VicOne

xNexus

洗練された検出と攻撃分析-VicOneの次世代VSOCプラットフォーム

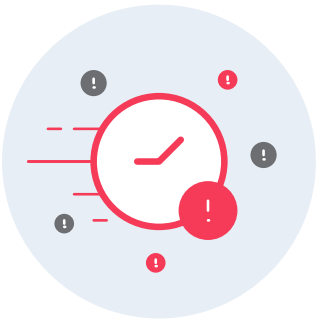
旧来のVSOCプラットフォームによるセキュリティ監視の課題とその理由

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。

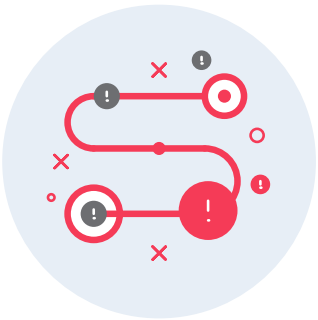
多量のノイズ情報

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いますが*、同様のケースは自動車業界でも起こり得るでしょう。



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インテリジェンスが含まれず、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。



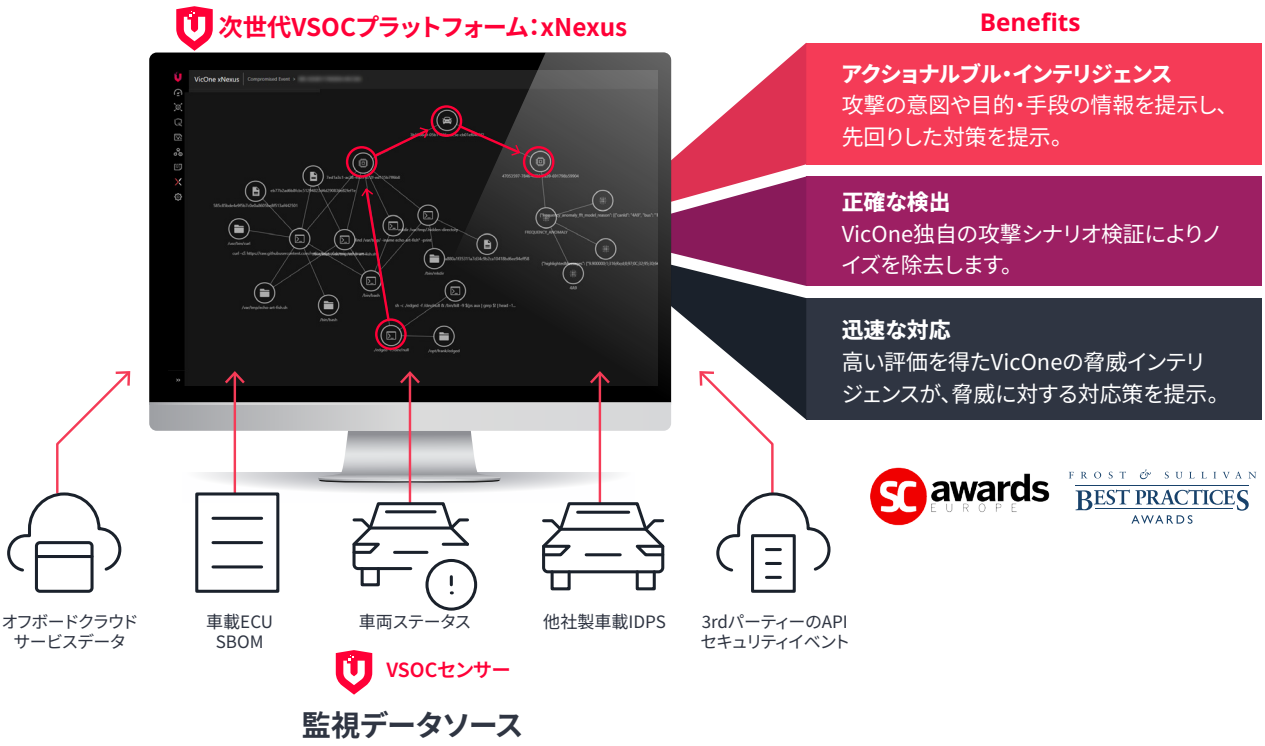
原因追跡が困難

今日のVSOCプラットフォームは検出したインシデントをブレイクダウンして、攻撃の戦術とテクニックを特定することに苦心しています。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。

*トレンドマイクロ社調べ

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

xNexusは統合された車載VSOCセンサーから情報を分析し、サイバー攻撃の発生源や目的、手口等を明らかにします。



SC awards EUROPE　FROST & SULLIVAN BEST PRACTICES AWARDS

xNexusの特長

- **データ正規化**
  VicOneは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、早期実現をいたします。
- **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。
- **APIセキュリティリスクの可視化**
  従来のVSOCシステムが対象にしているクラウド関連のAPIのみならず、車両および車両を含むエコシステム全体のAPI関連のサイバーリスクを可視化します。
- **リスクの検出と管理**
  xNexusはネットワークリスク、異常な挙動や状態、既知およびゼロデイ脆弱性およびサイバー攻撃痕跡を検出します。
- **SDV化に向けたリスクへの備え**
  xNexusは、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。

xNexus

詳しくはVicOneウェブサイトをご覧ください。(VicOne.com/jp もしくは右記QRコードをスキャンしてアクセス)