tenable

電力產業基本要件：

網路安全檢查清單上的前三大功能

目錄

簡介

推動電力產業數位轉型的兩大因素是什麼？降低成本與提高效率。

虛實整合系統(CPS)囊括了操作技術和工業控制系統(ICS)，可用於最佳化從遠端系統管理到監控電線及變壓器的運作狀況等業務及操作流程，以及發揮更高的燃油使用效率。資料顯示，數位轉型措施使電力供應商的能源產能提高達 10%[1]，且每年為電力產業省下 800 億美元，也就是每年總發電成本的 5%[2]。

隨著數位化帶來的正向成果，卻也衍生了副產品：網路風險。2022 年全球發生的所有網路攻擊事件中，有十分之一(**10.7%**)鎖定的是能源業者(包括電力公用事業公司和石油與天然氣公司)，成為第四大最常遭到攻擊的產業[3]。在北美的所有網路攻擊事件中，**20%** 發生在能源產業，成為 2022 年該地區遭到最多攻擊的產業[3]。

隨著電力供應商的利潤中心漸趨數位化，管理網路風險勢在必行，但說來容易卻難以實行。多數電力供應商難以確切知道風險所在之處，因為他們的環境中混雜著新舊設備。為了化解網路攻擊造成他們的大規模電力系統(BES)/大規模能源系統(BPS)停機的風險，能源業者在數位轉型的同時，必須將網路安全視為當務之急。

大規模電力系統(BES)：

BES 由與高電壓傳輸系統互連的多台發電機和儲電設施以及傳輸系統本身所構成。

(資料來源：energyknowledgebase.com)

大規模能源系統(BPS)：

(BPS)是一種大規模的互連電力系統，由發電和輸電設施構成。

(資料來源：techtarget.com)

發電及配電產業需要採取全方位的網路安全方法，這種方法牽涉到結合技術控制、原則及程序，以便將網路攻擊得逞的風險降到最低。幸好您可以採取一些措施以因應稽核人員的稽核作業並加強防禦機制。

建構 OT 資安策略時請考量下列三大功能：

資產辨識及分類

電力公用事業使用複雜的 ICS/OT 系統來管理發電、輸電及配電等重大營運活動。新型的公用事業基礎設施由新舊設備混雜而成，這使得辨識風險所在之處成為業者的一大難題。為了維持 BES/BPS 的穩定性，公用事業必須能夠盤點其網路資產並根據其對發電、輸電和配電的重要性加以分門別類。

弱點評估

OT/ICS 系統的設備生命週期較長，多數設備都使用已停產 (EOL) 的軟體，這些軟體當中存在由來已久的弱點。自 1988 年以來發現的 OT 弱點多達 20 多萬個[3]，定期的弱點評估可讓電力公司找出資安弱點所在之處。然而，隨時修補漏洞並不見得一律可行，找出弱點才能藉由強化弱點裝置的網路來減輕風險。電力公用事業必須持續不斷地評估弱點，才能在面臨可能影響服務穩定性的新興威脅時制敵機先。優良的弱點管理方案可提供電力公司保持系統安全及穩健所需的網路風險認知。

威脅偵測

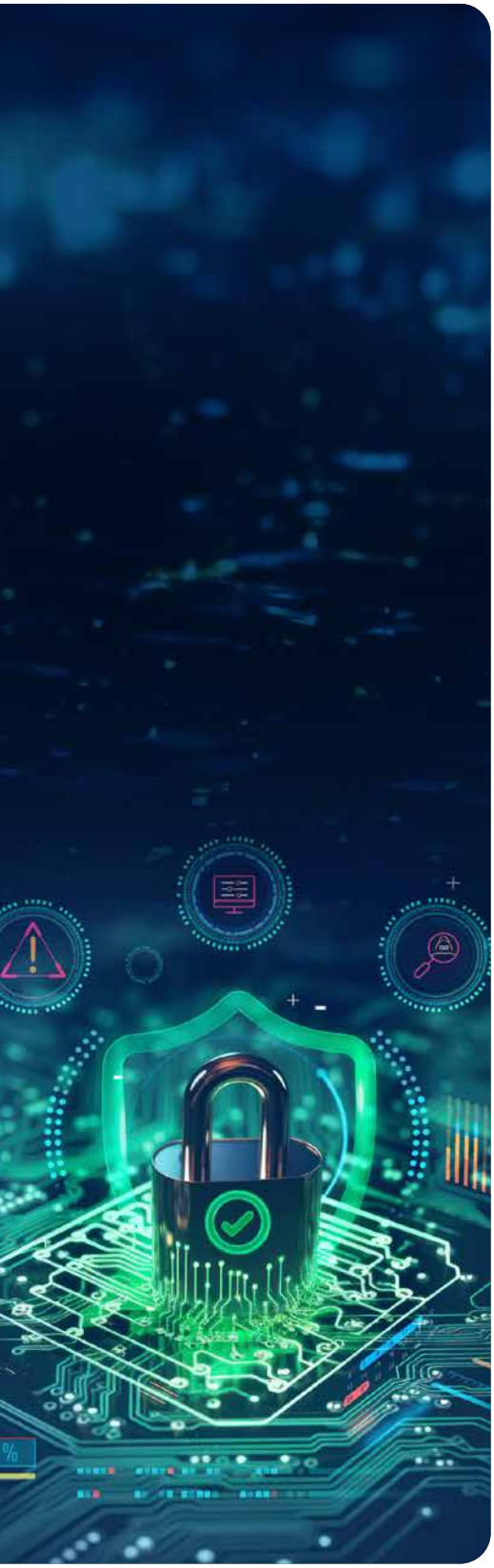
隨著威脅態勢瞬息萬變，電力公用事業需要 24 小時全天候不間斷的威脅偵測，才能察覺 ICS 網路上的運作異常情況。為了保護大規模電力系統免受惡意活動與電網故障等實體及網路威脅的危害，監控網路安全活動是不可或缺的一環。公用事業勢必得持續不斷地監控 ICS 系統，才能察覺可能會中斷電力輸送與穩定性的網路活動並加以防禦。

TENABLE 如何提供協助：

1. 深入的資產能見度與標示：

保障 BES 安全的第一步，便是能夠搜尋 ICS 資產、編列其目錄並加以分門別類。看不到的敵人最可怕。為了解決這個問題，Tenable 的工業網路安全解決方案 Tenable OT Security 採用多元的搜尋方法偵測資產，一開始先被動地監控網路流量，找出所有相連的 IT 和 OT 系統。系統一旦經過準確的分類，Tenable OT Security 便能使用其原生通訊協定安全地查詢 OT 系統，同時充分運用內嵌的 Tenable Nessus 主動掃描 IT 系統，進而傳回詳盡的資產庫，列明每個系統元件的型號、系列、類型、序號、韌體版本、作業系統版本、硬體版本和底層設定。

等到資產都驗明正身後，Tenable OT Security 便以視覺化呈現方式將資產之間的通訊資料流加以對應，清楚顯示系統之間的相互依存關係。這份完整的資產對應圖有助於將資產分類為對 BES 有高度、中度或低度影響，其依據的標準如下：資產位於網路上的什麼位置；該資產一旦外洩，對員工的安全有何影響；資產在發電/輸電中扮演的角色；資產對輸電網路穩定性有何潛在影響。正確的分門別類有助於資安從業人員判斷適當的資安控管措施，並協助他們滿足合規規定。例如，您當地的監管機構或許認為高度影響力的 BES 網路系統必須在四小時內通報資安事端，而中度影響力的系統只要在 24 小時內通報即可。準確的網路資產分類還可以引導您執行網路分段、存取控制及記錄規定等防禦措施。



2. 風險型弱點評估與管理：

評估 ICS 系統中的弱點並將評估結果整合至整體弱點管理程序中，是積極管理風險的重點。然而，排定新舊系統中成百上千個潛在弱點的優先順序可能是個令人卻步的艱鉅任務。Tenable OT Security 利用即時資產庫和通訊資料流分析計算出 Asset Criticality Ratings (ACR)，根據資產萬一外洩對企業造成的影響來評定資產的優先順序。ACR 可讓安全團隊釐清哪些資產若外洩會造成最嚴重的穩定性或安全風險，這樣安全團隊便能將全副心力放在風險評分最高的資產上。而且，Tenable 還有業界最完善的弱點資料庫，其中包含了 145,000 多個弱點偵測 plugin。這等無與倫比的專業能力加上 Tenable 採用 AI 技術的風險型弱點優先順序評分 (VPR)，從業人員得以根據弱點的可利用性以及對 BES 穩定性的潛在影響判斷哪些弱點應優先修復。

一旦能源產業的資安方案釐清哪些電網資產最關鍵以及哪些弱點最有可能遭到刺探利用，便能將資源集中在最能有效降低網路風險的修復措施上，這些修復措施也能盡量降低萬一 OT 系統遭到入侵可能帶來的衝擊。Tenable 可讓公用事業聚焦在以風險為準而排定優先順序的資產和威脅上，同時加強防禦工事，抵禦可能破壞輸電網路穩定性和安全的實際攻擊。隨著威脅和新弱點與日俱增，Tenable 提供的是電力公用事業保障重大基礎設施並積極強化其網路安全態勢所需的資產型弱點深入解析。

3. 即時威脅偵測與設定監控：

Tenable OT Security 能透過即時監控 ICS 環境是否出現安全威脅來捍衛重大基礎設施。多重偵測引擎不僅能讓這種方法達到效果，還能降低 BES 系統中斷的風險，符合美國北美電力可靠度企業 (NERC) 重大基礎設施防護 (CIP) 的規定。透過立即可用的自訂原則規則並整合 Suricata 開放原始碼入侵偵測系統 (IDS) 特徵碼，達到威脅偵測的效果，使安全團隊獲得更有意義並可作為行動依據的警示，根據這些警示安心地採取行動。此外，偵測引擎可同時找出網路以及各台裝置上的異常行為，並揭開惡意內部人員、設定錯誤的元件引起的風險或工業惡意軟體的曝險。

Tenable OT Security 會擷取 ICS 及資料採集與監控 (SCADA) 裝置設定、韌體版本、軟體修補程式、完整階梯邏輯、診斷緩衝區和標籤結構等的快照，藉此定出已知的資產「良好」狀態基準。擷取這些基準後，Tenable OT Security 就能留存輸電網路資產變更和後續操作的完整歷程記錄，即時監控裝置設定和行為是否偏離基準。取得並保留 IT 和 OT 資產的歷程快照後，輸電網路安全專家就可以調查未經授權的修改或異常活動，這些修改或活動可能表示潛在的風險或外洩的元件。追蹤裝置設定可記錄調整活動，藉此提供稽核支援，因為手動彙整多個迥異的 ICS 環境的活動記錄是極為繁重的工作。再者，掌握裝置設定的能見度也能讓安全團隊透過可能嚴重破壞穩定性的惡意行為和錯誤設定而察覺新興的 OT 威脅。

關於 Tenable

Tenable® 是一家曝險管理公司。全球大約有 43,000 多家企業仰賴 Tenable 協助瞭解並降低網路風險。身為 Nessus® 的創造者，Tenable 拓展了本身在弱點方面的專業知識，以提供全球第一個可在任何運算平台上查看和維護任何數位資產安全的平台。在 Tenable 的客戶中，包含大約 60% 的財星 500 大企業、大約 40% 的全球 2,000 大企業以及大型政府機構。

如需深入瞭解，請前往 zh-tw.tenable.com。

總結

Tenable 的 OT 安全解決方案在業界首屈一指，它將資產能見度、弱點管理和威脅偵測合而為一，一舉克服了電力業者面臨的多個難題。有了 Tenable 一流的 OT 專業能力、思維領導力和客戶支援，能源業者就能有效地防護重大基礎設施，抵禦日益攀升、可能有礙輸電網路運作和穩定性的網路威脅。由於鎖定工業控制系統下手的先進攻擊與日俱增，Tenable OT Security 具備公用事業保障 BES 網路系統、確保符合法規並積極強化網路防禦工事所必備的功能。

關於 Tenable OT Security

Tenable OT Security 可掌握工業環境、重大基礎設施的能見度、安全措施和控管措施，還能建構管理系統；更重要的是，它可以協助企業維持生產力、符合法規要求並抵制網路攻擊，確保安全無虞。Tenable OT Security 利用享有專利的多元搜尋方法，安全地掌握裝置和虛實整合系統的能見度而不會造成中斷，提供詳盡的資產庫，透過單一介面深入瞭解全球所有據點的資產實際情況。從弱點管理及威脅偵測到設定控制及報告等，Tenable OT Security 讓企業得以排定處置措施的優先順序，使其 IT 和 OT 安全團隊能夠更加合作無間。

資料來源

1. www.mckinsey.com/industries/oil-and-gas/our-insights/digital-transformation-in-energy-achieving-escape-velocity
2. www.mdpi.com/1999-4893/16/4/211
3. www.ibm.com/reports/threat-intelligence

請與我們聯絡：

請傳送電子郵件至 sales@tenable.com 或前往 zh-tw.tenable.com/contact