

報道関係者各位

ウィズセキュア、クラウドプラットフォーム向けの アイデンティティ保護ソリューションの提供を開始

～ リモートワークやクラウドの普及とともに増加するアイデンティティベースの攻撃を検出 ～

2024年6月7日
ウィズセキュア株式会社

クラウドベースのビジネスメールやその他のアプリケーションへのアクセスを標的とした攻撃が増加するなか、先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (本社: フィンランド・ヘルシンキ、以下、ウィズセキュア) は本日、WithSecure™ Elements Extended Detection and Response (XDR) の新しいモジュールとなる、Microsoft Entra ID などのクラウドプラットフォームを使用したリモートワーク環境を保護する WithSecure Elements Identity Security (以下、Identity Security) の提供を開始しました。

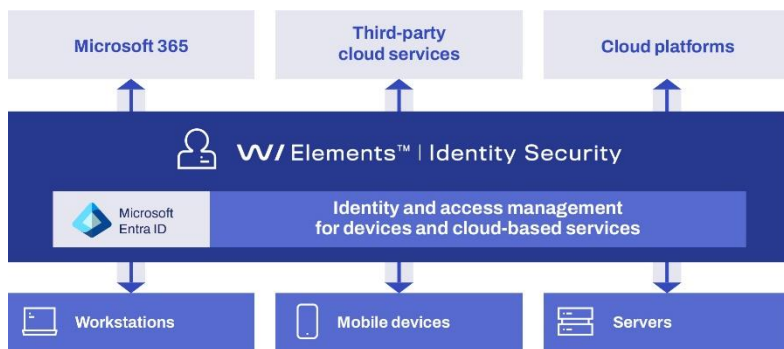
WithSecure Elements XDR は、エンドポイントや電子メールなどを含むクラウドベースのコラボレーションツールに対して高度な保護を提供するだけでなく、Microsoft 365 やその他のサービスへのアクセスに使用される Microsoft Entra ID のアイデンティティベースの脅威の検知や、侵害を受けた可能性のあるユーザーの検出を行います。これは、企業が直面するさまざまな高度な脅威から最新の情報テクノロジーを保護するための中心的な役割を果たす機能です。

リサーチ会社である Gartner 社はアイデンティティを標的とした攻撃について、「アイデンティティインフラに対するサイバー攻撃は一般的なものとなってきており、『アイデンティティファースト』というセキュリティのアプローチは、セキュリティ対策をおこなう部門にとっては制御すべき重要な領域なのです。」と語っています*1。一方、Identity Defined Security Alliance の最近の調査によると、組織の 90% が昨年、アイデンティティに関連する侵害を受けたと報告しています。*2

アイデンティティを標的とした攻撃が増加する中、これらの攻撃を可視化し、対策を講じることが重要です。従来の EDR コントロールではこうした可視化はできないため、ユーザーによる XDR ソリューションへの投資が不可欠となります。WithSecure で XDR のプロダクトディレクターを務める Mika Arasola (ミカ・アロソーラ) は、こうした状況に関して次のように述べています。

「当社のセキュリティエキスパートたちは Countercept Managed Detection and Response (MDR) サービスを利用いただいている顧客と共同で、1年以上にわたって検知の可能性を高めるための最適化をおこなってきました。当社の顧客とパートナーは脅威を認識しており、また、最新の IT 資産とリモートワーク環境の保護の必要性を理解しています。」

Identity Security は、Microsoft 365 などのクラウドプラットフォームへのアクセスに「盗まれた認証情報」が使用された場合に、危険なユーザーとセッションを特定することで、潜在的な危険に直面するユーザーを検出します。このソリューションはまた、疑わしい役割の割り当てや同意設定の変更など、さらなる攻撃につながる手法を特定し、それを強調して表示します。



WithSecure の Managed Detection and Incident & Response Operations の責任者である Diego Fuschini (ディエゴ・フスチーニ) は、アイデンティティへの攻撃についてこう語っています。
「攻撃者にとって、アイデンティティは新たな境界であり、アイデンティティベースの攻撃の増加が予想されます。AI の利用により、フィッシングはより精巧なものになっていくでしょう。」

WithSecure Elements XDR ソリューションには、攻撃のライフサイクル全体にわたって攻撃を検出することで、より高度な防御を提供します。巧妙なフィッシングメールによって従業員が騙されて不正なアクセスを提供したり、詐欺への支払いをしてしまったり、うっかりユーザー名／パスワード／多要素認証 (MFA) プロンプトを提供してしまうことを防ぐための追加的なコントロールが含まれます。

WithSecure Elements XDR が持つメリットには、最新の IT 環境における攻撃の可視化、AI を搭載したツールによる迅速な検出、調査、幅広いコンテキストでの脅威への対応、柔軟な 24 時間サービスによる顧客チームのパフォーマンスの増強などが含まれます。

WithSecure Elements Identity Security の詳細については以下のページをご覧ください:

<https://www.withsecure.com/jp-ja/solutions/software-and-services/withsecure-elements-identity-security>

*1:

Gartner Insights, Cybersecurity Trends: Optimize for Resilience and Performance, January 2024,

<https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends>

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

*2

2023 Trends in Identity Security report by The Identity Defined Security Alliance,

<https://www.idsalliance.org/press-release/new-study-reveals-only-49-of-organizations-proactively-invest-in-identity-protection-prior-to-a-security-incident/>

ウィズセキュア Web サイト:

<https://www.withsecure.com/jp-ja/>

ウィズセキュアプレスページ:

<https://www.withsecure.com/jp-ja/whats-new/pressroom>

WithSecure™について

ウィズセキュアは、多くのヨーロッパ企業に選ばれるサイバーセキュリティパートナーです。世界中の IT サービスプロバイダー、MSSP、ユーザー企業から、中堅・中小企業を保護するアウトカム(成果)ベースのサイバーセキュリティソリューションにおいて大きな信頼を勝ち取っています。ウィズセキュアはヨーロッパにおけるデータ保護の規制に準拠し、プライバシー、データ主権、コンプライアンスに注力しています。



当社は 35 年以上の経験を持ち、ユーザー企業の消極的／保守的なサイバーセキュリティ対策から積極的／先進的なアプローチへのパラダイムシフトのサポートのためのポートフォリオを持っています。ウィズセキュアはパートナーとの協力的な成長へのコミットメントに基づく柔軟な商業モデルを提供し、ダイナミックなサイバーセキュリティの世界において両者の成功を保証します。

ウィズセキュアの最先端のポートフォリオの中心となるのは、AI を搭載したテクノロジー、人の専門知識、コ・セキュリティ (共同セキュリティ) サービスをシームレスに統合する Elements Cloud です。さらに、エンドポイントおよびクラウドの保護、脅威の検出と対応、エクスポージャー管理にまたがるモジュール式の機能により、中堅・中小企業ユーザーのセキュリティ対策を強固なものとしします。

1988 年に設立されたウィズセキュア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。詳細は www.withsecure.com をご覧ください。また、X (旧 Twitter) アカウント @WithSecure_JP https://twitter.com/WithSecure_JP でも情報の発信をおこなっています。