クラウドストライクソリューション

CROWDSTRIKE

CROWDSTRIKE FALCON アイデンティティ保護モジュール

フリクションレスな Active Directory (AD) セキュリティ

世界中のどこにいても仕事ができるようになった現代において、フリクションレス（摩擦のない）セキュリティの実現に必要となるのは、組織のネットワーク内部または外部を問わず、すべてのユーザーを認証、認可し、セキュリティ設定とセキュリティポスチャについて継続的に検証したうえで、アプリケーションやデータへのアクセスを許可または維持する体制です。

すでにシングルサインオン (SSO) と多要素認証 (MFA) を採用済みの場合でも、まだアプリケーションのクラウドへの移行を行っている途中であっても、CrowdStrike Falcon® アイデンティティ保護ソリューションは、監査にパスしてセキュリティテストを成功させるために必要な情報と支援を提供できます。

アイデンティティ攻撃の識別 / 検知のみ、または積極的な防御、いずれにも対応できるよう Active Directory（AD）セキュリティのユースケースに応じて、Falcon は二つのアイデンティティ保護製品（Falcon Identity Threat Detection と Falcon Identity Threat Protection）をご提供しています。

要点

Falcon アイデンティティ保護ソリューションは 2 つのモジュールから構成されています：

Falcon Identity Threat Detection (ITD): AD セキュリティの第一段階として、アイデンティティのリスク分析を行い、認証システムやクレデンシャルに対する脅威をいち早く検知

Falcon Identity Threat Protection: ほぼすべての MFA/SSO プロバイダーと組み合わせて、アイデンティティ、振る舞い、リスク分析を使用し、リアルタイムの脅威防止と IT ポリシーの適用によるフリクションレスなセキュリティを実現し、リアルタイムで脅威に対抗

FALCON IDENTITY THREAT DETECTION (ITD): AD セキュリティアラート

CrowdStrike Falcon Identity Threat Detection (ITD) は、AD セキュリティの第一段階です。Falcon ITD は、ライブトラフィックを振る舞いベースラインおよびルールと比較してアイデンティティベースの攻撃や異常を可視化し、攻撃とラテラルムーブメントを検知します。不正なユーザーや、ネットワークまたはクラウド内でのクレデンシャルの動きに関するリアルタイムの Active Directory セキュリティアラートを提供します。

Falcon ITD で以下が可能になります :

- 組織のサービスアカウント、特権ユーザー、ユーザークレデンシャルをすべて表示する
- ネットワーク攻撃の検出と調査に「誰が」と言うコンテキストを加え、個々のクレデンシャルの振る舞い分析を可能にする
- すべての認証トランザクションを追跡し、リスクが高まった時（新しいシステムへのアクセスや追加の特権の付与など）またはトラフィックが異常な場合（ユーザーの通常の振る舞いパターンとは異なる場合）に警告する
- 認証段階のイベントのコンテキストにネットワークセキュリティのベストプラクティスを組み合わせることで、アーキテクチャとセキュリティチーム両方の理解を深める

ローカルのレガシーアプリからクラウド環境のスタックまで、あらゆる場所でユーザー認証アクティビティを確認することは、アイデンティティとアクセスに対する AD セキュリティを効果的に管理するための最初のステップです。

FALCON IDENTITY THREAT PROTECTION: フリクションレスな条件付きアクセス

脅威に特化した世界最大の統合データファブリックである CrowdStrike Security Cloud を利用する Falcon Identity Threat Prevention は、アイデンティティ、振る舞い、リスク分析を用いたリアルタイムの脅威防止と IT ポリシー適用により、フリクションレスなセキュリティを実現します。

これまで、認証済みユーザーを対象にする内部アプリケーションは安全だと考えられていましたが、企業間の境界が曖昧になった昨今においては、侵害されたシステムや侵害されたユーザーからアクセスできる状態になっています。

Falcon Identity Threat Protection:

- ハイブリッド環境におけるアプリケーション、リソース、アイデンティティストアへのアクセスを一元的に可視化し、制御
- アイデンティティの検証により真のアクセスインシデントを認識して自動解決することで、アラートの信頼度を向上させ、ノイズを低減
- クラウドシステムとレガシーシステム全体に対して一貫したリスクベースのポリシーを摩擦なく適用 — アクションには、ブロック、許可、監査、MFA を使用したステップアップが含まれる
- 関連する認証ログのみを保存することで、ログストレージコストのオーバーヘッドを削減

より成熟したセキュリティ運用においては、ユーザーにストレスを与えずにサービスアカウントと特権アカウントを保護できるように、ハイブリッド環境のリアルタイムでのコントロールが求められる場合もあるでしょう。Falcon Identity Threat Protection は、リスクベースのアダプティブ認証を提供することで、エンドユーザーに MFA のストレスを与えずにそのような制御を実現します。

機能比較 : FALCON IDENTITY THREAT DETECTION VS FALCON IDENTITY THREAT PROTECTION

機能	FALCON IDENTITY THREAT DETECTION	FALCON IDENTITY THREAT PROTECTION
Microsoft AD アカウント分析	○	○
Azure AD アカウント分析	○	○
インサイトと分析	○	○
セキュリティ評価	○	○
AD セキュリティインシデントの検知	○	○
ライブトラフィックの詳細なパケットインスペクション	○	○
認証と認可アクセス要求に対するリアルタイムの脅威検知	○	○
リアルタイムのクラウドアクティビティの可視性、ベースライン、AD FS および Okta または PingFederate を介したフェデレーションアクセスの監視	○	○
Okta、Azure AD、Ping のイベント分析を使用した、ほぼリアルタイムのクラウドアクティビティの可視性、ベースライン化、監視	○	○
監視または適用のためのポリシー作成	×	○
リアルタイムのクラウドアクティビティの適用（ブロック、MFA など）	×	○
Microsoft AD へのリアルタイムの適用とセキュリティで保護されたアクセス（ブロック、MFA など）	×	○
カスタム脅威検知—ポリシールールからリアルタイムでアラート作成	×	○
レポート（カスタム含む）	インシデント、アクティビティ、脅威ハンター（カスタム）の各レポートのみ	○
脅威ハンティング	○	○
API サポート	有—SIEM または SOAR ツールのみ対応	すべてに加えて SSO と MFA ツール
イベントを報告するための E メール連携	○	○
テクニカルサポート	○	○

侵害の 80% はクレデンシャルの侵害に関連しているため、Falcon アイデンティティ保護製品は、アイデンティティをセグメント化し、AD セキュリティの分析と適用を自動化することにより、セキュリティポスチャを改善します。

拡張 MFA によるセキュリティポスチャの改善：アイデンティティ検証 /MFA ツールを、レガシー / 専有システムや、従来は MFA と統合されていなかったレガシーシステム（デスクトップ、PowerShell などのツール、NTLM 経由の RDP などのプロトコルなど）を含む任意のリソースまたはアプリケーションに拡張して、攻撃対象領域を削減します。

強化されたアイデンティティストアのセキュリティ体制：アカウントをハニートークンとして指定し、攻撃経路に特化したインサイトを使用して、攻撃者を重要なリソースから安全におびき出します。SMB から DC への認証イベントを即座に可視化し、パスワードを共有するアカウントを可視化することで、クレデンシャル スタッフィングの脆弱性を軽減します。

CROWDSTRIKE FALCON アイデンティティ保護モジュール

どちらのモジュールも、以下の Active Directory 攻撃を検知します：

- アカウント列挙攻撃による偵察（BloodHound、Kerberoasting）
- Bronze Bit (CVE-2020-17049)
- ブルートフォース攻撃 (LDAP サンプルバインド、NTLM、Kerberos）
- クレデンシャルスキャン（オンプレミス）
- クラウドベースの（Azure AD）ブルートフォース / クレデンシャルスキャン
- DCSync — Active Directory レプリケーション
- DCShadow
- 特権昇格のための偽造 PAC（セキュリティ情報 MS-14-068）
- Golden Ticket
- 隠しオブジェクト検知
- NTLM リレー攻撃（MS Exchange 含む）
- Overpass-the-Hash（複数の方法 - Mimikatz、CrackMapExec）
- Pass-the-Hash（Impacket、CrackMapExec、Metasploit）
- Pass-the-Ticket
- エクスプロイトの試行 (CredSSP) CVE-2018-0886
- リモート実行の試行
- スケルトンキーと Mimikatz スケルトンキー
- 疑わしい NTLM 認証の改ざん (CVE-2019-1040)
- ZeroLogin (CVE-2020-1472)

どちらのモジュールも、以下の「不正なクレデンシャル」または異常な振る舞いを可視化します：

- アクセス禁止国からのアクセス
- 特権グループへのユーザー追加
- 異常な DCE/RPC
- Bronze Bit (CVE-2020-17049)
- ポリシールールを使用したカスタム脅威検知
- 過剰なアクセス（サーバー）
- 過剰なアクセス（サービス）
- 過剰なアクセス（ワークステーション）
- 隠しオブジェクト検知
- アイデンティティ検証の拒否
- アイデンティティ検証のタイムアウト
- サービスアカウントの誤用
- 不審な VPN 接続—ユーザーの異常なジオロケーション
- サーバーへの異常なアクセス
- サービスへの異常なアクセス
- 異常なプロトコル実装
- レピュテーションスコアが低い IP の使用
- 古いエンドポイントの使用

潜在的に悪意のあるアイデンティティトラフィックを特定する必要がある場合、あるいはリスクベースの条件付きアクセスを作成してそれに対抗する場合の、いずれにおいても、クラウドストライクはお客様に最適な製品を提供します。

デモをスケジュール

詳細については **www.crowdstrike.jp** をご覧ください。

クラウドストライクについて

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), は、サイバーセキュリティのグローバルリーダーであり、エンドポイント、クラウドワークロード、アイデンティティ、データを含む企業におけるリスクを考える上で重要な領域を保護する世界最先端のクラウドネイティブのプラットフォームにより、現代のセキュリティを再定義しています。

CrowdStrike Falcon® プラットフォームは、CrowdStrike Security Cloud を搭載し、リアルタイムの攻撃指標、脅威インテリジェンス、進化する攻撃者の戦術、企業全体からの充実したテレメトリーを活用して、超高精度の検知、自動化された保護と修復、精鋭による脅威ハンティング、優先付けられた脆弱性の可観測性を提供します。

Falcon プラットフォームは、軽量なシングルエージェント・アーキテクチャを備え、クラウド上に構築されており、迅速かつスケーラブルな展開、優れた保護とパフォーマンス、複雑さの低減、短期間での価値提供を実現します。

CrowdStrike: **We stop breaches**

詳細情報：
https://www.crowdstrike.jp/

ソーシャルメディア：Blog | Twitter | LinkedIn | Facebook | Instagram

無料トライアル：
https://go.crowdstrike.com/try-falcon-prevent-jp.html