X-FORT

內部威脅的真相：UAM+AI 掌握員工不當行為

X-FORT 電子資料控管系統

精品科技 資安顧問 許祐福

FineArt

有獎徵答

根據IBM 2024年發佈的《資料外洩成本報告》
哪一種資安事件造成的平均損害金額最高?

A. 商業電子郵件詐騙
B. 社交工程
C. 網路釣魚
D. 惡意內部人員

Agenda

內部風險的現狀與挑戰

法律與合規框架下的企業資料保護策略

模擬案例— UAM+AI 掌握員工不當行為

X-FORT

Agenda

內部風險的現狀與挑戰

法律與合規框架下的企業資料保護策略

模擬案例— UAM+AI 掌握員工不當行為

X-FORT

內部人員導致的資料外洩趨勢連年成長

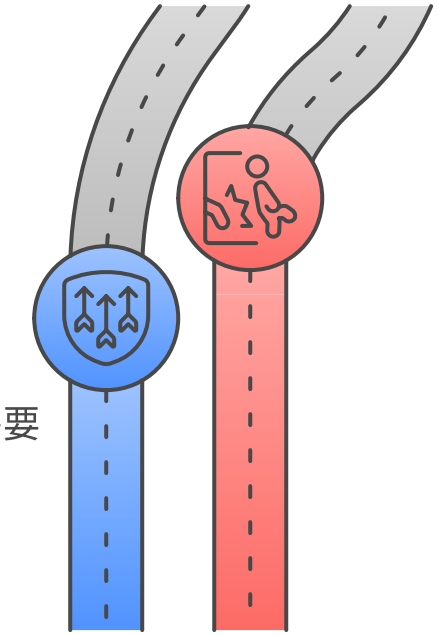
如何分配資訊安全資源？

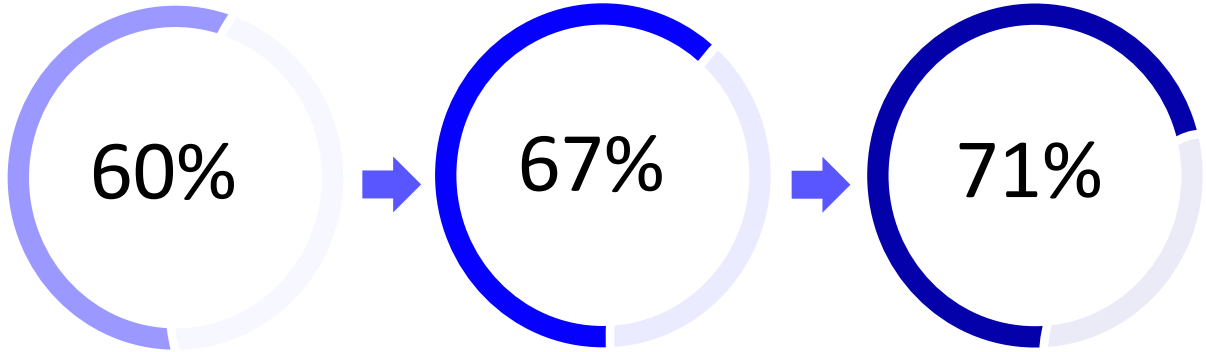
外部威脅

外部攻擊數量多
且被視為主要風險

內部威脅

內部威脅上升，需要
更多關注



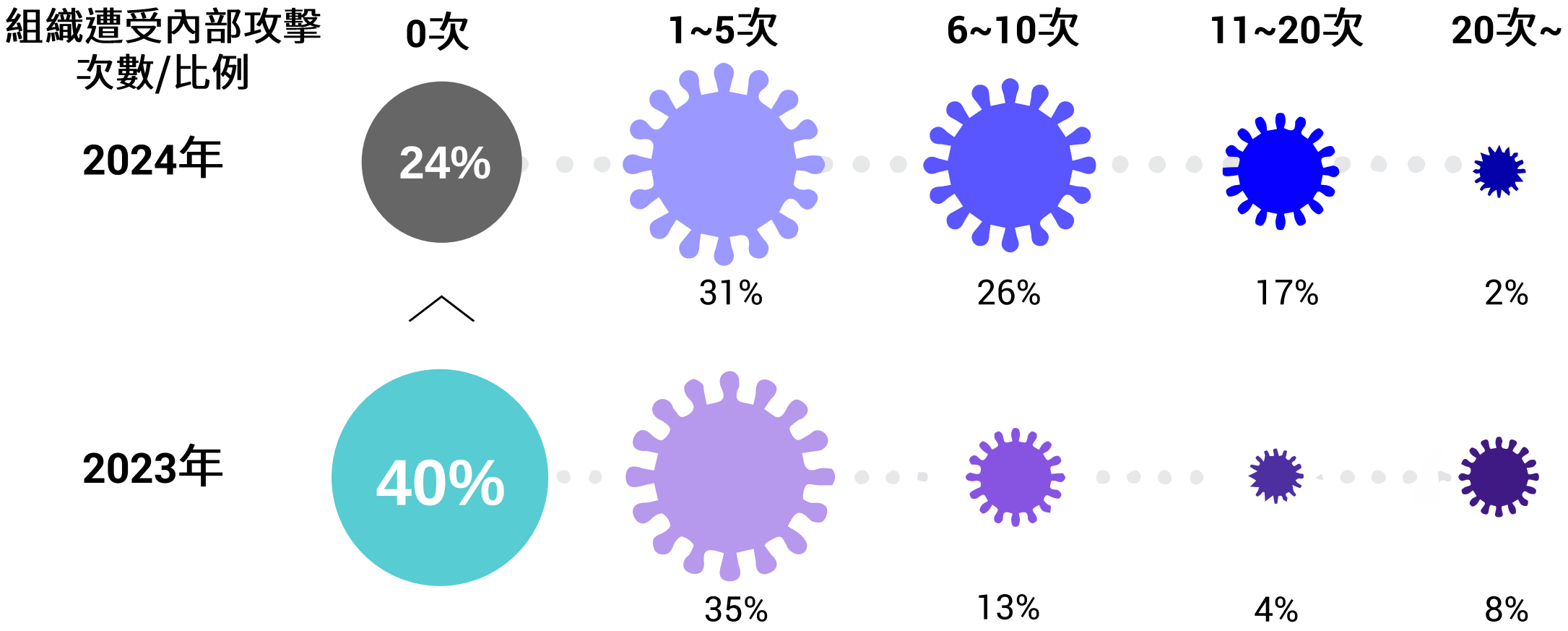


Ponemon Institute 的資料外洩成本報告
每年發生21至40 起內部威脅事件的組織比例，持續增加*

* Ponemon Institute: Cost of Insider Risk Global Report 2023

X-FORT

內部人員導致的資料外洩趨勢連年成長



*Cybersecurity Insiders: 2023 & 2024 Insider Threat Report

X-FORT

只有不到3成的組織自認已準備好應對內部威脅

完全配備

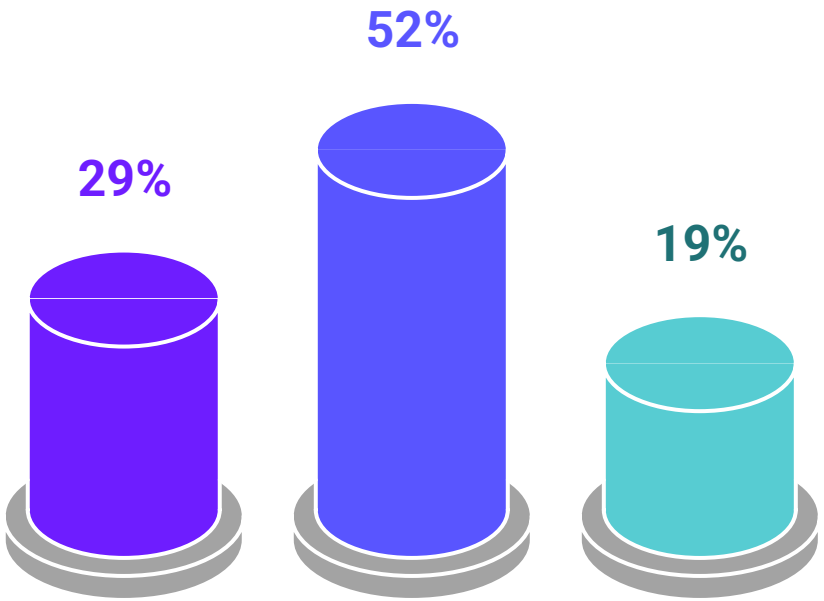
組織完全配備應對內部威脅的工具

部分配備

擁有工具但存在顯著差距

缺乏配備

缺乏有效監控和保護工具

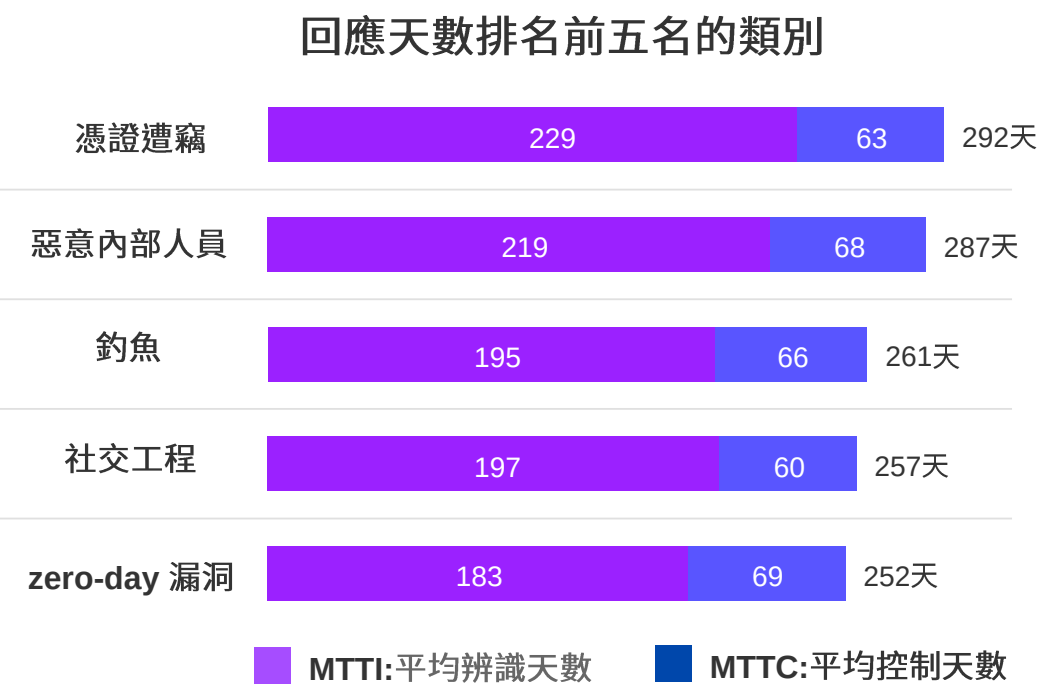


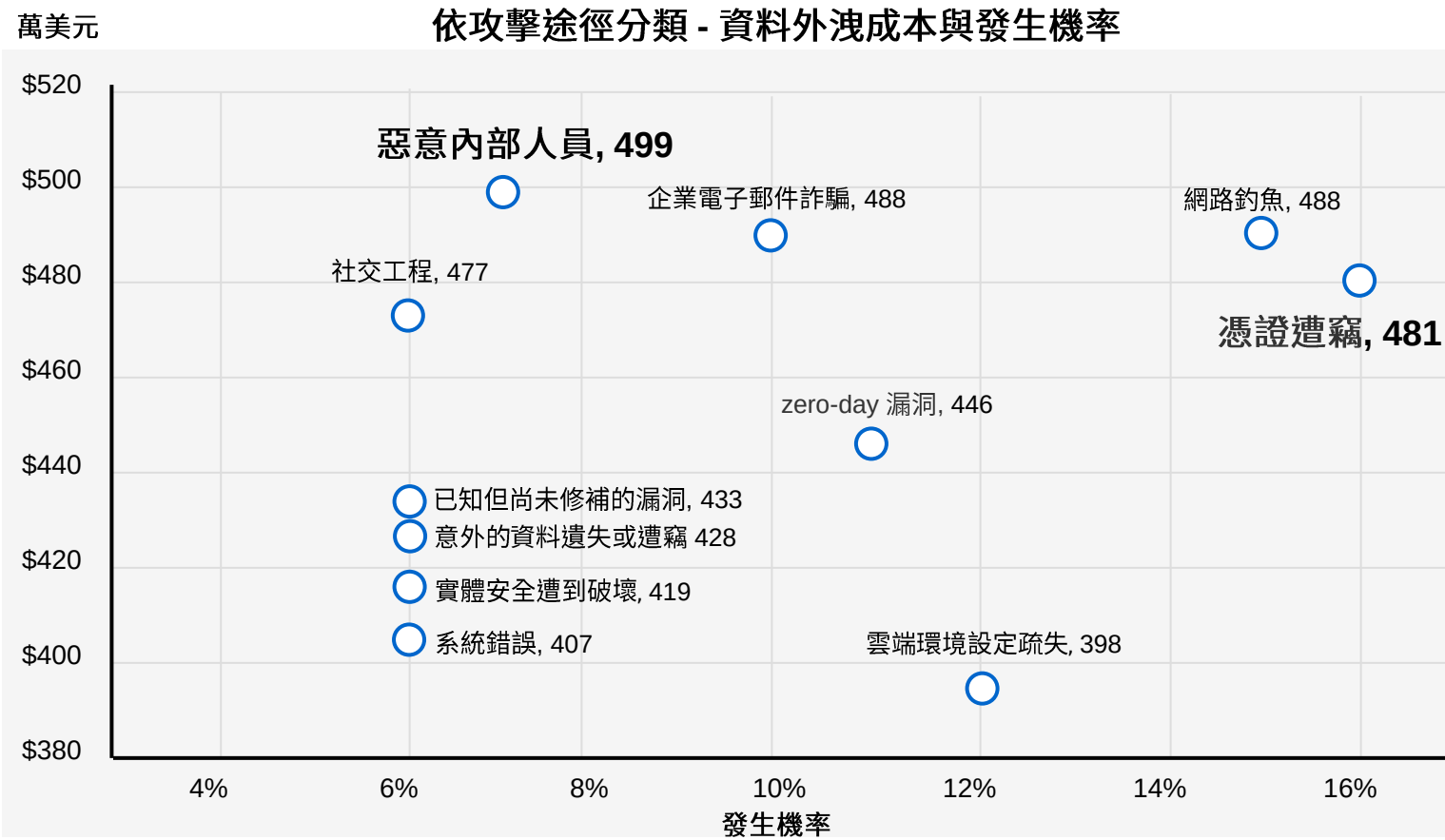
* IBM: Cost of a Data Breach Report 2024

X-FORT

企業的識別與處置時間、成本

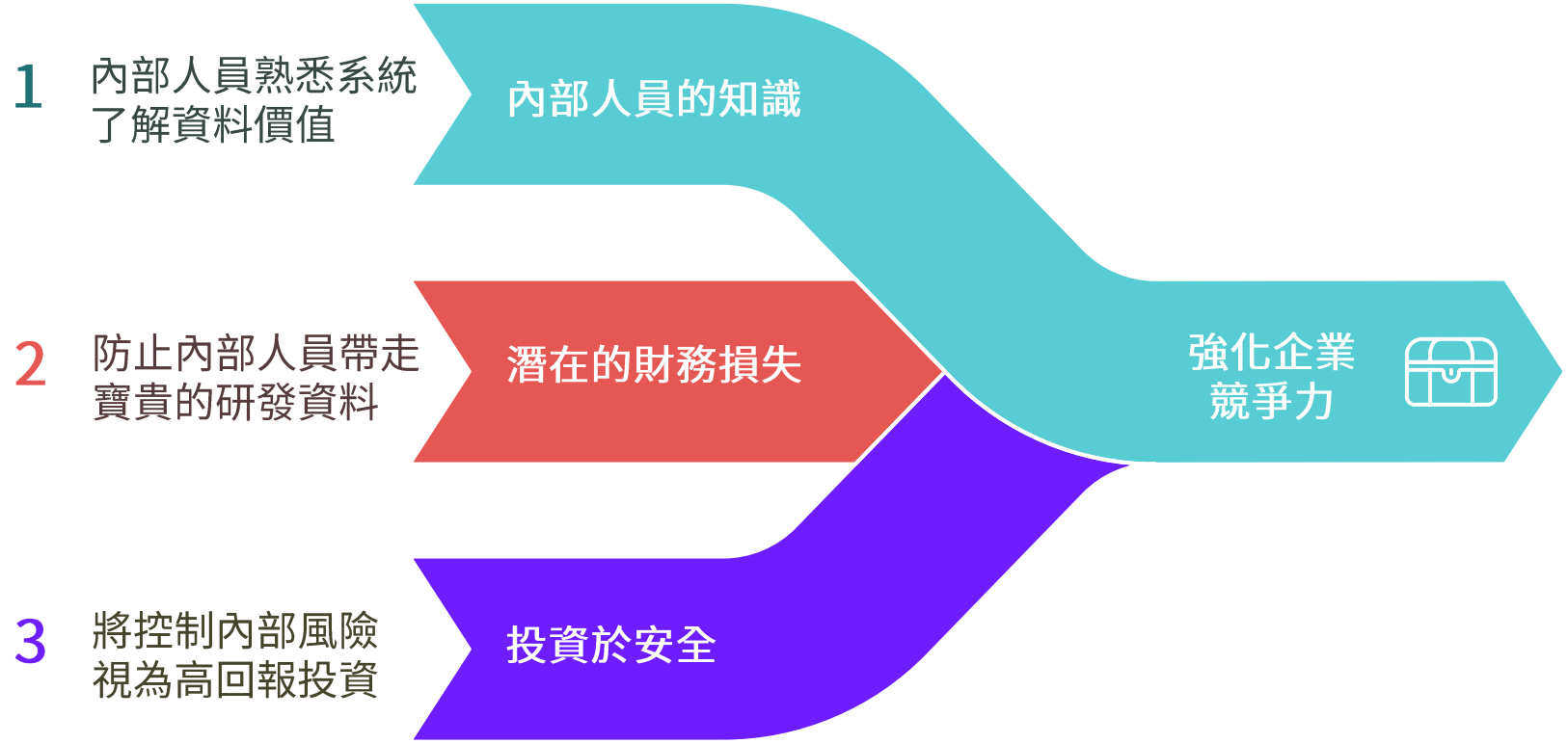
- 憑證遭竊或是惡意內部人員行為，企業平均需292天和287天才能發現並控制違規行為
- 內部人員攻擊的平均損失加處理成本高達499萬美元，為所有資安事故中成本最高





* IBM: Cost of a Data Breach Report 2024

內部風險管理是企業競爭的重要戰略武器



X-FORT

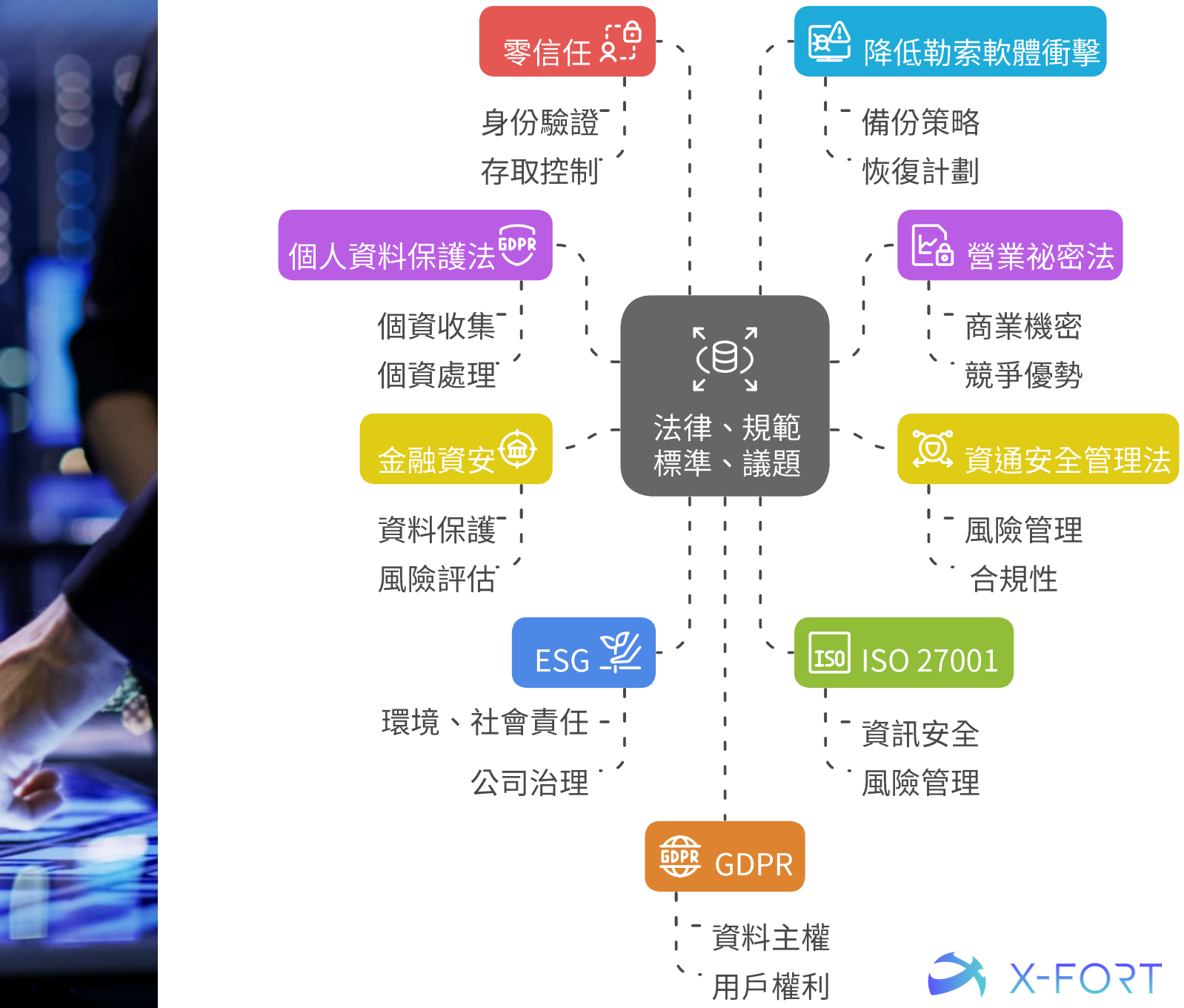
Agenda

內部風險的現狀與挑戰

法律與合規框架下的企業資料保護策略

模擬案例— UAM+AI 掌握員工不當行為

X-FORT


法律、規範
標準、議題
零信任
身份驗證
存取控制
降低勒索軟體衝擊
備份策略
恢復計劃
個人資料保護法
GDPR
個資收集
個資處理
營業祕密法
商業機密
競爭優勢
金融資安
資料保護
風險評估
資通安全管理法
風險管理
合規性
ESG
環境、社會責任
公司治理
ISO 27001
資訊安全
風險管理
GDPR
資料主權
用戶權利

X-FORT

金管會: 三大面向強化上市櫃公司資安

監理協助

加入TWCERT/CC，共享資安情資

導入ISO27001並取得第三方認證

納入公司治理評鑑指標加分項目

公司治理

設立資安長及專責單位

資安納入內部控制、年度稽核項目

資安納入公司治理評鑑

資訊揭露

發生重大資安事件，應即時發布重大訊息

年報及公開說明書揭露重大資安風險

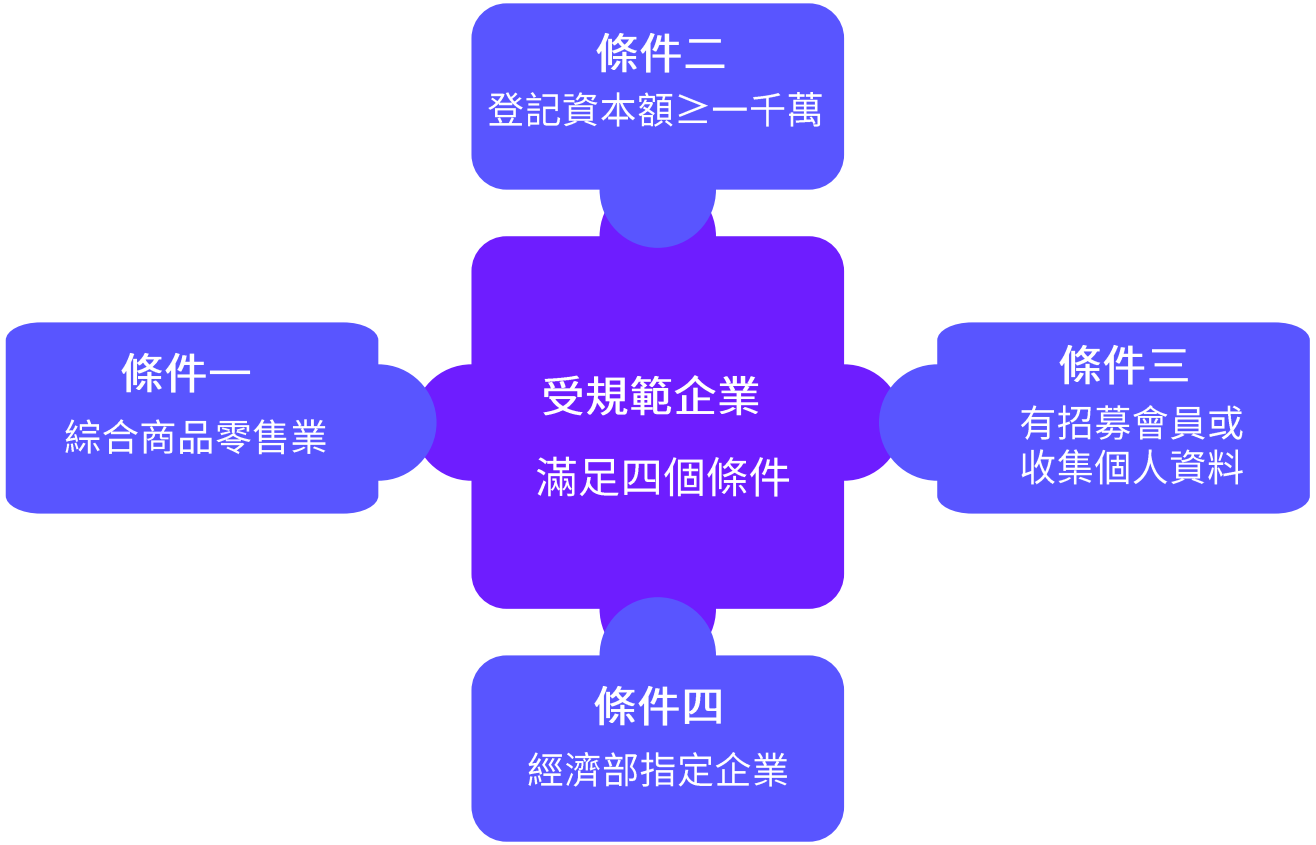
說明資通安全管理政策、方案及投入資源

相關罰則：

- 金管會: 發生重大資安事件未即時公告，最高可罰**新台幣500萬罰鍰**
- 個資法: 如發生個資外洩等事件，須**受主管機關調查**
- 個資法: 發生個資外洩，如持續未改善或情節重大，**最高可裁罰1500萬**

X-FORT

經濟部: 要求零售業落實個資保護



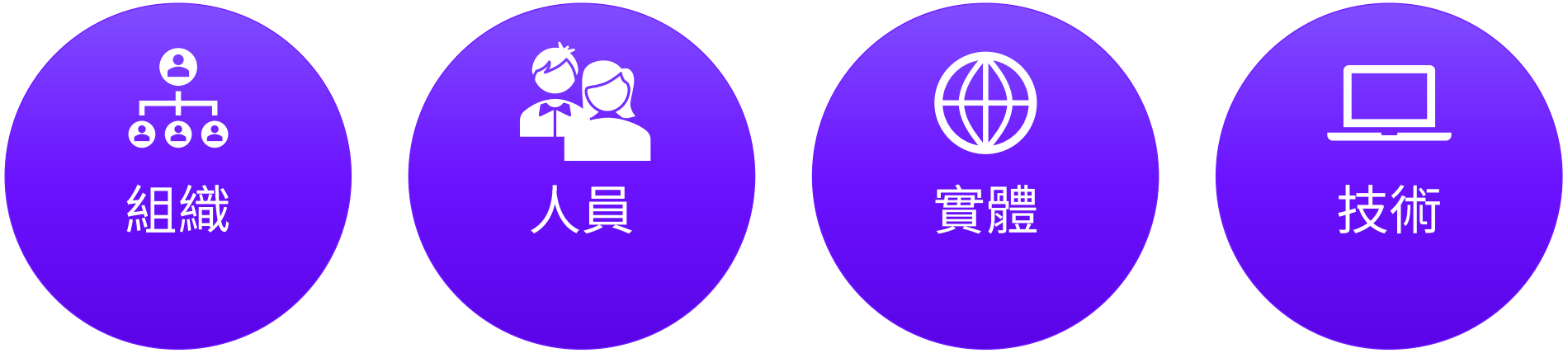
需於5月12日前訂定
「個資檔案安全維護計畫」

衝擊約6,800家企業

風險提示： 資料外洩、駭客入侵、內部失誤可能導致客戶信任損失
應對策略： 訂定並落實個資保護計劃，避免法律責任及品牌聲譽損害

X-FORT

ISO 27001: 2022 改版–明確引入DLP、資訊分類技術



X-FORT

金管會鼓勵金融業: 以零信任思維深化資安防護

身分

- 採多因子身分驗證
- 優先選擇安全強度較高、可抗網路釣魚者

➢ 動態認證碼
➢ FIDO
➢ 晶片卡

設備

- 可識別為已納管之設備
- 具設備健康合規性管理

➢ 作業系統更新
➢ 防毒軟體/病毒碼更新
➢ 端點監測

網路

- 全程加密傳輸
- 具適當網段分割，採最小需求原則的網路連線

➢ 建議採各系統獨立之網段區隔

應用程式

- 包含源自內部與外部的安全性檢測
- 採最小授權原則

資料

- 資料分類，依身分別支援最小授權規則
- 機敏性資料加密儲存

* 金管會: 金融業導入零信任架構參考指引

設備安全狀態

設備

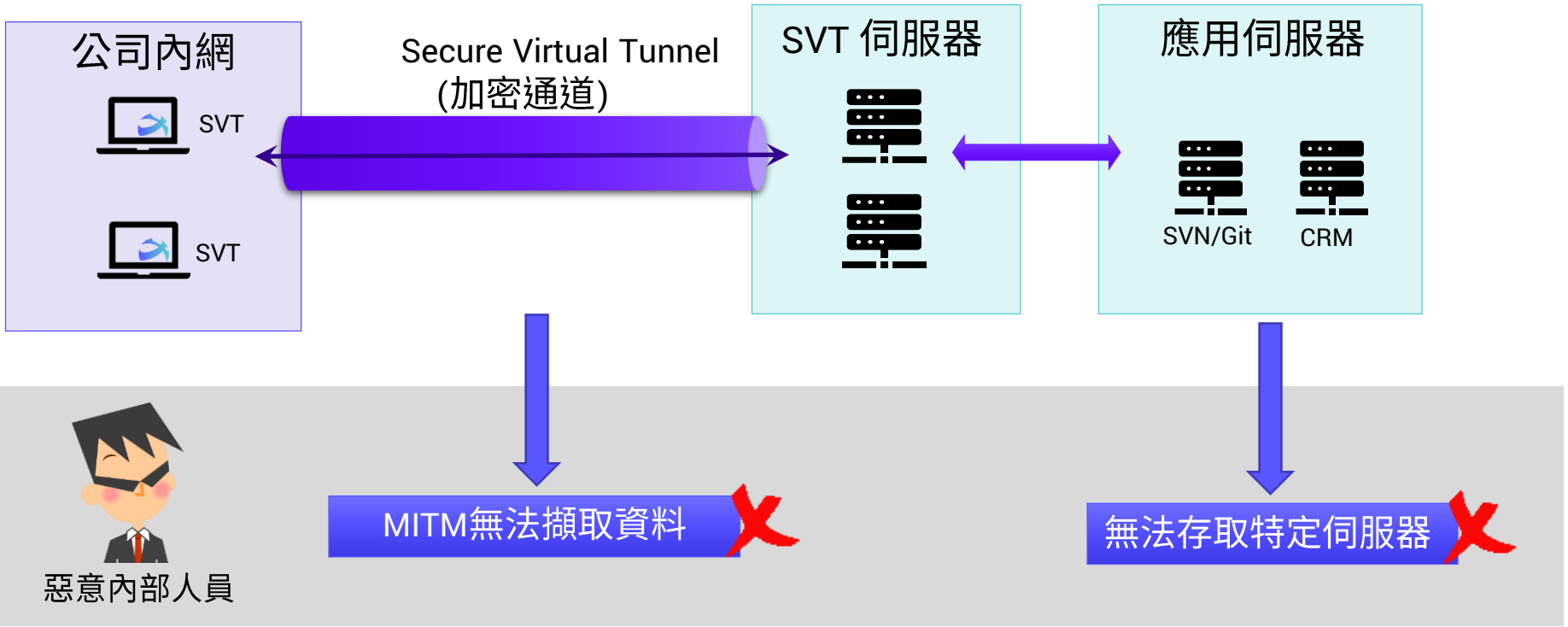
- 可識別為已納管之設備
- 設備健康合規性管理
- 作業系統、防毒軟體更新

網路零信任 - Agent-Based 微分割

網路

- 全程加密傳輸
- 網段分割
- 最小需求原則

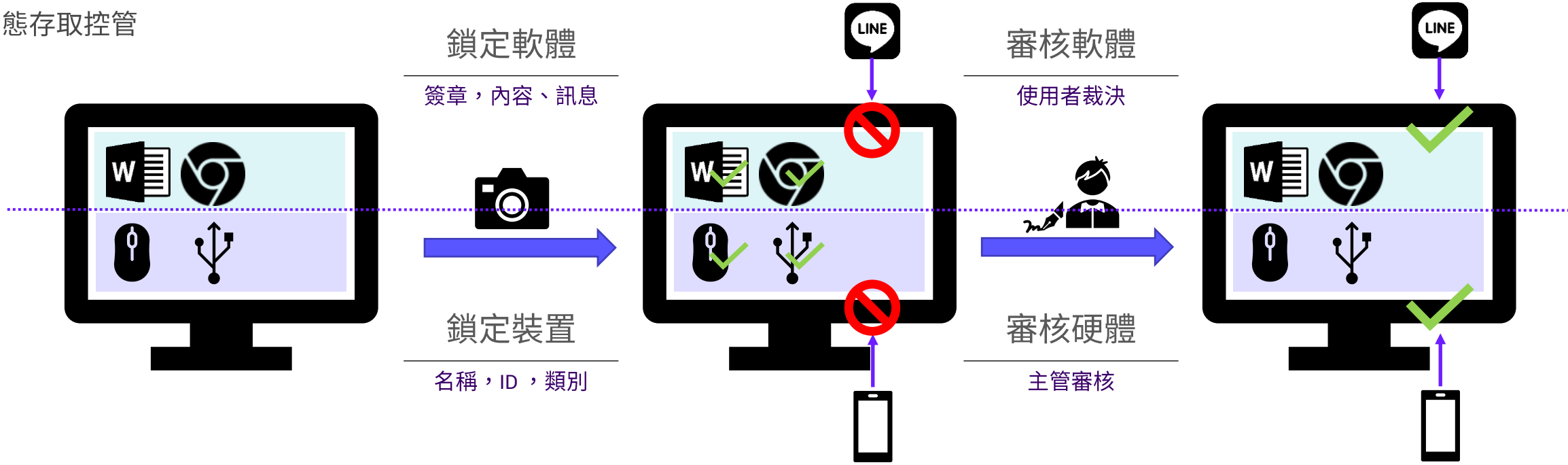
- 識別信任裝置，基於角色的存取控制(Role-Based Access Control)
- 防止MITM或軟體竊取入侵行為
- 應用系統可跨平台



應用程式與硬體裝置零信任

應用程式

- 安全性檢測
- 最小授權原則
- 動態存取控管



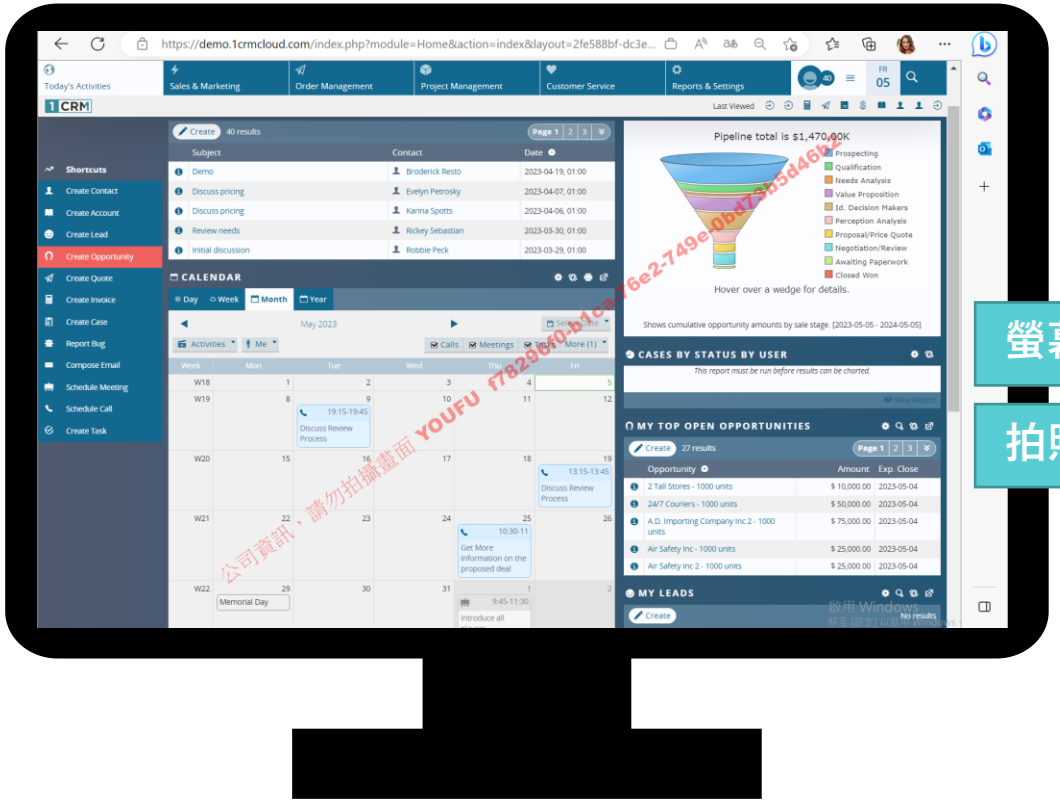
X-FORT

應用程式 –最小授權原則

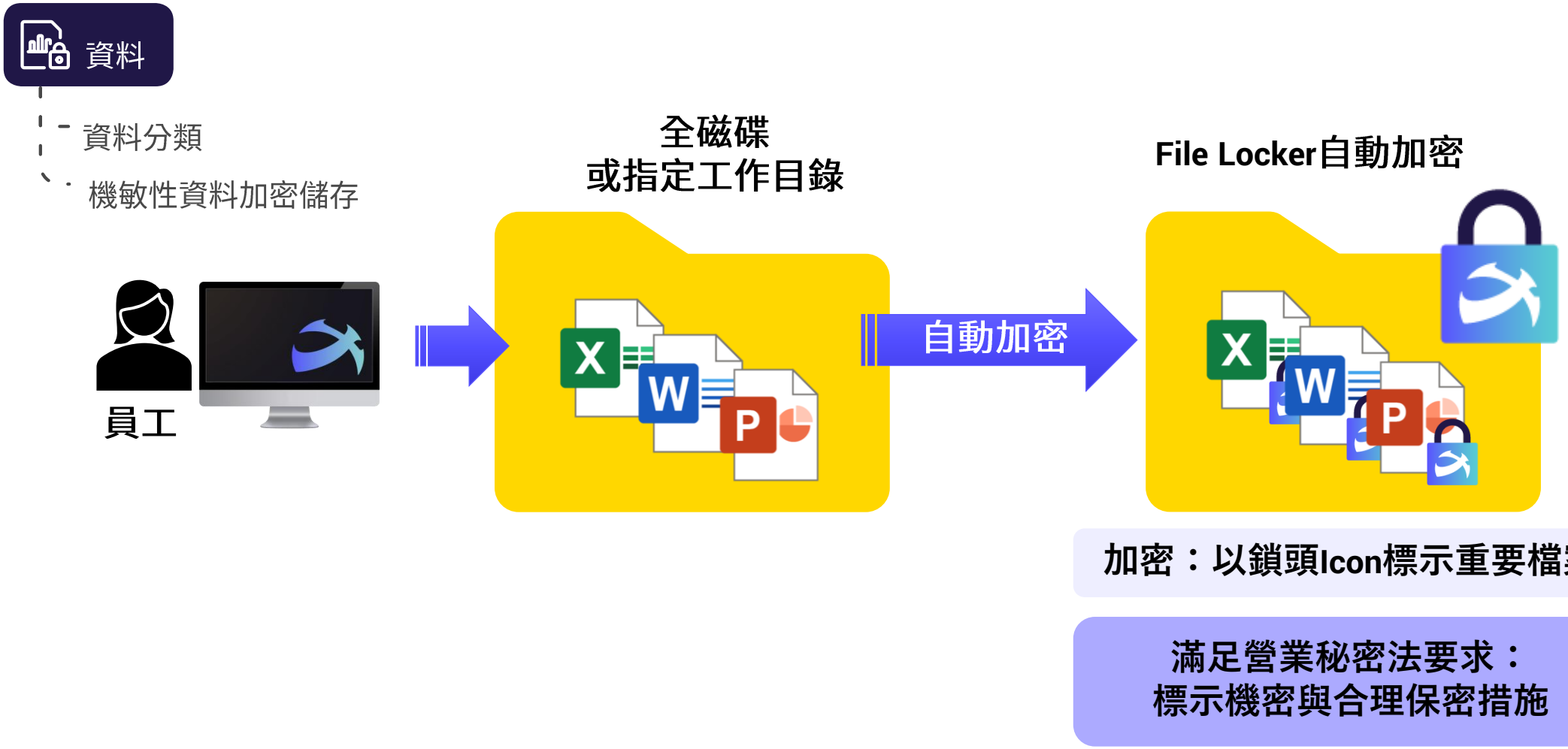
應用程式

- 安全性檢測
- 最小授權原則
- 動態存取控管

- **使用重要系統或客戶資料，禁止複製內容包含**
  - **禁止複製**
  - **禁止列印**
  - **禁止另存新檔**
  - **禁用螢幕截圖**
  - **顯示螢幕浮水印，提醒員工遵守資安規範**

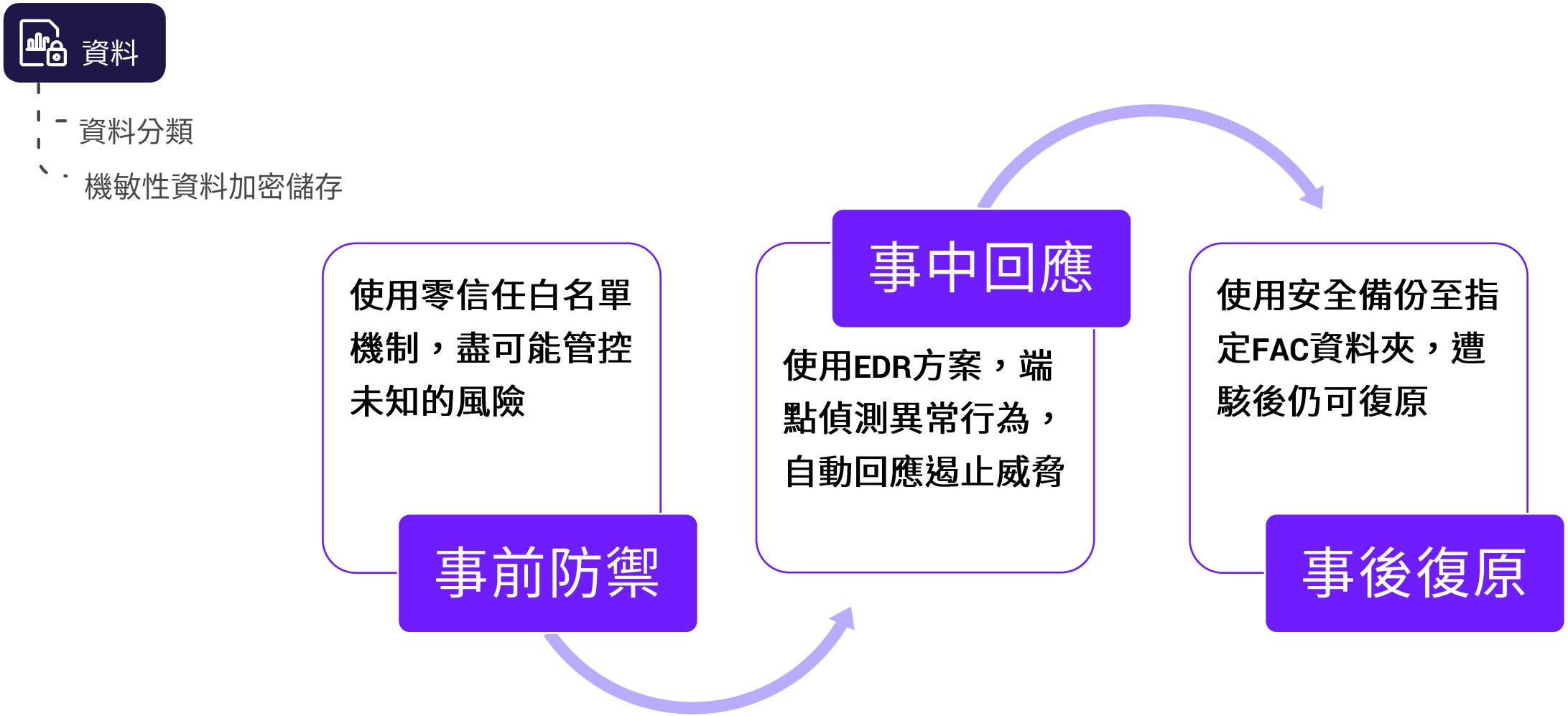


資料安全 – 清查重要檔案並自動加密



X-FORT

降低勒索軟體 (Ransomware) 攻擊可能性



X-FORT

Agenda

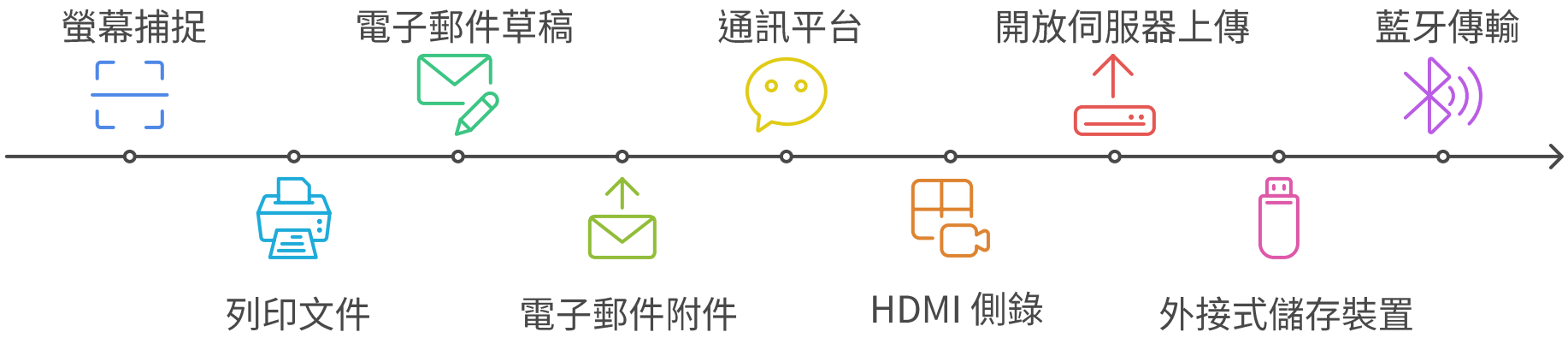
內部風險的現狀與挑戰

法律與合規框架下的企業資料保護策略

模擬案例— UAM+AI 掌握員工不當行為

X-FORT

MITRE: 潛在風險指標 (Potential Risk Indicators, PRIs) -資料竊取



X-FORT

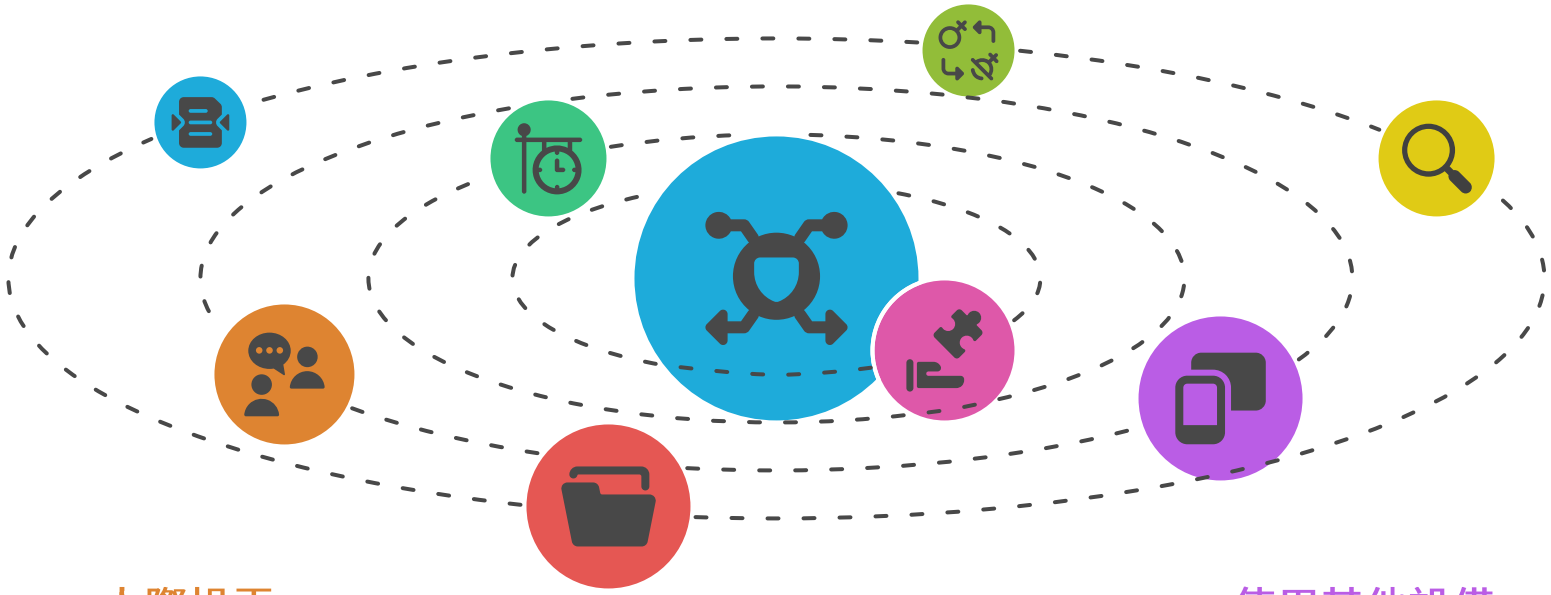
MITRE: Potential Risk Indicators (PRIs) - 規避行為

內容轉換
轉換內容
以避免被檢測

時間管理
錯開時間
以避免被注意

混合活動
參與多種活動以混淆

學習和偵查
搜尋規避技術



人際操弄
請他人協助完成

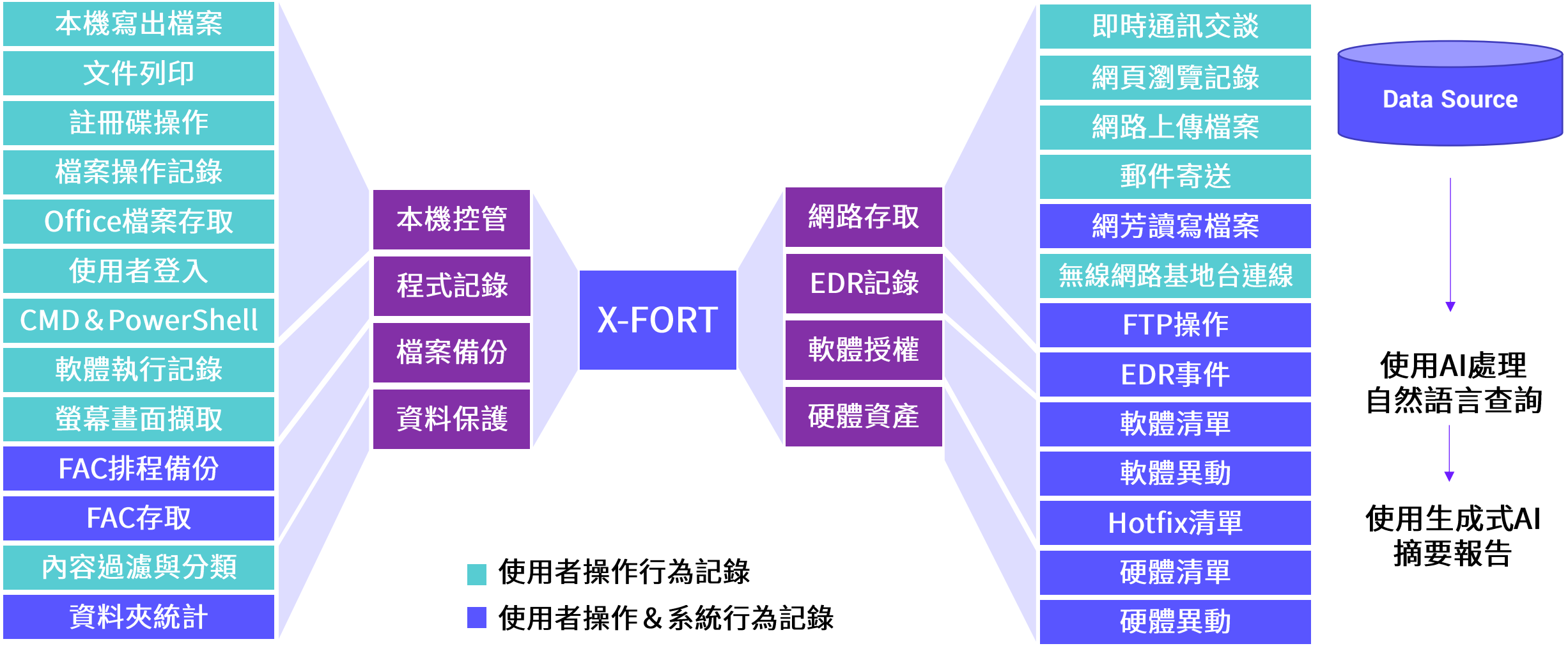
蒐集內容
儲存內容以備
將來使用

混淆檔案內容
混淆內容以
掩蓋其意圖

使用其他設備
使用不同的設備
以避免檢測

X-FORT

全方位的使用者與電腦操作記錄



*僅列舉代表性記錄, 未涵蓋X-FORT所有記錄/資料類型

X-FORT

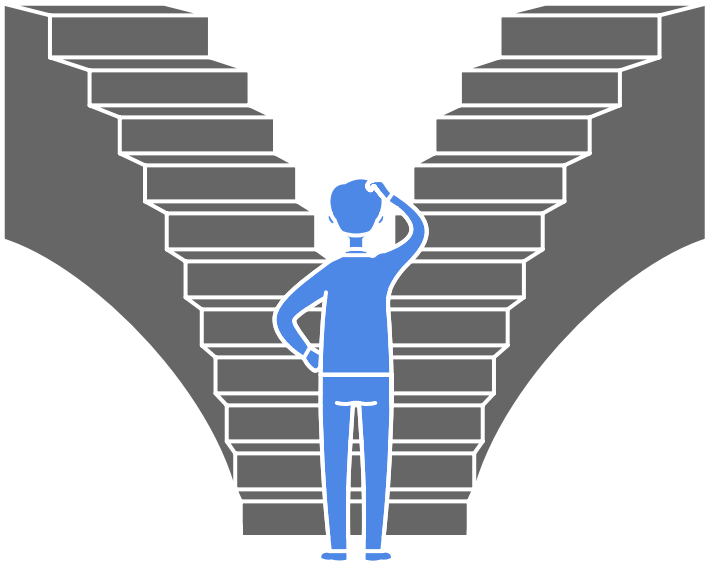
模擬情境 - 資料外洩是無心的還是故意？

無心的疏忽

行為是意外的，沒有惡意的意圖

惡意行為

行為是故意的，旨在洩漏敏感資料



事件背景

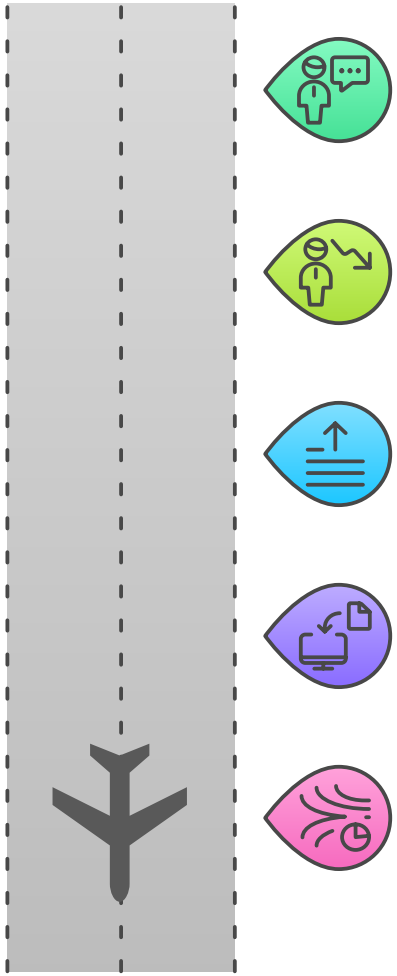
- 早上9點半，資安團隊接收到一則系統警報：一名業務人員使用LINE傳出大量檔案，行為遠超同部門的正常範圍
- 你被指派為調查人員，負責查出異常原因

初步分析

- 與當事人面談，當事人聲稱，他只想寫出一個檔案，不小心選到多個檔案，才會誤觸警報!

X-FORT

內部安全事件處理序列



報告給高階主管

向資安長和人事經理報告

人事經理的反應

人事經理披露，該名人員上周已提出離職申請

高階主管的指示

指示謹慎處理調查

電腦和活動記錄的審查

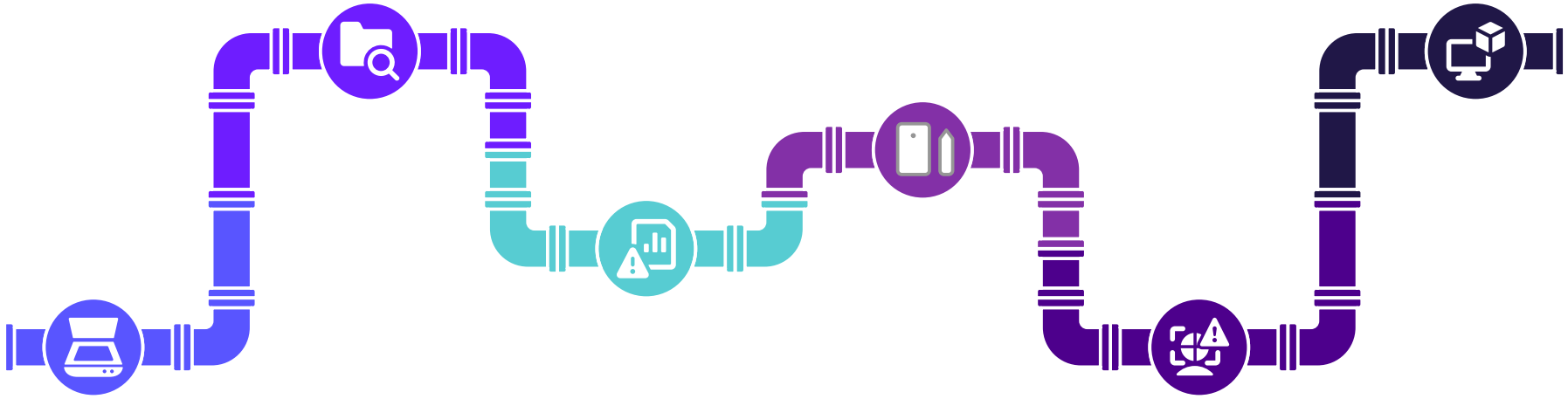
審查電腦檔案和活動記錄

進一步分析的委託

提出分析結果，作為高階主管決策依據

X-FORT

清查使用者電腦內所有檔案



01

啟動掃描工具

開始對電腦
進行全面掃描

02

掃描檔案

檢查檔案以
識別敏感內容

03

發現機敏資料

識別電腦內
有多少敏感資料

04

標記檔案

為檔案貼上
分類標籤

05

計算分數

計算整體 & 個別
檔案安全性

06

風險處置

針對高風險檔案
加密、搬移、刪除

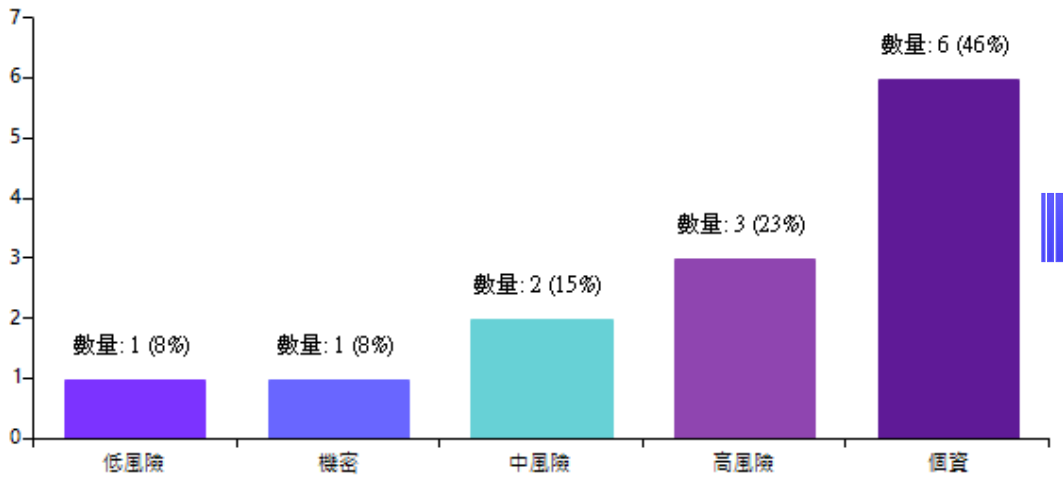
X-FORT

使用者端掃描結果與處置

蒐集內容

全面掃描

掃描結果



高風險檔案清單

從掃描結果發現，該人員電腦內，有許多不屬於該人員負責的專案或客戶資料

X-FORT

UAM 使用者活動監控 + AI: 掌握不當行為

識別分析需求

分析網路行為
和檔案操作

使用資安儀表版

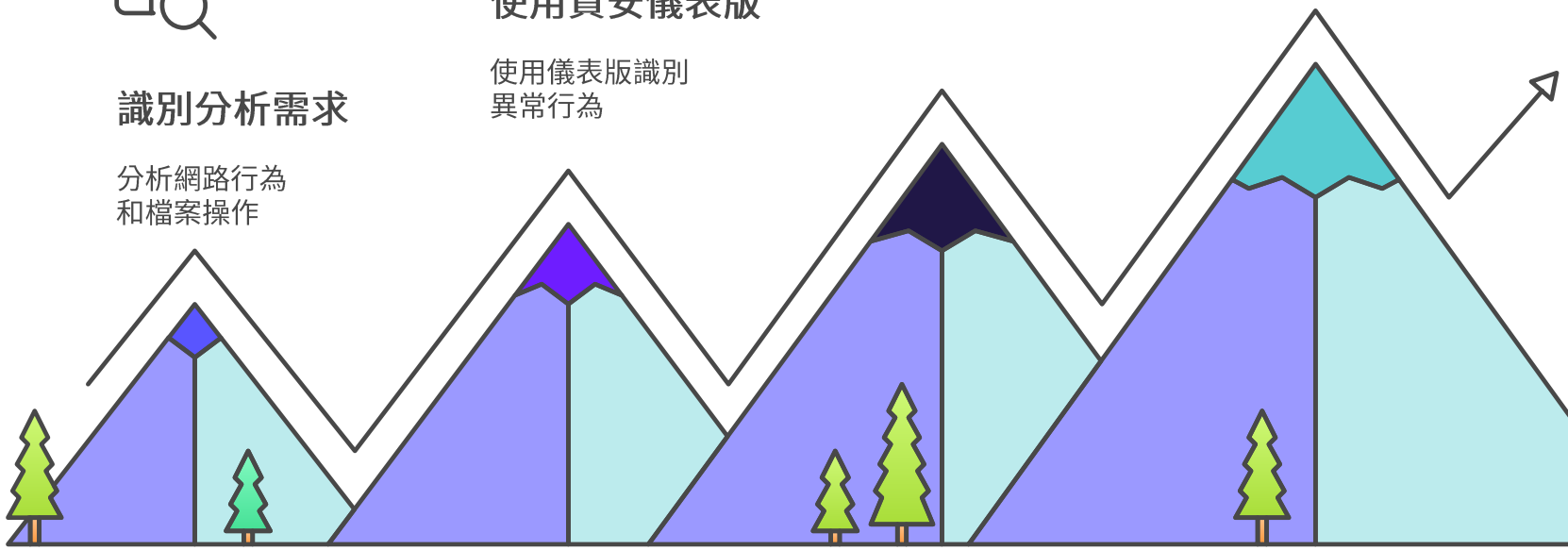
使用儀表版識別
異常行為

應用自然語言查詢

使用查詢語言找到異常

利用LLM進行摘要

使用LLM讀取和摘要
活動記錄



X-FORT

分析使用者行為 - 發現異常

Google 搜尋

搜尋如何
規避監控的方法

詢問 ChatGPT 關於
規避技術的問題

ChatGPT 詢問

檔案混淆

嘗試掩蓋檔案
以隱藏行為

透過 Line 傳出
大量敏感檔案

敏感檔案

VPN WiFi 規避

使用個人 Wi-Fi
以避免監控

將檔案上傳至
個人郵件或雲端硬碟

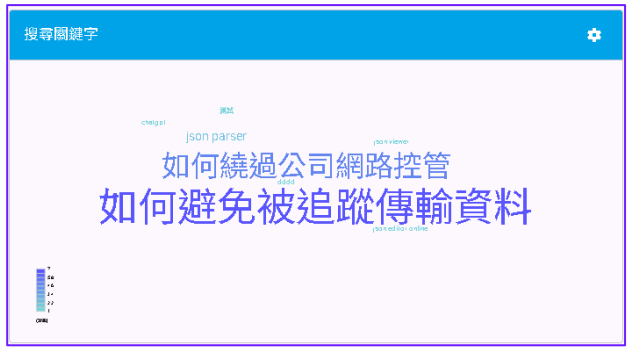
檔案上傳

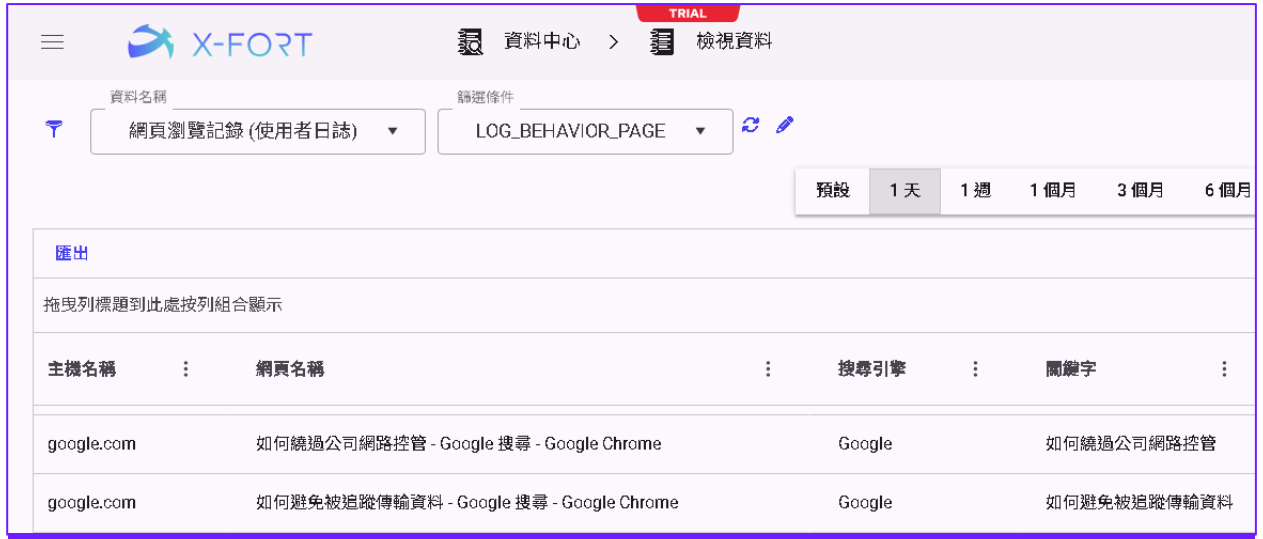
X-FORT

曾使用 Google 搜尋: 規避公司網路控管

學習和偵查

Google 搜尋





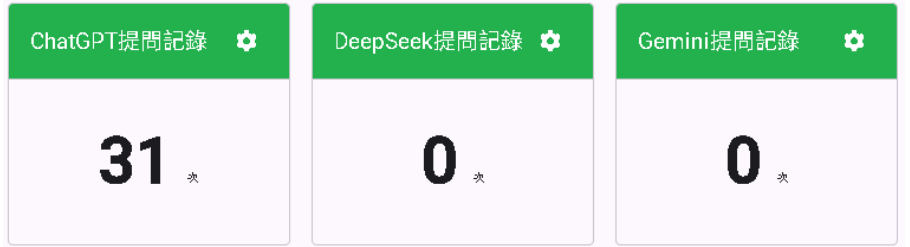
查看搜尋關鍵字

X-FORT

曾經在 ChatGPT 詢問，規避監控的技術

學習和偵查

詢問 ChatGPT 規避技術



上傳程式名稱	上傳網址	主機名稱
chrome.exe	https://chatgpt.com/backend-api/conversation/init	chatgpt.com
chrome.exe	https://chatgpt.com/backend-api/conversation	chatgpt.com
chrome.exe	https://chatgpt.com/backend-api/conversation	chatgpt.com
chrome.exe	https://chatgpt.com/backend-api/conversation/init	chatgpt.com

*Dump.txt - 記事本

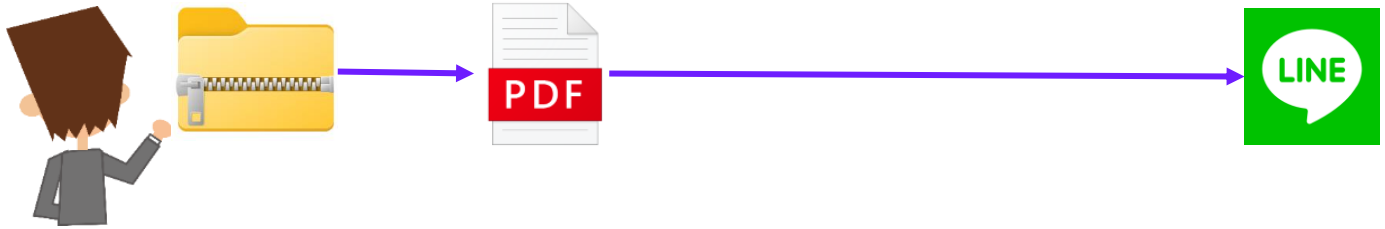
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明


```
{
"action":"next",
"messages":[
{
"id":"bbed9d8a-0fad-4a5f-bb1f-90891b1d14bd",
"author":{
"role":"user"
},
"create_time":1742033094.42,
"content":{
"content_type":"text",
"parts":[
"如何繞過公司網路控管"
]
```


查看 ChatGPT 提問內容

將 .zip 檔案更改為 .pdf 後用 LINE 傳送檔案

內容混淆



X-FORT 資料中心 > 檢視資料

資料名稱: 檔案操作 (使用者)　篩選條件: (SYSTEM) 檔案操作記錄 (更名)

匯出

拖曳列標題到此處按列組合顯示

動作類型	來源檔案名稱	來源檔案副檔名	目的檔案名稱	目的檔案副檔名
更名檔案	體驗檔案.zip	zip	體驗檔案.pdf	pdf

更改檔案副檔名

X-FORT 資料中心 > 檢視資料 TRIAL

資料名稱: 網路上傳檔案　篩選條件: LOG_IM_FILE_TRANSFER　預設 1 天 1 週 1 個月 3 個月

匯出

拖曳列標題到此處按列組合顯示

檔案名稱	視窗標題	已符合資訊類型	已符合分類標籤
體驗檔案.pdf	LINE	C#程式碼關鍵字(2),身分證字號(215),手機(191),中文地址(58),Email(81)	中風險,個資

仍被辨識出壓縮檔，並一一過濾檔案內容

X-FORT

使用私人 Wi-Fi，寄送檔案到私人Gmail信箱

使用其他設備

使用私人 Wi-Fi 的連線記錄

將公司檔案寄到 Gmail，且有夾帶附檔

X-FORT

分析X-FORT-console記錄

混合活動

人際操弄

分析X-FORT-console記錄

作者：FaChatGPTOne

機密文件的列印記錄

從即時通訊交談記錄分析資料外洩風險

分析與工作無關的網頁瀏覽記錄

從郵件記錄分析資料外洩風險

傳訊息給 分析X-FORT-console記錄.....

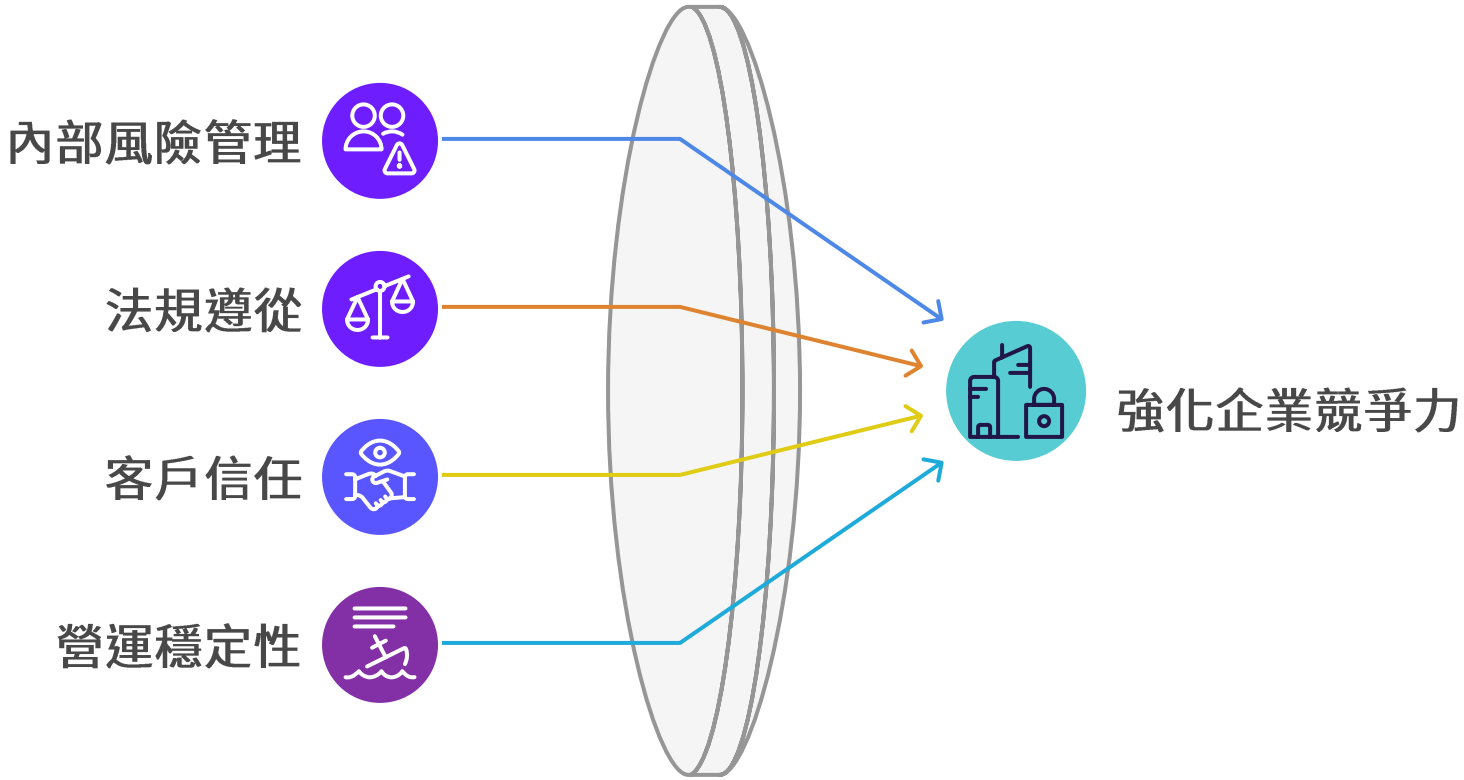
調查結論與後續措施

- **下午5點，向高階主管、和人事主管報告**
- **符合多項MITRE的潛在風險指標，推測當事人屬於主動的惡意行為**
- **高階主管要求法務長一同處理，保全證據力**

- **後續措施**
  - 即刻處置： 停用系統帳號、扣留設備、保全證據
  - 內部檢討： 檢視監控制度、權限控管、加強資安意識教育

X-FORT

將內部資安視為戰略投資，形成企業核心競爭力



使用者行為記錄

查詢

AI幫助發現異常

分析

X-FORT提供控管

對策

落實資安政策

落實

資安講座

09:00 多層次端點防護打造最強資安堡壘

11:00 UAM+AI 掌握員工不當行為

12:30 金融安全新格局，從內到外的防禦

13:30 零售業個資攻防戰，全方位安全策略

14:30 ISO 27001企業合規的高效解決方案

1F Q201 精品科技攤位

場場遊戲等你來挑戰!

X-FORT

資安巡航 守護無垠

Ultimate Security for Business Longevity

FineArt