



數位發展部 數位產業署  
Administration for  
Digital Industries, moda

# 企業資安成熟度評級與企業資安外部曝險分析介紹

# 簡介

## 1

### 企業資安成熟度評級

- 資安評級：問卷題目參考CMMC及NIST SP-800-171國際資安標準，為臺灣國內第一套結合IT/OT的中文資安自評系統，協助企業**掌握公司內部的整體資安成熟度**

## 2

### 企業資安外部曝險分析

- 資安曝險分析：檢測「網路通訊埠安全、DNS健康狀況、IP地址信譽、網站服務安全」的風險分析工具，協助企業**掌握企業外部網路資產風險**

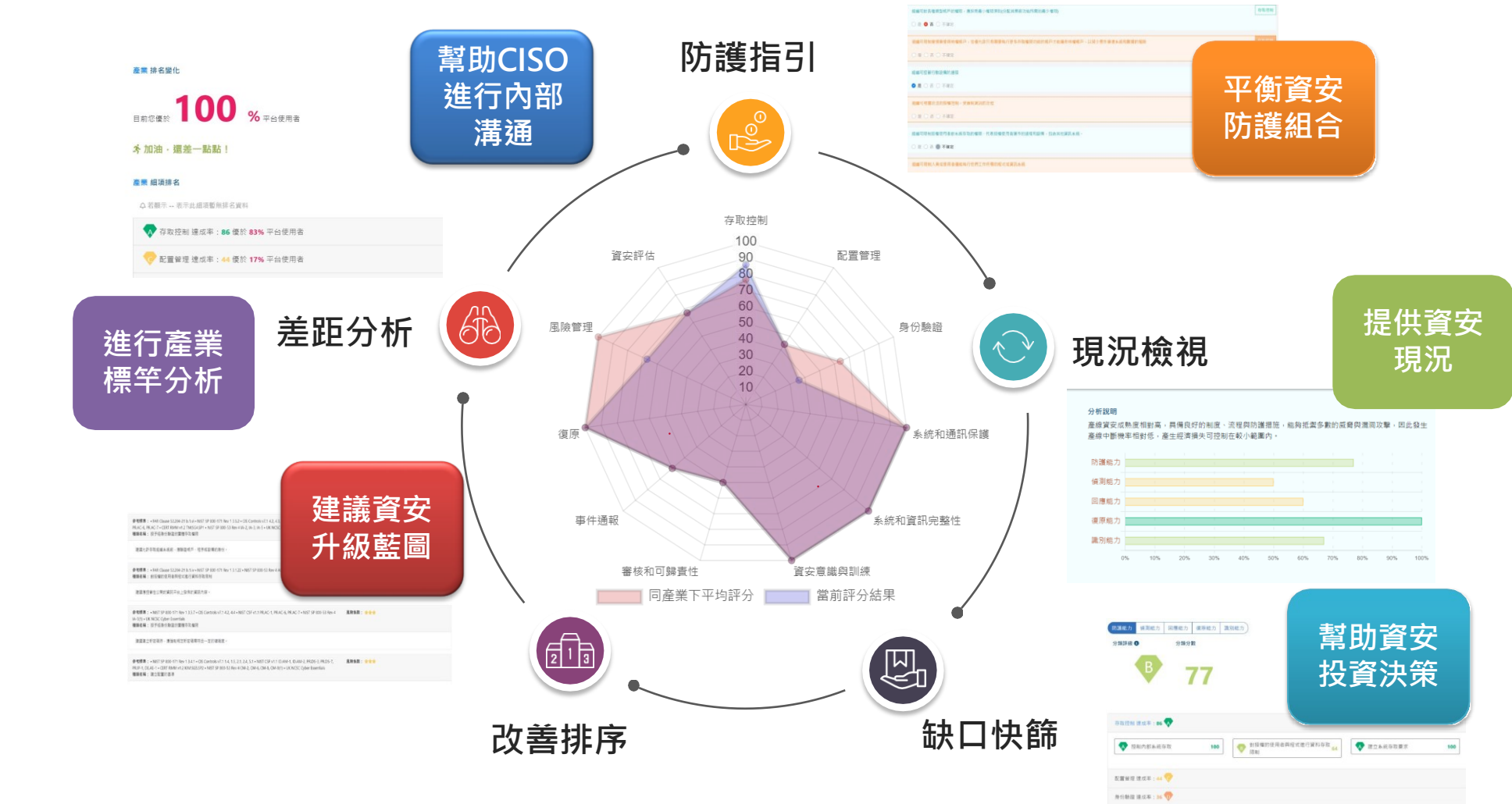
# 企業資安成熟度評級問卷

	完整版
題數	171
構面劃分	回應能力、防護能力、偵測能力、復原能力、識別能力
評級計算方式	絕對分數平均分級
加權總分	100
等級	A~E

# 五大構面細項與比重

辨識能力	防護能力	偵測能力	回應能力	復原能力
資產管理(1%)	存取控制(14%)	審核和可歸責性(8%)	事件通報(8%)	系統備份與復原(2%)
風險管理(7%)	資安意識與訓練(3%)	情境意識(2%)	8%	2%
資安評估(5%)	配置管理 (6%)	10%		
	身份驗證(6%)			
	資安維護(4%)			
	媒體防護(5%)			
	人員安全(1%)			
	實體保護(4%)			
	系統和通訊保護(16%)			
	系統和資訊完整性(8%)			
13%	67%			

# 五大功能快速掌握資安現況



# 評級結果與雷達圖

分數 / 總分

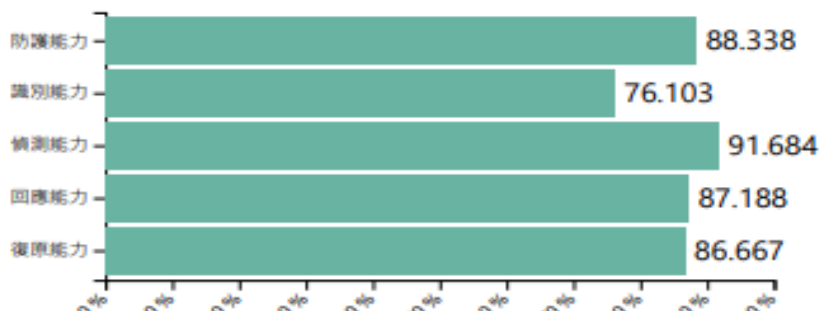
947.3/1086

加權分數

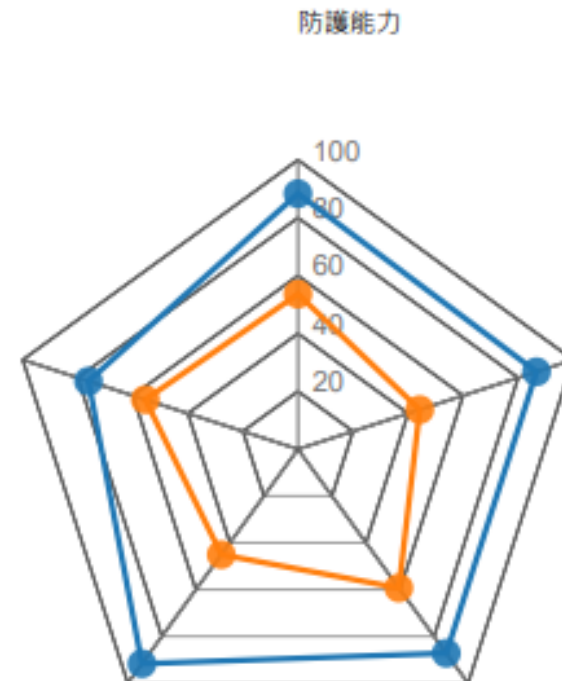
87.228

此次評級

B



識別能力



復原能力

偵測能力

回應能力

● 當前評分結果

● 同次進行測驗同業

參考標準：◇ CMMC modification of Draft NIST SP 800-171B 3.1.3e

◇ CIS Controls v7.1 12.1, 12.2, 13.1, 13.3, 14.1, 14.2, 14.5, 14.6, 14.7, 15.6, 15.10

◇ NIST CSF v1.1 ID.AM-3, PR.AC-5, PR.DS-5, PR.PT-4, DE.AE-1

◇ NIST SP 800-53 Rev 4 AC-4, AC-4(1), AC-4(6), AC-4(8), AC-4(12), AC-4(13), AC-4(15), AC-4(20)

種類名稱：控制內部系統存取

風險係數：⚠️⚠️⚠️⚠️

建議組織應該要控制資訊流，它涉及允許資訊在系統內和系統之間移動的位置。一般而言，資訊流控制主要在管理機敏資料授權和機敏資料未授權組件/系統之間流動，組織必須阻止機敏資料移動到未指定的儲存設備或未指定的可處理機敏資料的網域。

# 填答運作機制

## 工研院計畫辦公室

- ✓ 帳戶註冊、帳號開通、使用方式釋義或系統問題排除
- ✓ 媒合資安顧問與企業會員

## SECPAAS資安顧問

- ✓ 輔導企業會員完成資安評級 (輔導訪視紀錄)
- ✓ 產出評估報告

## 企業會員

- ✓ 獲得1對1顧問輔導  
使用評級分數作為計畫提案方向及改善基準
- ✓ 資安評級報告 (資安成熟度落差分析/常見資安不良實務說明/資安解決方案/流程改善建議)



數位發展部 數位產業署  
Administration for  
Digital Industries, moda

# 企業資安外部曝險分析介紹



# 資安曝險分析系統

## 企業外部資安曝險評估項目



網路通訊  
埠安全



DNS  
健康狀況



IP地址  
信譽



網站服務  
安全



應用程式  
安全



端點安全



修補升級  
作業效率



資料外洩  
狀況



威脅情資  
整合



被社交工  
程可能性

### 主/被動式掃描模組

透過**掃描**評估企業的網路資產安全狀況，從通訊埠、網站到應用程式，確定可能的風險點，並**依據評估結果給予風險評分**。

### 合規檢測模組

確認網路資產是否**符合規範**，同時評估企業對新威脅的響應速度和**升級效率**。

### 情資蒐集模組

整合多方**威脅情報來源**，從公開資料進行分析，評估企業可能面對的威脅與風險，特別關注駭客的目標與關切度，**助企業提前預防潛在攻擊**。

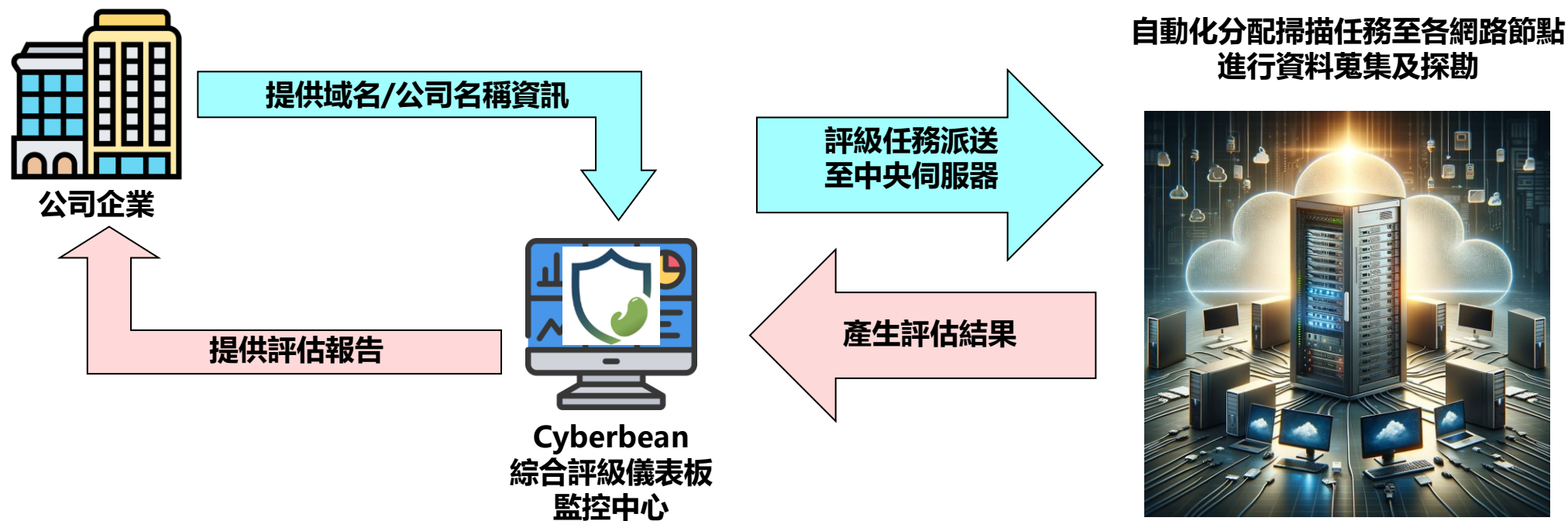
自動化評估流程搭配資料精準篩選產生視覺化報告

# 資安曝險分析項目

	項目	功能說明
	<b>網路通訊埠安全</b> (Network Security)	<p>檢測企業可能存在的邊緣網路資產，並按照潛在風險等級給予該企業相應的積分，用以衡量其外部網路的整體安全性，協助企業加強其網路安全，從而有效降低資安風險。</p>
	<b>域名系統健康狀況評估</b> (DNS Health)	<p>提供DNS運行狀況檢查，包括DNS解析的可用性、DNS服務器的配置以及DNS安全強度等方面進行檢測，從中評估DNS的整體健康狀況，並根據安全性的​​高低給予積分。這個模組可幫助企業評估其DNS的安全強度，並提供改善建議，以提高企業的安全性</p>
	<b>IP地址信譽</b> (IP Reputation)	<p>檢測IP地址的聲譽，包含是否曾經發送垃圾郵件、參與過惡意活動或任何形式的可疑駭客行為，透過這些評估項目來評估IP地址的安全強度並給予積分。這些細節的檢測有助於評估IP地址在網絡上的信譽和風險等級，讓企業在選擇合作夥伴、限制網路訪問權限等方面有更全面的安全考量。</p>
	<b>網站服務安全</b> (Web Security)	<p>評估企業外部網站的安全性。透過檢測，可以發現網站可能存在的風險，並根據風險等級給予相應的積分。而在檢測的過程中，將確保不影響網站的正常營運。</p>

# 資安曝險分析服務申請

- 請至<https://cyberbean.app>註冊會員，俾利申請掃描服務



由Cyberbean平台所提供的企業外部網路資產資安曝險分析為一訂閱型之SaaS服務模式

# 資安曝險分析報告範例(1/4)

上次掃描時間：2023-08-10

網站服務安全評估

75 / 100



已發現 4 處高風險

IP地址信譽

93 / 100



已發現 0 處IP信譽問題

網路通訊埠安全

95 / 100



已發現 0 處CVE驗證待確認

域名系統健康狀況評估

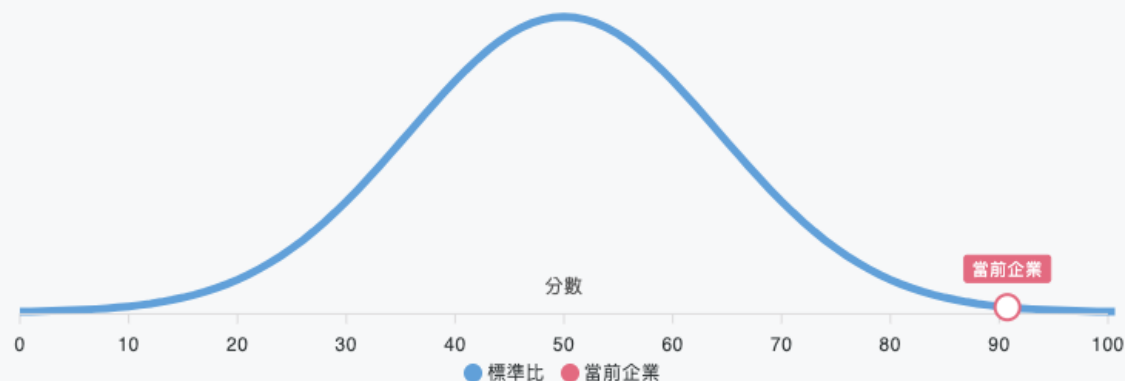
100 / 100



已發現 2 處DNS配置異常

當前企業評級排名：110

(因目前使用者眾多，排名更動會較頻繁)



# 資安曝險分析報告範例(2/4)



## 資安曝險分析報告

公司域名：[REDACTED]  
 報告產出日：2023年09月08日  
 Prepared：財團法人工業技術研究院  
 By：  
 執行單位：資通系統與資訊安全組 資安攻防技術部  
 F200

### 評級服務聲明

本探悉評級報告之內容，僅針對分佈式節點掃描過程所發現之網路資產，以資訊安全專業角度揭露資產下之網路應用、服務、開放通訊埠、域名系統（DNS）等潛在風險，礙於專案範圍和執行時程之限制，受測單位仍應持續留意與評估相關潛在之安全風險。

本份報告中各項補強建議之執行方式，需由受測單位自行評估適切改善方案，整體資訊環境之安全防護非由本次檢測工作所能涵蓋，若須進行進階資安驗證需洽詢專業資安團隊進行進階驗證。

### 評級結果

評級項目	目標值	當前值	通過與否
網站應用安全	90 (A)	85 (B)	No
IP 地址信譽	90 (A)	92 (A)	Yes
網路通訊埠安全	90 (A)	95 (A)	Yes
域名系統健康度	90 (A)	100(A)	Yes

### 網站應用安全

## Web Application Security

85 (B)

使用網站應用安全掃描器（Web Application Security Scanner），對目標網站進行無害的安全評估，掃描器會快速與網站建立正常連接，並自動化執行共**53**項非攻擊行為檢測，掃描可在數分鐘內完成，且不影響目標網站營運，以下結果將呈現目標網站面臨之風險，並提供細節報告及相關建議。

本次掃描的結果概要檢附在表 1，表 2 則統計了所有網站的各級風險數量，共找到**0**個高風險；**3**個中風險；**6**個低風險；**6**個資訊洩漏以及**0**個其他。最後，報告將依照找到的風險由高到低呈現風險的詳細資料以及擁有該風險的目標網站。

表 1 本次安全掃描風險統計

高風險	中風險	低風險	資訊洩漏	其他
0	3	6	6	0

# 資安曝險分析報告範例(3/4)



資安豆  
Cyber Bean

我的儀表版

Overview

Domains

工具箱

資安評級工具與服務

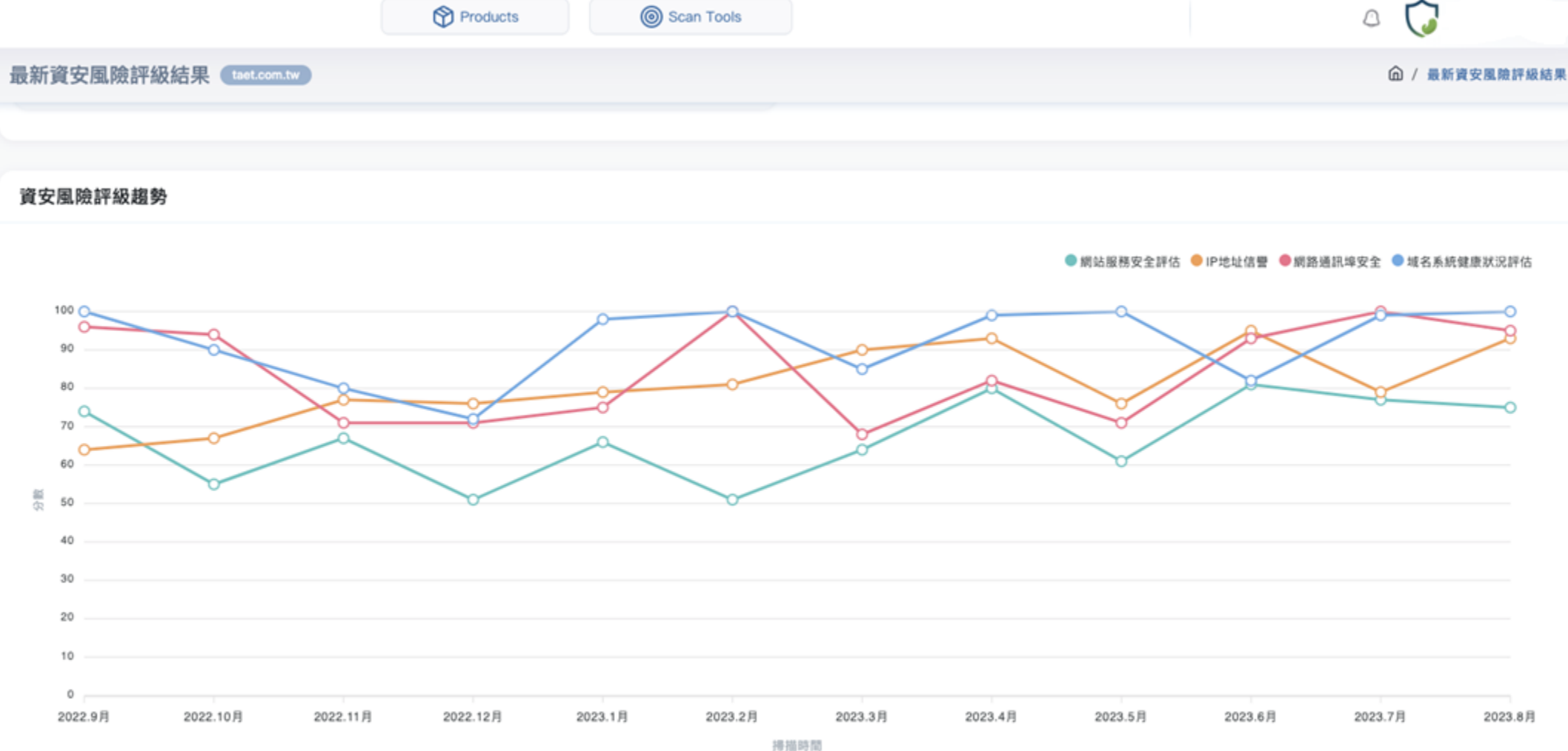
評級記錄簿

企業資安評級比較分析

報告下載(PDF)

資訊專區

最新訊息



# 資安曝險分析報告範例(4/4)

## 企業資安評級比較分析

🏠 / 企業資安評級比較分析

### 貴司目前在

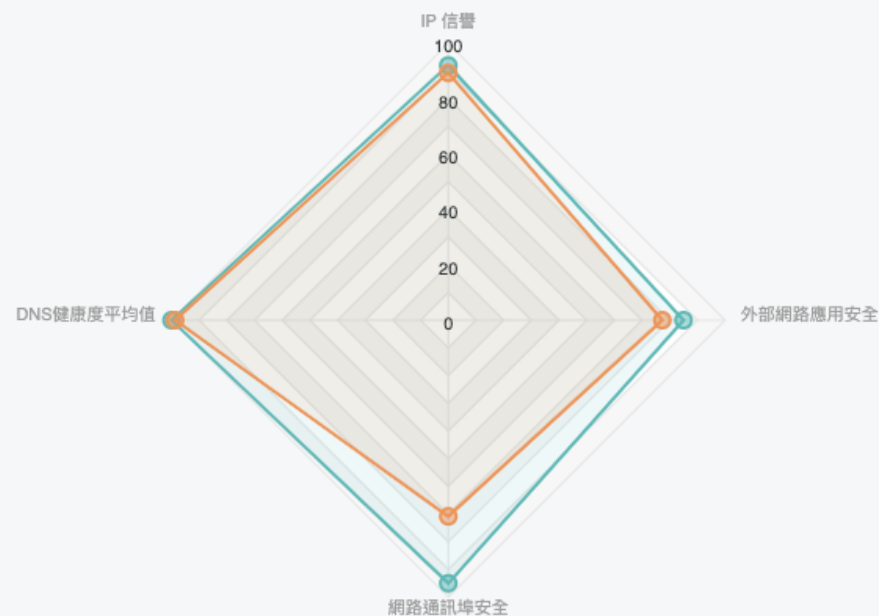
外部網路應用安全領域， **略高於** 於企業平均值  
 IP地址信譽領域， **等於** 於企業平均值  
 網路通訊埠安全領域， **高於** 於企業平均值  
 域名系統健康狀況評估領域， **等於** 於企業平均值

此次評測結果已經贏過 **87%** 的企業用戶！

目前在評級服務中總級分排行第 **6** 名

以下為貴司此次評級結果與當下企業平均值之比較：

● 此次評級結果 ● 企業資安評級平均值



感謝您的聆聽

Thank You



數位發展部 數位產業署  
Administration for  
Digital Industries, moda