FIREEYE™

產品型錄

關鍵基礎設施資安健檢

瞭解您關鍵基礎設施中暴露的弱點，並制定一個可達成的計畫，以降低系統的網路資安風險

關鍵優點

- 最不具侵入性的評估方式，可避免在 ICS 環境遇到軟體代理程式和網路掃描所伴隨的相關運作風險
- 辨識 ICS 的資安漏洞、不當設定和其他缺陷
- 由 ICS 專家使用 ICS 感知工具，以人工方式分析匿名及可疑的活動
- 依據生產流程特有的相關風險和考量，排定優先順序、客製化的可行建議，並放入適當的情境

Mandiant 是備受全球企業信賴的顧問，在處理世界各地的進階威脅發動者方面，擁有 10 年以上的豐富經驗。我們會在發生資安入侵事件後，支持組織渡過最關鍵的時刻，並積極協助組織提升偵測、回應及遏制能力。關鍵基礎設施資安健檢 Industrial Control Systems (ICS) HealthCheck 將 Mandiant 對威脅行為知識和回應資安事件的經驗，與我們 ICS 顧問的網域專業知識加以結合，以深入評估您的 ICS 網路實際運作時，在妥善區隔、防護及監控方面的表現度。

概觀

如果要評估產業裝置的整體網路資安狀態，ICS HealthCheck 可謂為最不具侵入性的評估方式。若組織擔心軟體型代理程式、網路掃描或其他較具侵入性的資安評估技術會伴隨相關的運作風險時，ICS HealthCheck 就是專為這類組織的需求而設計的評估方式。ICS HealthCheck 不但加入以工作坊為基礎的 ICS 架構審查，還結合了對防火牆的設定和 ICS 即時網路流量的詳細技術分析。

Mandiant 的 ICS 專家對營運技術 (Operational Technology，OT) 十分了解，也會直接與負責 OT 的工程師攜手合作，讓網路資安的最佳作法能妥善適應 ICS 環境。我們還會和 IT 資安主管合作，賦予他們網域知識和公信力，才能有效地在討論網路資安時和他們的 OT 團隊互動。

我們的作法

架構式風險分析與威脅塑模

記錄目前的網路情形

- 審查現有架構圖、資料流程和設計。
- 清查及評估使用中的產業通訊協定。
- 針對軟硬體部署審查現有的資安標準。

您可獲得的好處

- **威脅模型圖：**
  呈現您 ICS 的圖表，其中含有各種對應的威脅媒介，而攻擊者可能會利用這些威脅媒介干擾您的作業或拖慢其速度；同時還會討論如何為適當的資安控制項排定優先順序。
- **ICS HealthCheck 報告：**
  一份詳細的技術報告，描述 Mandiant 觀察到的情況，包括所有資安弱點、不當設定、架構弱點、可疑的網路流量或異常活動，並針對每個觀察項目附上可行且定有優先順序的技術性建議，此外還會提供在評估過程中發現的重點摘要。
- **策略和技術建議的展示：**
  提供一份敘述我們觀察結果和建議的摘要給技術及管理階層的利害關係人。

開發威脅模型

- 在與客戶的 IT 和營運/工程人員進行的互動式工作坊中，取得從討論中產生的架構圖，並建立威脅模型的基礎。
- 依據我們對真實世界中各種攻擊手法的廣泛知識，就控制系統可能會遭受的攻擊，建立視覺化的呈現方式。
- 協助排定 ICS 的資安控制項實作優先順序，以找出暴露程度最大且風險最高的攻擊媒介。

排定控制項的優先順序

- 與技術團隊更快共同得出討論結果，以找出適當的資安控制項來處理發現的威脅。
- 針對可能的控制項，以價值為導向排列優先順序，同時衡量降低風險、成本/付出心力與實作速度等各方面的因素。

技術數據分析

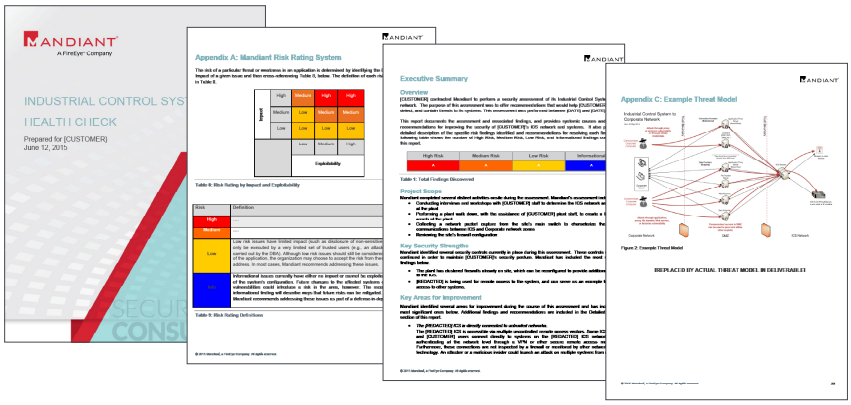
網路區段審查：我們會從部署於客戶 ICS 網路中的 FireEye PX 裝置，分析網路封包擷取檔案。審查封包擷取後，將可瞭解是否有以下類型的資安風險：

- ICS 與網際網路或企業網路之間的非預期連線
- 雙網路介面裝置
- 越過 ICS 防火牆的 ICS 通訊協定
- 匿名的電腦對電腦連線

資安裝置設定審查：我們會審查網路資安裝置（例如防火牆）的設定及其規則集的功效。例如：

- 進入 ICS 網路的輸入流量應一律經由 DMZ 安排路由程序。
- 不得直接存取 ICS 網路，也不得從 ICS 網路直接連接網際網路。

報告範例



要知道更多關於 FireEye，請參閱：**www.FireEye.com**

FireEye Taiwan | 台灣火眼有限公司
| 10683 台北市信義路四段 6 號 6 樓
+886 2 5551 1268 | FIREEYE |
taiwan@FireEye.com

關於 FireEye, Inc.
FireEye 是一間情報主導的資安公司。作為客戶資安監控的無縫、可擴展的延伸，FireEye提供單一平台，將創新的資安技術、國家級別的威脅情報和世界知名的Mandiant® 諮詢融合在一起。藉由此方法，FireEye 為努力準備、預防和應對網路攻擊的組織，消除資安機制的複雜性和重擔。