



NetWitness Respond User Guide

for Version 11.1



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

March 2018

Contents

NetWitness Respond Process	7
NetWitness Respond Workflow	8
Responding to Incidents	9
Responding to Incidents Workflow	11
Review Prioritized Incident List	11
View the Incidents List	11
Filter the Incident List	13
Remove My Filters from the Incident List View	16
View My Incidents	16
Find an Incident	16
Sort the Incidents List	17
View Unassigned Incidents	18
Assign Incidents to Myself	18
Unassign an Incident	20
Determine which Incidents Require Action	21
View Incident Details	21
View Basic Summary Information about the Incident	23
View the Indicators and Enrichments	25
View and Study the Events	27
View and Study the Entities Involved in the Events	30
Filter the Data in the Incident Details View	32
View the Tasks associated with an Incident	35
View Incident Notes	35
Find Related Indicators	36
Add Related Indicators to the Incident	38
Investigate the Incident	40
View Contextual Information	40
Add an Entity to a Whitelist	43
Create a List	43
Pivot to NetWitness Endpoint	44

Pivot to Investigate	44
Document Steps Taken Outside of NetWitness	45
View the Journal Entries for an Incident	46
Add a Note	47
Delete a Note	48
Escalate or Remediate the Incident	49
Update an Incident	49
Change Incident Status	49
Change Incident Priority	52
Assign incidents to other Analysts	55
Rename an Incident	57
View All Incident Tasks	58
Filter the Tasks List	60
Remove My Filters from the Tasks List	62
Create a Task	62
Find a Task	66
Modify a Task	67
Delete a Task	71
Close an Incident	73
Reviewing Alerts	74
View Alerts	74
Filter the Alerts List	76
Remove My Filters from the Alerts List	79
View Alert Summary Information	79
View Event Details for an Alert	80
Investigate Events	84
View Contextual Information	84
Add an Entity to a Whitelist	87
Create a Whitelist	87
Pivot to NetWitness Endpoint	88
Pivot to Investigation	88
Create an Incident Manually	88
Add Alerts to an Incident	90
Delete Alerts	92

NetWitness Respond Reference Information	94
Incidents List View	95
Workflow	95
What do you want to do?	96
Related Topics	96
Quick Look	97
Incidents List View	97
Incidents List	99
Filters Panel	100
Overview Panel	102
Toolbar Actions	104
Incident Details View	105
Workflow	105
What do you want to do?	106
Related Topics	107
Quick Look	107
Overview Panel	109
Indicators Panel	109
Nodal Graph	110
Events Datasheet	113
Journal Panel	116
Tasks Panel	117
Related Indicators Panel	118
Toolbar Actions	120
Alerts List View	122
Workflow	122
What do you want to do?	122
Related Topics	123
Alerts List View	123
Alerts List	124
Filters Panel	127
Overview Panel	129
Toolbar Actions	132
Alert Details View	133
Workflow	133
What do you want to do?	133

Related Topics	134
Alert Details View	134
Overview Panel	135
Events Panel	135
Events List	136
Event Details	136
Event Metadata	137
Event Source or Destination Device Attributes	138
Event Source or Destination User Attributes	139
Toolbar Actions	140
Tasks List View	141
What do you want to do?	141
Related Topics	141
Tasks List	142
Task Overview Panel	146
Toolbar Actions	148
Add/Remove from List Dialog	149
What do you want to do?	149
Add/Remove from List	150
Context Lookup Panel - Respond View	153
What do you want to do?	153
Related Topics	154
Contextual Information Displayed in the Context Lookup Panel	154

NetWitness Respond Process

NetWitness Suite Respond collects alerts from multiple sources and provides the ability to group them logically and start an Incident Respond workflow to investigate and remediate the security issues raised. NetWitness Suite Respond enables you to configure rules that aggregate Alerts into Incidents. Alerts will be normalized by the system to a common format to provide users with a consistent view for the rule criteria regardless of the data source. You can build query criteria based on the alert data with the ability to query on fields that are common as well as specific to data sources.

The rule engine allows you to group similar alerts together into an Incident so that the investigation and remediation workflow can be shared across a set of similar alerts. You can create rules that can group alerts into incidents depending on a common value they share for one or two attributes (for example, source hostname) or if they are reported within a limited time window (for example, alerts that are within four hours of each other).

If an alert matches a rule, an incident is created using the criteria. As new alerts are ingested, if an existing Incident was already created that matched those criteria, and that incident is not "in progress" yet, the new alerts will continue to be added to the same incident. If there is no existing incident for the grouped value (for example, the specific hostname) or the time window, a new incident will be created and the alert will be added to it.

You can have multiple incident rules. The rules can either group alerts into Incidents or suppress alerts from being matched by any rule, hence the rules are ranked top-to-bottom and only the first rule to match an incoming alert is used to include that alert in an incident. The Incidents provide a context for the alerts, provide tools to record the investigation status, and track the progress of associated tasks.

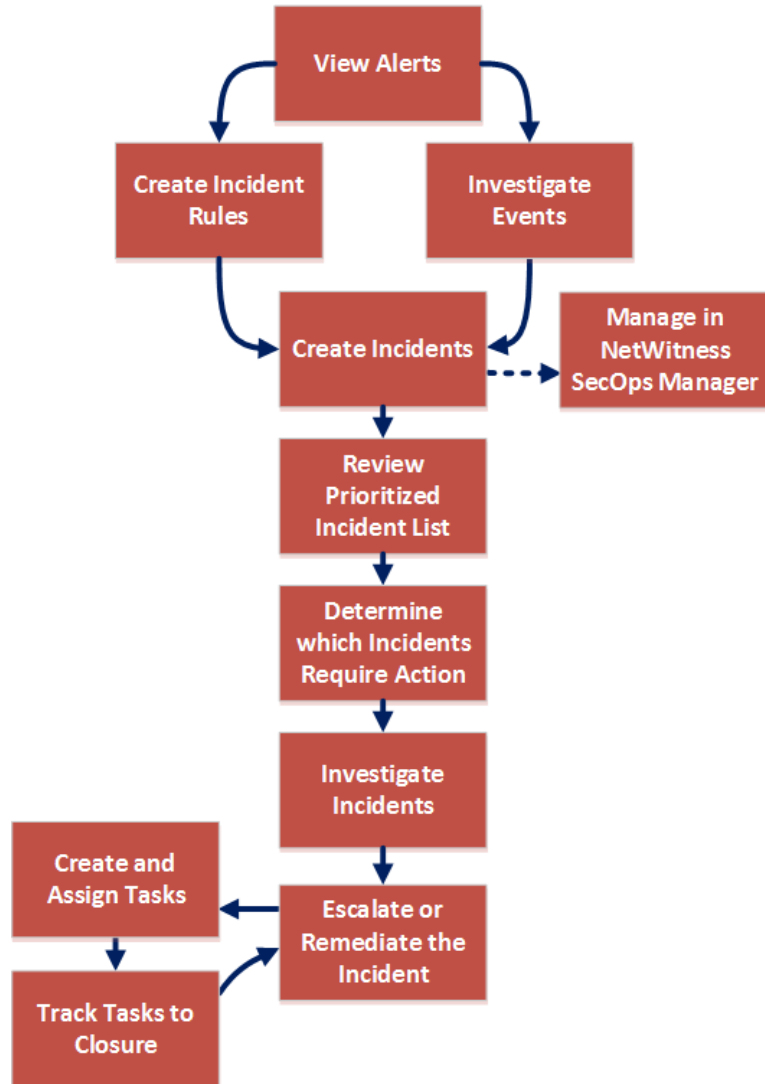
The stages in the NetWitness Respond process are:

- Review Alerts
- Create Incidents
- Respond to Incidents:
 - Review Prioritized Incident List
 - Determine which Incidents Require Action
 - Investigate Incidents
 - Escalate or Remediate the Incident (This includes creating and assigning tasks as well as tracking tasks to closure.)

You also have the option of managing incidents in RSA NetWitness® SecOps Manager instead of NetWitness Respond.

NetWitness Respond Workflow

The following figure shows the high-level NetWitness Respond workflow process.



Responding to Incidents

An *Incident* is a logically grouped set of alerts created automatically by the Incident Aggregation Engine and grouped by a specific criteria. An Incident, available in the Respond view, allows an Analyst to triage, investigate, and remediate these groups of alerts. Incidents can be moved between users, notated, and explored using a nodal graph. Incidents allow users to ensure that they understand the full scope of an attack or event in their NetWitness Suite system and then take action.

The **Respond** view is designed to help you quickly identify the ongoing issues in your network and work with other Analysts to quickly solve the issues.

The Respond view presents Incident Responders with a queue of incidents in severity order. When you take an incident from the queue, you receive relevant supporting data to help you investigate the incident. This enables you to determine the incident scope so you can escalate or remediate it as appropriate.

Within the Respond view, you can see Incidents, Alerts, and Tasks:

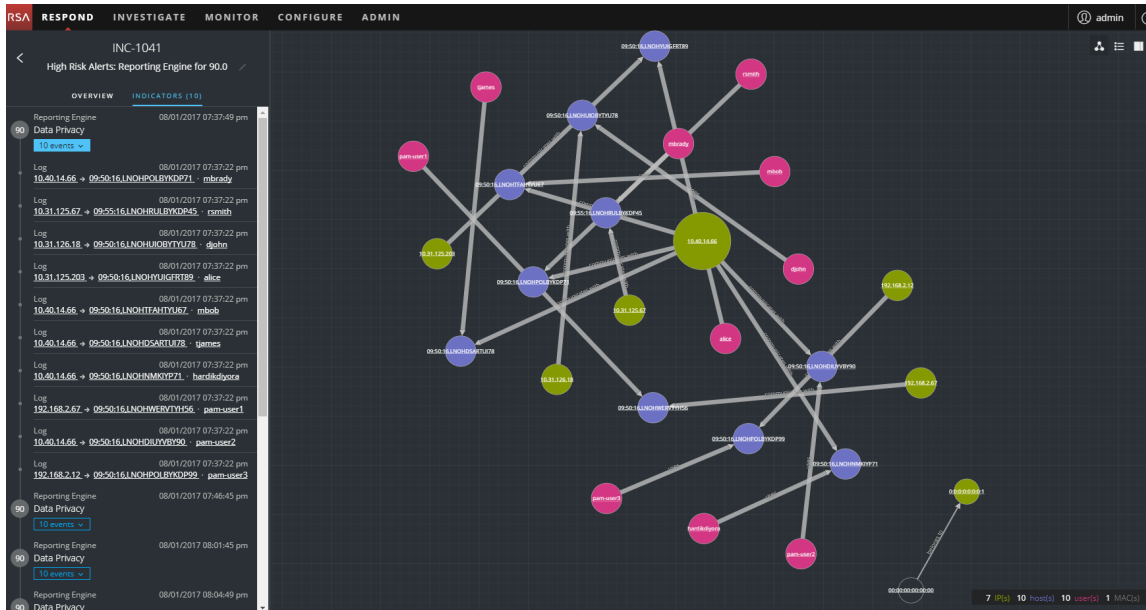
- **Incidents:** Enables you to respond to and manage incidents from start to finish.
- **Alerts:** Enables you to manage alerts from all sources received by NetWitness Suite and create incidents from selected alerts.
- **Tasks:** Enables you to view and manage the complete list of tasks created for all incidents.

If you navigate to RESPOND > Incidents, you can see the Incidents List view and from there you can access the Incident Details view for a selected incident. These are the main views that you use to respond to incidents. The following figure shows the list of prioritized incidents in the **Incidents List** view.

The screenshot shows the NetWitness Respond interface with the 'Incidents' view selected. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'Incidents' section has sub-tabs for 'Alerts' and 'Tasks'. A 'Filters' sidebar on the left allows for filtering by 'TIME RANGE', 'INCIDENT ID', 'PRIORITY', 'STATUS', 'ASSIGNEE', and 'CATEGORIES'. The main table displays a list of incidents with columns for 'CREATED', 'PRIORITY', 'RISK SCORE', 'ID', 'NAME', 'STATUS', 'ASSIGNEE', and 'ALERTS'. Action buttons like 'Change Priority', 'Change Status', 'Change Assignee', and 'Delete' are visible above the table. The table shows 1000 out of 20442 items, with 2 selected.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
2017/10/30 18:33:35	HIGH	50	INC-213288	Test123	Task Requested	deploy_admin	1
2017/10/25 17:48:36	HIGH	80	INC-213280	Test Rule for http-log	New		1
2017/10/25 17:48:36	HIGH	80	INC-213279	Test Rule for http-log	New		1
2017/10/25 17:48:36	HIGH	80	INC-213278	Test Rule for http-log	New		5
2017/10/25 17:48:36	HIGH	80	INC-213277	Test Rule for http-log	New		6
2017/10/25 17:48:36	HIGH	80	INC-213276	Test Rule for http-log	New		12
2017/10/25 17:48:36	HIGH	80	INC-213275	Test Rule for http-log	New		6
2017/10/25 17:48:36	HIGH	80	INC-213274	Test Rule for http-log	New		3
2017/10/25 17:48:36	HIGH	80	INC-213273	Test Rule for http-log	New		4
2017/10/25 17:48:36	HIGH	80	INC-213272	Test Rule for http-log	New		3
2017/10/25 17:48:36	HIGH	80	INC-213271	Test Rule for http-log	New		4
2017/10/25 17:48:36	HIGH	80	INC-213270	Test Rule for http-log	New		2
2017/10/25 17:48:36	HIGH	80	INC-213269	Test Rule for http-log	New		1
2017/10/25 17:48:36	HIGH	80	INC-213268	Test Rule for http-log	New		4
2017/10/25 17:48:36	HIGH	80	INC-213267	Test Rule for http-log	New		5
2017/10/25 17:48:36	HIGH	80	INC-213266	Test Rule for http-log	New		7
2017/10/25 17:48:36	HIGH	80	INC-213265	Test Rule for http-log	New		12
2017/10/25 17:48:36	HIGH	80	INC-213263	Test Rule for http-log	New		3
2017/10/25 17:48:36	HIGH	80	INC-213262	Test Rule for http-log	New		1

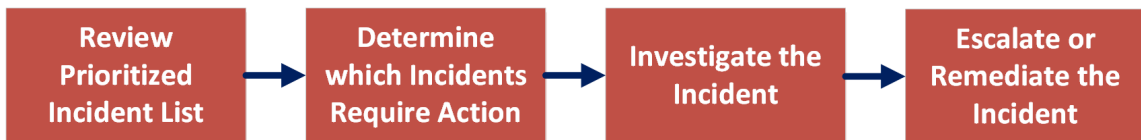
The next figure shows an example of details available in the **Incident Details** view.



The Respond view is designed to make it easy to evaluate incidents, contextualize that data, collaborate with other analysts, and pivot to a deep-dive investigation as needed.

Responding to Incidents Workflow

This workflow shows the high-level process that Incident Responders use to respond to incidents in NetWitness Suite.



First, you review the list of prioritized incidents, which shows basic information about each incident, and determine which incidents require action. You can click a link in an incident to get a clearer picture of the incident with supporting details in the Incident Details view. From there, you can further investigate the incident. You can then determine how to respond to the incident, by escalating or remediating it.

These are the basic steps for responding to an incident:

1. [Review Prioritized Incident List](#)
2. [Determine which Incidents Require Action](#)
3. [Investigate the Incident](#)
4. [Escalate or Remediate the Incident](#)

Review Prioritized Incident List

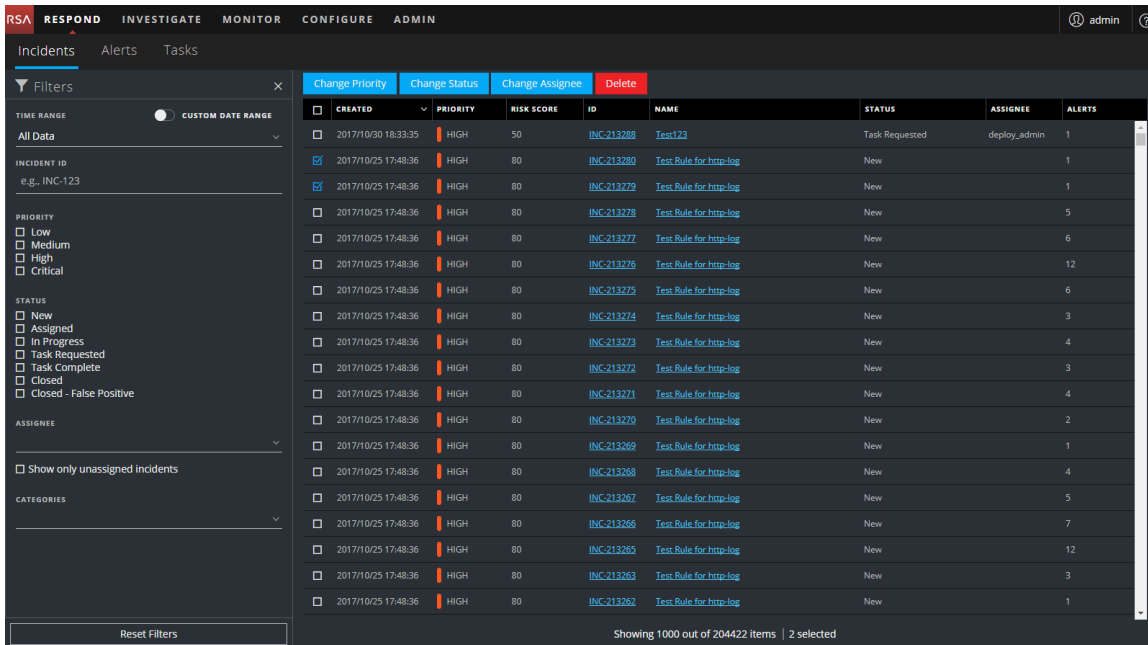
In the Respond view, you can view the list of prioritized incidents. The incident list shows both active and closed incidents.

View the Incidents List

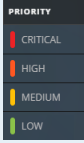
After logging in to NetWitness Suite, most Incident Responders see the Respond view, which is set as the default view. If you have a different initial view, you can navigate to the Respond view.

1. Log in to NetWitness Suite.

The Respond view shows the list of incidents, also referred to as the Incident List view.



2. If you do not see the incidents list in the Respond view, go to **RESPOND > Incidents**.
3. Scroll through the incidents list, which shows basic information about each incident as described in the following table.


Column	Description
CREATED	Shows the creation date of the incident.
PRIORITY	Shows the incident priority. Priority can be Critical, High, Medium or Low. The Priority is color coded, where red indicates a Critical incident, orange represents a High risk incident, yellow indicates a Medium risk incident, and green represents a Low risk incident. For example: 
RISK SCORE	Shows the incident risk score. The risk score indicates the risk of the incident as calculated via an algorithm and is between 0-100. 100 is the highest risk score.
ID	Shows the automatically created incident number. Each incident is assigned a unique number that you can use to track the incident.

Column	Description
NAME	Shows the incident name. The incident name is derived from the rule used to trigger the incident. Click the link to go to the Incident Details view for the selected incident.
STATUS	Shows the incident status. The status can be: New, Assigned, In Progress, Task Requested, Task Complete, Closed, and Closed- False Positive.
ASSIGNEE	Shows the team member currently assigned to the incident.
ALERTS	Shows the number of alerts associated with the incident. An incident may include many alerts. A large number of alerts might mean that you are experiencing a large-scale attack.

At the bottom of the list, you can see the number of incidents on the current page, the total number of incidents, and the number selected. For example: **Showing 1000 out of 1115 items | 3 selected.** The maximum number of incidents that you can view at one time is 1,000.

Filter the Incident List

The number of incidents in the Incidents List view can be very large, making it difficult to locate particular incidents. The Filter enables you to specify those incidents that you would like to view. You can also choose the timeframe when those incidents occurred. For example, you may want to view all of the new critical incidents created within the last hour.

1. Verify that the Filters panel appears to the left of the incidents list. If you do not see the Filters panel, in the Incident List view toolbar, click , which opens the Filters panel.

Filters [X]

TIME RANGE **CUSTOM DATE RANGE**

All Data [v]

INCIDENT ID
e.g., INC-123

PRIORITY

- Low
- Medium
- High
- Critical

STATUS

- New
- Assigned
- In Progress
- Task Requested
- Task Complete
- Closed
- Closed - False Positive

ASSIGNEE [v]

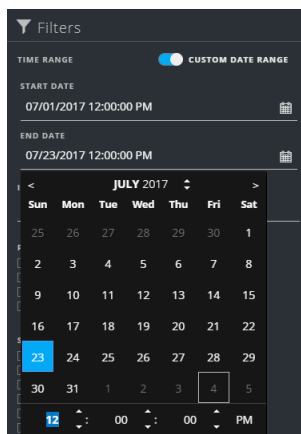
Show only unassigned incidents

CATEGORIES [v]

Reset Filters

- In the Filters panel, select one or more options to filter the incidents list:
 - TIME RANGE:** You can select a specific time period from the Time Range drop-down list. The time range is based on the creation date of the incidents. For example, if you select Last Hour, you will see incidents that were created within the last 60 minutes.
 - CUSTOM DATE RANGE:** You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to


view the Start Date and End Date fields. Select the dates and times from the calendar.



- **INCIDENT ID:** Type the Incident ID for an incident you would like to locate, for example INC-1050.
- **PRIORITY:** Select the priorities that you would like to view.
- **STATUS:** Select one or more incident statuses. For example, select Closed - False Positive to view only false positive incidents, which were initially identified as suspicious, but then they were later found to be safe.
- **ASSIGNEE:** Select the assignee or assignees of the incidents that you would like to view. For example, if you only want to view the incidents assigned to Cale or Stanley, select Cale and Stanley from the Assignee drop-down list. If you want to view incidents regardless of the assignee, do not make a selection under Assignee. (Available in version 11.1 and Later) To view only unassigned incidents, select **Show only unassigned incidents**.
- **CATEGORIES:** Select one or more categories from the drop-down list. For example, if you only want to view incidents classified with the Backdoor or Privilege abuse categories, select Backdoor and Privilege abuse.


The incidents list shows a list of incidents that meet your selection criteria. You can see the number of incidents in your filtered list at the bottom of the incident list.

Showing 89 out of 89 items | 0 selected

3. Click  to close the Filters panel and return to the Incidents List view, which now shows your filtered incidents.


Remove My Filters from the Incident List View

NetWitness Suite remembers your filter selections in the Incident List view. You can remove your filter selections when you no longer need them. For example, if you are not seeing the number of incidents that you expect to see or you want to view all of the incidents in your incident list, you can reset your filters.

1. In the Incident List view toolbar, click .
The Filters panel appears to the left of the incidents list.
2. At the bottom of the Filters panel, click **Reset Filters**.

View My Incidents


You can view your incidents by filtering the incidents by your username.

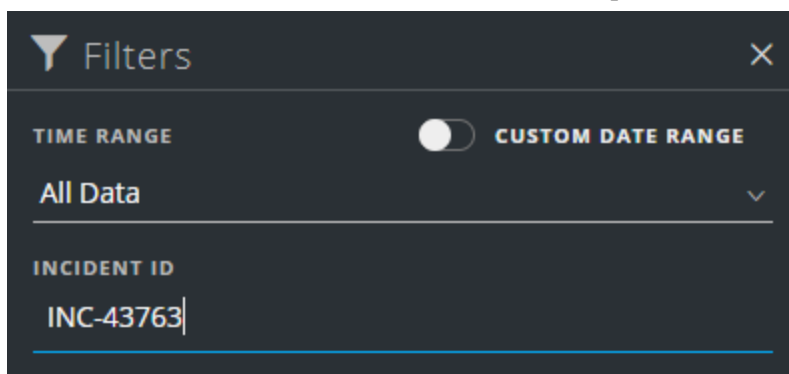
1. If you cannot see the Filter panel, in the Incident List view toolbar, click .
2. In the Filter panel, under ASSIGNEE, select your username from the drop-down list.
The incidents list shows the incidents that are assigned to you.

Find an Incident

If you know the Incident ID, you can quickly locate an incident using the Filter. For example, you may want to locate a specific incident out of thousands of incidents.

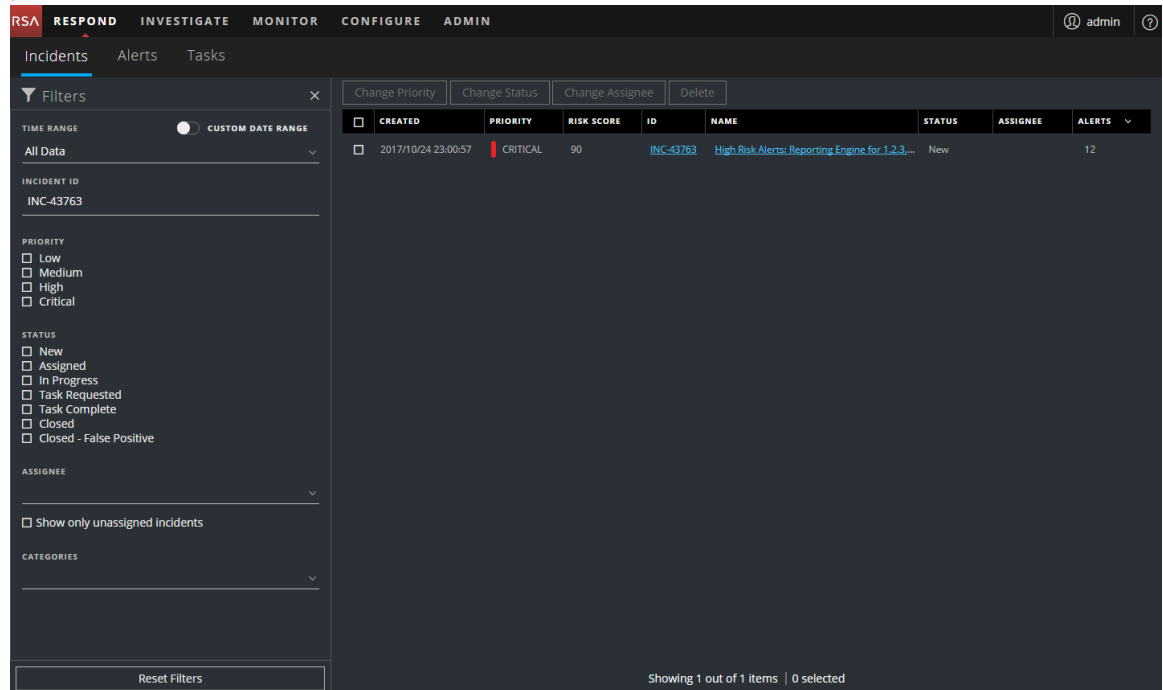
1. Go to **RESPOND > Incidents**.

The Filters panel appears to the left of the incidents list. If you do not see the Filters panel, in the Incident Lists view toolbar, click , which opens the Filters panel.



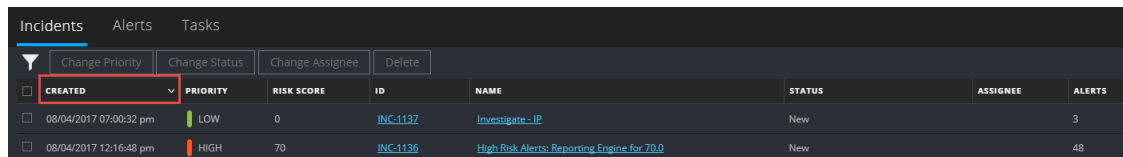
2. In the INCIDENT ID field, type the INCIDENT ID for an incident that you would like to locate, for example INC-43763.

The specified incident appears in your incident list. If you do not see any results, try resetting your filters.



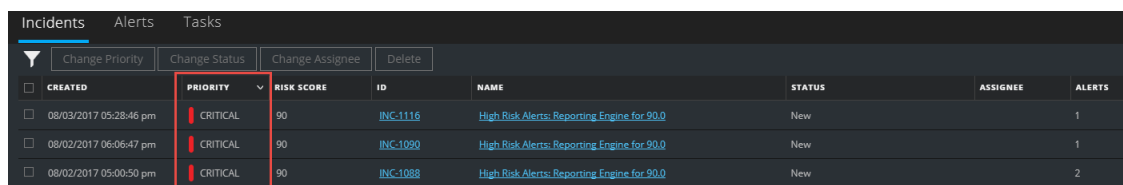
Sort the Incidents List

The default sort for the incidents list is by Created date in descending order (newest on the top).



You change the sort order of the incidents list by clicking a column in the list.

For example, to prioritize the incidents, you can sort your view by the Priority column. To do this, hover over the Priority column and click the down arrow ▾. The incident list sorts by Priority in descending order (highest priority on top), as shown in the following figure.




To sort by Priority in ascending order (lowest priority on top), click the up arrow ▲. as shown in the following figure.

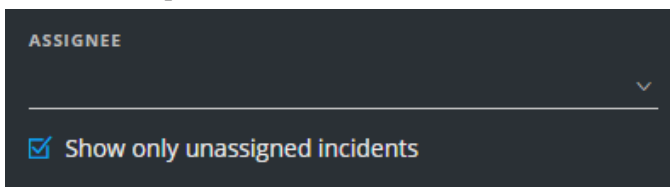
CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 07:00:32 pm	LOW	0	INC-1137	Investigate - IP	New		3
07/21/2017 06:33:40 am	MEDIUM	90	INC-610	High Risk Alerts: ESA for 90.0	In Progress	DPO Newtitness	60
08/02/2017 01:07:53 pm	MEDIUM	0	INC-1082	Test 1 (ID#3W-8*1)	Assigned	Anisha	2

View Unassigned Incidents

This option is available in version 11.1 and later.

You can view unassigned incidents using the Filter.

1. If you cannot see the Filter panel, in the Incident List view toolbar, click .
2. In the Filters panel, under ASSIGNEE, select **Show only unassigned incidents**.



The incidents list will be filtered to show unassigned incidents.

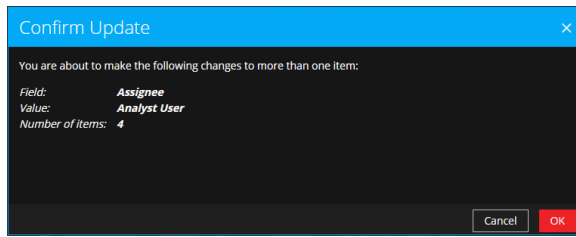
Assign Incidents to Myself

1. In the Incident List view, select one or more incidents that you want to assign to yourself.
2. Click **Change Assignee** and select your username from the drop-down list.

CREATED	PRIORITY	RISK SCORE	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	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	HIGH	70	INC-1118	High Risk Alerts: Reporting Engine for 70.0	New		60

Showing 1000 out of 1115 items | 4 selected

- If you selected more than one incident, in the Confirm Update dialog, click **OK**.



You will see a successful change notification.

The screenshot shows the NetWitness Respond interface. At the top, there is a navigation bar with tabs for 'RESPOND', 'INVESTIGATE', 'MONITOR', and 'CONFIGURE'. A green notification banner at the top center says 'Your change was successful'. Below the navigation bar, there are tabs for 'Incidents', 'Alerts', and 'Tasks'. Under the 'Incidents' tab, there are buttons for 'Change Priority', 'Change Status', 'Change Assignee', and 'Delete'. The main area displays a table of incidents. The 'ASSIGNEE' column is highlighted with a red box, and the 'ALERTS' column is also visible. The table contains the following data:

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	HIGH	70	INC-1118	High Risk Alerts: Reporting Engine for 70.0	New		60

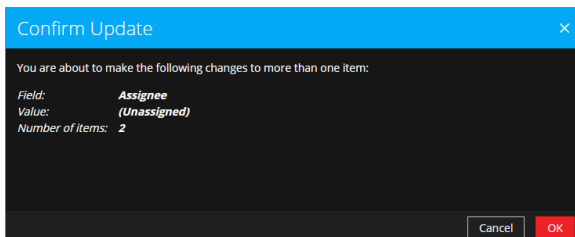
Showing 1000 out of 1115 items | 4 selected

Unassign an Incident

1. In the Incident List view, select one or more incidents that you want to unassign.
2. Click **Change Assignee** and select **(Unassigned)** from the drop-down list.

CREATED	PRIOR...	RISK	NAME	STATUS	ASSIGNEE	AL...
2017/10/17 15:24...	HIGH	70	High Risk Alerts: ESA for 70.0	New		2245
2017/10/17 15:14...	HIGH	70	High Risk Alerts: ESA for 70.0	New		2040
2017/10/17 15:58...	LOW	70	MANUALLY CREATED INCIDENT ID@#5%8...	New		1001
2017/10/17 14:33...	HIGH	80	Suspected C&C with us.bc.yahoo.com	Assigned	Respond Analyst	1001
2017/10/25 15:28...	HIGH	70	INC-198902 Test Rule for ESA-IP source exists	Assigned	Respond Analyst	1000
2017/10/25 15:28...	HIGH	70	INC-198900 Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:28...	HIGH	70	INC-198898 Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:28...	HIGH	70	INC-198889 Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:27...	HIGH	70	INC-198887 Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:27...	HIGH	70	INC-198885 Test Rule for ESA-IP source exists	New		1000
2017/10/17 16:12...	LOW	70	INC-2593 this is created manually using Respond UI...	New		1000
2017/10/17 15:26...	HIGH	70	INC-2590 High Risk Alerts: ESA for 70.0	New		1000
2017/10/17 15:26...	HIGH	70	INC-2589 High Risk Alerts: ESA for 70.0	New		1000
2017/10/17 15:14...	HIGH	70	INC-2582 High Risk Alerts: ESA for 70.0	New		1000
2017/10/17 15:14...	HIGH	70	INC-2581 High Risk Alerts: ESA for 70.0	New		960
2017/10/17 20:15...	HIGH	80	INC-2935 Suspected C&C with m5.apple.com	New		695
2017/10/17 20:15...	HIGH	80	INC-2951 Suspected C&C with m5.rsa.com	New		663

3. If you selected more than one incident, in the Confirm Update dialog, click **OK**.



4. Verify that the Status is still correct and make changes as required. To change the status, select one or more incidents, click **Change Status**, and select a new status. For example, if you assigned an incident to yourself by mistake, you can unassign the incident and then change the Status from Assigned back to New.

Determine which Incidents Require Action

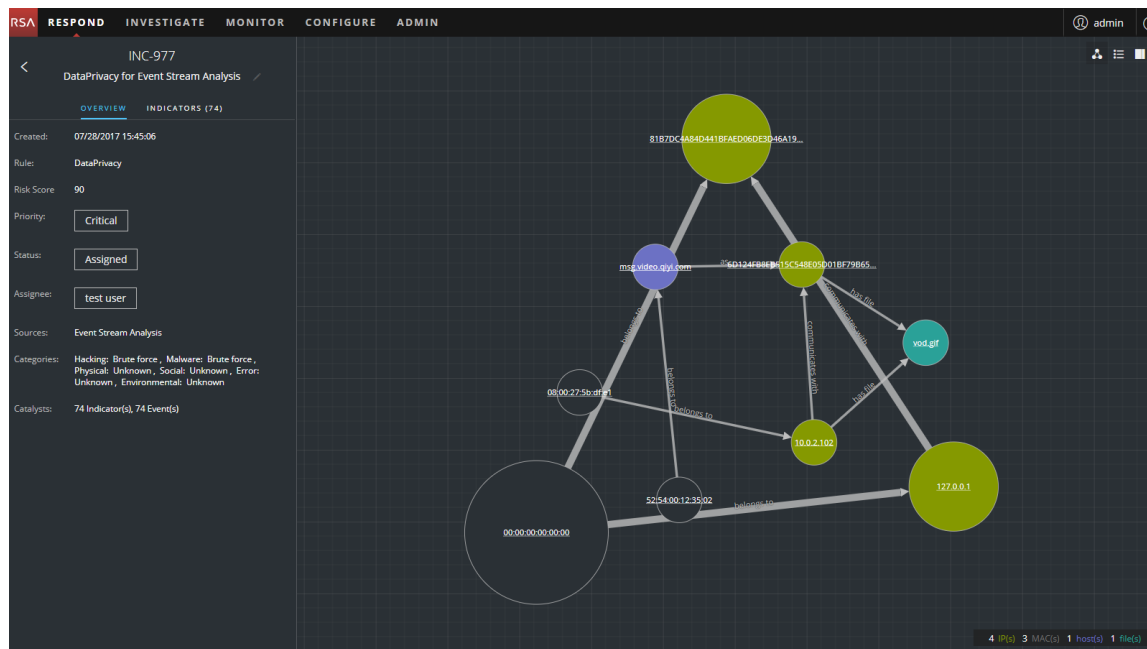
Once you get the general information about the incident from the Incident List view, you can go to the Incident Details view for more information to determine the action required.

View Incident Details

To view details for an incident, in the Incidents List view, choose an incident to view and then click the link in the ID or NAME column for that incident.

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 05:20:48	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

The Incident Details view for the selected incident appears with the Overview panel and Nodal Graph in view.



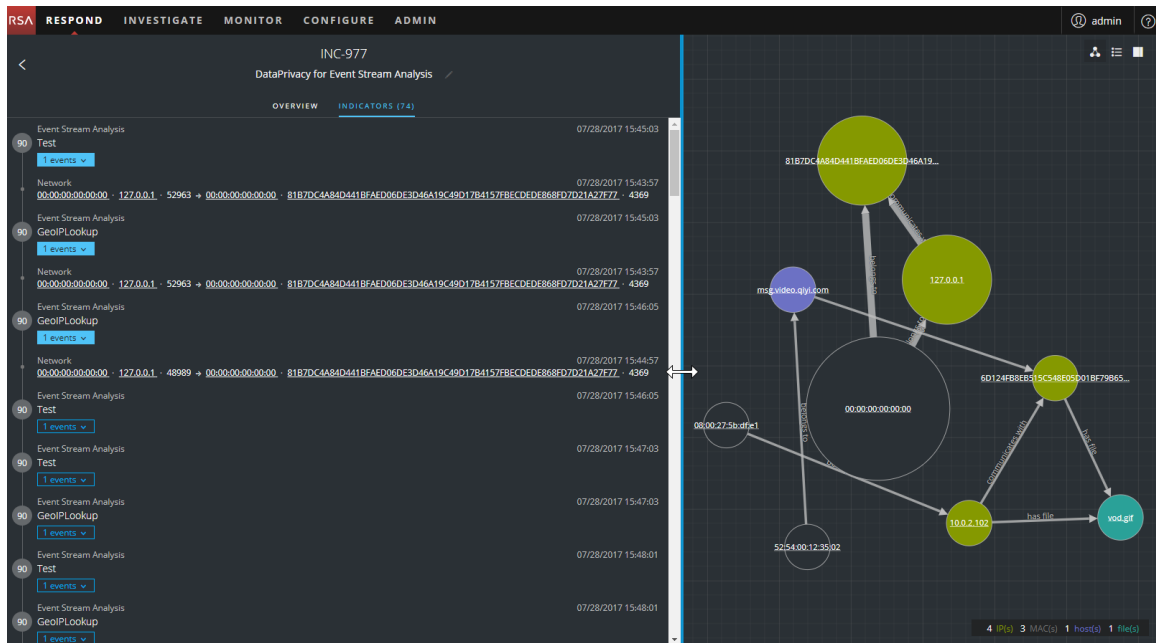
The Incident Details view has the following panels:

- **OVERVIEW:** The incident overview panel contains high-level summary information about the incident, such as the score, priority, alerts, and status. You have the option to change the incident Priority, Status, and Assignee.
- **INDICATORS:** The Indicators panel contains a chronological listing of indicators. *Indicators* are alerts, such as an ESA alert or a NetWitness Endpoint alert. This listing helps you to connect indicators and notable data. For example, an IP address connected to a command and communication ESA alert might also have triggered a NetWitness Endpoint alert or other suspicious activities.
- **Nodal Graph:** The nodal graph is an interactive graph that shows the relationship between the entities involved in the incident. An *Entity* is a specified piece of meta, such as IP address, MAC address, user, host, domain, file name, or file hash.
- **Events:** The Events panel, also known as the Events table, lists the events associated with the incident. It also shows event source and destination information along with additional information depending on the event type. You can click an event in the list to view the detailed data for that event.
- **JOURNAL:** The Journal panel enables you to access the Journal for the selected incident, which allows you to communicate and collaborate with other analysts. You can post notes to

a journal, add Investigation Milestone tags (Reconnaissance, Delivery, Exploitation, Installation, Command and control), and view the history of activity on your incident.

- **TASKS:** The Tasks panel shows all of the tasks that have been created for the incident. You can also create additional tasks from here.
- **RELATED:** The Related Indicators panel enables you to search the NetWitness Suite alerts database to find alerts that are related to this incident. You can also add related alerts that you find to the incident.

To view more information in the left-side panel without scrolling, you can hover over the right edge and drag the line to resize the panel as shown in the following figure:

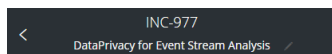


View Basic Summary Information about the Incident

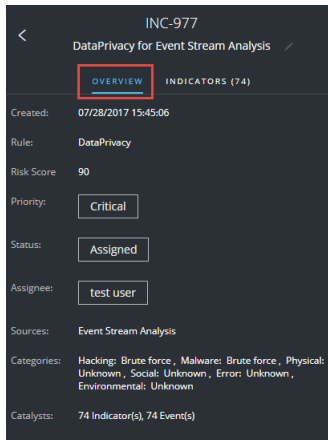
You can view basic summary information about an incident in the Overview panel.

Above the Overview panel, you can see the following information:

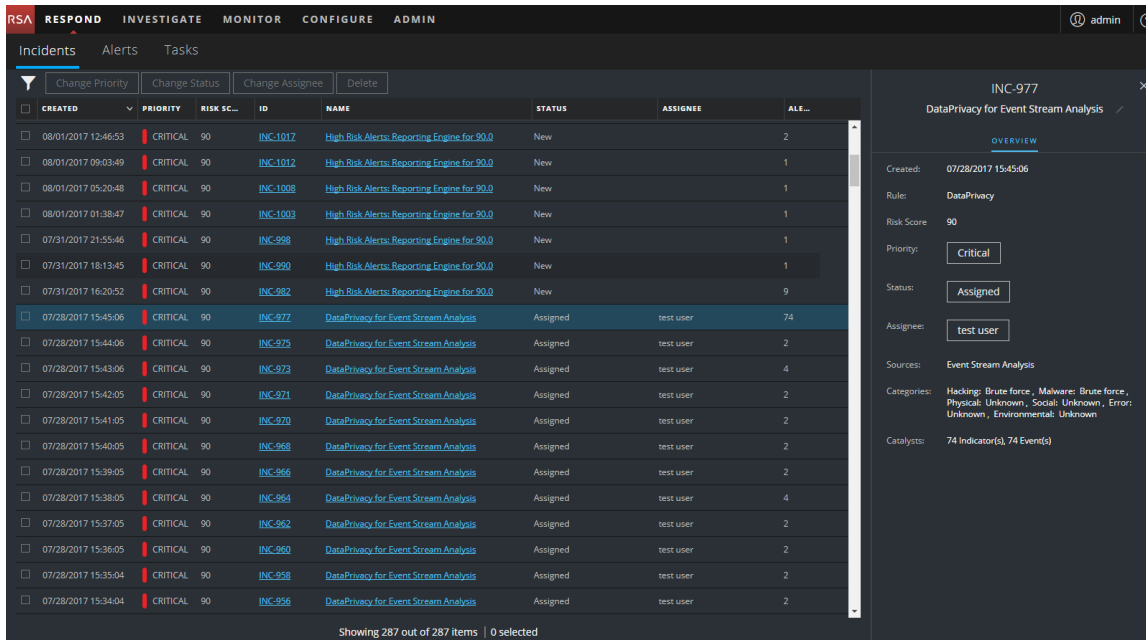
- **Incident ID:** This is an automatically created unique ID assigned to the incident.
- **Name:** The incident name is derived from the rule used to trigger the incident.



To view the Overview panel from the Incident Details view, select **OVERVIEW** in the left panel.



To view the Overview panel from the Incidents List view, click an incident in the list. The Overview panel appears on the right.



The Overview panel contains basic summary information about the selected incident:

- **Created:** Shows the creation date and time of the incident.
- **Rule / By:** Shows the name of the rule that created the incident or the name of the person who created the incident.
- **Risk Score:** Indicates the risk of the incident as calculated via an algorithm and is between 0-100. 100 is the highest risk score.
- **Priority:** Shows the incident priority. Priority can be Critical, High, Medium or Low.

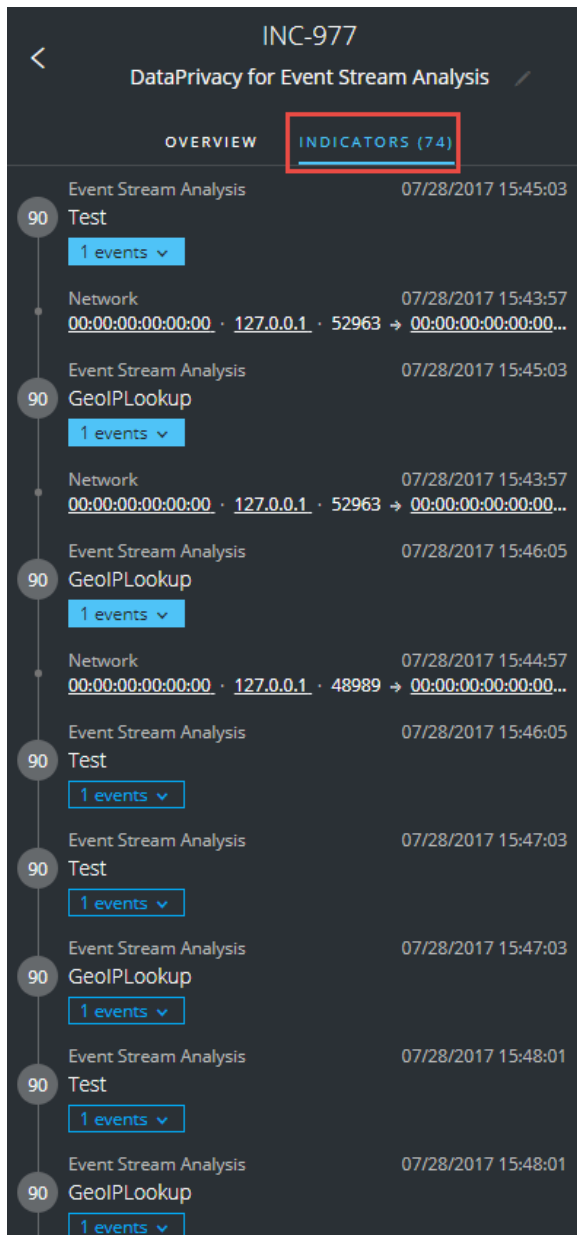
- **Status:** Shows the incident status. The status can be New, Assigned, In Progress, Task Requested, Task Complete, Closed, and Closed - False Positive. After you create a task, the status changes to Task Requested.
- **Assignee:** Shows the team member currently assigned to the incident.
- **Sources:** Indicates the data sources used to locate the suspicious activity.
- **Categories:** Shows the categories of the incident events.
- **Catalysts:** Shows the count of indicators that gave rise to the incident.

View the Indicators and Enrichments

Note: *Indicators* are alerts, such as an ESA alert or a NetWitness Endpoint alert.

You can find indicators, events, and enrichments on the Indicators panel. The Indicators panel is a Chronological listing of indicators that helps you to find enrichments and events related to the triggering indicator. For example, an indicator might be a Command and Control alert, a NetWitness Endpoint alert, a Suspicious Domain (C2) alert, or an alert from an Event Stream Analysis (ESA) rule. The Indicators panel helps you to aggregate and order these indicators (alerts) from different systems so that you can see how they are related and also help you develop a timeline of a given attack.

To view the Indicators panel, in the left panel of the Incident Details view, select **INDICATORS**.



Indicators are alerts, such as an ESA alert or a NetWitness Endpoint alert. This listing helps you to connect indicators and notable data. For example, indicators can show the data found by your rules. In the Indicators panel, the risk score for an indicator is shown within a solid-colored circle.

Data source information is shown below the names of the indicators. You can also see the creation date and time of the indicator and the number of events in the indicator. When data is available, you can see the number of enrichments. You can click the event and enrichment buttons to view the details.

View and Study the Events

You can view and study the events associated with the incident from the Events panel. It shows information about the events, such as event time, source IP, destination IP, detector IP, source user, destination user, and file information about the events. The amount of information listed depends on the event type.

There are two types of events:

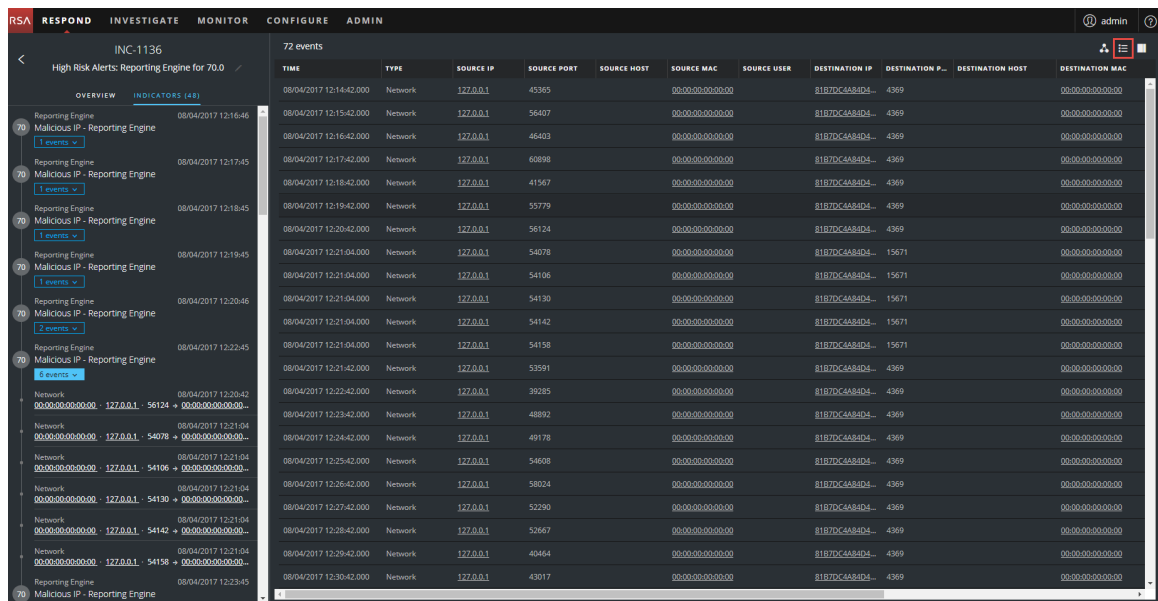
- A transaction between two machines (a Source and a Destination)
- An anomaly detected on a single machine (a Detector)

Some events will only have a Detector. For example, NetWitness Endpoint finds malware on your machine. Other events will have a Source and Destination. For example, packet data shows communication between your machine and a Command and Control (C2) domain.

You can drill further into an event to get detailed data about the event.

To view and study the events:

1. To view the Events panel, in the Incident Details view toolbar, click .



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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	4369		00:00:00:00:00:00
08/04/2017 12:19:42.000	Network	127.0.0.1	55779		00:00:00:00:00:00		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	15671		00:00:00:00:00:00
08/04/2017 12:21:04.000	Network	127.0.0.1	54106		00:00:00:00:00:00		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	4369		00:00:00:00:00:00
08/04/2017 12:27:42.000	Network	127.0.0.1	52290		00:00:00:00:00:00		8187DC4A84D4	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		8187DC4A84D4	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		8187DC4A84D4	4369		00:00:00:00:00:00
08/04/2017 12:30:42.000	Network	127.0.0.1	43017		00:00:00:00:00:00		8187DC4A84D4	4369		00:00:00:00:00:00

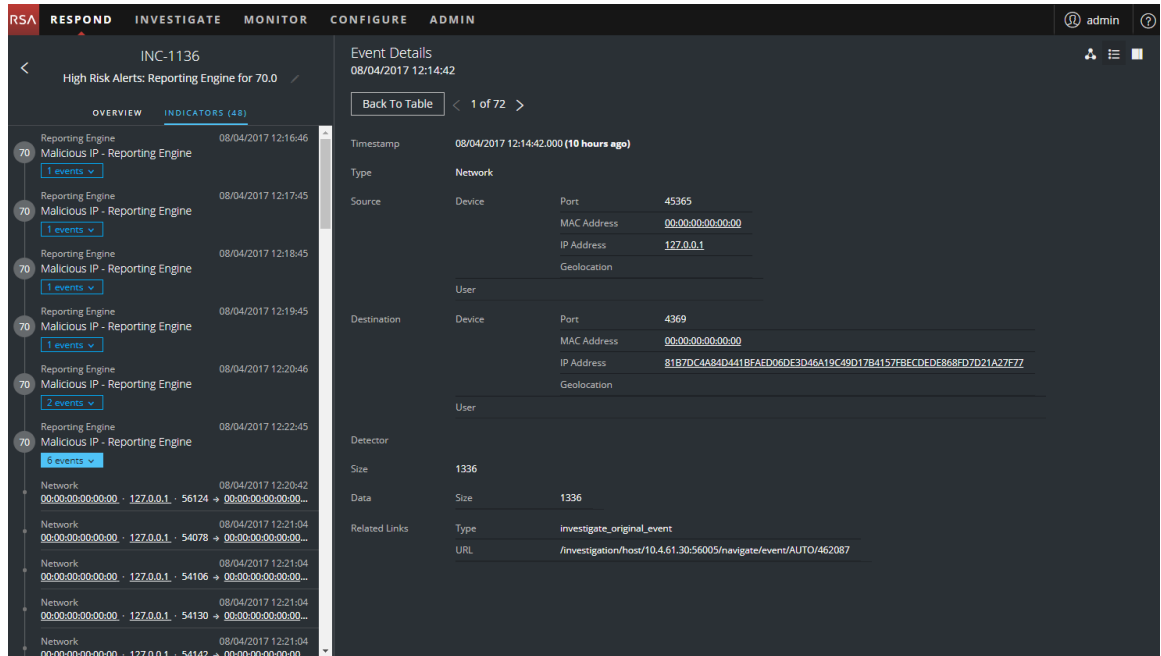
The Events panel shows a list of information about each event as shown in the following table.

Column	Description
TIME	Shows the time the event occurred.
TYPE	Shows the type of alert, such as Log and Network.
SOURCE IP	Shows the source IP address if there was a transaction between two machines.
SOURCE PORT	Shows the source port of the transaction. The source and destination ports can be on the same IP address.
SOURCE HOST	Shows the source host where the event took place.
SOURCE MAC	Shows the MAC address of the source machine.
SOURCE USER	Shows the user of the source machine.
DESTINATION IP	Shows the destination IP address if there was a transaction between two machines
DESTINATION PORT	Shows the destination port of the transaction. The source and destination ports can be on the same IP address.
DESTINATION HOST	Shows the destination host where the event took place.
DESTINATION MAC	Shows the MAC address of the destination machine.
DESTINATION USER	Shows the user of the destination machine.
DETECTOR IP	Shows the IP address of the machine where an anomaly was detected.
FILE NAME	Shows the file name if a file is involved with the event.
FILE HASH	Shows a hash of the file contents.

If there is only one event in the list, you will see the event details for that event instead of a list.

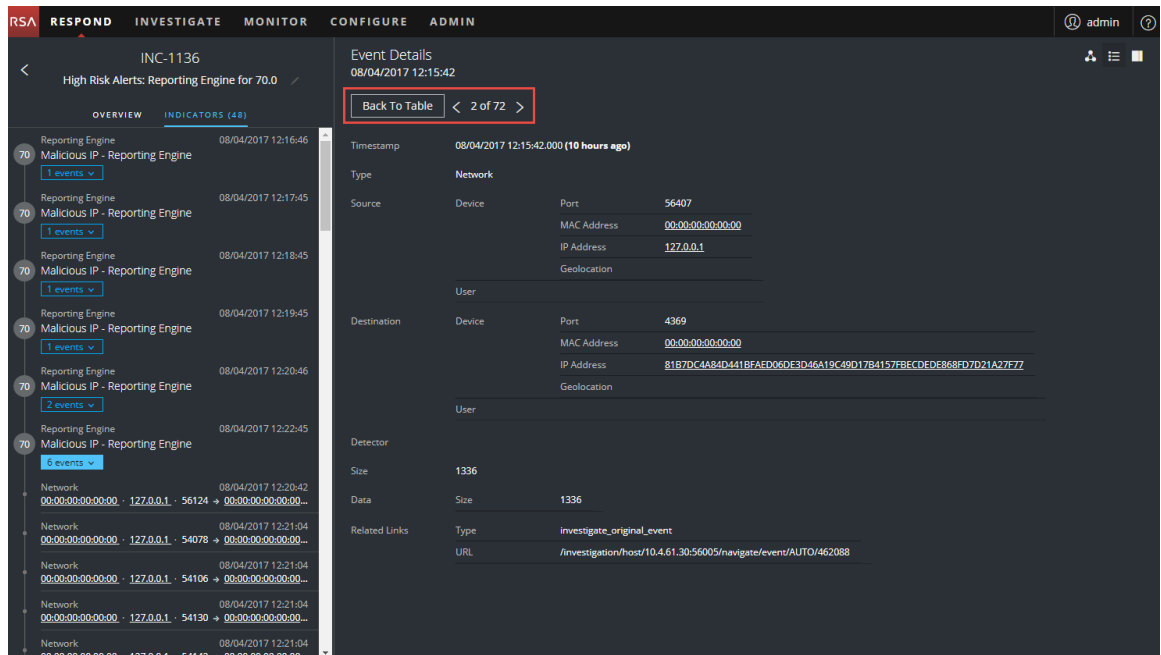
2. Click an event in the Events list to view the Event details.

This example shows the event details for the first event in the list.



3. Use the Event Details navigation to view details for additional events.

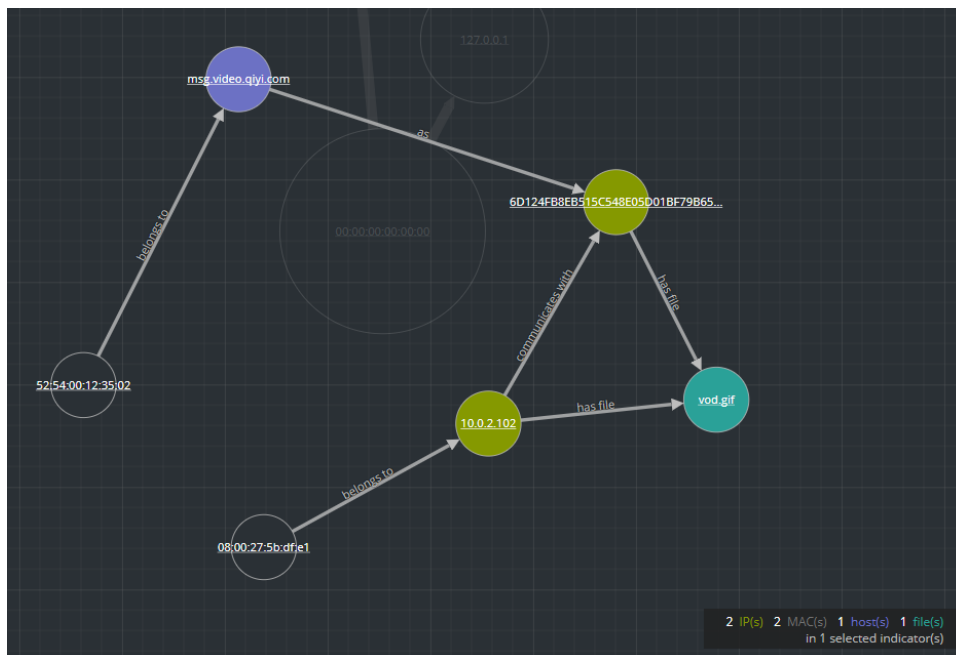
This example shows the second event in the list.



View and Study the Entities Involved in the Events

An *Entity* is either an IP address, MAC address, user, host, domain, file name, or file hash. The nodal graph is an interactive graph that you can move around to get a better understanding of how the entities involved in the events relate to each other. The nodal graphs look different depending on the type of event, the number of machines involved, whether the machines are associated with users, and if there are files associated with the event.

The following figure shows an example nodal graph with six nodes.



If you look closely at the nodal graph, you can see circles that represent nodes. A nodal graph can contain one or more of the following types of nodes:

- **IP address** (If the event is a detected anomaly, you can see a Detector IP. If the event is a transaction, you can see a Destination IP and a Source IP.)
- **MAC address** (You may see a MAC address for each type of IP address.)
- **User** (If the machine is associated with a user, you can see a user node.)
- **Host**
- **Domain**
- **Filename** (If the event involves files, you can see a filename.)
- **File Hash** (If the event involves files, you may see a file hash.)

The legend at the bottom of the nodal graph shows the number of nodes of each type and the color coding of the nodes.

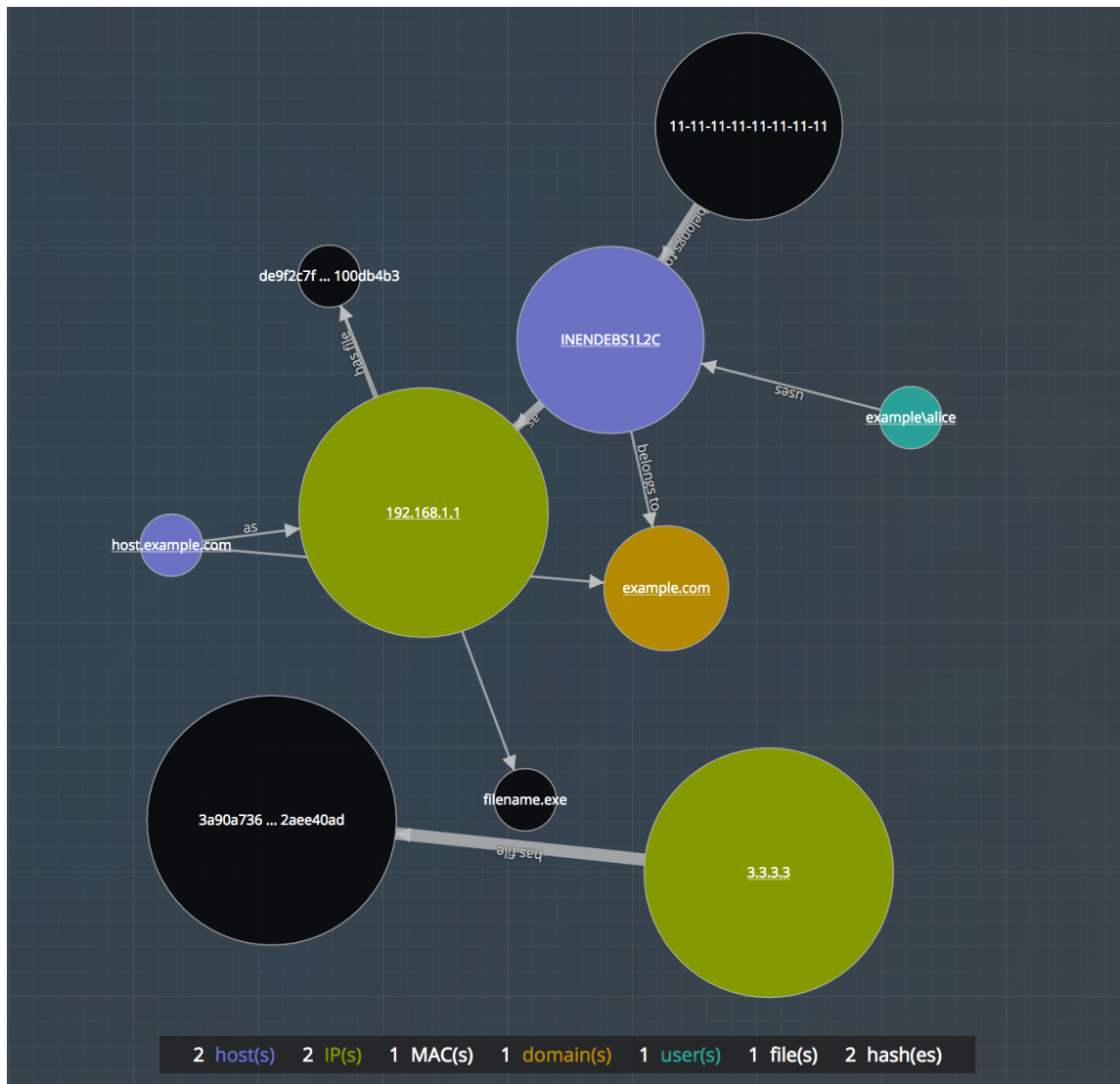
You can click any node and drag it to reposition it.

The arrows between the nodes provide additional information about the entity relationships:

- **Communicates with:** An arrow between a Source machine node (IP address or MAC address) and a Destination machine node labeled with "communicates with" shows the direction of the communication.
- **As:** An arrow between nodes labeled with "as" provides additional information about the IP address that the arrow points to. In the above example, there is an arrow from the host node circle that points to a hashed IP address node that is labeled with "as". This indicates that the name on the host node circle is the hostname of that IP address and is not a different entity.
- **Has file:** An Arrow between a machine node (IP address, MAC address, or Host) and a file hash node labeled with "has" indicates that the IP address has that file.
- **Uses:** An arrow between a User node and a machine node (IP address, MAC address, or Host) labeled with "uses" shows the machine that the user was using during the event.
- **Is named:** An arrow from a File Hash node to a File Name node labeled with "is named" indicates that the file hash corresponds to a file with that name.
- **Belongs to:** An arrow between two nodes labeled with "belongs to" indicates that they pertain to the same node. For example, an arrow between a MAC address and a Host labeled with "belongs to" indicates that it is the MAC address for the host.

Larger line size arrows indicate more communication between the nodes. Larger nodes (circles) indicate more activity than smaller nodes. The larger nodes are the most common entities mentioned in the events.

The following nodal graph example has ten nodes.

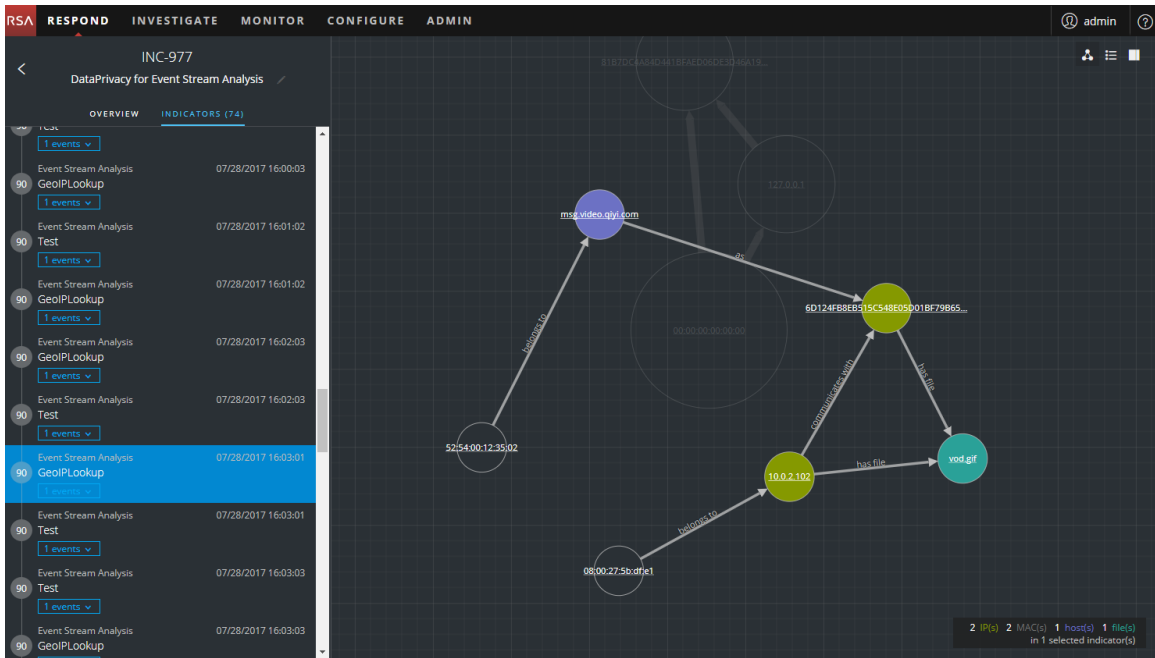


In this example, notice that there are two IP nodes that have a lot of activity. They both have files, but they do not communicate with each other. The IP address at the top (192.168.1.1) represents one machine with two hostnames (host.example.com and INENDEBS1L2C) in the example.com domain. The MAC address of the machine is 11-11-11-11-11-11-11-11-11 and Alice uses it.

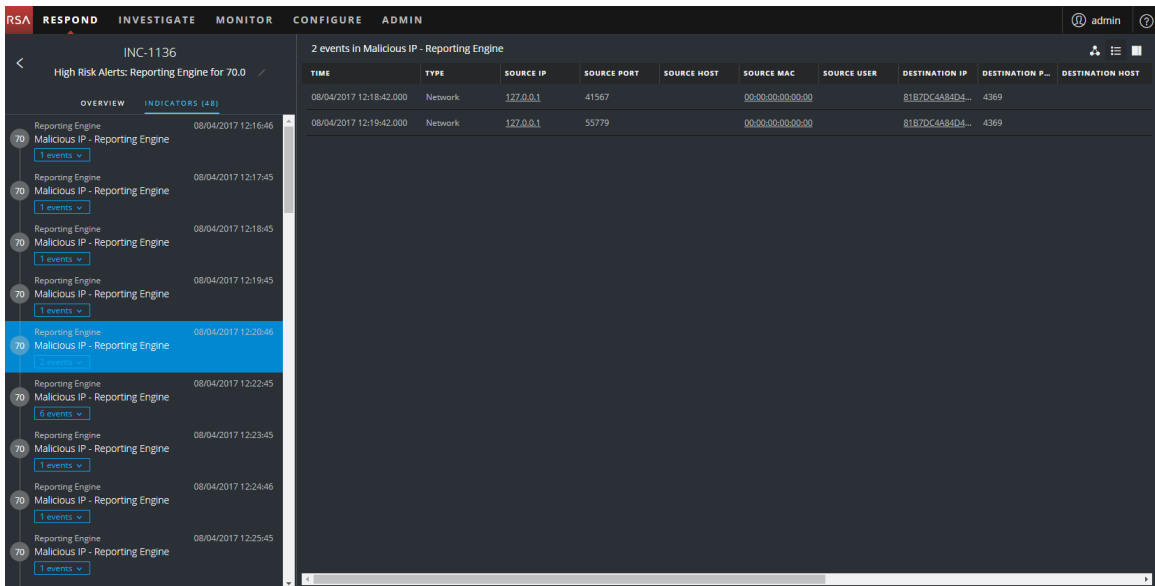
Filter the Data in the Incident Details View

You can click indicators in the Indicators panel to filter what you can see in the nodal graph and the Events list.

If you select an indicator to filter the nodal graph, data that is not part of your selection is dimmed, but it is still in view as shown in the following figure.



If you select an indicator to filter the events list, only the events for that indicator are shown in the list. The following figure shows an indicator selected that contains two events. The filtered Events list shows those two events.



If you select an indicator to filter the events list and there is only one event for that indicator, you can see the event details for that event as shown in the following figure.

INC-1136
High Risk Alerts: Reporting Engine for 70.0

OVERVIEW INDICATORS (48)

Reporting Engine 08/04/2017 12:16:46
70 Malicious IP - Reporting Engine
1 events

Reporting Engine 08/04/2017 12:17:45
70 Malicious IP - Reporting Engine
1 events

Reporting Engine 08/04/2017 12:18:45
70 Malicious IP - Reporting Engine
1 events

Reporting Engine 08/04/2017 12:19:45
70 Malicious IP - Reporting Engine
1 events

Reporting Engine 08/04/2017 12:20:46
70 Malicious IP - Reporting Engine
2 events

Reporting Engine 08/04/2017 12:22:45
70 Malicious IP - Reporting Engine
6 events

Reporting Engine 08/04/2017 12:23:45
70 Malicious IP - Reporting Engine
1 events

Reporting Engine 08/04/2017 12:24:46
70 Malicious IP - Reporting Engine
1 events

Reporting Engine 08/04/2017 12:25:45
70 Malicious IP - Reporting Engine
1 events

Reporting Engine 08/04/2017 12:26:45
70 Malicious IP - Reporting Engine
1 events

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 172.0.0.1
Geolocation

User

Destination Device Port 4369
MAC Address 00:00:00:00:00:00
IP Address 81B7DC4A840441BFACD060E3D45A19C45017B4157FBCE0DE868FD7D21A27E77
Geolocation

User

Detector


Size 1336

Data Size 1336

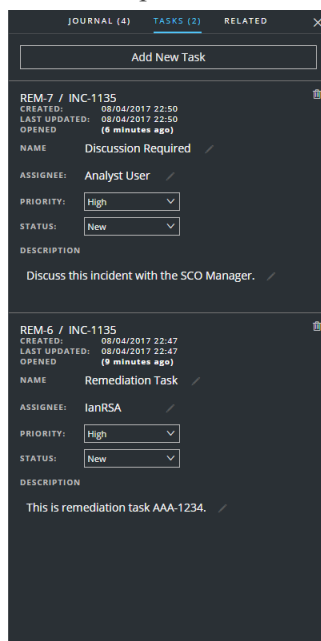
Related Links Type Investigate_original_event
URL /investigation/hosts/10.4.61.30:56005/navigate/event/AUTO/462091

View the Tasks associated with an Incident

Threat responders and other analysts can create tasks for an incident and track those tasks to completion. This can be very helpful, for example, when you require actions on incidents from teams outside of your security operations. You can view the tasks associated with an incident in the Incident Details view.

1. Go to **RESPOND > Incidents** and locate the incident that you want to view in the Incidents List.
2. Click the link in the **ID** or **NAME** field of the incident to go to the Incidents Details view.
3. In the Incident Details view toolbar, click .
The Journal panel opens.
4. Click the **TASKS** tab.

The Tasks panel shows all of the tasks for the incident.




For more information about tasks, see [Tasks List View](#), [View All Incident Tasks](#), and [Create a Task](#).

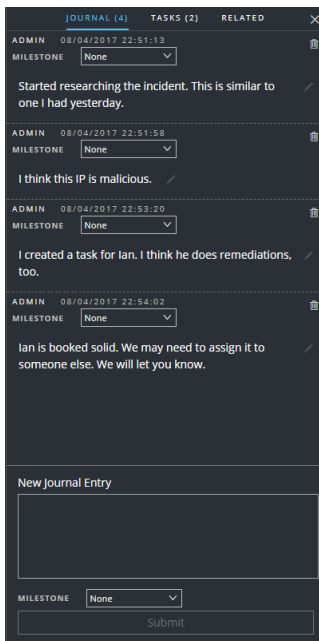
View Incident Notes

The incident Journal enables you to view the history of activity on your incident. You can view journal entries from other analysts and also communicate and collaborate with them.

1. Go to **RESPOND > Incidents** and locate the incident that you want to view in the Incidents List.

2. Click the link in the **ID** or **NAME** field of the incident to go to the Incidents Details view.
3. In the Incident Details view toolbar, click .


The Journal panel shows all of the journal entries for the incident.



Find Related Indicators

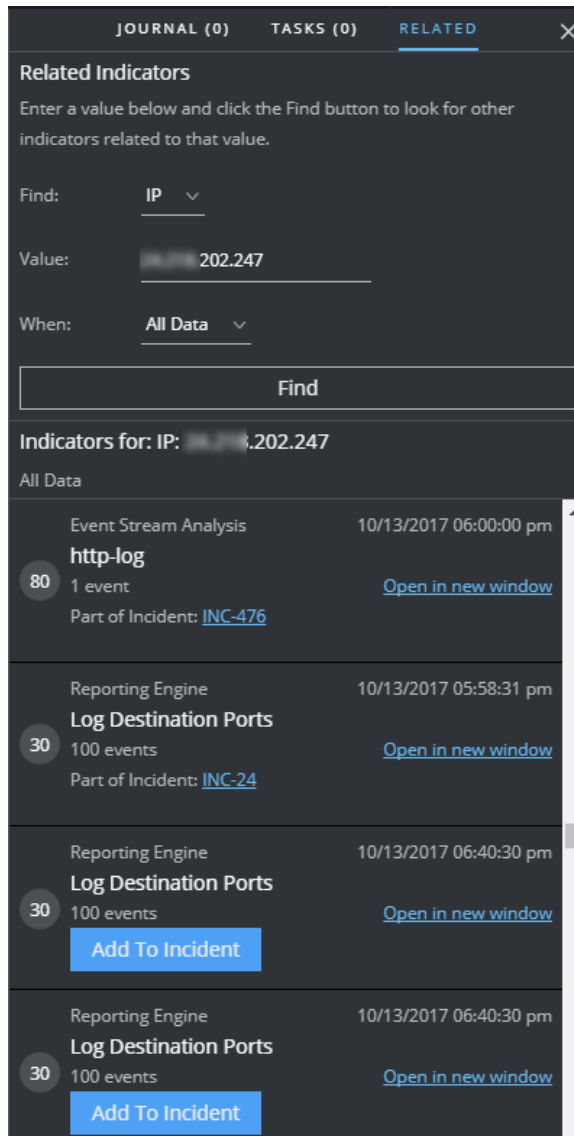
Related Indicators are alerts that were not originally part of the selected incident, but they are related in some way to the incident. The relationship may or may not be obvious. For example, related indicators can involve one or more entities from the incident, but they can also be related due to some intelligence outside of NetWitness Suite.

In the Incident Details view Related panel, you can search for an entity (such as IP, MAC, Host, Domain, User, Filename, or Hash) in other alerts outside of the current incident.

1. Go to **RESPOND > Incidents** and locate the incident that you want to view in the Incidents List.
2. Click the link in the **ID** or **NAME** field of the incident to go to the Incidents Details view.
3. In the Incident Details view toolbar, click .

The Journal panel opens on the right.

- Click the **RELATED** tab.



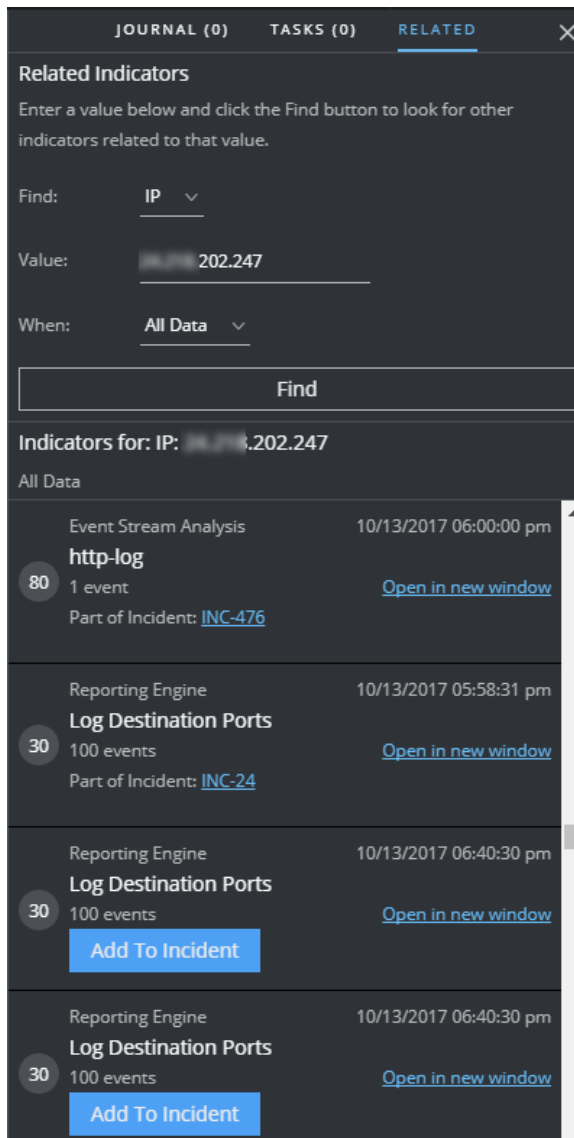
- Click **Find**.

A list of related indicators (alerts) appear below the **Find** button in the **Indicators for** section. If an alert is not part of another incident, you can click the **Add to Incident** button to add the related indicator (alert) to the current incident. See [Add Related Indicators to the Incident](#) below.

Add Related Indicators to the Incident

You can add related indicators (alerts) to the current incident from Related Indicators panel. An indicator that is already part of an incident cannot be part of another incident. In the search results, if an alert is not already part of an incident, it has an **Add to Incident** button.

1. In the **RELATED** (Related Indicators) panel, do a search to find related indicators. See [Find Related Indicators](#) above.



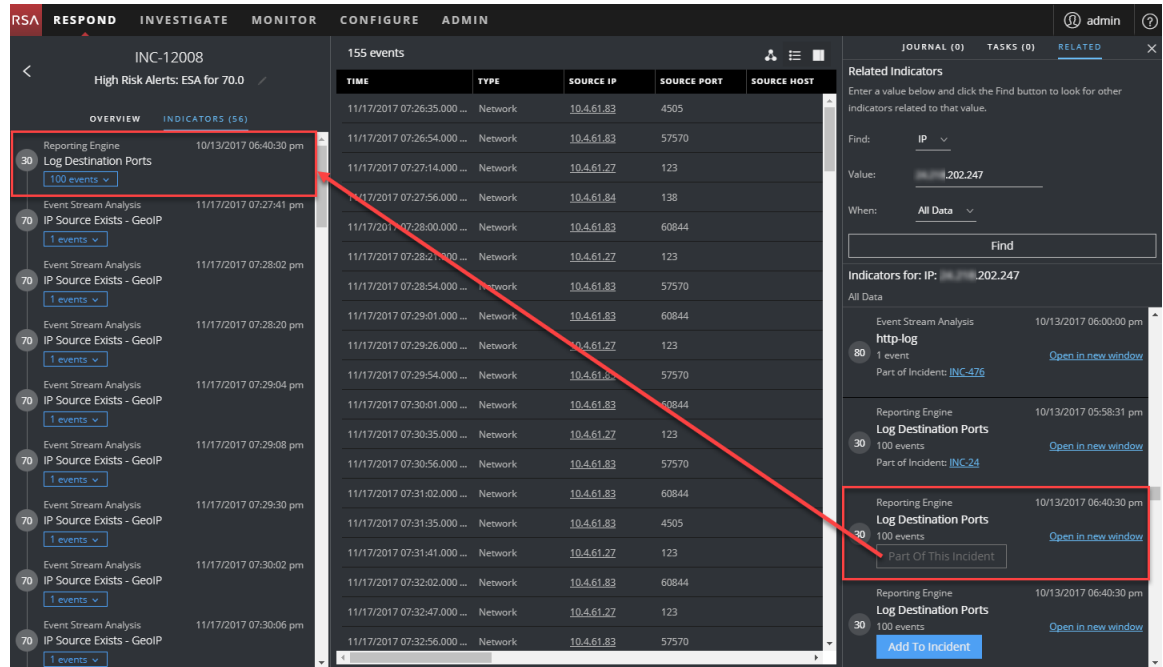
The screenshot shows the 'RELATED' panel in NetWitness Respond. At the top, there are tabs for 'JOURNAL (0)', 'TASKS (0)', and 'RELATED'. Below the tabs, the panel is titled 'Related Indicators' and contains a search form. The search form has a 'Find:' dropdown set to 'IP', a 'Value:' input field containing '202.247', and a 'When:' dropdown set to 'All Data'. A 'Find' button is located below the search form. Below the search form, the results are displayed under the heading 'Indicators for: IP: 202.247'. The results are listed under the 'All Data' filter. There are four entries in the list:

Event Stream Analysis	10/13/2017 06:00:00 pm
http-log 80 1 event Part of Incident: INC-476	Open in new window
Reporting Engine Log Destination Ports 30 100 events Part of Incident: INC-24	Open in new window
Reporting Engine Log Destination Ports 30 100 events	Open in new window Add To Incident
Reporting Engine Log Destination Ports 30 100 events	Open in new window Add To Incident

2. Review the alerts in the search results. The **Indicators for** section (below the Find button) lists the related indicators (alerts).

- To inspect the details of an alert before adding it as a related indicator to the incident, you can click the **Open in New Window** link to view the alert details for that indicator.
- For each alert that you want to add to the current incident as a related indicator, click the **Add to Incident** button.

The selected related indicator adds to the Indicators panel on the left. The button in the Related Indicators panel on the right now shows **Part of This Incident**.



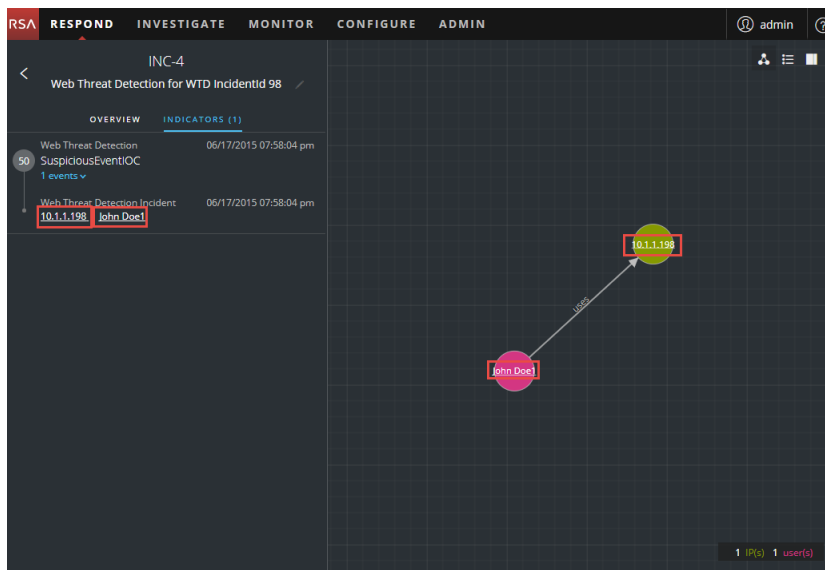
Investigate the Incident

To further investigate an incident within the Incident Details view, you can find links that take you to additional contextual information about the incident when it is available. This additional context can help you understand additional technical context and business context about a specific entity in the incident. It can also provide additional information that you may want to research to ensure that you understand the full scope of the incident.

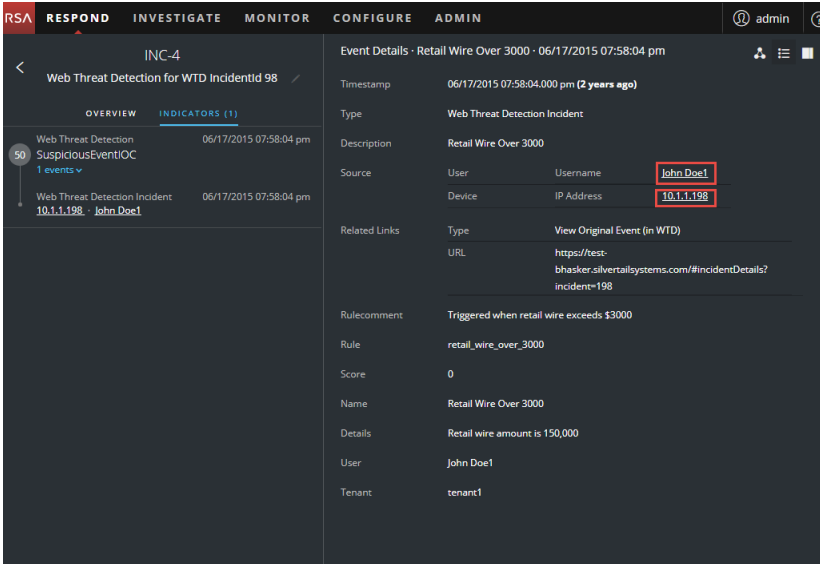
View Contextual Information

In the Indicators panel, Events List panel, Event Details panel, or the Nodal Graph, you can see underlined entities. If an entity is underlined, NetWitness Suite is populating information about that entity type in the Context Hub. There may be additional information available about that entity in the Context Hub.

The following figure shows underlined entities in the Indicators panel and the Nodal Graph.



The following figure shows underlined entities in the Event Details panel.

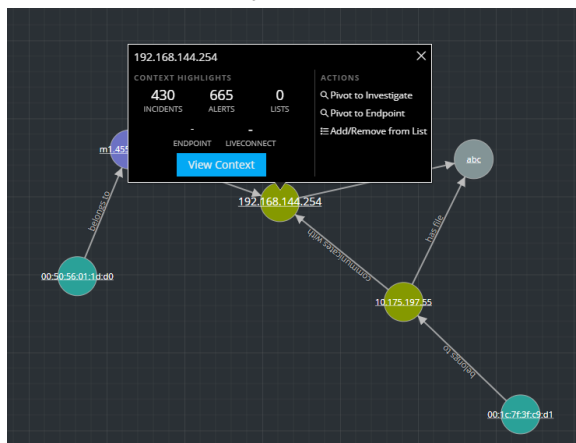


The Context Hub is preconfigured with meta fields mapped to the entities. NetWitness Respond and Investigate use these default mappings for context lookup. For information about adding meta keys, see "Configure Settings for a Data Source" in the *Context Hub Configuration Guide*.

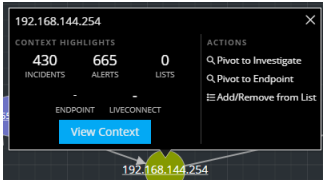
Caution: For the Context Lookup to work correctly in the Respond and Investigate views, RSA recommends that when mapping meta keys in the **ADMIN > SYSTEM > Investigations > Context Lookup** tab, you add only meta keys to the Meta Key Mappings, not fields in the MongoDB. For example, ip.address is a meta key and ip_address is not a meta key (it is a field in the MongoDB).

To view contextual information:

1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over an underlined entity.
A context tooltip appears with a quick summary of the type of context data that is available for the selected entity.



The context tooltip has two sections: Context Highlights and Actions.



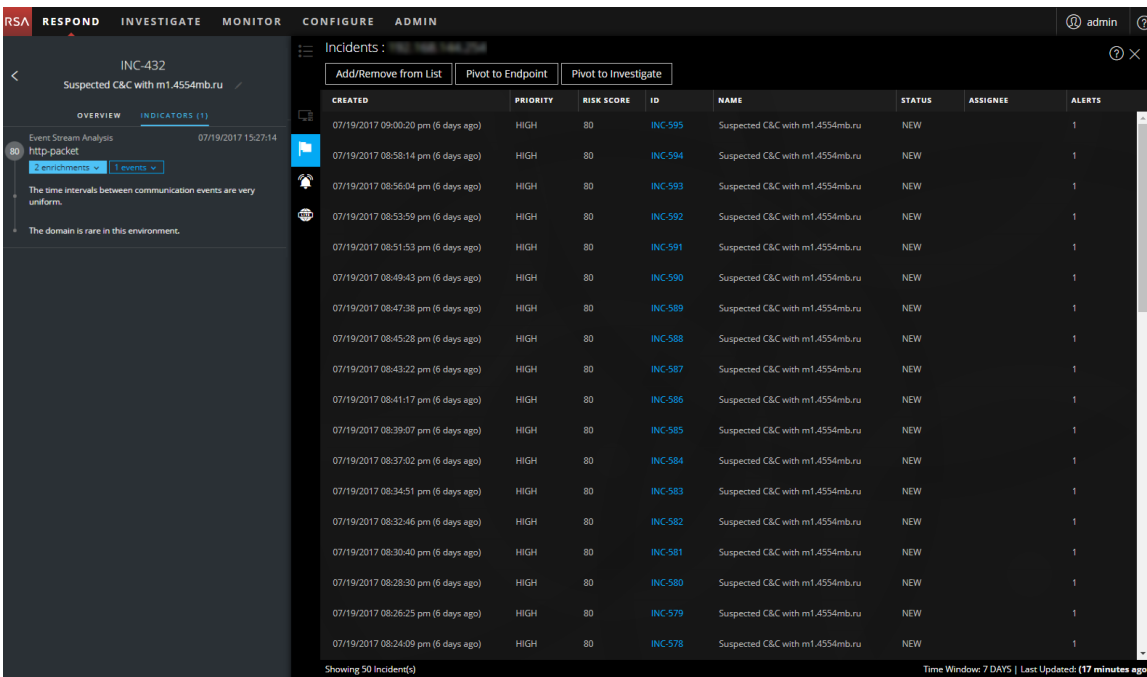
The information in the **Context Highlights** section helps you to determine the actions that you would like to take. It can show related data for Incidents, Alerts, Lists, Endpoint, and Live Connect. Depending on your data, you may be able to click these items for more information. The above example shows 430 related incidents, 665 alerts, 0 lists, and no information in NetWitness Endpoint or Live Connect that mentions the IP address entity, 192.168.144.254.

The **Actions** section lists the available actions. In the above example, the Pivot to Investigate, Pivot to Endpoint, and Add/Remove from List options are available. For more information, see [Pivot to Investigate](#), [Pivot to NetWitness Endpoint](#), and [Add an Entity to a Whitelist](#).

- To see more details about the selected entity, click the **View Context** button.

The Context Lookup panel opens and shows all of the information related to the entity.

The following example shows contextual information for a selected source IP address. It lists all of the incidents that mention the IP address.



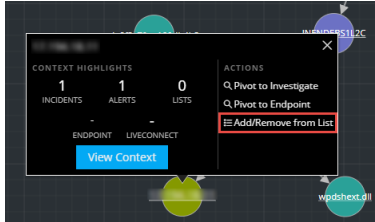
To understand the different views within the Context Hub Lookup panel, see [Context Lookup Panel - Respond View](#).

Add an Entity to a Whitelist

You can add any underlined entity to a list, such as a Whitelist or Blacklist, from a context tooltip. For example, to reduce false positives, you may want to whitelist an underlined domain to exclude it from the related entities.

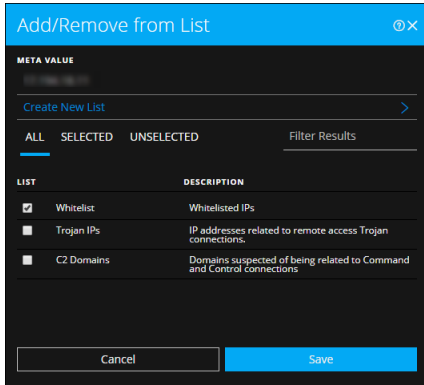
1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over the underlined entity that you would like to add to a Context Hub list.

A context tooltip appears showing the available actions.



2. In the **ACTIONS** section of the tooltip, click **Add/Remove from List**.

The Add/Remove from List dialog shows the available lists.



3. Select one or more lists and click **Save**.

The entity appears on the selected lists.

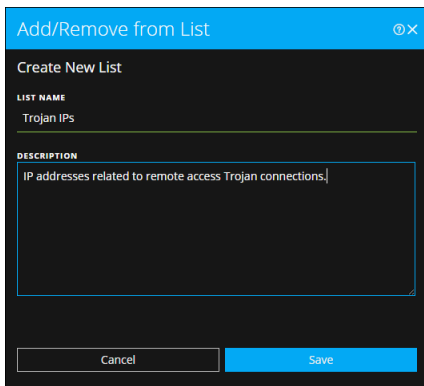
[Add/Remove from List Dialog](#) provides additional information.

Create a List

You can create lists in Context Hub from the Respond view. In addition to using lists to whitelist and blacklist entities, you can use lists to monitor entities for abnormal behavior. For example, to improve the visibility of a suspicious IP address and Domain under investigation, you may want to include them in two separate lists. One list could be for domains suspected of being related to command and control connections, and another list could be for IP addresses related to remote access Trojan connections. You can then identify indicators of compromise using these lists.

To create a list in Context Hub:

1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over the underlined entity that you would like to add to a Context Hub list.
A context tooltip appears showing the available actions.
2. In the **ACTIONS** section of the tooltip, click **Add/Remove from List**.
3. In the Add/Remove from List dialog, click **Create New List**.



4. Type a unique **List NAME** for the list. The list name is not case sensitive.
5. (Optional) Type a **DESCRIPTION** for the list.
Analysts with the appropriate permissions can also export lists in CSV format to send to other analysts for further tracking and analysis. The *Context Hub Configuration Guide* provides additional information.

Pivot to NetWitness Endpoint

If you have the NetWitness Endpoint thick client application installed, you can launch it through the context tooltip. From there, you can further investigate a suspicious IP address, Host, or MAC address.

1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Endpoint**.

The NetWitness Endpoint thick client application opens outside of your web browser.

For more information on the thick client, see the *NetWitness Endpoint User Guide*.

Pivot to Investigate

For a more thorough investigation of the incident, you can access the Investigate view.

1. In the Indicators panel, Events List, Event Details, or the Nodal Graph, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Investigate**.
The Investigate Navigate view opens, which enables you to perform a deeper dive investigation.

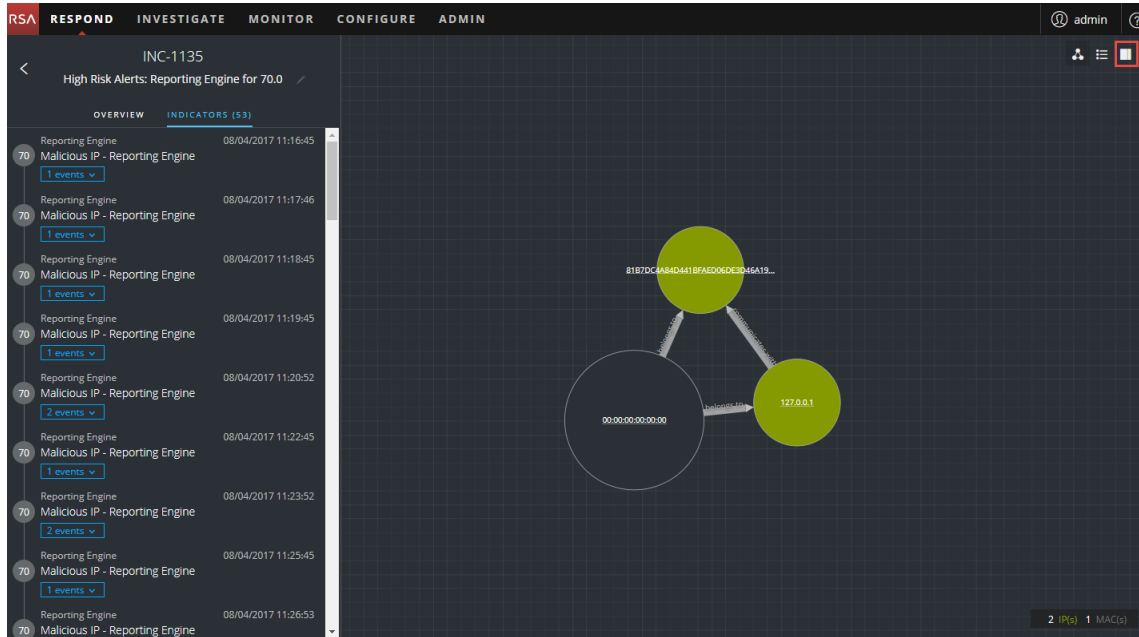
For more information, see the *NetWitness Investigate User Guide*.

Document Steps Taken Outside of NetWitness

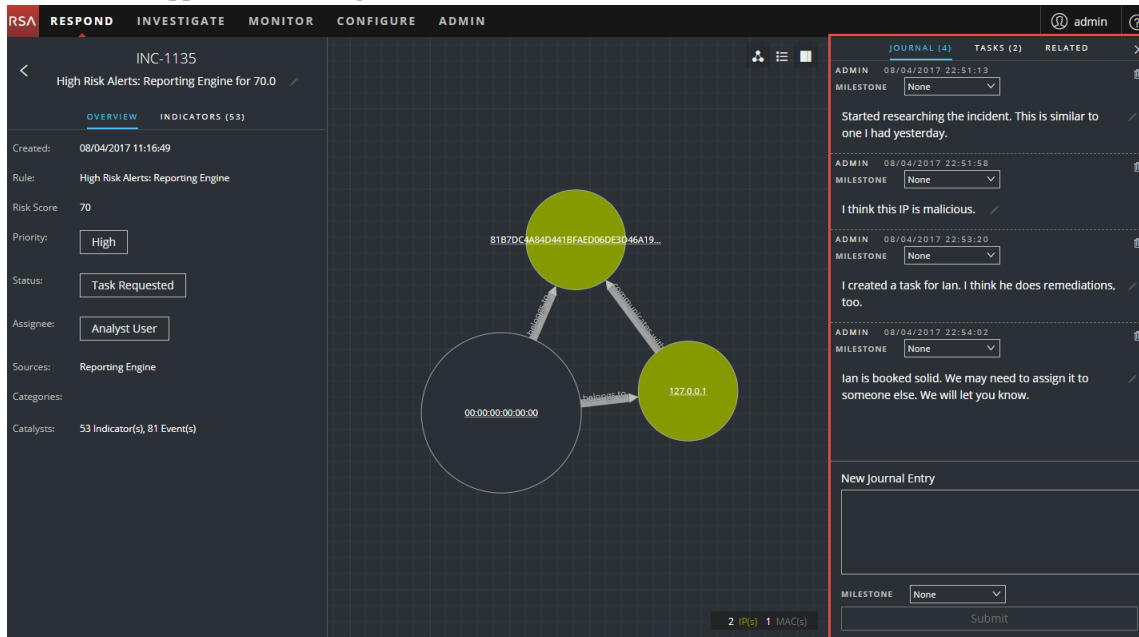
The journal shows notes added by analysts and it enables you to collaborate with your peers. You can post notes to a journal, add Investigation Milestone tags (Reconnaissance, Delivery, Exploitation, Installation, Command and control), and view the history of activity on your incident.

View the Journal Entries for an Incident

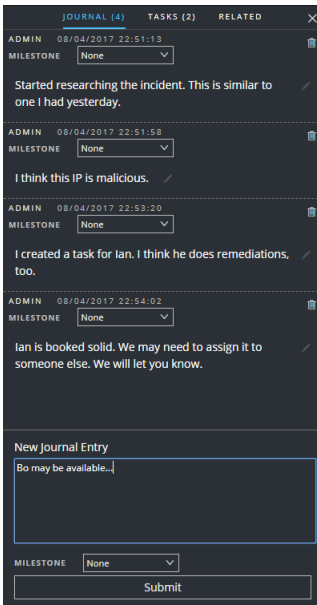
In the Incident Details view toolbar, click .



The Journal appears on the right side of the Incident Details view.



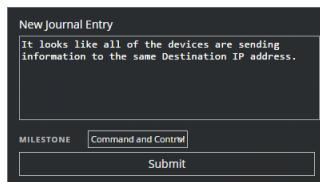
The Journal shows the history of activity on an incident. For each journal entry, you can see the author and time of the entry.



Add a Note

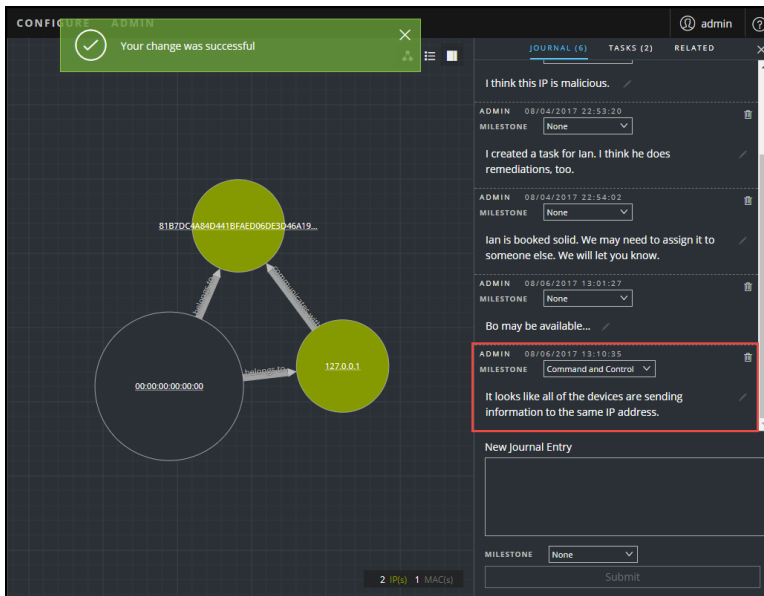
Typically, you will want to add a note to allow another analyst to understand the incident, or add a note for posterity so that your investigative steps are documented.

1. At the bottom of the Journal panel, type your note in the **New Journal Entry** box.




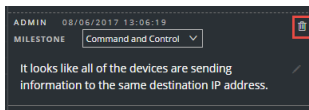
2. (Optional) Select an Investigation Milestone from the drop-down list (Reconnassance, Delivery, Exploitation, Installation, Command and Control, Action On Objective, Containment, Eradication, and Closure).

- After you finish your note, click, **Submit**.
Your new journal entry appears in the Journal.



Delete a Note

- In the Journal panel, locate the journal entry that you would like to delete.
- Click the trash can (delete) icon  next to the journal entry.



- In the confirmation dialog that appears, click **OK** to confirm that you want to delete the journal entry. This action cannot be reversed.

Escalate or Remediate the Incident

You may want to assign incidents to another Analyst or change the status and priority of an incident as you gather more information about it. This is useful if, for example, you upgrade the priority of an incident from **medium** to **high** after determining that the incident is major breach.

Update an Incident

You can update an incident from several places. You can change the priority, status, or assignee from the Incident List view and the Incident Details view. For example, if you are an Analyst, you may want to assign yourself a case from the Incident List view if you see that it is related to another case you are working on. If you are an SOC Manager or an Administrator, you may want to view unassigned incidents from the Incident List view and assign the incidents as they come in. SOC Managers and Administrators can do bulk updates of the priority, status, or assignee instead of updating them one incident at a time.

From the Details view, you might want to change the status to In Progress once you begin working on an incident, and then update it to Closed or Closed - False Positive after you resolve the issue. Or you might change the priority of the incident to Medium or High as you determine the details of the case.

Change Incident Status

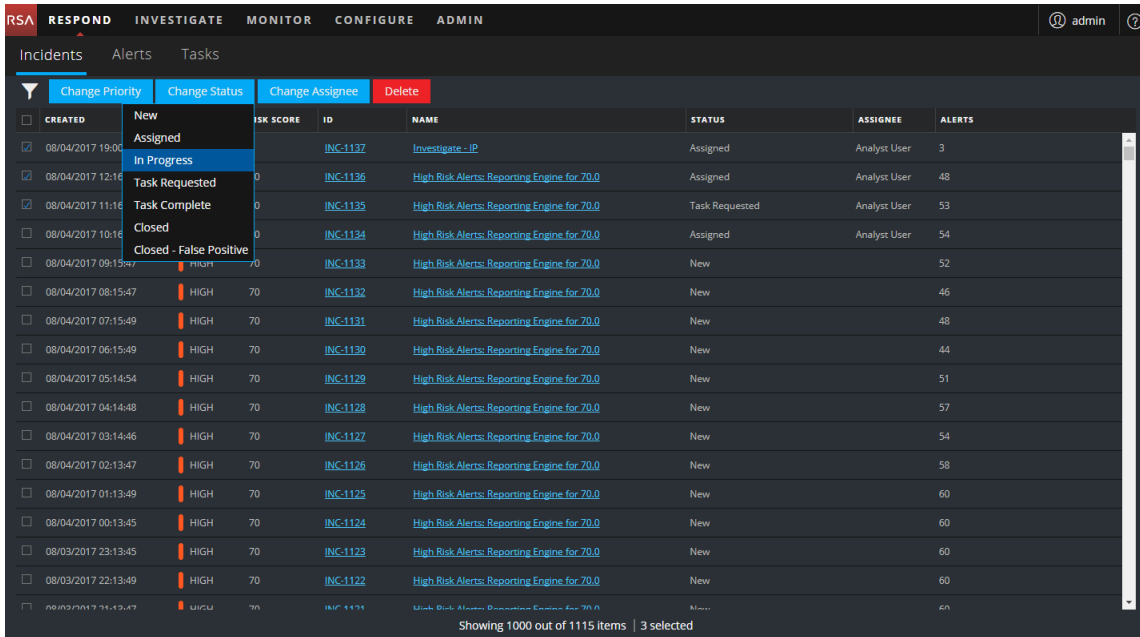
When an incident first appears in the incident list, it has an initial status of New. You can update the status as you complete your work on the incident. The following statuses are available:

- New
- Assigned
- In Progress
- Task Requested
- Task Complete
- Closed
- Closed - False Positive

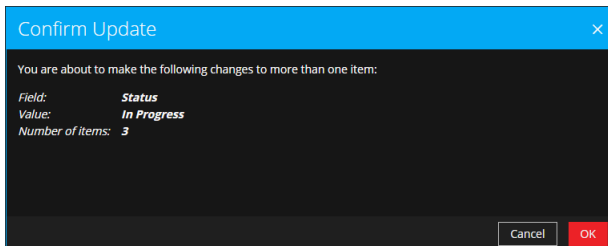
To update the status of multiple incidents:

1. In the Incidents List view, select one or more incidents that you would like to change. To select all of the incidents on the page, select the box in the incidents list header row. The number of incidents selected appears incidents list footer.

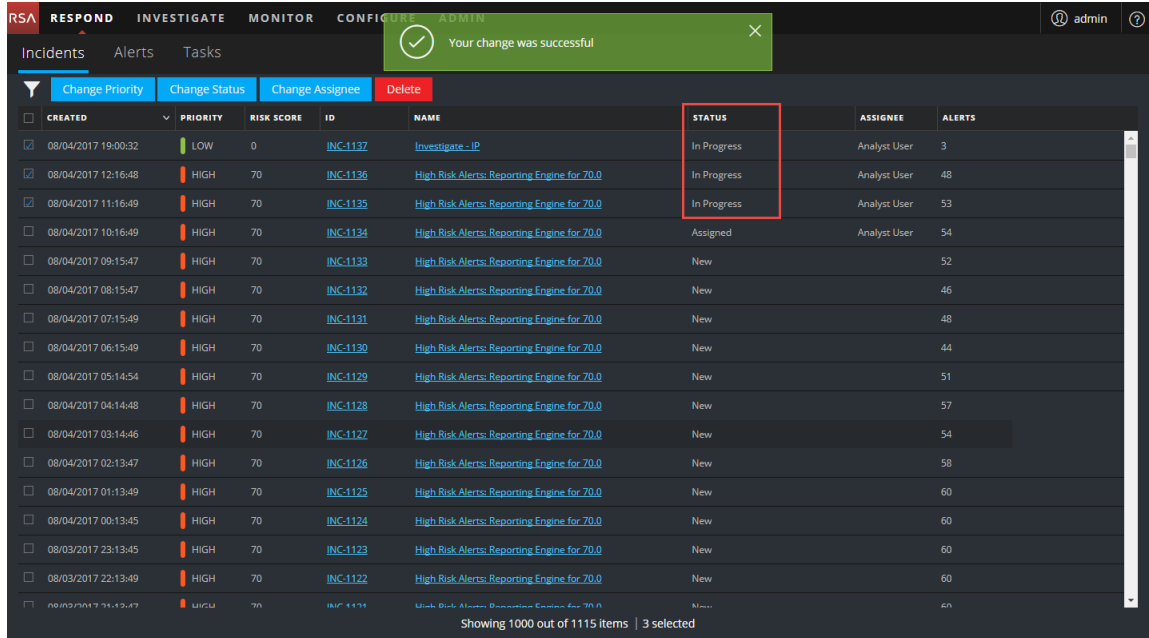
- Click **Change Status** and select a status from the drop-down list. In this example, the current status is Assigned, but the Analyst would like to change it to In Progress for the selected incidents.



- If you select more than one incident, in the **Confirm Update** dialog, click **OK**.

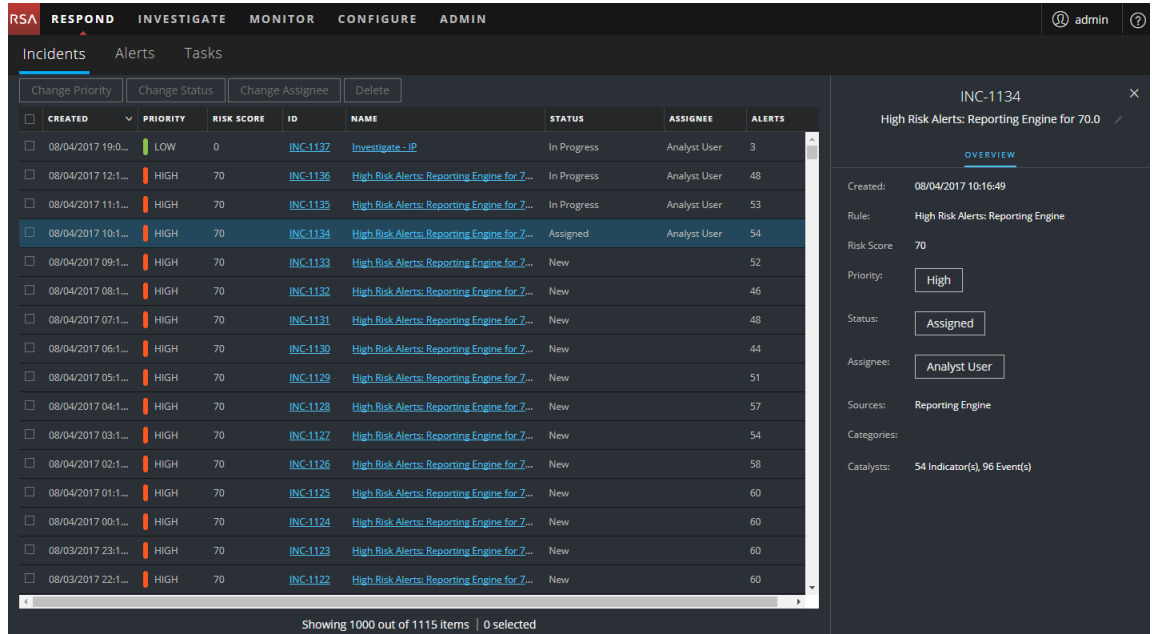


You will see a successful change notification. In this example, the status of the updated incidents now show In Progress.

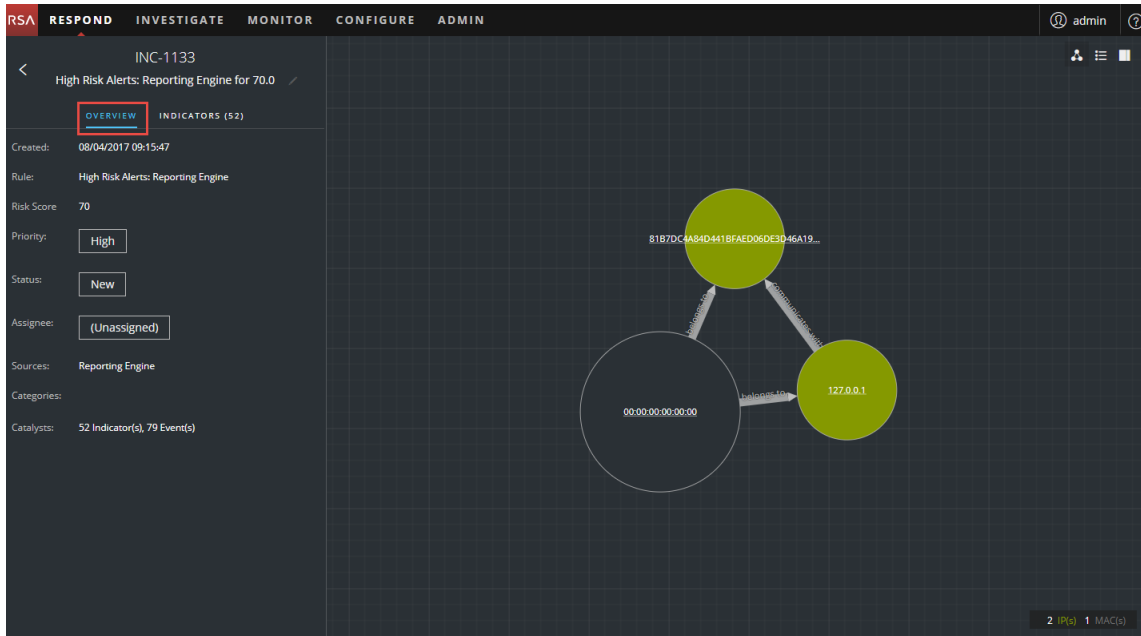


To change the status of a single incident from the Overview panel:

1. To open the Overview panel, do one of the following:
 - From the Incidents List view, click an incident that needs a status update.

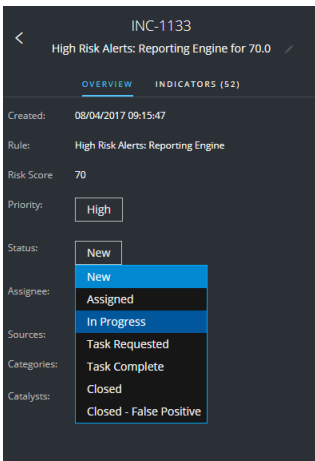


- From the Incident Details view, click the **OVERVIEW** tab.



In the Overview panel, the Status button shows the current status of the incident.

- Click the **Status** button and select a status from the drop-down list.



You will see a successful change notification.



Change Incident Priority

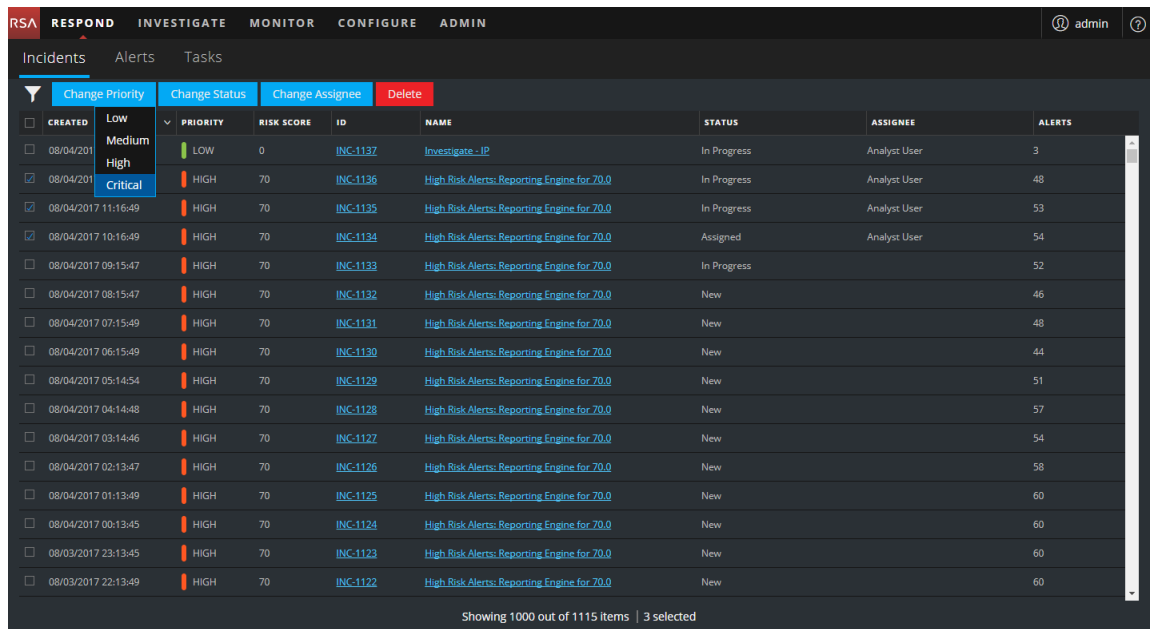
The incident list is sorted by Priority by default. You can update the priority as you study the details of the case. The following priorities are available:

- Critical
- High
- Medium
- Low

Note: You cannot change the priority of a closed incident.

To update the priority of multiple incidents:

1. In the Incidents List view, select one or more incidents that you would like to change. To select all of the incidents on the page, select the box in the incidents list header row. The number of incidents selected appears in the incidents list footer.
2. Click **Change Priority** and select a priority from the drop-down list. In this example, the current priority is High, but the Analyst would like to change it to Critical for the selected incidents.



3. If you select more than one incident, in the **Confirm Update** dialog, click **OK**.
You will see a successful change notification. In this example, the status of the updated

incidents now show Critical.

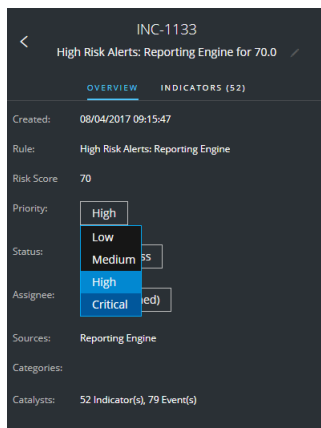
CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 19:00:32	LOW	0	INC-1137	Investigate - IP	In Progress	Analyst User	3
08/04/2017 12:16:48	CRITICAL	70	INC-1136	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	48
08/04/2017 11:16:49	CRITICAL	70	INC-1135	High Risk Alerts: Reporting Engine for 70.0	In Progress	Analyst User	53
08/04/2017 10:16:49	CRITICAL	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	In Progress		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

Showing 1000 out of 1115 items | 3 selected

To change the priority of a single incident from the Overview panel

- To open the Overview panel, do one of the following:
 - From the Incidents List view, click an incident that needs a priority update.
 - From the Incident Details view, click the **OVERVIEW** tab.

In the Overview panel, the Priority button shows the current priority of the incident.
- Click the **Priority** button and select a status from the drop-down list.



You will see a successful change notification. The Priority button changes to show the new incident priority.



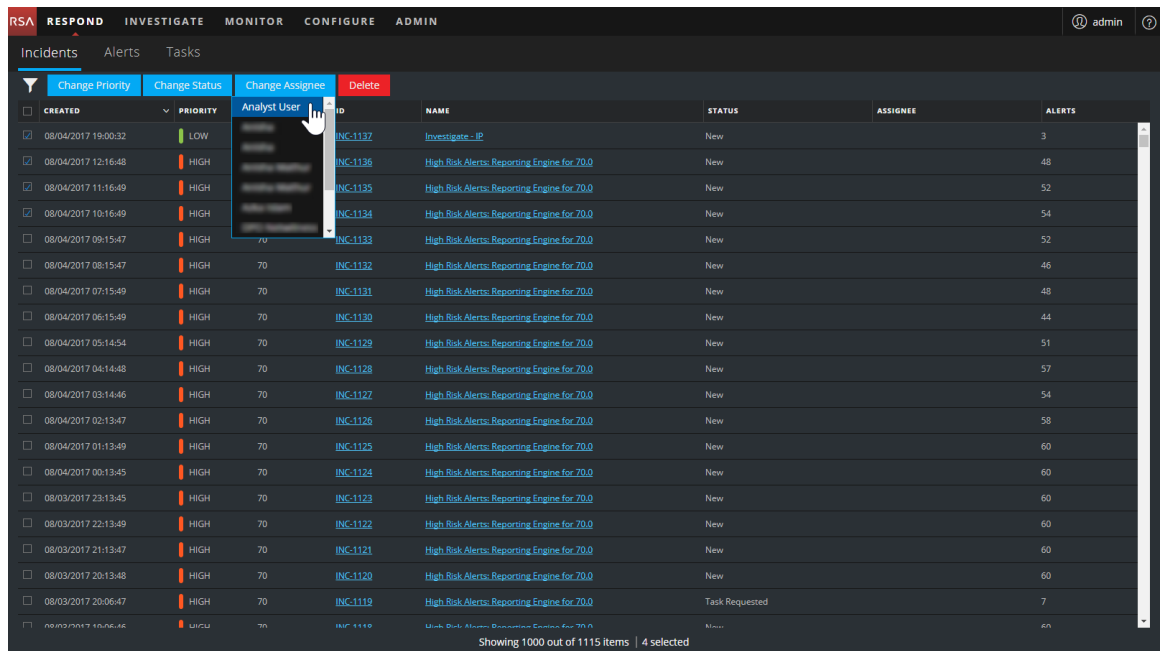
Assign incidents to other Analysts

You can assign incidents to other Analysts in the same way as you assign incidents to yourself. SOC Managers and Administrators can assign multiple incidents to a user at the same time.

Note: You cannot change the assignee of a closed incident.

To assign multiple incidents to a user:

1. In the Incidents List view, select the incidents that you would like to assign to a user. To select all of the incidents on the page, select the box in the incidents list header row. The number of incidents selected appears in the incidents list footer.
2. Click **Change Assignee** and select a user from the drop-down list. In this example, the incidents are unassigned, but they should be assigned to an Analyst.



- If you select more than one incident, in the **Confirm Update** dialog, click **OK**.

You will see a successful change notification. The assignee changes to the selected user.

The screenshot shows the NetWitness Respond interface. At the top, there is a navigation bar with tabs for 'RESPOND', 'INVESTIGATE', 'MONITOR', and 'CONFIGURE'. A green notification banner at the top center says 'Your change was successful'. Below the navigation bar, there are buttons for 'Change Priority', 'Change Status', 'Change Assignee', and 'Delete'. The main area is a table of incidents with the following columns: CREATED, PRIORITY, RISK SCORE, ID, NAME, STATUS, ASSIGNEE, and ALERTS. The 'ASSIGNEE' column is highlighted with a red box. The table contains 20 rows of incident data.

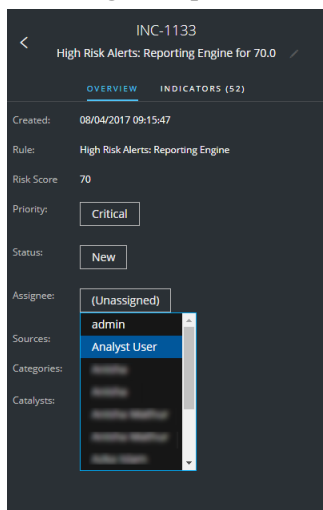
CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
08/04/2017 19:00:32	LOW	0	INC-1137	Investigate - IP	Assigned	Analyst User	3
08/04/2017 12:16:48	HIGH	70	INC-1136	High Risk Alerts: Reporting Engine for 70.0	Assigned	Analyst User	48
08/04/2017 11:16:49	HIGH	70	INC-1135	High Risk Alerts: Reporting 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

Showing 1000 out of 1115 items | 4 selected

To assign a user to an incident from the Overview panel:

1. To open the Overview panel, do one of the following:
 - From the Incidents List view, click an incident that needs a priority update.
 - From the Incident Details view, click the **OVERVIEW** tab.

In the Overview panel, the Priority button shows the current priority of the incident. In the following example, the Assignee button has a current status of Unassigned.



2. Click the **Assignee** button and select a user from the drop-down list.
You will see a successful change notification. The Assignee button changes to show the assigned user.

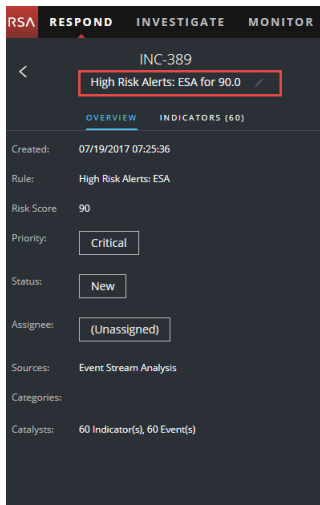


Rename an Incident

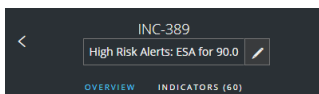
You can rename an incident from the Overview panel in the Incidents List view and the Incident Details view. For example, you may want to rename an incident to provide clarification about the issue, especially if multiple incidents have the same name.

1. Go to **RESPOND > Incidents**.
2. To open the Overview panel, do one of the following:
 - From the Incidents List view, click an incident that needs a name change.
The Overview panel opens.
 - From the Incident Details view, go to the **OVERVIEW** panel.
In the header above the Overview panel, you can see the Incident ID and the incident

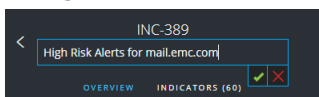
name.



3. Click the incident name in the header to open a text editor.



4. Type a new name for the incident in the text editor and click the check mark to confirm the change.

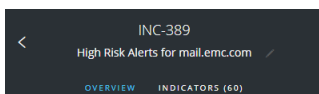


For example, you can change "High Risk Alerts: ESA for 90.0" to "Alerts for mail.emc.com" for more clarification.

You will see a successful change notification.



The incident name field shows the new name.

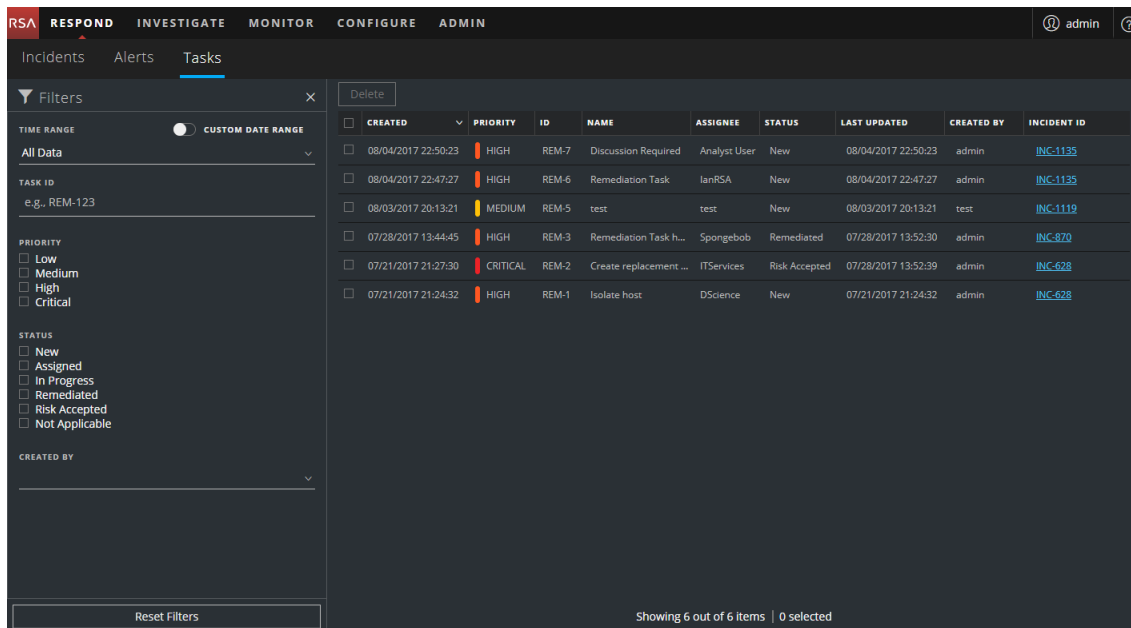


View All Incident Tasks

When additional work is required for an incident, you can create tasks for the incident and track the progress on those tasks. This is helpful, for example, when the work being done is outside security operations or you make a request for a computer reimage. In the Tasks List view, you can manage and track the tasks, to closure.

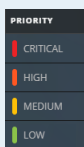
1. Go to **RESPOND > Tasks**.

The Tasks List view displays a list of all incident tasks.



2. Scroll through the tasks list, which shows basic information about each task as described in the following table.

Column	Description
CREATED	Displays the date when the task was created.
PRIORITY	Displays the priority assigned to the task. The priority can be any of the following: Critical, High, Medium, or Low. The Priority is also color coded, where red indicates Critical , orange represents High risk, yellow indicates Medium risk, and green represents Low risk as shown in the following figure:
ID	Displays the task ID.
NAME	Displays the task name.
ASSIGNEE	Displays the name of the user assigned to the task.




Column	Description
STATUS	Displays the status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable.
LAST UPDATED	Displays the date and time when the task was last updated.
CREATED BY	Displays the user who created the task.
INCIDENT ID	Displays the incident ID for which the task was created. Click the ID to display the details of the incident.

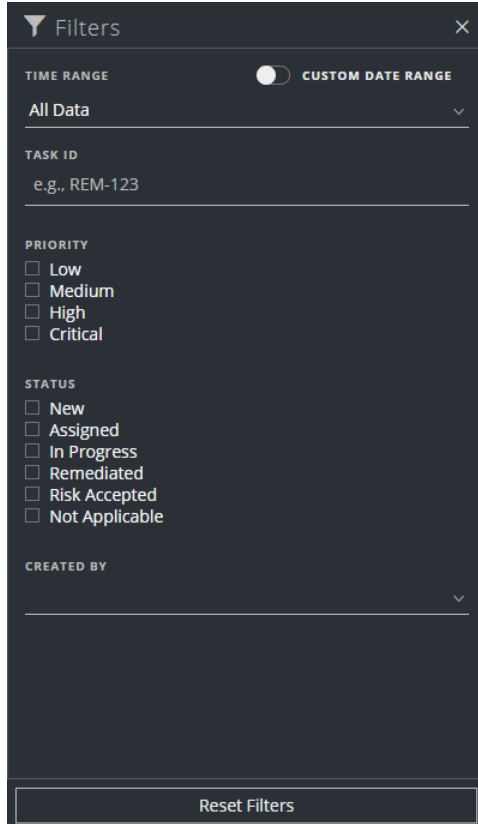
At the bottom of the list, you can see the number of tasks on the current page, the total number of tasks, and the number of tasks selected. For example: **Showing 6 out of 6 items | 2 selected.**

Filter the Tasks List

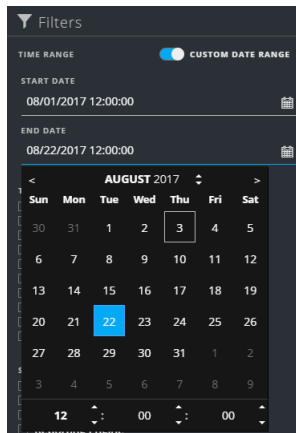
The number of tasks in the Tasks List can be very large, making it difficult to locate particular tasks. The Filter enables you to specify those tasks that you would like to view, such as tasks created within the last 7 days. You can also search for a specific task.

1. Go to **RESPOND > Tasks**.

The Filters panel appears to the left of the Tasks list. If you do not see the Filters panel, in the Tasks List view toolbar, click , which opens the Filters panel.



2. In the Filters panel, select one or more options to filter the incidents list:
 - **TIME RANGE:** You can select a specific time period from the Time Range drop-down list. The time range is based on the creation date of the tasks. For example, if you select Last Hour, you will see tasks that were created within the last 60 minutes.
 - **CUSTOM DATE RANGE:** You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of CUSTOM DATE RANGE to view the Start Date and End Date fields. Select the dates and times from the calendar.



- **TASK ID:** Type the Task ID for a task that you would like to locate, for example REM-123.
- **PRIORITY:** Select the priorities that you would like to view.
- **STATUS:** Select one or more incident statuses. For example, select Remediated to view completed remediation tasks.
- **CREATED BY:** Select the user who created the tasks that you would like to view. For example, if you only want to view the tasks created by Edwardo, select Edwardo from the CREATED BY drop-down list. If you want to view tasks regardless of the person who created the task, do not make a selection under CREATED BY.

The Tasks List shows a list of tasks that meet your selection criteria. You can see the number of items in your filtered list at the bottom of the tasks list.


For example: **Showing 6 out of 6 items**

3. If you want to close the Filters panel, click **X**. Your filters remain in place until you remove them.

Remove My Filters from the Tasks List

NetWitness Suite remembers your filter selections in the Tasks Listview. You can remove your filter selections when you no longer need them. For example, if you are not seeing the number of tasks that you expect to see or you want to view all of the tasks in your tasks list, you can reset your filters.

1. Go to **RESPOND > Tasks**.

The Filters panel appears to the left of the tasks list. If you do not see the Filters panel, in the Tasks List view toolbar, click , which opens the Filters panel.

2. At the bottom of the Filters panel, click **Reset Filters**.

Create a Task

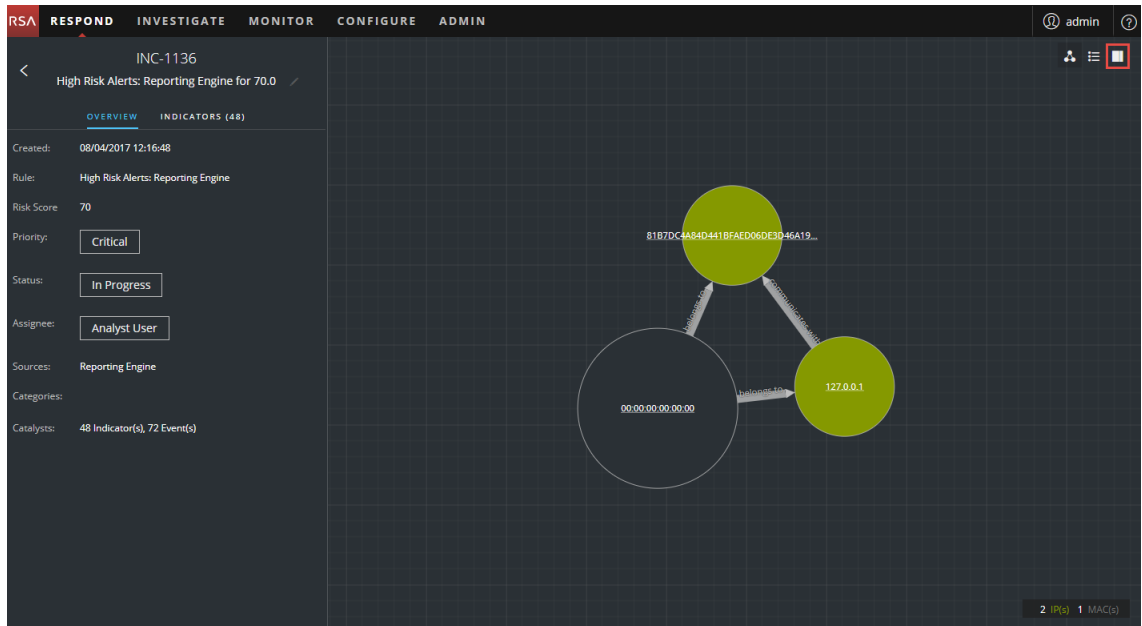
After you investigate an incident and know more about it, you can create a task, assign it to a user, and track it to closure. You create tasks from the Incident Details view.


1. Go to **RESPOND > Incidents**.

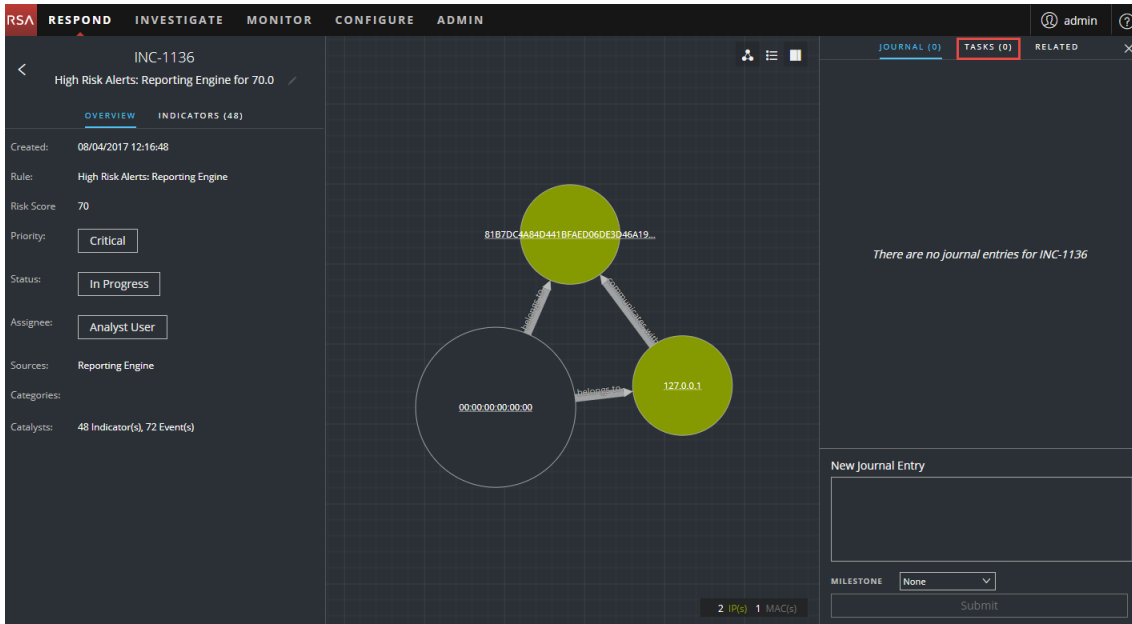
The Incidents List view displays a list of all incidents.

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

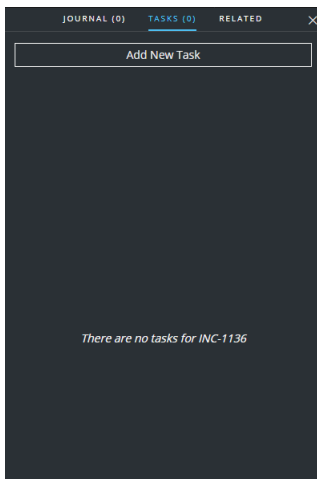
2. Locate the incident that needs a task and click the link in the ID or NAME field. The Incident Details view opens.



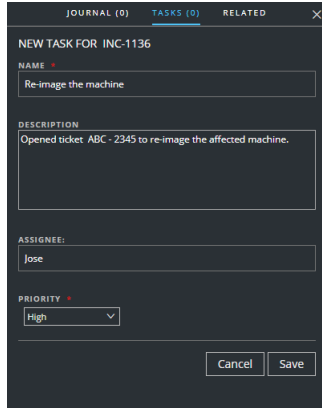
- In the toolbar at the top right of the Incident Details view, select . The Journal panel opens.



- Select the **TASKS** tab.



- In the Tasks panel, click **Add New Task**. You will see the new task fields.



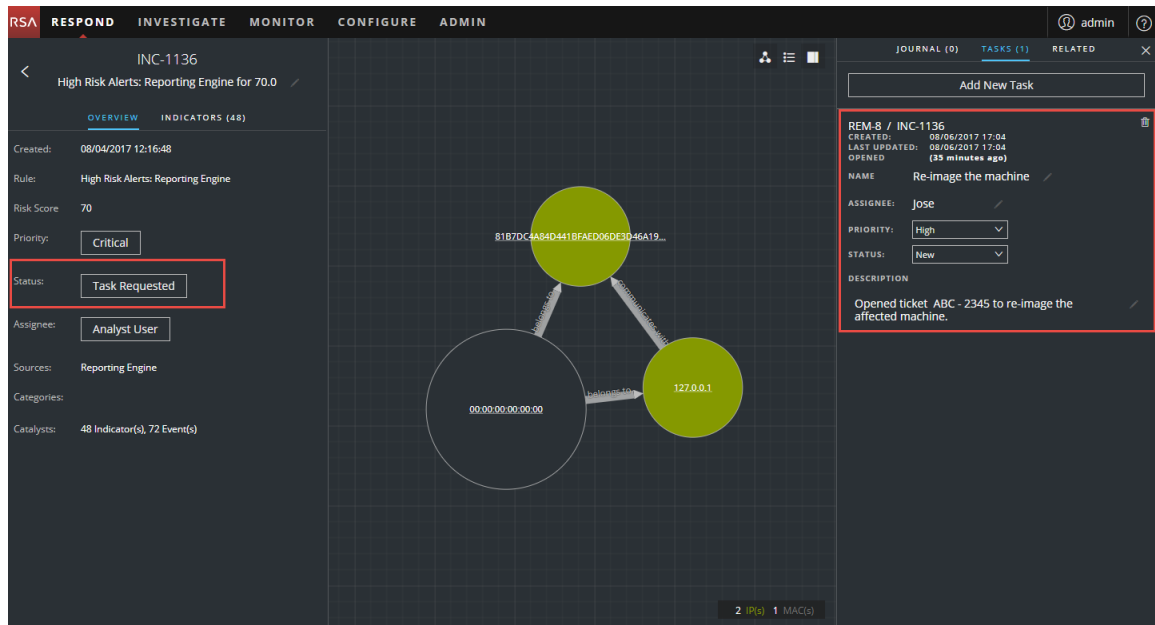
If the incident is in a closed state (Closed or Closed - False Positive), the Add New Task button is disabled.

6. Provide the following information:

- **Name** - Name of the task. For example: Re-image the machine.
- **Description** - (Optional) Type information that describes the task. You may want to include any applicable reference numbers.
- **Assignee** - (Optional) Type the username of the user to whom the task is to be assigned.
- **Priority** - Click the priority button and select a priority for the tasks from the drop-down list: Low, Medium, High, or Critical.

7. Click **Save**.

You will see a confirmation that your change was successful. The incident status changes to **Task Requested**. The task appears in the Tasks panel for this incident.



It also appears in the Tasks list (RESPOND > Tasks), which shows a list of all incident

tasks.

The screenshot displays the NetWitness Respond interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The user is logged in as 'admin'. The main view is 'Tasks', showing a list of tasks with columns for 'CREATED', 'PRIORITY', 'ID', 'NAME', 'ASSIGNEE', 'STATUS', 'LAST UPDATED', 'CREATED BY', and 'INCIDENT ID'. The tasks listed are:

CREATED	PRIORITY	ID	NAME	ASSIGNEE	STATUS	LAST UPDATED	CREATED BY	INCIDENT ID
08/06/2017 17:04:46	HIGH	REM-8	Re-image the machine	Jose	New	08/06/2017 17:04:46	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	Remediation Task	IanRSA	New	08/04/2017 22:47:27	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 ho...	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

The detailed view for task REM-8 shows the following information:

- Incident ID: [INC-1136](#)
- Created: 08/06/2017 17:04:46
- Last Updated: 08/06/2017 17:04:46
- Priority:
- Status:
- Assignee: [Jose](#)
- Description: Opened ticket ABC - 2345 to re-image the affected machine.


At the bottom of the task list, it says 'Showing 7 out of 7 items | 0 selected'.

Note: If you do not see the status change, you may need to refresh your internet browser.

Find a Task

If you know the Task ID, you can quickly locate a task using the Filter. For example, you may want to locate a specific task out of thousands of tasks.

1. Go to **RESPOND > Tasks**.

The Filters panel appears to the left of the Tasks list. If you do not see the Filters panel, in the Tasks List view toolbar, click , which opens the Filters panel.

Filters

TIME RANGE CUSTOM DATE RANGE

All Data

TASK ID

REM-1234

PRIORITY

Low

Medium

High

Critical

STATUS

New

Assigned

In Progress

Remediated

Risk Accepted

Not Applicable

CREATED BY

Reset Filters

2. In the TASK ID field, type the Task ID for a task that you would like to locate, for example REM-1234.
The specified task appears in your task list. If you do not see any results, try resetting your filters.

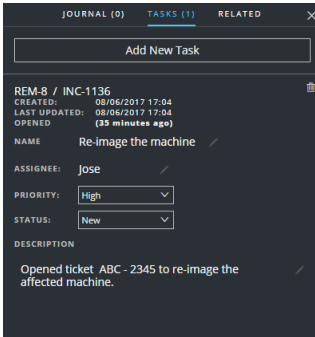
Modify a Task

You can modify a task from within an incident and from the Tasks list. For example, you may want to show the status of the task as In Progress and add some additional information to the task. If the task is in a closed state (Not Applicable, Risk Accepted, or Remediated), you cannot modify the Priority or Assignee.

To modify a Task from within an incident:

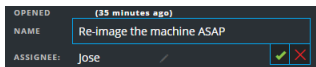
1. Go to **RESPOND > Incidents**.
The Incidents List view displays a list of all incidents.
2. Locate the incident that needs a task update and click the link in the **ID** or **NAME** field.
The Incident Details view opens.
3. In the toolbar at the top right of the view, select **📖**.
The Journal panel opens.

4. Select the **TASKS** tab.
5. In the Tasks panel, a pencil icon indicates a text field that you can change. A button indicates that there is a drop-down list to make a selection.



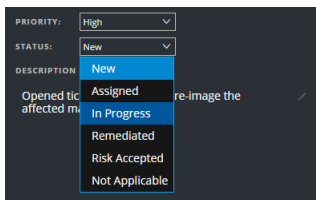
6. You can modify any of the following fields:

- **NAME** - Click the current task name to open a text editor.

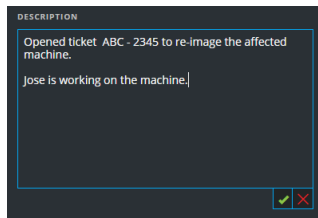


Click the check mark to confirm the change. For example, you can change "Re-image the machine" to "Re-image the machine ASAP."

- **ASSIGNEE** - Click (Unassigned) or the name of the previous assignee to open a text editor. Type the username of the user to whom the task is to be assigned. Click the check mark to confirm the change.
- **PRIORITY** - Click the Priority button and select a priority for the task from the drop-down list: Low, Medium, High, or Critical.
- **STATUS** - Click the Status button and select a status for the task from the drop-down list: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable. For example, you can change the status to In Progress.



- **DESCRIPTION** - Click the text underneath the description to open a text editor.

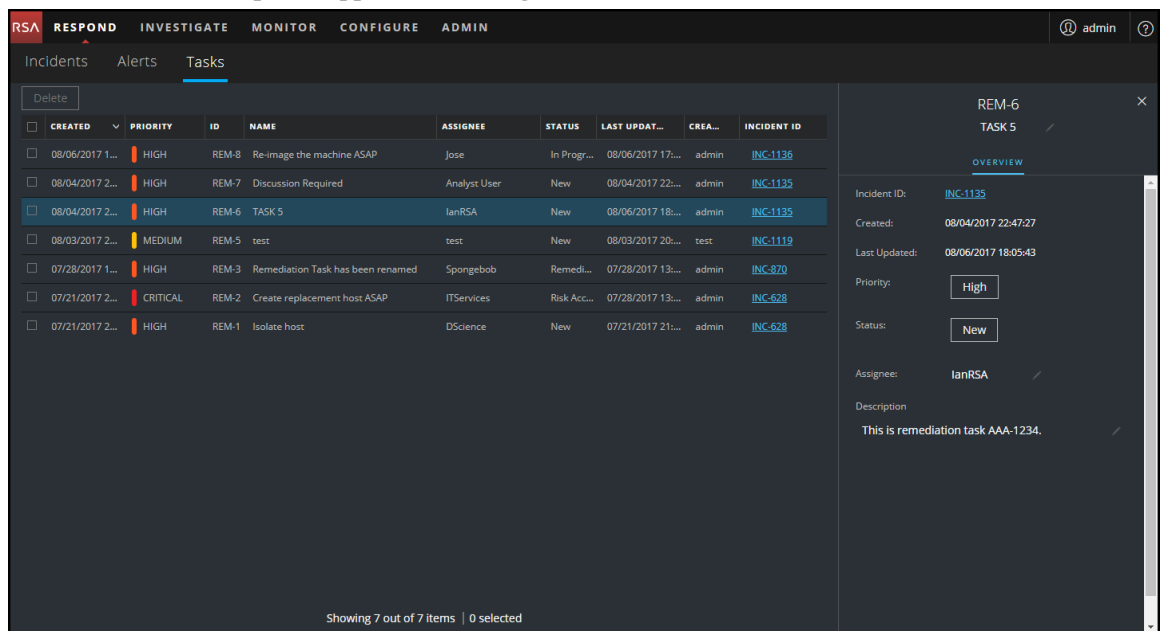


Modify the text and click the check mark to confirm the change.

For each change that you make, you will see a confirmation that your change was successful.

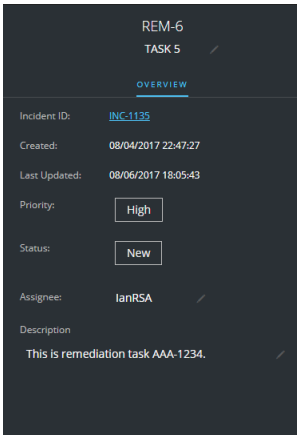
To modify a Task from the Tasks list:

1. Go to **RESPOND > Tasks**.
The Tasks List view displays a list of all incident tasks.
2. In the Tasks list, click the task that you want to update.
The Task Overview panel appears to the right of the tasks list.



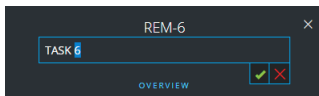
In the Task Overview panel, a pencil icon indicates a text field that you can change. A

button indicates that there is a drop-down list to make a selection.



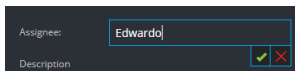
3. You can modify any of the following fields:

- **<Task Name>** - At the top of the Task Overview panel, below the Task ID, click the current task name to open a text editor.



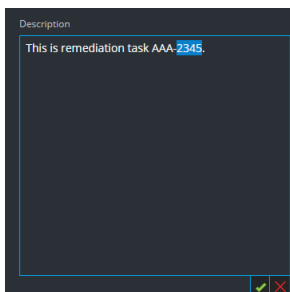
Click the check mark to confirm the change. For example, you can change TASK 5 to TASK 6.

- **Priority** - Click the Priority button and select a priority for the task from the drop-down list: Low, Medium, High, or Critical.
- **Status** - Click the Status button and select a status for the task from the drop-down list: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable.
- **Assignee** - Click (Unassigned) or the name of the previous assignee to open a text editor. Type the username of the user to whom the task is to be assigned.



Click the check mark to confirm the change.

- **Description** - Click the text underneath the description to open a text editor.




Modify the text and click the check mark to confirm the change.

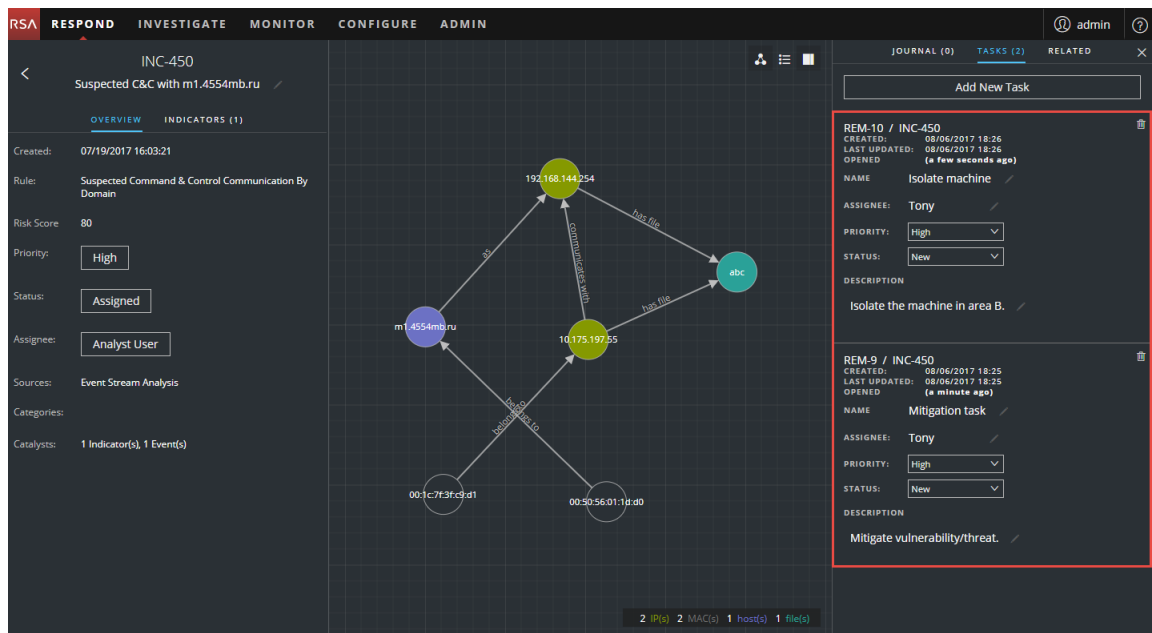
For each change that you make, you will see a confirmation that your change was successful.

Delete a Task

You can delete a task, if, for example, you created it in error or you find that it is not needed. You can delete a task from within an incident and also from the Tasks List view. In the Tasks List view, you can delete multiple tasks at the same time.

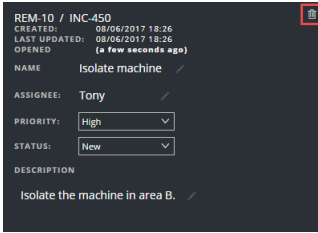
To Delete a Task from within an incident:

1. Go to **RESPOND > Incidents**.
The Incidents List view displays a list of all incidents.
2. Locate the incident that needs a task update and click the link in the **ID** or **NAME** field.
The Incident Details view opens.
3. In the toolbar at the top right of the view, select .
The Journal panel opens.
4. Select the **TASKS** tab.
5. In the Tasks panel, you can see the tasks created for the incident.

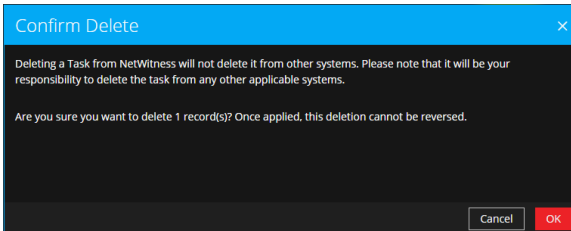


The screenshot displays the NetWitness Respond interface for incident INC-450. On the left, the 'OVERVIEW' panel shows incident details: Created: 07/19/2017 16:03:21, Rule: Suspected Command & Control Communication By Domain, Risk Score: 80, Priority: High, Status: Assigned, Assignee: Analyst User, Sources: Event Stream Analysis, and Catalysts: 1 Indicator(s), 1 Event(s). The central network diagram shows nodes for m1.4554mb.ru, 192.168.144.254, 10.175.197.55, 00:c7:f3f:c3:d1, and 00:50:56:01:1d:d0, with relationships like 'is', 'communicates with', and 'has file'. On the right, the 'TASKS (2)' panel lists two tasks: REM-10 / INC-450 (Isolate machine) and REM-9 / INC-450 (Mitigation task), both assigned to Tony with a High priority and New status.

- Click  to the right of the task that you want to delete.



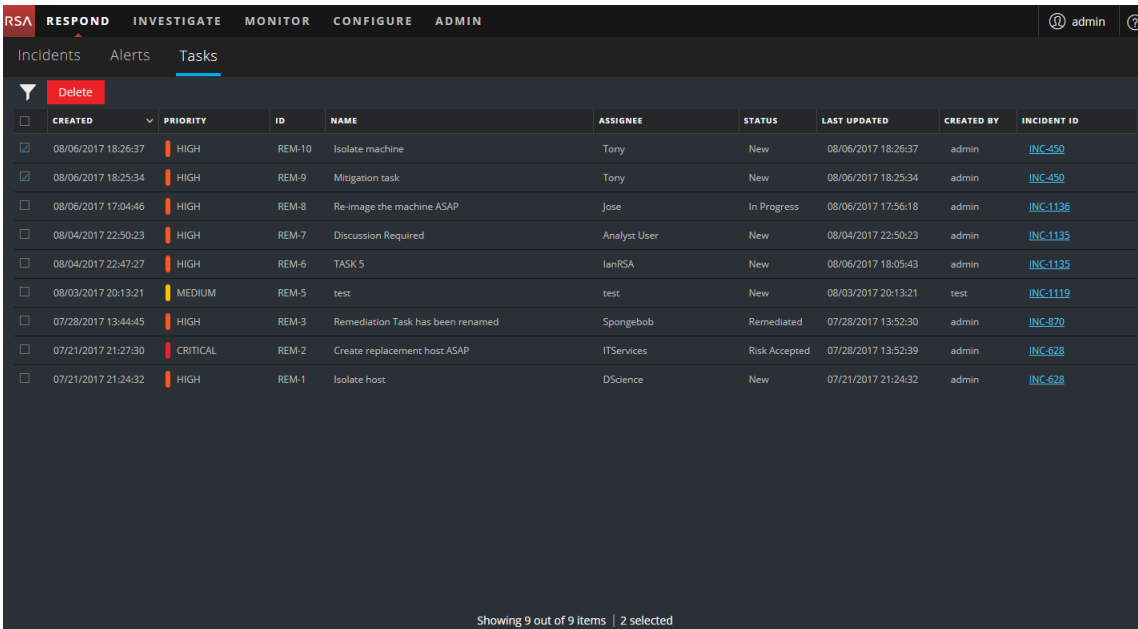
- Confirm that you want to delete the task and click **OK**.



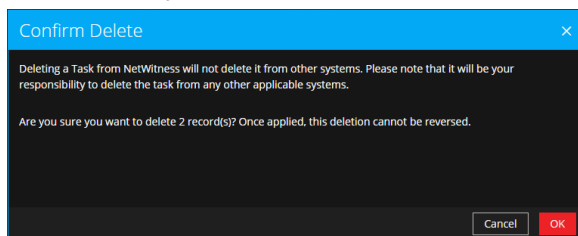
The task is deleted from NetWitness Suite. Deleting tasks from NetWitness Suite does not delete them from other systems.

To Delete Tasks from the Tasks List:

- Go to **RESPOND > Tasks**.
The Tasks List view displays a list of all incident tasks.
- In the Tasks list, select the tasks that you want to delete and click **Delete**.



3. Confirm that you want to delete the tasks and click **OK**.



The tasks are deleted from NetWitness Suite. Deleting tasks from NetWitness Suite does not delete them from other systems.

Close an Incident

When you have arrived at a solution after investigating an incident and remediating it, you close the incident.

1. Go to **RESPOND > Incidents**.
2. In the Incident List view, select the incident that you want to close and click **Change Status**.
3. Select **Closed** from the drop-down list.

You will see a successful change notification. The incident is now closed. You cannot change the priority or assignee of a closed incident.

Note: You can also close an incident in the Overview panel. You can close multiple incidents at the same time in the Incident List view. [Change Incident Status](#) provides additional details.

Reviewing Alerts

NetWitness Suite enables you to view a consolidated list of threat alerts generated from multiple sources in one location. You can find these alerts in the RESPOND > Alerts view. The source of the alerts can be ESA correlation rules, ESA Analytics, NetWitness Endpoint, Malware Analysis, Reporting Engine, as well as many others. You can see the original source of the alerts, the alert severity, and additional alert details.

Note: ESA correlation rule alerts can ONLY be found in the RESPOND > Alerts view.

To better manage a large number of alerts, you have the ability to filter the alerts list based criteria that you specify, such as severity, time range, and alert source. For example, you may want to filter the alerts to only show those alerts with a severity between 90 and 100 that are not already part of an incident. You can then select a group of alerts to create an incident or add to an existing incident.

You can perform the following procedures to review and manage alerts:

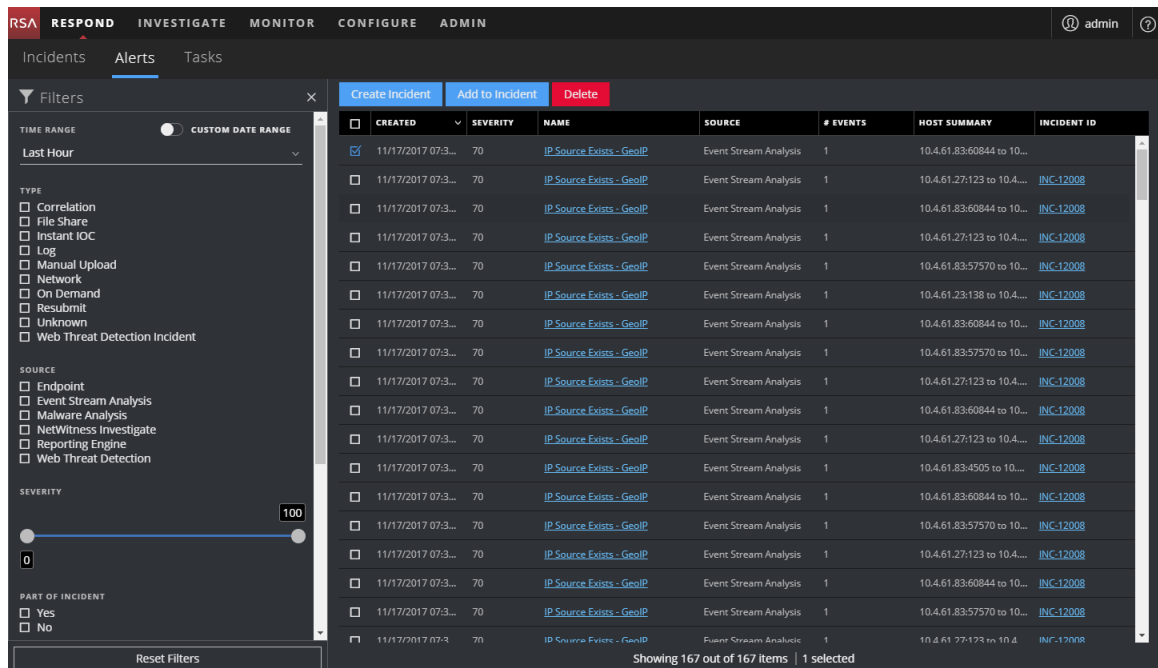
- [View Alerts](#)
- [Filter the Alerts List](#)
- [Remove My Filters from the Alerts List](#)
- [View Alert Summary Information](#)
- [View Event Details for an Alert](#)
- [Investigate Events](#)
- [Create an Incident Manually](#)
- [Add Alerts to an Incident](#)
- [Delete Alerts](#)

View Alerts

In the Alerts List view you can browse through various alerts from multiple sources, filter them, and group them to create incidents. This procedure shows you how to access the alerts list.

1. Go to **RESPOND > Alerts**.

The Alerts List view displays a list of all NetWitness Suite alerts.



2. Scroll through the alerts list, which shows basic information about each alert as described in the following table.

Column	Description
CREATED	Displays the date and time when the alert was recorded in the source system.
SEVERITY	Displays the level of severity of the alert. The values are from 1 through 100.
NAME	Displays a basic description of the alert.
SOURCE	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, Event Stream Analysis (ESA Correlation Rules), ESA Analytics, Reporting Engine, Web Threat Detection, and many others.
# EVENTS	Indicates the number of events contained within an alert. This varies depending on the source of the alert. For example, NetWitness Endpoint and Malware Analysis alerts always have one Event. For certain types of alerts, a high number of events may mean that the alert is more risky.


Column	Description
HOST SUMMARY	Displays details of the host like the host name from where the alert was triggered. The details may include information about the source and destination hosts in an Alert. Some alerts may describe events across more than one host .
INCIDENT ID	Shows the Incident ID of the alert. If there is no incident ID, the alert does not belong to any incident and you can create an incident to include this alert or the alert can be added to an existing incident.

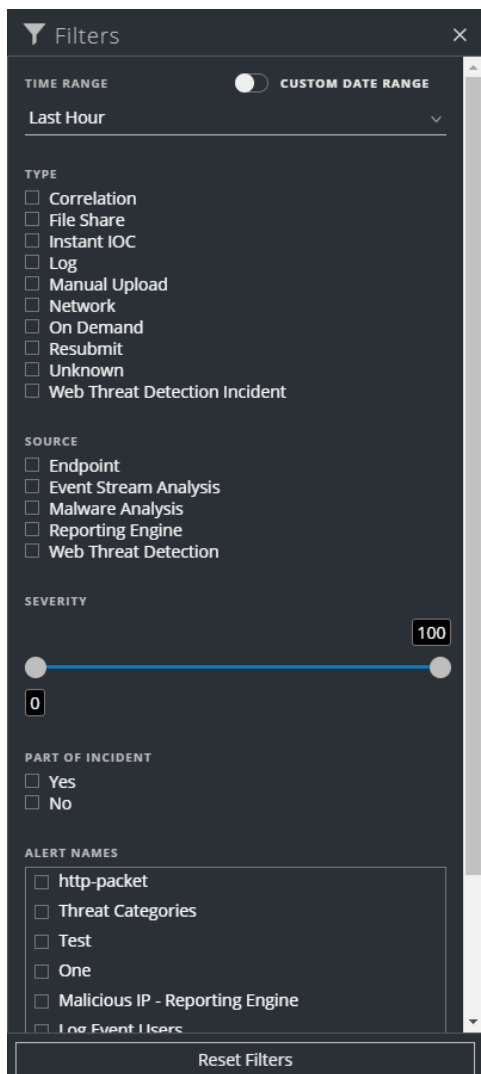
At the bottom of the list, you can see the number of alerts on the current page and the total number of alerts. For example: **Showing 377 out of 377 items**

Filter the Alerts List

The number of alerts in the Alerts List can be very large, making it difficult to locate particular alerts. The Filter enables you to view the alerts you want to see, for example, alerts from a particular source, alerts of a particular severity, alerts that are not part of an incident, and so on.

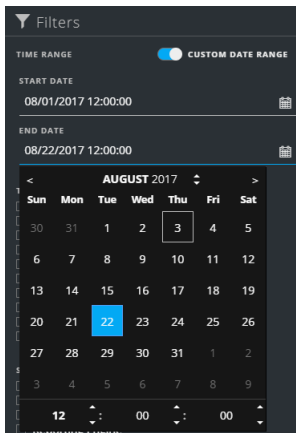
1. Go to **RESPOND > Alerts**.

The Filters panel appears to the left of the Alerts list. If you do not see the Filters panel, in the Alerts List view toolbar, click , which opens the Filters panel.



2. In the Filters panel, select one or more options to filter the alerts list:
 - **TIME RANGE:** You can select a specific time period from the Time Range drop-down list. The time range is based on the date that the alerts were received. For example, if you select Last Hour, you will see alerts that were received within the last 60 minutes.
 - **CUSTOM DATE RANGE:** You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of CUSTOM DATE RANGE to view the Start Date and End Date fields. Select the dates and times from the

calendar.



- **TYPE:** Select the type of events in the alert to view, for example, logs, network sessions, and so on.
- **SOURCE:** Select one or more sources to view alerts triggered by the selected sources. For example, to view NetWitness Endpoint alerts only, select Endpoint as the source.
- **SEVERITY:** Select the the level of severity of the alerts to view. The values are from 1 through 100. For example, to concentrate on the highest severity alerts first, you may want to view only those alerts with a severity from 90 to 100.
- **PART OF INCIDENT:** To view only alerts that are not part of an incident, select **No**. To view only alerts that are part of an incident, select **Yes**. For example, when you are ready to create an incident from a group of alerts, you can select No to view only those alerts that are not currently part of an incident.
- **ALERT NAMES:** Select the name of the alert to view. You can use this filter to search for all alerts generated by a specific rule or source, for example, Malicious IP - Reporting Engine.

The Alerts List shows a list of alerts that meet your selection criteria. You can see the number of items in your filtered list at the bottom of the alerts list.

For example: **Showing 30 out of 30 items**

3. If you want to close the Filters panel, click **X**. Your filters remain in place until you remove them.

Remove My Filters from the Alerts List

NetWitness Suite remembers your filter selections in the Alerts List view. You can remove your filter selections when you no longer need them. For example, if you are not seeing the number of alerts that you expect to see or you want to view all of the alerts in your alerts list, you can reset your filters.

1. Go to **RESPOND > Alerts**.

The Filters panel appears to the left of the alerts list. If you do not see the Filters panel, in the Alerts List view toolbar, click , which opens the Filters panel.

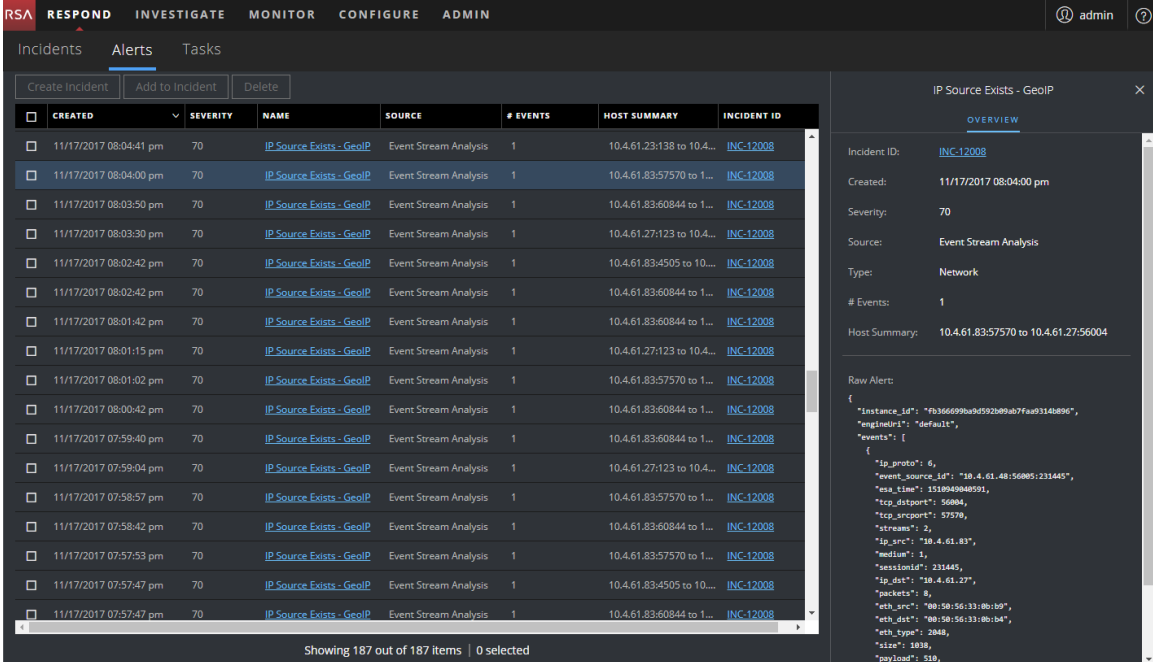
2. At the bottom of the Filters panel, click **Reset Filters**.

View Alert Summary Information

In addition to viewing basic information about an alert, you can also view raw alert metadata in the Overview panel.

1. In the Alerts list, click the alert that you want to view.

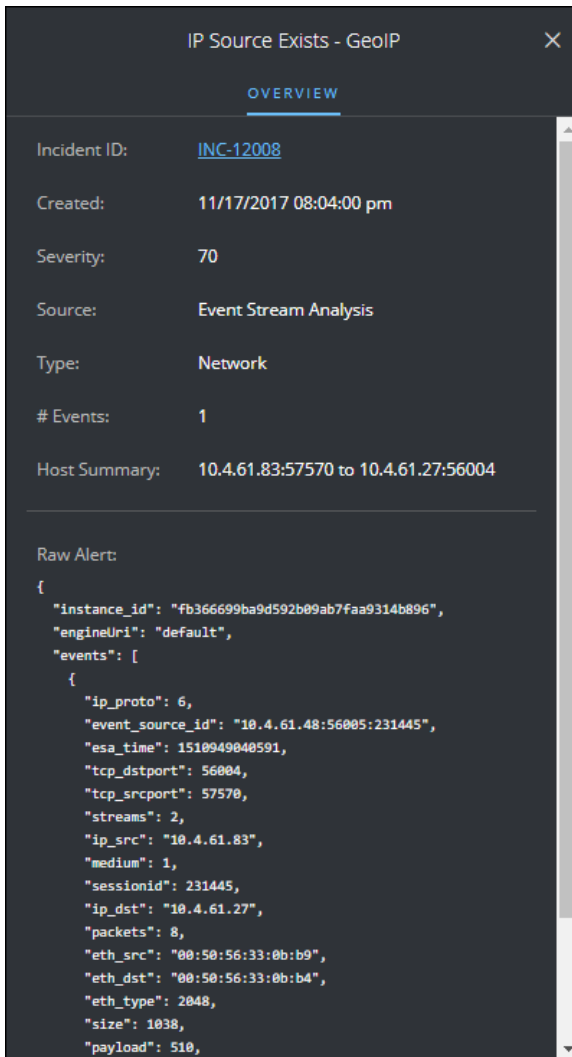
The Alert Overview panel appears to the right of the Alerts list.



The screenshot shows the NetWitness Respond interface. The top navigation bar includes 'RSA', 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The user is logged in as 'admin'. The main view is 'Alerts', with sub-tabs for 'Incidents' and 'Tasks'. A toolbar contains 'Create Incident', 'Add to Incident', and 'Delete' buttons. Below the toolbar is a table of alerts with columns: 'CREATED', 'SEVERITY', 'NAME', 'SOURCE', '# EVENTS', 'HOST SUMMARY', and 'INCIDENT ID'. The table shows 187 items, with the first few rows highlighted. The right-hand side of the interface displays the 'Overview' panel for a selected alert titled 'IP Source Exists - GeoIP'. This panel shows details such as Incident ID (INC-12008), Created time (11/17/2017 08:04:00 pm), Severity (70), Source (Event Stream Analysis), Type (Network), # Events (1), and Host Summary (10.4.61.83:57570 to 10.4.61.27:56004). The 'Raw Alert' section displays a JSON object with various fields like instance_id, engine_id, event_time, tcp_dport, tcp_sport, streams, ip_src, medium, sessionid, ip_dst, packets, eth_src, eth_dst, eth_type, size, and payload.

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID
11/17/2017 08:04:41 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.23:138 to 10.4...	INC-12008
11/17/2017 08:04:00 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:57570 to 1...	INC-12008
11/17/2017 08:03:50 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:60844 to 1...	INC-12008
11/17/2017 08:03:30 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.27:123 to 10.4...	INC-12008
11/17/2017 08:02:42 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:4505 to 10...	INC-12008
11/17/2017 08:02:42 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:60844 to 1...	INC-12008
11/17/2017 08:01:42 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:60844 to 1...	INC-12008
11/17/2017 08:01:15 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.27:123 to 10.4...	INC-12008
11/17/2017 08:01:02 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:57570 to 1...	INC-12008
11/17/2017 08:00:42 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:60844 to 1...	INC-12008
11/17/2017 07:59:40 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:60844 to 1...	INC-12008
11/17/2017 07:59:04 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.27:123 to 10.4...	INC-12008
11/17/2017 07:58:57 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:57570 to 1...	INC-12008
11/17/2017 07:58:42 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:60844 to 1...	INC-12008
11/17/2017 07:57:53 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:57570 to 1...	INC-12008
11/17/2017 07:57:47 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:4505 to 10...	INC-12008
11/17/2017 07:57:47 pm	70	IP Source Exists - GeoIP	Event Stream Analysis	1	10.4.61.83:60844 to 1...	INC-12008

2. In the Raw Alert section, you can scroll to view the raw alert metadata.



IP Source Exists - GeolP

OVERVIEW

Incident ID: [INC-12008](#)

Created: 11/17/2017 08:04:00 pm

Severity: 70

Source: Event Stream Analysis

Type: Network

Events: 1

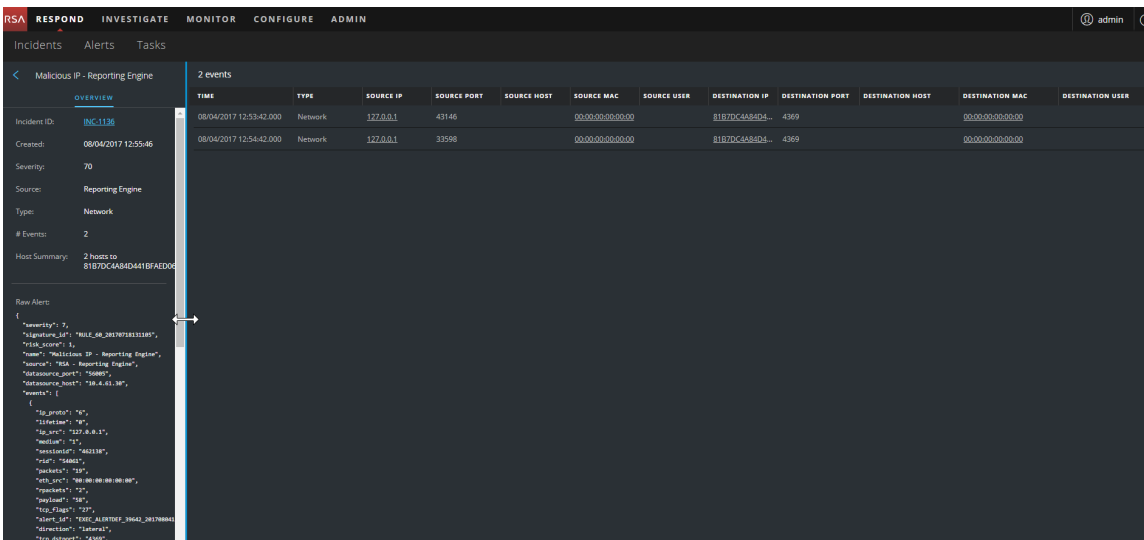
Host Summary: 10.4.61.83:57570 to 10.4.61.27:56004

Raw Alert:

```
{
  "instance_id": "fb366699ba9d592b09ab7Faa9314b896",
  "engineUri": "default",
  "events": [
    {
      "ip_proto": 6,
      "event_source_id": "10.4.61.48:56005:231445",
      "esa_time": 1510949040591,
      "tcp_dstport": 56004,
      "tcp_srcport": 57570,
      "streams": 2,
      "ip_src": "10.4.61.83",
      "medium": 1,
      "sessionid": 231445,
      "ip_dst": "10.4.61.27",
      "packets": 8,
      "eth_src": "00:50:56:33:0b:b9",
      "eth_dst": "00:50:56:33:0b:b4",
      "eth_type": 2048,
      "size": 1038,
      "payload": 510,
    }
  ]
}
```

View Event Details for an Alert

After you review the general information about the alert in the Alerts List view, you can go to the Alert Details view for more detailed information to determine the action required. An alert contains one or more events. In the Alert Details view, you can drill down into an alert to get additional event details and further investigate the alert. The following figure shows an example of the Alert Details view.



The Overview panel on the left has the same information for an alert as the Overview panel in the Alerts List view.

The Events panel on the right shows information about the events in the alert, such as event time, source IP, destination IP, detector IP, source user, destination user, and file information about the events. The amount of information listed depends on the event type.

There are two types of events:

- A transaction between two machines (a Source and a Destination)
- An anomaly detected on a single machine (a Detector)

Some events will only have a Detector. For example, NetWitness Endpoint finds malware on your machine. Other events will have a Source and Destination. For example, packet data shows communication between your machine and a Command and Control (C2) domain.

You can drill further into an event to get detailed data about the event.

To View the Event Details for an Alert:

1. To view event details for an alert, in the Alerts List view, choose an alert to view and then click the link in the NAME column for that alert.

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	127.0.0.1:60051 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	127.0.0.1:47073 to 8187DC4A84D441BF...	

Showing 54 out of 54 items | 0 selected

The Alerts Details view shows the Overview panel on the left and the Events panel on the 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 17:25:44.000	Network	127.0.0.1	40699		00:00:00:00:00:00		8187DC4A84D4...	4369		00:00:00:00:00:00	
08/04/2017 17:26:04.000	Network	127.0.0.1	54078		00:00:00:00:00:00		8187DC4A84D4...	15671		00:00:00:00:00:00	
08/04/2017 17:26:04.000	Network	127.0.0.1	54106		00:00:00:00:00:00		8187DC4A84D4...	15671		00:00:00:00:00:00	
08/04/2017 17:26:04.000	Network	127.0.0.1	54130		00:00:00:00:00:00		8187DC4A84D4...	15671		00:00:00:00:00:00	
08/04/2017 17:26:04.000	Network	127.0.0.1	54142		00:00:00:00:00:00		8187DC4A84D4...	15671		00:00:00:00:00:00	
08/04/2017 17:26:04.000	Network	127.0.0.1	54158		00:00:00:00:00:00		8187DC4A84D4...	15671		00:00:00:00:00:00	

The Events panel shows a list of events with information about each event. The following table shows some of the columns that can appear in the Events List (Events Table).

Column	Description
TIME	Shows the time the event occurred.
TYPE	Shows the type of alert, such as Log and Network.

Column	Description
SOURCE IP	Shows the source IP address if there was a transaction between two machines.
DESTINATION IP	Shows the destination IP address if there was a transaction between two machines
DETECTOR IP	Shows the IP address of the machine where an anomaly was detected.
SOURCE USER	Shows the user of the source machine.
DESTINATION USER	Shows the user of the destination machine.
FILE NAME	Shows the file name if a file is involved with the event.
FILE HASH	Shows a hash of the file contents.

If there is only one event in the list, you will see the event details for that event instead of a list.

2. Click an event in the Events list to view the Event details.

This example shows the event details for the first event in the list.

The screenshot displays the NetWitness Respond interface. At the top, there is a navigation bar with the following tabs: **RESPOND**, **INVESTIGATE**, **MONITOR**, **CONFIGURE**, and **ADMIN**. The user is logged in as **admin**. Below the navigation bar, there are tabs for **Incidents**, **Alerts**, and **Tasks**. The main content area is titled **Malicious IP - Reporting Engine** and is divided into two sections: **OVERVIEW** and **Event Details**.

OVERVIEW section:

- Incident ID: (None)
- Created: 08/04/2017 06:17:45 pm
- Severity: 70
- Source: Reporting Engine
- Type: Network
- # Events: 6
- Host Summary: 6 hosts to 2 hosts

Event Details section (Timestamp: 08/04/2017 06:15:45 pm (5 minutes ago)):

- Back To Table < 1 of 6 >
- Timestamp: 08/04/2017 06:15:45.000 pm (5 minutes ago)
- Type: Network
- Source:

Device	Port	57830
MAC Address	00:00:00:00:00:00	
IP Address	177.0.0.1	
Geolocation		
- User: (None)
- Destination:

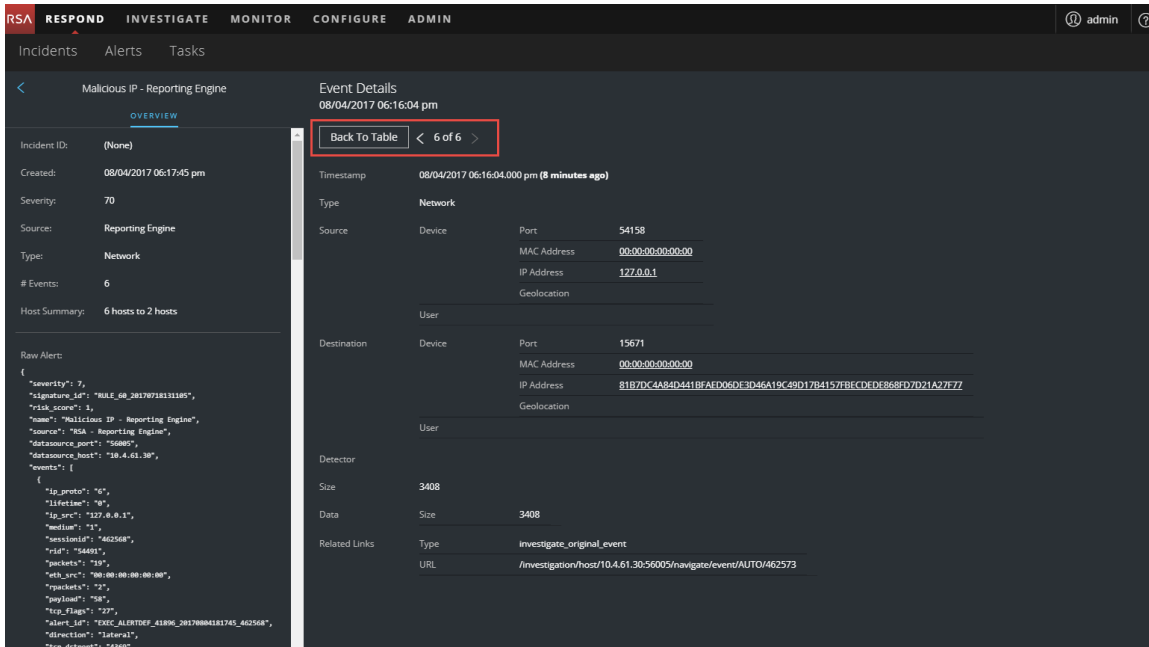
Device	Port	4369
MAC Address	00:00:00:00:00:00	
IP Address	81B7DC4AR4D441BFAED06DE3D46A19C49D17B4157BCCDE868FD7D21A27F77	
Geolocation		
- Detector: 1336
- Size: 1336
- Data: 1336
- Related Links:

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

Raw Alert:

```
{
  "severity": 7,
  "signature_id": "RULE_00_20170718111195",
  "risk_score": 3,
  "name": "Malicious IP - Reporting Engine",
  "source": "RSA - Reporting Engine",
  "data_source_port": "56005",
  "data_source_host": "10.4.61.30",
  "events": [
    {
      "ip_proto": "50",
      "lifetime": "0",
      "ip_src": "177.0.0.1",
      "medium": "1",
      "destination_ip": "462568",
      "id": "54491",
      "packets": "19",
      "eth_src": "00:00:00:00:00:00",
      "packets": "2",
      "payload": "0x",
      "tcp_flags": "27",
      "alert_id": "F56C_ALERTDEF_41896_20170804181745_462568",
      "direction": "false",
      "tcp_dstport": "4369"
    }
  ]
}
```

- Use the page navigation to the right of the Back To Table button to view other events. This example shows the event details for the last event in the list.



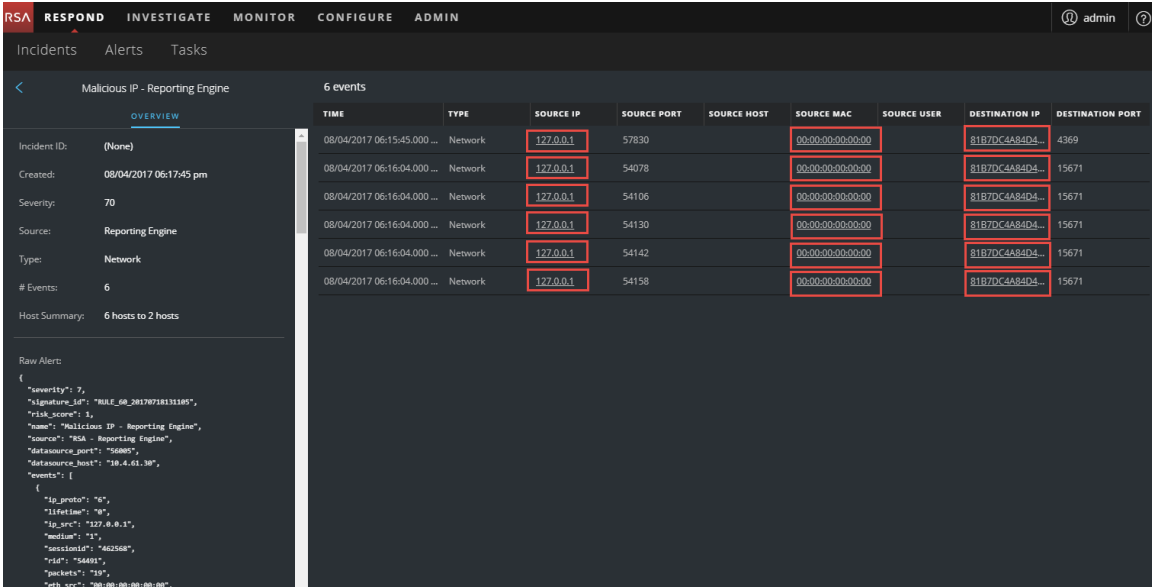
See [Alert Details View](#) for detailed information about the event data listed in the Alert Details panel.

Investigate Events

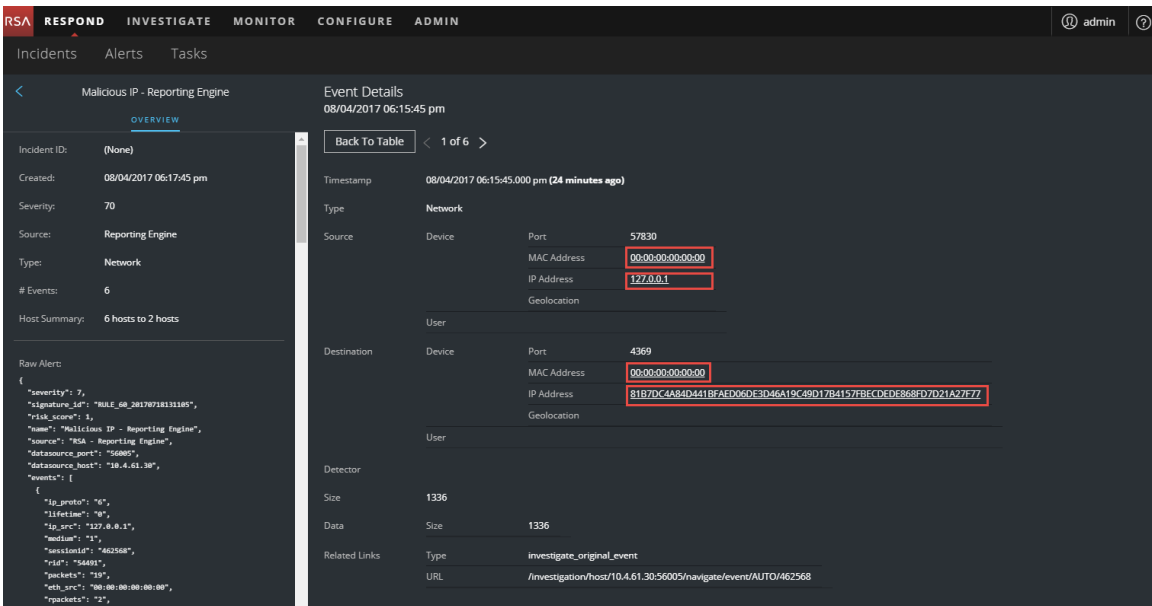
To further investigate the events, you can find links that take you to additional contextual information. From there, you have options available depending on your selection.

View Contextual Information

In the Alert Details view, you can see underlined entities in the Events panel. An underlined entity is considered an entity in the Context Hub and has additional contextual information available. The following figure shows underlined entities in the Events list.



The following figure shows underlined entities in the Events Details.

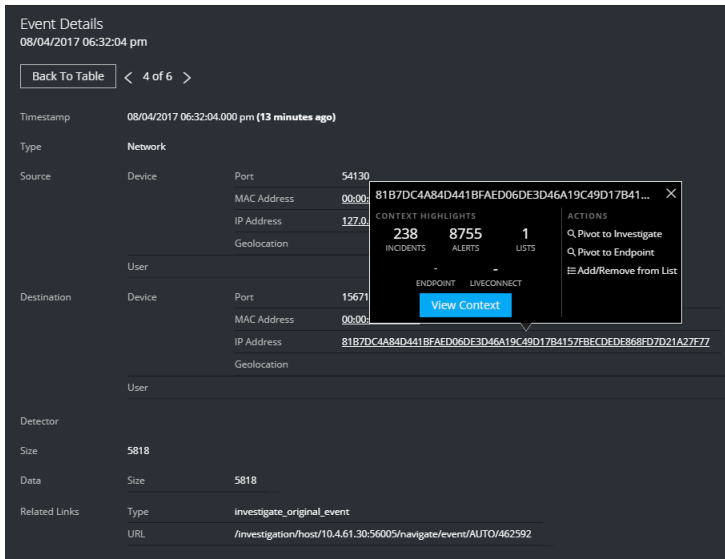


The Context Hub is preconfigured with meta fields mapped to the entities. NetWitness Respond and Investigation use these default mappings for context lookup. For information about adding meta keys, see "Configure Settings for a Data Source" in the *Context Hub Configuration Guide*.

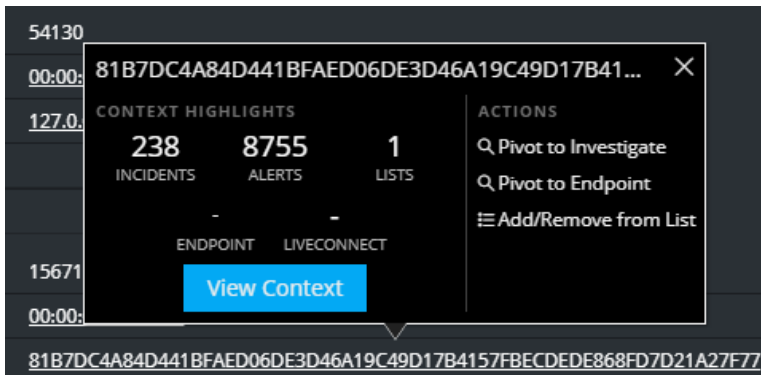
Caution: For the Context Lookup to work correctly in the Respond and Investigate views, RSA recommends that when mapping meta keys in the **ADMIN > SYSTEM > Investigations > Context Lookup** tab, you add only meta keys to the Meta Key Mappings, not fields in the MongoDB. For example, ip.address is a meta key and ip_address is not a meta key (it is a field in the MongoDB).

To View Contextual Information:

1. In the Alert Details view Events List or Event Details, hover over an underlined entity. A context tooltip appears with a quick summary of the type of context data that is available for the selected entity.



The context tooltip has two sections: Context Highlights and Actions.



The information in the **Context Highlights** section helps you to determine the actions that you would like to take. It shows the number of related alerts and incidents. Depending on your data, you may be able to click these numbered items for more information. The above example shows 238 related incidents, and 8,755 related alerts, and 1 related context hub list.

The **Actions** section lists the available actions. In the above example, the Pivot to Investigate, Pivot to Endpoint, and Add/Remove From List options are available.

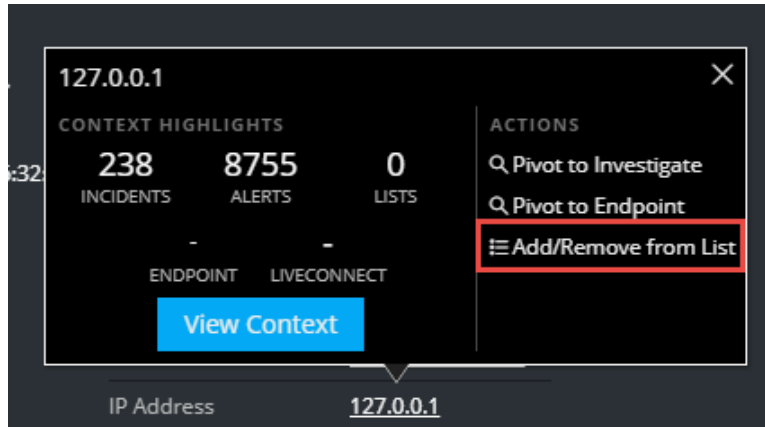
2. To see more details about the selected entity, click the **View Context** button. The Context panel opens and shows all of the information related to the entity. [Context Lookup Panel - Respond View](#) provides additional information.

Add an Entity to a Whitelist

You can add any underlined entity to a list, such as a Whitelist or Blacklist, from a context tooltip. For example, to reduce false positives, you may want to whitelist an underlined domain to exclude it from the related entities.

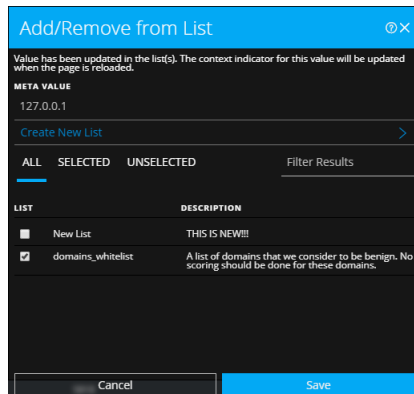
1. In the Alert Details view Events List or Event Details, hover over the underlined entity that you would like to add to a Context Hub list.

A context tooltip appears showing the available actions.



2. In the **Actions** section of the tooltip, click **Add/Remove from List**.

The Add/Remove From List dialog shows the available lists.



3. Select one or more lists and click **Save**.

The entity appears on the selected lists.

[Add/Remove from List Dialog](#) provides additional information.

Create a Whitelist

You can create a whitelist in the Context Hub in the same way as you would create it in the Incident Details view, see [Create a List](#).

Pivot to NetWitness Endpoint

If you have the NetWitness Endpoint thick client application installed, you can launch it through the context tooltip. From there, you can further investigate a suspicious IP address, Host, or MAC address.

1. In the Events List or Event Details in the Alert Details view, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Endpoint**.

The NetWitness Endpoint thick client application opens outside of your web browser.

For more information on the thick client, see the *NetWitness Endpoint User Guide*.

Pivot to Investigation

For a more thorough investigation of the incident, you can access the Investigate view.

1. In the Events List or Event Details in the Alert Details view, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Investigate**.

The Investigate Navigate view opens, which enables you to perform a deeper dive investigation.

For more information, see the *NetWitness Investigate User Guide*.

Create an Incident Manually

You can create incidents manually from alerts in the Alerts List view. The alerts that you select cannot be part of another incident. Incidents created manually from alerts default to Low priority, but you can change the priority after you create it. You cannot add categories to manually created incidents.

Note: Incidents can be created manually or automatically. An Alert can only be associated with one Incident. You can create incident rules to analyze the alerts collected and group them into incidents depending on which rules they match. For details, see the "Create an Incident Rule for Alerts" topic in the *NetWitness Respond Configuration Guide*.

To Create an Incident Manually:

1. Go to **RESPOND > Alerts**.
2. Select one or more alerts in the Alerts List.

Note: Selecting alerts that do not have incident IDs enable the **Create Incident** button. If the alert is already part of an incident, the button is disabled. You can filter alerts that are not part of an incident by selecting the option **PART OF INCIDENT** as **No** in the Filters panel.

	CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID
<input checked="" type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 16 hosts	
<input checked="" type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	22 hosts to 20 hosts	
<input checked="" type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	22 hosts to 17 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	23 hosts to 20 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	19 hosts to 16 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	17 hosts to 13 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	21 hosts to 17 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 15 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	26 hosts to 21 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	20 hosts to 19 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 14 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	20 hosts to 19 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 17 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	22 hosts to 21 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	19 hosts to 19 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	20 hosts to 18 hosts	

Showing 543 out of 543 items | 3 selected

3. Click **Create Incident**.

The **Create Incident** dialog is displayed.

Create Incident
✕

An incident will be created from the selected 3 alert(s). Please provide a name for the incident.

INCIDENT NAME

Investigate - IP

Cancel
OK

4. In the **INCIDENT NAME** field, type a name to identify the incident. For example, Investigate - IP.

5. Click **OK**.

The screenshot shows the NetWitness Respond interface. At the top, there are navigation tabs: RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. A green notification box at the top center says: "You successfully created the incident INC-12011 from the selected alerts. The incident's priority has been set to LOW by default." Below this, there are buttons for "Create Incident", "Add to Incident", and "Delete". The main area is a table of alerts with columns: CREATED, SEVERITY, NAME, SOURCE, # EVENTS, HOST SUMMARY, and INCIDENT ID. Three rows are selected, each with a checkbox checked and a link in the INCIDENT ID column. At the bottom of the table, it says "Showing 543 out of 543 items" and "3 selected".

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID	
<input checked="" type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 16 hosts	INC-12011
<input checked="" type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	22 hosts to 20 hosts	INC-12011
<input checked="" type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	22 hosts to 17 hosts	INC-12011
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	23 hosts to 20 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	19 hosts to 16 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	17 hosts to 13 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	21 hosts to 17 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 15 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	26 hosts to 21 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	20 hosts to 19 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 14 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	20 hosts to 19 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 17 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	22 hosts to 21 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	19 hosts to 19 hosts	
<input type="checkbox"/>	10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	20 hosts to 18 hosts	

You will see a confirmation message that an incident was created from the selected alerts. The new incident ID appears as a link in the INCIDENT ID column of the selected alerts. If you click the link, it takes you to the Incident Details view for that incident, where you can update information, such as changing Priority from low to high.

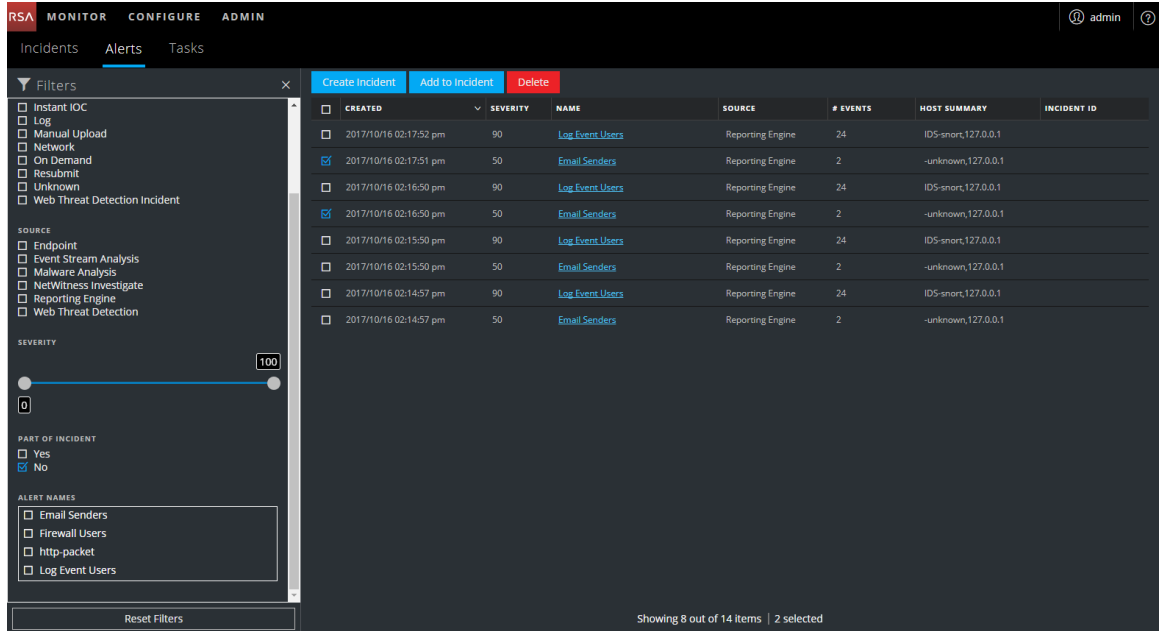
Add Alerts to an Incident

Note: This option is available in version 11.1 and later.

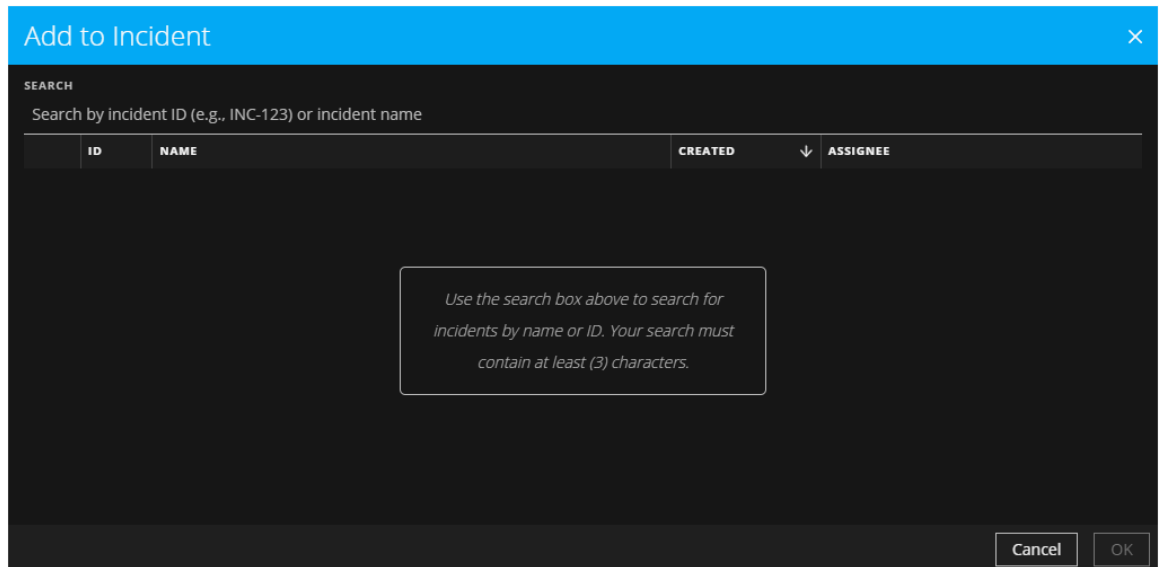
If you have alerts that fit a particular existing incident, you do not have to create a new incident. Instead, you can add alerts to that incident from the Alerts List view. The alerts that you select cannot be part of another incident.

1. Go to **RESPOND > Alerts**.
2. In the Alerts List, select one or more alerts that you want to add to an incident, and click **Add to Incident**.

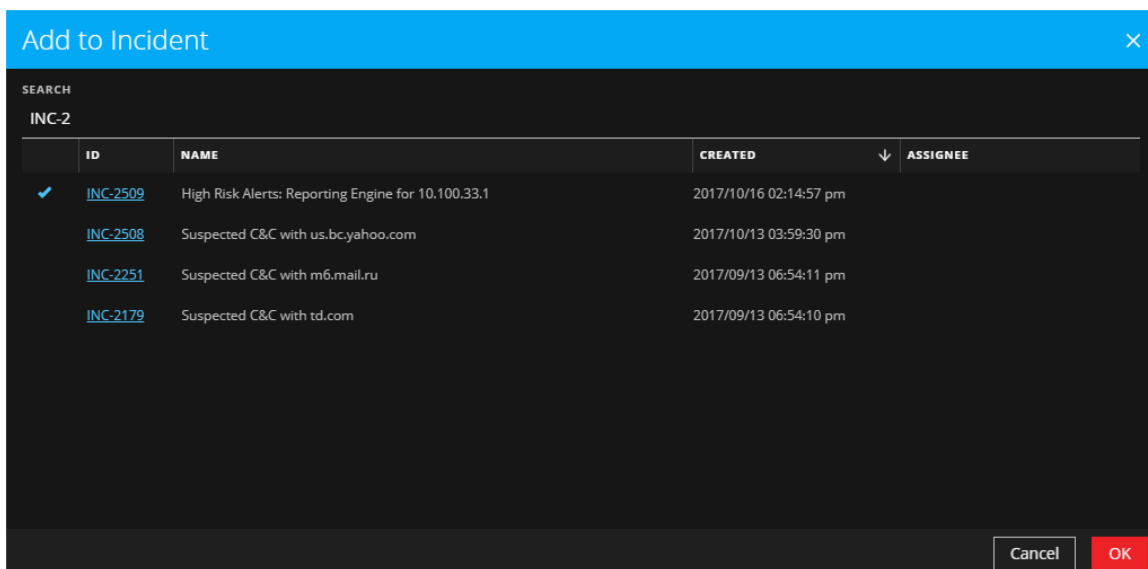
Note: Selecting alerts that do not have incident IDs enable the **Add to Incident** button. If the alert is already part of an incident, the button is disabled. You can filter alerts that are not part of an incident by selecting the option **PART OF INCIDENT** as **No** in the Filters panel.



3. In the **Add to Incident** dialog, type at least three characters in the **Search** field to search for the incident by **Name** or **Incident ID**.



4. In the results list, select the incident that will receive the selected alerts and click **OK**.



The selected alert or alerts are now part of the selected incident and will have that incident ID.

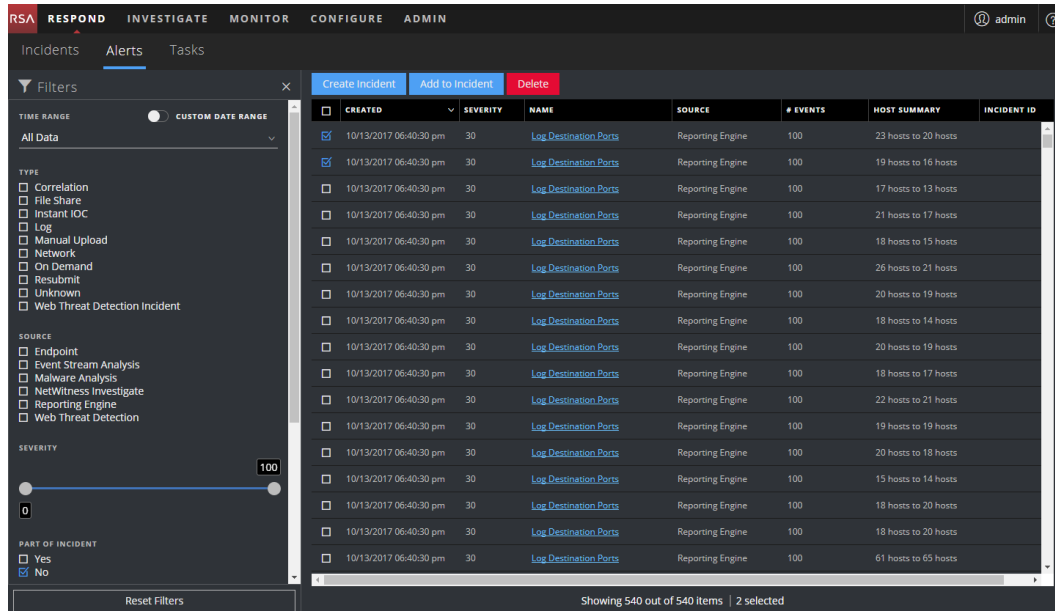
Delete Alerts

Users with the appropriate permissions, such as Administrators and Data Privacy Officers, can delete alerts. This procedure is helpful when you want to remove unnecessary or non-relevant alerts. Deleting these alerts frees up disk space.

1. Go to **RESPOND > Alerts**.

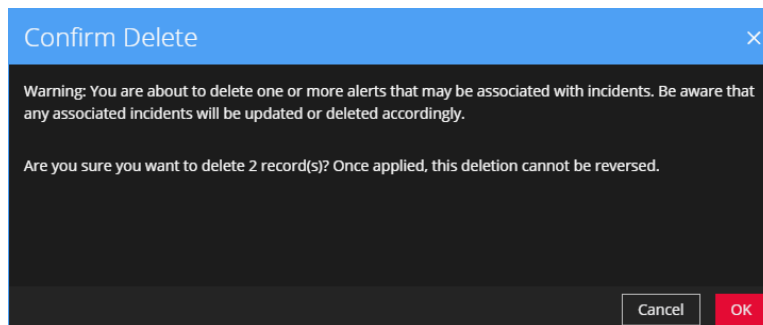
The Alerts List view displays a list of all NetWitness Suite alerts.

- In the Alerts list, select the alerts that you want to delete and click **Delete**.



If you do not have permission to delete alerts, you will not see the Delete button.

- Confirm that you want to delete the alerts and click **OK**.



The alerts are deleted from NetWitness Suite. If a deleted alert is the only alert in an incident, the incident is also deleted. If the deleted alert is not the only alert in an incident, the incident is updated to reflect the deletion.

NetWitness Respond Reference Information

The Respond view user interface provides access to NetWitness Respond functions. This topic contains descriptions of the user interfaces as well as other reference information to help users understand the functions of NetWitness Respond.

Topics

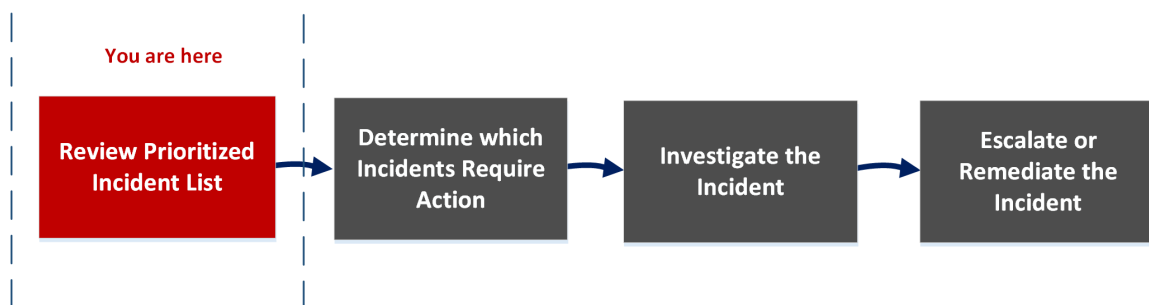
- [Incidents List View](#)
- [Incident Details View](#)
- [Alerts List View](#)
- [Alert Details View](#)
- [Tasks List View](#)
- [Add/Remove from List Dialog](#)
- [Context Lookup Panel - Respond View](#)

Incidents List View

The Incidents List view (RESPOND > Incidents) shows Incident Responders and other Analysts a prioritized results list of incidents created from various sources. For example, your results list could show incidents created from ESA rules, NetWitness Endpoint, or ESA Analytics modules for Automated Threat Detection, such as C2 for packets or logs. From the Incidents List view, you have easy access to the information that you need to quickly triage and manage incidents through completion.

Workflow

This workflow shows the high-level process that Incident Responders use to respond to incidents in NetWitness Suite.



In the Incidents List view, you can review the list of prioritized incidents, which shows basic information about each incident. You can also change the assignee, priority, and status of the incidents. Because the results can be large in the incidents list, you have the option to filter those incidents by time range, incident ID, custom date range, priority, status, assignee, and categories.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts, and SOC Manager	View prioritized incidents*	Review Prioritized Incident List
Incident Responders, Analysts, and SOC Manager	Filter and sort the incident list*	Filter the Incident List
Incident Responders, Analysts	View my incidents*	View My Incidents
Incident Responders, Analysts	Assign incidents to myself*	Assign Incidents to Myself
Incident Responders, Analysts, and SOC Manager	Find Incidents*	Find an Incident
Incident Responders, Analysts, and SOC Manager	Update an incident.*	Escalate or Remediate the Incident
Incident Responders, Analysts	View incident details.	Determine which Incidents Require Action
Incident Responders, Analysts	Further Investigate an incident.	Investigate the Incident
Incident Responders, Analysts, and SOC Manager	Create a task.	Escalate or Remediate the Incident

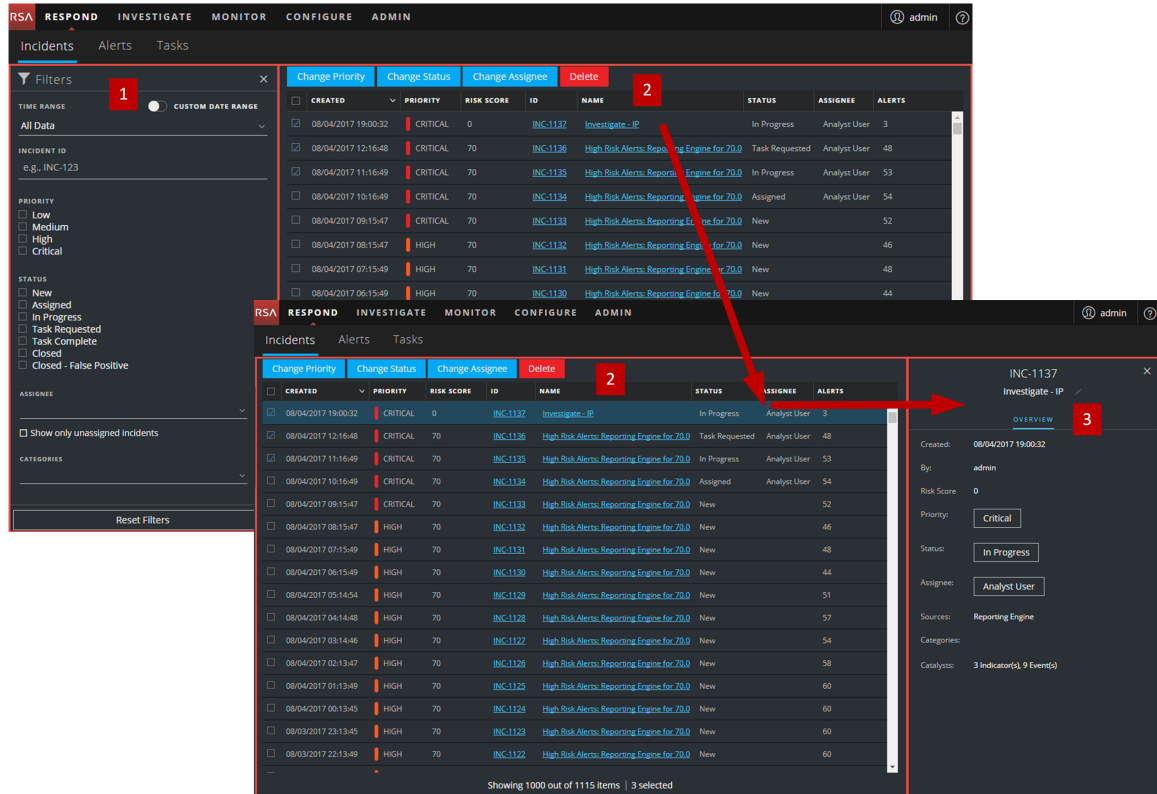
*You can complete these tasks here (that is in the Incidents List view).

Related Topics

- [Incident Details View](#)
- [Responding to Incidents](#)

Quick Look

The following example shows the initial Incidents List view with the Filter panel. You can open the Overview panel for an incident by clicking an incident in the Incident List.



- 1 Filters Panel
- 2 Incidents List
- 3 Overview Panel

You can go directly to the Incident Details view from the Incidents List by clicking the hyperlinked ID or NAME. The Overview panel is also available in the Incident Details view. For more information about the Incidents Details view, see [Incident Details View](#).

Incidents List View

To access the Incidents List view, go to **RESPOND > Incidents**. The Incidents List view displays a list of all incidents. The Incidents List view consists of a Filters panel, an Incidents List, and an Incidents Overview panel.

The following figure shows the Filter Panel on the left and the Incidents List on the right.

The screenshot displays the NetWitness Respond interface. On the left, the 'Incidents' panel is active, showing a list of incidents with columns for Created, Priority, Risk Score, ID, Name, Status, Assignee, and Alerts. The list includes incidents such as 'Suspected C&C with mail.ly.it', 'High Risk Alerts: ESA for 70.0', and 'Test Rule for http-log'. The right panel shows the 'Incidents Overview' for incident INC-2711, detailing its creation time, rule, risk score, priority, status, assignee, sources, categories, and catalysts.

Created	Priority	Risk Score	ID	Name	Status	Assignee	Alerts
2017/10/17 20:15...	HIGH	80	INC-2711	Suspected C&C with mail.ly.it	New		75737
2017/10/17 15:09...	HIGH	70	INC-2514	High Risk Alerts: ESA for 70.0	New		8878
2017/10/17 15:24...	HIGH	70	INC-2588	High Risk Alerts: ESA for 70.0	New		2245
2017/10/17 15:14...	HIGH	70	INC-2580	High Risk Alerts: ESA for 70.0	New		2040
2017/10/17 19:09...	CRITICAL	70	INC-2594	Test 1000 Incidents	Task Requested	deploy_ad...	1003
2017/10/17 15:58...	LOW	70	INC-2592	MANUALLY CREATED INCIDENT!@#...	New		1001
2017/10/17 14:33...	HIGH	80	INC-2513	Suspected C&C with us.bc.yahoo.com	New		1001
2017/10/25 15:28...	HIGH	70	INC-198902	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:28...	HIGH	70	INC-198900	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:28...	HIGH	70	INC-198898	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:28...	HIGH	70	INC-198889	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:27...	HIGH	70	INC-198887	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:27...	HIGH	70	INC-198885	Test Rule for ESA-IP source exists	New		1000
2017/10/24 22:35...	HIGH	80	INC-43642	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43641	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43640	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43639	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43638	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43637	Test Rule for http-log	New		1000
2017/10/24 22:34...	HIGH	80	INC-43636	Test Rule for http-log	New		1000

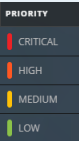
The following figure shows the Incidents List on the left and the Incidents Overview panel on the right.

This screenshot is similar to the one above, showing the NetWitness Respond interface. The 'Incidents' panel on the left displays a list of incidents. The 'Incidents Overview' panel on the right provides detailed information for incident INC-2711, including its creation time, rule, risk score, priority, status, assignee, sources, categories, and catalysts.

Created	Priority	Risk Score	ID	Name	Status	Assignee	Alerts
2017/10/17 20:15...	HIGH	80	INC-2711	Suspected C&C with mail.ly.it	New		75737
2017/10/17 15:09...	HIGH	70	INC-2514	High Risk Alerts: ESA for 70.0	New		8878
2017/10/17 15:24...	HIGH	70	INC-2588	High Risk Alerts: ESA for 70.0	New		2245
2017/10/17 15:14...	HIGH	70	INC-2580	High Risk Alerts: ESA for 70.0	New		2040
2017/10/17 19:09...	CRITICAL	70	INC-2594	Test 1000 Incidents	Task Requested	deploy_ad...	1003
2017/10/17 15:58...	LOW	70	INC-2592	MANUALLY CREATED INCIDENT!@#...	New		1001
2017/10/17 14:33...	HIGH	80	INC-2513	Suspected C&C with us.bc.yahoo.com	New		1001
2017/10/25 15:28...	HIGH	70	INC-198902	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:28...	HIGH	70	INC-198900	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:28...	HIGH	70	INC-198898	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:28...	HIGH	70	INC-198889	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:27...	HIGH	70	INC-198887	Test Rule for ESA-IP source exists	New		1000
2017/10/25 15:27...	HIGH	70	INC-198885	Test Rule for ESA-IP source exists	New		1000
2017/10/24 22:35...	HIGH	80	INC-43642	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43641	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43640	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43639	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43638	Test Rule for http-log	New		1000
2017/10/24 22:35...	HIGH	80	INC-43637	Test Rule for http-log	New		1000
2017/10/24 22:34...	HIGH	80	INC-43636	Test Rule for http-log	New		1000

Incidents List

The Incidents List shows a list of all of the prioritized incidents. You can filter this list to show only incidents of interest.

Column	Description
CREATED	Shows the creation date of the incident.
PRIORITY	Shows the incident priority. Priority can be Critical, High, Medium or Low. The Priority is color coded, where red indicates a Critical incident, orange represents a High risk incident, yellow indicates a Medium risk incident, and green represents a Low risk incident. For example: 
RISK SCORE	Shows the incident risk score. The risk score indicates the risk of the incident as calculated via an algorithm and is between 0-100. 100 is the highest risk score.
ID	Shows the automatically created incident number. Each incident is assigned a unique number that you can use to track the incident.
NAME	Shows the incident name. The incident name is derived from the rule used to trigger the incident. Click the link to go to the Incident Details view for the selected incident.
STATUS	Shows the incident status. The status can be: New, Assigned, In Progress, Task Requested, Task Complete, Closed, and Closed-False Positive.
ASSIGNEE	Shows the team member currently assigned to the incident.
ALERTS	Shows the number of alerts associated with the incident. An incident may include many alerts. A large number of alerts might mean that you are experiencing a large-scale attack.

At the bottom of the list, you can see the number of incidents on the current page, the total number of incidents, and the number of incidents selected. For example: **Showing 1000 out of 2517 items | 2 selected**. The maximum number of incidents that you can view at one time is 1,000.

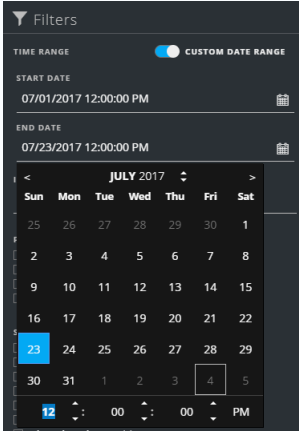
Filters Panel

The following figure shows the filters available in the Filters panel.

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

- TIME RANGE**: Includes a toggle switch for 'CUSTOM DATE RANGE'.
- All Data**: A dropdown menu.
- 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.
- Show only unassigned incidents**: A checkbox.
- CATEGORIES**: A dropdown menu.
- Reset Filters**: A button at the bottom of the panel.

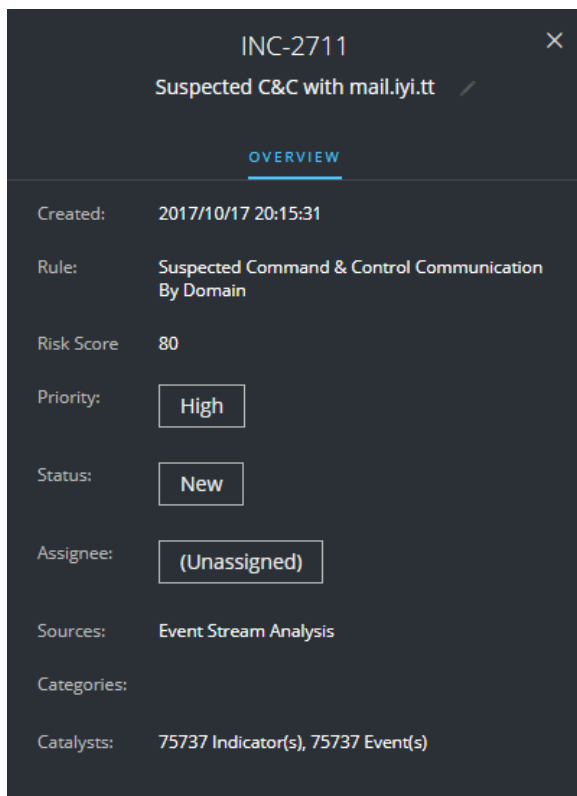
The Filters panel, on the left of the Incidents List view, has options that you can use to filter the incidents list. When you navigate away from the Filters panel, the Incidents List view retains your filter selections.

Option	Description
TIME RANGE	You can select a specific time period from the Time Range drop-down list. The time range is based on the received date of the alerts. For example, if you select Last Hour, you will see alerts that were received within the last 60 minutes.
CUSTOM DATE RANGE	<p>You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to view the Start Date and End Date fields. Select the dates and times from the calendar.</p> 
INCIDENT ID	You can type the Incident ID for an incident you would like to locate, for example INC-1050.
PRIORITY	Select the priorities that you would like to view.
STATUS	Select one or more incident statuses. For example, select Closed - False Positive to view only false positive incidents, which were initially identified as suspicious, but then they were later found to be safe.

Option	Description
ASSIGNEE	Select the assignee or assignees of the incidents that you would like to view. For example, if you only want to view the incidents assigned to Cale or Stanley, select Cale and Stanley from the Assignee drop-down list. If you want to view incidents regardless of the assignee, do not make a selection under Assignee. (Available in version 11.1 and Later) To view only unassigned incidents, select Show only unassigned incidents .
CATEGORIES	Select one or more categories from the drop-down list. For example, if you only want to view incidents classified with the Backdoor or Privilege abuse categories, select Backdoor and Privilege abuse.
Reset Filters	Removes your filter selections.

Overview Panel

The Overview panel shows basic summary information about a selected incident. From the Incidents List, you can click an incident to access the Overview panel. The Overview panel in the Incident Details view contains the same information.





The following table lists the fields displayed in the Incident Overview panel.

Field	Description
<Incident ID>	Displays the Incident ID.
<Incident Name>	Displays the name of the incident. You can click the incident name to change it. For example, rules can create many incidents with the same name. You can change the incident names to be more specific.
Created	Shows the creation date and time of the incident.
Rule / By	Shows the name of the rule that created the incident or the name of the person who created the incident.
RiskScore	Indicates the risk of the incident as calculated via an algorithm and is between 0-100. 100 is the highest risk score.
Priority	Shows the incident priority. Priority can be Critical, High, Medium or Low. To change the priority, you can click the Priority button and select a new priority from the drop-down list.
Status	Shows the incident status. The status can be New, Assigned, In Progress, Task Requested, Task Complete, Closed, and Closed - False Positive. To change the status, you can click the Status button and select a new status from the drop-down list.
Assignee	Shows the team member currently assigned to the incident. To change the assignee you can click the Assignee button and select a new assignee from the drop-down list.
Sources	Displays the data sources used to locate the suspicious activity.
Categories	Displays the categories of the incident events.
Catalysts	Displays the count of indicators that gave rise to the incident.

Toolbar Actions

This table lists the toolbar actions available in the Incidents List view.

Option	Description
	Enables you to open the Filters panel so that you can specify the alerts that you would like to see in the Alerts List.
	Closes the panel.
Change Priority button	Allows you to change the Priority of one or more selected incidents in the Incidents List.
Change Status button	Allows you to change the Status of one or more selected incidents.
Change Assignee button	Allows you to change the Assignee of one or more selected incidents.
Delete button	Allows you to delete the selected incidents if you have the appropriate permissions, such as an Administrator or Data Privacy Officer.

Incident Details View

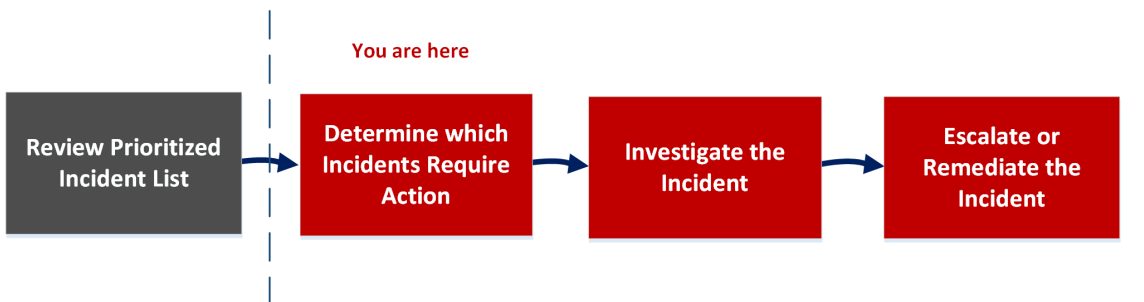
In the Incident Details view (RESPOND > Incidents > click an ID or NAME hyperlink in the Incidents List), you can view and access extensive incident details. The Incident Details view contains multiple panels that provide the following benefits:

- **Overview:** View an incident summary and update the incident.
- **Indicators:** View the indicators (alerts) involved in the incident, the events within those alerts, and available enrichment information.
- **Nodal Graph:** Visualize the size and interactions between entities (IP address, MAC address, user, host, domain, file name, or file hash).
- **Events Datasheet:** Study the events associated with the incident.
- **Journal:** Add notes and collaborate with other analysts.
- **Tasks:** Create incident tasks and track them to closure.
- **Related Indicators:** View indicators (alerts) that are related to the incident and add them to the incident if they are not associated with an incident.

You can also filter the data in the Incident Details view to study indicators and entities of interest.

Workflow

This workflow shows the high-level process that Incident Responders use to respond to incidents in NetWitness Suite.



In the Incident Details view, you can use the extensive information provided about the incidents to determine which incidents require action. You also have the tools and information to investigate the incident, and then escalate or remediate it.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts, and SOC Manager	View prioritized incidents, filter and sort the incident list, find incidents, view my incidents, and assign incidents to myself.	Review Prioritized Incident List
Incident Responders, Analysts	View incident details.*	View Incident Details
Incident Responders, Analysts	View alerts and enrichments.*	View the Indicators and Enrichments
Incident Responders, Analysts	View events.*	View and Study the Events
Incident Responders, Analysts	View a graph of the entities involved in the events.*	View and Study the Entities Involved in the Events
Incident Responders, Analysts	Filter the incident data.*	Filter the Data in the Incident Details View
Incident Responders, Analysts	View and add incident notes.*	View Incident Notes and Document Steps Taken Outside of NetWitness
Incident Responders, Analysts	View and create tasks.*	View the Tasks associated with an Incident and Create a Task
Incident Responders, Analysts	Add related alerts and add them to the incident.*	Find Related Indicators and Add Related Indicators to the Incident
Incident Responders, Analysts	View contextual information about an incident from Context Hub.*	View Contextual Information

Role	I want to ...	Show me how
Incident Responders, Analysts	Reduce false positives by adding an entity to the whitelist.*	Add an Entity to a Whitelist
Incident Responders, Analysts	Pivot to Investigation.*	Pivot to Investigate
Incident Responders, Analysts	Pivot to NetWitness Endpoint.*	Pivot to NetWitness Endpoint
Incident Responders, Analysts	Update or close an incident.*	Update an Incident and Close an Incident
Incident Responders, Analysts, and SOC Manager	View all tasks.	Escalate or Remediate the Incident
Incident Responders, Analysts, and SOC Manager	Bulk update incidents and tasks.	Escalate or Remediate the Incident

*You can complete these tasks here (that is in the Incident Details view).

Related Topics

- [Incidents List View](#)
- [Determine which Incidents Require Action](#)
- [Investigate the Incident](#)
- [Escalate or Remediate the Incident](#)

Quick Look

The following example shows the locations of the Incident Details view panels.

The screenshot shows the NetWitness Respond interface with several panels highlighted by red boxes and numbers:

- 1**: Overview Panel (Click the OVERVIEW tab to view it.)
- 2**: Indicators Panel
- 3**: Nodal Graph
- 5**: Journal Panel
- 6**: Tasks Panel (Click the TASKS tab to view it.)

This section shows the Events Datasheet (4) and Event Details view:

TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION PORT	DESTINATION HOST	DESTINATION MAC	DESTINATION USER
07/21/2017 20:18:36.000	Network		40232	00:00:00:00:00:00	E1B7DC448BD4-4399		E1B7DC448BD4-4399				
07/21/2017 20:19:36.000	Network		42259	00:00:00:00:00:00	E1B7DC448BD4-4399		E1B7DC448BD4-4399				
07/21/2017 20:20:36.000	Network		33233	00:00:00:00:00:00	E1B7DC448BD4-4399		E1B7DC448BD4-4399				
07/21/2017 20:21:06.000	Network		56650	00:00:27:26:dff1	02124FB8B51-80		02124FB8B51-80				
07/21/2017 20:21:36.000	Network		42372	00:00:00:00:00:00	E1B7DC448BD4-4399		E1B7DC448BD4-4399				
07/21/2017 20:22:36.000	Network		39773	00:00:00:00:00:00	E1B7DC448BD4-4399		E1B7DC448BD4-4399				

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

- 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: [Redacted]
- Destination: Device, Port: 4399, MAC Address: 00:00:00:00:00:00, IP Address: E1B7DC448BD41BFAED90E3D46A19...69D17841578BC, COLDEMBID7021542977, Geolocation: [Redacted]
- User: [Redacted]
- Detector: [Redacted]
- Size: 1410
- Data: Size: 1410
- Related Links: Type: Investigate_original_event, URL: Investigate/host/10.4.61.30:50005/investigaterevents/AUTO/20741

This section shows the Tasks Panel (6) and Related Indicators Panel (7):

Tasks Panel (6):

- REM-2 / INC-628**: Create replacement host ASAP. Assignee: ITServics. Priority: Critical. Status: Risk Accepted. Description: Re-image a host to use for replacement.
- REM-1 / INC-628**: Isolate host. Assignee: DScience. Priority: High. Status: New. Description: Isolate the host for further study.

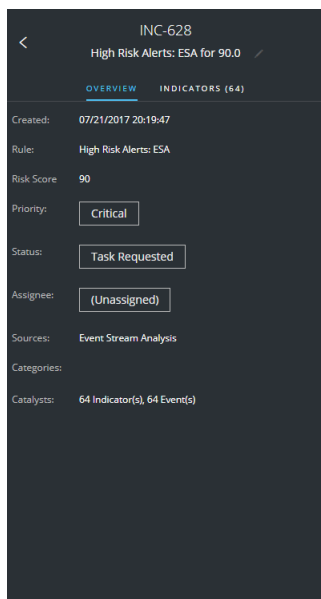
Related Indicators Panel (7):

Find: MAC. Value: 52:54:00:12:35:02. When: All Data. Look in: Source, Destination, Detector. Indicators for MAC: 52:54:00:12:35:02. All Data - Destination. Event Stream Analysis 07/21/2017 20:17:11. Test 90 1 event. Part of Incident: INC-627. Open in new window. Event Stream Analysis 07/21/2017 20:22:11. Test 90 1 event. Part of This Incident. Open in new window. Event Stream Analysis 07/21/2017 20:27:12. Test 90 1 event. Open in new window.

- 1 Overview Panel (Click the OVERVIEW tab to view it.)
- 2 Indicators Panel
- 3 Nodal Graph
- 4 Events Datasheet (Click an event in the Events List to view Event Details.).
- 5 Journal Panel
- 6 Tasks Panel (Click the TASKS tab to view it.)
- 7 Related Indicators Panel (Click the RELATED tab to view it.)

Overview Panel

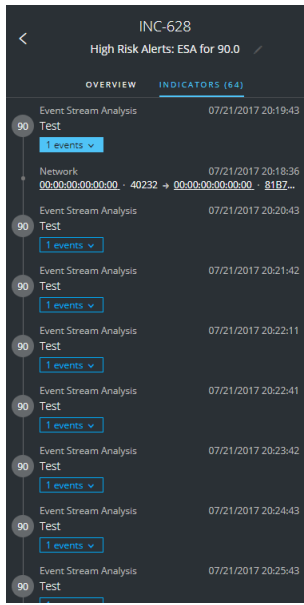
The Overview panel shows basic summary information about a selected incident. It also allows you to change the incident name and update the incident priority, status, and assignee. The Overview panel in the Incidents List view contains the same information. The Incidents List view [Overview Panel](#) topic provides details.



Indicators Panel

The Indicators panel contains a chronological listing of indicators. *Indicators* are alerts, such as an ESA alert or a NetWitness Endpoint alert. (This is different than a timeline, which provides a visual representation of the timing of the events in the incident). This listing helps you to connect indicators and notable data. For example, an IP address connected to a command and communication ESA alert might also have triggered a NetWitness Endpoint alert or other suspicious activities.

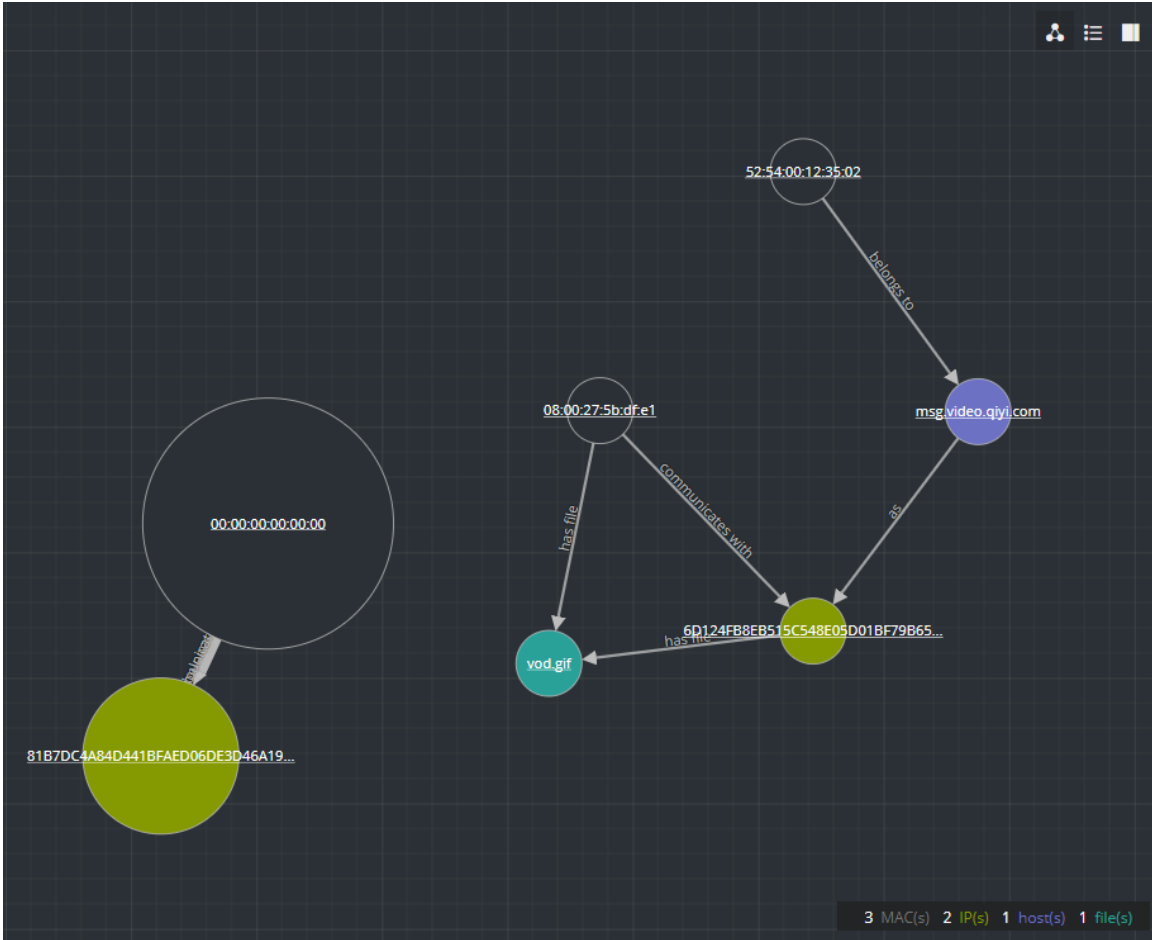
To view the Indicators panel, in the left panel of the Incident Details view, select **INDICATORS**.



Data source information is shown below the names of the indicators. You can also see the creation date and time of the indicator and the number of events in the indicator.

Nodal Graph

The nodal graph is an interactive graph that shows the entities involved in the incident. An *Entity* is a specified piece of meta, such as IP address, MAC address, user, host, domain, file name, or file hash.



Nodes

In the nodal graph, circles represent nodes. The following table describes the nodal graph node types.

Node	Description
IP address	If the event is a detected anomaly, you can see a Detector IP. If the event is a transaction, you can see a Destination IP and a Source IP.
MAC address	You may see a MAC address for each type of IP address.
User	If the machine is associated with a user, you can see a user node.
Host	A host can be physical equipment or a virtual machine, designated by a Fully Qualified Domain Name (FQDN) or IP address, on which any service is installed.

Node	Description
Domain	
Filename	If the event involves files, you can see a filename.
File Hash	If the event involves files, you may see a file hash.

The legend at the bottom of the nodal graph shows the number of nodes of each type and the color coding of the nodes. It also helps you to locate the entities when the values, such as the IP addresses, are hashed.

You can click any node and drag it to reposition it.

Arrows

The arrows between the nodes provide additional information about the entity relationships. The following table describes the nodal graph arrow types.

Arrow	Description
Communicates with	An arrow between a Source machine node (IP address or MAC address) and a Destination machine node labeled with "communicates with" shows the direction of the communication.
As	An arrow between nodes labeled with "as" provides additional information about the IP address that the arrow points to. For example, if there is an arrow from the host node circle that points to an IP address node that is labeled with "as", it indicates that the name on the host node circle is the hostname of that IP address and is not a different entity.
Has file	An Arrow between a machine node (IP address, MAC address, or Host) and a file hash node labeled with "has" indicates that the IP address has that file.
Uses	An arrow between a User node and a machine node (IP address, MAC address, or Host) labeled with "uses" shows the machine that the user was using during the event.
Is named	An arrow from a File Hash node to a File Name node labeled with "is named" indicates that the file hash corresponds to a file with that name.

Arrow	Description
Belongs to	An arrow between two nodes labeled with "belongs to" indicates that they pertain to the same node. For example, an arrow between a MAC address and a Host labeled with "belongs to" indicates that it is the MAC address of the host.

Larger line size arrows indicate more communication between the nodes. Larger nodes (circles) indicate more activity than smaller nodes. The larger nodes are the most common entities mentioned in the events.

Events Datasheet

The Events datasheet shows the events associated with the incident. It shows information about the events, such as event time, source IP, destination IP, detector IP, source user, destination user, and file information about the events. The amount of information listed depends on the event type.

The Events datasheet shows an Events List for multiple events or Event Details for a single event.

Events List

The following figure shows the Events List.

64 events

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		6D124FB8EB51...	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		6D124FB8EB51...	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		6D124FB8EB51...	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

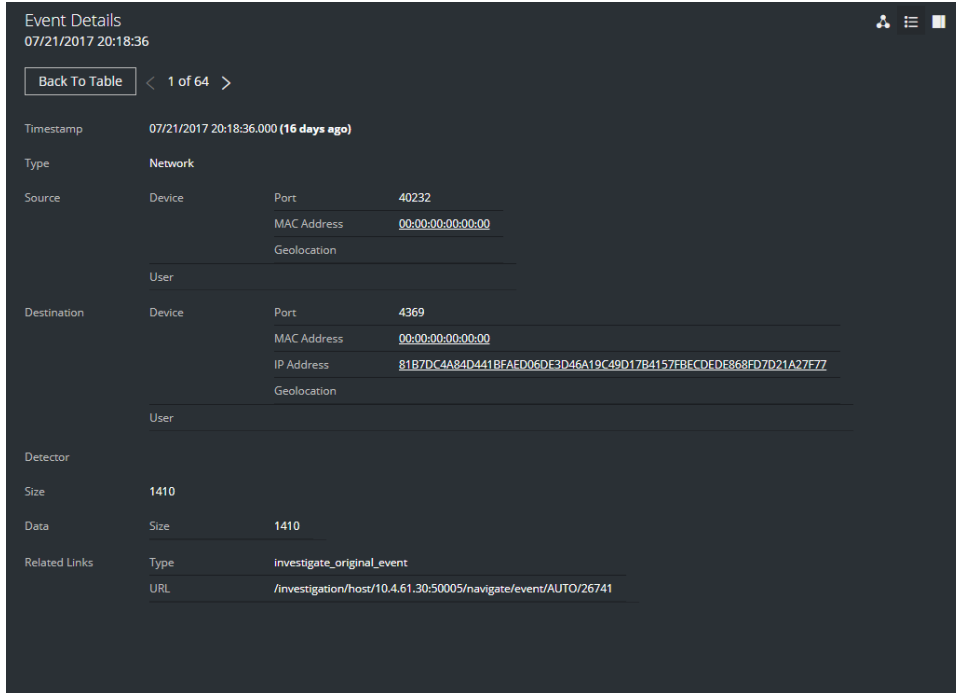
The following table describes the columns in the Events list.

Column	Description
TIME	Shows the time the event occurred.
TYPE	Shows the type of alert, such as Log and Network.
SOURCE IP	Shows the source IP address if there was a transaction between two machines.
SOURCE PORT	Shows the source port of the transaction. The source and destination ports can be on the same IP address.
SOURCE HOST	Shows the destination host where the event took place.
SOURCE MAC	Shows the MAC address of the source machine.
SOURCE USER	Shows the user of the source machine.

Column	Description
DESTINATION IP	Shows the destination IP address if there was a transaction between two machines
DESTINATION PORT	Shows the destination port of the transaction. The source and destination ports can be on the same IP address.
DESTINATION HOST	Shows the HOST name of the destination machine.
DESTINATION MAC	Shows the MAC address of the destination machine.
DESTINATION USER	Shows the user of the destination machine.
DETECTOR IP	Shows the IP address of the machine where an anomaly was detected.
FILE NAME	Shows the file name if a file is involved with the event.
FILE HASH	Shows a hash of the file contents.

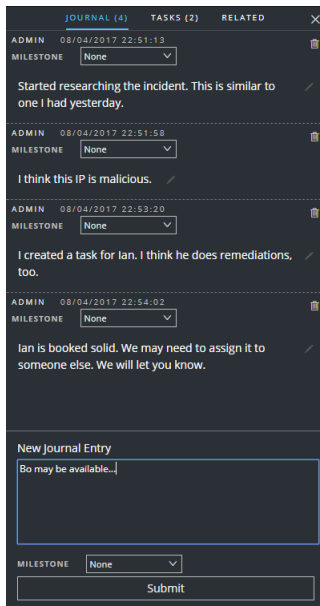
Event Details

To view the event details, you click an event in the event list. If there is only one event in the list, you will see the event details for that event instead of a list.



Journal Panel

The incident Journal shows the history of activity on your incident.

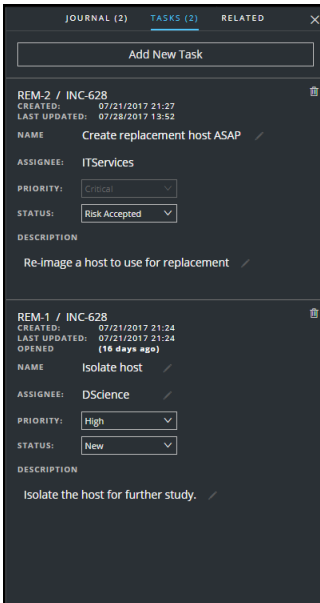


The following table describes the New Journal Entry options.

Field	Description
New Journal Entry	Type your note in the field.
Milestone	(Optional) Select a milestone, if applicable. This field is used to track significant events for the incident.
Submit button	Click submit to add an entry to the journal. Your journal entry will be visible to anyone who views the incident.

Tasks Panel

In the Tasks panel, you can manage and track the incident tasks to closure.



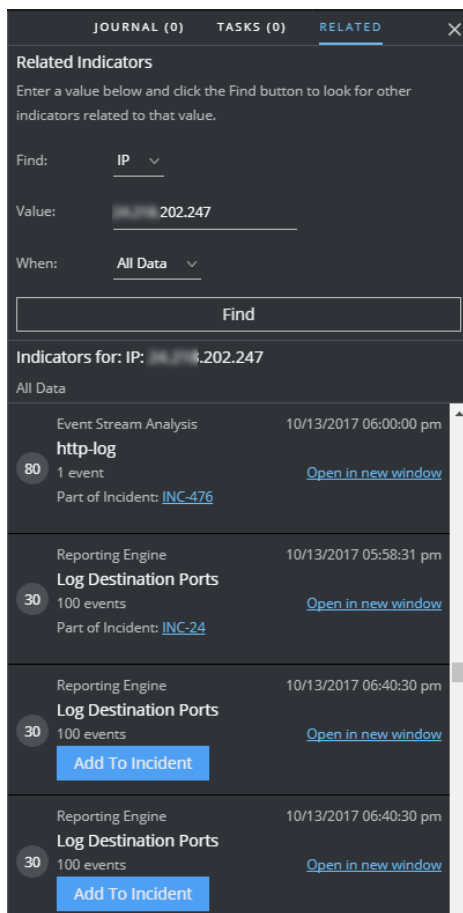
The following table describes the Task fields.

Field	Description
<Task ID / <Incident ID>	The autogenerated Task ID / The incident associated with the task.
CREATED	The created date of the task.
LAST UPDATED	The date that the task was last modified.
OPENED	The time that passed since the task was opened. For example, 3 minutes ago or 2 days ago.

Field	Description
NAME	The name of the task. For example: Re-image the machine. You can click this field to edit it.
ASSIGNEE	The username of the user assigned to the task. You can click this field to edit it.
PRIORITY	The priority of the task: Low, Medium, High, or Critical. You can click the priority button and select a new priority for the task from the drop-down list.
STATUS	The status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable. You can click the status button and select a new status for the task from the drop-down list.
DESCRIPTION	Type information that describes the task. You may want to include any applicable reference numbers. You can click this field to edit it.

Related Indicators Panel

The Related Indicators panel enables you to search the NetWitness Suite alerts database to find alerts that are related to this incident. You can add alerts that you find to the incident if they are not already associated with an incident.



The following table describes the fields in the search section at the top of the panel.





Field	Description
Find	Select the entity that you would like to locate in the alerts. For example, IP.
Value	Type the value of the entity. For example, type the actual IP address of the entity.
When	Select a time range to search for the alerts. For example, Last 24 hours.
Find button	Initiates the search. A list of related indicators appear below the Find button in the Indicators for section.



The following table describes the options in the **Indicators for** (results) section at the bottom of the panel.

Option	Description
Indicators For:	Shows the search results.

Option	Description
Open in new window link	Shows alert details for the indicator.
Add To Incident button	Adds the related indicator to the incident. The related indicator adds to the Indicators panel.
Part Of This Incident button	Shows that the indicator is already part of the incident.

Toolbar Actions

Option	Description
	(Back to Incidents) Enables you to navigate back to the Incidents List view.
	Closes the panel.
	Deletes the entry, such as a journal entry or task.
Priority button	(In the Overview panel) Allows you to change the Priority of one or more selected incidents in the Incidents List.
Status button	(In the Overview panel) Allows you to change the Status of one or more selected incidents.
Assignee button	(In the Overview panel) Allows you to change the Assignee of one or more selected incidents.
	Enables you to view the Nodal Graph.
(View: Graph)	

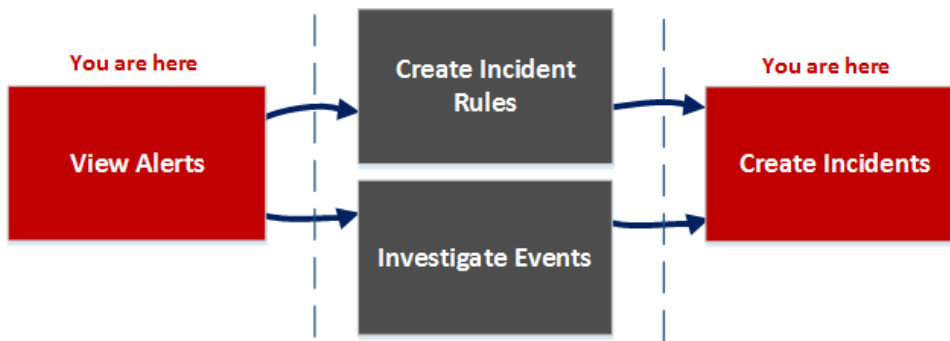
Option	Description
 (View: Datasheet)	Enables you to view the Events datasheet, which can appear as an Events List for multiple events or Event Details for a single event.
 (Journal, Tasks, and Related)	Enables you to view the Journal, Tasks, and Related Indicators panels.

Alerts List View

The Alerts List view (RESPOND > Alerts) enables you to view all of the threat alerts and indicators received by NetWitness Suite in one location. This can include alerts received from ESA Correlation Rules, ESA Analytics, Malware Analysis, Reporting Engine, NetWitness Endpoint, as well as many others. In the Alerts List view you can browse through various alerts, filter them, and group them to create incidents.

Workflow

This workflow shows the high-level process that Analysts use to review alerts and create incidents.



In the Alerts List view, you can review a list of alerts from all sources received by NetWitness Suite. After that, you can investigate those alerts further and create incidents from the alerts or you can create incident rules to create incidents.

Note: You can use NetWitness Suite Automated Threat Detection to create incidents without manually creating rules.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts	View all alerts in NetWitness Suite.*	View Alerts
Incident Responders, Analysts	Filter alerts.*	Filter the Alerts List

Role	I want to ...	Show me how
Incident Responders, Analysts	View alert overview information and raw alert metadata.*	View Alert Summary Information
Incident Responders, Analysts	Create incidents from alerts.*	Create an Incident Manually
Incident Responders, Analysts	(Available in version 11.1 and Later) Add alerts to an existing incident.*	Add Alerts to an Incident
Administrators, Data Privacy Officers	Delete alerts.*	Delete Alerts
SOC Managers, Administrators	Create incident rules.	See "Create an Incident Rule for Alerts" in the <i>NetWitness Respond Configuration Guide</i> .
Incident Responders, Analysts	Investigate the events in an alert.	View Event Details for an Alert and Investigate Events
Incident Responders, Analysts	Add related alerts to an existing incident.	Add Related Indicators to the Incident

*You can complete these tasks here (that is in the Alerts List view).

Related Topics

- [Alert Details View](#)
- [Reviewing Alerts](#)

Alerts List View

To access the Alerts List view, go to **RESPOND > Alerts**. The Alerts List view displays a list of all alerts and indicators received by the Respond Server database in NetWitness Suite. The following figure shows the Filters panel on the left.


The Alerts List view consists of a Filters panel, an Alerts List, and an Alert Overview panel. You can click an alert in the Alerts list to view the Alert Overview panel on the right.

Alerts List

The Alerts List shows all of the alerts in NetWitness Suite. You can filter this list to only show alerts of interest.

Created	Severity	Name	Source	# Events	Host Summary	Incident ID
10/13/2017 06:40:36 pm	30	Email Senders	Reporting Engine	1	--unknown,127.0.0.1	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	16 hosts to 15 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	38	7 hosts to 7 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 16 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	22 hosts to 20 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	22 hosts to 17 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	23 hosts to 20 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	19 hosts to 16 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	17 hosts to 13 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	21 hosts to 17 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 15 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	26 hosts to 21 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	20 hosts to 19 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 14 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	20 hosts to 19 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	18 hosts to 17 hosts	
10/13/2017 06:40:30 pm	30	Log Destination Ports	Reporting Engine	100	22 hosts to 21 hosts	

Showing 546 out of 546 items | 3 selected

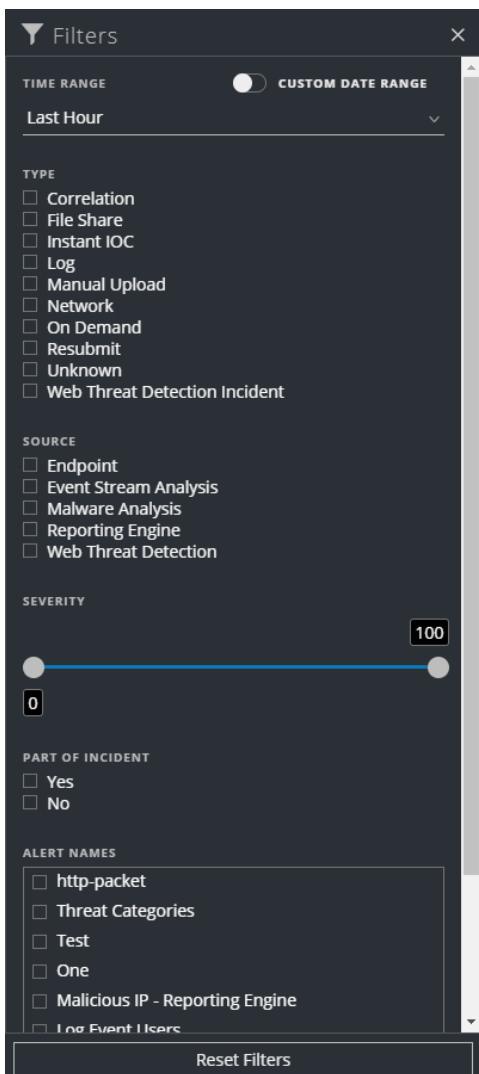
Column	Description
	Enables you to select one or more alerts to delete. Users with the appropriate permissions, such as Administrators and Data Privacy Officers, can delete alerts.
CREATED	Displays the date and time when the alert was recorded in the source system.
SEVERITY	Displays the level of severity of the alert. The values are from 1 through 100.
NAME	Displays a basic description of the alert.
SOURCE	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, ESA correlation rules, ESA Analytics, Reporting Engine, and many others.
# EVENTS	Indicates the number of events contained within an alert. This varies depending on the source of the alert. For example, NetWitness Endpoint and Malware Analysis alerts always have one Event. For certain types of alerts, a high number of events may mean that the alert is more risky.

Column	Description
HOST SUMMARY	Displays details of the host like the host name from where the alert was triggered. The details may include information about the source and destination hosts in an Alert. Some alerts may describe events across more than one host .
INCIDENT ID	Shows the Incident ID of the alert. If there is no incident ID, the alert does not belong to any incident and you can create an incident to include this alert or the alert can be added to an existing incident.

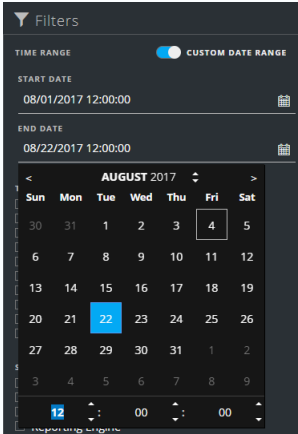
At the bottom of the list, you can see the number of alerts on the current page, the total number of alerts, and the number of alerts selected. For example: **Showing 377 out of 377 items | 3 selected**

Filters Panel

The following figure shows the filters available in the Filters panel.



The Filters panel, on the left of the Alerts List view, has options that you can use to filter the alerts list. When you navigate away from the Filters panel, the Alerts List view retains your filter selections.

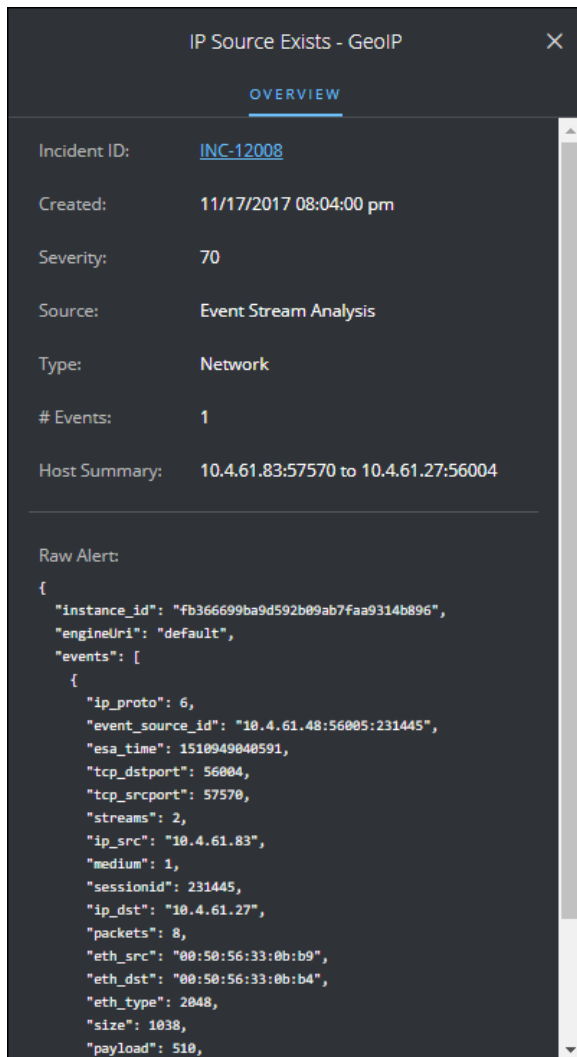
Option	Description
TIME RANGE	You can select a specific time period from the Time Range drop-down list. The time range is based on the received date of the alerts. For example, if you select Last Hour, you will see alerts that were received within the last 60 minutes.
CUSTOM DATE RANGE	<p>You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to view the Start Date and End Date fields. Select the dates and times from the calendar.</p> 
TYPE	Indicates the type of events in the alert, for example, logs, network sessions, and so on.
SOURCE	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, Event Stream Analysis (ESA Correlation Rules), ESA Analytics, Reporting Engine, Web Threat Detection, and many others.
SEVERITY	Displays the level of severity of the alert. The values are from 1 through 100.

Option	Description
PART OF INCIDENT	Categorizes alerts on whether or not they are associated with an incident. Select Yes to view alerts that are part of an incident. Select No to view alerts that are not part of an incident. For example, before you create incidents from alerts, you may want to select No to view only those alerts that are not already part of an incident.
ALERT NAMES	Shows the name of the alert. You can use this filter to search for all alerts generated by a specific rule or source, for example, Malicious IP - Reporting Engine.
Reset Filters	Removes your filter selections.

The Alerts List shows a list of alerts that meet your selection criteria. You can see the number of items in your filtered list at the bottom of the alerts list. For example: **Showing 30 out of 30 items**

Overview Panel

The Overview panel shows basic summary information about a selected alert and raw alert metadata. The Overview panel in the Alert Details view contains the same information, but in the Alerts Details view, you can expand the panel to view more information.





The following table lists the fields displayed in the Alert Overview panel.

Field	Description
<Alert Name>	Displays the name of the alert.
Incident ID	Displays the Incident ID associated with the alert. You can click the incident ID link to go to the Incident Details view of the associated incident. If there is no incident ID, the alert does not belong to an incident. You can create an incident for this alert or you can add it to an incident.
Created	Displays the date and time when the alert was created.

Field	Description
Severity	Displays the level of severity of the alert. The values are from 1 through 100.
Source	Displays the original source of the alert. The source of the alerts can be NetWitness Endpoint, Malware Analysis, ESA correlation rules, ESA Analytics, Reporting Engine, and many others.
Type	Indicates the type of events in the alert, for example, logs, network sessions, and so on.
# Events	Indicates the number of events contained within an alert. This varies depending on the source of the alert. For example, NetWitness Endpoint and Malware Analysis alerts always have one Event. For certain types of alerts, a high number of events may mean that the alert is more risky.
Raw Alert	Shows the raw alert metadata.

Toolbar Actions

This table lists the toolbar actions available in the Alerts List view.

Option	Description
	Enables you to open the Filters panel so that you can specify the alerts that you would like to see in the Alerts List.
	Closes the panel.
Create Incident button	Enables you to create incidents from alerts. The alerts cannot be part of an incident. To get a list of alerts without incidents, you can filter the Alerts List, In the PART OF INCIDENT section, select No.
Add to Incident button	(This option is available in version 11.1 and later.) Enables you to add selected alerts to an incident. The alerts cannot be part of an incident. To get a list of alerts without incidents, you can filter the Alerts List. In the PART OF INCIDENT section, select No.
Delete button	Allows you to delete alerts.

Alert Details View

In the Alert Details view (RESPOND > Alerts > click a NAME hyperlink in the Alerts List), you can view summary information about an alert, such as the source of the alert, the number of events within the alert, and whether it is part of an incident. You can also view detailed information about the events within the alert as well as the event metadata.

Workflow

This workflow shows the high-level process that Analysts use to review alerts and create incidents.



After reviewing the alerts list, in the Alert Details view, you can investigate those alerts further and create incidents from the alerts. In the CONFIGURE > Incident Rules view, you can create incident rules to create incidents.

Note: You can also use NetWitness Suite Automated Threat Detection to create incidents without manually creating rules.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts	View all alerts in NetWitness Suite.	View Alerts
SOC Managers, Administrators	Create incident rules.	See "Create an Incident Rule for Alerts" in the <i>NetWitness Respond Configuration Guide</i> .

Role	I want to ...	Show me how
Incident Responders, Analysts	View a list of events in the alert.*	View Event Details for an Alert
Incident Responders, Analysts	View event metadata for each event in the alert.*	View Event Details for an Alert
Incident Responders, Analysts	Further investigate the events in the alert.*	Investigate Events
Incident Responders, Analysts	Add alerts to an existing incident.	Add Alerts to an Incident Add Related Indicators to the Incident
Incident Responders, Analysts	Create incidents from alerts.	Create an Incident Manually
Data Privacy Officers, Administrators	Delete alerts.	Delete Alerts

*You can complete these tasks here (that is in the Alerts Details view).

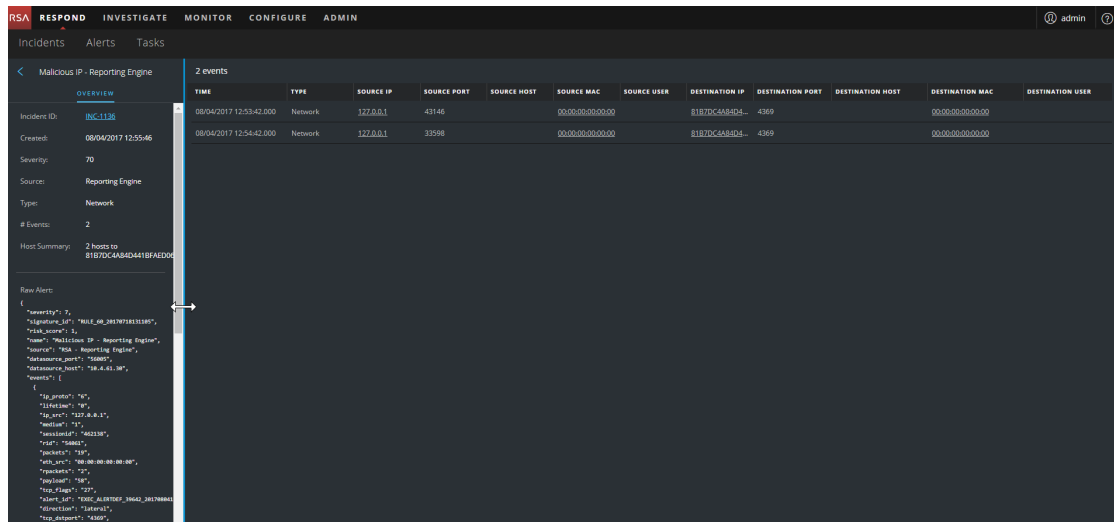
Related Topics

- [Alerts List View](#)
- [Reviewing Alerts](#)

Alert Details View

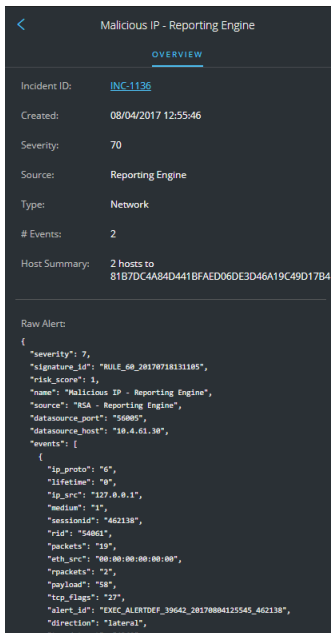
1. To access the Alert Details view, go to **RESPOND > Alerts**.
2. In the Alerts list, choose an alert to view and then click the link in the NAME column for that alert.
The Alert Details view has an Overview panel on the left and the Events panel on the right.

You can resize the panels to show more information as shown in the following figure.



Overview Panel

The Overview panel shows basic summary information about a selected alert. The Overview panel on the Alerts List view contains the same information. The Alerts List view [Overview Panel](#) topic provides details.



Events Panel

The Events panel can show an Events List if there is more than one event in the alert. If there is only one event in the alert, or you click an event in the Events List, you can see Event Details in the Events panel.

Events List

The Events List for a selected alert shows all of the events contained in that alert.

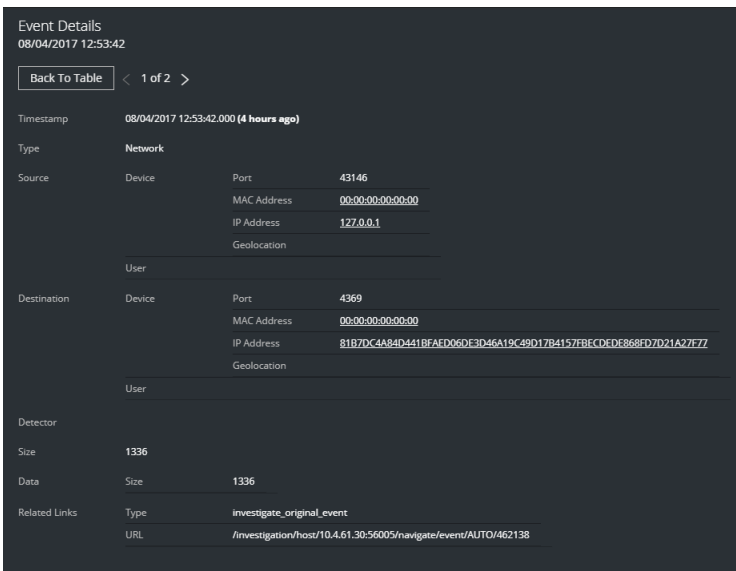
TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION PORT	DESTINATION HOST	DESTINATION MAC	DESTINATION USER
08/04/2017 12:53:42.000	Network	127.0.0.1	43146		00:00:00:00:00:00		81B7DC4A84D4...	4369		00:00:00:00:00:00	
08/04/2017 12:54:42.000	Network	127.0.0.1	33598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

The following table lists some of the columns shown in the Events List, which provide a summary of the listed events.

Column	Description
TIME	Shows the time the event occurred.
TYPE	Shows the type of alert, such as Log and Network.
SOURCE IP	Shows the source IP address if there was a transaction between two machines.
DESTINATION IP	Shows the destination IP address if there was a transaction between two machines.
DETECTOR IP	Shows the IP address of the machine where an anomaly was detected.
SOURCE USER	Shows the user of the source machine.
DESTINATION USER	Shows the user of the destination machine.
FILE NAME	Shows the file name if a file is involved with the event.
FILE HASH	Shows a hash of the file contents.

Event Details

The Event Details in the Events panel shows the event metadata for each event in the alert.



Event Metadata

The following table lists some event metadata sections and subsections shown in the first two columns in the Event Details. This is not an extensive list.

Section	Subsection	Description
Data		Shows information about the data involved with the event, such as the files involved. There may be 0 or more per event.
	Filename	Shows the file name if a file is involved with the event.
	Hash	Shows a hash of the file contents, for example, MD5 or SHA1.
	Size	Shows the size of the transmission or file involved with the event.
Description		Displays a general description of the event.
Destination		Shows the destination device and user.
	Device	Shows information about the destination device. See Event Source or Destination Device Attributes below.
	User	Shows information about the user or users of the destination. See Event Source or Destination User Attributes below.

Section	Subsection	Description
Detector		Shows the host or software product that detected the issue. This is most relevant for malware scanners and logs
	Device Class	Shows the device class of the product that detected the alert.
	IP Address	Shows the IP address of the product that detected the alert.
	Product Name	Shows the name of the product that detected the alert.
Domain		Shows the domain associated with the event.
Enrichment		Shows available enrichment information.
Related Links		If available, it shows a link back to the user interface (UI) of the source product.
	Type	Shows the type of event, such as <code>investigate_original_event</code> .
	URL	Shows the URL link back to the UI of the source product.
Size		Shows the size of the transmission or file involved.
Source		Shows the source device and user.
	Device	Shows information about the source machine. See Event Source or Destination Device Attributes below.
	User	Shows information about the user or users of the source machine. See Event Source or Destination User Attributes below.
Timestamp		Shows the time that the event occurred.
Type		Shows the type of the alert, such as log, network, correlation, Resubmit, Manual Upload, On Demand, File Share, or Instant IOC.

Event Source or Destination Device Attributes

The following table lists attributes for an event source or destination device that can be shown in the Events Details.

Name	Description
Asset Type	Displays the type of device, for example, desktop, laptop, server, network equipment, tablet, and so on.
BusinessUnit	Shows the business unit associated with the .
Compliance Rating	Shows the compliance rating of the device. It can be Low, Medium, or High.
Criticality	Shows how critical the device is to the business (business criticality).
Facility	Shows the location of the device.
Geolocation	Shows the geographic location for the host. It can contain the following attributes: city, country, latitude, longitude, organization, and domain.
IP Address	Shows the IP address of the device.
MAC Address	Shows the MAC address of the device.
Netbios Name	Shows the NetBIOS name for the device.
Port	Displays the TCP port, UDP port, or the IP Src port (the first one available) used to connect to and from the host.

Event Source or Destination User Attributes


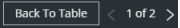
The following table lists attributes for an event source or destination user that can be shown in the Events Details.

Attribute Name	Description
AD Domain	Shows the Active Directory domain.
AD Username	Shows the Active Directory username.

Attribute Name	Description
Email Address	Shows the email address of the user.
Username	Shows a general name if you do not know the source of the username, such as UNIX or a username in a particular system.

Toolbar Actions

This table lists the toolbar actions available in the Alert Details view.

Option	Description
	(Back to Alerts) Enables you to navigate back to the Alerts List view.
	Click the arrows to navigate through the event meta details for each event in the alert. The numbers, such as "1 of 2" show the number of the event that you are currently viewing. Click Back to Table to go back to the Events List view, which is also known as the Events Table.

Tasks List View

After investigating incidents, in the Tasks List view (RESPOND > Tasks), you can create and track incident tasks. For example, you can create remediation tasks when you require actions on incidents from teams outside of your security operations. You can reference external ticket numbers within the tasks and then track those tasks to completion. You can also modify and delete tasks as required, depending on your user permissions.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts	View tasks	View All Incident Tasks and View the Tasks associated with an Incident
Incident Responders, Analysts	Filter tasks.	Filter the Tasks List
Incident Responders, Analysts	Create a task.	Create a Task
Incident Responders, Analysts	Find and modify tasks.	Find a Task and Modify a Task
Incident Responders, Analysts	Close a task (Change the Status to Remediated, Risk Accepted, or Not Applicable).	Modify a Task
Incident Responders, Analysts, SOC Managers	Delete a task.	Delete a Task

Related Topics

- [Incident Details View](#)
- [Escalate or Remediate the Incident](#)

Tasks List

To access the Tasks List view, go to **RESPOND > Tasks**. The Tasks List view displays a list of all incident tasks.


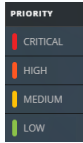
CREATED	PRIORITY	ID	NAME	ASSIGNEE	STATUS	LAST UPDATED	CREATED BY	INCIDENT ID
08/06/2017 18:26:37	HIGH	REM-10	Isolate machine	Tony	New	08/06/2017 18:26:37	admin	INC-450
08/06/2017 18:25:34	HIGH	REM-9	Mitigation task	Tony	New	08/06/2017 18:25:34	admin	INC-450
08/06/2017 17:04:46	HIGH	REM-8	Re-image the 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

The Tasks List view consists of a Filters panel, a Tasks List, and a Task Overview panel. The following figure shows the Tasks List and the Overview panel.

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

Tasks List

The Tasks List shows all of the incident tasks. You can filter this list to show only tasks of interest.

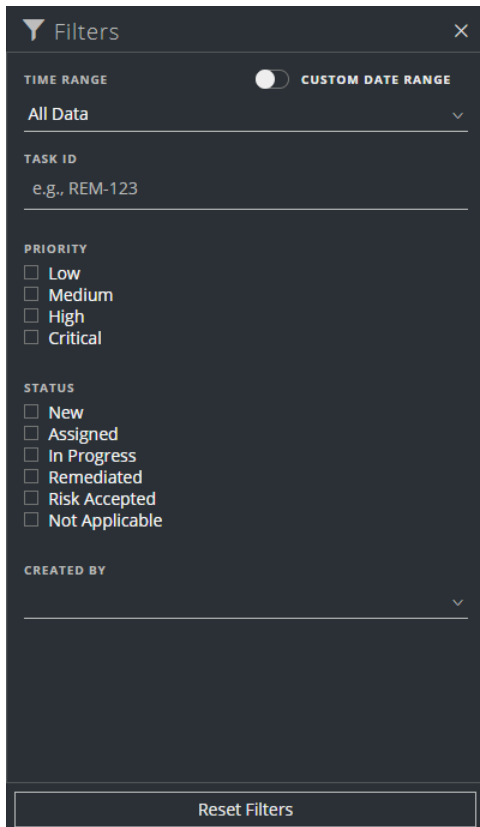
Column	Description
	Enables you to select one or more tasks to modify or delete. Users with the appropriate permissions can make bulk updates and delete tasks, such as SOC Managers. For example, an SOC Manager may want to assign multiple tasks to a user at the same time.
CREATED	Displays the date when the task was created.
PRIORITY	Displays the priority assigned to the task. The priority can be any of the following: Critical, High, Medium, or Low. The Priority is also color coded, where red indicates Critical , orange represents High risk, yellow indicates Medium risk, and green represents Low risk as shown in the following figure: 
ID	Displays the task ID.
NAME	Displays the task name.
ASSIGNEE	Displays the name of the user assigned to the task.
STATUS	Displays the status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable.
LAST UPDATED	Displays the date and time when the task was last updated.
CREATED BY	Displays the user who created the task.

Column	Description
INCIDENT ID	Displays the incident ID for which the task was created. Click the ID to display the details of the incident.

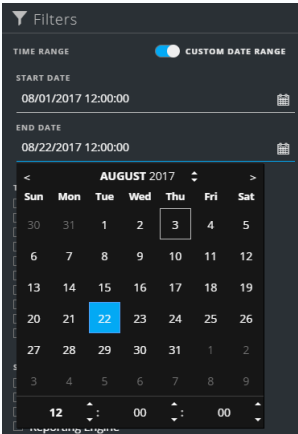
At the bottom of the list, you can see the number of tasks on the current page and the total number of tasks. For example: **Showing 23 out of 23 items**

Filters Panel

The following figure shows the filters available in the Filters panel.



The Filters panel, on the left of the Tasks List view, has options that you can use to filter the incident tasks.

Option	Description
TIME RANGE	You can select a specific time period from the Time Range drop-down list. The time range is based on the creation date of the tasks. For example, if you select Last Hour, you will see tasks that were created within the last 60 minutes.
CUSTOM DATE RANGE	<p>You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to view the Start Date and End Date fields. Select the dates and times from the calendar.</p> 
TASK ID	You can type the Task ID for a task that you would like to locate, for example REM-123.
PRIORITY	<p>You can select the priorities that you would like to view. If you make one or more selections, the Tasks list shows only those tasks with the selected priorities.</p> <p>For example: If you select Critical, the Tasks list shows only the tasks with a priority set to Critical.</p>
STATUS	<p>You can select the statuses that you would like to view. If you make one or more selections, the Tasks list shows only those tasks with the selected statuses.</p> <p>For example: If you select Assigned, the Tasks panel shows only the tasks that are assigned to users.</p>

Option	Description
CREATED BY	You can select the user who created the tasks that you would like to view. For example, if you only want to view the tasks created by Edwardo, select Edwardo from the CREATED BY drop-down list. If you want to view tasks regardless of the person who created the task, do not make a selection under CREATED BY.
Reset Filters	Removes your filter selections.

The Tasks List shows a list of tasks that meet your selection criteria. You can see the number of items in your filtered list at the bottom of the tasks list. For example: **Showing 18 out of 18 items**

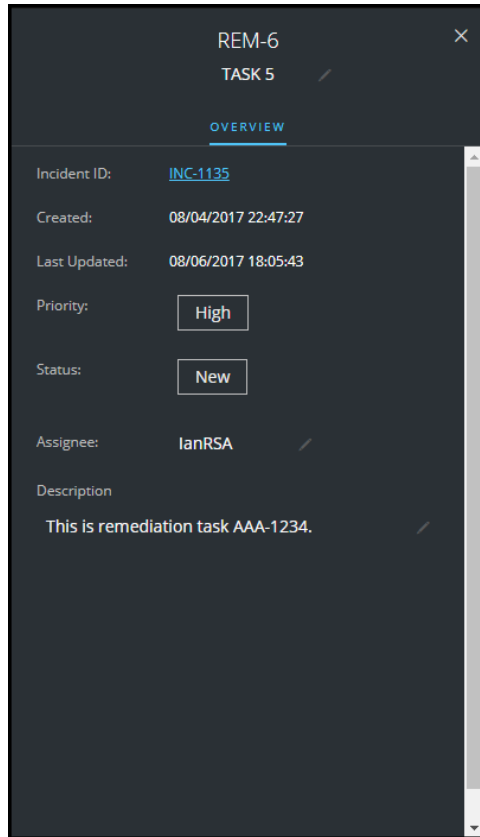
Task Overview Panel

To access the Task Overview panel:

1. Go to **RESPOND > Tasks**.

2. In the Task list, click the task that you want to view.

The Task Overview panel appears to the right of the Tasks list.





The following table lists the fields displayed in the Task Overview panel.

Field	Description
<Task ID>	Displays the automatically assigned task ID.
<Task Name>	Displays the task name. This is an editable field. To change the task name, you can click the current task name to open a text editor. For example, you can change a task name from "Reimage a Laptop" to "Reimage a Server".
Incident ID	Displays the Incident ID for which the task was created. Click the ID to display the details of the Incident.
Created	Displays details about the date and time when the task was created.

Field	Description
Last Updated	Displays the date and time when the task was last updated.
Priority	Displays the priority of the task: Low, Medium, High, or Critical. To change the priority, you can click the priority button and select a priority for the task from the drop-down list.
Status	Displays the status of the task: New, Assigned, In Progress, Remediated, Risk Accepted, and Not Applicable. To change the status, you can click the status button and select a status for the task from the drop-down list.
Assignee	Displays the user assigned to the task. To change the user assigned to the task, you can click (Unassigned) or the name of the previous assignee to open a text editor.
Description	Shows task details. To modify the description, you can click the text underneath the description to open a text editor.

Toolbar Actions

This table lists the toolbar actions available in the Tasks List view.

Option	Description
	Enables you to open the Filters panel so that you can specify the tasks that you would like to see in the Tasks List.
	Closes the panel.
Delete button	Allows you to delete the selected tasks.

Add/Remove from List Dialog

The Add/Remove from List dialog allows you to add or remove an entity or meta value to an existing list or create a new list. For example, when you look up an IP address and you find it suspicious or interesting, you can add it to a relevant list, which has been added a data source. This improves the visibility of the suspicious IP addresses. You can also add entities or meta values to different lists. For example, you can add them to one list for suspected domains related to command and control connections and to another list for Trojan connections IP addresses related to remote access. If a list is not available, you can create a list. You can also remove the entity or meta value from a list.

Note: From the Add/Remove from List dialog, you can only add or remove entities or meta values from single column lists added as a datasource, not multi-column lists. And when you edit a list or a value in a list from the nodal view or the context lookup view, ensure to refresh the web page to view the updated data.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts	Add an entity to a list.	From the Incident Details view, see Add an Entity to a Whitelist . From the Alert Details view, Add an Entity to a Whitelist .
Incident Responders, Analysts	Create a whitelist, blacklist, or other list.	Create a List
Administrators	Add a Context Hub list as a data source.	See "Configure Lists as a Data Source" in the <i>Context Hub Configuration Guide</i> .
Administrators	Import or export a list for Context Hub.	See "Import or Export Lists for Context Hub" in the <i>Context Hub Configuration Guide</i> .

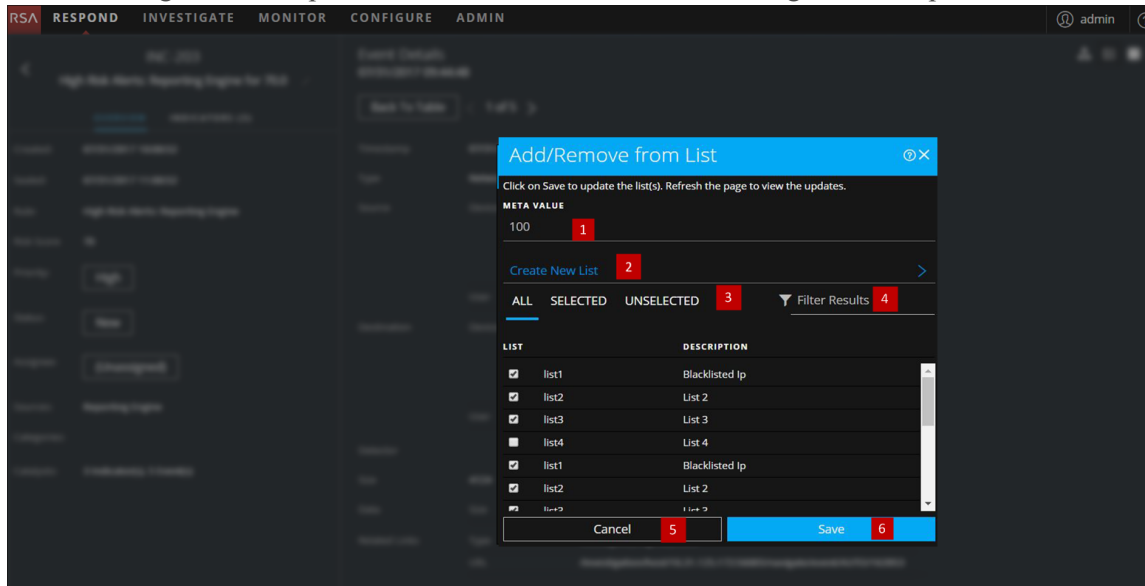
Related Topics

- [Investigate the Incident](#)
- [Reviewing Alerts](#)
- [View Contextual Information](#) (Incident Details view)
- [View Contextual Information](#) (Alert Details view)

Note: You cannot delete a list, but you can delete values within a list.

Quick Look

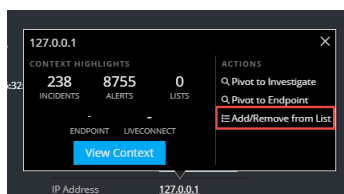
The following is an example of the **Add/Remove from List** dialog in the Respond view.



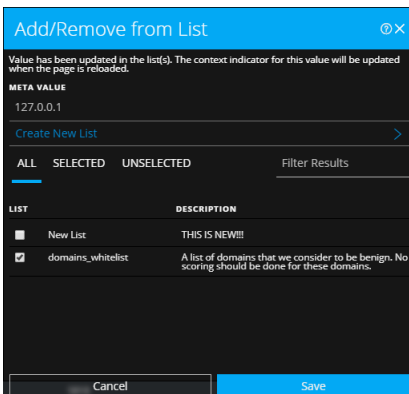
- 1 Entities or meta values to be added or removed.
- 2 Create a new list using the selected meta.
- 3 Select any of the tabs: All, Selected, or Unselected.
- 4 Search using the list name or description.
- 5 Cancel the action.
- 6 Save to update lists or create a new list.

Add/Remove from List

To access the Add/Remove from List dialog, in the Incident Details view or the Alert Details view, hover over the underlined entity that you would like to add or remove from a Context Hub list. A context tooltip appears showing the available actions.



In the Actions section of the tooltip, click Add/Remove from List. The Add/Remove From List dialog shows the available lists.



The following table shows the options in the Add/Remove from List dialog.

Option	Description
META VALUE	Displays the selected entity or meta value that needs to be added to or removed from one or more lists. You can also create a new list using the selected value.
Create New List	When clicked, it displays a dialog to create a new list using the selected meta value.
ALL	Shows all of the available Context Hub lists. The lists that contain the selected entity or meta value are selected. Select a checkbox to add an entity or meta value to a list. Clear a checkbox to remove it from the list.
SELECTED	Shows only the lists that contain the selected entity or meta value. (All lists are selected.)
UNSELECTED	Shows only the lists that do not contain the selected entity or meta value. (All lists are unselected.)
Filter Results	Enter the name or description of a specific list to search from multiple lists.
LIST	Displays the name of all the lists.

Option	Description
DESCRIPTION	Displays information about the selected list. The description that you provide when creating a list appears in this dialog. For example: This list contains all of the blacklisted IP addresses.
Cancel	Cancels the operation.
Save	Saves the changes.

Context Lookup Panel - Respond View

The Context Hub service brings together contextual information from several data sources into the Respond view so that analysts can make better decisions during their analysis and take appropriate action. Seeing the entities, meta values, and contextual information in a single interface helps analysts to prioritize and identify areas of interest. For example, recently created incidents and alerts from the Respond view involving a given entity or meta value will be displayed when the analyst queries for additional information for that entity or meta value. The Context Lookup panel displays contextual information for the selected entities or meta values such as IP address, User, Host, Domain, File Name, or File Hash. The data available depends on the configured sources in the Context Hub.

The Context Lookup panel displays the contextual information based on the data available on the configured sources in the Context Hub.

What do you want to do?

Role	I want to ...	Show me how
Incident Responders, Analysts, Threat Hunters	Navigate to the Context Lookup panel.	From the Incident Details view, see View Contextual Information . From the Alert Details view, see View Contextual Information .
Incident Responders, Analysts, Threat Hunters	Understand the information in the Context Lookup panel for a selected entity.	See the information in this topic.
Administrator	Configure Data Sources for Context Hub.	See "Configure Data Sources for Context Hub" in the <i>Context Hub Configuration Guide</i> .
Administrator	Configure Context Hub settings.	See "Configure Context Hub Data Source Settings" in the <i>Context Hub Configuration Guide</i> .

Related Topics

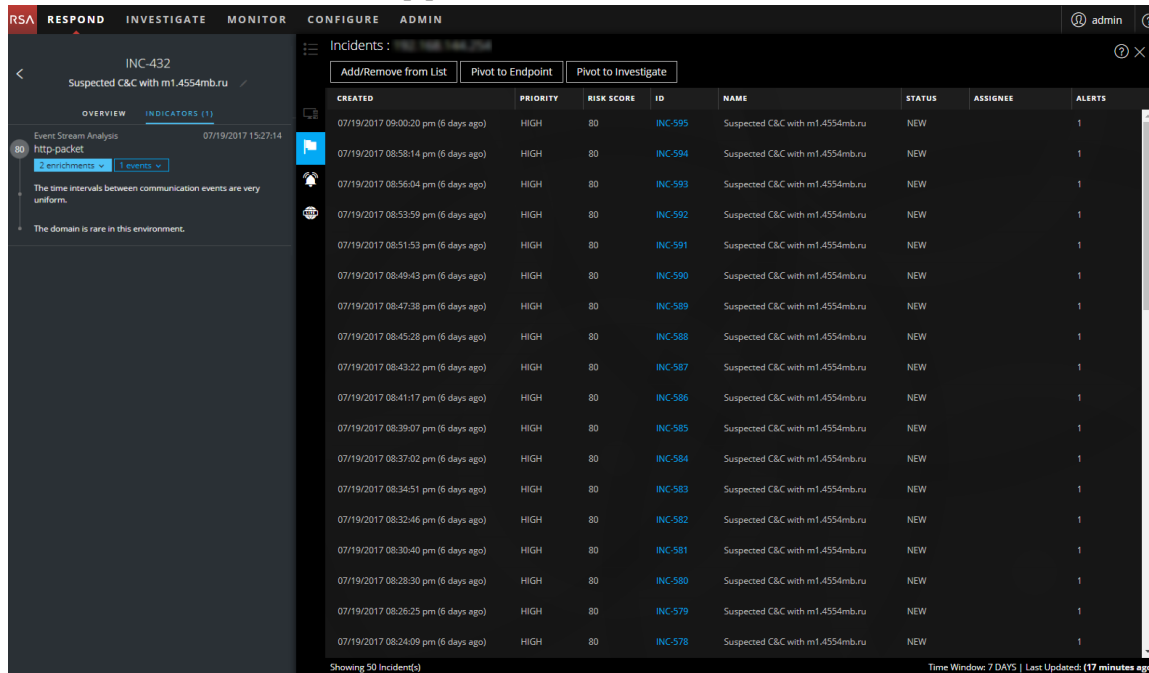
- [Investigate the Incident](#)
- [Reviewing Alerts](#)

Contextual Information Displayed in the Context Lookup Panel




The contextual information or query results displayed in the Context Lookup panel depends on the selected entity and the associated data sources.





The Context Lookup panel has separate tabs for each of the data sources. The List data source tab is the first in the context panel followed by Archer, Endpoint, Incidents, Alerts and Live Connect.

The following figure displays the Context Lookup panel for a selected entity in the Incident Details view. The Context Lookup panel Incidents tab is in view.



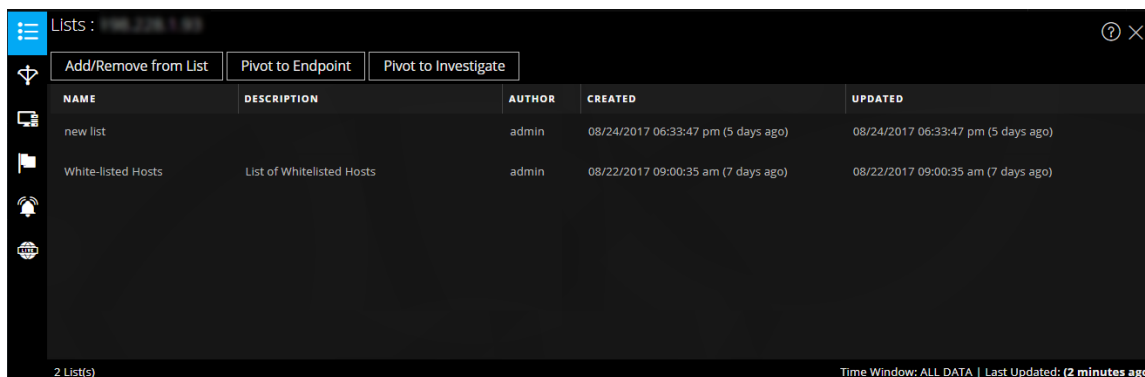
The following table describes the data available on each tab and the supported entities.

Tab	Description	Supported Entities
 (Lists)	Displays all of the list data associated with the selected entity or meta value. The result is sorted by the last updated list.	All entities
 (Archer)	Displays asset information along with criticality ratings using the Archer data source.	IP and Host
 (Active Directory)	Displays all user information for the selected user.	User

Tab	Description	Supported Entities
 (NetWitness Endpoint)	Displays the NetWitness Endpoint data source information for the selected entity or meta value, which includes the Machines, Modules, and IIOC levels. Modules are by highest IOC score to lowest IOC score and IIOC levels are sorted by highest IOC levels to lowest IOC levels.	IP, MAC address, and Host
 (Incidents)	Displays the list of incidents associated with the selected entity or meta value. The result is sorted by newest incidents to oldest incidents.	All entities
 (Alerts)	Displays the list of alerts associated with the selected entity or meta value. The result is sorted by newest alerts to oldest alerts.	All entities
 (Live Connect)	Displays information related to Live Connect.	IP, Domain, and Filehash

Lists

The Context Lookup panel for Lists shows one or more lists associated with the selected entity or meta value. The following figure is an example of the Context Panel for Lists.

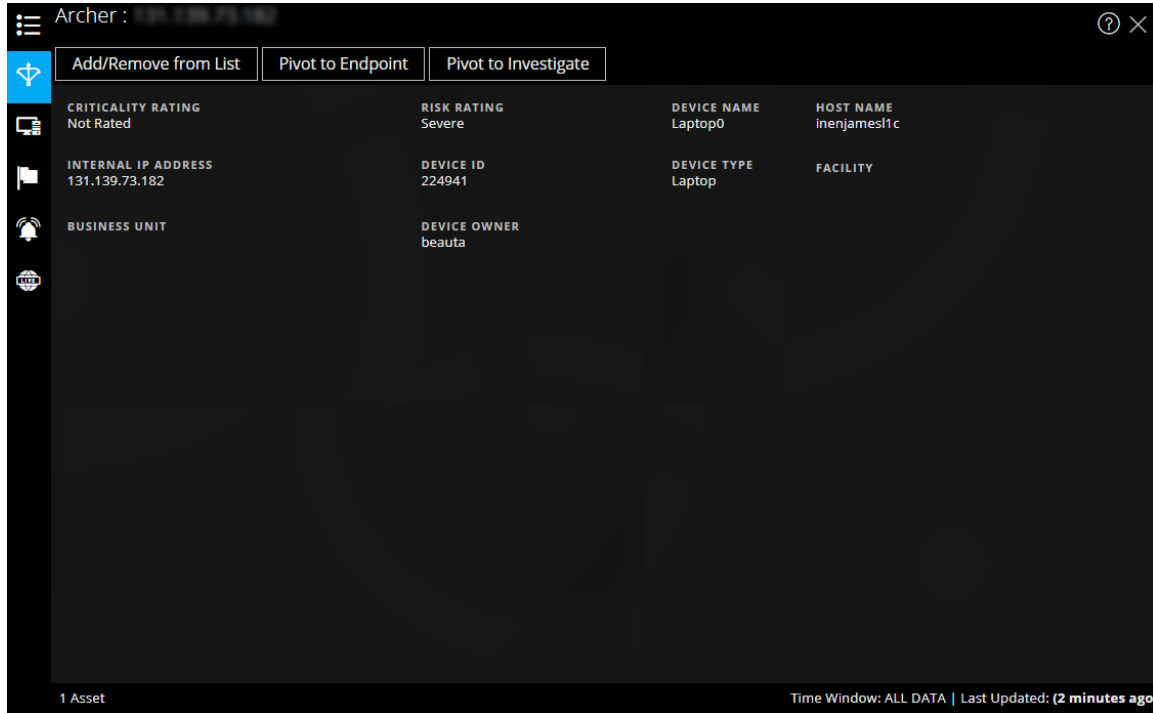


The following information is displayed for Lists.

Field	Description
Name	The name of the list (defined while creating the list).
Description	The description of the list (defined while creating the list).
Author	The owner who created the list.
Created	The date when the list was created.
Updated	The date when the list was last updated or modified.
Count	The number of lists in which the selected entity or meta value is available.
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Responses dialog. By default, all Lists data is fetched.
Last Updated	The time when Context Hub fetched and stored the lookup data in cache.

Archer

The Context Lookup panel for Archer displays asset information along with criticality ratings using the Archer data source for IP and Host entities and meta values. The following figure is an example of the Context Panel for Archer.



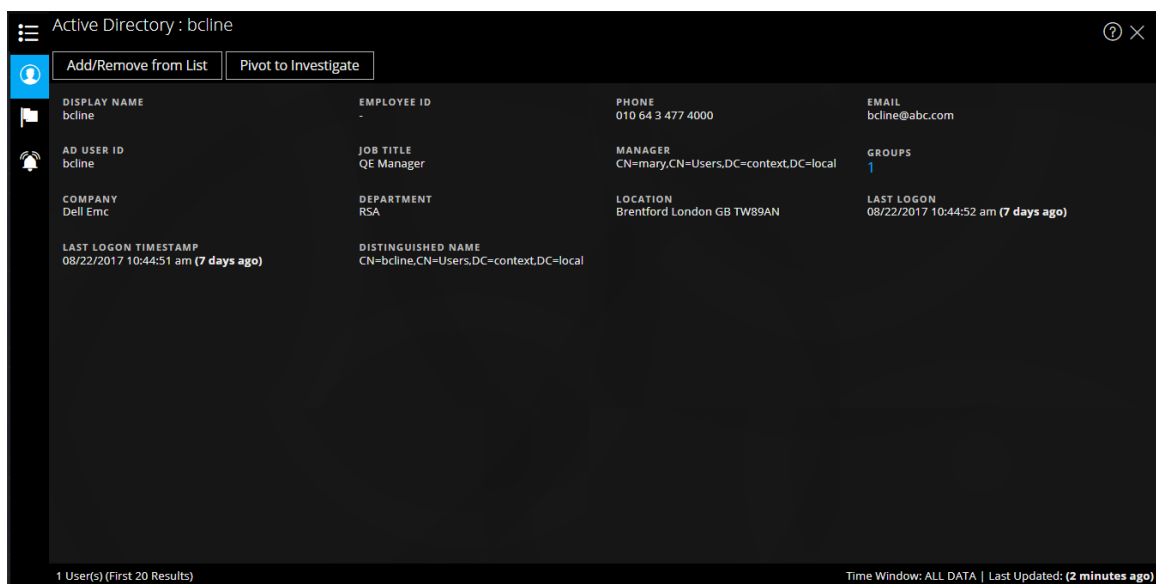
The following information is displayed for Archer.

Field	Description
Criticality Rating	Displays the device operational Criticality based on the applications it supports. The criticality ratings can be set as Not Rated, Low, Medium-Low, Medium, Medium-High, or High .
Device ID	Displays the automatically populated value that uniquely identifies the record across all applications within the system.
Device Name	Displays the unique name of the device.
Device Owner	Displays the owner(s) of the device who is responsible for the device and receives read and update rights of the record.
Host Name	Displays the host name of the device.

Field	Description
Facilities	Provides links to records in the Facilities application that are related to this device.
Business Unit	Provides links to records in the Business Unit application that are related to this device.
Risk Rating	Calculates the risk rating for the device based on the most recent assessment and the average risk rating of facilities using the device. The risk rating can be set as Severe, High, Medium, Low, or Minimal.
Type	Displays the device type such as Server, laptop, desktop etc.
IP Address	Displays the primary internal IP address of the device.
Count	Displays the number of assets available.
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Responses Dialog. By default, all data for Archer is fetched.
Last Updated	The time when Context Hub fetched and stored the lookup data in cache.

Active Directory

The following figure is an example of a Context Panel for Active Directory.



The Context Lookup panel for Active Directory displays all the related information, incidents, and alerts for a user. You can perform a look up using the following formats:

- userPrincipalName
- Domain\UserName
- sAMAccountName

If the user exists in multi-domain or multi-forest, all the related context information is displayed for the specific user.

The following information is displayed for Active Directory.

Field	Description
Display Name	Displays the name of the specific user.
Employee ID	Displays the employee ID of the specific user.
Phone	Displays the phone number of the specific user.
Email	Displays the email ID of the specific user.
AD User ID	Displays the unique identification of the specific user within an organization.
Job Title	Displays the designation of the specific user.
Manager	Displays the manager's name of the
Groups	Displays the list of groups the specific user is a member.
Company	Displays the name of the company the specific user belongs to.
Department	Displays the department name within the organization that the specific user belongs to.
Location	Displays the location of the specific user.
Last Logon	Displays the time when the specific user logged into to the system only if the Global Catalogue is defined.
Last Logon TimeStamp	Displays the time when the specific user logged into to the system.
Distinguished Name	Displays the unique name assigned to the user.
Count	Displays the number of users.

Field	Description
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Data Source Settings dialog. By default, all data for Active Directory is fetched.
Last Updated	The time when Context Hub fetched and stored the lookup data in cache.

NetWitness Endpoint

The following information is displayed in the Context Lookup panel for NetWitness Endpoint.

NetWitness Endpoint : 10.63.0.225

Buttons: Add/Remove from List, Pivot to Endpoint, Pivot to Investigate

Summary Metrics:

- # 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

Top Suspicious Modules (IIOC Score > 1)

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

Machine IOC Levels

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)

The following information is displayed for IIOC.

Field	Description
# Of Modules	Displays the number modules that are looked up.
Admin Status	Displays the admin status (if any).
Last Updated	Displays the time when the data was last refreshed.
Last Login	Displays the time when the user last logged in.
MAC Address	Machine MAC Address.

Field	Description
Operating System	Version of the Operating System used by the NetWitness Endpoint machine.
Machine Status	Displays if the looked you module is Online, Offline, Active, or Inactive.
IP Address	Displays the IP address of the specific Module.

The following information is displayed for Modules.

Field	Description
IIOC Score	A machine IIOC score is an aggregated score based on the module scores. This is based on the value set for "Minimum IIOC Score" field in the Context Hub Data Source Settings The default value for "Minimum IIOC Score" is 500. See the "Configure Context Hub Data Source Settings" topic in the <i>Context Hub Configuration Guide</i> .
Module Name	Name of the module that is looked up.
Analytic Score	Number of active files for the selected machine.
Machine Count	Indicates when the scan results were last updated in NetWitness Endpoint database.
Signature	Indicates if the file is signed or unsigned, valid or invalid, and provides signatory information. For example, Google, Apple, and so on.

The following information is displayed for Machines.

Field	Description
IOC Levels	Displays the IOC levels.
Description	Displays the description for the IOC level if available.
Last executed	Displays the time when the action was executed.
Count	Displays the number of hosts that are looked up.

Field	Description
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Data Source Settings dialog. By default, all data for NetWitness Endpoint is fetched.
Last Updated	Indicates when the scan results were last updated in NetWitness Endpoint database.

Alerts

The following figure is an example of Context Panel for Alerts that is displayed based on time first (Newest to Oldest) and then severity.

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	

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

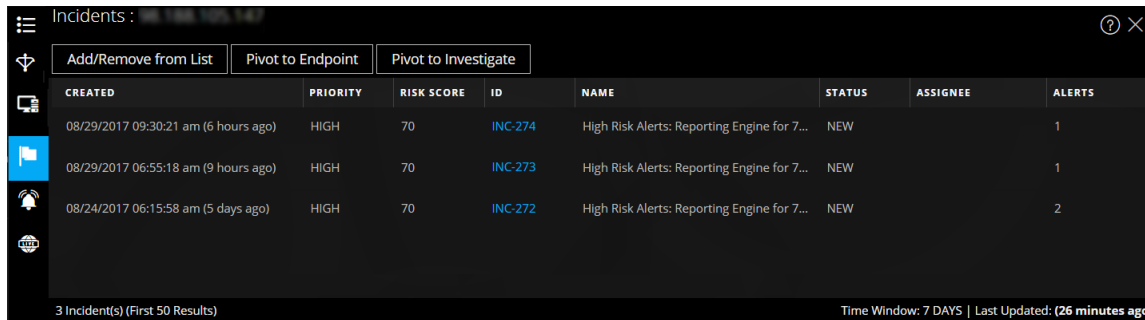
The following information is displayed in the Context Lookup panel for Alerts.

Field	Description
Created	Date and time when the alert was created.
Severity	Severity value of the alerts
Name	Name of the Alert. Click the name to view the details of a specific alert.
Source	Alert source name from where the alert is triggered.
#Events	Number of events associated with the alert.

Field	Description
Incident ID	This is the ID of the incident that the alert is associated with (If any). Click the ID to view the details of a specific alert.
Count	Displays the number of alerts. By default only the first 100 alerts are displayed. For more information on how to configure the settings, see the "Configure Context Hub Data Source Settings" topic in the <i>Context Hub Configuration Guide</i> .
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Data Source Settings dialog. By default, the alert data for last 7 days is fetched.
Last Updated	Indicates when contextual data was last fetched from data source.

Incidents

The following figure is an example of the Context Panel for Incidents, which is based on time first (Newest to Oldest) and then priority status.



The following information is displayed in the Context Lookup panel for Incidents.

Field	Description
Created	Date when the incident was created
Priority	Priority status of the incidents
Risk Score	Risk score of the incidents
ID	Incident ID of the incident and on clicking displays further details about the incident
Name	Incident Name

Field	Description
Status	Status of the incident
Assignee	Current owner of the incident
Alerts	Number of alerts associated with the incident
Count	Displays the number of incidents. By default only the first 100 alerts are displayed. For more information on how configure the settings, see the "Configure Context Hub Data Source Settings" topic in the <i>Context Hub Configuration Guide</i> .
Time Window	This is based on the value that is set for the "Query Last" field in the Configure Data Source Settings dialog. By default, the alert data for last 7 days is fetched.
Last Updated	Indicates when contextual data was last fetched from data source.

Live Connect

The following figure is an example of a Context Panel for Live Connect.


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

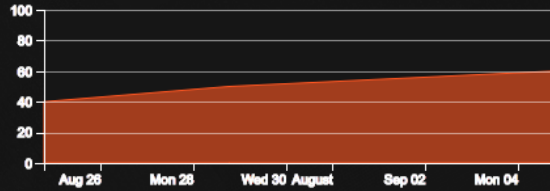
Community Activity

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>
---	--

The Live Connect Panel displays the following information:

- Review Status
- Live Connect Risk Assessment
- Risk Indicators
- Community Activity
- WHOIS
- Related Files, Domains, and IPs
- Identity
- Certificate Information

The following information is displayed in the Context Lookup panel for Live Connect.

Field	Description
Review Status	<p>Displays the review status of the selected Live Connect entity (IP, file, or domain) based on the analyst activity. This gives the visibility of the analyst activity within an organization.</p> <p>Status Below are the types of status:</p> <ul style="list-style-type: none"> • New: If lookup results for an IP address is viewed for the first time within the organization. • Viewed: If any analyst within the organization has already viewed the lookup results for an IP address. • Marked as Safe: If any analyst within the organization has already viewed the lookup results and marked the IP address as safe. • Marked as Risky: If any analyst within the organization has already viewed the lookup results and marked the IP address as risky.

Field	Description
Risk Assessment	<p>Displays the risk assessment for the selected Live Connect entity (IP, file, or domain) based on the Live Connect analysis and analyst feedback. The Risk Assessment categories are:</p> <ul style="list-style-type: none">• Safe: The Live Connect entity is considered to be safe.• Unknown: Live Connect does not have enough information about this entity to calculate the risk.• High Risk: Marked as "High Risk" based on the analysis and risk reasons provided by the community. The entities marked as "High Risk" requires immediate attention.• Suspicious: Marked as "Suspicious" based on the analysis and risk reasons provided by the community. The analysis indicates potentially threatening activity that requires action.• Unsafe: Marked as "Suspicious" based on the analysis and risk reasons provided by the community. <p>The entity is rated as High Risk, Suspicious, or Unsafe and displays the associated risk reasons accordingly.</p>

Field	Description
Risk Assessment Feedback	<p data-bbox="462 283 1347 352">Risk Assessment Feedback allows the analyst to submit threat intelligence feedback about an entity to the Live Connect server.</p> <ul style="list-style-type: none"> <li data-bbox="462 378 738 409">• Analyst Skill Level <p data-bbox="495 424 987 455">Below are the Analyst skill level options:</p> <ul style="list-style-type: none"> <li data-bbox="495 483 1421 604">○ Tier 1 - Analysts at this level generally define procedures for remediation, and decide if an incident should be escalated to other areas in a SOC (Security Operation center). This is the default value. <li data-bbox="495 632 1377 709">○ Tier 2 - Analysts investigates incidents, and captures intelligence from investigation to feedback into the various work flows in a SOC. <li data-bbox="495 737 1383 861">○ Tier 3 - Analysts who shares the investigation results to the SOC organization. They generally manage incidents and have a wide breadth and depth in the skills and tools necessary for incident response. <div data-bbox="500 884 1421 1020" style="border: 1px solid green; padding: 5px;"> <p data-bbox="506 898 1398 1003">Note: While creating a new user for NetWitness Suite (Analyst), an administrator should be able to identify the user as Tier 1, Tier 2, or Tier 3 Analyst.</p> </div> <ul style="list-style-type: none"> <li data-bbox="462 1058 1421 1701">• Risk Confirmation - The risk confirmation for the selected Live Connect entity (IP, file, or domain). The Risk confirmation categories are: <ul style="list-style-type: none"> <li data-bbox="495 1161 1182 1192">○ Safe: The Live Connect entity is considered to be safe. <li data-bbox="495 1220 1421 1297">○ Unknown: The analyst does not have enough information to provide a risk confirmation <li data-bbox="495 1325 1421 1446">○ High Risk: Marked as "High Risk" based on the analysis and risk reasons provided by the community. The entities marked as "High Risk" requires immediate attention. <li data-bbox="495 1474 1421 1596">○ Suspicious: Marked as "Suspicious" based on the analysis and risk reasons provided by the community. The analysis indicates potentially threatening activity that requires action. <li data-bbox="495 1623 1338 1701">○ Unsafe: Marked as "Unsafe" based on the analysis and risk reasons provided by the community. <li data-bbox="462 1728 1421 1862">• Confidence Level - The confidence level of an analyst in providing feedback for the Live Connect entity. The confidence level categories are: <ul style="list-style-type: none"> <li data-bbox="495 1835 592 1866">○ High

Field	Description
-------	-------------

- Medium
- Low.
- **Risk Indicator Tags** - Allows you to select a tag category based on the analysis.

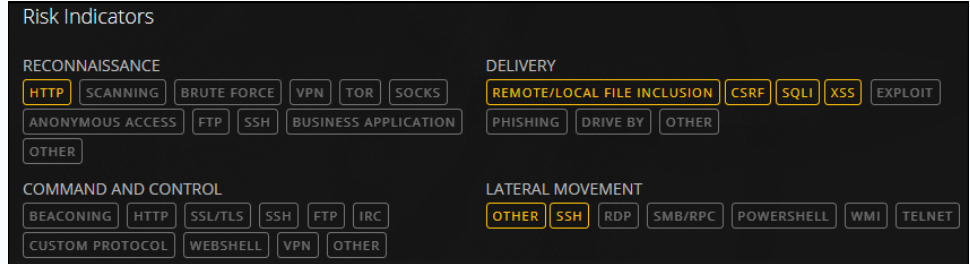
The screenshot shows a 'Risk Assessment Feedback' form with the following elements:

- ANALYST SKILL LEVEL:** Tier 1 (dropdown menu)
- RISK CONFIRMATION:** Select... (dropdown menu)
- CONFIDENCE LEVEL:** Select... (dropdown menu)
- RISK INDICATOR TAGS:** (dropdown menu)
- Submit:** A blue button to submit the feedback.

Community Activity	<p>Community activities such as:</p> <ul style="list-style-type: none"> • Date first seen in the community. • Time since the IP/File/Domain was seen for the first time (Current time - First seen time). <p>Trending Community Activity:</p> <p>If the IP address is known within the RSA community, a graphical representation of the community activity trend is displayed for the following:</p> <ul style="list-style-type: none"> • Users (in %) who have viewed the IP address in the Live Connect community over time. • Users (in %) who submitted feedback for the IP address. • Users (in %) who marked the IP address as unsafe over time.
--------------------	--

Field	Description
-------	-------------

Risk Indicators	Risk Indicators are highlighted based on the tags that are assigned by the community to the entities (IPs, Files, or Domains).
-----------------	--



The tags are categorized as given below:

- Reconnaissance
- Delivery
- Command and Control
- Lateral Movement
- Privilege Escalation
- Packaging and Exfiltration

These tags are samples and vary based on the inputs received from the community on the Live Connect server.

The analyst can choose the appropriate risk indicator tags while providing the review feedback.

A highlighted tag indicates that the selected entity is associated with that particular category and tag. Clicking a highlighted tag displays the description of the tag.

Field	Description
Identity	<p>Provides the following identity information for the selected entity or meta value:</p> <p>For IP address:</p> <ul style="list-style-type: none">• Autonomous System Number (ASN)• Prefix• Country Code and Country Name• Registrant (Organization)• Date <p>For File Hash:</p> <ul style="list-style-type: none">• File Name• File Size• MD5• SH1• SH256• Compile Time• Mime Type <p>For Domain:</p> <ul style="list-style-type: none">• Domain Name• Associated IP Address
Certificate Information	<p>Provides the following certificate information for the selected file hash:</p> <ul style="list-style-type: none">• Certificate Issuer• Validity of the Certificate• Signature Algorithm• Certificate Serial Number

Field	Description																		
<p>WHO IS Information</p>	<p>The WHO IS information provides the ownership details for a given domain.</p> <div data-bbox="462 331 1287 747" 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>ORGANIZATION Google Inc.</td> <td></td> <td></td> </tr> </table> </div> <p>The following information of the domain owner is displayed:</p> <ul style="list-style-type: none"> • Created Date • Updated Date • Expired Date • Type (Registration Type) • Name • Organization • Address with Postal code • Country • Phone • Fax • Email 	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.																			

Field	Description
Related Files	<p>Related Files are displayed for entity types IP and Domain. A list of known associated files are displayed along with the following information:</p> <ul style="list-style-type: none">• Live Connect Risk Rating (Safe, Risky, or Unknown)• File Name• MD5• Compile Time and Date• API Function Import Hash• Mime Type
Related Domains	<p>Related Domains are displayed for entity types IP and Files. A list of known associated domains are displayed along with the following information:</p> <ul style="list-style-type: none">• Live Connect Risk Rating (Safe, Risky, or Unknown)• Domain Name• Country Name• Registered Date• Expired Date• Registrant Email address

Field	Description
-------	-------------

Related IPs Related IPs are displayed for entity types Domain and Files. A list of known associated IPs are displayed along with the following information:

- Live Connect Risk Rating (Safe, Risky, or Unknown)
- IP Address
- Domain Name
- Country Code and Country Name
- Country Name
- Registered Date
- Expired Date
- Registrant Email address

Related Files (5)

LC RISK RATING	FILE NAME	MD5	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	2ymh2gnnb6pgq2r.gre...		09/22/2017 10:59:25 ...	09/22/2017 10:59:25 ...	

