LogRhythm と BeyondTrust エンタープライズセキュリティソリューションの統合

製品概要

統合されたエンタープライズセキュリティのための LogRhythm：

* 脆弱で攻撃される可能性のある資産に対する動的な防御策
* 多方向の行動分析でリアルタイムのセキュリティインテリジェンスを提供
* 対象のデバイスに対して焦点が当たった自動スキャニング
* 統合的な脆弱管理との密接な統合

LogRhythm と BeyondTrust 社はエンタープライズセキュリティ分析および脆弱性管理のための統合ソリューションを開発しました。LogRhythm は自動的に BeyondTrust 社の RetinaCS からの脆弱データを取り込み、状況認知と統合的なセキュリティインテリジェンスに基づいたリアルタイムでのサイバー脅威に対する防御を提供します。

この 2 つの製品の統合により以下の機能が提供されます：

- IT 環境全体にわたり未適用のパッチや構成上の弱点などを含む脆弱ポイントのリアルタイムでの相関関係を作成し、エンタープライズの脅威インテリジェンスを提供する。
- ネットワークセキュリティデータと多方向からの行動分析を合わせることで可視性を向上し、違反検知機能を強化する。
- 意味のあるイベントと条件ロジックおよび現行の脅威分析をひも付することで正確な脅威検知を行い、フォールスポジティブやフォールスネガティブの件数を削減する。

BeyondTrust の脆弱性、脅威管理機能と LogRhythm　SIEM2.0 プラットフォームの多方向からの行動分析を合わせることでエンタープライズ規模の環境へ継続したリアルタイムの脅威検知と対応を提供します。

LogRhythm

LogRhythm 社はビックデータセキュリティ分析のリーダであり LogManagement および SIEM2.0、ファイルインテグリティ監視、ホストアクティビティ監視、などを一つの統合したソリューションでシームレスに提供します。常に変化している脅威の状況と併せて変

化する対応への課題を解決するためにセキュリティ、コンプライアンス、運用支援向け高パフォーマンスの完全製品群を提供します。LogRhythm は IT 環境で何が今現実に起こっているか、現状把握および行動可能な指針への統合的で有用な情報を提供します。

LogRhythmSIEM2.0 プラットフォームは以下の機能を提供します：

* Log とイベントの完全に統合化した管理
* 自動的に行動および統計のプロファイル提示
* 高度な相関性およびパターンの認識
* ファイルのインテグリティおよびホストアクティビティの監視
* 強力で高速な捜査、検索
* インテリジェントでプロセス駆動の SmartResponse
* 容易な操作性と管理

BeyondTrust

BeyondTrust 社は現況認識セキュリティインテリジェンスを提供する唯一のセキュリティソリューションベンダです。IT セキュリティリスクを削減するための可視性と制御を企業に提供しつつ同時にコンプライアンスレポートの作成を簡易にします。

我々はユーザ自身がインフラと IT 環境全体にわたるデータを防御することを可能にします。すべてのデバイス、たとえそれがデスクトップ上、データセンタ内、ポケット内、バーチャルマシン、クラウド上どこに対象があっても、可能な限り安全にします。

我々のソリューションはサイバー攻撃のもとになる脆弱性を検知し修正し、また間違え、意図的に限らずシステムやデバイス特権を不正利用することで起きる内部からの脅威を阻止します。つまり内部からまた外部からの脅威を防御するのです。

BeyondTrust は一貫したポリシ駆動の脆弱性および特権管理を提供し、役割ベースのアクセス管理、監視、ログ取得、監査、レポート機能で企業の資産を内部、外部から保護します。IT ガバナンスを可能にすることでセキュリティの強化、生産性の改善、コンプライアンス達成、また物理、仮想、モバイル、クラウド環境にわたってコストの削減を可能にします。

LogRhythm と BeyondTrust は密接に連携され BeyondTrust の RetinaCS 脆弱性管理ソリューションと LogRhythm の SIEM2.0 脅威管理機能が合体します。この 2 つのソリューションが合わさることでユーザは異常な行動、内部、外部からの脅威を検知し、現行の正確なエンタープライズ状況とインテリジェンスに基づき違反を阻止できます。

重要な資産の保護：

課題：高度化、洗練されまたどんどん進化している脅威に対応する為に、そして本当の意味でのエンタープライズセキュリティインテリジェンスを得るために組織は現行の脆弱データと実際に進行している攻撃の間のギャップを橋渡しする必要があります。

ソリューション： LogRhythm は BeyondTrust の RetinaCS 脆弱スキャンよりのデータとその他のマシンデータを合わせて高度な相関性およびパターン認識を提供します。高優先度の警告は既知の脆弱性が脆弱であると認識される対象のシステム上に悪用され、攻撃が仕掛けられようとしているときに生成されます。

更なる利点： SmartResponse のプラグインによりその対象の脆弱システムを孤立させ、即座に防御策を実行し環境内で攻撃が拡散するのを防ぐことが可能になります。

リスク管理：

課題：モバイルデバイスの広がり、クラウドアプリケーションおよび仮想環境の利用拡大などはセキュリティやリスク管理への複雑性を増します。課題の一つに攻撃が狙っているシステムやデータに悪用できるネットワーク内の弱点を検知することです。

ソリューション： RetinaCS は統合されたプラットフォームで IT 環境全体にわたる特権および脆弱に関するデータを取り込み、レポートします。LogRhythm がこれらのデータとその他のマシンデータとの相関性を取り、行動分析に照らしてネットワーク内の異常な行動不審な動きを検知します。

更なる利点： LogRhythm の AI エンジンにより行動が自動的にプロファイリングされ、アプリケーション、ホストネットワークに対する判断ラインや許容範囲の行動リストを作成します。これにより怪しい行動の検知や脆弱システムのプライオリティ付けの無駄な時間が削減されます。