Secureworks®

Secureworks Taegis IDR

ID侵害リスクを90秒未満で検知[1]し、IDを標的とする攻撃対象領域の最小化、また経時的な推移（ベンチマーク）を提供します。

Secureworksは、IDセキュリティ対策を回避する脅威に対する検知と対応の機能を提供し、MITRE ATT&CKの「認証情報アクセス」テクニックのすべてから組織を保護します[2]。組織のセキュリティ体制を強化するために設計されたアドオンであるTaegis™ IDRは、組織環境を常時モニタリングして設定ミスやリスクを特定するとともに、ダークウェブ等で侵害された認証情報のインテリジェンスを提供します。レガシーソリューションでは検知に数日を要するようなID侵害のリスクを90秒未満で検知1し、IDを標的とする攻撃対象領域の最小化、また長期的なベンチマークを提供します。

IDを標的とする攻撃対象領域の最小化

Microsoft Entra ID環境の95%で設定ミスが発生しています[3]。Taegis IDRは同様の環境を常時スキャンして、設定ミスやIDに関連するセキュリティギャップを特定し、リスクの優先付けを行います。適切な対策を講じない限り、サイバー犯罪者は上述のリスク露出を利用して権限昇格を行い、IDベースの攻撃を実行します。Taegis IDRのIdentity Posture Dashboardを活用すれば、セキュリティチームは条件付きアクセスポリシー、ユーザーに関連付けられていないアカウント、過度の権限が付与されたアカウント、高リスクのアプリケーションなどから生じるギャップにすばやく対処できます。

認証情報の漏洩や窃取のリスクを低減

Secureworksが実施した調査より、ダークウェブの某マーケットプレイスにて窃取された認証情報の販売件数が過去3年で688%増加したことが明らかになりました[4]。Taegis IDRは認証情報の漏洩を監視してアラート化するため、セキュリティチームは、窃取された認証情報を悪用した攻撃で被害が生じるリスクを大幅に低減できます。Taegis IDRはユーザーによる高リスクな行動を特定し、窃取または侵害された認証情報を悪用したシステムへのアクセスを監視しつつ、予期しない場所からのログインなどの異常なログインパターンを検知します。

導入のメリット

Microsoft Entra IDにおける露出リスクを90秒未満で検知[1]し、IDを標的とする攻撃対象領域を縮小

ダークウェブをスキャンして認証情報の漏洩を監視し、データ侵害によりログイン認証情報が公開された場合にアラート化

ユーザーによる高リスクな行動を特定し、窃取された認証情報に関連する異常なアクティビティを検知

システム全体にわたって**IDに関する情報を迅速かつ包括的に可視化**し、効果的なリスクへの対処を支援

MITRE ATT&CKの「認証情報アクセス」テクニックのすべてを検知[2]し、自動化されたプレイブックにより脅威の対応を迅速化

ID環境の包括的な可視化

システム全体におけるID情報を迅速かつ包括的に可視化し、安全なID管理を実現。ユーザー、グループ、デバイス、アプリケーションの全体を把握し、ID環境における変化をモニタリングできます。すべてのIDに対して効果的な対策を講じることで、リスクを攻撃者に悪用される前に修正し、緊急度の高いリスクを解消できます。Taegis IDRはTaegis XDRプラットフォームで一元的に管理できるため、ID、エンドポイント、ネットワーク、クラウド、Eメール、その他のビジネスシステム全体を包括的に保護できます。

IDに関する脅威への保護

昨年、90%の組織がID侵害を受けています[5]。Taegisは、IDベースの脅威に対する検知、優先順位付け、対応を自動的に実行し、脅威によるビジネスへの被害を未然に防止します。Secureworksのソリューションを導入することで、Kerberoasting攻撃、パスワードスプレー攻撃、総当たり攻撃などの高度な脅威を攻撃チェーンの早期段階で検知します。また自動化された方法で迅速かつ正確に対応できます。セキュリティチームは導入後、簡単に自動化されたプレイブックによって対策を効率化し、ID侵害の発生時にユーザーの無効化、強制的なパスワードリセット、アカウントのロック、セッションの取り消しなどのアクションを即座に実行可能です。

> **Taegis IDRのID関連リスク可視性向上効果には感嘆しました。またID関連の情報をXDRポータル上で簡単に把握できるメリットは非常に大きいです。**
>
> **Richard Hay**氏、
> First Community Bank、
> 上級情報セキュリティ担当者

> **Taegis IDRによって、懸念していたAzureおよびMicrosoftのエコシステム領域のリスク（条件付きアクセスポリシーにおけるギャップや、安全性の低いアプリケーション、過度の権限が付与されていたアプリケーションなど）を可視化できるようになりました。**
>
> 上級情報セキュリティ担当者

1. Secureworksの既存顧客のデータに基づいてIDの露出の検知に要する平均時間を算出
2. MITRE ATT&CKフレームワークにマッピングされたTaegisの検知性能に基づく
3. SecureworksのCounter Threat Unit™（CTU™）が実施した数千件のインシデント対応から収集されたデータに基づく
4. Secureworks CTUが社内で収集したデータに基づく
5. Identity Defined Security Alliance（IDSA）、『2023 Trends in Securing Digital Identities』、2023年7月

Secureworks®

Secureworks（NASDAQ：SCWX）は、サイバーセキュリティのグローバルリーダーです。20年以上におよび蓄積してきた、実環境からの検知データ、セキュリティ運用に関する専門知識、脅威インテリジェンスおよび脅威のリサーチを基盤とする、SaaSベースのオープンXDRプラットフォーム「Secureworks®Taegis™」を通じて、全世界のお客様を保護しています。Taegisは世界各地の数千の組織のセキュリティ運用に利用されています。AIを活用するTaegisの先進的な機能を利用することで、組織は高度な脅威の検知、調査における効率性とチーム間の連携の強化、的確な対策アクションの自動化を推進しています。

詳細につきましては、**03-4400-9373**、またはsecureworks.jpをご覧ください。