VicOne

xNexus

精度の高い検出と攻撃分析 —
VicOneの次世代VSOCプラットフォーム

旧来の VSOC プラットフォームによる セキュリティ監視の課題と理由

多くのOEMが導入の容易さからクラウドベースのVSOC
（車両セキュリティオペレーションセンター）プラットフォームを選択しています
しかし、攻撃対象がクラウドから車載コンポーネントやインフラに拡大した現在、
従来型のVSOCプラットフォームではセキュリティ監視に死角が生じる可能性があります

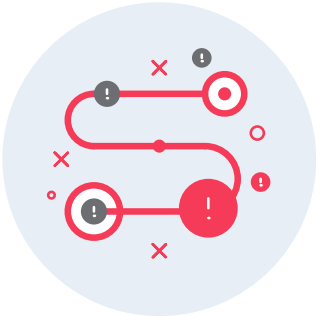
多量のノイズ情報

今日のVSOCプラットフォームに用いられるAIによる検知は、あらゆる“不審な異常”を検出しますが、これはしばしばオペレーターの「アラート疲れ」を引き起こします
IT SOCチームの55%がこれら大量のアラートに対応できていないと回答*しており、同様のケースは自動車業界でも起こり得るでしょう

*トレンドマイクロ社調べ

迅速な対応が困難

一般的な設計のログ収集機能しか持たないVSOCプラットフォームでは、しばしば収集したログに攻撃発生源を含む対策を講じるための実用的な分析結果が含まれず、さらなる手作業での調査が必要となるケースが発生します
この結果、検出したリスクへの対処が遅れる可能性があります

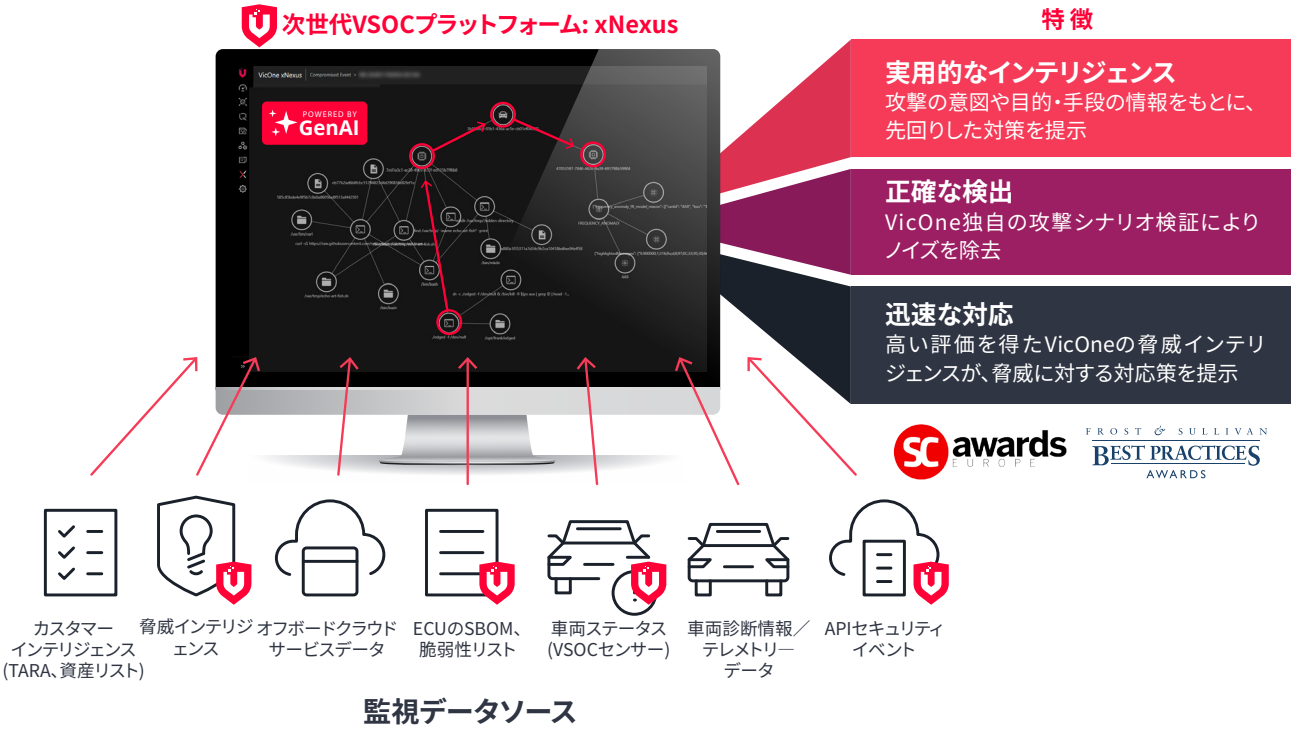


原因追跡が困難

今日のVSOCプラットフォームは、検出したインシデントを細分化して、攻撃の戦術とテクニックを特定することに苦慮しています
攻撃側の目的と手段の理解を欠いた状態では、サイバー攻撃の復旧と再発防止は困難なものになります

サイバー攻撃を可視化し、分析を可能にする VicOneの次世代VSOCプラットフォーム

xNexusは監視データソースから情報を統合化して分析し、サイバー攻撃の発生源や目的、手口等を明らかにします



xNexusの特長

- **データの正規化**
  お客様データレイク内の各種データをVSOCで統合可能なフォーマットに正確に正規化し早期のデータ統合を実現します
- **シームレスな統合**
  xNexusは、自社のみならず3rdパーティーのIDS/IPS、脆弱性管理システムやSIEMなど、お客様の既存環境との統合が可能です
- **生成AIを活用した分析**
  エキスパートによる調査と独自の大規模言語モデル(LLM)アプローチによるAI分析を組み合わせ、アラート評価、脅威情報の集約、レポート作成などVSOCチームの日常業務をサポートします
- **柔軟なスケーラビリティ**
  車載システムのエージェント有無に関わらず、モニタリング可能なデータに応じてシステムを柔軟に構成できるため、高い費用対効果で車両の長期ライフサイクルに対応します
- **SDV化に向けたリスクへの備え**
  xNexusは、API－クラウド－車両－サービスアプリ間の挙動の完全な可視化が可能です
- **必要なデータをピンポイントで**
  お客様が必要とする関連データを的確に特定することで、不必要なデータ要求や時間のかかるやり取りを省きます

xNexusSolutionBrief_2024.08.23
Copyright © 2024 VicOne Corp.
All Rights Reserved.

詳しくは VicOne ウェブサイトをご覧ください
(VicOne.com/jp もしくは右の QR コードよりアクセス)