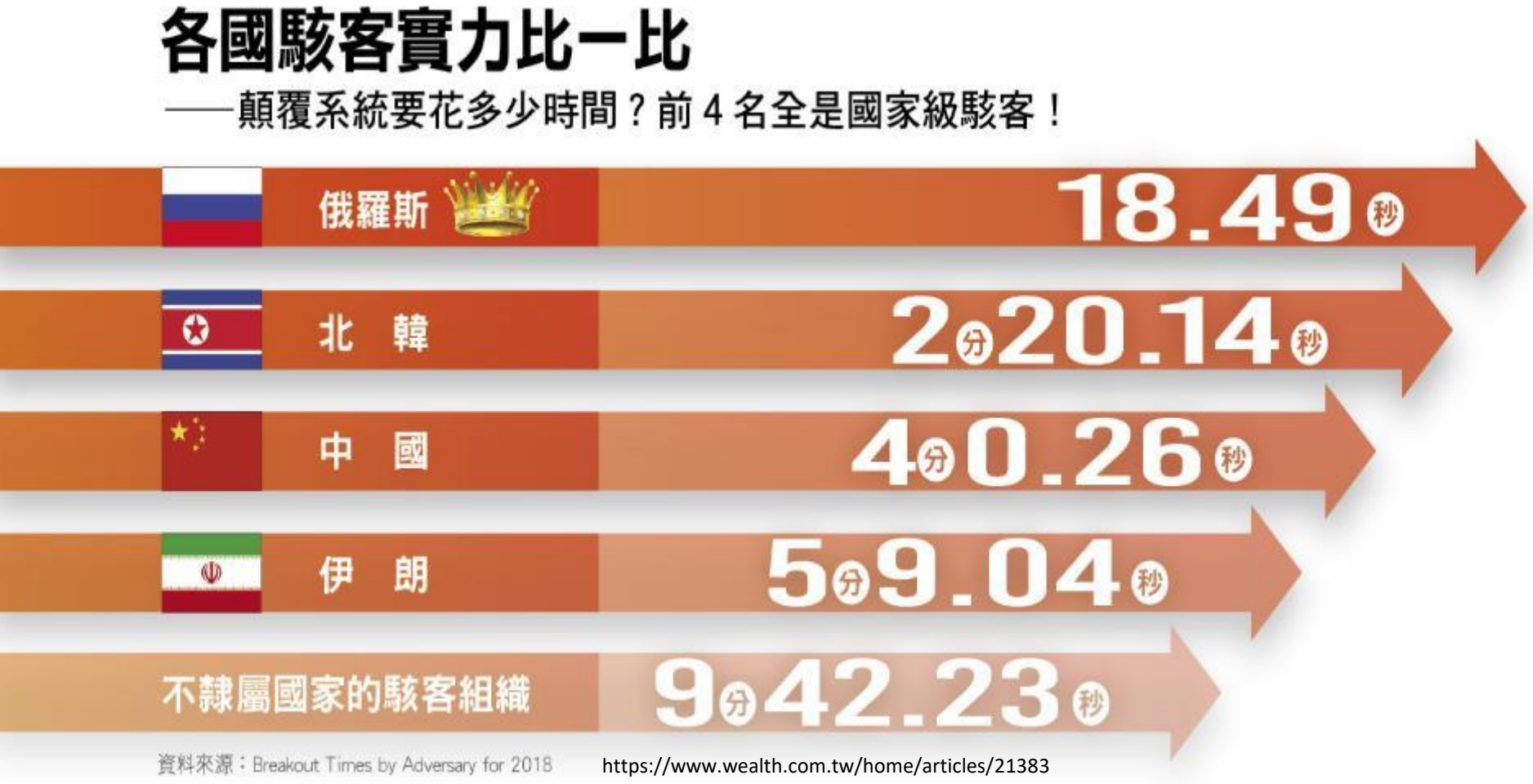
資料來源: https://www.owasp.org/index.php/Testing_Guide_Introduction

從漏洞揭露開始，攻擊威脅就存在



Source: https://www.infosecurity-magazine.com/news/companies-average-120-days-patch/

駭客競速比賽

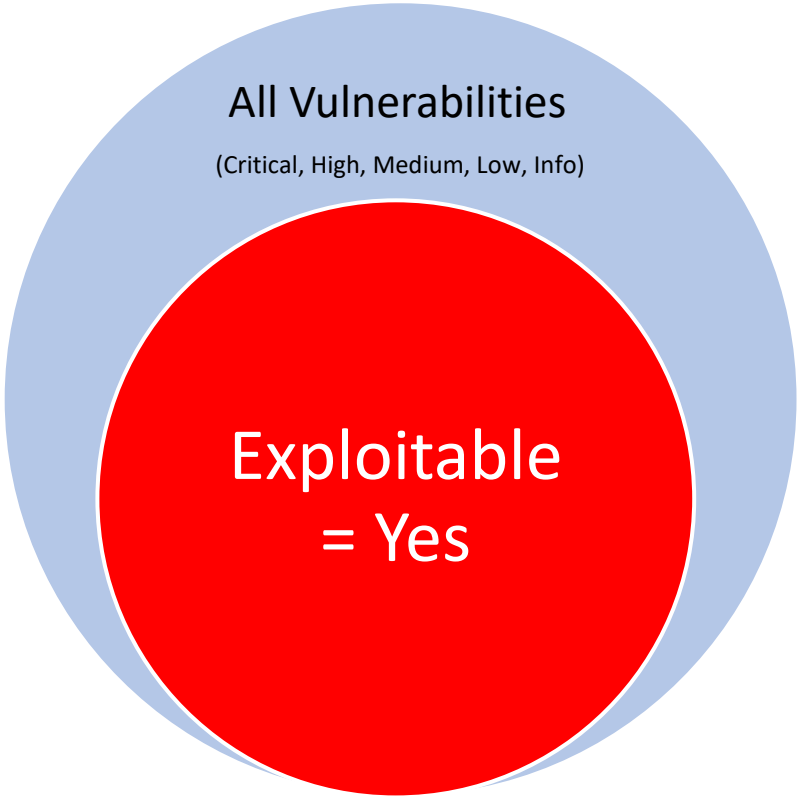


https://www.wealth.com.tw/home/articles/21383

弱點漏洞的利用「Exploitable」

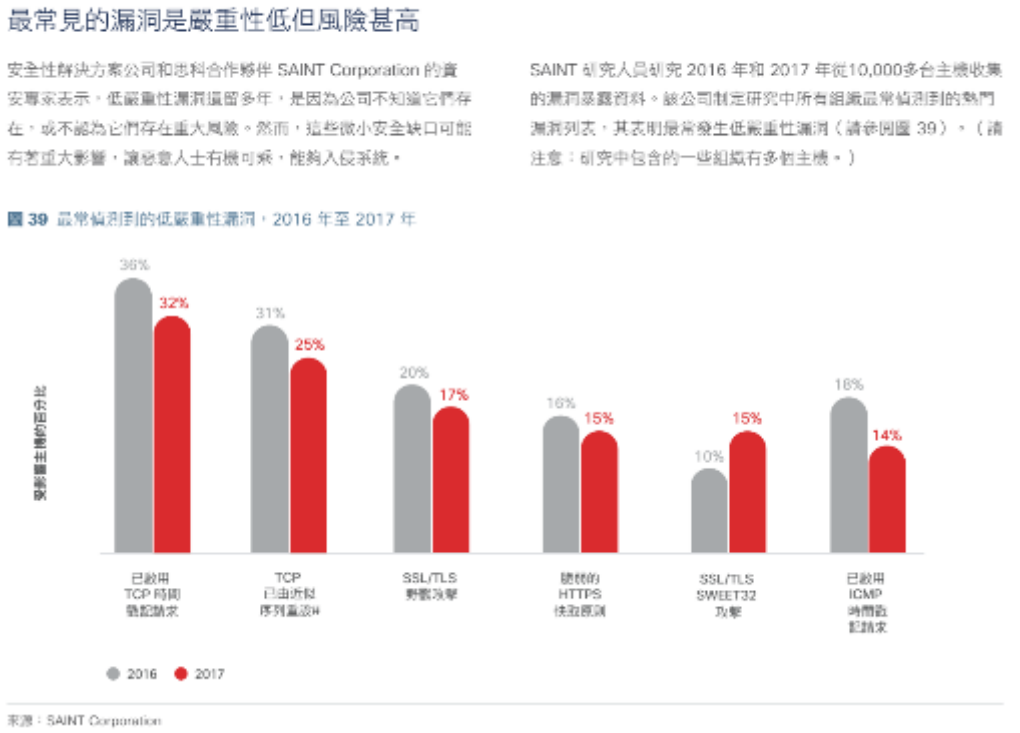
漏洞弱點不一定是絕對&立即威脅，必須搭配適當的條件才能被利用。

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)。



cisco

2018年度網路安全報告



「滲透測試」是弱點檢測的衍伸

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。

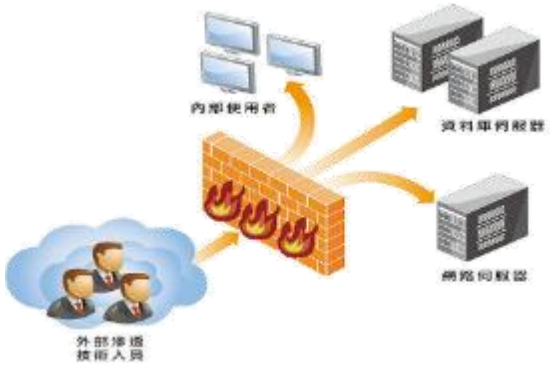
白箱測試 vs. 黑箱測試 的優缺差異

以Web系統為例:

	優點	缺點
白箱測試	1.弱點偵測正確率高 2.提供較適當修正建議	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	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	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

滲透測試的入門之法

- 滲透測試技術≠駭客養成
- 駭客技術也不會像駭客任務的技能下載

- 知識: Domain Knowledge, Know-how
- 技術: 技術, 技巧, 工具
- 經驗: 新聞資訊, LAB實做, 實戰
- 想像力與好奇心

學習資訊參考

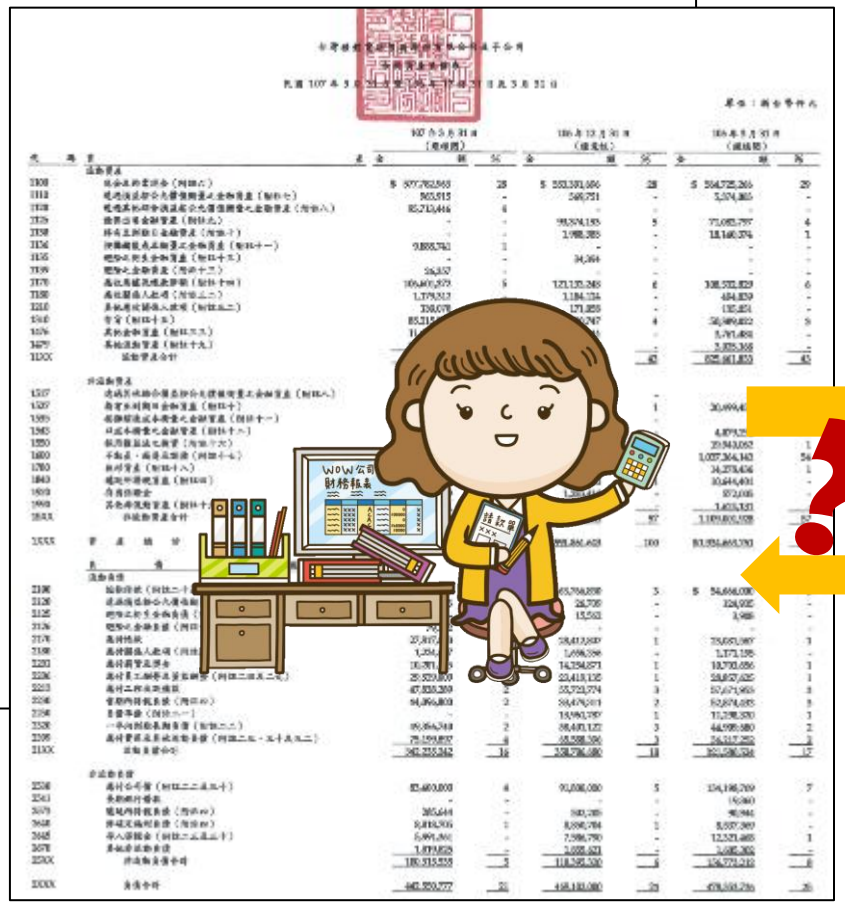
https://www.kali.org/

大綱簡介

- 前言
- 為什麼一定要掃描弱點
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

「看報告」是門學問

財務報告



醫療檢查報告

腫瘤篩檢 Tumor Markers

人類絨毛膜素【男】B-HCG	<1.2	mIU/ml	≤

放射線檢查 Radiology Examination

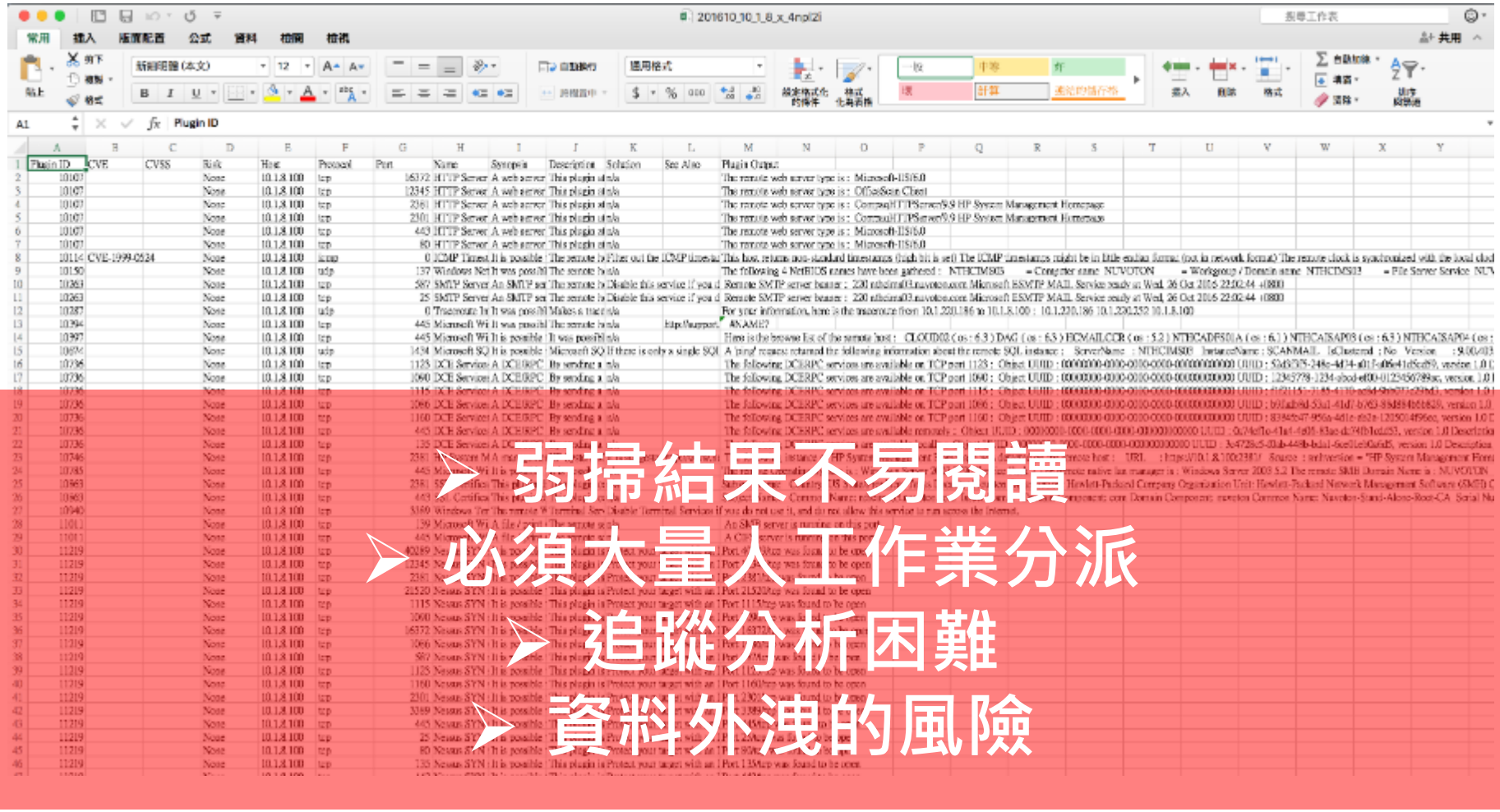
胸部正面1張 Chest X-ray	無異狀		
腰椎骨質密度檢查之平均骨密度 BMD	0.838	(g/CM2)	
腰椎骨質密度檢查之骨密度百分比 BMD	87	(%)	
腰椎骨質密度檢查之結論 BMD	骨質流失(T-score：-1.1)		>=-1.0
右髖骨骨質密度檢查之平均骨密度 BMD	0.85	(g/CM2)	
右髖骨骨質密度檢查之骨密度百分比	91		
右髖骨骨質密度檢查之結論 BMD	正常(T-score：-0.6)		>=-1.0

十二導程心電圖檢查 12-lead

	正常參考	5/29	第	6/24
C	4~10 10	11.6	二	7.5
BC	4.5~5.9	3.53	次	4.09
Platelet	150~440	359	入	296
Hgb	14~18 g/d	11.2	院	13.1
	7~20 mg/d	19		12
	0.7~1.5 mg/d	1.1		1.13
CK	≤171 U/L			
CK-MB	≤16.0 U/L	97		
C.R.P	≤3.0 mg/L	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	
APTT	23.9~34.9	27.5	32.0	37.4

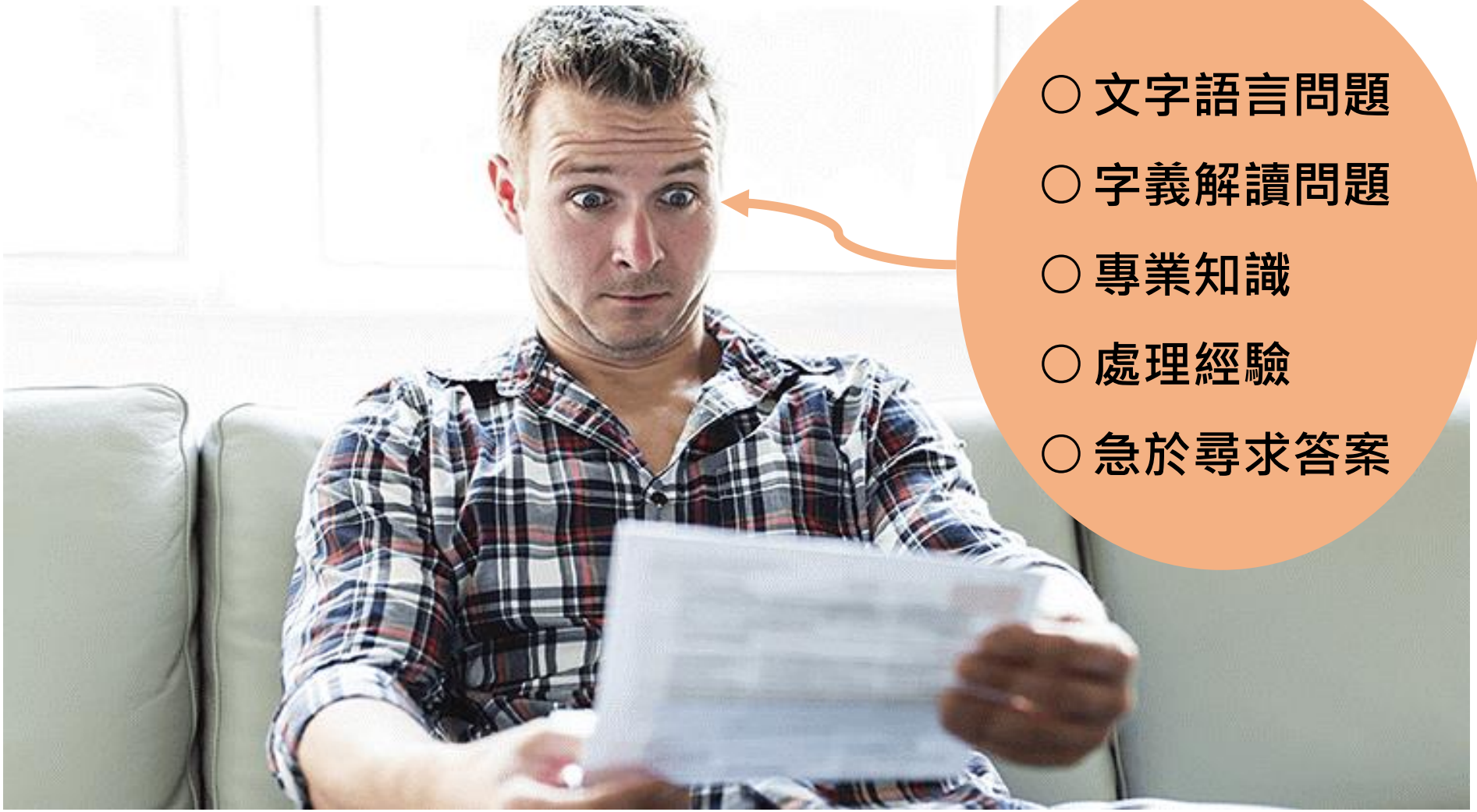
備註：紅色字體代表檢查數值異常

看弱掃報告令人厭世

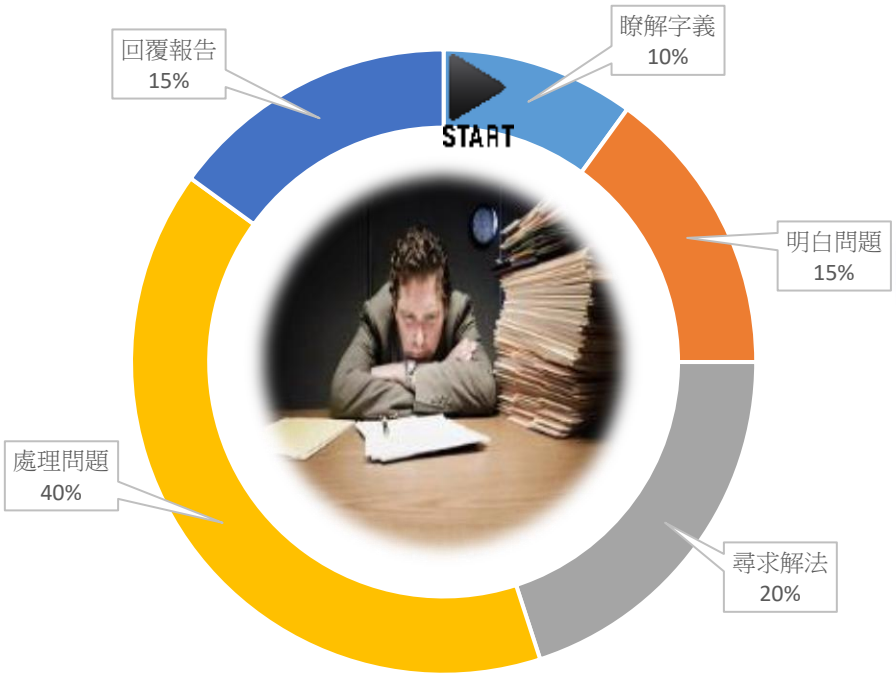


- 弱掃結果不易閱讀
- 必須大量人工作業分派
- 追蹤分析困難
- 資料外洩的風險

天呀... 弱掃報告又來了.



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

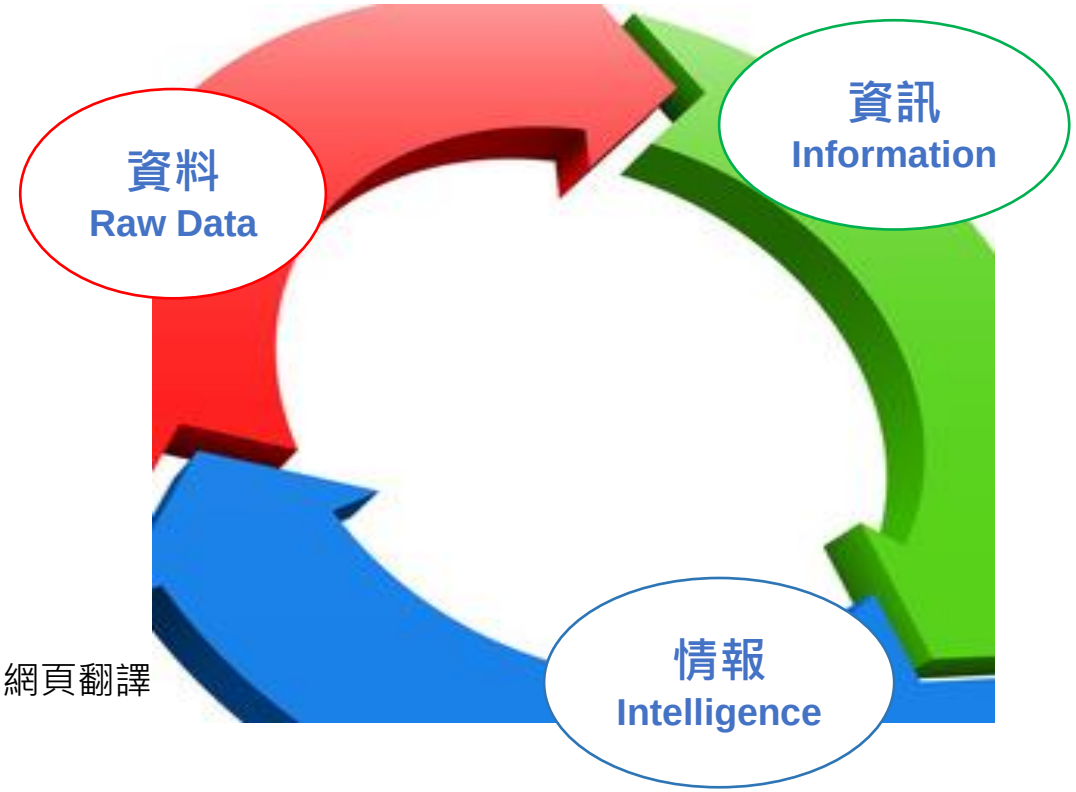
減少
弱點曝光
(風險空窗期)

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

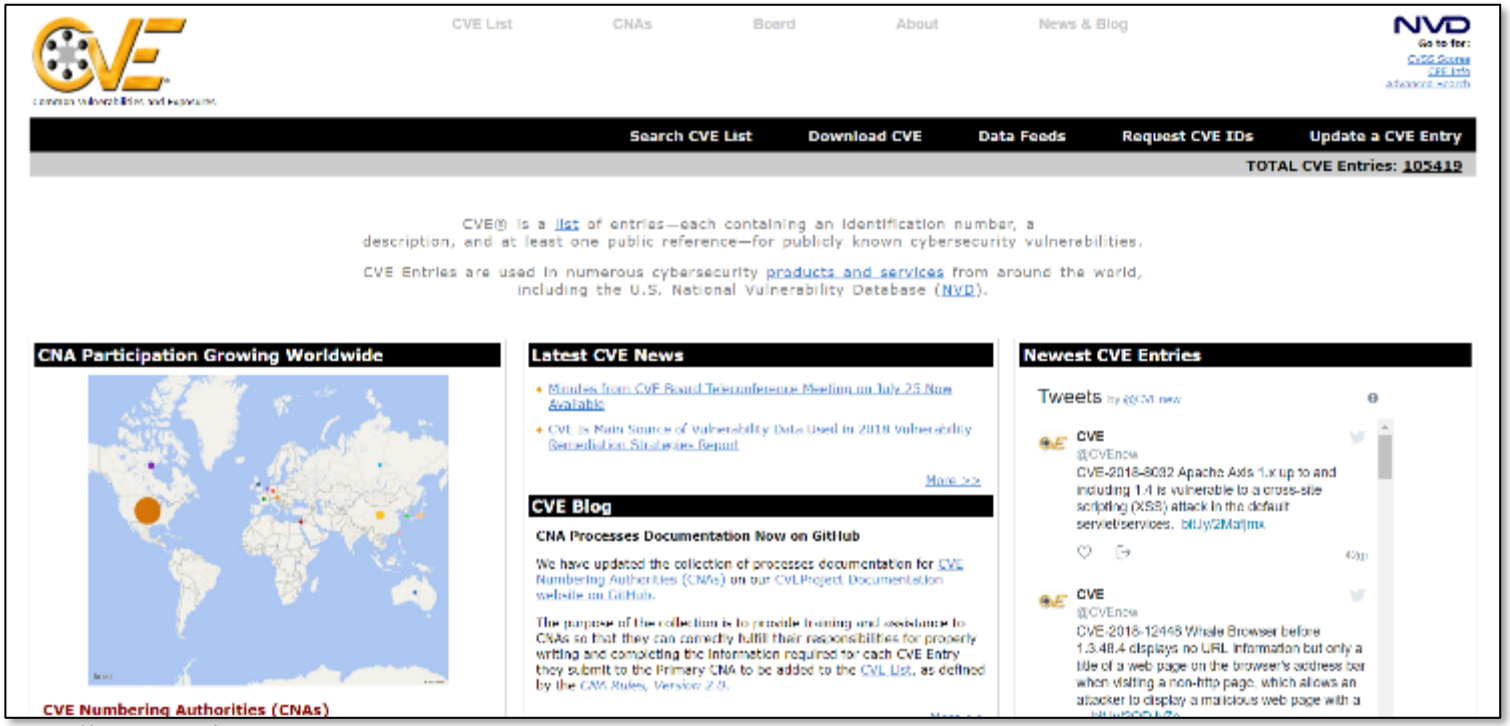


- **相關資源的幫助**
  - 翻譯工具, 例: Google Chrome 網頁翻譯
  - 搜尋工具, 例: Google Search
  - 弱點相關資訊網站, 例: CVE Details, Vuldb, Exploit-db, Tenable 等
  - 資安訊息相關網站, 例: iThome security, TW-CERT, TACERT 等

CVE (通用弱點披露)

Common Vulnerabilities and Exposures

- 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.



https://cve.mitre.org/

CVE 的注意事項

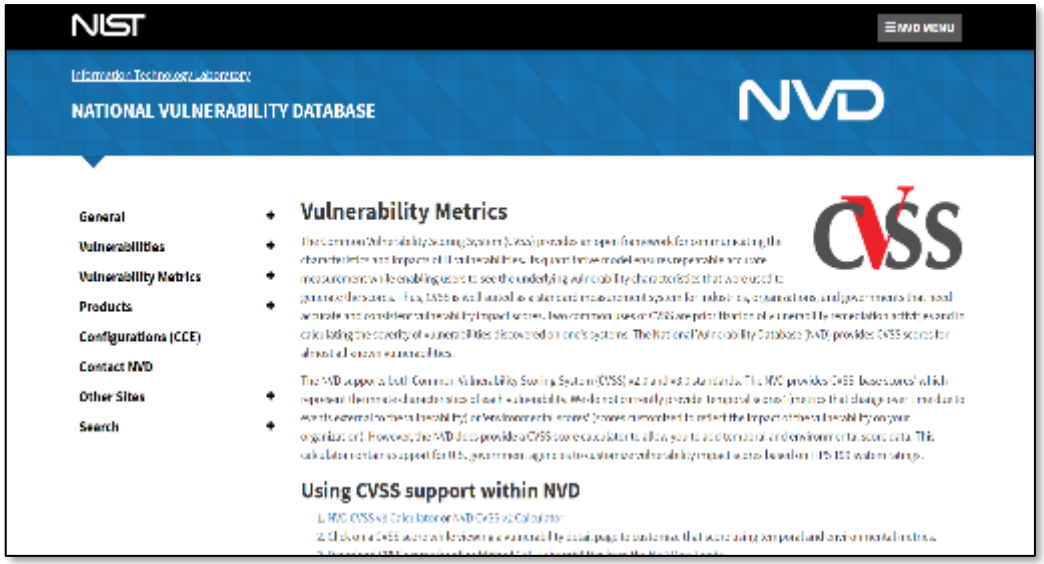
- CVE不是唯一的弱點資料來源! (其他組織或製造商公佈, 例: 微軟MS)
- 多數的弱掃工具 是依據CVE公佈弱點資訊，建立掃描檢測方式，但各家的方法不盡相同.
- 掃描發現的弱點不一定具有CVE編號! (可能已發現存在攻擊威脅但尚未完成驗證階段，亦可視為「未知威脅Unknow Threat」).
- 發現的弱點並須經過CVE組織確認驗證程序後，才會給予CVE編號.
- 零日漏洞(Zero-day exploit 或 0-Day) 通常指「還沒有修補程式方法的漏洞」.
- 同一弱點威脅可能具備有多個CVE，需視修補建議方式評估達成.

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)

Common Vulnerability Scoring System



https://nvd.nist.gov/vuln-metrics/cvss

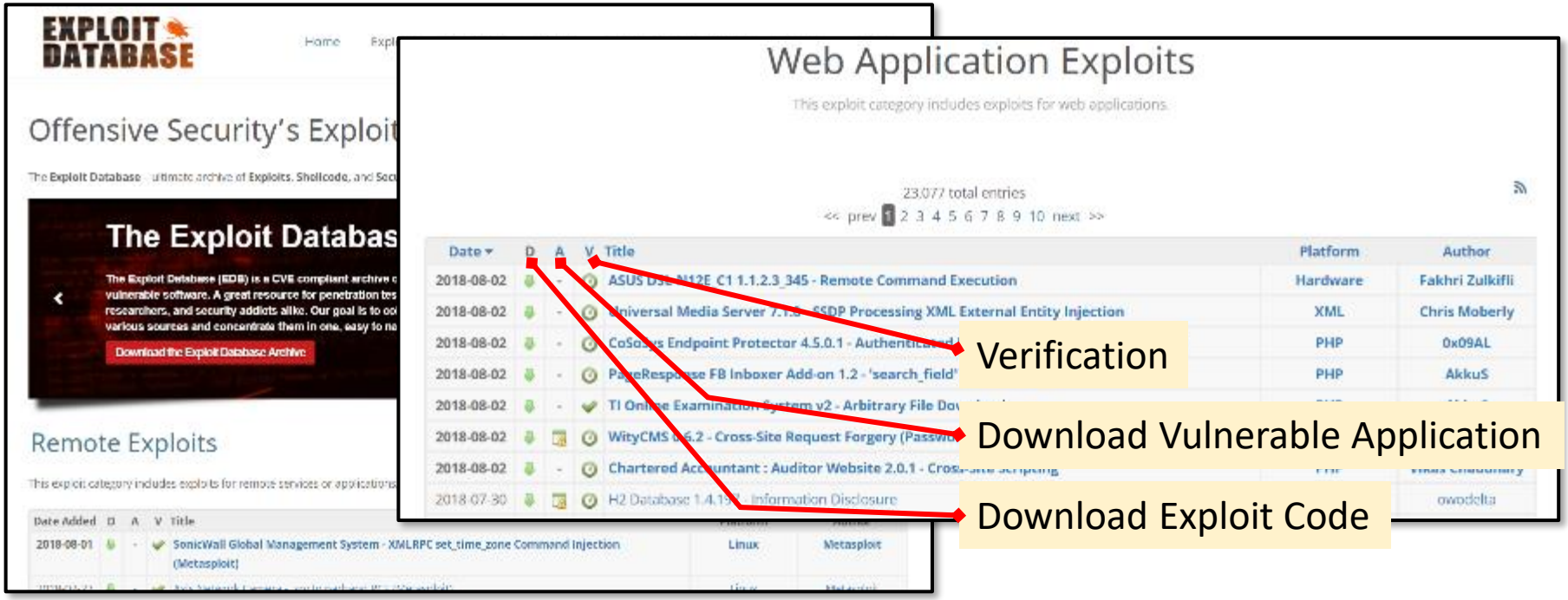
NVD Vulnerability Severity Ratings

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

- 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。
- 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.



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

https://www.cvedetails.com/

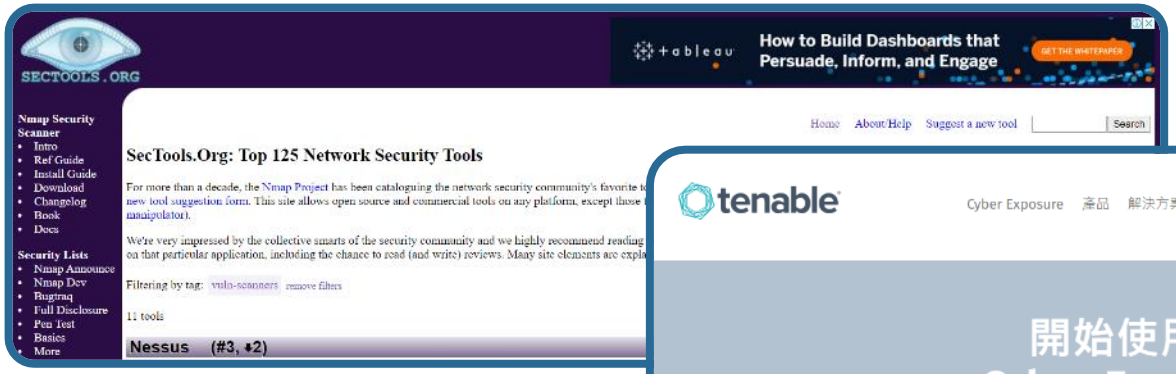
https://vuldb.com/?

https://www.tenable.com/plugins

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

弱點工具參考資源

NMAP https://sectools.org/tag/vuln-scanners/



Tenable https://zh-tw.tenable.com/try

ZAP https://www.zaproxy.org/

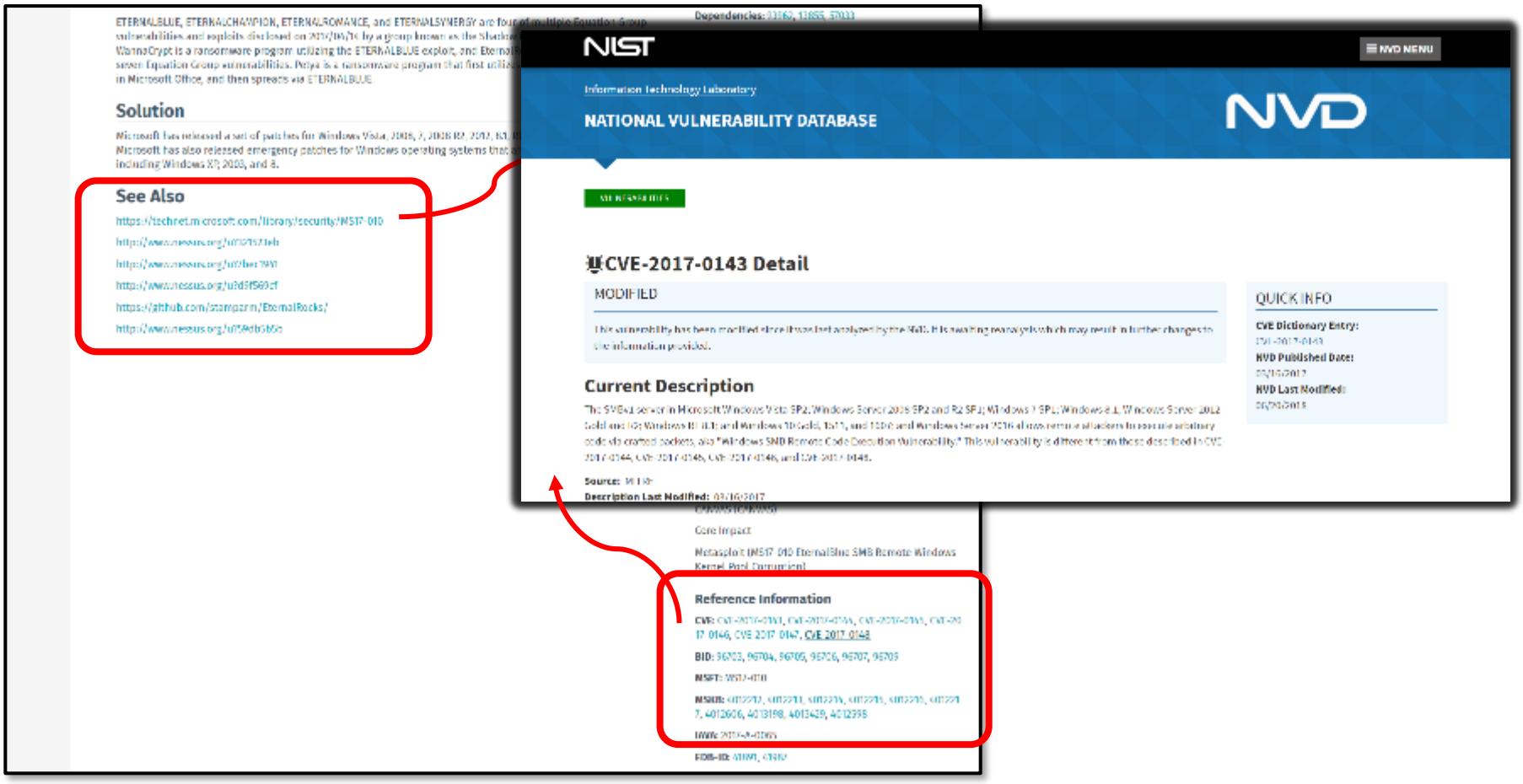
善用網路資源查找資安資訊

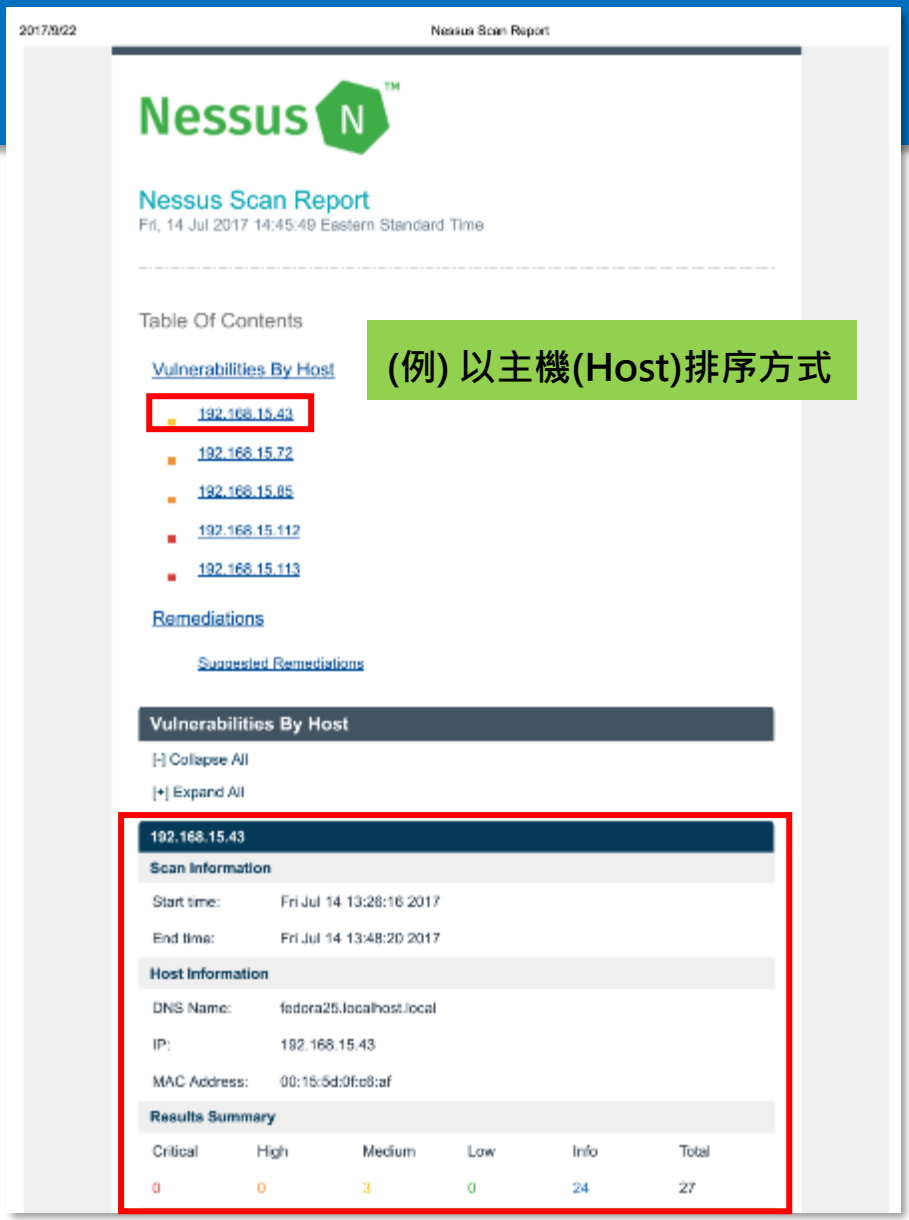
- 國內主要IT資安媒體

- 全球主要的搜尋引擎

善用工具(1) Google 網頁翻譯

善用工具(2) 商業弱掃廠商的資訊資源



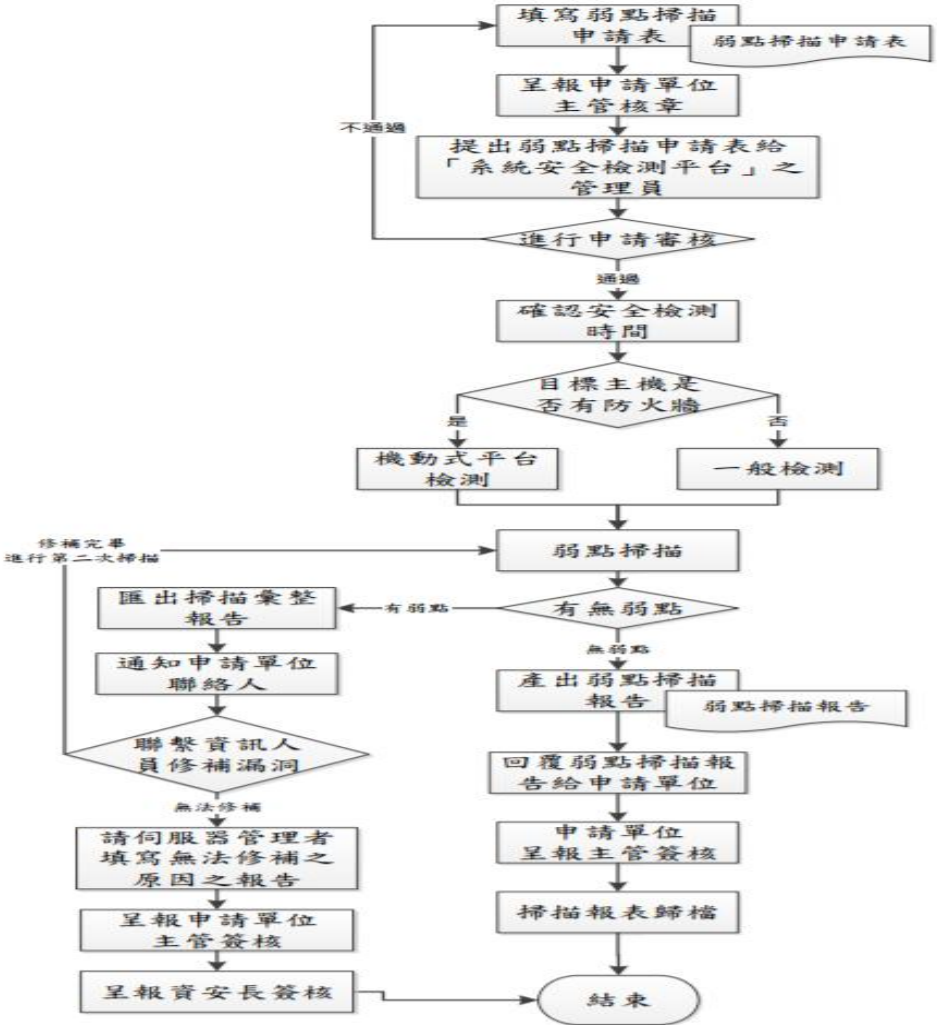


報告範本(高階)

大綱簡介

- 前言
- 為什麼一定要掃描弱點
- 防毒軟體、弱點掃描、滲透測試的差異性
- 我收到了弱掃報告，可是看不懂
- 怎樣找到最合適自己的弱掃工具
- Q&A

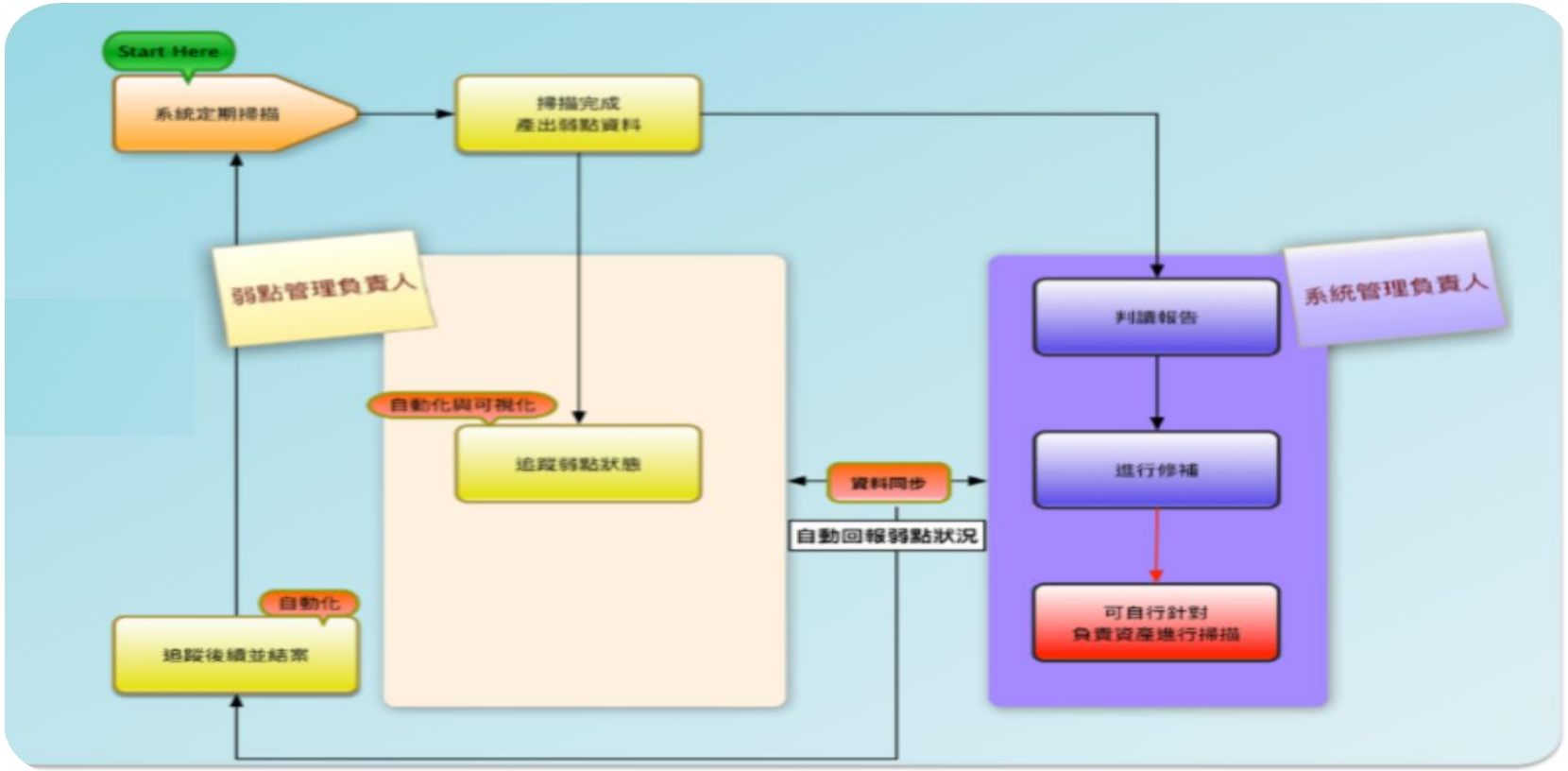
弱點掃描執行的困難多多



- 人工執行作業困難
  - 工具操作問題
  - 作業排程問題
- 執行結果管理困難
  - 結果彙整問題
  - 報告遞發問題
- 修補矯正確認困難
  - 修補優先問題
  - 矯正複測問題
- 持續追蹤困難
  - 資料庫更新問題
  - 開單追蹤問題

怎樣的弱掃工具才稱手?

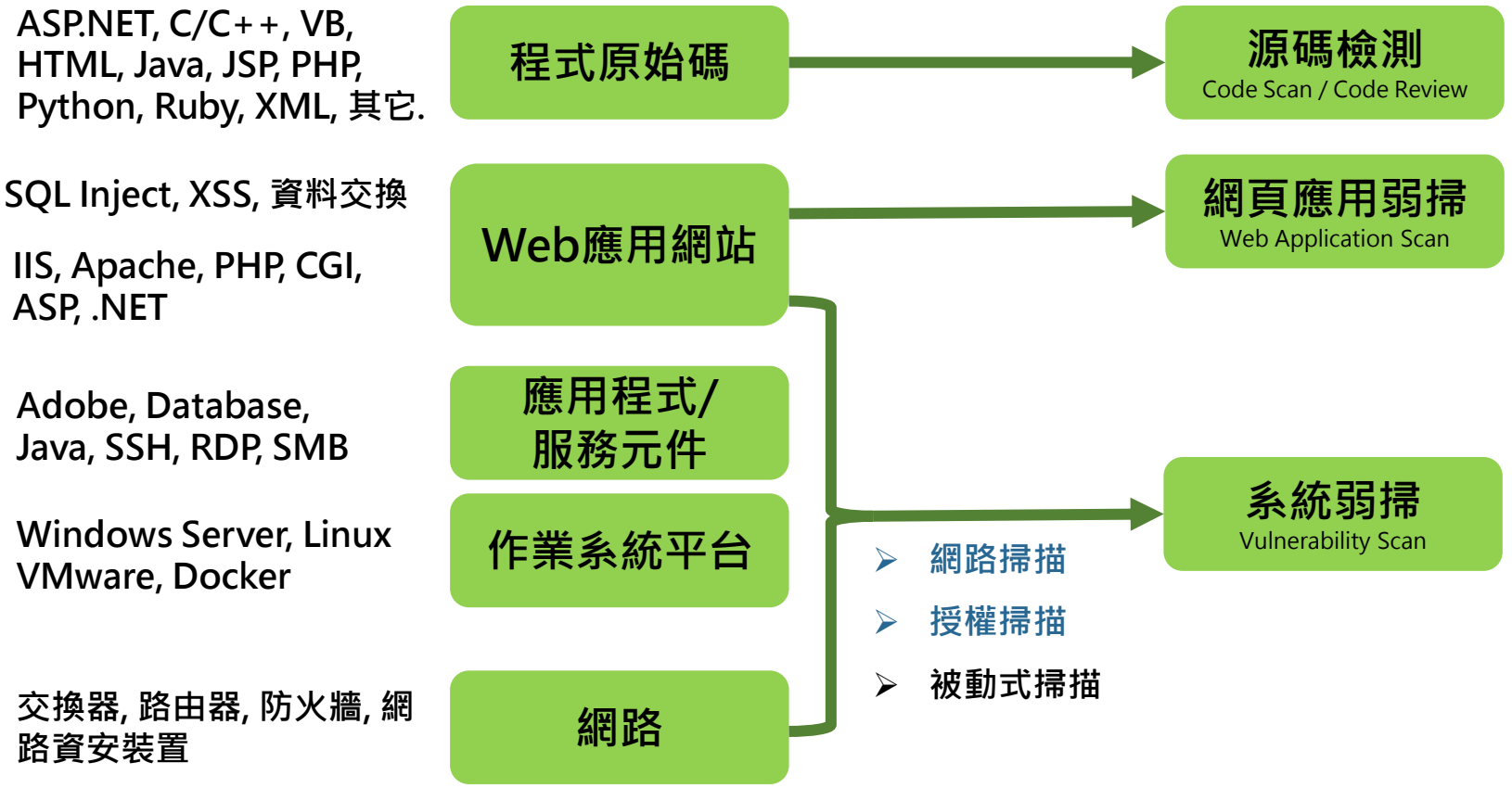
智能化　自動化　可視化　可管理



選擇合適的弱掃工具

- **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**

因應弱掃目的，選擇適當工具



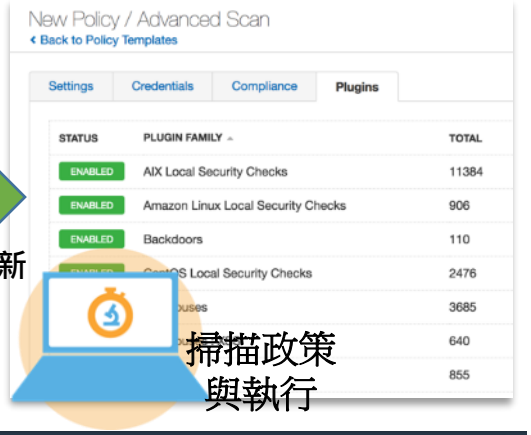
商業系統 vs. 開源系統

	商業版本	開源版本	社群版本
 費用付出	建議: 實務管理 或 規模檢測	建議: 個人研究 或 基礎評估	
 開發投入			
 功能設計			
 維護更新			
 支援協助			

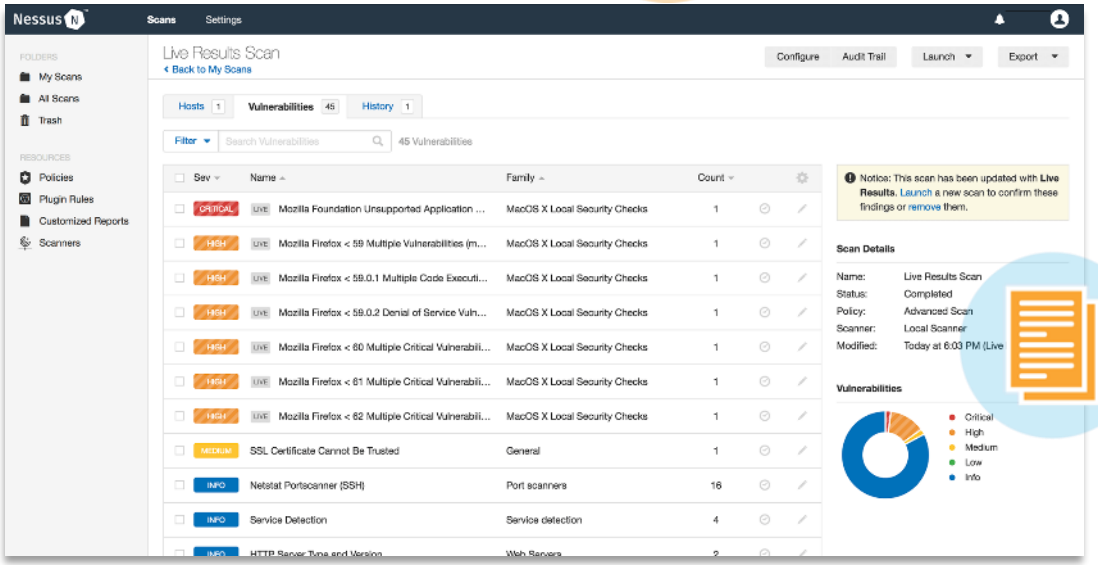
商業系統

研究/情資

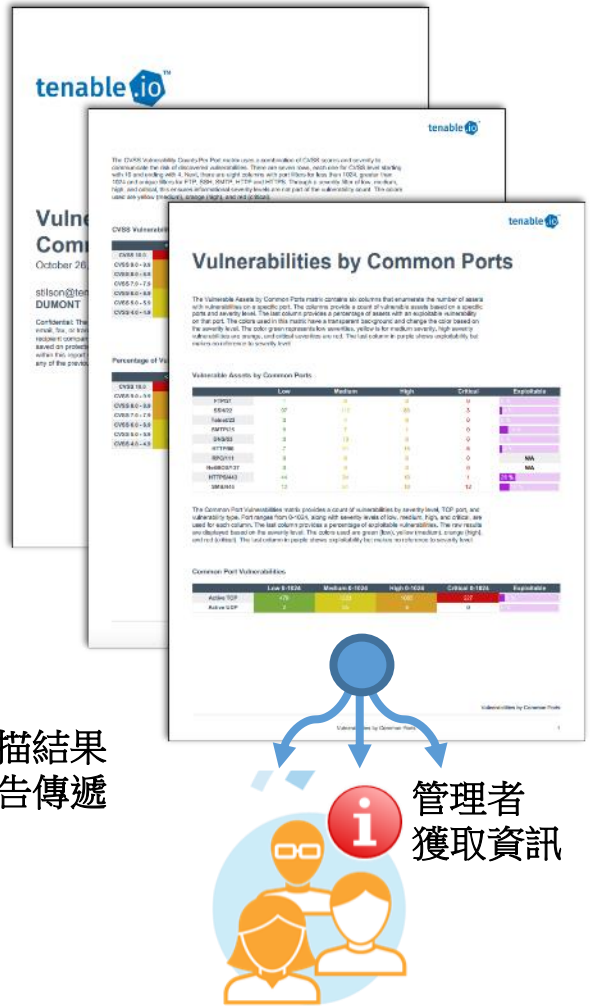
自動更新



掃描政策與執行

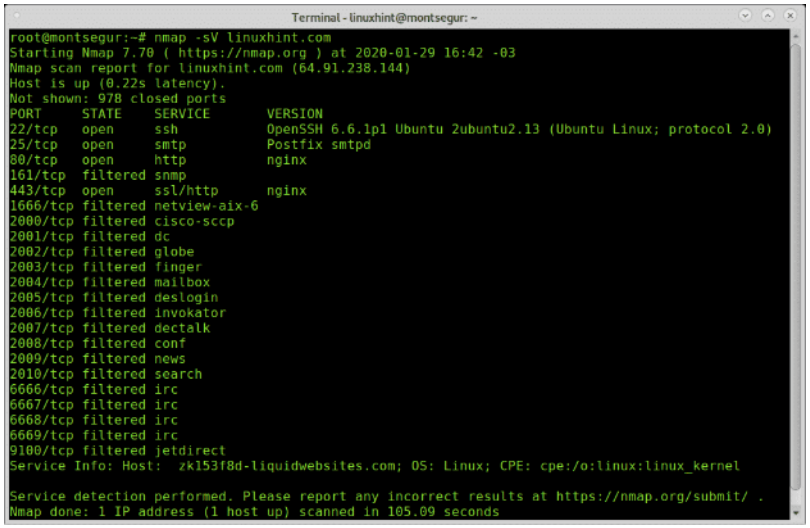


掃描結果報告傳遞



管理者獲取資訊

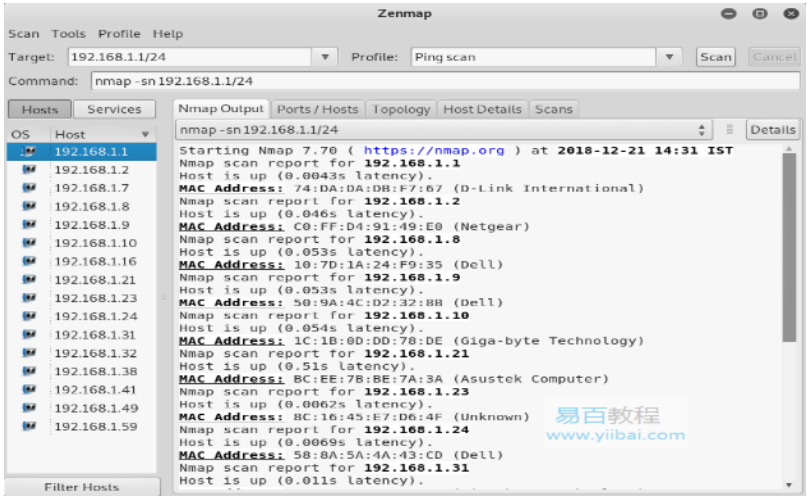
開源系統



自行研究摸索架設

自行修改或找尋檢測範本

Zenmap



自行產出結果

社群版本

數聯- 3S網站檢診服務 https://catd.issdu.com.tw/

(#案例參考)

弱掃工具必須有方法的使用

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:

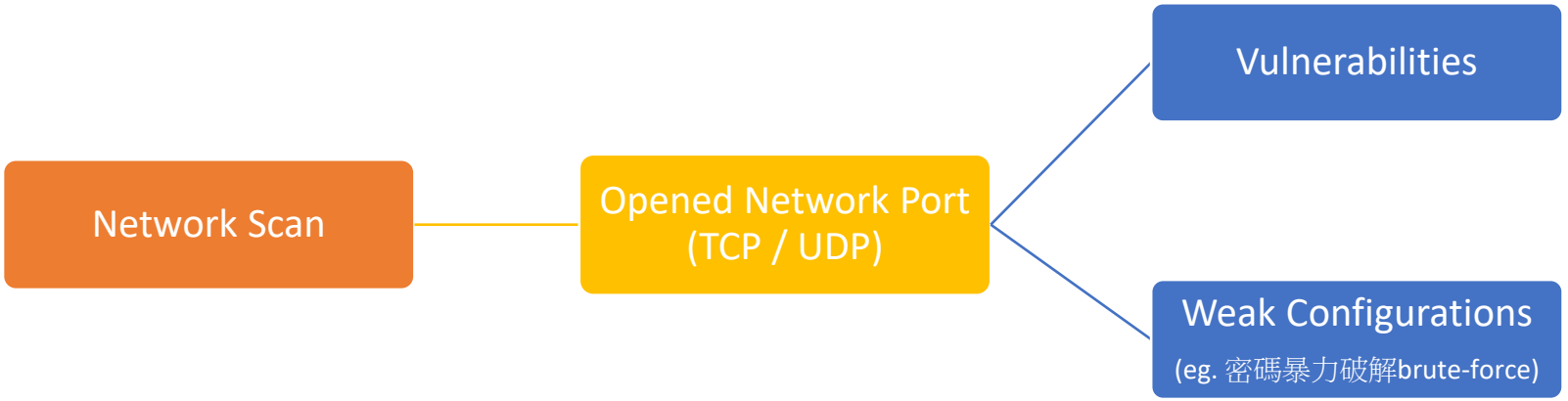
- 一般掃描政策.
- 進階掃描政策.
- 掃描頻率與週期

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)

網路掃描 (Network Scan)

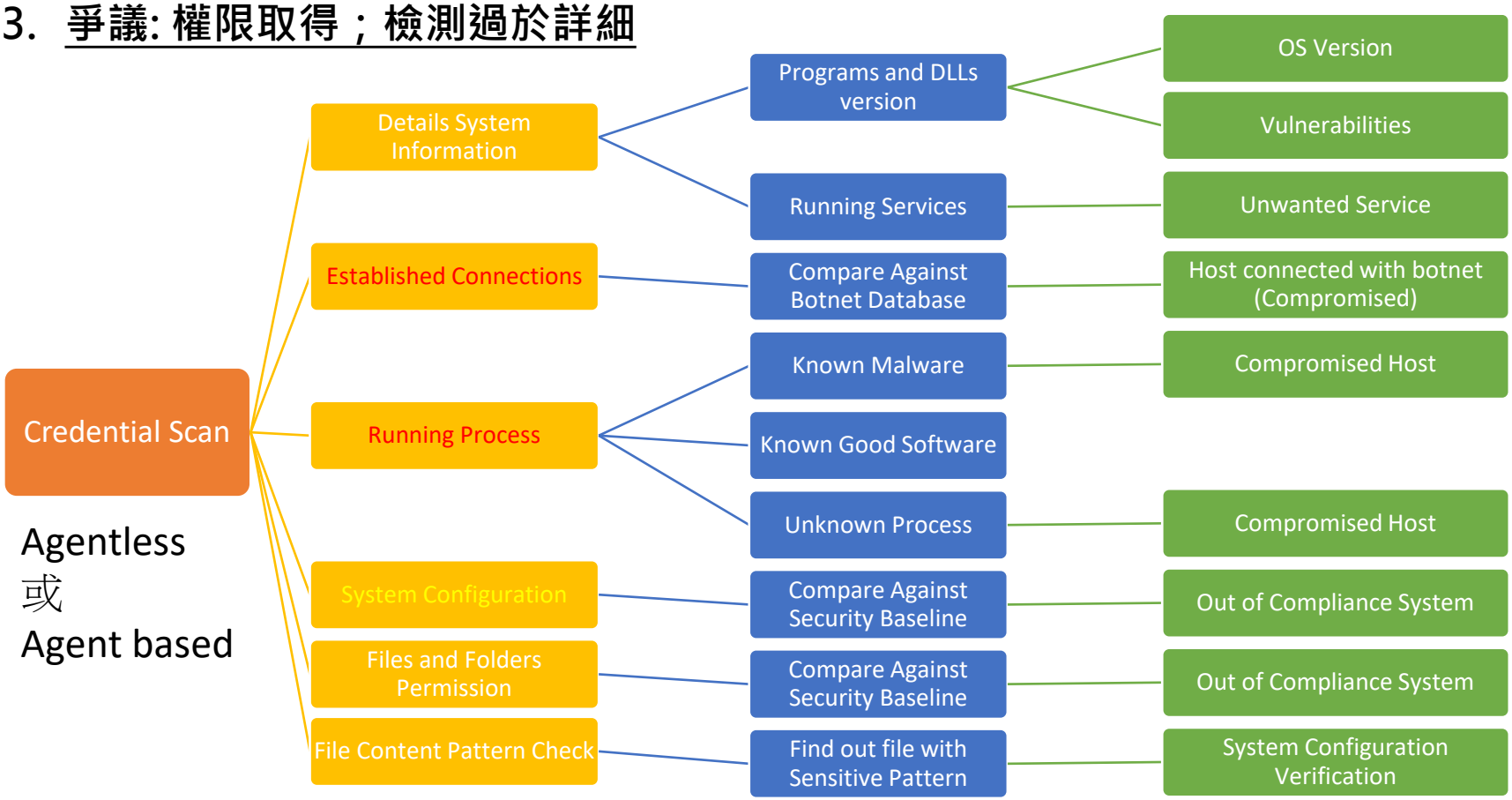
1. 檢測目標系統存在使用的網路埠進行探測與比對
2. 也稱“基本掃描”
3. 爭議：識別的準確性問題



1. 需開放弱掃主機的IP
2. 需允許所有的Port (UDP/TCP)
3. 建立大量的Port Scans及Sessions
4. 耗用網路傳輸頻寬

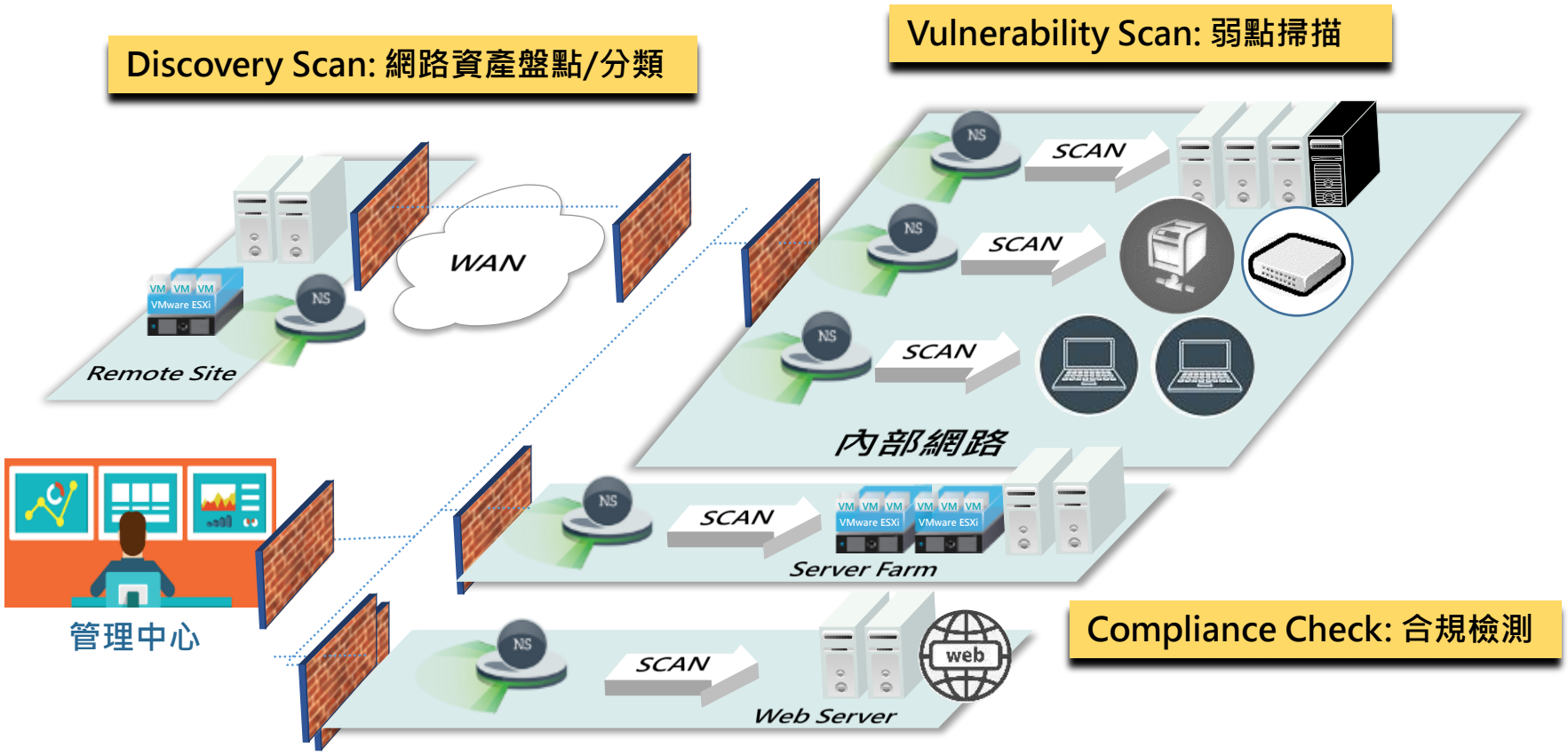
授權掃描 (Credential Scan)

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

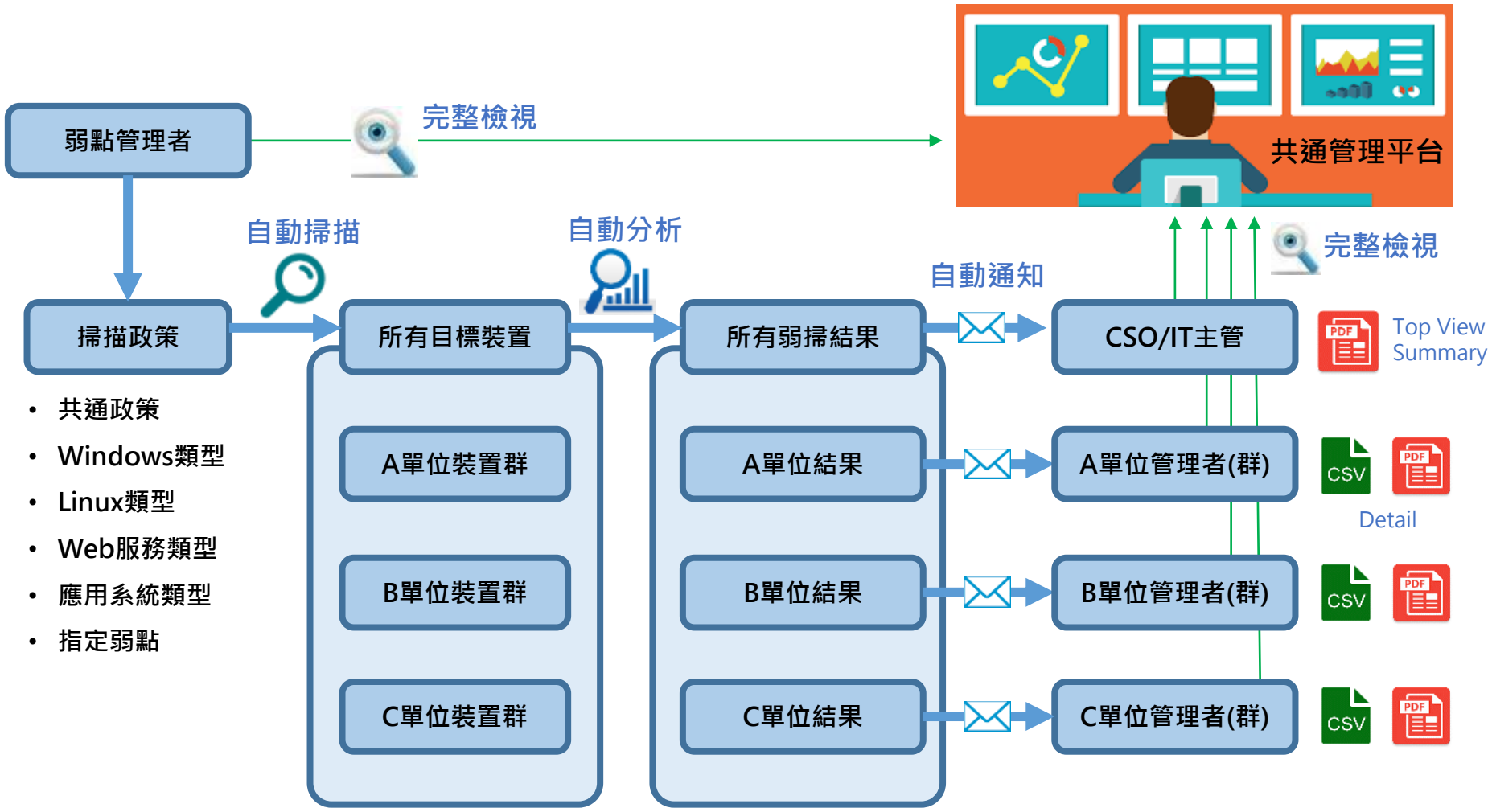


弱掃部署模式

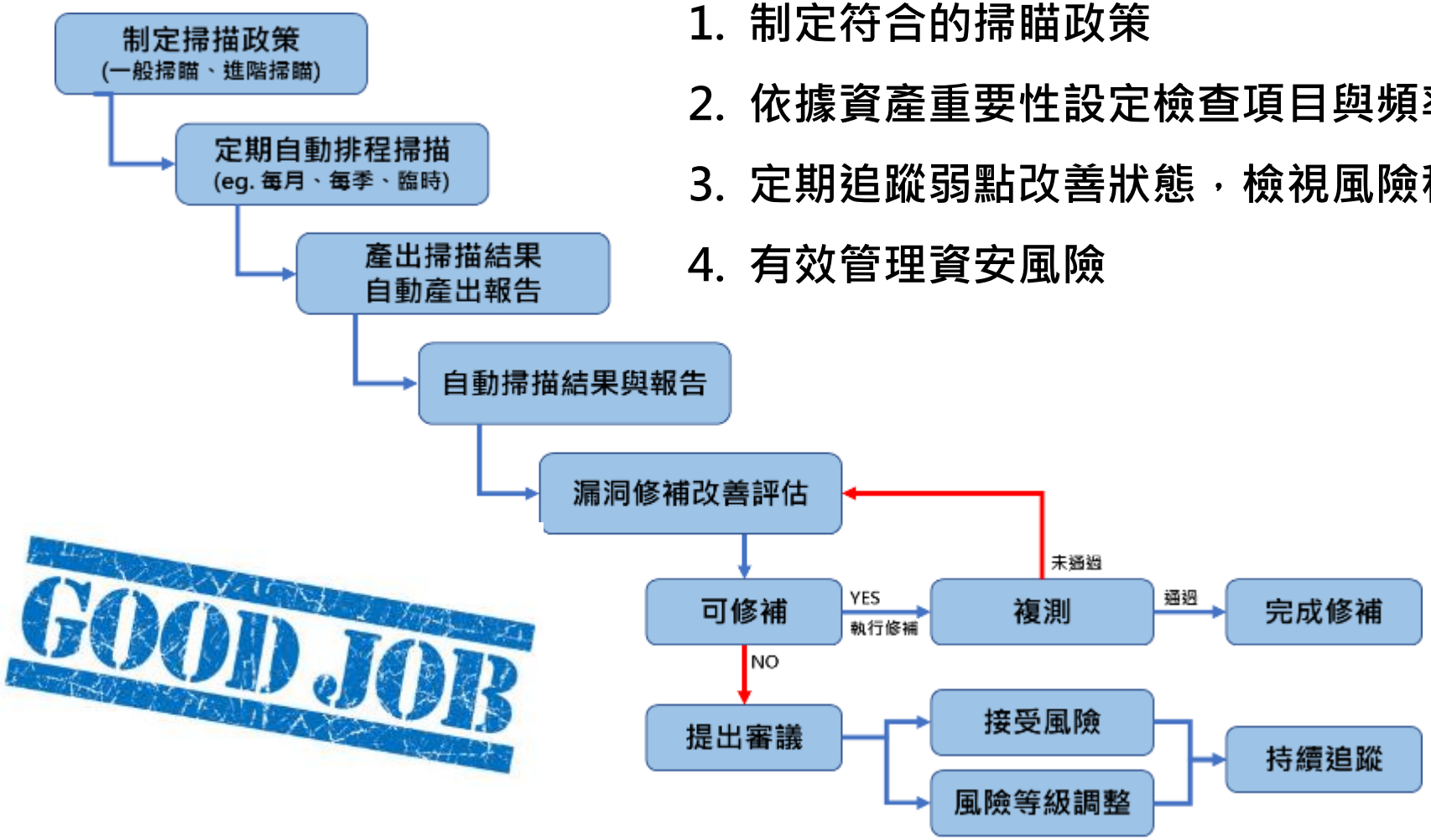
分散式部署 / 集中化監控 / 分權管理模式



弱掃作業自動化

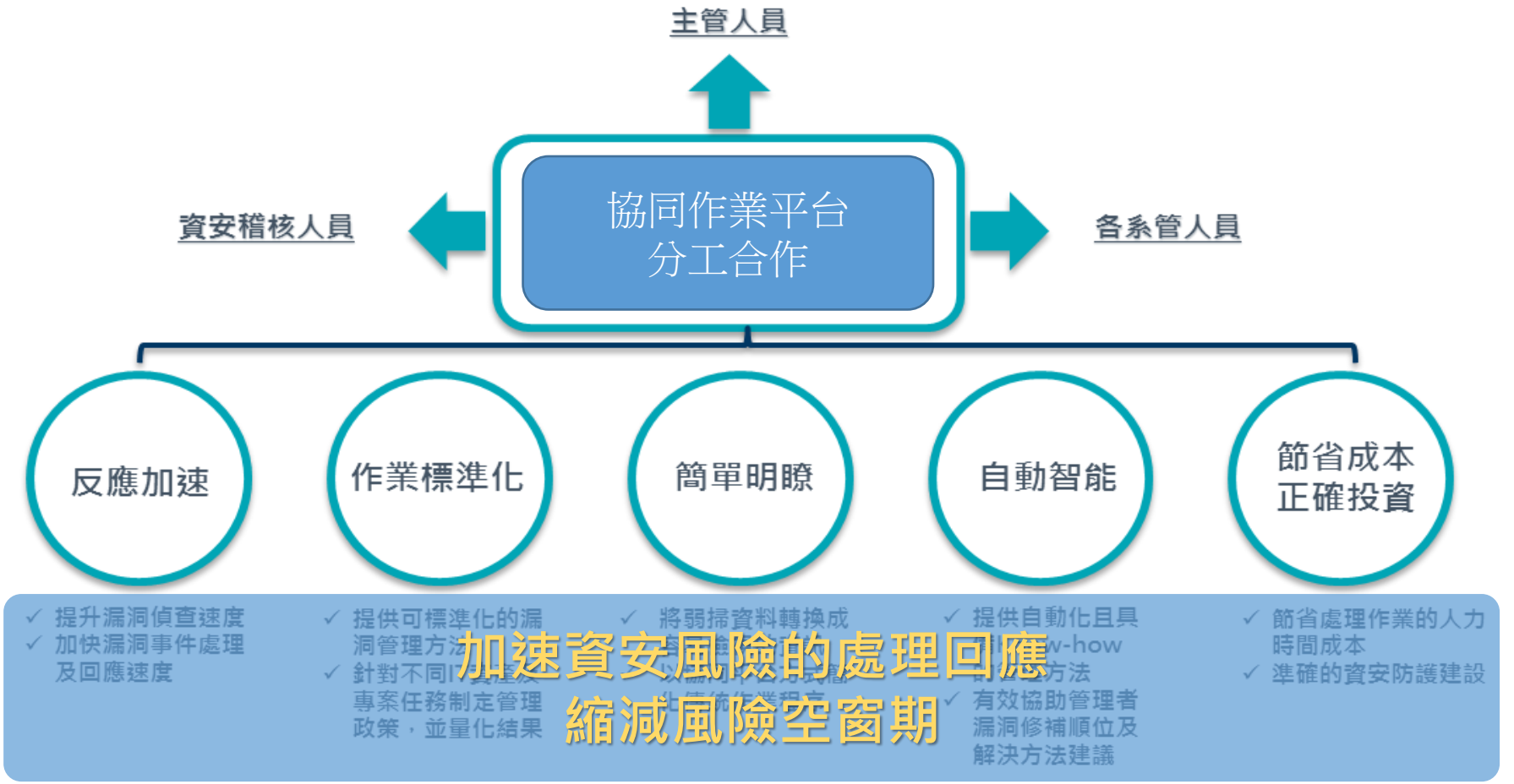


配合資安治理政策，建立弱點風險管理機制



1. 制定符合的掃瞄政策
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

新型態弱掃管理的效益訴求



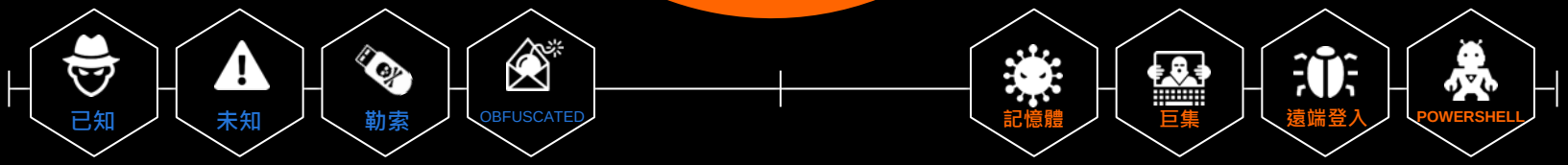
攻擊型態萬變不離 弱點利用

47%

攻擊使用
惡意程式

53%

攻擊使用
非惡意程式

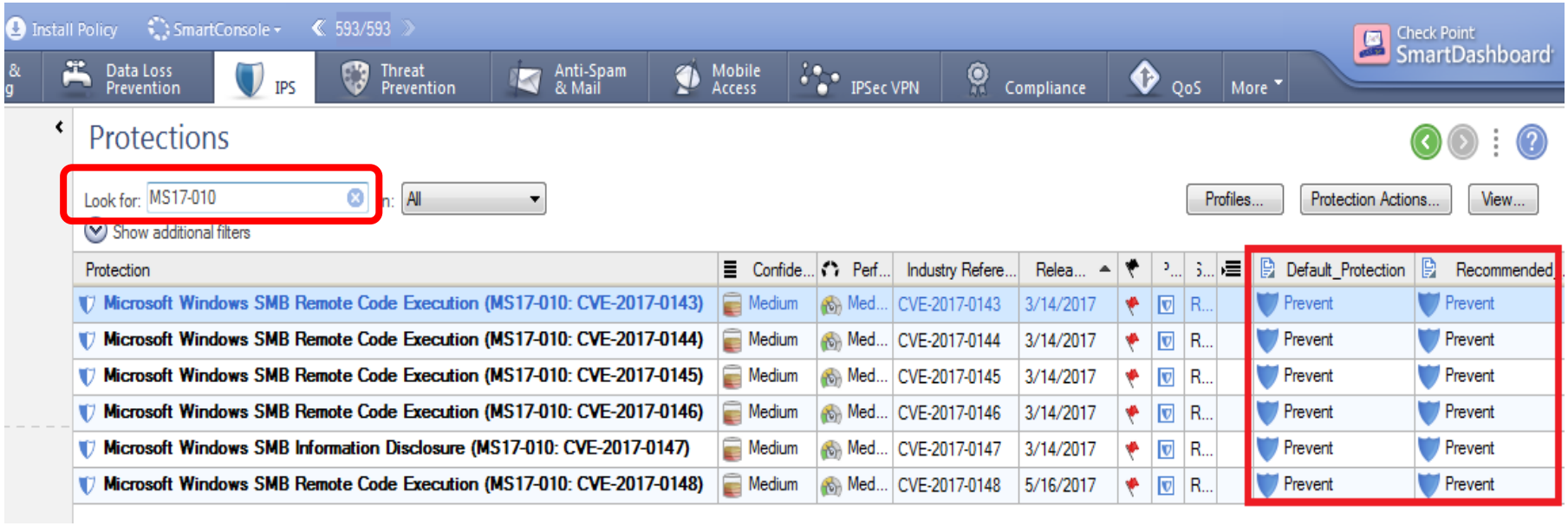


惡意程式攻擊
Malware

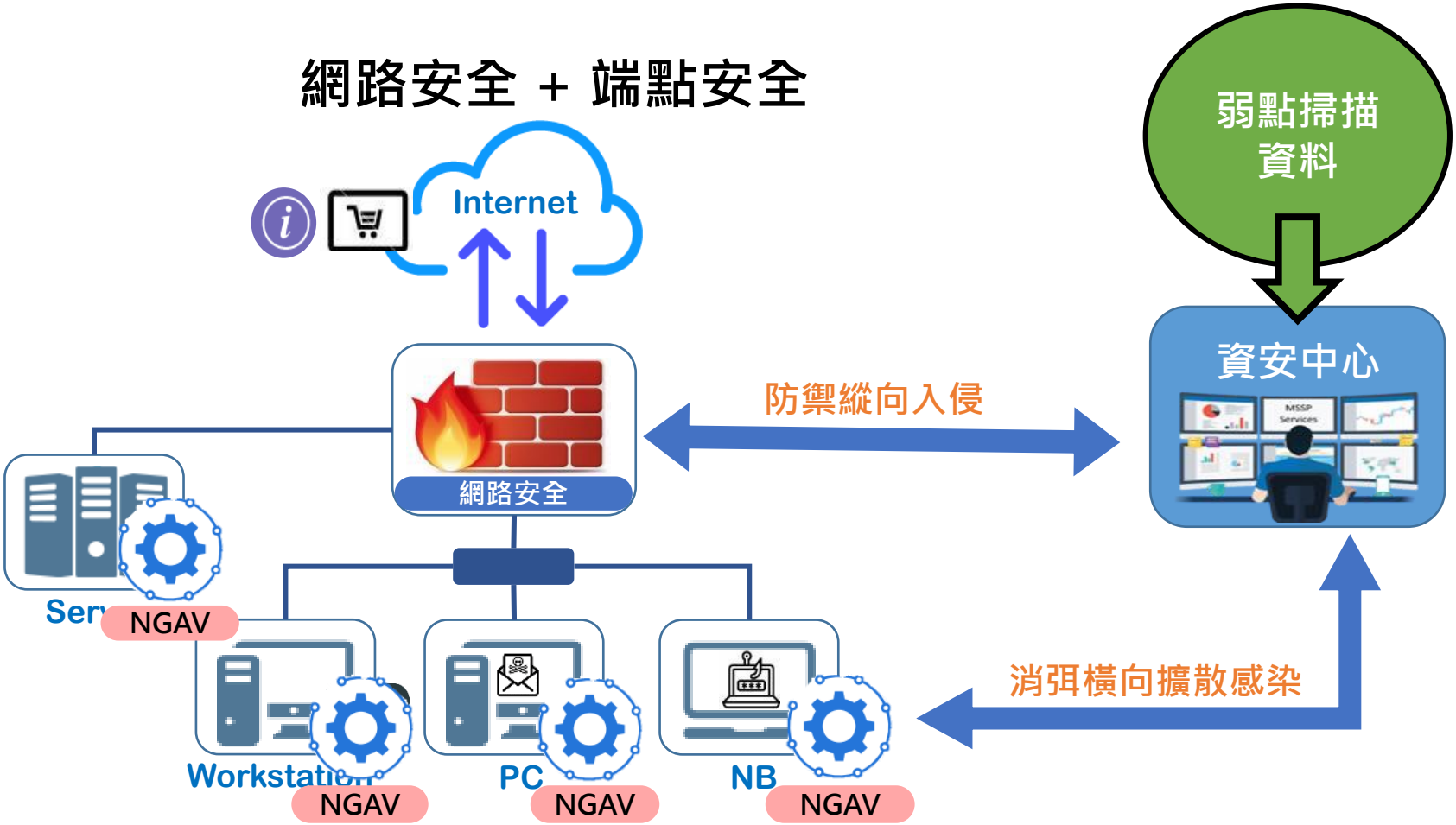
非惡意程式攻擊
Malwareless

弱點掃描資料的防護應用

1. 結合修補派送系統，準確快速消弭存在漏洞.
2. 結合網路及端點安全系統，建立檢查規則及虛擬修補防護.
3. 結合情資分析中心，持續觀測威脅變化.



快速建立防護網



結語

- 現代化思維 Modernization
- 弱點優先評級 Vulnerability Priority Rating
- 自適應控管 Adaptive control
- 零信任 Zero Trust
- 感知預測 Awareness & Prediction

“天下武功无坚不摧，
唯快不破！

——— 李小龙

Q&A