BlackBerry
Intelligent Security. Everywhere.

データシート

セキュリティ侵害評価

過去の侵害を特定・評価して
将来のインシデントを未然に防ぐ

脅威アクターは、検知を回避するよう明確に設計された戦術、技法、手順（TTP）を使用して、攻撃の数を継続的に増やし、高度化を進めています。このようなリスクの高い環境において、組織はどのように自らのサイバー防御がすでに侵害されているか否かを確実に認識することができるでしょうか。侵害が発生した場合、どのように侵害の性質、範囲、影響を迅速に判断し、攻撃を封じ込め、被害を修復するための措置を講じることができるでしょうか。

今日の多くの組織には、これらの質問に自信を持って答えるために必要な可視性、ツールセット、リソース、経験が不足しています。憂慮すべき動向が続いており、2019 年には、組織がデータ侵害を特定するまでに平均 206 日、封じ込めるまでにさらに 73 日かかりました。これは前年比で 5% 近くの増加となっています。[1]

206
日

データ侵害の特定にかかる期間

＋

73
日

封じ込めにかかる期間

2019 年には、組織がデータ侵害を特定するまでに平均 206 日、封じ込めるまでにさらに 73 日かかりました。これは前年比で 5% 近くの増加となっています。

出典:2019 Cost of a Data Breach Report. IBM セキュリティ

1 2019 Cost of a Data Breach Report.IBM セキュリティ

BlackBerry® Security Services Compromise Assessment（CA）を使用すると、お客様がさらされているサイバーリスクを包括的に分析することで、この不確実性を軽減することができます。CA は企業全体のデータを収集し、不審なアクティビティを示す証拠がないかどうか分析します。また、お客様のネットワーク環境や業務にもたらされるリスクに基づき、詳細な調査のために侵入の痕跡（IOC）に優先順位を設定します。重点分野は以下のとおりです。

- データの持ち出しと破壊行為
- コマンドアンドコントロールアクティビティ
- ユーザー認証の異常
- マルウェアの持続性メカニズム
- 脆弱なネットワークホストとアプリケーションの構成

過去の侵害の証拠が発見された場合、BlackBerry Security Services CA のエキスパートは、侵害が発生した時期、場所、手法を判断して、再発防止のための戦術的な推奨事項を提供できます。侵害が現在進行中の場合は、インシデント対処（IR）にシームレスに移行し、キルチェーンの追跡、TTP の特定、修復とクリーンアップの支援を行います。

独自のツールとプロセスに人工知能（AI）テクノロジーを統合することで、BlackBerry Security Services CA チームは、予備段階の結果を迅速に生成し、多くの場合、初回データの収集の完了から数時間以内に、コモディティ化した攻撃や APT 攻撃を検知します。コンサルティングの終了時、お客様はレポートを受け取ります。このレポートには、脅威ハンティングの調査結果と、サイバー攻撃からの回復力を高めて攻撃対象領域を減らすための推奨事項が詳述されています。このサポートを受けるために、BlackBerry の既存顧客である必要はありません。あらゆる組織で BlackBerry Security Services をご利用いただけます。

サービスの概要

BlackBerry Security Services CA のコンサルタントは、環境リスクを評価し、セキュリティインシデントを特定し、ネットワーク環境で継続的な脅威アクターのアクティビティを発見するために、AI を活用したベストプラクティス手法を採用しています。BlackBerry Security Services CA によるすべてのコンサルティングでは、脅威ハンティングと攻撃対象領域の削減という 2 つの領域に対応し、初回評価からターゲット評価のフェーズに進みます。

初回評価

初回評価フェーズでは、BlackBerry Security Services CA チームが異常な動作、IOC、および環境に対するその他のリスクを探索するために必要なデータを捕捉する、軽量なソフトウェアとスクリプトのパッケージがお客様に提供されます。通常、このデータにはエンドポイントからのファイルシステムのメタデータ、ネットワークデバイスからのログデータ、補助セキュリティシステムからのイベントデータやアラートデータなどがあります。次に、BlackBerry Security Services CA チームは、独自のクラウドベースのツールと手法を利用して、データを正規化し、コンテキストに応じて理解し、情報を付加してフォーマットします。これにより生成されるフォレンジックアーティファクトは、独自の分析エンジンで処理され、さらなる調査が必要なホストとアクティビティを特定するためにレビューされます。

ターゲット評価

ターゲット評価フェーズ中には、スタンドアロンの実行可能ファイルを対象ホストに導入し、初回評価中にフラグが付けられた不審なアクティビティに関して、より詳細なフォレンジックデータを収集します。アクティブな侵害が検知された場合、BlackBerry Security Services CA チームは、インシデント対処（IR）にただちに移行し、ベストプラクティスの IR 手法を活用してキルチェーンを追跡し、悪用された脆弱性を文書化し、影響を評価し、修復計画を作成することができます。

成果物

コンサルティングの完了時、BlackBerry Security Services CA コンサルティングチームは、その調査結果と推奨事項を記載した包括的なレポートを提出します。

- **脅威ハンティングの調査結果**：過去または現在の侵害が検知された場合、レポートには、侵害の性質、範囲、環境への影響が詳述されます。
- **攻撃対象領域の削減に関する調査結果**：リスクに応じて優先順位を付けた攻撃対象領域の削減機会の評価とともに、企業のセキュリティ体制の改善に対する戦略的かつ戦術的な推奨事項が詳述されます。

コンサルティング中に見つかったセキュリティ上の問題について議論し、セキュリティ意識の高い組織文化を醸成するために、お客様のリーダー、経営陣、技術者とのグループプレゼンテーションのスケジュールを立てることができます。

予想される業務上のメリット

BlackBerry Security Services CA のコンサルティングは、サイバーリスクの管理に対してプロアクティブな予防ベースのアプローチを取るために組織を支援します。また、過去の侵害を特定し、その再発を防ぐために原因を評価することができます。現在進行中の侵害は、追跡し、封じ込め、修復することができます。これにより、組織のセキュリティ体制に対する信頼を回復することが可能になります。以下のような一般的なメリットがあります。

- **迅速な対処**：従来のコンサルティング企業が顧客の環境を評価し、潜在的な侵害に対処するためにかかる期間は数週間にわたることがあり、修復とクリーンアップのコストが増大するだけでなく、被害が拡大する場合もあります。BlackBerry Security Services CA のコンサルタントは、世界中のあらゆる場所で一貫したクラス最高のサービスをただちに提供することができます。

BlackBerry Security Services CA のコンサルティングは、サイバーリスクの管理に対してプロアクティブな予防ベースのアプローチを取るために組織を支援します。

- **迅速な結果**：BlackBerry Security Services CA チームは、ベストプラクティスに基づき、現場で実証済みの AI を活用した手法によって、迅速に結果を生成します。
- **包括的な分析**：BlackBerry 独自のツールは、ネットワーク全体のフォレンジック分析をサポートし、数千もの過去のコンサルティングから得られた IOC を活用しています。
- **運用負荷の小さいデータ収集**：データ収集方法は効率的かつ透過的であり、ほとんどすべてのアーティファクトが収集されます。
- **社内セキュリティチームのスキル開発の機会**：BlackBerry Security Services CA のコンサルタントによって実施される戦略的なマルウェア、フォレンジック、ログ分析のレポート作成は、教育とスキル開発のための貴重な機会を社内チームに提供します。
- **プロアクティブなリスクの低減**：組織は、さらされるリスクを減らし、将来のインシデントを予防する方法を過去の侵害から学びます。

もっと詳しく

インシデント対応と封じ込めのための BlackBerry Security Services の詳細については、コンサルテーション依頼フォームをご利用いただくか、お急ぎの場合は 03-5575-1511（代表番号）までお問い合わせください。

BlackBerry Security Services について

BlackBerry Security Services コンサルティングにより、お客様は、ゼロタッチ、ゼロトラストのアーキテクチャ内で、ミッションクリティカルな業務をセキュリティで保護し、エンドポイント、ワークスペース、ID を管理することができます。当社のコンサルタントは、組織がさらされるサイバーリスクを最小限にし、豊富な資金に支えられた持続的な攻撃を防御するために必要な深い知識と調査の経験を提供します。お客様と連携することにより、当社は、防御ファーストの手法を活用して、幅広いサイバーセキュリティの課題に対処し、強力かつ効果的なセキュリティ体制を構築するためにお客様を支援します。BlackBerry Security Services ソリューションの包括的なリストについては、当社のコンサルティングに関するトップページをご覧ください。

詳細については、BlackBerry.com にアクセスし、@BlackBerryJPsec をフォローしてください。

BlackBerry
Intelligent Security. Everywhere.

BB20-0407 | 200710