



NetWitness Respond User Guide

for RSA NetWitness® Platform 11.3



Copyright © 1994-2019 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.

April 2019

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	12
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	19
Unassign an Incident	21
Determine which Incidents Require Action	22
View Incident Details	23
View Basic Summary Information about the Incident	25
View the Indicators and Enrichments	27
View and Study the Events	28
View C2 Enrichment Information for Suspected C&C Incidents	31
View and Study the Entities Involved in the Events	33
Select Node Types to View on the Nodal Graph	35
Filter the Data in the Incident Details View	38
View the Tasks associated with an Incident	39
View Incident Notes	40
Find Related Indicators	40
Add Related Indicators to the Incident	42
Investigate the Incident	44
View Contextual Information	45
Add an Entity to a Whitelist	48
Create a List	49
View the Reputation Status of a File Hash	50
Pivot to Investigate > Navigate	52
Pivot to Investigate > Hosts/Files	52
Pivot to NetWitness Endpoint Thick Client	53

Pivot to Archer	53
View Event Analysis Details for Indicators	54
Migration Considerations	54
View User Entity Behavior Analytics for Indicators	58
Document Steps Taken Outside of NetWitness	58
View the Journal Entries for an Incident	59
Add a Note	60
Delete a Note	62
Escalate or Remediate the Incident	63
Send an Incident to RSA Archer	63
View All Incidents Sent to Archer	66
Update an Incident	66
Change Incident Status	67
Change Incident Priority	70
Assign Incidents to other Analysts	73
Rename an Incident	75
View All Incident Tasks	77
Filter the Tasks List	78
Remove My Filters from the Tasks List	80
Create a Task	81
Find a Task	86
Modify a Task	86
Delete a Task	90
Close an Incident	93
Reviewing Alerts	94
View Alerts	94
Filter the Alerts List	96
Remove My Filters from the Alerts List	98
View Alert Summary Information	98
View Event Details for an Alert	100
Investigate Events	104
View Contextual Information	104
Add an Entity to a Whitelist	107
Create a Whitelist	108
Pivot to Investigate > Navigate	108
Pivot to Investigate > Hosts/Files	108
Pivot to Endpoint Thick Client	109
Pivot to Archer	109
Create an Incident Manually	110
Add Alerts to an Incident	113

Delete Alerts	115
NetWitness Respond Reference Information	117
Incidents List View	118
Workflow	118
What do you want to do?	119
Related Topics	119
Quick Look	119
Incidents List View	120
Incidents List	121
Filters Panel	123
Overview Panel	125
Toolbar Actions	126
Incident Details View	128
Workflow	128
What do you want to do?	129
Related Topics	130
Quick Look	131
Overview Panel	133
Indicators Panel	133
Event Analysis	134
User Entity Behavior Analytics	136
Nodal Graph	137
Events List	140
Journal Panel	145
Tasks Panel	146
Related Indicators Panel	148
Toolbar Actions	149
Alerts List View	151
Workflow	151
What do you want to do?	151
Related Topics	152
Quick Look	152
Alerts List	154
Filters Panel	156
Overview Panel	158
Toolbar Actions	159
Alert Details View	160
Workflow	160
What do you want to do?	160
Related Topics	161

Quick Look	161
Overview Panel	162
Events Panel	163
Events List	163
Event Details	164
Event Metadata	164
Event Source or Destination Device Attributes	166
Event Source or Destination User Attributes	166
Toolbar Actions	166
Tasks List View	168
What do you want to do?	168
Related Topics	168
Quick Look	168
Tasks List	169
Filters Panel	171
Task Overview Panel	172
Toolbar Actions	174
Add/Remove from List Dialog	175
What do you want to do?	175
Related Topics	175
Quick Look	176
Context Lookup Panel - Respond View	179
What do you want to do?	179
Related Topics	179
Contextual Information Displayed in the Context Lookup Panel	180

NetWitness Respond Process

NetWitness 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 Respond enables you to configure rules that aggregate Alerts into Incidents. Alerts are 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 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 is created and the alert is 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.

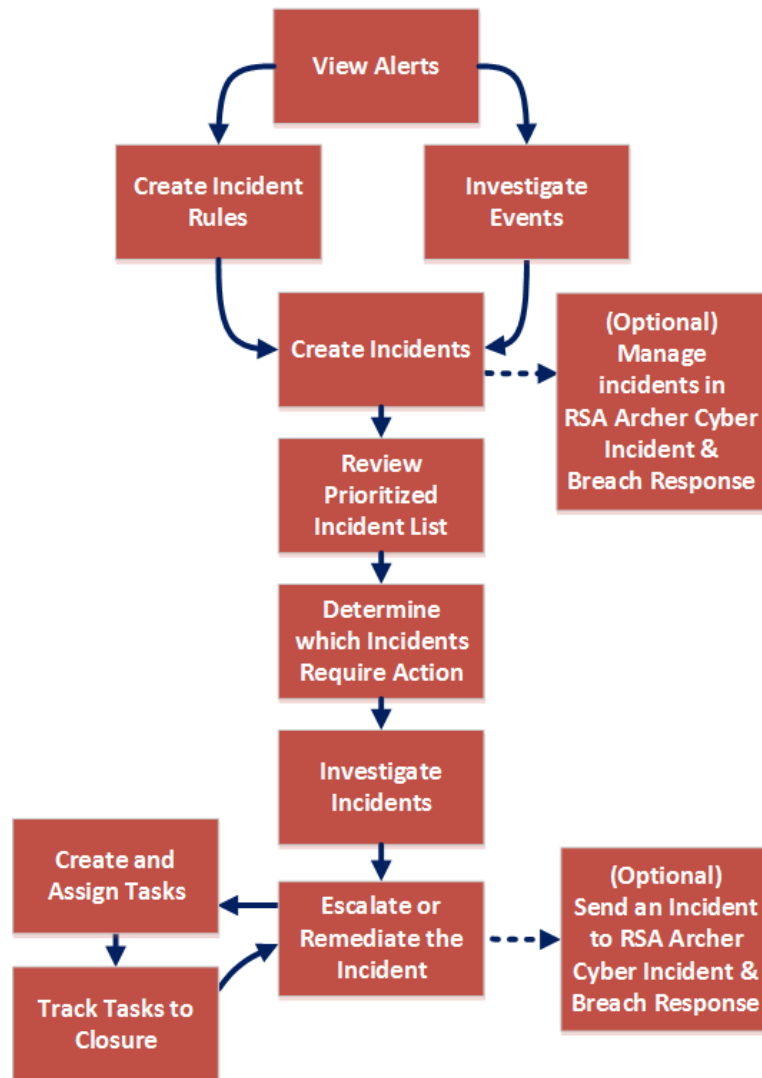
The stages in the NetWitness Respond process are:

- 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. In version 11.2 and later, if RSA Archer is configured as a data source in Context Hub, you can send incidents to RSA Archer® Cyber Incident & Breach Response.)

You also have the option of managing incidents in Archer Cyber Incident & Breach Response 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 RSA NetWitness® Platform 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.

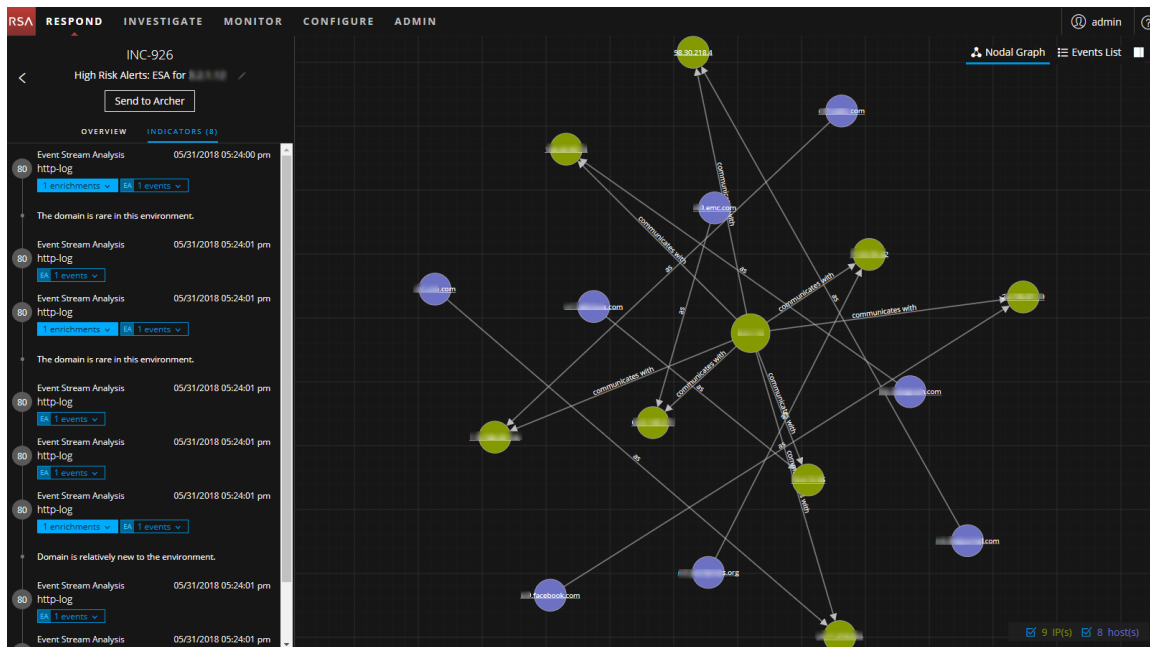
Within the Respond view, you can see Incidents, Alerts, and Tasks:

- **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 Platform 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.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
06/04/2018 04:59:52 pm	CRITICAL	90	INC-1707	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
06/04/2018 04:11:51 pm	CRITICAL	90	INC-1706	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 08:31:50 pm	CRITICAL	90	INC-1705	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 07:42:00 pm	CRITICAL	90	INC-1704	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1702	ESA	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1701	High Risk Alerts: ESA for 10.0.0.48	New		4
05/31/2018 05:24:52 pm	HIGH	80	INC-1700	High Risk Alerts: ESA for 10.0.0.48	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1699	High Risk Alerts: ESA for 10.0.0.48	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1698	High Risk Alerts: ESA for 10.0.1.11	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1697	High Risk Alerts: ESA for 10.0.0.196	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1696	High Risk Alerts: ESA for 10.0.0.53	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1695	High Risk Alerts: ESA for 10.0.1.20	New		1
05/31/2018 05:24:52 pm	MEDIUM	80	INC-1694	High Risk Alerts: ESA for 10.0.1.23	Assigned		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1693	High Risk Alerts: ESA for 10.0.2.232	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1692	High Risk Alerts: ESA for 10.0.3.93	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1691	High Risk Alerts: ESA for 10.0.0.166	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1690	High Risk Alerts: ESA for 10.0.0.28	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1689	High Risk Alerts: ESA for 10.0.3.140	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1688	High Risk Alerts: ESA for 10.0.3.142	New		1

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



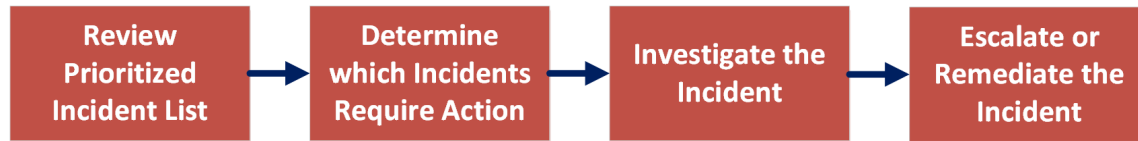
The Respond view is designed to make it easy to evaluate incidents, contextualize that data, collaborate with other analysts, and pivot to a deep-dive investigation as needed. The following figure shows an example of an event analysis in the Incident Details view.

REQUEST	Packet 1	Packet 2
000000	00 50 56 33 11 c8 00 50 56 33 11 c8 00 45 00	00 50 56 33 11 c8 00 50 56 33 11 c8 00 45 00
000016	00 3c 56 fd 40 00 40 06 55 8f 8a 04 3d 8c 8a 04	00 28 5e 7c 40 00 40 06 4e 24 8a 04 3d 1c 8a 04
000032	3d 1c 92 c4 11 9a 96 aa 05 38 00 00 00 a0 02	3d 8c 11 9a 92 c4 00 00 00 96 aa 05 39 50 14
000048	72 10 8e 5e 00 00 02 04 05 b4 04 02 00 0a 05 29	00 00 e1 5e 00 00 00 00 00 00 00 00 00 00 00
000064	53 c5 00 00 00 01 03 03 07	

EVENT META	SESSIONID	TIME	SIZE	PAYLOAD	MEDIUM	ETH.SRC	ETH.DST	ETH.TYPE	IP.SRC	IP.DST	IP.ALL	NETNAME	DIRECTION	IP.PROTO	TCP.FLAGS	TCP.SRCPORT	PORT.ALL	PORT.SRC.ALL	TCP.DSTPORT	PORT.ALL	PORT.DST.ALL	SERVICE	STREAMS
208294	05/31/2018 05:25:26 pm	134	0	1	00:50:56:33:11:C8	00:50:56:33:11:C8	00:50:56:33:11:C6	2048					lateral	6	22	37572	37572	37572	4506	4506	4506	0	2

Responding to Incidents Workflow

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



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.

This topic contains the following basic incident list procedures:

- [View the Incidents List](#)
- [Filter the Incident List](#)
- [Remove My Filters from the Incident List View](#)
- [View My Incidents](#)
- [Find an Incident](#)
- [Sort the Incidents List](#)
- [View Unassigned Incidents](#)
- [Assign Incidents to Myself](#)
- [Unassign an Incident](#)

View the Incidents List

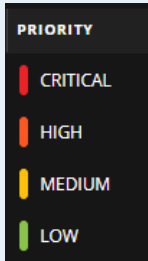
After logging in to NetWitness Platform, most Incident Responders see the Respond view, which is set as the default view. If you have a different initial view, you can navigate to the Respond view.

1. Log in to NetWitness Platform.

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

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
06/04/2018 04:59:52 pm	CRITICAL	90	INC-1707	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
06/04/2018 04:11:51 pm	CRITICAL	90	INC-1706	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 08:31:50 pm	CRITICAL	90	INC-1705	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 07:42:00 pm	CRITICAL	90	INC-1704	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1702	ESA	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1701	High Risk Alerts: ESA for 10.0.0.48	New		4
05/31/2018 05:24:52 pm	HIGH	80	INC-1700	High Risk Alerts: ESA for 10.0.0.48	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1699	High Risk Alerts: ESA for 10.0.0.48	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1698	High Risk Alerts: ESA for 10.0.1.11	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1697	High Risk Alerts: ESA for 10.0.0.196	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1696	High Risk Alerts: ESA for 10.0.0.53	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1695	High Risk Alerts: ESA for 10.0.1.20	New		1
05/31/2018 05:24:52 pm	MEDIUM	80	INC-1694	High Risk Alerts: ESA for 10.0.1.23	Assigned		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1693	High Risk Alerts: ESA for 10.0.2.232	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1692	High Risk Alerts: ESA for 10.0.3.93	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1691	High Risk Alerts: ESA for 10.0.0.166	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1690	High Risk Alerts: ESA for 10.0.0.28	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1689	High Risk Alerts: ESA for 10.0.3.140	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1688	High Risk Alerts: ESA for 10.0.3.142	New		1

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	<p>Shows the incident priority. Priority can be Critical, High, Medium or Low.</p> <p>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:</p> 
RISK SCORE	Shows the incident risk score. The risk score indicates the risk of the incident as calculated using an algorithm and is between 0-100. 100 is the highest risk score.

Column	Description
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 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]

SENT TO ARCHER

- ☐ Yes
- ☐ No

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 can 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.

Filters

TIME RANGE ☒ **CUSTOM DATE RANGE**

START DATE
04/01/2018 12:00:00 PM

END DATE
04/23/2018 12:00:00 PM

APRIL 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12


12 : 00 : 00 PM

- **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.
- **SENT TO ARCHER:** (In version 11.2 and later, if RSA Archer is configured as a data source in Context Hub, you can send incidents to Archer Cyber Incident & Breach Response and this option

will be available in NetWitness Respond.) To view incidents that were sent to Archer, select **Yes**. For incidents that were not sent to Archer, select **No**.


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 1000 out of 91205 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 Platform 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

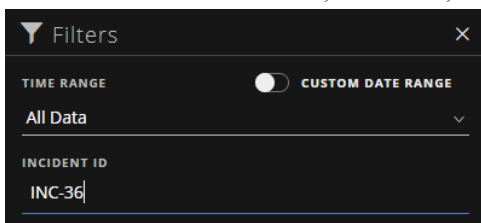
You can view your incidents by filtering the incidents by your username.

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-36.

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

The screenshot shows the NetWitness Respond interface with the 'Incidents' tab selected. On the left, a 'Filters' sidebar is open, showing various filter categories: TIME RANGE (All Data), INCIDENT ID (INC-36), PRIORITY (Low, Medium, High, Critical), STATUS (New, Assigned, In Progress, Task Requested, Task Complete, Closed, Closed - False Positive), ASSIGNEE, CATEGORIES, and SENT TO ARCHER (Yes, No). The main incident list on the right shows one item: INC-36, Suspected C&C with [redacted].com, Status: New, Alerts: 1. The interface includes buttons for 'Change Priority', 'Change Status', 'Change Assignee', and 'Delete'.

Sort the Incidents List

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

	CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
<input type="checkbox"/>	04/23/2018 10:08:04 pm	MEDIUM	70	INC-97571	Investigate - IP	Assigned	Analyst User	3
<input type="checkbox"/>	04/23/2018 10:08:04 pm	MEDIUM	70	INC-97570	Investigate - IP	Assigned	Analyst User	0
<input type="checkbox"/>	04/23/2018 10:08:04 pm	MEDIUM	70	INC-97569	Investigate - IP	Assigned	Analyst User	3


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

For example, to prioritize the incidents, you can sort your view by clicking the Priority column header.

The following figure shows the incidents list sorted by Priority in ascending order  (lowest priority on top).

	CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
<input type="checkbox"/>	03/21/2018 07:57:47 pm	LOW	10	INC-15	Web Threat Detection for	Task Requested		1
<input type="checkbox"/>	03/21/2018 07:59:52 pm	LOW	10	INC-17	High Risk Alerts: ESA for 1...	New		7
<input type="checkbox"/>	03/21/2018 07:59:52 pm	LOW	10	INC-18	High Risk Alerts: ESA for 9...	New		7


To sort by Priority in descending order (highest priority on top), click the Priority column header again. The highest priority incidents are at the top as shown in the following figure.

Incidents Alerts Tasks								
	Change Priority	Change Status	Change Assignee	Delete				
<input type="checkbox"/>	CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
<input type="checkbox"/>	04/16/2018 06:24:15 pm	CRITICAL	50	INC-97525	Incident with special chara...	Assigned	admin	12
<input type="checkbox"/>	04/12/2018 07:43:12 pm	CRITICAL	100	INC-91235	High Risk Alerts: Malware ...	New		1
<input type="checkbox"/>	04/12/2018 07:37:15 pm	CRITICAL	100	INC-91234	High Risk Alerts: Malware ...	New		2

View Unassigned Incidents

Note: 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**.

ASSIGNEE

☒ Show only unassigned incidents

The incidents list is 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.

The screenshot displays the NetWitness Respond Incident List view. The top navigation bar includes RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The user 'admin' is logged in. The 'Incidents' tab is active, showing a table of incidents. The table has columns for CREATED, PRIORITY, ASSIGNEE, NAME, STATUS, ASSIGNEE, and ALERTS. A dropdown menu is open for the 'Change Assignee' button, showing a list of users including 'admin' and 'Analyst User'. The 'Analyst User' is highlighted. The table contains 17 incidents, all with a status of 'New' and a priority of 'HIGH'.

CREATED	PRIORITY	ASSIGNEE	NAME	STATUS	ASSIGNEE	ALERTS
04/12/2018 10:51:16 pm	HIGH	admin	Suspected C&C with www.rivoblog.com	New		1
04/12/2018 10:51:16 pm	HIGH	Analyst User	Suspected C&C with photos-979.ll.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97522	Suspected C&C with espn.starwave.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97521	Suspected C&C with photos-896.ll.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97520	Suspected C&C with ly115w.bay115.mail.live.com	New		2
04/12/2018 10:51:16 pm	HIGH	INC-97519	Suspected C&C with www.professional-resume-example.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97518	Suspected C&C with graphics.cstv.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97517	Suspected C&C with dcc.weather.com	New		2
04/12/2018 10:51:16 pm	HIGH	INC-97516	Suspected C&C with cl.exot.net	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97515	Suspected C&C with i7.photobucket.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97514	Suspected C&C with ad.yieldmanager.com	New		10
04/12/2018 10:51:16 pm	HIGH	INC-97513	Suspected C&C with userpic.livejournal.com	New		3
04/12/2018 10:51:16 pm	HIGH	INC-97512	Suspected C&C with www.californiapsychics.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97511	Suspected C&C with my.gwu.edu	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97510	Suspected C&C with photos-193.ll.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97509	Suspected C&C with photos-285.ll.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97508	Suspected C&C with icons-pe.woug.com	New		2
04/12/2018 10:51:16 pm	HIGH	INC-97507	Suspected C&C with am6.sitemeter.com	New		1
04/12/2018 10:51:16 pm	HIGH	INC-97506	Suspected C&C with photos-2.ak.facebook.com	New		17

Showing 1000 out of 97524 items | 3 selected

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

The screenshot shows the 'Confirm Update' dialog box. The title bar is 'Confirm Update' with a close button. The main text reads: 'You are about to make the following changes to more than one item:'. Below this, it displays the following information: 'Field: Assignee', 'Value: Analyst User', and 'Number of items: 4'. At the bottom, there are 'Cancel' and 'OK' buttons.

You can see a successful change notification.

RSA

RESPOND

INVESTIGATE

MONITOR

CONFIGURE

ADMIN

admin

Incidents

Alerts

Tasks

✓

Your change was successful

×

Change Priority

Change Status

Change Assignee

Delete

	CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
<input checked="" type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97524	Suspected C&C with www.tivoblog.com	Assigned	Analyst User	1
<input checked="" type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97523	Suspected C&C with photos-979.jl.facebook.com	Assigned	Analyst User	1
<input checked="" type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97522	Suspected C&C with espn.starwave.com	Assigned	Analyst User	1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97521	Suspected C&C with photos-896.jl.facebook.com	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97520	Suspected C&C with by115u.bay115.mail.live.com	New		2
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97519	Suspected C&C with www.professional-resume-example.com	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97518	Suspected C&C with graphics.cstv.com	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97517	Suspected C&C with dco.weather.com	New		2
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97516	Suspected C&C with clexart.net	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97515	Suspected C&C with i7.photobucket.com	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97514	Suspected C&C with ad.yieldmanager.com	New		10
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97513	Suspected C&C with userpic.livejournal.com	New		3
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97512	Suspected C&C with www.californiapsychics.com	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97511	Suspected C&C with my.gwu.edu	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97510	Suspected C&C with photos-193.jl.facebook.com	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97509	Suspected C&C with photos-285.jl.facebook.com	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97508	Suspected C&C with icons-pe.woup.com	New		2
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97507	Suspected C&C with sm6.sitemeter.com	New		1
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97506	Suspected C&C with photos-cak.facebook.com	New		17

Showing 1000 out of 97524 items | 3 selected

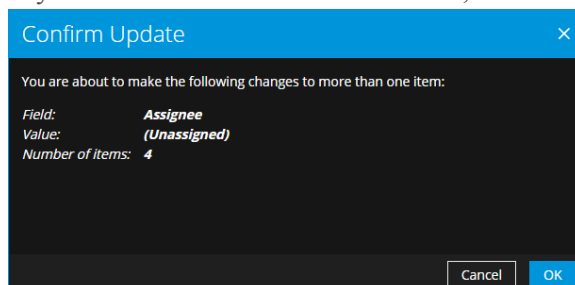
Unassign an Incident

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	PRIORITY	RISK	NAME	STATUS	ASSIGNEE	ALERTS
04/04/2018 06:26:41 pm	HIGH	50	High Risk Alerts: Reporting Engine for 10.4...	Assigned	Analyst User	2
04/04/2018 06:25:41 pm	HIGH	50	High Risk Alerts: Reporting Engine for 10.4...	Assigned	Analyst User	1
04/04/2018 06:23:36 pm	HIGH	50	High Risk Alerts: Reporting Engine for 10.4...	Assigned	Analyst User	1
04/04/2018 06:11:40 pm	HIGH	50	INC-91230 High Risk Alerts: Reporting Engine for 10.4...	Assigned	Analyst User	1
04/04/2018 06:10:39 pm	HIGH	50	INC-91229 High Risk Alerts: Reporting Engine for 10.4...	New		1
04/04/2018 06:07:42 pm	HIGH	70	INC-91228 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91227 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91226 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91225 High Risk Alerts: ESA for ...	New		4
04/04/2018 06:07:42 pm	HIGH	70	INC-91224 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91223 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91222 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91221 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91220 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91219 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91218 High Risk Alerts: ESA for ...	New		2
04/04/2018 06:07:42 pm	HIGH	70	INC-91217 High Risk Alerts: ESA for ...	New		2

Showing 1000 out of 91232 items | 4 selected

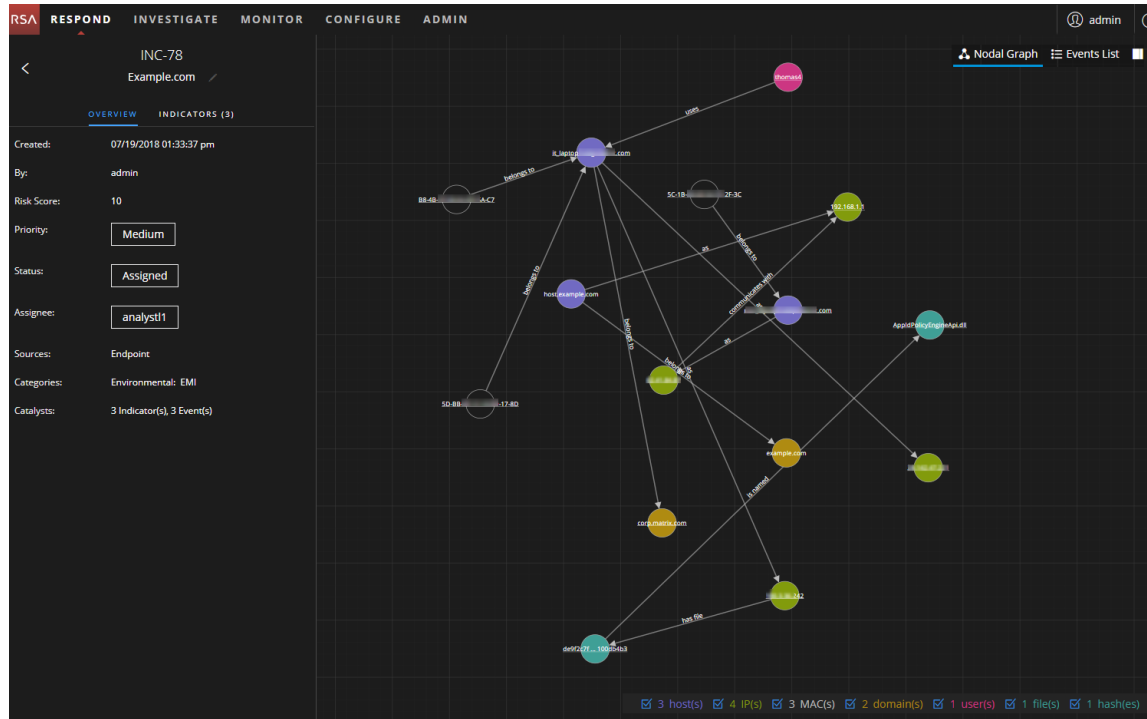
3. If you selected more than one incident, in the Confirm Update dialog, click **OK**.



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.



You can perform the following procedures in the Incident Details view to determine the action required on an incident:

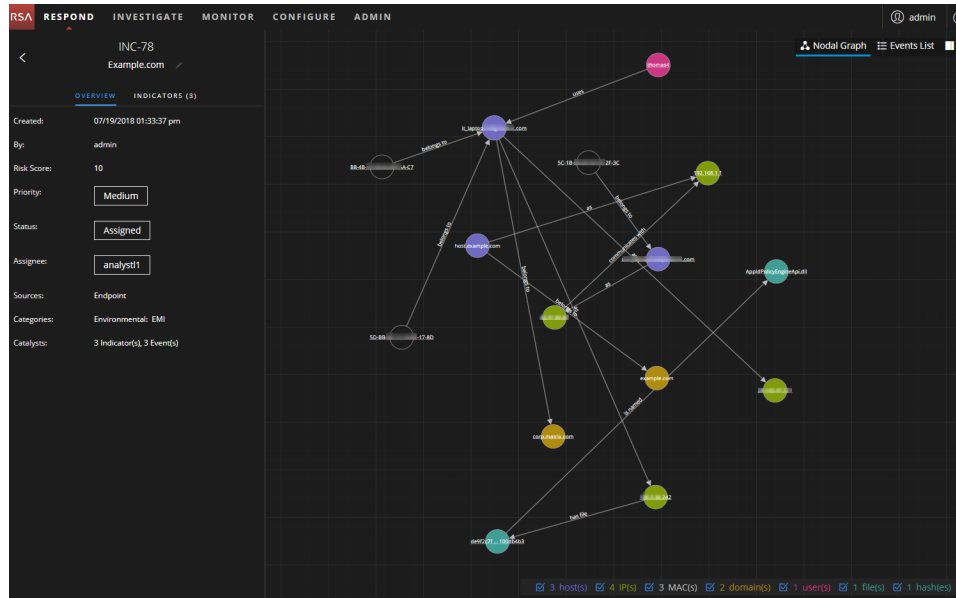
- [View Incident Details](#)
- [View Basic Summary Information about the Incident](#)
- [View the Indicators and Enrichments](#)
- [View and Study the Events](#)
- [View C2 Enrichment Information for Suspected C&C Incidents](#)
- [View and Study the Entities Involved in the Events](#)
- [Select Node Types to View on the Nodal Graph](#)
- [Filter the Data in the Incident Details View](#)
- [View the Tasks associated with an Incident](#)
- [View Incident Notes](#)
- [Find Related Indicators](#)
- [Add Related Indicators to the Incident](#)

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
07/13/2018 04:49:21 pm	HIGH	60	INC-59	High Risk Alerts: ESA for 60.0	New		7
07/13/2018 04:49:22 pm	HIGH	50	INC-60	High Risk Alerts: ESA for 50.0	New		4
07/13/2018 04:49:22 pm	CRITICAL	90	INC-61	High Risk Alerts: ESA for 90.0	New		1
07/13/2018 04:49:22 pm	HIGH	70	INC-62	High Risk Alerts: ESA for 70.0	New		7
07/13/2018 04:49:27 pm	CRITICAL	100	INC-63	High Risk Alerts: Malware Analysis for 100.0	New		4
07/13/2018 04:49:27 pm	CRITICAL	100	INC-64	High Risk Alerts: Malware Analysis for 100.0	New		1
07/13/2018 04:49:27 pm	CRITICAL	90	INC-65	High Risk Alerts: Malware Analysis for 90.0	New		4
07/13/2018 04:49:27 pm	CRITICAL	90	INC-66	High Risk Alerts: Malware Analysis for 90.0	New		4
07/13/2018 04:49:27 pm	CRITICAL	90	INC-67	High Risk Alerts: Malware Analysis for 90.0	New		5
07/13/2018 04:49:27 pm	CRITICAL	90	INC-68	High Risk Alerts: Malware Analysis for 90.0	New		4
07/13/2018 04:49:27 pm	CRITICAL	90	INC-69	High Risk Alerts: Malware Analysis for 90.0	New		1
07/13/2018 04:49:27 pm	CRITICAL	90	INC-70	High Risk Alerts: Malware Analysis for 90.0	New		1
07/13/2018 04:49:27 pm	CRITICAL	90	INC-71	High Risk Alerts: Malware Analysis for 90.0	New		1
07/13/2018 04:49:32 pm	HIGH	60	INC-72	High Risk Alerts: Reporting Engine for 60.0	New		9
07/13/2018 04:49:32 pm	HIGH	70	INC-73	High Risk Alerts: Reporting Engine for 70.0	New		9
07/13/2018 04:49:48 pm	LOW	10	INC-74	Web Threat Detection for	New		1
07/13/2018 04:49:48 pm	HIGH	50	INC-75	Web Threat Detection for WTD IncidentId 98	New		1
07/13/2018 05:17:32 pm	HIGH	70	INC-76	Custom Advance Rule for Tue Aug 12 13:53:4...	Assigned	Respond	7
07/13/2018 05:27:41 pm	LOW	10	INC-77	Copy of Custom Advance Rule for Sun Aug 13...	Assigned	Respond	14
07/19/2018 01:33:37 pm	MEDIUM	10	INC-78	Example.com	Assigned	analyst1	3

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



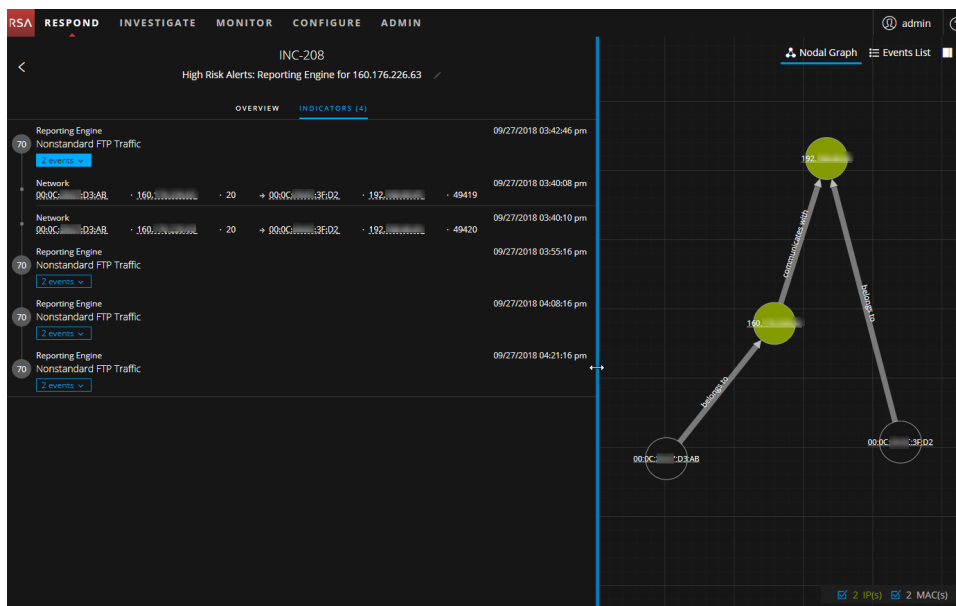
The Incident Details view has the following panels:

- **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 send the incident to RSA Archer

and 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 List:** The Events List, 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 the top of 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, Action on Objective, Containment, Eradication, and Closure), 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 Platform 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:

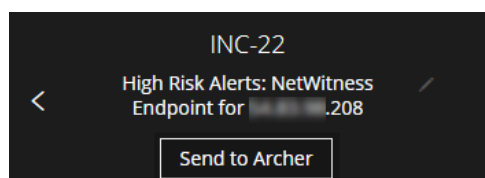


View Basic Summary Information about the Incident

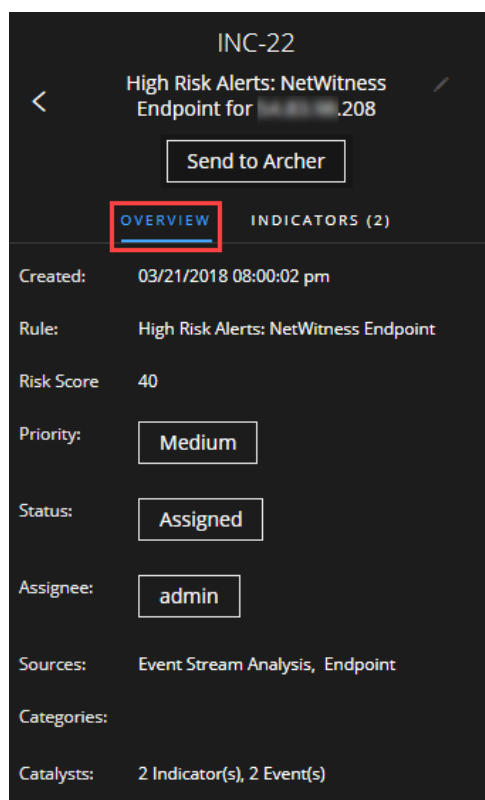
You can view basic summary information about an incident in the Overview panel.

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.
- **Send to Archer / Sent to Archer:** (In version 11.2 and later, if RSA Archer is configured as a data source in Context Hub, you can send incidents to Archer Cyber Incident & Breach Response and this option is available in NetWitness Respond.) This shows whether an incident has been sent to Archer Cyber Incident & Breach Response. An incident sent to Archer shows as Sent to Archer. An incident that has not been sent to Archer shows as Send to Archer. You can click the Send to Archer button to send the incident to Archer Cyber Incident & Breach Response.



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 screenshot displays the NetWitness Respond interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. Below this, the 'Incidents' tab is active, showing a list of incidents. The incident list has columns for 'CREATED', 'PRIORITY', 'RISK SCORE', 'ID', 'NAME', 'STATUS', 'ASSIGNEE', and 'ALERTS'. Incident INC-22 is selected, and its details are shown in the 'OVERVIEW' panel on the right.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
03/21/2018 07:57:37 pm	CRITICAL	90	INC-14	High Risk Alerts: Malware Analysis for 10.1...	New		1
03/21/2018 07:57:47 pm	LOW	10	INC-15	Web Threat Detection for	Task Requested		1
03/21/2018 07:57:47 pm	HIGH	50	INC-16	Web Threat Detection for WTD IncidentId 98	New		1
03/21/2018 07:59:52 pm	LOW	10	INC-17	High Risk Alerts: ESA for 10.100.229.36	New		7
03/21/2018 07:59:52 pm	LOW	10	INC-18	High Risk Alerts: ESA for	New		7
03/21/2018 07:59:52 pm	LOW	10	INC-19	High Risk Alerts: ESA for	New		7
03/21/2018 07:59:52 pm	MEDIUM	25	INC-20	High Risk Alerts: ESA for 10.42.42.211	New		2
03/21/2018 07:59:52 pm	LOW	10	INC-21	High Risk Alerts: ESA for 10.81.10.30	New		7
03/21/2018 08:00:02 pm	MEDIUM	40	INC-22	High Risk Alerts: NetWitness Endpoint for ...	Assigned	admin	2
03/21/2018 08:00:02 pm	LOW	10	INC-23	High Risk Alerts: NetWitness Endpoint for ...	Assigned	admin	1
03/21/2018 08:00:02 pm	LOW	10	INC-24	High Risk Alerts: NetWitness Endpoint for ...	Assigned	admin	1
03/21/2018 08:00:02 pm	LOW	10	INC-25	High Risk Alerts: NetWitness Endpoint for ...	Assigned		1
03/21/2018 08:00:02 pm	CRITICAL	10	INC-26	High Risk Alerts: NetWitness Endpoint for ...	In Progress	deploy_admin	1
03/21/2018 08:00:02 pm	LOW	10	INC-27	High Risk Alerts: NetWitness Endpoint for ...	Task Requested	admin	1
04/03/2018 02:02:04 pm	HIGH	60	INC-28	High Risk Alerts: Reporting Engine for	New		1
04/03/2018 02:10:38 pm	HIGH	70	INC-29	High Risk Alerts: Reporting Engine for 192	New		1
04/03/2018 02:20:58 pm	HIGH	70	INC-30	High Risk Alerts: Reporting Engine for 192	New		1
04/03/2018 02:28:36 pm	CRITICAL	90	INC-31	High Risk Alerts: Malware Analysis for 10.1...	New		1
04/03/2018 02:30:12 pm	HIGH	50	INC-32	High Risk Alerts: ESA for 10.42.42.211	In Progress		1
04/03/2018 02:31:12 pm	LOW	10	INC-33	Web Threat Detection for	In Progress		1

The Overview panel for INC-22 shows the following details:

- Created:** 03/21/2018 08:00:02 pm
- Rule:** High Risk Alerts: NetWitness Endpoint
- Risk Score:** 40
- Priority:** Medium
- Status:** Assigned
- Assignee:** admin
- Sources:** Event Stream Analysis, Endpoint
- Categories:**
- Catalysts:** 2 Indicator(s), 2 Event(s)

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

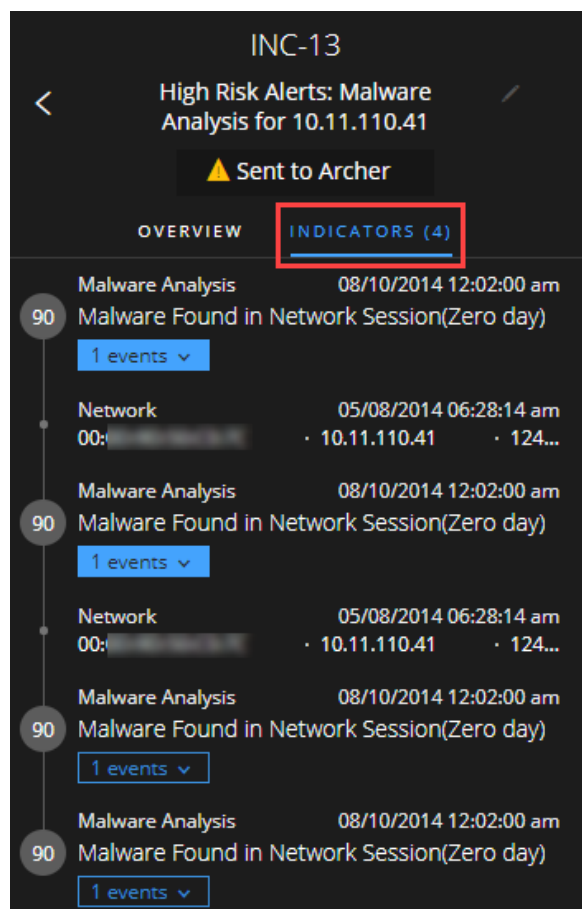
- **Created:** Shows the creation date and time of the incident.
- **Rule / By:** Shows the name of the rule that created the incident or the name of the person who created the incident.
- **Risk Score:** Indicates the risk of the incident as calculated via an algorithm and is between 0-100. 100 is the 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.

Note: The maximum number of indicators (alerts) displayed in the Indicators panel is 1,000.

View and Study the Events

You can view and study the events associated with the incident from the Events List. 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:

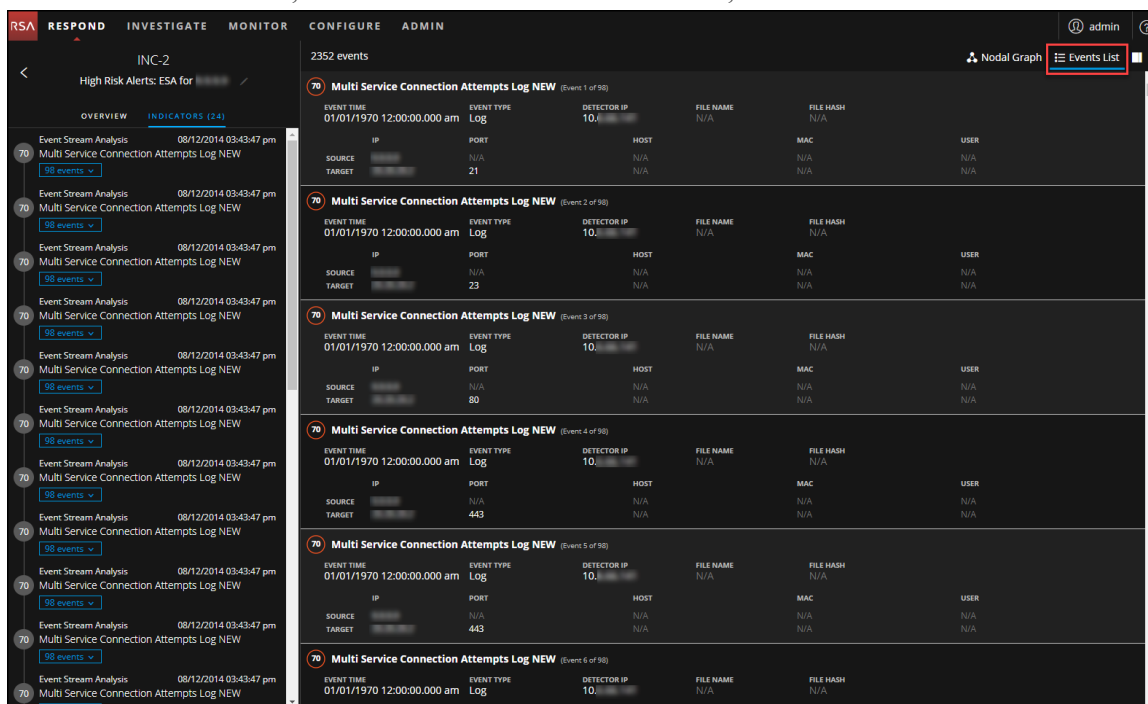
- A transaction between two machines (a Source and a Destination)
- An anomaly detected on a single machine (a Detector)

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 List, in the Incident Details view toolbar, click .



The screenshot displays the NetWitness Respond interface for incident INC-2. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main content area shows a list of events under the heading '2352 events'. The 'Events List' button in the top right corner of the main content area is highlighted with a red box. The list of events includes details such as Event Time, Event Type, Detector IP, File Name, File Hash, Source IP, Port, Host, MAC, and User. The events are categorized as 'Multi Service Connection Attempts Log NEW'.

The Events List shows different information about each event depending on the event type. The maximum number of events displayed in the Events List is 1,000.

The following table lists typical event information. For details specific to endpoint events, see [Events List](#).

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

- Click the top of an event in the Events List to view the event details.
This example shows the event details for a selected event in the list.

The screenshot displays the NetWitness Respond interface. On the left, the 'INC-2' incident is active, showing a list of events under the 'INDICATORS (24)' tab. The main panel shows the details for a selected event, 'Multi Service Connection Attempts Log NEW' (Event 1 of 98). The event details are organized into several sections:

- Event Summary:** Event Time: 01/01/1970 12:00:00.000 am, Event Type: Log, Detector IP: 10.1.1.1, File Name: N/A, File Hash: N/A.
- Source Information:** IP: 10.1.1.1, Port: 21, Host: N/A, MAC: N/A, User: N/A.
- Target Information:** IP: 10.1.1.1, Port: 23, Host: N/A, MAC: N/A, User: N/A.
- Geolocation:** Country: United States, City: N/A, Latitude: N/A, Longitude: N/A.
- Organization:** Corporation: N/A.
- Device Information:** Device Class: Firewall, IP Address: 10.1.1.1, Product Name: ciscoasa, Size: 152, Data Size: 152, Device Type: ciscoasa.
- Event Source:** Concentrator: local:50005, Event Source ID: 28742, Target Domain: csc.com.
- Related Links:** [Investigate Original Event](#)

- To view the events for a specific indicator (alert), click the indicator in the Indicators panel on the left to view the events for that indicator in the Events List on the right.
This example shows the events for a selected indicator.

The screenshot displays the NetWitness Respond interface. On the left, the 'INC-2' incident is active, showing a list of events under the 'INDICATORS (24)' tab. The main panel shows the events for a selected indicator, 'Multi Service Connection Attempts Log NEW' (Event 1 of 98). The events are listed in a table with columns for Event Time, Event Type, Detector IP, File Name, File Hash, and User. The events are filtered by the selected indicator, showing a list of events for 'Multi Service Connection Attempts Log NEW'.

- To view event details for a specific indicator event, select an event in the Indicators panel. Click the top of the event to view the details.

The following example shows information for the selected event.

The screenshot displays the NetWitness Respond interface. On the left, the 'INC-2' panel shows a list of events under 'High Risk Alerts: ESA for'. The selected event is 'Multi Service Connection Attempts Log NEW'. The main panel shows the event details for this event, including source and target information, geolocation, and related links.

EVENT TIME	EVENT TYPE	DETECTOR IP	FILE NAME	FILE HASH
01/01/1970 12:00:00 am	Log	10.10.10.10	N/A	N/A

SOURCE	TARGET	DETECTOR
DEVICE	DEVICE	DEVICE CLASS
IP ADDRESS	PORT	Firewall
10.10.10.10	80	
GEOLOCATION	IP ADDRESS	IP ADDRESS
COUNTRY	10.10.10.10	10.10.10.10
United States		
CITY	GEOLOCATION	PRODUCT NAME
United States	COUNTRY	ciscoasa
LATITUDE	CITY	SIZE
152	152	152
DATA	SIZE	152
152	152	152
DEVICE TYPE	EVENT SOURCE	
ciscoasa	Concentrator	Local50005
EVENT SOURCE ID	28743	
TARGET DOMAIN	csc.com	

RELATED LINKS
[Investigate Original Event](#)

If you have additional Investigate-server permissions, you can also access Event Analysis details for events. See [View Event Analysis Details for Indicators](#). If you have the UEBA_Analysts role, you can access UEBA details for indicators. See [View User Entity Behavior Analytics for Indicators](#).

View C2 Enrichment Information for Suspected C&C Incidents

Note: This procedure applies to incidents from ESA Analytics in NetWitness Platform 11.3 and later.

The Events List in version 11.3 does not show the Command and Control (C2) enrichment information for HTTP packet alerts in Suspected C&C incidents. However, you can view the C2 enrichment information in the Alert Details view.

- Go to **RESPOND > Incidents**, look for a **Suspected C&C** incident, and note the incident ID.

The screenshot displays the NetWitness Respond interface, specifically the 'Incidents' panel. The 'Filters' section shows 'All Data' selected. The 'Incident ID' field is set to 'e.g., INC-123'. The 'Priority' section shows 'High' selected. The table below lists incidents with columns for 'CREATED', 'PRIORITY', 'RISK S...', 'ID', 'NAME', 'STATUS', 'ASSIGNEE', and 'ALERTS'.

CREATED	PRIORITY	RISK S...	ID	NAME	STATUS	ASSIGNEE	ALERTS
02/25/2019 03:45:07 pm	HIGH	80	INC-14070	High Risk Alerts: ESA for...	New		2
02/25/2019 03:43:00 pm	HIGH	80	INC-14068	Suspected C&C with mu...	New		6
02/25/2019 03:43:00 pm	HIGH	80	INC-14067	Suspected C&C with pk...	New		1
02/25/2019 03:43:00 pm	HIGH	80	INC-14066	Suspected C&C with sys...	New		1
02/25/2019 03:43:00 pm	HIGH	80	INC-14065	Suspected C&C with pk...	New		1
02/25/2019 03:40:01 pm	HIGH	80	INC-14064	Suspected C&C with to...	New		1

2. Go to **RESPOND > Alerts** and in the Filters panel, select the following to locate an alert in the Alerts list with the incident ID noted above:
 - a. In the **Part of Incident** section, select **Yes**.
 - b. In **Alert Names** section, select **http-packet**.

If you are still not able to locate an alert in the Alerts list with the incident ID noted above, try filtering your alerts list more using the time range of the incident.

The screenshot shows the NetWitness Respond interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'Alerts' tab is active. On the left, the 'Filters' panel is expanded, showing 'Part of Incident' set to 'Yes' and 'Alert Names' with 'http-packet' selected. The main table displays a list of alerts with columns: CREATED, SEVERITY, NAME, SOURCE, # EVENTS, HOST SUMMARY, and INCIDENT ID. One alert is highlighted in red, showing a severity of 80 and a name of 'http-packet'.

3. In the Alerts list, click the **http-packet** link in the **NAME** field of the alert associated with the incident ID.
The Event Details view shows the C2 enrichment information.

The screenshot shows the 'Event Details' view for an 'http-packet' alert. The left sidebar displays incident information: Incident ID: INC-14086, Created: 02/25/2019 03:49:00 pm, Severity: 80, Source: Event Stream Analysis, Type: Network, # Events: 1, and Host Summary. The main panel shows event details for the timestamp 02/25/2019 03:33:08 pm. The 'Enrichment' section is expanded, showing details for 'Domain Registration' and 'Command and Control'. The 'Domain Registration' section includes fields like Domain, Registrar, and Risk Score. The 'Command and Control' section includes fields like Confidence, Score, and Period.

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.)

In NetWitness Platform 11.3 events, nodes for source filename and file hash are supported, but nodes for target filename and file hash are not supported.

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

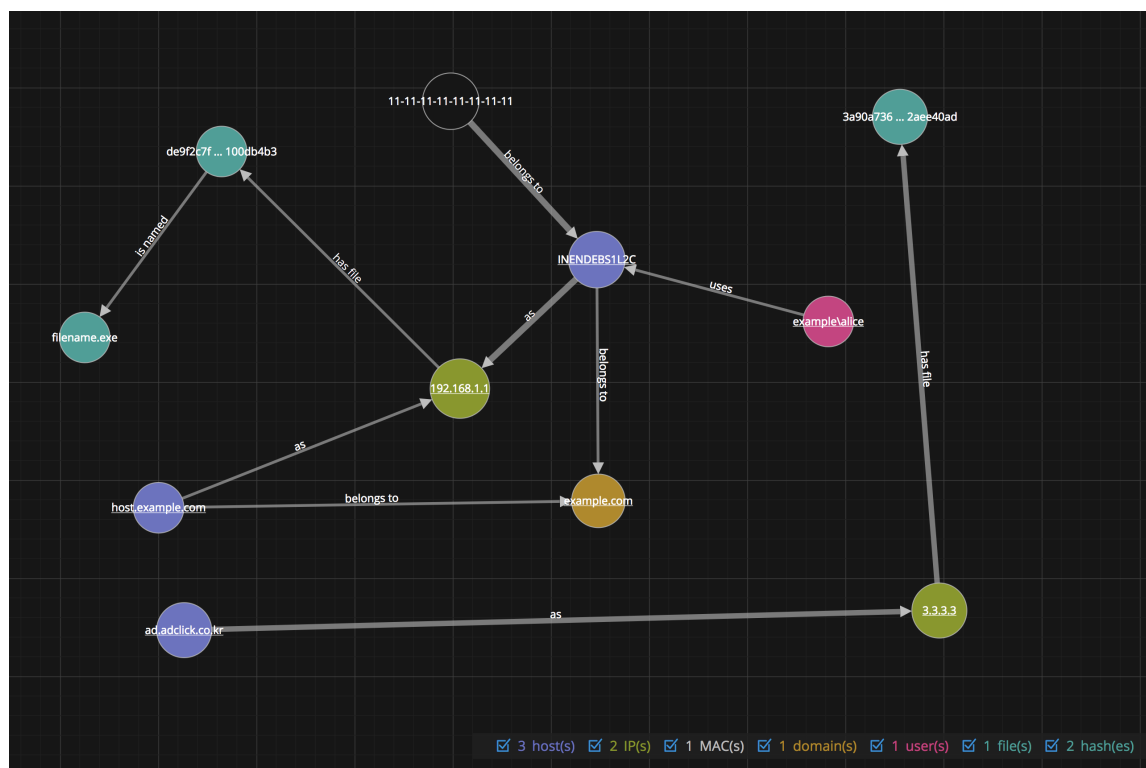
You can click any node and drag it to reposition it.

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 an 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 11 nodes.



In this example, notice that there are two IP nodes. They both have hashed 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 11-11-11-11-11-11-11-11-11-11 and Alice uses it.

Select Node Types to View on the Nodal Graph

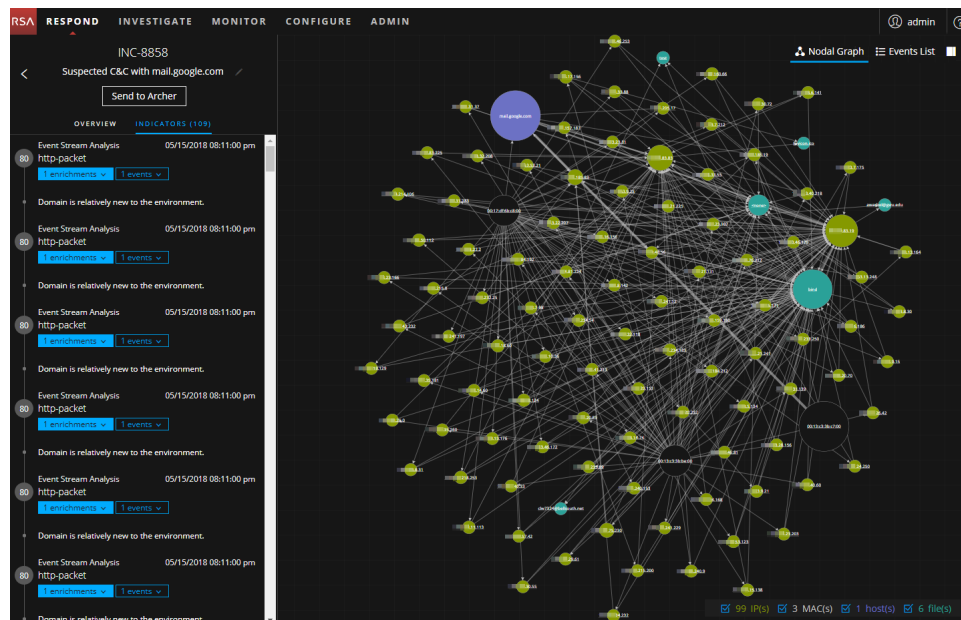
Note: This option is available in version 11.2 and later.

In the Incident Details view nodal graph, you can hide node types to further study the interactions between the entities on the nodal graph.

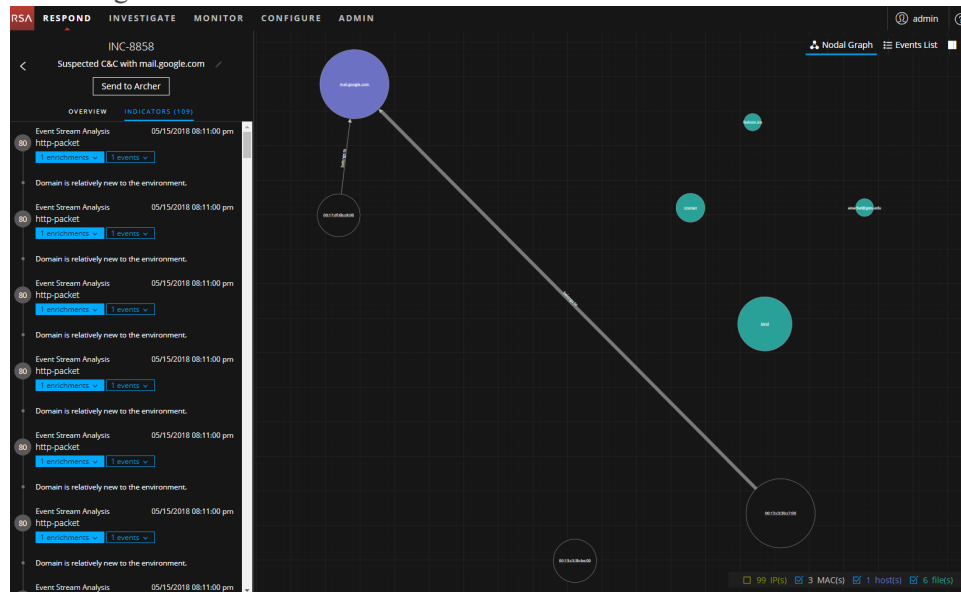
1. Go to **RESPOND > Incidents**.
2. In the Incidents List view, choose an incident to view and then click the link in the **ID** or **NAME** column for that incident.
The Incident Details view for the selected incident appears with the Nodal Graph in view. The legend below the nodal graph has all of the entity node types selected by default.

- To include (unhide) node types, select the checkbox for the node types that you would like to appear in the nodal graph.

Hiding node types can be especially helpful if the nodal diagram includes over 100 nodes as shown in the following figure.



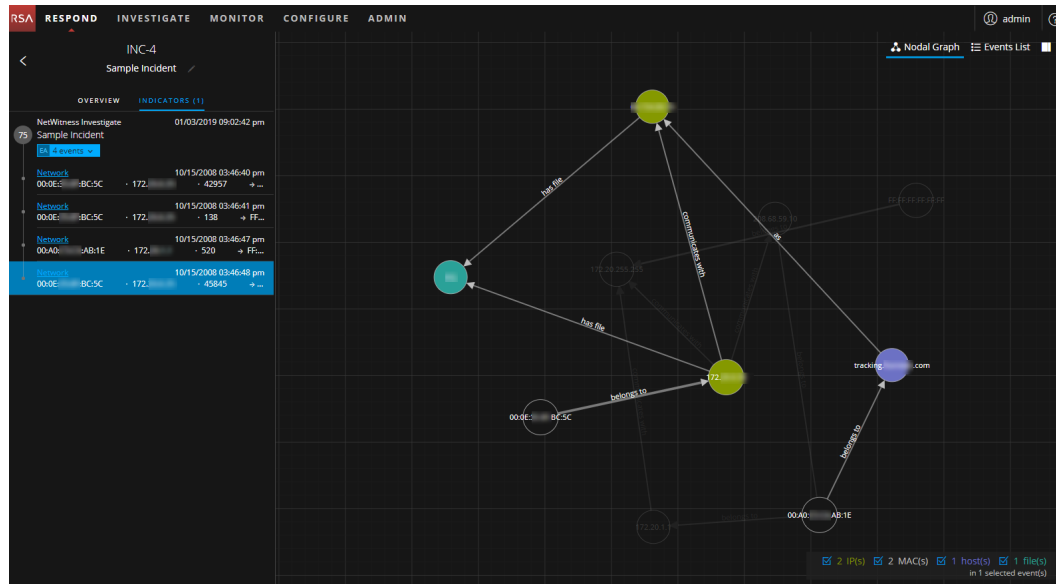
After hiding the IP node types, you can get a better understanding of what is happening with the remaining nodes.



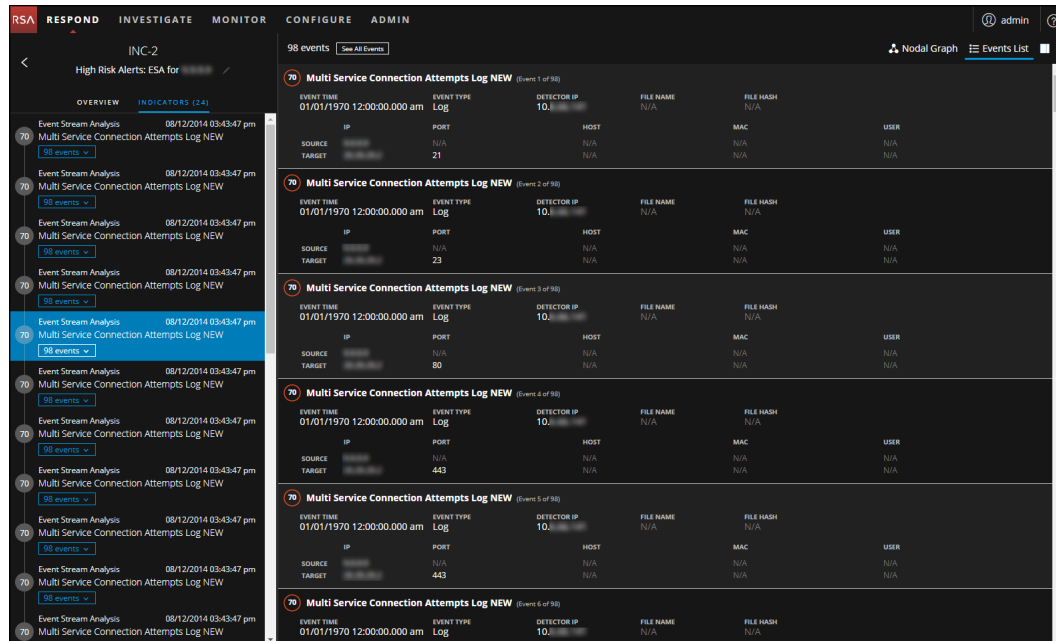
Filter the Data in the Incident Details View

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 ninety-eight events. The filtered Events List shows those ninety-eight events.



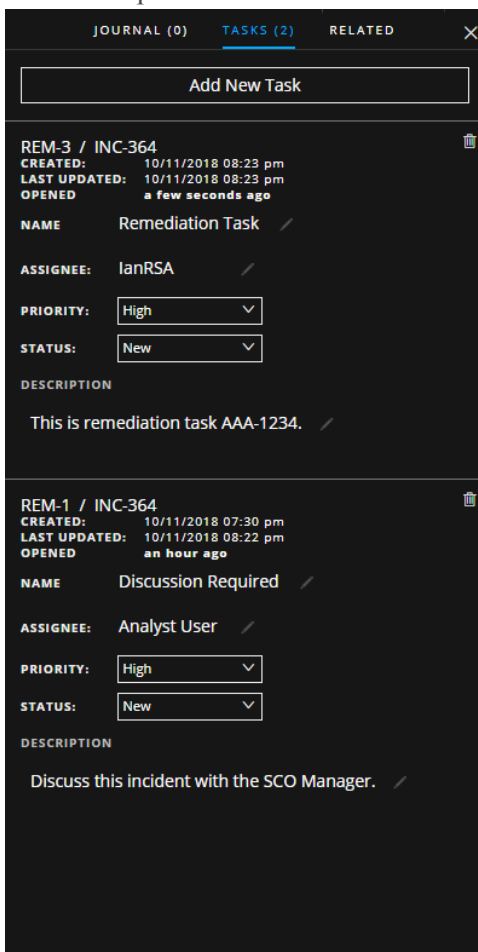
View the Tasks associated with an Incident

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.



JOURNAL (0) **TASKS (2)** RELATED X

Add New Task

REM-3 / INC-364
CREATED: 10/11/2018 08:23 pm
LAST UPDATED: 10/11/2018 08:23 pm
OPENED a few seconds ago

NAME Remediation Task /

ASSIGNEE: IanRSA /

PRIORITY: High ▾

STATUS: New ▾

DESCRIPTION
This is remediation task AAA-1234. /

REM-1 / INC-364
CREATED: 10/11/2018 07:30 pm
LAST UPDATED: 10/11/2018 08:22 pm
OPENED an hour ago

NAME Discussion Required /

ASSIGNEE: Analyst User /

PRIORITY: High ▾

STATUS: New ▾

DESCRIPTION
Discuss this incident with the SCO Manager. /

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

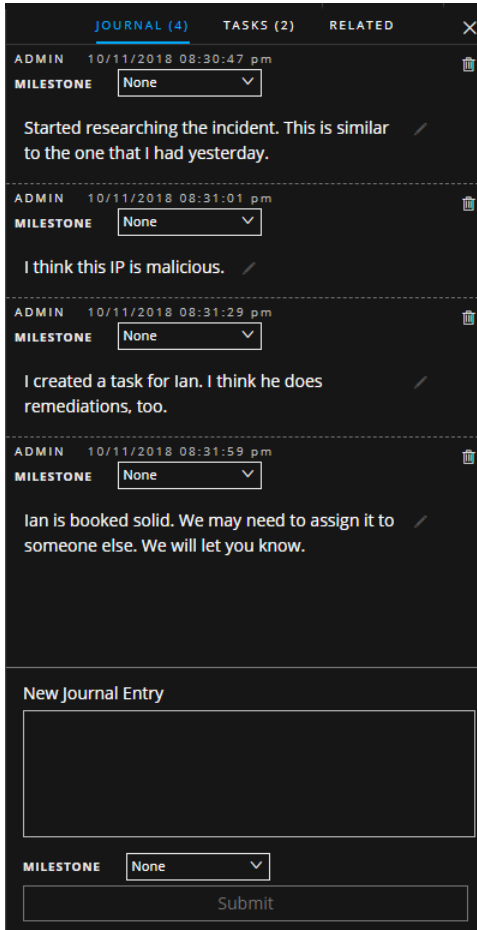
View Incident Notes

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.



The screenshot shows the 'JOURNAL (4)' panel with the following entries:

ADMIN	10/11/2018 08:30:47 pm	MILESTONE	None	
				Started researching the incident. This is similar to the one that I had yesterday.
ADMIN	10/11/2018 08:31:01 pm	MILESTONE	None	
				I think this IP is malicious.
ADMIN	10/11/2018 08:31:29 pm	MILESTONE	None	
				I created a task for Ian. I think he does remediations, too.
ADMIN	10/11/2018 08:31:59 pm	MILESTONE	None	
				Ian is booked solid. We may need to assign it to someone else. We will let you know.

New Journal Entry


MILESTONE

Find Related Indicators

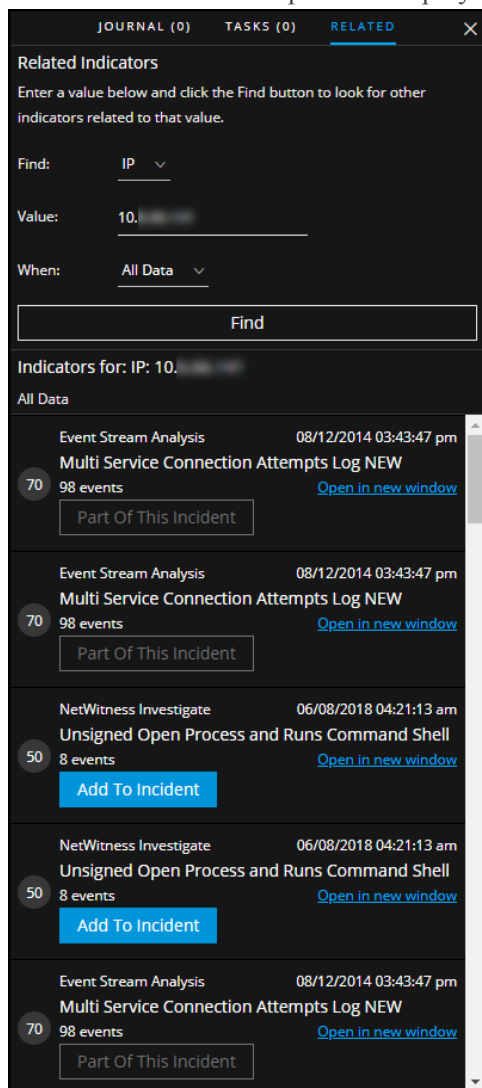
Related Indicators are alerts that were not originally part of the selected incident, but they are related in some way to the incident. The relationship may or may not be obvious. For example, related indicators can involve one or more entities from the incident, but they can also be related due to some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

In the Incident Details view Related Indicators 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.

4. Click the **RELATED** tab. The Related Indicators panel is displayed.



5. In the **Find** field, select the entity type to search, such as IP.
6. In the **Value** field, type a value for the entity, such as a specific IP address.
7. In the **When** field, select the time period to search, such as the Last 24 Hours.

8. 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 Indicators panel, do a search to find related indicators. See [Find Related Indicators](#) above.

The screenshot shows the 'Related Indicators' panel in NetWitness Respond. At the top, there are tabs for 'JOURNAL (0)', 'TASKS (0)', and 'RELATED'. The 'RELATED' tab is active. Below the tabs, there's a search section with the title 'Related Indicators' and instructions: 'Enter a value below and click the Find button to look for other indicators related to that value.' The search fields are: 'Find:' with a dropdown menu set to 'IP', 'Value:' with the text '10.10.10.10', and 'When:' with a dropdown menu set to 'All Data'. Below these fields is a 'Find' button. The results section is titled 'Indicators for: IP: 10.10.10.10' and shows a list of indicators. Each entry includes a count in a circle (e.g., 70, 50), the event name, the date/time, and a status (e.g., 'NEW'). Some entries have an 'Add To Incident' button, while others have a 'Part Of This Incident' button. A 'Part Of This Incident' button is also present at the top of the results list.

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**.

The screenshot displays the NetWitness Respond interface for incident INC-2. The left sidebar shows a list of indicators, including 'Multi Service Connection Attempts Log NEW' and 'NetWitness Investigate Unsigned Open Process and Runs Command Shell'. The main panel shows details for the selected indicator, including event time, event type, detector IP, file name, file hash, and source/target information. The right sidebar shows the 'Related Indicators' panel, which lists indicators related to the current incident. A red box highlights the 'Add To Incident' button in the 'Related Indicators' panel, and a red arrow points to the 'Add To Incident' button in the 'Related Indicators' panel.

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.

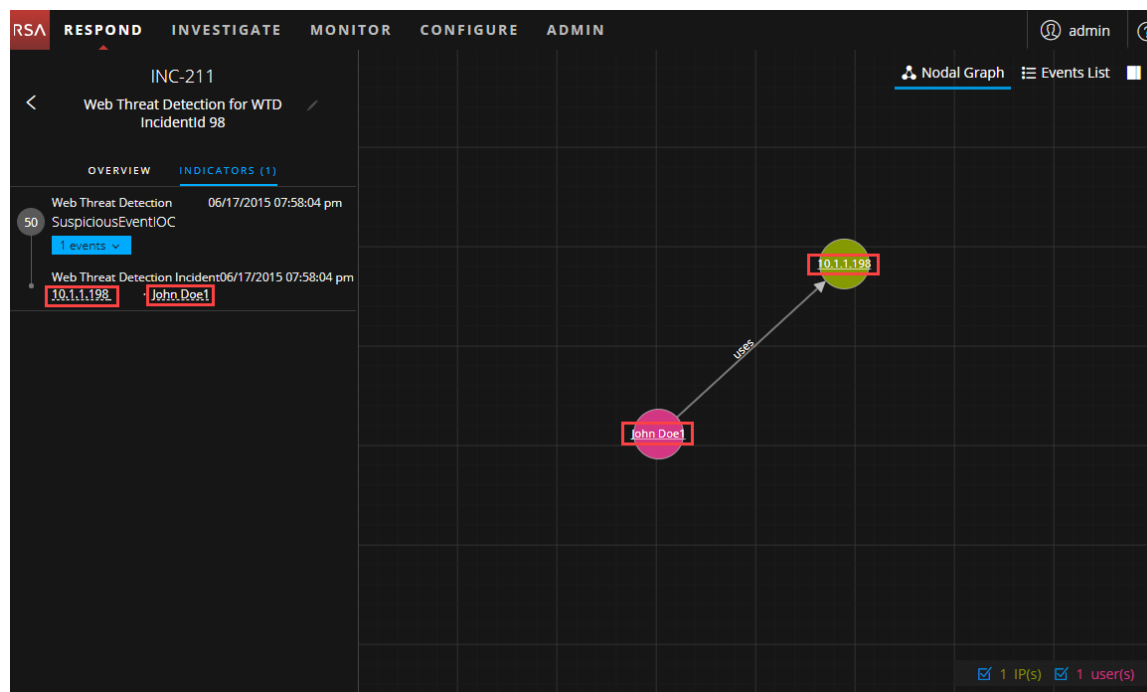
You can perform the following procedures to further investigate an incident:

- [View Contextual Information](#)
- [Add an Entity to a Whitelist](#)
- [Create a List](#)
- [View the Reputation Status of a File Hash](#)
- [Pivot to Investigate > Navigate](#)
- [Pivot to Investigate > Hosts/Files](#)
- [Pivot to NetWitness Endpoint Thick Client](#)
- [Pivot to Archer](#)
- [View Event Analysis Details for Indicators](#)
- [View User Entity Behavior Analytics for Indicators](#)
- [Document Steps Taken Outside of NetWitness](#)
 - [View the Journal Entries for an Incident](#)
 - [Add a Note](#)
 - [Delete a Note](#)

View Contextual Information

In the Indicators panel, Events List, or the Nodal Graph, you can view the underlined entities. If an entity is underlined, NetWitness Platform 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 Events list details.

The screenshot shows the NetWitness Respond interface. On the left, the 'INC-211' incident is selected, showing 'Web Threat Detection for WTD IncidentId 98'. The 'OVERVIEW' tab is active, displaying a list of events. One event, 'Web Threat Detection SuspiciousEventIOC', is highlighted. A context tooltip is shown for this event, displaying the following information:

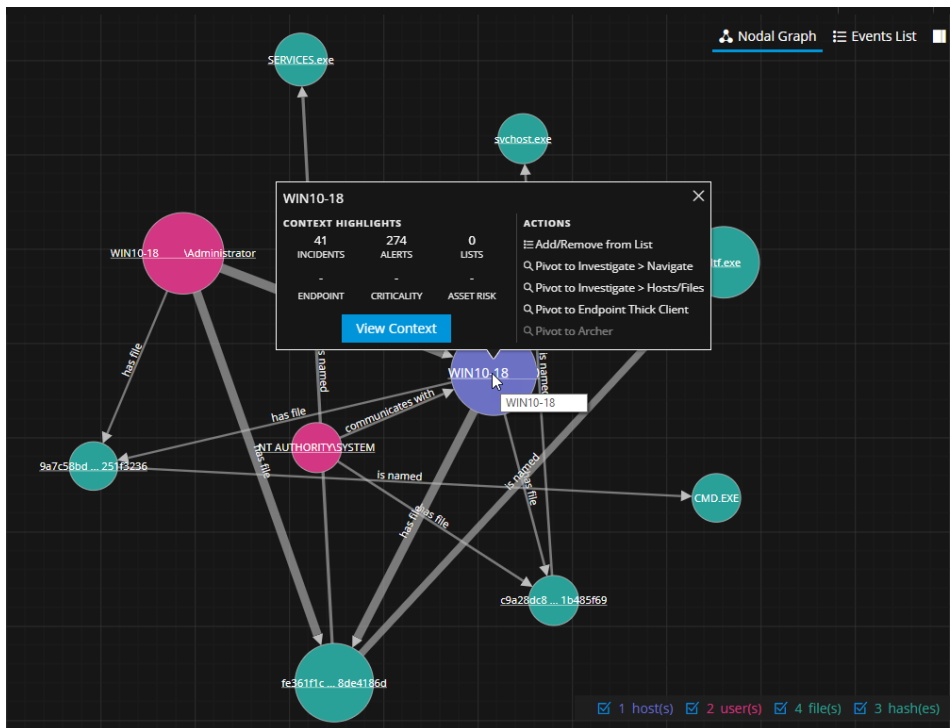
1 event	
SuspiciousEventIOC (Event 1 of 1)	
EVENT TIME	06/17/2015 07:58:04 pm
EVENT TYPE	Web Threat D...
DETECTOR IP	N/A
FILE NAME	N/A
FILE HASH	N/A
SOURCE	
USER	John.Doe1
USERNAME	John.Doe1
DEVICE	10.1.1.198
IP ADDRESS	10.1.1.198
RULECOMMENT	
Triggered when retail wire exceeds \$3000	
RULE	retail_wire_over_3000
RELATED LINKS	
View Original Event (in Wtd)	
SCORE	
N/A	
NAME	
Retail Wire Over 3000	
DETAILS	
Retail wire amount is 150,000	
USER	
John Doe1	
TENANT	
tenant1	

The Context Hub is preconfigured with meta fields mapped to the entities. NetWitness Respond and NetWitness 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*.

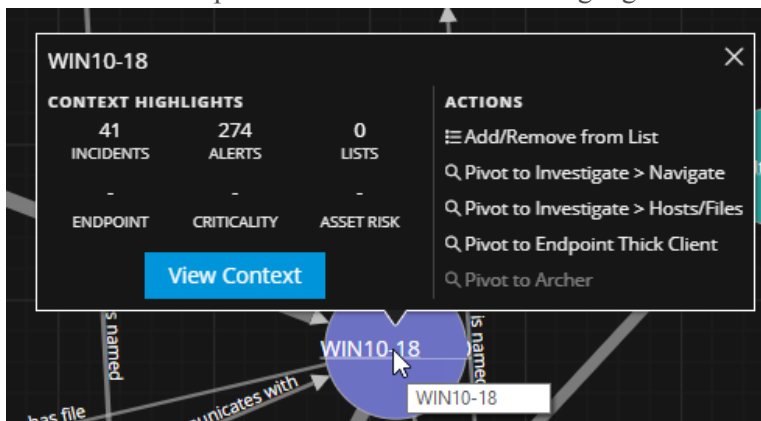
Caution: For the Context Lookup to work correctly in the Respond and Investigate views, RSA recommends that when mapping meta keys in the **ADMIN > System > Investigation > Context Lookup** tab, you add only meta keys to the Meta Key Mappings, not fields in the MongoDB. For example, `ip.address` is a 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, 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, Live Connect, Criticality, Asset Risk, and Reputation. Depending on your data, you may be able to click these items for more information.

The above example shows 41 related incidents, 274 alerts, 0 lists for the selected host, and no information available for endpoint, criticality, and asset risk.

- The **Actions** section lists the available actions. In the above example, the Add/Remove from List, Pivot to Investigate > Navigate, Pivot to Investigate > Hosts/Files and Pivot to Endpoint Thick Client options are available.

Note: The Pivot to Archer link is disabled when Archer data is not available or when the Archer data source is not responding. Check that the RSA Archer configuration is enabled and configured properly.

For more information, see [Pivot to Investigate > Navigate](#), [Pivot to Archer](#), [Pivot to NetWitness Endpoint Thick Client](#), [Pivot to Investigate > Hosts/Files](#), 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 host. It lists all of the incidents that mention that host.

The screenshot shows the NetWitness Respond interface with the Context Hub Lookup panel open for entity INC-1070. The panel displays a list of incidents related to the entity, including details like Created, Priority, Risk Score, ID, Name, Status, Assignee, and Alerts.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
03/14/2019 03:30:03 pm (25 minutes ago)	CRITICAL	100	INC-1070	Threshold Breached for HOST WIN10-18	NEW		1
03/14/2019 03:30:02 pm (25 minutes ago)	CRITICAL	100	INC-1069	Threshold Breached for FILE def.exe	NEW		1
03/14/2019 03:29:56 pm (25 minutes ago)	HIGH	70	INC-1066	High Risk Alerts: NetWitness Endpoint fo...	NEW		1
03/14/2019 03:29:56 pm (25 minutes ago)	HIGH	70	INC-1065	High Risk Alerts: NetWitness Endpoint fo...	NEW		1
03/14/2019 03:29:56 pm (25 minutes ago)	HIGH	70	INC-1064	High Risk Alerts: NetWitness Endpoint fo...	NEW		1
03/14/2019 03:29:56 pm (25 minutes ago)	HIGH	70	INC-1063	High Risk Alerts: NetWitness Endpoint fo...	NEW		11
03/14/2019 03:29:55 pm (25 minutes ago)	HIGH	75	INC-1062	High Risk Alerts: NetWitness Endpoint fo...	NEW		28
03/14/2019 03:29:55 pm (25 minutes ago)	HIGH	72	INC-1061	High Risk Alerts: NetWitness Endpoint fo...	NEW		9
03/14/2019 03:29:55 pm (25 minutes ago)	HIGH	70	INC-1060	High Risk Alerts: NetWitness Endpoint fo...	NEW		1
03/14/2019 03:29:55 pm (25 minutes ago)	HIGH	70	INC-1059	High Risk Alerts: NetWitness Endpoint fo...	NEW		1
03/14/2019 03:29:55 pm (25 minutes ago)	HIGH	70	INC-1058	High Risk Alerts: NetWitness Endpoint fo...	NEW		1
03/14/2019 03:29:55 pm (25 minutes ago)	HIGH	70	INC-1057	High Risk Alerts: NetWitness Endpoint fo...	NEW		1
03/14/2019 03:29:55 pm (25 minutes ago)	HIGH	70	INC-1056	High Risk Alerts: NetWitness Endpoint fo...	NEW		11
03/14/2019 03:29:55 pm (25 minutes ago)	HIGH	70	INC-1055	High Risk Alerts: NetWitness Endpoint fo...	NEW		2
03/14/2019 03:29:55 pm (25 minutes ago)	HIGH	70	INC-1054	High Risk Alerts: NetWitness Endpoint fo...	NEW		2

41 Incident(s) (First 50 Results) Time Window: 7 DAYS | Last Updated: 17 minutes ago

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

Add an Entity to a Whitelist

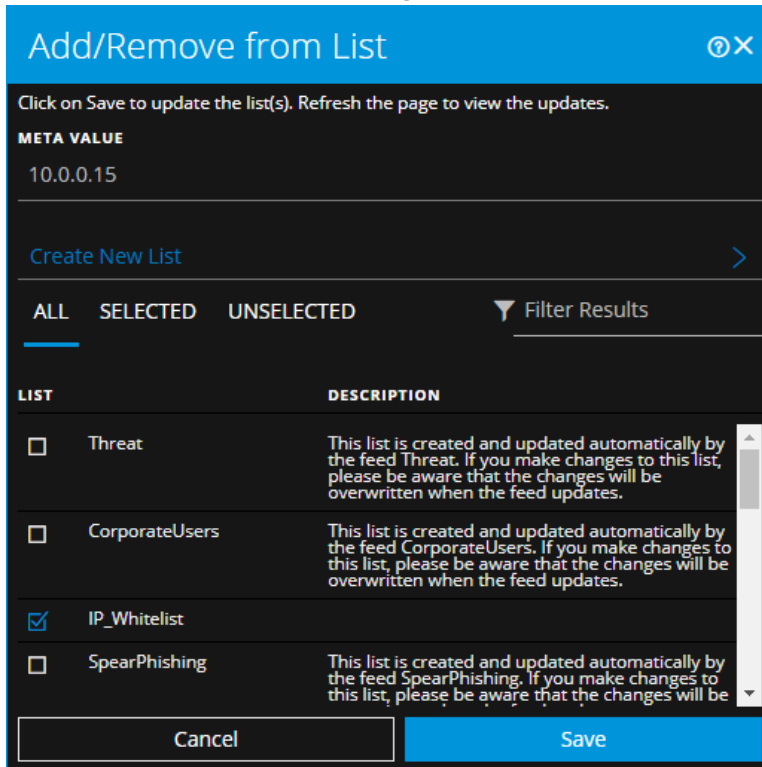
You can add any underlined entity to a list, such as a Whitelist or Blacklist, from a context tooltip. For example, to reduce false positives, you may want to whitelist an underlined domain to exclude it from the related entities.

- In the Indicators panel, Events List, 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.

The screenshot shows a context tooltip for IP address 10.0.0.15. The tooltip displays 'CONTEXT HIGHLIGHTS' with 158 INCIDENTS, 232 ALERTS, and 2 LISTS. It also shows 'ACTIONS' including 'Add/Remove from List', 'Pivot to Investigate > Navigate', 'Pivot to Investigate > Hosts/Files', 'Pivot to Endpoint Thick Client', and 'Pivot to Archer'. A 'View Context' button is visible at the bottom.

- In the **ACTIONS** section of the tooltip, click **Add/Remove from List**.
The Add/Remove from List dialog shows the available lists.



- Select one or more lists and click **Save**.
The entity appears on the selected lists.
[Add/Remove from List Dialog](#) provides additional information.

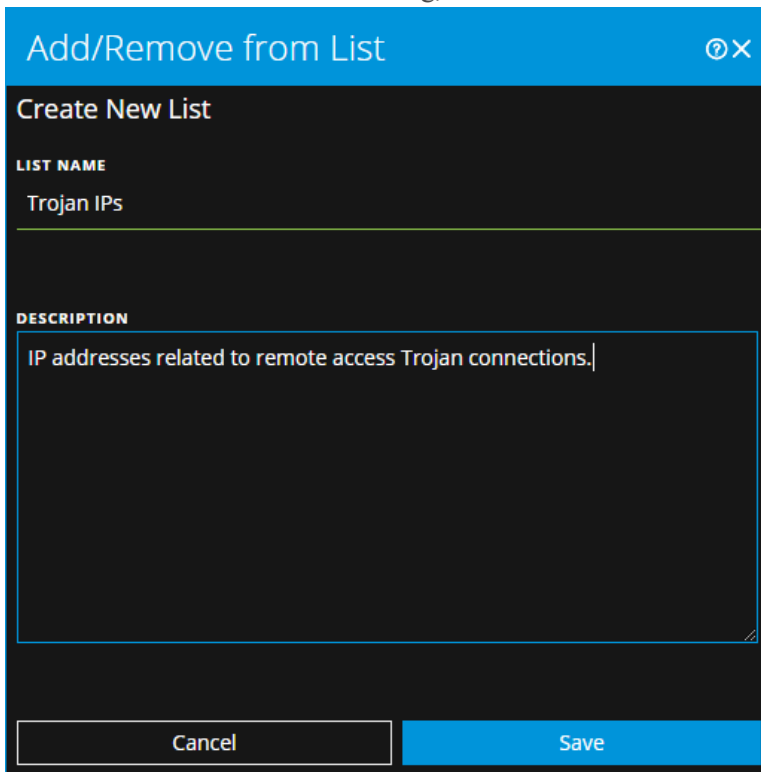
Create a List

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:

- In the Indicators panel, Events List, 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.
- In the **ACTIONS** section of the tooltip, click **Add/Remove from List**.

3. In the Add/Remove from List dialog, click **Create New List**.



The screenshot shows a dialog box titled "Add/Remove from List". Inside, there's a section "Create New List". It has two input fields: "LIST NAME" with the value "Trojan IPs" and "DESCRIPTION" with the value "IP addresses related to remote access Trojan connections.". At the bottom, there are "Cancel" and "Save" buttons.

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.

View the Reputation Status of a File Hash

The File Reputation service available on RSA Live checks the reputation of every file hash against an extensive database of known file hashes updated in real-time. The file reputation is displayed on the **Investigate** and **Respond** views. On **View Context** lookup, if the reputation status changes, Context Hub notifies the change in reputation status to all Endpoint servers. Information about the file hash such as any suspicious or malicious activity on the file is populated from Context Hub. There may be additional information available about that entity in the Context Hub.

The following table describes the file hash reputations.

Reputation	Description
Malicious	File hash is labeled as malicious.
Suspicious	File hash is suspected to be malicious.
Unknown	File hash is not known.

Reputation	Description
Known	File hash information is known to the file reputation service and does not have any previous bad record.
Known Good	File hash information is known good, such as files signed by Microsoft or RSA.
Invalid	File hash format is invalid.

Note: A reputation status is visible for a file hash entity only and File Reputation service supports maximum of 10 million files for a reputation of file hash..

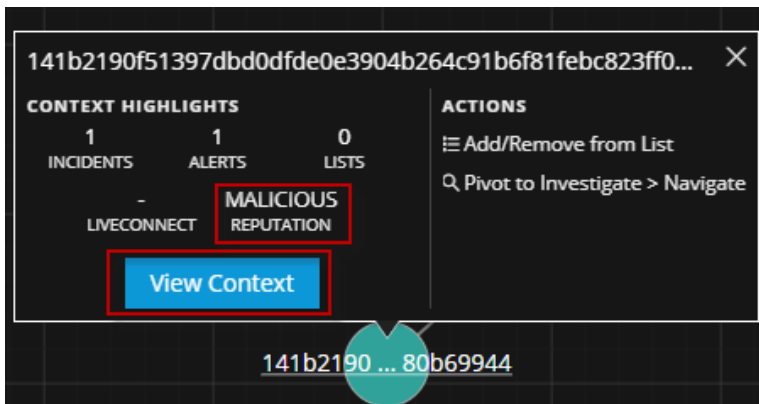
The suspicious or malicious files are available for further analysis in the **Investigate > Navigate** view and **Investigate > Event Analysis** view. For more information on the file reputation service, see the *Live Services Management Guide* the *Endpoint User Guide*.

To view the reputation of a file hash:


1. Go to **RESPOND > Incidents**.
2. In the Incidents List view, choose an incident to view and then click the link in the **ID** or **NAME** column for that incident.
The Incident Details view is displayed.

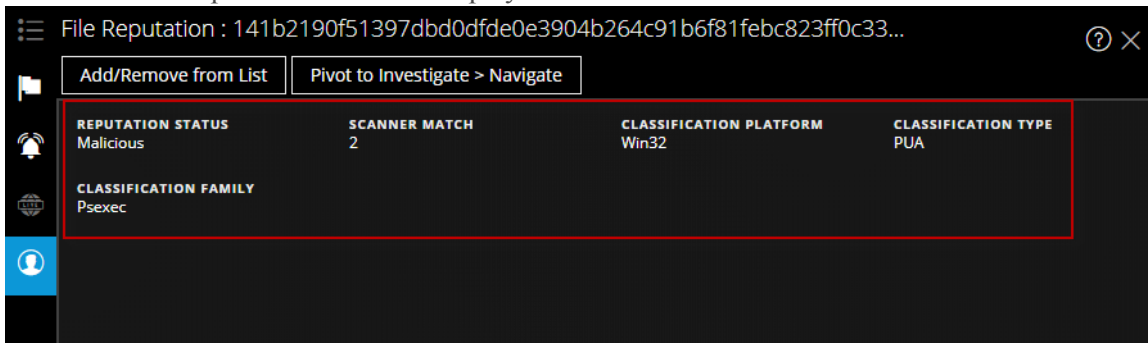
The screenshot shows the NetWitness Respond web interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The left sidebar contains a 'Filters' panel with sections for TIME RANGE, INCIDENT ID, PRIORITY, and STATUS. The main content area is titled 'Incidents' and features a table with columns: CREATED, PRI..., MIS..., ID, NAME, STATUS, and ASSIGNEE. The first row of the table is highlighted with a red box, showing an incident with ID 'INC-5' and NAME 'Malicious -141b2190f51397dbd0d...'. The table also includes action buttons like 'Change Priority', 'Change Status', 'Change Assignee', and 'Delete'.

3. Hover over the file hash entity.
The context tooltip displays the reputation status of the selected file hash entity.



4. Click **View Context** or **REPUTATION** to view the reputation status information.

5. Click **File Reputation** datasource  to view further details.
The details for reputation status are displayed.



Pivot to Investigate > Navigate

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

1. In the Indicators panel, Events List, 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 > Navigate**.
The Investigate Navigate view opens, which enables you to perform a deep dive investigation.

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

Pivot to Investigate > Hosts/Files

For a more thorough information about specific Hosts and Files, you can access the Investigate Hosts and Files views.

1. In the Indicators panel, Events List, or the Nodal Graph, hover over any entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Investigate > Hosts/Files**.
If you hover over a host or IP or MAC address entity and click **Pivot to Investigate > Hosts/Files**, it

displays the **Investigate > Hosts** view with a specific host listed.

If you hover over a filename or file hash entity and click **Pivot to Investigate > Hosts/Files** it displays the **Investigate > Files** view with a specific file listed.

Note: By default, the search for entities is on the previously selected Endpoint Server. However, you can select a different Endpoint Server to fetch the information or data.

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

Pivot to NetWitness Endpoint Thick Client

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.

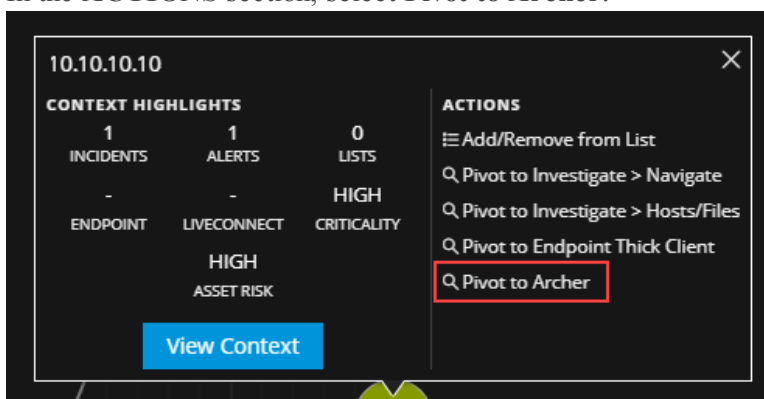
1. In the Indicators panel, Events List, or the Nodal Graph, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Endpoint Thick Client**.
The NetWitness Endpoint thick client application opens outside of your web browser.

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

Pivot to Archer

For viewing more details about the device in RSA Archer® Cyber Incident & Breach Response, you can pivot to the device details page. This information is displayed only for IP address, host, and Mac address.

1. In the Indicators panel, Events List, or the Nodal Graph, hover over any underlined entity (IP address, host, and Mac address) to access a context tooltip.
2. In the **ACTIONS** section, select **Pivot to Archer**.



3. The device details page in **RSA Archer Cyber Incident & Breach Response** opens if you are logged in to the application, otherwise the login screen is displayed.

Note: The Pivot to Archer link is disabled when Archer data is not available or when the Archer Datasource is not responding. Check that the RSA Archer configuration is enabled and configured properly.

For more information, see the *RSA Archer Integration Guide*.

View Event Analysis Details for Indicators

In the Incident Details view Indicators panel, you can drill deeper into the events associated with the listed indicators to get a better understanding of the events. In the Event Analysis panel, you can view raw events and metadata with interactive features that enhance your ability to find meaningful patterns in the data. You can examine network, log, and endpoint events in the Event Analysis panel. The Event Analysis panel in the Respond view shows the Event Analysis view from Investigate for specific indicator events. For detailed information about the Event Analysis view, see the *NetWitness Investigate User Guide*.

Note: You must have the following Investigate-server permissions to view Event Analysis in the Respond view:

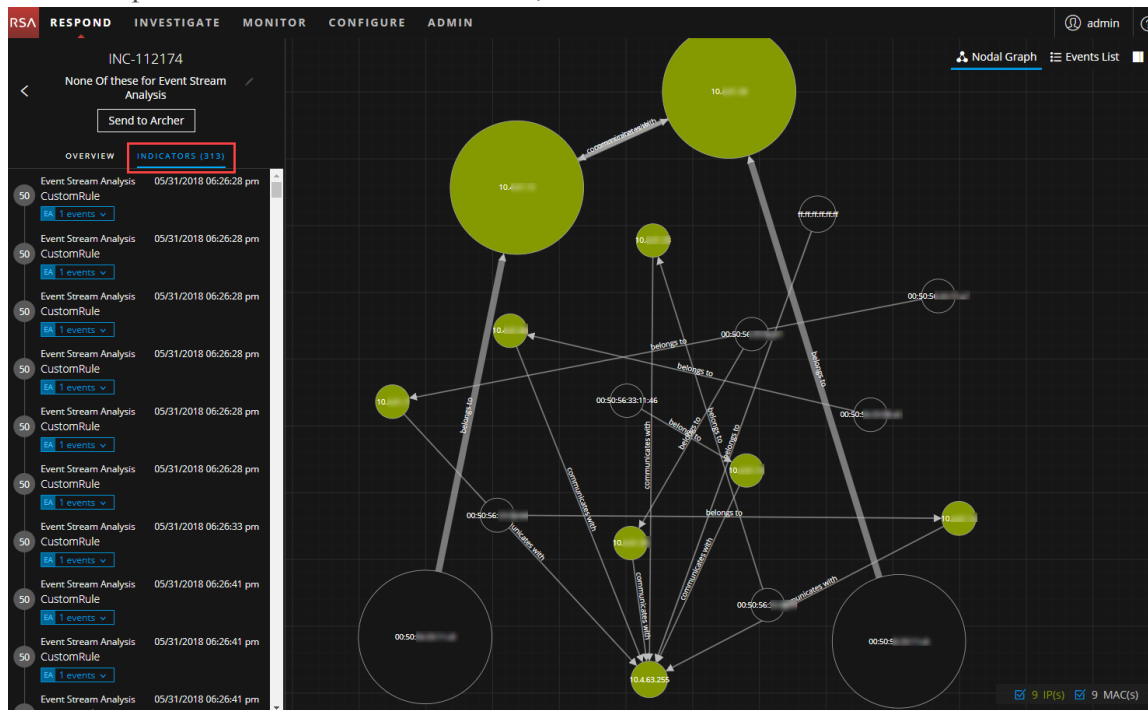
- event.read
- content.reconstruct
- content.export

Migration Considerations

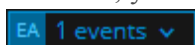
Migrated incidents from NetWitness Platform versions before 11.2 will not show the Event Analysis panel in the Respond Incident Details view Indicators panel. Likewise, if you use alerts that were migrated from versions before 11.2 to create incidents in 11.3, you will also not be able to view the Event Analysis panel in the Respond view for those incidents.

To access Event Analysis details for an event in the Indicators panel:

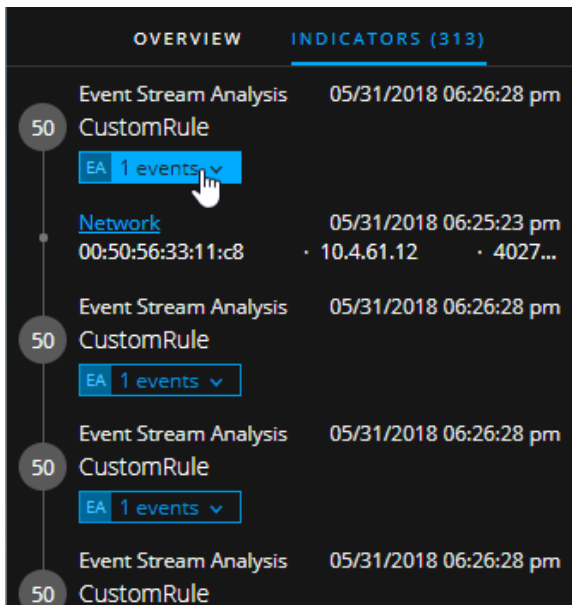
1. Go to **RESPOND > Incidents**.
2. In the Incidents List view, choose an incident to view and then click the link in the **ID** or **NAME** column for that incident.
The Incident Details view is displayed.
3. In the left panel of the Incident Details view, select **INDICATORS**.



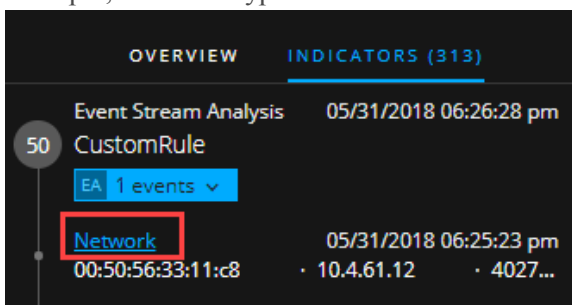
Data source information is shown below the names of the indicators. You can also see the creation date and time as well as the number of events in the indicator. If Event Analysis (EA) information is available, you can see an **EA** icon in front of the event as shown in the following figure.



- Click an event with an **EA** icon to view additional event information.



- Click an event type hyperlink within the event to open the Event Analysis panel. In the following example, the event type is Network.



The Event Analysis panel shows event details for the event, such as packet analysis details. The information available can vary based on the event type.

The screenshot displays the NetWitness Respond Event Analysis view. The interface is divided into several sections:

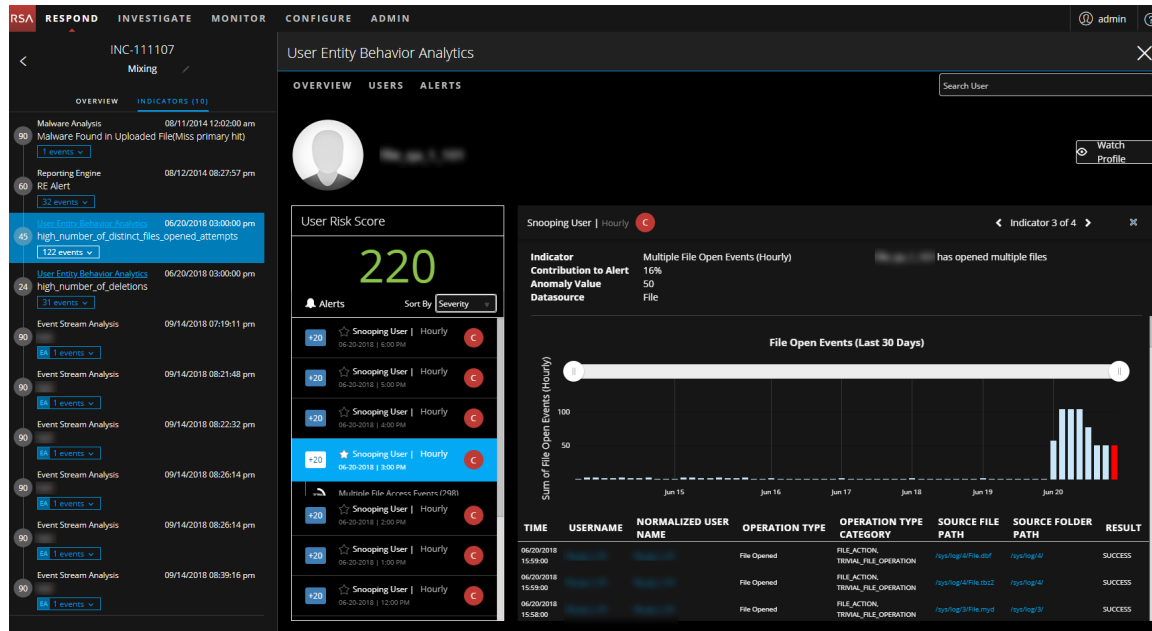
- Left Panel:** A list of events under the heading "INC-112174". The selected event is "Event Stream Analysis CustomRule" with a timestamp of "05/31/2018 06:25:23 pm".
- Top Bar:** Contains the "RESPOND" logo and navigation tabs: "INVESTIGATE", "MONITOR", "CONFIGURE", and "ADMIN".
- Event Analysis Section:**
 - Network Event Details:** Shows "NW SERVICE ELD - Concentrator", "SESSION ID 209868", "SOURCE IP:PORT 10.4.61.12 : 40276", "DESTINATION IP:PORT 10.4.61.28 : 4506", "SERVICE 0", and "FIRST PACKET TIME 05/31/2018 06:25:23.301 pm".
 - Packet Analysis:** Displays "Packet 1" and "Packet 2" with their respective hex and ASCII data. Packet 1 is a request with ID 11597412 and SEQ 2447188567. Packet 2 is a response with ID 11597413 and SEQ 0.
 - Event Meta:** Provides additional details about the event, including "SESSIONID 209868", "TIME 05/31/2018 06:25:23 pm", "SIZE 134", "PAYLOAD 0", "MEDIUM 1", and various network-related fields like "ETH.SRC", "ETH.DST", "IP.SRC", "IP.DST", "IP.ALL", "NETNAME", "DIRECTION", "IP.PROTO", "TCP.FLAGS", "TCP.SRCPOR", "PORT.ALL", "PORT.SRC.ALL", "TCP.DSTPORT", and "PORT.ALL".

For detailed information about the Event Analysis view, see the *NetWitness Investigate User Guide*.

Note: If you want to send the Event Analysis URL link to another analyst, you can copy the event type hyperlink.

View User Entity Behavior Analytics for Indicators

RSA NetWitness UEBA (User and Entity Behavior Analytics) is an advanced analytics solution for discovering, investigating, and monitoring risky behaviors across all users and entities in your network environment. You can access UEBA from the Respond Incident Details view Indicators panel. Indicators with a **User Entity Behavior Analytics** hyperlink have additional UEBA information available. For detailed information about UEBA, see the *NetWitness UEBA User Guide*.

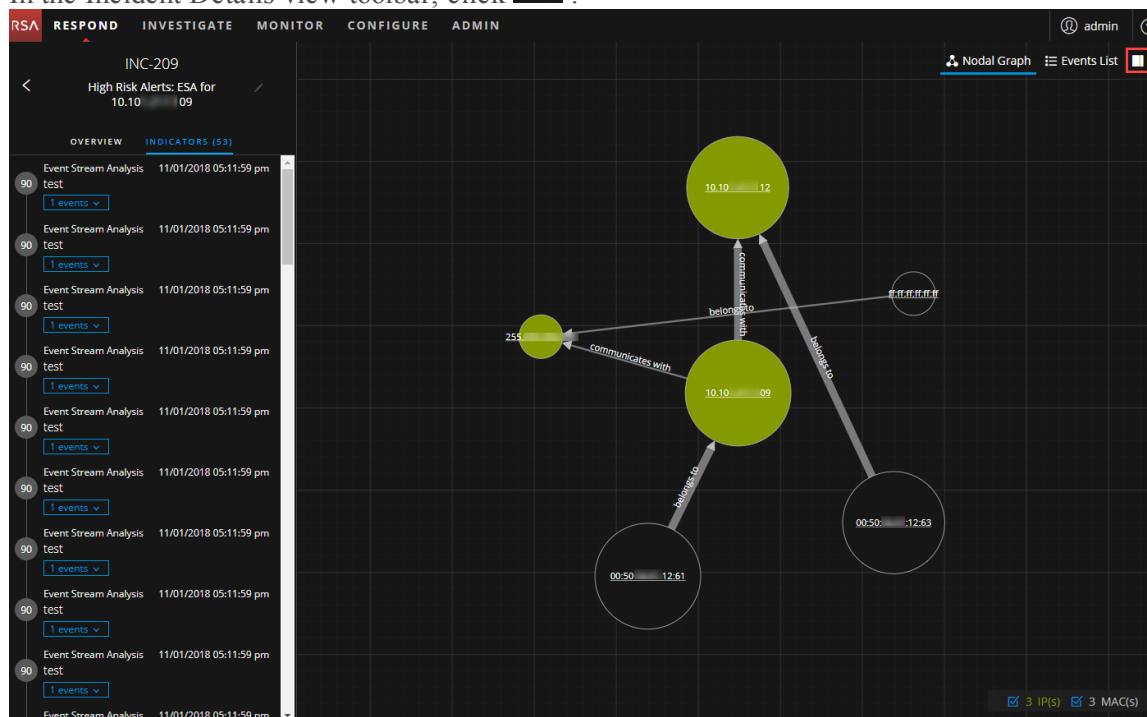


Document Steps Taken Outside of NetWitness

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, Action on Objective, Containment, Eradication, and Closure), and view the history of activity on your incident.


View the Journal Entries for an Incident

In the Incident Details view toolbar, click .



The screenshot shows the NetWitness Respond interface. On the left, the 'INC-209' incident details are visible, including a list of event stream analysis events. The main area displays a nodal graph with nodes representing IP addresses and their relationships. The toolbar at the top right includes icons for Nodal Graph, Events List, and the Journal icon (highlighted with a red square).

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



The screenshot shows the NetWitness Respond interface with the Journal panel open on the right. The Journal panel displays a list of journal entries with timestamps and descriptions. The main area displays the same nodal graph as the previous screenshot.

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

The screenshot displays the 'JOURNAL (4)' tab in the NetWitness Respond interface. It shows a list of four journal entries, each with a header containing the author 'ADMIN' and the timestamp, followed by a 'MILESTONE' dropdown menu set to 'None' and a trash icon. The entries are as follows:

- Entry 1:** 01/07/2019 10:25:19 p.m. Content: "Started researching the incident. This is similar to one I had yesterday."
- Entry 2:** 01/07/2019 10:25:35 p.m. Content: "I think this IP is malicious."
- Entry 3:** 01/07/2019 10:26:15 p.m. Content: "I created a task for Ian. I think he does remediations, too."
- Entry 4:** 01/07/2019 10:26:43 p.m. Content: "Ian is booked solid. We may need to assign it to someone else. We will let you know."

Below the list is a 'New Journal Entry' section with a text area containing the placeholder text 'Pierre may be available...'. At the bottom of this section is another 'MILESTONE' dropdown menu set to 'None' and a 'Submit' button.

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.

New Journal Entry

It looks like all of the devices are sending information to the same destination IP address

MILESTONE Command and Control

Submit

2. (Optional) Select an Investigation Milestone from the drop-down list (Reconnaissance, Delivery, Exploitation, Installation, Command and Control, Action On Objective, Containment, Eradication, and Closure).
3. After you finish your note, click, **Submit**.
Your new journal entry appears in the Journal.

TOR CONFIGURE ADMIN

✓ Your change was successful

Nodal Graph Events List

JOURNAL (6) TASKS (0) RELATED

ADMIN 01/07/2019 10:25:19 pm
MILESTONE None
Started researching the incident. This is similar to one I had yesterday.

ADMIN 01/07/2019 10:25:35 pm
MILESTONE None
I think this IP is malicious.

ADMIN 01/07/2019 10:26:15 pm
MILESTONE None
I created a task for Ian. I think he does remediations, too.

ADMIN 01/07/2019 10:26:43 pm
MILESTONE None
Ian is booked solid. We may need to assign it to someone else. We will let you know.

ADMIN 01/07/2019 10:33:29 pm
MILESTONE None
Pierre may be available...

ADMIN 01/07/2019 10:38:07 pm
MILESTONE Command and Control
It looks like all of the devices are sending information to the same destination IP address.


New Journal Entry

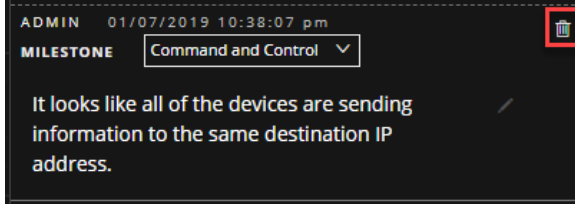
MILESTONE None

Submit

3 IP(s) 3 MAC(s)

Delete a Note

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



3. 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 escalate an incident, 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 high to critical after determining that the incident is a major breach. You may also want to send the incident to RSA Archer® Cyber Incident & Breach Response for additional analysis and action.

You can perform the following procedures to escalate or remediate an incident:

- [Send an Incident to RSA Archer](#)
- [View All Incidents Sent to Archer](#)
- [Update an Incident](#)
- [Change Incident Status](#)
- [Change Incident Priority](#)
- [Assign Incidents to other Analysts](#)
- [Rename an Incident](#)
- [View All Incident Tasks](#)
- [Filter the Tasks List](#)
- [Remove My Filters from the Tasks List](#)
- [Create a Task](#)
- [Find a Task](#)
- [Modify a Task](#)
- [Delete a Task](#)
- [Close an Incident](#)

Send an Incident to RSA Archer

Note: This option is available in version 11.2 and later. If RSA Archer is configured as a data source in Context Hub, you can send incidents to RSA Archer and you will be able to see the Send to Archer option and Sent to Archer Status in NetWitness Respond.

When you send an incident to Archer, a Sent to Archer notification appears within the incident. When configured, the NetWitness Platform can start additional business processes in Archer Cyber Incident & Breach Response. You can view all of the incidents that were sent to Archer Cyber Incident & Breach Response using the filter in the Incident Lists view.

You send an incident to Archer by clicking the Send to Archer button in the Overview panel in the Incident Lists view or the Incident Details view.

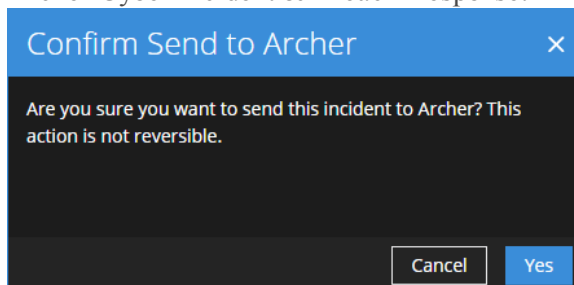
Caution: The **Send to Archer** action is not reversible.

1. Go to **RESPOND > Incidents**.
2. From the Incidents List view, click the incident that you want to send to Archer Cyber Incident & Breach Response.

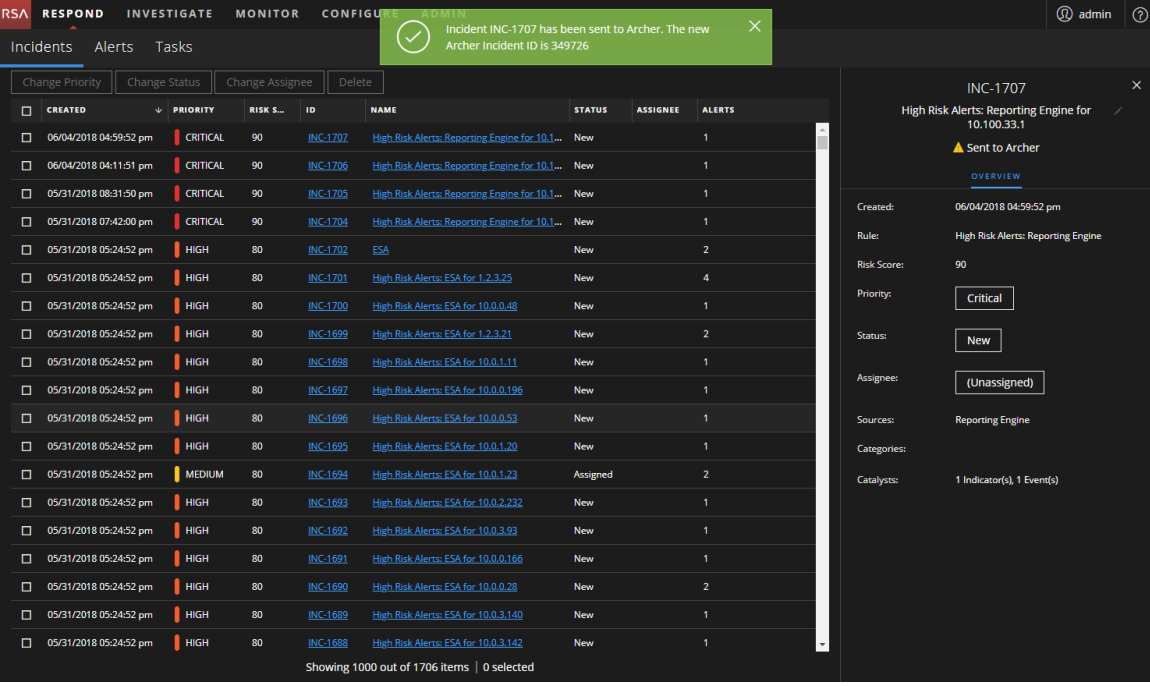
The Overview panel appears on the right.

The screenshot shows the NetWitness Respond interface. The top navigation bar includes 'RSA', 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'Incidents' tab is selected. Below the navigation bar, there are buttons for 'Change Priority', 'Change Status', 'Change Assignee', and 'Delete'. The main area displays a table of incidents with columns: CREATED, PRIORITY, RISK S., ID, NAME, STATUS, ASSIGNEE, and ALERTS. The first incident, INC-1707, is highlighted. To the right, the 'Overview' panel for INC-1707 is shown, displaying details such as 'Created: 06/04/2018 04:59:52 pm', 'Rule: High Risk Alerts: Reporting Engine for 10.100.33.1', 'Risk Score: 90', 'Priority: Critical', 'Status: New', 'Assignee: (Unassigned)', 'Source: Reporting Engine', and 'Categories: 1 Indicator(s), 1 Event(s)'. A 'Send to Archer' button is visible in the Overview panel.

3. In the Overview panel, click **Send to Archer**.
4. Read the **Confirm Send to Archer** dialog and then click **Yes** to confirm sending the incident to Archer Cyber Incident & Breach Response. This action is not reversible.



You will receive a confirmation that the incident was sent to Archer along with an Archer incident ID. In the Overview panel, the Send to Archer button changes to Sent to Archer.




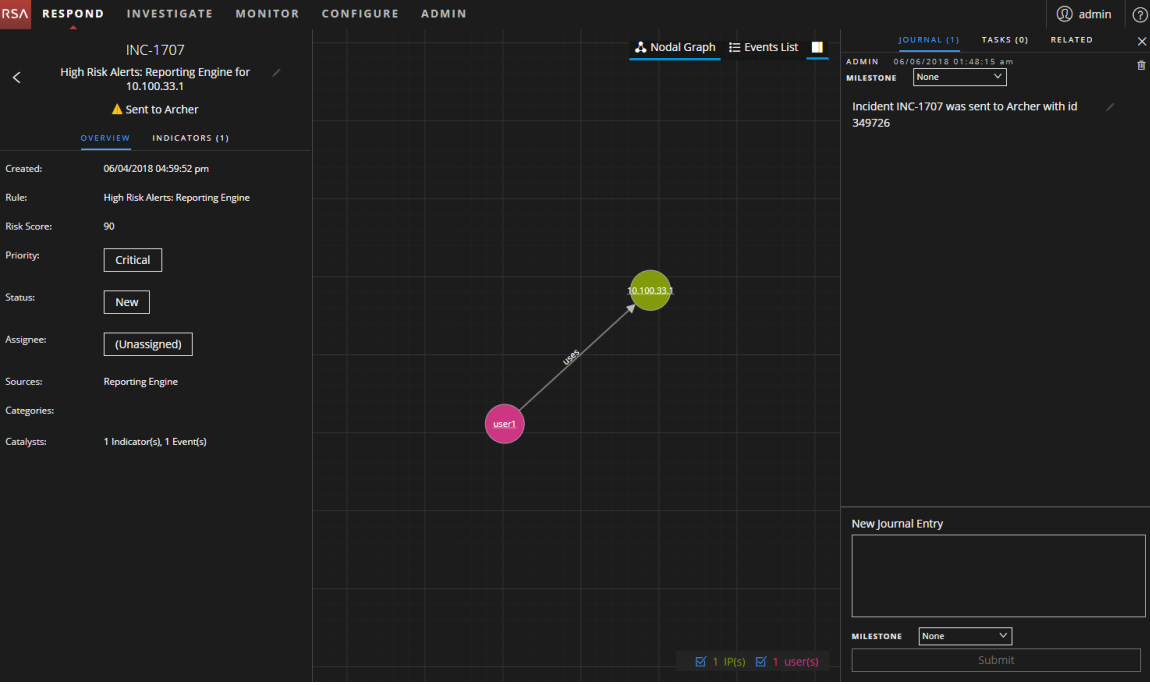
The screenshot shows the NetWitness Respond interface. At the top, there's a navigation bar with tabs: RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. A green notification banner at the top right states: "Incident INC-1707 has been sent to Archer. The new Archer incident ID is 349726". Below the navigation bar, there's a sub-header with tabs: Incidents, Alerts, and Tasks. Under the Incidents tab, there's a table with columns: CREATED, PRIORITY, RISK S., ID, NAME, STATUS, ASSIGNEE, and ALERTS. The table lists several incidents, with the first one being INC-1707, which is highlighted. To the right of the table, there's a details panel for incident INC-1707. The panel shows the incident name "High Risk Alerts: Reporting Engine for 10.100.33.1", a "Sent to Archer" notification, and an "OVERVIEW" section with fields for Created, Rule, Risk Score, Priority, Status, Assignee, Source, Categories, and Catalysts.

CREATED	PRIORITY	RISK S.	ID	NAME	STATUS	ASSIGNEE	ALERTS
06/04/2018 04:59:52 pm	CRITICAL	90	INC-1707	High Risk Alerts: Reporting Engine for 10.1...	New		1
06/04/2018 04:11:51 pm	CRITICAL	90	INC-1706	High Risk Alerts: Reporting Engine for 10.1...	New		1
05/31/2018 08:31:50 pm	CRITICAL	90	INC-1705	High Risk Alerts: Reporting Engine for 10.1...	New		1
05/31/2018 07:42:00 pm	CRITICAL	90	INC-1704	High Risk Alerts: Reporting Engine for 10.1...	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1702	ESA	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1701	High Risk Alerts: ESA for 1.2.3.25	New		4
05/31/2018 05:24:52 pm	HIGH	80	INC-1700	High Risk Alerts: ESA for 10.0.0.48	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1699	High Risk Alerts: ESA for 1.2.3.21	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1698	High Risk Alerts: ESA for 10.0.1.11	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1697	High Risk Alerts: ESA for 10.0.0.196	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1696	High Risk Alerts: ESA for 10.0.0.53	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1695	High Risk Alerts: ESA for 10.0.1.20	New		1
05/31/2018 05:24:52 pm	MEDIUM	80	INC-1694	High Risk Alerts: ESA for 10.0.1.23	Assigned		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1693	High Risk Alerts: ESA for 10.0.2.232	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1692	High Risk Alerts: ESA for 10.0.3.93	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1691	High Risk Alerts: ESA for 10.0.0.166	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1690	High Risk Alerts: ESA for 10.0.0.28	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1689	High Risk Alerts: ESA for 10.0.3.140	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1688	High Risk Alerts: ESA for 10.0.3.142	New		1

Showing 1000 out of 1706 items | 0 selected

In the Incident Details view (click the link in the ID or NAME field of the incident sent to Archer) you can see the Sent to Archer notification above the Overview and Indicators panels. If you also

click the  icon to open the Journal, you can see a system journal entry that shows that the incident was sent to Archer and it now has an Archer ID number.



The screenshot shows the NetWitness Respond interface with the Journal view selected for incident INC-1707. The left sidebar shows the incident details, including the "Sent to Archer" notification. The main area displays a Nodal Graph with a single node labeled "user1" and a link to "10.100.33.1". The right sidebar shows the Journal view with a table of entries. The first entry is a system journal entry stating "Incident INC-1707 was sent to Archer with id 349726". Below the table, there's a "New Journal Entry" form with a text area and a "Submit" button.

JOURNAL (1)	TASKS (0)	RELATED
ADMIN 06/06/2018 01:48:15 am		
MILESTONE	None	
Incident INC-1707 was sent to Archer with id 349726		

New Journal Entry


MILESTONE: None

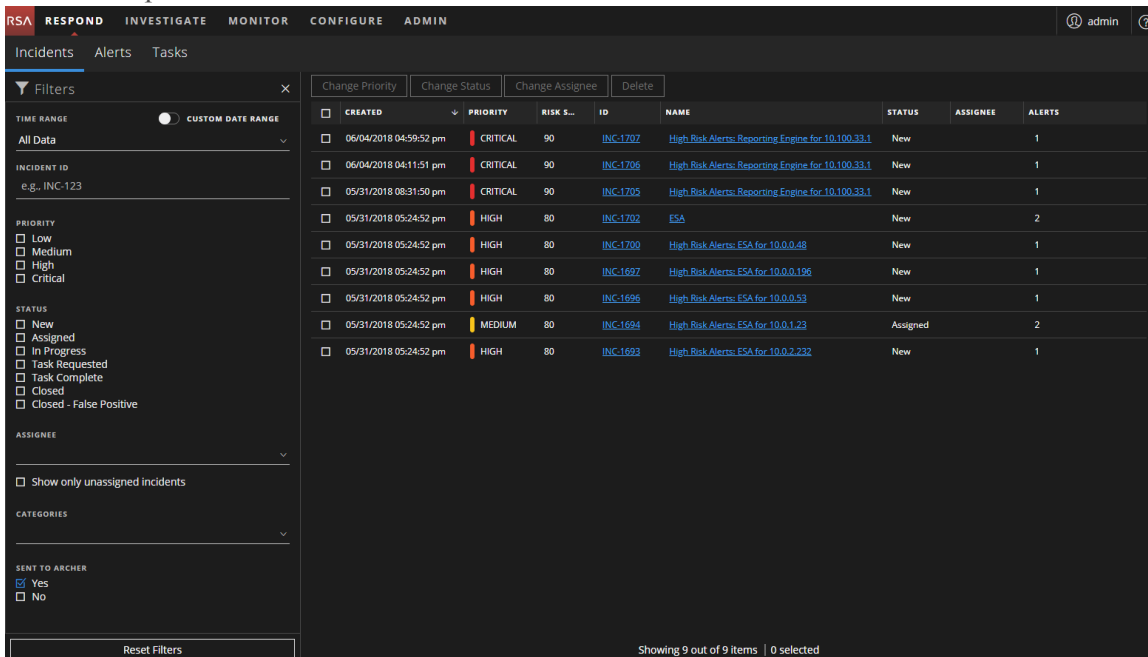
Submit

View All Incidents Sent to Archer

Note: This option is available in version 11.2 and later. If RSA Archer is configured as a data source in Context Hub, you can send incidents to RSA Archer and you will be able to see the Sent to Archer option and Sent to Archer Status in NetWitness Respond.

You can view incidents sent to Archer Cyber Incident & Breach Response using the Filter.

1. Go to **RESPOND > Incidents**.
The Incidents List is displayed.
2. If you cannot see the Filters panel, in the Incident List view toolbar, click .
3. In the Filters panel, under SENT TO ARCHER, select **Yes**.
The incidents list will be filtered to show incidents that were sent to Archer Cyber Incident & Breach Response.



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 'Incidents' tab is selected. On the left, the 'Filters' panel is open, showing various filter options. Under 'SENT TO ARCHER', the 'Yes' checkbox is selected. The main table displays a list of incidents with columns: CREATED, PRIORITY, RISK S..., ID, NAME, STATUS, ASSIGNEE, and ALERTS. The table shows 9 items, with 0 selected.

CREATED	PRIORITY	RISK S...	ID	NAME	STATUS	ASSIGNEE	ALERTS
06/04/2018 04:59:52 pm	CRITICAL	90	INC-1707	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
06/04/2018 04:11:51 pm	CRITICAL	90	INC-1706	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 08:31:50 pm	CRITICAL	90	INC-1705	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1702	ESA	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1700	High Risk Alerts: ESA for 10.0.0.48	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1697	High Risk Alerts: ESA for 10.0.0.196	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1696	High Risk Alerts: ESA for 10.0.0.53	New		1
05/31/2018 05:24:52 pm	MEDIUM	80	INC-1694	High Risk Alerts: ESA for 10.0.1.23	Assigned		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1693	High Risk Alerts: ESA for 10.0.2.232	New		1

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

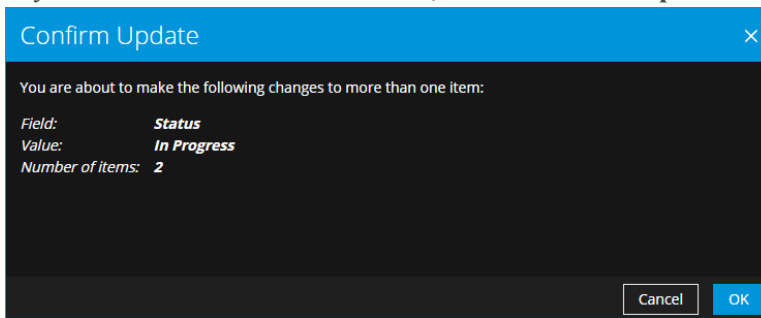
To update the status of multiple incidents:

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 in the incidents list footer.
2. 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.

CREATED	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
04/12/2018 10:00	80	INC-96894	Suspected C&C with mt0.google.com	New		3
04/12/2018 10:00	80	INC-96893	Suspected C&C with ts.richmedia.yahoo.com	New		4
04/12/2018 10:00	80	INC-96892	Suspected C&C with www.dallasnews.com	New		1
04/12/2018 10:00	80	INC-96891	Suspected C&C with headlines.favorites.aol.com	New		2
04/12/2018 10:00	80	INC-96890	Suspected C&C with www.ilboa.org	New		1
04/12/2018 10:50:58 pm	80	INC-96889	Suspected C&C with www.weather.com	New		3
04/12/2018 10:50:58 pm	80	INC-96888	Suspected C&C with i.yimg.com	New		5
04/12/2018 10:50:58 pm	80	INC-96887	Suspected C&C with us.f513.mail.yahoo.com	New		1
04/12/2018 10:50:58 pm	80	INC-96886	Suspected C&C with lh.pricegrabber.com	New		2
04/12/2018 10:50:58 pm	80	INC-96885	Suspected C&C with hearstmagazines.112.2o7.net	New		2
04/12/2018 10:50:58 pm	80	INC-96884	Suspected C&C with psu.facebook.com	New		1
04/12/2018 10:50:58 pm	80	INC-96883	Suspected C&C with b.mail.google.com	New		28
04/12/2018 10:50:58 pm	80	INC-96882	Suspected C&C with www.walmart.com	New		1
04/12/2018 10:50:58 pm	80	INC-96881	Suspected C&C with www.troymixtapes.com	New		1
04/12/2018 10:50:58 pm	80	INC-96880	Suspected C&C with bc.facebook.com	New		1
04/12/2018 10:50:58 pm	80	INC-96879	Suspected C&C with redir.metaservices.microsoft.com	New		1
04/12/2018 10:50:58 pm	80	INC-96878	Suspected C&C with us.f556.mail.yahoo.com	New		1
04/12/2018 10:50:58 pm	80	INC-96877	Suspected C&C with us.inf.ads.yahoo.com	New		2
04/12/2018 10:50:58 pm	80	INC-96876	Suspected C&C with www.orbitz.com	New		2

Showing 1000 out of 97523 items | 2 selected

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



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

The screenshot shows the NetWitness Respond interface. At the top, there is a navigation bar with tabs: INCIDENTS, ALERTS, TASKS, and a green notification banner that says "Your change was successful". Below the navigation bar, there are buttons for "Change Priority", "Change Status", "Change Assignee", and "Delete". The main area displays a table of incidents. The "STATUS" column is highlighted with a red box, showing "In Progress" for the first two incidents and "New" for the others. The table has columns for CREATED, PRIORITY, RISK SCORE, ID, NAME, STATUS, ASSIGNEE, and ALERTS.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
04/12/2018 10:50:58 pm	HIGH	80	INC-96894	Suspected C&C with mt0.google.com	In Progress		3
04/12/2018 10:50:58 pm	HIGH	80	INC-96893	Suspected C&C with ts.richmedia.yahoo.com	In Progress		4
04/12/2018 10:50:58 pm	HIGH	80	INC-96892	Suspected C&C with www.dallasnews.com	New		1
04/12/2018 10:50:58 pm	HIGH	80	INC-96891	Suspected C&C with headlines.favorites.aol.com	New		2
04/12/2018 10:50:58 pm	HIGH	80	INC-96890	Suspected C&C with www.ilboa.org	New		1
04/12/2018 10:50:58 pm	HIGH	80	INC-96889	Suspected C&C with www.weather.com	New		3
04/12/2018 10:50:58 pm	HIGH	80	INC-96888	Suspected C&C with i.ytimg.com	New		5
04/12/2018 10:50:58 pm	HIGH	80	INC-96887	Suspected C&C with us.P13.mail.yahoo.com	New		1
04/12/2018 10:50:58 pm	HIGH	80	INC-96886	Suspected C&C with lh.pricegrabber.com	New		2
04/12/2018 10:50:58 pm	HIGH	80	INC-96885	Suspected C&C with hearstmagazines.112.2o7.net	New		2
04/12/2018 10:50:58 pm	HIGH	80	INC-96884	Suspected C&C with psu.facebook.com	New		1
04/12/2018 10:50:58 pm	HIGH	80	INC-96883	Suspected C&C with b.mail.google.com	New		28
04/12/2018 10:50:58 pm	HIGH	80	INC-96882	Suspected C&C with www.walmart.com	New		1
04/12/2018 10:50:58 pm	HIGH	80	INC-96881	Suspected C&C with www.tinymixtapes.com	New		1
04/12/2018 10:50:58 pm	HIGH	80	INC-96880	Suspected C&C with bc.facebook.com	New		1
04/12/2018 10:50:58 pm	HIGH	80	INC-96879	Suspected C&C with redir.metaservices.microsoft.com	New		1
04/12/2018 10:50:58 pm	HIGH	80	INC-96878	Suspected C&C with us.B36.mail.yahoo.com	New		1
04/12/2018 10:50:58 pm	HIGH	80	INC-96877	Suspected C&C with us.inf.ads.yahoo.com	New		2
04/12/2018 10:50:58 pm	HIGH	80	INC-96876	Suspected C&C with www.orbitz.com	New		2

Showing 1000 out of 97523 items | 2 selected

To change the status 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 status update.

The screenshot shows the NetWitness Respond interface. The top navigation bar includes RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The left sidebar has tabs for Incidents, Alerts, and Tasks. The main area displays a table of incidents. The incident INC-96892 is selected, and its details are shown in the Overview panel on the right.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE
04/12/2018 10:50:58 pm	HIGH	80	INC-96894	Suspected C&C with mt0.google.com	In Progress	
04/12/2018 10:50:58 pm	HIGH	80	INC-96893	Suspected C&C with ts.richmedia.yahoo.com	In Progress	
04/12/2018 10:50:58 pm	HIGH	80	INC-96892	Suspected C&C with www.dallasnews.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96891	Suspected C&C with headlines.favorites.a-	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96890	Suspected C&C with www.ilboa.org	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96889	Suspected C&C with www.weather.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96888	Suspected C&C with lytimg.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96887	Suspected C&C with us.f513.mail.yahoo.co-	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96886	Suspected C&C with lh.pricegrabber.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96885	Suspected C&C with hearstmagazines.112-	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96884	Suspected C&C with psu.facebook.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96883	Suspected C&C with b.mail.google.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96882	Suspected C&C with www.walmart.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96881	Suspected C&C with www.tinytapes.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96880	Suspected C&C with bc.facebook.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96879	Suspected C&C with redir.metaservices.mt-	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96878	Suspected C&C with us.f356.mail.yahoo.co-	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96877	Suspected C&C with us.inf.ads.yahoo.com	New	
04/12/2018 10:50:58 pm	HIGH	80	INC-96876	Suspected C&C with www.orbits.com	New	

Showing 1000 out of 97523 items | 0 selected

INC-96892
Suspected C&C with www.dallasnews.com
Send to Archer

OVERVIEW

Created: 04/12/2018 10:50:58 pm
Rule: Suspected Command & Control Communication By Domain
Risk Score: 80
Priority: High
Status: New
Assignee: (Unassigned)
Sources: Event Stream Analysis
Categories:
Catalysts: 1 Indicator(s), 1 Event(s)

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

The screenshot shows the NetWitness Respond interface with the Incident Details view for INC-96892. The Overview tab is selected, displaying a summary of the incident on the left and a Nodal Graph on the right.

INC-96892
Suspected C&C with www.dallasnews.com
Send to Archer

OVERVIEW INDICATORS (1)

Created: 04/12/2018 10:50:58 pm
Rule: Suspected Command & Control Communication By Domain
Risk Score: 80
Priority: High
Status: New
Assignee: (Unassigned)
Sources: Event Stream Analysis
Categories:
Catalysts: 1 Indicator(s), 1 Event(s)

Nodal Graph

The Nodal Graph shows a network of indicators and their relationships. Key indicators include:

- IP: 250.33 (Yellow node)
- IP: 233.178 (Yellow node)
- Domain: www.dallasnews.com (Blue node)
- File: go_button_small.jpg (Green node)
- IP: 00:17:af:6b:c8:00 (Grey node)
- IP: 00:15:c3:3b:c7:00 (Grey node)

Relationships shown:

- IP: 250.33 has file go_button_small.jpg
- IP: 250.33 communicates with IP: 233.178
- IP: 233.178 has file go_button_small.jpg
- Domain: www.dallasnews.com is related to IP: 233.178
- IP: 00:17:af:6b:c8:00 is related to IP: 233.178
- IP: 00:15:c3:3b:c7:00 is related to IP: 233.178

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

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

INC-96892

Suspected C&C with
www.dallasnews.com

Send to Archer

OVERVIEW INDICATORS (1)

Created: 04/12/2018 10:50:58 pm

Rule: Suspected Command & Control Communication By Domain

Risk Score: 80

Priority: High

Status: New

Assignee:

Sources:

Categories:

Catalysts:

New

Assigned

In Progress

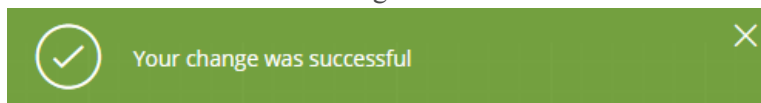
Task Requested

Task Complete

Closed

Closed - False Positive

You can 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.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
04/12/2018 10:51:16 pm	High	80	INC-97524	Suspected C&C with www.tivoblog.com	In Progress		1
04/12/2018 10:51:16 pm	High	80	INC-97523	Suspected C&C with photos:979.ll.facebook.com	In Progress		1
04/12/2018 10:51:16 pm	High	80	INC-97522	Suspected C&C with espn.starwave.com	In Progress		1
04/12/2018 10:51:16 pm	High	80	INC-97521	Suspected C&C with photos:896.ll.facebook.com	New		1
04/12/2018 10:51:16 pm	High	80	INC-97520	Suspected C&C with by115w.bay115.mail.live.com	New		2
04/12/2018 10:51:16 pm	High	80	INC-97519	Suspected C&C with www.professional-resume-example.com	New		1
04/12/2018 10:51:16 pm	High	80	INC-97518	Suspected C&C with graphics.cstv.com	New		1
04/12/2018 10:51:16 pm	High	80	INC-97517	Suspected C&C with dco.weather.com	New		2
04/12/2018 10:51:16 pm	High	80	INC-97516	Suspected C&C with cl-exct.net	New		1
04/12/2018 10:51:16 pm	High	80	INC-97515	Suspected C&C with t7.photobucket.com	New		1
04/12/2018 10:51:16 pm	High	80	INC-97514	Suspected C&C with ad.yieldmanager.com	New		10
04/12/2018 10:51:16 pm	High	80	INC-97513	Suspected C&C with usepic.livejournal.com	New		3
04/12/2018 10:51:16 pm	High	80	INC-97512	Suspected C&C with www.californiapsychics.com	New		1
04/12/2018 10:51:16 pm	High	80	INC-97511	Suspected C&C with my.gwu.edu	New		1
04/12/2018 10:51:16 pm	High	80	INC-97510	Suspected C&C with photos:193.ll.facebook.com	New		1
04/12/2018 10:51:16 pm	High	80	INC-97509	Suspected C&C with photos:285.ll.facebook.com	New		1
04/12/2018 10:51:16 pm	High	80	INC-97508	Suspected C&C with icons-pe.waug.com	New		2
04/12/2018 10:51:16 pm	High	80	INC-97507	Suspected C&C with sm6.sitemeter.com	New		1
04/12/2018 10:51:16 pm	High	80	INC-97506	Suspected C&C with photos:cak.facebook.com	New		17

Showing 1000 out of 97524 items | 3 selected

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

now show Critical.

The screenshot shows the NetWitness Respond interface with the 'Incidents' tab selected. A green notification banner at the top indicates 'Your change was successful'. Below the notification, there are buttons for 'Change Priority', 'Change Status', 'Change Assignee', and 'Delete'. The main table lists incidents with columns: CREATED, PRIORITY, RISK SCORE, ID, NAME, STATUS, ASSIGNEE, and ALERTS. Three incidents are selected with checkboxes, and their priority is set to 'CRITICAL'.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
04/12/2018 10:51:16 pm	CRITICAL	80	INC-97524	Suspected C&C with www.tweeblog.com	In Progress		1
04/12/2018 10:51:16 pm	CRITICAL	80	INC-97523	Suspected C&C with photos-979.ii.facebook.com	In Progress		1
04/12/2018 10:51:16 pm	CRITICAL	80	INC-97522	Suspected C&C with espn.starwave.com	In Progress		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97521	Suspected C&C with photos-896.ii.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97520	Suspected C&C with by115w.bay115.mail.live.com	New		2
04/12/2018 10:51:16 pm	HIGH	80	INC-97519	Suspected C&C with www.professional-resume-example.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97518	Suspected C&C with graphics.cstv.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97517	Suspected C&C with dco.weather.com	New		2
04/12/2018 10:51:16 pm	HIGH	80	INC-97516	Suspected C&C with clexact.net	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97515	Suspected C&C with i7.photobucket.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97514	Suspected C&C with ad.yieldmanager.com	New		10
04/12/2018 10:51:16 pm	HIGH	80	INC-97513	Suspected C&C with userpic.livejournal.com	New		3
04/12/2018 10:51:16 pm	HIGH	80	INC-97512	Suspected C&C with www.californiapsychics.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97511	Suspected C&C with my.gwu.edu	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97510	Suspected C&C with photos-193.ii.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97509	Suspected C&C with photos-285.ii.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97508	Suspected C&C with icons.pe.wau.com	New		2
04/12/2018 10:51:16 pm	HIGH	80	INC-97507	Suspected C&C with sm6.sitemeter.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97506	Suspected C&C with photos-c.alk.facebook.com	New		17

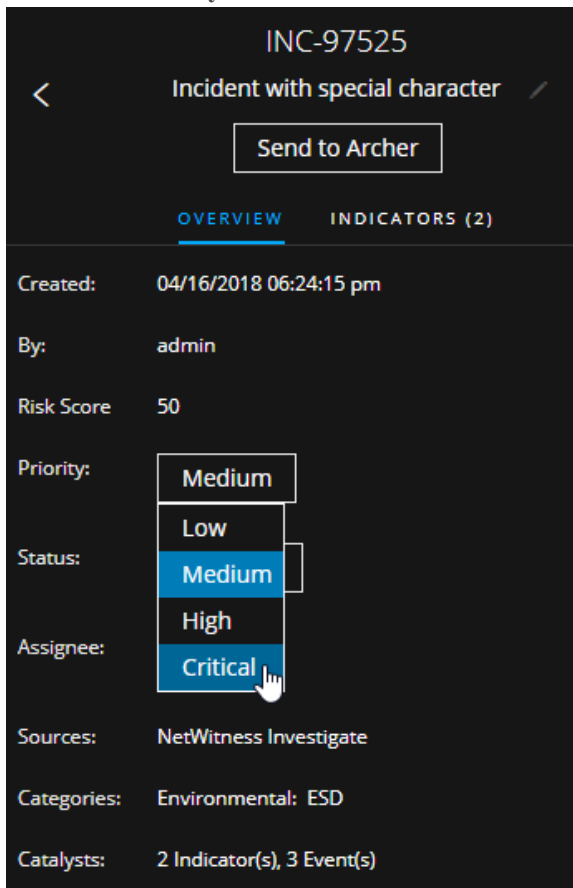
Showing 1000 out of 97524 items | 3 selected

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.

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



INC-97525

< Incident with special character

Send to Archer

OVERVIEW INDICATORS (2)

Created: 04/16/2018 06:24:15 pm

By: admin

Risk Score 50

Priority: Medium

Status: Medium

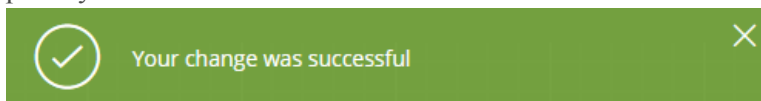
Assignee: Critical

Sources: NetWitness Investigate

Categories: Environmental: ESD

Catalysts: 2 Indicator(s), 3 Event(s)

You can 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.

- 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.

The screenshot shows the NetWitness Respond interface with the 'Incidents' tab selected. A table of incidents is displayed with columns: CREATED, PRIORITY, RISK SCORE, ID, NAME, STATUS, ASSIGNEE, and ALERTS. Three incidents are selected (checked). The 'Change Assignee' button is clicked, opening a dropdown menu with 'admin' and 'Analyst User' options. The 'Analyst User' option is highlighted.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
04/12/2018 10:51:16 pm	HIGH	80	INC-97524	Suspected C&C with www.tivoblog.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97523	Suspected C&C with photos-979.ill.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97522	Suspected C&C with espn.starwave.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97521	Suspected C&C with photos-896.ill.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97520	Suspected C&C with by115w.bay115.mail.live.com	New		2
04/12/2018 10:51:16 pm	HIGH	80	INC-97519	Suspected C&C with www.professional-resume-example.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97518	Suspected C&C with graphics.csv.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97517	Suspected C&C with dcc.weather.com	New		2
04/12/2018 10:51:16 pm	HIGH	80	INC-97516	Suspected C&C with clexct.net	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97515	Suspected C&C with 17.photobucket.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97514	Suspected C&C with ad.yieldmanager.com	New		10
04/12/2018 10:51:16 pm	HIGH	80	INC-97513	Suspected C&C with usernic.livejournal.com	New		3
04/12/2018 10:51:16 pm	HIGH	80	INC-97512	Suspected C&C with www.californiapsychics.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97511	Suspected C&C with my.gwu.edu	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97510	Suspected C&C with photos-193.ill.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97509	Suspected C&C with photos-283.ill.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97508	Suspected C&C with icons-pe.wuug.com	New		2
04/12/2018 10:51:16 pm	HIGH	80	INC-97507	Suspected C&C with smf.sitemeter.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97506	Suspected C&C with photos-c.ak.facebook.com	New		17

Showing 1000 out of 97524 items | 3 selected

- If you select more than one incident, in the **Confirm Update** dialog, click **OK**. You can see a successful change notification. The assignee changes to the selected user.

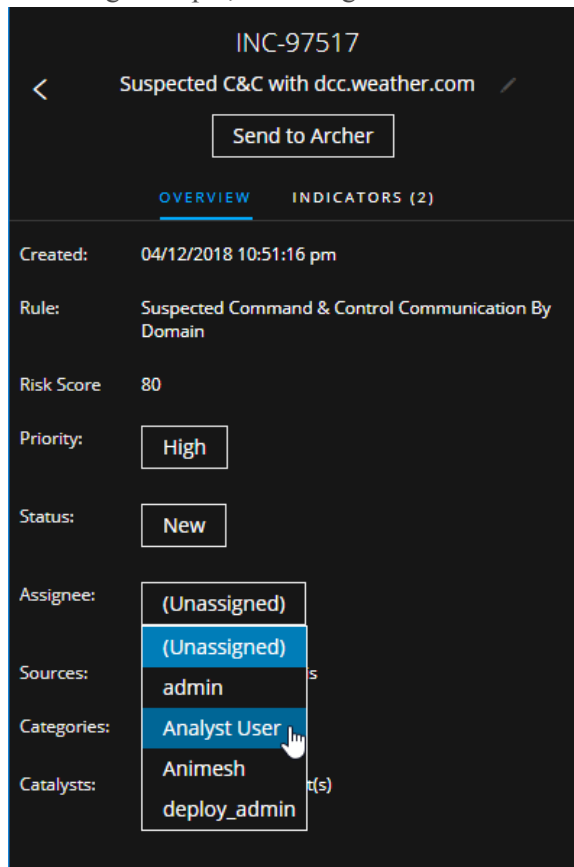
The screenshot shows the NetWitness Respond interface with a green notification banner at the top stating 'Your change was successful'. The table of incidents is updated, and the 'ASSIGNEE' column for the three selected incidents now shows 'Analyst User'.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
04/12/2018 10:51:16 pm	HIGH	80	INC-97524	Suspected C&C with www.tivoblog.com	Assigned	Analyst User	1
04/12/2018 10:51:16 pm	HIGH	80	INC-97523	Suspected C&C with photos-979.ill.facebook.com	Assigned	Analyst User	1
04/12/2018 10:51:16 pm	HIGH	80	INC-97522	Suspected C&C with espn.starwave.com	Assigned	Analyst User	1
04/12/2018 10:51:16 pm	HIGH	80	INC-97521	Suspected C&C with photos-896.ill.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97520	Suspected C&C with by115w.bay115.mail.live.com	New		2
04/12/2018 10:51:16 pm	HIGH	80	INC-97519	Suspected C&C with www.professional-resume-example.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97518	Suspected C&C with graphics.csv.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97517	Suspected C&C with dcc.weather.com	New		2
04/12/2018 10:51:16 pm	HIGH	80	INC-97516	Suspected C&C with clexct.net	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97515	Suspected C&C with 17.photobucket.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97514	Suspected C&C with ad.yieldmanager.com	New		10
04/12/2018 10:51:16 pm	HIGH	80	INC-97513	Suspected C&C with usernic.livejournal.com	New		3
04/12/2018 10:51:16 pm	HIGH	80	INC-97512	Suspected C&C with www.californiapsychics.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97511	Suspected C&C with my.gwu.edu	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97510	Suspected C&C with photos-193.ill.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97509	Suspected C&C with photos-283.ill.facebook.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97508	Suspected C&C with icons-pe.wuug.com	New		2
04/12/2018 10:51:16 pm	HIGH	80	INC-97507	Suspected C&C with smf.sitemeter.com	New		1
04/12/2018 10:51:16 pm	HIGH	80	INC-97506	Suspected C&C with photos-c.ak.facebook.com	New		17

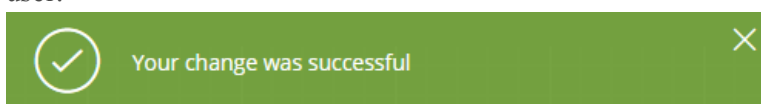
Showing 1000 out of 97524 items | 3 selected

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 you would like to assign to a user.
 - From the Incident Details view, click the **OVERVIEW** tab.In the Overview panel, the Assignee button shows the current assignee of the incident. In the following example, the Assignee button has a current status of Unassigned.

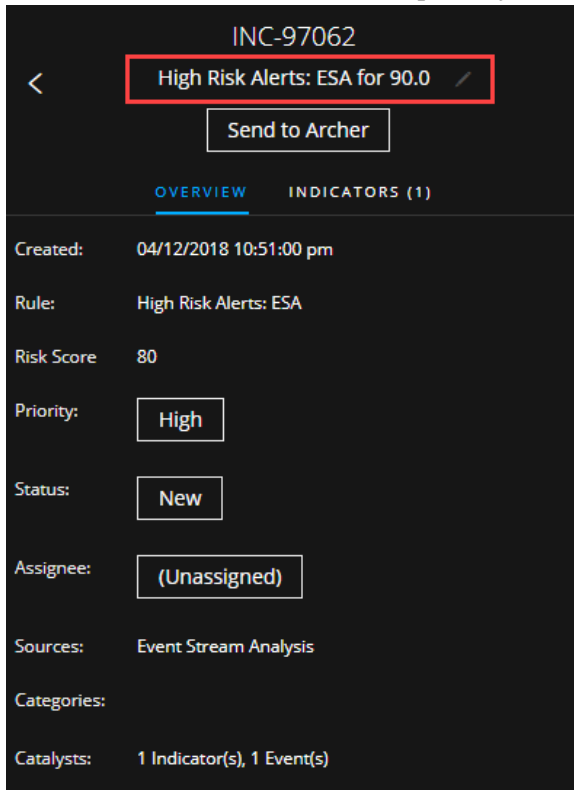


2. Click the **Assignee** button and select a user from the drop-down list.
You can see a successful change notification. The Assignee button changes to show the assigned user.

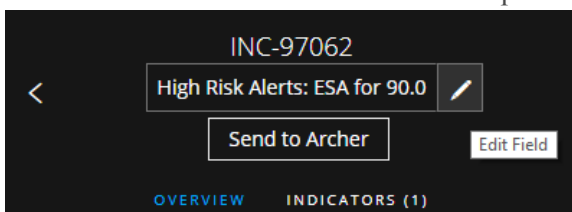
**Rename an Incident**

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.

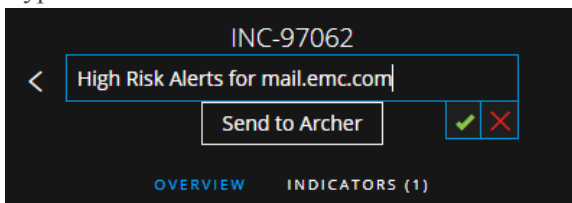
1. Go to **RESPOND > Incidents**.
2. To open the Overview panel, do one of the following:
 - From the Incidents List view, click an incident that needs a name change.
The Overview panel opens.
 - From the Incident Details view, go to the **OVERVIEW** panel.
In the header above the Overview panel, you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



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

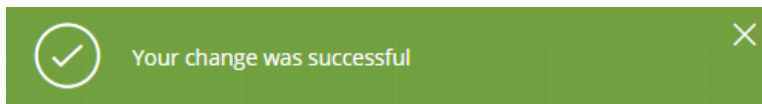


4. Type a new name for the incident in the text editor and click the check mark to confirm the change.

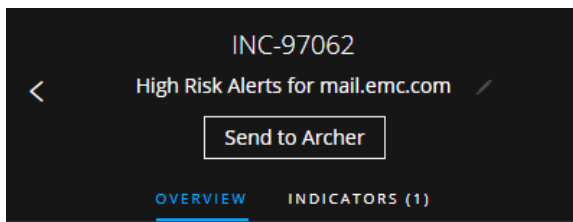


For example, you can change "High Risk Alerts: ESA for 90.0" to "Alerts for mail.emc.com" for more clarification.

You can see a successful change notification.



The incident name field shows the new name.

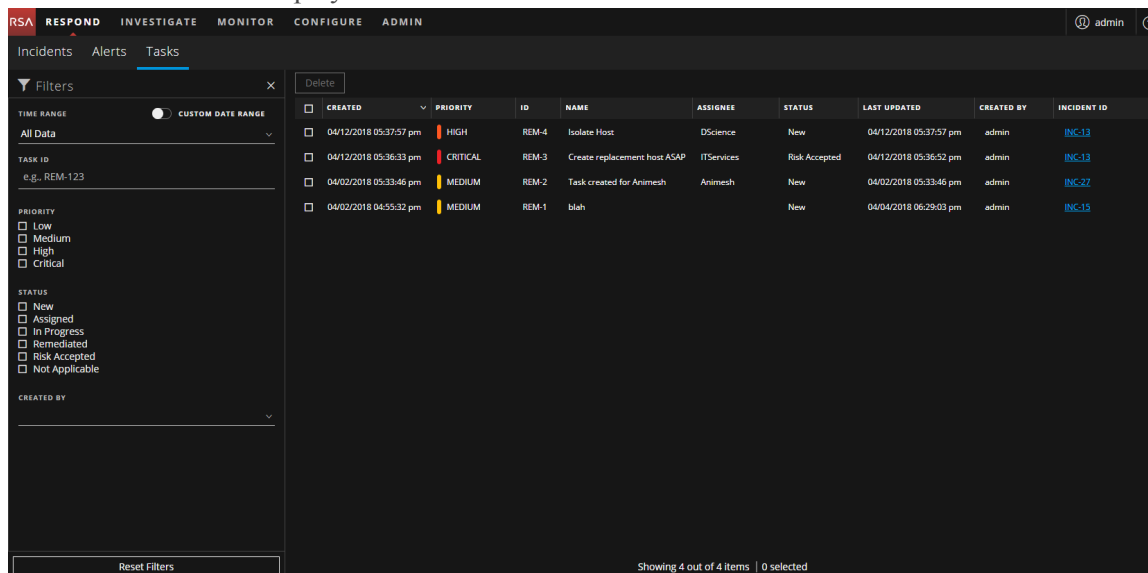


View All Incident Tasks

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.

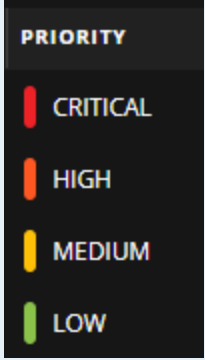
1. Go to **RESPOND > Tasks**.

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.

Column	Description
PRIORITY	<p>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:</p> 
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.
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.

Filters

×

TIME RANGE

CUSTOM DATE RANGE

All Data

▼

TASK ID

e.g., REM-123

PRIORITY

☐ Low
☐ Medium
☐ High
☐ Critical

STATUS

☐ New
☐ Assigned
☐ In Progress
☐ Remediated
☐ Risk Accepted
☐ Not Applicable

CREATED BY

▼

Reset Filters

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 can 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 Platform remembers your filter selections in the Tasks List view. 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.

RSA

RESPOND

INVESTIGATE

MONITOR

CONFIGURE

ADMIN

Incidents

Alerts

Tasks

Filters

TIME RANGE

CUSTOM DATE RANGE

All Data

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

Show only unassigned incidents

CATEGORIES

SENT TO ARCHIVER

Yes

No

Reset Filters

Change Priority

Change Status

Change Assignee

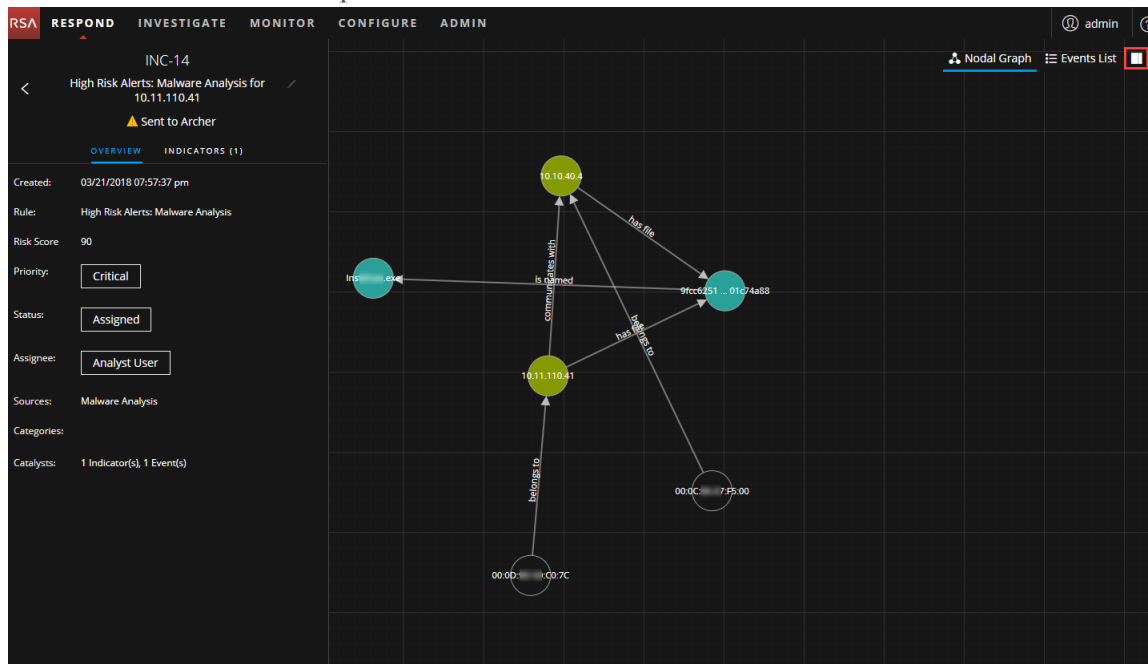
Delete


CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
<input type="checkbox"/>	04/12/2018 07:43:12 pm	CRITICAL	100	INC-91235	High Risk Alerts: Malware Analysis for 127.0.0.1	New	1
<input type="checkbox"/>	04/12/2018 07:37:15 pm	CRITICAL	100	INC-91234	High Risk Alerts: Malware Analysis for 127.0.0.1	New	2
<input type="checkbox"/>	04/04/2018 03:54:42 pm	CRITICAL	100	INC-3396	High Risk Alerts: Malware Analysis for 10.11.110.41	New	2
<input type="checkbox"/>	04/03/2018 02:28:36 pm	CRITICAL	90	INC-31	High Risk Alerts: Malware Analysis for 10.11.110.41	New	1
<input type="checkbox"/>	03/21/2018 08:00:02 pm	CRITICAL	10	INC-26	High Risk Alerts: NewWitness Endpoint for 10.11.110.41	In Progress	deploy_admin
<input type="checkbox"/>	03/21/2018 07:57:37 pm	CRITICAL	90	INC-16	High Risk Alerts: Malware Analysis for 10.11.110.41	Assigned	Analyst User
<input type="checkbox"/>	03/21/2018 07:57:37 pm	CRITICAL	90	INC-13	High Risk Alerts: Malware Analysis for 10.11.110.41	Task Requested	4
<input type="checkbox"/>	03/21/2018 07:57:37 pm	CRITICAL	100	INC-12	High Risk Alerts: Malware Analysis for 10.7.232.72	New	1
<input type="checkbox"/>	03/21/2018 07:57:37 pm	CRITICAL	100	INC-11	High Risk Alerts: Malware Analysis for 10.7.232.72	New	4
<input type="checkbox"/>	03/21/2018 07:57:37 pm	CRITICAL	90	INC-10	High Risk Alerts: Malware Analysis for 10.25.51.142	New	1
<input type="checkbox"/>	03/21/2018 07:57:37 pm	CRITICAL	90	INC-9	High Risk Alerts: Malware Analysis for 10.25.51.142	New	1
<input type="checkbox"/>	03/21/2018 07:57:36 pm	CRITICAL	90	INC-8	High Risk Alerts: Malware Analysis for 10.25.51.142	New	4
<input type="checkbox"/>	03/21/2018 07:57:36 pm	CRITICAL	90	INC-7	High Risk Alerts: Malware Analysis for 10.25.51.142	New	5
<input type="checkbox"/>	03/21/2018 07:57:36 pm	CRITICAL	90	INC-6	High Risk Alerts: Malware Analysis for 10.25.51.142	New	4
<input type="checkbox"/>	04/16/2018 07:30:28 pm	HIGH	50	INC-97526	Incident for UTE-8	Assigned	admin
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97524	Suspected C&C with www.tyrolblog.com	Assigned	Analyst User
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97523	Suspected C&C with www.facebook.com	Assigned	Analyst User
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97522	Suspected C&C with open.starwave.com	Assigned	Analyst User
<input type="checkbox"/>	04/12/2018 10:51:16 pm	HIGH	80	INC-97521	Suspected C&C with www.facebook.com	New	1


Showing 1000 out of 97525 items | 0 selected

2. Locate the incident that needs a task and click the link in the **ID** or **NAME** field.

The Incident Details view opens.

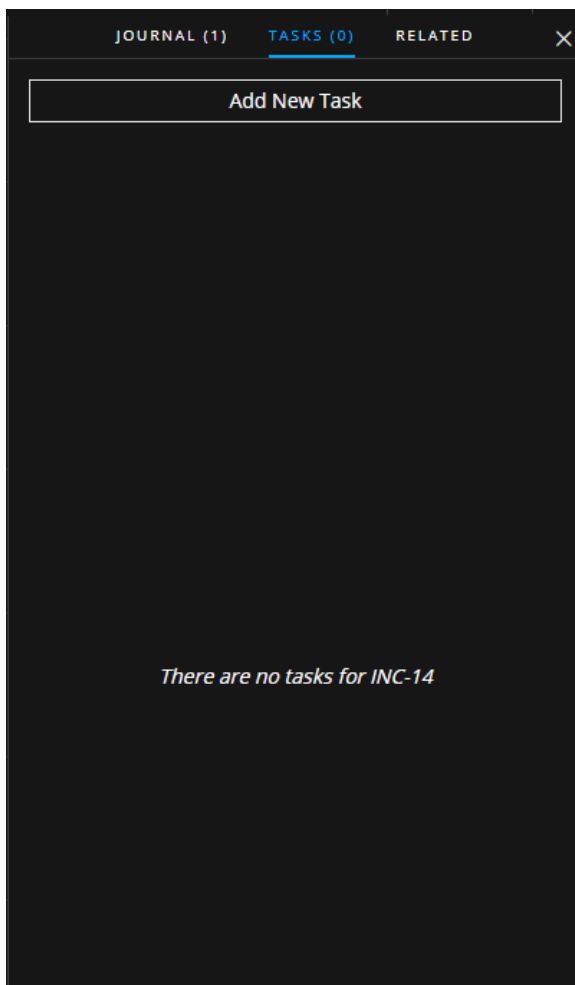


3. In the toolbar at the top right of the Incident Details view, select . The Journal panel opens.



The screenshot displays the NetWitness Respond interface. On the left, the 'INC-14' incident details are shown, including a high-risk alert for malware analysis on 10.11.110.41, a critical priority, and an assigned status to an analyst user. The main area features a 'Nodal Graph' showing relationships between IP addresses (10.10.40.4, 10.11.110.41, 10.10.40.4) and a file hash (9fcc6451...01c74ab8). The right-hand 'JOURNAL (1)' panel is active, showing an admin action on 03/30/2018 at 05:54:10 pm, with a milestone of 'None' and the note 'Incident was escalated'. A 'New Journal Entry' form is visible at the bottom right.

4. Click the **TASKS** tab.



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

The screenshot shows a modal window titled "NEW TASK FOR INC-14". At the top, there are three tabs: "JOURNAL (1)", "TASKS (0)", and "RELATED". The "TASKS (0)" tab is selected. The form contains the following fields:

- NAME ***: A text input field containing "Re-image the machine".
- DESCRIPTION**: A text area containing "Opened ticket ABC-2345 to re-image the affected machine.".
- ASSIGNEE:**: A text input field containing "Jose".
- PRIORITY ***: A dropdown menu with "High" selected.

At the bottom right, there are two buttons: "Cancel" and "Save".

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 can 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.

The screenshot displays the NetWitness Respond interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main view is titled 'INC-14' and shows 'High Risk Alerts: Malware Analysis for 10.11.110.41'. The status is 'Task Requested'. A task 'Re-image the machine' is shown in the right pane. The task details include: NAME: Re-image the machine, ASSIGNEE: Jose, PRIORITY: High, STATUS: New, and DESCRIPTION: Opened ticket ABC-2345 to re-image the affected machine.

In the Incidents List view, the incident status also changes to Task Requested.

The screenshot displays the NetWitness Respond interface showing the Incidents List view. The table lists incidents with columns: CREATED, PRIORITY, RISK, ID, NAME, STATUS, ASSIGNEE, and A... The incident INC-14 is highlighted with a status of 'Task Requested'.

CREATED	PRIORITY	RISK	ID	NAME	STATUS	ASSIGNEE	A...
04/12/2018 07:4...	CRITI...	100	INC-21235	High Risk Alerts: Malware Analysis for 12...	New		1
04/12/2018 07:3...	CRITI...	100	INC-21234	High Risk Alerts: Malware Analysis for 12...	New		2
04/04/2018 03:5...	CRITI...	100	INC-3396	High Risk Alerts: Malware Analysis for 12...	New		2
04/03/2018 02:2...	CRITI...	90	INC-31	High Risk Alerts: Malware Analysis for 10...	New		1
03/21/2018 08:0...	CRITI...	10	INC-26	High Risk Alerts: NetWitness Endpoint fo...	In Progress	deploy_admin	1
03/21/2018 07:5...	CRITI...	90	INC-14	High Risk Alerts: Malware Analysis for 10...	Task Requested	Analyst User	1
03/21/2018 07:5...	CRITI...	90	INC-13	High Risk Alerts: Malware Analysis for 10...	Task Requested		4
03/21/2018 07:5...	CRITI...	100	INC-12	High Risk Alerts: Malware Analysis for 10...	New		1
03/21/2018 07:5...	CRITI...	100	INC-11	High Risk Alerts: Malware Analysis for 10...	New		4
03/21/2018 07:5...	CRITI...	90	INC-10	High Risk Alerts: Malware Analysis for 10...	New		1
03/21/2018 07:5...	CRITI...	90	INC-9	High Risk Alerts: Malware Analysis for 10...	New		1
03/21/2018 07:5...	CRITI...	90	INC-8	High Risk Alerts: Malware Analysis for 10...	New		4
03/21/2018 07:5...	CRITI...	90	INC-7	High Risk Alerts: Malware Analysis for 10...	New		5
03/21/2018 07:5...	CRITI...	90	INC-6	High Risk Alerts: Malware Analysis for 10...	New		4
04/16/2018 07:3...	HIGH	50	INC-97526	Incident for UTE-8	Assigned	admin	1
04/12/2018 10:5...	HIGH	80	INC-97524	Suspected C&C with www.stvoblog.com	Assigned	Analyst User	1
04/12/2018 10:5...	HIGH	80	INC-97523	Suspected C&C with facebook	Assigned	Analyst User	1
04/12/2018 10:5...	HIGH	80	INC-97522	Suspected C&C with espn.starwave.com	Assigned	Analyst User	1
04/12/2018 10:5...	HIGH	80	INC-97521	Suspected C&C with facebook	New		1

Showing 1000 out of 97525 items | 0 selected

The task also appears in the Tasks list (RESPOND > Tasks), which shows a list of all incident tasks.

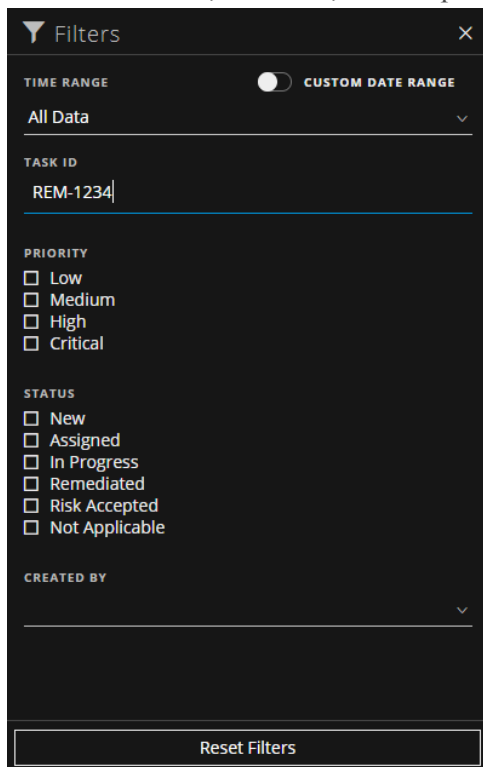
Note: If you do not see the status change, you may need to refresh your internet browser.

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.



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

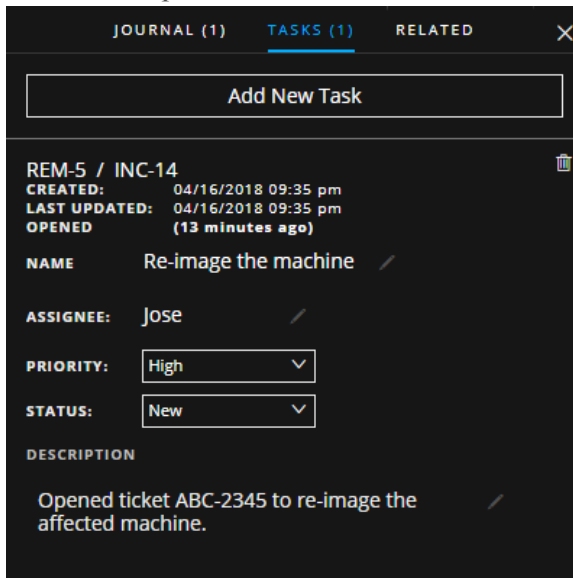
You can modify a task from within an incident and from the Tasks list. For example, you may want to show the status of the task as In Progress and add some additional information to the task. If the task is in a closed state (Not Applicable, Risk Accepted, or Remediated), you cannot modify the Priority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

To modify a Task from within an incident:

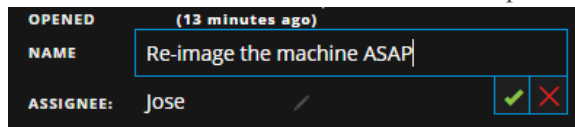
1. Go to **RESPOND > Incidents**.
The Incidents List view displays a list of all incidents.
2. Locate the incident that needs a task update and click the link in the **ID** or **NAME** field.

The Incident Details view opens.

3. In the toolbar at the top right of the view, select . The Journal panel opens.
4. Click 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.



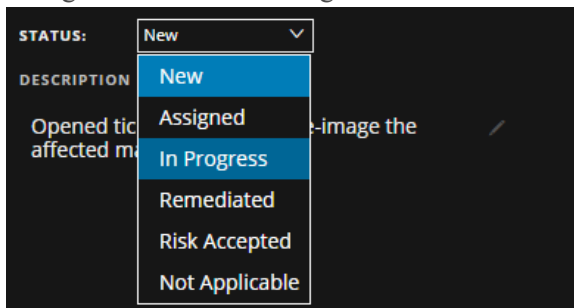
6. You can modify any of the following fields:
 - **NAME** - Click the current task name to open a text editor.



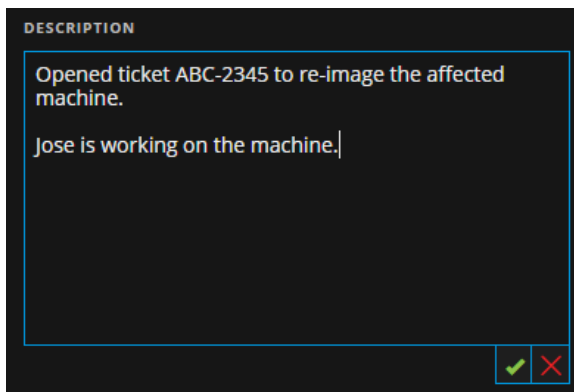
Click the check mark to confirm the change. For example, you can change "Re-image the machine" to "Re-image the machine ASAP."

- **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.

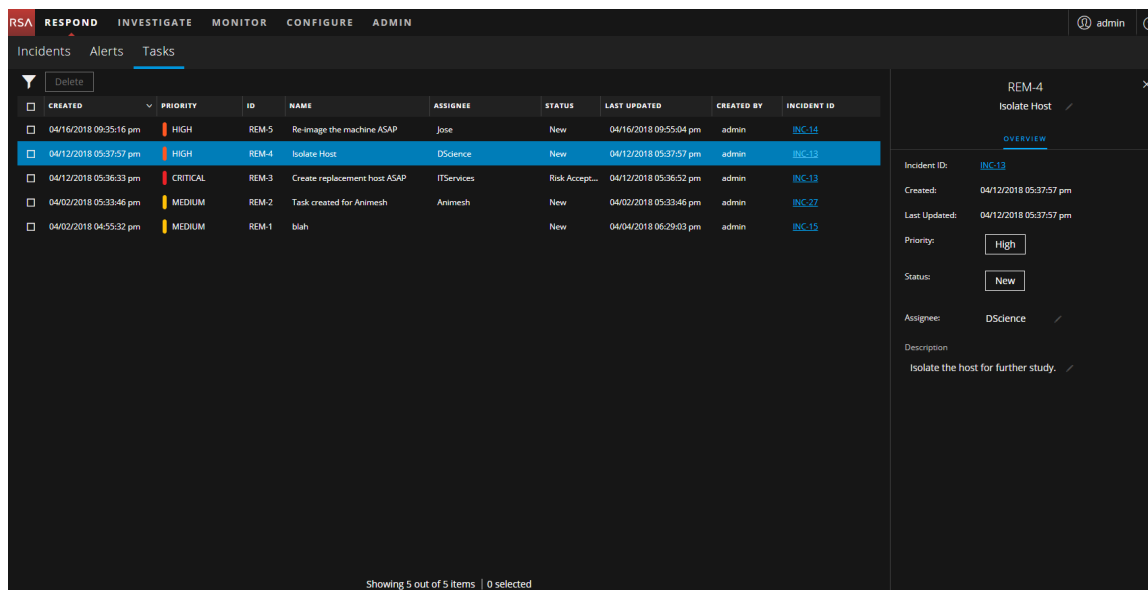


Modify the text and click the check mark to confirm the change.

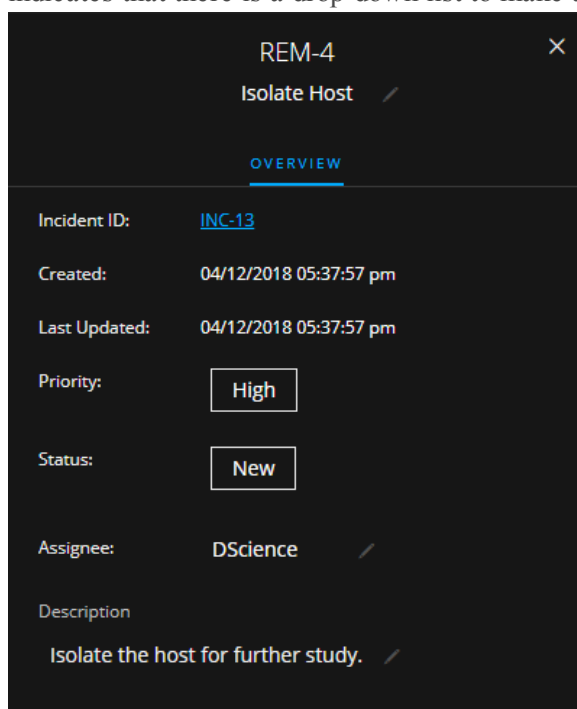
For each change that you make, you can see a confirmation that your change was successful.

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.

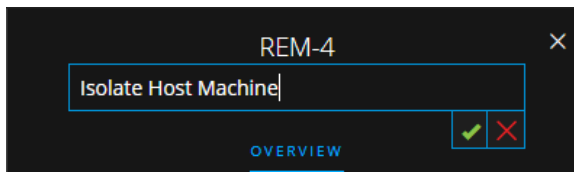


In the Task Overview panel, a pencil icon indicates a text field that you can change. A button indicates that there is a drop-down list to make a selection.



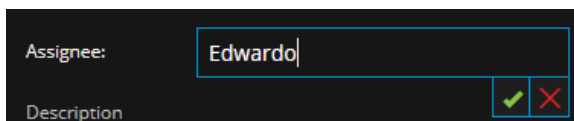
3. You can modify any of the following fields:

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



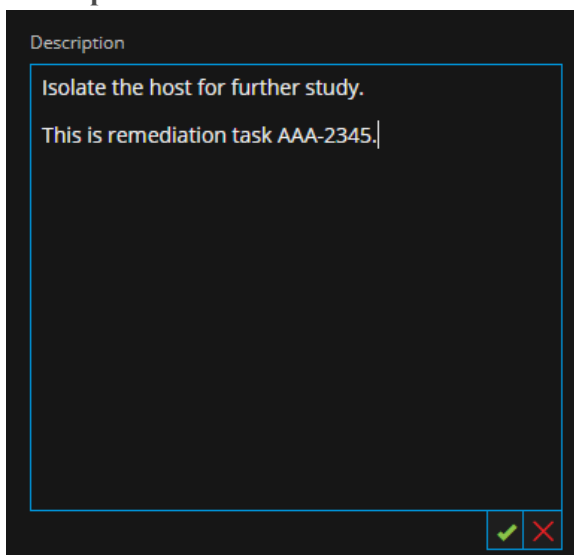
Click the check mark to confirm the change. For example, you can change Isolate Host to Isolate Host Machine.

- **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.

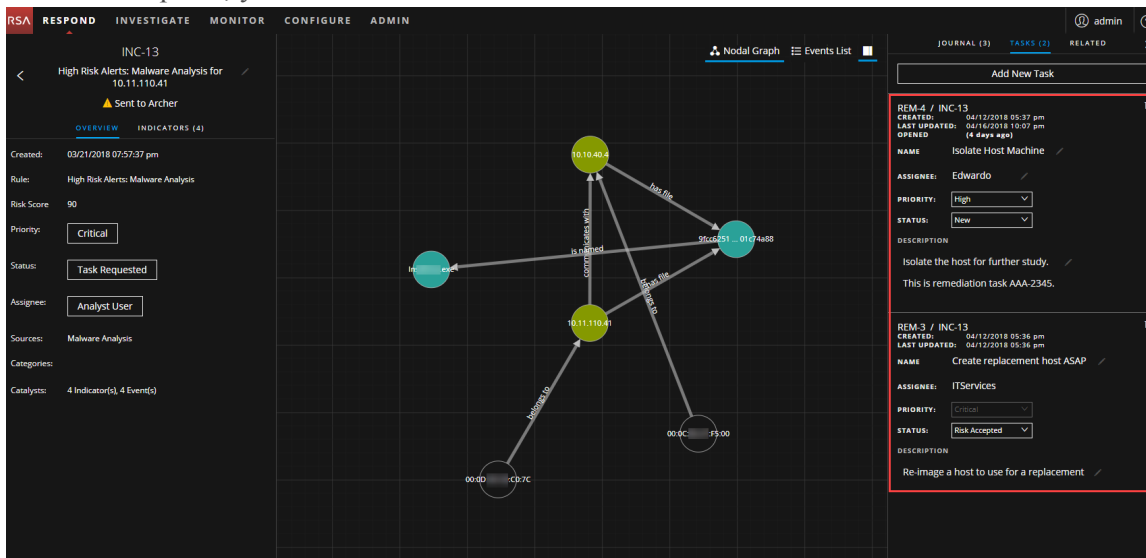
For each change that you make, you can see a confirmation that your change was successful.

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.

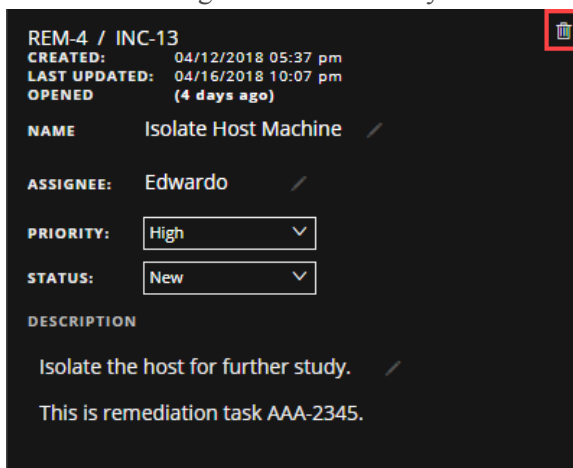
To Delete a Task from within an incident:

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. Click the **TASKS** tab.
5. In the Tasks panel, you can see the tasks created for the incident.



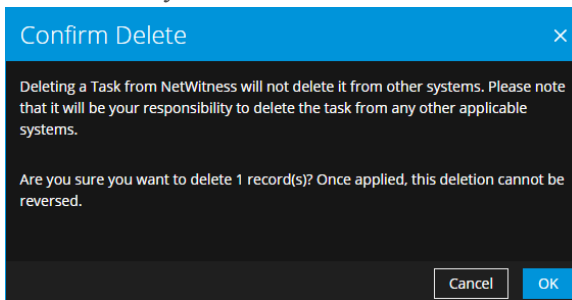
The screenshot shows the NetWitness Respond interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main area displays the Incident Details for INC-13. On the left, there's a sidebar with incident details like 'Created: 03/21/2018 07:57:37 pm', 'Rule: High Risk Alerts: Malware Analysis', 'Risk Score: 90', 'Priority: Critical', 'Status: Task Requested', 'Assignee: Analyst User', 'Sources: Malware Analysis', 'Categories:', and 'Catalysts: 4 Indicator(s), 4 Event(s)'. The central area shows a Nodal Graph with nodes representing IP addresses and their relationships. On the right, there's a panel with tabs for JOURNAL (3), TASKS (7), and RELATED. The TASKS tab is selected, showing a list of tasks. The task 'Isolate Host Machine' is highlighted with a red box.

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



The screenshot shows the task details for 'Isolate Host Machine'. The task is assigned to Edwardo, has a priority of High, and a status of New. The description is 'Isolate the host for further study. This is remediation task AAA-2345.' A red box highlights the delete icon in the top right corner.

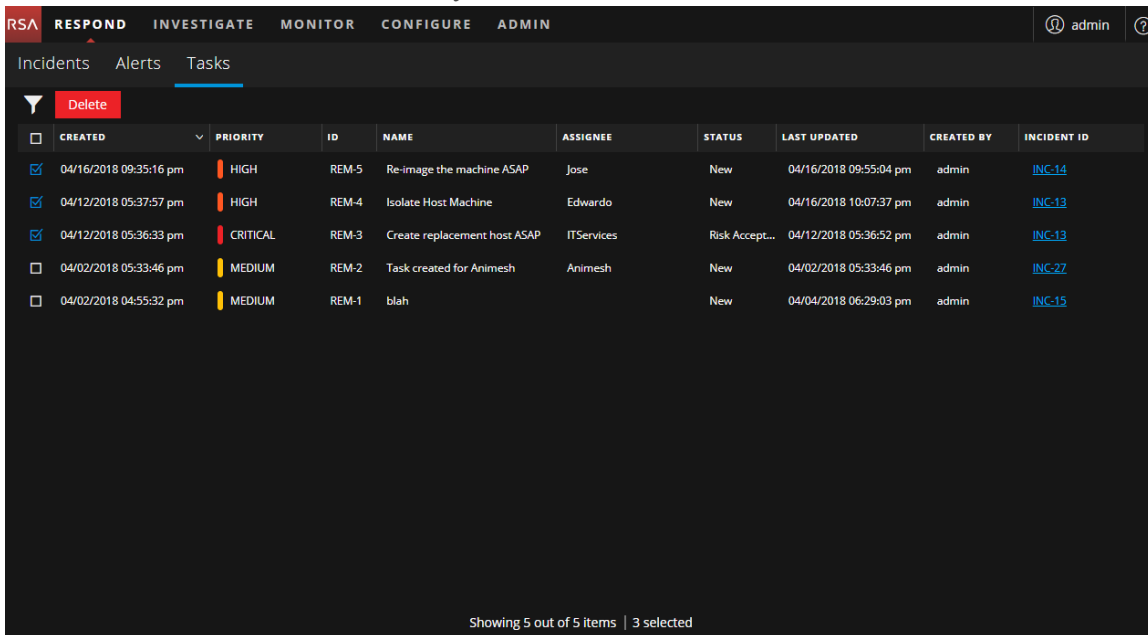
- Confirm that you want to delete the task and click **OK**.



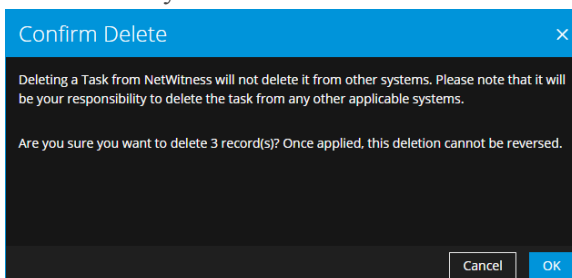
The task is deleted from NetWitness Platform. Deleting tasks from NetWitness Platform does not delete them from other systems.

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**.



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



The tasks are deleted from NetWitness Platform. Deleting tasks from NetWitness Platform 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 can 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 Platform 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, Risk Scoring, as well as many others. You can see the 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 on 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:

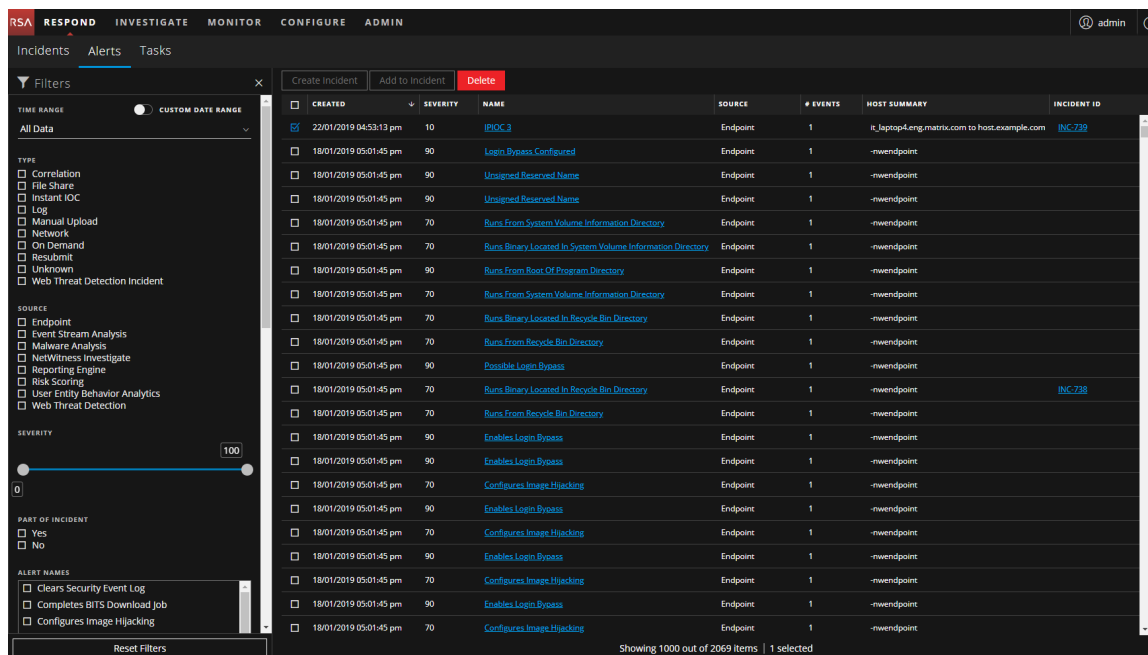
- [View Alerts](#)
- [Filter the Alerts List](#)
- [Remove My Filters from the Alerts List](#)
- [View Alert Summary Information](#)
- [View Event Details for an Alert](#)
- [Investigate Events](#)
- [Create an Incident Manually](#)
- [Add Alerts to an Incident](#)
- [Delete Alerts](#)

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 Platform 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, Risk Scoring, and many others. Note: In NetWitness Platform 11.3 and later, the Endpoint source includes Endpoint alerts from all NetWitness Endpoint versions. If one of the events in an alert has a <code>device_type</code> of <code>nwendpoint</code> , the source changes to Endpoint.
# 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.
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.

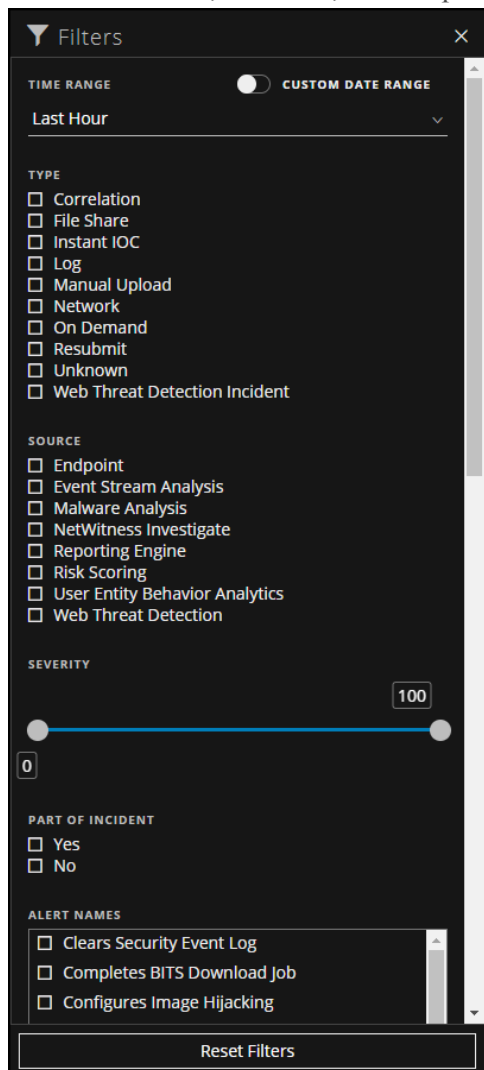
At the bottom of the list, you can see the number of alerts on the current page and the total number of alerts. For example: **Showing 1000 out of 2069 items**

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.



Filters

TIME RANGE ☐ CUSTOM DATE RANGE

Last Hour

TYPE

- ☐ Correlation
- ☐ File Share
- ☐ Instant IOC
- ☐ Log
- ☐ Manual Upload
- ☐ Network
- ☐ On Demand
- ☐ Resubmit
- ☐ Unknown
- ☐ Web Threat Detection Incident

SOURCE

- ☐ Endpoint
- ☐ Event Stream Analysis
- ☐ Malware Analysis
- ☐ NetWitness Investigate
- ☐ Reporting Engine
- ☐ Risk Scoring
- ☐ User Entity Behavior Analytics
- ☐ Web Threat Detection

SEVERITY

0 100

PART OF INCIDENT

- ☐ Yes
- ☐ No

ALERT NAMES

- ☐ Clears Security Event Log
- ☐ Completes BITS Download Job
- ☐ Configures Image Hijacking

Reset Filters

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 can 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. In NetWitness Platform 11.3 and later, if one of the events in an alert has a device_type of nwendpoint, Endpoint is included in the Type field.
- **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. In NetWitness Platform 11.3 and later, the **Endpoint** source includes Endpoint alerts from all NetWitness Endpoint versions. If one of the events in an alert has a device_type of nwendpoint, the source changes to Endpoint. A **Risk Scoring** source is available in NetWitness Platform 11.3 and later. NetWitness Respond automatically creates incidents from alerts that are over the specified file and host alert thresholds for risk score. For more information, see the *NetWitness Respond Configuration Guide*.
- **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 Platform 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.

RESPOND

INVESTIGATE

MONITOR

CONFIGURE

ADMIN

admin

Incidents Alerts Tasks

Create Incident

Add to Incident

Delete

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID
22/01/2019 04:53:13 pm	10	IPIOC3	Endpoint	1	it_laptop4.eng.matrix.com to h...	INC-739
18/01/2019 05:01:45 pm	90	Login Bypass Configured	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Unsigned Reserved Name	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Unsigned Reserved Name	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Runs From System Volume Information Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Runs Binary Located In System Volume Information Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Runs From Root Of Program Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Runs From System Volume Information Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Runs Binary Located In Recycle Bin Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Runs From Recycle Bin Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Possible Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Runs Binary Located In Recycle Bin Directory	Endpoint	1	-rwendpoint	INC-738
18/01/2019 05:01:45 pm	70	Runs From Recycle Bin Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-rwendpoint	

Showing 1000 out of 2069 items | 0 selected

Login Bypass Configured

OVERVIEW

Incident ID: (None)

Created: 18/01/2019 05:01:45 pm

Severity: 90

Source: Endpoint

Type: Endpoint

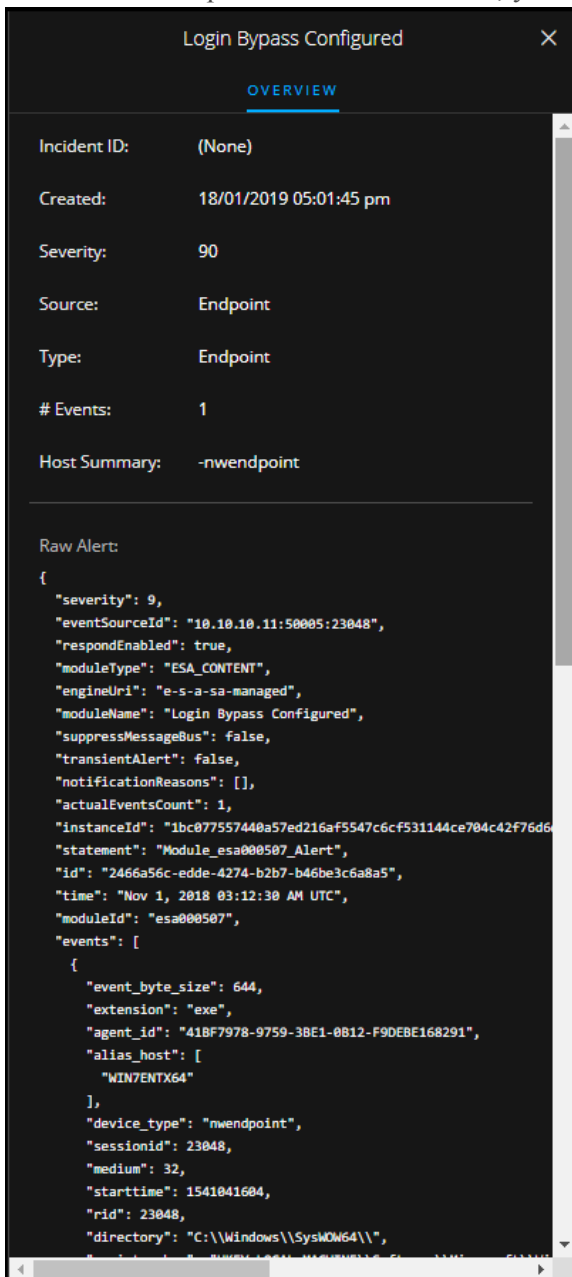
Events: 1

Host Summary: -rwendpoint

Raw Alert:

```
{
  "severity": 90,
  "eventSourceId": "18-18-18-11:50005:23000",
  "responseEnabled": true,
  "moduleType": "CIS_CONTAINER",
  "engineId": "e-s-a-s-a-managed",
  "moduleName": "Login Bypass Configured",
  "responseMessageId": "false",
  "responseAlert": false,
  "notificationReason": {},
  "notificationCount": 1,
  "instanceId": "18c07557440a7e2d26f9547dcf931146a706a62f7f06",
  "statement": "Module_rsa000507_Alert",
  "ip": "18c07557440a7e2d26f9547dcf931146a706a62f7f06",
  "time": "Nov 1, 2018 01:12:38 AM UTC",
  "module": "rsa000507",
  "events": [
    {
      "event_type": 644,
      "extension": "new",
      "agent_ip": "41879798-9759-38E1-8B12-F00E8168201",
      "alias_host": [
        "WIN787504"
      ],
      "device_type": "rwendpoint",
      "extension": "23000",
      "module": 32,
      "start_time": 1541861004,
      "year": 23000,
      "directory": "C:\\Windows\\System32\\",
    }
  ]
}
```

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



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 screenshot displays the NetWitness Respond interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The user is logged in as 'admin'. The main content area is divided into two panels. The left panel, titled 'RE bad rule', shows an overview of an alert with the following details:

- Incident ID: INC-91233
- Created: 04/04/2018 06:27:37 pm
- Severity: 50
- Source: Reporting Engine
- Type: Network
- # Events: 9
- Host Summary: 9 hosts to 2 hosts

Below the overview is a 'Raw Alert' section containing a JSON object with details about the alert, including severity, signature, risk score, name, source, data source port, data source host, and a list of events.

The right panel, titled '9 events', displays a table of events. The table has the following columns: TIME, TYPE, SOURCE IP, SOURCE PORT, SOURCE HOST, SOURCE MAC, SOURCE USER, DESTINATION IP, and DESTINATION PORT. The events are listed as follows:

TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION PORT
04/04/2018 06:25:35.000 pm	Network	10.4.61.17	53529		00:50:56:33:10:6D		10.4.61.32	5671
04/04/2018 06:25:35.000 pm	Network	10.4.61.17	42388		00:50:56:33:10:6D		10.4.61.32	5671
04/04/2018 06:25:36.000 pm	Network	10.4.61.17	38494		00:50:56:33:10:6D		10.4.61.32	5671
04/04/2018 06:25:36.000 pm	Network	10.4.61.17	41763		00:50:56:33:10:6D		10.4.61.32	5671
04/04/2018 06:25:44.000 pm	Network	10.4.61.32	123		00:50:56:33:10:6E		10.4.61.17	123
04/04/2018 06:26:05.000 pm	Network	10.4.61.17	40944		00:50:56:33:10:6D		10.4.61.32	5671
04/04/2018 06:26:05.000 pm	Network	10.4.61.17	46346		00:50:56:33:10:6D		10.4.61.32	5671
04/04/2018 06:26:06.000 pm	Network	10.4.61.17	48759		00:50:56:33:10:6D		10.4.61.32	5671
04/04/2018 06:26:06.000 pm	Network	10.4.61.17	44657		00:50:56:33:10:6D		10.4.61.32	5671

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
04/04/2018 06:27:37 pm	50	RE bad rule	Reporting Engine	9	9 hosts to 2 hosts	INC-91233
04/04/2018 06:26:36 pm	50	RE bad rule	Reporting Engine	10	10 hosts to 3 hosts	INC-91233
04/04/2018 06:25:36 pm	50	RE bad rule	Reporting Engine	9	9 hosts to 2 hosts	INC-91232
04/04/2018 06:24:36 pm	50	RE bad rule	Reporting Engine	10	10 hosts to 3 hosts	INC-11169
04/04/2018 06:23:36 pm	50	RE bad rule	Reporting Engine	14	14 hosts to 4 hosts	INC-91231
04/04/2018 06:22:36 pm	50	RE bad rule	Reporting Engine	12	12 hosts to 5 hosts	INC-24016
04/04/2018 06:21:37 pm	50	RE bad rule	Reporting Engine	12	12 hosts to 5 hosts	INC-11169
04/04/2018 06:20:36 pm	50	RE bad rule	Reporting Engine	10	10 hosts to 3 hosts	INC-24016
04/04/2018 06:19:36 pm	50	RE bad rule	Reporting Engine	10	10 hosts to 3 hosts	INC-11169
04/04/2018 06:18:37 pm	50	RE bad rule	Reporting Engine	9	9 hosts to 4 hosts	INC-25522
04/04/2018 06:17:36 pm	50	RE bad rule	Reporting Engine	10	10 hosts to 3 hosts	INC-11169
04/04/2018 06:16:36 pm	50	RE bad rule	Reporting Engine	12	12 hosts to 5 hosts	INC-11169
04/04/2018 06:15:37 pm	50	RE bad rule	Reporting Engine	13	13 hosts to 4 hosts	INC-11169
04/04/2018 06:14:36 pm	50	RE bad rule	Reporting Engine	9	9 hosts to 4 hosts	INC-11169
04/04/2018 06:13:36 pm	50	RE bad rule	Reporting Engine	11	11 hosts to 4 hosts	INC-25522
04/04/2018 06:12:37 pm	50	RE bad rule	Reporting Engine	12	12 hosts to 3 hosts	INC-11169
04/04/2018 06:11:36 pm	50	RE bad rule	Reporting Engine	15	15 hosts to 6 hosts	INC-91230
04/04/2018 06:10:36 pm	50	RE bad rule	Reporting Engine	11	11 hosts to 5 hosts	INC-91229
04/04/2018 06:09:37 pm	50	RE bad rule	Reporting Engine	12	12 hosts to 3 hosts	INC-11169

Showing 1000 out of 3180 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
04/04/2018 06:22:35.000 pm	Network	10.4.61.17	37402		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:22:35.000 pm	Network	10.4.61.17	60659		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:22:36.000 pm	Network	10.4.61.17	52606		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:22:36.000 pm	Network	10.4.61.17	36908		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:23:05.000 pm	Network	10.4.61.17	50398		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:23:05.000 pm	Network	10.4.61.17	59281		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:23:06.000 pm	Network	10.4.61.17	38498		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:23:06.000 pm	Network	10.4.61.17	25132		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:23:28.000 pm	Network	10.4.61.32	56004		00:50:56:33:10:6E		10.4.61.17	45182		00:50:56:33:10:6D
04/04/2018 06:23:33.000 pm	Network	10.4.61.32	123		00:50:56:33:10:6E		10.4.61.17	123		00:50:56:33:10:6D

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.
SOURCE IP	Shows the source IP address if there was a transaction between two machines.

Column	Description
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 see only the event details for that event instead of a list.

- 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.

Event Details
04/04/2018 06:22:35 pm

Back To Table < 1 of 10 >

Incident ID: INC-11169		Timestamp: 04/04/2018 06:22:35.000 pm (13 days ago)		
Created: 04/04/2018 06:24:36 pm		Type: Network		
Severity: 50		Source:		
Sources: Reporting Engine		Device	Port 37402	
Type: Network		MAC Address	00:50:56:33:10:6D	
# Events: 10		IP Address	10.4.61.17	
Host Summary: 10 hosts to 3 hosts		Geolocation		
Raw Alert:		Destination:		
<pre>{ "severity": 5, "signature_id": "RULE_08_20180403163411", "risk_score": 1, "name": "RE bad rule", "source": "RSA - Reporting Engine", "datasource_port": "56005", "datasource_host": "10.4.61.44", "events": [{ "ip_proto": "0", "lifetime": "0", "ip_src": "10.4.61.17", "media": "IP", "sessionId": "201710", "rid": "186080", "inv_context": "event analysis,protocol analysis", "packets": "28", "feed_name": "Investigation", "threat_category": "nonstandard", "eth_src": "08:50:56:33:10:6D", "analysis_service": "ssl over non-standard port", "payload": "2337", "tcp_flags": "33", "alert_id": "bad08053", "risk_info": "ssl over non-standard port", "direction": "lateral", "tcp_dstport": "5671", "tcp_srcport": "37402" }] }</pre>		User		
		Device	Port 5671	
		MAC Address	00:50:56:33:10:6E	
		IP Address	10.4.61.32	
		Geolocation		
		Detector:		
		Size	4175	
		Data	Size 4175	
		Related Links:	Type investigate_original_event	
			URL /investigation/host/10.4.61.44:56005/navigate/event/AUTO/201710	
Event Source:	10.4.61.44:56005			
Analysis Service:	ssl over non-standard port			
Event Source Id:	201710			
Site Categorization:	nonstandard			

- 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.

The screenshot displays the NetWitness Respond interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The user is logged in as 'admin'. The left sidebar shows incident details for 'INC-11169', including creation time, severity, source, type, number of events, and host summary. The main panel is titled 'Event Details' for the timestamp '04/04/2018 06:23:33 pm'. It features a 'Back To Table' button and a navigation control '< 10 of 10 >'. Below this, there are sections for 'Source' and 'Destination' with details like Device, Port, MAC Address, IP Address, and Geolocation. The 'Detector' section shows 'Size' and 'Data'. The 'Related Links' section includes 'investigate_original_event' and a URL. The 'Event Source' and 'Event Source Id' are also listed. The 'Raw Alert' section shows a JSON representation of the event data.

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.

TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION PORT
09/26/2018 04:33:44.000 ...	Network	192.168.1.110	20		00:01:01:01:80:34		192.168.1.112	1828
09/26/2018 04:33:44.000 ...	Network	192.168.1.110	20		00:01:01:01:80:34		192.168.1.112	1829
09/26/2018 04:33:44.000 ...	Network	192.168.1.110	20		00:01:01:01:80:34		192.168.1.112	1830
09/26/2018 04:33:45.000 ...	Network	192.168.1.110	20		00:01:01:01:80:34		192.168.1.112	1831
09/26/2018 04:33:45.000 ...	Network	192.168.1.110	20		00:01:01:01:80:34		192.168.1.112	1832
09/26/2018 04:33:45.000 ...	Network	192.168.1.110	20		00:01:01:01:80:34		192.168.1.112	1833

The following figure shows underlined entities in the Events Details.

Entity	Value
Timestamp	09/26/2018 04:33:44.000 pm 4 months ago
Type	Network
Source	Device: Port 20, MAC Address 00:01:01:01:80:34, IP Address 192.168.1.110, Geolocation
Target	Device: Port 1828, MAC Address 00:20:50:50:EF:7E, IP Address 192.168.1.112, Geolocation
Detector	User
Size	2044
Data	Size 2044
Event Source	10.10.10.38:56003
Analysis Service	ftp over non-standard port
Event Source ID	4210220

The Context Hub is preconfigured with meta fields mapped to the entities. NetWitness Respond and NetWitness 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 > Investigation > 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 screenshot shows the 'Event Details' page for an event on 03/21/2019 at 04:25:43 am. The event is of type 'Network'. The source is a device with port 20 and MAC address 00:00:29:E7:E7:AB. The target is a device with IP address 192.168.00.00. A context tooltip is displayed over the IP address, showing 'CONTEXT HIGHLIGHTS' and 'ACTIONS'.

CONTEXT HIGHLIGHTS		
27 INCIDENTS	35 ALERTS	1 LISTS
- ENDPOINT	- LIVECONNECT	- CRITICALITY
- ASSET RISK		

[View Context](#)

ACTIONS
≡ Add/Remove from List
🔍 Pivot to Investigate > Navigate
🔍 Pivot to Investigate > Hosts/Files
🔍 Pivot to Endpoint Thick Client
🔍 Pivot to Archer

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

This is a close-up of the context tooltip shown in the previous image. It displays the IP address 192.168.00.00 and the context highlights and actions sections.

CONTEXT HIGHLIGHTS		
27 INCIDENTS	35 ALERTS	1 LISTS
- ENDPOINT	- LIVECONNECT	- CRITICALITY
- ASSET RISK		

[View Context](#)

ACTIONS
≡ Add/Remove from List
🔍 Pivot to Investigate > Navigate
🔍 Pivot to Investigate > Hosts/Files
🔍 Pivot to Endpoint Thick Client
🔍 Pivot to Archer

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 27 related incidents, 35 related alerts, and one list associated with the selected IP address. There is no information for Endpoint, Live Connect, Criticality, or Asset Risk.

The **Actions** section lists the available actions. In the above example, the Add/Remove From List,

Pivot to Investigate > Navigate, and Pivot to Endpoint Thick Client options are available.

Note: The Pivot to Archer link is disabled when Archer data is not available or when the Archer Datasource is not responding. Check that the RSA Archer configuration is enabled and configured properly.

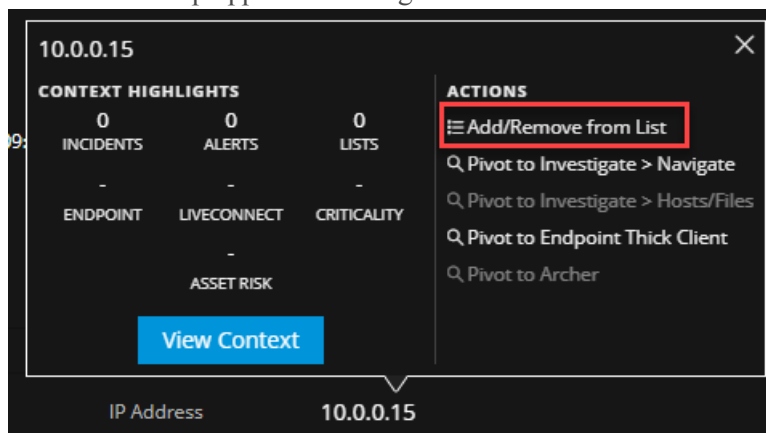
For more information, see [Pivot to Investigate > Navigate](#), [Pivot to Investigate > Hosts/Files](#), [Pivot to Archer](#), [Pivot to Endpoint Thick Client](#), and [Add an Entity to a Whitelist](#).

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.

Add/Remove from List ⓘ ✕

Click on Save to update the list(s). Refresh the page to view the updates.

META VALUE
10.0.0.15

[Create New List](#) >

ALL **SELECTED** **UNSELECTED** Filter Results

LIST	DESCRIPTION
<input type="checkbox"/> Threat	This list is created and updated automatically by the feed Threat. If you make changes to this list, please be aware that the changes will be overwritten when the feed updates.
<input type="checkbox"/> CorporateUsers	This list is created and updated automatically by the feed CorporateUsers. If you make changes to this list, please be aware that the changes will be overwritten when the feed updates.
<input checked="" type="checkbox"/> IP_Whitelist	
<input type="checkbox"/> SpearPhishing	This list is created and updated automatically by the feed SpearPhishing. If you make changes to this list, please be aware that the changes will be

Cancel Save

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 Investigate > Navigate

For a more thorough investigation of the incident, you can access the Investigate Navigate 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 > Navigate**.
The Investigate Navigate view opens, which enables you to perform a deeper dive investigation.

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

Pivot to Investigate > Hosts/Files

For a more thorough information about specific Hosts and Files, you can access the Investigate Hosts and Files views.

1. In the Events List or Event Details in the Alert Details view, hover over any entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Investigate > Hosts/Files**.
If you hover over a host or IP or MAC address entity and click **Pivot to Investigate > Hosts/Files**, it displays the **Investigate > Hosts** view with a specific host listed.
If you hover over a filename or file hash entity and click **Pivot to Investigate > Hosts/Files** it displays the **Investigate > Files** view with a specific file listed.

Note: By default, the search for entities is on the previously selected Endpoint Server. However, you can select a different Endpoint Server to fetch the information or data.

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

Pivot to Endpoint Thick Client

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.

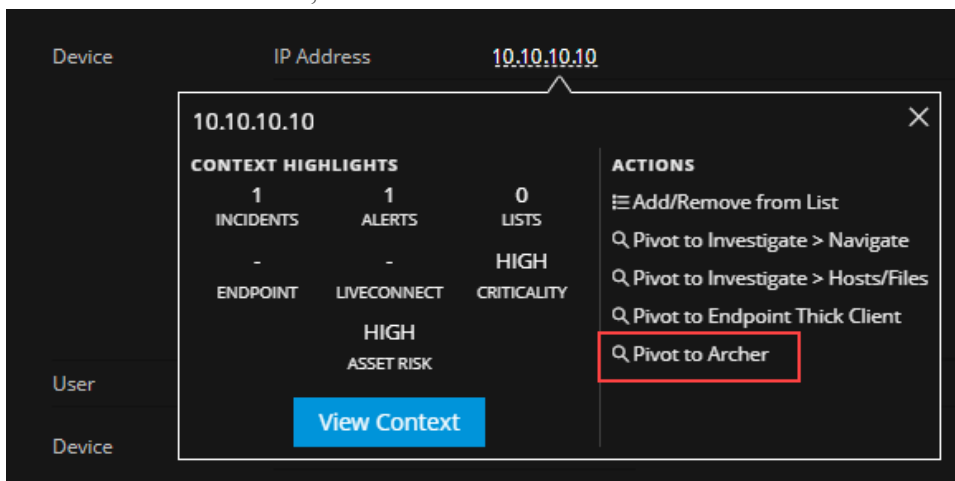
1. In the Events List or Event Details in the Alert Details view, hover over any underlined entity to access a context tooltip.
2. In the **ACTIONS** section of the tooltip, select **Pivot to Endpoint Thick Client**.
The NetWitness Endpoint thick client application opens outside of your web browser.

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

Pivot to Archer

For viewing more details about a device in RSA Archer Cyber Incident & Breach Response, you can pivot to the device details page. This information is displayed only for IP address, host, and 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, select **Pivot to Archer**.



3. The device details page in **RSA Archer Cyber Incident & Breach Response** opens if you are logged in to the application, otherwise the login screen is displayed.

The screenshot shows the RSA Archer GRC interface for the device ECAT-WIN-2008. The top navigation bar includes tabs for Audit Management, Issue Management, and Operational Risk Management, along with a 'SHOW ALL' button and a search icon. The main content area is titled 'ECAT-WIN-2008 Devices' and includes a toolbar with actions like NEW, COPY, SAVE, EDIT, DELETE, RELATED, RECALCULATE, EXPORT, PRINT, and EMAIL. The 'GENERAL INFORMATION' section displays the following details:

- Device ID: DID-224935
- Device Name: ECAT-WIN-2008
- Type: Fibre Channel SAN Switch
- Record Status: Updated
- Category:
- Business Unit: [Payroll](#) [US-Finance](#)
- Description:

The 'PERSONNEL' section shows the following information:

- Device Owner: 1, Admin1
- Device Manager: 2, admin
- Alternate Administrator(s):

The bottom of the interface features a footer with the RSA Archer GRC logo, the text 'Enterprise Governance, Risk and Compliance', and the version 'Version 6.2 P1'.

Note: The Pivot to Archer link is disabled when Archer data is not available or when the Archer Datasource is not responding. Check that the RSA Archer configuration is enabled and configured properly.

For more information, see the *RSA Archer Integration 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.

In version 11.2 and later, you can change the assignee, category, and priority when you create an incident manually from alerts.

In version 11.1, 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 in version 11.1.

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.

NSA

RESPOND

INVESTIGATE

MONITOR

CONFIGURE

ADMIN

admin

Incidents

Alerts

Tasks

Create Incident

Add to Incident

Delete

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID
<input checked="" type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
<input checked="" type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA_Session ID	Event Stream Analysis	1	-unknown	
<input checked="" type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA_Session ID	Event Stream Analysis	1	Router-junosrouter	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA_Session ID	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA_Session ID	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	Router-junosrouter	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA_Session ID	Event Stream Analysis	1	Router-junosrouter	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	Router-junosrouter	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA_Session ID	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA_Session ID	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA_Session ID	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
<input type="checkbox"/> 04/03/2018 04:42:03 pm	70	ESA_Session ID	Event Stream Analysis	1	-unknown	

Showing 1000 out of 30239 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

PRIORITY

MEDIUM

ASSIGNEE

ANALYST USER

CATEGORIES

HACKING: USE OF STOLEN CRED

Cancel OK

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

5. In the **PRIORITY** field, select a priority for the incident. The priority defaults to Low.

6. (Optional) If you are ready to assign the incident, in the **ASSIGNEE** field, select a specific user.
7. (Optional) In the **CATEGORIES** field, you can select a category to classify the incident, such as Hacking: Use of Stolen Creds. This is also helpful when trying to locate the incident later using the incidents filter.
8. Click **OK**.

You can 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.

The screenshot shows the NetWitness Respond interface. At the top, there's a navigation bar with tabs: INCIDENTS, ALERTS, TASKS, and a dropdown menu. A green confirmation message is displayed: "You successfully created the incident INC-97566 from the selected alerts." Below this, there's a table of alerts. The table has columns: CREATED, SEVERITY, NAME, SOURCE, # EVENTS, HOST SUMMARY, and INCIDENT ID. Three rows are highlighted with a red border, showing the incident ID INC-97566 for each alert.

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	INC-97566
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	-unknown	INC-97566
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	INC-97566
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	Router-junosrouter	
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	Router-junosrouter	
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	Router-junosrouter	
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	Router-junosrouter	
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA Rule	Event Stream Analysis	1	-unknown	
04/03/2018 04:42:03 pm	70	ESA - Session ID	Event Stream Analysis	1	-unknown	

Showing 1000 out of 30239 items | 3 selected

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 to high or assigning the incident to another user. The following figure shows the Incident Details view Overview panel for the new incident.

INC-97566

Investigate - IP

Send to Archer

OVERVIEW INDICATORS

Created: 04/23/2018 10:08:03 pm

By: admin

Risk Score: 70

Priority: Medium

Status: Assigned

Assignee: Analyst User

Sources: Event Stream Analysis

Categories: Hacking: Use of stolen creds

Catalysts: 3 Indicator(s), 3 Event(s)

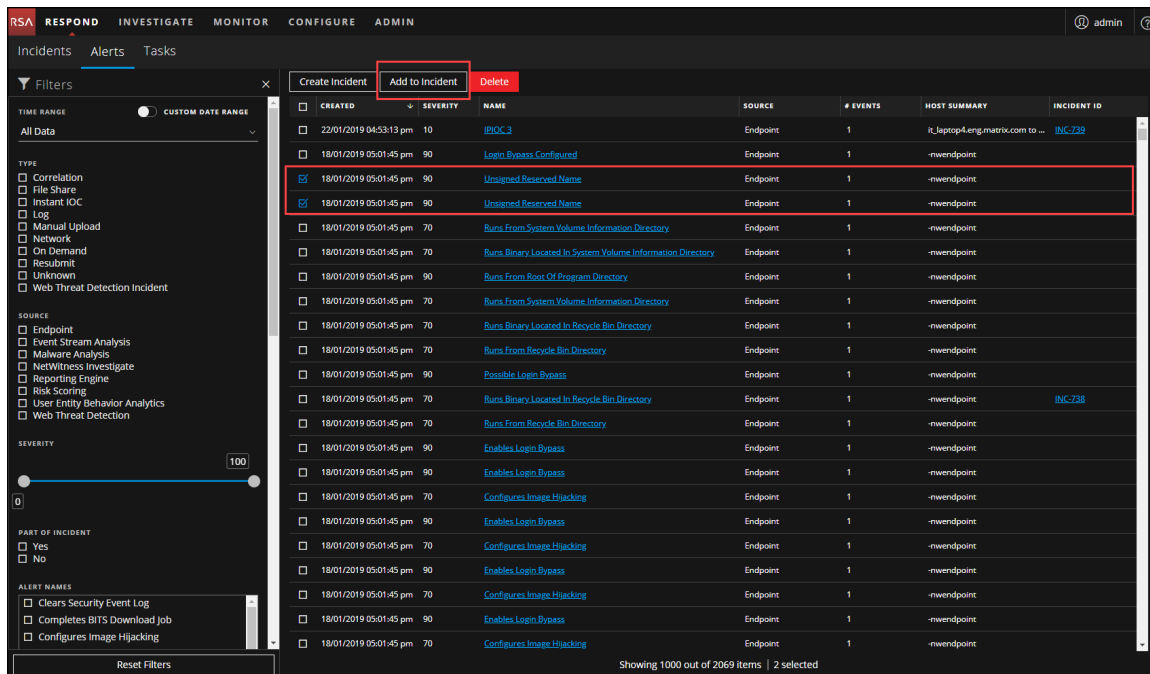
Add Alerts to an Incident

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**.

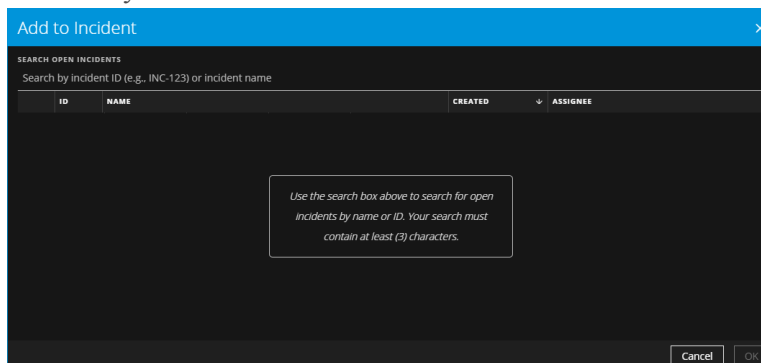
Note: Selecting alerts that do not have incident IDs enable the **Add to Incident** button. If the alert is already part of an incident, the button is disabled. You can filter alerts that are not part of an incident by selecting the option **PART OF INCIDENT** as **No** in the Filters panel.



The screenshot shows the NetWitness Respond interface. The 'Add to Incident' dialog box is open, and the 'Add to Incident' button is highlighted. The main table lists various incidents with columns for ID, NAME, CREATED, SEVERITY, and ASSIGNEE. The incident INC-739 is selected.

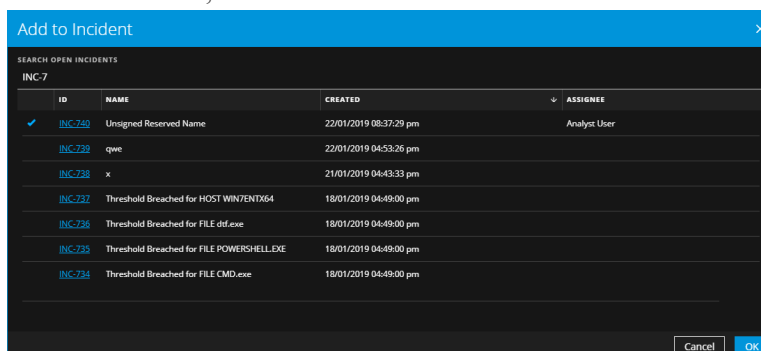
ID	NAME	CREATED	SEVERITY	ASSIGNEE
INC-739	Unsigned Reserved Name	22/01/2019 08:37:29 pm	90	Analyst User
INC-739	qwe	22/01/2019 04:53:26 pm	90	
INC-738	x	21/01/2019 04:43:33 pm	90	
INC-737	Threshold Breached for HOST WIN7/NTLMA	18/01/2019 04:49:00 pm	90	
INC-736	Threshold Breached for FILE dtd.exe	18/01/2019 04:49:00 pm	90	
INC-735	Threshold Breached for FILE POWERSHELL.EXE	18/01/2019 04:49:00 pm	90	
INC-734	Threshold Breached for FILE CMD.exe	18/01/2019 04:49:00 pm	90	

- 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**.



The screenshot shows the 'Add to Incident' dialog box. The search field is empty, and a message提示 is displayed: "Use the search box above to search for open incidents by name or ID. Your search must contain at least (3) characters."

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



The screenshot shows the 'Add to Incident' dialog box. The search field contains 'INC-7', and the results list shows several incidents. The incident INC-740 is selected.

ID	NAME	CREATED	ASSIGNEE
INC-740	Unsigned Reserved Name	22/01/2019 08:37:29 pm	Analyst User
INC-739	qwe	22/01/2019 04:53:26 pm	
INC-738	x	21/01/2019 04:43:33 pm	
INC-737	Threshold Breached for HOST WIN7/NTLMA	18/01/2019 04:49:00 pm	
INC-736	Threshold Breached for FILE dtd.exe	18/01/2019 04:49:00 pm	
INC-735	Threshold Breached for FILE POWERSHELL.EXE	18/01/2019 04:49:00 pm	
INC-734	Threshold Breached for FILE CMD.exe	18/01/2019 04:49:00 pm	

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

The screenshot displays the NetWitness Respond Alerts interface. A green notification banner at the top states "You successfully added the selected alerts to INC-740." The interface shows a list of alerts with columns: CREATED, SEVERITY, NAME, SOURCE, # EVENTS, HOST SUMMARY, and INCIDENT ID. Two alerts are selected and highlighted with a red box, both with the incident ID "INC-740". The left sidebar contains filters for TYPE, SOURCE, SEVERITY, PART OF INCIDENT, and ALERT NAMES. The bottom status bar indicates "Showing 1000 out of 2069 items | 2 selected".

CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID
22/01/2019 04:53:13 pm	10	@IOC 2	Endpoint	1	it_laptop4-eng.matrix.com to ...	INC-729
18/01/2019 05:01:45 pm	90	Login Bypass Configured	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Unsigned Reserved Name	Endpoint	1	-rwendpoint	INC-740
18/01/2019 05:01:45 pm	90	Unsigned Reserved Name	Endpoint	1	-rwendpoint	INC-740
18/01/2019 05:01:45 pm	70	Burns From System Volume Information ...	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Burns Binary Located In System Volume I...	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Burns From Root Of Program Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Burns From System Volume Information ...	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Burns Binary Located In Recycle Bin Direc...	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Burns From Recycle Bin Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Possible Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Burns Binary Located In Recycle Bin Direc...	Endpoint	1	-rwendpoint	INC-738
18/01/2019 05:01:45 pm	70	Burns From Recycle Bin Directory	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Configures Image Hijacking	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Configures Image Hijacking	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Configures Image Hijacking	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-rwendpoint	
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-rwendpoint	

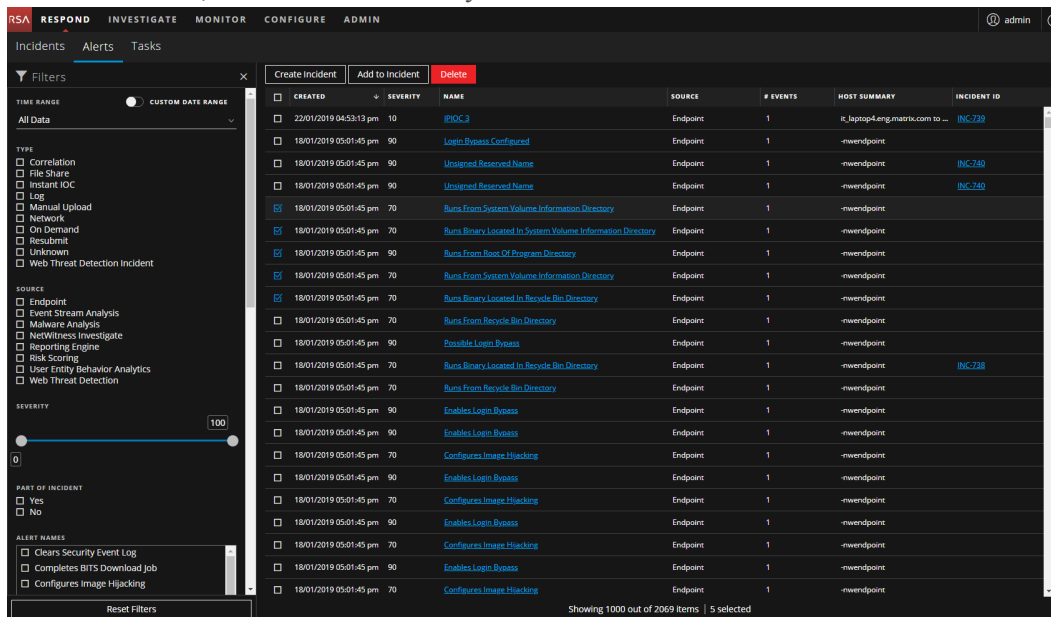
Delete Alerts

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**.

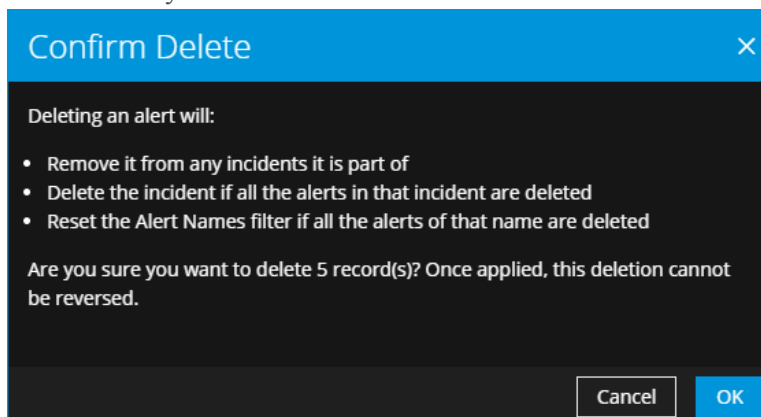
The Alerts List view displays a list of all NetWitness Platform alerts.

- 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 Platform. 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

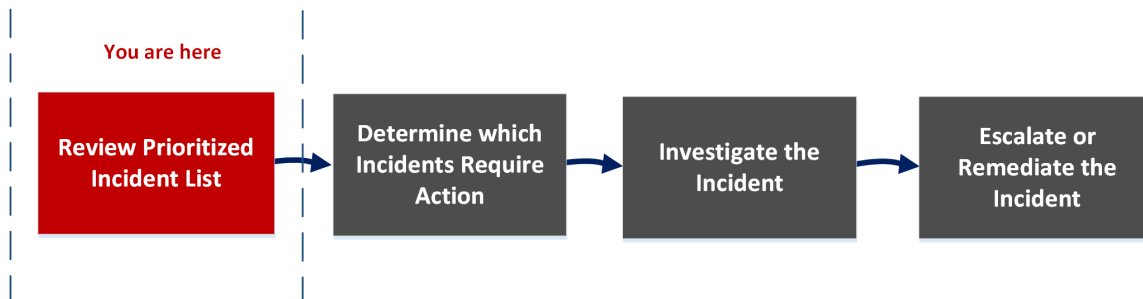
- [Incidents List View](#)
- [Incident Details View](#)
- [Alerts List View](#)
- [Alert Details View](#)
- [Tasks List View](#)
- [Add/Remove from List Dialog](#)
- [Context Lookup Panel - Respond View](#)

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 Platform.



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	Send an incident to Archer Cyber Incident & Breach Response or 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.

The figure consists of two screenshots of the NetWitness Respond interface. The top screenshot shows the 'Incidents' list view. On the left is a 'Filters' panel (labeled 1) with sections for 'TIME RANGE', 'INCIDENT ID', 'PRIORITY', 'STATUS', 'ASSIGNEE', and 'CATEGORIES'. The main area is a table of incidents (labeled 2) with columns: 'CREATED', 'PRIORITY', 'RISK SCORE', 'ID', 'NAME', 'STATUS', 'ASSIGNEE', and 'ALERTS'. The bottom screenshot shows the 'Incident Details' view for incident INC-1707 (labeled 3). On the right is an 'Overview' panel with details like 'Created', 'Rule', 'Risk Score', 'Priority', 'Status', 'Assignees', 'Sources', 'Categories', and 'Catalysts'. On the left is a detailed list of incidents related to INC-1707, with columns similar to the top screenshot.

- 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.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
06/04/2018 04:59:52 pm	CRITICAL	90	INC-1707	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
06/04/2018 04:11:51 pm	CRITICAL	90	INC-1706	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 08:31:50 pm	CRITICAL	90	INC-1705	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 07:42:00 pm	CRITICAL	90	INC-1704	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1702	ESA	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1701	High Risk Alerts: ESA for 10.0.0.111	New		4
05/31/2018 05:24:52 pm	HIGH	80	INC-1700	High Risk Alerts: ESA for 10.0.0.48	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1699	High Risk Alerts: ESA for 10.0.0.196	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1698	High Risk Alerts: ESA for 10.0.0.111	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1697	High Risk Alerts: ESA for 10.0.0.196	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1696	High Risk Alerts: ESA for 10.0.0.53	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1695	High Risk Alerts: ESA for 10.0.1.20	New		1
05/31/2018 05:24:52 pm	MEDIUM	80	INC-1694	High Risk Alerts: ESA for 10.0.1.23	Assigned		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1693	High Risk Alerts: ESA for 10.0.2.232	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1692	High Risk Alerts: ESA for 10.0.3.93	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1691	High Risk Alerts: ESA for 10.0.0.166	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1690	High Risk Alerts: ESA for 10.0.0.28	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1689	High Risk Alerts: ESA for 10.0.3.140	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1688	High Risk Alerts: ESA for 10.0.3.142	New		1

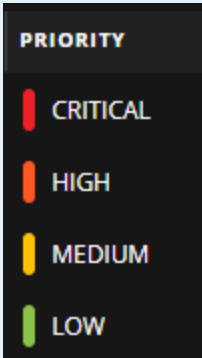
The following figure shows the Incidents List on the left and the Incidents Overview panel on the right.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
06/04/2018 04:59:52 pm	CRITICAL	90	INC-1707	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
06/04/2018 04:11:51 pm	CRITICAL	90	INC-1706	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 08:31:50 pm	CRITICAL	90	INC-1705	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 07:42:00 pm	CRITICAL	90	INC-1704	High Risk Alerts: Reporting Engine for 10.100.33.1	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1702	ESA	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1701	High Risk Alerts: ESA for 10.0.0.111	New		4
05/31/2018 05:24:52 pm	HIGH	80	INC-1700	High Risk Alerts: ESA for 10.0.0.48	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1699	High Risk Alerts: ESA for 10.0.0.196	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1698	High Risk Alerts: ESA for 10.0.0.111	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1697	High Risk Alerts: ESA for 10.0.0.196	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1696	High Risk Alerts: ESA for 10.0.0.53	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1695	High Risk Alerts: ESA for 10.0.1.20	New		1
05/31/2018 05:24:52 pm	MEDIUM	80	INC-1694	High Risk Alerts: ESA for 10.0.1.23	Assigned		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1693	High Risk Alerts: ESA for 10.0.2.232	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1692	High Risk Alerts: ESA for 10.0.3.93	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1691	High Risk Alerts: ESA for 10.0.0.166	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1690	High Risk Alerts: ESA for 10.0.0.28	New		2
05/31/2018 05:24:52 pm	HIGH	80	INC-1689	High Risk Alerts: ESA for 10.0.3.140	New		1
05/31/2018 05:24:52 pm	HIGH	80	INC-1688	High Risk Alerts: ESA for 10.0.3.142	New		1

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.

Column	Description
PRIORITY	<p>Shows the incident priority. Priority can be Critical, High, Medium or Low.</p> <p>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:</p> 
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

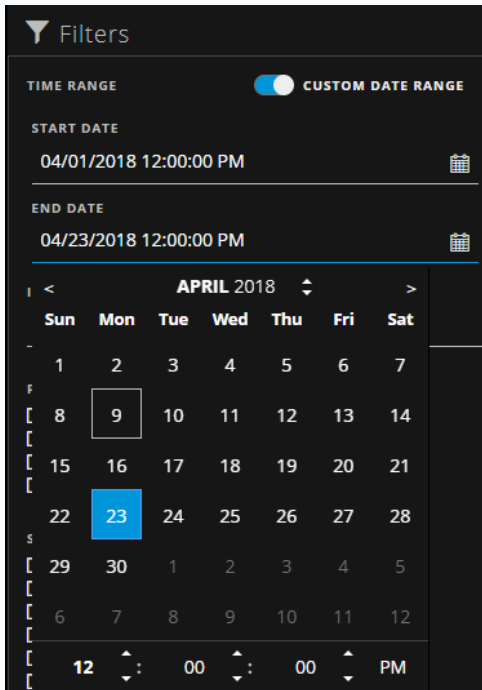
The following figure shows the filters available in the Filters panel.

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

- TIME RANGE**: A toggle switch for 'CUSTOM DATE RANGE'.
- INCIDENT ID**: A text input field with the placeholder 'e.g., INC-123'.
- PRIORITY**: Checkboxes for Low, Medium, High, and Critical.
- STATUS**: Checkboxes for New, Assigned, In Progress, Task Requested, Task Complete, Closed, and Closed - False Positive.
- ASSIGNEE**: A dropdown menu.
- CATEGORIES**: A dropdown menu.
- SENT TO ARCHER**: Checkboxes for Yes and No.
- Reset Filters**: A button at the bottom.

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 can see alerts that were received within the last 60 minutes.

Option	Description
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.
ASSIGNEE	<p>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.</p> <p>(Available in version 11.1 and later) To view only unassigned incidents, select Show only unassigned incidents.</p>
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.
SENT TO ARCHER	(In version 11.2 and later, if RSA Archer is configured as a data source in Context Hub, you can send incidents to Archer Cyber Incident & Breach Response and this option will be available in NetWitness Respond.) To view incidents that were sent to Archer, select Yes . For incidents that were not sent to Archer, select No .
Reset Filters	Removes your filter selections.


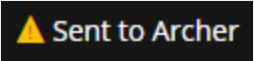
Overview Panel

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 screenshot shows a dark-themed user interface for an incident overview. At the top, the incident ID 'INC-14' is displayed with a close button. Below it, the rule name 'High Risk Alerts: Malware Analysis for 10.' is shown with an edit icon. A 'Send to Archer' button is present. The 'OVERVIEW' tab is selected. The main area lists incident details: 'Created: 03/21/2018 07:57:37 pm', 'Rule: High Risk Alerts: Malware Analysis', 'Risk Score: 90', 'Priority: Critical' (in a button), 'Status: New' (in a button), 'Assignee: (Unassigned)' (in a button), 'Sources: Malware Analysis', 'Categories:' (empty), and 'Catalysts: 1 Indicator(s), 1 Event(s)'.



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

Field	Description
<Incident ID>	Displays the Incident ID.

Field	Description
Send to Archer / Sent to Archer	<p>(In version 11.2 and later, if RSA Archer is configured as a data source in Context Hub, you can escalate incidents to Archer Cyber Incident & Breach Response and this option will be available in NetWitness Respond.) Shows whether the incident was sent to Archer Cyber Incident & Breach Response:</p> <ul style="list-style-type: none"> • Send to Archer: The incident was not sent to Archer. You can click the Send to Archer button to send the incident to Archer Cyber Incident & Breach Response for additional processing. This action is not reversible.  • Sent to Archer: The incident was sent to Archer Cyber Incident & Breach Response for additional analysis and action. 
<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 incidents that you would like to see in the Incidents 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

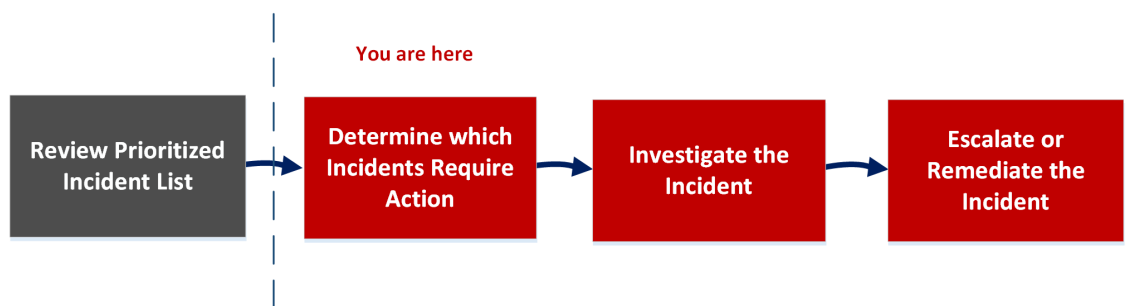
In the Incident Details view (RESPOND > Incidents > click an ID or NAME hyperlink in the Incidents List), you can view and access extensive incident details. The Incident Details view contains multiple panels that provide the following benefits:

- **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. You can also access Event Analysis details for some events and perform event reconnaissance.
- **Nodal Graph:** Visualize the size and interactions between entities (IP address, MAC address, user, host, domain, file name, or file hash).
- **Events List:** 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 Platform.



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 (Additional permissions required)	View Event Analysis for an event.*	View Event Analysis Details for Indicators
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
Incident Responders, Analysts	Reduce false positives by adding an entity to a whitelist.*	Add an Entity to a Whitelist
Incident Responders, Analysts	Pivot to NetWitness Investigate.*	Pivot to Investigate > Navigate
Incident Responders, Analysts	Pivot to NetWitness Endpoint.*	Pivot to NetWitness Endpoint Thick Client
Incident Responders, Analysts, and SOC Manager	Send an incident to Archer Cyber Incident & Breach Response.*	Send an Incident to RSA Archer

Role	I want to ...	Show me how
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 image displays three screenshots of the NetWitness Respond interface, illustrating the locations of the Incident Details view panels. Red arrows and numbers 1 through 7 point to specific UI elements across these panels.

Top Screenshot (Incident Overview):

- 1:** Points to the Incident Overview panel on the left, showing details for INC-212.
- 2:** Points to the Overview tab in the left sidebar.
- 3:** Points to the Nodal Graph in the center, showing a network diagram with nodes like 'Identified Hosts' and 'Wintel Security'.
- 4:** Points to the Events List tab in the top right, showing a list of events.
- 5:** Points to the Journal tab in the top right, showing a list of journal entries.
- 6:** Points to the Tasks tab in the top right, showing a list of tasks.
- 7:** Points to the Related Indicators tab in the top right, showing a list of related indicators.

Bottom-Left Screenshot (Event Details):

- 4:** Points to the Event Details panel, showing details for a specific event.

Bottom-Right Screenshot (Tasks and Related Indicators):

- 6:** Points to the Add New Task button in the Tasks panel.
- 7:** Points to the Find button in the Related Indicators panel.

The top screenshot displays the 'Event Analysis' window. It shows network event details for a specific packet, including session ID, source IP, destination IP, and service. The window is divided into sections for 'REQUEST' and 'RESPONSE' packets, showing hex and ASCII data. A red arrow points to the 'Event Analysis' tab, and another points to the 'Packet Analysis' dropdown.

The bottom screenshot displays the 'User Entity Behavior Analytics' window. It shows a user risk score of 220 and a list of alerts. A red arrow points to the 'User Entity Behavior Analytics' tab, and another points to the 'User Risk Score' section. The window also includes a bar chart for 'File Delete Events (Last 30 Days)' and a table of events.

- 1 Overview Panel (Click the OVERVIEW tab to view it.)
- 2 Indicators Panel
- 3 Nodal Graph
- 4 Events List (Click the top of 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.)
- 8 Event Analysis (Click an event type hyperlink in the Indicators panel to view the Event Analysis.)
- 9 UEBA (Click a User Entity Behavior Analytics hyperlink in the Indicators panel to view UEBA.)

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.

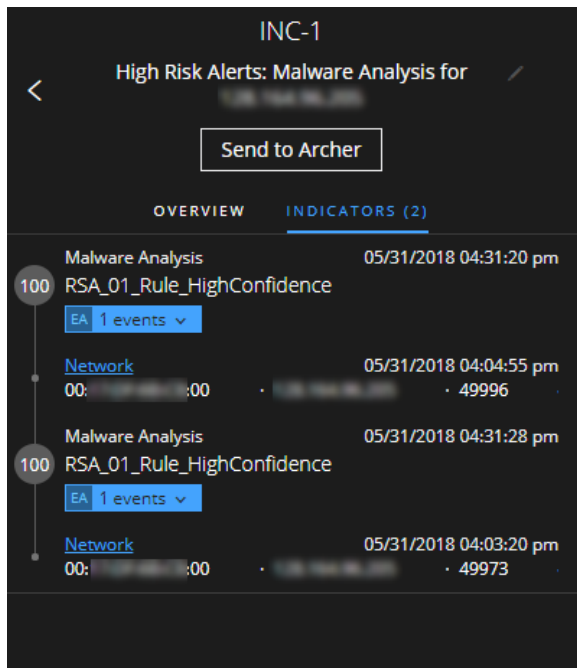
The screenshot shows the 'Overview Panel' for incident 'INC-1'. At the top, there is a back arrow, the incident name 'INC-1', and a title 'High Risk Alerts: Malware Analysis for'. Below the title is a 'Send to Archer' button. The panel has two tabs: 'OVERVIEW' (selected) and 'INDICATORS (2)'. The 'OVERVIEW' tab displays the following information:

Created:	05/31/2018 04:31:26 pm
Rule:	High Risk Alerts: Malware Analysis
Risk Score:	100
Priority:	<input type="button" value="Critical"/>
Status:	<input type="button" value="Task Requested"/>
Assignee:	<input type="button" value="(Unassigned)"/>
Sources:	Malware Analysis
Categories:	
Catalysts:	2 Indicator(s), 2 Event(s)

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. In the Indicators panel, you can drill deeper into the events associated with the listed indicators to get a better understanding of the events.

Note: The maximum number of indicators (alerts) displayed in the Indicators panel is 1,000.

Event Analysis

You can perform an Event Analysis from the Indicators panel. Events preceded by an **EA** (Event Analysis) have event reconnaissance information available: **EA 1 events**. You can select an event type hyperlink, such as **Network**, to access an event analysis for the selected event.

In the Event Analysis panel, you can view raw events and metadata with interactive features that enhance your ability to find meaningful patterns in the data. You can examine network, log, and endpoint events. The Event Analysis panel in the Respond view shows the Event Analysis view from Investigate for specific indicator events. For detailed information about the Event Analysis view, see the *NetWitness Investigate User Guide*.

Event Analysis

Network Event Details

Packet Analysis

Download PCAP

COMMON FILE PATTERNS

SHADE BYTES

DISPLAY PAYLOADS ONLY

NW SERVICE

PH - Concentrator

SESSION ID

220101

SOURCE IP:PORT

10. : 50941

DESTINATION IP:PORT

10. : 5671

SERVICE

443

FIRST PACKET TIME

09/14/2018 07:18:07 pm

LAST PACKET TIME

09/14/2018 07:18:07 pm

CALCULATED PACKET SIZE

4207 bytes

CALCULATED PAYLOAD SIZE

2349 bytes

CALCULATED PACKET COUNT

28

REQUEST

Packet 1

09/14/2018 07:18:07.560 pm

ID 14394694

SEQ 3615759429

PAYLOAD 0 Bytes

000000

00 50 56 33 19 d4 00 50 56 33 19 d7 08 00 45 00

000016

00 3c 44 4d 40 00 40 06 68 35 0a 04 3d 26 0a 04

000032

3d 0c c6 fd 16 27 d7 84 1c 45 00 00 00 a0 02

000048

72 10 0d 06 00 00 02 04 05 b4 04 02 08 0a 10 e9

000064

58 08 00 00 00 00 01 03 03 07

RESPONSE

Packet 2

09/14/2018 07:18:07.560 pm

ID 14394695

SEQ 1141126299

PAYLOAD 0 Bytes

000000

00 50 56 33 19 d7 00 50 56 33 19 d4 08 00 45 00

000016

00 3c 00 00 40 00 40 06 68 35 0a 04 3d 26 0a 04

000032

3d 26 16 27 c6 fd 44 04 34 9b d7 84 1c 46 a0 12

000048

71 20 8e 68 00 00 02 04 05 b4 04 02 08 0a 10 bf

000064

46 91 10 e9 58 08 01 03 03 07

REQUEST

Packet 3

09/14/2018 07:18:07.560 pm

ID 14394696

SEQ 3615759430

PAYLOAD 0 Bytes

000000

00 50 56 33 19 d4 00 50 56 33 19 d7 08 00 45 00

000016

00 34 44 4e 40 00 40 06 68 3c 0a 04 3d 26 0a 04

000032

3d 0c c6 fd 16 27 d7 84 1c 46 44 04 34 9c 80 10

000048

00 e5 dd cc 00 00 01 01 08 0a 10 e9 58 08 10 bf

000064

46 91

REQUEST

Packet 4

09/14/2018 07:18:07.561 pm

ID 14394697

SEQ 3615759430

PAYLOAD 118 Bytes

000000

00 50 56 33 19 d4 00 50 56 33 19 d7 08 00 45 00

000016

00 aa 44 4f 40 00 40 06 67 c5 0a 04 3d 26 0a 04

000032

3d 0c c6 fd 16 27 d7 84 1c 46 44 04 34 9c 80 18

000048

00 e5 32 e8 00 00 01 01 08 0a 10 e9 58 09 10 bf

EVENT META

SESSIONID

220101

TIME

09/14/2018 07:18:07 pm

SIZE

4207

PAYLOAD

2349

MEDIUM

1

ETH.SRC

00 : :07

ETH.ALL

00 : :07

ETH.DST

00 : :04

ETH.ALL

00 : :04

ETH.TYPE

2048

IP.SRC

10. :

IP.ALL

10. :

IP.DST

10. :

IP.ALL

10. :

IP.PROTO

6

TCP.FLAGS

31

TCP.SRCPORT

50941

PORT.ALL

50941

PORT.SRC.ALL

50941

TCP.DSTPORT

5671

PORT.ALL

5671

PORT.DST.ALL

5671

SERVICE

443

STREAMS

2

PACKETS

28

LIFETIME

0

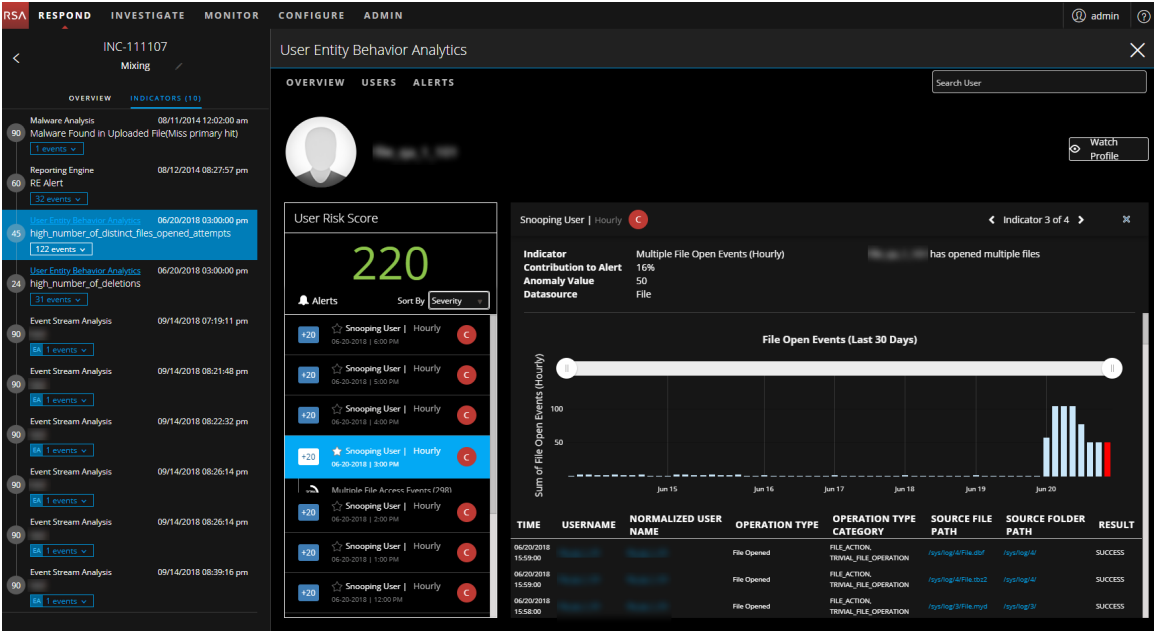
Note: Migrated incidents from NetWitness Platform versions before 11.2 will not show the Event Analysis panel in the Respond Incident Details view Indicators panel. Likewise, if you use alerts that were migrated from versions before 11.2 to create incidents in 11.3, you will also not be able to view the Event Analysis panel in the Respond view for those incidents.

135

NetWitness Respond Reference Information

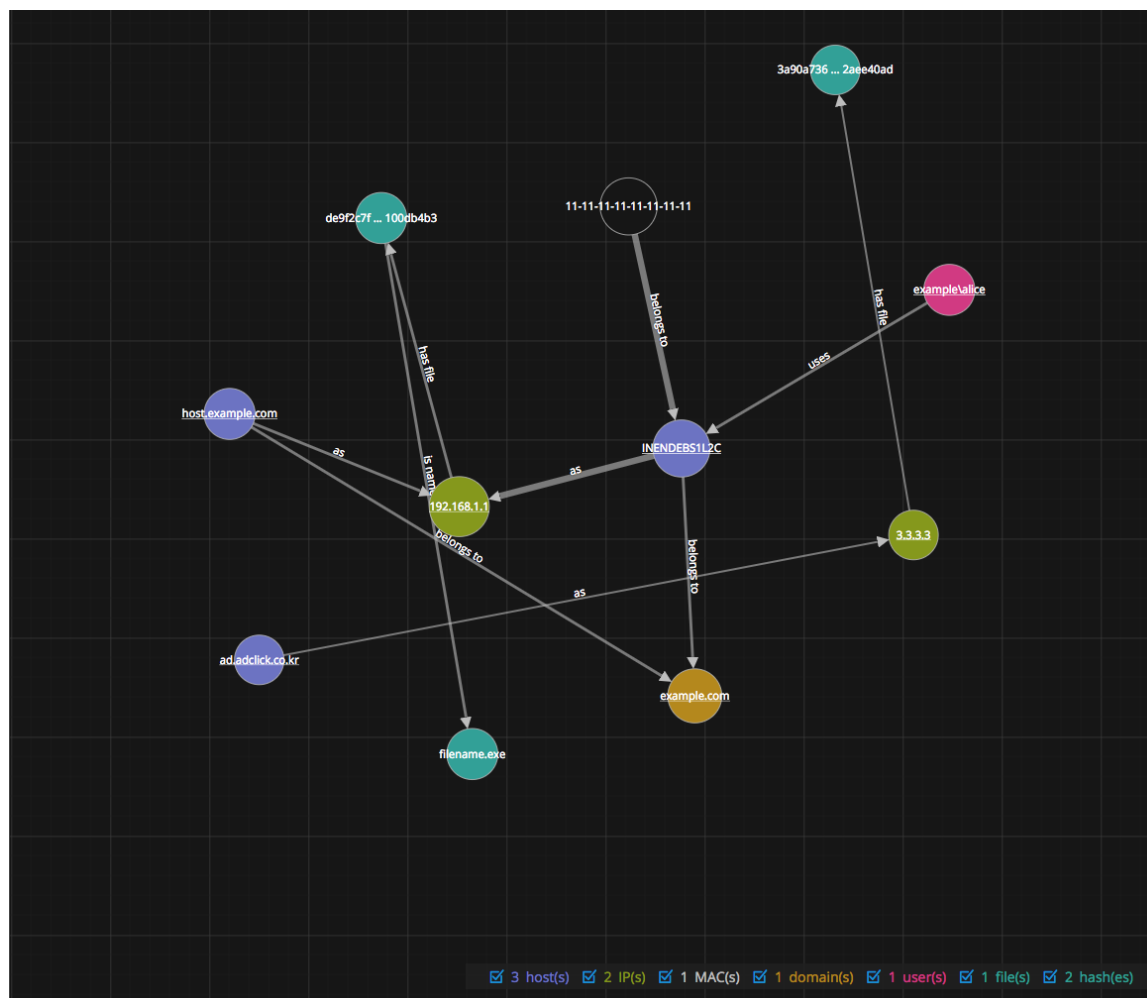
User Entity Behavior Analytics

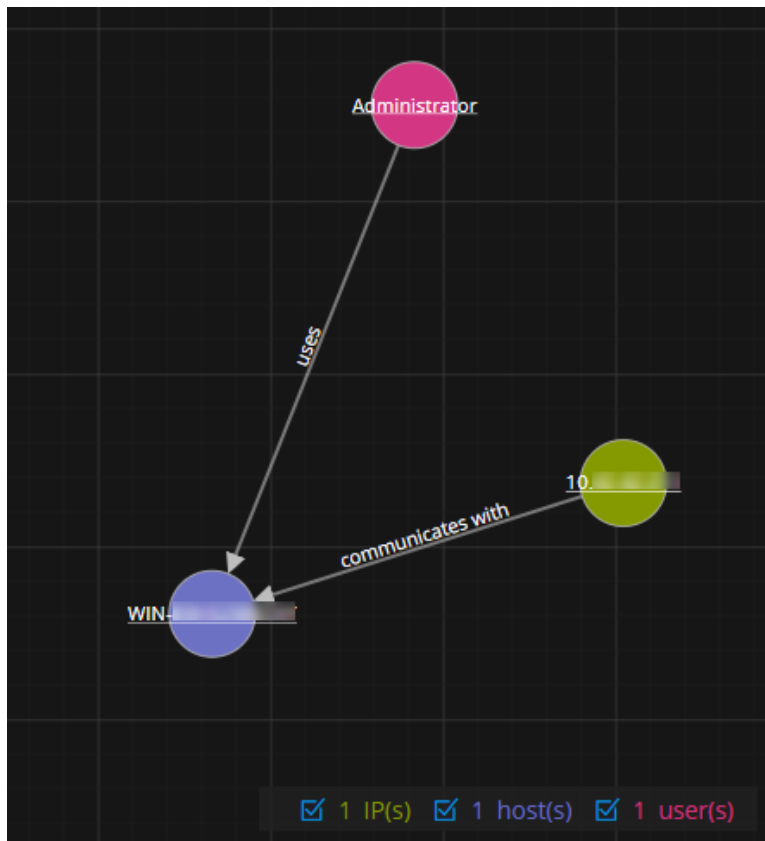
RSA NetWitness UEBA (User and Entity Behavior Analytics) is an advanced analytics solution for discovering, investigating, and monitoring risky behaviors across all users and entities in your network environment. You can access UEBA from the Respond Incident Details view Indicators panel. Indicators with a **User Entity Behavior Analytics** hyperlink have additional UEBA information available. For detailed information about UEBA, see the *NetWitness UEBA User Guide*.



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

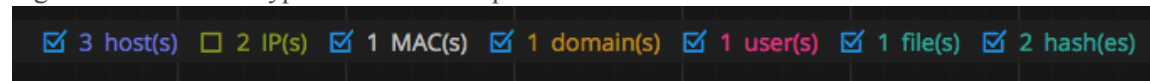
In the nodal graph, circles represent nodes. The following table describes the nodal graph node types.

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.
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.

In NetWitness Platform version 11.2 and later, you can select the node types that you want to view by clearing or selecting the checkboxes in the legend. The following figure shows an example nodal graph legend with all node types selected except IP.



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.
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 List

The Events List 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, target user, and file information about the events. The amount of information listed depends on the event type. The maximum number of events displayed in the Events List is 1,000.

The following figure shows an Events List for network events.

53 events

Nodal Graph Events List

90	test (Event 1 of 1)	EVENT TIME 11/01/2018 05:07:08.000 pm	EVENT TYPE Network	DETECTOR IP N/A	FILE NAME N/A	FILE HASH N/A
		IP	PORT	HOST		MAC
SOURCE	10.10.10.09	51304		N/A		00:50:50:12:61
TARGET	10.10.10.12	5671		N/A		00:50:50:12:63

90	test (Event 1 of 1)	EVENT TIME 11/01/2018 05:07:10.000 pm	EVENT TYPE Network	DETECTOR IP N/A	FILE NAME N/A	FILE HASH N/A
		IP	PORT	HOST		MAC
SOURCE	10.10.10.09	46292		N/A		00:50:50:12:61
TARGET	10.10.10.12	5671		N/A		00:50:50:12:63

90	test (Event 1 of 1)	EVENT TIME 11/01/2018 05:08:08.000 pm	EVENT TYPE Network	DETECTOR IP N/A	FILE NAME N/A	FILE HASH N/A
		IP	PORT	HOST		MAC
SOURCE	10.10.10.09	57522		N/A		00:50:50:12:61
TARGET	10.10.10.12	5671		N/A		00:50:50:12:63

90	test (Event 1 of 1)	EVENT TIME 11/01/2018 05:08:38.000 pm	EVENT TYPE Network	DETECTOR IP N/A	FILE NAME N/A	FILE HASH N/A
		IP	PORT	HOST		MAC
SOURCE	10.10.10.09	53820		N/A		00:50:50:12:61
TARGET	10.10.10.12	5671		N/A		00:50:50:12:63

90	test (Event 1 of 1)	EVENT TIME 11/01/2018 05:10:10.000 pm	EVENT TYPE Network	DETECTOR IP N/A	FILE NAME N/A	FILE HASH N/A
		IP	PORT	HOST		MAC
SOURCE	10.10.10.09	55902		N/A		00:50:50:12:61
TARGET	10.10.10.12	5671		N/A		00:50:50:12:63

Each event has a header row with the following information:

- **Risk score:** This is the risk score of the indicator (alert) that contains the event.
- **Title:** This is the name of the event.
- **Event x of x:** This indicates the number of the event out of the total number of events in the indicator.

For example, the following event header shows that this event is event 2 of 2 for an indicator (alert) that has a risk score of 90. The event name is **In Program Data Followed by SSL Over Non Standard Port**.

90	In Program Data Followed by SSL Over Non Standard Port (Event 2 of 2)
----	---

The following table describes the fields in the Events List for network or log events.

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

The following figure shows an Events List for NetWitness Endpoint events.

5 events

90 Enables Login Bypass (Event 1 of 1)

EVENT TIME	EVENT TYPE	CATEGORY	ACTION	HOSTNAME	USER ACCOUNT	OPERATING SYSTEM	FILE HASH
11/01/2018 06:27:20.000 pm	Endpoint	Process Event	createProcess	WIN7ENTX64	N/A	windows	N/A
	FILE NAME	LAUNCH ARGUMENT		PATH			HASH
SOURCE	dtf.exe	dtf.exe -dll:oci.dll -Log:endpoint.log -xml:summary:endpoint.xml -testcase		C:\Users\user\Desktop\amd64\			7a08ef8f741e4130fd441280392799780575803669 69fe4557cd3383651d6bf7
TARGET	REG.exe	REG.exe ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe" /f		C:\Windows\system32\			4e66b857b7010db8d44e4e28d73eb81a99bd69153 50bb9a63cd86671051b22f0e

90 Enables Login Bypass (Event 1 of 1)

EVENT TIME	EVENT TYPE	CATEGORY	ACTION	HOSTNAME	USER ACCOUNT	OPERATING SYSTEM	FILE HASH
11/01/2018 06:27:20.000 pm	Endpoint	Process Event	createProcess	WIN7ENTX64	N/A	windows	N/A
	FILE NAME	LAUNCH ARGUMENT		PATH			HASH
SOURCE	dtf.exe	dtf.exe -dll:oci.dll -Log:endpoint.log -xml:summary:endpoint.xml -testcase		C:\Users\user\Desktop\amd64\			7a08ef8f741e4130fd441280392799780575803669 69fe4557cd3383651d6bf7
TARGET	REG.exe	REG.exe ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe" /f		C:\Windows\system32\			4e66b857b7010db8d44e4e28d73eb81a99bd69153 50bb9a63cd86671051b22f0e

70 Runs From Recycle Bin Directory (Event 1 of 1)

EVENT TIME	EVENT TYPE	CATEGORY	ACTION	HOSTNAME	USER ACCOUNT	OPERATING SYSTEM	FILE HASH
11/01/2018 06:27:20.000 pm	Endpoint	Process Event	createProcess	WIN7ENTX64	N/A	windows	N/A
	FILE NAME	LAUNCH ARGUMENT		PATH			HASH
SOURCE	RecyBinModule.exe	RecyBinModule.exe -dll:C:\Users\user\Desktop\amd64\oci.dll -log:C:\Users\user\Desktop\amd64\pra.log -testcase:30		C:\\$Recycle.Bin\142639821\			7a08ef8f741e4130fd441280392799780575803669 69fe4557cd3383651d6bf7
TARGET	cmd.exe	cmd.exe /C sc stop dtfsvc && sc delete dtfsvc		C:\Windows\System32\			8651e663d5effb9022046ab46452a102d1f31f5edb 90ac87d8db023fe54b92f0

70 Runs From System Volume Information Directory (Event 1 of 1)

EVENT TIME	EVENT TYPE	CATEGORY	ACTION	HOSTNAME	USER ACCOUNT	OPERATING SYSTEM	FILE HASH
11/01/2018 06:27:20.000 pm	Endpoint	Process Event	createProcess	WIN7ENTX64	N/A	windows	N/A
	FILE NAME	LAUNCH ARGUMENT		PATH			HASH
SOURCE	SysVoluPath.exe	SysVoluPath.exe -dll:C:\Users\user\Desktop\amd64\oci.dll -log:C:\Users\user\Desktop\amd64\pra.log		C:\System Volume Information\142652925\			7a08ef8f741e4130fd441280392799780575803669 69fe4557cd3383651d6bf7

The following table describes the fields in the Events List for NetWitness Endpoint events. NetWitness Endpoint events have an Endpoint Event Type and an nwendpoint Device Type. NetWitness Endpoint events from version 4.4.x and earlier can have an Event Type that shows the origin of the event.

Field	Description
EVENT TIME	Shows the time the event occurred.
EVENT TYPE	Shows the type of alert, such as Endpoint or Log. NetWitness Endpoint events have an Endpoint event type. NetWitness Endpoint events from version 4.4.x and earlier can have an Event Type that shows the origin of the event.
CATEGORY	Shows the NetWitness Endpoint category.
ACTION	Shows the action that the file performed.
HOSTNAME	Shows the name of the machine that is running the agent.
USER ACCOUNT	Shows the username of the actively logged in user.
OPERATING SYSTEM	Shows the operating system of the agent.
FILE HASH	Shows the checksum of the file.

Field	Description
SOURCE FILENAME	Shows the name of the source file.
SOURCE LAUNCH ARGUMENT	Shows the command line argument for the running process.
SOURCE PATH	Shows the path of the source file.
SOURCE HASH	Shows the checksum of the source file.
SOURCE IP ADDRESS	Shows the IP address of the agent.
SOURCE PORT	Shows the source port of the connection.
TARGET FILENAME	Shows the name of the target file.
TARGET LAUNCH ARGUMENT	Shows the command line argument for the running process.
TARGET PATH	Shows the path of the target file.
TARGET HASH	Shows the checksum of the target file.
TARGET IP ADDRESS	Shows the destination IP address of this NetWitness Platform activity.
TARGET PORT	Shows the destination port of the connection.
EVENT SOURCE	Shows the hostname or IP address along with the port of the of the Core service that holds the event information.
DEVICE TYPE	Shows the type of the device from which the data is sent or collected. For example, it shows <code>nwendpoint</code> for NetWitness Endpoint.

Event Details

To view the event details, you can click the top of an event in the Events List. The details appear below the event. Viewing inline event details enables you to keep the context of the event as it relates to the other events.

The following figure shows an indicator (alert) selected in the Indicators panel. The events for that indicator appear in the Events List on the right. You can see the event details below the selected event.

The screenshot shows the NetWitness Respond interface. On the left, the 'INDICATORS (5)' panel lists several 'Nonstandard FTP Traffic' events. The main panel on the right displays the details for a selected event, 'Nonstandard FTP Traffic' (Event 1 of 2).

EVENT TIME	EVENT TYPE	DETECTOR IP	FILE NAME	FILE HASH
09/27/2018 02:49:19.000 pm	Network	N/A	N/A	N/A

SOURCE	TARGET	EVENT SOURCE
DEVICE PORT 20 MAC ADDRESS 00:0C:29:29:D3:AB IP ADDRESS 10.10.10.63 GEOLOCATION COUNTRY Morocco LATITUDE 32 ORGANIZATION Telecom LONGITUDE -52 USER N/A	DEVICE PORT 49419 MAC ADDRESS 00:0C:29:29:3E:D2 IP ADDRESS 192.168.60.65 GEOLOCATION N/A USER N/A DETECTOR N/A SIZE 24144 DATA SIZE 24144	10.10.10.38:56003 ANALYSIS SERVICE ftp over non-standard port EVENT SOURCE ID 4730249 ANALYSIS SESSION ratio low transmitted,inbound traffic,session size 10-50k SITE CATEGORIZATION nonstandard

RELATED LINKS
[Investigate Original Event](#)

The following figure shows a specific indicator event selected in the Indicators panel. Information about the selected event appears in the Events List on the right. You can see the event details below the selected event in the list.

The screenshot shows the NetWitness Respond interface. On the left, the 'INDICATORS (5)' panel lists several 'Nonstandard FTP Traffic' events. The main panel on the right displays the details for a selected event, 'Nonstandard FTP Traffic' (Event 2 of 2).

EVENT TIME	EVENT TYPE	DETECTOR IP	FILE NAME	FILE HASH
09/27/2018 02:49:21.000 pm	Network	N/A	N/A	N/A

SOURCE	TARGET	EVENT SOURCE
DEVICE PORT 20 MAC ADDRESS 00:0C:29:29:D3:AB IP ADDRESS 10.10.10.63 GEOLOCATION COUNTRY Morocco LATITUDE 32 ORGANIZATION Telecom LONGITUDE -52 USER N/A	DEVICE PORT 49420 MAC ADDRESS 00:0C:29:29:3E:D2 IP ADDRESS 192.168.60.65 GEOLOCATION N/A USER N/A DETECTOR N/A SIZE 7544 DATA SIZE 7544	10.10.10.38:56003 ANALYSIS SERVICE ftp over non-standard port EVENT SOURCE ID 4730250 ANALYSIS SESSION ratio low transmitted,inbound traffic,session size 5-10k SITE CATEGORIZATION nonstandard

RELATED LINKS
[Investigate Original Event](#)

Journal Panel

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

The screenshot displays the 'JOURNAL (4)' tab of the NetWitness Respond interface. It shows a list of four journal entries, each with a timestamp, user (ADMIN), and a 'MILESTONE' dropdown menu set to 'None'. The entries describe research progress and task assignments. Below the list is a 'New Journal Entry' section with a text area containing 'Pierre may be available...', a 'MILESTONE' dropdown set to 'None', and a 'Submit' button.

ADMIN	Timestamp	MILESTONE	Description
ADMIN	01/07/2019 10:25:19 pm	None	Started researching the incident. This is similar to one I had yesterday.
ADMIN	01/07/2019 10:25:35 pm	None	I think this IP is malicious.
ADMIN	01/07/2019 10:26:15 pm	None	I created a task for Ian. I think he does remediations, too.
ADMIN	01/07/2019 10:26:43 pm	None	Ian is booked solid. We may need to assign it to someone else. We will let you know.

New Journal Entry

Pierre may be available...

MILESTONE None

Submit

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.

Field	Description
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 screenshot shows the 'TASKS (2)' tab in the NetWitness Respond interface. At the top, there are tabs for 'JOURNAL (3)', 'TASKS (2)', and 'RELATED', with a close button 'X'. Below the tabs is a button labeled 'Add New Task'. The main area displays two task cards for incident 'INC-212'.

Task 1: REM-2 / INC-212

- CREATED:** 01/08/2019 12:41 am
- LAST UPDATED:** 01/08/2019 12:41 am
- OPENED:** 14 hours ago
- NAME:** Create replacement host ASAP
- ASSIGNEE:** IT Services
- PRIORITY:** High (dropdown menu)
- STATUS:** New (dropdown menu)
- DESCRIPTION:** There is no description for this task

Task 2: REM-1 / INC-212

- CREATED:** 01/08/2019 12:40 am
- LAST UPDATED:** 01/08/2019 12:40 am
- OPENED:** 14 hours ago
- NAME:** Isolate Host
- ASSIGNEE:** DScience
- PRIORITY:** High (dropdown menu)
- STATUS:** New (dropdown menu)
- DESCRIPTION:** Get the host off of the network and examine it.

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.

Field	Description
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.
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 Platform 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.

Related Indicators

Enter a value below and click the Find button to look for other indicators related to that value.

Find:

Value:

When:

Indicators for: IP: 10.10.10.98

All Data

Event Stream Analysis	11/01/2018 04:22:54 pm	SAMPLE - Whitelist - From outside of Germany, P...	1 event	Open in new window	<input type="button" value="Add To Incident"/>
Event Stream Analysis	11/01/2018 04:22:54 pm	SAMPLE - P2P Software as Detected by an Intrusi...	1 event	Open in new window	<input type="button" value="Add To Incident"/>
Event Stream Analysis	11/01/2018 04:22:54 pm	SAMPLE - Whitelist - From outside of Germany, P...	1 event	Open in new window	<input type="button" value="Add To Incident"/>
Event Stream Analysis	11/01/2018 04:22:54 pm	SAMPLE - Whitelist - From outside of Germany, P...	1 event	Open in new window	<input type="button" value="Part Of This Incident"/>
Event Stream Analysis	11/01/2018 04:22:54 pm	SAMPLE - Whitelist - From outside of Germany, P...			

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.



Field	Description
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.
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.
 Nodal Graph	Enables you to view the Nodal Graph.
 Events List	Enables you to view the incident Events List. Clicking the top of an event enables you to view the event details below it.

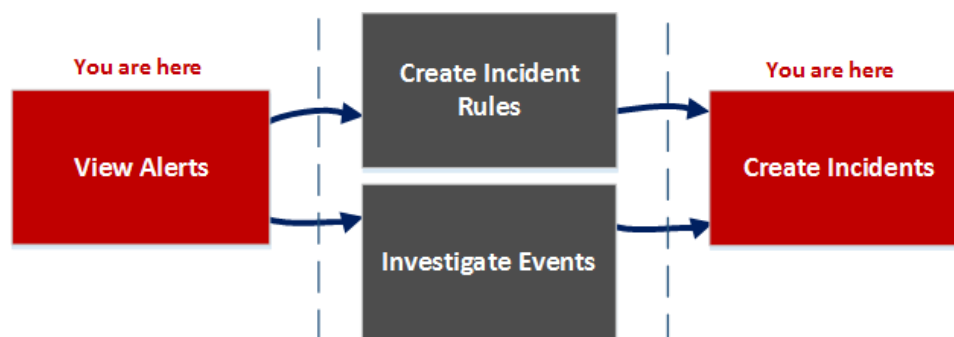
Option	Description
 (Journal, Tasks, and Related)	Enables you to view the Journal, Tasks, and Related Indicators panels.
	Enables you to show or hide the Header, Request, Response, or Meta in the Event Analysis panel in the Respond Incident Details view. For more information about Event Analysis, see the Event Analysis view in the <i>NetWitness Investigate User Guide</i> .

Alerts List View

The Alerts List view (RESPOND > Alerts) enables you to view all of the threat alerts and indicators received by NetWitness Platform 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 Platform. 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 Platform 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 Platform.*	View Alerts
Incident Responders, Analysts	Filter alerts.*	Filter the Alerts List
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

Role	I want to ...	Show me how
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](#)

Quick Look

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 Platform. 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 Platform. You can filter this list to only show alerts of interest.

RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN							
Incidents Alerts Tasks							
Create Incident Add to Incident Delete							
CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID	
22/01/2019 04:53:13 pm	10	IPOC 3	Endpoint	1	it_laptop4.eng.matrix.com to host.example.com	INC-739	
18/01/2019 05:01:45 pm	90	Login Bypass Configured	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	90	Unsigned Reserved Name	Endpoint	1	-nwendpoint	INC-740	
18/01/2019 05:01:45 pm	90	Unsigned Reserved Name	Endpoint	1	-nwendpoint	INC-740	
18/01/2019 05:01:45 pm	70	Burns From System Volume Information Directory	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Burns Binary Located In System Volume Information Directory	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	90	Burns From Root Of Program Directory	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Burns From System Volume Information Directory	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Burns Binary Located In Recycle Bin Directory	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Burns From Recycle Bin Directory	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	90	Possible Login Bypass	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Burns Binary Located In Recycle Bin Directory	Endpoint	1	-nwendpoint	INC-738	
18/01/2019 05:01:45 pm	70	Burns From Recycle Bin Directory	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	90	Enables Login Bypass	Endpoint	1	-nwendpoint		
18/01/2019 05:01:45 pm	70	Configures Image Hijacking	Endpoint	1	-nwendpoint		


Showing 1000 out of 2069 items | 1 selected

The following Alerts List view is filtered for Risk Scoring Alerts.

RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN							
Incidents Alerts Tasks							
Create Incident Add to Incident Delete							
CREATED	SEVERITY	NAME	SOURCE	# EVENTS	HOST SUMMARY	INCIDENT ID	
18/01/2019 04:49:00 pm	90	Threshold Breached for HOST_WINZENTX64	Risk Scoring	92	-nwendpoint	INC-737	
18/01/2019 04:49:00 pm	90	Threshold Breached for FILE_dbl.exe	Risk Scoring	82	-nwendpoint	INC-736	
18/01/2019 04:49:00 pm	90	Threshold Breached for FILE_POWERSHELLEXE	Risk Scoring	4	-nwendpoint	INC-735	
18/01/2019 04:49:00 pm	90	Threshold Breached for FILE_CMD.exe	Risk Scoring	4	-nwendpoint	INC-734	

Showing 4 out of 4 items | 1 selected

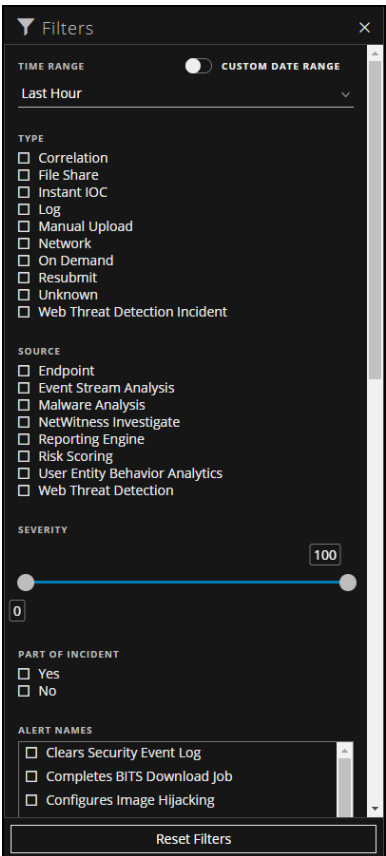
The following table describes the columns in the Alerts List.

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	<p>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, Risk Scoring, and many others.</p> <div> <p>Note: In NetWitness Platform 11.3 and later, the Endpoint source includes Endpoint alerts from all NetWitness Endpoint versions. If one of the events in an alert has a <code>device_type</code> of <code>nwendpoint</code>, the source changes to Endpoint.</p> </div>
# 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.
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 4 out of 4 items | 1 selected**

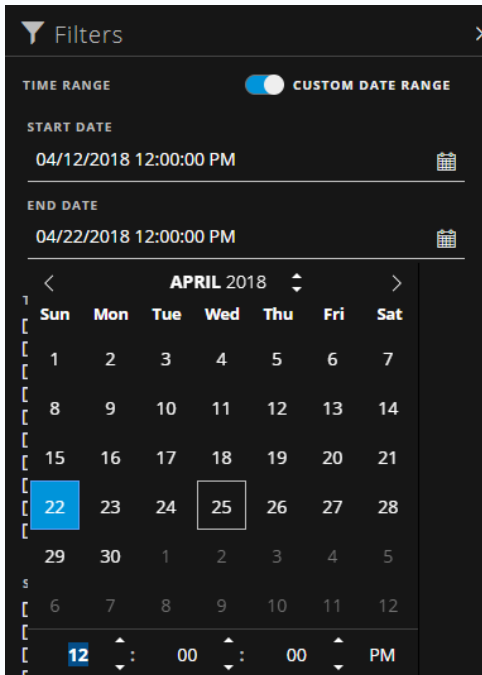
Filters Panel

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.

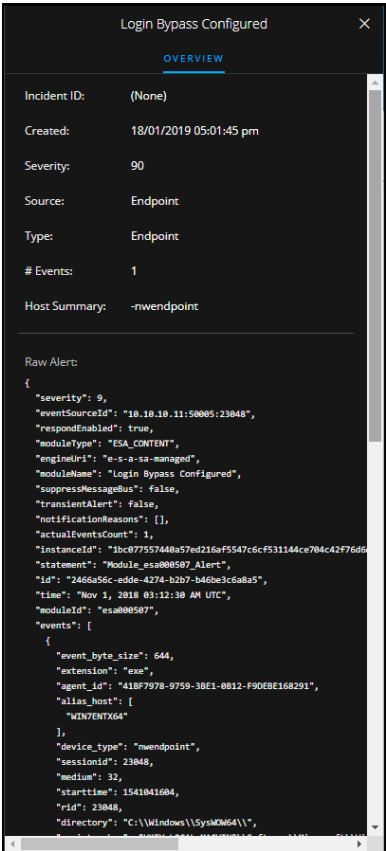
Option	Description
TIME RANGE	You can select a specific time period from the Time Range drop-down list. The time range is based on the received date of the alerts. For example, if you select Last Hour, you can see alerts that were received within the last 60 minutes.

Option	Description
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	<p>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, Risk Scoring, and many others.</p> <p>Note: In NetWitness Platform 11.3 and later, the Endpoint source includes Endpoint alerts from all NetWitness Endpoint versions. If one of the events in an alert has a device_type of <code>nwendpoint</code>, the source changes to Endpoint.</p>
SEVERITY	Displays the level of severity of the alert. The values are from 1 through 100.
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 4 out of 4 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.
Severity	Displays the level of severity of the alert. The values are from 1 through 100.

Field	Description
Source	<p>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, Risk Scoring, and many others.</p> <p>Note: In NetWitness Platform 11.3 and later, the Endpoint source includes Endpoint alerts from all NetWitness Endpoint versions. If one of the events in an alert has a device_type of <code>nwendpoint</code>, the source changes to Endpoint.</p>
Type	<p>Indicates the type of events in the alert, for example, logs, network sessions, and so on. There can be multiple types listed.</p> <p>Note: In NetWitness Platform 11.3 and later, the Endpoint source includes Endpoint alerts from all NetWitness Endpoint versions. If one of the events in an alert has a device_type of <code>nwendpoint</code>, the source changes to Endpoint.</p>
# 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.

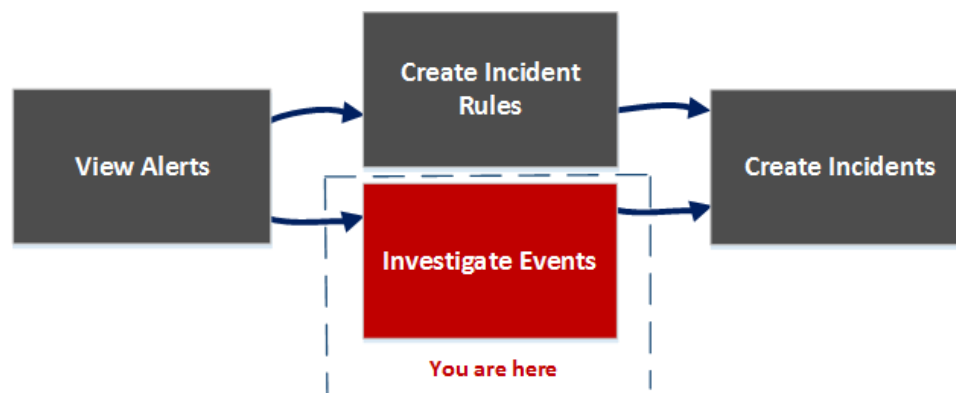
Option	Description
	Enables you to open the Filters panel so that you can specify the alerts that you would like to see in the Alerts List.
	Closes the panel.
Create Incident button	Enables you to create incidents from alerts. The alerts cannot be part of an incident. To get a list of alerts without 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 Platform 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 Platform.	View 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	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

Role	I want to ...	Show me how
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](#)

Quick Look

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.

RE bad rule

OVERVIEW

Incident ID: [INC-91233](#)

Created: 04/04/2018 06:27:37 pm

Severity: 50

Source: Reporting Engine

Type: Network

Events: 9

Host Summary: 9 hosts to 2 hosts

Raw Alert:

```
{
  "severity": 5,
  "signature_id": "RULE_68_20180403163411",
  "risk_score": 1,
  "name": "RE bad rule",
  "source": "RSA - Reporting Engine",
  "datasource_port": "56005",
  "datasource_host": "10.4.61.44",
  "events": [
    {
      "ip_proto": "6",
      "lifetime": "8",
      "ip_src": "10.4.61.17",
      "medium": "1",
      "sessionid": "281739",
      "rid": "186629",
      "inv_context": "event analysis, protocol analysis",
      "packets": "28",
      "feed_name": "Investigation",
      "threat_category": "nonstandard",
      "eth_src": "08:50:56:33:10:60",
      "analysis_service": "ssl over non-standard port",
      "payload": "23137",
      "tcp_flags": "31",
      "alert_id": "no06075",
      "risk_info": "ssl over non-standard port",
      "direction": "lateral",
      "top_offset": "0801",
      "top_offset": "5325",
      "streams": "2",
      "ip_dst": "10.4.61.32",
      "inv_category": "operations"
    }
  ]
}
```

TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DEST
04/04/2018 06:25:35.000 pm	Network	10.4.61.17	53529		00:50:56:33:10:60		10.4.61.32	5671
04/04/2018 06:25:35.000 pm	Network	10.4.61.17	42388		00:50:56:33:10:60		10.4.61.32	5671
04/04/2018 06:25:36.000 pm	Network	10.4.61.17	38494		00:50:56:33:10:60		10.4.61.32	5671
04/04/2018 06:25:36.000 pm	Network	10.4.61.17	41763		00:50:56:33:10:60		10.4.61.32	5671
04/04/2018 06:25:44.000 pm	Network	10.4.61.32	123		00:50:56:33:10:6E		10.4.61.17	123
04/04/2018 06:26:05.000 pm	Network	10.4.61.17	40944		00:50:56:33:10:60		10.4.61.32	5671
04/04/2018 06:26:05.000 pm	Network	10.4.61.17	46346		00:50:56:33:10:60		10.4.61.32	5671
04/04/2018 06:26:06.000 pm	Network	10.4.61.17	48759		00:50:56:33:10:60		10.4.61.32	5671
04/04/2018 06:26:06.000 pm	Network	10.4.61.17	44657		00:50:56:33:10:60		10.4.61.32	5671

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.

RE bad rule

OVERVIEW

Incident ID: [INC-91233](#)

Created: 04/04/2018 06:27:37 pm

Severity: 50

Source: Reporting Engine

Type: Network

Events: 9

Host Summary: 9 hosts to 2 hosts

Raw Alert:

```
{
  "severity": 5,
  "signature_id": "RULE_68_20180403163411",
  "risk_score": 1,
  "name": "RE bad rule",
  "source": "RSA - Reporting Engine",
  "datasource_port": "56005",
  "datasource_host": "10.4.61.44",
  "events": [
    {
      "ip_proto": "6",
      "lifetime": "8",
      "ip_src": "10.4.61.17",
      "medium": "1",
      "sessionid": "281739",
      "rid": "186629",
      "inv_context": "event analysis, protocol analysis",
      "packets": "28",
      "feed_name": "Investigation",
      "threat_category": "nonstandard",
      "eth_src": "08:50:56:33:10:60",
      "analysis_service": "ssl over non-standard port",
      "payload": "23137",
      "tcp_flags": "31",
      "alert_id": "no06075",
      "risk_info": "ssl over non-standard port",
      "direction": "lateral",
      "top_offset": "0801",
      "top_offset": "5325",
      "streams": "2",
      "ip_dst": "10.4.61.32",
      "inv_category": "operations"
    }
  ]
}
```

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.

9 events										
TIME	TYPE	SOURCE IP	SOURCE PORT	SOURCE HOST	SOURCE MAC	SOURCE USER	DESTINATION IP	DESTINATION PORT	DESTINATION HOST	DESTINATION MAC
04/04/2018 06:25:35.000 pm	Network	10.4.61.17	53529		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:25:35.000 pm	Network	10.4.61.17	42388		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:25:36.000 pm	Network	10.4.61.17	38494		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:25:36.000 pm	Network	10.4.61.17	41763		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:25:44.000 pm	Network	10.4.61.32	123		00:50:56:33:10:6E		10.4.61.17	123		00:50:56:33:10:6D
04/04/2018 06:26:05.000 pm	Network	10.4.61.17	40944		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:26:05.000 pm	Network	10.4.61.17	46346		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:26:06.000 pm	Network	10.4.61.17	48759		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E
04/04/2018 06:26:06.000 pm	Network	10.4.61.17	44657		00:50:56:33:10:6D		10.4.61.32	5671		00:50:56:33:10:6E

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 Details

08/15/2018 06:55:45 pm

Back To Table

< 1 of 11 >

Timestamp	08/15/2018 06:55:45.000 pm (9 minutes ago)		
Type	Network		
Source	Device	Port	41158
		MAC Address	00:50:.....C1
		IP Address	10.
		Geolocation	
	User		
Destination	Device	Port	5671
		MAC Address	00:50:.....BF
		IP Address	10.
		Geolocation	
	User		
Detector			
Size	4191		
Data	Size	4191	
Event Source	10.:56003		
Event Source ID	241348		
Related Links	Investigate Original Event		

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.
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 investigate_original_event.
	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 device.
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.
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?

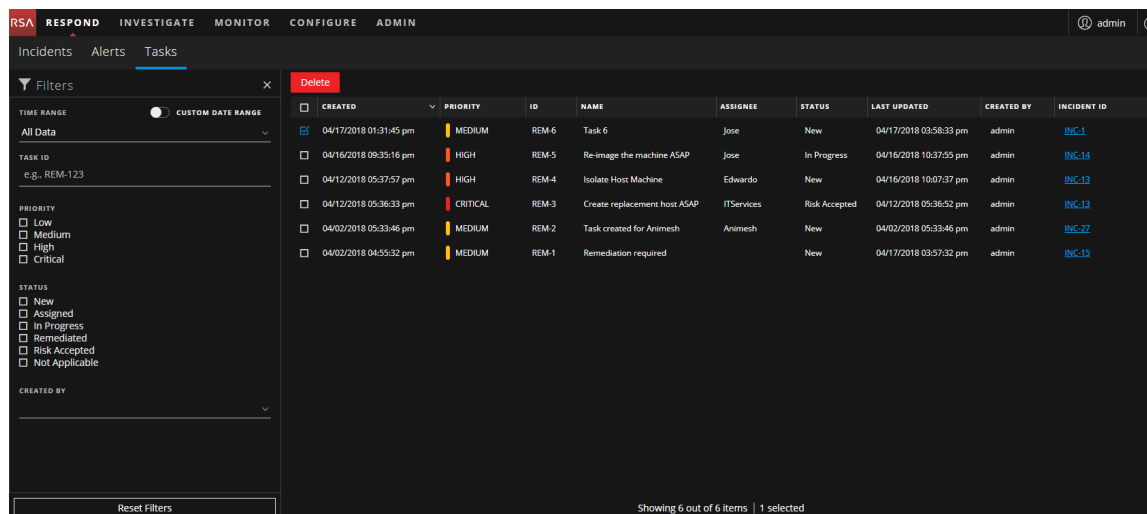
Role	I want to ...	Show me how
Incident Responders, Analysts	View tasks	View All Incident Tasks and View the Tasks associated with an Incident
Incident Responders, Analysts	Filter tasks.	Filter the Tasks List
Incident Responders, Analysts	Create a task.	Create a Task
Incident Responders, Analysts	Find 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

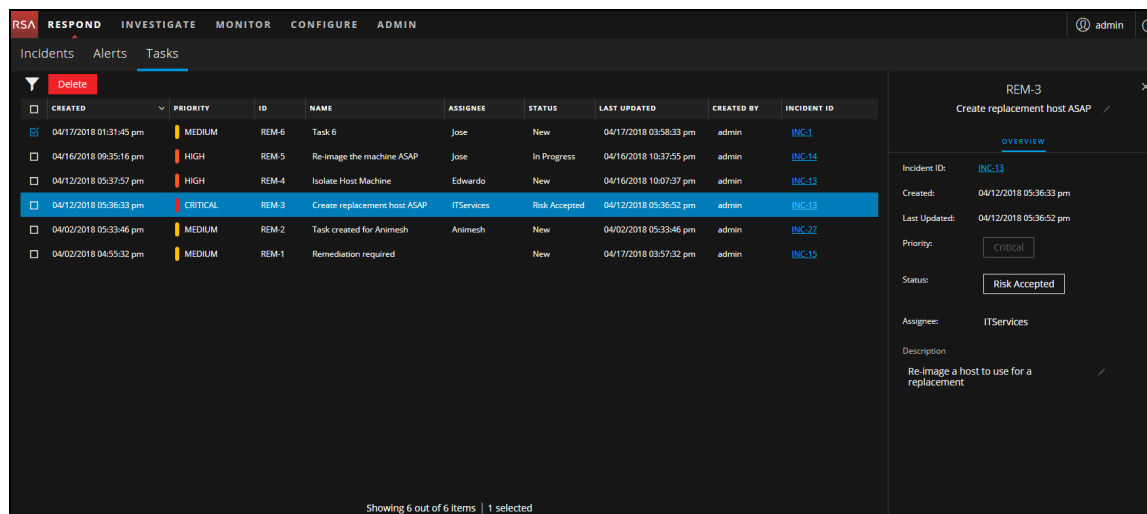
- [Incident Details View](#)
- [Escalate or Remediate the Incident](#)

Quick Look

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




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.



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.

Column	Description
PRIORITY	<p>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:</p> 
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.
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

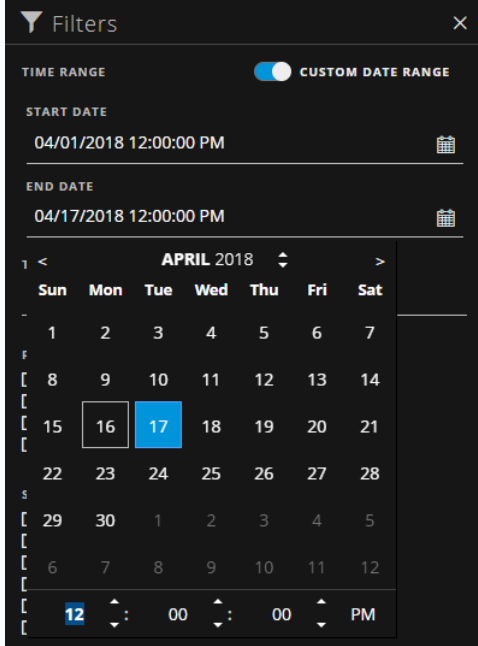
The following figure shows the filters available in the Filters panel.

The screenshot shows a 'Filters' panel with a close button (X) in the top right. It contains the following sections:

- TIME RANGE**: A toggle switch is currently set to 'CUSTOM DATE RANGE'. Below it is a dropdown menu showing 'All Data'.
- TASK ID**: A text input field with the placeholder text 'e.g., REM-123'.
- PRIORITY**: Four checkboxes labeled 'Low', 'Medium', 'High', and 'Critical'.
- STATUS**: Six checkboxes labeled 'New', 'Assigned', 'In Progress', 'Remediated', 'Risk Accepted', and 'Not Applicable'.
- CREATED BY**: A dropdown menu.
- Reset Filters**: A button at the bottom of the 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 can see tasks that were created within the last 60 minutes.

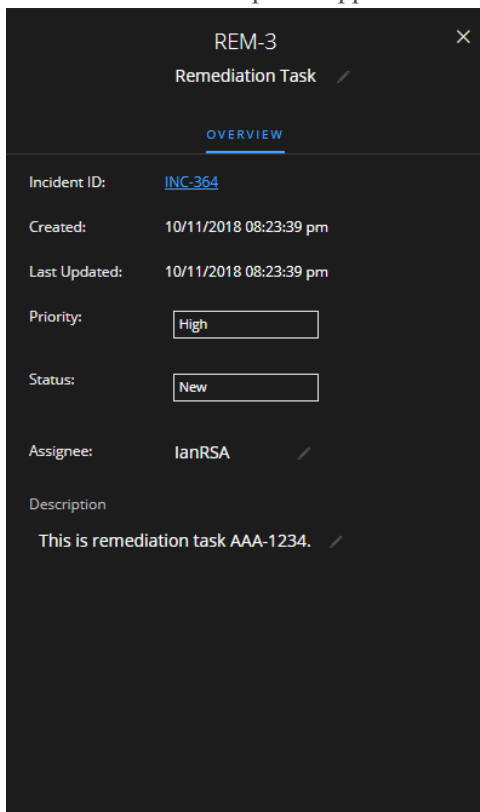
Option	Description
CUSTOM DATE RANGE	<p>You can specify a specific date range instead of selecting a Time Range option. To do this, click the white circle in front of Custom Date Range to view the Start Date and End Date fields. Select the dates and times from the calendar.</p> 
TASK ID	You can type 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>
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.



REM-3

Remediation Task

OVERVIEW

Incident ID: [INC-364](#)

Created: 10/11/2018 08:23:39 pm

Last Updated: 10/11/2018 08:23:39 pm

Priority:

Status:

Assignee: IanRSA

Description

This is remediation task AAA-1234.



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.
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.

Field	Description
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.

Add/Remove from List

Click on Save to update the list(s). Refresh the page to view the updates.

META VALUE

1

Create New List 2

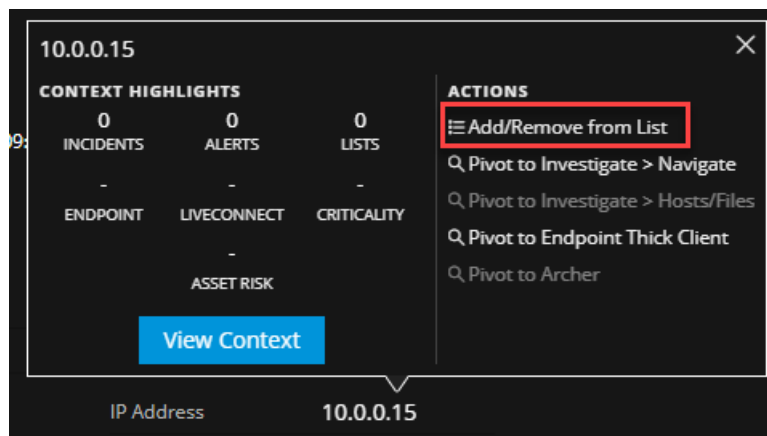
ALL SELECTED UNSELECTED 3 Filter Results 4

LIST	DESCRIPTION
<input type="checkbox"/> Threat	This list is created and updated automatically by the feed Threat. If you make changes to this list, please be aware that the changes will be overwritten when the feed updates.
<input type="checkbox"/> CorporateUsers	This list is created and updated automatically by the feed CorporateUsers. If you make changes to this list, please be aware that the changes will be overwritten when the feed updates.
<input type="checkbox"/> IP_Whitelist	
<input type="checkbox"/> SpearPhishing	This list is created and updated automatically by the feed SpearPhishing. If you make changes to this list, please be aware that the changes will be overwritten when the feed updates.

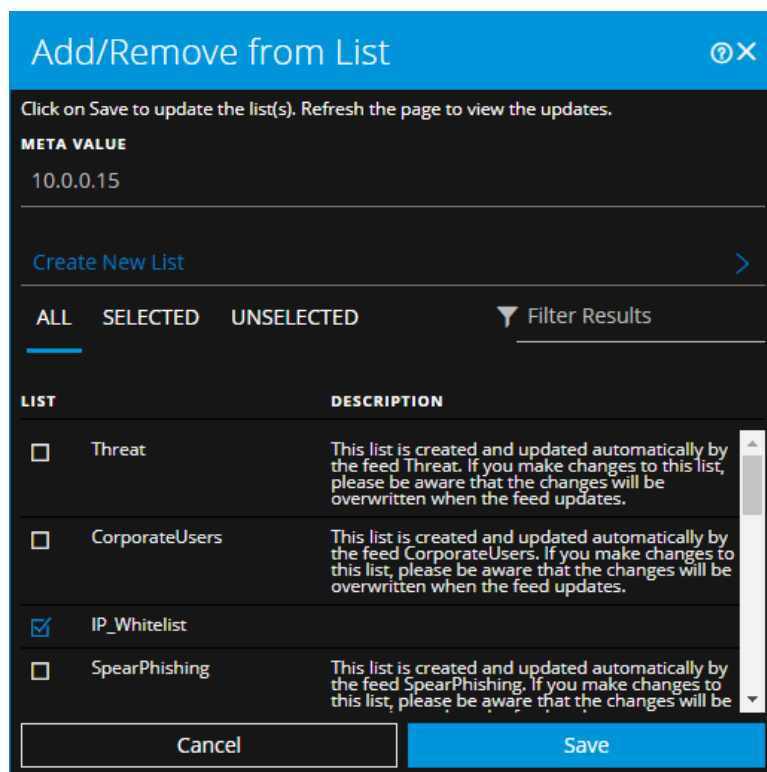
Cancel 5 Save 6

- 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.

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.

Option	Description
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.
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 tabs are: List data source, Archer, Active Directory, Endpoint, Incidents, Alerts, and Live Connect. The following figure shows the Context Lookup panel for a selected entity in the Incident Details view with the Incidents tab in view.

CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
04/24/2018 11:33:50 am (2 days ago)	CRITICAL	90	INC-50	Incident for CH	ASSIGNED	admin	2
04/23/2018 11:33:50 am (3 days ago)	CRITICAL	90	INC-49	Incident for CH	ASSIGNED	admin	2
04/22/2018 11:33:50 am (4 days ago)	CRITICAL	90	INC-48	Incident for CH	ASSIGNED	admin	2
04/21/2018 11:33:50 am (5 days ago)	CRITICAL	90	INC-47	Incident for CH	ASSIGNED	admin	2
04/20/2018 11:33:50 am (6 days ago)	CRITICAL	90	INC-46	Incident for CH	ASSIGNED	admin	2
04/19/2018 11:33:50 am (7 days ago)	CRITICAL	90	INC-45	Incident for CH	ASSIGNED	admin	2

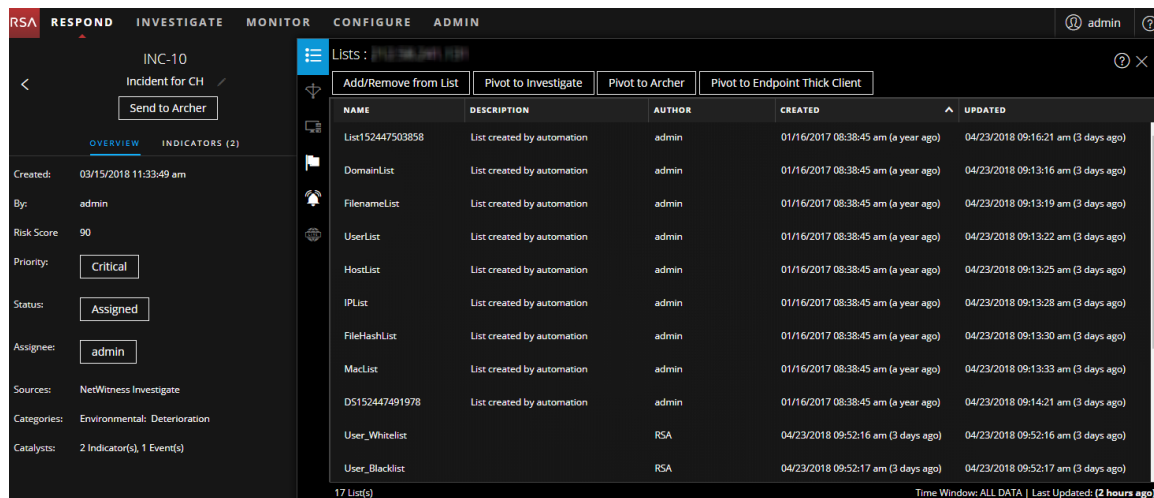
The following table describes the data available on each tab and the supported entities.

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, Host, and Mac
 (Active Directory)	Displays all user information for the selected user.	User
 (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 IIOC score to lowest IIOC score and IIOC levels are sorted by highest IIOC levels to lowest IIOC 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

Tab	Description	Supported 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
 (File Reputation)	Displays file reputation status for Filehash entities.	Filehash entities

Lists Tab

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, and the table describes the fields.



NAME	DESCRIPTION	AUTHOR	CREATED	UPDATED
List152447503858	List created by automation	admin	01/16/2017 08:38:45 am (a year ago)	04/23/2018 09:16:21 am (3 days ago)
DomainList	List created by automation	admin	01/16/2017 08:38:45 am (a year ago)	04/23/2018 09:13:16 am (3 days ago)
FilenameList	List created by automation	admin	01/16/2017 08:38:45 am (a year ago)	04/23/2018 09:13:19 am (3 days ago)
UserList	List created by automation	admin	01/16/2017 08:38:45 am (a year ago)	04/23/2018 09:13:22 am (3 days ago)
HostList	List created by automation	admin	01/16/2017 08:38:45 am (a year ago)	04/23/2018 09:13:25 am (3 days ago)
IPList	List created by automation	admin	01/16/2017 08:38:45 am (a year ago)	04/23/2018 09:13:28 am (3 days ago)
FileHashList	List created by automation	admin	01/16/2017 08:38:45 am (a year ago)	04/23/2018 09:13:30 am (3 days ago)
MacList	List created by automation	admin	01/16/2017 08:38:45 am (a year ago)	04/23/2018 09:13:33 am (3 days ago)
DS152447491978	List created by automation	admin	01/16/2017 08:38:45 am (a year ago)	04/23/2018 09:14:21 am (3 days ago)
User_Whitelist		RSA	04/23/2018 09:52:16 am (3 days ago)	04/23/2018 09:52:16 am (3 days ago)
User_Blacklist		RSA	04/23/2018 09:52:17 am (3 days ago)	04/23/2018 09:52:17 am (3 days ago)

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.

Field	Description
Time Window	The time window based on the value 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 Tab

The Context Lookup panel for Archer displays asset information along with criticality ratings using the Archer data source for IP, Host, and Mac entities. The following figure is an example of the Context Lookup panel for Archer, and the table describes each field.

The screenshot shows the NetWitness Respond interface with the Archer tab selected. The left sidebar displays a list of incidents, including 'INC-10 Incident for CH' and 'NetWitness Investigate Incident for CH'. The main panel shows the asset details for 'ECAT-WIN-2008' with the following information:

CRITICALITY RATING	RISK RATING	DEVICE NAME	HOSTNAME
High	High	ECAT-WIN-2008	ftp.netwitness.com
INTERNAL IP ADDRESS	DEVICE ID	DEVICE TYPE	MAC ADDRESS
66.104.20.243	224935	Fibre Channel SAN Switch	00:13:E8:AF:68:0F
FACILITY	BUSINESS UNIT	DEVICE OWNER	BUSINESS PROCESSES
Austin D2	US-Finance,Payroll	1, Admin1,2, admin	Busi. Process 1,Busi. Process 2

At the bottom of the panel, it indicates '1 Asset' and 'Time Window: ALL DATA | Last Updated: (a few seconds ago)'.

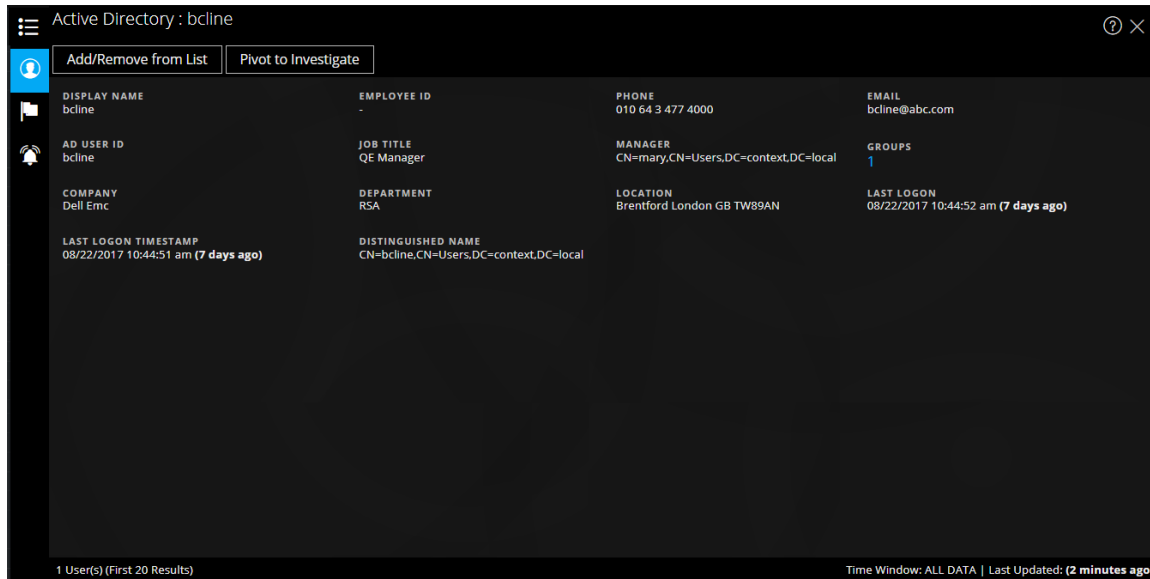
Field	Description
Criticality Rating	The device operational criticality based on the applications it supports. The criticality ratings can be set as Not Rated, Low, Medium-Low, Medium, Medium-High, or High.
Risk Rating	The calculated risk rating for the device based on the most recent assessment and the average risk rating of facilities using the device. The risk rating can be set as Severe, High, Medium, Low, or Minimal.
Device Name	The unique name of the device.
Host Name	The host name of the device.
IP Address	The primary internal IP address of the device.
Device ID	The automatically populated value that uniquely identifies the record across all applications within the system.
Type	The device type, for example, server, laptop, desktop, and others.
Facilities	Links to records in the Facilities application that are related to this device.
Business Unit	Links to records in the Business Unit application that are related to this device. For more than three business unit values, you can hover over the field to view the values.

Field	Description
Device Owner	The person who is responsible for the device and receives read and update rights of the record.
Count	The number of assets available.
Time Window	The time window 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.

Note: In the localized versions, only these twelve fields are displayed: Criticality Rating, Risk Rating, Device Owner, Business Unit, Host Name, MAC Address, Facilities, IP Address, Type, Device ID, Device Name, and Business Processes.

Active Directory Tab

The following figure is an example of a Context Lookup 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.

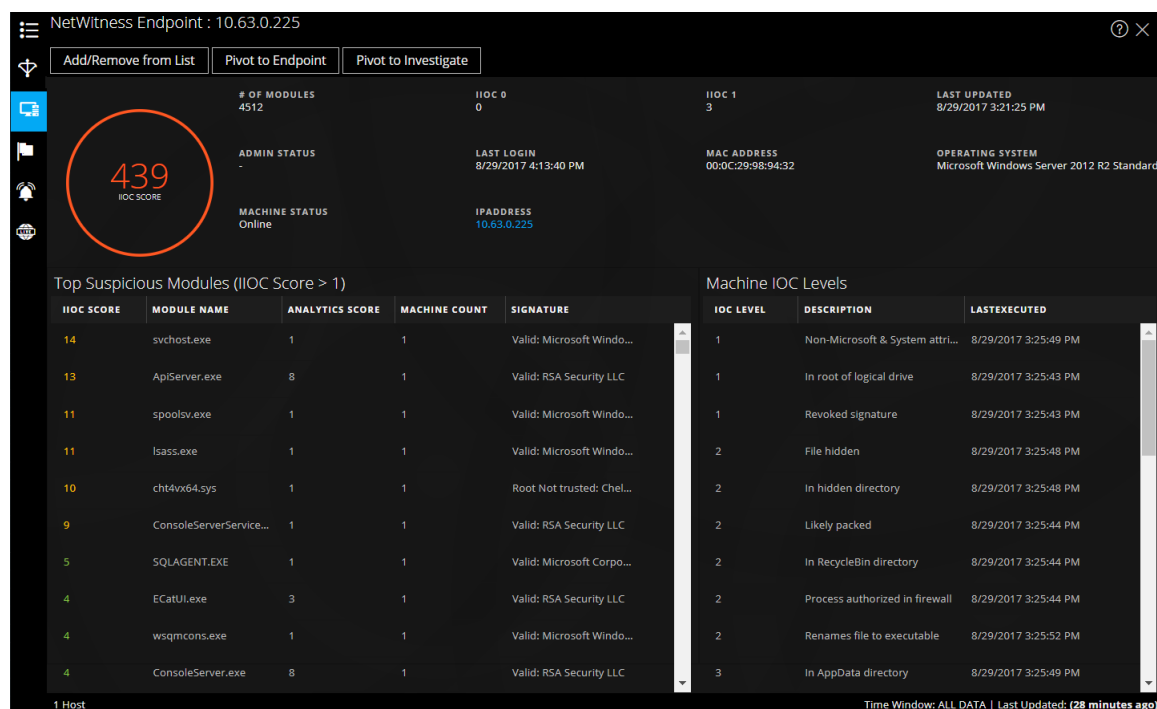
The following information is displayed for Active Directory.

Field	Description
Display Name	The name of the user.
Employee ID	The employee ID of the user.
Phone	The phone number of the user.
Email	The email ID of the user.
AD User ID	The unique identification of the user within an organization.
Job Title	The designation of the user.
Manager	The name of the user's manager.
Groups	The list of groups of which the user is a member.
Company	The name of the user's company.

Field	Description
Department	The department name to which the user belongs within the organization.
Location	The location of the user.
Last Logon	The time when the user logged into the system, only if the Global Catalogue is defined.
Last Logon TimeStamp	The time when the user logged into the system.
Distinguished Name	The unique name assigned to the user.
Count	The number of users.
Time Window	The time window 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 Tab

The following figure is an example of the Context Lookup panel for NetWitness Endpoint.



The following information displayed for IIOCs.

Field	Description
# Of Modules	The number modules that are looked up.

Field	Description
Admin Status	The admin status (if any).
Last Updated	The time when the data was last refreshed.
Last Login	The time when the user last logged in.
MAC Address	The Machine MAC Address.
Operating System	The Version of the Operating System used by the NetWitness Endpoint machine.
Machine Status	The state of the module being viewed: Online, Offline, Active, or Inactive.
IP Address	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 dialog. The default value for Minimum IIOC Score is 500. See "Configure Context Hub Data Source Settings" in the <i>Context Hub Configuration Guide</i> .
Module Name	The name of the module that is being looked up.
Analystic Score	The number of active files for the selected machine.
Machine Count	The number of machines on which that particular IOC got triggered.
Signature	Indicator of whether the file is signed or unsigned, valid or invalid, and signatory information. For example, Google, Apple, and so on.

The following information is displayed for machines.

Field	Description
IOC Levels	The IOC levels.
Description	The description for the IOC level if available.
Last executed	The time when the action was executed.
Count	The number of hosts that are being looked up.
Time Window	The time window based on the value set for the Query Last field in the Configure Data Source Settings dialog. By default, all data for NetWitness Endpoint is fetched.
Last Updated	The time when scan results were last updated in NetWitness Endpoint database.

Alerts Tab

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...
04/24/2018 11:33:50 am (5 days...	90	Incident for CH	NetWitness Investigate	1	INC-50
04/23/2018 11:33:50 am (6 days...	90	Incident for CH	NetWitness Investigate	1	INC-49
04/22/2018 11:33:50 am (7 days...	90	Incident for CH	NetWitness Investigate	1	INC-48
04/22/2018 11:33:50 am (7 days...	90	Incident for CH	NetWitness Investigate	1	INC-48

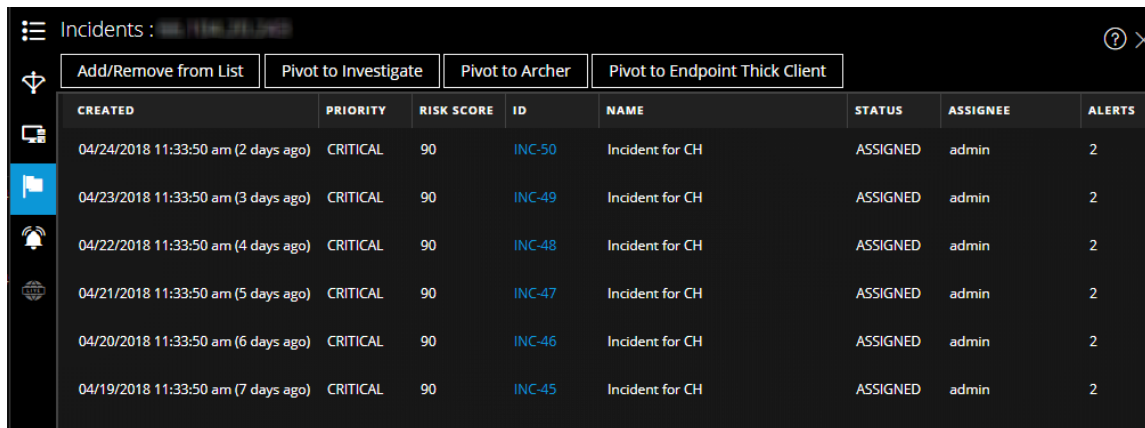
4 Alert(s) (First 50 Results) Time Window: 7 DAYS | Last Updated: (a minute ago)

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

Field	Description
Created	The date and time when the alert was created.
Severity	The severity value of the alerts.
Name	The name of the alert. You can click the name to view the details of a specific alert.
Source	The alert source name from which the alert is triggered.
#Events	The number of events associated with the alert.
Incident ID	The ID of the incident (if any) with which the alert is associated. You can click the ID to view the details of a specific alert.
Count	The number of alerts. By default only the first 100 alerts are displayed. For more information on how to configure the settings, see "Configure Context Hub Data Source Settings" in the <i>Context Hub Configuration Guide</i> .
Time Window	The time window based on the value 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	The time when contextual data was last fetched from data source.

Incidents Tab

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.



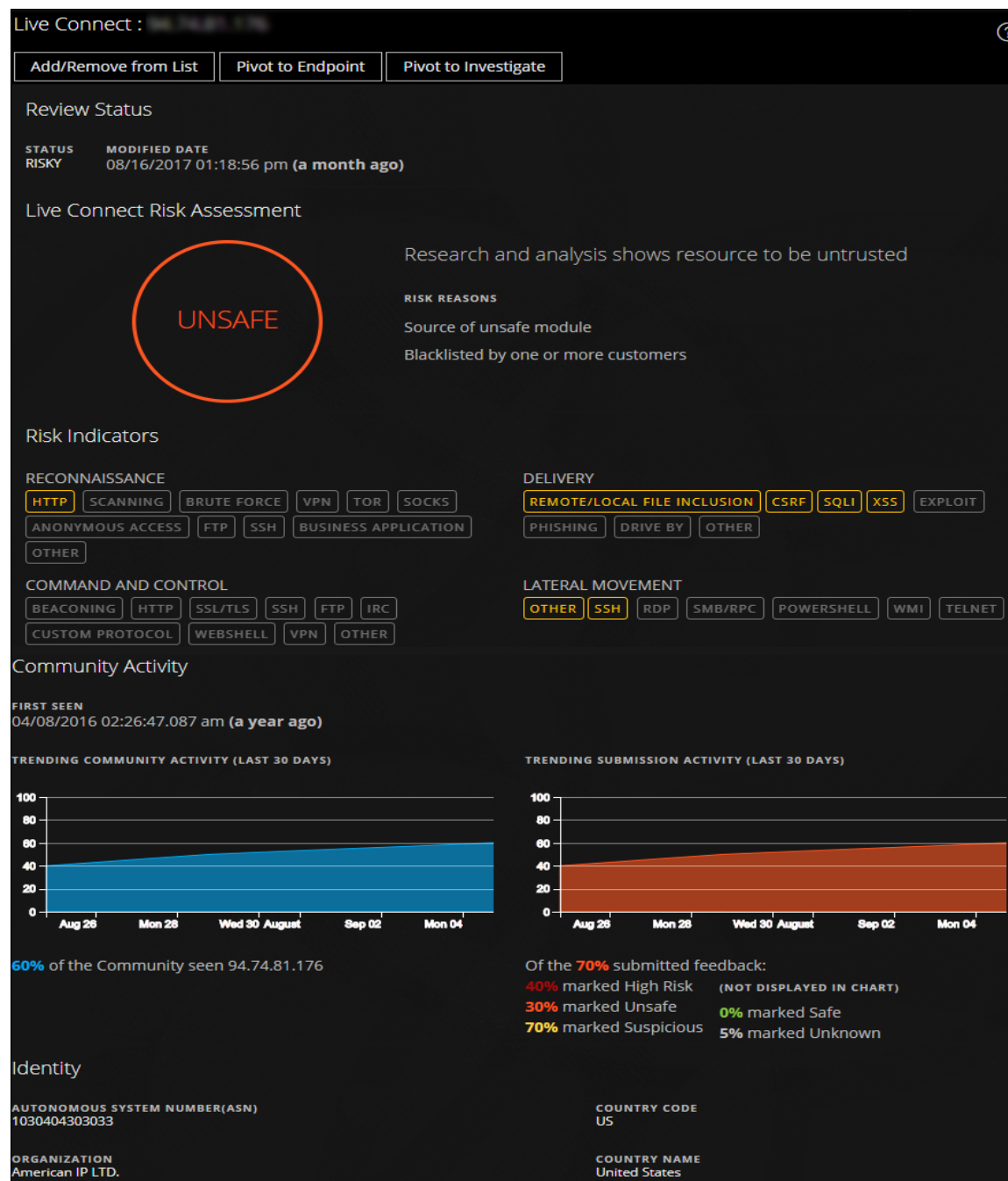
CREATED	PRIORITY	RISK SCORE	ID	NAME	STATUS	ASSIGNEE	ALERTS
04/24/2018 11:33:50 am (2 days ago)	CRITICAL	90	INC-50	Incident for CH	ASSIGNED	admin	2
04/23/2018 11:33:50 am (3 days ago)	CRITICAL	90	INC-49	Incident for CH	ASSIGNED	admin	2
04/22/2018 11:33:50 am (4 days ago)	CRITICAL	90	INC-48	Incident for CH	ASSIGNED	admin	2
04/21/2018 11:33:50 am (5 days ago)	CRITICAL	90	INC-47	Incident for CH	ASSIGNED	admin	2
04/20/2018 11:33:50 am (6 days ago)	CRITICAL	90	INC-46	Incident for CH	ASSIGNED	admin	2
04/19/2018 11:33:50 am (7 days ago)	CRITICAL	90	INC-45	Incident for CH	ASSIGNED	admin	2

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

Field	Description
Created	The date when the incident was created.
Priority	The priority status of the incidents.
Risk Score	The risk score of the incidents.
ID	The Incident ID of the incident. You can click on the ID to display further details about the incident.
Name	The incident name.
Status	The status of the incident
Assignee	The current owner of the incident.
Alerts	The number of alerts associated with the incident.
Count	The number of incidents. By default only the first 100 incidents are displayed. For more information on how configure the settings, see "Configure Context Hub Data Source Settings" in the <i>Context Hub Configuration Guide</i> .
Time Window	The time window based on the value 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	The time when contextual data was last fetched from data source.

Live Connect Tab

The following figure is an example of a Context Panel for Live Connect, and the table describes the information displayed.



Field	Description
Review Status	<p>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: Lookup results for an IP address are viewed for the first time within the organization. • Viewed: Any analyst within the organization has already viewed the lookup results for an IP address. • Marked as Safe: Any analyst within the organization has already viewed the lookup results and marked the IP address as safe. • Marked as Risky: Any analyst within the organization has already viewed the lookup results and marked the IP address as risky.
Risk Assessment	<p>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. Entities marked as high risk require 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 unsafe 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

Risk Assessment Feedback allows the analyst to submit threat intelligence feedback about an entity to the Live Connect server.

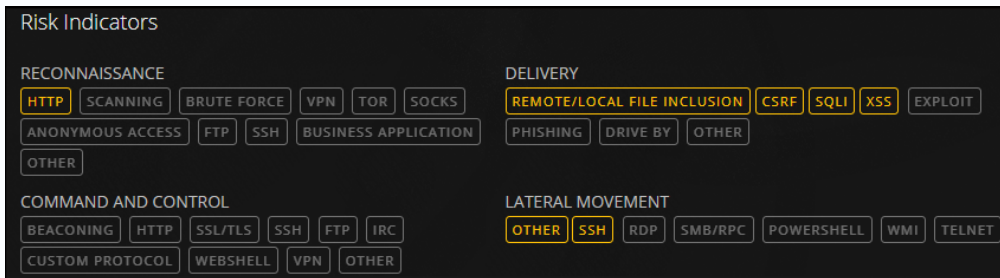
- **Analyst Skill Level**

Below are the Analyst skill level options:

- **Tier 1** - Analysts at this level define procedures for remediation, and decide if an incident should be escalated to other areas in a Security Operation center (SOC). This is the default value.
- **Tier 2** - Analysts who investigate incidents and capture intelligence from an investigation to feed back into the various workflows in a SOC.
- **Tier 3** - Analysts who share the investigation results to the SOC organization. They generally manage incidents and have a wide breadth and depth of skills and tools necessary for incident response.

Note: While creating a new user for NetWitness Platform (Analyst), an administrator should be able to identify the user as Tier 1, Tier 2, or Tier 3 Analyst.

- **Risk Confirmation** - The risk confirmation for the selected Live Connect entity (IP, file, or domain). The Risk confirmation categories are:
 - **Safe:** The Live Connect entity is considered to be safe.
 - **Unknown:** The analyst does not have enough information to provide a risk confirmation
 - **High Risk:** Marked as high risk based on the analysis and risk reasons provided by the community. Entities marked as high risk require 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 unsafe based on the analysis and risk reasons provided by the community.
- **Confidence Level** - The confidence level of an analyst in providing feedback for the Live Connect entity. The confidence level categories are: High, Medium, and Low.
- **Risk Indicator Tags** - Allows you to select a tag category based on the analysis.

Field	Description
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.
Risk Indicators	 <p>Risk indicators are highlighted based on the tags that are assigned by the community to the entities (IPs, Files, or Domains).</p> <p>The tags are categorized as follows: Reconnaissance, Delivery, Command and Control, Lateral Movement, Privilege Escalation, and Packaging and Exfiltration.</p> <p>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.</p>
Identity	<p>Provides the following identity information for the selected entity or meta value:</p> <p>For IP address: Autonomous System Number (ASN), Prefix, Country Code and Country Name, Registrant (Organization), and Date.</p> <p>For File Hash: File Name, File Size, MD5, SH1, SH256, Compile Time, and Mime Type.</p> <p>For Domain: Domain Name and Associated IP Address.</p>
Certificate Information	<p>Provides the following certificate information for the selected file hash: Certificate Issuer, Validity of the Certificate, Signature Algorithm, and Certificate Serial Number.</p>

Field	Description																		
WHO IS Information	<div><div><div>WHOIS</div><table><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></div> <p>The WHO IS information provides the ownership details for a given domain.</p> <p>The following information about the domain owner is displayed: Created Date, Updated Date, Expired Date, Type (Registration Type), Name, Organization, Address with Postal code, Country, Phone, Fax, and Email.</p>	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.																			
Related Files	Related Files are displayed for entity types IP and Domain. A list of known associated files is displayed along with the following information: Live Connect Risk Rating (Safe, Risky, or Unknown), File Name, MD5, Compile Time and Date, API Function, Import Hash, and Mime Type.																		
Related Domains	Related Domains are displayed for entity types IP and Files. A list of known associated domains is displayed along with the following information: Live Connect Risk Rating (Safe, Risky, or Unknown), Domain Name, Country Name, Registered Date, Expired Date, and Registrant Email address.																		

Field

Description

Related IPs

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	2ymh2gnnbg6pgq2r.gre...		09/22/2017 10:59:25 ...	09/22/2017 10:59:25 ...	

Related IPs are displayed for entity types Domain and Files. A list of known associated IPs is 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, and Registrant Email address.

File Reputation Tab

The Context Lookup panel for File Reputation displays the file reputation status of a file.

CONFIGURE ADMIN

admin

File Reputation : 64ff3472497e2a1a7df1c45febdde051

Add/Remove from List

Pivot to Investigate > Navigate

File Reputation : 141b2190f51397dbd0dfde0e3904b264c91b6f81febc823...

Add/Remove from List

Pivot to Investigate > Navigate

REPUTATION STATUS Malicious	SCANNER MATCH 2	CLASSIFICATION PLATFORM Win32	CLASSIFICATION TYPE PUA
CLASSIFICATION FAMILY Psexec			

Field	Description
Reputation Status	Reputation Status of filehash. For more information about reputation status, see <i>"View Reputation of files"</i> in the Investigate User Guide.

Field	Description
Scanner Match	Number of scanners that detected malware or suspicious activity in the last scan.
Classification Platform	Classification for the queried filehash based on the platform. For example, the platform can be Win 32.
Classification Type	Classification for the queried filehash based on the type.
Classification Family	Classification for the queried filehash based on the malware family name.