Cortex XDR

ディテクション&レスポンスにおけるセキュリティのサイロ化の打破

セキュリティ チームは、ランサムウェアやサイバースパイからファイルレス攻撃、そして有害なデータ侵害までのさまざまな脅威に直面しています。しかし、多くのセキュリティ アナリストが最も頭を痛めているのは、ニュースの見出しを席巻している無数のリスクではなく、毎日繰り返し行わなければならない作業です。インシデントをトリアージして、膨大な未処理のアラートを減らしていかなければならないのです。

このホワイトペーパーでは、セキュリティ アナリストが直面する難題について説明します。膨大なアラートや、非常に成熟したセキュリティ運用センター (SOC) の手にも余る複雑な調査プロセスなどです。そして、Cortex XDR を使用してセキュリティ運用のあらゆる段階でのディテクション & レスポンスに取り組むためのフレームワークを提案します。マルウェア、標的型攻撃、内部関係者の不正利用に対する不安が高まる中、Cortex XDR のようなツールが、脅威を排除して運用を簡素化する隠れた武器となる可能性があります。

包囲されたアナリスト

現在セキュリティ チームは、絶え間ない攻撃と終わりの見えないアラートという、2 つの難題に直面しています。攻撃者は無数の攻撃を成功するまでやみくもに仕掛けてくる可能性があることを、セキュリティ チームは知っています。侵入を減らすために、チームは通常複数のセキュリティ レイヤーを展開しますが、これらのツールでは平均で 1 週間に 11,000 件という膨大な数のアラートが生成されます。[1]

これらすべてのアラートに遅れず対処するために、多くのアナリストはできるだけ多くのアラートをトリアージして必要な措置を直ちに講じるよう努めています。これらのアラートには、調査に欠かせない重要な関連情報が不足していることが多く、アナリストは詳細を明らかにするために貴重な時間を費やすことを余儀なくされます。セキュリティ チームの 53% は、受信するアラートのうち半分も確認できていません。膨大な数の不正確で不完全なアラートが紛れ込んでいるからです。そして、そのためにビジネス リスクが高まっています。[2]

あらゆる場所に不正に侵入してきた脅威を検出する

攻撃の急増により、組織はその規模にかかわらず、ディテクション & レスポンス機能の採用を迫られてきました。それに対処するため、IT セキュリティ業界では、エンドポイント ディテクション & レスポンス (EDR)、ネットワーク ディテクション & レスポンス (NDR)、ユーザーの振る舞い分析 (UBA) などの多数のサイロ化ツールを導入してきました。しかし、これらのサイロ化ツールは、狭い範囲のアクティビティにしか対応できず、操作するには長年の専門的経験を必要とします。これらのツールをプロビジョニングするセキュリティ チームは、新しいネットワーク センサーとエンドポイント エージェントをさまざまな場所で導入して維持管理するためのコストを負担しなければなりません。

一方、ディテクション & レスポンス ツールを導入していない組織は、非常に巧妙なマルウェア、悪意のある内部関係者、標的型攻撃などの気づかれにくい攻撃を見逃してしまう可能性があります。これは、最新型の攻撃には、従来のようなセキュリティ侵害の痕跡 (IoC) となるもの (攻撃シグネチャや悪意のあるドメインなど) を使用しないことが多いためです。これらの脅威を検出する唯一の方法は、機械学習と分析を使用して、(アラートだけでなく) アクティビティを経時的にデータソース全体にわたって調べることです。

手作業での調査により攻撃者の滞留時間が増加

攻撃を検出しただけで終わることはできません。アナリストはアラートを調査し、詳細 (誰が、何を、いつ、なぜ、どうしたのか) を評価して、どのような対策を講じるべきかを判断する必要もあります。残念ながら、現在の多くのセキュリティ ツールでは、ユーザー、エンドポイント、ネットワーク、アプリケーション、脅威インテリジェンスについての限られた情報のみを大まかに伝えるアラートしか表示されません。このようなアラートでは、調査とレスポンスに必要な詳しい状況が示されることはめったにありません。結果として、アナリストは攻撃について明確に把握するために、あちこちのコンソールから手作業でデータを集めなければなりません。例えば、ネットワークに関するアラートを調査する場合、アナリストは、各インシデントに関連するエンドポイント、ネットワーク アクティビティ、ユーザーを特定するために、分析や相関付けといった手間のかかる作業を行う必要があります。現在の複雑でサイロ化されたツールでは、専門家でなければ難解な調査を進めることができません。

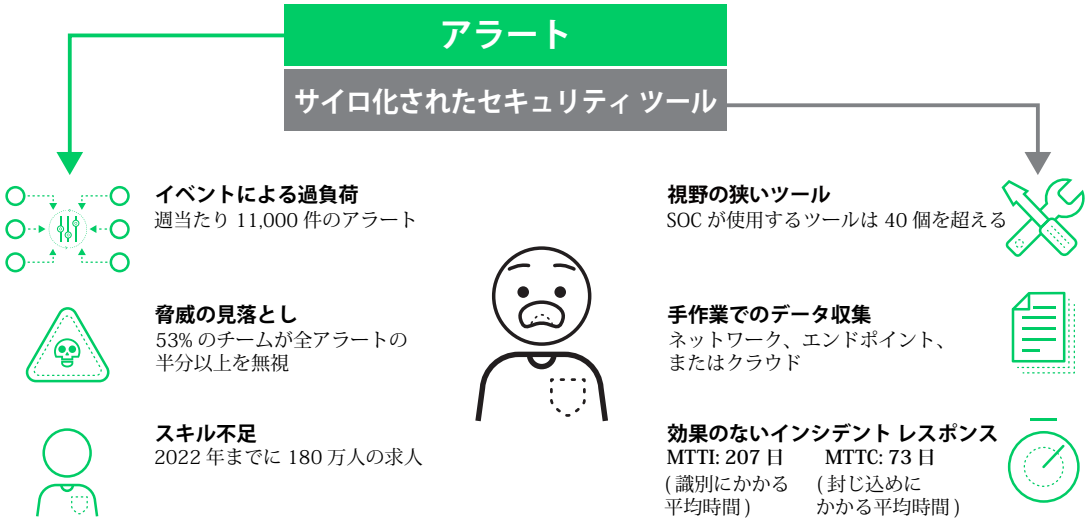
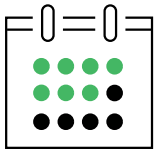


図 1: セキュリティ アナリストの多くの負担

1.「The State of Security Operations Report, 2021」、Forrester、
https://www.paloaltonetworks.com/resources/research/state-of-secops-forrester-consulting-study

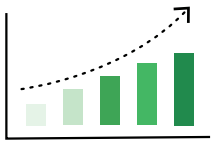
2. 同上

これらのツール同士が連携することはめったにないため、アナリストは、すべての適用ポイントにおけるレスポンスの方法を簡単に統合することはできません。攻撃を迅速にブロックするのではなく、チケットを送信するか、他のチーム メンバーにセキュリティ ポリシーの更新を依頼する必要があります。これには数日から数週間かかることがあります。ですから、組織が侵害を特定して封じ込めるまでに、平均してそれぞれ 207 日と 73 日かかるのも当然のことです[3]。セキュリティ チームはサイバーセキュリティの専門家の不足という問題に直面しており、セキュリティのサイロ化を打破してインシデント レスポンスを簡素化する必要に迫られています。そうしないと、サイバー攻撃の防御が難しくなります。



侵害の識別にかかる
平均期間 (MTTI) が増加 :

207 日



侵害の封じ込めにかかる
平均期間 (MTTC) が増加 :

73 日

図 2: MTTI と MTTC の改善

何が必要か

現在のセキュリティ運用の課題を解決するには、新しいアプローチが必要です。すなわち、検出や脅威のハンティングから、トリアージ、調査、レスポンスに至る、セキュリティ運用のあらゆる段階を容易にするアプローチです。この新しいアプローチでは 3 つの統合機能が必要で、それらを組み合わせてリスクを軽減し、運用を簡素化します。

- **優れた脅威防御** : 高効果の防御により、考えられるすべてのもの (リアルタイムまたはほぼリアルタイムで自動的にブロックできる、99% を超える攻撃) を阻止できます。手作業での検証は必要ありません。必要なのは、すべてのデジタル資産にわたる一貫した統合型防御です。
- **AI と機械学習** : 収集されるデータの量は増え続けており、脅威を特定するための手作業によるデータ分析や相関付けの作業をアナリストに押し付けるわけにはいかなくなっています。組織に固有の特性を学習し、予想される振る舞いのベースラインを構築して高度な攻撃を検出するには、機械学習と分析が必要です。
- **自動化** : アナリストが攻撃を迅速に確認するには、調査に関するあらゆる詳細が示された実用的なアラートが必要になります。また、経験豊かなアナリストでなくても攻撃の根本的な原因を容易に把握できなければなりません。

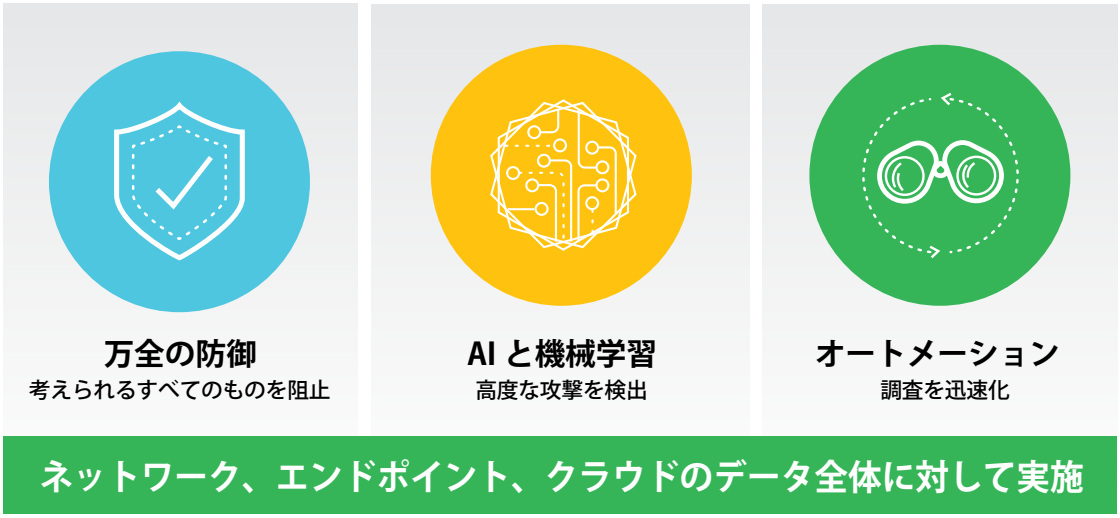


図 3: 重要な統合機能

これら 3 つを統合した機能を、すべての重要資産 (ネットワーク、エンドポイント、クラウドなど) で連携させることができれば、高度化する脅威に打ち勝つことができます。

Cortex XDR の拡張ディテクション & レスポンス

Cortex XDR® は、業界初の拡張型のディテクション & レスポンス プラットフォームで、ネットワーク、エンドポイント、クラウド、サードパーティのデータを統合し、高度な攻撃を阻止します。組織が運用を簡素化しながらデジタル資産とユーザーを保護できるようにするため、Cortex XDR はゼロから設計されています。

3.「2020 Cost of a Data Breach Study」、Ponemon Institute、2020 年 7 月、https://www.ibm.com/downloads/cas/861MNWN2.

振る舞い分析を使用して、ネットワークを標的とした未知の非常に巧妙な脅威を識別します。機械学習と AI モデルは、管理対象のデバイスであろうと、管理対象外のデバイスであろうと、あらゆるソースから脅威を見つけ出します。

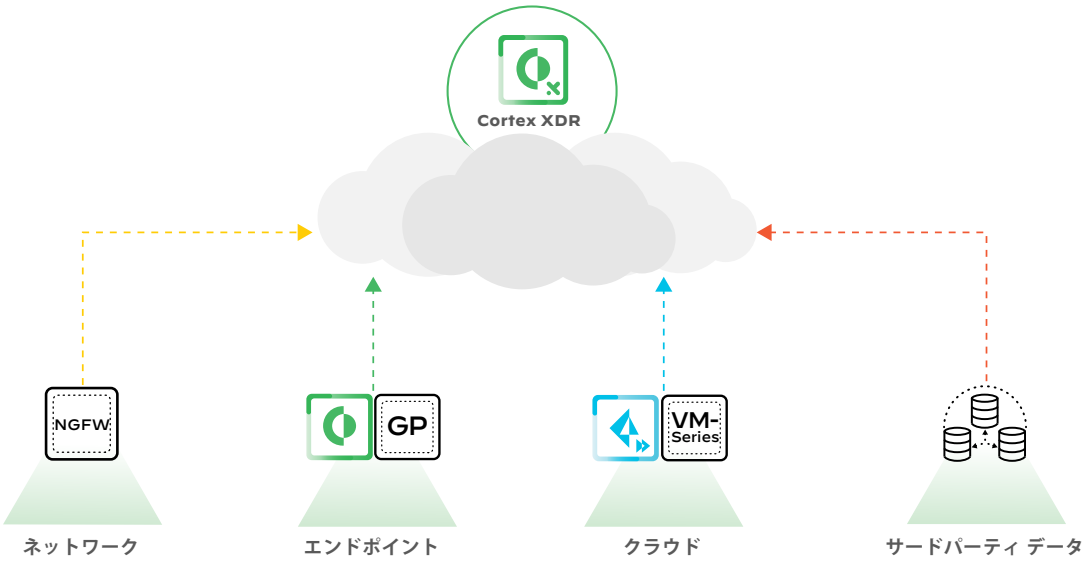


図 4: Cortex XDR による複数のソースからのデータの分析

Cortex XDR を使用すると、各アラートの詳細を把握して調査を迅速化できます。さまざまな種類のデータを統合して、アラートの根本原因とタイムラインを明らかにし、アナリストが経験の有無にかかわらずトリアージを実行できるようにします。適用ポイントとの緊密な統合によって、組織のどこからでも脅威に対応したり、ホストをクリーンな状態に簡単に復元したりできます。

Cortex XDR では、既存のネットワーク、エンドポイント、クラウド セキュリティをセンサーおよび適用ポイントとして使用できるので、新しいソフトウェアやハードウェアを導入する必要性がなくなります。Cortex XDR の使用に必要なデータ ソースは 1 つのみですが、データの統合と分析のメリットを享受するには、複数のデータ ソースが必要です。スケーラブルで安全なクラウドベースのデータ リポジトリにすべてのデータを保存することで、オンプレミスでの面倒なログ インフラストラクチャのプロビジョニングが不要になります。

Cortex XDR はセキュリティ運用のあらゆる段階でお客様を保護します

攻撃者は常に革新的な技術を使用しています。攻撃者に先手を打つには、セキュリティ チームはクラス最高の防御機能で攻撃を未然にブロックし、活動中の脅威を発見して阻止するための、反復可能なプロセスを実装する必要があります。Cortex XDR には、以下の 4 つの反復ステップを実行するためのツールが用意されています。

1. 自動脅威防御
2. 正確な検出
3. 迅速な調査
4. インテリジェントな対応

このフレームワークは、現在および将来にわたって組織を保護するために必要なすべてのものを提供します。

閉ループの防御、ディテクション & レスポンスの実現

完全な可視性を確保しながら、既知および未知の脅威を防御

鉄壁のセキュリティは優れた防御から始まります。そのために、Cortex XDR はクラス最高の防御を実現し、エクスプロイト、マルウェア、ランサムウェア、ファイルレス攻撃を阻止します。エンドポイントへの影響を最小限に抑えるように設計された軽量 Cortex XDR エージェントは、Cortex XDR 用のイベント データを収集しながら、攻撃をブロックします。

Cortex XDR エージェントは、マルウェアの感染を引き起こすエクスプロイトをブロックするための広範にわたるエクスプロイト防御モジュールをはじめとする、完全な防御スタックを装備しています。新しい攻撃手法への対処方法を常に学習している、AI を活用した適応型ローカル分析エンジンが、すべてのファイルを調べます。振る舞いベースの脅威防御エンジンは、複数の関連するプロセスの振る舞いを調べて、攻撃が発生すると同時に発見します。

複数の防御方法を組み合わせた次世代アンチウィルス (NGAV) は、エンドポイントの保護能力が特に優れています。マルウェア防御サービスのパロアルトネットワークス WildFire® と連携して、クラウド内の疑わしいファイルを分析し、すべてのパロアルトネットワークス セキュリティ製品にわたる保護を統合します。統合クラウド型エージェントをエンドポイントに迅速に導入し、ディテクション & レスポンスのための高度な攻撃のブロックとデータの収集を即座に開始できます。

AV-Comparatives が実施した Endpoint Protection and Response テスト (2021 年) で、Cortex XDR は戦略リーダーに選出されました。

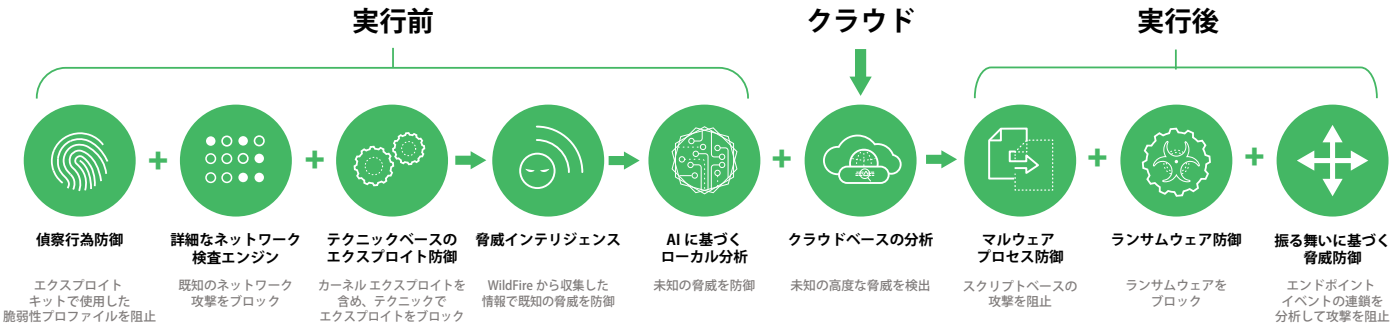


図 5: マルウェア、エクスプロイト、ファイルレス攻撃を自動的に防御

USB デバイスの安全な管理

USB デバイスは、バックアップ ストレージから周辺装置までのさまざまな用途で使用できますが、リスクを招くことがあります。マルウェアに感染したフラッシュ ドライブ、キーボード、または Web カメラをユーザーが無意識にコンピュータに接続したり、機密データをバックアップ用ディスク ドライブにコピーしたりすると、組織が攻撃にさらされます。Cortex XDR には強力なデバイス制御モジュールが同梱されており、ホストに他のエンドポイント エージェントをインストールすることなく USB デバイスへのアクセスを保護できます。Active Directory® のグループと組織単位に基づいてポリシーを割り当てたり、デバイス タイプごとに使用状況を制限したり、読み取り専用や読み取り / 書き込みのポリシー例外をベンダー、製品、シリアル番号で割り当てたりすることができます。デバイス制御モジュールで USB デバイスへのアクセスを簡単に管理でき、USB に起因する脅威が軽減されたという安心感を得られます。

ホスト ファイアウォールとディスク暗号化によるエンドポイント データ保護

ホスト ファイアウォールとディスク暗号化の機能を統合すると、セキュリティ リスクを軽減して規制要件に対応することができます。Cortex XDR ホスト ファイアウォールでは、インバウンドとアウトバウンドの通信を Windows® や macOS® のエンドポイントで制御できます。さらに、ディスク暗号化のルールとポリシーを作成することで、エンドポイントで BitLocker® や FileVault® の暗号化や復号化を適用できます。Cortex XDR は BitLocker や FileVault で暗号化されたエンドポイントを完全に可視化し、暗号化されたすべてのドライブの一覧を表示します。ホスト ファイアウォールとディスク暗号化により、エンドポイント セキュリティ ポリシーを Cortex XDR から集中管理できます。

かつてない可視性と迅速なレスポンスを Host Insights で実現

エンドポイントを保護するには、エンドポイントのすべての設定とコンテンツについて明確に把握してからリスクについて理解します。脅威を特定したら、迅速に阻止して複数のエンドポイントに拡散しないようにする必要があります。

Cortex XDR のアドオン モジュールである Host Insights は、これらすべての機能と追加の機能を提供します。Host Insights は、脆弱性評価、アプリケーションとシステムの可視化、そして強力な索敵せん滅機能により、脅威を特定し、封じ込めます。また、エンドポイントの可視化と攻撃の封じ込めのための包括的な手段を提供し、脅威にさらされるリスクを軽減して将来の侵害を防ぎます。

Host Insights は以下の機能を備えています。

- **索敵せん滅**：すべてのエンドポイントで脅威を迅速に検出して根絶できます。この強力な機能により、管理対象の Windows エンドポイントですべてのファイルの索引処理が行われるので、組織全体をスイープし、悪意のあるファイルをリアルタイムで検出して削除することができます。特定のホストで、きめ細かな設定に基づいて、ファイルやディレクトリを除外することができます。
- **ホスト インベントリ**：セキュリティ ギャップを特定し、Windows ホストの重要な設定とファイルを完全に可視化して防御態勢を強化することができます。ユーザー、グループ、アプリケーション、サービス、ドライバ、Autoruns、共有、ディスク、システム設定に関する情報を表示できます。ホストに関するすべての詳細情報を一元的に取得し、セキュリティの問題を迅速に特定して、追加のホスト コンテキストにより調査を迅速化できます。

図 6: Host Insights モジュール

- **脆弱性評価**：すべてのエンドポイントにおける脆弱性への露出と現在のパッチ レベルがリアルタイムで可視化され、軽減策に優先順位が付与されます。Cortex XDR は、米国立標準技術研究所 (NIST: National Institute of Standards and Technology) と Microsoft Security Response Center から提供される脆弱性の重大度に関する最新情報に基づいて、Linux や Windows のエンドポイントの脆弱性を明らかにします。エンドポイントにインストールされた Windows のマイクロソフト サポート技術情報 (KB) の更新内容も確認できます。

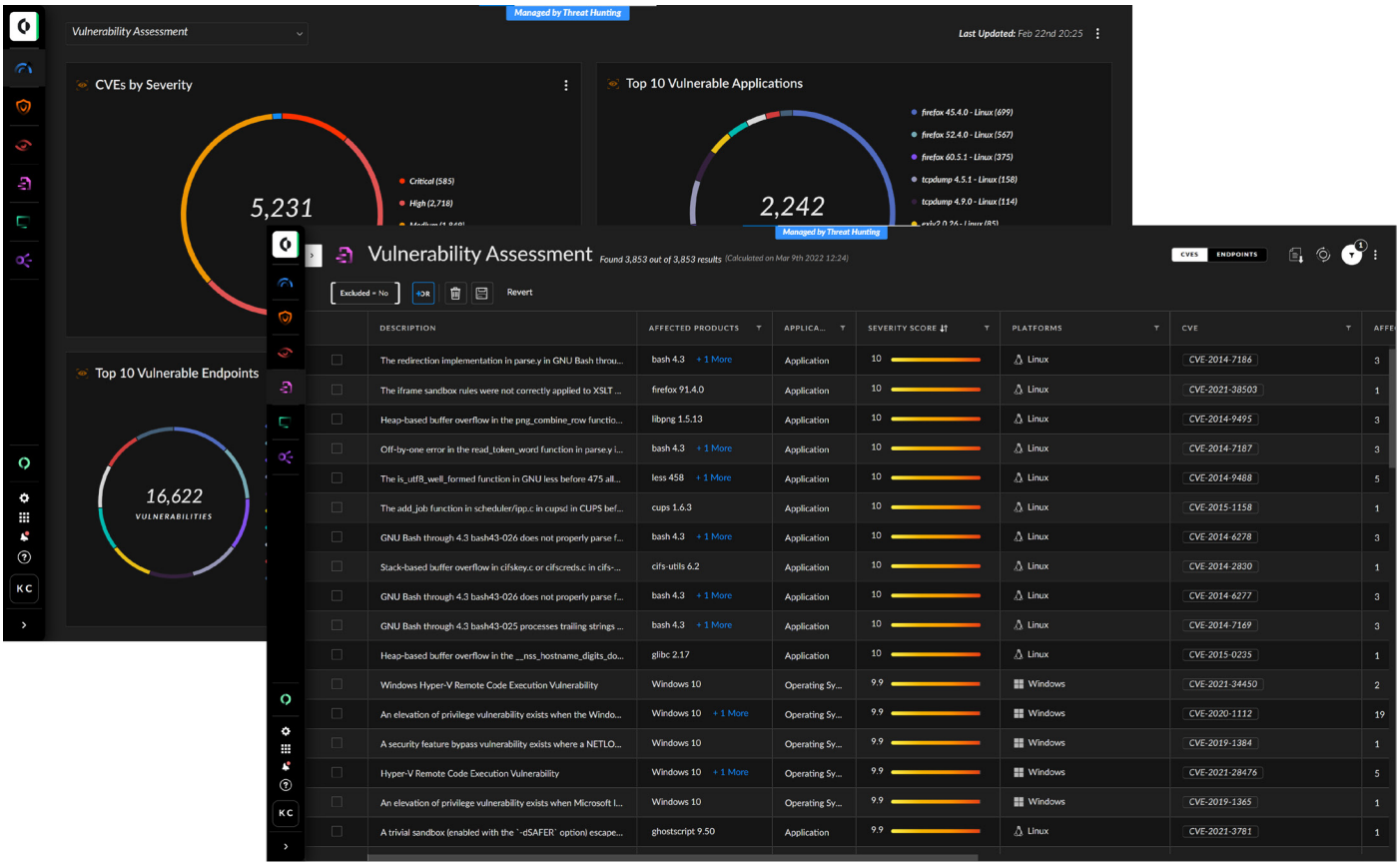


図 7: 最新 CVE データの脆弱性一覧表

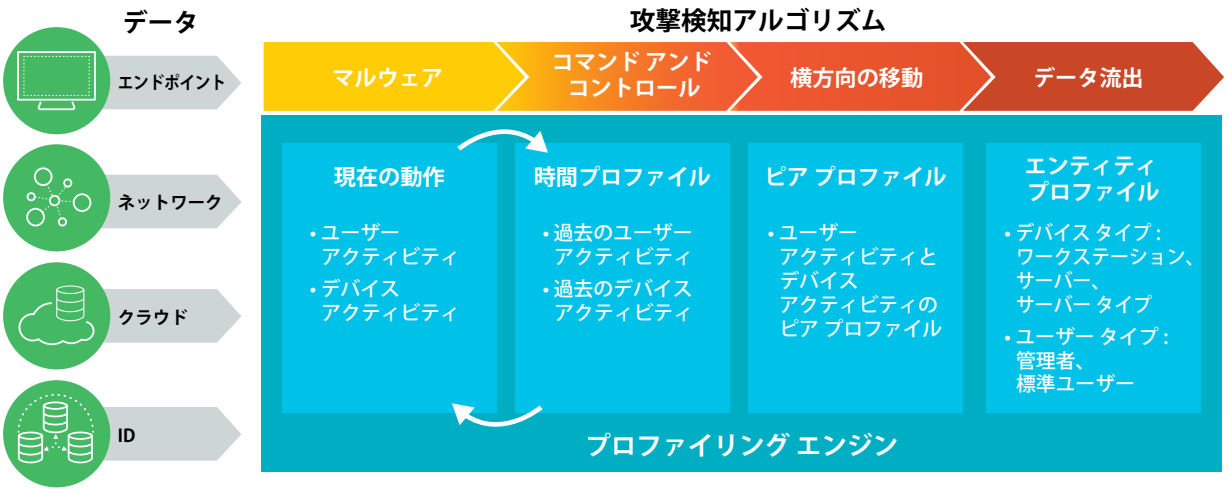


図 8: Cortex XDR の振る舞い分析アーキテクチャ

振る舞い分析と AI による攻撃の自動検出

Cortex XDR は、分析と機械学習を利用して気づかれにくい攻撃を見つけ出します。そのため、セキュリティ チームが攻撃の「滞在時間」を減らして侵害を迅速に封じ込めることができます。データ ソースから収集された豊富なデータを分析することから始めて、完全な可視性をもたらし、死角をなくします。また、ネットワーク、エンドポイント、クラウドの資産ら収集されたデータを統合して、攻撃を正確に検出し、調査を簡素化します。

Cortex XDR は、従来の脅威ログではほとんど確認が不可能な属性を含め、1,000 件を超える次元の振る舞いを追跡します。さらに、以下の機能を使用してユーザーとデバイスの振る舞いをプロファイルします。

- **教師なし機械学習** : Cortex XDR は、ユーザーとデバイスの振る舞いをベースライン化し、ピア グループ分析を実行して、デバイスを該当する振る舞いのグループに分類します。そして、これらのプロファイルに基づき、過去の振る舞いやピアの振る舞いと比較して異常を検出します。例えば、マルウェアの振る舞い、コマンド アンド コントロール、横方向の移動、データの引き出しなどの悪意のあるアクティビティを検出します。
- **教師付き機械学習** : Cortex XDR は、ネットワーク トラフィックの多様な特性を監視して、Windows コンピュータ、Apple iPhone®、脆弱性スキャナーなどの種類ごとに、各デバイスを分類します。また Cortex XDR は、どのユーザーが IT 管理者か一般ユーザーかを学習します。Cortex XDR は、教師付き機械学習を使用し、ユーザーまたはデバイスの種類に基づいた予想される振る舞いからの逸脱を認識し、誤検知を削減します。

ID 分析でユーザーベースの脅威に的を絞る

Cortex XDR 用 ID 分析アドオンなら、セキュリティ チームが従来のツールでは確認できなかった、リスクをもたらす悪意のあるユーザーの振る舞いを検出できます。ID 分析では、認証、エンドポイント、ネットワーク、クラウド、脅威ログなどの幅広いデータセットを長期にわたり調査して、ユーザーの振る舞いをプロファイルします。現在のユーザーの振る舞いを確立されたベースラインと比較することで、認証情報の盗難、ブルートフォース、「ありえない移動」などの攻撃を極めて高精度で特定します。ID 分析で動きの速い攻撃者の裏をかくことができるよう、検出アルゴリズムはクラウドベースの分析と指標を活用して継続的に改善されています。ID 分析アラートは、攻撃のステップバイステップ分析結果を表示するために、自動的に他のアラートとともにグループ分けされます。

カスタム ルールによる回避型脅威の検出

危惧される脅威や機密資産を標的にした攻撃をセキュリティ チームがカスタム ルールにより特定できます。Cortex XDR では IoC(マルウェア ハッシュなど) に基づくアラートをトリガできるほか、特定の攻撃者の戦術、手法、手順 (TTP) を、セキュリティ侵害の振る舞いの兆候 (BIOC) と呼ばれるカスタム ルールとして公開することもできます。高度な検出では、相関ルールに基づき、Cortex XDR の強力な XQL クエリ言語を使用して、振る舞いの複雑な組み合わせを 1 つまたは複数のデータセットからピンポイントで特定することができます。相関ルールを使用すると、システムやアプリケーションの悪用を特定できるだけでなく、攻撃を回避する手段が存在しない段階で発生するゼロデイ攻撃を検出でき、攻撃者がマルウェアの名前、ハッシュ、または IP アドレスを操作しても脅威を確実に発見できます。

アナリストは、プロセス、ファイル、ネットワーク、レジストリ情報など、多数のさまざまなパラメータに基づいてルールを定義できます。500 個を超える定義済みルールをそのまま使用して、持続的な脅威、改ざん、権限昇格、横方向の移動などの広範な脅威を検出します。これらの検出機能は毎日休みなく動作し、安心感を与えてくれます。

Cortex XDR により検査されるデータ

Cortex XDR は、パロアルトネットワークスの物理 NGFW と仮想 NGFW、および Prisma ®Access により収集されたトラフィック ログ、拡張アプリケーション ログ、脅威ログでプロトコルレベルのメタデータを分析します。Cortex XDR エージェントのエンドポイント データ、サードパーティ アラート、ログ データも調べます。Cortex XDR では、接続の頻度、トラフィックの送信元と宛先、使用されるプロトコルなどの、数百種類もの次元の振る舞いに基づいてプロファイルを構築することで、ユーザーおよびデバイスの予想される振る舞いを学習できます。Cortex XDR は、内部トラフィックとともに、クライアントやサーバーからインターネットへのアウトバウンド トラフィックも監視します。

セッションレベルのデータ

ファイアウォール トラフィック ログは、以下のような、ユーザーやデバイスの振る舞いをプロファイルするために必要なメタデータを提供します。

- 送信元 IP、宛先 IP、送信元ポート、宛先ポート
- 送受信バイト数
- 接続時間
- DNS、HTTP、DHCP、RPC、ARP、ICMP などに関するトランザクションレベルのデータを含む強化されたアプリケーション ログ
- App-ID™テクノロジからのアプリケーション詳細

ユーザー データ

Cortex XDR は、ネットワーク トラフィックとエンドポイント データを分析して、次のようなユーザー コンテキストを抽出します。

- ログインしているユーザー
- マシンの通常のユーザー
- 通信を開始したプロセスを作成したユーザー
- Directory Sync からのユーザー グループと組織ユニット
- Okta、Azure Active Directory、PingOne、PingFederate、Kerberos、Windows イベント ログの認証イベント

クラウド データ

Cortex XDR は、以下のような包括的なクラウド ログを収集します。

- Prisma Access と VM-Series
- Google Cloud Platform と Google Kubernetes Engine (GKE)
- Amazon CloudWatch と AWS CloudTrail
- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)

エンドポイント データ

Cortex XDR は、以下のような、あらゆるエンドポイント アクティビティを分析します。

- ファイルの作成、削除、更新
- ファイルのハッシュ値
- ファイル パス
- プロセス名
- レジストリの変更
- CLI 引数、RPC コール、コード インジェクション
- USB などのハードウェア イベント
- イベント ログの操作
- Cortex XDR エージェントのセキュリティ アラート
- WildFire マルウェアの判定

ホスト データ

Cortex XDR は、以下を追跡することによってマシンを識別します。

- ホスト名
- MAC アドレス
- オペレーティング システム

データ保持

- 最低 30 日間

脅威の捕捉と IoC の検索

アナリストが独自に検索を実行する場合も、調査を拡大する場合も、脅威のハンティングはセキュリティ運用で重要な役割を果たします。検索クエリを使用すると、セキュリティ チームは、特定のホスト、ファイル、プロセス、レジストリの更新、ネットワーク接続などを検索して、疑わしいアクティビティを発見できます。クエリには、「ホスト上の特定のプロセスによって特定のファイルにどのような変更が加えられましたか」といった明確なものも、「ドメイン内で実行されているすべてのプロセスを示してください」といった自由回答式のものもあります。セキュリティ チームは、新しいクエリ言語を学ぶことなく、攻撃の振る舞いや従来の IoC を検索できます。アナリストは結果をフィルタ処理して、確認するイベントの数を減らし、隠れた脅威を明らかにすることができます。高度な脅威ハンターでは、ワイルドカードと正規表現を使用した複雑なクエリの実行、検索結果の集約と可視化、全データを対象とした XQL 検索が可能です。セキュリティ チームは、脅威インテリジェンスとネットワーク、エンドポイント、クラウドの全データを組み合わせて活用することで、過去の攻撃を見つけられるほか、進行中のインシデントを数秒で明らかにできます。

データ統合と自動化により調査を 8 倍高速化

セキュリティ チームが脅威のトリアージと分析を迅速に行うには、完全な調査コンテキストが手元になければなりません。Cortex XDR は、アラートのトリアージとインシデント レスポンスを迅速化するいくつかの重要な機能を提供します。独自のインシデント管理ビューで、関連アラートをグループ化して、攻撃に関するすべての要素を表示します。たとえば、影響のあったホストやユーザー、脅威インテリジェンスの詳細情報、主要アーティファクト (例 : インシデントに関係するドメイン、IP アドレス、プロセス) などです。アラートのグループ化と重複除去により、アラートの数が 98% 減少し、アラート疲れが緩和されます。インシデント スコアリングにより、高リスクのインシデントのランクと優先順位を付けて、重要なインシデントに焦点を絞ります。セキュリティ チームはインシデントとアラートのソート、フィルタ処理、またはエクスポートが可能です。1 回のクリックで、あらゆるソースからのアラートを調査して、根本原因、レピュテーション、一連の関連イベントを即座に把握することができるので、誰でも簡単に脅威を検証することができます。

セキュリティ チームは、以下の分析ビューを使用して、あらゆるイベントで生じた問題に最終的に答えることができます。

- **根本原因分析ビュー** : 特許取得済みの独自の分析エンジンが、何十億ものイベントを継続的にレビューして、それぞれの脅威をもたらしている一連のイベントを特定します。攻撃がどのような順序で行われたかを根本的な原因にまで遡って可視化し、各要素に関する重要な詳細情報を提供することで、複雑な攻撃についても把握しやすくします。アナリストは、手作業でイベントを相関付けたりコンソール間を行き来したりすることなく、どのエンドポイント プロセスがネットワークまたはクラウドのセキュリティ アラートの原因となっているかを即座に確認できます。

図 9: Cortex XDR におけるアラートの根本原因と重要なアーティファクトの表示

- **タイムライン分析ビュー** : すべての攻撃アクティビティのフォレンジック タイムラインには、インシデント調査の実用的な詳細情報が表示され、アナリストは、範囲、影響、次のステップを数秒で判断できます。情報アラートにより複雑なイベントも把握しやすくなるほか、インシデントで確認された攻撃者の戦術や手法のすべてが MITRE ATT&CK® の可視化機能により表示されます。

Cortex XDR は、未処理のアラートへの対処や困難で時間のかかる分析に苦労しているセキュリティ チームを支援します。さらに、直感的で視覚的なコンテキストに基づいたツールを使用して、アラートのトリアージとインシデント調査を簡素化します。数時間、数日間、または数週間かかっていた分析を、詳しい専門知識がなくても、すべて数秒または数分で完了することができます。

脅威への対処と適用

脅威を特定したら、すぐに封じ込める必要があります。Cortex XDR を使用すると、セキュリティ チームは、ネットワーク、エンドポイント、クラウドの脅威を 1 つのコンソールで即座に排除できます。適用ポイントとの緊密な統合により、セキュリティ チームは、マルウェアの拡散を迅速に阻止し、デバイスとの間のネットワーク アクティビティを制限して、不正ドメインなどの脅威防御リストを更新することができます。

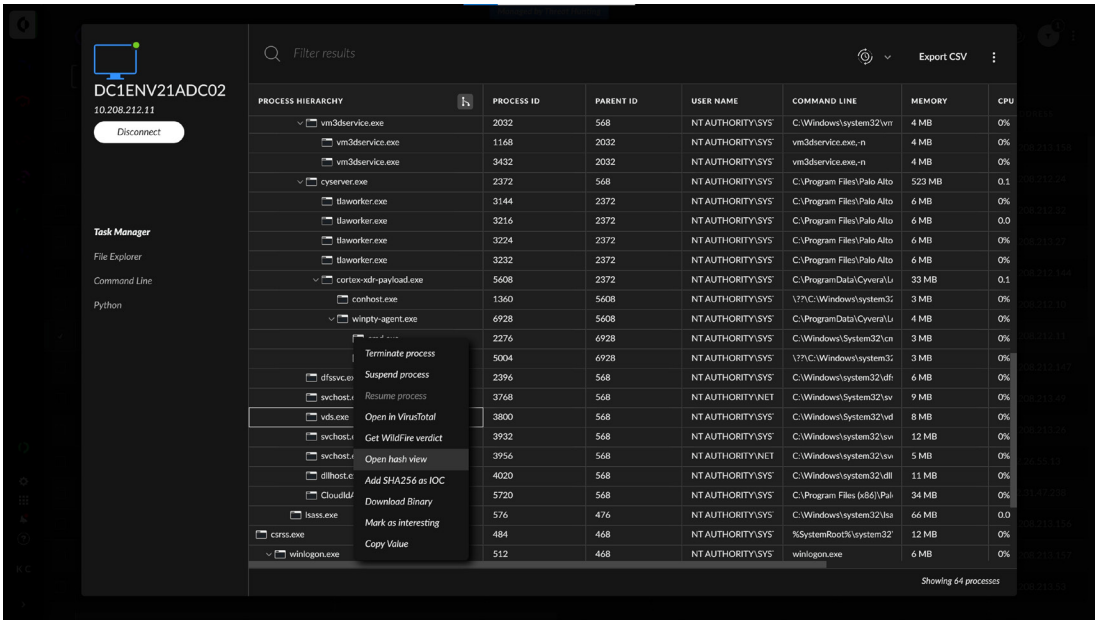


図 10: Cortex XDR Live Terminal Task Manager

以下が可能になる柔軟なレスポンス オプションで迅速に脅威に対処できます。

- **エンドポイントの隔離** :Cortex XDR 管理コンソールへのトラフィックを除き、侵害されたエンドポイント上のすべてのネットワーク アクセスを無効化し、それらのエンドポイントが他のエンドポイントと通信したり、他のエンドポイントを感染させたりするのを防ぎます。
- **プロセスの終了** : 実行中のマルウェアが、悪意のあるアクティビティをエンドポイントで実行し続けないようにします。
- **再実行のブロック** : 該当のファイルをポリシーのブラックリストに追加して、ブロックします。
- **悪意のあるファイルの検疫** : 悪意のあるファイルを Cortex XDR エージェントによる検疫が済んでいない場合はファイルを検疫して作業ディレクトリから削除します。
- **特定のファイルの取得** : さらに詳しく調べるために調査中のエンドポイントからファイルを取得します。
- **エンドポイント直接アクセス** : 極めて柔軟なレスポンス操作が Live Terminal で実現されます。たとえば、Python®、PowerShell®、またはシステムのコマンドやスクリプトの実行、アクティブ プ プロセスのレビューと管理、ファイルの表示、移動、またはダウンロードなどです。セキュリティ チームは作業中に、完全な監査を実行しながら、ホスト上の実稼働環境でプロセスを終了 / 削除することもできます。エンド ユーザーは、その間ずっと、脅威を排除しながら、中断やダウンタイムなしに作業を続けることができます。
- **オープン API の使用** : サードパーティ管理ツールと統合し、ポリシーを適用して、あらゆる場所からエージェント情報を収集します。
- **Cortex XSOAR との統合** : セキュリティ オーケストレーション、自動化、レスポンスが実現されます。セキュリティ チームはインシデント データを Cortex XSOAR と共有することで、450 個を超えるサードパーティ ツールにわたる、プレイブックに基づいた自動レスポンスが可能になります。Cortex XSOAR のプレイブックで、Cortex XDR のインシデントの取り込み、関連アラートの取得、Cortex XDR のインシデント フィールドの更新を、プレイブックのタスクとして自動的に実行できます。
- **Python ベース スクリプトの実行** :Cortex XSOAR などの Cortex XDR の管理コンソールやオーケストレーション ツールから行います。セキュリティ チームは、標準装備のスクリプトにより、この強力な機能を簡単に活用できます。
- **ファイルの迅速な検索と削除** : 組織全体で、索敵せん滅機能によりエンドポイント ファイルを索引処理します。
- **ホストをクリーンな状態に復元** : 修復策の提案機能を使用して行います。修復策の提案機能により、次の手順が推奨され、インシデントで特定されたすべての活動を解決できるようになるので、レスポンスが簡単になります。悪意のあるファイルやレジストリ キーが削除されるだけでなく、被害のあったファイルやレジストリ キーも復旧され、しかもカスタムスクリプトの再イメージングや作成は不要なため、攻撃から迅速に復旧できます。

管理、レポート作成、トリアージ、レスポンスの統合

Cortex XDR は、エンドポイントのポリシー管理、検出、調査、レスポンスの各機能を単一の Web ベース管理コンソールに統合し、シームレスなプラットフォームを実現します。カスタマイズ可能なダッシュボードでの迅速なセキュリティ ステータスの評価や、インシデントの要約、さらにグラフィカルレポートでのセキュリティの傾向の追跡が可能です。レポートはスケジュールしたりオンデマンドで生成したりできます。また、Cortex XDR エージェントを簡単に一元的に導入してアップグレードできます。

Cortex XDR は、脅威を予測して攻撃者の裏をかくよう、絶えず進化しています。業界で最も包括的なマルウェア分析サービスである WildFire と統合して、マルウェアを特定します。クラウド ネイティブのアプリケーションとして、コミュニティから得られる調査データを活用して、攻撃者の最新戦術を特定し、検出精度を向上させます。

MITRE | ATT&CK®

MITRE ATT&CK® ラウンド 3 テストにおいて Cortex XDR が保護と検出の総合スコアで最優秀と評価されました。これは、脅威を 100% 防御し、97% 可視化したことが認められたものです。

Forensics によるインシデント レスポンスの加速

Cortex XDR Forensics は強力なトリアージおよび調査ソリューションです。証拠の確認、脅威のハンティング、セキュリティ侵害調査を単一のコンソールから行えます。詳細データ収集機能を備えた Cortex XDR Forensics アドオン モジュールにより、豊富なフォレンジック アーティファクトに迅速にアクセスしたり、どこから攻撃が仕掛けられ、どのデータがインシデントでアクセスされたか (もしそのようなデータがあれば) を特定したりできるようになります。エンドツーエンドのソリューションとして、データ収集、分析、脅威ハンティング、修復といった、インシデント レスポンスのあらゆる手順に役立ちます。インシデント レスポンダーがインシデント レスポンダーのために設計したこのソリューションにより、調査が簡素化され、複数のセキュリティ ツールを使用することなく、Cortex XDR コンソールから攻撃者の挙動をくまなく追跡して、脅威を迅速に封じ込めることができます。

マネージド脅威ハンティングによる安心

Cortex XDR Managed Threat Hunting は、世界の名だたる脅威ハンターが 24 時間体制で脅威を監視する、エンドポイント、ネットワーク、クラウドの統合データ全体に対応した業界初の脅威ハンティング サービスです。弊社の Unit 42 専門家がお客様のために、国家が支援する攻撃者、サイバー犯罪者、悪意のある内部関係者、マルウェアなどの高度な脅威を検出します。弊社の脅威ハンターは、組織に潜んでいる攻撃者を検出するために、パロアルトネットワークスとサードパーティのセキュリティ ソリューションから得られる広範なデータを入念に調べます。

詳細な脅威レポートによって、攻撃のツール、手順、範囲が明らかになり、攻撃を迅速に根絶できます。また、影響レポートは、台頭する脅威に対して先手を打つのに役立ちます。

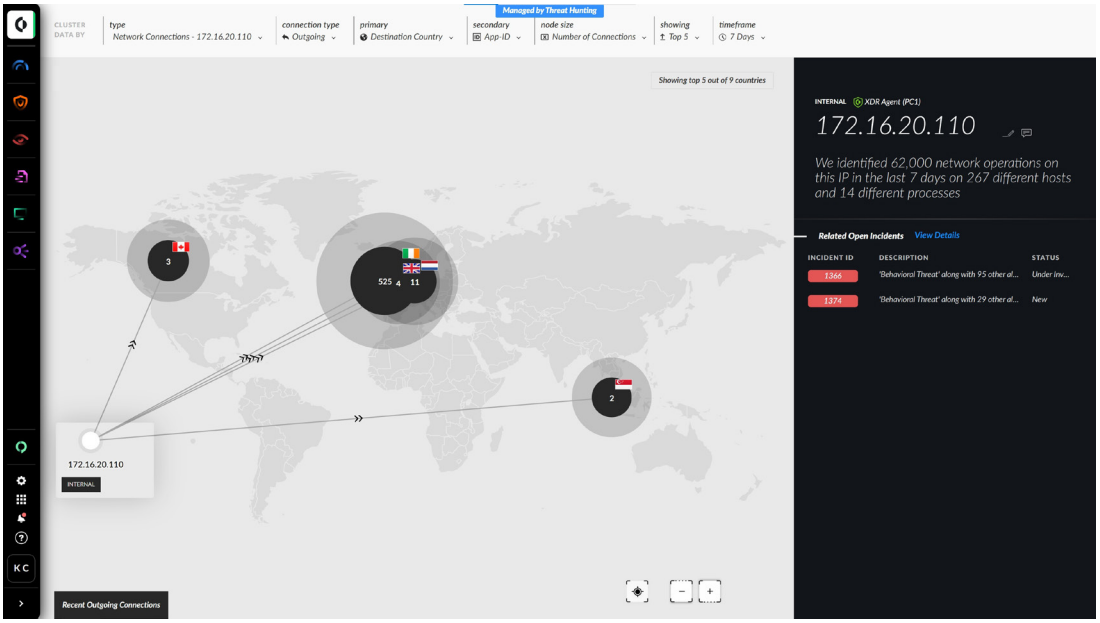


図 11: IP 表示 : IP アドレスに関する実用的な詳細情報と調査コンテキスト

クラウド導入の明るい見通し

Cortex XDR はクラウドベースのアプリなので、追加のオンプレミスのソフトウェアやハードウェアを導入する必要性がありません。Cortex XDR エージェントをはじめとする既存のパロアルトネットワークス製品をセンサーや適用ポイントとして使用して、セキュリティ運用を合理化します。パロアルトネットワークス インフラストラクチャから収集されたデータは、Cortex XDR プラットフォームに保存されます。このプラットフォームでは、サイズを拡大してディテクション & レスポンスに必要な大量のデータを効率的に処理することのできるログ ストレージが提供されます。Cortex XDR はすばやく導入することができ、時間をかけて新しい機器をセットアップする必要がなくなります。

Cortex XDR エージェントはすべてのエンドポイント (Windows、macOS、Linux、Chrome® OS、Android® のシステムなど) に簡単に導入でき、システムの再起動も不要です。物理サーバ、仮想マシン (VM)、コンテナに最適な Cortex XDR エージェントにより、モバイル デバイスからプライベート、パブリック、ハイブリッド、マルチクラウドの各環境までの、すべてのデジタル資産を保護できます。Cortex XDR により Kubernetes をスムーズに導入でき、セキュリティ スケールとクラウド ワークロードが保証されます。

ログ データをパロアルトネットワークスの次世代ファイアウォール、Prisma Access、Prisma Cloud、Cortex Xpanse、その他のセキュリティ インフラストラクチャから Cortex XDR に保存して、ログ管理と SIEM のコストを削減することができます。Cortex XDR は、オンプレミスのログ ストレージ、追加のセンサー、適用ポイントをなくすことで、サイロ化されたツールと比べて総所有コストを平均で 44% 削減します。また Cortex XDR は、攻撃を正確に検出し、調査を迅速に進められるようにして、セキュリティ運用チームの生産性を高めます。

Cortex XDR でセキュリティを向上

今はアナリストの心掛けが試される時代です。組織では、増え続ける脅威に対処するために、サイロ化されたツールの導入を進めていますが、そうしたツールは不完全で不正確なアラートを大量に発生させます。従来のセキュリティ情報とイベント管理 (SIEM) 製品は、クラウドベースの機械学習を使用してノイズをカットしたり検出が困難な攻撃を見つけ出したりするのではなく、セキュリティ インフラストラクチャによって識別された (そして、大抵は阻止された) 脅威に関するアラートの集約に的を絞っています。一方、サイロ化されたディテクション & レスポンス ツールの場合、IT スタッフは必要に迫られて追加のハードウェアやソフトウェアを導入したとしても、狭い視野の中で脅威を捉えることしかできず、死角が生まれてしまいます。そのため、アナリストは多数のツールから手掛かりとなる情報を収集して相関付けなければなりません。

Cortex XDR は、ネットワーク、エンドポイント、クラウドのデータをすべて統合して分析することにより、環境内のあらゆる場所に潜んでいる脅威を根絶するために必要な「秘密兵器」をアナリストに提供してします。Cortex XDR により、以下が可能になります。

- Cortex XDR エージェントにより高度なマルウェア、エクスプロイト、ファイルレス攻撃を防御
- 機械学習と分析により自動的にステルス攻撃を検出
- アラートの根本原因を明らかにし、アラートのトリアージと調査を迅速化して、すべてのセキュリティ アナリストの生産性を向上
- 複数の適用ポイントにわたってレスポンスを統合し、脅威を迅速に封じ込め
- クラウドのネイティブ導入により運用を簡素化、スケールとアジリティを向上

Cortex XDR を使用すると、ネットワーク、エンドポイント、クラウドの資産全体を完全に可視化でき、すべてのユーザーとデータが安全であることが保証されるので安心できます。

paloalto® NETWORKS | Cybersecurity Partner of Choice

〒100-0011
東京都千代田区内幸町2丁目1番6号
日比谷パークフロント15階

電話番号: 03-6205-8061
www.paloaltonetworks.jp

cortex_wp_xdr_031522