Trellix

WHITE PAPER

Trellix Wise™ for Private Cloud: 自律型SOC（Agentic SOC）の推進 翻訳版

状況の劇的な変化

かつて、XDR、SIEM、SOARのようなソリューションはすべて同じ成果、すなわち組織内のすべてのシグナルを集約して実際の脅威と誤検知を見分け、修復を自動化して被害を制限することによる高速な検知と修復を約束していました。これにより、少人数のSOCチームでも、AIを駆使した攻撃者が生み出す大量のアラートに対応できるはずでした。

コンセプトは妥当でしたが、基盤技術には欠陥がありました。XDRは必要な可視性と統合を完全に実現できず、脅威に悪用される死角を残しました。一方、SIEMやSOARの硬直したプレイブックは手動での調整を必要としました。現在、AIを駆使する敵に直面し、これらツールが解消を約束したボトルネックはさらに悪化しています。

大規模言語モデル（LLM）や生成AIは、攻撃者にとってゲームチェンジャーです。従来のSOCが調査の断片をつなぎ合わせている間に、攻撃者は攻撃チェーン全体を数分で実行できるようになりました。しかし、問題はスピードだけではありません。より巧妙に隠蔽された悪意のあるコードや、決してチェックされないことを狙って低～中程度のアラートの波に隠れる複雑な攻撃経路など、AIは攻撃の高度化と複雑化を著しく進行させました。

同時に、エージェンティックAIはSOCにとってもゲームチェンジャーとなります。XDR、SIEM、SOARでは解決できなかった課題を、スピードと高度な分析力をもって解決するために登場しています。このAI主導の攻撃の現代において、組織をマシンスピードで防御するためのツールと能力を防御側に提供します

。

エージェンティックSOC（自律型SOC）プログラム

エージェンティックSOCプログラムは、戦略、人材、プロセス、ガバナンス、そしてエージェンティックAIを使用して攻撃をハンティング、調査、対応するためのツールと機能の集合体で構成されます。当初、エージェンティックSOCプログラムはより迅速な検知と調査結果の提供に重点を置き、SOCアナリストがデータの相関付けに費やす時間を減らし、問題の分析と対応により多くの時間を割けるようにする可能性が高いです。時間が経つにつれ、AIの推論や結果に対する信頼と自信が高まるにつれて、SOCアナリストとエージェンティックシステムの連携は強固になります。最終的には、確度の高い調査結果に基づくエージェンティックSOCのポリシーとアクションが、より自律的なものとなっていきます。

エージェンティックSOCは単なるエンリッチメント付きのSOARではなく、SOCの組み込まれた運用手順によって制御され、透明で説明可能な方法でアクションを実行するために、調査コンテキストを動的に発見、収集、マッピングする目的に特化したディープエージェントのセットです。エージェントの役割は調査、修復、ハンティングに焦点を当てており、SOCのワークフローやプロセスを24時間体制で実行できます。もちろん、事前承認された自動化はすべて、人間が定義した組織のガードレールによって管理される必要があります。



Figure 1. エージェンティックSOC（自律型SOC）への道のりで問うべき5つの質問

主要な要件

- **マシンスピードでの防御：**AIを駆使した攻撃は、人間主導の運用（オペレーション）の対応スピードを超えて展開（進行）します。エージェンティックSOCは、このギャップをマシンスピードかつ大規模に埋めます。
- **結果に対する信頼と自信：**エージェントの決定や推論は、アナリスト、経営陣、規制当局のいずれに対しても説明可能で、監査可能かつ防御可能でなければなりません。
- **限られた予算でも拡張可能：**予測可能な固定コストモデルに基づくエージェンティックSOCは、既存のチームと予算でより広いカバレッジを提供します。
- **データ主権ルールの遵守：**エージェンティックSOCは、組織の規制およびセキュリティ要件に準拠している必要があります。一部の組織では、パブリッククラウド、共有SaaS、またはパブリックLLMに接続しないエージェンティックSOCを必要とします。

主要な機能

- **自律的なアラート調査：**調査エージェントは、受信したすべてのアラートをセキュリティ、組織、および手順のコンテキストに照らし合わせて自動的に評価、相関付け、トリアージし、低レベルのシグナルを証拠に裏付けられた完全な判定へと結びつけます。

- **ガバナンスに基づく脅威の修復：**修復エージェントは、判定をレスポンスに変換し、段階的な権限（完全自律型、ヒューマンインザループ、または手動のみ）の下、「すべて中止」スイッチを備えた状態で実行します。
- **プロアクティブなハンティング：**ハンティングエージェントは、インテリジェンスをテレメトリ全体にわたる継続的なハンティングに変換し、優先度の高いアラートを決して引き起こさないステルス性の高い脅威を表面化させます。
- **ロールベースのアクセスと制御：**きめ細かいRBAC、信頼度に応じたアクション制限、および承認ワークフローにより、エージェントのすべてのアクションがチームが承認した範囲内に確実に収まるようにします。

Trellix Wise for Private Cloud—エージェンティックSOCプログラムを推進する中核

Trellix Wise for Private Cloudは、エージェンティックSOCプログラムを推進する機能を担います。定額制の単一サブスクリプションとして提供され、お客様のハードウェアまたはVPC内で完全に実行されます。一般的なエージェンティックSOCソリューションとは異なり、エアギャップ環境でも完全にローカルで稼働できます。

AI主導の攻撃の時代に対抗する

Trellix Wise for Private Cloudは、アラートが発生した瞬間に100%調査し、低レベルのシグナル間の点と点を結びつけ、従来のツールが見逃す高度な攻撃を表面化させます。すべての判定には明確に定義された信頼度と監査可能な具体的な証拠が付随するため、SOCアナリストはデータ相関作業に時間を浪費することなく、戦略的な意思決定に専念できます。Trellix Wise for Private Cloudを使用することで、ついに形勢を逆転させ、SOCチームをプロアクティブで戦略的な防御に集中させるために必要なツールを手に入れることができます。

24時間365日のエージェンティックサポート

サブスクリプションには、SOC内のTier 1からTier 3のアナリストの役割をサポートするために構築された3つのコアエージェントが含まれています。これらのエージェントは調査、修復、ハンティングを専門としています。これらは24時間体制で稼働し、受信するアラートを100%検査します。Trellix Wise for Private Cloudは、ログイン、ディスカバリクエリ、認証情報イベント、ラテラルホップ、エグレススパイクなどをツールやホスト、時間をまたいで関連付けるといった、他のソリューションが無視する深いコンテキスト上の問いを提起し、回答します。アラートのコンテキスト特性を調査することで、システムは検証済みの判定をアナリストに提供し、アラートのキューに埋もれることなく戦略的な意思決定を行えるようにします。

- **調査エージェント：**常時稼働の初期対応者として設計されたTrellix Wise for Private Cloudの調査エージェントは、受信するすべてのアラートを数時間や数日ではなく数分で自動的に評価、相関付け、トリアージします。ローカルコンテキスト、ユーザーロール、メンテナンスパターンを取り込み、何が真の脅威で何が誤検知かを特定することで、組織固有の運用リズムを学習します。
- **修復エージェント：**対応できない発見は、単なる詳細な侵害記録に過ぎません。調査エージェントがTrellix Wise for Private Cloudの確認済みの調査結果を確定すると、修復エージェントが引き継ぎ、完全な証拠チェーンを継承して、影響範囲と関与するアセットのコンテキストをマッピングします。その後、それらをチームの権限に合わせて調整された、お客様が制御する管理された対応計画に変換します。信頼度が高くリスクの低い修復アクションは、最終的に自動化することができます。
- **ハンティングエージェント：**最も危険な脅威はルールに引っかからず、隙間に潜んでいます。当社のハンティングエージェントはアラートを待つのではなく、テレメトリ全体にわたって脆弱性や異常な行動を積極的に探しに行きます。これにより、検知システムが見逃すものを表面化させるプロアクティブなセキュリティが実現します。

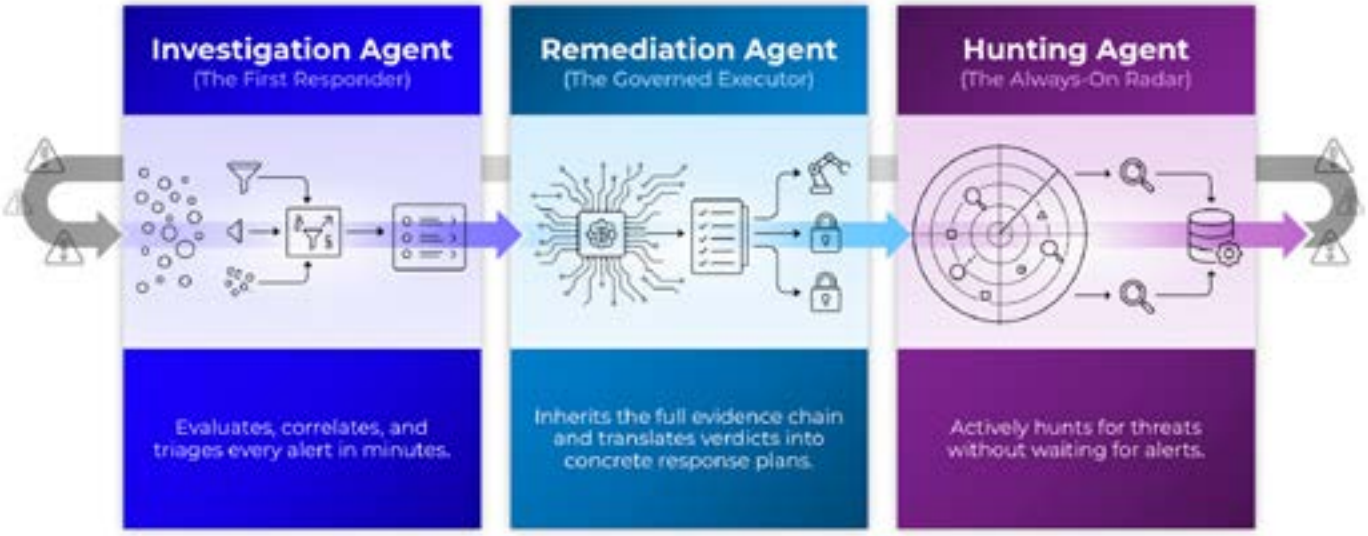


Figure 2. Trellix Wise for Private Cloudには、調査をサポートし、アラートに対応し、最新のインテリジェンスを使用して脅威をハンティングするエージェンティックチームが含まれています

実戦テスト済みのベストプラクティス

Trellix Wise for Private Cloudのエージェントは、数十年分に及ぶ文書化されたTrellixの脅威インテリジェンス研究と、実際のシナリオに基づく実戦テスト済みのベストプラクティスによってトレーニングされています。結果として、誤検知の微細な詳細を識別し、確実に有効な脅威を追跡できるようになります。

- **Trellix TRACEフレームワーク:**スピードは、その結果を信頼できてこそ意味があります。Trellix Wise for Private Cloudは、最も経験豊富なアナリストの作業手法をモデル化し、人間や一般的なAIが陥りやすいバイアスを排除した、構造化された反復可能な調査手法であるTRACEに従います。
  すべての調査は、Triage(トリアージ)、Range(範囲特定)、Analyze(分析)、Counteract(対抗)、Enhance(強化)の5つのフェーズを経て進み、各ステップで証拠に基づく結果を出し、さらにコンテキストが必要になった瞬間にいつでも後戻りできる自由度を備えています。
- **Trellix CHASEフレームワーク:**Trellix Wiseハンティングエージェントは、熟練したハンターの思考を体系化し、整ったアイデアから確証のある結果へと導く、CHASEと呼ばれる規律ある反復可能なフレームワークで動作します。エージェントは、お客様の構成に基づいて既存の検知ツール(SIEM、EDR、NDR、DLPなど)に対して複雑なクエリを実行し、ハンティング戦略の承認によって管理されます。
  すべてのハンティングは、Conceptualize(概念化)、Hunt(ハンティング)、Assess(評価)、Signal(シグナル化)、Enhance(強化)の5つのフェーズを経て、規律ある仮説が道筋を定め、徹底的なクロススタック実行が追跡を推進します。真のシグナルとノイズを分離する厳密な検証を実行し、具体的な調査結果とともに決定的な引き継ぎを行います。

再現性と信頼性の高い結果

重要な点として、Trellix Wise for Private Cloudは独自のSPLクエリを生成・実行して履歴コンテキストを引き出し、イベント、ユーザー、アセット、ハッシュ、行動ベースライン、レピュテーションを軸にして、すべてのハンターが最初に問う「これを以前に見たことがあるか？リスクはあるか？」という質問に答えます。そのクエリロジックはコード化、整理され、Trellix Wise for Private Cloud内に保存されており、生成されたすべてのクエリとツール呼び出しは不変の監査証跡としてキャプチャされます。

Trellix Wise for Private Cloudのエージェントは、孤立して推論するわけではありません。その出力はローカライズされたナレッジグラフを通じてお客様の環境に基づき、独自の調査および証拠データに対するアクティブ・コンテキスト・ラーニング（RAG）によって研ぎ澄まされます。すべての調査結果には、裏付けとなる証拠、MITRE ATT&CKマッピング、信頼度スコアが付随するため、アナリストはあらゆる判定と信頼度の根拠を検証できます。

その結果、環境に基づいた再現性と信頼性の高い調査が実現します。これは同時に、暗黙知が失われたり、アナリストの退職とともに使い捨てのクエリが使われなくなったり、シフトによって品質にばらつきが生じたりすることがないことも意味します。毎回、証拠に裏付けられた同じ厳格な調査プロセスが実行されます。

理解しやすい判定、監査可能な証跡、決して外に出ないデータ

Trellix Wise for Private Cloudはあらゆる判定を透明化し、何を観察し、どの程度確実であるかを示すため、そのまま続行するか、さらにコンテキストが必要かを決定できます。すべての判定には、調整された信頼度レベル、実際の証拠まで追跡可能な完全監査可能なホワイトボックスのケースファイル、お客様のデータに根ざし、経時的なAIの精度低下（ドリフト）に対して強化された推論が伴います。すべてはインフラストラクチャ内に留めることができるため、機密情報がクラウドに共有されることは決してありません。Trellix Wise for Private Cloudにより、最も規制が厳しくセキュリティを重視するチームでも、自らの条件に合ったエージェンティック防御をついに手に入れることができます。

- **絶対的な主権：**Trellix Wise for Private Cloudは、境界内で完全に稼働します。オンプレミスコネクタを備えたクラウドサービスではありません。完全なエアギャップネットワークを含め、環境内にデプロイされ完全に内部で動作する、エージェンティックSOCプログラムのコアです。モデル、ナレッジグラフ、学習されたコンテキスト、および推論のすべての段階がローカルで実行されます。Trellix Wise for Private Cloudが完全な能力で防御するために、環境、調査、または人員に関するいかなる情報も外部に出る必要はありません。主権は一部の顧客向けの後付けの導入オプションではなく、アーキテクチャの第一原則です。
- **透明性のある推論と監査可能性：**Trellix Wise for Private Cloudは判定を下す際、どのシステムに接続し、どのようなパターンを観察し、どのアクションを実行したかという推論の過程をユーザーが確実に理解できるようにし、必要に応じてAIの入出力に対する完全な監査可能性を提供します。その結果として得られる多層的な信頼度レベルにより、そのまま進めるのに十分か、あるいはシステムの精度を高めるためにどのような追加のコンテキストが必要かを判断できます。
- **制御とセキュリティ：**Trellix Wise for Private Cloudにより、アナリストは組織によって定義されたガードレールと標準作業手順の範囲内で、強力なエージェントを管理する戦略的な意思決定者になります。適切なガバナンスを確保するためのRBACも整備されています。当社のセキュア・バイ・デザインのアーキテクチャにより、すべての統合、すべての認証情報、およびすべてのモデルとのインタラクションが、最初から障害や攻撃に耐えうるアーキテクチャによって確実に保護されます。



Figure 3. Trellix Wise for Private Cloudは境界内で稼働し、データと推論を組織内に留めます

予測可能な予算と自らの条件で実現する最新化されたSOC

Trellix Wise for Private Cloudは、従量課金制の予測不可能なコストなしでSOCチームのアウトプットを向上させます。ハードウェアまたはコンピューティングリソースを選択することで容量を設定し、定額で従量制限なく稼働します。人間のアナリストが十分にいるSOCはなく、誰もが限界まで負担を強いられています。Trellix Wise for Private Cloudは貴重な人材を置き換えるのではなく、アナリストの役割を高め、その能力を拡大させます。戦術的な単純作業を吸収することで、チームは機械にはできない戦略的で高度な判断を要する仕事に解放されます。ジュニアアナリストの学習曲線は加速し、シニアアナリストは1日でより広範囲をカバーできるようになるため、新たな脅威の状況に対抗するためにSOCを真に最新化するのに必要なツールを提供します。

- **予測可能な定額制のサブスクリプションライセンス:**トークンベースの従量課金モデルでは、予算が厳しくなるにつれてAIの利用を制限せざるを得ません。Trellix Wise for Private Cloudは、独自の定額制、ハードウェアまたはコンピュートベースのサブスクリプションモデルを提供します。エージェントごとの追加料金や段階的な利用モデルはありません。従量制限のない防御のために、エージェンティックSOCに必要なすべてのコア要素を予測可能なコストで入手できます。
- **追加のデータ移行やデータレイクは不要:**ほとんどのエージェンティックSOCセキュリティベンダーは、システムから価値を得る前にすべてのテレメトリを自社のデータレイクにダンプして正規化させるため、すでに所有しているデータの保存に二重に費用を支払うことになり、データ移行に数ヶ月かかることもあります。Trellix Wise for Private Cloudはこれを覆します。アラートをトリガーとして取り込み、既存のシステムを直接クエリしてコンテキストを取得します。データは元の場所にとどまります。構築、データ入力、または支払いを必要とする別個のデータレイクはありません。

実現への道筋

現代のSOCにおける最も過酷な現実は、アラートがキューで待機しているすべての秒が、攻撃者がラテラルムーブメントを行い、権限を昇格させ、チームが開く時間のなかった低レベルのイベントのノイズの中に消え去るために使われる時間だということです。ほとんどのチームはすでに自らを守るためのインテリジェンスを持っています。不足していたのは、マシンスピードで、大規模に、そして自らの条件に基づいて行動する能力でした。Trellix Wise for Private Cloudはこのギャップを埋めるため、次の侵害発生によって導入の必要性に迫られるのを待つのではなく、今日からエージェンティックSOCの運用を開始できます。

次のステップへ

Trellix Wise for Private Cloudの詳細はこちらから

デモのご要望はこちらから

Copyright © 2026 Musarubra US LLC