Carbon Black.

Cb Defense ユーザー ガイド

Cb Predictive Security Cloud

2018 年 10 月 25 日

著作権表示

- Python Seasurf - Copyright (c) 2011 by Max Countryman. Python simplejson - Copyright (c) 2006 Bob Ippolito
- Python sqlalchemy - Copyright (c) 2005–2014 Michael Bayer and contributors. SQLAlchemy は Michael Bayer の商標です。
- Python sqlalchemy-migrate - Copyright (c) 2009 Evan Rosson, Jan Dittberner, Domen Kozar Python tempita - Copyright (c) 2008 Ian Bicking and Contributors
- Python urllib3 - Copyright (c) 2012 Andy McCurdy
- Python werkzeug - Copyright (c) 2013 by the Werkzeug Team （詳細については 「作者」を参照）QUnitJS - Copyright (c) 2013 jQuery Foundation, http://jquery.org/
- RabbitMQ - Copyright (c) 2007–2013 GoPivotal, Inc. All Rights Reserved. redis - Copyright (c) by Salvatore Sanfilippo and Pieter Noordhuis
- Rekall - Copyright (c) 2007-2011 Volatile Systems, Copyright (c) 2013-2016 Google Inc. All Rights Reserved.
- Simple Logging Facade for Java - Copyright (c) 2004–2013 QOS.ch Six - Copyright (c) 2010–2015 Benjamin Peterson
- Six - yum distribution - Copyright (c) 2010–2015 Benjamin Peterson
- Spymemcached / Java Memcached - Copyright (c) 2006–2009 Dustin Sallings and Copyright (c) 2009–2011 Couchbase, Inc.
- Supervisord - Supervisor is Copyright (c) 2006–2015 Agendaless Consulting and Contributors. Underscore - (c) 2009–2012 Jeremy Ashkenas, DocumentCloud Inc.
- Zlib - Copyright (c) 1995–2013 Jean-loup Gailly and Mark Adler

以下に定める条件に従い、上記のサードパーティ ソフトウェアおよび関連文書ファイル（まとめて以下「ソフトウェア」）の複製を取得するすべての個人に対し、ソフトウェアを無制限に扱うことを無償で許可します。これには、ソフトウェアの複製を使用、複写、変更、結合、掲載、頒布、サブライセンス、および / または販売する権利、およびソフトウェアを提供する相手に同じことを許可する権利も無制限に含まれます。

上記の著作権表示および本許諾表示を、ソフトウェアのすべての複製または重要な部分に記載するものとします。

上記のソフトウェアは、著作権保持者および貢献者によって「現状のまま」提供されており、明示黙示を問わず、商品性および特定の目的への適合性に関する暗黙の保証を含め、またこれに限定されず、いかなる保証もありません。著作権所有者または貢献者は、かかる損害の可能性を通知されていた場合であっても、本ソフトウェアの使用により生じる契約上、無過失責任上、または不法行為上 （過失またはその他を含む）であるかどうかにかかわらず、責任の理論により発生する直接的、間接的、特別、懲罰的、または派生的に生じるいかなる損害 （代替の商品またはサービスの調達、使用機会、データ、または利益の損失、または事業の中断が含まれるがこれに限定されない）の一切の責任を負いません。

Carbon Black, Inc.
1100 Winter Street, Waltham, MA 02451 USA
電話 : 617.393.7400 FAX: 617.393.7499
E メール : support@carbonblack.com
Web: http://www.carbonblack.com

内容

タスク リスト

タスクの実行手順 ..

第 1 章

作業の開始

この章では、Cb Defense およびこのユーザー ガイドについて説明します。また Carbon Black テクニカル サポートへの連絡方法について説明し、Cb Defense のホーム ページとして機能するダッシュボードを紹介します。

概要

Cb Defense は、マルウェアをはじめとするさまざまな攻撃を防止するクラウドベースのセキュリティ ソリューションです。軽量な 1 つのセンサーの検出および対応機能によって実現されるストリーミング防御テクノロジを提供します。

Cb Defense はエンドポイントを保護し、エンドポイントに対する可視化を提供することにより、チームがセキュリティ ギャップを解消できるようにします。Cb Defense の技術によりエンドポイント情報を収集し、データ サイエンスを活用して攻撃者の動作を分析し、それに対応します。

Cb Defense はエンドポイントに展開された軽量センサーと、高度な行動分析、インシデント対応用の検索、構成、およびレポート機能が搭載されたバックエンドの分析エンジンで構成されます。

Cb Defense のデータ保持期間

過去 30 日間のすべてのイベントをインターラクティブな検索および分析に利用できます。アラートに関連付けられているすべてのイベントは、さらに長期間保持されます。

アラートに関連付けられていないイベントは、30 日後に削除されます。アラートは 30 日より前のものであっても表示できます。また、これらのアラートに関連付けられたイベントも表示できます。

たとえば、検索期間を 3 か月としてイベントを検索したとします。この場合、過去 30 日間のすべてのイベントと、アラートに関連付けられた過去 3 か月間のイベントが検索されます。

本ガイドの内容

Cb Defense ユーザー ガイドは、Cb Defense センサーのエンドポイントでの管理、Cb Defense 管理コンソールを使用したアラートの監視およびアラートへの対応についてのガイドです。

本バージョンの Cb Defense ユーザー ガイドの更新内容を次の表に示します。

表 1: 更新内容

場所	変更内容
第 3 章 「ユーザーの管理」	• 表示ユーザーに並べ替え機能と検索機能を追加しました。
第 6 章 「アラートの視覚的表示」	• [Alert Triage （アラートのトリアージ）] ページの変更に合わせて、画面キャプチャと説明を更新しました。
第 11 章 「通知およびコネクター」	• [Connectors （コネクター）] ページの変更を反映して内容を更新しました。
付録 C、「バックグラウンド スキャンの仕様」	• 高速スキャン オプションを追加して、スキャンの情報を更新しました。

Carbon Black テクニカル サポート

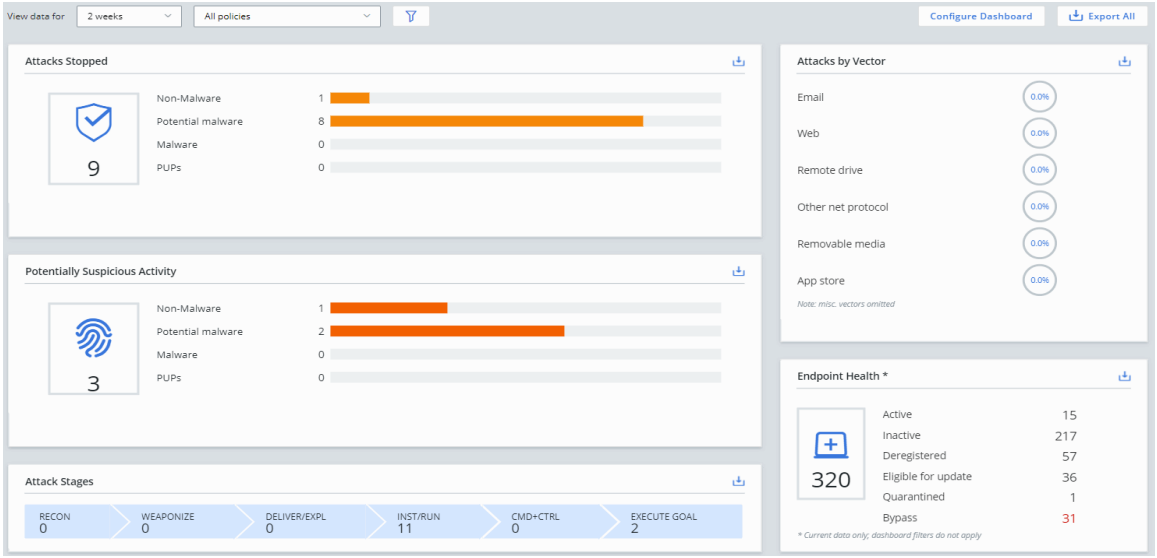
その他の Carbon Black テクニカル ガイドおよびナレッジ ベースの記事については、Carbon Black User eXchange を参照してください。

Carbon Black User eXchange で回答が見つからない場合は、次の方法で Carbon Black テクニカル サポートまでお問い合わせください。

- PSC にログインし、[Help （ヘルプ）] をクリックし、[Support （サポート）] をクリックします。
- Web: http://www.carbonblack.com
- E メール : support@carbonblack.com
- 電話 : 617.393.7400
- FAX: 617.393.7499

ダッシュボード

PSC にログインすると、**ダッシュボード**がホーム ページとして表示されます。



ダッシュボードには、システムで実行中の処理のスナップショットが表示され、関心のある項目にすばやく移動することができます。また、Cb Defense が保護するエンドポイントで何が起きているかも表示されます。

ダッシュボードの上部にあるオプションを使用すると、アラートの検索時間を設定したり、アラートを表示するポリシーを指定したりできます。デフォルトでは、[All Policies（すべてのポリシー）] が選択されています。

注意

各パネルでは、表示されるデータに期間とオプションのフィルターが適用されます。ただし、例外として、[Endpoint Health（エンドポイントの正常性）] ウィジェットのデータは、この条件の影響を受けません。

Cb Defense 管理コンソールのページ（**アラート リスト**や [Investigate（調査）] など）で明確に変更されない限り、期間の設定は、すべてのページで保持されます。

次の条件を設定し、**ダッシュボード**に表示するデータをフィルターすることもできます。

- [Alert Priority（アラートの優先度）]: 表示するアラートの優先度スコアを選択します。デフォルト値は 3 です。選択した優先度スコア以上のアラートがすべて表示されます。“Priority score（優先度スコア）” を参照してください。
- [Group Alerts（アラートのグループ化）] を [OFF（オフ）] または [ON（オン）] に設定します。デフォルト値は [OFF（オフ）] です。
- [Include monitored alerts（監視対象アラートを含める）] はデフォルトで無効です。監視対象アラートは、アラートのレベルに達しない関心対象のアクティビティです。
- [Include dismissed alerts（棄却されたアラートを含める）] はデフォルトで無効です。

[Export All（すべてエクスポート）] をクリックすると、ページ上のすべてのデータが CSV ファイルにエクスポートされます。個々のデータ セットをダウンロードするには、そのウィジェットで下向き矢印をクリックします。エクスポート機能を使用するには、ブラウザーでポップアップを有効にしておく必要があります。

注意

Cb Defense 管理コンソールのセッションは、何の操作も行われないまま 1 時間を経過するとタイムアウトになります。

ダッシュボードの構成

ウィジェットは、**ダッシュボード**上で好みの順序に並べ替えて表示することができます。ウィジェットを並べ替えるには、ウィジェット上部のヘッダー部分をマウスでクリックし、新しい場所にドラッグします。また、ウィジェット右下のハンドルをクリックし、水平にドラッグすると、ウィジェットのサイズを変更できます。

さらにダッシュボードに表示するウィジェットを選択できます。

ダッシュボードを構成する：

1. PSC にログインし、**ダッシュボード** をクリックして、[Configure Dashboard （ダッシュボードを構成）] をクリックします。
2. ウィジェットを削除するには、ウィジェットに表示された赤い丸をクリックします。
3. ウィジェットを追加するには、ページ下部のウィジェットをクリックします。
4. ダッシュボードの構成が完了したら、[Save Configuration （構成を保存）] をクリックします。

[Attacks Stopped （阻止された攻撃）]

[Attacks Stopped （阻止された攻撃）] ウィジェットには、指定された時間枠およびポリシーにおいて Cb Defense が阻止した攻撃の概要が表示されます。

これらの攻撃は、ポリシー設定によりすべて阻止されています（“ ポリシーによる攻撃からの防御 ” を参照）。

このウィジェットはインターラクティブです。いずれかの攻撃タイプをクリックすると、そのタイプの攻撃の**アラート リスト** ページが開きます（“ アラート リスト ページ（Alerts List page）” を参照）。

攻撃タイプの定義を次の表に示します。

表 2: 攻撃タイプ

タイプ	説明
非マルウェア	不正な動作またはローカル ブラックリストにより阻止された、一般にマルウェアとして認識されないプロセス。これには、レピュテーションは良いが（PowerShell や Winword.exe ファイルなど）、不正な動作をするケースが含まれます。
潜在的なマルウェア	エンドポイントで悪意のあるアクションを実行する脅威のあるソフトウェア。有益なアクションも悪意のあるアクションも実行できるファイル。
マルウェア	エンドポイント上で攻撃者のために悪意のあるアクションを実行することのみが目的であると認定されたファイル。
PUP	潜在的に迷惑なプログラム。PUP は、被害が最も少ないものでも煩わしい結果をもたらし （ポップアップ広告の配信）、マルウェアの配信に利用されることもあります。

[Potentially Suspicious Activity （潜在的に疑わしいアクティビティ）]

[Potentially Suspicious Activity（潜在的に疑わしいアクティビティ）] ウィジェットには、Cb Defense により検出されたが、ポリシー ルールに従ったために、指定された時間枠およびポリシーにおいて阻止されなかったアクティビティの概要が表示されます。“ ポリシーによる攻撃からの防御 ” を参照してください。

このウィジェットはインターラクティブです。いずれかのイベント タイプをクリックすると、そのタイプのイベントの アラート リスト ページが開きます（“ アラート リスト ページ （Alerts List page）” を参照）。

潜在的に疑わしいアクティビティのタイプについては、表 2、「攻撃タイプ」を参照してください。

[Attack Stages （攻撃段階）]

ダッシュボードの [Attack Stages （攻撃段階）] ウィジェットには、指定された時間枠およびポリシーにおける攻撃段階の棒グラフが含まれています。

棒グラフは対話式です。棒グラフをクリックすると、**アラート リスト** ページにアクセスし、関連するアラートの詳細を表示できます （“ アラート リスト ページ （Alerts List page）” を参照）。

攻撃段階の定義を次の表に示します。

表 3: [Attack Stages （攻撃段階）]

段階	説明
調査	ターゲットを調査、識別、および選択します。
武器化	配信可能なペイロードを作成します。
配信 / 利用	配信して、コードを実行します。
インストール / 実行	バック ドアをインストールし、永続アクセスを許可します。
コマンドおよび制御	外部デバイスからコードで通信します。
目的の実行	目的を達成します。

[Attacks by Vector （ベクター別の攻撃）]

[Attacks by vector（ベクター別の攻撃）] ウィジェットには、指定された時間枠およびポリシーにおいて攻撃が発生したベクターが表示されます。

このウィジェットはインターラクティブです。いずれかのパーセンテージをクリックすると、選択したタイプのベクターの**アラート リスト** ページが開きます （“ アラート リスト ページ （Alerts List page）” を参照）。

[Endpoint Health （エンドポイントの正常性）]

[Endpoint Health （エンドポイントの正常性）] ウィジェットには、エンドポイントのセンサーの状態が表示されます。このウィジェットの状態は対話式です。いずれかの状態をクリックすると、[Endpoints（エンドポイント）] ページに移動し、展開したセンサーのうち選択した状態のものが表示されます。“ 展開したセンサーの表示 ” を参照してください。

赤色のテキストは、センサーでアクション （センサーの隔離モードまたはバイパス モードの解除など）が必要な可能性があることを示しています。

センサーのカテゴリを次の表に示します。

表 4: センサーのカテゴリ

段階	説明
Active （アクティブ）	センサーが登録され、過去 30 日以内にチェックインされました。
Inactive （非アクティブ）	センサーは登録されましたが、チェックインされていない期間が 30 日を超えています。
Deregistered （登録取り消し）	センサーがアンインストールされています。
Eligible for Update （更新可能）	センサーを新しいバージョンに更新できます。“センサーの更新 ” を参照してください。
Quarantined （隔離）	管理者がセンサーを隔離しました。このモードの場合、センサー ホストは Cb Defense とのみ通信できます。“ デバイスの隔離 ” を参照してください。
Bypass （バイパス）	管理者またはエンド ユーザーがこのセンサーをバイパス モードにしました。この状態の間は、センサーから Cb Defense バックエンドにデータが送信されません。 センサー バイパス（ユーザー アクション）- エンド ユーザーがセンサー UI からセンサーをバイパス モードにしました （センサー UI が有効の場合）。“[Cb Defense Settings （Cb Defense 設定）] タブ ” を参照してください。 センサー バイパス（管理者アクション）- 管理者が Cb Defense 管理コンソールからセンサーをバイパス モードにしました。

第 2 章

センサーの管理

PSC センサーは Cb Defense が保護するすべての Windows と macOS のエンドポイントにインストールされます。センサーは、Carbon Black 分析および Cb Defense 管理コンソールと通信します。

この章では、PSC センサーを表示、更新、アンインストールする方法、およびセンサーグループを使用してセンサーを管理する方法について説明します。

PSC センサーのインストール方法については、『PSC センサー インストール ガイド』を参照してください。

展開したセンサーの表示

組織全体に展開したセンサーを表示できます。

センサーを表示する：

PSC にログインし、[Endpoints （エンドポイント）] をクリックします。

センサーの並べ替え可能なリストが表示されます。次の表では、リストの内容について説明します。

表 5: センサー情報

[Title（タイトル）]	説明
Status	センサーのステータスを表すアイコン。表 6、「センサーのステータス タイプ」を参照してください。
Device Name（デバイス名）	センサーをインストールしたエンドポイントのホスト名。
User（ユーザー）	センサーを登録したユーザー。
Device Info（デバイス情報）	エンドポイントで実行されているオペレーティング システムとセンサーのバージョン。
Group/Policy（グループ / ポリシー）	センサーが属しているセンサー グループ。“ ポリシー割り当ての管理 ” を参照してください。 センサー グループのメンバーではなく、ポリシーに手動で割り当てられたセンサーは、[Manually assigned （手動で割り当て）] としてここに表示されます。センサーのメタデータがどのグループの条件にも合致しない場合、そのセンサーは [Unassigned（未割り当て）] としてここに表示されます。 センサーが属しているポリシー。“ ポリシーによる攻撃からの防御 ” を参照してください。
T	エンドポイントのターゲットバリュー。“ ターゲットバリュー （Target value）” を参照してください。

[Title（タイトル）]	説明
Last Check-in（最終チェックイン）	センサーが Cb Defense バックエンドに最後に接続した日時。
Take Action（アクション実行）	ここには次の 3 つのアイコンが表示されます。 **[Investigate （調査）]** アイコンをクリックすると、  **[Investigate （調査）]** ページが開きます。 **[Live Response]** アイコンをクリックすると、このデバイスの Live Response セッションが開きます（Live Response がこのデバイスで有効な場合）。 >_ ごみ箱アイコンをクリックすると、リストから保留中のセンサーが削除されます。 

リストは [Policy（ポリシー）] または [Status（ステータス）] でフィルターできます。これを行うには、各ドロップダウン メニューをクリックします。センサーのステータス タイプのリストについては、表 6、「センサーのステータス タイプ」を参照してください。

横に下向き矢印がある列見出しでテーブルの内容を並べ替えたり、特定のセンサーを検索したりできます。NOT ブール演算子を使用して、最新バージョン以外のすべてのバージョンのセンサーを検索できます。以下に例を示します。

- "NOT 3.2.0.213" で検索すると、バージョン 3.2.0.213 以外のすべてのセンサーのリストが返されます。
- "-3.2.0.213" で検索すると、3.2.0.213 より古いすべてのセンサーのリストが返されます。
- "NOT 3.2.0.213 NOT 3.0.2.2" で検索すると、バージョン 3.2.0.213 または 3.0.2.2 以外のセンサーのリストが返されます。

センサーの横にある山括弧 「**>**」をクリックすると、センサーの追加情報を表示できます。このアクションでは、次のセンサー データが表示されます。

- デバイス ID （Device ID）
- 内部 IP アドレス
- 外部 IP アドレス
- センサーが Cb Defense に登録された日付
- スキャン エンジンのバージョン
- Live Response ステータス

センサー グループを作成した場合 （“ ポリシー自動割り当て用のセンサー グループの管理 ” を参照）、センサー グループ名をクリックし、そのセンサー グループに属するセンサーだけを表示することができます。その場合、次の追加情報が表示されます。

- センサー グループに属するセンサーの数。
- 定義された条件に基づき、センサー　グループに属するセンサーのオペレーティング システム。[Any （すべて）]、[Windows]、または [macOS] のいずれかです。
- このセンサー グループ内のセンサーに対するポリシーの割り当て。
- センサー　グループのメンバーシップを定義する条件。メンバーシップの条件が複数ある場合は、[More （詳細）] をクリックすると、すべての条件が表示されます。

表示されているセンサーのリストは [Status （ステータス）] でフィルターできます。

表 6: センサーのステータス タイプ

ステータス	表示されるデバイス
All（すべて）	組織内のセンサーがインストールされているすべてのデバイス。
Active（アクティブ）	過去 30 日以内にチェックインされたデバイス。これはデフォルトのビューです。
Inactive（非アクティブ）	過去 30 日以内にチェックインされなかったデバイス。
Pending（保留中）	インストールに関する E メールがユーザーに送信されたが、センサーがまだインストールされていないデバイス。
Deregistered（登録取り消し）	センサーがアンインストールされたデバイス。
Errors（エラー）	センサーがエラーを報告しているデバイス。Carbon Black テクニカル サポートにお問い合わせください。“Carbon Black テクニカル サポート ” を参照してください。
Bypass（バイパス）	センサーがバイパス モードのデバイス。このモードでは、センサーからクラウドにデータが送信されません。
Eligible for Update（更新可能）	より新しいバージョンのセンサーが提供されています。“ センサーの更新 ” を参照してください。
Quarantined（隔離）	管理者が隔離したデバイス。“ デバイスの隔離 ” を参照してください。

センサーの更新

センサーは、常に最新の状態にしておくことが重要です。サポートされているオペレーティング システムとセンサーのバージョンについては、『Supported Carbon Black sensors and agents』を参照してください。

センサーの更新を管理するには、次の 2 つの方法があります。

- 選択したデバイス上のセンサーを更新します。この場合、ネットワーク速度の低下を最小限に抑えるために、一度に更新できるセンサーは最大 100 個に制限されます。“ 選択したデバイス上のセンサーの更新 ” を参照してください。
- センサーは再インストールすることができます。『PSC センサー インストール ガイド』を参照してください。

備考

センサーを更新すると、Windows が警告なしで再起動する場合があります。重要なマシンでセンサーを更新するときは、この点に注意してください。

macOS 3.0 以降のセンサーを High Sierra 以上でアップグレードするには、KEXT 承認が必要です。デバイスが承認を使用してプロビジョニングされていない場合、センサーはバイパス モードに切り替わります。Carbon Black は、アップグレードの前に、MDM ソリューションを使用して承認をプッシュしておくことをお勧めします。

『インストール / アップグレード用に Mac Sensor 3.0 KEXT を承認する方法』を参照してください。

選択したデバイス上のセンサーの更新

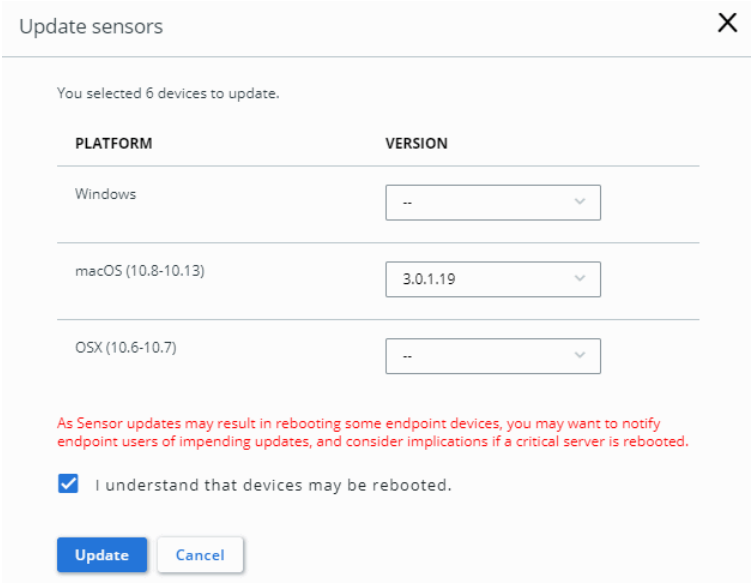
選択したデバイス上のセンサーを更新することにより、センサーの展開を制御し、ネットワーク帯域幅の飽和を低減できます。一度に更新できるセンサーは最大 100 個に制限されています。この更新には、4 時間かかります。

センサーの更新を開始すると、選択されたセンサーは、次回 Cb Defense バックエンドにチェックインしたときに更新するように指示するメッセージを受け取ります。

選択したデバイス上のセンサーを更新する :

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. 更新するセンサーを検索して選択します （“ 展開したセンサーの表示 ” を参照）。
3. [Device Names （デバイス名）] の横にあるチェックボックスをオンにして、表示されているすべてのデバイスを選択するか、表示されているリストで、デバイスを個々に選択します。
4. [Take Action （アクション実行）] をクリックしてから、[Update Sensors （センサーの更新）] をクリックします。

5. [Version （バージョン）] ドロップダウン メニューから、センサーのバージョンを選択します。デバイスの再起動を認めるチェックボックスをオンにして、[Update（更新）] ボタンをクリックします。



注意

更新対象として選択したデバイスが 100 個を超えると、一度に 100 個のセンサーしか更新できないという旨の警告が表示されます。最初の 100 個のセンサーを更新することを選択できます。

ポリシー割り当ての管理

Cb Defense の各センサーは、センサーに適用するポリシー ルールを決定する 1 つのポリシーに割り当てられます。“ ポリシーによる攻撃からの防御 ” を参照してください。

無人インストール時に指定していない限り、または新しいセンサーが自動的に割り当てられるセンサー グループを作成していない限り、新しいセンサーは、デフォルトで " 標準 " ポリシー に属します。

有人インストール時にポリシーを設定することはできません。ただし、センサーのポリシーを手動で構成することは可能です。または、センサーを自動ポリシー登録用のセンサー グループに加えることもできます。

注意

センサー グループと自動登録は、Windows v3.1 以降および macOS v3.2 以降のセンサー バージョンでのみ利用できます。

センサーのデフォルト ポリシーの手動変更

センサーのデフォルト ポリシーを手動で変更するには、次の 3 つの方法があります。

- [Investigate （調査）] ページを使用する。
- **アラート リスト** ページを使用する。
- [Sensor Management （センサーの管理）] ページを使用する。ここでは、この方法について説明します。

センサーのデフォルト ポリシーを手動で変更する :

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. 変更するセンサーを検索して選択します （“ 展開したセンサーの表示 ” を参照）。
3. [Device Names （デバイス名）] の横にあるチェックボックスをオンにして、表示されているすべてのデバイスを選択するか、表示されているリストで、デバイスを個々に選択します。
4. [Take Action （アクション実行）] をクリックしてから、[Assign policy （ポリシーの割り当て）] をクリックします。
5. ドロップダウン　メニューで新しいポリシーを選択します。すべてのセンサーを選択した場合、チェックボックスをオンにしてその選択を確認する必要があります。選択したデバイスの自動割り当てのオン / オフを切り替えることができます。[Save （保存）] をクリックします。

ポリシー自動割り当て用のセンサー グループの管理

Windows センサー v3.1 以降または macOS センサー v3.2 以降を展開している場合は、センサー グループを作成し、それらのグループにセンサーを追加できます。センサー グループ内のすべてのセンサーは、センサーに関連付けられているメタデータと定義した条件に基づいて、ポリシーに自動で割り当てられます。これにより、多数のセンサーの管理にかかる時間を節約できます。

Cb Defense センサー v3.1 以降のメタデータには、次の情報が含まれます。

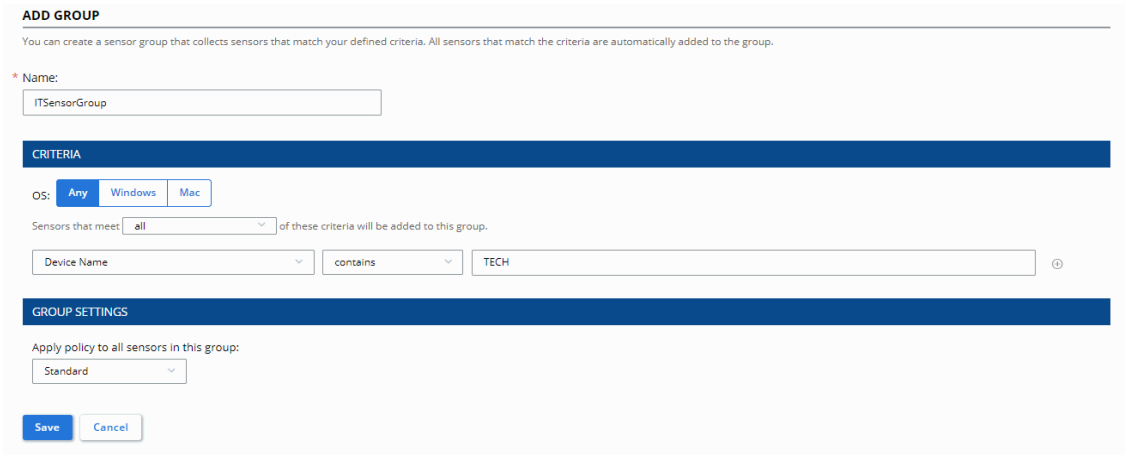
- オペレーティング システム （すべて、Windows、macOS）
- Active Directory 組織単位
- Active Directory ドメイン
- Active Directory 識別名
- デバイス ホスト名
- サブネット（サブネット フィルターはセンサーの内部 IP アドレスに適用されます）。

Windows v3.1 または macOS v3.2 より前のバージョンの Cb Defense センサーのメタデータには、次の情報が含まれます。

- オペレーティング システム （すべて、Windows、macOS）
- デバイス ホスト名
- サブネット （サブネット フィルターはセンサーの内部 IP アドレスに適用されます）

センサー グループを追加する：

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. [Add Group （グループの追加）] をクリックします。



3. グループの一意の名前を入力します。
4. センサーをグループに追加する条件を指定します。
   a. デフォルトでは、指定したすべての条件に一致するセンサーのみがグループに追加されます。ただし、この設定を OR 条件に変更することもできます。これを行うには、[Sensors that meet all of these criteria will be added to this group（これらの条件すべてを満たすセンサーをこのグループに追加）] のドロップダウン メニューをクリックし、設定を [all（すべて）] ではなく [any（いずれか）] に変更します。

b. このセンサー グループに含めるセンサーのオペレーティング システムを選択します。すべてのオペレーティング システム、Windows、または macOS から選択できます。
c. センサーのメタデータに基づく条件を追加します。たとえば、Active Directory の組織単位 （財務部門など）を指定したり、192 で始まるサブネットの範囲を指定したりできます。
d. 指定が完了するまで、条件を追加し続けます。

5. [Policy（ポリシー）] ドロップダウン メニューを使用して、センサーを追加するポリシーを指定します。デフォルトのポリシーは標準ポリシー （Standard）です。
6. [Save （保存）] をクリックします。

[Endpoints （エンドポイント）] ページの左上隅に、新しいセンサー グループが [Processing（処理中）] と表示されます。変更を加えられるよう Cb Defense は 2 分間待機してから、これらの変更を処理します。ステータスは続いて [Up to Date （最新）] に変わります。センサーは Cb Defense にチェックインしたときに、新しいセンサー グループに追加されます。

センサー グループを作成すると、センサー グループは [Endpoints （エンドポイント）] ページの左側に表示されます。[>>] をクリックすると、センサー グループの追加情報を表示できます。

センサー グループはリストの上から順に処理されます。たとえば、作成した条件に基づいて判断すると、複数のセンサー グループに当てはまるセンサーがあるとします。しかし、センサーが所属できるセンサー グループは 1 つだけです。この場合、センサーはリストに表示されている最初のセンサー グループに追加されます。

センサーグループのリストを並べ替えることで、処理順序を変更できます。[Edit（編集）] をクリックし、リスト内の新しい位置にセンサー グループをドラッグします。

いずれかのセンサー グループをクリックすると、そのグループに属するセンサーだけが表示されます。右側のパネルに、“ 展開したセンサーの表示 ” で説明するとおり、センサーがテーブル ビューで表示されます。

コマンド ラインから Windows センサーを管理する

Windows センサー v3.3 のリリースに伴い、RepCLI コマンド ライン ツールを使用して、エンドポイントで直接センサーを管理できるようになりました。このツールは、開発者によるテストや、サポートによるトラブルシューティングと修理、ローカル管理の目的で内部的に使用できます。

RepCLI は、userSid によって認証されます。RepCLI ツールを有効にするには、無人センサーのインストール時に、<CLI_USERS>= <sid> フィールドを指定します。指定されたユーザー グループに属するすべてのメンバーが、認証済み RepCLI コマンドを使用できます。

オプションで、Cb Defense を管理するユーザーのサブセットを特定し、このフィールドを使用して認証することができます。Repcli 専用のユーザーアカウントを設定することもできます。

Carbon Black は、当初は RepCLI 機能を使用する予定がない場合でも、インストール時に新しい AD ユーザー グループを作成し、ユーザー SID を指定しておくことをお勧めします。そうすることで、問題のあるセンサーを修復する必要があるがバックエンドに接続できない場合に、RepCLI コマンドを使用してセンサーを修復できます。

macOS センサーの無人バイパス制御の有効化と無効化

macOS センサー v3.1 以降のセンサー バイパス モードは、無人バイパス制御コマンド ライン オプションを使用して有効化および無効化できます。ユーザーは、センサーのトラブルシューティングや、診断とログを収集し、エンドポイントを潜在的に重大な状態から回復させることができます。

センサーのバイパスを有効にして保護を無効にしたり、センサーのバイパスを無効にして保護を有効にしたりするには、ユーザーを認証するための有効なアンインストール コードが必要です。またエンドポイントで管理者権限が必要です。

無人バイパス制御を有効にするには、次の手順を実行します。

1. アンインストール コードを必要とするポリシーを設定し、アンインストール コードを取得します。“ センサーのアンインストール ” を参照してください。
2. コマンド ラインを実行して、バイパス制御を有効または無効にします。

無人バイパス制御を有効にし、保護を無効にする :

1. 以下のコマンドを実行します。

```
sudo /Applications/Confer.app/uninstall -b uninstall_code
```

無人バイパス制御を無効にし、保護を有効にする :

1. 以下のコマンドを実行します。

```
sudo /Applications/Confer.app/uninstall -n uninstall_code
```

更新されたステータスが [Sensor Management （センサー管理）] ページに表示されます。またエンドポイント UI が有効な場合は、そこにも表示されます。

Windows Update 用の Windows レジストリ キーの設定

Carbon Black では、Windows Update との互換性を保つのに必要なレジストリ キーを設定する方法を用意しています。

詳細については、Windows KB 4072699 を参照してください。

レジストリ キーを設定する :

1. PSC にログインし、[Settings （設定）] をクリックして [General （一般）] をクリックします。
2. [Send Registry Key （レジストリ キーを送信）] をクリックします。

ALLOW REGKEY を設定すると、各 Windows 3.1 以降のセンサーが次回 Cb Defense にチェックインしたときに、レジストリ キーがインストールされます。

正常にインストールされると、次のレジストリ キーと値が作成されます。

```
Key="HKEY_LOCAL_MACHINE"Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat"
Value Name="cadca5fe-87d3-4b96-b7fb-a231484277cc"
Type="REG_DWORD”
Data="0x00000000”
```

注意

管理者権限のあるすべてのユーザーが、レジストリ キーを手動で削除できます。Microsoft では、キーの作成後はそのキーの変更および削除を行わないことを推奨しています。

センサーのアンインストール

PSC コンソールを使用してエンドポイント上のセンサーをアンインストールできます。または、エンドポイントでアンインストールすることもできます。

v3.1 以降のセンサーを展開している場合は、一意のランダム生成コードを要求することで、エンドポイントでのセンサーのアンインストール操作を防止することができます。この設定は、ポリシー単位で有効になります。アンインストール コードは大文字と小文字が区別されます。

エンドポイントでセンサーをアンインストールする際にコードを要求する：

1. PSC にログインし、[Enforce （適用）] をクリックして [Policies （ポリシー）] をクリックします。
2. この機能を有効にするポリシーを選択します。
3. [Cb Defense Settings（Cb Defense 設定）] タブで [Require Code to Uninstall Sensor（センサーのアンインストールにコードが必要）] チェックボックスをオンにします。
4. [Save （保存）] をクリックして変更を保存します。

この設定を有効にすると、エンドポイントからセンサーをアンインストールするために、個別のデバイス アンインストール コードまたは会社登録取り消しコードが必要になります。PSC コンソールを使用する場合は、センサーのアンインストールにコードは必要ありません。

個別のデバイス アンインストール コードは、センサーが Cb Defense に登録されるときに自動生成されます。

センサー アンインストール コードを確認する：

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. センサーの横にある「**>**」をクリックします。アンインストール コードが基本センサー データの下に表示されます。

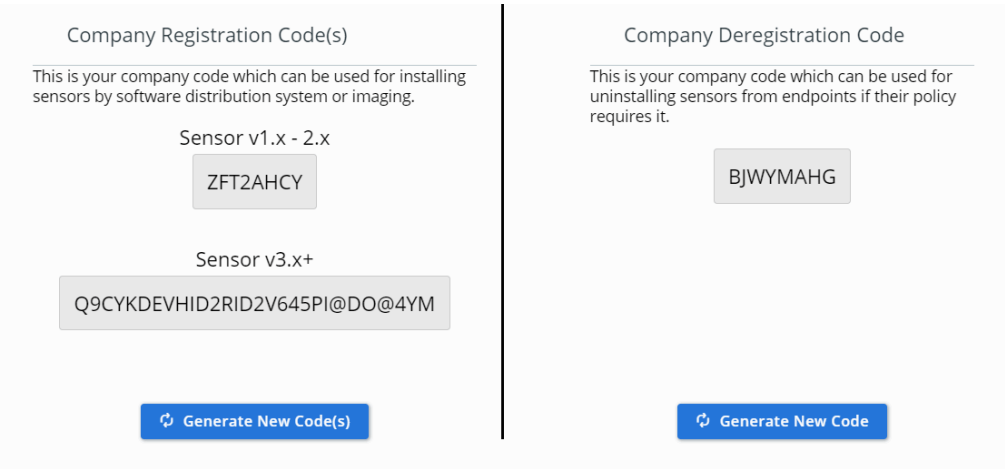
会社登録取り消しコードを生成し、このコードを使用して組織のセンサーをアンインストールすることもできます。

> **警告**
>
> 会社登録取り消しコードを使用すると、組織のセンサーをすべてアンインストールできます。組織全体で使用できる単一のコードを使用しない場合は、会社登録取り消しコードを生成しないでください。

会社登録取り消しコードを生成する：

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. [Sensor Options （センサー オプション）] をクリックし、[Company codes （会社コード）] をクリックします。

3. [Company Deregistration Code(s)（会社登録取り消しコード）] の下にある [Generate New Code(s)（新しいコードの生成）] ボタンをクリックします。



Windows エンドポイントでセンサーをアンインストールする：

1. 管理者権限でコマンド プロンプト ウィンドウを開きます。
2. `Confer` ディレクトリに移動します。
3. 次のコマンドを実行します。デバイス アンインストール コードまたは会社登録取り消しコードを要求するよう Cb Defense を構成している場合は、コマンドの一部としてコードを入力します （例：`uninstall.exe /uninstall 35EQCCYG??`
4. `Confer` ディレクトリとログ ファイルは、センサーをアンインストールした後も残ります。

ヒント

バッチ ファイルまたはシステム管理ツールを使用すると、複数のセンサーをアンインストールできます。

macOS センサーの無人アンインストールを実行する：

1. 管理者権限でターミナルを開きます。
2. `sudo /Applications/Confer.app/uninstall -y` と入力します。
3. [Enter （入力）] をクリックします。

注意

デフォルトでは、この方法はインターラクティブであり、`-y` パラメーターを指定しない限り、確認メッセージが要求されます。すべてのコマンド ライン パラメーターを表示するには、`-h` パラメーターを指定してコマンドを実行します。

デバイス アンインストール コードまたは会社登録取り消しコードを要求するよう Cb Defense を構成している場合は、コマンドの一部としてコードを入力します。以下に例を示します。

```
sudo /Applications/Confer.app/uninstall -y -c 35EQCCYG
```

PSC コンソールを使用してセンサーをアンインストールする：

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. アンインストールするセンサーを検索して選択します （“ 展開したセンサーの表示 ” を参照）。
3. [Device Names （デバイス名）] の横にあるチェックボックスをオンにして、表示されているすべてのデバイスを選択するか、表示されているリストで、デバイスを個々に選択します。
4. [Take Action（アクション実行）] をクリックしてから、[Uninstall（アンインストール）] をクリックします。

センサーはアンインストール後も [Endpoint （エンドポイント）] ページ上に表示されたままになります。

登録が取り消されたセンサーを手動で削除する：

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. センサーのリストをフィルターして、登録を取り消したセンサーだけを表示します（“ 展開したセンサーの表示 ” を参照）。
3. 削除するセンサーを選択します。
4. [Take Action（アクション実行）] をクリックしてから、[Delete deregistered devices（登録を取り消したデバイスの削除）] をクリックします。削除を確認するように求められます。

登録が取り消されたセンサーを自動で削除する：

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. [Sensor Options（センサー オプション）] をクリックし、[Sensor settings（センサー設定）] をクリックします。
3. [Auto-delete registered sensors（登録が取り消されたセンサーの自動削除）] を選択し、指定する時間枠を設定します。[Save （保存）] をクリックします。

第 3 章

ユーザーの管理

各 Cb Defense ユーザーは、ユーザー名とパスワードを使用して Cb Defense にログインする必要があります。ユーザーには次の 3 種類があります。

- 完全な管理者権限。
- 完全な管理者権限と Live Response 管理者権限。
- 表示のみの権限。ユーザーが持つ権限が表示のみの権限の場合、ユーザー インターフェイスの一部の要素 （たとえば、[Take Action （アクション実行）]）が表示されません。

Live Response 管理者ロールは管理者ロールよりも優先されます。この権限を付与できるのは、Live Response 管理者権限を持つ別のユーザーのみです。既存のお客様の場合、管理者権限を持つすべてのユーザーが Live Response 管理者ロールに昇格されます。ユーザーを確認して、Live Response アクセス権が不要な管理者は降格することをお勧めします。

この章では、Cb Defense ユーザーの管理方法と監査ログの表示方法について説明します。

ユーザーを表示する：

1. PSC にログインし、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。

   現在のすべてのユーザーのリストが表示されます。名、姓、E メール、または役割による並べ替えや、ユーザーの検索を行うことができます。

ユーザーの詳細を変更する：

1. PSC にログインし、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。
2. 変更するユーザーの隣の [Edit （編集）] ボタンをクリックします。

ユーザーを追加する：

1. PSC にログインし、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。
2. [Add User （ユーザーを追加）] をクリックします。
3. 新しいユーザーについて次の詳細情報を入力し、[Add （追加）] をクリックします。
4. ログインしてパスワードを作成するように勧める E メールが新しいユーザーに送信されます。パスワードは、次の特性を備えている必要があります。
   - 1 文字以上の小文字
   - 1 文字以上の大文字
   - 1 文字以上の数字
   - 1 文字以上の特殊文字
   - 8 文字以上

ユーザーを削除する：

1. PSC にログインし、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。
2. 削除するユーザーの [Edit （編集）] ボタンの横にある下向き矢印をクリックします。
3. [Delete （削除）] をクリックします。

監査ログの監視

監査ログを監視する：

1. PSC にログインし、[Settings （設定）] をクリックして [Audit Log （監査ログ）] をクリックします。

   Cb Defense 管理者によって実行されたアクティビティの一覧がテーブルに表示されます。

2. パフォーマンスを高速化し、不要なログを [Audit Log （監査ログ）] テーブルから削除するには、右上隅にある [Flagged （フラグ付き）] および [Verbose （詳細）] スライダー ボタンを使用します。
   - [Flagged（フラグ付き）] - このオプションを有効にすると、[Audit Log（監査ログ）] テーブルにフラグ付きのエントリのみが表示されます。たとえば、ユーザーが疑わしい IP アドレス （ユーザーがログインに使用した最後の 5 つの IP アドレスのどれにも該当しない IP アドレス）から Cb Defense にログインしたとします。このアクティビティはフラグ付きとしてマークされます。
   - [Verbose （詳細）] - このオプションを無効にすると、[Audit Log （監査ログ）] テーブルに表示アクションのみが表示されます。有効にすると、編集 / 更新 / 作成アクションが表示されます。このオプションのデフォルト設定は [Verbose（詳細）] = [Off （オフ）] です。

第 4 章

プレミスの定義

Cb Defense では、組織の境界線を定義できます。これは、攻撃時にエンドポイントがオンプレミスとオフプレミスのいずれに存在するかを判断するのに役立ちます。

この章では、境界線の定義方法について説明します。

センサーがオンプレミスとオフプレミスのどちらに存在するかの判断には、完全修飾ドメイン名 （FQDN）と IP アドレスという 2 つの条件が使用されます。

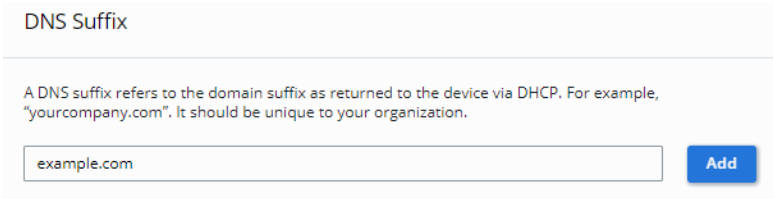
デバイスで関連する FQDN がネットワーク アダプターに登録されている場合、そのデバイスがオンプレミスとして認識されるための有効な条件が表示されます。また、デバイスが組織のネットワークにも接続されており、センサーが [Reachable Hosts （到達可能なホスト）] で定義されている IP アドレスの 1 つ以上を ping できる場合、これもデバイスをオンプレミスとして定義する条件となります。デバイスがオンプレミスであると判断するには、これらの条件の一方または両方が満たされている必要があります。いずれの条件も満たされていない場合、デバイスはオフプレミスとなります。

注意

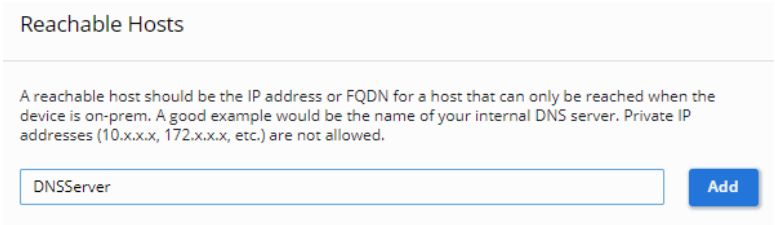
ホーム ネットワーク デバイスまたはリモート ネットワーク デバイスが [Reachable Hosts（到達可能なホスト）] の条件と一致する場合、この条件を満たすことができ、その結果として、センサーは自身が実際はオフプレミスのときでも、オンプレミスであると報告します。

境界線を設定する：

1. PSC にログインし、[Settings （設定）] をクリックして [General （一般）] をクリックします。
2. 次のアクションの一方または両方を実行します。
   a. [DNS suffix（DNS サフィックス）] テキスト ボックスにドメインを追加し、[Add （追加）] をクリックします。



   b. 到達可能なホストを追加して、[Add （追加）] をクリックします。



第 5 章

アラートの表示およびアラートに対するアクションの実行

この章では、[Alerts （アラート）] ページについて説明します。このページでは、アラートの検索、アラートの詳細の表示、アラートへのメモおよび検索可能ラベル （タグ）の追加、複数のデバイスのアラートの管理などを実行できます。

アラートの深刻度 （Alert severity）

Cb Defense で検出されたすべてのアラートは、深刻度別にグループ化されます。通知をセットアップするときはアラートの深刻度と優先度を考慮する必要があります（“ 通知およびコネクター ” を参照）。

- [Threat （脅威）] – 悪意のあるアクティビティである可能性が高い。
- [Monitored （監視対象）] – 対応を要するレベルには達していないが、破壊的である可能性があり、注意を要する行動が含まれる一連の行動データです。

Priority score （優先度スコア）

優先度スコアは、アラートの相対的重要度に基づいて優先順位を付けたもので、[Attack Stages （攻撃段階）] パネルにおおまかにマッピングされます （“[Attack Stages （攻撃段階）]” を参照）。

一般に、スコアが高いほど敵対者または攻撃がその目的達成に近いことを示します。たとえば、特定のマルウェアの目的が永続性にある場合、アラートの優先度は高くなりません。その目的がユーザー データの暗号化、パスワードの盗み取り、システム ファイルへの損害などの場合、このアラートの優先度は高くなります。

例 :

- **レベル 1 と 2 のアラート** – ポート スキャン、マルウェア ドロップ、システム構成ファイルへの変更、永続性などのアクティビティを検出します。
- **レベル 3、4、5 のアラート** – マルウェアの実行、一般のウィルスに似た挙動、ユーザー入力の監視、メモリ スクレイピングの可能性、パスワードの盗み取りなどのアクティビティを検出します。
- **レベル 6 以上のアラート** – 一般的に、脆弱性を突く攻撃、リバース コマンド シェル、プロセスのハロウイング、破壊的なマルウェア、非表示のプロセスとツールセット、不要なネットワーク通信を行うアプリケーションなどです。

ターゲットバリュー （Target value）

ターゲットバリューはデバイスが属しているポリシーによって定義されます（“ ポリシーによる攻撃からの防御 ” を参照）。特定のデバイスで検出された任意の脅威の脅威レベルを計算する際に乗数としての役割を果たします。

- **低いターゲットバリュー** – 脅威レベルが低くなります。
- **中間ターゲットバリュー** – ベースラインを表します （乗数なし）。

- **高いターゲットバリューおよびミッション クリティカルなターゲットバリュー** – 同じ状況下でどちらも脅威レベルが高くなります。その結果、説明は同じでもアラートの優先度が異なる 2 つ以上のアラートが表示される場合があります。

アラート リスト ページ （Alerts List page）

[アラート （Alerts）] ページには、[Navigation （ナビゲーション）] パネルからアクセスできます。[Alerts （アラート）] ページには、(検索またはフィルターを使用して特定のアラートを表示している場合を除き）すべてのアラートが一覧表示されます。

[アラート（Alerts）] ページでは、特定された脅威が並べ替え可能なビューで表示されます。アラートには、迅速なトリアージと対応を求めることができるイベントを特定するための優先度スコアが割り当てられています。

ヒント

アラートの視覚的表現を表示する方法については、“ アラートの視覚的表示 ” を参照してください。

[Alerts（アラート）] ページでは、アラートの検索、検索するアラートの期間の設定、[Group Alerts （アラートのグループ化）] の [ON （オン）] と [Group Alerts （アラートのグループ化）] の [OFF （オフ）] の切り替え、および検索条件の保存を行うことができます。

アラートを選択すると、[Alerts（アラート）] ページの上部パネルに、主なプロセス（“ アラートの影響を受ける主なプロセスの表示 ” を参照）やデバイス詳細（“ デバイス詳細の表示 ” を参照）など、選択したアラートに関する情報が表示されます。上部パネルの右上隅にある [X] をクリックすると、パネルを閉じることができます。新しいアラートを選択すると、パネルが自動的にもう一度開きます。

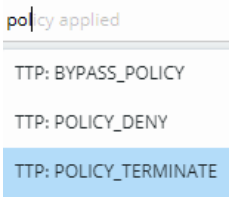
アラートの検索

[Alerts （アラート）] ページの上部の [Search （検索）] テキスト ボックスでは、デバイス、アプリケーション、特定のアラート、およびキーワードに基づいてアラートを検索できます。

すべてのアラートを表示するには、[Search （検索）] テキスト ボックスを空にしたまま **Enter** キーを押します。

表示される検索結果は、ページ上部の [Time（時間）] ドロップダウン メニューで指定された時間枠に基づきます。時間枠の設定には、3 時間、1 日、1 週間、2 週間、1 か月、3 か月、全期間、またはカスタム設定を指定できます。

検索テキスト ボックスに入力を開始すると、テキスト ボックスにキーワードの候補が表示されます。これらのキーワードはキーと値のペアの一部です。キーワードの候補を選択するには、キーボードの **Tab** キーまたは右向き矢印を押します。または、キーワード全体を入力し、その後にコロンを付ける方法もあります。選択可能な値のリストがテキスト ボックスの下に表示されます。



選択したら、**Enter** キーを押してキーと値のペアを選択します。キーと値のペアを選択すると、検索結果が返されるまでの時間が短くなります。

検索テキスト ボックスにキーと値のペアを複数入力した場合、AND 演算子が自動的にキーと値の各ペアの間に設定されます。AND 演算子を OR または NOT に変更できます。

検索の名前を入力すると、検索テキスト ボックスには保存した検索も表示されます。

たとえば、次の画像に示す 2 つのキーと値のペアでは、Windows オペレーティング システムを実行しているデバイスで発生した、COMMON_WHITE_LIST レピュテーションを持つすべてのアラートが返されます。

アラート ページのキーと値のペアを次の表に示します。

表 7: アラート ページのキーと値のペア

キー	定義	例
application name（アプリケーション名）	アプリケーションの名前。	Chrome.exe、cmd.exe、python.py
application hash（アプリケーション ハッシュ）	アプリケーションの SHA256 ハッシュ。	8c5996dd3348f351f892f8878823e1952f468c6b4cf38d20e9f7a0f96d767630
incident ID（インシデント ID）	アラートの一意の識別子。	XZUJKYJ1
priority score（優先度スコア）	イベントの重要度レベル （1 ～ 10）。詳細については、“Priority score （優先度スコア）” を参照してください。	3, 4
device ID（デバイス ID）	デバイスの一意のシステム識別子。	37668
operating system（オペレーティング システム）	デバイスのオペレーティング システム （Microsoft Windows または macOS）。	Windows
email address（E メール アドレス）	デバイスを登録したユーザーの E メール アドレス。	someone@example.com
policy（ポリシー）	ポリシーの名前。	Standard
TTP	Cb Defense によって分類された脅威の痕跡。“TTP のリファレンス ” を参照してください。	FILE_DROP、RUN_ANOTHER_APP

キー	定義	例
reputation（レピュテーション）	Cb Defense によって識別されたアプリケーションのレピュテーション。	TRUSTED_WHITE_LIST
threat source（脅威のソース）	イベントまたはアラートのトリガー元のベクター。	app_store、removable media、other_net_protocol、remote_drive、web、email
threat category（脅威カテゴリ）	Cb Defense によって識別された脅威のカテゴリ。	non_malware、malware
policy applied（ポリシー適用済み）	ポリシーが監視対象の一連のイベントに適用されたかどうかを示します。	APPLIED、NOT_APPLIED

キーと値のペアをオフに切り替えるには、**[Enable Advanced Search （高度な検索の有効化）]** ボタンをクリックします。キーと値のペアをオンに切り替えるには、**[Disable Advanced Search （高度な検索の無効化）]** をクリックします。

注意

キーと値のペアの使用は推奨であり、必須ではありません。クエリの作成に、キーと値のペアを使用する必要はありません。

キーフレーズや語句の基本的な検索を実行できます。単一の語は、特殊文字を使用せずに入力できます。複数の語やフレーズは、引用符で囲む必要があります。これにより、CB Defense は、複数の語やフレーズを、複数の検索語句ではなく、単一の検索語句として理解します。

検索時、1 つ以上の語句がアラートで見つかる場合があります。これには、イベント ID、イベントの説明、さまざまな攻撃手口（TTP）、イベント サマリーの情報などの項目の検索が含まれます。

アプリケーションについては、アプリケーション名、ハッシュ、レピュテーションなどの項目の検索が可能です。デバイスについては、デバイス名、ポリシー、オペレーティング システム、ユーザー （センサー登録時に使用された E メール アドレス）などの項目の検索が可能です。ネットワークについては、オンプレミス、オフプレミス、IP アドレス、ポート、接続タイプの検索が可能です。

イベント、アプリケーション、デバイス、またはネットワーク情報の高度な検索機能を実行できます。検索にはブール演算子とワイルドカードを使用できます。検索では、大文字と小文字は区別されません。

検索では、複数の語句を組み合わせることができます。論理演算子を使用して、検索の照合時に満たす必要がある特定の条件を指定できます。

- **OR** は、指定したいずれかの条件が true の場合に結果を表示します。たとえば、ドメイン名と IP アドレスを OR で結んで検索します。
- **AND** は、両方の条件が true の場合に結果を表示します。たとえば、ポートとプロトコルを AND で結んで検索したり、アプリケーションとアプリケーション実行元のデバイスを AND で結んで検索したりできます。

- **NOT** は、条件を除外して検索します。たとえば、KNOWN_ MALWARE を検索するときに zbot.exe マルウェアを NOT で結ぶと、zbot.exe を除くすべての既知のマルウェアが返されます。

最初の 3 文字以上に続くアスタリスクを 1 文字以上に対応するワイルドカードとして使用できます。末尾の疑問符は、疑問符の代わりの 1 文字を含むフレーズと一致します。

簡易検索例 :

```
powershell*
```

この検索を実行すると、"PowerShell" を含むすべてのアラートが返されます。

高度な検索例 :

```
"github.com" OR "192.198.55.55"?TCP AND 443? OR?UDP AND 80?
KNOWN_MALWARE AND NOT zbot.exe
```

この検索を実行すると、発信元が github.com または IP アドレス 192.198.55.55 のポート 443 またはポート 80 の UDP であり、 `zbot.exe` を除く既知のマルウェアのアラートがすべて返されます。

クエリを入力した後、**Enter** キーを押します。

ヒント

POLICY_TERMINATE または POLICY_DENY を検索することで、すべてのポリシー アクション （ブロック / 終了）を取得できます。OR 演算子を使用すると、その両方を検索できます。

[Search （検索）] テキスト ボックスの横の [?] をクリックすると、検索の例やヒントが表示されます。

高度な検索クエリ語句をすべて網羅したリストについては、“ 高度な検索語句 ” を参照してください。

テーブル内の検索結果が検索パラメーターに従って更新されます。検索は累積的に行われるため、検索を複数回実行する場合は、新しい検索を開始する前に [Clear All （すべてを消去）] をクリックします。ページ上部の [Save（保存）] ボタンをクリックすると、検索を保存できます。

検索結果のフィルタリング

[Alerts（アラート）] ページの左パネルでは、検索結果テーブルに表示される結果をフィルターできます。結果は、次の要素でフィルターできます。

[Category （カテゴリ）]

[Category （カテゴリ）] リストには、2 つのカテゴリ タイプと 2 つの調整可能なフィルターが含まれています。

[Threat （脅威）] カテゴリ （Threat category）

[Monitored（監視対象）] カテゴリは、対応を要するレベルには達していないが、破壊的である可能性があり、注意を要する行動が含まれる一連の行動データです。

[Threat （脅威）] カテゴリは、一連の行動データと、悪意ある行動を示すコンテキスト情報です。

ターゲットバリュー （Target value）

左側のバー フィルターには、ターゲットバリューでデバイスをフィルター処理できる 4 つのバーが含まれています （“ ターゲットバリュー （Target value）” を参照）。[+] をクリックするとターゲットバリューが大きくなり、[-] をクリックするとターゲットバリューが小さくなります。

- 1 = 低
- 2 = 中
- 3 = 高
- 4 = ミッション クリティカル

[Alert Priority （アラートの優先度）]

アラートを優先度 （**P**）スコアでフィルターできます。優先度スコアは 1 から 10 の範囲です （1 が最低）。(“Priority score （優先度スコア）” を参照）。[-] をクリックすると優先度スコアが小さくなり、[+] をクリックすると優先度スコアが大きくなります。

[Devices （デバイス）]

[Devices （デバイス）] リストでは、特定のデバイスのみが表示されるようにアラートをフィルターできます。1 つのデバイスまたは複数のデバイスのすべてのアラートを表示できます。

Applications （アプリケーション）

多くの攻撃には、複数のアプリケーションが関連しています。表示されるアラートのリストを、特定のアプリケーションに関連するアラートのみに絞り込んで表示することができます。

[Workflow （ワークフロー）]

[Workflow （ワークフロー）] リストでは、チームによって引き続き監視されているかまたは棄却されているかに基づいて脅威をフィルターできます。アラートは、このページまたは [Alert Triage （アラートのトリアージ）] ページで棄却することができます。[Alert Triage （アラートのトリアージ）] ページの詳細については、“ アラートの視覚的表示 ” を参照してください。

[Reputation （レピュテーション）]

[Reputation （レピュテーション）] リストでは、関連オブジェクトのレピュテーションに基づいて検索結果をフィルターできます。レピュテーションの種類は次のとおりです。

- Not listed （リストになし）
- Suspected malware （疑わしいマルウェア）
- Common white list （一般的なホワイト リスト）
- PUP
- 信頼できるホワイト リスト
- 既知のマルウェア

“ レピュテーションの管理 ” を参照してください。

Status

[Status（ステータス）] リストでは、防止ポリシーが適用されたアラートか、マルウェアが実行されたケースまたは実行されなかったケースのみが表示されるように結果をフィルターできます。[Status （ステータス）] リストの内容は次のとおりです。

- Did not run （未実行）
- Ran （実行済み）
- No policy applied （ポリシー未適用）
- policy applied （ポリシー適用済み）

[Policies （ポリシー）]

[Policies （ポリシー）] リストでは、アラート作成時にセンサーが割り当てられたポリシーに基づいて結果をフィルターできます。“ ポリシーによる攻撃からの防御 ” を参照してください。

[Tags （タグ）]

[Tags （タグ）] リストには、アラートに割り当てることができるタグ （短いラベル）が含まれています。タグに基づいて並べ替えや検索を行うことができます。

検索結果の表示

アラート検索結果テーブルには、情報が含まれた複数の列があります。ここでは、これらの列について説明します。

注意

[Group Alerts （アラートのグループ化）] を [ON （オン）] に設定すると、複数のデバイス上の同一の脅威が [Alerts Results （アラート結果）] テーブルでグループ化されます。“ 複数のデバイスにおけるアラートの管理 ” を参照してください。

表 8: 検索結果

列	説明
チェックボックス	アラートまたはアラートのグループの横にあるチェックボックスをオンにして、棄却するアラートを選択できます。表示されたすべてのアラートを選択するには、検索結果テーブルの上にあるチェックボックスをクリックします。この選択には、現在のページに表示できるアラートのみが含まれます。組織内のすべてのアラートが含まれるわけではありません。「アラートの棄却」(41 ページ) を参照してください。
Status	各アラートのステータスは、次のいずれかです。 • policy applied （ポリシー適用済み） • Ran （実行済み） • メモ追加 • タグ追加
First Seen （最初の認識日時）	このアラートが最初に発生した日付と時刻。この列に基づいて並べ替えを行うことができます。
Reason （理由）	アラートの理由。
P	[P] 列はアラートに関連付けられた優先度スコアを示しています。“Priority score （優先度スコア）” を参照してください。
T	アラートに関連付けられたターゲットバリュー。“ ターゲットバリュー （Target value）” を参照してください。
Device （デバイス）	アラートに関連付けられたデバイスに関する情報が表示されます。ユーザーの E メール アドレスとデバイスのホスト名が表示されます。グループ化されたアラートを表示している場合はこの列は表示されないことに注意してください。
Take Action （アクション実行）	[Take Action （アクション実行）] 列には、アラートに対して実行できるいくつかのオプションが表示されます。表 9、「アクションのオプション」を参照してください。

表 9: アクションのオプション

アイコン	説明
	アラートのグループ化されたセットを示します。グループ化を解除するには、このアイコンをクリックします。
	このアイコンをクリックすると、[Alert Triage（アラートのトリアージ）] ページに移動します。“ アラートの視覚的表示 ” を参照してください。
	このアイコンをクリックすると、[Investigate （調査）] ページに移動します。“ アラートの調査 ” を参照してください。
	このアイコンをクリックすると、アラートに対して実行できる追加のアクションが表示されます。 • アラートを棄却する。 • アラートの通知履歴を表示する。

アラートの棄却

アラートを棄却する方法はいくつかあります。1 つのデバイスまたはすべてのデバイスでアラートを棄却することができます。一度に複数のアラートを棄却したり、今後発生する同じアラートをすべて棄却したりすることができます。棄却されたアラートは、監査ログに表示されます。

アラートを棄却する際、必要に応じて棄却の理由を選択できます。次の理由が一覧に表示されます。

- [False Positive （偽陽性）]
- [Alert list cleanup/duplicate （アラートのクリーンアップ / 重複）]
- [Known good software/behavior （品質確認済みのソフトウェア / 動作）]
- [Investigated/escalated （調査済み / 報告済み）]

注意

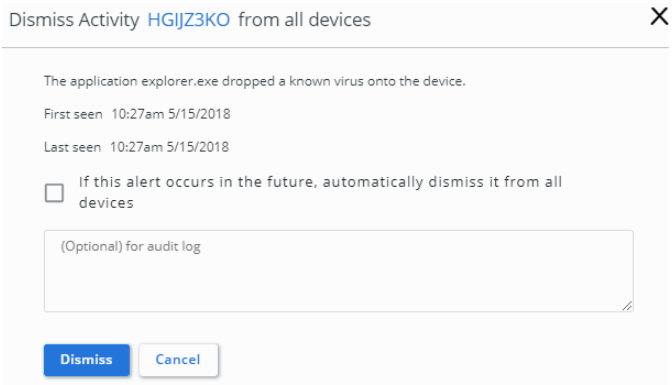
アラートの棄却と E メール通知は、連動していません。今後発生するすべてのアラートを棄却しても、アラートに関する E メール通知は届きます。

1 つのデバイスでアラートを棄却するには :

1. [アラート リスト （Alerts List）] ページの右上にある [Group Alerts （アラートのグループ化）] をオフにします。
2. 棄却するアラートの横にある [Take Action （アクション実行）] メニューをクリックします。
3. [Dismiss （棄却）] をクリックします。[Dismiss （棄却）] をもう一度クリックして、アラートの棄却を確定します。

すべてのデバイスでアラートを棄却する：

1. [アラート リスト （Alerts List）] ページの右上にある [Group Alerts （アラートのグループ化）] をオンにします。
2. 棄却するアラートの横にある [Take Action （アクション実**行）]** メニューをクリックします。
3. [Dismiss on all devices （すべてのデバイスで棄却）] をクリックします。



注意 : アラートに異なる SHA256 ハッシュが表示される場合があります。複数のデバイスでアラートを棄却するには、オブジェクトのハッシュが同じである必要があります。

4. 必要に応じて、今後発生する同じアラートをすべて棄却するには、[If this alert occurs in the future, automatically dismiss it from all devices（今後このアラートが発生した場合に、すべてのデバイスで自動的に棄却する）] のチェックボックスを選択します。

   注意 : 今後のアラートを棄却するオプションは、ハッシュや TTP などの一意の識別子に基づいています。識別子が変更された場合は、再び同じアラートを受け取ります。
5. [Dismiss （棄却）] をクリックします。

複数のアラートを棄却する：

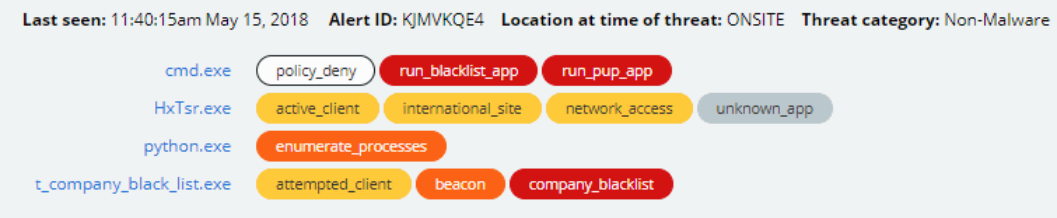
1. 棄却するアラートを選択します。表示されたすべてのアラートを棄却するには、検索結果テーブルの上の見出しに表示されているチェックボックスを選択します。

   注意 : すべてのアラートを選択した場合は、現在表示されているアラートのみが棄却されます。
2. [Dismiss Alerts （アラートの棄却）] をクリックします。
3. 必要に応じて、今後発生する同じアラートをすべて棄却するには、[If this alert occurs in the future, automatically dismiss it from all devices（今後このアラートが発生した場合に、すべてのデバイスで自動的に棄却する）] のチェックボックスを選択します。
4. [Dismiss （棄却）] をクリックします。

アラートを棄却すると、そのアクションは監査ログに記録されます。複数のアラートを棄却した場合は、そのアクションは "Process alert dismissal request for 3 alert(s)（3 つのアラートに対してアラート棄却要求を処理）" として記録されます。その後、棄却されたアラートがそれぞれ処理されると、この処理は個々のアクションとして監査ログに記録されます。“ 監査ログの監視 ” を参照してください。

アラートの展開

アラートを展開するには、[Status （ステータス）] 列の左側の [>] をクリックします。アラートのビューが展開されて追加の情報が表示されます。



ヒント :“TTP のリファレンス ” を参照してください。

アラートの影響を受ける主なプロセスの表示

検索結果テーブルでアラートをクリックすると、**[Primary process（主なプロセス）]** タブがデフォルトで選択されます。

> **注意**
>
> [Product（製品）] フィールドは、アプリケーションが属する製品の名前が表示されます。たとえば、 `cmd.exe` は Windows オペレーティング システムに属します。

アラートに対してアクションを実行するには、[Take Action （アクション実行）] の横にある下向き矢印をクリックします。以下のオプションがあります。

- アプリケーションを組織のホワイトリストまたはブラックリストに追加する。“ レピュテーションの管理 ” を参照してください。
- アプリケーション プロセスを終了する。
- 分析のためにアプリケーションをアップロードする。“ 疑わしいファイルのアップロード ” を参照してください。
- VirusTotal で、さまざまなソースからのハッシュに関する最新情報を確認する。
- アプリケーションを削除する。アプリケーションは、このエンドポイントからのみ 1 回だけ削除することも、すべてのエンドポイントからアプリケーションを削除することもできます。

  重要 : すべてのエンドポイントからアプリケーションを削除すると、組織内のすべてのエンドポイントからアプリケーションが永久に削除されます。削除を取り消すことはできません。削除されたアプリケーションは受信ボックスで確認することができます。

デバイス詳細の表示

アラートに関連付けられているデバイスの詳細を表示する :

1. 検索結果テーブルでアラートをクリックします。
2. [Device （デバイス）] タブをクリックします。
3. デバイスに対してアクションを実行するには、[Take Action （アクション実行）] の横にある下向き矢印をクリックします。以下のオプションがあります。
   - バックグラウンド スキャンを有効または無効にする。
   - バイパスを有効または無効にする。
   - ホストを隔離する、または隔離を解除する。隔離されたデバイスは Cb Defense とのみ通信できます。センサーは、デバイスが隔離されていることを示す通知を Cb Defense から受け取ります。“ デバイスの隔離 ” を参照してください。
   - センサーとの Live Response セッションを開始する。“Live Response の使用 ” を参照してください。

アラートのメモとタグの表示および追加

[Notes/Tags （メモ / タグ）] タブを使用して、脅威を確認した管理者によって追加されたメモおよびタグを表示できます。

メモ / タグにアクセスする :

1. 検索結果テーブルでアラートをダブルクリックし、[Notes/Tags（メモ / タグ）] タブを選択します。このアラートに関して管理者が残したすべてのメモやタグが [Notes/Tags （メモ / タグ）] パネルに表示されます。
2. このアラートに新しいメモまたはタグを追加するには、新しいメモまたはタグを対応するテキスト ボックスに入力し、**Enter** キーを押します。

複数のデバイスにおけるアラートの管理

[Group Alerts （アラートのグループ化）] を [ON （オン）] に設定すると、複数のデバイスで同じアラートが発生した場合に、これらのアラートが検索結果テーブルで 1 行にまとめられます。

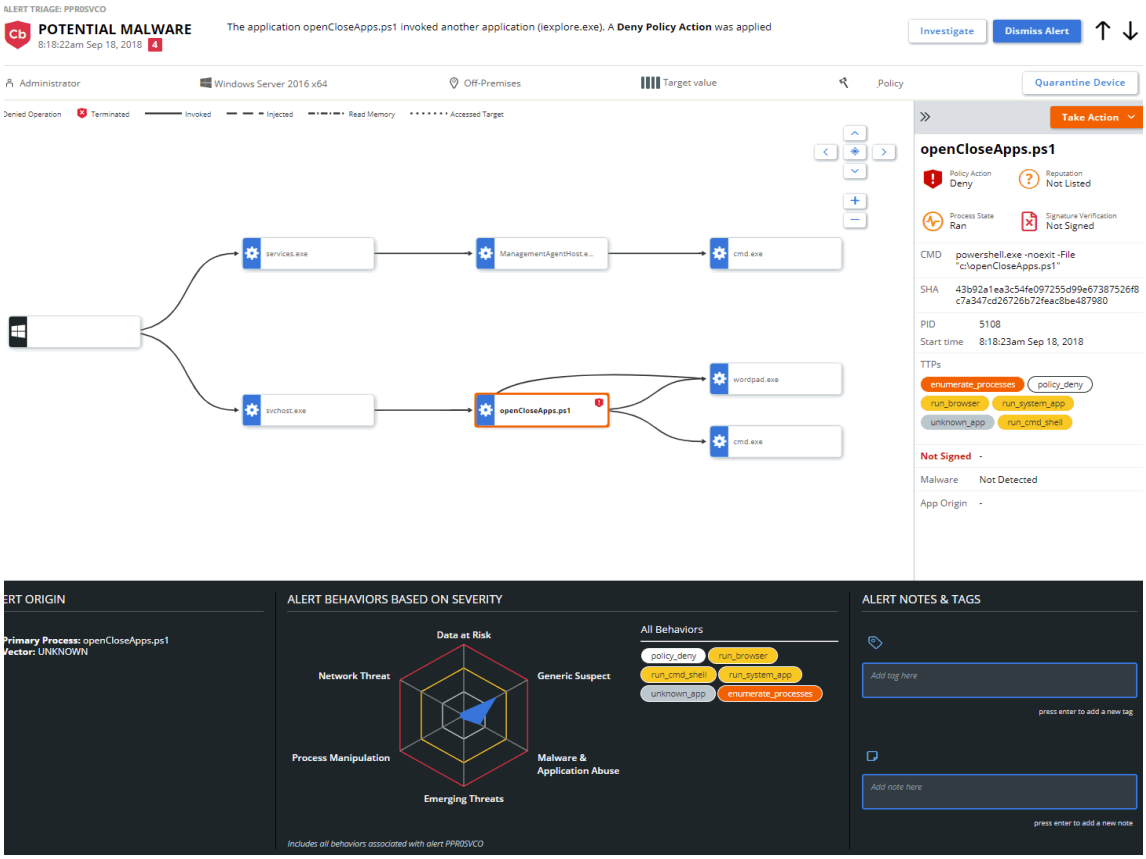
[Group（グループ）] アイコンをクリックすると、アラートの 1 つのセットのグループ化を解除してアラートを個別に表示できます。また、ページの上部にある [Groups Alerts （アラートのグループ化）] を [OFF （オフ）] に切り替えて、すべてのグループ化を解除することもできます。グループ化を再度有効にするには、[Groups Alerts （アラートのグループ化）] を [ON （オン）] に切り替えます。

アラートをグループ化すると、複数のデバイス間でアラートを棄却することができます。“ アラートの棄却 ” を参照してください。

第 6 章

アラートの視覚的表示

[Alert Triage（アラートのトリアージ）] ページでは、アラートが視覚的に表示されます。



[Alert Triage（アラートのトリアージ）] ページには、[Alerts（アラート）] ページ（“ アラートの表示およびアラートに対するアクションの実行 ” を参照）または [Investigate（調査）] ページ （“ アラートの調査 ” を参照）からアクセスできます。

通知を作成すると、通知 E メール内のアラート リンクから [Alert Triage （アラートのトリアージ）] ページに直接移動できます。“ 通知およびコネクター ” を参照してください。

[Alert Triage（アラートのトリアージ）] ページの上部パネルは [Alert Triage Reason（アラートのトリアージの理由）] パネルと呼ばれます。このパネルには、次の表に示されている情報が表示されます。

表 10: [Alert Triage Reason （アラートのトリアージの理由）] パネル

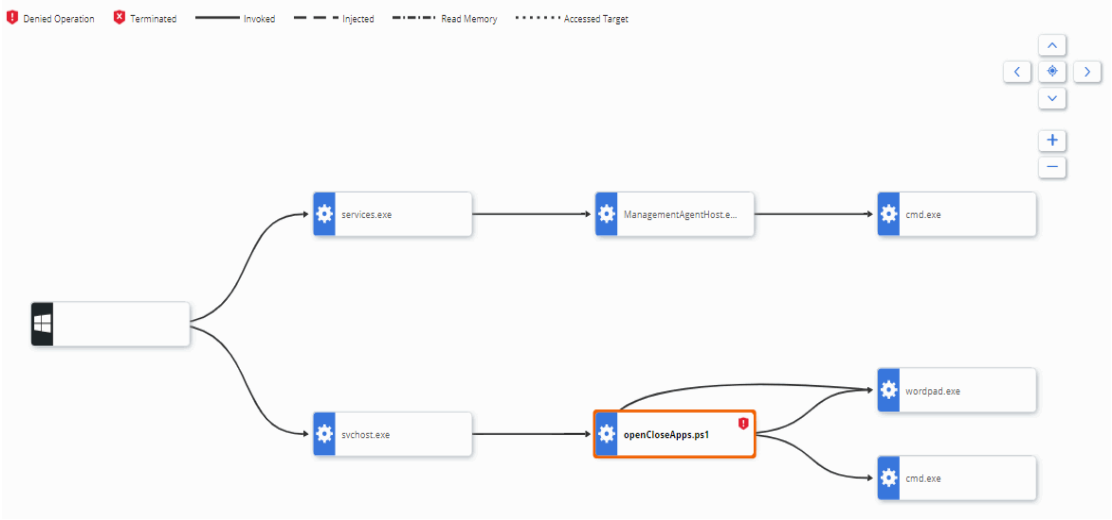
項目	説明
Alert Triage ID（アラートのトリアージ ID）	Cb Defense がこのアラートに対して生成した一意の ID。
Attack Type（攻撃タイプ）	検出された攻撃のタイプ。攻撃タイプの詳細については、表 2、「攻撃タイプ」を参照してください。
Reason （理由）	アラートの理由。
Date and Time（日時）	アラートが最初に発生した日時。
Priority Score（優先度スコア）	優先度スコアは 1 から 10 の範囲です （1 が最低）。“Priority score（優先度スコア）” を参照してください。
User（ユーザー）	アラート発生時にホストにログインしていたユーザーの名前。
Operating System（オペレーティング システム）	アラートが発生したときにホスト デバイス上で実行されていたオペレーティング システム。
Location（場所）	アラートが発生したときにデバイスがオンプレミスであったかオフプレミスであったかを示します。
[Target Value（ターゲットバリュー）]	デバイスのターゲットバリュー。“ ターゲットバリュー （Target value）” を参照してください。
ポリシー	ホスト デバイスのポリシー。

このパネルでは、次のアクションを実行できます。

- アラートを調査する。[Investigate （調査）] をクリックして [Investigate （調査）] ページに移動し、アラートの詳細な分析を行います （“ アラートの調査 ” を参照）。
- アラートを棄却する、または棄却操作を解除する。棄却する理由を説明するコメントを追加するよう求められます。棄却操作の完了後、アラートの表示に戻りますが、詳細は淡色表示されます。
- ホスト デバイスをネットワークの他の部分から隔離して PSC とだけ通信するようにする。“ デバイスの隔離 ” を参照してください。
- センサーとの Live Response セッションを開始する。“Live Response の使用 ” を参照してください。
- [Alert Triage （アラートのトリアージ）] ページの右上にある上向き矢印と下向き矢印をクリックして、アラート リスト内を移動する。

[Process Graph （プロセスグラフ）] パネル

[Alert Triage （アラートのトリアージ）] ページの [Process Graph （プロセスグラフ）] パネルには、アラートが視覚的に表示されます。これは、*" プロセス ツリー "* と呼ばれます。攻撃ストリーム （プロセス、ファイル、またはネットワーク接続）内の各イベントは、プロセス ツリーに " ノード " として表示されます。



攻撃元は画像の左側に表示されます。攻撃ストリーム内の後続の各イベントは、攻撃が進行するにつれて左から右に進みます。このパネルでは、ビューをパンできるほか、ズームインまたはズームアウトして表示する詳細情報の量を増減することができます。パネル上で画像全体をクリックしてドラッグすることができます。

プロセス ツリーには、次の 4 つのノード タイプがあります。

- プロセス ツリーの一番左にあるルート 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 アイコンは、デバイス上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。該当する場合、デバイスのデバイス名、ユーザー名、および IP アドレスも表示されます。
- 実行されていたプロセスまたは実行中のプロセスは、歯車のアイコンでプロセス ツリーに表示されます。プロセスの名前が表示されます。ストリーム内の任意のプロセスをクリックすると、そのプロセスの詳細が [Selected Process （選択したプロセス）] パネルに表示されます（“[Selected Process（選択したプロセス）] パネル ” を参照）。
- ディスク上に作成されたファイルは、ドキュメントとしてプロセス　ツリーに表示されます。ファイル名が表示されます。ファイルをクリックして追加情報を表示することはできません。
- 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。IP アドレスをクリックして追加情報を表示することはできません。

処理が拒否された場合、拒否されたプロセスの横のグラフに感嘆符 (**!**) が表示されます。プロセスが終了した場合、終了したプロセスの横のグラフに **X** が表示されます。

プロセス ツリーには、次の 4 種類の線が表示されます。

- [Invoked （呼び出し）]: 実線は、あるプロセスが別のプロセス、ファイル、またはネットワーク接続を呼び出したことを示します。
- [Injected （挿入）]: 破線は、あるプロセスが別のプロセスにコードを挿入したことを示します。

- [Read Memory （メモリ読み取り）]: 点線と破線の組み合わせは、あるプロセスが別のプロセスの仮想メモリを読み取ろうとしたことを示しています（プロセスへの挿入は行っていません）。
- [Accessed Target （ターゲットにアクセス）]: 点線は、あるプロセスが別のプロセスに侵入しようとしたことを示しています （プロセスへの挿入は行っていません）。

[Selected Process （選択したプロセス）] パネル

[Selected Process （選択したプロセス）] パネルには、プロセス グラフで現在選択されているノードに関する次の情報が表示されます。

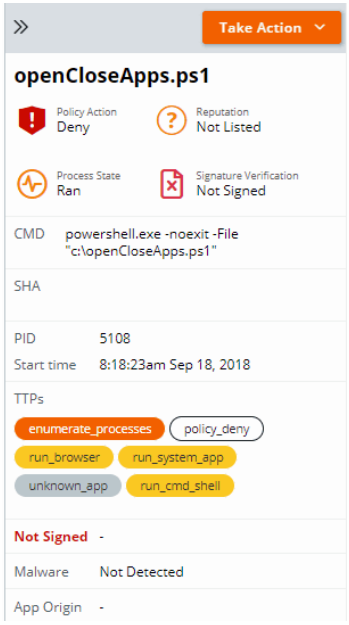


表 11: [Selected Process （選択したプロセス）] パネル

項目	説明
APP Origin（アプリの発生元）	選択されたプロセスの発生元。
CMD	実行されたプロセスの名前。
Date and Time（日時）	プロセスが実行された日時。
マルウェア（Malware）	アプリケーションが既知のマルウェアであるかどうか。このフィールドには、ベクター、マルウェア名、およびマルウェア タイプが含まれます。
Policy Action（ポリシー アクション）	実行されたあらゆるポリシー アクション。

項目	説明
Process State（プロセスの状態）	選択されたプロセスの状態。
レピュテーション（Reputation）	アプリケーションのレピュテーション。“ レピュテーションの管理 ” を参照してください。
Signature（署名）	アプリケーションの署名者 （署名されている場合）と、アプリケーションが属する製品。たとえば、 `cmd.exe` は Windows オペレーティング システムに属します。
Signature Verification（署名検証）	アプリケーションが署名されているかどうかを示します。
SHA	プロセスの SHA256 ハッシュ。
TTP	選択したプロセスに関連付けられている攻撃手口 （TTP）。円の色は TTP の深刻度を表します。色の凡例については、表 13、「TTP の色と深刻度の凡例」を参照してください。“TTP のリファレンス ” を参照してください。

このパネルでは、次のアクションを実行できます。

- アプリケーションをホワイトリストまたはブラックリストに追加する。
- プロセスを終了する。
- アプリケーションのアップロードを要求する。アプリケーションは受信ボックスにアップロードされます。“ 疑わしいファイルのアップロード ” を参照してください。
- VirusTotal で、さまざまなソースからのハッシュに関する最新情報を確認する。
- アプリケーションを削除する。アプリケーションはこのデバイスからのみ 1 回だけ削除されます。または、すべてのデバイスからアプリケーションを削除することもできます。削除されたアプリケーションは受信ボックスで確認することができます。“ 受信ボックスのファイルを表示する :” を参照してください。

重要

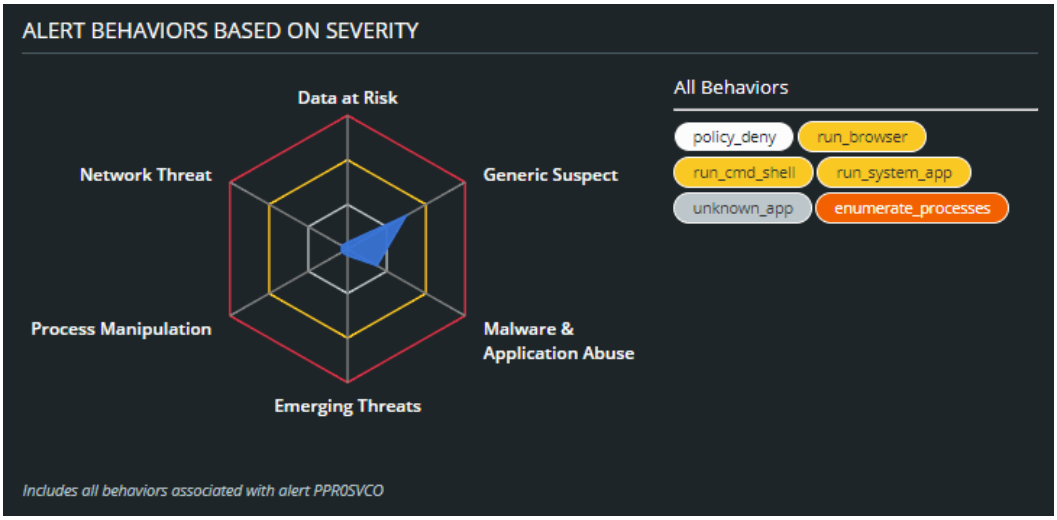
すべてのデバイスからアプリケーションを削除すると、組織内のすべてのデバイスからアプリケーションが " 永久 " に削除されます。

[Alert Origin （アラート発生元）]

ページの左下のパネルには、アラートの主なプロセスがどのようにホストに導入されたかが示されます。**[説明 （説明）]** フィールドには、主なプロセスがディスクに書き込まれた方法に関する詳細情報が表示されます。Cb Defense のインストールにあらかじめ用意されたファイルは、[Detected by Cb Defense （Cb Defense によって検出）] として表示されます。

[Alert behaviors based on severity （深刻度に基づくアラートの動作）]

ページの下部の中央セクションには、深刻度に基づくアラートの動作が示されます。このセクションには、"TTP スパイダー グラフ " と呼ばれる対話型グラフがあります。



グラフの各セグメントには、TTP カテゴリのラベルが付けられています。これらのカテゴリについては、] を参照してください。

表 12: アラートの動作のカテゴリ

Category （カテゴリ）	説明
Data at Risk（データの危険性）	Cb Defense によって保護されているエンドポイント上のデータの機密性、可用性、または整合性を損なう意図がある動作に焦点を当てます。このカテゴリに分類される TTP の例として、ランサムウェア タイプの動作や、ユーザーの資格情報にアクセスする試みがあります。
Emerging Threats（新しい脅威）	マルウェア以外の攻撃に関連する動作に焦点を当てます。これには、通常、PowerShell などのネイティブ コマンド ライン ユーティリティの悪用や、バッファ オーバーフローなどの関連するアクティビティの悪用などの動作が該当します。これは、特に Cb Defense センサーの改変を目的とした悪意のある動作を表しています。
Generic Suspect（一般的な危険性）	主に複数のマルウェア ファミリに共通する一方で、既知の正常なアプリケーションでも一般的に見られる動作を含みます。この動作の例として、デバイスを再起動しても持続したり、システム上で実行中のプロセスを列挙したりする試みがあります。
Malware & Application Abuse（マルウェアとアプリケーションの悪用）	一般的に悪いレピュテーションを持つファイル （実行ファイルまたは一般的なスクリプト タイプ）または既知の悪いレピュテーションを持つファイルを実行しているアプリケーションに関連する TTP を表します。このカテゴリは、システム アプリケーションの実行の監視も表します。ただし、悪意のあるアクションではない可能性が高いため、これらの TTP には低い優先度が与えられます。
Network Threat（ネットワーク脅威）	ネットワークを介して通信するプロセスまたは着信接続をリッスンするプロセスを含むすべての TTP が含まれます。
Process Manipulation（プロセス操作）	Cb Defense で保護されたデバイス上で実行されている他のプロセスのメモリを変更または読み取る目的をよく表している動作に焦点を当てます。高度な攻撃でよく見られるアクティビティの 1 つの例として、別のプロセスのメモリにコードを挿入するアクティビティがあります。

グラフの任意のカテゴリ ラベルをクリックすると、関連する TTP が表示されます。アラートに関連付けられているすべての TTP を表示するには、グラフの青色でハイライト表示されたセクションをクリックします。“TTP” を参照してください。

TTP は、アラートの深刻度を反映した色で表示されます。色とその深刻度ステータスを次の表に示します。

表 13: TTP の色と深刻度の凡例

色	深刻度
暗い赤色	深刻
明るい赤色	[High （高）]
オレンジ	中
黄色	低
灰色	None （なし）

メモおよびタグ

右下のパネルでは、このアラートに関するメモやタグを表示したり書き込んだりすることができます。タグまたはメモを対応するテキスト ボックスに入力し、**Enter** キーを押します。

タグに基づいてアラートを検索することができます。］を参照してください。

第 7 章

アラートの調査

[Investigate（調査）] ページでは、アラートを調査して分析できます。[Investigate （調査）] ページは、次の場所からアクセスできます。

- [Navigation （ナビゲーション）] バー。
- [Alerts List （アラート リスト）] ページ （“ アラート リスト ページ （Alerts List page）” を参照）。
- [Endpoints （エンドポイント）] ページ （“ 展開したセンサーの表示 ” を参照）。
- [Alert Triage（アラートのトリアージ）] ページ（“ アラートの視覚的表示 ” を参照）。

[Investigate （調査）] ページには、以下の 4 つのメイン タブがあります。

- [Events （イベント）] タブ - “ イベントの調査 ” を参照。
- [Applications （アプリケーション）] タブ - “ アプリケーションの調査 ” を参照。
- [Devices （デバイス）] タブ - “ デバイスの調査 ” を参照。
- [Network （ネットワーク）] タブ - “ ネットワーク接続の調査 ” を参照。

すべてのタブには、[Event Time Line （イベントのタイムライン）] サブタブがあります。“ ライムラインの表示 ” を参照してください。

これらの 4 つの主要なタブには、フィルターの選択およびイベントの特性に応じて、他にもさまざまなサブタブが含まれる場合があります。

- [Devices （デバイス）] サブタブ - “[Device （デバイス）] サブタブの表示 ” を参照。
- [Parent App（親アプリ）]、[Selected App（選択されたアプリ）]、[Target App（ターゲット アプリ）] の各サブタブ - “[App （アプリ）] サブタブの表示 ” を参照。
- [Notes/Tags（メモ / タグ）] サブタブ - “[Notes/Tags（メモ / タグ）] サブタブの表示 ” を参照。
- [Threat（脅威）] サブタブ - “[Notes/Tags（メモ / タグ）] サブタブの表示 ” を参照。

調査するイベントの検索

調査するイベントを検索できます。たとえば、デバイス、アプリケーション、特定のアラート、キーワードを検索できます。

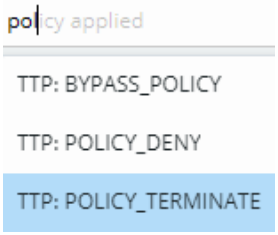
すべてのイベントを表示するには、[Search （検索）] テキスト ボックスを空にしたまま **Enter** キーを押します。

検索結果は、ページ上部の [Time（時間）] ドロップダウン メニューで指定された時間枠に基づきます。時間枠の設定には、3 時間、1 日、1 週間、2 週間、1 か月、3 か月、全期間、またはカスタム設定を指定できます。

環境内のエンドポイントにどのように新しいポリシーが適用されるのかを予測するのに役立つ一意の検索候補が 8 つあります。[Investigate （調査）] 検索テキスト ボックスをクリックすると、8 つの検索候補が表示されます。これらの名前はポリシー ルールの操作に基づいています。検索は、脅威の痕跡と TTP の組み合わせで構成されます。

レピュテーション （アプリケーションの分野）と検索候補 （操作の分野）を組み合わせて使用すると、環境内のイベントをマッピングして高度なポリシー（Advanced）ルールを作成するのに役立ちます。“ 権限、ブロック、隔離に関するポリシー ルールの作成 ” を参照してください。

検索候補を選択する必要はありません。検索テキスト ボックスに入力を開始すると、テキスト ボックスにキーワードの候補が表示されます。これらのキーワードはキーと値のペアの一部です。キーワードの候補を選択するには、キーボードの **Tab** キーまたは右向き矢印を押します。または、キーワード全体を入力し、その後にコロンを付ける方法もあります。選択可能な値のリストがテキスト ボックスの下に表示されます。



選択したら、**Enter** キーを押してキーと値のペアを選択します。

検索テキスト ボックスにキーと値のペアを複数入力することもできます。

検索テキスト ボックスのコピー アイコンを使用すると、検索文字列をコピーできます。

検索の名前を入力すると、検索テキスト ボックスには保存した検索も表示されます。

たとえば、次の画像に示す 2 つのキーと値のペアでは、Windows オペレーティング システムを実行しているデバイスで発生した、TTP ATTEMPTED_CLIENT を持つすべてのイベントが返されます。

[Investigate （調査）] ページのキーと値のペアを次の表に示します。

表 14: [Investigate （調査）] ページのキーと値のペア

キー	定義	例
application name（アプリケーション名）	アプリケーションの名前。	Chrome.exe、cmd.exe、python.py
application hash（アプリケーション ハッシュ）	アプリケーションの SHA256 ハッシュ。	8c5996dd3348f351f892f8878823e1952f468c6b4cf38d20e9f7a0f96d767630
application hash（MD5）（アプリケーション ハッシュ （MD5））	アプリケーションの MD5 ハッシュ。	7c02d432566b56e1c224173c9c7792ac
event ID（イベント ID）	イベントの一意の識別子。	0f89def3988711e79869e1c8480ed70a
incident ID（インシデント ID）	アラートの一意の識別子。	XZUJKYJ
priority score（優先度スコア）	イベントの重要度レベル （1 ～ 10）。“Priority score （優先度スコア）” を参照してください。	3, 4
location（場所）	デバイスの場所 （オンプレミスまたはオフプレミス）。	Onsite、Offsite
IP address（IP アドレス）	ネットワーク関連イベントで識別された IP アドレス。	192.168.0.1
device name（デバイス名）	デバイスの一意のホスト名。	SampleDevice01
device ID（デバイス ID）	デバイスの一意のシステム識別子。	37668
operating system（オペレーティング システム）	デバイスのオペレーティング システム （Microsoft Windows または macOS）。	Windows
email address（E メール アドレス）	デバイスを登録したユーザーの E メール アドレス。	someone@example.com
policy（ポリシー）	ポリシーの名前。	Standard
event type（イベント タイプ）	イベントのタイプ。	network、file_create、registry_access、system_api_call、create_process、data_access、policy_action

キー	定義	例
TTP	Cb Defense によって分類された脅威の痕跡。“TTP のリファレンス ” を参照してください。	FILE_DROP、RUN_ANOTHER_APP
reputation（レピュテーション）	Cb Defense によって識別されたアプリケーションのレピュテーション。	TRUSTED_WHITE_LIST
attack stage（攻撃段階）	イベントの攻撃段階。“[Attack Stages （攻撃段階）]” を参照してください。	recon、weaponize、deliver/expl、inst/run、cmd+ctrl、execute goal
operation（操作）	ポリシー ルールで操作にマッピングします。	Communicates over the network（ネットワーク経由で通信）

詳細な検索語句を入力すると、特定のアラートを検索できます。たとえば、各アラートには複数のタイプのレピュテーションが割り当てられています。all.reputation、parent.reputation、target.reputation、または primary.reputation を検索できます。使用できる詳細な検索語句を次の表に示します。

表 15: 詳細な検索語句

語句	詳細な検索語句
Reputation（レピュテーション）	• all.reputation • parent.reputation • target.reputation • primary.reputation
Applied Reputation（適用されたレピュテーション）	• all.applied reputation • parent.applied reputation • target.applied reputation • primary.applied reputation
Application Name（アプリケーション名）	• all.app name • parent.app name • target.app name • primary.app name
IP address（IP アドレス）	• all.IP address • peer.IP • device.IP • source.IP • destination.IP
Application Hash（アプリケーション ハッシュ）	• all.SHA256 • parent.SHA256 • target.SHA256 • primary.SHA256

キーと値のペアをオフに切り替えるには、[Enable Advanced Search（高度な検索の有効化）] ボタンをクリックします。キーと値のペアをオンに切り替えるには、[Disable Advanced Search （高度な検索の無効化）] をクリックします。

注意

キーと値のペアの使用は推奨であり、必須ではありません。クエリの作成に、キーと値のペアを使用する必要はありません。

キーフレーズや語句の基本的な検索を実行できます。単一の語は、特殊文字を使用せずに入力できます。複数の語やフレーズは、引用符で囲む必要があります。これにより、CB Defense は、複数の語やフレーズを、複数の検索語句ではなく、単一の検索語句として理解します。

検索時、1 つ以上の語句がイベントで見つかる場合があります。これには、イベント ID、イベントの説明、さまざまな攻撃手口（TTP）、イベント サマリーの情報などの項目の検索が含まれます。

アプリケーションについては、アプリケーション名、ハッシュ、レピュテーションなどの項目の検索が可能です。デバイスについては、デバイス名、ポリシー、オペレーティングシステム、ユーザー （センサー登録時に使用された E メール アドレス）などの項目の検索が可能です。ネットワークについては、オンプレミス、オフプレミス、IP アドレス、ポート、接続タイプの検索が可能です。

イベント、アプリケーション、デバイス、またはネットワーク情報の高度な検索機能を実行できます。検索にはブール演算子とワイルドカードを使用できます。検索では、大文字と小文字は区別されません。

検索では、複数の語句を組み合わせることができます。論理演算子を使用して、検索の照合時に満たす必要がある特定の条件を指定できます。

- **OR** は、指定したいずれかの条件が true の場合に結果を表示します。たとえば、ドメイン名と IP アドレスを OR で結んで検索します。
- **AND** は、両方の条件が true の場合に結果を表示します。たとえば、ポートとプロトコルを AND で結んで検索したり、アプリケーションとアプリケーション実行元のデバイスを AND で結んで検索したりできます。
- **NOT** は、条件を除外して検索します。たとえば、KNOWN_ MALWARE を検索するときに zbot.exe マルウェアを NOT で結ぶと、zbot.exe を除くすべての既知のマルウェアが返されます。

最初の 3 文字以上に続くアスタリスクを 1 文字以上に対応するワイルドカードとして使用できます。末尾の疑問符は、疑問符の代わりの 1 文字を含むフレーズと一致します。

簡易検索例 :

```
powershell*
```

この検索を実行すると、"PowerShell" を含むすべてのイベントが返されます。

高度な検索例 :

```
"github.com" OR "192.198.55.55"?TCP AND 443? OR?UDP AND 80?
KNOWN_MALWARE AND NOT zbot.exe
```

この検索を実行すると、発信元が github.com または IP アドレス 192.198.55.55 のポート 443 またはポート 80 の UDP であり、zbot.exe を除く既知のマルウェアのイベントがすべて返されます。

クエリを入力した後、**Enter** キーを押します。

ヒント

POLICY_TERMINATE または POLICY_DENY を検索することで、すべてのポリシー アクション （ブロック / 終了）を取得できます。OR 演算子を使用すると、その両方を検索できます。

[Search （検索）] テキスト ボックスの横の [?] をクリックすると、検索の例やヒントが表示されます。

高度な検索クエリ語句をすべて網羅したリストについては、“ 高度な検索語句 ” を参照してください。

検索は累積的に行われるため、検索を複数回実行する場合は、新しい検索を開始する前に [Clear All （すべてを消去）] をクリックします。ページ上部の [Save （保存）] ボタンをクリックすると、検索を保存できます。

検索結果のフィルタリング

[Investigate （調査）] ページの左パネルでは、検索結果テーブルに表示される結果をフィルターできます。結果は、次の要素でフィルターできます。

- [Devices （デバイス）] リストでは、特定のデバイスで発生したイベントを表示するように検索結果をフィルターできます。1 つ以上のデバイスを選択すると、[Alerts （アラート）] フィルターが表示され、1 つのアラートに焦点を当てることができます。
- [Connections to（接続先）] 選択した接続のみを表示するように検索結果をフィルターできます。接続は、ドメイン名または IP アドレスで定義されます。
- 特定のアプリケーションに関連するイベントのみが含まれるようにリストをフィルターします。

イベントの調査

[Investigate （調査）] ページでは、デフォルトで [Events （イベント）] タブが選択されています。このタブでは、Cb Defense に保存されているすべてのイベントの詳細を調査できます。これらのイベントには、デバイスにインストールされているアプリケーションが実行したすべての操作 （失敗した操作と成功した操作）などが含まれています。操作が Cb Defense によってブロックまたは終了された場合は、POLICY_DENY または POLICY_TERMINATE という TTP がイベントに付加されます。

指定した時間枠内のすべてのイベントを表示し、イベントの時刻でテーブルを並べ替えることができます。

このタブには、検索時点のアプリケーション レピュテーションが表示されます。たとえば、以前は不明であったアプリケーションが**リストにない**というレピュテーションを持っているとします。ただし、イベント後にレピュテーションが**一般的な適応型ホワイトリスト**にアップグレードされる場合があります。この場合、検索結果内に**一般的な適応型ホワイトリスト**が表示されます。

アプリケーション レピュテーションのハッシュ値の詳細については、次を参照してください。
『Cb Defense: How to Confirm Reputation of a Hash at the Time of Policy Action』

アプリケーション名のハイパーリンクをクリックすると、そのアプリケーションに関連するすべてのイベントを検索できます。またホスト名のハイパーリンクをクリックすると、そのエンドポイント上のすべてのイベントを検索できます。

表示されるデータの詳細については、次の内容を参照してください。

- “[Category （カテゴリ）]”
- “[Attack Stages （攻撃段階）]”
- “Priority score （優先度スコア）”
- “ レピュテーションの管理 ”
- “TTP のリファレンス ”

イベントの詳細情報を表示するには、イベント行の左側にある **[>]** をクリックして展開します。

アプリケーションの調査

[Applications （アプリケーション）] タブには、一意のアプリケーション ハッシュで生成されたイベントの総数に関する詳細なレポートが表示されます。アプリケーション ハッシュを選択すると、アプリケーションのさらに詳細な情報の表示、レピュテーションの管理、アプリケーションに対するアクションの実行が可能になります。アプリケーションに割り当てたレピュテーションは、保護されたすべてのエンドポイントに適用されます。

レピュテーションは、オブジェクトに与えられた信頼または不信頼のレベルです。Cb Defense ファイルのレピュテーションは、既知の正常なオブジェクトと既知の不正なオブジェクトの複数のソースに基づいています。“ レピュテーションの管理 ” を参照してください。

個々のアプリケーションのレピュテーションを変更するには、アプリケーションの横にある [Whitelist（ホワイトリスト）] または [Blacklist（ブラックリスト）] をクリックします。

デバイスの調査

[Devices （デバイス）] タブには、デバイスで生成されたイベントの総数に関する詳細なレポートが表示されます。デバイスを選択すると、デバイスの詳細をさらに表示したり、デバイスに対してアクションを実行したりできます。

ネットワーク接続の調査

[Network（ネットワーク）] タブには、環境内のすべてのアプリケーションが生成した、すべてのネットワーク関連イベントのリストが表示されます。イベントを選択すると、特定のアプリケーション、デバイス、その他の基準 （宛先 IP アドレス、ポートなど）で生成されたネットワーク イベントに関する詳細が表示されます。

[Service （サービス）] フィールドには、ネットワーク接続を確立したプロトコルとポートが表示されます。

アプリケーション名をクリックすると、そのアプリケーションに関連するすべてのイベントを表示できます。またデバイス名をクリックすると、そのデバイスに関連するすべてのイベントを表示できます。

詳細については、イベントの左側にある **[>]** をクリックします。

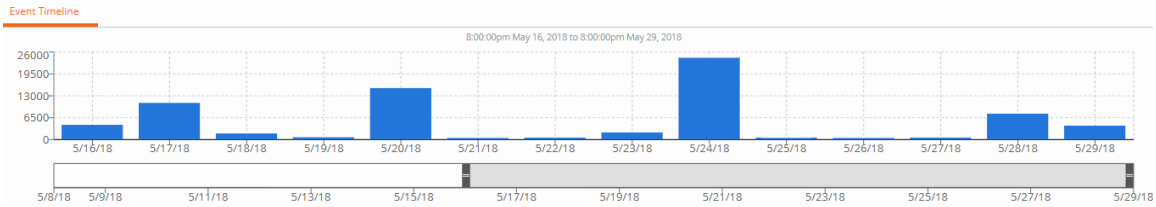
[Investigate （調査）] ページのサブタブの使用

このセクションでは、[Investigate （調査）] ページで使用可能な各種のサブタブについて説明します。使用可能なサブタブは、フィルター オプションや調査するイベントの特性によって異なります。

ヒント：どのサブタブからでも、[Alert Triage （アラートのトリアージ）] アイコンをクリックして、[Alert Triage （アラートのトリアージ）] ページに移動できます。

ライムラインの表示

[Time Line （タイムライン）] サブタブは、すべてのタブで常に表示されます。イベントが発生したタイムラインを表示するには、[Time Line （タイムライン）] サブタブをクリックします。



[Time Line （タイムライン）] サブタブには、特定のスナップショットのイベントの詳細を時間ごとに表示できる対話型タイムラインが表示されます。

グラフの青色の棒は、イベントが発生した日付を示します。タイム ラインにカーソルを合わせると、その時点に発生したイベントの数が表示されます。

時間の区分は、さらに絞り込むことができます。灰色のタイムライン バーを左右にスライドすると、対象とする時間の区分のアラートの詳細が表示されます。検索結果テーブルは、選択内容に応じて更新されます。

注意

タイムラインは、ブラウザーのローカル タイムゾーンに基づきます。これは、個々のエンドポイントおよびイベントのタイムゾーンとは異なる場合があります。

[Device （デバイス）] サブタブの表示

選択したイベントに関連するデバイスの情報を表示するには、[Device （デバイス）] サブタブをクリックします。

[Take Action （アクション実行）] 下向き矢印をクリックすると、デバイスに対して次のいずれかのアクションを実行できます。

- バックグラウンド スキャンを有効または無効にする。
- バイパスを有効または無効にする。
- ホストを隔離する、または隔離を解除する。隔離されている間、ホストは Cb Defense とのみ通信できます。センサーは、デバイスが隔離されていることを示す通知を Cb Defense から受け取ります。
- センサーとの Live Response セッションを開始する。“Live Response の使用 ” を参照してください。

[App （アプリ）] サブタブの表示

選択したイベントに関連するアプリケーションの情報を表示するには、[Selected App（選択されたアプリ）]（または [Target App（ターゲット アプリ）] もしくは [Parent App（親アプリ）]）をクリックします。**ターゲット アプリ**は、**選択されたアプリ**が呼び出すアプリケーションです。**親アプリ**は、**選択されたアプリ**を呼び出したアプリケーションです。

[Signed By （署名者）] フィールドで、[Add （追加）] をクリックすると、この証明書を信頼済み公開者のリストに追加できます。

[Origin （発生元）] フィールドで [Show More （詳細を表示）] をクリックすると、アプリケーションの発生元に関する詳細情報が表示されます。またアプリケーション名をクリックすると、アプリケーション自体に関する詳細情報が表示されます。

[Product（製品）] フィールドには、アプリケーションが属する製品の名前が表示されます。たとえば、 `cmd.exe` は Windows オペレーティング システムに属します。

[Take Action （アクション実行）] 下向き矢印をクリックすると、次のアクションを実行できます。

- アプリケーションをホワイトリストまたはブラックリストに追加する。
- アプリケーション プロセスを終了する。
- アプリケーションのアップロードを要求する。アプリケーションは、分析のために受信ボックスにアップロードされます。“ 疑わしいファイルのアップロード ” を参照してください。
- VirusTotal で、さまざまなソースからのハッシュに関する最新情報を確認する。
- アプリケーションを削除する。アプリケーションはこのデバイスからのみ 1 回だけ削除されます。または、すべてのデバイスからアプリケーションを削除することもできます。

備考

削除するアプリケーションを正しく選択していることを確認してください。削除できるのは、選択されたアプリケーション、ターゲット アプリケーション、または親アプリケーションです。

すべてのデバイスからアプリケーションを削除すると、組織内のすべてのデバイスからアプリケーションが永久に削除されます。削除を取り消すことはできません。削除されたアプリケーションは受信ボックスで確認することができます。以下を参照してください。アプリケーションを削除する。アプリケーションはこのデバイスからのみ 1 回だけ削除されます。または、すべてのデバイスからアプリケーションを削除することもできます。

[Notes/Tags （メモ / タグ）] サブタブの表示

イベントにメモまたはタグが含まれている場合は、このタブに表示されます。ここでメモまたはタグを追加するには、対応するテキスト ボックスにメモまたはタグを入力し、**Enter** キーを押します。

[Alerts （アラート）] サブタブの表示

このタブには、選択したイベントと関連する TTP の理由が表示されます。アプリケーションを削除する。アプリケーションはこのデバイスからのみ 1 回だけ削除されます。または、すべてのデバイスからアプリケーションを削除することもできます。を参照してください。

このタブでは、アラート データを含む STIX ドキュメントを保存できます。

STIX ドキュメントを保存する :

1. 説明の右上隅にある [Share （共有）] をクリックします。
2. [Download a STIX document（STIX ドキュメントのダウンロード）] をクリックします。

第 8 章

インシデント対応

この章では、Cb Defense のインシデント対応について説明します。

Cb Defense では、次の方法で直接脅威に対応できます。

- エンドポイントをネットワークの他の部分から隔離できます。隔離されたエンドポイントは、Cb Defense バックエンドに対してのみネットワーク アクセスが可能です。
- 既知のマルウェアをエンドポイントから直接削除することができます。
- Live Response を使用すると、エンドポイント上でプロセスを終了し、その他のファイルの削除や必要な修復を行うことができます。

デバイスの隔離

Cb Defense でエンドポイントを隔離するには、次の 3 つの方法があります。

- [Investigate （調査）] ページを使用する。“[Device （デバイス）] サブタブの表示 ” を参照してください。
- [Alert Triage（アラートのトリアージ）] ページを使用する。“ アラートの視覚的表示 ” を参照してください。
- [Endpoints （エンドポイント）] ページを使用する。ここでは、この方法について説明します。

[Endpoints （エンドポイント）] ページでデバイスを隔離する :

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. 隔離するデバイスを選択します。（“ 展開したセンサーの表示 ” を参照）。
3. [Take Action （アクション実行）] メニューをクリックし、[Quarantine devices （デバイスの隔離）] をクリックします。アクションを確認するように求められます。[Yes （はい）] をクリックします。

エンドポイントが実際に隔離されるまでには、数分かかる場合があります。エンドポイントのセンサーがチェックインすると、Cb Defense バックエンドは、エンドポイントを隔離するようセンサーに指示します。隔離されたエンドポイントは、隔離状態を解除するまで隔離されたままとなります。

エンドポイントを隔離したら、修復手順を開始できます。修復が完了したら、隔離したエンドポイントへの接続を回復するために、上記の手順を実行し、[Take Action（アクション実行）] メニューから [Unquarantine devices （デバイスの隔離を解除）] をクリックします。

マルウェアの削除

Cb Defense 管理コンソールを使用してエンドポイントからマルウェアを削除することができます。

Cb Defense によってマルウェアの実行が防がれても、マルウェアがエンドポイントに存在している場合があります。

[Malware Removal （マルウェアの削除）] ページでは、組織内のすべてのマルウェア ファイルを表示して削除することができます。このページには、過去 6 か月間に収集されたこれまでのマルウェアのデータが表示されます。このデータは、取り込まれるまでに数日間かかることもあります。

マルウェアを削除すると、ハッシュが一括削除されます。1 つのアクションを開始することで、組織全体のマルウェアを削除できます。

既知のマルウェアの自動削除

指定した時間枠 （1 日、1 週間、2 収監、1 か月のいずれか）で既知のマルウェアを自動削除するポリシー設定を有効にすることができます。“[Cb Defense Settings （Cb Defense 設定）] タブ ” を参照してください。

ポリシー設定と時間枠を構成すると、時間枠の終了時に新しいマルウェアが削除されます。削除されるのは、実行可能なマルウェアのみです。

注意 : 既知のマルウェアが自動的に削除されないように、ホワイトリストに登録することができます。

マルウェアが削除されると、その参照が [Detected（検出済み）] ページから [Deleted（削除済み）] ページに移動します。検出されたマルウェアは、監査ログにも記録されます。

以下のファイルは自動削除されません。

- Microsoft によって署名されたファイル
- Carbon Black ファイル
- ハッシュが変更されたファイル

警告

削除されたファイルは復元できません。ファイルは恒久的に削除されます。

検出済みのマルウェア

検出済みのマルウェアについては、[Malware Removal （マルウェアの削除）] ページに次の情報が表示されます。

表 16: 検出済みのマルウェア

項目	説明
ハッシュ	マルウェア ファイルのハッシュ。ハッシュの最初と最後の 5 文字のみ表示されます。ハイライト表示してから右クリックすると、ハッシュをコピーすることができます。ハッシュをクリックすると、その項目の [Investigate （調査）] ページを開くことができます。“ アラートの調査 ” を参照してください。
File （ファイル）	マルウェアのファイル名。
Device （デバイス）	マルウェアが検出されたエンドポイント。
ポリシー	デバイスが割り当てられているポリシー。
First Seen （最初の認識日時）	マルウェアが最初に検出された日時。
Last Deleted （最終削除日時）	マルウェアがこのエンドポイントから削除された最終日時。
Auto Delete in （自動削除までの日数）	自動削除が有効な場合に、マルウェアが削除されるまでの残りの日数。

ページ上部の [Search （検索）] テキスト ボックスを使用すると、特定のマルウェアを検索することができます。項目のリストは、次の列で並べ替えることができます。

- [Hash （ハッシュ）]
- ファイル
- Device （デバイス）
- First Seen （最初の認識日時）

マルウェアに対して、次のアクションを実行できます。

- [Investigate （調査）] アイコンをクリックして、[Investigate （調査）] ページを開きます。詳細については、“ アラートの調査 ” を参照してください。
- マルウェアの横にある下向き矢印をクリックすると、次のアクションを実行できます。
  - ファイルをホワイトリストに追加する。
  - ファイルをブラックリストに追加する。
  - ファイルのアップロードを要求する。
  - VirusTotal でマルウェアを検索する。
  - アプリケーションを削除する。

アプリケーションを削除する場合、アクションを確認する必要があります。

マルウェアを現在のデバイスからのみ削除することも、すべてのデバイスから削除することもできます。

既知のマルウェア以外のレピュテーションを持つファイルを削除する場合、削除を 2 回確認する必要があります。

ホワイトリストとブラックリストの詳細については、“ レピュテーションの管理 ” を参照してください。

削除済みのマルウェア

削除済みのマルウェアについては、[Malware Removal （マルウェアの削除）] ページに次の情報が表示されます。

表 17: 削除済みのマルウェア

項目	説明
ハッシュ	マルウェア ファイルのハッシュ。ハッシュの最初と最後の 5 文字のみ表示されます。ハイライト表示してから右クリックすると、ハッシュをコピーすることができます。ハッシュをクリックすると、その項目の [Investigate （調査）] ページを開くことができます。“ アラートの調査 ” を参照してください。
File （ファイル）	マルウェアのファイル名。
Device （デバイス）	マルウェアが検出されたデバイス。
ポリシー	デバイスが割り当てられているポリシー。
First Seen （最初の認識日時）	マルウェアが最初に検出された日時。
Last Delete Requested （最後に削除を要求した日時）	削除要求がセンサーに送信された日時。
Status （ステータス）	削除のステータス。ステータスは、次のいずれかです。 • 検出済み - マルウェアがデバイスに存在しています。 • 削除保留中 - 削除要求が送信され、デバイスで削除が実行されるのを待機しています。 • 削除済み - 削除が実行されたことがデバイスから報告されました。

Live Response の使用

Cb Defense センサー バージョン 3.0 以降が動作しているエンドポイントが接続されている場合、Cb Defense Live Response は、そのエンドポイントに対するコマンド ライン インターフェイスを開きます。センサーには、Live Response が有効であるポリシーを割り当てる必要があります。Live Response を使用すると、リモートで調査を実行し、継続中の攻撃を封じ込め、脅威を修復できます。たとえば、Live Response では、ディレクトリ内容の確認、プロセスの強制終了、センサー管理対象コンピューターからのファイルの取得などの操作を実行できます。

注意

Live Response 機能を使用する場合は、ユーザーのコンピューターおよびファイルにアクセスする際に組織のポリシーに準拠する必要があります。

Cb Defense Live Response は、API を介してプログラムで使用できます。詳細については、次を参照してください。
https://developer.carbonblack.com/

Live Response を使用するには、Live Response 管理者でなければなりません。“ ユーザーの管理 ” を参照してください。

Live Response は、デフォルトでは無効になっています。

ポリシーに対して Live Response を有効にする :

1. PSC にログインし、[Enforce （適用）] をクリックして [Policies （ポリシー）] をクリックします。
2. Live Response を有効にするセンサーを含むポリシーを選択します。
3. [Cb Defense Settings （Cb Defense 設定）] パネルで [Enable Live Response （Live Response の有効化）] を選択します。
4. [Save （保存）] をクリックします。

ポリシーに対して Live Response を有効にした後、このポリシーの一部のエンドポイントに対して Live Response を無効にすることができます。

注意

下記の方法で Live Response を無効にした場合は、エンドポイントにセンサーを再展開し、それらのエンドポイントに対して Live Response を再び有効にする必要があります。

（ポリシーごとではなく）一部のエンドポイントに対して Live Response を無効にする :

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. Live Response を無効にするセンサーを選択します。“展開したセンサーの表示” を参照してください。
3. [Take Action （アクション実行）] メニューで [Disable Live Response （Live Response の無効化）] をクリックします。このアクションには、確認が必要です。

`DISABLE_LIVE_RESPONSE` パラメーターを使用すると、無人インストール時にセンサーに対して Live Response を無効にすることもできます。詳細については、『PSC センサー インストール ガイド』を参照してください。

Live Response の使用

特定のエンドポイントに対して Live Response を起動する場合は、" セッション " を作成してそのセッションにアタッチします。セッションのインターフェイスには、エンドポイントに関する情報と、そのエンドポイントを操作するためのコマンド ウィンドウがあります。

最大 100 個のセッションを同時に実行できます。また、複数のユーザーを同じセッションにアタッチすることもできます。2 人以上のユーザーがほぼ同時に特定のセッション経由でコマンドを送信した場合は、1 つのコマンドの実行が終了してから次のコマンドが開始されます。他のユーザーが実行している処理を取り消したり変更したりすることもできます。各セッションのコマンド数は 250 個に制限されています。

Live Response セッションを開始するには、次の 4 つの方法があります。

- **アラート リスト** ページを使用する。“ デバイス詳細の表示 ” を参照してください。
- [Alert Triage（アラートのトリアージ）] ページを使用する。“ アラートの視覚的表示 ” を参照してください。
- [Investigate （調査）] ページを使用する。“[Device （デバイス）] サブタブの表示 ” を参照してください。
- [Endpoints （エンドポイント）] ページを使用する。ここでは、この方法について説明します。

Live Response セッションを開始するには :

1. PSC にログインし、[Endpoints （エンドポイント）] をクリックします。
2. Live Response セッションを開始するセンサーの [Investigate（調査）] アイコンの横にあるコマンド プロンプト アイコンをクリックします。

注意 : セッションを開始できるのは、3.0 以降のセンサーで、Live Response がポリシーによって有効になっており、過去 10 分以内にチェックインしたものに限られます。

[Live Response] コンソールが開き、左側にコマンド ウィンドウ、右側に情報パネルが表示されます。コマンド ウィンドウのプロンプトには、Live Response がアクティブになっているデバイス ID と現在のディレクトリが表示されます。

コマンド ウィンドウには、ステータス インジケーターとメッセージが表示されます。ステータス インジケーターでは、次の色コードが使用されます。

- 緑 – センサーが接続されており、セッションが確立されています。エンドポイントのホスト名が表示されます。
- 黄 - Cb Defense バックエンドがセンサーのチェックインを待機しているか、アタッチされているセッションがないのでエンドポイントが接続されていません。
- 赤 - センサーとのセッションを確立できません。原因は、エンドポイントがオフラインであるか、センサーが無効になっているか、センサーのバージョンで Live Response がサポートされていないためです。

使用できるコマンドの一覧を表示するには、コマンド ウィンドウの中をクリックして `help` コマンドを入力します。特定のコマンドに関するヘルプを表示するには、`help commandname` と入力します。

[Information （情報）] パネルに次の情報が表示されます。

- エンドポイントの名前。
- センサーが属しているポリシー。

- オペレーティング システム。
- センサーのバージョン。
- デバイスのターゲットバリュー。
- 内部 IP アドレスと外部 IP アドレス。
- センサーの最終チェックインの日時。
- コマンド インターフェイスで入力できるコマンドの一覧。
- 過去 24 時間以内にデバイスで発生したアラート アクティビティ。

[Information （情報）] パネルは、縮小したり、展開したりできます。

Live Response コマンドの一覧については、表 18、「Live Response セッションのコマンド」を参照してください。この表の説明では、" リモート ホスト " は Live Response を通じてアクセスされるエンドポイントを指しています。" ローカル ホスト " は、ユーザーが Cb Defense コンソールにアクセスしているホストを指しています。これらのコマンドはすべて SYSTEM コンテキストで実行されます。

注意

コマンドとオプションは、ここで説明する方法に従って使用してください。DOS コマンド インターフェイスのコマンドと同じ Live Response コマンドもありますが、オプションは Live Response 固有のものです。

表 18: Live Response セッションのコマンド

コマンド	説明
cd [dir]	現在の作業ディレクトリを別のディレクトリに変更します。絶対パス、相対パス、ドライブ固有のパス、またはネットワーク共有パスで指定できます。
clear	コンソール画面を消去します。`cls` コマンドを使用しても同じ操作が可能です。
delete [path]	path 引数で指定されたファイルを削除します。このファイルは恒久的に削除され、ごみ箱には送られません。
detach	現在の Live Response セッションから切り離します。アタッチされていないセッションは、タイムアウトになるまでライブな状態を維持します。デフォルトのタイムアウトは 5 分です。
dir	現在のディレクトリ内のファイルの一覧を表示します。
drives	リモート ホスト上のドライブの一覧を表示します。このコマンドは Windows 専用です。

コマンド	説明

exec [processpath]	現在のリモート ホスト上で processpath 引数で指定されたプロセスをバックグラウンドで実行します。デフォルトでは、プロセスは直ちに実行され、実行結果は標準出力 （stdout）と標準エラー出力 （stderr）に送られます。
	次のようにオプションを組み合わせて使用できます。
	• exec `-o outputfile processpath` – プロセス出力を指定のリモート ファイルにリダイレクトします。リダイレクトしたファイルはダウンロードできます。
	• exec `-w processpath` – プロセスの終了を待機したうえで戻ります。
	次の例のようにオプションを組み合わせて実行し、スクリプトの出力を捕捉できます。
	exec `-o c:\output.txt -w`
	`c:\scripts\some_script.cmd`
	processpath 引数にはプロセスへの完全なパスを指定する必要があります。以下に例を示します。
	`c:\windows\system32\notepad.exe`

get [path]	path 引数で指定されたファイルをリモート ホストから取得し、ローカル ホストにダウンロードします。
help	Live Response セッションの各コマンドが簡単な説明とともに一覧表示されます。コマンド名を追加すると、その指定したコマンドの説明が表示され、オプションなどの詳しい説明があれば、それも表示されます。以下に例を示します。 `help dir`
kill	指定されたプロセスを終了します。
memdump [filepath]	全体のメモリ ダンプを取得し、指定されたファイル パスに保存します。このファイル パスではファイル名も指定する必要があります。 メモリのダンプには数分を要することがあります。その間は、Live Response のウィンドウに （*）アイコンが表示されています。 このコマンドは Windows 専用です。
mkdir	リモート ホスト上にディレクトリを作成します。
ps または tasklist	リモート ホストからプロセスの一覧を取得します。 このコマンドの出力には、各プロセスの記述に [Analyze（分析）] リンクがあります。このリンクをクリックすると、そのプロセスの [Process Analysis （プロセス解析）] ページが開きます。 新たに検出されたプロセスの解析情報は、まだ完全には Cb Defense データベースにコミットされていないことがあり、その場合は表示されません。 このリンクをクリックすると、Live Response コンソールから移動することになるので、そのコンテキストは失われます。

コマンド	説明
put [remotepath]	ローカル ホストにあるファイルを、指定されたパスのリモート ホストに配置します。このコマンドを Live Response で入力した後、ブラウザーの [Open（開く）] ダイアログで目的のファイルを指定します。
pwd	現在の作業ディレクトリを出力します。
reg	Windows のレジストリ設定を表示または変更します（Windows エンドポイントのみ）。このコマンドの構文は次のとおりです。 reg *[action] [key] [options]* 詳細については、Live Response のコマンド ウィンドウで `help reg` を使用してください。 表 19、「Live Response のレジストリ （reg）コマンドのアクション」を参照してください。

Windows センサーの Live Response セッションでは、`reg` コマンドを使用してリモート コンピューターの Windows レジストリに直接アクセスできます。

`reg` コマンドのアクションとそのオプションを表 19、「Live Response のレジストリ（reg）コマンドのアクション」に示します。これらのオプションは、Windows でデフォルトの `reg.exe` コマンドと同じ構文を使用できるようにすることを意図したものです。

どの `reg` コマンドのアクションでも、そのキーで参照するハイブ （Hive）は短い形式と長い形式のどちらでも使用できます （例 : HKLM または `HKEY_LOCAL_MACHINE`）。キー パスに空白が含まれている場合、"`HKLM\SOFTWARE\VMware, Inc.`" のように、キー パス全体を引用符で囲む必要があります。

表 19: Live Response のレジストリ （reg）コマンドのアクション

[Action （アクション）]	説明

query	形式 : reg query [key] [options]
	オプション :
	-v - キーではなく値に対するクエリを実行します。
	例 :
	`reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
	`reg query -v HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SecurityHealth`

add	形式 : reg add [key] 例 : `reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
set	形式 : reg set *[key] [options]* オプション : -t – 追加するキーのタイプ。次の各タイプを指定できます。 • `REG_BINARY` • `REG_SZ` • `REG_EXPAND_SZ` • `REG_MULTI_SZ` • `REG_DWORD` • `REG_DWORD_BIG_ENDIAN` • `REG_QWORD` -d – データ 例 : `reg set HKLM\Software\Microsoft\Windows\CurrentVersion\Run -t REG_SZ -d c:\windows\system32\calc.exe`
delete	形式 : reg delete [key] [options] オプション : -v – キーではなく指定された値を削除します。 例 : `reg delete HKLM\Software\Microsoft\Windows\CurrentVersion\ -v Run`

情報を提供するコマンドもあれば、エンドポイントを変更できるコマンドもあります。情報コマンドをいくつか実行し、このインターフェイスに慣れてからエンドポイントの変更作業に入ることをお勧めします。

接続やコマンドにエラーや問題があるとステータス メッセージやエラー メッセージが表示されます。コマンドまたは `pwd` コマンドを使用して、接続を確認することもできます。

Live Response セッションを終了する：

1. Live Response コマンド ウィンドウで `detach -q` コマンドを入力するか、Live Response コンソールで [End my Session （セッションの終了）] ボタンをクリックします。セッションが終了し、センサーから切断されたというメッセージが表示されます。

   また、アクティビティが発生しない場合はセッションがタイムアウトになります。タイムアウト値は 5 分です。

Live Response の拡張

Live Response には、エンドポイントにファイルを配置する `put` と、エンドポイント上でプロセスを実行する `exec` が組み込みコマンドとして用意されています。したがって、組み込みコマンドを超える範囲まで Live Response の機能を拡張できます。

たとえば、次のアクションを実行できます。

- 実行可能ファイルをアップロードし、メモリ上でカスタム シグネチャを検索する。
- `sbag.exe` をアップロードして、Shellbags アーティファクトでレジストリを解析する。
- カスタムの PowerShell スクリプトをアップロードして、 `powershell.exe` でそれを実行する。

アクティビティのログ記録とダウンロード

Live Response のアクティビティは、アクセスされるセンサーと Cb Defense バックエンドに記録されます。Live Response でアクセスするどのセンサーでも、セッションで実行されたコマンドは `cblr.log` ファイルに記録されます。このファイルは、エンドポイント上の Cb Defense センサーのインストール先フォルダーにあります。

Live Response のアクティビティは、Cb Defense の監査ログで確認できます。

監査ログを表示する：

1. PSC にログインし、[Settings （設定）] をクリックして [Audit Log （監査ログ）] をクリックします。

> **注意**
>
> Live Response セッションで実行されたすべてのコマンドを確認するには、監査ログの [Verbose（詳細）] 設定を [ON（オン）] にします。[Verbose（詳細）] を [OFF （オフ）] にすると、Live Response セッションの開始と終了のみがログに表示されます。

第 9 章

レピュテーションの管理

この章では、ホワイトリストとブラックリストを使用してレピュテーションを管理する方法について説明します。

レピュテーションは、オブジェクトに与えられた信頼または不信頼のレベルです。Cb Defense ファイルのレピュテーションは、既知の正常なオブジェクトと既知の不正なオブジェクトの複数のソースに基づいています。ハッシュ、IT ツール、および証明書に基づいてアプリケーションをホワイトリストまたはブラックリストに登録できます。

次の表に、可能なレピュテーション値とその定義を示します。

表 20: レピュテーション

値	定義
COMPANY_WHITE_LIST（会社のホワイトリスト）	一般に、組織に固有の通常とは異なる挙動がある場合、管理者はこのアプリケーションまたはハッシュを明示的にホワイトリストに載せています。
COMMON_WHITE_LIST（一般的な適応型ホワイトリスト）	分析後のハッシュ レピュテーションはすべての組織で信頼済みとして見なされます。
NOT_LISTED（リストにない）	センサーがバックエンドにレピュテーションを要求しましたが、バックエンドの内部リストにそのハッシュがありません。これは、通常、ハッシュが新しいことを意味します。Cb Defense 分析とインテリジェンス フィードからレピュテーションを判断するために利用できる情報はありません。このレピュテーションは、ゼロデイ マルウェアからの保護に役立ち、多くの場合、新しいハッシュ / 更新されたアプリケーションに割り当てられます。
UNKNOWN （未知）	センサーがレピュテーション要求をまだ送信していません。これは、通常、センサーが Cb Defense バックエンドに接続できないことを意味します。
COMPANY_BLACK_LIST（会社のブラックリスト）	お客様がブラックリストに手動でハッシュを追加した悪意のある挙動または保証されない挙動。選択した組織に固有。
KNOWN_MALWARE（既知のマルウェア）	レピュテーションは Cb Defense 分析とインテリジェンス フィードから判断されます。ハッシュは既知のマルウェアです。
SUSPECT_MALWARE（疑わしいマルウェア）	レピュテーションは Cb Defense 分析とインテリジェンス フィードから判断されます。アプリケーションまたはハッシュは疑わしいマルウェアです。
PUP （潜在的に迷惑なプログラム）	レピュテーションは Cb Defense 分析とインテリジェンス フィードから判断されます。アプリケーションまたはハッシュは、アドウェアやポップアップなどの PUP です。
TRUSTED_WHITE_LIST（信頼できるホワイトリスト）	レピュテーションは Cb Defense 分析とインテリジェンス フィードから判断されます。ハッシュは、Cb Defense クラウド /Cb Defense センサーによって判断された既知の正当なハッシュです。

注意

ハッシュをホワイトリストに明示的に載せると、そのハッシュが会社のホワイトリストに追加されるというメリットがあります。このことは、偽陽性と考えられるアラートに対処する際に、特に役立つ可能性があります。

Cb Defense アラートは、関係するファイルのレピュテーションおよび Cb Defense センサーがエンドポイントで確認した動作に基づいています。アラートを作成するアルゴリズムでは、信頼できるホワイトリストのレピュテーションと会社のホワイトリストのレピュテーションが区別されます。インジケーターとしては、悪意のある動作である可能性が低いとする、会社のホワイトリストのレピュテーションが優先されます。したがって、特定のアプリケーションを会社のホワイトリストに追加することで、不必要なアラートを排除したり、不必要なアラートの相対的な脅威レベルを下げたりするのに役立つ可能性があります。

レピュテーションに基づいたアプリケーションの表示

レピュテーションに基づいてアプリケーションを表示する :

1. PSC にログインし、[Enforce （適用）] をクリックして [Reputation （レピュテーション）] をクリックします。
2. 次のいずれかのリスト オプションをクリックして、ビューをフィルターします。
   a. [All（すべて）] - ブラックリスト / ホワイトリストのレピュテーションにかかわらず、すべてのアプリケーションを表示します。
   b. [Blacklist （ブラックリスト）] - ブラックリストに載っているアプリケーションをすべて表示します。
   c. [Whitelist （ホワイトリスト）] - ホワイトリストに載っているアプリケーションをすべて表示します。
3. **タイプ**でフィルターすることもできます。
   a. [All （すべて）] - すべてのタイプを表示します。
   b. [Hash （ハッシュ）] - ハッシュに基づくレピュテーションを表示します。
   c. [IT Tools （IT ツール）] - IT ツールに基づくレピュテーションを表示します。
   d. [Certs （証明書）] - 証明書に基づくレピュテーションを表示します。

[Investigate （調査）] ページからのレピュテーションの管理

[Investigate （調査）] **ページからレピュテーションを管理する：**

1. PSC にログインし、[Investigate （調査）] をクリックします。
2. [Search（検索）] フィールドに値を入力し、**Enter** キーを押してイベントを検索します。（“ 調査するイベントの検索 ” を参照）。
3. 検索結果テーブルでイベントを選択します。
4. [Selected Application （選択されたアプリケーション）]、[Target Application （ターゲット アプリケーション）] [Parent Application （親アプリケーション）] のいずれか適切なタブを選択し、**[Signed by （署名者）]** フィールドの横の **[Add （追加）]** ボタンをクリックします。

[Malware Removal （マルウェアの削除）] ページからのレピュテーションの管理

[Malware Removal （マルウェアの削除）] ページからレピュテーションを管理する：

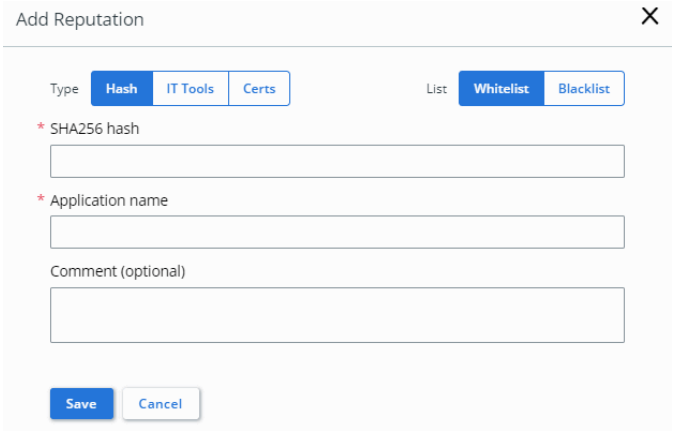
1. PSC にログインし、[Enforce （適用）] をクリックして [Malware Removal （マルウェアの削除）] をクリックします。
2. [Search（検索）] フィールドに値を入力し、**Enter** キーを押してイベントを検索します。
3. 検索結果テーブルで項目を選択します。
4. 項目の横にある下向き矢印をクリックし、[Add to Whitelist （ホワイトリストに追加）] または [Add to Blacklist （ブラックリストに追加）] をクリックします。

ハッシュに基づいたレピュテーションの管理

ハッシュに基づいてレピュテーションを管理する：

1. PSC にログインし、[Enforce （適用）] をクリックして [Reputation （レピュテーション）] をクリックします。
2. 右上隅の [Add （追加）] をクリックします。

3. [Add Reputation （レピュテーションの追加）] ダイアログで、タイプとして [Hash（ハッシュ）] を選択し、[Whitelist（ホワイトリスト）] または [Blacklist（ブラックリスト）] を選択して、ハッシュに基づいてアプリケーションをレピュテーション リストに追加します。



4. 必要なデータ （およびオプションのデータ）を入力し、[Save （保存）] をクリックします。

ホワイトリストへの IT ツールの登録

IT ツール機能を使用すると、既知の IT ツールによってドロップされるコードに高い初期信頼を割り当てることができます。IT ツールによってドロップされるプログラムおよびスクリプトが作成済みのルールに合致する場合、次の信頼処理が適用されます。

- 実行時に静的分析やクラウド レピュテーションのために中断することはありません。
- LOCAL_WHITE レピュテーションと初期信頼が割り当てられます。

この機能を使用して、IT ツールによってドロップされるコードに初期信頼を割り当てるメリットは次のとおりです。

- IT　ツールが即座に実行される新しいコードを大量にドロップするときに、認められるパフォーマンスへの影響が最小限に抑えられます。
- 新しいコードの実行が妨害されません。ドロップされるコードは、" 不明なコードをブロック " ポリシー ルールなどの厳格な予防ポリシー ルールが実施されている場合でもブロックされません。

このホワイトリスト機能の悪用を防止するため、IT ツールのホワイトリスト機能には一部制限があります。新しいコードの実行時にコードに対する分析が後からバックグラウンドで行われます。ファイルが Cb Defense にとって既知のマルウェアである場合、最初の実行後に構成済みのポリシー適用ルールがファイルに適用されます。これらのファイルは、多くの点で以前から存在するファイルとして扱われます。引き続きスキャンおよび分析の対象になりますが、初期信頼が設定されているため、センサーによって実行を妨げられることはありません。

次のレピュテーションは、IT ツールのホワイトリストよりも優先されます。

- 会社のホワイトリスト
- 会社のブラックリスト
- 信頼できるホワイトリスト

- 既知のマルウェア
- 疑わしいマルウェア
- PUP マルウェア

IT ツール機能のユース ケースとして以下が挙げられます。

- ソフトウェア展開 IT ツール - SCCM や Casper などの既知のインストーラー ツール。
- `*.msi` ファイルなど、プロセスがコード ドロッパーとして機能する一部の実行可能インストーラー。
- コンパイラー / リンカー、IDE、スクリプト エディター（vi や emacs など）などの開発者ツール。開発ツールを IT ツールとして扱うことで、既に実施されているポリシー ルールの適用に関する開発者エクスペリエンスが向上します。

IT ツールをホワイトリストに登録する :

1. PSC にログインし、[Enforce （適用）] をクリックして [Reputation （レピュテーション）] をクリックします。
2. 右上隅の [Add （追加）] をクリックします。
3. [Add Reputation（レピュテーションの追加）] ダイアログで、タイプとして [IT Tools（IT ツール）] を選択します。右上隅の [Whitelist （ホワイトリスト）] がデフォルトで選択されています。
4. [Path（パス）] フィールドを追加します。コードをドロップし、初期信頼が適用され、実行が許可される IT ツールのパスを入力します。例: `**\Trusted_Installer.exe`。

   注意 : IT ツールのパスを指定する際は、ドライブ文字と次の表に示すワイルドカードを使用できます。UNC パスがサポートされています。

表 21: ワイルドカード

ワイルドカード	説明	例

*	1 つのサブディレクトリ レベルまで 0 文字以上の連続する文字に一致します。	`C:\program files*\custom application\*.exe`
		次のディレクトリ内のすべての実行可能ファイルがホワイトリストに登録されます。
		`c:\program files\custom application\`
		`c:\program files?x86?\custom application\`

**	すべてのサブディレクトリ レベルでパスに部分一致し、再帰的です。	`C:\Python27\Lib\site-packages\**` そのディレクトリとすべてのサブディレクトリ内のすべてのファイルがホワイトリストに登録されます。
?	その位置の 0 または 1 文字と一致します。	`C:\Program Files\Microsoft Visual Studio 1?.0\**` MS Visual Studio のバージョン 1 またはバージョン 10 ～ 19 のすべてのファイルがホワイトリストに登録されます。

5. [Include all child processes （すべての子プロセスを含める）] - オンにした場合、[Path （パス）] フィールドで定義されている IT ツールの子プロセスによってドロップされるファイルにも初期信頼が適用されます。この機能は、IT ツールが子プロセスを生成して処理を委任し、子プロセスがコピーなどの汎用的な実行可能コマンドを表す場合に便利です。このルールを使用すると、子のコピー コマンドを （このプロセス内でのみ）一時的に IT ツールとして扱って IT ツールの信頼チェーンを維持できます。子プロセスがコピーなどの汎用的な実行可能コマンドでなく、IT ツールのユース ケースに適合する場合は、このオプションをオンにする代わりにそのコマンド用の IT ツール ルールを別に作成できます。
6. [Comment （コメント）] - ユーザーがこの変更の理由を確認するときに役立つコメントを入力します。これは追跡目的にのみ使用されます。
7. [Add （追加）] をクリックして変更内容を保存します。

ホワイトリストへの証明書の登録

証明書機能を使用すると、特定の信頼証明書によって署名されたコードに高い初期信頼を割り当てることができます。署名付きのプログラムおよびスクリプトが作成済みのルールに合致する場合、次の信頼処理が適用されます。

- 実行時に静的分析やクラウド レピュテーションのために中断することはありません。
- LOCAL_WHITE レピュテーションと初期信頼が割り当てられます。

この機能を使用するメリットは、ファイルが信頼されている IT ツールによって作成された場合と同じです。

- パフォーマンスへの影響が最小限に抑えられます。
- 特定の証明書によって署名されたファイルの最初の実行がブロックされません。

ホワイトリストは絶対的なものではなく、後から分析が行われます。信頼証明書によって署名されたファイルが既知のマルウェアで、ブロック ポリシーが構成されている場合、ファイルが実行されると後で中断され、ブロックされます。

次のレピュテーションは、証明書のホワイトリストよりも優先されます。

- 会社のホワイトリスト
- 会社のブラックリスト
- 信頼できるホワイトリスト
- 既知のマルウェア
- 疑わしいマルウェア
- PUP マルウェア

証明書機能のユース ケースとして以下が挙げられます。

- オペレーティング システム ファイル。Microsoft や Apple によって署名されたファイルなどが該当します。これらのファイルには初期信頼が適用されるため、オペレーティング システムのアップグレード中の影響が最小限に抑えられます。
- 組織内で使用され、特定の証明書によって署名されている優先ツール。

証明書機能を使用するための要件は次のとおりです。

- ファイルが有効な証明書によって署名され、検証されている必要があります。
- 証明書サブジェクトおよび認証局が証明書ルールに構成されている必要があります。

証明書をホワイトリストに登録する :

1. PSC にログインし、[Enforce （適用）] をクリックして [Reputation （レピュテーション）] をクリックします。
2. 右上隅の [Add （追加）] をクリックします。
3. [Add Reputation （レピュテーションの追加）] ダイアログで、タイプとして [Certs （証明書）] を選択します。右上隅の [Whitelist （ホワイトリスト）] がデフォルトで選択されています。
4. [Signed by （署名者）] - 対応する証明書サブジェクトを入力します。"*" ワイルドカード文字を使用できます。たとえば、「My Company Inc.」または「My Company*”」と入力します。

   警告 : 証明書をホワイトリストに登録する際は、できるだけ具体的に指定することをお勧めします。ワイルドカードを使用すると、信頼できる認証局によって署名されていると見せかけている悪意のあるソフトウェアが実質的にホワイトリストに登録される可能性があります。
5. [Certificate Authority（認証局）] - 入力することを推奨しますが、必須ではありません。
6. [Comment （コメント）] - 管理者がこの変更の理由を確認するときに役立つコメントを入力します。これは追跡目的にのみ使用されます。
7. [Add （追加）] をクリックして変更内容を保存します。

ハッシュの追加による複数のアプリケーションのレピュテーションの管理

ハッシュを追加して複数のアプリケーションのレピュテーションを管理する :

1. PSC にログインし、[Enforce （適用）] をクリックして [Reputation （レピュテーション）] をクリックします。
2. [Upload （アップロード）] をクリックします。
3. [Upload Reputations （レピュテーションのアップロード）] ダイアログで、[File Format（ファイル形式）] を展開して使用可能な適切な `.csv` ファイル形式を表示します。[Select （選択）] をクリックして `.csv` ファイルを参照します。

4. [Upload （アップロード）] をクリックします。ファイルが正常にアップロードされると、左上隅に成功メッセージが表示されます。

注意

MD5 はサポートされていません。ハッシュは SHA256 形式で、6 つ以上のフィールドが必要です。空のフィールドがある場合は、次のように空のフィールドをコンマで指定します。

```
Field1, Field2,, Field4,, Field6
```

必須フィールドは次の順序で指定する必要があります。

```
list type, indicator type, indicator value, description,
application name
```

各フィールドの説明は次のとおりです。

リスト タイプ : 次のいずれかです。

- black_list
- white_list

インジケーター タイプ : インジケーター sha256

インジケーター値 : 実際のファイル ハッシュ （sha256 形式）

説明 : このエントリを説明するテキスト

アプリケーション名 : オプション

自動ブラックリストの構成

脅威レベルが指定したしきい値以上のアプリケーションを自動的にブラックリストに登録するよう Cb Defense を構成できます。

自動ブラックリストを構成する :

1. PSC にログインし、[Enforce （適用）] をクリックして [Reputation （レピュテーション）] をクリックします。
2. 右上隅の [Auto Blacklist （自動ブラックリスト）] をクリックします。
3. 脅威レベルのしきい値を設定します。定義した脅威レベル以上のアプリケーションはすべてブラックリストに追加されます。[Save （保存）] をクリックします。

第 10 章

ポリシーによる攻撃からの防御

この章では、定義済みポリシーに基づいて防御策を講じる方法について説明します。

Cb Defense では、防止策はポリシーでのルールの定義に基づきます。各センサーは、1 つのポリシーに割り当てられます。“ ポリシー割り当ての管理 ” を参照してください。

組み込みのポリシー

2017 年 10 月リリースの Cb Defense では、3 種類のポリシーが Cb Defense に組み込まれています。これらのポリシーは削除できませんが、設定を変更することはできます。これらのポリシーは、一般的なユース ケース用のテンプレートとして設計されています。これらのポリシーにはセンサーを割り当てられます。また新規作成したポリシーに、ポリシー設定を複製することができます。

標準ポリシー （Standard）

標準ポリシー（Standard）は、新しいセンサーに適用されるデフォルトのポリシーです。新規展開の開始点として推奨されます。

標準ポリシー （Standard）では、既知のマルウェアと疑わしいマルウェアがブロックされます。最も危険性の高い操作 （メモリ スクレイピングやコード インジェクション）を防止します。

組織で社内アプリケーションやカスタム アプリケーションを数多く使用している場合は、組織の環境に Cb Defense を展開しても、Carbon Black がこれらのアプリケーションのレピュテーションを取得することはありません。この場合、標準ポリシー（Standard）のルールによって、不必要なブロックや偽陽性が生じる可能性があります。これらのアプリケーションがシステム上重要な場合、標準ポリシー （Standard）のルールを確認し、組織のニーズに合わせて調整する必要があります。

監視対象ポリシー （Monitored）

監視対象ポリシー（Monitored）は、エンドポイントのみが監視されます。防御機能はありません。既知のマルウェアを含め、いかなるアクティビティもブロックされません。ただし、すべてのアプリケーション アクティビティが監視され、**ダッシュボード**にこれらのイベントが記録されるため、ポリシー ルールを実装する前に、すべてのアプリケーション アクティビティを評価できます。ローカル スキャンはデフォルトで無効になっています。

“ ダッシュボード ” を参照してください。

高度なポリシー （Advanced）

高度なポリシー （Advanced）は、標準ポリシー （Standard）の機能をベースとして、それを拡張したものです。多くの場合は偽陽性である、危険性の高い動作を防止します。このポリシーの設定には、Windows および macOS エンドポイントの Office アプリケーション設定も含まれています。また、システム ユーティリティの操作をブロックします。

新しいまたは高度なポリシー （Advanced）ルールを実装する場合は、段階的にロールアウトするアプローチをとることをお勧めします。たとえば、高度なポリシー（Advanced）をパイロット ユーザーのグループに割り当てることができます。その状態で正規のソフトウェアに対して偽陽性が検出されず、ブロックも行われなければ、実稼働環境のユーザーを高度なポリシー （Advanced）に追加することができます。または、1 つの高度なポリシー （Advanced）ルールを、ベータ版またはユーザー受入テスト （UAT）の全ユーザーに適用することができます。この新しいルールを追加しても正規のソフトウェアに対して偽陽性が検出されず、ブロックも行われなければ、引き続き同じ方法でより高度なルールを環境に導入していくことができます。高度なポリシー （Advanced）ルールは、高度な攻撃を阻止し、これらから防御します。

ポリシーおよびポリシー設定の表示

ポリシーを表示する：

1. PSC にログインし、[Enforce （適用）] をクリックして [Policies （ポリシー）] をクリックします。

   左側の [Policy（ポリシー）] パネルに、すべてのポリシーが、各ポリシーのセンサーの数と共に表示されます。

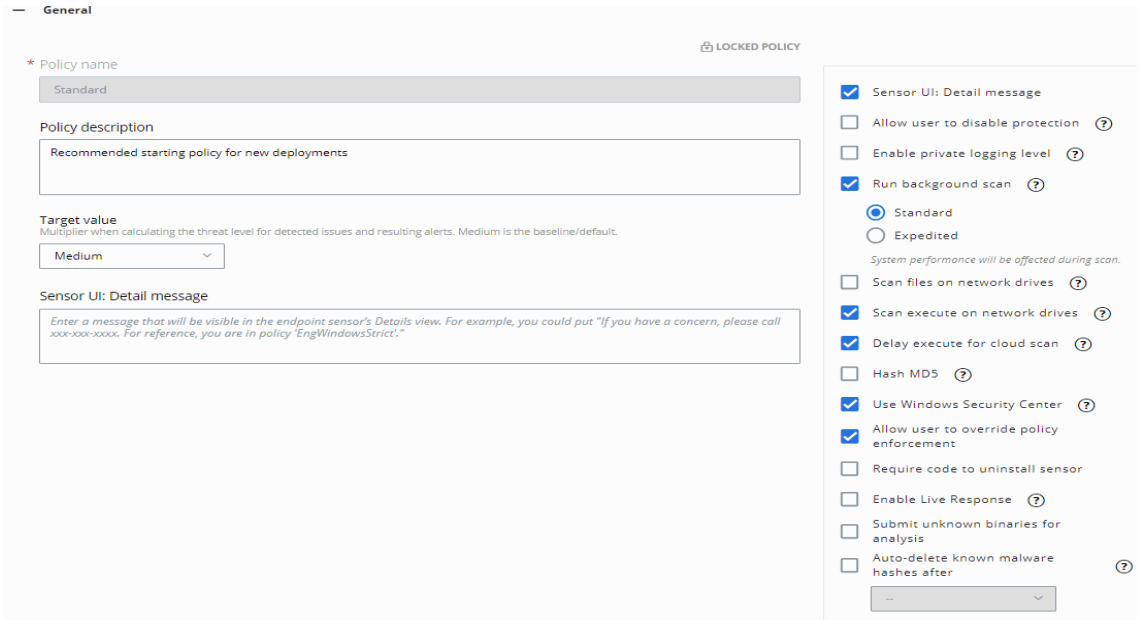
ポリシー設定を表示する：

1. 左側のパネルで、ポリシーをクリックして選択します。右側のパネルにポリシー設定が表示されます。

2 つのタブ（[Cb Defense Settings（Cb Defense 設定）] タブと [Local Scan Settings（ローカル スキャン設定）] タブ）があります。次のセクションでは、これらのタブについて説明します。

[Cb Defense Settings （Cb Defense 設定）] タブ

左側の [Policy （ポリシー）] パネルでポリシーを選択すると、そのポリシーに関連する設定が右側の [Cb Defense Settings （Cb Defense 設定）] タブに表示されます。



これらの設定を次の表に示します。

注意

このタブの [Blocking and Isolation （ブロックと隔離）]、[Permissions （権限）]、および [Uploads （アップロード）] パネルについては、“ 権限、ブロック、隔離に関するポリシー ルールの作成 ” を参照してください。

表 22: [Cb Defense Settings （Cb Defense 設定）] タブ

項目	説明
Policy Name （ポリシー名）	Policy Name （ポリシー名）
Policy 説明 （ポリシーの説明）	policy 説明 （ポリシーの説明）
[Target Value （ターゲットバリュー）]	このポリシーに関連付けられている、選択したターゲットバリュー。選択可能な値は、[Low （低）]、[Medium （中）]、[High （高）]、または [Mission Critical （ミッション クリティカル）] です。“ ターゲットバリュー （Target value）” を参照してください。

表 22: [Cb Defense Settings （Cb Defense 設定）] タブ

項目	説明
センサー UI: 詳細メッセージ	このオプションを選択して、エンドポイントでセンサー UI を表示します。センサーのポップアップ ダイアログに表示するメッセージを入力できます。mailto リンクがサポートされています。センサー UI で使用されるテキストの一部として HTML マークアップを入力できます。HTML ハイパーリンクを入力すると、リンクでプロトコル （HTTP など）が使用されます。 以下に例を示します。 `<a href="http://www.google.com">google</a>`
Allow user to disable protection（ユーザーによる保護の無効化を許可）	オンにした場合、Cb Defense センサーが [Protection （保護）] のオン / オフ切り替えボタン付きで表示され、エンド ユーザーがセンサーをバイパス モードに設定できるようになります。 このオプションは、[Show Sensor UI: Detail message （センサー UI を表示 : 詳細メッセージ）] がオンでない場合、灰色で表示されます。 この **保護** トグルは、単一ユーザー向けに設計されているオペレーティング システムのみで表示されます。ターミナル サーバーでは、**保護**トグルは表示されません。 この設定はバージョン 2.x 以降のセンサーにのみ適用されます。1.0.x センサーでは、ユーザーが保護を無効にできる機能は削除できません。
Enable private logging level（プライベート ログ レベルを有効化）	このオプションをオンにした場合、レピュテーションが不明なスクリプト ファイルはアップロードされません。また、アップロードされるイベントから潜在的な機密情報が削除されます。これには以下があります。 • 編集中のコマンドライン引数 • 曖昧なドキュメント ファイル名 • 関連するドメイン名に解決されない IP アドレス
Run background scan（バックグラウンド スキャンを実行）	オンにした場合、センサーは最初の 1 回限りのインベントリ スキャンをバックグラウンドで実行し、エンドポイント上の既存のマルウェア ファイルを特定します。この機能を使用すると、センサーをインストールするエンドポイント上に存在する既存のファイルをより効果的にマルウェアから保護できます。 標準バックグラウンド スキャンは、（エンドポイント上のファイルの数に応じて）完了までに 3 ～ 5 日間かかり、システム リソースの消費量が少ない低優先度モードで実行されます。このスキャンの使用が推奨されます。 高速スキャン オプションは、24 時間で完了します。テストや緊急事態でのみ推奨されます。これを使用した場合、システム パフォーマンスに影響が生じます。高速スキャンは、Windows センサー バージョン 3.3 以降にのみ適用できます。 センサーは、展開時にバックグラウンド スキャンを 1 回呼び出します。 現在のバックグラウンド スキャンの状態は、NT イベント ログまたは syslog に "BACKGROUND_SCAN" タグ付きで記録されます。

表 22: [Cb Defense Settings （Cb Defense 設定）] タブ

項目	説明
Scan files on network drives（ネットワーク ドライブ上のファイルをスキャン）	オンにした場合、センサーはネットワーク ドライブ上のファイルをファイルの読み取り時にスキャンします。この設定のデフォルト値はオフです。 最適なパフォーマンスを達成するには、この設定をオフにしてください。
Scan execute on network drives（ネットワーク ドライブ上の実行をスキャン）	オンにした場合、センサーはネットワーク ドライブ上のファイルをファイルの実行時にスキャンします。 この設定はバージョン 2.0 以降のセンサーにのみ適用されます。1.0 センサーは常にネットワーク ドライブを実行時にスキャンします。
Delay Execute for Cloud Scan （クラウド スキャンの実行を遅延）	このオプションでは、ローカル スキャンから不確定な結果が返された場合に、レピュテーション情報がバックエンドから取得できるようになるまで、Cb Defense が実行可能ファイルの起動を遅延するかどうかを指定します。これは推奨されている設定です。 この設定は Windows バージョン 2.0 以降のセンサーにのみ適用されます。
Create MD5 hash（MD5 ハッシュを作成）	MD5 ハッシュをログに記録するには、このオプションをオンにします。このオプションは、Cb Defense のセキュリティの有効性には影響しません。このオプションをオフにすると、Cb Defense は MD5 ハッシュをログに記録しません。最適なパフォーマンスを達成するには、この設定をオンにしないでください。 この設定はバージョン 2.0 以降のセンサーにのみ適用されます。1.0 センサーでは、常に MD5 ハッシュが作成されます。
Use Windows Security Center（Windows セキュリティ センターを使用）	Windows セキュリティ センターとともに Cb Defense をエンドポイントのウイルス対策ソフトウェアとして設定するには、このオプションをオンにします。“Windows セキュリティ センター統合の無効化または有効化 ” を参照してください。 この設定は Windows バージョン 2.10 以降のセンサーにのみ適用されます。
Require code to uninstall sensor（センサーのアンインストールにコードが必要）	センサーをエンドポイントからアンインストールするアクションをパスワードで保護するには、このオプションをオンにします。このオプションを有効にした場合、このポリシーに属するセンサーをアンインストールするには、登録取り消しコードを入力する必要があります。“ センサーのアンインストール ” を参照してください。 この設定はバージョン 3.1 以降のセンサーにのみ適用されます。
Enable Live Response（Live Response を有効にする）	このポリシーに対して Cb Defense Live Response を有効にするには、このオプションをオンにします。“Live Response の使用 ” を参照してください。 この設定はバージョン 3.0 以降のセンサーにのみ適用されます。

表 22: [Cb Defense Settings （Cb Defense 設定）] タブ

項目	説明
Submit unknown binaries for analysis （分析のための不明なバイナリの送信）	このオプションを選択すると、Carbon Black およびサードパーティが、不明なバイナリをクラウド分析用にアップロードできます。“ クラウド分析 ” を参照してください。 この設定はバージョン 3.2 以降のセンサーにのみ適用されます。
Auto-delete known malware after... （既知のマルウェアの自動削除を起動するまでの時間）	このオプションを有効にすると、指定した時間の経過後に、Cb Defense で既知のマルウェアが自動削除されます。“ マルウェアの削除 ” を参照してください。 この設定は、macOS センサー バージョン 3.2.2 以降、または Windows センサー バージョン 3.2.1 以降に適用されます。

[Local Scan Settings （ローカル スキャン設定）] タブ

[Local Scan Settings （ローカル スキャン設定）] タブをクリックすると、選択したポリシーに関連付けられたローカル スキャナー設定が表示されます。

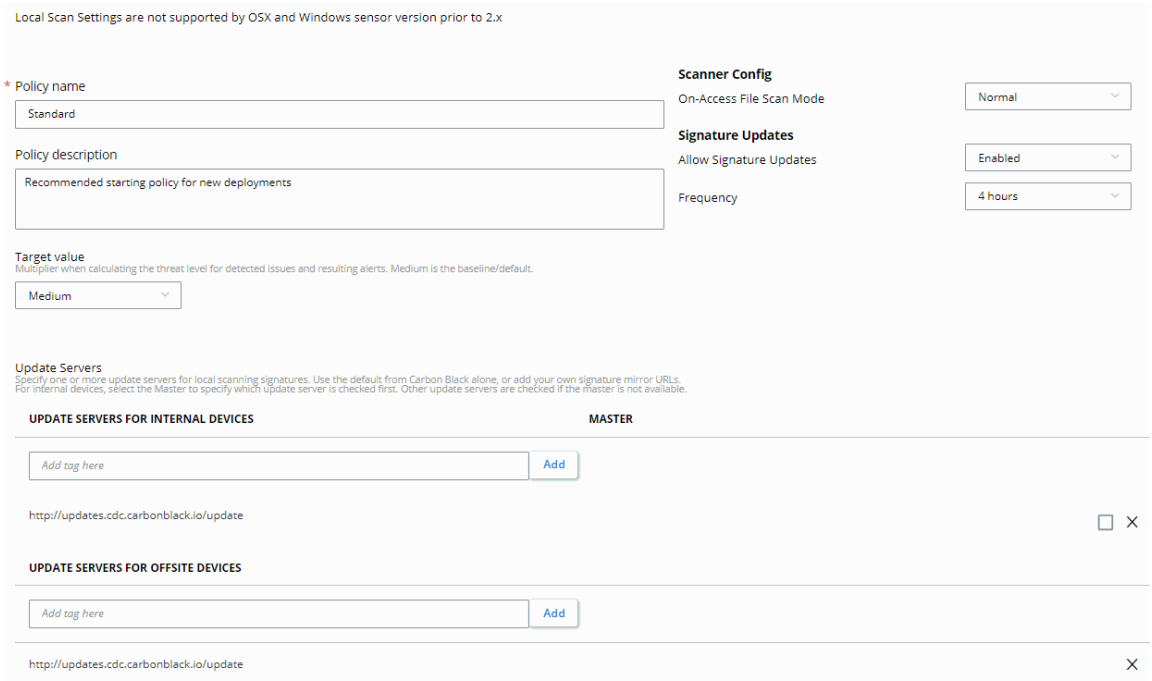


表 23: [Local Scan Settings （ローカル スキャン設定）] パネル

[Title （タイトル）]	説明
Policy Name （ポリシー名）	Policy Name （ポリシー名）
Policy 説明 （ポリシーの説明）	Policy 説明 （ポリシーの説明）。
[Target Value （ターゲットバリュー）]	このポリシーに関連付けられている、選択したターゲット バリュー。選択可能な値は、[Low （低）]、[Medium （中）]、[High （高）]、または [Mission Critical （ミッション クリティカル）] です。“ ターゲットバリュー （Target value）” を参照してください。
Scanner Config （スキャナーの構成）	[On-Access File Scan Mode （オンアクセス ファイル スキャン モード）]: • [Disabled （無効）] - ファイルのスキャンは実行されません。 • [Normal （標準）] - 新しいファイル （exe、dll、スクリプト）をそのファイルの最初の実行時 （ハッシュによって判断されます）にスキャンします。 • [Aggressive （積極的）] - すべてのファイルを実行時にスキャンします。割り当てられたレピュテーションとポリシー ルールが適用されます。
Signature Updates （シグネチャの更新）	[Allow Signature Updates （シグネチャの更新を許可）]: • [Enabled （有効）] - スキャナーのシグネチャの更新を有効にします。 • [Disabled （無効）] - スキャナーのシグネチャの更新を無効にします。 **[Update every…（… ごとに更新）]** - ローカル ファイルのスキャンの実行間隔を選択できます。
Update Servers for Internal Devices （内部デバイス用更新サーバー）	内部デバイス用の更新サーバーを追加できます。デフォルトのミラー インフラストラクチャ （http://updates.cdc.carbonblack.io/update） を使用することも、表示されるフィールドに独自のミラー デバイスの URL を入力することもできます。“ シグネチャ ミラーの手順 ” を参照してください。
Update Servers for Offsite Devices （オフサイト デバイス用の更新サーバー）	オフサイト デバイス用の更新サーバーを追加できます。デフォルトのミラー インフラストラクチャ （http://updates.cdc.carbonblack.io/update） を使用することも、表示されるフィールドに独自のミラー デバイスの URL を入力することもできます。“ シグネチャ ミラーの手順 ” を参照してください。

ポリシーの追加

新しいポリシーを追加する：

1. [New Policy （新規ポリシー）] をクリックします。
2. [Add Policy（ポリシーの追加）] ページで、必要な情報を入力して [Add （追加）] をクリックします。

権限、ブロック、隔離に関するポリシー ルールの作成

このセクションでは、権限またはブロック用のポリシー ルールを作成する方法について説明します。

注意

Cb Defense Windows Sensor バージョン 1.0.6.178 以降では、以下で説明するようにポリシー ルールでドライブ文字と ?、*、および ** 構文を使用できます。macOS は影響を受けません。

v.1.0.6.178 より前のバージョンの Windows Sensor では、C:\ 構文をボリュームの識別に使用してポリシー ルールを定義することはできません。使用できるのは C:\ を指定する **\ 構文だけです。

Windows Sensor v.1.0.6.178 以降では、C:\ を使用したポリシー ルールがサポートされます。**\ を使用するポリシー ルールは、サポートされるすべての Cb Defense Windows Sensor バージョンで引き続き機能します。そのため、古いポリシー ルールを作成し直して **\ を C:\ に修正する必要はありません。macOS は影響を受けません。

次の表に、可能なポリシー アクション値とその定義を示します。

表 24: ポリシー アクション

Value （値）	定義
TERMINATE （プロセスまたは脅威が終了）	ポリシー設定に従って、レピュテーションや行動に基づきプロセスを終了するアクション。
DENY （要求されたリソースを拒否）	ポリシー設定に従って、レピュテーションや行動に基づきリソースを拒否するアクション。

ポリシー作成に関するベスト プラクティス

- カスタム　ポリシーは、ホワイトリストおよびブラックリストに記載されたオブジェクト / ハッシュよりも優先されます。
- 実稼働環境に配置する前にポリシーをテストすることが重要です。1 つ以上のデバイスを含むテスト ポリシーを作成し、権限または除外をテストします。ルールを追加すると、そのポリシーが割り当てられているすべてのデバイスが影響を受けます。テスト ルールの検証が済んだら、そのルールを実稼働環境に配置します。
- 何か変化が起きないか注意します。これにより、問題が発生した場合にルールを取り消して追加のテストを行うことが容易になります。

ポリシー ルールでのワイルドカードの使用方法

アプリケーション パス ルールを使用すると、次のものにルールを柔軟に適用できます。

- 特定のアプリケーション パス。たとえば、`c:\Program Files\MyApp\myapp.exe` など。
- 特定のフォルダー内のすべてのファイル。たとえば、`c:\Program Files\MyApp\*` など。
- 特定のフォルダーおよびサブフォルダー内のすべてのファイル。たとえば、`c:\Program Files\MyApp\**` など。
- 特定のサブフォルダー内のすべてのファイル（上位フォルダーが不明な場合）。たとえば、`c:\Users\*\Desktop\build\**` と設定し、すべてのユーザー名を対象にする場合など。
- ワイルドカードで指定した、一連のフォルダー内のすべてのファイル。たとえば、`c:\Program Files\WindowsApps\Microsoft.WindowsStore*\**` など。

疑問符 （?）を 1 つのスペース文字を示すワイルド カードとして使用できます。

[Permissions （権限）] パネル

権限ルールを使用すると、動作の許可、動作の許可と記録、または Cb Defense による特定のパスの完全なバイパスを行うことができます。

たとえば、**" パス … のアプリケーションが … の操作を実行しようとした場合、バイパスする "** というルールでは、Cb Defense はそのパスでのすべての動作を棄却します。このバイパス ルールにより、このパスで処理される動作が一切認識されなくなるため、セキュリティ リスクが生じるおそれがあります。合致するパスから実行されるマルウェアはセンサーによって検出されず、Cb Defense バックエンドに記録されません。

ポリシー ルール （バイパス ルールを含む）では、UNC パスがサポートされます。

権限ルールを作成するケースとして次が挙げられます。

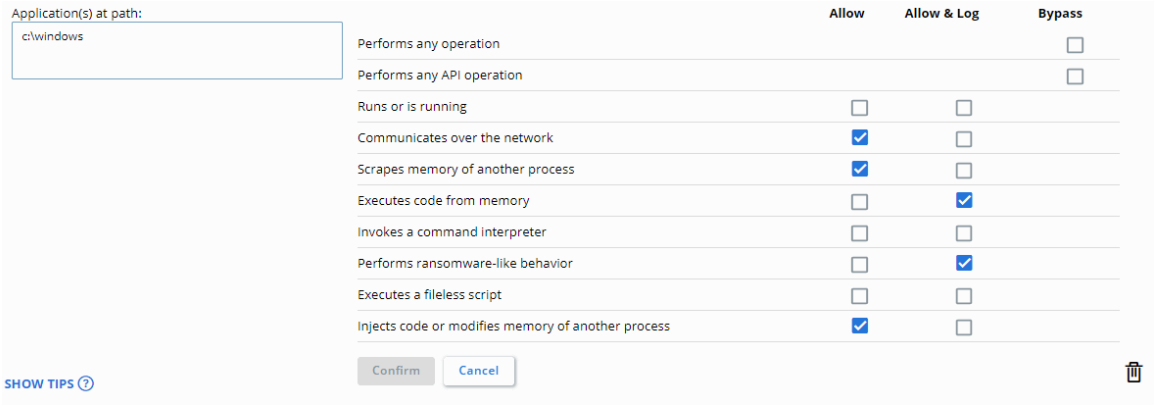
- その他の AV 製品やセキュリティ製品の例外の設定
- ソフトウェア開発者のワークステーションの障害除去

[Policy （ポリシー）] ページの左側にある [Policy （ポリシー）] パネルでポリシーを選択すると、そのポリシーに関連する権限が右側の [Permissions（権限）] パネルに表示されます。

権限ルールを作成または編集する：

1. 左側のパネルで、表示または編集するポリシーを選択します。
2. [Policy （ポリシー）] ページの右側のパネルで、[Cb Defense Settings （Cb Defense 設定）] タブをクリックし、[Permissions（権限）] の横にある矢印をクリックします。

3. [Add Application Path（アプリケーション パスの追加）] をクリックするか、既存のルールの隣にある鉛筆アイコンをクリックして編集します。



4. アプリケーション パスを入力します。複数のパスをコンマで区切って入力できます。
5. [Operation Attempt （操作の試行）] と目的の [Action （アクション）] を選択し、[Confirm （確認）] をクリックします。ごみ箱アイコンをクリックすると、ルールを削除できます。
6. ポリシーの変更が完了したら、[Save （保存）] をクリックします。

ポリシーから別のポリシーまたはすべてのポリシーにルールをコピーすることができます。“ ルールのコピー ” を参照してください。

注意

任意のルールの横にある [Investigate （調査）] アイコンをクリックすると、[Investigate （調査）] ページが開き、ルール プロパティに設定されている検索パラメーターが使用されます。“ アラートの調査 ” を参照してください。

次の表では、[Permissions （権限）] パネルについて説明します。

表 25: [Permissions （権限）] パネル

[Title （タイトル）]	説明
Process （プロセス）	権限ルールの最初の要素であるアプリケーションに関する説明が表示されます。アプリケーション パスを入力する必要があります。
Operation Attempt （操作の試行）	権限ルールの 2 番目の要素である操作に関する説明が表示されます。選択可能な値は次のとおりです。 • Performs any operation （なんらかの操作を実行） • Performs any API operation （なんらかの API 操作を実行） • Runs or is running （実行または実行中） • Communicates over the network （ネットワーク経由で通信） • Scrapes memory of another process （他のプロセスのメモリに対するスクレイピング） • Executes code from memory （メモリからコードを実行） • Invokes a command interpreter （コマンド インタープリターを起動） • Performs ransomware-like behavior （ランサムウェアのような振る舞いを実行） • Executes a fileless script （ファイルレス スクリプトを実行） • Injects code or modifies memory of another process （コードを挿入または他のプロセスのメモリを変更） 表 26、「各操作の概要」を参照してください。
[Action （アクション）]	[Application （アプリケーション）] と [Operation （操作）] の選択に基づいて実行されるアクションに関する説明が表示されます。選択可能な値は次のとおりです。 • [Allow （許可）] - 指定されたパスで、指定された動作を許可します。このパスでの指定された動作はログ記録されず、データが Cb Defense バックエンドに送信されることもありません。 • [Allow & Log （許可および記録）] - 指定されたパスで、指定された動作を許可します。すべてのアクティビティがログに記録され、Cb Defense バックエンドに報告されます。 • [Bypass （バイパス）] - このオプションは [Tries to perform any operation （なんらかの操作の実行を試行）] または [Tries to perform any API operation （なんらかの API 操作の実行を試行）] を選択した場合にのみ使用できます。センサーによって実行可能ファイルが監視されません。何もブロックされず、何もログに記録されません。アクティビティを一切参照できないため、このアクションは最後の手段として考える必要があります。

次の表では、各操作について説明します。

表 26: 各操作の概要

Operation Attempt（操作の試行）	説明
Performs any operation（なんらかの操作を実行）	この操作は [Runs or is running（実行または実行中）] に似ていますが、操作を実行しようとしている実行可能ファイルが Cb Defense によって監視される点が異なります。
Performs any API operation（なんらかの API 操作を実行）*	Cb Defense による防止が有効になっている場合、サードパーティ アプリケーションによっては、パフォーマンスの問題が発生することがあります。この場合、すべての API 操作をバイパスするように権限ルールを構成すると、そうしたサードパーティ アプリケーションとの相互運用性の問題に対処できます。この権限ルールでは、そうしたアプリケーションの実行が許可されますが、Cb Defense が次のポリシー レビューについて防止を強制しなくなります。 • Tries to scrape memory （メモリ スクレイピングを試行） • Tries to inject code （コード インジェクションを試行） • Tries to execute code from memory （メモリからのコードの実行を試行） • Master Boot Record protection for Performs ransomware-like behavior （ランサムウェアのような振る舞いの実行に対してマスター ブート レコードを保護）
Runs or is running（実行または実行中）	エンドポイントの初期スキャンが完了すると、デバイス上の各アプリケーションにレピュテーションが割り当てられます。Cb Defense によってすべての実行中のプロセスが確認され、指定されたルールに基づいてアプリケーションがシャットダウンされます。組み込みのロジックにより、重要なシステム（lsass など）のシャットダウンは防止されます。
Communicates over the network（ネットワーク経由で通信）	Cb Defense によって特定のアプリケーションに関連するすべてのネットワーク アクティビティにフラグが付けられます。
Scrapes memory of another process（他のプロセスのメモリに対するスクレイピング）	主なユース ケースは次のとおりです。 • Lsass を標的としたターゲット型メモリ スクレイピング。 • 複数のプロセスが列挙されており、これらのプロセスのメモリの読み取りが試みられている。 これはターゲット型の操作であるため、偽陽性の可能性はわずかです。通常、これは一律のルールとして使用できるため、適用された環境で偽陽性を受信する可能性が少なくなります。
Executes code from memory（メモリからコードを実行）	この操作はターゲット型ではないため、正しく使用しないと、偽陽性のフラグが付けられる危険性が高まります。関連する TTP は SUSPICIOUS_BEHAVIOR です。これは、動的メモリ（バッファ オーバーフローやアンパックされたコードなど）からコードを実行しているアプリケーションを検索します。ただし、この TTP は処理中のスクリプトにもフラグを付けます。たとえば、環境でマクロが使用されている場合、マクロにフラグが付けられます。

Operation Attempt（操作の試行）	説明
Invokes an untrusted process（信頼できないプロセスを起動）	レピュテーションを調べます。具体的には、ADAPTIVE_WHITE_APP、UNKNOWN_APP、DETECTED_SUSPECT_APP、DETECTED_PUP_APP、DETECTED_BLACKLIST_APP、および DETECTED_MALWARE_APP （およびこれに類似する値）です。ルールは選択したアクションに適用されます。
Invokes a command interpreter（コマンド インタープリターを起動）	シェル（コマンド ライン ツール）の呼び出しが試みられます。サポートされているコマンド インタープリターは次のとおりです。 • `cmd.exe` • `powershell.exe` • `wscript.exe/cscript.exe` • `wmic.exe` • `mshta.exe` • `sh?bash?dsch?zsh?tcsh?python?macOS?`
Performs ransomware-like behavior（ランサムウェアのような振る舞いを実行）	ランサムウェアのような振る舞いでは、次の状況を検出するためにシステム ストレージが監視されます。 • Cb Defense センサー以外のプロセスが、センサー所有の隠しファイルの変更を試みている。センサーが所有するいくつかのおとりファイルがファイルシステムのさまざまな場所に隠されています。これらのファイルは、ランサムウェアの興味を引くように設計されており、ランサムウェア攻撃の初期段階で暗号化されます。 • プロセスが Microsoft Windows オペレーティング システムのボリューム シャドウ コピー バックアップの操作を試行している。 • プロセスがシステムの起動ディスクのマスター ブート レコード（MBR）へのデータ書き込みを試行している。 この操作のルールに一致し、上記のいずれかの状況に合致したプロセスは終了され、このアクティビティを報告するアラートが生成されます。 “ ランサムウェア ” を参照してください。
Executes a fileless script（ファイルレス スクリプトを実行）	コマンド インタープリターが、スクリプト ファイルからの読み取りではなく、コマンド ラインへのスクリプトの入力に利用されているかどうかを特定します。
Injects code or modifies memory of another process（コードを挿入または他のプロセスのメモリを変更）	主なユース ケースは次のとおりです。 • Cb Defense では、通常はコード インジェクションを試みることがなく、問題がないことがわかっているアプリケーションのリストを管理しています。コード インジェクションを試みた場合、Cb Defense が対処します。 • あらゆる種類のターゲット型のプロセス ハロウイング。 Cb Defense では、これらの特定のアクションを防止するために、この 2 つのユース ケースに焦点を当てています。偽陽性の可能性はわずかです。

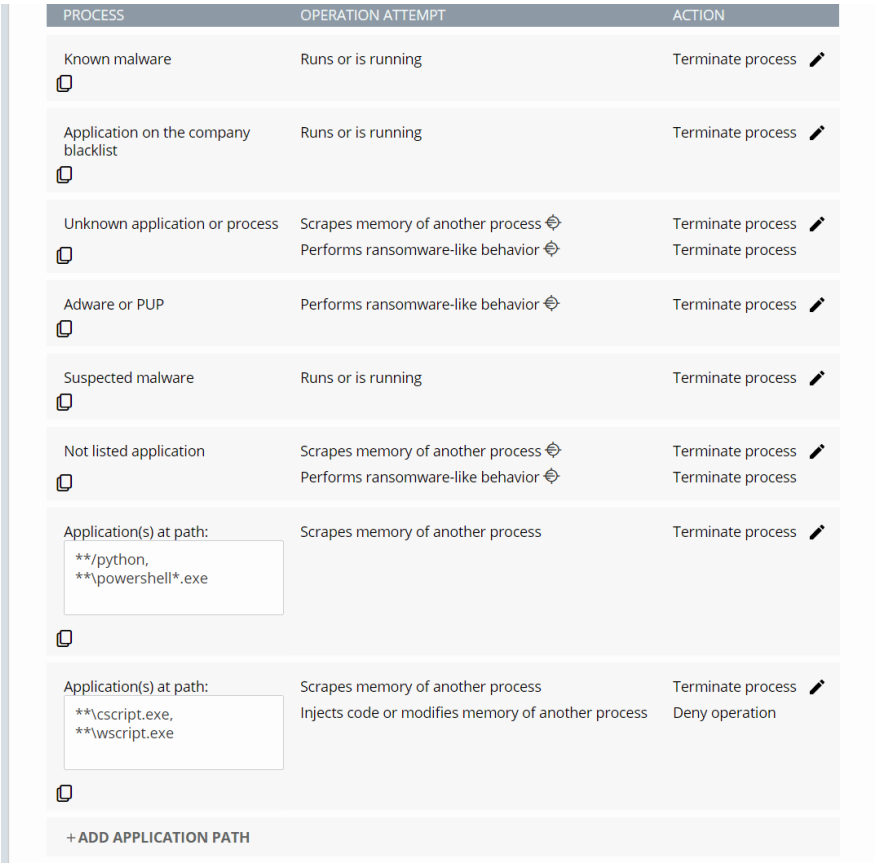
* 権限ルールのみ。

[Blocking and Isolation （ブロックおよび分離）] パネル

[Policy （ポリシー）] ページの左側にある [Policy （ポリシー）] パネルでポリシーを選択すると、そのポリシーに関連するブロックと隔離の設定が右側の [Blocking and Isolation （ブロックと隔離）] パネルに表示されます。

ブロックと隔離ルールを作成または編集する：

1. 左側のパネルで、表示または編集するポリシーを選択します。
2. [Policy （ポリシー）] ページの右側のパネルで、[Cb Defense Settings （Cb Defense 設定）] タブをクリックし、[Blocking and Isolation （ブロックと隔離）] の隣にある矢印をクリックします。



3. 編集するルールの隣にある鉛筆アイコンをクリックして編集するか、[Add Application Path （アプリケーション パスの追加）] をクリックして新しいアプリケーション パスを追加します。複数のパスをコンマで区切って入力できます。
4. [Operation Attempt （操作の試行）] と目的の [Action （アクション）] を選択し、[Confirm （確認）] をクリックします。ごみ箱アイコンをクリックすると、ルールを削除できます。

   注意 :[Action （アクション）] を [Terminate process （プロセスを終了）] に設定すると、同時に操作を拒否することはできません。
5. ポリシーの変更が完了したら、[Save （保存）] をクリックします。

   注意 ： 任意のルールの隣にある [Investigate （調査）] アイコンをクリックすると、[Investigate （調査）] ページが開き、ルール プロパティに設定されている検索パラメーターが使用されます。“ アラートの調査 ” を参照してください。

ポリシーから別のポリシーまたはすべてのポリシーにルールをコピーすることができます。“ ルールのコピー ” を参照してください。

次の表では、[Blocking and Isolation （ブロックと隔離）] パネルについて説明します。

表 27: [Blocking and Isolation （ブロックおよび分離）] パネル

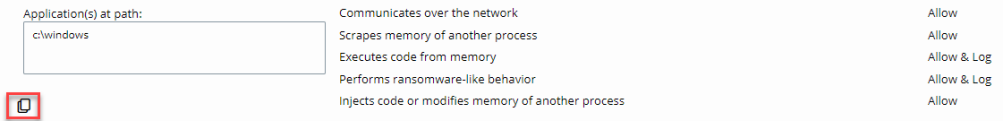
[Title （タイトル）]	説明
Process （プロセス）	ブロックおよび分離ルールの最初の要素であるアプリケーションに関する説明が表示されます。
Operation Attempt （操作の試行）	ブロックと隔離ルールの 2 番目の要素である操作に関する説明が表示されます。次のオプションから [Operation Attempt （操作の試行）] の値を選択します。 • Runs or is running （実行または実行中） • Communicates over the network （ネットワーク経由で通信） • Scrapes memory of another process （他のプロセスのメモリに対するスクレイピング） • Executes code from memory （メモリからコードを実行） • Invokes a process not on the whitelist （ホワイトリストにないプロセスを起動） • Invokes a command interpreter （コマンド インタープリターを起動） • Performs ransomware-like behavior （ランサムウェアのような振る舞いを実行） • Executes a fileless script （ファイルレス スクリプトを実行） • Injects code or modifies memory of another process （コードを挿入または他のプロセスのメモリを変更） 表 26、「各操作の概要」を参照してください。
[Action （アクション）]	[Application （アプリケーション）] と [Operation （操作）] の選択に基づいて実行されるアクションに関する説明が表示されます。選択可能な値は次のとおりです。 • Deny operation （操作を拒否） • Terminate process （プロセスを終了）

ルールのコピー

ポリシーから別のポリシーまたはすべてのポリシーにルールをコピーすることができます。ルールを作成すると、ルールのすぐ左下にコピー アイコンが表示されます。

ルールをコピーする：

1. コピーするルールの下にあるコピー アイコンをクリックします。



2. [All Policies（すべてのポリシー）] をクリックして、ルールをすべてのポリシーにコピーするか、[Select Policies （ポリシーの選択）] をクリックして、ポリシーを選択します。
3. [Select Policies （ポリシーの選択）] をクリックした場合は、[Search for a policy（ポリシーの検索）] テキスト ボックスにカーソルを移動します。既存のポリシーが表示されます。リストからポリシーを選択したり、検索テキスト ボックスにポリシー名を入力したりすることができます。一度に複数のポリシーを選択できます。
4. [Copy （コピー）] をクリックします。コピーしたルールによってポリシーが更新されたことを示す確認メッセージを受け取ります。

コピー元のルール セットがコピー先のルールと競合する場合は、ルールの競合を管理するためのモーダル ウィンドウが表示されます。特定のルールの置換またはスキップを行うか、[Apply selection to all conflicts（選択内容をすべての競合に適用）] チェックボックスをオンにして、競合するすべてのルールの置換またはスキップを一度に行うことができます。

ランサムウェア

リリースされた Cb Defense センサーのバージョン 3.0 では、ランサムウェアのような振る舞いを処理するポリシー ルールを設定できます。

ランサムウェア ポリシー ルールを設定する：

1. 左側のパネルで、編集するポリシーをクリックします。
2. 右側のパネルの [Permissions（権限）] または [Blocking and Isolation（ブロックと隔離）] で、[Add Application Path （アプリケーション パスの追加）] を選択し、アプリケーション パスを入力してから、[Performs ransomware-like behavior （ランサムウェアのような振る舞いを実行）] を選択します。
3. [Confirm （確認）] をクリックします。ポリシーの変更が完了したら、[Save （保存）] をクリックします。

[Performs ransomware-like behavior（ランサムウェアのような振る舞いを実行）] に対して選択できるアクションは、[Terminate process （プロセスを終了）] のみです。これは、ランサムウェアが最初に暗号化を試みるファイルへのアクセスを拒否しても、アプリケーションによる今後の暗号化操作の試行が防止されないためです。パフォーマンスとセキュリティ上の理由から、サポートされるアクションは [Terminate process （プロセスを終了）] のみとなります。

疑わしいマルウェア、PUP、リストにない、および未知の各レピュテーションに関するルールを、ランサムウェアに対する保護ポリシーに追加することをお勧めします。

Windows および OSX では、Microsoft PowerShell と Python が一般的なターゲットですが、コマンド ラインの一部としてコードを受け取ることができれば、どのコマンド インタープリターでも、悪意のあるアクティビティの潜在的なソースとなります。保護を強化するには、スクリプト インタープリター用のパスベースのルールを含めることを検討してください。

最も安全なランサムウェア ポリシーは、デフォルト拒否です。これにより、特別に承認されたアプリケーションを除き、すべてのアプリケーションによるランサムウェアのような振る舞いの実行を防止します。アプリケーションの正規のアクティビティがランサムウェアの操作によく似ている場合に、そのアプリケーションによって生成された偽陽性を処理するための調整がこのポリシーには必要です。高いレピュテーション（TRUSTED_WHITE_LIST など）を持つアプリケーションが侵害される場合がありますが、デフォルト拒否ポリシーの利点は、そうしたアプリケーションに由来するランサムウェアの動作からの保護が可能であることです。考えられるすべてのアプリケーションを列挙する必要はありません。たとえば、アプリケーション パスを **** に設定してから、[Performs ransomeware-like behavior （ランサムウェアのような振る舞いを実行）] を [Terminate process （プロセスを終了）] に設定します。

ポリシー ルールを実稼働システムに適用する前に、1 台の代表的なホスト上でデフォルト拒否ポリシーを徹底的にテストする必要があります。偽陽性に対処したら、さらに数台のエンドポイントをポリシーに移動するという方法で、段階的にロールアウトを実行します。検出された新しい偽陽性に対処するために、各エンドポイント グループの追加間隔を数日空けます。

ランサムウェアのような振る舞いのルールによって良好なソフトウェアが終了される場合は、次で説明するホワイトリストへの追加方法のいずれかを使用します。

Cb Defense: アプリケーションをホワイトリストに追加する方法

ランサムウェア ポリシー ルールをエンドポイントに適用すると、センサー UI が有効な場合、センサー UI にメッセージが表示されます。[Details （詳細）] をクリックすると、終了したプロセスに関する詳細情報が表示されます。

ポリシー ルールおよび TTP

Cb Defense では、センサーによって、動作が個別の TTP （Tactics, Techniques, and Procedures: 攻撃手口）として捕捉されます。Cb Defense クラウドの分析コンポーネントによって、TTP はグループとして分析され、（適宜）アラートにコンパイルされます。“TTP のリファレンス ” を参照してください。

Cb Defense の技術によりエンドポイント情報を環境全体から収集し、データ サイエンスを活用して攻撃者の動作を分析し、それに応じて自動的に調整します。TTP は、アラートにつながるさまざまなアクションのディスクリプターとして使用されます。TTP は Cb Defense のポリシー アクションによって検出、防止された攻撃に関するコンテキストを示します。適用されるポリシーは、TTP によって決定されるのではありません。

適用されるポリシーが TTP によって決定されないため、TTP が特定のポリシー アクションの実行時点を示すとは限りません。ただし、特定のレピュテーションまたは名前 / パスを持つアプリケーションに特定のポリシー ルールが適用された時点で通常表面化する TTP については、[Investigate（調査）] ページでクエリを実行できます。“ アラートの調査 ” を参照してください。

例として processEffectiveReputation:[*Reputation*] というクエリが挙げられます。 *Reputation* は次のいずれかの値に置き換えます。

- KNOWN_MALWARE です。
- COMPANY_BLACK_LIST
- UNKNOWN（未知）
- PUP
- SUSPECT_MALWARE です。
- NOT_LISTED

ヒント

processEffectiveReputation は、大文字と小文字が区別されます。

TTP は、ブロックおよび分離操作と相関付けられていません。ただし、[Investigate（調査）] ページで、threatIndicators および TTP 文字列を、processEffectiveReputation およびレピュテーションと組み合わせて使用して、特定の検索結果を生成できます。このようにすると、指定したブロックと隔離のルールによって、どのアプリケーションがブロックされた可能性があるのかを把握しやすくなります。

たとえば、ルール **"Tries to scrape memory of another process（他のプロセスのメモリ スクレイピングを試行）"** をトリガーできる **Not Listed （リストにない）**アプリケーションを検索するために、次のクエリを実行できます。

```
processEffectiveReputation:NOT_LISTED and
threatIndicators:RAM_SCRAPING or
threatIndicators:READ_SECURITY_DATA
```

クエリの例を次の表に示します。

表 28: TTP クエリの例

操作	クエリ文字列
Executes code from memory（メモリからコードを実行）	• `threatIndicators:SUSPICIOUS_BEHAVIOR` • `threatIndicators:PACKED_CALL`
Scrapes memory of another process（他のプロセスのメモリに対するスクレイピング）	• `threatIndicators:RAM_SCRAPING` • `threatIndicators:READ_SECURITY_DATA`
Communicates over the network（ネットワーク経由で通信）	• `threatIndicators:NETWORK_ACCESS`（成功した接続） • `threatIndicators:ATTEMPTED_SERVER`（失敗した受信接続）
Performs ransomware-like behavior（ランサムウェアのような振る舞いを実行）	• `threatIndicators:KNOWN_RANSOMWARE` • `threatIndicators:DATA_TO_ENCRYPTION?trusted_whitelist` でない場合） • `threatIndicators:SET_SYSTEM_FILE or KERNEL_ACCESS`
Injects code or modifies memory of another process（コードを挿入または他のプロセスのメモリを変更）	• `threatIndicators:INJECT_CODE` • `threatIndicators:HAS_INJECTED_CODE` • `threatIndicators:COMPROMISED_PROCESS` • `threatIndicators:PROCESS_IMAGE_REPLACED` • `threatIndicators:MODIFY_PROCESS` • `threatIndicators:HOLLOW_PROCESS`
Invokes an untrusted application（信頼できないアプリケーションを起動）	• `threatIndicators:ADAPTIVE_WHITE_APP` • `threatIndicators:UNKNOWN_APP` • `threatIndicators:DETECTED_SUSPECT_APP` • `threatIndicators:DETECTED_PUP_APP` • `threatIndicators:DETECTED_BLACKLIST_APP` • `threatIndicators:DETECTED_MALWARE_APP`
Invokes a command interpreter（コマンド インタープリターを起動）	このポリシーにマップされる TTP のセットはありません。

注意

上記のクエリには、括弧内の情報は含めないでください。

アップロード パスの拒否または許可

センサーが特定のファイル パスからアップロードを送信するのを防いだり、許可したりすることができます。

アップロード ファイル パスを拒否または許可する：

1. Cb Defense の [Settings （設定）] パネルの下部で、[Uploads （アップロード）] を展開します。
2. アップロードを拒否または許可するファイル パスを入力し、[Save （保存）] をクリックします。

第 11 章

通知およびコネクター

この章では、検出目的の通知をセットアップする方法について説明します。また、コネクターを作成する方法についても説明します。これにより、コネクターで通知を受信し、Cb Defense API を呼び出せるようになります。

通知タイプ

次の 3 つの通知タイプを追加できます。

- **アラート優先度に基づく通知** – アラート優先度がしきい値を超えると通知が行われます。“Priority score （優先度スコア）” を参照してください。
- **攻撃手口（TTP）に基づく通知** – アラートが特定の TTP を示すと通知が行われます。TTP のリストから選択するか、特定の TTP を入力できます。“TTP のリファレンス ” を参照してください。
- **ポリシー アクションに基づく通知** – ポリシー アクションが強制されると通知が行われます。ポリシーにより行われるアクションに基づいて、これらの通知が設定可能です。この通知タイプでは、ポリシー ルールに基づいてアプリケーション、プロセス、またはネットワーク接続が終了されたか拒否された場合に、通知を行います。“ ポリシーによる攻撃からの防御 ” を参照してください。

通知はアラートまたはポリシー アクションの検出に基づいて生成され、管理者に E メールで送信できます。またコネクターが構成されていれば、接続されているシステムに送信することもできます。

通知の表示

現在構成されている通知を表示する：

1. PSC にログインし、[Settings （設定）] をクリックして [Notifications （通知）] をクリックします。

   現在構成されているすべての通知が表示されます。

2. 通知の右側にある鉛筆のアイコンをクリックすると通知を編集できます。また通知の右側にある [x] アイコンをクリックすると通知を削除できます。
3. 通知の履歴を表示するには、通知の右側にある時計のアイコンをクリックします。確認する通知の時間枠を選択します。

   表示されたリストに、その通知ルールに関するすべての通知が示されます。このリストには、スケジュールされている通知、送信済みの通知、トリガーされなかった通知に加え、これらの通知に関連するタイムスタンプとルールが表示されます。トリガーされなかった通知には説明が含まれます。

   通知は、通知のコンテキストを容易に理解できるように、分類および色分けされます。用意されている通知タイプは次のとおりです。

- 運用に関わる問題 - 監視中 （オレンジ）
- 運用に関わる問題 - 解決済み （緑）
- スケジュールされたメンテナンス - ダウンタイムあり （黄色）
- スケジュールされたメンテナンス - ダウンタイムなし （黄色）
- サポート アラート （オレンジ）

通知の追加

通知を追加する：

1. PSC にログインし、**[S**ettings （設定）] をクリックして [Notifications （通知）] をクリックします。
2. [Add Notification （通知の追加）] をクリックし、[Add Notification （通知の追加）] ページに通知の詳細を入力して、[Add （追加）] をクリックします。

TTP に基づく通知と脅威スコアに基づく通知の両方をセットアップすると、同一のアラートに対して E メールを 2 通受信する可能性があります。2 つの E メール アドレス （通知タイプごとに 1 つずつ）をセットアップすることをお勧めします。これにより、複数の通知を受け取ることから生じる混乱を避けることができます。

ヒント

Cb Defense から受信する E メールの数を減らすには、[Send at most one email notification for a given threat type per day（指定された脅威タイプに対して 1 日あたり最大 1 通の E メール通知を送信する）] を選択します。

注意

この目的で使用される E メール アドレスは、登録された Cb Defense ユーザーと関連付けられている必要があります。“ ユーザーの管理 ” を参照してください。

コネクターの追加と構成

Carbon Black のオープン API プラットフォームを使用すると、SIEM をはじめとする各種セキュリティ製品、チケット追跡システム、および独自のカスタム スクリプトを確実に統合できます。Carbon Black では、事前作成のコネクターを提供して、Syslog を通じた SIEM との統合、Splunk アドオン経由の Splunk との直接統合、QRadar アプリを介した IBM QRadar との統合に対応しています。その他の統合パートナーについては、Cb Integration Network の Web サイト（https://www.carbonblack.com/why-cb/integration-network/） を参照してください。Cb Defense API の詳細については、Developer Network の Web サイト（https://developer.carbonblack.com/）を参照してください。

注意

コネクターは、ユーザーに付与されている権限を継承します。コネクター ID と API キーは、Cb Defense コンソールのログイン パスワードと同様、[Connectors （コネクター）] ページの内部で保護してください。コネクターの認証情報が侵害された場合は、“ コネクターの API キーを表示または再生成する :” に示す手順で、影響を受ける API キーを直ちに再生成します。

次の手順でコネクターを作成した後、SIEM コネクターを通知ルールに関連付けます。

Cb Defense では、各統合ポイントがコネクターによって定義されます。

コネクターを追加する :

1. PSC にログインし、[Settings （設定）] をクリックして [Connectors （コネクター）] をクリックします。
2. [Add （追加）] をクリックして、以下の情報を入力します。
   - Name （名前）– コンソールの各コネクターを特定します。Cb Defense 組織に関連付けられるコネクターを一意に識別するものであれば、どのような名前でも指定できます。
   - Connector type （コネクター タイプ）– SIEM、API、および Live Response。
     SIEM コネクターは、通知 API を介してのみ通知を受信できます。Splunk アドオン、QRadar アプリ、または Syslog コネクターを構成するには、SIEM コネクターを使用します。
     API コネクターは、通知 API と Live Response API を除くすべての API を呼び出すことができます。
     Live Response コネクターは、通知 API を除くすべての API を呼び出すことができます。
   - Authorized IP addresses （許可されている IP アドレス）– （オプション）このコネクターの使用が許可されている IP アドレスまたは CIDR 表記の IP アドレス範囲 （例 : 192.0.2.x サブネットのすべてのホストの場合は、192.0.2.0/24）。リストが空の場合は、どの IP アドレスでもこのコネクターに対して API を呼び出すことができます。RFC 1918 の各アドレス （192.168.0.0/16、10.0.0.0/8、および 172.16.0.0/12）は、パブリックにルーティングできず、許可された IP アドレスとして使用することはできません。パブリック IP アドレスを見つけ、そのアドレスまたはアドレス範囲をこの構成オプションで使用してください。
   - 説明 （説明）– （オプション）このコネクターに関連付けられた任意のテキスト。
3. [Add （追加）] をクリックします。

コネクターの認証情報が侵害された場合は、API キーを再生成します。統合時に API キーを再入力する必要があります。

コネクターの API キーを表示または再生成する :

1. PSC にログインし、[Settings （設定）] をクリックして [Connectors （コネクター）] をクリックします。
2. 対象のコネクターで、[Actions （アクション）] 列の下向き矢印をクリックします。
3. **[API Key （API キー）]** をクリックします。**[Copy （コピー）]** アイコンをクリックして API キーをコピーするか、**[Generate new API key （新しい API キーを生成）]** をクリックします。

不要になったコネクターは削除します。

コネクターを削除する：

1. PSC にログインし、[Settings （設定）] をクリックして [Connectors （コネクター）] をクリックします。
2. 対象のコネクターで、[Actions （アクション）] 列の下向き矢印をクリックします。
3. [Delete （削除）] をクリックします。

注意

まずコネクターに関連付けられた通知ルールを削除せずに、コネクターを削除しようとすると、"409" エラーが発生します。関連付けられた通知ルールからまずコネクターを削除した後、コネクターを削除します。

Carbon Black は、ダウンロード可能な 2 つの事前に作成されたコネクターと、サンプル API スクリプトを提供しています。これにより、独自の統合を容易に作成することが可能です。Carbon Black の事前に作成された統合の詳細については、次のリソースを参照してください。

- Splunk 統合：
  - Splunk 向け Cb Defense アドオンは、Cb Defense から通知を取り込んで Splunk SIEM に提供します。このアドオンをダウンロードして Splunk または Splunk Cloud インスタンスにインストールする手順については、https://splunkbase.splunk.com/app/3545/#/details を参照してください。
  - Splunk 向け Cb Defense アプリは、Cb Defense と Splunk の間で、対話的ダッシュボードや API 接続など、双方向の統合を提供します。このアプリをダウンロードして Splunk または Splunk Cloud インスタンスにインストールする手順については、https://splunkbase.splunk.com/app/3905/#/details を参照してください。Cb Defense アプリをインストールするには、その前に Cb Defense アドオンをインストールする必要があります。
- QRadar 統合：
  - https://exchange.xforce.ibmcloud.com/ ハブの IBM X-Force App Exchange にアクセスします。"Cb Defense App for IBM QRadar" を検索して、IBM QRadar と統合する Cb Defense アプリをインストールするためのインストール手順とダウンロード リンクを確認します。
- syslog 統合：
  - Carbon Black は、CEF スタイルまたは JSON スタイルの syslog 入力を受け付ける他の SIEM に、Cb Defense 通知をプッシュする事前作成の Syslog 統合を提供しています。Syslog 統合の詳細については、https://developer.carbonblack.com/reference/cb-defense/connectors/#cb-defense-syslog-connector を参照してください。

Carbon Black API の使用方法の詳細については、次のリソースを参照してください。

- Cb Integration Network の Web サイト （https://www.carbonblack.com/why-cb/integration-network/）には、Carbon Black と当社のテクノロジー パートナーが提供する事前作成の統合に関する情報が用意されています。
- Developer Network の Web サイト （https://developer.carbonblack.com）。API リファレンスドキュメントと、Cb Defense のオープン API に関するその他のチュートリアルが用意されています。この情報は、独自の統合を開発する場合だけでなく、Carbon Black による事前作成の Splunk 統合や QRadar 統合をインストールして構成する場合にも使用できます。
- cbapi Python モジュール。Cb Defense API に対する使いやすい Python インターフェイスを提供します。cbapi モジュールについては、https://cbapi.readthedocs.io を参照してください。また、ソース コード （サンプル スクリプトを含む）を https://github.com/carbonblack/cbapi-python から入手できます。
- この API を使用している他のユーザーに質問したり、交流したりするには、User eXchange の Developer Relations（https://community.carbonblack.com/community/resources/developer-relations）にアクセスしてください。

第 12 章

疑わしいファイルのアップロード

疑わしいファイルは、Cb Defense にアップロードして次のいずれかの方法で分析できます。

- ファイルのアップロードを手動で要求することにより、疑わしいファイルを Cb Defense にアップロードできます。アップロードは管理者の受信ボックスに表示されます。センサーによってアップロードされたファイルをダウンロードして、手動で分析を実行できます。

  注意

  アップロードしたファイルは、2 週間後に期限切れになります。期限切れになったファイルをダウンロードしようとすると、タイムアウト エラーが発生します。

- 未知のバイナリをクラウド分析用に送信することができます。“**クラウド分析**” を参照してください。

手動によるファイルのアップロード要求

調査中に、関心対象となるファイルや疑わしいファイルを Cb Defense にアップロードするよう要求できます。後でこれらのファイルを Cb Defense の受信ボックスからダウンロードし、Cb Defense の外部で必要に応じて分析を実行できます。

手動によるファイルのアップロードを要求する：

1. PSC にログインし、[Investigate （調査）] をクリックします。
2. 分析するアプリケーションを検索して選択します。
3. [Actions （アクション）] メニューで、[Request Upload （アップロード要求）] をクリックします。

   注意 :[Alerts （アラート）] > [Primary Process （主なプロセス）] ページから [Actions （アクション）] > [Request Upload（アップロード要求）] オプションにアクセスすることもできます。“ **アラートの影響を受ける主なプロセスの表示** ” を参照してください。

4. **[Send （送信）]** をクリックします。

受信ボックスのファイルを表示する：

1. PSC にログインし、[Settings （設定）] をクリックして [Inbox （受信ボックス）] をクリックします。

   受信ボックスに表示されている項目が、次のいずれかの状態になっています。

   - [Triggered （トリガー済み）] - アクションは、バックエンドによって記録されました。
   - [Sent To Sensor （センサーに送信済み）] - センサーはチェックイン済みで、アクションを取得しました。

2. アップロードしたファイルをダウンロードするには、ファイル名の隣にある [Download （ダウンロード）] アイコンをクリックします。

手動によるファイル アップロードの制限事項

手動によるファイルのアップロードには、次のファイルの制限事項が適用されます。

Windows

注意

Windows では、[Private Logging Level （プライベート ロギング レベル）] が有効になっている場合、スクリプト ファイルのアップロードに制限はありません。

“**[Cb Defense Settings （Cb Defense 設定）] タブ** ” を参照してください。

次のファイル拡張子の Windows ファイルは、Cb Defense で分析用にアップロードできます。

- `.exe`
- `.dll`
- `.sys`
- `.ocx`
- `.drv`
- `.scr`
- `.pif`
- `.ex_`
- `.msi`
- `.vb`
- `.vbs`
- `.jar`

macOS

注意

macOS では、[Private Logging Level （プライベート ロギング レベル）] が有効になっている場合、スクリプトはアップロードされません。[Allow Executable Uploads for Scans （スキャン用に実行可能ファイルのアップロードを許可）] が選択されていない場合、タイプに関係なくすべてのスクリプトのアップロードは無効になります。

詳細については、 “**[Cb Defense Settings （Cb Defense 設定）] タブ** ” を参照してください。

次のような一般の macOS オブジェクト タイプは分析用にアップロードできます。

- Perl
- Python
- Ruby
- Shell
- TCL
- PHP

- Applescript

次のオブジェクトはアップロードできません。

- `/etc` ディレクトリ内のファイル
- 次の拡張子が含まれるファイル
  - `.class`
  - `.js`
  - `.pkg` および `.dmg` （ファイル サイズ > 20 MB）
- スクリプト （[Private Logging Level （プライベート ロギング レベル）] が有効になっている場合。“**[Cb Defense Settings （Cb Defense 設定）] タブ** ” を参照）
- 次のようなドキュメント ファイル
  - Keynote
  - PDF
  - MS Office
  - Open Office （magic と拡張子の両方で決定）
- テキスト ファイルやランダムなバイナリ データなどの Magic Cookie が含まれていないファイル

> **注意**
>
> Magic Cookie は、ファイルに関連する特別なファイル形式を識別するファイルの最初の 4 バイトを参照します。

クラウド分析

この機能は、未知のバイナリをサードパーティ パートナーによってさらに分析することで、セキュリティの有効性をさらに高めます。クラウド分析が機能するためには、ローカル スキャナをオンにし、センサー バージョン 3.2 以上を使用する必要があります。

クラウド分析を有効にする：

1. PSC にログインし、[Enforce （適用）] をクリックして [Policies （ポリシー）] をクリックします。
2. クラウド バイナリ分析を有効にするポリシーを選択します。
3. 右側のパネルで、[Submit unknown binaries for analysis（分析のための不明なバイナリの送信）] のチェックボックスをオンにします。
4. この機能にオプトインし、それによって共有データを Carbon Black およびサードパーティと共有することを確認します。
5. [Save （保存）] をクリックします。

注意

この機能にオプトインすると、バイナリ ファイル （ファイルの内容を含む）が分析のために Carbon Black にアップロードされます。Carbon Black は、脅威分析を補助するデータ処理下請業者として、サードパーティ ベンダーの Avira Operations GmbH & Co. KG （以下 「Avira」）を利用します。バイナリ ファイルは、Avira のネットワークに送信されます。Avira は適用される契約に基づき、Carbon Black の義務を満たすためのみにデータを処理し、その他の目的でデータを使用することはありません。Avira は、データ保護のための適切なセキュリティと運用方法を整備しており、データ処理にあたっては、適用されるすべてのデータ プライバシー法に準拠します。情報は、米国または EU にあるデータ センターで、Avira によって処理されます。

お客様は、このサービスを使用する間、かかるデータすべての正確性、品質、完全性、適法性、信頼性、適切性、および知的財産の所有権または使用権や Carbon Black に転送する権利について、単独で責任を負うものとします。Carbon Black のプライバシー ポリシーは、https://www.carbonblack.com/privacy-policy/ で参照できます（Carbon Black が随時変更することがあります）。

クラウド分析用にアップロードされたファイルを表示する :

1. PSC にログインし、[Settings （設定）] をクリックして [Cloud Analysis （クラウド分析）] をクリックします。次のデータが表示されます。
   - ファイルがアップロードされた日時。
   - ファイルのアップロード元のエンドポイントの名前。
   - アップロードしたファイルの名前。
   - アップロードしたファイルの SHA256 ハッシュ。
   - 分析結果。

第 13 章

認証および統合

この章では、Cb Defense で 2 段階認証をセットアップする方法と、Okta、Ping Identity、および OneLogin との SAML 統合をセットアップする方法について説明します。また、Windows セキュリティ センターとの Cb Defense 統合を無効または有効にする方法についても説明します。

2 段階認証の有効化

DUO または Google 2 段階認証 （2FA）を有効にして Cb Defense で使用できます。どちらのオプションを有効にした場合も、ユーザーが次回ログインしたときに、ソフトウェアをインストールし、対応するシステムのアカウントをセットアップすることを求めるプロンプトが発生します。

注意

この機能を有効にするには、2 人以上のユーザーが Cb Defense に登録されている必要があります。これにより、必要に応じて 1 人のユーザーが他のユーザーの資格情報をリセットすることができます。“ ユーザーの管理 ” を参照してください。

DUO 2FA の有効化

DUO 2FA を有効にする：

1. PSC にログインし、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。
2. 2FA はデフォルトで無効になっています。[DUO Security （DUO セキュリティ）] をクリックして有効にします。PSC にログインする組織内の全員を代表して DUO 2FA を確認するように求められます。[DUO Security Settings （DUO セキュリティ設定）] ポップアップ モーダル ウィンドウに、DUO 認証をセットアップする方法が示されます。
3. DUO にログインした後、[DUO Dashboard （DUO ダッシュボード）] に移動し、[Applications （アプリケーション）] をクリックします。
4. [+ Protect an Application （+ アプリケーションを保護する）] ボタンをクリックします。
5. "Web SDK" を検索し、[Protect this Application （このアプリケーションを保護する）] を選択します。[Web SDK （Web SDK）] ページに、統合鍵、秘密鍵、および API ホスト名が含まれた詳細ボックスが表示されます。
6. これらのボックスのそれぞれから鍵をコピーし、ステップ 2 で表示された DUO 構成ポップアップ モーダル ウィンドウの対応するボックスに貼り付けます。
7. [Submit （送信）] をクリックして構成を保存します。確認メッセージと [DUO Settings （DUO 設定）] ボタンが表示されます。このボタンをクリックすると、組織の DUO 設定を再構成することができます。

   組織のユーザーが次回ログインするときは、DUO を使用して認証する必要があります。

Google 2FA の有効化

Google 2FA を有効にする :

1. PSC にログインし、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。
2. 2FA はデフォルトで無効になっています。[Google Authenticator（Google 認証システム）] をクリックして有効にします。Google 2FA を確認するように求められます。組織のユーザーが次回ログインするときは、Google 認証システムを使用して認証する必要があります。
3. PSC からログアウトして [Login（ログイン）] ページに戻ります。ユーザーの E メール アドレスとパスワードを使用してログインします。
4. iOS または Android 版の Google 認証システム アプリをダウンロードし、モバイル デバイスにインストールします。
5. モバイル デバイスで Google 認証システム アプリを開き、バーコードをスキャンして Google 2FA のセットアップ プロセスを完了します。
6. Google 2FA がアクティブ化されたことを確認するポップアップ モーダル ウィンドウが表示されます。
7. モバイル デバイスに表示された 6 桁のコードを入力して、PSC コンソールに対する認証を実行します。

Okta との SAML 統合の有効化

Okta との SAML 統合を有効にする :

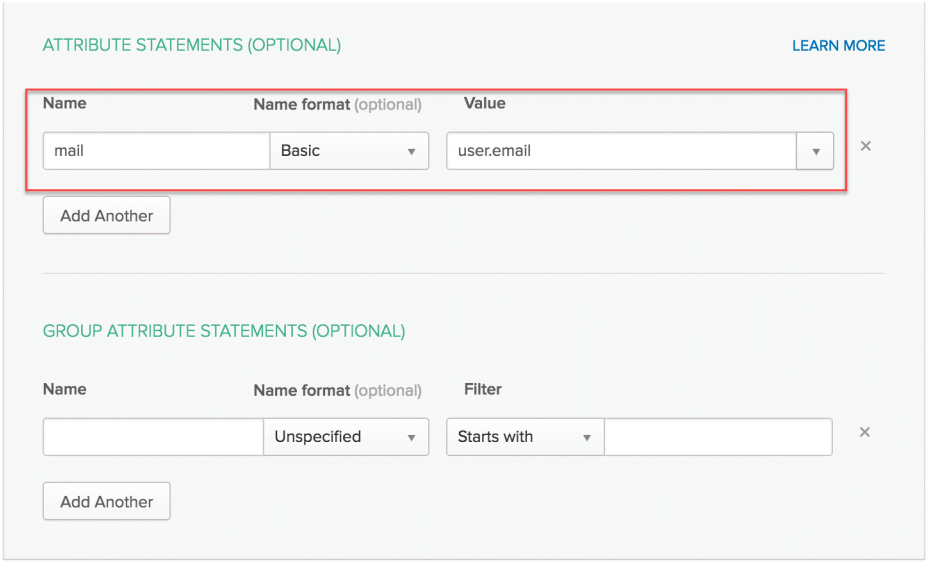
1. PSC にログインします。
2. PSC の 2 番目のインスタンスを新しいブラウザー タブで起動します。
3. PSC の 2 番目のインスタンスで、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。

   注意 : 2 番目のブラウザー タブは、なんらかの構成が間違っているために、SAML を使用してもログインできない場合に役立ちます。この場合、2 番目のインスタンスに戻って SAML を無効にします。その後が、設定を確認することも、Carbon Black テクニカル サポートに問い合わせることもできます。“Carbon Black テクニカル サポート ” を参照してください。
4. PSC の 1 番目のインスタンスで、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。
5. SAML はデフォルトで無効になっています。[Enabled （有効化）] をクリックして有効にします。
6. [SAML Configure （SAML 構成）] ページで、[Other （その他）] をクリックします。
7. [Email Attribute Name（E メール属性名）] フィールドで、値を [mail（メール）] のままにします。
8. Okta にログインし、以下の手順を実行します。
   a. [Applications （アプリケーション）] をクリックします。
   b. [Create New App （新しいアプリの作成）] をクリックします。
   c. アプリのタイプとして [SAML 2.0] を選択します。

d. アプリに名前を付け、[Next （次へ）] をクリックします。

e. Cb Defense の [Audience （対象ユーザー）] と [ACS URL] の値 （これらは同じ URL です）をコピーし、Okta の [Single sign on URL （シングル サインオン URL）] フィールドと [Audience URI （SP Entity ID）（対象ユーザー URI （SP エンティティ ID））] フィールドに貼り付けます。

f. [Attribute Statement （属性ステートメント）] を次のスクリーンショットに示すとおりに設定します。



g. [I’m an Okta customer adding an Internal app （私は、内部アプリを追加している Okta ユーザーです）] を選択して、[Finish （完了）] をクリックします。

h. [View Setup Instructions （セットアップ手順の表示）] をクリックします。

i. [Login URL/SignOn URL （ログイン URL/ サインオン URL）] フィールドの値をコピーし、Cb Defense の [SAML Config （SAML 構成）] ページの [Single Sign On URL （シングル サインオン URL）] フィールドに貼り付けます。

j. [Save （保存）] をクリックします。

9. 新しいブラウザー タブまたはウィンドウを開き、SAML 認証を確認します。

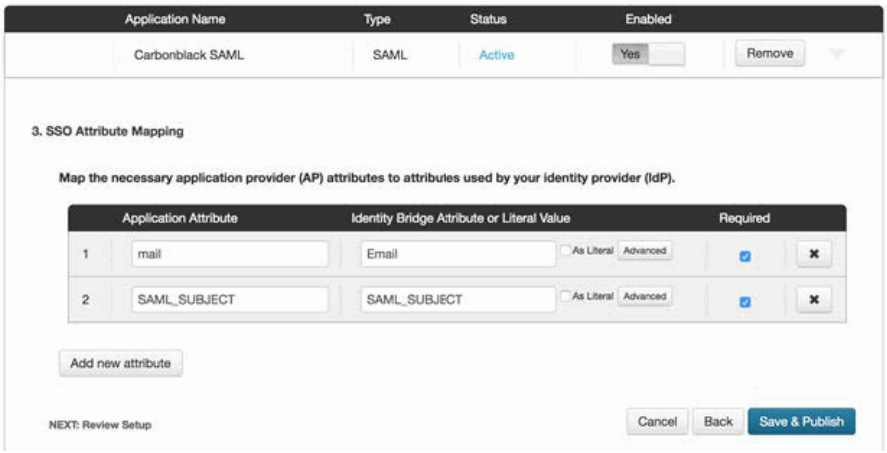
Ping Identity との SAML 統合の有効化

Ping Identity との SAML 統合を有効にする：

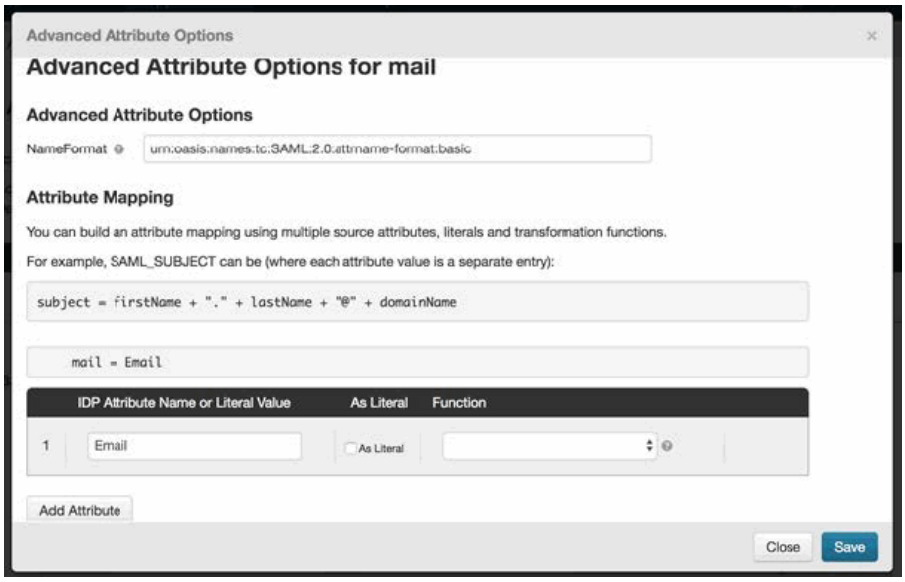
1. PSC にログインします。
2. PSC の 2 番目のインスタンスを新しいブラウザー タブで起動します。
3. PSC の 2 番目のインスタンスで、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。

   注意：2 番目のブラウザー タブは、なんらかの構成が間違っているために、SAML を使用してもログインできない場合に役立ちます。この場合、2 番目のインスタンスに戻って SAML を無効にします。その後が、設定を確認することも、Carbon Black テクニカル サポートに問い合わせることもできます。“Carbon Black テクニカル サポート ” を参照してください。

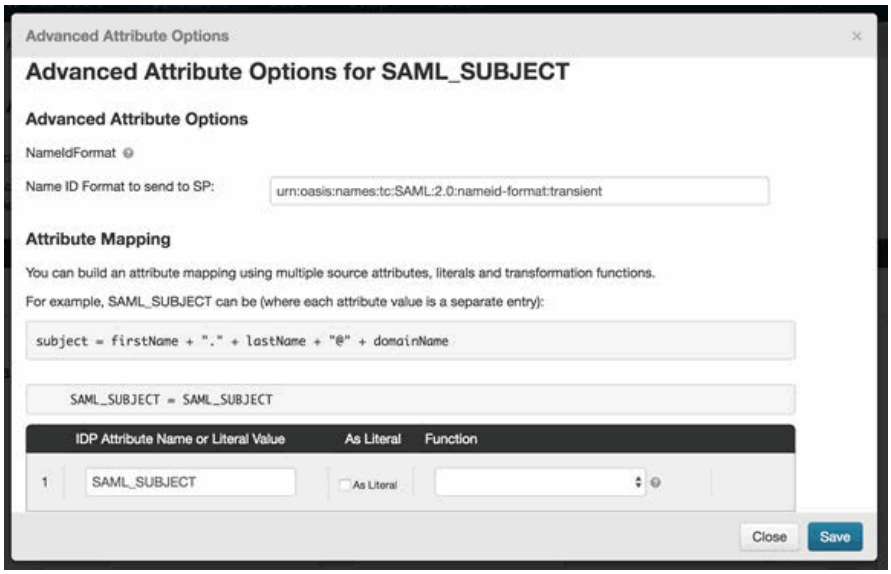
4. PSC の 1 番目のインスタンスで、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。
5. SAML はデフォルトで無効になっています。[Enabled （有効化）] をクリックして有効にします。
6. [SAML Configure （SAML 構成）] ページで、[Other （その他）] をクリックします。
7. [Email Attribute Name（E メール属性名）] フィールドで、値を [mail（メール）] のままにします。
8. Ping Identity にログインし、以下の手順を実行します。
   a. admin.pingone.com に移動します。
   b. アカウントを作成するか、ログインします。
   c. [Admin （管理）] をクリックし、https://admin.pingone.com/web-portal/dashboard#）に移動します。
   d. [Admin （管理）] ダッシュボードで、[Applications （アプリケーション）] タブをクリックします。
   e. [Add application （アプリケーションの追加）] をクリックします。
   f. [New SAML application （新しい SAML アプリケーション）] をクリックします。
   g. [Application Name （アプリケーション名）]、[Application 説明 （アプリケーションの説明）]、[Category （カテゴリ）]、[Graphics （グラフィック）] （オプション）の各フィールドに入力します。[Continue to Next Step （次のステップに進む）] をクリックします。
   h. [I have the SAML configuration tab selected （SAML 構成タブを選択しました）] タブをクリックします。
   i. [Cb Defense SAML] ページで、[ACS] フィールドとエンティティ ID を入力します。
   j. [Continue to Next Step （次のステップに進む）] をクリックします。
   k. [Add new attribute （新しい属性の追加）] をクリックします。
   l. 次に示すとおりフィールドに入力します。



m. **メール** フィールドの [Advanced （詳細）] をクリックし、次に示すフィールドに入力します。[Save （保存）] をクリックします。



n. **SAML サブジェクト** フィールドの [Advanced （詳細）] をクリックし、次に示すとおりフィールドに入力します。[Save （保存）] をクリックします。



o. [Save & Publish （保存 & 発行）] をクリックします。

p. [Review Setup （セットアップの確認）] セクションで SAML 署名証明書をコピーし、Cb Defense の [SAML Config （SAML 構成）] ページに貼り付けます。さらに、SSO URL をコピーして Cb Defense の [SAML Config （SAML 構成）] ページに貼り付けます。

q. PingOne アカウントの E メール アドレスが Cb Defense ユーザーの E メール アドレスと異なる場合、[Users （ユーザー）] タブをクリックし、PingOne ログイン アカウントの E メール アドレスを構成します。

9. Cb Defense の [SAML Config （SAML 構成）] ページに戻り、[Save （保存）] をクリックします。

10. 新しいブラウザー タブまたはウィンドウを開き、SAML 認証を確認します。

OneLogin との SAML 統合の有効化

OneLogin との SAML 統合を有効にする :

1. PSC にログインします。
2. PSC の 2 番目のインスタンスを新しいブラウザー タブで起動します。
3. PSC の 2 番目のインスタンスで、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。

   注意 : 2 番目のブラウザー タブは、なんらかの構成が間違っているために、SAML を使用してもログインできない場合に役立ちます。この場合、2 番目のインスタンスに戻って SAML を無効にします。その後が、設定を確認することも、Carbon Black テクニカル サポートに問い合わせることもできます。“Carbon Black テクニカル サポート ” を参照してください。
4. PSC の 1 番目のインスタンスで、[Settings （設定）] をクリックして [Users （ユーザー）] をクリックします。
5. [Add Admin （管理者の追加）] をクリックします。
6. OneLogin ユーザーに割り当てる E メール アドレスを入力します。
7. ユーザー ロールを選択して [Add （追加）] をクリックします。
8. SAML はデフォルトで無効になっています。[Enabled （有効化）] をクリックして有効にします。
9. [SAML Configure （SAML 構成）] ページで、[Other （その他）] をクリックします。
10. 2 番目のブラウザー タブまたは新しいウィンドウで OneLogin にログインします。
11. OneLogin 管理者ダッシュボードで [Apps （アプリ）] > [Add Apps （アプリの追加）] に移動します。
12. **SAML Test Connector** を検索し、検索結果から最初の結果を選択します。
13. 結果を保存します。OneLogin の [Info（情報）] ページに移動します。[Configuration（構成）] タブをクリックします。
14. 表示名フィールドに 「Cb Defense」と入力します。
15. [Cb Defense SAML Enabled （Cb Defense SAML 有効）] ページで、[Audience （対象ユーザー）] フィールドの URL をコピーします。
16. Onelogin で、コピーしたテキストを [RelayState]、[Audience （対象ユーザー）]、および [Recipient （受信者）] フィールドに貼り付けます。
17. [Cb Defense SAML Enabled（Cb Defense SAML 有効）] ページで、[ACS（Consumer）URL Validator （ACS （コンシューマー）URL バリデーター）] フィールドの URL をコピーします。
18. Onelogin で、コピーしたテキストを [ACS （Consumer）URL Validator* （ACS （コンシューマー）URL バリデーター *）] フィールドに入力します。
19. [Cb Defense SAML Enabled（Cb Defense SAML 有効）] ページで、[ACS（Consumer）URL （ACS （コンシューマー）URL）] フィールドの URL をコピーします。
20. Onelogin.com で、コピーしたテキストを [ACS （Consumer）URL* （ACS （コンシューマー）URL*）] フィールドに入力します。
21. [Save （保存）] をクリックして、Onelogin.com での構成変更を保存します。

22. [Parameters （パラメーター）] タブをクリックします。
23. [SAML Test Connector（IdP）Field（SAML テスト コネクター（IdP）フィールド）] が [mail （メール）] で [Value （値）] が [Email （E メール）] のパラメーターを追加します （カスタム パラメーター）。
24. [SSO] タブをクリックします。
25. X.509 証明書をコピーします。
26. その値を Cb Defense の [X509 Certificate（X509 証明書）] フィールドに貼り付けます。

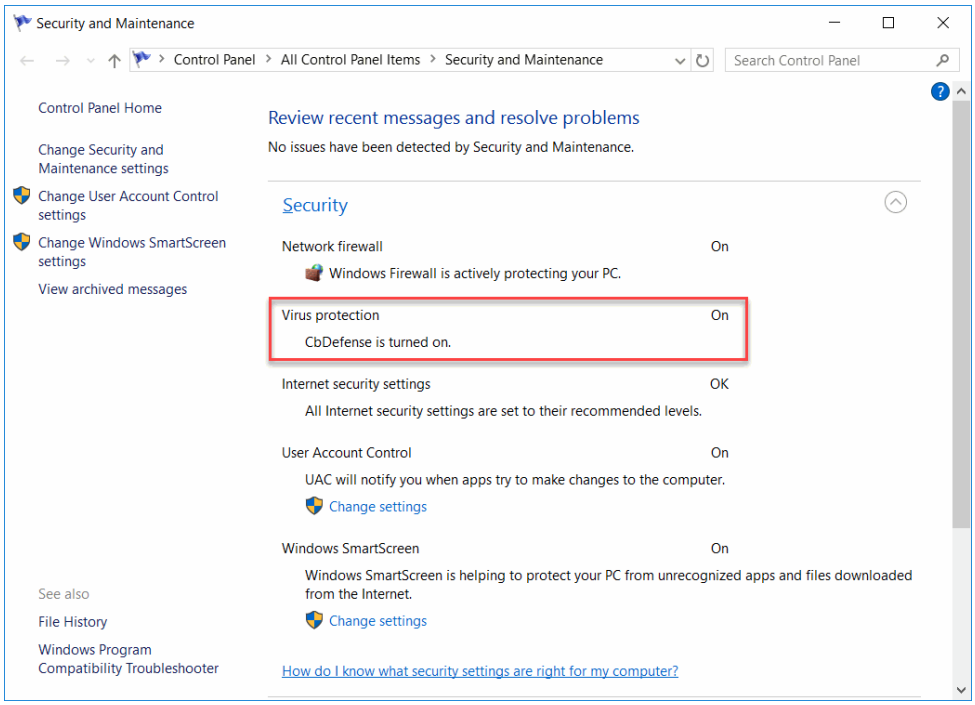
> **注意**
>
> X509 証明書のデータをコピーするときは注意が必要です。空白や改行が誤ってい含まれていると、"Request failed with status code 400（ステータス コード 400 のために要求が失敗しました）" というエラー メッセージが返されます。このメッセージが発生するが、構成を確認しても問題が見つからない場合、証明書の情報を 1 行ずつコンソールにコピーしてみてください。

27. Onelogin で、[SAML 2.0 Endpoint （HTTP）（SAML 2.0 エンドポイント （HTTP））] フィールドの値をコピーします。
28. その値を Cb Defense の [Single Sign On URL （HTTP-Redirect Binding）（シングル サインオン URL （HTTP-Redirect Binding））] フィールドに貼り付けます。
29. [Save （保存）] をクリックします。
30. 新しいブラウザー タブまたはウィンドウを開き、SAML 認証を確認します。

Windows セキュリティ センター統合の無効化または有効化

Windows セキュリティ センター（WSC）では、Windows デバイスにアンチウィルス プロバイダーがインストールされていることが求められます。Cb Defense は、WSC に対応する、Microsoft 社認定アンチウィルス プロバイダーです。

Windows 7 以降のオペレーティング システムが実行されているデバイス上で Cb Defense を WSC と統合し、Cb Defense をアンチウィルス プロバイダーとして指定できます。Cb Defense センサー バージョン 2.1.0.11 以降を使用している必要があります。Cb Defense を有効にすると、デバイスのアンチウィルス プロバイダーとして表示されます。



注意

エンド ユーザーは、コントロール パネルの [セキュリティとメンテナンス] を使用して WSC 統合を無効または有効にすることができます。

新しい組織に対しては、標準ポリシー（Standard）のポリシー設定によって、WSC 統合がデフォルトで有効になります。WSC 統合は無効にすることができます。WSC 統合を無効にしても Cb Defense は無効になりません。

既存の組織では、WSC 統合を明示的に有効にする必要があります。

Cb Defense の WSC 統合を無効にする：

1. PSC にログインし、[Enforce （適用）] をクリックして [Policies （ポリシー）] をクリックします。
2. 左側のパネルで、WSC 統合を無効にするポリシーをクリックします。
3. 右側のパネルで、[Use Windows Security Center （Windows セキュリティ センターを使用）] チェックボックスをオフにして WSC 統合を無効にします。[Save （保存）] をクリックします。

Cb Defense の WSC 統合を有効にする：

1. PSC にログインし、**[Enforce** （適用）] をクリックして [Policies （ポリシー）] をクリックします。
2. 左側のパネルで、WSC と統合するポリシーをクリックします。このポリシーのすべてのセンサーが WSC と統合されます。
3. 右側のパネルで、[Use Windows Security Center （Windows セキュリティ センターを使用）] チェックボックスをオンにして WSC 統合を有効にします。[Save （保存）] をクリックします。

Appendix A

TTP のリファレンス

Cb Defense では、動作は個別の TTP（Tactics, Techniques, and Procedures: 攻撃手口）として捕捉されます。動作はセンサーによってデバイスで捕捉され、バックエンド プラットフォームで分析エンジンによってアラートにコンパイルされる（適用される場合）グループとして分析されます。

この付録には、TTP の定義と可能な値が記載されています。

表 29: TTP

タグ	検出箇所	カテゴリ	設定の状態	説明
ACCESS_CALENDAR	センサー	Data at Risk（潜在的に危険なデータ）	ファイルシステムのフィルター ドライバーが、ターゲット ファイルの拡張子に基づいて読み取りアクセスを特定するように設定されています。	カレンダー アプリケーション データ ファイルにアクセスします。たとえば、Outlook などです。
ACCESS_CONTACTS	センサー	Data at Risk（データの危険性）	ファイルシステムのフィルター ドライバーが、ターゲット ファイルの拡張子に基づいて読み取りアクセスを特定するように設定されています。	連絡先リストや電話番号リストのアプリケーション データにアクセスします。
ACCESS_DATA_FILES	センサー	Data at Risk（データの危険性）	ファイルシステムのフィルター ドライバーが、ターゲット ファイルの拡張子に基づいて読み取りアクセスを特定するように設定されています。	データ ファイルにアクセスします。
ACCESS_EMAIL_DATA	センサー	Data at Risk（データの危険性）	ファイルシステムのフィルター ドライバーが、ターゲット ファイルの拡張子に基づいて読み取りアクセスを特定するように設定されています。	E メールの内容にアクセスします。
ACTIVE_CLIENT	センサー	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーが、IPv4 または IPv6 接続が正常に開始されたことを特定するように設定されています。	アプリケーションがネットワーク接続を正常に開始しました。

タグ	検出箇所	カテゴリ	設定の状態	説明
ACTIVE_SERVER	センサー	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーが、受け入れた IPv4 または IPv6 接続を特定するように設定されています。	アプリケーションがネットワーク接続を正常に受け入れました。
ADAPTIVE_WHITE_APP	分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行可能ファイルが検出されました。実行可能ファイルのレピュテーション は ADAPTIVE_WHITE_APP です。また、アプリケーションは署名されておらず、新しいもの（30 日未満）です。	スキャンでクリーンと判定された不明なアプリケーション。
ATTEMPTED_CLIENT	センサー	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーが、IPv4 または IPv6 接続の開始に失敗したことを特定するように設定されています。	アプリケーションがネットワーク接続の開始を試み、失敗しました。
ATTEMPTED_SERVER	センサー	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーが、IPv4 または IPv6 接続の受け入れに失敗したことを特定するように設定されています。	アプリケーションがネットワーク接続の受け入れを試み、失敗しました。
BEACON	分析	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーがネットワーク ソケット接続（ユーザーランド フックの使用を含む）を実行しましたが、失敗しました。	レピュテーションの低いアプリケーション（ADAPTIVE_WHITE 以下）の初回実行が、http/s 経由でサーバーへのビーコン登録を試みましたが、失敗しました。
BUFFER_OVERFLOW_CALL	センサー	Emerging Threats（新しい脅威）	ユーザーランド フックが、書き込み可能メモリからの API 呼び出しを特定するように設定されています。	アプリケーションがバッファ オーバーフローからのシステム コールを試みました。

タグ	検出箇所	カテゴリ	設定の状態	説明
BYPASS_POLICY	センサー	Emerging Threats（新しい脅威）	特別に作成されたコマンド ライン引数を含んでいるドライバー コールバックを特定しました。	アプリケーションがデバイスのデフォルト セキュリティ ポリシーのバイパスを試みました。
CODE_DROP	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ファイルシステムのフィルター ドライバーが、新しいバイナリやスクリプトの作成をターゲット ファイルの拡張子に基づいて特定するように設定されています。	アプリケーションが実行可能ファイルまたはスクリプトをドロップしました。
COMPANY_BLACKLIST	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	バイナリのハッシュの実行が禁止され、COMPANY_BLACKLIST になりました。	アプリケーションが会社のブラックリストに載っています。
COMPROMISED_PROCESS	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックが、侵害されたアプリケーション（E メール、Office、ブラウザー アプリケーションなど）によってバッファ オーバーフロー、プロセス ハロウイング、またはコード インジェクションを実行するプロセスを特定するように設定されています。	バッファ オーバーフロー、コード インジェクション、プロセス ハロウイングなどのプロセス変更によってプロセスが侵害されています。
COPY_PROCESS_MEMORY	センサー	Data at Risk（データの危険性）	ユーザーランド フックが、他のプロセスのメモリ スナップショットを取得したアプリケーションを特定するように設定されています。	アプリケーションが他のプロセスのメモリ スナップショットを取得しました。

タグ	検出箇所	カテゴリ	設定の状態	説明
DATA_TO_ENCRYPTION	センサー	Data at Risk（データの危険性）	プロセスがランサムウェアおとりファイルの変更を試みます。	Cb Defense がファイルシステムに配置した特別なランサムウェアおとりファイルの 1 つをアプリケーションが変更を試みました。これらのファイルはセンサーで制御されており、Cb Defense 以外のアプリケーションが変更してはなりません。
DETECTED_BLACKLIST_APP	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	検出された実行可能ファイルのハッシュのレピュテーションが COMPANY_BLACKLIST です。	ブラックリストに載っているアプリケーションがファイルシステムで検出されました。
DETECTED_MALWARE_APP	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	検出された実行可能ファイルのハッシュまたはローカル スキャンのレピュテーションが KNOWN_MALWARE です。	マルウェア アプリケーションがファイルシステムで検出されました。
DETECTED_PUP_APP	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	検出された実行可能ファイルのハッシュまたはローカル スキャンのレピュテーションが PUP です。	潜在的に迷惑なアプリケーション（PUP） がファイルシステムで検出されました。
DETECTED_SUSPECT_APP	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	検出された実行可能ファイルのハッシュまたはローカル スキャンのレピュテーションが SUSPECT_MALWARE です。	疑わしいアプリケーションがファイルシステムで検出されました。
DUMP_PROCESS_MEMORY	センサー	Data at Risk（データの危険性）	ユーザーランド API フックが、プロセスのメモリ ダンプを検出するように設定されています。	アプリケーションがファイルシステムで他のプロセスのメモリ ダンプを作成しました。

タグ	検出箇所	カテゴリ	設定の状態	説明
EMAIL_CLIENT	センサー	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーが、E メール プロトコル（SMTP、SMTPS、POP3、POP3S、IMAP、IMAP2、IMAPS など）を使用するクライアント接続を特定するように設定されています。	E メール アプリケーションではないアプリケーション（不明なアプリケーション）が E メール クライアントとして機能し、E メール ポートにデータを送信しています。
ENUMERATE_PROCESSES	センサー	Generic Suspect（一般的な危険性）	ユーザーランド API フックが、プロセス列挙を検出するように設定されています。	プロセスが、ホストで実行中の他のプロセスのリストを取得しようとしています。
FAKE_APP	分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ファイルシステム ドライバーが、正しくないディレクトリから実行されている " 一般に知られている " Windows アプリケーション（explorer、winlogin、lsass など）をパスによって特定するように設定されています。	一般に知られているアプリケーションに偽装している可能性のあるアプリケーション。
FILE_TRANSFER	センサー	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーが、FTP で IPv4 または IPv6 接続を正常に確立、接続、または拒否したことを特定するように設定されています。	アプリケーションがネットワーク経由でファイルを転送しようとしています。
FILE_UPLOAD	分析	Network Threat（ネットワーク脅威）	ユーザーランド フック、ネットワーク フィルター ドライバー、およびファイル システム フィルター ドライバーが、メモリ スクレイピングの後にネットワーク接続を実行するプロセスを特定するように設定されています。	アプリケーションが盗難データをネットワーク経由でアップロードしている可能性があります。

タグ	検出箇所	カテゴリ	設定の状態	説明
FILE_UPLOAD	分析	Network Threat（ネットワーク脅威）	ユーザーランド フック、ネットワーク フィルター ドライバー、およびファイル システム フィルター ドライバーが、デバイスで（なんらかのプロセスによって）メモリ スクレイピングが実行されている間にリモート ネットワーク共有にファイルを作成しているプロセスを特定するように設定されています。	アプリケーションが盗難データをネットワーク経由でアップロードしている可能性があります。
FILELESS	分析	Emerging Threats（新しい脅威）	コマンド ラインまたはレジストリからスクリプトを実行するコマンド ライン引数を含んでいるドライバー コールバックが特定されています。	スクリプト インタープリターがディスクに存在しないスクリプトを操作しています。
FIXED_PORT_LISTEN	センサー	Network Threat（ネットワーク脅威）	IPv4 または IPv6 ネットワーク フィルター ドライバーが、固定ポートで接続をリッスンするように設定されています。	アプリケーションが固定ポートをリッスンしています。
HAS_BUFFER_OVERFLOW	センサー	Emerging Threats（新しい脅威）	ユーザーランド フックが、書き込み可能メモリからの API 呼び出しを特定するように設定されています。	このプロセスでバッファ オーバーフローが発見されました。
HAS_COMPROMISED_CODE	センサー	Process Manipulation（プロセス操作）	COMPROMISED_PROCESS が危険性の高いさまざまな関数のいずれかを呼び出しました。	侵害されたプロセスが複数の関数のいずれかを呼び出しました。
HAS_INJECTED_CODE	分析	Process Manipulation（プロセス操作）	プロセスが侵害された場合、分析がそれを追跡し、別のプロセスにコードを挿入します。	プロセスが挿入されたコードを実行しています。

タグ	検出箇所	カテゴリ	設定の状態	説明
HAS_MALWARE_CODE	センサー（Sensor）	Process Manipulation（プロセス操作）	MALWARE_APP が危険性の高いさまざまな手法のいずれかを使用してプロセスインジェクションを実行しました。	不明なマルウェアによってプロセスが挿入されました。
HAS_PACKED_CODE	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックにより書き込み可能メモリからの API 呼び出しが特定されました。	アプリケーションに動的コード（書き込み可能メモリ。バッファ オーバーフローを除く） が含まれています。
HAS_PUP_CODE	センサー	Process Manipulation（プロセス操作）	PUP_APP がさまざまな手法のいずれかを使用してプロセスインジェクションを実行しました。	PUP によってプロセスが挿入されました。
HAS_SCRIPT_DLL	センサー	Generic Suspect（一般的な危険性）	ドライバー ルーチンが、メモリ内スクリプト インタープリターをロードするプロセスを特定するように設定されています。	プロセスがメモリ内スクリプト インタープリターをロードしています。
HAS_SUSPECT_CODE	センサー	Process Manipulation（プロセス操作）	SUSPECT_APP がさまざまな手法のいずれかを使用してプロセス インジェクションを実行しました。	疑わしいマルウェアによってプロセスが挿入されました。
HIDDEN_PROCESS	センサー	Generic Suspect（一般的な危険性）	定期的なユーザー レベルのプロセス コールが参照できないプロセスに起因するイベント。	センサーが非表示のプロセスを検出しました。
HOLLOW_PROCESS	センサー	Process Manipulation（プロセス操作）	複数のユーザー レベルのフックが、プロセスが他のプロセスに置き換えられることを示す特定のコールのシーケンスを特定するように設定されています。	通常、サスペンド状態のプロセスを作り出し、それを悪意のあるプロセスに置き換えることにより実行される、プロセスの存在を隠すために使用される手法。
IMPERSONATE_SYSTEM	分析	Process Manipulation（プロセス操作）	プロセスに関連付けられているユーザー名が実行中に NT AUTHORITY\\SYSTEM に変更された時点で設定されます。	プロセスに関連付けられたユーザー名を追跡し、関連付けられたユーザー名が system/root に変更されないか監視します。

タグ	検出箇所	カテゴリ	設定の状態	説明
INSTALL	センサー	Generic Suspect（一般的な危険性）	ファイルシステム フィルター ドライバーが、実行可能インストーラーによる新しいバイナリやスクリプトの作成をターゲット ファイルの拡張子に基づいて特定するように設定されています。	インストール プロセスが実行されています。
INJECT_CODE	センサー	Process Manipulation（プロセス操作）	複数のカーネル、OS、およびユーザー レベルの手法が、他のプロセス空間へのコード挿入を試みているアプリケーションを特定するように設定されています。	アプリケーションが他のプロセスにコードを挿入しようとしています。
INJECT_INPUT	センサー	Generic Suspect（一般的な危険性）	ユーザーランド フックが、プロセスに入力を挿入する試みを特定するように設定されています。	アプリケーションが入力をプロセスに挿入しようとしています。
INTERNATIONAL_SITE	分析	Network Threat（ネットワーク脅威）	地域別 IP が、IPv4 および IPv6 接続の接続元や接続先を特定するように設定されています。	アプリケーションが他国（米国を除く）のピア IP アドレスと通信しようとしています。
IRC	センサー	Network Threat（ネットワーク脅威）	IPv4 または IPv6 ネットワーク フィルター ドライバーが、共通の IRC ポートを使用している接続を特定するように設定されています。	アプリケーションがインターネット リレー チャット ポートを介して通信しようとします。
KERNEL_ACCESS	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	プロセスがシステムのマスター ブート レコード（MBR）を変更しようとします。	アプリケーションがシステムのハード ドライブに直接アクセスし、ディスクの MBR 部分にデータを書き込もうとします。マルウェアは、この方法を使用して、起動時にシステムの動作を変更します。

タグ	検出箇所	カテゴリ	設定の状態	説明
KNOWN_APT	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリは APT です。	アプリケーションは高度な永続的脅威です。
KNOWN_BACKDOOR	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリはバックドアです。	アプリケーションはシステムへの既知のバックドアです。
KNOWN_DOWNLOADER	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリはダウンローダーです。	アプリケーションは悪意のある既知のダウンローダーです。
KNOWN_DROPPER	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリはドロッパーです。	アプリケーションは実行可能ファイルの既知のドロッパーです。
KNOWN_KEYLOGGER	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリはキーロガーです。	キーボード入力を監視することで知られているアプリケーションです。

タグ	検出箇所	カテゴリ	設定の状態	説明
KNOWN_PASSWORD_STEALER	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリはパスワード スティーラーです。	パスワードを読み取ることで知られているアプリケーションです。
KNOWN_RANSOMWARE	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリはランサムウェアです。	アプリケーションは既知のランサムウェアです。
KNOWN_ROOTKIT	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリはルートキットです。	アプリケーションは既知のルート キットです。
KNOWN_ROGUE	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリは非承認です。	アプリケーションは既知の非承認アプリケーションです。
KNOWN_WORM	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは KNOWN_MALWARE、カテゴリはワームです。	アプリケーションは既知のワームです。

タグ	検出箇所	カテゴリ	設定の状態	説明
LOW_REPUTATION_SITE	分析	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーが、サイト レピュテーション スコアが低いピア IP アドレスまたはドメインへの接続を特定するように設定されています。	アプリケーションによってレピュテーションの低いピアにネットワークが接続されました。
MALWARE_APP	分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップまたはローカル スキャナーで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは MALWARE です。	アプリケーションは既知のマルウェア アプリケーションです。
MALWARE_DROP	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	CODE_DROP が検出されました。ドロップされたアプリケーションのレピュテーションは KNOWN_MALWARE と SUSPECT_MALWARE のどちらかです。	アプリケーションによってマルウェア アプリケーションがドロップされました。
MODIFY_KERNEL	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックがカーネル領域への変更を行ったプロセスを特定しました。	アプリケーションが Null ページ割り当てによりシステム カーネルを変更しました。
MODIFY_MEMORY_PROTECTION	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックが、副次的なプロセスのメモリ権限を変更するプロセスを検出するように設定されています。	アプリケーションがプロセスのメモリ保護設定を変更しています。
MODIFY_OWN_PROCESS	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックが、自身へのハンドルを開くプロセスを検出するように設定されています。	アプリケーションが自身を変更する権限を使用して独自のプロセスを開くことを試みました。
MODIFY_PROCESS_EXECUTION	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックが、他のプロセスのスレッドの実行コンテキストを変更する試みを特定するように設定されています。	アプリケーションが他のプロセスのスレッド（EAX または EIP）の実行コンテキストを変更しようとしました。

タグ	検出箇所	カテゴリ	設定の状態	説明
MODIFY_PROCESS	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックが、別のプロセスを開こうとしているアプリケーションを特定するように設定されています。	アプリケーションがターゲットのプロセスを変更できる権限を使用して別のプロセスを開くことを試みました。
MODIFY_SENSOR	センサー	Emerging Threats（新しい脅威）	ユーザーランド フック が、Cb Defense センサーを変更または無効化する試みを特定するように設定されています。	改ざんからの保護 - アプリケーションが Cb Defense センサーを変更しようとしました。
MODIFY_SERVICE	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックが、Windows サービスの制御、作成、または削除を試みるアプリケーションを特定するように設定されています。	アプリケーションが Windows サービスを制御、作成、または削除しようとしました。
MODIFY_SERVICE	センサー	Process Manipulation（プロセス操作）	ドライバー コールバックが、システム ユーティリティ アプリケーションを起動してサービスを制御（net.exe stop xxx など）する実行可能ファイルを特定するように設定されています。	アプリケーションがユーティリティ アプリケーションを実行してサービスを制御しようとしました。
MONITOR_MICROPHONE	センサー	Data at Risk（データの危険性）	ユーザーランド フックが、マイクの監視を試みるアプリケーションを特定するように設定されています。	アプリケーションがマイクを監視しようとしました。
MONITOR_USER_INPUT	センサー	Data at Risk（データの危険性）	ユーザーランド フックが、ユーザー入力の監視を試みるアプリケーションを特定するように設定されています。	アプリケーションがユーザー入力（キーボードまたはマウス）を監視しようとしました。
MONITOR_WEBCAM	センサー	Data at Risk（データの危険性）	ユーザーランド フックが、搭載されているカメラの監視を試みるアプリケーションを特定するように設定されています。	アプリケーションが Web カメラを監視しようとしました。

タグ	検出箇所	カテゴリ	設定の状態	説明
NETWORK_ACCESS	センサー	Network Threat（ネットワーク脅威）	IPv4 または IPv6 ネットワーク フィルター ドライバーが、ネットワーク接続を正常に開始したか、または受け入れました。	アプリケーションがネットワーク接続を正常に開始したか、または受け入れました。
NON_STANDARD_PORT	センサー	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーが共通プロトコルのポートを検証しています。http 以外のリクエスト実行をもとに、信頼できないアプリケーションを特定します。	Internet Assigned Numbers Authority（IANA）が指定するポートとは別のポートでのネットワーク トラフィック通過のプロセス。たとえば、通常はポート 21 でリッスンするように構成される FTP をポート 8081 で通す場合など。
PACKED_CALL	センサー	Emerging Threats（新しい脅威）	ユーザーランド フックが、書き込み可能メモリからの API 呼び出しを特定するように設定されています。	アプリケーションが動的コード（書き込み可能メモリ。バッファ オーバーフローを除く）からのシステム コールを試みました。
PACKED_CODE	分析	Process Manipulation（プロセス操作）	スクリプト インタープリターおよびアプリケーションの引数によっては、引数がエンコーディング、難読化、ファイルレス実行などに関連する場合にこれがオンに設定されます。	プロセスに、アンパックされたコードが含まれています。
PERSIST	センサー（Sensor）	Generic Suspect（一般的な危険性）	ファイル システム ドライバーが、再起動時やアプリケーション削除時に持続性を有効にするレジストリ変更（ASEP: Auto-start extensibility points）を特定するように設定されています。	永続的アプリケーション。

タグ	検出箇所	カテゴリ	設定の状態	説明
PHISHING	センサー	Generic Suspect（一般的な危険性）	E メール アプリケーションによって Web ブラウザーが起動されるドライバー コールバックが特定されています。	E メール クライアントによるブラウザーの起動。
PHONE_HOME	センサー	Network Threat（ネットワーク脅威）	IPv4 または IPv6 ネットワーク フィルター ドライバーが、センサーに対してポート スキャンを実行したホストへのクライアント接続を特定するように設定されています。	アプリケーションがスキャニング ホストへの接続を試みています。
POLICY_DENY	センサー	Policy Action（ポリシー アクション）	分析機能はこの情報をセンサーから受信し、それに従ってこの値を設定します。	試みられたアクションは、ポリシーによって阻止されました。
POLICY_TERMINATE	センサー	Policy Action（ポリシー アクション）	分析機能はこの情報をセンサーから受信し、それに従ってこの値を設定します。	プロセスがポリシーによって終了されました。
PRIVILEGE_ESCALATE	分析	Process Manipulation（プロセス操作）	プロセスに関連付けられているユーザー名が実行中に "NT AUTHORITY\\SYSTEM" に変更された時点、またはプロセスが管理権限を獲得した時点で設定されます。	実際のシステム権限が（ユーザー名のコンテキストだけではなく）プロセスに関連付けられているかどうかを確認してください。
PROCESS_IMAGE_REPLACED	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックは、プロセスのメインの実行可能ファイル セクションの上書きやその他の関連操作（セクションのサスペンドやマッピング解除など）に関与する特定の API が起動されるのを監視します。	アプリケーションの主要な実行可能コードが他のコードに置き換えられました。

タグ	検出箇所	カテゴリ	設定の状態	説明
PUP_APP	分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップまたはローカル スキャナーで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは PUP です。	アプリケーションは潜在的に迷惑なプログラムです。
RAM_SCRAPING	センサーおよび分析	Data at Risk（データの危険性）	ユーザーランド フックが、アプリケーションによるプロセス メモリの読み取りの試行を検出するように設定されています。	プロセスが他のプロセスによって使用されているメモリに対してスクレイピングを試みている場合。
READ_PROCESS_MEMORY	センサー	Data at Risk（データの危険性）	ユーザーランド フックが、プロセス メモリを読み取ろうとしているアプリケーションを検出するように設定されています。	アプリケーションがプロセス メモリを読み取ろうとしています。
READ_SECURITY_DATA	センサー	Data at Risk（データの危険性）	ユーザーランド フックが、特権セキュリティ情報を読み取ろうとしているアプリケーションを検出するように設定されています。	アプリケーションが特権セキュリティ情報 （lsass.exe など）を読み取ろうとしています。
REVERSE_SHELL	センサーおよび分析	Emerging Threats（新しい脅威）	ユーザーランド フックが、ネットワーク接続経由でコンソールに対する読み取り/書き込みを行うプロセスを特定するように設定されています。	ネットワーク上の親からコマンドをインターラクティブに受け取っているコマンド シェル（cmd.exe など）。
RUN_ANOTHER_APP	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フックが、別のアプリケーションの実行を試みるアプリケーションを特定するように設定されています。	アプリケーションが別のアプリケーションを実行しようとしました。

タグ	検出箇所	カテゴリ	設定の状態	説明
RUN_BLACKLIST_APP	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フック が、RUN_ANOTHER_APP の実行を試みるアプリケーションを特定するように設定されています。child_proc は COMPANY_BLACKLIST です。	アプリケーションがブラックリストに載っているアプリケーションを実行しようとしました。
RUN_BROWSER	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フック が、RUN_ANOTHER_APP の実行を試みるアプリケーションを特定するように設定されています。child_proc は一般的なブラウザーの実行可能ファイルです。	アプリケーションがブラウザーを実行しようとしました。
RUN_CMD_SHELL	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フック が、RUN_ANOTHER_APP の実行を試みるアプリケーションを特定するように設定されています。child_proc は Windows のシェルです。	アプリケーションがコマンド シェルを実行しようとしました。
RUN_MALWARE_APP	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フック が、RUN_ANOTHER_APP の実行を試みるアプリケーションを特定するように設定されています。child_proc は MALWARE_APP です。	アプリケーションがマルウェア アプリケーションを実行しようとしました。
RUN_NET_UTILITY	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フック が、RUN_ANOTHER_APP の実行を試みるアプリケーションを特定するように設定されています。子ターゲット プロセスは "netsh.exe" などの一般的なネットワーク ユーティリティです。	アプリケーションがネットワーク ユーティリティ アプリケーションを実行しようとしました。

タグ	検出箇所	カテゴリ	設定の状態	説明
RUN_PUP_APP	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フック が、RUN_ANOTHER_APP の実行を試みるアプリケーションを特定するように設定されています。child_proc は PUP_APP です。	アプリケーションが PUP アプリケーションを実行しようとしました。
RUN_SUSPECT_APP	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フック が、RUN_ANOTHER_APP の実行を試みるアプリケーションを特定するように設定されています。child_proc は SUSPECT_APP です。	アプリケーションが疑わしいレピュテーションを持つアプリケーションを実行しようとしました。
RUN_SYSTEM_APP	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フック が、RUN_ANOTHER_APP の実行を試みるアプリケーションを特定するように設定されています。子プロセスはシステム アプリケーション（"windows"、"windows\system32"、"windows\sysWOW64"、"\windows\WinSxS**" ディレクトリに配置されているアプリケーションまたは dll）です。	アプリケーションがシステム アプリケーションを実行しようとしました。
RUN_SYSTEM_UTILITY	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ユーザーランド フック が、RUN_ANOTHER_APP の実行を試みるアプリケーションを特定するように設定されています。child_proc は regedit などのシステム ユーティリティです。	アプリケーションがシステム ユーティリティ（regedit など）を実行しようとしました。

タグ	検出箇所	カテゴリ	設定の状態	説明
SET_APP_CONFIG	センサー	Generic Suspect（一般的な危険性）	ユーザーランド フックが、レジストリ（Microsoft Office セキュリティ キー）を変更するアプリケーションまたはシステム アプリケーション構成パラメーターを設定するアプリケーションを特定するように設定されています。	アプリケーションがシステム アプリケーションの構成パラメーターを設定しました。
SET_APP_LAUNCH	センサー	Generic Suspect（一般的な危険性）	ユーザーランド フックが、他のアプリケーションの起動条件や起動方法に影響を与えるレジストリ（Autoruns キー、Run、RunOnce、Load、Shell および Open コマンド）の変更を試みるアプリケーションを特定するように設定されています。	アプリケーションが他のアプリケーションの起動条件や起動方法に影響を与えるキーを変更しようとしました。
SET_BROWSER_CONFIG	センサー	Generic Suspect（一般的な危険性）	ユーザーランド フックが、レジストリ（ActiveX コントロールのインストール、インターネット設定、システム証明書、Internet Explorer キー、ブラウザー ヘルパー オブジェクト、COM InProcServer）の変更を試みるアプリケーションを特定するように設定されています。	アプリケーションがブラウザー設定を変更しようとしました。
SET_LOGIN_OPS	分析	Emerging Threats（新しい脅威）	Windows ログオン プロセスに関連するキーのレジストリ変更の監視により設定されます。	アプリケーションが Windows ログオンまたはユーザー名に関連するプロセスを変更しようとしました。

タグ	検出箇所	カテゴリ	設定の状態	説明
SET_REBOOT_OPS	センサー	Generic Suspect（一般的な危険性）	ユーザーランド フックが、レジストリ（BootExecute、Session Manager のファイル操作）の変更を試みるアプリケーションを特定するように設定されています。	アプリケーションが再起動構成操作を設定しようとしました。
SET_REMOTE_ACCESS	センサー	Emerging Threats（新しい脅威）	ユーザーランド フックが、レジストリ（SecurePipeServers の winreg の設定、Lanman パラメーターなど）の変更を試みるアプリケーションを特定するように設定されています。	アプリケーションがリモート アクセス構成を設定しようとしました。
SET_SYSTEM_AUDIT	センサー	Generic Suspect（一般的な危険性）	ユーザーランド フックが、レジストリ（TaskManager キー、DisableRegistryTools）の変更を試みるアプリケーションを特定するように設定されています。	アプリケーションがシステム監視パラメーターを設定しようとしました。
SET_SYSTEM_CONFIG	センサー	Generic Suspect（一般的な危険性）	ユーザーランド フックが、レジストリ（Uninstall キー、壁紙など）の変更またはシステム構成データ ファイル（etc\hosts など）の変更を試みるアプリケーションを特定するように設定されています。	アプリケーションがシステム構成パラメーターを設定しようとしました。
SET_SYSTEM_FILE	センサー	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	プロセスがシステムのマスター ブート レコード（MBR）を変更しようとします。	アプリケーションがシステムのハード ドライブに直接アクセスし、ディスクの MBR 部分にデータを書き込もうとします。マルウェアは、この方法を使用して、起動時にシステムの動作を変更します。

タグ	検出箇所	カテゴリ	設定の状態	説明
SET_SYSTEM_SECURITY	センサー	Generic Suspect（一般的な危険性）	ユーザーランド フックが、レジストリ（Autoruns キー、UserInit、Run、RunOnce、Load、BootExecute、AppInit_DLLs、Shell および Open コマンド、Uninstall キー、COM InProcServer、ActiveX コントロールのインストールなど）の変更を試みるアプリケーションを特定するように設定されています。	アプリケーションがシステム セキュリティ操作を設定または変更しようとします。
SUSPECT_APP	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップまたはローカル スキャナーで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは SUSPECT です。また、アプリケーションは署名されていません。	AV により、アプリケーションに悪意がある可能性があることが特定されました。
SUSPENDED_PROCESS	センサー	Process Manipulation（プロセス操作）	ユーザーランド フックが、サスペンド状態で作成されたプロセスを特定するように設定されています。	サスペンド状態で作成されたプロセスが変更されます（実行前）。
SUSPICIOUS_BEHAVIOR	分析	Generic Suspect（一般的な危険性）	ユーザーランド フックが、動的メモリ（バッファ オーバーフローやアンパックされたコードなど）からコードを実行しており、かつ通常はネットワーク上で通信しないアプリケーション（"calc.exe" など）を呼び出してネットワーク通信などを行っているアプリケーションを特定するように設定されています。	通常とは異なるアプリケーションの挙動に注意が必要です。

タグ	検出箇所	カテゴリ	設定の状態	説明
SUSPICIOUS_DOMAIN	センサーおよび分析	Network Threat（ネットワーク脅威）	ネットワーク フィルター ドライバーが、INTERNATIONAL_SITE が ISO 3166-1 国コード（CU、IR、SD、SY、IQ、LY、KP、YE など）の場合を特定するように設定されています。	アプリケーションが疑わしいネットワーク ドメインに接続しています（ISO 3166-1 国コードに基づく）。
SUSPICIOUS_SITE	センサーおよび分析	Network Threat（ネットワーク脅威）	IPv4 または IPv6 ネットワーク フィルター ドライバーが、疑わしい INTERNATIONAL_SITE（RU、CN のドメインなど）からの接続の受け入れを特定するように設定されています。	アプリケーションが疑わしい他国サイトからの受信ネットワーク接続を受け入れます。
UNKNOWN_APP	センサーおよび分析	Malware & Application Abuse（マルウェアとアプリケーションの悪用）	ハッシュ ルックアップで実行中の実行可能ファイルが検出されました。実行可能ファイルのレピュテーションは not_listed（不明）です。また、アプリケーションは署名されていません。	アプリケーションのレピュテーションが不明です。

Appendix B

シグネチャ ミラーの手順

この付録では、Linux および Windows 向けの Cb Defense シグネチャ ミラーの手順について説明します。

ミラー サーバーのハードウェア要件

Cb Defense のミラー サーバーのハードウェア要件は以下のとおりです。

- 2 GHz CPU
- 4 GB RAM

ローカルのミラー サーバーのパフォーマンスは、以下をはじめとするさまざまな要因の影響を受けます。

- ミラー サーバーが更新を行うエンドポイントの数
- ネットワーク帯域幅
- 更新頻度

大規模な環境に対応するために、複数のミラー サーバーを展開できます。

シグネチャ ミラーの手順 （Linux）

このセクションでは、Cb Defense ローカル スキャン シグネチャのローカル リポジトリをミラー化する手順を示します。シグネチャ定義のダウンロードと更新について説明します。

ミラー サーバーは複数台を使用できますが、1 つのポリシーに対して使用できるのは、1 台のミラー サーバーのみです。

前提条件

この手順の前提条件は次のとおりです。

- オペレーティング システムが Linux であること。
- 指定された URL にある HTTP サーバーに定義がホストされていること。この URL は、所定のポリシーの [Local Scanning （ローカル スキャン）] 設定の [Update Servers （更新サーバー）] フィールドに入力します。

シグネチャのミラー化

Cb Defense ローカル スキャン シグネチャのローカル ミラーを作成するには、次の手順に従います。

1. `cbdMirrorServerUtil_v2.2.zip` パッケージを https://community.carbonblack.com/docs/DOC-5950 からダウンロードします。パスワードは "cbdefense_mirror" です。
2. お使いの Linux システムのアーキテクチャに適したパッケージを選択します。
3. 次のファイルを Linux システムに配置します。

- avupdate_msg.avr
- avupdate.bin
- HBEDV.KEY
- update_1.cfg
- update_2.cfg
- update_defs.sh

4. 次のコマンドを使用して新しいシグネチャ ミラーを作成します。

   ```
   ./update_defs.sh some_dir
   ```

5. 任意の HTTP サーバーを使用して some_dir ディレクトリを提供します。
6. some_dir ディレクトリを表す URL を指すように [Update Servers （更新サーバー）] フィールドを更新します。

注意

ステップ 4 のコマンドを数時間ごとに実行して当社のミラーから最新の更新を取得することを推奨します。

シグネチャ ミラーの手順 （Windows）

このセクションでは、Cb Defense ローカル スキャン シグネチャのローカル リポジトリをミラー化する手順を示します。シグネチャ定義のダウンロードと更新について説明します。

ミラー サーバーは複数台を使用できますが、1 つのポリシーに対して使用できるのは、1 台のミラー サーバーのみです。

前提条件

この手順の前提条件は次のとおりです。

- オペレーティング システムが 64 ビット Windows であること。
- 指定された URL にある HTTP サーバーに定義がホストされていること。この URL は、所定のポリシーの [Local Scanning （ローカル スキャン）] 設定の [Update Servers （更新サーバー）] フィールドに入力します。

シグネチャのミラー化

Cb Defense ローカル スキャン シグネチャのローカル ミラーを作成する：

1. `cbdMirrorServerUtil_v2.2.zip` パッケージを https://community.carbonblack.com/docs/DOC-5950 からダウンロードします。
2. zip ファイルを解凍します。さらに 3 つの zip ファイルがあります。Windows の場合、`cbdMirrorServerUtil_win_x64.zip` という zip ファイルを使用します。
3. 次のファイルを一時フォルダーに展開します。
   - `upd_msg.avr`
   - `upd.exe`
   - `avupdate.dll`
   - `msvcr120.dl`
   - `HBEDV.KEY`
   - `do_update.bat`
4. AV シグネチャの更新ファイル用のディレクトリを作成します。
5. 管理者としてコマンド プロンプト ウィンドウを開き、次のコマンドを使用して新しいシグネチャ ミラーを作成します。

   `cd \{ 一時フォルダー }`

   `do_update.bat { ステップ 4 で作成したフォルダー }`

   ステップ 4 で作成したフォルダーには、次のフォルダーが作成されます。
   - `32`
   - `64`
   - `ave2`
   - `idx`
   - `x_vdf`
6. IIS Web サイトを作成します。
   a. IIS マネージャーを開きます。
   b. [サイト] を右クリックし、[Web サイトの追加] をクリックします。
   c. この Web サイトが AV シグネチャの更新用であることがわかるサイト名を指定します。
   d. [アプリケーション プール] フィールドは **DefaultAppPool** のままにします。

e. [物理パス] では、ステップ 4 で作成したディレクトリを参照します。
f. [種類] = [http]、[IP アドレス] = [未使用の IP アドレスすべて]、[ポート] = 80 のままにします。
g. [ホスト名] フィールドに、ミラー サーバーの名前を入力します。
h. [Web サイトを直ちに開始する] を選択します。
i. [OK] をクリックします。
j. IIS ナビゲーション パネルの [サイト] で、ステップ 6c で設定したサイト名を選択します。
k. [ディレクトリの参照] をダブルクリックし、[有効] をクリックします。
l. [MIME の種類] をダブルクリックします。
m. 拡張子が `.idx` で種類が **text/plain** の新しい MIME の種類を追加します。

7. コマンド プロンプト ウィンドウで、 `iisreset` コマンドを実行します。
8. ステップ 6 の URL が機能することをテストするために、ブラウザーを開き、「**http://{** *ステップ 6g のホスト名* **}**」と入力します。ステップ 5 で作成したフォルダーが表示されることを確認します。

注意

`do_update.bat` では Cb Cloud から最新の更新が 1 回のみダウンロードされるため、Windows のタスク スケジューラなどのアプリケーションを使用して、ミラー サーバーで毎日指定した時刻にスクリプトが自動的に実行されるようにすることをお勧めします。こうすると、ミラー サーバーに最新のシグネチャ更新が常に適用されるようになります。このコマンドは、`%TEMP%\scanner\upd.log` にログ ファイルを生成してログを追加します。問題のトラブルシューティングにこのログ ファイルを使用できます。

ポリシー設定の [Local Scanning （ローカル スキャン）] パネルの [Update Servers Master （更新サーバー マスター）] チェックボックスは、ミラー サーバーへの接続に影響する場合があります。ミラー サーバーから更新されたシグネチャを受け取ることができないセンサーがある場合は、このチェックボックスをオンまたはオフに切り替えることで、問題が解決します。

Appendix C

バックグラウンド スキャンの仕様

この付録には、Windows および macOS エンドポイントのバックグラウンド スキャンの仕様が記載されています。

バックグラウンド スキャンは、ポリシー単位で有効になります。

ポリシーのバックグラウンド スキャンを有効にする：

1. PSC にログインし、[Enforce （適用）] をクリックして [Policies （ポリシー）] をクリックします。
2. 左側の [Policy （ポリシー）] パネルで、バックグラウンド スキャンを有効にするポリシーをクリックします。
3. 右側のパネルで、[Run background scan （バックグラウンド スキャン実行）] チェックボックスをオンにします。[Save （保存）] をクリックします。

オンにした場合、センサーは最初の 1 回限りのインベントリ スキャンをバックグラウンドで実行し、エンドポイント上の既存のマルウェア ファイルを特定します。この機能を使用すると、センサーをインストールするエンドポイント上に存在する既存のファイルをより効果的にマルウェアから保護できます。

標準バックグラウンド スキャンは、（エンドポイント上のファイルの数に応じて）完了までに 3 ～ 5 日間かかり、システム リソースの消費量が少ない低優先度モードで実行されます。このスキャンの使用が推奨されます。

高速スキャン オプションは、24 時間で完了します。テストや緊急事態でのみ推奨されます。これを使用した場合、システム パフォーマンスに影響が生じます。高速スキャンは、Windows センサー バージョン 3.3 以降にのみ適用できます。

バックグラウンド スキャンは、ポリシーの変更が適用されるとすぐに始まります。そのポリシーを使用してセンサーを展開した場合は、インストール後すぐにスキャンが始まります。

現在のバックグラウンド スキャンの状態は、NT イベント ログまたは syslog に "BACKGROUND_SCAN" タグ付きで記録されます。RepMgr により、スキャンの起動時のステータスが記録され、それ以降は 24 時間ごとにステータスが記録されます。スキャン完了時のステータス メッセージは "BACKGROUND_SCAN:COMPLETE （BACKGROUND_SCAN: 完了）" です。

Windows バックグラウンド スキャンの仕様

Windows スキャン ファイル タイプ

バイナリ ファイル

- dll
- exe
- sys
- drv
- scr
- pif
- ex_

スクリプト ファイル

- com
- hta
- inf
- ins
- isp
- jar
- msi
- ocx
- pl
- py
- reg
- vb
- vbe
- vbs
- ws
- wsf
- wsh
- ps1
- ps1xml
- psc1
- psd1
- psm1

データ ファイル

- pdf

ユーザー ファイル

- tax
- iif

企業ファイル

- pdf
- pps
- ppsm
- ppsx
- ppt
- pptm
- pptx
- rtf
- swf
- xls
- xlsx
- xlsm （まだ追加されていません）
- xlsb （まだ追加されていません）
- dme
- frm
- ldf
- mdb
- mdf
- myd
- myi
- ndf
- opt

E メール ファイル

- dbx
- mbx
- ost
- pst
- snm
- toc
- edb
- oeb

連絡先ファイル

- wab
- pab
- mab
- contact
- mml
- vcf
- aba
- na2
- ldif
- abbu
- aby
- olk

カレンダー ファイル

- ics
- icbu
- cal
- ical
- wcd
- dba

macOS バックグラウンド スキャンの仕様

macOS スキャン ファイル タイプ

macOS センサーでは、ファイル マジック ヘッダー検出とファイル拡張子の両方に基づいて、バックグラウンド スキャンによるスキャンの対象となるファイル タイプが判定されます。

マジック ヘッダー検出は、ファイルに拡張子がない場合や、任意の （難読化された）拡張子が付けられている場合に使用されます。

バイナリ ファイル

- Apple 実行可能ファイル
- Apple ドライバー拡張機能
- Apple 動的ライブラリ
- Windows 実行可能ファイル
- Windows 動的ライブラリ

インストーラー ファイル

- Apple インストーラー （DMG、PKG）
- 拡張子でのみ : Windows MSI ファイル、Android APK インストーラー

Windows スクリプト ファイル （拡張子でのみ）

- bat
- chm
- cmd
- com
- hta
- inf
- ins
- isp
- ocx
- reg
- vb
- vbe
- vbs
- ws
- wsf
- wsh
- ps1
- ps1xml
- psc1
- psd1
- psm1

スクリプト ファイル

- java （クラスおよび jar）
- Perl
- Python
- PHP
- Ruby
- Shell
- AppleScript
- インタープリターの関連付けを示す "#!" ファイル ヘッダーを含む他のスクリプト ファイル

データ ファイル

- Adobe PDF
- MS Office
- Open Office

Appendix D

Cb Defense for VMware

この付録では、Cb Defense が提供する Cb Defense for VMware と VMware AppDefense との統合機能について説明します。

この内容は、Cb Defense for VMware 製品にのみ適用されます。

概要

Cb Defense for VMware の VMware AppDefense 統合機能を使用すると、セキュリティ チームおよび IT 運用管理チームは、複数のゲストに対応する複雑なアプリケーション、関連するネットワーク トラフィック、およびエンドポイントの疑わしい動作に対する可視性を高めることができます。AppDefense と Cb Defense for VMware の両方を使用して SDDC を保護することが、推奨されるセキュリティ ガバナンスのベスト プラクティスとなります。

この統合により、次のことが実現されます。

- 関連するアプリケーション コンテキストと VMware の詳細を直接 Cb Defense に提供することで、アラートのトリアージ プロセスの平均解決時間（MTTR）を削減します。この統合により、重大なアラートが Cb Defense から AppDefense コンソールに転送され、AppDefense アラームが Cb Defense 管理コンソールに転送されることで、可視性が高まります。AppDefense の修復アクションを直接 Cb Defense 管理コンソールから適用することも、その逆も可能です。
- IT およびセキュリティ運用管理チームがソフトウェア定義データ センターで標準化されたセキュリティ制御を確実に行えるよう支援します。

VMware AppDefense は、VMware ハイパーバイザーを使用して、仮想マシン ゲストで目的のアプリケーションの状態をあらゆるレベル（OS カーネル、プロセスの動作、およびネットワーク接続）で監視するデータ センター セキュリティ ツールです。AppDefense では、ゲストのワークロードを個別に表示しません。代わりに、より幅広いアプリケーションの範囲の一部としてワークロードを管理します。これにより、個々のマシンの動作ではなく、データ センターにおけるインターラクティブな動作をより詳しく把握できます。

一般的な概念

Cb Defense と AppDefense には多くの類似点があります。ただし、いくつかの重要な違いもあります。このセクションでは、Cb Defense と AppDefense の動作と用語の違いについて説明します。

- ホワイトリストへの追加は、Cb Defense のアクションです。Cb Defense では組織レベルでアプリケーションをホワイトリストに登録します。このことが AppDefense 設定に影響することはありません。“ レピュテーションの管理 ” を参照してください。
- プロセスの許可は AppDefense のアクションです。これにより、特定の AppDefense の範囲にある特定の AppDefense サービスのために、AppDefense でアプリケーションをホワイトリストに登録します。このことが Cb Defense 設定に影響することはありません。
- 動作の許可は AppDefense のアクションです。これにより、アプリケーションによる（プロセス、IP アドレス、ポートで構成される）細かい動作を AppDefense でホワイトリストに登録できます。このことが Cb Defense 設定に影響することはありません。

デバイスを隔離するには、次の 2 つの方法があります。Cb Defense による隔離を使用する方法と、VMware NSX による隔離 （デバイスに対して有効な場合）を使用する方法です。“ 仮想マシンの隔離 ” を参照してください。

AppDefense は、次の条件に基づいて AppDefense 深刻度スコアを Cb Defense アラートに割り当てます。このマッピングは、Cb Defense 管理コンソールで Cb Defense アラートに対する AppDefense アラームの並べ替えやフィルターにも使用されます。

表 30: AppDefense 深刻度スコア

AppDefense 深刻度レベル	Cb Defense アラート優先度スコア
情報	1
マイナー	4
深刻	7
重大	9

グループ化されたアラートおよびアラーム

すべての Cb Defense アラートはグループ化できます。

AppDefense アラームの範囲、サービス、デバイス、アラーム タイプ、プロセス名、およびプロセス パスが同じである場合、それらのアラームはグループ化できます。以下の AppDefense アラーム タイプをグループ化できます。

- 受信接続
- 送信接続
- プロセス監視

アラームがグループ化されている場合、ページ上部にアラームの合計数が表示されます。AppDefense でアラームを表示するには、ページ上部の [AppDefense] アイコンをクリックします。

“ 複数のデバイスにおけるアラートの管理 ” を参照してください。

用語

次の表に示すように、Cb Defense と AppDefense では、それぞれ異なる用語を使用しています。

表 31: Cb Defense と AppDefense の用語

Cb Defense	AppDefense
アラート	アラーム
デバイス （OS ホスト名）	メンバー （仮想マシン名）
棄却	クリア

Cb Defense では、" ホスト名 " は、デバイスのオペレーティング システムのホスト名を指します。VMware では、" ホスト名 " は vCenter の仮想マシン名を指します。

要件

Cb Defense for VMware では、次の VMware 仮想マシン構成が必要です。

- Windows Server 2008 R2 以降のオペレーティング システム
- vCenter 6.5 以降
- vSphere ESXi 6.5 以降
- VMware Tools
- VM ハードウェア バージョン 13 以降
- AppDefense ホスト モジュール、ゲスト モジュール、およびアプライアンスの最新バージョンは、AppDefense コンソールのダウンロード セクションから入手できます。

注意

AppDefense の一番の目的は、インフラストラクチャではなく、アプリケーション関連のセキュリティを構成することです。そのため、AppDefense では、未サポートの仮想マシンが SDDC アプリケーションに属している場合に、これらの仮想マシンを AppDefense の範囲とサービスに追加できます。ただし、上記の要件に適合しない仮想マシンは、AppDefense で保護することができません。

VMware 統合の有効化

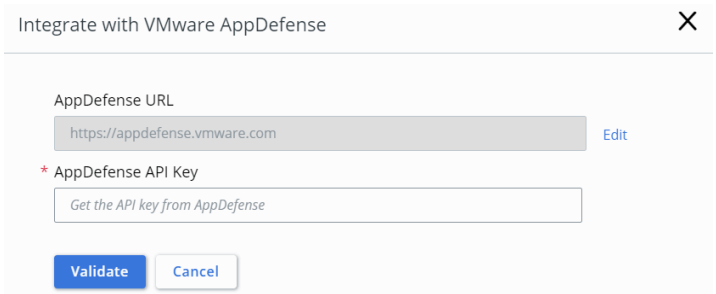
統合を有効化するには、VMware によって AppDefense がプロビジョニングされていなければなりません。

Cb Defense for VMware を購入し、VMware によって AppDefense がプロビジョニングされた後に、統合を有効化する必要があります。統合の有効化と無効化には、完全な Cb Defense 管理者特権が必要です。

VMware 統合を有効化する :

1. PSC にログインし、[Settings（設定）] をクリックして [VMware] をクリックします。

   注意 :[VMware] タブは、Cb Defense for VMware 製品のライセンスを購入した場合にのみ表示されます。このライセンスを購入しても [VMware] タブが表示されない場合は、Cb Defense の担当者にお問い合わせください。
2. [Start （開始）] をクリックし、EULA に同意します。[Submit （送信）] をクリックします。
3. [Integrate with VMware AppDefense（VMware AppDefense との統合）] ダイアログが表示されます。[AppDefense URL （AppDefense の URL）] が自動的に入力されます。ベータ プログラムまたは POC に参加していて URL の編集を指示された場合を除き、デフォルトの URL を受け入れます。



4. 必要な **AppDefense API キー**を収集するには、VMware AppDefense に移動して、ページの左下隅にある歯車をクリックします。[Integrations （統合）] をクリックし、[Provision New API Key（新しい API キーのプロビジョニング）] をクリックします。生成されたキーがテキスト ファイルに表示されます。このキーをコピーして [AppDefense API Key （AppDefense API キー）] フィールドに貼り付け、[Validate（検証）] をクリックします。仮想マシンのリストが表示されます。

   注意 : 仮想マシンの数が多い場合は、リストが作成されるまでに数分かかることがあります。

VMware 統合を解除することもできます。この操作は、次の場合に実行します。

- 環境から AppDefense を削除する場合。
- AppDefense で新しい AppDefense API キーが生成された場合。
- 技術的なトラブルシューティングを行う場合。

重要

統合を無効化すると、関連するすべての VMware とアプリケーション コンテキストのデータが削除されます。

VMware 統合を解除する :

1. PSC にログインし、[Settings（設定）] をクリックして [VMware] をクリックします。
2. [Remove Integration （統合の解除）] をクリックし、解除を確認します。

VMware アラートの表示

VMware アラートには、このセクションで説明するように複数のビューがあります。

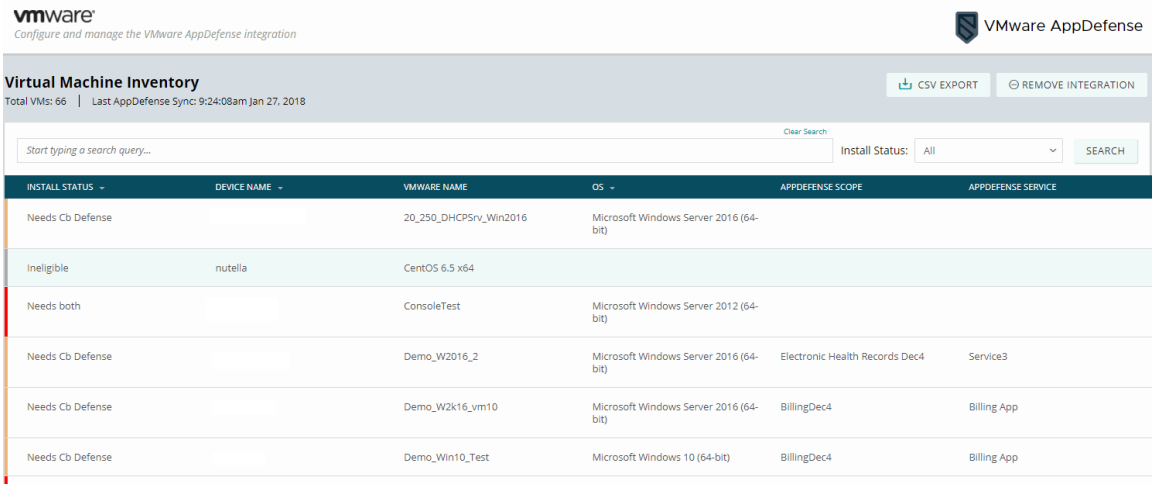
Cb Defense での VMware インベントリの表示

Cb Defense for VMware を有効化した後、[Cb Defense VMware] ページに VMware 仮想マシンの並べ替え可能なリストを表示できます。

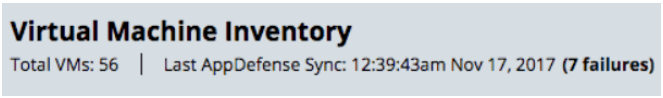
VMware インベントリを表示する：

1. PSC にログインし、[Settings（設定）] をクリックして [VMware] をクリックします。

   Cb Defense が AppDefense と最後に同期した日時と、統合に存在している仮想マシンの総数を確認できます。



同期は数分ごとに行われます。同期に成功しなかった場合は、最後に同期に成功した日時がページに表示されます。この場合、失敗した同期の試行回数が表示されます。



5 回以上同期の試行に失敗している場合は、かなりの時間 AppDefense との接続が行われていないことを意味します。

仮想マシンを検索し、表示されたリストを CSV ファイルにエクスポートできます。また、選択したインストール ステータスに一致する仮想マシンのみを表示することもできます。次の表に、**インストール ステータス**のオプションを示します。

AppDefense 内の仮想マシンに関する詳細な情報を収集するには、Cb Defense から直接 [Scope Name （範囲の名前）] ハイパーリンクをクリックします。

表 32: VMware 仮想マシンのインストール ステータス

Status	説明
All （すべて）	すべての VMware 仮想マシンが表示されます。
Both Installed（両方ともインストール済み）	Cb Defense と AppDefense が、両方ともこの仮想マシンにインストールされています。Cb Defense および AppDefense コンソールですべての統合機能が有効化されています。
Needs one or both（一方または両方が必要）	仮想マシンは AppDefense および Cb Defense の保護対象であり、両方の製品をサポートしますが、どちらかがインストールされていません。 仮想マシンは、次のいずれかの状態です。 • Cb Defense がインストールされていますが、AppDefense をサポートしていません （たとえば、仮想マシンが未サポートのバージョンのオペレーティング システム、vSphere、または vCenter を実行しています）。 • AppDefense がインストールされていますが、Cb Defense をサポートしていません （たとえば、Linux 仮想マシンです）。
All Eligible Installed（保護対象にすべてインストール済み）	すべての保護対象の仮想マシンに Cb Defense または AppDefense がインストールされていますが、Cb Defense と AppDefense の両方をインストールする要件を満たしていません。 デバイスが Cb Defense の保護対象であっても AppDefense の保護対象ではない場合に、Cb Defense がインストールされていると、インストール ステータスは [All Eligible Installed （保護対象にすべてインストール済み）] になります。 デバイスが AppDefense の保護対象であっても Cb Defense の保護対象ではない場合に、AppDefense がインストールされていると、インストール ステータスは [All Eligible Installed（保護対象にすべてインストール済み）] になります。
Needs Cb Defense（Cb Defense が必要）	仮想マシンに AppDefense がインストールされていて、Cb Defense のインストールが可能ですが、現在 Cb Defense がインストールされていません。
Needs AppDefense（AppDefense が必要）	仮想マシンに Cb Defense がインストールされていて、AppDefense のインストールが可能ですが、現在 AppDefense がインストールされていません。
Needs Both（両方とも必要）	仮想マシンは AppDefense および Cb Defense の両方の保護対象ですが、両方ともインストールされていません。
Ineligible （保護対象外）	仮想マシンは AppDefense および Cb Defense による保護の対象ではありません。
VMware Tools Missing（VMware Tools なし）	仮想マシンに VMware Tools がインストールされていません。VMware Tools は、インストール ステータスを判断するための前提条件となります。したがって、インストール ステータスを判断できません。

インストール ステータスは、仮想マシンに対して必要なアクションを示すために色分けされています。この色分けは、セキュリティ ガバナンスのベスト プラクティスに基づいています。

[Install Status （インストール ステータス）] の左にある色分けされた行に、以下の仮想マシン ステータスが表示されます。

表 33: VMware 仮想マシンの色分け

色	意味	対応するインストール ステータス
緑	データ センターに対して確実にセキュリティ ガバナンスのベスト プラクティスを実施するためのアクションは必要ありません。	• Both Installed （両方ともインストール済み） • All Eligible Installed （保護対象にすべてインストール済み）
オレンジ	セキュリティ ガバナンスのベスト プラクティスに従うために、なんらかのアクションが必要となる可能性があります。	• Needs Cb Defense （Cb Defense が必要） • Needs AppDefense （AppDefense が必要）
赤	仮想マシンに最小限のセキュリティを施すために、なんらかのアクションを行う必要があります。	• Needs Both （両方とも必要）
灰色	仮想マシンが保護対象外であるか、システムに仮想マシンに関する十分な情報がなく、推奨するアクションを行う必要があるかどうか判断できません。“ 要件 ” を参照してください。	• Ineligible （保護対象外） • VMware Tools がありません

注意

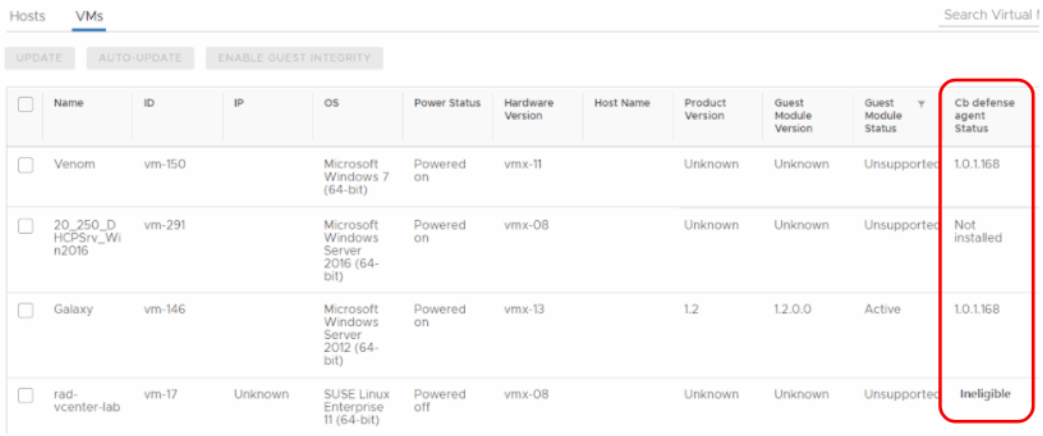
インストール ステータス フィルター [Needs one or both（1 つまたは両方が必要）] は、特定の色に対応付けされていません。これには、[Needs both（両方とも必要）] ステータス （赤）、[Needs Cb Defense （Cb Defense が必要）] ステータス （オレンジ）、および [Needs AppDefense （AppDefense が必要）] ステータス （オレンジ）が含まれます。

仮想マシンのリストには、次の表で説明する情報が含まれています。

表 34: 仮想マシンのデータ

[Title（タイトル）]	説明
Install Status（インストール ステータス）	仮想マシンのインストール ステータス。表 32、「VMware 仮想マシンのインストール ステータス」を参照してください。
Device Name（デバイス名）	仮想マシンのオペレーティング システム ホスト名。
VMware Name（VMware 名）	仮想マシンの vCenter 名。
OS	仮想マシン上で実行されているオペレーティング システムのバージョン。
AppDefense Scope（AppDefense の範囲）	仮想マシンに適用される AppDefense の範囲。
AppDefense Service（AppDefense サービス）	仮想マシンを実行している AppDefense サービス。

AppDefense では、非管理のアセットを表示するアラートのインベントリ ビューが提供されています。



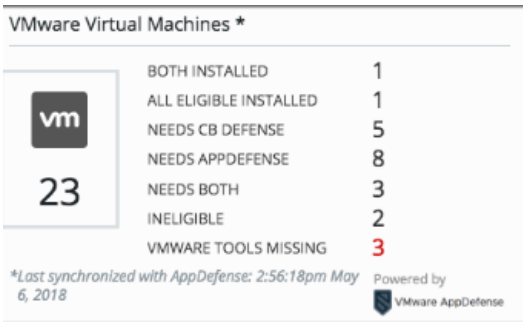
[Cb Defense Agent Status（Cb Defense エージェントのステータス）] 列には、仮想マシン上の Cb Defense センサーのステータスが示されます。これは、次のいずれかです。

- インストールされている Cb Defense センサーのバージョン。
- [Eligible （保護対象）] - Cb Defense オペレーティング システムの要件に基づいて、この仮想マシンは Cb Defense の保護対象になっていますが、Cb Defense センサーがインストールされていません。
- Cb Defense オペレーティング システムの要件に基づいて、Cb Defense センサーの保護対象外です。

ダッシュボードでの VMware 仮想マシン情報の表示

Cb Defense ダッシュボードには、Cb Defense に登録されている VMware 仮想マシンの総数や仮想マシンのインストール ステータスなど、VMware 仮想マシンの情報を表示できます。

VMware Tools がインストールされていない仮想マシンがある場合は、[VMware Tools Missing （VMware Tools なし）] が表示され、VMware Tools のない仮想マシンの数が示されます。



カテゴリに含まれている特定の仮想マシンを表示するには、インストール ステータスをクリックします。[VMware] ページにそのステータスの仮想マシンのリストが表示されます。“VMware アラートの表示 ” を参照してください。

インストール ステータスの状態については、“VMware 仮想マシンのインストール ステータス ” を参照してください。

注意

ダッシュボード上の VMware データは、CSV ファイルにダウンロードすることはできません。

VMware 仮想マシン センサーの表示

組織全体に展開したセンサーを表示できます。

センサーを表示する :

1. PSC にログインし、**[Endpoints （エンドポイント）]** をクリックします。

   デバイスの並べ替え可能なリストが表示されます。“ 展開したセンサーの表示 ” を参照してください。

センサーの横にある 「**>**」をクリックすると、追加情報を表示できます。

VMware 仮想マシンの場合、基本センサー データの下に表示される追加情報には、表 35、「VMware メタデータ」に記載されているメタデータも含まれます。AppDefense が VMware 仮想マシンにインストールされていない場合、VMware AppDefense のロゴ、AppDefense のバージョン、および AppDefense のステータスは表示されません。

アラートの表示および修復

2 種類の VMware アラートが Cb Defense 管理コンソールに表示されます。これらには以下のものがあります。

- AppDefense がインストールされているデバイスに対する Cb Defense アラート。“AppDefense がインストールされているデバイスに対する Cb Defense アラートの操作 ” を参照してください。
- 保護モードの範囲を持つ、次のいずれかのタイプの AppDefense アラーム :
  - 受信接続
  - 送信接続
  - プロセス監視
  - ゲスト整合性
  - ホスト整合性

  “Cb Defense での AppDefense アラームの操作 ” を参照してください。

アラートの操作方法の詳細については、このユーザー ガイドの次のセクションを参照してください。

- “ アラートの表示およびアラートに対するアクションの実行 ”.
- “ アラートの視覚的表示 ”.
- “ アラートの調査 ”.

アラート リスト ページでアラートを検索する方法については、「アラートの検索」(34 ページ) を参照してください。

AppDefense がインストールされているデバイスに対する Cb Defense アラートの操作

アラート リスト ページでの VMware メタデータの表示

注意

VMware 仮想マシンに対する Cb Defense アラートは、AppDefense コンソールにも表示されます。“VMware AppDefense での Cb Defense アラートの表示 ” を参照してください。

VMware 仮想マシンで発生したアラートの場合は、追加のメタデータが表示されます。

VMware メタデータを表示する :

1. アラート リスト ページに移動します。

   注意 : アラートをフィルターして VMware アラートのみを表示するには、左側のパネルで [VMware Virtual Machines （VMware 仮想マシン）] フィルターをクリックします。次の深刻度レベルに基づいて、VMware アラートをフィルターすることもできます。レベルは、[Info （情報）]、[Minor （マイナー）]、[Serious （深刻）]、[Critical （重大）] です。デフォルトで Cb Defense 脅威が選択されます。
2. VMware 仮想マシンで発生したアラートを選択します。
3. [VM Virtual Machine （VM 仮想マシン）] タブをクリックします。次の情報が表示されます。

表 35: VMware メタデータ

メタデータ	説明	関連性
Install Status（インストール ステータス）	仮想マシンのインストール ステータス。表 32、「VMware 仮想マシンのインストール ステータス」を参照してください。	セキュリティ ガバナンス
VM Name（VM 名）	vCenter で仮想マシン名に割り当てられた名前。	仮想マシンの識別
VM ID	VMware の内部識別子で、vSphere によって生成されます。	仮想マシンの識別
VM UUID	仮想マシンに対して vCenter が作成した一意の識別子。	仮想マシンの識別
vCenter UUID	仮想マシンを管理する vCenter インスタンスの一意の識別子。	仮想マシンの識別
MAC address（MAC アドレス）	仮想マシンの MAC アドレス。	仮想マシンの識別
AppDefense Version（AppDefense のバージョン）	仮想マシン上で実行されている AppDefense エージェントのバージョン（ゲスト モジュール）。	統合の詳細
AppDefense Status（AppDefense のステータス）	仮想マシン上で実行されている AppDefense エージェントのステータス。ステータスは、[Running （実行中）]、[Unloaded （アンロード済み）]、または [Disconnected （接続されていない）] になります。	統合の詳細
Scope Name（範囲名）	AppDefense がこの仮想マシンに割り当てた VMware の範囲の名前。	コンテキスト
Scope State（範囲の状態）	仮想マシンに適用される範囲の状態。 検出モードでは一定の期間内に、許可された動作が学習されます。 保護モードでは、ルールが範囲に適用されます。違反があると、アラームが生成されます。	コンテキスト
Service Name（サービス名）	仮想マシンが実行されている、AppDefense が割り当てた VMware サービスの名前。	コンテキスト
Service Type（サービス タイプ）	VMware のサービス タイプ。	コンテキスト
VMs in Service（サービス内の VM）	識別された AppDefense サービスの一部となっている仮想マシンの総数。	コンテキスト

アラート リスト ページの詳細については、“ アラートの表示およびアラートに対するアクションの実行 ” を参照してください。

注意 : すべての既知の VMware 仮想マシンには、AppDefense の最小要件に適合しない場合でも、Install Status （インストール ステータス）、VM name （VM 名）、VM ID、VM UUID、vCenter UUID、および MAC Address （MAC アドレス） が含まれています。AppDefense による保護の対象にならない仮想マシンには、AppDefense の範囲およびサービスに追加されている場合、**範囲**および**サービス**に関する情報も含まれています。ただし、AppDefense Version （AppDefense のバージョン） と AppDefense Status （AppDefense のステータス）が含まれているのは、AppDefense がインストールされている仮想マシンのみです。

AppDefense がインストールされているデバイスに対する Cb Defense アラートの調査

[Investigate （調査）] ページでアラートを調査できます。[Investigate （調査）] ページには、**アラート リスト** ページまたは**ナビゲーション** パネルからアクセスできます。“ アラートの調査 ” を参照してください。

VMware 仮想マシンで発生したアラートの場合は、追加のメタデータが表示されます。

VMware メタデータを表示する :

1. [Investigate （調査）] ページに移動します。
2. VMware 仮想マシンで発生したアラートを選択します。
3. [VM Virtual Machine （VM 仮想マシン）] タブをクリックします。表 35、「VMware メタデータ」を参照してください。

AppDefense がインストールされているデバイスに対する Cb Defense アラートの視覚的表示

他のアラートを視覚的に表示するのと同じ方法で、AppDefense がインストールされているデバイスに対するアラートを視覚的に表示できます。“ アラートの視覚的表示 ” を参照してください。

ノードは、[Alert Triage （アラートのトリアージ）] ページの [Process Graph （プロセスグラフ）] パネルに VM ラベルとともに表示されます。このノードをクリックすると、アラートをホストした仮想マシンについて VMware の追加情報を表示できます。この情報については、表 35、「VMware メタデータ」で説明します。

以下の方法でメタデータを使用すると、アラートのトリアージを行うことができます。

表 36: メタデータを使用してアラートのトリアージを行う方法

メタデータ	用途	カテゴリ
Install Status （インストール ステータス）	セキュリティ ガバナンスのベスト プラクティスに従う （Cb Defense と AppDefense の両方をインストールする）ためにアクションが必要かどうかを判断するのに役立ちます。	セキュリティ ガバナンス
AppDefense Version （AppDefense のバージョン）	この値を見て、適切なバージョンを実行しているかどうかを確認できます。これは、特にトラブルシューティングで役立ちます。このフィールドは、AppDefense が仮想マシンにインストールされている場合にのみ入力されます。	統合の詳細

メタデータ	用途	カテゴリ
AppDefense Status（AppDefense のステータス）	トラブルシューティング時に使用すると、予期したとおりに AppDefense エージェントが通信しているかどうかを判断できます。このフィールドは、AppDefense が仮想マシンにインストールされている場合にのみ入力されます。	統合の詳細
VM Name（VM 名）	VMware 製品の仮想マシンをすばやく見つけることができます。	仮想マシンの識別
VM ID	VMware 製品の仮想マシンをすばやく見つけることができます。	仮想マシンの識別
VM UUID	VM UUID と vCenter UUID を組み合わせると、仮想マシンが属している vCenter がわからなくても、VMware インフラストラクチャ内の仮想マシンを検索し、すばやく見つけることができます。	仮想マシンの識別
vCenter UUID	VM UUID と vCenter UUID を組み合わせると、仮想マシンが属している vCenter がわからなくても、VMware インフラストラクチャ内の仮想マシンを検索し、すばやく見つけることができます。	仮想マシンの識別
MAC Address（MAC アドレス）	ネットワーク サブネット上の各デバイスには、一意の MAC アドレスがあります。MAC アドレスは変更されることがないため、ネットワークの問題を診断する場合に役立ちます。	仮想マシンの識別
Scope Name（範囲名）	AppDefense の範囲は、この仮想マシンが属している SDDC アプリケーションを特定するのに利用できます。この情報は、仮想マシンがビジネス上重要なシステムに及ぼす影響を把握するのに役立ちます。	コンテキスト
Scope State（範囲の状態）	AppDefense によって仮想マシンがアクティブに保護されているかどうかを示します。	コンテキスト
Service Name（サービス名）	この仮想マシンが属している AppDefense の範囲内のサービスを示します。この情報は、仮想マシンがビジネス上重要なシステムに及ぼす影響を把握するのに役立ちます。	コンテキスト
Service Type（サービス タイプ）	サービスの処理を示します。この情報は、仮想マシンがビジネス上重要なシステムに及ぼす影響を把握するのに役立ちます。	コンテキスト
VMs in Service（サービス内の VM）	サービスに組み込まれている冗長性の程度を示します。この情報は、仮想マシンがビジネス上重要なシステムに及ぼす影響を把握するのに役立ちます。	コンテキスト

次の例では、[Alert Triage （アラートのトリアージ）] ページの [Selected Process （選択したプロセス）] パネルに表示される情報を使用してアラートのトリアージを行う方法について説明します。

例

- Zelda は VMware 仮想マシン上の脅威アラートに気付き、[Alert Triage （アラートのトリアージ）] ページへのリンクをクリックします。
- 次に [Alert Triage （アラートのトリアージ）] ページの [Process Graph （プロセス グラフ）] パネルでノードをクリックして、[Selected Process （選択したプロセス）] パネルに仮想マシンの詳細を表示します。Zelda はデータを確認し、アラートの深刻度と仮想マシンに対するアクションが及ぼす影響を把握します。
- さらに、Zelda はコンテキストのメタデータを表示します。**AppDefense Scope （AppDefense の範囲）**を確認して、アプリケーションがどの程度ビジネス上重要であるかを判断します。その後、**AppDefense Service （AppDefense サービス）**および **AppDefense Service Type （AppDefense サービス タイプ）**メタデータを表示して、このサービスがアプリケーションに対して実用上どの程度重要であるかを判断します。また、**VMs in Service （サービス内の VM）**メタデータを表示して、冗長性に基づいてその仮想マシンがサービスに及ぼす影響を把握します。仮想マシンの識別メタデータ （VM Name （VM 名）、VM ID、VM UUID、vCenter UUID、および MAC address （MAC アドレス））を確認することで、仮想マシンをすばやく特定できます。このようにして、Zelda は確認した条件に従って適切な修復手順を決定できます。
- Zelda は仮想マシンを管理する IT 部門に連絡し、発生した問題とその解決に必要な手順について説明します。

[Alert Triage （アラートのトリアージ）] ページに表示されたデータを利用して、Zelda は ビジネスへの影響に基づいて最適な修復アクションを決定し、影響を受ける部門に対して適切に問題を説明しました。

Cb Defense での AppDefense アラームの操作

Cb Defense 管理コンソールの次のページで、AppDefense アラームを表示して操作することができます。

- **アラート リスト** — “アラートの表示およびアラートに対するアクションの実行” を参照してください。
- **[Investigate （調査）]** — “ アラートの調査 ” を参照してください。

アラート リスト ページでの AppDefense アラームの表示と修復

ヒント

アラートをフィルターしてアラート リスト ページに VMware アラートのみを表示するには、左側のパネルで [VMware Virtual Machines （VMware 仮想マシン）] フィルターをクリックします。

アラート リスト ページでアラートを検索する方法については、“ アラートの検索 ” を参照してください。

検索結果テーブルで、アラームごとに次のデータが表示されます。

表 37: VMware Appdefense のアラーム列のデータ

列	説明
チェックボックス	アラームまたはアラームのグループの横にあるチェックボックスをオンにして、棄却するアラートを選択できます。表示されたすべてのアラームを選択するには、検索結果テーブルの上にあるチェックボックスをクリックします。この選択には、現在のページに表示できるアラームのみが含まれます。組織内のすべてのアラームが含まれるわけではありません。“ アラートの棄却 ” を参照してください。
Status（ステータス）	アラートが AppDefense アラームである場合は、ステータスは **AppDefense** です。
First Seen（最初の認識日時）	このアラームが最初に発生した日付と時刻。この列に基づいて並べ替えを行うことができます。
Reason（理由）	アラームの理由。AppDefense アラームの場合、このデータにはアラーム タイプ、範囲、およびサービスが含まれます。
P	**[P]** 列はアラームに関連付けられた AppDefense 深刻度レベルを示しています。深刻度レベルの詳細については、表 30、「AppDefense 深刻度スコア」を参照してください。
T	アラームに関連付けられた AppDefense ターゲット バリュー。
Device（デバイス）	AppDefense デバイス名。この名前をクリックすると、[Investigate（調査）] ページでこのイベントに移動できます。
Take Action（アクション実行）	[Take Action （アクション実行）] 列では、AppDefense でアラームを表示するか、アラームを棄却することができます。Cb Defense 管理コンソールを使用して AppDefense アラームを棄却すると、AppDefense コンソールで対応する AppDefense アラーム /Cb Defense アラートがクリアされることに注意してください。AppDefense ではアラームのクリアを解除することはできません。

アラームを展開して追加のデータを表示するには、アラームの横にあるシェブロンをクリックします。次の情報が表示されます。

表 38: VMware アラーム用に展開されたデータ

項目	説明
Last Seen（最後の認識日時）	最後にアラームが検出された日時。
アラーム ID	VMware アラームの識別子。
アラート ID（Alert ID）	Cb Defense アラートの識別子。
OS	デバイス上で実行されているオペレーティング システム。
Last Action（最終アクション）	アラームに対して実行された最終アクション。

[Primary Process （主なプロセス）] タブ

[Primary Process （主なプロセス）] タブには、アラームによって影響を受ける主なプロセスの情報が表示されます。表示される情報は、アラーム タイプに関連します。

主なプロセスのデータを表示する：

1. 検索結果テーブルでアラームをクリックします。
2. [Primary Process （主なプロセス）] タブをクリックします （デフォルトで選択されています）。

   次の表に、各アラーム タイプに関連付けられたデータの説明を示します。

表 39: VMware アラーム用の [Primary Process （主なプロセス）] タブ - 受信接続と送信接続

項目	説明
Application （アプリケーション）	アプリケーションの名前。
SHA256	アプリケーションの SHA256 ハッシュ。
Violation Type （違反タイプ）	違反タイプ。これらには以下のものがあります。 • 受信接続 • 送信接続 • プロセス監視 • ゲスト整合性 • ホスト整合性
MD5	アプリケーションの MD5 ハッシュ。
Process Path （プロセス パス）	ファイル システムでのプロセス実行ファイルの場所。
CLI	コマンド ライン インターフェイスの情報。これらの詳細によって、実行可能ファイルの起動に使用されたオプションが示されます。
Local IP （ローカル IP）	仮想マシンのローカル IP アドレス。
Local Port （ローカル ポート）	仮想マシンのローカル ポート。
プロトコル	プロトコル タイプ。
Remote IP （リモート IP）（送信接続のみ）	リモート ピア接続の IP アドレス。
Remote Port （リモート ポート）（送信接続のみ）	リモート ピア接続のポート番号。
Trust （信頼度）	Cb Reputation Service によって決定されるハッシュのレピュテーション信頼度スコア。

項目	説明
[Threat （脅威）]	Cb Reputation Service によって決定されるハッシュのレピュテーション脅威スコア。

表 40: VMware アラーム用の [Primary Process （主なプロセス）] タブ - プロセ

項目	説明
Violation Type（違反タイプ）	違反タイプ。これらには以下のものがあります。 • 受信接続 • 送信接続 • プロセス監視 • ゲスト整合性 • ホスト整合性
SHA256	アプリケーションの SHA256 ハッシュ。
Process Path（プロセス パス）	ファイル システムでのプロセス実行ファイルの場所。
MD5	アプリケーションの MD5 ハッシュ。
CLI	コマンド ライン インターフェイスの情報。これらの詳細によって、実行可能ファイルの起動に使用されたオプションが示されます。
Parent Process Path（親プロセスのパス）	ファイル システムでの親プロセス実行ファイルの場所。
Parent SHA256（親 SHA256）	親アプリケーションの SHA256 ハッシュ。
Parent MD5（親 MD5）	親アプリケーションの MD5 ハッシュ。
Parent CLI（親 CLI）	親プロセスのコマンド ライン インターフェイスの情報。これらの詳細によって、親実行可能ファイルの起動に使用されたオプションが示されます。

ス監視

アラーム タイプがホスト整合性またはゲスト整合性の場合は、[Primary Process （主なプロセス）] タブは表示されません。代わりに、[Violation Details （違反の詳細）] タブが表示されます。

[Violation Details （違反の詳細）] タブには、次の情報が表示されます。このタブにはアクションはありません。

表 41: VMware アラーム用の [Violation Details （違反の詳細）] タブ - ホスト整合性とゲスト整合性

項目	説明
Num of Bytes Written （書き込まれたバイト数）	違反時に書き込まれたバイト数。
Physical Page Number （物理ページ番号）	影響を受けた物理ページ。
Writer Name （書き込みモジュール名）	影響を受けたソース モジュール。
Violated Address （違反先アドレス）	違反が生じたアドレス。
Violating Address （違反元アドレス）	違反の要因となったアドレス。

[Device （デバイス）] **タブ**

“ デバイス詳細の表示 ” を参照してください。

AppDefense アラームに対して、[Device（デバイス）] タブで以下のアクションを実行できます。

デバイスでアクションを実行する：

1. 検索結果テーブルでアラームをクリックします。
2. [Device （デバイス）] タブをクリックします。
3. [Take Action （アクション実行）] ドロップダウン メニューをクリックします。標準の Cb Defense アクション以外にも、以下のいずれかの AppDefense アクションを選択できます。
   - [Suspend （サスペンド）]: 仮想マシンをサスペンド状態にします。
   - [Snapshot （スナップショット）]: 仮想マシンのスナップショットを取得します。
   - [Power off （パワーオフ）]: 仮想マシンをパワーオフ状態にします。
   - [NSX Quarantine （NSX 隔離）]:AppDefense を介して NSX が仮想マシン上で有効化されている場合に、NSX を使用して仮想マシンを隔離できます。“NSX 隔離 ” を参照してください。

備考

[Investigate （調査）] ページのアラームに対しても同じアクションを実行できます。“ アラートの調査 ” を参照してください。

Cb Defense または AppDefense から AppDefense アクションを取り消すことはできません。vSphere または NSX を使用してのみ、アクションを取り消すことができます。

[Notes/Tags （メモ / タグ）] **タブ**

アラームに関連付けられたメモおよびタグを表示する：

1. 検索結果テーブルでアラームをクリックします。
2. [Notes/Tags （メモ / タグ）] タブをクリックします。

   アラームに対して実行されたアクションが、このタブでメモとしてログに記録されます。メモには次の情報が記録されます。

   - アラートが検出された場所 （Cb Defense または AppDefense）。
   - 実行されたアクションとその実行者。
   - アクションが発生した日時。

   Cb Defense と AppDefense の両方で開始できるアクションのみが、メモとして表示されます。

VMware AppDefense での Cb Defense アラートの表示

VMware 仮想マシンに対する Cb Defense 脅威アラートは、AppDefense アラームとして AppDefense コンソールに表示されます。Cb Defense が監視するアラートは、AppDefense コンソールには表示されません。

VMware AppDefense では、Cb Defense アラートのコンパクトなビューとそのアラートに関する Cb Defense の [Alert Triage （アラートのトリアージ）] ページへのリンクを使用できます。

“ アラートの視覚的表示 ” および “AppDefense がインストールされているデバイスに対する Cb Defense アラートの調査 ” を参照してください。次に示す Cb Defense アラート ID のハイパーリンクをクリックして、AppDefense から [Alert Triage （アラートのトリアージ）] ページに直接移動することができます。

AppDefense の [Alarm View （アラーム ビュー）] ページで、以下のアクションを Cb Defense に対して実行できます。

- AppDefense のアクション :
  - [Suspend （サスペンド）]: 仮想マシンをサスペンド状態にします。
  - [Snapshot （スナップショット）]: 仮想マシンのスナップショットを取得します。
  - [Power off （パワーオフ）]: 仮想マシンをパワーオフ状態にします。
  - [NSX Quarantine （NSX 隔離）]:NSX を使用して仮想マシンを隔離します。
- Cb Defense のアクション :
  - [Add to Blacklist （ブラックリストに追加）]:Cb Defense ブラックリストにプロセス ハッシュを追加します。
  - Cb Quarantine （Cb 隔離）:Cb Defense を使用して仮想マシンを隔離します。

備考

Cb Defense または AppDefense から AppDefense 修復アクションを取り消すことはできません。AppDefense アクションを取り消すには、vSphere または NSX を使用する必要があります。

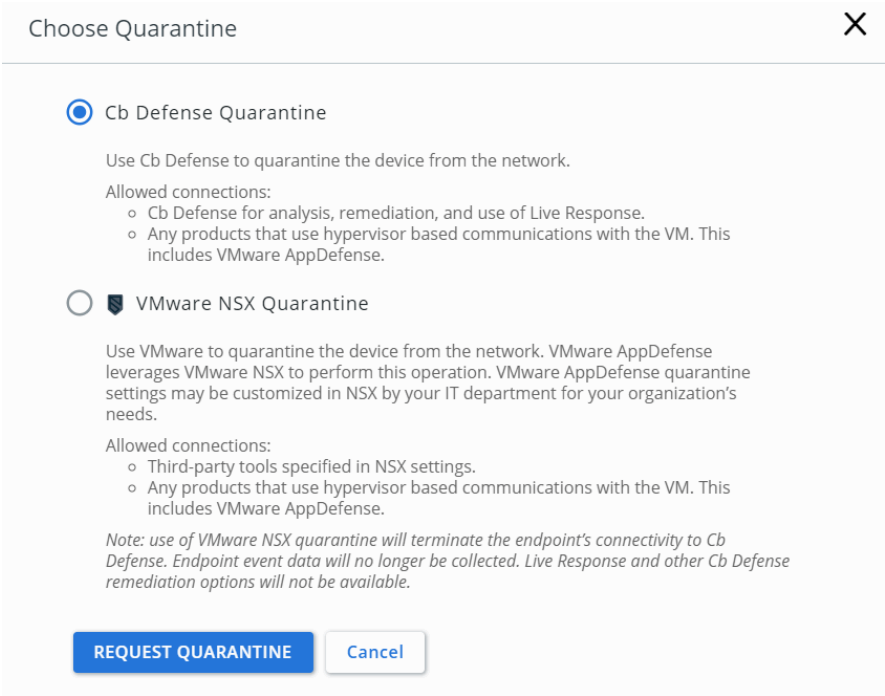
AppDefense コンソールではアラームをクリアできますが、このアクションでは Cb Defense 管理コンソールでアラートは棄却されません。AppDefense ではクリアするアクションを取り消すことはできません。

AppDefense でアラームをクリアすると、Cb Defense ではアラームにメモが追加され、アラームが棄却されたことが示されます。

Cb Defense 管理コンソールを使用して AppDefense アラームまたは Cb Defense アラートを棄却すると、AppDefense コンソールで対応する AppDefense アラーム /Cb Defense アラートがクリアされます。

仮想マシンの隔離

Cb Defense 隔離または NSX 隔離を使用して、仮想マシンを隔離できます。NSX 隔離は、個別の仮想マシン単位で利用できます。NSX が有効化されている仮想マシンで、[Quarantine Device （デバイスの隔離）] または [NSX Quarantine （NSX 隔離）] をクリックすると、Cb Defense 隔離または NSX 隔離のうち、どちらかの種類の隔離アクションを選択できるモーダル ウィンドウが表示されます。



同時に Cb 隔離 と NSX 隔離の両方をデバイスに適用しないでください。Cb Defense 以外の製品を使用してデバイスが隔離された場合は、そのデバイスはオフラインとして表示されます。

Cb Defense 隔離

Cb Defense 隔離では、すべての受信トラフィックおよび送信トラフィックをオペレーティング システム レベルでブロックします。Cb Defense で仮想マシンを隔離した場合、仮想マシンとの （ネットワーク ベースの通信ではなく）ハイパーバイザー ベースの通信を使用するすべての製品が、隔離した仮想マシンと通信できます。この機能は、AppDefense、vSphere、NSX など、ほとんどの VMware 製品に備わっています。

Cb Defense では、隔離された仮想マシンとの接続が維持されます。この機能は、分析および修復を目的とする場合に役立ちます。たとえば、Cb Defense によって隔離された仮想マシンに対して Live Response アクションを実行できます （“Live Response の使用 ” を参照）。

組織で NSX を使用していない場合、または修復を目的として Cb Defense で仮想マシンとの接続を維持する場合に、Cb Defense を使用することをお勧めします。

Cb Defense でデバイスを隔離する方法の詳細については、“ デバイスの隔離 ” を参照してください。

NSX 隔離

VMware AppDefense では、この操作を実行するために NSX を使用します。NSX は NSX 隔離設定に基づいてネットワークのその他の部分から仮想マシンを隔離します。この設定をカスタマイズして、サードパーティ製品による接続を承認できます。NSX 隔離により、ハイパーバイザー レベルで受信ネットワーク接続および送信ネットワーク接続が遮断されます。

NSX 隔離を使用してデバイスを隔離すると、Cb Defense とのエンドポイントでの接続は終了します。そのため、Live Response やその他の Cb Defense 修復オプションは使用できません。Cb Defense では、仮想マシンはオフラインとして表示されます。

NSX によって隔離された仮想マシンは Cb Defense および AppDefense のどちらでも隔離を解除することができません。仮想マシンの隔離を解除するには、NSX に対して管理者アクセスが必要です。

Appendix E

Cb Defense の通信

ネットワーク プロキシとファイアウォールの構成が不適切な場合、Cb Defense センサー（Windows および macOS エンドポイントに展開）と Cb Defense バックエンド（クラウド内で Amazon Web Services 経由で安全に稼働）との間で通信障害が発生する場合があります。

この付録では、Cb Defense センサーと Cb Defense バックエンドとの間で適切に通信が行われるように、ネットワーク インフラストラクチャとエンドポイント デバイスを構成する方法について説明します。

Cb Defense バックエンドへのアクセス

組織のアセットがクラウド内の Cb Defense バックエンドにアクセスするには、次の 3 つの方法があります。

- 管理目的や、アラートを表示および調査する場合は、Web ブラウザーから TCP/443（HTTPS）経由で Cb Defense 管理コンソールに接続できます。
- センサーは、TCP/443 経由で Cb Defense バックエンド サーバーに接続できます。また、バックエンド サーバーは、ポート TCP/54443 でセンサーをリッスンします。
- ポート TCP/443 で API を介してクラウド サービスにアクセスするように組織のアプリケーションを作成できます。詳細については、https://developer.carbonblack.com/ を参照してください。

Cb Defense バックエンドの URL については、正規のサポート担当者にお問い合わせください。Web UI アクセス、センサーの通信、およびバックエンド API の URL は、それぞれ異なります。

注意

Cb Defense バックエンドのアーキテクチャでは、動的に管理されるロード バランサーを使用しているため、パブリック IP が頻繁に変更されます。このような方法により、サービスに必要なレベルのスケーラビリティと信頼性を実現しています。そのため、静的パブリック IP アドレスは提供していません。TCP/443 および Cb Defense の代替ポート TCP/54443 経由で送信接続を許可するようにファイアウォールまたはプロキシのバイパス ルールを構成して、Cb Defense バックエンドへのアクセスを許可することをお勧めします。

ファイアウォールまたはプロキシの設定では、静的 IP、IP の範囲、またはサブネットをホワイトリストに登録したり、除外したりすることはできません。ホワイトリストに登録したり、除外したりできるのは、URL のみです。

デバイス サービス URL は、バックエンド インスタンスごとに異なります。現在使用中のバックエンドを確認するには、ログイン URL を調べてください。

ファイアウォールの構成

ファイアウォールで保護されたネットワーク内の Cb Defense バックエンドに Cb Defense センサーが接続するには、いくつかの方法があります。

- センサーとバックエンドが TCP/443 経由で通信することを許可するように、ネットワーク ファイアウォールでバイパスを構成します。これは多くの場合、最も簡単な方法です。
- Cb Defense の代替ポート TCP/54443 への送信接続を許可するように、ネットワーク ファイアウォールでバイパスを構成します。
- Cb Defense バックエンド アプリケーションにアクセスするための変更がネットワーク ファイアウォールで行われなかった場合、センサーは既存のプロキシ経由で接続を試みます。

プロキシの構成

Cb Defense センサーは、さまざまなメカニズムを使用して、ネットワーク プロキシの有無を確認します。プロキシが検出された場合 （または、インストール時にプロキシが指定された場合）、センサーはそのプロキシの使用を試みます。プロキシが検出されなかった場合、センサーはポート 443 または 54443 経由で直接接続を試みます。

無人センサーをインストールするときのプロキシ構成の詳細については、『PSC センサー インストール ガイド』を参照してください。

センサーが Cb Defense バックエンドと通信するときに使用する方法

センサーが Cb Defense バックエンドとの通信を試みるときに使用する方法を次に示します。

- センサーのインストール時に構成される静的構成プロキシ
- TCP/443 経由での直接接続
- ローカル システムのオペレーティング システム設定からのプロキシとプロキシ認証情報 （該当する場合）の自動検出

標準 SSL ポート経由で接続を確立できない場合、センサーは代替ポート （TCP/54443）にフェイルオーバーできます。

注意

Cb Defense センサーは、最初のインストール時にプロキシ設定の自動検出を試みます。これにはテストが必要です。プロキシの自動検出が成功しない場合は、無人インストール時に MSI コマンド ラインにプロキシ IP とポートが含まれるようにパラメーターを定義する必要があります。

ユーザー認証が必要な場合、エンド ユーザーは認証情報を入力するように求められる場合があります。通常、プロキシ認証情報が要求される環境では、この状況は発生しません。これは、センサーが使用する既存の構成では、エンド ユーザーは認証情報の入力を求められないためです。

ネットワーク プロキシの通過を回避（または、ファイアウォールによるブロックを回避）するには、センサーからバックエンドへの送信接続を許可するように、プロキシ サーバー / ファイアウォールでバイパスを構成することが必要な場合があります。バイパス構成のオプションを次に示します。

- TCP/443 経由で Cb Defense ドメインへの送信接続を許可するように、ファイアウォールまたはプロキシでバイパスを構成します。
- Cb Defense の代替ポート TCP/54443 への送信接続を許可するように、ファイアウォールまたはプロキシでバイパスを構成します。

警告

Cb Defense バックエンド サーバーのホスト ドメイン名は、サーバーの証明書に含まれています。ネットワーク プロキシやゲートウェイによっては、証明書を検証した結果、AWS で実行しているシステムの実際のホスト名と証明書とで名前が一致しないために、Cb Defense バックエンド アプリケーションの接続を拒否する場合があります。この状況が発生した場合は、バックエンド サーバーの証明書を検証しないように、プロキシまたはゲートウェイを構成する必要があります。証明書またはサーバーの証明書内のホスト名にはアクセスできないことに注意してください。

接続メカニズムの優先度

Cb Defense センサーは、Cb Defense バックエンドに接続できない場合、過去に動作したことが確認されている設定を、最新のものから試します。これらの設定には、以下が含まれます。

- プロキシ
- プロキシなし
- 認証情報
- 認証情報なし
- インストール時に使用されたプロキシ
- 直接接続
- 代替 54443 ポート

Cb Defense センサーは、次の順番で接続を試みます。

1. センサーのインストール時に指定された静的に構成されているプロキシ　サーバーを使用します。
2. プロキシを使用せずにバックエンドへの直接接続を試みます。
3. プロキシを使用せずに代替ポート 54443 を介してバックエンドへの直接接続を試みます。
4. 動的プロキシ（インターネット / ネットワーク設定）が存在する場合は、認証情報なしで動的プロキシを試みます。
5. その他の試行に失敗してプロキシが指定され、認証情報が必要である場合、センサーは最後の手段としてこの接続を試みます。

プロキシ サーバーへの接続が試行されるたびに、センサーは次への接続を試みます。

- 構成済みのプロキシ ポート
- 代替ポート 54443 （センサーのインストール時に構成済みの場合）

Appendix F

高度な検索語句

この付録では、アラート リスト ページまたは [Investigate （調査）] ページの高度な検索クエリで使用できる検索語について説明します。

表 42: 高度な検索語句

検索クエリ	説明
Alert （アラート）	
attack stage （攻撃段階）	"killChainStatus" とほぼ同じですが、異なるクエリ値を使用します。有効な値については、を参照してください。
deviceSecurityEventCode	アラートに関連付けられているイベントのアラート ID です。
killChainStatus	キル チェーンの各段階にマッピングされます。有効な値については、を参照してください。
threatScore	イベントが脅威に関連付けられている場合の 1 ～ 10 の優先度。
Device （デバイス）	
agentLocation	オンプレミスまたはオフプレミス。“ プレミスの定義 ” を参照してください。
deviceName	エンドポイントのホスト名。
deviceId	センサーに関連付けられているデバイス ID。
deviceIpAddress	デバイスの IP アドレス。パブリック IP でのみ機能します。
deviceType	メジャー OS タイプ : Windows または MAC。 例 :deviceType:win*、deviceType:mac。
deviceVersion	OS の詳細なバージョンを表す文字列。 例 : deviceVersion:"Windows 10 x64"。
email	インストール ユーザーに関連付けれらた E メール アドレス。ドメイン名は不要です。
groupName	イベント時にセンサーがあったポリシー。部分的テキスト検索がサポートされます。
targetPriorityType	イベント時にポリシーによって定義されていた LOW （低）|MEDIUM （中）|HIGH （高）|CRITICAL （重大）のいずれか。
General （一般）	
eventId	このイベントの一意の識別子。
eventType	イベントのタイプ。例 : eventType:Network。

検索クエリ	説明
Operation	ポリシー操作に一致するイベント。の「操作の試行」を参照してください。
syslogLevel	イベントに関連付けられている Syslog レベル。syslogLevel:"NOTICE" = 監視対象イベント、syslogLevel:"WARNING" = 脅威イベント。
threatIndicators	イベントに関連付けられた TTP。例 :["ADAPTIVE_WHITE_APP", "ACTIVE_SERVER", "NETWORK_ACCESS"]。
TTP	イベントに関連付けられた TTP。例 : INJECT_CODE。
Network（ネットワーク）	
destAddress	ネットワーク イベントの宛先 IP アドレス。
destPort	ネットワーク イベントの宛先ポート。
service	ネットワーク接続の L4 プロトコルとポート番号を示すテキスト文字列。例 : TCP/80、UDP/53。引用符で囲む必要があります。
sourceAddress	ネットワーク イベント内の発信元 IP アドレス。デバイスの IP アドレスとは異なる場合があります。
sourcePort	ネットワーク イベント内の接続の発信元ポート。
Process （プロセス）	
applicationName	イベントの主なプロセスの名前。
applicationPath	イベントの主なプロセスのフル パス。
commandLine	イベントの主なプロセスによって確認されるコマンド ライン。テキスト検索内の空白は、AND として処理されます。
parentCommandLine	イベントの親プロセスによって確認されるコマンド ライン。テキスト検索内の空白は、AND として処理されます。
parentHash	イベントの親プロセスの SHA256。
parentName	イベントの親アプリケーションの名前。
parentPid	イベントの親プロセスに関連付けられたプロセス ID。
processHash	イベントの主なプロセスの SHA256 ハッシュ。
processId	イベントの主なプロセスに関連付けられたプロセス ID。
processMd5Hash	イベントの主なプロセスの MD5 ハッシュ （ポリシーでこの機能が有効な場合）。
targetAppName	イベントの子プロセスの名前。
targetCommandLine	イベントの子プロセスによって確認されるコマンド ライン。空白は AND 演算子として処理されます。

検索クエリ	説明
targetHash	イベントの子プロセスの SHA256。
targetMd5Hash	イベントの子プロセスの MD5 ハッシュ （ポリシーでこの機能が有効な場合）。
targetPid	イベントの子プロセスのプロセス ID。
userName	イベントの主なプロセスに関連付けられたユーザー コンテキスト。
レピュテーション（Reputation）	
childEffectiveReputation	ポリシー適用に使用されるイベントの子プロセスのレピュテーション。有効なレピュテーション：COMPANY_WHITE_LIST、COMPANY_BLACK_LIST、LOCAL_WHITE、COMMON_WHITE_LIST、TRUSTED_WHITE_LIST、NOT_LISTED、KNOWN_MALWARE、UNKNOWN、PUP、SUSPECT_MALWARE。
childEffectiveReputationSource	ポリシー適用に使用されるイベントの子プロセスのレピュテーション ソース。有効なレピュテーション ソース：AV、CERT、CLOUD、HASH_REPUTATION_LIST、PRE_EXISTING、WHITE_DATABASE、YARA、VECTOR、CERT、CHECKSUM、SELF、NO_HOOK。
parentEffectiveReputation	ポリシー適用に使用されるイベントの親プロセスのレピュテーション。有効なレピュテーション：COMPANY_WHITE_LIST、COMPANY_BLACK_LIST、LOCAL_WHITE、COMMON_WHITE_LIST、TRUSTED_WHITE_LIST、NOT_LISTED、KNOWN_MALWARE、UNKNOWN、PUP、SUSPECT_MALWARE。
parentEffectiveReputationSource	ポリシー適用に使用されるイベントの親プロセスのレピュテーション ソース。有効なレピュテーション ソース：AV、CERT、CLOUD、HASH_REPUTATION_LIST、PRE_EXISTING、WHITE_DATABASE、YARA、VECTOR、CERT、CHECKSUM、SELF、NO_HOOK。
parentReputationProperty	イベントの親プロセスのレピュテーション。有効なレピュテーション: COMPANY_WHITE_LIST、COMPANY_BLACK_LIST、LOCAL_WHITE、COMMON_WHITE_LIST、TRUSTED_WHITE_LIST、NOT_LISTED、KNOWN_MALWARE、UNKNOWN、PUP、SUSPECT_MALWARE。
processEffectiveReputation	ポリシー適用に使用されるイベントの主なプロセスのレピュテーション。有効なレピュテーション：COMPANY_WHITE_LIST、COMPANY_BLACK_LIST、LOCAL_WHITE、COMMON_WHITE_LIST、TRUSTED_WHITE_LIST、NOT_LISTED、KNOWN_MALWARE、UNKNOWN、PUP、SUSPECT_MALWARE。

検索クエリ	説明
processEffectiveReputationSource	ポリシー適用に使用されるイベントの主なプロセスのレピュテーション ソース。有効なレピュテーション ソース：AV、CERT、CLOUD、HASH_REPUTATION_LIST、PRE_EXISTING、WHITE_DATABASE、YARA、VECTOR、CERT、CHECKSUM、SELF、NO_HOOK。
processReputationProperty	イベントの主なプロセスのレピュテーション。有効なレピュテーション： COMPANY_WHITE_LIST、COMPANY_BLACK_LIST、LOCAL_WHITE、COMMON_WHITE_LIST、TRUSTED_WHITE_LIST、NOT_LISTED、KNOWN_MALWARE、UNKNOWN、PUP、SUSPECT_MALWARE。
targetEffectiveReputation	ポリシー適用に使用されるイベントの子プロセスのレピュテーション。有効なレピュテーション：COMPANY_WHITE_LIST、COMPANY_BLACK_LIST、LOCAL_WHITE、COMMON_WHITE_LIST、TRUSTED_WHITE_LIST、NOT_LISTED、KNOWN_MALWARE、UNKNOWN、PUP、SUSPECT_MALWARE、NOT_LISTED。
targetEffectiveReputationSource	ポリシー適用に使用されるイベントの子プロセスのレピュテーション ソース。有効なレピュテーション ソース：AV、CERT、CLOUD、HASH_REPUTATION_LIST、PRE_EXISTING、WHITE_DATABASE、YARA、VECTOR、CERT、CHECKSUM、SELF、NO_HOOK。
targetReputationProperty	イベントの子プロセスのレピュテーション。有効なレピュテーション： COMPANY_WHITE_LIST、COMPANY_BLACK_LIST、LOCAL_WHITE、COMMON_WHITE_LIST、TRUSTED_WHITE_LIST、NOT_LISTED、KNOWN_MALWARE、UNKNOWN、PUP、SUSPECT_MALWARE、NOT_LISTED。

表 43: キル チェーンの段階 - クエリ

クエリ	説明
調査	ターゲットを調査、識別、および選択します。
武器化	配信可能なペイロードを作成します。
deliver_exploit	配信して、コードを実行します。
install_run	バック ドアをインストールし、永続アクセスを許可します。
COMMAND_AND_CONTROL	外部デバイスからコードで通信します。
Execute_Goal	目的を達成します。

Appendix G

用語集

語句	定義
アラート ID （Alert ID）	「インシデント ID （Incident ID）」を参照してください。
アラートの深刻度（Alert severity）	Cb Defense で検出されたすべてのアラートは、深刻度別にグループ化されます。アラートの深刻度レベルを次に示します。 • Threat （脅威）– 悪意のあるアクティビティである可能性が高い。 • Monitored （監視対象）– 組織への危険要因となる可能性があるため、確認が必要。 「優先度スコア （Priority Score）」も参照してください。
[Alert Triage （アラートのトリアージ）] ページ（Alert Triage page）	アラートを視覚的に表示できる Cb Defense 管理コンソールのページ。“ アラートの視覚的表示 ” を参照してください。
アラート リスト ページ（Alerts List page）	アラートの検索やアラートへの対応が可能な Cb Defense 管理コンソールのページ。“ アラートの表示およびアラートに対するアクションの実行 ” を参照してください。
分析プラットフォーム（Analytics platform）	Cb Defense 分析プラットフォームは、センサーから送信されたイベント データを分析し、脅威情報を生成します。
アーティファクト（Artifact）	アーティファクトとは、実行前に分析が行われるバイナリ ファイルなどのファイルです。Cb Defense では次のアーティファクトが検出されます。 • （初期バックグラウンド スキャンに関係なく）ディスクに書き込まれたすべての実行可能ファイル • 実行されているすべての実行可能ファイル （センサー インストールの前から存在する実行可能ファイルおよびネットワーク共有上の実行可能ファイルを含む） バックグラウンド スキャンでは、センサーのインストール前から存在するが実行されていない実行可能ファイルが検出されます。
動作 （Behavior）	動作とは、エンドポイントのターゲット リソースに対するプロセスまたはプログラムの挙動です。動作は個別の TTP （Tactics, Techniques, and Procedures: 攻撃手口）として捕捉されます。動作はセンサーによってデバイスで捕捉され、バックエンドの分析エンジンによってアラートにコンパイルされる （適用される場合）グループとして分析されます。“TTP のリファレンス ” を参照してください。
バイパス モード（Bypass mode）	エンド ユーザーまたは管理者によって、センサーがバイパス モードにされます。このモードでは、センサーと Cb Defense バックエンド間で通信が行われません。

語句	定義
Cb Defense 管理コンソール （Cb Defense Management Console）	Cb Defense 管理コンソールを使用すると、センサー展開およびデバイス登録ステータスのチェック、ポリシーとアラートの構成および適用、セキュリティ イベントのレビューなどを実行できます。“ 作業の開始 ” を参照してください。
ダッシュボード（Dashboard）	Cb Defense にログインすると、**ダッシュボード**がホームページとして表示されます。**ダッシュボード**には、システムで実行中の処理のスナップショットが表示され、関心のある項目にすばやく移動することができます。また、Cb Defense が保護するデバイスで何が起きているかも表示されます。“ ダッシュボード ” を参照してください。
（リソースの）拒否（Deny （resources））	ポリシー設定に従って、レピュテーションや行動に基づきリソースを拒否するアクション。
デバイス ID （Device ID）	インストール済みの各センサーに対応する一意の識別子。 同じデバイス上でセンサーをアンインストールして、再インストールした場合は、同じデバイス名に対して複数のデバイス ID が存在します。この場合、Cb Defense 管理コンソールには、1 つのアクティブ デバイスと 1 つの登録が取り消されたデバイスが表示されます。これらのデバイスは、デバイス ID は異なりますが、同じデバイス名を共有しています。
デバイス ユーザー（Device user）	センサーをインストールまたは登録したユーザー。[Sensor Management （センサーの管理）] ページでは、**ユーザー**と呼ばれます。[Investigate （調査）] ページの [Device （デバイス）] タブ、および展開されたイベント詳細の [Email（E メール）] では [Sensor Installed by（センサーのインストール ユーザー）] として表示されます。
エンドポイント（Endpoint）	デバイスやホストとも呼ばれます。
イベント ID （Event ID）	各管理対象デバイスから記録された関心対象のイベント。イベントによっては、アラートに昇格されるものもあります。
インシデント ID（Incident ID）	インシデント ID（アラート ID とも呼ばれる）は、アラートのフラグが設定されたイベントを指し、基となるイベントの動作およびデバイスに固有の属性に応じて決まります。 複数のイベント （イベント ID）がすべて同じインシデント ID を共有することがありますが、イベントにはインシデント ID が 1 つだけ割り当てられるので、イベント ID あたりのインシデント ID の数は 1 つのみです。インシデント ID は 8 文字の文字列で、[Investigate （調査）] ページおよび [Alert Triage （アラートのトリアージ）] ページのイベントの詳細で確認できます。イベント ID は、**アラート リスト** ページで検索できます。**アラート リスト** ページで [Investigate （調査）] ボタンをクリックすると、URL にインシデント ID が表示されます。「スレッド ID（Threat ID）」も参照してください。

語句	定義
[Investigate （調査）] ページ （Investigate page）	[Investigate（調査）] ページでは、アラートを徹底的に調査して分析できます。“ アラートの調査 ” を参照してください。
Live Response	Cb Defense センサー バージョン 3.0 以降が動作しているエンドポイントが接続されている場合、Cb Defense Live Response は、そのエンドポイントに対するコマンド ライン インターフェイスを開きます。センサーには、Live Response が有効であるポリシーを割り当てる必要があります。Live Response を使用すると、リモートで調査を実行し、継続中の攻撃を封じ込め、脅威を修復できます。“Live Response の使用 ” を参照してください。
ローカル スキャン （Local scanning）	Cb Defense センサーには、アプリケーションを実行する前に静的ファイル分析を有効にするローカル スキャン機能がオプションで含まれています。“[Local Scan Settings（ローカル スキャン設定）] タブ ” を参照してください。
マルウェア （Malware）	エンドポイント上で攻撃者のために悪意のあるアクションを実行することのみが目的であると認定されたファイル。
MD5 ハッシュ （MD5 hash）	MD5 アルゴリズムは、128 ビットのハッシュ値を生成するハッシュ関数です。
非マルウェア （Non-malware）	不正な動作またはローカル ブラックリストにより阻止された、一般にマルウェアとして認識されないプロセス。これには、レピュテーションは良いが （PowerShell や Winword.exe ファイルなど） 、不正な動作をするケースが含まれます。
通知 （Notification）	新たに発見された脅威は、E メールや SIEM コネクターによる通知など、さまざまなメカニズムを介して通知できます。“ 通知およびコネクター ” を参照してください。
オンプレミス / オフプレミス （On-premises/Off-premises）	センサーがオンプレミスとオフプレミスのどちらに存在するかの判断には、完全修飾ドメイン名 （FQDN） と IP アドレスという 2 つの条件が使用されます。 “ プレミスの定義 ” を参照してください。
ポリシー	防御動作を決定するポリシー ルールのグループ。各センサーは、1 つのポリシーに割り当てられます。“ ポリシーによる攻撃からの防御 ” を参照してください。
潜在的なマルウェア （Potential malware）	エンドポイントで悪意のあるアクションを実行する脅威のあるソフトウェア。有益なアクションも悪意のあるアクションも実行できるファイル。
阻止 （Prevention）	悪意のあるコードや動作が発見された場合の実行内容をセンサーに伝えるポリシー ルールによって、悪意のある動作が阻止されます。“ ポリシーによる攻撃からの防御 ” を参照してください。

語句	定義
優先度スコア（Priority score）	優先度スコアは、アラートの相対的重要度に基づいて優先順位を付けたもので、[Attack Stages （攻撃段階）] パネルにおおまかにマッピングされます （表 3、「[Attack Stages （攻撃段階）]」を参照）。 一般に、スコアが高いほど敵対者または攻撃がその目的達成に近いことを示します。たとえば、特定のマルウェアの目的が永続性にある場合、アラートの優先度は高くなりません。その目的がユーザー データの暗号化、パスワードの盗み取り、システム ファイルへの損害などの場合、このアラートの優先度は高くなります。 優先度スコアは、*脅威レベル*、*脅威スコア*、*脅威優先度*、またはアラート優先度とも呼ばれます。
プロセス ユーザー（Process user）	調査中のプロセスを実行したユーザー。これは、ログオン ユーザーまたはシステム ユーザーのいずれかです。
PUP	潜在的に迷惑なプログラム。PUP は、被害が最も少ないものでも煩わしい結果をもたらし （ポップアップ広告の配信）、マルウェアの配信に利用されることもあります。
隔離（Quarantine）	デバイスをネットワークの他の部分から隔離できます。隔離されたデバイスは、Cb Defense バックエンドに対してのみネットワーク アクセスが可能です。“ デバイスの隔離 ” を参照してください。
レピュテーション（Reputation）	レピュテーションは、オブジェクトに与えられた信頼または不信頼のレベルです。Cb Defense ファイルのレピュテーションは、既知の正常なオブジェクトと既知の不正なオブジェクトの複数のソースに基づいています。たとえば、ハッシュ、IT ツール、および証明書に基づいてアプリケーションをホワイトリストまたはブラックリストに登録できます。“ レピュテーションの管理 ” を参照してください。
SAML 統合（SAML integration）	SAML （Security Assertion Markup Language）は、当事者間で認証および承認データを交換するためのオープン スタンダードです。SAML を使用することにより、Cb Defense を Okta、Ping Identity、および OneLogin と統合できます。“ 認証および統合 ” を参照してください。
センサー （Sensor）	Cb Defense は、Windows ベースおよび macOS ベースのシステムに対応したホスト ベースの軽量なセンサーを使用します。このセンサーにはクイック インストール プロセスがあるため、システム パフォーマンス、CPU、ネットワーク、ディスク、およびバッテリー寿命への大きな影響は（ほとんどの場合）ありません。インストール後、センサーの管理は Cb Defense 管理コンソールで行います。
センサー グループ（Sensor group）	センサー グループを作成し、そのグループにセンサーを追加できます。センサー グループ内のすべてのセンサーは、センサーに関連付けられているメタデータと定義した条件に基づいて、ポリシーに自動で割り当てられます。“ ポリシー自動割り当て用のセンサー グループの管理 ” を参照してください。

語句	定義
SHA256 ハッシュ（SHA256 hash）	SHA（Secure Hash Algorithm）は、暗号ハッシュ機能です。暗号ハッシュは、テキストまたはデータ ファイルの署名に似ています。SHA-256 アルゴリズムは、256 ビット（32 バイト）のハッシュを生成します。
シグネチャ ミラー サーバー（Signature mirror server）	Cb Defense ローカル スキャン シグネチャのローカル リポジトリ。“シグネチャ ミラーの手順” を参照してください。
スパイダー グラフ（Spider graph）	アラートに関連付けられている TTP を示す対話型グラフ。[Alert Triage （アラートのトリアージ）] ページに表示されます。“[Alert behaviors based on severity （深刻度に基づくアラートの動作）]” を参照してください。
ターゲットバリュー（Target value）	ターゲットバリューはデバイスが属しているポリシーによって定義されます。特定のデバイスで検出された任意の脅威の脅威レベルを計算する際に乗数としての役割を果たします。 • 低いターゲットバリュー – 脅威レベルが低くなります。 • 中間ターゲットバリュー – ベースラインを表します（乗数なし）。 • 高いターゲットバリューおよびミッション クリティカルなターゲットバリュー – 同じ状況下でどちらも脅威レベルが高くなります。その結果、説明は同じでも優先度スコアが異なる 2 つ以上のアラートが表示される場合があります。
（プロセスの）終了（Terminate （process））	ポリシー設定に従って、レピュテーションや行動に基づきプロセスを終了するアクション。
[Threat （脅威）] カテゴリ（Threat category）	[Monitored（監視対象）] カテゴリは、対応を要するレベルには達していないが、破壊的である可能性があり、注意を要する行動が含まれる一連の行動データです。 [Threat （脅威）] カテゴリは、一連の行動データと、デバイス上の悪意ある行動を示すコンテキスト情報です。
脅威 ID （Threat ID）	脅威 ID はアラートに対応しており、デバイスには依存しない、アラートからの属性のサブセットに応じて決まります。**アラート リスト** ページから [Investigate （調査）] ボタンをクリックすると、[Investigate （調査）] ページの URL にこの 32 文字の文字列が表示されます。**アラート リスト** ページで脅威 ID を検索すると、同じ脅威 ID に関連付けられている他のアラートを調べることができます。複数のインシデント ID が同じ脅威 ID を共有することがあります。 「インシデント ID （Incident ID）」も参照してください。
TTP	Cb Defense では、動作は個別の TTP（Tactics, Techniques, and Procedures: 攻撃手口）として捕捉されます。動作はセンサーによってデバイスで捕捉され、バックエンド プラットフォームで分析エンジンによってアラートにコンパイルされる （適用される場合）グループとして分析されます。“TTP のリファレンス ” を参照してください。