Solution overview

WithSecure™ Elements **Endpoint Detection and Response**

WithSecure™ Elements – サイバーリスク、複雑性、非効率性を低減

目次

最終更新日：2021年5月

1. はじめに

標的型サイバーセキュリティ攻撃は分析と対応が難しく、実際にデータが侵害される前であっても企業にとって非常にコストのかかる問題になる可能性があります。攻撃の影響を修復するためには、平均で2か月以上、コストも200万ドル近くかかるという調査もあります。[1] 従来型のウイルス対策ソリューションではファイルレス攻撃の検知は難しく、標的型攻撃は数か月または数年も見過ごされてしまうこともあります。[2] WithSecure™ Elements Endpoint Detection and Responseソリューションは、セキュリティ環境のコンテキストを可視化し、脅威の識別を自動化することで、サイバー犯罪者などの不正な第3者へ向けて露出された重要データ、機密データ、またはその他の保護されたデータの侵害が発生する前に、攻撃を阻止することができます。

WithSecure™ Elements の柔軟性により復元力のあるサイバーセキュリティを実現

現代のアジャイルなビジネス環境においては、変化し続けることこそが常態です。WithSecure™ Elementsは、ビジネスと脅威のいずれの変化にも柔軟に適応し、組織とともに成長するセキュリティソリューションを、オールインワンのパッケージで提供します。ライセンスモデルや使用する機能も柔軟に選択できます。WithSecure™ Elementにsは脆弱性管理、パッチ管理、エンドポイント保護、検知と対応などのサイバーセキュリティに必要なあらゆるコンポーネントが一つの軽量なソフトウェアパッケージに統合されており、クラウドベースの管理コンソールから一括管理できます。このコンソールからMicrosoft 365コラボレーションサービスのセキュリティを管理することもできます。

このソリューションは、ウィズセキュアのパートナーによるフルマネージドのサブスクリプションサービスとして、あるいはセルフマネージドのクラウドソリューションとしてご利用頂けます。セルフマネージドサービスからフルマネージドサービスへの移行は簡単で、サイバーセキュリティのスキルを持った担当者の採用に苦労している企業でも、変化し続ける攻撃ランドスケープの中でセキュリティレベルを維持することができます。

WithSecure™ Elementsは4つのソリューションから構成されており、すべてをWithSecure™ Elements Security Centerで管理することができます。

WithSecure™ Elements Endpoint Protection：

ウィズセキュアのエンドポイント保護はクラウドネイティブな実装で、AIを搭載しており、AV-TESTの「Best Protection」賞を何度も受賞しています。ブラウザーから簡単に導入することができ、すべてのエンドポイントのセキュリティを管理して、企業を攻撃から守ります。WithSecure™ Elements Endpoint Protectionは、モバイル、デスクトップ、ラップトップ、サーバーを保護します。

WithSecure™ Elements Endpoint Detection and Response:

ウィズセキュアのエンドポイントにおける検知と対応は、高度な脅威を完全に可視化します。独自のBroad Context Detectionにより、アラートのノイズを最小限に抑えてインシデントに集中することができ、自動化されたレスポンスにより24時間体制で効果的に侵害を阻止することができます。WithSecure™ Elements Endpoint Detection and Responseは、デスクトップ、ラップトップ、サーバーを保護します。

WithSecure™ Elements Vulnerability Management:

ネットワークや資産に潜む重大な脆弱性を発見し、管理します。脆弱性を見つけ、優先順位をつけて自動的にパッチを適用することで、攻撃対象領域を減らし、攻撃者の侵入経路を最小限に抑えます。

WithSecure™ Elements Collaboration Protection：

Microsoft 365が標準でサポートしているメールセキュリティ機能を強化し、メールやURLを介した攻撃を防ぐ高度なセキュリティを提供します。クラウド間統合のため、ソリューションの導入と管理が容易です。

WithSecure™ Elements Endpoint Protection、Endpoint Detection and Response、そしてVulnerability Managementは、単一のソフトウェアパッケージに統合されており、自動的に更新されるため、ソフトウェアの導入と管理にかかる時間とコストを削減できます。

統合ソリューションのメリット

WithSecure™ Elementsの各ソリューションはモジュール構造になっており、多様なニーズに柔軟に対応します。セキュリティ機能が統合されているため、ライセンス管理が簡単で、セキュリティ管理の手間も少なく、生産性を高めることができます。しかも、既存のサイバーセキュリティ環境を邪魔することはありません。
WithSecure™ Elements Security Center はクラウドベースのコンソールで、すべてのエンドポイントとクラウドサービスの可視性、インサイト、管理を一元化します。これは、ウィズセキュアのマネージドサービスプロバイダーのいずれかによって完全に管理されますが、困難なケースではウィズセキュアからのオンデマンドサポートの元でセルフマネージドとして自己管理することもできます。

Security Centerは、Endpoint Protection、Endpoint Protection and Response、Vulnerability ManagementおよびMicrosoft 365保護を組み合わせたセキュリティステータスを単一のビューで表示します。

[1] Ponemon Instituteの「2018 Cost of a Data Breach Report」には、データの流出を特定するまでに業界によって150日から287日の時間がかかり、データ流出への対応に平均69日間、176万ドルが費やされたことが示されています。

[2] Ponemon Instituteの「2020 Cost of a Data Breach Report」によると、データ流出の特定から封じ込めまでにかかった平均時間は280日でした。

すべてのエンドポイントソリューション（Elements Endpoint Protection、Endpoint Detection and Response、Vulnerability Management）は、一つのソフトウェアエージェントを共有しており、導入は一度ですみます。そしてアドオンソリューションは、追加のソリューションを展開することなく有効化することができます。WithSecure™ Elements Collaboration Protectionは、エンドポイントへのインストールが不要なクラウドベースのソリューションです。

WithSecure™ Elementsのソリューションは導入や管理のメリットに加えて、企業のセキュリティ上のメリットを最大化するために連携するように設計されています。WithSecure™ Elementsは、セキュリティイベントやアラートと XDR 機能を組み合わせることで、孤立したソリューションの壁を取り払い、統合されたセキュリティを提供することができます。

WithSecure™ Elements

	Endpoint Protection Standard	Endpoint Protection Premium	Detection and Response	Vulnerability Management	Collaboration Protection
高度なアンチマルウェアおよびパッチ管理	✓	✓			
データ保護とアプリケーション制御を備えたアンチランサムウェア		✓			
高度な脅威保護			✓		
脆弱性管理と優先度付け				✓	
Microsoft 365のための高度な保護					✓

注：サポートされる機能は、プラットフォームによって異なります

WithSecure™ Elements Endpoint Detection and Response とは

WithSecure™ Elements Endpoint Detection and Responseは、コンテキストレベルでエンドポイントの検知と対応（EDR）を行う主導的なソリューションであり、企業はIT環境とセキュリティ状況を即座に可視化し、攻撃を速やかに検知することでビジネスとその機密データを保護し、専門家の指導の元で迅速に対応できるようになります。

ウィズセキュアのソリューションは、深いレベルでの双方向のインテリジェンスと高いレベルの自動化により、侵害が発生する前であっても高度な脅威から保護します。企業ネットワークの監視対象のホストに軽量なクライアントをインストールし、インシデントを検知します。このクライアントは、ファイルアクセス、プロセスの起動、ネットワーク接続の開始、レジストリまたはシステムログへの書き込みなどの行動イベントに関するデータを収集します。そしてこれらのイベントが、このソリューションによって分析されるのです。このソリューションは、リアルタイムの検知に加えて、履歴データに基づいた検知も行います。ウィズセキュアでは、このテクノロジーと人間の専門知識を組み合わせて、世界クラスのエンドポイントの検知と対応を可能にします。

このソリューションはウィズセキュアによってサポートされているため、検知結果をウィズセキュアにエスカレートさせて、検知された脅威を経験豊富なサイバーセキュリティの専門家にさらに分析してもらうことができます。

このソリューションは、テクノロジーと脅威インテリジェンス、およびパートナーによるサービスを組み合わせてオールインワンの侵害検知および対応サービスとして提供する、マネージドEDRサービスとしてもご利用いただけます。マネージドEDRサービスは、企業のIT部門を脅威の監視とインシデント管理から解放し、真の脅威が検知された場合にのみアラートを発します。

しかし結局のところ、最先端のテクノロジーは解決策の一部に過ぎません。テクノロジーは、その背後にいる「人間」と同じ能力しか持ち得ないからです。ウィズセキュアの脅威ハンターと研究者は業界を主導する専門家であり、サイバーセキュリティ市場で最高の成果を提供することに専念しています。ウィズセキュアでは、テクノロジーと卓越した人間の専門知識を組み合わせて、世界クラスのエンドポイントの検知と対応のソリューションを提供します。

予防は、攻撃者の活動を妨害します

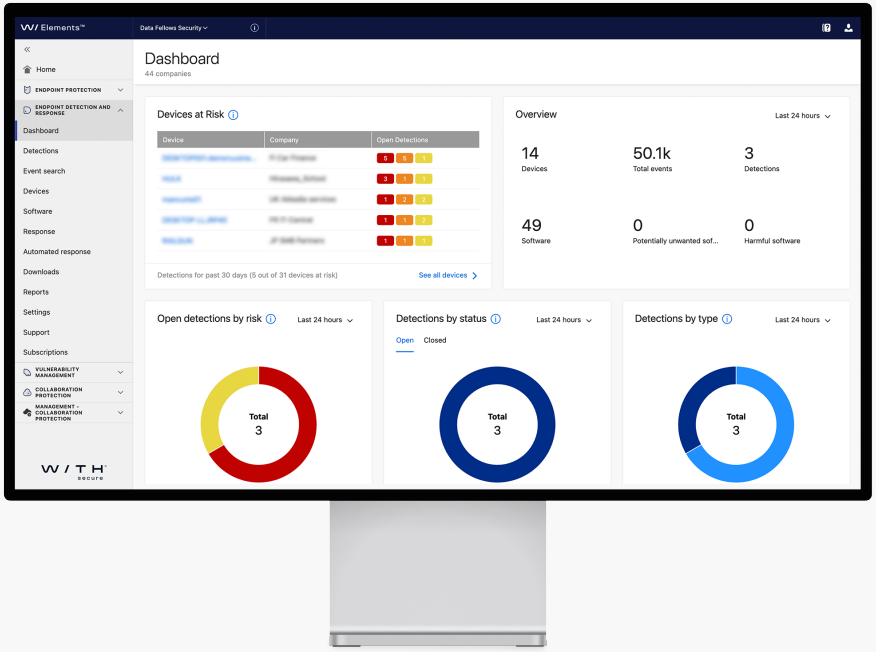
高度な攻撃者は、あらゆる障害を乗り越えてネットワークに侵入するスキルを持っているかも知れませんが、だからといって彼らのために赤い絨毯をを敷いて迎え入れる必要もありません。侵害される前から防止に力を注ぐことで、攻撃者がネットワークを侵害するのを少しでも難しくさせることができます。攻撃への障害を増やし、より多くの努力を強いることができれば、彼らのコスト構造が変化し、それが抑止力として働く可能性があります。

WithSecure™ Elements Endpoint Detection and Responseは、侵害された後に高度な攻撃を検知するためのソリューションであり、ランサムウェアなどのコモディティ型の脅威を阻止するために、強力なエンドポイント保護ソリューションを組み合わせる必要があります。

2. 主なメリット

WithSecure™ Elements Endpoint Detection and Responseソリューションを使用すると、ファイルレス技術を使用した高度な脅威と標的型攻撃を、データ侵害が発生する前に検知することができ、ウィズセキュアの最先端テクノロジーを利用していつでもそれらを迅速に分析して対応することができるよう準備を整えることができます。

このソリューションが可視性、検知、および対応のために提供する主なメリットのいくつかを以下に示します：



IT環境とセキュリティ状況を即座にコンテキストとして可視化します

- アプリケーションとエンドポイントのインベントリを使用して、IT環境の状況とセキュリティの可視性を向上させます
- マルウェアだけでなく、さまざまな行動イベントを収集して相互に関連付けることにより、正規の利用中の操作ミスを簡単に特定できます
- 幅広いコンテキストとホストの重要度を考慮したアラートにより、標的型攻撃を特定し、迅速に対応できます

侵害を迅速に検知し、ビジネスと重要データを保護します

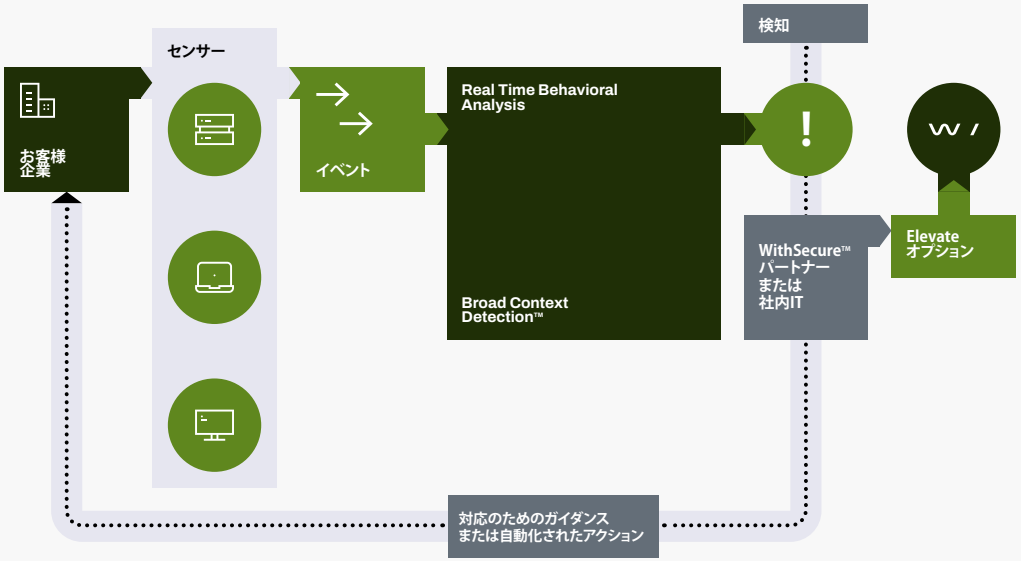
- 標的型攻撃を迅速に検知して阻止し、ビジネスの中断や企業のレピュテーションへの影響を防ぎます
- 高度な脅威の検知と対応の機能を数日で設定することができ、侵害が発生する前に迅速に準備を整えることができます
- EDR機能が有効化されているときにエンドポイントで実行されメモリ内で活動している脅威や攻撃の兆候を特定します
- PCI、HIPAA、およびデータ侵害から72時間以内に報告することを要求するEUのGDPRの規制要件を満たしています

攻撃を受けた場合に、自動化とガイダンスによって迅速に対応することも、自社SOCでの調査のために完全なインシデントデータを使用することもできます

- 組み込まれた自動化とインテリジェンスにより、現実の高度な脅威と標的型攻撃への迅速な対応を支援し、チームがそれに集中できるようにします
- アラートを受信した際に、どのように対応すべきかに関するガイダンスを受け取ることができ、24時間体制で対応アクションを自動化するオプションを用意しています（自動化機能はアップデートとして導入されます）
- ウィズセキュアの専門家がサポートするウィズセキュア認定のマネージドサービスプロバイダーに高度な脅威監視をアウトソーシングすることで、チームのスキルやリソースの不足を埋めることができます
- 脅威ハンティングを行えるお客様またはパートナー様向けには、脅威ハンティングサービスのイベント検索によってインシデントに関する完全なデータを提供します

3. ソリューション概要

WithSecure™ Elements Endpoint Detection and Responseソリューションは、簡単に導入できるクライアントとクラウドベースのElements Security Centerの組み合わせであり、オプションで認定パートナーによるマネージドサービスが提供されます。このソリューションは、高度な脅威と標的型攻撃を検知するための機能と、全体的なリスクと対応方法を明確にするためのBroad Context Detection™ による広範なコンテキスト検知を提供します。オンサイト部分には、企業のエンドポイントにインストールされるエンドポイントの監視と対応のクライアントが含まれます。



この図は、WithSecure™ Elements Endpoint Detection and Responseソリューションがどのように機能するかを大まかに説明したものです：

1. **軽量なクライアント**が、攻撃者によって行なわれるさまざまなエンドポイントでのアクティビティを監視し、行動イベントをクラウドへ向けてリアルタイムにストリーミング送信します
2. **リアルタイムの行動データ分析**により、イベントをトリガーしたプロセスとその他の行動の両方にフラグを立てて監視します
3. **Broad Context Detection™ のメカニズム**がデータをさらに絞り込み、関連するイベントを互いにコンテキストに配置し、実際の攻撃をすばやく識別し、リスクレベル、ホストの重要度、および一般的な脅威ランドスケープに関連して優先順位を付けます
4. **検知された内容が確認されると、**脅威を封じ込めて修復するために必要な手順を示し、ITチームとセキュリティチームをガイドします

3.1 管理ポータル：Elements Security Center

WithSecure™ Elements Endpoint Detection and Responseソリューションを使用すると、直感的に操作できるWebベースのコンソールから、エンドポイント上の高度な脅威を簡単にデプロイおよび管理し、監視できます。これにより、ユーザーがオフィスにいるか外出中かに関わらず、ネットワーク全体のIT環境とセキュリティ状況を即座にコンテキストとして確認できます。

管理ポータルは、要求の厳しいマルチサイト環境でのセキュリティ管理を簡素化し、強化するように設計されています。

以下に、このソリューションが高度な脅威の監視と管理にかかる時間とリソースを大幅に削減する方法をご紹介します：

- このソリューションは、あらゆるエンドポイント保護ソリューションと連携できるように設計されており、ウィズセキュアのエンドポイントセキュリティソリューションとは単一クライアントによる接続と管理インフラの元で機能します
- WithSecure™ Elements Endpoint Detection and Responseと組み合わせることで、マルウェアと高度な脅威の両方を可視化し、管理できるようになります
- 検知はすぐに役立つ視覚的情報として表示され、影響を受けるすべてのホスト、関連するイベント、および推奨されるアクションを含むタイムライン上の標的型攻撃の広範なコンテキストを提供します
- エンドポイントとシステムツールの高度な脅威管理を単一のエンドポイントセキュリティポータルに統合することにより、全体的な管理が大幅に簡素化され、時間を節約できます
- このソリューションはウィズセキュアが運用するクラウドベースのサービスのため、インストール作業およびサーバーのハードウェアやソフトウェアなどの保守作業は不要です：必要なのはブラウザとインターネット接続だけです

管理ポータルは、Microsoft Internet Explorer、Microsoft Edge、Mozilla Firefox、Google Chrome、Safariブラウザの最新バージョンで動作します。

管理ポータルは以下の言語で提供されています（2021年5月現在）：英語、フィンランド語、フランス語、ドイツ語、イタリア語、日本語、ポーランド語、ポルトガル語、スペイン語（LatAm）、スウェーデン語。

パートナー向けの管理ポータルには、エンドカスタマーのレポート、すべての監視対象企業の概要を表示する便利なダッシュボード、各々の監視対象企業独自のダッシュボードへのアクセスなど、サービスプロバイダーを支援するために特別に設計された機能が含まれています。

3.2 エンドポイントクライアント

エンドポイントクライアントは、異常を検知するために設計された軽量で目立たない監視ツールです。これらの異常には、企業内のすべてのWindowsおよびMacOSコンピューターで起こり得る未知の新しいイベントや、悪意のあるアクティビティに関連する可能性が高い一連のイベントが含まれます。このクライアントはエンドポイントから行動イベントデータを収集し、さまざまなエンドポイント保護ソリューションと連携するように設計されていますが、ウィズセキュアのエンドポイントセキュリティソリューションとは、単一クライアントでの接続とクラウドベースの管理インフラの元でシームレスに機能します。

右の表に、サポートされているオペレーティングシステムと機能を示します。

WithSecure™ Elements

	Windows workstations	Windows servers	Mac os	Linux
オペレーティングシステム	7 / 8 / 10	2019 / 2016 / 2012 /2011 / 2008 R2	10.12 or newer	
ウィズセキュアとの単一クライアント接続	Yes	Yes	Yes	Yes
行動イベント	Yes	Yes	Yes	Yes
アプリケーションの可視性	Yes	Yes	No*	No*
リモートホストの隔離	Yes	Yes	Yes	Yes

*** 将来のリリース予定：この機能はまだ利用できません。** 手動での操作により、WithSecure™ Business Suiteで利用できます。**

システム要件とクライアント展開の**詳細については**、https://help.f-secure.com/product.html#business/edr/latest/en/deploymentlatest-enのユーザーガイドを参照してください。

3.3 アプリケーションの可視性

IT環境とクラウドサービスを広範囲に可視化することで、高度な脅威やデータ漏洩に晒されるリスクを減らすことができます。ウィズセキュアのアプリケーションの可視性により、企業のネットワーク全体のエンドポイントで実行されているすべてのアクティブなアプリケーションを一覧表示できるため、不要な、もしくは未知の有害なアプリケーションを簡単に特定できます。

アプリケーションの可視性を使用すると、望ましくない可能性のあるアプリケーション（PUA：Potentially Unwanted Applications）と望ましくないアプリケーション（UA：Unwanted Applications）を識別できます。「望ましくない可能性のあるアプリケーション」には、望ましくない、または望ましくないと見なされる可能性のある行動または特性が見られます。「望ましくないアプリケーション」には、デバイスまたはデータに深刻な影響を与える行動または特性が見られます。

「望ましくない可能性がある」（PUA）として識別されるアプリケーションは、次のようなことを行える可能性があります：

- プライバシーや生産性に影響を与えます：たとえば、個人情報を公開したり、不正なアクションを実行したりします
- デバイスのリソースに過度の負荷をかけます：たとえば、過剰な量のストレージまたはメモリを使用します
- デバイスまたはデバイスに保存されている情報のセキュリティを危険に晒します：たとえば、予期しないコンテンツやアプリケーションに対して無防備な状態にします

これらの行動や特性がデバイスやデータに与える影響は、軽度から重度までさまざまです。しかし、これらのアプリケーションをマルウェアとして分類しなければならないほど有害ではありません。

イベントデータを収集し、脅威を検知して封じ込める

WithSecure™ Elements Endpoint Detection and Responseは、さまざまなエンドポイントからデータを収集し、お客様の環境における脅威の検知と阻止を支援します。このデータは、3つの異なる方法で提供されます：

1. **Broad Context Detection™：**この脅威特定方法は自動化されており、企業のエンドポイントから収集された膨大な行動イベントデータから真の脅威を発見できるように設計されています。また、WithSecure™ Elevate機能が組み込まれており、対応が困難なケースを解決するためにサイバーセキュリティエキスパートに専門的な指導を依頼することができます。
2. **Event Search：**この組み込みの機能を使用すると、Broad Context Detectionに関連する、企業のエンドポイントから収集したイベントデータを表示、検索して調査することができます。
3. **Event Search for Threat Hunting：**この高度な機能により、エンドポイントから収集されたすべての生のイベントデータを調査して処理できます。SOCのセキュリティ専門家がこの高度なフィルタリング機能を活用すれば、プロアクティブな脅威ハンティングにより、最も巧妙で見つけにくい脅威でも、検知して阻止することができます。
   Event Search for Threat Huntingは、WithSecure™ Elements Endpoint Detection and Responseのオプションコンポーネントです。

3.4 行動分析

行動分析は、大量の行動データイベントの中から高度な脅威を特定して、疑わしいイベントや、悪意を持っているかもしれない未知のイベントを特定するための中核的な機能です。

ウィズセキュアは、アクティビティに基づいて関連させることができる複数の疑わしいイベントを収集するために、行動、レピュテーション、ビッグデータのリアルタイム分析と機械学習を使用します。この行動分析機能は、攻撃者の戦術・技術・手順（TTP）の一環として実行される小さな個々のイベントから、悪意のある隠れたアクティビティを検知するために人工知能を活用します。行動分析は、監視対象の企業およびホスト、そしてIT環境全体に関連した検知のリスクスコアリングに影響を与える自動ホストプロファイル識別で使用されます。

この人工知能には、検知を継続的に改善し、誤検知を減らすために機械学習機能が含まれています。行動分析機能は、ウィズセキュアがデータサイエンスとサイバーセキュリティの専門知識を組み合わせた代表的な事例であり、このアプローチを「人と機械」と呼んでいます。

3.5 Broad Context Detection™

ウィズセキュア独自のBroad Context Detection™は、検知の数を絞り込むように設計されており、システムまたはデータが危険にさらされていることを示す可能性の高い、少数の有意なインシデントを検知します。

Broad Context Detection™は、標的型攻撃で使用される戦術・技術・手順（TTP）を管理者に警告することにより、侵害の兆候にフラグを立てます。これには、たとえば次のような疑わしいアクションが含まれます：

- 標準プログラムの異常な活動
- 標準ではない実行可能ファイルからの実行中のプロセスの呼び出し
- 予期しないスクリプトの実行
- 標準プロセスからのシステムツールの予期しない実行

Broad Context Detection™は、関連性のある検知のみを表示し、リスクレベル、影響を受けるホストの重要度に関する情報、および一般的な脅威の状況に基づいて重要度を割り当てます。単一のイベントであれば攻撃の兆候ではない場合もありますが、短い時間内で複数の検知が発生した場合には重要度の高いアラートとなり、インシデントの可能性があるとしてBroad Context Detection™が起動されることがあります。

これらのアプローチの結果として、ITチームには比較的短い確認済みの検知のリストが提供され、それぞれに異なる優先度レベルと推奨される対応アクションのフラグが付けられます。したがって、チームは最初に何に注力すべきかを知るだけでなく、対応する方法も知ることになり、自信を持って迅速にそれらを行うことができます。

Broad Context Detection™の詳細については、ホワイトペーパーを参照してください。

3.6 インシデント管理

このソリューションには、Broad Context Detection™ による検知を確認して管理するためのインシデント管理機能が組み込まれています。新しい検知が、詳細を表示してアクションを実行するための管理ポータルへの直接のアクセスを含んだEメールアラートをトリガーします。

Broad Context Detection™ による検知は、重要度と信頼レベルから自動的に計算されるリスクスコアに基づいてダッシュボードに一覧表示されます。リスクスコアが低く重要度の低いBroad Context Detection™ による検知もリストに表示されますが、それは、ゆっくりと進化する攻撃は、最終的にリスクスコアの高い、より深刻なインシデントになる可能性があるためです。

インシデント管理のアクションとしては、Broad Context Detection™ による検知を承認するか、「進行中」「監視中」「確認済みとしてクローズ」「誤検知としてクローズ」「未確認としてクローズ」にマーク付けすることです。Broad Context Detection™の誤検知をマークすると、同じ検知タイプに一致する将来の検知を自動的にクローズし、パラメータを「自動誤検知」として処理します。

3.7 対応のためのガイダンス

ソリューションに組み込まれた対応のためのガイダンスに従って、検知が確認された後に脅威を封じ込めて修正する際に必要な手順を実行することができます。封じ込めと修復の手順には、ユーザーへの通知やホストの隔離など、推奨される対応アクションが含まれます。

ウィズセキュアのサイバーセキュリティの専門家は、独自の経験を活かしてさまざまな一般的な脅威を分析し、ソリューションをトレーニングしてきました。そのためこのソリューションは、さまざまな高度な脅威に対応するためのわかりやすいガイダンスと、それに関連する対応方法のガイダンスを提供できます。

対応のためのガイダンスにより、スキルの低いITおよびセキュリティチームのメンバーでも、脅威を封じ込めて修正するための正しいアクションを簡単に実行できます。

Broad Context Detection™ が検知するアクティビティの例

検知用のデータは継続的に分析されており、Broad Context Detection™とウィズセキュアの脅威ハンターによって多くの種類の攻撃が新たに特定されているため、このリストには既知の攻撃以外も含まれます。

- ホストを標的とした**指示型攻撃**
- ホスト間の移動を伴う**ラテラルムーブメント**（横展開）
- 攻撃の一環としての情報の**なりすまし**
- 同じホスト上のプロセスを使用するなどの**永続性確保**
- 管理者権限へのブルートフォースなどによる**権限昇格**
- 標的のマシン/ネットワークへのアクセスと制御に繋がる**クレデンシャルへのアクセス**
- 標的のマシン/ネットワークから攻撃者が情報を盗み出すことを支援する**流出**
- 疑わしいパラメータを使用するなどの**異常なプロセス実行**
- 複数のドキュメントタイプやルートにアクセスしないシステムファイルなどの**異常なファイルアクセス**
- クライアントの設定を変更したり、クライアントを無効にしたりするなどの**クライアントの不正な変更**
- カーネルモードや他のアプリケーションなどの別プロセスへの**インジェクション**の試み
- リモートホストに対して開始された**C&C（コマンドアンドコントロール）ネットワーク接続**
- スクリプトのロード元として異常であるとフラグが立てられた**攻撃者からのPowerShellスクリプト**
- 永続性確保の一部として多く行なわれる**PowerShellによるPowerShellスクリプトの変更**
- モジュールをロードしたプロセスからのPowerShellによる**DLLの異常な使用**
- ラテラルムーブメント（横展開）に使用される可能性のある**リモート接続と実行**

3.8 Elevate to WithSecure™

ウィズセキュアは、検知結果についてウィズセキュアのサイバーセキュリティ専門家による脅威分析とガイダンスが必要な場合に備えて、オプションの脅威分析サービスを用意しています。Elevate to WithSecure™は一連のケースを分析するためのプレミアムサービスで、事前に注文する必要があります。

ウィズセキュアの脅威アナリストは、このソリューションを介してElevate to WithSecure™のリクエストを受け、特定の検知の周辺のクライアントから収集されたメタデータ全体にアクセスする許可を与えられます。

ウィズセキュアの脅威アナリストはSLA目標の2時間以内にリクエストをピックアップし、追加の証拠を収集し、ソリューションを介して脅威を検証するために専門家のガイダンスを提供し、オプションで脅威調査を提供するなどにより、潜在的なインシデントのタイプを特定する作業を開始します。

- Threat Validation（脅威の検証）は、Broad Context Detection™に関して過去7日間に発見された追加の情報を提供します。これには、専門家が作成した検知の概要と説明、および対応アクションが必要かどうかを判断するのに役立つその他の関連データが含まれます。
- Threat Investigation（脅威の調査）は、すべての直近および過去のデータを活用して、特定のBroad Context Detection™について詳細な調査を行います。このオプションには、検知された攻撃タイプについての包括的なレポートとともに、サイバーセキュリティの専門家による実用的なインシデント対応ガイダンスも含まれています。

Elevate to WithSecure™サービスは、手法とテクノロジー、ネットワークルート、トラフィックのオリジン、タイムラインなど、疑わしい潜在的なインシデントに関連する技術的証拠の分析に重点を置いています。ただし、ウィズセキュアのチームはソリューションを通じてガイダンスを提供するだけであり、インシデント対応をサポートするための追加のプロフェッショナルサービスについては、別途契約する必要があります。お客様が犯罪を疑う場合は、関係当局に連絡してこの脅威の調査レポートを提出することをお勧めしています。

3.9 アクションの自動化

標的型サイバー攻撃の影響を軽減するための自動対応アクションが用意されており、営業時間外にリスクレベルが十分に高まった場合にはサイバー攻撃を自動的に封じ込めます。この機能は、営業時間中にのみ検知の監視およびインシデントへの対応を行うチーム向けに特別に開発されたもので、夜間や週末でも自動で最初の対応アクションを行います。

4. データセキュリティ

4.1 データ保護と機密性

エンドポイントから収集された行動イベントデータは、お客様との契約中は1年間のローリングベースでEU（アイルランド）内に保存され、契約終了後2か月以内に削除されます。

このソリューションは、従業員の活動や興味、または会話のプロファイリングなど、セキュリティに関連しない活動を監視することを目的としていません。データ収集において注目している点は、個々の従業員、ビジネス文書、またはEメールの内容ではありません。詳細については、ソリューション固有のプライバシーポリシーを参照してください。

フィンランドを拠点とするウィズセキュアは、フィンランドとEU（欧州連合）双方の厳格なプライバシーとセキュリティに関する法規制を遵守しています。またウィズセキュアはEUのプライバシーフレームワークに準拠しており、プライバシーに対するお客様のニーズを理解しています。ウィズセキュアはEUデータ保護指令のフィンランドでの実装に基づいて運営されており、WithSecure™ Elements Endpoint Detection and Responseソリューションは、EU一般データ保護規則（GDPR）に従って設計されています。ウィズセキュアのGDPRへの準拠の詳細については、https://www.WithSecure.com/GDPRを参照してください。

4.2 データセキュリティ対策

セキュリティ企業として、ウィズセキュアはデータセンターのセキュリティは非常に重要であると考えており、以下を含む数十におよぶセキュリティ対策を行っています：

- セキュリティ・バイ・デザイン：ウィズセキュアのシステムは、セキュリティを確保するためにゼロから設計されています。私たちは、概念化と設計の初期段階から実装と運用に至るまで、テクノロジーとシステムの開発にプライバシーとセキュリティを組み込んでいます。
- 厳格なアクセス制御：ウィズセキュアの従業員のうち、厳選された少数のグループのみがお客様のデータにアクセスできます。アクセス権とレベルは、定義された責任に合致する最小特権の概念に基づき、職務と役割に基づいて決められます。
- 運用時の強力なセキュリティ：運用におけるセキュリティはウィズセキュアが日常行っている業務で、脆弱性管理、マルウェア防止、システムまたはデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティイベントの強力なインシデント管理プロセスを含みます。

4.3 データセンター

WithSecure™ Elements Endpoint Detection and Responseソリューションは、Amazon Web Services（AWS）のデータセンターを使用してレスポンス時間の短縮と必要に応じたスケーラビリティを実現し、可能な限り最高の可用性と耐障害性を確保しています。AWSは、各データセンターがTier 3+ガイドラインに準拠していることを確認しています。AWSデータセンターの詳細については、https://aws.amazon.com/compliance/を参照してください。

エンドポイントから収集された行動イベントデータは、ヨーロッパ（アイルランド）のAWSに保存されます。WithSecure™ Elements Endpoint Detection and Responseサブスクリプションには1年間のデータ保持が含まれており、収集されたデータの量に応じた追加のデータストレージ料金は必要ありません。

WithSecure™ について

WithSecure™は、ITサービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちはAIを活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は30年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988年に設立されたWithSecure™は本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。

ウィズセキュア株式会社
〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル2階
Tel: 03-4578-7710 / E-mail : japan@f-secure.co.jp
https://www.withsecure.com/
2022/05

WITH secure™