報道関係者各位

ウィズセキュア、クラウドセキュリティの設定管理チェック機能をリリース

～ サイバー攻撃者が設定の不備を突く前にクラウドセキュリティの確保を ～

2023 年 5 月 24 日
ウィズセキュア株式会社

企業がインフラをクラウドサービスに移行する際、セキュリティの確保が万全でないことも珍しくはありません。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 (旧社名: F-Secure、本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウィズセキュア) は、攻撃者がクラウド設定の不備を突いてネットワークを侵害することを阻止するために、同社の WithSecure Elements セキュリティプラットフォームに新モジュールとなる『Cloud Security Posture Management』(以下、CSPM)を追加したことを発表しました。

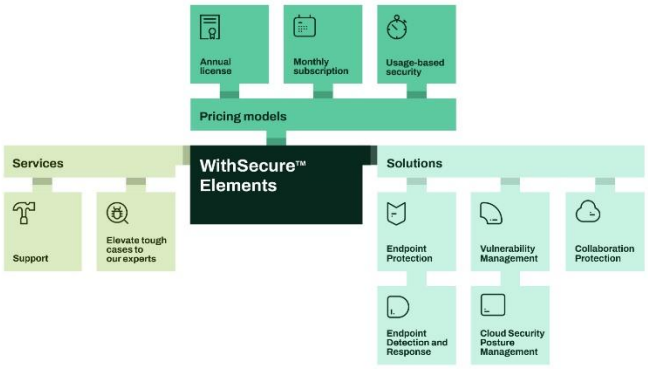
クラウドベースの IaaS (Infrastructure-as-a-Service = サービスとしてのインフラ) を企業の IT 資産に組み込むことは、今や一般的なものになっています。クラウドへの移行には多くのメリットがありますが、同時に、IaaS プラットフォームの急速な拡大、クラウドセキュリティにおけるスキルと経験を持つ専門家の不足、GDPR をはじめとした様々な規制、そして全体的な複雑さなどの新たな課題も出現してきます。多くの企業が複数のパブリッククラウドサービスプロバイダーを並行して利用していることもまた、クラウドインフラのセキュリティ確保の難しさに拍車をかけています。

ウィズセキュアでプロダクト部門長を務める Leszek Tasiemski (レシェック・タシエムスキー) はこうした状況を次のように解説しています。
「クラウドインフラのセキュリティ確保は、様々な理由により、非常に困難な作業となります。クラウドは通常、従来のインフラと比較して抽象化されたレイヤーを提供するため、従来のセキュリティとクラウド特有のセキュリティの両方において懸念が生じます。多くのユーザーにとって、自身とクラウドサービスプロバイダーのどちらがセキュリティのどの部分に責任を負うかという、責任共有モデルを正しく理解することは簡単ではありません。」

セキュリティ上の課題が積み重なると、重大な問題に発展する可能性があります。2022 年にウィズセキュアが実施したマーケットリサーチ*1 によると、過去 12 ヶ月間に 24%の企業が自社のクラウドプラットフォームに影響を与えるセキュリティの設定ミスを発見、そして約 34%の企業が設定ミス以外の脆弱性を発見していたことがわかりました。

Tasiemski はまた、こう付け加えています。
「Amazon の IMDSv1 のように、クラウドレイヤーに脆弱性があるケースもあります。サイバー犯罪者は小さな脆弱性をも探し当て、そこを突いてきます。私たちが日々ニュースで耳にするようなインシデントでは、こうした設定ミスが敵にうまく攻撃されることが増えてきています。」

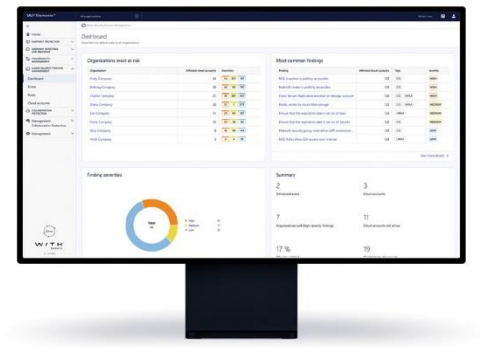
CSPM は、クラウドベースのセキュリティプラットフォームである WithSecure Elements の新モジュールであり、ユーザーは既存のエンドポイント保護 (EPP)、エンドポイントでの検知と対応 (EDR)、脆弱性管理、コラボレーション保護と同様に、必要な機能を柔軟に選択することができます。CSPM は一般的なクラウドベースの IaaS プラットフォームの脆弱性や設定ミスに関連するリスクを管理することを目的としており、AWS と Microsoft Azure のプラットフォームに対応しています。



(WithSecure Elements ポートフォリオ)

Cloud Security Posture Management の主なメリットは以下の通りです:

- リスクレベルに基づいて設定ミスを特定し、優先順位を付け、対策を添付して説明
- 設定は、必要以上に寛容な IAM 権限、暗号化されていない保存データ、パブリック IP アドレスにアクセスできるクラウドインスタンス、インシデント調査のためのロギングが有効かどうか、さらに既存のクラウドセキュリティ問題や新たなクラウドセキュリティ問題を確認
- ウィズセキュアのコンサルタントが持つ専門知識とリサーチ能力により、チェックが脅威モデルに適合し、ユーザーに真のセキュリティバリューを提供
- 専用ダッシュボードでは、セキュリティの状態の経年変化やセキュリティの状態に関する様々なインサイトなど、注意を払うべき重要情報をわかりやすいグラフで提供
- WithSecure Elements のエンドポイント保護 (EPP)、エンドポイントでの検知と対応 (EDR)、脆弱性管理、コラボレーション保護などのモジュールと共通のポータルで、マルチベンダーおよびマルチクラウドを管理
- CIS や NIST CSF などへの準拠を維持するのに役立つ、具体的なルールやフラグ立てを実行
- MSP や MSSP などのパートナーが、CSPM をマネージドサービスとして顧客に提供が可能



(管理ポータル)

WithSecure Elements Cloud Security Posture Management の詳細についてはこちらのページをご覧ください:
https://www.withsecure.com/en/solutions/software-and-services/elements-cloud-service-posture-management

*1: WithSecure 2022 B2B マーケットサーベイ。2022 年 5 月に 12 ヶ国 (日本／フィンランド／イギリス／フランス／ドイツ／ベルギー／オランダ／デンマーク／ノルウェー／スウェーデン／アメリカ／カナダ) で 3,072 人を対象にオンラインによる調査を実施。回答者は、IT／クラウド／ネットワークセキュリティの製品およびサービスを導入する企業／団体内の IT 意思決定者／IT インフルエンサー／経営幹部である。

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、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検出し、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、Twitter @WithSecure_JP でも情報の発信をおこなっています。