3S資安檢測

ISSDU Security Subscription Service

System Vulnerability Security

防駭定檢

系統弱點是現今所有資安事件攻擊手段的開端

系統弱點是所有資安攻擊事件過程中最主要的威脅根源。不論是應用軟體、網路裝置、雲端平台等任何型態的系統，都存在著各式各樣的弱點。當系統弱點一旦被揭露曝光時，接隨而來將是駭客組織針對弱點開採進行犯罪攻擊的各式資安威脅；令人聞之色變的勒索病毒便是利用各式系統弱點橫掃全球。

近來最知名且破壞力最大的勒索病毒莫過於「WannaCry」，駭客利用存在於微軟系統的SMB弱點，快速且大範圍攻佔全球各產業的資訊系統，隨後演化出多個變種版本持續威脅著，而且結合社交工程郵件誘騙企業員工遭受感染。系統弱點造成危害不只是勒索病毒，也包括資料竊取、後門入侵、服務癱瘓、系統破壞等各種攻擊手法，根據2020年全球資安調查報告，企業組織所遭受的資安事件中有高達90%以上是肇因於系統弱點，其中主要為「弱點已知但修補改善不全」以及更多「未被檢出的最新弱點」，弱點在未能監控跟管理下，曾經受害企業遭到同種但變異的弱點威脅機率將近7成。

及早發現，提前預防 是斷開駭客攻擊鏈的最佳資安防護策略

系統弱點所涵蓋的系統類型不斷擴大，被發現的弱點數量成長暴增。國際資安弱點資料庫NIST的統計，2020年新增弱點數將從19000一躍突破超過20,000！單以微軟的修補程式日Patch Tuesday 發布最新的弱點資訊來看，平均每月弱點數量為100多項，有超過70%以上為重大及嚴重等級。駭客針對這些被公布的弱點製作各種惡意程式散布於地下網路，其中利用人性弱點的社交工程郵件發動攻擊是最有效果的一種，再嚴密的資安防護也擋不住人員的疏忽跟可利用的弱點，提升企業資安成熟度才是確保企業資安防護投資有效性的方法。

3S資安檢測服務 - 防駭定檢 針對企業用戶經常發生的資安風險層面所精心設計，提供訂閱用戶完整的資安檢測需求，可有效幫助企業預先於駭客發動資安攻擊鏈之前，提早做好防護準備。

3S資安訂閱服務
輕鬆、快速、零負擔

3S資安訂閱服務 是為企業用戶提供從資安產品安裝建置到資安防護維運等各層面都能滿足的資安訂閱服務，能夠真正有效協助企業用戶解決在資安防護議題上常面對到的煩惱與痛點！

3S資安訂閱服務提供的內容涵蓋有：

- **多樣化的資安解決方案（Solutions）**
- **月付訂閱模式（Subscription）**
- **資安託管服務（MSS）**

3S資安訂閱服務 因應現代企業數位化或數位轉型的資安防護提升需求，**將資安產品解決方案與專業資安服務能量相互結合，提供具備有 國際級、高規格、高效能，但卻「輕鬆負擔」的嶄新資安服務模式。**協助企業降低跨入數位轉型的資安門檻。

將**人（資安專家人才）、事（資安管理跟事件監控）、物（各種方案的資安防護系統）**做好配套，以一站式完整服務的模式提供給訂閱用戶，以滿足企業在使用資安解決方案時，所需要的日常維運服務與專業諮詢。同時將數聯資安團隊豐沛的資安專業能量與訂閱用戶共享，讓訂閱用戶都能享有與大型企業級別可比擬的專業資安服務。

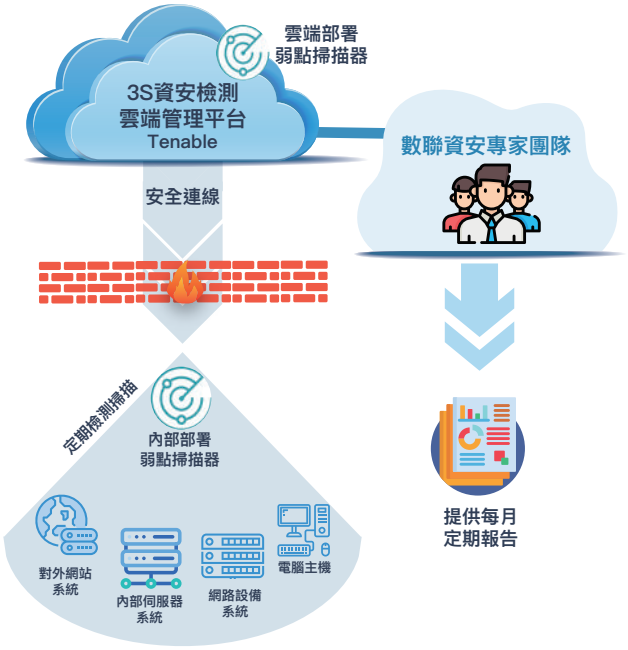
同時透過訂閱租賃的付費方式，企業用戶可將資本支出(CAPEX)負擔轉換成快速輕鬆享用的維運費用(OPEX)方式，有效達成降低營運成本的效益。

3S 系統弱點檢測服務，大幅提升資安防護有效性

系統弱點如同埋伏在企業網路中的不定時炸彈，平時應積極的持續檢測，在最新公佈的資安事件中迅速盤查出相關弱點，以對應的解決方案進行必要的修補更新或補強防護控制。系統弱點所造成的資安議題已成為新常態，建立企業系統弱點管理的新思維將有助於企業安心應對。

3S資安檢測服務 - 防駭定檢 採用領先全球的Tenable弱點檢測解決方案，可於系統所在環境中進行網路掃描，依據弱點安全政策定期自動檢測與盤查最新弱點威脅，是新符合新世代系統資安弱點管理方法。

以現代化的雲端平台管理模式，提供專屬的弱點掃描器透過彈性的弱點掃描器部署架構，能同時針對企業內部網路、網際網路、及雲端系統資產目標進行弱點安全檢測，利用遠程安全加密通訊更新執行政策指令、最新弱點情資、檢測結果，以及數聯資安專家協助。



▲3S系統弱點檢測服務運行架構

3S 駭客定檢-系統弱點檢測服務效益

符合弱點檢測信任標準

採用領先全球業界公認標準的弱點掃瞄解決方案 Tenable，支援國際弱點資料標準的CVE，以及CVSS v2與v3的弱點風險評分基準，符合國內外資安檢測顧問的信任標準。

全球最新且最豐富的弱點資料涵蓋率

掌握全球最豐富深入且涵蓋率最廣的弱點情資，提供10萬多個涵蓋各種應用程式與作業系統的弱點檢測Plugin，包含 5 萬多個CVE弱點資料，每週在弱點披露24小時內即發佈 100 個以上的Plugin快速更新。

高準確率、高效率、高速的檢測

檢測準確度達到六個標準差，每100萬次掃描中僅有 0.32 次誤報；並且結合多項主要情資來源，包括與第三方弱點及威脅資料中歸納出弱點遭攻擊者利用的機率，透過獨家的機器學習演算法，找出可利用性最高的弱點，排定弱點的優先順序。

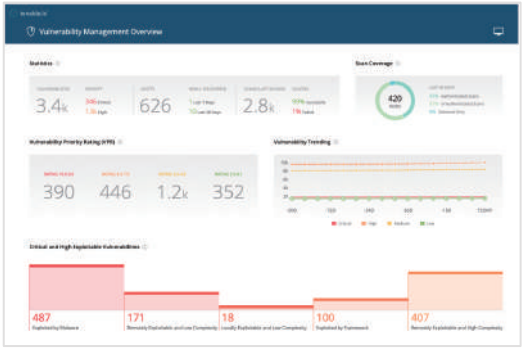
專屬的弱點掃描器，確保掃描品質與可靠度

3S資安檢測服務提供專屬的弱點掃描器，簡化並加速企業系統弱點檢測作業上的繁瑣作業，並確保服務上的安全可靠度。

聰明的弱點管理幫助正確的資安防護，並避免無效投資

傳統的資安防護設計多半在不清楚企業存在弱點威脅下，而未能正確設計出有效的資安防護措施，相對造成資安投資上無法發揮效果。新一代系統弱點管理在持續檢測、監控、及預測企業重要資產的風險曝露指數，幫助資安防護投入更正確有效果。

弱點評估流程步驟



▲智慧化的弱點管理，快速效率掌握整體的資安風險概況

3S 社交工程郵件演練服務

94%
94%惡意軟體
是透過電子郵道傳送

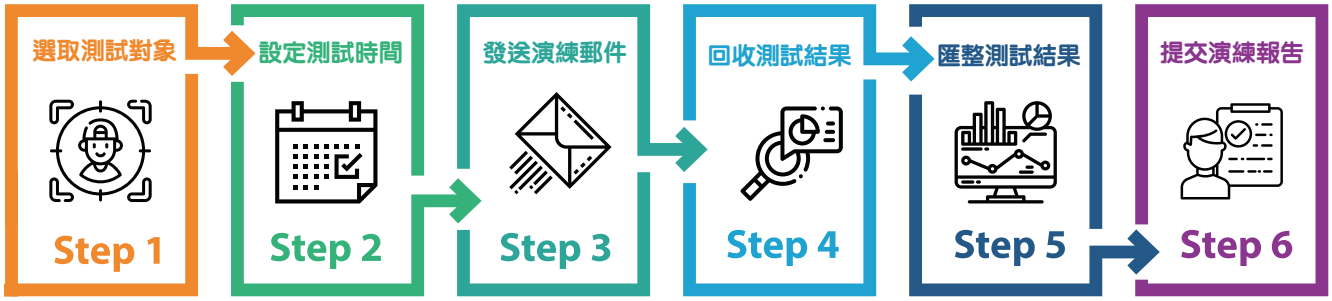
80%
超過80%的資安事件
是藉由社交工程郵件攻擊

54.7%
54.7%的企業資安風險
來自於員工資安意識不足

現今駭客攻擊手法詭譎多變，尤其是「**社交工程郵件**」更是駭客最慣用也容易成功的招數。利用人性的好奇心及容易疏於防範的詭計所精心策劃的電子郵件，經常能順利突破企業的資安防護網。根據Verizon針對數千筆資安事件的調查，**80%的資安事件是來自於社交工程郵件所造成**。這些來自駭客的郵件往往夾帶惡意程式或勒索病毒，利用各種時下最為人關心注意的話題或是工作相關主旨，企業內部員工一旦被誘騙點開就受駭了。駭客利用社交工程郵件潛伏侵入企業環境中，探勘挖掘出環境中所有可利用的系統弱點並逐步發動殺手攻擊，造成企業遭受重大的資安傷害跟金錢損失。

社交工程郵件演練是政府資安法及金融資安管理所被重點要求的資安任務之一，其目的就在於透過演練過程進而達到員工提升資安意識自覺性及檢測電子郵件防護效果，因此在3S資安檢測服務中也提供企業單位針對員工進行社交工程郵件演練，有助於企業資安成熟度的提升，減少駭客惡意程式與勒索病毒侵入的機率。

3S 社交工程郵件演練服務流程



3S 網站健康監測服務

企業網站等同於存在於網路世界的另一種型態呈現，尤其近年來跨境電商興起，網站具備的商務功能對於企業來說更加重要。根據天下雜誌調查，2020年因為疫情關係更促使國內電子商務類的營收成長率平均達到10.22%，但由於企業網站多數以自行架設或線上服務租用，往往急於上線營運而忽略網站的安全性，造成每5個網站就有1個暴露於駭客攻擊風險下，一旦企業網站受駭將造成客戶個資外洩、網站服務停擺、以及企業商譽受損，嚴重衝擊企業的形象與信任度。

3S資安檢測服務提供是一項提供訂閱用戶企業網站安全健康的必要狀態檢測服務，針對重點網站5大安全指標的監測，透過輕量無負擔的監測方式，週期性持續的觀測企業網站健康狀態並給予評量等級，幫助企業輕鬆快速地體檢網站健康。

SSL憑證
SSL憑證是企業商務網站的安全規範，確保線上交易跟客戶資料的傳送被安全信任；網站如果沒有SSL加密，客戶的敏感資訊與機密資訊就會暴露在駭客的眼前！

Cookie安全相關設定
網站設定不當，造成網頁回應 (Header)顯露過多資訊，幫助駭客更容易判斷如何攻擊您的網站。經常檢查企業網站是否有這些不當設定，能夠大幅降低網站安全風險。

網站主機開啟port - NMAP
網站大門敞開？知道您的企業網站主機開啟哪些服務入口(Port)嗎？ 這些服務入口是必要的嗎？曝露不必要的接口於網際網路中，就如同門戶大開，置身在被駭風險之中。

DNS相關資訊
網域名稱(DNS)代表您的網站的地址門牌，但是曝露子網域在外，等同幫助駭客搜集網站資產分佈，增加入侵管道情報，將子網域資訊隱藏起來有助於避免駭客注意。

網頁元件
CMS內容管理系統是現今網站架設的熱門選擇，例如WordPress、Joomla、Durpal等，這些系統能夠方便且快速建立網站，並有豐富的外掛資源可以使用。但也由於使用者中眾多，開源軟體成為駭客攻擊最好的目標。使用前了解套件或版本是否存在問題，提早做好安全性防範。

3S資安檢測服務 - 防駭定檢

企業資安如同人類健康，而資安威脅就像是不斷出現的各種病毒病菌；在面對攻擊目標方式不同的各種資安威脅時，最有效的策略就是揪出危害健康的原因並進行預防災害及資安防護的準備，才是上策。對於正要邁入數位轉型升級階段的企業來說，隨著藉由網路數位化與世界接軌的同時，資安風險威脅也必然隨之而來。對於企業來說，資安已經是一項需要但困難的議題，尤其在無法掌握企業究竟存在哪些曝露於被攻擊的風險中的資安弱點的情形之下，資安防護的投資往往在缺乏資訊下而沒能發揮應有的保護效果，造成事倍功半的困境。

3S資安檢測服務 - 防駭定檢 以服務為導向，結合專業的工具方法與專家建議，並提供友善清晰的企業資安健康檢測報告。能夠幫助用戶以 **有效率、低負擔、少人力** 的管理方法確保企業健康安全，提升企業數位升級中的資安成熟度。提供下列三大服務項目：

系統弱點檢測

採用領先全球的Tenable弱點評估解決方案，以國際資安檢測的信任標準為基礎。透過雲端管理與企業內部網路掃描方式，針對企業內部重要的目標系統進行弱點風險檢測評估。

- 持續監測系統弱點，協助用戶及早發現存在的資安威脅，落實風險控管。
- 弱點監測月報告，提供威脅指數及風險順位，更有效率進行修補及防護措施。
- 準確有效的預防資安威脅。

訂閱服務方案內容

- 主機系統弱點檢測服務
- 檢測系統主機訂閱數量：100台起
- 享有每月一次定期排程遠端檢測及檢測結果報告。
- 提供 5x8 上班時間專家線上諮詢
- 專用弱點掃描器設備一台

註：本服務不含複測及弱點修補支援

社交工程郵件演練

勒索軟體攻擊多數藉由社交工程郵件手法進入企業內部，進而利用系統弱點展開攻擊。定期持續透過社交工程郵件演練是最能幫助企業量測郵件安全及員工資安意識警覺性，從而加以改善的方法。

- 量測企業郵件安全防護檢測能力。
- 提升內部員工資安意識及警覺性。

訂閱服務方案內容

- 提供5封社交工程郵件樣本進行發送。
- 100個企業電子郵件帳號進行演練檢測。
- 每年一次的演練服務及檢測報告。

註：本服務不含複測

網站健康監測

網站是企業數位的重要服務之一，網站健康狀態監測是針對網站的5大安全指標進行遠端安心檢查，持續監測網站安全，提供網站安全評量系數。

- 針對企業網站常見的5大安全指標持續監測，把關企業網站安全，降低被駭風險。
- 5大指標：SSL憑證、Cookie安全設定、Port 服務端口、DNS資訊、Wordpress 元件

訂閱服務方案內容

- 網站健康狀態監測服務
- 針對3個企業網站URL進行持續監測。
- 每月一次定期排程遠端檢測及每月監測評量報告。

註：本服務不含複測及客制化

3S資安檢測服務

防 駭 定 檢

諮詢熱線：(02) 7721-1688
服務信箱：3S@issdu.com.tw
WWW.ISSDU.COM.TW

Visit Us on

Follow Us on