



## Cb Defense の作業の開始

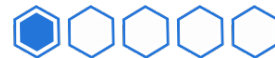
Cb Defense では、高度な予測モデルを使用してエンドポイント データを分析し、システムが危険にさらされる前に攻撃を阻止します。

**基本の 5 ステップで Cb Defense を始める**





# 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)

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。

## Admin (管理者)

アラートを表示してアクションを実行します。

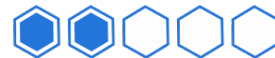
## Live Response Admin (Live Response 管理者)

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

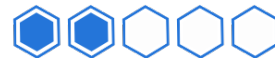
1. **[Endpoints (エンドポイント)]** をクリックします。
2. **[Sensor Options (センサー オプション)]** をクリックし、**[Add User(s) (ユーザーの追加)]** をクリックします。ユーザーはダウンロードリンクとインストールコードが記載された電子メールを受け取ります。センサーをインストールするには、エンドポイントの管理者権限が必要です。
3. Cb Defense で保護する各エンドポイントに PSC センサーをインストールします。デフォルトでは、新しくインストールされたセンサーには標準ポリシーが使用されます。

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

アラートのフィルタリング

ダッシュボードのウィジェットの表示、非表示、並べ替え

ダッシュボードデータを CSV ファイルへダウンロード

ポリシー ルールに基づいて拒否または終了された脅威を表示

ポリシー ルールが適用されていないアクティビティを表示

エンドポイント上にあるセンサーのステータスを表示


The dashboard displays the following data:


- Attacks Stopped:** 9 total attacks. Breakdown: Non-Malware (1), Potential malware (8), Malware (0), PUPs (0).
- Potentially Suspicious Activity:** 3 total activities. Breakdown: Non-Malware (1), Potential malware (2), Malware (0), PUPs (0).
- Attacks by Vector:** All vectors (Email, Web, Remote drive, Other net protocol, Removable media, App store) show 0.0%.
- Endpoint Health:** 320 total endpoints. Breakdown: Active (15), Inactive (217), Deregistered (57), Eligible for update (36), Quarantined (1), Bypass (31).
- Attack Stages:** RECON (0), WEAPONIZE (0), DELIVER/EXPL (0), INST/RUN (11), CMD+CTRL (0), EXECUTE GOAL (2).

## 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。定期的にはアラートを確認し、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。

STATUS	FIRST SEEN	REASON	P	T	DEVICE	TAKE ACTION
Policy Applied Ran	6:03:17pm Jun 18, 2018	The application cmd.exe invoked another application (eventguide.pdf) on behalf of eventguide[1].pdf. A Deny Policy Action was applied	4			

eventguide[1].pdf run\_another\_app run\_cmd\_shell unknown\_app  
cmd.exe policy\_deny run\_unknown\_app  
explorer.exe policy\_deny  
taskhost.exe enumerate\_processes

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。

## 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。

The screenshot displays the Carbon Black Alert Triage interface. At the top, a notification reads: "NON-MALWARE 6:03:17pm Jun 18, 2018 The application cmd.exe invoked another application (eventguide.pdf) on behalf of eventguide(1).pdf. A Deny Policy Action was applied". The interface shows a process tree on the left with nodes like services.exe, taskhost.exe, userinit.exe, explorer.exe, lexplore.exe, eventguide(1).pdf, cmd.exe, and adobe\_updater.exe. A legend identifies symbols for Denied Operation, Terminated, Invoked, Injected, Read Memory, and Accessed Target. A right-hand pane shows the selected node "eventguide.pdf" with a "Take Action" button and a "Summary" section containing: Reputation Not Listed, Process State Ran, Signature Verification Not Signed, and File Deleted Not Deleted. Below this is a "Process Details" section with expandable items for TTP, Signature, Malware, and Application Origin. A legend at the bottom right explains the "Deny Policy Action" icon.

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

## 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。

ドロップダウンアイコンをクリックすると、情報ウィンドウが拡大します。

Enter a search term and select a suggestion to create a query

View by Events Applications Devices Network

1 - 20 of 6253 Clear all

6:03:18pm Jun 18, 2018 cmd.exe The application C:\Windows\System32\cmd.exe invoked the application C:\Users\...\Desktop\eventguide.pdf. The operation was blocked by Cb Defense.

**Event ID:** 8393937e734311e8a4d77da3c0c5b66f **Agent location:** Off-Premise **Category:** Threat **Process started:** A few seconds ago **Alert ID:** ZKLCQOKG **Attack Stage:** INSTALL\_RUN **Priority score:** 4

**Device IP address:** ... **Device version:** Windows 7 x86 SP: 1 **User Name:** ... **Sensor installed By:** ... **Parent name:** eventguide[1].pdf **Parent process ID:** 3544

**Parent reputation:** NOT\_LISTED **Parent reputation (applied, cloud):** NOT\_LISTED **Parent SHA:** ec51cc8c044a460abd753678cf0e3806eed7451a01aca721a5e00a28dc08d884

**Parent command line:** "C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe" "C:\Users\...\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XPKU987E\eventguide[1].pdf"

**Process name:** cmd.exe **Process ID:** 3392 **App reputation:** TRUSTED\_WHITE\_LIST **App reputation (applied, white database):** TRUSTED\_WHITE\_LIST **App MDS:** ad7b9c14083b52bc532fba5948342b98

**App SHA:** 17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae

**Command line:**  
"C:\Windows\System32\cmd.exe" /Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\eventguide.pdf" (cd "Desktop"))&(if exist "My Documents\eventguide.pdf" (cd "My Documents"))&(if exist "Documents\eventguide.pdf" (cd "Documents"))&(if exist "Escritorio\eventguide.pdf" (cd "Escritorio"))&(start eventguide.pdf) To view the encry

**Target Name:** eventguide.pdf **Target Process ID:** 4294967295 **Target Reputation:** NOT\_LISTED **Target Reputation (applied, AV scan):** KNOWN\_MALWARE

**Target SHA:** ea6ae3c227c61a6a2ad69acdc50d08d64bdbb70e7c58b2a65a8d44abcddec15f0 **Target command line:** eventguide.pdf **TTPs:** RUN\_UNKNOWN\_APP, POLICY\_DENY

『Cb Defense: レピュテーションの優先度』を参照してください。



# 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

必要でない場合は、有効化しない

悪意のある/疑いのある/意図しないアプリケーションがないか環境をスキャン

オンアクセス ファイル スキャンモードは Aggressive (積極的) に設定

- Sensor UI: Detail message
- Allow user to disable protection
- Enable private logging level
- Run background scan
- Standard
- Expedited

*System performance will be affected during scan.*

**Scanner Config**

On-Access File Scan Mode

- Scan files on network drives
- Scan execute on network drives
- Delay execute for cloud scan
- Hash MD5
- Use Windows Security Center
- Allow user to override policy enforcement
- Require code to uninstall sensor
- Submit unknown binaries for analysis
- Auto-delete known malware hashes after

クラウドからのレピュテーションデータの更新を要求 (新しい脅威に対して有効)

センサーの不正なアンインストールを防止

クラウド分析を有効化

既知のマルウェアの自動削除を有効化

# 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ください。

[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](#)