「弱點掃描 vs. 滲透測試」傻傻分不清?!

黃繼民 | 創泓科技-資深技術顧問

UNIFORCE 創泓科技

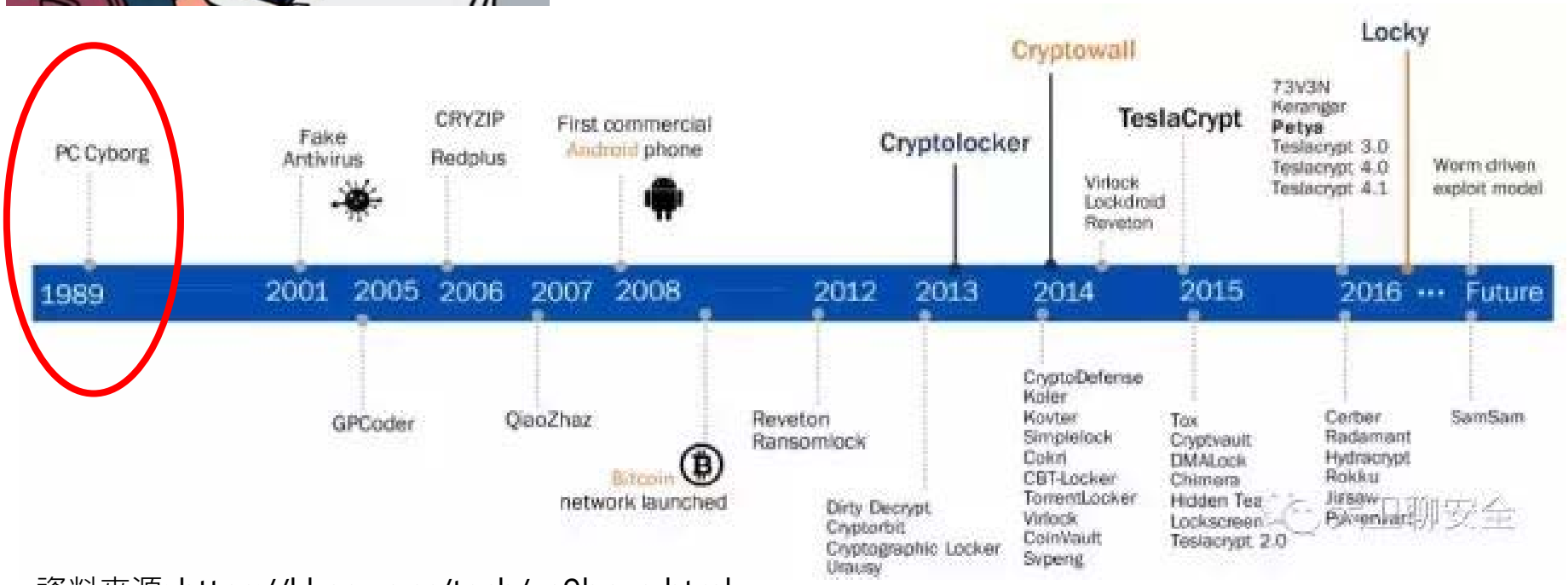
大綱介紹

- 新世代資安威脅的樣貌
- 弱點不是病, 弱起來要人命
- 弱點掃瞄與滲透測試的微妙關係
- 正視弱點才能掌控資安風險
- 面對更多未知的驚奇
- Q&A

UNIFORCE 創泓科技

資安威脅分析

勒索威脅當道



資料來源: https://kknews.cc/tech/va9bnzq.html

UNIFORCE 創泓科技

加密勒索軟體運作方式

管道媒介

1) 攻擊者利用社交工程的方法，含有勒索軟體或釣魚連結的郵件發送到用戶的郵箱，或者在某些網站通過掛馬的方式，誘騙用戶點擊。

利用關鍵

2) 用戶運行惡意文件或點擊釣魚連結後，勒索程序將利用終端系統存在的漏洞，在終端安裝並運行，並且有可能向C&C主機發起連接請求。

準備程序

3) 惡意程序連接到C&C主機後，基於受害者終端的特定信息生成密鑰組，並將公鑰下載到終端上。

執行運作

4) 勒索軟體在後台檢索文件，同時生成AES密鑰對檢索到的文件進行加密處理；加密完成後用RSA的公鑰再將AES密鑰進行加密，並保存到文件中。

得手

5) 攻擊者發出勒索信息，以各種方式通知用戶支付贖金。

乖乖付贖金 | **災害備份還原** | **駭客大發慈悲** | **破解加密金鑰** | **放棄 Game Over**

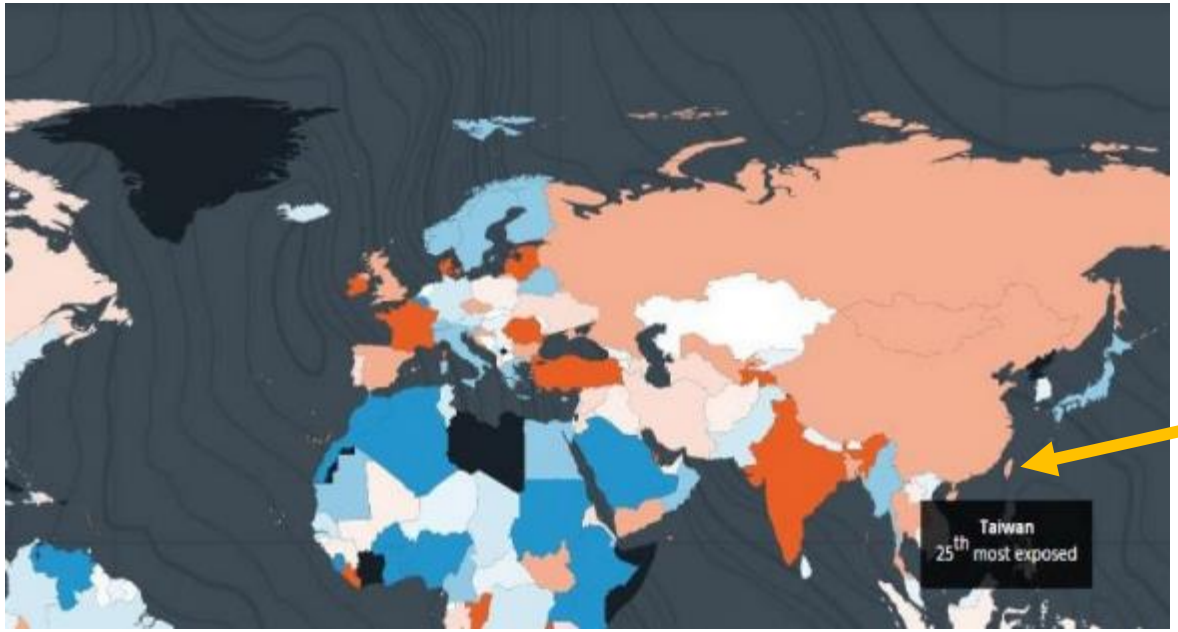
UNIFORCE 創泓科技

案例: WannaCry (想哭) 加密勒索威脅

UNIFORCE 創泓科技

案例: WannaCry (想哭) 加密勒索威脅

- 2017年5月爆發史上影響最大的全球性勒索蠕蟲事件.
- 五個小時內影響覆蓋美國、俄羅斯、整個歐洲等100多個國家. (超過20多萬台電腦受害)
- 中國多個高校校內網、大型企業內網和政府機構專網中招.
- SMB 漏洞MS17-010，微軟已在今年3月份發布了該漏洞的補丁.
- 嚴重程度之高，微軟破例釋出Win XP及Win Server 2003等系統修補. (最近一次: 2014年)

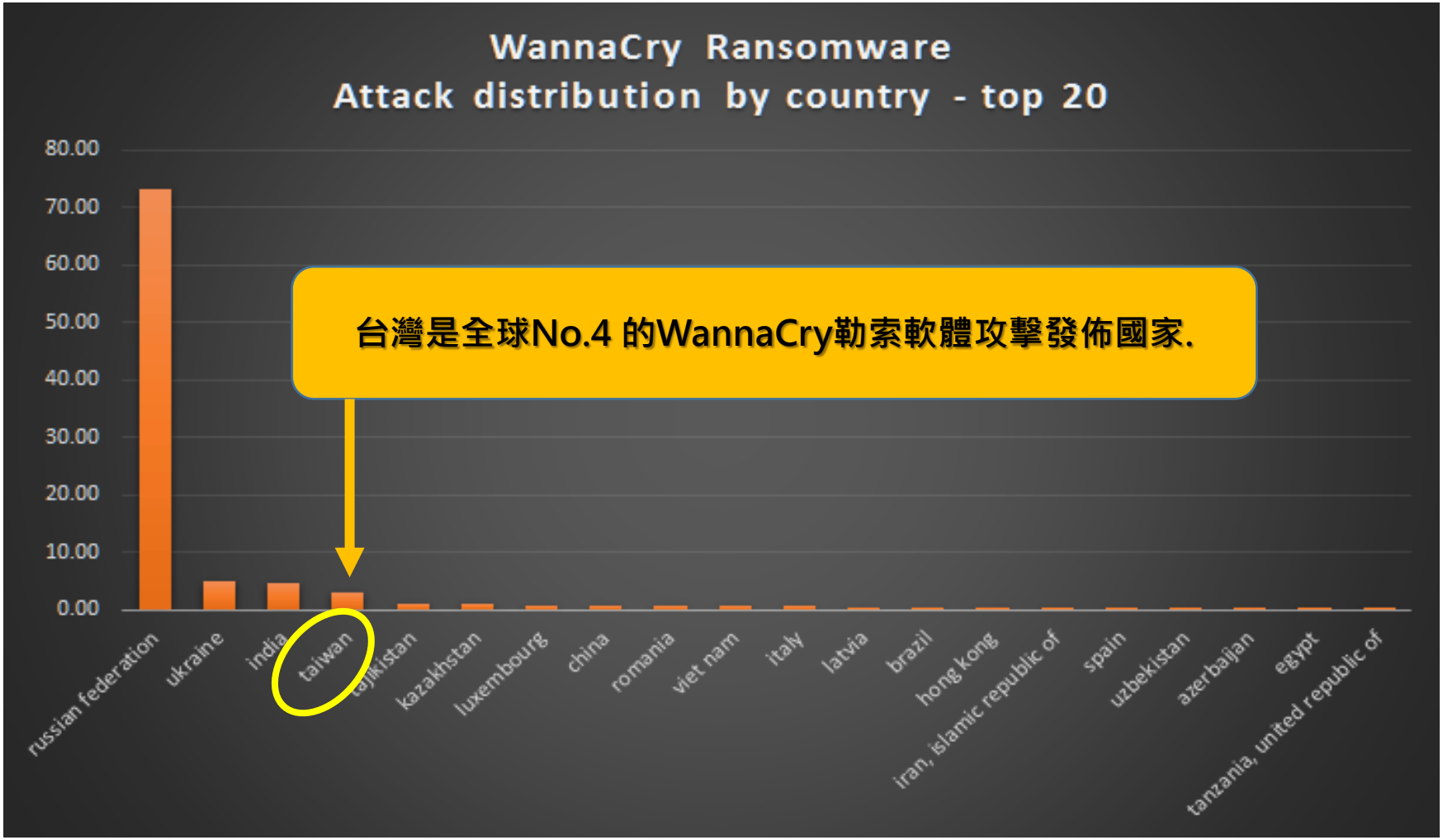


WannaCry肆虐全球時，全球網路有超過500萬個開放的SMB節點.
根據各國IP數量及服務曝光數量加以排名，台灣排名第25.

資料來源:
Rapid7 National exposure index 2017

UNIFORCE 創泓科技

案例: WannaCry (想哭) 加密勒索威脅



資料來源: Securelist.

UNIFORCE 創泓科技

案例:「想哭」變種... Petya & Not Petya...

標題	[國際]Petya勒索軟體作者公開解密主密鑰，可以解Petya系列但不適用notpetya (petwrap)
發佈日期	2017-07-12 12:56:59
參考位址	https://themerkle.com/original-petya-developer-releases-master-decryption-key-for-all-variants/

消息內容

●重點摘要：
1.2017年6月28日Not Petya勒索軟體造成許多國家多種災情，而近日Petya勒索軟體的作者(自稱為Janus Cybercrime Solutions)則正式公開了他的解密主密鑰，可以用來解密遭到所有Petya家族加密的檔案。Petya家族一共有三個不同的版本，依照被感染後出現紅色、黃色以及綠色的骷髏頭而定。
2.雖然NotPetya是根據Petya變種而來，但NotPetya用了不同的加密方式，因此這組密鑰無法用來破解NotPetya的受害檔案。

●參考鏈結：
[1]https://themerkle.com/original-petya-devel
[2]http://www.techbang.com/posts/52462-pet
draw

UNIFORCE 創泓科技

案例: SambaCry加密勒索威脅

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

導入DevOps的25堂課！ 一站拓展IoT人脈與商機 14.2%企業願意聘用大資料人才

新聞

卡巴斯基：鎖定SambaCry漏洞的攻擊現身了，被用來開採Monero

卡巴斯基透過誘捕系統發現首個針對SambaCry的攻擊程式，但並非像WannaCry用來散佈勒索軟體，這支攻擊程式被用來植入虛擬貨幣Monero採礦工具，一個月來為駭客賺進98個Monero，約5500美元。

文/ 陳曉莉 | 2017-06-12 發表

讚 4.3 萬 按讚加入iThome粉絲團 讚 363 分享 G+

鎖定「SambaCry」漏洞的新威脅現身， Linux 使用者請盡速更新系統

POSTED ON 2017 年 07 月 20 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

Samba的資安弱點即使經過修補，新的弱點也陸續出現。趨勢科技近期發現駭客可利用SMB弱點 (CVE-2017-7494) 進行攻擊，影響範圍為Samba 3.5.0開始的所有版本。

除了Windows作業系統主機以外，Linux作業系統只要啟用SMB服務，也有可能遭受攻擊。駭客會利用此弱點攻擊 Linux 系統設備 (包含網路儲存設備 (NAS)、IoT設備)，一旦成功後即植入惡意程式。

企業環境 (政府、製造業、金融業) 大量使用 Linux 作業系統伺服器，且大部分均為關鍵業務系統。而Linux常被認為系統安全性高，較不會被入侵，因此較易疏於管理、更新、防護。駭客可能利用此情形，結合目標式攻擊與內網擴散手法攻擊此弱點，入侵至伺服器後加密檔案，進行勒索。因此，趨勢科技建議您，除了Windows作業系統需安裝修補程式外， Linux 作業系統也應時時保持更新。

若客戶在內部網路發現此弱點攻擊事件，極可能代表攻擊已進入到內網擴散階段，可搭配DDI偵測內網擴散攻擊來源。

UNIFORCE 創泓科技

案例: 校園網路印表機勒索威脅

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

比特幣集體勒索又來了，這次鎖定全臺4千校！不只大學，桃園3小學也出現駭客勒索信

桃園市有3所中小學近日收到駭客恐嚇信，揚言若不支付比特幣，就會在3月1日癱瘓學校網路。此外，也有部分大學同樣收到駭客威脅信。駭客利用連線印表機的公開IP和預設密碼，侵入學校網路列印。

文/ 黃弘瑜 | 2017-02-22 發表

按讚加入iThome粉絲團 分享 2,281 G+1 5

各級學校在印表機收到駭客勒索信

有關因應校園網路勒索處置說明

106.02.23

有關媒體報導「駭客侵入校園，透過網路印表機列印勒索支付比特幣」事件，本部於今年春節後即陸續接獲此事件通報，並於2月16日起透過臺灣學術網路危機處理中心(TACERT)，發送資安事件通知予各校，同時呈報行政院，並即時調查彙整收到駭客恐嚇信學校清單。

本次事件中學校收到勒索傳真，勒索支付日期為2月20日及3月1日前完成，據了解，學校並無實際支付。透過臺灣學術網路危機處理中心(TACERT)通報系統，學校若有問題及疑慮可即時回報，本部將即時掌握受害情況，網路印表機列印勒索建議採取適當作法，防護措施建議如下：

1. 請設定網路印表機之強度夠(強健)的密碼。
2. 關閉網路印表機不使用的服務(通訊埠 Port)
3. 不使用公開的網際網路IP位址(例如140.112.x.x)改用虛擬IP位址(例如 10.1.x.x)，如使用公開的網際網路位址，建議裝置設備納入防火牆防護範圍。
4. 阻擋外部存取網路印表機的權限(例如 9100 通訊埠)。
5. 對於個人電腦重要檔案資料，請妥為備份並另行儲存。
6. 提醒各校對於物聯網設備(如網路攝影機)，亦應一併檢查是否有資安漏洞，並納入資安防護範圍。

另外，本部已請教育體系資安防護團隊加強網路資安偵測，各校若有資安入侵攻擊事件時，請逕依資安通報應變程序通報，本部將儘速協

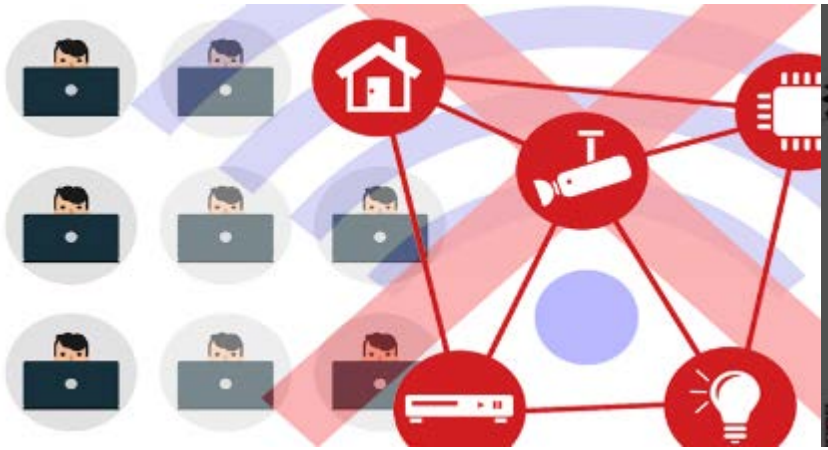
假設:

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?

UNIFORCE 創泓科技

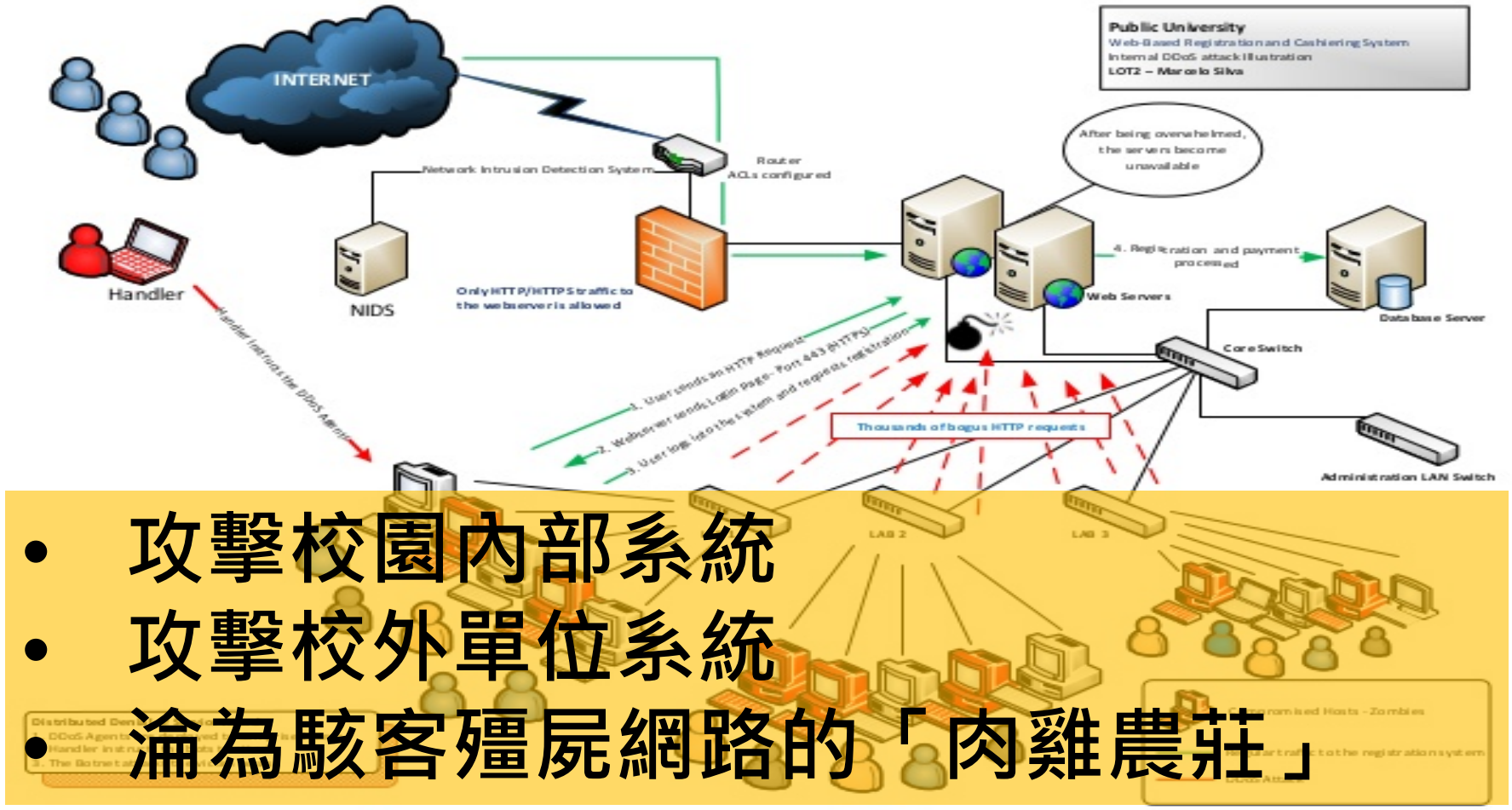
案例: 物聯網裝置殭屍網路攻擊Mirai

- Mirai (未來) 殭屍網路
- 2017年10月爆發史上影響最大的DDoS攻擊事件，創下每秒Tb級的攻擊流量.
- 大量利用Linux嵌入系統的物聯網裝置 (IP Camera, IP分享器, 家用Router等).
- 透過IP白名單規避，通過超過60種常用預設使用者名稱和密碼辨別出易受攻擊的裝置.
- 攻擊目標: 美國大型網路服務公司Dyn所管理的DNS服務系統.
- 影響包括Twitter、Amazon、Spotify及Netflix等使用Dyn公司服務的網路公司.
- Mirai作者開放攻擊程式碼，已產生Windows形態的變種.



UNIFORCE 創泓科技

校園網路利用攻擊威脅



- 攻擊校園內部系統
- 攻擊校外單位系統
- 淪為駭客殭屍網路的「肉雞農莊」

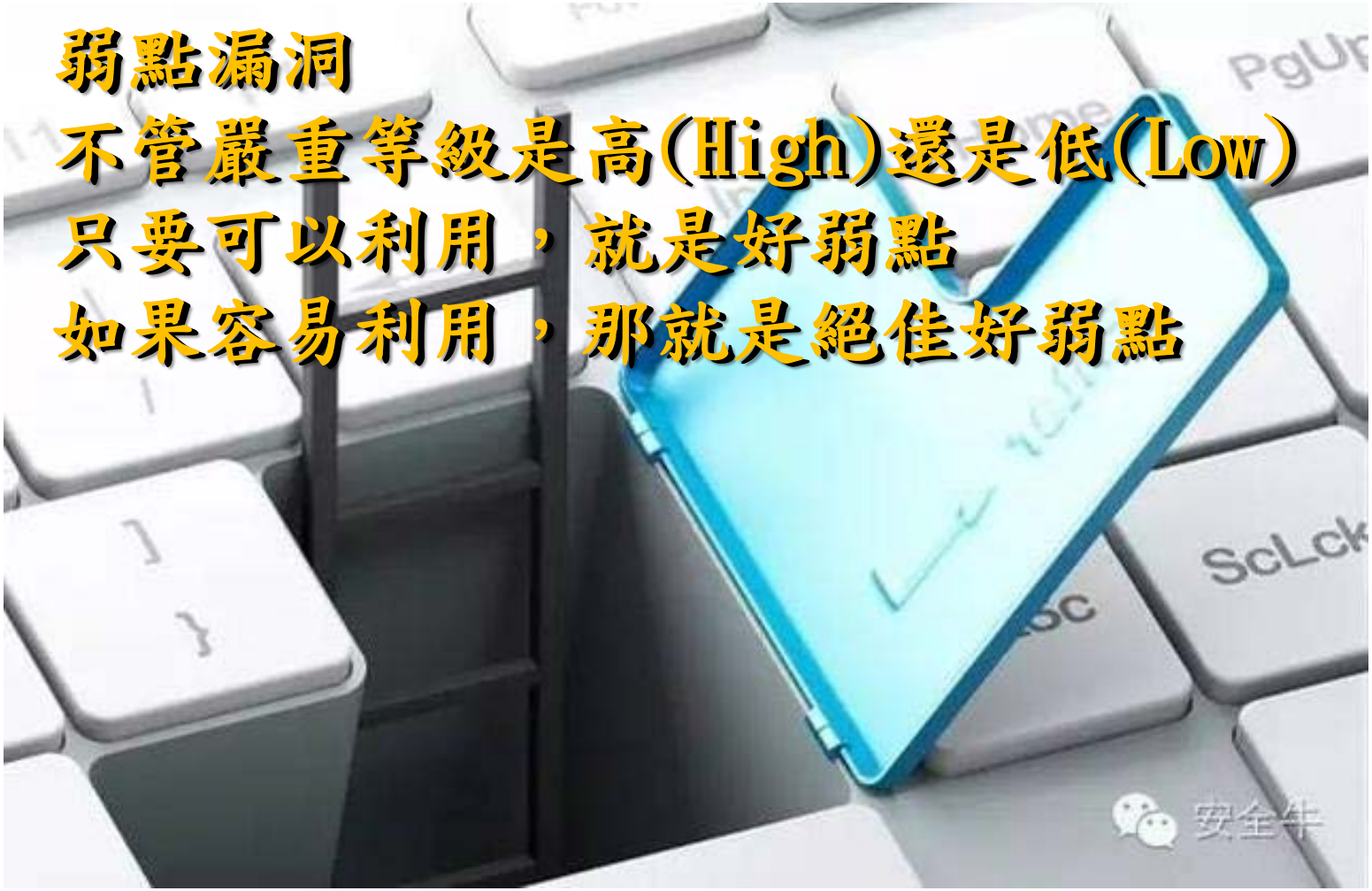
UNIFORCE 創泓科技

大綱介紹

- 新世代資安威脅的樣貌
- 弱點不是病, 弱起來要人命
- 弱點掃瞄與滲透測試的微妙關係
- 正視弱點才能掌控資安風險
- 面對更多未知的驚奇
- Q&A

UNIFORCE 創泓科技

怎麼看待「弱點漏洞」



UNIFORCE 創泓科技

現今資安威脅有近9成利用漏洞!!

惡意程式

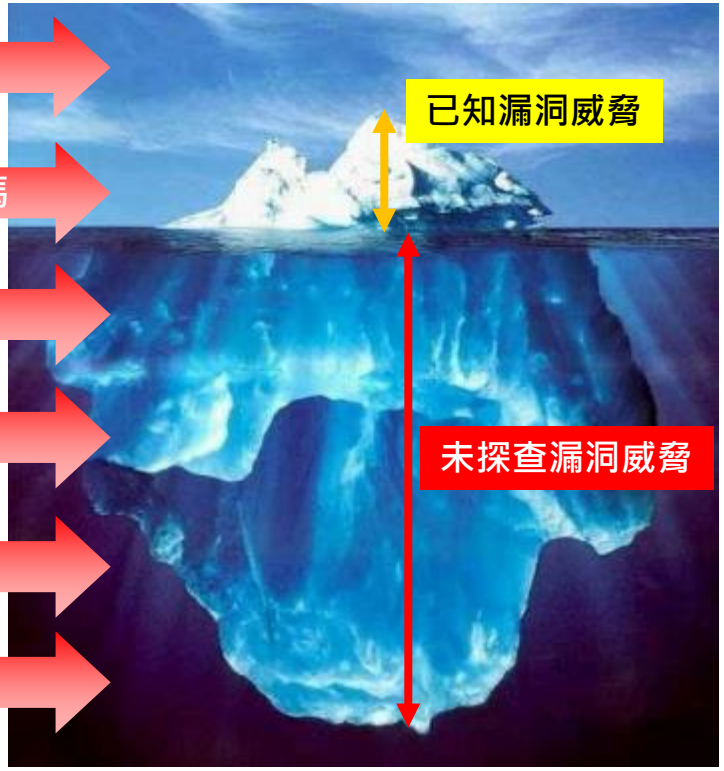
殭屍/木馬

跳板攻擊

資料竊取

釣魚詐欺

目標攻擊

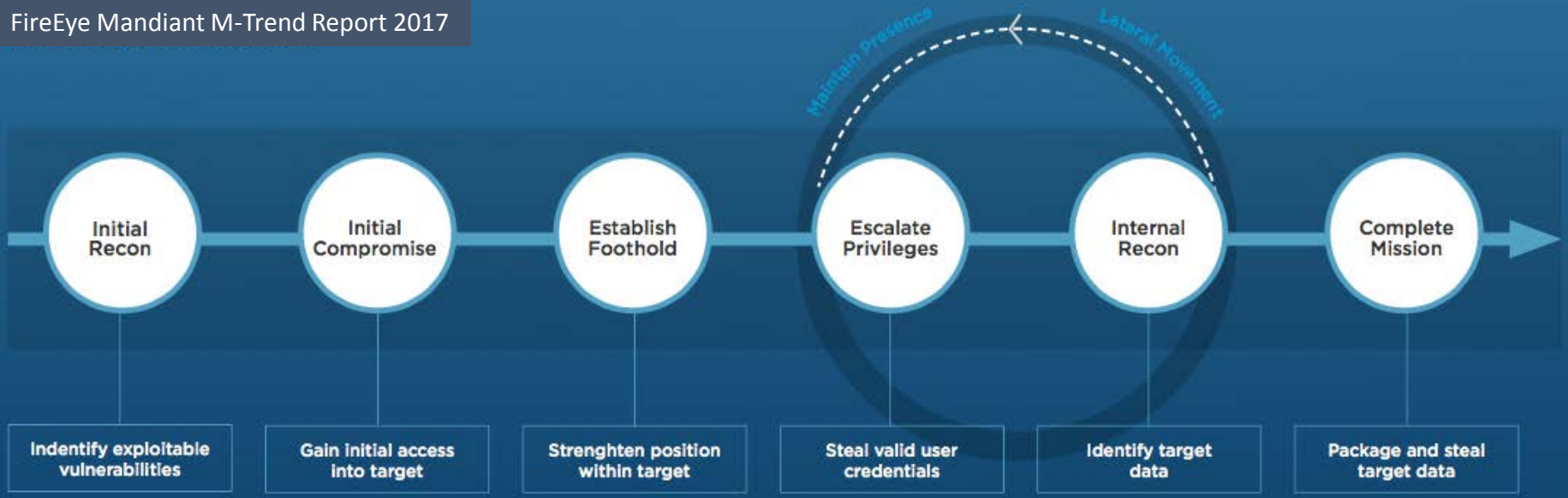


有洞嗎?
洞在哪裡?
又如何?
都很正常呀!?
證明看看?
很麻煩內>_<

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

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

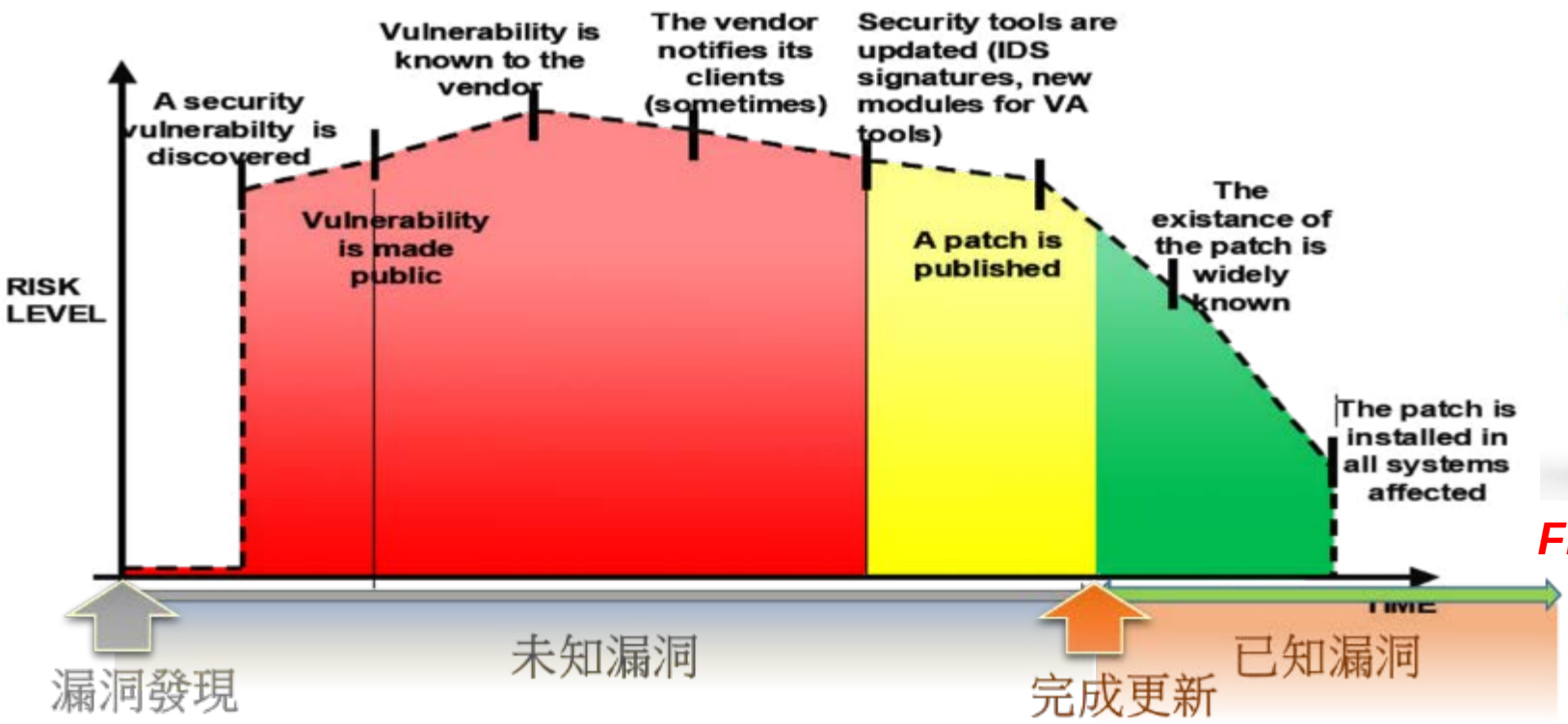
零時差漏洞 (也就是從未被發現的新漏洞) 最近出現的頻率越來越高，更糟的是，這些危險的漏洞經常都是在駭客攻擊事件發生之後，人們才知道漏洞的存在。

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

弱點漏洞的生命週期

Window of Vulnerability



Finish ?

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

UNIFORCE 創泓科技

弱點無處不在，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

微軟修補了45個漏洞，包含5個已被開採的

微軟修補由Google揭露的安全漏洞

Linux磁碟加密工具Cryptsetup爆重大漏洞

重要商務系統弱點

甲骨文一次修補276個安全漏洞，寫下新

甲骨文修補308個安全漏洞，創新紀錄!

應用程式弱點導致資料外洩

Adobe搶修已遭攻擊的Flash漏洞

DB弱點導致伺服器淪

MySQL爆最高權限漏洞，MariaDB、P

「黑護士」來襲! 資安業者以一台筆電癱瘓思科與合勤防火牆（更新：合勤緊急釋出更新）

賽門鐵克防毒軟體爆漏洞，25項企業及消費安全產品可能受駭

防毒軟體有漏洞已不是新聞。事實上，Google Project Zero就曾在Eset、趨勢科技PC-Cillin、卡巴斯基、FireEye、McAfee等發現有安全漏洞，甚至賽門鐵克自己

新聞

看電影小心駭客利用惡意字幕接管你的電腦

Check Point發現駭客可利用惡意字幕檔案，結合媒體播放器或串流播放平台的漏洞，自遠端掌控使用者的裝置，包含PC、手機或智慧電視，從而竊取裝置上的資訊。

文/ 陳曉莉 | 2017-05-24 發表

資安系統弱點導致防護破壞

UNIFORCE 創泓科技

弱點無處不在，魔鬼藏在細節中

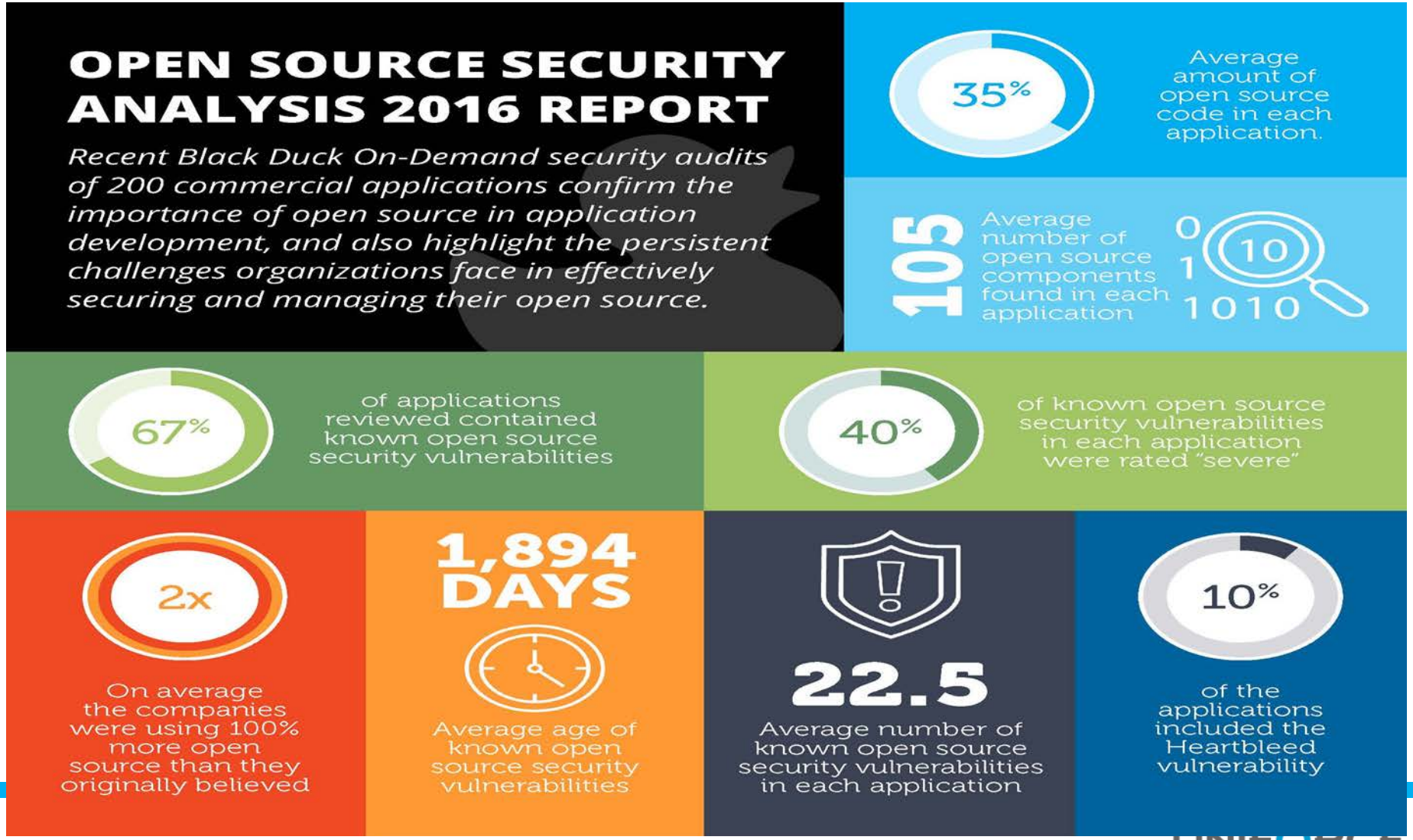
UNIFORCE 創泓科技

弱點無處不在，魔鬼藏在細節中

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。

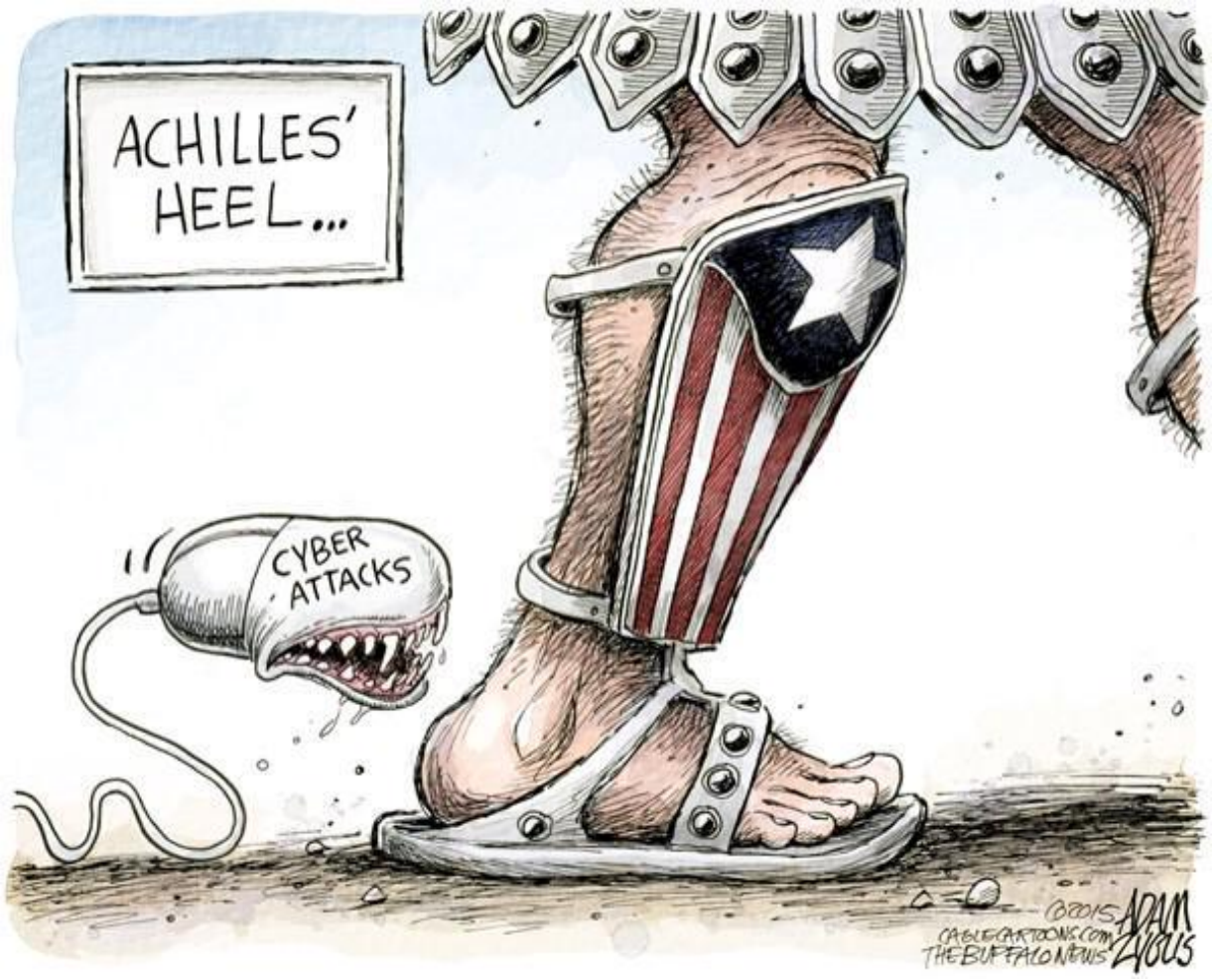
UNIFORCE 創泓科技

開源軟體(Open Source) 安全分析



資料來源: Black Duck Software

安全脆弱度，只需要一個正確的點



UNIFORCE 創泓科技

資安防護工事上的迷思

資安防護足夠了嗎?

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

資安信任鍊的破壞

UNIFORCE 創泓科技

大綱介紹

- 新世代資安威脅的樣貌
- 弱點不是病, 弱起來要人命
- 弱點掃瞄與滲透測試的微妙關係
- 正視弱點才能掌控資安風險
- 面對更多未知的驚奇
- Q&A

UNIFORCE 創泓科技

弱點掃瞄與滲透測試的微妙關係

「健康」的標準

圖像來源: 美國隊長 電影劇照

UNIFORCE 創泓科技

弱點掃瞄與滲透測試的微妙關係

體能檢驗

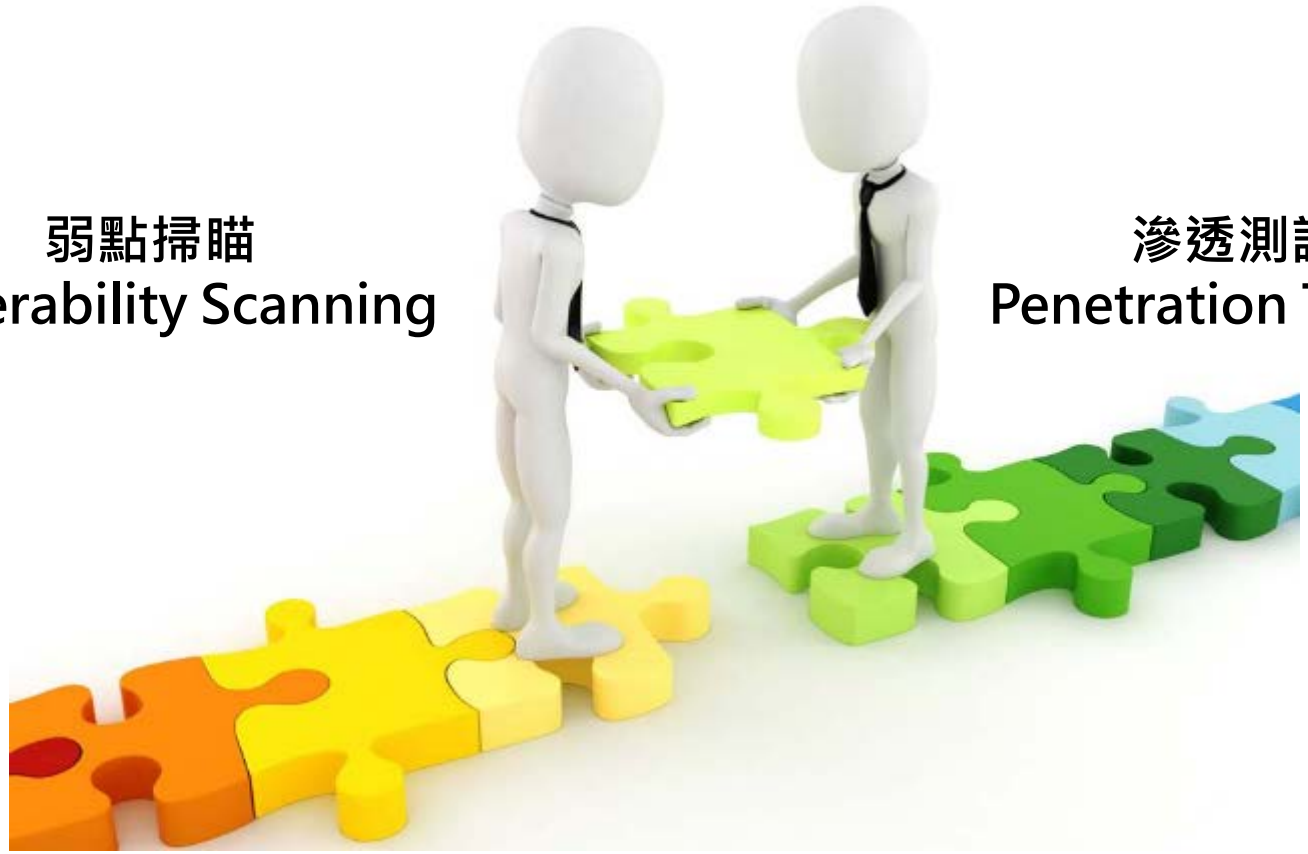
健康檢查

UNIFORCE 創泓科技

弱點掃瞄與滲透測試的微妙關係

目的相同的不同檢驗方式.

弱點掃瞄
Vulnerability Scanning



滲透測試
Penetration Testing

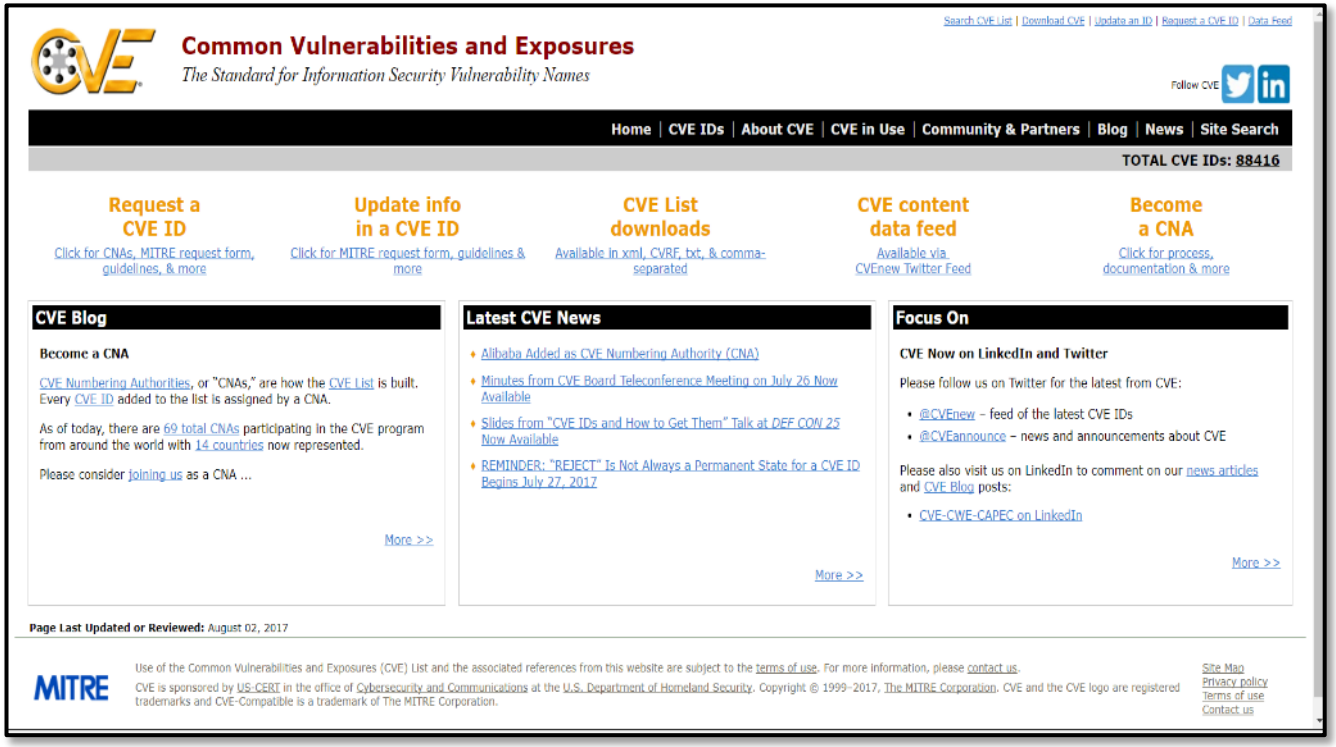
UNIFORCE 創泓科技

弱點掃瞄與滲透測試的微妙關係

	弱點掃瞄	滲透測試
效果	發現存在資安風險威脅的必要作業	檢驗強度的最佳手段
範圍	廣泛性	針對性
頻率	常態性	任務性
程序	前	後
作業執行	相對容易	相對複雜

弱點漏洞的相關資安組織 - CVE

- CVE (Common Vulnerabilities and Exposures,通用漏洞披露)，又稱常見弱點與漏洞，是一個與資訊安全有關的資料庫，收集各種資安弱點及漏洞並給予編號以便於公眾查閱。
- 此資料庫現由美國非營利組織MITRE所屬的National Cybersecurity FFRDC所營運維護。
- 每一個通用漏洞披露都賦予一個專屬的編號，格式如下：CVE-YYYY-NNNN。

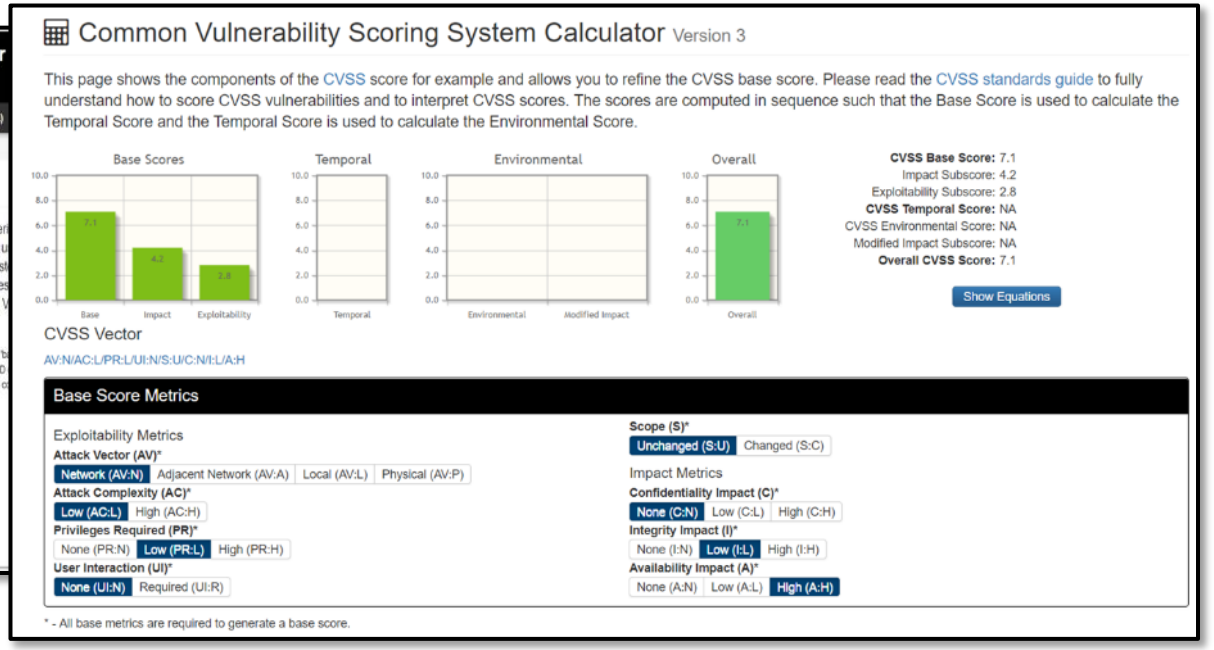


https://cve.mitre.org/

弱點漏洞的相關資安組織-CVSS

- CVSS (Common Vulnerability Scoring System, 漏洞評鑑系統) 由美國國家基礎建設諮詢委員會 (NIAC) 委託製作，是一套公開的評鑑標準。
- CVSS是運用數學方程式來判定弱點分數，普遍被認為較具中立性。
- CVSS的判定標準，包含威脅的嚴重性，遠端網路是否能遙控資安漏洞、利用網路弱點，攻擊者是否需要登入才會產生威脅等等，都被列入評比。
- CVSS的評分分數從0分到10分，0代表沒有發現弱點，而10則代表最高風險。
  (註: 得分7~10的漏洞:嚴重；得分在4~6.9之間: 中級漏洞；得分在0~3.9之間: 低級漏洞)

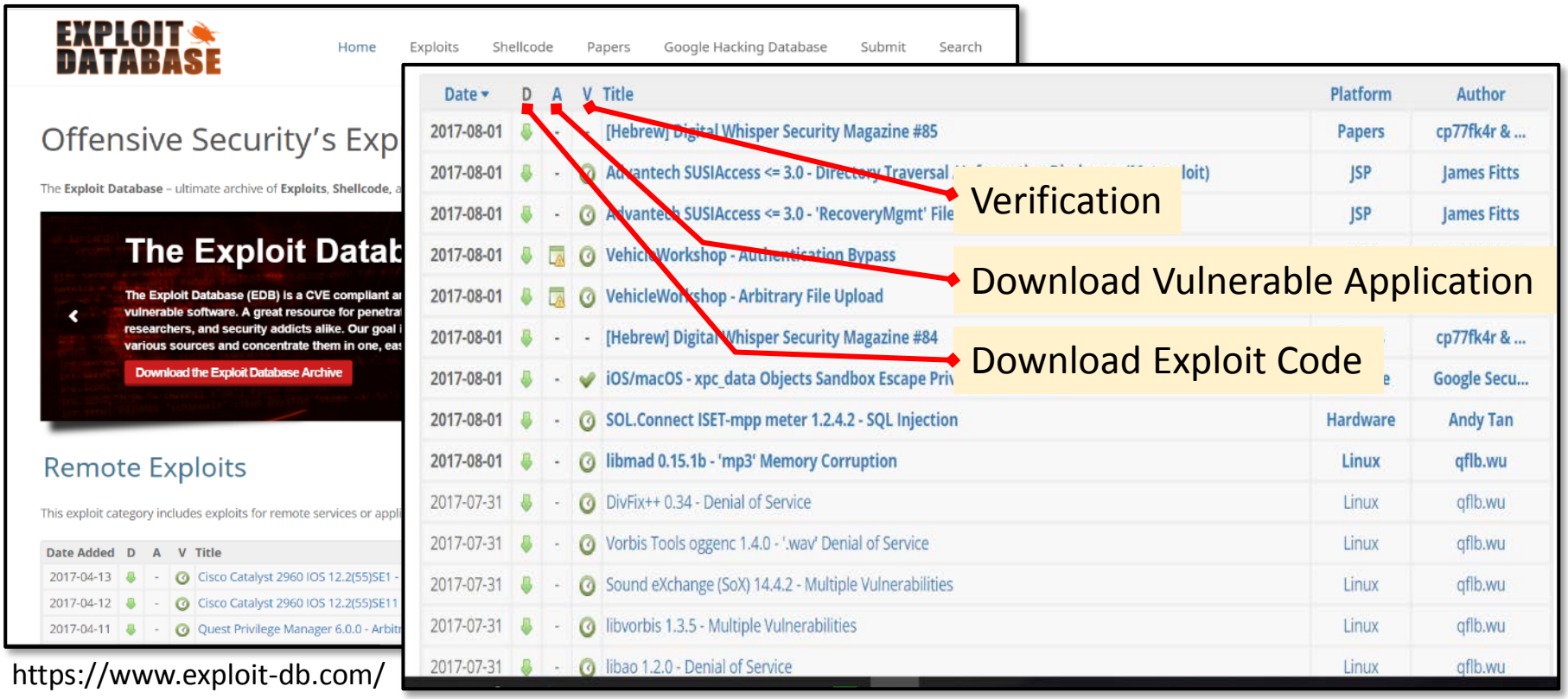
https://nvd.nist.gov/vuln-metrics/cvss



UNIFORCE 創泓科技

弱點漏洞的相關資安組織-Exploit-DB

- Exploits Database（https://www.exploit-db.com/）號稱全球漏洞庫，網站收集了來自全球白帽提交的各類漏洞訊息及利用代碼，吸引著無數安全界愛好者。
- 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

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)。

2015年最盛行的加密勒索利用工具: Angler

CVE編號	有漏洞的應用程式	確認日期	第一個加以整合的漏洞攻擊包	修補程式發布日期
CVE-2015-8651	Adobe Flash	2016-01-26	Angler	2015-12-28
CVE-2015-8446	Adobe Flash	2015-12-15	Angler	2015-12-08
CVE-2015-7645	Adobe Flash	2015-10-29	Angler	2015-10-16

最近有一波新的勒索病毒 Ransomware (勒索軟體/綁架病毒),自三月底開始爆發。Proofpoint的研究人員加上安全分析師Frank Ruiz所提供的情報，發現了一個被稱為「CryptXXX」的新勒索軟體，根據其描述，它與早期的勒索軟體Reveton有明顯的關聯。

這個勒索病毒 Ransomware是由BEDEP惡意軟體所散播，透過Angler漏洞攻擊套件來感染系統。研究人員在文章內描述「Angler漏洞攻擊套件結合BEDEP來散播勒索軟體和Dridex 222」。這代表放有Angler漏洞攻擊套件的網頁被用來散播CryptXXX。此攻擊套件接著利用系統漏洞來植入BEDEP。因為其「惡意軟體下載」能力，CryptXXX會以第二段感染的方式出現，它是會延遲執行的DLL程式，至少要等待62分鐘才會作用。一旦勒索病毒 Ransomware開始執行，它會加密檔案並加上.crypt副檔名。

UNIFORCE 創泓科技

可利用的弱點漏洞 Exploitable

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。

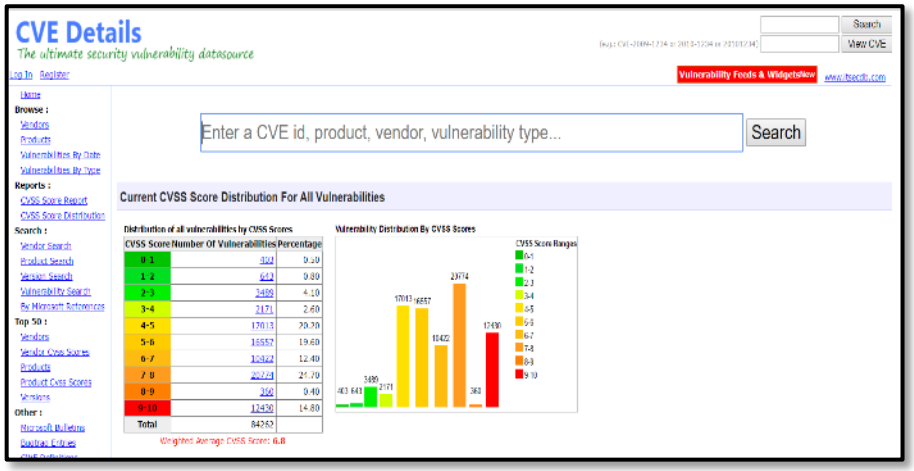
根據Bleeping Computer表示，EternalRocks可能會繞過電腦防毒軟體的偵測，造成受害者不易察覺遭入侵。而且，它沒有設置kill switch的功能，快速在網路上掃描易遭攻擊的電腦IP，隨機發動攻擊。不僅如此，駭客能夠利用EternalRocks和其他惡意程式結合，如勒索軟體、銀行木馬、RATs和其他攻擊程式。

Exploit-db公佈可利用code及方法

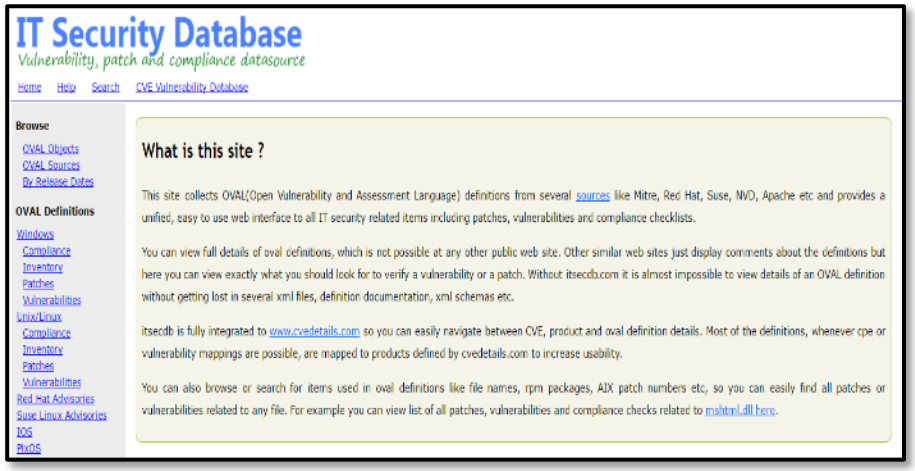
Date	D	Title
2017-08-01		[Hebrew] Digital Whisper Security Magazine #85
2017-08-01		[Hebrew] Digital Whisper Security Magazine #84
2017-07-16		How to exploit ETERNALROMANCE/SYNERGY on Windows Server 2016
2017-07-12		Hidden Network: Detecting Hidden Networks created with USB Devices
2017-07-03		[French] 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/



http://www.itsecdb.com/oval/

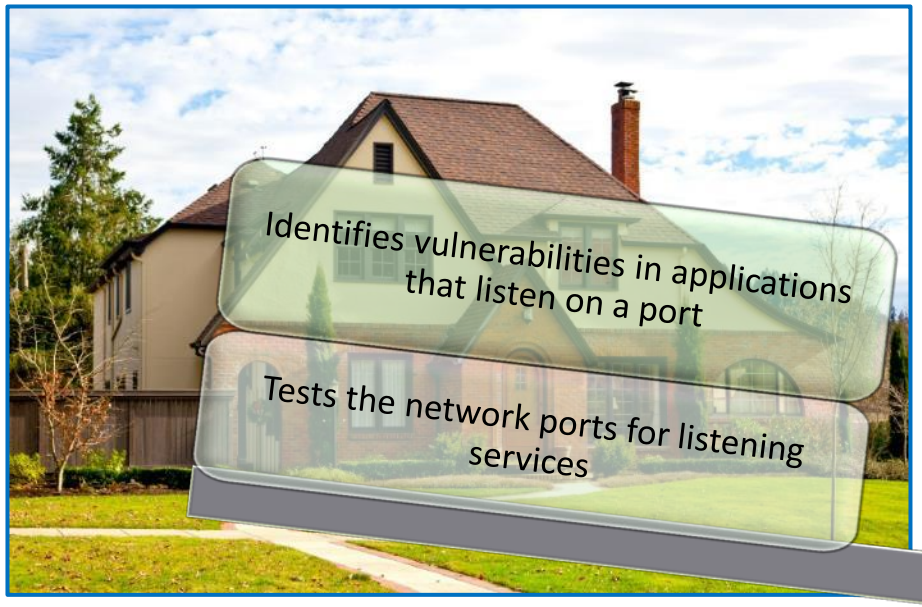
http://www.tenable.com/plugins/index.php?view=all

https://www.shodan.io/

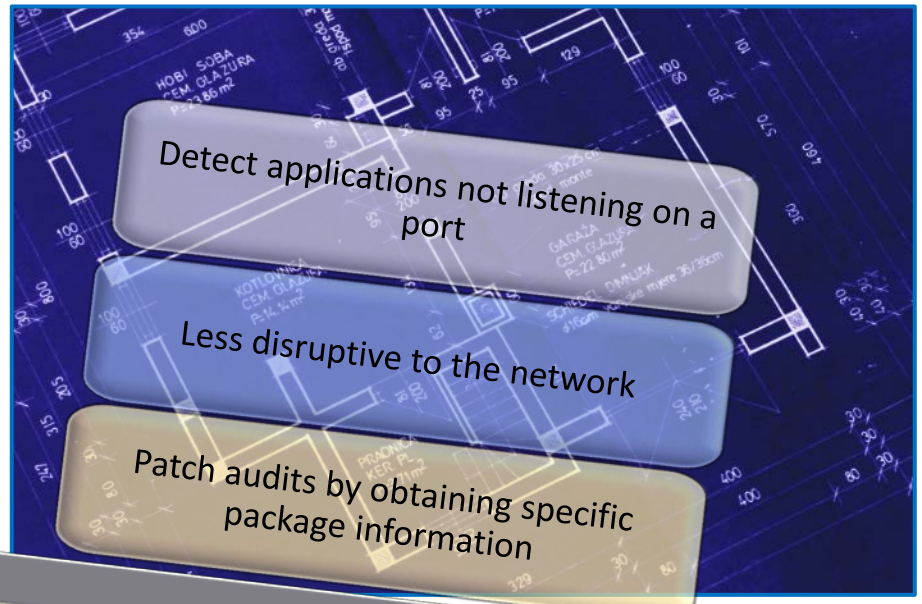
UNIFORCE 創泓科技

常見弱點掃瞄方式

網路掃描 (Network Scan)



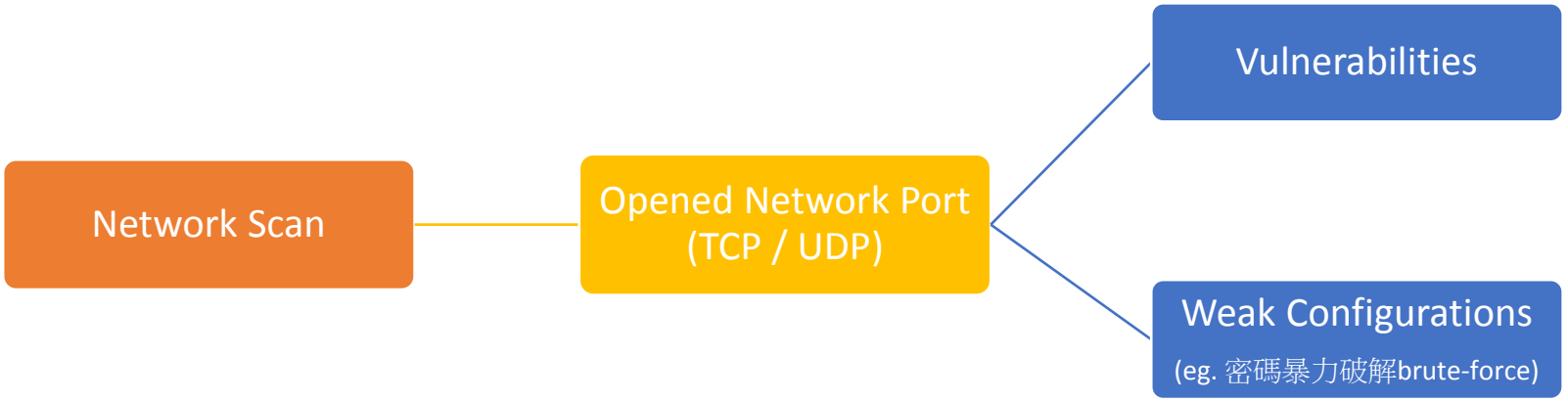
授權掃描 (Credential Scan)



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

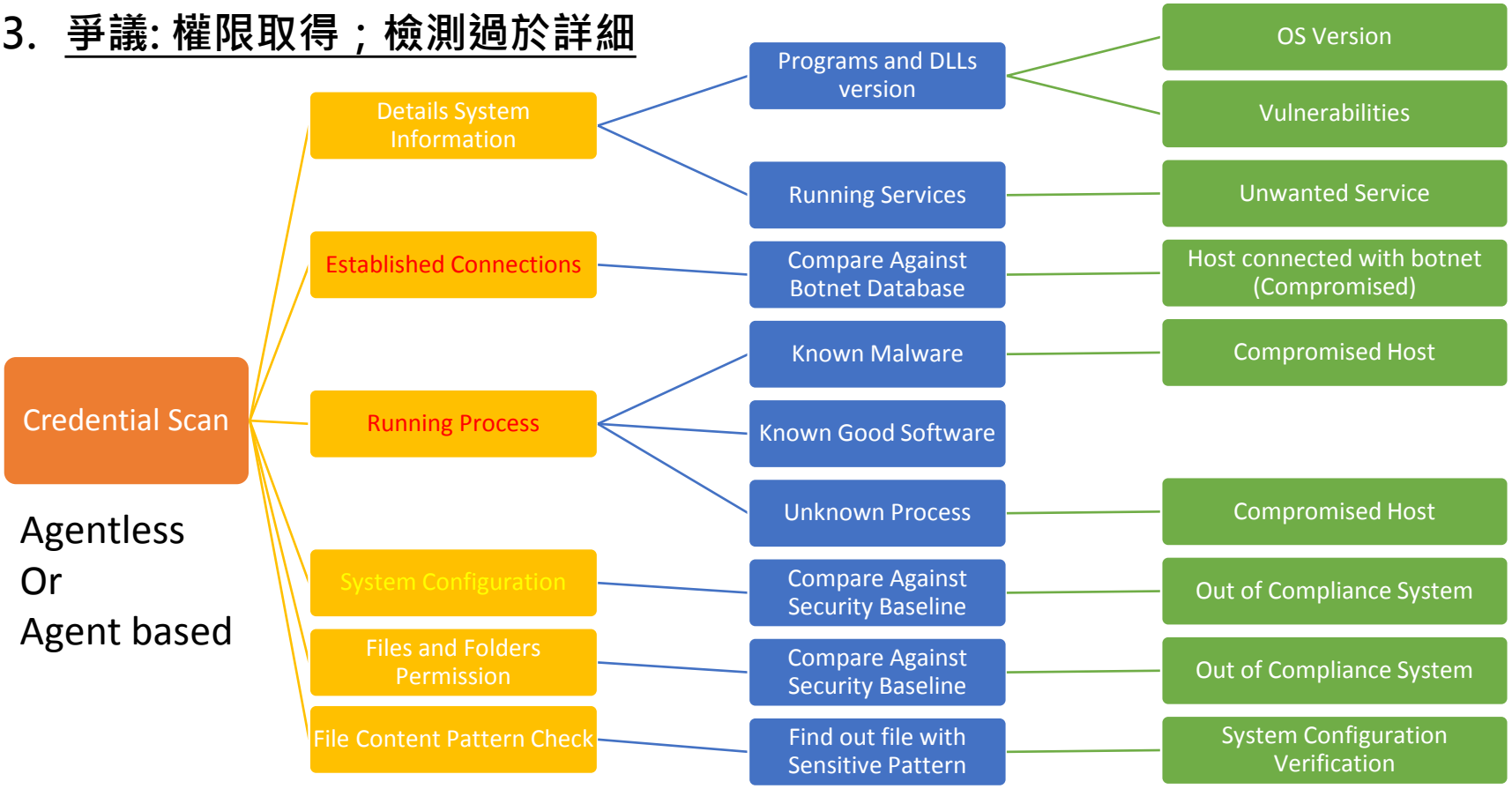


1. 需開放弱掃主機的IP
2. 需允許所有的Port (UDP/TCP)
3. 建立大量的Port Scans及Sessions
4. 耗用網路傳輸頻寬

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

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

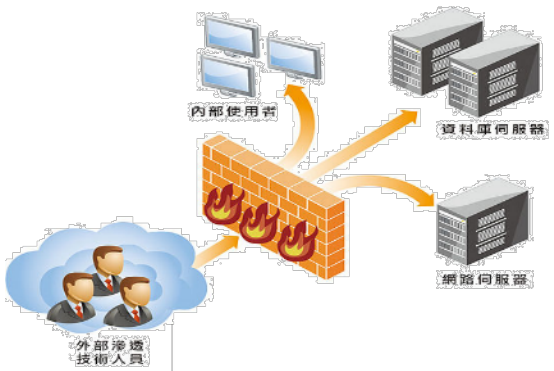
以Web系統為例:

	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

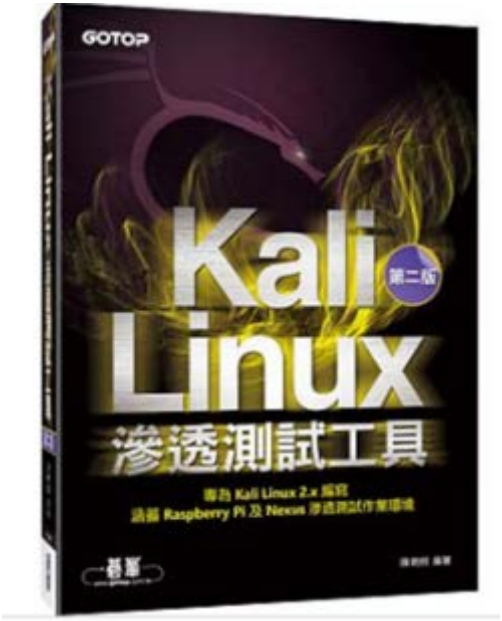
UNIFORCE 創泓科技

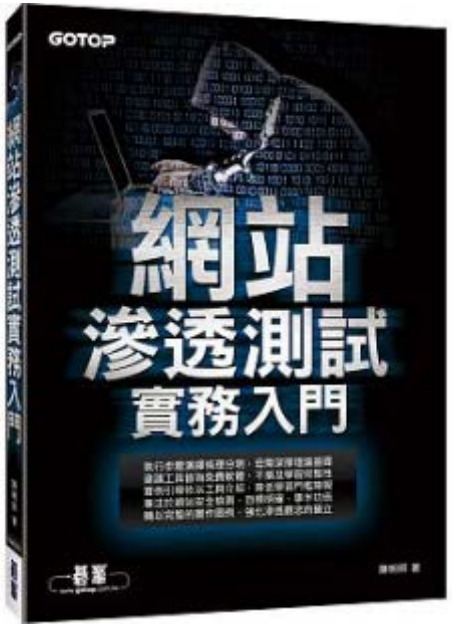
滲透測試資源參考

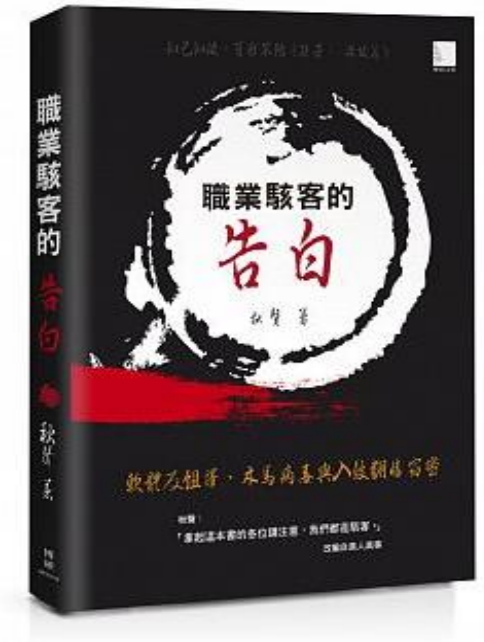
https://www.kali.org/

UNIFORCE 創泓科技

滲透測試資源參考







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

弱點掃瞄與滲透測試的真義

- ✓ 是健檢，不是攻擊
- ✓ 是稽查，不是竊取
- ✓ 是幫助，不是找麻煩

圖片來源: Dreamstime

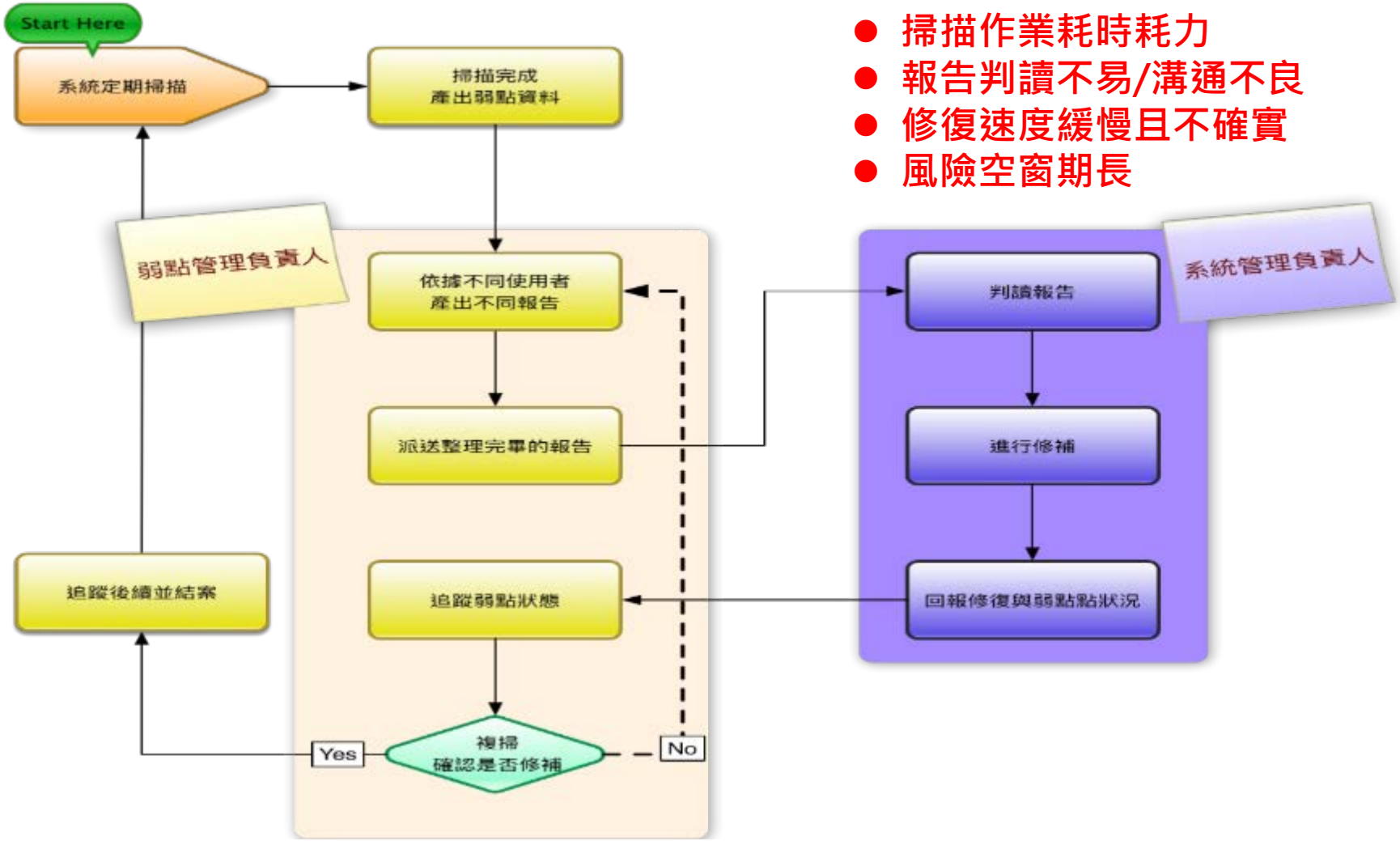
UNIFORCE 創泓科技

大綱介紹

- 新世代資安威脅的樣貌
- 弱點不是病, 弱起來要人命
- 弱點掃瞄與滲透測試的微妙關係
- 正視弱點才能掌控資安風險
- 面對更多未知的驚奇
- Q&A

UNIFORCE 創泓科技

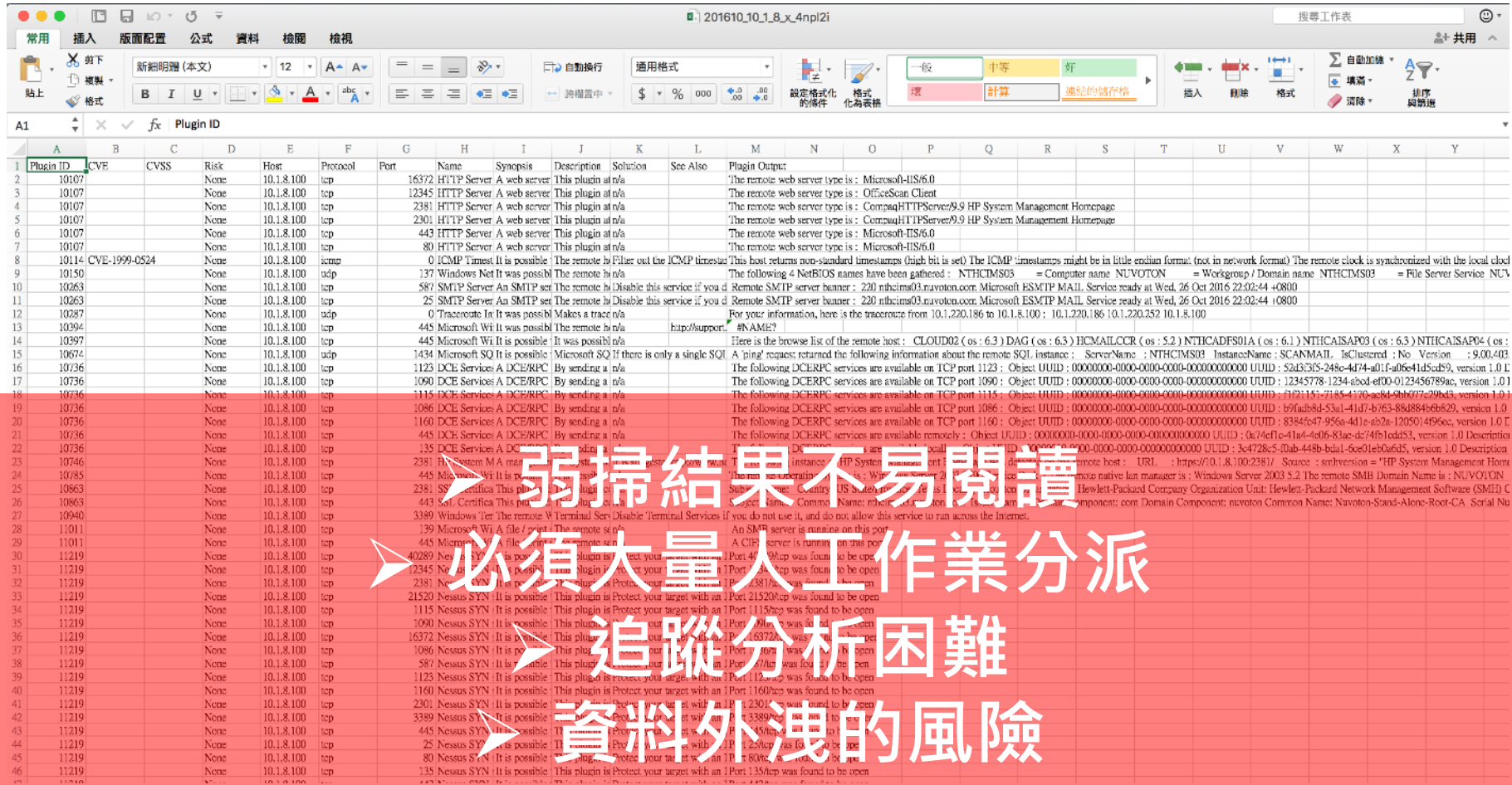
弱掃稽核的困擾



- 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

弱掃稽核的困擾

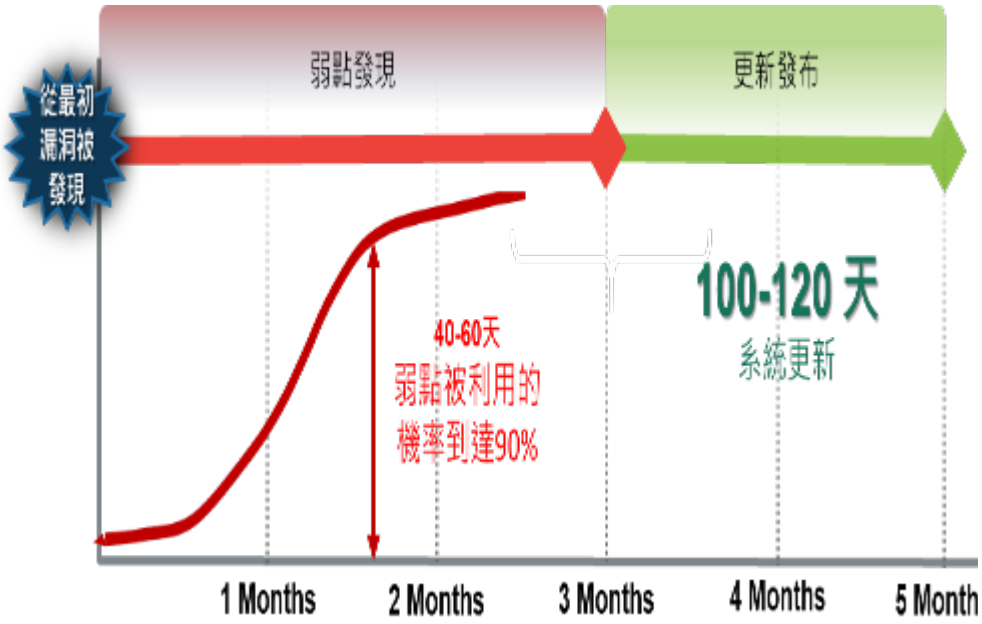


- 弱掃結果不易閱讀
- 必須大量人工作業分派
- 追蹤分析困難
- 資料外洩的風險

UNIFORCE 創泓科技

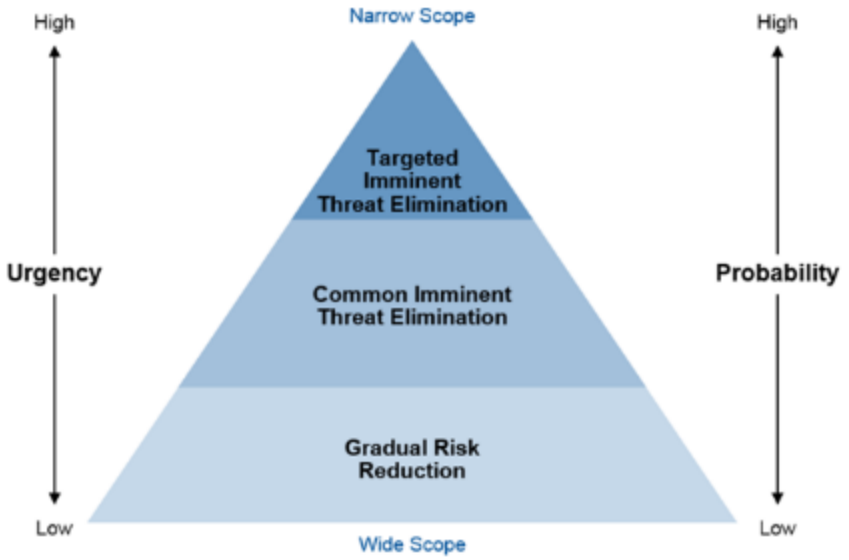
當務之急: 有效率的弱點管理

處理作業拖越久，風險空窗期越高!



有效的修補程序可降低風險度

Figure 1. Gradual Risk Reduction and Imminent Threat Elimination



Source: Gartner (September 2016)

UNIFORCE 創泓科技

弱點管理方法建立

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:

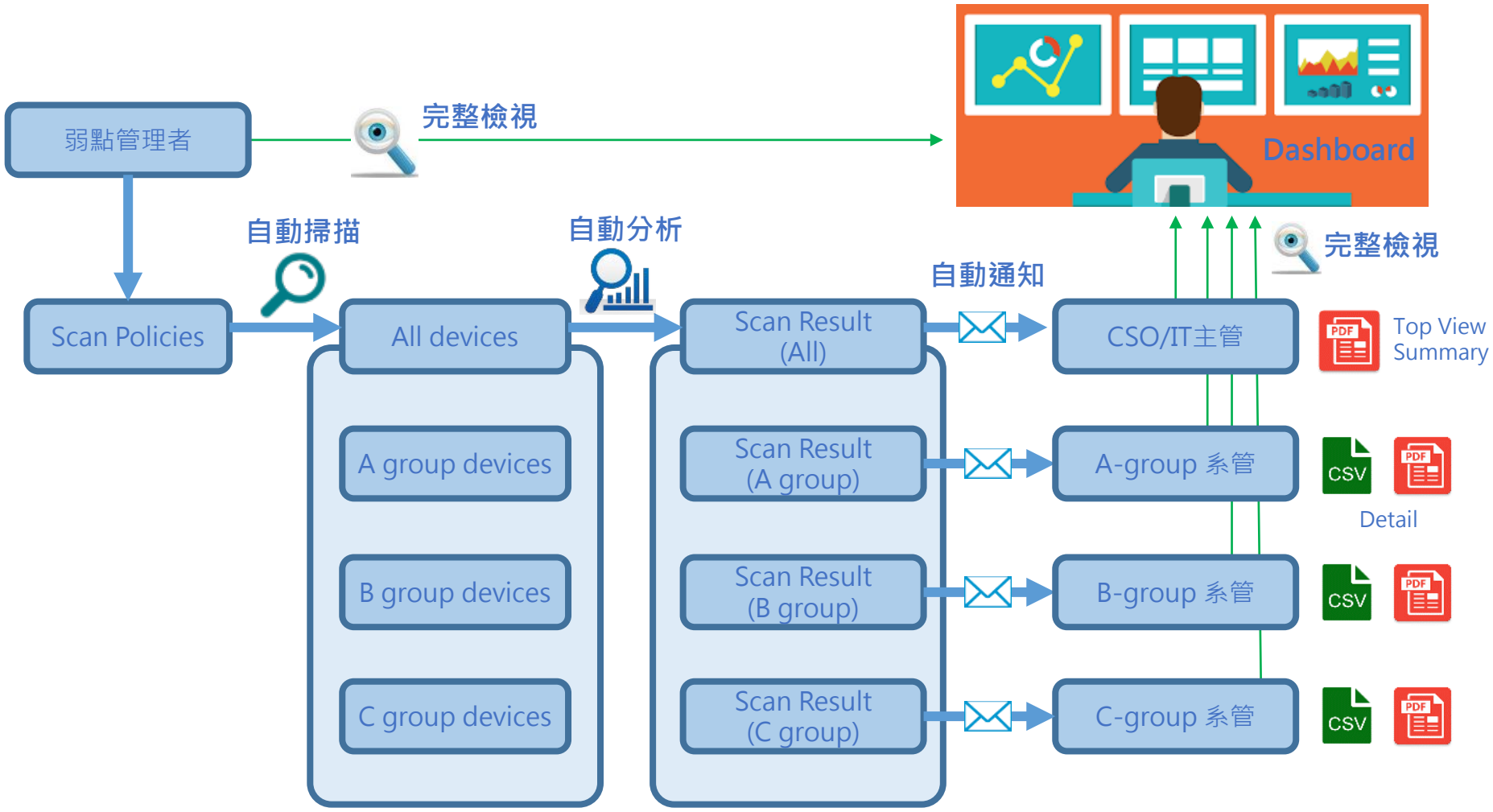
- 群組: 網路(網段)、主機、系統、專案負責.
- 權限: 檢視權限、管理範圍、弱掃執行、風險管理

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



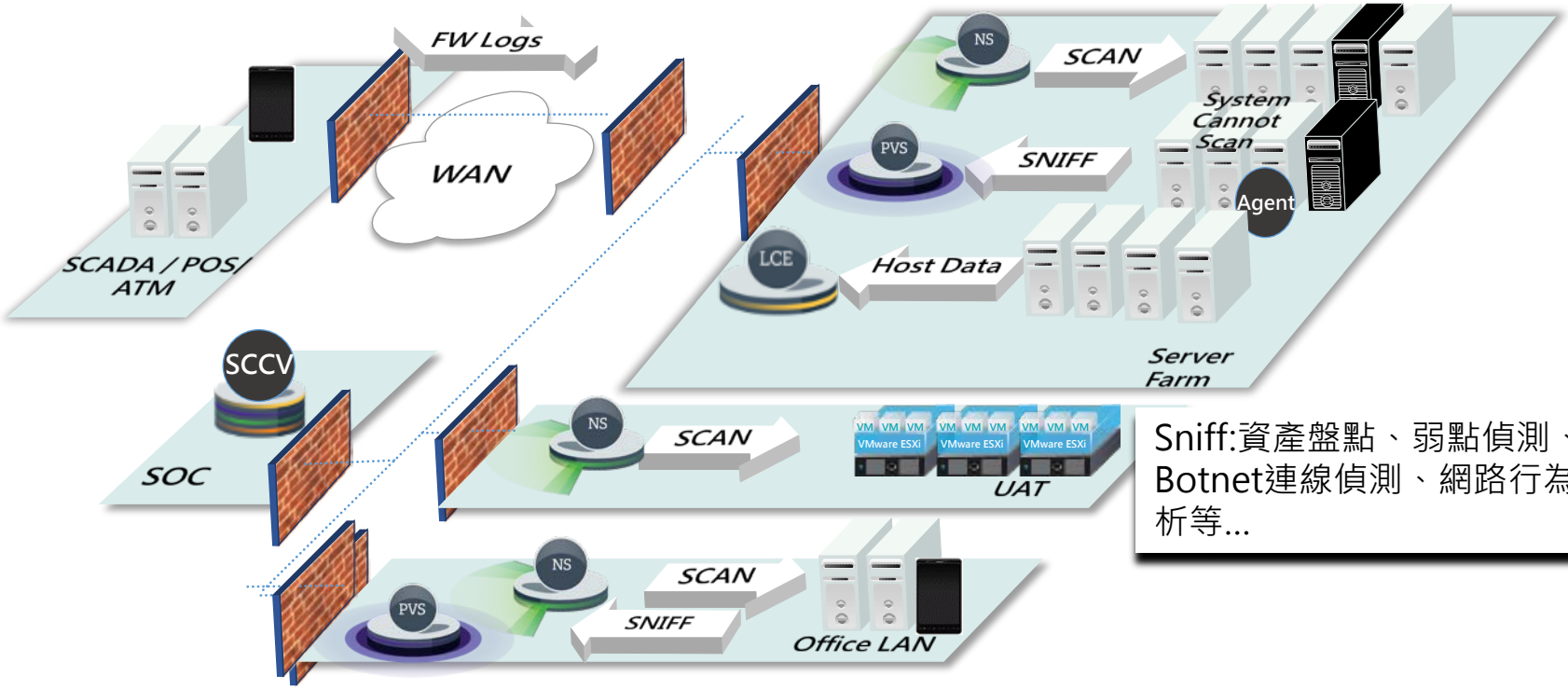
UNIFORCE 創泓科技

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

風險管理方式: 接受風險/調整等級

弱點修補改善困難之處

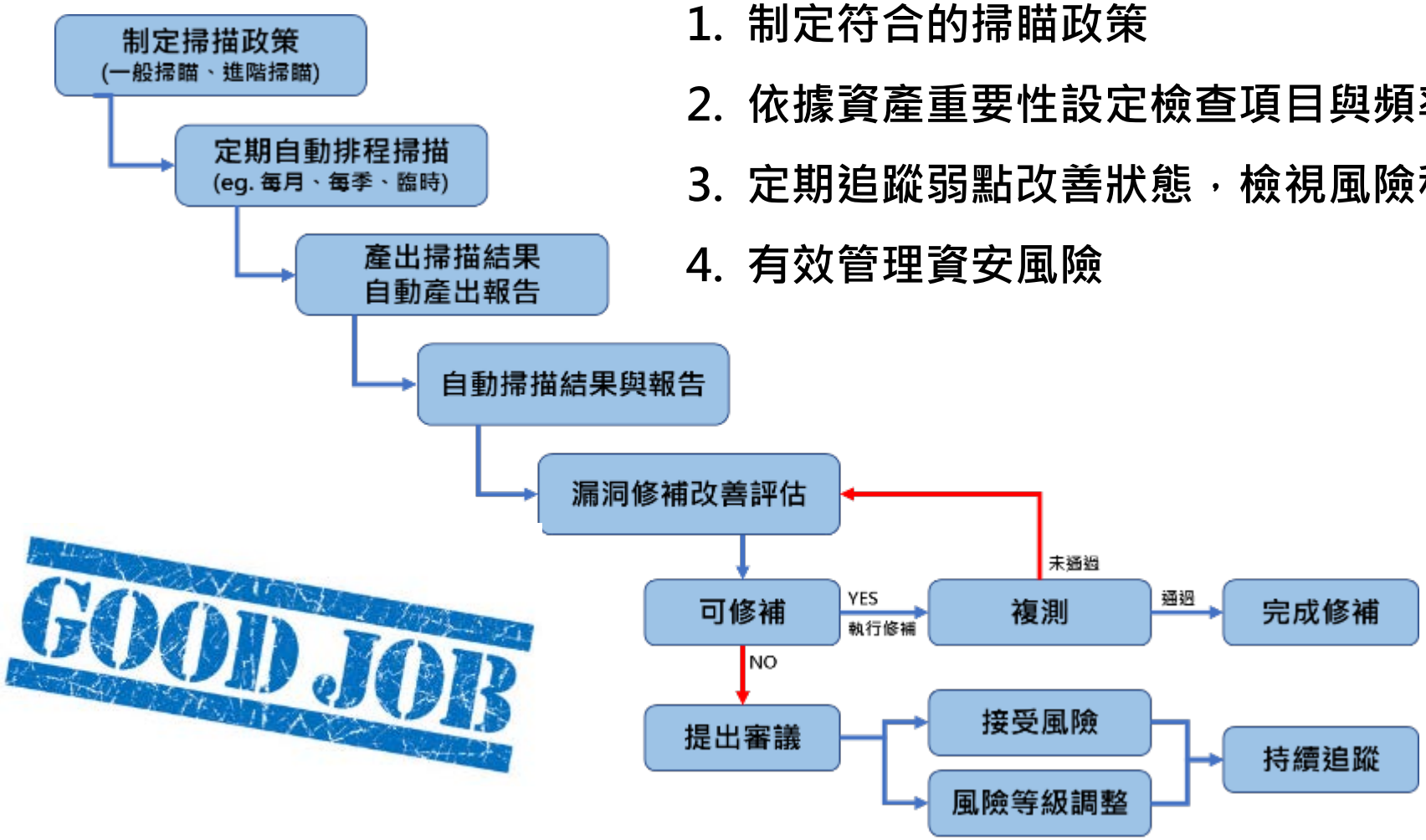
- 系統版本無法更新修補（如產品生命結束、版本過於老舊、或無保固續約、無服務商）。
- 系統版本暫時無法更新修補（如等待正式修補程式釋出、或測試評估中）。
- 系統為不可取代性之重要或敏感業務應用服務，必須計畫性修補。
- 修補程式對於應用程式或系統有不利的影響。
- 修補方式不符合成本效益。
- 建議修補方式，但應用程式或系統的設定不允許更改。
- 該弱點結果經確認為「誤判」或「特殊情況」。

弱點接受或調整的條件

已透過補強性措施(如防火牆、存取控制、帳號管控、隔離控管、事件日誌紀錄）或虛擬修補（Virtual Patching）方式達到安全保護與風險控制，經與內部提報並決議可列定風險可接受之弱點或資產。

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

弱點檢視管理

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

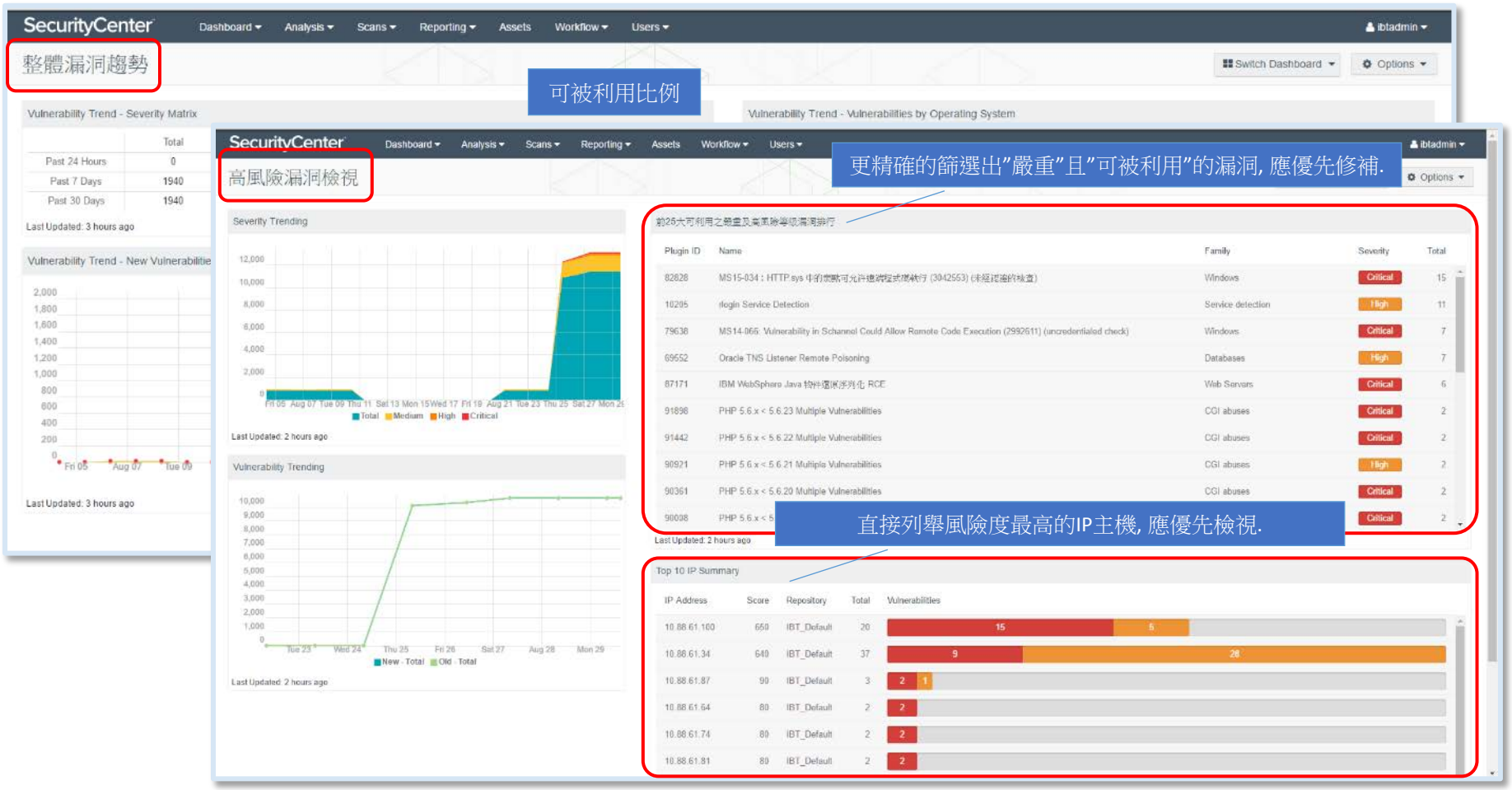
前10大IP列表

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

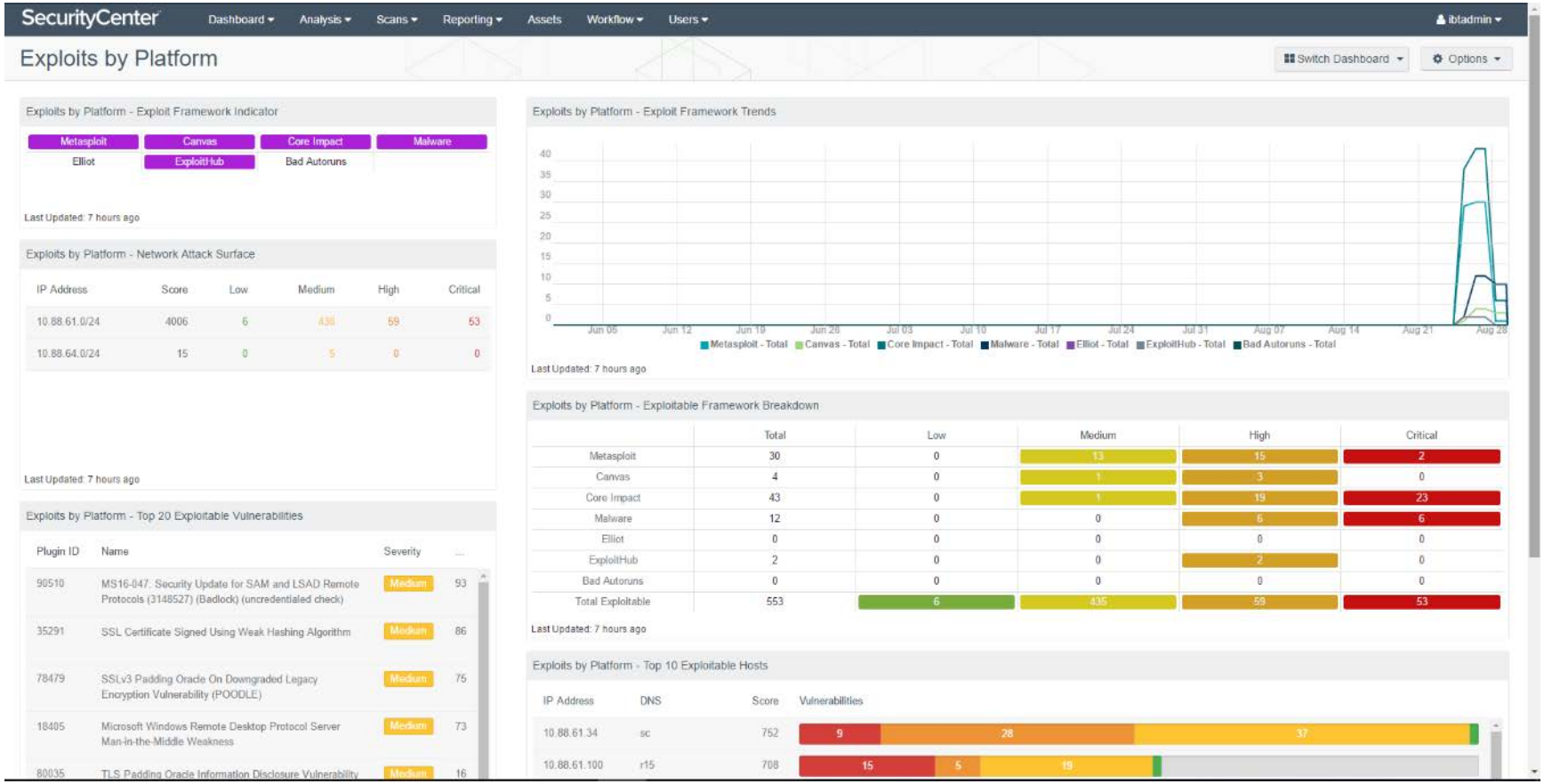
弱點檢視管理



UNIFORCE 創泓科技

弱點分析管理

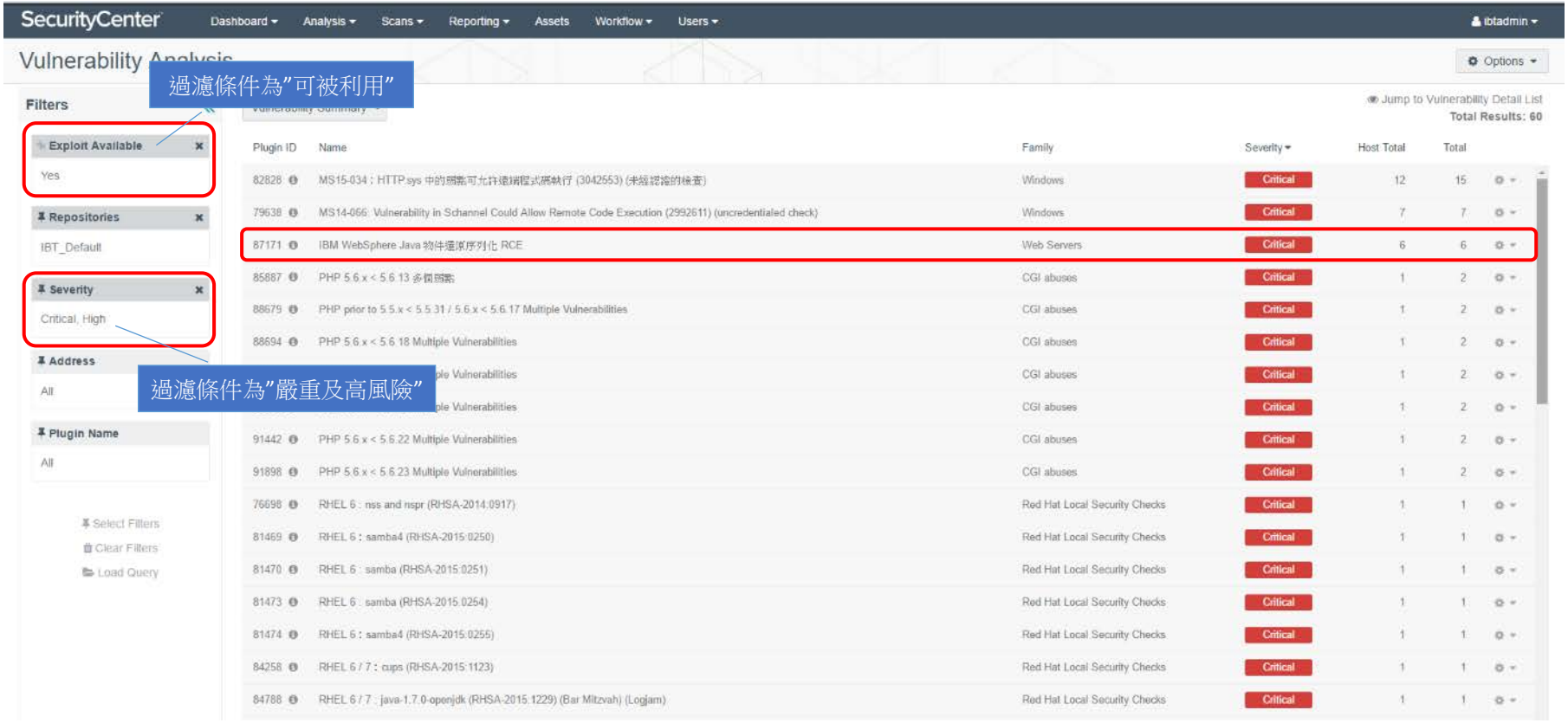
可利用弱點套件(Exploitable)分析



UNIFORCE 創泓科技

弱點分析管理

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.



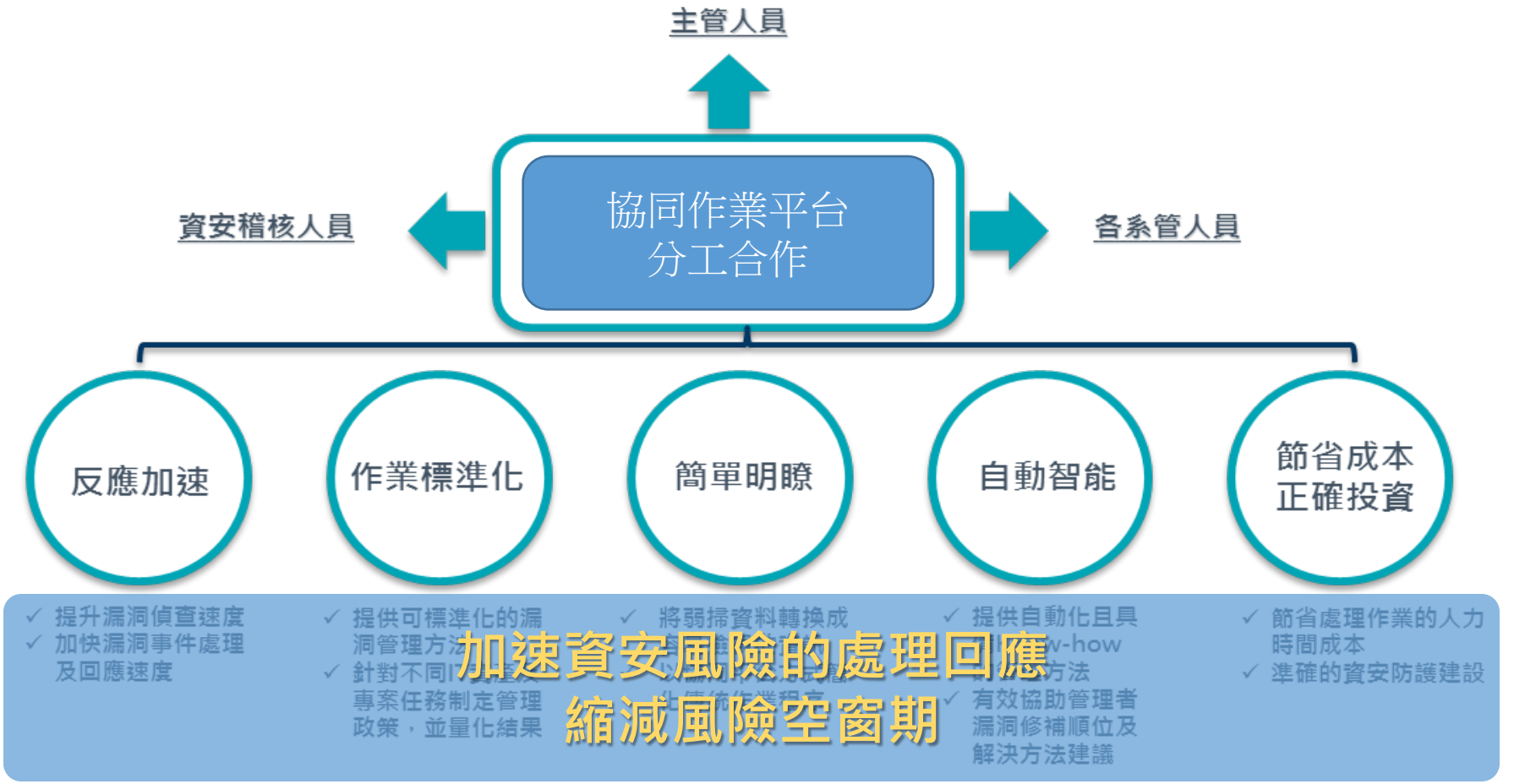
UNIFORCE 創泓科技

弱點分析管理

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

大綱介紹

- 新世代資安威脅的樣貌
- 弱點不是病, 弱起來要人命
- 弱點掃瞄與滲透測試的微妙關係
- 正視弱點才能掌控資安風險
- 面對更多未知的驚奇
- Q&A

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

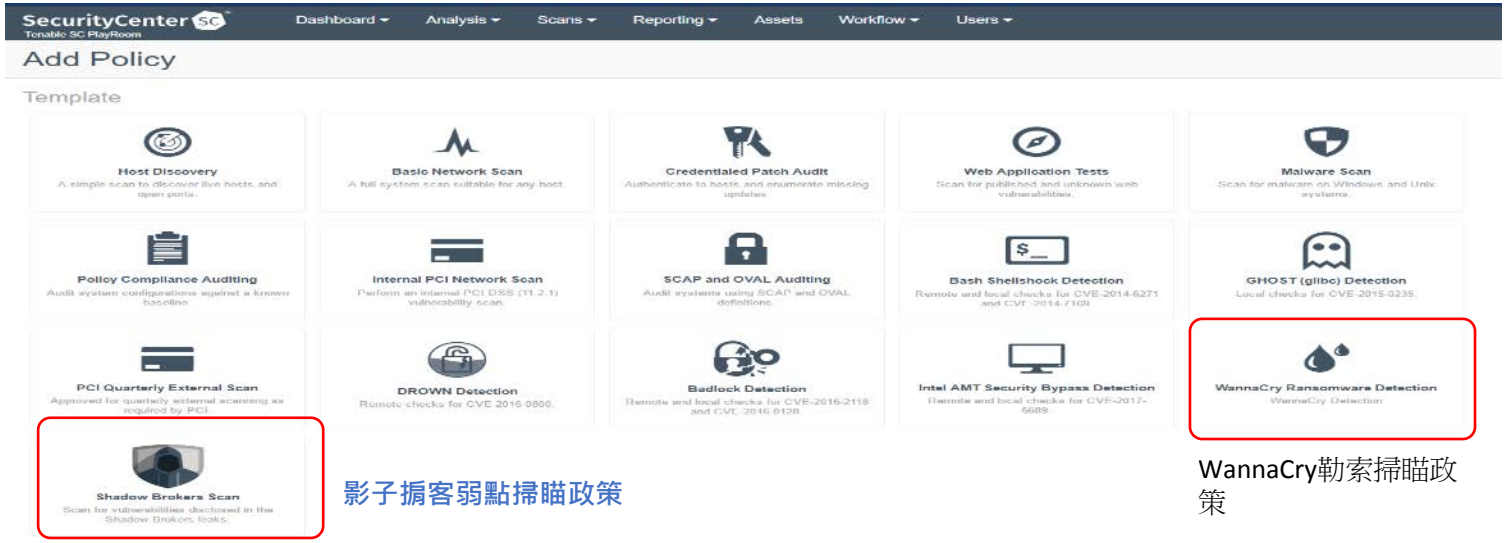
確認弱點資訊 (1天)	執行弱點掃瞄作業 (3-5天)	弱掃結果彙整分析 (1天)	弱點結果派送 (1天)
本次專案弱掃系統廠商提供快速的情報資訊，弱點資料更新頻率為每日更新，可減少弱點資訊搜找的時間.	本次專案弱掃系統提供多個弱點掃描器的授權部署，並且可由中央管理設定排程自動執行掃瞄作業，並將掃描結果自動回報儲放於中央系統. 並且可以僅針對指定的弱點項目(如本次WannaCry)進行指定盤查，可減少掃瞄作業對主機的耗能與時間. 整體可加速弱掃速率，並減少作業所耗用的人力時間成本.	本次專案弱掃系統於弱掃作業過程便已將結果回報儲放於中央系統資料庫，可直接套用相關的報告範本(如WannaCry)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

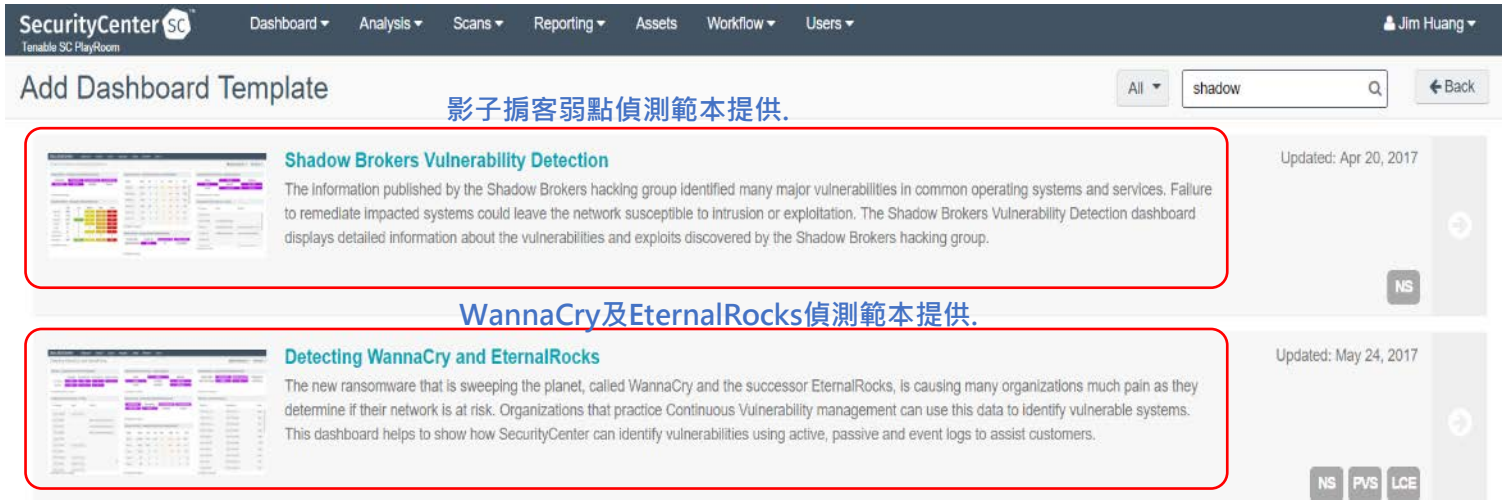
提供重大威脅的弱點掃瞄政策，管理者可直接選用.



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.



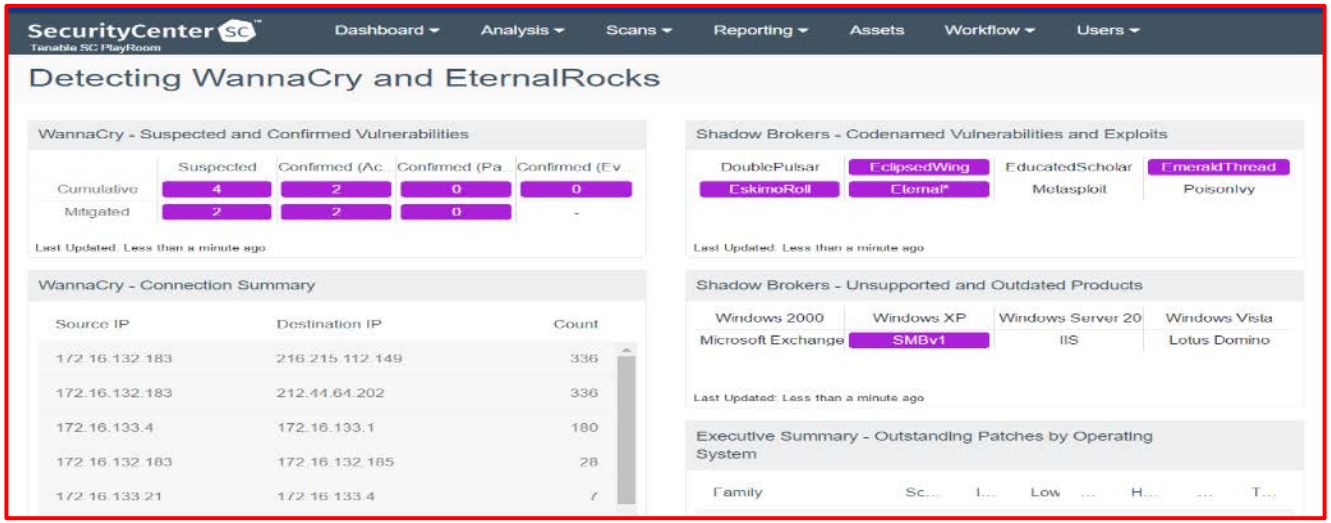
影子掮客弱點偵測範本提供.

WannaCry及EternalRocks偵測範本提供.

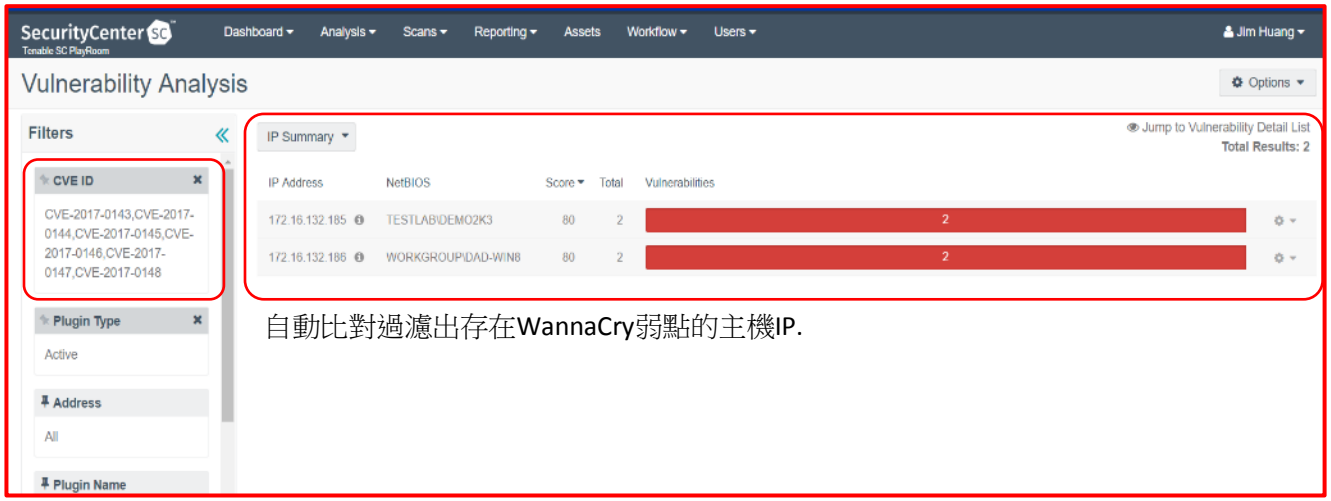
UNIFORCE 創泓科技

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

結語

- 避免讓風險空窗期延宕，快速發現、快速應對、快速釐清。
- 避免過度反應，理性面對弱點威脅。
- 避免固守舊知看待新事物，弱點威脅並非一成不變。
- 避免一昧倚賴防禦器具，對症下藥的佈署設計才能發揮防護效果。
- 避免一視同仁的管理政策，對應正確的方式可以事半功倍與精確。
- 避免追求完美完全的要求，快速反應與效率處理才是最佳。
- 避免消極的責任分派與究責，建立積極的分工合作與獎勵。
- 避免夢想一勞永逸的靈丹妙法，尋求上手的工具與管理機制會更實際。

UNIFORCE 創泓科技

大綱介紹

Q & A

UNIFORCE 創泓科技