解決方案簡介

網路實體系統的曝險管理

在持續變化的風險現況中強化 CPS

為了跟上數位轉型的持續發展進度，製造、醫療保健和其他關鍵基礎設施產業的組織必須超越網路實體系統(CPS)的傳統弱點管理，並建立更為廣泛且更加動態的計畫，來管理其整體面臨的風險。

因為 CPS 環境的獨特性質，會需要一種專業的方法，讓這些組織能夠建立一個曝險管理計畫，將資產複雜度、獨特的治理，以及 CPS 環境的企業關鍵營運結果納入考量。這種方法涵蓋一個可重複的週期性措施，以超越修補漏洞或劇本等傳統的方法將安全性最佳化。

曝險管理

Gartner®將持續性威脅曝險管理(CTEM)定義為「讓企業能夠以持續且一致的方式，評估企業數位和實體資產可存取性、曝險程度和可利用性的一組流程和功能」。

Gartner 表示：「在成熟的任何階段，CTEM 週期都必須包含五個必須完成的步驟：範圍界定、探索、排定優先順序、驗證和調度。建立 CTEM 計畫的組織可以利用工具來盤點和分類資產與弱點，模擬或測試攻擊形式，以及其他形式的結構評估流程和技術。重要的是，CTEM 計畫必須為基礎結構團隊、系統和專案所有者提供有效且可據以行動的途徑，以便根據結果採取行動。」[1]

[1] Gartner，實施持續性威脅曝險管理(CTEM)計畫，Jeremy D'Hoinne、Pete Shoard、Mitchell Schneider，2023 年 10 月 11 日。GARTNER 是 Gartner, Inc.及/或其子公司在美國和國際上的註冊商標及服務標誌，並於此獲授權使用。版權所有。

[2] Gartner，如何管理網路安全威脅而非事件，Kasey Panetta，2023 年 8 月 12 日。GARTNER 是 Gartner, Inc.及/或其子公司在美國和國際上的註冊商標及服務標誌，並於此獲授權使用。版權所有。

曝險管理的驅動力

管理 CPS 風險需要更加動態的方法

Claroty Team82 對超過 2000 萬個 CPS 所做的分析顯示，38%風險最高的弱點遭到傳統弱點管理方法忽略，揭露出可能會被惡意攻擊者利用的主要盲點。

僅仰賴以 CVSS 為主的方法存在忽略關鍵曝險和弱點入侵可行性的風險。

確保 CPS 安全的責任已轉移到 IT 部門

在製造和關鍵基礎設施產業部門中，超過 95%的 CISO 正在或即將負責其組織的安全，範圍不僅涵蓋 IT 環境，也涵蓋 CPS 環境，直接影響業務成果。

轉移到曝險管理將有助於把整個組織的所有風險納入考量。

產業及監管壓力

從 PATCH 法案到 FedRAMP 第 5 版，近期的監管發展明確表示，軟體物料清單(SBOM)的透明度是了解供應商供應鏈中嵌入式弱點潛在風險的關鍵。

目前的解決方案缺乏 CPS 專業知識和垂直知識，以驗證完整的攻擊路徑和協助符合法務遵循。

> 38%風險最高的 CPS 遭到傳統弱點管理方法忽略

利用 Claroty 進行 CPS 曝險管理

改採動態曝險管理計畫需要實施更為成熟與策略導向、具備偵測與回應能力的預防控制措施。Claroty 提供一系列的客製化功能來支援 CPS 專屬的曝險管理流程：

範圍界定

儘管 CPS 對業務成果有潛在影響，但通常會遭到安全計畫忽略。Claroty 解決方案是專為網路實體系統所設計，有助於辨識關鍵業務營運和排定其優先順序。

探索

CPS 需要專業知識，才能有效辨識和評估曝險。Claroty 使用多種探索技術來分析 CPS、繪製網路通訊圖，以及找出弱點和其他曝險情況的關聯。

排定優先順序

Claroty 獨特的風險架構、來自 CISA KEV 和 EPSS 的資料摘要，以及多重曝險考量，可以突顯出特定的攻擊媒介，評估可利用性和影響，以及提供量化的修復建議。

驗證

若要確認曝險的可利用性，必須對涉及的 CPS 和環境有深入的了解。Claroty 可以協助驗證 VEX 檔案歸屬於資產的漏洞，以及利用我們和 CPS 供應商的多個 OEM 聯盟。

調度

若要運用這個週期，則需執行在整個過程中收集的見解。Claroty 整合各種企業解決方案並提供詳細的報告，以協助實現無縫的曝險修復工作流程。

Claroty 花費數年的時間，協助數千個組織以更有效的方式和更高的效率強化 CPS 網路風險結構，提供全方位的 CPS 安全解決方案產品組合，為製造和其他關鍵基礎設施產業組織的整體曝險管理發展過程提供支援。請造訪 claroty.com，以進一步了解 Claroty 如何為您的 CPS 曝險管理發展過程提供支援。

關於 Claroty

Claroty 能夠協助組織保護工業(OT)、醫療保健(IoMT)，以及企業(IoT)環境中的網路實體系統：擴展物聯網(XIoT)。公司的整合平台可以將客戶現有的基礎網路架構整合，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，請瀏覽 claroty.com 或傳送電子郵件至 contact@claroty.com。