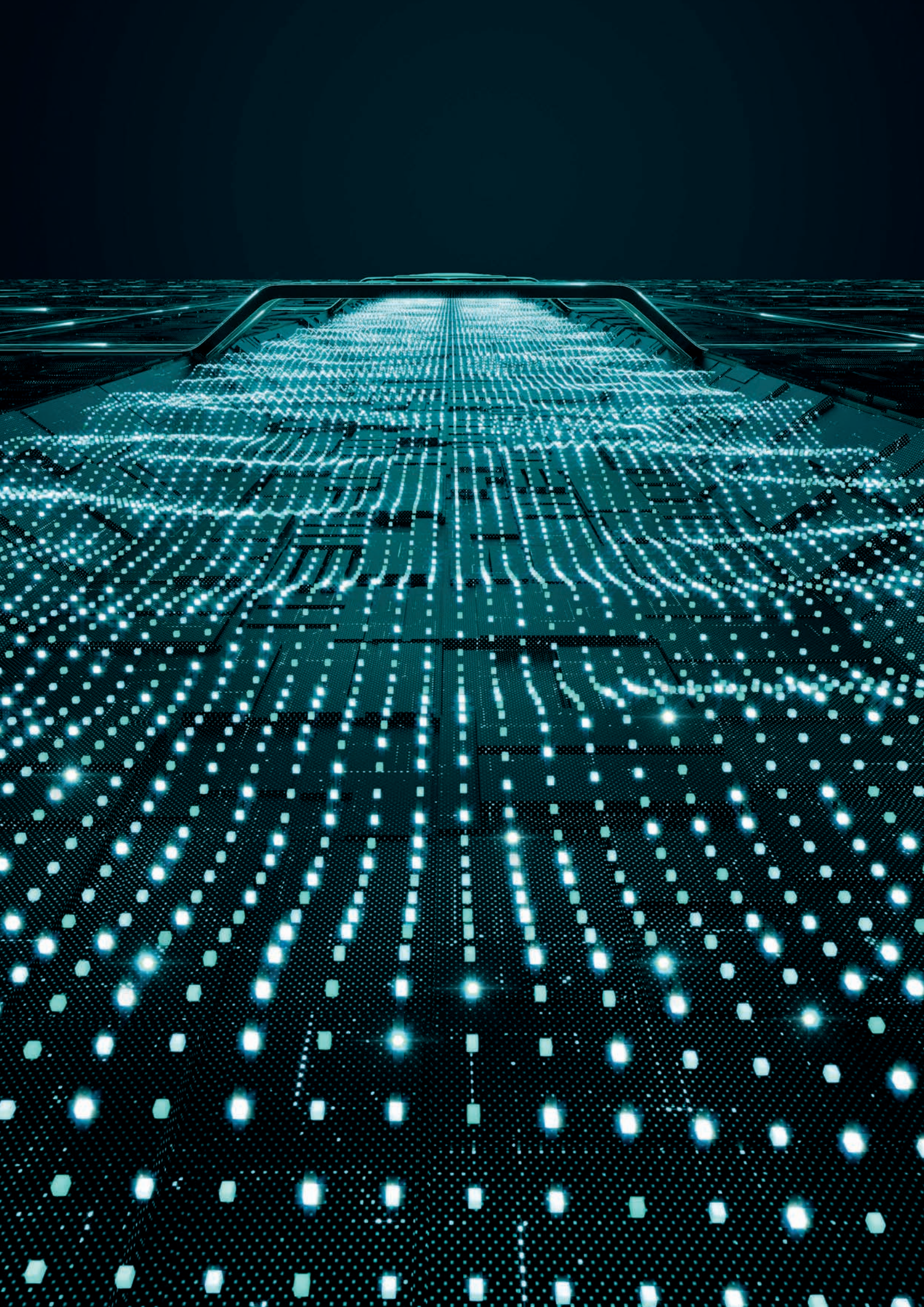
SOLUTION OVERVIEW

INSPECT

セキュリティ侵害の予防と可視化
攻撃による影響の復旧で優れた効果を発揮する
XDRコンポーネント

Progress. Protected.



XDR (Extended Detection & Response) ソリューションとは？

ESET Inspect は、一元管理ツールである ESET PROTECT プラットフォームに組み込まれている XDR コンポーネントです。異常な振る舞いやセキュリティ侵害の特定、リスク評価、インシデント対応、調査、修復を行うためのツールです。

インシデント対応の担当者は、ESET Inspect を利用して、ネットワークと接続されているデバイスのすべてのアクティビティを監視し、そのリスクを評価できます。また、必要な場合には、迅速に修正アクションを自動化できます。ESET は 800 以上の検出ルールを提供し、包括的な脅威ハンティングを実現します。

XDR を利用する理由

情報漏えい

企業は、情報漏えいが発生したことを特定するだけでなく、攻撃を封じ込め、修正しなければなりません。これらすべての対応は、事業を中断することなく、正確かつ効果的に実施する必要があります。このような専門的なすべての調査を行う準備ができている企業は少なく、多くの企業が外部のセキュリティベンダーに対応を委託しています。新たな脅威、従業員によるリスクの高い振る舞い、望ましくないアプリケーションによる企業利益の損失や評判の失墜を防止するためには、コンピュータの可視化を強化する必要があります。

金融、小売、ヘルスケア、公共部門などの組織では、業務の特性上、機密情報を扱っていることから、情報漏えいが最も多く発生しています。しかし、他の業界も決して安全というわけではありません。ハッカーは攻撃の労力と見返りを常に天秤にかけているだけです。

APT（持続的標的型攻撃）と標的型攻撃

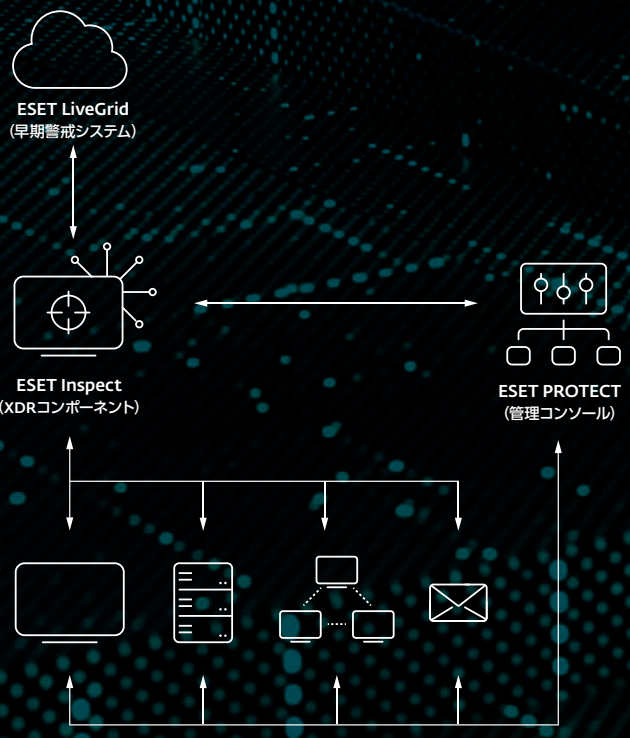
XDR システムは通常、脅威ハンティングによって APT や標的型攻撃を特定し、インシデント対応にかかる時間を短縮し、将来の攻撃を未然に防ぐために利用されます。APT を特定することは企業にとって特に重要です。数日から数ヶ月間検出を回避しながらネットワークに潜在して悪意のある活動を行う最新の攻撃への備えが十分にできている企業は多くないためです。

組織の可視性を向上

大企業にとって、フィッシング攻撃や従業員の不正など企業内の関係者による脅威は大きな問題になっています。大企業はフィッシング攻撃の対象となる従業員数が膨大であり、格好の標的になっています。たった1人の従業員でもフィッシングの罠に陥ると、企業全体のセキュリティが侵害される恐れもあります。そのため、大企業はフィッシングの攻撃者にとってその攻撃が成功する確率が高い標的となっています。企業内の関係者による攻撃も、大規模企業にとって重大な脅威の1つです。従業員数が多いほど、誰かが企業の利益に反する行動をとる確率は高くなります。

一般的にXDR システムは、組織にとって必要な可視化を提供し、すべてのデバイスのあらゆる問題を可視化・特定し、ブロックおよび修正できるようにします。たとえば、ESET Inspect は、Word ファイルなどの通常の業務で使用されるドキュメントを装った悪意のあるスクリプトを迅速に特定し、その実行を停止します。

また、セキュリティチームは **ESET 独自の振る舞いや評価ベースの検出機能**を簡単に利用できるようになるほか、ESET の LiveGrid（早期警告システム）に参加している1億台以上のエンドポイントから収集されるフィードバックもリアルタイムに提供されます。



新たな脅威、**従業員によるリスクの高い振る舞い**、**望ましくないアプリケーション**による企業利益の損失や評判の失墜を防止するためには、コンピュータの可視化が必要です。

ESET の特長

予防、検出、応答まで網羅する包括的なソリューション

ネットワークで発生するあらゆるセキュリティ問題を迅速に分析して修正します。ESET は多層防御のアプローチを実装しており、各セキュリティ階層から ESET Inspect にデータが送信されます。ESET は膨大なデータをリアルタイムに分析し、脅威を確実に検出します。

実績豊富なセキュリティベンダーのソリューション

ESET とサイバーセキュリティ脅威との戦いの歴史は 30 年以上にわたります。科学に基づくソリューションを提供する企業として、その軌跡の中で、機械学習、クラウドテクノロジー、最先端技術を自社で開発しています。

予防は治療に勝る

ESET の XDR に対するアプローチには、多数の受賞歴のある ESET が培ってきた予防テクノロジーが組み込まれています。脅威を未然に防ぎ、被害を最小限に抑えるには侵入・感染前の予防が最も重要です。ESET は高品質な多層防御構造の検出テクノロジーによって、最も効果的な予防を実現します。

可視化

判りやすい検出ルール（800 以上で随時追加）、高精度なセキュリティ侵害の痕跡（IoC）、検索機能、そしてネットワークにある実行ファイルの詳細なレビュー機能によって、攻撃との関連が疑われるあらゆる要素を特定します。

簡単に導入してすぐに利用可能

ESET ソリューションの特長は、導入してすぐに利用できるだけではありません。設定変更も容易に行え、担当者のスキルや経験レベルに応じて、詳細に検出ルールなどを変更できます。

柔軟な展開

ESET のセキュリティソリューションは自社のニーズに合わせて柔軟に展開できます。ESET Inspect は、自社のオンプレミスサーバーまたはクラウドベースの環境から実行でき、TCO の目標やハードウェアキャパシティに応じて設定を調整できます。

MITRE ATT&CK™

ESET Inspect は、検出した脅威を MITRE ATT&CK ™フレームワークに関連付けて表示します。これにより、複雑な脅威であってもワンクリックで包括的な情報を得ることができます。

レピュテーションシステム

セキュリティ担当者は、ESET の広範なフィルタリング機能と堅牢なレピュテーションシステムを使用して、無害が判別されているアプリケーションを識別できます。ESET のシステムには何億ものファイルのデータベースがあり、セキュリティチームは誤検出を発生させることなく、悪意の恐れがある新たなファイルの解析に時間を割くことができます。

自動化とカスタマイズ

ESET Inspect は簡単に調整でき、高度な自動化が可能です。初期設定時に、事前に設定されたユーザープロファイルを使用して、必要な対話レベル、保存するデータのタイプと量を選択すると、学習モードによって組織の環境がマッピングされ、誤検出を抑止する除外の提案が行われます。

活用事例

ランサムウェアへの徹底的な脅威検出

現在のランサムウェアは、ネットワーク内で秘密裏に活動し、できるだけ多くのエンドポイントへの拡散を試みます。コンピュータのバックアップにも侵入して破壊し、保存しているイメージをロールバックしても、ランサムウェアの実行を防止できない場合があります。

ESET Inspect エージェントは、ESET エンドポイントセキュリティソリューションの機能を拡張し、ネットワークにすでに潜在している可能性のあるランサムウェアをプロアクティブに検出します。ランサムウェア攻撃の典型的なシナリオでは、ユーザーに添付ファイル付きのメールが送信されます。ユーザーがその Word ファイルを開くと、マクロを有効にするように求められます。ユーザーがマクロを有効にすると、実行ファイルがシステムに展開され、マップされているドライブなど可能な限り多くのドライブに保存されているファイルの暗号化を開始します。

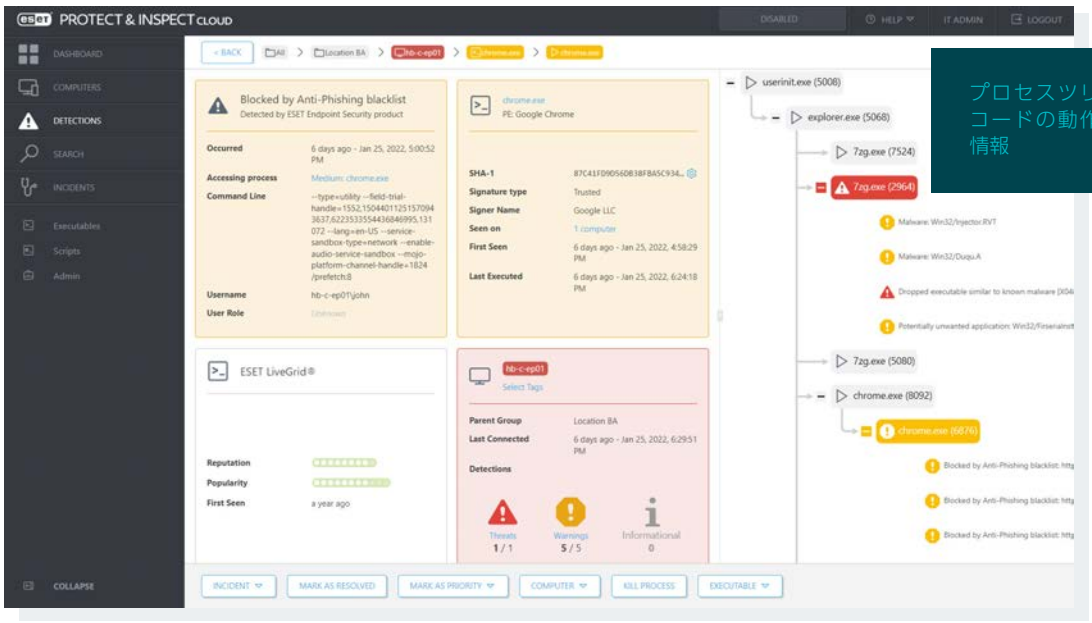
セキュリティ担当者は ESET Inspect を使用すると、このような振る舞いに対するアラートを確認できます。数回クリックするだけで、何が影響を受けているか、実行ファイル、スクリプト、アクションがいつどこで実行されたかを確認でき、根本原因を分析できます。

活用事例

ある企業は、ランサムウェア攻撃で見られる振る舞いがネットワークで確認された場合、迅速に通知を受けることができ、ランサムウェアをプロアクティブに検出するツールを必要としています。

解決方法

- ✓ 一時フォルダから実行されるアプリケーションを検出するルールを追加します。
- ✓ Office ファイル（Word、Excel、PowerPoint）が別のスクリプトや実行可能ファイルを実行する振る舞いを検出するルールを追加します。
- ✓ ランサムウェアが一般的に使用する拡張子がデバイスで確認された場合に警告します。
- ✓ ESET エンドポイントセキュリティソリューションのランサムウェアシールドのアラートを同じコンソールで表示します。



プロセスツリーと悪意あるコードの動作に関する詳細情報

振る舞い検出と従業員の無意識な行動

悪意のない一般の従業員が、セキュリティ上の最も大きな弱点となることが多くあります。

ESET Inspect は、トリガーされた各種のアラーム数をコンピュータ別にソートして、組織の中で脆弱となっている可能性がある箇所を簡単に特定します。特定のユーザーが多くのアラームを発生させている場合、そのユーザーのアクティビティを検証しなければなりません。

活用事例

ネットワークには、マルウェアの侵入を繰り返し許しているユーザーが存在します。同じユーザーが何度も感染するケースが見られます。そのユーザーはリスクの高い行動をしている可能性があります。また、他のユーザーよりも多く標的にされている理由が何かあるはずですが、どのように対応したら良いでしょうか？

解決方法

- ✓ 問題のあるユーザーやデバイスを簡単に確認できます。
- ✓ 根本原因を迅速に分析し、感染する原因を突き止めることができます。
- ✓ メール、Web、USB デバイスなど、特定された感染経路を修復します。

脅威ハンティングと脅威のブロック

ESET Inspect の最も優れている能力は、脅威をしらみつぶしに調査する脅威ハンティングです。

ファイルの特性やレピュテーション、デジタル署名、振る舞い、およびコンテキスト情報に基づいてフィルタを適用し、悪意のあるアクティビティを簡単に特定、調査できます。複数のフィルタを設定することで脅威ハンティングのタスクを自動化し、企業の環境に合わせて検出のしきい値を調整できます。

悪意のあるアクティビティも簡単に特定して調査できます。

活用事例

早期警戒システムやセキュリティオペレーションセンター（SOC）が新たな脅威を警告しています。次にどのような対策を講ずる必要があるでしょうか？

解決方法

- ✓ 早期警戒システムを活用して、今後予測される脅威や新たな脅威に関するデータを取得します。
- ✓ 新しい脅威が存在しないかすべてのコンピュータを調査します。
- ✓ すべてのコンピュータを調査し、警告が出される前に脅威が存在していたことを示すセキュリティ侵害の指標（IoC）を特定します。
- ✓ ネットワークへの脅威の侵入や、組織内での実行を防止します。

ネットワークの可視化

ESET Inspect はオープンアーキテクチャを採用しており、セキュリティ担当者は、攻撃手法の検出ルールを自社環境に合わせて調整できます。

また、ESET Inspect は柔軟に設定でき、Torrent アプリケーション、クラウドストレージ、Tor による匿名性の高いブラウジング、独自のサーバーの起動、および他の望ましくないソフトウェアなど、特定のソフトウェアの使用について組織のポリシーを規定して、その違反を検出できます。

活用事例

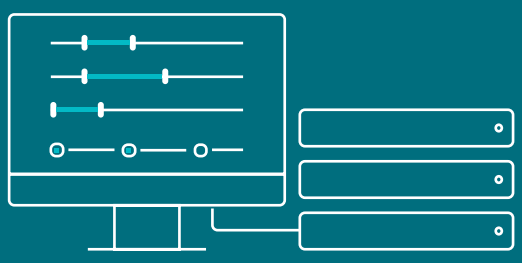
ユーザーがシステムで実行しているアプリケーションについて懸念している企業もあるでしょう。従来型のインストールアプリケーションだけでなく、実際にマシンにはインストールされないポータブルアプリケーションについても留意する必要があります。これらのアプリケーションを適切に管理するにはどうすれば良いでしょうか？

解決方法

- ✓ デバイスにインストールされるすべてのアプリケーションを簡単に表示してフィルタリングできます。
- ✓ デバイスのすべてのスクリプトを表示してフィルタリングできます。
- ✓ 承認されていないスクリプトやアプリケーションの実行を簡単にブロックできます。
- ✓ 承認されていないアプリケーションをユーザーに通知し、自動的にアンインストールして修復できます。

従来型のインストールアプリケーションだけでなく、実際にマシンにはインストールされないポータブルアプリケーションについても留意する必要があります。これらのアプリケーションを適切に管理するにはどうすれば良いでしょうか？

セキュリティチームは、攻撃手法の**検出ルール**を、自社環境に合わせて**調整**できます。



状況や環境の変化を考慮した調査と修復

アクティビティが悪意があるかどうかの判断は、状況や環境といったコンテキストによって変わる場合があります。

ネットワーク管理者のコンピュータで実行されるアクティビティは、財務部門のコンピュータのアクティビティとは大きく異なります。コンピュータを適切にグループ化すれば、セキュリティチームは、このユーザーが各マシンで特定の活動を行う権利があるかどうかを簡単に識別できます。ESET PROTECT のエンドポイントグループと ESET Inspect のルールを同期することで、優れたコンテキスト情報を得ることができます。

活用事例

データは背後にあるコンテキストを考慮して判断しなければなりません。適切な判断を下すためには、アラートの内容や、問題が発生したデバイスやユーザーについて把握する必要があります。

解決方法

- ✓ Active Directory、自動と手動のグループ化によって、すべてのコンピュータを識別し、ソートできます。
- ✓ グループ化したコンピュータに基づいて、アプリケーションやスクリプトを許可またはブロックします。
- ✓ ユーザーに応じて、アプリケーションやスクリプトを許可またはブロックします。
- ✓ 特定のグループのみが通知を受信するようにできます。

専門のセキュリティチームを必要としない容易なセットアップと対応

専門のセキュリティチームがいたとしても、多くのアラームが発生している中で優先順位をつけ、次のステップをすばやく決定することは困難を極めることが多くあります。

ESET Inspect では、アラーム発生時に修復への次の手順が必ず提案されます。ESET Inspect で脅威を特定すると、クイックレスポンス機能を利用できます。ハッシュを基準として特定のファイルをブロックしたり、プロセスを強制終了して隔離したり、選択したマシンをリモートから隔離したり、電源をオフにしたりできます。

活用事例

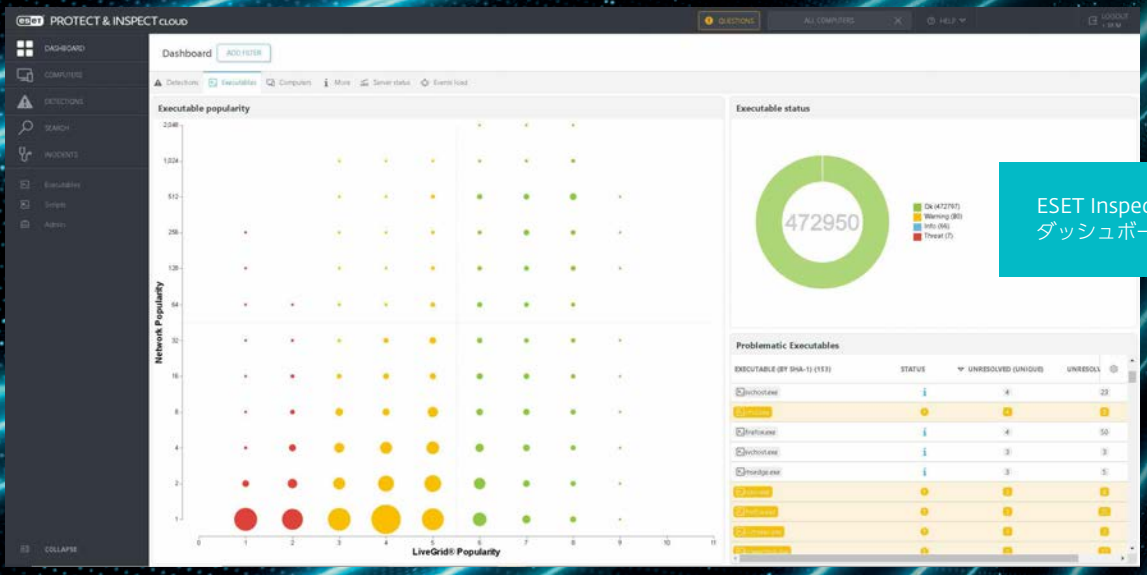
すべての企業に専門のセキュリティチームが存在するわけではありませんので、高度な検出ルールを作成して実装することは容易ではありません。

解決方法

- ✓ 300 以上の設定済のルールが組み込まれています。
- ✓ デバイスをブロック、電源オフ、隔離するボタンをクリックして、簡単に問題に対応できます。
- ✓ アラームが発生するときに、その修復への案と次に実行すべきステップを提案します。
- ✓ ルールは XML 言語で編集でき、細かな調整や新規作成も容易に行えます。

アクティビティが悪意があるかどうかの判断は、状況や環境といったコンテキストによって変わる場合があります。ESET PROTECT のエンドポイントグループと ESET Inspect のルールを同期することで、優れたコンテキスト情報を得ることができます。

ESET Inspect では、アラーム発生時に修復への次の手順が必ず提案されます。



ESET Inspect のダッシュボード

ESET Inspect の機能

インシデント管理システム

検出、コンピュータ、実行ファイル、プロセスなどのオブジェクトを論理的な単位にグループ化し、悪意の可能性があるイベントを、関連するユーザーアクションと一緒にタイムライン上に表示します。ESET Inspect は、インシデントのトリアージ、調査、解決の段階で大いに役立つ、すべての関連イベントとオブジェクト情報をインシデント対応の担当者に自動的に提供します。

ライブレスポンスオプション

エンドポイントの再起動とシャットダウン、他のネットワークからのエンドポイントの隔離、オンデマンドスキャンの実行、実行中のプロセスの強制終了、ハッシュ値に基づくアプリケーションのブロックなど、ESET Inspect ではワンクリックで簡単にアクションを実行できます。さらに、ESET Inspect のターミナルと呼ばれるライブレスポンスオプションによって、セキュリティ担当者は PowerShell の調査や修復オプションなど包括的な機能を利用できます。

根本原因分析

悪意の可能性があるイベントチェーンの根本原因分析と詳細なプロセスツリーを簡単に表示でき、攻撃の起点となったファイルや操作などの詳細レベルにドリルダウンして原因を特定します。マルウェアの専門家が作成した、悪意のない一般の操作や悪意のある攻撃に関する豊富なコンテキストと説明に基づいて、意思決定をすることが可能です。

パブリック API

ESET Inspect は、検出結果と修復内容にアクセスしてエクスポートできるパブリック REST API を実装しており、SIEM、SOAR、チケット発行システムなどのツールと効果的に統合できます。

脅威ハンティング

強力なクエリーベースの IOC 検索機能を使用し、データにフィルターを適用して、ファイルの特性、レピュテーション、デジタル署名、振る舞い、またはコンテキスト情報に基づいて分類します。複数のフィルターを設定すれば、APT や標的型攻撃を検出して阻止する機能など、脅威ハンティングやインシデント対応を自動化して簡略化できます。

安全でスムーズなリモートアクセス

コンソールとエンドポイントの両方に簡単に接続できなければ、インシデント対応とセキュリティサービスをスムーズに利用することはできません。ESET のソリューションでは、サードパーティツールを使用せずに最高レベルのセキュリティ対策を実施しながら、リアルタイムに近いスピードで接続できます。

ワンクリックで隔離

マルウェアがネットワーク内で拡散するのをすばやく阻止するネットワークアクセスポリシーを定義します。ESET Inspect のインターフェースでは、簡単なワンクリック操作で、セキュリティが侵害されたデバイスをネットワークから隔離できます。また、隔離状態のデバイスを簡単に元に戻すこともできます。

異常と振る舞いの検出

実行ファイルによるアクションを確認し、ESET の LiveGrid レピュテーションシステムを利用して、実行されたプロセスが安全であるか、攻撃の恐れがあるかをすばやく評価します。マルウェアやシグネチャを単に検出するルールではなく、振る舞いベースで攻撃を検出するルールによって、ユーザーに関連する異常なインシデントを監視できます。セキュリティチームは、ユーザーや部門を基準としてコンピュータをグループ化することで、ユーザーに特定のアクションを実行する権限があるかどうかを判断できます。

タグ付け

コンピュータ、アラーム、例外、タスク、実行ファイル、プロセス、スクリプトなどのオブジェクトに対して、タグを割り当て / 割り当て解除して、すばやくフィルタリングできます。タグはユーザー間で共有されます。また、一度作成すると数秒で割り当てることができます。

セキュリティ侵害の指標

ハッシュ、レジストリの変更、ファイルの変更、ネットワーク接続など、30 種類以上の指標に基づいてモジュールを表示してブロックします。

インテグレーション

ESET Inspect は、振る舞いとレピュテーションをベースとした ESET 独自の検出機能をセキュリティチームに提供します。すべてのルールは XML で簡単に編集できます。細かな調整ができ、SIEM との統合など、企業環境の特定のニーズに合わせて簡単に作成できます。

企業ポリシー違反の検出

組織のネットワーク内のあらゆるコンピュータで悪意のあるモジュールが実行されないようにブロックします。ESET Inspect のオープンアーキテクチャでは、Torrent アプリケーション、クラウドストレージ、Tor ブラウザ、その他の不要なソフトウェアなど、特定のソフトウェアの使用についてポリシーを適用し、ポリシー違反を柔軟に検出できます。

高度なスコアリング機能

インシデントに重要度を割り当てるスコアリング機能により、重要度の高いアラームから優先に対応できるようになり、管理者はインシデントが発生している可能性が高いコンピュータを迅速に特定できます。

ローカルでのデータ収集

新たに実行されたモジュールについて、実行時間、実行したユーザー、マシンでの滞在時間、攻撃されたデバイスなどの総合的なデータを表示します。すべてのデータはローカルに保存され、機密データが外部に漏洩するのを防止します。

ESET について

ESET は 30 年間にわたり世界中の個人および法人に向けて、業界をリードする革新的な IT セキュリティソフトとサービスを開発し、サイバーセキュリティ脅威に対する包括的な多層防御ソリューションを提供してきました。

ESET は長年にわたり、マルウェアの予防、検出、対応を行う機械学習とクラウドテクノロジーのパイオニアとして活動しています。ESET は、科学的な研究開発を世界的に推進している非上場企業です。

数値で見る ESET

10 億人＋
インターネットユーザーを保護

40 万＋
顧客数

200 ＋
国と地域に展開

13
世界各国の研究開発拠点

ESET の顧客

MITSUBISHI MOTORS
Drive your Ambition

2017 年から
9,000 台以上の
エンドポイントを保護

Allianz Suisse

2016 年から
4,000 以上の
メールボックスを保護

Canon Marketing Japan Group

2016 年から
32,000 台以上の
エンドポイントを保護

2008 年から
ISP セキュリティ
パートナーとなり、
200 万の顧客基盤を保護

業界最高レベルの標準への挑戦

AV comparatives APPROVED Business Security DEC 2021

ESET は、AV-Comparatives が
2021 年 12 月に実施した
ビジネスセキュリティテストの
ビジネスセキュリティ部門で
APPROVED の評価を獲得しました。

Leader WINTER 2022

ESET の製品は、グローバルな
ユーザーレビュープラットフォームで
ある「G2」において常に
上位にランクインしており、世界中の
お客様から高く評価されています。

FORRESTER®

ESET のソリューションは、
「The Forrester Tech Tide(TM)：
Zero Trust Threat Detection And
Response, Q2 2021（2021 年第 2
四半期ゼロトラスト脅威検出と応答）」
など主要なアナリスト企業から
定期的に高く評価されています。

Digital Security
Progress. Protected.