資安眼

您知道企業外部資產、網站主機，存在多少對外暴露的威脅風險?

近日國際上重大的資安事件，造成實際上財物的損失往往都來自於金融資安詐騙或是偽冒合法的供應商交易；再偽造合法身分與誤導金流。供應商安全與企業自身的網站風險評估越發重要。

雖然傳統上都可以漏洞掃描評估外部網站或服務是否存有容易被駭侵的漏洞，但 APT 威脅都是下班或是假期時間，加上長時間的潛伏期，令企業難以防範。

國際知名的資訊顧問的公司 GARTNER 建議 ：

“隨著企業 IT 變得更加分散，需要新的工具來可視化組織攻擊面的管理並判斷改善的優先順序。安全和風險管理領導者可以從將資產和風險上下文聚合到一個平台，雖時間控與瞭解企業的外部攻擊面 “。

資安眼

提供整個企業網域暴露之弱點，以非侵入方式持續檢測，可選擇達三十天/ 年約。提供網域邊界清查、風險分數、弱點項目與潛在風險改善建議。只需要提供企業的網域(Domain)，就可以得到整個往育下所有數位資產的曝險評估結果。

產品說明

以非侵入性方式評估公司的外部網域攻擊面，自動執行了數百次測試來評估三個不同的層面，包含：網路資產(Network、IT)、網路應用(Application)、人為風險其中存在的弱點與攻擊層面，也會以風險分數與發現報告的方式呈現。

服務效益

此服務幫助企業識別網域邊界；自動識別企業位於網路上所有數位資產並標示風險。除了快速啟用的自動服務外，也能選擇由專人針對企業的網站安全提供諮詢建議，改善外部網站資安風險之現況。