ソリューションブリーフ

Veeam Recon Scanner：データの回復力を確保するプロアクティブな脅威検出機能

概要

Recon Scannerは、特許申請中の軽量ソフトウェアエージェントであり、Veeam Data Platform Premium Editionに統合されています。VeeamがCovewareと共同で開発したこのソリューションは、実際のランサムウェアインシデントに基づいたプロアクティブな挙動検出を提供するデータ保護市場唯一のソリューションです。

動作のしくみ

Recon ScannerはVeeam環境を継続的に監視し、次の項目を対象とします。

- 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向けの新しいVeeamアプリには、Recon Scannerの検出結果も含まれています。

ソリューションブリーフ

事例

Veeam Data Platform Premium Edition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 Scanner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。

補完技術

Recon ScannerはVeeam Data Platformの包括的なセキュリティ機能群の一部であり、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、ファイルのリネーム、またはファイル拡張子の変更などの活動を検知します。
- **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数百万種類のマルウェアを検出するために設計されています。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。

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 Scanner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。

Veeam Softwareについて

Veeam®は、データの回復力におけるNo. 1のグローバル市場リーダーとして、あらゆる分野の企業が、障害の発生時に自信を持って状況を管理し、すべてのデータを必要な場所で必要なときに利用できる世界を目指しています。Veeamでは、この「根源的な回復力」を通じてお客様が堅牢な回復力を実現できるよう、革新的なソリューションの開発に力を注いでいます。Veeamのソリューションは、データの回復力を強化できるように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。米国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、Global 2000の67%の企業も含め、全世界で55万社を超えるお客様にご信頼いただいており、さまざまなサービスや製品の提供を通じてお客様をご支援しています。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/jpをご覧になるか、LinkedIn（@veeam-software）およびX（@veeam）にてVeeamをフォローしてください。

→ 詳細はこちら：veeam.com

→ ここをクリックしてRecon Scannerの動作をご覧ください。