數據手冊

Claroty xDome

工業網路安全之旅的模組化 XIoT 解決方案

XIoT 安全挑戰

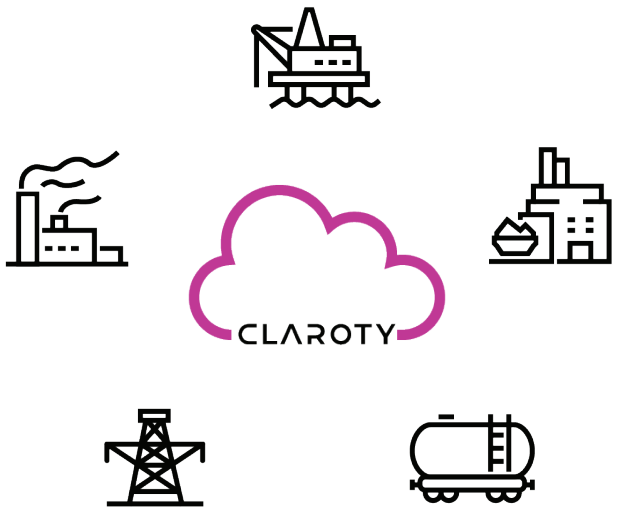
企業組織需要網路安全保障，來維護網路和操作彈性。然而，這兩個目標越來越難以實現。這些挑戰的根源在於擴展物聯網（XIoT）的發展。在數字轉型的推動下，這一龐大的網宇實體網路涵蓋了從工業環境中的傳統 OT 資產到「智慧」照明系統和暖通空調系統，甚至是聯網型自動售貨機的方方面面。儘管具有明顯的業務優勢，但這種網宇實體連線也在製造新的安全盲點和不斷增長的攻擊面，這對操作環境的可用性、完整性和安全性構成了相當大的風險。

在 XIoT 具有挑戰性的安全和風險條件下，實現和維護網路和操作彈性絕非不可能，但這確實要滿足一系列嚴格的要求，而傳統解決方案或通用方法根本無法滿足這些要求。Claroty xDome 跨越了整個網路安全過程，從為企業組織提供全面的資產可視化，識別、測量和確定風險優先順序，到部署零信任保護控制，再到通過廣泛的集成生態系統優化威脅檢測。xDome 是一個模組化平台，SaaS 平台，通過以下方式明確了 XIoT 的網路安全決策：

- 資產探索
- 弱點與風險管理
- 網路保護
- 威脅檢測
- 資產管理
- 變更管理

xDome 優勢一覽

- 通過基於 SaaS 的模組化工業網路安全平台，增強整個 XIoT 的網路安全
- 支援從資產探索到全面網路安全集成及優化的完整行業網路安全之旅
- 可擴展性強，高度靈活且易於使用，無論面對何種網路規模、架構或終端用戶多樣性，總能找到適合您的解決方案
- 與安全解決方案無縫集成，將現有網路安全控制擴展到工業環境

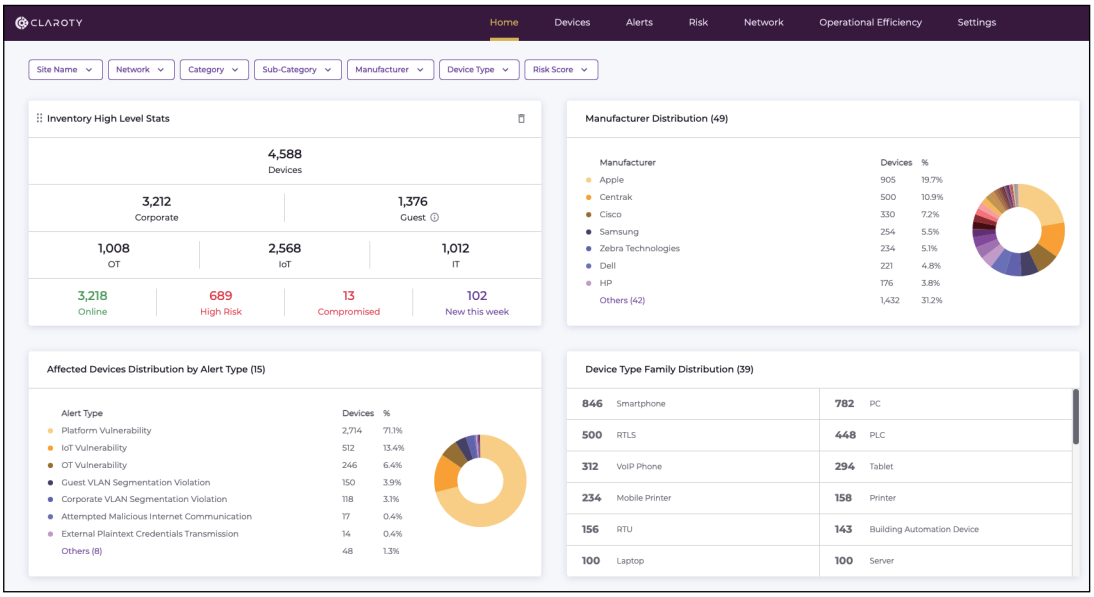


版權© 2021 Claroty Ltd. 版權所有

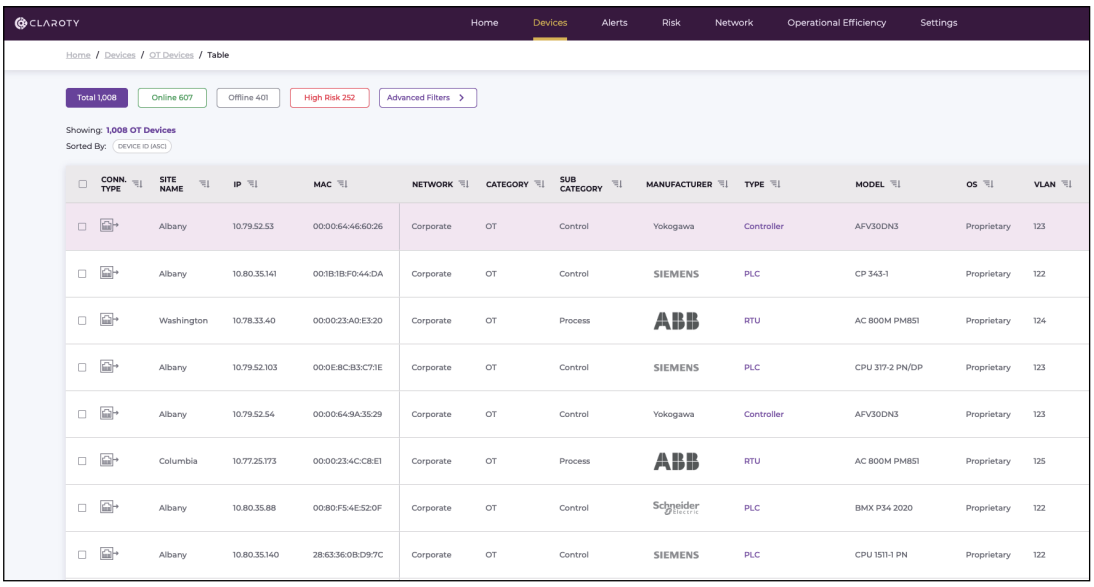
資產探索

有效的工業網路安全始於了解需要保護的內容，這就是為什麼全面的 XIoT 資產清單是工業網路安全之旅的基礎。Claroty xDome 利用最廣泛、最深入的 XIoT 協議覆蓋組合，加之 Claroty Team82 對這些協議特定領域的研究，可提供關於 XIoT 資產的細緻、集中的清單。Claroty 是唯一一家能夠通過三種不同、高度靈活的方法提供這種可視性的供應商，這些方法可以根據每個環境的獨特需求進行組合或單獨使用：

- **被動監控**：持續監控網路流量，以識別和豐富資產詳細資訊和通訊配置檔案
- **Claroty Edge**:戰略性部署，可快速、安全地查詢網路中難以訪問或無法到達的部分
- **集成生態系統**：與通用 CMDB 和資產管理工具無縫集成，進一步豐富資產詳細資訊並優化企業資產管理



Claroty xDome 主頁控制面板



Claroty xDome OT 資產清單

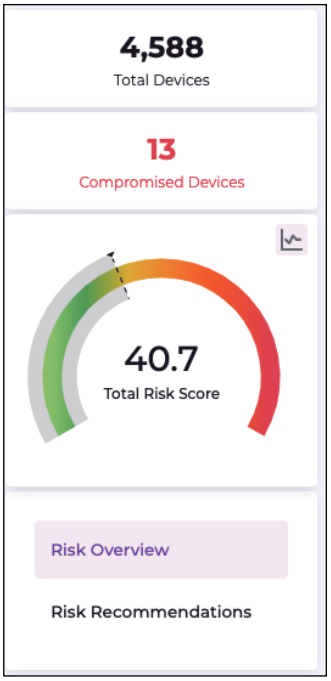
版權© 2021 Claroty Ltd. 版權所有

弱點與風險管理

xDome 自動將每個 XIoT 資產與我們屢獲殊榮的 Team82 研究人員的最新漏洞調查結果進行比對，並與我們龐大的 CVE 和其他弱點資料庫相關聯。xDome 能夠按要求完全自訂企業組織的風險容忍度，提供量身定製的風險評分和安全建議，在整個網路中推行風險降低行動。亮點包括以下功能：

- 簡化漏洞識別，並管理補救規劃和執行
- 安全地使用漏洞掃描程式和協調工具來識別工業環境中的 IT 風險
- 根據實際及模擬的影響後果確定風險緩解的優先順序

這意味著形成一個整體的、具體到企業組織的洞察視角，可了解整體風險、漏洞的潛在影響，並了解最有可能被利用的領域。因此，使用者可以更有效地識別、優先處理和修復工業環境中的漏洞。



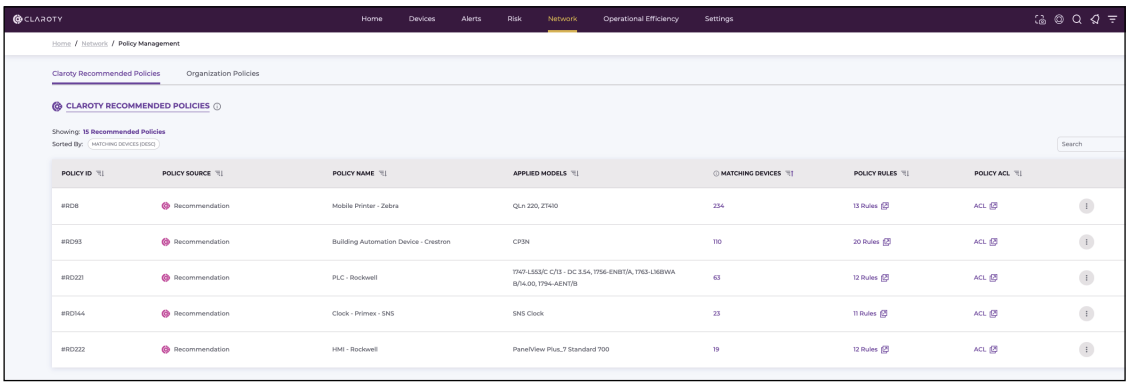
網路風險評分

網路保護

在 Claroty 的深入領域專業知識的支援下，xDome 利用其提供的對 XIoT 資產及其行為模式的可視性，來自動定義並推薦網路通訊策略。此自動化解決方案使您可以在不影響公司組織營運的前提下，更輕鬆地通過現有安全基礎架構來監控、改進和實施這些策略。這些策略也是動態的，可以在實施之前進行模擬以演示網路影響，從而幫助企業組織緊跟覆雜環境中不斷變化的情況。

作為網路分段的一種方法，Claroty 的網路保護功能有助於為「零信任」實踐奠定基礎，這些實踐是提高企業組織工業網路安全態勢的核心：

提高網路架構內資產的可視性 | **提供正常網路通訊的基線檢視** | **通過政策監控和執行來降低風險**



Claroty xDome 建議的策略檢視

版權© 2021 Claroty Ltd. 版權所有

威脅檢測

xDome 已經意識到針對工業環境的威脅的頻率及影響不斷增加，因此它採用了一種彈性檢測模式以持續監測您的環境，在已知威脅和新興威脅剛剛顯現時就將它們及時發現並報告。Claroty xDome 可自動分析所有 XIoT 資產及其通訊模式，以便為正常網路行為生成基線，確定合法流量的特徵，以消除誤報异常，並實時提醒使用者已知、未知和新出現的威脅。亮點包括：

- **統一警報系統**：Claroty xDome 通過其獨樹一幟的裝置可視性深度和補救工作流能力，提供自動監控、優先排序和回應警報的方法。
- **特定領域的威脅情報**：作為一個由SaaS支援的解決方案，Claroty 至少每周都會收到自動檢測更新，因此企業組織始終使用最新的威脅情報。
- **廣泛的集成機會**：Claroty xDome 通過與 SIEM、EDR 和其他安全解決方案的現有集成，將現有的 SOC 功能擴展到操作環境中。

資產及變更管理

在探索、豐富和分析了整個工業環境中的所有 XIoT 資產之後，Claroty 將協助企業組織簡化資產及變更管理。憑藉其強大的基於角色的訪問控制，企業組織可以按特定使用者和分組來自動執行資產管理工作流，從而節省管理時間並減少操作人員的維護時間。

xDome 為使用者提供了管理各種資產需求所需的工具：

- **監控資產更新**：xDome持續監控漏洞、過時軟體、EoL指標和其他需要更新的變動，從而維護資產，時期隨時可用
- **簡化 SLA 法務遵循**：xDome可通過可用性、位置資料和自定義屬性輕鬆識別並報告特定資產的 SLA 法務遵循狀態
- **識別資產變更**：網路新增，配置變更以及異常情況都屬於 xDome 監控的眾多變量，旨在支援 MoC 程式
- **支援稽核要求**：高階報告功能以及與版本控制和備份工具的集成增強了通過 xDome 進行的利益相關方溝通。

關於 Claroty

Claroty 的使命是保護工業（OT）、保健（IoMT）和企業（IoT）環境（即：擴展物聯網（XIoT））中的所有網宇實體系統。該公司的全方位平台可以和客戶現有的基礎結構與程式無縫連線，同時提供可視性、威脅偵測、風險和弱點管理，以及安全遠端存取使用的各種工業網路安全控制。

在世界最大的投資公司和頂尖工業自動化供應商的支援下，Claroty 已被數百家組織部署在全球數千個地點。公司的總部位於紐約市，業務遍及歐洲、亞太地區和拉丁美洲。

Cyberworld
台灣科明大同科技有限公司

CLAROTY FOCUS PARTNER PROGRAM AUTHORIZED INDUSTRIAL

大中華區總代理
網址 www.cyberworld.com.tw
電話 +886-2-7724-8320
電郵 info@cyberworld.com.tw

CLAROTY
版權© 2021 Claroty Ltd. 版權所有