CLAROTY

產品概要

CLAROTY 平台

工業網路安全解決方案

Claroty 平台是一個完整的工業網路安全解決方案，採用 Claroty 的持續威脅偵測(CTD)、安全遠端存取(SRA)以及 Edge 技術。無論其現有網路安全計畫的規模、架構或本質為何，此平台均可和任何工業環境無縫整合。高度靈活和快速部署的選項，讓 Claroty 平台找出並保護網路中的所有營運技術(OT)、物聯網(IoT)和工業物聯網(IIoT)資產，並且透過專利偵測技術自動偵測鎖定這些資產的最初期威脅指標。為了進一步擴大這些控制功能的價值，Claroty 擁有一個龐大的整合生態系統、可靠的 API，並採用業界唯一具有整合式遠端事件管理功能的解決方案，可橫跨整個事件生命週期。

Claroty CTD

- 快速探索和管理所有資產，提供完整的工業網路可視性
- 即時偵測已知和零日威脅及行為和操作異常
- 利用根本原因分析、風險資訊及評價內容自動充實警示
- 找出OT遠端使用者活動和異常事件與惡意指標的關聯性
- 持續監控完全符合的弱點並提供AI導向的網路分區及分割
- 可以採用內部部署，或是透過支援全企業工業網路安全資料管理的軟體即服務選項CTD.Live進行部署

Claroty SRA

- 保護、控制及簡化工業網路遠端存取
- 將遠端及第三方使用者帶來的風險降到最低
- 依照零信任和最小權限的原則執行IT/OT安全最佳實務
- 針對未經授權變更、即時疑難排解，以及緊急中斷連線提供所有OT遠端工作階段的全面監控
- 能夠進行持續稽核供維護、法務遵循和鑑識使用
- 提供高可用性的靈活設定選項，以及目錄服務和防毒解決方案整合

Claroty Edge

- 讓您幾乎即時完全掌握工業環境中所有OT、IoT和IT的資產
- 提高辨識及管理風險和弱點的速度、簡易性和有效性
- 不需要硬體、網路變更、設定，或是任何實體使用空間
- 無論地理位置分布或架構為何，所有網路皆適用
- 協助優化事件回應工作，其中包括影響評估、範圍界定和事件後鑑識
- 立即提供詳細資訊供稽核和法務遵循或併購盡職調查使用

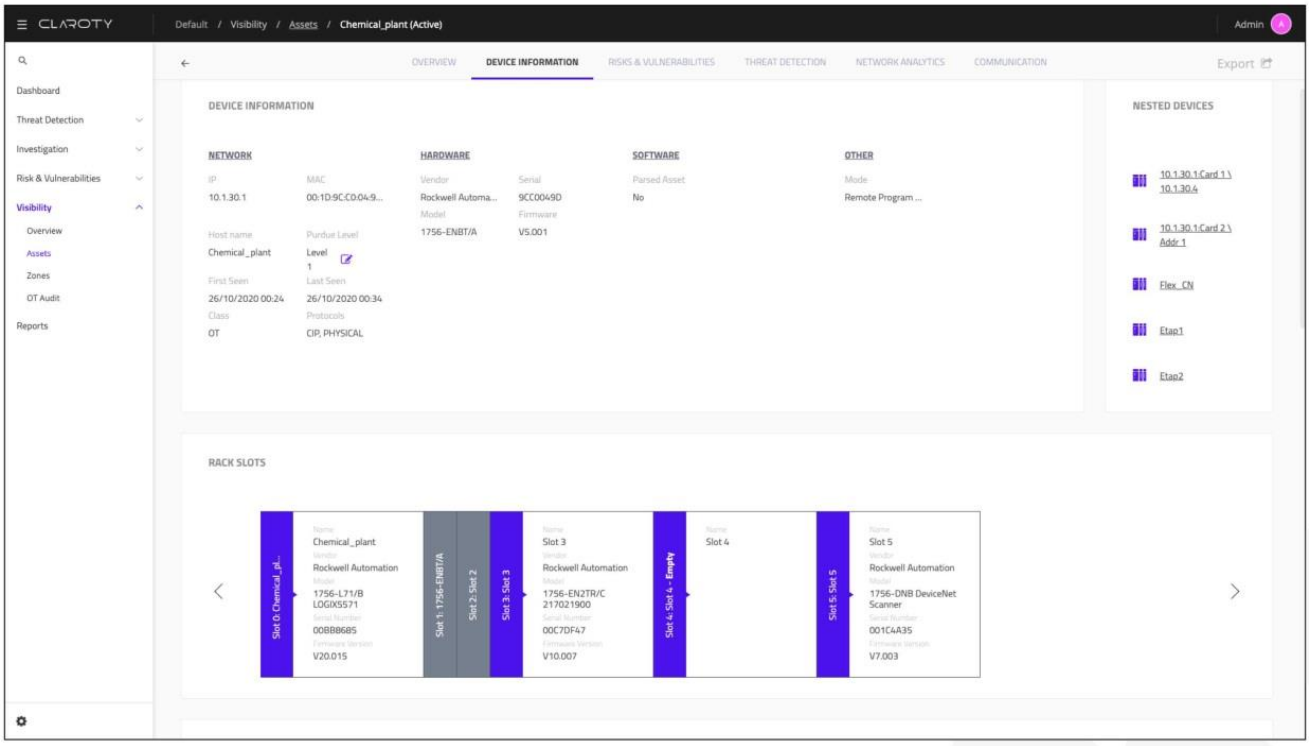
偵測 → 調查 → 回應

利用業界用途最廣泛的工業網路安全控制功能，以及完全整合遠端事件管理功能的組合，在最廣闊的攻擊面保護您的工業環境。

可視性

有效的工業網路安全始於得知需要保護的對象。Claroty 平台支援業界最完整的通訊協定清單，涵蓋的範圍無可比擬，這些可在工業環境中找到的通訊協定，包括專屬和標準的營運技術(OT)、物聯網(IoT)、工業物聯網(IIoT)、建築物管理系統(BMS)以及資訊技術(IT)通訊協定。對網路通訊的深入了解提供無可比擬的資產、網路和處理程序可視性：

- **資產可視性**涵蓋串列網路等工業網路中的所有裝置，以及型號、防火牆版本，以及自訂資產屬性等有關每個裝置的廣泛屬性。
- **網路可視性**包括遠端存取等所有網路工作階段，以及這些工作階段的頻寬、採取的動作、進行的變更和其他相關詳細資料。
- **處理程序可視性**追蹤所有的OT作業和涉及工業資產相關的所有處理程序程式碼區段與標籤值。



CTD 資產詳細資料頁面

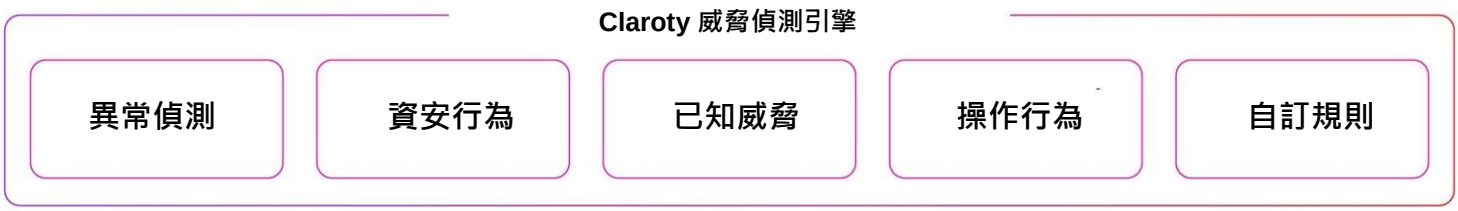
保護

Claroty 平台可以針對存在網路中的固有風險提供見解。這些包括重大弱點和錯誤設定，人員和供應商之中的不良安全實務，以及不可靠、未受監控和缺乏效率的遠端存取機制。不僅可以讓使用者辨識這些高風險區域並排定其優先順序，還可以部署主動式控制和緩解功能來管理網路開放。

- **虛擬區域：**在一般情況下會根據網路通訊進行自動虛擬網路分割，建立具成本效益的實體分割替代方案，並提供對跨區違規的即時警示機制。
- **攻擊方式對應：**辨識並分析工業環境中的弱點與風險，計算攻擊者最有可能以何種形式入侵網路。
- **遠端存取控制：**SRA使用多重要素驗證、以用途和群組為主的階層式存取權限和即時佈建的組合，嚴格控制、監控和簡化對網路的遠端存取。

偵測

Claroty 的彈性威脅偵測模式會剖析工業網路中的所有資產、通訊和處理程序，建立我們五個威脅偵測引擎可利用的精確行為基準。Claroty 平台讓企業能夠在警示出現時快速且有效做出回應，在分秒必爭的情況下提供想要省時所需的內容和資訊。



Claroty 利用最新的威脅情報持續監控已知和未知的威脅、自動去除誤判、將相關警示連結至一系列的事件，以及提供如何在威脅影響營運之前加以緩解的明確方向。

- **情境警示風險評分：**由獨特的演算法所產生的單一指標，提供觸發每次警示的情境脈絡。
- **根本原因分析：**與相同攻擊或事件相關的所有事件均會分成單一警示，提供一系列事件的綜合觀點以及根本原因分析。
- **遠端工作階段監控與稽核：**您可以即時監控OT遠端工作階段，並且輕鬆稽核完整長度的紀錄。

整合

整個企業的互連能力會導致融合式 IT/OT 工業網路的複雜度增加，使攻擊面擴大。Claroty 平台消除了長期限制以安全與高效率的方式連線工業網路處理其他業務的障礙，因此可以透過整合協同作用提升營運效率並降低整體擁有成本：

- **整合生態系統：**Claroty擁有SIEM、SOAR和CMDB解決方案等多種IT安全工具，可以簡化系統管理並縮短工業網路安全的學習曲線。
- **API Explorer：**API Explorer是以Swagger架構建立，讓使用者能夠利用CTD提供的大量網路資訊來建立Claroty環境外的自訂即時摘要。
- **Claroty Edge及CTD.Live：**Edge提供資產和網路風險的立即可視性，搭配CTD.Live的雲端式報告建立功能，有助於連結企業組織的網路安全計畫及其監管、全企業風險及法務遵循計畫。

關於Claroty

Claroty 是一家工業網路安全公司。Claroty 獲得全球最大企業的信任，可以協助客戶找出、保護與管理其營運技術(OT)、物聯網(IoT)和工業物聯網(IIoT)資產。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，全部都可以大幅降低整體擁有成本。Claroty 獲得頂尖工業自動化供應商的支援和採用，擁有龐大的合作夥伴生態系統和獲獎的研究團隊。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，在七大洲均有部署。

與我們聯絡
contact@claroty.com

如需進一步了解，請造訪 **www.claroty.com**。