後疫情時代郵件威脅與雲端資安應用策略

Openfind 網擎資訊
張世鋒 Neil Chang
2020/10/13

Openfind

數位疫情的來臨

台灣 1 年因資安威脅造成的經濟損失約 **8,100 億元**

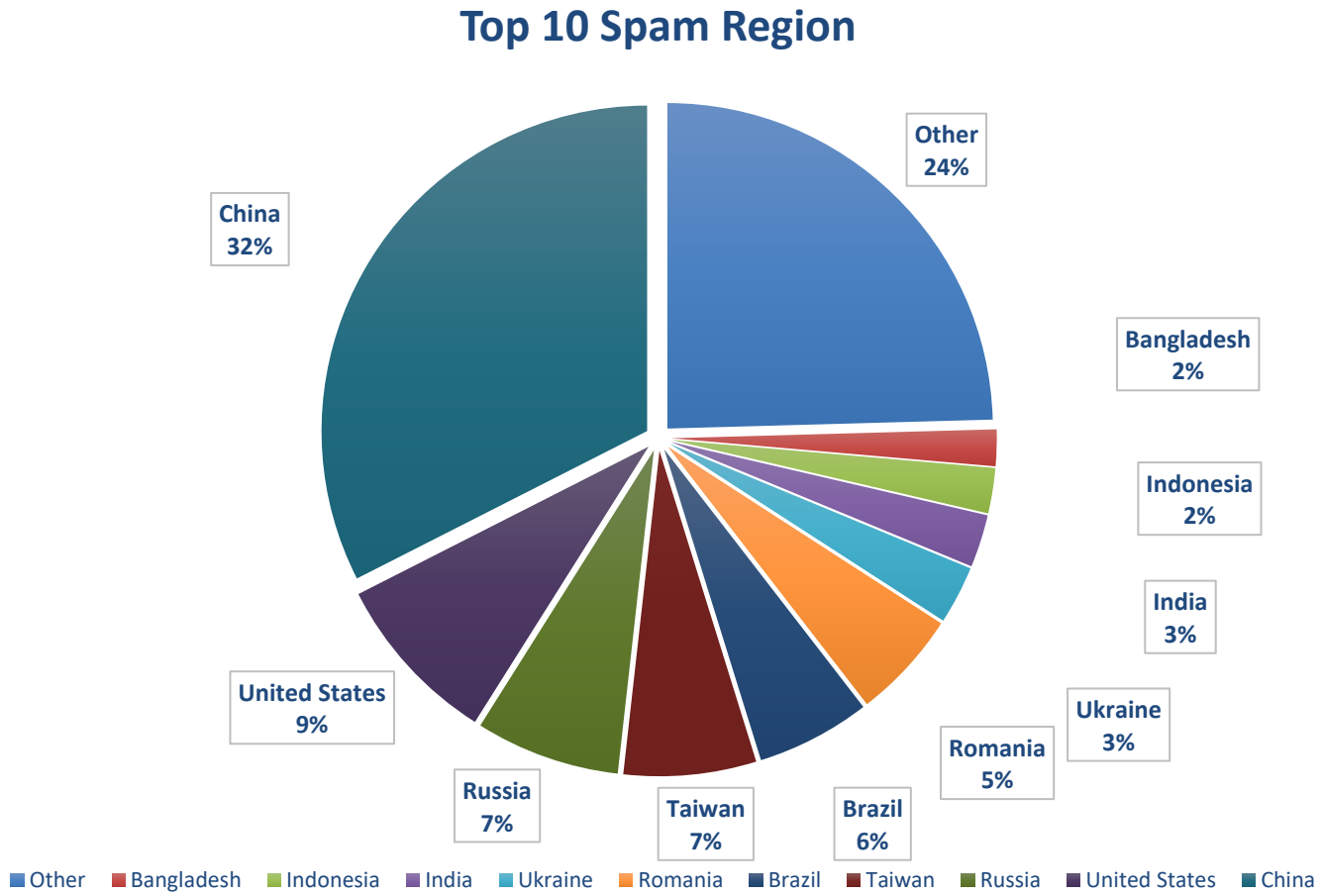
台灣企業每週遭僵屍網路攻擊超過 1,664 次是**全球平均 4 倍**

台灣公部門平均每月面對 **3,000 萬次**駭客攻擊

勒索軟體入侵政府和醫院

2019 年 **113 個地方政府機關**、**764 家醫療院所**受害

2020 年前五名垃圾信來源
中國、美國、俄羅斯、巴西、台灣



進階釣魚詐騙攻擊正持續地增加

使用者更加難以設防的社交工程攻擊

偽冒寄件者身份

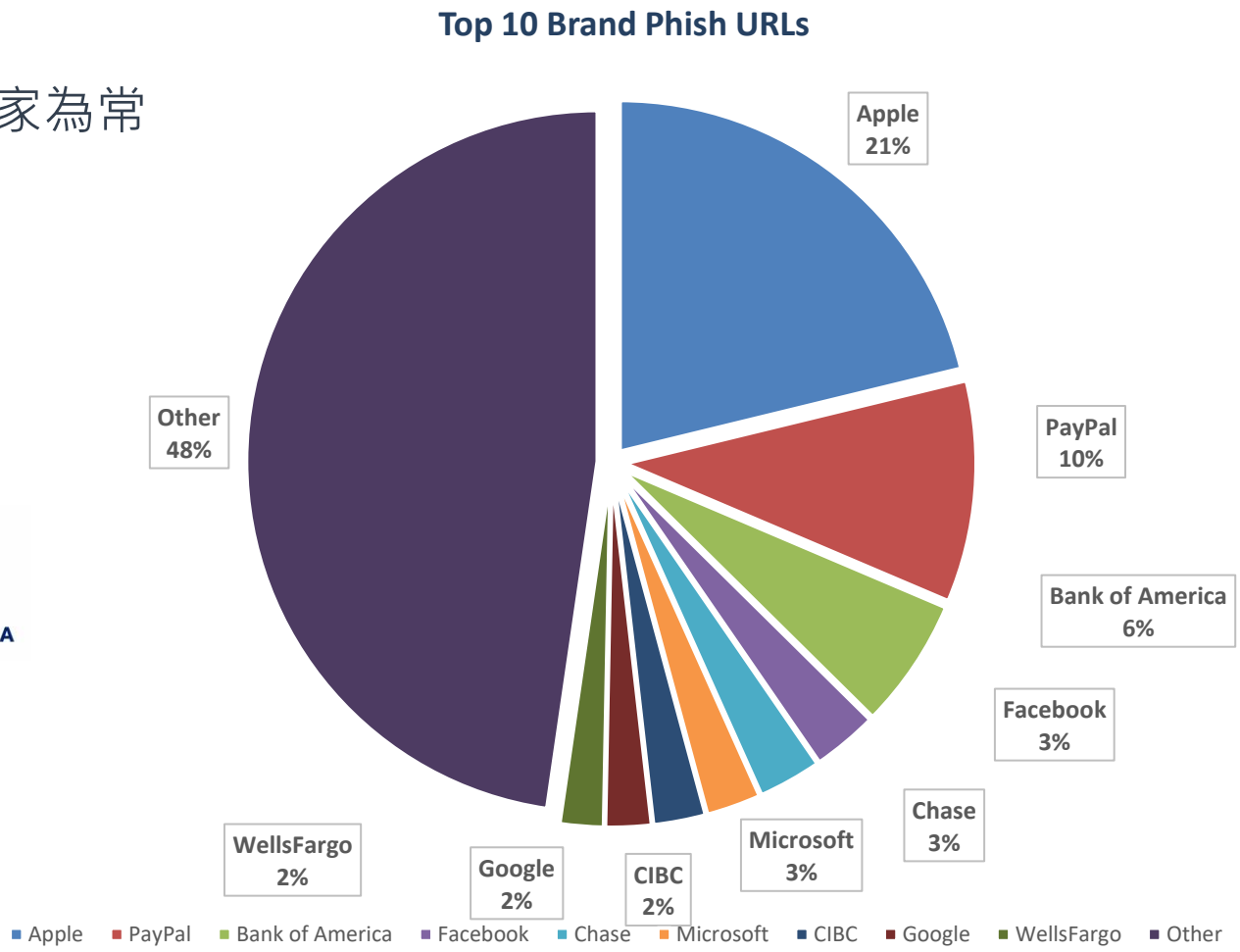
- 熟識資訊或偽冒知名品牌。
- 撰寫切身相關的標題與內文。

假借熱門時事話題

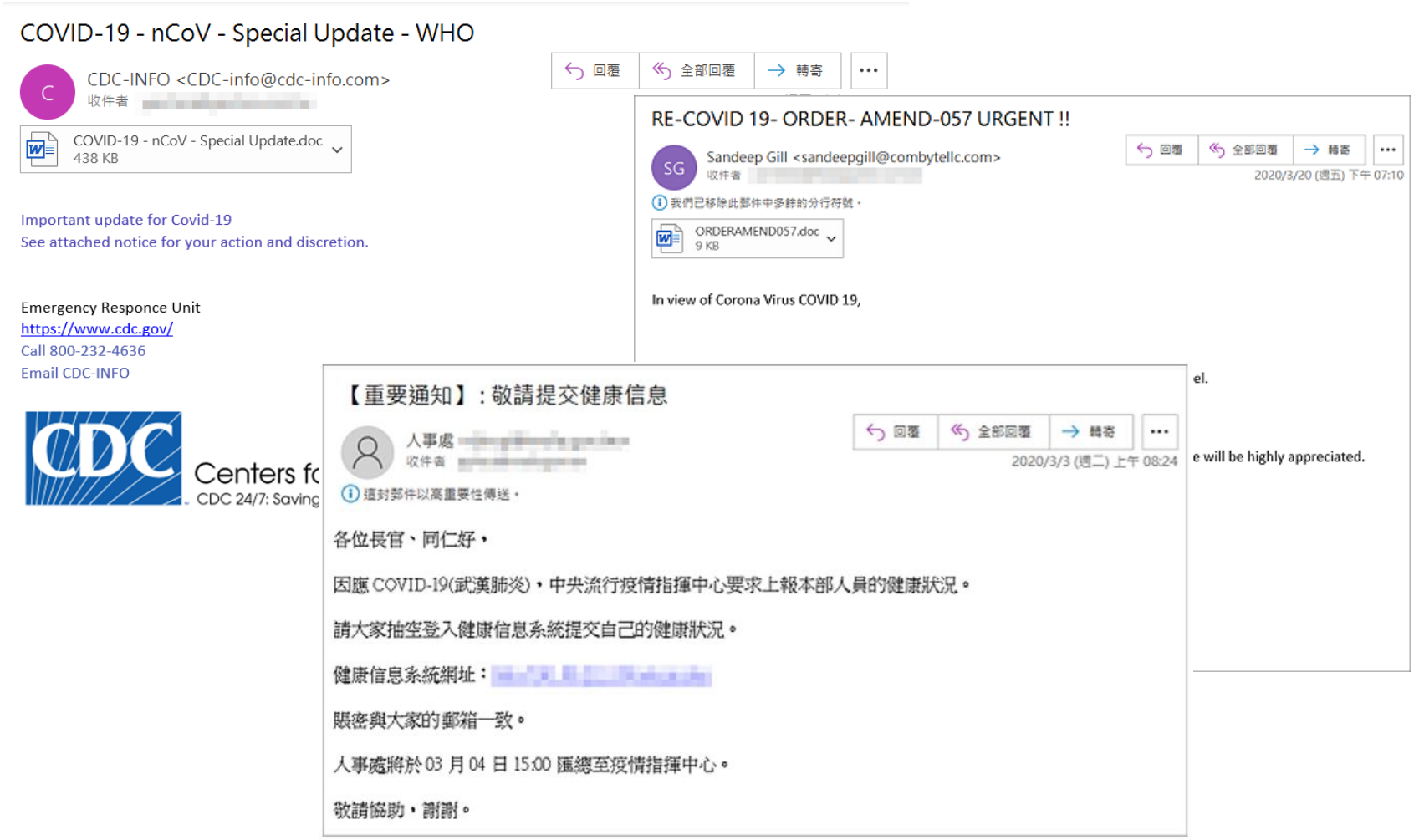
- 國際時事或新聞勾起興趣。
- 誘人前往惡意網頁騙取帳密資訊。

2020 前十大偽冒品牌釣魚網址

- 樣本數100 萬筆。
- 前 10 名中就有 6 家為常見知名品牌。

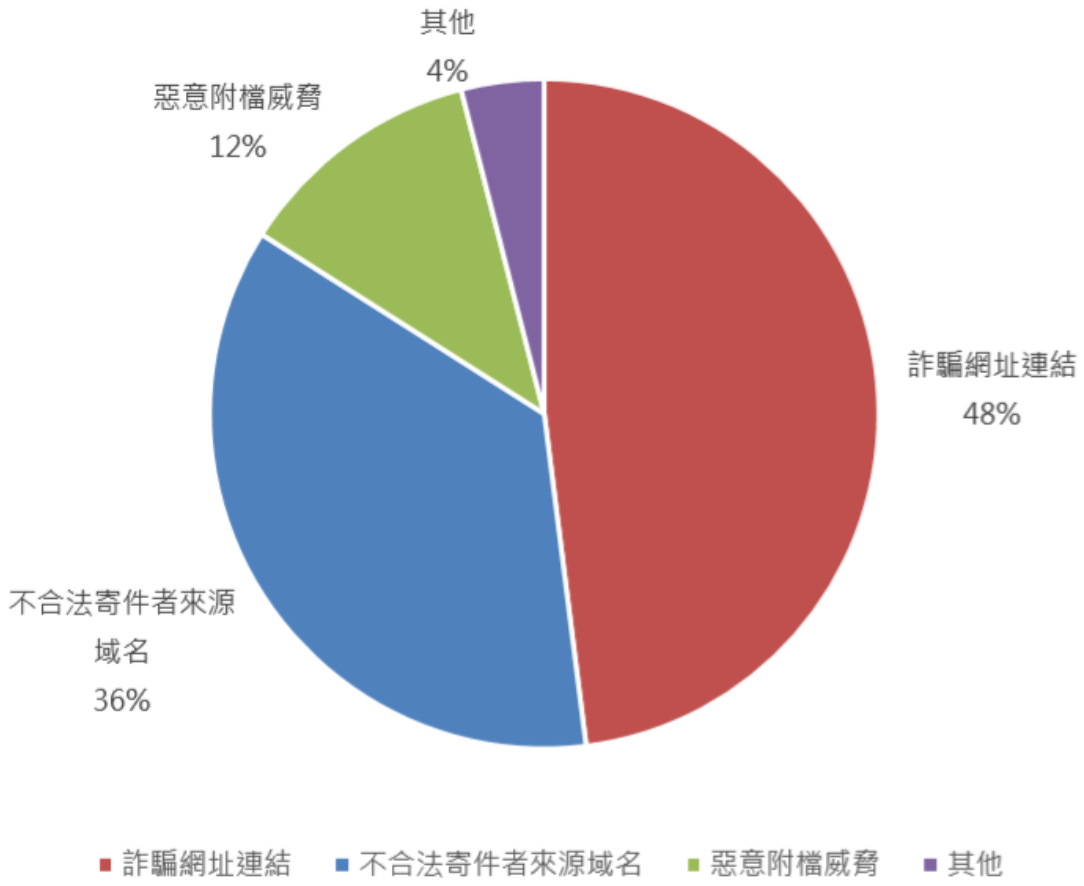


以新冠病毒為主題的進階釣魚詐騙



台灣本地電子郵件詐騙趨勢

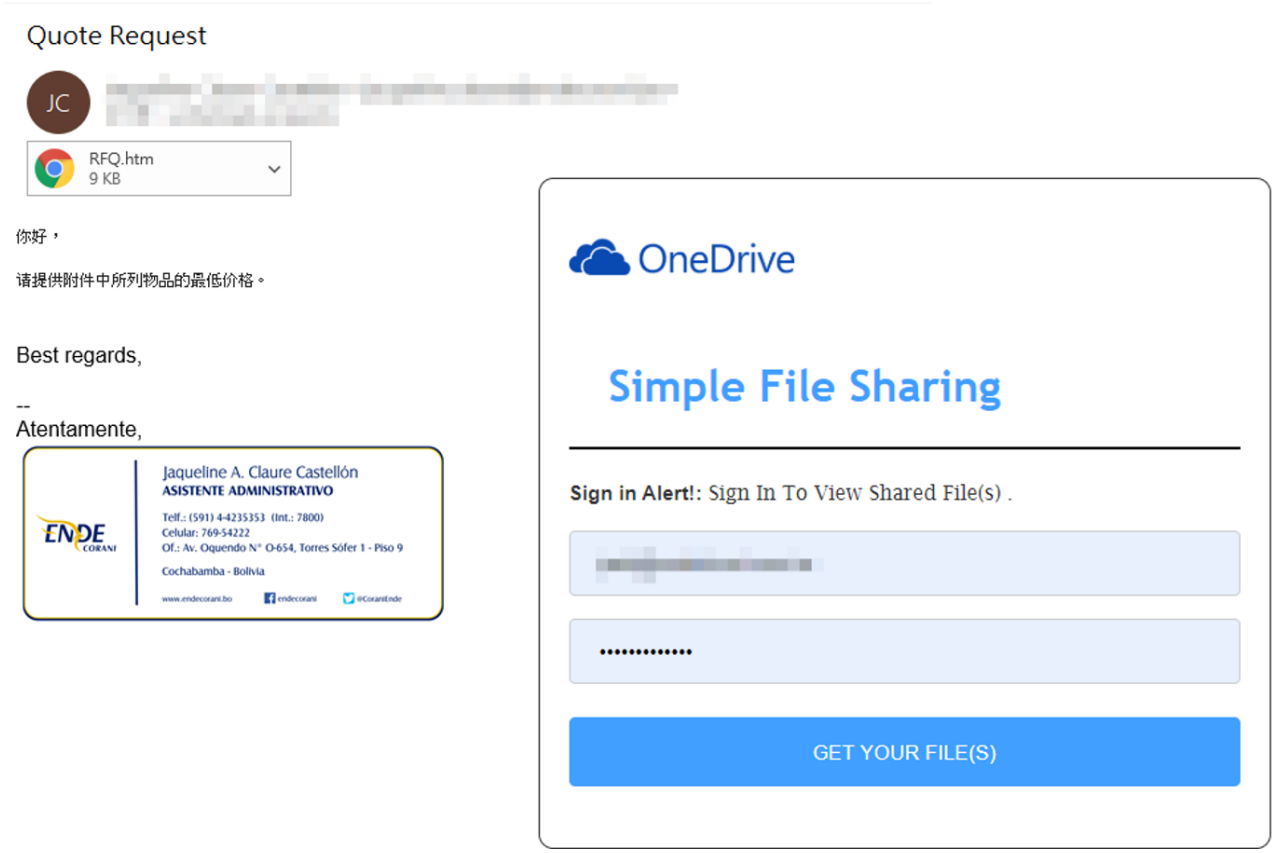
- 超過八成以上來自不可信任的寄件者與網站。
- 利用網址改寫騙取使用者誤觸連結。



偽冒商業訊息的詐騙信

URL 隱藏在郵件附件躲避傳統垃圾信過濾機制

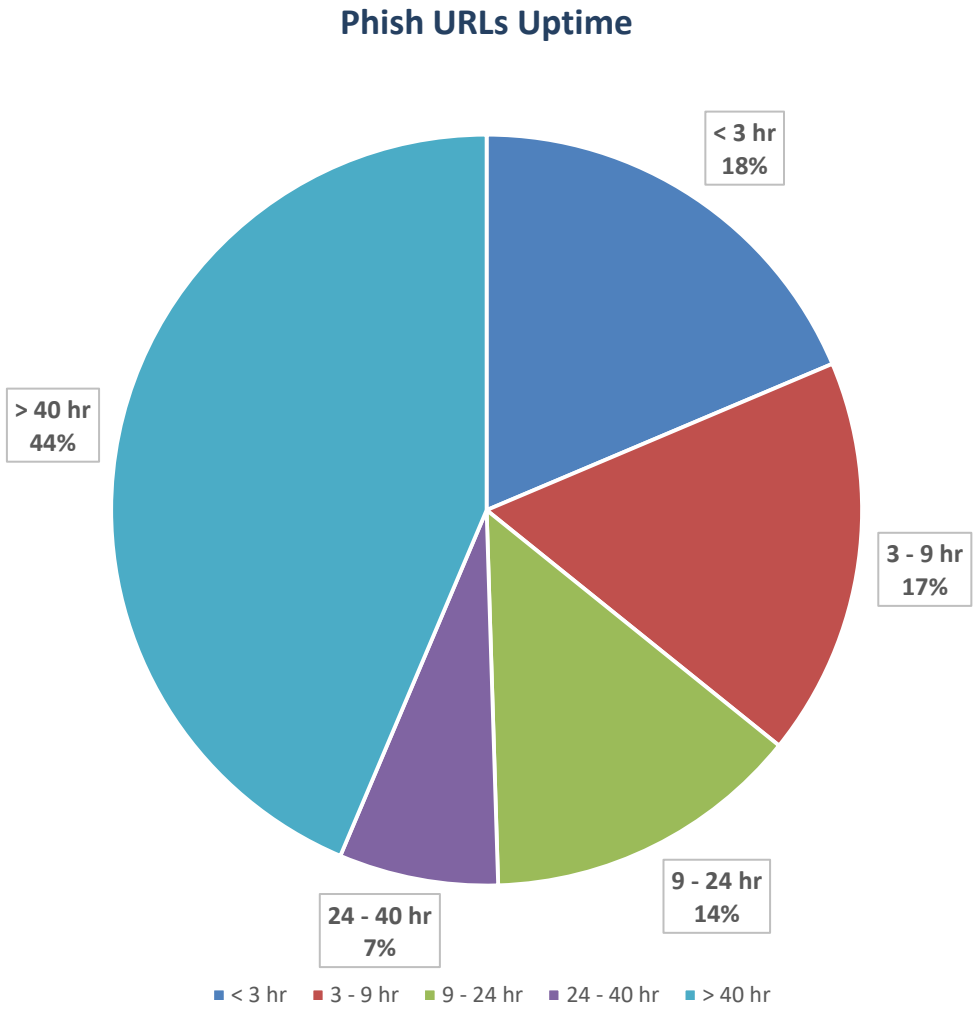
偽冒知名品牌的登入頁面。



超過 50% 釣魚網站持續活躍 24 小時以上

釣魚網站活躍度

- 約 20%（3 小時內消失）
- 約 50%（24 小時內消失）
- 超過 40%（大於 40 小時）



Openfind

資料來源 : Openfind 資安威脅報告

讓你更安心的讀取一封信?

寄件者來源

信件內文安全

信件附檔安全

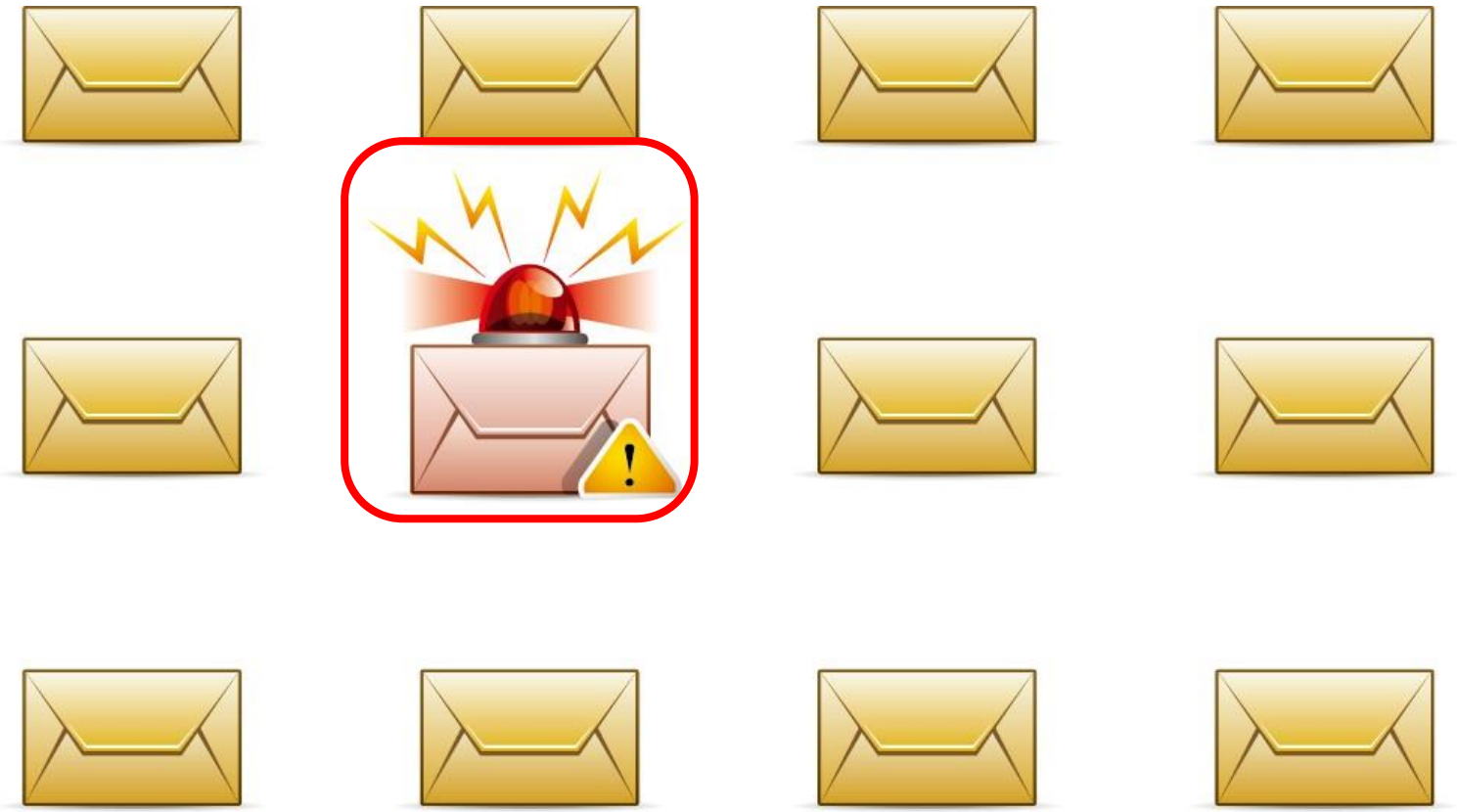
詐騙意圖分析

人臉辨識的新技術應用....

資料來源: https://vmaker.tw/archives/27264

敏捷回應郵件威脅

Optimization, Big-Data, Machine-learning, Prediction



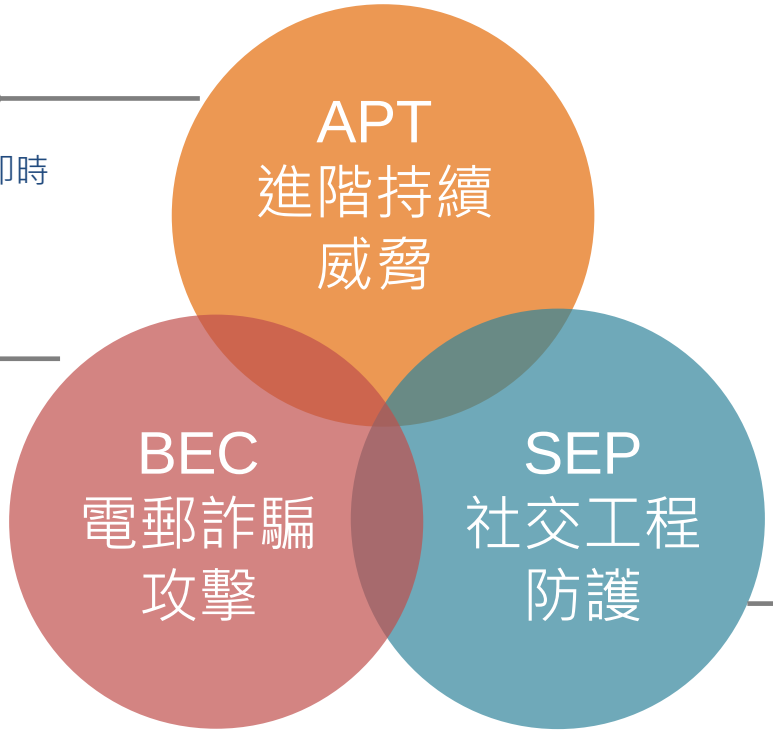
資安警覺 x 敏捷回應

沙箱防護阻擋威脅

國際合作的防護技術，Sandbox 即時
智慧運算，偵測進階魚叉式攻擊

智慧 AI 判斷詐騙信

偵測詐騙意圖，配合全球國際
與本地樣本分析，主動警示

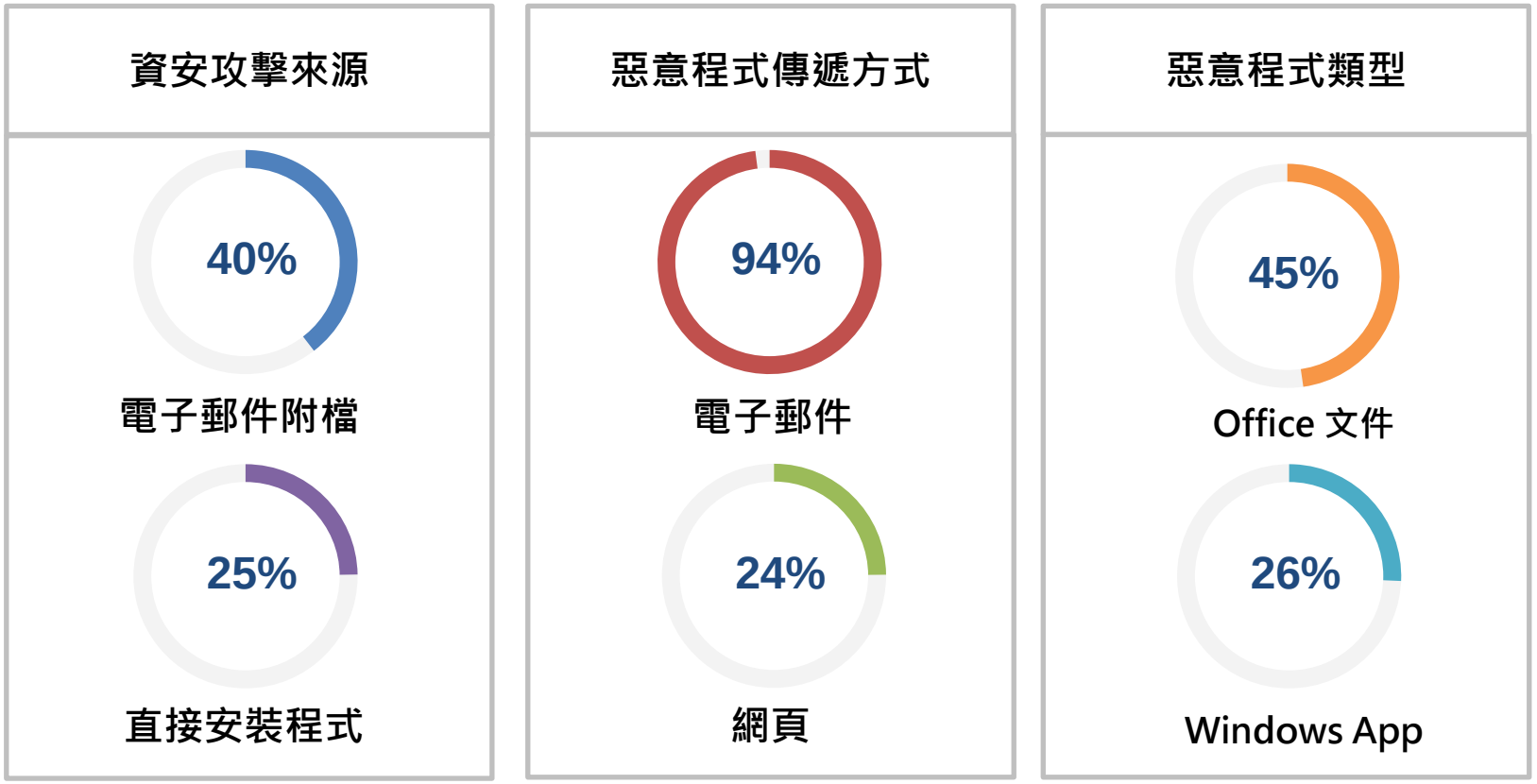


監控釣魚網址行為

攔阻社交工程網址之點擊，
以完整記錄協助追查及內部管理

APT 進階持續威脅統計

主要來源：電子郵件附檔與隱含連結



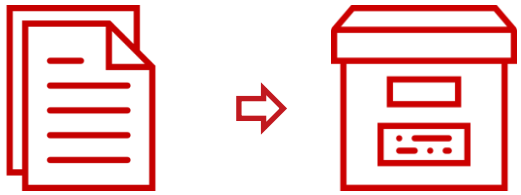
Reference: 2019 Data Breach Investigations Report

APT 進階持續威脅防護

提供檔案執行的環境，確認**檔案/連結**的實際行為

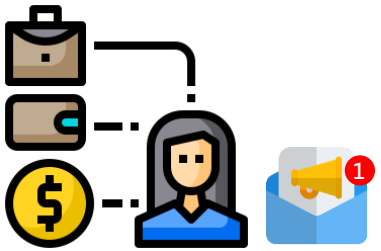
附件含惡意執行檔

帶有後門程式的 URL　　**沙箱分析**



- 自動化執行
- 模擬真實環境
- 檢測威脅行為
- 追蹤潛在威脅
- 事件分析報告

用 AI 協助電郵詐騙防護



信件內文語意分析

- 交易意圖
- 轉帳意圖
- 特殊字典擋
- 寫信風格分析

使用者行為分析

- 往來對象
- 收發信行為、內容
- 資料外洩風險預測
- 異常行為分析

BEC 電郵詐騙防護

可疑的相似網域

範例：相似網域的樣式

mailcloud.com.tw -> mailc1oud.com.tw
l ➔ 1 (數字)
openfind.com.tw -> openfind.corn.tw
m ➔ rn
mail2000.com.tw -> mail2000.c0m.tw
o ➔ 0 (數字)

陌生網域寄件者

範例：以 14 天為閥值

10 天前曾寄給 vendor.com (舊網域)

30 天前曾寄給 partner.com (新發現)

未曾寄給 spoofing.com (新發現)

偽冒內部使用者(員工)

peter@internal.com

local-part domain-part

範例：
From：peter <peter@internal.com>
內部使用者 peter
From：peter <peter@external.com>
外部網域意圖假冒 peter

來信與回覆地址不一致

範例：

From: sales <sales@mypartner.com>
Reply-to: sales <sales@spoofing.com>
回覆位址不一致

註：Gmail, Hotmail 等免費信箱
沒有 Reply-to 標頭則不檢查

BEC 電郵詐騙預警

回信 全回 轉寄 | 標籤 移至 | 廣告信 | 檢視 更多

標題

[疑似詐騙信]Payment urgent !!

歡迎使用Mail2000電子郵件系統

來源: sales <sales@vendor.corn> 外部相似網域
標題: [疑似詐騙信]Payment urgent !!
日期: Tue, 30 Apr 2019 18:23:41
附檔(1): payment.docx (13KB)

請勿依他人指示操作提款機!

ATM沒有解除或設定分期付款的功能!

ATM沒有身分辨識功能!

ATM只能把錢轉出，不能轉入!

查詢更多防詐訊息

此郵件包含可疑特徵，且來自於公司外部，請再三確認。 內文警告標語

Dear Sir

Payment have been made and attached is the wire transfer receipt.

Please confirm receipt of payment. 語意分析，匯款請求

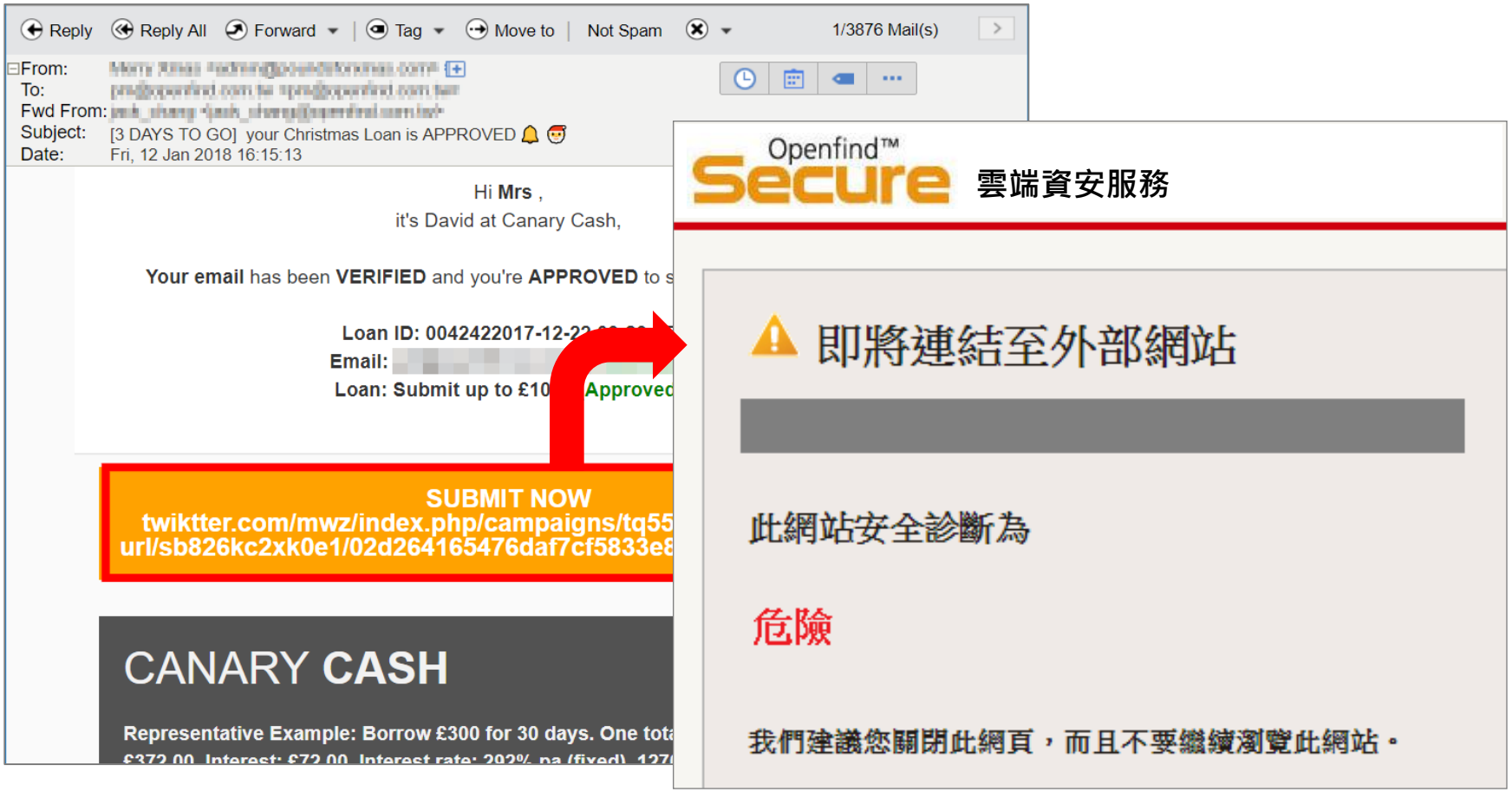
Kind Regards

Johnathon Howson

社交工程攻擊的種類

社交工程的網址防護預警

第一時間過濾 URL，第二時間網址防護分析



Gartner：2020 年全球雲端安全市場規模將達 90 億美元

防火牆 (Firewall)、網站安全 (Web)、郵件傳送 (SMTP)
都將以雲端服務的方式提供即時的資安防護

TechNews 科技新報

https://technews.tw/2019/03/06/cloud-security-market-2020/

SOPHOS

Symantec. Endpoint Protection Cloud

McAfee MVISION Cloud

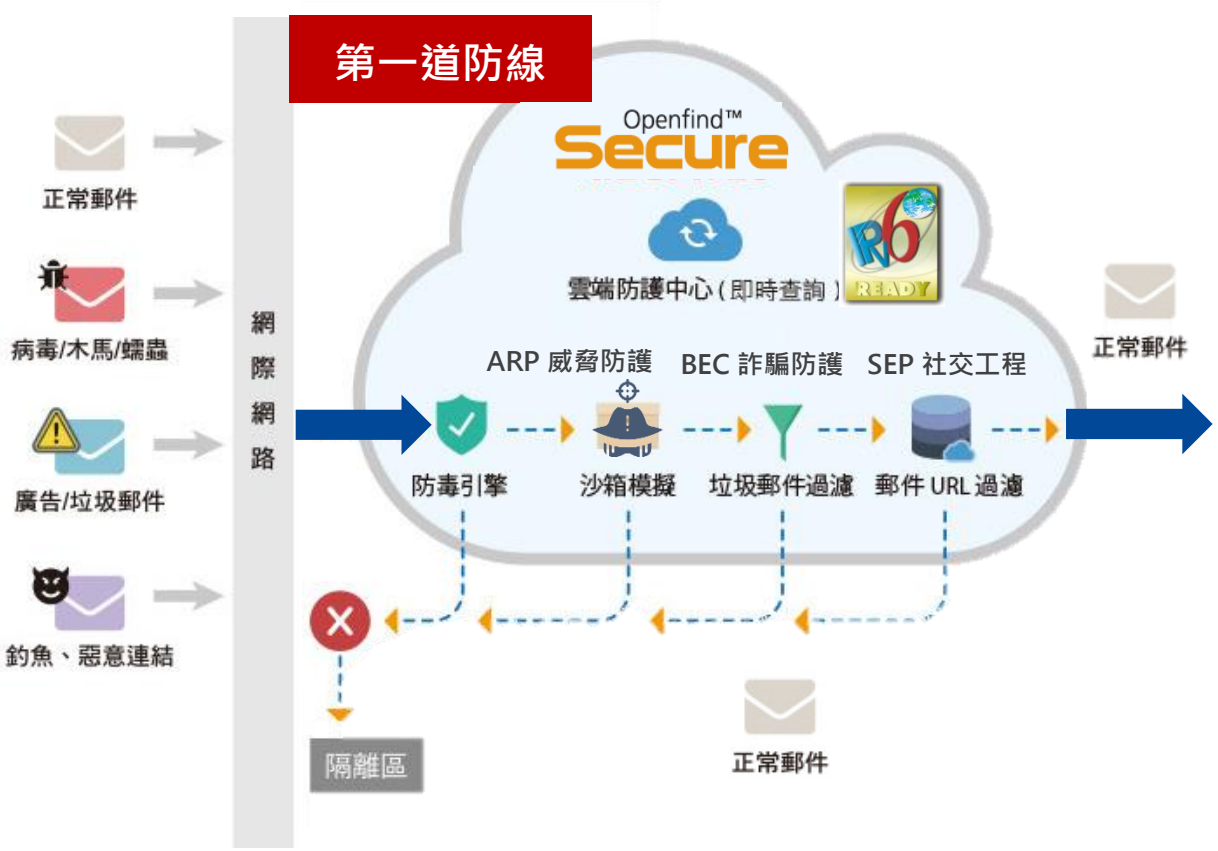
TREND MICRO SMART Protection Network™

CISCO

paloalto NETWORKS WF

雲端資安防護成為新趨勢

全球**大數據**樣本 x **7*24** 小時 x **Zero-hour** 防禦



雲端&自建型郵件系統

Microsoft 365

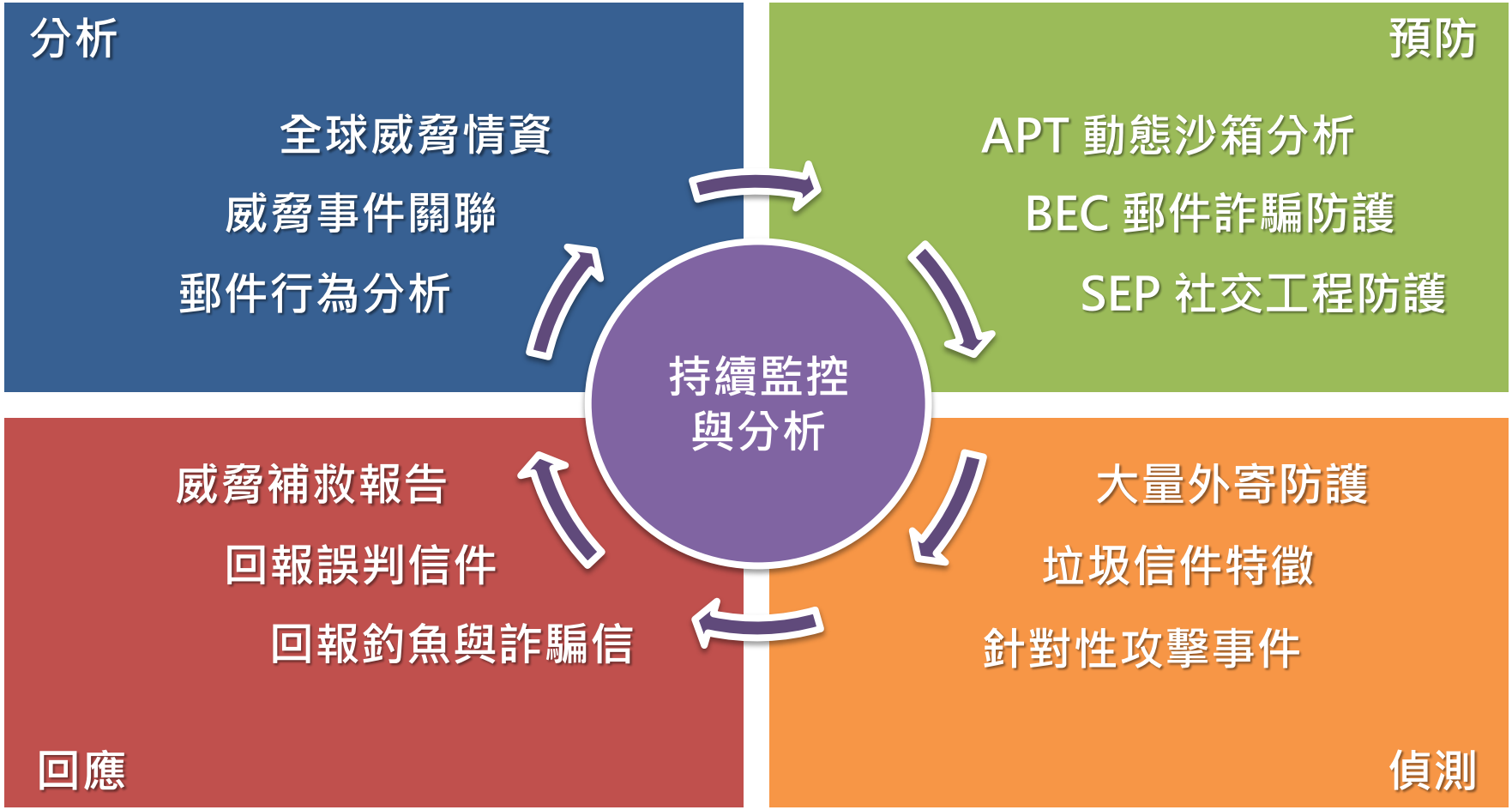
G Suite

Openfind™ MailCloud 企業雲端服務

Exchange

Openfind™ MAIL2000 電子郵件系統

阻擋資安威脅於企業之外



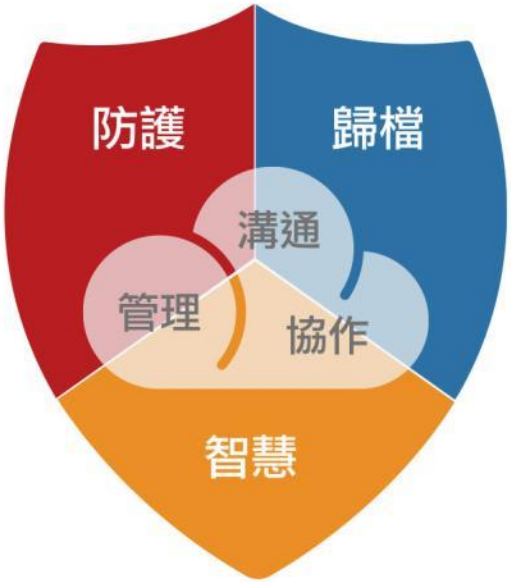
提供台灣在地化專業雲端信箱服務

Openfind™ MailGates 郵件防護系統

Openfind™ Mail2000 電子郵件系統

Openfind™ MailCloud 企業雲端服務

Openfind™ Enterprise Search 企業搜尋探勘系統



Openfind™ Secure 雲端資安服務

Openfind™ MailAudit 郵件稽核系統

Openfind™ MailCloud Messenger 企業溝通平台

Openfind™ ArkEase Pro 雲端儲存服務

Openfind™ MailBase 郵件歸檔管理系統

Q&A | **Email：neil_chang@openfind.com** **URL：www.openfind.com**