SGS社と実現する 一気通貫の自動車向け サイバーセキュリティ

2025年5月23日

VicOne株式会社
日本地域代表　ヴァイスプレジデント
小田　章展

VicOne
Driving Automotive Cybersecurity Forward

自己紹介

小田　章展（Oda Akinobu）

＜所属・担当＞
日本地域代表　ヴァイスプレジデント
セールス ＆ ビジネス開発統括

＜経歴サマリ＞

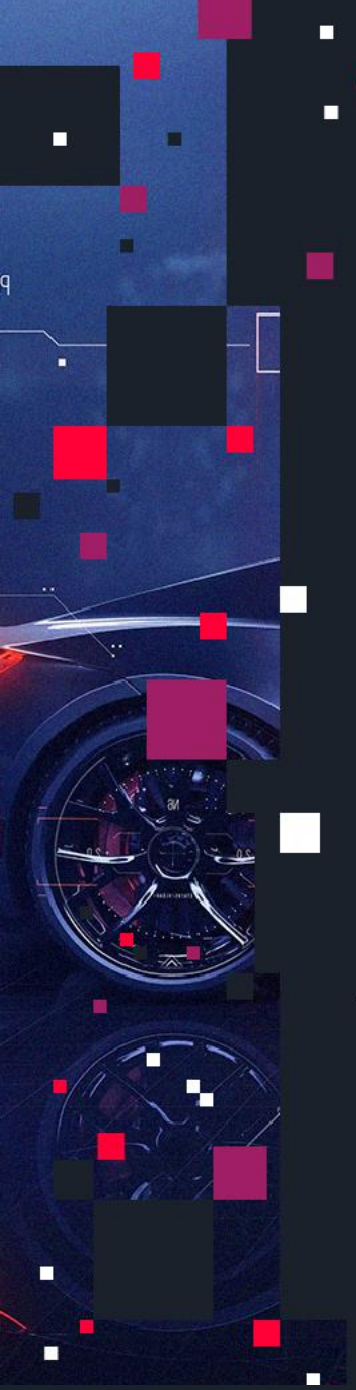
日系電機メーカー	エレクトロニクス商社	コンサルティングファーム	現職 セキュリティベンダー
カーナビ設計開発	IoT FAE・事業開発	IoTコンサル	•セキュリティBiz開発 •新会社VicOne立上

IoT、セキュリティ系の事業開発・コンサル

ベンチャー立上

Agenda

1. 自動車業界を取り巻く状況
2. 会社紹介
3. VicOneのソリューション
4. SGS社との協業によるトータルソリューション
5. まとめ



1. 自動車を取り巻く状況

自動車のテクノロジー進化とセキュリティの必要性の向上

自動車を取り巻くテクノロジーは日々進化しており、IT等の他分野で活用されている技術が続々と自動車に展開。同時にサイバーセキュリティの重要性が高まっている

Connected

Electric (EV)

OTA

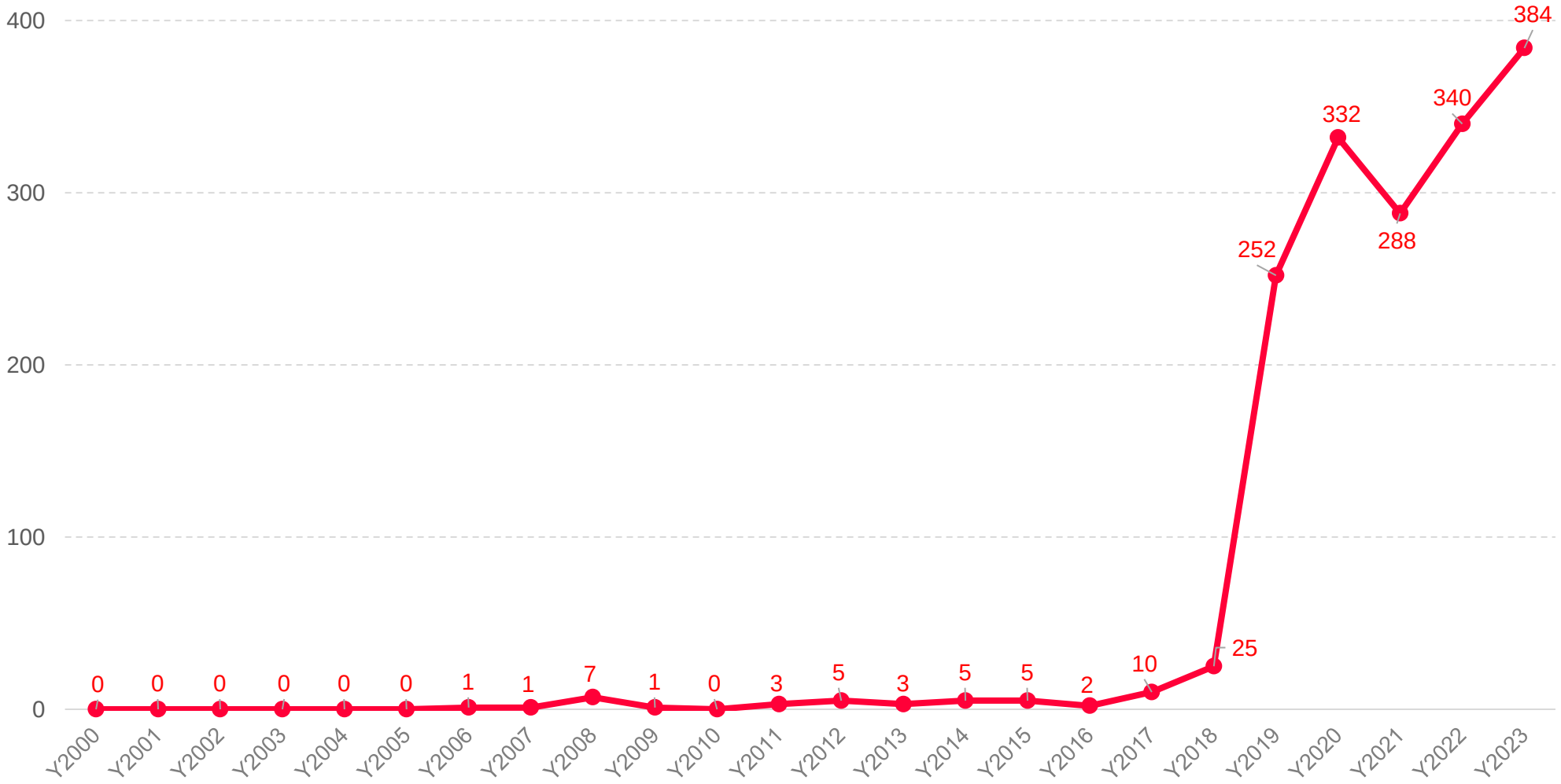
SDV

自動運転

AI

自動車関連の脆弱性の増加と態勢強化の必要性

2018年以降、IoT等のコネクテッドテクノロジーの普及に伴い、自動車関連の脆弱性は年々増加する傾向にあり、自動車に対するサイバーセキュリティの重要性が上昇

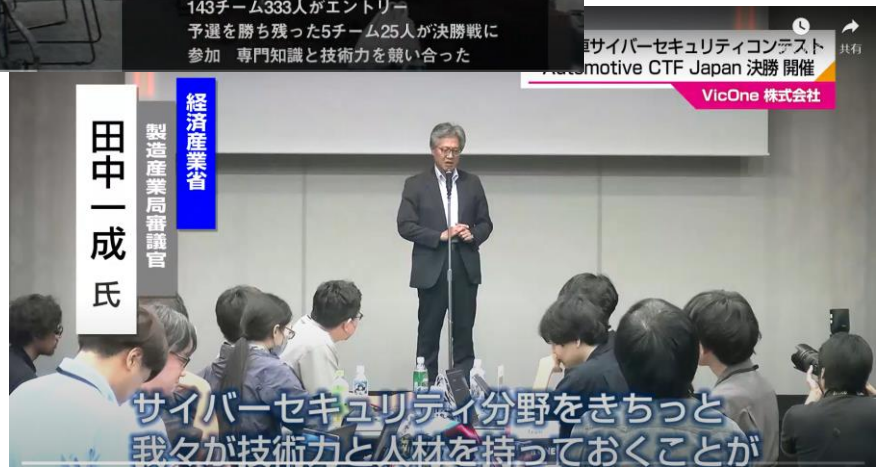


出典：自動車システムの公開脆弱性数（VicOneとNVDのデータベースより集計）

自動車向けセキュリティコンテスト

VicOneでは、自動車に特化した脆弱性発見コンテストを計画、実施しています。
これら活動で得られた知見を製品技術に活かしています

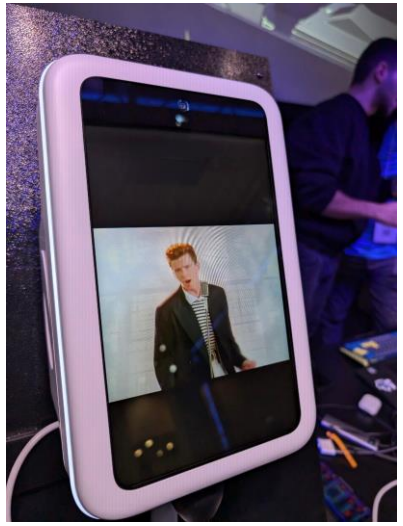
Automotive CTF（2024年7～10月）

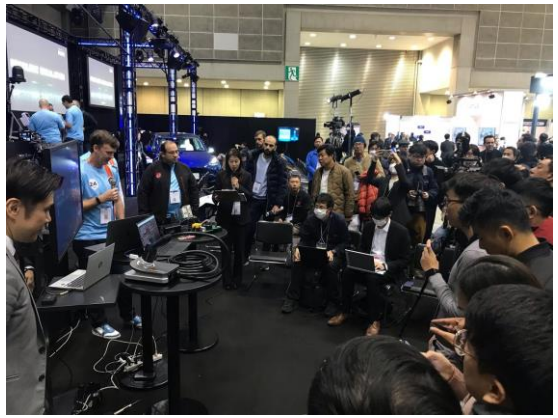


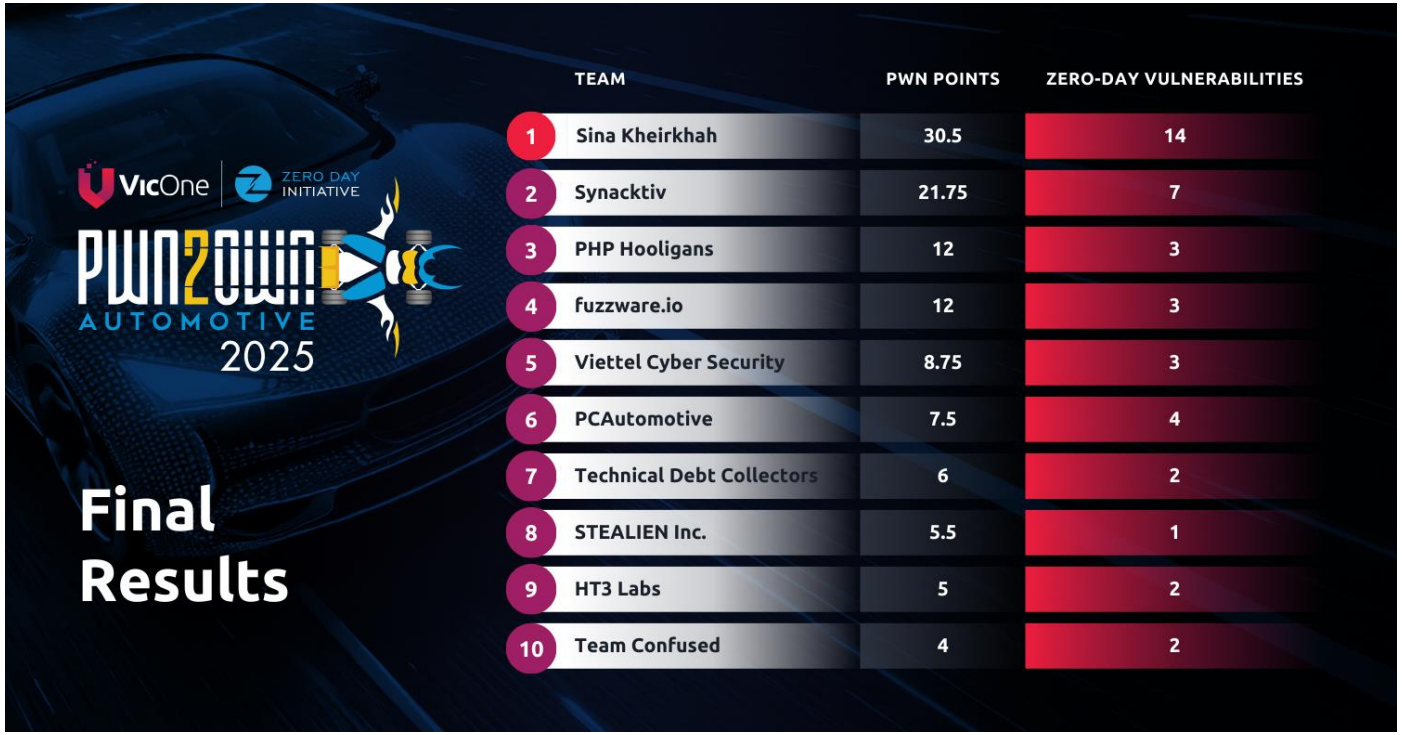
Pwn2Own Automotive（2025年1月）

Pwn2Own 2025実施結果概要

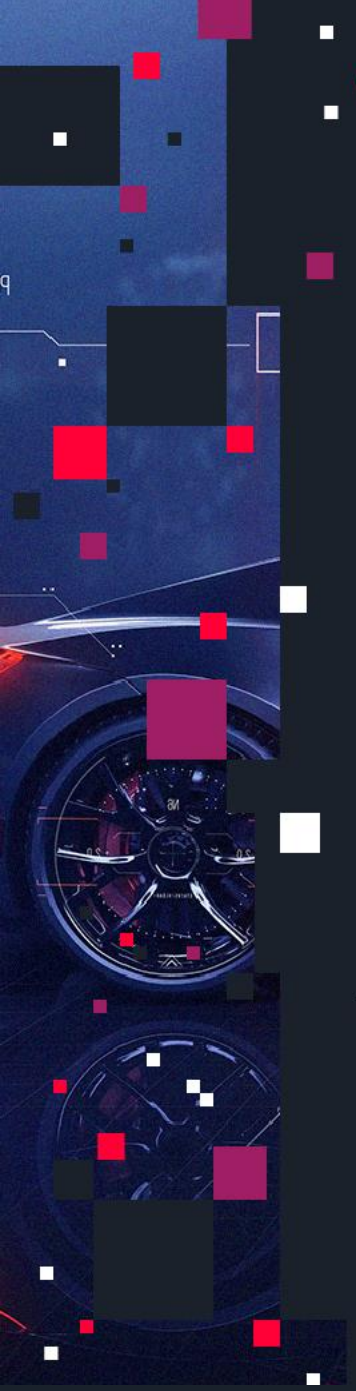
Pwn2Own 2025では、3日間を通して発見されたゼロデイ脆弱性は49件、賞金総額は$1,000,000を超えた





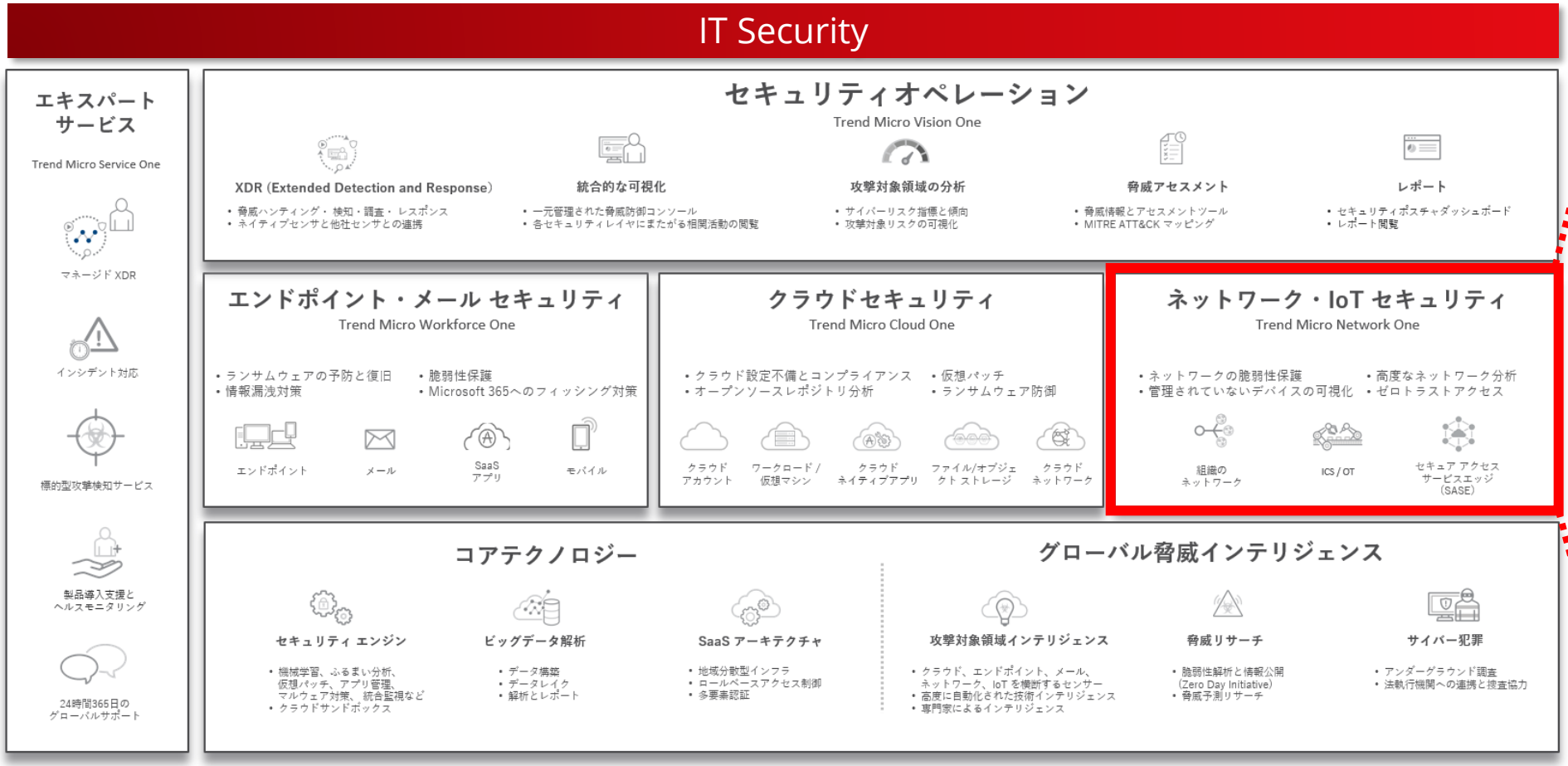


	TEAM	PWN POINTS	ZERO-DAY VULNERABILITIES
1	Sina Kheirkhah	30.5	14
2	Synacktiv	21.75	7
3	PHP Hooligans	12	3
4	fuzzware.io	12	3
5	Viettel Cyber Security	8.75	3
6	PCAutomotive	7.5	4
7	Technical Debt Collectors	6	2
8	STEALIEN Inc.	5.5	1
9	HT3 Labs	5	2
10	Team Confused	4	2



2. 会社紹介

Trend Microの戦略子会社VicOne



Smart Factory Security

txOne networks

Connected Car Security

VicOne
Driving Automotive Cybersecurity Forward

5G network Security

CTONE

日本組織体制

CEO
Max Cheng

日本地域代表
Vice President　小田　章展

ビジネス開発部
Vice President　小田 章展

- セールスグループ
- ビジネス開発グループ
- マーケティンググループ
- アシスタント

エンジニアリング部　執行役員
Sr. Director　原 聖樹

- SEグループ
- セキュリティリサーチグループ
- R&Dグループ

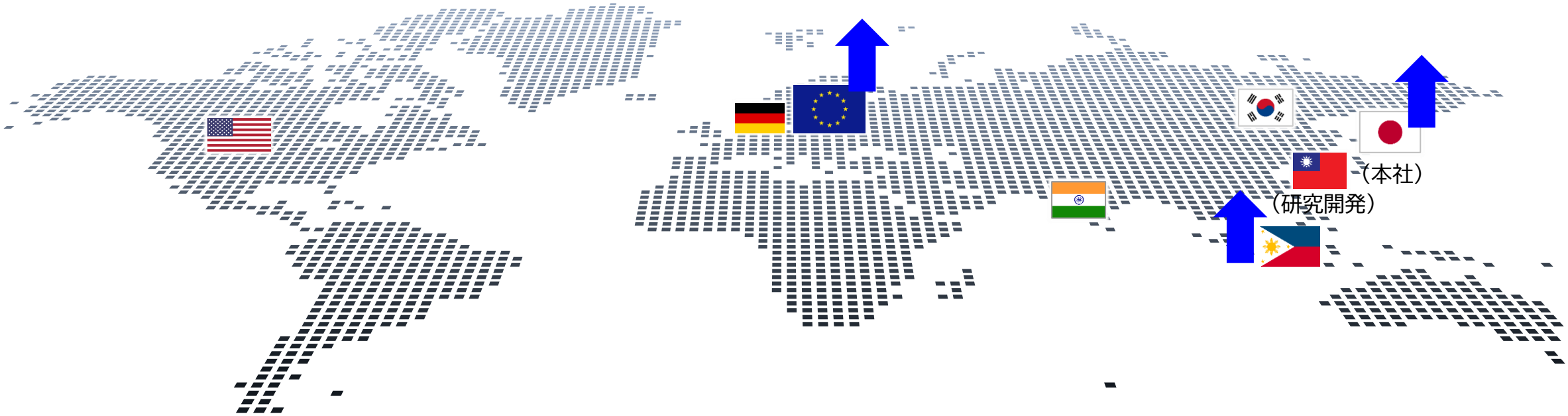
Global PM

- リージョナルPM

HR

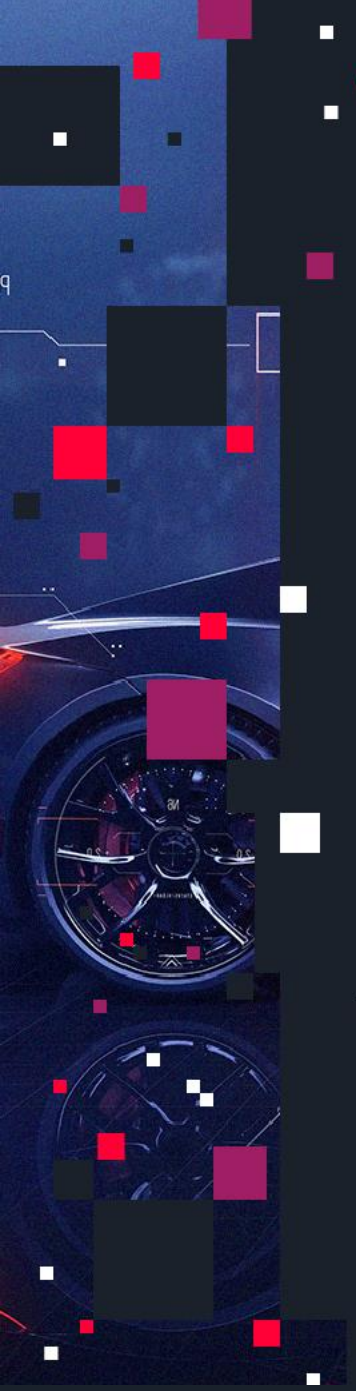
Finance

Globalビジネス状況



＜取組中案件及び事例＞

- VSOC（xNexus）
  - 乗用車、商用車、自動運転ベンダー、EV Charger
- 車載IDS/IPS（xCarbon）
  - 乗用車、商用車、Tier1
- SBOM生成・脆弱性管理（xZETA）
  - 乗用車、建機・農機、Tier1
- ペネトレーションテスト（xScope）
  - 乗用車、Tier1
- リサーチ・コンサルティング
  - 乗用車、商用車、保険、団体
- 教育・トレーニング
  - 乗用車、商社、保険



3. VicOneのソリューション

脅威・脆弱性の調査・発見から対策まで実施している企業

■ 一般的な脅威・脆弱性対応の流れ

弊社強み

ZDI*、Threat Researcherを中心とした
世界No.1の脆弱性の調査・発見・分析活動

ZERO DAY INITIATIVE　TREND MICRO research　VicOne

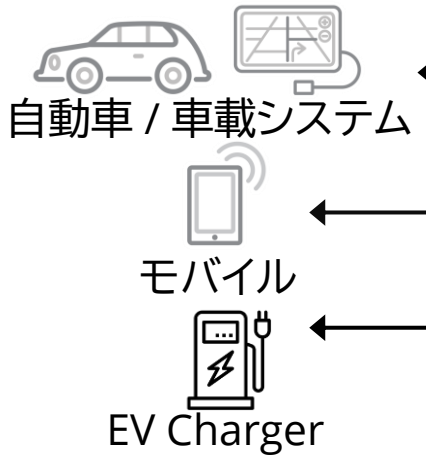
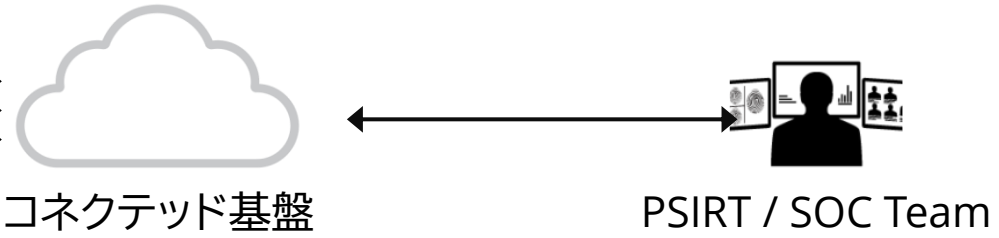
Cloud、PC、Network、産業機器、車載、IT-SOC、VSOCまで
幅広いセキュリティ対策ソリューション

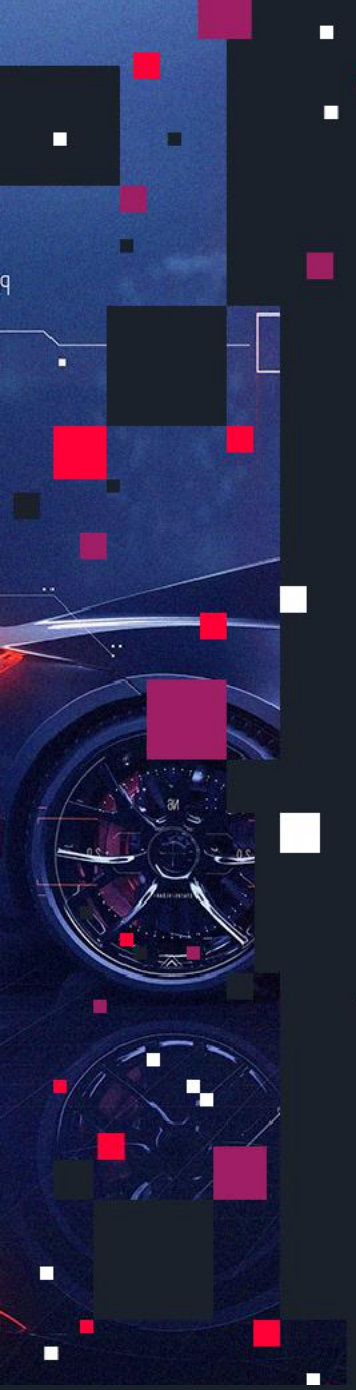
自動車関連脅威・実態等に関する調査

自動車関連脅威研究レポート

9月発行のレポート

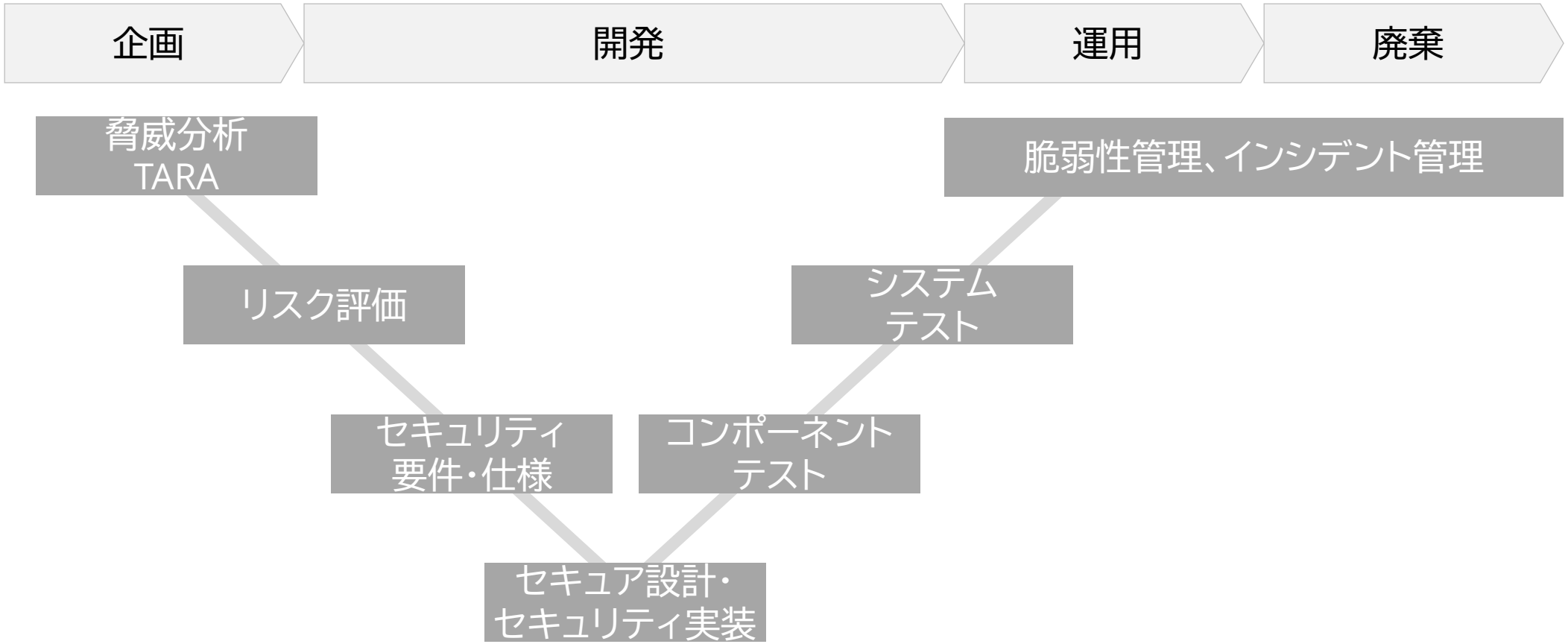
自動車向けセキュリティソリューションマップ

	On Board	Off Board
コネクテッドカーシステム		
VicOne セキュリティソリューション	**xCarbon** 車載器向け組込セキュリティソフトウェア **Smart Cockpit Protection** Android OS向けSecurity Application **xZETA** SBOM生成・脆弱性管理ツール **Security Agent for EV Charger** EV Charger向け組込セキュリティソフトウェア	**xNexus** VSOC（Vehicle Security Operation Center）向け分析・可視化Platform
	xAurient 自動車向け脅威インテリジェンスサービス	
	自動車向けセキュリティサービス ペネトレーションテスト、TARA、教育・トレーニング	



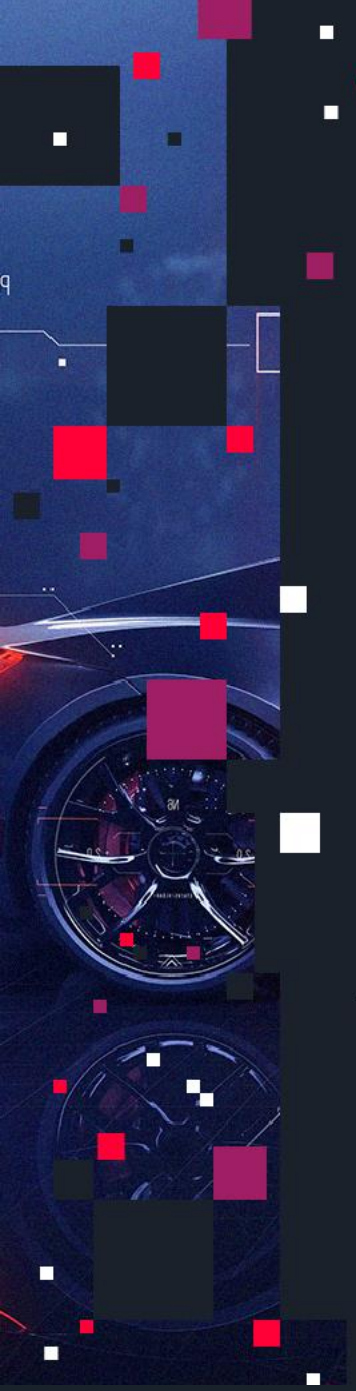
4. SGS社との協業による トータルソリューション

SGS社との協業によるサイバーセキュリティカバレッジ



SGS
TARA支援、コンサル・トレーニング
コンサルティング・運用支援

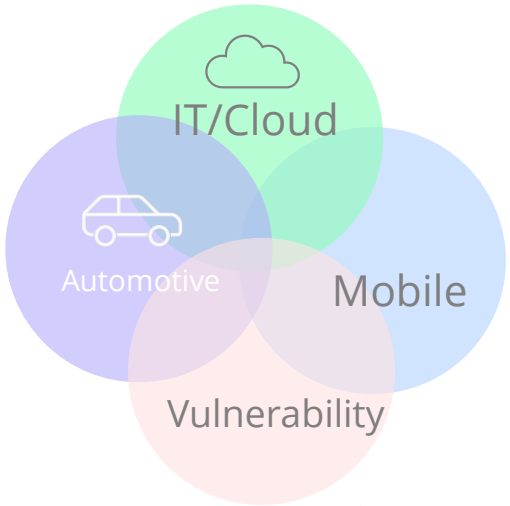
VicOne
TARA支援
車載セキュリティ、テストサービス
VSOC、SBOM・脆弱性管理
Threat Intelligence Service



Threat Intelligence Service 『xAurient』

VicOneの脅威情報のカバレッジ

35+ Year of
Threat Intelligence



TREND MICRO™ VicOne

ZERO DAY INITIATIVE **#1** in Public Vulnerability Disclosure*

*Quantifying the Public Vulnerability Market, Omdia, May 2022

SC awards EUROPE 2023 WINNER

Best Threat Intelligence

VicOne

Best Threat Intelligence

Coverage

- Trend Micro/ZDI/VicOne
- Global Law Enforcement Collab ★
- Zero-day Vulnerabilities ★
- Undisclosed Vulnerabilities ★
- Known Vulnerabilities
- Open-source Intelligence
- Deep Web Crawling
- Dark Web Crawling ★
- Anti-cybercrime Groups ★
- Automotive Security Community
- Social Networks

VicOneの脅威インテリジェンスサービスのコンセプト

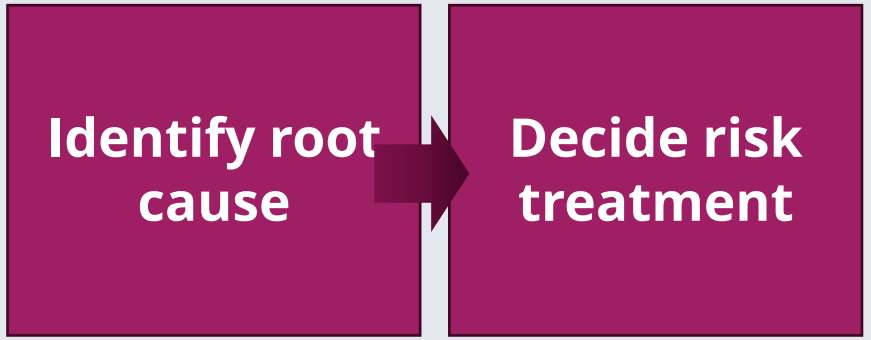
VicOne

Automotive Threat Intelligence

THREAT INTELLIGENCE

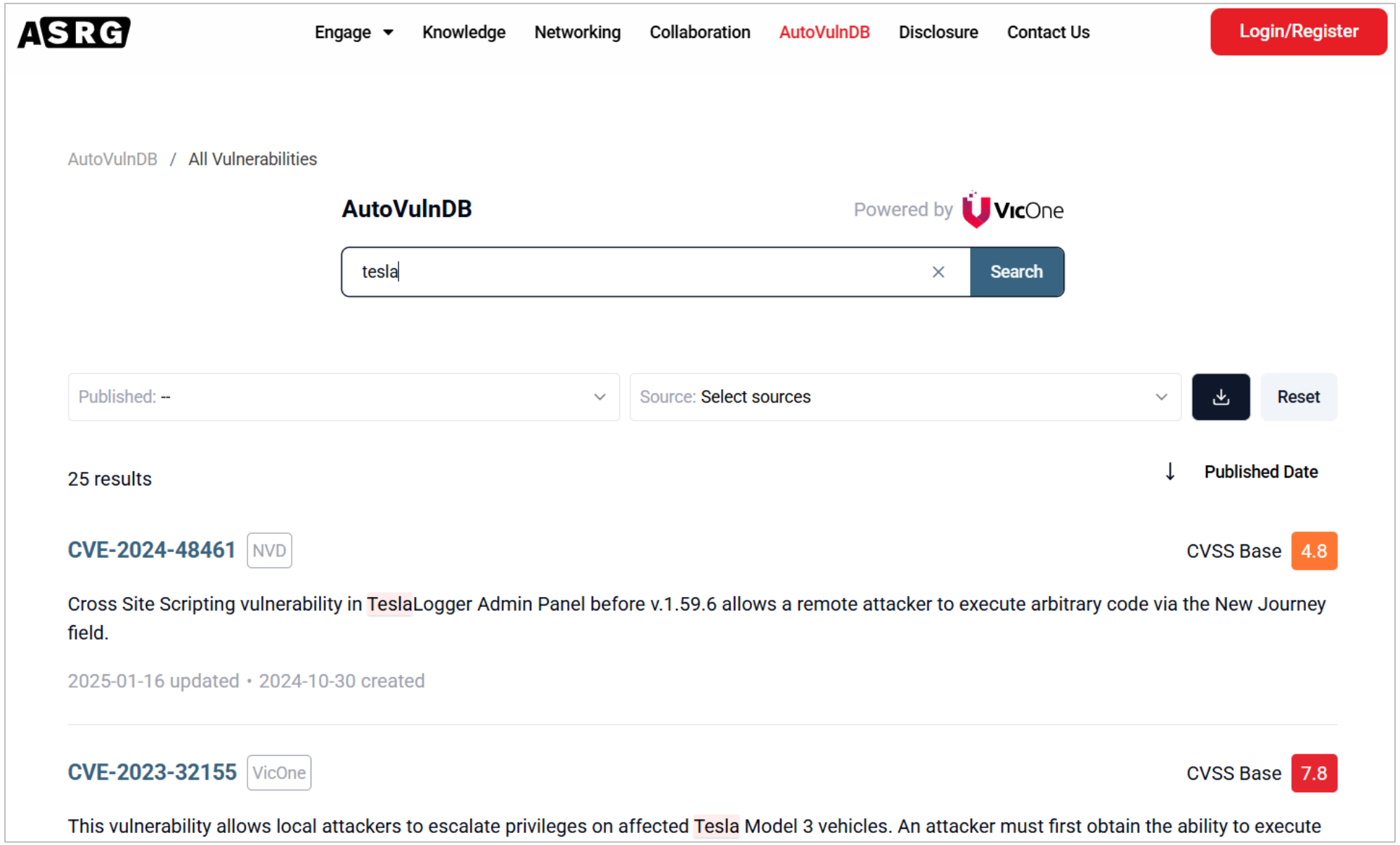
UNR155: CSMS--Continuous monitoring | ISO/SAE 21434: 8.3 Cybersecurity monitoring

ユーザーの対応事項



- UNR155: CSMS--Risk Assessment, Risk Mitigation
- ISO/SAE 21434: Clause 15--Threat analysis and risk assessment methods

参考）ASRG様向けAutoVulnDBの構築支援・提供

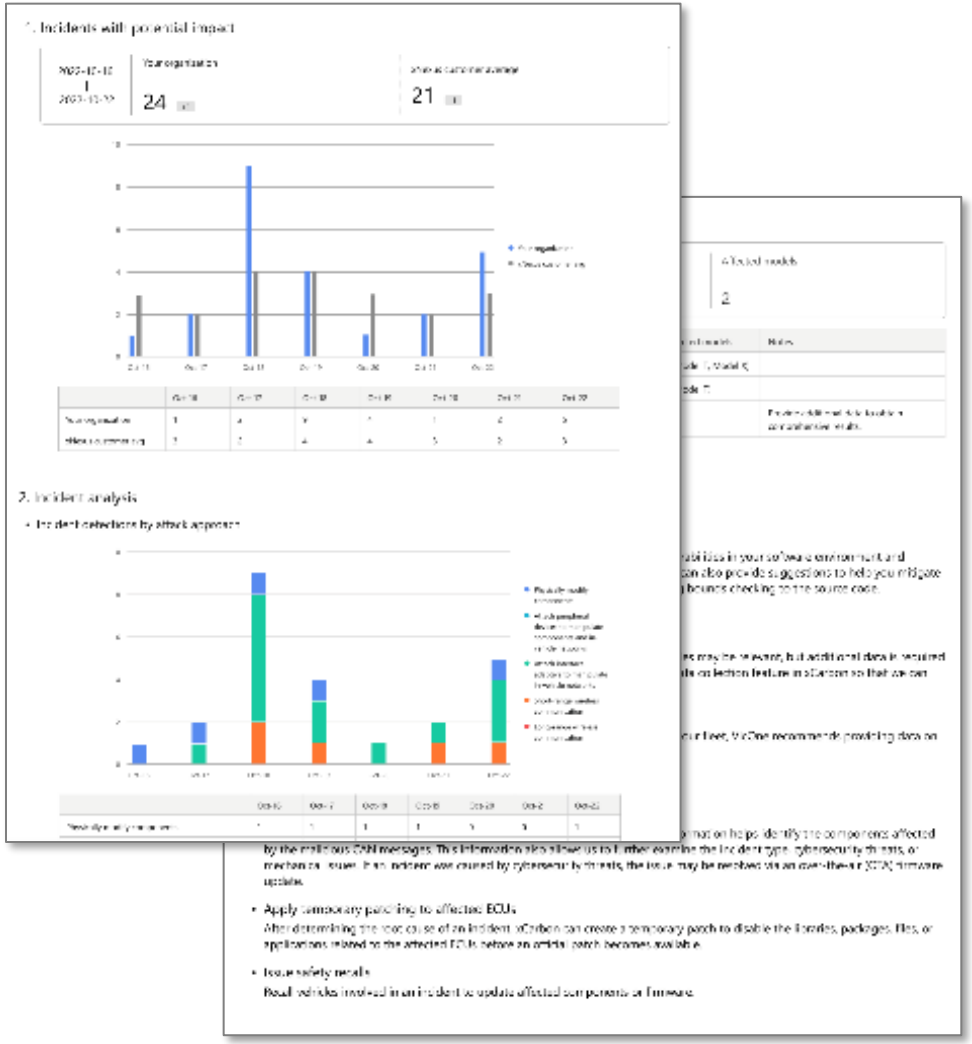


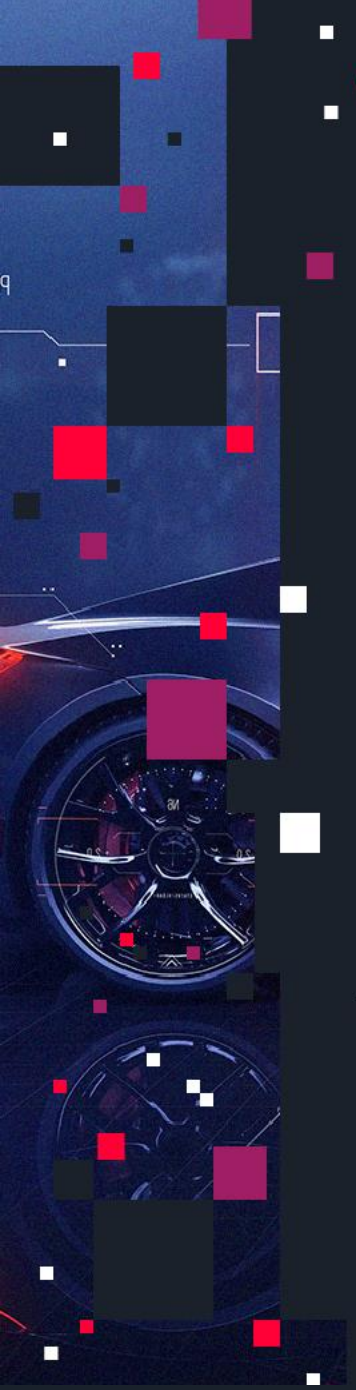
参考）OEM様向けカスタム脅威レポート提供例

OEM様
Security Team

OEM様ご要求事項

- 調査･分析対象範囲
- OEM様関心事項
- OEM様環境に
  合わせた分析
- 弊社視点の脅威分析
- 頻度





SBOM生成・脆弱性管理ツール『xZETA』

北米での中国・ロシアに関する規制強化　概要

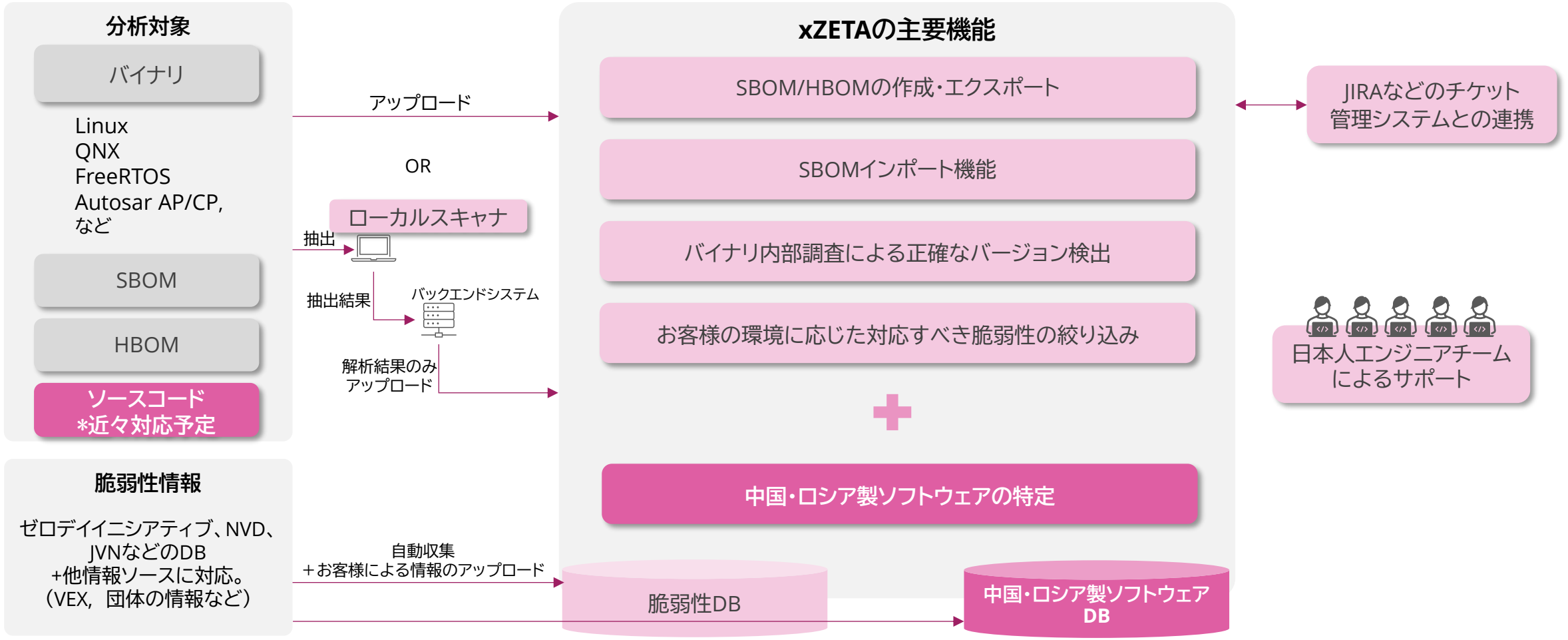
北米では、コネクテッドカーが中国やロシアのサプライヤーと繋がる脅威を排除する規制が施工され、北米でのビジネスのためには、2027年から規制対応が必要

背景・目的	コネクテッドカーが中国・ロシアと繋がる可能性及びそれによる脅威を排除するため、 これら国のサプライヤーによるソフトウェア及びハードウェアの使用が禁止されることとなった
対象車	10,001ポンド（約4,500kg）以下のコネクテッドカー ※商用車は追って規制化される予定。建機、農機、鉄道等は対象外
対象システム	以下に関わる全てのソフトウェア及びハードウェア • 車両通信システム（VCS：Vehicle Connectivity System） • 自動運転システム（ADS：Automated Driving System）
規制有効化時期	• ソフトウェア：2027年～ • ハードウェア：2030年～　※モデルイヤーのない車種は2029年～

自動車メーカーが北米向けビジネス継続のためには、
BOM（SBOM、HBOM）の管理と中国・ロシアサプライヤーのケアが必要

VicOneのSBOM・脆弱性管理ツール『xZETA』

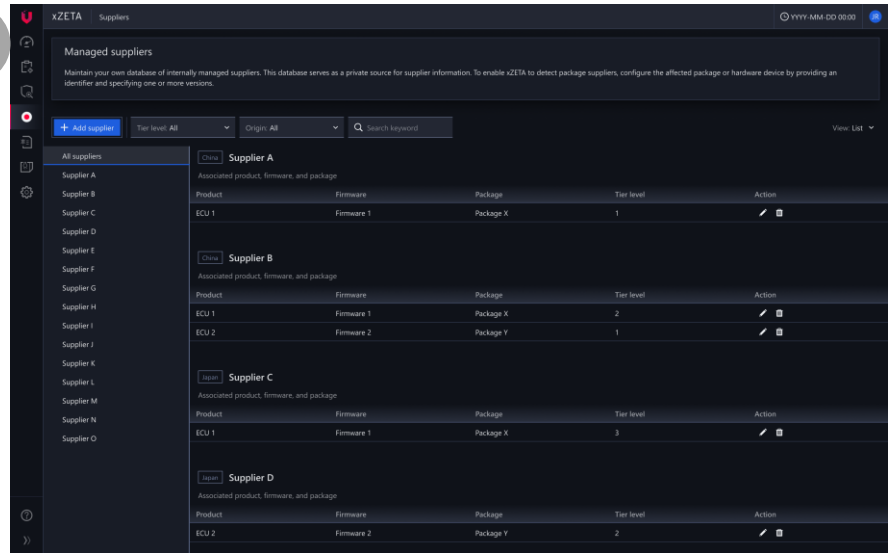
自動車業界に特化したSBOM・脆弱性管理ツールとして、業界特有のニーズを素早く取り込み、新たな機能を日々アップデートしています。



『xZETA』で検討中のサプライヤー管理機能　※イメージ

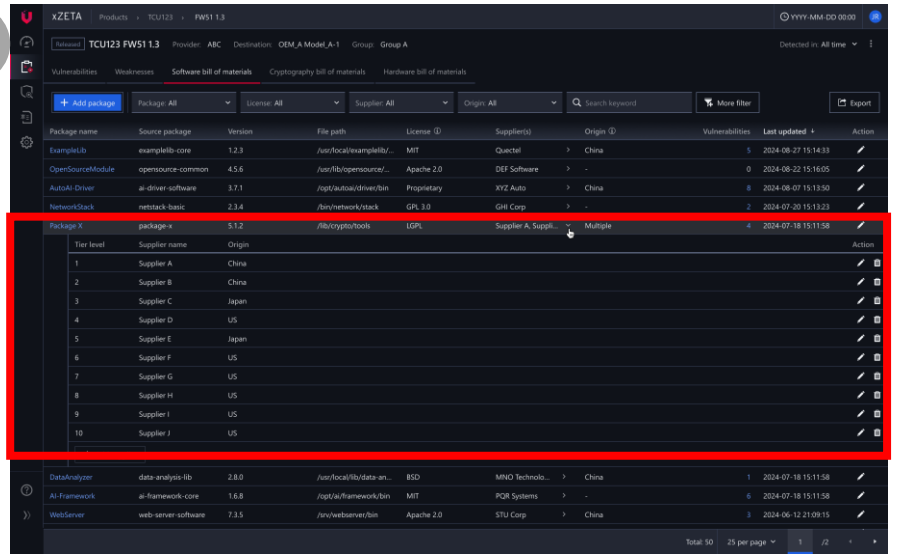
サプライヤーマスター登録

1



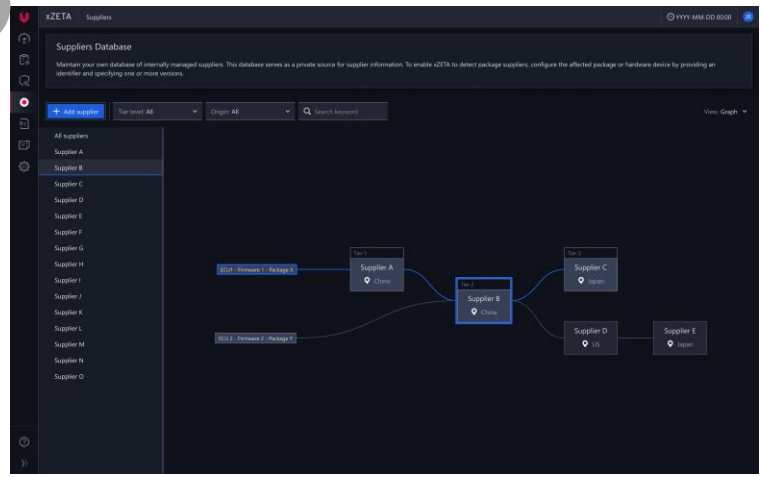
サプライヤー階層管理

2

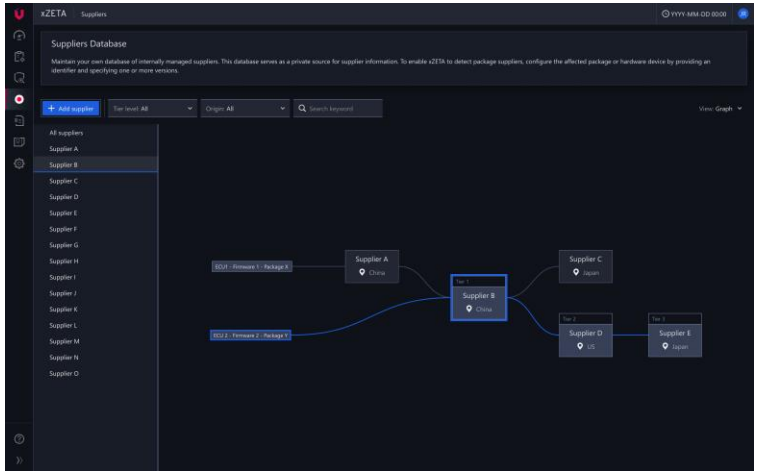


3

例1）ECU①－A社－B社－C社

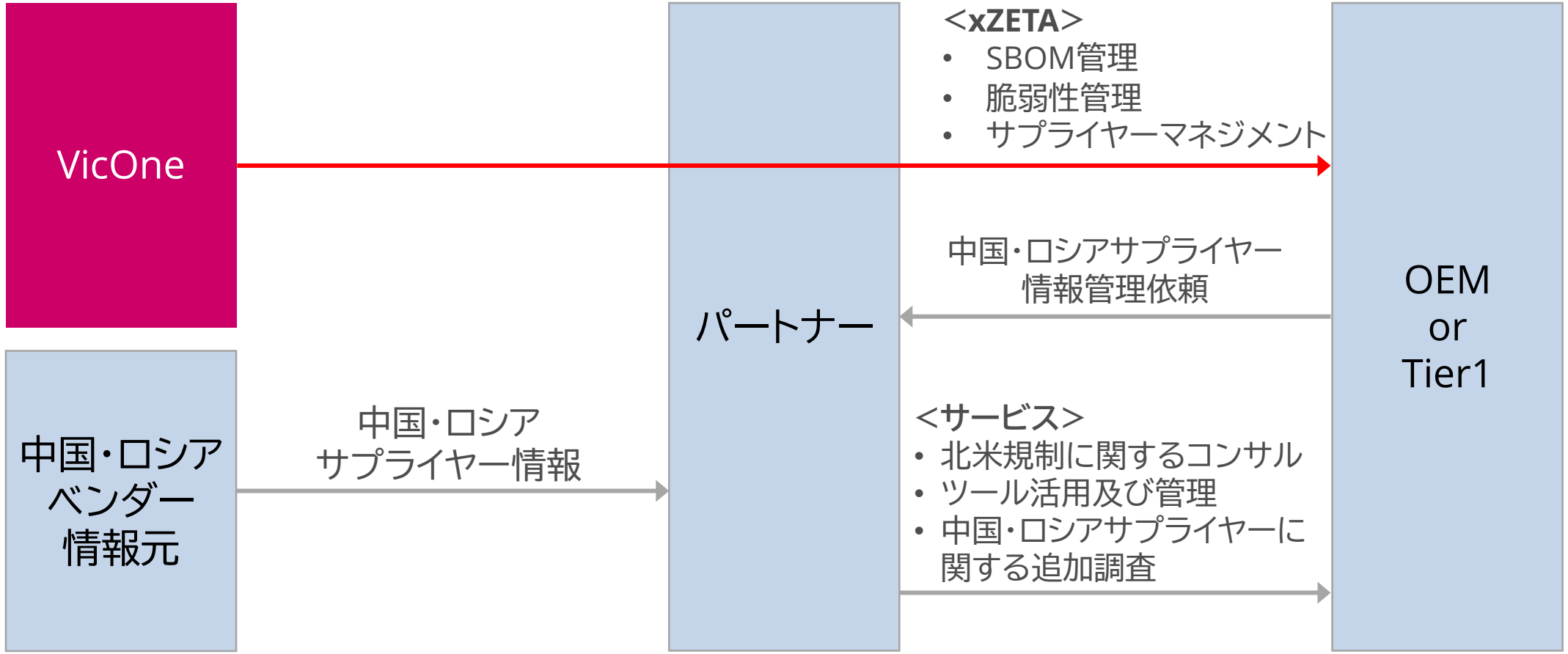


例2）ECU②－B社－C社



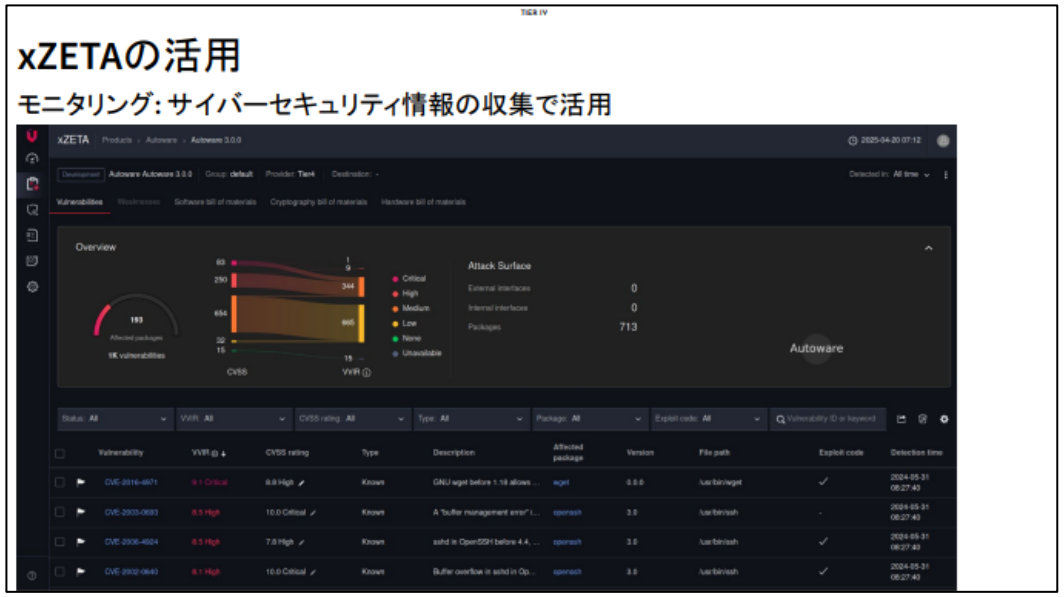
サプライヤー管理に関する提供ビジネススキーム・体制

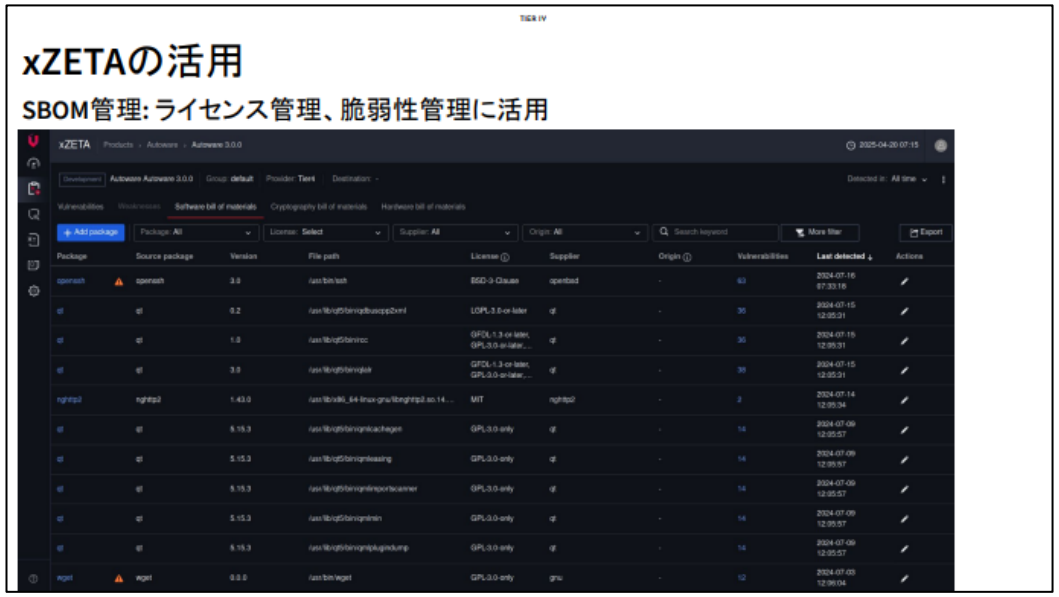
弊社パートナー企業と協力し、以下のような体制でご支援することが可能です。
支援内容詳細については、お客様のご要望に合わせて調整致します。

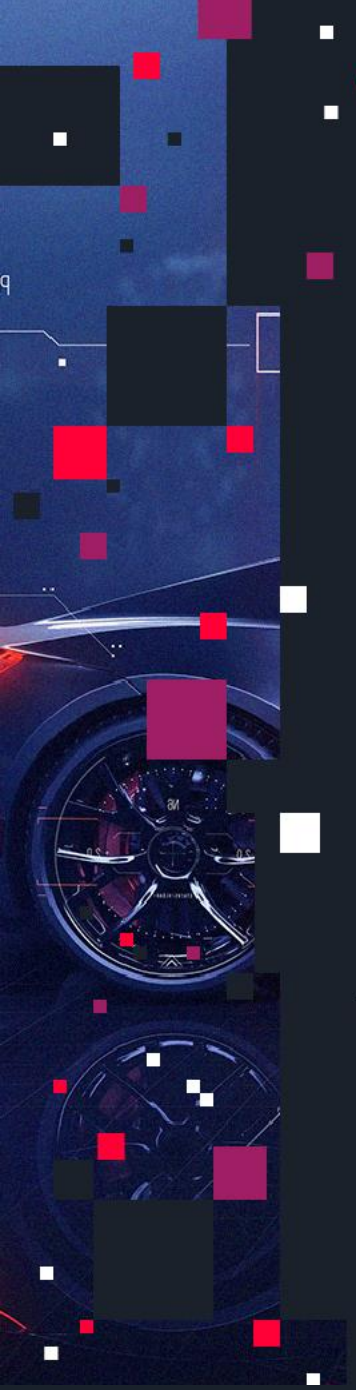


参考）xZETAに関するお客様事例『TierIV様』

自動運転ソフトウェア企業のTierIV様はOSS等の管理や脆弱性対応のため、xZETAを活用中







ペネトレーションテストサービス『xScope』

これまでのペネトレーションテスト実施実績

トレンドマイクロを含め過去15年間で100以上のお客様にペネトレーションテストを提供。自動車関連企業様を含め、様々な企業様、技術領域をご支援しています。

実施経験分野・企業カテゴリー

- 自動車
- 航空
- コンピュータ
- 重電
- 家電
- 半導体
- 電力
- 石油/ガス
- 鉄/金属
- 通信/モバイル
- ヘルスケア
- 流通
- 運輸/輸送
- 銀行/金融
- 保険
- メディア
- 教育
- 政府/公共
- NGO
- 軍/防衛
- その他

実施技術領域

■Automotive
- IVI
- ECU
- OTA
- Secure Boot

■Enterprise
- Web
- Server

■Cloud
- AWS
- Azure
- GCP

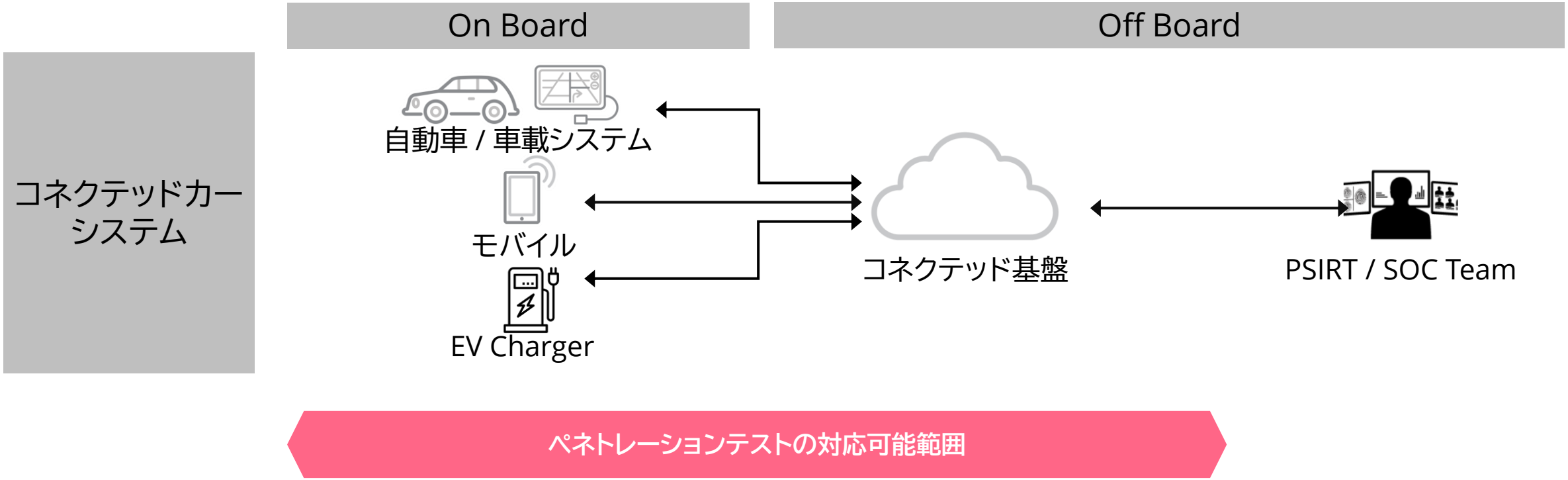
■Mobile Application
- Android App
- iOS App

■IoT/Network
- Network H/W
  - Router
  - Camera
  - NAS
- 他Smart Device

ペネトレーションテストの進め方・アプローチ概要

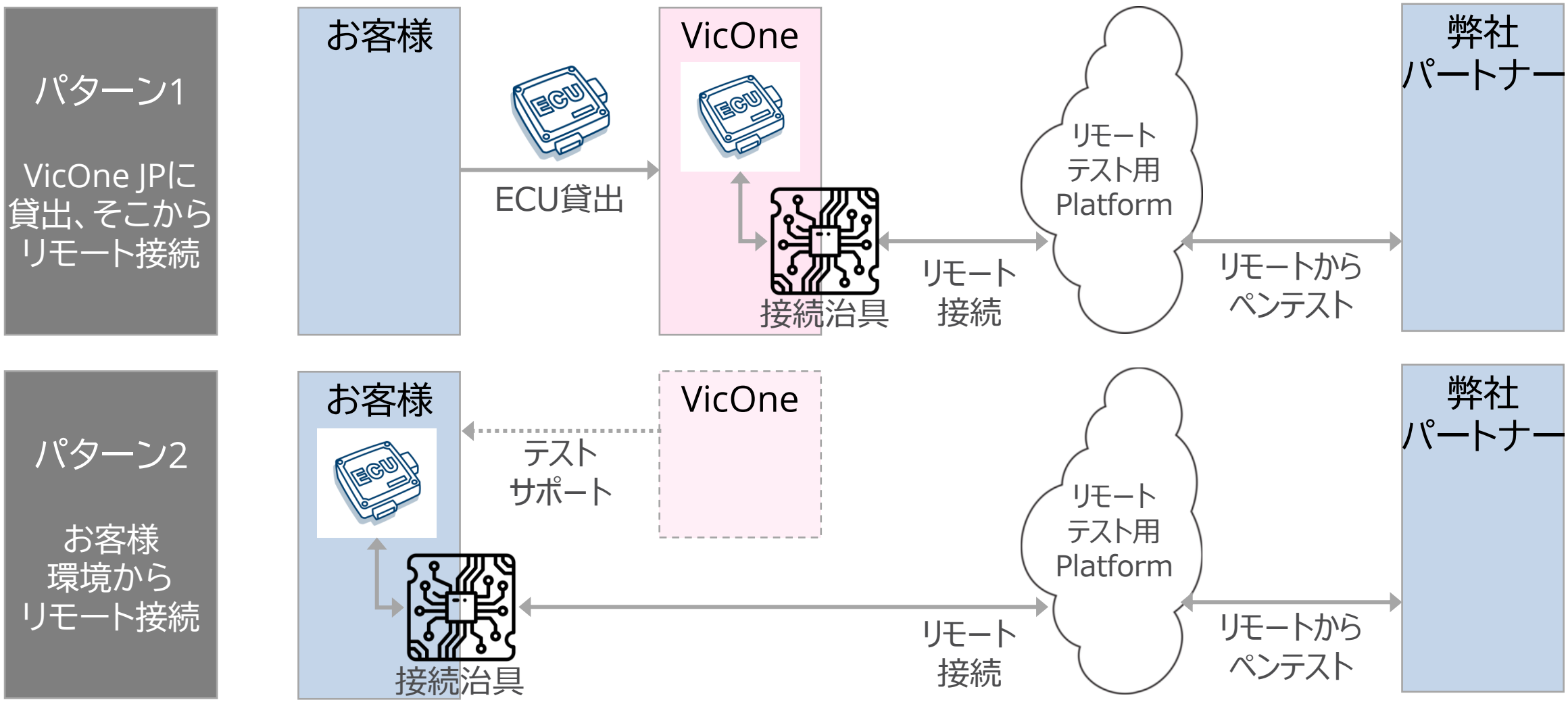
事前調整	作業準備	ペネトレーション テスト	レポート	サポート
•貴社担当者様と 事前確認・調整 •テスト種類 •対象数 •日程 •制限事項 等	•環境準備・整備 •ツール準備 •疎通確認	•ペネトレーション テスト実施 •開発担当者様との トラブル シューティング対応 （アクセス不可、画面遷移方法が不明等）	•実施結果に関する レポート提出	•結果に対する フォロー/サポート •対策実施に関する ご支援

ペネトレーションテストの対応可能範囲



テストプラットフォームを活用した車載機器向けテスト

リモートテスト用の『接続治具』及び『リモートテスト用Platform』を用いることで、
リモートからECU等の実機に対するペネトレーションテストのご提供が可能です。



テストプラットフォーム活用のメリット / デメリット

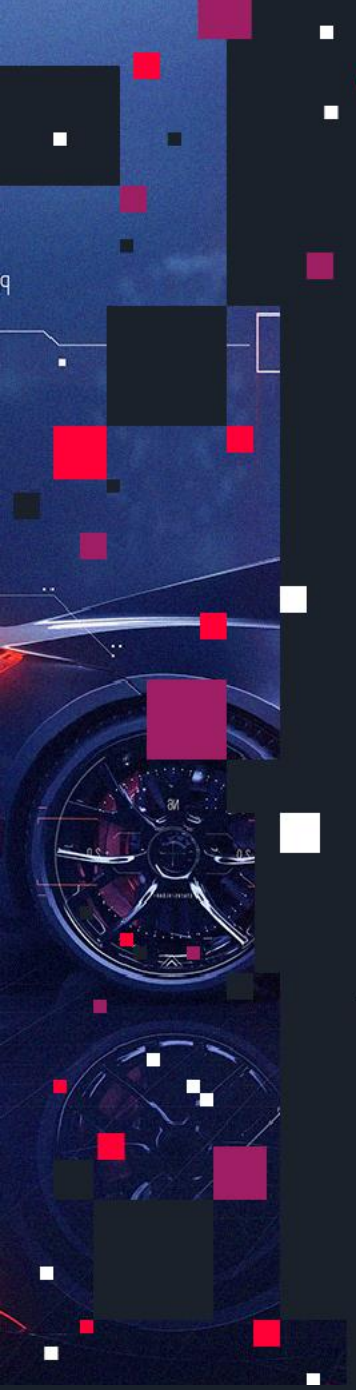
テストプラットフォームを活用することで、一部テストにおける制限は生じるものの、
コスト削減やリードタイム短縮等の多くのメリットを得ることができます

メリット例

- テストの半自動化
  （自動テスト、自動レポート出力等）
- テスト工数・期間の削減
- コスト削減
- 以降、運用が簡単
  ※場合によっては自社で運用が可能

デメリット例

- 実機に対するフォルトインジェクションなど、一部の
  試験は困難、または不可
- テスト環境準備は初期に必要



5. まとめ

まとめ

- SDVやAIなど自動車に関する技術進化に伴い、セキュリティに必要性が高まっていると共に、必要なセキュリティの技術やスコープも変わってきている

- VicOneでは、自動車向けのサイバーセキュリティソリューションやサービスを提供しており、SGS社が提供する分析、コンサルティング、トレーニング等のサービスと補完し合うことで、お客様のセキュリティ活動をトータルで支援が可能

- VicOneではソリューション、サービスを随時拡大中
  - xAurient ・・・ 新サービス。お客様に適したThreat Intelligence Serviceを提供
  - xZETA ・・・ SBOM機能を強化。US規制にも対応。ソースコードスキャンにも対応予定
  - xScope ・・・ 車載器向けペネトレーションテスト等、対応可能範囲を拡大中

Thank You

VicOne

Driving Automotive Cybersecurity Forward

