掌握資安零信任的關鍵元件應用

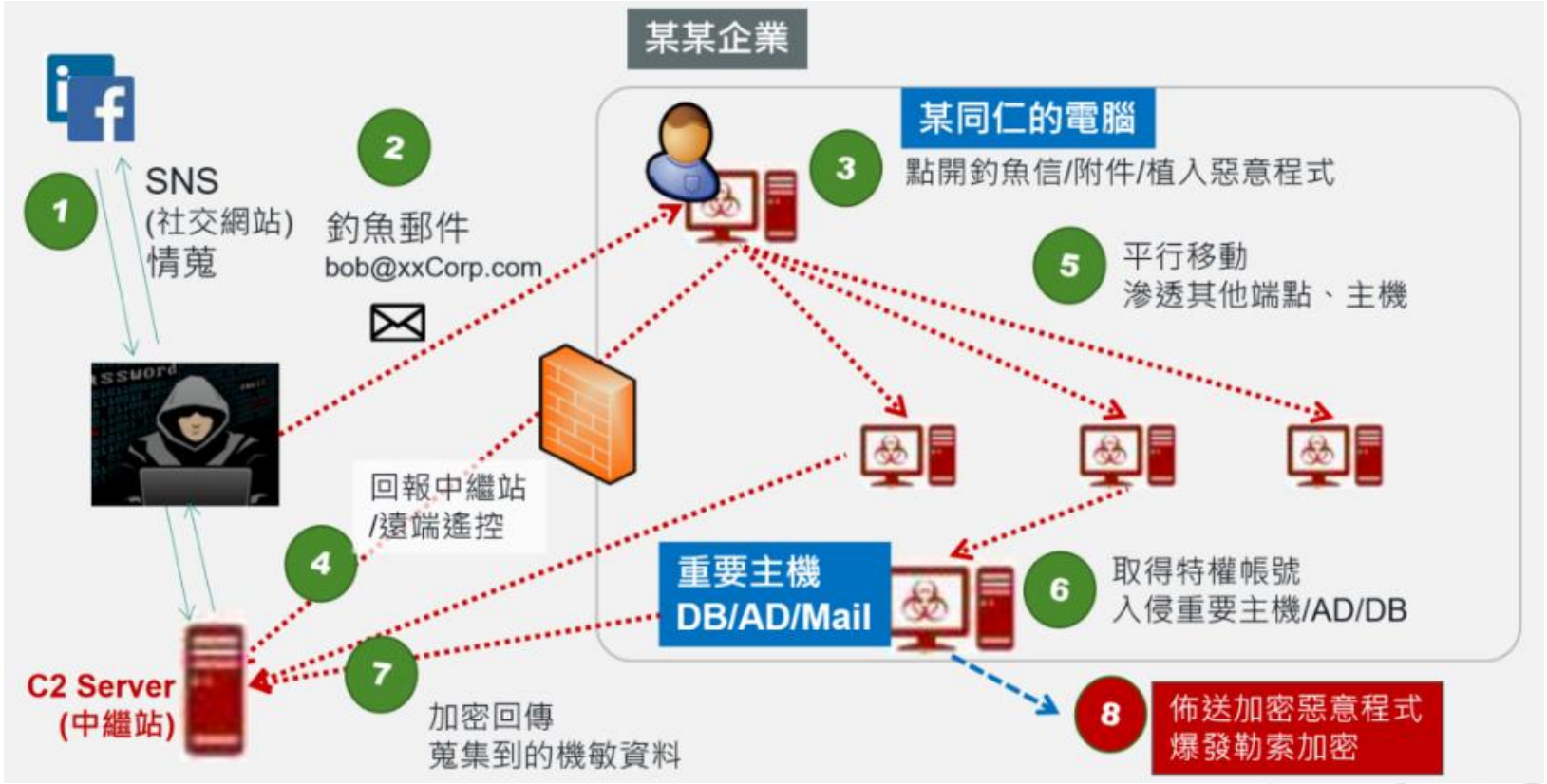
林皇興 **Lambert Lin**

達友科技 **Docutek Solutions, Inc / CISSP**

2022-09-20

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

從 2022 年初的一家電子業 [加密勒索] 攻擊事件談起



Copyright © 2022 Docutek Solutions, inc. All rights reserved.

請問此攻擊案例，企業已有層層防護，為何還會淪陷?

端點、伺服器都有裝**防毒軟體**.....

有安裝**NGFW**...

NGFW有開啟 **IPS**

NGFW 有運行**網址分類庫**，阻擋C&C、**惡意網站**...

Email Gateway 有過濾釣魚、惡意內容郵件...

郵件有經過 **Sandbox** 檢測惡意郵件...

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

Ransomware或 APT攻擊 常見的初始入侵手法/ Initial Access

Social Engineering 與 Weaponized Document 武器化文檔

寄送社交工程釣魚信件，引誘收件者開啟惡意附件、文檔

HTML Smuggling / Watering Hole 水坑式攻擊網站

引誘使用者開啟惡意連結、透過瀏覽 [水坑式惡意網站]，利用瀏覽器漏洞完成惡意程式植入

社交工程釣魚 Credential Phishing/ 帳密竊取

偷竊帳密/撞庫攻擊、暴力破解: 然後使用者身分利用.... (登入M365雲端, 企業 VPN, RDP, 應用系統

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

然而，要如何做到**Prevention（預防）**
讓使用者可以自由瀏覽、交換資料、
收發郵件，但又避免威脅發生?

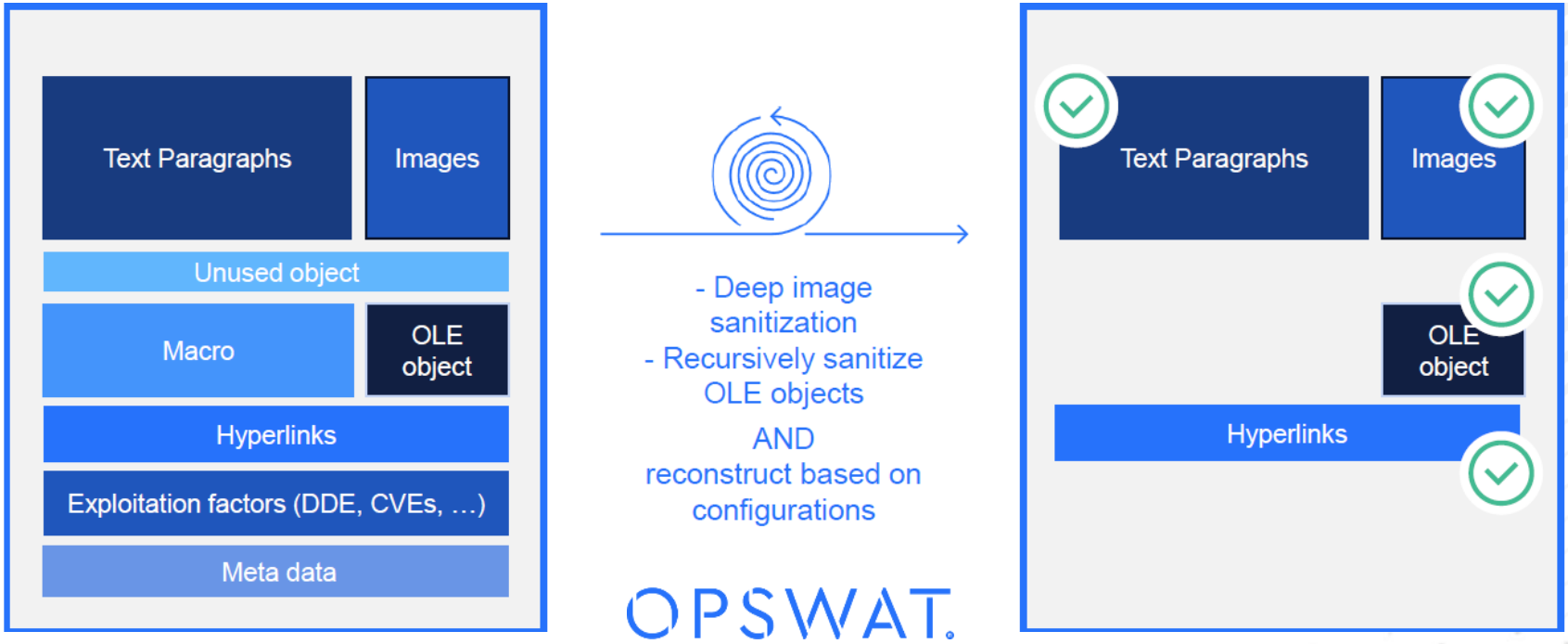
Copyright © 2022 Docutek Solutions, inc. All rights reserved.

第一個要介紹的零信任關鍵元件:
CDR 文件清洗引擎
Content Disarm & Reconstruction

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

關於文件內容清洗CDR，以微軟 Office 文件為例

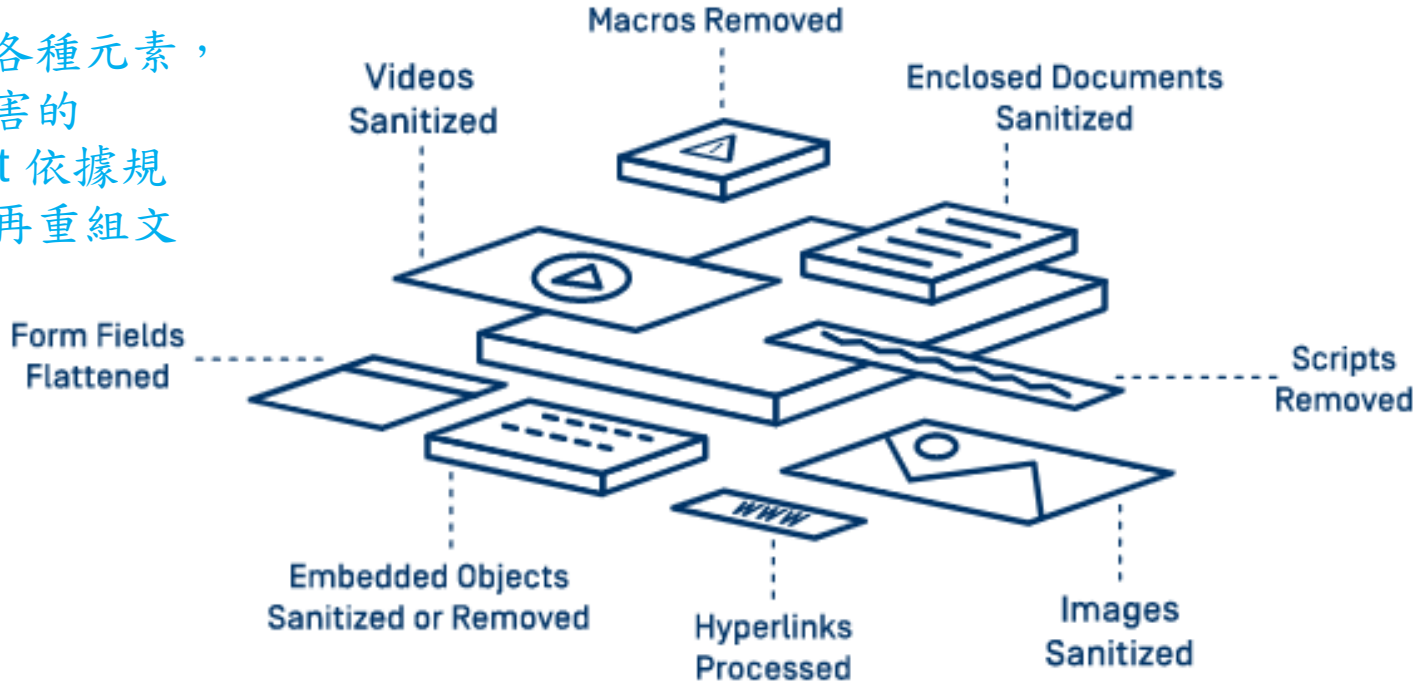
Content Disarm & Reconstruction 內容無害化與重組



Copyright © 2022 Docutek Solutions, inc. All rights reserved.

防範 Zero-Day 以及 Advanced Evasive Malware

拆解文件中的各種元素，將可能造成危害的 Active Content 依據規則進行剝除，再重組文件



零信任

OPSWAT.

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

關於 Deep CDR 文件淨化功能

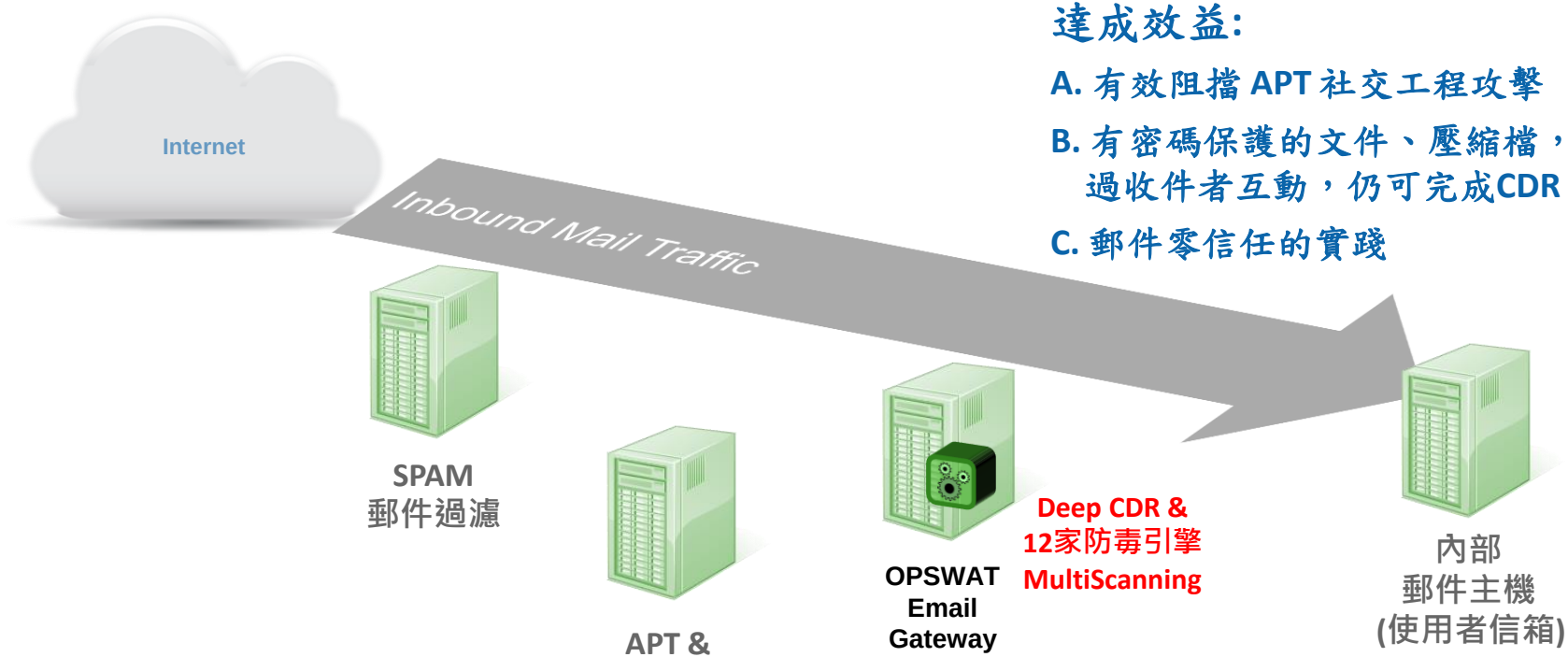
識別檔案格式
(真實格式檢查)
(支援 110+ 檔案格式)

圖片轉換 &依政策
剃除不需要的元素
(例如 script , macro, OLE, DDE 物件, 超連結… 各種元件)

重組並保持
可視內容/格式

OPSWAT.

6000+人的國內某金控, 郵件CDR清洗架構案例



達成效益:

A. 有效阻擋 APT 社交工程攻擊

B. 有密碼保護的文件、壓縮檔，透過收件者互動，仍可完成CDR 清洗

C. 郵件零信任的實踐

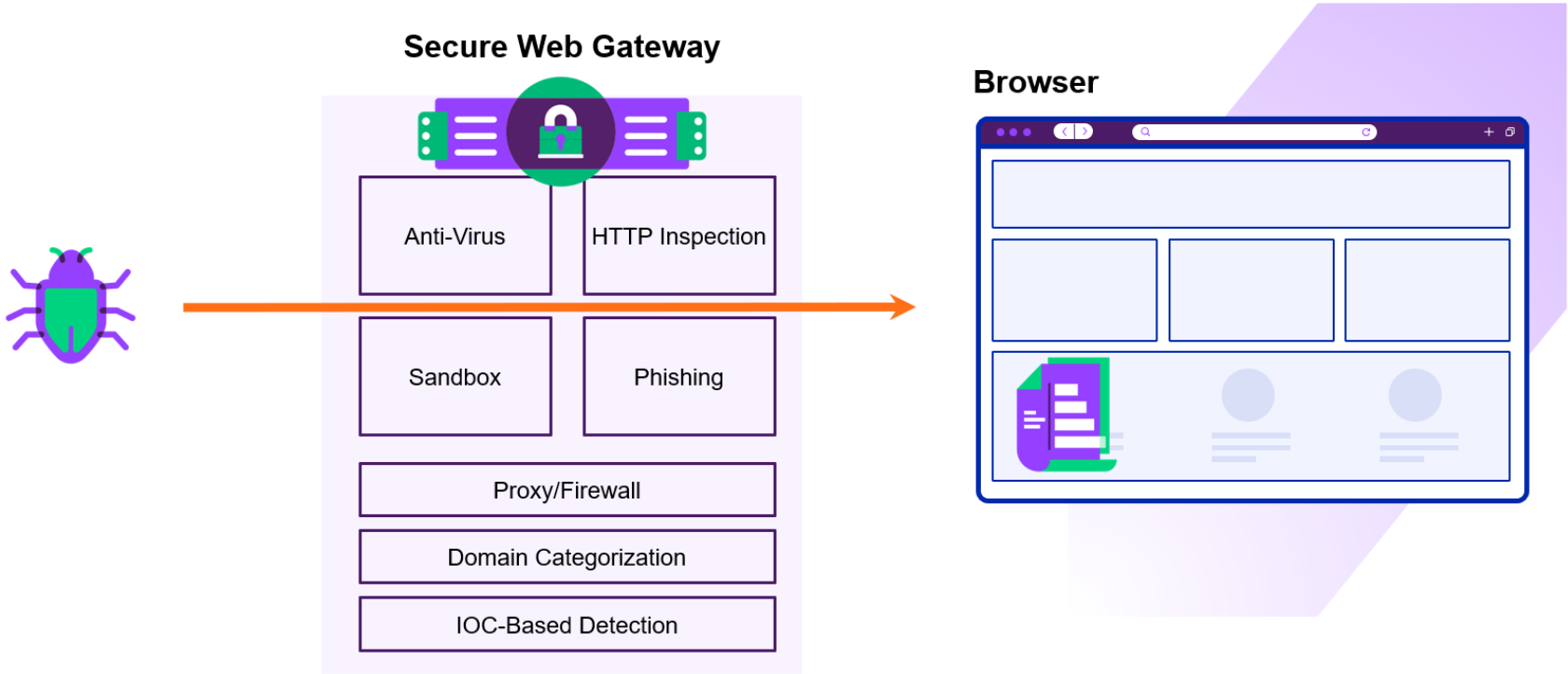
OPSWAT.

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

第二個要介紹的零信任關鍵元件:
RBI /上網隔離
Remote Browsing Isolation

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

網頁瀏覽是新的入侵攻擊管道



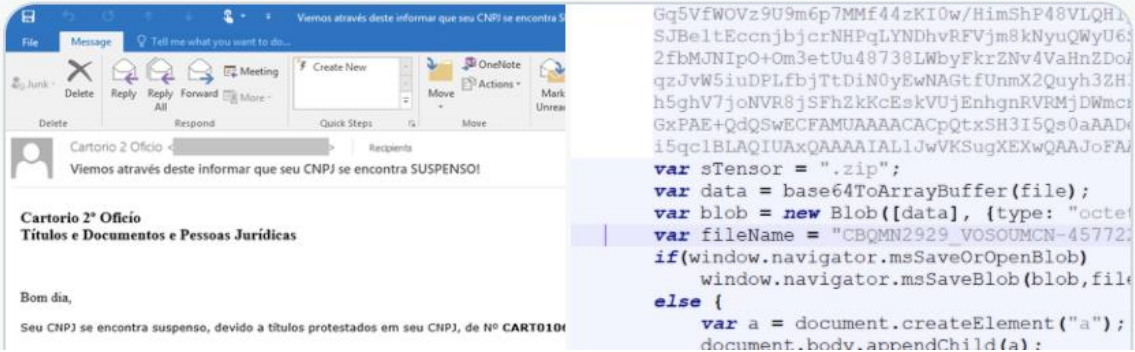
Copyright © 2022 Docutek Solutions, inc. All rights reserved.

HTML Smuggling

Microsoft Security Intelligence @M... · Jul 23, 2021

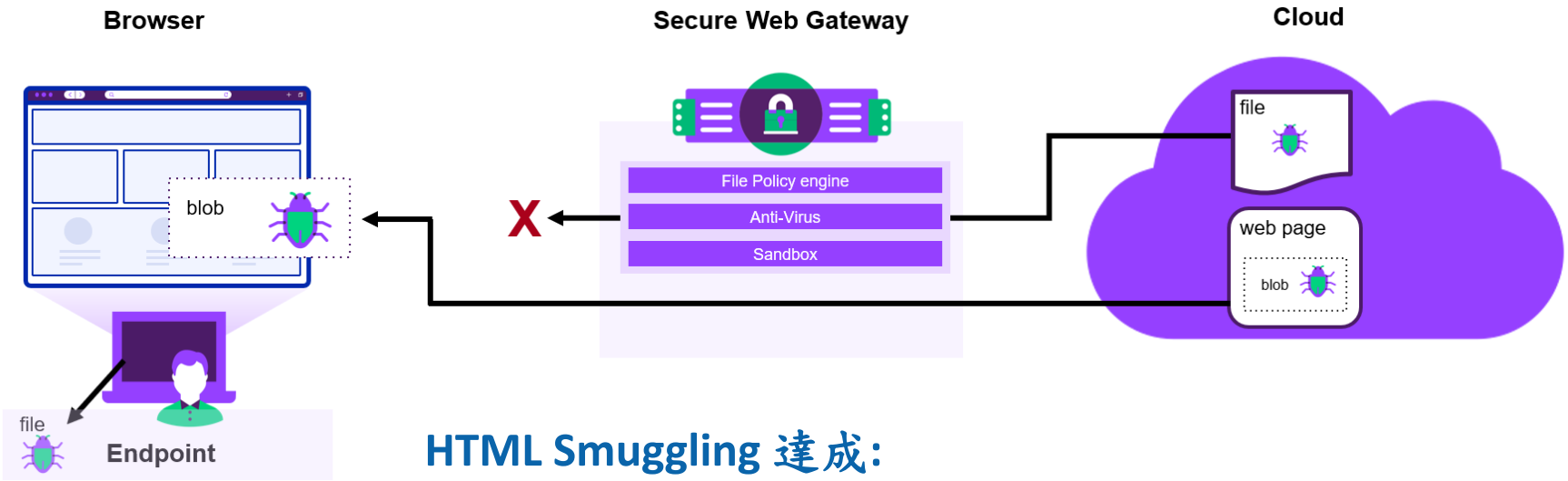
Replying to @MsftSecIntel

In a malware campaign that we have been tracking for weeks, attackers are sending out emails with malicious links that, when clicked, drops components embedded in an HTML page via HTML smuggling. This eventually leads to the dropping of a ZIP archive containing a JavaScript file.



Copyright © 2022 Docutek Solutions, inc. All rights reserved.

HTML Smuggling 攻擊方法



HTML Smuggling 達成:

A. 以 Java Script 動態生成檔案

B. 規避企業技有的各種上網閘道偵測

C. 規避沙箱的分析

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

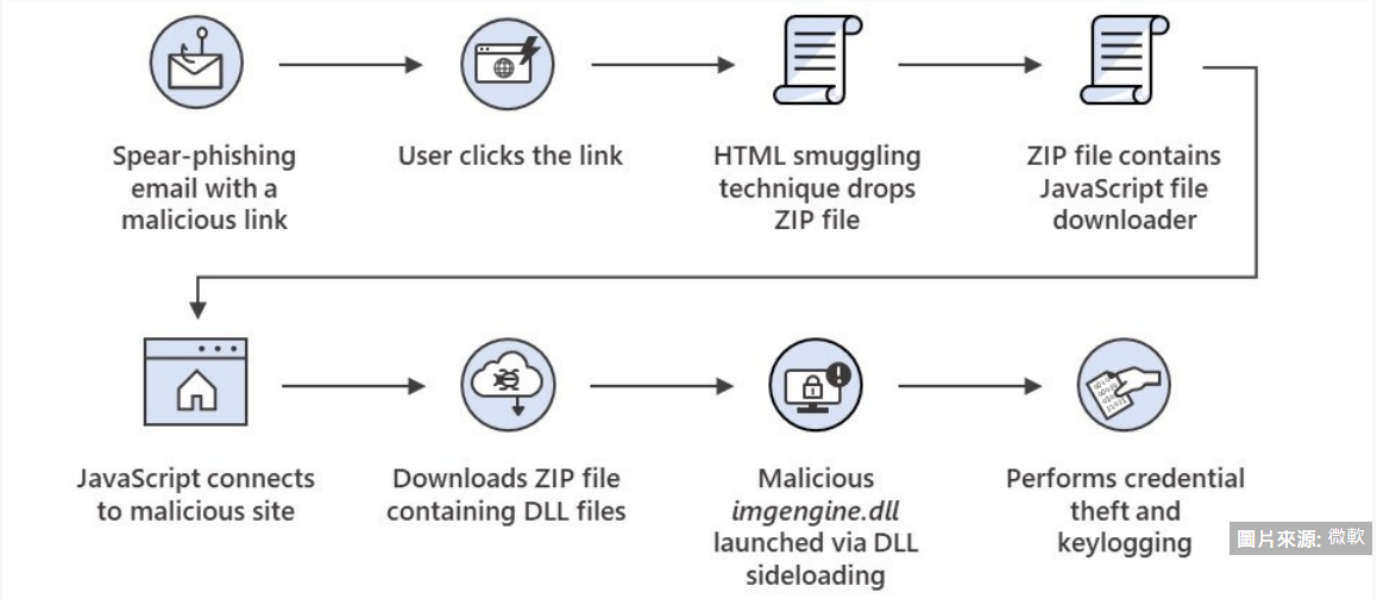
iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 IT EXPI

以HTML挾帶手法躲避偵測的網釣攻擊越來越多了

微軟觀察到今年下半有多起網釣攻擊，都濫用HTML5或JavaScript的合法功能來隱匿行蹤，藉此躲過Web代理程式和電子郵件閘道的檢查

文/ 林妍溱 | 2021-11-15 發表

讚 512 分享

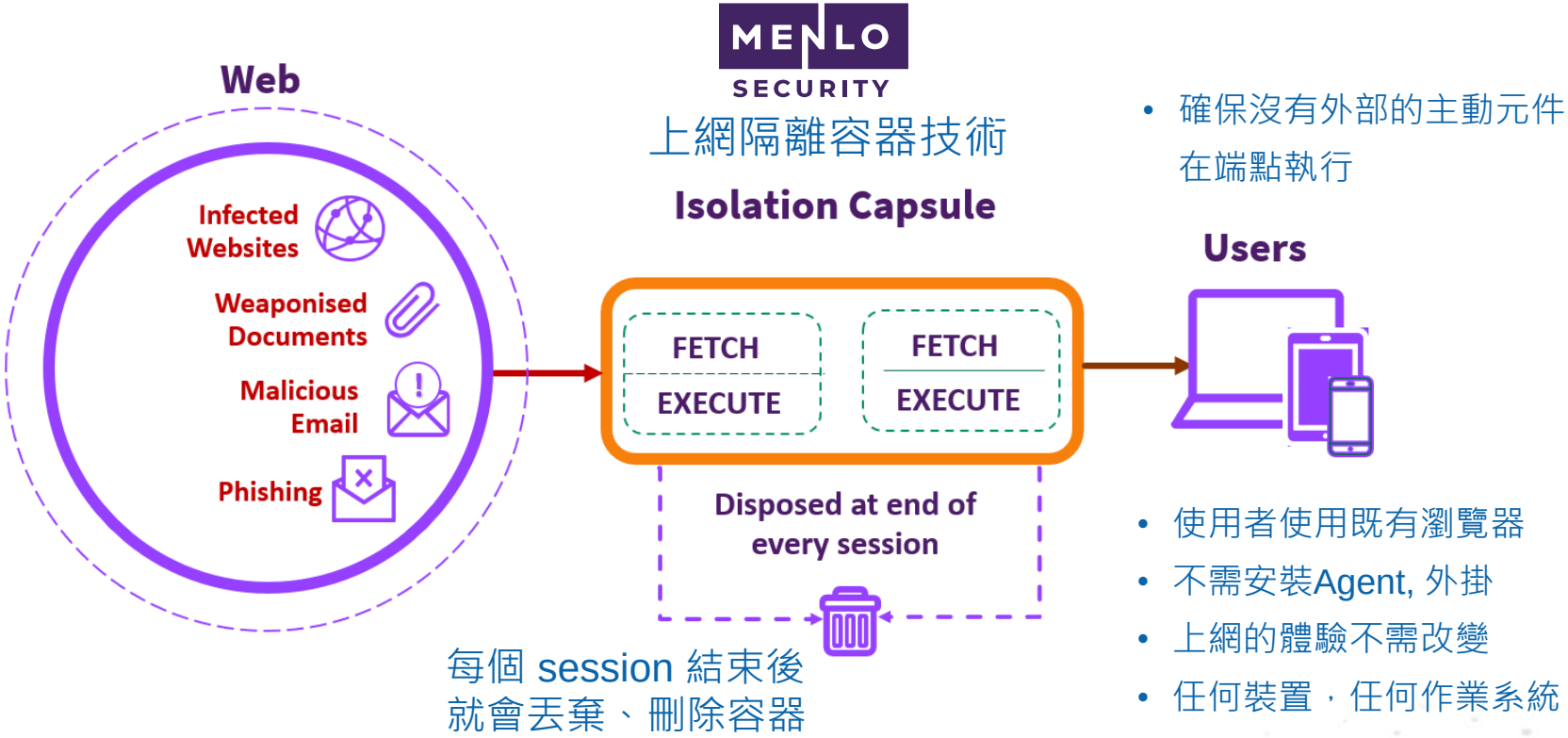


iThome 2021/11/15 有一篇報導在描述該手法

https://www.ithome.com.tw/news/147831

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

上網隔離技術可以防護各種瀏覽網頁造成的攻擊

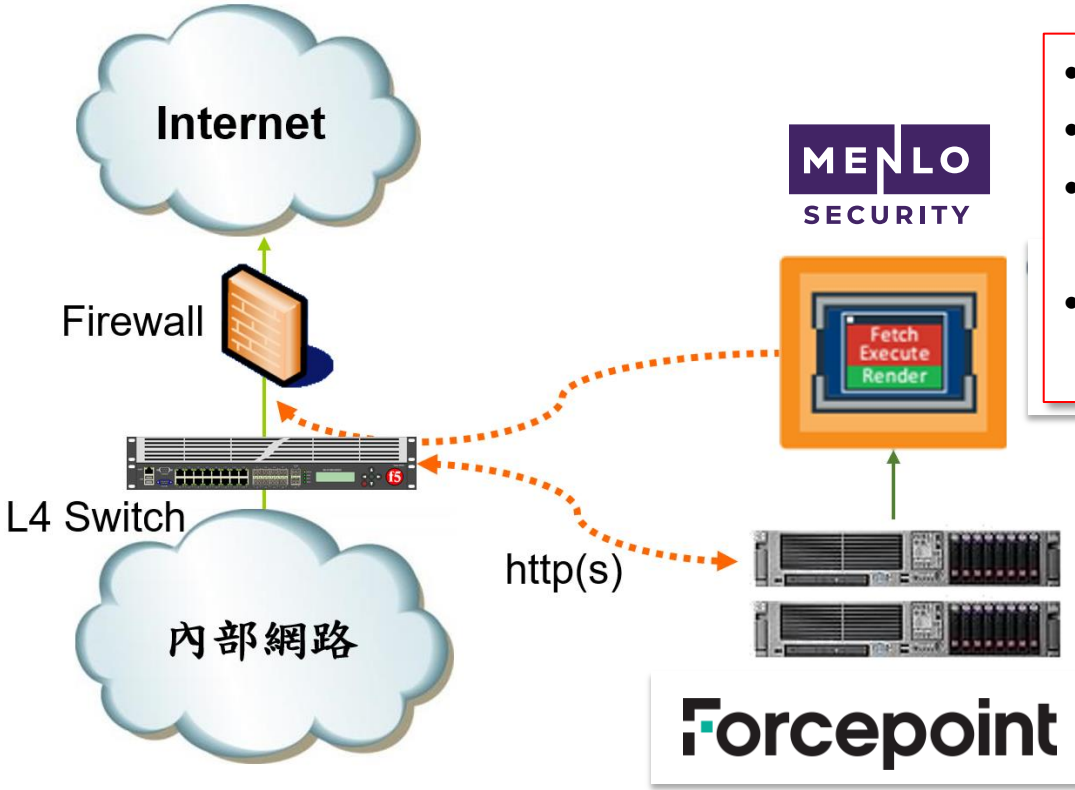


- 確保沒有外部的主動元件在端點執行

- 使用者使用既有瀏覽器
- 不需安裝Agent, 外掛
- 上網的體驗不需改變
- 任何裝置，任何作業系統

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

某國內大型銀行的應用案例



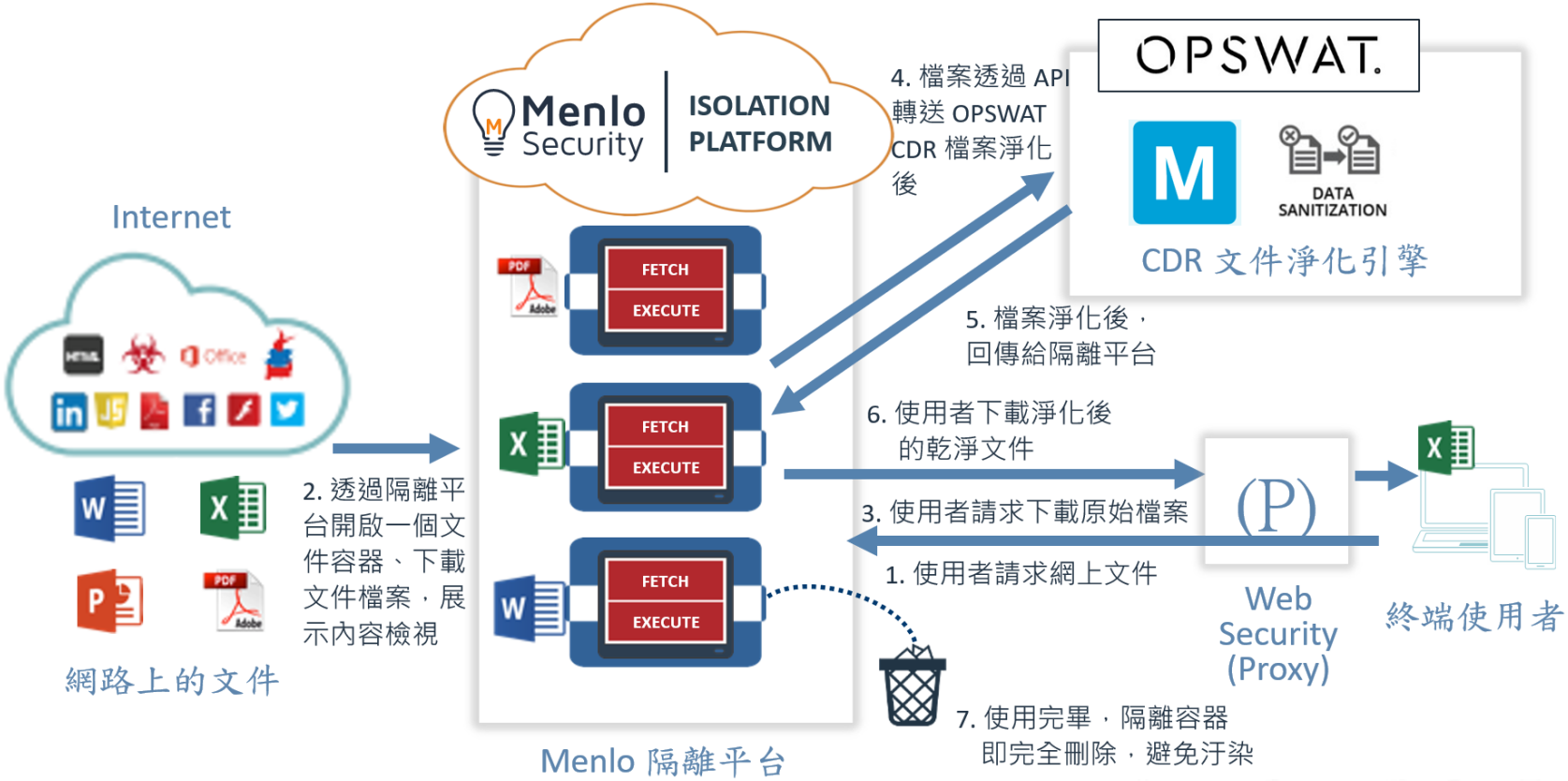
- 採用雲端的隔離平台
- Isolation-All 所有網站隔離
- 於 Forcepoint Proxy 上透過 Upstream Proxy整合設定
- 部份海外據點直接導入雲端隔離平台

Upstream Proxy /Proxy Chaining

Web Security Gateway (Proxy)

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

某晶圓廠的應用案例



Copyright © 2022 Docutek Solutions, inc. All rights reserved.

跨不同安全等級網路之零信任資料交換安全

OPSWAT.

(低安全等級網路)

OA/訪客/VDI 網路

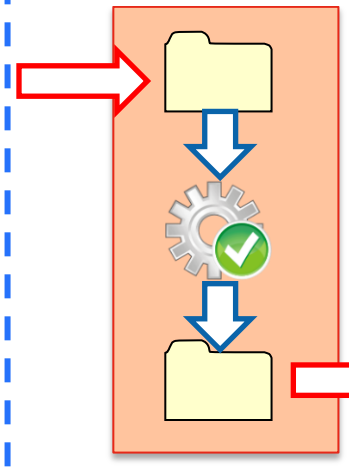
各種
文件

執行檔
補釘程式
安裝程式
Firmware

DLL EXE MSI

各種原始碼

隔離、
檔案清洗
&檢疫機制



OPSWAT
MetaDefender
(CDR, 多防毒8/12/16~
,執行檔漏洞情資引擎)

(更高安全等級要求)

FAB 晶圓廠/管制區

DLL EXE MSI

清洗、檢疫
後的文件 &
檔案

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

實體隔離網路之資料交換需求

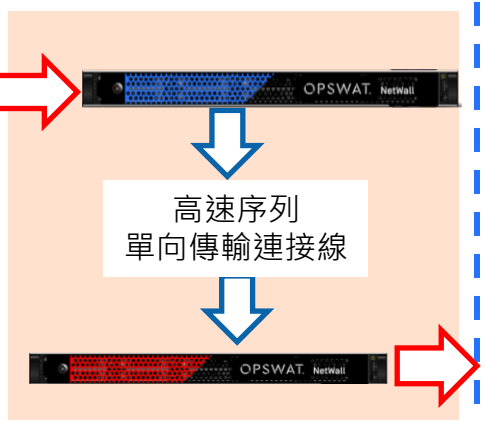
OPSWAT.

工控設備 OT/IoT網路

以工廠自動化為例

- Historian 系統記錄傳輸
- Syslog 紀錄
- 設定檔備份
- 各種檔案…

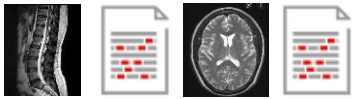
網路隔離
傳輸閘道



OPSWAT
Netwall
單向傳輸閘道器

IT 網路/資料中心

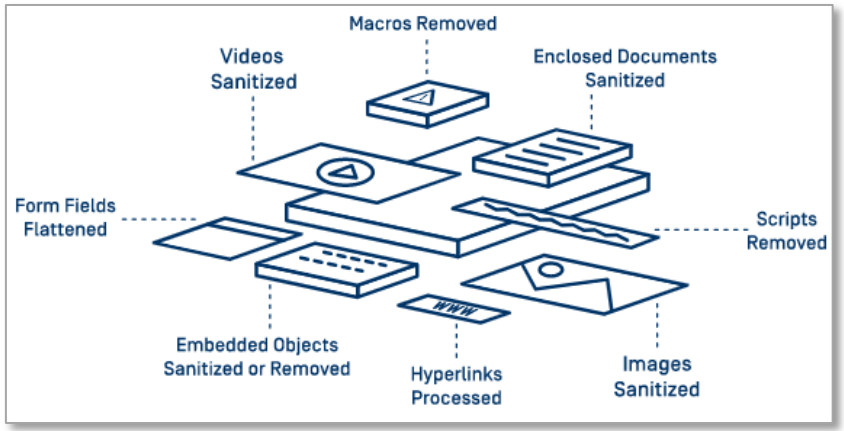
各種
檔案



Copyright © 2022 Docutek Solutions, inc. All rights reserved.

總結 / 掌握資安零信任的關鍵元件應用

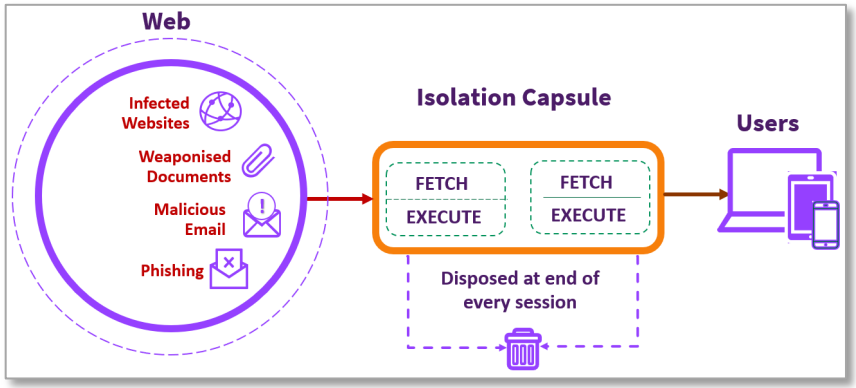
OPSWAT.



CDR 文件清洗 + 多防毒掃描檢疫

確保跨網路的檔案交換之零信任安全

MENLO SECURITY



Web Isolation 上網隔離容器技術

確保網頁瀏覽之零信任安全

Copyright © 2022 Docutek Solutions, inc. All rights reserved.

Thank You

林皇興 **Lambert Lin**

達友科技 **Docutek Solutions, Inc / CISSP**

lambert@docutek.com.tw

Copyright © 2022 Docutek Solutions, inc. All rights reserved.