onward SECURITY

お問い合わせ

# 世界有名な IoT デバイスメーカーは、HERCULES SecFlow と HERCULES SecDevice を使用し、安全な開発ライフサイクル（SSDLC）を実現

## 顧客情報

A 社は世界有名な IoT デバイスメーカーです。長年にわたりネットワーク製品市場に深く関わっており、高い評価を得ています。その製品の多くは世界中で販売されており、市場シェアが高いため、モノのインターネットの時代では、ハッカーが攻撃を仕掛ける標的になっています。

IoT デバイスへの頻繁な攻撃の中で、A 社が解決すべきことは、ファームウェア証明書の不適切な処理によって引き起こされる悪意のある攻撃、アカウントシークレットは弱い暗号化で保存されるため、ハッカーはデバイスにハッキングすることができます。デバイスの脆弱性は、ハッカーの攻撃経路の踏み台になる可能性があり、深刻な場合には、消費者のプライバシー漏洩のリスクにつながる可能性があります。これらの問題は、消費者や政府機関の懸念を引き起こしています。

A 社は、開発プロセス中に Security by Design の概念を導入することで、これらのセキュリティ問題の原因を防ぐことができると考えています。よって、安全な開発ライフサイクル（SSDLC、Secure Software Development Life Cycle）を導入して、このような問題の発生を早期に減らすことにしました。

## 挑戦に直面する

A 社が開発プロセスにセキュリティ要素を早期に導入することを決定したときから、開発チームは過去の開発プロセス中に製品の不安全な要素について考え始めました。例えば：

1. **自社製品が多いため、モデル仕様もたくさんあります。製品モデルを確認して脆弱性を見つけるため、時間がかかります。**
2. **オープンソースソフトウェア（Open Source）は多数あり、分散しているため、サードパーティパッケージを利用し、脆弱性を把握するのは困難です。**
3. **脆弱性情報の把握が遅すぎるため、情報セキュリティの専門家に公開される速度に追いつくことができません。**
4. **既存の管理ツールは、安全開発ライフサイクル（SSDLC, Secure Software Development Life Cycle）のセキュリティ要件を満たすことができません。**

A 社は、解決すべき上記の問題の一覧を知った後、その課題を解決できる支援ツールを見つけ始めましたが、市場に出回っているツールのほとんどは単一の開発管理、例えば脆弱性スキャンと脆弱性管理などのニーズを満たすことしかできないことがわかりました。上記の問題が解決される前に、複数の新しいツールが導入されると、セキュリティの問題が解決されないだけでなく、複数のツールの管理が増加します。したがって、使用するツールは簡単に管理できることを重要な考慮事項の 1 つになります。いくつかの評価を行った後、A 社は開発プロセスの幅とセキュリティテストの深さを満たし、上記の課題を解決できる**「SecFlow 製品情報セキュリティ管理システム」**と**「SecDevice 脆弱性検出自動化ツール」**の採用を決定しました。

onward SECURITY

## 導入プログラム

A 社は**「SecFlow 製品情報セキュリティ管理システム」**を使用し、セキュリティプロセス管理、製品セキュリティ脆弱性管理とアクティブな製品セキュリティイベントの監視と通知などの機能で、開発チーム、セキュリティチームとメンテナンスチームの編成と連携を支援し、安全なソフトウェア開発ライフサイクル（SSDLC）を迅速に確立します。同時に**「SecDevice 脆弱性検出自動化ツール」**を使用し、製品のセキュリティテストと安全性の評価を行っています。この二つのツールを使用するポイントは：

- **製品管理チームは独自の脆弱性データベースを構築し、オープンソースの脆弱性を自動的にカ確認します**
  SecFlow の製品管理機能は、最新の脆弱性を脆弱性データベースと比較されます。A 社の製品 PM は、セキュリティ分析を実行し、外部委託した開発チームが使用するオープンソースの脆弱性を自動的に検出します。この機能により、PM チームが脆弱性比較作業の時間が大幅に節約されます。よって、製品開発プロセスに既存の脆弱性があるオープンソースの使用を直接回避し、製品のセキュリティ問題の可能性を事前に回避できます。
- **セキュリティチームは、リアルタイムのセキュリティインテリジェンスを使用し、新たに公開された脆弱性に対する早期の対策を策定できます**
  A 社のセキュリティチームは今まで、脆弱性情報を受動的に収集し、手動の方法を使用して製品担当者に脆弱性対応策を策定するように通知してきました。SecFlow を導入した後、彼らは毎日セキュリティインシデントと脆弱性情報を約 70 個の情報源を届けてきました。インテリジェンス関連機能により、情報セキュリティインシデントのデータベースに新たに公開された脆弱性が自動的にリストされ、PM チーム、RD チームとセキュリティチームに通知します。これにより、製品セキュリティチームはセキュリティインシデントへの対応時間を 2 ～ 3 か月から 2 週間に短縮しました。
- **テストチームは、未知の脆弱性をテストスコープに組み込みます**
  製品が出荷される前の品質テストと検証段階では、機能と仕様の検証に加えて、A 社のテストチームは SecDevice のファジングテスト機能を使用して、「バッファオーバーフロー」、「フォーマット文字列」、「 コマンドインジェクション」などとその他の未知の脆弱性を検出できます。悪意のある攻撃に対する製品の堅牢性も検証できます。同時に、SecDevice は、製品の安全性テストツールとしても使用され、サプライヤーの納品を検証し、テストと納品中に製品に品質を確保します。
- **セキュリティチームはサードパーティツールを統合し、最も完全なテスト記録を保存します**
  A 社のセキュリティチームは、SecFlow のテストレポート管理機能を使用して、製品開発中に SecDevice とほかのサードパーティセキュリティツールが発生したセキュリティテストレポートと対応記録を保存し、将来に社内だけではなく、外部検査にも情報セキュリティテストデータを利用できます。

## 導入メリット

SecFlow と SecDevice を導入した後、Security by Design の実行することに加えて、いくつかの全体的な利点ももたらします。

1. **単一のシステムで製品管理チームの「製品情報セキュリティリスク管理」とセキュリティチームの「インシデント対応」のニーズを満たし、管理の複雑さを軽減します。**
2. **単一のシステムで SSDLC プロセスにセキュリティチームの全ての管理要件を満たし、人員の学習コストを削減します。**
3. **インテリジェンス収集と相関機能は、セキュリティチームがリアルタイムで脆弱性を見つけ、対応時間を短縮することに役立ちます。**
4. **開発プロセス中にテストチームを支援して、既知と未知の脆弱性を検出し、製造前の製品品質を改善します。**

IoT の世界に、インターネットに接続されているデバイスの種類が多くなり、ハッカーが攻撃できる脆弱性もより多くなります。ネットワーク化されたすべてのデバイスが製造前のテストを強化し、開発段階に先立って設計上の安全性を考えなければなりません。よって、製造後にに脆弱性の見つかるリスクを大幅に減らすことができます。