自動車業界のシステム・セキュリティ

乗車から降車までの間、乗員とその個人データを安全に保護するソフトウェア・ベースのセキュアな車載テクノロジーの開発を支援します。

概要

現在の自動車は乗員の身体の安全を確保することはもちろん、機微な個人データへのモバイル・アクセス・ポイントとしての役割も求められるようになっています。これに伴い、自動車に対するドライバーの懸念も高まっています。自動車におけるソフトウェアの役割がますます大きくなる中、アプリケーションを内製するにせよソフトウェアをサプライチェーンから調達するにせよ、現状のアプリケーション・セキュリティではもはや自動車メーカーの要求に応えることができません。悪意のあるハッカーはソースコードの弱点、パッチ未適用のオープンソース脆弱性、不適切なアプリケーション・セキュリティ・プラクティスなどを突いて攻撃を仕掛けてきます。このように、ソフトウェアが今、大きなリスク要因となっています。

セキュリティを中心に据えた開発とテストの重要性

ブラック・ダックが提供する実証済みのメソドロジーと自動化ソリューションは、開発ライフサイクルの全ステージおよびソフトウェア・サプライチェーン全体でシステム・セキュリティの強度を高めます。乗車から降車までの間、乗員とその個人データを安全に保護するソフトウェア・ベースのセキュアな車載テクノロジーを開発できるように、ブラック・ダックは世界中の OEM およびティア 1、ティア 2 サプライヤを支援しています。ソースコードおよびバイナリに含まれるサードパーティ・コンポーネントの検出、セキュリティ脆弱性と使用中のライセンスの優先付け、コードの重大な不具合や弱点の発見など、これらはすべて開発段階で自動的な実行をサポートします。また、設計の欠陥、制御の不具合、資産の脆弱性などシステムにとっての全体的なリスク要因を特定することによって、開発ライフサイクルの設計フェーズもサポートします。

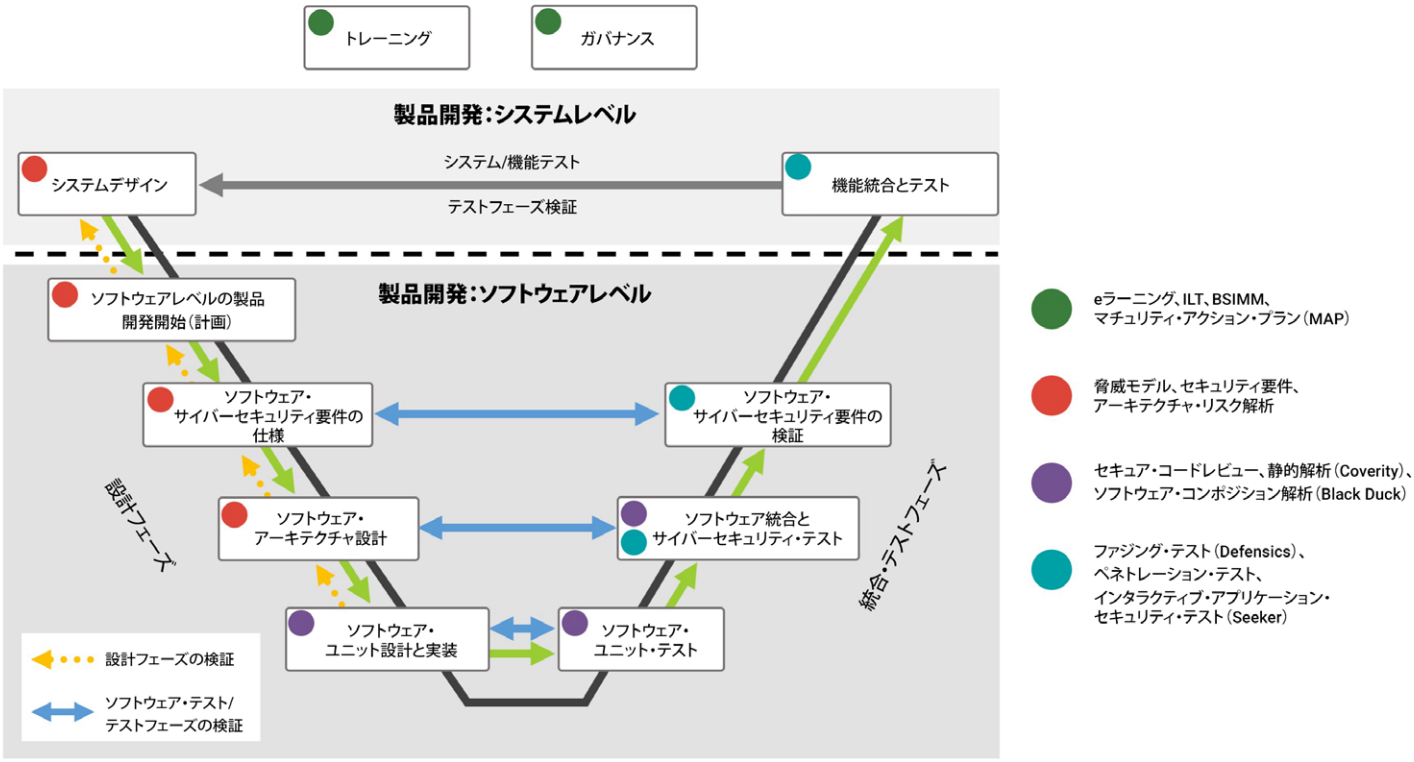
開発ライフサイクルとサプライチェーン全体を通じてリスクを管理

ブラック・ダックは、自動車業界のシステム・セキュリティに対してテクノロジー・リスク管理の基本に則ったアプローチを採用しています。自動車業界特有のニーズをサポートするため、ブラック・ダックは自動車業界の企業にとって特に重要性の高い以下のような活動を実施しています。

- バスに対する解析、ファジング、キャプチャ、リバース・エンジニアリング
- 車両エコシステムの脅威モデリングとアーキテクチャ・リスク解析
- 組み込みコードに対するレビュー、ペネトレーション・テスト、リバース・エンジニアリング
- 通信インターフェイス・テスト（オンボード、ワイヤレス、ディーラー、製造）
- テレマティクス、インフォテインメント、ヘッドユニットのテスト
- 証明書、暗号化、鍵保存に関する解析とテスト
- プログラムの設計と開発
- ソフトウェア・セキュリティ・トレーニング

開発ライフサイクル全体にわたる安全性とセキュリティへの取り組み

私たちはシステム開発ライフサイクルと、セキュリティが安全性と品質に与える影響を理解しています。



車載ソフトウェアに最高水準のセキュリティを

ツール	業界をリードするブラック・ダックの静的解析 (ISO 26262 認証取得済み、MISRA および AUTOSAR のコーディング・ガイドラインをサポート)、ファジング・テスト (CAN、CAN-FD などをサポート)、インタラクティブ・アプリケーション・セキュリティ・テスト、ソフトウェア・コンポジション解析ツールにより、ソフトウェア・スタックに潜む脆弱性を見つけます。 ソースコードおよびバイナリに含まれるサードパーティのオープンソース・コンポーネントを検出します。脆弱性は開発期間だけでなく本番環境のコンテナまで追跡し、修正します。サードパーティのライセンスを特定し、コンプライアンス違反を防ぐためのポリシーを設定できます。
組み込みペネトレーション・テスト	ECU などの組み込みシステムの機能とセキュリティを検証し、組込みソフトウェア・スタックに潜む脆弱性を特定します
アーキテクチャ / 設計	アーキテクチャ・リスク解析と脅威モデリングにより、アーキテクチャ、設計、システムの不具合と欠陥を見つけます。
トレーニング	インストラクターによる指導、e ラーニング、バーチャル・クラスなどさまざまな形態のセキュリティ・トレーニング・コースを通じ、開発者のセキュリティ意識を高めることができます
セキュリティ統合のためのプログラム	プログラムの成熟度をアセスメントする BSIMM、マチュリティ・アクション・プラン (MAP)、セキュリティ・メトリクス、各種ソフトウェア・セキュリティ・イニシアティブ・プログラム

システム・リスクへの対処のストラテジーを定義

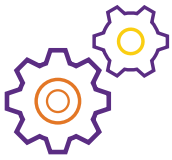
視認性を高める

- 開発およびテスト・プラクティスの弱点と不備を特定
- セキュリティの知見を SDLC 全体および本番環境へ拡張

シフトレフト

- 品質、セキュリティ、安全を SDLC 全体に統合
- 開発スピードを損なわず問題を早期に検出

自動化



- 継続的テストにより、遅れや人的ミスの可能性を防止
- トリガー、ワークフロー、ポリシーを確立

維持管理

- 脆弱性や不具合を管理、監視
- ソフトウェア・サプライチェーン全体でリスクの移転を追跡

円滑化

- ビルトイン方式のセキュリティと品質
- 開発ワークフローに統合

意識の確立

- 従業員全体のセキュリティ意識を最大限に向上
- セキュリティのスキルを高め、成果への利害関係を全員で共有

ブラック・ダックの製品

Coverity
静的解析

Black Duck
ソフトウェア・コンポジション解析

Seeker & Defensics
動的解析

ブラック・ダックのサービス

プロフェッショナル・サービス

セキュリティ戦略と企画

マネージド・サービス

自動車業界への関与

ブラック・ダックは自動車業界全体でサイバー・セキュリティに関するベスト・プラクティスの発展と普及に全力で取り組んでおり、幅広い業界団体で積極的な活動を展開しています。

SAE INTERNATIONAL
ISO
MISRA
AUTOMOTIVE GRADE LINUX
UL
DEKRA
AUTOSAR

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。
詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社
www.blackduck.com/jp