RSA NETWITNESS® PLATFORM

リリース ノート

RSA NetWitness® Platform 11.4

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、https://www.rsa.com/ja-jp/company/rsa-trademarks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、Dell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

本製品はRSA 以外のサードパーティ製ソフトウェアを実装している場合があります。本製品を使用することにより、本製品のユーザは、本製品に含まれているサード 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

掲載される情報は、公開した時点でDellが正確であるとみなす情報であり、この情報は予告なく変更されることがあります。

10月 2020

目次

新機能

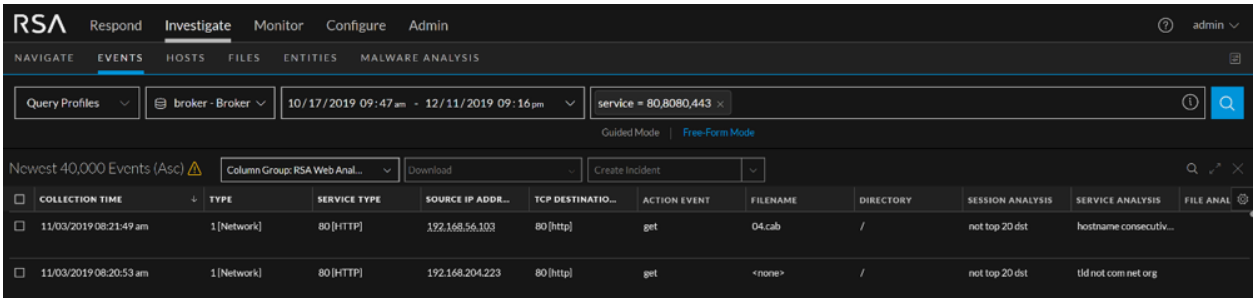
RSA NetWitness® Platform 11.4は、セキュリティ オペレーション センター(SOC) のすべてのロールに新機能と機能拡張を提供します。RSA NetWitness Platform 11.4は、検出範囲の拡大と、アナリストの利便性向上により、企業を標的とした脅威をアナリストがより見つけやすく、対応しやすくしています。主な機能には、[調査]ビューの機能向上、[対応]ビューでのインシデントのノード グラフ表示の機能拡張、複数拠点にアナリスト用ユーザ インタフェースを分散配置することによる遅延の削減などが含まれます。

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

イベント分析へのワークフローを集約

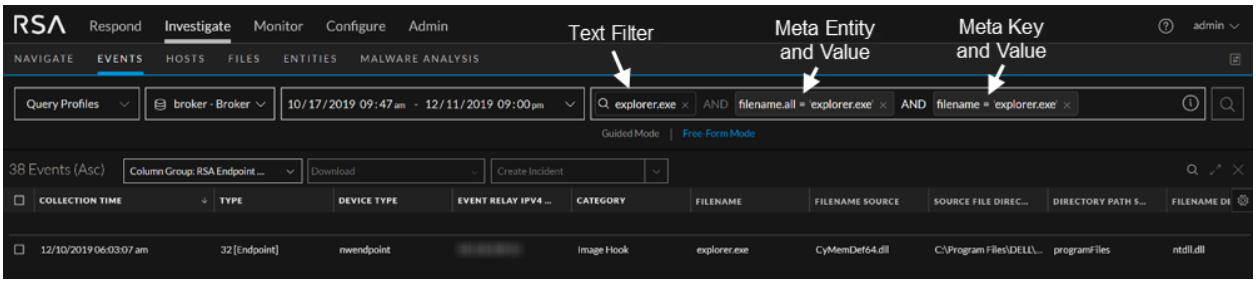
アナリストがイベントを分析する際のデフォルトのワークフローを最適化し、複数のビューを移動する必要性を減らしました。従来2つの独立したワークフロー([イベント分析]ビューと[イベント]ビュー) で提供していた機能を組み合わせ(詳細はこのドキュメント内で別途説明) 、単一のワークフローでイベントを分析できるようになりました。デフォルトでは、以前のワークフローは[調査]メニューに表示されませんが、過渡期の対応として、アナリストからの要望があれば、管理者は以前のワークフローを再有効化することができます。詳細は、『*IInvestigate ユーザ ガイド*』で「NetWitness Investigateの仕組み」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



テキスト フィルタによるクエリ

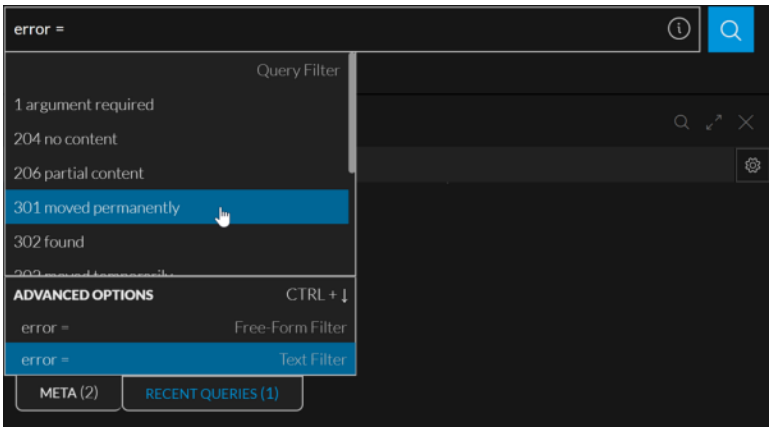
アナリストはフィルタを作成して、クエリを実行することにより、表示するイベントを制限します。通常、フィルタを作成するにはメタ キーを知っている必要があります。テキスト フィルタは、見つけたい値があるのに、どこで検索すればよいか(つまり、どのメタ キーを検索すればよいか) 確信できない場合に便利です。テキスト フィルタは、値がインデックスされたすべてのメタ キーを対象に、大文字と小文字を区別せず、検索を実行します。例えば、あるファイル名を見つけたい場合、クエリ バーをクリックし、完全なファイル名を入力し、[**テキスト フィルタ**]をクリックします。テキスト フィルタは、調査対象のサービスおよび時間範囲を対象に、インデックスされたすべてのデータを検索し、指定されたテキストと完全に一致した結果を返します。

次の図はアナリストが値を検索する際に使用できる複数の方法を示しています。テキスト フィルタを使用する場合、メタ キーを知っている必要はありません。メタ エンティティを使用する場合、ある程度のメタ キーの知識が必要です。特定のメタ キーと値を指定する場合は、使用可能なメタ キーやインデックスについてより詳細な知識が必要です。詳細は、『*Investigate ユーザ ガイド*』で「データ セット内の任意の場所で値を検索するためのテキスト フィルタの追加」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



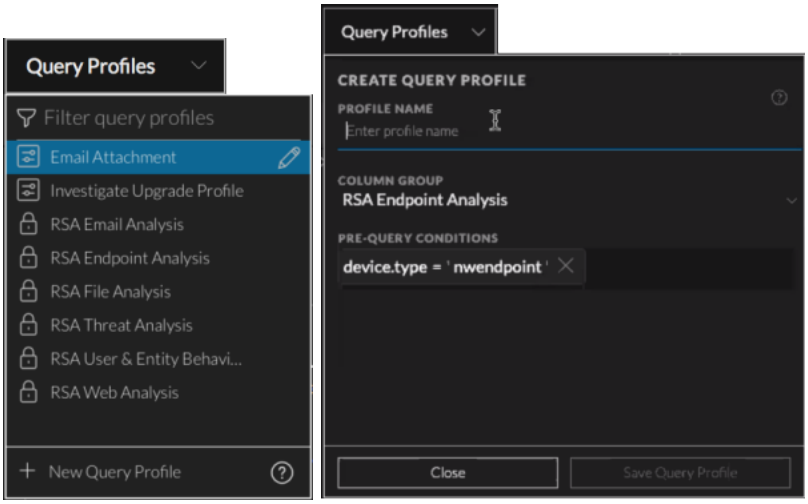
クエリ作成時にメタ値の候補を自動表示

[イベント]ビューのクエリ バーにクエリを入力する時、メタ値やメタ値の形式がいつでも直ぐにわかるわけではありません。アナリストがクエリを入力する時、値の候補を自動的に表示することにより、その環境のデータを事前に把握していなくても、関連するクエリを作成できるよう支援します。詳細は、『*IInvestigate ユーザ ガイド*』で「ガイド モードでのクエリの作成」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



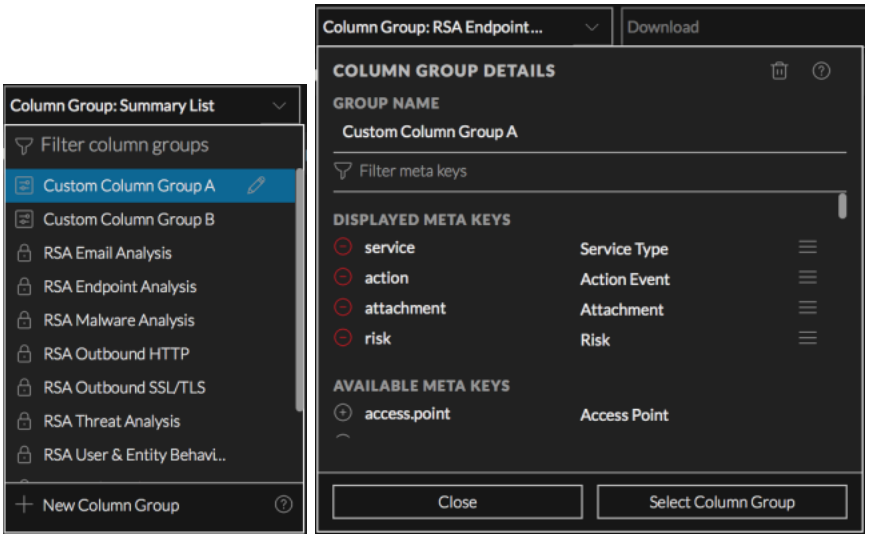
[イベント]ビューのクエリ プロファイル

アナリストが[調査]ビューを使用する時、列グループやフィルタを使用して表示する結果データを絞り込むことができます。特定の列グループとフィルタが役立つ場合は、それらをクエリ プロファイルとして保存し、再利用できます。調査を始めたばかりのアナリストは、一般的な調査のタイプに合わせて標準提供されるクエリ プロファイルを使用できます。調査の経験を積んだら、カスタムのクエリ プロファイルを作成し、編集、削除、保存できます。標準提供のプロファイルもカスタムのプロファイルも、全アナリスト共通で使用できます。詳細は、『*IInvestigate ユーザ ガイド*』で「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。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



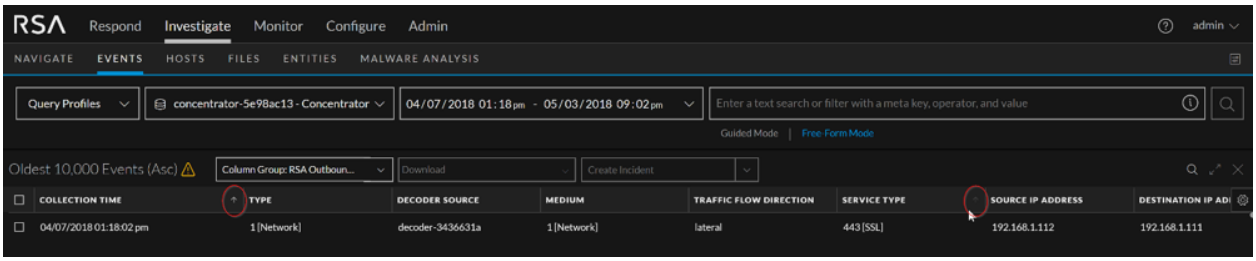
[イベント]ビューのカスタム列グループ

アナリストが調査で数千件のイベントを検査する時、標準提供またはカスタムの列グループを使用して、結果に配置するデータを調査シナリオに応じて選択できます。アナリストは、調査のパターンに応じて、列を手動で選択することもできます。選択した列をカスタム グループとして保存し、再利用できます。カスタム列グループは、全アナリスト共通で使用、編集できます。詳細は、『*Investigate ユーザ ガイド*』で「イベント リストでの列と列グループの使用」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



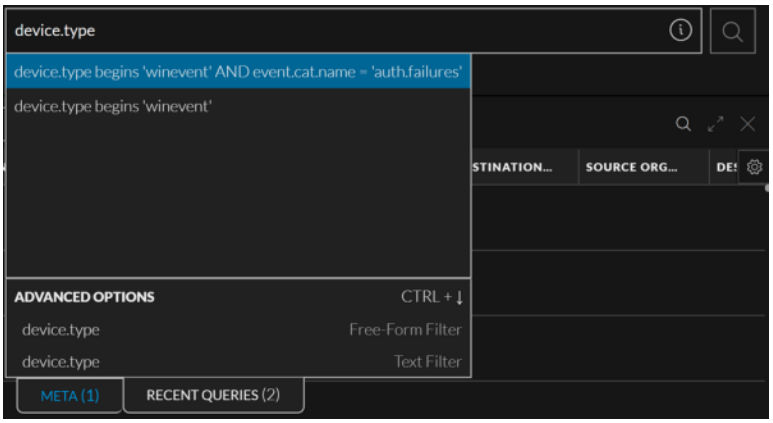
イベント リストの結果のソート

アナリストは[イベント]ビューにイベントを表示する際、ソート可能な列とソート方向を選択して、イベントをソートできます。イベント取得時は、デフォルトの収集時間(meta key = `time`) でソートされますが、その結果を別の列、例えばソースIPアドレス(meta key = `ip.src`) でソートし、同じ時間範囲に同じ接続のイベントがないか確認できます。詳細は、『*IInvestigate ユーザガイド*』で「イベント リストでの列と列グループの使用」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



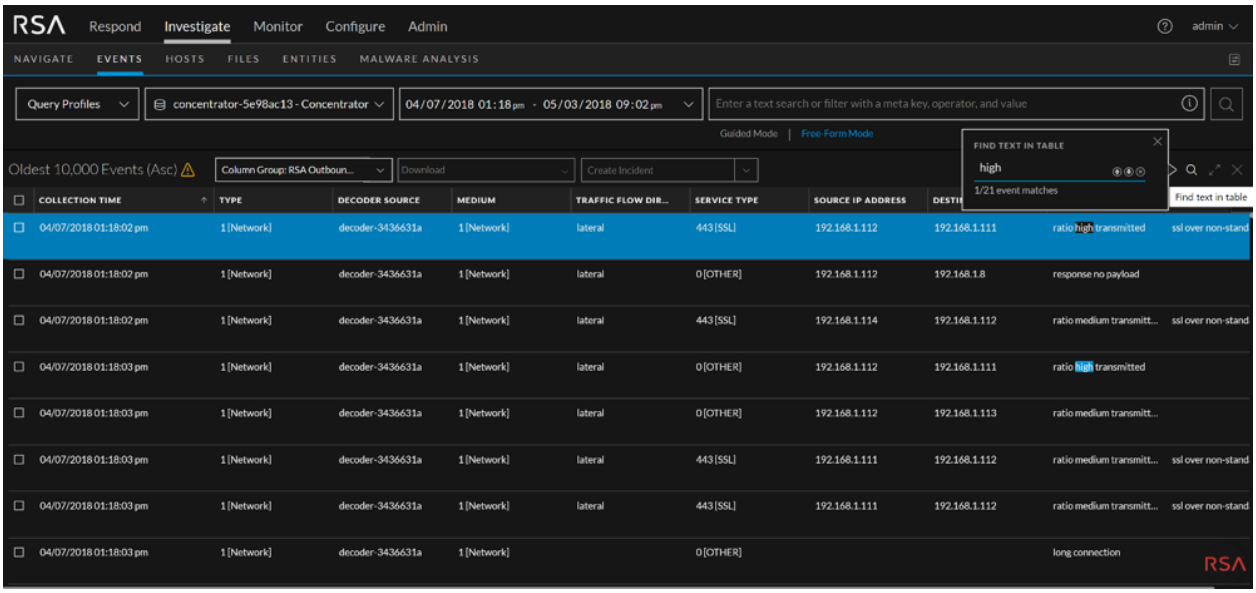
最近実行したクエリの使用により[イベント]ビューでのクエリ作成を補助

アナリストが効率的にクエリを作成できるよう、[イベント]ビューのクエリ バーに最近実行したクエリが表示されるようになりました。アナリストがクエリ バーにフィルタを入力する時、以前実行したクエリが候補として表示され、それらを使用してクエリを作成できます。候補のリストはアナリストの入力に沿って絞り込まれ、入力したテキストを含んだ、最も関連性の高いクエリから表示されます。クエリを選択すると、クエリ バーにフィルタとして追加され、必要に応じて編集できます。詳細は、『*IInvestigate ユーザガイド*』で「最近のクエリからのフィルタの挿入」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



[イベント]リスト内のテキスト検索と強調表示

クエリ結果に膨大なデータが含まれる場合、その中から情報を検索し、強調表示できるようになりました。この機能を使用すれば、フィルタを変更して再クエリで結果を絞り込む場合のように、前後のイベントの情報を失うことがありません。アナリストは、[イベント]リスト内の文字列を検索して強調表示し、キーボードのEnterキーを押して強調表示された文字列から文字列へ移動できます。詳細は、『*Investigate ユーザ ガイド*』で「[イベント]パネルでのテキスト文字列の検索」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



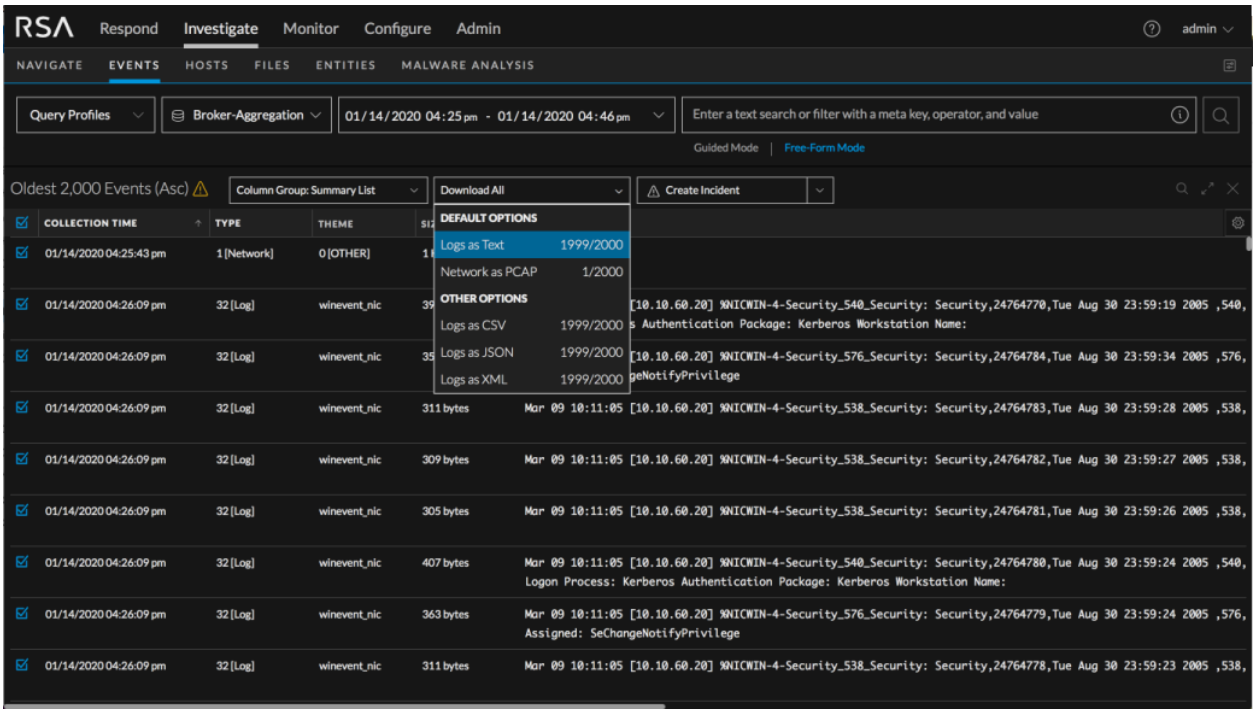
ガイド モードでの複雑なクエリ作成時の省略表記、数値範囲、括弧処理

クエリ バーのフィルタ自動入力機能が拡張され、数値範囲(`tcp.dstport=80-85`)、コンマを使用した複数の`OR`演算子[||]を含むクエリ(`src.port=0-1023, 1024-1050, 65535`)、値としてのIPv4またはIPv6サブネット指定(`10.0.0.0/8`)などの省略表記がサポートされるようになりました。また、マッピングされたエイリアス(`service = 'http'`)を数値(`service=80`)の代わりに使用できるようになりました。以前のバージョンでは、このような省略記号を使用して複雑なフィルタを作成する場合、自動入力機能のないフリー フォーム モードを使用する必要がありました。

更に、より簡単に、括弧を含むクエリを入力または貼り付けたり、複数のフィルタを括弧で囲んだり、有効な括弧を壊すことなく括弧を削除できるようになりました。フィルタを作成または編集する時、閉じていない括弧がないよう自動的にチェックされます。詳細は、『*Investigate ユーザ ガイド*』で「バージョン11.4のクエリ ビルダ」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

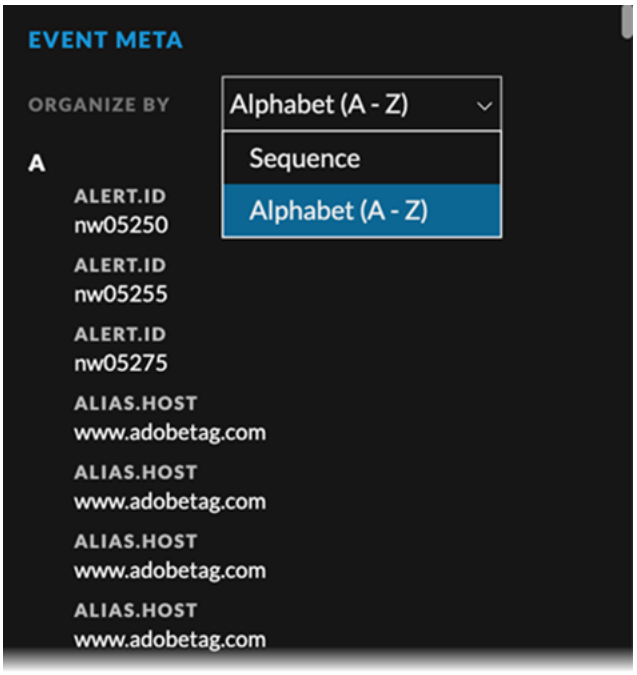
[イベント]ビューからのPCAP、メタ データ、ログのダウンロード

アナリストは[イベント]リストの任意のデータを抽出し、証拠として保存したり、より詳細な調査のために保存したりできます。単一のイベントまたは複数のイベントを選択し、RAWデータ(ログ、パケット)をダウンロードできます。詳細は、『*IInvestigate ユーザ ガイド*』で「[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。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



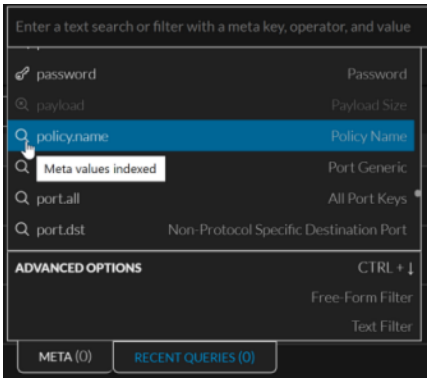
[イベント メタ]パネルのレイアウト変更

[イベント]ビューに表示される結果に関連するメタ データを確認する際、目的のメタ データがより簡単に見つかるよう、リストに表示されるメタ データの順番を変更できるようになりました。メタ データのリストは、より直感的になるようレイアウトが変更され、必要に応じてアルファベット順または出現した順で並べ替えできます。詳細は、『*Investigate ユーザ ガイド*』で「イベントの関連メタデータを表示する」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



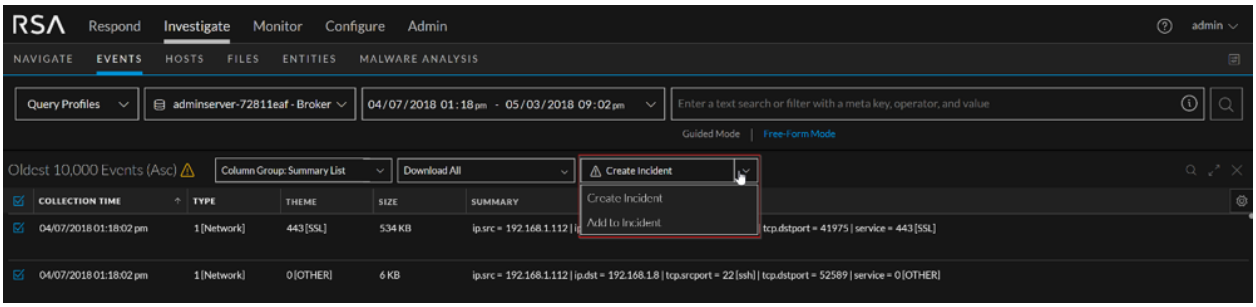
クエリの自動入力メニューにメタ キーのインデックス レベルを表示

クエリの作成時、各メタ データのインデックスがどのように定義されているかが表示されるため、アナリストは実行できるクエリのタイプと実行できないクエリのタイプを判断できます。ガイド モードの自動入力メニューには、メタ キーのインデックス レベルを示すアイコンも表示されます。詳細は、『*Investigate* ユーザ ガイド』で「ガイド モードでの視覚的なフィードバック」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



[調査]ビュー からのインシデント作成と編集

[イベント]ビューで調査する時、アナリストは、クエリ結果のイベントを新規または既存のインシデントに追加できます。一度に1000件のイベントを追加できるため、インシデントの証拠を追加するために[対応]ビューと[調査]ビューを往復する頻度が減り、ワークフローが改善されました。詳細は、『*IInvestigate* ユーザ ガイド』で「[イベント]ビューでのインシデントへのイベントの追加」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

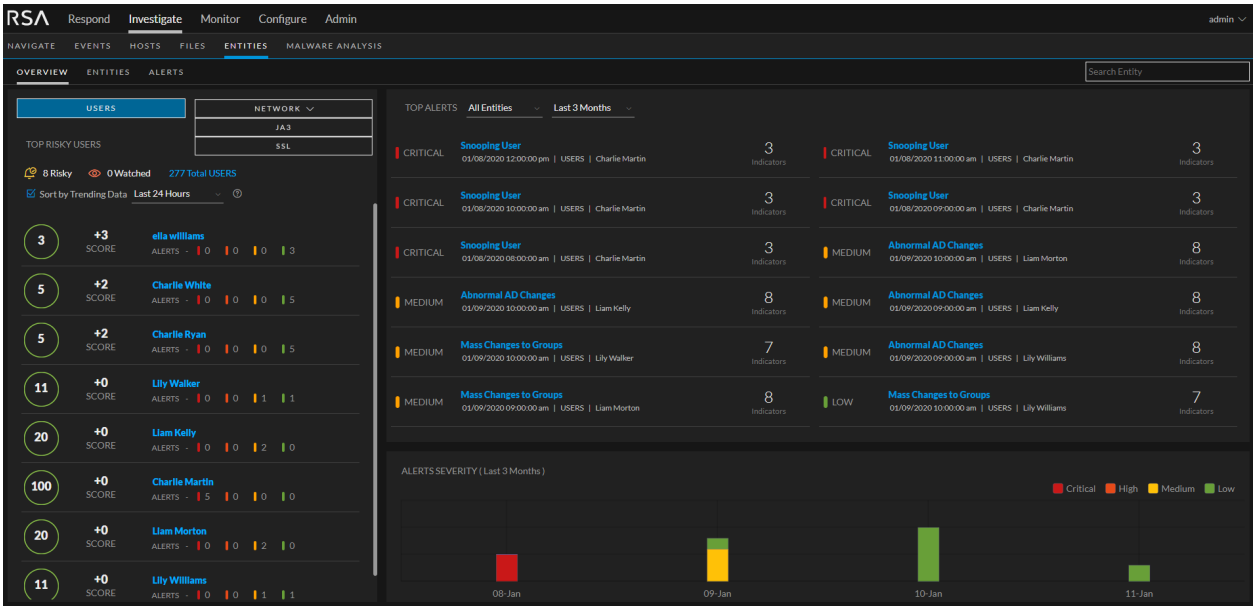


NetWitness UEBA

ネットワーク データを使用した高度な分析

UEBAは、ネットワーク モデルをサポートします。ネットワーク モデルは、ネットワーク(パケット) データを使用して、正当なHTTPSセッションの中に隠れた潜在的な悪意ある通信を検出します。特定のポート、ドメイン、組織、SSLサブジェクト宛てに送信される異常なアウトバウンド通信量など、ネットワークの様々な異常を検出できます。

新しく追加されたTLSデータ ソースは、JA3とSSLサブジェクトという2つの新しいエンティティをサポートし、データ窃取やフィッシングなどのアラート タイプに分類される異常を検出します。



エンティティ調査のフィルタ

UEBAユーザ インタフェースが機能拡張され、ユーザ エンティティ、ネットワーク エンティティを調査するアナリストにとってより使いやすくなりました。ユーザ エンティティ、ネットワーク エンティティに対する複数のフィルタ オプションの追加により、アナリストは調査対象の絞り込みができます。

トレンド データのサポート

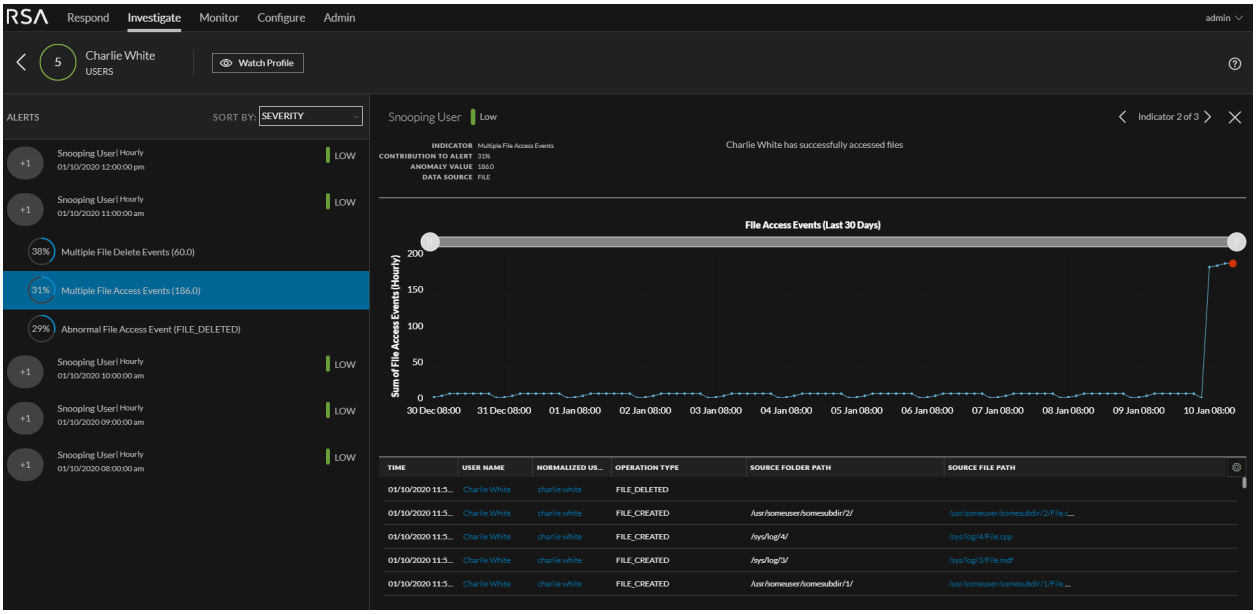
ダッシュボードにトレンド上位のエンティティが表示されるようになりました。トレンド データは、前日または前週のユーザ スコアまたはネットワーク スコアの増加を表します。

クイック ソート オプション

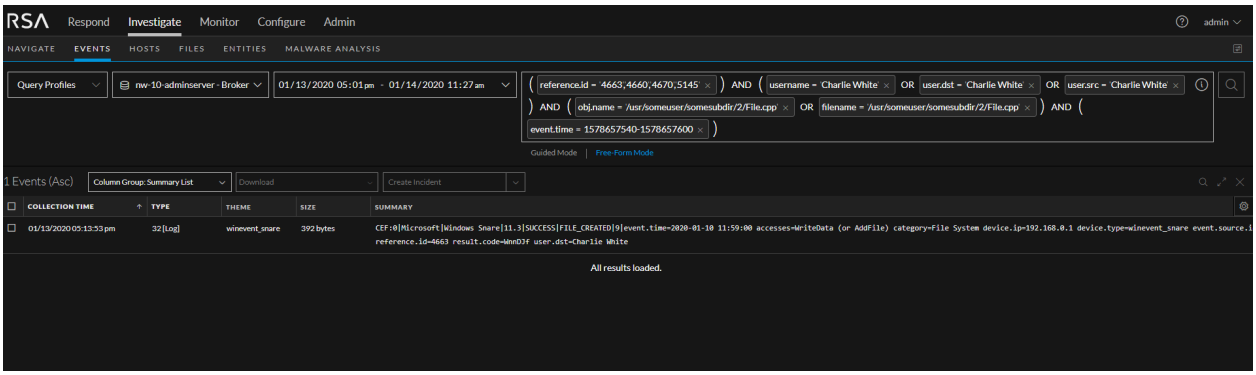
新しいフィルタが追加され、上位アラート データを、エンティティ タイプと期間によってフィルタできるようになりました。例えば、「全タイプ」、「ユーザ」、「JA3」、「SSL」のいずれかを選択し、「直近 24時間」、「直近 7日間」、「直近 1か月」、「直近 3か月」のいずれかの期間を選択して表示できます。

UEBAからイベントへの移行の改善

アナリストが脅威の詳細を調査するためにRAWイベントを表示できるよう、複数の移行オプションが追加されました。調査が簡単になるよう、アナリストにはインジケータに貢献したイベントのリストが表示されます。例えば、ユーザの調査をしたい場合は、[ユーザ名]列の下のユーザ名をクリックします。



選択したユーザのイベントの詳細が[**調査**]>[**イベント**]ビューに表示されます。



インシデント対応

ノード グラフの改善

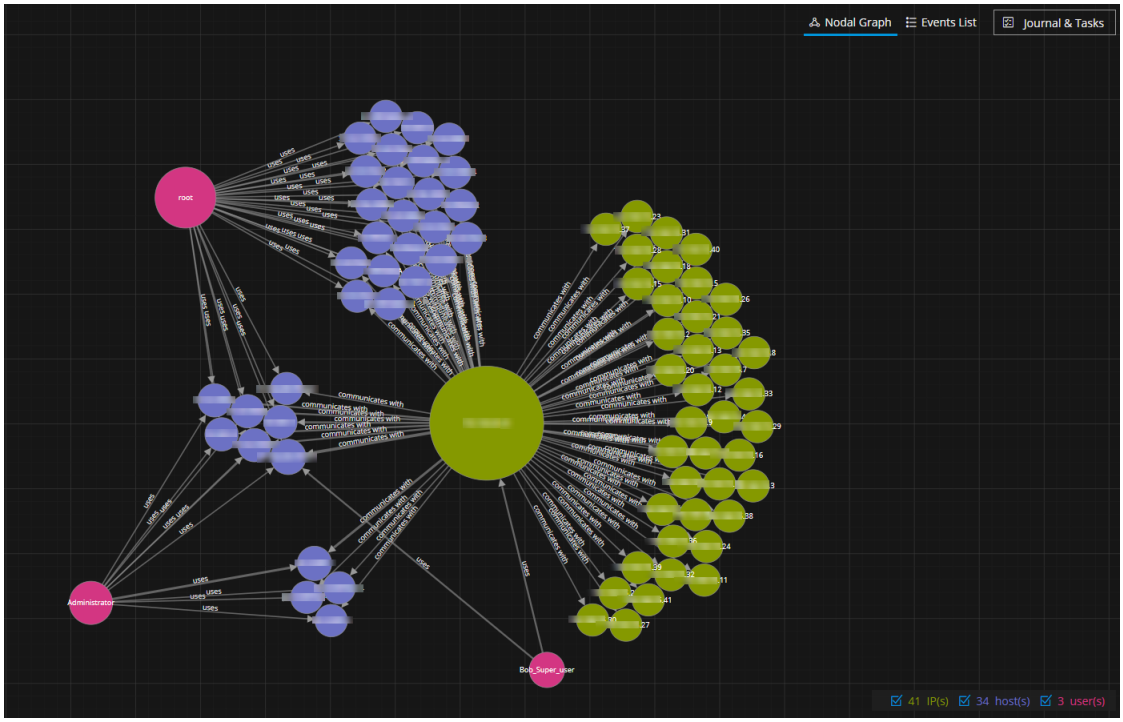
このリリースでは、アナリストが最低限の操作で初見からインシデントを理解できるようノード グラフが改善されました。

アナリストがインシデントに対応する時、次のような利点を提供します。

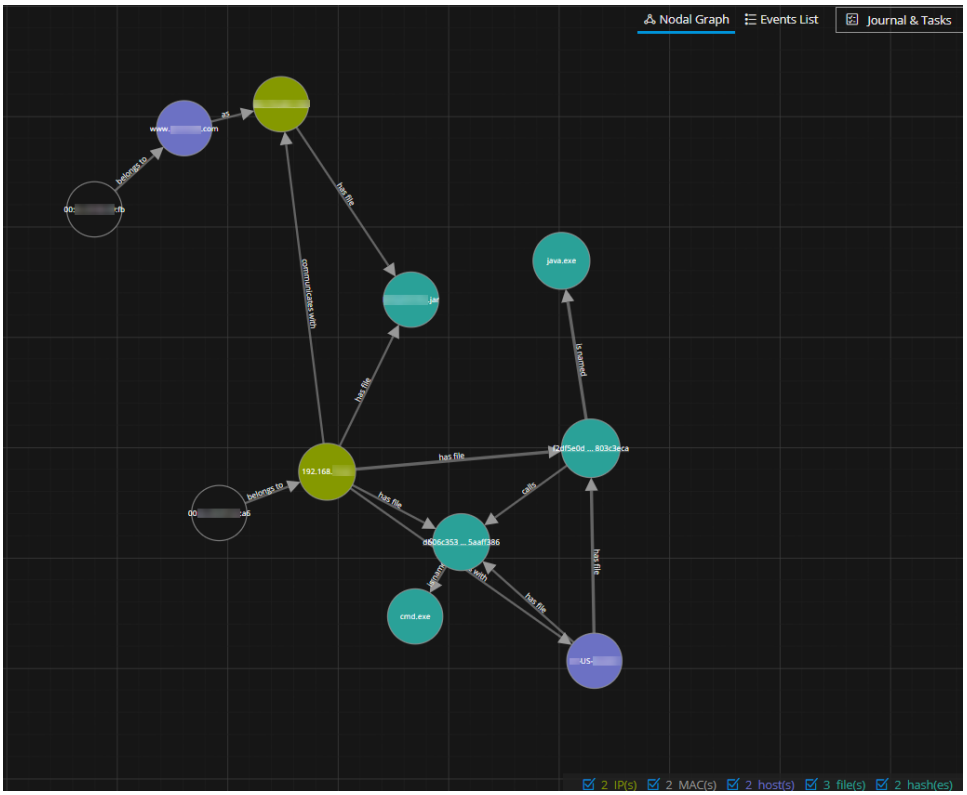
- ノード グラフは、対象となるデータセットの範囲、共通点、異常の特定を助け、アナリストの分析に有益なコンテキスト情報を提供します。
- 多くの場合、アナリストが追加の操作をしなくてもノード グラフの最初のレイアウトから有益な洞察を得ることができます。
- 最初のレイアウトで明確に理解できない場合や、異なる配置で表示してみたい場合は、少数のノードの位置をマウスのドラッグで調整すれば、新しいノード グラフ効果によって、より高速に、より洞察に満ちた関係性やクラスタが表示されます。以前のリリースでは、アナリストが見やすいレイアウトになるまで各ノードの位置を手動で調整できましたが、非常に時間がかかりました。

新しいノード グラフには次の動作と機能が追加されています。

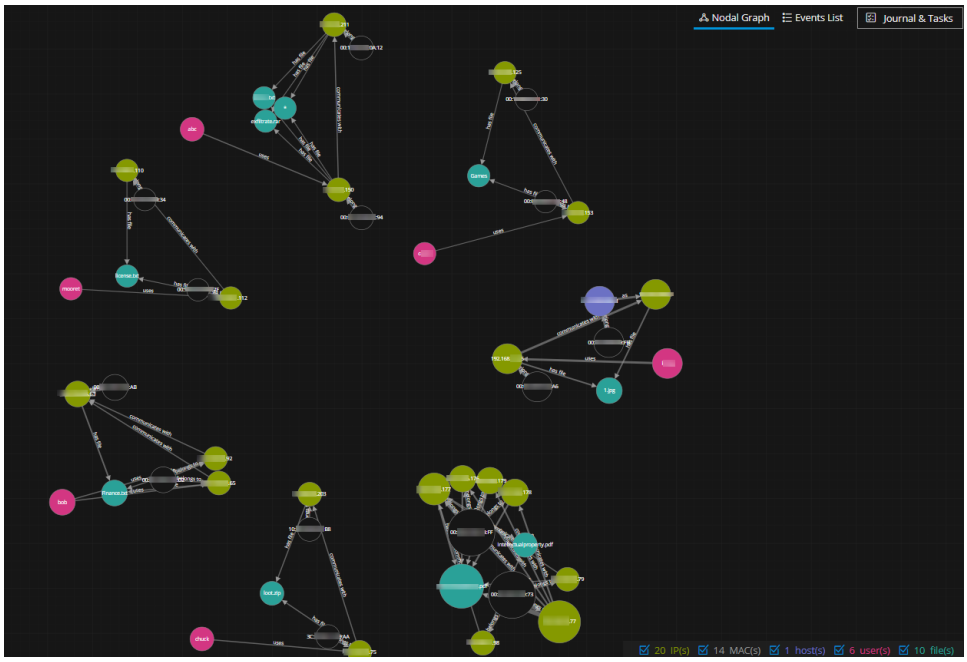
- 同じタイプのエンティティは、できるだけクラスタにまとめて配置されます。以前のリリースでは、エンティティのタイプ、関係、サイズに関係なく、すべてのノードが均等に配置されていました。



- 属性とアクションが区別しやすくなりました。属性を表す矢印("as"、"is named"、"belongs to"、"has file") は、アクションを表す矢印("call"、"communicates with") よりも短くなる傾向があります。



- 末端ノード(1つのエンティティと単一の関係しか持たないノード) は、相手エンティティに対してより大きな強調効果を持ちます。こうした2つのノードはできるだけ近接して配置されます。以前のリリースでは、強調効果が均等であったため、多くの関係が交差し、どのノードがどのノードと関係あるのかがわかりにくくなっていました。
- 関連のないグラフ(例えば、エンティティと関係で構成された各クラスタの間に関連がない場合など) は、離して配置されます。以前のリリースでは、関連のないグラフも1つにまとめて表示していたため、すべてのノード間に関係があるように見えていました。



ドラッグされたノードは、その場所に固定されます。ノードをダブルクリックすると固定が解除され、再度ノード効果が適用されるようになります。

アラート検索の改善

[アラート リスト]ビュー([対応]＞[アラート]) には、NetWitness PlatformのRespond Serverが受信したすべてのアラートが表示されます。このリストをアラート名でフィルタする機能が改善されました。例えば、特定のルールによって生成されたアラートを表示したい場合、フィルタにアラート名の一部を入力し、一致する候補の中からアラート名を選択してフィルタに指定することができます。以前のリリースのように、長いリストを上から下までスクロールする必要はありません。また、[フィルタ]パネルには、選択中のアラート名だけが表示されるため、選択中のアラート名を簡単に確認し、フィルタから削除することができます。

インシデント検索機能の改善

[インシデント リスト]ビュー([対応]＞[インシデント]) のフィルタが改善され、インシデント検索の時間を短縮できます。インシデントを検索する時、「INC-」プレフィックスを入力する必要がなくなりました。インシデント番号を入力するだけで検索できます。例えば、「INC-1050」を検索する場合は、「1050」と入力します。

対応のメール通知の改善

インシデント対応のメール通知に関連情報が追加されました。メール受信後、インシデントが更新されたのか新規作成されたのか、誰が変更したのかを知るために、NetWitness Platformにログインする必要がなくなりました。インシデント対応のメール通知には次の情報が追加されました。

- インシデントの新規作成と更新のメール通知をより簡単に区別できます。
- インシデントの新規作成と更新のメール通知の件名には、インシデントIDとインシデント名が追加されます。
- インシデントの新規作成と更新のメール通知の本文では、インシデントを新規作成または更新したユーザとインシデント担当者の情報を確認できます。

インシデント ルールのエクスポートとインポート

[インシデント ルール]ビュー([構成]＞[インシデント ルール]) から、インシデント ルールをエクスポートおよびインポートできるようになりました。インシデント ルールをエクスポートし、同じリリース バージョンの別のNetWitness Serverとインシデント ルールを共有することができます。エクスポートしたインシデント ルールは、ZIPファイル形式で、2つのJSONファイル(1つはインシデント ルール、もう1つはインシデント ルール スキーマ) が含まれます。上級ユーザは、必要に応じて、エクスポートされたZIPファイルのインシデント ルールを編集できます。

詳細クエリ モードのインシデント ルールはエクスポートできません。ルール ビルダを使用して作成されたインシデント ルールのみエクスポートできます。

詳細は、『*NetWitness Respond Configuration Guide*』を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

一度に複数のインシデント ルールを有効化／無効化

インシデント ルールを素早く有効化または無効化するため、SOCマネージャとアナリストは、[インシデント ルール]ビュー([構成]＞[インシデント ルール]) で複数のインシデント ルールを選択できるようになりました。以前のリリースでは、各インシデント ルールの詳細にアクセスし、1度に1つのインシデント ルールしか有効化できませんでした。

インシデントへのアクセス制限

デフォルトでは、[対応]ビューへのアクセス権を持つすべてのユーザが、すべてのインシデント、アラート、タスクを表示することができます。インシデントへのアクセス制限を有効化すると、制限されたユーザは自身のインシデントとアラート、自身のインシデントに関連付けられたタスクのみを表示できます。インシデントへのアクセス制限は、[管理]＞[セキュリティ]＞[設定]タブで構成できます。

この制限に関する詳細は、『*System Security and User Management Guide*』または『*NetWitness Respond Configuration Guide*』で「Restrict Access to Incidents」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

Health and Wellness(BETA)

Health and Wellness(BETA) は、ホストとサービスのパフォーマンスやリソース利用率などを監視するための最新、強力、シンプルなソリューションです。優れたグラフ機能を提供し、大規模なNetWintess導入環境における重要なホストやサービスの異常を簡単にアラートや通知で知らせることができます。11.4では、専用の仮想ホストのみにHealth and Wellness Search(BETA) を導入できます。

注： 11.4ではベータ版として提供され、完全な機能は実装されていません(例えば、Kibanaの認証が統合されていない、アラートを出力アクションに送信できないなど) 。

Health and Wellness(BETA) は次のような機能を提供します。

1. インタラクティブなグラフを使用したダッシュボード
2. カスタマイズ コンテンツ(グラフ、アラート、ダッシュボードなど) を簡単に作成可能
3. データに関するアラートとアラート条件のカスタマイズ

Kibanaユーザ インタフェース(UI) には大量のメトリックを簡単に表示することができ、管理者はリアルタイムのHealth and Wellnessグラフを動的に作成することができます。

ダッシュボード、インタラクティブ グラフなどの組み込みコンテンツの利用により、迅速に監視を構成できます。詳細は、『*System Maintenance Guide*』で「Monitor Health and Wellness Beta Using Kibana UI」を参照してください。導入手順については、『*Deployment Guide*』で「Deployment Options, Health & Wellness Search (Beta Version for Standalone Virtual Host Only)」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

Health and Wellness(BETA) に関するフィードバックは、nw.health.wellness.feedback@rsa.comにお送りください。

エンドポイントの調査

感染したホストをネットワークから隔離

アナリストは、マルウェアへの感染が疑われるホストをネットワークから隔離することにより、高度な調査を実行し、攻撃の広がりを制御することができます。アナリストは、脅威がアクティブな間に、安全にマルウェアの動作を調査することができます。隔離状態のホストでは、すべてのイベントがEndpoint Serverに報告され、ホスト上のアクティビティは完全に可視化されたままです。詳細は、『*NetWitness Endpoint User Guide*』で「Isolating Hosts from Network」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

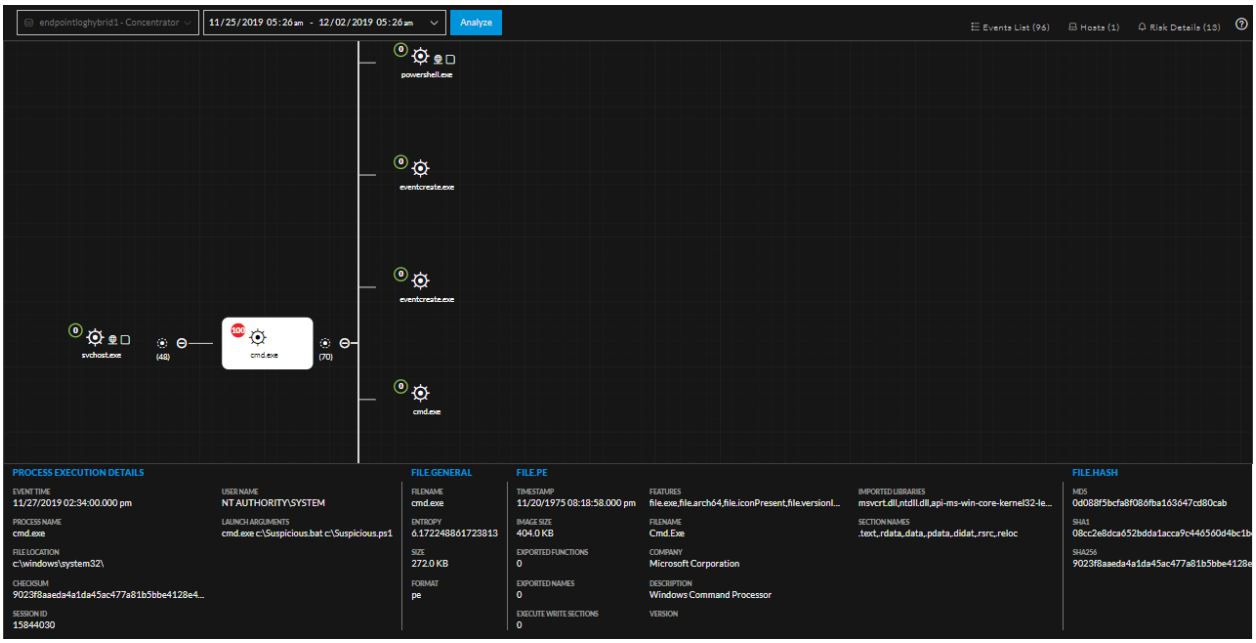
高度なフォレンジック調査

マルウェアへの感染が疑われるホストがある場合、アナリストはそのホストからマスター ファイル テーブル(MFT) をダウンロードして、より高度なフォレンジック調査を実行することができます。例えば、ホストにログインすることなく、攻撃の時間帯に作成されたファイルを検索したり、ファイル名のパターンを検索したりすることができます。また、MFT内の疑わしいファイルをダウンロードして、さらに詳しく調査することもできます。

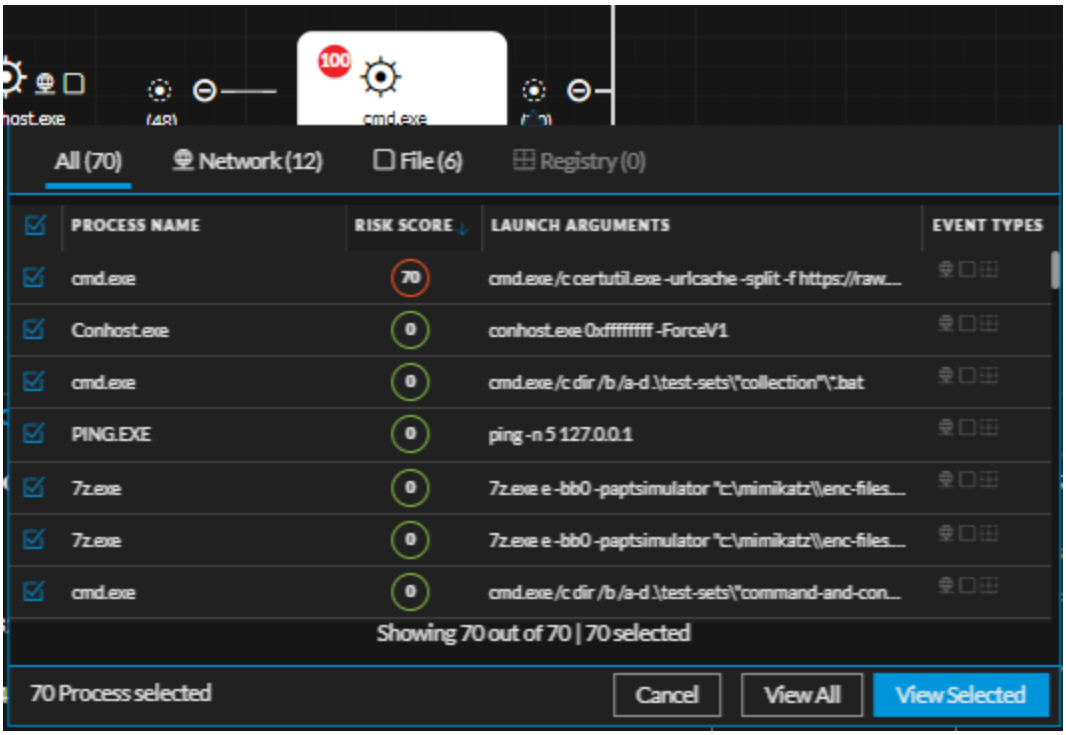
ホスト上の疑わしいプロセスのフォレンジック調査のため、アナリストはプロセスまたはシステムのダンプをダウンロードすることができます。詳細は、『*NetWitness Endpoint User Guide*』で「Performing Host Forensics」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

プロセス分析の利便性向上

アナリストのワークフローをより簡単かつ直感的にするため、プロセス ビューアにより多くのコンテキスト情報(関連するイベント、プロセスが存在するホスト、リスクの詳細など) が表示されるようになりました。アナリストは、各ノードのリスク スコア、イベント タイプ(ネットワーク、ファイル、または、レジストリ) 、プロセスの詳細な実行情報、ファイル プロパティを表示できます。


endpointloghybrid1 - Concentrator
11/25/2019 05:26 am - 12/02/2019 05:26 am
Analyze
Events List (96)
Hosts (1)
Risk Details (13)
powershell.exe
eventcreate.exe
eventcreate.exe
cmd.exe
svchost.exe
(48)
cmd.exe
(70)
PROCESS EXECUTION DETAILS
EVENT TIME
11/27/2019 02:34:00.000 pm
USER NAME
NT AUTHORITY\SYSTEM
PROCESS NAME
cmd.exe
LAUNCH ARGUMENTS
cmd.exe c:\Suspicious.bat c:\Suspicious.ps1
FILE LOCATION
c:\windows\system32\
CHECKSUM
9023f8aaeda4a1da45ac477a81b5bbe4128e4...
SESSION ID
15844030
FILE.GENERAL
FILENAME
cmd.exe
ENTROPY
6.172248861723813
SIZE
272.0 KB
FORMAT
pe
FILE.PE
TIMESTAMP
11/20/1975 08:18:58.000 pm
IMAGE SIZE
404.0 KB
EXPORTED FUNCTIONS
0
EXPORTED NAMES
0
EXECUTE WRITE SECTIONS
0
FEATURES
file.exe,file.arch64,file.iconPresent,file.versionI...
FILENAME
Cmd.Exe
COMPANY
Microsoft Corporation
DESCRIPTION
Windows Command Processor
VERSION
IMPORTED LIBRARIES
msvcrt.dll,ntdll.dll,api-ms-win-core-kernel32-le...
SECTION NAMES
.text,.rdata,.data,.pdata,.didat,.rsrc,.reloc
FILE.HASH
MD5
0d088f5bcfa8f086fba163647cd80cab
SHA1
08cc2e8dca652bdda1acca9c446560d4bc1b
SHA256
9023f8aaeda4a1da45ac477a81b5bbe4128e

調査が多方向に分散することを防ぐため、イベント タイプにより子プロセスの範囲を狭め、必要なプロセスだけを詳細に調査することができます。詳細は、『*NetWitness Endpoint User Guide*』で「Investigating a Process」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。



ホスト数集計の利便性向上

アナリストのワークフローをより簡単かつ直感的にするため、ファイルのホスト数集計機能が向上しました。[On Hosts(ホスト数)]列で並べ替えとフィルタができるようになり、各ファイルが存在するホスト数を比較できます。ファイルが存在するホスト数が少ないほど、詳細な調査の必要性が高くなります。

[ホスト]ビューと[ファイル]ビューでは、[**Active On**(存在する場所)]列の名前が[**On Hosts**(ホスト数)]列に変更されました。

詳細は、『*NetWitness Endpoint User Guide*』で「Investigating Files」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

REST APIの追加

Security Orchestration Automation and Response(SOAR)機能の拡張と、NetWitness Endpointのサードパーティ アプリケーションとの統合のため、新しいAPIが追加されました。新しいAPIには、システム ダンプのダウンロード、プロセス ダンプのダウンロード、ネットワーク隔離をリクエストするAPIが含まれます。詳細は、『*NetWitness Platform API User Guide*』を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

ホストの詳細のフィルタ

大量のファイルのリストにフィルタを設定しないまま分析を続けると、ユーザ インタフェースの操作が煩わしくなり、必要以上に時間もかかります。ファイルをより短時間で分析できるよう、ファイル名、プロセス名、ファイル ステータス、レピュテーション、署名、リスク スコアなどのフィルタを設定し、ホストの詳細ページに表示されるファイルを絞り込むことができます。詳細は、『*NetWitness Endpoint User Guide*』で「Investigating Hosts」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

ファイル自動ダウンロードのサポート

アナリストがより詳細な分析を行い、疑わしいファイルを特定できるよう、ファイルが自動的にダウンロードされます。自動的にダウンロードするファイルの数を制限するため、条件に合致したファイルのみがダウンロードされるようポリシーを構成できます。デフォルトでは、署名がなく、1 MB未満のファイルのみがダウンロードされます。詳細は、『*NetWitness Endpoint Configuration Guide*』で「Creating Groups and Policies」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

エンドポイントの構成

エンドポイント エージェントによるログ ファイル収集

エージェントは、Endpoint Detection and Response(EDR) 機能とWindowsログ収集に加えて、ログ ファイル収集(収集プロトコルとしてファイル収集を使用するイベント ソースからの収集) をサポートするようになりました。この収集方式は、サポート対象のイベント ソース タイプのホストから一元管理のためにログを収集する場合の推奨方式になります。SFTPからこの収集方式への切り替えは、非常に簡単です。詳細は、『*NetWitness Endpoint Configuration Guide*』で「Replace Windows SFTP Agents」を参照してください。SFTPエージェントは、引き続きサポートされますが、将来的にはサポート対象外になります。

現在サポートされているイベント ソース タイプの一覧は、『*NetWitness Endpoint Configuration Guide*』で「Currently Supported File Log Event Source Types」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

エンドポイント エージェントのサポート対象OSバージョンの追加

11.3のサポート対象のオペレーティング システムのバージョンに加え、次のバージョンがサポートされます。

- macOS 10.15 Catalina
- CentOS 8.x
- Red Hat Enterprise Linux 8.x
- Windows 10 version 1909

詳細は、『*NetWitness Endpoint Agent Installation Guide*』を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

Broker、Concentrator、Decoder、Log Decoderサービス

10G環境でのBerkeley Packet Filter(BPF) サポート

10G環境のDecoderでBerkeley Packet Filtersを使用できるようになりました。これにより、パケットやログの処理、特に高速パケット キャプチャ処理がより効率的に管理されます。詳細は、『*Decoder and Log Decoder Configuration Guide*』で「(Optional) Configure System-Level (BPF) Packet Filtering」と「Configure 10G Capability」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

IPv4インデックスでのCIDR範囲の最適化

コア データベースのIPv4データ タイプのインデックスでは、一般的な/8、/16、/24のサブネット サイズについて、CIDR範囲のインデックスが自動的に作成されるようになりました。これにより、これらのCIDR範囲を検索するクエリ処理の時間が大幅に短縮されます。

HTTP/2セッションの可視化

HTTP/2ストリームのヘッダーから取得したメタ データを検索し、HTTP/2セッションを可視化することができます。詳細は、『*Decoder Configuration Guide for RSA NetWitness Platform*』で「HTTP Parsers」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

Event Stream Analysis(ESA)

データ プライバシー保護のため、全アラート出力から機微情報のメタ キーを削除可能に

データ プライバシー保護のため、データ ソースに関係なく、すべてのアラート出力から機微情報を含むメタ キーを削除できるようになりました。ESA Correlationサービスでは、機微情報を含むメタ キーを`global-private-fields`パラメータに追加することにより、すべてのアラートの出力から削除することができます。詳細は、『*ESA Configuration Guide*』で「How to Remove Sensitive Meta Keys from Global Alerts」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

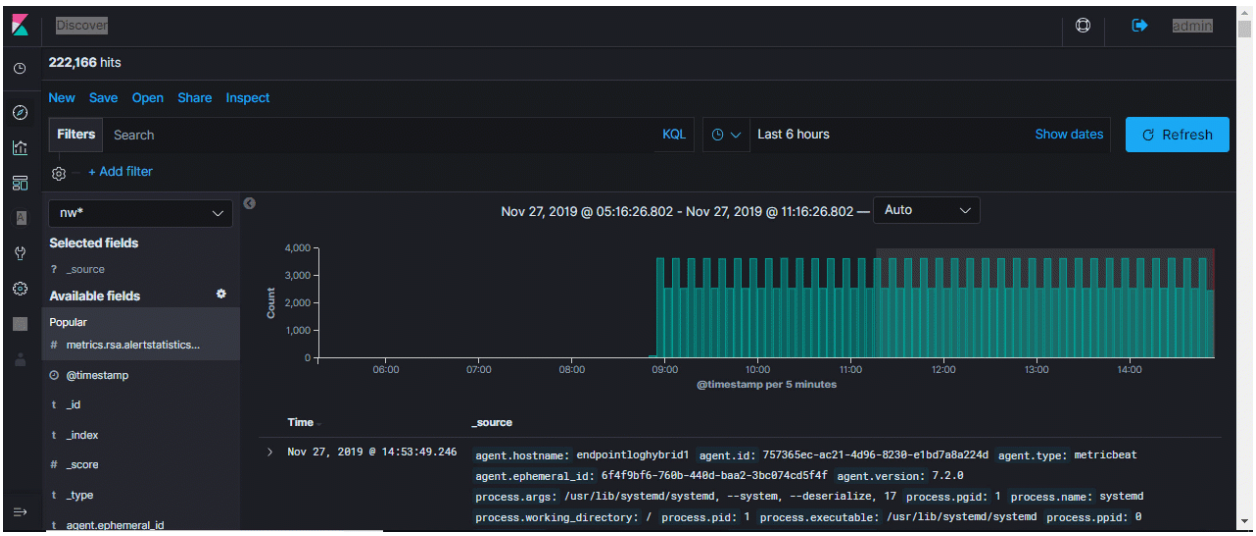
Esperバージョンを 7.1.0から 8.2.0に更新

NetWitness Platformバージョン11.4のESA Correlationは、Esperバージョン 8.2.0をサポートします。

ログ収集

NetWitness Platform UIからインポートされたSyslog RFC-5424ログのエクスポート

RAWログを保存する時に、RFC-5424の転送フォーマットが維持されます。



フォーマットが維持されるため、元々のソースと収集コンテキストを使用して、これらのログをリプレイでき、NetWitness Platformはログの本当の送信元を正確に反映できます。

ログ統計のパフォーマンス向上

11.4では、NetWitnessがアイドル状態のイベント ソースを除外するため、Log Decoderから送信されるイベント ソース数の統計が減少します。[イベント ソース]の[管理]タブには、こうしたアイドル状態のイベント ソースも引き続き表示されますが、ストレージ領域やログへのアクセスには影響しません。

管理と構成

シングル サイン オン認証

管理者のNetWitness Platformでの認証を簡略化するため、シングル サイン オンがサポートされます。NetWitness Platformは、IDプロバイダ(IDP) としてActive Directory Federation Services(ADFS) をサポートし、シングル サイン オンのプロトコルとしてSAML 2.0を使用します。詳細は、『*System Security and User Management Guide*』で「Configure Single Sign-On」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

SSOを使用すると、NetWitnessユーザは初回の認証に成功すれば、毎回ログインを要求されなくなります。

構成メニューの改善

[構成]タブのメニューが変更されました。アナリストおよびその他のRSA NetWitness Platformユーザには次の利点があります。

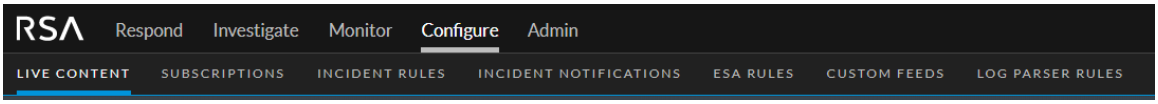
- [**Respond Notifications**(対応の通知)]は[**Incident Notifications**(インシデント通知)]に名前が変更されました。インシデントの通知しか関係しないためです。
- [**Live Content**(Live コンテンツ)]と[**Subscriptions**(サブスクリプション)]を隣に配置しました。サブスクリプションするのは、Live経由のコンテンツのみであるためです。

以前の[構成]タブのサブメニューの順番

Live Content | Incident Rules | Respond Notifications | ESA Rules | Subscriptions | Custom Feeds | Log Parser Rules

新しい[構成]タブのサブメニューの順番

Live Content | Subscriptions | Incident Rules | Incident Notifications | ESA Rules | Custom Feeds | Log Parser Rules



アナリスト用ユーザ インタフェース(UI) 分散のため複数NW Serverをサポート

アナリストの利用を目的として、複数のNetWitness Platform UIのインスタンスを導入できるようになりました。Analyst UIインスタンスは、地理的に離れた拠点に導入できます。NW Serverホスト上のプライマリUIのみにアクセスする場合と比較して、遅延の削減、パフォーマンス向上などの効果を期待できます。

Analyst UIのインスタンスまたはホストは、他のNetWitnessコンポーネント ホストと同じ方法で導入できます。

機能と制限事項

Analyst UIホストは次の機能を提供します。

- 組織の特定のグループ(例えば、Americas、EMEA、APAC、Tier 1 Analysts、Tier 3 Analystsなど) に導入します。
- Analyst UIホストを地域ごとに導入する場合、その地域のBrokerに直接クエリを発行できるため、プライマリUI経由でアクセスする場合に比べ遅延が少ない。
- プライマリUIの負荷軽減
- 自身のReporting Engine(RE)
- 計画的または計画外の理由で利用不可になった場合、プライマリUIおよび他のAnalyst UIインスタンスに影響しない
- プライマリUIと同じプレクエリフィルタ検証、データ プライバシー保護、RBAC機能を提供
- 認証と構成はプライマリNW Serverに移動
- 管理機能にはアクセスできない。すべての管理機能はプライマリUIで実行。
- コンテンツ(ESAルール、アプリケーション ルール、フィード) の作成、管理はできない。すべてのコンテンツの作成、管理はプライマリUIで実行。

導入手順の詳細については、『*Deployment Guide*』で「Deployment Options, Analyst User Interface」を参照してください。ダッシュボードの詳細については、『*Getting Started Guide*』で「Dashboards in the Analyst User Interface」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

NetWitnessサイレント インストール機能

管理者は、迅速に環境を構築するため、NetWitnessのインストールを自動化したい場合があるかもしれません。`-silent`コマンドを`nwsetup-tui`スクリプトに指定することにより、入力プロンプトが表示されることなく、インストールを実行できるようになりました。スクリプトのプロンプトへの応答は、あらかじめコマンドラインに指定しておくことにより、ホストのインストールを自動化できます。

保存用に最適化された新しいLog Hybrid

11.4では、保存用に最適化された新しいLog Hybridのオプション(シリーズ6E Hybridのみで利用可) が追加されました。次のような最適化が行われています。

- RAWログとメタの圧縮を有効化
- Decoderのインデックスを有効化することにより、メタ キャッシュ ボリュームの必要性を無くし、使用可能な容量として割り当て
- 複数のRAIDグループを単一のRAID 6構成に統合

保存用に最適化されたLog Hybridは、他のNetWitness Hybridホストと同じ方法で導入できます。

シリーズ6 Analyticsハードウェア(旧 : ESA物理ホスト) へのNW Server導入

シリーズ6 AnalyticsハードウェアにNW Serverホストを導入できるようになりました。シリーズ6 Analyticsハードウェアは、NW Serverを通常導入する標準のコア アプライアンスよりも、メモリとストレージの容量が大きくなっています。このため、全体的に応答が早く、Report Engine用のストレージ領域も増やせます。

既存のLog DecoderホストへのEndpoint Serverのインストール

11.4では、既存のLog DecoderホストにEndpoint Serverをインストールできます。詳細は、『*Physical Host or Virtual Host Installation Guides*』で「Install an Endpoint Service Category on an Existing Log Decoder」を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧を、「総合目次」で確認できます。

アップグレードの改善

アップグレード後のリフレッシュ前にRespondサービスの正規化スクリプトを自動バックアップ

カスタマイズしたRespondサービスの正規化スクリプトを手動でバックアップする必要がなくなりました。以下のRespondサービスの正規化スクリプトは自動的に、**/var/lib/netwitness/respond-server/scripts.bak-<timestamp>**ディレクトリ(**<timestamp>**は、バックアップが完了した時間) にバックアップされます。

```
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_ueba_alerts.js
normalize_wtd_alerts.js
utils.js
```

カスタマイズしたファイルが将来上書きされることを避けるため、NetWitness Platform 11.4以降ではカスタムの正規化スクリプトを利用できます。正規化スクリプト ファイルをカスタマイズした場合、ファイル名の先頭にプリフィックスとして「custom」を付加します(**custom_normalize_<alert type>.js**) 。

```
custom_normalize_alerts.js
custom_normalize_core_alerts.js
custom_normalize_ecat_alerts.js
custom_normalize_ma_alerts.js
custom_normalize_ueba_alerts.js
custom_normalize_wtd_alerts.js
```

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。

セキュリティ修正

追跡番号	説明
ASOC-86436	CentOS 7 kernel security update (Important) - https://access.redhat.com/errata/RHSA-2019:3834
ASOC-86435	CentOS 7 kernel security update (Important) - https://access.redhat.com/errata/RHSA-2019:3872
ASOC-85738	CentOS 7 sudo security update (Important) - https://access.redhat.com/errata/RHSA-2019:3197
ASOC-85372	CentOS 7 java-11-openjdk security update (Important) - https://access.redhat.com/errata/RHSA-2019:3127
ASOC-85371	CentOS 7 java-1.8.0-openjdk security update (Important) - https://access.redhat.com/errata/RHSA-2019:3128
ASOC-85296	CentOS 7 kernel security and bug fix update (Important) - https://access.redhat.com/errata/RHSA-2019:3055
ASOC-85267	CentOS 7 libcgroup security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2047
ASOC-85266	CentOS 7 libjpeg-turbo security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2052
ASOC-84843	CentOS 7 kernel security update (Important) - https://access.redhat.com/errata/RHSA-2019:2829
ASOC-84228	CentOS 7 libmspack security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2049
ASOC-83893	CentOS 7 kernel security, bug fix, and enhancement update (Important) - https://access.redhat.com/errata/RHSA-2019:2029
ASOC-83892	CentOS 7 pango security update (Important) - https://access.redhat.com/errata/RHSA-2019:2571
ASOC-83891	CentOS 7 httpd security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2343
ASOC-83890	CentOS 7 kernel security and bug fix update (Important) - https://access.redhat.com/errata/RHSA-2019:2600
ASOC-82840	CentOS 7 glibc security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2118

追跡番号	説明
ASOC-82839	CentOS 7 elfutils security, bug fix, and enhancement update (Low) - https://access.redhat.com/errata/RHSA-2019:2197
ASOC-82838	CentOS 7 dhcp security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2060
ASOC-82837	CentOS 7 curl security and bug fix update (Low) - https://access.redhat.com/errata/RHSA-2019:2181
ASOC-82836	CentOS 7 binutils security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2075
ASOC-82835	CentOS 7 bind security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2057
ASOC-82834	CentOS 7 libssh2 security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2136
ASOC-82833	CentOS 7 libtiff security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2053
ASOC-82832	CentOS 7 Xorg security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2079
ASOC-82831	CentOS 7 linux-firmware security, bug fix, and enhancement update (Important) - https://access.redhat.com/errata/RHSA-2019:2169
ASOC-82830	CentOS 7 mariadb security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2327
ASOC-82829	CentOS 7 nss, nss-softokn, nss-util, and nspr security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2237
ASOC-82828	CentOS 7 ntp security, bug fix, and enhancement update (Low) - https://access.redhat.com/errata/RHSA-2019:2077
ASOC-82827	CentOS 7 openssh security, bug fix, and enhancement update (Low) - https://access.redhat.com/errata/RHSA-2019:2143
ASOC-82826	CentOS 7 openssl security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2304
ASOC-82825	CentOS 7 polkit security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2046
ASOC-82824	CentOS 7 procps-ng security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2189
ASOC-82823	CentOS 7 python security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2030
ASOC-82822	CentOS 7 python-requests security update (Low) - https://access.redhat.com/errata/RHSA-2019:2035

追跡番号	説明
ASOC-82821	CentOS 7 python-urllib3 security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2272
ASOC-82820	CentOS 7 rsyslog security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2110
ASOC-82819	CentOS 7 samba security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2099
ASOC-82818	CentOS 7 systemd security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2091
ASOC-82817	CentOS 7 unixODBC security update (Moderate) - https://access.redhat.com/errata/RHSA-2019:2336
ASOC-82816	CentOS 7 unzip security update (Low) - https://access.redhat.com/errata/RHSA-2019:2159
ASOC-72421	CentOS 7 bind security update (Moderate) https://access.redhat.com/errata/RHSA-2019:0194
ASOC-72419	CentOS 7 systemd security update (Low) - https://access.redhat.com/errata/RHSA-2019:0201
ASOC-72418	CentOS 7 kernel security, bug fix, and enhancement update (Important) - https://access.redhat.com/errata/RHSA-2019:0163
ASOC-70086	CentOS 7 samba security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3056
ASOC-70079	CentOS 7 kernel security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3651
ASOC-69381	CentOS 7 libmspack Security Update (Low) - https://access.redhat.com/errata/RHSA-2018:3327
ASOC-69302	CentOS 7 fuse Security Update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3324
ASOC-69297	CentOS 7 openssl Security Update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3221
ASOC-69294	curl and nss-pem security and bug fix update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3157
ASOC-68872	GNOME security, bug fix, and enhancement update (Moderate) - https://access.redhat.com/errata/RHSA-2018:3140
ASOC-68844	X.org X11 security, bug fix, and enhancement update (Low) - https://access.redhat.com/errata/RHSA-2018:3059
ASOC-68833	CentOS 7 xorg-x11-server Security Update (Important) - https://access.redhat.com/errata/RHSA-2018:3410

追跡番号	説明
ASOC-67478	CentOS 7 xorg-x11-server Security Update (Moderate) - https://lists.centos.org/pipermail/centos-announce/2018-October/023075.html
ASOC-59640	CentOS 7 python Security Update (Moderate) - https://access.redhat.com/errata/RHSA-2018:2123

ログ収集の修正

追跡番号	説明
ASOC-82596	**問題**:プラグインの変換パラメータ `<includeNullValueParameters>` が、Nullトークンを空の文字列に置換しませんでした。 Transform XMLファイルにパラメータを追加しました。このファイルは、プラグインの作成と構成を行うためのファイルです。新しいパラメータは、"includeEmptyValueParameters"です。このパラメータを**TRUE**に設定すると、変換後の出力に、値が空のパラメータや空のリストが含まれます。デフォルトの**FALSE**に設定すると、空のパラメータは変換後の出力から削除されます。 また、既存の"includeNullValueParameters"は正しく動作するよう更新されました。更新前は、このパラメータにより値が空のパラメータが不正に出力に追加されたり、削除されており、Null値のパラメータに対しては何もしませんでした。更新後は、このパラメータを**TRUE**に設定するとNullトークンの項目を変換後の出力に追加し、デフォルトの**FALSE**に設定すると、出力からNull値のパラメータを削除します。

Event Stream Analysis(ESA) の修正

追跡番号	説明
ASOC-87267	**問題**:[サービス]ビューで無効化した評価版のESAルールが、アップグレード後に有効化されました。 この問題は修正されました。修正前は、アップグレード後や再導入した時に、評価版のESAルールのステータスが変更される場合がありました。NetWitness Platform 11.4では、評価版のESAルールのステータスがアップグレード後や導入時に変更されることはありません。例えば、評価版ルールを無効化し([構成]>[ESAルール]>[サービス]タブ) 、導入環境に再導入([構成]>[ESAルール]>[サービス]タブ) しても、評価版ルールは無効化されたままです。

管理の修正

追跡番号	説明
ASOC-86557 ASOC-87065	ポリシーに[発行日]を指定していないと[発行日]が毎日更新されるため、スキャン スケジュールが毎日開始していました。
ASOC-59607	Syslogサーバの構成を更新すると、`rsa-audit-server-output.conf` ファイルに重複したエントリーが作成されました。
ASOC-59240	監査ログに、Common Event Format (CEF) テンプレートを適用すると、メタ値のバック スラッシュ(または、円マーク) 文字(“¥”, “¥n”, “¥r") が正しくエスケープ処理されませんでした。例えば、「CORP¥user」は「CORPuser」、「CORP¥nancy」は「CORP ancy」、「CORP¥randy」は「CORP andy」と表示されました。

調査の修正

追跡番号	説明
ASOC-73826	[イベント分析]ビューのクエリ コンソールで、サービスがオフラインの時も情報アイコンがエラー アイコンに変わりませんでした。
ASOC-73224	[イベント分析]ビューでクエリ結果のイベントを取得している時、完了に5分以上かかると、すでに表示中のイベントが画面から消えていました。
ASOC-60464	[イベント]ビューから大きなPCAPを抽出する時、5分経過すると処理がタイムアウトしますが、ジョブ トレイのエラー メッセージにはクエリ時間が8時間と表示されました。

既知の問題

このリリースの未修正の問題の一覧は、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。

アップグレード パス

NetWitness Platform 11.4.0.0は次 のアップグレード パスをサポートしています。

- RSA NetWitness® Platform 11.2.x.xから11.4.0.0
- RSA NetWitness® Platform 11.3.0.xから11.4.0.0
- RSA NetWitness® Platform 11.3.1.xから11.4.0.0
- RSA NetWitness® Platform 11.3.2.xから11.4.0.0

1.4.0.0へのアップグレード の詳 細 は、RSA LinkのNetWitness Platformド キュメント ページで「Installation and Upgrade Guides」を参 照してください。RSA NetWitness Platform 11.xのすべてのド キュメント の一 覧 を、「総 合 目 次」 で確 認 できます。

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 11.4 Online Documentation	https://community.rsa.com/community/products/netwitness/documentation
RSA NetWitness Platform 11.4 Installation and Upgrade Instructions	https://community.rsa.com/community/products/netwitness/documentation「Installation & Upgrade Guides」セクション
RSA NetWitness Platform Hardware Setup Guides	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA Content for RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

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@emc.comまでメールで送信してください。

サポートされなくなった機能

次の表は、RSA NetWitness® Platform 11.2以降サポートされなくなった機能について説明しています。

11.2.0.0 以降でサポートされなくなった機能

機能	メモ
11.2以前のEvent Stream Analysisサービスの機能の一部	Event Stream Analysisサービス(11.2以前) の次の機能はRSA Correlationサービス(11.3以降) では提供されません。 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. エンリッチメント ソースとしてのデータベースの使用 (Context Hubリストにより置換) 4. エンリッチメント ソースとしての Warehouse Analytics の使用(Context Hubリストにより置換) 5. エンリッチメント ソースとしてのデータベース接続の使用(Context Hubリストにより置換) 6. エンリッチメント ソースとしての自動更新インメモリテーブルの使用(Context Hubリストにより置換) 7. キャプチャ時間による並べ替え 8. メモリプール
Endpoint Hybrid	11.3.0.0以降では、「 Endpoint Hybrid」ホスト タイプはサポートされません。

サポート情報

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
- 更に情報が必要な場合は、カスタマサポートにご連絡ください。

カスタマサポートに連絡する時は、コンピュータ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
メール	support@rsa.com
各国のお問い合わせ窓口	http://japan.emc.com/support/rsa/contact/phone-numbers.htm
コミュニティ	https://community.rsa.com/community/support
ベーシックサポート	月曜日から金曜日、現地時間の午前 9時から午後 5時まで利用可能です。
拡張サポート	新規の重大度1の問題について24時間365日の技術サポートを提供します。

改訂履歴

改訂番号	日付	説明
1.0	2020年1月	初版リリース