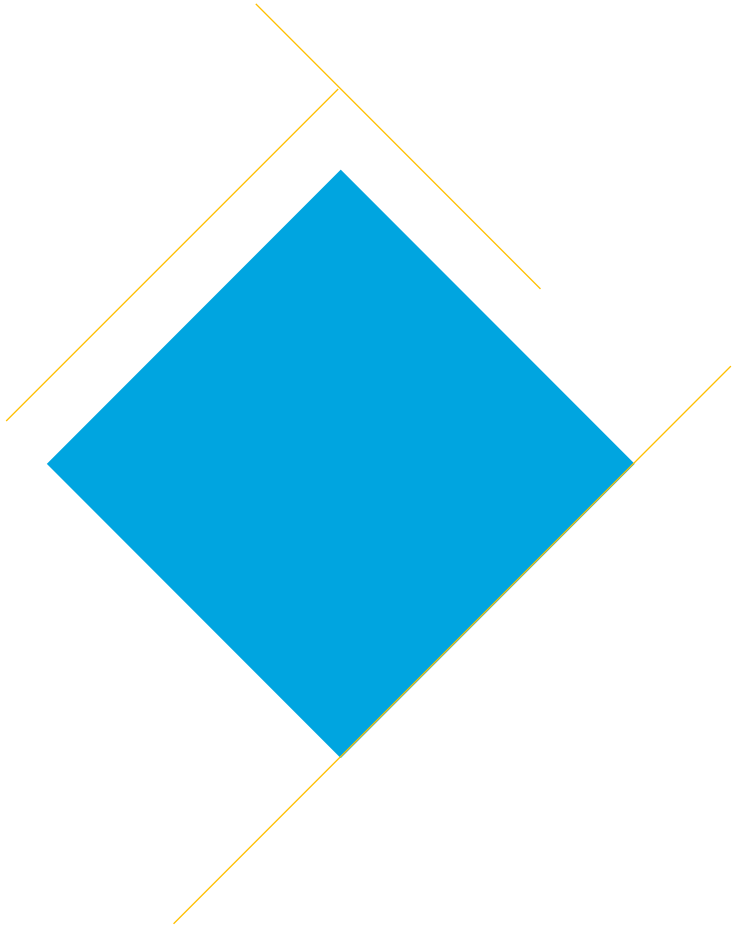
CKmates
銓鍇國際股份有限公司
Provide all you need

數位轉型過程不可忽視的資安隱憂與檢測工具

產品經理 樊博文

Jul/14, 2021



數位轉型趨勢與網路威脅

資訊安全檢測服務介紹

資訊安全防護服務介紹

總結

資訊安全檢測服務

Let's Go Cloud

COVID-19疫情帶動數位轉型趨勢

CKmates
Provide all you need

數位轉型工具普及且多元化 使用成本急遽下降

履歷紀錄與通路

AI生產管理

美中貿易戰及COVID-19造成邊境鎖國，使得製造業零組件替代性不足與斷鏈，數位營運需求提升

- 供應鏈自中國大陸出走異地備援成主流
- 分散式生產供應鏈模式，技術分流降低風險
- 分散式製造壓力劇增區域產業生態競爭
- AI智慧化排程、預測生產交期，降低庫存

數位原生世代正在主導消費市場轉變

28.6%

千禧(Y)世代

1981-1994年出生

- 56%善用數位工具
- 41%無市內電話
- 80%將行動電話放在床邊

數位轉型是企業面對市場趨勢及消費人口喜好變遷的必然壓力。千禧(Y)世代與Z世代躍居國內外民生消費市場的主力，現有市場結構已經或正在被快速顛覆

COVID-19改變社會與經濟型態，強調低度接觸互動、安全服務模式，帶動數位服務新商機

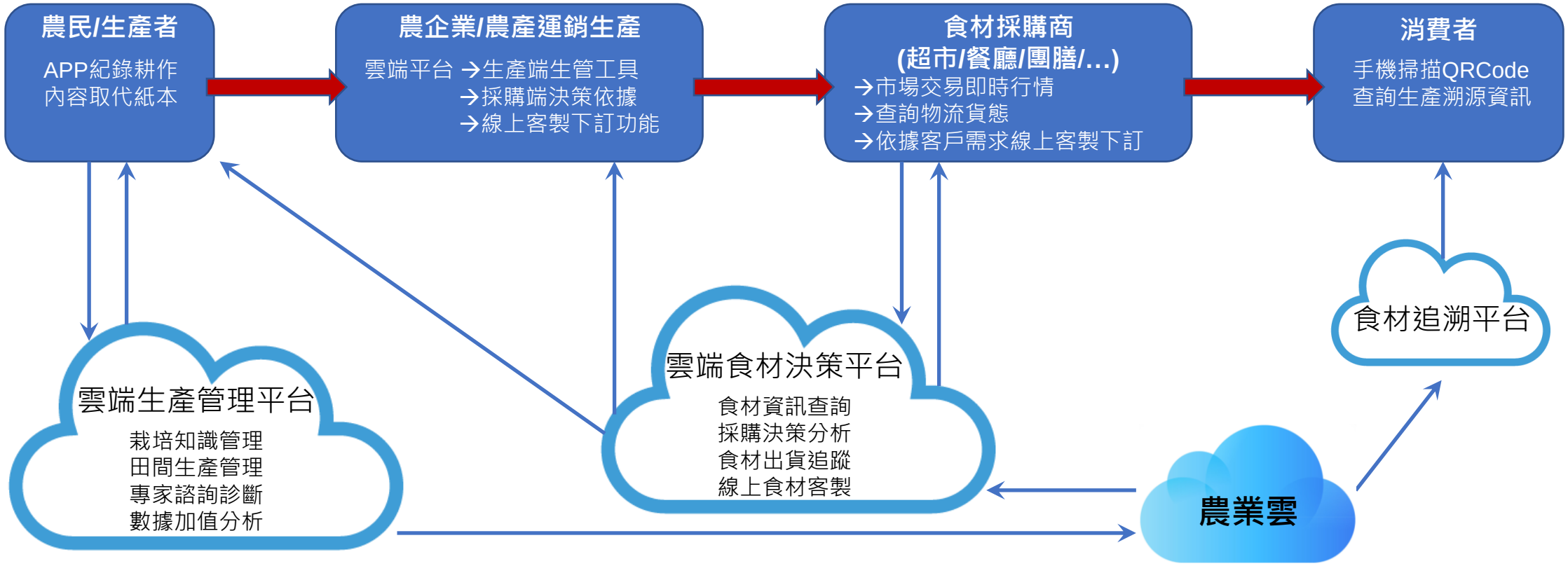
- 低接觸使得電商更蓬勃線上銷售已成必備條件
- 餐飲外送已成消費常態低接觸服務模式興起
- 手機及雲端服務逐漸普及，導入成本下降
- 遠距工作/育樂/策展線上與線下互動體驗

手機訂購服務

蔬菜箱外送

資料來源: 經濟部中小企業處

數位產業鏈正在形成


農民/生產者
APP紀錄耕作
內容取代紙本
農企業/農產運銷生產
雲端平台 →生產端生管工具
→採購端決策依據
→線上客製下訂功能
食材採購商
(超市/餐廳/團膳/...)
→市場交易即時行情
→查詢物流貨態
→依據客戶需求線上客製下訂
消費者
手機掃描QRCode
查詢生產溯源資訊
雲端生產管理平台
栽培知識管理
田間生產管理
專家諮詢診斷
數據加值分析
雲端食材決策平台
食材資訊查詢
採購決策分析
食材出貨追蹤
線上食材客製
食材追溯平台
農業雲

Let's Go Cloud

但是網路威脅依舊形影不離

CKmates
Provide all you need

透過勒索病毒獲利的模式，仍將是網路犯罪的主流，而其他型態的數位勒索也將進一步發展。

居家辦公成駭客攻擊破口 台灣網路攻擊量單月增17%

劉季清／台北報導 2021.06.10

COVID-19疫情下 歐洲嚴重網路攻擊事件翻倍

2021/6/10 18:27

2021.04.27 | 資訊安全

電子五哥屢屢遭資安威脅！證交所要求未來企業遭駭客勒索需發佈重大訊息

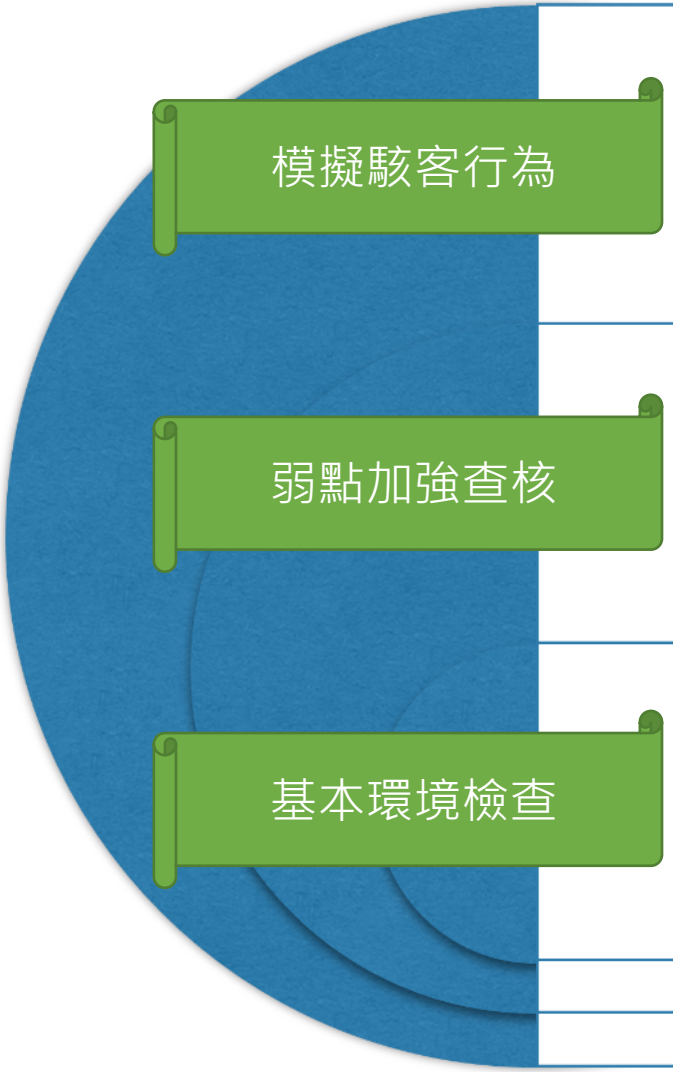
駭客攻擊事件層出不窮！廣達驚傳遭REvil竊取產品藍圖及個資，要求支付5000萬美元贖金，若超過期限將改1億美元，由於廣達不從，駭客轉呼籲蘋果支付。

資訊安全檢測服務

Let's Go Cloud

資訊安全檢測服務項目

CKmates
Provide all you need



滲透測試

- 根據弱點掃描結果，對主機的弱點進行模擬攻擊行為，確認該弱點的有效性與影響範圍
- 建議每年對重要系統至少執行一次滲透測試

進階弱點掃描

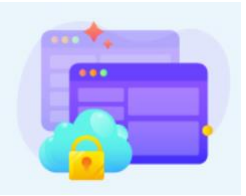
- 為基礎弱點掃描的延伸，會根據其掃描結果加入人工檢測動作來進一步判斷，以減少誤判
- 建議每一季的基礎弱點掃描可提升為進階掃描

基礎弱點掃描

- 使用自動工具進行檢測一般常見弱點，例如：未上Patch的軟體、弱密碼認證和設定錯誤等等項目
- 建議每月執行一次，其結果可用於趨勢分析、偵測網路上的新增設備，以及發現新的弱點等等

什麼是弱點掃描?

- 弱點掃描是針對企業組織資訊系統的弱點，進行偵測、有效性評估，和判定影響程度的一連串過程。
- 藉由掃描工具取得弱點清單的檢測方式，企業可以藉此了解自己目前網路環境或系統上存在的弱點並加以修復，避免被有心人士利用。
- 由於弱點隨著時間演變，定期進行弱點掃描已成必要，許多資安標準如 ISO27001 也將定期弱點掃描列為必要檢查項目。
- 弱點掃描服務可分為：
  - 基礎弱點掃描服務: 使用自動化掃描工具檢測一般弱點，建議每月執行一次
  - 進階弱點掃描服務: 人工進行判讀與檢測相關弱點，降低誤判機率，建議每季執行一次



網頁弱點掃描

- 檢測常見弱點項目如SQL Injection、XSS等。
- 針對程式存取權限進行檢查（如：GET、PUT、DELETE）。
- 依據不同網頁程式碼如PHP、JSP、ASP等，進行相對應的弱點測試與檢查。
- 依循 OWASP Top 10 弱點檢測項目。

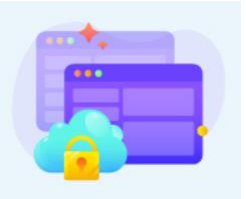
系統弱點掃描

- 針對作業系統、網路相關設備及一般通用軟體（如資料庫等）安全性問題進行檢測。
- 掃描所開啟的服務（Port），並進行弱點測試。
- 使用非侵入性的檢測方式（如阻斷服務）。

什麼是滲透測試?

- 滲透測試 (Penetration Test)，以駭客思維及手法模擬攻擊測試企業的網站、應用程式、設備等軟硬體，檢測企業設備之資訊系統和網路的安全性，主動分析可能導致系統漏洞的潛在弱點，並針對弱點進行實際驗證。
- 滲透測試可以達成 ：
  - 模擬大部分駭客的攻擊方式來檢測系統漏洞
  - 試圖找出大部分可被入侵的弱點
- 滲透測試不可以達成：
  - 在測試期間找出所有的潛在或未知的弱點
- 在現實環境下，我們會假設駭客有無限的時間來試圖攻破系統
- 建議每年執行一次滲透測試

主機滲透測試



網站滲透測試

APP滲透測試

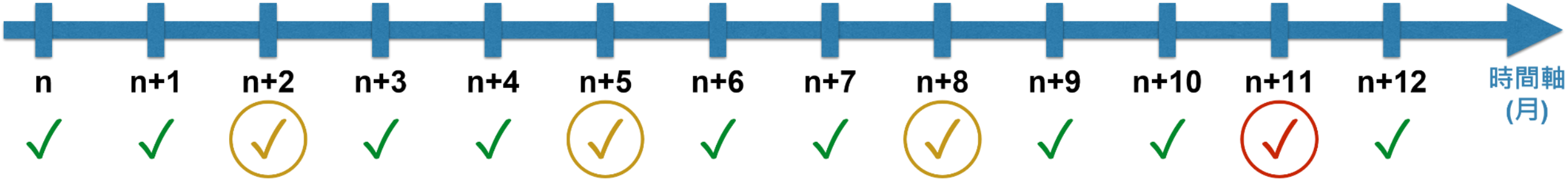
特殊滲透測試

業界資安測試標準

- OSSTMM
  - 參考公開標準OSSTMM（Open Source Security Testing Methodology Manual）框架進行測試步驟
- SANS Top 20 Internet Vulnerabilities
  - 參考SANS所列出的前20大資安嚴重弱點，範圍涵蓋Windows、Unix，及其他跨平台軟體和網路設備的弱點
- OWASP
  - OWASP(開放Web軟體安全計畫 - Open Web Application Security Project)是一個開放社群、非營利性組織，長期致力於改善網頁應用程式與網頁服務的安全性，本測試亦參考OWASP定期公布的前10大Web弱點

資訊安全檢測服務最佳實務

- ✓ 基礎弱點掃描建議每月執行
- ✓ 進階弱點掃描建議每季執行
- ✓ 滲透測試建議每年執行



資訊安全檢測服務效益

即時檢視

幫助企業審視主機系統、網路設備、企業網站等資訊資產所存在的弱點，再透過弱點掃描報告進行後續補強或其他改善方案。

安全評估

經由專業弱點掃描軟體與顧問經驗，幫助企業評估內部系統與網路安全，減少已知的漏洞攻擊機會。

優先修補

協助系統管理者在有限的時間與資源內優先修補高風險漏洞，增強防禦並保障資訊資產。

降低風險

透過顧問建議來協助組織修訂資訊安全政策，降低企業風險。

Let's Go Cloud

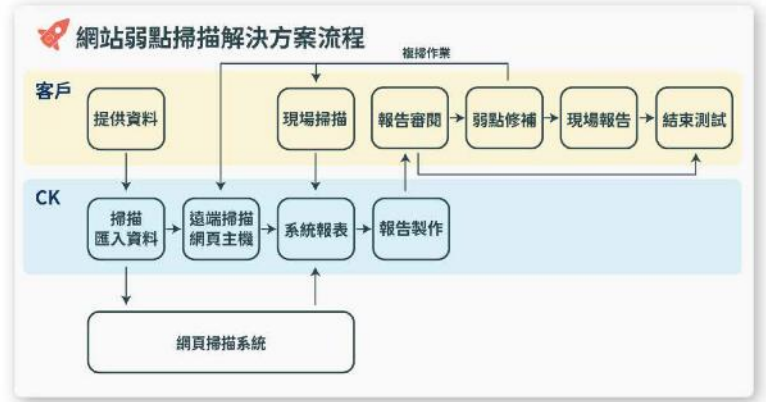
Successful Case – XX電商網站

CKmates Provide all you need

■ **專案資訊與需求:**

- 網站曾遭遇駭客爬蟲、注入攻擊，以及失效的身分認證等問題
- 規劃升級改寫網站程式，需要強化**網站服務安全性**，避免線上交易損失，專注業績發展
- 需要**檢查網頁弱點與程式存取權**並提出報告書給予建議

■ **本案相關圖表:**



解決方案

- 含單一URL，提供初掃與複掃 (驗證初掃弱點是否已修復)，含資安顧問服務、技術諮詢與協助修復弱點
- 量身打造合適的掃瞄政策並調整掃描政策

服務組合

資安顧問服務-網站弱點掃描解決方案

效益分析

- 改善網站安全弱點後，不再發生線上交易損失，業績成長20%

Let's Go Cloud

Successful Case – XX生科

CKmates
Provide all you need

■ **專案資訊與需求:**

- IT部門換血，公司內網建置設定保存不全，接手人員需要全面檢視防火牆、主機與應用程式，，進行**風險管控與弱點修補**
- 擔心駭客竊入公司主機綁架營運相關資料，需要**維護公司運營資產資料安全**，並能繼續聚焦企業發展，擴大運營規模

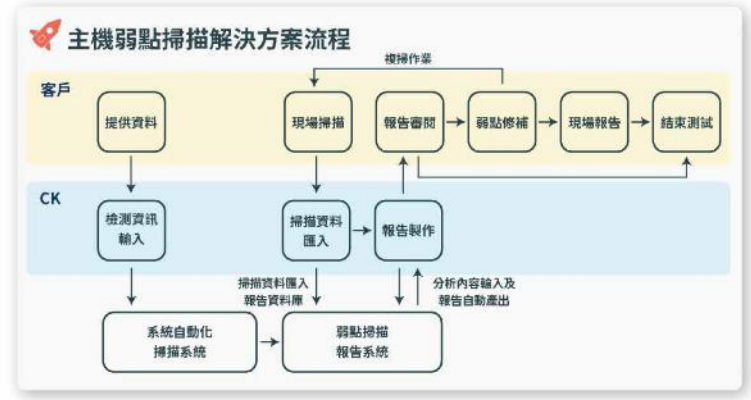
解決方案

- 同一個 Class C網段且IP在100個以內，提供初掃與複掃 (驗證初掃弱點是否已修復)，含資安顧問服務、技術諮詢與協助修復弱點
- 量身打造合適的掃瞄政策並調整掃描政策

服務組合

資安顧問服務-主機弱點掃描解決方案

■ **本案相關圖表:**



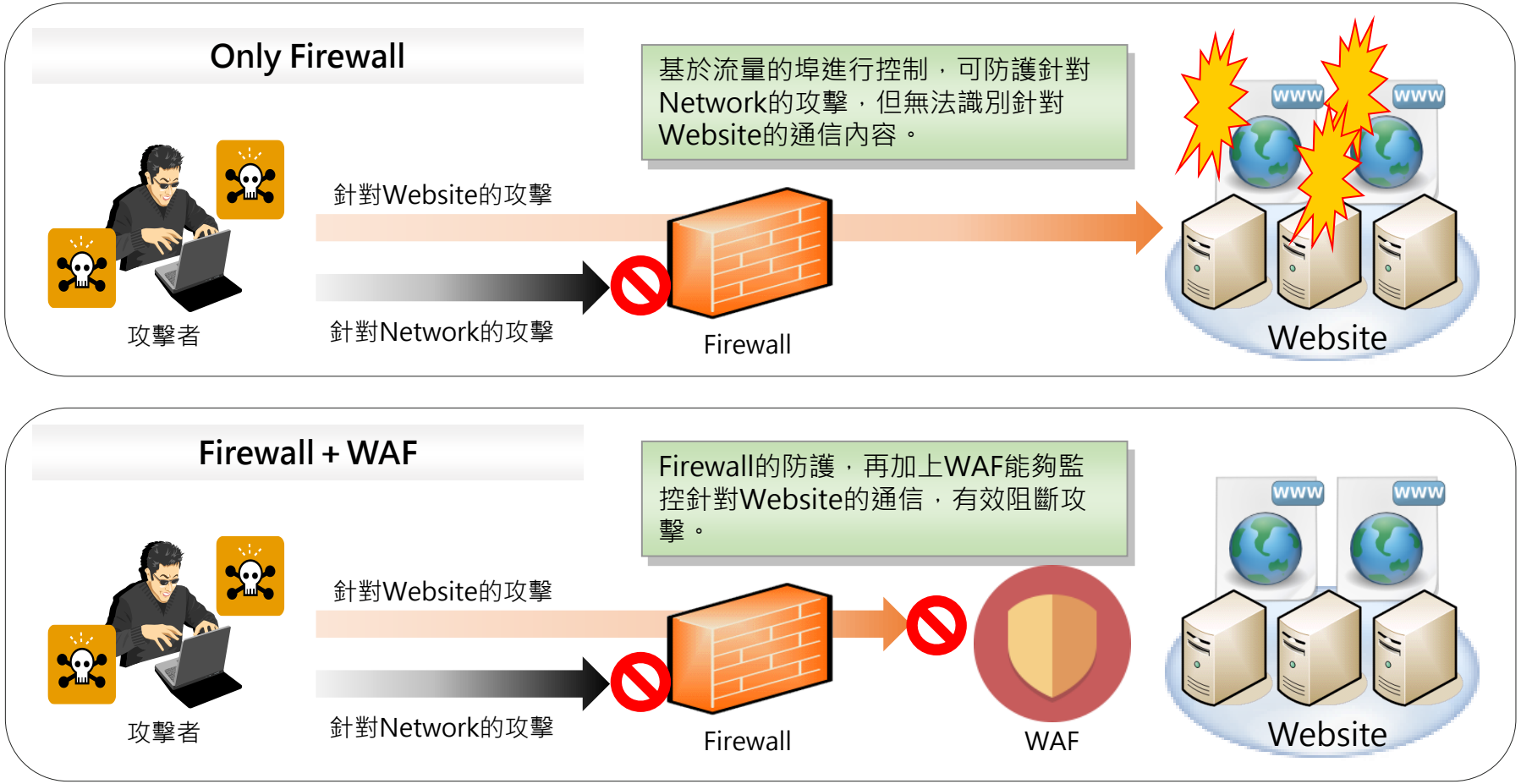
效益分析

- 公司內網經過弱點修補強化，無須換購硬體設備，節省預算新台幣100萬元
- IT人員大幅減少加班時數，節約5%人事支出成本

資訊安全防護服務

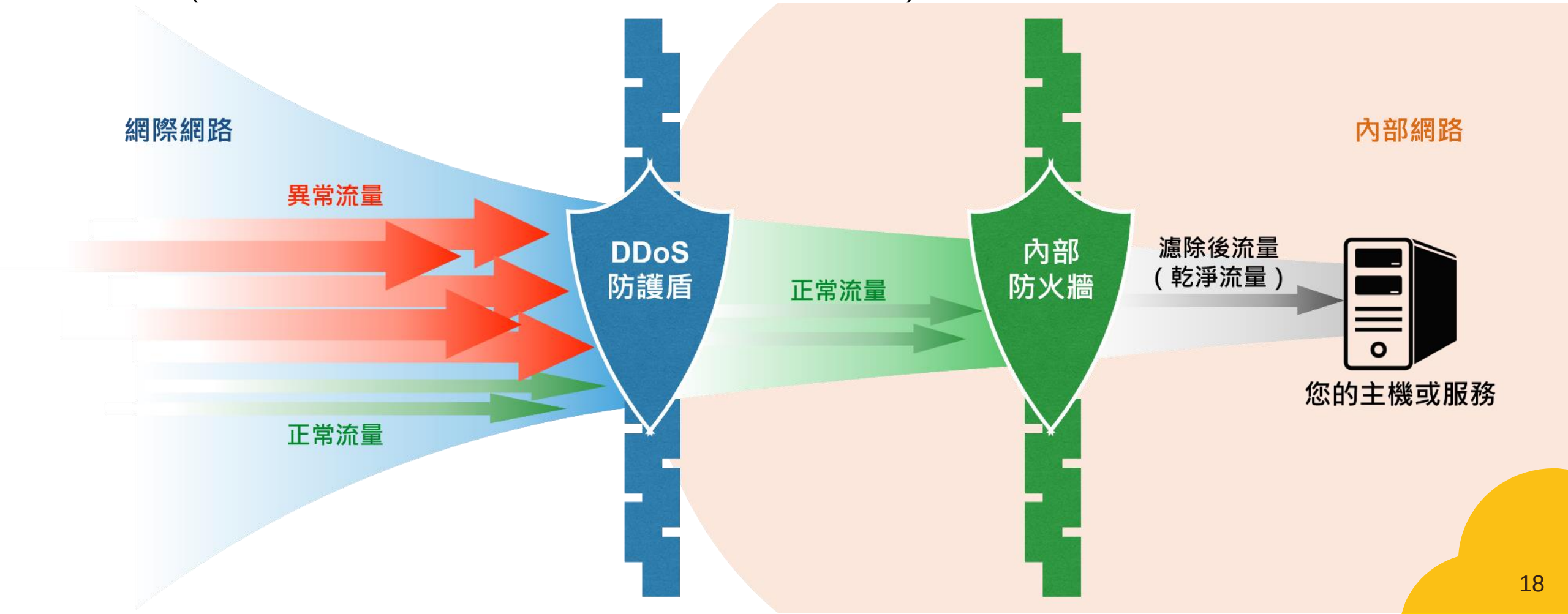
針對網站營運的防護服務

一般的Firewall防火牆設備都是基於流量的連接埠(L3/L4)進行控制管理（如只允許放行80/443 port）。
然而針對網站的非法入侵都是通過通信內容(L7)本身進行的攻擊行為，單靠Firewall防火牆設備無法達到防禦效果。
WAF（Web Application Firewall）為解決這一挑戰提供了很好的解決方案。



分散式拒絕服務(DDoS)流量清洗服務

阻斷服務攻擊(denial-of-service attack，簡稱DoS攻擊)亦稱洪水攻擊，是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。
當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時，稱為分散式阻斷服務攻擊(distributed denial-of-service attack，簡稱DDoS攻擊)。



總結

Let's Go Cloud

資安事件的潛在影響

CKmates
Provide all you need

資安事件的潛在成本


既有服務中斷導致股價遭受影響下滑。
營運中斷
商譽損失
因爆出新聞事件導致客戶要求改善，在改善稽核完成前停止合作。
高層下台
主官\管負起督導責任，黯然下台，承辦與相關人員亦被追查

鐵齒

不跳黃河心不死

不見棺材不掉淚

勿恃敵之不來
恃吾有以待之

LIKE US NOW!

Ckmates漫步雲端 facebook

THANK YOU