CLAROTY ICS 風險與弱點半年報：2021 上半年

作者：Claroty Team82

CLAROTY

目錄

執行摘要

2021 年上半年對工業網路安全而言是史上最大的考驗。

許多公司都享受到將設備連到網際網路並在 IT 系統管理下融合營運技術(OT)果實。然而，這樣的趨勢卻向威脅發動者發出了某種信號，尤其是對專門以勒索跟不當獲利為主的威脅發動者而言。當線上暴露的資產數量以飛快的速度成長，隨之而來的就是不斷增加的缺陷與弱點：未修補的弱點、不安全的認證、薄弱的組態設定以及過時的工業協定。

在今年上半年裡，這些共同的缺陷導致了針對 Colonial Pipeline 與 JBS Foods 等引起社會關注的勒索軟體攻擊事件，以及對佛羅里達州奧德馬爾市淨水廠(還有一次在灣區)等令人不敢置信的攻擊事件。這些事件讓工業控制系統與 OT 網路的安全性成為社會的關注點。

美國政府也注意到事件的嚴重性，進而在行政命令、國家安全備忘錄與相關部門中呼籲確保這些系統與網路的安全性，不僅需提高系統所有權人與營運商的危機意識，更強調對 ICS 與 OT 的攻擊可能進一步威脅國家安全與公共安全。

Claroty 今天發布了第三份一年兩次的 ICS 風險與弱點分析報告。此報告是由我們的研究團隊(Team82)對整個 ICS 領域所使用的先進自動化產品，進行弱點定義與分析後所得的結果。Team82 對上半年公開揭露的 ICS 弱點進行全面性了解，其中包括 Team82 所發現的弱點以及受影響供應商、獨立安全研究人員與其他組織內部專家所發現的弱點。

此報告是 OT 安全經理與營運商的重要資源，不僅呈現出工業設備中普遍存在之弱點的相關數據，更提供與其相關的必要情境，讓大家可評估各自環境中所面臨的風險。

讓我們一起來看一年兩次的 ICS 風險與弱點分析報告所呈現的部分關鍵數據點：2021 年上半年：

ICS 安全研究與揭露趨勢

- 在 2021 年上半年，總計公布 **637** 個 ICS 弱點，總共影響 76 家供應商所銷售的產品。在我們的 2020 年下半報告中，總計揭露 **449** 個弱點，總共影響 **59** 個供應商。**70.93%**的弱點被歸類為高度或嚴重，與 2020 年下半年相當。
- Claroty 的 Team82 總共揭露 **70** 個弱點，而這些弱點已在 2021 年上半年修補或緩解。這些弱點總共影響 **20** 家自動化技術供應商。
- 在 2020 年下半年，Team82 揭露了 **41** 個弱點，總共影響 **14** 家供應商。
- 2021 年上半年揭露的弱點中有 **80.85%**由受影響供應商以外的外部來源所發現，其中包括研究組織、包括第三方公司、獨立研究人員與學術界等。

- **42** 位新研究人員揭露了於 2021 年上半年公布的弱點。新的研究人員主要專注於引領市場的自動化供應商，同時也發現四家新受影響的供應商。

- 在受影響的供應商中，Siemens 被公布的弱點數量最多，總共 **146** 個，其中許多弱點是由 Siemens CERT 所進行之內部研究而揭露的。

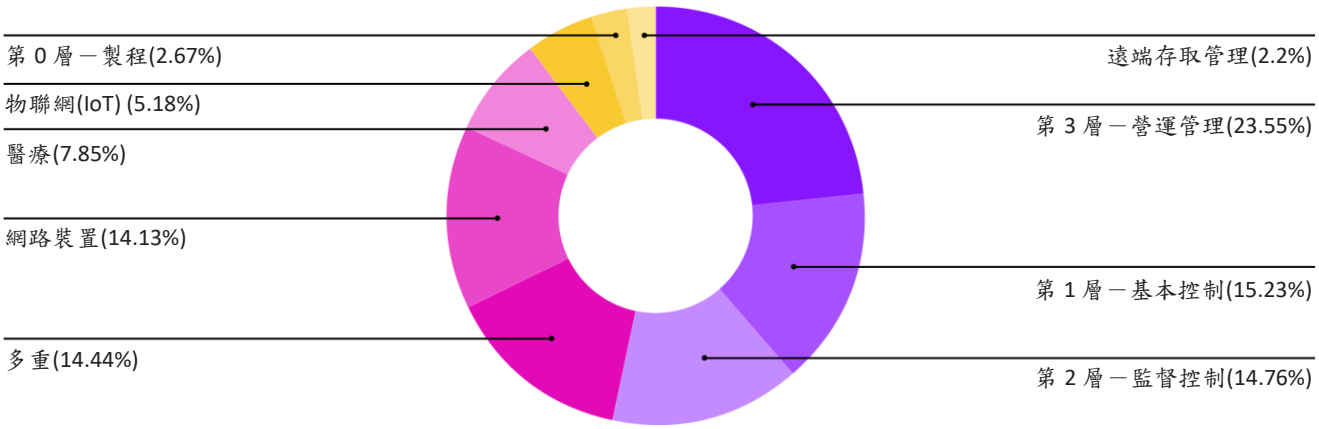
- 總計有 **20** 家在 2020 年時產品未受 ICS 弱點影響的供應商於 2021 年上半年至少揭露了一項弱點。

來自 ICS 弱點的威脅與風險

- 2021 年上半年揭露的最大弱點比例影響到普渡模型的第 3 層：營運管理(23.55%)，其次是第 1 層：基本控制(15.23%)與第 2 層：監督控制(14.76%)。

  營運管理可以成為融合式 IT 網路的關鍵交點。這些系統包括對生產工作流程至關重要的伺服器與資料庫，或者將所收集的數據饋送到更高階商業系統的伺服器與資料庫，而且部分系統將在雲端執行。基本控制級別是可程式化邏輯控制器(PLC)、遠程終端裝置(RTU)與其他監控級別為「0」之設備(例如泵、致動器、感測器等)的控制器。監控級別是人機界面(HMI)、SCADA 軟體以及其他負責監控與處理第 1 層之數據的工具。

受影響的產品系列



- 守衛者必須了解威脅發動者可能會採取哪些攻擊方式來破壞工業網路，這一點至關重要。對潛在弱點的適當可視化有助於組織排列修補工作及其他風險管理活動的優先順序。我們的數據集中在兩個主要的攻擊方式上：遠端與本機。

  可被遠端利用的弱點：Team82 的數據顯示，**61.38%**的安全弱點讓來自 IT 或 OT 網路外部的攻擊得以進行；該數字低於 2020 年下半年，當時有 **71.49%**可被遠端利用。

  本機攻擊方式：另一方面，可被本機攻擊方式利用的弱點從 2020 年下半年的 **18.93%**上升到 **31.55%**。對於 **72.14%**的弱點，攻擊者仰賴使用者互動來執行利用這些弱點所需的操作，例如透過垃圾郵件或網路釣魚進行社交工程。進一步剖析：

  - 在透過本機攻擊方式利用的營運管理弱點中，有 **94.38%**需要使用者互動才能進行。因此防止網路釣魚與垃圾郵件以及阻擋勒索軟體與其他潛在破壞性攻擊之技術的需求開始上升。
  - 對於 **39.87%**屬於本機攻擊方式的弱點，因不需使用者互動，故其複雜度較低。攻擊者可期待每次都能複製此成功方程式，且不需要可存取目標設定或檔案的權限。

- 總計有 **65%**的弱點極可能導致可用性完全喪失。

- 由於許多已知的原因，更新工業控制系統或 SCADA 軟體的挑戰性通常很大，主要與正常運作時間及可用性要求有關。由於開發與執行更新所涉及的複雜性，韌體更新也很困難。這些週期需要的時間可能比傳統的 IT 修補管理更長，且通常導致緩解措施成為守衛者能採取的唯一補救選項。

  緩解與補救措施：Team82 的數據與這些趨勢相關。

  - 2021 年上半年揭露的 637 個 ICS 弱點中有 **25.59%**沒有進行修復或僅部分補救。
  - 在未補救或僅部分補救的弱點中，**61.96%**存在於韌體中。
  - 在未補救或僅部分補救的弱點中，**55.21%**可能導致遠端程式碼的執行，**47.85%**在被成功利用時可能導致拒絕服務的情形。
  - 在已補救的 **74.4%**弱點中，**59.49%**需要進行軟體修復。
  - 總計 637 個弱點中有 **6.43%**影響到不再受支援且生命週期已終止的產品，這表示該產品應該被取代。如果無法進行翻修與更換，則應採取任何受推薦的緩解措施。
  - **51.22%**影響生命週期已終止之產品的弱點是在韌體中發現的。

趨勢觀察

在我們深入探討 Team82 2021 年上半年弱點揭露數據中的數字前，了解至少未來六個月內可能產生影響的三個主要趨勢非常重要：OT 雲端搬遷、針對關鍵基礎設施與 OT 的無情勒索與勒索軟體攻擊，以及即將實施的美國網路相關法規。

OT 雲端搬遷

無可否認，目前的趨勢正驅使企業將雲端導入工業流程中。這麼做可為企業提供許多重要益處，包括：

- 更好的遙測與設備效能分析
- 邏輯與遠端設備配置管理
- 診斷與故障排除的改善
- 關於流程的集中視圖
- 備援(對持續營運至關重要)

這是數位化轉型的一體兩面，當企業開始從雲端管理 OT 與 IT 時，這樣的融合將帶來許多共同風險。

OT 曾是離線不上網的，但現在將連接到雲端，並為攻擊者提供更大的可攻擊面。隨著將雲端導入 OT 中的組織不斷增加，對威脅發動者而言可能是一個機會，他們將可針對因大規模連網而突然暴露的弱點進行攻擊。這對試圖影響工業營運的勒索軟體與勒索式攻擊而言可能是好消息，即使在 Colonial Pipeline 與 JBS Foods 的案例中亦然。

數據安全曾經是工業流程中風險較小的變數，現在也將被視為優先事項，尤其是在不容許出錯且監管嚴格的產業中。組織不僅須評估威脅，也必須評估風險，例如缺乏支援加密與身份驗證的協定等。

例如，加密可能會使某些工具無法完全存取網路資產。在離線環境中，這被視為可接受的風險，但是一旦資產在網路上公開，情況就不同了。最好的做法是，數據應在傳輸過程中加密，並在靜止時也加密，以確保在發生事故時可進行充分的復原。隨著企業開始將諸如 Historian 資料庫等服務與應用程式置於雲端，並從 PLC 等第 1 層的設備接收數據，這一點尤其明顯。

身份驗證與身份管理也必須納入組織的雲端 OT 縱深防禦計畫。COVID-19 疫情加速了遠距工作的普及，而 2 月的奧德馬爾市事件已證明對系統存取與權限管理的控制不足所產生的風險。

解析雲端：遷移到以雲端為基礎的架構通常代表著組織的部分基礎架構(IT 或 OT)由第三方雲端服務提供商(如 Google、Amazon 與 Microsoft)的遠端伺服器託管。基礎架構包括一個雲端的管理平台，以支援組織所提供之服務的不同使用者，例如管理員或工程師。以使用者與角色為基礎的規範必須定義使用者可以執行的功能以及其角色所擁有的權限。

雲端運算分為三種類型：公共、私有與混合。

- **公共：**由多個組織與資源共享的雲端運算透過網際網路執行。
- **私有：**屬於單一組織專有的雲端運算。可位於本機或由第三方提供商託管並在私有網路上維護。
- **混合：**結合公共雲與私有雲的雲端運算。可允許在兩個環境之間移動數據與服務。

當提到 OT 雲端時，這些概念仍然適用。操作員與管理員可以透過管理平台更改設定、編輯組態與管理工廠網路。

OT 網路遷移到以雲端為基礎的架構需要網路連線，並在由雲端管理控制台所管理的所有站點上建立單一控制點。現在一個簡單的弱點(例如身份驗證過程中缺少驗證權杖)可能就讓攻擊者接管可存取所有設備的雲端管理控制台。IT 資訊安全中常見的弱點也成為 OT 的安全挑戰。

勒索軟體與勒索攻擊

雖然我們還沒看到專門攻擊第 1 層之設備的勒索軟體，但威脅發動者已成功對工業營運產生衝擊。Colonial Pipeline 即為一個明顯的例子，在 IT 系統(而不是 OT)被勒索軟體感染後，該公司謹慎地關閉了美國東岸的燃油輸送管線。

現在的攻擊者在使用勒索軟體時已變得更加狡猾，並積極尋找他們認為最有可能支付高額贖金的受害者。雖然政府機關、醫療院所與學校曾被認為是威脅發動者喜愛的目標，但大型製造業與民生必須的公共事業現在反而處於虎口當中。

圖謀不當利益之威脅發動者的另一種策略為：以高級的手法盜取機密性業務或客戶資料，並以公開揭露此資訊或讓關鍵系統感染勒索軟體等方式來威脅受害者。亦即，威脅發動者主要瞄準可滿足其要求的高價值組織，因此讓企業倍感威脅。據了解，Colonial Pipeline 與 JBS Foods 都支付了數百萬美元的加密貨幣給威脅發動者，以恢復其加密系統。

隨著越來越多企業將 ICS 設備連接到網路並融合 OT 與 IT，網路資產的可視化將變得至關重要，且可能被攻擊者利用之軟體與韌體弱點的相關訊息也同樣重要。例如，在採用 Windows 系統的機器上所執行的工程工作站中，其缺陷可能讓攻擊者得以破壞 IT 與 OT 網路之間的交點並修改流程，甚至投放勒索軟體並阻礙攸關公共安全的關鍵服務或國家安全。

除了可進行網路釣魚攻擊的電子郵件外，守衛者亦需關注遠端存取的安全以及在虛擬私有網路與其他網路攻擊方式中所發現的弱點。Team82 的數據顯示超過 60%的弱點可透過網路攻擊方式進行遠端利用。這強調了保護遠端存取連線與網路 ICS 設備的重要性，且必須在攻擊者能跨網路或網域移動並竊取數據甚至投放惡意軟體(例如勒索軟體)前切斷攻擊。

美國網路相關法規待審中

從 2021 年上半年在奧德馬爾市、Colonial Pipeline 與 JBS Foods 發生的攻擊事件來看，當關鍵基礎設施與製造業暴露在網路上時是非常脆弱的。這些攻擊事件證明攻擊者能夠找出弱點並改變公共飲水中的化學物質濃度，或運用勒索軟體關閉燃油與食品配送系統。

此一針對 OT 的惡意攻擊事件引起晚間新聞與其他主流媒體的注意，同時也喚醒了美國政府。許多由政府支持的網路相關活動更指出工業網路安全對國家安全與美國經濟至關重要。

拜登總統於 7 月簽署了一項關鍵基礎設施的國家安全備忘錄，此備忘錄提出了工業控制系統的網路安全倡議，目的在使民間業者與營運商能自願努力讓其系統具備抵擋當前威脅的能力。美國政府將在 9 月前訂出績效目標，而這些自願性的努力將不可避免地讓可提供 OT 網路與威脅檢測可視化的技術成為強制部署項目。

此備忘錄主要依循在 5 月份簽署行政命令，旨在改善民營企業與政府機關之間的威脅訊息共享、促進聯邦政府網路安全標準的現代化、強化供應鏈安全、建立網路安全審查委員會、建立一套應對網路攻擊事件的標準方針、改進對聯邦政府網路之攻擊的偵測能力並提升其調查與補救的能力。

在此之前已進行為期 100 天的補強工作來改善電網網路安全，此一補強工作的主要目標亦包括改善民營公共事業與政府之間的訊息共享。透過 TSA，拜登政府也對 Colonial Pipeline 事件做出強烈反應，並發布一項安全指令，要求提高管線網路的韌性，包括在偵測到攻擊事件後 12 小時內務必進行通報、定期執行弱點評估以利防範勒索軟體攻擊。

正如我們所期待的，在此攻擊事件發生後，華盛頓的法案草案納入了強制通報的要求。我們也必須保持謹慎與耐心，方能確保這些指令的任何一項都不會對資源相對不足的小型公用事業營運商或關鍵基礎設施營運商帶來額外的風險或不切實際的要求。

政府必須在「識別並消除威脅發動者的目標」與「對接受輔導與補助而受益之企業的監督」之間求取平衡。政府也必須了解 OT 弱點管理的現實面，以及在高可用性環境中修補工業設備的挑戰，或者更新過去幾十年來都不需連網或升級的設備所面臨的挑戰。

這是關鍵基礎設施的動態守衛者必須面對的問題，而美國政府必須了解這一點，以確保在缺乏即時修補選項時或在完整軟體或韌體更新發布前，守衛者可以獲得所需的緩解措施。

關於 Claroty TEAM82

Claroty 的 Team82 是一個屢獲殊榮的營運技術(OT)研究團隊，以其開發的專利 OT 相關威脅特徵碼、OT 通訊協定分析以及探索與揭露工業控制系統(ICS)弱點而聞名。Team82 致力於強化 OT 安全並擁有業界規模最大的 ICS 測試實驗室，而且與頂尖的工業自動化供應商密切合作以評估其產品的安全性。

到目前為止，Team82 已經發現並揭露超過 **150** 個 ICS 弱點，其中有 **70** 個是在 2021 年上半年間所揭露。這個數字超過了 Team82 在 2020 年全年的揭露數量。根據第三方研究機構所揭露的訊息，Claroty 也有一項產品存在弱點，而此弱點已透過私下揭露，修補程式與補救建議已於 6 月份發布。

Team82 意識到，對於了解 ICS 風險與弱點情境的迫切需求，以及 Claroty 研究人員發現的弱點在該情境中的重要性，因此開發了一套自動化收集與分析工具，可以從可信任的公開來源中提取 ICS 弱點資料，這些公開來源包括國家弱點資料庫(NVD)、工業控制系統電腦緊急應變團隊(ICS-CERT)、CERT@VDE、MITRE，以及工業自動化供應商 Schneider Electric 與 Siemens。

這套工具的輸出結果可以揭露與 ICS 弱點相關的關鍵趨勢和歸納後的含意、這些弱點對工業網路造成的風險，以及除了其他屬性以外在不同供應商、產品、地理位置、時間間隔、危險性分數和影響等的變化。這些輸出結果是這整篇報告中研究和分析的基礎。

第 1 部分：CLAROTY 發現並於 2021 年上半年所揭露的 ICS 弱點評估

Team 82 在 2021 年上半年發現並揭露了 70 個弱點，超過 Claroty 在 2020 年揭露的弱點數量。總體而言，Team82 已經揭露 150 多個影響 ICS 設備與 OT 協定的弱點。

Team82 的工業控制系統研究著重在多個參數上，以便為 ICS 領域與產業安全提供最大的益處和貢獻。Team82 與供應商與合作夥伴保持密切聯繫，並接獲與特定產品與版本相關的輸入與要求。團隊的部分研究參數包括：

- 平台、裝置或設備的共通點
- 在供應商修補產品的某個弱點之前，攻擊者發現和利用該弱點的潛在損害
- 多少數量的裝置會受到弱點影響
- Claroty 客戶所使用的產品

Team82 的研究檢查影響業界許多部門的各種供應商和產品。由於這些參數，Claroty 也研究第三方產品。Team82 在 2021 年上半年所發現的 70 個弱點影響了 20 家自動化技術供應商。受影響的供應商與 ICS 產品類型如下列兩個圖表所示：

1.1. 受影響的 ICS 供應商

受 Team82 在 2021 年上半年揭露之 70 個弱點所影響的 20 家自動化技術供應商。

供應商

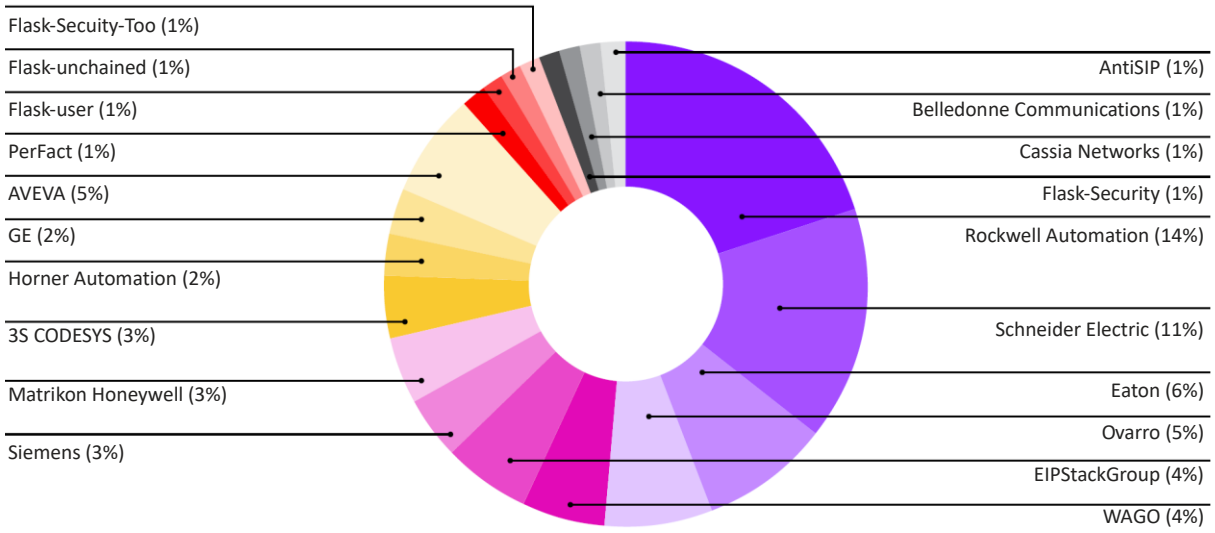


圖 1.1：受 Team82 揭露所影響的供應商分類。

1.2. 受影響的 ICS 產品類型

Team82 揭露的弱點主要在普渡模型的第 3 層：營運管理，以及第 2 層：監督控制。

目標產品系列

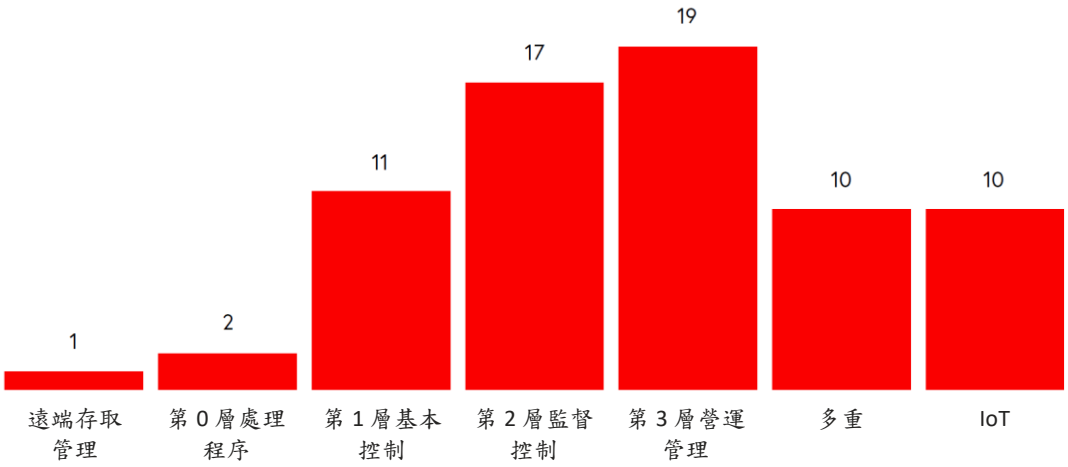


圖 1.2：按產品系列類型區分 Team82 所發現的弱點。

第 2 部分：2021 年上半年所揭露的所有 ICS 弱點評估

本節提供 2021 年上半年所發布所有工業控制系統弱點的統計分析與情境評估。

以下數據包含 Team82 發現與揭露的弱點，以及其他研究人員、供應商與第三方機構在 2021 年上半年公開揭露的所有弱點。Team82 的訊息來源包括：國家弱點資料庫(NVD)、ICS-CERT、CERT@VDE、Siemens、Schneider Electric 與 MITRE。

2.1. ICS 弱點總數

2021 年上半年發布了 637 個 ICS 弱點，總共影響 76 家 ICS 供應商：

已發布的弱點

637

已識別的弱點總數

受影響的供應商

76

受影響供應商總數

2.2. 2021 年上半年弱點發現的來源

在 2021 年上半年所揭露的弱點有 **80.85%** 是由受影響供應商以外的外部來源所發現。外部來源包含許多研究組織，其中包括第三方公司、獨立研究人員與學術機構等。

弱點研究來源

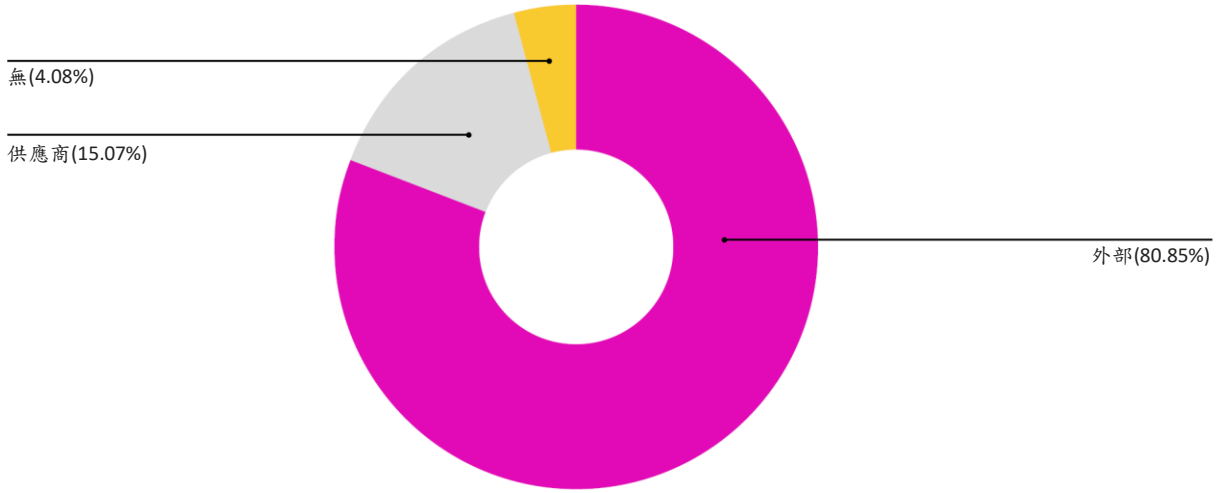


圖 2.2a：弱點依發現來源的分類。

下圖將外部來源(以第三方公司為主)所揭露的弱點數量分類，其中有 **341** 個弱點**(53.87%)**是在 2021 年上半年發現。這些發現的弱點有許多是由網路安全公司的研究人員發現，表示研究範圍擴大到包含工業控制系統以及 IT 安全研究在內。值得一提的是，部分的揭露資訊是多個研究團體之間合作，其他則是不同研究人員分別發現與揭露相同的弱點(這在 2021 年上半年就佔了 **139** 個弱點)。

研究團體

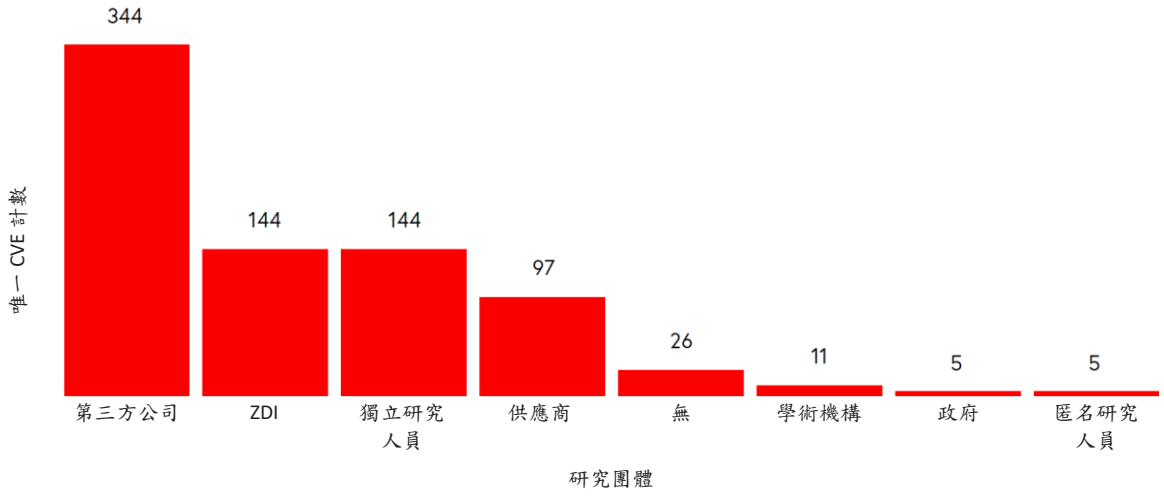


圖 2.2b：發現的弱點依研究團體分類。

請注意與研究人員合作並為零日弱點報告提供獎金的第三方公司零日計畫(ZDI)所揭露的弱點數量。如下所示，2021 年上半年透過 ZDI 進行的揭露數量是 2020 年全年的兩倍多。在 2021 年上半年，22.6%揭露的弱點與 ZDI 有關，較往年大幅增加：

- 在 2021 年上半年，所揭露的 ICS 弱點有 **22.6%**與 ZDI 有關
- 在 2020 年全年，所揭露的弱點有 **11.08%**與 ZDI 有關
- 在 2019 年全年，所揭露的弱點有 **12%**與 ZDI 有關
- 在 2018 年全年，所揭露的弱點有 **16.81%**與 ZDI 有關

Team82 亦指出，2021 年上半年有 42 名新研究人員發布弱點，下圖數據將新進入者按類型區分。

Team82 的資料也指出，新進研究人員鎖定 Rockwell Automation、Schneider Electric、Siemens 等引領市場的供應商。在這 42 位新進的研究人員中，有 **4** 位在 2021 年上半年發現 4 間新受到影響的供應商。其他人則主要檢視過去曾受影響的供應商。應該注意的是，ICS 與 SCADA 設備跟軟體可能很難取得且成本高昂，尤其對新進研究人員而言。這也可能是大家專注於引領市場的供應商的原因之一，因其產品較容易取得。

僅限新研究人員

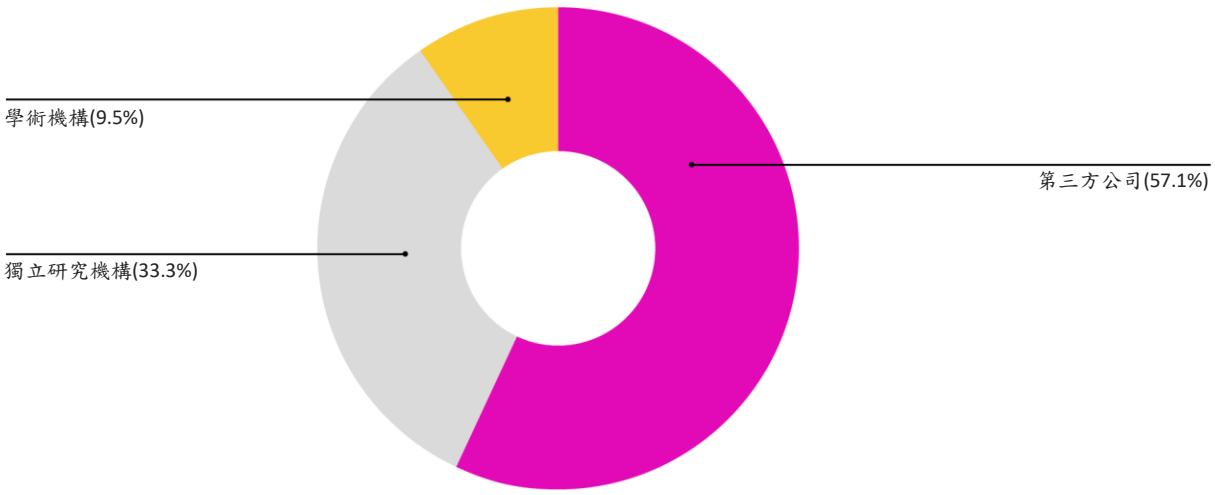


圖 2.2c：回報 ICS 弱點的新進研究人員分類。

2.3 受影響的 ICS 供應商

2021 年上半年揭露的 **637** 個 ICS 弱點影響了 **76** 家供應商的產品，受影響的供應商數量較 2020 年下半年增加，當時僅有 **59** 家受影響供應商，而 2020 年上半年有 **53** 家受影響。

在受影響的供應商中，Siemens 被公布的弱點數量最多，總共有 146 個，其中許多弱點是由 Siemens CERT 所進行之內部研究而揭露的，其次是 Schneider Electric、Rockwell Automation、WAGO 與 Advantech。

非常重要的是，會受到大量已揭露的弱點影響，不一定表示供應商的安全結構薄弱或研究能力有限。配置大量資源來測試其產品安全性的供應商，和忽略對其產品進行相同程度檢查的供應商相比，發現更多弱點的可能性較高。每個供應商的年代、目錄與現有數量，對於影響其產品的已揭露弱點數量往往也會有影響。

前 5 名受影響的供應商

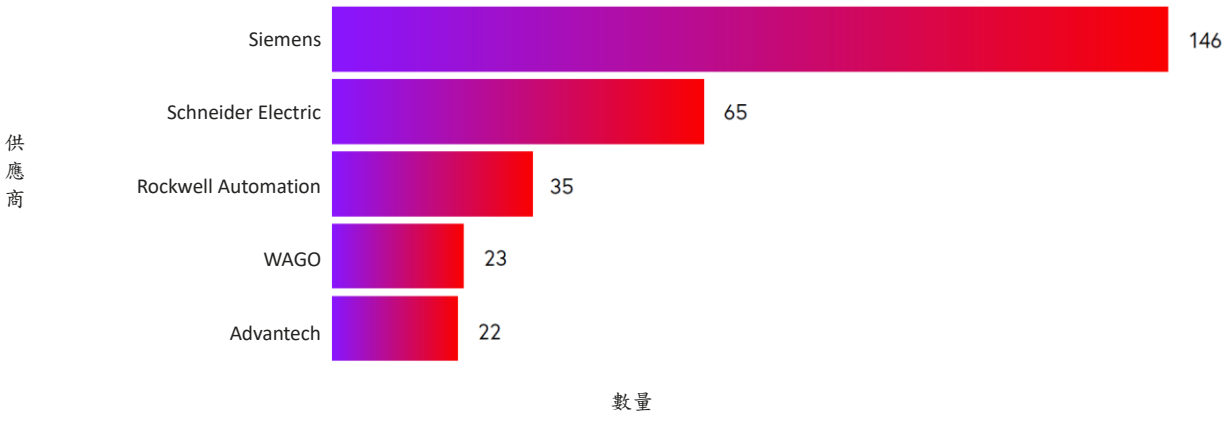


圖 2.3a：前 5 名受弱點影響的供應商。

2.4 2021 年上半年首次被揭露弱點的 ICS 供應商

在 2021 年上半年，產品並未受到 2020 年所揭露 ICS 弱點影響的 20 家供應商，受到至少一個 2021 年上半年所揭露 ICS 弱點的影響。

- 其中 6 家供應商專注於醫療技術，3 家專注於自動化，兩家專注於製造
- 在這些新受到影響的供應商(20 家中的 16 家)中，會對其造成影響的弱點是由先前揭露弱點的研究人員所發現

供應商	主要產業
Claroty	工業網路安全
ThroughTek	IoT 與 M2M 監控解決方案
AGG Software	數據採集、數據記錄與監控軟體
ZOLL	醫療
Hillrom	醫療
GENIVI Alliance	汽車
Mesa Labs	醫療
Datakit	CAD 數據交換
Unified Automation GmbH	工業自動化
Cassia Networks	藍牙 IoT
EIPStackGroup	開源乙太網路/IP
JTEKT Corporation	汽車
Ovarro	工業自動化
Weintek	工業自動化
PerFact	資訊技術
Luxion	照明技術
Hamilton Medical AG	醫療
Hilscher Gesellschaft fur Systemautomation mbH	製造
SOOIL Developments Co. Ltd.	醫療
Innokas Medical	醫療

2.5 受影響的 ICS 產品

韌體/軟體

針對每個揭露的弱點，我們將容易受到攻擊的元件標記為韌體或軟體。在某些情況下，弱點會同時影響包含韌體與軟體的多個元件。在 2021 年上半年，多數弱點都會影響軟體元件，但軟體相對於韌體較容易修補，因此守衛者能夠在其環境中優先進行修補。

韌體/軟體

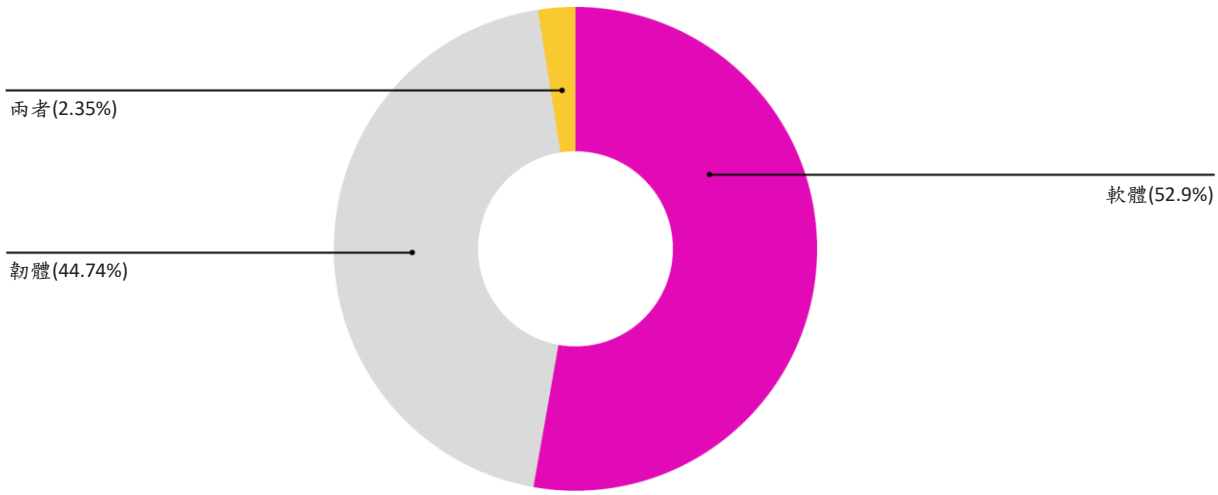


圖 2.5a：軟體與韌體中的弱點分類。

產品系列類別

在檢測產品系列中的韌體和軟體弱點時，還有更值得注意的部分。必須了解的是，雖然弱點是在可以歸類為韌體或軟體元件中找到，但我們必須考量受到這些弱點影響的產品。例如，可能有容易受到攻擊的軟體設定在人機介面(HMI)上執行，或是有乙太網路模組連接到泵浦。下圖顯示受到這些弱點影響的產品系列，其類別如下所示：

受影響的產品系列

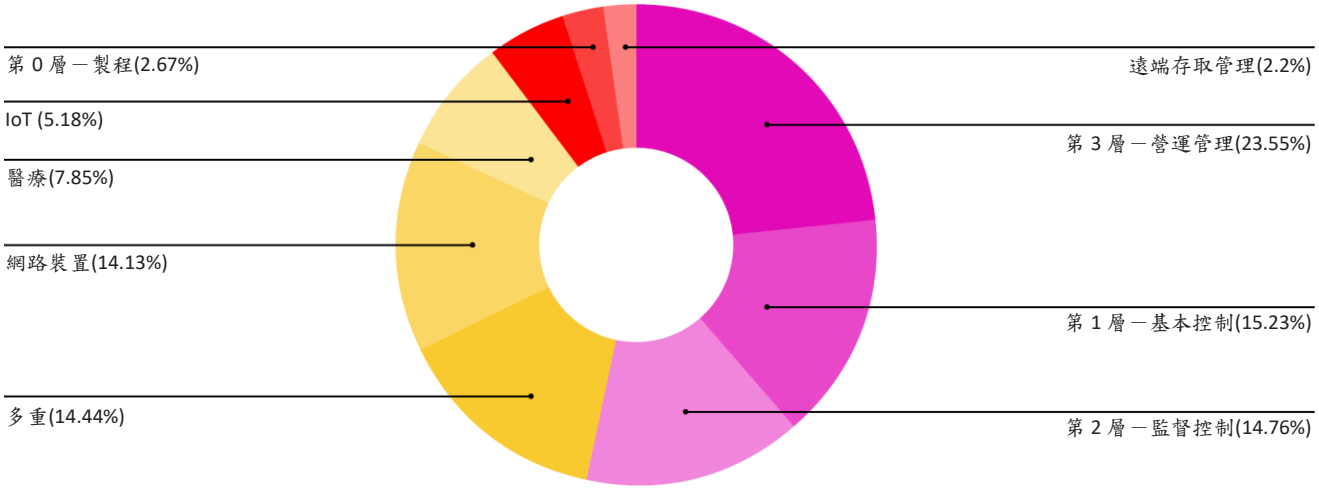


圖 2.5b：受影響產品系列分類。

由於 **23.55%**的弱點會影響普渡模型的營運管理(第 3 層)級別，以下解釋為什麼我們看到許多弱點影響軟體元件。在所發現的弱點中，有 **30%**會影響普渡模型的基本控制(第 1 層)與監督控制(第 2 層)。當然，在影響這些等級時，攻擊者也會接觸較低等級並影響製程本身，讓這些等級成為具有吸引力的目標。

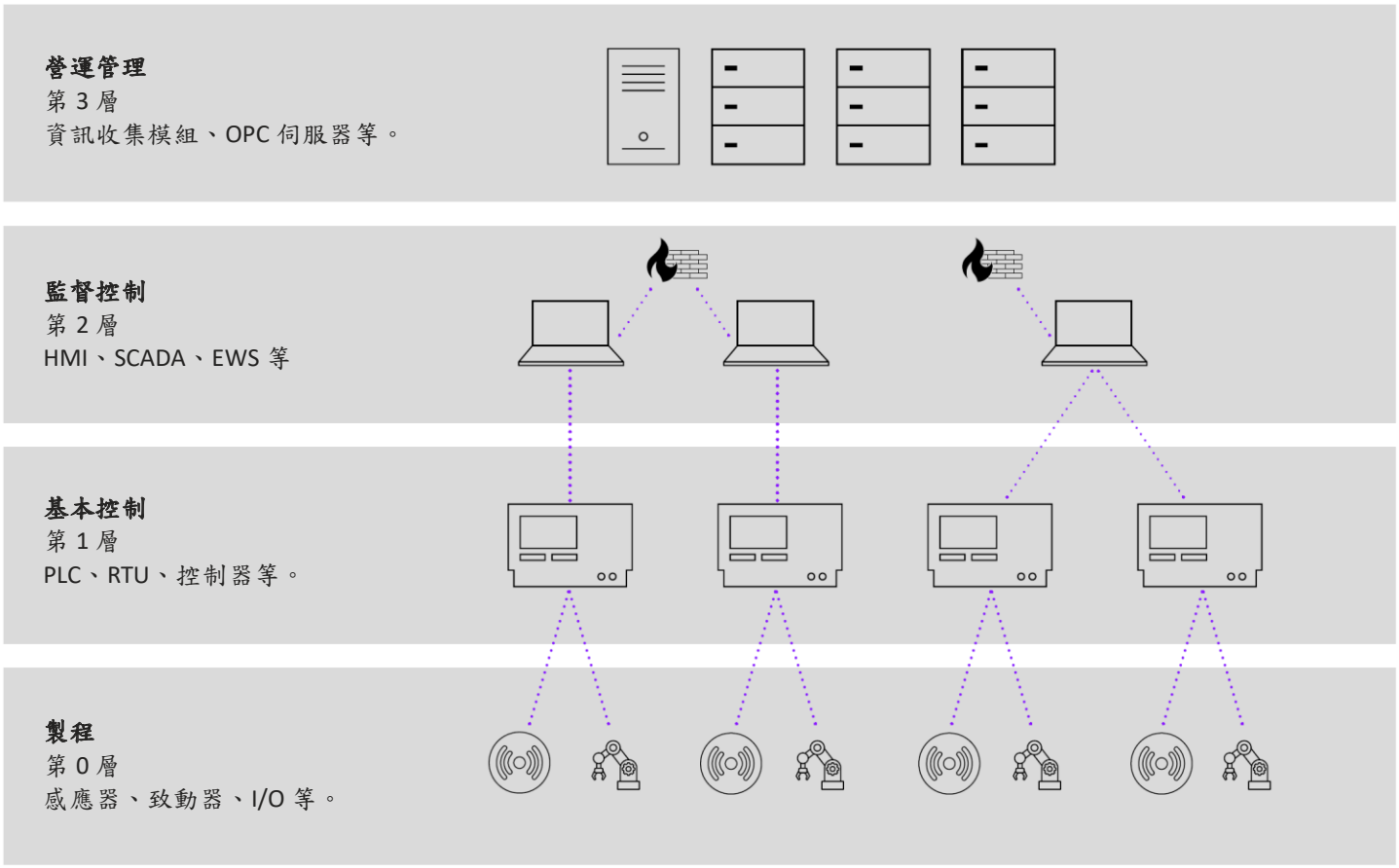


圖 2.5c：工業控制系統的普渡模型 0 - 3 層。

我們需注意圖 2.5b 中的多重類別——此類別主要包含第三方元件弱點(在過去一年中有很多這樣的弱點)，通常在每次的揭露中這部分都包含許多個弱點。它們通常會影響許多供應商與產品，所強調的是針對第三方弱點採用的防護與緩解措施(從可視性與風險評估開始)，這是 OT 網路安全中不可或缺的一部份。

在研究每個類別時，您可以將容易受到弱點影響的元件區分為韌體、軟體或兩者。相較於基本控制(第 1 層)的弱點是以韌體為主，營運管理(第 3 層)與監督控制(第 2 層)的弱點大多數是以軟體為主。由於無法隨時修補，特別是第 1 層裝置韌體中的弱點，所以建議投資在分區隔離、遠端存取防護，以及監督控制等級的防護，因為如此可以直接和基本控制等級連結。

產品系列中的韌體/軟體部分

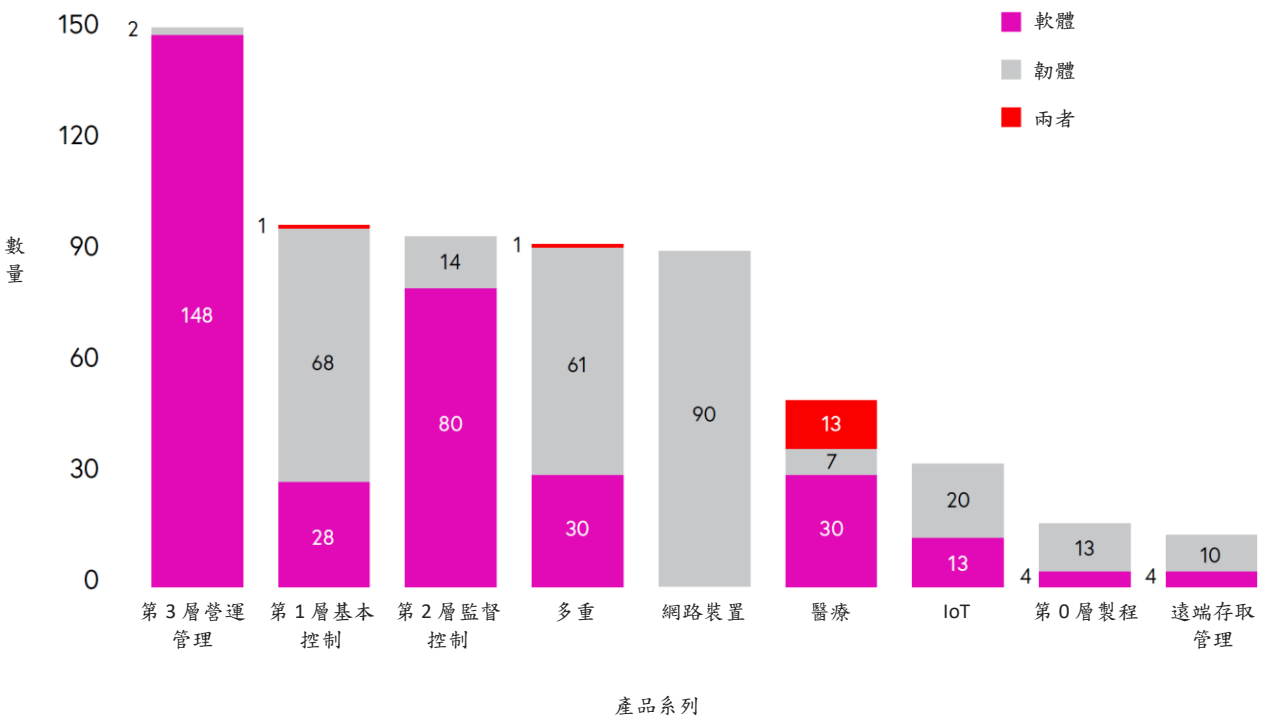


圖 2.5d：韌體與軟體的弱點依產品系列分類。

第 3 部分：緩解與補救措施

3.1 緩解

考慮到我們之前描述的軟體與韌體修補挑戰，緩解措施通常是唯一可開放給守衛者的補救措施。然而，儘管守衛者主要仰賴緩解措施，ICS-CERT 對供應商的建議或警示有時卻缺乏相關的縱深防禦建議。

關於採取行動的建議(例如阻擋特定連接埠或更新過時的協定)很重要，但應該注意的是，在這些建議生效前，基本工必須先做好。

Team82 關於主要緩解步驟的數據(如下)證實了這一點。例如，網路分區隔離與遠端安全存取是最重要的兩個步驟，其重要性優於我們列表中的其他選項(包括流量限制、以使用者與角色為基礎的規範以及最小權限原則)，因此守衛者應該優先考慮這兩個步驟。

主要緩解步驟

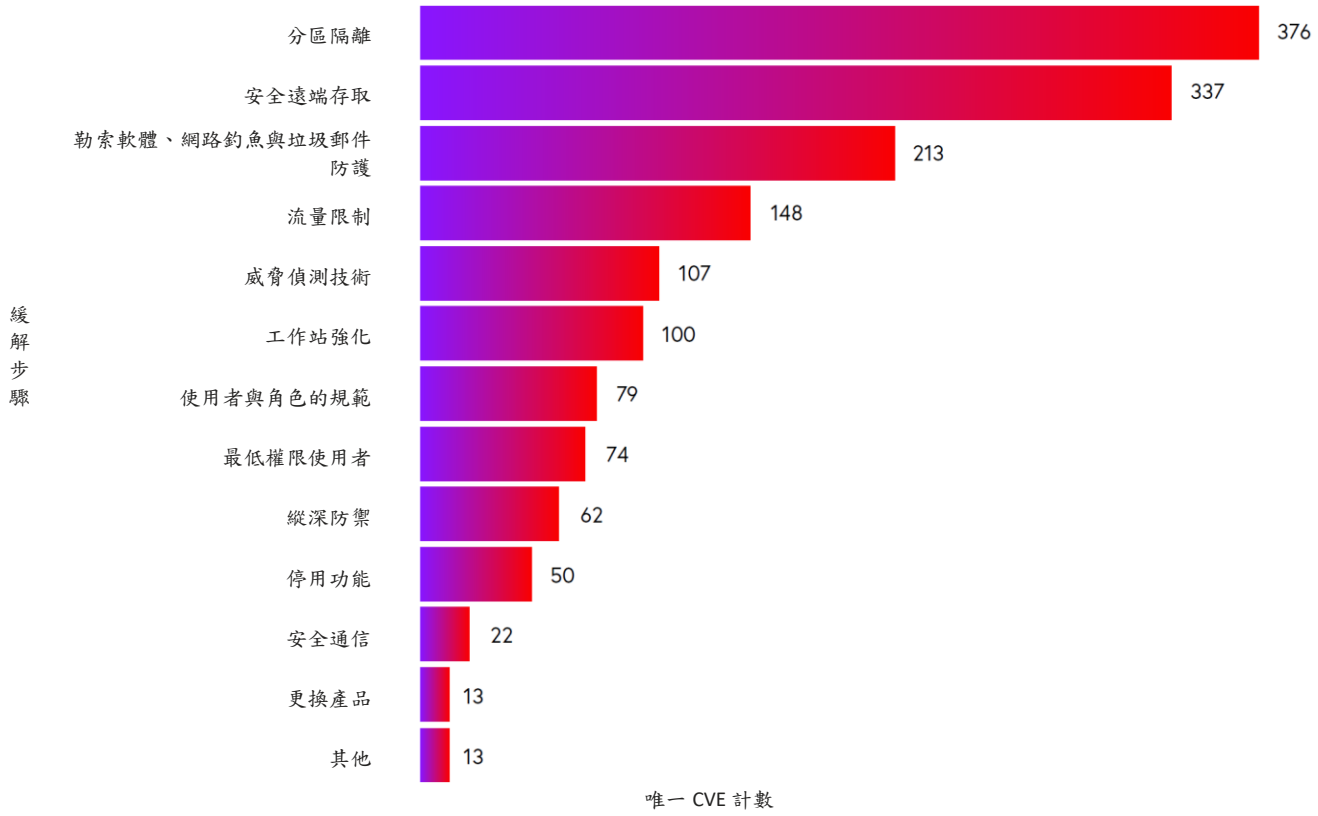


圖 3.1a：主要緩解步驟分類。

OT 網路分區隔離是一項重要的控制措施，因為離線而不上網已成為過去式，並且隨著企業將數據、應用程式、基礎架構與服務遷移到雲端，其邊境將很有可能遭到入侵。分區隔離可能涉及虛擬分區，也就是針對工程與其他製程導向的功能量身定製特定的策略。檢查流量與 OT 專用協定的能力對於防止異常行為也至關重要。

作為主要緩解步驟之一，遠端安全存取緊接在分區隔離之後。如奧德馬爾市事件所帶來的啟示，企業在管理因新冠疫情而形成的遠端勞動力時，合適的存取控制與權限管理非常重要。安全的遠端存取解決方案不僅必須對可疑活動發出警報，而且還必須能夠即時或依照需求來調查特定的工作階段，並允許管理員透過斷開工作階段或採取其他措施來控制或補救所產生的損害。

3.2 補救

在 2021 年上半年揭露的 637 個 ICS 弱點中，**25.59%**沒有可用的修復程式，或者僅部分補救；**13.5%**—影響 17 家供應商—沒有補救，**12.1%**—影響 12 家供應商—**部分**補救，這表示並非所有受影響的產品都有可用的修復程式。

- 在未補救或部分補救的弱點中，**61.96%**存在於韌體中(另外 4.29%存在於軟體或韌體中)，產品主要部署在網路裝置(37.62%)與普渡模型的第 1 層基本控制(19.8%)。
- 在未補救或部分補救的弱點中，**55.21%**在被利用時可能導致遠端程式碼執行。
- 在未補救或部分補救的弱點中，**47.85%**在被利用時可能導致拒絕服務攻擊，以上的部分弱點可能產生多重影響，例如同時導致遠端程式碼執行與拒絕服務。

影響 70 家供應商的 637 個弱點有 **74.4%**具備補救措施。多數(59.5%)更新屬於軟體修復(另外 1.69%則包含軟體與韌體)，故再次證明修補軟體比韌體相對容易，守衛者可在其環境中優先修補。

在檢視有軟體修復程式的產品時，大多數**(51.42%)**處於第 3 層：營運管理，其次是第 2 層：監督控制**(19.86%)**。

受影響的產品系列

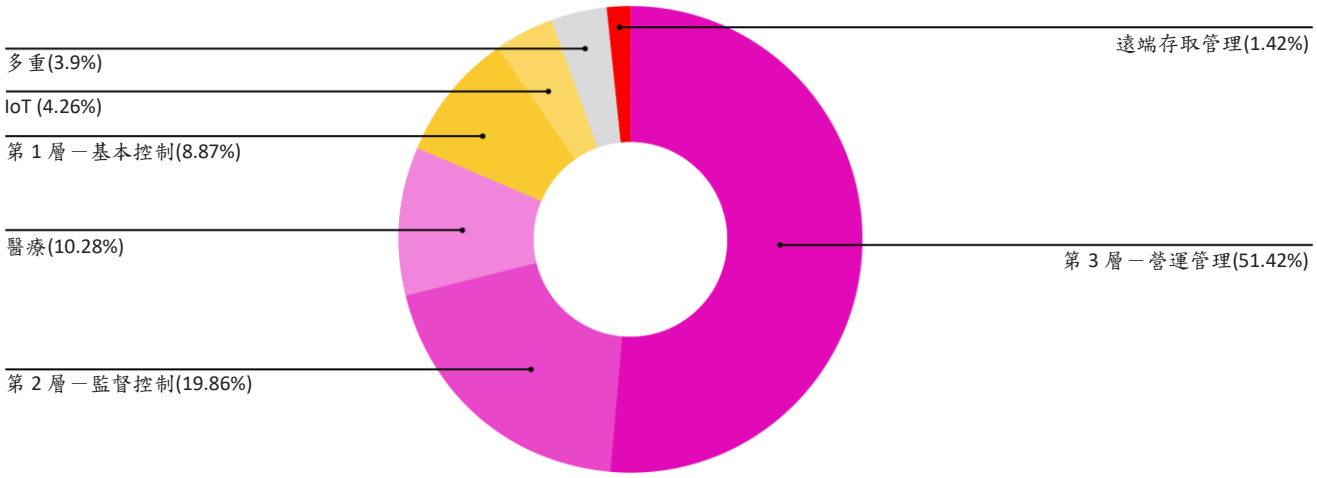


圖 3.2a：按產品系列劃分的軟體補救。

至於韌體，似乎除了無法隨著時間進行補救外，其可用的補救解決方案也較少。若確實有韌體補救措施存在，Team82 的數據顯示大多數是針對網路裝置**(28.26%)**，其次為第 1 層：基本控制**(26.09%)**。因此即使在韌體中，也可能有某些更新的優先順序，因為更新網路裝置(例如交換器)比升級 PLC 或 RTU 更容易也更有可能。

受影響的產品系列

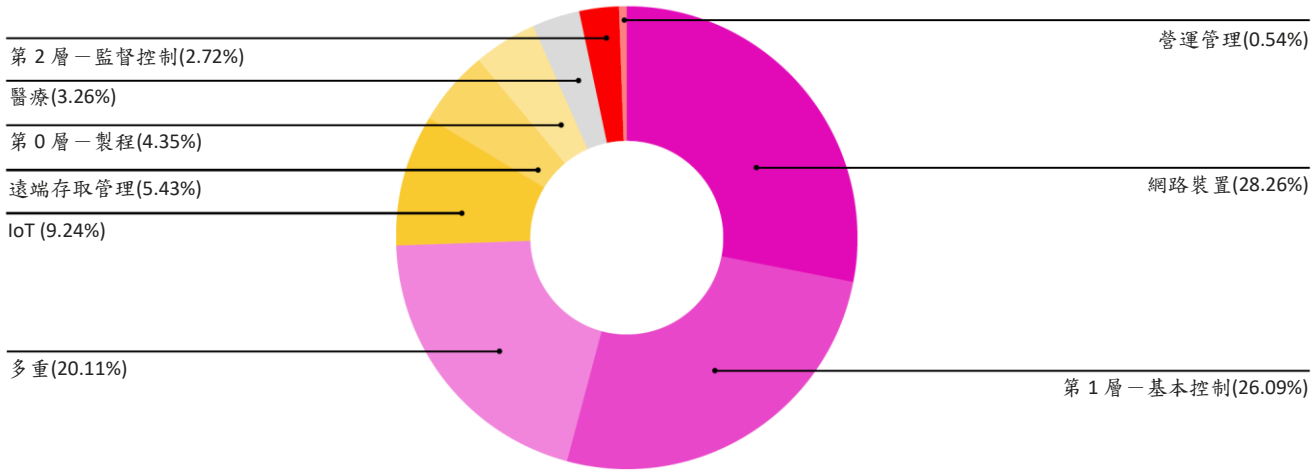


圖 3.2b：按產品系列劃分的韌體補救。

3.3 生命週期終止產品

在總計 637 個弱點中，有 6.43%會影響因供應商不再支援而沒有補救計畫的生命週期終止產品。

- 其中 51.22%的弱點存在於韌體中(另外 14.63%存在於軟體或韌體中)。
- 如下所示，這些生命週期終止產品主要部署在網路的各個級別：

受影響的產品系列

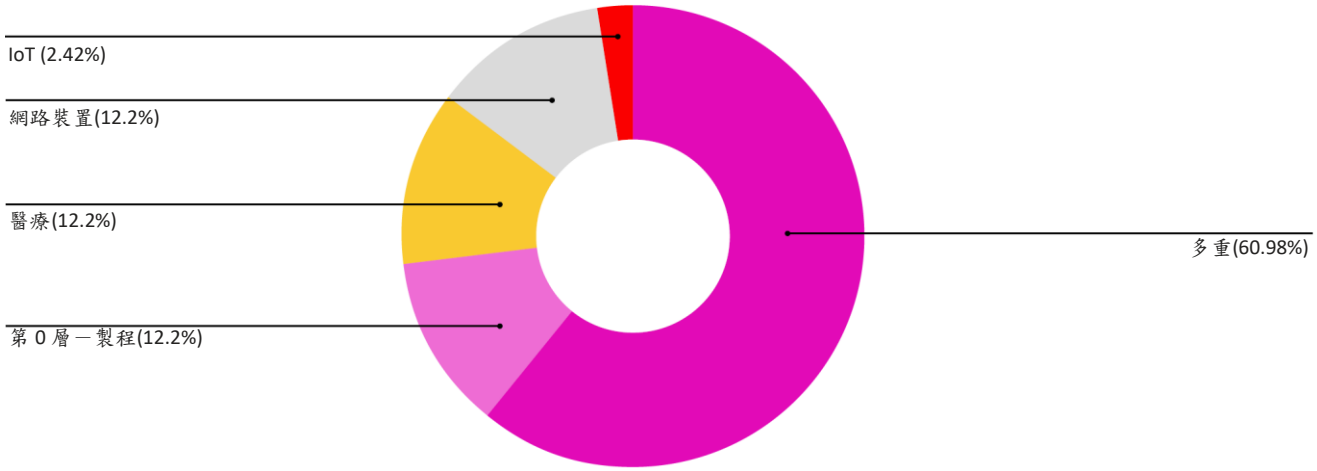


圖 3.3a：受影響的生命週期終止產品。

- **97.56%**影響生命週期終止產品的弱點可透過網路攻擊方式來進行遠端利用。
- **63.41%**的弱點在被利用時可能導致遠端程式碼執行。
- **24.39%**的弱點在被利用時可能導致拒絕服務。

關於生命週期終止產品，更換為新品前唯一的解決方案是緩解(如果可能)。軟體的更新與修補比韌體容易，因韌體更新可能需要數月甚至數年的時間才能完成開發並導入。加上補救解決方案不多，因此可理解到守衛者主要仰賴緩解措施。

第 4 部分：CVSS 資訊

通用弱點評分系統(CVSS)包含三個維度：第一個是「基本維度」，它代表弱點的特徵不隨時間與使用者環境而改變，主要包括兩組指標：可侵入性與影響。

4.1 利用能力指標

這些指標代表可以用來利用弱點的技術方法和難度。

如下圖所示，**61.38%**的弱點可以透過網路攻擊方式進行遠端利用。這突顯出保護遠端存取連線與對外連接網際網路之 ICS 裝置的重要性。儘管透過網路仍是主要的攻擊方式，但此數字已較 2020 年下半年(71.49%)下降，因我們看到本機攻擊方式開始增加。

其中 **72.14%**屬於本機攻擊方式的弱點，攻擊者仰賴使用者互動來執行利用這些弱點所需的行動。這包括網路釣魚和垃圾郵件等社交工程技巧。危機意識與保護措施是非常重要的，採用此類技術的攻擊手段正呈現上升趨勢，使用者應遵守本報告所建議的安全措施。

攻擊方式分佈

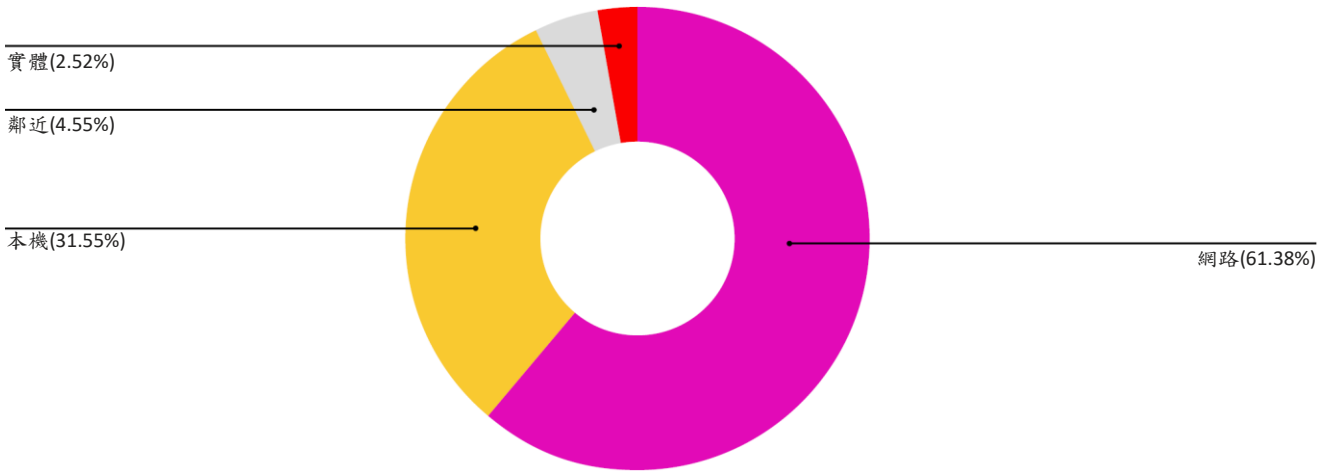


圖 4.1a：與 ICS 弱點相關的攻擊方式。

本機攻擊方式幾乎以營運管理和監督控制等級為主。除此之外，在透過本機攻擊方式利用的營運控制弱點中，有 **94.38%**需要使用者互動才能利用。

攻擊者對使用者互動的依賴，表示對擁有關鍵資產存取權限的人員而言，危機意識與保護社交工程策略是非常重要的。

每個產品系列的攻擊方式

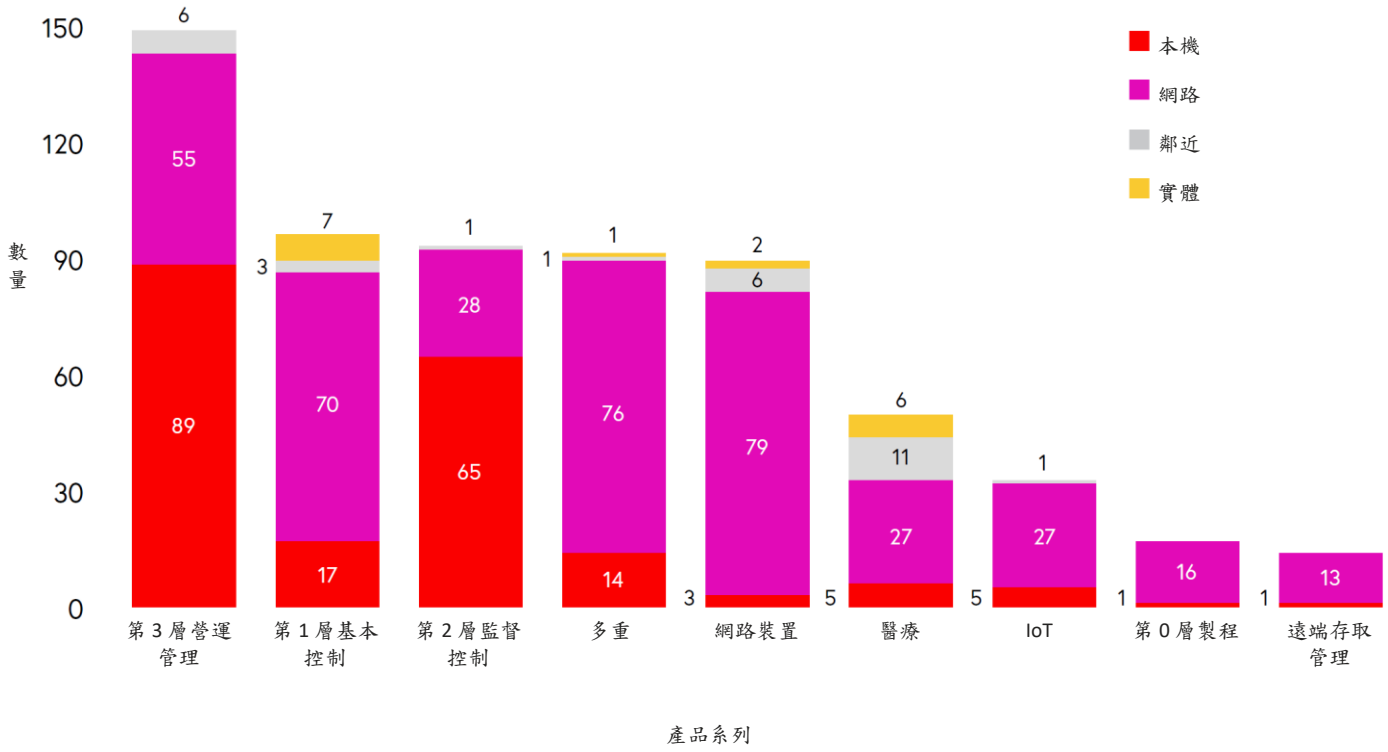


圖 4.1b：按產品系列劃分的攻擊方式。

攻擊複雜度

這個指標代表必須存在攻擊者無法控制的條件，如此他們才能夠利用弱點。例如，成功的攻擊取決於攻擊者是否蒐集組態設定的知識。

89.64%的弱點可以將其利用與攻擊的複雜度視為低度，表示這些弱點不需要特殊條件，而且攻擊者預期每次都能複製此成功方程式。

CVSS 攻擊複雜度

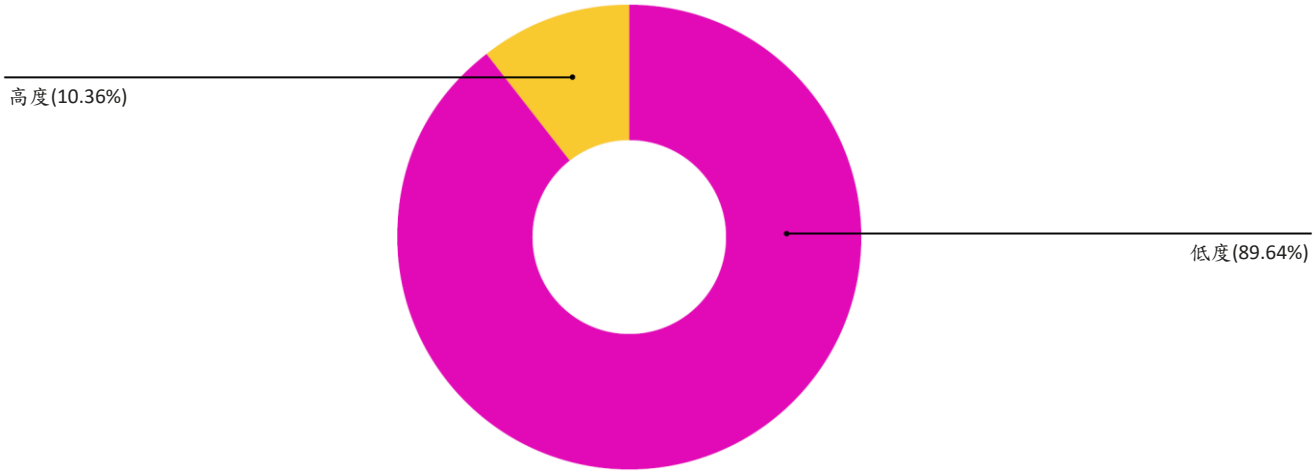


圖 4.1c：根據 CVSS 評分的攻擊複雜性。

4.2 需要的權限

這個指標代表攻擊者在成功利用弱點之前必須擁有的權限等級。

如下圖所示，在 **73.78%**的弱點中，攻擊者未獲授權即可展開攻擊，而且對目標的設定或檔案不需要進行任何存取。

需要的 CVSS 權限

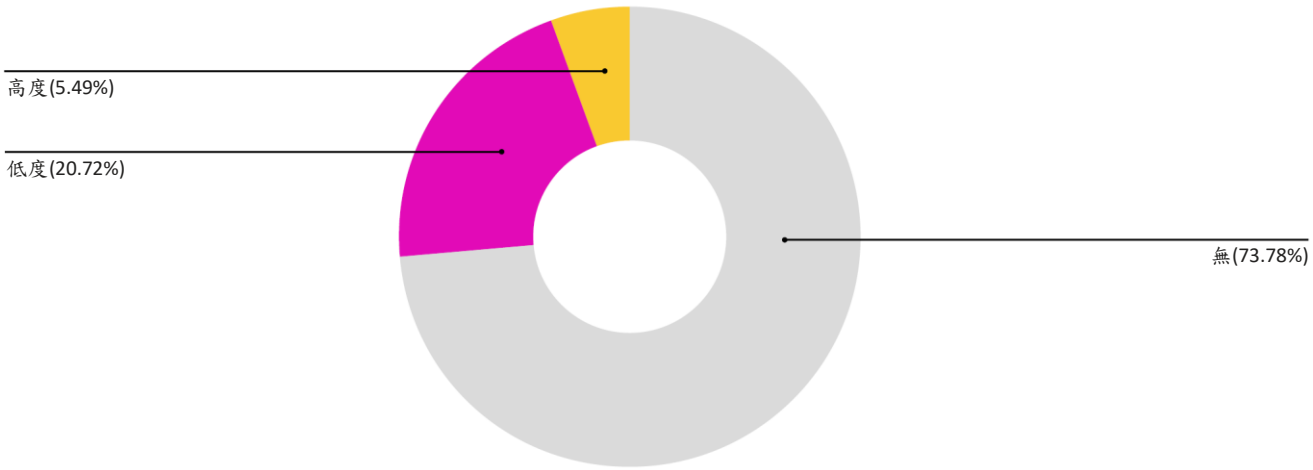


圖 4.2a：利用弱點所需的權限。

使用者互動

這個指標代表攻擊者是否需要個別使用者的參與、或使用者發起的流程才能利用弱點。

如下圖所示，**66.25%**的弱點不需要使用者互動。

CVSS 使用者互動

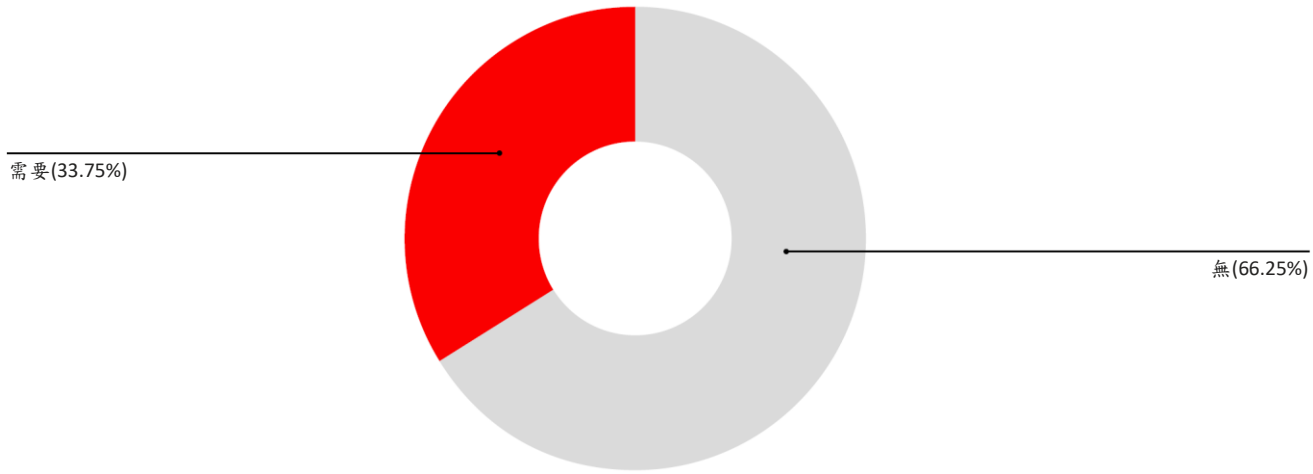


圖 4.2b：利用弱點所需的使用者互動。

4.3 影響指標

這些指標代表成功利用每個弱點的直接後果。CVSS 系統會根據 CIA 三要素(保密性、完整性和可用性)衡量影響。雖然 CIA 三要素在技術上與任何類型的網路均有關，但未包含可以視為 OT 網路最重要的兩個風險變數：可靠性和安全性。

保密性

這項指標代表成功利用弱點對資訊資源保密性所產生的影響。

如下圖所示，超過 94.5%的弱點對保密性的影響為低或無。提醒您，正如前面所提到的，雖然保密性對 IT 安全非常重要，但在 OT 網路中卻不是那麼重要的風險變數。

CVSS 保密性

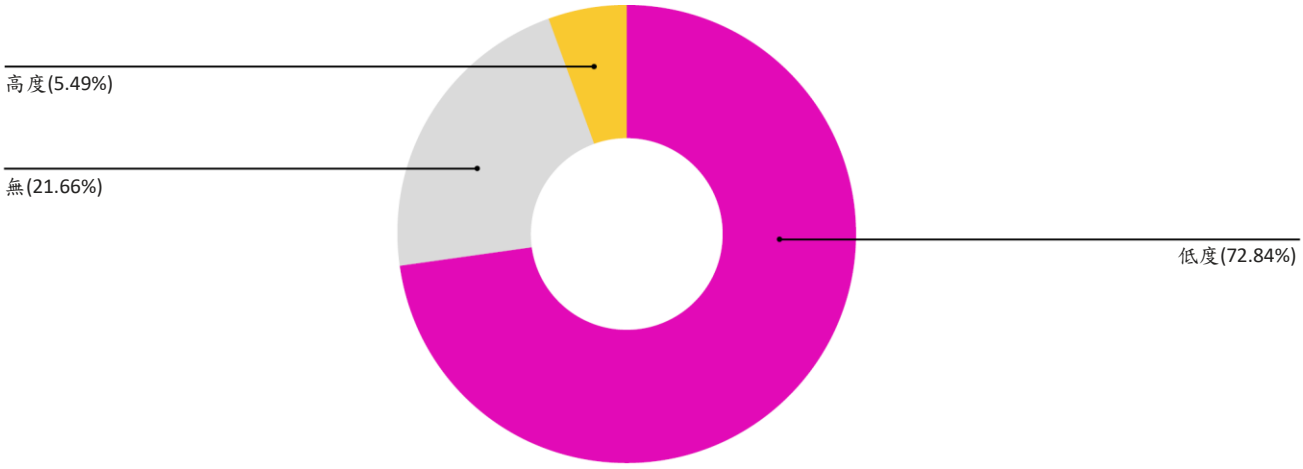


圖 4.3a：對保密性的影響。

完整性

這項指標代表成功利用弱點對資訊完整性所產生的影響。

如下圖所示，**69.7%**的弱點對保密性的影響是無或完全沒有。同樣如先前所述，這項指標顯示雖然資訊的完整性在 IT 安全中非常重要，但卻是 OT 網路中沒那麼重要的風險變數。

CVSS 完整性

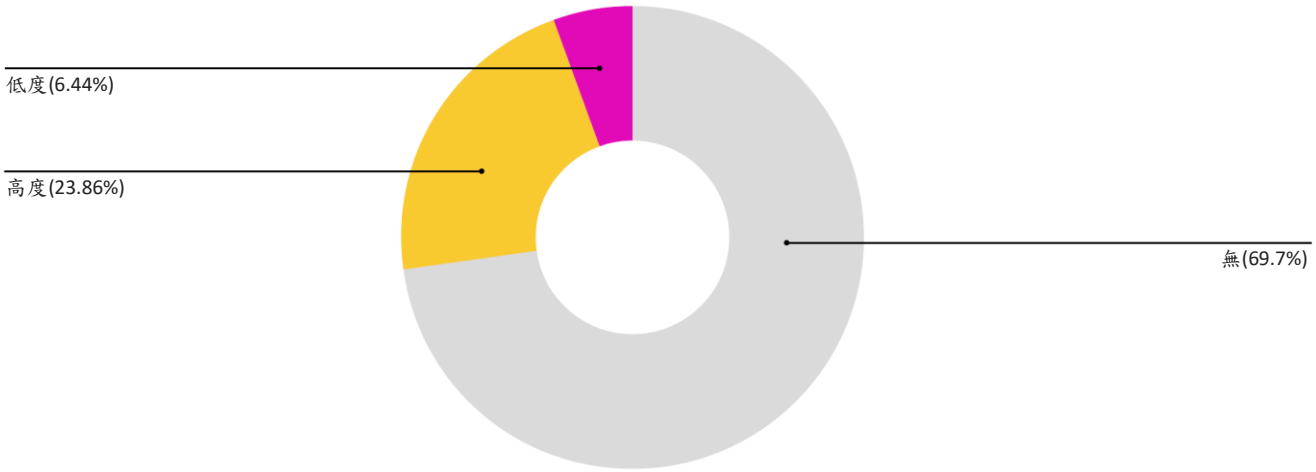


圖 4.3a：對保密性的影響。

可用性

這項指標代表成功利用弱點對受影響元件的可用性所產生的影響。

如下圖所示，65%的弱點對可用性的影響為高度。這代表可用性完全喪失，導致拒絕對資源的存取。此外，可用性部分喪失，但卻是重要的部分—例如，拒絕建立新連線的能力。

CVSS 可用性

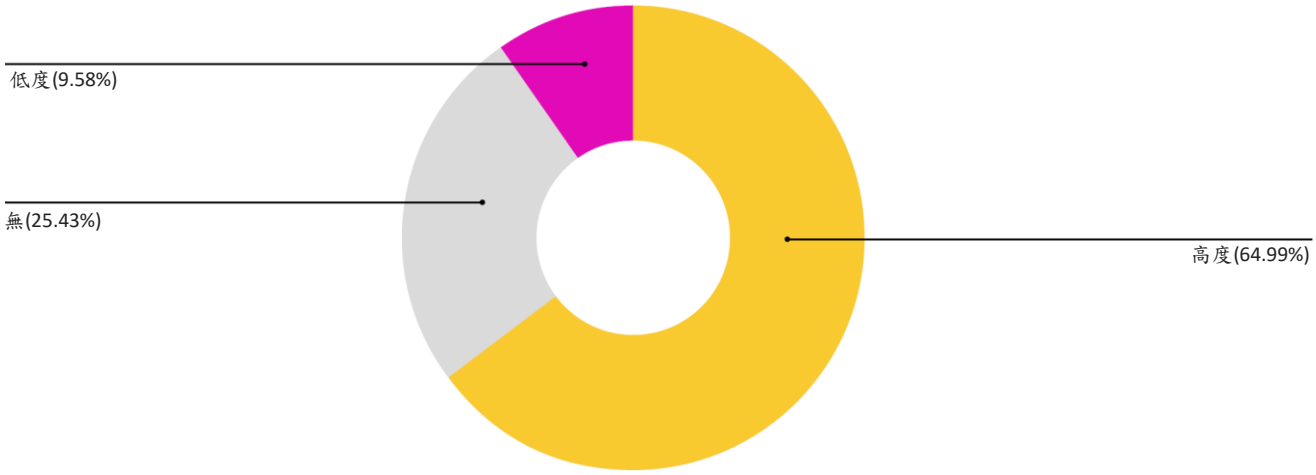


圖 4.3c：對可用性的影響。

4.4 範圍

這個指標代表元件中的弱點是否會對其「安全範圍」外的元件內資源造成影響。如下圖所示，有 87.28%的弱點範圍沒有改變，表示這些遭到利用的弱點只會影響相同安全範圍內的資源。

CVSS 範圍

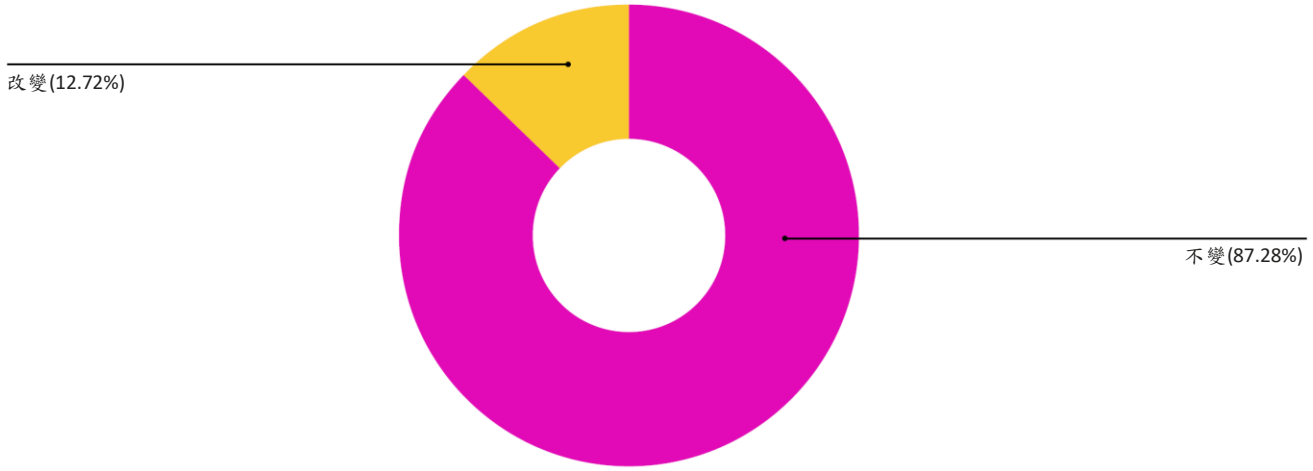


圖 4.4a：CVSS 範圍。

4.5 CVSS 分數

上述所有指標都會經過衡量並計算出代表弱點嚴重性的最終 CVSS 分數。此分數範圍分為四類：低、中、高與嚴重。

70.64%的 ICS 弱點被歸類為高度或嚴重。這項觀察結果反映出 ICS 安全研究人員大多傾向將重點放在找出具有最大潛在影響的弱點，以便將傷害減到最少。

這項觀察也和先前的發現吻合，即大多數弱點並不複雜、不需要權限或仰賴使用者互動，以及可能導致可用性完全喪失。

CVSS 分類部分

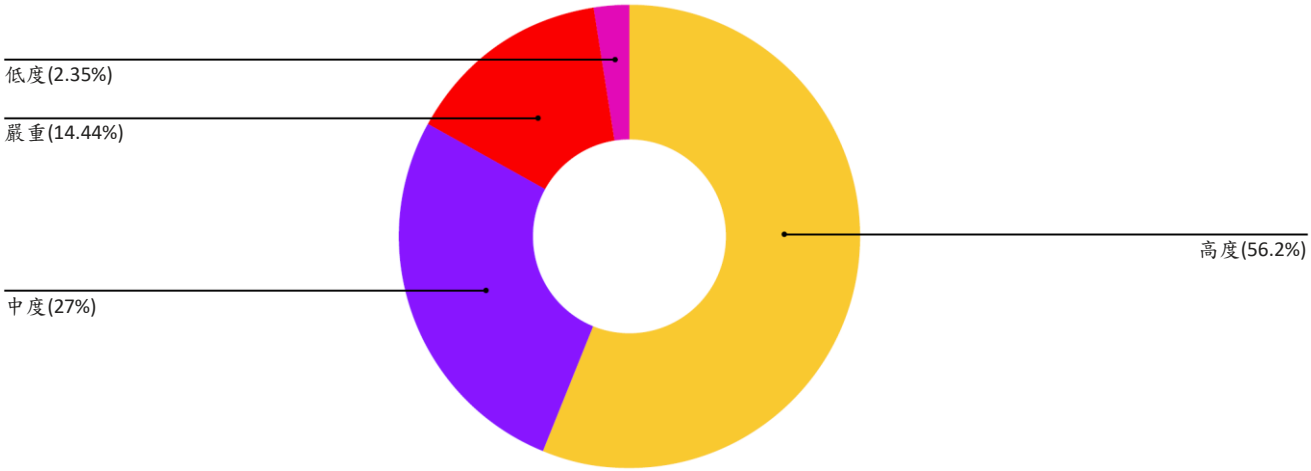


圖 4.5a：按關鍵程度劃分 CVSS 分數。

第 5 部分：所利用的 CWE

在 2021 年上半年間揭露的 ICS 弱點中，列舉的安全弱點－或常見弱點列表(CWE)－有助於說明大部分弱點的 CVSS 分數都可以歸類為高度或嚴重的原因。

來自 Team82 數據的**前五名最普遍的 CWE** 在 MITRE 公司 2021 年 CWE 前 25 名最危險的軟體缺失列表中很顯眼。這些弱點相對容易利用，進而讓攻擊者造成嚴重破壞。

這些 CWE 包括：

CWE-787 越界寫入

軟體寫入資料超出結尾，或是在預期緩衝區開始之前寫入資料。這通常發生在指標或其索引遞增或遞減到超出緩衝區界線的位置，或指標算數導致有效記憶體位置以外的位置時。成功利用可能會導致資料損毀、拒絕服務或程式碼執行。

- 這個 CWE 出現在 **11.5%**的弱點中，高於 2020 年下半年的 **6.74%**。
- 這個 CWE 在 MITRE 的 2021 年前 25 大最危險軟體弱點中排名第一。

CWE-125 越界讀取

軟體讀取資料超出結尾，或是在預期緩衝區開始之前讀取資料。成功利用可以產生讀取記憶體和繞過防護機制的能力。

- 這個 CWE 出現在 **5.68%**的弱點中，高於 2020 年下半年的 **5.65%**。
- 這個 CWE 在 MITRE 的 2021 年前 25 大最危險軟體弱點中排名第三。

CWE-20 不正確的輸入驗證

若產品進行不正確的輸入驗證或不驗證輸入，可能進而影響程式的控制流或數據流。若軟體進行不正確的輸入驗證，將讓攻擊者以出乎意料的方式「製作」輸入。成功利用可能導致控制流被更改、記憶體修改、拒絕服務或程式碼執行。

- 這個 CWE 出現在 **3.93%**的弱點中，高於 2020 年下半年的 **3.85%**。
- 這個 CWE 在 MITRE 的 2021 年前 25 大最危險軟體錯誤中排名第 4。

CWE-119 記憶體緩衝區界限內的操作限制不當

軟體對記憶體緩衝區執行操作，但卻可以讀取或寫入緩衝區預期界限之外的記憶體位置。成功利用可能導致任意程式碼執行、系統當機、預期控制流的改變或讀取敏感訊息的能力。

- 這個 CWE 出現在 **3.93%**的弱點中，高於 2020 年下半年的 **1.93%**。
- 這個 CWE 在 MITRE 的 2021 年前 25 大最危險軟體弱點中排名第 17。

ICS 弱點以 CWE 為基準的潛在影響

下圖描述 2021 年上半年間發佈以 CWE 為基準的 ICS 弱點最常見潛在影響，反映出遠端程式碼執行在 OT 安全研究社群重點領域的特殊地位。

遠端程式碼執行的背後是明顯的第二級潛在影響：導致拒絕服務、繞過保護機制，並允許攻擊者修改記憶體或讀取應用程式數據。

依影響計算的弱點數量

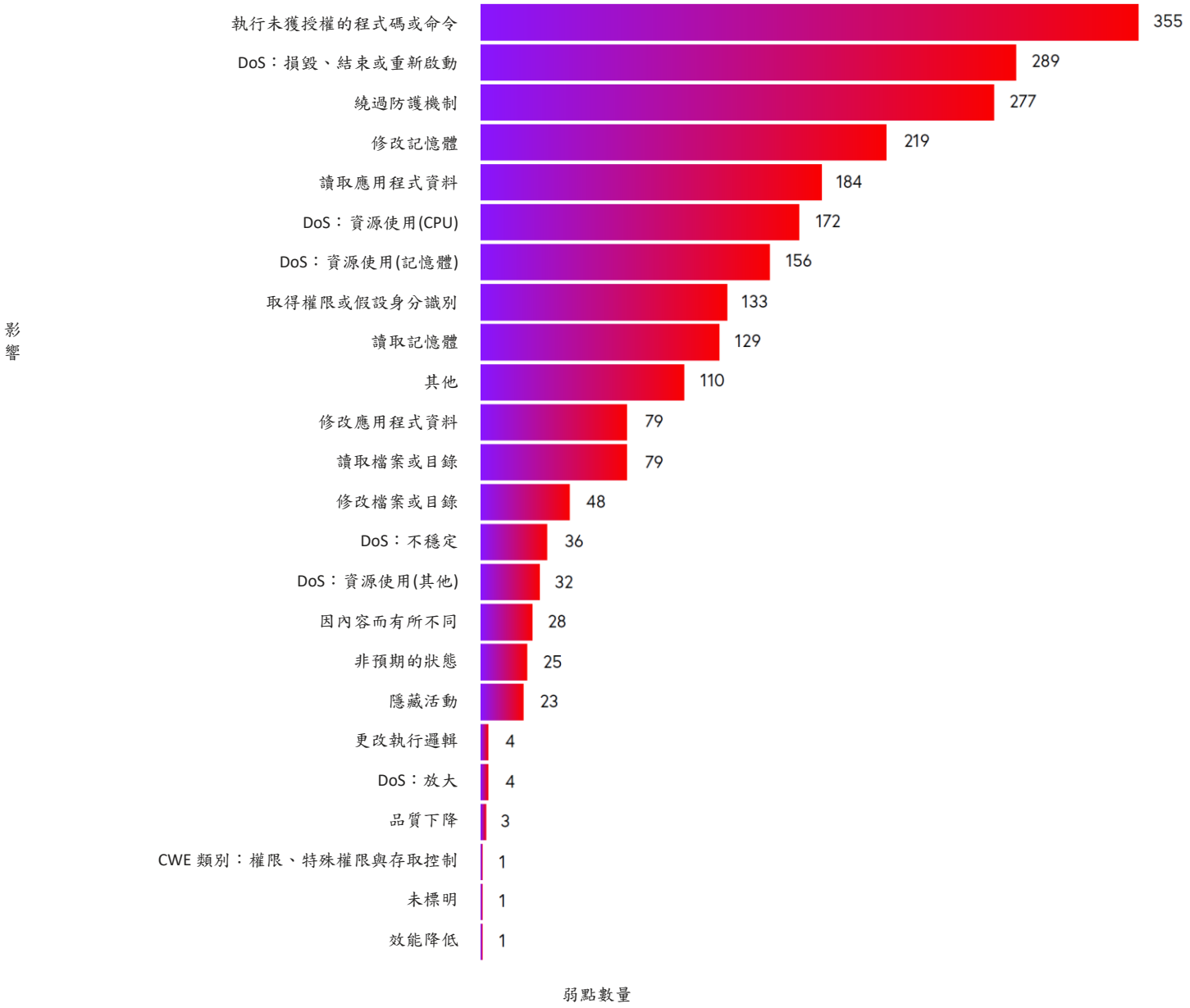


圖 5a：按 CWE 影響劃分的弱點數量。

透過 2019 年、2020 年與 2021 年上半年的 ICS 弱點資料比較，顯示遠端程式碼執行期限與拒絕服務是前兩大最常見的影響。

可能導致遠端程式碼執行的弱點數量比去年大幅增加 **64.35%**，亦較 2019 年上半年明顯增加 74%，而拒絕服務**(+68%, +102.1%)**與繞過保護機制**(+87.16%, +102.2%)**也比 2019 年上半年顯著增加。

依前 15 大影響計算的弱點數量逐年比較

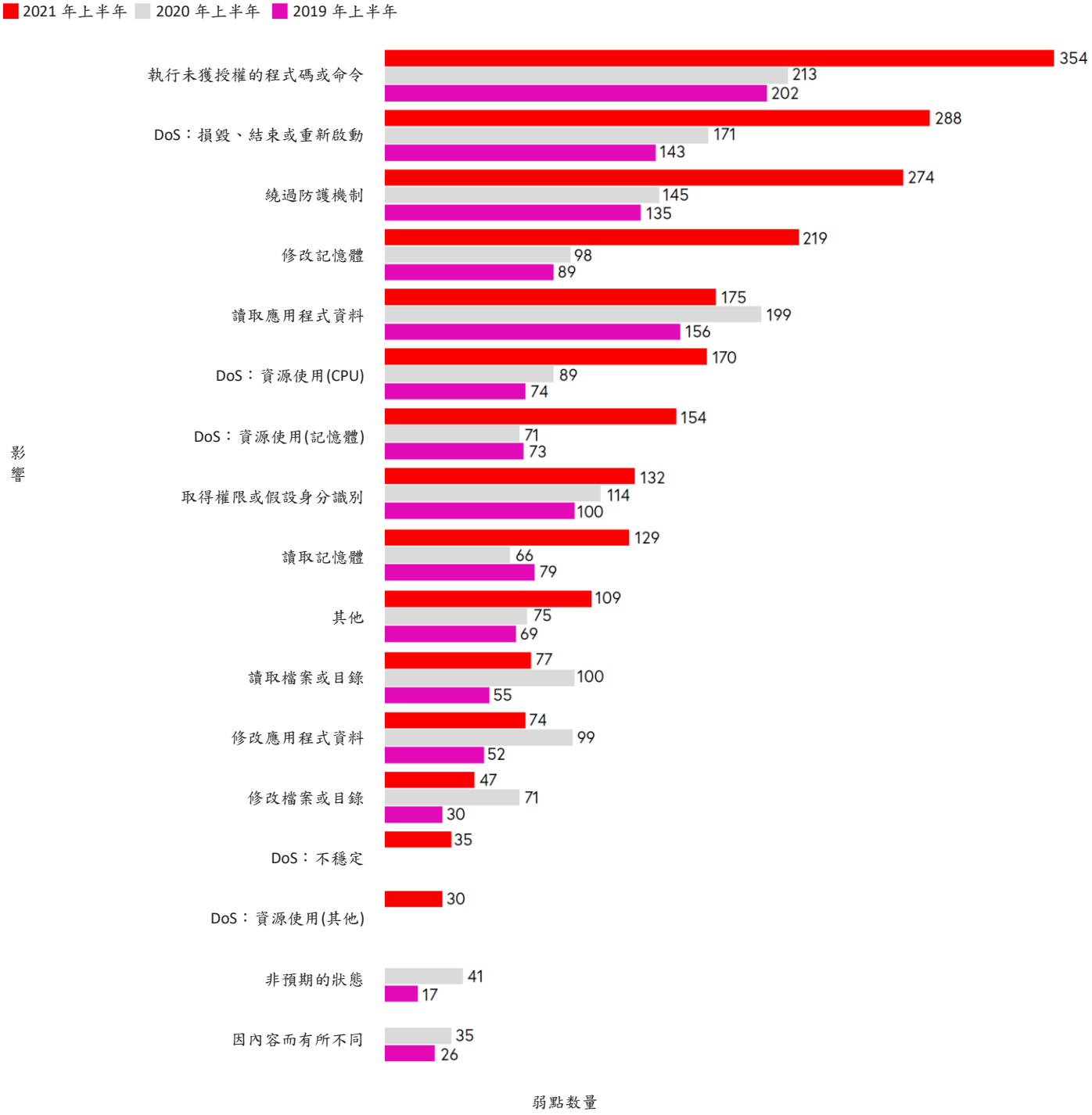


圖 5b：依影響計算的弱點數量逐年比較。

第 6 部分：與 2021 年上半年 ICS 風險與弱點情境相關的重要事件

Team82 團隊評估，下列事件與趨勢可能在某種程度上有助於 2021 年上半年 ICS 風險與弱點情境的塑造。

COLONIAL PIPELINE 攻擊事件

Colonial Pipeline 是美國東岸最大的汽油、柴油與天然氣經銷商，該公司受到勒索軟體攻擊後，石油與天然氣的輸送皆受到很大影響。5 月 7 日關閉——這是該公司 57 年來第一次關閉——對產業造成巨大影響，因為東岸約 45%的燃油均由 Colonial Pipeline 供應。關閉導致汽油與家庭暖氣用油價格上漲，許多加油站的燃油也完全耗盡。Colonial Pipeline 於 5 月 13 日恢復營運。

DarkSide 是一家銷售勒索軟體即服務(RaaS)的俄羅斯網路犯罪組織，據了解此次攻擊行動由該組織負責。如果不滿足其贖金要求，DarkSide 將竊取敏感數據並勒索受害者，同時威脅公布這些數據。根據先前的報導，DarkSide 似乎只尋找能夠支付高額贖金的受害者，且他們聲稱不會攻擊醫療機構、教育機構或政府機構。Colonial Pipeline 支付了 440 萬美元的比特幣贖金(其中 230 萬美元被美國追回)，但據報導，DarkSide 在攻擊事件發生後不久即停止營運。

如需進一步了解 Colonial Pipelines 攻擊事件的相關資訊，請參閱：
https://claroty.com/2021/05/10/blog-research-colonial-pipeline/

奧德馬爾市淨水廠遭駭

2 月 5 日，佛羅里達州奧德馬爾市的一家淨水廠遭駭客攻擊。奧德馬爾市淨水廠內的操作員偵測到兩次來自工廠外部的入侵，其中第二次入侵來自遠端攻擊者，該攻擊者透過 TeamViewer 遠端桌面連線軟體進行攻擊(此軟體是一種用於技術支援的合法遠端存取解決方案)。

遠端攻擊者將住宅與商業飲用水中氫氧化鈉的含量從 100ppm 更改為 11,100ppm。將氫氧化鈉或鹼液加入水中可控制酸度並去除某些金屬。鹼液也是下水道清潔劑的主要成分，屬於腐蝕性物質，如果誤食將對人體造成危險。

操作員切斷了攻擊者的存取管道，並在水處理系統原有的保護措施支援下，阻止受污染的水流向公眾。

如需進一步了解奧德馬爾市攻擊事件的相關資訊，請參閱：
https://www.claroty.com/2021/02/16/blog-research-oldsmar-water-hack-highlights-systemic-problems-undermining-critical-infrastructure/

JBS FOODS 攻擊事件

全球最大的肉品供應商 JBS 於 5 月 30 日遭到勒索軟體攻擊，導致澳洲、加拿大與美國的工廠均關閉，美國工廠的關閉使美國的肉品加工能力減少近五分之一。聯邦調查局將這次攻擊歸咎於 REvil (也稱為 Sodinokibi)。

REvil 是一個提供 RaaS 服務的駭客組織。他們以勒索大筆贖金、攻擊大型企業以及在加密前竊取數據進行雙重勒索而聞名，他們將這些訊息發佈在暗網裡一個名為「快樂部落客」的網站上。

JBS 擁有備份系統，可使用該系統來恢復操作並恢復數據。無論如何，據報導該公司向攻擊者支付了 1,100 萬美元的贖金，以恢復正常運作。

如需進一步了解 JBS 攻擊事件的相關資訊，請參閱：
https://claroty.com/2021/06/02/blog-jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test/

第 7 部分：建議

Team82 針對我們在本報告中分享的弱點趨勢推薦了這些安全措施。

網路分區隔離

隨著離線不上網的工業設備已成為過去，越來越多設備連到網路並透過雲端進行管理，因此必須優先考慮網路分區隔離等縱深防禦措施。對網路管理員的建議：

- 以虛擬方式將網路分區隔離並以能夠遠端管理的方式進行配置。
- 針對工程與其他製程導向功能，建立量身定製的區域專用策略。
- 保留檢查流量與 OT 專用協定的能力，以偵測並抵禦異常行為。

遠端存取連線保護

無論世界是否取消 COVID-19 疫情期間的諸多限制措施，遠端勞動力已成為新常態。隨著組織中越來越多人透過遠端的方式存取企業資源，組織必須確保遠端存取連線的安全。在 OT 環境與關鍵基礎設施中，這一點至關重要，因為操作員與工程師必需能安全地遠端存取工業資產，以確保可用性與安全性。我們鼓勵安全從業人員採取下列措施：

- 驗證 VPN 版本是否已修補並更新到最新版本
- 監控遠端連線，尤其是與 OT 網路與 ICS 設備的連線
- 實施精密的使用者存取權限與管理控制
- 強制執行多重身份驗證

勒索軟體、網路釣魚和垃圾郵件防護

遠距離工作增加，對以電子郵件做為重要通訊機制的依賴也隨之增加。因此，這些情況也讓鎖定個人的網路釣魚或垃圾郵件攻擊增加，而且勒索軟體和其他惡意程式感染的風險也因此增加。使用者應遵守以下建議：

- 切勿開啟來自不信任來源的電子郵件，或是下載不信任來源的軟體
- 若有來自不明寄件者的電子郵件，切勿點選其中的連結或附件
- 切勿透過電子郵件提供密碼、個人或財務資訊給任何人(敏感性資訊也會被用於敲詐勒索)
- 一律確認電子郵件寄件者的電子郵件地址、姓名和網域
- 頻繁備份重要檔案，並將這些檔案和主系統分開儲存
- 使用防毒、防垃圾郵件和防間諜軟體來保護裝置
- 立即回報網路釣魚電子郵件給適當的資安或 IT 人員

保護營運管理與基本監督控制

2021 年上半年揭露的多數 ICS 與 SCADA 弱點主要影響第 3 層：營運管理(Historian、OPC 伺服器等)，其次是第 1 層：基本控制(控制器、PLC、RTU)與第 2 層：監督控制(HMI、SCADA 與工程工作站)。

相較於基本控制是以韌體為主，營運管理和監督控制的弱點大多數是以軟體為主。由於無法隨時修補，特別是第 1 層裝置韌體中的弱點，所以建議投資在分區隔離、遠端存取防護，以及營運管理和監督控制等級更妥善的防護，藉此存取基本控制等級，最終便可取得取得流程本身的存取權限。其他建議包括：

- 使用加密、存取控制清單，以及適合 OT 網路的適當遠端存取技術等機制來保護遠端存取連線。
- 維持資產庫存和分區隔離。
- 評估風險和優先處理重大修補程式。
- 確保裝置受到密碼保護並執行嚴格的密碼有效性。
- 實行複雜的角色和原則式行政存取。
- 如同我們所看到的，以第 2 層弱點為主的本機攻擊方式大多數仰賴使用者互動，因此會遵循針對社交工程技術的最佳實務。

致謝

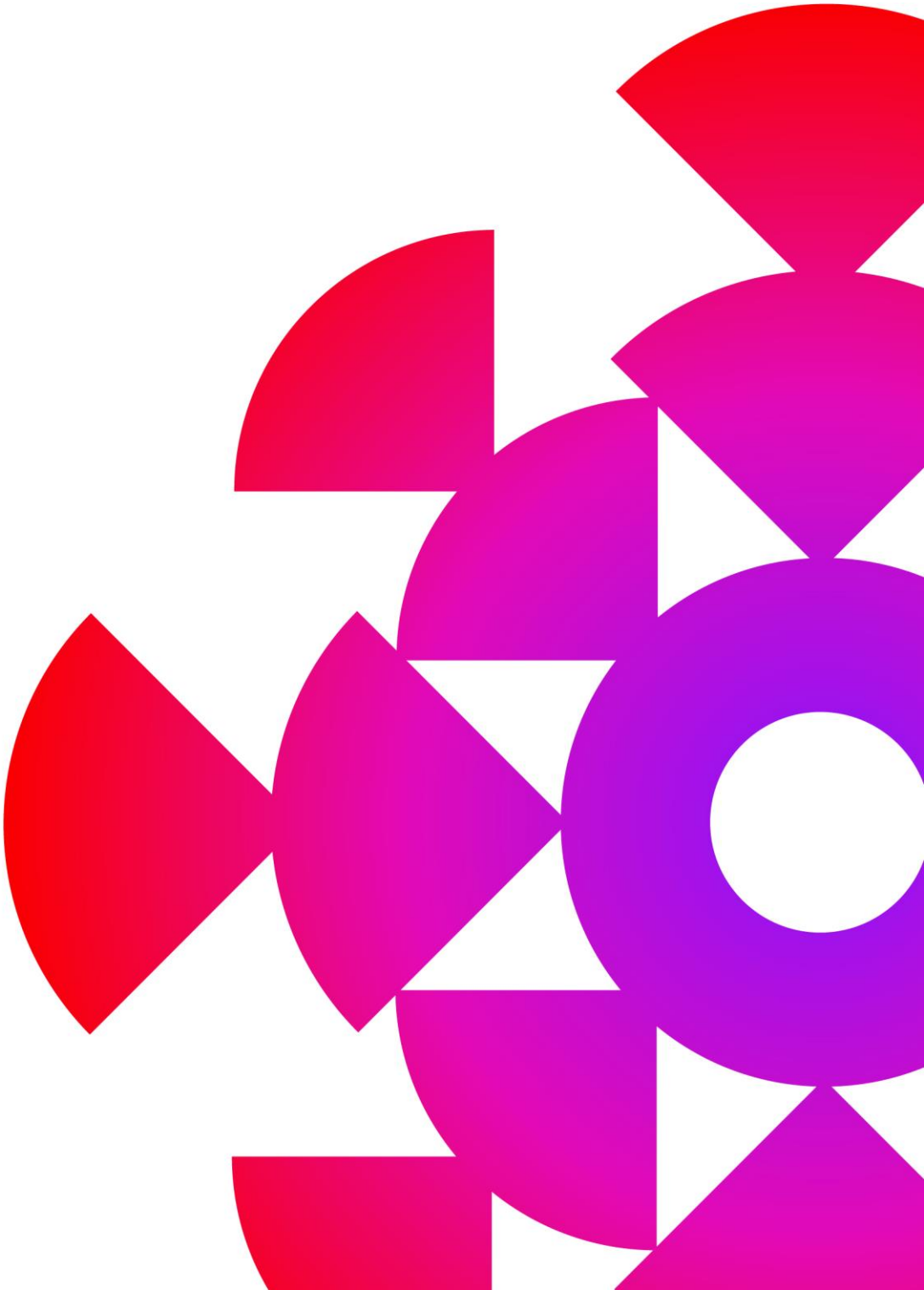
這份報告的主要作者是 Claroty 的安全研究人員 Chen Fradkin。

貢獻者包括：Claroty 的安全研究團隊組長 Rotem Mesika、創新總監 Nadav Erez、弱點研究團隊主管 Sharon Brizinov，以及 Claroty 的研究副總 Amir Preminger。特別感謝整個 Claroty 研究團隊為這份報告的各個方面和催生這份報告的研究工作提供傑出的支援。

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。

如需進一步了解，請造訪 www.claroty.com。



CLAROTY