CISCO DUO

アイデンティティセキュリティプログラムの構築

CISO 向けブループリント

Matt Caulfield
Cisco Duo 製品担当 VP

はじめに

Duo の『アイデンティティ セキュリティ プログラムの構築』ブループリントは、組織のアイデンティティを保護し、アカウントの乗っ取りを防ぐための究極のガイドです。

アイデンティティ セキュリティ プログラムを構築するのは大変なことに思えるかもしれません。「優れたプログラム」の基準がよくわからない場合はなおさらです。ですが、案ずることはありません。このブループリントでは、実践的なガイダンスを提供し、成功するプログラムの概要を説明します。

多要素認証（MFA）からシングルサインオン（SSO）、リスクベースの認証（RBA）、アイデンティティ セキュリティ態勢管理（ISPM）、アイデンティティ脅威の検出と対応（ITDR）まで、今話題の用語をすべて取り上げています。といっても、いわゆる BDIAH（略語地獄にはまるという意味の「Bogged Down In Acronym Hell」の頭文字）にならないようにわかりやすく説明するのでご安心ください。

組織によって状況が異なることを念頭に置きながら、できる限り有益なガイドになるよう工夫しています。そのため、アイデンティティ セキュリティにアプローチするうえでの定義、フレームワーク、いくつかの推奨事項も盛り込みました。

組織によって事情は異なるため、本ガイドがあらゆるケースに対応できる万能のソリューションでないことは承知しています。むしろ、興味のある内容を選んで目を通していただければ幸いです。最初から読み進めていくのではなく、ご自身や所属されている組織にとって最も重要なセクションを中心に読むことができます。

では早速、従業員のアイデンティティを保護して組織を安全に保つために、アイデンティティ セキュリティ プログラムの構築を開始しましょう。

エグゼクティブサマリー

アイデンティティ セキュリティはテレワークと SaaS が普及した今の時代には不可欠なものであり、アイデンティティ セキュリティのハイジーン（衛生管理）が十分でない場合、企業はサイバー攻撃による被害を受けやすくなります。それなのに多くの組織は、効果的なアイデンティティ セキュリティ プログラムに何が必要かを理解するのに苦労しています。本書では、目標の調整、能力の構築、主要な成果に焦点を当てた実践的なガイダンスを提供します。

ユーザー管理、アクセス管理、認証、アイデンティティ脅威の検出と対応など、アイデンティティ セキュリティの最も重要な領域に関するアドバイスをご紹介するものです。アイデンティティ セキュリティに投資する際のビジネス推進要因には、侵害の防止、コンプライアンスの向上、サードパーティリスクの管理、業務効率の向上、従業員の満足度の向上などがあります。

アイデンティティ セキュリティ プログラムの構築

目次

はじめに ____ 2

エグゼクティブサマリー ____ 2

01 アイデンティティ セキュリティの定義 ____ 4

アイデンティティは新たなファイアウォール ____ 5

セキュリティチームと IAM チームの分断 ____ 6

アイデンティティ セキュリティの定義 ____ 7

02 アイデンティティ セキュリティの 4 つの柱 ____ 8

識別 ____ 9

保護 ____ 16

検出 ____ 25

対応 ____ 31

03 主要な関係者と責任 ____ 34

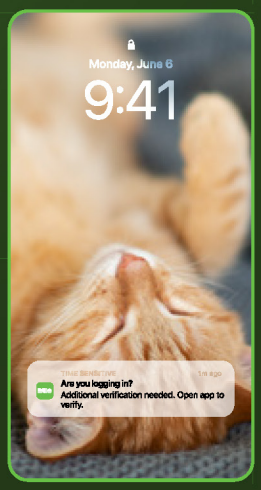
主要な関係者 ____ 35

アイデンティティ セキュリティにおける責任 ____ 38

04 主なビジネス成果 ____ 39

05 重要業績評価指標 ____ 41

まとめ ____ 44



01

アイデンティティセキュリティの定義

アイデンティティは新たなファイアウォール

ここ数年「アイデンティティは新たなファイアウォール」という言葉をよく耳にします。しかし、これは何を意味するのでしょうか。

サイバーセキュリティに対する従来型のアプローチは、ファイアウォールや侵入検知システムなどのセキュリティテクノロジーを活用して、組織のネットワークの周囲に「境界」を構築するというものでした。このアプローチは、内部ネットワークと外部世界の間に強力なバリアを作成すれば脅威を阻止できるという前提に基づいています。

ところが、組織がデータとアプリケーションをクラウドに移行したことにより、従業員はさまざまなデバイスを使ってどこからでもアクセスできるようになったため、このアプローチの効果はどんどん薄れてきています。この新しい環境では、境界は穴だらけで、脅威は検出されずに簡単にすり抜けてしまいます。

攻撃者は、システムをハッキングすることよりも、システムにログインすることに力を入れるようになっている。

アイデンティティは、セキュリティチームが以前のネットワークセキュリティで実現していた可視性を取り戻すための唯一の方法です。さらに、新たなファイアウォールとしてアイデンティティに焦点を当てることで、脅威を排除することに依存するセキュリティ態勢から、脅威が侵入することを想定して被害を制限することに重点を置くセキュリティ態勢に移行できます。

アイデンティティベースのセキュリティとは、組織のリソースにアクセスするすべてのユーザー、デバイス、アプリケーションが、アイデンティティに基づいて認証および承認されることを意味します。こうすることで、攻撃者がユーザーのログイン情報にアクセスした場合や、デバイスが侵害された場合でも、権限とポリシーに基づいてアクセスを制限できます。

© 2024 Cisco and/or its affiliates. All rights reserved.

セキュリティチームと IAM チームの分断

アイデンティティ セキュリティ プログラムの成功にとって障害となる理由

アイデンティティは企業のセキュリティにとって重要であり、テレワークとクラウドベースのツールへの移行によって、その重要性は高まる一方です。しかし、セキュリティチームと IAM チームの間には往々にして大きなギャップが存在し、アイデンティティ セキュリティ プログラムを成功させるうえで障害となります。

攻撃者は長年にわたってアイデンティティを標的とした攻撃を展開しており、Active Directory（AD）が攻撃対象になることも少なくありません。セキュリティチームは AD ベースの攻撃の可視性を高めていますが、IT チームと IAM チームが他にも多数のアイデンティティツールを導入しており、そのほとんどがクラウドベースです。

多くの場合、これらのプラットフォームはセキュリティチームにとって大きな盲点となります。Identity Defined Security Alliance（IDSA）によると、ワークフォース IAM の所有権を持っているセキュリティ専門家は 53% にすぎません。[1]

アイデンティティとセキュリティの統合は進んでいますが、セキュリティチームはいまだに IAM チームから独立して機能しています。

IDSA のホワイトペーパー『セキュリティチームはリスクにどのように対処しているか』（原題：How Security Teams Are Addressing Risk）によると、こうした分断が生じる理由として、セキュリティチームと組織の目標が一致していない（33%）、報告体制が整っていない（30%）、セキュリティチームはこれまで関与してこなかった（30%）、他のチームからの抵抗がある（24%）などが挙げられています。[2]

分断に対処するには、共同のアイデンティティ インシデント対応計画、文書化されたアクセスポリシーの共有、ポリシーの適用を証明するレポートが必要です。セキュリティチームは、IAM の重要性とその導入についてのベストプラクティスを理解する必要があります。一方 IAM チームは、セキュリティを優先し、セキュリティチームと緊密に連携して、組織の全体的なセキュリティ態勢を管理する必要があります。

注釈：

1. Identity and Access Management: The Stakeholder Perspective、Identity Defined Security Alliance

2. How Security Teams are Addressing Risk、Identity Defined Security Alliance

© 2024 Cisco and/or its affiliates. All rights reserved.

アイデンティティ セキュリティの定義

効果的なアイデンティティ セキュリティ プログラムの構築について説明する前に、まず「アイデンティティ」と「アイデンティティ セキュリティ」、その他関連する用語を定義しておきたいと思います。

ユーザー

組織のシステムやネットワークにアクセスする必要がある個人。

アカウント

組織のアイデンティティおよびアクセス管理システム内で作成される、ユーザー、サードパーティ、請負業者、およびマシンアカウントのデジタル表現。

アイデンティティ

組織のシステムとネットワークで、個人またはエンティティを識別するための情報。これには、ユーザー名、ロール、パスワード、アクセス権限、履歴コンテキストなどの属性が含まれる。

アイデンティティ セキュリティとは？

アイデンティティ セキュリティは、デジタルアイデンティティとそれに関連するアクセス権限を保護することに焦点を当てているため、組織のサイバーセキュリティ プログラムの重要な要素です。

ネットワーク、エンドポイント、電子メールセキュリティといった従来のセキュリティ領域が主にインフラストラクチャやデータを保護するのに対して、アイデンティティ セキュリティの保護対象は、インフラストラクチャとデータへのアクセス権を付与するアイデンティティです。

アイデンティティ セキュリティ

人間とマシンのアイデンティティの保護。ユーザーが本人であることと、権限を与えられた操作を行っていることを確認します。これには、承認されたユーザーのみが機密情報にアクセスできるようにし、攻撃者によってデータが侵害されないようにすることが含まれます。

© 2024 Cisco and/or its affiliates. All rights reserved.

02

アイデンティティセキュリティの4つの柱

01

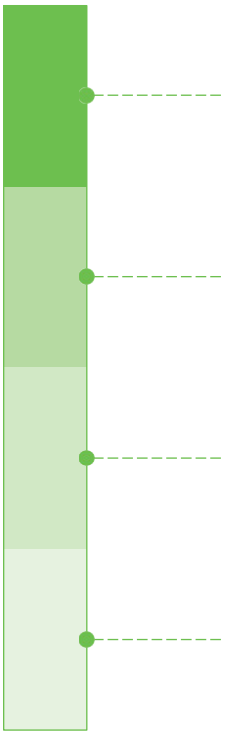
識別

把握していないものを保護することはできません。組織のアイデンティティ セキュリティ プログラムの最初のステップは、保護すべき対象を識別することです。

ユーザーとデバイスのインベントリの構築

ゼロトラスト セキュリティモデルを導入するうえで重要なのは、ユーザーが誰で、どのリソースにアクセスする必要があるかを把握することです。そのためには、正確なユーザーインベントリを構築する必要があります。Center for Internet Security（CIS）は、承認されたデバイスおよびユーザーと、承認されていないデバイスおよびユーザーの正確なインベントリを維持して、承認されたユーザーのみがシステムにアクセスできるようにすることも推奨しています。[3]正確なユーザーインベントリがなければ、セキュリティリスクを識別して軽減することは困難です。

ほとんどの場合、インベントリはまず表形式で提供されます。アイデンティティの包括的なリストは、通常 1 ~ 2 日で生成できます。インベントリの構築が進むにつれて、チームは検索可能なインベントリを作成し、孤立アカウントや非アクティブなアカウントの削除など、対象を絞ったアクションを実行できるようになります。最終的な目標は、インベントリをほぼリアルタイムで継続的に更新することです。これにより、チームはセキュリティとハイジーンの両方の問題を継続的にモニターできます。



レベル 3

セキュリティとハイジーンのアクティブなプロセスを使用したほぼリアルタイムのインベントリ。

レベル 2

孤立アカウントの削除など、対象を絞ったアクションを実行できる検索可能なインベントリ。

レベル 1

24 ~ 72 時間以内に表形式で生成される包括的なユーザーインベントリ。

レベル 0

一元化されたユーザーインベントリがない。

注釈：

3. CIS Critical Security Controls Version 8、Center for Internet Security

© 2024 Cisco and/or its affiliates. All rights reserved.

ユーザーとデバイスの完全なインベントリという課題

組織は、プラットフォーム間でユーザーデータを統合することでアイデンティティの統合ビューに影響が出てしまうという課題に直面しています。

- アイデンティティ プロバイダーは、属性やスキーマが異なるさまざまな形式でデータを保存しているため、システム間、特に人事ディレクトリとアイデンティティ プロバイダー間でのデータのマッピングと調整は容易ではありません。
- データ品質はさまざまですが、多くの場合、クラウドベースのアイデンティティ プロバイダーのデータに比べ、人事ディレクトリのデータのほうがより正確で最新です。このため、ユーザーアイデンティティの統合ビューを作成する際に不整合が発生してしまいます。
- 個人は企業データにアクセスできる複数のアカウント（Gmail、Yahoo など）を持っており、1 企業あたり平均 340.5 個の個人アカウントが存在します。[4] これらのアカウントは企業アカウントにリンクされています。

ユーザーインベントリの KPI

孤立アカウントの数

HRIS（人事情報システム）との不一致の数

一意でない ID や共有 ID の数

管理者アカウントの数

ゲストアクセス

Entra ID 内のゲストアカウントは、組織と協力するために招待された外部ユーザーのアイデンティティです。ゲストアカウントを組織に招待するには、ドキュメントへのリンクを送信したり、Teams で外部の電子メールアドレスにメッセージを送信したりするだけで済みます。

ゲストアカウントは、Office 365 でのコラボレーションとアクセス管理に不可欠ですが、データ損失やデータ漏洩の主要なリスクにもなります。たとえば解雇されると思っている従業員が、報復として、個人の Gmail や Microsoft クラウドアカウントで情報を共有する可能性があります。

注釈：

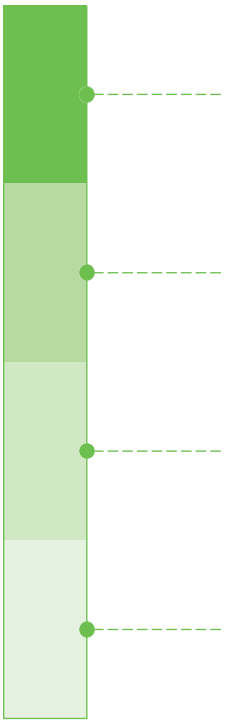
4. State of Identity Security research reveals 40% of accounts use weak or no form of multi-factor authentication to protect identities、Oort

© 2024 Cisco and/or its affiliates. All rights reserved.

組織には少なくとも、ゲストアカウントの管理、ゲストアカウントの定期的な確認、非アクティブまたは不要なゲストアカウントの削除についてのポリシーが必要です。

このプロセスは自動化することができ、ゲストアカウントに MFA など追加の制御を適用することも可能です。

最終的に、組織はゲストアカウントを完全に追跡、モニタリングし、不審なアクティビティを検出できるレベルに到達することを目指す必要があります。まもなく退職する従業員が個人アカウントを招待するといったことも不審なアクティビティに該当します。



レベル 3

ゲストアカウントの追跡、モニタリング、脅威検出（自己招待を含む）。

レベル 2

招待、削除、アクティビティのモニタリングの自動化とゲストアカウントへの MFA の適用。

レベル 1

ゲストアカウントのポリシーベースの管理（非アクティブアカウントの確認と再評価を含む）。

レベル 0

ゲストアカウントを管理するプロセスが定義されていない。

ゲストアカウントを管理するためのチェックリスト

ポリシーの策定

何か別のことを始める場合もそうですが、まずは適切なレベルのポリシーを検討します。これについては、業界の規制で定められていることもあります。ポリシーに関する重要な考慮事項としては次のようなものがあります。

- **あまりにも制約事項の多いポリシーは逆効果になる可能性がある。**非常に制約の厳しいポリシーを導入する前に、他の方法でコンテンツを共有しようとする人が現れる可能性を考慮する必要があります。独自に考えた方法は、ゲストアカウントに比べて規制するのが簡単ではないかもしれません。
- **招待プロセス。**まず、招待プロセスの仕組み、招待できる人、招待できる期間、招待するコンテンツの種類に関するプロセスを策定します。
- **招待の追跡。**招待の有効期限を設定し、現在のアクセスレビュープロセスにリンクします。

© 2024 Cisco and/or its affiliates. All rights reserved.

- **アトリビューションの管理。**ユーザーを招待した人への明確なリンクを維持し、個人的な招待や、招待した人が退職したときの対処方法に関するポリシーを設定します。
- **双方向ビューの取得。**a）ユーザーが誰を招待したのか、b）誰が招待の所有者なのかを双方向で確認できるようにします。これにより、組織内の担当者がそれらのアクションに対して責任を負うことになります。

確認および削除

- **定期的な削除。**組織はデータの損失と漏洩を減らすために、ゲストアカウントを定期的に削除する必要があります。
- **招待。**承諾されていない招待や、1 週間経過しても放置されている招待を削除します。

多要素認証

- **多要素認証の設定。**ゲストアカウントに多要素認証を設定することで、適切なユーザーが適切な情報にアクセスできるようになるため、アイデンティティ盗難のリスクを減らすことができます。
- **ゲストアカウントの MFA はアクセスを許可するデータにリンクする。**内部的に規制および管理されているデータに外部ユーザーが MFA を使用してアクセスするのは望ましくありません。

ゲスト権限の制限

- **計画的に実施する。**企業データへの不正アクセスのリスクを軽減するために、ゲストユーザーの権限を制限する必要があります。
- **アプリケーションポリシー。**非特権ユーザーにサードパーティ製アプリケーションの登録を許可してはいけません。
- **既存の保護対策を活用する。**AAD グループ機能へのユーザーアクセスを制限するには、アクセスパネルのグループ機能にアクセスするユーザー機能を制限する設定を有効にする必要があります。

ゲストアクセスの KPI

非アクティブなゲストアカウントの数

孤立ゲストアカウントの数

過剰にアクセスしているゲストアカウントの数

© 2024 Cisco and/or its affiliates. All rights reserved.

マシンのアイデンティティ

人間のユーザーだけでなく、マシンにもアイデンティティの追跡が必要となるロールや機能があります。適切なユーザー管理により、組織はマシンのアイデンティティとそれに関連するアクセス権限を特定して管理できます。

人間以外のアイデンティティには、人間から一歩離れたすべてのアカウントが含まれます。たとえば、共有メールボックス、サービスアカウント、ネットワークデバイスが挙げられます。

43%

マシンのアイデンティティは、平均的な企業内の全アイデンティティの 43% を占める。[5]

マシンのアイデンティティとして最もよく知られているのはサービスアカウントです。サービスアカウントは通常、特定のアプリケーションやサービスに対応するために作成され、さまざまなシステムにまたがって存在することがあるため、追跡して管理するのが困難です。

さらに、サービスアカウントに特権がある場合は機密リソースにアクセスできるため、潜在的な攻撃者の格好の標的となります。サービスアカウントは複数のユーザーやアプリケーションで共有されることもあり、その結果、シナリオが複雑になり、セキュリティリスクが高まります。

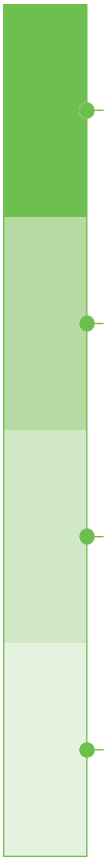
最も重要なのは、明確なプロセスの設定から始めることです。このプロセスでは、すべてのサービスアカウントが 1 人にリンクされるようにします。つまり、「責任の所在」が 1 つになります。理想的には、誰かが退職した場合に備えて、アカウントを複数の人間に紐付けておくとよいでしょう。また、所有権を移行するための標準的なプロセスを用意し、チームはそれに従うようにしましょう。

注釈：

5. Machines make up 43% of digital identities on enterprise networks、Security Magazine

© 2024 Cisco and/or its affiliates. All rights reserved.

このプロセスが成熟するにつれて、サービスアカウントの作成と廃止を自動化し、ユーザーインベントリに反映されるようにすることができます。最終的には、ジャストインタイムのプロビジョニングの使用や、1 回限りのタスクに使用できるエフェメラル サービス アカウントの導入を検討するとよいでしょう。



レベル 3

エフェメラル サービス アカウントの自動作成、JIT プロビジョニング、ロギング。

レベル 2

サービスアカウントの作成と廃止の自動化、インベントリへの反映。

レベル 1

所有権の移行を含む、サービスアカウントを管理するためのプロセス（書類作業）。

レベル 0

マシンのアイデンティティを管理するためのプロセスが定義されていない。

マシンのアイデンティティの KPI

所有者が不明なサービスアカウントの数

デフォルトのパスワードを使用しているサービスアカウントの数

キーが期限切れになったサービスアカウントの数

© 2024 Cisco and/or its affiliates. All rights reserved.

アイデンティティからデバイスへのマッピング

ユーザーがログインしているデバイスをマッピングすることで、セキュリティチームは、管理対象外のデバイスからのアクセスなのか、既知のデバイスからのアクセスなのかを識別できます。これにより、チームは機密データや資産への不正アクセスを防止できます。デバイス信頼ポリシーは、従業員が個人のデバイスを使用して会社のリソースにアクセスすることがあるテレワークの時代では特に重要です。ゼロトラスト セキュリティポリシーを適用することで、セキュリティチームは本人確認に基づいてアクセスを許可する前に、すべてのアクセス要求が認証および承認されるようにすることができます。

さらに、デバイスをマッピングすることで、組織は安全な BYOD ポリシーを作成できます。機密データや資産へのアクセスを許可する前にデバイスのセキュリティ要件を指定することで、セキュリティチームは信頼できるデバイスのみにアクセスを許可することができます。加えて、アイデンティティ ファブリックは、デバイスが指定のセキュリティ要件を順守しているかどうかを追跡し、デバイスが順守していない場合はアクセスを取り消すことができます。

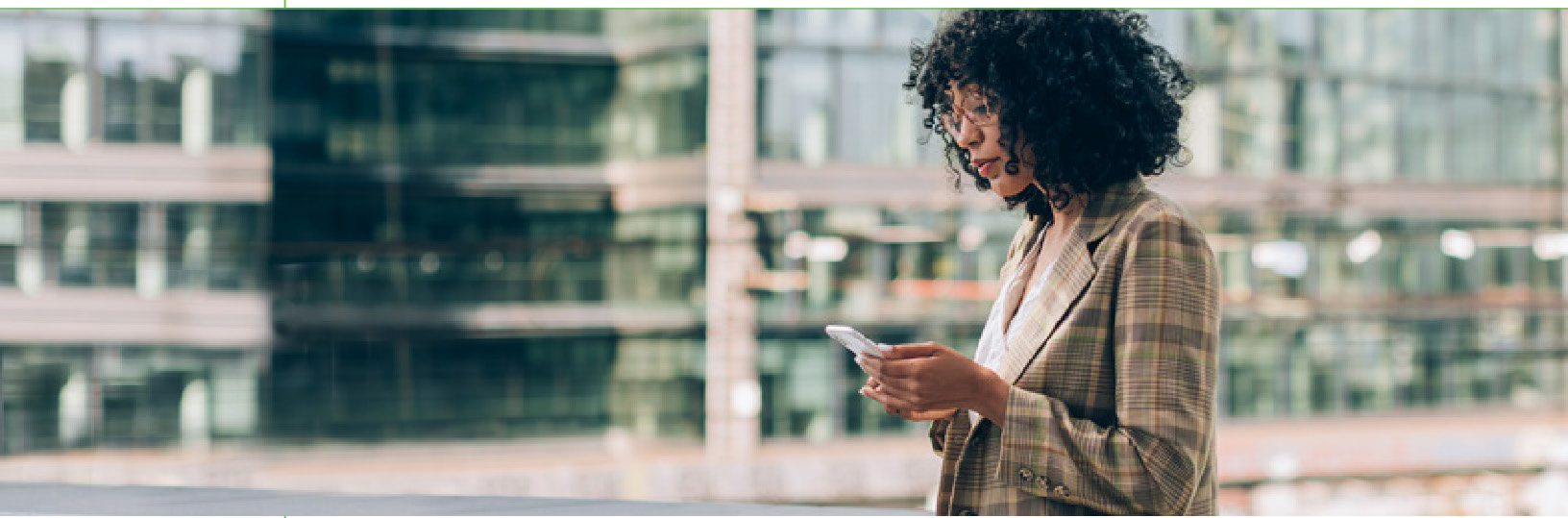
ハイジーンに関する考慮事項

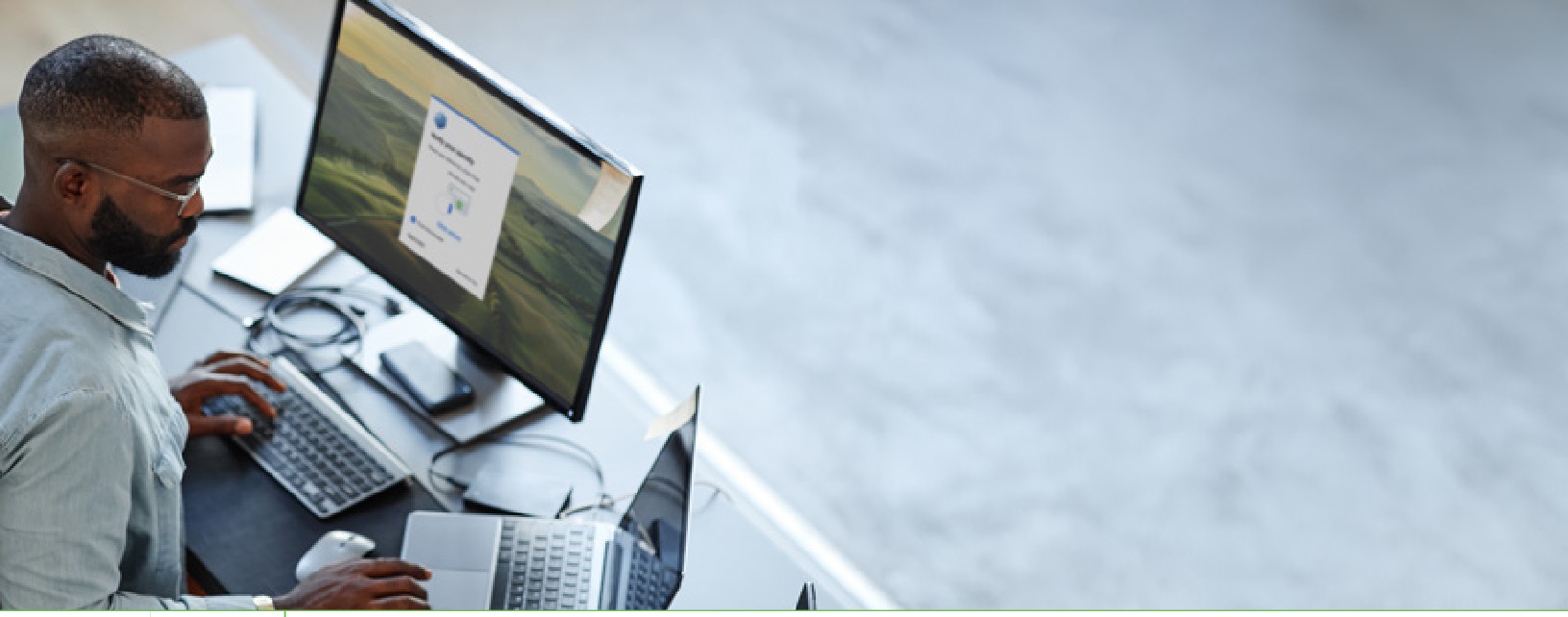
効果的なユーザーインベントリを維持するには、アイデンティティの不一致とハイジーンを常に把握することが重要です。そのためには、ユーザーについて、またさまざまなシステムやアプリケーションに対するユーザーのアクセス権について、正確で最新の情報を維持する必要があります。

アイデンティティの不一致やハイジーンの管理に不備があると、セキュリティ侵害、不正アクセス、その他のセキュリティリスクにつながる可能性があります。

IGA プロジェクトと PAM プロジェクトにとっても、IAM ハイジーンの強化は重要です。IAM の基盤に欠陥があると、プロジェクトの成功はとても見込めません。たとえば IAM システム内に休眠アカウントや孤立アカウントが多数ある場合、IGA プロジェクトと PAM プロジェクトでユーザーアクセスを正確かつ包括的に可視化し制御するのに苦労することになります。

IAM ハイジーンが十分でなければ、IGA プロジェクトと PAM プロジェクトで、ユーザーアクセスに対する正確で包括的な可視性と制御を実現するのは難しくなるでしょう。





02

保護

識別に続く次のステップは、アイデンティティの保護です。アイデンティティ セキュリティ戦略では、入社したユーザー、異動するユーザー、退職するユーザーを扱うプロセスで重要な要素を考慮する必要があります。

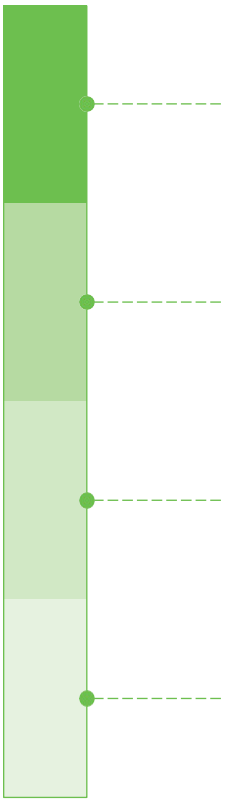
オンボーディングと移行

オンボーディングと移行とは、業務に必要なリソースとシステムへのアクセス権を新入社員に付与し、その権限（エンタイトルメント）が社員の職務に適していることを確認するプロセスのことです。オンボーディングプロセスは、攻撃者にとって最大のチャンスにもなります。このプロセスは、フィッシング、ソーシャルエンジニアリング、ブルートフォース攻撃などの攻撃に対して脆弱です。この段階でアカウントに不正アクセスされると、独自の形式の MFA が登録される可能性があります。

そのため、ディレクトリなどの IT システムへのオンボーディングだけでなく、MFA などのセキュリティ管理へのオンボーディングについても、登録ワークフローの保護は欠かせません。本人確認（ユーザーが本人であることを最初に確認すること）は、このプロセスの要です。しかし、講じるべき策は他にもあります。オンボーディングの一環としてバイパスコードの使用を制限する、部分的な登録をモニタリングする、登録プロセス中に不審なアクティビティがないかを評価するなどの対策も、オンボーディングのセキュリティ強化に役立ちます。

アクセス管理によって、このプロセスを合理化し、新入社員に必要なアクセス権を迅速かつ効率的に付与できます。オンボーディングプロセスを自動化することで、企業は新入社員の生産性を初日から確保し、不正アクセスやデータ侵害のリスクを軽減できます。

© 2024 Cisco and/or its affiliates. All rights reserved.



レベル 3

モニタリングとアラートの受信、コンプライアンスの確保、セルフサービス機能の有効化。

レベル 2

オンボーディングとプロビジョニングの手順の自動化による効率向上。

レベル 1

プロセスの確立、すべてのロールのワークフローの明示。

レベル 0

オンボーディングのプロセスが定義されていない。

エンタイトルメント

エンタイトルメントとは、特定のリソース、システム、データにアクセスするためにユーザーに付与される特定の権限と特権のことです。アクセス管理により、各ユーザーには職務を遂行するために必要なエンタイトルメントのみが付与され、それ以上のエンタイトルメントは付与されないようにすることができます。

エンタイトルメントは、組織のクラウド インフラストラクチャ内のユーザーまたはユーザーグループに適用されます。アプリケーションとエンタイトルメントへのアクセスは、直接の割り当てではなく、グループメンバーシップを通じて行う必要があります。組織が成熟するにつれて、これらのグループメンバーシップは人事ロールのニーズに基づいて自動化できます。適切なエンタイトルメントを設定したら、アクセスポリシーにもグループのエンタイトルメントを反映する必要があります。

オンボーディングの KPI

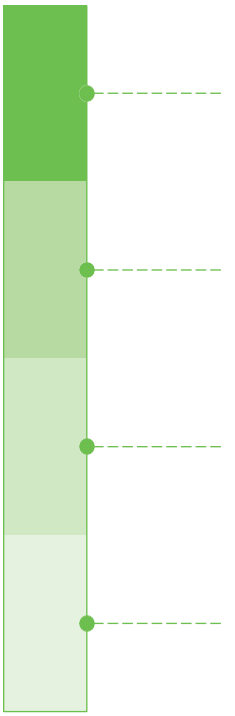
新入社員のオンボーディングが完了するまでのスピード

過剰なアクセス権を持つユーザーの数

© 2024 Cisco and/or its affiliates. All rights reserved.

オフボーディングとプロビジョニング解除

オフボーディングとプロビジョニング解除とは、従業員が退職したり役割が変わったりしたときに、リソース、システム、データへのアクセス権を削除するプロセスを指します。アクセス管理は、このプロセスを自動化し、アクセスを迅速かつ完全に取り消すのに役立ちます。これにより、すでに退職した元従業員が機密データやシステムにアクセスするリスクを軽減できます。オフボーディングプロセスを自動化すれば、組織はアクセスを迅速に取り消すことができ、データ侵害のリスクを軽減できます。



レベル 3

モニタリング、アラートの受信、コンプライアンスの確保、自動化システムとの統合。

レベル 2

オフボーディングとプロビジョニング解除の手順の自動化による効率向上。

レベル 1

プロセスの確立、ワークフローの明示、すべてのロールと人員に対応。

レベル 0

オフボーディングとプロビジョニング解除のプロセスが定義されていない。

オフボーディングの KPI

SLA 内で無効になっている退職したユーザーのアカウントの割合

© 2024 Cisco and/or its affiliates. All rights reserved.

シングルサインオン

ログイン情報のハイジーンとは、適切なパスワード管理を習慣にし、サイバー脅威から機密情報を保護することです。この問題を解決するのがシングルサインオン（SSO）です。ユーザーは一度の認証で複数のシステムやアプリケーションにアクセスでき、ログイン情報を何度も入力する必要がなくなります。SSO を使用すると、ユーザーは複数のユーザー名とパスワードを覚えなくてもよくなります。また、さまざまなシステムにアクセスするための時間と労力が削減され、生産性が向上します。これは、クレデンシャル スタッフィング攻撃や他のパスワードベースの攻撃を防ぐのに役立ちます。

SSO ツールを使用して、オンボーディングとプロビジョニング解除の負担を軽減することもできます。SSO 機能は人事ディレクトリに基づいて自動的に提供され、すべてを一元的に管理します。

同時に、SSO の重要性が高まるにつれて、適切にモニタリングされなければ、SSO 自体が単一障害点になりかねません。最も成熟した SSO の導入では、SSO はファイアウォールのような扱いとなり、イベントデータを把握して追跡します。

なお、多くのアプリケーション プロバイダーの場合、SSO 機能を有効化するには追加料金を支払う必要があります。シスコとしては、こうした「SSO 課税」のようなやり方は好ましくないと考えており、カスタマーサポートに問い合わせる価値があるのではないかと思います。

© 2024 Cisco and/or its affiliates. All rights reserved.

セッションの長さの要件

より高度な SSO の導入では、セッションの長さの要件の調整に重点を置く必要があります。これは、ユーザーが認証された状態を維持できる時間を決定するルールです。この時間を過ぎると自動的にログアウトされます。これらの要件は、ユーザーがコンピュータから離れた場合、デバイスが盗難または紛失に遭った場合、またはセッションがハイジャックされた場合に、機密データやリソースへの不正アクセスのリスクを軽減するのに役立ちます。

セッションの長さの要件は、キオスクや公共のコンピュータなど、複数の人が共有のコンピュータやデバイスを使用する状況において不可欠なセキュリティ管理です。セッションの長さの要件は、一定期間操作がなかった場合にユーザーを自動的にログアウトさせることで、機密データやリソースへの不正アクセスを防止するのに役立ちます。

なお、アイデンティティデータを評価する（つまり、前のセクションで取り上げた「識別」のステップを構築する）ことで、信頼できるシナリオではセッションの長さを延長することも可能なはずです。ユーザーが常に同じ場所から、同じ信頼できるデバイスでアクセスしている場合、ユーザーの負担を減らしてアクセスを迅速化できます。セキュリティによって成果がもたらされるのです。誰が想像したでしょうか。

セッションハイジャック攻撃では、通常はセッショントークンのために管理される Web セッション制御メカニズムが悪用されます。[6]

注釈：

6. Session hijacking attack、OWASP

SSO の KPI

SSO を使用しているビジネスアプリケーションの数

パスワードの複雑さ

過去 30 日間にパスワードが更新されたアカウントの割合

ダイレクトアクセスが許可されたアプリケーションの数

© 2024 Cisco and/or its affiliates. All rights reserved.

多要素認証

多要素認証（MFA）は、本人であることを証明するために 2 種類以上の認証要素を提供することをユーザーに要求するセキュリティメカニズムです。認証要素とは、ユーザーが知っているもの（パスワードなど）、ユーザーが持っているもの（トークンなど）、ユーザーが本人であることを示すもの（指紋など）です。

MFA には、ユーザー名とパスワード以外に追加のセキュリティレイヤが備わっています。攻撃者がユーザーのパスワードを入手できたとしても、機密データやリソースにアクセスするにはユーザーの他の認証要素にアクセスする必要があります。

40.20%

強力な MFA が有効になっていないアカウントの割合。平均的な企業におけるアイデンティティ セキュリティの状況（Oort による調査）[7]

多くのフレームワークでは「異なるタイプの 2 つ以上の認証要素」が必要ですが、すべての要素が同じように有効とは限りません。残念ながら、SMS や電子メール OTP（ワンタイムパスワード）のような既存の第 2 要素の多くは、フィッシングなどの攻撃を受けやすくなっています。40% 以上のアカウントでは、強力な MFA が有効になっていません。

MFA 要素の強度

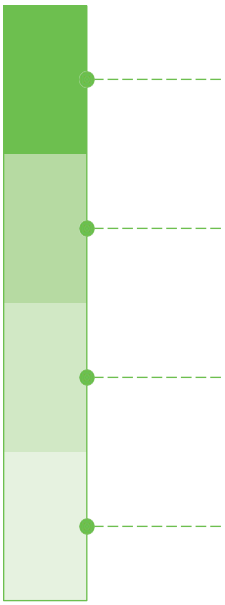
最低でも、100% のユーザーが暗号化された安全な MFA を使用できるようにしなければなりません。例外が存在する場合は、ポリシーに明確に記載し、包括的なカバレッジについても説明する必要があります。

注釈：

7. State of Identity Security、Oort

© 2024 Cisco and/or its affiliates. All rights reserved.

より成熟した組織では、フィッシング耐性のある MFA を実現し、MFA のアクティビティをモニタリングする計画があります。また、MFA フラッディングなどの MFA の脅威を検出するルールを少なくとも 1 つ作成します。最も成熟した組織では、最終的にはパスワードレス MFA を導入し、リカバリプロセスを定義してトラッキングします。



レベル 3

パスワードレス MFA ポリシー、リカバリプロセスのモニタリングとトラッキング。

レベル 2

フィッシング耐性のある MFA の計画、アクティビティのモニタリング、MFA ベースの脅威検出。

レベル 1

明確な例外ポリシーがある、100% 暗号化された安全な MFA。

レベル 0

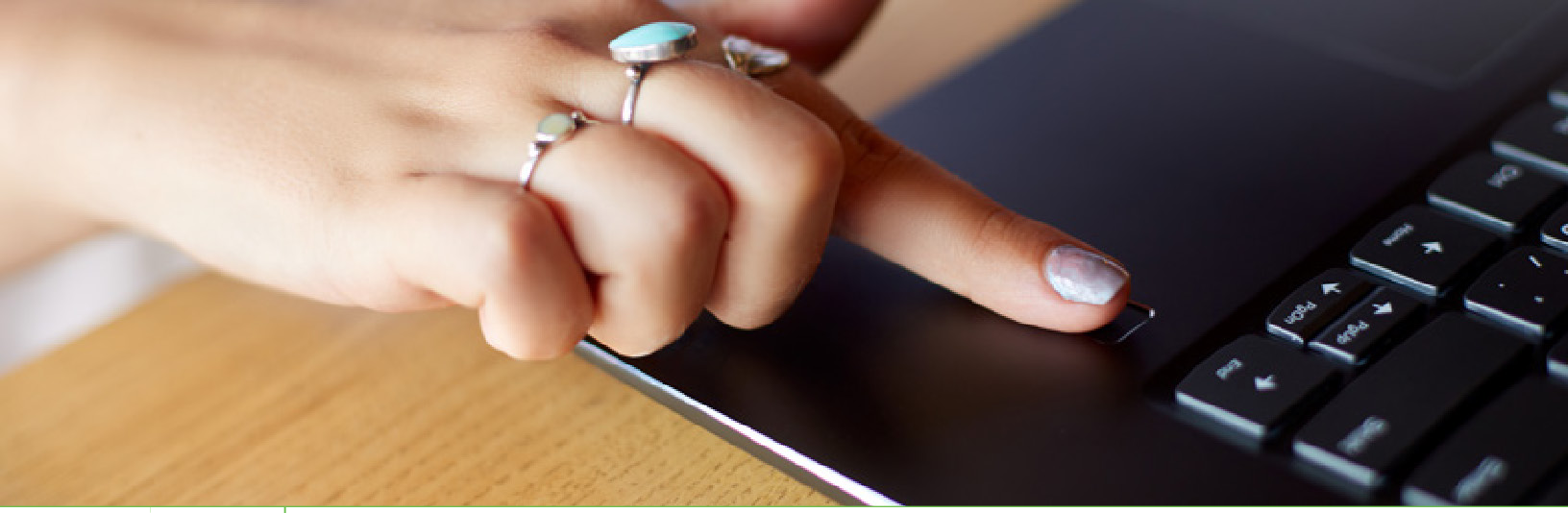
MFA が導入されていない、または限定的である。

MFA の KPI

多要素認証の使用が設定されているユーザーアカウントの割合

強力な MFA を使用しているユーザーアカウントの割合

© 2024 Cisco and/or its affiliates. All rights reserved.



アクセスポリシー

多要素認証（MFA）は、本人であることを証明するために 2 種類以上の認証要素を提供することをユーザーに要求するセキュリティメカニズムです。認証要素とは、ユーザーが知っているもの（パスワードなど）、ユーザーが持っているもの（トークンなど）、ユーザーが本人であることを示すもの（指紋など）です。

MFA には、ユーザー名とパスワード以外に追加のセキュリティレイヤが備わっています。攻撃者がユーザーのパスワードを入手できたとしても、機密データやリソースにアクセスするにはユーザーの他の認証要素にアクセスする必要があります。

場所または IP ポリシー

望ましくないアクセスを防ぐ有効な方法の 1 つとして、事業を行っている場所や IP 範囲へのアクセスを制限することが挙げられます。従業員が米国とカナダにしかいない場合は、会社のリソースへのアクセスをこの 2 か国に制限するとよいでしょう。そうすれば、攻撃者が従業員になりすまして信頼できる地域以外から会社のネットワークにアクセスしようとしても、ブロックできます。

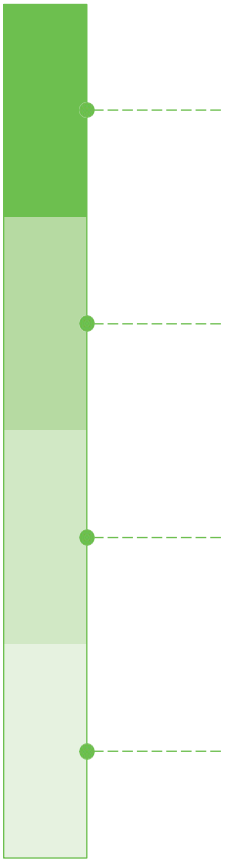
また、「既知の不正な」IP（攻撃者や攻撃手法に関連付けられた IP アドレス）のリストを保持し、リストアップされた IP をブロックするのも有効です。この場合、既知の不正な IP のリストを最新の状態に保つという、かなり先回りの作業を行う手間が発生します。しかし、これでハッキングやエクスプロイトの最近の状況を常に把握できるので、いずれにせよ有意義なことです。

デバイス信頼ポリシー

信頼できるデバイスからしか会社のリソースにはアクセスできないようにすれば、ログイン情報の侵害をしっかりと防止できます。攻撃者がユーザー名、パスワード、さらには MFA コードまで盗んでアクセスしようとしたとしても、使用しているデバイスが正しいものでない場合や認識済みのものでない場合はブロックされます。環境内のすべてのデバイスを管理しない限り、この種のポリシーを適用するのは難しいと感じられるかもしれませんし、セキュリティを非常に重視している企業の場合は、管理対象デバイスのみを許可するほうがよいのかもしれません。ただし今は、多くのアイデンティティ プロバイダーが、やや軽量なデバイス管理機能を提供しており、エンドユーザーがユーザーディレクトリに自分のデバイスを「登録」できるようになっています。この登録を行うと、ディレクトリがユーザーのアイデンティティを信頼できるデバイスにリンクできるので、事前に登録したデバイスしかログインに使用できないようにポリシーを設定できます。

© 2024 Cisco and/or its affiliates. All rights reserved.

デバイス信頼ポリシーを拡張して、認証時にデバイスのアセスメントも行うようにすることも可能です。多くのツールは、デバイスで実行されているソフトウェアが最新かどうかや、適切なセキュリティソフトウェアが実行されているかどうかを確認できるようになっています。信頼できるデバイスのチェックと合わせてセキュリティ態勢のアセスメントを行うことで、防御システムは攻撃者の侵入手段をさらに絞り込めます。



レベル 3

アクセスをモニタリングし、アクセス要件を動的に変更。

レベル 2

信頼できるデバイスポリシーを導入。

レベル 1

リスクのある国や IP からのアクセスについては、ブロックするか、認証要件を引き上げる。

レベル 0

すべてのユーザーに同じアクセスポリシーを適用。

アクセスポリシーの KPI

信頼できるまたは既知の場所、IP からのアクセスの割合

認証時にリスクを評価したアクセスの割合

信頼できるデバイスからのアクセスの割合

© 2024 Cisco and/or its affiliates. All rights reserved.

03

検出

ログの取り込み

アイデンティティベースの脅威を検出する前に、適切なソースから適切なログを収集、保存、保持する必要があります。これらのログを使用すれば、脅威の検出にもコンプライアンスにも役立ちます。

たとえばサーベンスオクスリー（SOX）法では、失敗したログイン回数を収集することが義務付けられています。[3] 以下に示すとおり、これに関連する CIS および NIST 管理策のセクションもあります。

ログの収集	CIS CSC 8.12 サービスプロバイダーのログを収集する	NIST CSF DE.AE-3 複数のソースとセンサーからイベントデータが収集され関連付けられている
	CIS CSC 8.2 監査ログを収集する	NIST CSF DE.DP-4 イベント検出情報が周知されている

注釈：

8. H.R.3763 - Sarbanes-Oxley Act of 2002、Congress.gov

© 2024 Cisco and/or its affiliates. All rights reserved.

オンプレミスとクラウドベースの収集

オンプレミスの Active Directory（AD）は IAM プログラムの一般的なデータソースであり、重要なユーザーアイデンティティとアクセスデータが含まれています。AD ログを監視することで、ログイン試行やユーザー権限の変更など、ユーザーアクティビティに関するインサイトが得られます。

Entra ID、Okta、Duo、AWS などのクラウドベースの IAM ソリューションも、重要なユーザーアイデンティティを提供し、データにアクセスします。これらのソースからのログとイベントを監視することで、潜在的な脅威を特定し、セキュリティポリシーを順守できます。

現在のデジタル環境では多くの組織が、Google、Slack、Salesforce、GitHub などの従来とは異なるアイデンティティ プロバイダーを利用してユーザーアイデンティティと重要なリソースへのアクセスを管理しています。そのため、アイデンティティ脅威の検出を効果的に行うには、従来とは異なるこうしたアイデンティティ プロバイダーも対象に含める必要があります。従来とは異なるアイデンティティを侵害して重要なリソースに不正アクセスする攻撃が増加しているため、これらのアイデンティティに関連するインシデントをモニターして対応することが極めて重要です。

25%

アイデンティティログをセキュリティ情報イベント管理（SIEM）に転送している組織のうち、実際にそれらのログを使用している組織は 25% にすぎない。

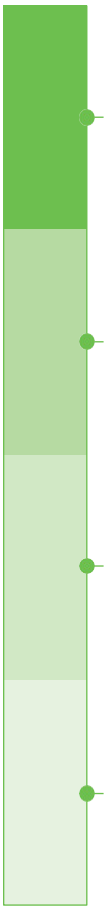
従来とは異なるアイデンティティ プロバイダーを ITDR 戦略に組み込むことで、使用しているプロバイダーに関係なく、アイデンティティ関連のインシデントをプロアクティブに特定して対応できます。ITDR に対するこの包括的なアプローチにより、アイデンティティ関連のインシデントを検出して対応する組織の能力が向上し、データ侵害などのセキュリティインシデントのリスクが軽減されます。

最後になりますが、アイデンティティ プロバイダーからログを収集していても、それだけでは、ログを実際に活用できる状態であるとは限りません。実際、アイデンティティログを転送している組織のうち実際にそれらのログを使用している組織は 25% にすぎません。[9]

注釈：

9. How Detection Posture Management Can Help CISOs Track the Right Metrics、CardinalOps

© 2024 Cisco and/or its affiliates. All rights reserved.



レベル 3

アイデンティティ データ エンジニアリングによるデータの包括的な理解と最適化。

レベル 2

ルールによるデータの積極的な活用と分析の自動化。

レベル 1

アイデンティティのソースを SIEM に集約し、保持ポリシーを検証。

レベル 0

アイデンティティログやデータを収集していない。

収集の KPI

失敗したログインの回数

アラート応答時間

© 2024 Cisco and/or its affiliates. All rights reserved.

検出方法

効果的なアイデンティティ脅威検出機能に必要なのは、さまざまな方法を使用することです。最も簡単なのは、IOC ベースの検出です。ただし、セキュリティチームは MITRE ATT&CK フレームワークに沿った手法に注力するようになってきています。たとえば Duo Trust Monitor 機能の場合、以下に挙げるあらゆる検出形式を適用できますが、適用対象は Duo のログとアクティビティに限定されます。一方、他の ITDR 機能は、特定のタイプの検出形式に特化している場合もあります。

検出へのアプローチ

IOC 主導型の検出

侵害の兆候（IOC）は、既知の悪意のある IP アドレスやマルウェアのシグニチャなど、悪意のあるアクティビティを示す特定のアーティファクトのことです。IOC 主導型の検出では、ネットワークトラフィックと IOC のシステムログを監視して、潜在的な脅威を特定します。このアプローチは事後対応型で、既知の脅威の検出に依存しています。

長所：検出の作成と対応が簡単。

短所：IOC はすぐに古くなってしまうため、事後対応型ブロッキングのメリットは限定的。

アクティビティ主導型の検出

アクティビティ主導型の検出では、異常なアクティビティがないかユーザーの行動をモニターします。このアプローチでは、機械学習アルゴリズムと人工知能を使用して、各ユーザーの通常の行動の基準を確立し、基準からの逸脱があれば、それについてユーザーにアラートを出します。不審な管理者アクティビティもアラートの対象になり得ます（対象とすべきです）。

長所：IOC だけでなく行動をモニターできる。

短所：従来の UEBA ソリューションには多くのノイズが伴う。

TTP 主導型の検出

戦術、手法、手順（TTP）とは、攻撃者が目的を達成するために使用する方法のことです。TTP 主導型の検出では、攻撃者が使用する TTP を特定し、ネットワークやエンドポイントで同様のアクティビティがないかモニタリングします。このアプローチは、特定の IOC ではなく、攻撃者の行動を特定することに重点を置いています。

長所：攻撃者が実際に行うことと一致する。IOC とは異なり、攻撃者は多くの場合、同じような手法を使用する。

短所：マッピングする手法が数多くあり、絶えず追加されている。

© 2024 Cisco and/or its affiliates. All rights reserved.

MITRE ATT&CK

関連する手法、サブ手法、データソース

手法

ブルートフォース攻撃（T1110）

リモート アクセス ソフトウェア（T1219）

検出（T1087）

Web セッション Cookie の窃取（T1539）

有効なアカウント（T1078）

アカウント操作（T1098）

アカウント操作：クラウドロールの追加（T1098.003）

アカウントの侵害：電子メールアカウント（T1586.002）

多要素認証要求の生成（T1621）

サブ手法

有効なアカウント：デフォルトのアカウント（T1078.001）

有効なアカウント：クラウドアカウント（T1078.004）

ブルートフォース攻撃：パスワードスプレー攻撃（T1110.003）

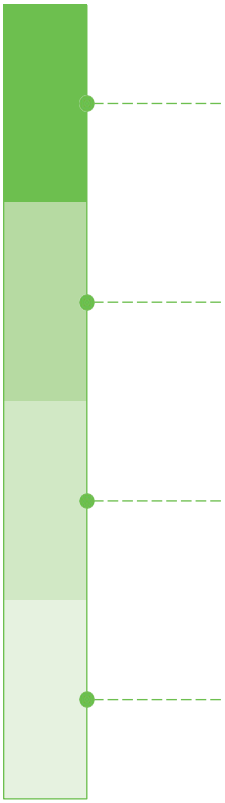
ブルートフォース攻撃：クレデンシャルスタッフィング攻撃（T1110.004）

データソース

Active Directory（AD ログイン情報のリクエスト、オブジェクトへのアクセス、オブジェクトの作成、オブジェクトの削除、オブジェクトの変更を含む）

ログオンセッション（ユーザーアカウント）

© 2024 Cisco and/or its affiliates. All rights reserved.



レベル 3

アイデンティティ データ エンジニアリングによるデータの包括的な理解と最適化。

レベル 2

ルールによるデータの積極的な活用と分析の自動化。

レベル 1

アイデンティティのソースを SIEM に集約し、保持ポリシーを検証。

レベル 0

アイデンティティログやデータを収集していない。

検出の KPI

ブロックされた不審な IP アドレスの数

あり得ない移動イベントの数

テナントイベントが発生した新しい国の数

侵害を受けたユーザーを検出するまでの時間

© 2024 Cisco and/or its affiliates. All rights reserved.

04

対応

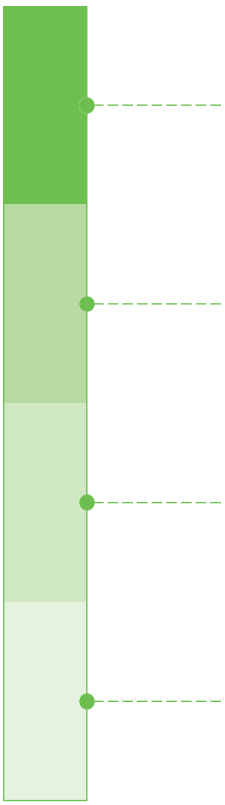
アイデンティティの脅威を検出するのは素晴らしいことですが、それはアクションや対応に反映されなければなりません。対応には 2 つのアプローチがあります。1 つは、ツールを統合し、技術的な対応を自動化するというものです。自動対応は、検出と適切な対応措置をシンプルにマッピングできる場合に最適です。たとえばアイデンティティベースの検出ツールがアラートを出したとします。このアラートが出された背景にある情報を別のさまざまなツールに転送すれば、対応に役立てることができます。認証やアクセスなどの制御ポイントでは、アラートからもたらされた新しい背景情報に基づいて対策を打てます。今後の認証要件を変更することもできるし、緊急の場合はアクセスを取り消すことも可能です。分析結果をアクセス管理制御への入力として使用する場合、自動化できるポイントは多数存在します。

しかし、多くのユースケースでは、自動で対応するのは非常に困難です。検出シナリオの多くは「あいまい」で、画一的な対応はできません。場合によっては、ユーザーを自動的にブロックするのは適切な対応ではないかもしれませんが、不審なアクティビティがあった場合は、徹底的な調査が必要となることも大いにあり得ます。

そのため、組織はこれらの脅威に対応するための明確なプロセスをハンドブックに定め、文書化する必要があります。SLA が定義されたチケット発行プラットフォームと連携するのが理想的です。対応ハンドブックには、アイデンティティ関連のインシデントに対応する際にセキュリティチームが従うための明確で実用的なガイダンスが含まれており、一貫性のある効果的な対応を実現します。

対応ハンドブックを使用することで、セキュリティチームはインシデントの性質と範囲を迅速かつ正確に特定し、対応に優先順位を付け、インシデントの封じ込めと修復に必要なアクションを実行できます。

© 2024 Cisco and/or its affiliates. All rights reserved.



レベル 3

ML 主導、自己修復型、データサイエンス、対応メトリックの継続的な改善。

レベル 2

制御ポイントツールによる自動対応。

レベル 1

SLA が定義されているチケット発行プラットフォームと連携するハンドブック主導型の対応。

レベル 0

対応ハンドブックなし。アドホック対応のみ。

アイデンティティに関するインシデント対応計画の作成

インシデント対応計画は、セキュリティインシデントが発生した場合にとるべき手順をまとめたものです。インシデントを特定して封じ込め、影響を評価し、インシデントから回復するための手順が含まれています。

対応計画ハンドブックは、効果的かつ包括的なものにするために、定期的に見直して更新する必要があります。アイデンティティ インシデント対応計画に関する重要な考慮事項を次に示します。

- **ビジネス意思決定者を定める。**アイデンティティ インシデント発生時に重要な意思決定を行う組織内の主要な関係者を特定します。これには、経営陣、IT リーダー、法定代理人、広報チームなどが含まれます。明確なコミュニケーションラインを確保し、意思決定権を指定して、迅速かつ調整された対応を促進します。
- **アクションのエスカレーション。**アイデンティティ インシデントへの即時の対応として実行する具体的なアクションについて、詳細な計画を策定します。これには、影響を受けたアカウントの隔離、侵害されたログイン情報のリセット、不正セッションの終了の手順を含める必要があります。これらのアクションの実行に関与する IT チームの役割と責任を明確に定義し、必要なツールとリソースを提供します。

© 2024 Cisco and/or its affiliates. All rights reserved.

- **ポリシーと例外の文書化。**アクセスポリシー、MFA のガイドライン、組織内での適用方法を包括的に文書化します。これらのポリシーを周知徹底し、定期的にレビューし、順守されているかどうかを積極的にモニターします。さらに、ポリシーの例外に関する明確なガイドラインを定め、例外を許可してトラッキングするプロセスも文書化します。
- **外部とのコミュニケーション。**アイデンティティ インシデントが発生した場合に、顧客、パートナー、規制機関などの外部の関係者に対応するためのコミュニケーション計画を作成します。既知の情報、未知の情報、影響を受ける関係者への潜在的な影響を考慮して、共有できる情報を明確に定義します。インシデント対応プロセスを通じてタイムリーで正確な最新情報を提供する広報担当者を指名します。
- **データ共有。**侵害の兆候（IOC）や攻撃に使用される MITRE ATT&CK 手法など、インシデントに関連するデータを共有するためのプロトコルを確立します。同業他社、サイバーセキュリティ組織、法執行機関と協力して情報を共有します。
- **法的規制。**データ侵害通知法や業界固有のコンプライアンス要件など、アイデンティティ インシデントに関連する法規制上の義務について十分に理解しておきます。インシデント対応計画が、指定された期間内にこれらの義務と通知要件に適合するようにします。
- **レジリエンス計画。**重要なシステムとデータの定期的なバックアップを含む、堅牢なレジリエンス計画を作成します。バックアッププロセスの有効性を保証するために、バックアッププロセスを定期的にテストして検証します。定期的に訓練と演習を実施して、レジリエンス計画を検証し、改善が必要な領域を特定します。

© 2024 Cisco and/or its affiliates. All rights reserved.

03

主要な関係者と責任

主要な関係者

アイデンティティ セキュリティ プログラムには、プログラムの導入を確実に成功させるために、異なる役割と責任を持つさまざまな関係者が関与します。各組織には独自の役割と責任があるため、これはあくまで参考として扱ってください。

エンドユーザー

従業員やパートナーなど、組織のシステムの情報を使用する個人。エンドユーザーは、アイデンティティ セキュリティ プログラムで重視される必要があります。

期待される成果：情報への安全かつ確実なアクセス、個人データの保護、機密情報への不正アクセスの防止。

責任：パスワード管理のベストプラクティス、不審なアクティビティの報告、組織のセキュリティポリシーの順守。

CISO（最高情報セキュリティ責任者）

CISO は、組織のセキュリティプログラムを監督し、それがビジネス目標に沿っていることを確認する責任があります。最も一般的には、アイデンティティ セキュリティを推進する立場にあります。

期待される成果：組織のリスクの最小化、組織のセキュリティ態勢の強化、法的規制への準拠の維持。

責任：セキュリティ戦略の策定、経営陣へのセキュリティリスクの伝達、セキュリティチームへのガイダンスの提供。

© 2024 Cisco and/or its affiliates. All rights reserved.

セキュリティチーム

セキュリティチームは、脅威検出、インフラストラクチャ管理、脆弱性管理など、組織のセキュリティ態勢のモニタリングを担当します。

期待される成果：リスクの特定と軽減、データ侵害の防止、セキュリティインシデントの影響の最小化。

責任：定期的なセキュリティ評価の実施、インシデント対応計画の実施、セキュリティログのモニタリング。

IAM（アイデンティティとアクセスの管理）チーム

適切なツールを適切な人材にタイムリーに提供することで、安全な事業運営を実現します。

期待される成果：ユーザーがシステムとデータに適切なレベルでアクセスできるようにし、不正アクセスのリスクを最小限に抑え、法的規制の順守を維持。

責任：アクセスポリシーの定義、ユーザーアカウントとデバイスの管理、ユーザーアクティビティのモニタリング。

サイバー脅威インテリジェンスチーム

組織に対する脅威を追跡および分析し、ビジネスへの潜在的な影響を把握する責任があります。

期待される成果：一般的な攻撃者の手口から保護。

責任：アイデンティティに基づく手口、最近の攻撃の IOC、侵害されたログイン情報の検出に関する評価を提供。

CIO（最高情報責任者）

組織の情報テクノロジー インフラストラクチャ管理に責任を持ち、組織のビジネス目標を確実にサポートします。

期待される成果：IT を組織の戦略的目標に一致させ、IT の効率を高め、IT のコストを管理。

責任：アイデンティティ セキュリティ プログラムの実施を監督し、それが組織のセキュリティ要件および法的規制を満たしていることを確認し、プログラムをサポートするリソースを提供。

© 2024 Cisco and/or its affiliates. All rights reserved.

IT ヘルプデスク

エンドユーザーにテクニカルサポートを提供します。

期待される成果：パスワードのリセットやアカウントのロックアウトなど、アイデンティティとアクセスに関連する問題をタイムリーかつ安全な方法で解決。

責任：アクセスを許可する前にユーザーのアイデンティティを確認し、確立されたセキュリティ手順に従い、セキュリティインシデントを適切なチームにエスカレーション。

コンプライアンスチーム

該当する法的規制と業界標準に組織が準拠していることを確認します。

期待される成果：法的規制の順守の維持、罰則の回避、組織の評判の強化。

責任：コンプライアンス要件を評価し、それらの要件を満たすための管理策を導入し、コンプライアンス状況を報告。

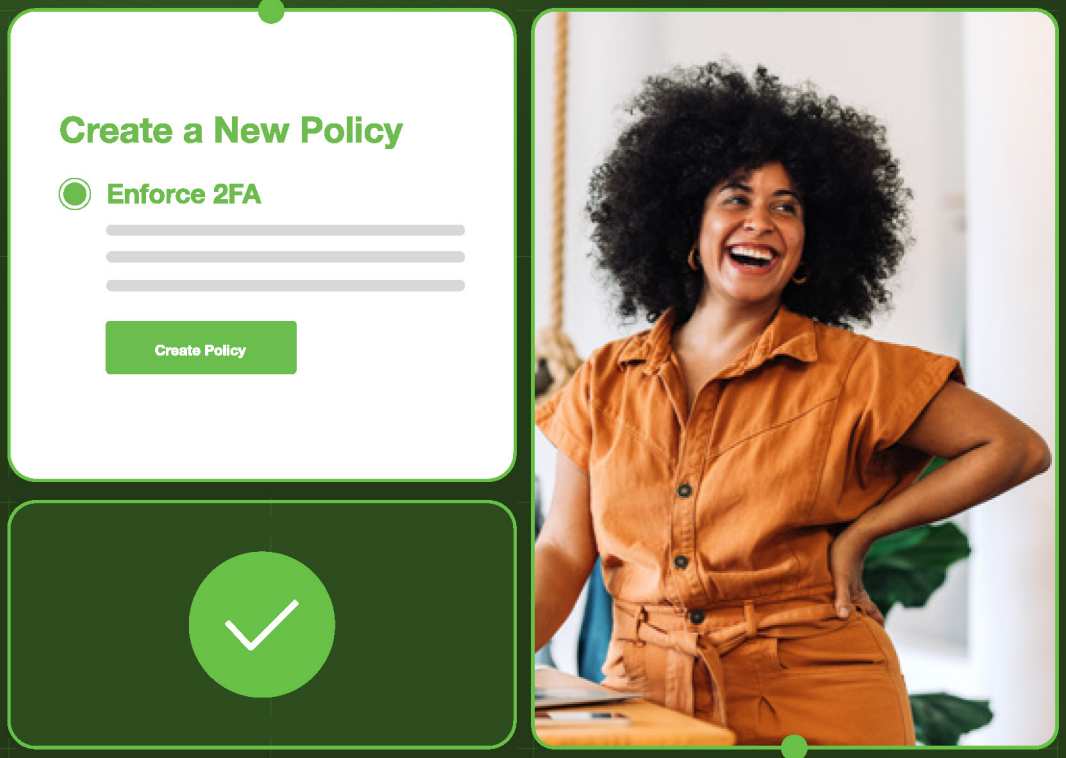
© 2024 Cisco and/or its affiliates. All rights reserved.

アイデンティティ セキュリティにおける責任

「一般的な」アイデンティティ セキュリティ プログラムの RASCI（Responsible、Accountable、Supporting、Consulted、Informed（実行責任者、説明責任者、協業先、相談先、報告先）の略）マトリックスを作成してみました（実際は、組織ごとに異なります）。これには、報告先が CIO である IAM チームと、報告先が CISO であるセキュリティチームが含まれます。

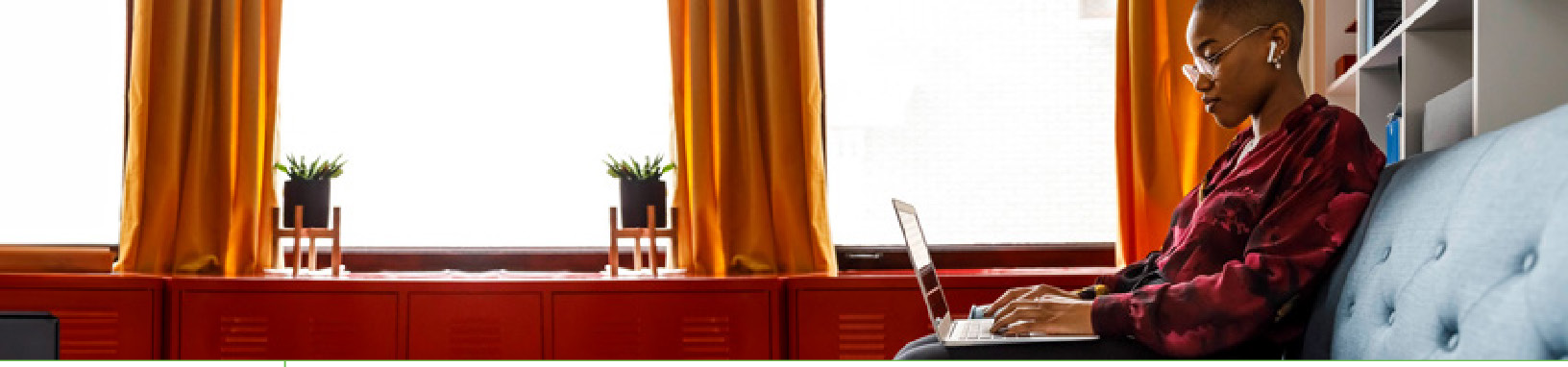
	CISO	CIO	セキュリティチーム	IAM/IT チーム	脅威インテリジェンス	IT ヘルプデスク	コンプライアンスチーム
識別							
ユーザーインベントリの構築	A	S	C	R			
ゲストアクセスの管理	S	A	S	R			I
マシンのアイデンティティの管理	I	A	C	R			
保護							
オンボーディング	I	A	C	R		S	I
プロビジョニング解除	I	A	C	R		S	I
シングルサインオン	I	A	C	R	S	S	I
多要素認証	C	A	C	R	S	S	I
ユーザーアクセス	I	A	C	R			I
検出							
収集	A	I	R	S	S		
検出	A	I	R	S	S		
対応							
対応	A	I	R	S	S	S	
			R	A	S	C	I
			実行責任者	説明責任者	協業先	相談先	報告先

© 2024 Cisco and/or its affiliates. All rights reserved.



04

主なビジネス成果



主なビジネス成果

強力なアイデンティティ セキュリティ プログラムを使用することにより、単にセキュリティリスクを軽減するだけでなく、重要なビジネス成果を実現できます。独自のビジネス成果を定義し、それを既知のビジネス推進要因に対応づけることをお勧めします。

強力なアイデンティティ セキュリティ プログラムを導入することで得られる 5 つの主要なビジネス成果を以下にご紹介します。

1. **侵害の防止**：アイデンティティ セキュリティ プログラムは、ネットワークセキュリティとアカウントハイジーンを強化することで、侵害を未然に防ぐことができます。また、侵害されたアカウントに迅速に対応し、潜在的な侵害の影響を軽減することもできます。これは、ブランドと評判を保護することにもつながります。

2. **コンプライアンス**：SOX、NIST、SOC 2、PCI DSS、HIPAA、GDPR などのさまざまな規制基準とフレームワークを順守することは、多くの組織にとって大きな負担となっています。アイデンティティ セキュリティ プログラムでは、アクセス制御の可視性が高まり、セキュリティハイジーンが強化されるため、コンプライアンスを確保することができます。

3. **サードパーティのリスク**：多くの組織は、システムやデータへのサードパーティのアクセス管理に苦慮しています。強力なアイデンティティ セキュリティ プログラムにより、ゲストアカウントの管理とサードパーティのアクティビティをモニターし、サードパーティのアクセスに起因するデータ侵害のリスクを軽減できます。

4. **業務効率**：アイデンティティ セキュリティ プログラムが適切に設計されていれば、パスワードのリセットとレポートに必要な時間と労力が削減され、業務効率が向上します。不要なアクセスを排除し、ライセンスコストを削減し、アクセス管理プロセスを合理化することも可能です。

5. **従業員の満足度**：強力なアイデンティティ セキュリティ プログラムから従業員が得られるメリットには、リソースへの迅速で簡単なアクセス、パスワードレス認証、迅速なパスワードリセットがあります。このようなプログラムにより、従業員の満足度と生産性が向上し、定着率と全体的な仕事の満足度が向上します。

強力なアイデンティティ セキュリティ プログラムを使用することにより、単にセキュリティリスクを軽減するだけでなく、重要なビジネス成果を実現できます。組織は、明確なビジネス成果を事前に定義し、それを既知のビジネス推進要因とリスクに結びつけることで、アイデンティティ セキュリティ プログラムに対する経営陣の支持を確保し、測定可能なビジネス価値を生み出すプログラムを確実に設計できます。

© 2024 Cisco and/or its affiliates. All rights reserved.

05

重要業績評価指標

重要業績評価指標

これらすべての分野をまとめることで、アイデンティティ セキュリティ プログラムを長期的に測定できる、説得力のある一連の重要業績評価指標（KPI）を策定できます。

これらはアイデンティティ セキュリティの 4 つの柱をすべて活用し、サイバーセキュリティとビジネスの成果を明確に対応づけています。

NIST CSF のステージ	アイデンティティ機能	KPI の例	サイバーセキュリティの成果	ビジネス成果
識別	ユーザーインベントリ	孤立アカウントの数 HRIS（人事情報システム）との不一致の数 一意でない ID と共有 ID の数 管理者アカウントの数	ゼロトラストへの移行	侵害の防止、従業員の満足度、コンプライアンスの向上
	マシンのアイデンティティ	所有者が不明なサービスアカウントの数 デフォルトのパスワードを使用している、あるいはキーが期限切れになったサービスアカウントの数	不正アクセスの削減	侵害の防止とブランドの評判
	ゲストアカウント	非アクティブなゲストアカウントの数 過剰にアクセスしているゲストアカウントの数 アクセスがあった管理対象外のデバイスの数	攻撃対象領域を縮小	侵害の防止、サードパーティのリスク、コンプライアンスの向上と監査所見の削減
保護	オンボーディング	新入社員のオンボーディングが完了するまでのスピード 過剰なアクセス権を持つユーザーの数 ユーザーアカウント作成の満足度	アカウント乗っ取りの防止	業務効率、侵害の防止
	プロビジョニング解除	SLA 内で無効になっている退職したユーザーのアカウントの割合 迅速なプロビジョニング解除	不正アクセスとデータ損失の削減	業務効率、侵害（アカウント乗っ取り）の防止
	SSO	SSO で保護されているビジネスアプリケーションの割合 ダイレクトアクセスされるアプリケーションの数 パスワードの複雑さ 使用されていないアプリケーションの数 1 日あたりのログインの回数	アカウント乗っ取りの防止	侵害の防止、従業員の満足度
	MFA	多要素認証の使用が設定されているユーザーアカウントの割合 MFA を使用しているゲストアカウントの割合 強力な形式の MFA（FIDO2、パスワードレス、パスキー、番号照合）を使用しているユーザーアカウントの割合	アカウント乗っ取りの防止	侵害の防止、コンプライアンスの向上、サードパーティのリスク
	アクセスポリシー	信頼できるまたは既知の場所、IP からのアクセスの割合 認証時にリスクを評価したアクセスの割合 信頼できるデバイスからのアクセスの割合	重要なデータへのアクセス制限	侵害の防止、コンプライアンスの向上

© 2024 Cisco and/or its affiliates. All rights reserved.

NIST CSF のステージ	アイデンティティ機能	KPI の例	サイバーセキュリティの成果	ビジネス成果
検出	収集	失敗したログイン（SOX 法で規定）の回数 異常なアクセスイベントの数 ユーザーから報告された不審なアクティビティの数 管理対象外エンドポイントの数 MFA を使用していない特権ユーザーの数	「行動の基準」と独自のリスクプロファイルの策定 不正アクセスの削減	コンプライアンスの向上と監査所見の削減、業務効率
	検出	並列セッションの数 あり得ない移動イベントの数 ブロックされた不審な IP アドレスの数 ブルートフォース攻撃と侵害されたユーザーの検出にかかった平均時間 重要なリスクイベントの 1 日あたりの発生数	侵害されたユーザーと組織内に潜む脅威の迅速な検出	侵害の防止、業務効率
対応	対応	パスワードリセットにかかる平均時間 誤検出の割合 認証関連のヘルプデスクチケットの数 自己修復で実施された OS/ブラウザのデバイス更新の回数 緩和された MITRE ATT&CK サブ手法の数 トリアージされたリスクイベントの 1 日あたりの数 改善されたアクセスポリシーの数	平均修復時間の短縮 アカウント乗っ取りの防止 ビジネスの現状に合わせた最適化と保護	業務効率、コンプライアンスの向上、侵害の防止

ヒント：上場企業の場合は、Form 10-K を確認して現在のビジネスリスクを把握します。

© 2024 Cisco and/or its affiliates. All rights reserved.

まとめ

冒頭および各セクションで述べてきたポイントの繰り返しになりますが、本書は、組織にアイデンティティ セキュリティを確実に導入する方法を提供するものではありません。機能を整理して有効性を測定するために利用できる主要なフレームワークを紹介するためのものです。現在お使いの IT ツールとセキュリティツールを利用して、ご紹介した取り組みの大部分を始めることができるでしょう。

ですが、Cisco Duo が、あらゆる規模の組織がアイデンティティ セキュリティの向上という成果を達成できるよう支援したいと考えていることについて、触れないわけにはいきません。Duo のアプローチは、アイデンティティベースの脅威の識別、保護、検出、対応を一貫して行うと同時に、従業員のシームレスなアクセスを確保する**継続的なアイデンティティ セキュリティ**の実践方法を構築することです。
アイデンティティベースの攻撃を阻止し、世界水準のユーザー体験を IT およびセキュリティの専門家とエンドユーザーに提供するために、Duo をお役立ていただければ幸いです。

アイデンティティ セキュリティ プログラムに着手するうえで、Duo をどのようにご活用いただけるかについては、**継続的なアイデンティティ セキュリティ**のページで詳細をご確認ください。**無料トライアル**もご利用いただけます。

Cisco Duo は、最先端のアクセス管理スイートによって侵害から保護します。強力な多層防御と革新的な機能で、正当なユーザーのアクセスを許可し、攻撃者の侵入を防ぎます。Duo は、信頼できるパートナーとして、ユーザーの生産性を向上させつつ、強固なセキュリティをすばやく実現します。

duo.com から、無料で製品をお試しいただけます。

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco およびシスコのロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。1365265887 07/2024