Threat Assessment

假期攻擊模式：台灣企業資安的結構性警訊

年假無防線？從圓山大飯店到南光製藥的連環攻擊解析

STRATEGIC THREAT INTELLIGENCE BRIEFING // LUNAR NEW YEAR INCIDENTS

關鍵洞察：5 家企業，5 個產業，1 個模式

受害者 (Victims)

圓山大飯店、南光製藥、機車製造龍頭、國際物流、某醫院。

核心弱點 (Core Weakness)

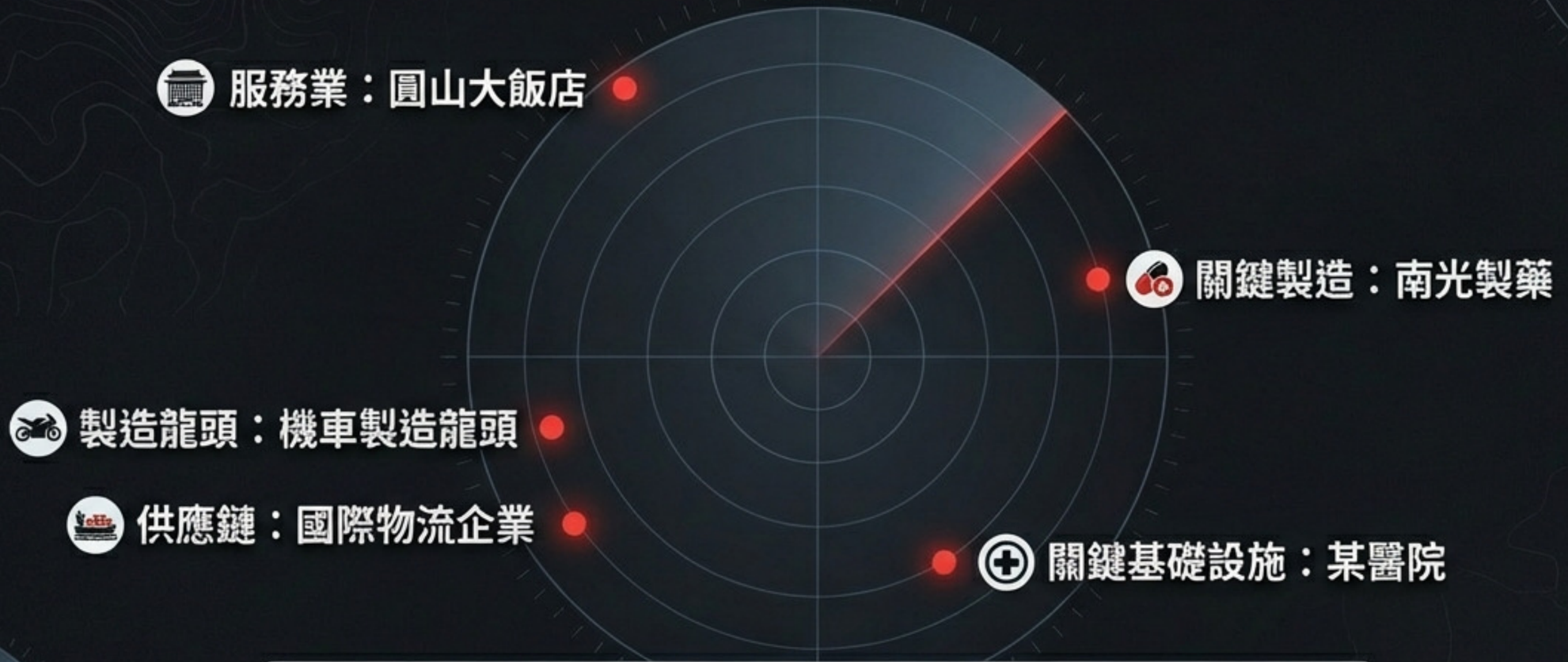
駭客專挑農層春節的「防禦真空期」下手。

攻擊演變 (Evolution)

從單純竊取資料轉向「癱瘓營運」與「勒索最大化」。

「這不是單一事件，這是一個明確的趨勢訊號。」

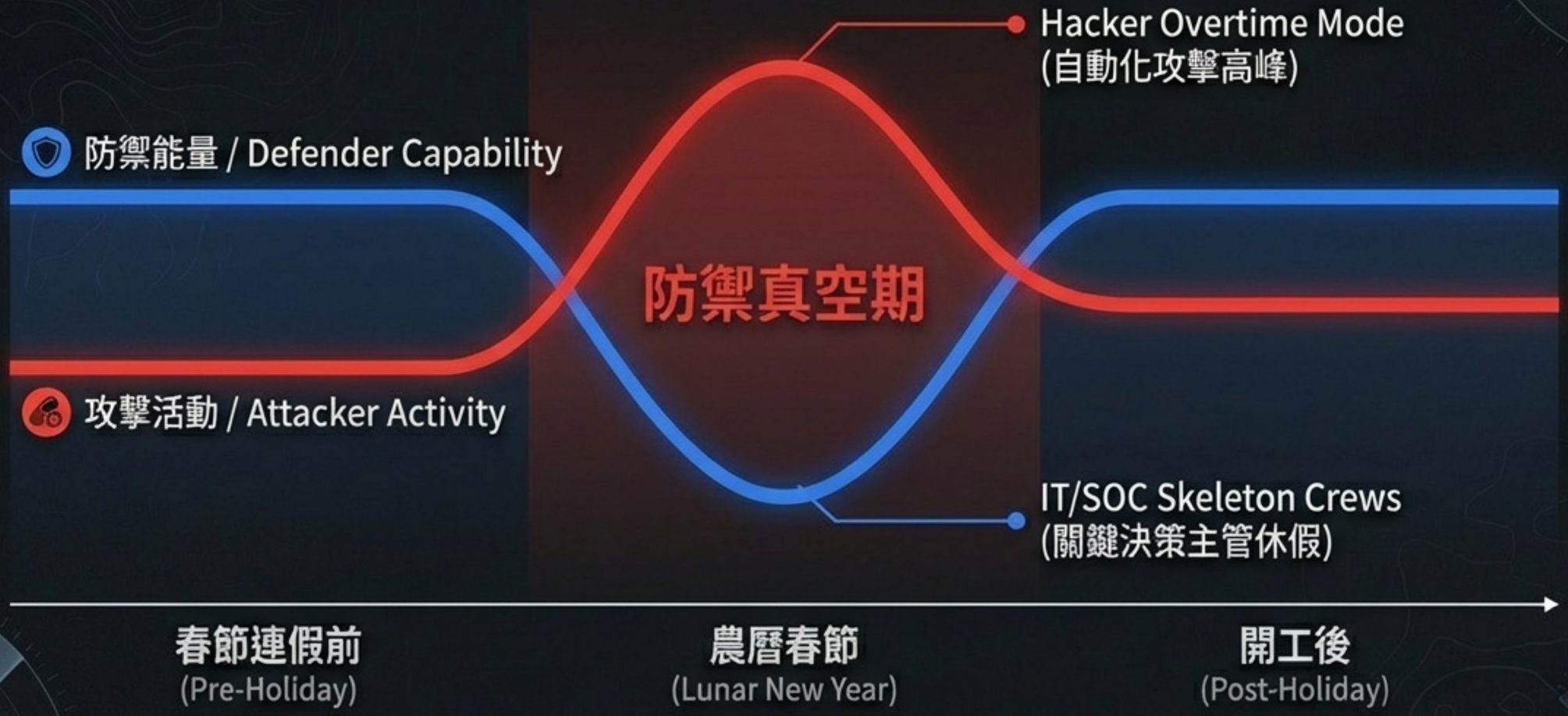
產業極度分散：攻擊已全面常態化



Insight：攻擊不再是針對特定產業的精準行動，而是大規模的自動化掃描。

產業分佈極度分散 = 每個產業都在射程範圍內

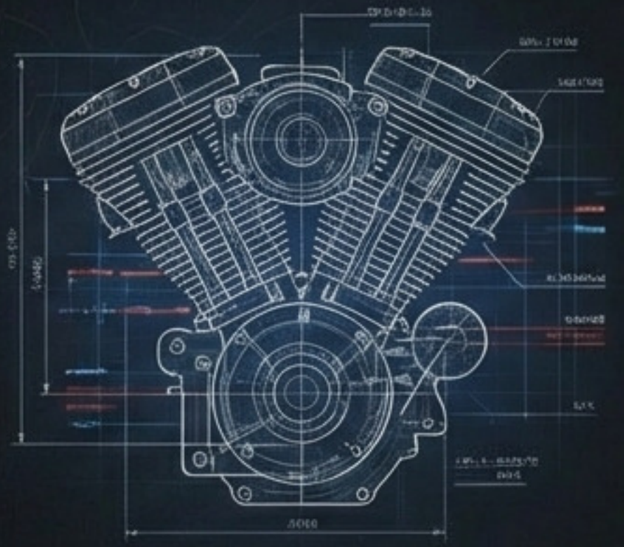
假期攻擊模式 (Holiday Attack Pattern) 定義



攻擊者邏輯：「他們不挑你最忙的時候，而是挑你最鬆懈的時候。」

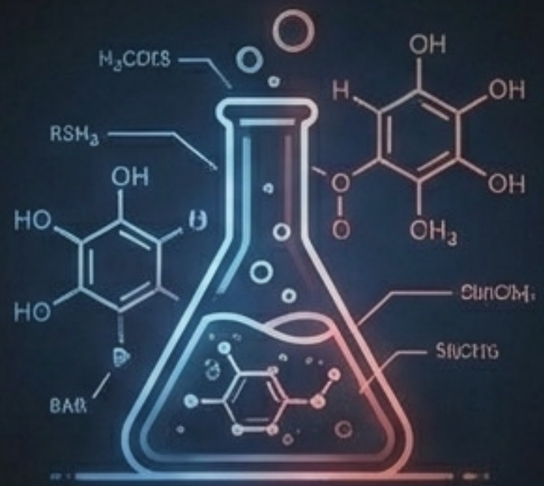
營運風險：當商業機密成為勒索籌碼

機車製造龍頭 vs. Space Bears



- **損失**：專利文件、財務資訊、3D 設計模型、測試研發結果外洩。
- **影響**：涉及長期競爭優勢與智慧財產風險。

南光製藥 vs. INC Ransom



- **損失**：駭客宣稱取得 430GB 內部資料，給予 4 週談判期限。
- **影響**：重大訊息發布，啟動緊急應變。

社會風險：當信任與生命安全受到威脅

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

某醫院 (vs. Meduza Locker)

勒索 7 萬美元。出現於暗網後 3 天即消失（暗示私下談判成功或已支付贖金）。

國際物流 (vs. The Gentlemen)

影響跨國貿易與運輸運作，供應鏈核心節點受創。

圓山大飯店

主動通報，請求調查局介入。面對公眾信任危機。

Insight：攻擊目的轉向「營運中斷」— 越不能停機，就越可能付贖。

攻擊工業化：你被鎖定不是因為有名，而是因為有漏洞

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

現代攻擊組織運作像科技公司，而非傳統駭客。

RaaS
(Ransomware-as-a-Service)
改變了遊戲規則。

結構性破口一：假期防禦設計不足

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

平日營運模型 (Current Model)	戰備模型 (Required Model)
- 設計針對一般上班時間	- 365 天 24 小時無休監控
- 依賴人工介入與審核	- 自動化阻斷機制
- 外包支援有延遲	- 預先授權的緊急應變

Insight：攻擊者沒有假期。SOC 若無持續監控能力，假期就是風險真空期。

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

結構性破口二：補丁與資產治理落後

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

許多成功入侵的根本原因，在於資產盤點與弱點管理的落差。

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

結構性破口三：資安仍被視為成本，而非風險治理

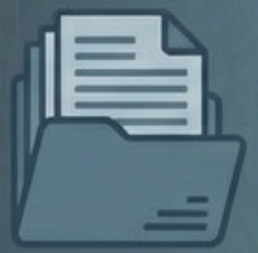
THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

資安不是 IT 問題，而是董事會層級的風險問題。

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

目標轉移：從竊取資料轉向癱瘓營運

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES



單純資料竊取

癱瘓營運
(Operational Paralysis)

「越不能停機的產業，就越是勒索軟體的完美目標。」

Attackers know that downtime costs > ransom costs.

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

常態被攻擊時代已經來臨

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

~~會不會被打？ (Will I get hit?)~~

什麼時候被打？ (When will I get hit?)

台灣企業已全面進入此階段。 韌性 (Resilience) 是唯一的生存策略。

建立韌性：不靠運氣，靠準備

THREAT ASSESSMENT DOSSIER // CLASSIFICATION: HIGH-STAKES

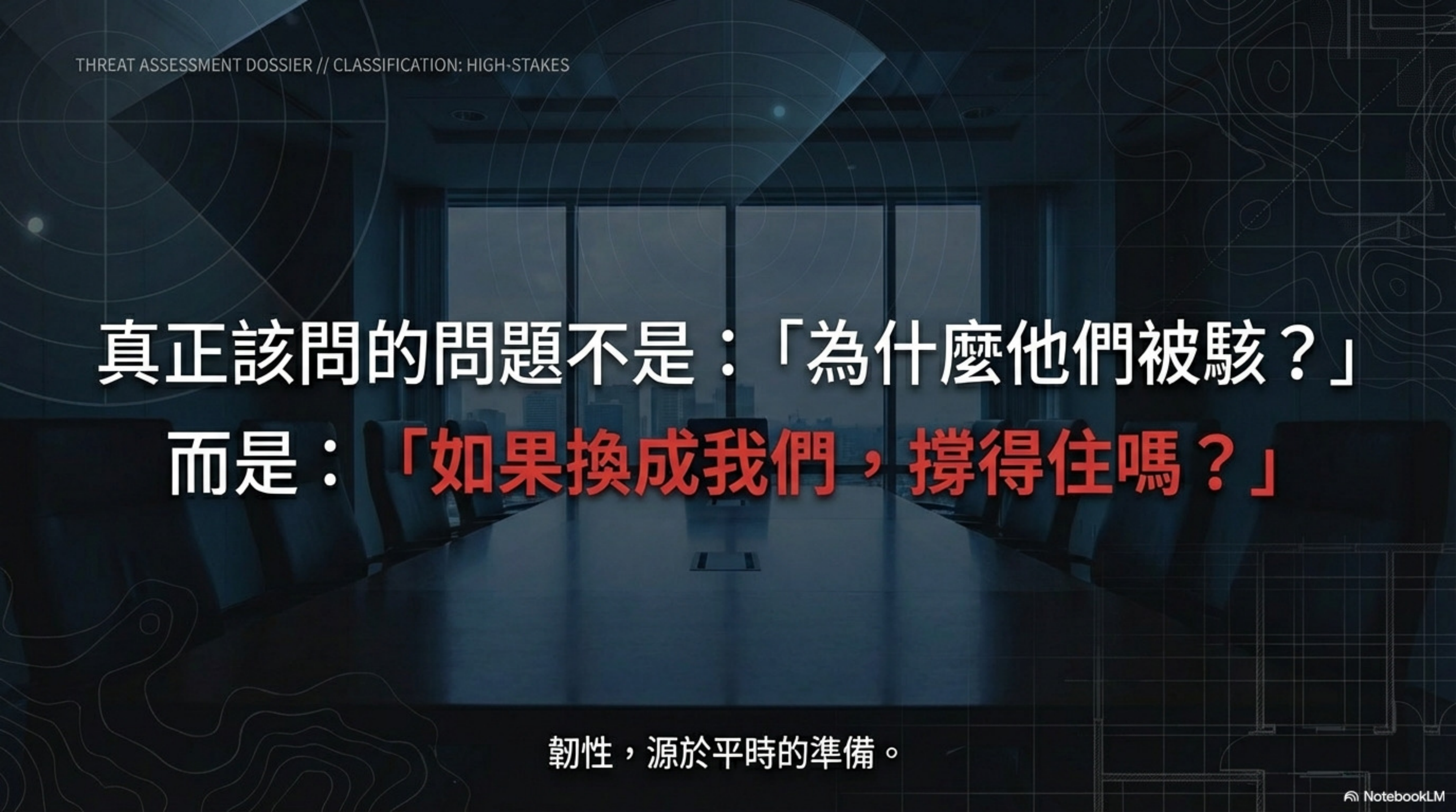
01. 持續監控
(No holiday gaps)

02. 即時應變
(Pre-approved authority)

03. 實戰演練
(Drills)

04. 風險意識
(Board visibility)

目標：從 Cybersecurity 轉向 Operational **Resilience** (營運韌性)



韌性，源於平時的準備。

資料來源與參考

- Primary Source: Holiday Attack Pattern（假期攻擊模式）：年假無防線？從圓山大飯店到南光製藥 (2026/02/25)
- Intelligence Provider: 竣盟科技 BLab 情資 (Billows Technology BLab)
- Disclaimer: Analysis based on publicly available data and threat intelligence reports as of Feb 2026.

Data Integrity: Verified & Cross-Referenced