Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Next Generation SmartEvent

ビッグデータを高速に分析しセキュリティ脅威を可視化

課題

近年、セキュリティ関連の「ビッグデータ化」の勢いは拡大する一方です。組織のネットワークを構成するモバイル・デバイスやエンドポイント、ゲートウェイの増加により、かつてないほど多くのデータが生成されているのが大きな理由です。各種デバイスで日々生成される膨大なログやイベント情報、セキュリティ・インシデント情報の監視に必要なリソースは右肩上がりに増え、セキュリティ・イベント管理の重要性が高まると同時に、問題はますます複雑化しています。

従来のイベント分析ツールは、セキュリティ関連のビッグデータを効率よく処理する機能が不足し、十分な機能を備えていても使い勝手に問題を抱えていました。多くの組織は、日々蓄積される大量のデータに潜む重要なイベントや本物のセキュリティ脅威の切り分けに苦労しています。

そこで求められているのが、ビッグデータを蓄積してリアルタイム分析を行う高機能なイベント監視ソリューションです。シンプルで使い勝手に優れ、フィルタリングしたデータから重要なイベントのみを抽出し、セキュリティ脅威を素早く検出、調査する強力なセキュリティ分析機能が期待されています。また、使用デバイスやタイミングを問わず監視機能が利用可能で、十分な情報を基に的確な判断を下す機能も重要です。

解決策

Next Generation SmartEventは、ネットワーク上で発生しているアクティビティをフィルタリングして、リアルタイムで可視化するソリューションです。カスタマイズ可能なビューで自社に関係するアクティビティのみを監視し、ワンクリックでイベント情報に対応するルールや保護機能を作成できます。レポートのカスタマイズにも対応しており、主要な関係者は、ネットワークで発生している重要なセキュリティ・アクティビティを素早く把握し、自身の担当に関係するデータに絞って対策を検討できます。監視対象を重要なイベントに絞り込むことも可能で、無駄な時間を節約し、緊急性の高いイベントから優先的にインシデント対応を進められます。

ビッグデータに基づく検出技術を導入したNext Generation SmartEventは、わずか数秒でセキュリティ脅威を検出します。フォレンジック分析に適応した詳細ビューへの移動も、概要ビューからワンクリックで済みます。また、サジェスト機能と履歴機能を備えた全文検索を使用すれば、未整理のデータを素早く分析して重要なセキュリティ・イベントを見つけ出すことができます。Next Generation SmartEventなら、数十億件のログ情報の収集、処理、検索がわずか数秒で終了します。

さらに「場所を選ばない監視」を可能にするWebポータルにより、ネットワークのセキュリティ状況を常に把握し、あらゆるセキュリティ脅威を監視できます。セキュリティ状況を確認、制御する際には、Next Generation SmartEventに場所や時間を問わずアクセス可能なWebポータルが効果を発揮します。

社内からでもモバイル環境からでも、重要なネットワーク・アクティビティを可視化したうえで、セキュリティ・ビッグデータを効率よく管理、分析し、十分な情報を基に素早く的確な判断を下すことができるのです。

製品の特徴

- カスタマイズ可能な可視性
- セキュリティ担当者やネットワーク・エンジニア、経営幹部向けの緻密でカスタマイズ可能なレポート
- タブレット対応Webポータルにより、「場所を選ばない監視」が実現
- 1日あたり数十億件のログを分析
- 膨大な量のログをわずか数秒で検索
- ワンクリックで詳細ビューに移動し、フォレンジック分析を実施
- 複数のログを相関分析して不審なアクティビティを検出
- わずか数秒で週次のアクティビティ・レポートを作成
- あらゆるセキュリティ脅威やネットワーク・コンポーネントの状態を単一のビューで把握*
- ファイアウォール、IPS、アンチウイルス、アンチボット、脅威エミュレーション、URLフィルタリング、アプリケーション制御が統合されたセキュリティ・ゲートウェイの監視を一元化

*2014年下半期で対応予定

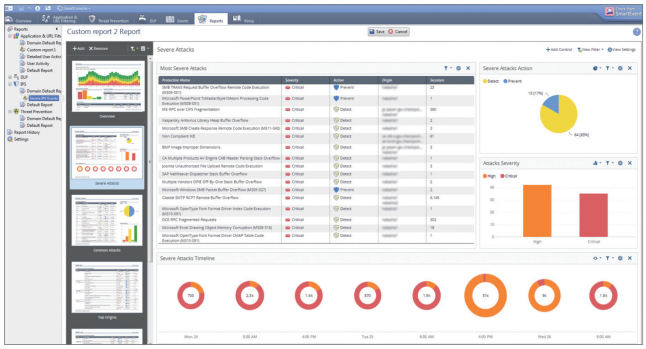
製品の利点

- カスタマイズ可能な可視性により、重要なセキュリティ・アクティビティを常に把握
- ビッグデータに潜む脅威を数秒以内に検出
- 「場所を選ばない監視」により、いつでもどこからでもNext Generation SmartEventにアクセスし、ネットワークを監視
- セキュリティの状況や傾向を容易に把握
- セキュリティ・インシデントを素早く調査
- カスタマイズしたレポートを素早く作成し、関係者に配布して、最新のセキュリティ状況を常に把握
- 複数のログを相関分析し、未整理のデータから不審なアクティビティを検出
- 小規模企業から大規模企業、データセンターまであらゆる規模の環境に対応

Check Point Next Generation SmartEventの特徴

カスタマイズ可能な可視性

いかなる組織においても、セキュリティの状況やイベント、ネットワークの利用状況に関するさまざまな情報入手は欠かせません。Next Generation SmartEventで作成したビューとレポートで、自社に関連する情報のみを反映、表示するよう最適化すれば、攻撃の重大度を始めとして、頻度の高い攻撃、攻撃の発信源や対象まで、各種情報についての理解向上につながります。また、ウィジェットの追加やグラフ形式のカスタマイズを行ってデータ表示をさらに最適化すれば、セキュリティ・データの確認も容易になります。

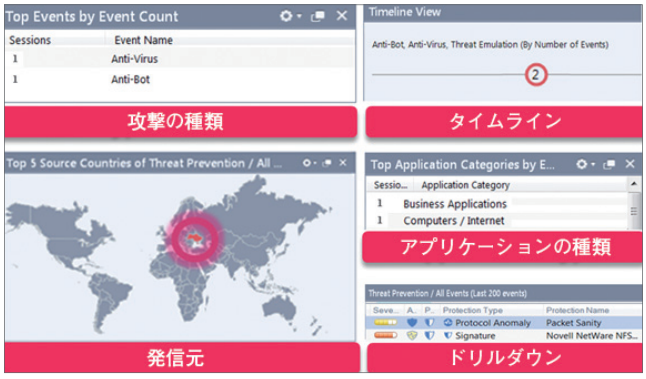


カスタマイズ可能なレポーティング

Next Generation SmartEventを使用すると、組織内の特定の関係者向けにカスタマイズかつ最適化されたレポートを柔軟に作成できるようになります。経営幹部は前月のハイリスクなイベントについての概要で済む場合も、部下がアクセスしているサイトまで把握したい部長クラスにとっては物足りません。関係者に関連する情報だけをまとめたレポートを容易に作成できるNext Generation SmartEventを利用すると、セキュリティ上の決断を下す際に必要となる情報を多くの判断材料に基づいて素早く確認できるようになります。

セキュリティ・インシデントを素早く調査

Next Generation SmartEventは、ワンクリックでセキュリティ・インシデントを調査できます。「概要ビュー」で1回クリックすれば、攻撃の種類やタイムライン、アプリケーションの種類、発信元など、フォレンジック分析に必要な情報をまとめた詳細ビューに移動できます。フォレンジック調査から潜在的な脅威の詳細な把握まで、迅速なインシデント調査が実現します。



Next Generation SmartEventでは、数十億件に及ぶログをわずか数秒で検索できる全文検索機能も使用できます。検索履歴やサジェスト、よく使う候補も表示され、検索作業が効率化します。

ログを相関分析して不審なアクティビティを検出

Next Generation SmartEventでは、すべてのアクティビティとイベントを監視して複数のログを相関分析し、不審なアクティビティを検出します。迅速なデータ分析に加え、カスタムのイベント・ログの作成も可能なため、複数の地域で同時に同じログイン情報が使用されている場合など、矛盾や不一致が確認されると直ちに管理者に通知されます。

前例のないスピードと拡張性

1日で膨大な量のログを処理するNext Generation SmartEventは、あらゆる規模の組織に前例のないパフォーマンスを提供します。小・中規模企業から大規模企業、データセンターまであらゆる組織が、ビッグデータに潜む脅威を秒単位で検出できるようになります。

週次のアクティビティ・レポート作成に必要な時間はわずか数秒です。1億件を超えるログを保存している大規模なデータベースの検索に至っては、1秒も待たずにフォレンジック分析や法令遵守に役立つ情報が抽出されます。Next Generation SmartEventは、複雑なセキュリティ環境にも対応する拡張性とスピードを実現しています。

「場所を選ばない監視」

Next Generation SmartEventでは、ネットワークの状態をどこからでも詳細に把握できます。専用のWebポータルが用意されており、時間や場所を問わず、モバイル・デバイスやタブレット端末からNext Generation SmartEventにアクセスできます。

Smart-1 Appliance[1]

Smart-1 Appliance	205	210	225	3050	3150
					
インストール済みSoftware Blade	SmartEvent[2]、SmartReporter[2]、Logging & Status				
管理可能なゲートウェイ数	5	10	25	50	150以上[3]
ストレージ(HDD)	1TB x 1	2TB x 1	2TB x 2	2TB x 4	2TB x 12(最大) 2TB x 6 (デフォルト)
ファイバ・チャネルSANカード	-	-	オプション[4]	オプション	オプション
LOM(Lights Out Management)	-	-	GbEポート x 1	GbEポート x 1	GbEポート x 1
イベント・ログ／秒	280	480	950[5]	3,000[6]	7,500[7]
ログ・サイズ(GB)／日	3.5	6.5	13	40	100
最大ユーザ数	900	1,600	3,000	10,000	25,000

[1] NG SmartEventバージョンは、専用のSmartEventアプライアンス上で利用可能。 [2] 他のSecurity Management Software Bladesに含まれるとき、1年用SmartEventのライセンスが利用可能。SmartEventライセンスは、専用のSmartEventアプライアンス上で4年間利用可能。 [3] 最大5,000の1100アプライアンスを管理可能。 [4] Smart-1 225はSANカードの装着の有無を発注時に選択可能。なおSANカードは、後日追加などSmart-1 225向けに個別発注は不可。 [5] 32GBのメモリ使用時。 [6] 128GBのメモリ使用時。 [7] 256GBのメモリ使用時。

Next Generation SmartEvent Software Bladeの仕様

機能	説明
可視化	
概要ビュー	Software Bladeのアクティビティの概要を把握できる、緻密でカスタマイズ可能なビュー
タイムライン・ビュー	リアルタイムのイベント情報および傾向をグラフィカルに表示
マップ・ビュー	イベントに関連するトラフィックの発信元／発信元IPを、地図上にピンポイントで表示
重要な統計情報	重要な防御機能やアプリケーション、ユーザなどの概要を表示
チャート・ビュー	イベントの統計を、棒グラフまたは円グラフで表示
イベントのクイック・ビュー	タイプ、関連トラフィックの発信元／送信先、ユーザ、国別にイベントを素早く分類
イベント解析	
事前定義のイベント相関分析ルール	チェック・ポイントのベスト・プラクティスに基づく、業界で一般的なセキュリティ問題に対応した事前定義のイベント相関分析ルール
セキュリティ・イベントのカスタマイズ	独自のイベント相関分析ルールを作成してあらゆるセキュリティ・イベントを監視
全文検索	サジェストや検索履歴、よく使う候補も確認できる使いやすい検索機能で、膨大なイベントを素早く検索
フォレンジック調査	タイムラインおよびマップの各ビューでイベントをダブルクリックし、パケット・レベルまで素早くドリルダウン
アイデンティティの記録	Active Directoryの情報に基づき、IPアドレスをユーザ名にマッピング
Client Infoアプリケーション	デバイスを右クリックして、各種情報(プロセス、ホットフィックス、脆弱性)にリモートからアクセス
脆弱性評価	セキュリティ・イベントの評価機能を内蔵

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

レポーティング	
事前定義済みレポート	一般的なセキュリティ・ニーズをカバーする、事前定義済みのグラフィカルなレポート・テンプレート
カスタマイズ可能なレポート	カテゴリ、フィルタ、グラフの形式を選択して、関連情報を最適にビジュアル表示
セキュリティ・イベントへの対応策	
イベント・チケット	チケット・ワークフローにより、管理者にイベントを割り当て
グローバルな例外とイベント固有の例外	製品、発信元、宛先、サービスごとにイベントの除外／例外をカスタマイズ
自動対応アクション	重要なイベント用の自動警告メカニズム
修復オプション	イベントの解析結果に基づき、セキュリティ・ポリシーを容易に変更
データ・ソース	
チェック・ポイント製品	事前定義されたルールに基づくイベントの相関分析が可能
サードパーティのセキュリティ製品	事前定義された複数のサードパーティ・ログ形式をサポート
グラフィカルなログ解析ツール	他のサードパーティのsyslogもサポート
Windowsのイベント	Windowsに関連するイベントを変換し総合的なイベントとして表示
その他	
拡張性に優れた分散アーキテクチャ	ログ・サーバ、イベント相関分析サーバ、イベント・サーバを別々のシステムに導入可能

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

P/N EDB2590 2014.06