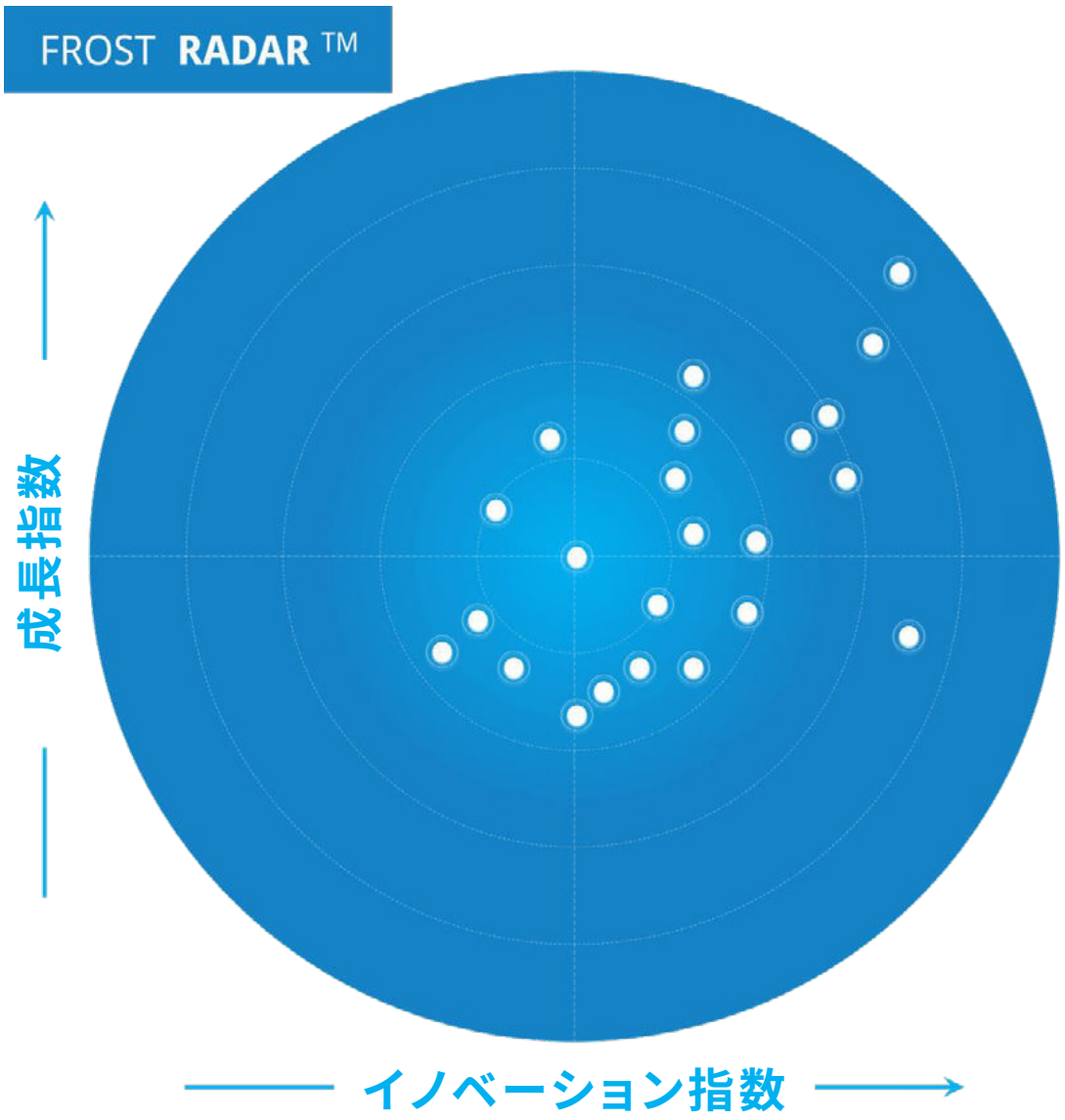
自動車サイバーセキュリティ 2024

企業のアクションを促すためのベンチマークシステム - 新たな取引や成長パイプラインを醸成するイノベーション

著者Dorothy Amy
寄稿Thanigesh Parthasarathi



PF9E-42
May 2024

リサーチ概要

このFrost Radar™では、自動車メーカー（OEM）やTier1サプライヤー向けの先進的なサイバーセキュリティ・ソリューションを積極的に推奨している自動車サイバーセキュリティ分野の大手企業7社を取り上げています。

このRadarは、Argus Cyber Security、Upstream Security、Karamba Security Ltd、AUTOCRYPT、Cybellum Technologies LTD、VicOne、ETAS GmbHなど、自動車業界が直面するサイバーセキュリティの課題に取り組む主要なサイバーセキュリティのスペシャリスト企業を評価しています。

このRadarでは、イノベーション指数と成長指数に基づいてこれらのベンダーを評価し、各社の市場における強さを示しています。この分析では、各社のサイバーセキュリティ製品、研究開発（R&D）の取り組み、収益の流れ、投資活動、顧客基盤、将来戦略について概要をまとめています。さらに、各ベンダーのサイバーセキュリティ技術と、自動車サイバーセキュリティのランドスケープにおけるその採用の根拠について深掘りしています。

このFrost Radar™を読めば、業界関係者は、自動車業界におけるサイバーセキュリティの課題、ビジネスモデルのシフトの予測、自動車サイバーセキュリティベンダーとの協業時に考慮すべき重要な機能の特定について、貴重な洞察を得ることができます。

フロスト&サリバンは、業界の多くの企業を分析しています。その中からリーダーシップやその他の卓越性に基づいてさらなる分析を行う企業を選び、10項目の「成長」と「イノベーション」の基準でベンチマークを行い、Frost Radar™でのポジションを確定します。本レポートでは、Frost Radar™における各企業の強みと、その強みに最も適したビジネスチャンスを考慮した競合プロファイルを紹介しています。

戦略的重要性

自動車のサイバーセキュリティ業界は、自動車へのデジタル技術の統合が進むにつれて牽引力を増しています。自動車のコネクテッド化が進み、自動運転機能が組み込まれるにつれて、サイバー脅威から車両システムを保護することが急務となっています。この業界の特徴は、新興の自動車セキュリティを専門とするサイバーセキュリティ企業の登場と、昔から続く強固な自動車メーカーとテクノロジー企業との協力関係といえます。

AIを活用したサイバーセキュリティ・ソリューションは、積極的な脅威検知、異常検知、適応的な防御メカニズムを可能にすることで、自動車業界に革命をもたらそうとしています。これらの先進的なソリューションは、進化するサイバー脅威に対する自動車システムのレジリエンスを確保するために極めて重要になってくると思われます。

自動車メーカーが自動運転、V2G充電（Vehicle to Grid）、V2X通信（Vehicle to Everything）、OTA（Over-the-Air）アップデートなどの最先端技術を統合しようとする上で、強力なサイバーセキュリティ・ソリューションの必要性はますます高まっています。効果的な自動車サイバーセキュリティ・ソリューションは、サイバー攻撃のリスクを軽減するだけでなく、消費者の信頼を醸成し、次世代コネクテッドカーや自動運転技術の普及を促進します。

このFrost Radar™は、自動車サイバーセキュリティ業界における極めて重要な変化と技術的進歩を理解し、コネクテッドカーのエコシステム内で脅威が進化する中、関係者が自動車のセキュリティを強化するためにそれらをどのように活用しているかを示しています。

分析には、ベンダーと技術の評価、パートナーおよび顧客のエコシステム、競合指標と地域のフットプリント、業界概要が含まれます。業界概要では、消費者とステークホルダーの信頼を醸成し、スマートカーおよびコネクテッドカーの進化を促進し、自動車エコシステムの乗客の安全を確保するという点において自動車サイバーセキュリティの重要性を取り上げています。

成長環境

自動車サイバーセキュリティ業界は新たな成長段階にあり、デジタル技術の自動車への統合に伴うセキュリティとデータ・プライバシーのリスクの高まりを緩和するために、急速な拡大が見込まれています。コネクテッドカーや自動運転システムの普及に伴い、サイバーセキュリティの確保は自動車メーカーやバリューチェーン全体の関係者にとって最重要課題となっています。

車載侵入検知・防御システム、脅威評価・脆弱性管理、サイバーセキュリティ管理システムは、自動車のライフサイクル全体を通じて継続的に脅威を監視するよう求める規制に対応するために必要とされる主要なソリューションの一例です。

政府や規制機関は、自動車メーカーがコンプライアンスに適合できるよう、自動車のサイバーセキュリティ標準や規制を継続的に強化しています。例えば、国連欧州経済委員会（UNECE）のWP.29規制は、コネクテッドカーのサイバーセキュリティマネジメントシステムを義務付けており、自動車メーカーは製品開発とコンプライアンス戦略においてサイバーセキュリティ対策を優先するよう求められています。UNECEの規制要件（UN R155およびR156）は、欧州連合（EU）、英国、日本、韓国を含む54の加盟国に適用されます。非加盟国は、加盟国での販売を可能にするために、これらの規制の影響について見極めようとしています。

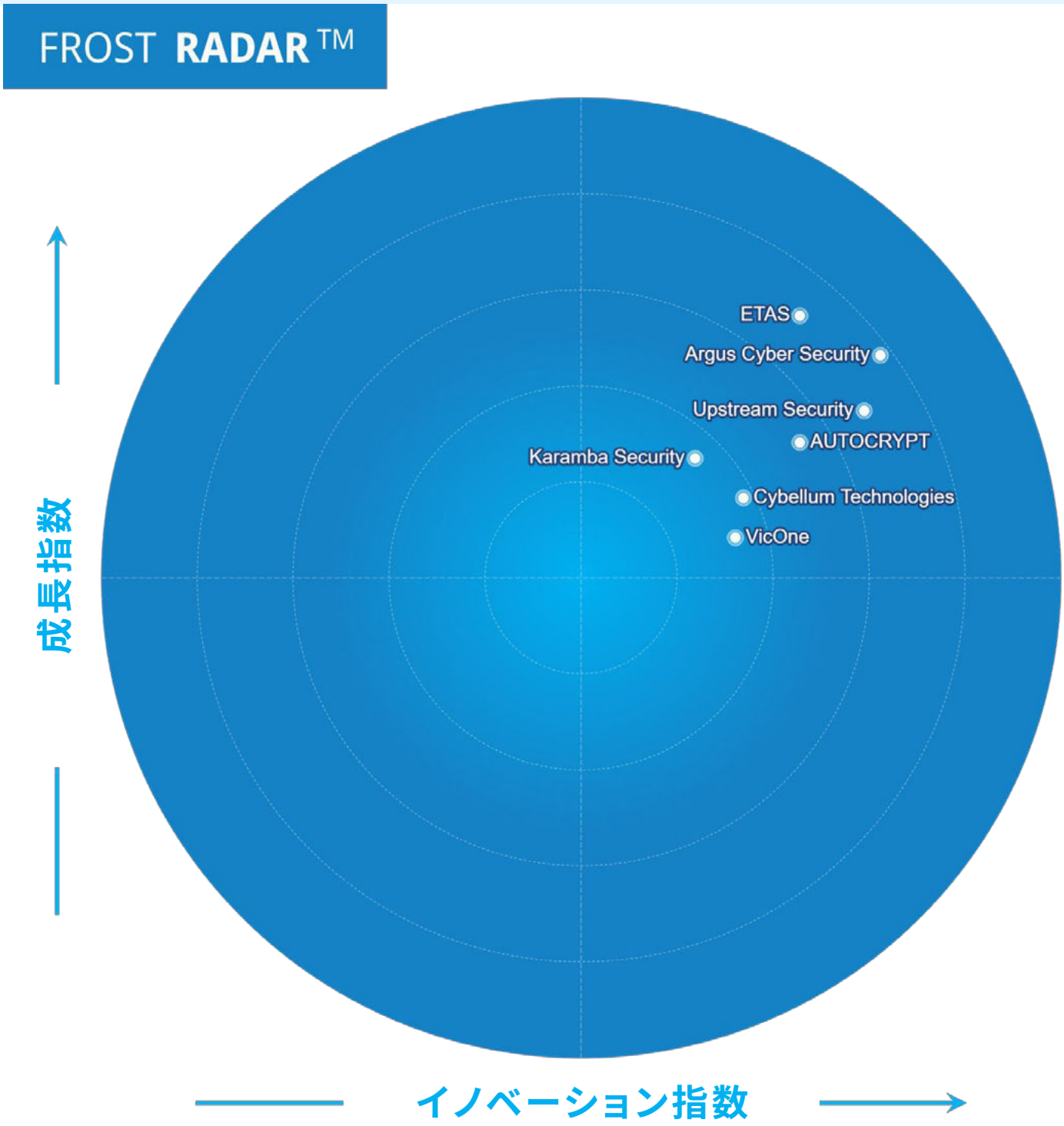
サイバーセキュリティの課題に効果的に対処するためには、関係者が一丸となって取り組む必要があることが認識されるにつれ、自動車メーカー、サイバーセキュリティ企業、テクノロジー・プロバイダ間の協力がますます広まっています。パートナーシップや提携は、イノベーションを醸成し、ベストプラクティスを共有し、自動車エコシステム特有の要件に合わせた最先端のサイバーセキュリティ・ソリューションの開発に貢献することを目的としています。

人工知能（AI）、機械学習（ML）、ブロックチェーンなどの技術の進歩は、自動車サイバーセキュリティの革新を促進します。AIを活用した脅威検知アルゴリズム、MLベースの異常検知システム、ブロックチェーンを活用したセキュアな通信プロトコルは、自動車のサイバーセキュリティへの取り組み方に革命をもたらし、進化するサイバー脅威に対する積極的な防御メカニズムを提供する態勢を整えています。

この独自分析に関連するフロスト&サリバンの調査

- Global Automotive Cybersecurity Growth Opportunities
- Global Quantum Computing Growth Opportunities

Frost Radar™



Source: Frost & Sullivan

競合環境

20以上のグローバル企業が存在する業界において、自動車業界における革新的なサイバーセキュリティ企業7社を以下のように特定しました。Argus Cyber Security、ETAS GmbH、Upstream Security、AUTOCRYPT、Cybellum Technologies LTD、Karamba Security Ltd、VicOne。

自動車のコネクティビティが高まるにつれて、サイバーセキュリティは自動車業界では重要な必須条件となっています。自動車OEMは、二輪車、スクーター、電動自転車、乗用車、ピックアップトラック、商用車、共有モビリティフリートなどの車両の型式承認を取得するために、UN R155やISO 21434などの自動車サイバーセキュリティ規制や標準に準拠する必要があります。

より厳格なセキュリティ規制を遵守するという差し迫ったニーズに対応するため、自動車業界ではサイバーセキュリティに独自のアプローチを採用するテクノロジー企業が急増しています。サイバーセキュリティの専門ベンダー、サイバーセキュリティ部門を統合したテクノロジー企業、社内にサイバーセキュリティ・チームを擁するティア1サプライヤーが、この領域で技術革新とより優れたソリューションの提供を競い合っています。

アルガスは、車載セキュリティ製品、アフターマーケットの自動車盗難防止ソリューション、脆弱性分析、脅威緩和ソリューション、車両セキュリティテスト、コンプライアンス関連サービスなど、サイバーセキュリティ・ソリューションの豊富なポートフォリオが評価され、イノベーション指数でトップの座を獲得しました。その包括的なポートフォリオに加え、同社は自動車ソフトウェア開発に特化した新しいDevSecOpsプラットフォームを立ち上げ、ソフトウェア開発プロセス全体のエンドツーエンドのセキュリティ対策を促進しています。アルガスは、対応が迫られる二輪車（2W）セグメント向けのコンプライアンスへのサービスからも明らかなように、進化する規制に適応する能力で際立っています。アルガスはまた、2021年以降500%という驚異的な収益成長を示し、成長指数でも2位にランクインしました。

ETAS GmbHは、Radarの成長リーダーとして、2023年には競合他社と比べて最も高い収益を記録し、力強い成長軌道を示しています。ヨーロッパ、アジア、アメリカ大陸にまたがる同社の広大なプレゼンスは、多様な地域で新規顧客を獲得する可能性を確固たるものにしています。

Upstream Securityは、画期的なクラウド対応アプリケーションと充実したソリューション・ポートフォリオにより、成長指数で2番目に高い順位を獲得しました。同社は、モビリティに特化した幅広いユースケースへの継続的な投資と、自動車分野でより多くの利用者を惹きつけるための戦略的パートナーシップによって差別化を図っています。

AUTOCRYPTは、V2Xと電気自動車充電のセキュリティソリューションの開発により、イノベーション指数で3位にランクし、競合他社と差別化されています。業界唯一のV2Xセキュリティソリューションを提供することで、自動運転車の未来を定義することに注力しています。V2Xソリューションは複数のV2Gルート環境に対応し、異なる車種を管理するサービスプロバイダーで長年の課題であった互換性問題を解決します。同社は現在までに合計37件の車両セキュリティ関連プロジェクトを受注しており、好調な収益をあげています。

Karambaの成長指数における競争力は、主に自動車業界における重要な顧客リストとセキュリティ契約によるものです。フォーチュン500の企業との契約を通じて、Karambaは100カ国以上で80万台のフリートに製品を提供しています。

CybellumとVicOneは、イノベーション指数でAUTOCRYPTに次ぐ2位を占めています。Cybellumの強力な製品セキュリティプラットフォーム、自動車関係者との先見的なパートナーシップ、強力な顧客は、その効果的な成長戦略を示しています。

しかし、製品ポートフォリオが少ないため、イノベーション指数における位置づけは限定的です。VicOneは、最近行ったClientronとの提携により、電気バスへのソリューションを拡張しましたが、アジア太平洋地域に主眼を置いているため、成長指数での位置づけは限定的です。

注：C2A Securityも対象として検討しましたが、過去2年間に製品の方向性が変わったため、客観的な比較ができませんでした。

アルガスサイバーセキュリティ

イノベーション

- アルガスサイバーセキュリティは、自動車部品、ネットワーク、車両を保護し、業界規制へのコンプライアンスを確保するために、OEMやサプライヤーを支援する自動車サイバーセキュリティへの包括的なアプローチをとっています。同社の多様な製品とサービスには、車載セキュリティ、脆弱性評価、脅威緩和、車両セキュリティテスト、コンプライアンス関連ソリューションが含まれます。
- アルガスは100件以上の自動車サイバーセキュリティ関連の特許を取得・出願中であり、自動車業界における様々なサイバーセキュリティの脆弱性に対応する独自のソリューションの拡張性を実証しています。
- 同社は、マイクロソフト、AWS、グーグル、Eviden、Checkpoint Software、IBMなどのテックリーダーと提携し、サイバーセキュリティ・ソリューションの機能を強化しています。
- dSPACE、Elektrobit、およびAmazon Alexaとのコラボレーションは、開発プロセスの合理化や音声アシスタントプラットフォームとの統合など、サイバーセキュリティソリューションの機能強化のためにパートナーシップを活用するアルガスの革新的なアプローチを明確にしています。
- Argus vDomeは、新車および中古車を盗難や不正行為から守る独自のサイバーセキュリティ製品です。vDomeは、悪意のあるデバイスを200マイクロ秒以下で検出します。CANバス上のすべてのECUを識別し、ECU信号ごとに固有の電気的シグネチャを作成します。
- 2024年、アルガスは自動車ソフトウェア開発に特化した新しいDevSecOpsプラットフォームを発表しました。OEMやTier1サプライヤー向けに設計されたこのプラットフォームは、ソフトウェア開発プロセスの全ての段階においてセキュリティ対策をシームレスに統合します。これにより、自動車メーカーは市場投入までの時間を短縮し、大幅なコスト削減を実現できます。
- AI技術を製品に組み込むことで、同社は顧客に魅力的なソリューションとデータ主導のインサイトを提供し、業界における競争力を高めています。

成長

- アルガスは、主に自動車サイバーセキュリティ・ソリューションに注力することで、2021年以降500%という目覚ましい収益の成長を遂げています。この大幅な増収は、成長指数の総合ランキングで2位を確保する同社の成長性に貢献しています。
- 100件以上の特許を取得・申請中であり、過去10年間に1億5,000万ユーロ以上を投資したアルガスは、自動車のサイバーセキュリティに特化した革新的なソリューションの開発に積極的であることを示しています。
- 現在までに、アルガスは91の顧客と45の量産プロジェクトを手掛けており、7,000万台以上の自動車にセキュリティを提供しており、自動車サイバーセキュリティ業界における目覚ましい収益の可能性を示しています。
- 2023年時点では、アルガスはシュトゥットガルト、デトロイト、韓国、東京など戦略的な地域にオフィスを設立しており、これは新たな地域で存在感をだし、成長の可能性を拡大する努力を反映しています。
- アルガスは従来の乗用車に対応するだけでなく、コネクテッドトラック、特に二輪セグメント（サイバーセキュリティ・プロバイダーは一握りしかいない）やシェアード・モビリティ・フリート事業者にもサービスを拡大しています。自動車業界内におけるサービスの多角化により、リーチ可能な市場規模が拡大しています。

フロストの視点

- アルガスは、革新を加速し、幅広いサービスとソリューションを構築するために、業界のリーダーたちとの模範的なパートナーシップを展開しており、自動車サイバーセキュリティ分野におけるイノベーションのリーダーシップを確固たるものにしています。
- アルガスのvDomeソリューションは、このタイプでは初めての画期的なアフターマーケット向け盗難防止製品であり、路上の何百万ものコネクテッドカーを保護する実行可能な手段を提供します。これは、今後3～5年間にわたってアルガスの重要な成長エンジンとなりえます。
- 同社は、オートバイ、スクーター、電動自転車を含む2輪車セグメントにおけるサイバーセキュリティのコンプライアンスサービスで際立っています。アルガスは、このニッチな2輪車セグメント向けに専用のセキュリティ製品を開発することで、先行者利益を確立し、サイバーセキュリティ業界における需要を喚起します。
- 自動車業界が電気自動車や自動運転車への移行を進める中で、これらの車両から生成されるデータを保護する需要が高まっています。アルガスは、V2X、V2G、電気自動車の充電インフラの通信を含むスマートモビリティエコシステムのサイバーセキュリティに関する課題に対処し、新たな機会を探ることを検討すべきです。

戦略的インサイト

1. 革新的な収益化モデルは、最先端のセキュリティソリューションに対する将来の需要を最大化することが期待されています。提供される保護のレベルや検出・防御されたセキュリティインシデントの数に基づいてサイバーセキュリティベンダーに支払いを行うような使用量に応じた価格モデルへとOEMが移行するかもしれません。また、サブスクリプションベースのサービスや利用する都度支払う契約も普及し、OEMはサイバーセキュリティコストの管理における柔軟性とスケーラビリティを得ることができるかもしれません。市場の動向に合わせて収益化戦略を適応させることで、サイバーセキュリティベンダーは自動車業界の関係者に大きな価値を提供し、長期的なパートナーシップと収益の成長を促進することができます。

2. 自動車エコシステム内のステークホルダー間の協力が、サイバー脅威を効果的に低減するために必要になるでしょう。OEM、サプライヤー、サイバーセキュリティ企業、規制機関、政府機関は、脅威インテリジェンス、ベストプラクティス、脆弱性の情報を共有するための協力的な枠組みを確立することを期待されています。こうしたエコシステムは集団防衛的なアプローチを促進し、自動車のサプライチェーン全体で新たな脅威の迅速な特定と緩和を可能にします。

3. 車両が「走るソフトウェア」となるにつれて、生成AI技術をサイバーセキュリティソリューションへ統合することが重要になります。ベンダーは生成AIを活用して、進化するサイバー脅威をリアルタイムで予測し、それに適応することで、自動車のサイバーセキュリティシステムのレジリエンスを強化するべきです。さらに、物理的な車両の仮想レプリカであるデジタルツインの開発により、潜在的なサイバー攻撃や脆弱性をシミュレーションすることで、積極的な脅威検出と緩和が可能になります。AIとサイバーセキュリティのこの融合は、予測的および先制的な防御メカニズムに重点を置くことで、自動車セキュリティ戦略の未来を形作るでしょう。

4. 今後数年間、世界中の行政機関は自動車サイバーセキュリティの状況を形作る上で重要な役割を果たすでしょう。路上の安全とデータプライバシー保護への関心が高まる中、規制機関はコネクテッドカーや自動運転車のサイバーセキュリティ標準を規定する厳しいガイドラインを導入していくでしょう。これにより、自動車メーカーは規制を遵守するための特別な取り組みを採用し、サイバーセキュリティ対策に多額の投資を行わなければなりません。これらの規制は、サイバーセキュリティ対策の実施において、より高い透明性と責任を求めるものになるでしょう。このため、OEMは積極的なリスク評価手法を採用し、コネクテッドカーや自動運転車のセキュリティを確保するために業界のベストプラクティスを維持する必要があります。

法的免責事項