

## セキュリティ管理

チェック・ポイントのセキュリティ管理ソリューションは、統一化されたポリシー管理、モニタリング、および分析を可能にします。

# Eventia Analyzer

セキュリティ・イベントの管理を簡素化

## 課題

今日のセキュリティ・アーキテクチャは、ネットワーク上で動作するサーバやホスト、アプリケーションを有害なアクティビティから保護するために数多くのデバイスで構成されており、複雑化、マルチレイヤ化が進んでいます。これらのデバイスが出力するログは膨大な量になるため、その分析には多大な時間と労力が必要になります。平均的な企業の場合、侵入検知システムが生成するメッセージは1日あたり50万件以上、ファイアウォールが生成するログ・レコードは1日あたり数百万件にもなる場合があります。また、ログに記録されたデータの中には、それ単体では特に問題のないアクティビティを示しているように見えながら、生のデータを相関分析してみると、異常なイベントや攻撃、ウイルス、ワームの痕跡であることが判明するものもあります。そのため企業は、各種のネットワーク・デバイスやセキュリティ・デバイスが生成する大量のデータの中から、価値のある重要なものだけを抽出することのできる管理手段を必要としています。

## 解決策

Eventia® Suiteは、ITセキュリティ部門が行うセキュリティ・ログの分析とレポートングにおいて、そのコストの低減と複雑さの軽減を支援するためのセキュリティ情報/セキュリティ・イベント管理 (SIEM) ソリューションです。Eventia Suiteは、セキュリティ・イベントの相関分析をリアルタイムで行うEventia Analyzer™と、集中レポートングと履歴傾向分析に使用するEventia Reporter™で構成されています。Eventia Analyzerは、チェック・ポイントの境界、内部、Web、およびエンドポイントのセキュリティ・デバイスのログ・データ、さらにはサードパーティ製セキュリティ・デバイスのログ・データを相関分析し、何らかの判断が求められる重要なイベントだけを優先的に自動抽出します。Eventia Analyzerは生成されたログ・データを自動的に集計して相関性分析を行うことにより、確認すべきデータ量を最小限に抑え、重要なセキュリティの脅威には、高い優先度を付けます。これらの脅威はデバイスごとに個別に確認するだけでは検出できないこともありますが、時系列で相関性分析を行うことによりパターンの異常性が見えてきます。セキュリティ・チームは、Eventia Analyzerを利用することで、環境内のデバイスから生成される膨大なデータを綿密に調査する必要がなくなり、ビジネスに重大な損害を与える可能性のある危険な脅威の調査と対策に集中できるようになります。

## 製品の概要

Eventia Analyzerは、さまざまなデバイスからのイベントを自動的に優先付けし、インテリジェントなアクションを実行する包括的なセキュリティ・イベント管理ソリューションです。

## 製品の特徴

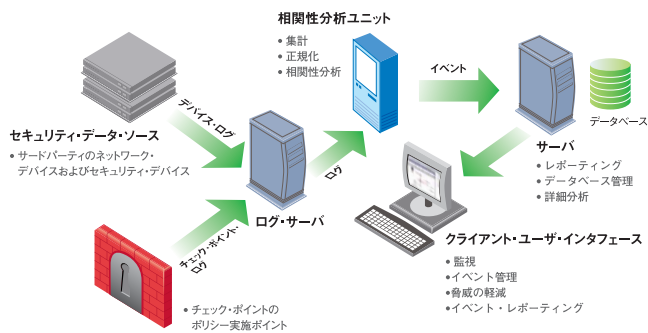
- チェック・ポイント・ゲートウェイおよびサードパーティ製製品のセキュリティ・イベントを一括して収集し、相関性を分析
- 通常のアクティビティを基に判断するインテリジェントな学習モード
- 定義済みセキュリティ・イベントとカスタム・セキュリティ・イベント
- 有害なアクティビティに対するリアルタイム・アラートおよび自動防御
- チェック・ポイントのSmartCenter™およびProvider-1®との統合
- サードパーティ・デバイスのログをチェック・ポイント形式に変換するログ解析エディタ (特許出願中)

## 製品の利点

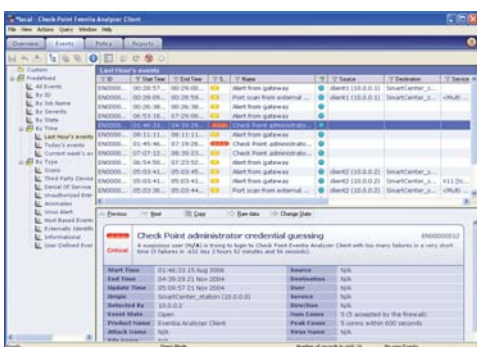
- ノイズをフィルタリングし、重要性の高いセキュリティ・イベントだけを抽出
- リアルタイムな対応により潜在的なリスクを軽減
- 最も重大な脅威に対応するため、既存のリソースを優先順位付け
- 容易な導入とTCOの低減
- 法令遵守要件に対応



NGXプラットフォームによりチェック・ポイントの統一されたセキュリティ・アーキテクチャを実現します。



Eventia Analyzerには、事前定義済みのイベントや、イベントを素早くカスタマイズするためのウィザードが多数用意されています。



Eventia Analyzerでは、特定のセキュリティ・イベントについて詳細に分析できるため、他のソリューションでは到底見つけることができない脅威の検知が可能になります。

## 拡張性のある分散アーキテクチャ

Eventia Analyzerは、拡張性のある柔軟なアーキテクチャを提供します。大規模な企業ネットワーク内で、各相関性分析ユニットは毎日数百万におよぶログの管理を行えます。Eventia Analyzerは単一のサーバにインストールすることもできますが、分散アーキテクチャを利用して処理負荷を複数の相関性分析ユニットに分散させるような柔軟な導入も可能です。

## 集中的なイベント相関性分析

Eventia Analyzerは、すべてのチェック・ポイント製品のほか、サードパーティ製のファイアウォール、ルータ、スイッチ、オペレーティング・システム、メール・サーバ、Webサーバ、侵入検知システム、アンチウイルス・アプリケーションなどが生成するセキュリティ・イベントを一括して相関性分析および管理できます。生成されたログ・データは、チェック・ポイントおよびサードパーティ・デバイスからの安全な接続を介してEventia Analyzerの相関性分析ユニットに収集され、一括して集計、正規化、分析が行われます。サードパーティ・デバイスのログは、Eventia Analyzerに組み込まれているログ解析技術(特許出願中)により簡単にチェック・ポイント形式に変換できます。各段階においてデータの少量化と相関性分析が

行われるため、重要なセキュリティ・イベントだけが詳細分析のために次の段階に送られます。ログ・データベースのデータ量が定義済みセキュリティ・イベント・ポリシーに設定されたパラメータを超えると、セキュリティ・イベントが起動されます。Eventia Analyzerには、事前定義済みのカスタマイズ可能なセキュリティ・イベントが多数用意されており、迅速な導入が可能です。これらのセキュリティ・イベントには、脆弱なホストを狙った不正なスキャン、不正なログイン、サービス拒否攻撃、ネットワークの異常、その他のホスト・ベースのアクティビティなどがあります。ウィザードや事前定義済みのイベントを使用してユーザ独自のイベントを簡単に作成でき、特定の用途に合わせてシステムを微調整することも可能です。セキュリティ・イベントは、さらに詳細に分析され、重要度レベルが割り当てられます。重要度レベルにしたがって、有害なアクティビティをゲートウェイで直ちに防御するために、自動アクションが起動されます。新しい情報が流入すると、状況の変化に対応して重要度レベルが調整されます。

## 簡単な導入

Eventia Analyzerは既存のSmartCenter™およびProvider-1®ログ・サーバとのインタフェースを備えているため、ログの収集や分析をデバイス・ログ・サーバごとに構成する必要はありません。Eventia Analyzerサーバは、SmartCenterまたはProvider-1で定義されているすべてのオブジェクトに自動的にアクセスし、それらを使用してセキュリティ・イベント・ポリシーを定義および実施します。このような緊密な統合によって、Eventia Analyzerがネットワークのトポロジを自動的に学習し、トポロジ要素の影響を受けやすい相関イベントを検出することを可能にしています。

## 容易な保守

ネットワークにインストールしたEventia Analyzerは、学習モードによって特定のサイトにおける通常のアクティビティ・パターンを基準化し、システムを微調整するためのポリシー変更を提案します。また、使いやすいイベント・ウィザードで、ユーザ固有の環境に合わせて柔軟にイベントをカスタマイズできます。インストールと保守が容易であるため、ITやセキュリティのスタッフを増員することなく対応できます。

システム要件	
プラットフォーム	Linux, SecurePlatform™, Solaris, Windows
対応OS/デバイス	<p>&lt;対応チェック・ポイント製品&gt;</p> <p>Connectra, Firewall-1 GX, Check Point Endpoint Security, UTM-1, VPN-1 Power, VPN-1 SecureClient, VPN-1 UTM</p> <p>&lt;サードパーティ製対応OS / デバイス&gt;</p> <p>3COMファイアウォール, Apache Webサーバ, Cisco PIXおよびIDS, Ciscoルータ, FreeBSD OS, Intrusshield, ISS RealSecure, Kaspersky Antivirus, Linux OS, NetContinuum, NetScreen, Sendmail, Snort IDS, Solaris OS, Symantec Antivirus, Tipping Point SMS, Trend Micro Antivirus, Windows OS</p>
対応するチェック・ポイント製品のバージョン	NGおよびNGXバージョン

## 製品に関するお問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社  
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F  
http://www.checkpoint.co.jp/ E-mail: info\_jp@checkpoint.com Tel : 03 (5367) 2500