Empowering Tomorrow's Automotive Software
www.etas.com

ESCRYPT 侵入検知 / 防止ソリューション

車両のライフサイクル全体に対する効率的なリスク管理

車両のコネクテッド化が進むにつれて攻撃の侵入経路が増え、脅威の状況は常に変化します。このセキュリティ侵害は、車両のみならずバックエンドサービスにまで及びます。

したがって、コネクテッドフリートに適切なセキュリティを維持するには、包括的かつ継続的な活動が必要です。今後制定される規制と標準によって、セキュリティの状況と潜在的な攻撃に関する詳細な知識が求められるでしょう。そのため、車両コンポーネントとその通信、フリートの IT インフラストラクチャ、そして自動車の脅威の状況全体といったライフサイクルアプローチが必要となります。

脅威の状況の変化

コネクテッドカーに対する脅威の状況は常に進化しています。

遵守すべき規制

コンプライアンスに準拠したサイバーセキュリティ管理は、自動車業界の管理者にとって重要な要素となっています。UN-R155 および ISO/SAE 21434 では、ライフサイクル全体にわたって車両セキュリティを確立し、型式認証を受けることが義務付けられています。

ETAS の提案

ETAS は、自動車メーカーが永続的なセキュリティ監視と継続的なライフサイクルを確立できるようにする、コネクテッドフリート向けの侵入検知 / 防止ソリューション (IDPS) を提供します。

包括的なエンドツーエンドソリューション

自動車向けの ESCRYPT IDPS ソリューションは、複数の車載 IDPS ソフトウェアコンポーネントと、バックエンド側のマネージドセキュリティサービスとしての ESCRYPT の車両セキュリティオペレーションセンター (VSOC) で構成されており、お客様の特定のニーズに合わせてカスタマイズ可能です。ETAS は IDPS についてオープンアーキテクチャのコンセプトを採用し、そのソリューションコンポーネントは、個々のビルディングブロックとしても利用できます。

ESCRYPT IDS センサは、重要なセキュリティイベント情報を引き出します：

- ESCRYPT CycurIDS-CAN による CAN、CAN-FD のネットワークベース侵入検知
- ESCRYPT-Cycur-IDS-ETH によるイーサネットのネットワークベース侵入検知
- ESCRYPT CycurGATE による車載イーサネットファイアウォール
- 豊富なオペレーティングシステムと外部インターフェースを備えたシステム向けのホストベースの侵入検知

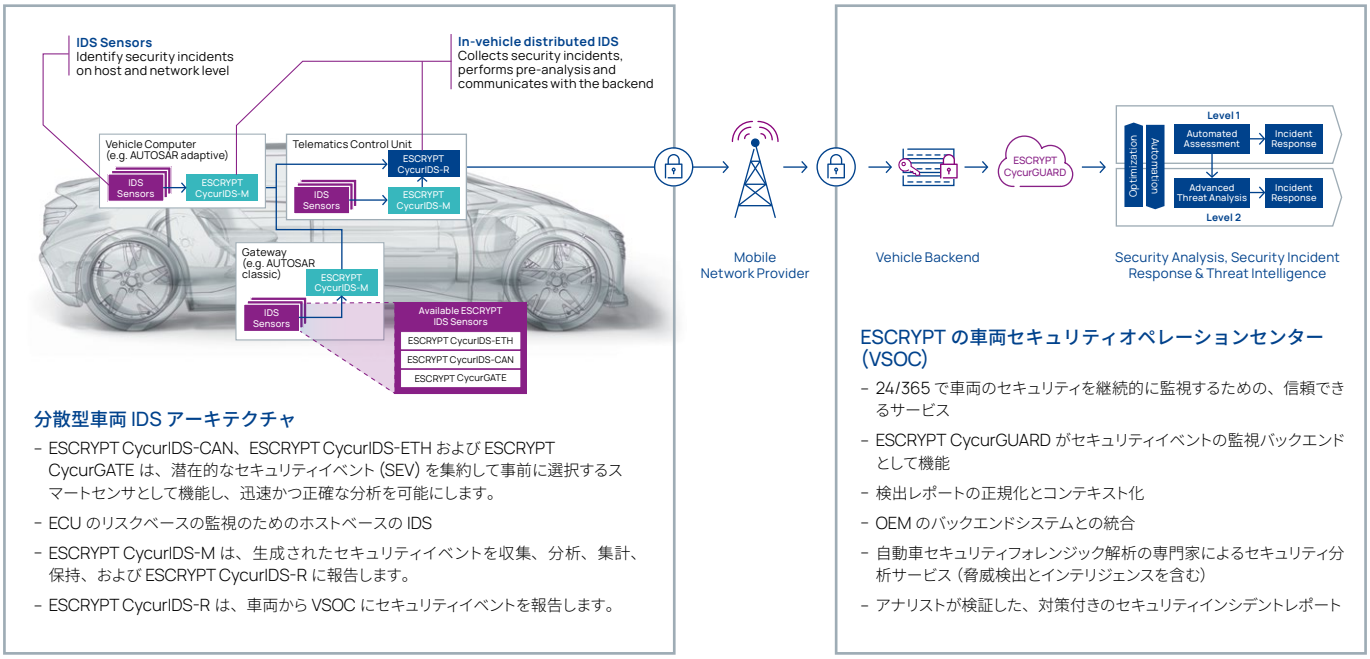
ESCRYPT 分散型 IDS フレームワークは、関連するセキュリティ イベント情報を選択、保持、転送します：

- ESCRYPT CycurIDS-M の 2 つのバリアント
  - 組み込み ECU 向け（Classic AUTOSAR または RTOS 向けの µC）
  - Adaptive AUTOSAR および / または POSIX OS を実行するプラットフォーム（µP）

  ECU、車両ドメイン、または車両全体のセキュリティイベント情報を管理。AUTOSAR IDS Manager (IdsM) 仕様に準拠した ESCRYPT CycurIDS-M バリアントを使用すると、任意のフィルタリング、保持、レポート作成計画に合わせて調整可能。
- 車両から VSOC へのセキュリティイベント情報をレポートする ESCRYPT CycurIDS-R

ESCRYPT Vehicle Security Operations Center は、フリート全体の監視を可能にします：

- ESCRYPT CycurGUARD は、ETAS のバックエンドソリューションを活用して、車両フリートと車両バックエンドシステムからのすべてのセキュリティイベント情報を統合
- 単一のソースから完全な車両セキュリティ運用サービスを提供



分散型車両 IDS アーキテクチャ

- ESCRYPT CycurIDS-CAN、ESCRYPT CycurIDS-ETH および ESCRYPT CycurGATE は、潜在的なセキュリティイベント (SEV) を集約して事前に選択するスマートセンサとして機能し、迅速かつ正確な分析を可能にします。
- ECU のリスクベースの監視のためのホストベースの IDS
- ESCRYPT CycurIDS-M は、生成されたセキュリティイベントを収集、分析、集計、保持、および ESCRYPT CycurIDS-R に報告します。
- ESCRYPT CycurIDS-R は、車両から VSOC にセキュリティイベントを報告します。

ESCRYPT の車両セキュリティオペレーションセンター (VSOC)

- 24/365 で車両のセキュリティを継続的に監視するための、信頼できるサービス
- ESCRYPT CycurGUARD がセキュリティイベントの監視バックエンドとして機能
- 検出レポートの正規化とコンテキスト化
- OEM のバックエンドシステムとの統合
- 自動車セキュリティフォレンジック解析の専門家によるセキュリティ分析サービス（脅威検出とインテリジェンスを含む）
- アナリストが検証した、対策付きのセキュリティインシデントレポート

脅威検出、脅威インテリジェンス

ESCRYPT-CycurGUARD は、コネクテッドフリート全体から収集されたデータを解析して新たな脅威の識別を可能にします。ETAS は、バックエンドの監視製品を使用して、運転中の車両の異常レポートの収集と解析を行う統合型ソリューションを提供します。

ESCRYPT CycurGUARD は、膨大なデータベースから関連するデータを収集、前処理することで、重大な脅威を確実に識別します。異なるドメイン（車両、インフラストラクチャ、バックエンドサービス）からのデータが相互に参照可能であり、SIEM（Security Incident & Event Management）が自動化や手作業でのすべての検知機能を利用できるようにします。

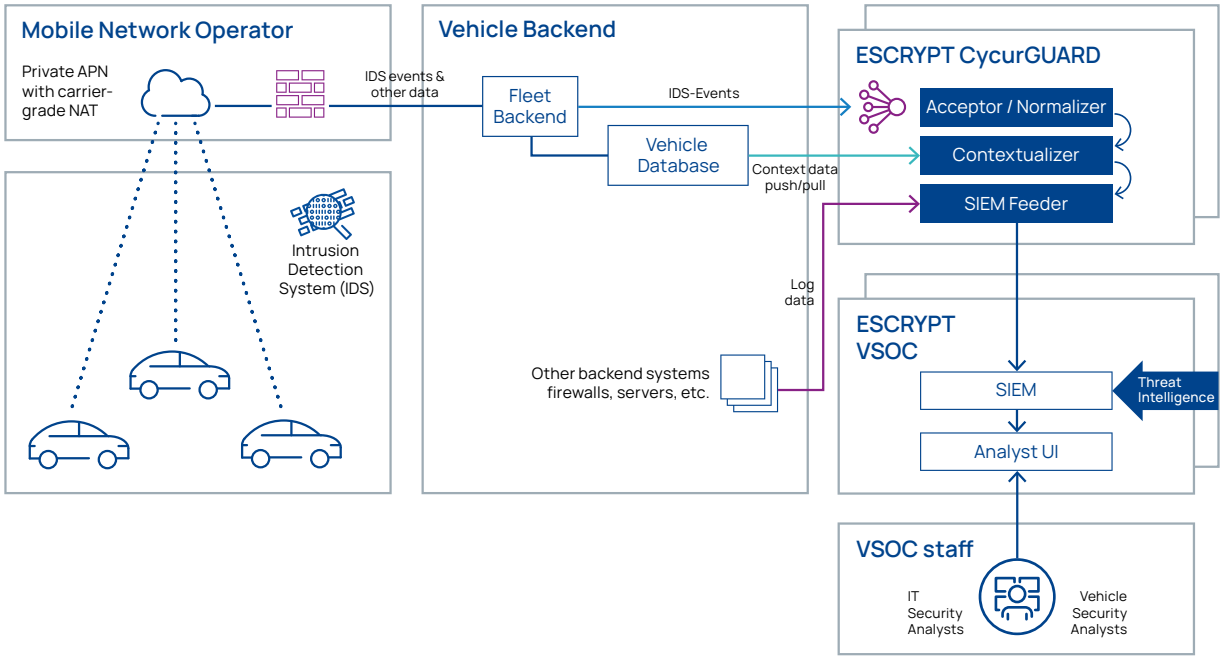
VSOC は、日々増大する、既知の攻撃パターンのデータベースを参照することで、差し迫った脅威を確実に特定し、アドホックまたは事前に作成されたレポートを使用してコネクテッドフリートの安全性やセキュリティを評価します。

インシデントレスポンスプロセスやセキュリティ分析は、自動車セキュリティに特化したフォレンジック解析のエキスパートに引き継がれます。主要な IT セキュリティサービスプロバイダによる包括的なハニーポットインフラや脅威インテリジェンスと、ETAS の自動車に特化したパブリックリソースとを組み合わせることで、専用の脅威インテリジェンスサービスを実現します。

強力なパートナーシップ

ETAS は、主要な IT セキュリティサービスプロバイダーと協力することで、セキュリティオペレーションセンター（SOC）のコミッショニング、インフラストラクチャ、サービスを提供しています。この協業により既存の SOC インフラストラクチャを拡張し、スキルのある自動車セキュリティアナリストとフォレンジック解析の専門家を加え、高度に専門的で、市場に対応した総合的なソリューションを作り上げました。

ETAS の車両セキュリティオペレーションセンターをご利用のお客様は、コネクテッドフリートの特定の要件に合わせて完全にカスタマイズされた、管理の行き届いたセキュリティサービスをご利用いただけます。



ESCRYPT 侵入検知 / 防止ソリューションのアドバンテージ

- 車両侵入検知 (IDS) とセンサによる分散フレームワーク、セキュリティ監視バックエンドと完成された SOC サービスによる包括的なセキュリティソリューション
- フィールドでの攻撃の継続的な監視
- 攻撃のタイムリーな検出
- フォレンジック解析の専門家によるセキュリティ分析
- フリート全体のアップデートにより、対策のロールアウトが可能
- 個々のコンポーネントとして、または車両フリートの必要性に合わせてカスタマイズされたエンドツーエンドのワンストップソリューションとして提供
- AUTOSAR 準拠
- UN-R155 などの法規制に準拠

ETAS の製品とソリューションに関するお問い合わせ：
info@etas.com

製品の詳細情報：
www.etas.com/IDPS

ETAS/COM-JP/03-2023