onward SECURITY

免費諮詢

全球知名 IoT 設備商運用 HERCULES SecFlow 與 HERCULES SecDevice 落實安全開發流程 (SSDLC)

客戶概況

A 公司為全球知名 IoT 設備商，其深耕在消費網路產品市場多年並擁有廣大知名度，旗下多項產品行銷全世界並擁有廣大市佔率，也因此在萬物皆可駭的物聯網時代裡，其產品便成為駭客鎖定攻擊的目標。

在物聯網設備頻繁攻擊事件中，A 公司面臨要解決的弱點包含設備韌體憑證處理不當而引發惡意攻擊；帳密採用弱加密儲存方式，駭客可以駭入設備；設備弱點可能成為駭客攻擊路徑中的跳板，嚴重的話會導致消費者隱私洩漏風險。這些問題引起消費者及政府機構的關注。

A 公司認為導致這些安全性問題的原因，是可以透過在開發過程中落實 Security by Design 的概念來預防，因此決定導入安全開發流程 (SSDLC, Secure Software Development Life Cycle)，以提早減少這類問題發生的機會。

面臨挑戰

當 A 公司決定提早在開發流程中注入安全因素後，開發團隊便開始思考過去在開發過程中可能導致產品不安全的因素，包含：

1. 自家產品型號多，盤點產品型號並發現弱點程序複雜或且需花大量時間

2. 開源軟體 (Open Source) 多且分散，使用第三方套件弱點難以掌握

3. 弱點資訊掌握太慢，跟不上被資安專家揭露弱點的速度

4. 既有管理工具無法滿足安全開發流程 (SSDLC, Secure Software Development Life Cycle) 中的資安要求

盤點出上述要解決的問題後，A 公司便著手開始尋找能解決上述挑戰的輔具工具，然而卻發現市面上工具多只能滿足單一的開發管理；弱點掃描；弱點管理等需求，A 公司認為上述問題尚未解決前若又再導入“多套”新工具，不但安全問題沒有解決，反而增加管理多項工具的工作。因此所採用的工具需能方便管理也成為考量的重點之一。幾經評估後 A 公司決定採用可滿足開發流程廣度又兼俱測試安全性深度的**「SecFlow 產品資安管理系統」**與**「SecDevice 弱點檢測自動化工具」**，以解決面臨的挑戰。

onward SECURITY

導入方案

A 公司運用**「SecFlow 產品資安管理系統」**進行安全流程管理、產品安全弱點管理、主動式產品安全事件監控與通報，協助組織連結開發、安全、維運團隊，快速建立安全的軟體開發流程 (SSDLC)；同時運用**「SecDevice 弱點檢測自動化工具」**進行產品檢測及安全性評估，在導入兩項方案後應用重點如下：

- **產品管理團隊自建專屬弱點資料庫自動盤點 Open Source 弱點**
  SecFlow 內建產品管理功能透過與存放最新弱點的弱點資料庫比對，A 公司的產品 PM 可執行安全分析並自動篩選出外包的開發團隊所使用的 Open Source 弱點，此功能為 PM 團隊省去大量弱點比對工作，讓團隊在開發產品過程中，直接避免使用已存在弱點的 Open Source，提前預防可能會造成產品的資安問題。
- **安全團隊透過即時安全情資，提早擬定新揭露的弱點對策**
  A 公司的安全團隊成員過往被動蒐集弱點資訊，且使用人工方式通知產品負責人擬定弱點因應措施的方式，在採用 SecFlow 後，每日截取近 70 個情資來源的風險事件及弱點資訊，透過內建情資關聯功能，可自動將被揭露的新弱點列入資安事件庫，同時通知 PM、RD 及安全負責人進行處理。這一點讓產品安全團隊大大提升事件反應時間，SecFlow 讓原本處理弱點需要 2-3 個月的時間，減少至 2 週。
- **測試團隊將未知弱點都納入測試範圍**
  產品出廠前的品質測試與驗證階段中，A 公司的測試團隊除了功能與規格的驗證外，另採用 SecDevice 模糊測試功能來發掘產品隱藏的「緩衝區溢位」、「格式化字串」與「命令注入」等未知弱點問題，驗証產品抵禦惡意攻擊的穩健度；同時 SecDevice 也做為驗證供應商交貨時的產品安全性測試工具，為產品在測試與交付過程中多增加一份品質的把關。
- **安全團隊整合第三方工具，並保存最完善的測試記錄**
  在產品開發過程所進行的第三方安全測試報告與處理記錄，A 公司的安全團隊運用 SecFlow 的測試報告管理功能，可保存來自 SecDevice 與其它第三方安全測試工具提供的檢測報告，以保存最完整的資安檢測資料，供未來內外部查核使用。

導入效益

客戶導入 SecFlow 與 SecDevice 後，除了成功落實 Security by Design 的任務外，還帶來幾項整體效益：

1. **單一系統即滿足產品管理團隊「產品資安風險管理」與安全團隊「事件反應」需求，降低管理複雜度。**
2. **單一系統滿足 SSDLC 流程中安全團隊對所有資安的管理需求，降低人員學習成本。**
3. **內建情資蒐集與關聯功能，協助安全團隊即時發現弱點，加快處理弱點時間。**
4. **開發過程中協助測試團隊進行已知及未知弱點偵測，提升產品量產前的產品品質。**

在萬物聯網的世界中，駭客能利用的弱點隨著設備連網的種類愈多，能攻擊的面向也愈加廣泛。所有聯網設備若能在產品量產前強化測試深度，甚至提前至開發階段把安全性納為設計考量重點，必然可以大大降低在產品量產上市後被揭漏重大弱點的風險。