

「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

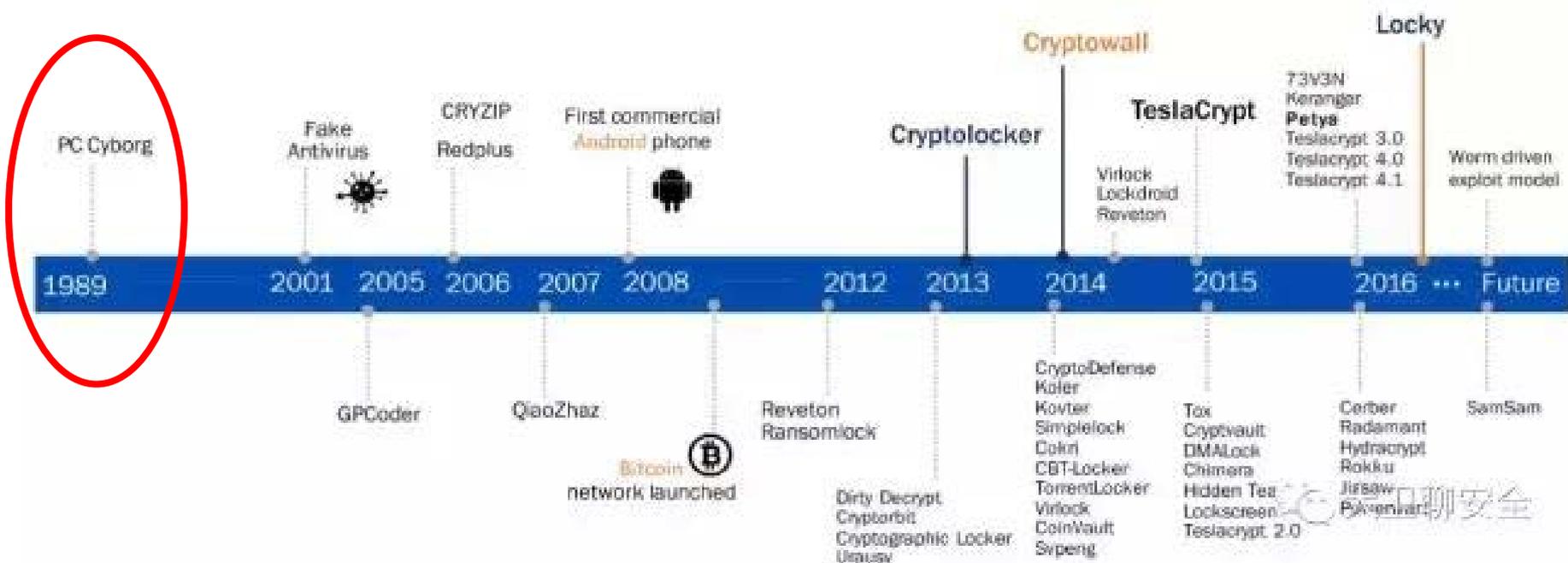
大綱介紹

- 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

資安威脅分析



勒索威脅當道



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

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

案例: WannaCry (想哭) 加密勒索威脅

Wana Decrypt0r 2.0

Oops, your files have been encrypted!

Chinese (traditional)

我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。

有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。但這是收費的，也不能無限期的推遲。請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。但想要恢復全部文檔，需要付款點費用。是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。最好3天之內付款費用，過了三天費用就會翻倍。還有，一個禮拜之內未付款，將會永遠恢復不了。對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪

Payment will be raised on
5/15/2017 23:41:55
Time Left
02:23:55:59

Your files will be lost on
5/19/2017 23:41:55
Time Left
06:23:55:59

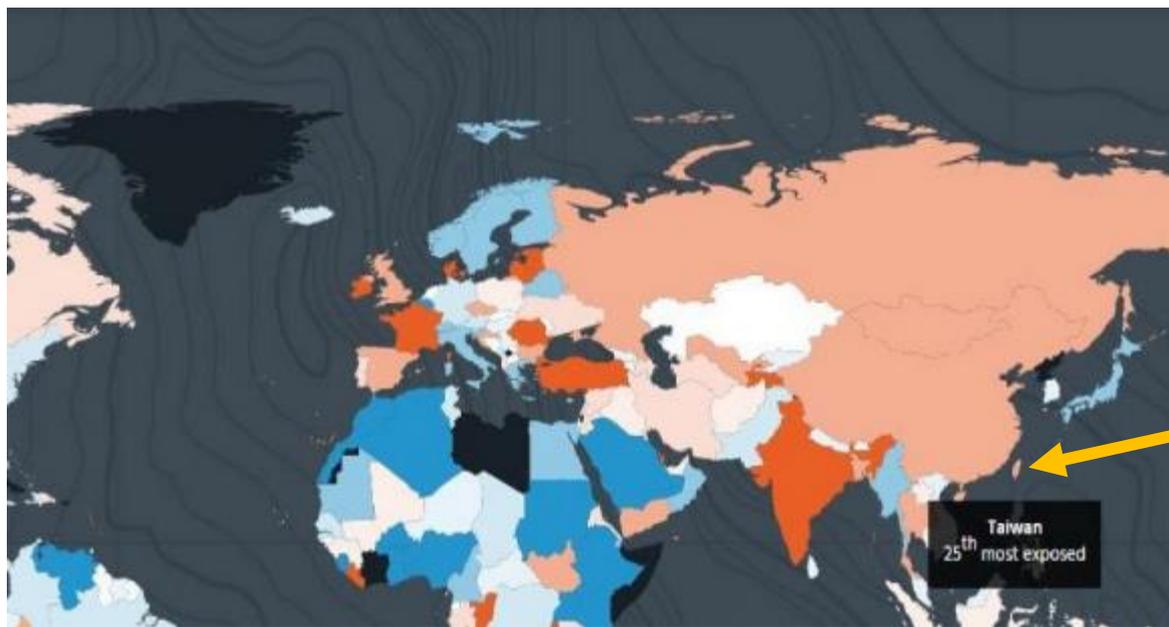
About bitcoin
How to buy bitcoins?
Contact Us

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

案例: WannaCry (想哭) 加密勒索威脅

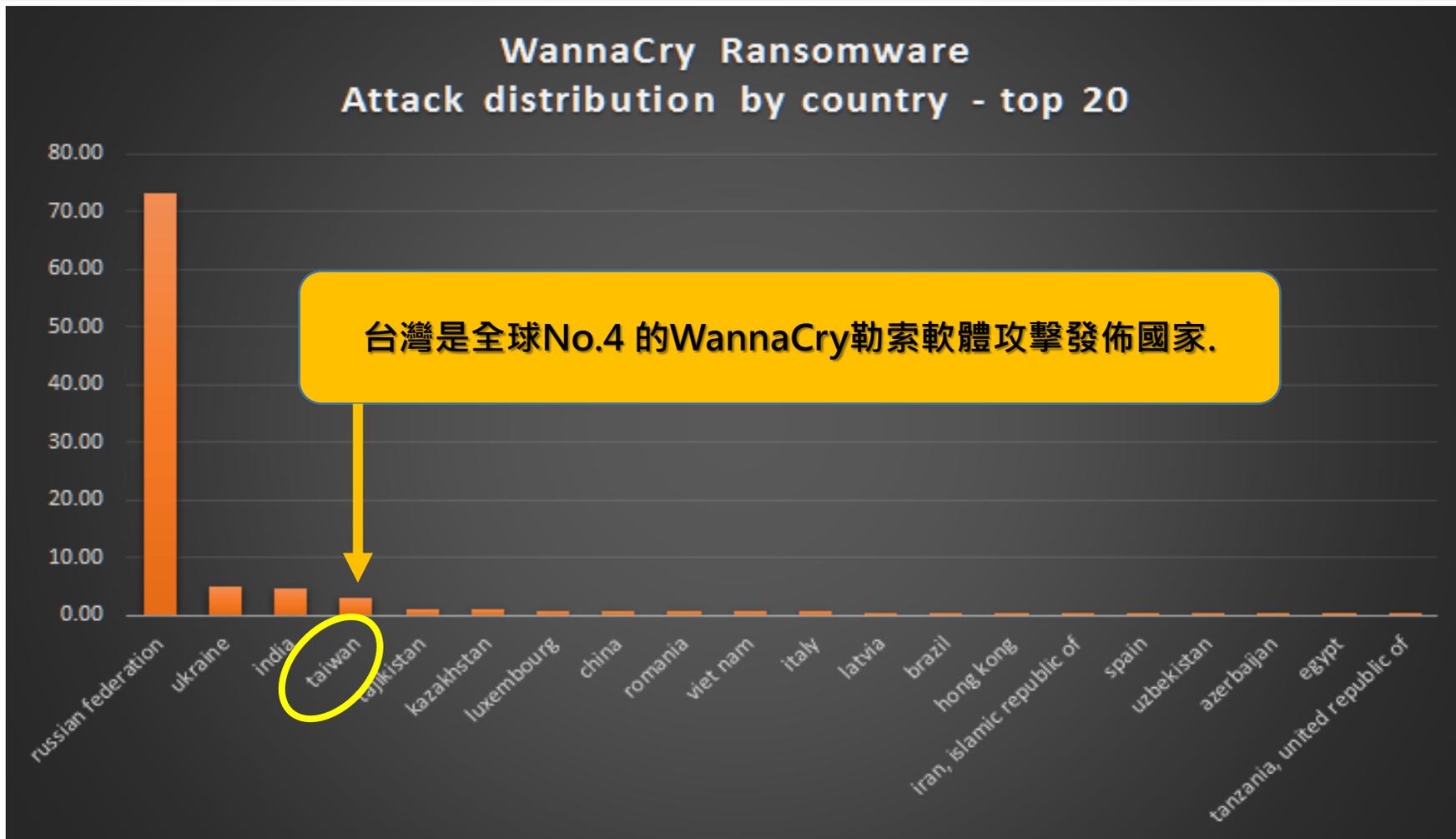
- 2017年5月爆發史上影響最大的全球性勒索蠕蟲事件。
- 五個小時內影響覆蓋美國、俄羅斯、整個歐洲等100多個國家。(超過20多萬台電腦受害)
- 中國多個高校校內網、大型企業內網和政府機構專網中招。
- SMB 漏洞MS17-010，微軟已在今年3月份發布了該漏洞的補丁。
- 嚴重程度之高，微軟破例釋出Win XP及Win Server 2003等系統修補。(最近一次: 2014年)



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

案例: WannaCry (想哭) 加密勒索威脅



資料來源: [Securelist](#).

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://themerle.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://themerle.com/original-petya-developer-releases-master-decryption-key-for-all-variants/>
- [2]<http://www.techbang.com/posts/52462-petya-draw>

Unwire.hk

Petya爆發

有 Win 更新也中招！比 WannaCry 強

全球電腦災難 2

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的資安弱點即便經過修補，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。

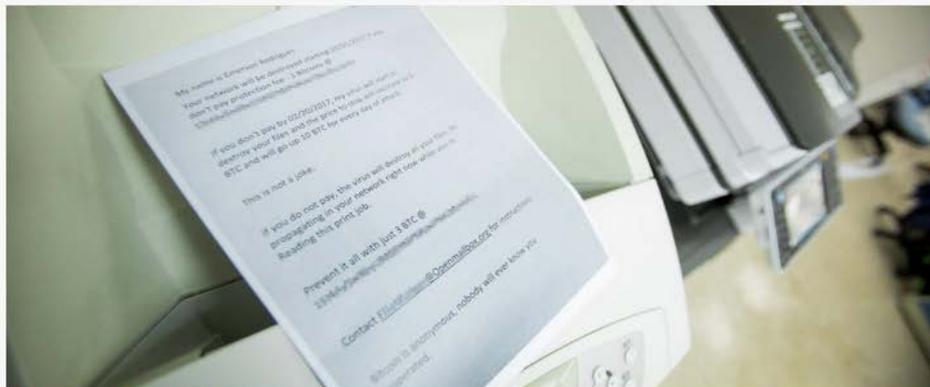
案例: 校園網路印表機勒索威脅

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/ 吳泓瑜 | 2017-02-22 發表

按讚加入iThome粉絲團 分享 2,281



各級學校在印表機收到駭客勒索信

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？

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。

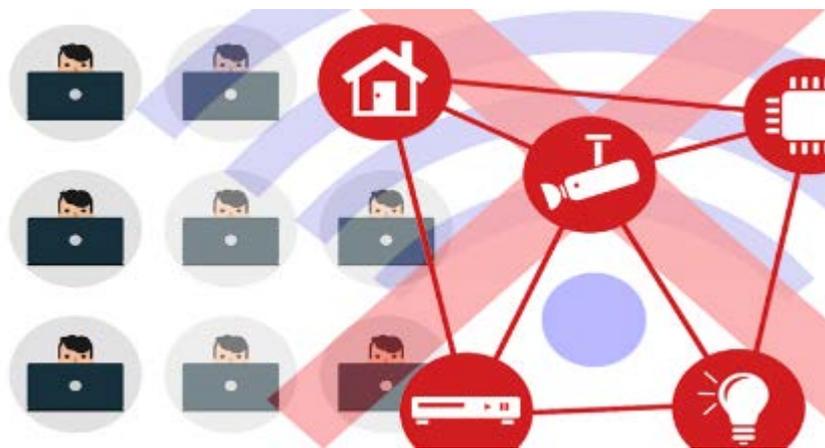
本次事件中學校收到勒索傳真，勒索支付日期為2月20日及3月1日前完成，據了解，學校並無實際支付。透過臺灣學術網路危機處理中心(TACERT)通報系統，學校若有問題及疑慮可即時回報，本部將即時掌握受害情況，網路印表機列印勒索建議採取適當作法，防護措施建議如下：

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。

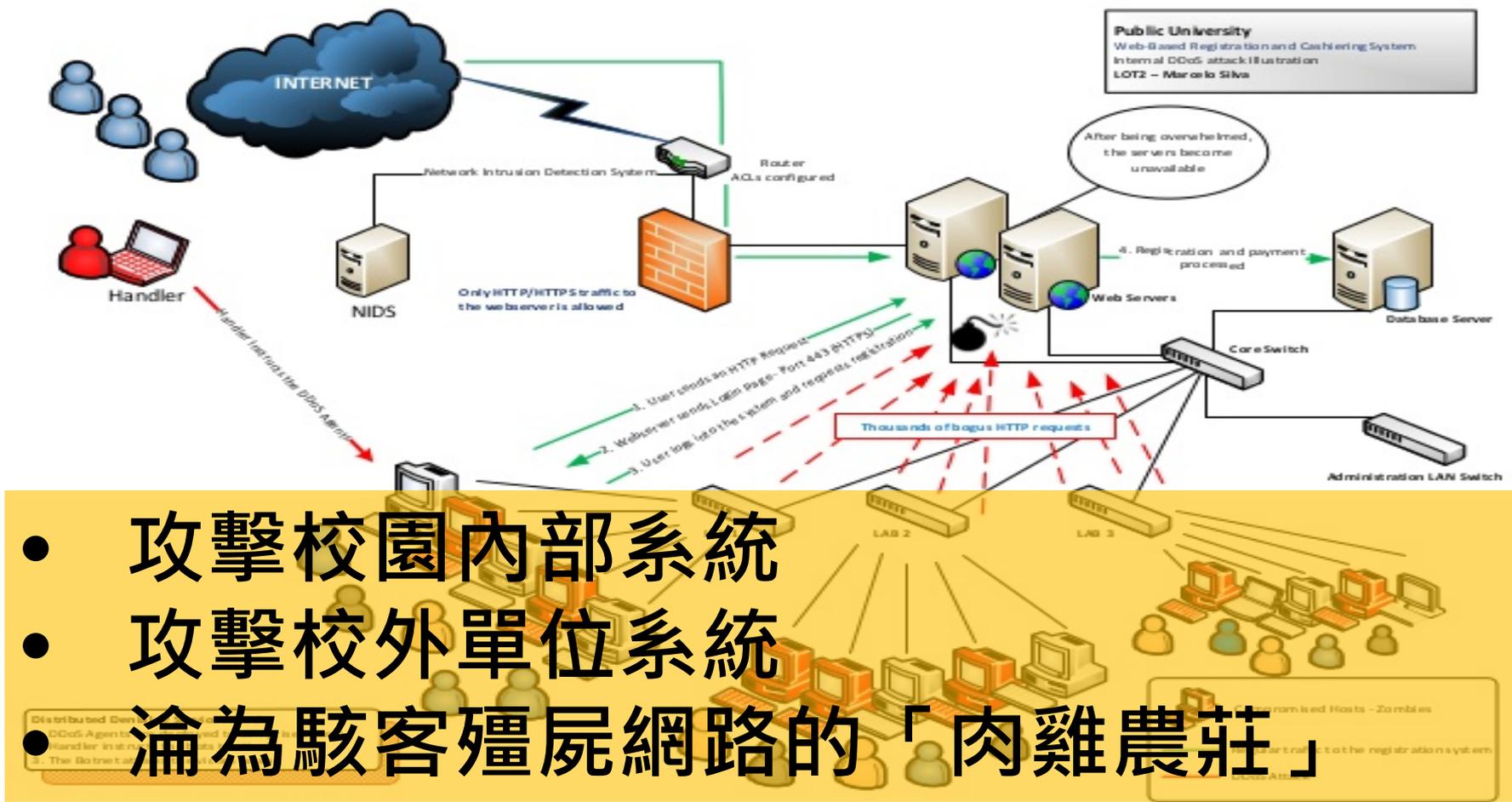
另外，本部已請教育體系資安防護團隊加強網路資安偵測，各校若有資安入侵攻擊事件時，請速依資安通報應變程序通報，本部將儘速協助處理。

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。



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」

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

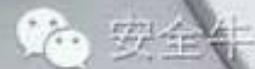
怎麼看待「弱點漏洞」

弱點漏洞

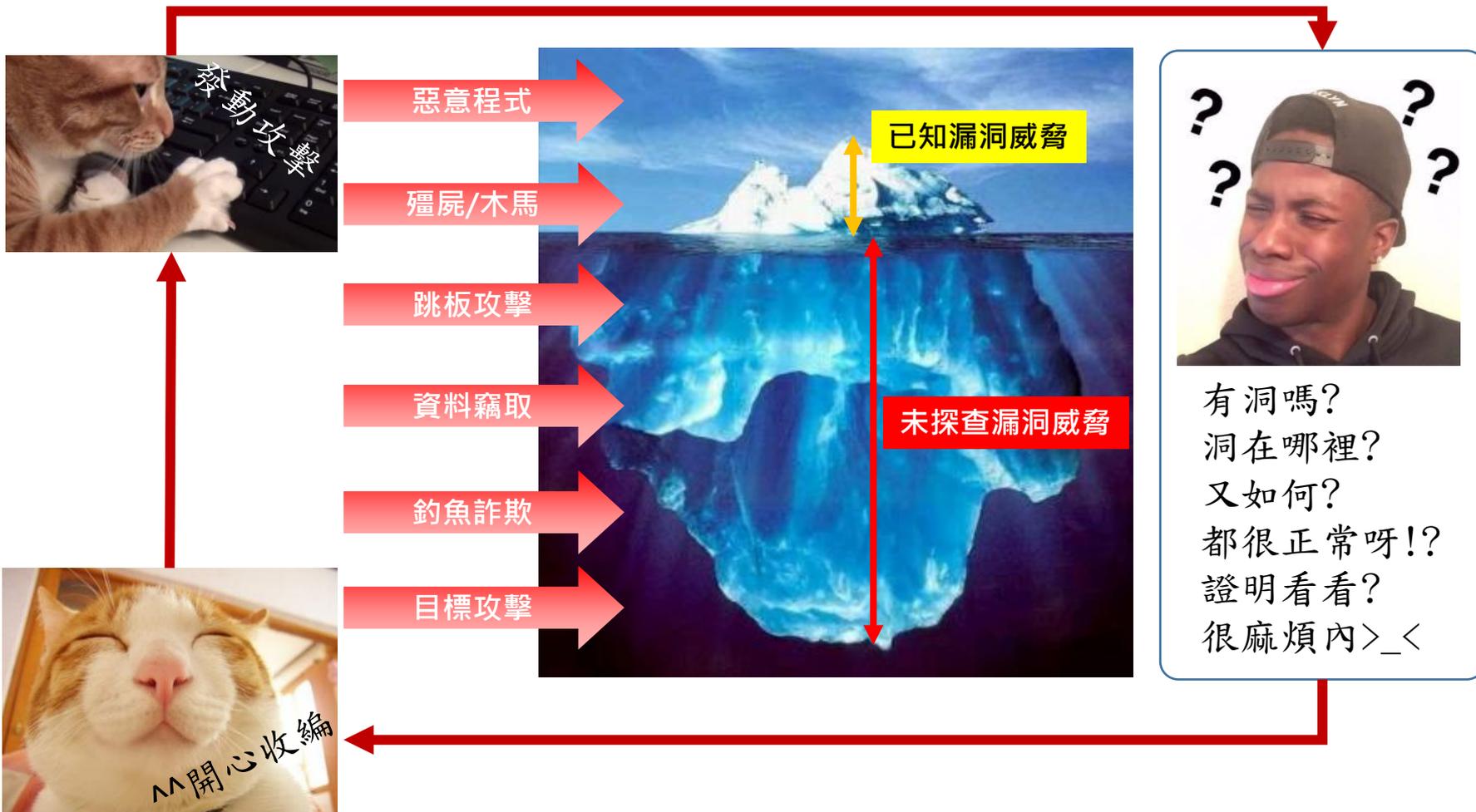
不管嚴重等級是高(High)還是低(Low)

只要可以利用，就是好弱點

如果容易利用，那就是絕佳好弱點



現今資安威脅有近9成利用漏洞！！



現今資安攻擊的「起手式」

FireEye Mandiant M-Trend Report 2017



侵入應用程式或OS
的漏洞 (Exploit)

回 Call 控制中心

下載惡意軟體本體

橫向散播

資料竊取



弱點漏洞是怎麼發生？

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

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

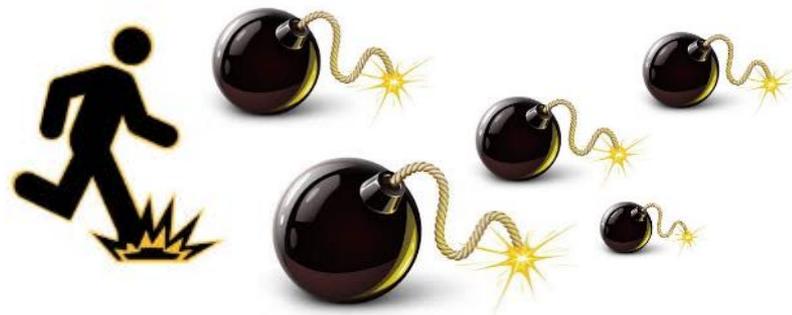
未來四年之內，零時差漏洞出現的頻率很可能提高到每天一次

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

Share

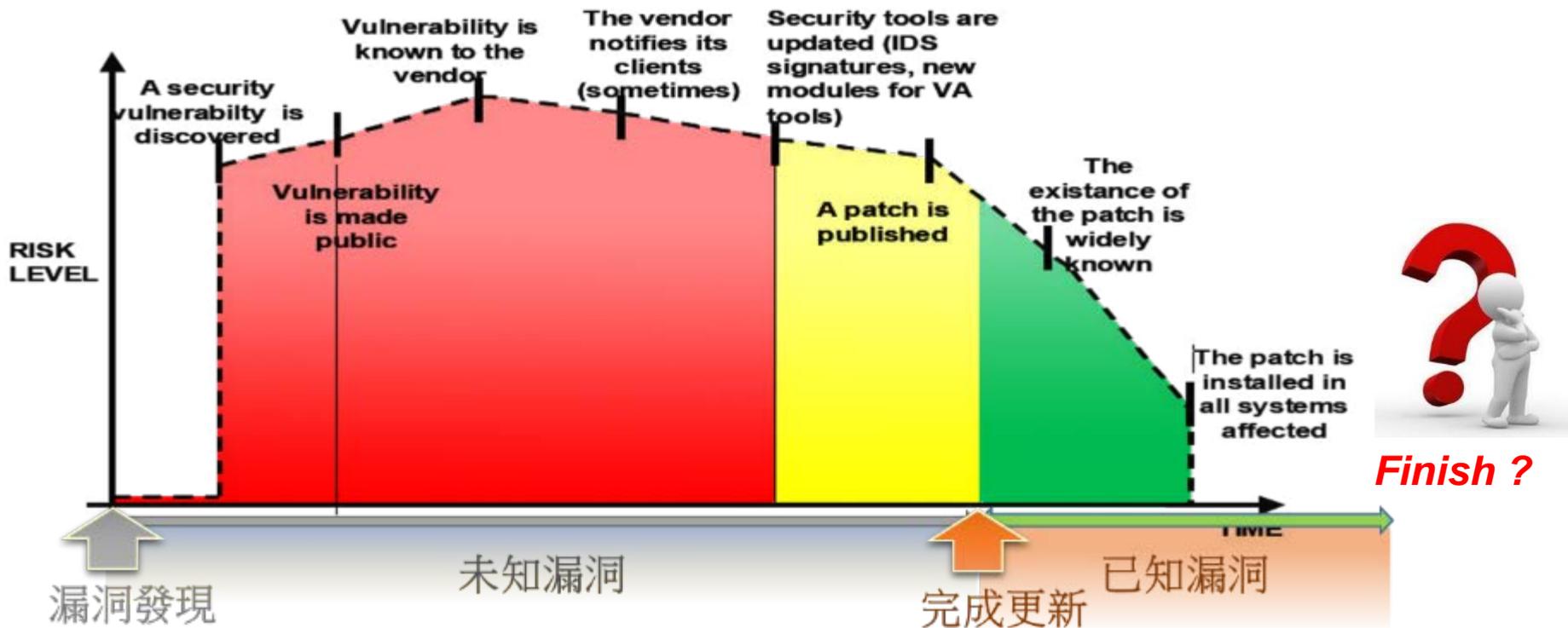
零時差漏洞 (也就是從未被發現的新漏洞) 最近出現的頻率越來越高，更糟的是，這些危險的漏洞經常都是在駭客攻擊事件發生之後，人們才知道漏洞的存在。

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



弱點漏洞的生命週期

Window of Vulnerability



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

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

從本月開始微軟首次採用新的Windows 更新政策，此次更新發布了10個安全公告，共修補45個漏洞，包含5個安全漏洞，可造成遠端程式攻擊，另外還包括5個已被開採的零日漏洞。

文/ 陳曉琪 | 2016-10-12 發表

微軟修補由Google揭露的安全漏洞

週二的例行更新修補了14個安全公告，涵蓋在 Microsoft Edge、Microsoft Office 辦公室產品、Windows 執行程式的零日安全漏洞，以及由來自Google揭露的漏洞。

文/ 陳曉琪 | 2016-10-12 發表

Linux磁碟加密工具Cryptsetup爆重大漏洞

該漏洞存在於使用LUKS統一全盤加密的Linux版本，LUKS為Linux系統加密的標準機制，通常用於Cryptsetup工具使用，受到影響的Linux版本包括Debian、SUSE Enterprise Linux、Red Hat Enterprise Linux、Ubuntu和Fedora。

文/ 陳曉琪 | 2016-11-30 發表

重要商務系統弱點

甲骨文一次修補276個安全漏洞，寫下新紀錄

甲骨文上周一口氣修補旗下84款產品共276個安全漏洞，一舉超越第一季例行修補的248個漏洞，創下甲骨文漏洞修補的紀錄，這批漏洞中有19個屬CVSS5評分9.8分的重大漏洞，甲骨文呼籲用戶應儘快更新。

文/ 陳曉琪 | 2016-07-26 發表

甲骨文修補308個安全漏洞，創新紀錄!

308個漏洞中有185個可能導致遠端程式攻擊，60.1%漏洞與甲骨文Oracle E-Business Suite，設備可能允許攻擊者管理、升級管理、人員管理、供應管理。

文/ 陳曉琪 | 2017-05-24 發表

應用程式弱點導致資料外洩

Adobe搶修已遭攻擊的Flash漏洞

使用者只要檢視惡意的Flash媒體檔案就可能觸發該漏洞，駭客藉此遠端執行任意程式，操控使用者的電腦，Adobe已接獲該漏洞的攻擊報告，目前集中於Windows系統，但其他平台也同樣曝露於漏洞的風險。

文/ 陳曉琪 | 2014-10-27 發表

DB弱點導致伺服器淪陷

MySQL爆最高權限漏洞，MariaDB、PerconaDB亦受影響

研究人員揭露了兩個MySQL漏洞分別為重大及高度風險漏洞，最嚴重可讓駭客取得資料庫最高權限，包含MySQL 5.5.51、MySQL 5.6.32及MySQL 5.7.14及之前版本，還有基於這些版本的MariaDB與PerconaDB。

文/ 陳曉琪 | 2016-11-03 發表



資安研究人員David Golinski周二 (11/1) 揭露了兩個MySQL最高權限漏洞，這批漏洞可能導致駭客取得資料庫的安全漏洞，這批漏洞可能導致駭客取得資料庫最高權限，包含MySQL 5.5.51、MySQL 5.6.32及MySQL 5.7.14及之前版本，還有基於這些版本的MariaDB與PerconaDB。

相關的漏洞編號是 CVE-2016-6664 及 CVE-2016-6665，後者則是高度風險漏洞，影響MySQL 5.5.51、MySQL 5.6.32及MySQL 5.7.14及之前版本，還有基於這些版本的MariaDB與PerconaDB。

文/ 陳曉琪 | 2017-05-24 發表

「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)

資安業者TDC Security Operations Center展示一項名為「黑護士」的攻擊行動，駭客利用CMP發動攻擊，癱瘓少量CMP Type 3 Code 3，只利用少量筆電，就能癱瘓包含思科、合勤、SonicWall及Palo Alto Networks的防火牆。

文/ 陳曉琪 | 2016-11-14 發表

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

由於賽門鐵克旗下多款安全產品採用相同核心引擎，整個連鎖的安全產品包含17項企業產品Symantec Endpoint Protection、Norton防病毒軟體，包括所有平台的Norton 360、Endpoint Protection、Email Security及Protection Engine等等，賽門鐵克已釋出更新修復漏洞。

文/ 陳曉琪 | 2016-09-30 發表



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

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

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/ 陳曉琪 | 2017-05-24 發表

資安系統弱點導致防護破壞

弱點無處不在，魔鬼藏在細節中

OpenSSL Heartbleed 漏洞危機特別報導

政府網站安全未明 資安辦 4月底才能掌握

駭客利用Heartbleed 漏洞入侵VPN 多因素認證防

IT產品Heartbleed災情大清查

OpenSSL又爆1998年就存在的嚴重漏洞，SSL

CVE-2014-0195是屬於「DTLS無效片斷漏洞」，可能讓駭客得以遠端執行任意程式碼，因此被SANS列為重大漏洞。但這次公布的六個漏洞最受關注的是CVE-2014-0224，這項已存在超過15年的「SSL/TLS中間人攻擊漏洞」，可能讓駭客得以用來破解SSL及TLS流量，甚至修改其中內容。

文/ 林妍濤 | 2014-06-06 發表

Cisco及Juniper針對HeartBleed漏洞發布緊急安全通告

面對網路有史以來最嚴重的OpenSSL HeartBleed漏洞，IT廠商皆嚴陣以待，網路設備大廠Cisco及Juniper也雙雙公佈HeartBleed安全漏洞的安全警報。

文/ 林妍濤 | 2014-04-11 發表

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

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

弱點無處不在，魔鬼藏在細節中

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，原因之一為大量的軟體與Bash Shell互動，如同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

讚 1.1萬 按讚加入iThome粉絲團 讚 分享 3,345 8+1 98

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

讚 7,706 按讚加入iThome粉絲團 讚 分享 1,128 8+1 18

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/ 林妍蓀 | 2014-10-07 發表

讚 7,706 按讚加入iThome粉絲團 讚 分享 120 8+1 0

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。

開源軟體(Open Source) 安全分析

OPEN SOURCE SECURITY ANALYSIS 2016 REPORT

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



Average amount of open source code in each application.

105

Average number of open source components found in each application



67% of applications reviewed contained known open source security vulnerabilities



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



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

1,894 DAYS



Average age of known open source security vulnerabilities



22.5

Average number of known open source security vulnerabilities in each application



10% of the applications included the Heartbleed vulnerability

安全脆弱度，只需要一個正確的点



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

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

弱點掃描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

弱點掃描與滲透測試的微妙關係

體能檢驗



健康檢查



弱點掃描與滲透測試的微妙關係

目的相同的不同檢驗方式.

弱點掃描
Vulnerability Scanning

滲透測試
Penetration Testing



弱點掃描與滲透測試的微妙關係

	弱點掃描	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。

The screenshot shows the CVE website homepage with the following elements:

- Header:** CVE logo, "Common Vulnerabilities and Exposures", "The Standard for Information Security Vulnerability Names", and navigation links (Home, CVE IDs, About CVE, CVE in Use, Community & Partners, Blog, News, Site Search). It also displays "TOTAL CVE IDs: 88416" and social media icons for Twitter and LinkedIn.
- Main Content Area:** Five columns of links: "Request a CVE ID", "Update info in a CVE ID", "CVE List downloads", "CVE content data feed", and "Become a CNA".
- Left Column (CVE Blog):** "Become a CNA" section with text about CNA participation and a "More >>" link.
- Middle Column (Latest CVE News):** "Latest CVE News" section with three news items: "Alibaba Added as CVE Numbering Authority (CNA)", "Minutes from CVE Board Teleconference Meeting on July 26 Now Available", and "Slides from 'CVE IDs and How to Get Them' Talk at DEF CON 25 Now Available". It also includes a "REMINDER: 'REJECT' Is Not Always a Permanent State for a CVE ID Begins July 27, 2017" and a "More >>" link.
- Right Column (Focus On):** "Focus On" section titled "CVE Now on LinkedIn and Twitter" with instructions to follow on social media and links to "@CVEnew" and "@CVEannounce". It also includes a "More >>" link.
- Footer:** MITRE logo, "Page Last Updated or Reviewed: August 02, 2017", and legal disclaimers regarding the use of the CVE List and associated references.

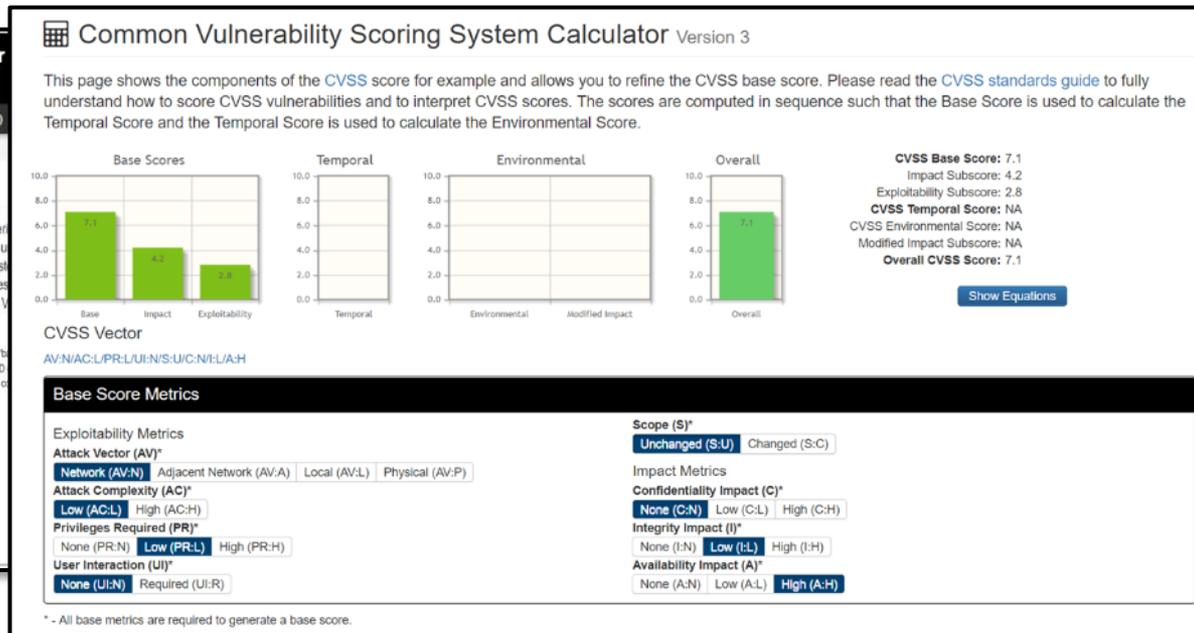
<https://cve.mitre.org/>

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>



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.

The screenshot shows the Exploit-DB website interface. The main navigation bar includes 'Home', 'Exploits', 'Shellcode', 'Papers', 'Google Hacking Database', 'Submit', and 'Search'. The page title is 'Offensive Security's Exploits Database'. A prominent banner reads 'The Exploit Database (EDB) is a CVE compliant archive of vulnerable software. A great resource for penetration testers, researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy-to-use location. Download the Exploit Database Archive'.

The 'Remote Exploits' section is visible, listing various exploits. A table of exploits is shown with columns for Date, D (Download), A (Authenticated), V (Verified), Title, Platform, and Author. Red arrows point from the 'D', 'A', and 'V' columns to yellow callout boxes with the following text:

- Verification** (points to the 'V' column)
- Download Vulnerable Application** (points to the 'A' column)
- Download Exploit Code** (points to the 'D' column)

Date	D	A	V	Title	Platform	Author
2017-08-01	✓	-	-	[Hebrew] Digital Whisper Security Magazine #85	Papers	cp77fk4r & ...
2017-08-01	✓	-	✓	Advantech SUSIAccess <= 3.0 - Directory Traversal (PoC)	JSP	James Fitts
2017-08-01	✓	-	✓	Advantech SUSIAccess <= 3.0 - 'RecoveryMgmt' File Upload	JSP	James Fitts
2017-08-01	✓	✓	✓	VehicleWorkshop - Authentication Bypass		
2017-08-01	✓	✓	✓	VehicleWorkshop - Arbitrary File Upload		
2017-08-01	✓	-	-	[Hebrew] Digital Whisper Security Magazine #84		cp77fk4r & ...
2017-08-01	✓	-	✓	iOS/macOS - xpc_data Objects Sandbox Escape Priv		Google Secu...
2017-08-01	✓	-	✓	SOL.Connect ISET-mpp meter 1.2.4.2 - SQL Injection	Hardware	Andy Tan
2017-08-01	✓	-	✓	libmad 0.15.1b - 'mp3' Memory Corruption	Linux	qflb.wu
2017-07-31	✓	-	✓	DivFix++ 0.34 - Denial of Service	Linux	qflb.wu
2017-07-31	✓	-	✓	Vorbis Tools oggenc 1.4.0 - '.wav' Denial of Service	Linux	qflb.wu
2017-07-31	✓	-	✓	Sound eXchange (SoX) 14.4.2 - Multiple Vulnerabilities	Linux	qflb.wu
2017-07-31	✓	-	✓	libvorbis 1.3.5 - Multiple Vulnerabilities	Linux	qflb.wu
2017-07-31	✓	-	✓	libao 1.2.0 - Denial of Service	Linux	qflb.wu

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

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。

All Vulnerabilities

(Critical, High, Medium, Low, Info)

Exploitable
= Yes

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

Exploit-db公佈可利用code及方法

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

弱點資訊參考資源

CVE Details
The ultimate security vulnerability datasource

Search: View CVE

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

Current CVSS Score Distribution For All Vulnerabilities

CVSS Score	Number Of Vulnerabilities	Percentage
0-3	302	0.30
1-2	603	0.60
3-3.9	2469	2.47
4-4	2171	2.17
4-5	17013	17.01
5-6	18557	18.56
6-7	12827	12.83
7-8	22229	22.23
8-9	252	0.25
9-10	12430	12.43
Total	84263	

Weighted Average CVSS Score: 6.8

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

IT Security Database
Vulnerability, patch and compliance datasource

Home Help Search CVE Vulnerability Database

What is this site ?

This site collects OVAL (Open Vulnerability and Assessment Language) definitions from several sources like Mitre, Red Hat, Suse, NVD, Apache etc and provides a unified, easy to use web interface to all IT security related items including patches, vulnerabilities and compliance checklists.

You can view full details of oval definitions, which is not possible at any other public web site. Other similar web sites just display comments about the definitions but here you can view exactly what you should look for to verify a vulnerability or a patch. Without itsecdb.com it is almost impossible to view details of an OVAL definition without getting lost in several xml files, definition documentation, xml schemas etc.

itsecdb is fully integrated to www.cvedetails.com so you can easily navigate between CVE, product and oval definition details. Most of the definitions, whenever cpe or vulnerability mappings are possible, are mapped to products defined by cvedetails.com to increase usability.

You can also browse or search for items used in oval definitions like file names, rpm packages, AIX patch numbers etc, so you can easily find all patches or vulnerabilities related to any file. For example you can view list of all patches, vulnerabilities and compliance checks related to [mshtml.dll](#) here.

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

tenable Cyber Exposure Products Services Company Partners Blog

Plugins

Plugins Newest Plugins Obtain an Activation Code View All Plugins Search

There are 89382 plugins, covering 39781 unique CVE IDs and 26050 unique Bugtraq IDs.

- AIX Local Security Checks
- Amazon Linux Local Security Checks
- Backdoors
- CentOS Local Security Checks
- CGI abuses
- CGI abuses : XSS
- CISCO
- Databases
- Debian Local Security Checks

Ready to Nessu
Get Nessus Pro
IPs, run con
Buy Nessu

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

SHODAN Explore Enterprise Access Contact Us

Devices Vulnerable to Heartbleed

Search for `ssl.cve-2014-0160` returned 237,539 results on 29-09-2016

Top Countries

1. United States	57,598
2. China	17,455
3. Germany	17,273
4. France	10,708
5. India	9,427
6. United Kingdom	9,268
7. Russian Federation	7,897
8. Korea, Republic of	7,525
9. Brazil	7,095
10. Japan	5,302

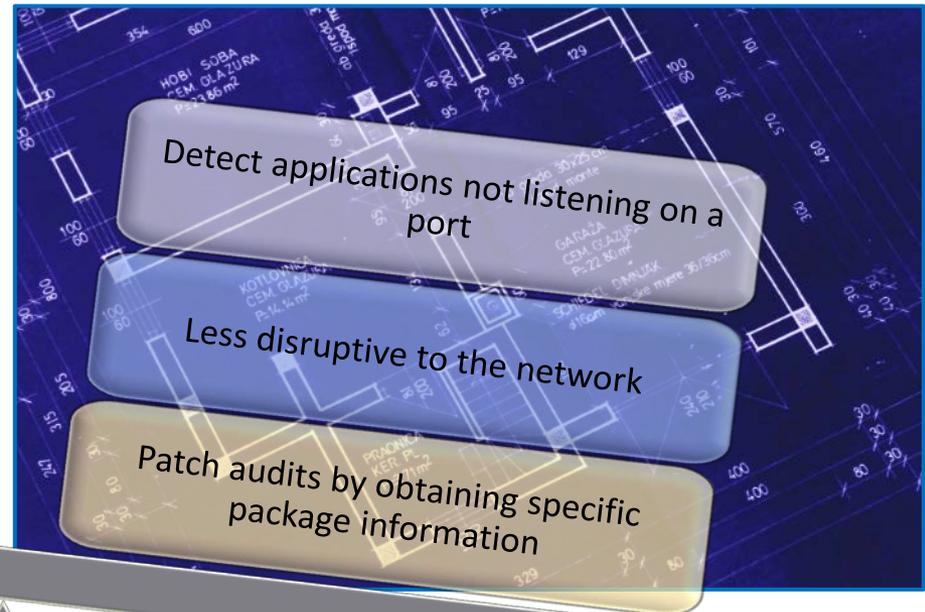
<https://www.shodan.io/>

常見弱點掃描方式

網路掃描 (Network Scan)

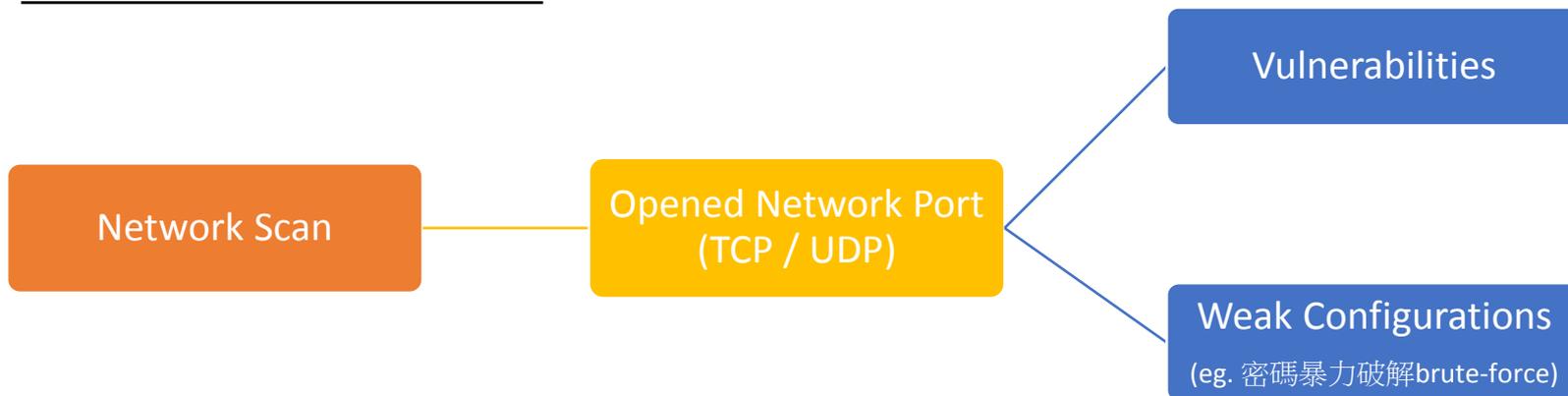


授權掃描 (Credential Scan)



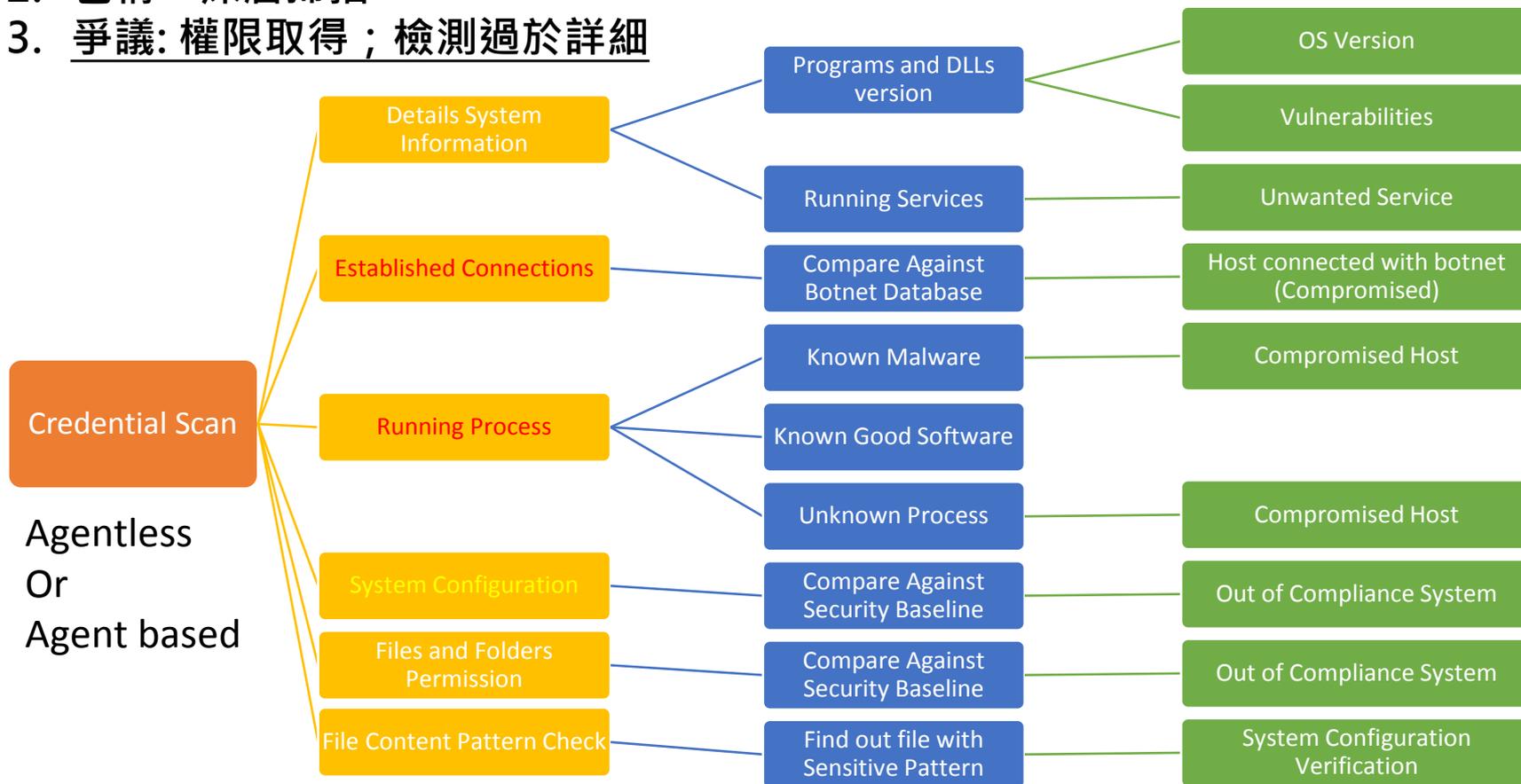
常見弱點掃描方式:網路掃描 (Network Scan)

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



常見弱點掃描方式: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



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。



白箱測試 vs. 黑箱測試 的優缺差異

以Web系統為例:

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

防護架構檢測

網站系統檢測

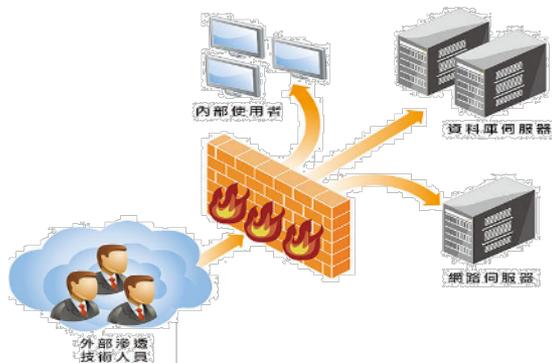
穿透檢測

原始碼檢測

周邊安全檢測

專業滲透測試服務的程序

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



常見的滲透測試議題

□ 訊息蒐集

□ 目標探測

□ 弱點評估

□ Web掃描

□ 社交工程

□ 資料庫探測與攻擊

□ 密碼破解

□ 漏洞利用

□ 提權工具

□ 持續控制工具

□ 無線網路攻擊

□ 壓力測試

□ 測試報告

滲透測試資源參考

A dark blue banner with a white dragon logo on the right side. The text on the left reads "APRIL 25, 2017" and "Kali Linux 2017.1 Release". A "READ MORE" button is centered at the bottom. On the right, there are three news snippets: "KALI LINUX NEWS Kali Drones, Portable CTF Builds, Raspberry Pi Craziiness and More!", "KALI LINUX NEWS, KALI Kali Linux 2017.1 Release", and "KALI LINUX NEWS Kali Linux Repository HTTPS Support".

APRIL 25, 2017

Kali Linux 2017.1 Release

READ MORE

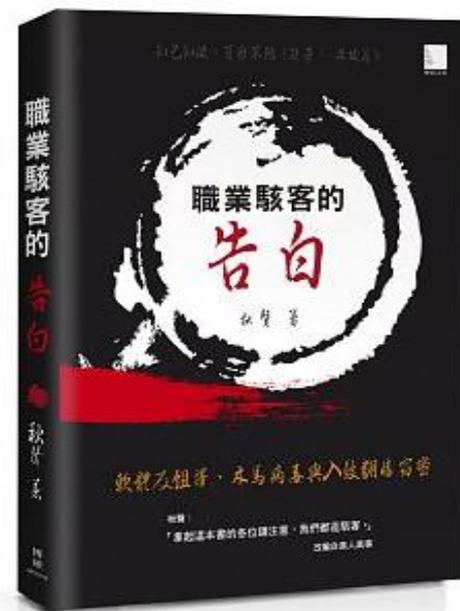
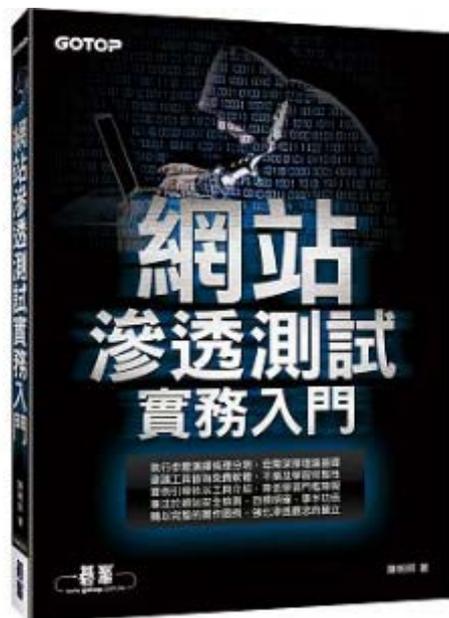
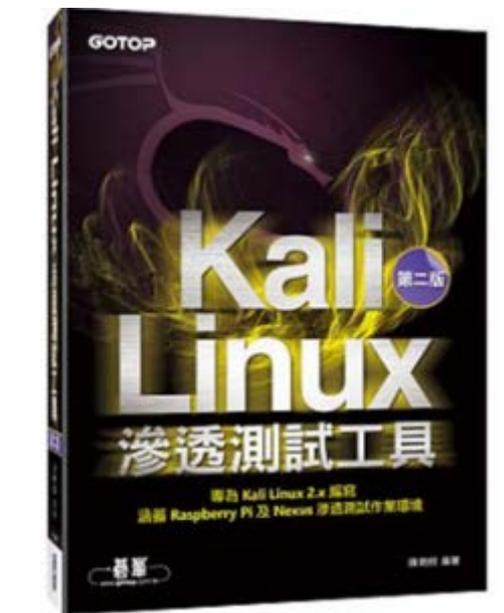
KALI LINUX NEWS
Kali Drones, Portable CTF
Builds, Raspberry Pi
Craziiness and More!

KALI LINUX NEWS, KALI
Kali Linux 2017.1 Release

KALI LINUX NEWS
Kali Linux Repository HTTPS
Support

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

滲透測試資源參考



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

弱點掃描與滲透測試的真義

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

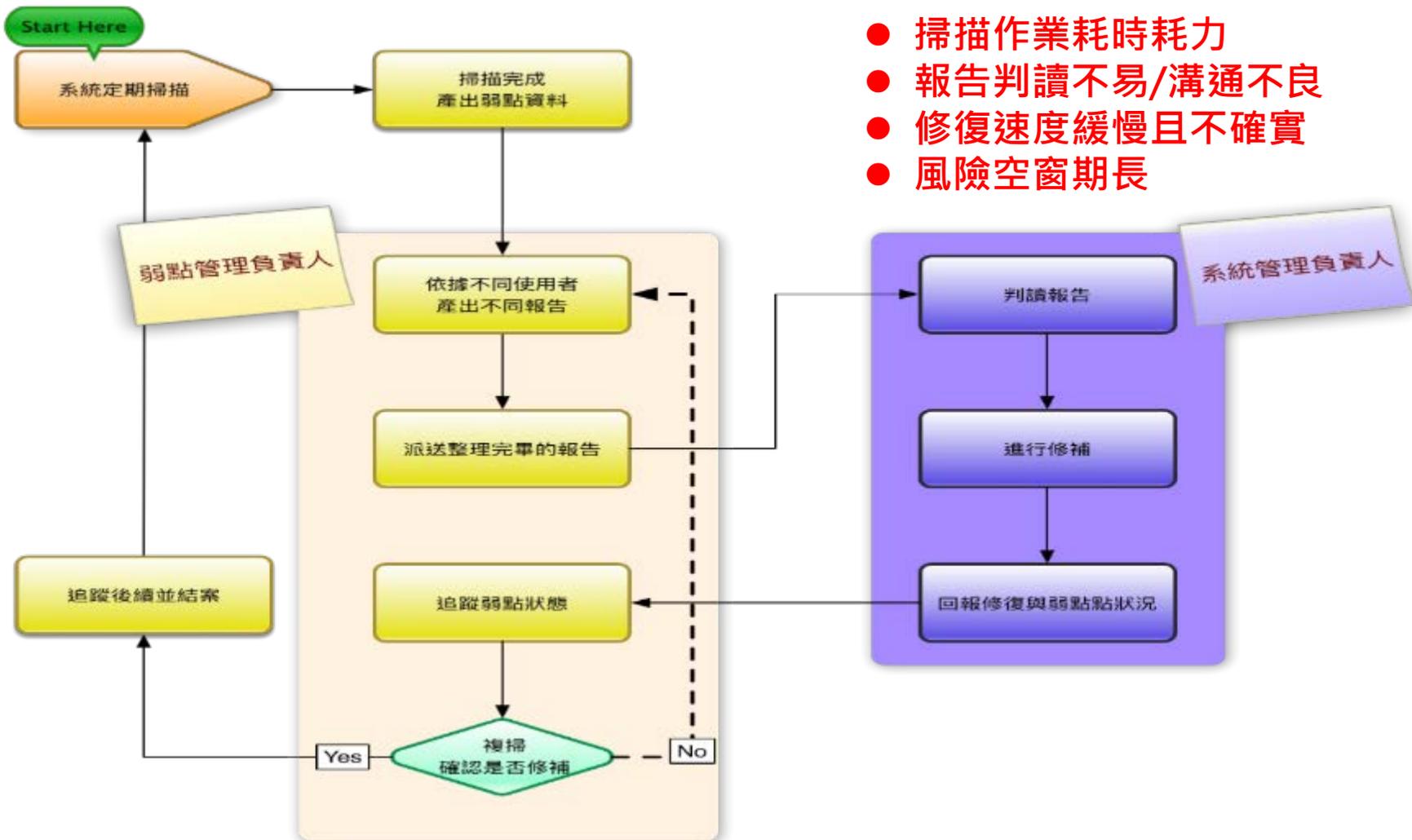


圖片來源: Dreamstime

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

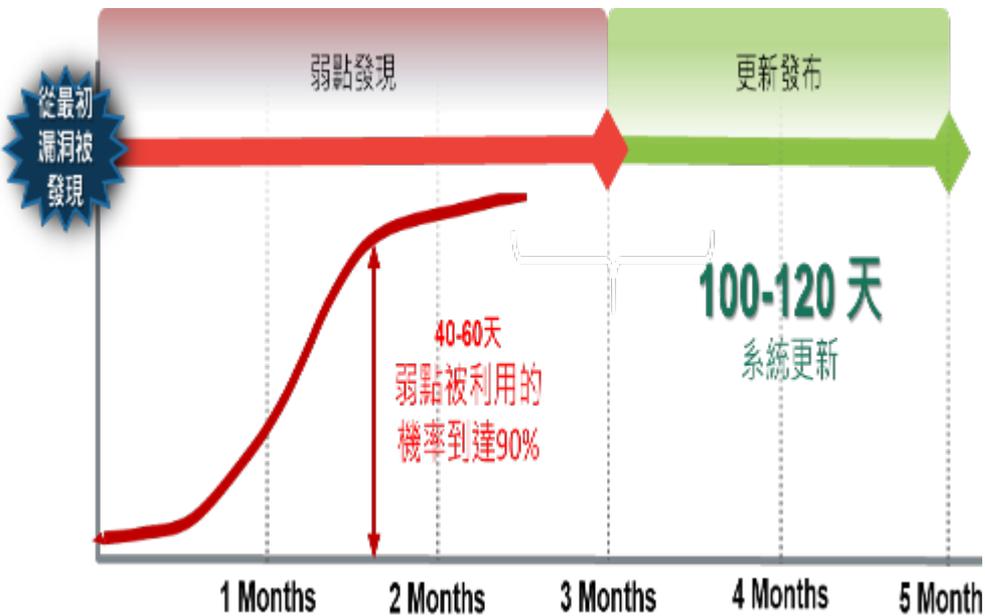
弱掃稽核的困擾



- 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

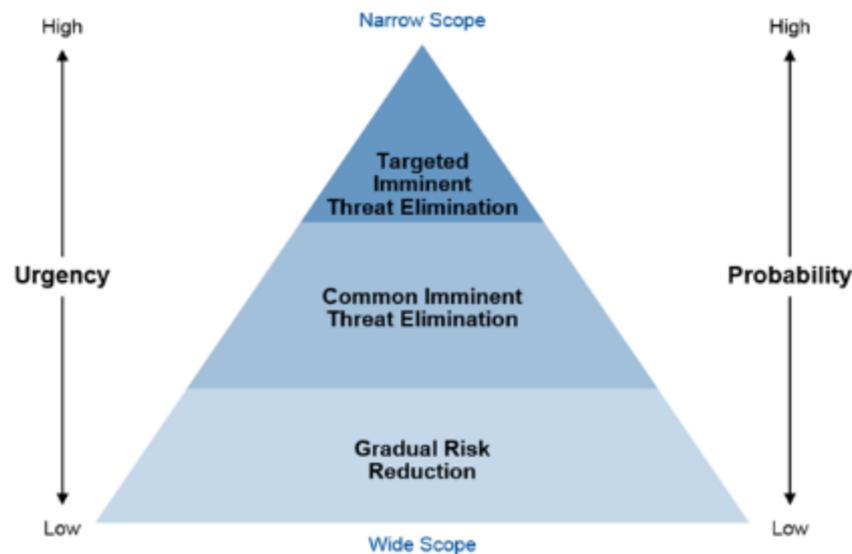
當務之急: 有效率的弱點管理

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)

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)

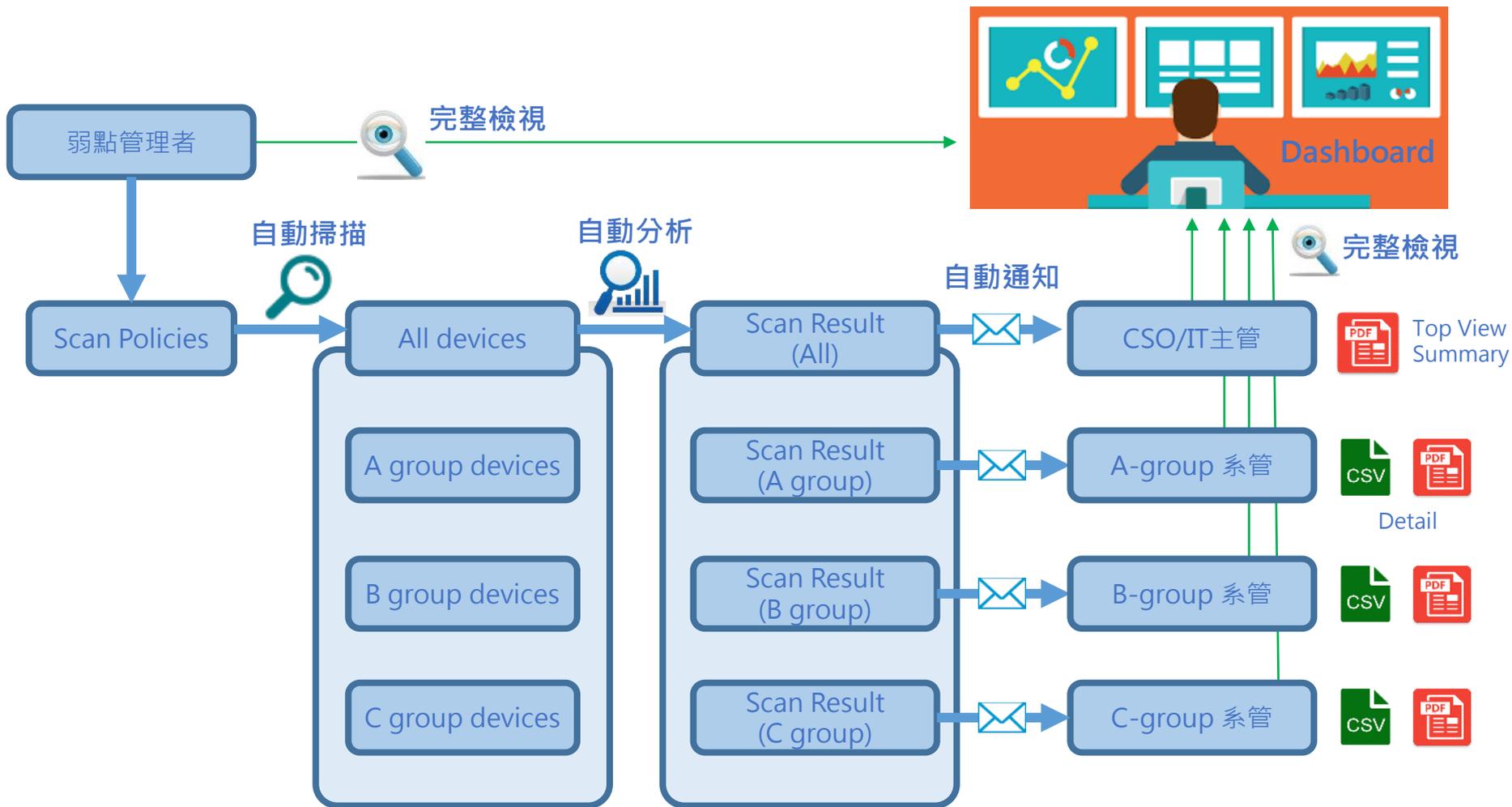
管理者群組建立:

- 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

弱掃作業自動化

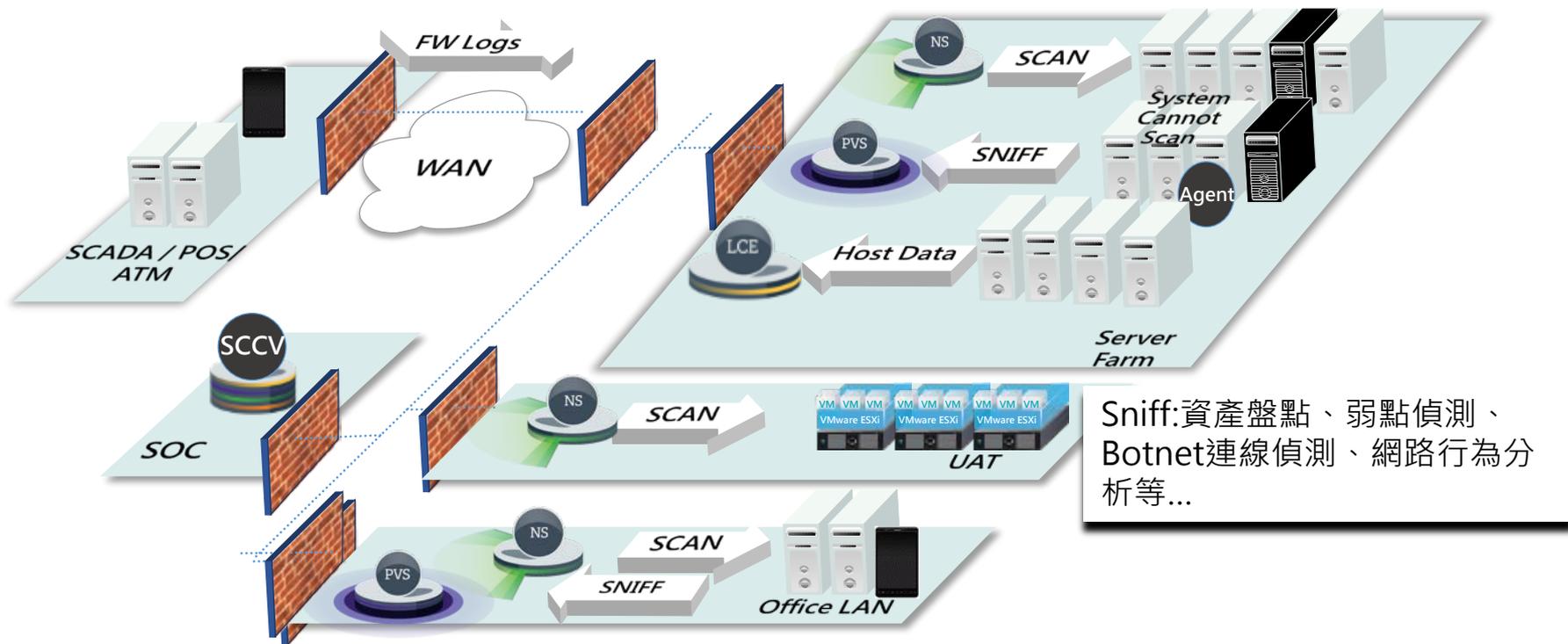


弱掃部署架構設計

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...

風險管理方式: 接受風險/調整等級

弱點修補改善困難之處

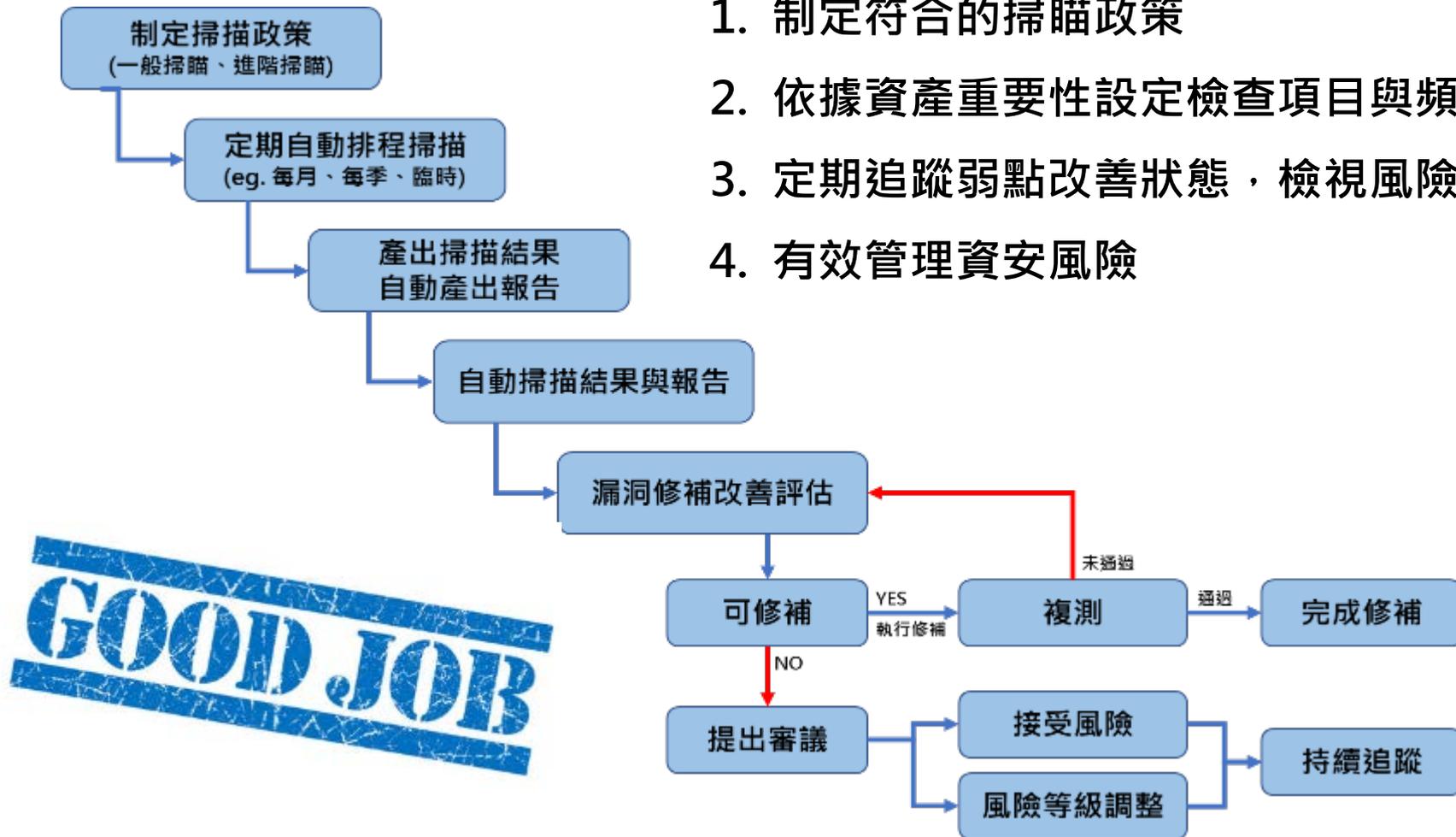
- 系統版本無法更新修補 (如產品生命結束、版本過於老舊、或無保固續約、無服務商) 。
- 系統版本暫時無法更新修補 (如等待正式修補程式釋出、或測試評估中) 。
- 系統為不可取代性之重要或敏感業務應用服務，必須計畫性修補。
- 修補程式對於應用程式或系統有不利的影響。
- 修補方式不符合成本效益。
- 建議修補方式，但應用程式或系統的設定不允許更改。
- 該弱點結果經確認為「誤判」或「特殊情況」。

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。

配合資安治理政策，建立弱點風險管理機制

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



弱點檢視管理

依風險等級統計

依嚴重等級的漏洞列表

依所有IP檢視漏洞列表

依所有漏洞列表

前10大弱點項目 **TopN 排行方式**

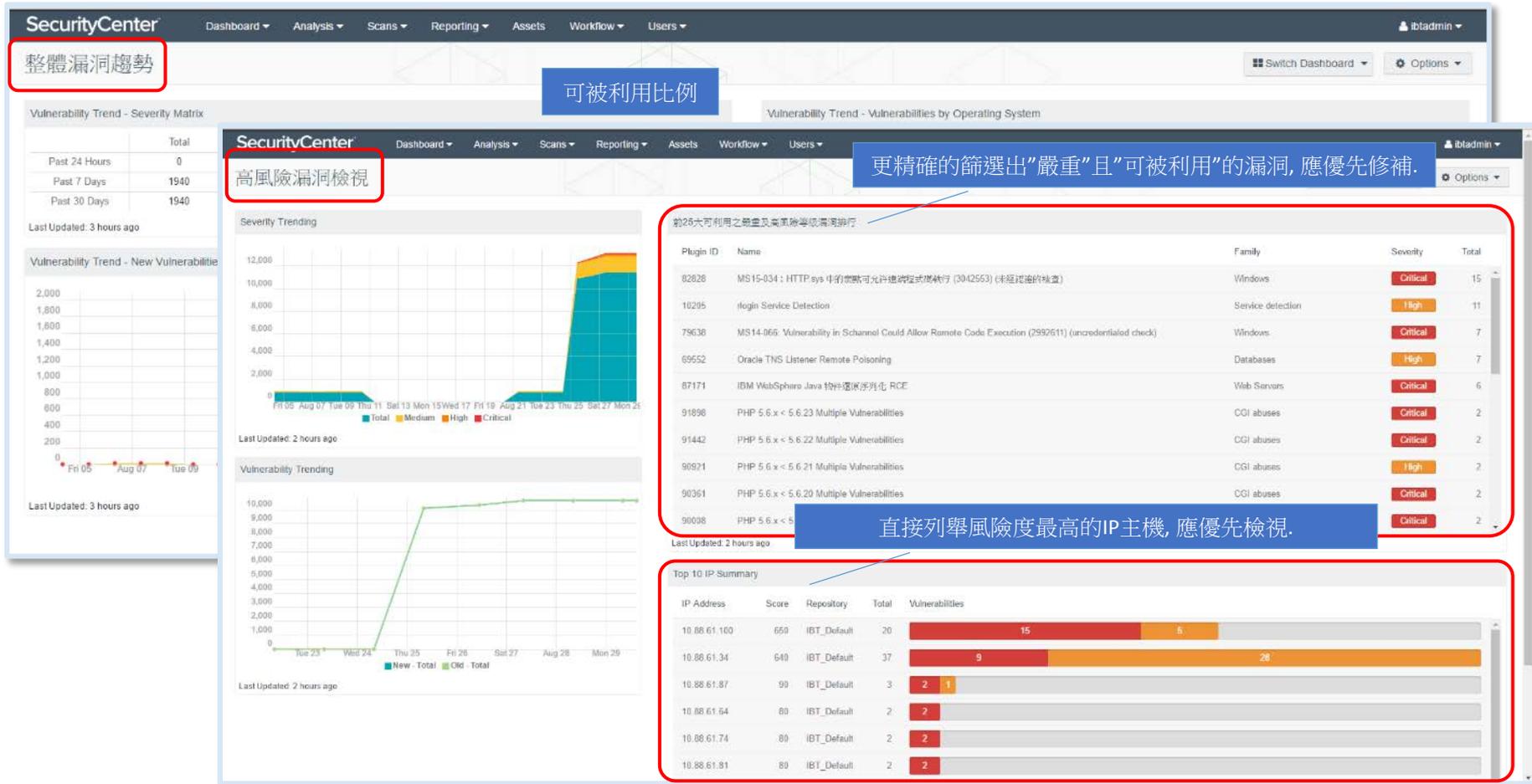
Plugin ID	Name	Family	Severity	Tot:
51192	無法信任 SSL 憑證	General	Medium	8
57582	SSL 自我簽署憑證	General	Medium	4
57608	需要 SMB 簽署	Misc.	Medium	3
85332	MS15-082: Vulnerability in RDP Could Allow Remote	Windows : Mi...	Medium	2

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	

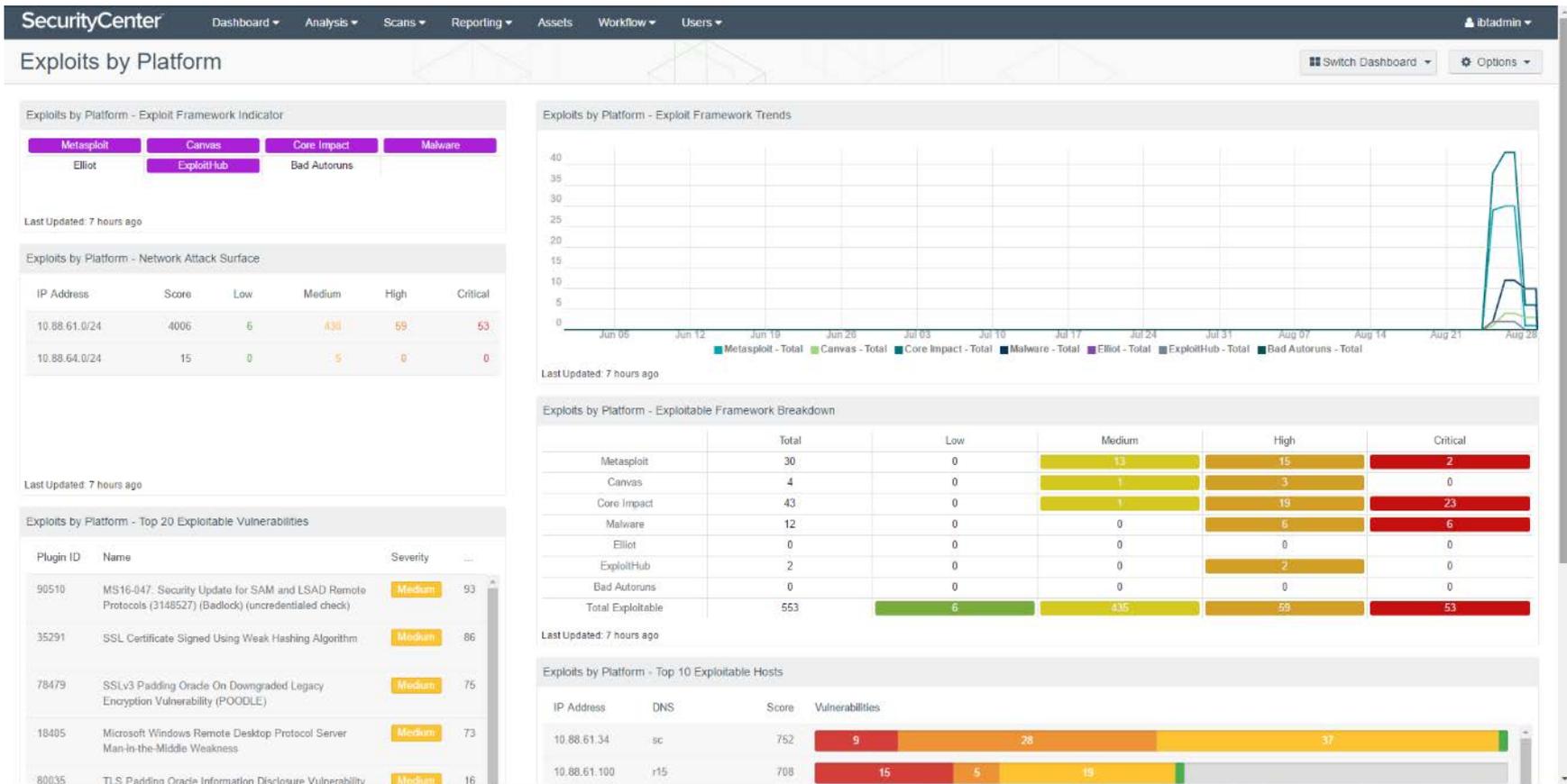
Last Updated: 3 days ago

弱點檢視管理



弱點分析管理

可利用弱點套件(Exploitable)分析



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。

The screenshot displays the SecurityCenter interface for Vulnerability Analysis. The top navigation bar includes Dashboard, Analysis, Scans, Reporting, Assets, Workflow, and Users. The main content area shows a list of vulnerabilities with columns for Plugin ID, Name, Family, Severity, Host Total, and Total. The severity of all listed vulnerabilities is 'Critical'. The interface includes a 'Filters' sidebar on the left with sections for Exploit Available, Repositories, Severity, and Address. The 'Exploit Available' filter is set to 'Yes', and the 'Severity' filter is set to 'Critical, High'. A red box highlights the 'Exploit Available' filter, and a blue callout box points to it with the text '過濾條件為“可被利用”'. Another red box highlights the 'Severity' filter, and a blue callout box points to it with the text '過濾條件為“嚴重及高風險”'. The table lists various vulnerabilities, including MS15-034, MS14-066, IBM WebSphere Java, and several PHP and RHEL vulnerabilities.

Plugin ID	Name	Family	Severity	Host Total	Total
82626	MS15-034 : HTTP.sys 中的弱點可允許遠端程式碼執行 (3042553) (未經認證的檢查)	Windows	Critical	12	15
79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unauthenticated check)	Windows	Critical	7	7
87171	IBM WebSphere Java 物件運算序列化 RCE	Web Servers	Critical	6	6
85887	PHP 5.6.x < 5.6.13 多個弱點	CGI abuses	Critical	1	2
88679	PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities	CGI abuses	Critical	1	2
88694	PHP 5.6.x < 5.6.18 Multiple Vulnerabilities	CGI abuses	Critical	1	2
91442	PHP 5.6.x < 5.6.22 Multiple Vulnerabilities	CGI abuses	Critical	1	2
91898	PHP 5.6.x < 5.6.23 Multiple Vulnerabilities	CGI abuses	Critical	1	2
76698	RHEL 6 : nss and nsspr (RHSA-2014.0917)	Red Hat Local Security Checks	Critical	1	1
81469	RHEL 6 : samba4 (RHSA-2015.0250)	Red Hat Local Security Checks	Critical	1	1
81470	RHEL 6 : samba (RHSA-2015.0251)	Red Hat Local Security Checks	Critical	1	1
81473	RHEL 6 : samba (RHSA-2015.0254)	Red Hat Local Security Checks	Critical	1	1
81474	RHEL 6 : samba4 (RHSA-2015.0255)	Red Hat Local Security Checks	Critical	1	1
84258	RHEL 6 / 7 : cups (RHSA-2015.1123)	Red Hat Local Security Checks	Critical	1	1
84788	RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2015.1229) (Bar Mitzvah) (Logjam)	Red Hat Local Security Checks	Critical	1	1

弱點分析管理

詳細的漏洞資訊、改建建議、及管理。

Critical IBM WebSphere Java 物件還原序列化 RCE (87171)

Synopsis
遠端 WebSphere Application Server 受到一個遠端程式碼執行弱點影響。

Description
遠端 IBM WebSphere Application Server 受到遠端程式碼執行弱點影響，這是因為未驗證的 Java 物件對 Apache Commons Collections (ACC) 程式庫進行不安全的還原序列化呼叫所導致。未經驗證的遠端攻擊者可惡意利用此弱點，傳送特製的 SOAP 要求，從而在目標主機上執行任意程式碼。

Solution
依照供應商公告，套用適當的過渡期修正。或者，確保 WebSphere Application Server 使用的所有暴露連接埠都會受到防火牆保護，免於來自任何公用網路的人侵。

See Also
Links:
[ibm.com](#)
[nessus.org](#)

Plugin Output
Nessus was able to exploit a Java deserialization vulnerability by sending a crafted Java object.

Discovery
First Discovered: 5 days ago
Last Observed: 5 days ago

Host Information
IP Address: 10.88.61.12 (8860 / TCP)
Repository: IBT_Default

Risk Information
Risk Factor: Critical
STIG Severity: I
CVSS Base Score: 10.0
CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:O/RC:N/D
CVSS Temporal Score: 8.3

Exploit Information
Patch Published: Nov 13, 2015
Exploit Available: Yes
Exploitability Ease: Exploits are available

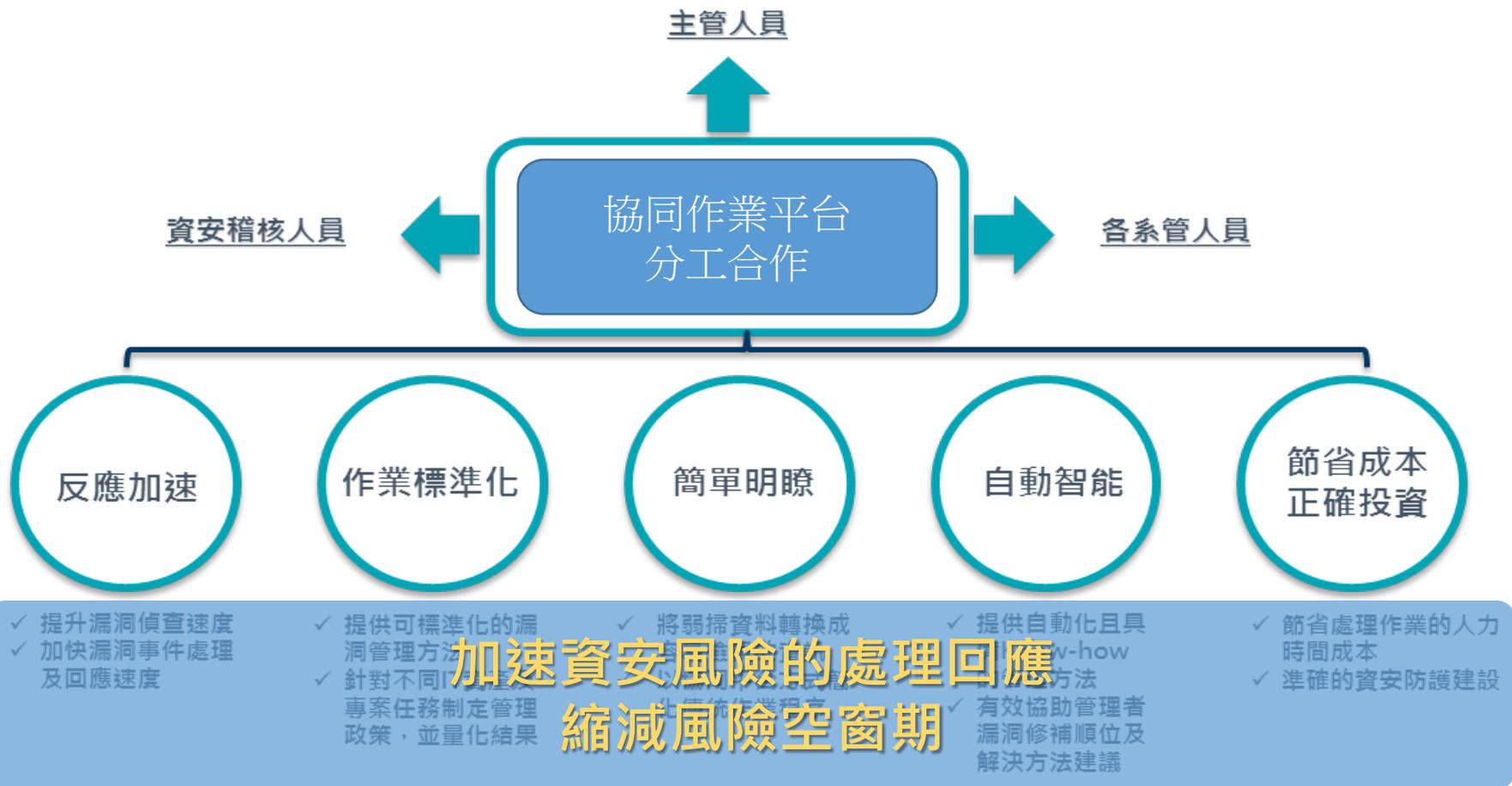
Plugin Details
Plugin ID: 87171
Published: Dec 2, 2015
Last Modified: May 2, 2016
Family: Web Servers
Version: Revision 1.5
Type: remote

Vulnerability Information
Published: Jan 28, 2015

Annotations:

- 針對修補執行複測確認 (Launch Remediation Scan, Recast Risk)
- 達到補強或補償性措施，確保漏洞的威脅可獲得控制，則漏洞風險可被接受(Accept Risk)或調整風險等級(Recast Risk).
- 漏洞問題描述，將完全支援中文。
- 建議解決方案。
建議1. 漏洞修補
建議2. 利用防火牆保護
- Plugin掃描執行結果
有助於發生具爭議或疑似誤判的掃描結果討論。

新型態弱掃管理的效益訴求



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

Case Study

環境規模: 某金融單位國內外共計2000多台Server

傳統弱掃方式

WannaCry
事件通報

確認弱點資訊
(3天)

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

執行弱點掃描作業
(15天)

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

弱掃結果彙整分析
(10天)

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

弱點結果派送
(3天)

將弱點彙整的報告結果派送至各相關人員，並逐一通知及確認修補時程。

系統平台導入後弱掃方式

WannaCry
事件通報

確認弱點資訊
(1天)

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

執行弱點掃描作業
(3-5天)

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

弱掃結果彙整分析
(1天)

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

弱點結果派送
(1天)

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

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



Case Study

提供重大威脅的弱點掃描政策，管理者可直接選用。

SecurityCenter SC Tenable SC PlayRoom Dashboard Analysis Scans Reporting Assets Workflow Users

Add Policy

Template

- Host Discovery
- Basic Network Scan
- Credentialed Patch Audit
- Web Application Tests
- Malware Scan
- Policy Compliance Auditing
- Internal PCI Network Scan
- SCAP and OVAL Auditing
- Dash Shellshock Detection
- GHOST (glibc) Detection
- PCI Quarterly External Scan
- DROWN Detection
- Badlock Detection
- Intel AMT Security Bypass Detection
- Shadow Brokers Scan**
- WannaCry Ransomware Detection**

影子擷客弱點掃描政策

WannaCry勒索掃描政策

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。

SecurityCenter SC Tenable SC PlayRoom Dashboard Analysis Scans Reporting Assets Workflow Users Jim Huang

Add Dashboard Template

影子擷客弱點偵測範本提供。

- Shadow Brokers Vulnerability Detection**
The information published by the Shadow Brokers hacking group identified many major vulnerabilities in common operating systems and services. Failure to remediate impacted systems could leave the network susceptible to intrusion or exploitation. The Shadow Brokers Vulnerability Detection dashboard displays detailed information about the vulnerabilities and exploits discovered by the Shadow Brokers hacking group.
- Detecting WannaCry and EternalRocks**
The new ransomware that is sweeping the planet, called WannaCry and the successor EternalRocks, is causing many organizations much pain as they determine if their network is at risk. Organizations that practice Continuous Vulnerability management can use this data to identify vulnerable systems. This dashboard helps to show how SecurityCenter can identify vulnerabilities using active, passive and event logs to assist customers.

WannaCry及EternalRocks偵測範本提供。

Case Study

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

The screenshot shows the SecurityCenter dashboard with the following sections:

- WannaCry - Suspected and Confirmed Vulnerabilities**

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

Last Updated: Less than a minute ago
- WannaCry - Connection Summary**

Source IP	Destination IP	Count
172.16.132.183	216.215.112.149	336
172.16.132.183	212.44.64.202	336
172.16.133.4	172.16.133.1	180
172.16.132.183	172.16.132.185	28
172.16.133.21	172.16.133.4	7
- Shadow Brokers - Codenamed Vulnerabilities and Exploits**
 - DoublePulsar, EclipsedWing, EducatedScholar, EmeraldThread, EskimoRoll, Elomaf, Metasploit, PoisonIvy
 - Last Updated: Less than a minute ago
- Shadow Brokers - Unsupported and Outdated Products**
 - Windows 2000, Windows XP, Windows Server 20, Windows Vista, Microsoft Exchange, SMBv1, IIS, Lotus Domino
 - Last Updated: Less than a minute ago
- Executive Summary - Outstanding Patches by Operating System**

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

自動套用WannaCry相關
的弱點項目進行過濾。

The screenshot shows the Vulnerability Analysis page with the following details:

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

IP Address	NetBIOS	Score	Total	Vulnerabilities
172.16.132.185	TESTLAB\DEMO2K3	80	2	2
172.16.132.186	WORKGROUP\DAAD-WIN8	80	2	2
- Jump to Vulnerability Detail List**
Total Results: 2

自動比對過濾出存在WannaCry弱點的主機IP。

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。

大綱介紹

Q&A

