RSA NETWITNESS® PLATFORM

リリース ノート

RSA NetWitness Platform 11.3

連絡先情報

RSA Link(https://community.rsa.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/emc-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、EMCが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事上の責任が課せられる可能性があります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Link の製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、これらの使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

EMC Corporationは、この資料に記載される情報が、発行日時点で正確であるとみなしています。この情報は予告なく変更されることがあります。

目次

はじめに

このドキュメントは、RSA NetWitness® Platform 11.3.0.0の機能拡張と修正について記述しています。RSA NetWitness® Platform 11.3.0.0を導入または更新する前にお読みください。

新機能

RSA NetWitness® Platform 11.3.0.0は、SOC(セキュリティ オペレーション センター) のすべての役割に新しい機能と機能拡張を提供します。次のような新機能が含まれます。

- ホストおよびファイルの分析機能の拡張により、悪意のあるアクティビティや不審なアクティビティの検出機能を強化。
- 操作性の向上により、インシデント対応者および脅威ハンターの作業を簡略化。
- ポリシーとライセンスの管理機能の向上により、管理者の管理作業を効率化。

NetWitness Endpoint

エンドポイント エージェント

11.3では、エージェントはWindowsログ収集に加え、EDR(エンドポイント検出および対応) 機能をサポートします。

詳細モード(要ライセンス) のエージェントは、EDR機能により、エンドポイント ホスト上のアクティビティを継続的に監視して詳細を可視化し、すべての動作およびプロセスを分析することができます。エージェントは、プロセス、ファイル、レジストリの変更、ネットワーク接続といった重要なアクションのデータをすべて記録し、イベントとしてほぼリアルタイムでサーバに送信します。エージェントは、イメージフック、カーネルフック、レジストリの不一致、不審なスレッドなどの異常を検出できます。さらに、Windowsログを収集します。詳細については、『*NetWitness Endpointユーザガイド*』を参照してください。

主要な機能は、次のとおりです。

- ユーザ コンソール上の操作の監視。この機能は、侵害されたホスト上で `cmd.exe`や `powershell.exe`などのWindows正規ファイルを使用してコマンドを実行するタイプのマルウェア攻撃の調査に不可欠です。
- 完全なコマンド ライン引数文字列の可視化。この情報は、フォレンジックおよび調査に重要です。

- ファイルまたはファイルレスのスクリプトの検出。スクリプトは、スクリプト エンジンではなく、直接プロセス イベントとしてレポートされます。現在サポートされるエンジンは、`powershell`、`cmd`、`cscript`、`wscript`、`rundll32`、`mshtml`、`javascript`です。
- エージェントの改ざん防止。ユーザ モードとカーネル モードの両方で、エージェントのレジストリキー、`exe`、および`sys`ファイルが保護されます。

エンドポイント エージェントは、ポリシーの構成に応じて、Insightsモードまたは詳細モードで動作させることができます。ポリシーの詳細については、『*NetWitness Endpoint構成ガイド*』を参照してください。

レガシーNetWitness Endpointエージェントと比較した11.3の主要な改善点

- カーネル内部構造からの分離
- ファイル ブロックのパフォーマンス向上。ブロックできるハッシュ数が大幅に増加しました。
- イベント収集上限の増加。イベントは、実行可能ファイル(ハッシュ) ではなく作成チェーン全体に関連付けられるようになりました。
- サードパーティ アプリケーションとの互換性と相互運用性の向上。

サポート対象のエージェント オペレーティング システム

次のオペレーティング システムがサポートされます。

- Windows 2019 Server
- Windows 10(32および64ビット) (バージョン1809まで)
- Red Hat Linux 7.x
- macOS 10.13 (High Sierra)
- macOS 10.14 (Mojave)

エージェントは、VMware環境のVDI(仮想デスクトップ インフラストラクチャ) にもインストールできます。詳細については、『*NetWitness Endpointエージェント インストール ガイド*』を参照してください。

導入環境の拡張と分散への対応

エージェントの数、場所、配布、エンドポイントから収集するデータに応じて、複数のEndpoint Log Hybridを追加して、導入環境を拡張することができます。Endpoint Brokerを導入することにより、導入環境のすべてのEndpoint Serverのデータを統合して表示することができます。詳細については、『*NetWitness Endpointユーザ ガイド*』と『*NetWitness Endpoint構成ガイド*』を参照してください。

グループとポリシー

エンドポイント エージェントの構成を効率的に管理および更新するために、管理者は、ポリシーを使用してエージェントをグループ化し、動作を管理できます。管理者は、デフォルトのポリシーまたはカスタマイズしたポリシーを使用できます。Windowsログの構成は、エージェント パッケージの生成時に指定するのではなく、Windowsログ ポリシーにより指定することができます。詳細については、『*NetWitness Endpoint構成ガイド*』を参照してください。

リスク スコアを使用したファイルとホストの分析

アナリストは、1から100の範囲のリスク スコアを使用して、ファイルまたはホストを調査できます。リスク要因(アラートとイベント)の詳細なコンテキストを参照しながら、不審なアクティビティや悪意のあるアクティビティを迅速に調査できます。詳細については、『*NetWitness Endpointユーザ ガイド*』を参照してください。

プロセスの可視化

プロセスを調査するアナリストのエクスペリエンスを向上させるため、次のような機能が直観的なユーザ インタフェースに追加されました。

- プロセスのイベント チェーン全体、プロセスの親子関係、関連するすべてのイベントを1つの時系列ビューで把握。
- ユーザ名、起動引数、レピュテーション、ファイル ステータス、署名者、署名、ファイル パスなどの重要なプロセス属性の分析。

詳細については、『*NetWitness Endpointユーザ ガイド*』を参照してください。

ファイルの分析と対応

アナリストは次の操作を実行できます。

- ファイル レピュテーション(既知の正常、無効、疑わしいなど)、Context Hub、リスク スコア、証明書ステータスなどを使用してファイルを分析する。
- GoogleまたはVirusTotalを使用して外部ルックアップを実行する。
- ファイルをダウンロードして、スクリプトの文字列検索やテキスト コンテンツを確認し、より詳細なファイル分析を行う。

調査後、アナリストは次の操作を実行できます。

- ファイルにステータスを割り当て、ブラックリストやホワイトリストなどに分類する。
- 悪意のあるファイルや感染したファイルをブロックし、脅威を改善する。

詳細については、『*NetWitness Endpointユーザ ガイド*』を参照してください。

既存のIIOCのアプリケーション ルール

NetWitness Endpoint 4.4.0.xの既存のIIOCは、NetWitness Platform 11.3 のデフォルトのアプリケーション ルールとして使用できます。詳細については、『*NetWitness Endpoint構成ガイド*』を参照してください。

ESAのエンドポイント リスク スコアリング ルールの追加

ESAのサンプル ルールに加えて、NetWitness Platformに、約400のルールを含むエンドポイント リスク スコアリング ルール バンドルが追加されました。これらのルールが生成したアラートは、定義されたリスク スコア閾値を超えた疑わしいファイルやホストのリスク スコアを計算するために使用されます。NetWitness Endpointを導入している場合は、ESAルールを追加するのと同じ方法でこのルール バンドルをESAルール導入環境に追加できます。ただし、ESAルール導入時に、エンドポイント データ ソース(Concentrator) を指定する必要があります。詳細については、『*ESA構成ガイド*』を参照してください。

エンドポイント イベントのための[調査]>[イベント分析]ビューの更新

- エンドポイント イベントの [テキスト分析] には、イベントを説明する分かりやすいテキストが表示されます。また、255文字より長い値のメタデータを表示することができます。
- 各セッションについて、イベントを[プロセス分析]で表示するか、[ホストの詳細]ビューに移動してイベントに関連づけられたホストの詳細情報を表示することができます。

NetWitness Respond

NetWitness Endpointのイベント リストの再設計

アナリストのエクスペリエンスを向上させ、エンドポイント イベントをNetWitness Respondに統合するため、イベント リストが再設計されました。新しいイベント リストでは、柔軟なレイアウトに、多様なデータがより分かりやすくレンダリングされます。NetWitness Endpoint用にカスタマイズされたイベント プレビューにはイベントの詳細がインライン表示され、アナリストは、この見やすくなったイベント プレビューを使用してイベントを迅速に把握し、トリアージすることができます。詳細については、『*NetWitness Respondユーザ ガイド*』を参照してください。

NetWitness Endpointのアラート リスト フィルタの改善

アラート リストのフィルタによりソースがエンドポイントのアラートをフィルタすると、NetWitness Endpoint 4.4.xとNetWitness Endpoint 11.xの両方のアラートが表示されます。

UEBAインシデント ルールの追加

新しいUser Entity Behavior Analytics(UEBA) デフォルト インシデント ルールが追加されました。このルールは、Classifier IDによってUEBAのアラートをグループ化し、インシデントを作成します。

NetWitness Endpointインシデント ルールの更新

NetWitness Endpointが導入されている場合、「High Risk Alerts: NetWitness Endpoint」デフォルト インシデント ルールは、NetWitness Endpointによって生成されたリスクスコアが「高」または「クリティカル」のアラートを収集します。収集されたアラートは、ホスト名によりグループ化され、インシデントが作成されます。詳細については、『*NetWitness Respond構成ガイド*』を参照してください。

エンドポイント リスク スコアリング インシデントの自動作成機能の追加

NetWitness Endpointが導入されている場合、エンドポイント リスク スコア閾値を構成すると、リスク スコア閾値を超えた不審なファイルやホストに対して、リスク スコアリング インシデントを自動的に作成できます。リスク スコア閾値の構成方法については、『*NetWitness Respond構成ガイド*』を参照してください。NetWitness Endpointの詳細については、『*NetWitness Endpoint構成ガイド*』を参照してください。

[対応]ビューから、[調査]の[ホスト]ビューおよび[ファイル]ビューへの移動

インシデントの詳細を調査するため、アナリストは [対応] ビューのコンテキスト ツールチップを使用して [調査] > [ホスト] ビューおよび[調査] > [ファイル]ビューにアクセスできます。

[対応]ビューでのファイル レピュテーション ステータスとファイル情報の表示

NetWitness PlatformにContext Hubが導入されている場合、アナリストは[対応]ビューと[調査]ビューで、ファイル ハッシュ エンティティの上にカーソルを合わせてコンテキスト ツールチップを開き、ファイルのレピュテーション ステータスを確認することができます。また、[コンテンツの表示]ボタンをクリックし、[コンテキスト ルックアップ] パネルを開いて、追加のファイル情報を表示することができます。

NetWitness UEBA

RSA NetWitness Endpointを使用した高度な分析

UEBAがNetWitness Endpointと統合され、NetWitness Platformの検出範囲が拡張されました。この統合の目的は、潜在的な攻撃者のアクティビティを特定することです。これを実現するため、次の2つのデータソースに注目します。

- プロセスの実行
- レジストリ変更

詳細については、『*NetWitness UEBAユーザ ガイド*』を参照してください。

[ユーザ プロファイル]ビューから[ホストの詳細]ビューまたは[プロセスの分析]ビューへのアクセス

アナリストは、[ユーザ プロファイル]ビューから[ホストの詳細]ビューまたは[プロセスの分析]ビューに移行して、ユーザ リスクに関連する異常なプロセスやホストの詳細情報を検索できます。詳細については、『*NetWitness UEBAユーザ ガイド*』を参照してください。

サポート対象のデータ ソースの追加

NetWitness UEBAは、RSA SecurIDデータ ソースをサポートするようになりました。

NetWitness Investigate

[イベント分析]ビューのイベント リストに表示できるイベント数を拡大

最大5万件のイベントを収集時間の昇順でイベント リストにロードできます。リスト内の移動を容易にするため、100行ごとに行番号インジケータが表示されます。ユーザ インタフェースの機能を使用して、表示されている内容とソート順を理解することができます。詳細については、『*NetWitness Investigateユーザ ガイド*』の「[イベント分析]ビューでのイベントの分析」を参照してください。

[イベント分析]ビューでのクエリの詳細ステータスの確認

[イベント分析]ビューのクエリビルダの情報アイコン ( ) をクリックすると、クエリコンソールが開きます。クエリコンソールは、実行中のクエリの進捗、警告、エラー、およびその他の詳細な情報を表示するユーザ インタフェースの新しい機能です。クエリが完了すると、クエリコンソールには、時間範囲、クエリ、クエリ対象のサービス、クエリを実行できなかったサービス、各サービスで検索とイベントの取得に要した時間が表示されます。クエリ全体をテキストとしてコピーすることができます。詳細については、『*NetWitness Investigateユーザ ガイド*』の「[イベント分析]ビューでのデータのフィルタ」を参照してください。

[ナビゲート]ビュー、[イベント]ビュー、[イベント分析]ビューでのアナリスト ワークフローの改善

アナリストが調査を支援するため、次の点が改善されました。

- [イベント]ビューでページを切り替えるとき、クエリ結果をキャッシュすることにより、ログ イベントをより高速にロードできるようになりました。
- [イベント]ビューに移動するときに、[ナビゲート]ビューで使用していた時間範囲が使用されます。
- [ナビゲート]ビューでは、メタ キーの名前の横に、簡単に理解できるメタ キーの説明が表示されます。詳細については、『*NetWitness Investigateユーザ ガイド*』の「[ナビゲート]ビュー」を参照してください。
- [イベント分析]ビューでカスタムの時間範囲を指定できるようになりました。事前定義の時間範囲に加えて、カスタムの時間範囲を入力できます。時間範囲に表示された年、月、日、時、分の値をクリックし直接編集できます。詳細については、『*NetWitness Investigateユーザ ガイド*』の「[イベント分析]ビューでのデータのフィルタ」を参照してください。

[イベント]ビューにロードされたイベントの詳細情報をフッターに表示

フッターのメッセージは、アナリストが[イベント]ビューに表示されている内容を理解するのに役立ちます。イベントがロードされていない場合は、「0件の一致イベント」と表示されます。その他に、管理者が設定したスキャン制限または結果制限に達していないかや、どのサービスの結果を表示しているかを確認できます。たとえば、「1～25件の一致イベントを表示(全100000件中。スキャン結果制限数に到達) 」というメッセージが表示される場合、スキャン制限に達したこと、スキャンしていないデータがまだ残っていることがわかります。詳細については、『*NetWitness Investigateユーザ ガイド*』の「[イベント]ビュー」を参照してください。

[ナビゲート]ビューおよび[イベント]ビューでの検索とクエリを高速化

アナリストが[ナビゲート]ビューでBrokerまたはConcentratorに対してクエリを実行する場合、サービスに新しく組み込まれたキャッシュの使用により、以前のクエリ条件のすべて、または一部を共有する後続のクエリの結果をより高速に取得できます。[イベント]ビューでは、テキスト値を指定する複雑な演算子を使用したクエリがキャッシュされるため、以前のクエリ条件のすべて、または一部を共有する後続のクエリの結果をより高速に取得できます。

[イベント分析]ビューのクエリビルダの新機能

- ガイド モードのクエリビルダでは、[詳細オプション]サブメニューの[フリーフォーム フィルタ]を選択することにより、複雑なフィルタを作成できます。このオプションは、ガイド モードのドロップダウン メニューから選択できます。長く複雑なクエリをペーストしたい場合は、従来のフリーフォーム モードを使用できます。
- フリーフォーム フィルタを含むクエリを実行すると、クエリを実行する前にフリーフォーム フィルタがサーバ側で検証されます。無効なフィルタが含まれる場合、クエリは実行されません。
- クエリの実行中に、進行中のクエリをキャンセルすることができます。クエリがキャンセルされると、[イベント]パネルのイベント数、フッター メッセージ、クエリ コンソールには、検出したイベントの合計数ではなく、キャンセル前にロードできたイベント数が表示されます。

詳細については、『*NetWitness Investigateユーザ ガイド*』の「[イベント分析]ビューでのイベントのフィルタ」を参照してください。

Endpoint Analysis列グループのメタ キーの更新

Endpoint Analysis列グループが更新され、エンドポイント調査のための新しいメタ キーが追加されました。これらのメタ キーは、[イベント]ビューと[イベント分析]ビューでエンドポイント イベントを表示するときに表示されます。

階層リンクの時間範囲の自動更新を制御するための新しい環境設定オプション

[イベント分析]ビューでは、[イベント環境設定]ダイアログの新しい設定項目により、階層リンクの時間範囲の自動更新を制御できます。特定の時間範囲の結果を表示している間であっても、新しい結果を検出するため1分間隔でサービスのポーリングが行われます。しかし、新しい結果を検出しても、現在の時間範囲のビューに新しい結果がロードされることはありません。デフォルトでは、階層リンクの時間範囲は、現在表示中の検索結果と同期したまま変更されません。[**時間範囲を自動的に更新**]チェックボックスをオンにすると、サービスに新しい結果が存在する場合、階層リンクの時間範囲が自動的に更新されます。時間範囲が更新されると、[クエリの送信]ボタンがアクティブになり、クリックして最新の結果を取得できます。

[調査]>[ホストの詳細]ビューからUEBAへアクセス

NetWitness UEBAがインストールされている場合、[ユーザ]ビューに移行して、ホストにログインしたユーザに関連するリスクを分析できます。詳細については、『*NetWitness UEBAユーザ ガイド*』を参照してください。

ESA(Event Stream Analysis)

ESA相関ルールを処理する新しいESA Correlationサービス

NetWitness Platform 11.3のESA Correlationサービスは、以前のバージョンのEvent Stream Analysisサービスに代わるものです。ESA Correlationサービスは、Event Stream Analysisサービスと同様に、ESAプライマリまたはESAセカンダリのホスト タイプにインストールされます。

ESAホストで実行できるESAサービスは次の2つです。

- ESA Correlation (ESA相関ルール)
- Event Stream Analytics Server(ESA Analytics)

[対応]ビューと[調査]ビューでエンリッチメント データの検索機能を提供するContexthub Serverサービスは、ESAプライマリ ホストでのみ実行されます。

ESA相関ルールごとに異なるデータ ソースの指定をサポート

データ ソース(Concentratorなど) をサービスごとに指定する代わりに、ESAルールの導入環境ごとに異なるデータ ソースを指定できるようになりました。たとえば、ある導入環境ではHTTPパケット データを含むConcentratorを使用し、別の導入環境ではHTTPログ データを含む別のConcentratorを使用することができます。詳細については、『*ESA相関ルール アラート ユーザ ガイド*』を参照してください。

ESAルールの導入環境のアップグレードに関する考慮事項については、該当するアップグレード ガイド、更新ガイド、および『*ESA構成ガイド*』を参照してください。

ESAでのConcentratorの圧縮レベルの調整をサポート

ESAルールの導入環境を作成し、データ ソースとして使用するConcentratorを構成するときに、ESAでのConcentratorのデータ圧縮レベルを設定することができます。詳細については、『*ESA相関ルール アラート ユーザ ガイド*』を参照してください。

ESAルールごとに[対応]ビューへのアラートの転送を有効化または無効化

個々のESAルールで、アラートのオンとオフを切り替えることができます。詳細については、『*ESA構成ガイド*』を参照してください。

ESPERバージョン5.3から7.1へのアップグレード

ESPERのバージョンが最新の7.1にアップグレードされました。

Log Collector

Log CollectorとVirtual Log Collectorのリストをソート

Log Collectorサービスでは、ローカルCollectorおよびリモートCollectorのドロップダウン メニューがアルファベット順にソートされるようになったため、表示するコレクタを見つけやすくなりました。

- ローカルCollectorの[リモートCollector]タブでは、[ソースの追加]ダイアログ ボックスに表示される[リモートCollector]フィールドがソートされます。
- Virtual Log Collectorの[ローカルCollector]タブでは、[宛先]および[ソース]フィールドがソートされます。

Log CollectorとLog Decoderのリストをソート

[管理]>[ヘルスモニター]>[イベント ソース モニタリング]ビューでは、[Log Collector]と[Log Decoder]ドロップダウン メニューがアルファベット順にソートようになったため、表示するアイテムを見つけやすくなりました。

ローカルLog CollectorのSyslogポート

11.3では、ローカルLog Collector(Log Decoderホスト上のLog Collector) は514および6514以外のポートでSyslogメッセージを受信することができます。これにより、EUC-KRやISO8897-9などの異なるエンコードのSyslogメッセージを受信することができます。Log Decoderサービスは引き続き、ポート514および6514でASCII/UTF-8のSyslogメッセージを受信します。

非標準Syslogメッセージのパススルーロジックを改善

リモートLog Collectorは、メッセージのヘッダーまたは本文が空の場合を除き、すべての非標準のSyslogメッセージを受け入れるようになりました。不要なメッセージは、Syslog収集のイベント フィルタで除外する必要があります。詳細については、『*ログ収集ガイド*』の「Collectorのイベント フィルタの構成」セクションを参照してください。Syslogフォーマットの詳細については、SyslogのRFC 3164およびRFC 5424 (https://www.ietf.org/standards/rfcs/) を参照してください。

コア サービス

SnortパーサでのUDMサポート

Snortパーサが更新され、新しいオプション(`udm=true`) が追加されました。このオプションにより、UDM(統合データモデル) キー セットが使用されます。詳細については、『*DecoderおよびLog Decoder構成ガイド*』の「Snortパーサ」を参照してください。

セキュアSMTPの復号

NetWitness Platformでは、RFC 3207(https://tools.ietf.org/html/rfc3207) に準拠した、Opportunistic SSL/TLS復号をサポートしています。HTTPSパーサのオプションに、STARTTLSコマンドを検索するセッションの宛先ポートのリストをコンマ区切り値(.csv) 形式で指定できます。また、少なくとも1つの暗号キーをアップロードします。これにより、STARTTLS機能が有効になります。詳細については、『*DecoderおよびLog Decoder構成ガイド*』の、「セキュアSMTPの復号」参照してください。

GeoIPパーサのサポート終了と、GeoIP2パーサへの置換

従来のGeoIPパーサはサポートされなくなりました。11.2で導入された新しいGeoIP2パーサに完全に置換されます。GeoIP2パーサは、GeoIPパーサのすべての機能に加えて、IPv4およびIPv6の変換を含む新しいMaxmindパッケージをサポートしています。

SDKのmax.query.memoryパラメータによるクエリのメモリ使用量の制限

従来は、max.where.clause.sessionsパラメータを使用して、単一のクエリでスキャンできるセッション数を制限していました。たとえば、ユーザのクエリがデータベースからすべてのメタを取得する場合、読み込んだセッション数がこの構成値に達すると、データベースは処理を停止していました。このパラメータは、今後のリリースでは廃止されます。今後は、max.query.memoryパラメータにより、クエリ全体のメモリ使用量を制限します。

外部ストレージでのPowerVault SEDの使用

検索用のログ データとパケット データを格納する外部ストレージとして、PowerVault SED(自己暗号化ドライブ)を使用できるようになしました。

Nグラム インデックスのパフォーマンス向上(11.2比較)によるフルテキスト検索の高速化

フルテキスト検索で使用するNグラム インデックスの挿入レートが改善されました。Nグラム インデックスの更新は、約2倍高速になりました。つまり、集計のパフォーマンスに大きな影響を与えることなく、より多くのConcentratorでNグラム インデックスを活用できます。この機能はデフォルトで無効になっています。Nグラム インデックスの詳細については、『*NetWitness Platformコア データベース チューニング ガイド*』の「インデックスのカスタマイズ」を参照してください。

データベース クエリ構文に新しいavglen関数を追加

クエリ構文にavglen関数が追加されました。この関数は、指定されたメタ値の平均の長さを返します。

管理

ハイブリッド コンポーネントをコア アプライアンス上に構成可能(これにより、ハイブリッド コンポーネントが複数のPowerVaultsを使用可能に)

Log HybridやNetwork (Packet) Hybridなどのハイブリッド カテゴリのサービスを、シリーズ6(R640)物理ホストにインストールできます。これにより、複数のPowerVault外部ストレージ デバイスをシリーズ6(R640)物理ホストに接続することができます。

PKI(公開鍵基盤)認証

PKI認証を使用すると、ユーザはデジタル証明書を使用して認証を行い、NetWitness PlatformのUIにアクセスすることができます。詳細については、『*システム セキュリティとユーザ管理ガイド*』を参照してください。

DISA STIGのサポート

バージョン11.3は、DISA STIG(Defense Information Systems Agency Security Technical Implementation Guide)コントロール グループのすべての監査ルールをサポートしています。11.3でサポートされているSTIGの詳細については、『*システム メンテナンス ガイド*』を参照してください。

証明書の再発行コマンド

`cert-reissue`コマンドが追加され、ホストの証明書を再発行できるようになりました。すべてのホストを11.3に更新した後、証明書が期限切れにならないように、すべてのホストの証明書をできるだけ早く再発行してください。証明書の有効期限が切れると、NetWitness導入環境が回復不可能な状態になります。11.3で証明書を再発行する方法の詳細については、『*システム構成ガイド*』を参照してください。

ウォーム、スタンバイNW Serverホスト(フェイルオーバー/高可用性のため) : 物理ホストのみ

ウォーム スタンバイNW Serverは、アクティブなNW Serverホストの重要なコンポーネントと構成を複製して、信頼性を高めます。ウォーム スタンバイNW Serverはスタンバイ モードのまま、アクティブなNW Serverから定期的にバックアップを受信します。アクティブなNW Serverに障害が発生した場合(オフラインになった場合)、フェイルオーバー手順を実行し、スタンバイNW Serverをアクティブにすることができます。11.3でウォーム スタンバイNW Serverをセットアップおよび管理する方法の詳細については、『NetWitness Platform*導入ガイド*』を参照してください。

ホストとサービスの構成データを統合するための新しいツール

NW-Consolidatorツールは、構成とデータをNetWitness Platform 10.6.6から11.3に移行する一部のお客様のみが利用できます。このツールは、導入環境に複数のSecurity AnalyticsとReporting Engineのインスタンスがあり、ホストとサービスの構成とデータを1つのインスタンスに統合する場合に使用します。ユーザ、グループ、ロール、フィード、レポートに関連するデータも統合できます。

ライセンス

Endpoint ServerおよびESA Correlation Serverライセンスのサポートと、すべての従量制ライセンスの統合

ライセンス ユーザ インタフェースの拡張により、管理者はライセンス情報を簡単に確認できるようになりました。[ライセンスの詳細] ページには、異なる従量制ライセンスの使用量が集約して表示され、使用量のトレンドも表示されます。管理者は、Endpoint ServerおよびESA Correlation Sserverを含む、導入環境内のすべてのライセンスを表示することができます。さらに、複数のNetWitness Server(ホット サーバおよびウォーム サーバ)のライセンスを構成できます。詳細については、『*ライセンス管理ガイド*』を参照してください。

脅威に基づく認証

RSA SecureID AccessとNetWitness Platformの統合

RSA SecureID AccessとNetWitness Platformを統合すると、NetWitness Platformで特定した不審なユーザに対して、RSA SecurID Access側でそれらのユーザのアクセス レベルを引き下げたり、ブロックすることができます。RSA SecurID Accessは、これらの制御を保証レベルやポリシーの定義により実現します。NetWitness Respond Serverが、インシデントから得た不審なユーザのメールIDをRSA SecureID Accessに送信します。Respond Serverの構成方法については、『*Respond構成ガイド*』を参照してください。

修正された問題

本セクションでは、前回のメジャー リリース以降に修正された問題について説明します。

セキュリティ

トラッキング番号	説明
ASOC-59254	カーネルのセキュリティ更新： https://access.redhat.com/errata/RHSA-2018:1965.
ASOC-58383	policycoreutilsのセキュリティ更新： https://access.redhat.com/errata/RHSA-2018:0913.
ASOC-58382	opensslのセキュリティ更新： https://access.redhat.com/errata/RHSA-2018:0998.

調査

トラッキング番号	説明
ASOC-61230	[ナビゲート]ビューまたは[イベント]ビューで[プロファイルの管理]ダイアログを使用して、プロファイルをインポートすると、新しくインポートされたプロファイルは[プロファイル]ドロップダウン メニューに追加されません。
ASOC-60941	[イベント]ビューでイベントを時間でソートすると、ネットワーク イベントとログ イベントを区別することなくすべてのイベントが時間順に表示されますが、[イベント分析]ビューでは、ソート方法が異なります。[イベント分析]ビューでは、ログ イベントとネットワーク イベントが混在することなく、代わりに、すべてのログ イベントを時間順にソートし、その後にすべてのネットワーク イベントを時間順にソートしたものが表示されます。
ASOC-50196	ドリルダウン ポイントのURLが非常に長い場合、[イベント分析]ビューでクエリを実行すると、エラー(414リクエスト エラー) が返される。
ASOC-49427	[イベント分析]ビューのクエリビルダは、フィルタにスペースが含まれていると応答しない。

対応

トラッキング番号	説明
ASOC-59243	特定のアラート ルールのすべてのアラートを削除した後、フィルタからそのアラート ルールが適切に削除されない。
ASOC-37533	カスタム インメモリ テーブルを作成し、ESAのエンリッチメント ソースとして追加した場合、その情報がESAアラートに表示されない。

ESA(Event Stream Analysis)

トラッキング番号	説明
ASOC-60511	アップグレードまたはESAホストのリブートにより、ESA CHルールが無効になる。
ASOC-60367	カスタム メタ キーを使用するESAルールがESA Serverに導入されない。
ASOC-26481	ESAの圧縮レベルを、他のアプライアンスと同様に設定することができない。
ASOC-14157	ESAに配列演算子の警告が表示される。

コア サービス

トラッキング番号	説明
ASOC-41902	Broker、Concentrator、Archiverの[SSL FIPS Mode]チェックボックスを無効化する必要がある。

アップグレード

トラッキング番号	説明
ASOC-49843	11.xへのアップグレード時に、Logstash出力構成ファイル内の監査ログ テンプレートが更新されない。
ASOC-42136	アップグレード後、静的チャートで調査リンクが無効になっている。

アップグレードに関する注意

RSA NetWitness® Platform 11.3.0.0では、以下のアップグレード パスがサポートされます。

- RSA NetWitness® Platform 10.6.6.xから11.3.0.0
- RSA NetWitness® Platform 11.0.x、11.1.x、11.2.xから11.3.0.0

11.3.0.0のインストールとアップグレードの詳細については、https://community.rsa.com/community/products/netwitness/113にアクセスし、「INSTALLATION & UPGRADE GUIDES」セクションの各ガイドを参照してください。

製品ドキュメント

本リリースでは、以下のドキュメントが提供されています。

ドキュメント	URL
RSA NetWitness Platform 11.3 オンライン ドキュメント	https://community.rsa.com/community/products/netwitness/documentation
RSA NetWitness Platform 11.3へのアップグレード手順とチェックリスト	https://community.rsa.com/community/products/netwitness/documentation
RSA NetWitness Platform ハードウェア セットアップ ガイド	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA NetWitness PlatformのRSAコンテンツ	https://community.rsa.com/community/products/netwitness/rsa-content

既知の問題

このリリースの未解決の問題については、https://community.rsa.com/community/products/netwitness/documentation/known-issuesを参照してください。回避策がある場合は、回避策の詳細または参照先が記載されています。

製品ドキュメントに関するフィードバック

RSA NetWitness Platformのドキュメントに関するフィードバックは、sahelpfeedback@rsa.comまでメールで送信してください。

サポートされない機能

次の表に、RSA NetWitness® Platform 11.1以降のリリースでサポートされなくなった機能に関する情報を示します。

11.1.0.0 以降のリリースでサポートされなくなった機能

番号	機能	注
1	Malware Colo	11.1.0.0以降のリリースでは、共存型のMalware Analysisはサポートされません。スタンドアロンのMalware Analysisを使用してください。
2	AIO(オール イン ワン)の導入	オール イン ワンの導入はサポートされません。新規インストールからAIOは削除されました。
3	スタンドアロンWarehouse Connector	スタンドアロンWarehouse Connectorはサポートされません。
4	管理機能	1. パスワードを忘れた場合のリンク。 2. パスワードの有効期限が切れたときのユーザへのメール通知。 3. ADユーザのテスト/検索。
5.	Pivotal	Pivotalはサポートされません。
6.	Warehouse Analytics	Warehouse Analyticsはサポートされません。

番号	機能	注
7.	11.2以前のEvent Stream Analysisサービスの一部の機能	11.3のESA Correlationサービスは、11.2以前のEvent Stream Analysisサービスの次の機能をサポートしていません。 1. 評価版ルールのメモリスナップショット 2. ESAのSNMP通知 3. データベース エンリッチメント ソース(Context Hubリストにより置換) 4. Warehouse Analyticsエンリッチメント ソース(Context Hubリストにより置換) 5. データベース接続エンリッチメント ソース(Context Hubリストにより置換) 6. 収集の時間指定 7. メモリプール
8.	Endpoint Hybrid	Endpoint Hybridホスト タイプは、11.3.0.0以降のリリースではサポートされません。

カスタマー サポートへのお問い合わせ

カスタマー サポートにお問い合わせいただく場合は、以下の情報を提供してください。

- お使いのRSA NetWitness Platform製品またはアプリケーションのバージョン番号
- お使いのハードウェアのタイプ

ご質問および技術的支援が必要な場合は、RSAカスタマー サポート(support@rsa.com) にメールでご連絡ください。

改訂履歴

リビジョン	日付	説明
1.0	2019年3月13日	Release to Operations