Orchestrating a brighter world NEC

WebSAM Network Flow Analyzer 3.2
WebSAM NetvisorPro V 9.5
強化内容のご紹介

2023年10月

日本電気株式会社

強化内容

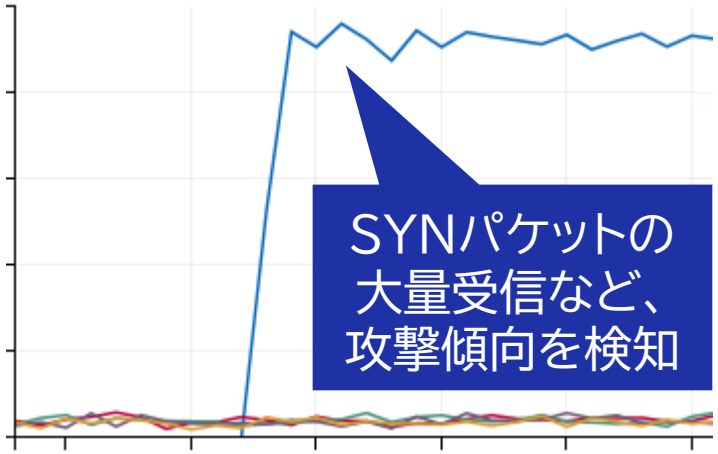
- 【新機能】セキュリティ分析・監視機能（NFA）
- ログイン状況の証跡ログ記録に対応（NFA）
- データ収集機能の強化（NVP）
- ヴィジェット表示対象の拡大（IMS）
- WebAPIの強化（IMS）
- 動作環境の拡大：RHEL9に対応（NVP/NFA/IMS）

フローデータを用いたセキュリティ分析

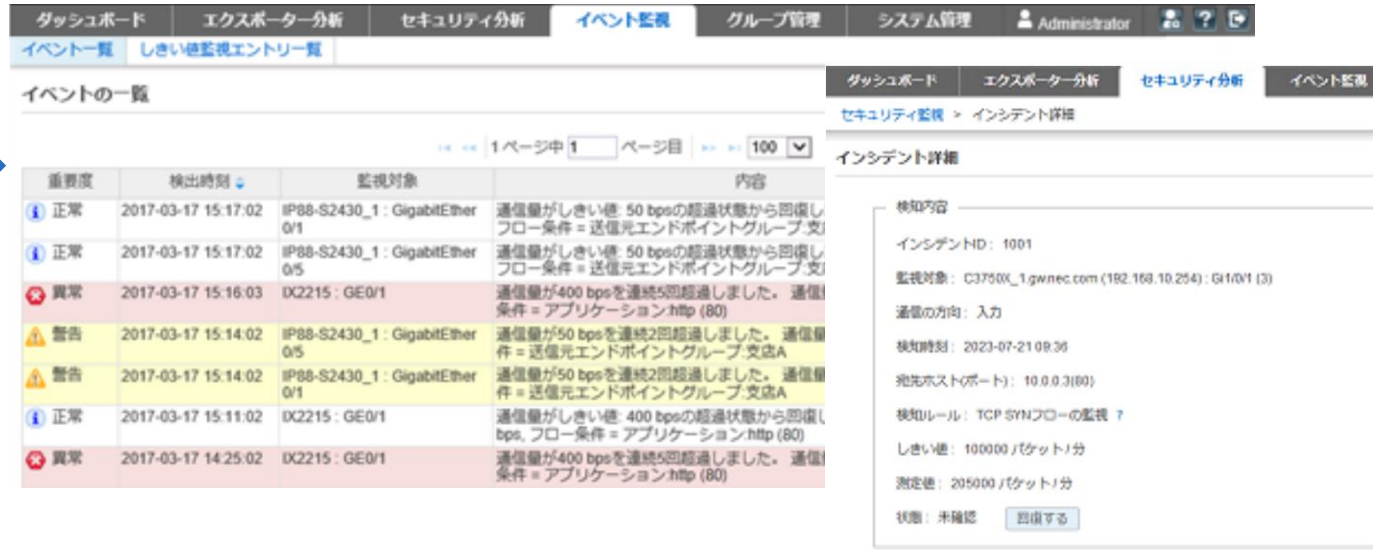
拡張機能ライセンス
Security Monitoring

フロー情報を分析し、トラフィックの振舞いからサイバー攻撃を検知
既存のエクスポーターを活用したセキュリティ監視を実現

- NFAが受信した集約前のフローデータを用いてセキュリティ観点での分析を実施
  - 監視対象のI/Fを通るフローのTCPフラグ値を分析し、DoS/DDoS攻撃およびスキャン攻撃の傾向を検知
- 既存のエクスポーターを活用することで、セキュリティ機器の導入に依らず様々な箇所でのセキュリティ監視が可能



イベント通知



ログイン状況の証跡ログ記録

NFAに対する各ユーザのログイン/ログアウト履歴を証跡ログとして記録
セキュリティインシデント発生時の追跡調査に対応

◆ セキュリティインシデント発生時に求められる監査機能を強化

■ セキュリティ監視機能の実装に伴い、製品自体のセキュリティ強化を実施

◆ ログイン/ログアウト履歴をテキストファイルに自動出力

出力例

2023-09-02 17:49:20.002 情報 成功 admin ログインしました。(ユーザー名=admin)

2023-09-02 17:50:15.021 情報 成功 admin ログアウトしました。(ユーザー名=admin)

2023-09-02 17:51:12.338 情報 失敗 admin ログインに失敗しました。(ユーザー名=admin)

データ収集機能の強化

NetvisorPro VにおけるMIB性能情報の表示対象を拡大すると共に、利便性の向上につながる強化を実施

- ユーザ独自のデータ種別を新たにサポート
  - MIB計算式のデータ種別をユーザ独自に定義することで集計・表示対象のデータ範囲を拡大可能
- しきい値監視機能の強化
  - 比較方法に以上(≧)、以下(≦)を追加　※従来は上回る(＞)、下回る(＜)のみ
  - しきい値と回復値に負の値を指定可能
  - しきい値超過アラートのアラート詳細に収集データの値を参照可能
- 負の取得値のサポート
  - 取得値やMIB計算式の計算結果が負の値でも性能データに出力可能
- MIB計算式の強化
  - Counter型・Counter64型のMIBを累積値でなく無加工の値として計算可能

ヴィジェット表示対象の拡大／WebAPIの強化

IMSのノード詳細画面およびネットワークインタフェース詳細画面における表示対象を拡大。合わせてWebAPIを強化しデータ取得対象を拡大

◆ NFAフロー情報の表示対象を追加

- ■ WebAPIでのデータ取得もサポート

追加項目
入力インターフェイスの使用量
出力インターフェイスの使用量
入力パケット損失数
出力パケット損失数
入力パケットエラー数
出力パケットエラー数

※従来は使用率/損失数/エラー率の表示のみ

◆ NVPが収集したMIB情報の表示対象を拡大

- ■ NVPで定義可能となった独自の「データ種別」に従い、より幅広い情報を表示可能
- ■ WebAPIでのデータ取得もサポート