tenable.ot
Powered by Indegy

工業網路安全解決方案簡介

迫近的安全網路風暴

現代工業營運常常橫跨複雜的資訊科技 (IT) 和操作技術 (OT) 基礎架構。標準的工業與關鍵基礎架構環境中存在著上千台裝置，透過工業物聯網 (IIoT) 連線者也越來越多。這為保護工業環境帶來新的挑戰，因為網路安全威脅更難偵測、調查和修復。

產業的網路安全難題

如今複雜的操作技術 (OT) 環境已成為新型攻擊鎖定的目標。IT 與 OT 的融合，以及物聯網 (IoT) 跨這兩種環境的快速應用，會擴大整體的攻擊破綻以及攻擊媒介。

若防護無法做到完整涵蓋，那麼攻擊 事件的發生只是遲早的問題。

針對工業營運與關鍵性基礎架構展開的攻擊，其終極目標是工業控制器。視產業類型而定，此控制器可能是指可程式化邏輯控制器 (PLC)、遠端終端裝置 (RTU) 或分散式控制系統 (DCS)。

這些控制器非常穩定，而且實際控制對象包羅萬象，從冷卻站到渦輪機、輸電網路、石油和天然氣等。

事實上是工業控制系統 (ICS) 使營運得以持續不中斷。由於它們的穩定性高，多數裝置都已行之有年。它們是推動現代化社會的主力，也因而成為攻擊的引爆點。

完備的 ICS 網路安全功能

Tenable.ot 能保護工業網路免於網路威脅、惡意內部人員及人為錯誤。從偵測及降低威脅到追蹤資產、弱點管理、組態控管及裝置完整性檢查，Tenable 的 ICS 安全性功能可在確保企業作業環境能見度、安全性與控管方面，發揮最大功效。

能見度

透過單一虛擬管理平台清楚明瞭貴公司融合式 IT/OT 環境中的實際情況。

安全性

抵抗精進的網路威脅對貴公司工業網路造成的危害，並避免駭客與惡意內部人員造成的風險。

掌控度

追蹤所有 ICS 裝置的「一切」變更，藉此全面掌握企業的作業網路。

Tenable.ot 擁有專供 IT 安全人員及 OT 工程師使用的完善安全工具及報告功能。它能為融合式 IT/OT 領域和工業控制系統 (ICS) 活動提供前所未有的能見度，並透過單一虛擬管理平台讓企業明瞭所有據點及其相關 OT 資產 (從 Windows Server 到 PLC 底層) 的實際情況。

解決方案元件

- **全方位的能見度**
  攻擊可能在 IT/OT 基礎架構中輕易傳播。只要利用單一平台，就能同時涵礙企業的 OT 與 IT 系統來管理及測量網路風險，使企業對於融合後的攻擊破綻有全方位的能見度。Tenable.ot 還能和領導性的 IT 安全及操作工具原生整合，例如貴公司的安全資訊及事件管理 (SIEM) 解決方案、記錄管理工具、新一代防火牆和工單系統。如此可共同建立一種互相信任的生態體系，使企業的所有安全產品彼此配合，造就安全的企業環境。

- **偵測與降低威脅**
  Tenable.ot 充分運用多重偵測引擎，找出可能影響 OT 作業的高風險活動與行為。這些引擎包括：

  原則導向引擎：利用此專有功能，企業可啟動預定的原則或建立自訂原則，將具體的精細活動 (這些活動可能意味著網路威脅或作業錯誤) 明列於白名單及/或黑名單中，一旦發生即可觸發警示。原則也會觸發系統對預定情況展開檢查。這種做法對於搜尋並不引人矚目的高風險活動 (例如惡意軟體、偵察活動、查詢人機介面 [HMI] 的裝置韌體版本) 而言非常重要。

  行為異常引擎：系統會根據網路流量模式偵測其偏離基準的情況。模式基準包括了時間範圍、通訊協定、裝置等綜合要素。另外，它還能偵測可疑掃描，顯示出網路中有惡意軟體或惡意裝置。引擎接著會傳送情境感知警示和詳細資訊給您的團隊，以供快速採取應變措施並針對狀況展開鑑識調查。

  特徵碼更新引擎：在與開放資安基金會 (OISF) 合作之下，Tenable.ot 充分運用 Suricata 特徵碼資料組以及 Tenable 的專屬特徵碼規則。藉由善用群眾外包資料，企業可偵測所有階段的攻擊並獲得與當下情況相關之可疑流量的警示，進而發現偵察活動、可利用的弱點、已安裝的惡意軟體、橫向傳播以及其他風險。威脅偵測引擎會匯入最新的特徵碼以應付不斷演化的新威脅。

- **資產庫與主動偵測**
  透過充分運用突破性的專利技術，Tenable.ot 使企業獲得對基礎架構無與倫比的能見度，不僅限於網路層面，還包括裝置層面。它可搭配原生通訊協定主動查詢企業 ICS 環境中的 IT 以及 OT 裝置，確認企業網路中的一切活動和行為。

- **風險型弱點管理**
  Tenable.ot 擁有全面且詳盡的 IT 及 OT 資產追蹤功能，利用 **Predictive Prioritization** 為貴公司 ICS 網路中的每一個資產產生弱點與風險等級。此類報告包含風險評分與詳細見解，搭配減輕風險的建議。

  Tenable 的弱點評估涵蓋多項參數，例如韌體版本、相關的 CVE、專屬研究、預設密碼、開放的連接埠、已安裝的 hotfix 等等。如此能讓授權人員快速找出最高風險，在弱點遭到攻擊者利用前依照優先順序進行修復。

關於 TENABLE

Tenable®, Inc. 是一家 Cyber Exposure 公司。全球超過有 30,000 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 拓展了自己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，有 50% 以上為財星 500 大企業，超過 30% 為為全球 2000 大企業和大型政府機構。如需深入瞭解，請前往 zh-tw.tenable.com。

- **組態控管**
  有了 Tenable.ot，貴公司就能追蹤惡意軟體和使用者透過網路或直接在裝置上執行的變更。

  組態控管提供了裝置組態隨時間變更的完整歷史記錄，包含特定階梯邏輯區段、診斷緩衝區、tag table 等精細資訊。如此能讓管理員利用備份快照建立「最後正確狀態」，更快速地復原和符合產業法規

Tenable.ot 元件

Tenable.ot 的解決方案由下列幾項元件組合而成：

- **核心平台**
  可直接收集及分析網路流量（透過與網路連線之交換器上的 SPAN 連接埠或透過網路分流器）及/或使用感測器傳輸而來的資料（內含所擷取的網路流量）。

- **主動式偵測附加元件：**(選用)
  含強化裝置型安全性與能見度的裝置查詢功能。

- **感測器**
  可在包含待監控裝置的各網路分段部署選配的小型輕便感測器，裝置經由網管型交換器與一個感測器連接。

如需詳細資訊：請前往 zh-tw.tenable.com
聯絡我們：請傳送電子郵件至 sales@tenable.com 或前往 zh-tw.tenable.com/contact