台灣大哥大
企業服務

EASM曝險評估

常見資安攻擊手法: 網路攻擊、帳號密碼洩露

在疫情後，隨著網路銷售的迅速興起，**網路攻擊**及**帳號密碼洩露**事件頻繁發生。此類洩漏可能引發個人信息被盜取及企業機密遭到泄露的風險，對公司的**財務、運營、信譽以及未來的安全性**構成重大威脅。企業需要快速便捷的系統自動化工具了解自身所面臨的資安風險。

缺乏簡易資安工具，能快速從網域了解自己的外部曝險

客戶痛點

- **網站數位足跡**數多 (駭客高機率攻擊的目標)。
- **帳號密碼**暴露將讓攻擊者可以精準鎖定目標，執行釣魚或直接滲透各項系統。
- **中大型企業：**釐清內部資安機制的完善程度 、 **中小企業：**資安預算不足。

客戶需求

- **快速**了解自身網域的外部曝險，進而循序漸進的改善
- 非人工作業的系統**自動化**檢測評估
- 資安技術性**合規量化指標**評級
- **顧問服務**提供詳盡的解決方案，協助企業快速鎖定修復目標

曝險評估EASM，能有效率地由外而內管理資安風險

- 資安曝險評估服務EASM 協助企業以簡單快速的方式，還原駭客視角檢驗企業在外的曝險程度，以**五大構面檢測項目**全自動部署全面檢視，只需輸入主**網域**名稱，**15分鐘**即可取得檢測報告

透過系統自動化15分鐘快速產出報告曝險等級

■ 報告提供技術性合規量化指標為資安評級，針對弱點細項提供線上顧問服務循序漸進的改善建議

五大檢測項目評級概觀

C

客戶 Client
OD 股份有限公司

受測日期 Date
2021 / Nov / 5

資安評級

系統性歸納由 MITRE 提出的 ATT&CK 資安框架及 NIAC 美國國家基礎建設諮詢委員會公開的 CVSS 通用漏洞評分系統，並根據即時風險情資調整評級權重，將各面向風險區間由高至低分為 A、B、C、D、F，5大級別

A B C D F

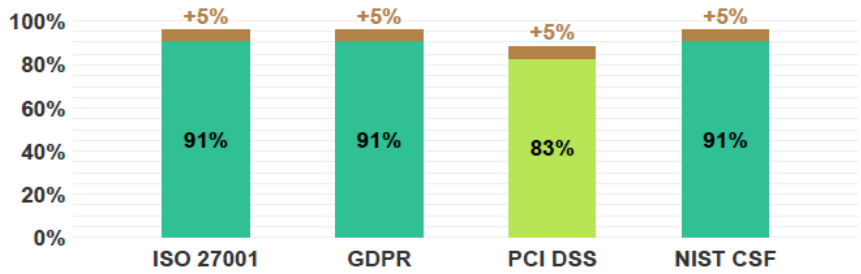
A+	網路服務	遠端控制	資料庫	應用服務	黑名單
B-	網站	網頁伺服器	網頁應用	憑證	網域
A-	電子郵件	郵件服務	DMARC	SPF	
C	帳號密碼	網路曝險			
A+	雲端安全	雲端儲存			

資安技術性合規量化指標

改善下列項目可提升資安評級及合規分數

C → C+

合規百分比



L M H

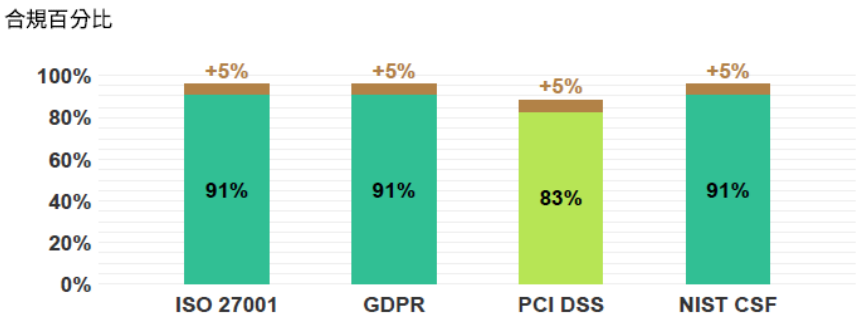
類別	子類別	項目	風險	複雜度
帳號密碼	網路曝險	帳密外洩	H	L

循序漸進的提升資安評級及合規分數

■ 針對弱點項目循序漸進的協助客戶提升資安評級分數達到A+及99%的合規量化指標

改善下列項目可提升資安評級及合規分數

C → C+

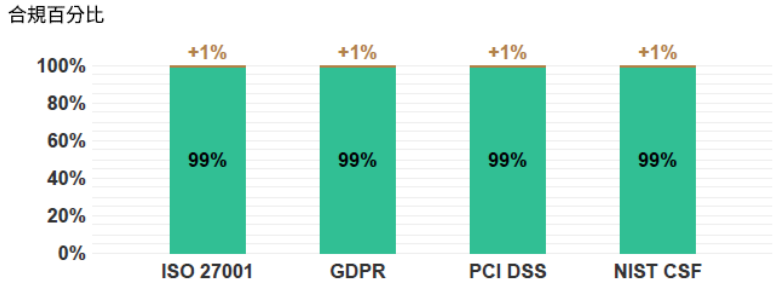


L M H

類別	子類別	項目	風險	複雜度
帳號密碼	網路曝險	帳密外洩	H	L

改善下列項目可提升資安評級及合規分數

B+ → A+



L M H

類別	子類別	項目	風險	複雜度
網站	憑證	LUCKY13	L	L
電子郵件	DMARC	DMARC 紀錄未採用最佳配置	L	L
網站	網域	相關的網域	L	H

輕量、彈性、非侵入性之資安檢測

- 以「**外部**」的角度，「**非侵入式**」檢測並不影響日常營運。
- 檢視企業的所有公開資訊以及數位足跡，可進一步瞭解**合作夥伴**、**同業**、**競爭對手**或**供應商**資安曝險及「**評級**」
- **快速**取得曝險評估報告

曝險評估-檢測標的

- 檢測標的為一個FQDN
- FQDN = Fully qualified domain name，又稱完全資格域名、完整網域名稱、絕對領域名稱、絕對域名。

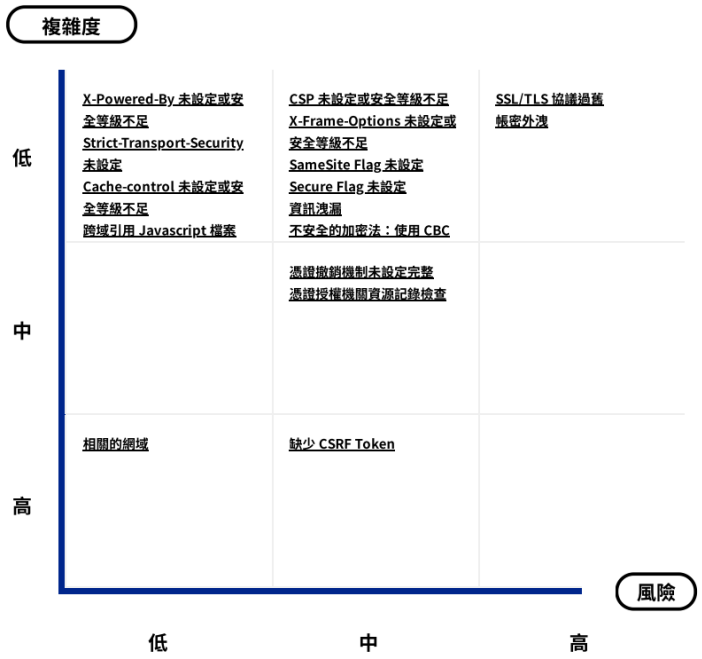
company.com.tw	這兩個網址都在「company.com.tw」下，會一同檢測。
company.com.tw/sitemap	
api.company.com.tw	前面多了「api」，指向到那台主機，視為獨立 FQDN。
company.com.hk	全新網址，獨立 FQDN。

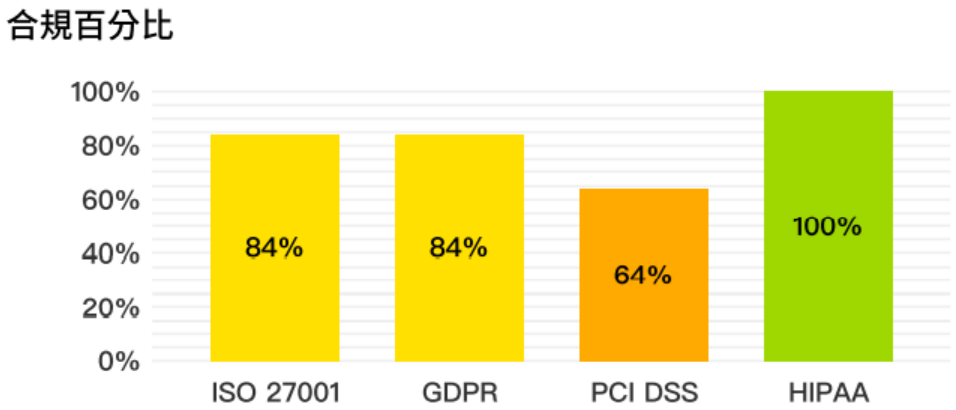
- 一句話解釋：“/”以後不同，都是包含在同一個檢測標的；“/”之前不同就算是不同的標的。

曝險評估五大檢測項目

網路服務 External Service	網站 Web Application	電子郵件 Email	帳號密碼 Credential	雲端安全 Cloud Security
遠端控制	網頁伺服器	郵件服務	網路曝險	雲端儲存
資料庫	網頁應用	DMARC		
應用服務	憑證	SPF		
黑名單	網域			

多維度資安曝險指標





子網域列表

1. api-uat.example.com
3. app-uat1.example.com
5. cva.example.com
7. mail.example.com
9. sso-uat.example.com
11. survey.example.com

資安評級提升象限圖

依風險、改善複雜度及自身資源綜合考量之改善指引。

合規百分比(技術面)

同時進行多個資安法規及標準的技術面合規管理。

外部資產盤點

可針對能透過外部存取之資訊資產執行評估，了解其可能存在之資安曝險。

曝險評估-評級概觀

客戶 Client
OD 股份有限公司

受測日期 Date
2021 / Nov / 5

資安評級

系統性歸納由 MITRE 提出的 ATT&CK 資安框架及 NIAC 美國國家基礎建設諮詢委員會公開的 CVSS 通用漏洞評分系統，並根據即時風險情資調整評級權重，將各面向風險區間由高至低分為 A、B、C、D、F，5大級別

A B C D F

A- 網路服務 External Service

- 遠端控制 Remote Control
- 資料庫 Database
- 應用服務 Remote Service
- 黑名單 Blacklist

- 建議參考曝險監控報告細節後，依據評級提升建議優先進行曝險改善。

B 網站 Web Application

- 網頁伺服器 Web Server
- 網頁應用 Web Application
- 憑證 Certificate
- 網域 Domain

- 建議參考曝險監控報告細節後，依據評級提升建議優先進行曝險改善。

B- 電子郵件 Email

- 郵件服務 Email Service
- DMARC Domain Authentication
- SPF Sender Policy Framework

- 建議參考曝險監控報告細節後，依據評級提升建議優先進行曝險改善。

C 帳號密碼 Credential

- 網路曝險 Credential Leakage

- 建議參考曝險監控報告細節後，依據評級提升建議優先進行曝險改善。

B 雲端安全 Cloud Security

- 雲端儲存 Cloud Storage

- 建議參考曝險監控報告細節後，依據評級提升建議優先進行曝險改善。

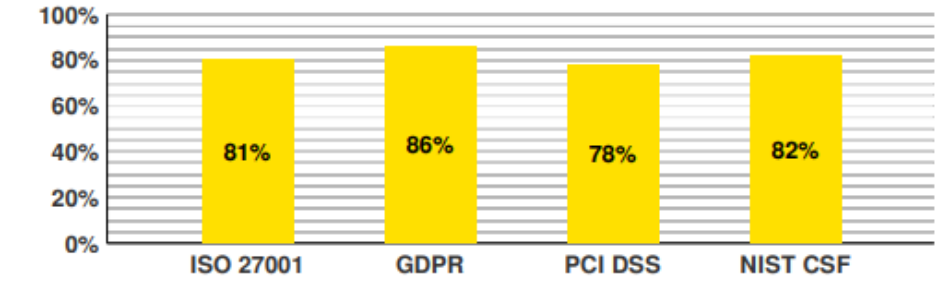
評級	A	B	C	D	F
對外資訊揭露	極度有限的資訊揭露	少數揭露的資訊可能被利用於攻擊	具有可被利用於攻擊的資訊	具有明顯可被利用於攻擊的資訊	大量明顯可被利用於攻擊的資訊
駭客攻擊動機	幾乎不會引發攻擊動機	低機率引發攻擊動機	有可能引發攻擊動機	高機率引發攻擊動機	極高機率引發攻擊動機
攻擊成功機率	攻擊很難成功	攻擊成功機率低	攻擊有可能會成功	攻擊通常會成功	極高機率會攻擊成功

曝險評評估報告

改善下列項目可提升資安評級及合規分數

C → B-

合規百分比



L M H

類別	子類別	項目	風險	複雜度
電子郵件	DMARC	沒有 DMARC 紀錄	H	M

H 電子郵件 | DMARC | 沒有 DMARC 紀錄

未找到 DMARC 紀錄。DMARC 紀錄是一筆 DNS 文字（TXT）記錄，幫助讓發信端和收信端雙方可確認對方身分，可用於防止詐騙和網路釣魚。DMARC 會指示收信方對於驗證失敗的信件該如何處理，此一政策有效的設定值包含：

- None：不採取任何行為
- Quarantine：隔離（不同伺服器行為不同，可能是集中到隔離中心、或是進入使用者垃圾信夾）
- Reject：拒絕，在 SMTP 傳輸層直接捨棄

DMARC 也可以設定回報用的電子信箱，幫助寄信者了解收信狀況。

M 改善建議

為避免此風險，建議參照以下準則：

- 請為您的網域設定 DMARC 紀錄（必須先設置 SPF 與 DKIM），詳細步驟請依照您的郵件系統來決定。

修改與配置方式請參考：

- DMARC 紀錄產生工具 : https://app.dmarcanalyzer.com/dns/dmarc
- Gsuite : https://support.google.com/a/answer/2466580?hl=en
- O365 : https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide
- SendGrid : https://sendgrid.com/docs/ui/sending-email/how-to-implement-dmarc/

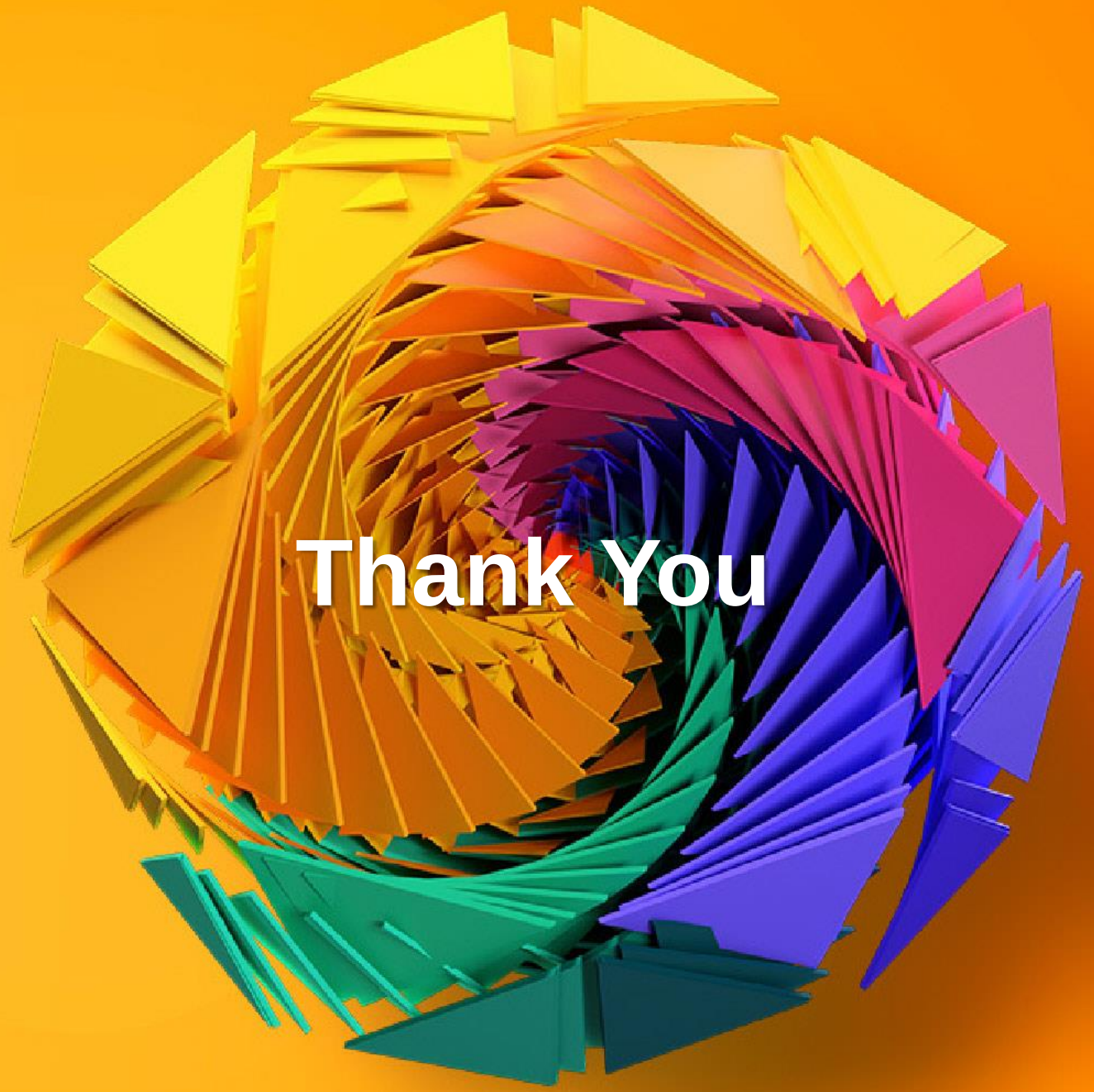
TWM曝險評估優勢

- **100+非侵入檢測項，還原駭客視角**
  - 納入亞洲/台灣常見攻擊手法(e.g. 偽冒信件)
- **輕量高效率檢測、不影響日常作業**
  - Good for Cyber Starter
- **評級提升優續指引**
  - 符合企業成本效益之漸進式修補建議
- **提供合規量化指標**
  - 提供ISO27001, PCI DSS, NIST CSF, GDPR 等技術性合規量化指標
- **延伸企業資安服務**
  - 協助企業持續優化資安場域
- **可綁定企業訂閱服務**
  - 首家電信公司推出EASM曝險訂閱方案

EASM曝險評估與他牌比較

項次	功能	TWM EASM	S業者	B業者	P業者	比較說明
1	檢測報告英文+繁中	V	V	X (英文)	X(英文)	TWM檢測報告原生撰寫繁體中文，易讀易懂
2	檢測周期	預計1-3個工作天	約一周	約一周	約一周	
3	原廠團隊	台灣	美國	美國	美國	從業務、行銷，產品、開發、售後服務較有優勢
4	銷售方式	一次性、月租型 訂閱制	網域數量計價	網域數量計價	第三方風險管理	因應新型詐騙型態持續更新
5	網域數量限制	不限制網域	限制網域	限制網域	限制網域	TWM無網域數量的限制
6	產品銷售含有顧問服務	V	X	X	X	TWM產品銷售含有顧問服務

台灣大哥大
企業服務



Thank You

曝險評估五大檢測項目(補充說明)

測項	說明
網路安全	**遠端控制**：是否有公開對外的遠端控制服務，確認該服務是否有入侵之可能性。 **資料庫**：是否有公開對外的資料庫服務，確認該資料庫是否具備已知漏洞。 **應用服務**：枚舉公司對外所有的應用服務，確認公司攻擊表面所存在之弱點。 **黑名單**：檢視暗網情資，了解自身是否因防護疏失，而已被列為惡意攻擊跳板黑名單。
網站安全	**網頁伺服器**：確認網頁伺服器所有未設置或安全等級不足之的安全性設置，並檢視該伺服器版本是否存在已知漏洞。 **網頁應用**：檢測不安全的標頭設定，避免用戶在與網站互動過程中敏感資訊之洩漏，及被偽冒請求的風險。 **憑證**：檢測憑證加密套件的安全性強度，確認網站是否使用到有漏洞之加密套件。 **網域**：列舉與公司相關的網域，了解是否存在會對公司造成影響的惡意網域。
電子郵件	**公開的對外郵件服務**：檢測公司是否有對外公開之郵件伺服器，避免該伺服因安全設置不完善造成資安破口。 **SPF**：檢測公司網域之 SPF 設定是否完善。SPF 設定主要確認郵件是否確實由公司所授權的伺服器發送，避免駭客假冒公司網域發釣魚信件給員工或客戶。 **DMARC**：檢測公司網域之 DMARC 設定是否完善。SPF 需搭配DMARC 設置能進一步強化收信方電子郵件閘道處理假冒電子郵件之能力，DMARC 也為 Gartner 2021 資安防禦十大重點之一。

曝險評估五大檢測項目(補充說明)

測項	說明
帳號密碼	**帳密外洩：**將公司帳號與知名資料庫進行比對。 **外部服務帳號：**檢測公司網域是否已註冊於常用之外部服務，有可能是駭客作為社交工程之攻擊準備，先使用公司網域註冊該等外部服務。 **暗網情資比對：**檢測公司網域是否於暗網中被提及，代表公司可能已有被開採之漏洞或機敏資料已被駭客於暗網中分享。
雲端安全	**公開的雲端儲存**：檢測企業是否有公開對外的雲端儲存體 (目前排名前幾名的資料外洩事件中，大多數的外洩管道即是透過公開的雲端儲存體，因此如何妥善管理好雲端儲存體，避免成為機密資訊外洩的管道，為雲端資安管理的重要課題之一。) **公開的公共程式庫**：檢測企業是否有公開對外的公共程式庫(公共程式庫中可能會存在組織內重要服務之程式碼、帳號密碼與歷史編輯紀錄，這些資訊都有機會被駭客進一步利用尋找漏洞並伺機攻擊公司。)