解決方案概要

Claroty 持續威脅偵測平台(CTD)

適用於現代 **OT** 網路的全方位內部部署 **CPS** 網路安全

數位化計畫和擴大遠距離工作讓企業轉型，導致原本隔離的營運技術**(OT)**環境變成和相應的資訊技術**(IT)**環境互相連線，進而促成融合式 **IT/OT** 網路的興起，而這些網路可以為提升 **OT** 環境中的創新和效率提供大好機會。不過，隨著組織持續採用數位轉型，其網路實體系統**(CPS)**的防護則因惡意網路攻擊者的威脅活動持續擴大而日益複雜。

現有的 **IT** 解決方案因為獨特的架構、使用專屬的通訊協定，以及環境和運作限制，並不足以保護 **CPS**。對於提供可以降低 **CPS** 網路風險，能夠以更快的速度創造價值並降低整體擁有成本的全方位解決方案，專門打造的 **OT** 安全非常重要。

Claroty 持續威脅偵測**(CTD)**是為協助營運及/或網路從業人員克服網路實體連線的挑戰所打造。獲得應變能力並非不可能-前提是需要一套完整扎實的要求，而以 **IT** 為主的傳統解決方案無法滿足這些要求。**CTD** 搭載無可比擬的 **CPS** 通訊協定庫和深入的產業知識，可以為 **OT** 環境提供優秀的可見性。如此可以進一步實施涵蓋整個網路實體資訊安全發展過程的核心網路安全控制。這些控制包括：

- 曝險管理
- 威脅偵測
- 遠端事件回應

概述

- 透過多種探索方法和部署機制提供工業環境的完整可視性
- 支援從資產探索到網路整合與最佳化的完整網路實體系統**(CPS)**網路安全發展過程
- 詳細的網路對應支援自動網路分區和虛擬網路分割
- 提供所有警示的情境化根本原因分析與風險評分
- 整合可以提升遠端工作階段事件回應與調查的 **Claroty xDome** 安全存取解決方案
- 利用 **SIEM**、防火牆、**SOAR**、**CMDB** 工具等現有的 **IT** 基礎結構，將既有的資訊安全功能延伸至工業環境

資產探索

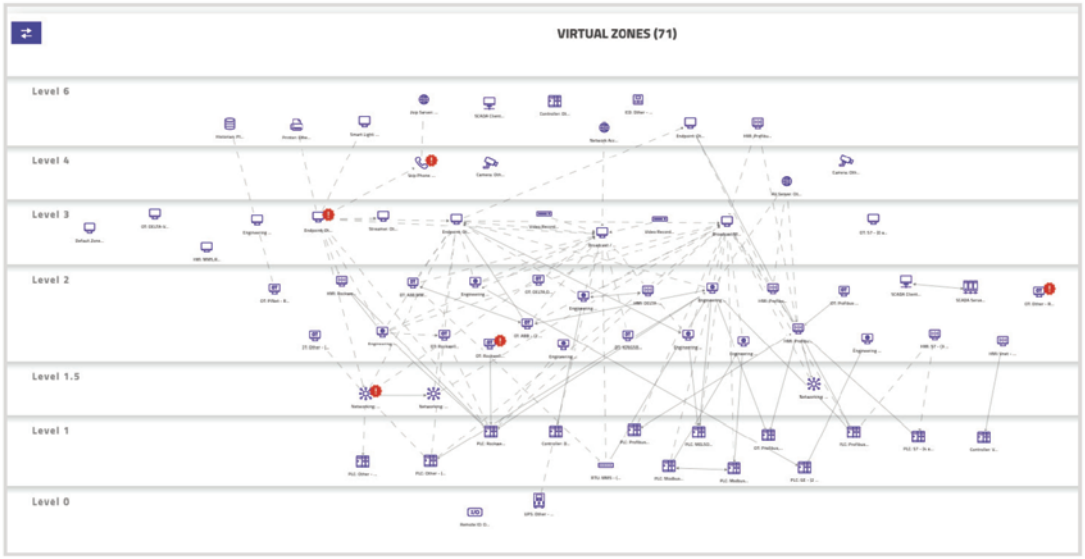
有效的 **OT** 網路安全始於完整工業設備資產可視性的取得。**CTD** 利用業界最廣泛與最深入的 **OT** 通訊協定並採用多種探索方法，可以確保最完整的網路及資產概況。

被動監控	安全查詢	Claroty Edge	專案檔分析
持續監控網路流量 以辨識資產概況	針對性探索其原生 通訊協定中的資產	透過本地的探索查詢 進行快速的主機資產分析	定期擷取離線設定檔 以擴充資產

Claroty CPS 探索方法

這種多管齊下的方法有助於找出不適合使用單一探索方法的工業環境，因此可以提供無可比擬的 **CPS** 環境可視性。這種深入的探索方式會體現在可視性的三個方面：

1. **探索廣度**：採用獨特、高度靈活的方法，可以搭配或單獨使用來建立完整的資產概況
2. **區域型對應**：利用深入的資產概況和通訊監控，將 **OT** 網路自動虛擬分割為虛擬區域。
3. **辨識資產變更**：在 **CTD** 監控的許多變數中，新增網路、設定變更和異常情況是支援變更管理程序所監控的其中一部份

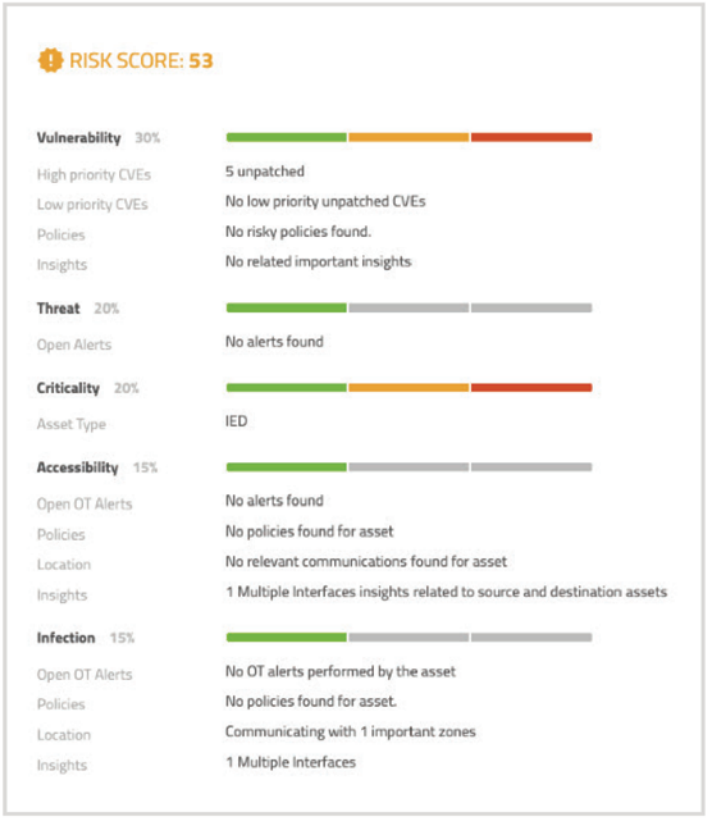


內含虛擬區域的 **Claroty CTD** 分割視圖

曝險管理

CTD 會將 **OT** 環境中的每項資產，如不安全的通訊協定、**CVE**、設定、不合格的安全實務做法，以及 **Claroty** 的 **Team82** 安全研究團隊所追蹤的其他弱點，與其廣泛的資料庫自動進行比較。因此，使用者能夠以更有效的方式辨識、排定優先順序，以及修復在工業網路中所面臨的風險。

- **辨識曝險情況：**分析資產以辨識其面臨的風險，包括弱點、錯誤配置、過時的見解等
- **攻擊向量對應：**透過已知風險的分析來計算攻擊者最有可能的網路入侵形式，以了解和驗證您的曝險情況
- **風險型評分：**根據弱點對您網路構成的獨特風險自動對其進行評估和評分，讓弱點的優先順序排定和修復更為可行及具備效率

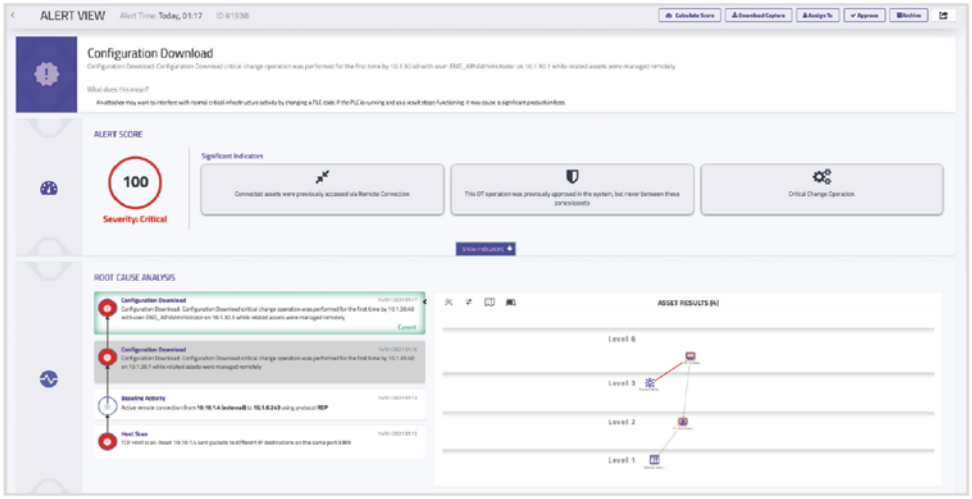


由五個獨特要素組成的 **CTD** 風險評分

威脅偵測

對 **OT** 網路的威脅可能看似簡單但通常極富創意，會利用我們遵循流程的強制性帶來風險。**CTD** 會利用多個偵測引擎自動分析 **OT** 網路中的所有資產、通訊和處理程序，產生具備合法流量特性的行為基準來去除誤判，以及針對異常和已知、未知與新興威脅即時提醒使用者。產品特性：

- **偵測已知和未知的威脅：**描述合法流量的特性來偵測異常通訊、辨識威脅特徵碼、降低誤判，以及針對已知、未知威脅即時提醒使用者。
- **營運事件警示：**持續監控工業環境中的關鍵變更，以協助確保您的製程完整性和運作時間，如此可以收到設定下載等行動的警示，讓您深入了解檔案中確切的程式碼變更。
- **MITRE ATT&CK 警示對應：**將警示對應至 **MITRE ATT&CK for ICS Framework**，以協助增加事件相關脈絡並找出已知的修復措施。
- **根本原因分析：**將相關警示和指標連結到單一連鎖事件，藉此降低網路雜訊、誤判率，以及整體警示疲勞，提供警示相關活動的綜合檢視頁面。



顯示根本原因分析和連鎖事件的 **Claroty CTD** 警示檢視

遠端事件回應

CTD 和 **Claroty xDome** 安全存取解決方案是 **CPS** 網路安全一體化方法的一部份，兩種解決方案整合同時運作的安全功能 - 讓使用者能夠從任何位置偵測、調查與回應事件。因此，企業組織可以利用下列方式來調整遠端、分散式或混合式工作環境的整體安全結構與工作流程：

在遠端工作階段期間直接在 CTD 中接收事件警示和相關指標

透過存取遠端記錄、即時監控，以及記錄的工作階段來調查遠端使用者活動

能夠以立即中斷遠端工作階段連線的方式來回應遠端事件

Claroty 的 CPS 防護

在各種製造和其他關鍵基礎設施部門，**Claroty** 無可比擬的產業專業知識以及廣泛的網路實體系統**(CPS)**知識，是我們全方位網路安全解決方案產品組合的基礎。這種防護始於 **Claroty** 對 **CPS** 網路及其中所有資產的深入了解。因為意識到每個 **CPS** 網路都是獨一無二，所以不可能有通用的方法來探索這些網路。

我們的解決方案搭配雲端式部署或內部部署的模式，即可免除購買和維護多點產品的需求，並且可以靈活選擇最適合資產擁有者的擴充性需求、成本考量與合規性需求的部署方法。這種 **CPS** 網路安全的動態方法正是 **Claroty** 能夠以最快的速度創造價值**(TTV)**和更低的整體擁有成本**(TCO)**，協助關鍵基礎設施企業將連線能力增加所致網路風險降低的原因**-**無論資產擁有者的 **CPS** 網路安全計畫規模或成熟度為何。

關於 Claroty

Claroty 利用一個以工業為主的平台重新定義網路實體系統**(CPS)**防護，這個無可比擬的平台是為保護關鍵基礎設施所打造。**Claroty** 平台提供最深入的資產可視性，以及專為市場上 **CPS** 所打造的最廣泛解決方案，其中包括曝險管理、網路防護、安全存取和威脅偵測**-**無論是搭配 **Claroty xDome** 在雲端使用，還是搭配 **Claroty** 持續威脅偵測**(CTD)**在內部部署使用均可。

在屢獲殊榮的威脅研究和廣泛的技術聯盟支援下，**Claroty** 平台讓企業組織能夠有效降低 **CPS** 風險，以最快的速度創造價值並降低整體擁有成本。**Claroty** 獲得數百家企業組織在全球數千個站台部署。公司總部位於紐約，業務遍及歐洲、亞太地區和拉丁美洲。如需進一步了解，請造訪 **claroty.com**。

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