Carbon Black.

Cb Defense の作業の開始

Cb Defense では、高度な予測モデルを使用してエンドポイント データを分析し、
システムが危険にさらされる前に攻撃を阻止します。

基本の 5 ステップで Cb Defense を始める

Carbon Black.

1 ユーザーを追加する

Cb Defense 管理コンソールの使用を開始するには、ユーザーを追加します

1. Predictive Security Cloud (PSC) にサインインし、**[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 (ユーザーの追加)]** をクリックして、以下のいずれかの権限を選択します。

View only (表示のみ)	**Admin (管理者)**	**Live Response Admin (Live Response 管理者)**
アラートを表示するのみで、アラートに対するアクションを実行できません。	アラートを表示してアクションを実行します。	アラートを表示してアクションを実行します。Live Response を使用して、エンドポイントでの問題を修復します。

ユーザーは、パスワードの作成とサインインのための電子メールの招待を受け取ります 。

Live Response 管理者を追加できるのは、Live Response 管理者のみです。

2 エンドポイントにセンサーをインストールする

少数のセンサーをインストールして、エンドポイントの保護を開始します

1. **[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、**[Add User(s) (ユーザーの追加)]** をクリックします。ユーザーはダウンロード リンクとインストール コードが記載された 電子メールを受け取ります 。センサーをインストールするには、エンドポイントの管理者権限が必要です。
3. Cb Defense で保護する各エンドポイントに PSC センサーをインストールします。デフォルトでは、新しくインストールされたセンサーには標準ポリシーが使用されます。

   PSC センサーがエンドポイントにインストールされるとすぐに、エンドポイントはポリシーによって保護されます。

スクリプトまたはソフトウェア配布ツールを使用して多数のセンサーをインストールするには、『PSC センサー インストール ガイド』を参照してください。ベスト プラクティスとして、最新バージョンのセンサーをインストールします。

2 センサー グループを作成する

後でセンサー グループを作成して、異なるチームやエンドポイントにわたってセンサーとポリシーを管理できます

Cb Defense を組織全体に展開する前に、センサー グループを作成して、組織内の以下のような異なるチームにわたってセンサーとポリシーを管理できます。

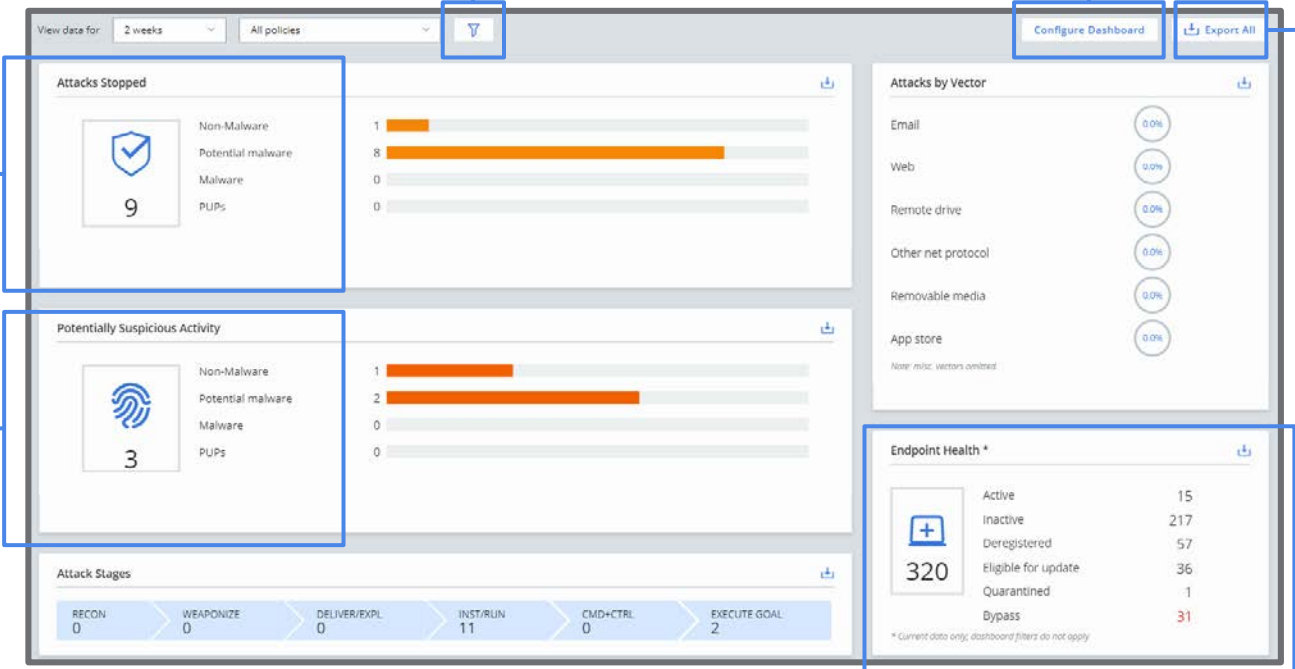
- 営業
- 財務
- IT
- エンジニアリングなど

チームの働き方や必要なセキュリティ レベルに応じて、ポリシーをカスタマイズできます。その後で、ポリシーをセンサー グループと関連付けることができます。センサー グループの新しいエンドポイントは、センサー グループに関連付けられているポリシーによって自動的に保護されます。

たとえば、センサー グループを Active Directory の財務 OU（組織単位）、または 100 で始まるサブネット アドレスを持つすべての Windows エンドポイントとして定義し、その後でそのセンサー グループ固有のポリシーを適用することができます。

3 ダッシュボードを表示する

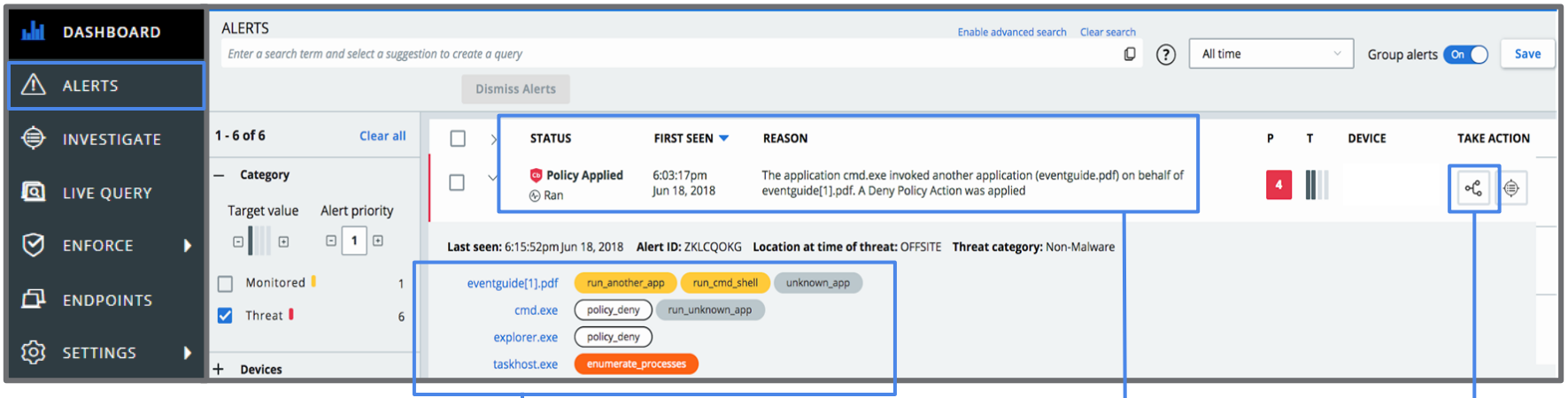
センサーをインストールしたら、ダッシュボードをクリックして、組織の全体像を把握します



4 アラートを表示する

[Alerts (アラート)] ページに、Cb Defense が挙げたアラートを表示します

Cb Defense は疑わしい動作と既知の脅威に基づいてアラートを挙げます。定期的にアラートを確認し、正常なアクティビティと攻撃を区別します。**アラートのトリアージ** アイコン をクリックして、イベントの流れを確認します。



TTP を見ると、Cb Defense がこのイベントまたは動作に対してアラートを挙げた理由がわかります。

この例では、cmd.exe アプリケーションが他のアプリケーションを呼び出しているため、拒否ポリシー アクションが適用されています。

アラートのトリアージ

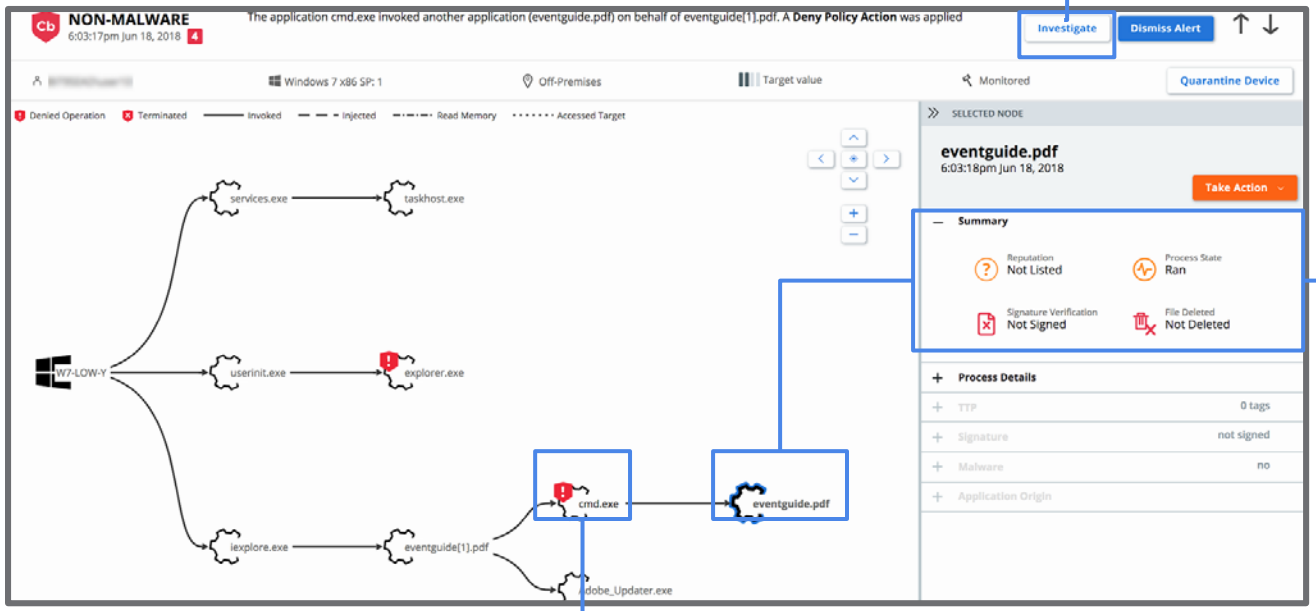
攻撃手口 (TTP) については、『Cb Defense ユーザー ガイド』を参照してください。

Carbon Black.

4 アラートのトリアージ

[Alert Triage (アラートのトリアージ)] ページで、プロセス ツリーを表示してイベントまたはノードを選択し、詳細情報を確認します

この例では、疑わしい .pdf ファイルに NOT_LISTED というレピュテーションが付けられています。この .pdf は署名されておらず、コマンド インタープリターを起動しました。このアラートを詳細に調査するには、**[Investigate (調査)]** をクリックします。



アラートの調査

選択したノードの属性の概要

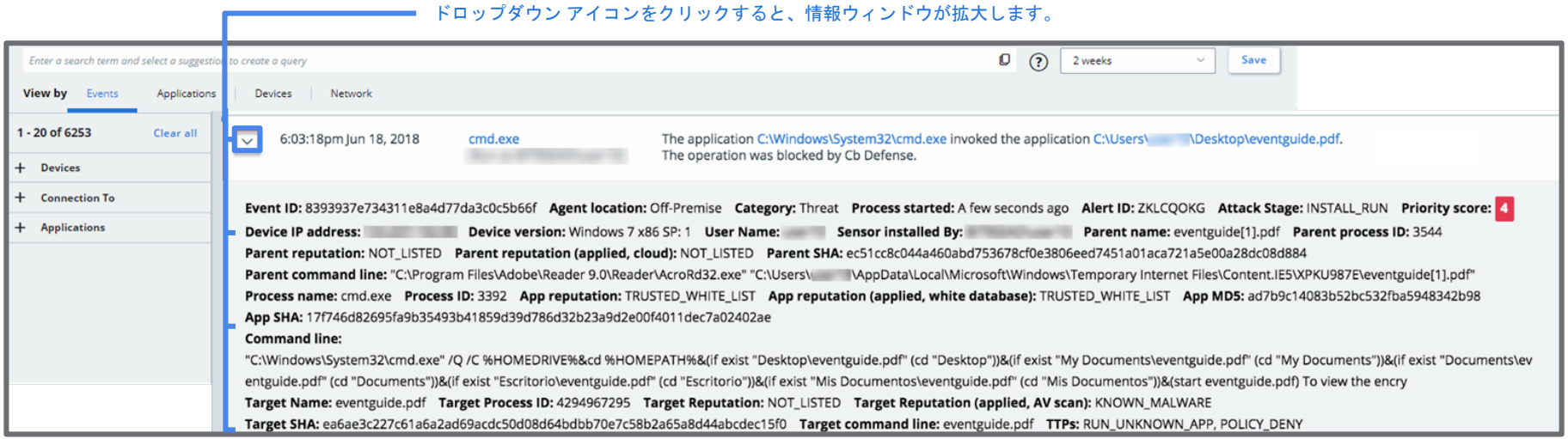
拒否された処理のポリシーを適用

Carbon Black.

4 アラートを調査する

[Investigate (調査)] ページに、イベントの詳細を表示します

イベントのその他の詳細情報 (ファイル ハッシュ、アプリケーション ハッシュ、親プロセス、子プロセス、ネットワーク接続、コマンドライン引数、TTP、ファイルのレピュテーションなど) を表示できます。ファイルのレピュテーションはクラウドの脅威インテリジェンスと PSC Reputation Service に基づいています。



『Cb Defense: レピュテーションの優先度』を参照してください。

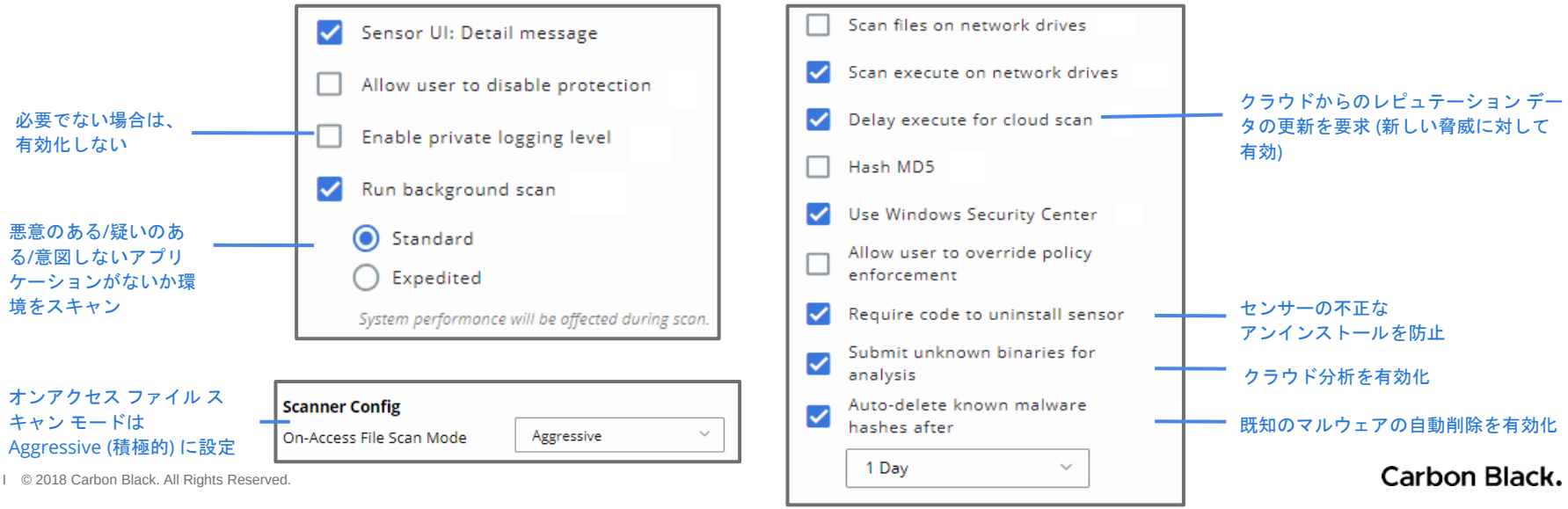
Carbon Black.

5 ポリシーを微調整する

組織のセキュリティ ニーズを満たせるようにポリシーをカスタマイズします

ポリシーは、エンドポイント上のアプリケーションの動作方法に関するルールを定義します。Cb Defense には事前定義済みの 3 つのポリシー、 **Standard** 、 **Monitored** 、 **Advanced** があります。これらのポリシーを使用することも、変更することも、または独自のカスタム ポリシーを作成することもできます。すべてのポリシーは、あらゆるタイプのマルウェアの実行、既知のプログラム、疑わしいプログラム、潜在的に迷惑なプログラムをブロックする必要があります。

推奨設定



次のステップ

組織のセキュリティをさらに強化するには

- センサー グループを作成する
- さらに多くのセンサーをインストールする
- ポリシーの微調整を継続する
- 2 段階認証を有効化する

詳細については Carbon Black User Exchange を参照してください。製品のドキュメント、リリース ノート、ナレッジ ベースの記事、サポート、ディスカッション、製品ニュース、最新情報などをご覧いただけます。

Cb Defense 製品のドキュメント
PSC 脅威調査
Cb Defense Ask Me Anything ウェビナー シリーズ
Carbon Black テクニカル サポート
Cb Defense ナレッジベースの記事
Carbon Black テクニカル アカデミー

