tenable OT Security

使用案例

保障智慧型輸電網路的安全

重要趨勢

- 工業物聯網與 IT 及 OT 的融合快速風行
- 互連性更高的大型分散式網路
- 再生與間歇性能源的問世
- 改採通用的 TCP/IP 型標準，如 IEC 61850 與 IEC 104

主要挑戰

- 分散式子工作站需要能妥善保障服務安全性的能見度與因果分析
- 對於時間和營運關鍵資源來說，為確保不出差錯的持續穩定供應，穩健性很重要
- 這些輸電網路產業涵蓋的龐大範圍與各種通訊協定都使其攻擊破綻大開

背景說明

輸電網路不斷地演進。由於智慧型輸電網路的崛起、再生資源的問世以及各種儲電方案的演變，輸電網路必須更加靈活有彈性才行。在採行風力和太陽能等間歇性能源時，如果要維持供需平衡，輸電網路必須能即時應變並靈活調控。這並非輕而易舉之事。

為了解決這些難題，輸電網路變得越來越智慧化、緊密互連，也更加數位化。因此，網路能見度、安全性和掌控度必須從輸電網路層面貫穿到間隔層和個人智慧型電子裝置 (IED)。改進智慧型輸電網路的互連性、充分運用新型的 TCP/IP 標準 (如 IEC- 61850 和 IEC-60870-5-104) 並採用新的資料擷取技術等，已成為公認的產業標準。

互連網路在提供高效率的同時，也帶來了範圍更廣的攻擊破綻，這些破綻可使網路攻擊從一家供應商快速傳播到下一家供應商。因此，以輸電網路為主的產業網路威脅成為安全性、穩定性和業務永續性的重大危害。

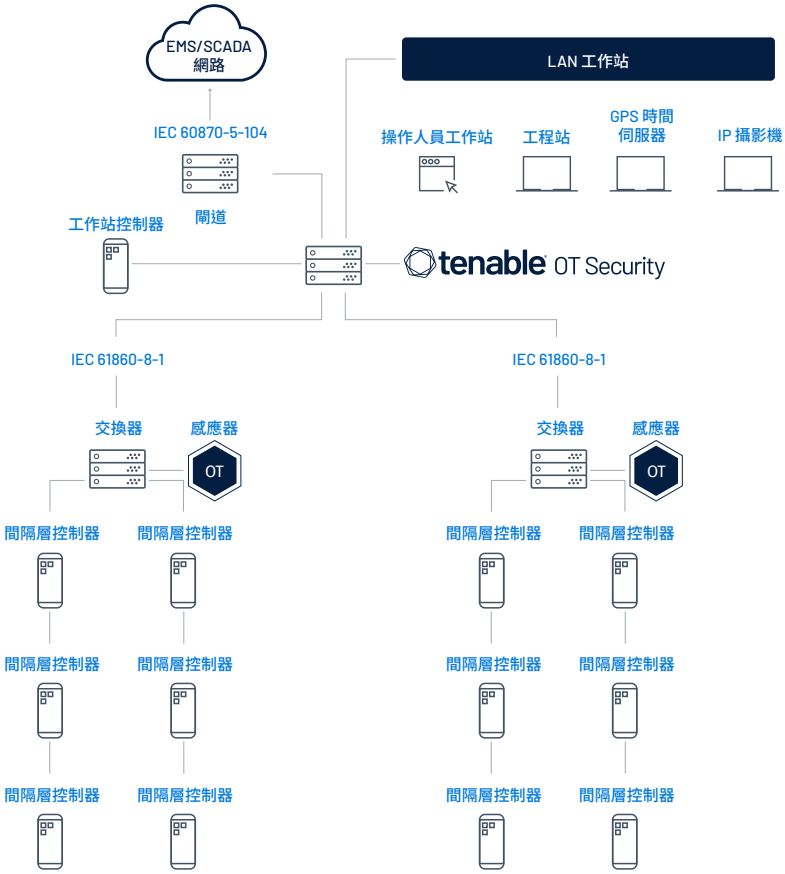
智慧型輸電網路攻擊大剖析

- 初步滲透輸電網路
- 利用網路上的某項資產建立灘頭堡
- 展開偵察活動，找出目標與易受攻擊的裝置
- 傳播到其他資產中，到達有意攻擊的目標
- 在攻擊的「最後一哩路」給予致命一擊，中斷輸電網路的運作

近期實例

- **2023 年 5 月：**新發現的 CosmicEnergy 惡意軟體就是一種可能會中斷發電並造成實體損壞的惡意軟體。(資料來源)
- **2022 年 4 月：**在俄羅斯攻擊烏克蘭之後不到兩個月內，就發現 Industroyer2 鎖定烏克蘭境內的區域性高壓電變電所發動攻擊。(資料來源)
- **2020 年中：**與中國串聯的 RedEcho 集團在地緣局勢緊張之際，利用 AXIOMATICASYMPTOTE 基礎設施大舉入侵印度的電力產業。(資料來源)

標準的 SCADA 部署



常見的輸電網路業標準

IEC 61850 電力公用事業自動化的通訊網路及系統

IEC 61970 包括通用資訊模型在內的能源管理系統應用程式介面

IEC 61968 配電管理的系統介面

IEC 61400-25 監控及控制風力發電廠的通訊

IEC 62325 能源市場通訊架構

IEC 62351 資料傳輸安全標準

IEC 62056 讀錶、電費與負載控制資料交換

IEC 61508 電力/電子/可程式化電子安全相關系統的功能安全

IEC 61131 可程式化控制器

IEC 61334 透過配電線路載波系統運作的配電自動化

ISO/IEC 14543 家庭電子系統 (HES) 架構

IEC 61499 分散式控管與自動化

IEEE 1547 分散式能源資源與互聯電力系統介面的互連與交互運作標準

無能見度，也看不出因果關係

在輸電網路環境中，網路攻擊的「最後一哩路」可能會傳送合法的通訊協定指令給控制器、繼電器與 IED。這些指令可能使用非專有通訊協定（如 IEC-61850、IEC-60870-5 和 DNP3 等），亦可能使用廠商專有的通訊協定。中斷運作可能對安全和輸電網路穩定性造成嚴重後果。

這些類型的事件都應該全數納入考量，然而，在最後一哩路階段之前，應該早先發現攻擊跡象。任何一處的流量都應該受到監控，包括子工作站的匯流排本身。必須明確瞭解事件本身並將詳細的因果關係納入考量，才能辨別事件到底在本質上是惡意攻擊，亦或只是正常運作的流程。解決方案必須能夠針對每個輸電網路的獨特需求加以調適，才能減少誤報情況並讓網路管理員能將全副心力放在維護正常運作上。

為了在攻擊進行的任何一個階段將其辨識出來，企業需要多重偵測引擎。

1. DPI 引擎同時適用於非專有與專有通訊協定，可區分攻擊的「最後一哩路」和偵察事件。
2. 一般的流量對應與流量視覺化呈現必須能察覺來自外部、試圖與內部網路進行通訊的可疑活動。
3. 需使用異常偵測機制來找出非正常網路作業流量模式。
4. 若能充分運用以特徵碼為基礎的偵測功能，就可以找出已知威脅。攻擊者會使用這些威脅透過網路來建立灘頭堡或加以傳播。

實體竄改

不同於通常位在單一大型建築物內的傳統式 IT 網路或製造廠，輸電網路會分散在一個範圍廣大的實體區域。有效的 OT 安全解決方案必須定期查詢位於所有據點的各個裝置，並辨識是否已執行任何變更。必須查詢網路上所有的 IED，因為它們掌控著輸電網路的正常運作。同時也必須查詢對一般網路作業有關鍵影響的伺服器、工作站、網路設備、閘道和 OT 裝置。

Tenable OT Security 充分運用專利的主動式查詢技術，同時也是首家專門針對電力網路推出主動式查詢引擎的廠商。此技術採用非專有與專有通訊協定的主動式查詢，以徹底瞭解實際情況並完整涵蓋分散式輸電網路中的所有裝置。

管理所有資產

電力網路通常都必須使用大型的基礎設施。各式各樣不同的裝置散佈在範圍廣大的區域內，有時甚至會橫跨好幾個網路。除了各種品牌和機型之外，網路通常還會設有多世代的裝置。解決方案必須能夠結合若干搜尋方法，以此建立整個分散式環境的最新資產庫。

為了使資產庫維持最新狀態並針對任何來源不明的變更獲得警示，必須使用資產追蹤功能。這樣才能針對電力網路中發現的所有類型裝置（如 IED、EMS 伺服器、GPS 時間伺服器、防護裝置等）提供必要的能見度。此功能可因應擁有多種異質裝置的大型網路規模而擴充。更重要的是，它能找出並未透過網路定時通訊的休眠裝置。

執行混合式資產追蹤的企業可被動地透過 SPAN 連接埠或感應器擷取網路通訊的詳細資訊，並找出每一則網路通訊涉及的所有資產以及具體詳細資訊。Tenable OT Security 將被動式技術與專利的主動式裝置查詢技術加以結合，以盤點包括「休眠」裝置（未定時通訊）在內的所有裝置。

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。

主動式弱點管理

電力網路通常會包含一組隨意升級或更換過的老舊裝置。各種裝置類型都有不同的修補程式層級，使得維持時時更新的修補程式管理計畫困難重重。此工作若手動執行，可能會發生疏失與錯誤，更遑論需耗費大量時間與心力。因此，隨時深入瞭解每台裝置的狀態與特性不可或缺。這包括必須能夠準確匹配裝置的特定狀況與相應的弱點知識庫，藉此免除誤報情況。由於輸電網路環境有著不斷變動的特性，知識庫的內容也必須定期更新，隨時反映最新發現的弱點。建置好準確的資產庫後，再充分運用主動式與被動式偵測機制，Tenable OT Security 就能擷取裝置的詳細資訊（例如機型、韌體、修補程式層級、已安裝的軟體、序號等）。如此一來，修補程式管理和安全工具才能反映所有裝置的最新狀態並妥善地保障其安全。

總結

網路安全現已成為電力網路眾所週知的核心風險。為了減輕該風險，產業必須獲得所有操作資產的全面能見度，這些資產包括 IED、RTU PLC、斷路器、電錶、傳動器和其他裝置。

Tenable OT Security 針對非專有與專有通訊協定使用被動式偵測和專利的主動式查詢技術，來偵測輸電網路環境中的所有威脅。Tenable OT Security 還研發出完善的原則機制，讓網路管理能配合各個網路的例行公事制定出相關規則。同時使用兩種安全機制搭配 Tenable OT Security 彈性的部署方案，可確保智慧型輸電網路的運作安全無虞並降低風險。

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 利用享有專利的混合搜尋方法，安全地掌握裝置和虛實整合系統的能見度而不造成中斷，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呈報等，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。