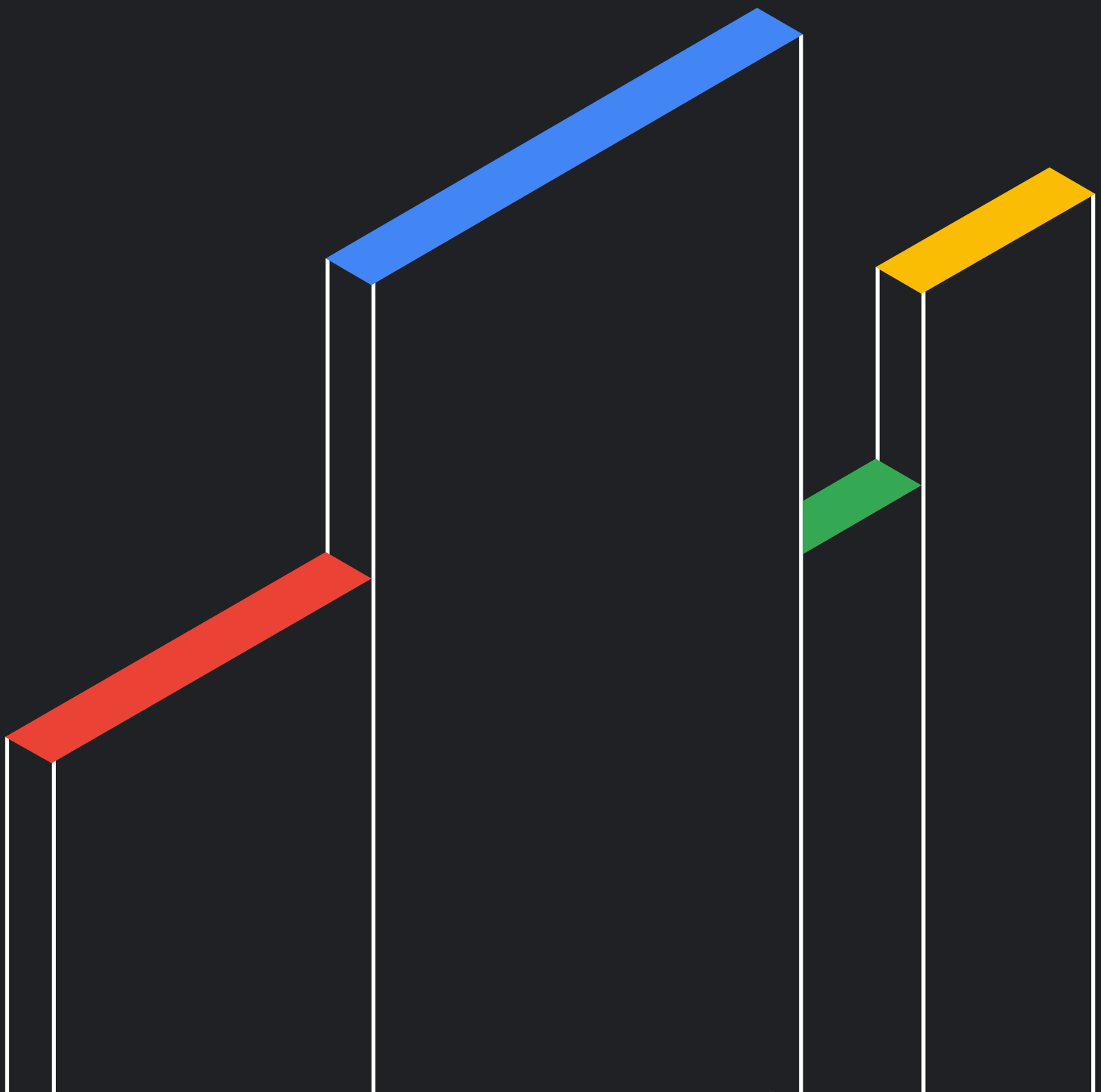
Mandiant

Google Cloud Security

M-Trends

2025 レポート

エグゼクティブ エディション



数字で見る: M-Trends のデータ

M-Trends 2025 で報告されている指標は、2024 年 1 月 1 日から 2024 年 12 月 31 日の間に行われた標的型攻撃アクティビティを Mandiant Consulting が調査した内容に基づいています。

概要

- 金銭目的のアクターの割合が、その他のアクターの割合を引き続き大幅に上回っています。2024 年に活動していた脅威グループの 55% は金銭目的で、2022 年の 48%、2023 年の 52% から着実に増加しています。諜報活動を目的とした脅威グループは 8% であり、2023 年の 10% 超からわずかに減少しています。
- 初期感染ベクトルで最も多かったのは、5 年連続で脆弱性利用型不正プログラム (33%) でした。認証情報の盗難 (16%) は 2024 年に 2 番目に多くなり、このベクトルがこの水準に達したのは初めてのことで、徐々に一般化しつつあることを裏付けています。上位 5 つのベクトルには、他にメール フィッシング (14%)、ウェブ侵害 (9%)、過去の侵害の利用 (8%) があります。
- 標的とされる頻度が高い業界は、金融 (17.4%)、ビジネス サービスとプロフェッショナル サービス (11.1%)、ハイテク (10.6%)、政府および行政機関 (9.5%)、医療 (9.3%) でした。このような標的の傾向は、過去のどの年もおおむね同様となっています。
- 悪意のあるアクティビティを組織が内部で発見した事例の割合は 43% であるのに対して、外部機関から指摘を受けるまで認識していなかった事例が 57% に上ります。外部からの通知の内訳は、法執行機関やサイバーセキュリティ ベンダーなどが 43%、敵対者からが 14% で、身代金要求という形で認識するケースがほとんどです。
- ランサムウェアの場合、攻撃者から通知を受けた事例の割合は 49% で、外部機関からの通知が 21%、内部での発見が 30% でした。
- 全世界での滞留時間の中央値は 2023 年の 10 日間から 11 日間に増加したものの、2022 年に報告された 16 日間を今回も下回っています。
- 全世界での滞留時間の中央値は、悪意のあるアクティビティを外部から通知された場合は 26 日間、攻撃者から通知された場合は 5 日間、組織が内部で発見した場合は 10 日間でした。
- 調査で確認された 205 のマルウェア ファミリーのうち、35% がバックドア、14% がランサムウェア、8% がドロッパー、7% がダウンローダ、6% がトンネラー、5% が認証情報窃取でした。このような内訳は、過去のどの年もおおむね同様となっています。従来のマルウェアが関係しないことが一般的な「環境寄生型」の手口も引き続き見受けられます。

必要とされる行動

- エンドポイント検出対応、高度な分析を利用したセキュリティ情報およびイベント管理 (SIEM)、ネットワーク トラフィック分析をはじめとする高度な脅威検出技術をデプロイし、最適化します。
- 定期的なスキャンによる脆弱性の有無の確認、リスクに基づいたパッチ適用の優先順位付け、可能な場合はパッチ適用プロセスの自動化によって、攻撃対象領域を最小限に抑えます。
- アクセス制御を強化し、最小権限などの適切な基本事項を実践します。ユーザーとアプリケーションの権限は必要なものに限定し、可能であれば FIDO2 準拠の多要素認証 (MFA) を適用して、アクセスログを定期的に確認してください。
- インシデント対応と復元に関する計画を策定し、定期的にテストします。計画には、ランサムウェアおよび自組織との関連性が強いその他の脅威について、具体的な対応方針を必ず盛り込んでください。机上演習とシミュレーションを定期的に行って計画の効果を検証し、対応時間を短縮します。
- 攻撃者の戦術を踏まえた現実的なエミュレーションによって、レッドチーム診断を行い防御の有効性を検証します。脆弱性と防御のギャップを洗い出すと同時に、セキュリティ チームによる検出と対応の所要時間も測定してください。
- 継続的なセキュリティ意識向上トレーニングとフィッシングのシミュレーションに投資します。フィッシング、ソーシャル エンジニアリング、ランサムウェアの手口を含めて、組織との関連性が強い最新の脅威について従業員教育を実施してください。

情報窃取型マルウェアが引き続き増加してエンタープライズ システムに対する脅威に

概要

- 認証情報やブラウザデータなどの機密情報を窃取する情報窃取型のマルウェアが増加基調にあり、組織は不正使用のリスクにさらされています。
- 脅威アクターは、情報窃取者のログから得た窃取済みの認証情報でシステムに初期アクセスし、データ窃盗や恐喝といった悪意のあるアクティビティにつなげています。
- 情報窃取型のマルウェアで窃取された認証情報を利用して UNC5537 が Snowflake の顧客データベース インスタンスを狙ったことで浮き彫りとなったのは、膨大な量の認証情報が情報窃取者のマーケットに出回っていることです。
- 仕事用の個人デバイスや請負業者のシステムは、他にない課題を生み出しています。たとえば、感染したパーソナル システムや同期されたブラウザで使われている企業の認証情報を情報窃取者が不正使用する恐れがあります。

必要とされる行動

- 強力な多要素認証（MFA）、特に中間者攻撃（AiTM）耐性のある MFA 手法を導入します。たとえば、ハードウェア セキュリティ キーやモバイル向け認証システム アプリです。
- 感染の監視と予防に向けてエンドポイントの検出と対応（EDR）システムおよび侵入検知システム（IDS）をデプロイして、エンドポイントのセキュリティを強化します。
- 個人デバイスと企業デバイスの使用を区別する厳密なポリシーを確立し、サードパーティ サプライヤーと契約業者のセキュリティ管理を確認します。
- ブラウザ管理を適用して、サードパーティ Cookie の制限、パスワード自動入力の無効化、未承認のブラウザ拡張機能の無効化を行います。
- ソフトウェアの使用に関するポリシーを確立し、信頼できないソースからダウンロードしないようユーザー トレーニングを実施します。確認済みのアプリケーションを取り扱うエンタープライズ アプリケーション ストアの導入を検討します。

北朝鮮のインサイダー脅威

概要

- 朝鮮民主主義人民共和国（北朝鮮）は国民をリモート IT 契約者として配置することで収益を生み、国益のための資金にしています。
- 北朝鮮の IT ワーカーは、窃取または偽造した身分証明書、虚偽の職歴や関係書類を利用して、多くの場合は米国内、またヨーロッパ内でもテクノロジー企業で高給の職位を確保しています。
- 雇用関係の終了後は、バーチャル プライベート ネットワーク（VPN）と現地のファシリテーターを利用して実際の位置情報を隠蔽し、企業システムへのアクセスを維持したうえで、正当なネットワーク トラフィックに紛れ込んで検出を回避します。
- 悪意のある直接的なアクティビティは限られていますが、企業のインフラストラクチャにアクセスされてしまうため、諜報活動、データ窃盗、恐喝に見舞われるリスクがあり、すでに何件かの恐喝事例が確認されています。

必要とされる行動

- 生体認証情報の確認を含めて従業員の徹底的な身元調査を実施し、学歴と職歴を独立した情報源と照らし合わせて確認します。
- 面接時のカメラ利用を必須として面接の手続きを厳格化し、映りたがらない採用希望者に警戒し、装っているペルソナやしぐさの矛盾を見落とさないようにします。
- 可能な場合、会社のノートパソコンは対面での受け取りを義務付けて身分証明書を確認します。従業員の書類に記載されていない住所にリソースを発送する際は追加の確認を行い、身元調査をあらためて確認します。
- エンドポイントの検出と対応（EDR）ツールをインストールして、リモート アクセス ソフトウェアや VPN 接続（特に Astrill VPN）がないかどうかを監視し、ヒューマン インターフェース デバイス（HID）の接続をロギングします。
- ユーザーによるアクセスの対象を各自の職務に必要なデータとリソースのみに制限して、最小権限でのアクセスを強制します。これにより、諜報活動、データ窃盗、恐喝の試みによって生じ得る損害を最小限に抑えます。

2024 年のイランの脅威ランドスケープ

概要

- イラン関連の脅威アクターによるサイバー作戦が 2024 年に増加し、特にイスラエルの組織を標的にして、侵入の成功率を高めるためにさまざまな手法が使用されていました。
- イラン関連の脅威アクターによるものと見られるカスタム マルウェアが 2023 年比で 35% 増と急増しており、45 を超えるマルウェア ファミリーが新たに発見されています。
- イスラエル国内を標的とした集中的な破壊工作や破壊活動ではワイパー マルウェアが利用されていることが多く、イラン関連の脅威アクターと手を組んだオンライン上のさまざまなペルソナによるハック アンド リーク活動をしばしば伴います。
- イラン関連の脅威アクターは、公開リソース、クラウド インフラストラクチャ、リモート モニタリングおよび管理 (RMM) ソフトウェアなどの正当なツールを駆使して検出を免れています。
- ソーシャル エンジニアリングのスキームはいっそう巧妙になっており、グラフィカル ユーザー インターフェース (GUI) を組み込んでマルウェアを擬装し、時事や雇用の話題を盛り込んで標的を欺きます。

必要とされる行動

- 特に特権付きアカウントを対象として、フィッシング耐性のある多要素認証 (MFA)、具体的には証明書ベースの認証 (CBA) と FIDO2 セキュリティ キーを適用し、認証情報の収集や MFA 回避の試みに対抗します。
- クラウド テクノロジーの採用にあたっては、セキュリティ管理の定義、クラウドベースのアクティビティの全面的な可視化、脅威ハンティング用データの提供、インシデント対応、継続的な監視を含めて、セキュリティ最優先の設計を導入します。
- 職場の外で個人を標的とするものも含めて、ますます複雑化しているソーシャル エンジニアリング キャンペーンの識別と対応を焦点として、包括的なユーザー意識向上トレーニングを実施します。
- 脅威アクターは、従来の検出手法を迂回できる RMM ソフトウェアなどの正当なツールを利用する可能性があるため、それらが利用されていないか注意します。異常な RMM アクティビティを監視し監査する機能を導入してください。検出設定を調整して、ツールの正当な使用は許可します。
- 集団での防御が重要であるため、業界や業種の枠を超えて連携し、イラン関連の脅威アクターからの防御に向けて脅威インテリジェンスやベスト プラクティスを共有します。

クラウド環境と Software as a Service 環境でのデータ窃盗の狡猾化

概要

- 攻撃者は広範なアクセスを得るために、ターゲットをオンプレミス ネットワークではなく、シングル サインオン（SSO）ポータルなどの中央認証機関のクラウドベースのストアに変えています。
- 従来のネットワーク管理を迂回するため、Software as a Service（SaaS）環境への特権付きアクセス権を持つユーザーを狙って、ソーシャル エンジニアリングを仕掛ける事例が増加しています。
- 攻撃者は、オンプレミス リソースとクラウド リソースを組み合わせたハイブリッド型の手口を駆使し、悪意のあるアクティビティを正当なトラフィックに紛れ込ませて検出を回避します。
- クラウド環境でのロギングとモニタリングが不十分な場合は死角が生まれ、攻撃者アクティビティの検出が本来の効果を発揮できず、調査が後手に回ることになります。
- 脅威アクターは、クラウドの責任共有モデルを十分に理解していない組織が管理をおざなりにしたリスクにつけ込んできます。

必要とされる行動

- すべてのクラウド サービスにわたって、ネットワーク トラフィック ログ、ファイアウォール ログ、ストレージ アクセス ログ、コンピューティングとリソース モニタリング、監査ログ、データベース ログ、Identity and Access Management（IAM）ログを含む包括的なロギングを有効にします。
- 多要素認証（MFA）を含む強力な IAM 手順を導入し、SSO ポータルや特権付きアカウントで疑わしいアクティビティがないかどうかを厳重に監視します。
- クラウド プロバイダや SaaS 利用時のサブスクリプションのレベルを定期的に再確認し、妥当性を検証して、必要なロギングとセキュリティ可視化に関する要件をプロバイダが確実に満たしている状態にします。
- クラウド環境や SaaS 環境を標的とするソーシャル エンジニアリングの手口についてユーザー トレーニングを実施し、パスワードの再設定と MFA の登録に関連するリクエストの検証について明確な手順を確立します。
- クラウド セキュリティの責任共有モデルを徹底的に理解し、組織とクラウド プロバイダのセキュリティ責任分担を明確にします。
- インシデント対応計画では、オンプレミスとクラウドのインテグレーション システムを対象とした検出、封じ込め、根絶、復旧の手順に焦点を当てて、ハイブリッド環境を必ず考慮に入れます。

クラウド侵害調査の共通のテーマ

概要

- クラウド境界をまたがり広く適用されている構成のミスに脅威アクターがつけ込み、たとえクラウド セキュリティが成熟している組織であってもそのクラウド環境へのアクセス権が不正に取得されてしまうという事例が増加しています。
- クラウドへの侵害を許すことにつながっている重要なテーマは 3 つあり、1) ID ソリューションに十分に高度なセキュリティ ポリシーが適用されておらず、2) オンプレミス インテグレーションの保護が適切ではなく、3) 広範なクラウド攻撃対象領域の可視化が不十分であることです。
- ID 侵害の発端としてよくあるのは、多要素認証 (MFA) などのセキュリティ管理が導入されていない ID アーキテクチャや実践慣行、容易に迂回できるパスワード再設定ポータル、不十分なサードパーティ アクセス制御です。
- オンプレミスとクラウド インフラストラクチャとのインテグレーションが適切に保護されていない場合は、攻撃者が環境間を垂直移動してクラウドのセキュリティ管理を迂回する恐れがあります。
- クラウドの攻撃対象領域には、ネットワークへの露出部だけでなくデータの列挙、認証情報の拡散、一般公開リソースも含まれており、このような広範にわたる攻撃対象領域を組織で事前対応的に特定し、縮小することが必要不可欠です。

必要とされる行動

- 強力な (フィッシング耐性のある) MFA を導入して ID のセキュリティを強化し、パスワード再設定プロセスを保護し、サードパーティによるアクセスを厳密に制御します。特権 ID 管理 (PIM) を利用し、外部人材向けに複数の異なる ID ストアを運用します。
- 信頼できるサービス インフラストラクチャの監査と保護、オンプレミス環境とクラウド環境とのコンピューティングおよびネットワークのインテグレーションによって、オンプレミスのインテグレーションを保護します。管理インターフェースへのアクセスを定期的に再確認し、制限するとともに、ネットワーク接続を適切にセグメント化します。
- データ列挙の管理、認証情報の拡散への対処、一般公開リソースの保護を通じて、クラウド攻撃対象領域を事前対応的に特定して縮小します。包括的な可視化とコンプライアンス モニタリングを目的として、クラウド セキュリティ ポスチャー管理プラットフォームを利用します。
- ID、リソース、ネットワーク、エンドポイントを含むすべてのレイヤにアクセス制限、強化策、継続的な検出戦略、事前対応型のアクションを含めた、総合的な多層セキュリティのアプローチを採用します。

Web3 と暗号通貨に対する脅威

概要

- 暗号通貨やブロックチェーンを含む Web3 テクノロジーを標的とした盗難、マネー ロンダリング、違法行為への資金提供がますます増加しています。
- 北朝鮮系をはじめとする脅威アクターは巧妙なソーシャル エンジニアリング戦術を駆使し、脆弱性を悪用して、膨大な量のデジタル アセットを窃取しています。
- 暗号通貨取引は資金の流れが難読化されているほか、スマート コントラクトには悪意のあるインフラストラクチャのホスティングにも悪用し得る不変性があることから、追跡や規制が難題になります。
- ユーザーのウォレットからの暗号通貨の窃盗には「ドレイナー」や悪意のあるスマート コントラクトが利用されており、「サービスとしてのドレイナー」(DaaS) マーケットが登場してこれらの攻撃に加担しています。
- Web3 テクノロジーを採用している組織は迅速なインテグレーションと堅牢なセキュリティとの兼ね合いに苦慮しており、標準的なセキュリティ制御をおろそかにすることが多く、技術的負債や攻撃対象領域の拡大につながっていることも少なくありません。

必要とされる行動

- トランザクション データ分析をエンドポイント テレメトリやセキュリティ テレメトリと組み合わせて、Web3 や暗号通貨のプラットフォームを標的とした悪意のあるアクティビティの検出能力を高めます。
- 基幹ウォレット インフラストラクチャや暗号制御のみを焦点とした取り組みだけで終わらせず、標準的なセキュリティ管理を確実に導入して維持することにより、技術的負担の発生を避けるとともに攻撃対象領域を縮小します。
- ソーシャル エンジニアリングの手口について、ユーザー向けの教育とトレーニングを実施します。脅威アクターはフィッシングや偽の求人情報といったソーシャル エンジニアリングを多用して初期アクセスを獲得しているため、従業員を対象としたトレーニングによってこれらの手口の認知度を高め、回避することが重要です。
- 脅威アクターは、取引ソフトウェアまたは暗号通貨ソフトウェアをトロイの木馬化してソフトウェア サプライ チェーンを侵害する恐れがあるため、サードパーティ ソフトウェアをデプロイする際はあらかじめ徹底的に調査、検証する必要があります。
- デジタル アセットの窃取を試みる、悪意のあるスマート コントラクトや「ドレイナー」に注意します。監視を導入して暗号通貨ウォレットへの不正アクセスを検出、防止します。

保護されていないデータ リポジトリ

概要

- 組織は、ファイル共有や SharePoint サイトといった内部データ リポジトリのセキュリティを見過ごしていることが少なくありません。
- これらのリポジトリは従業員が標準の権限でアクセスできることが通例であり、認証情報、財務データ、知的財産をはじめとする機密情報が保持されている場合もあります。
- 保護されていないデータ リポジトリは、金銭目的の脅威アクターにとって恐喝の標的に、高度標的型攻撃（APT）グループにとっては諜報活動の標的になります。
- データ リポジトリが保護されていない場合、脅威アクターはマルウェアやゼロデイ攻撃といった比較的高度な手法を使用せずに（権限昇格などの）目標を達成できることが多いため、脅威アクターが所期の目的を果たすうえで越えなければならないハードルが低くなります。

必要とされる行動

- データ リポジトリのインベントリ作成と監査を実施します。機密データの保存場所を特定し、そのコンテンツを定期的に再確認し、不要なデータや古いデータを削除します。
- 職務に必要なアクセス権のみがユーザーに付与されていることを確認し、読み取りアクセスと読み取り / 書き込みアクセスを区別し、包括的な権限を付与しないようにします。
- データ セキュリティのベスト プラクティス、機密データを保護することの重要性、データ漏洩事案を報告する方法について従業員向けのトレーニングを実施します。
- 転送時と保管時はいずれもデータを暗号化して、情報漏洩を抑制します。
- 公開されている認証情報とシークレットを自動化ツールで特定し、定期的なセキュリティ評価を実施して管理の効果を評価します。
- 重要なデータストアへのあらゆるアクセス試行について、FIDO2 準拠の多要素認証（MFA）を必須のセキュリティ対策として導入します。
- データ損失防止（DLP）のテクノロジーを導入して、機密データが安全な環境からメールやファイル共有を介して外部に出ることを効果的に防止します。

レポート全文をダウンロードする

サイバー インシデントが疑われる場合や、セキュリティ侵害が発生した場合は、Mandiant のインシデント対応のサポートにお問い合わせください。

Google Cloud

詳細: cloud.google.com