

Eventia Reporter

セキュリティ実施状況を可視化する強力なレポート・システム

課題

セキュリティ管理者は、ネットワークを効果的かつ安全に管理するために、ネットワークの使用状況や、セキュリティ実施状況について包括的で明確な全体像を必要としています。一方、経営者層は長期的な方向性や意思決定に役立ち、企業ネットワークの成長を効果的に管理することが可能なツールを必要としています。一般に、ネットワーク内に点在するさまざまなセキュリティ製品が吐き出すログ・ファイルには大量のデータが記録されますが、これらのログ・ファイルを手動で確認し、ネットワークやセキュリティの活動の長期的な傾向を追跡したり潜在的な問題を把握することは困難であり、多くの時間が必要となります。

解決策

チェック・ポイントのセキュリティ情報およびセキュリティ・イベントの管理を簡単に実現するEventia Suiteの一製品であるEventia Reporter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・ゲートウェイからログ・データを収集し、グラフィカルで見やすいレポートを生成する集中レポート・システムです。Eventia Reporterでは、企業全体のログデータの分析結果を統一した形式で表示するため、セキュリティ管理者は、ネットワークのセキュリティ状況を網羅的に把握することができます。管理者はEventia Reporterを利用することで、セキュリティやネットワークに関する最新の統計データをより高いレベルで簡単に参照できるため、ネットワーク・リソースの配置やセキュリティの最適化、法令遵守などに関する重要な意思決定をより適切に下すことが可能になります。Eventia Suiteには、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ことのできるEventia Analyzer™も含まれます。

集中レポート環境

Eventia Reporterには、事前定義されたレポートが多数用意されているので、レポート分析を行うたびにレポートに関する設定を行う手間を省略でき、管理に必要な時間とコストを削減することができます。これらのレポートは、ある特定製品用のレポートとして提供されるほか、いくつかのカテゴリに分類されて提供されています。例えば、複数の製品にまたがるセキュリティ/ネットワーク活動、ファイアウォール・セキュリティ/ネットワーク活動、エンドポイント・セキュリティ、アンチウイルスなどのカテゴリが用意されています。

各レポートは、ネットワーク上における特定タイプのトラフィックや活動に関して詳しい情報を提供するサブ・メニューで構成されています。また、ユーザごとに必要な情報の要件に合わせて、レポートをカスタマイズすることもできます。事前定義されたレポートが特定のニーズに対応できない場合、セキュリティ管理者は、必要なデータのみを抽出するようレポート・フィルタを調整するだけで、簡単にレポートをカスタマイズできます。

自動化されたレポートの配布とデータベースのメンテナンス

Eventia Reporterでは、管理者が常時介在することなく、定期的にレポートを生成するようスケジュールを設定できます。例えば、毎日指定した時刻、週または月の特定日、または指定日にレポートを生成するようスケジュール設定できます。複数のスケジュールを設定できるため、最も要求度の高いレポート・ニーズにも柔軟に対応できます。これらのレポートは、E-mail、FTPへのアップロード、またはWebサイトを通じて特定のユーザに自動配布することができます。

製品の概要

Eventia Reporter™は、チェック・ポイントの複数のゲートウェイより収集された大量のログ・データから重要な情報を素早く抽出するための分析およびレポート・システムです。

高い安全性と冗長性を備えたアーキテクチャ

- ネットワークの使用状況、セキュリティ、ユーザの活動を一元的にレポート
- レポートの自動スケジュール設定と自動配布が可能
- ログ・データベースの自動メンテナンス
- 優れたスケーラビリティとパフォーマンス

製品の利点

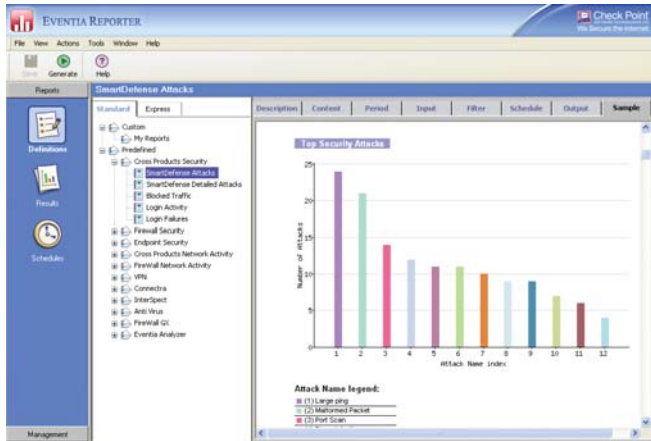
- セキュリティ・データへのアクセスを一元化するため、容易にデータの解析と傾向分析を行うことが可能
- セキュリティ投資に対する投資効果を明確化
- セキュリティとネットワーク活動に関する傾向分析のレポート作成を合理化
- 法令遵守を容易に監査することが可能



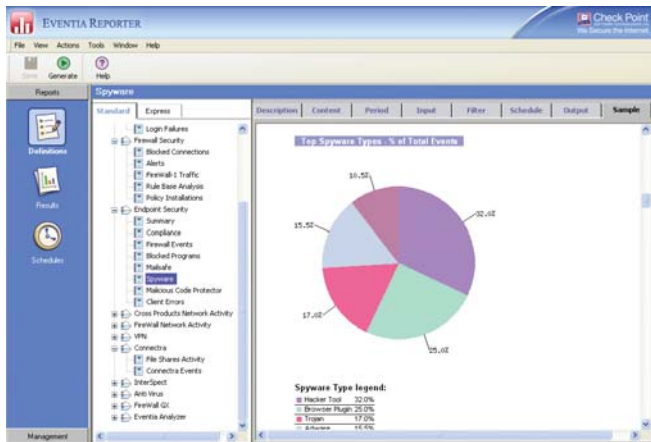
NGXプラットフォームによりチェック・ポイントの統一されたセキュリティ・アーキテクチャを実現します。

柔軟な導入と拡張が可

Eventia Reporterは、SmartCenter™環境とProvider-1®環境の両方に対応しています。Provider-1環境では、ネットワーク全体を対象とするグローバルなレポート環境として使用することも、特定のネットワーク・セグメントまたは顧客に限定したレポート環境として使用することもできます。また、大規模環境のレポート・ニーズに合わせ、Eventia Reporterを複数導入して並列に動作させることも可能です。Eventia Reporterには、大規模環境と小規模環境のどちらにも対応する幅広いインストール構成が用意されています。例えば、パフォーマンスや導入の柔軟性を重視する場合は、Eventia Reporterを専用マシンにインストールします。またコストの低さとシンプルさを重視する場合は、SmartCenterサーバまたはEventia Analyzerサーバと同じマシンにインストールできます。



Eventia Reporterでは、複数の製品にまたがるレポートを作成できます。図のレポートは、SmartDefense™によって検出された攻撃を示しています。



Eventia Reporterでは、境界セキュリティだけでなく、エンドポイント・セキュリティに関するレポートも作成できます。図のレポートは、エンドポイント・コンピュータで検出されたスパイウェアを示しています。

容易な傾向分析

Eventia Reporterによるレポートの生成を自動化すると、セキュリティやネットワークの状況を継続的かつ効率的に把握できるようになります。また管理者は、総合的なセキュリティ・パフォーマンス分析や監査を実施するための経営層や管理責任者向けのレポートを生成することもできます。

サポートされているオペレーティング・システム	
Eventia Reporter GUI	Solaris 9 Windows 2000/2003 Server/XP
Eventia Suite Server	RedHat Linux Enterprise 3.0 SecurePlatform™ Solaris 9 Windows 2000/2003 Server

注意：Eventia Reporterは、Nokiaオペレーティング・システム上で動作している専用のSmartCenterサーバにプラグインとしてインストールできます。ただし、Eventia Reporterは、ハードディスクを搭載しないNokiaプラットフォームで利用することはできません。

©2003-2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, Check Pointのロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, Firewall-1, Firewall-1 GX, Firewall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, puresecurityのロゴ, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL TurboCard, Security Management Portal, Sentivis, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, TurboCard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書に記載された製品は米国の特許No.5,606,668、5,835,726、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

P/N 502421-J 2008.02 ※記載された製品仕様は予告なく変更される場合があります。