データシート

Cb RESPONSE

業界をリードするインシデント対応と脅威ハンティングソリューション

Cb Responseは、最も正確なIR（インシデントレスポンス）および脅威ハンティングソリューションで、他のツールよりもより速く必要な回答を得ることができます。
すべての脅威の活動をキャプチャすることで、リアルタイムで脅威ハンティングを実行し、攻撃キルチェーン全体を可視化し、迅速にレスポンスと修復作業を実施できます。

あらゆる脅威が可視化され、全ての脅威活動をキャプチャ

今日の攻撃手法はより複雑化し、予測することが難しくなっています。攻撃者は、防御を潜り抜けるために様々な新規手法を編み出し続けています。攻撃を受ける前に「何が悪いのか」を知ることは不可能です。一つの解決策は、攻撃者のアクティビティが最初に脅威として検出されなかった場合でも、すべての脅威をキャプチャし、攻撃を可視化して対処することです。新規のマルウェアが攻撃の一部として自己削除する場合には、マルウェアが過去にエンドポイントに存在し、エンドポイントに対して何をしたのかを知ることが必要です。Cb Responseは、継続的にすべてのエンドポイントの活動を記録し、すべてのログを常時収集して集中管理することで、いつでも素早く過去のアクティビティへのアクセスを可能とし、セキュリティギャップが無いエンドポイントの可視性が得られます。
レスポンスに必要とする情報は常に利用可能であるため、迅速な調査が可能であり、疑問に対する確実な結論が得られます。
アラートの原因についての詳細が常に手元で参照できるため、アラート検証とトリアージ（処理の優先付け）が効率化されます。

攻撃のキルチェーンを可視化

すべての脅威のアクティビティをキャプチャするので、攻撃キルチェーン全体を可視化し、どのように攻撃されているかの詳細を容易に理解することができるようになります。
攻撃者がどこに行き、何をしたのか、また何を修復する必要があるのかが可視化されます。攻撃者がどのようにあなたを攻撃しているかを正確に把握できているので、自分の環境を防御する方法についてより良い対策を検討することができます。
ギャップの無いエンドポイント可視化によって、根本的な原因を常に把握し、将来の攻撃を阻止するためにセキュリティギャップを埋める対策が取れることになります。

攻撃キルチェーンを可視化することで、攻撃の根本的な原因と範囲を把握することができます。

導入のメリット

- **多量のアラートによる負担を軽減**
  アラートをより速くトリアージします
- **調査を迅速化**
  必要とする情報が常に利用可能なので、行き詰るということはありません
- **攻撃を確実に理解**
  攻撃者がどこに行って何をしたかが可視化されます
- **防御を潜り抜けた脅威を調査**
  脅威の潜伏期間およびダメージを減らします
- **次の攻撃が実行されないように対策**
  攻撃の根本的な原因を知ることで、セキュリティギャップや死角に取り組むことができます
- **IT運用の負担を軽減**
  不要なイメージの再構成やチケットを削減します
- **セキュリティの専門知識への要求を軽減**
  セキュリティチームの生産性を向上させます

提供方法：オンプレミス、クラウド提供またはパートナー経由
※日本では該当しない部分があります

使用例

- 情報漏えい対策
- 攻撃検出
- アラートの検証とトリアージ
- インシデント対応
- 攻撃の隔離
- 脅威のハンティング
- 攻撃後の修復
- 脅威の阻止

Carbon Black
Cb Responseは、私が本当に必要とした可視性を提供します。
― 金融サービス業　顧客

リアルタイムで脅威をハンティング

ギャップのないエンドポイント可視化によって、リアルタイムで脅威をハンティングすることができます。自身の環境固有の知識を活用して、既存の防御ツールを潜り抜け、検出ツールでも検知できなかった高度な脅威を積極的に追求し、発見することができます。
何か悪い事態が発生する前に、脅威ハンティングによって脅威や異常な動作を見つけることで、脅威の潜伏期間およびダメージを減らします。

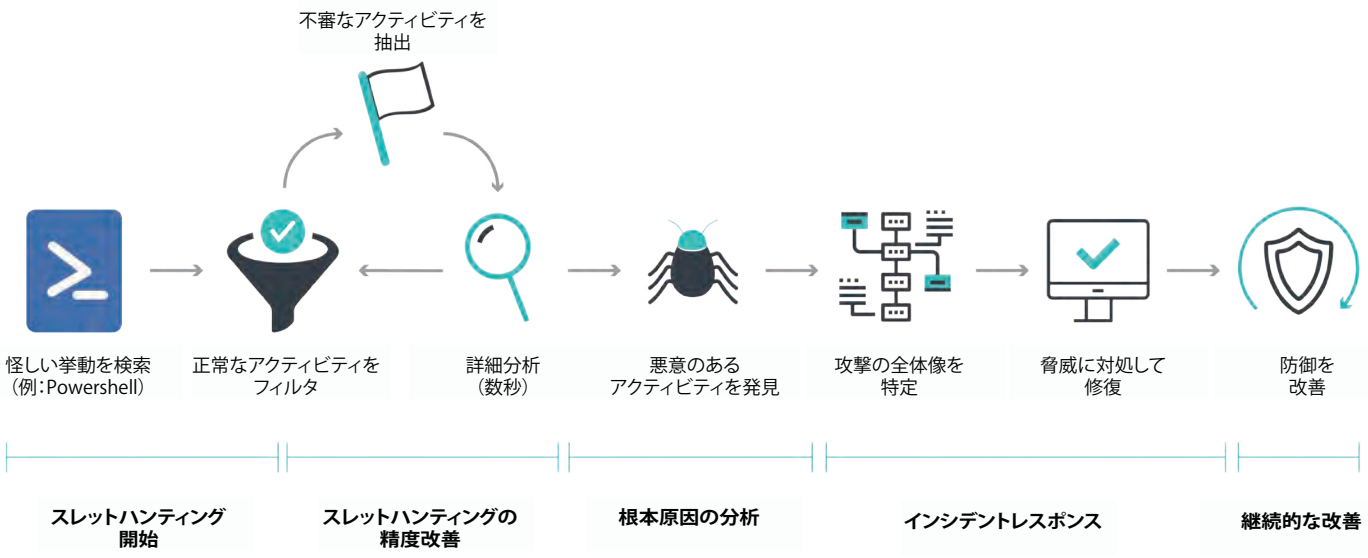
インシデントレスポンスと攻撃対象の修復

Cb Responseは、すべてのインシデント対応と脅威ハンティング、そして攻撃後の修復までを含む、単一のコンソールです。
検出された脅威に対して、対象エンドポイントを隔離したうえで、エンドポイントをリモートで調査してクリーンアップすることがどこからでも可能です。
詳細な根本的な原因と対応すべき範囲を用いてより正確な修復が可能となり、本当に必要な作業のみに限定することができます。不要なイメージからの復元作業を削減し、ITチームを必要以上に拘束することを避けることができます。

技術的特長

- CPU使用率1%未満
- RAM使用量20MB未満
- ネットワーク帯域幅使用は平均で50バイト/秒
- サーバとの双方向のSSL認証を通じて中間者攻撃に対する防御
- 管理、ストレージ、および制御を集中化

サポートされるプラットフォーム



Carbon Black Hunt Chain：Cb Responseユーザが利用可能な効果的な脅威回避および脅威ハンティングプロセス

NVC NETWORK VALUE COMPONENTS

株式会社ネットワークバリューコンポネンツ

〒144-0035 東京都大田区南蒲田2-16-2
電話: 03-5714-2050　　http://www.nvc.co.jp/