クラウドストライク製品

CROWDSTRIKE

FALCON LONG TERM REPOSITORY (LTR)

脅威コンテキストの強化と大規模かつ迅速なデータ管理で脅威ハンティングを再定義

課題：過去のデータと脅威コンテキストの欠如

現代のビジネスが推進するデジタルトランスフォーメーションの伸展により、リモートワーカーやクラウドワークロードだけでなく、企業のネットワークに接続されるデバイスと資産も増えています。これらの要因により、IT チームとセキュリティチームはエンドツーエンドの環境を完全に可視化して制御することができなくなり、組織の攻撃対象領域が増え、攻撃者はこれに乗じて悪用し続けています。

デジタルトランスフォーメーションは、最小限の予算とリソースしか持たずに苦慮している IT およびセキュリティの専門家に対して、利用可能なデータの量の増加ももたらします。彼らは、それらを効果的にコンテキスト化して潜在的な脅威に優先順位を付けるために、膨大な量のデータを保持・運用する負荷も負うことになります。

データの保存期間に制限があると、チームは攻撃の完全な履歴を確認することがほぼ不可能になり、脅威のコンテキストが限定され、効果的な脅威ハンティングと修復を妨げます。過去のデータやコンテキストデータにアクセスできないと、検出までの時間が遅くなり、セキュリティチームが可視性のギャップに陥り、重大な脅威アクティビティを見逃す可能性があります。さらに、ドエルタイム（侵害が発生してから検知されるまでの期間）が長くなり、組織が侵害のリスクにさらされる可能性も高まります。サイバー攻撃は進化し続け、侵害のリスクが高まる中、チームは IT データとセキュリティデータを統合して運用し、企業を効果的に保護するために必要な脅威のインサイトとコンテキストを取得する必要があります。

解決策：データの保存と管理をスケールアップして脅威ハンティングを強化

IT チームとセキュリティチームに対して環境全体についてのタイムリーでコンテクスチュアルなインサイトを提供し、脅威を効果的に検知・対応できるようにするには、豊富なセキュリティデータを保存、管理、分析するための経済的な方法が不可欠となります。CrowdStrike Falcon Long Term Repository ™ (Falcon LTR) は、さまざまな構造化データ、非構造化データ、半構造化データを組み合わせて、1 年以上の長期データ保持へのアクセスを提供し、拡大する攻撃対象領域全体の可視性と脅威コンテキストを取得できるようにします。

Falcon LTR は、CrowdStrike Falcon® プラットフォームから取得する侵害の痕跡 (IOC) との相関関係を含む、エンドポイント、ワークロード、アイデンティティにまたがる豊富なセキュリティデータを大量のログデータと組み合わせて、詳細でコンテクスチュアルかつ高速な分析を提供します。強力な検索および脅威ハンティング機能を使用して、リアルタイムのデータと長期の履歴データの両方から観察、分析、行動することで、潜在的な脅威をより迅速かつ正確に検知できます。長期間にわたり保存されたデータと、Falcon プラットフォームから得た豊富なセキュリティテレメトリとを組み合わせることで、セキュリティチームは脅威インサイトを強化し、攻撃経路を可視化して、より迅速に検知・対応することが可能になります。データの長期保存、コンテキスト分析、ボリュームに依存しない非常に高速な検索により、貴社独自のコンプライアンスとセキュリティのニーズを満たすことができます。

Falcon LTR は、スケーラブルなストレージと高度な圧縮技術により最小限のストレージとコンピューティングリソースで運用可能なため、費用対効果に優れており、TCO の削減と 1 年分以上のデータ検索が可能となります。CrowdStrike Falcon Data Replicator (FDR) を介して豊富な Falcon テレメトリを Falcon IOC と一緒に取り込み、保存・分析することにより、セキュリティチームは隠れた

主な利点

- 1 年以上にわたる長期間のデータ保持を実現し、かつてない規模で高度な脅威ハンティングと脅威分析の実行が可能
- エンドポイント、ワークロード、アイデンティティにまたがってシームレスに強化およびコンテキスト化された Falcon セキュリティテレメトリにより、タイムリーで実用的なインサイトを取得
- 最小限のストレージとコンピューティングリソースで長期保存が可能なため、総所有コストを低く抑えることが可能
- インデックスフリーの超高速履歴検索と、複雑なクエリを使用した 1 秒未満のライブ検索により脅威を迅速に発見可能
- Falcon IOC と相関付けた脅威インテリジェンスにより、プロアクティブな脅威ハンティングを実現

FALCON LONG TERM REPOSITORY (LTR)

脅威をプロアクティブに検索して発見することができます。また、データをふるいにかけて潜在的に悪意のある振る舞いを示唆する不規則性を検知することで高度標的型攻撃（APT 攻撃）を排除し、脆弱性が武器化される前に優先順位を付けて対処できます。世界で最も先進的でクラウドネイティブなセキュリティプラットフォームと、ログやデータの長期保存と可観測性を組み合わせることで、実用的なインサイトとリアルタイムの保護を得ることができます。

主な機能

脅威ハンティングとトラブルシューティングの変革

- **長期間のデータ保存：**Falcon LTR は 1 年以上にわたりデータを保持するため、セキュリティチームはより完全な過去データとリアルタイムデータにアクセスして、潜在的な脅威をより迅速に特定して検索を実行するために必要な脅威コンテキストを取得できます。これにより、これまでにない速度と規模で脅威ハンティングとトラブルシューティングを実行することが可能になります。
- **豊富なセキュリティテレメトリ：**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 から取得したデータを活用し、1 日あたり数兆のセキュリティイベントを攻撃の痕跡 (IOA) と相関させることで、継続的に取り込まれコンテキスト化されたセキュリティテレメトリを脅威分析と脅威ハンティングに役立てることができます。このテレメトリは、即座に検索可能で他のデータソースと相互参照することもできる、400 を超えるイベントタイプに関する情報を提供します。
- **相関付けされた脅威インテリジェンス：**Falcon IOC を含む Falcon プラットフォームの脅威インテリジェンスフィードが提供する実際の脅威コンテキストで既存のセキュリティデータを強化することにより、脅威に対する理解を深め、既知の攻撃者に関連した新しい攻撃をより適切に特定することができます。

スケーラブルなストレージと管理でセキュリティデータを運用

- **費用対効果の高いスケーラブルなストレージ：**迅速かつ効率的な運用のために、必要なだけストレージとコンピューティングリソースを利用でき、また労力ゼロで拡張することが可能です。スケーラブルなストレージと高度な圧縮技術により、優れたコスト効率で Falcon データを 1 年以上にわたり保存および管理できます。
- **高速かつカスタマイズ可能な検索：**機能豊富なクエリ言語と、超高速の履歴検索や 1 秒未満のライブ検索が実行可能なインデックスフリーのアーキテクチャを利用し、Falcon セキュリティデータに関する回答を即座に取得して、実用的なインサイトを取得することができます。
- **単一のインターフェイス：**分散したデータを 1 か所でシームレスに収集、分析し、さらに即座にアクセス。環境全体を包括する単一のビューを提供し、脅威ハンティングタスクに有意義なコンテキストを提供します。

可視性とコンテキストの強化

- **リアルタイムおよび過去のデータ：**振る舞いに関するインサイトを含む、完全で正確な脅威の調査と分析を可能にする豊富なリアルタイムおよび過去のデータを取得。コンプライアンスを達成し、攻撃経路や脆弱性を完全に可視化するのに役立ちます。
- **データ形式の一元化：**エンドポイント、ワークロード、アイデンティティにまたがる構造化データ、非構造化データ、半構造化データを簡単に組み合わせて検索し、攻撃対象領域を全体的に可視化します。
- **カスタムアラートとダッシュボード：**ストリーミングデータに基づいて、最も重要なイベントに対するカスタムアラートとダッシュボードをリアルタイムで有効にし、重大な脅威の迅速な検知と大規模な調査を可能にします。

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**

詳細はこちら：
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