CylanceOPTICS™の InstaQuery（IQ）による脅威ハンティング

機能紹介

CYLANCE

CylanceOPTICS の InstaQuery（IQ）による脅威ハンティング

セキュリティの世界では長らく、脅威ハンティングは現場での長年の経験を持つ一流のセキュリティアナリストにしか行えない作業だと考えられてきました。それらのアナリストは、専門家向けに設計されたツールを使用して複雑なハンティングを行い、隠れた脅威を見つけ出すことでそれらの脅威を軽減できます。

このようなスキルと経験を持ったハンティングの専門家たちが、重大なセキュリティ違反や無数のデータ侵害から多くの企業を救ってきたことは確かです。しかし残念ながら、一流のセキュリティアナリストの数は減る一方で、現在のセキュリティ人材の不足という現実から、大半の組織が社内に効果的なハンティング機能がない状況に置かれ、それは今なお続いています。

一方、CylanceOPTICS なら、すべてのセキュリティチームが InstaQuery（IQ）でスマートな脅威ハンティングを行えるようになります。

市場で主流となっている複雑で専門化された脅威ハンティングツールとは異なり、CylanceOPTICS の IQ 機能を使ったスマートな脅威ハンティングなら、誰もが脅威ハンティング機能を利用して、エンドポイントから収集されたフォレンジックに関連するデータに瞬時にアクセスできます。IQ を使用すると、セキュリティアナリストは、セキュリティ侵害、疑わしいアクティビティ、あるいは無数のエンドポイントからの情報が必要な特定のビジネスニーズがないか、全社規模の検索を行うことが可能になります。

CylanceOPTICS v2.0 では、ユーザーは IQ の検索ページから次の簡単な検索が行えます。

- ファイル
- レジストリキー
- プロセス
- ネットワーク接続

CylanceOPTICS は、検索を始める際に、要求された情報を求めて特定のエンドポイントにクエリを実行し、エンドポイント上に保存されているデータを照会して、すべての応答データを収集します。IQ の検索結果はクラウドに保存されるため、後で簡単に参照できます。

クエリが完了すると、ユーザーはテーブル形式で結果を確認することや、的を絞った検索を行うために、ファセットの詳細ビューを使用して、クエリの結果をより詳細に確認することもできます。このようなエンドポイントデータのシンプルな照会により、スキルレベルにかかわらず、誰もが数分以内に各自のエンドポイントアクティビティに対する洞察を得られるようになります。

次のテーブルは、アーティファクトごとに表示される IQ の結果の概要を示しています。

テクニカル詳細サマリー	
InstaQuery の結果	**説明**
Name	InstaQuery の名前
Description	InstaQuery の説明
Date Created	InstaQuery が作成された日付
Search Term	検索の対象である特定の値
Artifact	実行している検索の対象である項目のタイプ
Facet	検索の対象であるアーティファクトの属性
Zones	クエリに含まれているゾーン（このゾーン内のデバイスのみがこのクエリに含まれます）
Devices Queried	クエリに関連付けられたデバイスの数
Devices Responded	クエリ要求に応答したデバイスの数
Devices with Results	クエリに一致したデバイスの合計数
Total Results	クエリから返されたアーティファクトの合計数

アーティファクトタイプ：ファイル	
ファセット	**説明**
Path	ファイルへのパス
Created	ファイルが作成された日付
MD5	ファイルの MD5 ハッシュ
SHA256	ファイルの SHA256 ハッシュ
Device	ファイルが見つかったデバイスの名前
Owner	ファイルを所有するユーザーの名前

アーティファクトタイプ：プロセス	
ファセット	**説明**
Name	プロセスの名前
Start Date	プロセスを開始した日時
Image Path	プロセスの実行可能ファイルへのパス
Command Line	プロセスを開始するために使用したコマンド
Image MD5	ファイルの MD5 ハッシュ
Owner	プロセスの所有者
Device	プロセスが見つかったデバイスの名前

アーティファクトタイプ：ネットワーク接続	
ファセット	**説明**
Destination Address	ソースの接続先の IP アドレス 注：すべてのクエリは宛先 IP アドレスを対象に実行されます。
Destination Port	宛先に接続するために送信元 IP アドレスで使用するポート番号
Process Name	ネットワーク接続に関連するプロセスの名前
Image Path	プロセスの実行可能ファイルへのパス
Device	デバイスの名前

接続が特定の IP 範囲（プライベート、リンクローカル、ルーティング不可能、マルチキャスト、ループバック）に完全に限定されている場合、ネットワーク接続に関して表示される結果はフィルタリングされます。

アーティファクトタイプ：レジストリ	
ファセット	**説明**
Path	レジストリキーへのパス
Value Name	レジストリ値
File Path	レジストリキー、値、または値の内容から抽出されたファイルパス
File MD5	ファイルの MD5 ハッシュ
Is Persistence Point	変更されるレジストリキーが、CylanceOPTICS によって監視されているパーシスタンスポイントかどうか
Device	デバイスの名前

InstaQuery の結果ページでは、ユーザーは「Action」行を展開してさらなるアクションを実行できるほか、クエリを破棄できます。クエリを破棄した場合、クエリが「Previous Queries」リストから削除されます。

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)

201803-FF008