



● iCON 技術總監 Vince Tai 與 Fortinet 高級渠道經理 Patrick Hui 通力合作，為企業提供全面的網絡安全偵測及評估服務。

近年勒索軟件攻擊及數據洩密事故不斷發生，導致不少企業損失慘重。有見及此，香港著名系統整合商 iCON (ICON Business Systems Ltd) 引進 Fortinet 資訊保安方案，提供全面漏洞評估 (Vulnerability Assessment) 服務，協助企業找出潛在風險，堵塞錯漏。

ICON 漏洞評估服務 (VULNERABILITY ASSESSMENT)

Fortinet 全力支持

專業團隊查找隱藏威脅

iCON 技術總監 Vince Tai 表示：「今天企業 IT 基建由封閉系統延伸到雲端，越來越複雜，若不定期進行全面漏洞評估工作，便要冒上嚴重的法規及業務風險。」iCON 早在兩年前成立 CIA (Cloud Integrated and Advanced Solution) 團隊，由擁有 CISSP、CISA、CEH、CCIE 等專業資格的專家所組成，能深入企業資訊保安各個範疇如作業系統、資料庫、DNS、FTP、電郵系統、網絡基建、手機應用程式和外部連結等，提供專業的漏洞評估、審核及修復服務，主要分為以下五個階段：

第1步：計劃

識別並理解客戶環境並提供最佳解決方案評估策略

第2步：發現

確定並找出潛在的漏洞

第3步：分析

由安全專業人員分析調查結果

第4步：審查和修復

提醒客戶潛在的風險並提出補救方法

第5步：重新審計

確保適當的補救措施，並將風險保持在可接受的水平

Fortinet 全力支持

作為資深安全顧問，iCON 除了採用不同 open source/commercial 安全檢測工具外，還夥拍網絡安全供應商 Fortinet，借助 Fortinet 資訊保安架構 Security Fabric 的實力，保護現今多變的網絡環境。Vince Tai 表示，Fortinet 網站應用程式防火牆 (WAF) 能提供漏洞掃描和修補、行為攻擊偵測、進階可視化分析工具提供的即時攻擊洞察和報告等，曾幫助客戶

偵測 200 個保安漏洞，成功截阻潛伏的黑客攻擊。

Fortinet 與 iCON 合作多年，不但提供最新保安工具，還透過 FortiGuard Labs 頂級威脅研究團隊全力支持 iCON 漏洞評估服務。Fortinet 高級渠道經理 Patrick Hui 表示：「現時 Fortinet 每天處理來自 340 多萬台設備的全球威脅數據，並時刻保護超過 330,000 名客戶。」他指出，Fortinet 今年初於加拿大本拿比 (Burnaby) 開設威脅科研及發展中心，聘請近千名科技人才加強網絡安全科研工作，讓 Fortinet 合作夥伴如 iCON 享用最先進網絡保安技術。

企業每年驗身保平安

iCON 漏洞評估服務推出至今兩年，曾幫助不少政府部門、金融機構及大型企業修補網絡安全錯漏。Vince Tai 指出，最常見情況是因業務伺服器不能停止運作，無法即時更新修補檔。iCON 便會使用虛擬修補方式，例如使用 Fortinet 網路應用程式防火牆來堵塞漏洞。

除了大型企業，今天中型企業也開始了解漏洞評估服務的重要性，或許因工作繁重、人手不足而遲疑。但他強調，越遲進行漏洞評估工入，便會使現時業務系統錯失更多修補漏洞的機會，危機越來越大，也導致將來補救成本高昂。因此，他建議企業每年最少定期進行網絡安全檢查一次，而每逢引進新系統時，也應該再進行安全檢查一次，以策萬全。📌

ICON

網址：www.icon-info.com.hk 電話：+ 852 2748 3698

FORTINET

網址：www.fortinet.com 電話：+ 852 3708 3500