RSA NETWITNESS® PLATFORM

リリース ノート

RSA NetWitness® Platform 11.5

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 Conferenceのロゴ、RSA、その他の商標は、RSA Security LLCまたはその関連会社(「RSA」) の商標です。RSAの商標のリストについては、https://www.rsa.com/ja-jp/company/rsa-trademarksを参照してください。その他の商標は、各社の商標または登録商標です。

使用許諾契約

本ソフトウェアと関連ドキュメントは、RSA Security LLCまたはその関連会社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

本製品には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

本文書に記載される、RSA Security LLCまたはその関連会社(「RSA」) のいかなるソフトウェアの使用、複製、配布にも、適切なソフトウェア ライセンスが必要です。

RSAは、本文書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。

本文書に記載される情報は、「現状有姿」の条件で提供されています。RSAでは、本文書に記載される情報に関するいかなる内容についても表明保証条項を設けず、特に、商品性や特定の目的に対する適応性に対する黙示的保証は提供しません。

12月 2020

目次

新機能

RSA NetWitness® Platform 11.5は、セキュリティ オペレーション センター(SOC) のすべてのロールに新機能と機能拡張を提供します。

アップグレード パス

NetWitness Platform 11.5.0.0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 11.3.x.xから11.5.0.0*
- RSA NetWitness® Platform 11.4.x.xから11.5.0.0

* 11.2.x.x、11.3.0.0、または11.3.0.1からアップグレードする場合は、11.3.1.1にアップグレードしてから、11.5にアップグレードする必要があります。

11.5.0.0へのアップグレードの詳細は、『RSA NetWitness Platform 11.5アップグレード ガイド』を参照してください。

機能拡張

次のセクションでは、機能分野ごとに拡張内容を詳細に説明します。

- 調査 - SIEMとネットワークトラフィックの分析
- User Entity Behavior Analytics
- インシデント対応
- ヘルス モニタ
- エンドポイントの調査
- エンドポイントの構成
- Broker、Concentrator、Decoder、Log Decoderサービス
- Event Stream Analysis(ESA)
- 管理と構成
- Context Hub
- ログ収集
- ライセンス

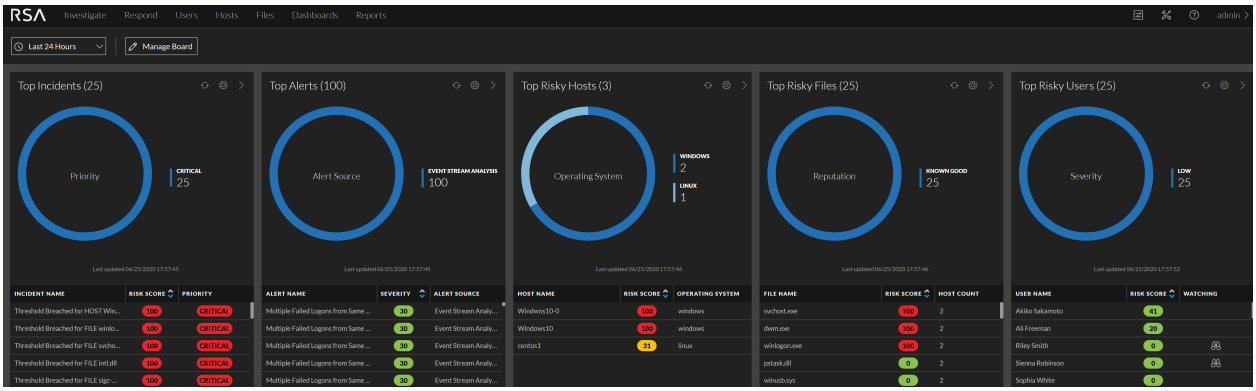
このセクションで言及されているドキュメントを見つけるには、RSA NetWitness Platform 11.x Master Table of Contents(https://community.rsa.com/docs/DOC-81328) にアクセスしてください。製品ドキュメントには、このリリースのドキュメントへのリンクが記載されています。

調査 - SIEMとネットワークトラフィックの分析

スプリングボード：検出とシグナルの統合ビュー

RSA NetWitness Platformに新しく追加されたスプリングボードは、プラットフォーム全体の検出結果とシグナルを単一のビューに表示する、使いやすいホーム ページです。アナリストはスプリングボード上の各パネルで、優先順位付けされたアラート、インシデント、高リスク ホスト、高リスク ユーザ、高リスク ファイル、焦点を絞ったイベント データを確認し、これまでになく迅速にハンティングと調査を行うことができます。

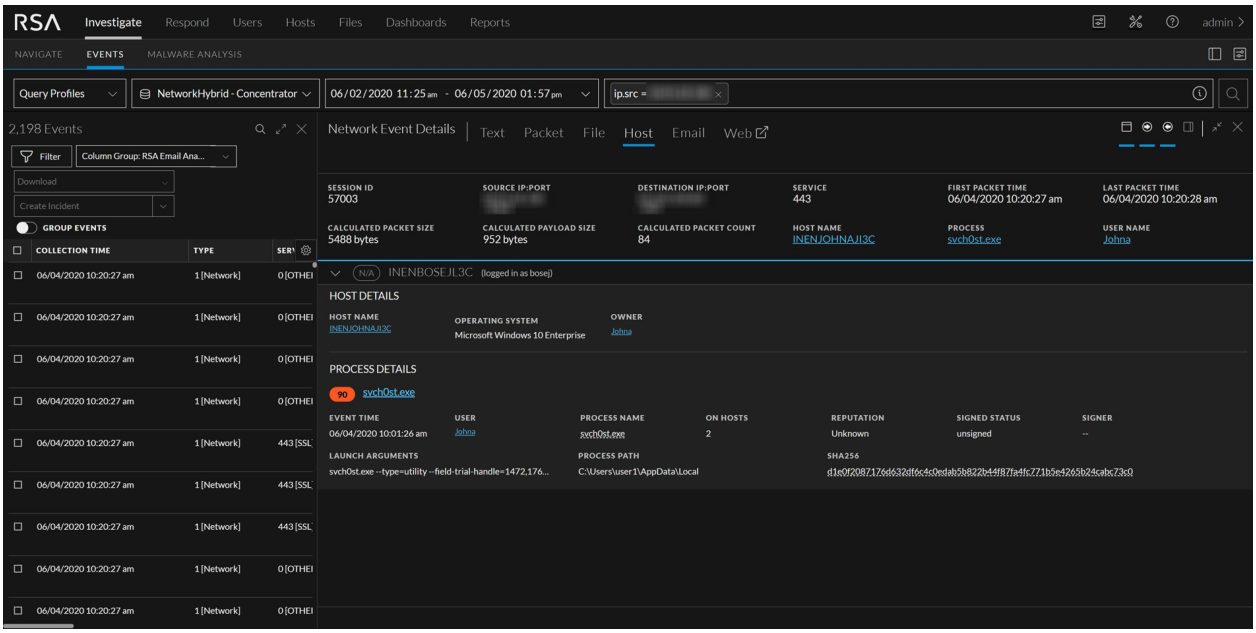
スプリングボードは管理者がカスタマイズでき、標準提供のパネルを編集したり、新しいパネルを作成して、事前定義されたクエリ条件によって焦点を絞ったイベント メタデータを表示することが可能です。詳細については、『NetWitness Platformスタート ガイド』の「スプリングボードの管理」を参照してください。



拡張ネットワーク可視化とエンドポイント データ エンリッチメント

拡張ネットワーク可視化により、ネットワーク(パケット) 導入環境のネットワーク イベントに、Endpointエージェントから収集したホストおよびプロセスのデータをエンリッチメントとして付加することができます。アナリストは、検出機能の拡張と豊富な情報に基づくネットワーク分析により、脅威の状況をより的確に把握できるようになります。エンドポイントからのホスト、ユーザ、およびプロセス情報は、ネットワークから収集された相関するネットワーク(パケット) イベントに付加されます。アナリストは、この相関ビューから、ユーザ、レピュテーション、リスク スコアなどの関連するエンドポイント情報へとドリルダウンすることもできます。詳細については、『*NetWitness Investigateユーザ ガイド*』で「 [イベント]ビューでのイベントの分析」を参照してください。

拡張ネットワーク可視化は、ポリシーで設定します。ポリシーの設定で、InsightsエージェントとAdvancedエージェントによるネットワーク イベントの追跡および監視を有効化し、ネットワーク(パケット) 相関のためにエンドポイント ネットワーク イベントを送信する頻度を最適化します。ポリシーで拡張ネットワーク可視化を有効にする方法の詳細については、「グループとポリシーの作成」を参照してください。

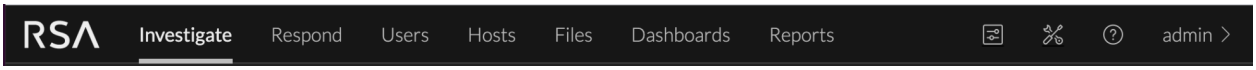


アナリストによる脅威の迅速な検出と対応を支援するナビゲーションの改善

アナリストがNetWitness Platformにログインすると、この製品の価値を引き出す最も一般的な方法がすぐにわかるようになっています。

- 最上位レベルのナビゲーションは、アナリストが脅威の検出と対応に使用する主要機能へのアクセスを提供します。以前は、アナリストは [ホスト]、 [ファイル]、[ユーザ]の各ビューにアクセスするために、 [調査]に移動する必要がありました。
- 管理タスクは右上隅にアイコンとして統合され、管理、構成、通知、ジョブ、ユーザ環境設定が一か所にまとめられました。

次の図は、通知とジョブを含む各ビューにアクセスできる最上位レベルのナビゲーションを示しています。詳細については、「NetWitness Platformの基本ナビゲーション」を参照してください。

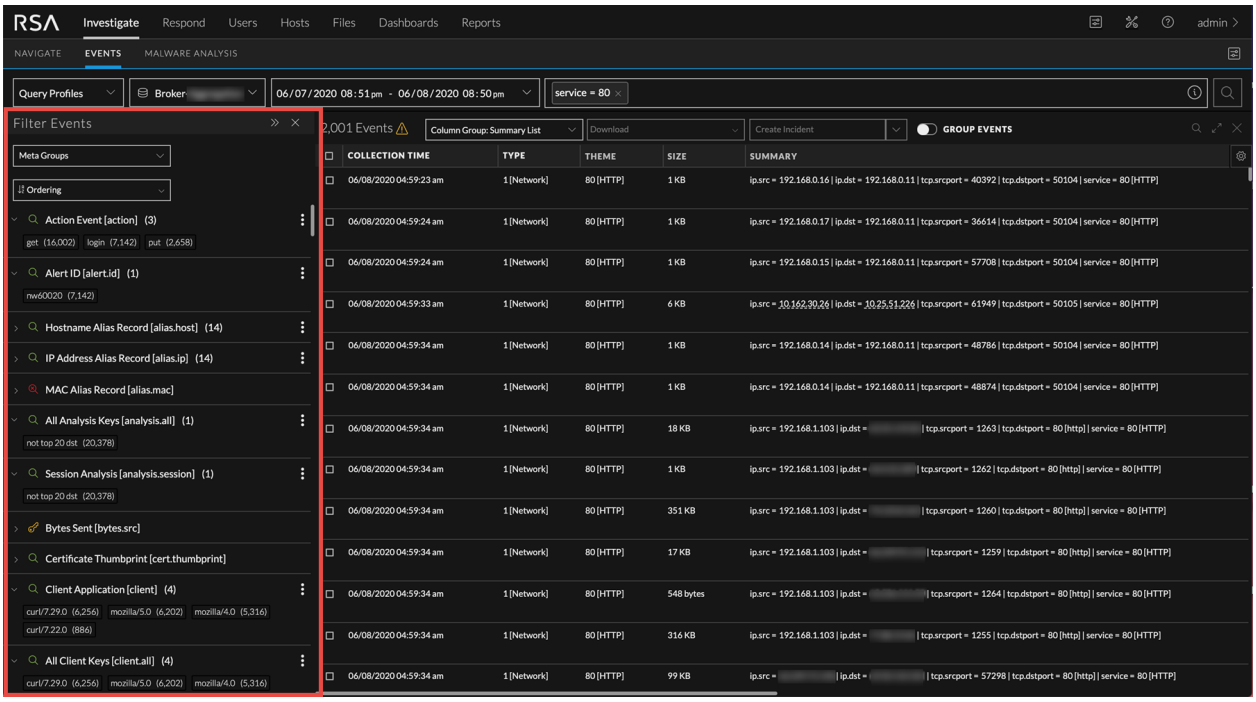


関連するメタデータを軸に [イベント]ビューのイベントを絞りこむ強力な新機能(ベータ)

[イベント]ビューに追加された [イベントの絞り込み]パネルでは、アナリストはメタデータを軸にして、イベントのサブセットを絞り込むことができます。このパネルは、イベントのリストをシーケンシャルに表示する [イベント]パネルの隣に表示されます。 [イベントの絞り込み]パネルでは、次の操作を行うことができます。

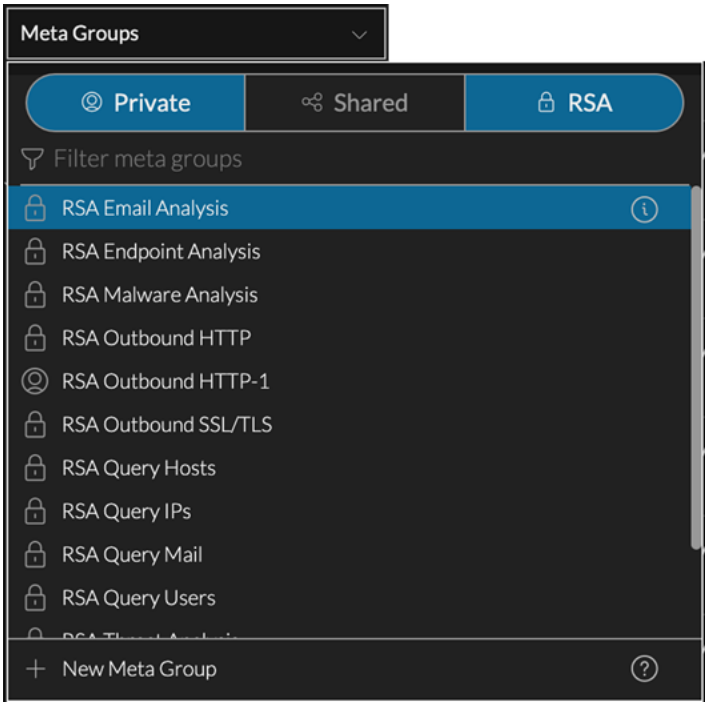
- メタ値をクリックして、結果のイベントを [イベント]パネルですぐに確認する。
- パネルを展開して、結果を確認する前にメタデータをさらに詳しく調べる。

この機能は、既存のカスタム ロール、Operators、UEBA Analysts、Content Administratorsを除くすべてのユーザ ロールでデフォルトで有効になっています。バージョン11.5にアップグレードする場合、管理者は既存のカスタム ロールに`investigate-server.event.filter`権限を追加する必要があります(「(オプション) ロールの追加と権限の割り当て」の「ロールに割り当てられた権限の変更」を参照)。詳細については、『NetWitness Investigateユーザ ガイド』の「 [イベント]ビューでのメタデータの調査(ベータ)」を参照してください。



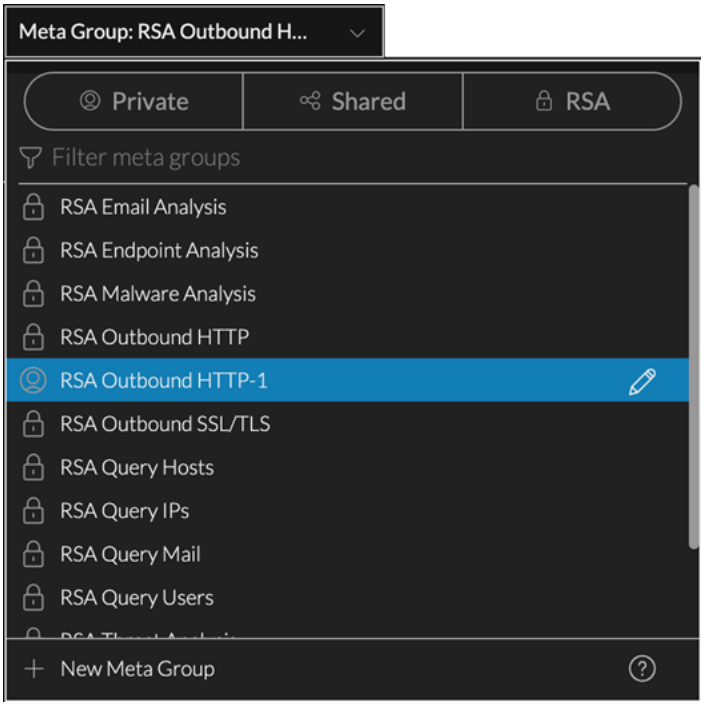
各ユーザのプライベート調査コンテンツとユーザ間で共有される調査コンテンツの分離

各ユーザは、他のユーザが表示または変更できないプライベートのプロファイル、メタ グループ、列グループを持ち、［イベント］ビューで使用することができます。コンテンツを管理するためのユーザ インタフェースはすっきりと整理されており、表示したいコンテンツのタイプ(共有、プライベート、RSA標準提供) を選択することにより、表示を制限できます。任意のタイプの任意のプロファイル、メタ グループ、列グループを複製することにより、編集して、共有またはプライベートに設定することができます。詳細については、「メタ グループを使用して関連性の高いメタ キーにフォーカス」、「イベント リストでの列と列グループの使用」、「クエリ プロファイルを使用した調査の共通領域のカプセル化」を参照してください。



メタ グループにより [イベント]ビューの各 イベントの属 性をアナリストが最 適 化

アナリストは、 [イベント]ビューで数 千 のイベントを調 査して確 認 するときに、メタ グループを使 用してイベントごとの属 性 (メタ キー) の順 序と数を最 適 化し、パターンを識 別して、さらなる調 査 が必 要 かどうかを判 断 できます。アナリストは、メタ グループの作 成 、複 製 、編 集 、削 除を行えます。標 準 提 供メタ グループと共 有メタ グループは、 [ナビゲート]ビューと [レガシー イベント]ビューで使 用されるメタ グループと同じあるのに対し、プライベート メタ グループは、 [イベント]ビューで1人 のユーザのみが使 用できます。詳 細については、「メタ グループを使 用して関 連 性 の高いメタ キーにフォーカス」を参 照してください。



メールの添 付ファイルとファイルをダウンロードするときの保 護を追 加

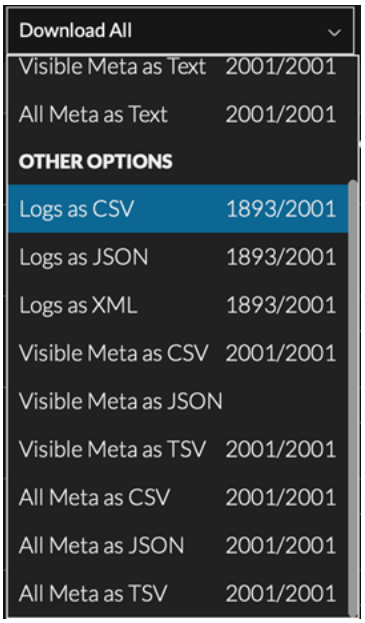
メールの添 付ファイルとファイルをダウンロードするときに、潜 在 的に悪 意 のあるファイルが自 動 的に開くのを防ぐことができます。パスワードで保 護されたzipアーカイブは、ウイルス対 策 ソフトウェアによって悪 意 のあるファイルのダウンロードが検 疫 されるのを防ぎますが、ファイルを開くには、パスワードとして `netwitness`を入 力する必 要 があります。詳 細については、「 [イベント]ビューでのデータのダウンロード 」を参 照してください。

[イベント]ビューでメタ値 を右 クリックしたときの、コンテキスト メニューのアクションの更 新

[イベント]ビューのコンテキスト メニューのアクション オプションとラベルが更 新され、 [Equalsドリルダウン]、 [新しいタブでEqualsドリルダウン]、再 フォーカス サブメニュー オプションが含 まれるようになりました。詳 細については、「結 果 の追 加 のコンテキストを検 索 」を参 照してください。

より詳細な分析や証拠のために [イベント]ビューのすべてのメタデータをダウンロードする機能を追加

新しいダウンロード オプション([すべてのメタ]) では、 [表示中のメタ]オプションでダウンロードされる表示中の列だけでなく、 [イベント]パネル内のすべてのメタデータがダウンロードされます。 [すべてのメタ] ダウンロード オプションは再構築でも使用できます。ダウンロードには、イベント リストに表示される列に関係なく、選択したイベントのメタデータがすべて含まれます。たとえば、メタ データベースに40個のメタ キーがある場合、列グループによりイベント リストに10個の列が表示されている場合でも、そのイベントの40個のメタ キーがすべてダウンロードしたファイルに含まれます。詳細については、『NetWitness Investigateユーザ ガイド』の「 [イベント]パネルでのイベントまたはメタデータのダウンロード」を参照してください。

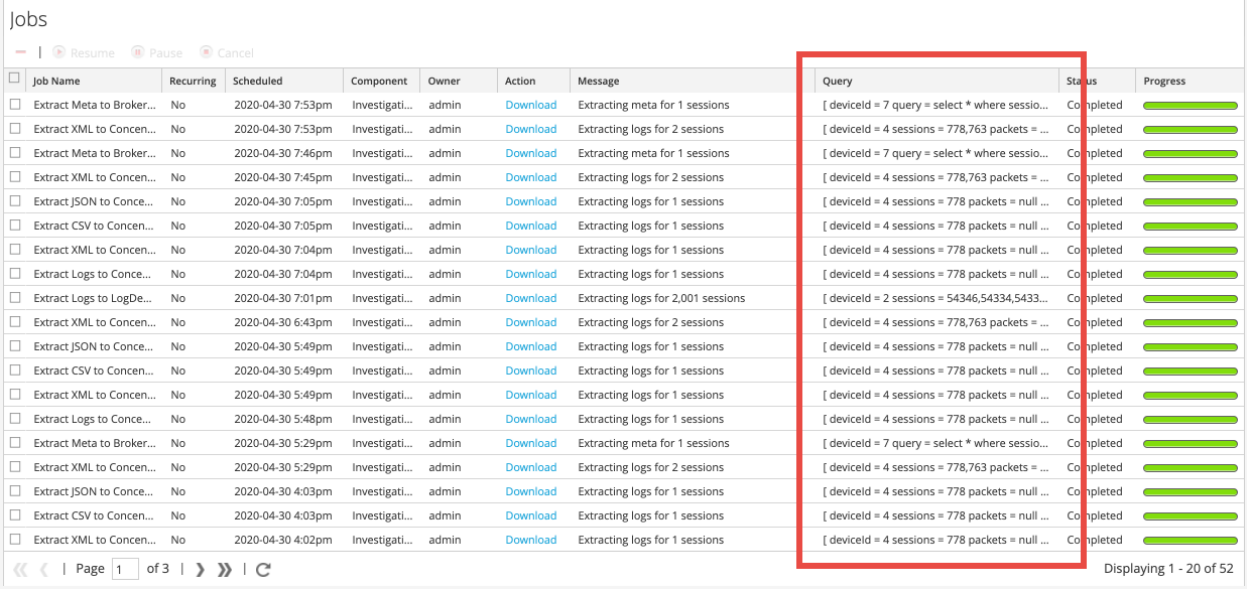


[イベント]ビューからのダウンロードに、人間可読の時間形式を使用するオプションにより利便性を向上

以前のダウンロードでは、理解するために何らかの変換が必要となるエポック形式が日付に使用されていました。管理者は、ダウンロードの時間形式を、 [イベント]パネルでの表示に似た読みやすい表現に設定できます。「`04/13/2020 09:17:36 am - 07:00 pm`」は、ユーザ インタフェースに表示される12時間制の時間の例です。ダウンロードでは、この時間がエポック形式の「`61547519856000`」に変換されます。管理者がダウンロードの時間形式を読みやすい表現に設定している場合、これと同じ時間は「`04-13-2020T09:17:36AM-07:00`」になります。詳細については、『NetWitness Investigateユーザ ガイド』の「時間範囲の選択」を参照してください。

失敗したジョブを開始したアクションまたはクエリをジョブ キューの詳細で識別

ジョブ キューで失敗したジョブを表示すると、ジョブを生成したクエリまたはアクションの詳細を確認できるため、そのジョブを開始したアクションまたはクエリを見つけるためにログを調べる必要がありません。ジョブが失敗した理由を特定して再実行するのが簡単になります。詳細については、「ジョブの管理」を参照してください。



User Entity Behavior Analytics

UEBAからネットワーク イベント表示への移行

アナリストは、インジケータを選択し、インジケータの下にあるイベント テーブルで移行リンクの1つをクリックすることにより、［イベント］ビューに移行し、ネットワーク イベントをさらに調査できるようになりました。詳細については、『NetWitness UEBAユーザ ガイド』を参照してください。

VPNログおよびAzure Active Directoryログの新しいデータ ソースと追加インジケータのサポート

UEBAでは、アナリストがVPNログとAzure Active Directoryログの分析を実行し、環境内のすべてのユーザの潜在的に危険な振る舞いを調査して監視するのに役立つ、新しいデータ ソースとインジケータのサポートを追加しました。たとえば、Azure Active DirectoryとVPNの両方での複数の認証失敗を異常なアクティビティとして特定し、「Multiple Failed Authentications - External Access」アラートをトリガできます。詳細については、『NetWitness UEBAユーザ ガイド』を参照してください。

新しいネットワーク インジケータ

新しいネットワーク インジケータは、ドメイン、SSLサブジェクト、宛先組織、宛先ポートなどの新しい外部ターゲットの出現や、新しいJA3ハッシュで使用できます。詳細については、『NetWitness UEBAユーザ ガイド』を参照してください。

物理導入環境のパフォーマンスの向上

UEBAモデルのベースラインを作成するために必要な履歴データの処理において、パフォーマンスが向上しました。詳細については、『NetWitness UEBAユーザ ガイド』を参照してください。

インシデント対応

[対応]ビューのインシデント リストとアラート リストで保存されたフィルタを使用可能

アナリストは、[対応]ビューのインシデント リストとアラート リストのフィルタを保存できます([対応]> [インシデント]および[対応]> [アラート])。たとえば、アナリストは、過去24時間の重大なインシデントのみを表示するインシデント フィルタを作成したい場合があります。また、過去24時間の特定のソースおよび特定の重大度のアラートのみを表示するアラート フィルタを作成したい場合があります。フィルタを保存しておくと、次のメリットがあります。

- アナリストは、特定のフィルタ条件を保存し、インシデントとアラートのリストにすばやく適用できます。
- 保存されたフィルタはグローバルであるため、すべてのアナリストが保存されたフィルタにアクセスできます。
- 保存されたフィルタを使用して、スプリングボードのパネルをカスタマイズできます。

スプリングボードで使用中のフィルタは削除できません。[対応]ビューの保存フィルタの詳細については、『NetWitness Respondユーザ ガイド』を参照してください。

Analystsロールには、必要なRespondの保存フィルタ権限がデフォルトで割り当てられています。必要な権限の詳細については、『システム セキュリティとユーザ管理ガイド』の「Respondの保存フィルタ権限」を参照してください。

ヘルス モニタ

稼働状態の監視機能の拡張

新ヘルス モニタは、改善された直感的なダッシュボード、監視、可視化機能を提供します。

これにより、稼働状態パラメータに関するさまざまな統計と詳細情報に基づいて、NetWitness Platform導入環境全体を可視化できるため、監視の複雑さが軽減されます。

これらのダッシュボード、監視、可視化機能のカスタマイズは、シンプル、柔軟、かつ使いやすさを特長としています。

以下は、新しく追加されたダッシュボードと改善されたダッシュボードの例です。

- **ESA Correlation概要ダッシュボード** - このダッシュボードには、ESA導入環境の稼働状態の統計とトレンドが表示されます。

- **ホスト ダッシュボード** - このダッシュボードには、導入環境内の選択したNetWitnessホストのリソース使用率と稼働状態の統計情報が表示されます。
- **ログ ダッシュボード** - このダッシュボードからは、NetWitness Platformのログ導入環境の洞察を得ることができます。

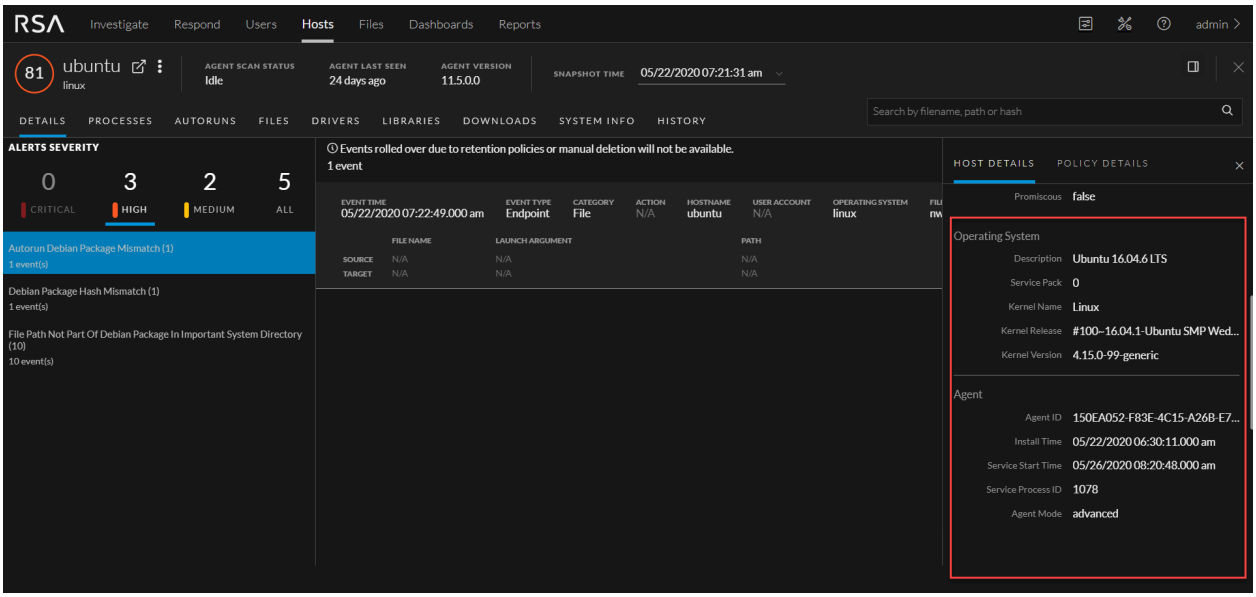
管理者は、アラート通知(メール通知やSyslog通知など)を使用して、稼働状態アラートを追加できます。また、必要に応じて、一定の期間、通知を抑制することもできます。

詳細については、『システム メンテナンス ガイド』の「新ヘルス モニタの監視」を参照してください。

エンドポイントの調査

Linuxエージェントがubuntuをサポート

エージェントのサポート対象に、Ubuntuバージョン16.04 LTS、18.04 LTS、20.04 LTSが追加されました。これにより、RSA NetWitnessは、ネットワーク内のUbuntuベースの資産に存在する脅威を検出できます。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。



WindowsエージェントがWindows 10(バージョン2004) をサポート

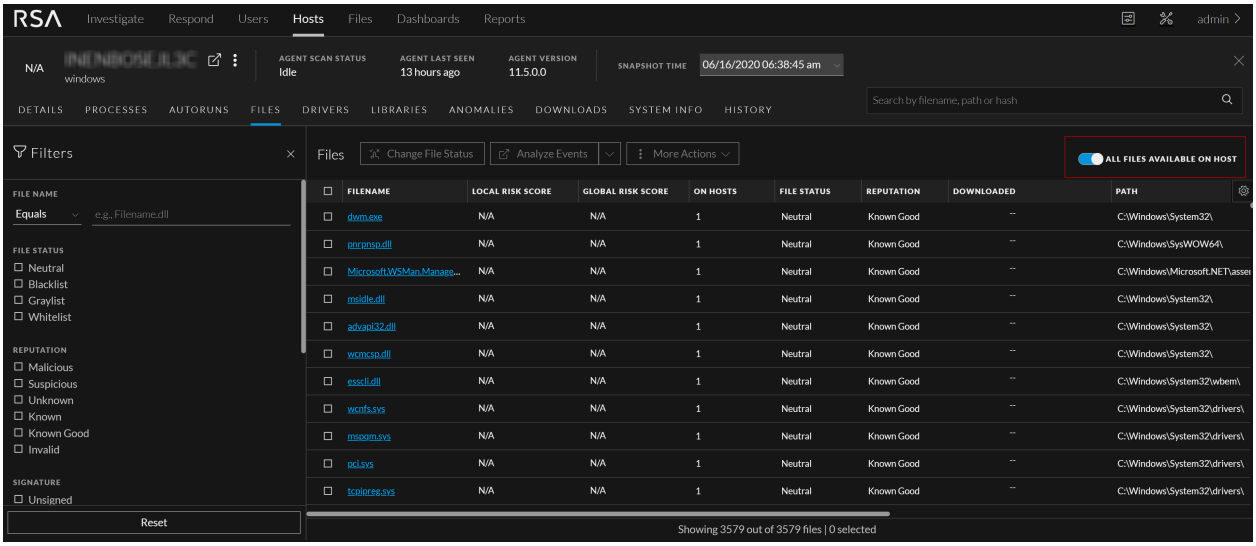
エージェントのサポート対象に、19041.329以降のWindows 10、バージョン2004(32ビットおよび64ビット) が追加されました。詳細については、『NetWitness Endpointエージェント インストール ガイド』を参照してください。

[ホスト]ビューの可視性の向上

アナリストは [**ホスト上のすべてのファイル**]オプションを使用して、特定のホストから報告されたすべてのファイルを表示し、調査を迅速化できます。以下のファイルが含まれます。

- スキャンおよび追跡により報告されたすべてのファイル
- 削除されたファイル

[**ホストで使用可能**]フィルタと [**ホストから削除済み**]フィルタも追加され、アナリストが分析対象ファイルを絞り込めるようになりました。詳細については、「ホストの調査」を参照してください。



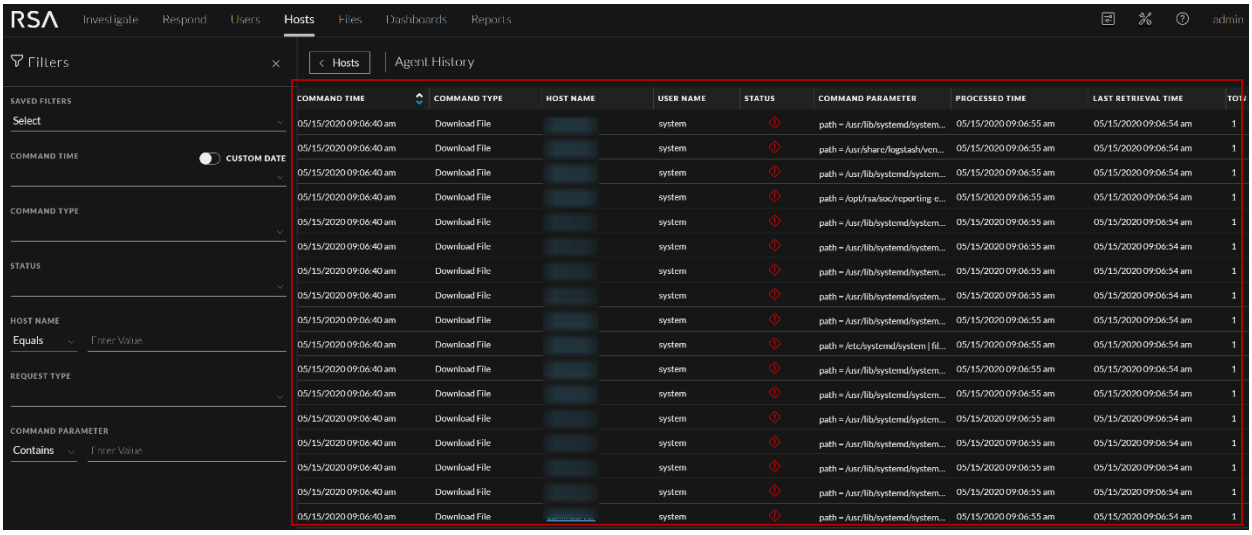
エージェント履歴の表示機能

エージェント履歴には、エージェントに対して発行され、ホスト上で実行されたコマンド(サーバ発行、またはアナリストの操作により発行) の詳細が一覧表示されます。これによりアナリストは、発行されたコマンドのステータス(成功、保留中、エラーなど) を確認できます。

たとえば、アナリストは、MFT、ファイル ダウンロード、システム ダンプなど、発行されたコマンドのステータスを複数のホストにわたって確認できます。

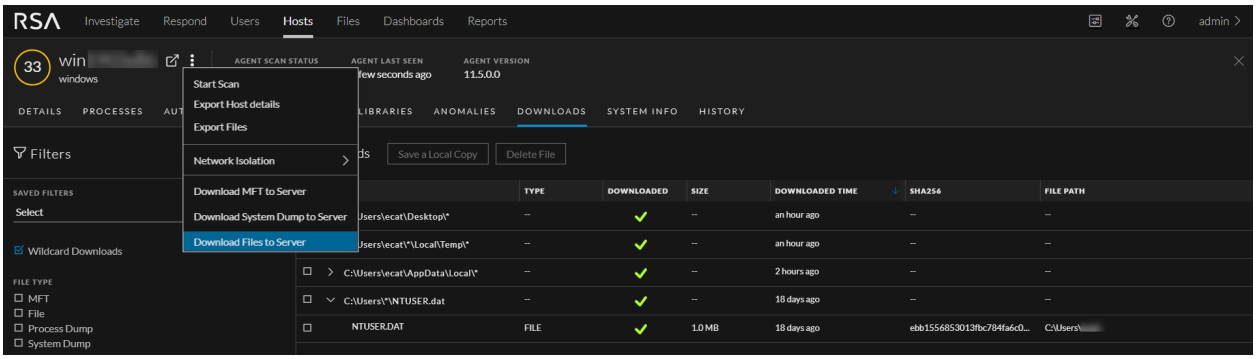
アナリストは、特定のホストのエージェント履歴を表示するか、グローバル エージェント履歴を表示するか選択できます。グローバル エージェント履歴には、さまざまなホストで発行されたコマンドに加え、コマンド タイプ、コマンド ステータス、コマンド パラメータなどの詳細が含まれています。

フィルタ機能により、コマンド履歴の詳細を選択的に表示できるため、アナリストは特定の情報に焦点を当てて、必要なアクションを実行できます。詳細については、「ホストの調査」を参照してください。



任意のファイルのダウンロード サポート

詳細な調査が必要な場合、アナリストは、スキャンまたは追跡の一部として報告されているかどうかに関係なく、ホスト上に存在するファイル(レジストリ ハイブ、ドキュメント、その他の任意のファイルなど) をダウンロードできるようになりました。アナリストは、ファイルのフル パス、ファイル名、またはワイルドカードを指定してファイルをダウンロードしたり、同時に複数のホストからファイルのダウンロードを要求したりできます。詳細については、「ホスト フォレンジックの実行」を参照してください。



エンドポイントの構成

ネットワーク帯域幅の調整パラメータ

ファイル ログ ポリシーとWindowsポリシーでは、新しい [**ネットワーク帯域幅の制御**] パラメータを使用して、エージェントがNetWitness Platformへの接続に使用するネットワーク帯域幅を制限できます。

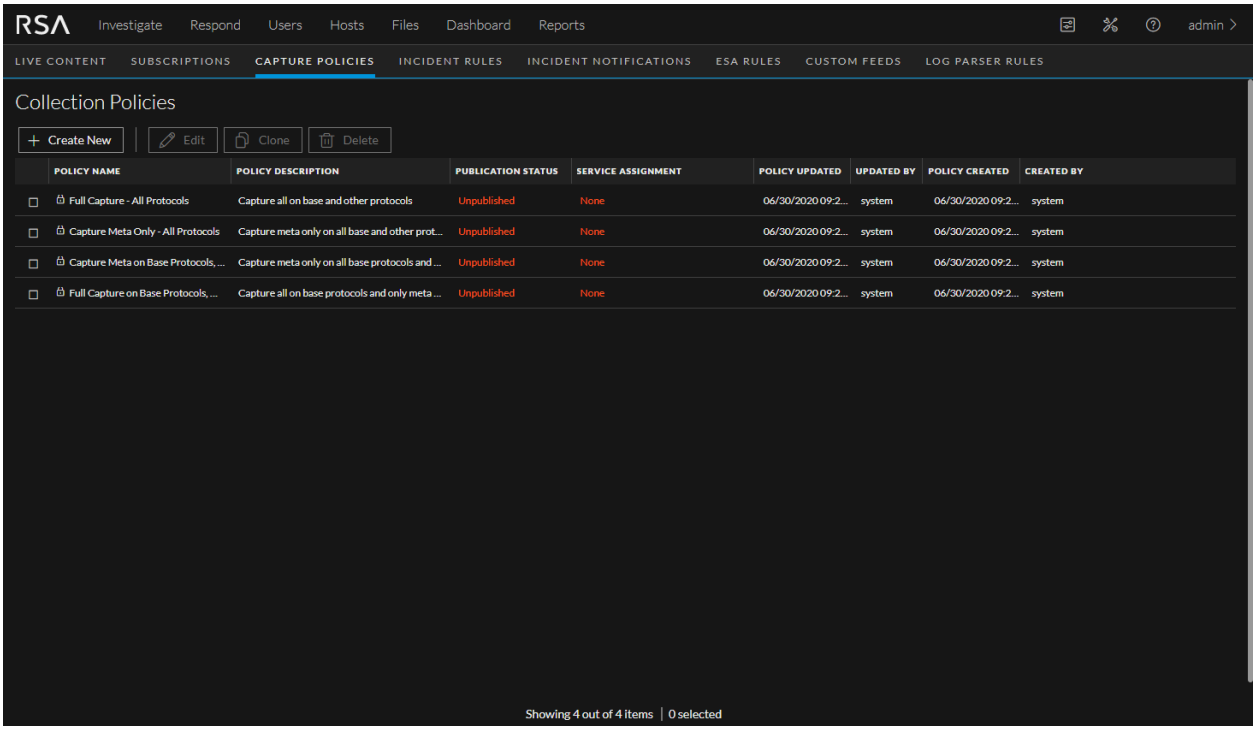
Broker、Concentrator、Decoder、Log Decoderサービス

選択的ネットワーク データ収集

選択的ネットワーク データ収集により、管理者は、一元管理された収集ポリシーを複数のNetwork Decoderに適用できます。これにより、ハード ドライブ領域などのDecoderリソースの使用率が向上し、コストの予測可能性が高まり、複数のDecoderを管理する負担が軽減されます。管理者はポリシーを使用して、保存されるトラフィックとその保存方法を決定します。各ポリシーには、サポートされているベース プロトコルのリストと、検出されたその他のプロトコルの処理方法の定義が含まれています。プロトコルの基本セットが使用可能なため、管理者はプロトコルごとに目的の収集レベルを選択できます。

注： Decoderがメタデータのみを収集するよう構成するオプションのライセンスが利用可能です。

管理者は、事前定義されたポリシーを導入するか、カスタム ポリシーを作成して導入環境をさらに制御できます。詳細については、『Decoder構成ガイド』の「選択的ネットワーク データ収集の構成」を参照してください。



Snortルール対象範囲の拡大

NetWitness Platformは、さまざまなSnortルールをサポートするようになりました。これにより、以前はサポートされていなかった、コミュニティで利用可能な検出ルールを使用できます。サポートされるようになった新しいルール パラメータには、次のものがあります。

- `nocase`
- `byte-extract`
- `byte-jump`
- `threshold`
- `depth`
- `offset`

詳細については、『Decoder構成ガイド』の「Decoder Snort検出」を参照してください。

データ収集中のNetwork DecoderとLog Decoderへのインポート

管理者は、Network DecoderとLog Decoderがリアルタイムにデータを収集する間も、データをインポートできるようになりました。これにより、ネットワーク外で収集されたデータを分析する際のダウンタイムがなくなります。

複数アダプタによるパケット収集

Network Decoderは、複数のインタフェースから同時にパケットを収集できるようになりました。この機能により、Network Decoderは各ネットワーク インタフェース カード(NIC)で同じネットワーク ルール、アプリケーション ルール、パーサを活用しながら、複数の物理NICから収集することが可能になります。

詳細については、『Decoder構成ガイド』の「(オプション) 複数アダプタによるパケット収集」を参照してください。

監査ログへのユーザ アカウントおよび集計アカウント情報の追加

以前は、アップストリーム デバイスの検索を必要とするクエリ(Brokerに対するクエリなど)をユーザが実行した場合に、アップストリーム デバイスの監査ログには集計アカウントのユーザ名のみが表示されていました。バージョン11.5では、集計アカウントに加え、クエリを送信した実際のユーザに関する情報が監査ログに含まれるようになりました。たとえば、監査ログには次のような情報が表示されます。

`User aggAccount (session 478, [::1]:1133, on behalf of <username of submitter>) has requested the SDK transforms.`

この情報は、複数レベルのBrokerとConcentratorを経由する場合にも表示されます。詳細については、「グローバル監査ログの確認」を参照してください。

セッション メタデータ リストにDecoder識別子の値を追加

Decoder識別子(`did`)の値は、どのDecoderがメタデータを生成したかを示します。`did`値を、各Decoderセッションのメタデータ リストで使用できるようになりました。これは、Concentratorがなく、Decoder自身がインデックス作成を行う環境にとって重要な機能です。

注: 11.4の初期バージョンの混在モード環境では、`did`値がセッションに含まれていることが検出されず、既存の`did`値が複製される可能性があります。

メタ専用Decoderの構成

管理者は、Log DecoderとNetwork Decoderがログやパケットを処理した後、ディスクに書き込む前に削除するよう構成できます。この機能はメタ専用Decoderと呼ばれ、多くのストレージ領域を節約できます(ただし、このオプションを使用すると、メタデータを生成したトラフィックを再構築できません)。この機能を使用すると、すべてのログとパケットが解析後に削除されるため、データベースに書き込まれることはありません。ログとパケットは通常どおりシステムを通過するため、解析やその他の操作には影響しません。詳細については、『Decoder構成ガイド』の「(オプション) メタ専用Decoderの構成」を参照してください。

Event Stream Analysis(ESA)

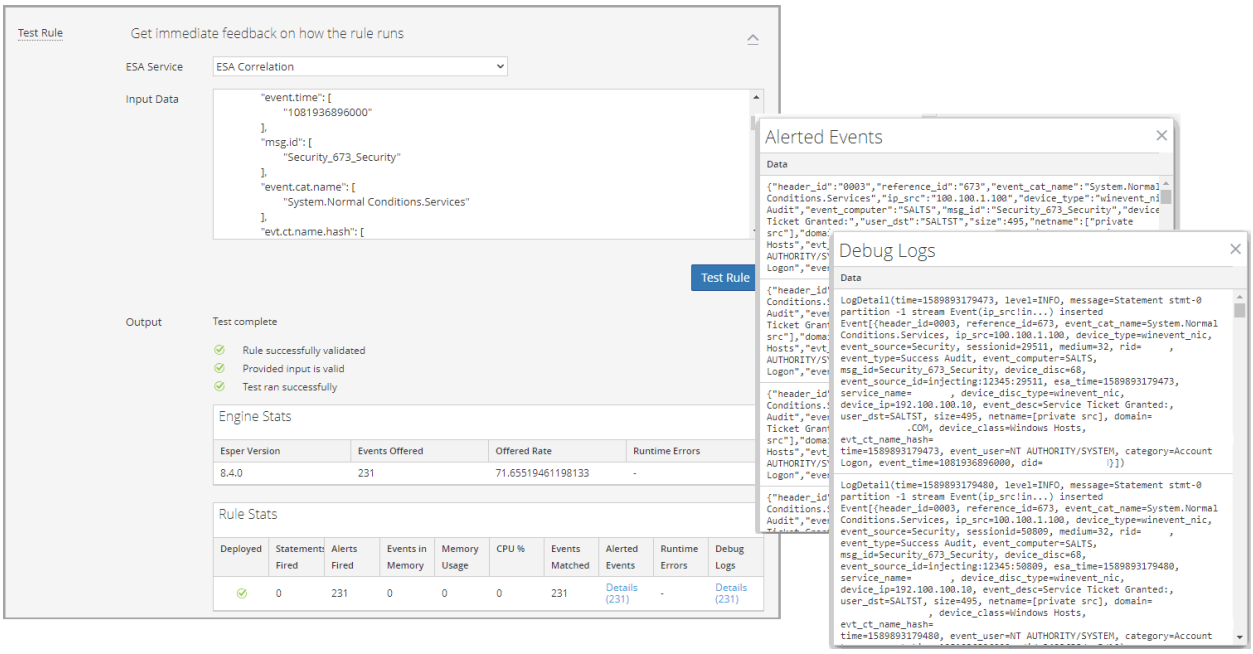
ESAルールごとにメモリ閾値を個別に構成

ESAルールがメモリを過剰に使用するのを防ぐため、ユーザは個々のESAルールにメモリ閾値を設定できるようになりました。メモリを使用するESAルール(期間ウィンドウやパターン マッチングを含むルールなど)には、メモリ閾値を設定します。メモリ閾値オプションは、評価版ルールと評価版以外のルールの両方で機能します。新しいルールには、デフォルトで100 MBのメモリ閾値が設定されます。バージョン11.5より前に存在していたルールにはデフォルト値がないため、メモリ閾値は設定されていません。

割り当てられたメモリ閾値をESAルールが超えた場合、ルールは個別に無効化され、  (構成)>[ESAルール]>[サービス]タブにそのルールのエラーが表示されます。そのルールのCPU%も確認できます。これは、各ルールが使用するESAルール導入環境のCPU使用率です。詳細については、「ESAルールのメモリ閾値の変更」の「個々の評価版ルールと非評価版ルールのメモリ閾値の変更」を参照してください。

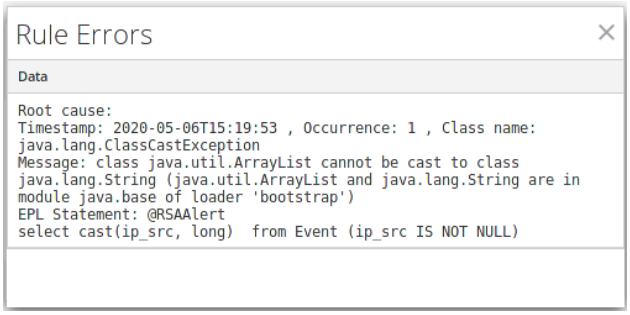
ルール ビルダまたは詳細EPLルール ビルダ内でのESAルールの検証

ESAルール ビルダ内で、ESAルールを検証して、ルールを導入する前にルール ロジックが期待どおりに機能しているかどうかを判断できます。外部Webサイトでルールをテストする代わりに、[調査]ビューからJSON形式のファイルにイベントをダウンロードし、イベントをコピーして、ルール ビルダの[テスト ルール]セクションの[入力データ]フィールドにペーストできます。



ルールの作成者は、テスト ルールの出力を見て、結果がルール要件を満たしているかどうかを判断できます。

出力には、ESA Correlationサービスの処理統計に加え、発生したアラート、メモリ内のイベント数、メモリ使用率、CPU%、一致したイベント数などの各ルールの個々の統計が表示されます。ルールによっては、アラートが発行されたイベント、ランタイム エラー、デバッグ ログへのリンクが使用可能になります。



[アラートが発行されたイベント]リンクをクリックすると、そのアラートの原因となったイベントをすばやく表示できます。デバッグ ログは、ESAルールのトラブルシューティングに役立ちます。

注： 出力にアラートは表示できますが、このテストではアラート通知は送信されません。

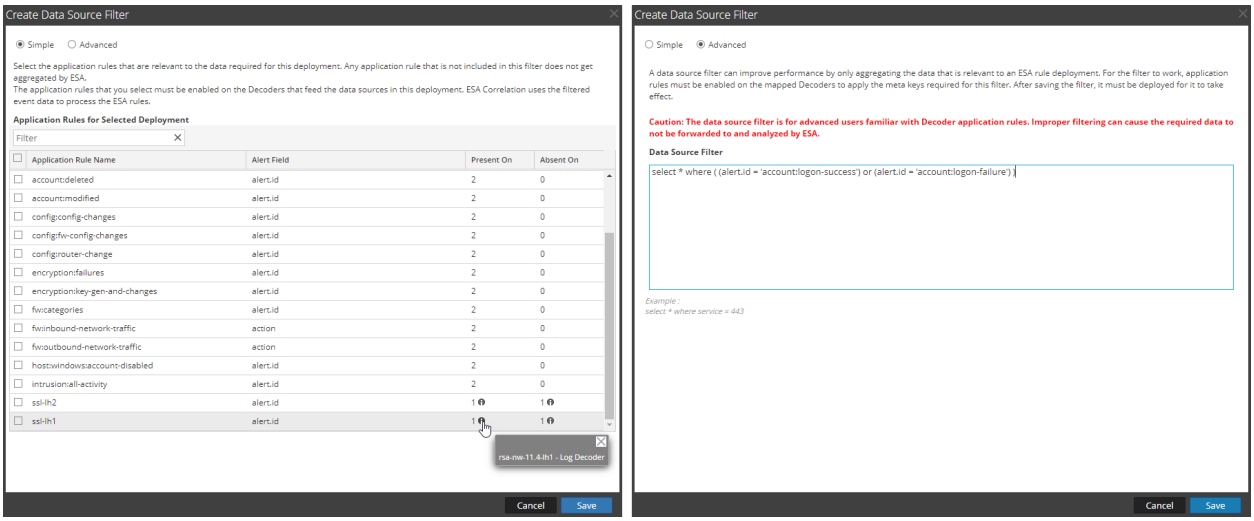
詳細については、『ESA相関ルール アラート ユーザ ガイド』の「ESAルールの検証」および「詳細EPLルールの検証」を参照してください。

Esperバージョンを8.2.0から8.4.0にアップグレード

NetWitness Platform 11.5では、ESA CorrelationサービスはEsperバージョン8.4.0をサポートしています。

ESAルール導入環境のデータ ソースのフィルタ オプション

パフォーマンスを向上させるため、オプションのデータ ソース フィルタをESAルール導入環境に追加して、導入環境と関連性の高いデータのみがESAに転送されるようにすることができます。フィルタは、アプリケーション ルールで構成され、選択したデータ ソースにマッピングされたDecoderに適用されます。



注意：データ ソース フィルタは、Decoderのアプリケーション ルールに精通している上級ユーザを対象としています。不適切なフィルタリングを行うと、必要なデータがESAに転送されず、分析されない可能性があります。

詳細については、『ESA相関ルール アラート ユーザ ガイド』の「(オプション) データ ソース フィルタの追加」を参照してください。

詳細EPLルールによるContext Hubリストの動的更新

詳細ルールで@RSAContextアノテーションを使用して、ルールの実行後にContext Hubリストへのデータの追加または削除を動的に行うことができます。たとえば、IPアドレスのブラックリストへの追加とホワイトリストからの削除を自動的に行うルールを作成できます。

単一列と複数列のContext Hubリストを更新できます。@RSAContextアノテーションは、Context Hubリストにアクセスできない場合はエラー処理も実行します。

詳細については、『ESA相関ルール アラート ユーザ ガイド』の「@RSAContextアノテーション(11.5以降)」を参照してください。

管理と構成

[イベント]ビューでのイベント絞り込みとメタ グループ管理のための新しい調査の権限を追加

3つの新しいinvestigate-server権限により、管理者は [イベント]ビューの新機能を制御できます。新しい権限により、アナリストは、 [イベント]ビューのベータ機能である [イベントの絞り込み]パネルを使用できるほか、 [イベント]ビューでメタ グループを表示および管理できます。新しい権限は、ほとんどのロールでデフォルトで有効になっています。バージョン11.5にアップグレードする場合、管理者は既存のカスタム ロールにinvestigate-server.event.filter、investigate-server.metagroup.read、および investigate-server.metagroup.manage権限を追加する必要があります。詳細については、「(オプション) ロールの追加と権限の割り当て」の「ロールに割り当てられた権限の変更」を参照してください。

[対応]ビューのインシデント リストとアラート リストで使用する新しい保存フィルタの管理権限

[対応]ビュー([対応]> [インシデント]および [対応]> [アラート]) でインシデントおよびアラートの保存フィルタを使用するには、respond-server.incident.manage、respond-server.incident.read、respond-server.alert.manage、respond-server.alert.readの各権限が必要です。Analystsロールには、必要なRespondフィルタ権限がデフォルトで割り当てられています。詳細については、「ロールの権限」の「Respond-server」を参照してください。

Reporting Engineのコンテンツを導入するためのReporting Engineコンテンツ管理者ロール

RSA NetWitness® Platformでは、LiveからReporting Engineのコンテンツを導入するための新しいロール「Reporting Engineコンテンツ管理者」が追加されました。Reporting Engineコンテンツ管理者のロールを持つユーザは、LiveからReporting Engineコンテンツ(ルール、レポート、チャート、スケジュール、リスト) を検索して導入したり、導入されたコンテンツを表示または変更したりできるため、導入済みコンテンツへの権限を追加するよう管理者に依頼する必要がなくなります。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。

Reporting Engineサービス自動リカバリのための新しいツール

RSA NetWitness® Platformでは、Reporting Engineサービスをアップグレード後に再起動できない場合に、Reporting Engineサービスをリストアするための新しいReporting Engine移行リカバリツールが追加されました。詳細については、「Reporting Engine移行リカバリツール」を参照してください。

スケジュール設定されたReporting Engineレポートの実行を停止するオプション

以前は、スケジュール設定された同じレポートが2つ以上同時に実行され、未完了の場合に、手動で停止する機能がありませんでした。スケジュール設定されたレポートが複数同時に実行されている場合、アナリストが必要に応じて個別にレポートを停止できるようになりました。詳細については、「Reportingユーザ ガイド」を参照してください。

IPアドレス変更プロセスの改善

管理者は、処理の中断を最小限に抑えながら、環境内の任意のホストのIPアドレス、ネットマスク、ゲートウェイを変更できるようになりました。NW Serverホストおよびコンポーネント ホストのネットワーク構成を変更するプロセスを簡略化するため、nwsetup-tuiスクリプトが更新されました。詳細については、『システム メンテナンス ガイド』の「ホスト ネットワーク構成の変更」を参照してください。

ウォーム スタンバイNW ServerにアクティブNW Serverとは異なるIPアドレスの指定が可能

管理者は、さまざまなネットワーク ゾーンや地理的な場所にスタンバイNW Serverを導入できるようになりました。スタンバイNW Serverには、別のIPアドレス(プライマリと異なる) を割り当てることができます。これにより、災害復旧機能も向上します。詳細については、「ウォーム スタンバイNW Serverホスト」の「プライマリNW ServerからセカンダリNW Serverへのフェールオーバー」を参照してください。

Context Hub

(STIX経由での) 脅威インテリジェンス統合の向上による脅威検出の拡張

NetWitness PlatformとStructured Threat Intelligence Expression(STIX) の統合は、整理された脅威インテリジェンス情報により脅威検出機能を強化し、攻撃のタイムリーな検出と対応を可能にします。アナリストがSTIXデータ ソースから取得した脅威インテリジェンス情報を調査するときに、各インジケータのコンテキストが表示されるようになりました。コンテキスト情報には、攻撃者と攻撃の詳細が含まれ、Context Hubから直接 [調査]ビューと [対応]ビューの両方で表示できます。

アナリストがこの機能を使用するには、指定されたSTIXソースから脅威インテリジェンス データを取得するように、管理者がSTIXデータ ソースを構成する必要があります。

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

構成の後、アナリストはカスタム フィード ワークフローを使用してカスタム フィードをプッシュできます。サポートされるデータ ソースは、TAXIIサーバ、RESTサーバ、ファイルです。詳細については、『Context Hub構成ガイド』を参照してください。

ログ収集

ますます多くのログ イベント ソースが、syslogやSNMPなどの従来の方法ではなく、標準化されていないAPIを介してログを提供するようになっています。そのため、各イベント ソースからログを収集するためのクライアントまたはプラグインをそれぞれのAPIを使用して記述する必要があります。プラス面は、これらのログが通常、JSONなどの構造化形式で提供されることです。NetWitness 11.5では、オープン形式のログ イベント ソースからの収集と解析を大幅に改善する機能が追加されています。

Logstashのサポート

Logstashは、リアルタイムのパイプライン機能を備え、活発なコミュニティによって支持されるオープンソースのデータ収集エンジンです。ログの収集、解析、変換のために、数十のプラグインがサポートされています。NetWitnessは、Logstashから収集されたログを受け入れることができるようになりました。これにより、NetWitnessが直接サポートする収集方法やパーサのないイベント ソースからの収集が可能になります。この収集処理では、ログはJSON形式で転送され、NetWitness Platformの新しいJSONマッピング UIを使用して、解析されたLogstashデータをNetWitnessメタに簡単にマッピングできます。詳細については、『LogstashとNetWitnessの統合ガイド』を参照してください。

JSONログ直接サポートとベータ版UI

NetWitness 11.5では、JSON 形式のログを解析する機能が追加されました。これによりアナリストは、変換されていない元の形式でログを表示し、本来のコンテキストを理解し、脅威インテリジェンス サイトから受信したセキュリティ侵害インジケータのデータに関連づけることができます。NetWitness UI内の新しいユーザ インタフェース(ベータ) により、管理者はログに含まれるJSONキーをNetWitnessの適切なメタキーにマッピングできます。このマッピングにより、ログを変換し、パーサを構築する必要がなくなります。詳細については、『ログ パーサ構成ガイド』を参照してください。

Log収集プラグインのRAWパススルー オプション

NetWitnessがLog DecoderでJSONイベント データを直接解析できるようになったため、ほとんどのクラウド ログをCEFに変換する必要がなくなりました。以前は、CEFへの変換のために、プラグインをJSONスキーマごとに個別に調整する必要がありました。すべてのRAW JSONイベント データをLog Decoderに直接送信できるようになりました。これにより、NetWitnessはログを元の形式で保持し、脅威インテリジェンス サイトとの相関のために使用できます。また、NetWitnessプラグインは、APIベースのログ収集をユニバーサルに実行できるようになります。たとえば、新しいプラグインを作成しなくても、さまざまなソース タイプのログをAWS CloudWatchから転送できます。

注： ProofpointおよびAzure Monitorの収集プラグインは、JSON形式のパーサを使用するように更新されています。JSON形式をサポートするために、これらのパーサをRSA Liveから導入する必要があります。

ライセンス

RSA NetWitness® Platformでは、ネットワーク フル パケット ライセンスに加えて、ネットワーク メタ専用ライセンスが追加されました。ネットワーク メタ専用ライセンスは、パケット ペイロードを収集して分析し、分析後にパケット ペイロード データを破棄します。このライセンスを使用すると、フル パケット収集が不要な環境にNetWitness Platformを導入できます。これにより、ストレージ スペースを最適に管理し、セッションの全ペイロードを保持することなく脅威を簡単に検出できます。ネットワーク メタ専用ライセンスは、分析されたネットワーク パケットのバイト数を測定し、ネットワーク フル パケット ライセンスとともに使用することも、単独で使用することもできます。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。

修正された問題

このセクションでは、最後のメジャー リリース後に修正された問題のリストを提供します。修正された問題の詳細については、RSA LinkのRSA NetWitness® Platformの既知の問題リストで「Fixed Version」列を参照してください。
https://community.rsa.com/community/products/netwitness/documentation/known-issues

ログ収集の修正

追跡番号	説明
ASOC-94276	TCP Syslogのパフォーマンスが改善されました。

管理の修正

追跡番号	説明
SACE-13620	バージョン11.4では、Decoderグループに定期実行フィードを導入できません。
SACE-13572	msearchオプションを使用してクエリを実行すると、「年が有効な範囲外です：1400..9999」というエラーが表示されます。
SACE-13278	11.4へのアップグレード後、NetWitness Platformへのログイン時にログインバナーが表示されません。
SACE-13124	15ドライブViper Shelf内のディスクが「UBad」状態の場合に、RAIDツールスクリプトが失敗します。
SACE-13060	[メール通知の定義]パネルで、ドメイン名の(.) 記号の後に文字が含まれている場合、ドメイン名を含んだメール アドレスを入力できません(例：XXX@innotec.security.com) 。

監査ログ

追跡番号	説明
ASOC-85468/ASOC-86055	RabbitMQがリセットされた場合、LogstashはRabbitMQに再接続されません。

追跡番号	説明
ASOC-77307	ルール ビルダでESAルールが作成、複製、削除されるときに、監査ログに十分なコンテキスト情報が書き込まれませんでした。NetWitness Platform 11.5では、ESA Correlationサーバの監査ログに加えて、NW Serverの新しい監査ログにも、ユーザがルール ライブラリでESAルールの追加、変更、フィルタリング、削除、エクスポート、インポートをいつ行ったかが記録されます。NW Serverの監査ログには、ユーザがESAルール導入環境をいつ追加、変更、導入したかも記録されます。ESAルール導入環境の変更には、導入環境のルールの追加、削除、更新に加え、導入環境へのデータ ソースまたはESA Correlationサービスの追加が含まれます。

調査の修正

追跡番号	説明
ASOC-92642	[イベント]ビューでバックスラッシュ(\) 文字を含む値を再フォーカスしても、結果が返されません。
ASOC-92534	メール再構築では、ファイル名の不整合が原因で、添付ファイルの [ダウンロード]ボタンが有効になりません。
ASOC-85375	値に®などの一部の文字が含まれている場合、メタ キーの値でクエリできず、メタ値がトランケートされます。
ASOC-50412	ダウンロードの開始時に、Investigateはブラウザのジョブ トレイに接続できず、ダウンロード スピナーがいつまでも表示されたままになります。

対応の修正

追跡番号	説明
ASOC-83210	インシデント メール通知に「変更者」フィールドが含まれていませんでした。NetWitness Platform 11.4では、自動生成されたインシデントが更新されたときに、更新を行ったタイムスタンプとユーザを示す「変更者」フィールドがメール通知に含まれていませんでした。この問題は11.5で修正されました。
ASOC-80896	Reporting Engineアラートによって生成されたインシデントでは、データ プライバシーが有効になっているにもかかわらず、クリア テキスト値が表示されます。修正前は、データ プライバシーが有効になっている導入環境では、クリア テキスト値とハッシュ値の両方が公開されるため、Reporting Engineアラートから生成されたインシデントにはクリア テキストのメタデータが表示されていました。修正により、データ プライバシーが有効になっている場合、Reporting Engineは、難読化されたハッシュ値のみをRespondに送信するようになりました。これにより、アナリストがインシデントを表示するときにデータ プライバシーが維持されます。

追跡番号	説明
ASOC-73173	イベント内のファイル名がグローバル ファイル名と一致していない場合、[ファイル]タブに一致するファイルが表示されません。修正前は、ノード グラフから [調査]> [ホスト]または [調査]> [ファイル]タブに移行してファイルを分析するときに、イベント内のファイル名とグローバル ファイル名の大文字/小文字が一致しない場合、結果は表示されませんでした。修正により、 [調査]> [ホスト]または [調査]> [ファイル]タブに移行するときに、大文字と小文字は区別されなくなりました。

コア サービス(Broker、Concentrator、Decoder、Archiver) の修正

追跡番号	説明
ASOC-90740	Log Decoderサービスは、再起動時にコアダンプしていました。
SACE-13702	REST APIを使用してBrokerに対してクエリを実行すると、誤った結果が表示されます。
SACE-13597	TLSセッションの場合、Ja3/Ja3sおよびcert.thumbprintのメタ キーが生成されませんでした。

Event Stream Analysis(ESA) の修正

追跡番号	説明
ASOC-87778	ESAルール導入環境の名前にコロン(:) が含まれると、ストリーム開始エラーが発生しました。ESAルールの導入環境の名前にコロン(:) が含まれていると、導入時にデータ集計を開始できませんでした。この問題はNetWitness Platform 11.5で修正されました。
ASOC-77307	ルール ビルダでESAルールが作成、複製、削除されるときに、監査ログに十分なコンテキスト情報が書き込まれませんでした。 NetWitness Platform 11.5では、ESA Correlationサーバの監査ログに加えて、NW Serverの新しい監査ログにも、ユーザがルール ライブラリでESAルールの追加、変更、フィルタリング、削除、エクスポート、インポートをいつ行ったかが記録されます。NW Serverの監査ログには、ユーザがESAルール導入環境をいつ追加、変更、導入したかも記録されます。ESAルール導入環境の変更には、導入環境のルールの追加、削除、更新に加え、導入環境へのデータ ソースまたはESA Correlationサービスの追加が含まれます。
SACE-12736	複数のユーザがESAルール導入環境を同時に編集し、変更を上書きできました。2人のユーザが同じESAルール導入環境を変更して、ルールを追加または削除する場合、 [**今すぐ導入**]を先にクリックしたユーザによってもう一方のユーザの変更が上書きされました。 NetWitness Platform 11.5では、複数のユーザがESAルール導入環境を同時に編集できますが、変更は上書きできなくなりました。

Reporting Engineの修正

追跡番号	説明
SACE-12893	カスタムの時間範囲でクエリを実行したときに、［レポート］>［アラート］タブに一部のアラートが表示されません。

エンドポイントの修正

追跡番号	説明
ASOC-86942	Endpointサーバを導入後、頻繁に異常状態になります。
SACE-13763	Redhat 8.xシステムにNetWitness Endpoint Agentをインストールできません。
SACE-13529	Endpoint Log Hybridとリレー サーバのテスト接続に失敗します。

更新の修正

追跡番号	説明
SACE-12658	固定IPアドレスを構成するためにCLIでnwsetup-tuiコマンドを実行すると失敗します。
SADOCS-1883	アップグレード前に、以前のリリースのリポジトリを削除する手順について説明が必要。『*RSA NetWitness Platform 11.5アップグレード ガイド*』に手順が追加されました。

既知の問題

このリリースの未解決の問題の一覧は、RSA Linkの次のURLを参照してください。
https://community.rsa.com/community/products/netwitness/documentation/known-issues
回避策が存在する場合は、回避策の詳細が記載されているか、参照先のリンクが提供されます。

サポート終了の機能

次の表では、RSA NetWitness® Platform 11.5以降のリリースでサポートが終了した機能について説明します。

11.5.0.0以降のリリースでサポートが終了した機能

注：Event Stream Analysis(ESA) のサポートは終了していません。ESA Correlationサービス(ESA相関ルール) はサポートされています。自動脅威検出に使用されるEvent Stream Analytics Serverサービス(ESA Analytics) のサポートは終了します。ESA Analyticsの代わりに、より機能豊富でパフォーマンスに優れたESA相関ルールを使用してください。

機能	メモ
ESA Analytics/自動脅威検出	Event Stream Analytics Server(ESA Analytics) サービスは、NetWitness Platformバージョン11.5以降でサポートが終了するため、使用できません。 [ESA Analyticsマッピング]パネルは、ユーザ インタフェース([管理]> [システム]) に表示されなくなりました。
WhoIs Lookupサービス	ESA Analyticsで使用される [WhoIsルックアップ構成]パネルは、ユーザ インタフェース([管理]> [システム]) に表示されなくなりました。
Warehouse Analytics	レガシーWarehouse AnalyticsはNetWitness Platform 11.0以降のリリースではサポートが終了し、ユーザ インタフェースに表示されなくなりました。

製品ドキュメント

このリリースでは、次のドキュメントが提供されます。

ドキュメント	参照場所
RSA NetWitness Platform 11.x 総合目次	https://community.rsa.com/docs/DOC-81328
RSA NetWitness Platform 11.5製品ドキュメント	https://community.rsa.com/community/products/netwitness/115
RSA NetWitness Platform 11.5アップグレード ガイド	https://community.rsa.com/docs/DOC-112676

製品ドキュメントへのフィードバック

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。

NetWitness Platformのサポート

セルフ サポート 用 のリソース

NetWitness Platformのインストールおよび使 用について支 援が必 要な場 合 は、次 の情 報をご利 用ください。

- 次 の場 所 でNetWitness Platformのすべてのドキュメントを参 照 できます。
  https://community.rsa.com/community/products/netwitness/documentation
- RSA Linkの [**Search**]と [**Ask it**]を使 用し、必 要な情 報を検 索 できます。
  https://community.rsa.com/welcome
- RSA NetWitness® Platformのナレッジベース
  https://community.rsa.com/community/products/netwitness/knowledge-base
- RSA NetWitness® Platformのトラブルシューティング情 報
  https://community.rsa.com/community/products/netwitness/documentation/troubleshooting
- RSA NetWitness® Platformのブログ投 稿
- さらに支 援が必 要な場 合 は、RSAサポートにお問い合 わせください。

RSAサポート へのお問い合 わせ

RSAサポートにお問い合 わせいただく場 合 は、PCにアクセスできる状 態 になっている必 要 があります。以 下 の情 報を提 供 できるよう準 備しておいてください。

- 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

質 問 や支 援が必 要な場 合 は、次 の連 絡 先をご使 用ください。

RSA Link	https://community.rsa.com メイン メニューで [**My Cases**]をクリックします。
各 国 のお問い合 わせ窓 口	https://community.rsa.com/docs/DOC-1294
コミュニティ	https://community.rsa.com/community/support

ビルド番号

次の表は、NetWitness Platform 11.5.0.0の各コンポーネントのビルド番号の一覧です。

コンポーネント	バージョン番号
NetWitness Platform Audit Plugins	11.5.0.0-4615.5.3fd9584cb.el7.noarch.rpm
NetWitness Platform Appliance	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Archiver	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Broker	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Concentrator	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Config Management	11.5.0.0-2008111220.5.ff9e424.el7.noarch.rpm
NetWitness Platform Config Server	11.5.0.0-200710072900.5.bd6a63c.el7.centos.noarch.rpm
NetWitness Platform Console	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Content Server	11.5.0.0-200630183429.5.512a4b8.el7.centos.noarch.rpm
NetWitness Platform ContextHub Server	11.5.0.0-200728093949.5.488ccfe.el7.centos.noarch.rpm
NetWitness Platform Correlation Server (ESA)	11.5.0.0-200806185527.5.4bcdaf3.el7.centos.noarch.rpm
NetWitness Platform Decoder	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Deployment Upgrade	11.5.0.0-2006261254.5.22cec34.el7.noarch.rpm
NetWitness Platform Endpoint Agents	11.5.0.0-2006151822.5.4bdbb4a.el7.x86_64.rpm
NetWitness Platform Endpoint Broker Server	11.5.0.0-200619040007.5.686adbd.el7.centos.noarch.rpm
NetWitness Platform Endpoint Server	11.5.0.0-200619014840.5.8b18a0a.el7.centos.noarch.rpm

NetWitness Platform Integration Server	11.5.0.0-200710042756.5.4e8cb86.el7.centos.noarch.rpm
NetWitness Platform Investigate Server	11.5.0.0-200708104951.5.5091482.el7.centos.noarch.rpm
NetWitness Platform Legacy Web Server	11.5.0.0-200810151928.5.9b5bd42.el7.centos.noarch.rpm
NetWitness Platform License Server	11.5.0.0-200709025209.5.da37a84.el7.centos.noarch.rpm
NetWitness Platform Log Decoder	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Log Player	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Malware Analytics Server	11.5.0.0-200723090201.5.461916c.el7.centos.x86_64.rpm
NetWitness Platform Metrics Server	11.5.0.0-200724014709.5.4d136f3.el7.centos.noarch.rpm
NetWitness Platform Orchestration Server	11.5.0.0-200805133852.5.bc285ed.el7.centos.noarch.rpm
NetWitness Platform Reporting Engine Server	11.5.0.0-5866.5.ddb451a8b.el7.x86_64.rpm
NetWitness Platform Respond Server	11.5.0.0-200731030842.5.f45aff7.el7.centos.noarch.rpm
NetWitness Platform Root CA Update	11.5.0.0-2006261255.5.470ba8b.el7.noarch.rpm
NetWitness Platform SDK	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform Security Server	11.5.0.0-200722041910.5.50e951c.el7.centos.noarch.rpm
NetWitness Platform Source Server	11.5.0.0-200624103220.5.1add390.el7.centos.noarch.rpm
NetWitness Platform User Interface	11.5.0.0-200804200134.5.b715e6362d.el7.centos.noarch.rpm
NetWitness Platform Workbench	11.5.0.0-11293.5.0c5da3886.el7.x86_64.rpm
NetWitness Platform SA Tools	11.5.0.0-2006261246.5.4688bd1.el7.noarch.rpm
NetWitness Platform SMS Runtime	11.5.0.0-4615.5.3fd9584cb.el7.x86_64.rpm
NetWitness Platform SMS Server	11.5.0.0-4615.5.3fd9584cb.el7.x86_64.rpm

改訂履歴

日付	説明
2020年8月	ベータ
2020年9月	初版リリース