用語集

インシデント事後のプレレビュー（PIR）：FalconセンサーとWindowsオペレーティングシステム（BSOD）に影響を及ぼしたコンテンツ設定の更新について

本文書は、以下の英語版（https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/）の翻訳です。
本翻訳版は、参照を容易にし、便宜上の目的でのみ提供されています。矛盾や曖昧さが生じた場合は、常に英語版が優先されるものとします。

	全般	技術
チャネルファイル	チャネルファイルはセンサーにとって動作マニュアルのようなもので、許可リスト/ブロックリストを含み、センサーの動作を指示します。 これらのファイルはホストコンピューターに保存され、管理者がFalconセンサーやポリシー設定を変更した時や、検知ロジックが更新された時などに動的に更新されます。	センサーが利用する動的構成ファイルです。ホワイトリストの詳細などの設定情報が含まれ、環境内の特定のFalconセンサー（または複数のセンサー）に送信されます。
コンテンツコンフィグレーション更新	クラウドストライクのポリシーと検知設定を更新するプロセスです。	Falconセンサーの動作に影響を与えるポリシー設定と検知コンテンツを更新するCrowdStrike　Falconのバックエンドプロセスです。
コンテンツコンフィグレーションシステム	チャネルファイルの作成と配布を管理します。	チャネルファイルの作成と配布を管理します。コンテンツコンフィグレーションシステムは、クラウド内のFalconプラットフォームの一部です。
コンテンツインタープリター	チャネルファイルからラピッドレスポンスコンテンツを読み取り、変換処理する、Falconセンサーのコンポーネントです。	チャネルファイルからラピッドレスポンスコンテンツを読み取り、変換処理する、Falconセンサーのコンポーネントで、これにより、顧客のポリシー構成に応じて、センサー検知エンジンが悪意のあるアクティビティを監視、検知、防御できます。
コンテンツバリデーター	展開する前にコンテンツの検証確認を行います。	コンテンツを展開する前に検証確認を行う、コンテンツコンフィグレーションシステムの一部です。
テンプレートタイプ	専門家が迅速に脅威に対応できるように事前作成済みのフォームです。これらのフォームはコードで記述されています。	新しいテレメトリと検知に活用できるようラピッドレスポンスコンテンツの一連のフィールドを事前に定義するセンサー機能です。
テンプレートタイプのストレステスト	信頼性とパフォーマンスを高めるため、さまざまな条件下でのテンプレートタイプのテストとしてクラウドストライクが実行するプロセスです。	信頼性とパフォーマンスを高めるため、さまざまな条件下で行うテンプレートタイプのテストです。テストは、様々なオペレーティングシステムとワークロードで構成されるステージング環境で実施されます。
テンプレートインスタンス	Falconセンサーが特定の振る舞いを監視、警戒、防止するための指示です。	Falconセンサーが監視、検知、防止すべき特定の1つの振る舞いを認識するための一連の指示です。
ラピッドレスポンスコンテンツ	コンピューターのセキュリティシステムを迅速に改善する特別な種類の更新です。メインプログラムを変更することなく、システムが新しいタイプの脅威を認識して阻止するのに役立ちます。 保護を最新の状態に保ち、最新の脅威に対処できるように、迅速に更新します。	Falconセンサーに動的な検知ロジックを更新して新しい脅威に迅速に対応する、一連のテンプレートインスタンスのセットです。
センサーコンテンツ	AIモデルやMLモデルを含む、脅威をセンサーが検知するための幅広い機能です。 センサーコンテンツはセンサーリリースに含まれ、クラウドから動的に更新されるものではありません。	オンセンサーのAIモデルやMLモデルを含む、脅威をセンサーが検知するための幅広い機能です。 センサーコンテンツはセンサーリリースに含まれ、クラウドから動的に更新されるものではありません。
名前付きパイプ	名前付きパイプを使用すると、異なるソフトウェアプログラムが同じコンピューター上で相互に通信できるようになります。	別々のプロセスが相互に通信できるようにするプロセス間の通信方式です。これは、InterProcessCommunication（IPC）と呼ばれます。

InterProcessCommunication（IPC）テンプレートタイプ	プロセス間の通信を伴う脅威を阻止するために使用されるテンプレートタイプです。	名前付きパイプなど、プロセス間の通信を伴う脅威を阻止するために使用されるテンプレートタイプです。
IPCテンプレートインスタンス	InterProcess　Communicationテンプレートタイプから作成された特定の構成です。 どの振る舞いを監視、検知、停止するかをセンサーに伝えます。	IPCテンプレートタイプから派生した特定の構成で、センサーが監視、検知、防御するための特定の振る舞いをマッピングします。 例えば、IPCテンプレートインスタンスを展開して、ネットワーク内でのマルウェアのラテラルムーブメントに対する名前付きパイプの不正使用を監視します。
センサー検知エンジン	Falconセンサーのコンポーネントは、悪意のあるアクティビティを検知して防止する役割を担います。	悪意のある活動を検知して防止する役割を担うFalconセンサーのコンポーネントです。顧客のポリシー構成に応じて、悪意のあるアクティビティを監視、検知、防御するために使用されます。
追加の用語		
行動ヒューリスティック	静的シグネチャではなく振る舞いのパターンに基づいて脅威を検知するために使用される手法です。	プロセスインジェクションや認証情報スキャンの検知など、静的シグネチャではなく振る舞いのパターンに基づいて脅威を検知するために使用される手法です。
フォールトインジェクション	システムに意図的エラーを導入し、システムがどのように応答するかを確認して弱点を特定し、システムの堅牢性と信頼性を高めるためのテスト方法です。	システムの堅牢性とエラー処理機能を検証するために、意図的にエラーを導入するテスト方法です。例えば、分散データベースシステムでのフォールトインジェクションには、特定のノードが一時的にアクセスできなくなるネットワークパーティションのシミュレーションが含まれる場合があります。
カナリア展開	広範囲にリリースする前に問題がないかテストするために、アップデートをまず少数のユーザーグループに展開するソフトウェア配布戦略です。	本格的な展開の前に機能性や問題を検証するために、少人数単位のユーザーに新しいソフトウェアを段階的に解放する展開戦略です。
ファジング	ランダムなデータや予期しないデータをソフトウェアプログラムに入力してバグや脆弱性を見つけ、ソフトウェアの安全性と信頼性を高めるテスト手法です。	ランダムなデータ、不正なデータ、予期しないデータをプログラムに入力して、システムクラッシュや予期しない振る舞いにつながる可能性のあるセキュリティ上の脆弱性、バグ、エッジケースを発見するテスト方法です。
アドバーサリーレスポンス	サイバーセキュリティなど、危害や混乱を引き起こそうとする人やモノに対抗または防御するために取られた行動または対応です。	高度な脅威インテリジェンス、フォレンジック分析、即時インシデント対応などによって、脅威を検知、分析、緩和し、攻撃を封じ込めて根絶します。
行動パターンマッチング	既知のパターンと比較することで一般的な振る舞いや傾向を特定し、特定の行動やイベントを予測または認識するのに役立つ方法です。	機械学習アルゴリズムと統計モデルを使用して異常を検知し、特定の行動やイベントを予測することで、データセット内の特定の振る舞いを既知のパターンと比較して識別し相関付ける高度な手法です。
例外処理	ソフトウェアが予期しない問題やエラーを管理・修正し、プログラムがクラッシュすることなくスムーズかつ継続的に実行できるようにする方法です。	実行時エラーを制御された方法で管理・応答するために使用されるプログラミングコンセプトで、失敗する可能性のあるコードを実行する「try　block」、特定のエラーが発生した場合に処理する「catch block」、クリーンアップコードを実行する「finally block」という3つの主要コンポーネントなどがあります。
境界外メモリ読み出し	プログラムが想定外のメモリを読み取るプログラミングエラーです。	プログラムが割り当てられた境界を超えてメモリにアクセスしたときに発生するプログラミングエラーです。
ドッグフーディング	自社で開発した製品を使用してテストし、改善するプロセスです。	自社で開発した製品やサービスを社内で使用して、その品質、機能性、ユーザー体験をテストし、検証するプロセスです。