VMware Carbon Black XDR ユーザー ガイド

2023 年 9 月 26 日

VMware Carbon Black Cloud

最新の技術ドキュメントは、 VMware の Web サイト （https://docs.vmware.com/jp/）

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
〒 108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

目次

VMware Carbon Black XDR ユーザー ガイド

1

VMware Carbon Black Extended Detection and Response (XDR) は、テレメトリを活用してラテラル セキュリティを大幅に強化します。セキュリティ チームは、VMware Carbon Black XDR を活用して環境全体の脅威を迅速に特定し、防止ポリシーを適用する際に十分な情報に基づいた意思決定を行うことができます。

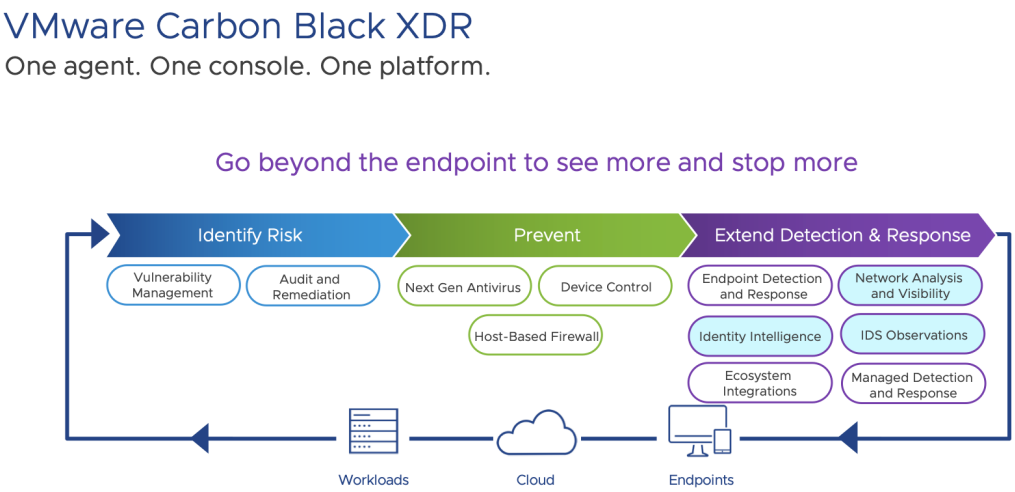
VMware Carbon Black XDR は、エンドポイントとワークロードのセキュリティ機能を統合し、ネットワークに対する重要な可視性を実現することで、死角を削減し、脅威をより迅速に検出します。

VMware Carbon Black XDR の概要 2

VMware Carbon Black XDR は、エンドポイント、ワークロード、ユーザー、およびネットワーク全体で可視性、分析、応答を拡張するツールとデータの統合です。

VMware Carbon Black XDR は、XDR のネットワーク テレメトリの追加に焦点を当て、ネットワーク パケットとプロセスに関する判断材料を提供します。

XDR の詳細については、Extended Detection and Response (XDR) とは?を参照してください。



VMware Carbon Black XDR は、Carbon Black Cloud Enterprise EDR の XDR を実装しています。この実装には、Carbon Black Cloud Windows センサー 3.9.1 MR1 以降が必要です。

VMware Carbon Black XDR を使用して、関連するネットワーク データを可視化および分析できます。例：

- ネットワーク接続の署名（JA3 および JA3S サムプリント）
- ネットワークの侵入検知
- セキュリティ ラッパーの詳細（TLS データ）
- 証明書の署名者（暗号化 - TLS データ）

- HTTP の詳細

次のトピックを参照してください。

- XDR のメリットは何ですか?
- XDR のユースケース。
- XDR と EDR の違いは何ですか?

XDR のメリットは何ですか?

XDR は、EDR を超える機能を備えており、組織の IT 環境を保護するためのいくつかの具体的なメリットがあります。次のようなメリットがあります。

可視性とコンテキストの向上

XDR は、セキュリティ環境を 360 度全方位から把握することができます。これにより、セキュリティ アナリストは、正規のソフトウェア、ポート、プロトコルさえ利用してあらゆるセキュリティ レイヤーに侵入する脅威を確認できます。攻撃の方法、ブループリント、エントリ ポイント、その他の影響を受けるユーザー、脅威の発生元、およびその拡散方法が収集されます。この追加のコンテキストと、それを理解するために必要な分析は、脅威に迅速に対応するために不可欠です。

優先順位付け

IT チームとセキュリティ チームは、多くの場合、セキュリティ サービスによって生成される無限のアラートに対応するのに苦労します。XDR のデータ分析と相関機能により、関連するアラートをグループ化し、優先順位を付け、最も重要なアラートのみを表示できます。

自動化

XDR による自動化の使用により、検出と応答が迅速化され、セキュリティ プロセスから手動の手順が削除されます。これにより、IT チームは大量のセキュリティ データを処理し、複雑なプロセスを繰り返し実行できます。

運用効率

XDR は、断片的なセキュリティ ツールの集合体ではなく、管理されたフリート全体にわたって脅威を全体的に把握することができます。これは、環境と広範なセキュリティ エコシステムに緊密に統合された、集中的なデータ収集と対応を提供します。

より迅速な検出と応答

これらのメリットが積み重なり、効果的なセキュリティ態勢を実現します。XDR は効率性を高めることで、脅威をより迅速に検出して応答できます。

洗練された応答

XDR の洗練された機能と優れた可視性により、特定のシステムへの応答を調整し、他の制御ポイントを活用して全体的な影響を最小限に抑えることができます。

XDR のユースケース。

XDR を使用してエンドポイントの脅威を検出して対応する方法は多数あります。以下は最も一般的なユースケースです。

脅威ハンティング

特定のネットワークに脅威がすでに存在する可能性は高いですが、多くのセキュリティ チームはプロアクティブな脅威ハンティングを行う時間を見つけるのに苦労しています。XDR のテレメトリおよび自動化機能を使用すると、この作業の多くを自動的に実行できるため、セキュリティ チームの負荷が大幅に軽減され、他のタスクと一緒に脅威ハンティングを実行できるようになります。

トリアージ

セキュリティ チームの最も重要な機能の 1 つは、アラートの優先順位付けまたはトリアージを行い、最も重要なアラートに迅速に対応することです。XDR は、強力な分析を使用して、何千ものアラートを少数の優先度の高いアラートに関連付けることで、ノイズを選別するのに役立ちます。

調査

XDR の広範なデータ収集、優れた可視性、および自動分析により、セキュリティ チームは脅威の発生元、拡散方法、他のユーザーやデバイスが影響を受ける可能性を迅速かつ容易に特定できます。これは、脅威を削除し、今後の脅威に対してネットワークを強化するために重要です。

XDR と EDR の違いは何ですか?

XDR は、ワークロード、デバイス、ユーザー、ネットワークなど、環境内のすべてのセキュリティ レイヤーにわたって EDR の機能を拡張します。

XDR は、EDR が提供する単一の視点ではなく、複数のセキュリティ レイヤーにわたるテレメトリと動作分析を可能にし、セキュリティ チームが全体像を把握できるようにします。

悪い攻撃者は攻撃を単一のセキュリティ レイヤーに制限しません。そのため、セキュリティ チームはビューを 1 つのレイヤーに制限することはできません。EDR によって、セキュリティ専門家は侵害された可能性のあるエンドポイントを可視化できますが、セキュリティ チームが認識する前に、攻撃がネットワークを越えて他のシステムに移動していた場合には十分ではありません。

ここで XDR が登場します。XDR は、可視性のギャップを回避するシステム全体のアクティビティの全体像を提供することで、セキュリティ チームが脅威の発生元と環境全体への拡散方法を理解できるようにします。XDR は、より優れた分析と相関機能および総合的な視点を提供します。

XDR データと手法

3

このトピックでは、Carbon Black Cloud コンソールで取得できる netconn データについて説明します。また、netconn トラフィックを識別して分類する侵入検知システム (IDS) と、アノマリを判断するためのネットワーク トラフィック分析 (NTA) も導入されています。

Netconn データ

XDR はネットワーク接続 (netconn) を分析し、これらの分析を脅威ハンティングと調査に対して表示します。検索できる netconn フィールドのリストについては、4 章 XDR 検索フィールドを参照してください。

観測データ タイプは、フィルタリングおよび並べ替えに使用できます。観測タイプの詳細については、調査 - 観測を参照してください。

- CB 分析
- コンテクスト アクティビティ
- TAU Intelligence
- 改ざん
- ブロックされたハッシュ
- 侵入検知システム
- ネットワーク トラフィックの分析
- ホストベースのファイアウォール
- 攻撃のインジケータ

侵入検知システム (IDS)

MicroIDS ネットワーク分類エンジンは netconn イベントで実行され、IP パケットを使用して接続を分類します。このエンジンは、Carbon Black Cloud 3.9 以降の Windows センサーに組み込まれています。

IDS には以下の利点があります。

- インバウンドおよびアウトバウンドのネットワーク トラフィックを監視する
- システムとネットワーク間を移動するデータを監視する
- ネットワーク パケットをキャプチャおよび分析して攻撃を検出する

- 異常なネットワーク トラフィックを特定する

[侵入検知システム] は、[アラート]、[プロセス]、[観測] 画面のフィルタ オプションです。

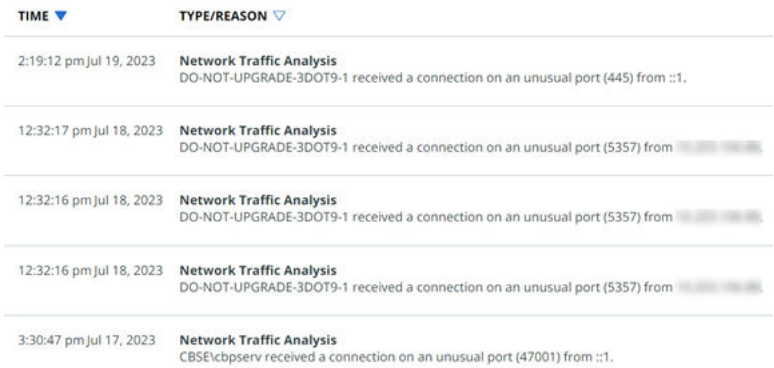
ネットワーク トラフィック分析 (NTA)

ネットワーク トラフィック分析 (NTA) は、ネットワークの可用性とアクティビティを監視して、アノマリを特定します。NTA のメリットは次のとおりです。

- 豊富なコンテキストを提供することで、ネットワークの可視性を向上
- アノマリ アクションの検出
- セキュリティ トリアージ調査の支援

ネットワーク パケットから抽出されたデータは、使用状況を追跡し、疑わしい動作を監視するのに役立ちます。

例：



Carbon Black は、次の 3 種類の NTA 検出器を示しています。

アラート タイプ	説明
IP プロファイラ	通常ホストが接続するリモート IP アドレスとは異なるリモート IP アドレスを持つローカル ホストとの接続を探します。
ユーザー エージェント プロファイラ	以前のデバイス アクティビティと比較して、ローカル デバイスから行われた接続で異常な HTTP ユーザー エージェントを探します。
ポート プロファイラ	ネットワーク接続のいずれかの側で異常なポート アクティビティを探します。このアラート タイプには、次の 4 つのバリエーションがあります。 ■ 外部ポート プロファイラ ■ 内部ポート プロファイラ ■ 外部サーバ ポート プロファイラ ■ 内部サーバ ポート プロファイラ

[ネットワーク トラフィック分析] は、[アラート]、[プロセス]、[観測] 画面のフィルタ オプションです。

MITRE ATT&CK 戦略と技術

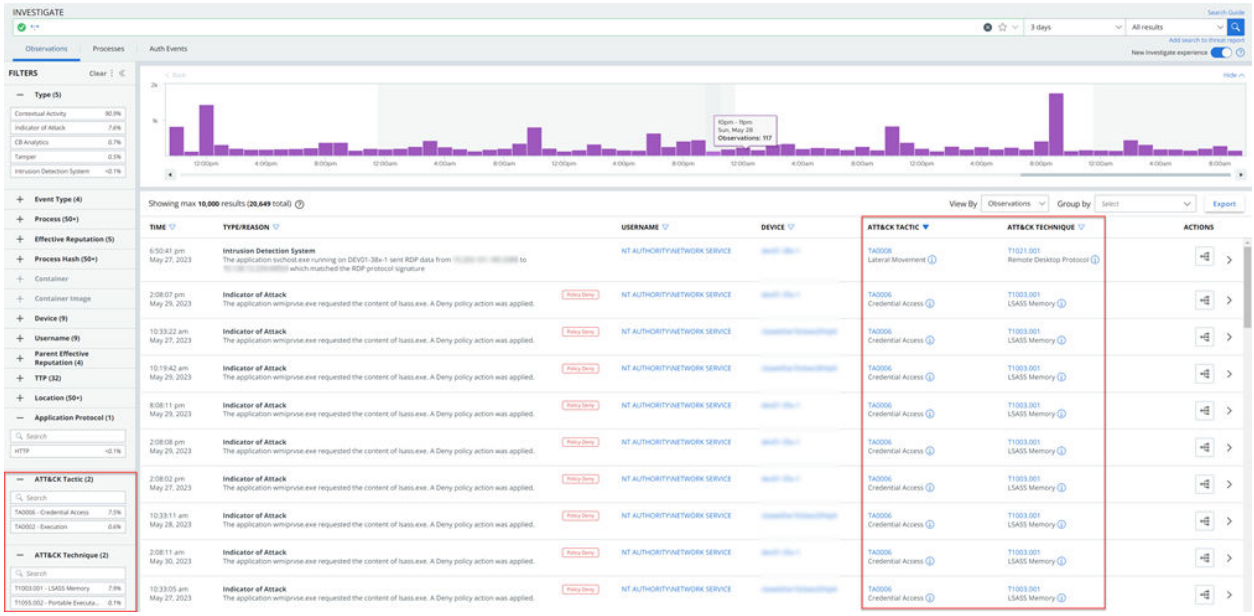
MITRE ATT&CK® は、Carbon Black Cloud コンソール全体および XDR に表示されます。XDR 固有ではありません。

MITRE ATT&CK は、敵対的な戦略と技術のナレッジベースとして、セキュリティ業界によって広く採用されています。MITRE ATT&CK の詳細については、MITRE ATT&CK（外部リンク）を参照してください。

戦略は、技術の背後にある目的を表します。たとえば、`TA0001` の MITRE ATT&CK 戦略 ID は、攻撃者がネットワークに侵入しようとしていることを示します。

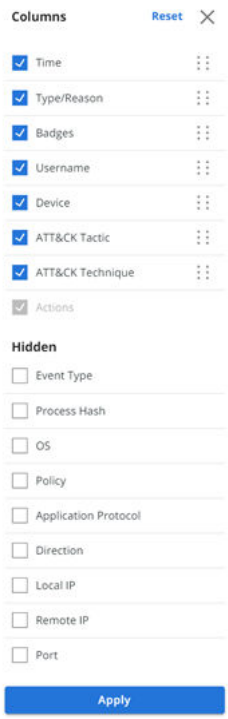
技術は、攻撃者がどのように攻撃しているかを表します。たとえば、`T1548.003` の MITRE ATT&CK 技術 ID は、攻撃者が権限を昇格するために sudo キャッシュを実行していることを示します。

[観測]、[アラート]、[プロセス]、[プロセス解析] 画面の `Tactic` フィールドと `Technique` フィールドをフィルタリング、検索、並べ替えできます。例：

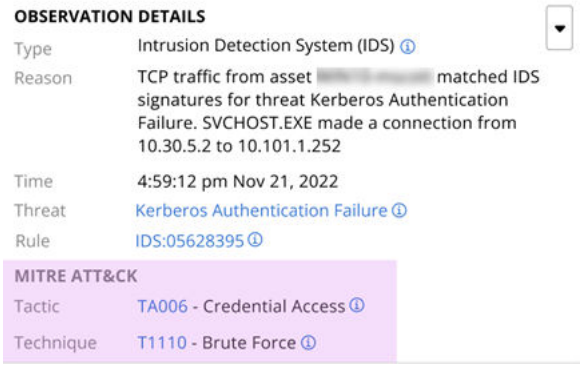

INVESTIGATE
Observations
Processes
Auth Events
FILTERS
Clear
Type (5)
Event Type (4)
Process (50+)
Effective Reputation (5)
Process Hash (50+)
Container
Container Image
Device (9)
Username (9)
Parent Effective Reputation (4)
TTP (32)
Location (50+)
Application Protocol (1)
ATT&CK Tactic (2)
ATT&CK Technique (2)
Showing max 10,000 results (20,649 total)
View By
Observations
Group by
Export
TIME
TYPE/REASON
USERNAME
DEVICE
ATT&CK TACTIC
ATT&CK TECHNIQUE
ACTIONS
Intrusion Detection System
Indicator of Attack
NT AUTHORITY\NETWORK SERVICE
Lateral Movement
Remote Desktop Protocol
Credential Access
LSASS Memory

ヒント:

- [観測] 画面と [アラート] 画面の表に [戦略] 列と [技術] 列の両方を表示するには、表の左下にある [表の構成] をクリックします。



- [情報] アイコンをクリックして、戦略または技術の概要を表示します。[情報] ペイン内で、[詳細] をクリックして MITRE Web サイトに移動して詳細を確認できます。
- [観測]、[アラート]、[アラートのトリアージ] 画面の [観測の詳細] ペインに MITRE ATT&CK 戦略と技術が表示されます。



XDR 検索フィールド

4

次のリストは、XDR により強化された netconn イベントの検索に使用できる検索フィールドを示しています。すべての検索フィールドの完全なリスト、説明、例については、製品内の『検索ガイド』を参照してください。

netconn_actions	netconn_application_protocol	netconn_bytes_received
netconn_bytes_sent	netconn_community_id	netconn_domain
netconn_first_packet_timestamp	netconn_ja3_local_fingerprint	netconn_ja3_local_fingerprint_fields
netconn_ja3_remote_fingerprint	netconn_ja3_remote_fingerprint_fields	netconn_last_packet_timestamp
netconn_remote_device_id	netconn_remote_device_name	netconn_request_headers
netconn_request_method	netconn_request_uri	netconn_response_headers
netconn_response_status_code	netconn_server_name_indication	netconn_tls_certificate_issuer_name
netconn_tls_certificate_subject_name	netconn_tls_certificate_not_valid_after	netconn_tls_certificate_not_valid_before
netconn_tls_version		

ポリシーによる XDR の無効化

5

XDR ネットワーク データ収集はデフォルトで有効になっています。ポリシーが割り当てられているセンサーの XDR ネットワーク データ収集を無効にできます。データ収集を無効にしても、VMware Carbon Black XDR は無効になりません。センサーが XDR ネットワーク データを収集するのを停止し、ノイズを低減するだけです。

手順

1 左側のナビゲーション ペインで、[適用] - [ポリシー] の順にクリックします。

2 ポリシーを選択します。

3 [Sensor (センサー)] タブをクリックします。

4 [XDR ネットワーク データ収集を有効にする] 設定のチェック ボックスを選択解除します。

5 [保存] をクリックします。

XDR データの取得

6

Carbon Black Cloud コンソールで XDR データを取得する方法はいくつかあります。

[プロセス]、[観測]、[アラート] 画面で XDR データを取得できます。

取得したデータは、これらの画面および [プロセス解析] 画面と [アラートのトリアージ] 画面で確認できます。

次のトピックを参照してください。

- [プロセス] または [観測] 画面での XDR データの取得
- [アラート] 画面での XDR データの取得

[プロセス] または [観測] 画面での XDR データの取得

[プロセス] または [観測] 画面でいくつかの種類の XDR データを取得する方法の例を次に示します。

手順

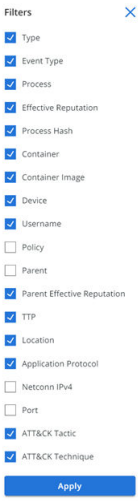
1 左側のナビゲーション ペインで、[調査] をクリックします。

2 [調査] 画面で [プロセス] または [観測] をクリックします。

3 左側の [フィルタ] ペインで、[アプリケーション プロトコル] までスクロールします。以下のプロトコルでフィルタリングできます。

- HTTP
- TLS
- RDP
- DNS
- SMB
- LDAP
- Kerberos

ヒント: 縦に並んだ 3 つのドットの [構成] メニューをクリックして、コンソールに表示されるフィルタを構成します。例：



4 検索クエリを構築して実行します。たとえば、`netconn_domain:go.microsoft.com` を検索します。

> **注：** 4 章 XDR 検索フィールドの netconn 固有の XDR 検索フィールドを参照してください。製品内『検索ガイド』のすべての検索フィールドを参照してください。

次のステップ

検索結果を表示および調査する方法については、 7 章 XDR データの確認 を参照してください。

[アラート] 画面での XDR データの取得

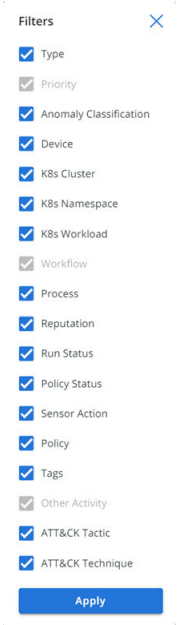
[アラート] 画面で XDR データを取得する方法の例を次に示します。

手順

1 左側のナビゲーション ペインで、[アラート] をクリックします。

2 左側の [フィルタ] ペインで、 [ATT&CK 戦略] までスクロールし、 `TA0002` を選択します。

> **ヒント:** 縦に並んだ 3 つのドットの [構成] メニューをクリックして、コンソールに表示されるフィルタを構成します。例：



3 検索クエリを構築して実行します。例：`Intrusion Detection System` をフィルタリングします。

または、[検索] バーで `type:INTRUSION_DETECTION_SYSTEM` を検索することもできます。

注： 4 章 XDR 検索フィールドの netconn 固有の XDR 検索フィールドを参照してください。製品内『検索ガイド』のすべての検索フィールドを参照してください。

次のステップ

検索結果を表示および調査する方法については、 7 章 XDR データの確認 を参照してください。

XDR データの確認

7

XDR および netconn データは、Carbon Black Cloud コンソールで確認できます。

XDR および netconn データは、さまざまな方法で表示および調査できます。例：

- [プロセス解析] 画面には、特定の netconns（プロトコル、タイムスタンプ、ヘッダー）に関する追加情報が表示されます。
- [アラートのトリアージ] 画面には、IDS 固有の netconns を強調表示するネットワーク ノードが含まれています。
- MITRE ATT&CK 戦略と技術は、[アラート]、[アラートのトリアージ]、[観測]、および [プロセス解析] 画面で使用できます。これらのフィールドを使用して、[プロセス] 画面でもフィルタリングおよび検索できます。

  注： MITRE ATT&CK は XDR に固有ではありません。Carbon Black Cloud インスタンスには、この情報が表示されます。
- [表の構成] オプションを使用して、プロセス中心およびネットワーク中心のビューを構築できます。
- `Application Protocol` フィルタは、[アラート]、[観測]、および [プロセス] 画面で使用できます。
- レポートされた netconn データからウォッチリストを構築できます。

詳細については、次のトピックを参照してください。

次のトピックを参照してください。

- [プロセス解析] 画面での XDR データの確認
- [観測] 画面での XDR データの確認
- [アラート] 画面での XDR データの確認
- [アラートのトリアージ] 画面での XDR データの確認

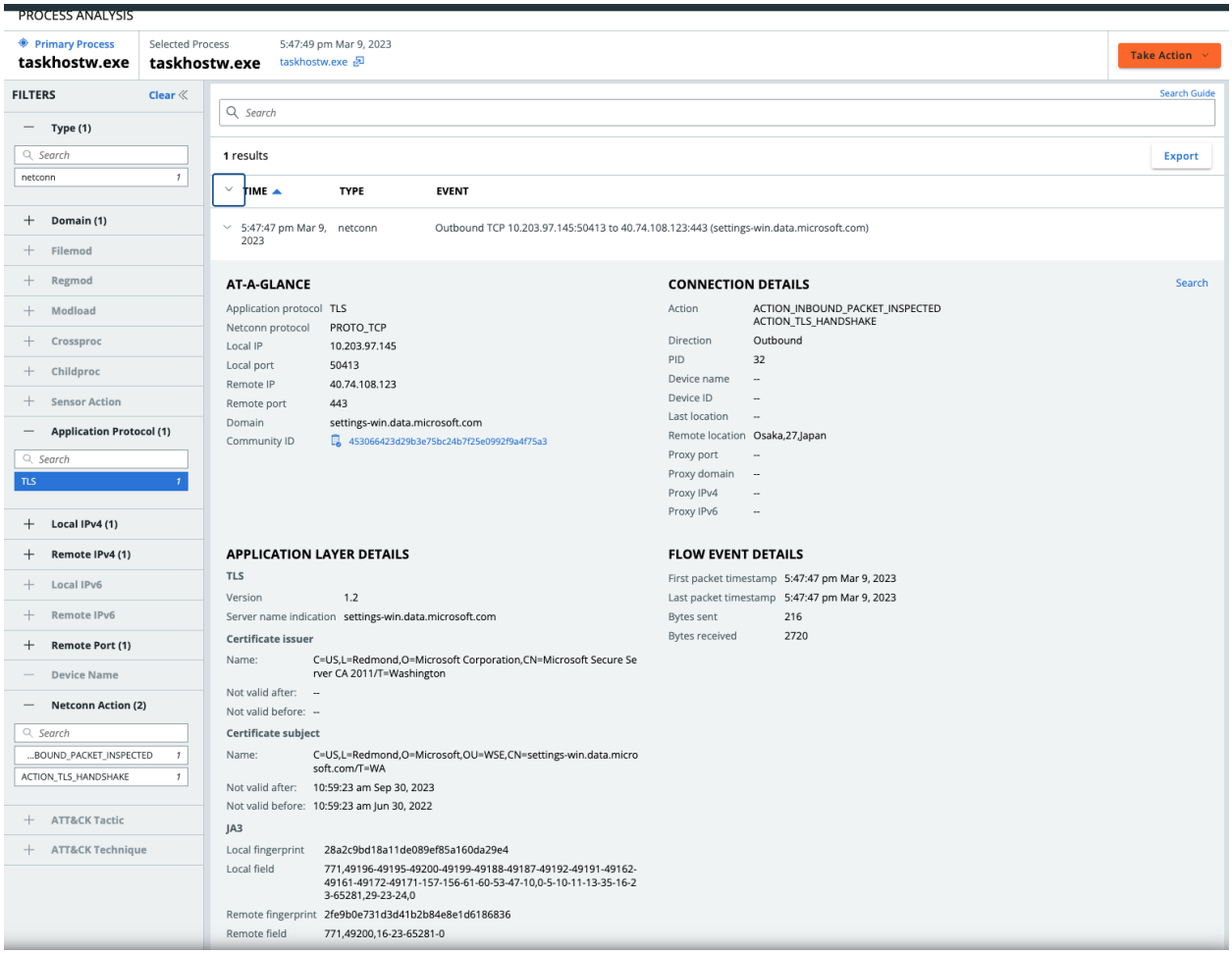
[プロセス解析] 画面での XDR データの確認

イベントを取得したら、[プロセス解析] 画面でデータを確認できます。

注： XDR アクティビティの取得方法については、[プロセス] または [観測] 画面での XDR データの取得 を参照してください。

左側のナビゲーション ペインで、[調査] をクリックし、[プロセス] または [観測] タブをクリックします。次に、目的のアイテムの [プロセス解析] アイコンをクリックします。

raw netconn の詳細を取得できるようになりました。たとえば、XDR 対応システムのプロトコル、タイムスタンプ、およびアプリケーション ヘッダー データが表示されます。

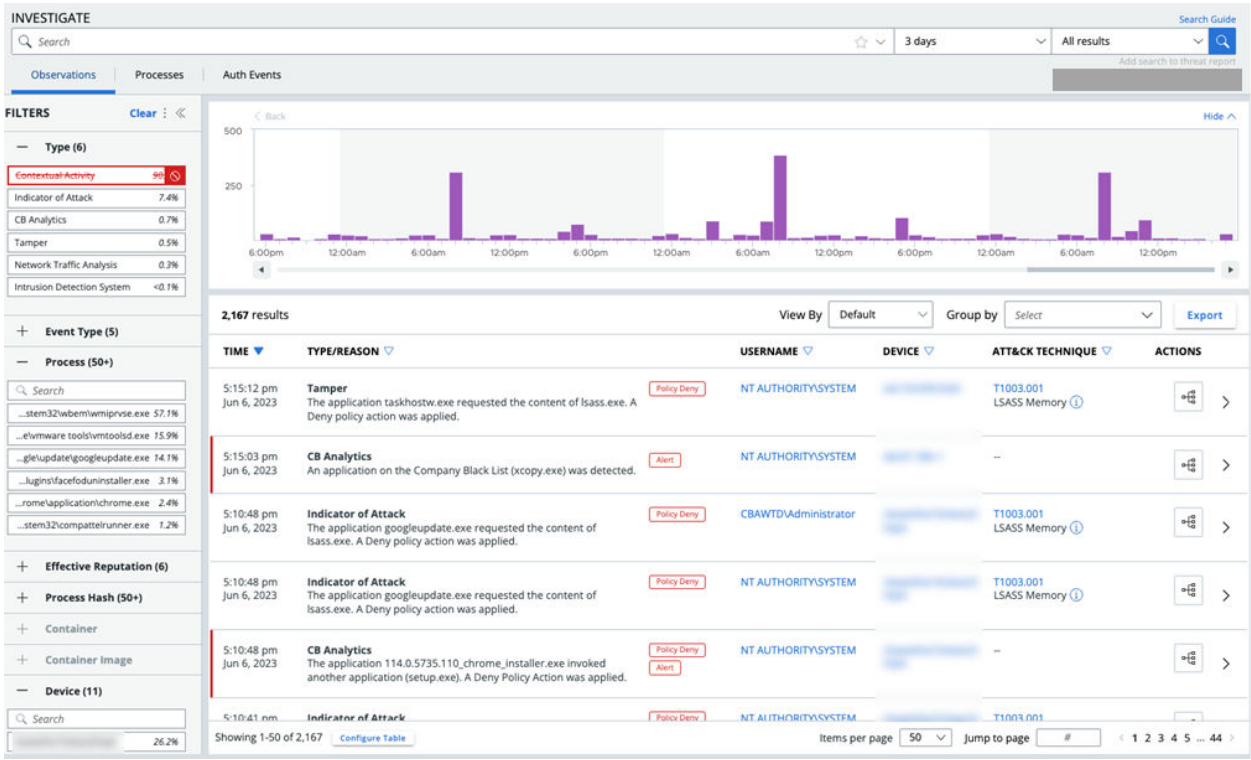


注： [プロセス解析] 画面の一般的な情報については、プロセス解析を参照してください。

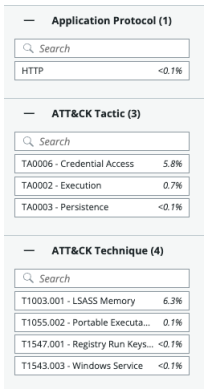
[観測] 画面での XDR データの確認

[観測] 画面で XDR データを取得および確認できます。

左側のナビゲーション ペインで、[調査] をクリックし、[観測] タブをクリックします。



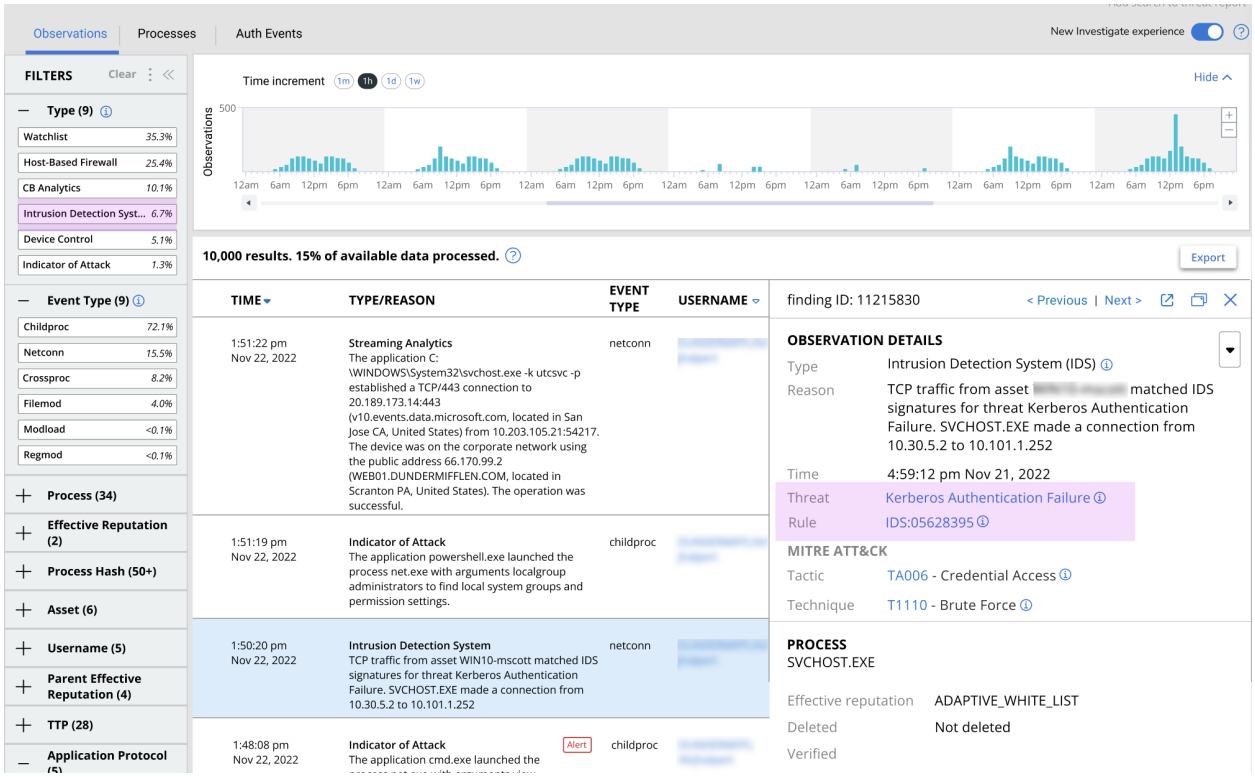
ヒント: 次のフィルタは、観測を検索するときに特に便利です。



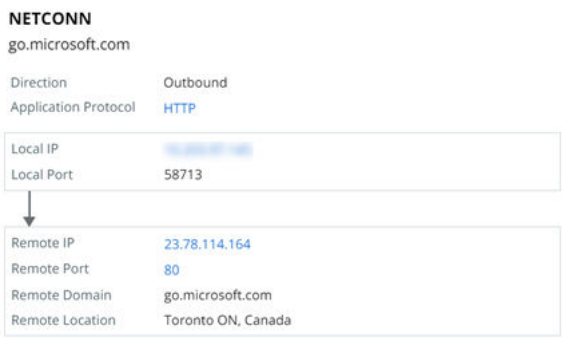
[観測詳細] ペインの XDR データ

目的のアイテムの横にある › アイコンをクリックします。

次の画像は、IDS 観測の詳細を示しています。XDR データが強調表示されます。



もう 1 つの例は、観測に関連付けられている netconn データを示しています。



注： [観測] 画面の一般的な情報については、調査 - 観測を参照してください。

[アラート] 画面での XDR データの確認

[アラート] 画面で XDR データを取得および確認できます。

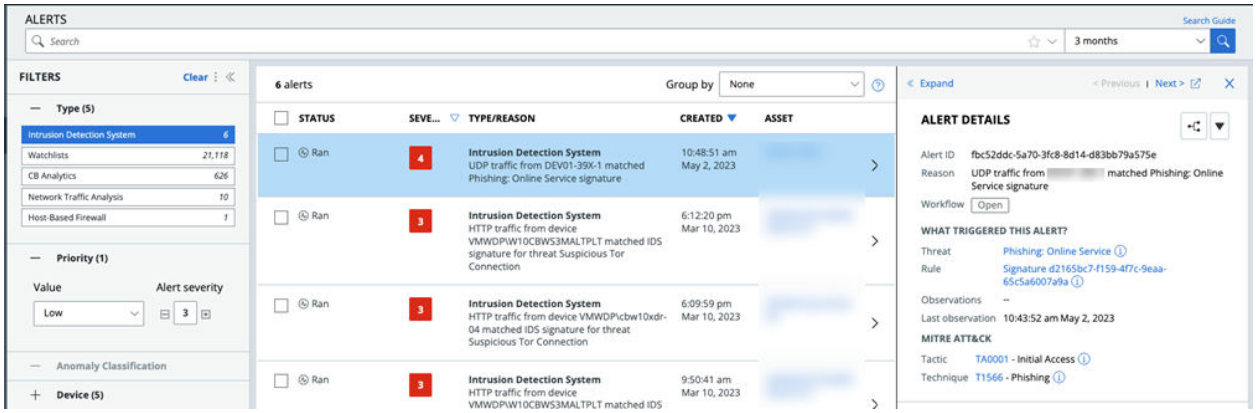
左側のナビゲーション ペインで、[アラート] をクリックします。

注：

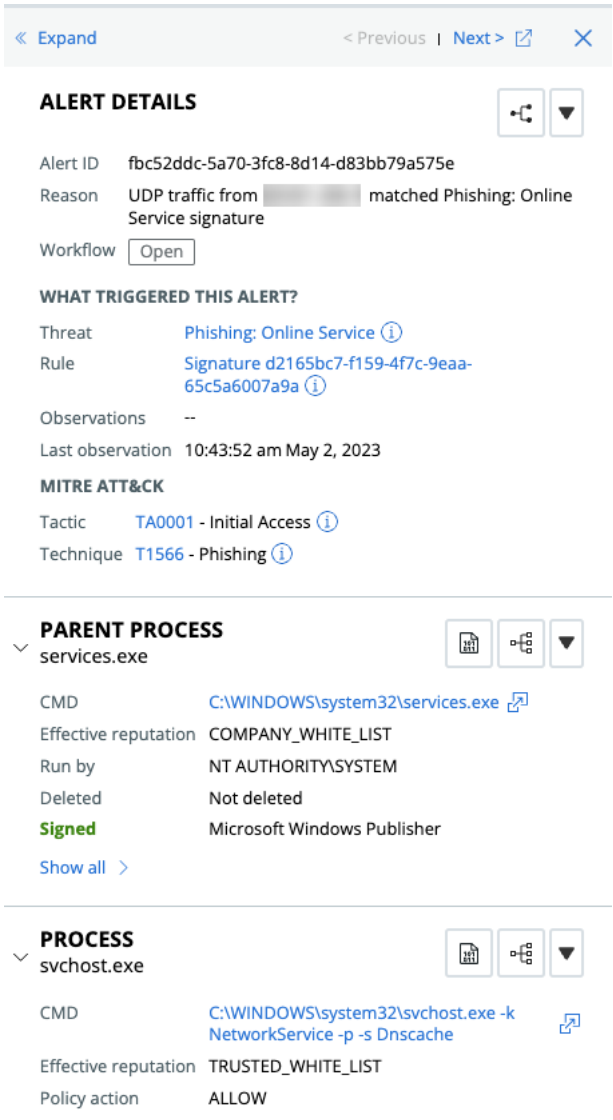
- このトピックでは、[アラート] 画面で netconn 生成プロセスを開いていることを前提としています。「[アラート] 画面での XDR データの取得」を参照してください。
- [アラート] 画面の一般的な情報については、アラートの詳細表示を参照してください。

目的のアイテムの横にある › アイコンをクリックします。

次の画像は、IDS アラートの例を示しています。



次の図は、アラートの詳細な [Netconn] 情報を示しています。



[アラートのトリアージ] 画面での XDR データの確認

XDR データを取得したら、[アラートのトリアージ] 画面でデータを確認できます。

注： XDR アラート データの取得手順については、[アラート] 画面での XDR データの取得を参照してください。

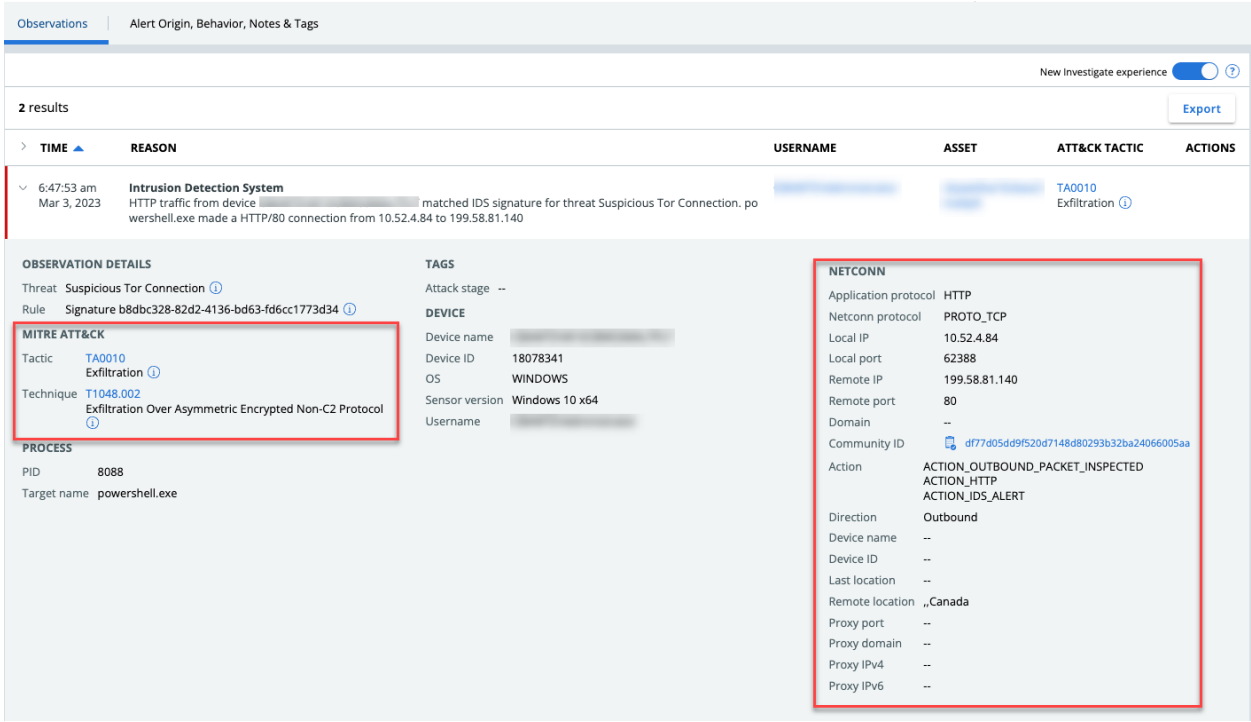
左側のナビゲーション ペインで、[アラート] をクリックし目的のアイテムの横にある [アラートのトリアージ] アイコンをクリックします。

[アラートのトリアージ] 図は、IDS 固有のネットワーク接続を強調表示するネットワーク ノード（ドメインまたは IP アドレス）を示しています。

下部のペインで、[観測] タブを選択して、次のフィールドを表示します。

- 観測が行われた [時間]
- 観測の [理由]。これは、強化されたイベントで以前に利用可能だったビューよりも詳細なビューです。
- 観測をトリガしたプロセスを実行した [ユーザー名]
- [アセット]
- [ATT&CK 戦略と技術]
- 使用可能な [アクション]

アラートを展開すると表示される [観測の詳細] ペインに、MITRE ATT&CK 戦略と技術およびその他の netconn データが表示されます。



注： [アラートのトリアージ] 画面の一般的な情報については、アラートの可視化を参照してください。

調査

8

エンドポイント上のアプリケーションおよびプロセスによって実行される失敗した操作と成功した操作の両方含む、Carbon Black Cloud に保存されているすべての観測の詳細を調査および分析できます。

注：

- Carbon Black Cloud Endpoint Standard 専用ユーザーの [調査] ページにタブが表示されません。デフォルト ビューは [観測] です。
- [観測]、[プロセス]、および [認証イベント] タブは Carbon Black Cloud Enterprise EDR ユーザーのみが使用できます。
- 2023 年 9 月 26 日の時点で、[強化されたイベント] はコンソールから削除されました。[観測] に置き換えられます。

検索結果からデータを収集し、観測とプロセスの詳細に基づいてアクションを実行できます。

[調査] 画面には、クエリの作成に役立つ組み込みの『検索ガイド』が表示されています。高度な検索機能を使用して、アラートに関する詳細情報を検索し、調査を実施して、環境から報告されるイベント、観測、プロセスの普及率を把握できます。VMware Carbon Black Cloud ユーザー ガイド のメイン セクションの「高度な検索技術」「」も参照してください。

値検索

検索時に完全な値を使用します。たとえば、`powershell` または末尾のワイルドカード：`power*`。

検索フィールド

検索フィールドを含むフォーム クエリ：`field:term`。例： `parent_name:powershell.exe`。

ワイルドカード

ワイルドカードを使用してクエリを拡張します。`?` は 1 つの文字に一致します。たとえば、`te?t` は「test」と「text」の結果を返します。`*` はゼロまたはそれ以上の連続文字に一致します。例：`tes*` は「test」、「testing」、「tester」の結果を返します

ファイル拡張子検索において先頭のワイルドカードが考えられます。例：`process_name:.exe`。

値を引用符で囲まない場合や、バックスラッシュで次の特殊文字（`+ - && || ! ( ) { } [ ] ^ " ~ * ? : /`）をエスケープした場合、ワイルドカードをパスに使用できます。例：**(1+1):2** を検索するには、次のように入力します：`\(1\+1\)\:2`。

演算子

演算子を使用してクエリを絞り込むことができます。演算子は大文字である必要があります。

- [AND] は両方の語句が存在する場合に結果を返します
- [OR] はいずれかの語句が存在する場合に結果を返します
- [NOT] は語句が存在しない場合に結果を返します

重要： [暗黙的な「AND」演算子に注意する]

演算子が使用されていない場合でも、暗黙的な「AND」があります。次の例では、両方のクエリで同じ結果が生成されます。

- この例では、「AND」は暗黙的です。

```
Process_name:X process_effective_reptuation:X
```

- この例では、「AND」はクエリの一部です。

```
Process_name:X AND process_effective_reptuation:X
```

エスケープ

サジェスト機能およびフィルタを使用する場合を除き、スラッシュ、コロン、およびスペースは手動でエスケープさせる必要があります。

日付/時間範囲

日付/時間範囲を使用してクエリを絞り込むことができます。例：`device_timestamp:[2022-10-25T14:00:00Z TO 2022-10-26T15:00:00Z]`。

個数検索

カウントを含むクエリーを、範囲やワイルドカードで絞り込むことができます。

- `[3 TO *]` は値が 3 で始まるカウント結果を返します。
- `[* TO 10]` は 10 までのカウント結果を返します。

次のトピックを参照してください。

- 調査 - プロセス
- 調査 - 観測

- 調査 - 認証イベント
- スクリプトベースの攻撃の調査
- プロセス ハッシュの取得
- 脅威レポートへの調査クエリの追加

調査 - プロセス

お使いの環境で実行されたすべてのプロセスの詳細を調査および分析します。

注： [プロセス] タブと [認証イベント] タブは、Carbon Black Cloud Enterprise EDR ユーザーのみが使用できます。

左側のナビゲーション ペインで、[調査] をクリックし、[プロセス] タブをクリックします。

ヒント: また、 プロセス検索 API を使用してセンサーによって報告されたすべてのデータを検索し、設定した特定の基準に基づいて 1 つ以上のプロセスを検索することもできます。

検索結果

製品内の『検索ガイド』を使用して、利用可能な検索語の完全なリストにアクセスし、詳細なクエリの作成に役立ててください。

各プロセスについての結果は以下を含みます。

- 最新のセンサー イベントと分析
- センサーが終了するか、プロセスを拒否するたび
- イベントがサブスクライブしたウォッチリストに一致するたび

プロセスの詳細と操作

キャレットをクリックして、右側のパネルにある追加のプロセス、観測、またはイベント情報を開きます。

- プロセスの名前の横にあるドロップダウン矢印をクリックし、プロセスに関するアクションを実行します。
- [詳細] をクリックして、追加のデバイスの詳細を表示し、デバイスでアクションを実行します。

表のプロセス名の横にバッジのインジケータが現われる場合があります。インジケータの例：

- [ウォッチリストのヒット:] プロセスには関連付けられたウォッチリストのヒットがあります。バッジをクリックして詳細情報を表示してください。
- [アラート:] プロセスには関連付けられたアラートがあります。バッジをクリックして、最も重大度の高いアラートについての追加情報を表示してください。リンクをクリックし、[アラート] 画面に表示される関連付けられたプロセスを持つすべてのアラートを表示します。
- [ポリシーの拒否:] プロセスを有効な状態にしておくが、さらなる操作は拒否するためのポリシーの処理が行われました。これは、プロセスが禁止された DLL のロードを拒否された場合に発生することがあります。場合によっては、プロセスが別のプロセスを開始しようとした場合に発生します。

- [ポリシーの終了:] プロセスを終了するためのポリシーの処理が行われました。

タイトル	説明
プロセス	プロセスの名前とパス。ハイパーリンクされた名前をクリックし、プロセス ツリーのネットワーク接続が可視化されるのを確認します。
デバイス	デバイスの登録名。
デバイス時間	与えられたプロセスのセグメントにおける最新のイベントのデバイス時間。
PID	OS によって定義される固有のプロセス識別子。
ユーザー名	プロセスが実施されたユーザーのコンテキスト。
Regmods	プロセスに関連付けられたレジストリの修正の総数。
Filemods	プロセスに関連付けられたファイルの修正の総数。
Netconns	プロセスに関連付けられたネットワーク接続の総数。
Modloads	プロセスに関連付けられたモジュールのロードの総数。
Childprocs	プロセスに関連付けられた子プロセスの総数。

プロセス解析

このセクションでは、Carbon Black Cloud コンソールの [プロセス解析] 画面について説明します。

注： VMware Carbon Black XDR がある場合は、[プロセス解析] 画面での XDR データの確認 も参照してください。

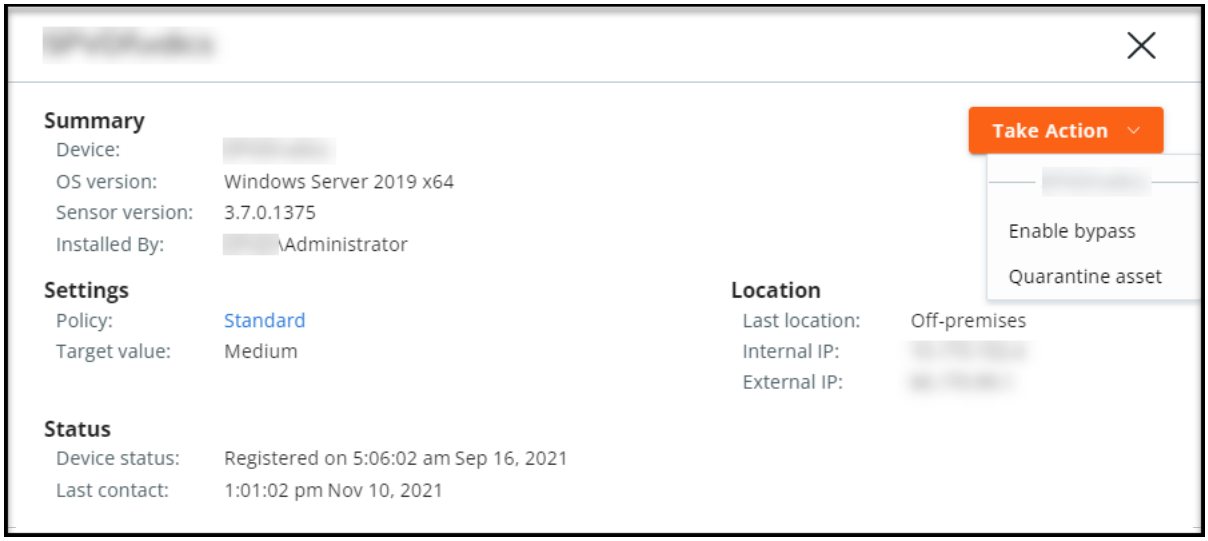
[プロセス解析] 画面の右上にあるオレンジ色の [アクション実行] ボタンをクリックすると、ハッシュを禁止リストにすばやく追加したり、デバイスのバイパス モードを有効または無効にしたり、デバイスを隔離または隔離解除したり、VirusTotal で検出を表示したりできます。

[プロセス解析] 画面の上部セクションには、次の情報が含まれています。

- 解析中のプライマリ プロセス
- 現在選択されているプロセス (ノード)
- 日付と時刻
- プロセス パス
- デバイスの詳細 (以下を含む):
  - 前回ログインしたユーザー
  - OS バージョン
  - デバイス名
  - IP アドレス
  - 位置

- 適用されたポリシー

[詳細] ボタンをクリックすると、このデバイスの詳細が表示されます。



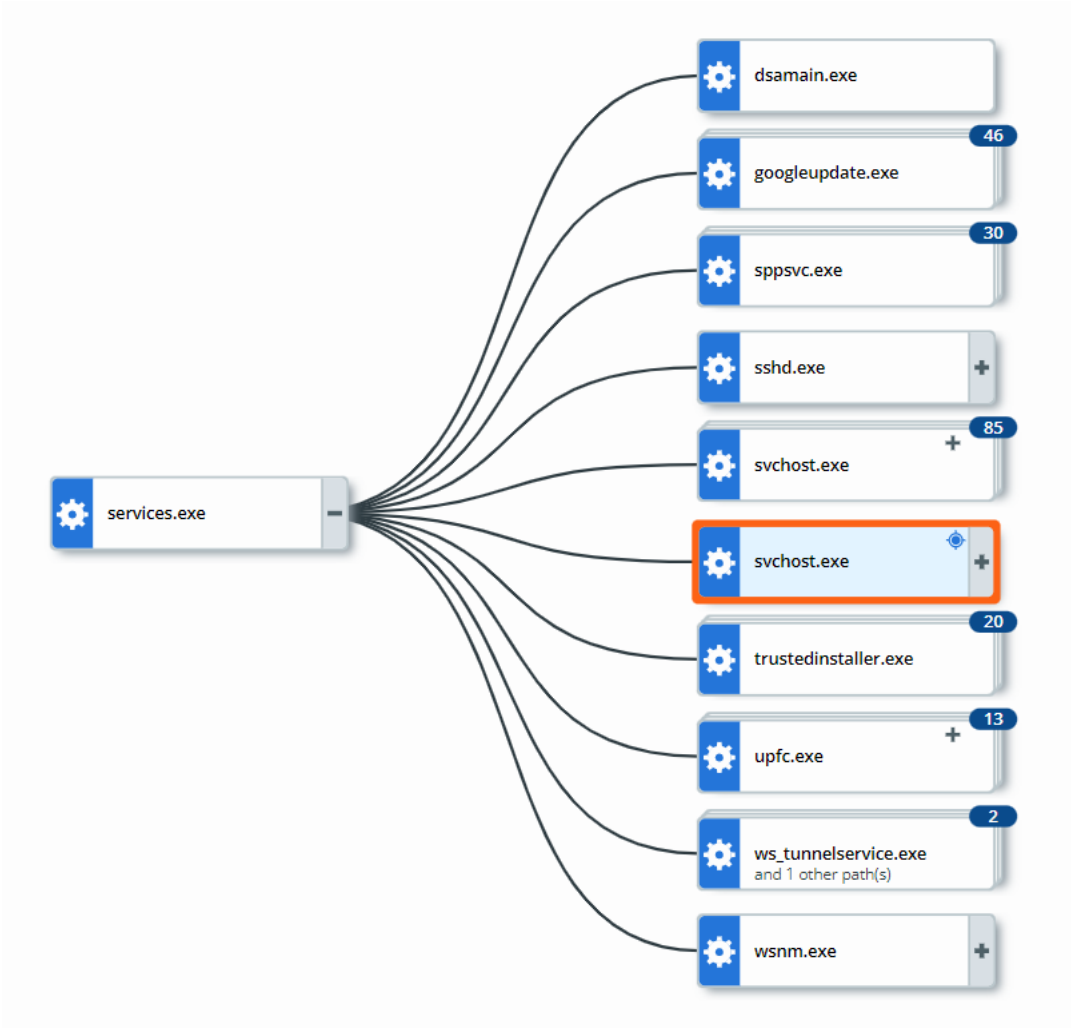
このビューにはその他の詳細が含まれています。

- センサーのバージョン
- インストールした者
- ターゲット バリュー
- デバイスの登録日
- デバイスの最終連絡日
- 最後の場所

このウィンドウの [アクション実行] ボタンをクリックすると、デバイスのバイパスまたは隔離を有効にできます。

プロセスの可視化

プロセスの可視化、またはプロセス ツリーは、[プロセス解析] ページのメイン セクションに表示されます。

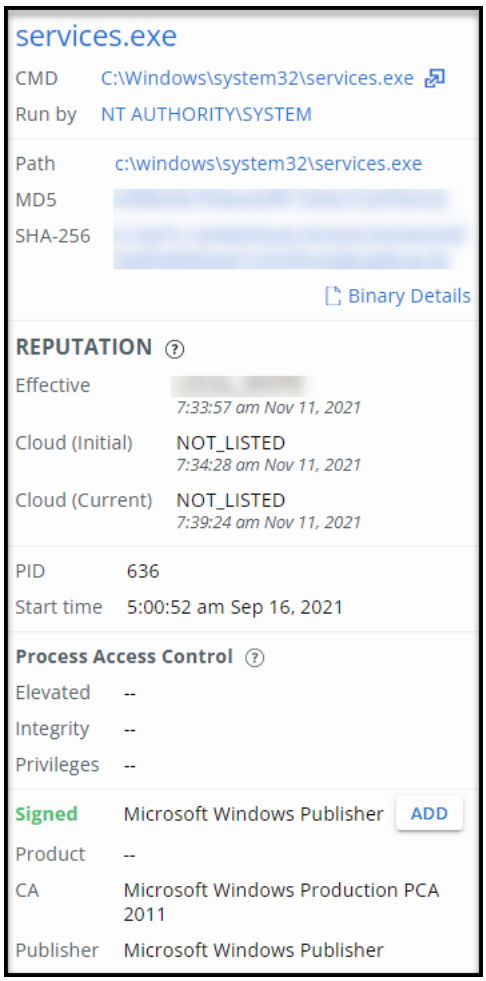


攻撃ストリームの各プロセスはプロセス ツリーにノードとして表示され、攻撃の発生元が左側に、その後の各イベントは、攻撃の進行に伴い左から右に表示されます。親または子プロセスが過剰にあるプロセス ツリーでは、すべてのノードが表示されない場合があります。

[ハッシュによるグループ分け] トグルをクリックすると、ハッシュでプロセスをグループ分けできます。このアクションにより、プロセス ツリーは、子プロセスまたはウォッチリストが存在するかどうかにかかわらず、同一のハッシュを持つすべてのプロセスをグループ化します。ターゲット ノードはグループ化されません。ハッシュでグループ化すると、ページに表示されるノードの数が減り、読みやすさが向上します。

選択されているノード

ノードをクリックして追加情報を表示し、[選択されているノード] の折りたたみパネルでアクションを実行します。



バイナリの詳細

[選択されているノード] パネルで [バイナリの詳細] ボタンを選択して、バイナリに関する追加の詳細情報を表示します。

注： [バイナリの詳細] ボタンは、Carbon Black Cloud Enterprise EDR でのみ使用できます。

レピュテーション

レピュテーションは、信頼度または不信度の特定のレベルです。

- [有効なレピュテーション] は、Carbon Black 分析、クラウド インテリジェンス、およびその他のデータに基づいて、イベントや観測が発生した時点でセンサーによって適用されるレピュテーションです。
- [クラウド レピュテーション (初期)] は、バックエンドによってイベントや観測が処理されたときに Carbon Black Cloud インテリジェンス ソースによってレポートされたハッシュ レピュテーションです。
- [クラウド レピュテーション (現在)] は、Carbon Black Cloud インテリジェンス ソースによってレポートされたハッシュ レピュテーションをリアルタイムでチェックしたものです。

注： [有効なレピュテーション]は、Endpoint Standard を実行しているユーザーにのみ適用されます。

プロセス アクセス コントロール

- [昇格]: 「True」の場合、プロセスは昇格した (管理者) コンテキストで実行されます。プロセスを昇格させると、UAC (ユーザー アクセス コントロール) を設定するポリシーは適用されません。
- [整合性]: 高 (管理者)、中 (標準ユーザー)、または低 (制限付き)。より高い整合性レベルを持つプロセスとの接触を防止することによって信頼度が強化されます。
- [権限]: セキュリティ ID (権限) をカプセル化するアクセス トークンが各プロセスに割り当てられます。権限は、プロセスを実行しようとしたときにセキュリティ境界を適用するのに役立ちます。

ウォッチリストのヒット

プロセスにオレンジ色の [が表示されます。] はプロセスがウォッチリストのヒットに関連していることを示します。この場合、[選択されているノード] ペインにも次のように表示されます。

- 最新のヒットの重要度スコア
- ヒットが見つかったレポートの名前
- ヒットが発生したクエリ
- ウォッチリストのヒットとしてキャプチャされたイベントの発生時刻

クエリのリンクを選択して、検索バーでクエリが事前に入力された [調査] 画面にピボットします。

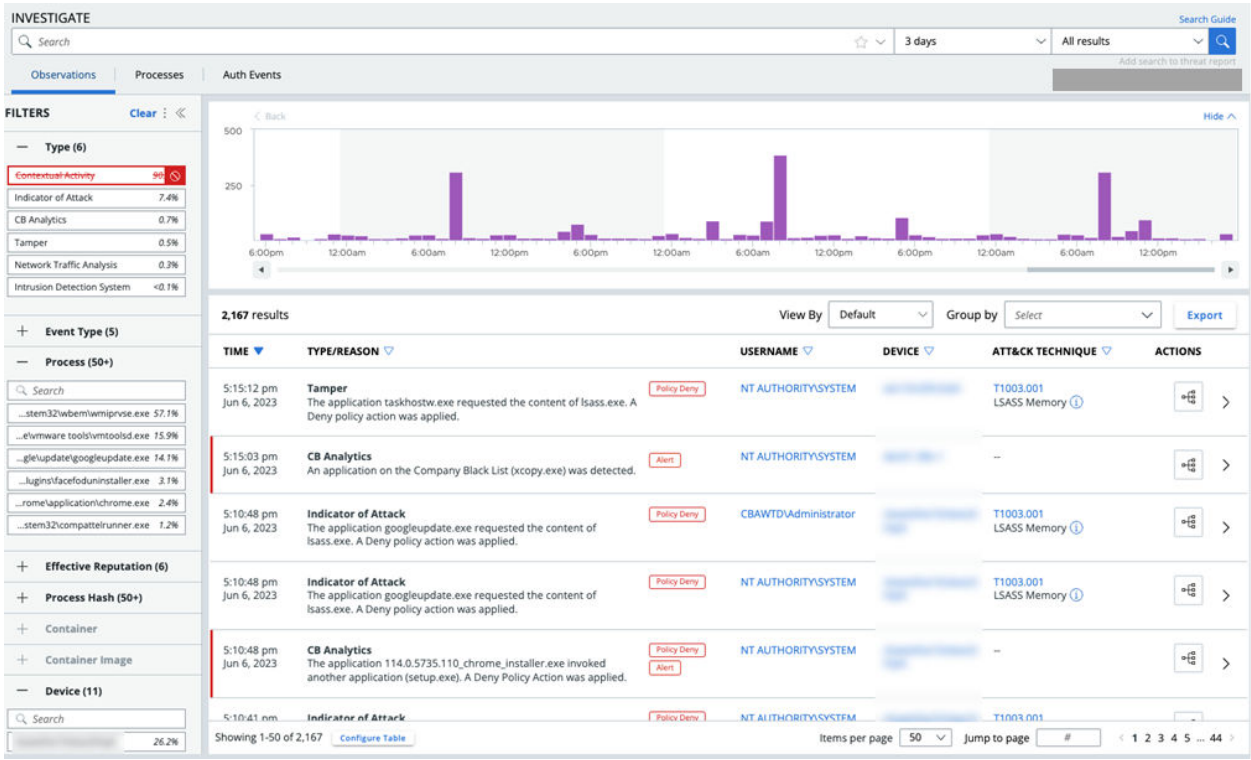
調査 - 観測

[観測] は、Carbon Black Cloud Endpoint Standard および VMware Carbon Black XDR ユーザーのデフォルトの調査ビューです。このページは、Carbon Black Cloud Endpoint Standard または VMware Carbon Black XDR を所有している Carbon Black Cloud Enterprise EDR ユーザーにも表示されます。

注：

- このセクションでは、[観測] 画面の一般的な説明を提供します。XDR 固有のデータに関する詳細については、[観測] 画面での XDR データの確認を参照してください。
- Carbon Black Cloud Enterprise EDR を持っていない Carbon Black Cloud Endpoint Standard のユーザーの場合は、[調査] 画面にタブ オプションはありません。[観測] はデフォルトの画面ビューです。

左側のナビゲーション ペインで、[調査] をクリックし、[観測] タブをクリックします。



ヒント: 観測 API を使用してすべての観測を検索し、検索条件に一致する 1 つ以上の特定の観測を検索することもできます。

観測の概要

[観測] 画面では、アラート生成が必ずしも重要であるとは限らない、環境内の興味深いアクティビティや疑わしいアクティビティを確認できます。

この画面では、1 つ以上のデバイス上の注目すべきアクティビティのストリームを検索できます。すべてのアセットによって報告されるすべての raw イベントを調査することを回避できます。この画面は、組織のすべてのアセットの全面的な検索を実行するための便利な手段を提供します。

観測は、フリート全体で注目に値する検索可能な調査結果です。これらは、[プロセス解析] 画面の raw イベントを補完します。すべての観測に対応する raw イベントがあるわけではありません。すべての観測が本当に疑わしいわけではありません。

観測されたイベントのより小さなサブセットがさらにアラート ステータスに昇格します。

そのため、観測は疑わしいイベントの中間レイヤーです。

観測の検索

このトピックでは、[観測] 画面で検索をフィルタリングする方法について説明します。

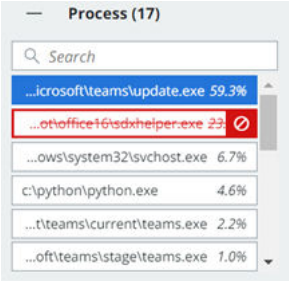
注： 検索結果には 10,000 件の結果制限が適用されます。

次の方法で検索結果をフィルタリングできます。

フィルタ	例
タイプ **注：** 観測タイプに観測 `Type` の説明を表示します。	■ CB 分析 ■ コンテクスト アクティビティ ■ TAU Intelligence ■ 改ざん ■ ブロックされたハッシュ ■ 侵入検知システム ■ ネットワーク トラフィックの分析 ■ ホストベースのファイアウォール ■ 攻撃のインジケータ
イベント タイプ	■ netconn ■ childproc ■ filemod ■ crossproc ■ regmod ■ modload ■ scriptload
プロセス	■ \system32\svchost.exe ■ system32\services
有効なレピュテーション	■ TRUSTED_WHITE_LIST ■ LOCAL_WHITE ■ COMPANY_WHITE_LIST ■ ADAPTIVE_WHITE_LIST ■ NOT_LISTED
プロセス ハッシュ	
デバイス	■ macOS_workstation ■ Windows11_workstation
ユーザー名	■ NETWORK SERVICE ■ SYSTEM ■ LOCAL SERVICE
親の有効なレピュテーション	■ TRUSTED_WHITE_LIST ■ LOCAL_WHITE ■ COMPANY_WHITE_LIST ■ ADAPTIVE_WHITE_LIST ■ NOT_LISTED
TTP	■ NETWORK_ACCESS ■ ACTIVE_SERVER ■ RUN_UNKNOWN_APP ■ CODE_DROP ■ POLICY_DENY ■ INTERNATIONAL_SITE

フィルタ	例
位置	■ シアトル、ワシントン州、アメリカ合衆国 ■ サンノゼ、カリフォルニア州、アメリカ合衆国 ■ ダブリン、L、アイルランド
アプリケーション プロトコル	■ HTTP ■ TLS
ATT&CK 戦略	■ TA0002 ■ TA0004
ATT&CK 技術	■ T1003.0001 ■ T1036.0005 ■ T1105

ヒント: フィルタの右側にある [除外] アイコンをクリックすると、検索結果を除外できます。例：



観測タイプ

このトピックでは、観測タイプについて説明します。

観測の検索の説明に従って、`Type` でクエリをフィルタリングできます。次の表で、これらのタイプについて説明します。

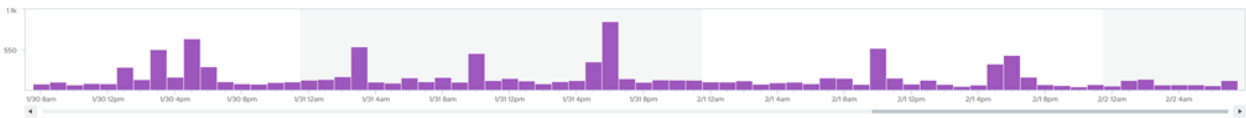
タイプ	説明
ブロックされたハッシュ	この観測タイプは、Carbon Black Cloud Enterprise EDR 環境にのみ適用されます。これは、プロセスがハッシュ禁止リストに表示されるハッシュをロードするときに表面化する観測とアラートで構成されます。
CB 分析	エンドポイントで実行されているプロセスの動作パターンを監視する Carbon Black Cloud 分析を使用して作成された観測とアラート。CB 分析アラートは攻撃を検出しますが、攻撃を防止することはありません。
コンテクスト アクティビティ	コンテキスト アクティビティは、センサーによってキャプチャされたイベントですが、Carbon Black 検出とは一致しません。これらのイベントは、潜在的な攻撃が観測されたのと同じ時にエンドポイントで何が発生していたかについてのコンテキストを確立するのに役立ちます。 コンテキスト アクティビティの観測がアラートに昇格すると、CB 分析観測として再分類されます。

タイプ	説明
ホストベースのファイアウォール	ネットワーク トラフィックがエンドポイントのホストベースのファイアウォール ルールに一致したときに生成される観測。
攻撃のインジケータ (IOA)	攻撃の既知のインジケータに一致し、ほとんどの場合、既知の MITRE ATT&CK 技術に関連付けられているエンドポイントの動作から発生する観測。攻撃のインジケータは、必ずしも本質的に悪意があるわけではありませんが、確認する必要があります。
侵入検知システム (IDS)	単一のネットワーク フローで既知の悪意のあるパターンまたは疑わしいパターンを示すネットワーク トラフィックに起因する観測とアラート。ほとんどの場合、これらの動作は既知の MITRE ATT&CK 技術にマッピングされます。 Carbon Black は、既知のシグネチャに対して疑わしいネットワーク トラフィックを監視します。このようなシグネチャが見つかると、IDS 観測が生成されます。
ネットワーク トラフィック分析 (NTA)	NTA は、ネットワークの可用性とアクティビティを監視して、アノマリを特定します。
改ざん	オペレーティング システムまたは Carbon Black Cloud センサーを改ざんしているプロセスの証拠をキャプチャする観測とアラート。 これらの観測とアラートは、センサーの改ざんの試みを検出して防止するポリシー ルールによって発生する可能性があります。
TAU Intelligence	Carbon Black Threat Intelligence Unit (TAU) からの特定の調査結果によって生成される観測。 このカテゴリには、センサーの動作パターンの分析を使用して作成された観測とアラートが含まれます。これらの観測とアラートが、防止につながることも少なくありません。

ヒストグラム

このトピックでは、[観測] 画面の上部にあるヒストグラムについて説明します。

ヒストグラムはインタラクティブです。ヒストグラムを表示または非表示にできます。



ヒストグラムとそれに関連付けられたデータは、次の方法で操作できます。

- ヒストグラム内の任意の場所をクリックして、特定の時間に発生したイベントに焦点を当てます。
- ヒストグラムの下部にあるスクロール バーを使用して、時間の前後に移動します。
- ヒストグラムにカーソルを合わせると、カーソルが [+] の記号に変わります。[+] をクリックアンドドラッグして、特定の時間セグメントに焦点を当てます。
- [< 戻る] ボタンをクリックして、前のヒストグラム ビューに戻ります（その外観を変更する前）。
- 特定の期間内に発生したイベント（1 分、10 分、1 時間、1 日など）をグループ化します。

グループ化の基準と表示方法

このトピックでは、[観測] 画面の [グループ化の基準] および [表示方法] の機能について説明します。

イベントを期間別にグループ化するだけでなく、次のフィールドでグループ化することもできます。

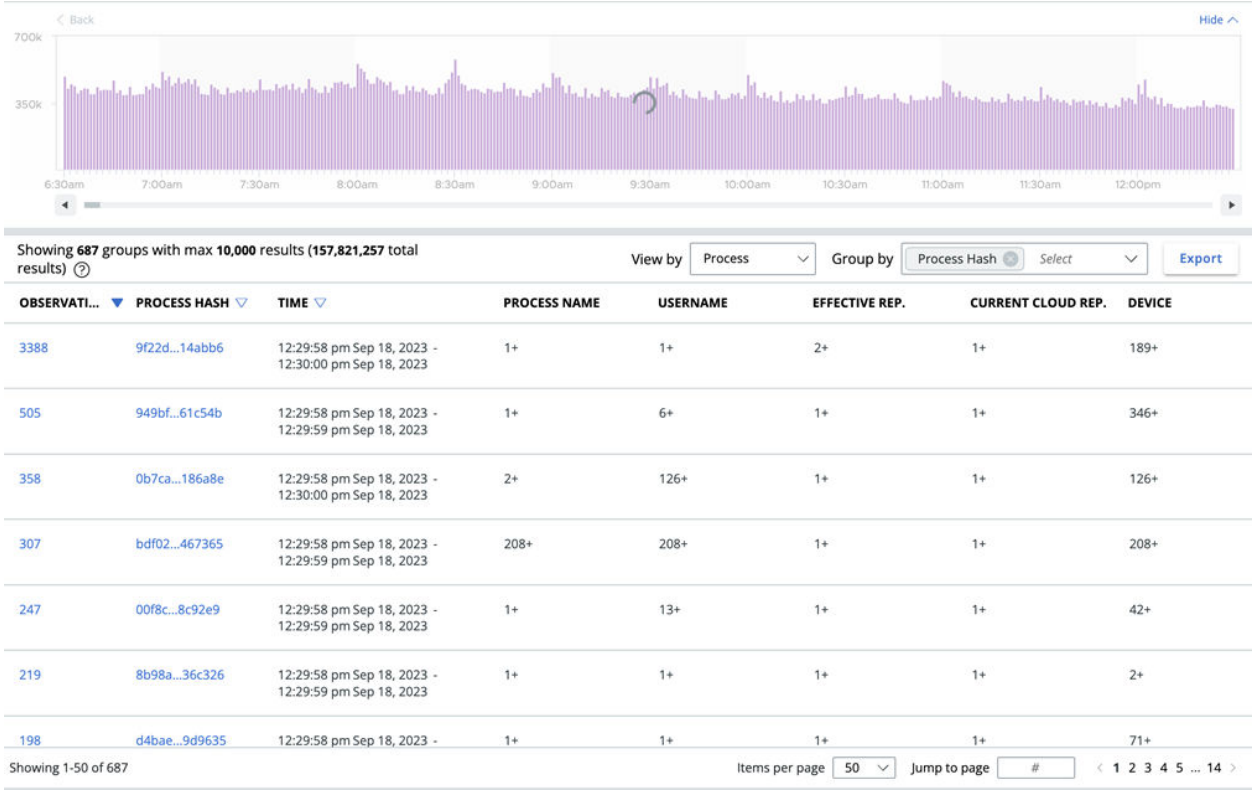
- タイプ
- デバイス
- ユーザー名
- ローカル IP アドレス
- リモート IP アドレス
- ATT&CK 戦略
- プロセス ハッシュ

注： グループ化できるのは、表に表示されるフィールドのみです。[グループ化] アクションを実行する前に、ページの下部にある [テーブルの構成] ボタンをクリックして、テーブルに表示する列（フィールド）を構成できます。

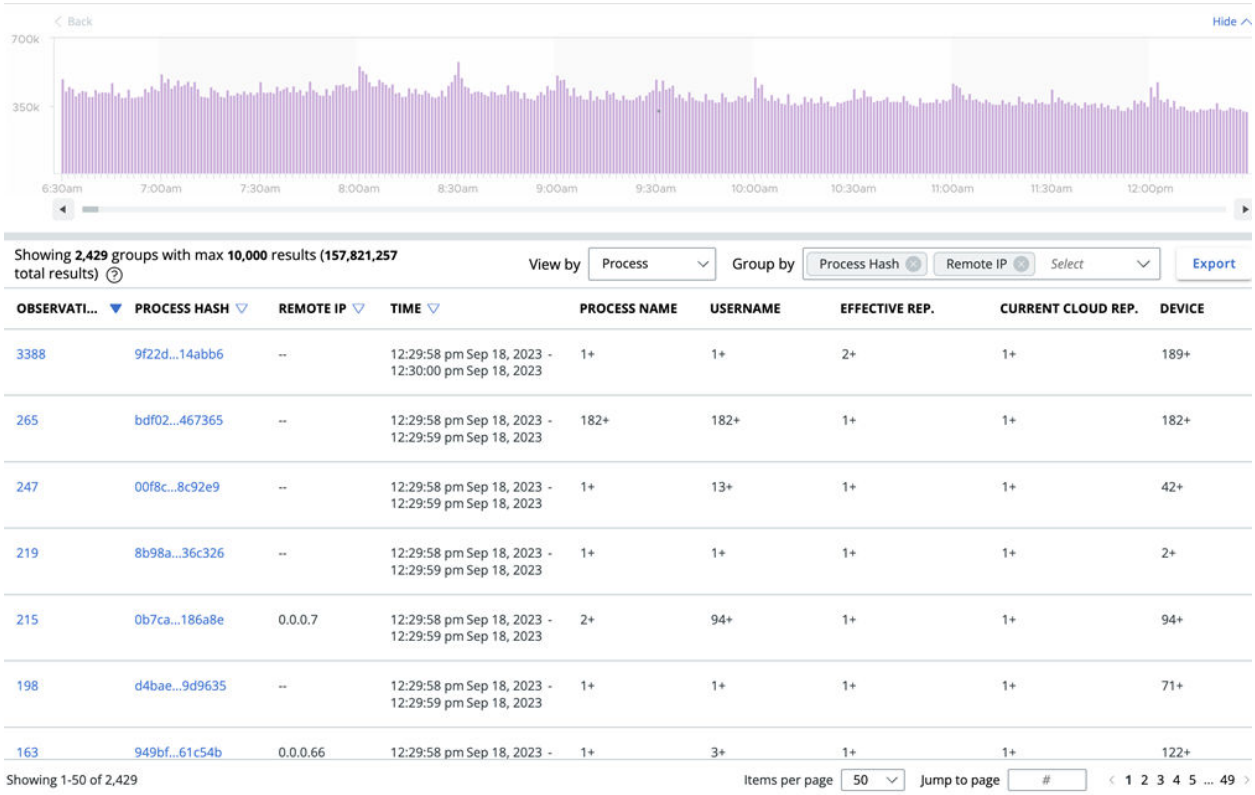
グループ化された結果には、10,000 件の結果制限が適用されます。

[表示方法] オプションで、[デフォルト]、[プロセス]、[デバイス]、または [ネットワーク] 別で表示できます。各ビューを構成して、各ビューに表示する列を決定するには、ページの下部にある [テーブルの構成] ボタンをクリックします。

[表示方法] と [グループ化] 機能を使用すると、結果の興味深い組み合わせを行うことができます。たとえば、[表示方法] を使用すると、データに適用する列セットをすばやく変更できます。[ネットワーク別に表示] を選択すると IP アドレス、ポート、およびプロトコルの列が表示されます。その後、[リモート IP アドレスでグループ化] して、各リモート IP アドレスで発生した観測の数を確認できます。また、[プロセス別に表示] と [プロセス ハッシュ別にグループ化] を使用して、環境内で実行されているすべてのアプリケーションを確認することもできます。

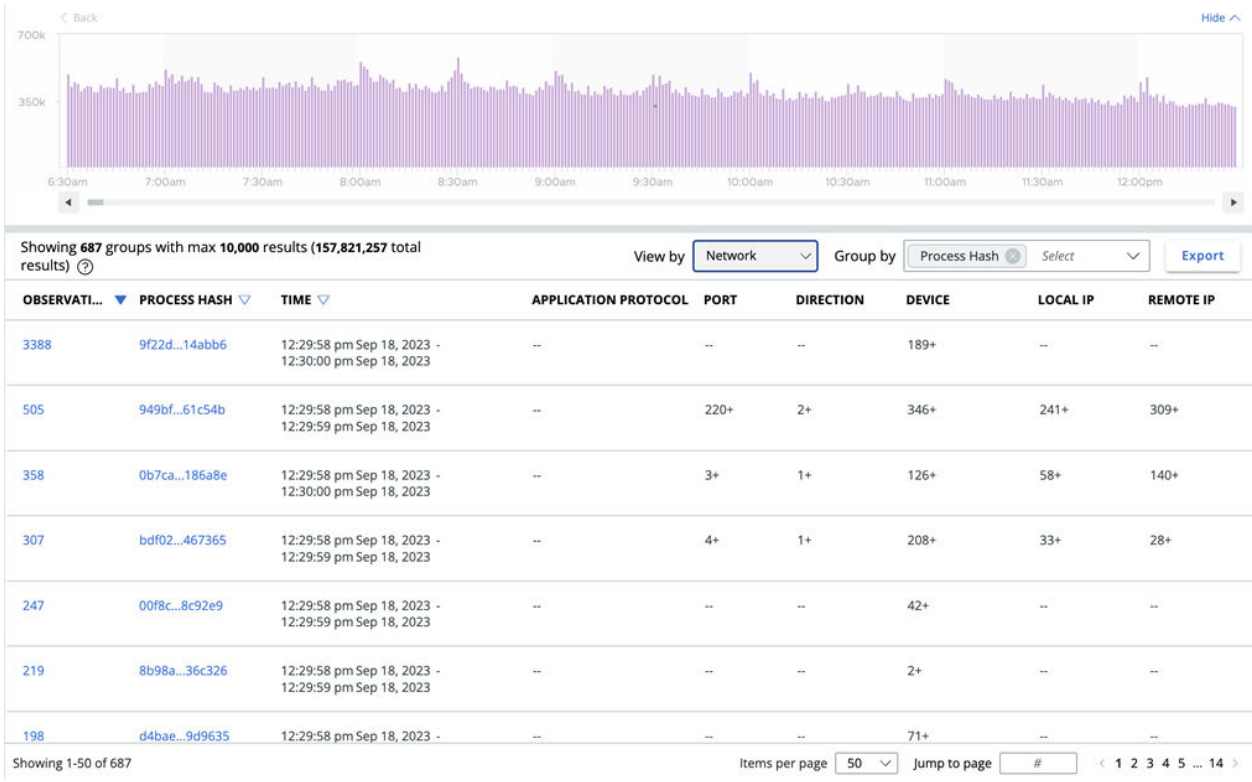


次に、[リモート IP アドレス別にグループ化] を追加して、各ソフトウェアまたはマルウェアの変異によって接触されたリモート IP アドレスの数を確認できます。



複数のグループ化を使用すると、複数の範囲にわたるアクティビティの広がりを確認できます。最初に [プロセス] 別、次に [IP アドレス] 別にグループ化すると、どのプロセスがどの IP アドレスに最も頻繁に接触しているかを表示できます。このビューは、特定の IP アドレスに接触しているユーザーを特定するのに役立ちます。

グループ化されたデータはさまざまな方法で表示できます。たとえば、[ネットワーク別に表示] してから [プロセス ハッシュ別にグループ化] して、どのプロセスが最も多くの IP アドレスに接触しているかを確認します。この組み合わせは、ノイズが最も多いプロセスを確認するのに役立ちます。



検索結果の観測

[観測] 画面で検索クエリを実行し、関心のあるデータ セットを取得すると、結果が表形式で表示されます。

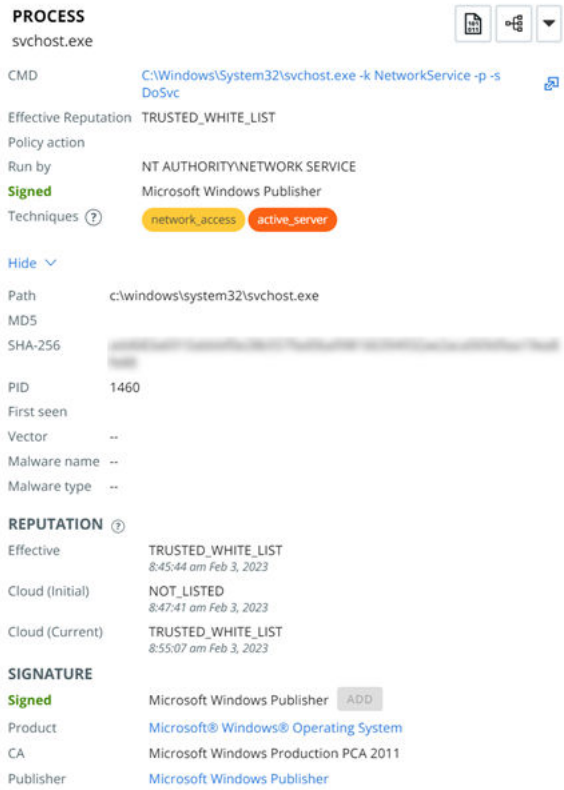
表示するオプションは次のとおりです。

- 表の右上にある [エクスポート] ボタンをクリックして、このデータをエクスポートします。
- グループ化の基準と表示方法の説明に従って結果をグループ化して表示します。
- ほとんどの列ヘッダーの横にある並べ替えキャレットを使用して表を並べ替えます。
- 表の左下にある [表の構成] ボタンをクリックして、表示する列をカスタマイズします。

ヒント: [表の構成] 機能を使用して、デフォルトで表示されない列（[ATT&CK TECHNIQUE] など）を追加できます。

観測のプロセスとそのすべてのイベントを表示するには、行の右側にある [プロセス解析] アイコンをクリックします。[プロセス解析] 画面での XDR データの確認とプロセス解析を参照してください。

イベントに関するその他の詳細を表示するには、行の右側にある › をクリックします。詳細のサマリが表示されます。任意のセクションで [すべて表示] をクリックすると、そのカテゴリのすべての詳細が表示されます。例：



このパネルから、イベントのバイナリの詳細を表示したり、[プロセス解析] 画面を開いたり、イベントに対してアクションを実行したりできます。

実行可能ファイルで使用可能なアクションは次のとおりです。

- 承認リストからハッシュを削除または禁止リストからハッシュを削除
- 禁止リストにハッシュを追加または承認リストにハッシュを追加
- アップロードをリクエスト
- VirusTotal で検索
- アプリケーションを削除

デバイスで使用可能なアクションは次のとおりです。

- バイパスを有効化
- アセットの隔離
- ライブ状態に移行

注： 検索クエリの作成については、製品内の『検索ガイド』を参照してください。

調査 - 認証イベント

Carbon Black Cloud Enterprise EDR は Identity Intelligence を搭載しています。Identity Intelligence は、Windows エンドポイントで発生する認証イベントを可視化します（Windows 10.0.15063 以降で実行している Carbon Black Cloud Windows Sensor 3.9.1 以降でサポート）。

注： [プロセス] タブと [認証イベント] タブは、Carbon Black Cloud Enterprise EDR ユーザーのみが使用できます。

Identity Intelligence は、Carbon Black Cloud Enterprise EDR がユーザー認証アクティビティに提供する可視性を向上させます。このタイプのエンドポイント テレメトリは、アノマリと脅威を特定するために不可欠です。

Identity Intelligence を使用すると、Carbon Black Cloud Enterprise EDR はさまざまなタイプの Windows 認証イベントを収集します。このイベントは、[調査] ページの [認証イベント] タブで報告されます。

Windows 認証イベントのレポートは、プロセス イベントのレポートを補完します。これにより、認証とプロセス アクティビティの相関が可能になり、よりコンテキストに富んだ脅威ハンティング、調査、インシデント応答が得られます。

認証イベント データは、次のイベント（およびその他）に関する判断材料を提供します。

- 攻撃者の認証ベースの戦略、技術、手順 (TTP)
- 対象のプロセス アクティビティが発生したときにエンドポイントにログインしていたユーザー
- エンドポイントへのログインを試行したが失敗したユーザー
- 総当たり攻撃
- 想定時間外にログインを試行しました
- アノマリまたは疑わしいソースからのリモート認証の試行
- 権限昇格の試行
- アカウントの変更
- 盗まれた認証情報の使用
- エンドポイント間の水平方向の移動
- インサイダー脅威の動作

Security Operations Center (SOC) アナリストが認証イベントのレポートから得られるメリットの一部は次のとおりです。

- エンドポイント アクティビティの可視性の向上
- 脅威ハンティングおよびインシデント応答中の追加のコンテキスト
- 認証イベントとプロセス イベントの相関関係の向上
- 平均応答時間の短縮 (MTTR)

- 統合：認証イベントの収集に対するサードパーティ ソリューションへの依存度が低下しました

ヒント: 認証イベント API を使用して、Windows エンドポイントで発生する認証イベントを可視化することもできます。

認証イベントの収集を有効にする

認証イベントの収集を有効にするには、次の手順を実行します。

手順

1 左側のナビゲーション ペインで、[適用] - [ポリシー] の順にクリックします。

2 変更するポリシーを選択します。

3 [センサー] タブをクリックします。

4 [認証イベントの収集を有効にする] チェック ボックスを選択します。

5 [保存] をクリックします。

コンソールでの認証イベントの表示

[調査] 画面の [認証イベント] タブには、Carbon Black Cloud Enterprise EDR ユーザーの Windows エンドポイントで発生するユーザー認証イベントが表示されます。

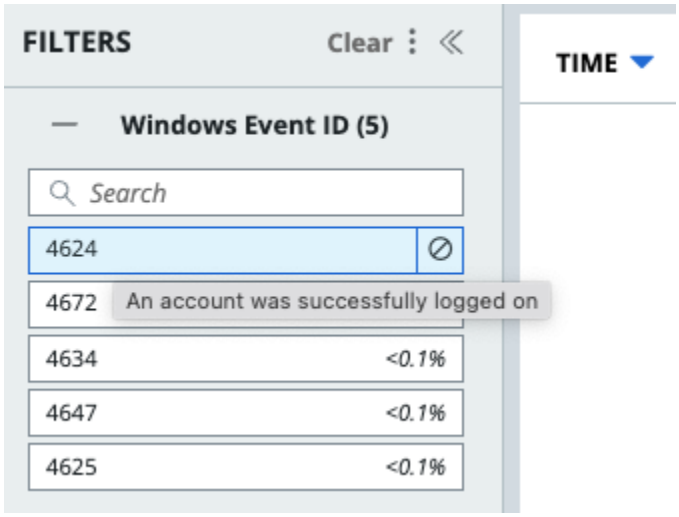
注： デフォルトでは、認証イベントの収集は無効になっています。[調査] 画面で認証イベントを表示するには、ポリシーで [認証イベントの収集を有効にする] 必要があります。認証イベントの収集を有効にするを参照してください。

左側のナビゲーション ペインで、[調査] をクリックし、[認証イベント] タブをクリックします。イベントを検索します。認証イベントの使用可能な検索フィールドを表示するには、製品内の『検索ガイド』を参照してください。イベントを次の基準でフィルタリングできます。

Windows イベント ID	ユーザー名	ユーザー ID (Windows セキュリティ ID)
ログイン タイプ	ログイン ID	ドメイン
リモート デバイス	リモート IP アドレス	ポート

権限	インタラクティブ ログイン	リモート ログイン
親プロセス	プロセス	デバイス

注： Windows イベント ID フィルタには、フィルタの上にカーソルを置くと表示されるツールチップ機能が含まれています。ツールチップには、Windows イベント ID を説明します。例：



Windows 認証イベント

このトピックでは、Carbon Black Cloud が収集して報告する認証イベントについて説明します。

Windows イベント ID	説明
4624	アカウントが正常にログインしました
4625	アカウントがログインに失敗しました
4634	アカウントがログオフされました
4647	ユーザーがログオフを開始しました
4672	新しいログインに割り当てられる特別な権限（管理者に相当）
4740	ユーザー アカウントがロックアウトされました
	ログイン セッションが検出されました

例：

TIME	EVENT ID	DESCRIPTION	USERNAME	DEVICE
1:21:13 am Nov 9, 2022	4624	An account was successfully logged on	SYSTEM	
1:21:13 am Nov 9, 2022	4672	Special privileges assigned to new logon		
1:21:11 am Nov 9, 2022	4634	An account was logged off		
12:52:11 am Nov 9, 2022	4624	An account was successfully logged on	SYSTEM	
12:52:11 am Nov 9, 2022	4672	Special privileges assigned to new logon		

`Logon session detected` イベントは、次の場合に発生します。

- ログイン イベントが発生した後、センサーは認証イベント機能をサポートするバージョンにアップグレードされましたが、センサーはアクティブなログイン セッションの存在を検出します。
- ログイン イベントの発生後に認証イベントの収集が有効になりましたが、センサーはアクティブなログイン セッションの存在を検出します。

アセットで認証イベントが発生したときに認証イベントの収集が非アクティブであったため、`Logon session detected` イベントにはイベント ID がありません。

[認証イベント] タブには、1 つ以上の共有属性で認証イベントをグループ化できる [グループ化の基準] 機能が導入されています。

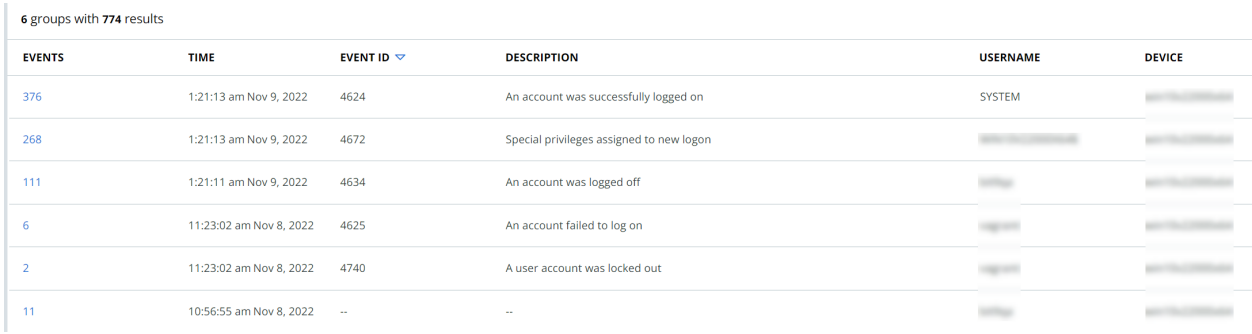
認証イベントは、次の基準でグループ化できます。

- Windows イベント ID
- ユーザー名
- デバイス
- リモート IP アドレス
- 時間 (1 分、10 分、1 時間、1 日)

たとえば、同じ Windows イベント ID を持つすべてのイベントをグループ化するには、[グループ化の基準] ドロップダウン メニューで [Windows イベント ID] を選択します。結果の表には、Windows イベント ID 別のグループ毎のイベント数が一覧表示されます。その数をクリックすると、グループが展開され、選択した時間範囲および/または結果数の基準内にある特定の Windows イベント ID のすべてのイベント (10,000 件の結果制限内) を表示することができます。

同じ 1 時間内に発生した同じ Windows イベント ID を持つイベントをグループ化するには、[グループ化の基準] ドロップダウン メニューで [Windows イベント ID] と [1 時間] を選択します。

認証イベントの結果には、複数の [グループ化の基準] 属性を一度に適用できます。[グループ化の基準] 属性を選択する順序は、結果のグループ化や表示方法には影響しません。[グループ化の基準] 属性の適用は順次行われるものではありません。



6 groups with 774 results

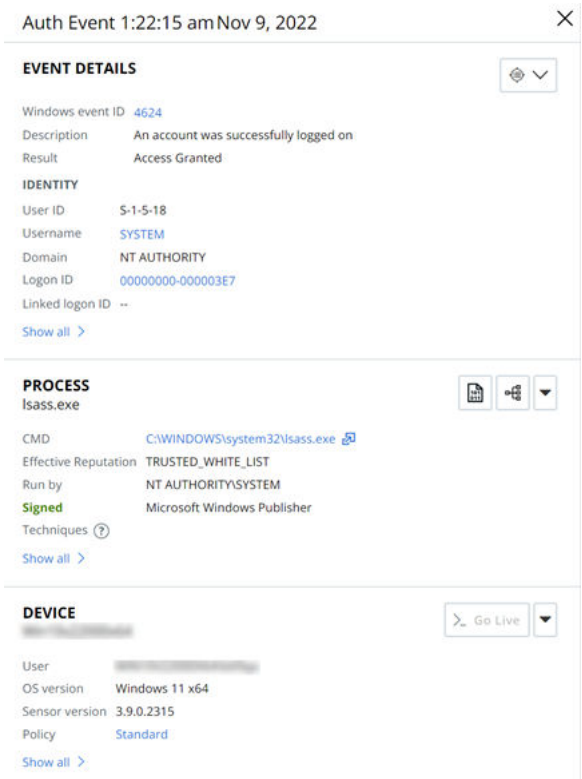
EVENTS	TIME	EVENT ID	DESCRIPTION	USERNAME	DEVICE
376	1:21:13 am Nov 9, 2022	4624	An account was successfully logged on	SYSTEM	
268	1:21:13 am Nov 9, 2022	4672	Special privileges assigned to new logon		
111	1:21:11 am Nov 9, 2022	4634	An account was logged off		
6	11:23:02 am Nov 8, 2022	4625	An account failed to log on		
2	11:23:02 am Nov 8, 2022	4740	A user account was locked out		
11	10:56:55 am Nov 8, 2022	--	--		

認証イベントの詳細

このトピックでは、認証イベントに使用できる拡張イベントの詳細について説明します。

左側のナビゲーション ペインで、[調査] をクリックし、[認証イベント] タブをクリックします。イベントを検索します。

任意のイベント行の右側にある › をクリックして、追加のイベント情報を表示します。



[グループ化] ドロップダウン メニューを使用して結果をグループ化し、認証イベント結果のグループの [>] をクリックすると、[イベントの詳細] パネルに [グループの詳細]、[前回のイベントの詳細]、[プロセス]、および [デバイス] セクションが表示されます。[グループの詳細] セクションには、以下の内容がまとめられています。

- [グループ化] の基準
- グループ内のイベント数
- グループ内の最初のイベントと最後のイベントの時間

- グループ内のイベント間で共通の追加情報

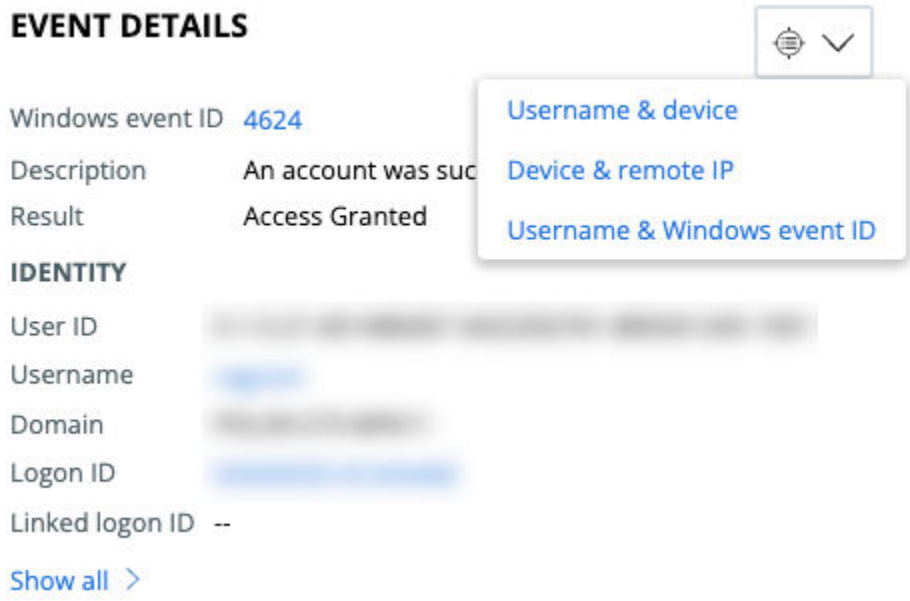
[前回のイベントの詳細] セクションには、グループ内の最新のイベントに関する情報が含まれます。

単一の認証イベント結果の [>] をクリックすると、[イベントの詳細] パネルに [イベントの詳細]、[プロセス]、および [デバイス] セクションが表示されます。

[認証イベント] 画面の [イベントの詳細] パネルには、複数属性の調査機能が導入されています。これにより、これらの属性に同じ値を持つ他の結果にピボットできます。ピボットに関しては以下のようなオプションがあります。

- ユーザー名とデバイス
- デバイスとリモート IP アドレス（リモート認証イベントで使用可能）
- ユーザー名と Windows イベント ID

この例では、 [調査] ドロップダウン メニューで [ユーザー名とデバイス] オプションを選択すると、`Username` と `Device` の値が同じ結果を検索できます。



単一属性のピボットがサポートされています。[イベントの詳細] パネルの一部の値がハイパーリンクされ、これらの値に基づいてピボットが有効になります。この例では、`4624` は `Windows event ID` フィールドにハイパーリンクされています。[4624] をクリックすると、[認証イベント] タブに `windows_event_id:4624` を持つすべての結果を検索できます。

スクリプトベースの攻撃の調査

スクリプトベースの攻撃は、通常、システムに入り込み、横方向に移動して損害を与えるのに使用されます。[Investigate (調査)] ページでは、スクリプトベースの攻撃に関する情報を見つけ、難読化された PowerShell スクリプトで悪意のあるコードを識別できます。

隠れた脅威を明らかにするために、Carbon Black Cloud コンソール内のツールは難読化された PowerShell スクリプトの内容をデコードできます。特定のイベントの右側のパネルで、デコードされたスクリプトを確認できます。構文の強調表示により、悪意のあるコンテンツを検索するときに、文字列コンテンツ、PowerShell コマンド、および関数呼び出しを簡単にスキャンできます。

難読化された PowerShell スクリプトの調査

Carbon Black Cloud コンソールは、難読化された PowerShell スクリプトの特定の詳細とデコードされたバージョンを公開できます。これは、これらのタイプの攻撃に対する可視性を強化するのに役立ちます。

この手順を使用すると、難読化された PowerShell スクリプトのデコードされた内容を表示できます。

手順

1 左側のナビゲーション ペインで、[調査] をクリックします。

2 製品の構成に応じて、次のいずれかを実行します。

製品	手順
Endpoint Standard	[調査] > [観測] ページで、実行可能ファイルが `powershell.exe` となっているプロセスを検索します。 検索機能は、直接入力して使用できます。 `process_name: powershell.exe` 検索の時間範囲を変更できます。結果をさらに絞り込むには、左側のペインのフィルタを使用します。 その他の検索フィールドについては、ページの右上に組み込まれた検索ガイドを参照してください。
Enterprise EDR	[プロセス] タブで、実行可能ファイルが `powershell.exe` であるプロセスを検索します。 検索機能は、直接入力して使用できます。 `process_name: powershell.exe` 検索の時間範囲を変更できます。結果をさらに絞り込むには、左側のペインのフィルタを使用します。 その他の検索フィールドについては、ページの右上に組み込まれた検索ガイドを参照してください。

3 調査するイベントまたはプロセスを選択します。行の最後でキャレット  をクリックします。[イベントの詳細] パネルの右側にイベントの詳細が表示されます。

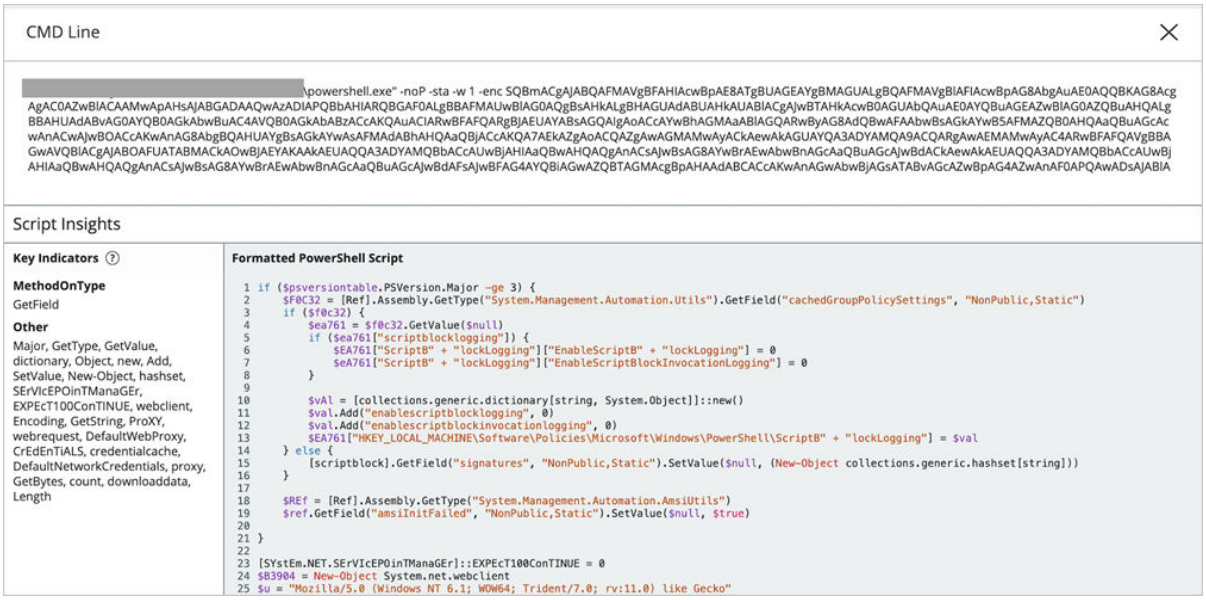
4 [イベントの詳細] パネルの [プロセス] セクションで、[CMD] 行を見つけ、展開アイコン  をクリックします。

結果

[Process CMD]の  をクリックすると、PowerShell 以外のプロセスと PowerShell プロセス間の出力の違いがわかります。

- PowerShell 以外のプロセスの場合、コマンド ライン引数は [CMD] の下に表示されます。

- 難読化された PowerShell プロセスの場合、[キー インジケータ] の下にデコードされたスクリプト コードは色付きテキストと強調表示されたキーワードが表示されます。



次のステップ

アラートのトリアージまたは脅威ハンティングに進み、目的が悪意のあるものかどうかを判断します。

プロセス ハッシュの取得

[調査] ページの [観測] タブでイベントのプロセス SHA-256 ハッシュを取得できます。

手順

1 左側のナビゲーション ペインで、[調査] をクリックし、[観測] タブをクリックします。

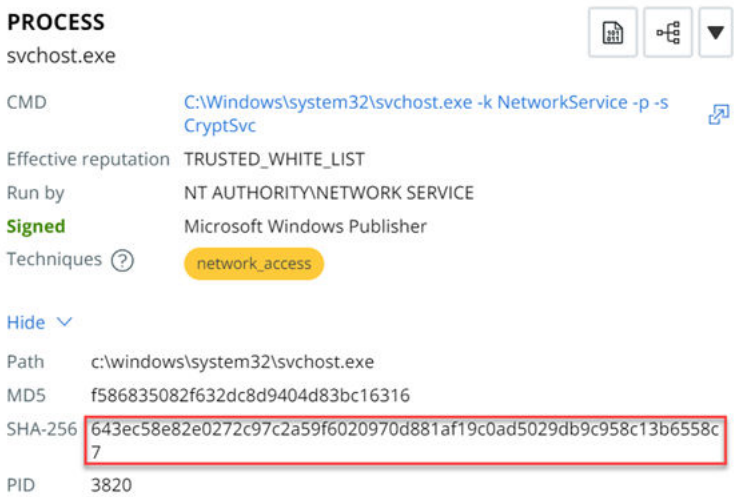
2 イベントの検索：左側のペインの [プロセス] フィルタを使用して、検索結果を絞り込むことができます。

3 検索結果テーブルの上にある [表示方法] ドロップダウン メニューで、 [プロセス] を選択します。

プロセス ハッシュは、検索結果テーブルの 2 番目の列に表示されます。

4 プロセス ハッシュをコピー（取得）する方法は 3 つあります。

- 切り詰められたプロセス ハッシュにカーソルを合わせます。完全なハッシュ値が表示されます。ハッシュ値を選択してから **Ctrl-C** を押してハッシュをコピーします。
- 切り詰められたプロセス ハッシュをクリックし、**Ctrl-C** を押してハッシュをコピーします。
- イベントの右側にあるキャレット  アイコンをクリックします。[イベントの詳細] ペインが開きます。[プロセス] セクションまで下にスクロールし、[すべて表示] をクリックします。ハッシュ値を選択し、**Ctrl-C** を押してハッシュをコピーします。



脅威レポートへの調査クエリの追加

既存または新規に作成されたウォッチリスト内の既存または新規に作成された脅威レポートにクエリを追加して、カスタム セキュリティ侵害インジケータ (IOC) を作成できます。

手順

1 左側のナビゲーション バーで、[調査] をクリックします。

2 検索テキスト ボックスからクエリを実行し結果を確認します。

3 このクエリをウォッチリストの IOC に含めるには、検索テキスト ボックスの下にある [脅威レポートに検索を追加] リンクをクリックします。

[クエリを追加] ウィンドウが表示されます。

4 次のいずれかを実行します。

- 既存のウォッチリストと脅威レポートを選択します。
  a [ウォッチリストを選択] セクションのドロップダウン メニューからウォッチリストを選択します。
  b [レポートへのクエリの追加] セクションのドロップダウン メニューから脅威レポートを選択します。
- 既存のウォッチリストを選択し、新しい脅威レポートを作成します。
  a [ウォッチリストを選択] セクションのドロップダウン メニューからウォッチリストを選択します。
  b [レポートにクエリを追加] セクションの [新規追加] をクリックします。
  c 新しい脅威レポートに分かりやすい名前を入力します。
  d オプションで、説明、ウォッチリスト ヒットをトリガする重要度のレベル、および新しい脅威レポートの関連タグを含めます。
- 新しいウォッチリストと脅威レポートを作成します。
  a [ウォッチリストを選択] セクションで [新規追加] をクリックします。
  b 新しいウォッチリストに分かりやすい名前を入力します。
  c オプションで、新しいウォッチリストの残りのフィールドに入力して、ウォッチリストの目的を指定します。

  [ヒット時のアラート]設定は、イベントがクエリと一致した場合に通知する方法（または通知するかどうか）を決定します。
  d [レポートにクエリを追加] セクションの [新規追加] をクリックします。
  e 新しい脅威レポートに分かりやすい名前を入力します。
  f オプションで、ウォッチリスト ヒットをトリガする重要度の説明とレベル、および新しい脅威レポートの関連タグを含めます。

5 変更を適用するには、[保存] をクリックします。

結果

画面の上部に「[IOC が正常に作成されました]」という通知が表示されます。

次のステップ

検索クエリを見つけ、それに対してアクションを実行します。

1 左側のナビゲーション バーで、[適用] - [ウォッチリスト] ページをクリックし、カスタム ウォッチリストを選択します。

2 [レポート] タブを選択し、カスタム脅威レポートの名前をクリックします。

IOC の下にリストされている、新しく追加されたクエリを表示し、そのクエリに対してアクションを実行できます。クエリを編集、無効化、削除、または調査できます。

アラート

9

アラートは、環境内の疑わしい動作と既知の脅威を示します。アラートを定期的に確認し、アクションを実行する必要があるか、またはポリシーの修正が必要であるかを判断することをお勧めします。

- 左側のナビゲーション ペインで、[アラート] をクリックします。
- アラートの詳細を展開して表示するには、表のアラート行を[ダブルクリック]します。

注： コンソール内のタイムスタンプはユーザーの現地のタイムゾーンで表示されます。タイムスタンプにカーソルを当て、UTC タイムゾーンに関連付けられた現地時間を表示します。

ヒント: アラート API を使用して、アラートの取得と管理を自動化することもできます。アラートの一括エクスポートも参照してください。

次のトピックを参照してください。

- アラートの詳細表示
- グループ アラート
- 脅威 ID でのアラートの表示
- アラート ワークフローの編集
- 検索の基本
- アラートのトリアージ
- スクリプト ホストの置き換えが発生

アラートの詳細表示

次の手順を使用して、アラートの詳細を表示します。

注： [アラート] 画面での XDR データの確認 も参照してください。

手順

1 左側のナビゲーション ペインで、[アラート] をクリックします。

注： Carbon Black 分析アラートに関するポリシーで対処されている場合は、表の [ステータス] 列に赤いシールド アイコン付きの [適用されるポリシー] が表示されます。

2 アラートの詳細を表示するには、次のいずれかの操作を行います。

- アラートをダブルクリックします。
- [アクション] 列の右側で [>] をクリックします。

展開された右側のペインが表示されます。[アラートの詳細] サマリ ペインには、アラートのタイプ、アラート ID、アラートの理由、ポリシーとルール名、ワークフローのステータスが表示されます。

3 [判定] の下の [すべて表示] をクリックして、[アノマリ分類] ペインを表示します。すべての組織および自分の組織のアラートの普及率を表示できます。普及率は、非常に一般的、平均、またはまれに分類されます。「アノマリ分類」を参照してください。

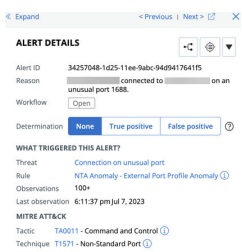
4 をクリックして[アラートの詳細] ペインを別のタブに表示し、さらにペインを開きます。

展開されたビューには、次のペインが表示されます。

- プロセス
- 子プロセス
- 関与するプロセス
- アセット
- 復旧
- アラート ID 履歴
- 脅威 ID 履歴

5 以下を行うことができます。

- [< 前] または [> 次] をクリックして、前または後続のアラートの詳細を表示します。
- アラートをさらにトリアージまたは調査するには、[アラートの詳細] セクションの右上隅にある各ボタンを使用します。
- アラートの原因を [このアラートをトリガした原因] セクションに表示します。観測の数が [100+] と表示される場合は、以下を実行できます。
  - [アラートのトリアージ] アイコン をクリックして、100 個の観測を表示します。
  - [調査] アイコン をクリックして、100 個を超える観測のすべてのデータを表示します。



6 右上隅にある [X] をクリックして、[アラートの詳細] ペインを閉じます。

アラートの種類

アラートは、[ウォッチリスト]、[USB デバイス制御]、[CB 分析]、[ホストベースのファイアウォール]、[コンテナ ランタイム]、または [侵入検知システム (IDS)] から発生します。[種類]フィルタを使用して各ソースからアラートを表示します。

[ウォッチリスト アラート]

ウォッチリストでは、潜在的な脅威と疑わしいアクティビティについて、環境を継続的に監視するカスタム検出が利用できます。

ウォッチリストからのアラートの受信はオプションであり、ウォッチリストをサブスクライブするか、カスタム ウォッチリストを作成するときに、[ウォッチリスト] 画面で設定できます。

[USB デバイス制御アラート]

エンド ユーザーがブロックされた USB デバイスにアクセスしようとすると、ポリシーの拒否アクションがトリガされアラートが発生します。USB デバイス制御アラートをトリアージしたり調査したりすることはできません。

[CB 分析アラート]

CB 分析アラートは、Carbon Black Cloud 分析エンジンで生成される検波です。

[ホストベースのファイアウォール アラート]

ホストベースのファイアウォール アラートは、定義されたファイアウォール ルールのいずれかに違反した場合にユーザーに通知します。ルールが [ポリシー] 画面で [ブロックとアラート] に設定されている場合、関連付けられたアラートが生成されます。

注： ホストベースのファイアウォール アラートには、最大 100 個の観測が含まれています。100 を超えると、Carbon Black Cloud は追加の重複観測を抑制します。

[コンテナ ランタイム アラート]

コンテナ ランタイム アラートは、コンテナ ランタイム ポリシーに従って悪意があると疑われる動作を示します。これらのアラートは、次のいずれかの結果です。

- ワークロードの動作のアノマリ、またはポート スキャンなどの既知の攻撃パターンに一致する動作の結果。
- レピュテーションが悪い IP アドレスへのアウトバウンド接続。

[侵入検知システム (IDS) アラート]

IDS は、ネットワーク アクティビティを既知のシグネチャに照らし合わせて監視し、潜在的な脅威と疑わしいアクティビティを監視します。

CB 分析アラートのキューを確認する場合、分析の優先順位決めと重点的な取り組みに役立つよう、フィルタ パネルの [脅威] ボックスのみ選択することをお勧めします。

注： IDS アラートには、最大 100 個の観測が含まれています。100 を超えると、Carbon Black Cloud は追加の重複観測を抑制します。

特定のアラート タイプの表示

この手順を使用して、特定のアラート タイプを表示します。

手順

1 左側のナビゲーション ペインで、[アラート] をクリックします。

2 [フィルタ] ペインの [タイプ] で、次のいずれかを選択して、そのタイプに固有のアラートを表示します。

- [CB 分析]
- [ウォッチリスト]
- [USB デバイス コントロール]
- [ホストベースのファイアウォール]
- [コンテナのランタイム]
- [侵入検知システム]

注： 1 度に複数のタイプを選択できます。

各アラートは、[フィルタ] ペインの右側のリストに表示されます。

3 アラートをダブルクリックするか、[アクション] 列の右の [>] をクリックして右のパネルを拡大表示します。

4 各アラートについて、右パネルの [アラートの詳細] セクションの右上隅にあるドロップダウン矢印を使用できます。

使用可能なオプションは、アラートのタイプによって異なります。「アラートでのアクション実行」を参照してください。

アラートおよびレポートの重要度

重要度スコアは、アラートの相対的重要性を示します。

[S] 列をクリックして、キューのアラートを重要度スコア別にソートし、すぐに注意が必要なアラートを特定します。

[CB 分析 - アラートの重要度]

アラートの重要度は、CB 分析アラートの相対的重要性を示します。

- [重要度 1 ～ 2：]ポート スキャン、マルウェアのドロップ、システム構成ファイルの変更、永続性などのアクティビティ。
- [重要度 3 ～ 5:] マルウェアの実行、汎用ウイルスのような動作、ユーザー入力の監視、潜在的なメモリ スクレイピング、パスワード盗難などのアクティビティ。
- [重要度 6 ～ 10:] リバース コマンド シェル、プロセス ハロウイング、破壊的なマルウェア、隠されたプロセスとツール セット、ネットワーク上で通信するがすべきではないアプリケーションなどのアクティビティ。

[ウォッチリスト - レポートの重要度]

レポートの重要度は、ウォッチリスト アラート内の脅威レポートの相対的重要性を示します。

レポートの重要度は、レポートの作成者によって決まります。独自のレポートを作成する場合、レポートの重要度を決定できます。1 は最も重要度が低く、10 は最も重要度が高くなります。

ターゲット バリュー

ターゲット バリューは、アラートの脅威レベルを計算する際の乗数として機能します。ターゲット バリューは、エンドポイントが属するポリシーにより定義されます。

ターゲット バリューは、アラート表の [T] 列の下にある塗りつぶされたバーの数で示されます。

- [低:] バー 1 本。脅威レベルは低くなる。
- [中:] バー 2 本。基本のターゲット バリュー。乗数は追加されない。
- [高/ミッション クリティカル:] バー 3 本または 4 本。どちらの値も、同じ状況下で脅威レベルを増加させる。説明が同じでアラートの重要度が異なる 2 つ以上のアラートが表示される場合がある。

アラート ID、イベント ID、および脅威 ID

3 つのタイプの ID があります。アプリケーションでそれぞれがどのように使用されるかを理解することが重要です。

[イベント ID]: 特定の時点に 1 台のデバイスで発生する 3 つまでの異なるハッシュ (親アプリ、選択したアプリ、ターゲット アプリ) を含む特定のアクション。イベント ID は [Investigate (調査)] ページのイベント詳細にあります。センサーからコンソールに送信されるすべてのイベントには、固有のイベント ID が割り当てられます。

[アラート ID]: 1 台のデバイスで同様の時間枠 (+/- 15 分) 内に発生する同様のイベント。イベント ID は、Carbon Black 分析によって 1 つのアラート ID にグループ化されます。各アラートには固有のアラート ID が割り当てられます。これは、後続のアラートのハッシュ、アクション、またはデバイスが同じ場合でも同様です。

[脅威 ID]: 複数のデバイスと時間枠にわたって結びつけられる同様のアラート。脅威 ID を使用して [Alerts (アラート)] ページで関連するアラート ID を検索できます。アプリケーションのハッシュが変更された場合は、新しい脅威 ID が割り当てられます。

アノマリ分類

[アノマリ分類] 機能は、関連する可能性が最も高いアラートを検出して自動的に識別します。この機能は、VMware Carbon Black XDR ユーザーおよび特定のウォッチリストで使用できます。

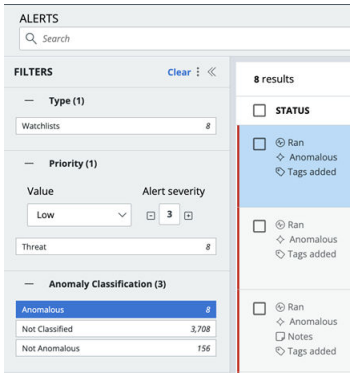
システムは、すべての組織および自分の組織内でアラートが何回確認されたかを調べることで、アラートの普及率を判断します。普及率のカテゴリには、非常に一般的、平均、またはまれがあります。アラートの普及率が全体的にまれな場合は、アノマリとしてマークされる可能性が高くなります。

この機能を使用すると、アノマリなアラートに焦点を当てて、潜在的な問題や脅威に迅速に対応できます。

[アノマリ分類フィルタ]

[アラート] 画面で、[アノマリ分類] フィルタを使用してアラートを 3 つのカテゴリにフィルタリングできます。

- [アノマリ] : アノマリであるアラートを表示します。
- [アノマリではない] : アノマリではないアラートを表示します。
- [分類されていない] : 分類されていないアラートを表示します。



アラートがアノマリの場合は、[ステータス] 列にアノマリ ステータスが表示されます。

アノマリ分類をオンにする

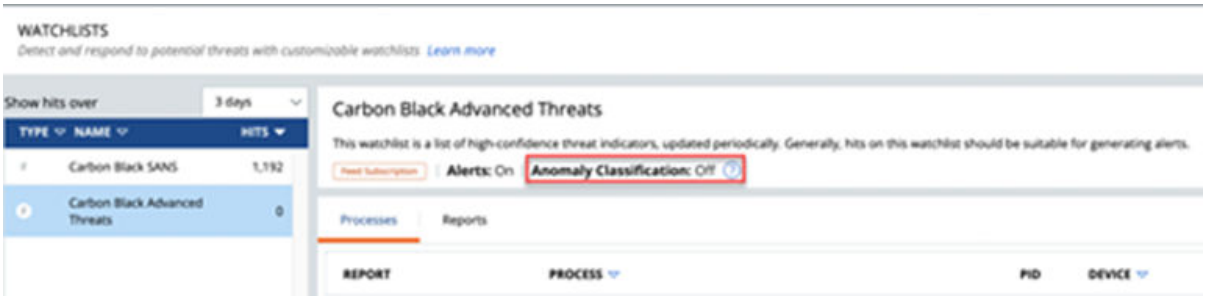
デフォルトで、[アノマリ分類] 機能は無効になっています。次の手順に従って、[Carbon Black Cloud Advanced Threats] ウォッチリストまたは [AntiMalware Scan Interface (AMSI) 脅威インテリジェンス] ウォッチリストの [アノマリ分類] 機能をオンにします。

手順

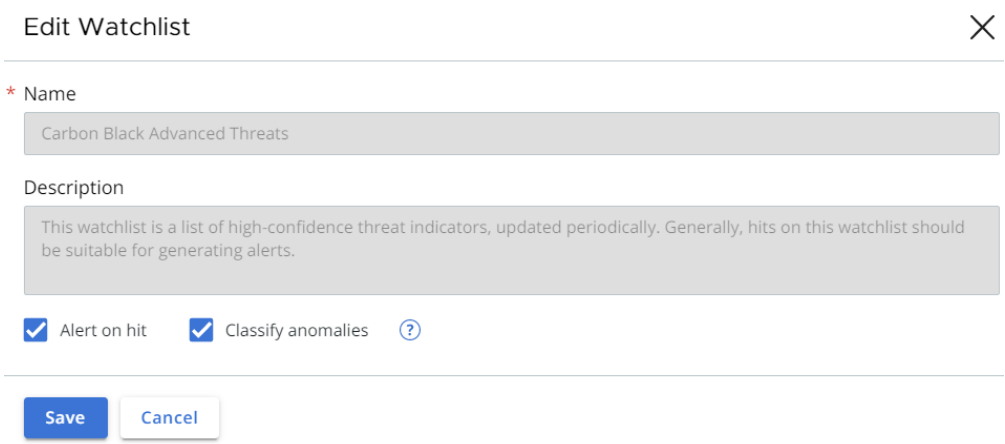
1 左側のナビゲーション ペインで、[適用] - [ウォッチリスト] の順にクリックします。

2 次のいずれかのウォッチリストをクリックします。

- Carbon Black Cloud Advanced Threats
- AMSI 脅威インテリジェンス



3 [アクション実行] をクリックし、ドロップダウン メニューから [編集] を選択します。



4 [ヒット時にアラート] チェック ボックスを選択します。

5 [アノマリの分類] チェック ボックスを選択します。

6 [保存] をクリックします。

グループ アラート

アラートをグループ化して、複数のエンドポイントにわたって発生する類似のアラートを 1 つの行に表示します。

注： デフォルトでは、アラートは自動的に [グループ化の基準：なし] に設定されます。

[グループ化の基準：なし] ビューでは、複数のデバイスでアラートが表示されている場合でも、すべてのアラートが単一のアラート行に個別に表示されます。

アラートの優先順位を特定し、個々のアラートに対していつアクションを実行する必要があるかを判断できます。

表の右上にある [グループ化の基準] ドロップダウン メニューを使用して、すべてのアラートを同じ脅威 ID でグループ化します。「グループ化の基準：脅威 ID」を参照してください。

[タイプ/理由] 列

[タイプ/理由] 列は、アラートの脅威 ID を決定し、アラートが作成された理由を説明します。

脅威 ID グループには以下が含まれます。

- ウォッチリスト
- CB 分析
- USB
- ホストベースのファイアウォール
- コンテナのランタイム
- IDS

ワークフロー列

[ワークフロー] 列は、アラートが開いているか閉じているかを示します。

[ワークフロー] 列でアラートのステータスをクリックして、次の情報を表示します。

- アラート ID
- ワークフローのステータスとタイムスタンプを更新したユーザー

注： ワークフロー列は、1 つのアラートに対してのみインタラクティブに表示されます。グループ化されたアラートのワークフロー ステータスをクリックすることはできません。

グループ化の基準：脅威 ID

脅威 ID でアラートをグループ化して、同じ脅威 ID を持つアラートの数を表示できます。

手順

1 [グループ化の基準：] のドロップダウン メニューをクリックします。

2 [脅威 ID] を選択します。

結果

[グループ化の基準：脅威 ID] アクションは、同じ脅威 ID を持つアラートを単一のアラート グループ行に配置します。

次のものを確認できます。

- 同じ脅威 ID を持つアラートの数
- アラートのグループの重要度のレベル
- アラートのタイプとアラートが作成された理由
- 特定の脅威 ID を持つアラートが作成された最初と最後の時刻
- 特定の脅威 ID のアラートがあるデバイスの数
- 同じ脅威 ID グループ内で、開かれたまたは閉じられたアラートの数

脅威 ID でのアラートの表示

この手順を使用して、脅威 ID グループ内のすべてのアラートを表示します。

手順

1 [グループ化の基準：脅威 ID] のドロップダウン メニューをクリックします。

2 表示するアラートを選択します。

3 [アクション] 列で [アラートを表示] をクリックします。

結果

新しいウィンドウに脅威 ID グループ内のアラートの詳細が表示されます。

脅威 ID の詳細の表示

この手順を使用して、[脅威 ID] ペインの詳細を表示します。

 をクリックすると、[アラートの詳細] ペインが別のタブに表示されます。

注： [< 前] または [> 次] をクリックして、前または後続のアラートの詳細を表示します。

[脅威 ID の詳細] ペインには、以下が表示されます。

- [脅威 ID のサマリ] ペイン
- [プロセス] ペイン
- [脅威 ID 履歴] ペイン

[脅威 ID のサマリ] ペイン

[脅威 ID のサマリ] ペインには、次のアラート グループに関する詳細が表示されます。

- タイプ
- 脅威 ID
- アラートの理由
- アラートが表示されたデバイスの数と頻度
- ワークフロー

[すべて表示] をクリックして脅威 ID のサマリから [アノマリ分類] ペインを表示します。すべての組織および自分の組織のアラートの普及率を表示できます。普及率は、非常に一般的、平均、またはまれに分類されます。「アノマリ分類」を参照してください。

[プロセス] ペイン

[プロセス] ペインには、脅威 ID アラートに関する次の情報が表示されます。

- 有効なレピュテーション
- 削除済み
- 署名
- 技術

[脅威 ID 履歴] ペイン

[脅威 ID 履歴] ペインに次の情報が表示されます。

- 脅威 ID
- アラートの理由

- アラートが表示されたデバイスの数とアラートの頻度

このペインには、脅威 ID アラートに追加されたユーザーのアクティビティとメモが表示されます。

[すべて表示] をクリックして、すべてのユーザー アクティビティ履歴を表示します。

メモの追加

[アラート ID 履歴] ペインと [脅威 ID 履歴] ペインにメモを追加できます。メモを削除することもできますが、別のユーザーが追加したメモは削除できません。

[すべて表示] オプションを使用すると、展開されたポップアップ ビューで [アラート ID 履歴] または [脅威 ID 履歴] ペインが開き、アラートに追加されたすべてのメモとアラートのワークフロー変更履歴が表示されます。

アラート ワークフローの編集

[ワークフロー] 列に、アラートのステータスが表示されます。

アラートのワークフローを [開く]、[閉じる]、または [進行中] に変更できます。

アラートを閉じたり開いたりする際に、今後はすべてのデバイスでアラートを自動的に開閉できます。

重要： [この脅威 ID を持つ今後のすべてのアラートを自動的に閉じる] オプションは、アラート API を使用して使用可能な脅威 ID に基づいています。脅威 ID の定義は、CB 分析、ウォッチリスト、USB デバイス制御、ホストベースのファイアウォール、コンテナのランタイム、侵入検知システムのアラート タイプによって若干異なります。

- [CB 分析]: 主要な攻撃者（通常は攻撃者の SHA-256 ハッシュ）と、Endpoint Standard 分析エンジンによって生成されるアラートの理由の組み合わせ。
- [ウォッチリスト]: ウォッチリストのヒットをトリガしたレポート。
- [USB デバイス制御]: 一意の USB デバイスを表します。
- [ホストベースのファイアウォール]: ホストベースのファイアウォール ルールと方向が同じアラート。
- [コンテナのランタイム]: 同じポリシーとルールを持つ、同じクラスタと名前空間内のアラート。
- [IDS]: 同じプロセスと IDS シグネチャまたはルールを持つアラート。

アラートに解除のフラグが付いている場合、同じ脅威 ID を含む今後のすべてのアラートが解除されます。

注： アラートは、異なる SHA-256 ハッシュを示す場合があります。複数のデバイス上のアラートを閉じるまたは開くには、オブジェクトのハッシュが同一である必要があります。

アラートを閉じる

この手順を使用して、アラートを閉じ、関連するすべてのアラートを閉じます。

手順

1 左側のナビゲーション ペインで、[アラート] をクリックします。

2 [グループ化の基準：なし] を選択します。

3 閉じるアラートをクリックします。

4 [アクション] 列で、ドロップダウン メニューをクリックします。

5 [閉じる] をクリックします。

[アラートを閉じる] ウィンドウが表示されます。

6 [閉じる理由] ドロップダウン メニューをクリックして、アラートを閉じる理由を選択します。

- 解決済み
- 理由なし
- 解決済み - 無害/既知
- 複製/クリーンアップ
- その他

7 [関連アラートの管理] セクションで、以下を実行するかどうかを選択します。

- 同じ脅威 ID を持つすべての既存アラートを閉じる
- 同じ脅威 ID を持つ今後のすべてのアラートを自動的に閉じる

注： [アラートを表示] をクリックして同じ脅威 ID を持つすべてのアラートを表示します。

8 アラートを閉じる理由、および今後のすべてのアラート（該当する場合）を概説するメモを他のユーザーに追加します。

9 [アラートを閉じる] をクリックします。

結果

アラートのワークフロー ステータスが [閉じる] に変わります。変更は、[アラート ID 履歴] ペインに記録されます。[アラート ID 履歴] ペインを使用して、アラートのワークフロー ステータスに対する以前の変更をすべて表示します。

アラートを開く

この手順を使用してアラートを開き、関連するすべてのアラートを開きます。

手順

1 左側のナビゲーション ペインで、[アラート] をクリックします。

2 [グループ化の基準：なし] を選択します。

3 閉じるアラートをクリックします。

4 [アクション] 列で、ドロップダウン メニューをクリックします。

5 [開く] をクリックします。

[アラートを開く] ウィンドウが表示されます。

6 [関連アラートの管理] セクションで、以下を実行するかどうかを選択します。

- 同じ脅威 ID を持つすべての既存アラートを開く

- 同じ脅威 ID を持つ今後のすべてのアラートを自動的に開く

注： [アラートを表示] をクリックして同じ脅威 ID を持つすべてのアラートを表示します。

7 アラートを開く理由、および今後のすべてのアラート(該当する場合)を概説するメモを他のユーザーに追加します。

8 [アラートを開く] をクリックします。

結果

アラートのワークフロー ステータスが [開く] に変わります。変更は、[アラート ID 履歴] ペインに記録されます。[アラート ID 履歴] ペインを使用して、アラートのワークフロー ステータスに対する以前の変更をすべて表示します。

アラートを進行中としてマーク

この手順を使用して、アラートを [進行中] としてマークします。

手順

1 左側のナビゲーション ペインで、[アラート] をクリックします。

2 [グループ化の基準：なし] を選択します。

3 アラートをクリックして閉じます。

4 [アクション] 列で、ドロップダウン メニューをクリックします。

5 [進行中としてマーク] をクリックします。

[アラートを進行中としてマーク] 画面が表示され、関連するすべてのアラートを管理できます。

6 同じ脅威 ID を持つすべてのアラートを [進行中] としてマークするかどうかを選択します。

注： [アラートを表示] をクリックして同じ脅威 ID を持つすべてのアラートを表示します。

7 [OK] をクリックします。

結果

アラートのワークフロー ステータスが [進行中] に変わります。変更は、[アラート ID 履歴] ペインに記録されます。[アラート ID 履歴] ペインを使用して、アラートのワークフロー ステータスに対する以前の変更をすべて表示します。

検索の基本

検索フィールドを使用する場合は、次の方法を使用できます。

[値検索]

検索する場合は完全な値 (例：powershell) または末尾のワイルドカード (例：power*) を使用してください。

[検索フィールド]

検索フィールドを含める場合、このようなクエリを作成してください: フィールド:用語

例：

```
parent_name:powershell.exe
```

[ワイルドカード]

ワイルドカードを使用してクエリを拡張します。* [?] 1 つの文字に一致します。たとえば、`te?t` と入力すると、「test」と「text」の結果が返されます * * 0 個以上の連続した文字に一致します。例：`tes*` は「test」、「testing」、「tester」の結果を返します

ファイル拡張子検索において先頭のワイルドカードが考えられます。

例：`process_name:.exe`

値を引用せずバックスラッシュを使用して次の特殊文字をエスケープした場合、ワイルドカードをパスで使用することができます：`+ - && || ! ( ) { } [ ] ^ " ~ * ? : /`

例：(1+1):2 を検索するには、次のように入力します：`\(1\+1\)\:2`

[演算子]

演算子を使用してクエリを絞り込みます。演算子は大文字である必要があります。

- [AND] 両方の語句が存在する場合に結果を返します
- [OR] いずれかの語句が存在する場合に結果を返します
- [NOT] 語句が存在しない場合に結果を返します

[エスケープ]

サジェスト機能およびフィルタを使用する場合を除き、スラッシュ、コロン、およびスペースは手動でエスケープする必要があります。

[日付/時間範囲]

適切な場合、日付/時間範囲を使用してクエリを絞り込みます。

例：`device_timestamp: [2018-10-25T14:00:00Z TO 2018-10-26T15:00:00Z]`

[個数検索]

範囲とワイルドカードのある個数を含んだクエリを絞り込みます。

- [3 TO *] 3 の値で始まる個数の結果を返します。
- [* TO 10] 最大 10 までの個数の結果を返します。

[アラート] 画面で確認されたアラート データが使用できなくなり、[観測] として分類されるようになりました

確認されたアラート データは、CB 分析でフィルタリングして [観測] 画面で検索できます。

1　左側のナビゲーション ペインで、[調査] - [観測] をクリックします。

2　[フィルタ] で [タイプ] - [CB 分析] を選択します。

[観測] 画面で、確認された古いアラートがアラートとしてマークされません。

注： 複雑なクエリの作成については、『VMware Carbon Black Cloud ユーザー ガイド』の「高度な検索方法」を参照してください。

アラートのトリアージ

アラートのトリアージ中に、アラートを調査し、アラートに対処するアクションを実行できます。

重要： [アラートのトリアージ] 画面に「データがありません」と表示された場合でも、システムはバックグラウンドでデータを収集している可能性があります。しばらくお待ちください。新しいアラートの数によっては、画面の入力に数分かかる場合があります。しばらく待ってから画面を更新すると、問題が解決する場合があります。(これは既知の問題であり、今後解決されます。)

- [調査] をクリックし、[調査] 画面のアラートをトリガした観測を表示および分析します。
- オレンジ色の [アクション実行] ボタンをクリックして、次の操作を行います。
  - 承認リストに追加
  - 禁止リストに追加
  - アップロードをリクエスト
  - VirusTotal で検索
  - アプリケーションを削除
- アラートをトリガした観測を [アラートの詳細] ペインに表示します。

  注： ホストベースのファイアウォールおよび IDS アラートには、最大 100 個の観測が含まれています。100 を超えると、Carbon Black Cloud は追加の重複観測を抑制します。

アラートの調査

このセクションでは、アラートを調査するためのベスト プラクティスについて説明します。

次の項目を確認します。

- 優先度スコア
- 親パスと名前
- 関連する TTP
- ファイルのレピュテーション
- ネットワーク接続
- イベントの詳細
- コマンド ライン (ある場合)

次の質問をします。

- 別のプログラムや機能が正常に呼び出されましたか?
- ファイルのパスは疑わしいですか?
- プロセスは「正常」パスで実行されていますか?
- どの攻撃段階に入っていましたか?
- レジストリは変更されましたか?
- ファイルのレピュテーションが心配でしたか?

必要に応じて、他のステップを実行します。

- 認識されない Google アプリケーションやファイルがある
- チームメイトに見落としたものについての確認を求める
- 参照される MITRE 技術またはウォッチリストのヒットを確認する
- 「カスタム時間」を使用してイベントを発生の 15 分前に確認し、より多くの洞察を得る
- 確認されたアクティビティのより多くのコンテキストを確認

アラートでのアクション実行

[アクション実行] ボタンから使用できる機能に加えて、CB 分析アラートに対して実行できるいくつかのアクションがあります。

アラートによりトリガされたデバイスの隔離

[デバイスを隔離] をクリックし、[隔離をリクエスト] をクリックします。

デバイスを隔離することで、疑わしいアクティビティやマルウェアがネットワークの残りの部分に影響するのを阻止します。デバイスは、隔離状態から削除されるまで隔離されたままになります。デバイスを隔離するには数分かかる場合があります。

隔離からデバイスを削除するには、[デバイスを隔離解除] をクリックします。

メモの追加

メモを追加することで、コンソール ユーザー間のコミュニケーション手段となるだけでなく、アラートの検索やフィルタリングが簡単にできます。「メモの追加」を参照してください。

開くまたは閉じる

アラートのワークフローを編集して、アラートを開いたり閉じたりします。「アラート ワークフローの編集」を参照してください。

Live Response の使用

[ライブの開始] をクリックして Live Response セッションを開始します。Live Response を使用して、リモート調査を実行し、進行中の攻撃を阻止し、脅威を修正します。Live Response の機能を使用するには、Carbon Black Cloud で Live Response の権限を持つロールをユーザーに割り当てる必要があります。「Live Response の使用」と「ユーザー ロール」を参照してください。

Live Response は、バージョン 3.0 以降のセンサーを実行し、Live Response が有効にされたポリシーが割り当てられたエンドポイントで使用できます。Live Response は、バイパス モードまたは隔離のデバイスで使用できます。

アラートに対する判定の追加

アラートが真陽性か誤検出かを判断できます。

[アラートの詳細] ペインを使用して、アラートに対して [真陽性] または [誤検出] アラートの判定を下します。

アナリストはフィードバックを提供することで、モデルのトレーニングに貢献し、時間の経過とともに分類システムの精度を高めることができます。ユーザーからのフィードバックを分析することで、システムは分類アルゴリズムを改善し、将来的に脅威を特定するためのトレーニングが強化されます。

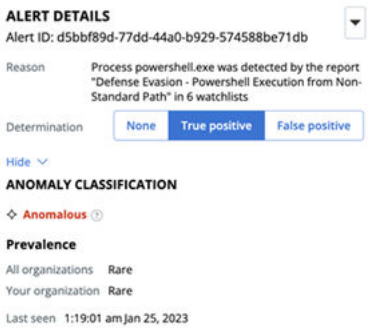
注： デフォルトでは、判定は [なし] に設定されています。

手順

1 左側のナビゲーション ペインで、[アラート] をクリックします。

2 アラートの詳細を表示するには、次のいずれかの操作を行います。

- アラートをダブルクリックします。
- [アクション] 列の右側で [>] をクリックします。



3 [真陽性] または [誤検出] をクリックして、アラートのアラート判定フィードバックを提供します。

注： このフィードバックは、モデルの予測出力ではなく、特定のアラート自体の評価に関連します。アラート分類システムはアラートの同じ入力ストリームに関する推論を行うため、フィードバックの提供はアラート分類システムのトレーニングに役立ちます。

正誤検出

このセクションでは、アラートの正誤検出について説明します。

正検出

正検出は、悪意があるとして正しくラベル付けされたアラートです。以下が含まれます。

- マルウェアやその他の脅威を含む可能性のあるファイルレス スクリプト攻撃または悪意のあるイベント
- KNOWN_MALWARE、SUSPECT_MALWARE、または PUP のレピュテーションを持つファイル、または NOT_LISTED (例：ゼロデイ(「0-day」)) のファイル
- 観察対象の動作または TTP は、環境の「正常な状態」に基づいて疑わしい場合があります
- [検出]：悪意のあるアクティビティが検出される場合がありますが、防止することはできません。通常、これはポリシーを強化する必要があることを意味します。
- [防止]：ブロックが行われる場合がありますが、おそらく攻撃のさまざまな段階が原因で、攻撃の一部のみが停止されている可能性があります。より強力なポリシーが必要な可能性があります。

誤検出

誤検出とは、KNOWN_MALWARE、SUSPECT_MALWARE、PUP など、脅威レピュテーションの 1 つとして、悪意のある、またはフラグ付きと誤ってラベル付けされたアラートです。

誤検出は、次の場合にトリガされます。

- 疑わしい動作または疑わしい TTP が確認されたため一般的なアプリケーションが誤ってフラグ付けされた
- カナリア ファイルに触れるソフトウェアがランサムウェア アラートをトリガする
- 不明な社内プログラムが疑わしいと見なされる
- 除外されていない可能性のあるプログラムが競合 (相互運用性や望ましくないブロックなど) を引き起こす

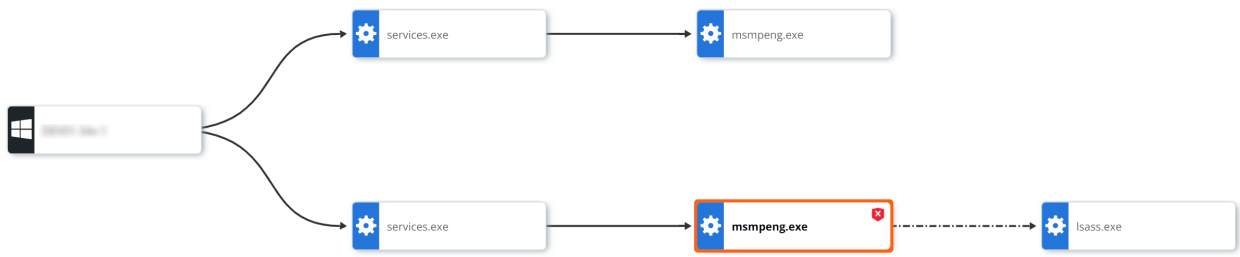
アラートの可視化

アラートの可視化またはプロセス ツリーにアクセスできます。

注： Carbon Black Cloud XDR がある場合は、[アラートのトリアージ] 画面での XDR データの確認 も参照してください。

[アラート] 画面で、目的のアイテムの横にある [アラートのトリアージ] アイコンをクリックします。[アラートのトリアージ] 画面が開きます。

攻撃ストリーム内の各イベント（プロセス、ファイル、またはネットワーク接続）は、プロセス ツリーにノードとして表示されます。攻撃の発生元が左側に表示され、その後の各イベントは攻撃の進行に応じて左から右に表示されます。



ノード タイプ

- [オペレーティング システム/ルート ノード]: プロセス ツリーの左端のルート ノードは、元のアクティビティが発生したホスト デバイスを表します。ルート ノード のアイコンは、デバイスで実行されていたオペレーティング システムを表します。
- [歯車/プロセス]: 実行済みまたは実行中のプロセス。
- [ドキュメント/ファイル:] ディスク上に作成されたファイル。
- [ネットワーク接続/IP アドレス:] IP アドレスはネットワーク接続アイコンとして表示されます。

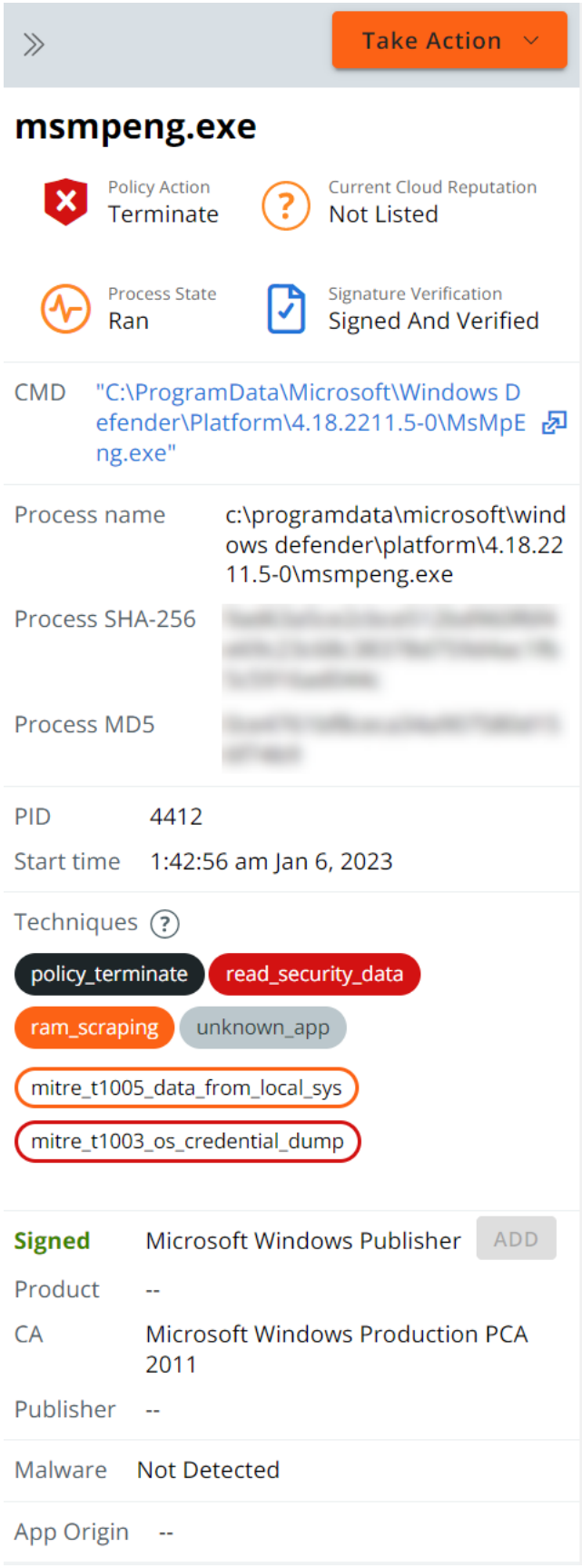
注： 操作が拒否された場合、感嘆符 ([!]) が拒否されたプロセスの横に表示されます。プロセスが終了すると、終了したプロセスの隣に [X] が表示されます。

ライン タイプ

- [呼び出し:] ソリッド ラインは、あるプロセスが他のプロセス、ファイル、またはネットワーク接続を呼び出したことを表します。
- [挿入:] ダッシュ ラインは、あるプロセスが他のプロセスにコードを挿入したことを表します。
- [メモリ読み取り:] ダッシュとドットのラインは、あるプロセスが他のプロセスの仮想メモリを読み取ろうとしたことを (ただし、プロセスには挿入しなかったことを) 表します。
- [ターゲットへのアクセス:] ドット ラインは、あるプロセスが他のプロセスを入力しようとしたことを (ただし、プロセスには挿入しなかったことを) 表します。

選択したノード パネル

ノードをクリックして追加情報を表示し、[選択されているノード] の折りたたみパネルでアクションを実行します。


Take Action
msmpeng.exe
Policy Action
Terminate
Current Cloud Reputation
Not Listed
Process State
Ran
Signature Verification
Signed And Verified
CMD
"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2211.5-0\MsMpEng.exe"
Process name
c:\programdata\microsoft\windows defender\platform\4.18.2211.5-0\msmpeng.exe
Process SHA-256
Process MD5
PID
4412
Start time
1:42:56 am Jan 6, 2023
Techniques
policy_terminate
read_security_data
ram_scraping
unknown_app
mitre_t1005_data_from_local_sys
mitre_t1003_os_credential_dump
Signed
Microsoft Windows Publisher
ADD
Product
--
CA
Microsoft Windows Production PCA 2011
Publisher
--
Malware
Not Detected
App Origin
--

アラートの発生元、動作、および TTP

[アラートのトリアージ] アイコンをクリックして、アラートの発生元および動作の詳細にアクセスできます。

[アラートの発生元:] どのようにして主プロセスがディスクに書き込まれたのかについての情報を含む、アラートの主プロセスがどのようにしてホストに導入されたのかについて記載します。

[重要度に基づくアラートの動作:] 重要度に基づくアラートの動作を説明し、インタラクティブな TTP グラフを表示します。グラフのセグメントは、アラート動作のカテゴリを示しています。カテゴリ ラベルまたはグラフ セグメントをクリックし、重要度別に色分けされたカテゴリの関連 TTP を確認することができます。

[TTP 色の重要度の凡例]

- [濃い赤:] 重大
- [明るい赤:] 高
- [オレンジ色:] 中
- [黄色:] 低
- [灰色:] なし

ヒント: 詳細については、『ユーザー ガイド』のメイン セクションの「TTP および MITRE 技術」および「TTP リファレンス」を参照してください。

アラート動作のカテゴリ

- [プロセス操作:] デバイス上で実行中の別のプロセスのメモリを変更および読み取る意図を持った動作。
  - [例:] 別のプロセスのメモリにコードを挿入します。
- [一般的な嫌疑:] 「良好」と認識されるアプリケーションによって共通に示される複数のマルウェア ファミリに一般的な動作。
  - [例:] デバイスの再起動以外に持続することを試み、システム上の実行プロセスを列挙します。
- [危険な状態のデータ:] エンドポイントのデータの機密性、利用可能性、または完全性を損なう意図を持った動作。
  - [例:] ユーザーの認証情報にアクセスするランサムウェア型の動作または試み。
- [新たな脅威:] マルウェア以外の攻撃に関連する動作。
  - [例:] PowerShell のようなネイティブ コマンド ライン ユーティリティの悪用およびバッファ オーバーフローなどの関連アクティビティのセキュリティ上の弱点を突く手段。
- [マルウェアおよびアプリケーションの悪用:] 一般的に「低い」レピュテーションと認識されるファイルに関連付けられた TTP、またはアプリケーションが低いレピュテーションで認識されているファイルを実行。

  注: このカテゴリはシステム アプリケーションのモニタリングについても示しています。ただし、悪意のないアクションである可能性が高いため、これらの TTP には、通常よりも低い優先度が設定されます。
- [ネットワークの脅威:] このネットワーク上で通信している、または受信接続を待機しているプロセスに関わるすべての TTP が含まれます。

スクリプト ホストの置き換えが発生

Carbon Black Cloud では、有効にするサービスに応じて、スクリプト ホストの置き換えが発生する可能性があります。

Carbon Black Cloud コンソール UI のさまざまなページで、同じプロセスの別の名前を表示できます。スクリプトを呼び出すプロセスの名前は、そのプロセスによって呼び出されるスクリプトの名前（ファイル）に置き換えられます。

たとえば、Carbon Black Cloud コンソールのイベントにはプロセス名として `PowerShell.exe` が表示され、別のイベントには `myscript.ps1` スクリプト名がプロセスとして表示されます。

呼び出しプロセスの名前が呼び出されるスクリプトの名前に変更されることを、スクリプト ホストの置き換えと呼びます。

Enterprise EDR サービスを有効にして [プロセス分析] 画面に移動すると、呼び出しプロセスの名前が `PowerShell.exe` として表示されます。センサーは名前の置き換えを実行せず、プロセス名はどこでも同じように表示されます。

Endpoint Standard サービスを有効にし、[アラートのトリアージ] 画面に移動すると、スクリプト ホストの置き換えにより、呼び出しプロセスの名前が `myscript.ps1` として表示されます。ここでセンサーは、PowerShell が `.ps1` ファイルを実行するときにスクリプト名をプロセス名として表示し、セキュリティ アナリストがイベントを調査しなくても簡単に動作を確認できるようにします。これは、V6 アラート API にも当てはまります。

Enterprise EDR 機能と Endpoint Standard 機能の両方が有効になっている場合、スクリプト ホストの置き換えが発生します。

ウォッチリスト IOC/検索に次のいずれかの検索語句を追加して、名前の置き換えの可視性を制御できます。

- `enhanced:true` - スクリプト（ファイル）名をプロセス名として記載するイベントのみを返します。
- `enhanced:false` - プロセス名をそのまま記載するイベントのみを返します。