



NetWitness Respond ユーザ ガイド

バージョン 11.0



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、民事および刑事責任が課せられることがあります。

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、本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せん。予告なく変更される場合があります。

2月 2018

目次

NetWitness Respondのインシデント対応プロセス	7
NetWitness Respondのインシデント対応ワークフロー	8
インシデントへの対応	9
インシデントへの対応のワークフロー	10
インシデントの優先順位リストの確認	11
インシデントリストの表示	11
インシデントリストのフィルタ	13
[インシデントリスト]ビューからのMyフィルタの削除	14
担当インシデントの表示	15
インシデントの検索	15
インシデントリストのソート	17
自分へのインシデントの割り当て	18
アクションが必要なインシデントの判断	20
インシデントの詳細の表示	20
インシデントに関する基本的なサマリ情報の表示	22
インジケータとエンリッチメントの表示	24
イベントの表示と調査	26
イベントに関連するエンティティの表示と調査	29
[インシデントの詳細]ビューでのデータのフィルタ処理	31
インシデントに関連するタスクの表示	34
インシデントメモの表示	35
関連インジケータの検索	35
インシデントへの関連インジケータの追加	37
インシデントの調査	39
コンテキスト情報の表示	39
ホワイトリストへのエンティティの追加	42
リストの作成	43
NetWitness Endpointへの移行	43
調査への移行	44
NetWitnessの外で実行した手順の記録	44

インシデントのジャーナル エントリーの表示	45
メモの追加	46
メモの削除	47
インシデントのエスカレーションまたは修正	48
インシデントの更新	48
インシデント ステータスの変更	48
インシデント優先度の変更	51
その他のアナリストへのインシデントの割り当て	54
インシデントの名称変更	56
すべてのインシデント タスクの表示	57
タスク リストのフィルタ	59
タスク リストからのMyフィルタの削除	61
タスクの作成	62
タスクの検索	66
タスクの変更	66
タスクの削除	70
インシデントのクローズ	72
アラートのレビュー	74
アラートの表示	74
アラート リストのフィルタ	76
アラート リストからのMyフィルタの削除	79
アラートのサマリ情報の表示	79
アラートのイベント詳細の表示	80
イベントの調査	84
コンテキスト情報の表示	84
ホワイトリストへのエンティティの追加	86
ホワイトリストの作成	87
NetWitness Endpointへの移行	87
調査への移行	87
インシデントの手動作成	88
アラートの削除	89
Netwitnessインシデント対応に関する参考情報	91
インシデント リスト ビュー	92
ワークフロー	92
どうしますか?	93

関連トピック	93
簡単な説明	94
インシデント リスト ビュー	94
インシデントのリスト	95
[フィルタ]パネル	98
[概要]パネル	100
ツールバーのアクション	102
[インシデントの詳細]ビュー	103
ワークフロー	103
どうしますか?	104
関連トピック	105
簡単な説明	105
[概要]パネル	107
[インジケータ]パネル	107
ノードのグラフ	108
イベント データシート	110
[ジャーナル]パネル	113
[タスク]パネル	113
[関連インジケータ]パネル	115
ツールバーのアクション	117
アラートのリスト ビュー	118
ワークフロー	118
どうしますか?	118
関連トピック	119
アラートのリスト ビュー	119
アラート リスト	120
[フィルタ]パネル	123
[概要]パネル	125
ツールバーのアクション	127
[アラートの詳細]ビュー	128
ワークフロー	128
どうしますか?	128
関連トピック	129
[アラートの詳細]ビュー	129
[概要]パネル	130
[イベント]パネル	131

イベント リスト	131
イベントの詳細情報	132
イベント メタデータ	132
イベントのソースまたは宛先 デバイスの属性	134
イベントのソースまたは宛先 ユーザーの属性	135
ツールバーのアクション	135
タスク リスト ビュー	136
どうしますか?	136
関連トピック	136
タスク リスト	137
タスクの[概要]パネル	141
ツールバーのアクション	143
[リストへの追加/削除]ダイアログ	144
どうしますか?	144
リストへの追加/削除	145
[コンテキスト検索]パネル- Respondビュー	148
どうしますか?	148
関連トピック	149
[コンテキスト ルックアップ]パネルに表示されたコンテキスト情報	149

NetWitness Respondのインシデント対応プロセス

NetWitness Suite Respondは、複数のソースからアラートを収集します。それらを論理的にグループ化し、インシデント対応ワークフローを開始して、発生したセキュリティの問題を調査、改善するための機能を提供します。NetWitness Suite NetWitness Respondでは、インシデントにアラートを統合するルールを構成できます。アラートはシステムによって共通の形式に標準化されるため、ユーザは、データソースに関係なく、一貫した方法でルール条件を管理できます。ルール条件は、データソースに固有のフィールドや共通のフィールドを使用してアラートデータに対するクエリを記述することにより構築できます。

ルールエンジンによって、類似するアラートはインシデントにグループ化され、このアラートのグループに対して調査および改善ワークフローを実行することができます。アラートが持つ1つまたは2つの属性値(ソースのホスト名など)や、アラートが報告された時間帯(4時間以内のアラートなど)などによって、アラートをインシデントにグループ化するルールを作成できます。

アラートがルールと一致する場合、グループ化の条件に従ってインシデントが作成されます。新しいアラートが報告された時に、条件に一致するインシデントがすでに作成済みの場合、そのインシデントがまだ「対応中」でなければ、新しいアラートは同じインシデントに追加されません。新しいアラートの値が、既存のインシデントのグループ化に使用されている値(特定のホスト名など)または時間帯と一致しない場合は、新しいインシデントが作成され、そのインシデントにアラートが追加されます。

統合ルールは複数設定できます。ルールでは、条件に一致したアラートをインシデントにグループ化するか、他のルールで評価されないよう抑制するかを選択できます。複数のルールを定義した場合、ルールは上から順に評価され、新しいアラートが最初に一致するルールのみが、そのアラートをインシデントに統合するために使用されます。インシデントは、アラートのコンテキスト情報を提供し、調査ステータスを記録するツールを提供し、改善の進行状況をトラッキングします。

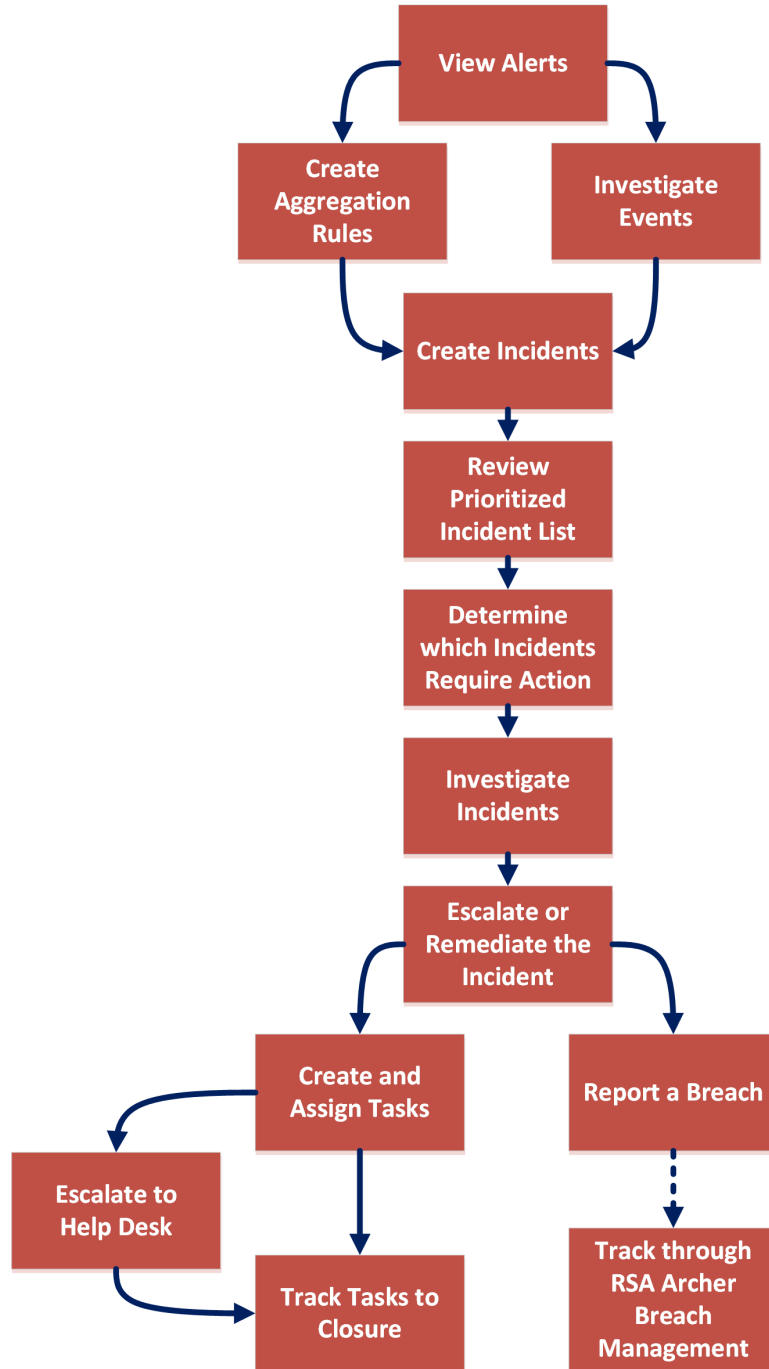
NetWitness Respondのインシデント対応プロセスの各ステージは次のとおりです。

- アラートのレビュー
- インシデントの作成
- インシデントへの対応:
 - 優先度別のインシデントリストのレビュー
 - アクションが必要なインシデントの判断
 - インシデントの調査
 - インシデントのエスカレーションまたは改善(タスクの作成、割り当て、クローズまでのトラッキングを含む)

NetWitness Respondの代わりにRSA NetWitness SecOps Managerでインシデントを管理するオプションもあります。

NetWitness Respondのインシデント対応ワークフロー

次の図は、NetWitness Respondのインシデント対応ワークフロープロセスの概要を示します。



インシデントへの対応

[対応]ビューは、ネットワーク内の進行中の問題をすばやく特定し、他のアナリストと協力して問題をすばやく解決するために役立つように設計されています。

[対応]ビューでは、インシデント対応者に重大度順のインシデントのキューが表示されます。キューからインシデントを取得すると、インシデントの調査に役立つ関連するサポート データを受け取ります。そのデータからインシデントの範囲を判断し、必要に応じてエスカレーションまたは修復することができます。

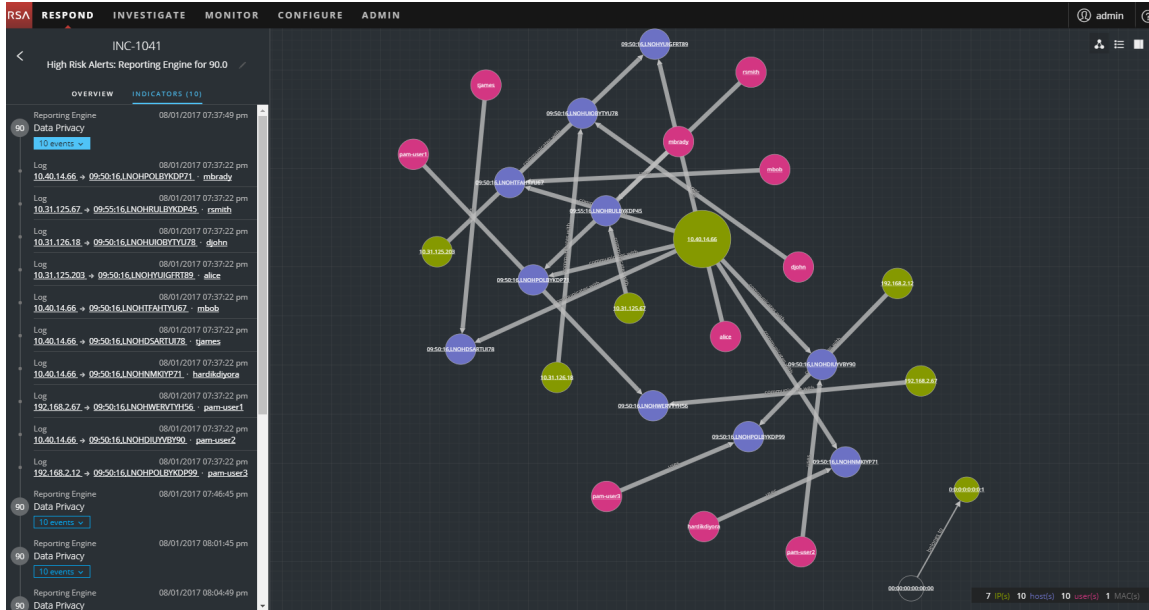
[対応]ビューでは、インシデント、アラート、タスクを表示することができます。

- **インシデント**: インシデントに対応し、最初から最後まで管理できます。
- **アラート**: NetWitness Suiteが受け取ったすべてのソースからのアラートを管理し、選択したアラートからのインシデントを作成できます。
- **タスク**: すべてのインシデントに作成されたタスクの詳細なリストを表示し、管理できます。

[対応] > [インシデント]に移動した場合、[インシデント リスト]ビューを表示し、そこから選択したインシデントの[インシデントの詳細]ビューにアクセスできます。これらは、インシデントへの対応に使用するメインビューです。次の図は、[インシデント リスト]ビュー内のインシデントの優先順位リストを示しています。

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/03/2017 05:28:46 pm	CRITICAL	90	INC-1116	High Risk Alerts: Reporting Engine for 90.0	New		1
08/02/2017 06:06:47 pm	CRITICAL	90	INC-1090	High Risk Alerts: Reporting Engine for 90.0	New		1
08/02/2017 05:00:50 pm	CRITICAL	90	INC-1088	High Risk Alerts: Reporting Engine for 90.0	New		2
08/02/2017 11:01:51 am	CRITICAL	90	INC-1078	High Risk Alerts: Reporting Engine for 90.0	New		1
08/02/2017 07:18:50 am	CRITICAL	90	INC-1074	High Risk Alerts: Reporting Engine for 90.0	New		1
08/02/2017 03:36:48 am	CRITICAL	90	INC-1069	High Risk Alerts: Reporting Engine for 90.0	New		1
08/02/2017 01:18:46 am	CRITICAL	90	INC-1064	High Risk Alerts: Reporting Engine for 90.0	New		1
08/02/2017 01:18:31 am	CRITICAL	90	INC-1061	High Risk Alerts: ESA for 90.0	Assigned	admin	1
08/01/2017 11:31:45 pm	CRITICAL	90	INC-1058	High Risk Alerts: Reporting Engine for 90.0	New		2
08/01/2017 08:39:46 pm	CRITICAL	90	INC-1051	High Risk Alerts: Reporting Engine for 90.0	New		2
08/01/2017 07:37:54 pm	CRITICAL	90	INC-1041	High Risk Alerts: Reporting Engine for 90.0	New		10
08/01/2017 05:59:46 pm	CRITICAL	90	INC-1035	High Risk Alerts: Reporting Engine for 90.0	New		1
08/01/2017 04:28:48 pm	CRITICAL	90	INC-1031	High Risk Alerts: Reporting Engine for 90.0	New		1
08/01/2017 02:38:48 pm	CRITICAL	90	INC-1023	High Risk Alerts: Reporting Engine for 90.0	New		1
08/01/2017 12:46:53 pm	CRITICAL	90	INC-1017	High Risk Alerts: Reporting Engine for 90.0	New		2
08/01/2017 09:03:49 am	CRITICAL	90	INC-1012	High Risk Alerts: Reporting Engine for 90.0	New		1
08/01/2017 05:20:48 am	CRITICAL	90	INC-1008	High Risk Alerts: Reporting Engine for 90.0	New		1
08/01/2017 01:38:47 am	CRITICAL	90	INC-1003	High Risk Alerts: Reporting Engine for 90.0	New		1
07/31/2017 09:55:46 pm	CRITICAL	90	INC-998	High Risk Alerts: Reporting Engine for 90.0	New		1
07/31/2017 06:13:45 am	CRITICAL	90	INC-990	High Risk Alerts: Reporting Engine for 90.0	New		1

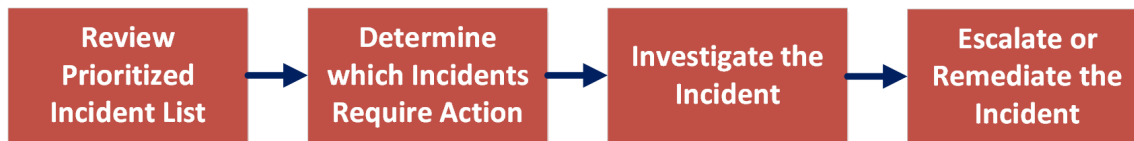
次の図は、[インシデントの詳細]ビューに表示される詳細の例を示しています。



[対応]ビューは、インシデントの評価、そのデータの文脈付け、他のアナリストとのコラボレーション、必要に応じたより詳細な調査への移行を簡単に行えるように設計されています。

インシデントへの対応のワークフロー

このワークフローは、NetWitness Suiteでインシデントに対応するためにインシデント対応者が使用するプロセスの概要を示しています。



最初に、各インシデントに関する基本的な情報を示した、インシデントの優先順位リストを確認して、どのインシデントにアクションが必要かを判断します。インシデント内のリンクをクリックすると、[インシデントの詳細]ビューに補足的な詳細情報が表示され、そのインシデントについて明確に把握できるようになります。その情報に基づいて、インシデントをさらに調査できます。その後、インシデントをエスカレーションまたは修復して、インシデントへの対応方法を決定できます。

インシデントに対応するための基本的なステップは次のとおりです。

1. [インシデントの優先順位リストの確認](#)
2. [アクションが必要なインシデントの判断](#)
3. [インシデントの調査](#)
4. [インシデントのエスカレーションまたは修正](#)

インシデントの優先順位リストの確認

[対応]ビューでは、インシデントの優先順位リストを表示できます。インシデントリストには、アクティブなインシデントとクローズしたインシデントの両方が表示されます。

インシデントリストの表示

ほとんどのインシデント対応者は、NetWitness Suiteにログインした後で、デフォルトビューとして設定されている[対応]ビューを表示します。別のビューが初期ビューに設定されている場合は、[対応]ビューに移動することができます。

1. NetWitness Suiteにログインします。

[対応]ビューには、[インシデントリスト]ビューとも呼ばれるインシデントのリストが表示されます。

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
07/18/2017 01:18:50 pm	HIGH	70	INC-1	High Risk Alerts: Reporting Engine for 70.0	Assigned		24
07/18/2017 03:05:10 pm	HIGH	80	INC-2	Suspected C&C with m1.455denbu	Assigned	DPO Newtiness	1
07/18/2017 03:07:16 pm	HIGH	80	INC-3	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:09:26 pm	HIGH	80	INC-4	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:11:31 pm	HIGH	80	INC-5	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:13:41 pm	HIGH	80	INC-6	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:15:46 pm	HIGH	80	INC-7	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:17:51 pm	HIGH	80	INC-8	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:20:01 pm	HIGH	80	INC-9	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:22:07 pm	HIGH	80	INC-10	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:24:17 pm	HIGH	80	INC-11	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:26:22 pm	HIGH	80	INC-12	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:28:32 pm	HIGH	80	INC-13	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:30:37 pm	HIGH	80	INC-14	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:32:42 pm	HIGH	80	INC-15	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:34:52 pm	HIGH	80	INC-16	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:36:58 pm	HIGH	80	INC-17	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:39:08 pm	HIGH	80	INC-18	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:41:13 pm	HIGH	80	INC-19	Suspected C&C with m1.455denbu	Assigned		1
07/18/2017 03:43:18 pm	HIGH	80	INC-20	Suspected C&C with m1.455denbu	Assigned		1

2. [対応]ビューにインシデントリストが表示されない場合は、で対応[]>[インシデント]を選択します。
3. インシデントリストをスクロールすると、次の表で説明する各インシデントに関する基本的な情報が表示されます。


列	説明
作成日	インシデントの作成日を示します。

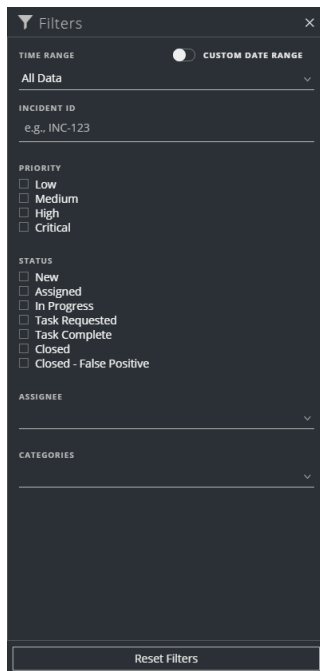
列	説明
優先度	<p>インシデントの優先度を示します。優先度はクリティカル、高、中、低を指定できます。</p> <p>優先度は色分けされ、赤はクリティカルなインシデント、オレンジは高リスクインシデント、黄色は中リスクインシデント、緑は低リスクインシデントを表します。例：</p> 
リスクスコア	<p>インシデントのリスクスコアを示します。リスクスコアはアルゴリズムで計算されたインシデントのリスクを示し、0～100の範囲です。100が最大のリスクスコアです。</p>
ID	<p>自動的に作成されたインシデント番号を示します。各インシデントには、インシデントのトラックに使用できる固有の番号が割り当てられています。</p>
名前	<p>インシデント名を示します。インシデント名は、インシデントのトリガーに使用されたルールから取得されます。リンクをクリックすると、選択したインシデントの[インシデントの詳細]ビューに移動します。</p>
ステータス	<p>インシデントのステータスを表示します。次のステータスがあります。新規、割り当て済み、対応中、タスクリクエスト済み、タスク完了、クローズ、クローズ- False Positive。</p>
割り当て先	<p>インシデントに現在割り当てられている、チームのメンバーを示します。</p>
アラート	<p>インシデントに関連するアラートの数を示します。1つのインシデントに多数のアラートが含まれる場合があります。多数のアラートがある場合は、大規模な攻撃を受けている可能性があります。</p>

リストの下部では、現在のページのインシデント数、インシデントの総数、選択した数を確認できます。例：「1115アイテム中1000個を表示中 | 3個が選択済み」のように表示されます。一度に表示できるインシデントの最大数は1,000です。

インシデント リストのフィルタ

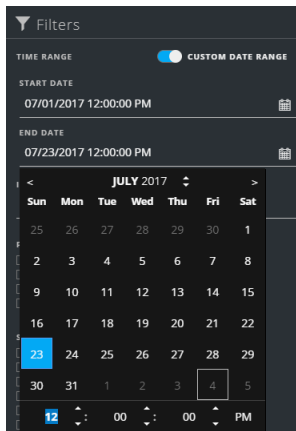
[インシデント リスト]ビュー内のインシデントの数は非常に多数になり、特定のインシデントを検索することが困難になることがあります。フィルタを使用すると、表示するインシデントを指定できます。また、それらのインシデントが発生した期間を選択することもできます。たとえば、過去1時間以内に作成された新しいクリティカル インシデントをすべて表示する必要が生じることがあります。

1. [フィルタ]パネルがインシデント リストの左に表示されていることを確認します。[フィルタ]パネルが表示されない場合は、[インシデント リスト]ビューのツールバーでをクリックすると [フィルタ]パネルが開きます。



2. [フィルタ]パネルで1つまたは複数のオプションを選択し、インシデントのリストをフィルタします。
 - **[時間範囲]**: [時間範囲]ドロップダウン リストから特定の期間を選択できます。時間範囲はインシデントの作成日に基づきます。たとえば、[直近1時間]を選択する場合は、過去60分以内に作成されたインシデントが表示されます。
 - **[カスタムの日付範囲]**: [時間範囲]オプションを選択する代わりに、特定の日付範囲を指定できます。これを行うには、[カスタムの日付範囲]の前にある白色の円をクリックし、[開始日]と[終了日]のフィールドを表示します。カレンダーから日付と時刻を選択

します。



- [インシデントID]: 検索するインシデントのインシデントID(INC-1050など)を入力します。
- [優先度]: 表示する優先度を選択します。
- [ステータス]: 1つまたは複数のインシデントのステータスを選択します。たとえば、誤検知インシデント(最初は疑わしいと判断され、後で安全であると判明したインシデント)のみを表示するには、[クローズ- False Positive]を選択します。
- [割り当て先]: 表示するインシデントの割り当て先を選択します。たとえば、CaleまたはStanleyに割り当てられたインシデントのみを表示する場合は、[割り当て先]ドロップダウンリストから[Cale]と[Stanley]を選択します。割り当て先に関係なくインシデントを表示する場合は、[割り当て先]で何も選択しないでください。
- [カテゴリ]: ドロップダウン リストから、1つまたは複数のカテゴリを選択します。たとえば、バックドアまたは権限の不正利用のカテゴリに分類されたインシデントのみを表示する場合は、[バックドア]と[権限の不正利用]を選択します。


インシデント リストには、選択条件を満たすインシデントのリストが表示されます。インシデント リストの下部では、フィルタ処理されたリストのインシデント数を確認できます。

Showing 89 out of 89 items | 0 selected

3. ✕をクリックして[フィルタ]パネルを閉じ、[インシデント リスト]ビューに戻ると、フィルタ処理されたインシデントが表示されます。


[インシデント リスト]ビューからのMyフィルタの削除

NetWitness Suiteでは、[インシデント リスト]ビューのフィルタ選択が記憶されます。不要な場合はフィルタ選択を削除することができます。たとえば、表示されるべきインシデント数が表示されない場合や、インシデント リストのすべてのインシデントを表示する場合は、フィルタをリセットできます。

1. [インシデント リスト]ビューのツールバーでをクリックします。
[フィルタ]パネルがインシデント リストの左に表示されます。
2. [フィルタ]パネルの下部で[フィルタのリセット]をクリックします。


担当インシデントの表示

担当インシデントを表示するには、インシデントを自分のユーザ名でフィルタ処理します。

1. [フィルタ]パネルが表示されない場合は、[インシデント リスト]ビューのツールバーでをクリックします。
2. [フィルタ]パネルの[割り当て先]で、ドロップダウン リストから自分のユーザ名を選択します。
自分に割り当てられているインシデントがインシデント リストに表示されます。

インシデントの検索

インシデントIDがわかっている場合は、フィルタを使用して、インシデントをすばやく見つけることができます。たとえば、数千のインシデントから特定のインシデントを見つける場合があります。

1. [対応]>[インシデント]に移動します。
[フィルタ]パネルがインシデント リストの左に表示されます。[フィルタ]パネルが表示されない場合は、[インシデント リスト]ビューのツールバーでをクリックすると[フィルタ]パネルが開きます。

- [インシデントID] フィールドに、検索するインシデントのインシデントID(INC-1110 など) を入力します。

指定したインシデントは、インシデント リストに表示されます。結果が表示されない場合は、フィルタをリセットしてください。

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGN...	ALERTS
08/03/2017 13:06:48	HIGH	70	INC-1110	High Risk Alerts: Reporting Engine for 70.0	New		60

Showing 1 out of 0 Items | 0 selected


インシデント リストのソート

インシデント リストのデフォルトのソート順は、作成日の降順です(最も新しい作成日が一番上)。

The screenshot shows the 'Incidents' tab with a table of incidents. The 'CREATED' column is highlighted with a red box, indicating it is the current sort order. The incidents are sorted by their creation date from newest to oldest.


CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 07:00:32 pm	LOW	0	INC-1137	Investigate - IP	New		3
08/04/2017 12:16:48 pm	HIGH	70	INC-1136	High Risk Alerts: Reporting Engine for 70.0	New		48

インシデント リストのソート順を変更するには、リストの列をクリックします。

たとえば、[優先度]列でビューをソートすると、優先度の順にインシデントを表示することができます。これを行うには、[優先度]列にポインターを合わせて、下矢印  をクリックします。インシデント リストが優先度の降順でソートされます(最高の優先度が一番上)(次の図を参照)。

The screenshot shows the 'Incidents' tab with the 'PRIORITY' column highlighted by a red box and a dropdown arrow, indicating it is the current sort order. The incidents are sorted by their priority from highest to lowest.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/03/2017 05:28:46 pm	CRITICAL	90	INC-1116	High Risk Alerts: Reporting Engine for 90.0	New		1
08/02/2017 06:06:47 pm	CRITICAL	90	INC-1090	High Risk Alerts: Reporting Engine for 90.0	New		1
08/02/2017 05:00:50 pm	CRITICAL	90	INC-1088	High Risk Alerts: Reporting Engine for 90.0	New		2

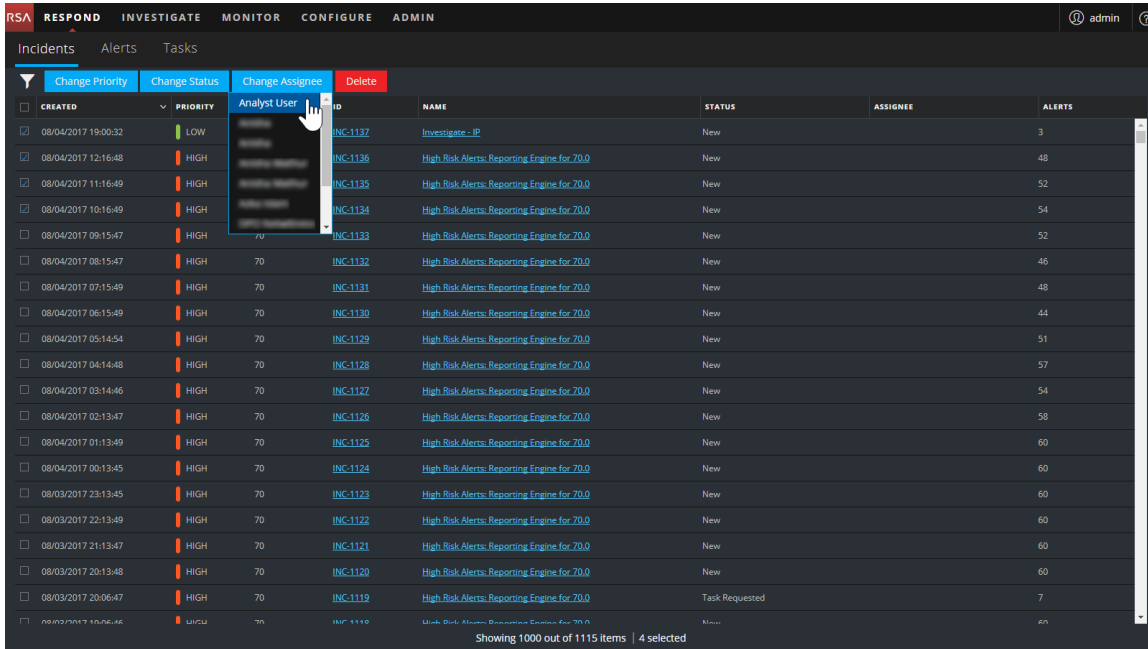
優先度の昇順でソートするには(最低の優先度が一番上)、上矢印  をクリックします(次の図を参照)。

The screenshot shows the 'Incidents' tab with the 'PRIORITY' column highlighted by a red box and an upward-pointing arrow, indicating it is the current sort order. The incidents are sorted by their priority from lowest to highest.

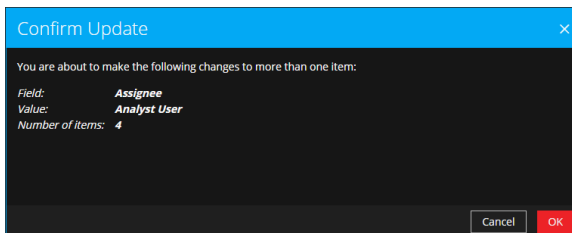
CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 07:00:32 pm	LOW	0	INC-1137	Investigate - IP	New		3
07/21/2017 06:33:40 am	MEDIUM	90	INC-610	High Risk Alerts: ESA for 90.0	In Progress	DPO Netwitness	60
08/02/2017 01:07:53 pm	MEDIUM	0	INC-1082	Test 1 ID#39-8*1	Assigned	Anisha	2

自分へのインシデントの割り当て

1. [インシデント リスト]ビューで、自分に割り当てる1つ以上のインシデントを選択します。
2. [割り当て先の変更]をクリックし、ドロップダウン リストから自分のユーザ名を選択します。



3. 複数のインシデントを選択した場合、[更新の確認]ダイアログで[OK]をクリックします。



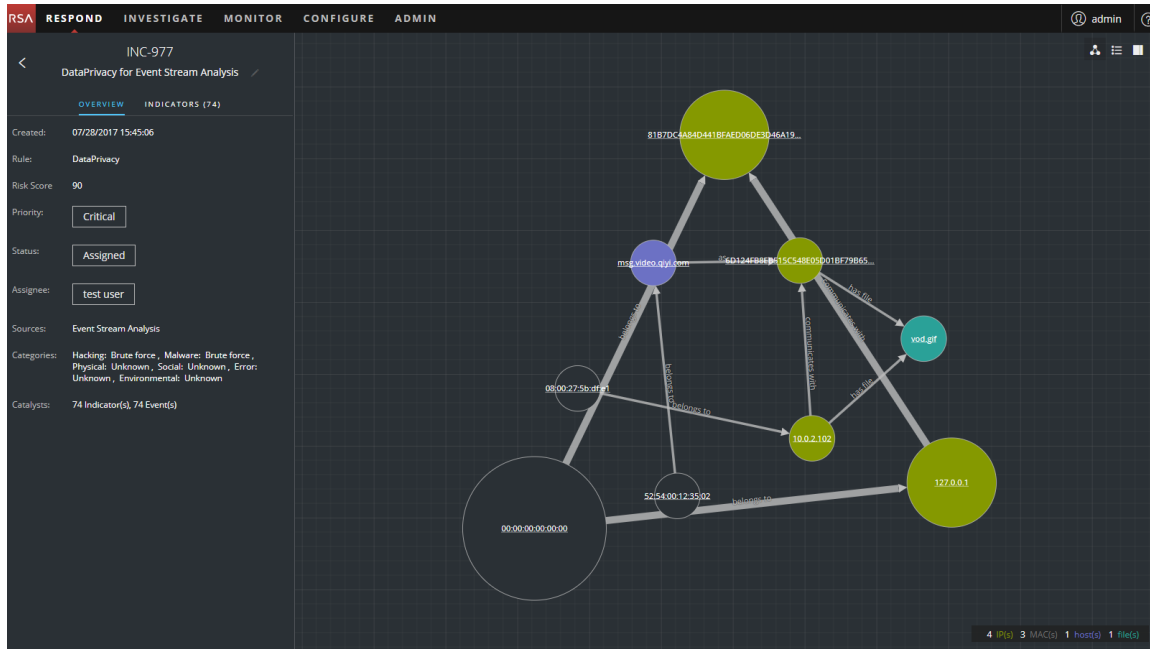
変更が成功した通知が表示されます。

The screenshot shows the NetWitness Respond interface with a green notification banner at the top stating "Your change was successful". Below the navigation tabs (Incidents, Alerts, Tasks), there are buttons for "Change Priority", "Change Status", "Change Assignee", and "Delete". A table of incidents is displayed with columns for CREATED, PRIORITY, RISK SCORE, ID, NAME, STATUS, ASSIGNEE, and ALERTS. The ASSIGNEE column is highlighted with a red box, showing "Analyst User" for several rows. The bottom of the interface indicates "Showing 1000 out of 1115 items | 4 selected".

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 19:00:32	LOW	0	INC-1137	Investigate - IP	Assigned	Analyst User	3
08/04/2017 12:16:48	HIGH	70	INC-1136	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	48
08/04/2017 11:16:49	HIGH	70	INC-1135	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	52
08/04/2017 10:16:49	HIGH	70	INC-1134	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	54
08/04/2017 09:15:47	HIGH	70	INC-1133	High Risk Alerts: Reporting Engine for 70.0	New		52
08/04/2017 08:15:47	HIGH	70	INC-1132	High Risk Alerts: Reporting Engine for 70.0	New		46
08/04/2017 07:15:49	HIGH	70	INC-1131	High Risk Alerts: Reporting Engine for 70.0	New		48
08/04/2017 06:15:49	HIGH	70	INC-1130	High Risk Alerts: Reporting Engine for 70.0	New		44
08/04/2017 05:14:54	HIGH	70	INC-1129	High Risk Alerts: Reporting Engine for 70.0	New		51
08/04/2017 04:14:48	HIGH	70	INC-1128	High Risk Alerts: Reporting Engine for 70.0	New		57
08/04/2017 03:14:46	HIGH	70	INC-1127	High Risk Alerts: Reporting Engine for 70.0	New		54
08/04/2017 02:13:47	HIGH	70	INC-1126	High Risk Alerts: Reporting Engine for 70.0	New		58
08/04/2017 01:13:49	HIGH	70	INC-1125	High Risk Alerts: Reporting Engine for 70.0	New		60
08/04/2017 00:13:45	HIGH	70	INC-1124	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 23:13:45	HIGH	70	INC-1123	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 22:13:49	HIGH	70	INC-1122	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 21:13:47	HIGH	70	INC-1121	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 20:13:48	HIGH	70	INC-1120	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 20:06:47	HIGH	70	INC-1119	High Risk Alerts: Reporting Engine for 70.0	Task Requested		7
08/03/2017 19:06:46	LOW	70	INC-1118	High Risk Alerts: Reporting Engine for 70.0	New		48

アクションが必要なインシデントの判断

[インシデント リスト]ビューから、インシデントに関する一般的な情報を取得すると、[インシデント 詳細]]ビューに移動して詳細情報を確認し必要なアクションを判断することができます。

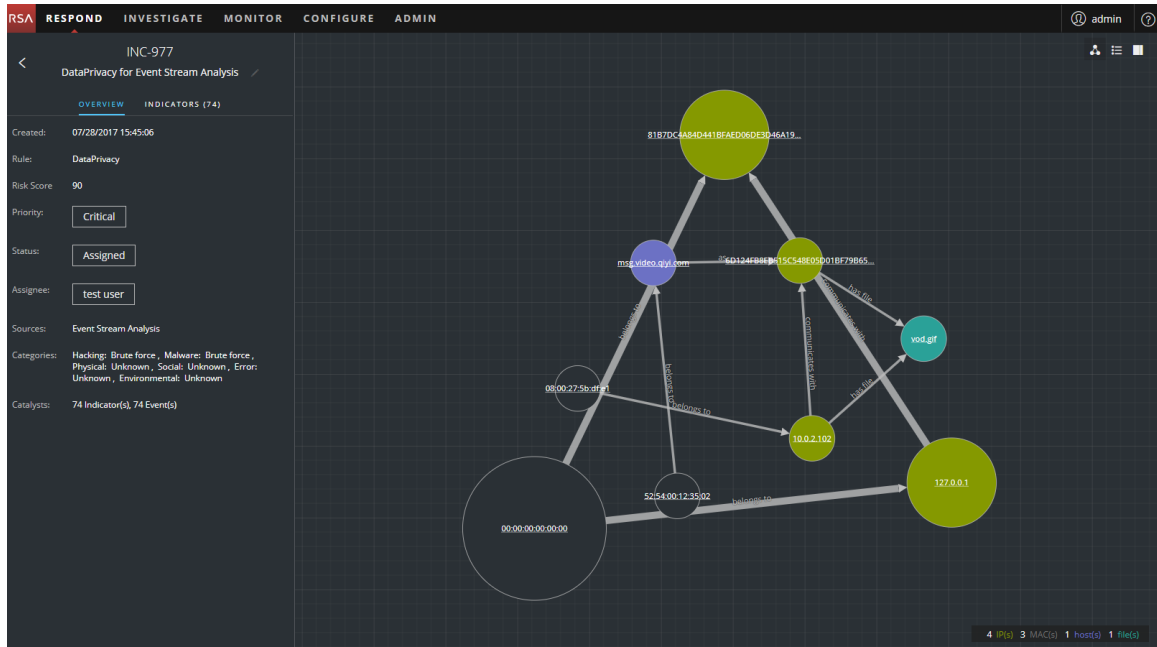


インシデントの詳細の表示

インシデントの詳細を表示するには、[インシデント リスト]ビューで、表示するインシデントを選択し、そのインシデントの[ID]または[名前]列のリンクをクリックします。

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/01/2017 09:03:49	CRITICAL	90	INC-1012	High Risk Alerts Reporting Engine for 90.0	New		1
08/01/2017 09:20:48	CRITICAL	90	INC-1008	High Risk Alerts Reporting Engine for 90.0	New		1
08/01/2017 01:38:47	CRITICAL	90	INC-1003	High Risk Alerts Reporting Engine for 90.0	New		1
07/31/2017 21:55:46	CRITICAL	90	INC-998	High Risk Alerts Reporting Engine for 90.0	New		1
07/31/2017 18:13:45	CRITICAL	90	INC-990	High Risk Alerts Reporting Engine for 90.0	New		1
07/31/2017 16:20:52	CRITICAL	90	INC-982	High Risk Alerts Reporting Engine for 90.0	New		9
07/28/2017 15:45:06	CRITICAL	90	INC-977	DataPrivacy for Event Stream Analysis	Assigned	test user	74
07/28/2017 15:44:06	CRITICAL	90	INC-975	DataPrivacy for Event Stream Analysis	Assigned	test user	2
07/28/2017 15:43:06	CRITICAL	90	INC-973	DataPrivacy for Event Stream Analysis	Assigned	test user	4
07/28/2017 15:42:05	CRITICAL	90	INC-971	DataPrivacy for Event Stream Analysis	Assigned	test user	2
07/28/2017 15:41:05	CRITICAL	90	INC-970	DataPrivacy for Event Stream Analysis	Assigned	test user	2
07/28/2017 15:40:05	CRITICAL	90	INC-968	DataPrivacy for Event Stream Analysis	Assigned	test user	2
07/28/2017 15:39:05	CRITICAL	90	INC-966	DataPrivacy for Event Stream Analysis	Assigned	test user	2
07/28/2017 15:38:05	CRITICAL	90	INC-964	DataPrivacy for Event Stream Analysis	Assigned	test user	4
07/28/2017 15:37:05	CRITICAL	90	INC-962	DataPrivacy for Event Stream Analysis	Assigned	test user	2
07/28/2017 15:36:05	CRITICAL	90	INC-960	DataPrivacy for Event Stream Analysis	Assigned	test user	2
07/28/2017 15:35:04	CRITICAL	90	INC-958	DataPrivacy for Event Stream Analysis	Assigned	test user	2
07/28/2017 15:34:04	CRITICAL	90	INC-956	DataPrivacy for Event Stream Analysis	Assigned	test user	2
07/28/2017 15:33:04	CRITICAL	90	INC-954	DataPrivacy for Event Stream Analysis	Assigned	test user	4

選択したインシデントの[インシデントの詳細]ビューが表示されます。このビューには[概要]パネルとノード グラフが表示されます。



[インシデントの詳細]ビューには次のパネルがあります。

- 概要:** インシデントの[概要]パネルには、リスクスコア、優先度、アラート、ステータスなど、インシデントに関する概要レベルのサマリ情報が含まれています。インシデントの優先度、ステータス、割り当て先を変更することができます。
- インジケータ:** [インジケータ]パネルには、インジケータの一覧が時系列に表示されます。インジケータは、ESAアラートやNetWitness Endpointアラートなどのアラートです。このリストは、インジケータと注目すべきデータを関連づけるのに役立ちます。たとえば、コマンド&コントロールESAアラートに関連するIPアドレスは、NetWitness Endpointアラートやその他の疑わしいアクティビティをトリガーする可能性があります。
- ノード グラフ:** ノード グラフは、インシデントに関連するエンティティ間の関係を表示する対話型のグラフです。エンティティは、IPアドレス、MACアドレス、ユーザ、ホスト、ドメイン、ファイル名、ファイルハッシュなどの特定のメタです。
- イベント:** [イベント]パネルはイベント テーブルとも呼ばれ、インシデントに関連するイベントを一覧表示します。イベントタイプに応じて、追加情報とともにイベントのソースと宛先の情報も表示されます。リスト内のイベントをクリックすると、そのイベントの詳細なデータを表示することができます。
- ジャーナル:** [ジャーナル]パネルでは、選択したインシデントのジャーナルにアクセスすることができます。ジャーナルは、他のアナリストと通信し、コラボレーションするために使用します。

ジャーナルにメモをポストし、調査マイルストーン タグ(予備調査、配信、悪用、インストール、コマンド&コントロール)を追加し、インシデントのアクティビティの履歴を表示できます。

- **タスク:** [タスク] パネルには、インシデントに対して作成されたすべてのタスクが表示されます。ここから追加のタスクを作成することもできます。
- **関係:** [関連インジケータ] パネルでは、NetWitness Suite アラート データベースを検索して、このインシデントに関連するアラートを探することができます。見つけた関連するアラートをインシデントに追加することもできます。

スクロールせずに左側のパネルにより多くの情報を表示するには、右端にカーソルを合わせ、次の図に示すように、線をドラッグしてパネルのサイズを変更することができます。

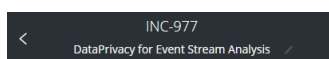
The screenshot displays the NetWitness Respond interface. On the left, there is a list of events under the heading 'DataPrivacy for Event Stream Analysis'. The events include 'Event Stream Analysis', 'Test', and 'Network' with various timestamps and IP addresses. On the right, there is a network diagram with nodes representing IP addresses and domains like 'msn.deo.qiyi.com', '127.0.0.1', '60124f88e8315c548e05d018f79865...', '10.0.2.102', and 'vod.gif'. A vertical blue line is positioned between the two panels, and a mouse cursor is shown dragging it to the right, indicating that the width of the left panel can be adjusted.

インシデントに関する基本的なサマリ情報の表示

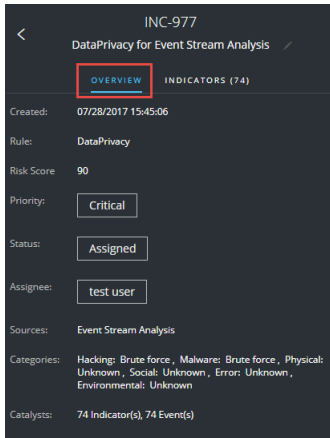
[概要] パネルでインシデントに関する基本的なサマリ情報を表示できます。

[概要] パネルの上部で、次の情報を確認できます。

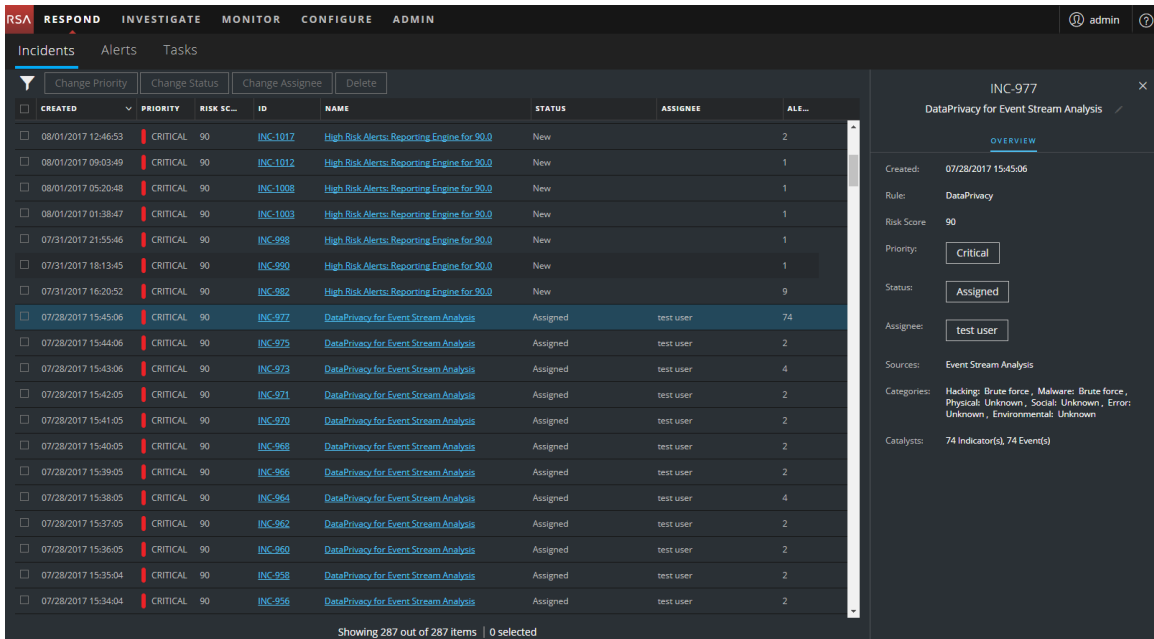
- **インシデントID:** これは、各インシデントに割り当てられる自動的に作成された固有の識別子です。
- **名前:** インシデント名は、インシデントをトリガーしたルールから取得されます。



[インシデントの詳細]ビューから[概要]パネルを表示するには、左側のパネルで[概要]を選択します。



[インシデント リスト]ビューから[概要]パネルを表示するには、リスト上のインシデントをクリックします。右側に[概要]パネルが表示されます。



[概要]パネルには、選択したインシデントについての基本的なサマリ情報が含まれています。

- **作成日**: インシデントの作成日時を示します。
- **ルール/By**: インシデントを作成したルールの名前またはインシデントを作成したユーザの名前を示します。
- **リスクスコア**: アルゴリズムにより計算されたインシデントのリスクを示し、0～100の範囲です。100が最大のリスクスコアです。

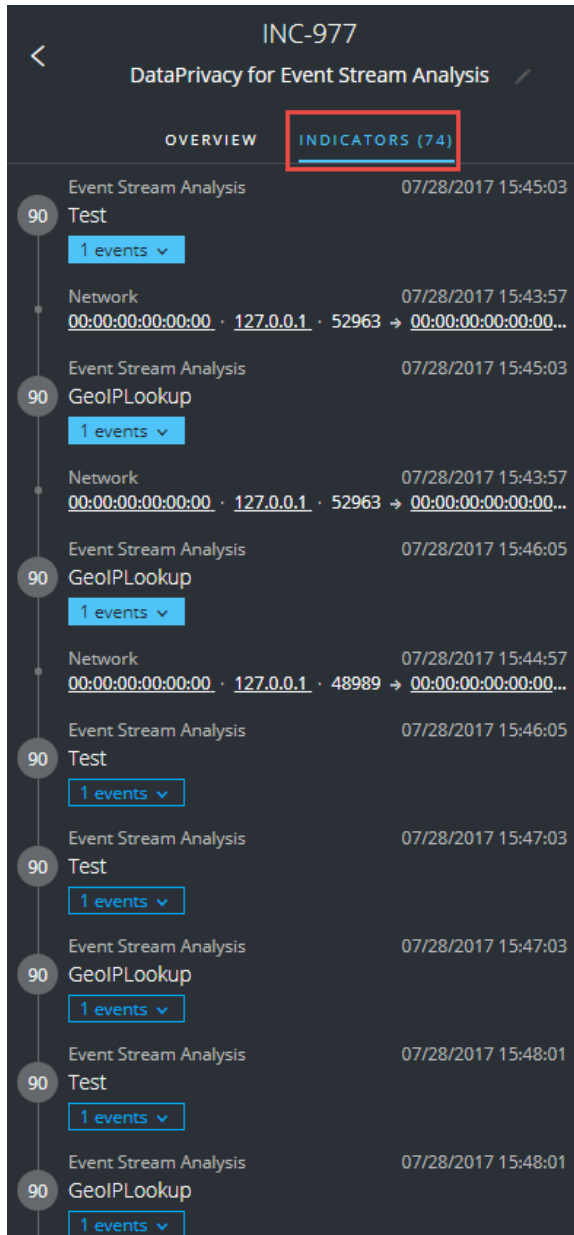
- **優先度**: インシデントの優先度を示します。優先度はクリティカル、高、中、低のいずれかです。
- **ステータス**: インシデントのステータスを表示します。ステータスは、新規、割り当て済み、対応中、タスクリクエスト中、タスク完了、クローズ、クローズ-False Positiveのいずれかです。タスクを作成すると、ステータスは[タスクリクエスト中]に変わります。
- **割り当て先**: インシデントに現在割り当てられている、チームのメンバーを示します。
- **ソース**: 疑わしいアクティビティの検出に使用されたデータソースを示します。
- **カテゴリ**: インシデント イベントのカテゴリを示します。
- **要因**: インシデントを発生させたインジケータのカウントを示します。

インジケータとエンリッチメントの表示

注: インジケータは、ESAアラートやNetWitness Endpointアラートなどのアラートです。

[インジケータ]パネルでは、インジケータ、イベント、エンリッチメントを検索できます。[インジケータ]パネルには、インジケータのリストが時系列に表示され、インジケータのトリガーとなったエンリッチメントとイベントを検索するのに役に立ちます。たとえば、インジケータには、コマンド&コントロールアラート、NetWitness Endpointアラート、疑わしいドメイン(C2)アラート、Event Stream Analysis(ESA)アラートなどがあります。[インジケータ]パネルは、異なるシステムで生成されたこれらのインジケータ(アラート)を統合し、並べ替えることにより、それぞれの関連を確認し、特定の攻撃の時間経過を把握するのに役に立ちます。

[インジケータ]パネルを表示するには、[インシデントの詳細]ビューの左側のパネルで[インジケータ]を選択します。



インジケータは、ESAアラートやNetWitness Endpointアラートなどのアラートです。このリストは、インジケータと注目すべきデータを関連づけるのに役立ちます。たとえば、インジケータには、ルールによって検出されたデータを表示できます。[インジケータ]パネルでは、単色で塗りつぶされた丸の中にインジケータのリスクスコアが表示されます。

データソースの情報は、インジケータの名前の下に表示されます。インジケータの作成日と時刻、インジケータのイベントの数も確認できます。データがある場合は、エンリッチメントの数を表示できます。イベントとエンリッチメントのボタンをクリックすると詳細を表示することができます。

イベントの表示と調査

[イベント]パネルから、インシデントに関連するイベントを表示して調査できます。イベント時間、ソースIP、宛先IP、検知器IP、ソースユーザ、宛先ユーザ、イベントに関するファイル情報など、イベントに関する情報が表示されます。表示される情報の量は、イベントタイプに依存します。

イベントには次の2つのタイプがあります。

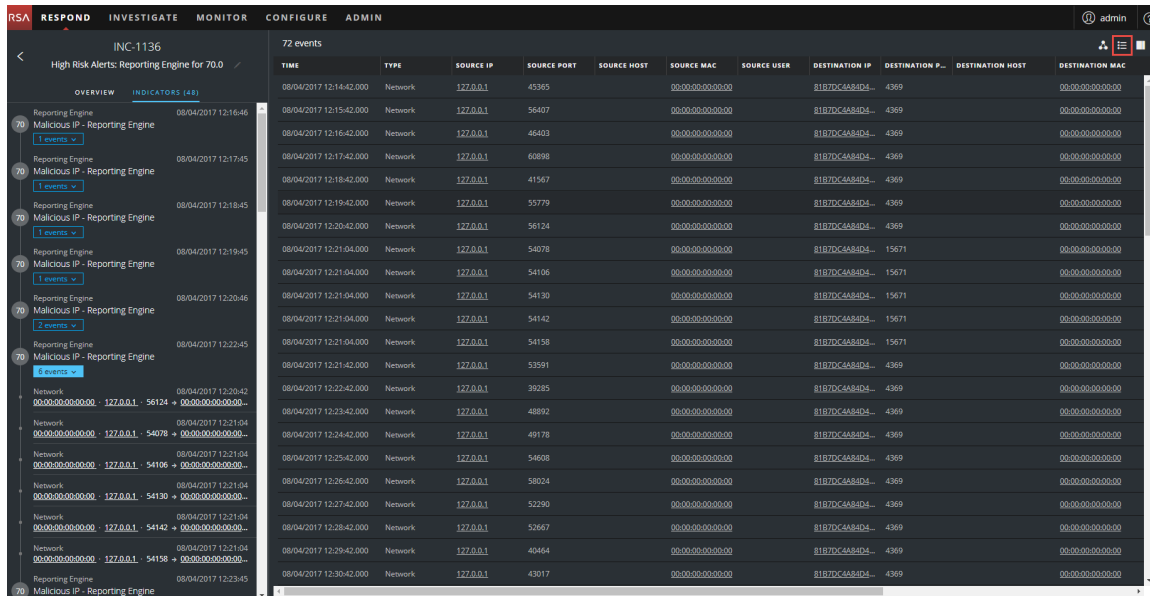
- 2台のマシン(ソースと宛先)間のトランザクション
- 1台のマシン(検知器)で検出された異常

一部のイベントには、検知器の情報しか含まれません。たとえば、NetWitness Endpointはマシンのマルウェアを検出します。その他のイベントは、ソースと宛先の情報を含んでいます。たとえば、パケットデータは、1台のマシンとコマンド&コントロール(C2)ドメイン間の通信を表します。

イベントをさらにドリルダウンして、イベントに関する詳細なデータを取得できます。

イベントを表示して調査するには、次の手順を実行します。

1. [イベント]パネルを表示するには、[インシデントの詳細]ビューのツールバーで、をクリックします。



TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION P.	DESTINATION HOST	DESTINATION MAC
08/04/2017 12:14:42.000	Network	127.0.0.1	43365		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:15:42.000	Network	127.0.0.1	56407		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:16:42.000	Network	127.0.0.1	46403		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:17:42.000	Network	127.0.0.1	60898		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:18:42.000	Network	127.0.0.1	41567		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:19:42.000	Network	127.0.0.1	53779		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:20:42.000	Network	127.0.0.1	56124		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:21:04.000	Network	127.0.0.1	54078		00:00:00:00:00:00		8187DC48B4D4	15671		00:00:00:00:00:00
08/04/2017 12:21:04.000	Network	127.0.0.1	54130		00:00:00:00:00:00		8187DC48B4D4	15671		00:00:00:00:00:00
08/04/2017 12:21:04.000	Network	127.0.0.1	54142		00:00:00:00:00:00		8187DC48B4D4	15671		00:00:00:00:00:00
08/04/2017 12:21:04.000	Network	127.0.0.1	54158		00:00:00:00:00:00		8187DC48B4D4	15671		00:00:00:00:00:00
08/04/2017 12:21:42.000	Network	127.0.0.1	53591		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:22:42.000	Network	127.0.0.1	39285		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:23:42.000	Network	127.0.0.1	48892		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:24:42.000	Network	127.0.0.1	49178		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:25:42.000	Network	127.0.0.1	54608		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:26:42.000	Network	127.0.0.1	58024		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:27:42.000	Network	127.0.0.1	52390		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:28:42.000	Network	127.0.0.1	52667		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:29:42.000	Network	127.0.0.1	40464		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00
08/04/2017 12:30:42.000	Network	127.0.0.1	43917		00:00:00:00:00:00		8187DC48B4D4	4369		00:00:00:00:00:00

[イベント]パネルに、各イベントの次の情報が一覧表示されます。

列	説明
時間	イベントの発生時刻を示します。

列	説明
タイプ	「Log」または「Network」などのアラートのタイプを示します。
ソースIP	2台のマシン間のトランザクションがあった場合は、ソースIPアドレスを示します。
ソースポート	トランザクションのソースポートを示します。ソースポートと宛先ポートが同じIPアドレス上に存在する場合があります。
ソースホスト	イベントが発生したソースホストを示します。
ソースMAC	ソースマシンのMACアドレスを示します。
ソースユーザ	ソースマシンのユーザを示します。
宛先IP	2台のマシン間のトランザクションがあった場合は、宛先IPアドレスを示します。
宛先ポート	トランザクションの宛先ポートを示します。ソースポートと宛先ポートが同じIPアドレス上に存在する場合があります。
宛先ホスト	イベントが発生した宛先ホストを示します。
宛先MAC	宛先マシンのMACアドレスを示します。
宛先ユーザ	宛先マシンのユーザを示します。
検知器のIP	異常を検出したマシンのIPアドレスを示します。
ファイル名	イベントにファイルが関連している場合は、ファイル名が表示されます。
ファイルハッシュ	ファイルの内容のハッシュを示します。

リストにイベントが1件しかない場合は、リストではなくそのイベントの詳細が表示されます。

2. [イベント]リストのイベントをクリックすると、イベントの詳細が表示されます。
この例では、イベント リストの最初のイベントの詳細を表示しています。

The screenshot shows the NetWitness Respond interface. The left sidebar displays a list of events under the heading 'INC-1136 High Risk Alerts: Reporting Engine for 70.0'. The first event is selected, and its details are shown in the main panel. The event details include:

- Timestamp: 08/04/2017 12:14:42 (10 hours ago)
- Type: Network
- Source: Device Port 45365, MAC Address 00:00:00:00:00:00, IP Address 127.0.0.1, Geolocation
- User
- Destination: Device Port 4369, MAC Address 00:00:00:00:00:00, IP Address 81B7DC4A84D441BFAED06DE3D46A19C49D17B4157FBCEDEE886FD7D21A27F77, Geolocation
- User
- Detector
- Size: 1336
- Data: Size 1336
- Related Links: Type investigate_original_event, URL /investigation/host/10.4.61.30:56005/navigate/event/AUTO/462087

3. 追加のイベントの詳細を表示するには、[イベントの詳細]ナビゲーションを使用します。
この例では、リストの2番目のイベントを示します。

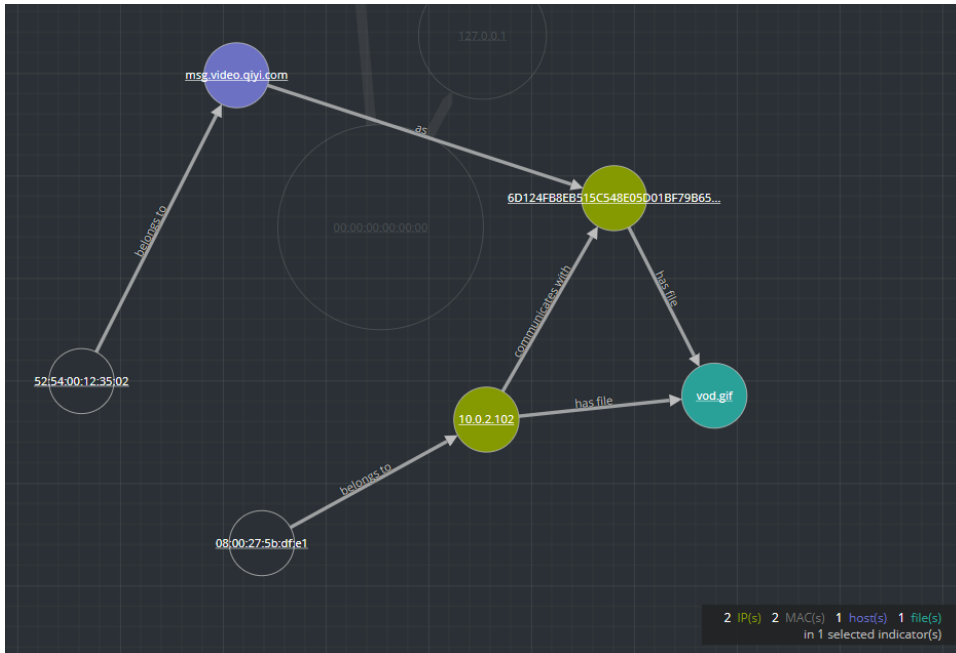
The screenshot shows the NetWitness Respond interface. The left sidebar displays a list of events under the heading 'INC-1136 High Risk Alerts: Reporting Engine for 70.0'. The second event is selected, and its details are shown in the main panel. The event details include:

- Timestamp: 08/04/2017 12:15:42 (10 hours ago)
- Type: Network
- Source: Device Port 56407, MAC Address 00:00:00:00:00:00, IP Address 127.0.0.1, Geolocation
- User
- Destination: Device Port 4369, MAC Address 00:00:00:00:00:00, IP Address 81B7DC4A84D441BFAED06DE3D46A19C49D17B4157FBCEDEE886FD7D21A27F77, Geolocation
- User
- Detector
- Size: 1336
- Data: Size 1336
- Related Links: Type investigate_original_event, URL /investigation/host/10.4.61.30:56005/navigate/event/AUTO/462088

イベントに関連するエンティティの表示と調査

エンティティは、IPアドレス、MACアドレス、ユーザ、ホスト、ドメイン、ファイル名、ファイルハッシュのいずれかです。ノード グラフは、イベントに関連するエンティティの相互関係をわかりやすく表示するための対話型のグラフです。ノード グラフは、イベントのタイプ、関係するマシンの数、マシンがユーザに関連付けられているかどうか、イベントに関連づけられたファイルがあるかどうかによって異なって表示されます。

次の図は、6つのノードを含むノード グラフの例です。



ノード グラフでは、各ノードは円で表現されます。ノード グラフには、次のタイプのノードが1つ以上含まれます。

- IPアドレス(イベントが異常の検出である場合は、検知器のIPが表示されます。イベントがトランザクションの場合は、宛先IPとソースIPが表示されます。)
- MACアドレス(各タイプのIPアドレスのMACアドレスが表示されます。)
- ユーザ(マシンがユーザに関連づけられている場合、ユーザノードが表示されます。)
- ホスト
- ドメイン
- ファイル名(イベントにファイルが関連する場合、ファイル名を確認できます。)
- ファイルハッシュ(イベントにファイルが関係する場合、ファイルハッシュが表示されます。)

ノード グラフの下部の凡例は、各タイプのノードの数と色を示します。

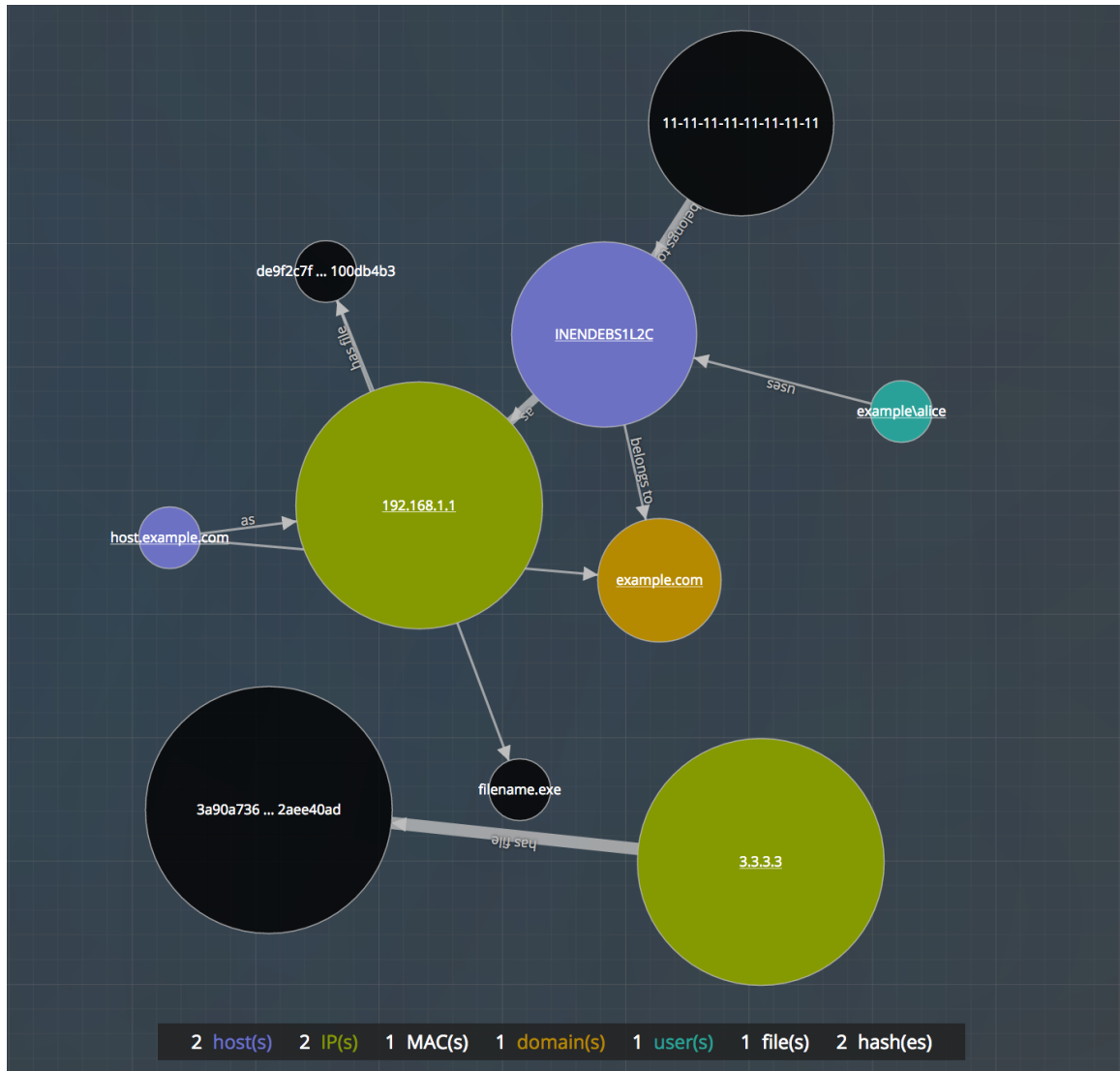
任意のノードをクリックし、ドラッグして位置を変更することができます。

ノード間の矢印は、エンティティの関係に関する追加情報を提供します。

- **communicates with**: ソース マシン ノード (IPアドレスまたはMACアドレス) と宛先 マシン ノード間を結ぶ「communicates with」というラベルの矢印は、通信の方向を示します。
- **as**: ノード間を結ぶ「as」というラベルの矢印は、矢印の先のIPアドレスに関する追加情報を提供します。上の例では、ホスト ノードからハッシュされたIPアドレス ノードに向かう矢印に、「as」というラベルが付けられています。これは、ホスト ノードに表示された名前が、IPアドレスのホスト名であり、異なるエンティティではないことを示します。
- **has file**: マシン ノード (IPアドレス、MACアドレス、ホスト) とファイル ハッシュ ノードを結ぶ「has file」というラベルの矢印は、IPアドレスがそのファイルを持つことを示します。
- **uses**: ユーザ ノードとマシン ノード (IPアドレス、MACアドレス、ホスト) を結ぶ「uses」というラベルの矢印は、ユーザがイベント中に使用していたマシンを示します。
- **is named**: ファイル ハッシュ ノードとファイル名 ノードを結ぶ「is named」というラベルの矢印は、ファイル ハッシュがその名前のファイルのものであることを示します。
- **belongs to**: 2つのノードを結ぶ「belongs to」というラベルの矢印は、これらが同じノードに属することを示します。たとえば、MACアドレスとホストの間の矢印に「belongs to」のラベルがある場合、MACアドレスがホストのものであることを示します。

矢印の線が太いほど、ノード間の通信が多いことを示します。大きなノード (円) は、小さいノードよりもアクティビティが多いことを示します。ノードが大きいほど、より多くのイベントに出現するエンティティであることを意味します。

次のノード グラフの例には、10個のノードがあります。

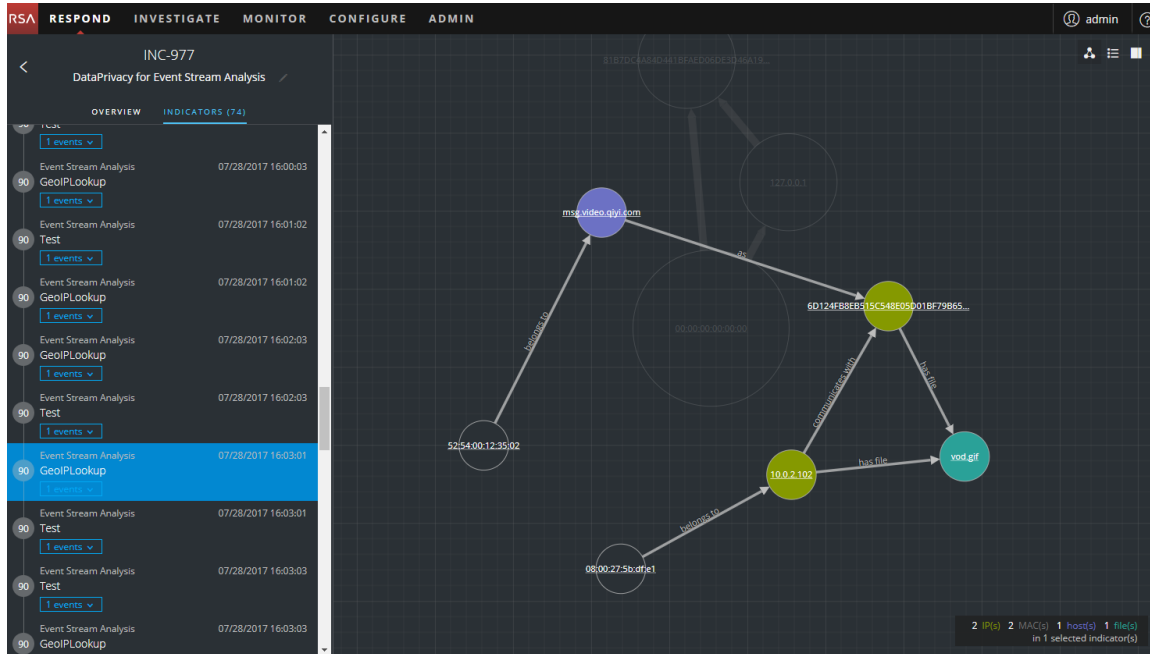


この例には、アクティビティの多い2つのIPノードがあります。どちらもファイルを持ちますが、相互に通信しません。上方のIPアドレス(192.168.1.1)は、example.comドメイン内の2つのホスト名(host.example.comとINENDEBS1L2C)を持つ1台のマシンを表します。マシンのMACアドレスは11-11-11-11-11-11-11-11-11で、Aliceが使用しています。

[インシデントの詳細]ビューでのデータのフィルタ処理

[インジケータ]パネルでインジケータをクリックして、ノード グラフとイベント リストに表示する情報をフィルタ処理することができます。

インジケータを選択しノード グラフをフィルタ処理すると、次の図のように、選択されていないデータはグレー表示されますが、グラフ内に残ります。



インジケータを選択しイベント リストをフィルタ処理すると、そのインジケータのイベントのみがリストに表示されます。次の図は、2つのイベントを含むインジケータを選択したものです。イベントのリストはフィルタ処理され、これら2つのイベントが表示されます。

TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION P...	DESTINATION HOST
08/04/2017 12:18:42.000	Network	127.0.0.1	41567		00:00:00:00:00:00		81B7DC4484D4...	4369	
08/04/2017 12:19:42.000	Network	127.0.0.1	55779		00:00:00:00:00:00		81B7DC4484D4...	4369	

インジケータを選択してイベント リストをフィルタ処理する場合、インジケータに1つのイベントしか含まれない場合は、次の図に示すように、そのイベントの詳細が表示されます。

The screenshot displays the NetWitness Respond interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The user 'admin' is logged in. The main content area is titled 'INC-1136' and 'High Risk Alerts: Reporting Engine for 70.0'. A list of alerts is shown on the left, with the selected event 'Malicious IP - Reporting Engine' highlighted in blue. The right pane shows 'Event Details' for the timestamp '08/04/2017 12:17:42'.

Event Details: 08/04/2017 12:17:42

Timestamp: 08/04/2017 12:17:42.000 (10 hours ago)

Type: Network

Source: Device Port 60898
 MAC Address 00:00:00:00:00:00
 IP Address 127.0.0.1
 Geolocation

Destination: Device Port 4369
 MAC Address 00:00:00:00:00:00
 IP Address 81B7DC4A84D441BFACD060E3D46A19C49D17B4157FBCC0DE888FD7D21A27E77
 Geolocation


Detector: 1336

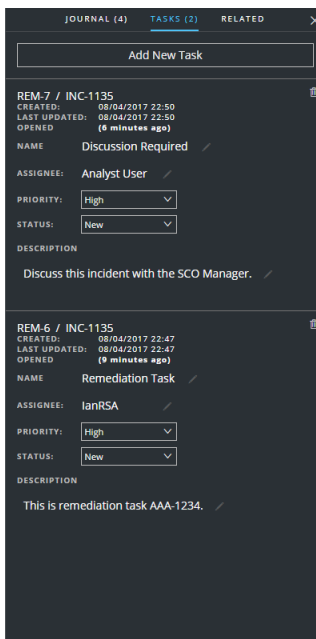
Data: Size 1336

Related Links: Type Investigate_original_event
 URL /investigation/hosts/10.4.61.30:56005/navigate/event/AUTO/462091

インシデントに関連するタスクの表示

脅威の対応者やその他のアナリストは、インシデントのタスクを作成し、それらのタスクを完了するまでトラッキングできます。これは、たとえば、インシデントの解決にSOCチーム以外のアクションが必要なときなどに非常に役に立ちます。[インシデントの詳細]ビューで、インシデントに関連するタスクを表示することができます。


1. [対応]>[インシデント]の順に移動し、インシデントのリストで表示するインシデントを検索します。
2. インシデントの[ID]または[名前]フィールドのリンクをクリックして、[インシデントの詳細]ビューに移動します。
3. [インシデントの詳細]ビューのツールバーでをクリックします。
[ジャーナル]パネルが表示されます。
4. [タスク]タブをクリックします。
[タスク]パネルに、インシデントのすべてのタスクが表示されます。

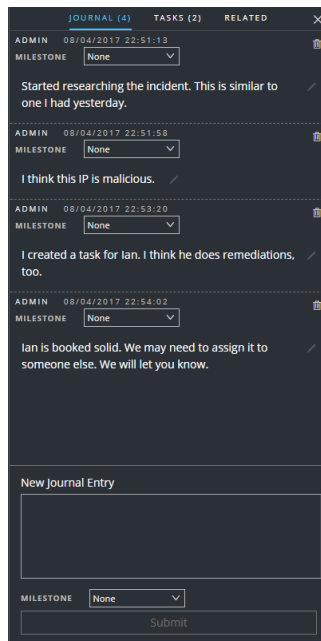


タスクの詳細については、「[タスクリストビュー](#)」、「[すべてのインシデントタスクの表示](#)」、「[タスクの作成](#)」を参照してください。

インシデント メモの表示

インシデントの[ジャーナル]では、インシデントのアクティビティの履歴を表示することができます。他のアナリストが追加したジャーナル エントリを表示でき、他のアナリストととの通信やコラボレーションのために使用できます。


1. [対応]>[インシデント]の順に移動し、インシデントのリストで表示するインシデントを検索します。
2. インシデントの[ID]または[名前]フィールドのリンクをクリックして、[インシデントの詳細]ビューに移動します。
3. [インシデントの詳細]ビューのツールバーでをクリックします。
[ジャーナル]パネルにインシデントのすべてのジャーナル エントリが表示されます。

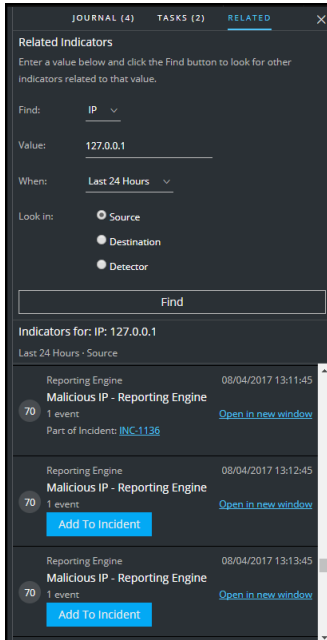


関連インジケータの検索

関連インジケータは、元々選択したインシデントには含まれていませんが、何らかの形で関連しているアラートです。関連が明らかな場合も、明らかでない場合もあります。たとえば、関連インジケータには、インシデントの1つまたは複数のエンティティが関与している場合もありますが、NetWitness Suiteの外部のインテリジェンスによって関連が示される場合もあります。

[インシデントの詳細]ビューの[関連インジケータ]パネルでは、現在のインシデント以外の他のアラートのエンティティ(IP、MAC、ホスト、ドメイン、ユーザ、ファイル名、ハッシュなど)を検索できます。

1. [対応]>[インシデント]の順に移動し、インシデントのリストで表示するインシデントを検索します。
2. インシデントの[ID]または[名前]フィールドのリンクをクリックして、[インシデントの詳細]ビューに移動します。
3. [インシデントの詳細]ビューのツールバーでをクリックします。
[ジャーナル]パネルが右側に表示されます。
4. [関係]タブをクリックします。



5. [関連インジケータ]パネルで、検索条件を入力します。
 - **検索**: アラート内で検索するエンティティを選択します。たとえば、[IP]を選択します。
 - **値**: エンティティの値を入力します。たとえば、エンティティの実際のIPアドレスを入力します。
 - **期間**: アラートを検索する時間範囲を選択します。たとえば、[直近24時間]を選択します。
 - **検査**: 検索するエンティティのタイプを指定します。
 ソース: 2台のマシン間のトランザクションのソースマシン。
 宛先: 2台のマシン間のトランザクションの宛先マシン。
 検知器: 異常が検出された1台のマシン。
 ドメイン: このオプションは、[検索]フィールドで[ドメイン]を選択すると使用可能です。

 たとえば、特定のIPアドレスがソースデバイスになっているアラートを検索する場合は、

[ソース]を選択します。次のデバイスのタイプごとに検索することができます: ソース、宛先、検知器

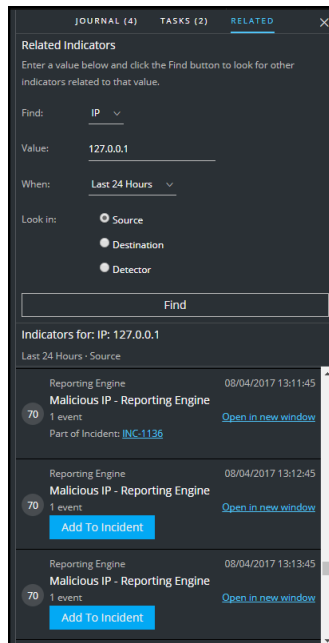
6. [検索]をクリックします。

関連インジケータ(アラート)のリストが、[検索]ボタンの下の[以下を示すインジケータ]セクションに表示されます。アラートが他のインシデントの一部でない場合は、[インシデントへの追加]ボタンをクリックして現在のインシデントに関連インジケータ(アラート)を追加することができます。後述の「[インシデントへの関連インジケータの追加](#)」を参照してください。

インシデントへの関連インジケータの追加

[関連インジケータ]パネルから、現在のインシデントに関連インジケータ(アラート)を追加できます。すでにインシデントの一部になっているインジケータは、他のインシデントに追加することはできません。アラートがまだインシデントの一部ではない場合は、検索結果に[インシデントへの追加]ボタンが表示されます。

1. [関連インジケータ]パネルで、関連インジケータを検索します。前述の「[関連インジケータの検索](#)」を参照してください。



2. 検索結果でアラートを確認します。[検索]ボタンの下の[以下を示すインジケータ]セクションに、関連インジケータ(アラート)のリストが表示されます。
3. アラートを関連インジケータとしてインシデントに追加する前に、詳細を調査するには、[新規ウィンドウで開く]リンクをクリックしてそのアラートの詳細を表示することができます。

4. 関連インジケータとして現在のインシデントに追加する各アラートで、[インシデントへの追加] ボタンをクリックします。

左側の[インジケータ]パネルに、選択した関連インジケータが追加されます。右側の[関連インジケータ]パネルのボタンの表示が、このインシデント生成]に変わります。

The screenshot displays the NetWitness Respond interface. The main window is titled 'INC-1135' and shows a list of 82 events. The left sidebar contains a list of indicators, with the bottom item 'Reporting Engine Malicious IP - Reporting Engine' selected and highlighted in red. The right sidebar shows the 'Related Indicators' panel, which includes a search field and a list of indicators. The bottom indicator in this list is also highlighted in red and has an 'Add To Incident' button. A red arrow points from the 'Add To Incident' button in the right sidebar to the selected indicator in the left sidebar.

TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER
Network	127.0.0.1	51135		00:00:00:00:00:00	
Network	127.0.0.1	40263		00:00:00:00:00:00	
Network	127.0.0.1	46015		00:00:00:00:00:00	
Network	127.0.0.1	39175		00:00:00:00:00:00	
Network	127.0.0.1	38229		00:00:00:00:00:00	
Network	127.0.0.1	41286		00:00:00:00:00:00	
Network	127.0.0.1	40504		00:00:00:00:00:00	
Network	127.0.0.1	54078		00:00:00:00:00:00	
Network	127.0.0.1	54106		00:00:00:00:00:00	
Network	127.0.0.1	54130		00:00:00:00:00:00	
Network	127.0.0.1	54142		00:00:00:00:00:00	
Network	127.0.0.1	54158		00:00:00:00:00:00	
Network	127.0.0.1	42204		00:00:00:00:00:00	
Network	127.0.0.1	57357		00:00:00:00:00:00	
Network	127.0.0.1	40070		00:00:00:00:00:00	
Network	127.0.0.1	32889		00:00:00:00:00:00	
Network	127.0.0.1	54186		00:00:00:00:00:00	
Network	127.0.0.1	58544		00:00:00:00:00:00	
Network	127.0.0.1	33125		00:00:00:00:00:00	

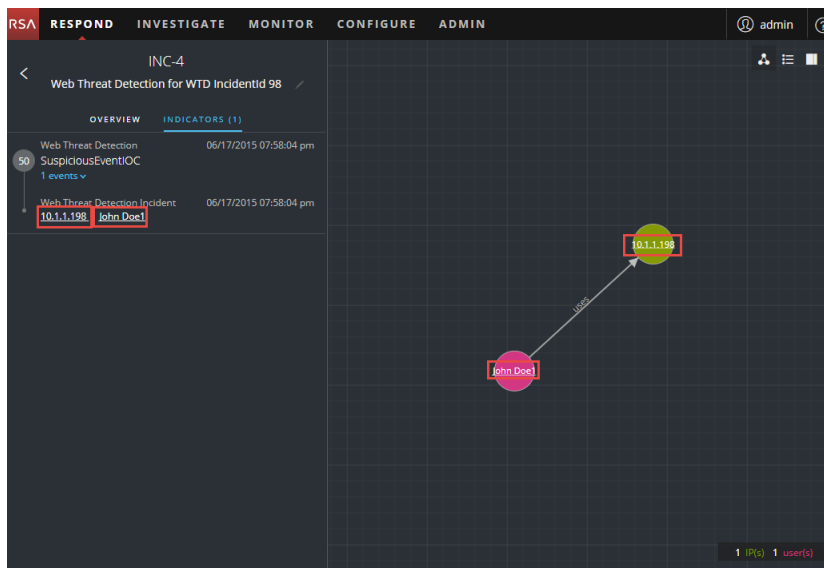
インシデントの調査

[インシデントの詳細]ビューには、インシデントをさらに詳しく調査するため、インシデントに関する追加のコンテキスト情報に移動するリンクが表示されます(情報がある場合)。この追加のコンテキストは、インシデントの特定のエンティティに関する技術的コンテキストとビジネスコンテキストを理解するのに役立ちます。インシデントの全体像を確実に把握するために必要となる追加の情報も提供されます。

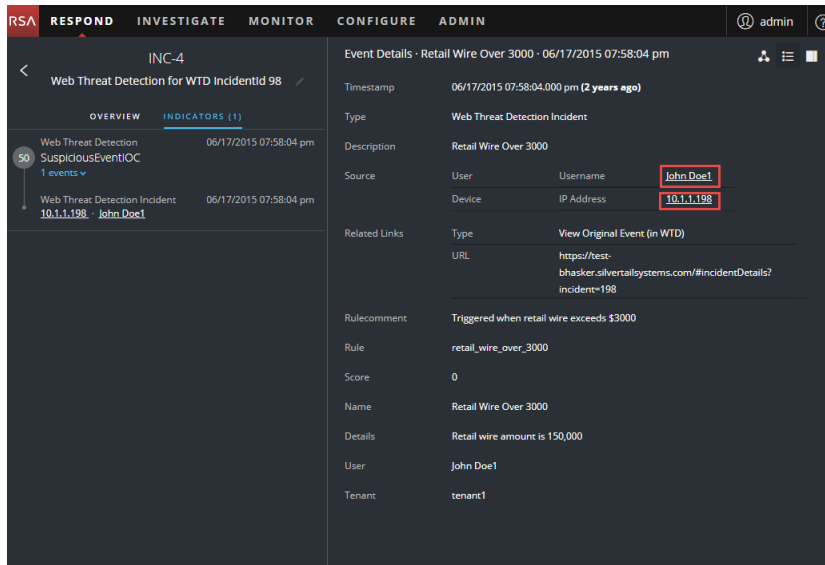
コンテキスト情報の表示

[インジケータ]パネル、[イベント リスト]パネル、[イベントの詳細]パネル、ノード グラフには、下線付きのエンティティが表示されます。エンティティに下線がある場合、NetWitness Suiteが Context Hubにそのエンティティタイプに関する情報を追加していることを意味します。つまり、Context Hubに、そのエンティティに関する追加情報が存在する可能性があります。

次の図は、[インジケータ]パネルとノード グラフの下線付きのエンティティを示します。



次の図は、[イベントの詳細]パネルの下線付きのエンティティを示します。

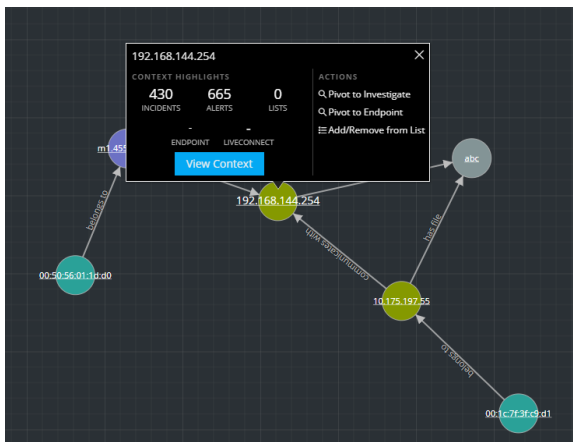


Context Hubには、エンティティとメタ フィールドのマッピングが事前構成されています。NetWitness RespondとInvestigateはコンテキスト ルックアップでこれらのデフォルトのマッピングを使用します。メタ キーを追加する方法については、「Context Hub構成ガイド」の「データ ソース設定の構成」を参照してください。

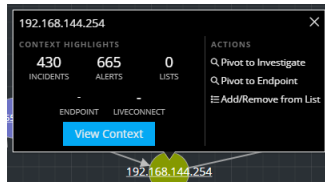
注意: コンテキスト ルックアップを[対応]ビューと[調査]ビューで正常に動作させるため、[管理] > [システム] > [Investigation] > [Context Lookup] タブでメタ キーをマッピングする際に、[Meta Key Mapping]にはメタ キーのみを追加し、MongoDBのフィールドは追加しないことを推奨します。たとえば、ip.addressはメタ キーですが、ip_addressはメタ キーではなくMongoDBのフィールドです。

コンテキスト情報を表示するには、次の手順を実行します。

1. [インジケータ]パネル、イベント リスト、イベントの詳細、ノード グラフで、下線付きのエンティティにマウスを合わせます。
コンテキスト ツールチップに、選択したエンティティで利用可能なコンテキスト データのタイプについて簡単なサマリが表示されます。



コンテキスト ツールチップには、2つのセクションがあります。[コンテキストのハイライト]と[アクション]です。



[コンテキストのハイライト]セクションの情報は、必要なアクションを判断するのに役立ちます。インシデント、アラート、リスト、Endpoint、Live Connectの関連するデータを表示できます。データによっては、これらのアイテムをクリックして詳細を確認できます。上の例は、IPアドレスエンティティ「192.168.144.254」について、430個の関連インシデント、665個のアラート、0個のリストがあり、NetWitness EndpointまたはLive Connectの情報は無いことを示しています。

[アクション]セクションでは、使用可能なアクションを示します。上の例では、[調査への移行]、[エンドポイントへの移行]、[リストへの追加/削除]オプションを使用できます。詳細については、「[調査への移行](#)」、「[NetWitness Endpointへの移行](#)」、「[ホワイト リストへのエンティティの追加](#)」を参照してください。

2. 選択したエンティティの詳細を表示するには、[コンテキストの表示] ボタンをクリックします。[コンテキスト ルックアップ] パネルが開き、エンティティに関連するすべての情報が表示されます。

次の例は、選択したソースIPアドレスのコンテキストの情報を示しています。選択したIPアドレスが含まれるすべてのインシデントが一覧表示されています。

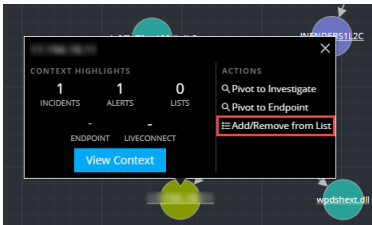
CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
07/19/2017 09:00:20 pm (6 days ago)	HIGH	80	INC-595	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:58:14 pm (6 days ago)	HIGH	80	INC-594	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:56:04 pm (6 days ago)	HIGH	80	INC-593	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:53:59 pm (6 days ago)	HIGH	80	INC-592	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:51:53 pm (6 days ago)	HIGH	80	INC-591	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:49:43 pm (6 days ago)	HIGH	80	INC-590	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:47:38 pm (6 days ago)	HIGH	80	INC-589	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:45:28 pm (6 days ago)	HIGH	80	INC-588	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:43:22 pm (6 days ago)	HIGH	80	INC-587	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:41:17 pm (6 days ago)	HIGH	80	INC-586	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:39:07 pm (6 days ago)	HIGH	80	INC-585	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:37:02 pm (6 days ago)	HIGH	80	INC-584	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:34:51 pm (6 days ago)	HIGH	80	INC-583	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:32:46 pm (6 days ago)	HIGH	80	INC-582	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:30:40 pm (6 days ago)	HIGH	80	INC-581	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:28:30 pm (6 days ago)	HIGH	80	INC-580	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:26:25 pm (6 days ago)	HIGH	80	INC-579	Suspected C&C with m1.4554mb.ru	NEW		1
07/19/2017 08:24:09 pm (6 days ago)	HIGH	80	INC-578	Suspected C&C with m1.4554mb.ru	NEW		1

Context Hubの[ルックアップ]パネル内のさまざまなビューを理解するには、「[\[コンテキスト検索\]パネル Respondビュー](#)」を参照してください。

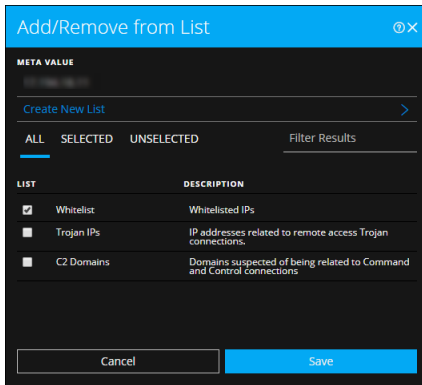
ホワイト リスト へのエンティティの追加

下線付きの任意のエンティティは、コンテキスト ツールチップから、ホワイトリストまたはブラックリストなどのリストに追加できます。たとえば、誤検知を減らすために、下線付きのドメインをホワイトリストに追加して、関連エンティティから除外します。

1. [インジケータ]パネル、イベント リスト、イベントの詳細、ノード グラフで、Context Hubのリストに追加したい下線付きのエンティティにマウスを合わせます。
コンテキスト ツールチップに使用可能なアクションが表示されます。



2. ツールチップの[アクション]セクションで、[リストへの追加/削除]をクリックします。
[リストへの追加/削除]ダイアログ ボックスに使用可能なリストが表示されます。



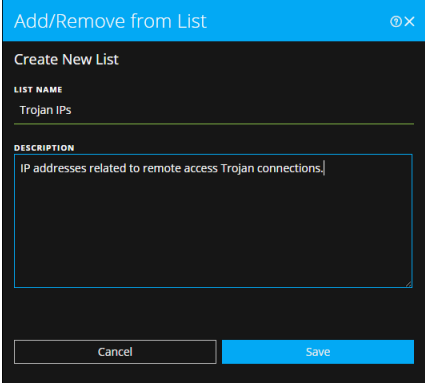
3. 1つ以上のリストを選択し、[保存]をクリックします。
エンティティが、選択したリストに表示されます。
[\[リストへの追加/削除\]ダイアログ](#)で追加情報を参照してください。

リストの作成

[対応]ビューから、Context Hubのリストを作成できます。エンティティのリストをホワイトリストおよびブラックリストとして使用するだけでなく、エンティティの異常な動作を監視するために使用できます。たとえば、調査中、疑わしいIPアドレスとドメインの可視性を高めるために、これらを2つの別々のリストに追加することができます。1つのリストは、コマンド&コントロールの接続に関連している疑いがあるドメインのリストとし、もう1つのリストは、リモートアクセスのトロイの木馬の接続に関連するIPアドレスのものとし、これらのリストを使用してセキュリティ侵害インジケータを特定できます。

Context Hubでリストを作成するには、次の手順を実行します。

1. [インジケータ]パネル、イベント リスト、イベントの詳細、ノード グラフで、Context Hubのリストに追加する下線付きのエンティティにマウスを合わせます。
コンテキスト ツールチップに使用可能なアクションが表示されます。
2. ツールチップの[アクション]セクションで、[リストへの追加/削除]をクリックします。
3. [リストへの追加/削除]ダイアログで、[新しいリストの作成]をクリックします。



4. リストの固有の[リスト名]を入力します。リスト名は大文字と小文字を区別しません。
5. (オプション) リストの[説明]を入力します。
適切な権限を持つアナリストは、他のアナリストに送信してさらに追跡と分析を行うために、CSV形式でリストをエクスポートすることもできます。詳細については、「*Context Hub構成ガイド*」を参照してください。

NetWitness Endpointへの移行

NetWitness Endpointシック クライアント アプリケーションがインストールされている場合は、コンテキスト ツールチップから起動できます。そこから、疑わしいIPアドレス、ホスト、MACアドレスをさらに調査できます。

1. [インジケータ] パネル、イベント リスト、イベントの詳細、ノード グラフで、コンテキスト ツールチップにアクセスしたい下線付きのエンティティにマウスを合わせます。
2. ツールチップの[アクション] セクションで、[エンドポイントへの移行] を選択します。
NetWitness Endpoint アプリケーションは、Web ブラウザの外で開きます。
詳細については、「*NetWitness Endpoint ユーザガイド*」を参照してください。

調査への移行

インシデントの詳細を調査するために、[調査] ビューにアクセスできます。

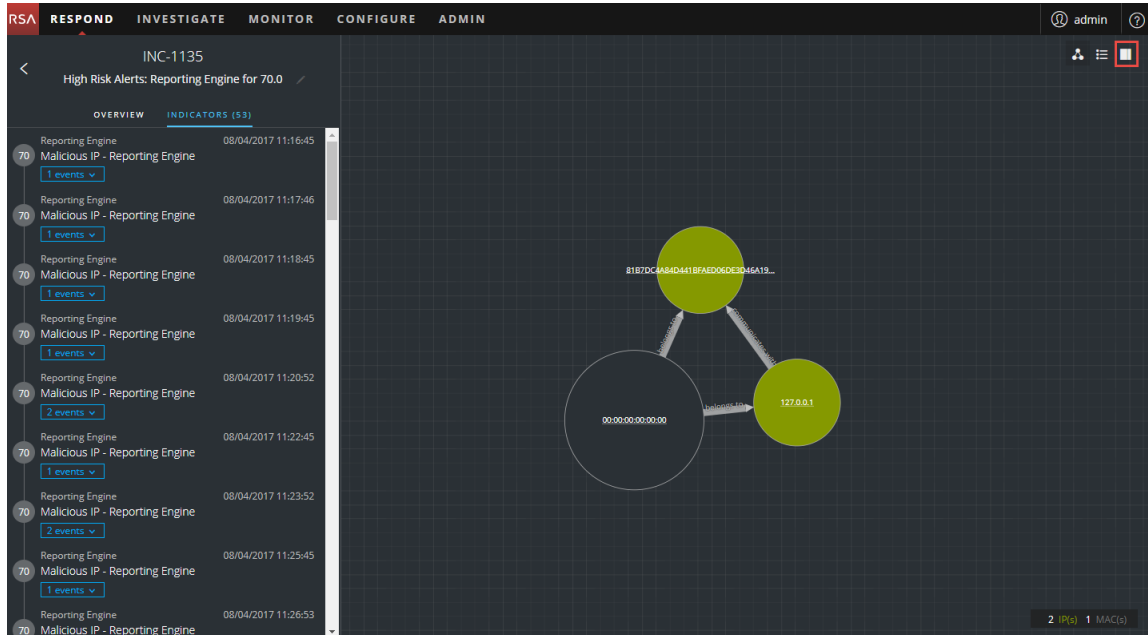
1. [インジケータ] パネル、イベント リスト、イベントの詳細、ノード グラフで、コンテキスト ツールチップにアクセスしたい下線付きのエンティティにマウスを合わせます。
2. ツールチップの[アクション] セクションで、[調査への移行] を選択します。
[調査] の[ナビゲート] ビューが開き、より詳細な調査を実行できます。
詳細については、「*調査およびマルウェア解析 ユーザガイド*」を参照してください。

NetWitnessの外で実行した手順の記録

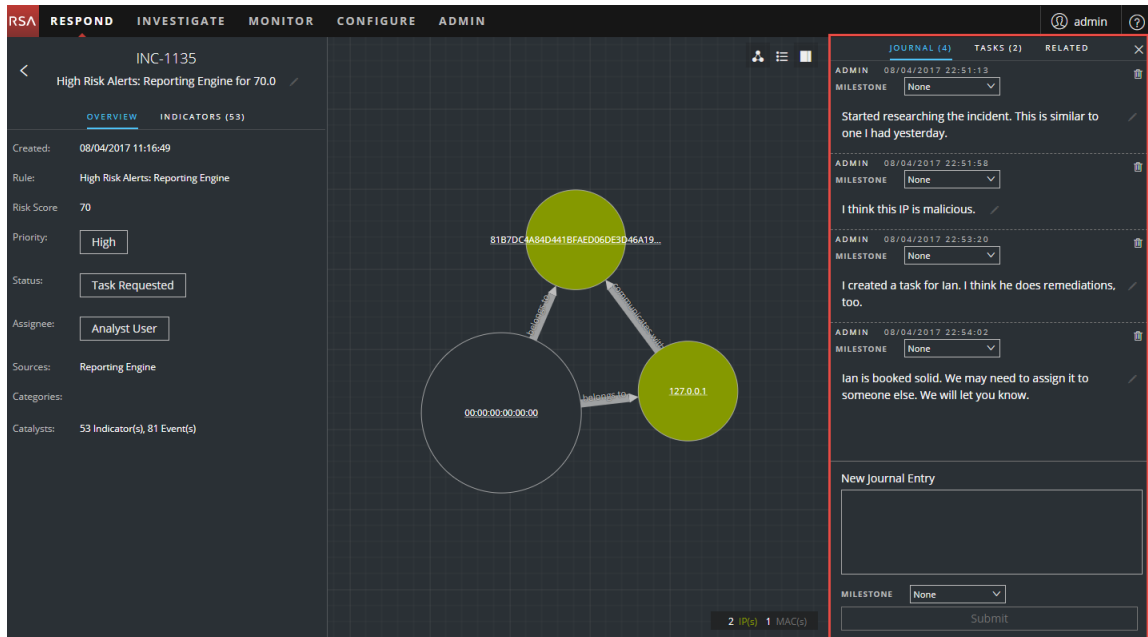
ジャーナルには、アナリストによって追加されたメモが表示され、同僚とコラボレーションすることができます。ジャーナルにメモを追加し、調査マイルストーン タグ(予備調査、配信、悪用、インスツール、コマンド & コントロール) を追加し、インシデントのアクティビティの履歴を表示できます。

インシデントのジャーナルエントリの表示

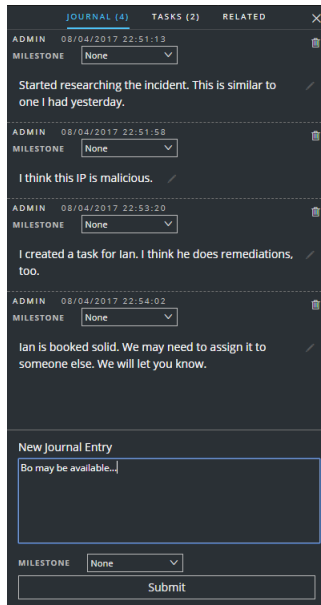
[インシデントの詳細]ビューのツールバーでをクリックします。



[インシデントの詳細]ビューの右側に[ジャーナル]が表示されます。



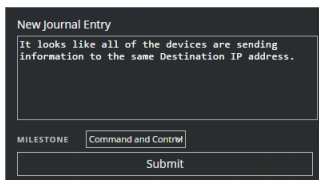
[ジャーナル] は、インシデントのアクティビティの履歴を示します。各ジャーナル エントリーの作成者と作成された時間を確認できます。



メモの追加

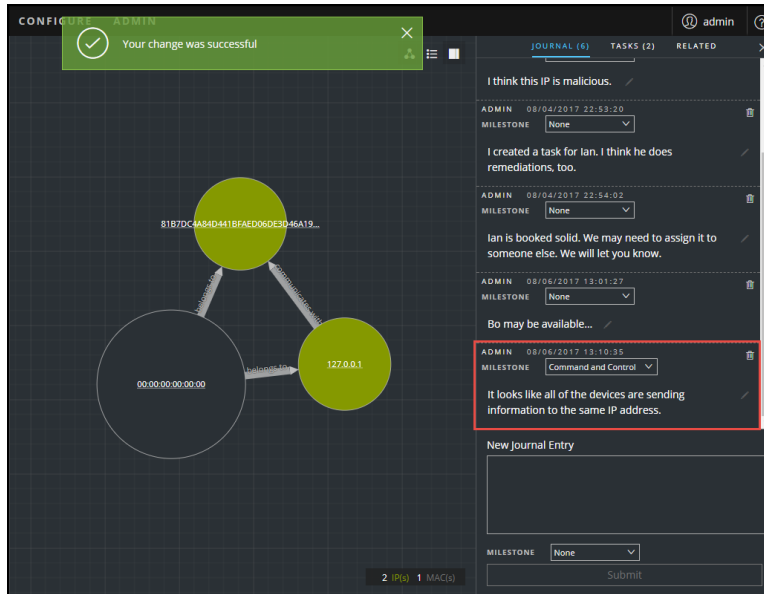
通常、他のアナリストがインシデントを把握できるようにメモを追加したり、後任者がわかるように調査手順を記録するためにメモを追加します。

1. [ジャーナル] パネルの下部で、[新しいジャーナル エントリー] ボックスにメモを入力します。




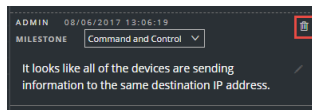
2. (オプション) ドロップダウン リストから調査マイルストーン(予備調査、配信、悪用、インストール、コマンド & コントロール、意図されたアクション、封じ込め、除去、終了) を選択します。

- メモの入力が完了したら、[送信]をクリックします。
[ジャーナル]に、新しいジャーナル エントリーが表示されます。



メモの削除

- [ジャーナル] パネルで、削除するジャーナル エントリーを見つけます。
- ジャーナル エントリーの横にあるごみ箱 (削除) アイコン をクリックします。



- 表示された確認ダイアログ ボックスで、[OK]をクリックしてジャーナル エントリーを削除することを確認します。このアクションは元に戻すことができません。

インシデントのエスカレーションまたは修正

詳細情報を収集するため、インシデントを別のアナリストに割り当てたり、インシデントのステータスと優先度を変更したりする場合があります。これは、たとえば、インシデントが主要な脆弱性であると判断した後、インシデントの優先度を中から高にアップグレードする場合に役立ちます。

インシデントの更新

インシデントは複数の場所から更新することができます。インシデントのリストビューと[インシデントの詳細]ビューからは、優先度、ステータス、割り当て先を変更できます。たとえば、アナリストの場合、取り組んでいるもう1つのケースに関連していることがわかったときにインシデントのリストビューから自分にケースを割り当てる必要があることがあります。SOCマネージャや管理者の場合、インシデントのリストビューから割り当てられていないインシデントを確認し、インシデントを発生時に割り当てる必要があることがあります。SOCマネージャと管理者は、優先度、ステータス、割り当て先を一度に1つのインシデントで更新するのではなく一括更新することができます。

詳細ビューからは、インシデントの作業を開始したらステータスを[対応中]に変更し、問題を解決した後に[クローズ]または[クローズ- False Positive]に更新する必要がある場合があります。または、ケースの詳細を判別したときに、インシデントの優先度を中または高に変更する必要がある場合があります。

インシデント ステータスの変更

インシデントはインシデントのリストに最初に表示されるとき、初期のステータスは新規になります。インシデントでの作業を完了すると、ステータスを更新できます。次のステータスが選択可能です。

- 新規
- 割り当て済み
- 対応中
- タスクリクエスト中
- タスク完了
- クローズ
- クローズ- False Positive

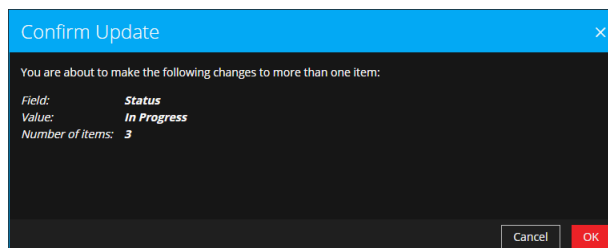
複数のインシデントのステータスを更新するには、次の手順を実行します。

1. インシデントのリストビューで、変更する1つまたは複数のインシデントを選択します。ページのすべてのインシデントを選択するには、インシデントのリストのヘッダー行でボックスを選択します。選択したインシデントの数は、インシデントリストのフッターに表示されます。
2. [ステータス変更]をクリックし、ドロップダウンリストからステータスを選択します。この例では、現在のステータスは[割り当て済み]ですが、アナリストは選択したインシデントのステータスを[対応中]に変更します。

CREATED	STATUS	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 19:00	In Progress	0	INC-1137	Investigate - IP	Assigned	Analyst User	3
08/04/2017 12:16	Task Requested	0	INC-1136	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	48
08/04/2017 11:16	Task Complete	0	INC-1135	High Risk Alerts: Reporting Engine for 70.0	Task Requested	Analyst User	53
08/04/2017 10:16	Closed	0	INC-1134	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	54
08/04/2017 09:15:47	Closed - False Positive	70	INC-1133	High Risk Alerts: Reporting Engine for 70.0	New		52
08/04/2017 08:15:47	HIGH	70	INC-1132	High Risk Alerts: Reporting Engine for 70.0	New		46
08/04/2017 07:15:49	HIGH	70	INC-1131	High Risk Alerts: Reporting Engine for 70.0	New		48
08/04/2017 06:15:49	HIGH	70	INC-1130	High Risk Alerts: Reporting Engine for 70.0	New		44
08/04/2017 05:14:54	HIGH	70	INC-1129	High Risk Alerts: Reporting Engine for 70.0	New		51
08/04/2017 04:14:48	HIGH	70	INC-1128	High Risk Alerts: Reporting Engine for 70.0	New		57
08/04/2017 03:14:46	HIGH	70	INC-1127	High Risk Alerts: Reporting Engine for 70.0	New		54
08/04/2017 02:13:47	HIGH	70	INC-1126	High Risk Alerts: Reporting Engine for 70.0	New		58
08/04/2017 01:13:49	HIGH	70	INC-1125	High Risk Alerts: Reporting Engine for 70.0	New		60
08/04/2017 00:13:45	HIGH	70	INC-1124	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 23:13:45	HIGH	70	INC-1123	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 22:13:49	HIGH	70	INC-1122	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 21:13:47	HIGH	70	INC-1121	High Risk Alerts: Reporting Engine for 70.0	New		60

Showing 1000 out of 1115 items | 3 selected

3. 複数のインシデントを選択した場合、[更新の確認]ダイアログで[OK]をクリックします。



変更が成功した通知が表示されます。この例では、更新されたインシデントのステータスが

[対応中]と表示されています。

The screenshot shows the NetWitness Respond interface with a notification 'Your change was successful'. Below the notification is a table of incidents. The 'STATUS' column for several incidents is highlighted in red, indicating they are 'In Progress'.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 19:00:32	LOW	0	INC-1137	Investigate - IP	In Progress	Analyst User	3
08/04/2017 12:16:48	HIGH	70	INC-1136	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	48
08/04/2017 11:16:49	HIGH	70	INC-1135	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	53
08/04/2017 10:16:49	HIGH	70	INC-1134	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	54
08/04/2017 09:15:47	HIGH	70	INC-1133	High Risk Alerts: Reporting Engine for 70.0	New		52
08/04/2017 08:15:47	HIGH	70	INC-1132	High Risk Alerts: Reporting Engine for 70.0	New		46
08/04/2017 07:15:49	HIGH	70	INC-1131	High Risk Alerts: Reporting Engine for 70.0	New		48
08/04/2017 06:15:49	HIGH	70	INC-1130	High Risk Alerts: Reporting Engine for 70.0	New		44
08/04/2017 05:14:54	HIGH	70	INC-1129	High Risk Alerts: Reporting Engine for 70.0	New		51
08/04/2017 04:14:48	HIGH	70	INC-1128	High Risk Alerts: Reporting Engine for 70.0	New		57
08/04/2017 03:14:46	HIGH	70	INC-1127	High Risk Alerts: Reporting Engine for 70.0	New		54
08/04/2017 02:13:47	HIGH	70	INC-1126	High Risk Alerts: Reporting Engine for 70.0	New		58
08/04/2017 01:13:49	HIGH	70	INC-1125	High Risk Alerts: Reporting Engine for 70.0	New		60
08/04/2017 00:13:45	HIGH	70	INC-1124	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 23:13:45	HIGH	70	INC-1123	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 22:13:49	HIGH	70	INC-1122	High Risk Alerts: Reporting Engine for 70.0	New		60

[概要]パネルから1つのインシデントのステータスを変更するには、次の手順を実行します。

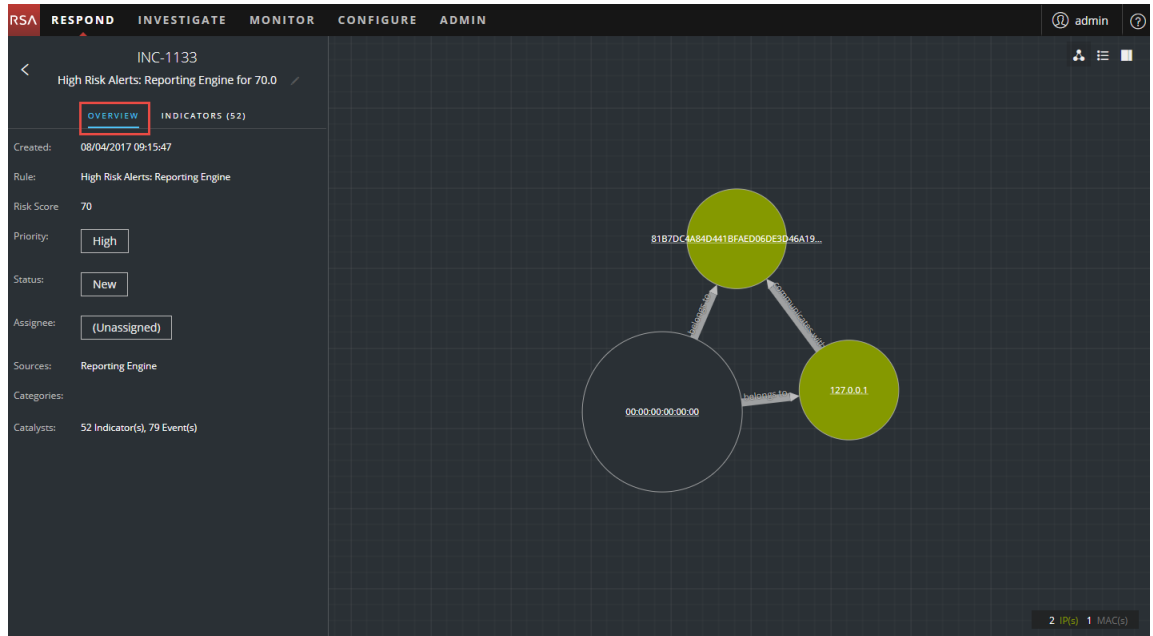
1. [概要]パネルを開くには、次のいずれかの操作を行います。

- インシデントのリストビューから、ステータス更新の必要があるインシデントをクリックします。

The screenshot shows the NetWitness Respond interface with the 'Overview' panel for incident INC-1134. The panel displays details such as Created, Rule, Risk Score, Priority, Status, Assignee, Sources, and Categories.

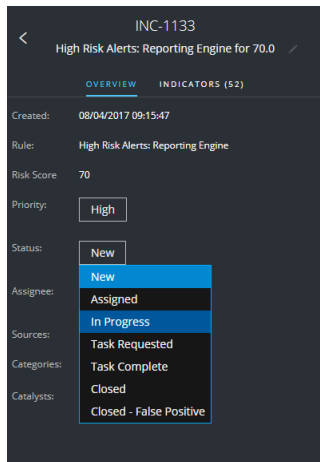
CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 19:00:32	LOW	0	INC-1137	Investigate - IP	In Progress	Analyst User	3
08/04/2017 12:16:48	HIGH	70	INC-1136	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	48
08/04/2017 11:16:49	HIGH	70	INC-1135	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	53
08/04/2017 10:16:49	HIGH	70	INC-1134	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	54
08/04/2017 09:15:47	HIGH	70	INC-1133	High Risk Alerts: Reporting Engine for 70.0	New		52
08/04/2017 08:15:47	HIGH	70	INC-1132	High Risk Alerts: Reporting Engine for 70.0	New		46
08/04/2017 07:15:49	HIGH	70	INC-1131	High Risk Alerts: Reporting Engine for 70.0	New		48
08/04/2017 06:15:49	HIGH	70	INC-1130	High Risk Alerts: Reporting Engine for 70.0	New		44
08/04/2017 05:14:54	HIGH	70	INC-1129	High Risk Alerts: Reporting Engine for 70.0	New		51
08/04/2017 04:14:48	HIGH	70	INC-1128	High Risk Alerts: Reporting Engine for 70.0	New		57
08/04/2017 03:14:46	HIGH	70	INC-1127	High Risk Alerts: Reporting Engine for 70.0	New		54
08/04/2017 02:13:47	HIGH	70	INC-1126	High Risk Alerts: Reporting Engine for 70.0	New		58
08/04/2017 01:13:49	HIGH	70	INC-1125	High Risk Alerts: Reporting Engine for 70.0	New		60
08/04/2017 00:13:45	HIGH	70	INC-1124	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 23:13:45	HIGH	70	INC-1123	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 22:13:49	HIGH	70	INC-1122	High Risk Alerts: Reporting Engine for 70.0	New		60

- [インシデントの詳細]ビューで、[概要]タブをクリックします。



[概要]パネルでは、[ステータス]ボタンにインシデントの現在のステータスが表示されます。

2. [ステータス]ボタンをクリックし、ドロップダウンリストからステータスを選択します。



変更が成功した通知が表示されます。



インシデント優先度の変更

インシデントのリストはデフォルトでは優先度でソートされています。優先度はケースの詳細を調査するときに更新できます。次の優先度が選択可能です。

- クリティカル
- 高
- 中
- 低

注: クローズしたインシデントの優先度を変更することはできません。

複数のインシデントの優先度を更新するには、次の手順を実行します。

1. インシデントのリストビューで、変更する1つまたは複数のインシデントを選択します。ページのすべてのインシデントを選択するには、インシデントのリストのヘッダー行でボックスを選択します。選択したインシデントの数は、インシデントリストのフッターに表示されます。
2. [優先度の変更]をクリックし、ドロップダウンリストから優先度を選択します。この例では、現在の優先度は[高]ですが、アナリストは選択したインシデントの優先度を[クリティカル]に変更します。

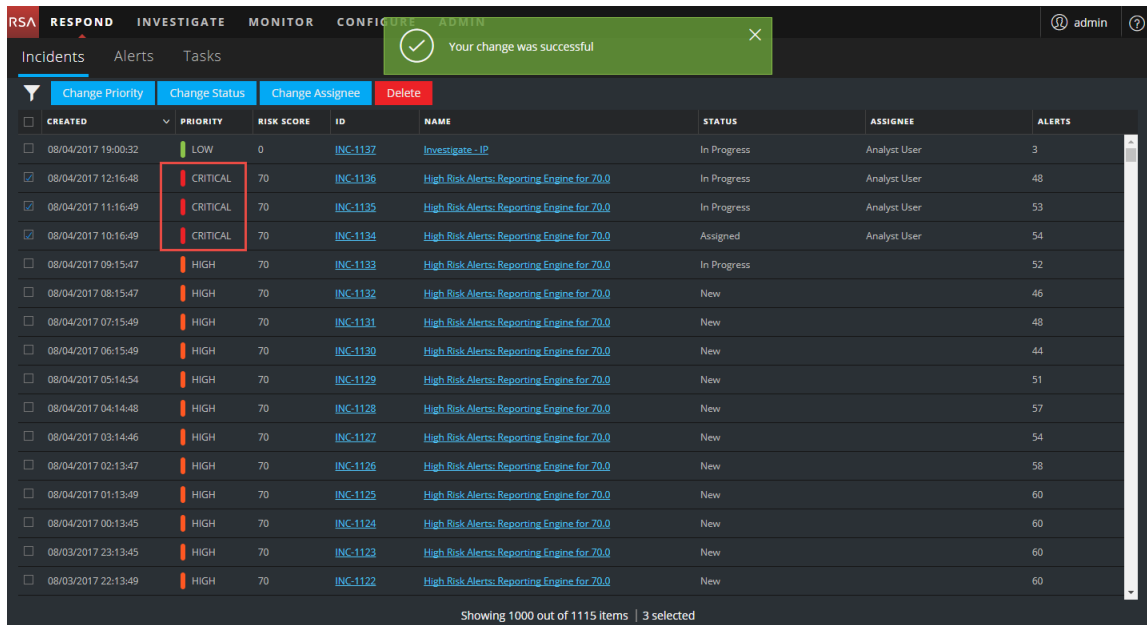
The screenshot shows the NetWitness Respond interface with the 'Incidents' tab selected. A dropdown menu is open over the 'Change Priority' button, showing options: Low, Medium, High, and Critical. The 'High' option is currently selected. The table below shows a list of incidents with columns for Created, Priority, Risk Score, ID, Name, Status, Assignee, and Alerts.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 11:16:49	HIGH	70	INC-1137	Investigate - IP	In Progress	Analyst User	3
08/04/2017 08:15:47	HIGH	70	INC-1136	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	48
08/04/2017 07:15:49	HIGH	70	INC-1135	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	53
08/04/2017 06:15:49	HIGH	70	INC-1134	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	54
08/04/2017 05:14:54	HIGH	70	INC-1133	High Risk Alerts: Reporting Engine for 70.0	In Progress		52
08/04/2017 04:14:48	HIGH	70	INC-1132	High Risk Alerts: Reporting Engine for 70.0	New		46
08/04/2017 03:14:46	HIGH	70	INC-1131	High Risk Alerts: Reporting Engine for 70.0	New		48
08/04/2017 02:13:47	HIGH	70	INC-1130	High Risk Alerts: Reporting Engine for 70.0	New		44
08/04/2017 01:13:49	HIGH	70	INC-1129	High Risk Alerts: Reporting Engine for 70.0	New		51
08/04/2017 00:13:45	HIGH	70	INC-1128	High Risk Alerts: Reporting Engine for 70.0	New		57
08/04/2017 00:13:45	HIGH	70	INC-1127	High Risk Alerts: Reporting Engine for 70.0	New		54
08/04/2017 00:13:45	HIGH	70	INC-1126	High Risk Alerts: Reporting Engine for 70.0	New		58
08/04/2017 00:13:45	HIGH	70	INC-1125	High Risk Alerts: Reporting Engine for 70.0	New		60
08/04/2017 00:13:45	HIGH	70	INC-1124	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 23:13:45	HIGH	70	INC-1123	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 22:13:49	HIGH	70	INC-1122	High Risk Alerts: Reporting Engine for 70.0	New		60

Showing 1000 out of 1115 items | 3 selected

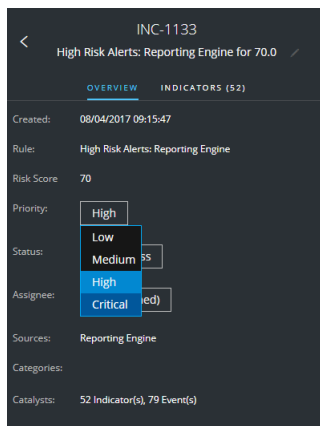
3. 複数のインシデントを選択した場合、[更新の確認]ダイアログで[OK]をクリックします。変更が成功した通知が表示されます。この例では、更新されたインシデントのステータスが

[クリティカル]と表示されています。



[概要]パネルから1つのインシデントの優先度を変更するには、次の手順を実行します。

- [概要]パネルを開くには、次のいずれかの操作を行います。
 - インシデントのリストビューから、優先度更新の必要があるインシデントをクリックします。
 - [インシデントの詳細]ビューで、[概要]タブをクリックします。
[概要]パネルでは、[優先度]ボタンにインシデントの現在の優先度が表示されます。
- [優先度]ボタンをクリックし、ドロップダウンリストからステータスを選択します。



変更が成功した通知が表示されます。新しいインシデントの優先度を表示するように[優先度]ボタンが変更されます。



その他のアナリストへのインシデントの割り当て

インシデントを自分自身に割り当てるときと同じ方法でその他のアナリストにインシデントを割り当てることができます。SOC マネージャや管理者は同時に複数のインシデントをユーザに割り当てることができます。

注: クローズしたインシデントの割り当て先を変更することはできません。

ユーザに複数のインシデントを割り当てるには、次の手順を実行します。

1. インシデントのリスト ビューで、ユーザに割り当てるインシデントを選択します。ページのすべてのインシデントを選択するには、インシデントのリストのヘッダー行でボックスを選択します。選択したインシデントの数は、インシデント リストのフッターに表示されます。
2. [割り当て先の変更] をクリックし、ドロップダウン リストからユーザを選択します。この例では、インシデントは割り当てられていませんが、アナリストに割り当てる必要があります。

The screenshot shows the NetWitness Respond interface with a table of incidents. The 'Change Assignee' button is highlighted, and a dropdown menu is open, showing a list of analyst users. The table columns include 'CREATED', 'PRIORITY', 'ID', 'NAME', 'STATUS', 'ASSIGNEE', and 'ALERTS'. The incidents listed are all 'High Risk Alerts: Reporting Engine for 70.0' with various creation times and IDs.

CREATED	PRIORITY	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 19:00:32	LOW	INC-1137	Investigate - IP	New		3
08/04/2017 12:16:48	HIGH	INC-1136	High Risk Alerts: Reporting Engine for 70.0	New		48
08/04/2017 11:16:49	HIGH	INC-1135	High Risk Alerts: Reporting Engine for 70.0	New		52
08/04/2017 10:16:49	HIGH	INC-1134	High Risk Alerts: Reporting Engine for 70.0	New		54
08/04/2017 09:15:47	HIGH	INC-1133	High Risk Alerts: Reporting Engine for 70.0	New		52
08/04/2017 08:15:47	HIGH	INC-1132	High Risk Alerts: Reporting Engine for 70.0	New		46
08/04/2017 07:15:49	HIGH	INC-1131	High Risk Alerts: Reporting Engine for 70.0	New		48
08/04/2017 06:15:49	HIGH	INC-1130	High Risk Alerts: Reporting Engine for 70.0	New		44
08/04/2017 05:14:54	HIGH	INC-1129	High Risk Alerts: Reporting Engine for 70.0	New		51
08/04/2017 04:14:48	HIGH	INC-1128	High Risk Alerts: Reporting Engine for 70.0	New		57
08/04/2017 03:14:46	HIGH	INC-1127	High Risk Alerts: Reporting Engine for 70.0	New		54
08/04/2017 02:13:47	HIGH	INC-1126	High Risk Alerts: Reporting Engine for 70.0	New		58
08/04/2017 01:13:49	HIGH	INC-1125	High Risk Alerts: Reporting Engine for 70.0	New		60
08/04/2017 00:13:45	HIGH	INC-1124	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 23:13:45	HIGH	INC-1123	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 22:13:49	HIGH	INC-1122	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 21:13:47	HIGH	INC-1121	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 20:13:48	HIGH	INC-1120	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 20:06:47	HIGH	INC-1119	High Risk Alerts: Reporting Engine for 70.0	Task Requested		7

Showing 1000 out of 1115 items | 4 selected

- 複数のインシデントを選択した場合、[更新の確認]ダイアログで[OK]をクリックします。変更が成功した通知が表示されます。割り当て先が選択したユーザーに変更されます。

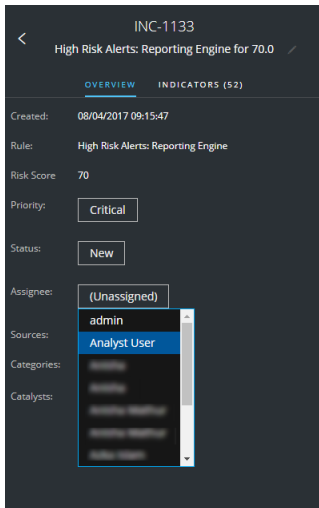
The screenshot shows the NetWitness Respond interface with a table of incidents. A green notification banner at the top states "Your change was successful". The table has columns for CREATED, PRIORITY, RISK SCORE, ID, NAME, STATUS, ASSIGNEE, and ALERTS. The ASSIGNEE column is highlighted with a red box, showing "Analyst User" for several rows. The table footer indicates "Showing 1000 out of 1115 items | 4 selected".

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 19:00:32	LOW	0	INC-1137	Investigate-IP	Assigned	Analyst User	3
08/04/2017 12:16:48	HIGH	70	INC-1136	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	48
08/04/2017 11:16:49	HIGH	70	INC-1135	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	52
08/04/2017 10:16:49	HIGH	70	INC-1134	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	54
08/04/2017 09:15:47	HIGH	70	INC-1133	High Risk Alerts: Reporting Engine for 70.0	New		52
08/04/2017 08:15:47	HIGH	70	INC-1132	High Risk Alerts: Reporting Engine for 70.0	New		46
08/04/2017 07:15:49	HIGH	70	INC-1131	High Risk Alerts: Reporting Engine for 70.0	New		48
08/04/2017 06:15:49	HIGH	70	INC-1130	High Risk Alerts: Reporting Engine for 70.0	New		44
08/04/2017 05:14:54	HIGH	70	INC-1129	High Risk Alerts: Reporting Engine for 70.0	New		51
08/04/2017 04:14:48	HIGH	70	INC-1128	High Risk Alerts: Reporting Engine for 70.0	New		57
08/04/2017 03:14:46	HIGH	70	INC-1127	High Risk Alerts: Reporting Engine for 70.0	New		54
08/04/2017 02:13:47	HIGH	70	INC-1126	High Risk Alerts: Reporting Engine for 70.0	New		58
08/04/2017 01:13:49	HIGH	70	INC-1125	High Risk Alerts: Reporting Engine for 70.0	New		60
08/04/2017 00:13:45	HIGH	70	INC-1124	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 23:13:45	HIGH	70	INC-1123	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 22:13:49	HIGH	70	INC-1122	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 21:13:47	HIGH	70	INC-1121	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 20:13:48	HIGH	70	INC-1120	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 20:06:47	HIGH	70	INC-1119	High Risk Alerts: Reporting Engine for 70.0	Task Requested		7
08/03/2017 19:06:48	HIGH	70	INC-1118	High Risk Alerts: Reporting Engine for 70.0	New		60

[概要]パネルからインシデントにユーザを割り当てるには、次の手順を実行します。

- [概要]パネルを開くには、次のいずれかの操作を行います。
 - インシデントのリストビューから、優先度更新の必要があるインシデントをクリックします。
 - [インシデントの詳細]ビューで、[概要]タブをクリックします。

[概要]パネルでは、[優先度]ボタンにインシデントの現在の優先度が表示されます。次の例では、[割り当て先]ボタンの現在のステータスは[未割り当て]です。



- [割り当て先]ボタンをクリックし、ドロップダウンリストからユーザを選択します。変更が成功した通知が表示されます。割り当てられたユーザを表示するように[割り当て先]ボタンが変更されます。



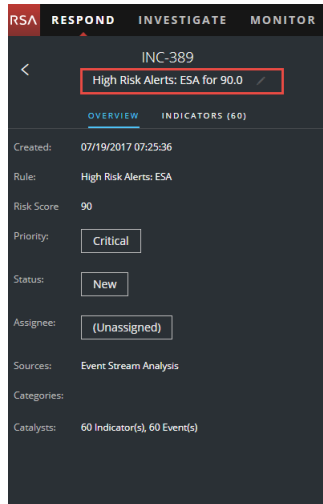
インシデントの名称変更

インシデントは、インシデントのリストビューと[インシデントの詳細]ビューの[概要]パネルから名称変更できます。たとえば、複数のインシデントの名前が同じ場合に問題について明確にするためにインシデントを名称変更する必要があることがあります。

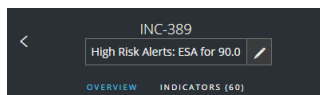
- [対応] > [インシデント]に移動します。
- [概要]パネルを開くには、次のいずれかの操作を行います。
 - インシデントのリストビューから、名前変更の必要があるインシデントをクリックします。

[概要]パネルが表示されます。

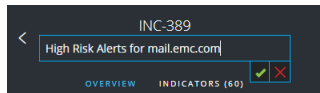
- [インシデントの詳細]ビューで、[概要]パネルに移動します。
[概要]パネルの上のヘッダーで、インシデントIDとインシデントの名前を確認できます。



3. ヘッダーでインシデントの名前をクリックし、テキスト エディタを開きます。



4. テキスト エディタでインシデントの新しい名前を入力し、チェック マークをクリックして変更を確認します。

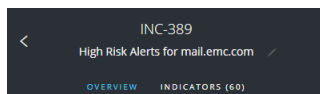


たとえば、「High Risk Alerts: ESA for 90.0」という名前を、より明確な「Alerts for mail.emc.com」に変更することができます。

変更が成功した通知が表示されます。



インシデントの名前のフィールドに新しい名前が表示されます。

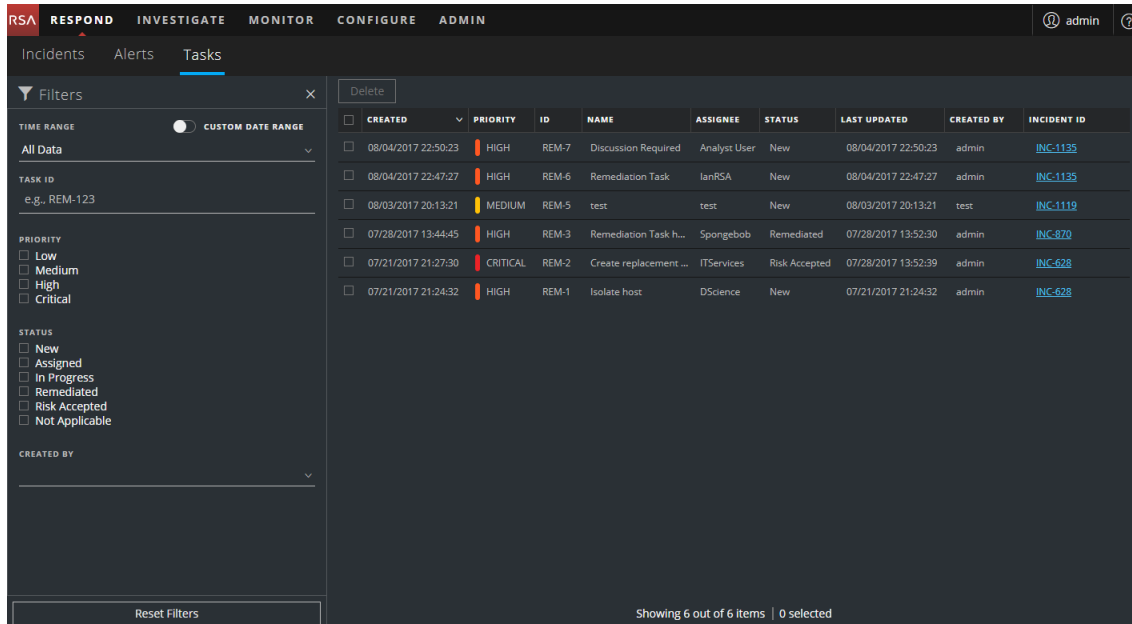


すべてのインシデント タスクの表示

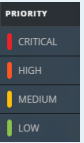
インシデントの追加作業が必要な場合は、インシデントのタスクを作成し、それらのタスクの進行状況をトラッキングすることができます。これは、たとえば、実行している作業がセキュリティオペレーションの範囲外であるときや、コンピューターの再イメージ化のリクエストを行うときに役立ちます。タスク リスト ビューでは、タスクをクローズまで管理およびトラッキングできます。

1. [対応]>[タスク]に移動します。

タスク リスト ビューに、すべてのインシデント タスクのリストが表示されます。



2. タスクのリストをスクロールすると、次の表で説明する各タスクに関する基本的な情報が表示されます。

列	説明
作成日	タスクが作成された日付が表示されます。
優先度	タスクに割り当てられた優先度が表示されます。優先度には次のいずれかを指定できます。クリティカル、高、中、低。優先度も色分けされています。次の図に示すように、赤は[クリティカル]、オレンジ色は[高]リスク、黄色は[中]リスク、緑は[低]リスクを示します。 
ID	タスクIDが表示されます。
名前	タスク名が表示されます。
割り当て先	タスクに割り当てられているユーザの名前が表示されます。


列	説明
ステータス	タスクのステータスが表示されます。[新規]、[割り当て済み]、[対応中]、[改善済み]、[リスク受容]、[該当なし]があります。
最終更新日	タスクの最終更新日時を表示します。
作成者	タスクを作成したユーザが表示されます。
インシデントID	タスクが作成されたインシデントIDが表示されます。インシデントの詳細を表示するには、IDをクリックします。

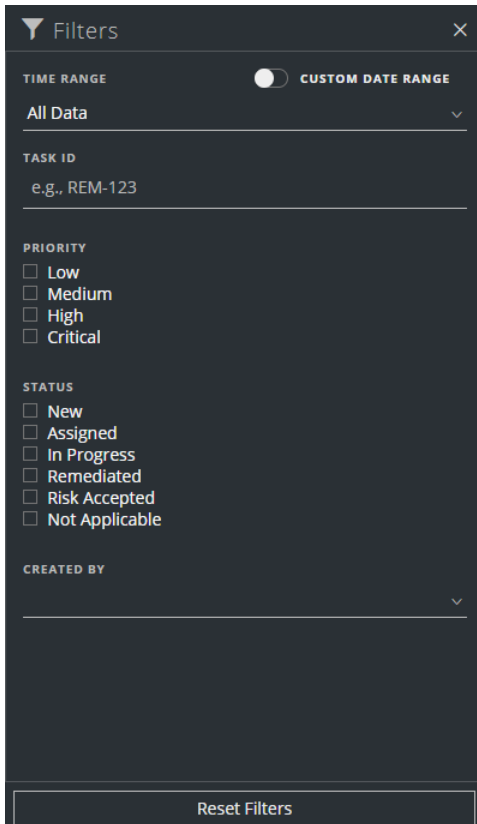
リストの下部では、現在のページのタスク数、タスクの総数、選択したタスクの数を確認できます。例:「6アイテム中6個を表示中 | 2個が選択済み」のように表示されます。

タスクリストのフィルタ

タスクリスト内のタスクの数は非常に多数になり、特定のタスクを検索することが困難になることがあります。フィルタでは、過去7日間に作成されたタスクなど、表示するタスクを指定することができます。特定のタスクを検索することもできます。

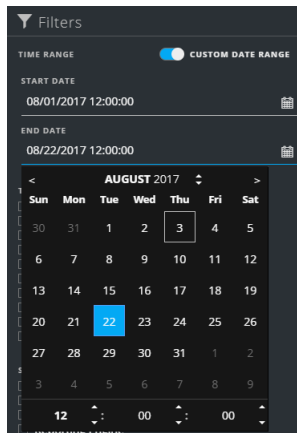
1. [対応] > [タスク] に移動します。

タスクリストの左側に[フィルタ]パネルが表示されます。[フィルタ]パネルが表示されない場合は、タスクリストビューのツールバーで  をクリックすると[フィルタ]パネルが開きます。



2. [フィルタ] パネルで1つまたは複数のオプションを選択し、インシデントのリストをフィルタします。
 - [時間範囲]: [時間範囲] ドロップダウン リストから特定の期間を選択できます。時間範囲はタスクの作成日に基づきます。たとえば、[直近1時間]を選択する場合は、過去60分以内に作成されたタスクが表示されます。
 - [カスタムの日付範囲]: [時間範囲] オプションを選択する代わりに、特定の日付範囲を指定できます。これを行うには、[カスタムの日付範囲]の前にある白色の円をクリックし、[開始日]と[終了日]のフィールドを表示します。カレンダーから日付と時刻を選択

します。



- **[タスクID]**: 検索するタスクのタスクIDを入力します(例: REM-123)。
- **[優先度]**: 表示する優先度を選択します。
- **[ステータス]**: 1つまたは複数のインシデントのステータスを選択します。たとえば、完了した改善タスクを表示するには、**[改善済み]**を選択します。
- **[作成者]**: 表示するタスクを作成したユーザーを選択します。たとえば、Edwardoによって作成されたタスクのみを表示する場合は、**[作成者]**ドロップダウンリストから**[Edwardo]**を選択します。タスクの作成者にかかわらずタスクを表示する場合は、**[作成者]**を選択しないでください。


タスクリストには、選択条件を満たすタスクのリストが表示されます。タスクリストの下部では、フィルタ処理されたリストのアイテム数を確認できます。

例: 「**6アイテム中6個を表示中**」のように表示されます

3. **[フィルタ]**パネルを閉じる場合は、**[X]**をクリックします。フィルタは、削除するまで設定されたままになります。

タスクリストからのMyフィルタの削除

NetWitness Suiteでは、タスクリストビューのフィルタ選択が記憶されます。不要な場合はフィルタ選択を削除することができます。たとえば、表示されるべきタスク数が表示されない場合や、タスクリストのすべてのタスクを表示する場合は、フィルタをリセットできます。

1. **[対応]** > **[タスク]**に移動します。
タスクリストの左側に**[フィルタ]**パネルが表示されます。**[フィルタ]**パネルが表示されない場合は、タスクリストビューのツールバーでをクリックすると**[フィルタ]**パネルが開きます。
2. **[フィルタ]**パネルの下部で**[フィルタのリセット]**をクリックします。

タスクの作成

インシデントを調査して詳細を把握したら、タスクを作成してユーザーに割り当て、クローズまでトラッキングすることができます。[インシデントの詳細]ビューからタスクを作成します。

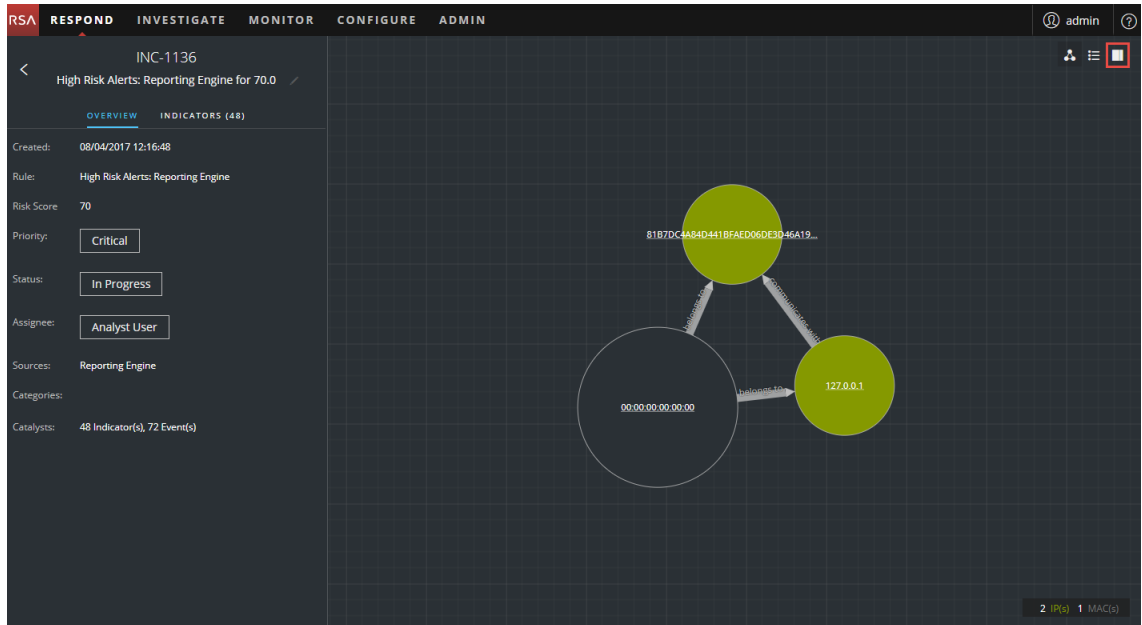
1. [対応]>[インシデント]に移動します。


インシデントのリストビューに、すべてのインシデントのリストが表示されます。

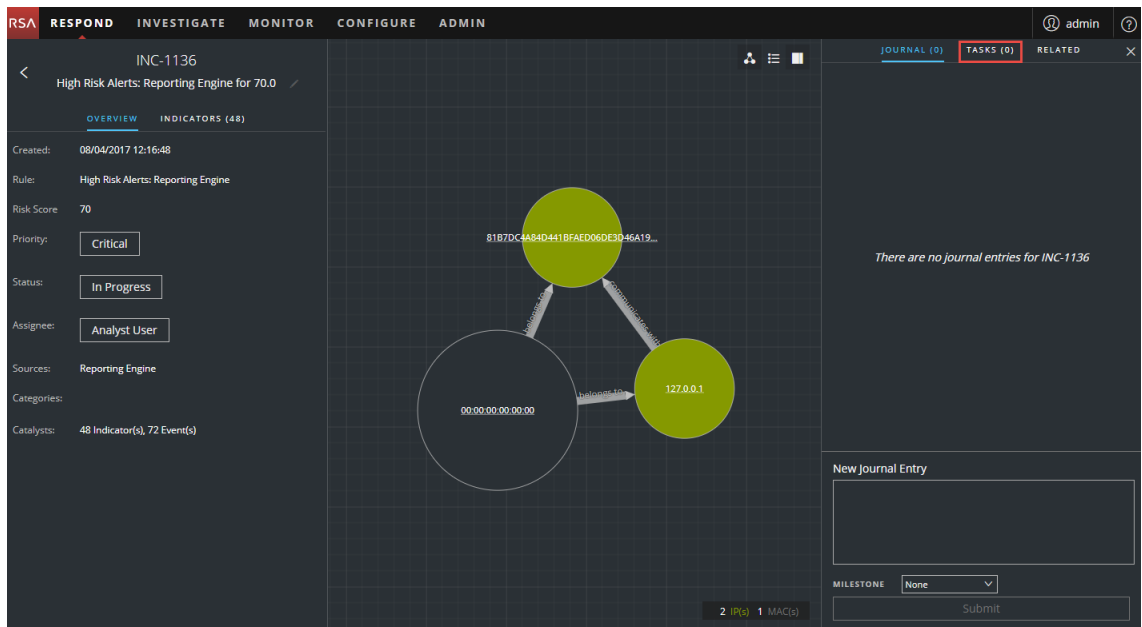
CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 19:0...	CRITICAL	0	INC-1137	Investigate -IP	In Progress	Analyst User	3
08/04/2017 12:1...	CRITICAL	70	INC-1136	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	48
08/04/2017 11:1...	CRITICAL	70	INC-1135	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	53
08/04/2017 10:1...	CRITICAL	70	INC-1134	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	54
08/04/2017 09:1...	CRITICAL	70	INC-1133	High Risk Alerts: Reporting Engine for 70.0	New		52
08/04/2017 08:1...	HIGH	70	INC-1132	High Risk Alerts: Reporting Engine for 70.0	New		46
08/04/2017 07:1...	HIGH	70	INC-1131	High Risk Alerts: Reporting Engine for 70.0	New		48
08/04/2017 06:1...	HIGH	70	INC-1130	High Risk Alerts: Reporting Engine for 70.0	New		44
08/04/2017 05:1...	HIGH	70	INC-1129	High Risk Alerts: Reporting Engine for 70.0	New		51
08/04/2017 04:1...	HIGH	70	INC-1128	High Risk Alerts: Reporting Engine for 70.0	New		57
08/04/2017 03:1...	HIGH	70	INC-1127	High Risk Alerts: Reporting Engine for 70.0	New		54
08/04/2017 02:1...	HIGH	70	INC-1126	High Risk Alerts: Reporting Engine for 70.0	New		58
08/04/2017 01:1...	HIGH	70	INC-1125	High Risk Alerts: Reporting Engine for 70.0	New		60
08/04/2017 00:1...	HIGH	70	INC-1124	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 23:1...	HIGH	70	INC-1123	High Risk Alerts: Reporting Engine for 70.0	New		60
08/03/2017 22:1...	HIGH	70	INC-1122	High Risk Alerts: Reporting Engine for 70.0	New		60

2. タスクが必要なインシデントを見つけて、[ID]または[名前]フィールドのリンクをクリックします。

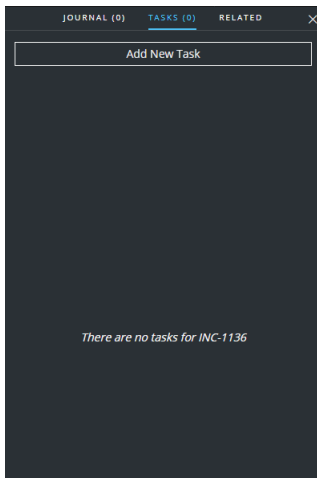
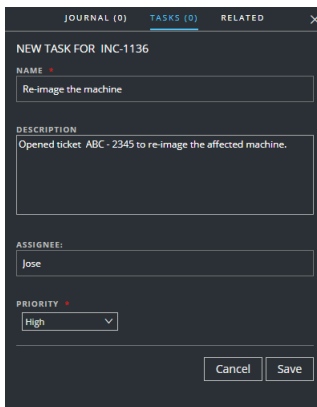
[インシデントの詳細]ビューが表示されます。



3. [インシデントの詳細]ビューの右上のツールバーで、を選択します。
[ジャーナル]パネルが表示されます。



4. [タスク] タブを選択します。

5. [タスク] パネルで、[新しいタスクの追加] をクリックします。
新しいタスクのフィールドが表示されます。

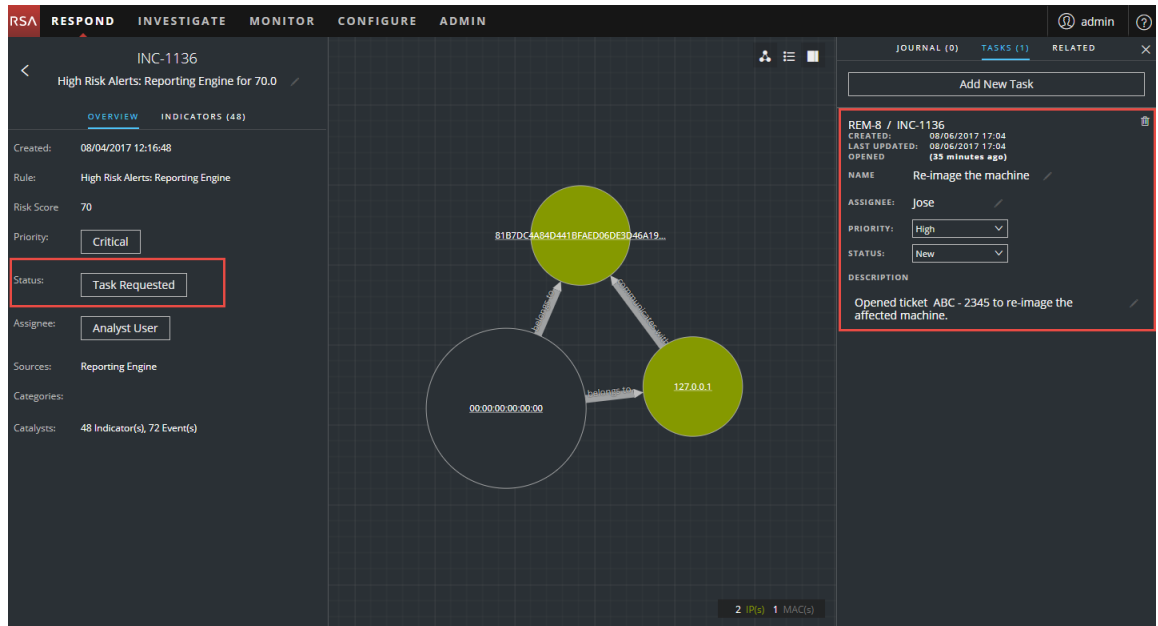
インシデントがクローズ状態 ([クローズ] または [クローズ- False Positive]) の場合、[新しいタスクの追加] ボタンは無効化されます。

6. 次の情報を入力します。

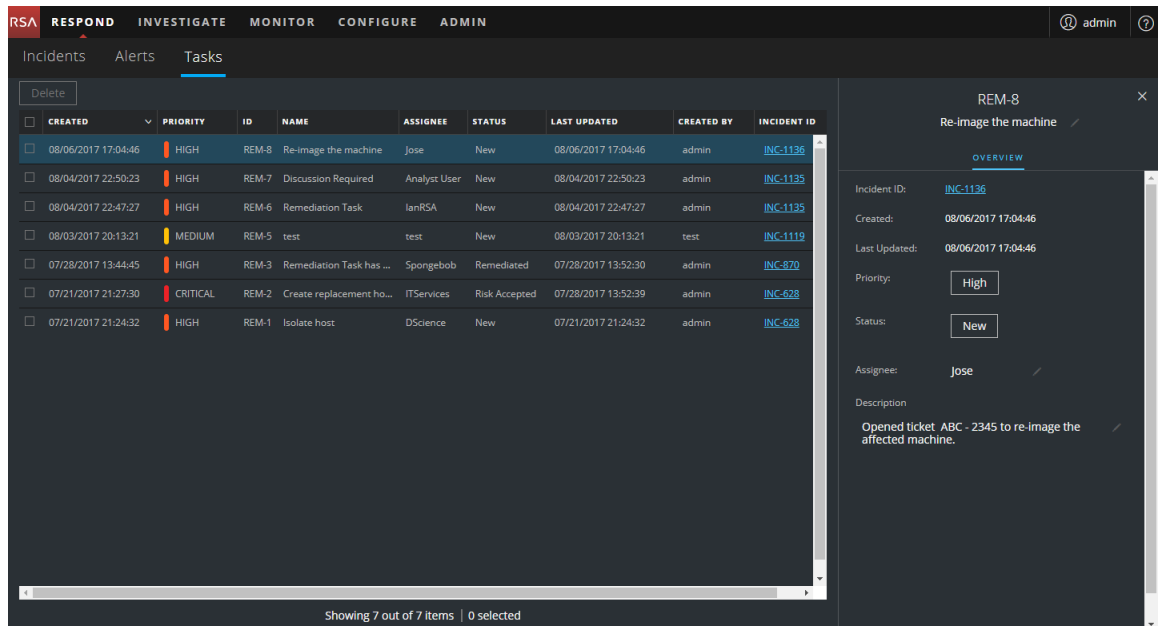
- [名前]: タスクの名前。例: 「マシンの再イメージ化」のように入力します。
- [説明]: (オプション) タスクの説明を入力します。該当する参照番号を含めることができます。
- [割り当て先]: (オプション) タスクの割り当て先となるユーザの名前を入力します。
- [優先度]: 優先度ボタンをクリックし、ドロップダウン リストからタスクの優先度を選択します。[低]、[中]、[高]、[クリティカル] の中から選択します。

7. [保存] をクリックします。

変更が成功したことの確認が表示されます。インシデント ステータスは [タスクがリクエストされました] に変更されます。このインシデントの [タスク] パネルにタスクが表示されます。



すべてのインシデント タスクのリストを表示する[タスク]リスト([対応] > [タスク])にも表示されます。




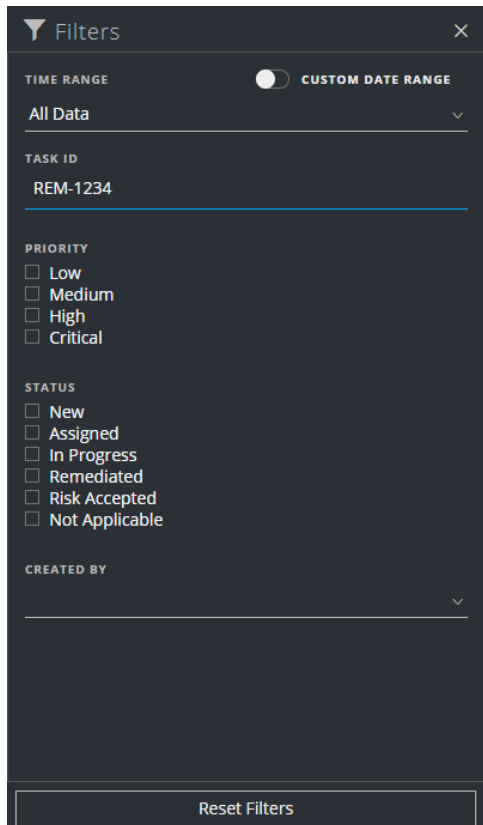
注: ステータスの変更が表示されない場合は、Webブラウザを更新する必要があることがあります。

タスクの検索

タスクIDがわかっている場合は、フィルタを使用して、タスクをすばやく見つけることができます。たとえば、数千のタスクから特定のタスクを見つけたる場合があります。

1. [対応] > [タスク] に移動します。

タスクリストの左側に[フィルタ]パネルが表示されます。[フィルタ]パネルが表示されない場合は、タスクリストビューのツールバーでをクリックすると[フィルタ]パネルが開きます。




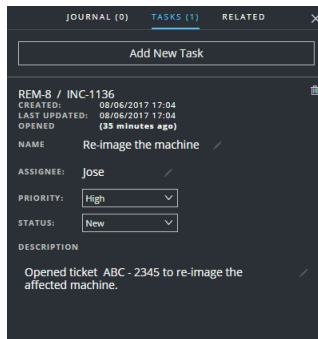
2. [タスクID]フィールドで、検索するタスクのタスクIDを入力します(例: REM-1234)。
タスクリストに指定されたタスクが表示されます。結果が表示されない場合は、フィルタをリセットしてください。

タスクの変更

インシデント内およびタスクリストからタスクを変更することができます。たとえば、タスクのステータスを[対応中]として表示し、追加情報をタスクに追加する場合があります。タスクがクローズ状態([該当なし]、[リスク受容]、[改善済み])の場合、[優先度]または[割り当て先]は変更できません。

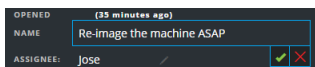
インシデント内からタスクを変更するには、次の手順を実行します。

1. [対応]>[インシデント]に移動します。
インシデントのリストビューに、すべてのインシデントのリストが表示されます。
2. タスクの更新が必要なインシデントを見つけて、[ID]または[名前]フィールドのリンクをクリックします。
[インシデントの詳細]ビューが表示されます。
3. ビューの右上のツールバーで、を選択します。
[ジャーナル]パネルが表示されます。
4. [タスク]タブを選択します。
5. [タスク]パネルの鉛筆アイコンは、変更できるテキストフィールドを示します。ボタンは、選択するドロップダウンリストがあることを示します。



6. 次のフィールドを変更できます。

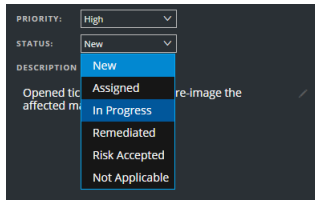
- [名前]: 現在のタスク名をクリックすると、テキストエディタが開きます。



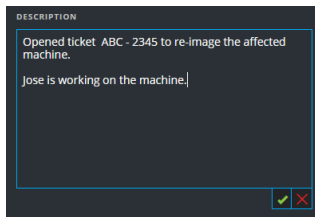
チェックマークをクリックして、変更を確認します。たとえば、「マシンの再イメージ化」を「マシンASAPの再イメージ化」に変更できます。

- [割り当て先]: [(未割り当て)]または以前の割り当て先の名前をクリックすると、テキストエディタが開きます。タスクの割り当て先となるユーザの名前を入力します。
チェックマークをクリックして、変更を確認します。
- [優先度]: [優先度]ボタンをクリックし、ドロップダウンリストからタスクの優先度を選択します。[低]、[中]、[高]、[クリティカル]の中から選択します。
- [ステータス]: [ステータス]ボタンをクリックし、ドロップダウンリストからタスクのステータスを選択します。[新規]、[割り当て済み]、[対応中]、[改善済み]、[リスク受容]、[該

当なし]があります。たとえば、[対応中]にステータスを変更することができます。



- [説明]: 説明の下のテキストをクリックすると、テキスト エディタが開きます。



テキストを変更してチェック マークをクリックし、変更を確認します。

行った変更ごとに、変更が成功したことの確認が表示されます。

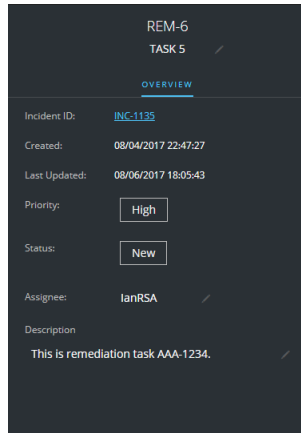
タスク リストからタスクを変更するには、次の手順を実行します。

1. [対応]>[タスク]に移動します。
タスク リスト ビューに、すべてのインシデント タスクのリストが表示されます。
2. タスク リストで、更新するタスクをクリックします。
タスク リストの右側にタスクの[概要]パネルが表示されます。

CREATED	PRIORITY	ID	NAME	ASSIGNEE	STATUS	LAST UPDAT...	CREA...	INCIDENT ID
08/06/2017 1...	HIGH	REM-8	Re-image the machine ASAP	Jose	In Progr...	08/06/2017 17:...	admin	INC-1136
08/04/2017 2...	HIGH	REM-7	Discussion Required	Analyst User	New	08/04/2017 22:...	admin	INC-1135
08/04/2017 2...	HIGH	REM-6	TASK 5	IanRSA	New	08/06/2017 18:...	admin	INC-1135
08/03/2017 2...	MEDIUM	REM-5	test	test	New	08/03/2017 20:...	test	INC-1119
07/28/2017 1...	HIGH	REM-3	Remediation Task has been renamed	Spongebob	Remedi...	07/28/2017 13:...	admin	INC-870
07/21/2017 2...	CRITICAL	REM-2	Create replacement host ASAP	ITServices	Risk Acc...	07/28/2017 13:...	admin	INC-628
07/21/2017 2...	HIGH	REM-1	Isolate host	DSscience	New	07/21/2017 21:...	admin	INC-628

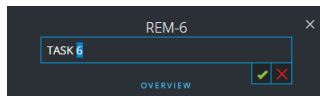
タスクの[概要]パネルの鉛筆アイコンは、変更できるテキスト フィールドを示します。ボタン

は、選択するドロップダウン リストがあることを示します。



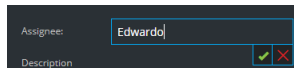
3. 次のフィールドを変更できます。

- **<タスク名>**: タスクの[概要]パネルの上部、タスクIDの下で、現在のタスク名をクリックすると、テキスト エディタが開きます。



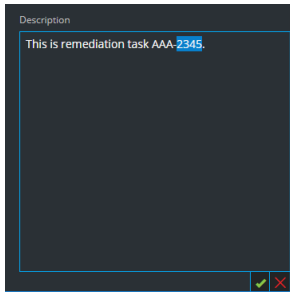
チェック マークをクリックして、変更を確認します。たとえば、タスク5をタスク6に変更することができます。

- **[優先度]**: [優先度] ボタンをクリックし、ドロップダウン リストからタスクの優先度を選択します。[低]、[中]、[高]、[クリティカル]の中から選択します。
- **[ステータス]**: [ステータス] ボタンをクリックし、ドロップダウン リストからタスクのステータスを選択します。[新規]、[割り当て済み]、[対応中]、[改善済み]、[リスク受容]、[該当なし]があります。
- **[割り当て先]**: [(未割り当て)] または以前の割り当て先の名前をクリックすると、テキスト エディタが開きます。タスクの割り当て先となるユーザの名前を入力します。



チェック マークをクリックして、変更を確認します。

- **[説明]**: 説明の下 のテキストをクリックすると、テキスト エディタが開きます。



テキストを変更してチェック マークをクリックし、変更を確認します。

行った変更ごとに、変更が成功したことの確認が表示されます。

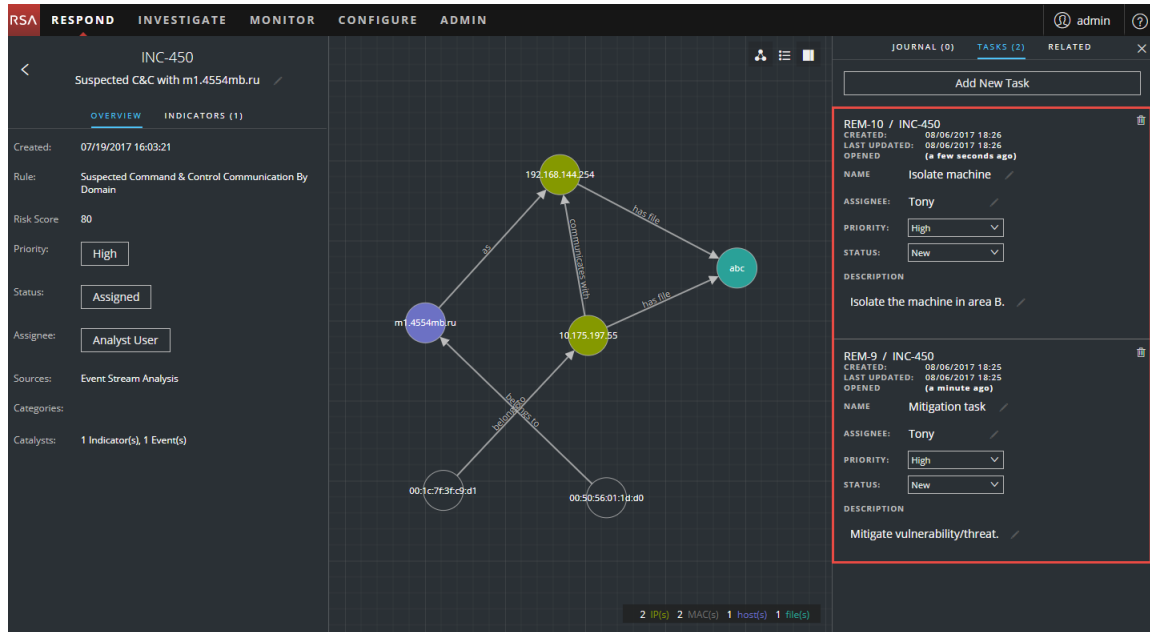
タスクの削除

間違って作成したタスクがある場合や、作成したタスクが不要であることがわかった場合は、タスクを削除できます。インシデント内およびタスク リスト ビューからタスクを削除することができます。タスク リスト ビューで、同時に複数のタスクを削除することができます。

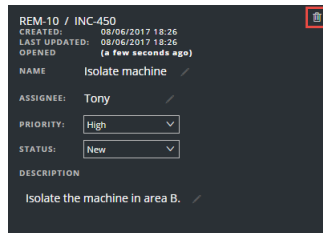
インシデント内からタスクを削除するには、次の手順を実行します。

1. **[対応]** > **[インシデント]** に移動します。
インシデントのリスト ビューに、すべてのインシデントのリストが表示されます。
2. タスクの更新が必要なインシデントを見つけて、**[ID]** または **[名前]** フィールドのリンクをクリックします。
[インシデントの詳細] ビューが表示されます。
3. ビューの右上のツールバーで、**■** を選択します。
[ジャーナル] パネルが表示されます。
4. **[タスク]** タブを選択します。

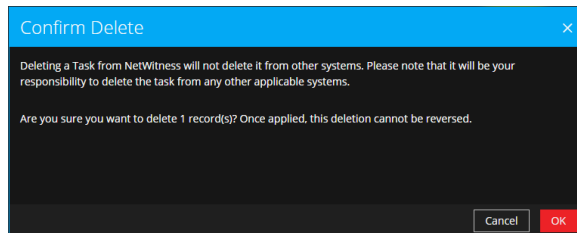
5. [タスク] パネルでは、インシデントに対して作成されたタスクを確認できます。



6. 削除するタスクの右にあるをクリックします。



7. タスクを削除することを確認し、[OK]をクリックします。

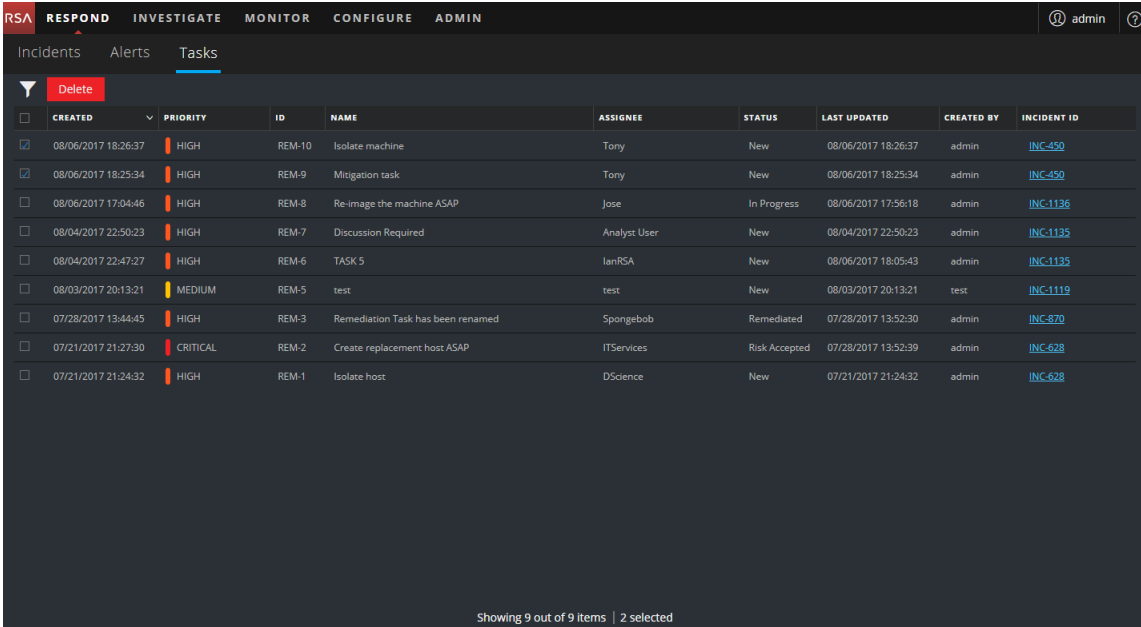


タスクがNetWitness Suiteから削除されます。NetWitness Suiteからタスクを削除しても、他のシステムからは削除されません。

タスク リストからタスクを削除するには、次の手順を実行します。

1. [対応] > [タスク]に移動します。
タスク リスト ビューに、すべてのインシデント タスクのリストが表示されます。

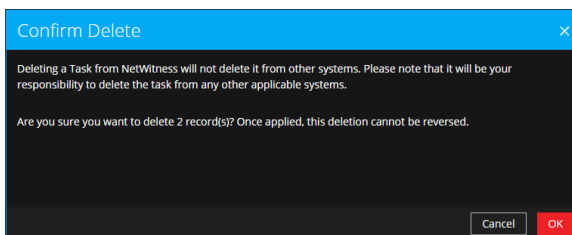
2. タスクリストで、削除するタスクを選択し、[削除]をクリックします。



CREATED	PRIORITY	ID	NAME	ASSIGNEE	STATUS	LAST UPDATED	CREATED BY	INCIDENT ID
08/06/2017 18:26:37	HIGH	REM-10	Isolate machine	Tony	New	08/06/2017 18:26:37	admin	INC-450
08/06/2017 18:25:34	HIGH	REM-9	Mitigation task	Tony	New	08/06/2017 18:25:34	admin	INC-450
08/06/2017 17:04:46	HIGH	REM-8	Re-image the machine ASAP	Jose	In Progress	08/06/2017 17:56:18	admin	INC-1136
08/04/2017 22:50:23	HIGH	REM-7	Discussion Required	Analyst User	New	08/04/2017 22:50:23	admin	INC-1135
08/04/2017 22:47:27	HIGH	REM-6	TASK 5	IanRSA	New	08/06/2017 18:05:43	admin	INC-1135
08/03/2017 20:13:21	MEDIUM	REM-5	test	test	New	08/03/2017 20:13:21	test	INC-1119
07/28/2017 13:44:45	HIGH	REM-3	Remediation Task has been renamed	Spongebob	Remediated	07/28/2017 13:52:30	admin	INC-870
07/21/2017 21:27:30	CRITICAL	REM-2	Create replacement host ASAP	ITServices	Risk Accepted	07/28/2017 13:52:39	admin	INC-628
07/21/2017 21:24:32	HIGH	REM-1	Isolate host	DScience	New	07/21/2017 21:24:32	admin	INC-628

Showing 9 out of 9 items | 2 selected

3. タスクを削除することを確認し、[OK]をクリックします。



タスクがNetWitness Suiteから削除されます。NetWitness Suiteからタスクを削除しても、他のシステムからは削除されません。

インシデントのクローズ

インシデントを調査し、対策を施してインシデントを解決したら、インシデントをクローズします。

- [対応]>[インシデント]に移動します。
- インシデントのリストビューで、クローズするインシデントを選択し、[ステータス変更]をクリックします。
- ドロップダウンリストから[クローズ]を選択します。
変更が成功した通知が表示されます。これでインシデントがクローズされました。クローズしたインシデントの優先度または割り当て先を変更することはできません。

注: [概要] パネルでもインシデントを閉じることができます。インシデントのリスト ビューでは同時に複数のインシデントをクローズできます。「[インシデント ステータスの変更](#)」で、詳細を参照してください。

アラートのレビュー

NetWitness Suiteでは、複数のソースから生成された脅威アラートの統合リストを1つの場所に表示できます。これらのアラートは、[対応] > [アラート]ビューで見ることができます。アラートのソースは、ESAの相関ルール、ESA Analytics、NetWitness Endpoint、Malware Analysis、Reporting Engine、その他多数にできます。アラートの元のソース、アラートの重大度、追加のアラートの詳細を表示できます。

注: ESA相関ルールのアラートは、[対応] > [アラート]ビューでのみ見ることができます。

大量のアラートをより良く管理するため、重大度、時間範囲、アラートソースなどの指定した条件に基づいてアラートリストをフィルタすることができます。たとえば、インシデントの一部となっていない、重大度が90~100のアラートのみを表示するようにアラートをフィルタすることができます。その後、アラートのグループを選択し、インシデントを作成したり既存のインシデントに追加したりすることもできます。

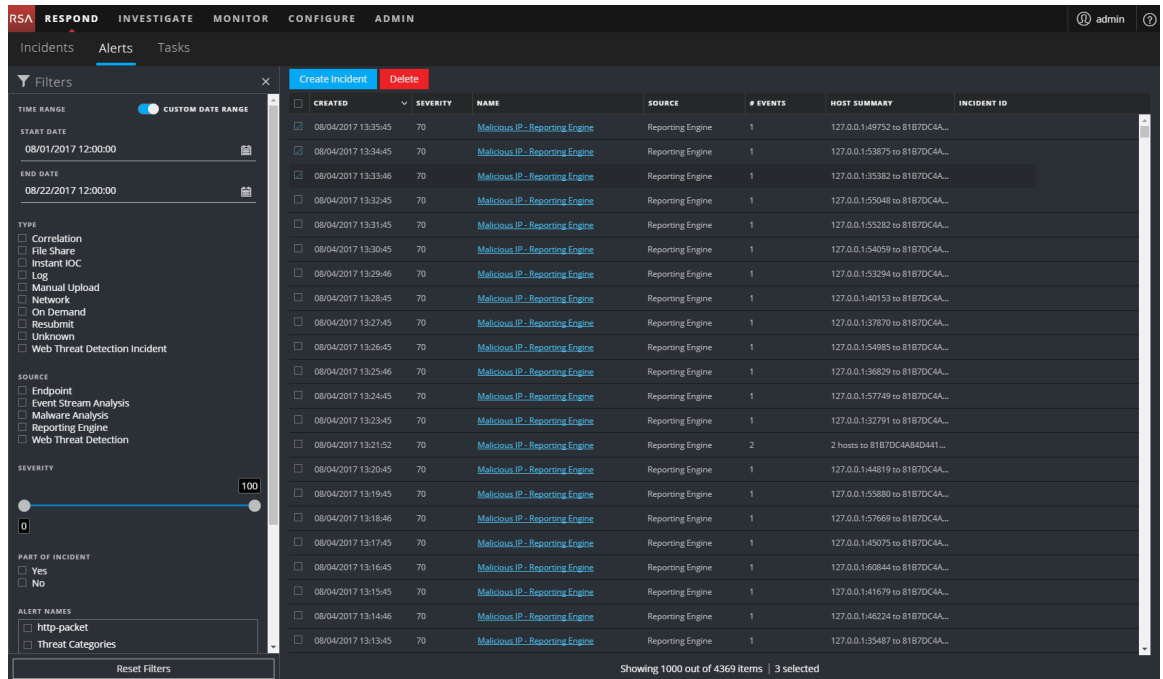
アラートのレビューおよび管理を行うには、次の手順を実行します。

- [アラートの表示](#)
- [アラートリストのフィルタ](#)
- [アラートリストからのMyフィルタの削除](#)
- [アラートのサマリ情報の表示](#)
- [アラートのイベント詳細の表示](#)
- [イベントの調査](#)
- [インシデントの手動作成](#)
- [アラートのレビュー](#)
- [アラートの削除](#)

アラートの表示

アラートのリストビューでは、複数のソースから各種のアラートを参照し、フィルタとグループ化を行ってインシデントを作成できます。この手順では、アラートリストにアクセスする方法を示します。

1. [対応] > [アラート]に移動します。
アラートのリストビューに、すべてのNetWitness Suiteアラートのリストが表示されます。



2. アラート リストをスクロールすると、次の表で説明する各アラートに関する基本的な情報が表示されます。


列	説明
作成日	アラートがソースシステムに記録された日時を表示します。
重大度	アラートの重大度のレベルを表示します。値は1～100です。
名前	アラートの基本的な説明を表示します。
ソース	アラートの元のソースを表示します。アラートのソースは、NetWitness Endpoint、Malware Analysis、Event Stream Analysis(ESA 関連ルール)、ESA Analytics、Reporting Engine、Web Threat Detection、その他多数のソースがあります。
イベント数	アラートに含まれるイベントの数を示します。この値は、ソースによって異なります。たとえば、NetWitness Endpointアラートと Malware Analysisアラートでは、常にイベントの数が1つになります。特定のタイプのアラートでは、イベント数が多いとより高いリスクを示すことがあります。

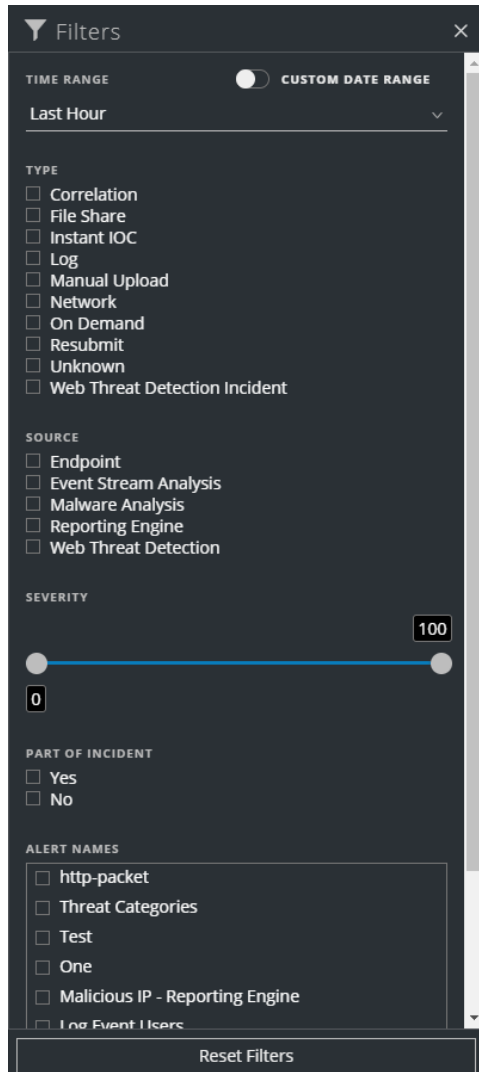
列	説明
ホスト サマリ	ホストの詳細(アラートのトリガー元のホスト名など)を表示します。詳細には、アラートのソース ホストや宛先ホストに関する情報が含まれる場合があります。アラートの中には、複数のホストにまたがってイベントを記述するものがあります。
インシデントID	アラートのインシデントIDを表示します。インシデントIDがない場合は、アラートがインシデントに属さないことを示します。この場合、このアラートを含めるインシデントを作成することも、アラートを既存のインシデントに追加することもできます。

リストの下部では、現在のページのアラート数と、アラートの総数を確認できます。例:「377アイテム中377個を表示中」のように表示されます

アラート リストのフィルタ

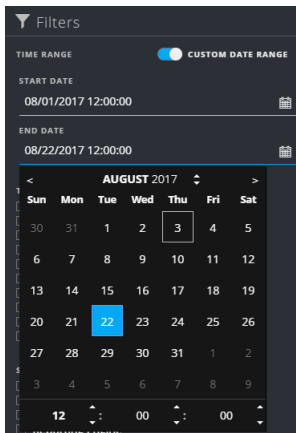
アラート リスト内のアラートの数は非常に多数になり、特定のアラートを検索することが困難になることがあります。フィルタを使用すると、特定のソースからのアラート、特定の重大度のアラート、インシデントの一部ではないアラートなど、目的のアラートを表示することができます。

1. [対応] > [アラート] に移動します。
アラート リストの左側に[フィルタ]パネルが表示されます。[フィルタ]パネルが表示されない場合は、アラート リスト ビューのツールバーで  をクリックすると[フィルタ]パネルが開きます。



2. [フィルタ]パネルで1つまたは複数のオプションを選択し、アラートのリストをフィルタします。
 - [時間範囲]: [時間範囲]ドロップダウンリストから特定の期間を選択できます。時間範囲は、アラートを受信した日付に基づきます。たとえば、[直近1時間]を選択する場合は、過去60分以内に受信されたアラートが表示されます。
 - [カスタムの日付範囲]: [時間範囲]オプションを選択する代わりに、特定の日付範囲を指定できます。これを行うには、[カスタムの日付範囲]の前にある白色の円をクリックし、[開始日]と[終了日]のフィールドを表示します。カレンダーから日付と時刻を選択

します。



- **[タイプ]**: 表示するアラートのイベントのタイプ(ログ、ネットワークセッションなど)を選択します。
- **[ソース]**: 1つまたは複数のソースを選択すると、そのソースによってトリガーされたアラートが表示されます。たとえば、NetWitness Endpointアラートののみを表示するには、ソースとして[エンドポイント]を選択します。
- **[重大度]**: 表示するアラートの重大度レベルを選択します。値は1~100です。たとえば、最高の重大度のアラートを最初に重点的に確認するには、90~100の重大度のアラートののみを表示することができます。
- **[インシデントの一部]**: インシデントの一部ではないアラートののみを表示するには、[No]を選択します。インシデントの一部であるアラートののみを表示するには、[Yes]を選択します。たとえば、アラートのグループからインシデントを作成しようとしているときは、[No]を選択すると、現在、インシデントの一部ではないアラートののみを表示することができます。
- **[アラート名]**: 表示するアラートの名前を選択します。このフィルタを使用すると、[悪意のあるIP: Reporting Engine]などの特定のルールまたはソースによって生成されたすべてのアラートを検索することができます。

アラート リストには、選択条件を満たすアラートのリストが表示されます。アラート リストの下部では、フィルタ処理されたリストのアイテム数を確認できます。


例: 「30アイテム中30個を表示中」のように表示されます

3. **[フィルタ]** パネルを閉じる場合は、[X]をクリックします。フィルタは、削除するまで設定されたままになります。

アラート リスト からの My フィルタの削除

NetWitness Suite では、アラート リスト ビューのフィルタ選択が記憶されます。不要な場合はフィルタ選択を削除することができます。たとえば、表示されるべきアラート数が表示されない場合や、アラート リストのすべてのアラートを表示する場合は、フィルタをリセットできます。

1. [対応] > [アラート] に移動します。

アラート リストの左側に [フィルタ] パネルが表示されます。[フィルタ] パネルが表示されない場合は、アラート リスト ビューのツールバーで  をクリックすると [フィルタ] パネルが開きます。

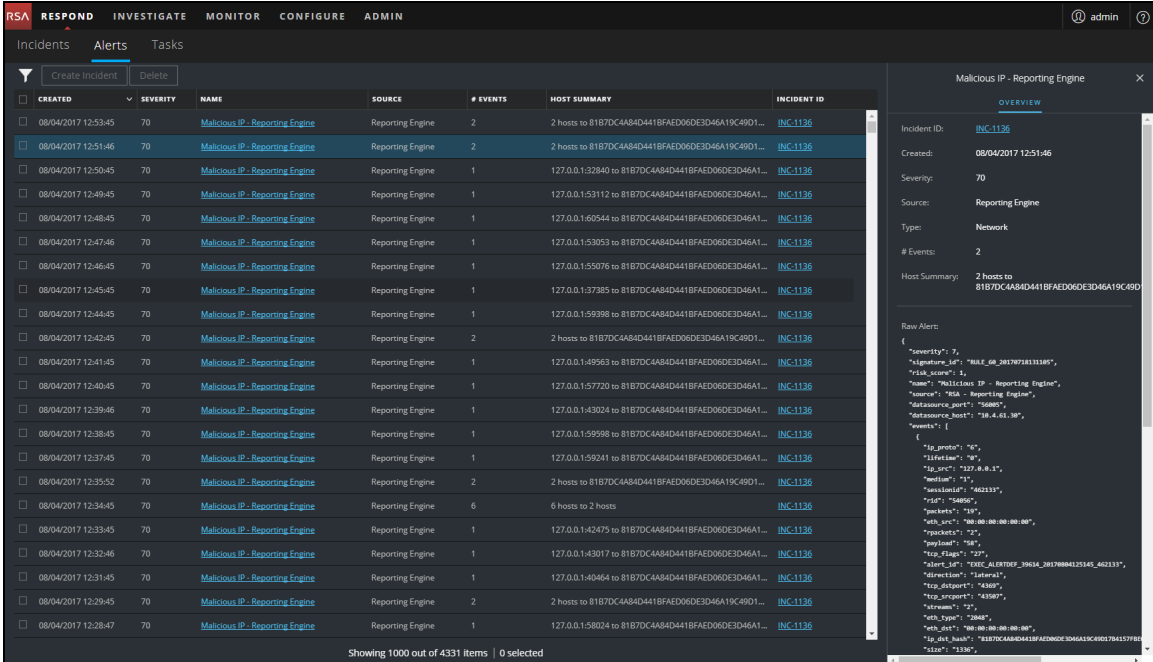
2. [フィルタ] パネルの下部で [フィルタのリセット] をクリックします。

アラートのサマリ情報の表示

アラートに関する基本的な情報の表示に加えて、RAW アラートのメタデータを [概要] パネルで表示することもできます。

1. アラート リストで、表示するアラートをクリックします。

アラート リストの右側にアラートの [概要] パネルが表示されます。



The screenshot displays the NetWitness Respond interface. The main window shows a table of alerts with columns: CREATED, SEVERITY, NAME, SOURCE, # EVENTS, HOST SUMMARY, and INCIDENT ID. The selected alert is: 08/04/2017 12:51:46, Severity 70, Name Malicious IP - Reporting Engine, Source Reporting Engine, # Events 2, Host Summary 2 hosts to 81B7DC4A84D441BFAD060E3D46A19C49D1... (INC-1136).

The right-hand panel shows the 'Malicious IP - Reporting Engine' alert details. It includes the Incident ID (INC-1136), Created time (08/04/2017 12:51:46), Severity (70), Source (Reporting Engine), Type (Network), # Events (2), and Host Summary (2 hosts to 81B7DC4A84D441BFAD060E3D46A19C49D1...). Below this, the 'Raw Alert' section shows the following JSON data:

```

{
  "severity": 70,
  "signature_id": "RULE_08_20170731313100",
  "risk_score": 1,
  "name": "Malicious IP - Reporting Engine",
  "source": "RSB - Reporting Engine",
  "datasource_port": "56000",
  "datasource_host": "10.4.63.30",
  "events": [
    {
      "ip_proto": "ig",
      "direction": "ig",
      "ip_src": "127.0.0.1",
      "ip_dst": "127.0.0.1",
      "protocol": "igmp",
      "source_ip": "10.4.63.30",
      "target_ip": "10.4.63.30",
      "action": "alert",
      "alert_msg": "EXEC_ALERT00F_39634_20170804125145_462333",
      "direction": "inbound",
      "tcp_dest_port": "56000",
      "tcp_src_port": "43500",
      "stream": "2",
      "eth_src": "08:00:00:00:00:00",
      "eth_dst": "08:00:00:00:00:00",
      "ip_dst_host": "81B7DC4A84D441BFAD060E3D46A19C49D1",
      "ip_src": "1330"
    }
  ]
}

```


左側の[概要]パネルには、アラートのリストビューの[概要]パネルと同じアラート情報があります。

右側の[イベント]パネルには、イベント時間、ソースIP、宛先IP、検知器IP、ソースのユーザ、宛先のユーザ、イベントに関するファイル情報など、アラートのイベントに関する情報が表示されます。表示される情報の量は、イベントタイプに依存します。

イベントには次の2つのタイプがあります。

- 2台のマシン(ソースと宛先)間のトランザクション
- 1台のマシン(検知器)で検出された異常

一部のイベントは、検知器のみを持ちます。たとえば、NetWitness Endpointはマシンのマルウェアを検出します。その他のイベントは、ソースと宛先を持ちます。たとえば、パケットデータは、マシンとC2(Command and Control)ドメイン間の通信を示しています。

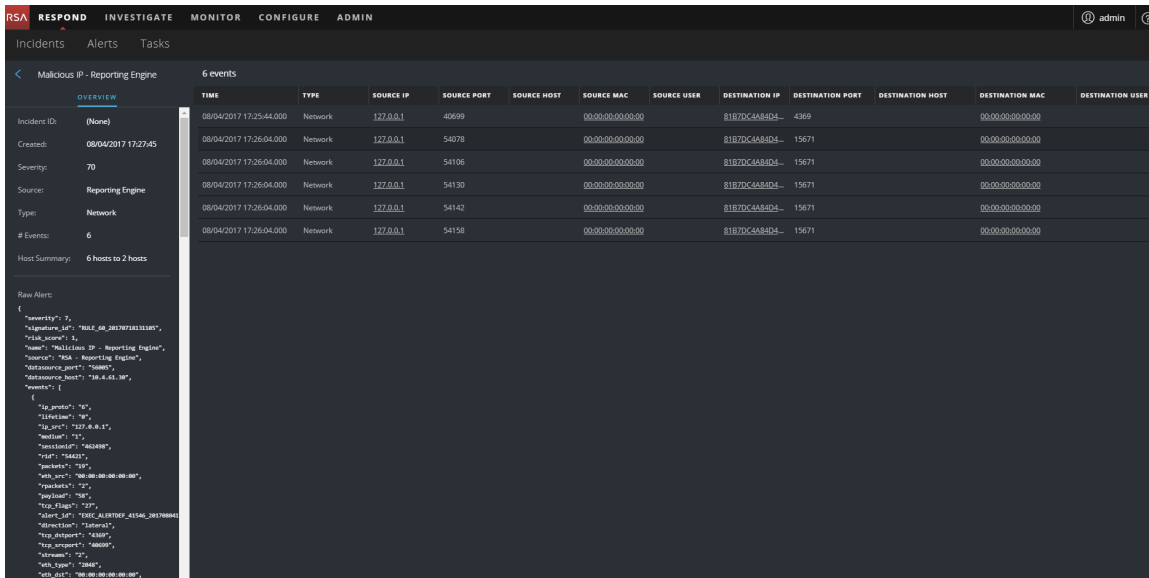
イベントをさらにドリルダウンして、イベントに関する詳細なデータを取得できます。

アラートのイベント詳細を表示するには、次の手順を実行します。

1. アラートのイベント詳細を表示するには、アラートのリストビューで表示するアラートを選択し、そのアラートの[名前]列のリンクをクリックします。

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID
08/04/2017 17:39:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:53972 to 8187DC4A84D441BF...	
08/04/2017 17:38:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:35751 to 8187DC4A84D441BF...	
08/04/2017 17:37:46	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:40803 to 8187DC4A84D441BF...	
08/04/2017 17:36:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:50337 to 8187DC4A84D441BF...	
08/04/2017 17:35:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:49682 to 8187DC4A84D441BF...	
08/04/2017 17:34:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:39861 to 8187DC4A84D441BF...	
08/04/2017 17:33:46	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:35012 to 8187DC4A84D441BF...	
08/04/2017 17:32:45	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 2 hosts	
08/04/2017 17:31:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:34101 to 8187DC4A84D441BF...	
08/04/2017 17:30:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:55635 to 8187DC4A84D441BF...	
08/04/2017 17:29:46	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:60061 to 8187DC4A84D441BF...	
08/04/2017 17:28:45	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 2 hosts	
08/04/2017 17:27:45	70	Malicious IP - Reporting Engine	Reporting Engine	6	6 hosts to 2 hosts	
08/04/2017 17:26:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:44802 to 8187DC4A84D441BF...	
08/04/2017 17:25:46	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:59132 to 8187DC4A84D441BF...	
08/04/2017 17:24:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:38089 to 8187DC4A84D441BF...	
08/04/2017 17:23:45	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 2 hosts	
08/04/2017 17:21:53	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 8187DC4A84D441BFAED06DE...	
08/04/2017 17:20:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:43271 to 8187DC4A84D441BF...	
08/04/2017 17:19:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:47973 to 8187DC4A84D441BF...	

[アラートの詳細]ビューでは、左側に[概要]パネル、右側に[イベント]パネルが表示されます。

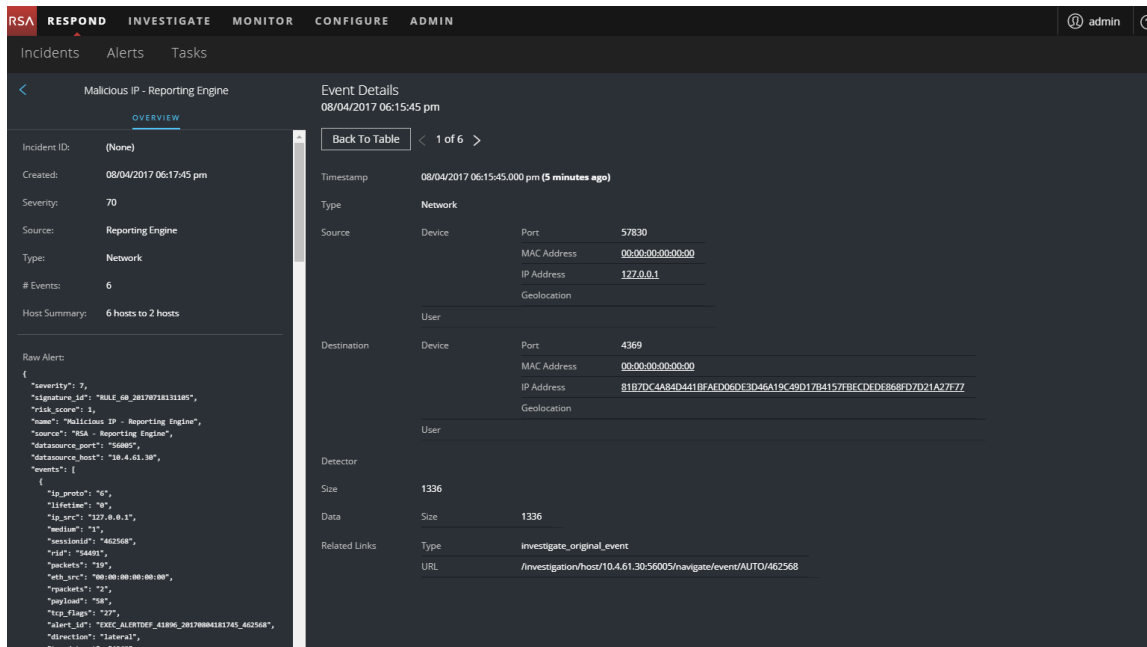


[イベント]パネルには、イベントのリストと、各イベントに関する情報が表示されます。次の表は、イベント リスト(イベント テーブル)に表示される列の一部を示しています。

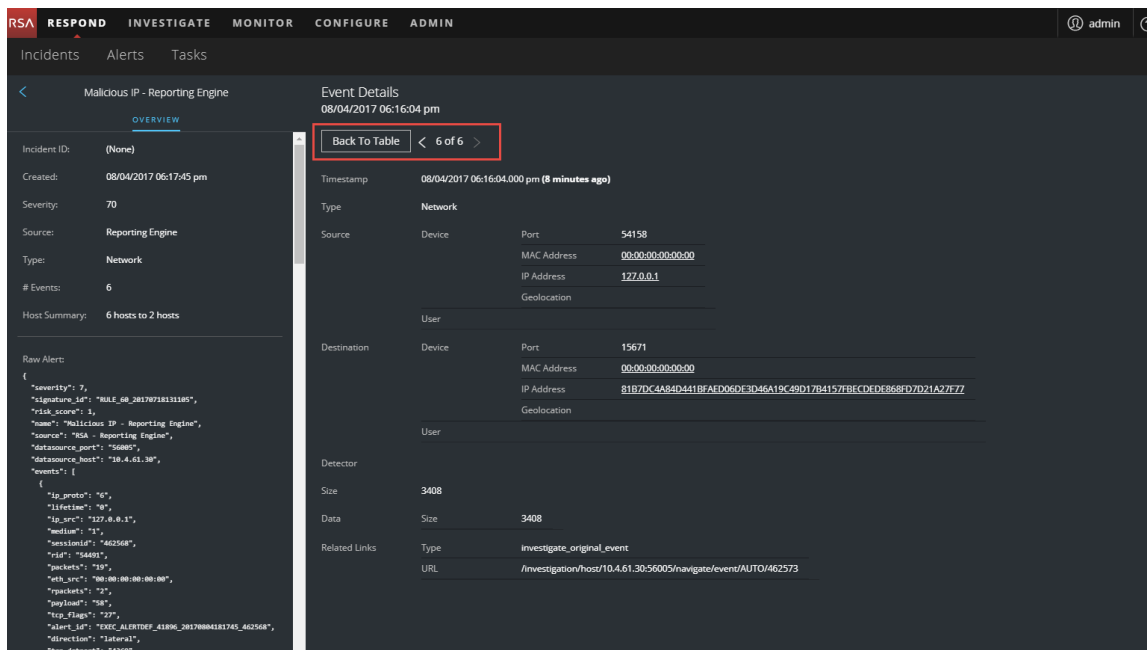
列	説明
時刻	イベントの発生時刻を示します。
タイプ	ログやネットワークなどのアラートのタイプを示します。
ソースIP	2台のマシン間のトランザクションがあった場合にソースIPアドレスを示します。
宛先IP	2台のマシン間のトランザクションがあった場合に宛先IPアドレスを示します。
検知器IP	異常が検出されたマシンのIPアドレスを示します。
ソース ユーザ	ソース マシンのユーザを示します。
宛先 ユーザ	宛先 マシンのユーザを示します。
ファイル名	ファイルがイベントと関連している場合にファイル名を示します。
ファイルハッシュ	ファイルの内容のハッシュを示します。

リストに1つのみのイベントがある場合は、リストではなくそのイベントの詳細が表示されます。

2. [イベント] リストのイベントをクリックし、イベントの詳細を表示します。
この例は、リストの最初のイベントのイベントの詳細を示しています。



3. その他のイベントを表示するには、[テーブルに戻る] ボタンの右側のページ ナビゲーションを使用します。この例は、リストの最後のイベントのイベントの詳細を示しています。



[アラートの詳細] パネルに表示されるイベント データに関する詳細については、[\[アラートの詳細\] ビュー](#)を参照してください。

イベントの調査

イベントをさらに調査するには、追加のコンテキスト情報へのリンクを使用します。リンク先では、選択内容に応じたオプションが提供されます。

コンテキスト情報の表示

[アラートの詳細]ビューでは、[イベント]パネルで下線付きのエンティティを確認できます。下線付きエンティティはContext Hubのエンティティとみなされ、使用可能な追加のコンテキスト情報があります。次の図は、イベント リストの下線付きのエンティティを示しています。

TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION PORT
08/04/2017 06:15:45.000 ...	Network	<u>127.0.0.1</u>	57830		<u>00:00:00:00:00:00</u>		<u>81B7DC4A84D4...</u>	4369
08/04/2017 06:16:04.000 ...	Network	<u>127.0.0.1</u>	54078		<u>00:00:00:00:00:00</u>		<u>81B7DC4A84D4...</u>	15671
08/04/2017 06:16:04.000 ...	Network	<u>127.0.0.1</u>	54106		<u>00:00:00:00:00:00</u>		<u>81B7DC4A84D4...</u>	15671
08/04/2017 06:16:04.000 ...	Network	<u>127.0.0.1</u>	54130		<u>00:00:00:00:00:00</u>		<u>81B7DC4A84D4...</u>	15671
08/04/2017 06:16:04.000 ...	Network	<u>127.0.0.1</u>	54142		<u>00:00:00:00:00:00</u>		<u>81B7DC4A84D4...</u>	15671
08/04/2017 06:16:04.000 ...	Network	<u>127.0.0.1</u>	54158		<u>00:00:00:00:00:00</u>		<u>81B7DC4A84D4...</u>	15671

次の図は、[イベントの詳細]の下線付きのエンティティを示しています。

Event Details
08/04/2017 06:15:45 pm

Back To Table < 1 of 6 >

Timestamp: 08/04/2017 06:15:45.000 pm (24 minutes ago)

Type: Network

Source: Device Port 57830
MAC Address 00:00:00:00:00:00
IP Address 127.0.0.1
Geolocation

User

Destination: Device Port 4369
MAC Address 00:00:00:00:00:00
IP Address 81B7DC4A84D4418FAED06DE3D36A19C49D17B4157FBECDEDE868FD7D21A27E77
Geolocation

User

Detector

Size: 1336

Data: Size 1336

Related Links: Type investigate_original_event
URL /investigation/host/10.4.61.30:56005/navigate/event/AUTO/462568

```
Raw Alert:
{
  "severity": 7,
  "signature_id": "MIL_E_08_2017073131185",
  "risk_score": 1,
  "name": "Malicious IP - Reporting Engine",
  "source": "RSA - Reporting Engine",
  "datasource_port": "56005",
  "datasource_host": "10.4.61.30",
  "events": [
    {
      "ip_proto": "6",
      "lifetime": "0",
      "ip_src": "127.0.0.1",
      "medium": "I",
      "sessionid": "462568",
      "rid": "54401",
      "packets": "19",
      "eth_src": "00:00:00:00:00:00",
      "packets": "2",
    }
  ]
}
```

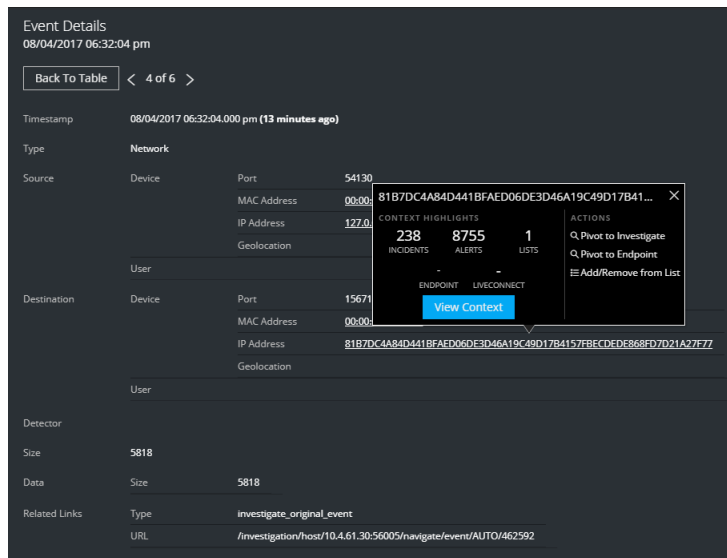

Context Hubは、エンティティにマップされたメタ フィールドで事前構成されます。NetWitness RespondとInvestigationはコンテキスト ルックアップでこれらのデフォルトのマッピングを使用します。メタ キーを追加する方法については、「Context Hub構成ガイド」の「データ ソース設定の構成」を参照してください。

注意: コンテキスト ルックアップをRespondとInvestigateのビューで正常に動作させるため、[管理] > [システム] > [調査] > [コンテキスト ルックアップ] タブでメタ キーをマップする際に、メタ キーをメタ キー マッピングにのみ追加し、MongoDBのフィールドには追加しないでください。たとえば、ip.addressはメタ キーで、ip_addressはメタ キーではありません(これは、MongoDBのフィールドです)。

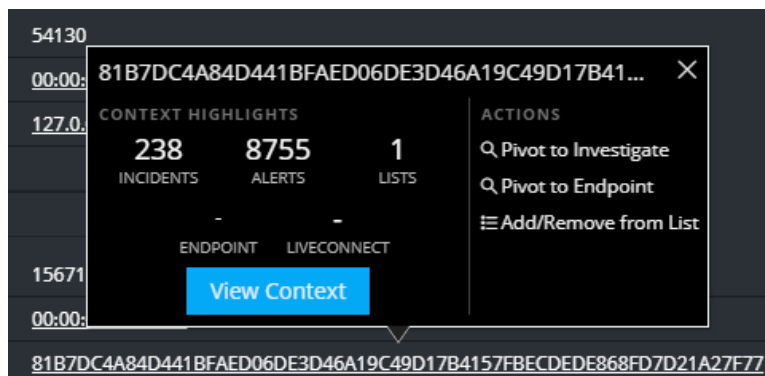
コンテキスト情報を表示するには、次の手順を実行します。

1. [アラートの詳細]ビューのイベント リストまたはイベントの詳細で、下線付きのエンティティにポインターを合わせます。

コンテキスト ツールチップに、選択したエンティティで利用可能なコンテキスト データのタイプの簡単なサマリが表示されます。



コンテキスト ツールチップには、[コンテキストのハイライト]と[アクション]という2つのセクションがあります。



[**コンテキストのハイライト**]セクションの情報は、希望するアクションを判断するのに役立ちます。このセクションには、関連するアラートとインシデントの数が表示されます。データによっては、これらの数字付きのアイテムをクリックして詳細を確認できます。前掲の例は、238個の関連インシデント、8,755個の関連アラート、1つの関連Context Hubリストを示しています。

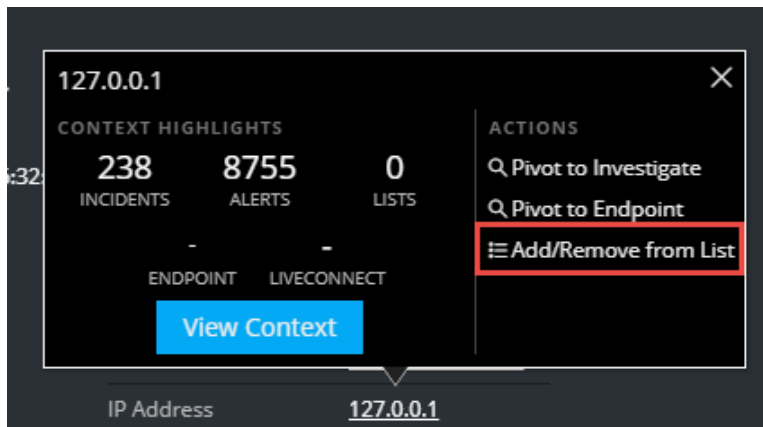
[**アクション**]セクションには、使用可能なアクションが表示されます。前掲の例では、[Investigateへの移行]、[エンドポイントへの移行]、[リストへの追加/削除]オプションを使用できます。

2. 選択したエンティティの詳細を表示するには、[**コンテキストの表示**]ボタンをクリックします。[コンテキスト]パネルが開き、エンティティに関連するすべての情報が表示されます。補足情報については、[\[コンテキスト検索\]パネル- Respondビュー](#)を参照してください。

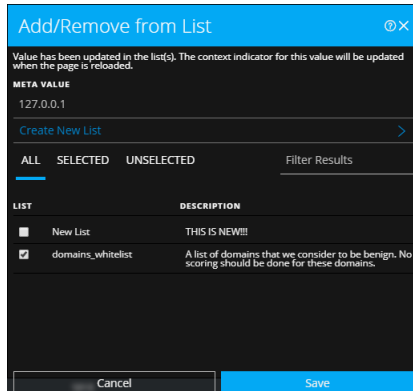
ホワイトリストへのエンティティの追加

下線付きの任意のエンティティは、コンテキスト ツールチップから、ホワイトリストまたはブラックリストなどのリストに追加できます。たとえば、誤検知を減らすためには、下線付きのドメインをホワイトリストして関連エンティティから除外します。

1. [アラートの詳細]ビューのイベント リストまたはイベントの詳細で、Context Hubリストに追加する下線付きのエンティティにポインターを合わせます。コンテキスト ツールチップに使用可能なアクションが表示されます。



2. ツールチップの[アクション]セクションで、[リストへの追加/削除]をクリックします。
[リストへの追加/削除]ダイアログボックスに使用可能なリストが表示されます。



3. 1つ以上のリストを選択し、[保存]をクリックします。
エンティティが、選択したリストに表示されます。
[\[リストへの追加/削除\]ダイアログ](#)に追加情報が提供されます。

ホワイトリストの作成

ホワイトリストは、[インシデントの詳細]ビューで作成する方法と同じ方法でContext Hubで作成できます。「[リストの作成](#)」を参照してください。

NetWitness Endpointへの移行

NetWitness Endpointシック クライアント アプリケーションがインストールされている場合は、コンテキスト ツールチップから起動できます。そこから、疑わしいIPアドレス、ホスト、MACアドレスをさらに調査できます。

1. [アラートの詳細]ビューのイベント リストまたはイベントの詳細で、下線付きのエンティティにポインターを合わせてコンテキスト ツールチップにアクセスします。
2. ツールチップの[アクション]セクションで、[Endpointへの移行]を選択します。
NetWitness Endpointアプリケーションは、Webブラウザの外で開きます。

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

調査への移行

インシデントの詳細を調査するには、Investigateビューにアクセスできます。

1. [アラートの詳細]ビューのイベント リストまたはイベントの詳細で、下線付きのエンティティにポインターを合わせてコンテキスト ツールチップにアクセスします。
2. ツールチップの[アクション]セクションで、[Investigateへの移行]を選択します。
Investigateの[ナビゲート]ビューが開き、より詳細な調査を実行できます。

詳細については、「*調査およびマルウェア解析ユーザガイド*」を参照してください。

インシデントの手動作成

アラートのリストビューでアラートからインシデントを手動で作成することができます。選択したアラートは、他のインシデントの一部にすることはできません。アラートから手動で作成されたインシデントのデフォルトの優先度は[低]ですが、優先度は作成した後に変更できます。手動で作成したインシデントにカテゴリを追加することはできません。

注: インシデントは手動または自動で作成することができます。1つのアラートは、1つのインシデントにのみ関連づけることができます。統合ルールを作成すると、収集されたアラートを分析し、一致したルールに応じてインシデントにグループ化することができます。詳細については、「*NetWitness Respond* 構成ガイド」の「アラートの統合ルールの作成」のトピックを参照してください。

インシデントを手動で作成するには、次の手順を実行します。

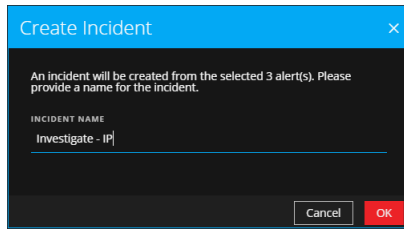
1. [対応] > [アラート] に移動します。
2. アラート リストで、1つまたは複数のアラートを選択します。

注: インシデントIDがないアラートを選択すると、[インシデントの作成] ボタンが有効化されます。アラートがすでにインシデントの一部である場合、このボタンは無効化されます。いずれのインシデントにも属していないアラートをフィルタするには、[フィルタ] パネルの[インシデントの一部] オプションで[いいえ]を選択します。

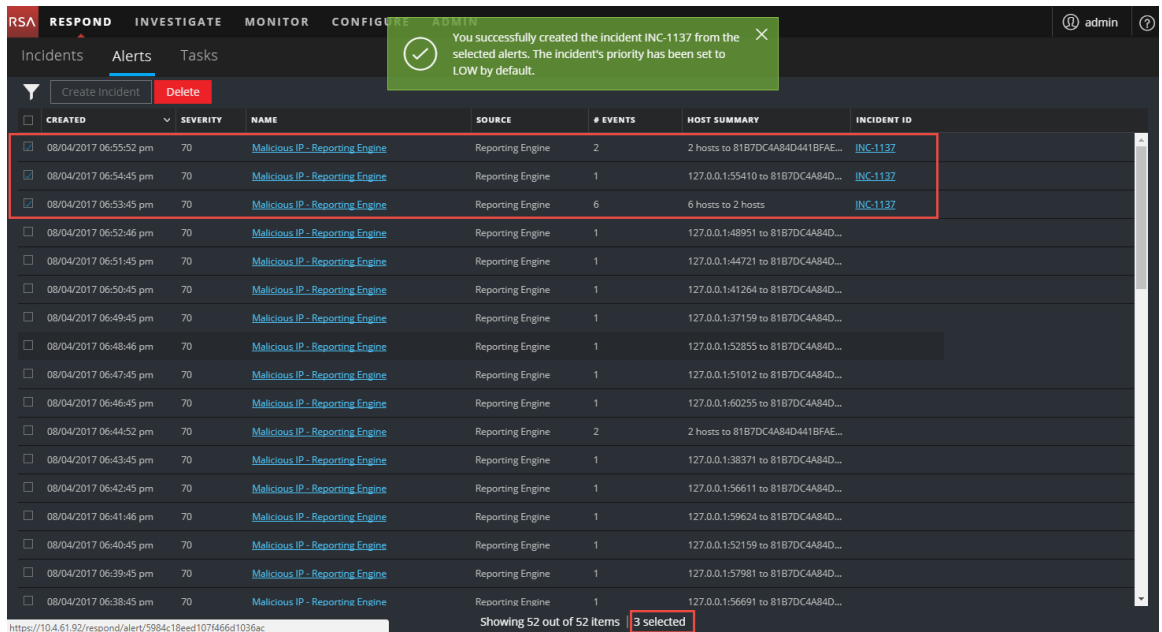
CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID
08/04/2017 06:55:52 pm	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 81B7DC4A84D441BFAE...	
08/04/2017 06:54:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.155410 to 81B7DC4A84D...	
08/04/2017 06:53:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	6	6 hosts to 2 hosts	
08/04/2017 06:52:46 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.148951 to 81B7DC4A84D...	
08/04/2017 06:51:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.144721 to 81B7DC4A84D...	
08/04/2017 06:50:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.141264 to 81B7DC4A84D...	
08/04/2017 06:49:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.137159 to 81B7DC4A84D...	
08/04/2017 06:48:46 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.152855 to 81B7DC4A84D...	
08/04/2017 06:47:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.151012 to 81B7DC4A84D...	
08/04/2017 06:46:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.160255 to 81B7DC4A84D...	
08/04/2017 06:44:52 pm	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 81B7DC4A84D441BFAE...	
08/04/2017 06:43:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.138371 to 81B7DC4A84D...	
08/04/2017 06:42:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.156611 to 81B7DC4A84D...	
08/04/2017 06:41:46 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.159624 to 81B7DC4A84D...	
08/04/2017 06:40:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.152159 to 81B7DC4A84D...	
08/04/2017 06:39:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.157981 to 81B7DC4A84D...	
08/04/2017 06:38:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.156691 to 81B7DC4A84D...	

Showing 52 out of 52 items | 3 selected

3. [インシデントの作成] をクリックします。
[インシデントの作成] ダイアログが表示されます。



4. [インシデント名]フィールドで、インシデントを識別する名前を入力します。たとえば、「Investigate - IP」です。
5. [OK]をクリックします。



選択したアラートからインシデントが作成されたことの確認メッセージが表示されます。新しいインシデントIDが、選択したアラートの[インシデントID]列にリンクとして表示されます。リンクをクリックした場合、そのインシデントの[インシデントの詳細]ビューが表示されます。ここでは、優先度を低から高に変更するなど、情報を更新することができます。

アラートの削除

管理者やデータ プライバシー責任者など、適切な権限を持つユーザは、アラートを削除できません。この手順は、不要または関連性のないアラートを削除するときに役立ちます。これらのアラートを削除すると、ディスク領域が解放されます。

1. [対応]>[アラート]に移動します。

アラートのリスト ビューに、すべてのNetWitness Suiteアラートのリストが表示されます。

2. アラート リストで、削除するアラートを選択し、[削除]をクリックします。

The screenshot shows the NetWitness Respond Alerts list. The table contains the following data:

Created	Severity	Name	Source	# Events	Host Summary	Incident ID
08/04/2017 07:31:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:33945 to 81B7DCA...	
08/04/2017 07:30:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:58016 to 81B7DCA...	
08/04/2017 07:29:46 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:44967 to 81B7DCA...	
08/04/2017 07:28:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:56799 to 81B7DCA...	
08/04/2017 07:27:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:45710 to 81B7DCA...	
08/04/2017 07:26:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:37605 to 81B7DCA...	
08/04/2017 07:25:46 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:56413 to 81B7DCA...	
08/04/2017 07:24:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:52582 to 81B7DCA...	
08/04/2017 07:23:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:36294 to 81B7DCA...	
08/04/2017 07:22:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:43898 to 81B7DCA...	
08/04/2017 07:21:46 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:57445 to 81B7DCA...	
08/04/2017 07:20:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:49017 to 81B7DCA...	
08/04/2017 07:19:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:47857 to 81B7DCA...	
08/04/2017 07:18:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:35185 to 81B7DCA...	
08/04/2017 07:17:46 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:42292 to 81B7DCA...	
08/04/2017 07:16:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:41878 to 81B7DCA...	
08/04/2017 07:15:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:40328 to 81B7DCA...	
08/04/2017 07:14:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	6	6 hosts to 2 hosts	
08/04/2017 07:13:46 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:49575 to 81B7DCA...	
08/04/2017 07:12:45 pm	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:48602 to 81B7DCA...	

アラートを削除する権限を持っていない場合、[削除]ボタンは表示されません。

3. アラートを削除することを確認し、[OK]をクリックします。

The 'Confirm Delete' dialog box contains the following text:

Warning: You are about to delete one or more alerts that may be associated with incidents. Be aware that any associated incidents will be updated or deleted accordingly.

Are you sure you want to delete 2 record(s)? Once applied, this deletion cannot be reversed.

アラートがNetWitness Suiteから削除されます。削除されたアラートがインシデントで唯一のアラートの場合は、インシデントも削除されます。削除されたアラートがインシデントで唯一のアラートでない場合は、削除を反映するようインシデントが更新されます。

Netwitnessインシデント対応に関する参考情報

[対応]ビューのユーザ インタフェースを使用すると、NetWitness Respond機能にアクセスできます。このトピックでは、ユーザ インタフェイスに関する説明のほか、Netwitnessインシデント対応機能を理解するうえで役立つ参考情報も示しています。

トピック

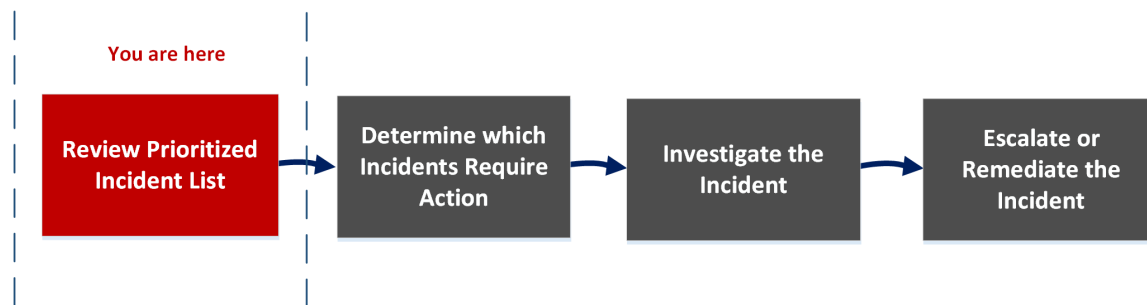
- [インシデント リスト ビュー](#)
- [\[インシデントの詳細\]ビュー](#)
- [アラートのリスト ビュー](#)
- [\[アラートの詳細\]ビュー](#)
- [タスク リスト ビュー](#)
- [\[リストへの追加/削除\]ダイアログ](#)
- [\[コンテキスト検索\]パネル- Respondビュー](#)

インシデント リスト ビュー

インシデント リスト ビュー([対応] > [インシデント])には、インシデント 対応者およびその他のアナリストの、さまざまなソースから作成されたインシデントの優先順位付けられた結果リストが表示されます。たとえば、結果リストには、パケットまたはログのC2などの、自動脅威検出のESAルール、NetWitness Endpoint、ESA Analyticsモジュールから作成されたインシデントが表示される場合があります。インシデント リスト ビューからは、インシデントを迅速に優先順位付けして完了まで管理するために必要な情報に簡単にアクセスできます。

ワークフロー

このワークフローは、NetWitness Suiteでインシデントに対応するためにインシデント 対応者が使用するプロセスの概要を示しています。



インシデント リスト ビューでは、各インシデントに関する基本情報を示す、優先順位付けされたインシデントのリストを確認できます。また、インシデントの割り当て先、優先度、ステータスを変更することもできます。インシデント リストの結果が大きくなる可能性があるため、時間範囲、インシデントID、カスタム日付範囲、優先度、ステータス、割り当て先、カテゴリ別にインシデントをフィルタするためのオプションがあります。

どうしますか？

ロール	処理オプション...	方法を確認する
インシデント対応者、アナリスト、SOCマネージャ	優先順位付けされたインシデントの表示*	インシデントの優先順位リストの確認
インシデント対応者、アナリスト、SOCマネージャ	インシデントリストのフィルタおよびソート*	インシデントリストのフィルタ
インシデント対応者、アナリスト	担当インシデントの表示*	担当インシデントの表示
インシデント対応者、アナリスト	自分へのインシデントの割り当て*	自分へのインシデントの割り当て
インシデント対応者、アナリスト、SOCマネージャ	インシデントの検索*	インシデントの検索
インシデント対応者、アナリスト、SOCマネージャ	インシデントの更新。*	インシデントのエスカレーションまたは修正
インシデント対応者、アナリスト	インシデント詳細の表示。	アクションが必要なインシデントの判断
インシデント対応者、アナリスト	さらに詳しいインシデントの調査。	インシデントの調査
インシデント対応者、アナリスト、SOCマネージャ	タスクの作成。	インシデントのエスカレーションまたは修正

*これらのタスクはここ(つまり、インシデントリストビュー)で完了できます。

関連トピック

- [\[インシデントの詳細\]ビュー](#)
- [インシデントへの対応](#)

簡単な説明

次の例は、[フィルタ]パネルがある最初のインシデント リスト ビューを示しています。インシデントのリストでインシデントをクリックすると、インシデントの[概要]パネルを開くことができます。

The image displays two screenshots of the NetWitness Respond interface. The top screenshot shows the 'Incidents' list view. On the left, there is a 'Filters' panel (labeled 1) with options for 'TIME RANGE', 'INCIDENT ID', 'PRIORITY', 'STATUS', 'ASSIGNEE', and 'CATEGORIES'. The main area shows a table of incidents (labeled 2) with columns for 'CREATED', 'PRIORITY', 'RISK SCORE', 'ID', 'NAME', 'STATUS', 'ASSIGNEE', and 'ALERTS'. The bottom screenshot shows the same list view with an incident detail panel (labeled 3) open for incident INC-1137. The detail panel shows information such as 'Created: 08/04/2017 19:00:32', 'By: admin', 'Risk Score: 0', 'Priority: Critical', 'Status: In Progress', 'Assignee: Analyst User', 'Sources: Reporting Engine', 'Categories:', and 'Catalysts: 3 Indicator(s), 9 Event(s)'. Red arrows indicate the flow from the filter panel to the list, and from a list item to the detail panel.

1 [フィルタ]パネル

2 インシデントのリスト

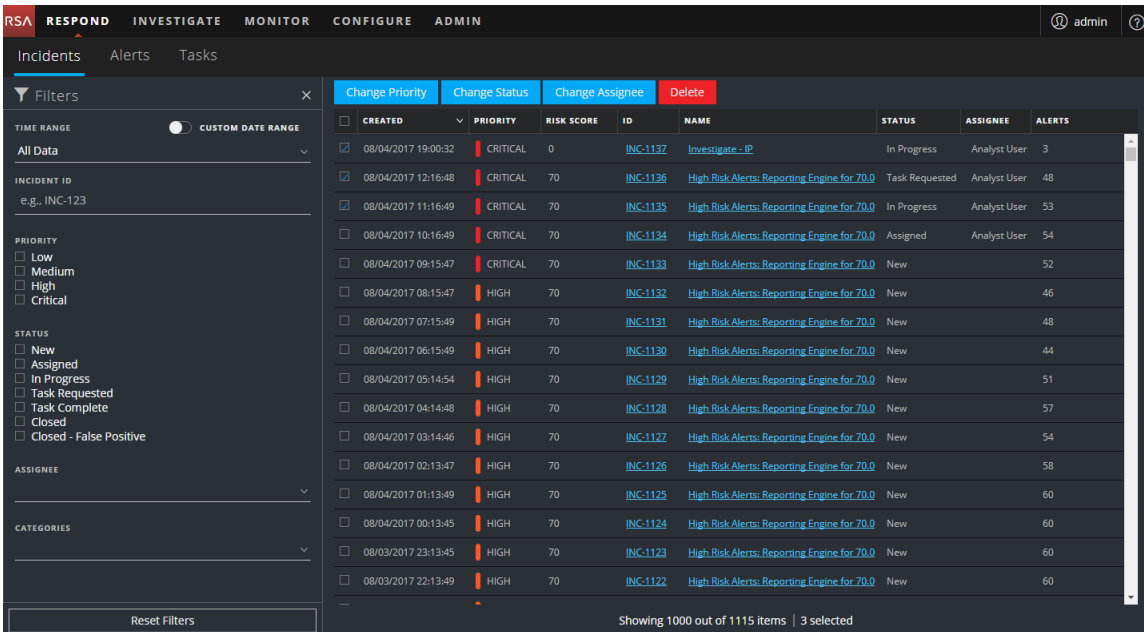
3 [概要]パネル

ハイパーリンクされたIDまたは名前をクリックすると、インシデントのリストから[インシデントの詳細]ビューに直接移動できます。[概要]パネルは、[インシデントの詳細]ビューでも使用できます。[インシデントの詳細]ビューの詳細については、「[\[インシデントの詳細\]ビュー](#)」を参照してください。

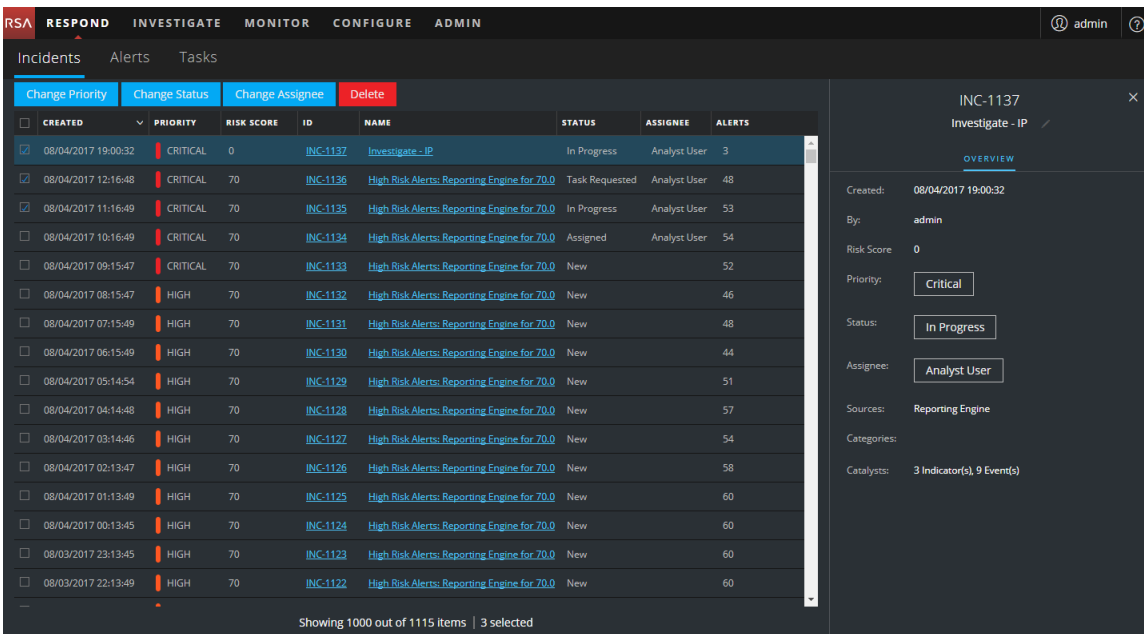
インシデント リスト ビュー

インシデント リスト ビューにアクセスするには、対応 > [インシデント]に移動します。インシデント リスト ビューには、すべてのインシデントのリストが表示されます。インシデント リスト ビューは、[フィルタ]パネル、インシデントのリスト、インシデントの[概要]パネルで構成されています。

次の図は、左側の[フィルタ]パネルと、右側のインシデントのリストを示しています。

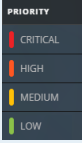


次の図は、左側のインシデントのリストと、右側のインシデントの[概要]パネルを示しています。



インシデントのリスト

インシデントのリストには、優先順位付けされたすべてのインシデントのリストが表示されます。このリストをフィルタして、関心のあるインシデントのみを表示することができます。

列	説明
作成日	インシデントの作成日を示します。
優先度	<p>インシデントの優先度を示します。優先度はクリティカル、高、中、低を指定できます。優先度は色分けされ、赤はクリティカルなインシデント、オレンジは高リスク インシデント、黄色は中リスク インシデント、緑は低リスク インシデントを表します。例：</p> 
リスクスコア	インシデントのリスク スコアを示します。リスク スコアはアルゴリズムで計算されたインシデントのリスクを示し、0～100の範囲です。100が最大のリスク スコアです。
ID	自動的に作成されたインシデント番号を示します。各インシデントには、インシデントのトラックに使用できる固有の番号が割り当てられています。
名前	インシデント名を示します。インシデント名は、インシデントのトリガーに使用されたルールから取得されます。リンクをクリックすると、選択したインシデントの[インシデントの詳細]ビューに移動します。
ステータス	インシデントのステータスを表示します。次のステータスがあります。新規、割り当て済み、対応中、タスク リクエスト 済み、タスク完了、クローズ、クローズ- False Positive。
割り当て先	インシデントに現在割り当てられている、チームのメンバーを示します。

列	説明
ア ラ ト	インシデントに関連するアラートの数を示します。1つのインシデントに多数のアラートが含まれる場合があります。多数のアラートがある場合は、大規模な攻撃を受けている可能性があります。

リストの下部では、現在のページのインシデント数、インシデントの総数、選択したインシデントの数を確認できます。例:「2,517アイテム中1,000個を表示中 | 2個が選択済み」のように表示されます。一度に表示できるインシデントの最大数は1,000です。

[フィルタ] パネル

次の図は、[フィルタ] パネルで使用可能なフィルタを示しています。

The screenshot shows a dark-themed 'Filters' panel with the following sections:

- TIME RANGE**: Includes a toggle switch for 'CUSTOM DATE RANGE'.
- INCIDENT ID**: A text input field with the example 'e.g., INC-123'.
- PRIORITY**: A list of checkboxes for 'Low', 'Medium', 'High', and 'Critical'.
- STATUS**: A list of checkboxes for 'New', 'Assigned', 'In Progress', 'Task Requested', 'Task Complete', 'Closed', and 'Closed - False Positive'.
- ASSIGNEE**: A dropdown menu.
- CATEGORIES**: A dropdown menu.
- Reset Filters**: A button at the bottom of the panel.

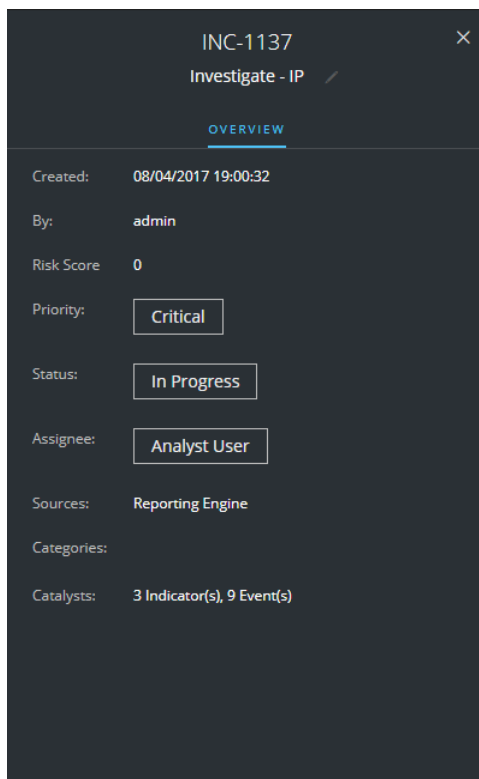
インシデント リスト ビューの左側にある[フィルタ]パネルには、インシデントのリストをフィルタするために使用できるオプションがあります。[フィルタ]パネルから移動しても、インシデント リストビューではフィルタの選択項目が保持されます。

オプション	説明
時間範囲	[時間範囲]ドロップダウン リストから特定の期間を選択できます。時間範囲は、アラートを受信した日付に基づきます。たとえば、[直近1時間]を選択する場合は、過去60分以内に受信されたアラートが表示されます。
カスタムの日付範囲	<p>[時間範囲]オプションを選択する代わりに、特定の日付範囲を指定できます。これを行うには、[カスタムの日付範囲]の前にある白色の円をクリックし、[開始日]と[終了日]のフィールドを表示します。カレンダーから日付と時刻を選択します。</p> 
インシデントID	検索するインシデントのインシデントID(INC-1050など)を入力できます。
優先度	表示する優先度を選択します。
ステータス	1つまたは複数のインシデントのステータスを選択します。たとえば、誤検知インシデント(最初は疑わしいと判断され、後で安全であると判明したインシデント)のみを表示するには、[クローズ- False Positive]を選択します。

オプション	説明
割り当て先	表示するインシデントの割り当て先を選択します。たとえば、CaleまたはStanleyに割り当てられたインシデントのみを表示する場合は、[割り当て先]ドロップダウン リストから[Cale]と[Stanley]を選択します。割り当て先に関係なくインシデントを表示する場合は、[割り当て先]で何も選択しないでください。
カテゴリ	ドロップダウン リストから、1つまたは複数のカテゴリを選択します。たとえば、バックドアまたは権限の不正利用のカテゴリに分類されたインシデントのみを表示する場合は、[バックドア]と[権限の不正利用]を選択します。
フィルタのリセット	フィルタの選択を解除します。

[概要]パネル

[概要]パネルには、選択したインシデントに関する基本的なサマリ情報が表示されます。インシデント リストから、インシデントをクリックして[概要]パネルにアクセスできます。[インシデントの詳細]ビューの[概要]パネルにも同じ情報が表示されます。





次の表に、インシデントの[概要]パネルに表示されるフィールドを示します。

フィールド	説明
<インシデントID>	インシデントIDが表示されます。
<インシデント名>	インシデントの名前が表示されます。インシデント名をクリックすると変更できます。たとえば、ルールによって多数の同じ名前のインシデントが作成される可能性があります。この場合、インシデント名をより具体的に変更することができます。
作成日	インシデントの作成日時を示します。
ルール/作成者	インシデントを作成したルールの名前またはインシデントを作成したユーザの名前を示します。
リスクスコア	アルゴリズムで計算されたインシデントのリスクを示し、0～100の範囲です。100が最大のリスクスコアです。
優先度	インシデントの優先度を示します。優先度はクリティカル、高、中、低を指定できます。優先度を変更するには、優先度ボタンをクリックし、ドロップダウンリストから新しい優先度を選択します。
ステータス	インシデントのステータスを表示します。ステータスは、新規、割り当て済み、対応中、タスクリクエスト済み、タスク完了、クローズ、クローズ- False Positiveにできます。ステータスを変更するには、ステータスボタンをクリックし、ドロップダウンリストから新しいステータスを選択します。
割り当て先	インシデントに現在割り当てられている、チームのメンバーを示します。割り当て先を変更するには、[割り当て先]ボタンをクリックし、ドロップダウンリストから新しい割り当て先を選択します。
ソース	疑わしいアクティビティの検出に使用されたデータソースを表示します。
カテゴリ	インシデント イベントのカテゴリを表示します。
要因	インシデントを発生させたインジケータのカウントを表示します。

ツールバーのアクション

この表には、インシデント リスト ビューで使用できるツールバーのアクションが示されています。

オプション	説明
	アラート リストに表示するアラートを指定できるように、[フィルタ]パネルを開くことができます。
	パネルを閉じます。
[優先度の変更]ボタン	インシデント リストで選択した1つ以上のインシデントの優先度を変更できます。
[ステータス変更]ボタン	選択した1つ以上のインシデントのステータスを変更できます。
[割り当て先の変更]ボタン	選択した1つ以上のインシデントの割り当て先を変更できます。
[削除]ボタン	管理者やデータ プライバシー責任者などの、適切な権限を持っている場合は、選択したインシデントを削除できます。

[インシデントの詳細]ビュー

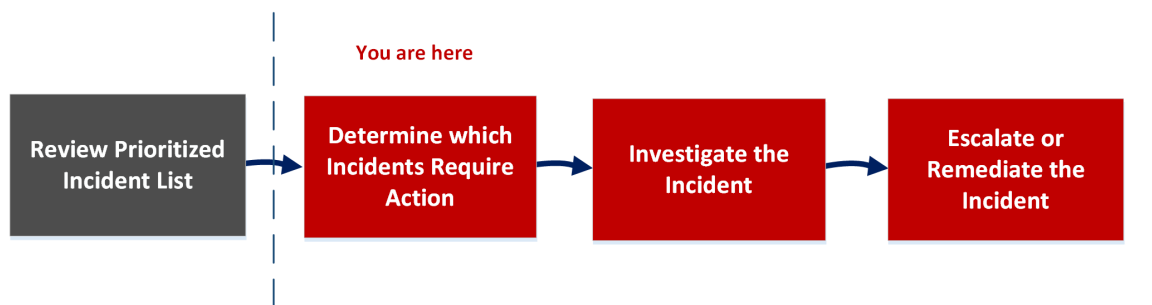
[インシデントの詳細]ビュー([RESPOND] > [インシデント] > インシデント リストのIDまたは名前のハイパーリンクをクリック)では、広範なインシデントの詳細を表示してアクセスすることができます。[インシデントの詳細]ビューには、次の機能が利用できる複数のパネルが含まれています。

- **概要:** インシデント サマリーを表示し、インシデントを更新します。
- **インジケータ:** インシデントに関連するインジケータ(アラート)、アラート内のイベント、使用可能なエンリッチメント情報を表示します。
- **ノードのグラフ:** エンティティ(IPアドレス、MACアドレス、ユーザー、ホスト、ドメイン、ファイル名、ファイルハッシュ)間のサイズと相互作用をビジュアル化します。
- **イベント データシート:** インシデントに関連するイベントを調査します。
- **ジャーナル:** メモを追加し、他のアナリストとの共同作業を行います。
- **タスク:** インシデント タスクを作成し、クローズまでトラックします。
- **関連インジケータ:** インシデントに関連するインジケータ(アラート)を表示し、インシデントに関連付けられていない場合はインシデントに追加します。

[インシデントの詳細]ビューでデータをフィルターして、関心のあるインジケータおよびエンティティを調査することもできます。

ワークフロー

このワークフローは、NetWitness Suiteでインシデントに対応するためにインシデント対応担当が使用するプロセスの概要を示しています。



[インシデントの詳細]ビューでは、インシデントについて提供された広範な情報を使用して、どのインシデントにアクションが必要かを判断できます。また、インシデントを調査し、エスカレーションまたは修正するためのツールと情報もあります。

どうしますか?

ロール	処理オプション...	方法を確認する
インシデント対応担当、アナリスト、SOCマネージャ	優先順位付けされたインシデントの表示、インシデントリストのフィルターとソート、インシデントの検索、担当インシデントの表示、自分へのインシデントの割り当て。	インシデントの優先順位リストの確認
インシデント対応担当、アナリスト	インシデントの詳細の表示。 *	インシデントの詳細の表示
インシデント対応担当、アナリスト	アラートとエンリッチメントの表示。 *	インジケータとエンリッチメントの表示
インシデント対応担当、アナリスト	イベントの表示。 *	イベントの表示と調査
インシデント対応担当、アナリスト	イベントに関連するエンティティのグラフの表示。 *	イベントに関連するエンティティの表示と調査
インシデント対応担当、アナリスト	インシデントのデータのフィルター。 *	[インシデントの詳細]ビューでのデータのフィルタ処理
インシデント対応担当、アナリスト	インシデント メモの表示と追加。 *	「 インシデント メモの表示 」および「 NetWitnessの外で実行した手順の記録 」
インシデント対応担当、アナリスト	タスクの表示と作成。 *	「 インシデントに関連するタスクの表示 」および「 タスクの作成 」
インシデント対応担当、アナリスト	関連するアラートの追加と、インシデントへのアラートの追加。 *	「 関連インジケータの検索 」および「 インシデントへの関連インジケータの追加 」

ロール	処理オプション...	方法を確認する
インシデント対応担当、アナリスト	Context Hubからのインシデントに関するコンテキスト情報の表示。*	コンテキスト情報の表示
インシデント対応担当、アナリスト	エンティティをホワイトリストに追加することによる誤検知の削減。*	ホワイトリストへのエンティティの追加
インシデント対応担当、アナリスト	Investigationへの移行。*	調査への移行
インシデント対応担当、アナリスト	NetWitness Endpointへの移行。*	NetWitness Endpointへの移行
インシデント対応担当、アナリスト	インシデントの更新またはクローズ。*	「 インシデントの更新 」および「 インシデントのクローズ 」
インシデント対応担当、アナリスト、SOCマネージャ	すべてのタスクの表示。	インシデントのエスカレーションまたは修正
インシデント対応担当、アナリスト、SOCマネージャ	インシデントとタスクのバルク更新。	インシデントのエスカレーションまたは修正

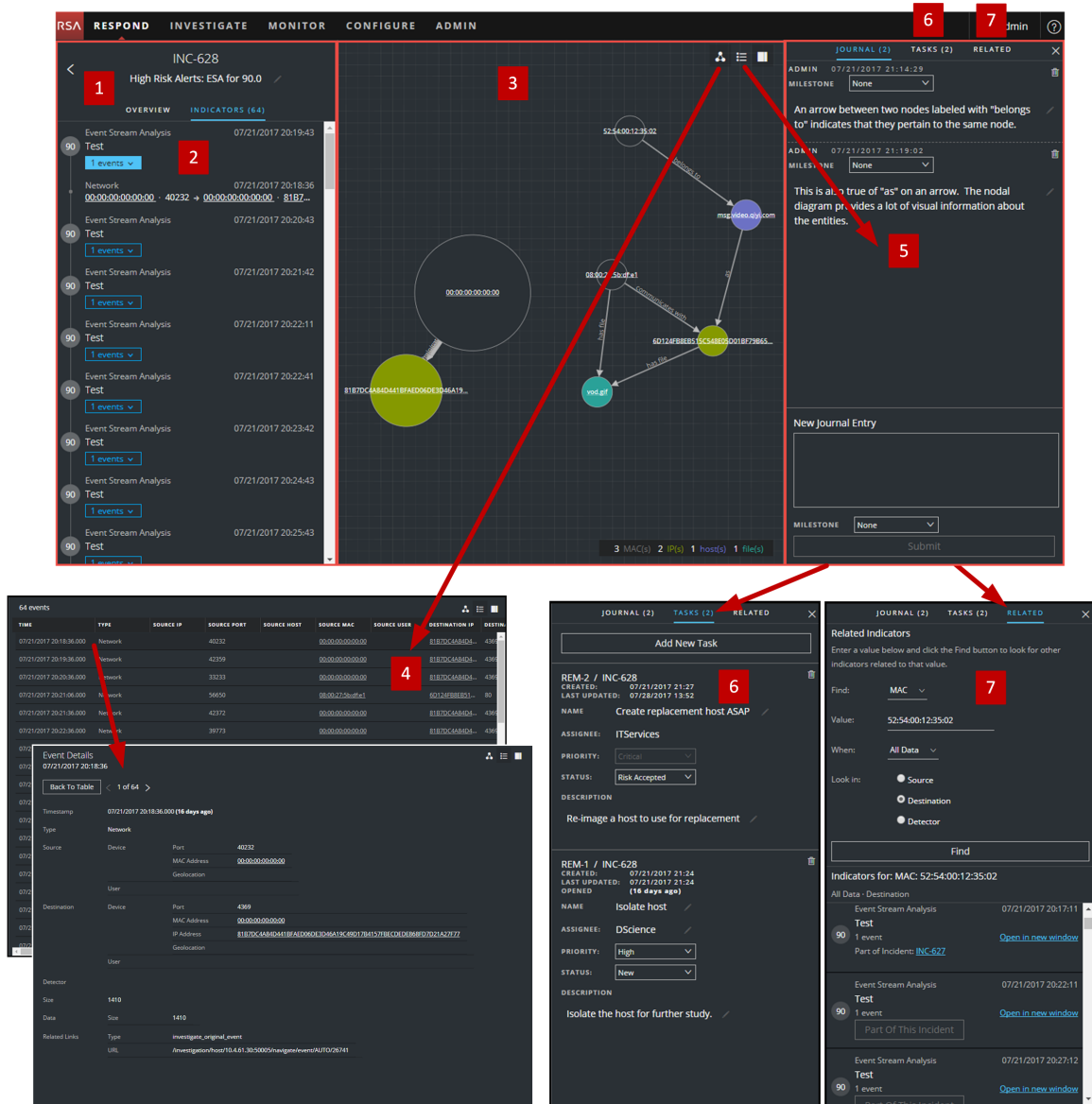
*これらのタスクはここ(つまり、[インシデントの詳細]ビュー)で完了できます。

関連トピック

- [インシデント リスト ビュー](#)
- [アクションが必要なインシデントの判断](#)
- [インシデントの調査](#)
- [インシデントのエスカレーションまたは修正](#)

簡単な説明

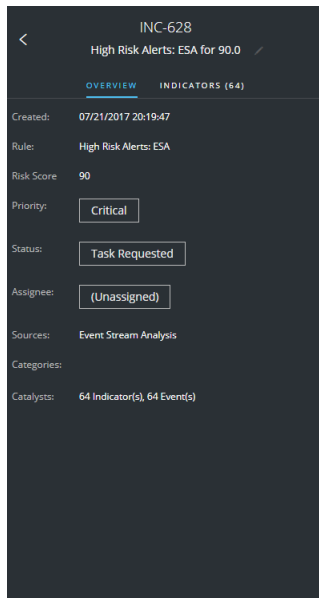
次の例は、[インシデントの詳細]ビューのパネルの場所を示しています。



- 1 [概要] パネル(表示するには、[概要] タブをクリックします)。
- 2 [インジケーター] パネル
- 3 ノードのグラフ
- 4 イベント データシート(イベントの詳細を表示するには、イベント リストのイベントをクリックします)。
- 5 [ジャーナル] パネル
- 6 [タスク] パネル(表示するには、[タスク] タブをクリックします)。
- 7 [関連インジケーター] パネル(表示するには、[関連] タブをクリックします)。

[概要]パネル

[概要]パネルには、選択したインシデントに関する基本的なサマリー情報が表示されます。また、インシデント名を変更することや、インシデントの優先度、ステータス、割り当て先を更新することもできます。[インシデント リスト]ビューの[概要]パネルにも同じ情報が表示されます。詳細については、[インシデント リスト]ビューの「[\[概要\]パネル](#)」のトピックを参照してください。



[インジケータ]パネル

[インジケータ]パネルには、インジケータの時系列の一覧が含まれています。インジケータは、ESAアラートやNetWitness Endpointアラートなどのアラートです。(タイムラインとは異なり、インシデント内のイベントのタイミングをビジュアル化して表示します)。このリストは、インジケータと重要なデータを接続するのに役立ちます。たとえば、コマンドに接続されているIPアドレスと通信ESAアラートもNetWitness Endpointアラートやその他の疑わしいアクティビティをトリガーすることがあります。

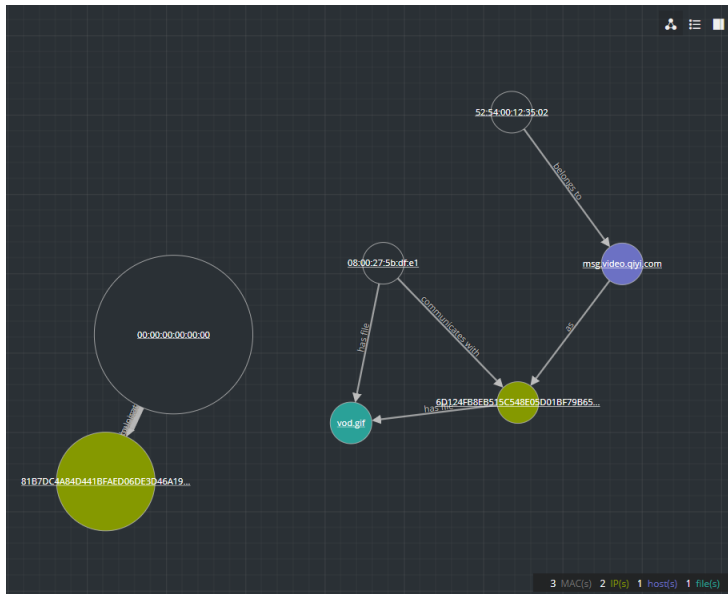
[インジケータ]パネルを表示するには、[インシデントの詳細]ビューの左側のパネルで[インジケータ]を選択します。

Indicator ID	Event Stream Analysis	Timestamp
90	Event Stream Analysis	07/21/2017 20:19:43
	Test	
	Network	07/21/2017 20:18:36
	00:00:00:00:00:00 - 40232 → 00:00:00:00:00:00 - 8187	
90	Event Stream Analysis	07/21/2017 20:20:43
	Test	
90	Event Stream Analysis	07/21/2017 20:21:42
	Test	
90	Event Stream Analysis	07/21/2017 20:22:11
	Test	
90	Event Stream Analysis	07/21/2017 20:22:41
	Test	
90	Event Stream Analysis	07/21/2017 20:23:42
	Test	
90	Event Stream Analysis	07/21/2017 20:24:43
	Test	
90	Event Stream Analysis	07/21/2017 20:25:43
	Test	

データソースの情報は、インジケータの名前の下に表示されます。インジケータの作成日付と時刻、インジケータのイベントの数も確認できます。

ノードのグラフ

ノードのグラフは、インシデントに関連するエンティティを表示する対話形式のグラフです。エンティティは、IPアドレス、MACアドレス、ユーザー、ホスト、ドメイン、ファイル名、ファイルハッシュなどの特定のメタです。



ノード

ノードのグラフでは、円がノードを表します。次の表は、ノードのグラフのノードのタイプの説明です。

ノード	説明
IPアドレス	イベントが検出された異常である場合は、検知器のIPが表示されます。イベントがトランザクションの場合は、デスティネーションIPとソースIPが表示されます。
MACアドレス	各タイプのIPアドレスのMACアドレスを確認できます。
ユーザー	マシンがユーザーに関連づけられている場合、ユーザーノードを確認できます。
ホスト	ホストは、任意のサービスがインストールされている、FQDN(完全修飾ドメイン名)またはIPアドレスで指定された、物理的な機器または仮想マシンです。
ドメイン	
ファイル名	イベントにファイルが関連する場合、ファイル名を確認できます。
ファイルハッシュ	イベントにファイルが関係する場合、ファイルハッシュを確認できます。

ノードのグラフの下部の凡例は、各タイプのノードの数とノードの色コードを示します。また、IPアドレスなどの値がハッシュされたときに、エンティティを見つけるためにも役立ちます。

任意のノードをクリックし、ドラッグして位置を変更することができます。

矢印

ノード間の矢印は、エンティティの関係に関する追加情報を提供します。次の表は、ノードのグラフの矢印のタイプの説明です。

矢印	説明
通信先	「通信先」というラベルが付けられたソースマシンノード(IPアドレスまたはMACアドレス)とデスティネーションマシンノード間の矢印は、通信の方向を示します。

矢印	説明
として	「として」というラベルが付けられたノード間の矢印は、矢印の先のIPアドレスに関する追加情報を提供します。たとえば、「として」というラベルが付けられたIPアドレスノードを指すホストノードの円からの矢印がある場合は、ホストノードの円の上にある名前がそのIPアドレスのホスト名であり、別のエンティティではないことを示します。
ファイルを持つ	「持つ」というラベルが付けられたマシンノード (IPアドレス、MACアドレス、ホスト) とファイルハッシュノード間の矢印は、IPアドレスがそのファイルを持つことを示します。
用途	「使用」というラベルが付けられたユーザーノードとマシンノード (IPアドレス、MACアドレス、ホスト) 間の矢印は、ユーザーがイベント中に使用していたマシンを示します。
名前は	「名前は」というラベルが付けられたファイルハッシュノードとファイル名ノード間の矢印は、ファイルハッシュがその名前のファイルに対応することを示します。
所属先	「所属先」というラベルが付けられた2台のノード間の矢印は、これらが同じノードに関連することを示します。たとえば、「所属先」というラベルが付けられたMACアドレスとホスト間の矢印は、それがホストのMACアドレスであることを示します。

線のサイズが太い矢印は、ノード間の通信が多いことを示します。大きなノード(円)は、小さいノードよりもアクティビティが多いことを示します。大きなノードは、イベントに記載されている最も一般的なエンティティです。

イベント データシート

イベント データシートには、インシデントに関連するイベントが表示されます。イベント時間、ソースIP、デスティネーションIP、検知器IP、ソースのユーザー、デスティネーションのユーザー、イベントに関するファイル情報など、イベントに関する情報が表示されます。表示される情報の量は、イベントタイプに依存します。

イベント データシートには、複数のイベントのイベント リストまたは1つのイベントのイベントの詳細が表示されます。

イベント リスト

次の図は、イベント リストを示しています。

TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION PORT
07/21/2017 20:18:36.000	Network		40232		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:19:36.000	Network		42359		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:20:36.000	Network		33233		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:21:06.000	Network		56650		08:00:27:5b:df:e1		6D124FB8E851...	80
07/21/2017 20:21:36.000	Network		42372		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:22:36.000	Network		39773		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:23:36.000	Network		45887		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:24:36.000	Network		37099		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:25:36.000	Network		42600		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:26:06.000	Network		56948		08:00:27:5b:df:e1		6D124FB8E851...	80
07/21/2017 20:26:36.000	Network		54561		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:27:36.000	Network		41407		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:28:36.000	Network		59201		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:29:36.000	Network		58709		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:30:36.000	Network		51224		00:00:00:00:00:00		81B7DC4A84D4...	4369
07/21/2017 20:31:06.000	Network		57255		08:00:27:5b:df:e1		6D124FB8E851...	80
07/21/2017 20:31:15.000	Network		57946		00:00:00:00:00:00		81B7DC4A84D4...	5672
07/21/2017 20:31:36.000	Network		41631		00:00:00:00:00:00		81B7DC4A84D4...	4369

次の表は、イベント リストの列を説明したものです。

列	説明
時刻	イベントの発生時刻を示します。
タイプ	ログやネットワークなどのアラートのタイプを示します。
ソースIP	2台のマシン間のトランザクションがあった場合は、ソースIPアドレスを示します。
ソースポート	トランザクションのソースポートを示します。同じIPアドレスに、ソースおよびデスティネーションポートがあることがあります。
ソースホスト	イベントが発生したデスティネーションホストを示します。
ソースMAC	ソースマシンのMACアドレスを示します。
ソースユーザー	ソースマシンのユーザーを示します。
デスティネーションIP	2台のマシン間のトランザクションがあった場合は、デスティネーションIPアドレスを示します。

列	説明
デスティネーション ポート	トランザクションのデスティネーション ポートを示します。同じIPアドレスに、ソースおよびデスティネーション ポートがあることがあります。
デスティネーション ホスト	デスティネーション マシンのホスト名を示します。
デスティネーション MAC	デスティネーション マシンのMACアドレスを示します。
デスティネーション ユーザー	デスティネーション マシンのユーザーを示します。
検知器 IP	異常が検出されたマシンのIPアドレスを示します。
ファイル名	ファイルがイベントと関連している場合は、ファイル名を示します。
ファイル ハッシュ	ファイルの内容のハッシュを示します。

イベントの詳細情報

イベントの詳細を表示するには、イベント リストのイベントをクリックします。リストに1つのみのイベントがある場合は、リストではなくそのイベントの詳細が表示されます。

Event Details
07/21/2017 20:18:36

[Back To Table](#) < 1 of 64 >

Timestamp: 07/21/2017 20:18:36.000 (16 days ago)

Type: Network

Source: Device: Port: 40232
MAC Address: 00:00:00:00:00:00
Geolocation

User:

Destination: Device: Port: 4369
MAC Address: 00:00:00:00:00:00
IP Address: 81B7DC4A84D441BFAED060E3D46A19C49D1784157FBECCDEE868FD7D21A27F77
Geolocation

User:

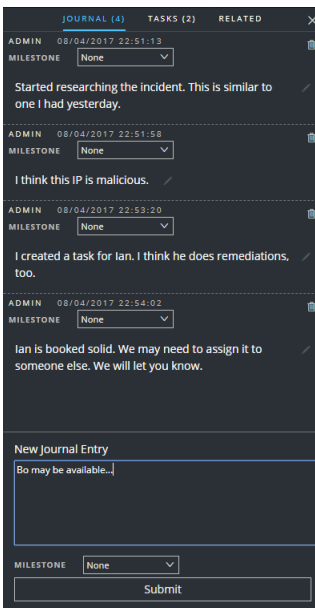
Detector: Size: 1410

Data: Size: 1410

Related Links: Type: investigate_original_event
URL: /investigation/hosts/10.4.61.30:50005/navigate/event/AUTO/26741

[ジャーナル] パネル

インシデントの[ジャーナル]は、インシデントのアクティビティの履歴を示します。

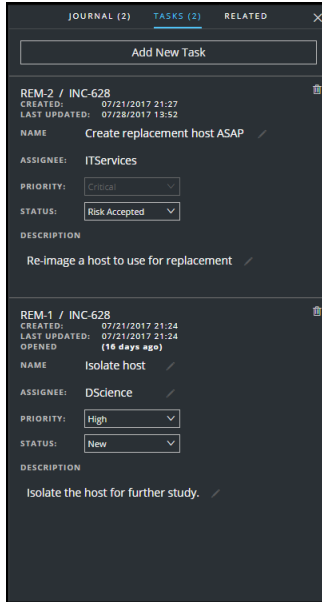


以下の表では、[新しいジャーナル エントリー]のオプションについて説明します。

フィールド	説明
新しいジャーナル エントリー	このフィールドにメモを入力します。
マイルストーン	(オプション) 該当する場合は、マイルストーンを選択します。このフィールドは、インシデントの重要なイベントをトラックするために使用されます。
[送信] ボタン	[送信]をクリックすると、ジャーナルにエントリーが追加されます。ジャーナル エントリーは、そのインシデントを表示するすべてのユーザーに表示されます。

[タスク] パネル

[タスク] パネルでは、インシデント タスクをクローズまで管理およびトラッキングできます。



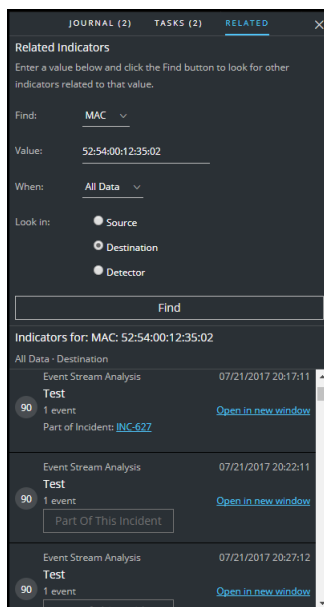
次の表に、[タスク]のフィールドの説明を示します。

フィールド	説明
<タスクID> / <インシデントID>	自動生成されたタスクID/タスクに関連付けられたインシデント。
作成日	タスクの作成日。
最終更新日	タスクが最後に変更された日付。
開いた日	タスクが開かれてから経過した時間。3分前や2日前などです。
名前	タスクの名前。例：マシンの再イメージ化。このフィールドをクリックすると編集することができます。
割り当て先	タスクに割り当てられたユーザーのユーザー名。このフィールドをクリックすると編集することができます。
優先度	タスクの優先度。低、中、高、クリティカルがあります。優先度ボタンをクリックし、ドロップダウンリストからタスクの新しい優先度を選択することができます。

フィールド	説明
ステータス	タスクのステータス。新規、割り当て済み、進行中、改善済み、リスク受容、該当なしがあります。ステータス ボタンをクリックし、ドロップダウン リストからタスクの新しいステータスを選択することができます。
説明	タスクについて説明するための情報を入力します。該当する参照番号を含めることができます。このフィールドをクリックすると編集することができます。

[関連インジケータ] パネル

[関連インジケータ] パネルでは、NetWitness Suite アラート データベースを検索して、このインシデントに関連するアラートを探することができます。アラートがインシデントにまだ関連付けられていない場合は、探したアラートをインシデントに追加できます。



次の表では、パネルの上部にある検索セクションのフィールドについて説明します。

フィールド	説明
検索	アラートで検索するエンティティを選択します。たとえば、IPなどです。
値	エンティティの値を入力します。たとえば、エンティティの実際のIPアドレスを入力します。

フィールド	説明
名称変更された	アラートを検索する時間範囲を選択します。たとえば、[直近24時間]を選択します。
検索場所	<p>検索するエンティティのタイプを指定します。</p> <ul style="list-style-type: none"> ・ ソース: 2台のマシン間のトランザクションのソース マシン。 ・ デスティネーション: 2台のマシン間のトランザクションのデスティネーション マシン。 ・ 検知器: 異常が検出された1台のマシン。 ・ ドメイン: このオプションは、[検索]フィールドで[ドメイン]を選択すると使用可能です。 <p>たとえば、特定のIPアドレスがソース デバイスとして機能する、アラートを検索するソースを選択します。次の各タイプのデバイスを個別に検索することができます。ソース、デスティネーション、検知器。</p>
[検索]ボタン	検索を開始します。関連インジケータのリストが、[インジケータ]セクションの[検索]ボタンの下に表示されます。

次の表では、パネルの下部にある[インジケータ](結果)セクションのオプションについて説明します。

オプション	説明
以下を示すインジケータ:	検索結果を表示します。
[新規ウィンドウで開く]リンク	インジケータのアラートの詳細を表示します。
[インシデントへの追加]ボタン	インシデントに関連インジケータを追加します。[インジケータ]パネルに、関連インジケータが追加されます。
[このインシデント生成]ボタン	インジケータがすでにインシデントの一部であることを示します。

ツールバーのアクション

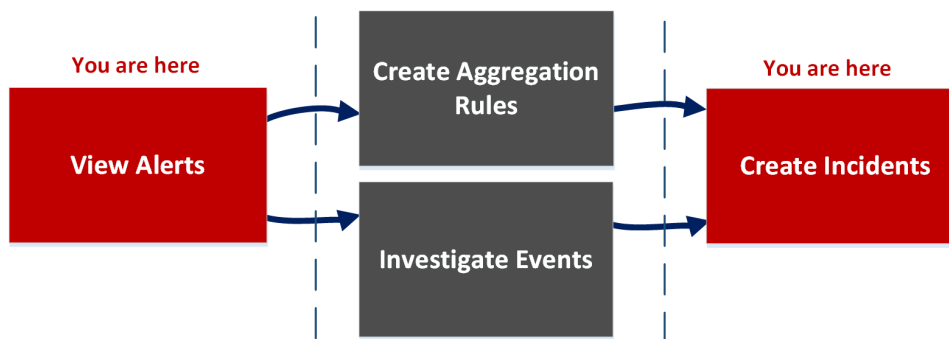
オプション	説明
	([インシデントに戻る]) インシデント リスト ビューに戻れます。
	パネルを閉じます。
	ジャーナル エントリーやタスクなどのエントリーを削除します。
[優先度] ボタン	([概要] パネル内) インシデント リストで選択した1つ以上のインシデントの優先度を変更できます。
[ステータス] ボタン	([概要] パネル内) 選択した1つ以上のインシデントのステータスを変更できます。
[割り当て先] ボタン	([概要] パネル内) 選択した1つ以上のインシデントの割り当て先を変更できます。
 (表示: グラフ)	ノードのグラフを表示できます。
 (表示: データシート)	イベント データシートを表示できます。イベント データシートには、複数のイベントのイベント リストまたは1つのイベントのイベントの詳細が表示されます。
 (ジャーナル、タスク、関連)	[ジャーナル] パネル、[タスク] パネル、[関連インジケータ] パネルを表示できます。

アラートのリスト ビュー

アラートのリスト ビュー([対応] > [アラート]) では、NetWitness Suiteが受信したすべての脅威アラートおよびインジケータを1つの場所に表示することができます。これには、ESAの相関ルール、ESA Analytics、Malware Analysis、Reporting Engine、NetWitness Endpoint、その他多数から受信したアラートを含めることができます。アラートのリスト ビューでは、各種のアラートを表示し、フィルタとグループ化を行ってインシデントを作成できます。

ワークフロー

このワークフローは、アナリストがアラートの確認やインシデントの作成に使用している上位レベルのプロセスを示しています。



アラートのリスト ビューでは、NetWitness Suiteが受信したすべてのソースからアラートのリストを確認することができます。その後、それらのアラートをさらに調査し、アラートからインシデントを作成したり、インシデントを作成する統合ルールを作成することができます。

注: NetWitness Suite 自動脅威検出を使用すると、手動でルールを作成することなくインシデントを作成できます。

どうしますか?

ロール	処理オプション...	方法を確認する
インシデント対応者、アナリスト	NetWitness Suiteですべてのアラートを表示する。*	アラートの表示
インシデント対応者、アナリスト	アラートをフィルタする。*	アラート リストのフィルタ

ロール	処理オプション...	方法を確認する
インシデント対応者、アナリスト	アラートの概要情報とRAWアラート メタデータを表示する。 *	アラートのサマリ情報の表示
インシデント対応者、アナリスト	アラートからインシデントを作成する。*	インシデントの手動作成
管理者、データプライバシー責任者	アラートを削除する。*	アラートの削除
SOCマネージャ、管理者	統合ルールを作成する。	「 <i>NetWitness Respond</i> 構成ガイド」の「アラートの統合ルールの作成」を参照してください。
インシデント対応者、アナリスト	アラートのイベントを調査する。	アラートのイベント詳細の表示 および イベントの調査
インシデント対応者、アナリスト	既存のインシデントにアラートを追加する。	インシデントへの関連インジケータの追加

*これらのタスクはここ(つまり、アラートのリスト ビュー)で完了できます。

関連トピック

- [\[アラートの詳細\]ビュー](#)
- [アラートのレビュー](#)

アラートのリスト ビュー

アラートのリスト ビューにアクセスするには[対応] > [アラート]に移動します。アラートのリスト ビューでは、NetWitness SuiteのRespond Serverデータベースが受信したすべてのアラートとインジケータのリストを表示できます。次の図の左側に[フィルタ]パネルを示します。

アラートのリストビューは、[フィルタ]パネル、アラートリスト、アラートの[概要]パネルで構成されます。アラートリストでアラートをクリックすると、右側にアラートの[概要]パネルを表示することができます。

アラート リスト

アラート リストにはNetWitness Suiteのすべてのアラートが表示されます。このリストをフィルタして、関心のあるアラートのみを表示することができます。

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID
08/04/2017 14:54:52	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 81B7DC4A84D441BFA...	
08/04/2017 14:53:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:37666 to 81B7DC4A84D...	
08/04/2017 14:51:53	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 81B7DC4A84D441BFA...	
08/04/2017 14:50:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:46295 to 81B7DC4A84D...	
08/04/2017 14:48:52	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 81B7DC4A84D441BFA...	
08/04/2017 14:47:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:43869 to 81B7DC4A84D...	
08/04/2017 14:45:53	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 81B7DC4A84D441BFA...	
08/04/2017 14:44:45	70	Malicious IP - Reporting Engine	Reporting Engine	6	6 hosts to 2 hosts	
08/04/2017 14:43:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:44012 to 81B7DC4A84D...	
08/04/2017 14:42:46	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:37634 to 81B7DC4A84D...	
08/04/2017 14:41:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:39783 to 81B7DC4A84D...	
08/04/2017 14:40:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:33011 to 81B7DC4A84D...	
08/04/2017 14:39:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:39369 to 81B7DC4A84D...	
08/04/2017 14:38:46	70	Malicious IP - Reporting Engine	Reporting Engine	6	6 hosts to 2 hosts	
08/04/2017 14:37:45	70	Malicious IP - Reporting Engine	Reporting Engine	6	6 hosts to 2 hosts	
08/04/2017 14:36:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:44754 to 81B7DC4A84D...	
08/04/2017 14:34:51	70	Malicious IP - Reporting Engine	Reporting Engine	2	2 hosts to 81B7DC4A84D441BFA...	
08/04/2017 14:33:45	70	Malicious IP - Reporting Engine	Reporting Engine	1	127.0.0.1:46207 to 81B7DC4A84D...	
08/04/2017 14:31:53	70	Malicious IP - Reporting Engine	Reporting Engine	7	7 hosts to 2 hosts	

Showing 52 out of 52 items | 3 selected

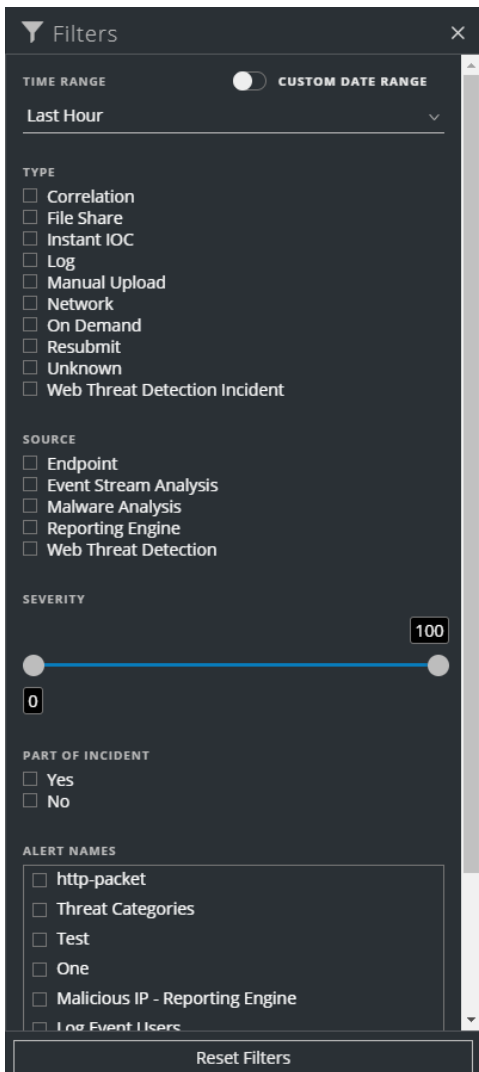
列	説明
	削除する1つまたは複数のアラートを選択できます。管理者やデータプライバシー責任者など、適切な権限を持つユーザは、アラートを削除できます。
作成日	アラートがソースシステムに記録された日時を表示します。
重大度	アラートの重大度のレベルを表示します。値は1～100です。
名前	アラートの基本的な説明を表示します。
ソース	アラートの元のソースを表示します。アラートのソースは、NetWitness Endpoint、Malware Analysis、ESAの相関ルール、ESA Analytics、Reporting Engine、その他多数のソースがあります。

列	説明
イベント数	アラートに含まれるイベントの数を示します。この値は、ソースによって異なります。たとえば、NetWitness EndpointアラートとMalware Analysisアラートでは、常にイベントの数が1つになります。特定のタイプのアラートでは、イベント数が多いとより高いリスクを示すことがあります。
ホスト サマリ	ホストの詳細(アラートのトリガー元のホスト名など)を表示します。詳細には、アラートのソースホストや宛先ホストに関する情報が含まれる場合があります。アラートの中には、複数のホストにまたがってイベントを記述するものがあります。
インシデントID	アラートのインシデントIDを表示します。インシデントIDがない場合は、アラートがインシデントに属さないことを示します。この場合、このアラートを含めるインシデントを作成することも、アラートを既存のインシデントに追加することもできます。

リストの下部では、現在のページのアラート数、アラートの総数、選択したアラートの数を確認できます。例:「377アイテム中377個を表示中 | 3個が選択済み」のように表示されます

[フィルタ]パネル

次の図は、[フィルタ]パネルで使用可能なフィルタを示しています。



アラートのリスト ビューの左側にある[フィルタ]パネルには、アラート リストをフィルタするために使用できるオプションがあります。[フィルタ]パネルから移動しても、アラートのリスト ビューではフィルタの選択項目が保持されます。

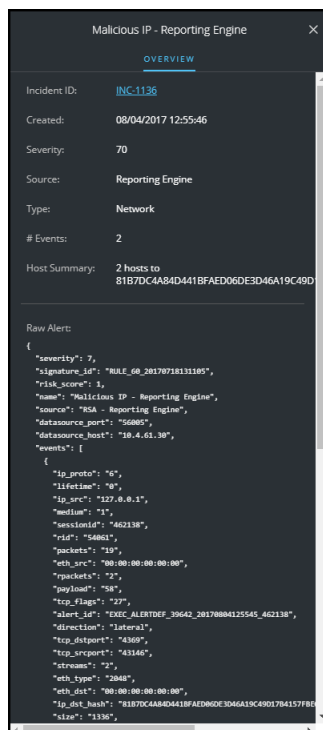
オプション	説明
時間範囲	[時間範囲]ドロップダウン リストから特定の期間を選択できます。時間範囲は、アラートを受信した日付に基づきます。たとえば、[直近1時間]を選択する場合は、過去60分以内に受信されたアラートが表示されます。
カスタムの日付範囲	<p>[時間範囲]オプションを選択する代わりに、特定の日付範囲を指定できます。これを行うには、[カスタムの日付範囲]の前にある白色の円をクリックし、[開始日]と[終了日]のフィールドを表示します。カレンダーから日付と時刻を選択します。</p> 
タイプ	アラートのイベントのタイプ(ログ、ネットワーク セッションなど)を示します。
ソース	アラートの元のソースを表示します。アラートのソースは、NetWitness Endpoint、Malware Analysis、Event Stream Analysis(ESA 関連ルール)、ESA Analytics、Reporting Engine、Web Threat Detection、その他多数のソースがあります。
重大度	アラートの重大度のレベルを表示します。値は1~100です。

オプション	説明
インシデント生成	アラートがインシデントに関連づけられているかどうかを分類します。インシデントの一部であるアラートを表示するには、[Yes]を選択します。インシデントの一部ではないアラートを表示するには、[No]を選択します。たとえば、アラートからインシデントを作成する前に、[No]を選択すると、インシデントの一部ではないアラートのみを表示することができます。
アラート名	アラートの名前を表示します。このフィルタを使用すると、[悪意のあるIP: Reporting Engine]などの特定のルールまたはソースによって生成されたすべてのアラートを検索することができます。
フィルタのリセット	フィルタの選択を解除します。

アラート リストには、選択条件を満たすアラートのリストが表示されます。アラート リストの下部では、フィルタ処理されたリストのアイテム数を確認できます。例:「30アイテム中30個を表示中」のように表示されます

[概要]パネル

[概要]パネルには、選択したアラートおよびRAWアラート メタデータに関する基本的なサマリ情報が表示されます。[アラートの詳細]ビューの[概要]パネルには同じ情報が含まれていますが、[アラートの詳細]ビューではパネルを展開して詳細情報を表示することができます。





次の表に、アラートの[概要]パネルに表示されるフィールドを示します。

フィールド	説明
<アラート名>	アラートの名前を表示します。
インシデントID	アラートに関連づけられているインシデントIDを表示します。インシデントIDリンクをクリックすると、関連づけられているインシデントの[インシデントの詳細]ビューに移動することができます。インシデントIDがない場合、アラートはインシデントに属しません。このアラートのインシデントを作成することも、インシデントに追加することもできます。
作成日	アラートが作成された日時を表示します。
重大度	アラートの重大度のレベルを表示します。値は1～100です。
ソース	アラートの元のソースを表示します。アラートのソースは、NetWitness Endpoint、Malware Analysis、ESAの相関ルール、ESA Analytics、Reporting Engine、その他多数のソースがあります。
タイプ	アラートのイベントのタイプ(ログ、ネットワークセッションなど)を示します。
イベント数	アラートに含まれるイベントの数を示します。この値は、ソースによって異なります。たとえば、NetWitness EndpointアラートとMalware Analysisアラートでは、常にイベントの数が1つになります。特定のタイプのアラートでは、イベント数が多いとより高いリスクを示すことがあります。
RAWアラート	RAWアラート メタデータが表示されます。

ツールバーのアクション

この表には、アラートのリスト ビューで使用できるツールバーのアクションが示されています。

オプション	説明
	アラート リストに表示するアラートを指定できるように、[フィルタ]パネルを開くことができます。
	パネルを閉じます。
[インシデントの作成] ボタン	アラートからインシデントを作成できます。アラートをインシデントの一部にすることはできません。インシデントなしのアラート リストを取得するには、アラート リストをフィルタできます。[インシデント生成]セクションで、[いいえ]を選択します。
[削除] ボタン	ルールを削除できます。

[アラートの詳細]ビュー

[アラートの詳細]ビュー([RESPOND]>[アラート])に移動してアラート リストで名前のハイパーリンクをクリック)で、アラートのソース、アラート内のイベントの数、インシデントの一部であるかどうかなど、アラートに関するサマリー情報を表示できます。イベントのメタデータのほか、アラート内のイベントに関する詳細情報を表示することもできます。

ワークフロー

このワークフローは、アナリストがアラートの確認やインシデントの作成に使用している上位レベルのプロセスを示しています。



[アラートの詳細]ビューでアラート リストを確認したら、それらのアラートをさらに調査し、アラートからインシデントを作成できます。[構成]>[インシデントのルール]ビューでは、インシデントを作成するための統合ルールを作成することができます。

注: NetWitness Suite 自動脅威検出を使用すると、手動でルールを作成することなくインシデントを作成することもできます。

どうしますか?

ロール	処理オプション...	方法を確認する
インシデント対応担当、アナリスト	NetWitness Suiteですべてのアラートを表示する。	アラートの表示
SOCマネージャ、管理者	統合ルールを作成する。	「NetWitness Respond 構成ガイド」の「アラートの統合ルールの作成」を参照してください。

ロール	処理オプション...	方法を確認する
インシデント対応担当、アナリスト	アラートでイベントのリストを表示する。*	アラートのイベント詳細の表示
インシデント対応担当、アナリスト	アラートで各イベントのイベントメタデータを表示する。*	アラートのイベント詳細の表示
インシデント対応担当、アナリスト	アラートでイベントをさらに調査する。*	イベントの調査
インシデント対応担当、アナリスト	既存のインシデントにアラートを追加する。	インシデントへの関連インジケータの追加
インシデント対応担当、アナリスト	アラートからインシデントを作成する。	インシデントの手動作成
データプライバシー責任者、管理者	アラートを削除する。	アラートの削除

*これらのタスクはここ(つまり、[アラートの詳細]ビュー)で完了できます。

関連トピック

- [アラートのリストビュー](#)
- [アラートのレビュー](#)

[アラートの詳細]ビュー

1. [アラートの詳細]ビューにアクセスするには、[対応]>[アラート]に移動します。
2. アラートのリストで表示するアラートを選択し、そのアラートの[名前]列のリンクをクリックします。
[アラートの詳細]ビューには、左側に[概要]パネル、右側に[イベント]パネルがあります。

次の図に示すように、より多くの情報を表示するようパネルのサイズを変更することができます。

The screenshot shows the NetWitness Respond interface with the following components:

- Navigation:** INCIDENTS, ALERTS, TASKS
- Incident Overview Panel (Left):**
 - Malicious IP - Reporting Engine
 - Overview
 - Incident ID: INC-1136
 - Created: 08/04/2017 12:55:46
 - Severity: 70
 - Source: Reporting Engine
 - Type: Network
 - # Events: 2
 - Host Summary: 2 hosts to 81B7DC4A84D441BFAED06...
 - Raw Alert: [JSON]
- Events Table (Right):**

TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION PORT	DESTINATION HOST	DESTINATION MAC	DESTINATION USER
08/04/2017 12:53:42.000	Network	127.0.0.1	43146		00:00:00:00:00:00		81B7DC4A84D4...	4369		00:00:00:00:00:00	
08/04/2017 12:54:42.000	Network	127.0.0.1	33598		00:00:00:00:00:00		81B7DC4A84D4...	4369		00:00:00:00:00:00	

[概要]パネル

[概要]パネルには、選択したアラートに関する基本的なサマリー情報が表示されます。アラートのリストビューの[概要]パネルにも同じ情報が表示されます。詳細については、アラートのリストビューの「[\[概要\]パネル](#)」のトピックを参照してください。

The screenshot shows the overview panel for the incident 'Malicious IP - Reporting Engine' with the following details:

- Overview
- Incident ID: INC-1136
- Created: 08/04/2017 12:55:46
- Severity: 70
- Source: Reporting Engine
- Type: Network
- # Events: 2
- Host Summary: 2 hosts to 81B7DC4A84D441BFAED06D3D46A19C49D17B41
- Raw Alert: [JSON]

[イベント]パネル

[イベント]パネルでは、アラートに複数のイベントがある場合、イベントリストを表示できます。アラートのイベントが1つのみの場合、またはイベントリストでイベントをクリックした場合、[イベント]パネルではイベントの詳細を表示できます。

イベントリスト

選択したアラートのイベントリストには、そのアラートに含まれているすべてのイベントが表示されます。

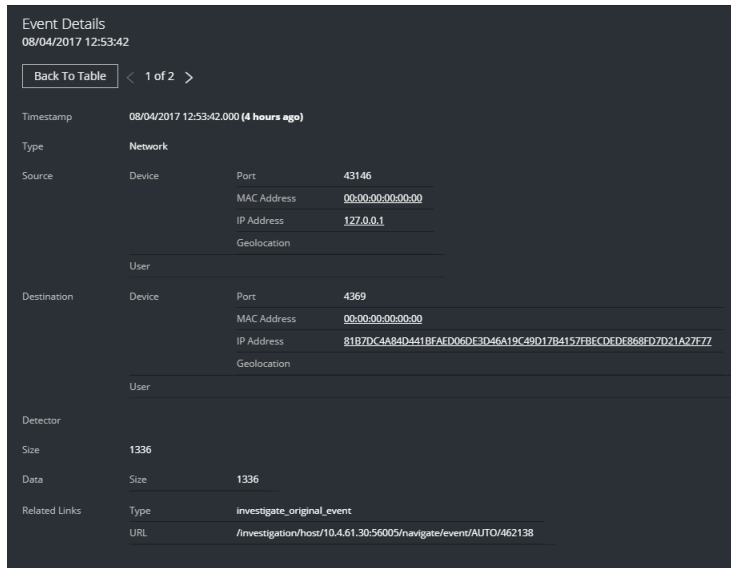
2 events											
TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION PORT	DESTINATION HOST	DESTINATION MAC	DESTINATION USER
08/04/2017 12:53:42.000	Network	127.0.0.1	43146		00:00:00:00:00:00		8187DC4A84D4...	4369		00:00:00:00:00:00	
08/04/2017 12:54:42.000	Network	127.0.0.1	33598		00:00:00:00:00:00		8187DC4A84D4...	4369		00:00:00:00:00:00	

次の表に、リストされたイベントのサマリーが記載されている、イベントリストに表示される列の一部を示します。

列	説明
時間	イベントの発生時刻を示します。
タイプ	ログやネットワークなどのアラートのタイプを示します。
ソースIP	2台のマシン間のトランザクションがあった場合は、ソースIPアドレスを示します。
デスティネーションIP	2台のマシン間のトランザクションがあった場合は、デスティネーションIPアドレスを示します。
検知器IP	異常が検出されたマシンのIPアドレスを示します。
ソースユーザー	ソースマシンのユーザーを示します。
デスティネーションユーザー	デスティネーションマシンのユーザーを示します。
ファイル名	ファイルがイベントと関連している場合は、ファイル名を示します。
ファイルハッシュ	ファイルの内容のハッシュを示します。

イベントの詳細情報

[イベント] パネルのイベントの詳細情報では、アラートの各イベントのイベント メタデータを示します。



イベント メタデータ

次の表に、[イベントの詳細情報]の最初の2列に表示される、一部のイベント メタデータ セクションおよびサブセクションを示します。これは、すべてを網羅するリストではありません。

セクション	サブセクション	説明
データ		関連するファイルなど、イベントに関連するデータに関する情報を表示します。イベントごとに0個以上あることがあります。
	ファイル名	ファイルがイベントと関連している場合は、ファイル名を示します。
	ハッシュ	MD5またはSHA1など、ファイルの内容のハッシュを示します。
	サイズ	イベントに関連する転送またはファイルのサイズを示します。
説明		イベントの一般的な説明が表示されます。

セクション	サブセクション	説明
宛先		宛先 デバイスとユーザーを示します。
	デバイス	宛先 デバイスに関する情報を示します。後述の「 イベントのソースまたは宛先デバイスの属性 」を参照してください。
	ユーザー	宛先のユーザーに関する情報を示します。後述の「 イベントのソースまたは宛先ユーザーの属性 」を参照してください。
検知器		問題が検出されたホストまたはソフトウェア製品を示します。これは、マルウェア スキャナーとログに最も高い関連性があります
	Device Class	アラートを検出した製品のデバイス クラスを示します。
	IPアドレス	アラートを検出した製品のIPアドレスを示します。
	製品名	アラートを検出した製品の名前を示します。
ドメイン		イベントに関連づけられたドメインを示します。
エンリッチメント		使用可能なエンリッチメント情報を示します。
関連リンク		利用可能な場合は、ソース製品のUI(ユーザー インターフェイス)に戻るリンクが示されます。
	タイプ	Investigate_original_eventなどのイベントのタイプを示します。
	URL	ソース製品のUIに戻るURLリンクを示します。
サイズ		関連する転送またはファイルのサイズを示します。
ソース		ソース デバイスとユーザーを示します。
	デバイス	ソース マシンに関する情報を示します。後述の「 イベントのソースまたは宛先デバイスの属性 」を参照してください。

セクション	サブセクション	説明
	ユーザー	ソース マシンのユーザーに関する情報を示します。後述の「 イベントのソースまたは宛先ユーザーの属性 」を参照してください。
タイムスタンプ		イベントの発生時刻を示します。
タイプ		ログ、ネットワーク、相関、再実行、手動アップロード、オンデマンド、ファイル共有、インスタントIOCなどのアラートのタイプを示します。

イベントのソースまたは宛先 デバイスの属性

次の表は、イベントの詳細に表示できるイベント ソースまたは宛先 デバイスの属性を示します。

名前	説明
資産タイプ	デスクトップ、ラップトップ、サーバ、ネットワーク機器、タブレットなどのデバイスのタイプを表示します。
ビジネスユニット	関連づけられているビジネス ユニットを示します。
コンプライアンス評価	デバイスのコンプライアンス評価を示します。低、中、高のいずれかにできます。
重要度	ビジネスにとってのデバイスの重要度(ビジネス上の重要度)を示します。
ファンリティ	デバイスの位置を示します。
GeoLocation	ホストの地理的位置を示します。都市、国、緯度、経度、組織、ドメインの属性を含めることができます。
IPアドレス	デバイスのIPアドレスを示します。
MACアドレス	デバイスのMACアドレスを示します。
netbios名	デバイスのnetbios名を示します。

名前	説明
ポート	ホストとの間の接続に使用したTCPポート、UDPポート、IP Srcポートのいずれか(使用可能な最初のポート)が表示されます。


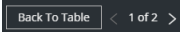
イベントのソースまたは宛先ユーザーの属性

次の表は、イベントの詳細に表示できるイベント ソースまたは宛先ユーザーの属性を示します。

属性名	説明
ADドメイン	Active Directoryドメインを示します。
ADユーザー名	Active Directoryユーザーの名前を示します。
メールアドレス	ユーザーのメールアドレスを示します。
ユーザー名	UNIXや特定のシステムのユーザー名など、ユーザー名のソースがわからない場合の一般的な名前を示します。

ツールバーのアクション

この表には、[アラートの詳細]ビューで使用できるツールバーのアクションが示されています。

オプション	説明
	(アラートに戻る) アラートのリスト ビューに戻ることができます。
	矢印をクリックすると、アラート内の各イベントのイベント メタ詳細に移動します。「1/2」などの番号は、現在表示されているイベントの番号を表示します。[テーブルに戻る]をクリックすると、イベント テーブルとも呼ばれるイベント リスト ビューに戻ります。

タスクリスト ビュー

インシデントを調査した後は、タスクリスト ビュー([RESPOND] > [タスク]) で、インシデント タスクを作成してトラックすることができます。たとえば、インシデントにセキュリティ運用以外のチームからのアクションが必要なときに、改善タスクを作成することができます。タスク内の外部チケット番号を参照し、それらのタスクを完了までトラックすることができます。ユーザー権限に応じて、必要に応じてタスクの変更や削除を行うこともできます。

どうしますか?

ロール	処理オプション...	方法を確認する
インシデント対応担当、アナリスト	タスクの表示	「すべてのインシデント タスクの表示」 および 「インシデントに関連するタスクの表示」
インシデント対応担当、アナリスト	タスクのフィルター。	タスクリストのフィルタ
インシデント対応担当、アナリスト	タスクの作成。	タスクの作成
インシデント対応担当、アナリスト	タスクの検索と変更。	「タスクの検索」 および 「タスクの変更」
インシデント対応担当、アナリスト	タスクのクローズ(改善済み、リスク受容、該当なしへのステータスの変更)。	タスクの変更
インシデント対応担当、アナリスト、SOC マネージャ	タスクの削除。	タスクの削除

関連トピック

- [\[インシデントの詳細\]ビュー](#)
- [インシデントのエスカレーションまたは修正](#)

タスクリスト

タスクリスト ビューにアクセスするには、対応 > [タスク] に移動します。タスクリスト ビューには、すべてのインシデント タスクが表示されます。

CREATED	PRIORITY	ID	NAME	ASSIGNEE	STATUS	LAST UPDATED	CREATED BY	INCIDENT ID
08/06/2017 18:26:37	HIGH	REM-10	Isolate machine	Tony	New	08/06/2017 18:26:37	admin	INC-450
08/06/2017 18:25:34	HIGH	REM-9	Mitigation task	Tony	New	08/06/2017 18:25:34	admin	INC-450
08/06/2017 17:04:46	HIGH	REM-8	Re-image the machine...	Jose	In Progress	08/06/2017 17:56:18	admin	INC-1136
08/04/2017 22:50:23	HIGH	REM-7	Discussion Required	Analyst User	New	08/04/2017 22:50:23	admin	INC-1135
08/04/2017 22:47:27	HIGH	REM-6	TASK 5	IanRSA	New	08/06/2017 18:05:43	admin	INC-1135
08/03/2017 20:13:21	MEDIUM	REM-5	test	test	New	08/03/2017 20:13:21	test	INC-1119
07/28/2017 13:44:45	HIGH	REM-3	Remediation Task has ...	Spongebob	Remediated	07/28/2017 13:52:30	admin	INC-870
07/21/2017 21:27:30	CRITICAL	REM-2	Create replacement h...	ITServices	Risk Accepted	07/28/2017 13:52:39	admin	INC-628
07/21/2017 21:24:32	HIGH	REM-1	Isolate host	DScience	New	07/21/2017 21:24:32	admin	INC-628

タスクリスト ビューは、[フィルター] パネル、タスクリスト、タスクの[概要] パネルで構成されています。次の図は、タスクリストと[概要] パネルを示しています。


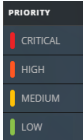
CREATED	PRIORITY	ID	NAME	ASSIGNEE	STATUS	LAST UPDATED	CREATED BY	INCIDENT ID
08/06/2017 18:26:37	HIGH	REM-10	Isolate machine	Tony	New	08/06/2017 18:26:37	admin	INC-450
08/06/2017 18:25:34	HIGH	REM-9	Mitigation task	Tony	New	08/06/2017 18:25:34	admin	INC-450
08/06/2017 17:04:46	HIGH	REM-8	Re-image the machine...	Jose	In Progress	08/06/2017 17:56:18	admin	INC-1136
08/04/2017 22:50:23	HIGH	REM-7	Discussion Required	Analyst User	New	08/04/2017 22:50:23	admin	INC-1135
08/04/2017 22:47:27	HIGH	REM-6	TASK 5	IanRSA	New	08/06/2017 18:05:43	admin	INC-1135
08/03/2017 20:13:21	MEDIUM	REM-5	test	test	New	08/03/2017 20:13:21	test	INC-1119
07/28/2017 13:44:45	HIGH	REM-3	Remediation Task has ...	Spongebob	Remediated	07/28/2017 13:52:30	admin	INC-870
07/21/2017 21:27:30	CRITICAL	REM-2	Create replacement h...	ITServices	Risk Accepted	07/28/2017 13:52:39	admin	INC-628
07/21/2017 21:24:32	HIGH	REM-1	Isolate host	DScience	New	07/21/2017 21:24:32	admin	INC-628

Task Overview (REM-6 TASK 5):

- Incident ID: [INC-1135](#)
- Created: 08/04/2017 22:47:27
- Last Updated: 08/06/2017 18:05:43
- Priority: High
- Status: New
- Assignee: IanRSA
- Description: This is remediation task AAA-1234.

タスクリスト

タスクリストには、すべてのインシデント タスクが表示されます。このリストをフィルターして、関心のあるタスクのみを表示することができます。

列	説明
	変更または削除する1つまたは複数のタスクを選択できます。SOC マネージャなどの適切な権限を持つユーザーは、バルク更新と、タスクの削除を行うことができます。たとえば、SOC マネージャが、同時に複数のタスクをユーザーに割り当てる場合があります。
作成日	タスクが作成された日付が表示されます。
優先度	タスクに割り当てられた優先度が表示されます。優先度には次のいずれかを指定できます。クリティカル、高、中、低。優先度も色分けされています。次の図に示すように、赤は[重大]、オレンジ色は[高]リスク、黄色は[中]リスク、緑は[低]リスクを示します。 
ID	タスクIDが表示されます。
名前	タスク名が表示されます。
割り当て先	タスクに割り当てられているユーザーの名前が表示されます。
ステータス	タスクのステータスが表示されます。新規、割り当て済み、進行中、改善済み、リスク受容、該当なしがあります。
最終更新日	タスクの最終更新日時を表示します。
作成者	タスクを作成したユーザーが表示されます。
インシデントID	タスクが作成されたインシデントIDが表示されます。インシデントの詳細を表示するには、IDをクリックします。

リストの下部では、現在のページのタスク数とタスクの総数を確認できます。例：23アイテム中23個を表示中

[フィルター]パネル

次の図は、[フィルター]パネルで使用可能なフィルターを示しています。

The screenshot shows a dark-themed 'Filters' panel. At the top, there is a close button (X) and a title 'Filters'. Below the title, there is a 'TIME RANGE' section with a toggle switch for 'CUSTOM DATE RANGE'. Underneath is a dropdown menu currently set to 'All Data'. The 'TASK ID' section has a text input field with the example 'e.g., REM-123'. The 'PRIORITY' section contains four checkboxes: 'Low', 'Medium', 'High', and 'Critical'. The 'STATUS' section contains six checkboxes: 'New', 'Assigned', 'In Progress', 'Remediated', 'Risk Accepted', and 'Not Applicable'. The 'CREATED BY' section has a dropdown menu. At the bottom of the panel is a 'Reset Filters' button.

タスク リスト ビューの左側にある[フィルター]パネルには、インシデント タスクをフィルターするために使用できるオプションがあります。

オプション	説明
時間範囲	[時間範囲]ドロップダウン リストから特定の期間を選択できます。時間範囲はタスクの作成日に基づきます。たとえば、[直近1時間]を選択する場合は、過去60分以内に作成されたタスクが表示されます。
カスタムの日付範囲	<p>[時間範囲]オプションを選択する代わりに、特定の日付範囲を指定できます。これを行うには、[カスタムの日付範囲]の前にある白色の円をクリックし、[開始日]と[終了日]のフィールドを表示します。カレンダーから日付と時刻を選択します。</p> 
タスクID	検索するタスクのタスクIDを入力できます(例:REM-123)。
優先度	<p>表示する優先度を選択できます。1つ以上の選択を行うと、タスクリストに選択した優先度のタスクのみが表示されます。</p> <p>例:[クリティカル]を選択した場合、タスクリストには優先度がクリティカルに設定されたタスクのみが表示されます。</p>
ステータス	<p>表示するステータスを選択できます。1つ以上の選択を行うと、タスクリストに選択したステータスのタスクのみが表示されます。</p> <p>例:[割り当て済み]を選択した場合、[タスク]パネルにはユーザーに割り当てられているタスクのみが表示されます。</p>

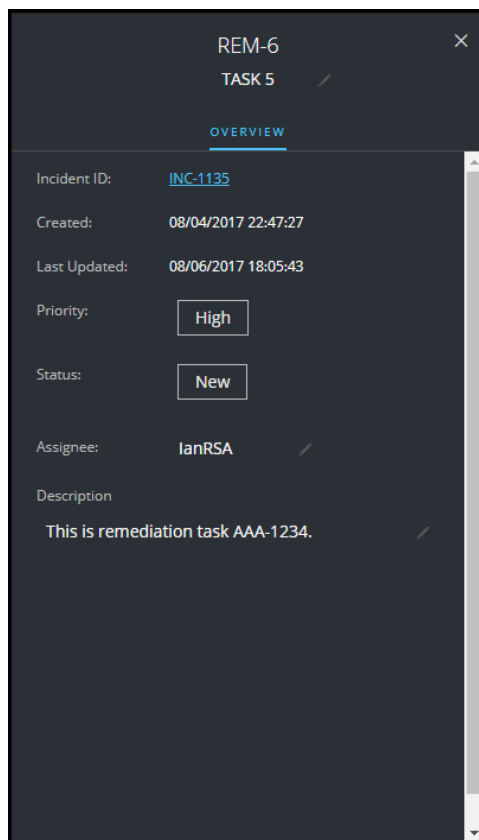
オプション	説明
作成者	表示するタスクを作成したユーザーを選択できます。たとえば、Edwardoによって作成されたタスクのみを表示する場合は、[作成者]ドロップダウンリストから[Edwardo]を選択します。タスクの作成者にかかわらずタスクを表示する場合は、[作成者]を選択しないでください。
フィルターのリセット	フィルターの選択を解除します。

タスクリストでは、選択条件を満たすタスクのリストを表示します。タスクリストの下部では、フィルター処理されたリストのアイテム数を確認できます。例：18アイテム中18個を表示中

タスクの[概要]パネル

タスクの[概要]パネルにアクセスするには：

1. [対応] > [タスク]に移動します。
2. タスクリストで、表示するタスクをクリックします。
タスクリストの右側にタスクの[概要]パネルが表示されます。





次の表に、タスクの[概要]パネルに表示されるフィールドを示します。

フィールド	説明
<タスクID>	自動的に割り当てられたタスクIDが表示されます。
<タスク名>	タスク名が表示されます。これは編集可能なフィールドです。タスク名を変更するには、現在のタスク名をクリックすると、テキスト エディタが開きます。たとえば、「Reimage a Laptop」から「Reimage a Server」にタスク名を変更できます。
インシデント ID	タスクが作成されたインシデントIDが表示されます。インシデントの詳細を表示するには、IDをクリックします。
作成日	タスクが作成された日時に関する詳細を表示します。
最終更新日	タスクの最終更新日時を表示します。
優先度	タスクの優先度が表示されます。低、中、高、クリティカルがあります。優先度を変更するには、優先度ボタンをクリックし、ドロップダウン リストからタスクの優先度を選択します。
ステータス	タスクのステータスが表示されます。新規、割り当て済み、進行中、改善済み、リスク受容、該当なしがあります。ステータスを変更するには、ステータスボタンをクリックし、ドロップダウン リストからタスクのステータスを選択します。
割り当て先	タスクに割り当てられているユーザーが表示されます。タスクに割り当てられているユーザーを変更するには、[未割り当て]または前の割り当て先の名前をクリックして、テキスト エディターを開きます。

フィールド	説明
説明	タスクの詳細が表示されます。説明を変更するには、説明の下のテキストをクリックすると、テキスト エディタが開きます。

ツールバーのアクション

この表には、タスク リスト ビューで使用できるツールバーのアクションが示されています。

オプション	説明
	タスクのリストに表示するタスクを指定できるように、[フィルター] パネルを開くことができます。
	パネルを閉じます。
[削除] ボタン	選択したタスクを削除できます。

[リストへの追加/削除]ダイアログ

[リストへの追加/削除]ダイアログを使用すると、既存のリストに対してエンティティまたはメタ値を追加または削除したり、新しいリストを作成したりできます。たとえば、IPアドレスを検索して疑わしい、または興味深いことを見つけたときは、データソースが追加されている関連リストに追加できます。これにより、疑わしいIPアドレスの可視性が向上します。さまざまなリストにエンティティまたはメタ値を追加することもできます。たとえば、コマンド&コントロール接続に関連する問題のあるドメインに関する1リストに追加し、リモート アクセスに関連するトロイの木馬接続IPアドレスに関する別のリストに追加することができます。リストを使用できない場合は、リストを作成できます。リストからエンティティまたはメタ値を削除することもできます。

注: [リストへの追加/削除]ダイアログからは、データソースとして追加された単一系列のリストからのみエンティティまたはメタ値を追加/削除でき、複数列のリストからはできません。また、ノードのビューまたはコンテキスト ルックアップビューからリストまたはリストの値を編集するときは、必ずWebページを更新して更新されたデータを表示してください。

どうしますか?

ロール	処理オプション...	方法を確認する
インシデント対応担当、アナリスト	リストにエンティティを追加する。	<p>[インシデントの詳細]ビューから、「ホワイトリストへのエンティティの追加」を参照してください。</p> <p>[インシデントの詳細]ビューから、ホワイトリストへのエンティティの追加を行います。</p>
インシデント対応担当、アナリスト	ホワイトリスト、ブラックリスト、その他のリストを作成する。	リストの作成
管理者	Context Hubリストをデータソースとして追加する。	「 <i>Context Hub構成ガイド</i> 」の「データソースとしてのリストの構成」を参照してください。
管理者	Context Hubのリストをインポートまたはエクスポートする。	「 <i>Context Hub構成ガイド</i> 」の「Context Hubのリストのインポートとエクスポート」を参照してください。

関連トピック

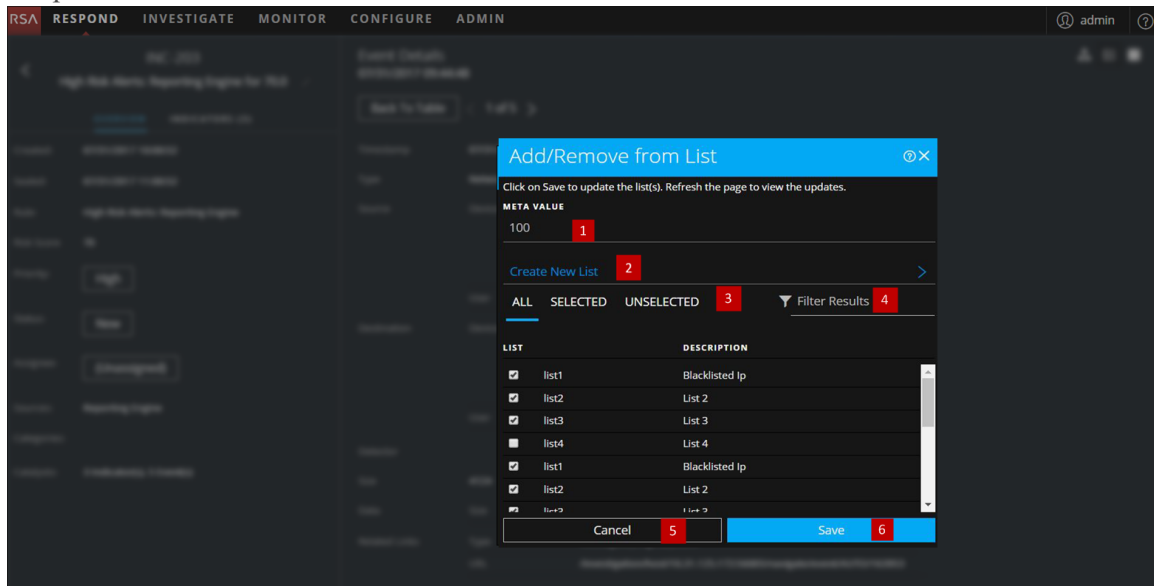
- [インシデントの調査](#)
- [アラートのレビュー](#)

- [コンテキスト情報の表示](#) ([インシデントの詳細]ビュー)
- [コンテキスト情報の表示](#) ([アラートの詳細]ビュー)

注: リストを削除することはできませんが、リスト内の値は削除できます。

簡単な説明

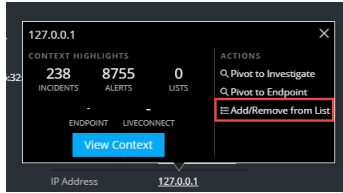
Respondビューの[リストへの追加/削除]ダイアログの例を次に示します。



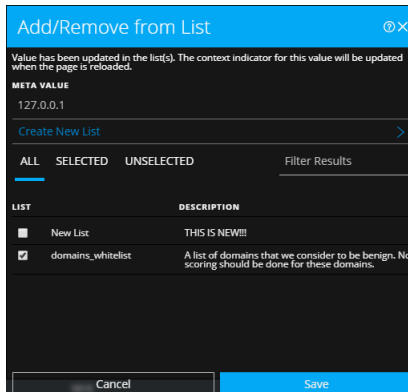
- 1 追加または削除するエンティティまたはメタ値。
- 2 選択したメタを使用して新しいリストを作成します。
- 3 任意のタブを選択します。[すべて]、[選択済み]、[未選択]のいずれかです。
- 4 リストの名前または説明を使用して検索します。
- 5 アクションをキャンセルします。
- 6 保存してリストを更新するか、新しいリストを作成します。

リストへの追加/削除

[リストへの追加/削除]ダイアログにアクセスするには、[インシデントの詳細]ビューまたは[アラートの詳細]ビューで、Context Hubリストから追加または削除する下線付きのエンティティにカーソルを合わせます。コンテキスト ツールチップに使用可能なアクションが表示されます。



ツールチップの[アクション]セクションで、[リストへの追加/削除]をクリックします。[リストへの追加/削除]ダイアログボックスに使用可能なリストが表示されます。



次の表に、[リストへの追加/削除]ダイアログのオプションを示します。

オプション	説明
メタ値	1つまたは複数のリストに追加、またはリストから削除する必要がある選択したエンティティまたはメタ値が表示されます。選択した値を使用して新しいリストを作成することもできます。
新しいリストの作成	クリックすると、選択されたメタ値を使用して新しいリストを作成するダイアログが表示されます。
すべて	使用できるContext Hubリストがすべて表示されます。選択したエンティティまたはメタ値を含むリストが選択されます。リストにエンティティまたはメタ値を追加するには、チェックボックスを選択します。リストから削除するには、チェックボックスをオフにします。
選択済み	選択したエンティティまたはメタ値を含むリストのみが表示されます。(すべてのリストが選択されます。)
未選択	選択したエンティティまたはメタ値を含まないリストのみが表示されます。(すべてのリストが選択解除されます。)

オプション	説明
結果のフィルタリング	複数のリストから検索するため、特定のリストの名前または説明を入力します。
リスト	リストすべての名前を表示します。
説明	選択したリストに関する情報を表示します。リストの作成時に指定した説明がこのダイアログに表示されます。次に例を挙げます。このリストには、ブラックリストのIPアドレスがすべて含まれます。
キャンセル	操作をキャンセルします。
保存	変更を保存します。

[コンテキスト検索]パネル- Respondビュー

Context Hubサービスでは、アナリストが分析を行い適切なアクションを行う際により的確な意思決定を行えるように、複数のデータソースから得られるコンテキスト情報をRespondビューに統合します。エンティティ、メタ値、コンテキスト情報を単一のインターフェイスで確認できるため、アナリストは関心のある領域に優先順位をつけて特定することができます。たとえば、アナリストが特定のエンティティまたはメタ値の追加情報のクエリーを実行すると、そのエンティティまたはメタ値に関してRespondビューで最近作成されたインシデントやアラートが表示されます。[コンテキスト ルックアップ]パネルには、IPアドレス、ユーザー、ホスト名、ドメイン、ファイル名、ファイルハッシュなどの選択したエンティティまたはメタ値に関するコンテキスト情報が表示されます。使用可能なデータは、Context Hub内の構成済みソースによって異なります。

[コンテキスト ルックアップ]パネルには、Context Hubの構成されたソースで使用できるデータに基づくコンテキスト情報が表示されます。

どうしますか?

ロール	処理オプション...	方法を確認する
インシデント対応担当、アナリスト、脅威ハンター	[コンテキスト ルックアップ]パネルへの移動。	[インシデントの詳細]ビューから行う場合は、「 コンテキスト情報の表示 」を参照してください。 [アラートの詳細]ビューから行う場合は、「 コンテキスト情報の表示 」を参照してください。
インシデント対応担当、アナリスト、脅威ハンター	選択したエンティティの[コンテキスト ルックアップ]パネルの情報について理解する。	このトピックの情報を参照してください。
管理者	Context Hubのデータソースの構成。	「 <i>Context Hub構成ガイド</i> 」の「Context Hubのデータソースの構成」を参照してください。
管理者	Context Hubの設定の構成。	「 <i>Context Hub構成ガイド</i> 」の「Context Hubのデータソース設定の構成」を参照してください。

関連トピック

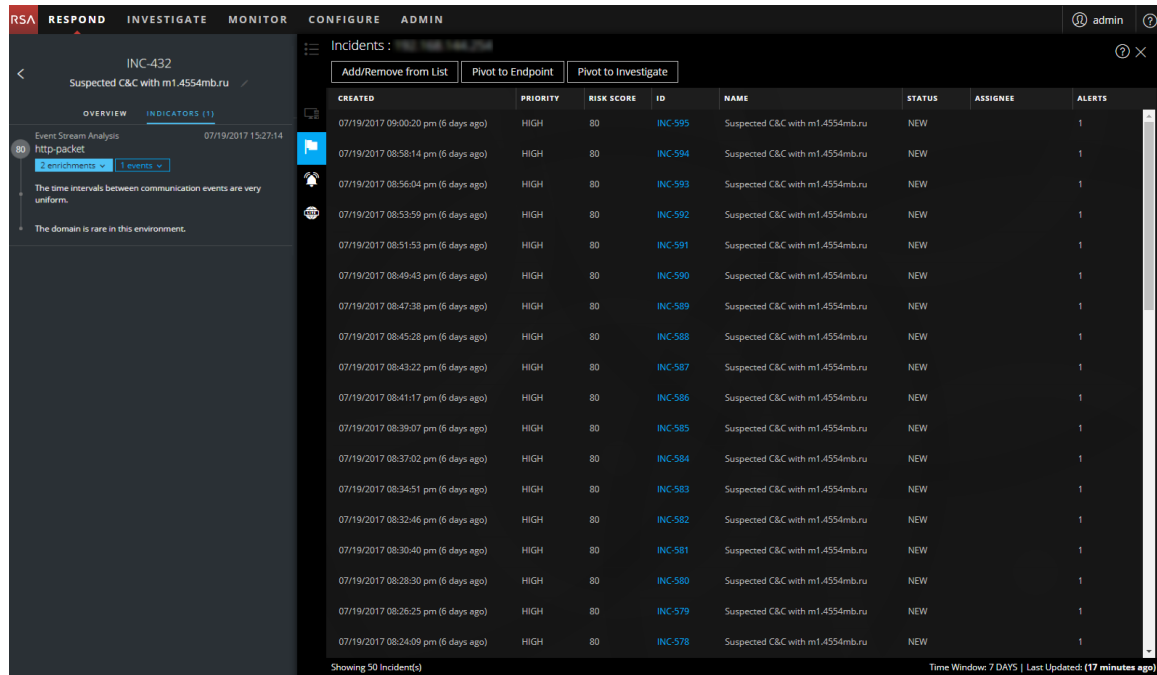
- [インシデントの調査](#)
- [アラートのレビュー](#)

[コンテキスト ルックアップ] パネルに表示されたコンテキスト情報




[コンテキスト ルックアップ] パネルに表示されるコンテキスト情報やクエリーの結果は、選択したエンティティと関連するデータソースに依存します。





[コンテキスト ルックアップ] パネルには、データソースごとに個別のタブがあります。[リスト データソース] タブがコンテキスト パネルに最初に表示され、[Archer]、[Endpoint]、[インシデント]、[アラート]、[Live Connect]が続きます。

次の図は、[インシデントの詳細]ビューで選択したエンティティの[コンテキスト ルックアップ]パネルを示しています。[コンテキスト ルックアップ]パネルの[インシデント]タブがビューにあります。



次の表は、各タブおよびサポートされるエンティティで使用可能なデータを示しています。

タブ	説明	サポートされるエンティティ
 (リスト)	選択したエンティティまたはメタ値に関連付けられているすべてのリストのデータを表示します。結果は、最後に更新されたリストによってソートされます。	すべてのエンティティ
 (Archer)	Archerデータソースを使用して、重要度評価とともにアセット情報を表示します。	IPとホスト
 (Active Directory)	選択したユーザーのすべてのユーザー情報を表示します。	ユーザー

タブ	説明	サポートされるエンティティ
 (NetWitness Endpoint)	マシン、モジュール、IIOCレベルを含む選択したエンティティまたはメタ値の NetWitness Endpoint データソースの情報を表示します。モジュールは最大 IOC スコアから最小 IIOC スコアの順にソートされ、IIOC レベルは最高 IOCL レベルから最低 IOCL レベルの順にソートされます。	IP、MAC アドレス、ホスト
 (インシデント)	選択したエンティティまたはメタ値に関連付けられているインシデントのリストを表示します。結果は、最新のインシデントから最も古いインシデントの順にソートされます。	すべてのエンティティ
 (アラート)	選択したエンティティまたはメタ値に関連付けられているアラートのリストを表示します。結果は、最新のアラートから最も古いアラートの順にソートされます。	すべてのエンティティ
 (Live Connect)	Live Connect に関連する情報を表示します。	IP、ドメイン、Filehash

リスト

[リスト] の [コンテキスト ルックアップ] パネルには、選択したエンティティまたはメタ値に関連付けられた、1 つ以上のリストが表示されます。次の図は、[リスト] の [コンテキスト] パネルの例です。

NAME	DESCRIPTION	AUTHOR	CREATED	UPDATED
new list		admin	08/24/2017 06:33:47 pm (5 days ago)	08/24/2017 06:33:47 pm (5 days ago)
White-listed Hosts	List of Whitelisted Hosts	admin	08/22/2017 09:00:35 am (7 days ago)	08/22/2017 09:00:35 am (7 days ago)

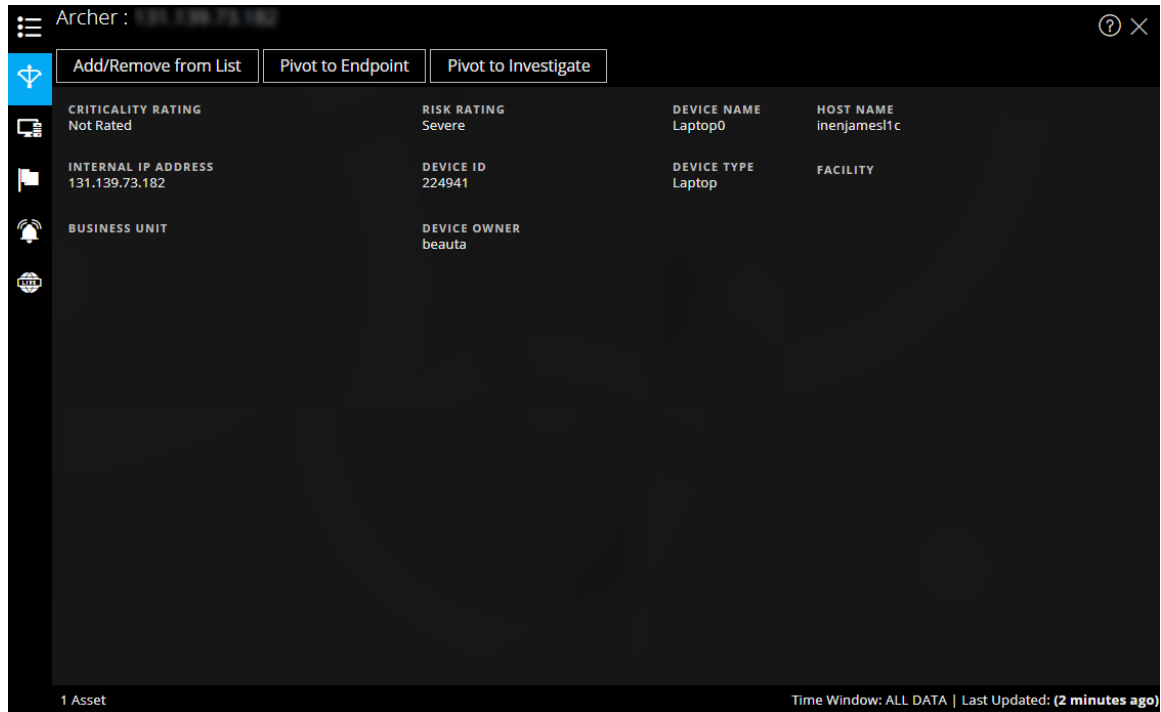
2 List(s) Time Window: ALL DATA | Last Updated: (2 minutes ago)

リストについて次の情報が表示されます。

フィールド	説明
名前	リストの名前(リストの作成時に定義)。
説明	リストの説明(リストの作成時に定義)。
作成者	リストを作成した所有者。
作成日	リストが作成された日付。
更新日	リストが最後に更新または変更された日付。
カウント	選択したエンティティまたはメタ値が使用可能なリストの数。
タイム ウィンドウ	これは[レスポンスの構成]ダイアログの[クエリーの対象期間]フィールドに設定された値に基づいています。デフォルトでは、[リスト]のすべてのデータがフェッチされます。
最終更新日	Context Hubがリックアップ データをフェッチしてキャッシュに保存した時刻。

Archer

[Archer] の [コンテキスト ルックアップ] パネルには、IP およびホストのエンティティとメタ値の Archer データソースを使用して、重要度評価とともにアセット情報が表示されます。次の図は、[Archer] の [コンテキスト] パネルの例です。



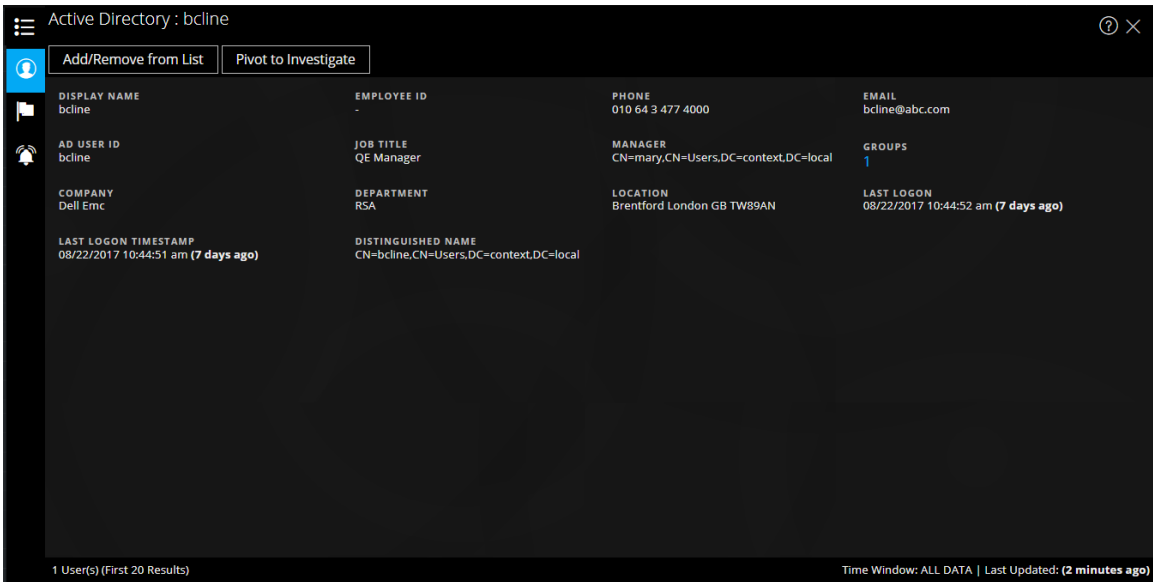
Archer について次の情報が表示されます。

フィールド	説明
重要度評価	デバイスがサポートするアプリケーションに基づいて算出されたデバイスの業務上の重要度を表示します。重要度評価は、未評価、低、中-低、中、中-高、高として設定することができます。
デバイスID	システム内のすべてのアプリケーションの間でレコードを一意に識別する、自動的に設定された値を表示します。
デバイス名	デバイスの固有の名前を表示します。
Device Owner	デバイスを担当し、レコードの読み取りおよび更新権限を持つデバイスの所有者を表示します。
ホスト名	デバイスのホスト名を表示します。

フィールド	説明
施設	このデバイスに関連する施設アプリケーション内のレコードへのリンクを提供します。
ビジネス ユニット	このデバイスに関連するビジネス ユニット アプリケーション内のレコードへのリンクを提供します。
リスク評価	最新の評価と、このデバイスを使用する施設の平均リスク評価から、デバイスのリスク評価を計算します。リスク評価は、重大、高、中、低、最小として設定することができます。
タイプ	サーバ、ノートパソコン、デスクトップなどのデバイスタイプを表示します。
IPアドレス	デバイスのプライマリ内部IPアドレスを表示します。
カウント	使用可能な資産の数を表示します。
タイム ウィンドウ	これは[レスポンスの構成]ダイアログの[クエリーの対象期間]フィールドに設定された値に基づいています。デフォルトでは、Archerのすべてのデータがフェッチされます。
最終更新日	Context Hubがルックアップ データをフェッチしてキャッシュに保存した時刻。

Active Directory

次の図は、[Active Directory]の[コンテキスト]パネルの例です。



Active Directoryの[コンテキスト ルックアップ]パネルには、ユーザーのすべての関連情報、インシデント、アラートが表示されます。次の形式を使用して検索を実行できます。

- userPrincipalName
- Domain\UserName
- sAMAccountName

マルチドメインまたはマルチフォレストのユーザーが存在する場合は、特定のユーザーのすべての関連コンテキスト情報が表示されます。

Active Directoryについて次の情報が表示されます。

フィールド	説明
表示名	特定のユーザーの名前を表示します。
従業員ID	特定のユーザーの従業員IDを表示します。
電話番号	特定のユーザーの電話番号を表示します。
Eメール	特定のユーザーのEメールIDを表示します。
ADユーザーID	組織内の特定のユーザーの固有のIDを表示します。
役職	特定のユーザーの役職を表示します。
マネージャ	マネージャの名前を表示します。
グループ	特定のユーザーがメンバーであるグループのリストを表示します。
会社	特定のユーザーが所属する会社の名前を表示します。

フィールド	説明
部門	特定のユーザーが所属する組織内の部門名を表示します。
所在地	特定のユーザーの所在地を表示します。
最終ログオン	グローバルカタログが定義されている場合にのみ、特定のユーザーがシステムにログインした時刻を表示します。
最終ログオンのタイムスタンプ	特定のユーザーがシステムにログインした時刻を表示します。
Distinguished Name	ユーザーに割り当てられている固有の名前を表示します。
カウント	ユーザーの数を表示します。
タイム ウィンドウ	これは[データソース設定の構成]ダイアログの[クエリーの対象期間]フィールドに設定された値に基づいています。デフォルトでは、Active Directoryのすべてのデータをフェッチします。
最終更新日	Context Hubがルックアップ データをフェッチしてキャッシュに保存した時刻。

NetWitness Endpoint

[NetWitness Endpoint]の[コンテキスト ルックアップ]パネルには以下の情報が表示されます。

The screenshot displays the NetWitness Endpoint interface for host 10.63.0.225. Key information includes:

- IOC Score:** 439
- # OF MODULES:** 4512
- IIOC 0:** 0
- IIOC 1:** 3
- LAST UPDATED:** 8/29/2017 3:21:25 PM
- ADMIN STATUS:** -
- LAST LOGIN:** 8/29/2017 4:13:40 PM
- MAC ADDRESS:** 00:0C:29:98:94:32
- OPERATING SYSTEM:** Microsoft Windows Server 2012 R2 Standard
- MACHINE STATUS:** Online
- IPADDRESS:** 10.63.0.225

Two tables are shown below the summary:

IIOC SCORE	MODULE NAME	ANALYTICS SCORE	MACHINE COUNT	SIGNATURE
14	svchost.exe	1	1	Valid: Microsoft Windo...
13	ApiServer.exe	8	1	Valid: RSA Security LLC
11	spoolsv.exe	1	1	Valid: Microsoft Windo...
11	lsass.exe	1	1	Valid: Microsoft Windo...
10	cht4vx64.sys	1	1	Root Not trusted: Chel...
9	ConsoleServerService...	1	1	Valid: RSA Security LLC
5	SQLAGENT.EXE	1	1	Valid: Microsoft Corpo...
4	ECatUI.exe	3	1	Valid: RSA Security LLC
4	wsqmcons.exe	1	1	Valid: Microsoft Windo...
4	ConsoleServer.exe	8	1	Valid: RSA Security LLC

IIOC LEVEL	DESCRIPTION	LASTEXECUTED
1	Non-Microsoft & System attri...	8/29/2017 3:25:49 PM
1	In root of logical drive	8/29/2017 3:25:43 PM
1	Revoked signature	8/29/2017 3:25:43 PM
2	File hidden	8/29/2017 3:25:48 PM
2	In hidden directory	8/29/2017 3:25:48 PM
2	Likely packed	8/29/2017 3:25:44 PM
2	In RecycleBin directory	8/29/2017 3:25:44 PM
2	Process authorized in firewall	8/29/2017 3:25:44 PM
2	Renames file to executable	8/29/2017 3:25:52 PM
3	In AppData directory	8/29/2017 3:25:49 PM

1 Host | Time Window: ALL DATA | Last Updated: (28 minutes ago)

IIOCについて次の情報が表示されます。

フィールド	説明
モジュール数	検索されたモジュール数を表示します。
管理ステータス	管理ステータスを表示します(ある場合)。
最終更新日	データが最後に更新された時刻を表示します。
最終ログイン	ユーザーが最後にログインした時刻を表示します。
MACアドレス	マシンのMACアドレス
オペレーティングシステム	NetWitness Endpointマシンで使用されるオペレーティングシステムのバージョン。
コンピュータのステータス	検索されたモジュールがオンライン、オフライン、アクティブ、非アクティブのいずれであるかを表示します。
IPアドレス	特定のモジュールのIPアドレスを表示します。

モジュールについて次の情報が表示されます。

フィールド	説明
IIOCスコア	マシンIIOCスコアは、モジュールのスコアに基づいて集計されたスコアです。これは、Context Hubのデータソース設定の[最小IIOCスコア]に設定された値に基づいています。[最小IIOCスコア]のデフォルト値は500です。「Context Hub構成ガイド」の「Context Hubのデータソース設定の構成」のトピックを参照してください。
Module Name	検索されたモジュールの名前。
解析スコア	選択したマシンのアクティブなファイルの数。
マシン数	NetWitness Endpointデータベースでスキャン結果が最後に更新された時刻を示します。
Signature	ファイルが署名されているかどうかと、有効か無効かを示し、GoogleやAppleなどの署名情報を提供します。

マシンについて次の情報が表示されます。

フィールド	説明
IOCLレベル	IOCLレベルを表示します。
説明	使用可能な場合に、IOCLレベルの説明を表示します。
前回の実行	アクションが実行された時刻を表示します。
カウント	検索されたホスト数を表示します。
タイム ウィンドウ	これは[データソース設定の構成]ダイアログの[クエリーの対象期間]フィールドに設定された値に基づいています。デフォルトでは、NetWitness Endpointのすべてのデータがフェッチされます。
最終更新日	NetWitness Endpointデータベースでスキャン結果が最後に更新された時刻を示します。

アラート

次の図は、最初に時間(新しい順)次に重大度に基づいて表示された[アラート]の[コンテキスト]パネルの例です。

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	INCIDENT ID
08/29/2017 09:30:17 am (6 hours ago)	70	ip rule	Reporting Engine	1	INC-274
08/29/2017 06:55:12 am (9 hours ago)	70	ip rule	Reporting Engine	1	INC-273
08/24/2017 06:22:58 am (5 days ago)	70	ip rule	Reporting Engine	4	INC-272
08/24/2017 06:22:50 am (5 days ago)	90	iprule	Event Stream Analysis	1	
08/24/2017 06:15:57 am (5 days ago)	70	ip rule	Reporting Engine	4	INC-272
08/24/2017 06:15:12 am (5 days ago)	90	iprule	Event Stream Analysis	1	

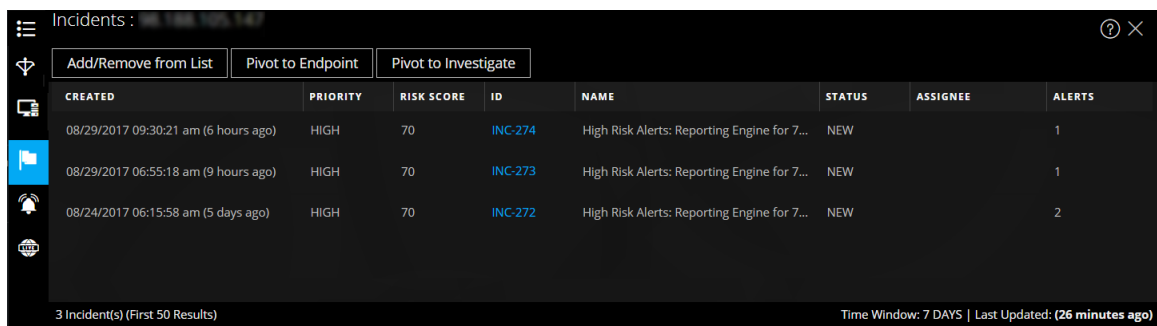
[アラート]の[コンテキスト ルックアップ]パネルには以下の情報が表示されます。

フィールド	説明
作成日	アラートが作成された日時。
重大度	アラートの重大度の値

フィールド	説明
名前	アラートの名前。名前をクリックすると特定のアラートの詳細が表示されます。
ソース	アラートがトリガーされた場所のアラートソース名。
イベント数	アラートに関連するイベントの数。
インシデントID	アラートが関連づけられているインシデントのIDです(該当する場合)。IDをクリックすると特定のアラートの詳細が表示されます。
カウント	アラートの数を表示します。デフォルトでは、最初の100件のアラートのみが表示されます。設定の構成方法の詳細については、「Context Hub 構成ガイド」の「Context Hubのデータソース設定の構成」のトピックを参照してください。
タイム ウィンドウ	これは[データソース設定の構成]ダイアログの[クエリーの対象期間]フィールドに設定された値に基づいています。デフォルトでは、過去7日間のアラートデータをフェッチします。
最終更新日	コンテキスト データがデータソースからフェッチされた前回の時刻を示します。

インシデント

次の図は、最初に時間(新しい順)次に優先度のステータスに基づいた[インシデント]の[コンテキスト]パネルの例です。



CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/29/2017 09:30:21 am (6 hours ago)	HIGH	70	INC-274	High Risk Alerts: Reporting Engine for 7...	NEW		1
08/29/2017 06:55:18 am (9 hours ago)	HIGH	70	INC-273	High Risk Alerts: Reporting Engine for 7...	NEW		1
08/24/2017 06:15:58 am (5 days ago)	HIGH	70	INC-272	High Risk Alerts: Reporting Engine for 7...	NEW		2

3 Incident(s) (First 50 Results) Time Window: 7 DAYS | Last Updated: (26 minutes ago)

[インシデント]の[コンテキスト ルックアップ]パネルには以下の情報が表示されます。

フィールド	説明
作成日	インシデントが作成された日付

フィールド	説明
優先度	インシデントの優先度のステータス
リスクスコア	インシデントのリスクスコア
ID	インシデントのインシデントID。クリックするとインシデントの詳細が表示されます
名前	インシデント名
ステータス	インシデントのステータス
割り当て先	インシデントの現在の所有者
アラート	インシデントに関連するアラートの数
カウント	インシデントの数を表示します。デフォルトでは、最初の100件のアラートのみが表示されます。設定の構成方法の詳細については、「 <i>Context Hub 構成ガイド</i> 」の「Context Hubのデータソース設定の構成」のトピックを参照してください。
タイム ウィンドウ	これは[データソース設定の構成]ダイアログの[クエリーの対象期間]フィールドに設定された値に基づいています。デフォルトでは、過去7日間のアラート データをフェッチします。
最終更新日	コンテキスト データがデータソースからフェッチされた前回の時刻を示します。

Live Connect

次の図は、[Live Connect]の[コンテキスト]パネルの例です。


Live Connect : ?

Add/Remove from List
Pivot to Endpoint
Pivot to Investigate

Review Status

STATUS **MODIFIED DATE**
 RISKY 08/16/2017 01:18:56 pm (a month ago)

Live Connect Risk Assessment



UNSAFE

Research and analysis shows resource to be untrusted

RISK REASONS

- Source of unsafe module
- Blacklisted by one or more customers

Risk Indicators

RECONNAISSANCE

HTTP SCANNING BRUTE FORCE VPN TOR SOCKS
ANONYMOUS ACCESS FTP SSH BUSINESS APPLICATION
OTHER

COMMAND AND CONTROL

BEACONING HTTP SSL/TLS SSH FTP IRC
CUSTOM PROTOCOL WEBSHELL VPN OTHER

DELIVERY

REMOTE/LOCAL FILE INCLUSION CSRF SQLI XSS EXPLOIT
PHISHING DRIVE BY OTHER

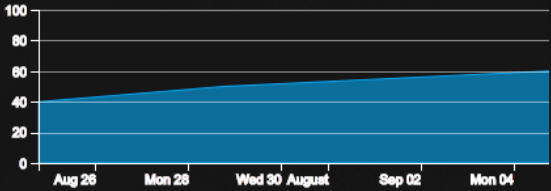
LATERAL MOVEMENT

OTHER SSH RDP SMB/RPC POWERSHELL WMI TELNET

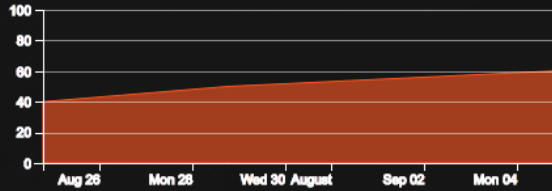
Community Activity

FIRST SEEN
04/08/2016 02:26:47.087 am (a year ago)

TRENDING COMMUNITY ACTIVITY (LAST 30 DAYS)



TRENDING SUBMISSION ACTIVITY (LAST 30 DAYS)



60% of the Community seen 94.74.81.176

Of the **70%** submitted feedback:

- 40%** marked High Risk (NOT DISPLAYED IN CHART)
- 30%** marked Unsafe
- 70%** marked Suspicious
- 0%** marked Safe
- 5%** marked Unknown

Identity

<p>AUTONOMOUS SYSTEM NUMBER(ASN) 1030404303033</p> <p>ORGANIZATION American IP LTD.</p>	<p>COUNTRY CODE US</p> <p>COUNTRY NAME United States</p>
---	--

[Live Connect] パネルには次の情報が表示されます。

- レビュー ステータス
- Live Connect リスク評価
- リスク インジケータ
- コミュニティ アクティビティ
- WHOIS
- 関連するファイル、ドメイン、IP
- ID
- 証明書情報

[Live Connect] の[コンテキスト ルックアップ] パネルには以下の情報が表示されます。

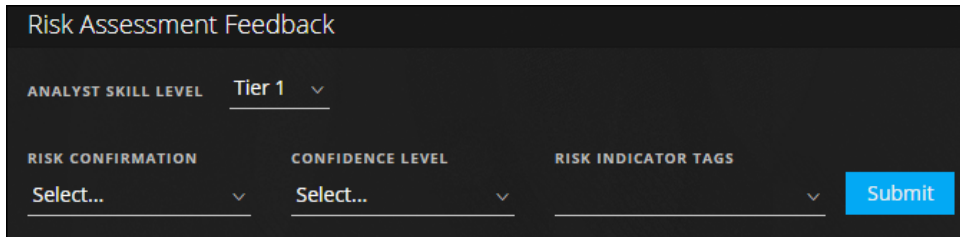
フィールド	説明
レビュー ステータス	<p>選択したLive Connectエンティティ(IP、ファイル、ドメイン) のアナリストのアクティビティに基づくレビュー ステータスを表示します。これにより、組織内で、アナリストのアクティビティの可視性が高まります。</p> <p>ステータス ステータスのタイプを以下に示します。</p> <ul style="list-style-type: none"> • 新規: IPアドレスのルックアップの結果が組織内で最初に表示された場合。 • 表示済み: 組織内のアナリストがIPアドレスのルックアップの結果をすでに表示済みの場合。 • 安全としてマーク: 組織内のアナリストがIPアドレスのルックアップの結果をすでに表示済みで安全としてマークしている場合。 • 高リスクとしてマーク: 組織内のアナリストがIPアドレスのルックアップの結果をすでに表示済みで高リスクとしてマークしている場合。

フィールド	説明
リスク評価	<p>Live Connectの分析とアナリスト フィードバックに基づく、選択したLive Connectエンティティ(IP、ファイル、ドメイン)のリスク評価を表示します。リスク評価のカテゴリは次のとおりです。</p> <ul style="list-style-type: none">• 安全: Live Connectエンティティは、安全であると見なされています。• 不明: Live Connectには、リスクを計算するためのこのエンティティに関する十分な情報がありません。• 高リスク: コミュニティによって提供される分析とリスクの理由に基づいて「高リスク」としてマークされています。「高リスク」とマークされたエンティティは、直ちに注意を要します。• 不審である: コミュニティによって提供される分析とリスクの理由に基づいて「不審である」としてマークされています。分析は、アクションを必要とする脅威となる可能性のあるアクティビティを示しています。• 安全でない: コミュニティによって提供される分析とリスクの理由に基づいて「不審である」としてマークされています。 <p>エンティティは高リスク、不審である、安全でないとして評価され、適宜関連するリスクの理由を表示します。</p>

フィー ルド	説明
リスク 評価の フィード バック	<p>リスク評価のフィードバックにより、アナリストはエンティティに関する脅威インテリジェンスのフィードバックをLive Connectサーバに送信できます。</p> <ul style="list-style-type: none"> アナリスト スキルレベル アナリスト スキルレベルのオプションを以下に示します。 <ul style="list-style-type: none"> Tier 1: このレベルのアナリストは一般的に修正のための処理手順を定義し、SOC(セキュリティオペレーションセンター)の他の領域にインシデントをエスカレーションする必要があるかどうかを判断します。これがデフォルト値です。 Tier 2: アナリストはインシデントを調査し、調査からSOC内のさまざまなワークフローへのフィードバックまで、インテリジェンスを収集します。 Tier 3: 調査結果をSOC組織と共有するアナリストです。一般的にインシデントを管理し、インシデント対応に必要なスキルとツールに関する幅広く深い知識があります。 <div style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p>注: NetWitness Suite(アナリスト)の新しいユーザーを作成するときに、管理者はユーザーをTier 1、Tier 2、Tier 3のアナリストとして特定できる必要があります。</p> </div> <ul style="list-style-type: none"> リスクの確認: 選択したLive Connectエンティティ(IP、ファイル、ドメイン)のリスクの確認です。リスクの確認のカテゴリは次のとおりです。 <ul style="list-style-type: none"> 安全: Live Connectエンティティは、安全であると見なされています。 不明: リスクの確認を行うために十分な情報がアナリストにありません 高リスク: コミュニティによって提供される分析とリスクの理由に基づいて「高リスク」としてマークされています。「高リスク」とマークされたエンティティは、直ちに注意を要します。 不審である: コミュニティによって提供される分析とリスクの理由に基づいて「不審である」としてマークされています。分析は、アクションを必要とする脅威となる可能性のあるアクティビティを示しています。 安全でない: コミュニティによって提供される分析とリスクの理由に基づいて「安全でない」としてマークされています。 信頼度レベル: Live Connectエンティティのフィードバックを提供することによるアナリストの信頼度レベルです。信頼度レベルのカテゴリは次のとおりです。

フィールド	説明
-------	----

- 高
- 中
- 低
- **リスクインジケータータグ:** 分析に基づいてタグカテゴリを選択できます。

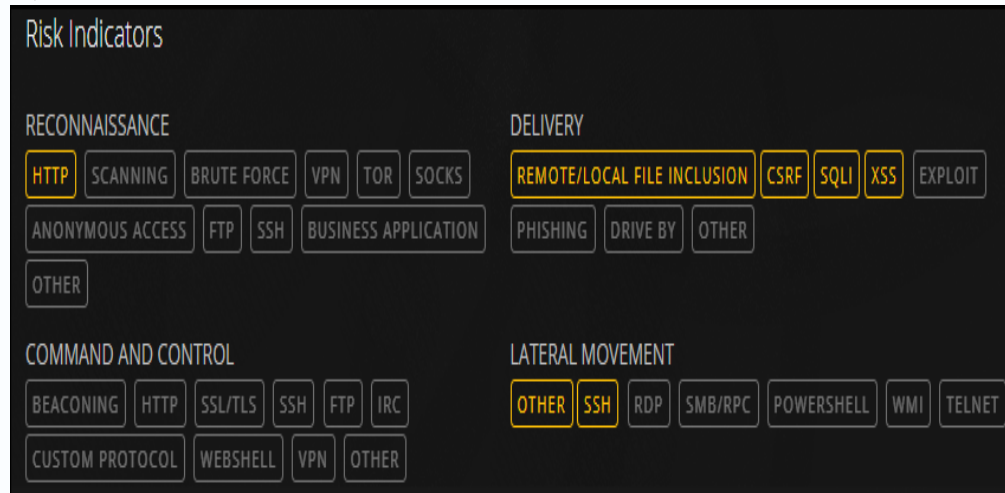


<p>コミュニティアクティビティ</p>	<p>次のようなコミュニティアクティビティ:</p> <ul style="list-style-type: none"> • コミュニティで最初に表示された日付。 • IP/ファイルドメインが最初に表示された時間からの経過時間(現在の時間-初めて表示された時間)。 <p>トレンドのコミュニティアクティビティ:</p> <p>RSAコミュニティの中で、IPアドレスが分かっている場合は、次のコミュニティアクティビティのトレンドのグラフィカル表示が表示されます。</p> <ul style="list-style-type: none"> • 所定の期間にLive ConnectコミュニティでIPアドレスを閲覧したユーザーの割合(%単位)。 • IPアドレスに関するフィードバックを送信したユーザーの割合(%単位)。 • 所定の期間にIPアドレスを安全でないとしてマークしたユーザーの割合(%単位)。
----------------------	--

**フィー
ルド**
説明

リスク
インジ
ケー
ター

リスク インジケーターは、コミュニティによってエンティティ(IPアドレス、ファイル、ドメイン)に割り当てられたタグに基づいてハイライト表示されます。



タグは、次のように分類されます。

- 予備調査
- 配信
- コマンド&コントロール
- ラテラルムーブメント
- 特権のエスカレーション
- パッケージと盗難

これらのタグはサンプルであり、Live Connectサーバでコミュニティから受信した入力によって異なります。

アナリストは、レビューのフィードバックを提供しながら、適切なリスク インジケータータグを選択できます。

ハイライト表示されたタグは、選択したエンティティがその特定のカテゴリとタグに関連づけられていることを示します。ハイライト表示されているタグをクリックすると、タグの説明が表示されます。

フィールド	説明
ID	<p>選択したエンティティまたはメタ値の次の識別情報を提供します。</p> <p>IPアドレスの場合：</p> <ul style="list-style-type: none">• ASN(Autonomous System Number)• プレフィックス• 国コードと国名• 登録者(組織)• 日付 <p>ファイルハッシュの場合：</p> <ul style="list-style-type: none">• ファイル名• ファイルサイズ• MD5• SH1• SH256• コンパイル時間• MIMEタイプ <p>ドメインの場合：</p> <ul style="list-style-type: none">• ドメイン名• 関連づけられているIPアドレス
証明書情報	<p>選択したファイルハッシュの次の証明書情報を示します。</p> <ul style="list-style-type: none">• 証明書の発行者• 証明書の妥当性• 署名アルゴリズム• 証明書のシリアル番号

フィールド	説明																		
WHO IS情報	<p>WHO IS情報は、特定のドメインの所有権の詳細を提供します。</p> <div data-bbox="321 390 1143 806" style="background-color: #333; color: #fff; padding: 10px;"> <p>WHOIS</p> <table border="0"> <tr> <td>CREATED DATE 09/01/2016 00:00</td> <td>STREET 1600 Amphitheatre Parkway</td> <td>PHONE +1.6502530000</td> </tr> <tr> <td>UPDATED DATE 11/27/2016 12:43</td> <td>CITY Mountain View</td> <td>FAX +1.6506188571</td> </tr> <tr> <td>EXPIRED DATE 10/01/2017 00:00</td> <td>STATE CA</td> <td>EMAIL dns-admin@google.com</td> </tr> <tr> <td>TYPE RegistryType</td> <td>POSTAL CODE 94043</td> <td></td> </tr> <tr> <td>NAME Admin</td> <td>COUNTRY US</td> <td></td> </tr> <tr> <td colspan="3">ORGANIZATION Google Inc.</td> </tr> </table> </div> <p>ドメイン所有者の次の情報が表示されます。</p> <ul style="list-style-type: none"> • 作成日 • 更新日 • 失効日 • タイプ(登録タイプ) • 名前 • 組織 • 郵便番号とアドレス • 国 • 電話番号 • Fax • Eメール 	CREATED DATE 09/01/2016 00:00	STREET 1600 Amphitheatre Parkway	PHONE +1.6502530000	UPDATED DATE 11/27/2016 12:43	CITY Mountain View	FAX +1.6506188571	EXPIRED DATE 10/01/2017 00:00	STATE CA	EMAIL dns-admin@google.com	TYPE RegistryType	POSTAL CODE 94043		NAME Admin	COUNTRY US		ORGANIZATION Google Inc.		
CREATED DATE 09/01/2016 00:00	STREET 1600 Amphitheatre Parkway	PHONE +1.6502530000																	
UPDATED DATE 11/27/2016 12:43	CITY Mountain View	FAX +1.6506188571																	
EXPIRED DATE 10/01/2017 00:00	STATE CA	EMAIL dns-admin@google.com																	
TYPE RegistryType	POSTAL CODE 94043																		
NAME Admin	COUNTRY US																		
ORGANIZATION Google Inc.																			

フィールド	説明
関連ファイル	<p>関連ファイルはエンティティタイプIPおよびドメインの場合に表示されます。既知の関連するファイルのリストが、次の情報とともに表示されます。</p> <ul style="list-style-type: none">• Live Connectのリスク評価(安全、高リスク、不明)• ファイル名• MD5• コンパイル時刻と日付• API関数インポート ハッシュ• MIMEタイプ
関連ドメイン	<p>関連ドメインはエンティティタイプIPおよびファイルの場合に表示されます。既知の関連するドメインのリストが、次の情報とともに表示されます。</p> <ul style="list-style-type: none">• Live Connectのリスク評価(安全、高リスク、不明)• ドメイン名• 国名• 登録日• 失効日• 登録者のEメールアドレス

フィールド

説明

関連IP 関連IPはエンティティタイプドメインおよびファイルの場合に表示されます。既知の関連するIPのリストが、次の情報とともに表示されます。

- Live Connectのリスク評価(安全、高リスク、不明)
- IPアドレス
- ドメイン名
- 国コードと国名
- 国名
- 登録日
- 失効日
- 登録者のEメール アドレス

Related Files (5)					
LC RISK RATING	FILE NAME	MDS	COMPILE DATE	API FUNCTION IMPORT HASH	
UNKNOWN	filename1	1a708f247cc6a7364b873c029bb...	09/22/2017 10:59:24 ...		
UNSAFE	filename2	2a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...		
UNKNOWN	filename3	1a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...		
UNSAFE	filename4	2a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...		
UNKNOWN	filename5	1a708f247cc6a7364b873c029bb...	09/22/2017 10:59:25 ...		

Related Domains (2)					
LC RISK RATING	DOMAIN	COUNTRY	REGISTERED DATE	EXPIRED DATE	REGISTRANT EMAIL
UNSAFE	27c73bq66y4xqoh7.dorfa...		09/22/2017 10:59:25 ...	09/22/2017 10:59:25 ...	
UNSAFE	2ymh2gnnbg6pgq2r.gre...		09/22/2017 10:59:25 ...	09/22/2017 10:59:25 ...	