tenable

LCE™

Tenable は、継続的な可視化と重要なコンテキストによって組織のセキュリティプログラムに変革力をもたらす継続的な監視を提供して、断固とした対策を実現可能にします。

製品概要

Tenable Log Correlation Engine®（LCE®）は Tenable SecurityCenter Continuous View®（SecurityCenter CV™）の重要なコンポーネントです。実際のネットワークトラフィックからのイベントログデータ、侵入検知データ、システムやアプリケーションのログ、インフラストラクチャ内のユーザー活動などを集積、正規化、相互に関連付けし、分析を行います。

LCE を使用する利点

- 企業内ネットワーク全体の様々なデバイスやアプリケーションによって生成されたログデータから、ユーザーとネットワークのアクティビティを正規化、相互に関連付けし、分析。
- 膨大なネットワークデバイスやアプリケーションで生成されたログの保存、圧縮、全文検索が可能。
- 監査可能なインフラストラクチャを維持することにより、社内ポリシーや規制要件へのコンプライアンスを証明。
- 無許可の変更や削除がないかファイルとディレクトリを監視。
- 組織の中で実行されているマルウェアや悪意のあるシステムプロセスを検出。
- ユーザーのアクセスログと動向を収集して、企業内脅威情報を作成し、社員がインターネットで見ている場所、アクセスしているシステム、実行しているプログラムなどをピンポイントで判別。
- 既存のルールと一致しないログを分類して保存し、詳細な分析を実施して、以前は見落とされていたであろうアクティビティに管理機能を提供。
- USB デバイス、CD-ROM、DVD などの利用状況について、ローカルとリモートの Windows システムを監視。
- ファイアウォールの瞬間的なトラフィック増大、ウェブアプリケーションのエラー率の変化、サービス妨害攻撃など、あらゆるログソースでのアクティビティのベースラインからの偏差を自動検出。

SecurityCenter CV の一コンポーネントとしての Log Correlation Engine

Tenable SecurityCenter CV は Tenable の継続的な監視プラットフォームであり、ネットワークヘルスの最も包括的で統合的なビューを提供します。

SecurityCenter CV は複数の Nessus®スキャナーのほか、複数の Nessus Network Monitor インスタンスや Log Correlation Engine サーバーを管理しながら、リアルタイムの脅威の検出、重大なログ/イベント監視、カスタムコンプライアンス監視機能の相関関係を、ロールベースの 1 つのインターフェイスで提供するために、ユーザーは結果を評価、通知、報告して、効果的な意思決定に役立てることができます。

SecurityCenter は、ネットワークのスキャン、パッシブモニタリング、および既存のアセットやネットワーク管理データツールとの統合の組み合わせにより、ネットワークアセットをカテゴリに体系化してから、これらすべての情報をエンタープライズ規模のログデータに相互に関連付けて、システムとネットワークアクティビティの包括的なビューを提供します。

主要機能

異常の検出とイベント相関性

イベントの収集が進むと、LCE は各デバイスの統計的プロファイリングを使用して、想定される動作に見られる変化を識別します。イベントタイプの増加、接続の増大、クライアントまたはサーバーの動作の劇的な変化など、異常な活動が検出された場合は、アラートが生成されます。

LCE には高度な相関性ルールが組み込まれています。これらのルールはワームの感染、ネットワーク異常、コンプライアンス違反、データ侵害、高度なセキュリティ脅威、ワイヤレスアクセスポイントの乱用など、様々な問題を探知します。これらのルールは TASL（Tenable アプリケーションスクリプティング言語）で記述されているため、必要に応じて定義の追加や変更ができます。

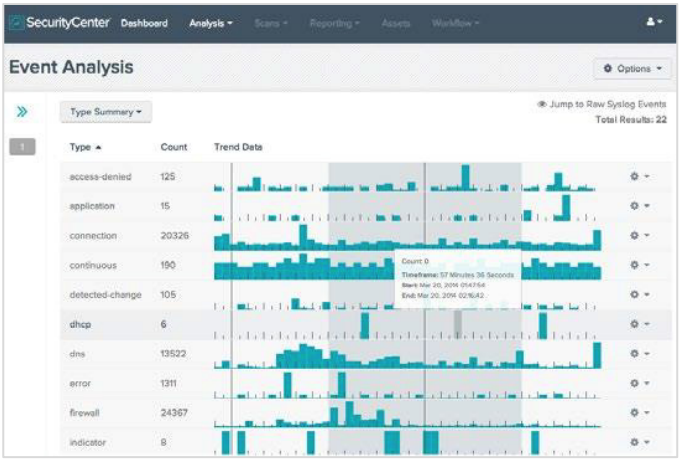
レポートと分析

SecurityCenter CV のフォレンジック分析とインシデント応答の機能、そしてセキュリティアプリの広範なライブラリは、脆弱性、脅威、侵害を統合したデータストア全体を 1 つのウェブインターフェイスから利用しています。以下はその一例です。

- **ログの保持** – Log Correlation Engine に送信されたログは、すべて同一のハードディスク上に保存するか、SYSLOG サーバーに転送するか、ストレージエリアネットワークに書き込んで、コンプライアンス遵守の取り組みやフォレンジック調査に役立てることができます。ログデータはローテーション、アーカイブ、圧縮形式で Log Correlation Engine 上に保存可能で、Log Correlation Engine のインターフェイスか SecurityCenter から検索できます。
- **Log Correlation Engine クライアント** – Log Correlation Engine はそれぞれが数千の Log Correlation Engine クライアントに接続可能で、Windows のログ、ウェブのログ、システムコマンド、syslog、ネットワークトラフィック、ファイルの整合性情報などを収集するよう設計されています。さらに、LCE ウェブクエリークライアントは AWS（アマゾンウェブサービス）からイベントをインポートして、クラウドアプリケーションを監視できます。また、Salesforce から、成功したログイン、失敗したログイン、ユーザー変更イベントをインポートすることもできます。

集中管理

Log Correlation Engine クライアントの一元的な運用管理機能によって、導入と管理の時間を大幅に節減します。これにより、効率的な展開とリアルタイムの構成変更が可能になります。



詳細情報：tenable.comにアクセスしてください
お問い合わせ：メール（subscriptionsales@tenable.com）でお問い合わせください。またはtenable.com/contactをご覧ください