ソリューションブリーフ

Recon：Veeamインフラストラクチャ用のプロアクティブな脅威検出機能

概要

Reconは、Veeam Data Platform AdvancedエディションおよびPremiumエディションに統合されている特許申請中の軽量ソフトウェアエージェントです。Coveware by Veeamと共同で開発したこのソリューションはデータ保護市場唯一のソリューションであり、実際のランサムウェアインシデントに基づき、プロアクティブな行動ベースの検出機能を提供します。

動作のしくみ

Reconは、以下を対象にVeeam環境を継続的に監視します。

- 不審なユーザーの行動と総当たり攻撃によるログイン試行
- 予期しないネットワーク接続
- ファイルの不審な操作やインストール
- データ窃取の試み

各イベントは分析され、既知の攻撃者の戦術や手法にマッピングされることで、IT・セキュリティチームが迅速に予防措置を講じることが可能になります。

主なメリット

- **積極的な脅威検出：**不審な活動をサイバー攻撃へと発展する前に検出します。
- **MITRE ATT&CKマッピング：**調査結果を敵対者の戦術、技術、手順（TTPs）に自動的に関連付けます。
- **迅速な導入：**Veeam Backup & Replicationサーバー、プロキシ、ゲートウェイ、Active Directoryサーバー、その他Veeam環境内のサーバー（最大10台）に簡単にインストールできます。
- **安全なデータ処理：**収集されたデータは、分析のために、暗号化されたクラウドベースのポータルに安全にアップロードされます。検出結果はVeeam Data Platform Threat Centerで利用可能です。
- **サードパーティ統合のためにAPI経由で利用可能な検出結果：**Microsoft Sentinel向けのVeeamアプリにはReconの検出結果が含まれます。

事例

Veeam Data Platform Premiumエディションを利用しているある自治体が、インフラストラクチャ全体にReconを導入しました。
国外IPからの総当たり攻撃を即時検出し、ITチームにアラートを出しました。迅速な対応が取られ、ログイン試行が遮断され、侵害やランサムウェア攻撃を未然に防ぎ、機密性の高い財務および個人データが保護されました。

なぜ重要なのか

ランサムウェアの脅威が急速に進化する中、組織はリアクティブな防御だけでは不十分です。Reconは、チームが被害が発生する前に脅威を検出し、対応できるようにすることで、比類のないデータの回復力と安心感を提供します。

補完技術

ReconはVeeam Data Platformの包括的なセキュリティ機能の一部であり、次が含まれます：

- **インラインスキャン：**インラインエントロピー分析を提供し、AIを活用したインプロセス検出によって、ランサムウェアの暗号化や、ダークWebリンク、身代金メモといったテキストアーティファクトを検出します。
- **ゲストインデックスデータスキャン：**バックアップ中に高度なファイルシステムアクティビティ分析を活用し、脅威を検出します。具体的には、疑わしいファイルの出現、大量のファイル削除、ファイル名の変更、またはファイル拡張子の変更などの活動を対象とします。
- **Veeam Threat Hunter：**業界最高レベルの機械学習とヒューリスティック分析、署名ベースのバックアップスキャナーであり、数百万種類のマルウェアを検出できる設計となっています。最新の保護を維持するため、マルウェアの署名データベースは頻繁に更新されます。
- **IoC（侵害の兆候）ツールスキャナー：**脅威アクターが利用するツールを特定し、影響が出る前に通知します。
- **セキュリティおよびコンプライアンスアナライザー：**バックアップ環境がセキュリティのベストプラクティスに準拠していることを診断する、組み込み型セキュリティ評価ツールです。

Veeam Softwareについて

データの回復力におけるNo. 1のグローバルマーケットリーダーであるVeeam®は、すべてのビジネスが、必要なときに必要な場所ですべてのデータを確実に制御し、混乱の後に回復できるべきだと考えています。Veeamはこれを「根源的な回復力」と呼んでおり、これをお客様の組織で実現するための革新的な方法を生み出すことに力を注いでいます。Veeamのソリューションは、データのバックアップ、データの復元、データポータビリティ、データセキュリティ、データインテリジェンスを提供することで、データの回復力を強化できるように構築されています。Veeamは、クラウド、仮想、物理、SaaS、Kubernetesの環境全体でアプリケーションやデータが保護され、常に利用可能な状態にすることで、ITリーダーやセキュリティリーダーに安心をもたらします。シアトルに本社を置き、30か国以上に事業拠点を構えるVeeamは、82%のFortune 500企業を含む全世界で55万社を超える顧客を保護しており、これらの顧客はVeeamを信頼してビジネス継続性を維持しています。根源的な回復力はVeeamから始まります。詳細については、www.veeam.comをご覧になるか、LinkedIn（@Veeam-Software）およびX（@Veeam）でVeeamをフォローしてください。