データシート

Cb Protection App for Splunk

サマリ:

Cb Protection App for Splunkは、Cb Protection Serverとエンドポイントのリアルタイムなデータに対する高度な分析とダッシュボードを提供します。これによりCb Protectionからのデータと関連するセキュリティイベントに対するより深い洞察を管理者は得ることができます。また、Cb Protectionのデータを Splunkの他のデータソースと相関させることで、分析と運用の改善を実現し、セキュリティチームに迅速かつ総合的な視点を提供します。

導入のメリット:

- Splunkの強力なデータ解析エンジンを活用することで、インフラ全体のアクティビティを一覧するといった、Cb Protectionのデータと他のデータソースを組み合わせる新たなダッシュボードの作成ができます。
- Cb Protectionへのより良いチューニングのために、導入された全てのエンドポイント状況を可視化できます。
- 単一ダッシュボードからファイルや端末の調査を迅速に行えます。
- インサイダーの脅威を検出し、管理者の監査を実行するために、すべての従業員の活動を可視化します。
- カスタムおよびアドホック・クエリを作成できます。

システム要件:

- Splunk 5.0以降
- Cb Protection 7.2以降

Cb ProtectionおよびSplunk

迅速に実用的なインテリジェンスの提供するためのデータ統合と可視化

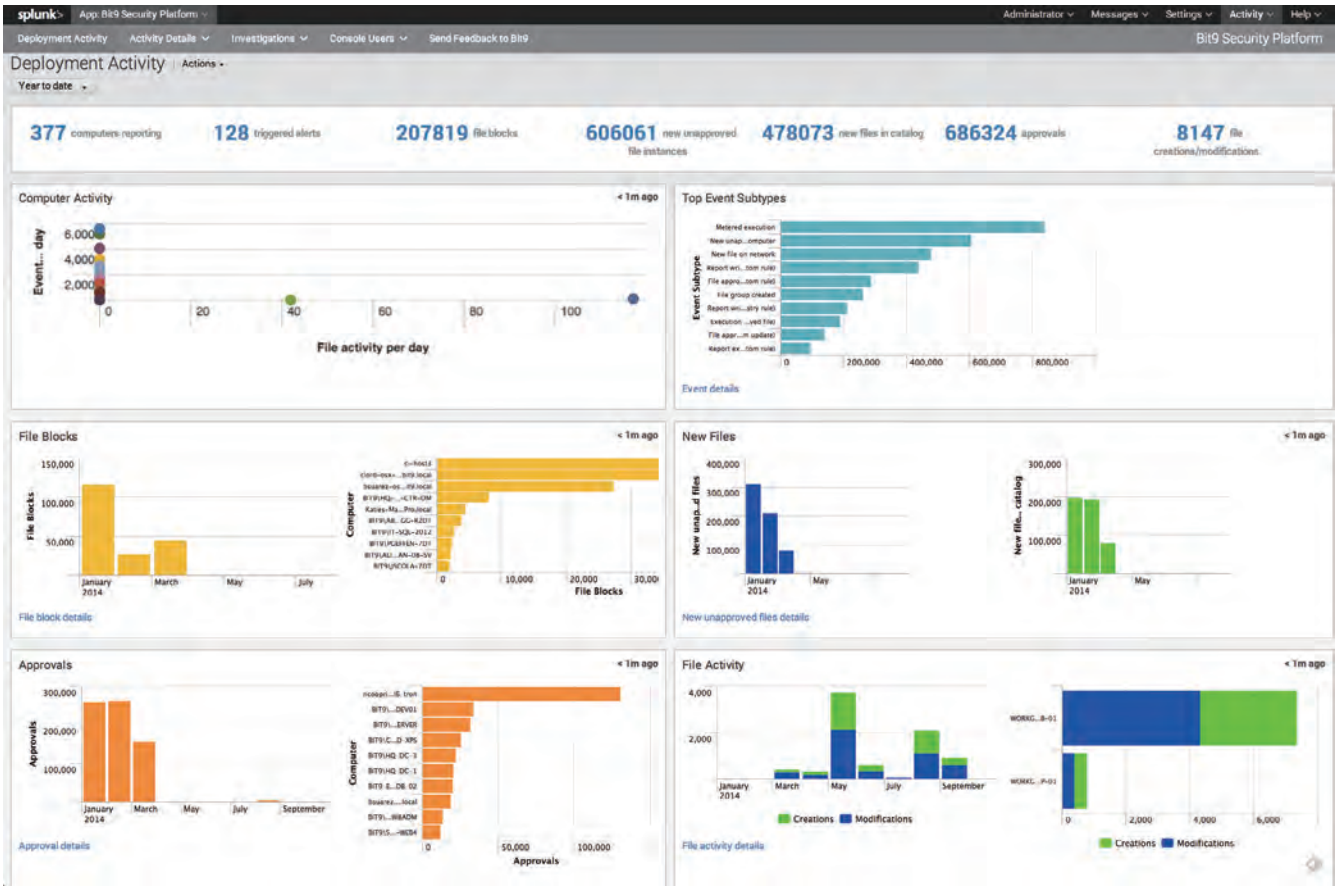
今日のセキュリティ運用チームは、主要なセキュリティと運用に関する質問への迅速な、一目で理解できる回答をするために、複数の情報源を組み合わせ、文脈分析を適用して、高速かつ実用的な情報を提供するツールを必要としています。
Carbon BlackとSplunkのパートナーシップにより、セキュリティチームは、ネットワークや組織内データソースといった関連するセキュリティ情報と、Cb Protectionのリアルタイムのエンドポイント情報を統合することができます。
統合を容易にし、運用インテリジェンスを向上させるために、Carbon BlackとSplunkは、高度なセキュリティレポートおよび分析のために、SplunkエンタープライズへCb Protectionからファイルアクティビティやイベントを自動的にインポートするアプリケーションを提供しています。
SplunkのApp Storeを介して無料で提供される「Cb Protection App for Splunk」は、Cb Protectionの運用管理を強化するSplunkの強力な可視化と分析機能を利用することで、より効率的なセキュリティ調査および監査のために、より高いレベルの実用的な情報を得ることができます。

「Cb Protection App for Splunk」の利用法:

- エンドポイントのアクティビティ（ファイルアクティビティ、ブロック、承認、アラート、イベントなど）を監視するためのプリセットビューおよび視覚的なダッシュボードによる運用の効率化
- 包括的かつタイムリーな調査のために単一のダッシュボードを使用して、特定ファイルやエンドポイント内部の調査を迅速に実行
- 信頼ソースへの変更を可視化することで管理者への監査の実施
- Cb Protectionアクティビティに対するカスタムおよびアドホック・クエリや、他のデータソースとCb Protectionのデータを相関させることによる、より深いレベルでの実用的な情報

CARBON BLACK
ARM YOUR ENDPOINTS

データシート: Cb Protection App for Splunk



Carbon Blackは、各顧客の次世代セキュリティ・インフラストラクチャ構築を支援するためには、ベンダー間の相互運用をサポートすることが必要だと考えています。高度な脅威に対するエンドツーエンドの保護を提供するソリューションを提供するため、Carbon BlackはSplunkや他の業界ネットワーク/SIEMのリーダーと提携しています。

Splunkや他の戦略的技術提携先とCarbon Blackの提携の詳細については、以下のURLをご覧ください:
www.carbonblack.com/solutions/ecosystem/

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/