怎樣找到你最需要的弱點工具

黃繼民 Jim Huang

創泓科技-資深技術顧問

jim@uniforcetech.com.tw

UNIFORCE 創泓科技

大綱簡介

- 前言
- 為什麼一定要掃描
- 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

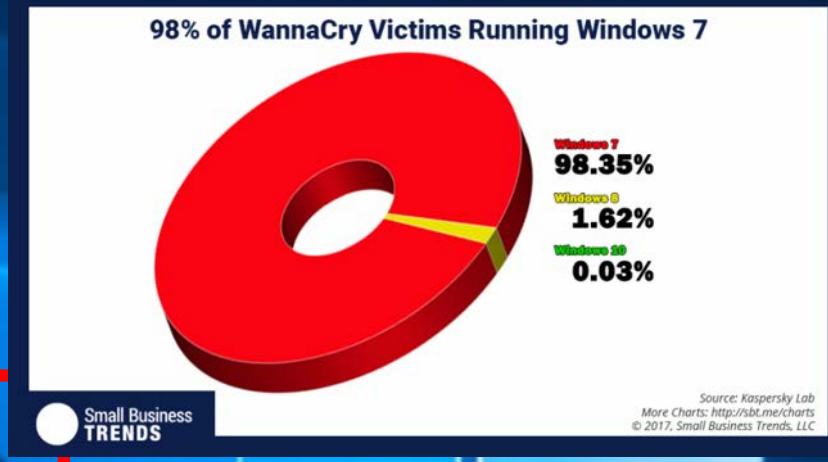
UNIFORCE 創泓科技

資安弱點武器化

- 美國安全單位NSA 遭到影子掮客組織入侵.
- 影子掮客釋出大量駭客工具於黑市.
- 針對Windows系統弱點的「永恆之藍」造成驚世攻擊WannaCry

UNIFORCE 創泓科技

永恆之藍 EternalBlue 效應



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 趨勢科技: 駭客利用「永恆之藍」入侵家用網路 台灣受攻擊次數連三週高居全球首位.

UNIFORCE 創泓科技

網路犯罪地下經濟

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」

WannaCry

WannaMine

UNIFORCE 創泓科技

可利用弱點持續增長變化

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?

Not Only

Home Device is Attacker

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

資料來源: TREND MICRO 趨勢科技

2018年 趨勢科技: 駭客利用「永恆之藍」入侵家用網路
台灣受攻擊次數連三週高居全球首位!

UNIFORCE 創泓科技

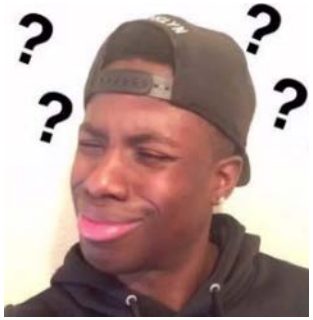
大綱簡介

- 前言
- 為什麼一定要掃描
- 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

UNIFORCE 創泓科技

為什麼一定要掃描

WHY NOT ?



因為害怕
- 怕多事
- 怕不懂
- 怕責罰

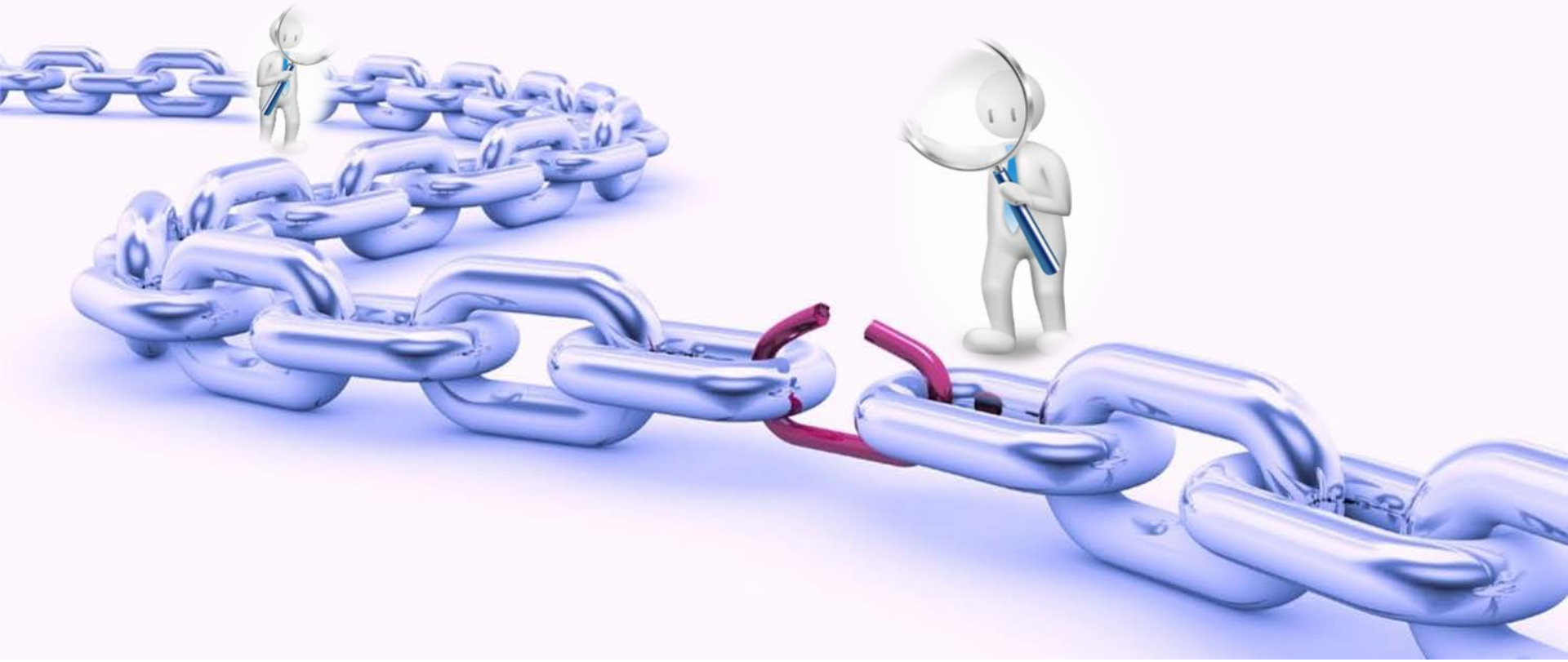
自我安慰
- 不曾出事
- 已有防護
- 不是目標
- 已合規範

UNIFORCE 創泓科技

弱點掃描目的

<<<從資安的視角>>>

掌握存在的弱點，提早應對準備，避免風險暴露.



UNIFORCE 創泓科技

現今資安威脅有高達90%是利用漏洞!!

惡意程式

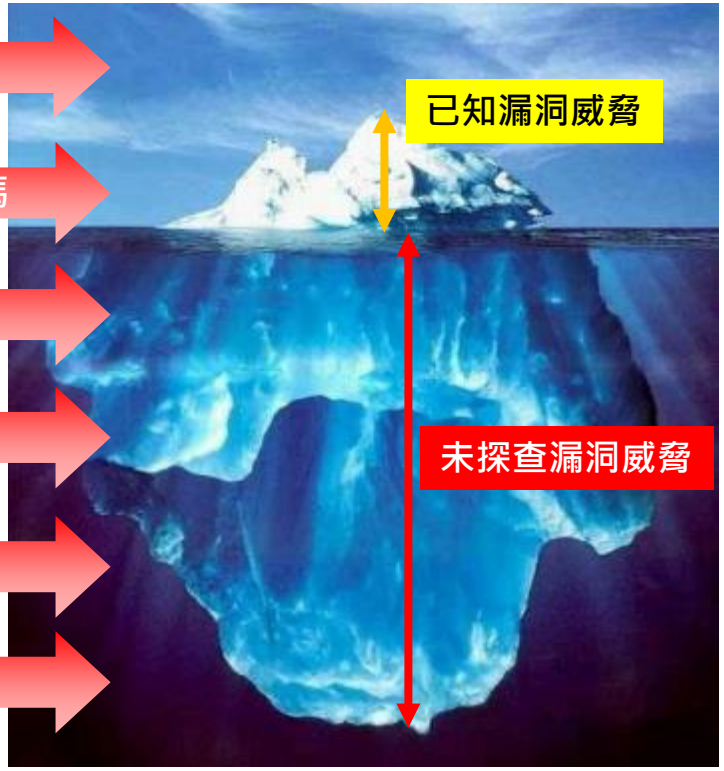
殭屍/木馬

跳板攻擊

資料竊取

釣魚詐欺

目標攻擊

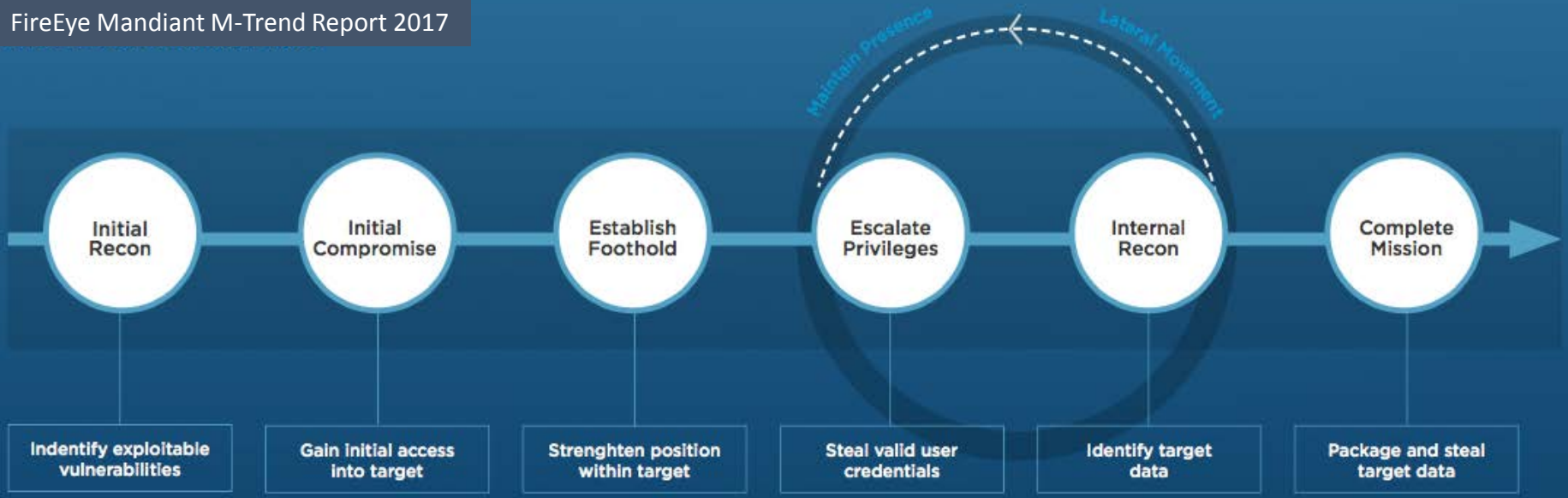


有洞嗎?
洞在哪裡?
又如何?
都很正常呀!?
證明看看?
很麻煩內>_<

UNIFORCE 創泓科技

現今資安攻擊的「起手式」

FireEye Mandiant M-Trend Report 2017



UNIFORCE 創泓科技

猜猜看，您認識以下哪些弱點?

Zip Slip目錄走訪漏洞

UNIFORCE 創泓科技

猜猜看，安全設備“安全”嗎?

UNIFORCE 創泓科技

弱點已無處不在，所產生的威脅不斷攀升

資料來源: iThome 新聞剪輯

作業系統弱點

重要商務系統弱點

UNIFORCE 創泓科技

弱點已無處不在，所產生的威脅不斷攀升

UNIFORCE 創泓科技

弱點已無處不在，所產生的威脅不斷攀升


iThome 新聞 產品評測 CIO 技術 專題 專欄 主題頻道 研討會 社群

Unix /Linux 的Bash Shell 出現重大漏洞，危險等級可能超越Heartbleed

Errata Security執行長表示，Shell Shock漏洞可能與Heartbleed一樣嚴重。原因之一為有大量的軟體與Bash Shell互動，如同有大量的產品使用內含Heartbleed漏洞的OpenSSL一樣，因此根本無法估計可能受影響的軟體數量。

文/ 陳曉莉 | 2014-09-25 發表


iThome 新聞 產品評測 CIO 技術 專題 專欄 主題頻道 研討會 社群

資安

Bash驚爆Shellshock漏洞，全球半數網站伺服器陷危機

近日，國外爆出嚴重的資安漏洞危機，多家資安網站及Linux廠商發出警告，一個名為Shellshock漏洞，可能導致使用 Bash Shell的作業系統，包括Linux、Unix為基礎的平臺、Mac OS X系統等成為駭客遠端入侵的工具，甚至使得全球超過半數網站伺服器，皆可能身陷危機之中。

文/ 余至浩 | 2014-09-26 發表


iThome

新聞

羅馬尼亞駭客利用Shellshock漏洞入侵雅虎，不小心打中Web log 漏洞

羅馬尼亞駭客試圖利用Shellshock漏洞在Unix主機上建立僵屍網路，並用以入侵雅虎伺服器。原先雅虎以為是主機有Shellshock漏洞而遭受攻擊，雅虎資安調查之後發現，其實駭客打中的是該公司Web log除錯工具一個剛好與Bash Shell一樣有「指令插入」瑕疵的漏洞。

文/ 林妍溱 | 2014-10-07 發表

註解: Bash是一個指令列shell （殼層）程式，廣泛存在於 Linux、BSD 和 Mac OS X 等UNIX-based的作業系統，使用者只要將指令輸入到一個簡單的文字式視窗，作業系統便會依指令運作。由於全球有超過半數的伺服器採用Linux，也讓這個漏洞的可能影響相當可怕，各方評估皆認為，嚴重程度可能超過Heartbleed。駭客一但成功攻擊一個網站或伺服器，特別是CGI 網頁伺服器，幾乎可以為所欲為，例如可以隨意修改網站內容，變更程式碼、竊取資料庫中的使用者資料，或者安裝後門等惡意程式。而根據各個資安機構指出，目前已開始出現了利用Shell Shock的攻擊案例。

UNIFORCE 創泓科技

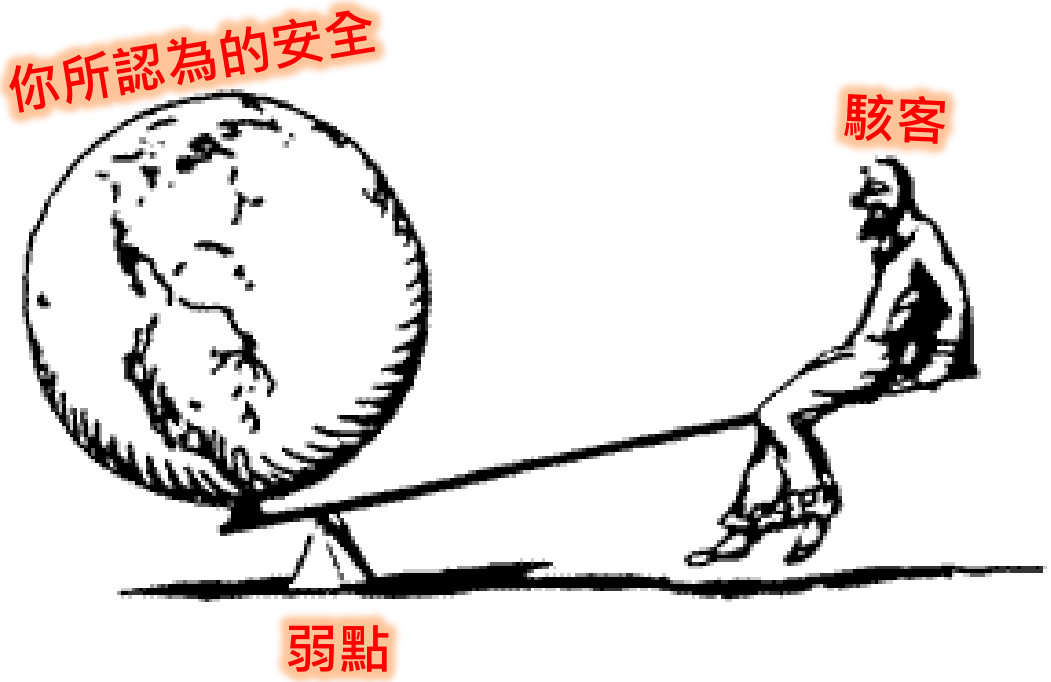
開源軟體(Open Source) 安全隱憂

資料來源: Black Duck Software

UNIFORCE 創泓科技

安全脆弱度，只需要一個正確的點

阿基里斯 vs. 阿基里德

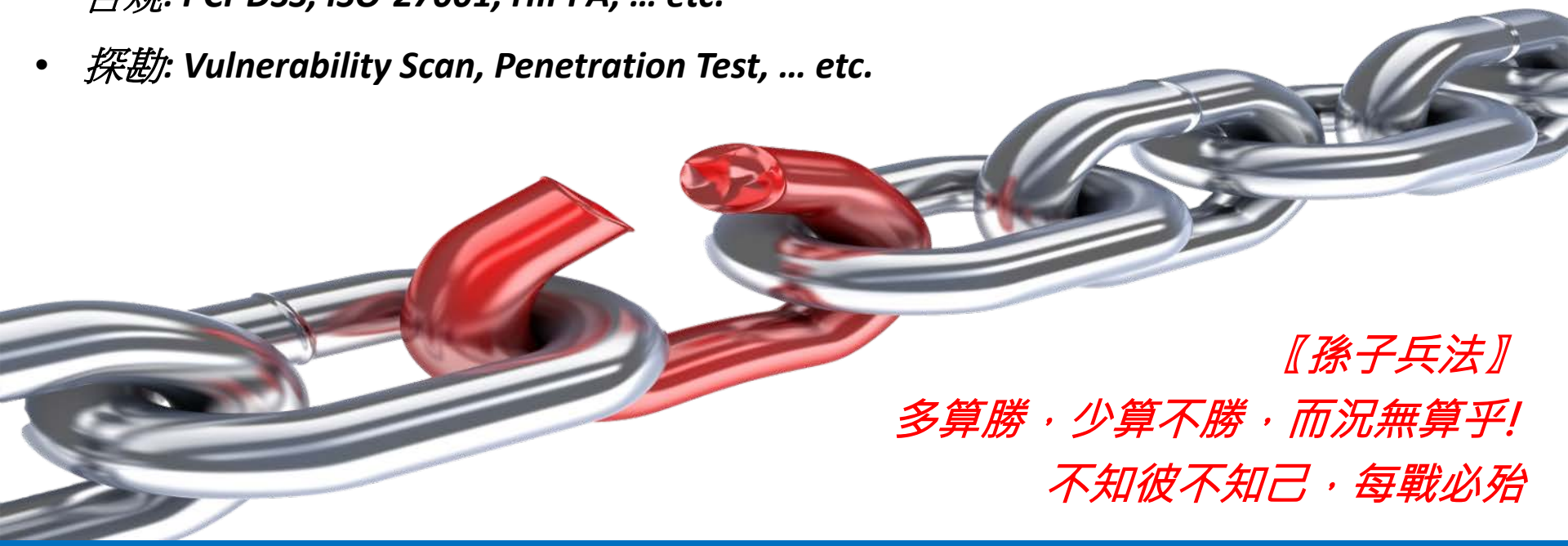


UNIFORCE 創泓科技

再問: 為什麼一定要掃描

資安防禦工事上的迷思

- *防護*: **Firewall, IPS, Anti-Virus, Content Security Gate, Endpoint Security, WAF, NAC, … etc.**
- *檢測*: **APT, Sandbox, Code review, …etc.**
- *分析*: **Log Analysis management, SIEM, SOC, …etc.**
- *合規*: **PCI-DSS, ISO-27001, HIPPA, … etc.**
- *探勘*: **Vulnerability Scan, Penetration Test, … etc.**



〖孫子兵法〗

多算勝，少算不勝，而況無算乎!

不知彼不知己，每戰必殆

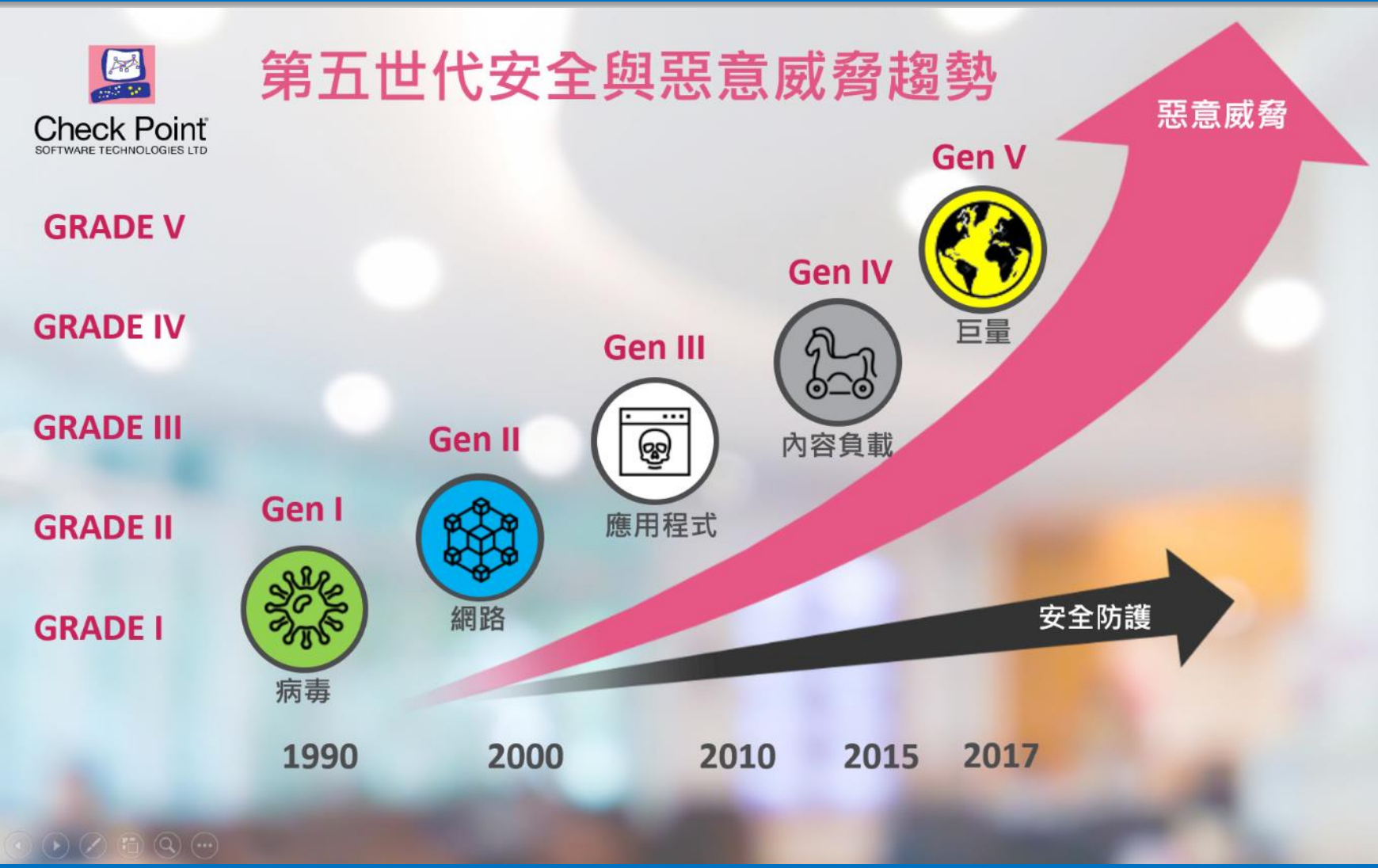
UNIFORCE 創泓科技

大綱簡介

- 前言
- 為什麼一定要掃描
- 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

UNIFORCE 創泓科技

不同世代的安全威脅演進



UNIFORCE 創泓科技

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

UNIFORCE 創泓科技

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

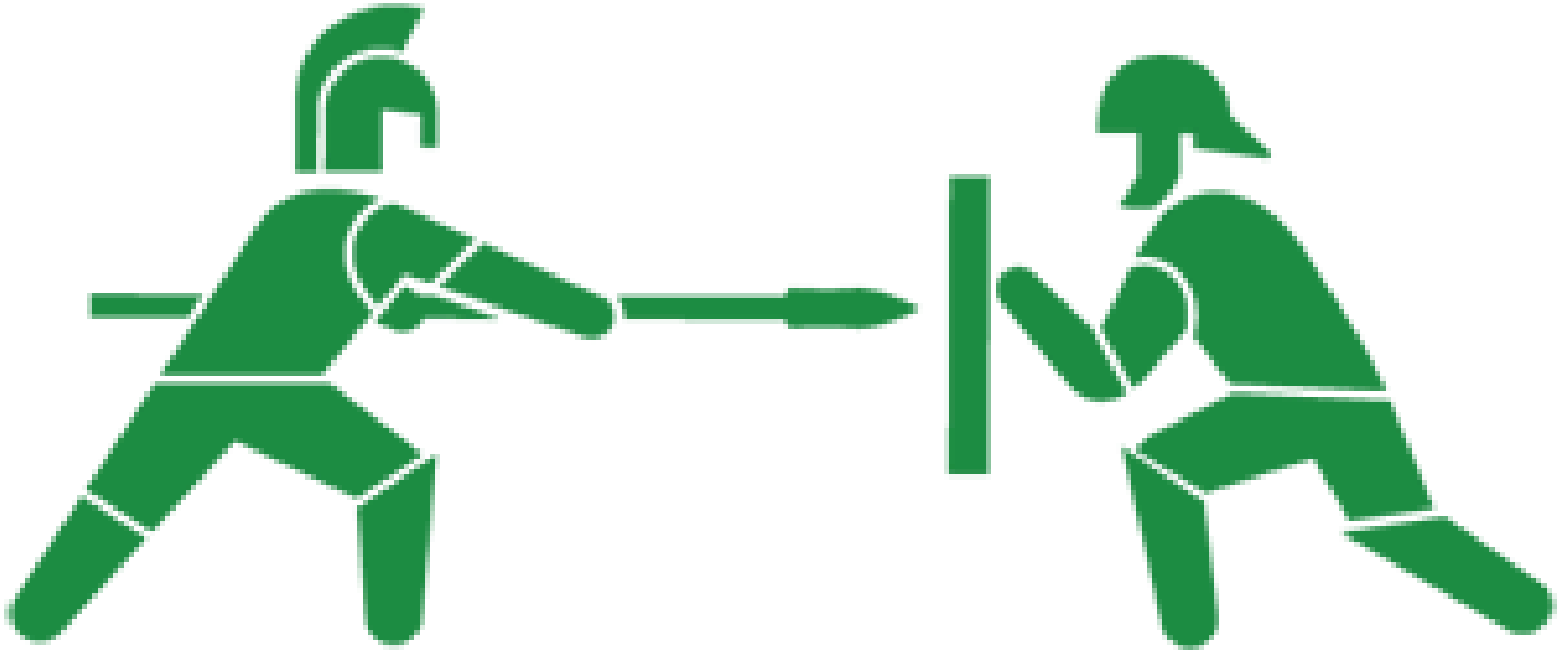
入侵防護
(FW/IPS/NGFW)

- **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**
- **防木馬程式**
- **防勒索軟體**

UNIFORCE 創泓科技

弱點掃瞄與滲透測試之間...?

對抗? 演練?

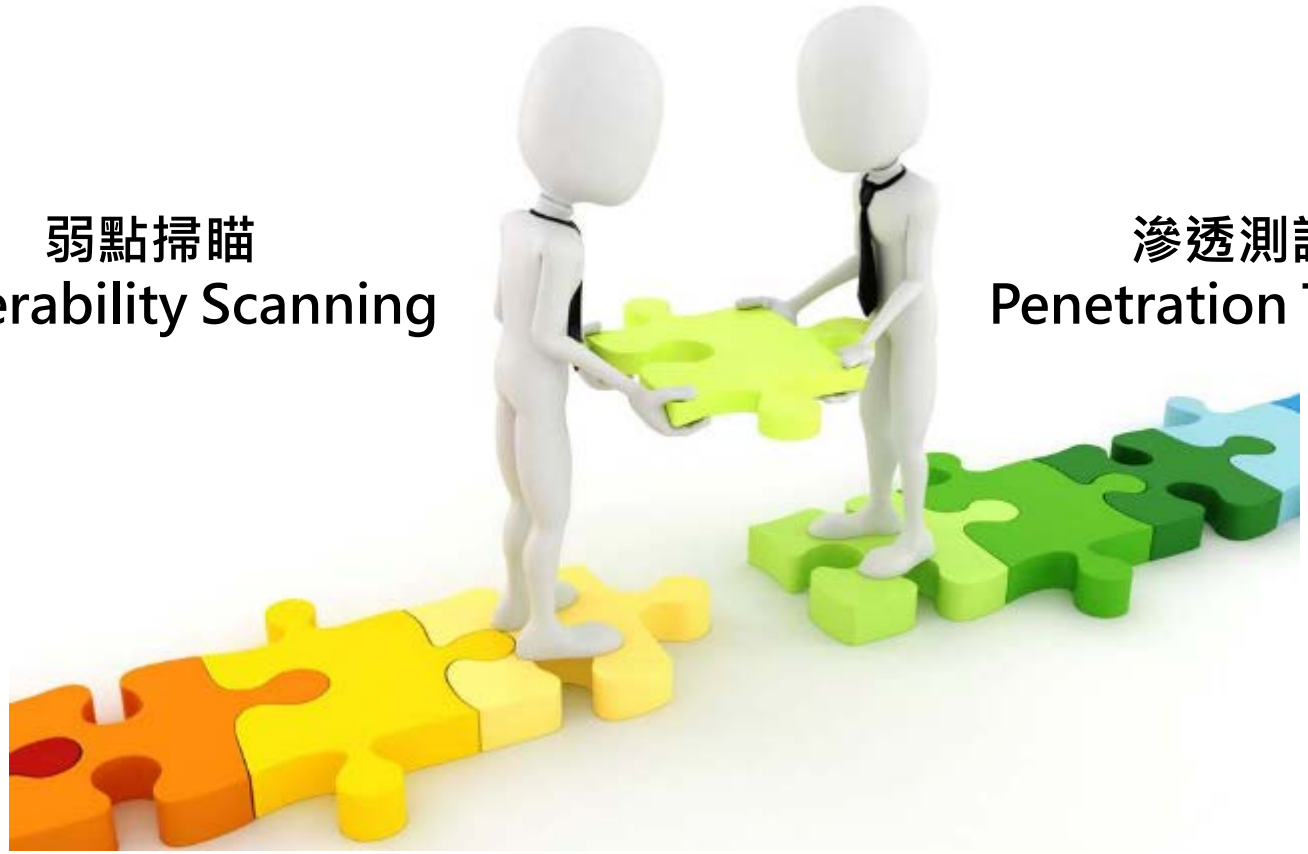


UNIFORCE 創泓科技

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.

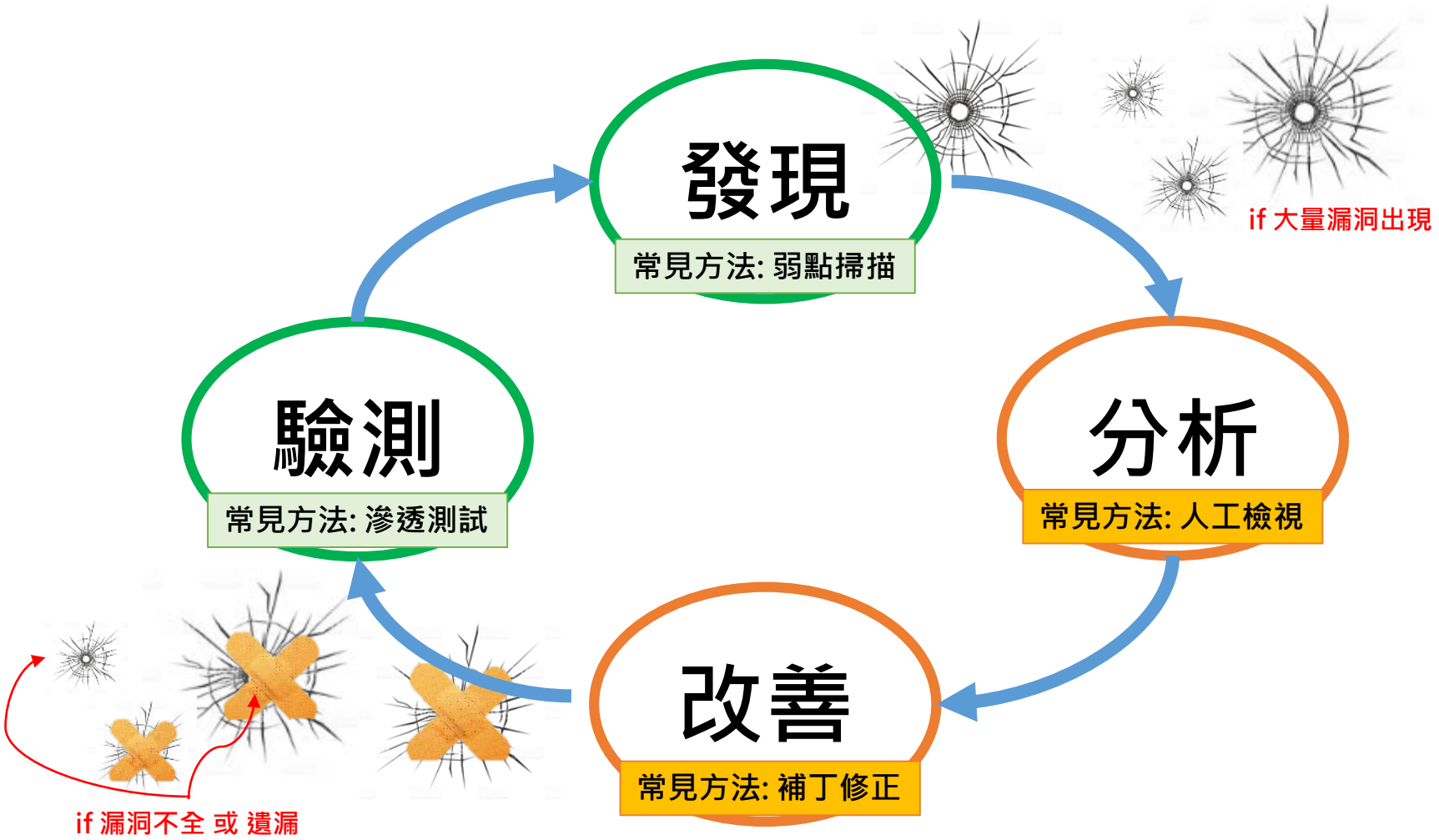
弱點掃瞄
Vulnerability Scanning



滲透測試
Penetration Testing

UNIFORCE 創泓科技

弱點掃瞄與滲透測試 是相互合作搭配



UNIFORCE 創泓科技

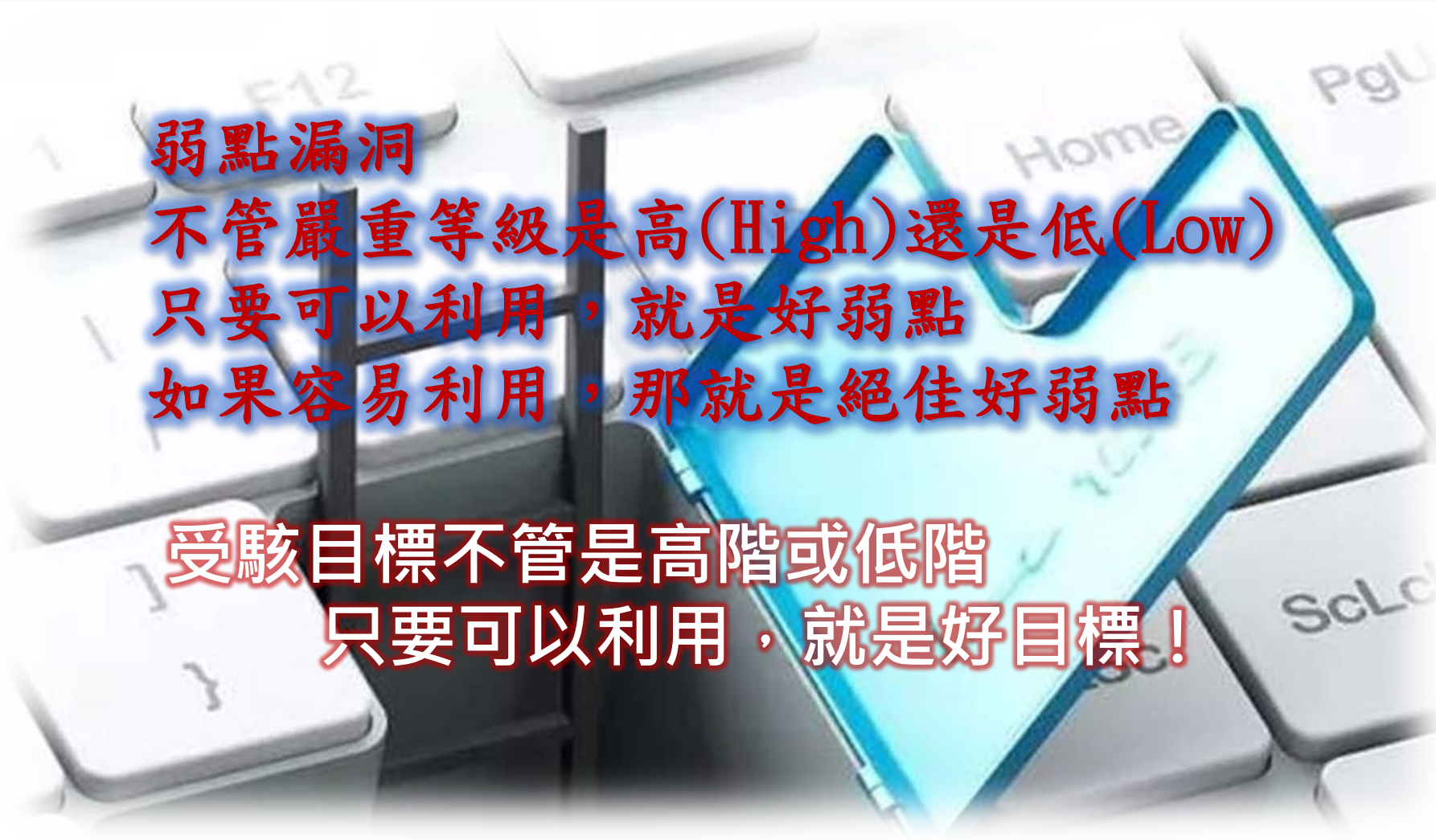
建立高效率的弱點安全管理

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

UNIFORCE 創泓科技

從資安怎麼看待「弱點(漏洞)」



UNIFORCE 創泓科技

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

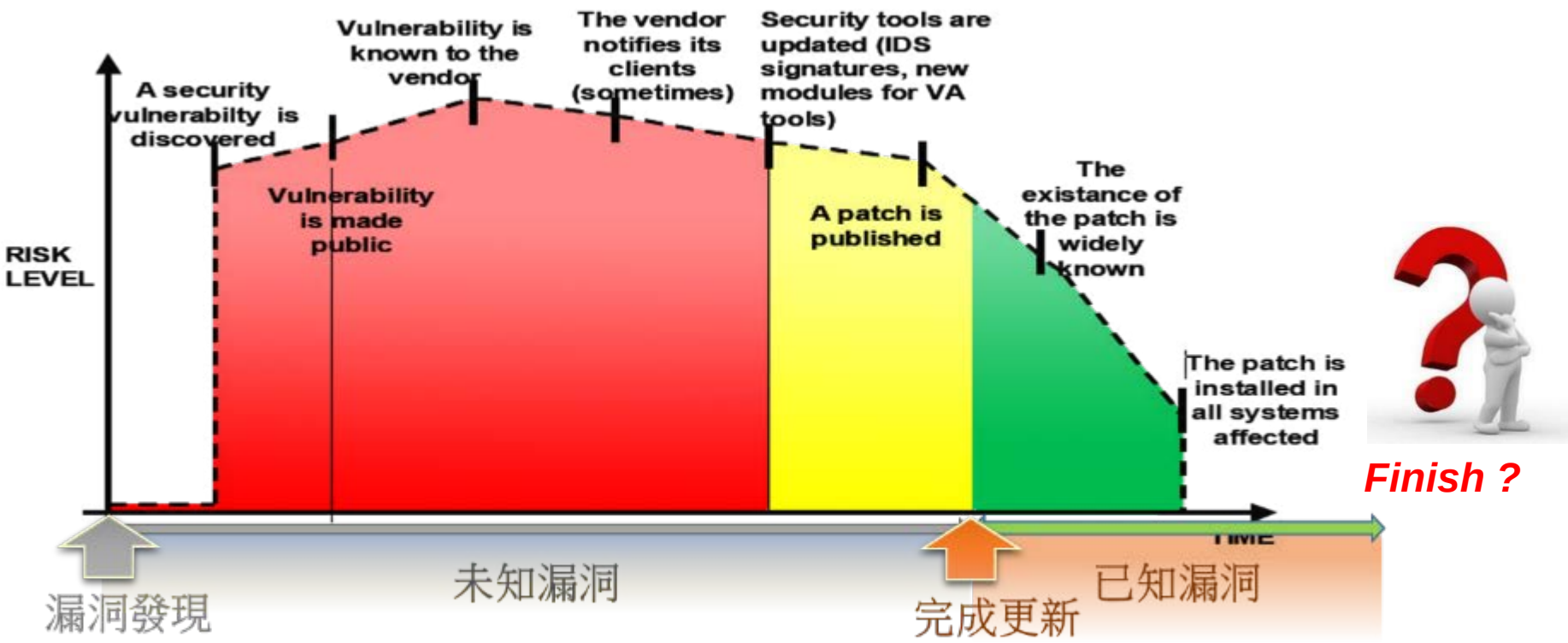
零時差漏洞 (也就是從未被發現的新漏洞) 最近出現的頻率越來越高，更糟的是，這些危險的漏洞經常都是在駭客攻擊事件發生之後，人們才知道漏洞的存在。

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)。

UNIFORCE 創泓科技

Zero-Day Attack 零日攻擊威脅

Window of Vulnerability

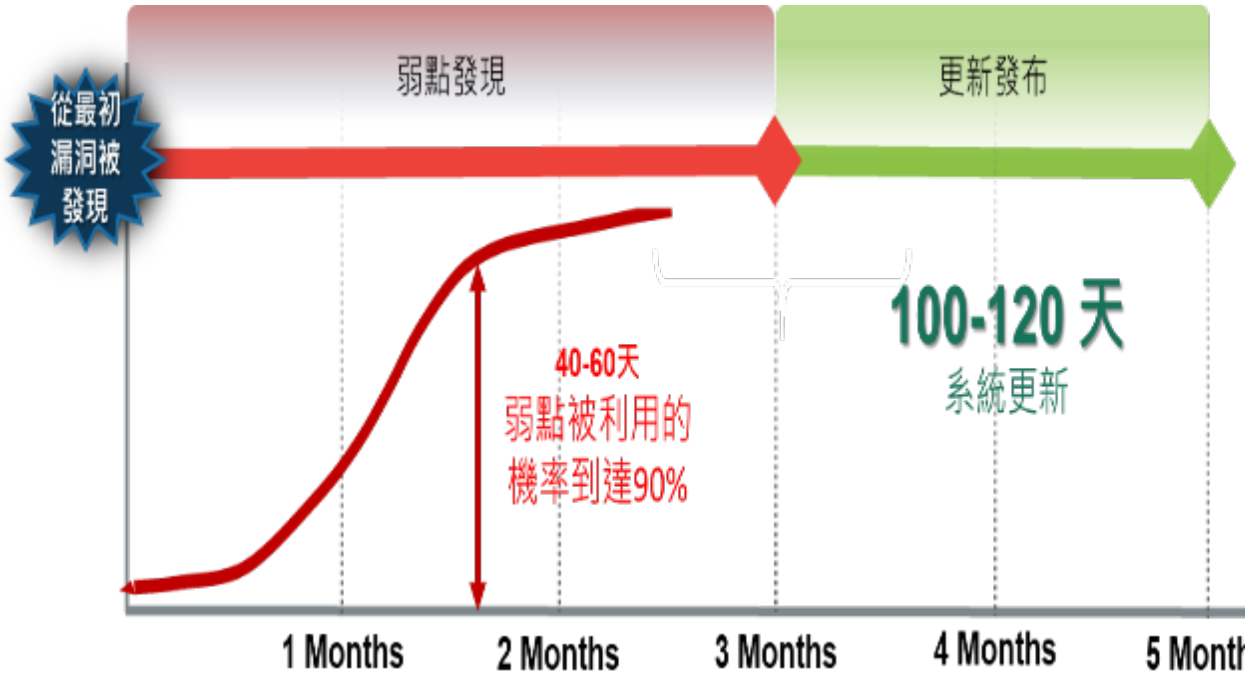


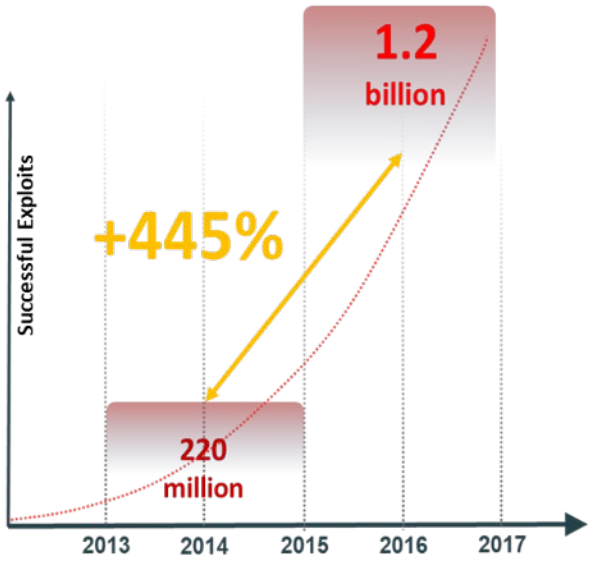
Finish ?

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

UNIFORCE 創泓科技

從漏洞揭露開始，攻擊威脅已然存在





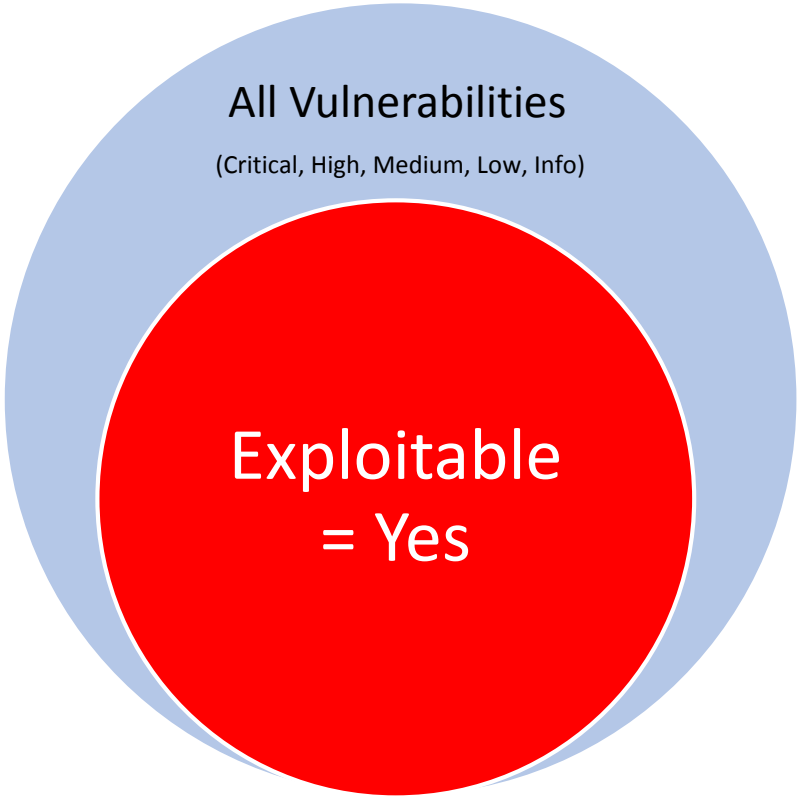
Source: https://www.infosecurity-magazine.com/news/companies-average-120-days-patch/

UNIFORCE 創泓科技

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)。



cisco

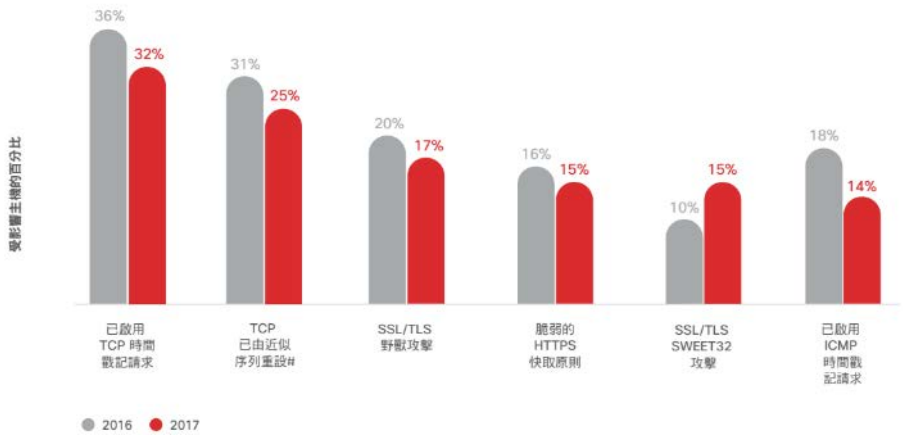
2018年度網路安全報告

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思科合作夥伴 SAINT Corporation 的資安專家表示，低嚴重性漏洞擅留多年，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著重大影響，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暴露資料。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

UNIFORCE 創泓科技

關於「滲透測試」

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。

UNIFORCE 創泓科技

白箱測試 vs. 黑箱測試 的優缺差異

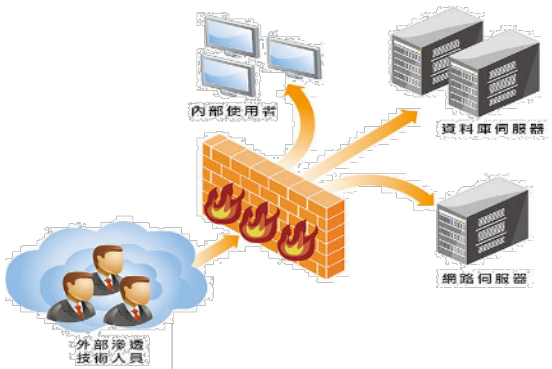
以Web系統為例:

	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

UNIFORCE 創泓科技

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」）

UNIFORCE 創泓科技

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

UNIFORCE 創泓科技

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

UNIFORCE 創泓科技

學習資訊參考

https://www.kali.org/

Kali Linux 2018.2 Release

OFFENSIVE security OSCP

CISSP

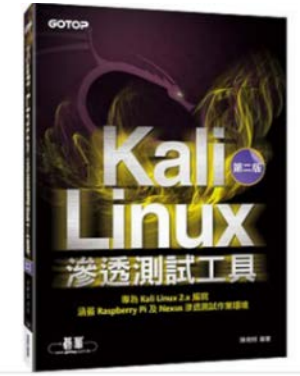
CISA Certified Information Systems Auditor An ISACA Certification

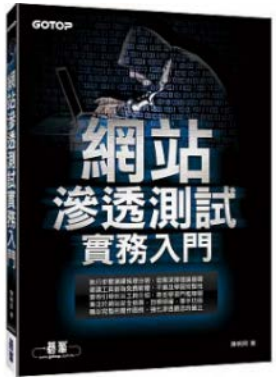
LEAD AUDITOR ISO 27001 Information Security Management System

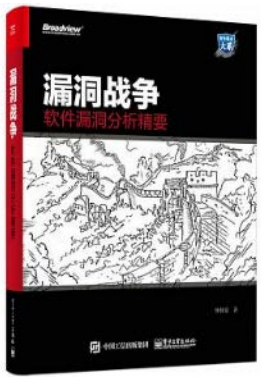
CEH Certified Ethical Hacker 駭客技術專家

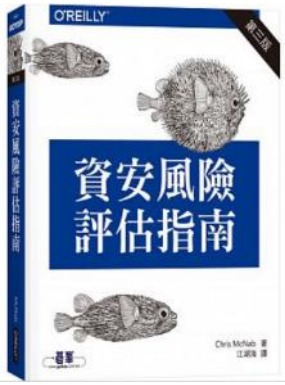
ECSA EC-Council Certified Security Analyst 資安分析專家

CHFI Computer Hacking Forensic INVESTIGATOR 資安鑑識調查專家









UNIFORCE 創泓科技

大綱簡介

- 前言
- 為什麼一定要掃描
- 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

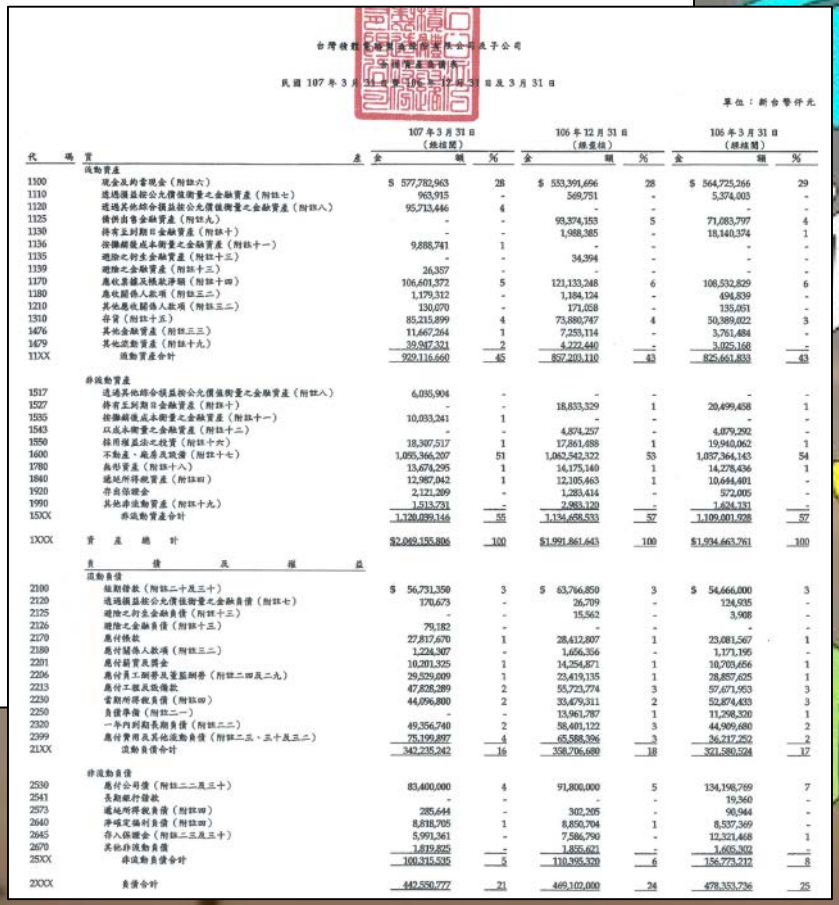
UNIFORCE 創泓科技

OMG... 弱掃報告又來了.

UNIFORCE 創泓科技

看不懂報告

財務報告



單位：新台幣仟元

代碼	資產	107年3月31日（經核閱） 金額	%	106年12月31日（經查核） 金額	%	106年3月31日（經核閱） 金額	%
	流動資產						
1100	現金及約當現金（附註六）	$ 577,782,963	28	$ 553,391,696	28	$ 564,725,266	29
1110	透過損益按公允價值衡量之金融資產（附註七）	963,915	-	569,751	-	5,374,003	-
1120	透過其他綜合損益按公允價值衡量之金融資產（附註八）	95,713,446	4	-	-	-	-
1125	備供出售金融資產（附註九）	-	-	93,374,153	5	71,083,797	4
1130	持有至到期日金融資產（附註十）	-	-	1,988,385	-	18,140,374	1
1136	按攤銷後成本衡量之金融資產（附註十一）	9,888,741	1	-	-	-	-
1135	避險之衍生金融資產（附註十三）	-	-	34,394	-	-	-
1139	避險之金融資產（附註十三）	26,357	-	-	-	-	-
1170	應收票據及帳款淨額（附註十四）	106,601,372	5	121,133,248	6	108,532,829	6
1180	應收關係人款項（附註三二）	1,179,312	-	1,184,124	-	494,839	-
1210	其他應收關係人款項（附註三二）	130,070	-	171,058	-	135,051	-
1310	存貨（附註十五）	85,215,899	4	73,880,747	4	50,389,022	3
1476	其他金融資產（附註三三）	11,667,264	1	7,253,114	-	3,761,484	-
1479	其他流動資產（附註十九）	39,947,321	2	4,222,440	-	3,025,168	-
11XX	流動資產合計	929,116,660	45	857,203,110	43	825,661,833	43
	非流動資產						
1517	透過其他綜合損益按公允價值衡量之金融資產（附註八）	6,035,904	-	-	-	-	-
1527	持有至到期日金融資產（附註十）	-	-	18,833,329	1	20,499,458	1
1535	按攤銷後成本衡量之金融資產（附註十一）	10,033,241	1	-	-	-	-
1543	以成本衡量之金融資產（附註十二）	-	-	4,874,257	-	4,879,292	-
1550	採用權益法之投資（附註十六）	18,307,517	1	17,861,488	1	19,940,062	1
1600	不動產、廠房及設備（附註十七）	1,055,366,207	51	1,062,542,322	53	1,037,364,143	54
1780	無形資產（附註十八）	13,674,295	1	14,175,140	1	14,278,436	1
1840	遞延所得稅資產（附註四）	12,987,042	1	12,105,463	1	10,644,401	-
1920	存出保證金	2,121,209	-	1,283,414	-	572,005	-
1990	其他非流動資產（附註十九）	1,513,731	-	2,983,129	-	1,624,131	-
15XX	非流動資產合計	1,120,039,146	55	1,134,458,533	57	1,109,001,928	57
1XXX	資產總計	$2,049,155,806	100	$1,991,661,643	100	$1,934,663,761	100
	負債及權益						
	流動負債						
2100	短期借款（附註二十及三十）	$ 56,731,350	3	$ 63,766,850	3	$ 54,666,000	3
2120	透過損益按公允價值衡量之金融負債（附註七）	170,673	-	26,709	-	124,935	-
2125	避險之衍生金融負債（附註十三）	-	-	15,562	-	3,908	-
2126	避險之金融負債（附註十三）	79,182	-	-	-	-	-
2170	應付帳款	27,817,670	1	28,412,807	1	23,081,567	1
2180	應付關係人款項（附註三二）	1,226,307	-	1,656,356	-	1,171,195	-
2201	應付薪資及獎金	10,201,325	1	14,254,871	1	10,703,656	1
2206	應付員工酬勞及董監酬勞（附註二四及二九）	29,329,609	1	23,419,135	1	28,857,625	1
2213	應付工程及設備款	47,805,289	2	55,723,774	3	57,671,953	3
2230	當期所得稅負債（附註四）	44,096,800	2	33,479,311	2	52,874,433	3
2250	負債準備（附註二一）	-	-	13,961,787	1	11,298,320	1
2320	一年內到期長期負債（附註二二）	49,356,740	2	58,401,122	3	44,909,680	2
2399	應付費用及其他流動負債（附註二五、三十及三二）	75,199,897	4	65,588,396	3	36,217,252	2
21XX	流動負債合計	342,235,242	16	358,706,680	18	321,580,524	17
	非流動負債						
2530	應付公司債（附註二二及三十）	83,400,000	4	91,806,000	5	134,198,769	7
2541	長期銀行借款	-	-	-	-	19,360	-
2573	遞延所得稅負債（附註四）	285,644	-	302,205	-	90,944	-
2640	淨確定福利負債（附註四）	8,818,705	1	8,850,704	1	8,537,369	-
2645	存入保證金（附註二三及三十）	5,991,361	-	7,586,790	-	12,321,468	1
2670	其他非流動負債	1,819,825	-	1,855,621	-	1,605,302	-
25XX	非流動負債合計	100,315,535	5	110,395,320	6	156,773,212	8
2XXX	負債合計	442,550,777	21	469,102,000	24	478,353,736	25

醫療檢查報告

癌症篩檢 Tumor Markers

人類絨毛激素【男】B-HCG	<1.2	mIU/ml	<5

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

靜態心電圖檢 ECG

十二導程心電圖檢查 12-lead ECG	正常(心跳次數：65次/分)	

腹部超音波 Abdominal Ultrasound

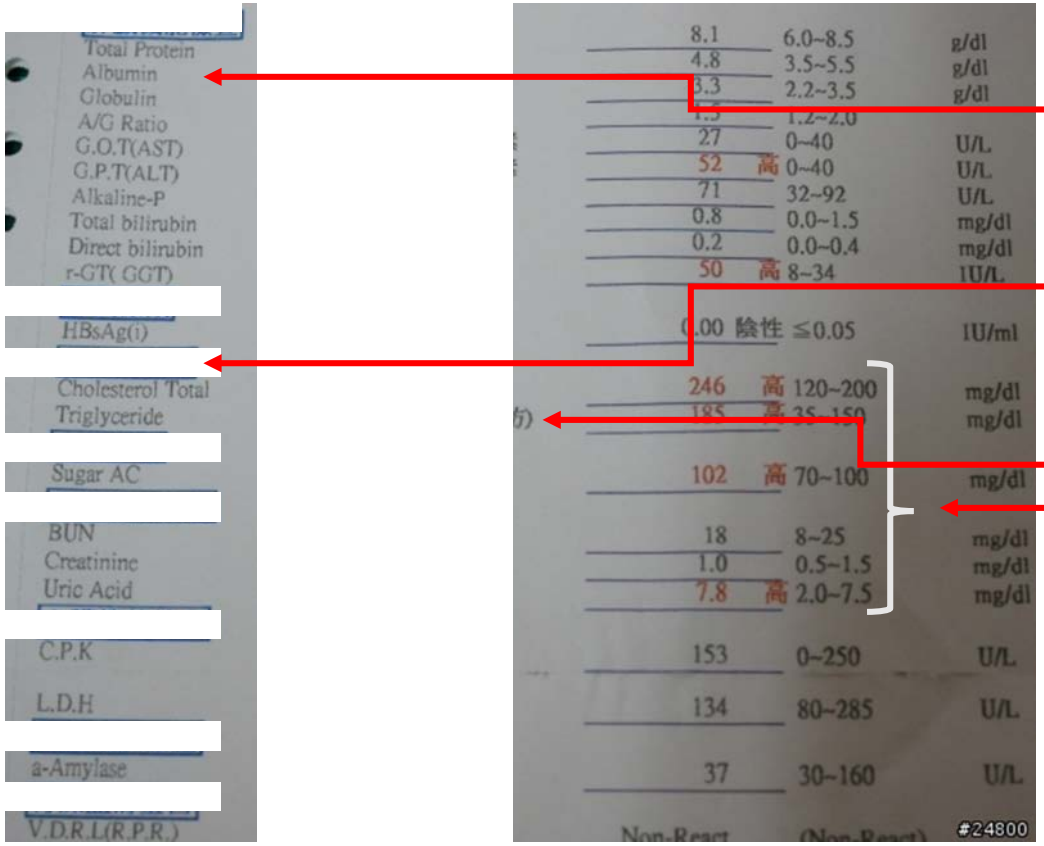
腹部超音波(肝臟) Liver	輕度脂肪肝；肝臟數顆囊腫，大小小於2公分	
腹部超音波(膽囊) Gallbladder	無異狀	

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 $10^3/\mu L$	11.8		17.1	11.6		7.5
RBC	4.5~5.9 $10^6/\mu L$	4.41		3.88	3.53		4.09
Platelet	150~440 $10^3/\mu L$	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

UNIFORCE 創泓科技

我不明白你的明白...@@

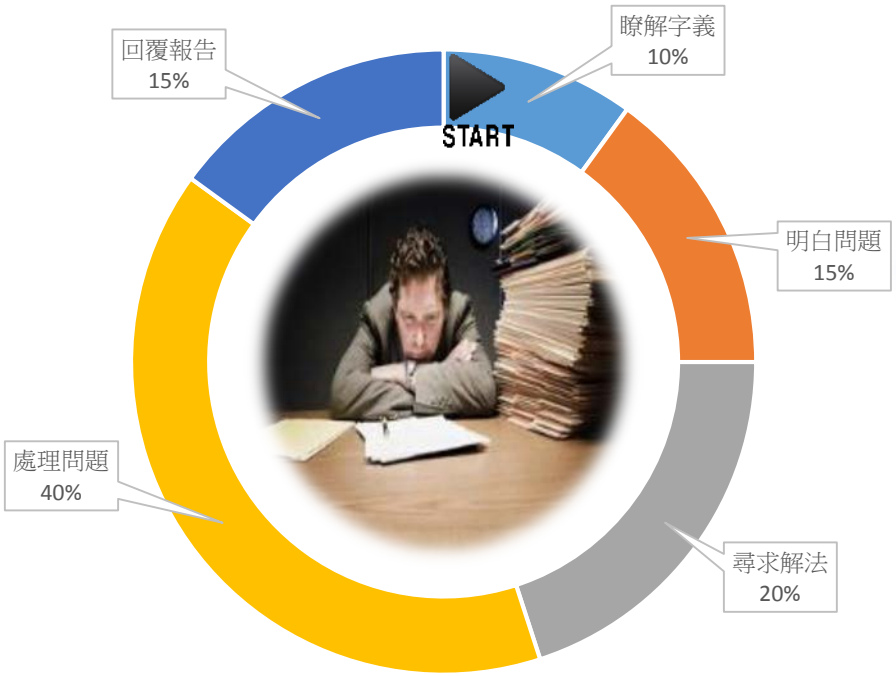


主要的問題

- ○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

UNIFORCE 創泓科技

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)

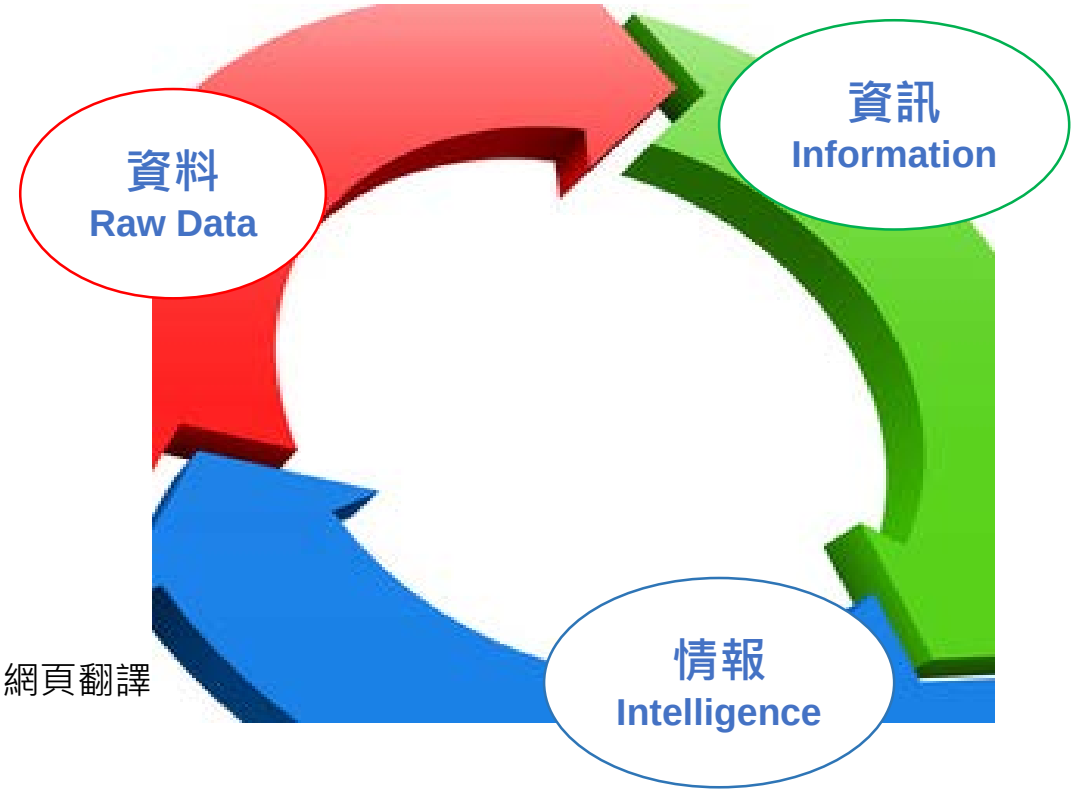
UNIFORCE 創泓科技

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)

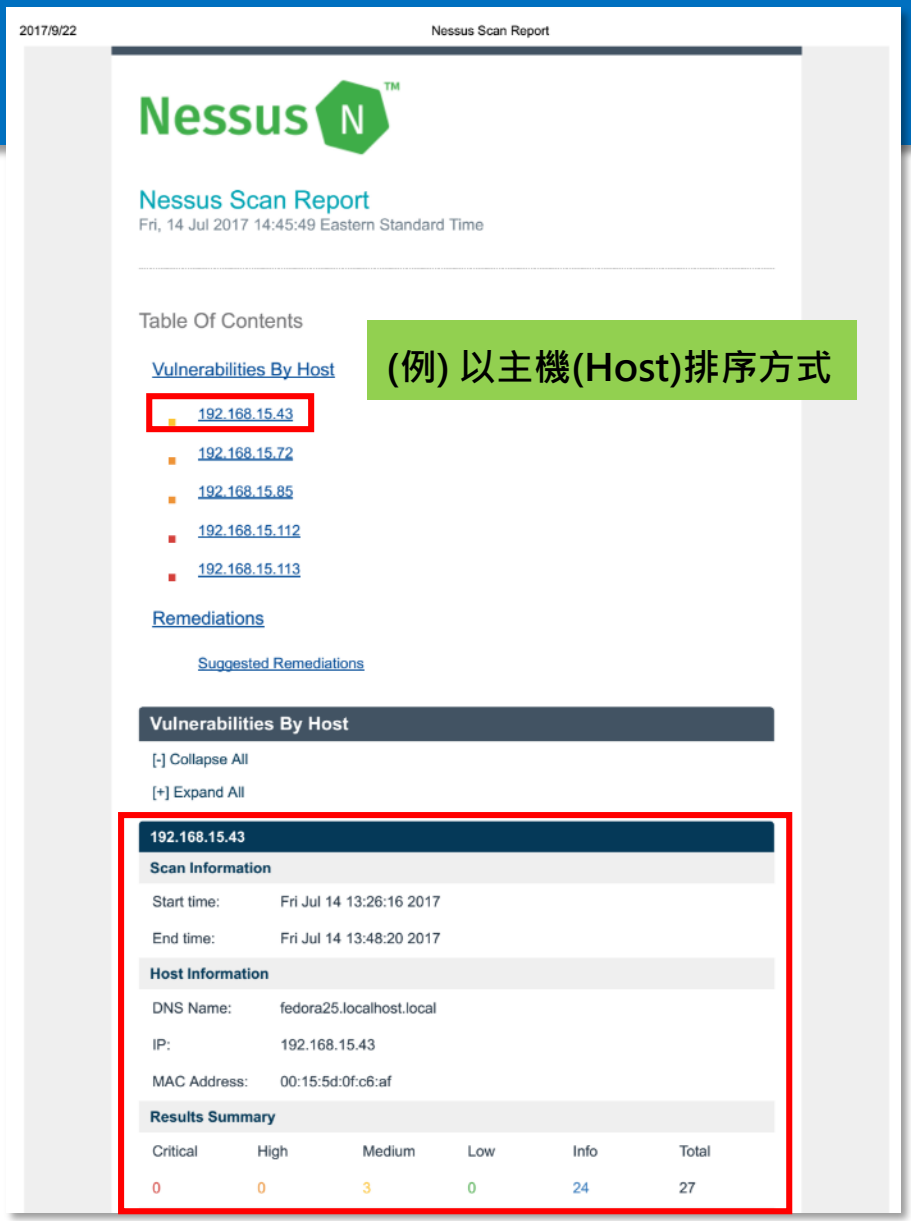
建立方便看懂的弱掃報告

- **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

UNIFORCE 創泓科技



UNIFORCE 創泓科技

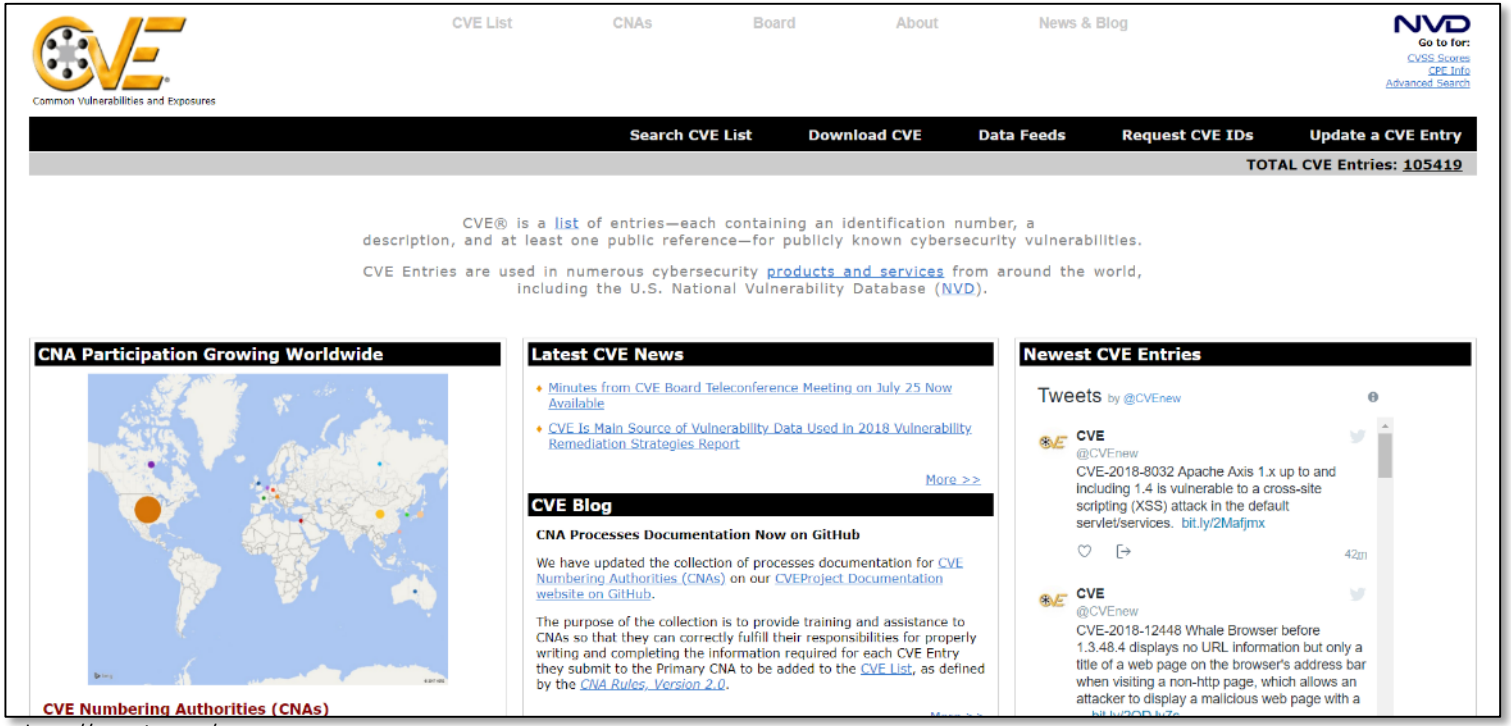
報告範本(高階)

UNIFORCE 創泓科技

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/

UNIFORCE 創泓科技

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.

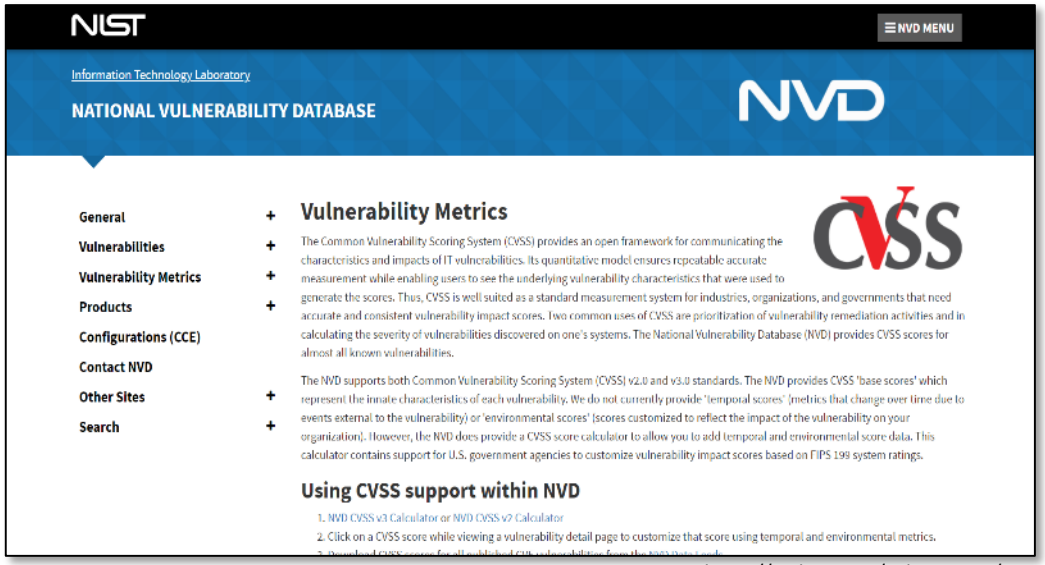
SMB弱點

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.	

UNIFORCE 創泓科技

CVSS (通用弱點評分系統)

Common Vulnerability Scoring System



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

NVD Vulnerability Severity Ratings

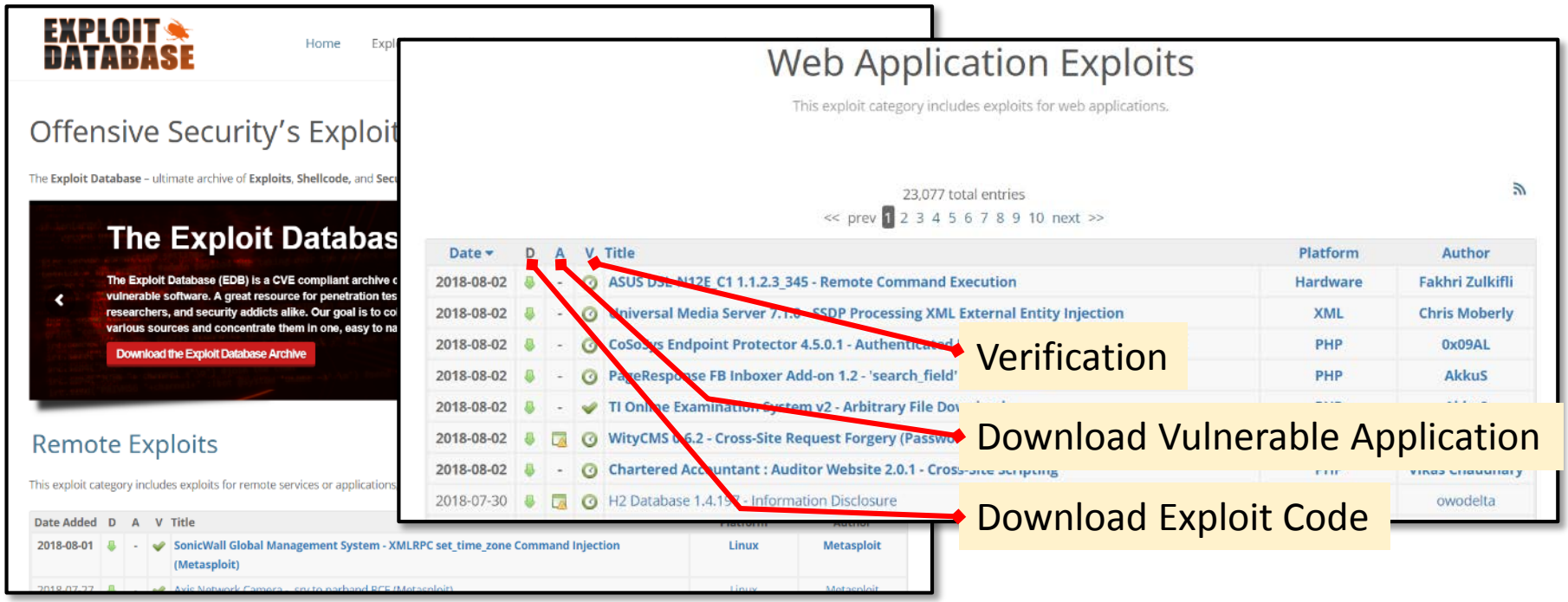
CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

- 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*。

UNIFORCE 創泓科技

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/

UNIFORCE 創泓科技

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。

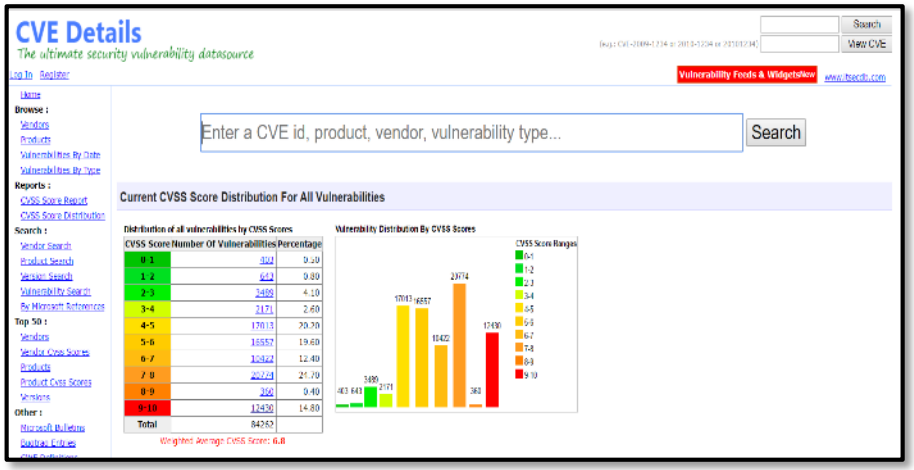
根據Bleeping Computer表示，EternalRocks可能會繞過電腦防毒軟體的偵測，造成受害者不易察覺遭入侵，而且，它沒有設置kill switch的功能，快速在網路上掃描易遭攻擊的電腦IP，隨機發動攻擊，不僅如此，駭客能夠利用EternalRocks和其他惡意程式結合，如勒索軟體、銀行木馬、RATs和其他攻擊程式。

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

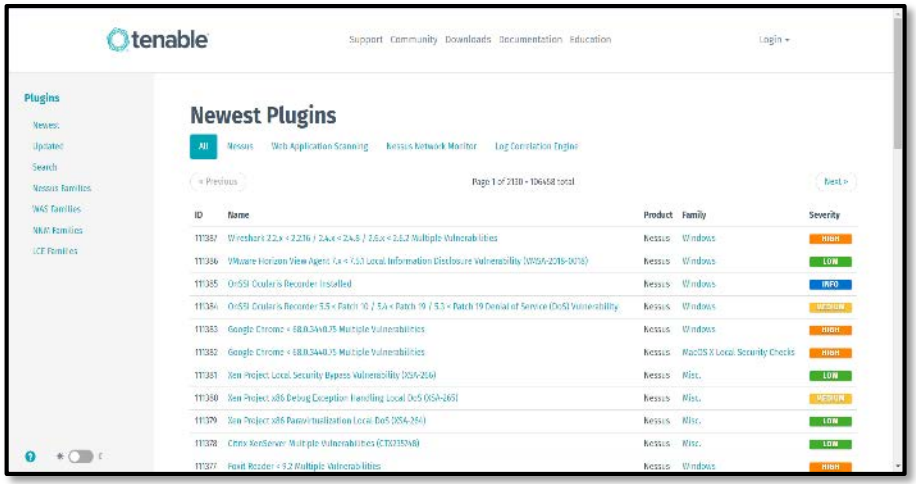
UNIFORCE 創泓科技

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

UNIFORCE 創泓科技

善用網路資源查找資安資訊

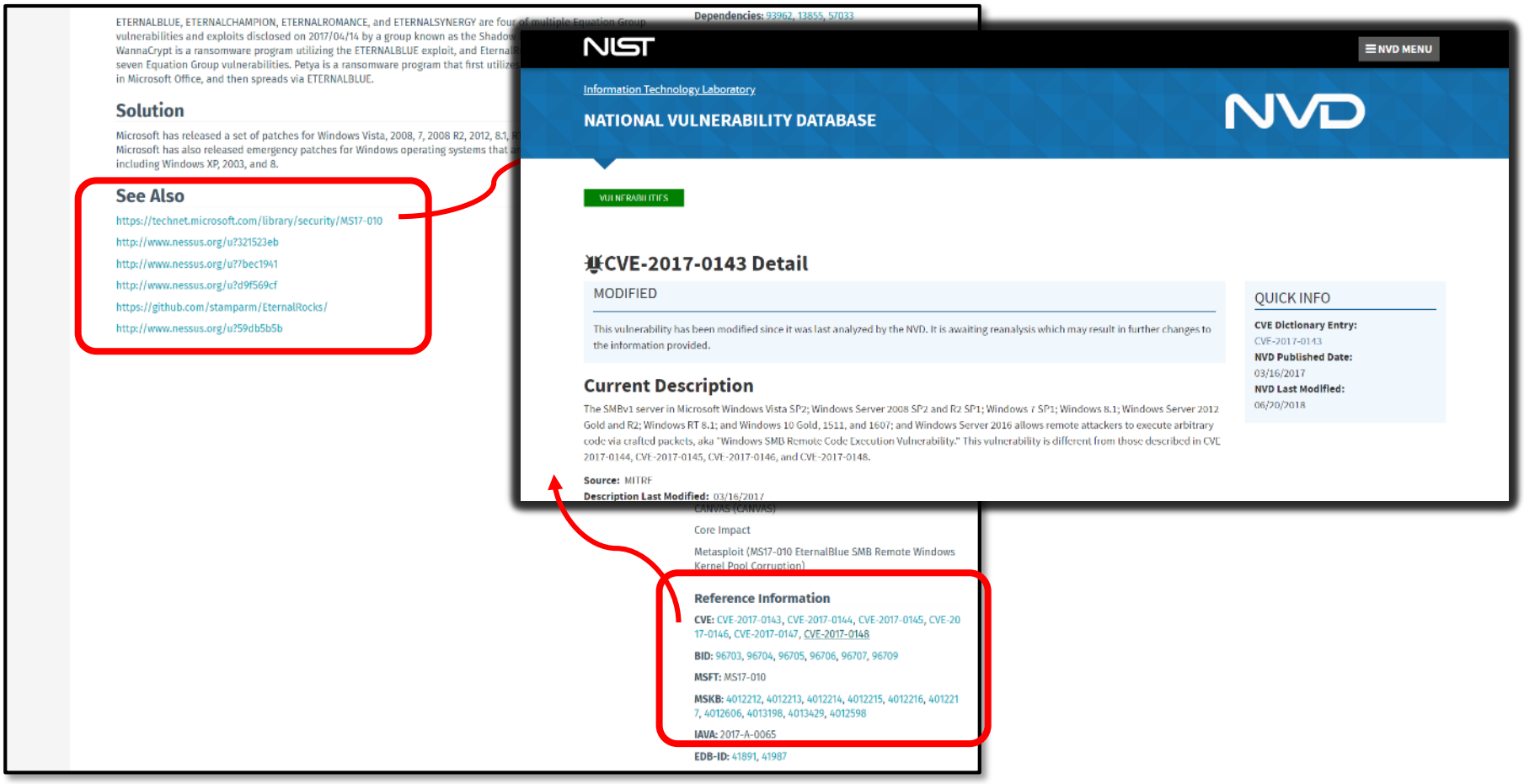
- 國內主要IT資安媒體

- 全球主要的搜尋引擎

UNIFORCE 創泓科技

善用工具(1) Google 網頁翻譯

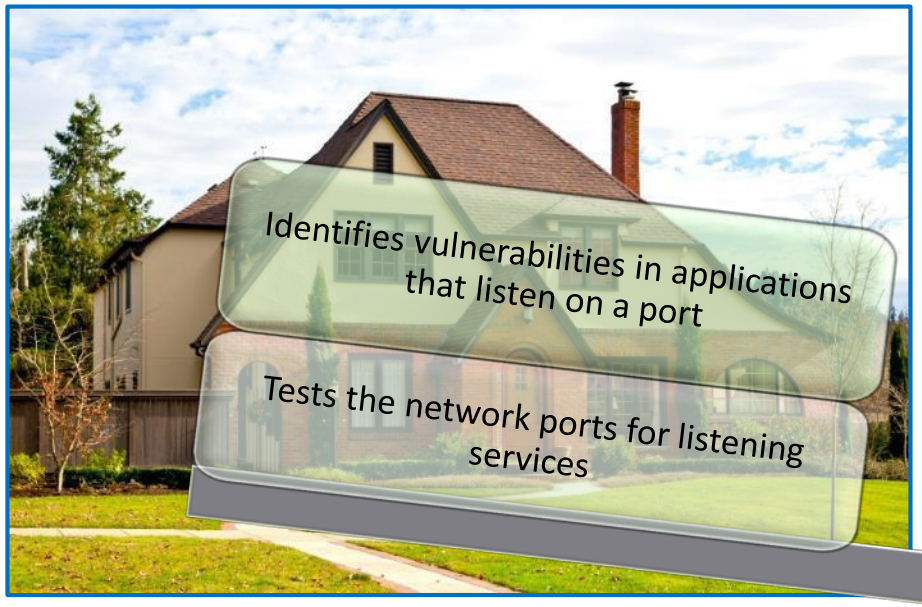
善用工具(2) 商業弱掃廠商的資訊資源



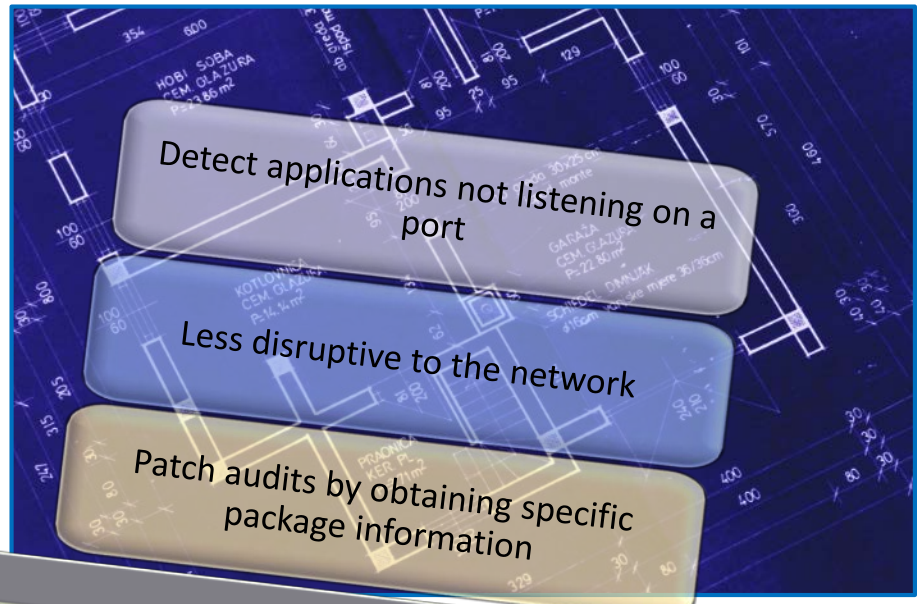
UNIFORCE 創泓科技

常見弱點掃瞄方式

網路掃描 (Network Scan)



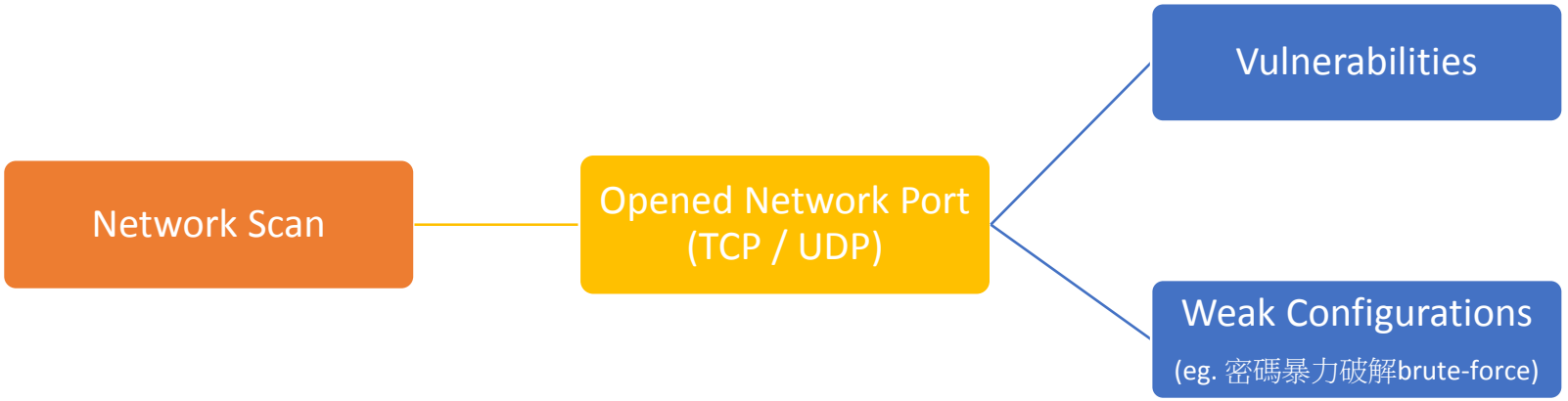
授權掃描 (Credential Scan)



UNIFORCE 創泓科技

常見弱點掃瞄方式: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

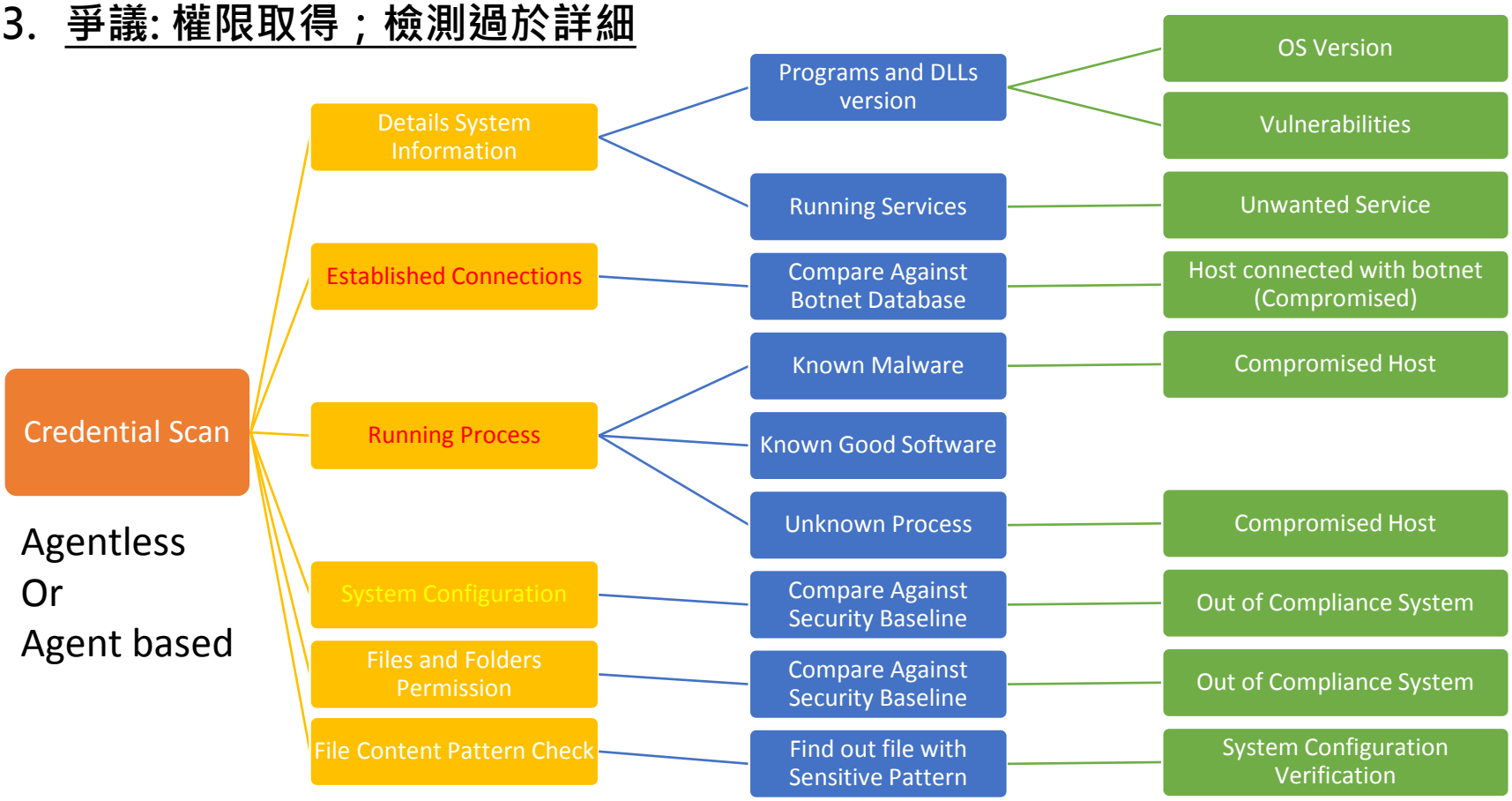


1. 需開放弱掃主機的IP
2. 需允許所有的Port (UDP/TCP)
3. 建立大量的Port Scans及Sessions
4. 耗用網路傳輸頻寬

UNIFORCE 創泓科技

常見弱點掃瞄方式: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



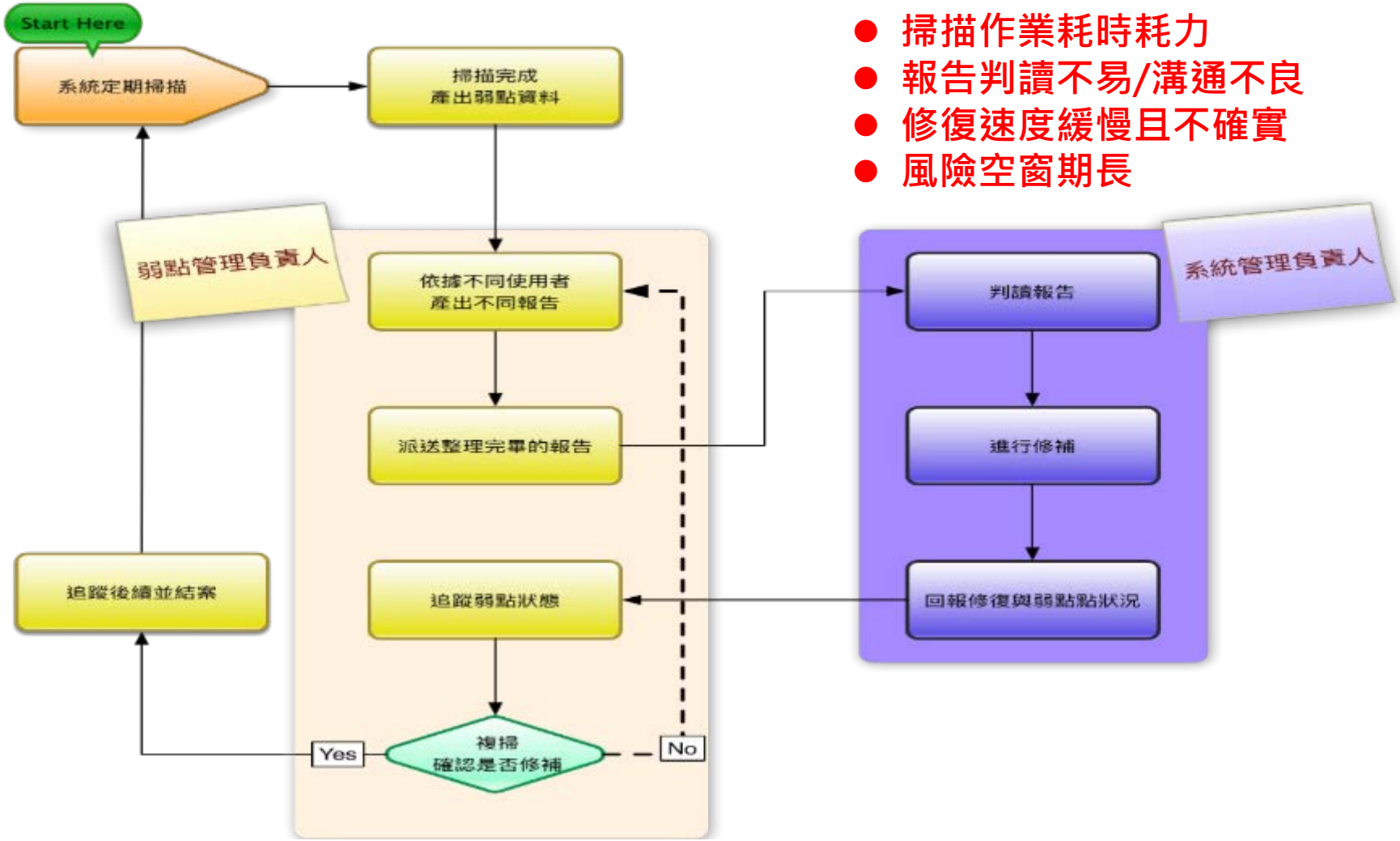
UNIFORCE 創泓科技

大綱簡介

- 前言
- 為什麼一定要掃描
- 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

UNIFORCE 創泓科技

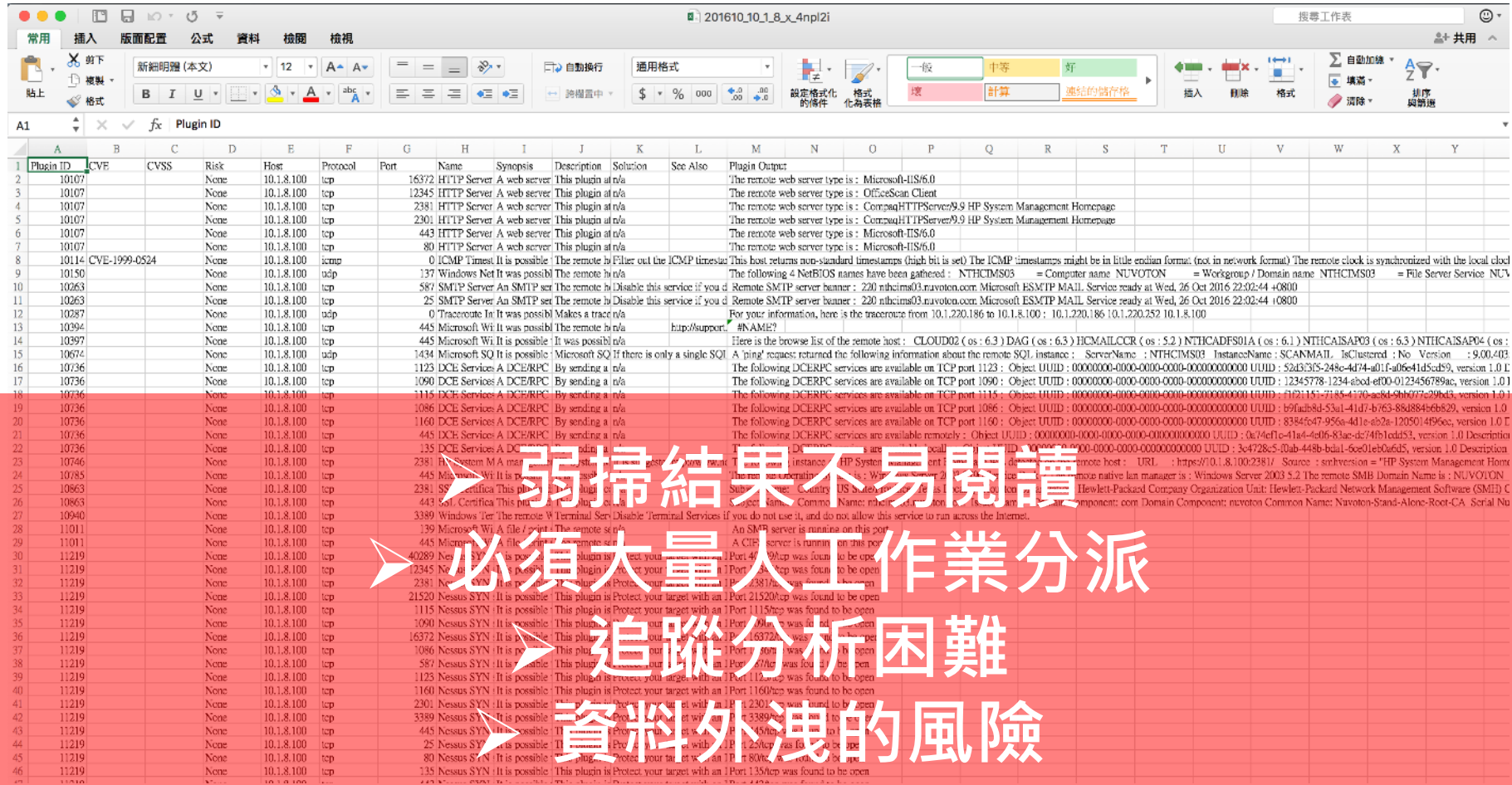
弱掃執行的困擾



- 掃描作業耗時耗力
- 報告判讀不易/溝通不良
- 修復速度緩慢且不確實
- 風險空窗期長

UNIFORCE 創泓科技

弱掃報告閱讀困難

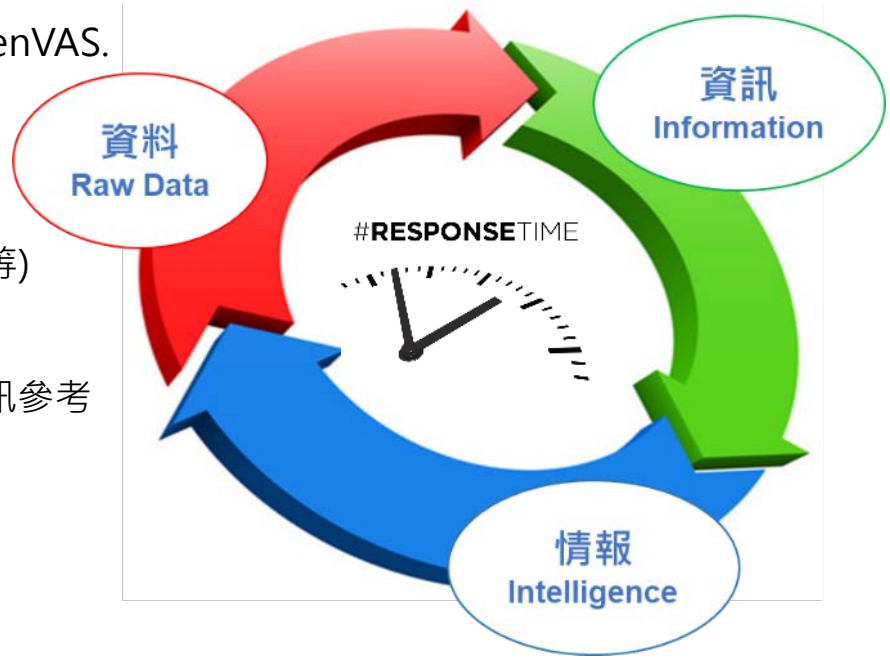


- 弱掃結果不易閱讀
- 必須大量人工作業分派
- 追蹤分析困難
- 資料外洩的風險

UNIFORCE 創泓科技

合適自己的弱掃工具

- **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**



UNIFORCE 創泓科技

工具影響弱點管理方法的建立

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)

管理者群組建立:

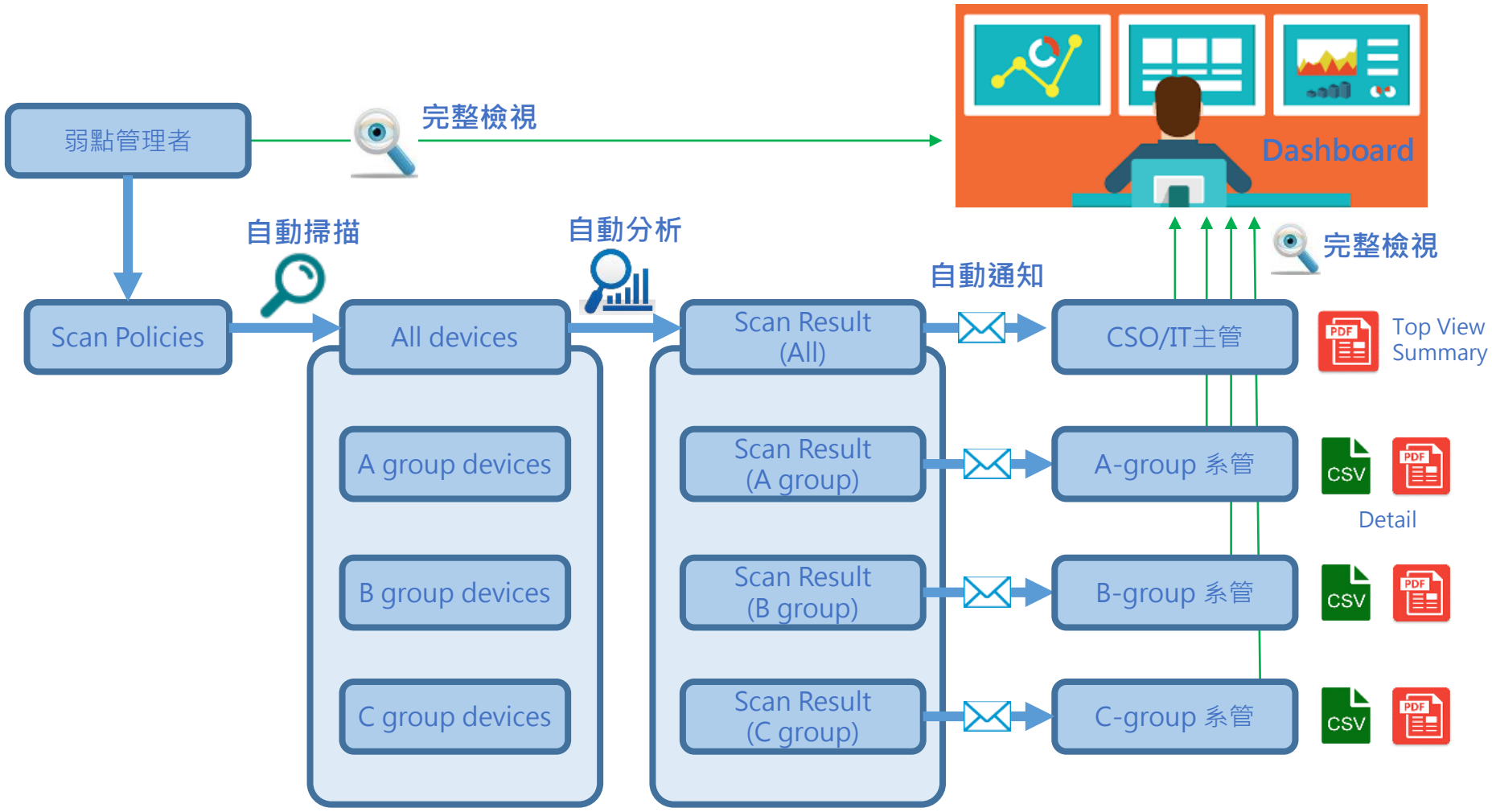
- 群組: 網路(網段)、主機、系統、專案負責.
- 權限: 檢視權限、管理範圍、弱掃執行、風險管理

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

UNIFORCE 創泓科技

弱掃作業自動化



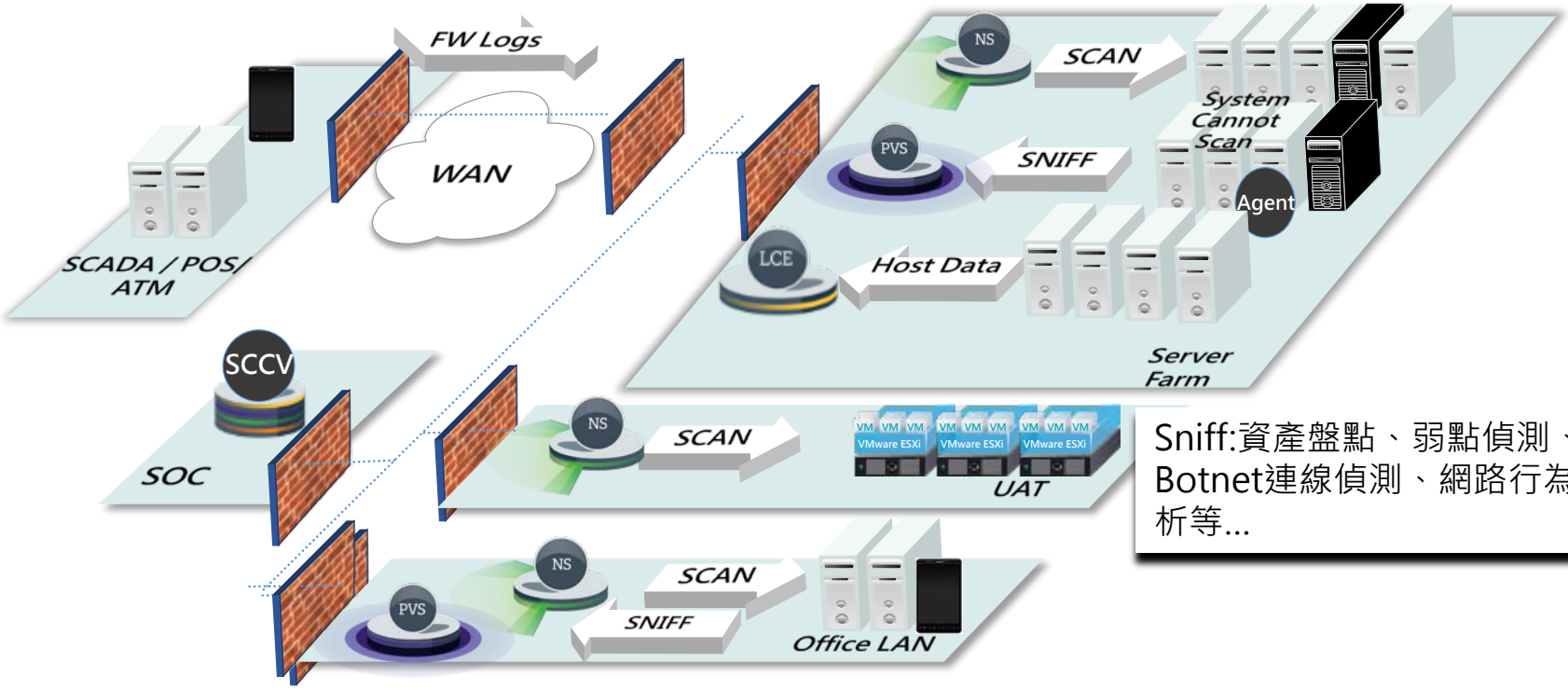
UNIFORCE 創泓科技

弱掃部署架構設計

分散式部署/集中化監控/分權管理模式

Host Data: 資產盤點、弱點偵測、主機活動等...

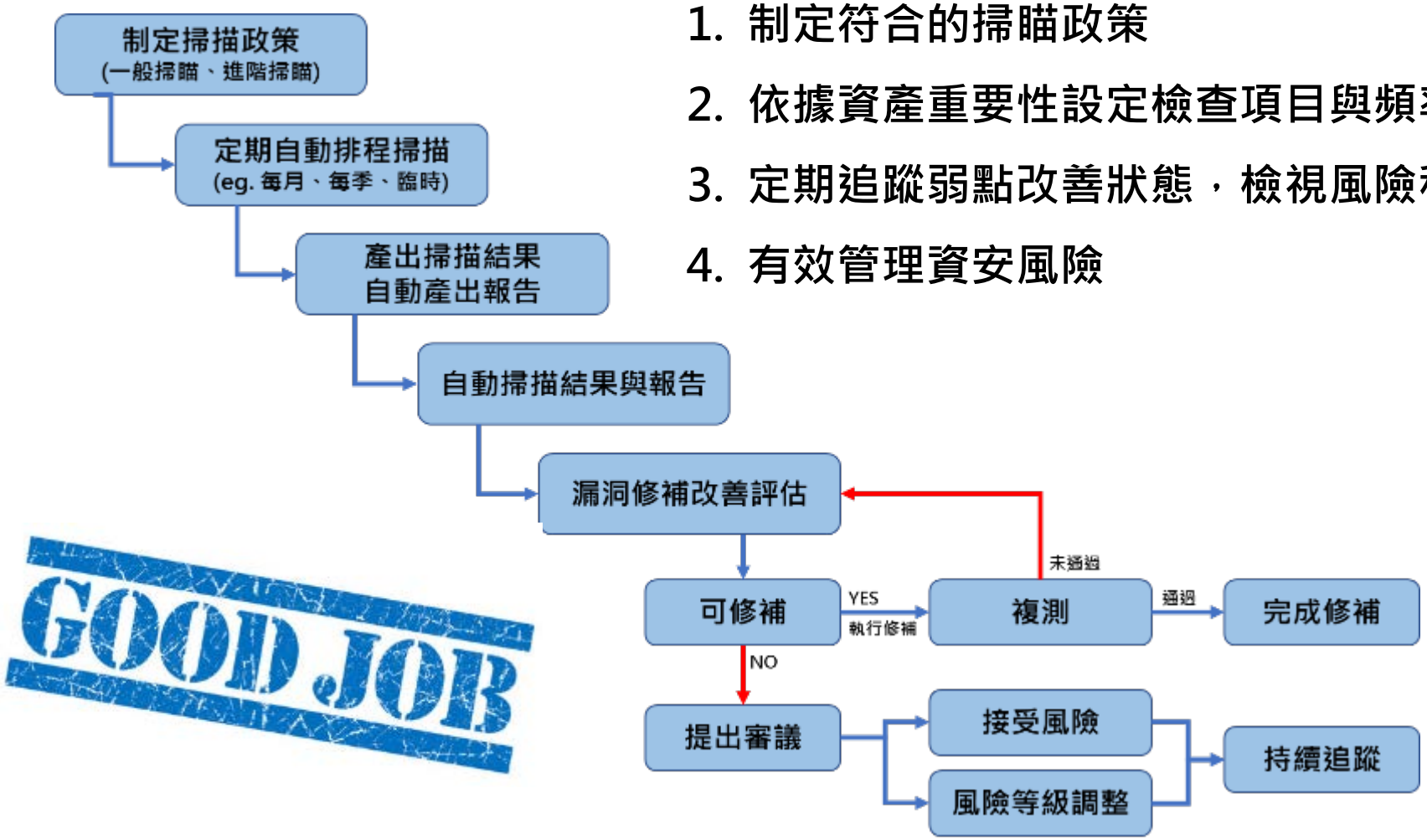
Scan:資產盤點、弱點偵測、惡意程式偵測、設定檔稽核等...



Sniff:資產盤點、弱點偵測、Botnet連線偵測、網路行為分析等...

UNIFORCE 創泓科技

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

UNIFORCE 創泓科技

整體弱點狀態檢視

TopN 排行方式

前10大弱點項目

Plugin ID	Name	Family	Severity	Tot
51192	無法信任 SSL 憑證	General	Medium	8
57582	SSL 自我簽署憑證	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

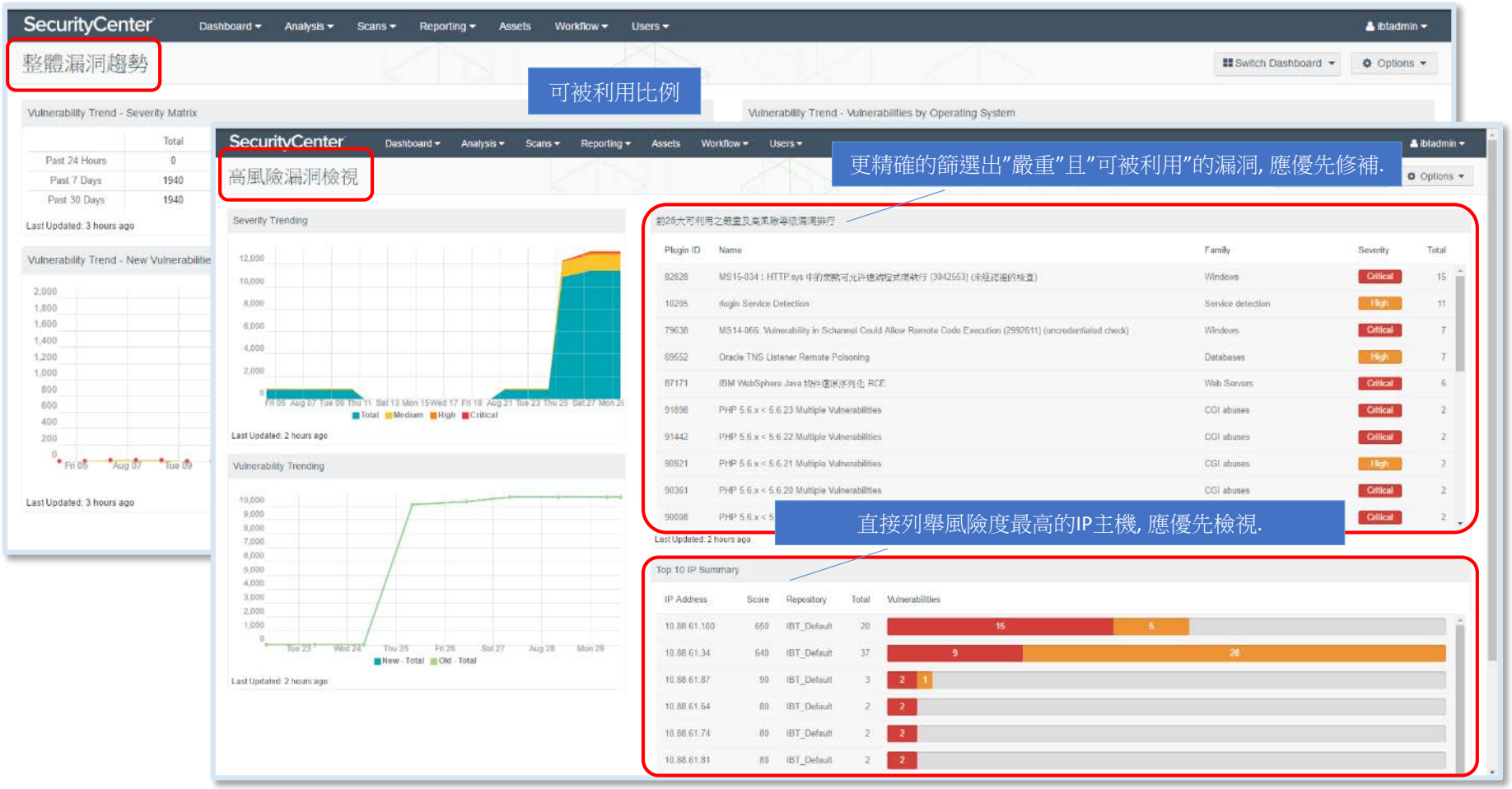
前10大IP列表

IP Address	Score	Repository	Total	Vulnerabilities
192.168.3.15	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	123
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	1	DMZ	5	
192.168.3.3	0	DMZ	1	
192.168.3.4	0	DMZ	1	

Last Updated: 3 days ago

UNIFORCE 創泓科技

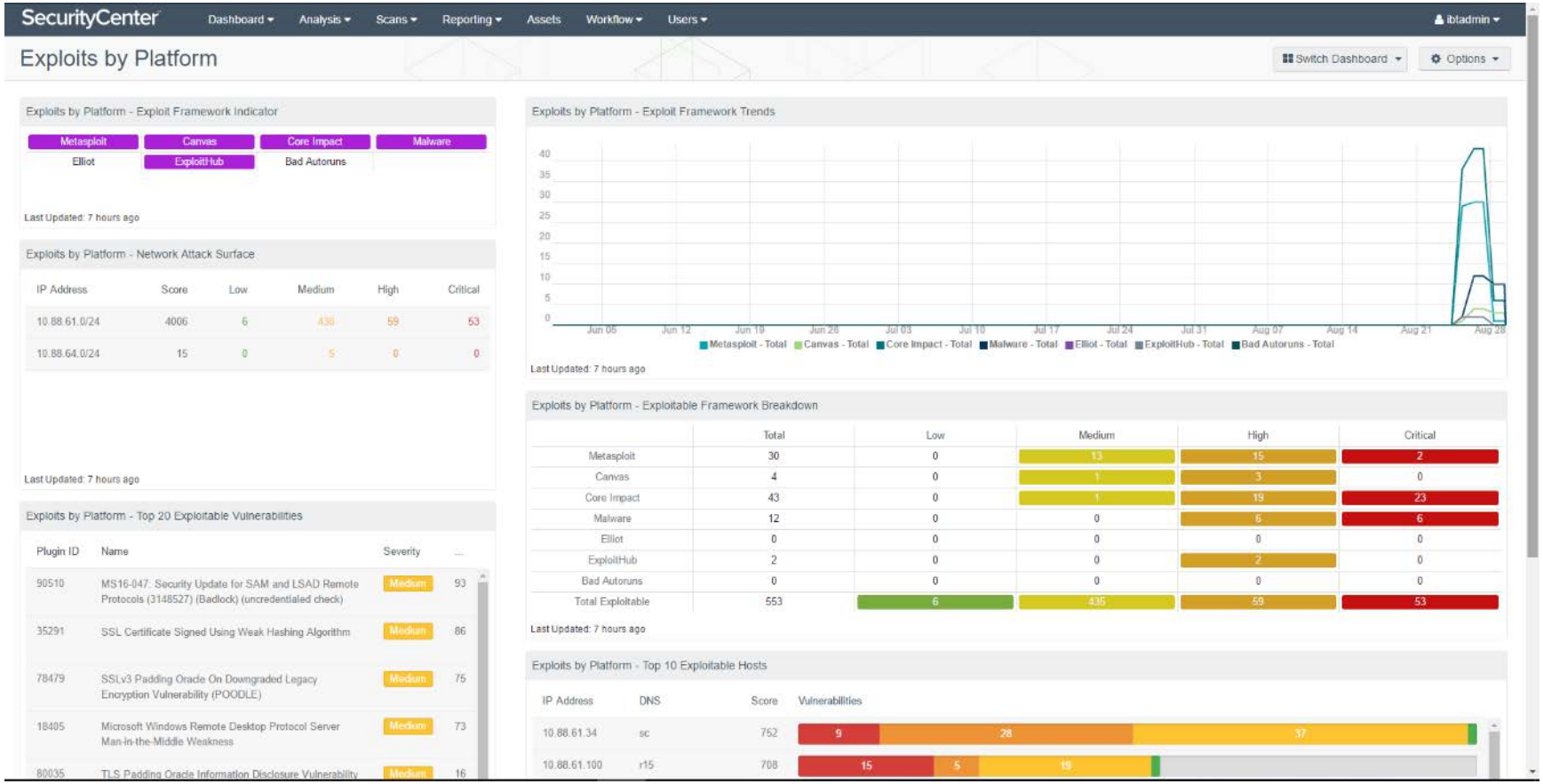
弱點分布情報快速檢視



UNIFORCE 創泓科技

可利用弱點分析

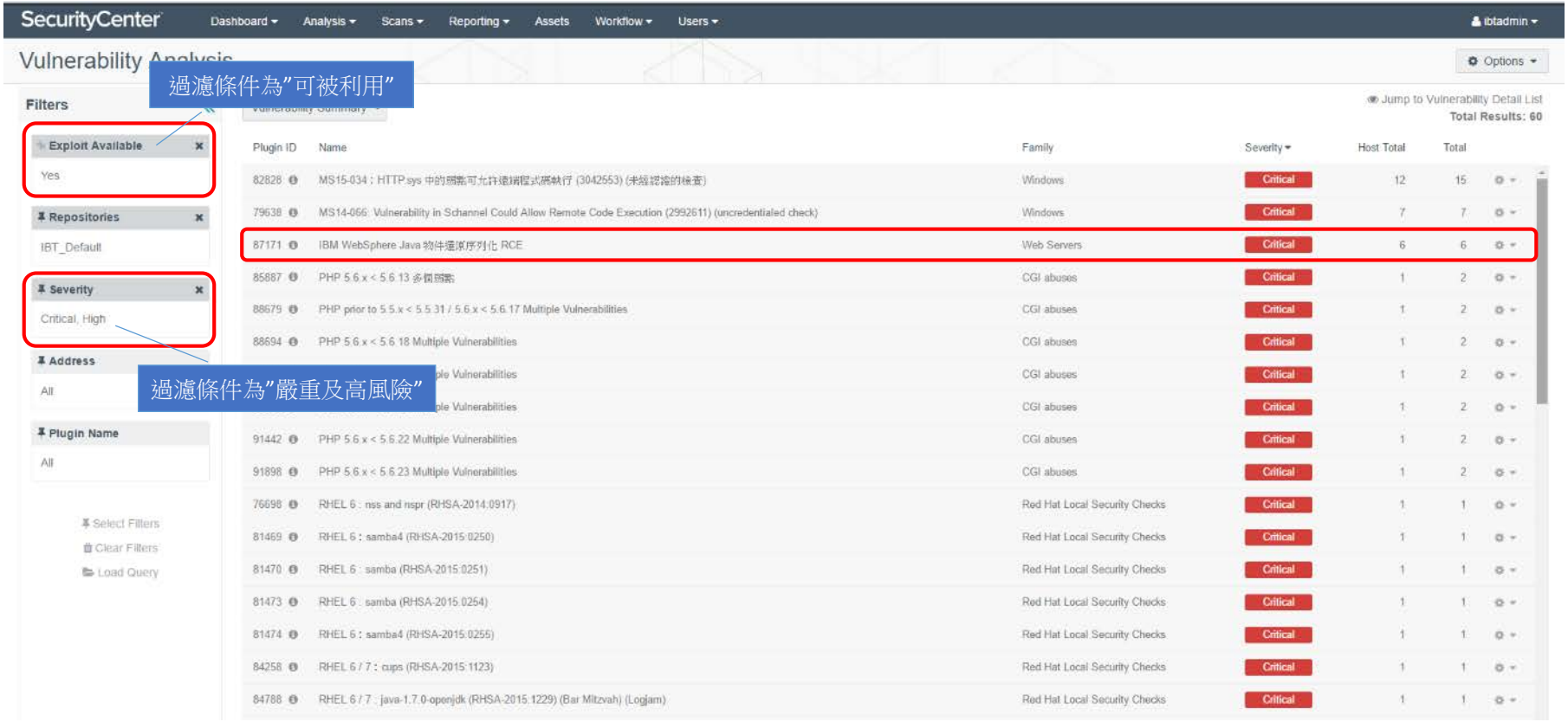
可利用弱點套件(Exploitable)分析



UNIFORCE 創泓科技

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.



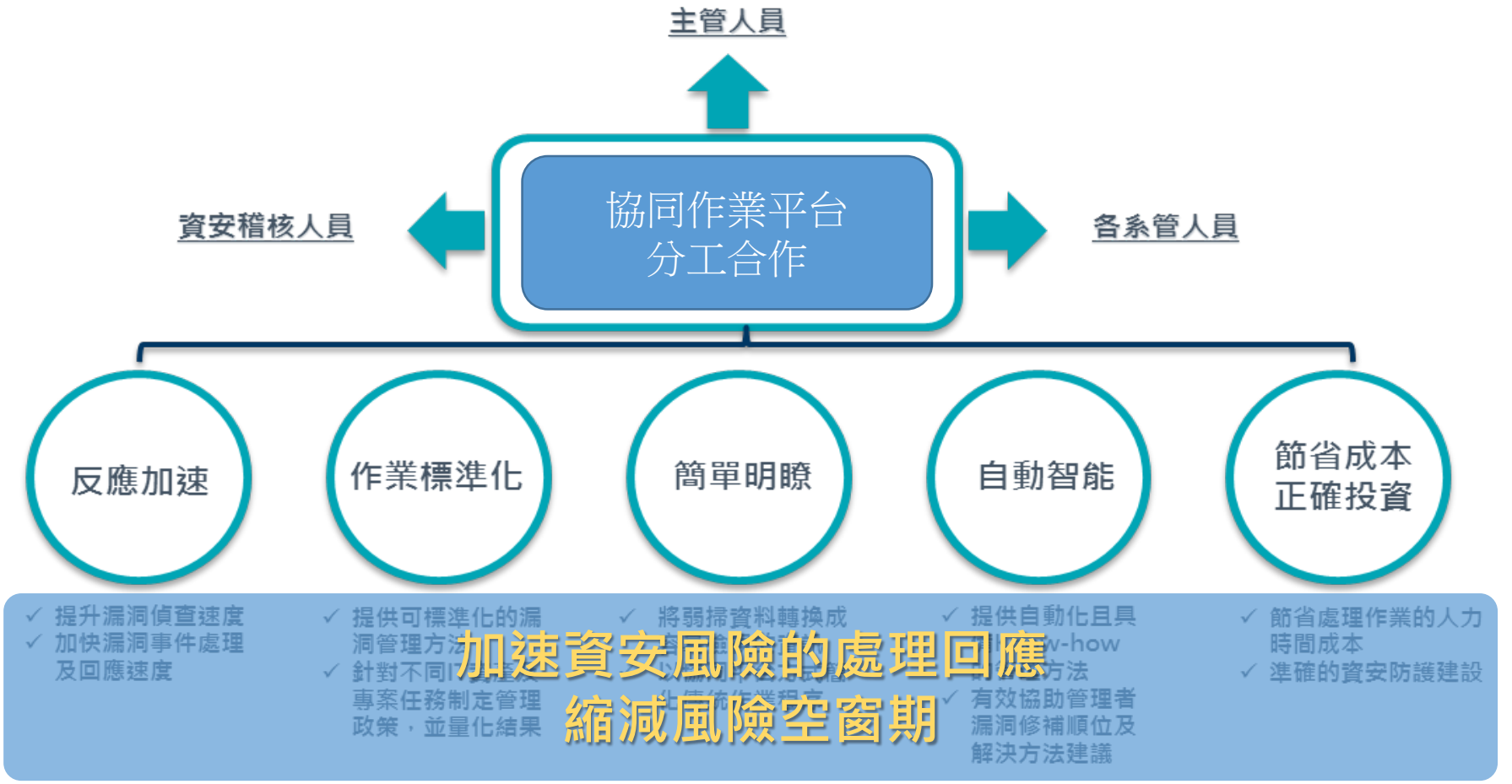
UNIFORCE 創泓科技

弱點資訊與建議取得

詳細的漏洞資訊、改建建議、及管理.

UNIFORCE 創泓科技

新型態弱掃管理的效益訴求



UNIFORCE 創泓科技

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)	執行弱點掃瞄作業 (15天)	弱掃結果彙整分析 (10天)	弱點結果派送 (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.	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.	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.	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

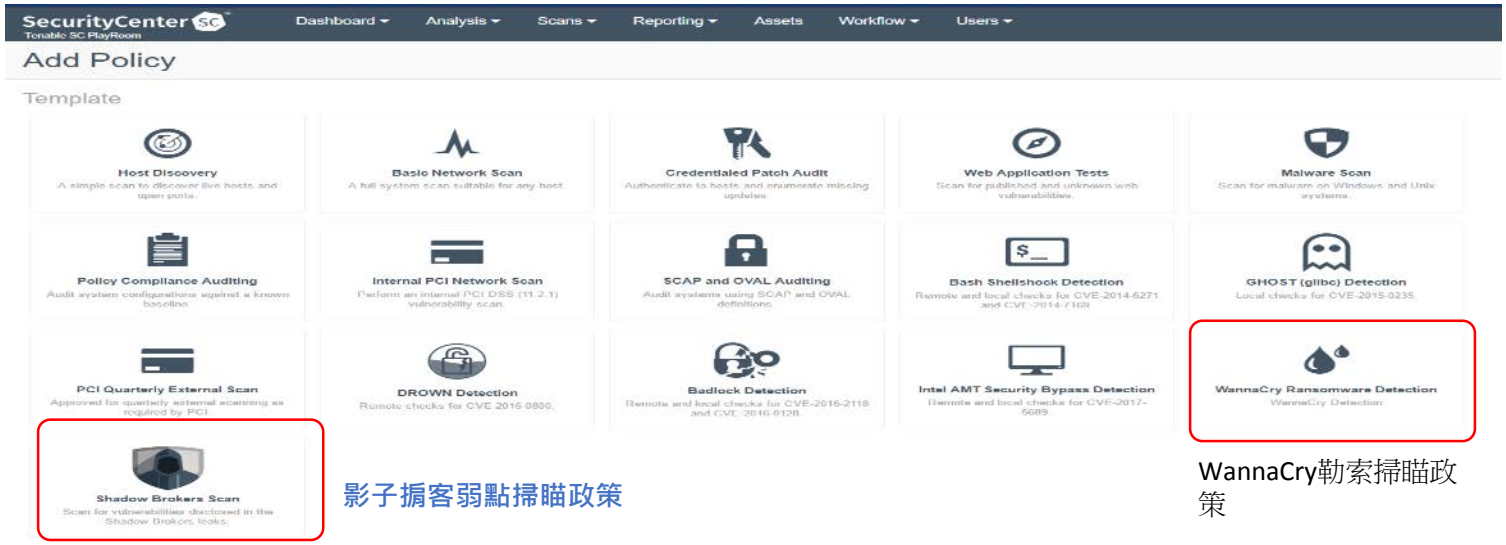
確認弱點資訊 (1天)	執行弱點掃瞄作業 (3-5天)	弱掃結果彙整分析 (1天)	弱點結果派送 (1天)
本次專案弱掃系統廠商提供快速的情報資訊，弱點資料更新頻率為每日更新，可減少弱點資訊搜找的時間.	本次專案弱掃系統提供多個弱點掃描器的授權部署，並且可由中央管理設定排程自動執行掃瞄作業，並將掃描結果自動回報儲放於中央系統. 並且可以僅針對指定的弱點項目(如本次WannaCry)進行指定盤查，可減少掃瞄作業對主機的耗能與時間. 整體可加速弱掃速率，並減少作業所耗用的人力時間成本.	本次專案弱掃系統於弱掃作業過程便已將結果回報儲放於中央系統資料庫，可直接套用相關的報告範本(如WannaCry)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.	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

UNIFORCE 創泓科技

Case Study

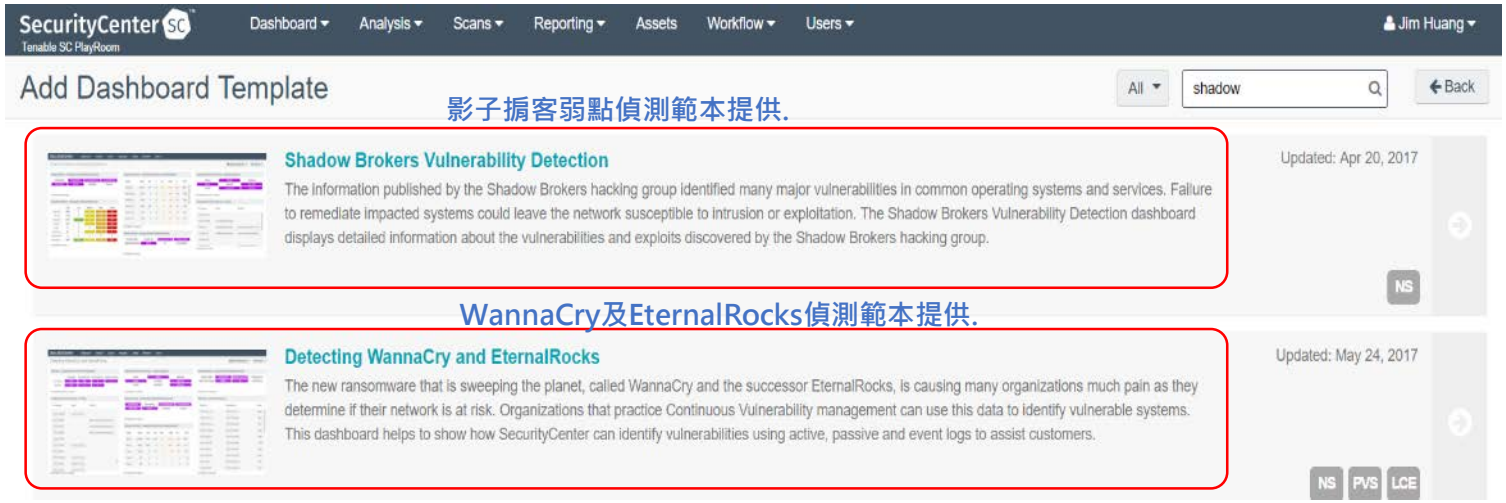
提供重大威脅的弱點掃瞄政策，管理者可直接選用.



影子掮客弱點掃瞄政策

WannaCry勒索掃瞄政策

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.



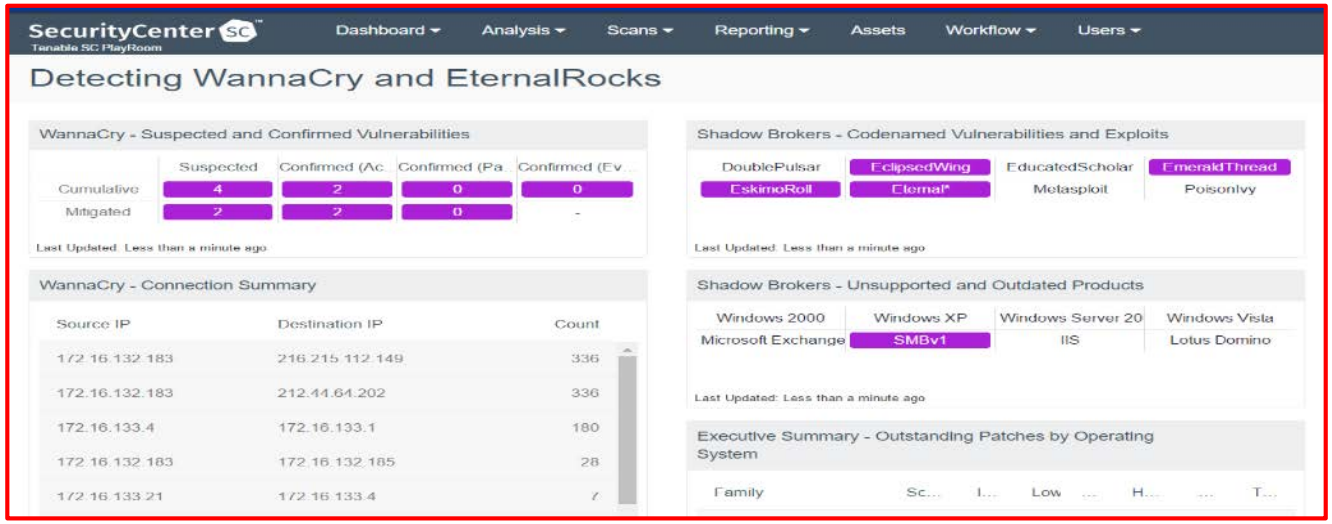
影子掮客弱點偵測範本提供.

WannaCry及EternalRocks偵測範本提供.

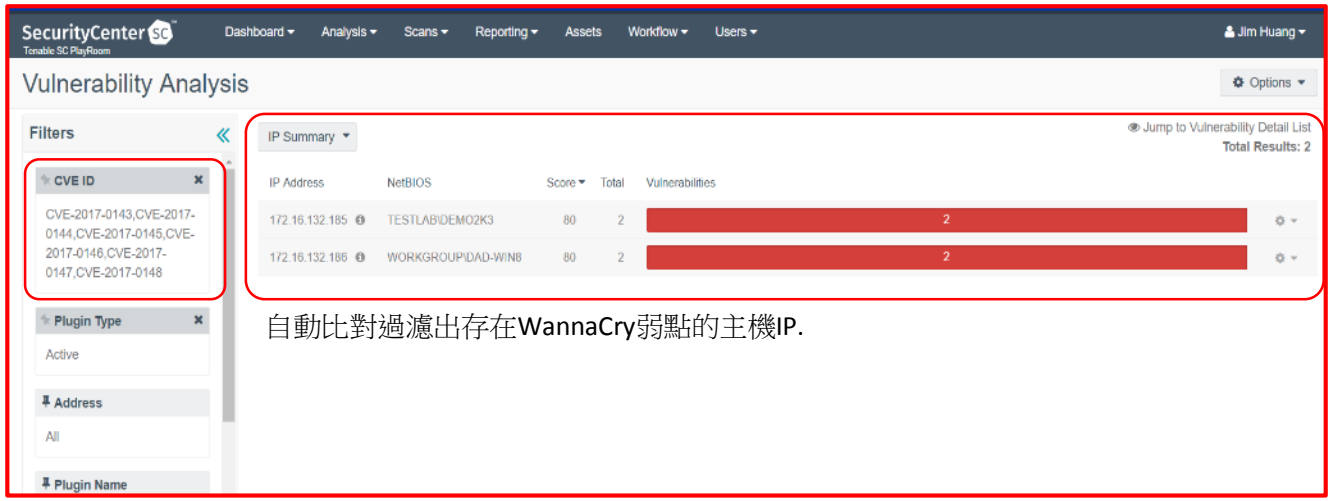
UNIFORCE 創泓科技

Case Study

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



自動套用WannaCry相關的弱點項目進行過濾.



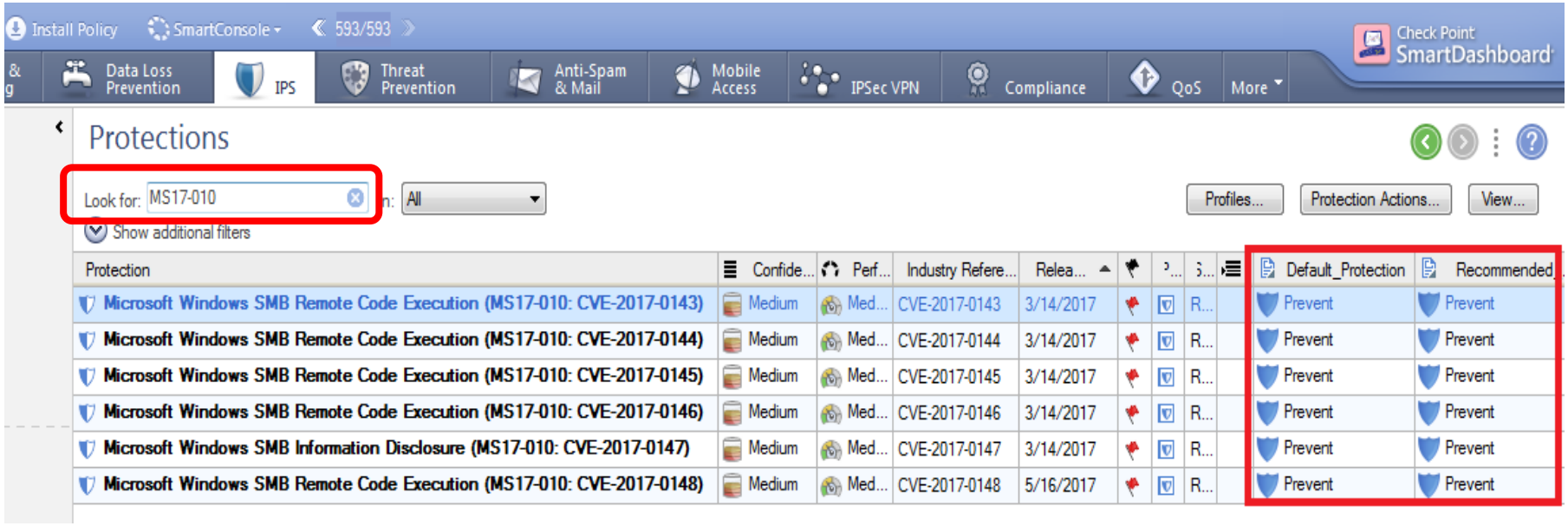
自動比對過濾出存在WannaCry弱點的主機IP.

UNIFORCE 創泓科技

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.



UNIFORCE 創泓科技

“天下武功无坚不摧，
唯快不破！

——— 李小龍

UNIFORCE 創泓科技

Q & A

UNIFORCE 創泓科技