Claroty持續威脅偵測平台(CTD)

工業網路安全挑戰與Claroty CTD

工業資訊安全挑戰

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工業網路的興起，而這些網路可以為提升工業環境中的創新和效率提供大好機會。儘管網路實體連線具有顯而易見的優點，但許多獨特和不熟悉的裝置類型利用通常為專屬的通訊協定進行通訊，這些不適合使用傳統IT安全解決方案提供防護的裝置類型會造成更大的攻擊面。

達到營運韌性並非不可能 - 但需要滿足困難的的需求條件，而這些條件無法被傳統的解決方案或一般化的方法所達到。在追求網路和營運應變能力的過程中，Claroty持續威脅偵測(CTD)是為協助工業環境克服網路實體連線挑戰所打造。

CTD擁有無可比擬的工業通訊協定資料庫、資產探索方法，以及在工業環境中實現完整可視性所需專屬DPI技術的支援。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：

- 資產探索
- 弱點及風險管理
- 網路防護
- 威脅偵測
- 資產及變更管理
- 遠端存取

CTD優勢一覽

- 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
- 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安全遠端存取解決方案(SRA)
- 整合SIEM、防火牆、SOAR、CMDB工具等現有的IT基礎設施，將既有的資訊安全功能延伸至工業環境

資產探索

有效的工業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工業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。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：

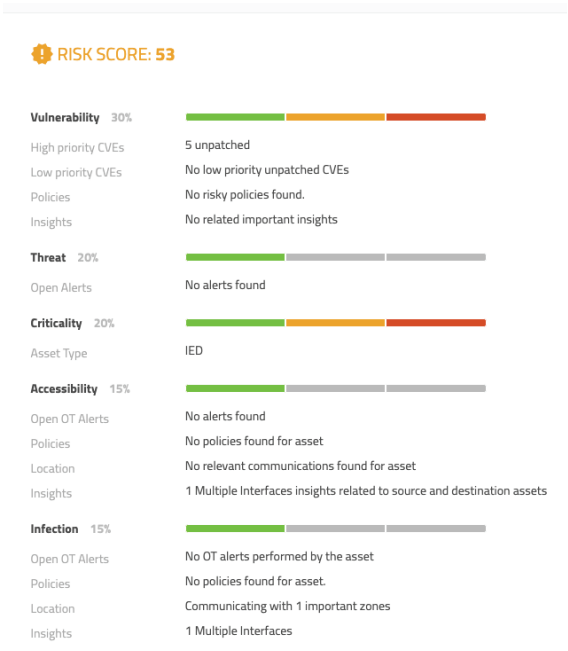
- **資產可視性**：涵蓋工業網路上的所有CPS資產，包含序列網路(serial networks)，以及每項資產的廣泛屬性
- **工作階段可視性**：包括所有工業網路工作階段及其頻寬、採取的動作、所做的變更、連線路徑，以及其他相關詳細資料
- **處理程序可視性**：包括追蹤所有工業營運相關操作，涉及CPS資產的所有處理程序程式碼區段與標記值，以及這些資產製程數值中可能表示對製程完整性構成威脅的任何異常變更

透過Claroty CTD發現的資產機架插槽可視性

弱點及風險管理

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。因此使用者能夠以有效的方式辨識、排定優先順序以及修復工業網路中的弱點。

- **完全符合的弱點**：利用已知的CVE，根據供應商、型號、韌體版本準確比對確切的資產，可以確保漏洞的有效優先順序和修復步驟
- **攻擊向量對應**：透過已知風險的辨識與分析來計算攻擊者最有可能的網路入侵形式，以更進一步了解您的風險現況
- **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

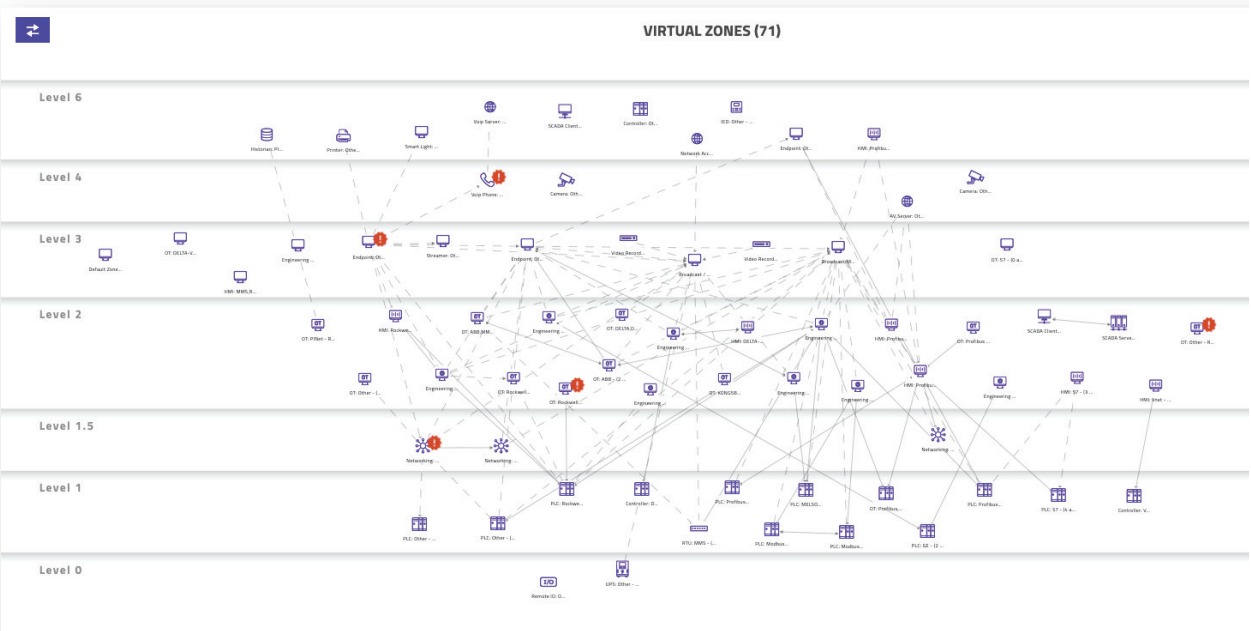


CTD的多重要素風險評分

網路防護

透過Claroty深入的領域專業知識支援，可以利用CTD獨特深入的可視性，將您的工業網路自動虛擬分割為虛擬區域 - 這些區域是在一般情況下會彼此互相通訊的資產邏輯群組。虛擬區域可以配合您環境的獨特通訊路徑量身定製，並提供一般網路行為的完整可視化圖表。虛擬區域有助於：

透過異常通訊警示 進行威脅偵測	提供具有成本效益的解決方案 來取代成本高昂的實體分割方案	將現有的網路通訊基礎結構 延伸到工業環境

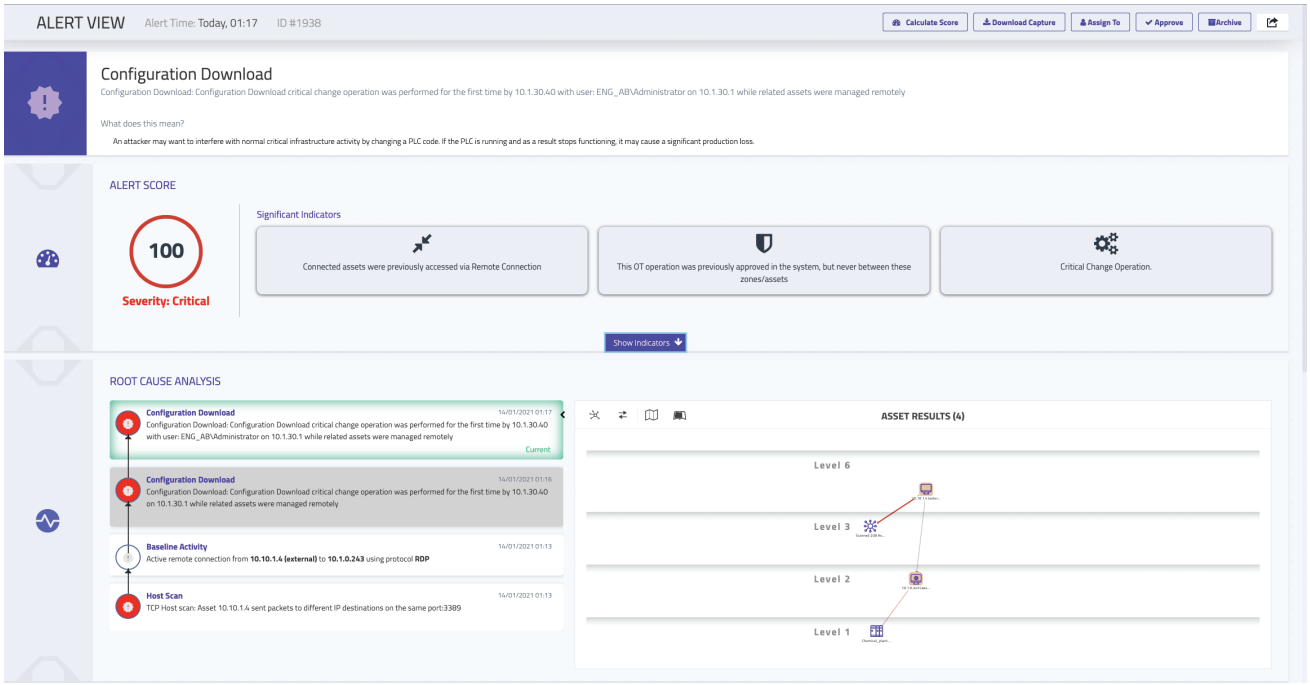


CTD虛擬區域的網路層對應

威脅偵測

對工業網路的威脅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工業網路中的所有資產、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，包含以下產品特性：

- **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

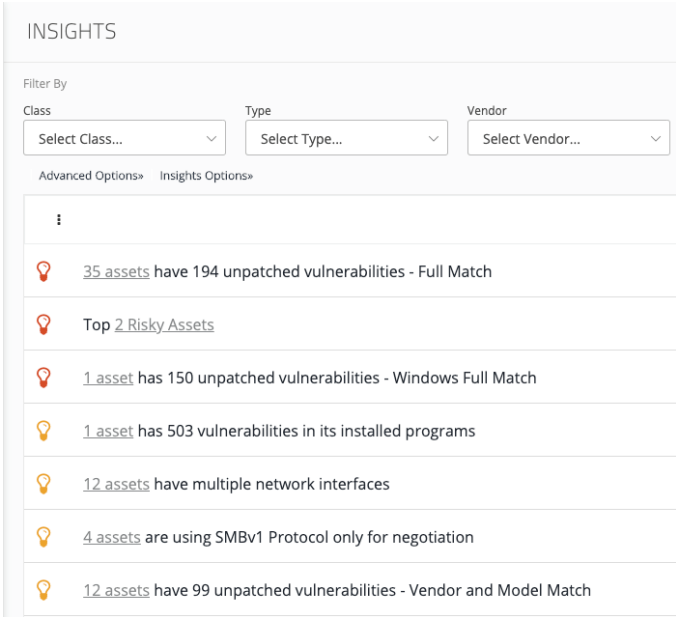


內含關鍵指標、連鎖事件，以及根本原因分析的CTD警示檢視頁面

資產及變更管理

透過可靠與深入的網路可視性支援，Claroty CTD讓企業組織能夠簡化資產及變更管理。透過自訂屬性，生命週期終止見解等指標，營運製程數值的辨識，以及全新、更新或報廢資產的持續監控，CTD讓作業員能夠簡化資產管理工作流程，以節省管理時間並減少作業人員的維護時段。CTD為使用者提供以下作業所需的工具：

- **監控資產更新**：CTD會持續監控弱點、過時軟體、生命週期終止指標，以及其他需要更新的變更，以協助保持資產可用性
- **簡化SLA法務遵循**：CTD可以透過可用性和自訂屬性來簡化特定資產的SLA法務遵循辨識與報告
- **辨識資產變更**：在CTD監控的許多變數中，網路新增、設定變更與異常是支援變更管理程式所監控的其中一部份



依網路風險排定優先順序的CTD安全見解

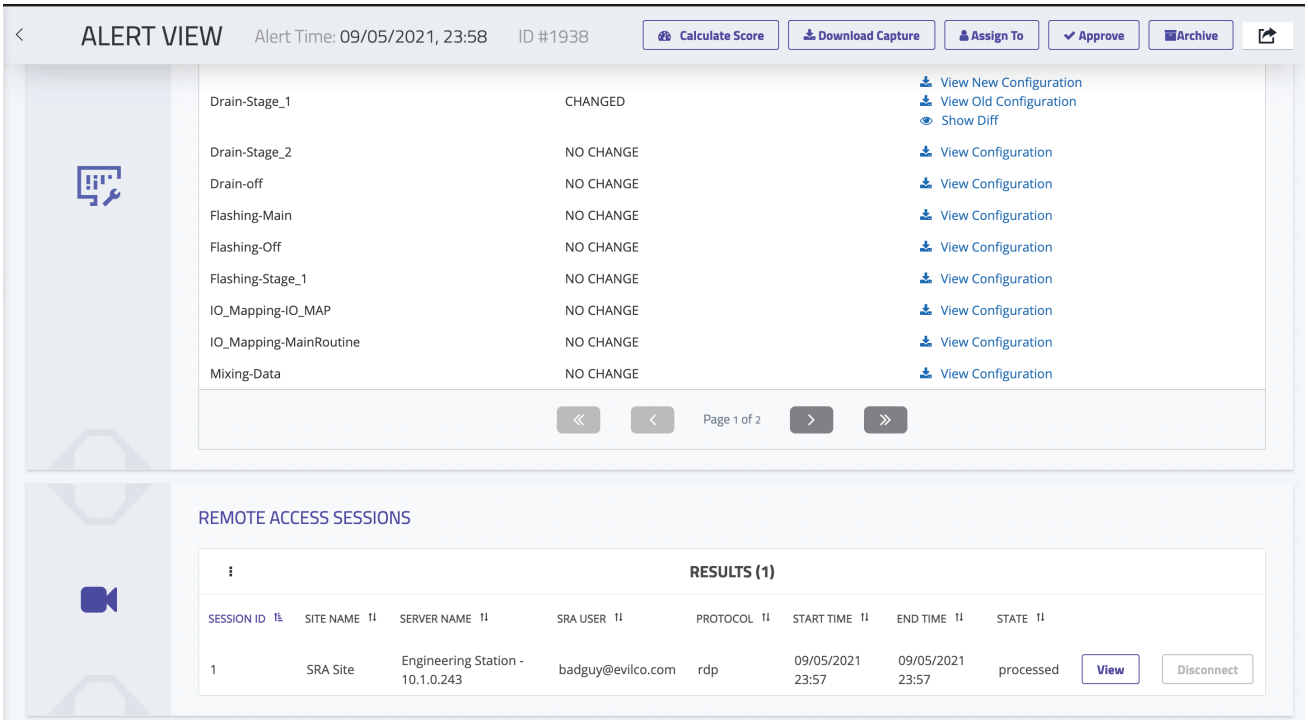
遠端事件管理

CTD和Claroty安全遠端存取(SRA)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



內含變更詳細資料和相關遠端工作階段記錄連結的CTD警示檢視頁面

關於Claroty

Claroty讓工業、醫療保健及商業組織能夠保護其環境中的所有網路實體系統：擴展物聯網(XIoT)。公司的整合平台可以將客戶現有的基礎結構整合，提供可視性、風險和弱點管理、威脅偵測，以及安全遠端存取的全方位控制。

Claroty獲得全球最大的投資公司和工業自動化供應商支援，有數百家企業組織在全球數以千計個站台部署。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。

智慧資安科技股份有限公司

服務專線　04-24523928 分機 300、301、302

電子信箱　servicedesk@unixecure.com.tw

台北據點　114 台北市內湖區基湖路 35 巷 13 號 8 樓

官方網站　facebook