クラウドストライク製品

CROWDSTRIKE

FALCON SURFACE: 外部攻撃対象領域管理 (EASM)

業界で最も完全な外部攻撃対象領域管理 (EASM) テクノロジーにより、公開された資産からのリスクを最小化して侵害を阻止します

組織のデジタル利用状況は、前例のない速さで拡大しています。クラウドへの移行、IoT、デジタルトランスフォーメーション、コネクテッドサプライチェーンパートナー等のトレンドは、インターネットに接続する資産、クラウドワークロード、Web サイト、ユーザークレデンシャル、S3 バケット、SSL 証明書、IoT、オペレーショナルテクノロジー (OT)、不正な IT デバイスなどの爆発的な増加をもたらしています。現在、デジタル資産の大半は、従来の企業インフラの外にあり、IT チームの直接的な管理の対象外となっています。

インターネットに接続されている資産があるということは、データ侵害につながる潜在的なリスクが存在する可能性があることを意味します。それらの資産の多くは脆弱性を抱えており、攻撃者は、インターネットに接続された資産を発見し、それを悪用するために偵察方法を改良し続けています。そのような攻撃者が脆弱性を発見する技術は、しばしばデジタル資産に対して適切なセキュリティハイジーンを施そうとする組織の能力を凌駕することがあります。残念なことに多くの場合、攻撃者はターゲット自身よりもターゲット組織のリスクエクスポージャーをよく理解しています。

CrowdStrike Falcon® Surface は、インターネットに接続され露出状態にある未知の資産を特定し、セキュリティチームが日々進化するデジタル境界を保護できるようにします。これにより、オンプレミス環境、子会社、クラウド、サードパーティーベンダーにまたがる中央集中型やリモート型のインターネットに露出したすべての資産を、ゼロタッチのアプローチで検出、優先順位付け、管理することができます。

Falcon Surface のインテリジェントなインターネットマッピングおよび関連付けテクノロジーは、インターネット全体を継続的にインデックス化し、企業の既知および未知の資産を自動的にマッピングし、公式ネットワーク範囲内外の露出、リスク、および不正な設定を検出します。すべての露出している資産は、コンテキスト化されたリスクスコアに従って自動的に分類、分析、優先順位付けされます。Falcon Surface は、すぐに実行可能で実用的な修復手順も生成します。

主な利点

24 時間 365 日の監視：比類ないリアルタイムディスカバリ機能が、世界で最も充実した攻撃者インテリジェンスによって強化された高信頼度のデータを生成

ビジネスコンテキストに沿ったリスクの優先順位付け：業界、CVE スコア、位置情報、攻撃履歴、アセットタイプ、手動編集等のコンテキストに基づいて重要なポイントにフォーカス

ガイド付き修復：すぐに実行可能でガイド付きの実用的な修復手順により、脆弱性にリアルタイムで対応

将来を見据えた対応：脆弱性管理、IT ハイジーン、CNAPP、包括的な CrowdStrike Falcon® プラットフォームにまたがり、アウトサイドインからインサイドアウトへと保護を拡張

CrowdStrike 製品

FALCON SURFACE: 外部攻撃対象領域管理 (EASM)

企業の攻撃対象領域を外部からの視点で見ることでセキュリティギャップをシャットダウン

Falcon Surface は、組織の露出した資産を継続的に可視化し、セキュリティチームが常に最新の資産インベントリであらゆる変更を把握することを可能にします。独自のリアルタイム 24/7 エンジンを使用して、世界中のインターネット全体をスキャンし、攻撃者の国の視点から組織の攻撃対象領域がどのように見えるかを確認することができます。そのマッピング機能は、毎年世界中で 70 億を超える露出した資産をインデックス化し、毎週 1 億 4,000 万件が特定されています。

- エコシステム全体のマッピングは、サードパーティベンダー、子会社、クラウド環境などのドメインアドレスのみに基づきます。非侵入型であり、エンドポイント、ノード、サーバー、IoT デバイス、OT など、さまざまな資産タイプを識別します。
- 人工知能（AI）対応のアソシエーションエンジンは、証明書やサブドメインなどの複数の識別子を通じて、「正式な」所有者かどうかにかかわらず、資産をその出所に関連付けます。さらに、このプラットフォームは、組織を特定の業界にマッチングさせることができます。これはネットワークセキュリティの最優先リスクをコンテキスト化するための重要な要素です。
- 詳細な検出パスにより、脆弱な露出した資産への関連付けを確認し、その履歴とコンテキストを理解できます。

業界をリードする攻撃者インテリジェンスと AI を活用したインサイトで攻撃対象領域のリスクに優先順位を付ける

クラウドストライクの業界をリードする脅威インテリジェンスと AI を活用した攻撃対象領域インサイトを利用することで、リスクとビジネスコンテキストに基づいて最もクリティカルな露出を把握し、最初に対処すべきものを判断できるようになります。Falcon Surface は、業界、CVE スコア、位置情報、攻撃履歴、資産タイプ、お客様による手動編集を考慮し、組織固有のニーズに合わせて設計された自動優先順位付けメトリックをお客様に提供します。Falcon Surface は、Slack、ServiceNow、Jira、その他のシステムを使用して、チームが戦略に沿った運用を推進し、データをワークフローにプッシュし、問題を迅速に解決できるようにするビルトイン統合機能により、アラートとアクションを合理化します。

モジュールの自動リスク優先順位付けは、以下に基づいて行われます：

- ビジネスコンテキスト：位置情報、業界、サイバー攻撃履歴など
- 資産タイプ
- CVE スコア
- マニュアル編集

露出とセキュリティの問題にはフラグが立てられ、動的に優先順位が付けられるため、セキュリティチームと IT チームはいつでも何に最初に取り組むべきかを把握できます。

セキュリティチームと IT チームに対して実行可能な修復手順を提供

アプリケーションのサポート終了（EOL）バージョンなどの特定したすべてのリスクに対して、Falcon Surface は、IT チームおよびセキュリティチームがリアルタイムで脆弱性を軽減できるように、すぐに実行可能な改善策を自動的に生成します。この精密でありながら明確な修復ステップにより、チームの生産性を最適化し、効率を高め、露出時間を短縮することができます。特別なスキルも知識も必要ありません—手順通りに進めるだけです。

一般的な使用例

- 未知のデジタル資産の発見
- 攻撃対象領域の管理
- クラウド開発の工程を保護
- 子会社のセキュリティを追跡
- サプライチェーンとサードパーティのリスクを監視
- M&A (合併買収) のセキュリティリスクを評価
- サイバー保険の保険料削減

クラウドストライクについて

CrowdStrike (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 およびワールドクラスの AI 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：**ブログ | Twitter | LinkedIn | Facebook | Instagram**

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