CylanceOPTICS™ 予防ファーストの EDR

v2.3 の新機能

CylanceOPTICS は、CylancePROTECT® が提供する脅威防御を拡張し、AI（人工知能）を使用してセキュリティインシデントを識別、防止できるように設計されたエンドポイント検知／対処（EDR）ソリューションです。

CylanceOPTICS は次の機能を備えています。

- AI 駆動型のインシデント検知防御
- オンデマンドでの侵入経路と根本原因分析
- スマートな脅威ハンティング
- リモートから端末の隔離を行うロックダウン機能
- リモート調査機能

v2.3 の新機能

CylanceOPTICS v2.3 では、ソリューションの機能が拡張され、以下の点が強化されています。

- **AI 駆動型のインシデント防御：**ファイルレス攻撃、悪意のある／疑わしいワンライナーコマンド、および悪意のあるアプリケーションの振る舞いに的を絞った機械学習型脅威検出モジュールがコンテキスト分析エンジンに組み込まれ、各エンドポイントで継続的に変化を監視し、既知の定義ルールベースでは検出が難しい脅威を発見します（詳細は 2 ページを参照してください）。
- **リモートフォレンジックデータの収集：**エンドポイントを操作して一連の高度なフォレンジックデータを収集したり、スクリプトやアプリケーションを実行して疑わしいイベントやセキュリティインシデントに関連する重要な情報をキャプチャしたりできるようになりました。
- **検知の詳細とデバイスロックダウンの強化：**ロックダウンと検知の詳細が以下のとおり強化されました。
  - 「イベントの説明」セクションが強化され、検知ルールのロジックが「自然言語」形式でわかりやすく表示されるようになりました。
  - 「イベントアーティファクト」セクションが強化され、イベントに関連するすべてのアーティファクトとファセットが含まれるようになりました。
  - ロックダウン期間を選択したり、現在のページ／ワークフローからロックダウンを開始したりできるようになりました。
- **デバイス情報の表示：**環境内のデバイスに関する次のような重要な情報にさらに簡単にアクセスできるようになりました。
  - 「デバイス名」がクリック可能になり、現在のページ内にスライド表示されるドロワーを使用してデバイスの情報を素早く表示できるようになりました。
  - デバイスドロワーから、デバイスをロックダウンしたり、パッケージ展開を開始したりできます。
  - 「デバイスの詳細」ページへのリンクを使用して、CylancePROTECT に固有の詳細情報を参照できます。
- **簡単になった例外ルール設定：**コンテキスト分析エンジン（CAE）によって生成された検知結果に対して素早く例外ルールを作成できるようになりました。これにより、潜在的な誤検知や、異常ではあるものの脅威ではないアクティビティをシンプルに監視対象外にできます。このような例外を使用することで、検知結果の量を減らし、大量のカスタムルールの必要性を最小限に抑えることができます。これらの例外を既存のルールに適用すると、以降、例外に一致するアクティビティを CAE で無視できます。

機械学習脅威検知モジュール：機能の詳細

CylanceOPTICS v2.3 は、AI（人工知能）／ML（機械学習）ベースのモデルにより、エンドポイント上で脅威予測検知と対処を実現する、市場初の EDR ソリューションです。トレーニングされた機械学習モデルは、各エンドポイントに直接展開され、遅延のない検知と対処を実現します。クラウドへのデータストリーミングやオンプレミスの専用ハードウェアは必要ありません。

初期リリースで提供されるCylanceOPTICSベースの機械学習モデルは次の3つです。

- **ファイルレス攻撃モデル:**いわゆる「ファイルレス」攻撃は、悪意のあるバイナリや疑わしいバイナリに依存しないという意味ではファイルレスと言えます。しかし、通常はシステムベースの他のアーティファクトに依存しており、CylanceOPTICSはこれらを容易に検知、相関できます。ファイルレス攻撃モデルは、システムユーティリティ呼び出しのコンテキストとパラメータを評価して、その攻撃が意図している結果を理解します。
- **悪意のあるワンライナーコマンドモデル:**cmd、PowerShell、wscriptなどのスクリプトエンジンは強力なIT運用ツールですが、悪意のある攻撃者が利用可能な機能が大量に公開されてしまいます。悪意のあるワンライナーモデルは、スクリプトの言語とコマンドラインコンテキストに重点を置いてコマンドラインスクリプトの内容を評価します。
- **悪意のあるアプリケーションの行動モデル:**膨大な数の攻撃が、企業環境でよく使われている、予測可能なわずかな数の信頼済みアプリケーションを標的にしています。悪意のあるアプリケーション行動モデルは、一般的なソフトウェアとオペレーティングシステム間の正当な対話処理を学習し、通常の処理から大きく外れる処理をすべてブロックします。

CylanceOPTICSにより収集されるエンドポイント上のデータ

イベントタイプ	イベントの説明
CylancePROTECT	• CylancePROTECTの検知または隔離イベントからのバックトレースにより、デバイスで観測されたマルウェアまでたどれる「ブレッドクラムトレイル」をユーザーに提供
ファイル	• ファイルの作成、変更、削除、名前変更イベントを、メタデータおよびファイル属性とともにキャプチャ • ファイル - プロセス関係を関連付け • 代替データストリームを識別 • リムーバブルデバイスのファイルを識別
プロセス	• プロセスの作成と終了 • モジュールロード • スレッドインジェクション • プロセスを、その所有ユーザーおよびイメージファイルと関連付け • プロセスを、そのすべてのアクティビティ（ファイル、レジストリキー、ネットワーク接続など）と関連付け
ネットワーク	• IPアドレス • レイヤ4プロトコル • 発信元と発信先のポート
レジストリ	• レジストリのキーおよび値の作成、変更、削除イベントを収集 • マルウェアがシステムの再起動後も存続するために使用する、120の「パーシスタンスポイント」を識別 • レジストリキー／値を、それらを作成したプロセスと関連付け • 専用のパーサーで永続レジストリキー／値を、存続しようとするファイルと関連付け
ユーザー	• 以前デバイスにログオンしたことのあるすべてのユーザーをキャプチャ • ユーザーとそれらのユーザーが実行したアクション（作成、変更、削除イベントを含む）を関連付け • ユーザーと悪意のあるアクティビティを関連付け
リムーバブルメディア	• リムーバブルメディアの挿入イベントを、コピー先／元ファイルおよび実行されたファイルと一緒に収集 • デバイスの詳細をキャプチャ • リムーバブルメディアを変更したか、リムーバブルメディアからファイルをコピーしたプロセスを識別 • CylancePROTECTで検知されたマルウェアがリムーバブルメディアから侵入したかどうかを識別

Cylance Japan 株式会社
〒100-6510
東京都千代田区丸の内 1-5-1　新丸の内ビルディング 10F
www.cylance.co.jp
03-6386-0061 (代表)

20180614-0648