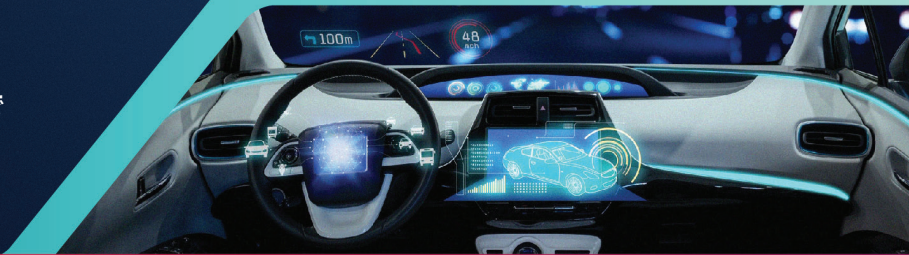




VicOne

Smart Cockpit Protection

Smart Cockpitのあらゆる側面を保護する：
個人データとプライバシーから外部接続まで



ソフトウェアを利用したサービスは、新たな収益源となります。顧客の個人情報 (PII) とデータプライバシーを守ることは、利用者からの信頼を得る上で重要です。Smart Cockpit Protectionの車載情報娯楽 (IVI) システム利用が増える中で、攻撃者は漏えいした個人情報を悪用し、顧客のSmart Cockpitや家庭ネットワークに侵入する可能性があります。これにより、攻撃者は顧客の車内や自宅での個人的な会話を盗聴したり、個人情報や車両の盗難も可能となります。顧客の個人情報、プライバシー、IVIシステム、外部接続を守る上で、車両が最も脆弱な攻撃対象になることを阻止する必要があります。

主な利点



顧客の個人情報を
保護する

VicOneのソリューションにより、自動車メーカー (OEM) は、顧客がOEMのアプリストアから直接ダウンロードするか、または車載情報娯楽 (IVI) システムにプリインストールされたSmart Cockpit用セキュリティアプリを提供できます。これにより、顧客の個人データを保護するだけでなく、OEMはサイバーセキュリティ対策からも収益を得ることが可能です。



ブランドイメージを
良好に保つ

顧客にSmart Cockpit用セッションアプリを購入する選択肢を提供することで、信頼を築き、顧客のロイヤリティを高めます。OEMは、これにより顧客が個人情報やプライバシーを守るための対策を提供できます。



新しい収益源を開拓

セキュリティを基盤として、OEMは顧客にさらに革新的なサービスを提供できます。さらに、サイバーセキュリティを収益化することで、新しい収益源を生み出すことができます。



アタックサーフェスの可
視性を広げる

システムレベルからアプリケーションレベルまでアタックサーフェスの可視性を拡大し、OEMにとって将来の脅威検出と対応のためのサポートとなります。

主要機能



車載情報娯楽 (IVI) におけるプライバシーと個人情報の保護

個人情報に過剰または不必要にアクセスする不審なアプリを検出し、ブロックします。これにより、個人情報の漏えいを防ぎます。



カーコンパニオンアプリの保護

セキュリティSDKをカーコンパニオンアプリに統合することで、OEMはアプリが安全なモバイル環境で動作することを保証し、個人情報の漏えいを防ぎます。



IVIアプリの脆弱性検出

IVIアプリには設計上の欠陥やゼロデイ脆弱性が存在することがあり、攻撃者に悪用される恐れがあります。脆弱なアプリを検出し特定することで、車の所有者がこれらを簡単にブロックし、個人情報の漏えいを防ぐことが可能です。



不正なURLの検出

定期的にブラウザの脆弱性をスキャンし、車両の所有者が不審なウェブサイトに接続しようとする際に警告します。これにより、攻撃者が個人情報にアクセスするのを防ぎます。



IVIアプリのパフォーマンスチェック

IVIアプリのパフォーマンスを継続的に監視し、電力消費やストレージ使用量を含め、異常があれば検出します。



IVIのプライバシーと身元保護

インターネットとダークウェブを監視し、顧客のクレジットカード情報、社会保障番号などの個人情報を保護します。個人情報が漏えいしたと判断されると、すぐに警告が出されます。

Smart Cockpitのセキュリティ強化

システムレベルからアプリケーションレベルまで

- 1 Smart CockpitモバイルSDK**
OEMのCar Companionアプリを保護する
- 2 Smart Cockpitセキュリティアプリ**
車載情報娯楽 (IVI) システム内の個人データ、プライバシー、外部接続をセキュアにする
- 3 xCarbon**
IDS/IPSでオンボード ECUをセキュアにする
- 4 xNexus**
VSOC向けXDRプラットフォームで脅威を検出し、対応する

