セキュリティー侵害の解剖

組織におけるサイバー
攻撃の事後分析

HashiCorp
an IBM Company

内容

エグゼクティブ・サマリー

「この仮説的な事後分析は、実際のセキュリティー侵害の例から組み立てられたものです」

あなたの組織がハッキングされました。何が起きたのか、攻撃者がどのようにシステムへアクセスしたのか、そして今後同様のインシデントを防止する方法を明らかにすることが求められます。

この恐ろしい、しかしあまりにもありふれたシナリオがこのホワイト・ペーパーの基礎となっており、架空の組織で大規模なサイバーセキュリティー侵害が発生した後に行われた仮説演習を説明しています。この演習では、有名な**MITRE ATT&CKフレームワーク**（敵対者の施策に関する世界的にアクセス可能な知識ベースと現実世界の観察に基づく手法）を活用して、攻撃者が使用する具体的な施策を理解し、脆弱性を特定して、将来の攻撃を阻止するために迅速に対処できるようにします。

MITRE ATT&CKフレームワークを使用した事後分析では、攻撃者が使用した5つの主要な施策を特定し、それぞれが攻撃者によってどのように使用されたかをレビューし（実際の組織での現実世界の侵害に照らして）、今後脆弱性を解消するために新たなプロセスやテクノロジーの導入に取り組む方法について示します。ホワイト・ペーパーでは、最新のアーキテクチャ向けに意図的に設計されたHashiCorpソリューションなど、さまざまなプロセスやテクノロジーの変更によって、データ侵害によるセキュリティの脆弱性をどのように修復できるかをレビューします。提示された事後分析は架空のものですが、実際のセキュリティー侵害の例から組み立てられており、レビューでは実際の組織に対してサイバー攻撃がどのように行われたかについて、文書化された施策を検証しています。

このアプローチは、今日のセキュリティの脆弱性を理解し、修正する際の難しさを明らかにするのに役立ちます。世界がクラウド、マルチクラウド、ハイブリッドアーキテクチャへと移行するにつれ、データセンターの周囲の境界を防御する必要性によって定義される従来の静的および IP ベースのセキュリティは、保護すべき明確な境界がなくなったため時代遅れになりつつあります。今日の動的なクラウドネイティブ・インフラストラクチャは、人間、サービス、デバイスによるリモートの一時的アクセスへの依存度が高まっていることが特徴で、パブリックにアクセス可能になり、常に敵対者によって積極的にスキャンされている可能性があります。これらの環境を保護するには、企業はよく理解されているセキュリティ技術を超える動きを取り、ゼロトラストや最小特権アクセスなどの新しいアプローチを採用した動的で ID ベースのモデルに移行する必要があります。

困難が増すにつれ、危険度はかつてないほど高くなっています。今日のサイバー攻撃は、コア・ビジネス・オペレーションに影響を及ぼし、数千万ドルもの自己負担、収益の損失、評判へのダメージ、さらには官公庁・自治体への罰金さえももたらす可能性があります。プラットフォームとセキュリティのチームは、ユーザーと顧客が引き続き必要なサービスにアクセスできるように、システムとアプリケーションの安全性、セキュリティ、性能を確保しながら、アジャイルのビジネス・プロセスと最新のテクノロジー・アーキテクチャを有効にするために次に進む必要があります。

侵害の調査 – 今後の事後分析

組織への侵入により重大な損害が発生しました。

– 顧客の個人情報とクレジットカードデータが抽出されました。
– 今後発売される製品のソースコードが盗まれました。
– 運用データレイクがランサムウェアによって暗号化され、すべてのビジネス活動が停止されました。
– ビジネスへの影響は数百万ドルに及びます。

「攻撃者はどのように侵入したのか？」をはじめ、答えなければならない質問がたくさんあります。

この悪夢のようなシナリオは、何千もの企業にとって冷酷な現実です。ですから、あなたに同じことが起こったとしても、それほど驚くべきではありません。

「攻撃者はどのように侵入したのか？」をはじめ、答えなければならない質問がたくさんあります。あなたは、プラットフォーム・オペレーション、セキュリティ、エンジニアリング・チームのメンバーから構成されるタスク・フォースの一員です。このタスク・フォースは、攻撃者がどのようにシステムにアクセスし、環境内でどのような動きを取り、機密データを盗んだかを迅速に把握し、セキュリティの脆弱性に速やかに取り組むために結成されました。チームの目標は、何が起こったのかを理解し、将来の攻撃から特定された脆弱性を解消するための新しいプロセスとテクノロジーを実装することです。

何よりも避けるべきことは、起こったことの再発です。そのため、攻撃者が何をしたか、また、テクノロジーやアーキテクチャの変更が、発見した脆弱性に対処するための選択肢にどのような影響を与えるかを理解することが重要です。

MITRE ATT&CK フレームワークの使い方

チームはログと監査証跡を精査し、攻撃者がシステムにアクセスするために使用した様々な施策を再構築してきました。作業を整理すべく、チームは広く使用されている**MITRE ATT&CKフレームワークを採用し**、攻撃者が使用した様々な施策と手法を分類しました。これにより、今後これらの脆弱性にどのように取り組むべきかをより深く理解できるようになります。

MITRE ATT&CKフレームワークは、実世界の観察に基づいたサイバー攻撃の施策とテクニックに関する知識ベースを収集したものです。ATT&CKはAdversarial Tactics、Techniques & Common Knowledgeの略語で、どのような攻撃行動が行われたかだけでなく、攻撃者が何を達成しようとしているのかという根底にある**動機**を特定するのに役立ちます。

このアプローチは、具体的な軽減施策の概要を説明し、今後の環境をさらに強化するためのより大規模なポリシーやインフラストラクチャ設計ストラテジーについて考察するするのに役立ちます。

今後に向けた脆弱性の軽減

「Amazon S3バケットの設定が誤っている場合、それが発見され、ネットワーク上に攻撃者が現れるまでに16分もかかりません。私たちは、今日では異なる視点で考察する必要があります」

Michael Wood、
HashiCorp現場CTO

チームの最優先事項は、まだ残っている脆弱性を迅速に解決することですが、2番目の優先事項は、将来にわたって耐えられる方法で解決することです。あなたの会社は急速に成長しており、テクノロジー・ストラテジーも進化しているため、この危機はより耐久性のあるセキュリティ対策を構築する機会となっています。

「事後分析の結果、システムのテクノロジーと設計は変更されていますが、セキュリティのテクノロジーと手順が追いついていないことが判明しました」

これまでの事後分析により、セキュリティ・テクノロジーと手順がシステム・テクノロジーと設計の進化に追いついていないことが明らかになりました。新たなセキュリティ課題をもたらす新しいテクノロジーのアプローチには、次のようなものがあります。

- **クラウドネイティブ・アーキテクチャ：**システム設計は、パブリックのマルチクラウド・コンテナ化アーキテクチャに基づいて進化し、その周りに構築されたよりアジャイルなDevOpsプロセスを備えています。
- **一時的なインフラストラクチャ：**最新のインフラストラクチャとシステムは、技術ニーズとビジネスニーズに迅速に対応するために、オンデマンドでプロビジョニングおよび廃止されます。
- **動的なワークロード：**現在、ワークロードは、さまざまな要件を満たすために、さまざまなリージョン、アベイラビリティ・ゾーン、パブリッククラウド・ベンダーに迅速に移行しています。

クラウドネイティブ・アーキテクチャー向けの最新セキュリティー体制の開発

システム・アーキテクチャが進化するにつれて、セキュリティー・モデルもそれに追いつくために変更する必要があります。以前は、データセンターの運用は、エンドポイントにIP 所在地を使用でき、ユーザーはLDAP、 Active Directory 、または同様のソリューションを使用できる、より閉鎖的な環境を提供していました。この城と堀のアプローチにより、これらの環境の静的かつ永続的なニーズに適したセキュリティ設計が提供されました。

最新のデータセンターとクラウド・インフラストラクチャには、最新のセキュリティー・ストラテジーが必要です。パブリッククラウドは定義上パブリックであり、外部エンティティから常にアドレス指定可能なIPを持ちます。これらのIP範囲は継続的にスキャンされており、敵対者にとって豊富な攻撃対象領域を提供します。マルチクラウド、マイクロサービス、一時的なリモートアクセス、急速に変化する環境の世界では、ファイアウォールの内側か外側かという概念はもはや意味がありません。すべてのアクセス要求は、送信元に関係なく、明確に認証および承認される必要があります。

ゼロトラストセキュリティへの動き

こうしたシステム・アーキテクチャの変化を受けて、チームや組織は、アプリケーションとインフラストラクチャを管理するためのゼロトラスト・セキュリティ・アプローチに移行しています。最新のパブリッククラウド・アーキテクチャにより、ネットワークBoundaryがより流動的になりました。ファイアウォールで保護された固定境界に依存し、外部のすべてが禁止され、内部のすべてが信頼されるという状況は、今日のクラウドネイティブ、一時的、動的システム・アーキテクチャの設計と一致しません。

明確な信頼の境界がなくなった場合は、機械と人間のやり取りを認証および承認するための別のアプローチが必要になります。ゼロトラスト・セキュリティ・モデルは、データセンターの静的およびIPベースのセキュリティをクラウドの動的なIDベースのセキュリティと交換します。このIDベースのアプローチにより、認証、認可、アクセスの一貫した標準を確保しながら、ソースに関係なく、複数のデータセンターや異なるパブリッククラウドにわたってすべてのアクティビティが管理されることが保証されます。

私たちの仮想的な事後分析では、セキュリティ・チームは、将来に向けたこれらの構造的なテクノロジーとセキュリティの変更を念頭に置きながら、現在のセキュリティの脆弱性を解消することと調和させています。

セキュリティのアプローチは、システム・アーキテクチャに合わせて進化する必要があります。

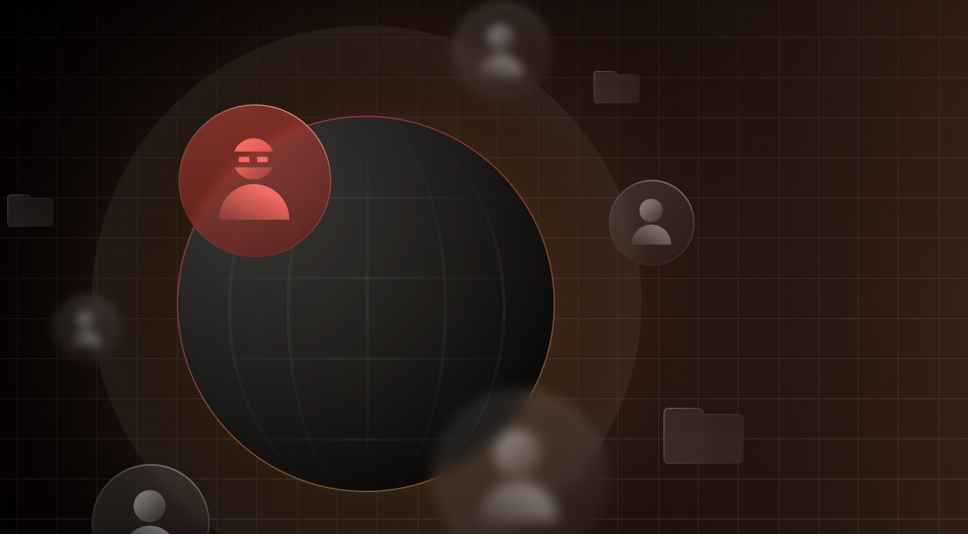
MITRE ATT&CKフレームワークを用いて、皆さんのチームは攻撃者がシステム内で動きまわるために使用した主要な施策 5 つを整理しました。また、事業の状況を踏まえた脆弱性への取り組み方を検討するとともに、今後それらのリスクにどのように取り組むべきかを評価しました。

事後分析

サイバー攻撃の解剖（MITRE ATT&CKフレームワーク）

ステップ1

初回アクセス



施策
敵はあなたのネットワークに侵入しようとしています。**この手法には、**フィッシングEメール、エクスプロイト公開アプリケーション、およびドライブバイ侵害が含まれます。

攻撃に利用される初期アクセスの例

RSA では、中堅社員に悪質なフィッシングEメールが送られ、社員のコンピュータにバックドアが仕掛けられていました。

ソニー・ピクチャーズでは、攻撃者が上級社員になりすまし、偽のApple ID認証ログインEメールを使用して、ソニーのネットワークでも使用されているパスワードを探りました。

当社への攻撃にその手口が使われた方法
一部の請負業者とのトレーニングセッションの一環として、キーとパスワードが盗まれ、ハードコードされた一連の秘密が誤って公開コードリポジトリに漏洩しました。攻撃者はこれを利用して、企業ネットワークに接続できるサンドボックス・システムへの最初の侵入を獲得しました。

問題を理解する
事後調査の結果、組織では秘密の拡散が問題となっており、GitHubリポジトリやAWS構成マネージャーなどの複数のクラウド・システムに秘密が散在していることが判明しました。一部の秘密ストレージ・サービスは個々のチームによって使用されるため、秘密のライフサイクル全体の追跡に問題が発生します。これらのサービスは、秘密情報を安全に保管し、保存時に暗号化しますが、秘密情報のバージョン管理、定期的な秘密情報のローテーション、全体的な管理はサポートしていません。環境全体でハードコードされた秘密をスキャンするプログラム的な方法はありません。

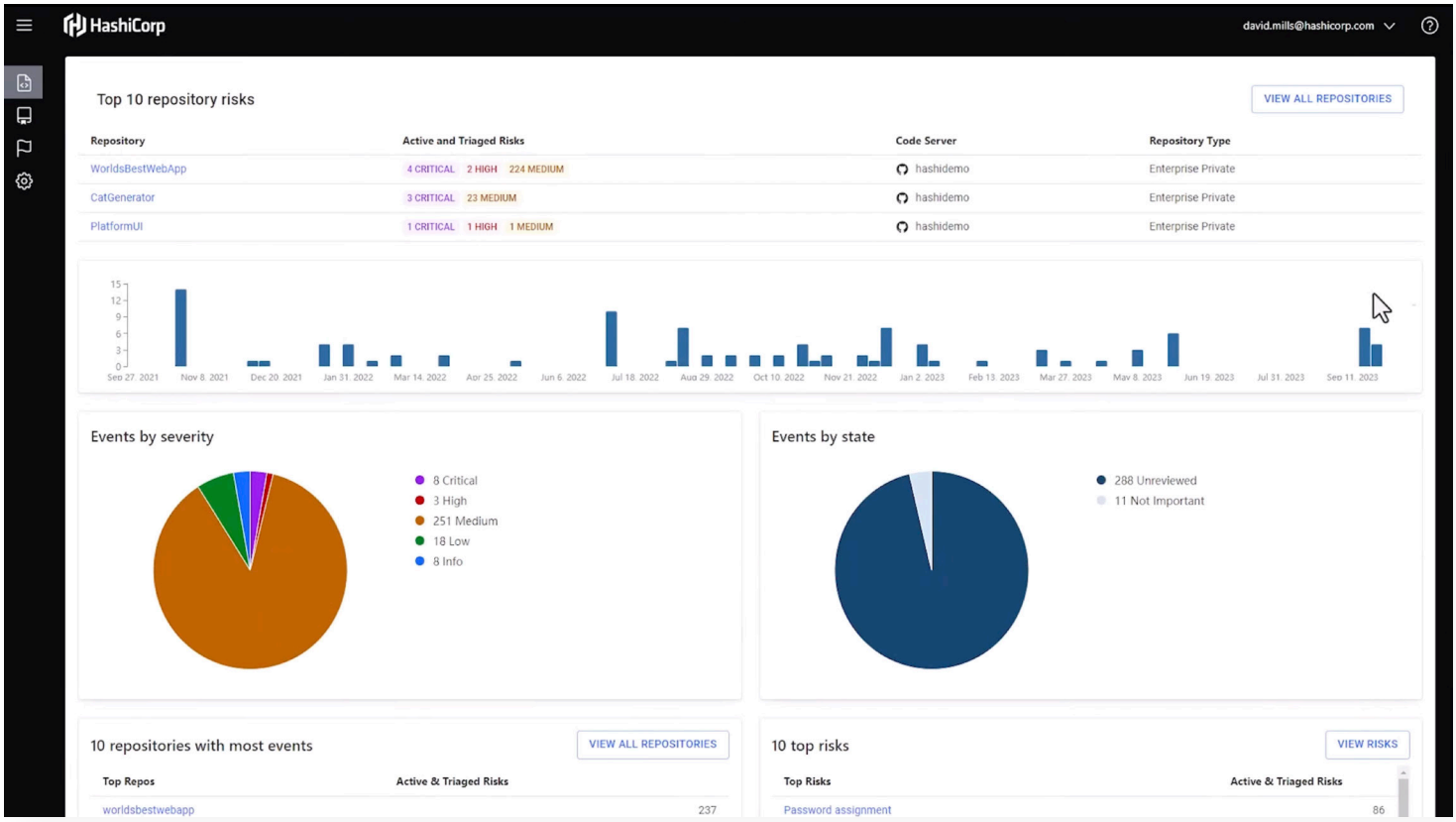
推奨事項
秘密のライフサイクルを管理し、安全なアクセスを実現するには、より集中化されたアプローチが必要です。

– 不適切に保管されたり、公開されたりする可能性のある秘密をスキャンして見つけ出し、すぐにアクセスを取り消します。
– 認証情報が漏洩するリスクを防止または軽減するために、ジャストインタイムまたは使い捨ての認証情報を提供および使用します。
– アクセスの範囲をより細かく設定するために、デフォルトで**最小権限アクセスを有効にします。**

HashiCorpによるセキュリティ脆弱性の修復
秘密管理に対する不十分な管理に取り組むためには、秘密と認証情報を管理するための新しいアプローチが必要です。盗難されやすい静的で永続的な認証情報の代わりに、 Hashicorp Vaultジャストインタイムの動的な認証情報を可能にします。認証情報は、時間制限があり、ジョブに対して細かくスコープ設定でき、異なるジョブに合わせて簡単に変更できます。これは、現代のシステムの一時的かつ動的なインフラストラクチャに類似しています。

さらに、 **HCP Vault Radarは**、ソースコード、 Gitリポジトリ、コラボレーションツールなど、ネットワーク全体に誤って公開されたシークレットをスキャンして検出し、Vault内でローテーションまたは保管することができます。Vault内で管理されているシークレットのデータ参照は、スキャンで検出された管理されていないシークレットと相関付けられるため、適切な修正を行うことができます。この場合、Vault外に公開されたシークレットを直ちに削除し、Vault内で管理されている対応するシークレットをローテーションする必要があります。

IDベースのセキュリティ制御により、セキュリティの層をさらに強化できます。ユーザーは、当社の既存のアイデンティティ・サービス・プロバイダーでシングル・サインオン・アクセスを認証し、HashiCorp Boundaryを使用して承認されたシステムに自動的にアクセスできます。ユーザーは、さまざまなシステムにアクセスするために、複数のキーとパスワードを確認したり、保管したり、コピー／貼り付けしたりする必要がなくなり、秘密が漏洩するリスクが低減します。代わりに、Boundaryによって、使い捨ての動的認証情報がユーザーセッションに目に見えない形で挿入され、よりシンプルで安全なパスワード不要のアクセスが可能になります。



HCP Vault Radarは、コード・リポジトリを含むさまざまな場所で秘密をスキャンします。

ステップ 2

特権エスカレーション

施策
敵はより高いレベルの権限を取得しようとしています。**この手法には、**有効なアカウントの探索、プロセス・インジェクション、およびアクセス・トークンの操作が含まれます。

攻撃で使用されている権限昇格の例

SolarWinds攻撃では、侵害されたSolarWinds Orionソフトウェアが、Active Directory、インフラストラクチャ・システム、さらにはSAMLシステムなどの他のTier 0 システムへの認証情報を収集するために使用されました。

Linux上のBashにおける**Shellshock**権限昇格の脆弱性により数百万のシステムが侵害され、侵害されたシステムのボットネットによって1日あたり数百万件の DDoS攻撃が実行されました。

当社への攻撃にその手口が使われた方法
サンドボックスへの最初のアクセスから、攻撃者はこのアクセス・ポイントを使用して、システム内に存在する請負業者のさまざまな認証情報を調べました。彼らは、より特権的なアクセス権を持つ新しい認証情報を作成し、ネットワークのより深い部分にアクセスできるようになりました。

問題を理解する
当社のセキュリティ対策を分析したところ、多くのユーザーが、特にクラウド・インフラストラクチャ全体で、必要以上の権限を付与されていることが判明しました。ユーザー・アカウントを監査すると、多くのユーザーが、アクセス可能であってはならない企業の**信頼のルートに**アクセスできることが判明しました。こうした権限が緩いアカウントとポリシーは、攻撃者がキー管理システム（KMS）やハードウェア・セキュリティー・モジュール（HSM）などの最初の信頼のルートや侵害されたユーザー・アカウントにアクセスできるようになると、最初の認証情報を超えて、ネットワーク参考情報、データベース、その他の重要な資産へのより高いレベルのアクセスを持つ追加のシークレットを作成できることを意味します。過度にエスカレートされた権限によって従来の特権アクセス管理（PAM）システムを回避することさえ可能になります。複数のクラウド・プロバイダーやシステム・インフラストラクチャにまたがるこの管理は、さらに複雑になります。

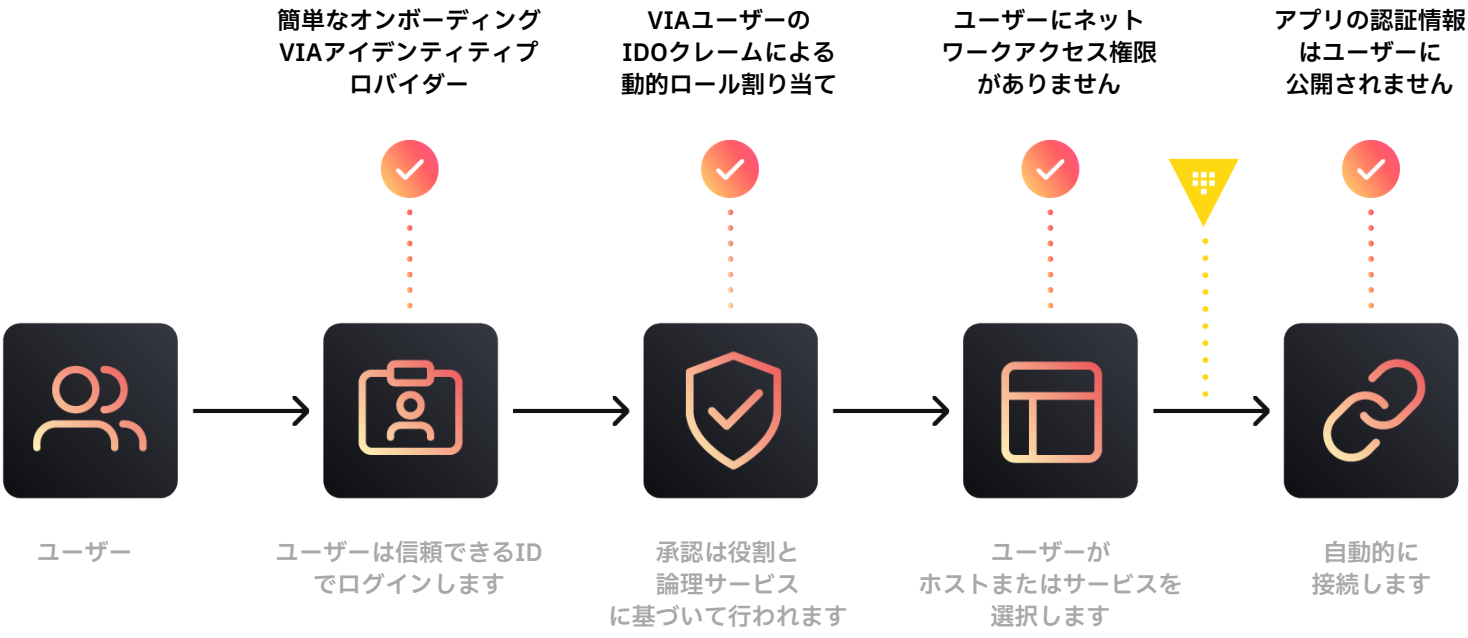
推奨事項
最小権限アクセスの原則に従い、ユーザーの生産性に影響を与えずに、権限の粒度を上げ、認証情報の有効期間を短縮します。

- 過度に広範囲で不必要な権限を拡張することなく、特定のジョブに対して適切なサイズの権限を設定します。
- 静的で永続的な認証情報から離れる動きを取り、ジャストインタイムで有効期間の短い認証情報を発行することで、攻撃対象領域を縮小します。
- 認証情報を簡素化し、より集中化された管理システムに移行することで、より一貫性のある制御が可能になります。

HashiCorpによるセキュリティ脆弱性の修復
この侵害により、認証情報の管理方法に対するアプローチを変更する必要があることが明らかになりました。アクセス・ポリシーを手動で構成するのは時間がかかり、特に複数のクラウドとインフラストラクチャにまたがって大規模に管理するには複雑すぎるため、このプロセスを管理するには一元集中型のソリューションが必要です。

Hashicorp Vaultは、認証情報の漏洩を防ぐために、一時的でオンデマンドの動的シークレットの作成と取り消しを提供します。これは、企業全体の集中型IDブローカー、秘密管理プラットフォーム、および暗号化サービスとして機能します。安全なユーザー・アクセスを実現するために、HashiCorp Boundaryはユーザーがシステムにログインするたびに権限を評価し、特権アクセスを大規模に適正化することを支援します。

Boundaryを導入すると、特権アクセスはVPNや要塞ホスト・アプローチよりも安全かつスケーラブルになります。ワーカーをネットワークへのエントリー・ポイントとして使用することで、攻撃対象領域を縮小します。また、Vaultは秘密を集中管理することで、秘密の拡散を制限します。



Hashicorp BoundaryとVaultを使用して認証と承認を簡素化し、セキュリティを強化します。

ステップ 3

認証情報：アクセス

施策
敵はアカウント名とパスワードを盗もうとしています。**この手法には、**ファイル内の認証情報の収集、OS認証情報のダンピング、およびキーロギングが含まれます。

攻撃に利用される認証情報アクセスの例

CircleCI では、従業員のノートPCにインストールされたマルウェアが有効な2FAバックアップSSOセッションを盗むために使用され、そこから従業員の運用アクセスが実行中のプロセスから運用の暗号化キーを抽出するために使用されました。

世界的な **WannaCry** ランサムウェア攻撃は、一般的に使用されている **Mimikatz** ツールを介した認証情報ダンプを活用して、侵害されたマシンから認証情報を収集し、さらにネットワークに拡散します。

当社への攻撃にその手口が使われた方法
攻撃者は、システムへのより深いアクセスを実現する一連の認証情報を使用して、共有ネットワーク・ドライブ上で認証情報を発見し、それを使用して管理者アクセスを持つ別の認証情報セットを作成し、ルート・アクセスを取得しました。

問題を理解する
システムの複雑さと規模の増大により、認証情報セットが大幅に拡散し、攻撃対象領域が拡大します。認証情報はあまりにも多くのシステムで保管されており、複雑さと煩雑さがさらに増大しています。市場の需要に対応するため迅速な動きを求められるというビジネス上の圧力の下で、ユーザーは利便性を優先し、認証情報を安全でない方法で保管してしまうことがあります。その結果、組織は脆弱な状態に置かれます。

推奨事項
正しい行動をより簡単にすることで、認証情報を公開したままにするなど、リスクの高いセキュリティの近道をユーザーが取らないようにします。

- 既存の ID プロバイダー（IdP）を通じて、ユーザーのシステムへの認証と承認を自動化します。
- 静的で広範な認証情報を置き換えて、一時的で範囲が限定された認証情報に移行し、攻撃ウィンドウを縮小します。
- 複数のクラウド・プロバイダーおよびシステム全体でキーを管理する集中化および標準化された方法をデプロイして、一貫性を高め、機密漏洩を防ぎます。

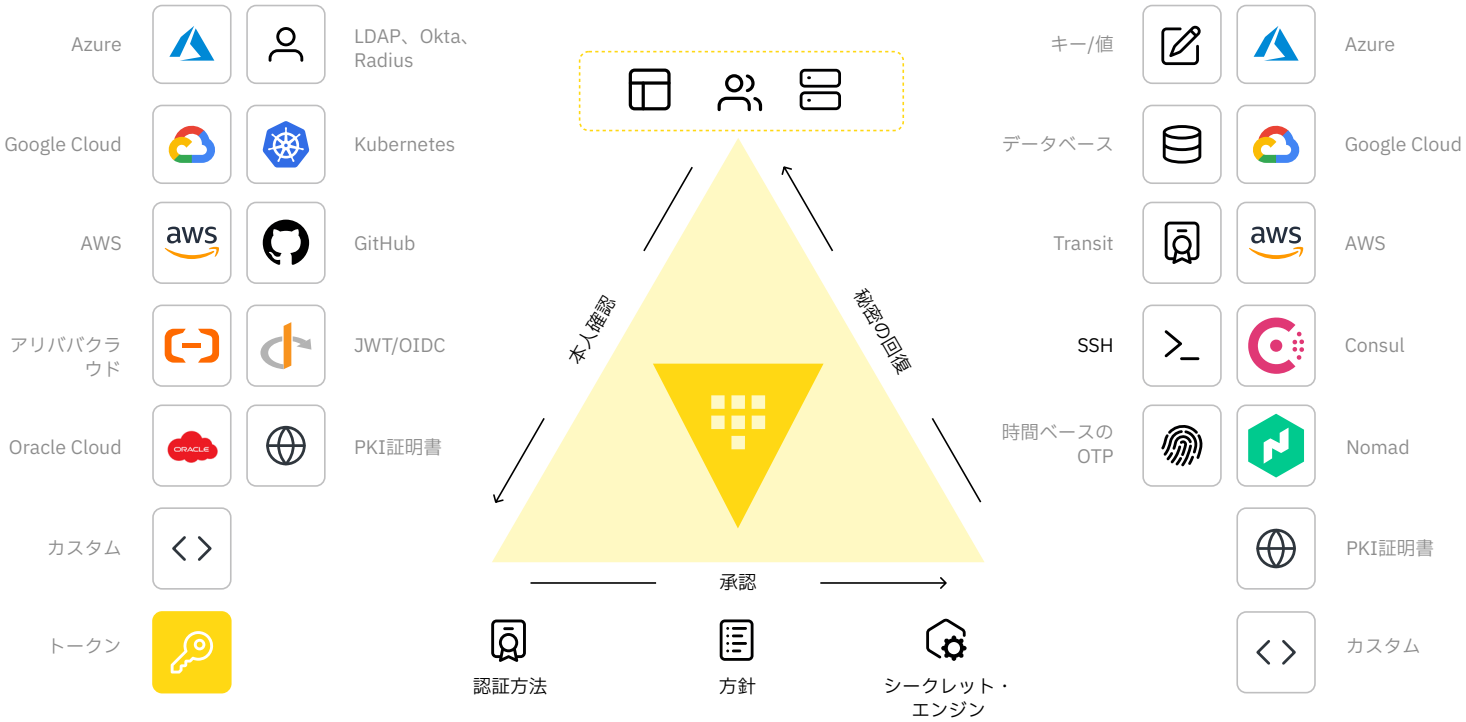
HashiCorpによるセキュリティ脆弱性の修復
ユーザーは、既存の ID プロバイダー（Okta、Kubernetes、Active Directoryなど）に認証してHashicorp Vaultにアクセスし、そこから必要なシステムやシークレットにアクセスできます。これは、ユーザーがすでに使い慣れている既存のIdPワークフローにうまく統合されます。

Vaultを使用すると、追加のインフラストラクチャで断片的で複雑なキー管理を採用することなく、認証情報、キー、その他の秘密を安全に保管および管理できます。Vaultを使用すると、シークレットの生成、ローテーション、有効期限切れを自動化して、静的シークレットの長期的な公開を制限できます。

最後に、 **Vault Secrets Syncは**、さまざまな KMS プロバイダーにわたるマルチクラウド環境でのキーの配布とライフサイクル管理のための API と標準化されたワークフローを提供します。各クラウド・プロバイダーの KMS サービスでキーを管理する代わりに、Vault Secrets Sync は、すべてのクラウドにわたるすべての暗号化キーの統一されたコントロール・ポイントを提供します。これらはオンデマンドで一元的に生成され、簡単にローテーションできると同時に、AWS KMS、 Microsoft Azure Key Vault、GoogleクラウドKMSなどのさまざまなKMSプロバイダーにネイティブな独自の暗号化機能も活用できます。また、Vaultは、コンテナ化された Kubernetesシステムでシークレットをネイティブに取得および同期するための安全な暗号化された方法を提供し、各サービスが一意に認証し、独自の認証情報を要求できるようにします。

さらに、HashiCorp Boundaryを活用して、認証情報をエンド・ユーザーに公開することなく、使い捨ての動的な認証情報をユーザー・セッションに挿入することで、システムへのパスワードレス・アクセスを実装し、紛失または盗難のリスクを軽減できます。

クライアント、人間、または機械



Hashicorp Vaultは、さまざまなシステムやクラウドにわたるシークレットを一元管理します。

ステップ 4

横方向動き

施策
攻撃者は、環境内で動きを広げようとしています。**攻撃手法には**、Pass-the-Hash、リモートデスクトッププロトコル、Windows管理者共有などがあります。

横移動が攻撃に利用される例

Target では、攻撃者はHVAC請負業者の認証情報を使用して、外部ポータルシステムから企業ネットワークへと動きを広げました。

マリオットは、スターウッド事業の買収前、数年にわたるスターウッドでの情報漏洩により、クレジットカードやパスポートなど数億件の顧客記録が流出したと発表しました。

当社への攻撃にその手口が使われた方法
攻撃者は、当社のネットワークにさらに侵入すると、環境内を動き回り始めました。彼らはネットワークをスキャンし、おそらくエクスプロイトする価値の高いシステムを探していました。また、彼らはさらに多くのシステムにアクセスし、リモート・デスクトップ接続などの手法を使用して、より多くのサーバーに侵入し、ランサムウェアをインストールしました。

問題を理解する
私たちの城と堀のセキュリティー体制は、一度私たちのネットワークに入ると寛容です。ネットワーク内の任意のシステムまたはユーザーは、ネットワーク内の他のすべてのシステムを自由に見ることができます。たとえ1つのシステムが侵害されたとしても、攻撃者が他のシステムにアクセスして侵害するための重要な足掛かりを与える可能性があります。

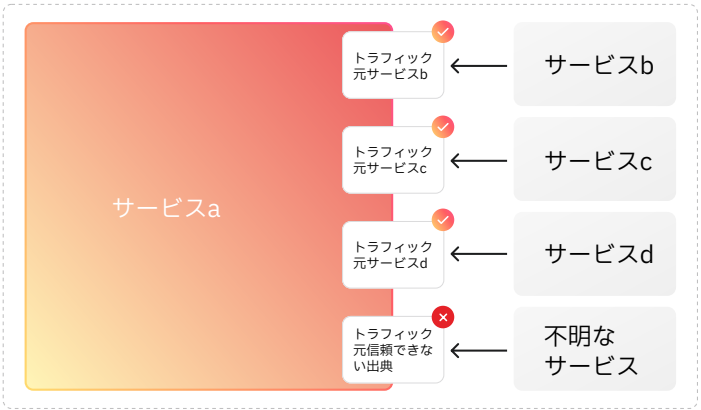
推奨事項
ゼロトラストのセキュリティ原則を採用して、システムのアクセスの粒度と範囲を拡大します。これにより、システム間の移動を防ぐことができます。

– サービスとアプリケーションの範囲をネットワーク全体ではなく特定の定義済みエンドポイントのみに限定するネットワーク・ルールを確立し、侵害されたサービスが他のサービスに影響を与えるのを防ぎます。
– 従業員がネットワーク上のすべてを閲覧（またはアクセス）できないように、従業員のアクセスを管理します。境界外で信頼のルートを確立した攻撃者はネットワークに侵入し、侵害された従業員アカウント1つによってシステム全体を公開できるようになります。
– 大規模に管理するには、このシステムを自動化する必要があります。現代の環境はますます複雑化しており、手動で追跡して保護するアクセス・ポイントが多すぎます。

HashiCorpによるセキュリティ脆弱性の修復
当社のインフラストラクチャにゼロトラスト・セキュリティー体制を採用すると、攻撃の爆発範囲を大幅に制限できます。HashiCorp Boundaryを使用すると、ユーザーをネットワークから完全に遮断して、ネットワークをより安全に保つことができます。ユーザーはファイアウォール内のHashiCorp Boundaryワーカーに接続し、ターゲット・システムへの安全な直接接続を仲介して、ジョブに必要な秘密を動的に挿入できるようになります。ユーザーは、VPNを使用してネットワークにアクセスする必要がなくなり、悪意のある人物に漏洩する可能性のある長期の秘密を管理する必要がなくなります。Boundaryは、ユーザーがアクセスできるシステムの範囲も制限します。

HashiCorp Vault は、TLS 証明書を発行する前に、適切な認証方式を用いて各サービスの ID を検証する証明機関（CA）としてもデプロイできます。証明書の作成、署名、更新のプロセスも自動化できるため、スケーリングとセキュリティが向上します。Vaultの集中管理により、認証情報を特定のターゲット・システムに限定して取得できます。たとえば、ユーザーが使用しているLinux システム上の1つのアプリケーション・プロセスへのユーザー・アクセスを制限し、ホスト上の他のLinuxプロセスへのアクセスを許可しないようにすることができます。このきめ細かな制御により、侵害を受けたユーザーやマシンがシステム内で横方向に移動するのを防ぐことができます。

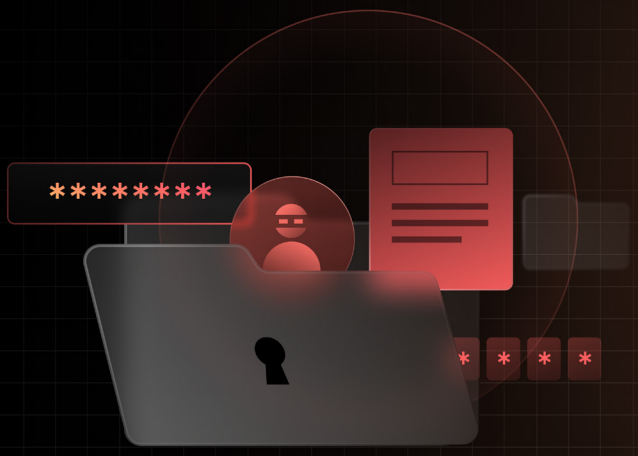
HashiCorp Consulによって明示的に許可されない限り、すべてのサービス間通信を拒否することで、ネットワーク・サービスは最小権限アクセスに対してさらに強化できます。各アプリケーション・エンドポイントは一意に識別、認証、承認され、それらの間のチャネルはTLS証明書で暗号化されます。たとえ攻撃者が特定のアプリケーションの弱点にアクセスできたとしても、横方向に動き回る能力は限られており、暗号化により傍受されたネットワーク通信は閲覧できなくなります。



HashiCorp Consulによって明示的に許可されない限り
サービス間通信は拒否されます。

ステップ 5

外部転送



施策
攻撃者はデータを盗もうとしています。**その手法には、**既存のコマンド制御チャネルや、代替プロトコルまたは自動抽出によるデータ移動が含まれます。

流出の例
攻撃に使用されている

Equifaxデータ侵害の際、氏名、社会保障番号、生年月日、所在地など1億4,500万人以上の個人情報が、通常のネットワーク・トラフィックを装う標準的な暗号化Webプロトコルを使用して少しずつ盗まれました。

Shields Healthcare Groupのデータ侵害では、影響を受けたデータには、名前、診断情報、治療計画、医療提供者情報、保険情報などが含まれている可能性があります。

当社への攻撃にその手口が使われた方法
攻撃者はルートアクセスを使用してアカウントを作成し、そのアカウントを使用して当社の顧客支払いデータベースを呼び出し、データを取得しました。その後、そのデータは少しずつ外部システムにルーティングされ、検知を回避しました。

問題を理解する
当社のセキュリティー体制は、暗号化データの解読を困難にする高度な暗号化アプローチにHSMを使用するなど、保存時の暗号化だけでなく転送時の暗号化にも参考情報を投資しています。ただし、信頼できるIPが有効なリクエストを送信し、HSMがすべてのデータを復号化してプレーンテキストで配信した場合、データは依然として脆弱なままとなり、簡単に盗まれる可能性があります。

推奨事項
暗号化ベスト・プラクティスと連携し、データへのアクセスと復号化方法に関する追加のセキュリティ層も実装します。

- データベースへのアクセス認証に関する追加の保護を実装し、侵害された信頼できるシステムが機密データを直接抽出できないようにします。
- データの追加のパーティションとスコープを実装して、内部アプリケーションや従業員であっても、より大きなデータ・ストア全体にアクセスできないようにします。

HashiCorpによるセキュリティ脆弱性の修復
暗号化ストラテジーの改善は、テクノロジーの観点からだけでなく、プロセスの観点からも必要です。Hashicorp Vault暗号化サービス・エンジンとして活用することで、データがデータベースに保存される前に暗号化できるようになります。つまり、データベースのユーザーIDパスワードを持っているだけでは不十分で、ユーザーはVaultで認証される必要があり、データを復号化するにはVaultトークンが必要になります。これにより、攻撃者は2つのシステムを破る必要があるため、データを盗み出すことがより困難になります。

Vaultは、データ・アクセスの範囲設定と分割にさらなる粒度を提供します。大規模なデータレイクやデータベースは多くの異なるアプリケーションで共有でき、Vaultを使用して異なるアプリケーションの異なるキーを一元的に定義できます。データの列または行は、異なるスコープ・アクセスを使用して異なる方法で暗号化できます。この制御の粒度は、ネットワーク内または内部従業員による攻撃から保護するのに役立ち、金融、医療、官公庁・自治体などの高度に規制された業種・業務において安全です。

アプリケーションごとにキーを管理するのはすぐに面倒になりますが、これをVaultにオフロードして集中管理、制御、監査を行うことができます。Hashicorp Vaultと Consulは、256ビットAESによる暗号化サービス（AES-GCM）を使用して、転送中および保存中のデータを保護します。

最後に、Boundaryセッション記録により、セキュリティ管理者はセッションを再生できます。これは、侵害が発生した後に特に重要です。セッション記録は、コンプライアンス要件を満たすのに役立つだけでなく、管理者が攻撃者が実行したコマンドやアクションを正確に確認できるようにすることで、修復を迅速化するのに役立ちます。特に、セッション記録は攻撃の5つのステップすべてに取り組むうえで役立ちます。

アイデンティティ駆動型制御

HashiCorpを使用した人間だけでなくマシン全体にわたるID主導の制御は、データ・セキュリティの維持に役立ちます。

その重要性は これまでになく 高まっています

セキュリティー侵害の影響はこれまで以上に大きくなっています。大規模なデータ侵害が発生すると、被害者は修復に数百万ドルの費用を負担する必要があり、顧客の信頼を大きく損なう可能性があります。また、組織がコア・ビジネスオペレーションのために自社のシステムとインフラストラクチャへの依存度を高めるにつれ、たとえデータが失われていないとしても、サイバー攻撃によるサービスの中断は壊滅的な影響を与える可能性があります。システムを修復し、データ侵害の影響に対処するには、特に組織のセキュリティと進行中の他のすべてのビジネスクリティカルなプロジェクトや取り組みとのバランスを取りながら、数か月の作業が必要になる場合があります。

「組織がコア・ビジネスオペレーションのインフラへの依存度を高めるにつれ、たとえデータが失われていないとしても、サイバー攻撃によるサービスの中断は壊滅的なものになる可能性があります」

チームの立場になってセキュリティー侵害をレビューすることは、そのようなインシデントの影響を認識し、セキュリティー体制を改善する必要がある箇所を明確にするのに役立ちます。そして、この演習で示したように、IDベースの認証と承認を使用するツールのデプロイは、このようなコストのかかる攻撃にさらされるリスクを軽減する最善の方法です。

新しいテクノロジーとプラットフォーム・アーキテクチャーによって新たな可能性が開かれる一方で、これらの新しい機能に対応するために、セキュリティ設計と原則に対する新たなアプローチも求められています。チーム、システム、プロセスをアジャイルに維持することは、オペレーションの安全性を確保しながら、将来の成長と成功に不可欠です。

IBMグループ企業のHashiCorpは、組織の速度を低下させることなく、ID ベースの制御を使用して保護、検査、接続を行うクリティカル・ゼロトラスト・セキュリティとアクセス・ソリューションを提供できます。

詳細はこちら、HashiCorpサイバーセキュリティー・ソリューションのデモを入手するには、HashiCorp営業チームにお問い合わせください： sales@bashicorp.com

2025年8月
アメリカ合衆国
で生産