Vdoo securing the connected everything

車載ソフトウェアコンポーネントのセキュリティ検証にVdooを選んだ自動車メーカーのケーススタディ

japan_info@vdoo.com

https://www.vdoo.jp

ニーズ

ある大手グローバル OEM では、自動車業界のトップイノベーターとして常に自社の車両接続機能を常に進化させ、顧客のドライビングエクスペリエンスと安全性を向上させています。

このメーカーの製品セキュリティチームは、接続型車両システムやその機能がますます複雑化することで新たに生まれたサイバーセキュリティのリスクを認識し、これらのリスクを制御・管理するためのプロセスやテクノロジーの導入に取り組んでいます。

さらに、同社は規制の強化、特に UNECE WP.29 サイバーセキュリティ規制を受け、生産の開始前・開始後の両方での新しいセキュリティプロセスやツールの導入に力を注ぐようになりました。

お客様の情報

- 国際的な自動車メーカー
- 本社: ヨーロッパ
- 自家用・商用自動車大手
- リスクや規制要件と共に高まる接続型自動車の製品セキュリティへの注目

課題

この OEM では、自社の自動車に多くの ECU が搭載され、それらのソフトウェアの複雑さが増していく中で、車両のサイバーセキュリティやリスク管理の要件に適切に対応することが困難になっていました。同社の製品セキュリティチームはセキュリティを大規模に実現させるため、自動車のライフサイクルのあらゆる段階で、現在手動または複数のツールを使用して行われているセキュリティ関連のタスクを自動化する必要があることを認識しました。

もう 1 つの大きな課題は、拡大するサプライチェーンのセキュリティに対する透明性と管理性の欠如でした。同メーカーは重要なセキュリティ情報をサプライヤーに頼らざるを得ず、社内で情報のテストや検証を行う能力が限られていました。

さらに、新たな脆弱性に対し迅速に優先順位を付け、影響を受ける車両を特定するための効果的なプロセスが導入されていませんでした。これは、継続的なリスクの評価および管理要件をサポートするうえで欠かせない重要な要素です。

製品セキュリティ分析の自動化

この OEM のグローバル製品セキュリティチームは、自社の車両のサイバーリスクを包括的かつ正確に評価する必要があります。この目標を達成するには、自社の自動車に搭載されている ECU のセキュリティ状況と、既存のソフトウェアセキュリティのギャップによる潜在的なリスクの影響を詳細に把握することが不可欠です。

サプライヤーから提供される他社製 ECU ソフトウェアについては、チームに必要な正確なセキュリティ情報を取得する手段がありませんでした。ソースコードにアクセスできないため、個々の ECU のソフトウェア部品表（SBOM）を特定し、脆弱性やリスクを検出し、それらの影響を評価する能力が限られていました。

さらに、社内でのソフトウェアのテストや検証には多くのリソースと時間が必要でした。同チームでは、ECU ソフトウェアのセキュリティ検証にさまざまな方法を使用していました。これらの方法には、ソースコードにアクセスできる場合の静的コード分析をはじめとするホワイトボックステストや、サプライヤーから提供されたソフトウェアのバイナリーとしてのファジングをはじめとするブラックボックステストがありました。複数のソースやツールから得られた結果の集約と分析には、非常に多くの手作業が必要でした。

そこでチームは、可視化と効率化を図り、規模を拡大させるために、Vdoo のセキュリティプラットフォームを検討することにしました。概念実証の成功後、同チームは複数の ECU の自動セキュリティ分析へのプラットフォームの使用開始を決定しました。

Vdoo により、ソフトウェアイメージをバイナリー形式でアップロードするだけで ECU を分析し、数分で包括的な結果を得られるようになりました。このプラットフォームは、次のような詳細情報を提供します。

- ソフトウェア部品表（SBOM）、既知の脆弱性、セキュリティリスク、ECU に検出された悪質なファイル
- ソフトウェアに検出されたゼロデイ攻撃に対する脆弱性、現在の侵入テストからの補完データ
- ECU 全体とその構成を考慮し、エクスプロイトとそれによる影響の可能性に基づいた、個々の問題のスマートな優先順位
- 明確な問題解決およびセキュリティ強化のガイダンス（このチームでは実際に重要な問題の迅速な解決に活用）

生産後の脆弱性の監視と優先順位付け

この OEM は、開発段階でのサイバーセキュリティの導入に加え、継続的な脆弱性管理体制の確立と、生産後のアセットに新たに発見された脆弱性に対するより迅速な優先順位付けでも、Vdoo と協力しています。

UNECE-WP.29 サイバーセキュリティ規制および ISO/SAE 21434 では、新たな脆弱性を特定し、それらによる実際の影響を評価し、影響を受けるアセットを把握するプロセスの導入が義務付けられています。この要件を満たすには、新たな脆弱性が発生したことを把握するための脅威インテリジェンス、ソフトウェアコンポーネントに基づきこれらの脆弱性による影響を受ける車両を特定する機能、そして脆弱性による実際のリスクを評価する機能を組み合わせる必要があります。

製品セキュリティチームでは、特定のソフトウェアコンポーネントに影響を与える新たな脆弱性が自社の ECU に影響を与えるかの判断などのタスクを、人手のかかる手作業で行っていました。そのため、これらのプロセスを効率化・自動化することで、効率性とスピードを大幅に向上させたいと考えていました。

同チームは、Vdoo プラットフォームの継続的な脆弱性監視機能を活用し、以前分析したすべての ECU ソフトウェアの脆弱性を自動的に監視することにしました。これにより、Vdoo が収集・調査し継続的に更新しているセキュリティ情報に基づく関連性の高いタイムリーなアラートと、分析段階で検出されたソフトウェア構成に基づいた影響を受ける ECU に関する情報の両方を利用できるようになりました。

同社は現在路上で使用されていて、脆弱性の影響を受けるコンポーネントが搭載されている車両を自動的に特定するため、現在 Vdoo と協力し、Vdoo プラットフォームと車載ソフトウェア管理システムの統合に取り組んでいます。

オープンソースコンプライアンスのサポート

この OEM の製品セキュリティチームは、Vdoo プラットフォームのソフトウェア構成分析機能をさらに活用するため、フリー・オープンソースソフトウェア（FOSS）のライセンスコンプライアンスを担当する組織内の別のグループに Vdoo を紹介しました。

同グループでは、ベンダーに提供された SBOM リストよりも、Vdoo プラットフォームが正確にオープンソースコンポーネントを特定できるかどうかを確認するための、概念実証を行いました。概念実証ではいくつかの ECU のソフトウェアイメージの自動スキャンが行われ、自動分析の結果を確認後、ベンダーに提供されたデータと照合されました。その結果、

Vdoo はより正確な SBOM 情報を提供し、オープンソースライセンスのより確実なコンプライアンスが実現できるという結論に達しました。

Vdoo プラットフォームを使用することで得られたメリット

- **効率化** – 自動セキュリティ評価、優先順位付け、強化ガイダンス、脆弱性監視、優先順位付け機能を活用することで、この OEM は既存の手動プロセスを拡張し、製品セキュリティ関連のタスクにかかる時間と労力を削減できました。
- **リスク管理の改善** – 社内開発ソフトウェアと他社製ソフトウェアの両方に関する包括的なセキュリティ調査結果が得られたことで、同社はサプライチェーンのリスクを新たなレベルで把握し、さらなる確証と独自の評価能力を得ることができました。
- **コンプライアンスへの対応** – FOSS の構成とライセンスに関する より詳細な情報、そして自動車のライフサイクルにおける全段階でサイバーセキュリティプロセスを導入できるツールが得られたことで、同社はコンプライアンス要件に対応することができました。