AI SPAM AI垃圾郵件防護

日趨嚴重的電子郵件攻擊

在2022年12月，美國網路安全暨基礎設施安全局所做的研究顯示，每十間企業約有八間企業的員工會成為網路釣魚的受害者。這樣的數據顯示，大多數人對於資安、郵件其實沒有戒心，尤其現今電子郵件攻擊更多樣化，如：APT、BEC 等針對性攻擊，讓一般的使用者防不勝防。

在各樣的攻擊下，駭客執行「零時差攻擊(Zero day vulnerability)」時，在Virus Total 這類掃描病毒的網站中，偽造的釣魚網站或是附檔經常會被視為無害的。因為零時差攻擊中的網站與附檔仍處在未知的型態，使用者無法利用電腦內建的防毒軟體偵測出病毒檔案、有害網站，往往會導致嚴重的後果。眾至資訊推出AI SPAM 的垃圾郵件過濾機制，就可以將有害的郵件阻擋在外，避免進入使用者的信箱中，保護使用者的資訊安全。

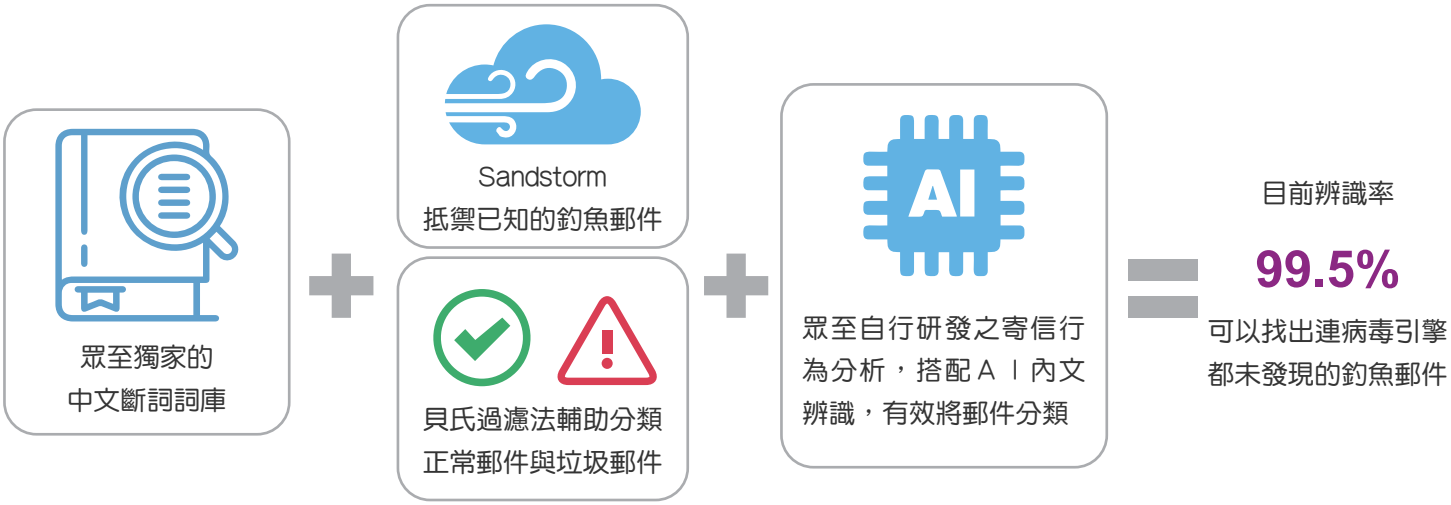
功能介紹

AI 語意分析

眾至資訊的AI SPAM將郵件主旨跟內文拆解，使用眾至資訊編修的中文斷詞資料庫。斷詞資料庫符合繁、簡體中文的使用習慣與用法，將郵件內容斷詞後進入AI 演算法分類。眾至的AI SPAM 資料庫有超過 100萬封以上的已分類郵件，資料庫中有五大分類，分別是：正常、通知型、電子報、垃圾跟釣魚郵件，AI 演算後會自動將新郵件歸類至五大類中。藉由郵件語意分類的輔助，將要求使用者「立刻」點擊郵件中網址或是開啟副檔的「零時差攻擊(Zero day vulnerability)」郵件阻擋在外。

內文過濾分析

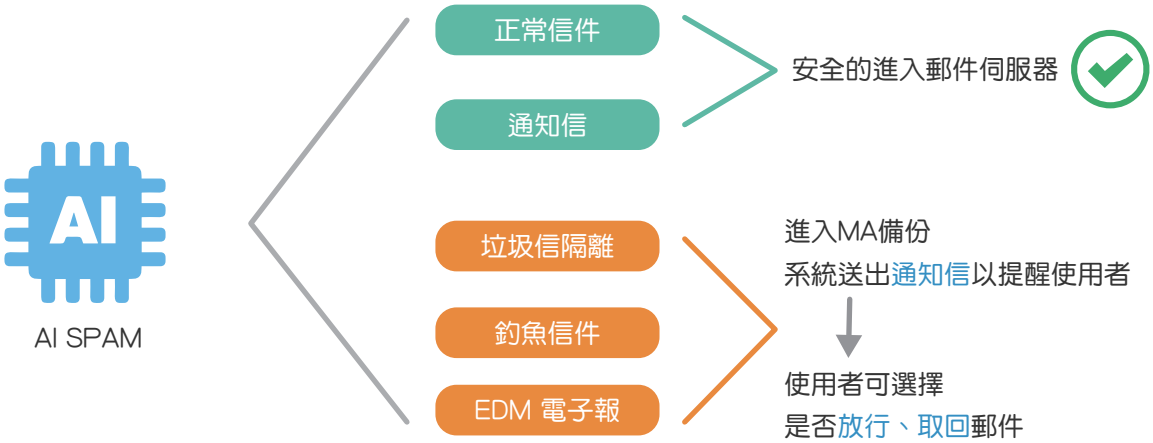
除了郵件意圖分類外，AI SPAM 系統會檢查內文中的URL連結跟附檔，是否包含已知的病毒跟危害的網址。透過眾至資訊Sandstorm 資料庫，阻隔已知的釣魚、木馬郵件，Sandstorm 中有超過100萬筆的木馬檔案跟200萬筆的釣魚網址。針對無法利用內文辨識出來的垃圾郵件，例如，短內文郵件、圖形文字郵件等，則用 BAYES 規則輔助判斷。



寄信行為分析

眾至資訊導入多種辨識方法降低誤判的機率。在 AI SPAM、Sandstorm 跟 BAYES 規則等以郵件內容為依據的第一層分類後，AI SPAM 系統再透過眾至資訊自行研發的寄件者行為分析機制，找出機器人電腦寄出、大量轉寄、非法轉寄、透過免費郵箱非法轉寄甚至是偽造網域等不合理的寄件者行為，同時，基礎的 SPF、DKIM 跟 DMARC 等寄件者網域查詢也會一併處理。

這些非正常管道寄出的郵件有一個特徵，他一定不會是正常往來的郵件，會被系統歸類為電子報、垃圾郵件，當使用者從通知信中再度確認寄件者跟郵件主旨安全無虞之後，可以從 AI SPAM 系統中取回。



功能特點

海量的中文斷詞詞庫

AI SPAM 的演算基礎就是繁、簡體中文斷詞資料庫，中文跟英文不一樣的地方是斷詞的精準度決定郵件意圖分析中的關鍵，例如：

我在交通大學的大學路上

斷詞決定了上述文字的語意分類，眾至資訊做的研究顯示，不斷詞跟斷詞後進入AI SPAM 的演算，準確度差距1-2%。這些微的差距，就呈現在最後郵件判斷的準確度上。藉由眾至資訊獨家建立的中文斷詞資料庫，讓 AI SPAM 在演算郵件分類上，更簡單跟準確。

AI SPAM 不斷精進

AI SPAM 判斷郵件內文意圖及寄件行為，區分正常跟惡意的郵件，降低使用者開啟釣魚郵件的機率，但是駭客攻擊的手法也是持續在進步，他們會把郵件偽造成跟真的郵件一樣，所以系統必須不斷的學習新的攻擊或是釣魚郵件，將這一些特徵都收錄在判斷資料庫或是演算邏輯中，AI SPAM 系統藉由不斷的自動學習機制，面對零時差攻擊的釣魚郵件時，能夠快速地做出判斷，讓郵件判斷的準確度高達 99.5%。