

TREND VISION ONE™

Security Operations (SecOps)

XDR、Agentic SIEM、SOARによるプロアクティブな検出、調査、対応で、攻撃者が潜む余地を排除

脅威と戦うセキュリティオペレーションセンター (SOC) に勝利をもたらす

セキュリティ管理部門は他の社員が気付かない脅威から組織を保護するという重責を担っていますが、人員が少なく、予算が限られ、分断化されたツールを使用している場合がほとんどです。多くの人員が疲弊し、他の担当部門との連携は協調よりも摩擦を生みがちです。その一方で、データ侵害の脅威は拡大しています。Ponemon InstituteとIBMが発表した「Cost of a Data Breach Report 2024」によれば、**2023年に発生したデータ漏洩事件の平均被害額は445万ドルに達し**、史上最高を記録しました。対応が遅い、分断化された、リアクティブなセキュリティを放置し続ける余裕はありません。従来型のセキュリティ情報イベント管理 (SIEM) システムは運用コストが高く、拡張が困難で、手作業での調整と調査に過度に依存しています。対応を迅速化するどころか、複雑さとノイズ情報によって担当部門を疲弊させています。

SOC 担当部門に必要なのは可視化だけではありません。明確性、優先順位付け、迅速かつ協調的なアクションも必要です。Trend Vision One™ Security Operations (SecOps) ソリューションは、トレンドマイクロの受賞歴のある XDR、Agentic SIEM、Agentic SOAR (セキュリティのオーケストレーション、自動化、および対応) を統合し、担当部門が最も重要な課題に集中して取り組めるよう支援します。脅威が急速に進化する中、SOC 担当部門もそれ以上に迅速に行動し対応する必要があります。

プロアクティブな機能によって従来のリアクティブなセキュリティを凌駕する

将来を見据えた設計

SecOpsは、迅速なセットアップとシームレスな統合を実現します。最新のテクノロジーを活用して高度なセキュリティ機能を低コストで提供します。導入当初から長期的な拡張性と効率性を確保します。

大規模言語モデル (LLM) の利点

スキーマを言語のように扱い、AIを使用してデータの背景にある意図を把握することで、手動ルールの必要性を削減します。

“

Trend Vision One™プラットフォームは、全ての情報を一箇所に取り込む機会を与えてくれました。また当社のサイバーセキュリティ担当部門が、異なるIT組織間の調整なしで、組織全体の攻撃やイベントに対処できるようになりました。

Samer Mansour氏
バイスプレジデント、CISO
Panasonic Corporation
North America 社



比類のないXDR基盤

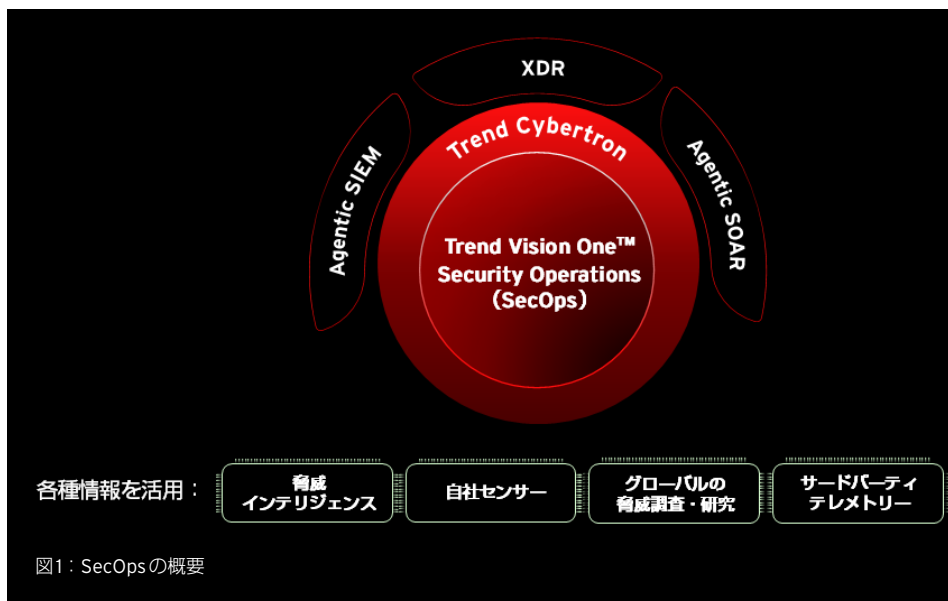
SecOpsはトレンドマイクロの先進的な自社センサーを搭載し、すべてのセキュリティレイヤを網羅する総合的な可視化を実現します。従来型SIEMでは見逃されがちな重要な検出ギャップを埋め、より強固な保護と盲点の排除を実現します。

脅威ハンティングの労力を削減

AIを活用したサイバーセキュリティアドバイザーである Trend Companion™ が、アナリストの調査を支援します。AIによる洞察を提供し、日常的なタスクを自動化し、手間のかかる作業を削減します。これにより、SOC担当部門は優先度の高い脅威に集中できるようになり、対応時間を短縮し、全体的な効率を高めることができます。

データを理解し、目的思考で動作

ログを処理するだけでなく人間の言語で考える Agentic (自律型) SIEM



サードパーティデータのシームレスな取り込み

分析データ（検出およびハンティング用）とアーカイブデータ（コンプライアンスおよび長期保存用）の両方を簡単に取り込むことができます。あらゆる種類のログを大規模かつリアルタイムで取り込むことで、変化し続ける環境を常に把握できます。

実用的なデータ可観測性を実現

多様なテレメトリを、言語ベースの相関付け機能と、AIによるノイズを排除する検出機能により、有益な洞察に変換します。データの解析やルールの作成に、手作業は必要ありません。

レポートとコンプライアンスの効率化

ログ保持、監査、規制関連報告をサポートする機能がすべて1つのコンソールに集約されているため、コンプライアンス対応の負担を軽減します。

データ保持の簡素化と拡張

拡張性と柔軟性に優れた戦略によって、業務に支障をきたすことなく重要な情報を保持できるため、コンプライアンスと保持要件に安心して対応できます。



2024 MITRE ATT&CK™ Enterprise Security Evaluationの結果

- 全主要ステップの分析カバレッジ100% (16/16)
- LinuxおよびmacOSの全サブステップの分析カバレッジ100%
- サーバプラットフォーム (Windows/Linux) の全サブステップの分析カバレッジ100%
- 全サブステップの分析カバレッジ99% (79/80)

全レイヤにわたり強力なネイティブ脅威カバレッジを実装

- **EDR (Endpoint Detection and Response)** : エンドポイントを詳細に可視化し、リアルタイムで相関付けることによって、エッジ上で脅威を検出して阻止
- **NDR (Network Detection and Response)** : ネットワーク内の管理外のデバイスや不正なデバイスに潜む脅威を可視化
- **CDR (Cloud Detection and Response)** : フルスタックのクラウド検出機能によって、ワークロード、コンテナ、クラスタを保護
- **ITDR (Identity Threat Detection and Response)** : リスクの高いユーザを特定し、侵害を受けたIDを早期に脅威シグナルに変換
- **EmDR (Email Detection and Response)** : メールを行動分析することで標的型攻撃やアカウント乗っ取りを検知
- **DDR (Data Detection and Response)** : 機密データの移動を追跡し、データ持ち出しの試みを即座に検知

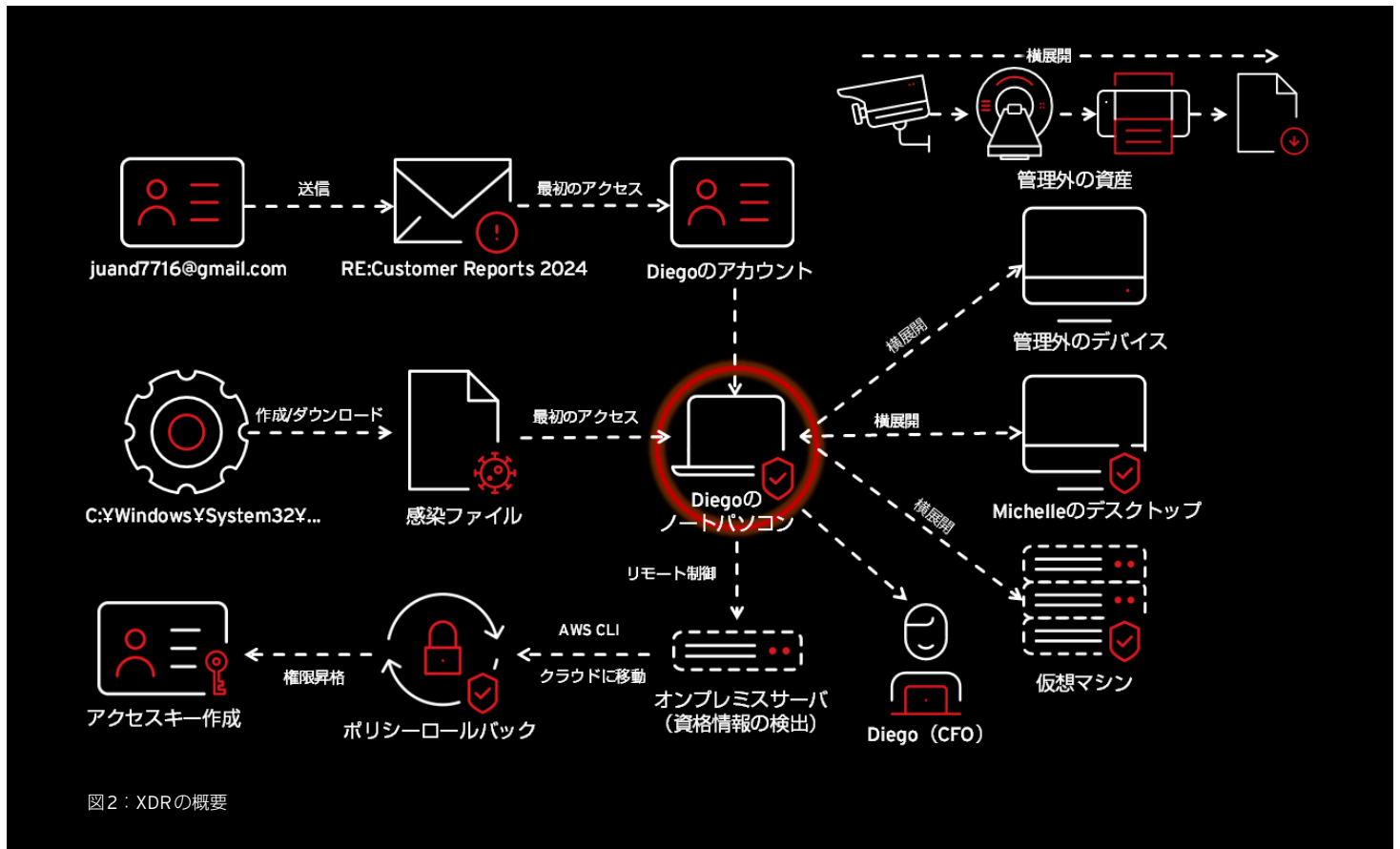


図2: XDRの概要

インシデント対応を再定義する Agentic SOAR

ノイズを減らし、アクションを迅速化。SOCのあらゆる施策から明確な価値を引き出す。

AIを活用した調査

自動優先順位付け機能とAI機能を備えたトレンドマイクロのワークベンチが、インシデントを要約し、次のステップをガイドし、最も重要な点を強調します。これにより、アラートを受けた担当部門は推測に頼ることなくアクションに移行できます。

エンドツーエンドのSOC自動化

トライアージから解決までの反復的なタスクは、AIと柔軟なケース管理機能によって肩代わりされ、最適化されます。SOC担当部門は手作業の無駄を省きながら、影響のある対応に集中して取り組むことができます。

連携するエコシステム

Agentic SOARは、オープンなAPIを使用して既存のワークフローやシステムと統合できるため、カスタマイズ可能なプレイブックやリアルタイムの連携を実現します。

先を見据えたワークフロー

アナリストはAgentic SOARが備える直感的なAI支援ワークフローを活用して、手作業を減らしながら脅威を発見し、その背景情報を迅速に把握できます。



プロアクティブセキュリティ、始動。

Trend Vision Oneは、サイバーリスクの管理（Cyber Risk Exposure Management）、セキュリティ運用（Security Operations）、多層防御を一元化し、脅威の予測と防止をサポートする唯一のAI-Powered エンタープライズサイバーセキュリティプラットフォームです。

トレンドマイクロについて

サイバーセキュリティの世界的なリーダーであるトレンドマイクロは、デジタルインフォメーションを安全に交換できる世界の実現に向けて取り組んでいます。Trend Vision One エンタープライズサイバーセキュリティプラットフォームは、数十年におよぶセキュリティ分野の知見、国際的な脅威研究、そして終わりのないイノベーションに基づき、AIを活用して50万以上の組織と、2億5,000万人以上の個人ユーザを、クラウド、ネットワークデバイス、エンドポイントなどのさまざまな環境で保護しています。

[TrendMicro.com](https://www.trendmicro.com)

Copyright ©2025 Trend Micro Incorporated. All rights reserved. Trend Micro, Trend Micro ロゴ, t ボールロゴ, Trend Vision One, および Trend Companion は、Trend Micro Incorporated の商標または登録商標です。その他の会社名および製品名は、各社の商標または登録商標です。本書に含まれる内容は予告なしに変更される場合があります。Trend Micro, Trend Micro ロゴ, および t ボールロゴは、米国特許商標庁に登録済みです。
[SB00_Security_Operations_Solution_Brief_250625US]

当社が収集する個人情報とその目的の詳細については、トレンドマイクロのWebサイトでプライバシーポリシーをご覧ください。[trendmicro.com/privacy](https://www.trendmicro.com/privacy)

**30日間の無料体験版を
お試しください**

[TrendMicro.com/trial](https://www.trendmicro.com/trial)