

# WELCOME TO SECURITY



新絲路科技股份有限公司  
New Silkera Network Corp.  
eEye Consultant Partner

## RETINA



## 弱點評估系統

**擁**擁有至少700種以上，隨時更新的弱點資料庫，而且是同類產品中，首次內建人工智慧機制，能從弱點資料庫中，加上駭客的思維，變化出更多的攻擊手法，探測管理者原本沒有料想到的弱點。

### 產品特色：

- 掃描各種網路弱點
- 圖形化操作介面
- CHAM獨家駭客探測
- Fix-it自動修復機能
- 定期稽核週期及政策範圍
- 人工智慧掃描判讀服務
- 智慧型稽核報表
- 模組及軟體自動更新
- 開放式架構可自訂模組

### 功能介紹：

- **弱點掃描**  
RETINA最主要的用途，是設計來識別與警告安全弱點、建議修補步驟、並統計在Internet、Intranet、Extranet環境內的網路安全漏洞，避免遭受到外界攻擊而造成損害。
- **圖形化介面**  
採用簡單易懂的圖形化介面，使用者不需預先了解各種弱點技術，只需One-click即可完成所有的弱點探測。探測完畢之後，也可以很輕易透過圖形化的顯示與操作，快速查詢各項結果的細節。
- **CHAM獨家技術**  
Common Hacking Attack Methods (簡稱CHAM) 技術，是唯一融合駭客思維的一種探測方式，CHAM擁有人工智慧的能力，來模擬駭客挖掘漏洞的程序及方法。透過這種獨家的CHAM技術，可以挖掘出市面上還沒有被發現的弱點。
- **定期稽核**  
系統弱點是會隨駭客的技術而增加的，因此管理者必須定期去檢查弱點是否增加。另一方面，透過定期稽核的功能，也可以了解系統風險程度的變化，讓決策者能調整安全預算，有效防止發生重大事故。RETINA可以指定時間週期，定期自動進行掃描作業，不需管理者以人工介入操作。
- **智慧型掃描**  
RETINA不僅僅依賴IETF所制定的通訊標準來掃描，內建的人工智慧模組，能自動判斷通訊埠真正執行的服務種類，選用正確的弱點資料庫進行掃描，避免因更換或自訂通訊埠，造成誤判以及稽核上的漏洞。
- **自動修復能力**  
為了方便管理者的修補作業，對於某些Windows平台的漏洞，RETINA可以提供自動修補的功能，例如：Registry、檔案權限等等，只要執行RETINA的主機有全網域的管理權，就可以從遠端去修補漏洞，讓管理者不需親自跑到每台電腦前面去個別設定。
- **智慧型報表**  
RETINA所產出的報表，可供決策者了解風險程度的變化，以及各種弱點的統計。也可以工程師知道弱點所在的位置，以及可行的修正方法。報表會提供豐富的資料，讓工程師了解應該如何進行修正，或該去何處下載修補軟體。
- **自動更新**  
RETINA可以隨時透過Internet，與eEye的安全中心取得聯繫，並自動下載最新的弱點資料庫，以保持稽核成果的有效性。管理者不需擔心忘了下載最新資料庫，而導致稽核的漏洞。
- **開放式架構**  
管理者可以自行撰寫弱點探測軟體，並加入RETINA的開放式架構中，成為控管項目的一部份。這個特色常用於探測自行開發的軟硬體，管理者不需等待外界的弱點資料庫出現，只要有能力自行探測，就可以對專屬的軟硬體進行稽核。

# VULNERABILITY IS OVER